HƯỚNG DẪN CÀI ĐẶT ELK STACK + FILEBEAT + NGINX

I. MỤC TIÊU

Thiết lập hệ thống giám sát log Nginx bằng ELK Stack (Elasticsearch, Logstash, Kibana) kết hợp với Filebeat.

Luồng dữ liệu:

```
Nginx → Filebeat → Logstash → Elasticsearch → Kibana
```

II. CẤU TRÚC THƯ MỤC

```
ElasticsearchNew/
├── docker-compose.yml
├── pipeline/
│   ├── nginx.conf
│   └── sample.conf
├── filebeat/
│   └── filebeat.yml
├── nginx/
│   ├── nginx.conf
│   └── logs/
│       ├── access.log
│       └── error.log
└── logs/
```

III. NỘI DUNG CẤU HÌNH

1. docker-compose.yml

```yaml
version: '3.8'

services:
  elasticsearch:
    image: docker.elastic.co/elasticsearch/elasticsearch:8.15.0
    container_name: elasticsearch
    environment:
      - discovery.type=single-node
      - xpack.security.enabled=false
```

```
      - ES_JAVA_OPTS=-Xms1g -Xmx1g
    ports:
      - "9200:9200"
    networks:
      - elknet

  kibana:
    image: docker.elastic.co/kibana/kibana:8.15.0
    container_name: kibana
    environment:
      - ELASTICSEARCH_HOSTS=http://elasticsearch:9200
    ports:
      - "5601:5601"
    depends_on:
      - elasticsearch
    networks:
      - elknet

  logstash:
    image: docker.elastic.co/logstash/logstash:8.15.0
    container_name: logstash
    volumes:
      - ./pipeline:/usr/share/logstash/pipeline
      - ./sample.logs:/tmp/csv/sample.log
    ports:
      - "5044:5044"
    depends_on:
      - elasticsearch
    networks:
      - elknet

  nginx:
    image: nginx:latest
    container_name: nginx
    volumes:
      - ./nginx/nginx.conf:/etc/nginx/nginx.conf:ro
      - ./nginx/logs:/var/log/nginx
    ports:
      - "8080:80"
    networks:
      - elknet

  filebeat:
    image: docker.elastic.co/beats/filebeat:8.15.0
    container_name: filebeat
    user: root
    volumes:
      - ./filebeat/filebeat.yml:/usr/share/filebeat/filebeat.yml:ro
      - ./nginx/logs:/var/log/nginx:ro
      - ./logs:/usr/share/filebeat/logs
    depends_on:
```

```
      - logstash
    networks:
      - elknet

networks:
  elknet:
    driver: bridge
```

---

2. nginx/nginx.conf

```
events {}

http {
    access_log /var/log/nginx/access.log;
    error_log /var/log/nginx/error.log;

    server {
        listen 80;
        server_name localhost;

        location = / {
            add_header Content-Type text/plain;
            return 200 'Hello from Nginx!';
        }

        location / {
            return 404 "Not Found\n";
        }
    }
}
```

---

3. filebeat/filebeat.yml

```
filebeat.inputs:
  - type: log
    enabled: true
    paths:
      - /var/log/nginx/*.log

output.logstash:
  hosts: ["logstash:5044"]

setup.template.enabled: false
setup.kibana:
  host: "kibana:5601"
```

```
logging:
  level: debug
  to_files: true
  to_stderr: true
  files:
    path: /usr/share/filebeat/logs
    name: filebeat
    keepfiles: 7
    permissions: 0644
```

---

4. pipeline/nginx.conf

```
input {
  beats {
    port => 5044
  }
}

filter {
  if "error.log" in [log][file][path] {
    grok {
      match => { "message" => "%{TIMESTAMP_ISO8601:nginx.time} \\\[%
{LOGLEVEL:nginx.level}\\\] %{NUMBER:pid:int}#%{NUMBER:tid:int}: %
{GREEDYDATA:nginx.message}" }
      overwrite => [ "message" ]
    }
    date {
      match => [ "nginx.time", "yyyy/MM/dd HH:mm:ss" ]
      target => "@timestamp"
    }
  } else if "access.log" in [log][file][path] {
    grok {
      match => { "message" => "%{COMBINEDAPACHELOG}" }
    }
    date {
      match => [ "timestamp", "dd/MMM/yyyy:HH:mm:ss Z" ]
      target => "@timestamp"
    }
  }
}

output {
  elasticsearch {
    hosts => ["http://elasticsearch:9200"]
    index => "nginx-logs-%{+YYYY.MM.dd}"
  }
  stdout { codec => rubydebug }
}
```

IV. CÁC BƯỚC TRIỂN KHAI

1. **Khởi động toàn bộ hệ thống**

```
docker-compose up -d
```

2. **Kiểm tra container**

```
docker ps
```

3. **Tạo log test**

```
curl localhost:8080/
curl localhost:8080/asdf
```

4. **Truy cập Kibana**
   http://localhost:5601 → Discover → tạo index pattern `nginx-logs-*`

V. KIỂM TRA & DEBUG

Lỗi	Nguyên nhân	Cách khắc phục
Không có log mới	Filebeat không gửi dữ liệu	`docker logs filebeat`
Logstash không nhận	Sai port hoặc tên service	`docker exec -it filebeat ping logstash`
Kibana không thấy index	Chưa tạo index pattern	Vào Discover → Add pattern
Nginx không sinh log	Cấu hình sai hoặc chưa reload	`nginx -t && nginx -s reload`

VI. KẾT LUẬN

Hệ thống ELK + Filebeat + Nginx giúp tự động thu thập, phân tích và hiển thị log tập trung. Có thể mở rộng thêm filter phân tích nâng cao hoặc cảnh báo qua Alerting của Kibana.