**ELK STACK**

* ELK Stack là một bộ công cụ phần mềm mã nguồn mở được sử dụng để quản lý log tập trung trong hệ thống microservice hoặc bất kỳ ứng dụng phân tán nào khác. ELK là viết tắt của ba thành phần chính trong bộ công cụ này: Elasticsearch, Logstash và Kibana
  + Elaticsearch: Trong ELK Stack, Elasticsearch đóng vai trò chính là nơi lưu trữ dữ liệu, bao gồm cả log, và cung cấp các tính năng mạnh mẽ để tìm kiếm, phân tích và truy xuất dữ liệu một cách nhanh chóng
  + Logstash: Logstash là một công cụ giúp thu thập, xử lý và chuyển đổi dữ liệu từ nhiều nguồn vào Elasticsearch. Nó có thể nhận dữ liệu từ nhiều nguồn khác nhau như log hệ thống, cơ sở dữ liệu, thông tin từ các ứng dụng và sau đó xử lý dữ liệu này để chuẩn hóa và định dạng lại trước khi gửi tới Elasticsearch
  + Kibana: Là một giao diện web đồ họa để trực quan hóa và thao tác dữ liệu được lưu trữ trong Elasticsearch
* Flow:

A diagram of a data processing process

Description automatically generated

* + Đầu tiên, log sẽ được đưa đến Logstash. (Thông qua nhiều con đường, ví dụ như server gửi UDP request chứa log tới URL của Logstash, hoặc Beat đọc file log và gửi lên Logstash)
  + Logstash sẽ đọc những log này, thêm những thông tin như thời gian, IP, parse dữ liệu từ log (server nào, độ nghiêm trọng, nội dung log) ra, sau đó ghi xuống database là Elasticsearch
  + Khi muốn xem log, người dùng vào URL của Kibana. Kibana sẽ đọc thông tin log trong Elasticsearch, hiển thị lên giao diện cho người dùng query và xử lý
* Lý do sử dụng ELK Stack: Với các hệ thống hoặc ứng dụng nhỏ, ta không cần giao mổ trâu đi giết gà làm gì, cứ ghi log ra file hoặc stdout của hệ thống là được Tuy nhiên với hệ thống lớn, gồm nhiều services lại là câu chuyện khác:
  + Quản lý log tập trung: Thay vì phải lọ mọ vào từng servers xem log thì chúng ta chỉ cần mở kibana trên trình duyệt web là có thể xem được log của tất cả các servers rồi
  + Dễ dàng tích hợp: dù chúng ta có dùng Nginx hay Apache, dùng MSSQL, MongoDB hay Redis, Logstash đều có thể đọc hiểu và xử lý log của chúng ta nên việc tích hợp rất dễ dàng
  + Search và filter mạnh mẽ: Elasticsearch cho phép lưu trữ thông tin kiểu NoSQL, hỗ trợ luôn Full-Text Search nên việc query log rất dễ dàng và mạnh mẽ, ngay cả với dữ liệu log cực kì lớn
  + Scale dễ dàng: Khi muốn xử lý nhiều log hơn, chúng ta chỉ việc tăng số nodes của Elasticsearch hoặc Logstash lên là xong
  + Dễ dàng triển khai và hoàn toàn miễn phí: Chúng ta có thể chạy bộ 3 này trên 1 server duy nhất, và không tốn tiền bản quyền vì các phần mềm này đều là mã nguồn mở + free
  + Cộng đồng mạnh, tutorial nhiều
* Demo ELK Stack:

Check Elastic Search server(Sau khi đã run Elastic Search server):

A screenshot of a computer program

Description automatically generated

Check Kibana server (Sau khi đã run Kibana server):

A screenshot of a computer

Description automatically generated

Cấu hình application.properties và controller:



A screen shot of a computer code

Description automatically generated

Run logstash server:

A screenshot of a computer program

Description automatically generated

Trên kibana server:

\*Danh sách các index lưu trữ ở Elastric Search:

A screenshot of a computer

Description automatically generated

\*Tạo pattern để truy cập vào các index mà chúng ta muốn theo dõi:

A screenshot of a computer

Description automatically generated

Truy cập vào “Discorver” để kiểm tra log của các pattern:

A screenshot of a computer

Description automatically generated