DEMO FLUENT-BIT & ELASTICSEARCH

\*\*\* giới thiệu demo: là mô hình mô phỏng đẩy log ngẫu nhiên trong 1 file log của 1 server có cài đặt fluent-bit sang elasticsearch từ xa (không trong server đó)

Mục lục demo:

1. Thành phần

2. Cấu hình

3. Kiểm tra

1. Thành phần

+ VM1: server chứa log cần được đẩy qua fluent-bit

- fluent-bit: lấy log thông qua file testLog.log để đẩy qua elasticsearch trên VM2

+ VM2: server nhận thông tin từ fluent-bit và xử lý tìm kiểm

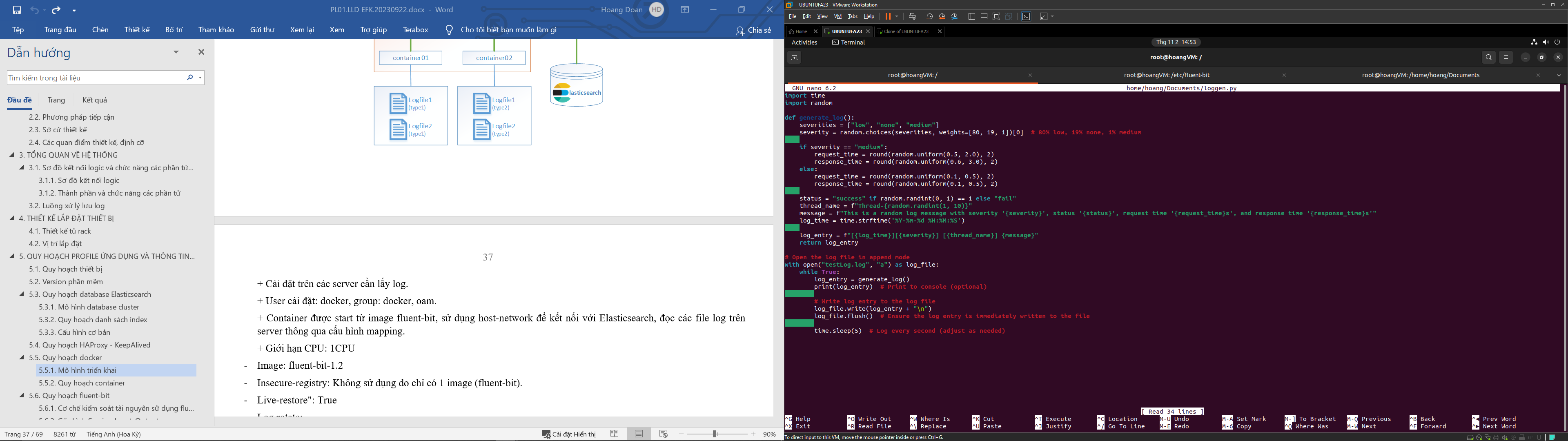
- elasticsearch: nhận log để tìm kiếm

- kibana: UI

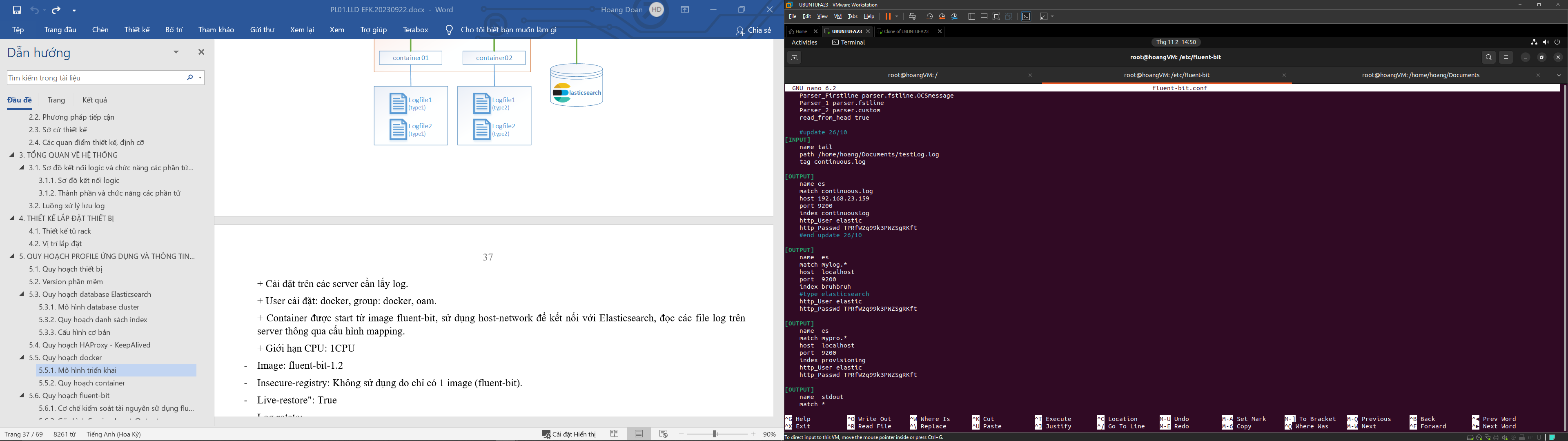
2. Cấu hình

VM1:

- tạo log ngẫu nhiên với file python tên loggen.py và viết vào một file log testLog.log



- fluent-bit: nhận file testLog.log và đẩy sang elasticsearch với địa chỉ IP của VM2



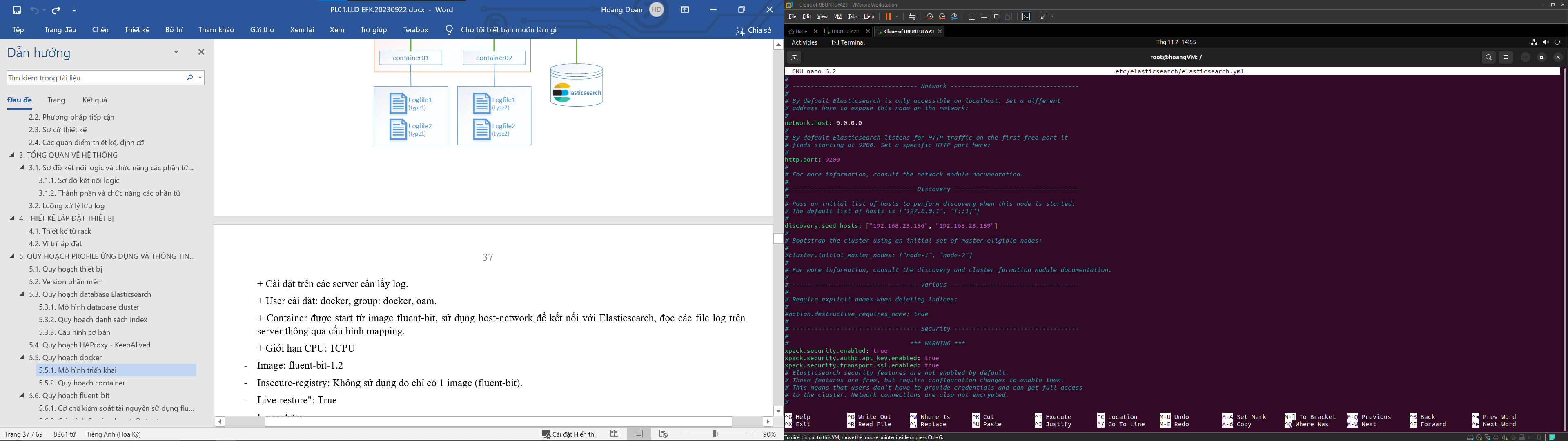
VM2:

- elasticsearch:

+network.host: 0.0.0.0 để elasticsearch có thể nghe được các địa chỉ khác (mặc định localhost -> chỉ nghe được máy chủ)

+ discovery.seed\_hosts: một cài đặt để trỏ đến các node trong cụm (ở đây có VM1 và VM2 vì cả hai đều có elasticsearch)

+ vì có setting bảo mật cho xpack (một extestion cung cấp bảo mật của Elastic Stack) nên sẽ phải set xpack.security.transport.ssl.enabled true (bảo mật cho các node khi giao tiếp)



3. Kiểm tra

- cho chạy file loggen.py để bắt đầu sản sinh log

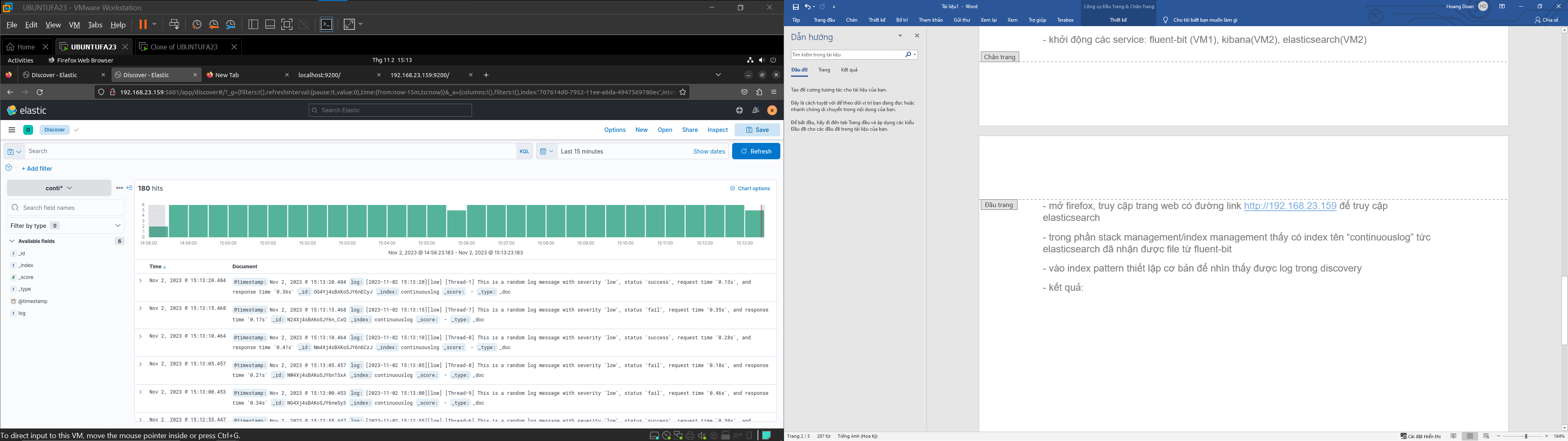
- khởi động các service: fluent-bit (VM1), kibana(VM2), elasticsearch(VM2)

- mở firefox, truy cập trang web có đường link <http://192.168.23.159> để truy cập elasticsearch

- trong phần stack management/index management thấy có index tên “continuouslog” tức elasticsearch đã nhận được file từ fluent-bit

- vào index pattern thiết lập cơ bản để nhìn thấy được log trong discovery

- kết quả:



Vậy là đã thành công.