Hướng dẫn cài đặt FileBeat on Ubuntu

Trước khi thực hiện ta thực hiện cập nhật hệ thống lên bản mới nhất theo câu lệnh sau:

**root@10-24-28-87:~# apt-get update -y**

Đầu tiên cài đặt gói cần thiết bằng lệnh sau:

**root@10-24-28-87:~# apt-get install apt-transport-https -y**

Tiếp đến tải xuống và **thêm khoá Elastcic Stack Key** bằng lệnh sau:

**root@10-24-28-87:~# wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo gpg --dearmor -o /usr/share/keyrings/elasticsearch-keyring.gpg**

Tiếp theo thêm kho lưu trữ Elasstic Stack 8 bằng lệnh sau:

**root@10-24-28-87:~# echo "deb [signed-by=/usr/share/keyrings/elasticsearch-keyring.gpg] https://artifacts.elastic.co/packages/8.x/apt stable main" | sudo tee /etc/apt/sources.list.d/elastic-8.x.list**

Tiếp theo thực hiện cập nhật repository và cài đặt filebeat

**root@10-24-28-87:~# apt-get update -y**

**root@10-24-28-87:~# apt-get install filebeat -y**

Sau khi cài đặt xong ta thực hiện cấu hình filebeat. Mặc định filebeat gửi dữ liệu về elasticsearch, bây giờ ta thực hiện cấu hình Filebeat gửi dữ liệu về Logtash bằng cách sửa file /etc/filebeat/filebeat.yml

**root@10-24-28-87:~# nano /etc/filebeat/filebeat.yml**

#-------------------------- General ----------------------

# The name of the shipper that publishes the network data. It can be used to group

# all the transactions sent by a single shipper in the web interface.

#name:

# The tags of the shipper are included in their own field with each

# transaction published.

#tags: ["service-X", "web-tier"]

# ==> Mục địch của việc tạo tags này khi server đẩy log lên logstash nếu có tag là linuxhost thì sẽ đánh index theo cấu hình logstash

# ==> ví dụ khi server cấu hình tags là linuxhost khi đẩy lên logstash sẽ đc đánh index có dạng index => "logstash\_linuxhost\_%{+YYYY.MM.dd}"

**tags: ["linuxhost"]**

#-------------------------- Elasticsearch output ------------------------------

# ==> không sử dụng đẩy log trực tiếp vào elasticsearch nên comment lại

# output.elasticsearch:

# Array of hosts to connect to.

# hosts: ["localhost:9200"]

#----------------------------- Logstash output --------------------------------

# ==> khai báo thông tin logstash gồm địa chỉ logstash và port logstash

**output.logstash:**

**# The Logstash hosts**

**hosts: ["logstash08-anhpt8.citigo.com.vn:31544"]**

Mặc định Filebeat đi kèm với rất nhiều modules. Bạn có thể liệt kê tất cả modules bằng lệnh sau:

**root@10-24-28-87:~# filebeat modules list**

Mặc định tất cả các modules đều bị tắt. Vì vậy bạn phải bật modules hệ thống để thu thập và phân tích các bản ghi được tạo bởi dịch vụ ghi nhật ký hệ thống. Bạn có thể bật modules hệ thống bằng lệnh sau:

**root@10-24-28-87:~# filebeat modules enable system**

Tiếp theo, bạn sẽ cần cấu hình module hệ thống để nhật ký xác thực chỉ đọc. Bạn có thể thực hiện việc này bằng cách chỉnh sửa tệp

**root@10-24-28-87:~# nano /etc/filebeat/modules.d/system.yml**

# Module: system

# Docs: https://www.elastic.co/guide/en/beats/filebeat/7.17/filebeat-module-system.html

- module: system

# Syslog

syslog:

enabled: false

# Set custom paths for the log files. If left empty,

# Filebeat will choose the paths depending on your OS.

#var.paths:

# Authorization logs

**auth:**

**enabled: true**

# Set custom paths for the log files. If left empty,

# Filebeat will choose the paths depending on your OS.

**var.paths: ["/var/log/auth.log"]**

## Config Multi log

#var.paths: ["/var/log/auth.log", "/var/log/syslog"]

Cuối cùng, khởi động dịch vụ **Filebeat** và cho phép nó khởi động sau khi hệ thống khởi động lại bằng lệnh sau:

**root@10-24-28-87:~#** systemctl start filebeat

**root@10-24-28-87:~#** systemctl enable filebeat

**root@10-24-28-87:~#** systemctl status filebeat

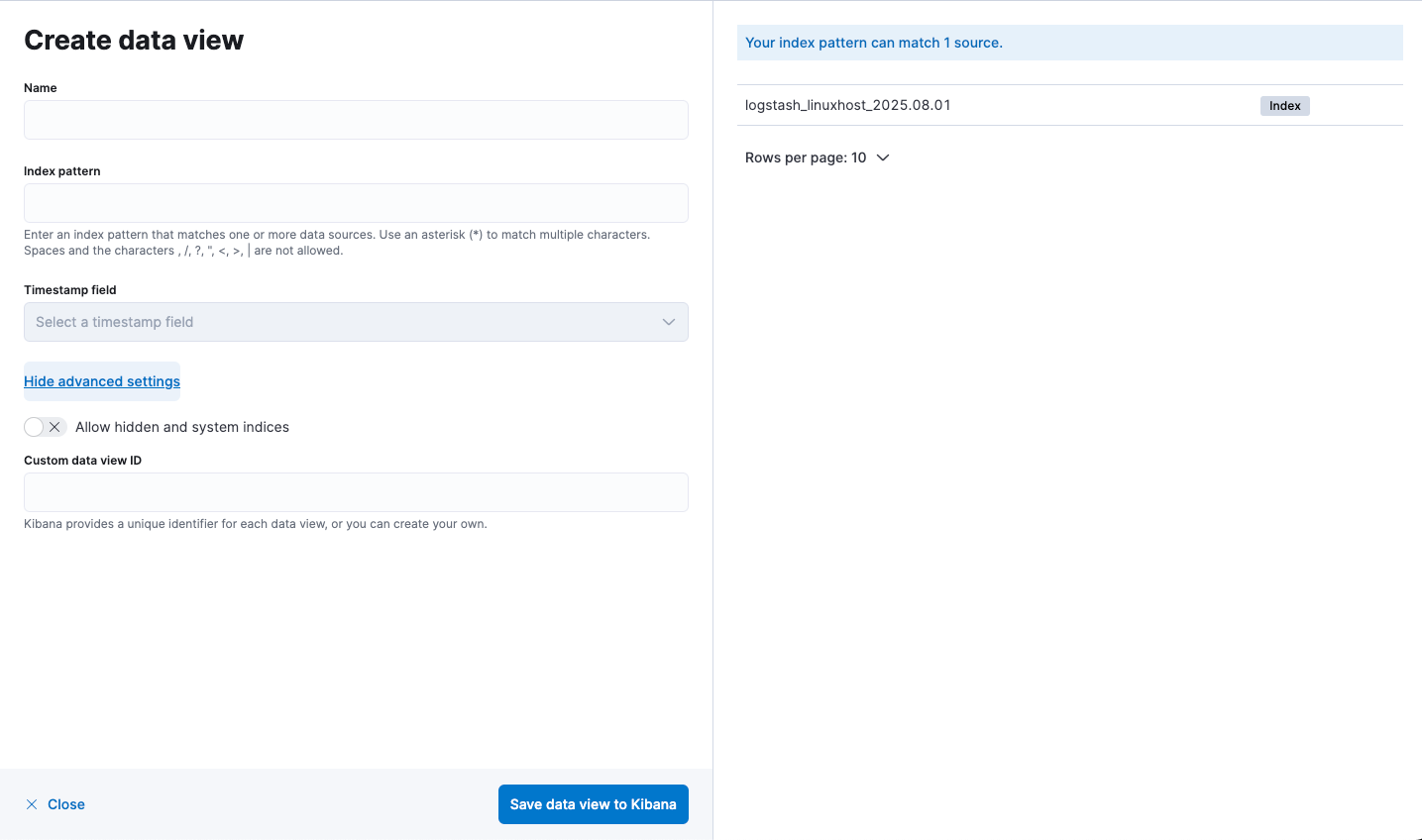
**Thêm Index on Kibana**

Bây giờ ta đăng nhập vào **Kibana** và nhấn vào **Stack Management** => **Data Views** => **Create data view** sau khi nhấn vào màn hình sẽ hiện cho ta 1 số thông tin để điền vào:

**Name:** Đặt tên cho Data View

**Index pattern:** Nhập index mà ta đã cấu hình ở phần logstash

**Timestamp field:** Chọn mặc định



Sau khi nhập xong các thông tin ta nhấn **Save data view to Kibana**

Bây giờ ta nhấn vào tab **Disconver** bên trái màn hình. Bạn sẽ có thể thấy dữ liệu của mình trong màn hình như sau:

