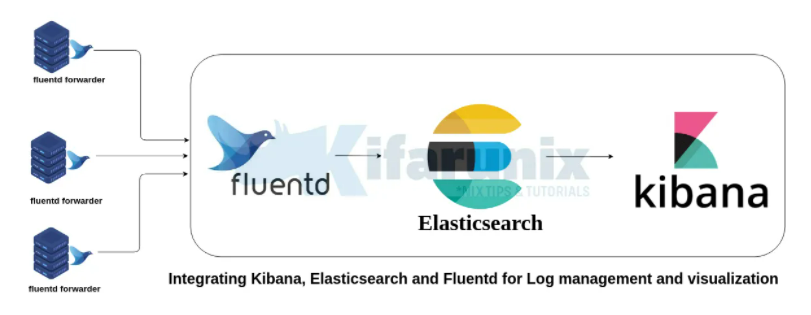
**EFK Stack on Ubuntu**

****

**Cơ chế hoạt động:**

1. Đầu tiên, log sẽ được đưa đến Fluentd.
2. Fluentd 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.
3. 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.
4. Log có nhiều loại (tag), do developer định nghĩa chẳng hạn access\_log error\_log, peformance\_log, api\_log. Khi Fluentd đọc log và phân loại từng loại log rồi gửi đến Elasticsearch, ở giao diện Kibana chúng ta chỉ cần add một số filter như access\_log chẳng hạn và query.

**Tài liệu tham khảo:**

1. [**https://kifarunix.com/setup-kibana-elasticsearch-and-fluentd-on-centos-8/**](https://kifarunix.com/setup-kibana-elasticsearch-and-fluentd-on-centos-8/)
2. [**https://blog.vietnamlab.vn/quan-ly-log-voi-logstash-elasticsearch-kibana/**](https://blog.vietnamlab.vn/quan-ly-log-voi-logstash-elasticsearch-kibana/)
3. **https://docs.fluentd.org/configuration/config-file**

### ****TẠO ÍT NHẤT 2 SERVER UBUNTU:****

***Ubuntu cài EFK nhận logs : 192.168.1.86***

***Ubuntu cài fluentd gửi logs: 192.168.1.87***

**Phần 1: Setup và config**

**Ubuntu cài EFK nhận logs : 192.168.1.86**

**Phải cài jdk:**

**sudo apt update**

**sudo apt install default-jre -y**

**sudo apt install default-jdk -y**

**Cài đặt và cấu hình Elasticsearch**

1. Đưa đầu ra của lệnh cURL vào chương trình apt-key, chương trình này sẽ thêm khóa GPG công khai vào APT.

curl -fsSL https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add -

1. Thêm danh sách nguồn đàn hồi vào thư mục sources.list.d, nơi APT sẽ tìm kiếm các nguồn mới:

echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" | sudo tee -a /etc/apt/sources.list.d/elastic-7.x.list

1. Tiếp theo, cập nhật danh sách gói của bạn để APT sẽ đọc nguồn Elastic mới:

sudo apt update

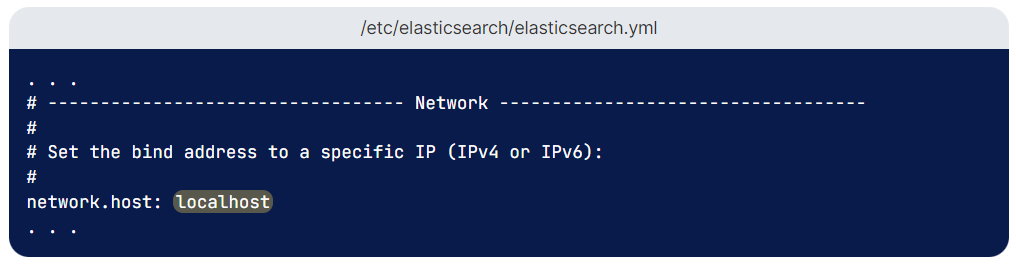
1. Sau đó cài đặt Elasticsearch bằng lệnh này:

sudo apt install elasticsearch

1. Cấu hình Elasticsearch:

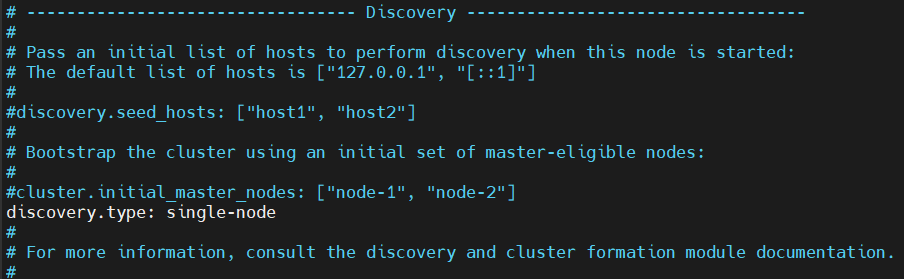
* Để định cấu hình Elasticsearch, sửa tệp cấu hình chính của nó elasticsearch.yml, nơi hầu hết các tùy chọn cấu hình của nó được lưu trữ. Tập tin này nằm trong thư mục /etc/elasticsearch

sudo nano /etc/elasticsearch/elasticsearch.yml



Thay localhost bằng IP của server đang setup: 192.168.1.86

* Vì đang chạy một nút Elasticsearch duy nhất, hãy chỉ định nút tương tự trong cấu hình bằng cách thêm dòng, discovery.type: single-node trong phần Discovery.



* Theo mặc định, **kích thước heap JVM** được đặt ở 1GB. Khuyên bạn nên đặt nó ở kích thước không quá một nửa tổng bộ nhớ RAM của bạn. Mở tệp sau để chỉnh sửa:

sudo nano /etc/elasticsearch/jvm.options



* Bắt đầu dịch vụ Elasticsearch với systemctl. Hãy cho Elasticsearch một chút thời gian để khởi động. Nếu không, bạn có thể gặp lỗi không thể kết nối.

sudo systemctl start elasticsearch

* Tiếp theo, hãy chạy lệnh sau để cho phép Elasticsearch khởi động mỗi khi máy chủ của bạn khởi động:

sudo systemctl enable elasticsearch

## Kiểm tra Elasticsearch

Hiện tại, Elasticsearch sẽ chạy trên cổng 9200. Bạn có thể kiểm tra nó bằng cURL và yêu cầu GET.

curl -X GET “http://***192.168.1.86***:9200”

### Cài đặt và cấu hình Kibana

## Bạn nên cài đặt Kibana tiếp theo. Kibana là một giao diện người dùng đồ họa để phân tích cú pháp và diễn giải các tệp logs đã thu thập.

## Chạy lệnh sau để cài đặt Kibana:

sudo apt-get install kibana

1. Tiếp theo, mở tệp cấu hình **kibana.yml**  để chỉnh sửa:

sudo nano /etc/kibana/kibana.yml

1. Kibana được đặt để chạy trên **localhost: 5601** theo mặc định. Để cho phép truy cập bên ngoài, hãy chỉnh sửa tệp cấu hình và thay thế giá trị của “server.host” bằng một IP giao diện.

sudo nano /etc/kibana/kibana.yml

Xóa dấu # ở đầu các dòng sau để kích hoạt chúng:

#server.port: 5601

#server.host: "your-hostname"

#elasticsearch.hosts: ["http://localhost:9200"]

* Sửa chúng thành:
* server.port: 5601
* server.host: "192.168.1.86"
* elasticsearch.hosts: ["http://192.168.1.86:9200"]

1. Bắt đầu dịch vụ Kibana:

sudo systemctl start kibana

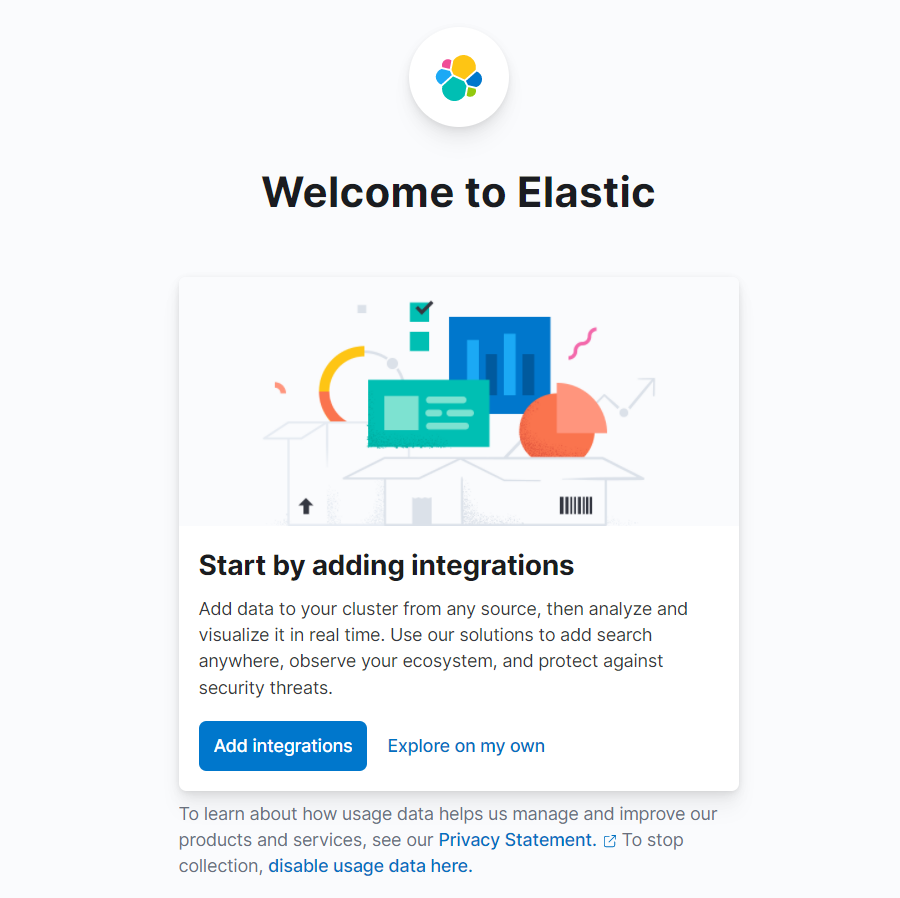
1. Tiếp theo, cấu hình Kibana để khởi chạy khi khởi động:

sudo systemctl enable kibana

### Kiểm tra Kibana

### Để truy cập Kibana, hãy mở trình duyệt web và duyệt đến địa chỉ sau:

http://192.168.1.86:5601



### Cài đặt và cấu hình FLUENTD Aggregator

### (sử dụng bản ổn định td-agent)

### Cài đặt từ Apt Repository

curl -fsSL https://toolbelt.treasuredata.com/sh/install-ubuntu-focal-td-agent4.sh | sh

### Chạy và bật Fluentd td-agent mỗi khi khởi động máy chủ:

sudo systemctl start td-agent

sudo systemctl enable td-agent

1. Cài đặt Plugin Fluentd Elasticsearch

sudo td-agent-gem install fluent-plugin-elasticsearch

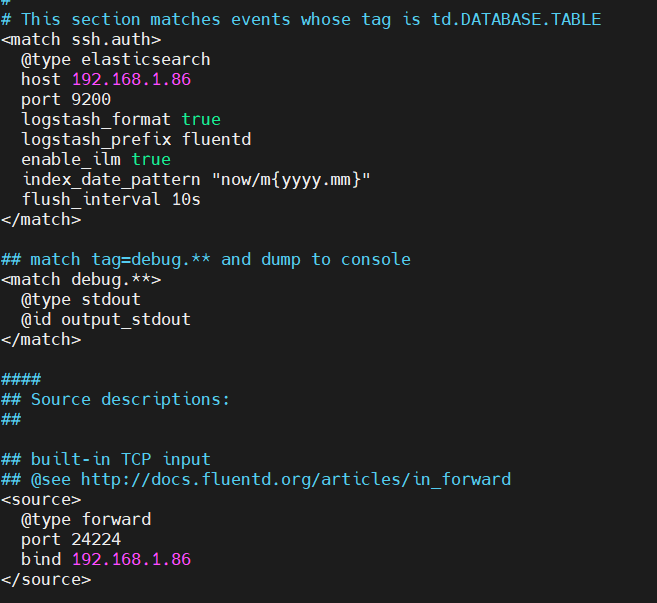
1. Gửi nhật ký đến Fluentd qua Internet, bạn cần cài đặt “**secure\_forward”** plugin đầu ra Fluentd để gửi dữ liệu một cách an toàn

sudo td-agent-gem install fluent-plugin-secure-forward

### Cấu hình [Fluentd Aggregator](https://kifarunix.com/setup-kibana-elasticsearch-and-fluentd-on-centos-8/#configure-fluentd-aggregator-centos-8) (Aggregator là nơi server tập trung logs)

sudo nano /etc/td-agent/td-agent.conf

* Sửa file config đó như sau:
* Host và bind thay bằng địa chỉ IP server các bạn đang setup
* Đoạn <match …> phải để dạng tag abc.xyz tùy sở thích. Vì sau này phần này sẽ phải trùng tag với bên phía server cài Fluentd gửi logs đoạn tag. Vậy nên mình sẽ để là <match ssh.auth>
* VD minh họa (IP server đang setup của mình là 192.168.1.86)



1. Khởi động lại Fluentd td-agent:

sudo systemctl restart td-agent

**Phần 2: Setup và config**

**Ubuntu cài fluentd gửi logs: 192.168.1.87**

### Cài đặt và cấu hình Fluent forwarder

**(Gửi Logs sang FLUENTD Aggregator)**

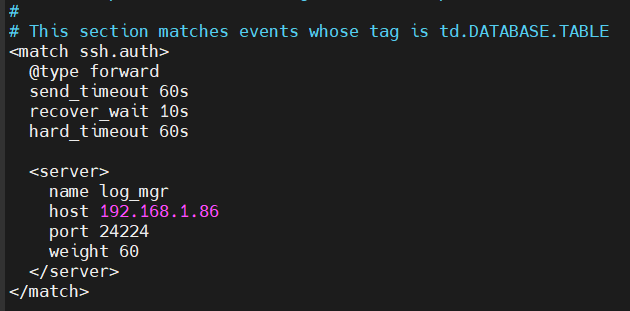
### Cài đặt từ Apt Repository

curl -fsSL https://toolbelt.treasuredata.com/sh/install-ubuntu-focal-td-agent4.sh | sh

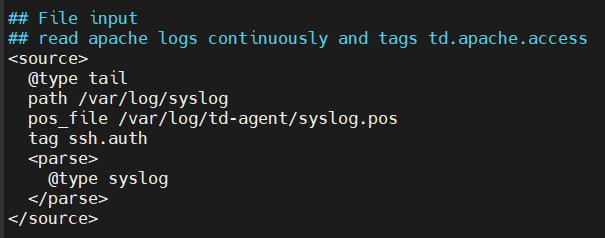
### Cấu hình [Fluentd forwarder](https://kifarunix.com/setup-kibana-elasticsearch-and-fluentd-on-centos-8/#configure-fluentd-aggregator-centos-8) (gửi logs sang FLUENTD Aggregator)

sudo nano /etc/td-agent/td-agent.conf

* Đoạn <match …> phải để tag bên trong là ssh.auth. Có thể xem lại giải thích ở phần FLUENTD Aggregator.



* Kéo xuống bên dưới phần <source> của ## File input
* VD: Chúng ta sửa cấu hình để đọc logs ở đường dẫn /var/log/syslog (các bạn có thể xem các file logs của Ubuntu ở đường dẫn /var/log)
* Chú ý: phần tag phải cùng với phần <match …> bên trên là: ssh.auth



### Cấp quyền đọc file logs cho Fluentd

* Theo mặc định, chỉ root mới có thể đọc logs. Kiểm tra bằng lệnh:

ll /var/log/syslog



* Bây giờ cấp quyền cho group và other quyền đọc file syslog:

sudo chmod og+r /var/log/syslog

* Kiểm tra lại:

ll /var/log/syslog



1. Khởi động lại Fluentd:

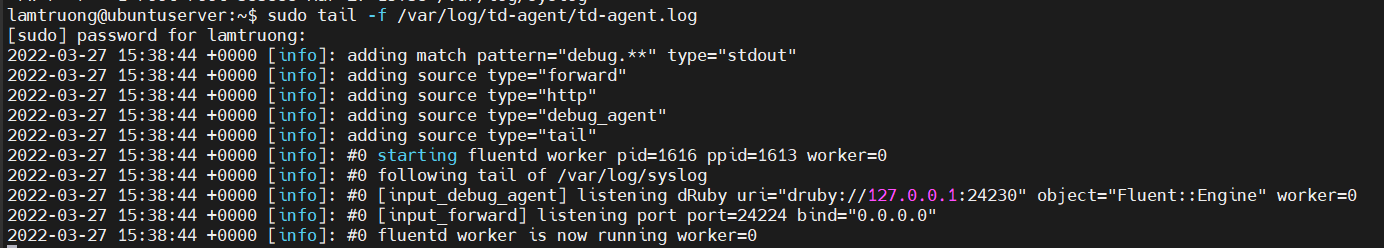
sudo systemctl restart td-agent

**Phần 3: Kiểm tra**

**Test logs trên URL Kibana**

* 1. Trên Ubunu 192.168.1.87 (Fluent forwarder)
  + Kiểm tra xem Fluent đã bắt đầu đọc logs tại /var/log/syslog hay chưa bằng lệnh:

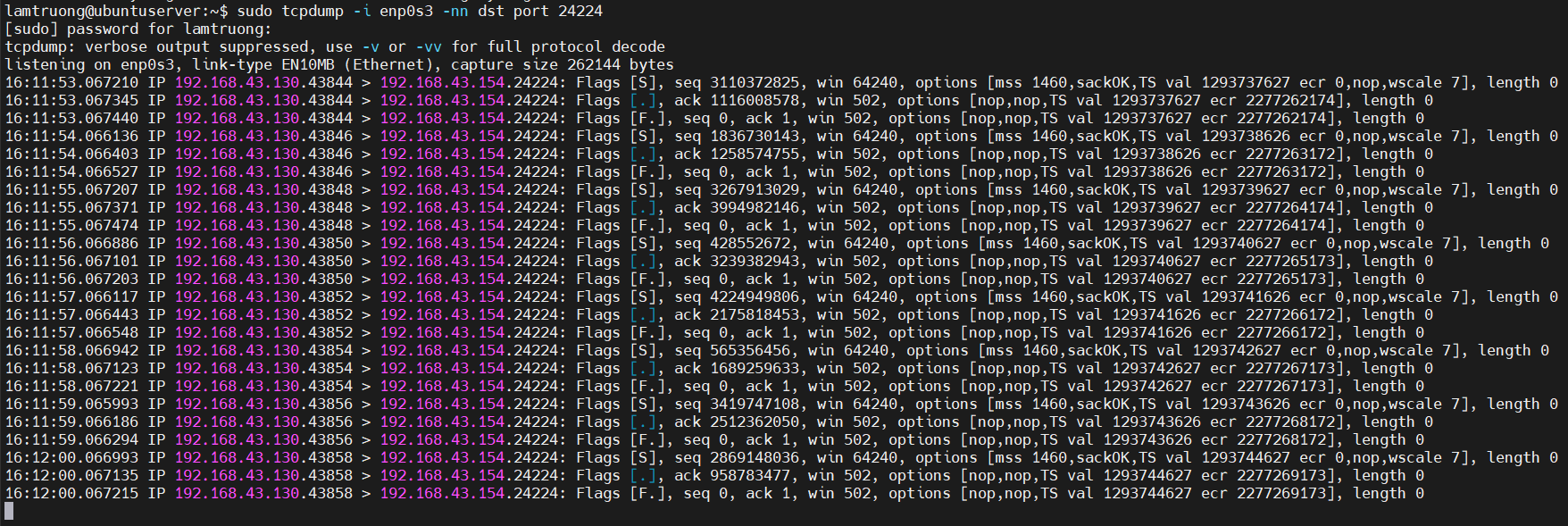
sudo tail -f /var/log/td-agent/td-agent.log



* 1. Trên Ubunu 192.168.1.86 (Fluent Aggregator)
  + Trên máy chủ Ubuntu đang chạy tổng hợp Elasticsearch, Kibana và Fluentd. Bạn có thể kiểm tra xem có bất kỳ dữ liệu nào đang được nhận trên cổng 24224 hay không:

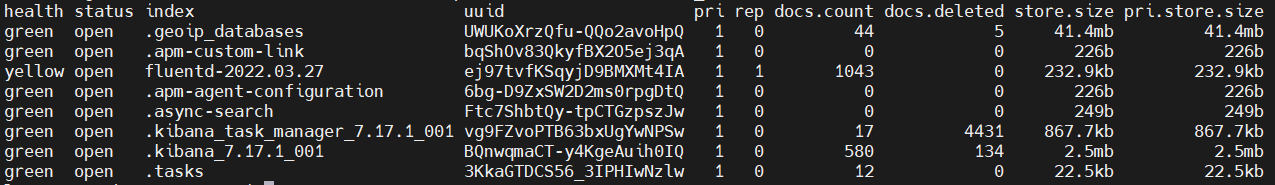
sudo tcpdump -i enp0s3 -nn dst port 24224

* + Card mạng của mình là enp0s3, các bạn có thể xem card mạng bằng lệnh ip a để xem card mạng của server là gì và sử dụng nó (Kiến thức cơ bản khi học về Linux).

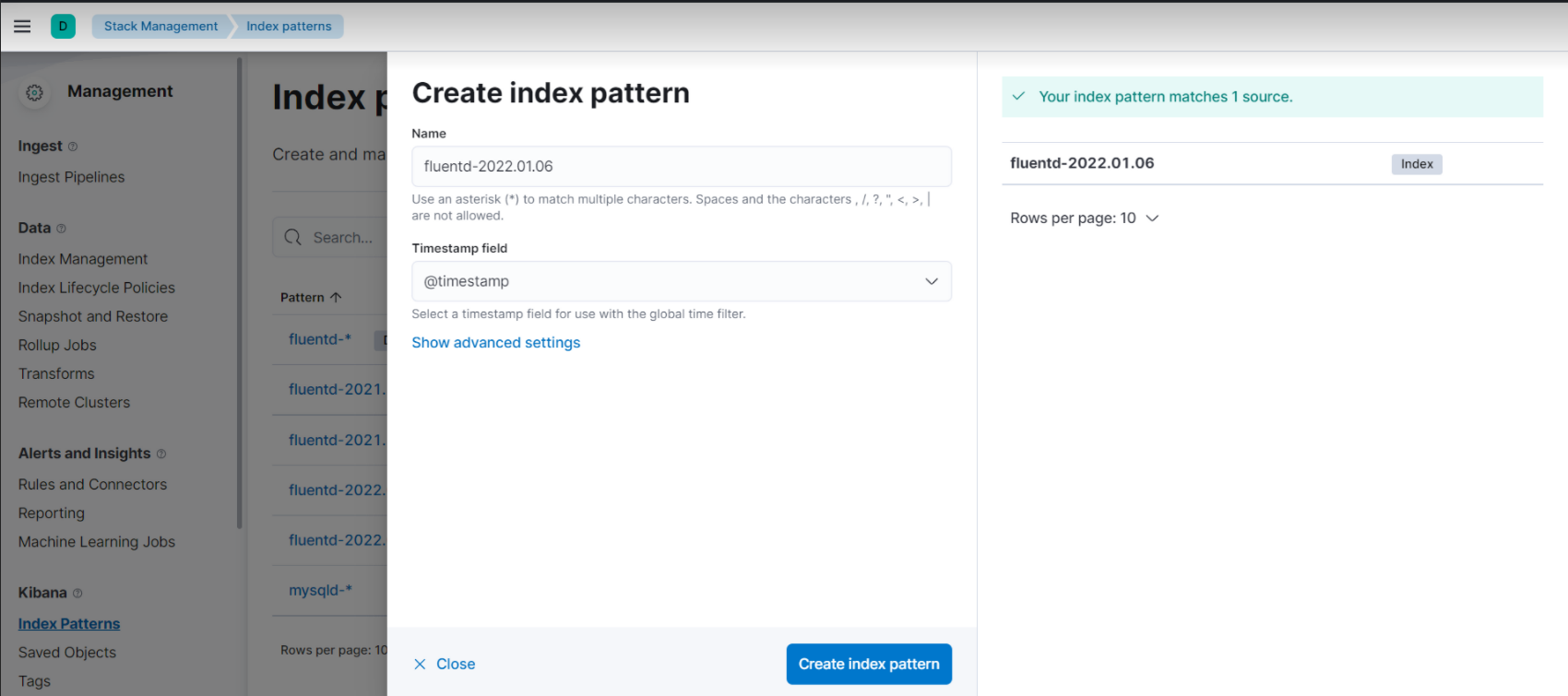


* + Sau đó, hãy kiểm tra xem chỉ mục Elasticsearch của bạn đã được tạo chưa (logstash\_prefix [Chỉ mục] – đoạn này ở phần config FLUENTD Aggregator) bằng lệnh:

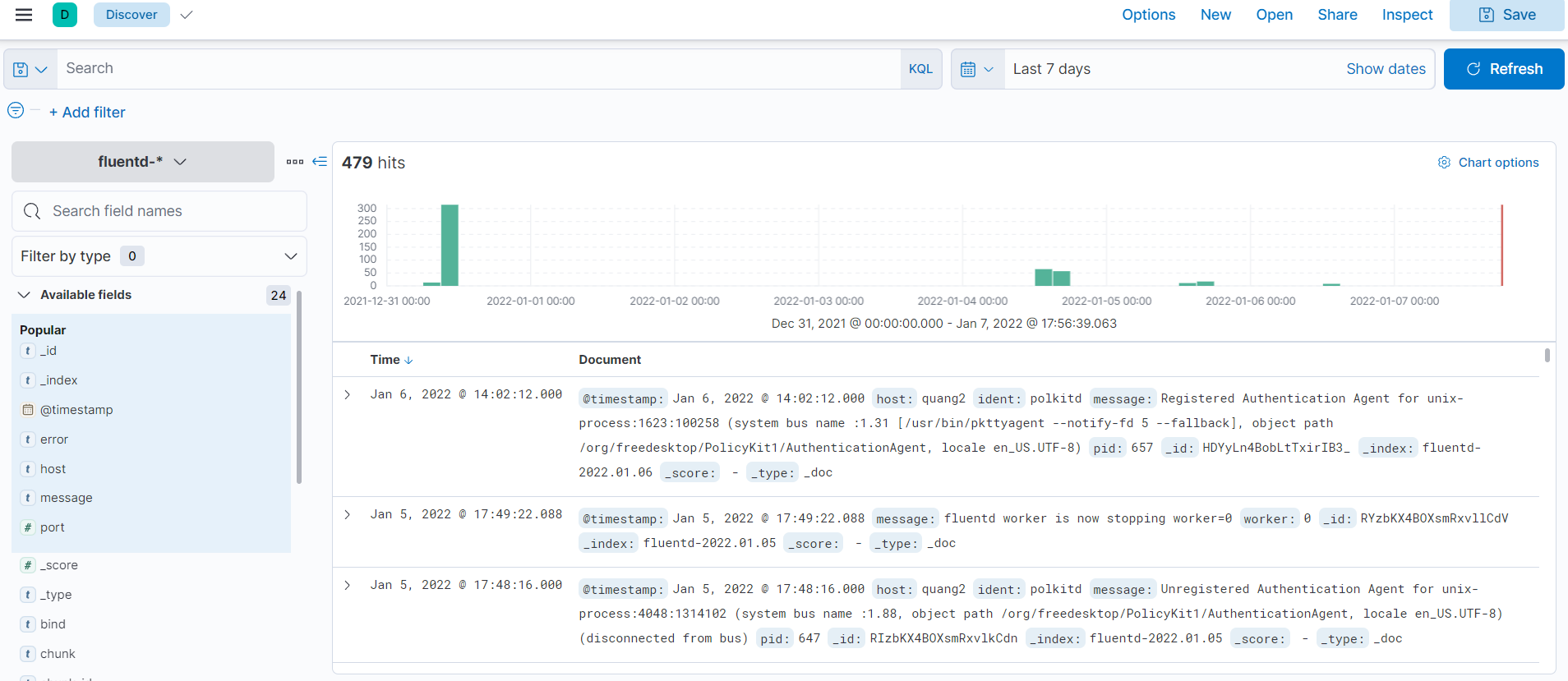
sudo curl -XGET <http://192.168.1.86:9200/_cat/indices?v>



* + - Phần health: yellow đó chính là chỉ mục fluentd do chúng ta đặt tên khi config.
  1. Tạo chỉ mục Fluentd Kibana:
  + Mở trình duyệt và truy cập vào: <http://192.168.1.86:5601>
  + Nhấn vào **tab Management (ở bảng điều khiển phía bên trái) > Kibana> Index Patterns > Create Index Pattern**. Đặt tên cho chỉ mục của bạn
  + Phần **Timestamp field** chọn **@timestamp** **>** **Create index patterm**



* 1. Xem dữ liệu Fluentd trên Kibana:
  + Khi bạn đã tạo chỉ mục Fluentd Kibana, bây giờ bạn có thể xem dữ liệu sự kiện của mình trên Kibana bằng cách nhấp vào tab **Discover** ở bảng điều khiển phía bên trái.



**Đó là toàn bộ bài học. Chúc các bạn thành công!!**