BỘ THÔNG TIN VÀ TRUYỀN THÔNG

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

KỸ THUẬT THEO DÕI, GIÁM SÁT AN TOÀN MẠNG

BÀI TẬP LỚN:

XÂY DỰNG HỆ THỐNG MÔ PHỎNG SOC

Người hướng dẫn : TS. Nguyễn Minh Hải

Nhóm : 11

Sinh viên thực hiện : NGUYỄN CÔNG LỰC

TP.HCM tháng 06 năm 2024

MỤC LỤC

ĐỀ TÀI

Xây dựng hệ thống mô phỏng SOC gồm các yêu cầu sau:

-Xây dựng 1 Website, dựng GW Nginx và Log lại các Request

-Sử dụng cơ chế Rsync file, Message Queue (Kafka ...) để bắn về hệ thống nhận Log

-Hệ thống nhận Log bao gồm Elastic Search và GrayLog để xử lý.

MÔ HÌNH CHUẨN BỊ

1. Một máy chủ web bao gồm:

- Website đã public: https://lucnguyen.nguyenconggioi.me với ip: http://3.0.59.80

- GW Nginx được gói thành Docker container image để bắt log các request đến website

- Tất cả chạy trên chạy trên AWS (Amazon Web Services)

2. Máy chủ nhận log(Ubuntu) bao gồm:

- Rsync file để đồng bộ file log từ máy chủ web về máy chủ nhận log

- Logstash: Công cụ thu thập log và đẩy vào Kafka.

- Kafka: Message broker để truyền log.

- Graylog: Hệ thống quản lý và tìm kiếm log

- Elasticsearch: Cơ sở dữ liệu lưu trữ và tìm kiếm log.

CHƯƠNG I: XÂY DỰNG 1 WEBSITE, DỰNG GW NGINX VÀ LOG LẠI CÁC REQUEST

1.1 Xây dựng website.

1.1 Xây dựng website

Deloy website https://lucnguyen.nguyenconggioi.me , ip trỏ đến là http://3.0.59.80

Đầu tiên truy cập vào amazon service

```
ssh -i "webpython.pem" ec2-user@ec2-3-0-59-80.ap-southeast-1.compute.amazonaws.com
Last login: Sat Jun 22 19:24:45 2024 from 1.53.235.140
   ,     #_
   ~\_  ####_        Amazon Linux 2
  ~~  \_#####\
  ~~     \###|       AL2 End of Life is 2025-06-30.
  ~~       \#/ ___
   ~~       V~' '->
    ~~~         /    A newer version of Amazon Linux is available!
      ~~._.   _/
         _/ _/       Amazon Linux 2023, GA and supported until 2028-03-15.
       _/m/'           https://aws.amazon.com/linux/amazon-linux-2023/
```

Giao diện terminal làm việc

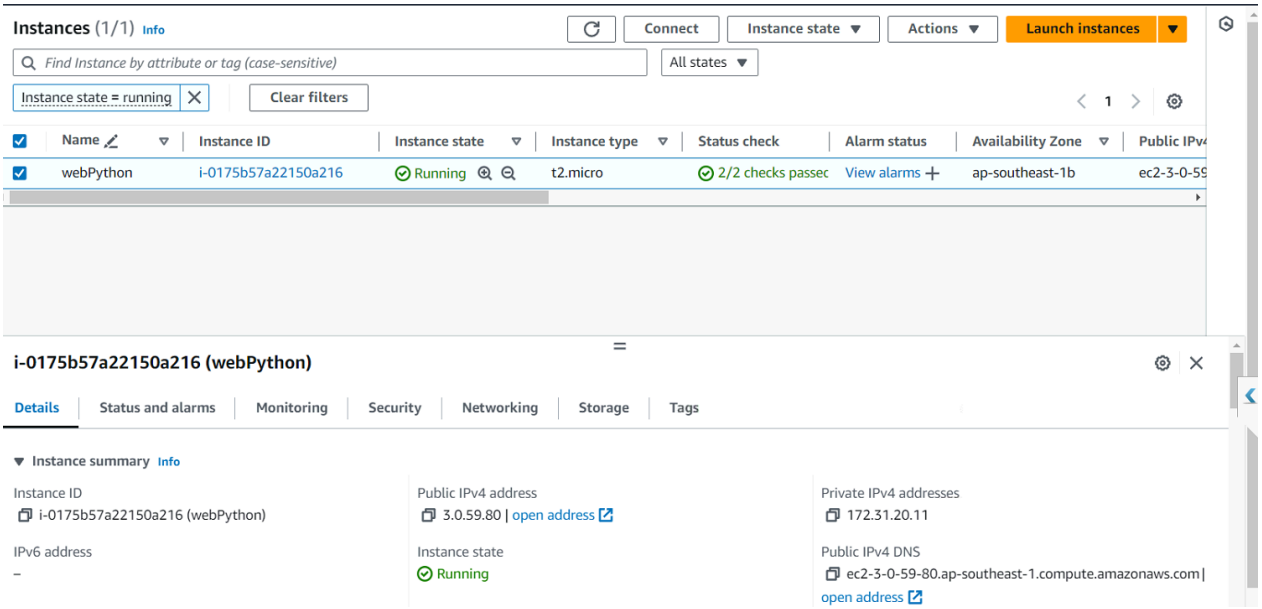
```
FROM python:3.9-slim-bullseye

WORKDIR /app

COPY requirements.txt requirements.txt
RUN pip3 install -r requirements.txt

COPY . .

CMD [ "python3", "-m" , "flask", "run", "--host=0.0.0.0"]
~
~
~
~
~
~
~
~
~
~
~
~
~
"Dockerfile" [noeol][dos] 10L, 198B
```

Cấu hình docker file của website trước khi upload

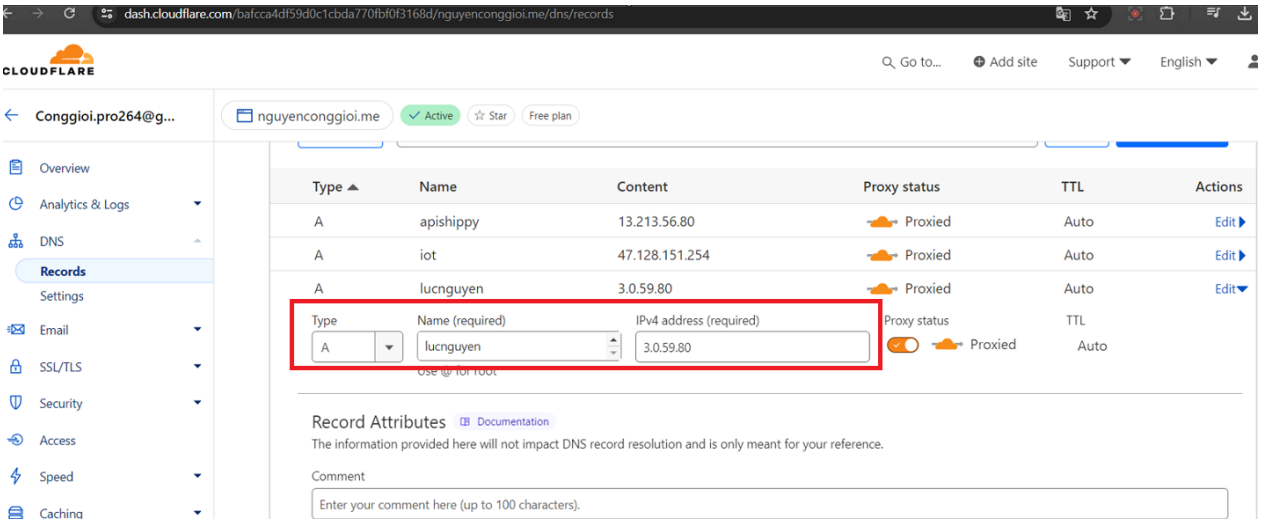
```
[ec2-user@ip-172-31-20-11 flaskAppDemo]$ docker build -t flaskimage .
[+] Building 11.7s (10/10) FINISHED                                                             docker:default
 => [internal] load build definition from Dockerfile                                                      0.0s
 => => transferring dockerfile: 237B                                                                      0.0s
 => [internal] load metadata for docker.io/library/python:3.9-slim-bullseye                               3.0s
 => [internal] load .dockerignore                                                                         0.0s
 => => transferring context: 2B                                                                           0.0s
 => [1/5] FROM docker.io/library/python:3.9-slim-bullseye@sha256:0f0c78a803a7121f04303024d30abe7b02cf4cd10d00ac7ff7168113527dfe1e   4.2s
 => => resolve docker.io/library/python:3.9-slim-bullseye@sha256:0f0c78a803a7121f04303024d30abe7b02cf4cd10d00ac7ff7168113527dfe1e   0.0s
 => => sha256:b4f2292e9e1d9ee90083dbefc726d80762d4c0754862f79bf8a08e0ec3e0606c 7.52kB / 7.52kB          0.0s
 => => sha256:f7b75fe1f735933f47315080637abf01f87962d47f8636a07ff4535ed7a4a133 31.43MB / 31.43MB        0.6s
 => => sha256:6fb769904474ac69efcbe3ca6529e9863496d804e7045697376496ab64885dc2 1.08MB / 1.08MB          0.6s
 => => sha256:6b4a7fcc3dd34edeb34d614f74dc4b90343f254ea5f0c45eef50af1a30d213f6 11.05MB / 11.05MB        2.0s
 => => sha256:0f0c78a803a7121f04303024d30abe7b02cf4cd10d00ac7ff7168113527dfe1e 1.86kB / 1.86kB          0.0s
 => => sha256:8ee0ec964a2aef26e5a1b5121b388e9c24934dde0e49867835c1f7184e98bb86 1.37kB / 1.37kB          0.0s
 => => extracting sha256:f7b75fe1f735933f47315080637abf01f87962d47f8636a07ff4535ed7a4a133                2.2s
 => => sha256:4cbb06924c135347f67574b407744f1ff7b140f5108949d414eb5e7f8d4a91c3 242B / 242B              1.2s
 => => sha256:a6c4281f07e9caa45d68b4ca4e32d5afcd55cf7875af3e753bc0119aaaef82c2 3.14MB / 3.14MB          2.6s
 => => extracting sha256:6fb769904474ac69efcbe3ca6529e9863496d804e7045697376496ab64885dc2                0.1s
 => => extracting sha256:6b4a7fcc3dd34edeb34d614f74dc4b90343f254ea5f0c45eef50af1a30d213f6                0.6s
 => => extracting sha256:4cbb06924c135347f67574b407744f1ff7b140f5108949d414eb5e7f8d4a91c3                0.0s
 => => extracting sha256:a6c4281f07e9caa45d68b4ca4e32d5afcd55cf7875af3e753bc0119aaaef82c2                0.4s
 => [internal] load build context                                                                         0.0s
 => => transferring context: 35.35kB                                                                      0.0s
 => [2/5] WORKDIR /app                                                                                    0.0s
 => [3/5] COPY requirements.txt requirements.txt                                                          0.0s
 => [4/5] RUN pip3 install -r requirements.txt                                                            3.9s
 => [5/5] COPY . .                                                                                        0.1s
```

```
[ec2-user@ip-172-31-20-11 flaskAppDemo]$ docker run -d -p 80:5000 flaskimage
d352112aaf75b237f70d477a84d1d00e3e414e219b18721883320dd17c29a9db
[ec2-user@ip-172-31-20-11 flaskAppDemo]$ docker ps
CONTAINER ID   IMAGE        COMMAND                  CREATED         STATUS         PORTS                                   NAMES
d352112aaf75   flaskimage   "python3 -m flask ru…"   3 seconds ago   Up 2 seconds   0.0.0.0:80->5000/tcp, :::80->5000/tcp   modest_brahmagupta
[ec2-user@ip-172-31-20-11 flaskAppDemo]$ curl localhost
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Home - My Flask App</title>
    <link rel="stylesheet" href="/static/style.css">
</head>
<body>
    <header>
        <nav>
            <a href="/">Home</a>
            <a href="/about">About</a>
            <a href="/contact">Contact</a>
            <a href="/blog">Blog</a>
```

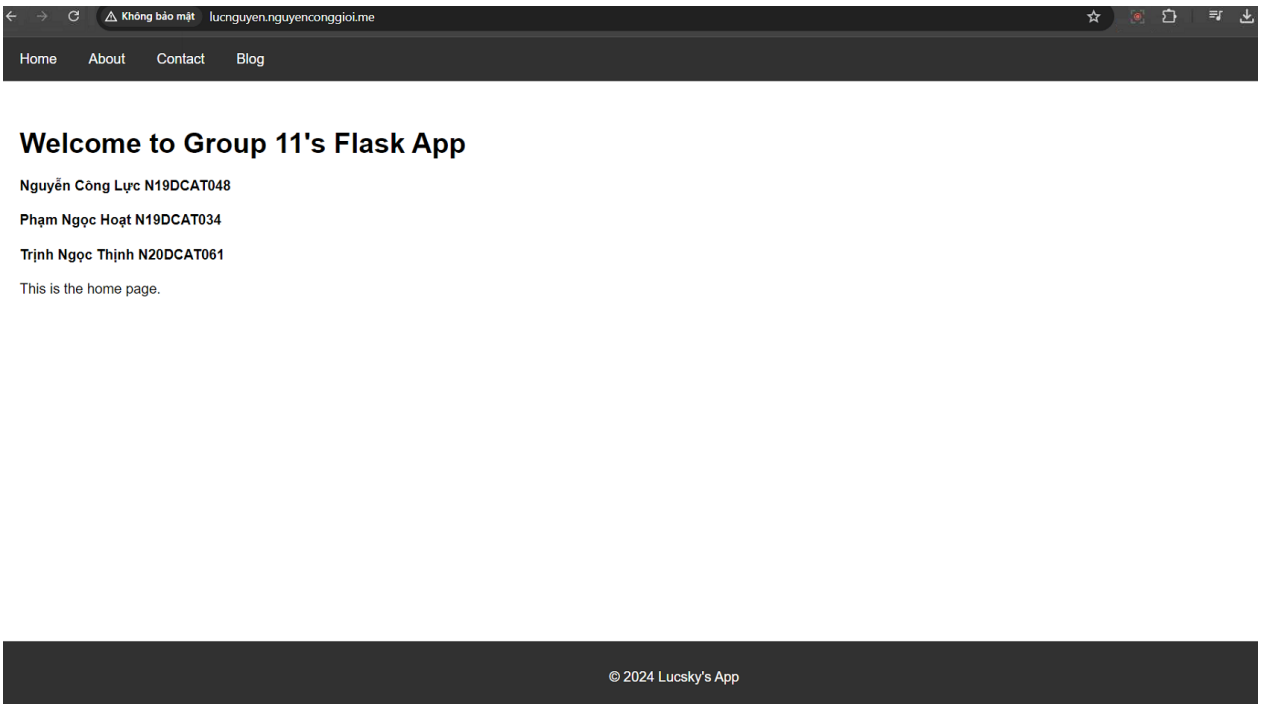
Upload website qua docker



Set IP cho website tại AWS



Set domain cho website

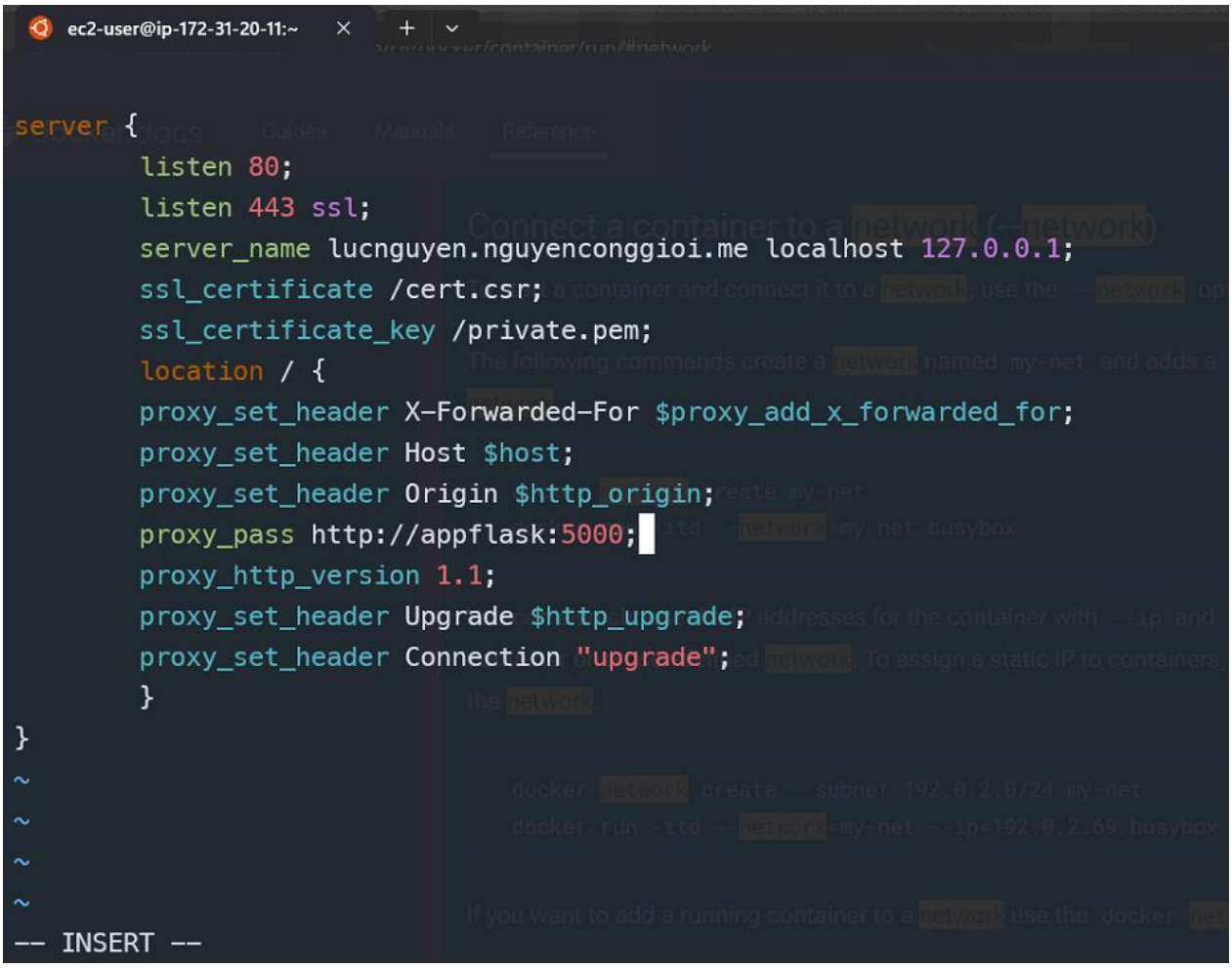


Giao diện website

Link website: https://lucnguyen.nguyenconggioi.me

1.2 Dựng Gateways Nginx và log lại các request

Cấu hình file config



Nội dung file config

File cấu hình docker file để upload Nginx

```
[ec2-user@ip-172-31-20-11 ~]$ docker network create -d bridge flask-network
ada0c8e96e2bdb5817df43b3918307bb9f2f7ff9e777cf535c7302a3e0fbbb84
```

Cấu hình card mạng để Nginx thông với website

```
[ec2-user@ip-172-31-20-11 ~]$ docker run --name nginxgw -v $(pwd)/:/var/log/nginx -itd --network=flask-network -p 80:80
-p 443:443 nginximage
6265a69daef2f963b5a90eb7ff5be2a6c283e16c313991f4073e30614e307f01
[ec2-user@ip-172-31-20-11 ~]$ docker ps
CONTAINER ID   IMAGE        COMMAND                  CREATED          STATUS          PORTS
                                    NAMES
6265a69daef2   nginximage   "/docker-entrypoint.…"   2 seconds ago    Up 1 second     0.0.0.0:80->80/tcp, :::80->80/tcp,
 0.0.0.0:443->443/tcp, :::443->443/tcp   nginxgw
4ac686e83848   flaskimage   "python3 -m flask ru…"   39 minutes ago   Up 39 minutes
                                    appflask
```

Upload container Nginx qua docker lên máy chủ web

Giờ đây các request vào website đã được log lại

```
[ec2-user@ip-172-31-20-11 ~]$ docker exec -it nginxgw sh
/ # cat /var/log/nginx/access.log
172.71.210.226 - - [22/Jun/2024:18:35:29 +0000] "GET / HTTP/1.1" 200 772 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)
 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.0.0 Safari/537.36" "2405:4803:c87e:ed50:dd67:94f7:1e19:bc5d"
172.71.210.226 - - [22/Jun/2024:18:35:30 +0000] "GET / HTTP/1.1" 200 772 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)
 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.0.0 Safari/537.36" "2405:4803:c87e:ed50:dd67:94f7:1e19:bc5d"
172.71.210.226 - - [22/Jun/2024:18:35:30 +0000] "GET / HTTP/1.1" 200 772 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)
 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.0.0 Safari/537.36" "2405:4803:c87e:ed50:dd67:94f7:1e19:bc5d"
172.71.218.104 - - [22/Jun/2024:18:36:05 +0000] "GET /g HTTP/1.1" 404 207 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64
) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.0.0 Safari/537.36" "2405:4803:c87e:ed50:dd67:94f7:1e19:bc5d"
172.71.214.182 - - [22/Jun/2024:18:43:51 +0000] "GET /g HTTP/1.1" 404 207 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64
) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.0.0 Safari/537.36" "2405:4803:c87e:ed50:dd67:94f7:1e19:bc5d"
172.68.225.194 - - [22/Jun/2024:18:44:00 +0000] "GET / HTTP/1.1" 200 772 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)
 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.0.0 Safari/537.36" "2405:4803:c87e:ed50:dd67:94f7:1e19:bc5d"
```

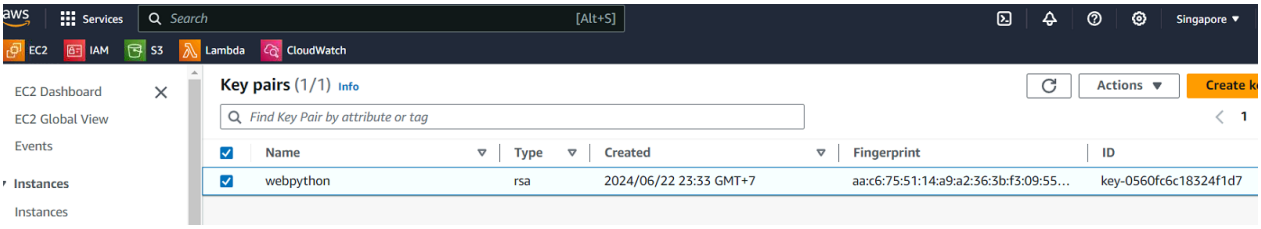
Xem access.log trên Nginx để check requests từ user

```
[ec2-user@ip-172-31-20-11 ~]$ docker exec -it nginxgw sh
/ # cat /var/log/nginx/error.log
2024/06/22 18:35:14 [notice] 1#1: using the "epoll" event method
2024/06/22 18:35:14 [notice] 1#1: nginx/1.27.0
2024/06/22 18:35:14 [notice] 1#1: built by gcc 13.2.1 20231014 (Alpine 13.2.1_git20231014)
2024/06/22 18:35:14 [notice] 1#1: OS: Linux 5.10.218-208.862.amzn2.x86_64
2024/06/22 18:35:14 [notice] 1#1: getrlimit(RLIMIT_NOFILE): 32768:65536
2024/06/22 18:35:14 [notice] 1#1: start worker processes
2024/06/22 18:35:14 [notice] 1#1: start worker process 29
```

Xem error.log của Nginx để check các vấn đề

CHƯƠNG II: SỬ DỤNG CƠ CHẾ RSYNC FILE, MESSAGE QUEUE (KAFKA ...) ĐỂ BẮN VỀ HỆ THỐNG NHẬN LOG(ELASTIC SEARCH VÀ GRAYLOG) ĐỂ XỬ LÝ.

2.1 Sử dụng cơ chế rsync file



Download SSH key

```
congluc@Nguyen-Cong-Luc:~$ sudo rsync -avze "ssh -i webpython.pem" ec2-user@3.0.59.80:/home/ec2-user/nginx /tmp/
receiving incremental file list
nginx/
nginx/access.log
nginx/error.log

sent 66 bytes  received 94,208 bytes  37,709.60 bytes/sec
total size is 3,194,098  speedup is 33.88
```

Khởi chạy rync để đồng bộ file nginx từ server web về server log(Ubuntu)

```
congluc@Nguyen-Cong-Luc:/tmp/nginx$ ls -al
total 3132
drwxrwxr-x  2 conggioi conggioi    4096 Jun 23 02:27 .
drwxrwxrwt 11 root     root        4096 Jun 23 16:29 ..
-rw-r--r--  1 root     root     3189217 Jun 23 16:22 access.log
-rw-r--r--  1 root     root        4881 Jun 23 16:19 error.log
```

Các log đã được đồng bộ

```
cat access.log
172.71.219.105 - - [22/Jun/2024:19:27:43 +0000] "GET / HTTP/1.1" 200 772 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.0.0 Safari/537.36" "2405:4803:c87e:ed50:dd67:94f7:1e19:bc5d"
172.71.214.80 - - [22/Jun/2024:19:29:40 +0000] "GET / HTTP/1.1" 200 772 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) A
ppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.0.0 Safari/537.36 Edg/126.0.0.0" "1.53.235.140"
172.71.210.18 - - [22/Jun/2024:19:32:08 +0000] "GET / HTTP/1.1" 200 772 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) A
ppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.0.0 Safari/537.36" "2405:4803:c87e:ed50:dd67:94f7:1e19:bc5d"
172.71.210.18 - - [22/Jun/2024:19:32:09 +0000] "GET / HTTP/1.1" 200 772 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) A
ppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.0.0 Safari/537.36" "2405:4803:c87e:ed50:dd67:94f7:1e19:bc5d"
172.71.218.107 - - [22/Jun/2024:19:32:11 +0000] "GET / HTTP/1.1" 200 772 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.0.0 Safari/537.36" "2405:4803:c87e:ed50:dd67:94f7:1e19:bc5d"
172.68.225.175 - - [22/Jun/2024:19:32:12 +0000] "GET /static/style.css HTTP/1.1" 304 0 "https://lucnguyen.nguyenconggioi
.me/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.0.0 Safari/537.36"
"2405:4803:c87e:ed50:dd67:94f7:1e19:bc5d"
117.211.232.194 - - [22/Jun/2024:19:38:28 +0000] "GET /boaform/admin/formLogin?username=ec8&psd=ec8 HTTP/1.0" 404 207 "-
" "-" "-"
172.168.41.87 - - [22/Jun/2024:19:50:46 +0000] "GET /actuator/health HTTP/1.1" 404 207 "-" "Mozilla/5.0 zgrab/0.x" "-"
172.68.225.194 - - [22/Jun/2024:19:55:25 +0000] "GET / HTTP/1.1" 200 772 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)
```

Xem access log

```
cat error.log
2024/06/22 19:27:36 [notice] 1#1: using the "epoll" event method
2024/06/22 19:27:36 [notice] 1#1: nginx/1.27.0
2024/06/22 19:27:36 [notice] 1#1: built by gcc 13.2.1 20231014 (Alpine 13.2.1_git20231014)
2024/06/22 19:27:36 [notice] 1#1: OS: Linux 5.10.218-208.862.amzn2.x86_64
2024/06/22 19:27:36 [notice] 1#1: getrlimit(RLIMIT_NOFILE): 32768:65536
2024/06/22 19:27:36 [notice] 1#1: start worker processes
2024/06/22 19:27:36 [notice] 1#1: start worker process 29
2024/06/22 19:32:12 [warn] 29#29: *10 upstream sent duplicate header line: "Date: Sat, 22 Jun 2024 19:32:12 GMT", previo
us value: "Date: Sat, 22 Jun 2024 19:32:12 GMT", ignored while reading response header from upstream, client: 172.68.225
.175, server: lucnguyen.nguyenconggioi.me, request: "GET /static/style.css HTTP/1.1", upstream: "http://172.18.0.2:5000/
static/style.css", host: "lucnguyen.nguyenconggioi.me", referrer: "https://lucnguyen.nguyenconggioi.me/"
2024/06/22 19:55:26 [warn] 29#29: *19 upstream sent duplicate header line: "Date: Sat, 22 Jun 2024 19:55:26 GMT", previo
us value: "Date: Sat, 22 Jun 2024 19:55:26 GMT", ignored while reading response header from upstream, client: 172.68.225
.174, server: lucnguyen.nguyenconggioi.me, request: "GET /static/style.css HTTP/1.1", upstream: "http://172.18.0.2:5000/
static/style.css", host: "lucnguyen.nguyenconggioi.me", referrer: "https://lucnguyen.nguyenconggioi.me/"
```

Xem error log

2.2 Sử dụng cơ chế Message Queue(Kafka)

*ZooKeeper cung cấp một kho lưu trữ tập trung cho các cấu hình của ứng dụng phân tán. Điều này giúp đảm bảo rằng tất cả các phần của hệ thống đều có cùng một cấu hình, tránh sự không nhất quán.

```
zookeeper:
    image: confluentinc/cp-zookeeper:7.3.2
    environment:
        ZOOKEEPER_CLIENT_PORT: 2181
        ZOOKEEPER_TICK_TIME: 2000
    ports:
        - "2181:2181"
```

Cấu hình ZooKeeper

* Fluentd là phần mềm thu thập dữ liệu, Fluentd có thể nhận log từ Ngnix và truyền tới kafka

```
worker_processes 1;

events {
    worker_connections 1024;
}

http {
    log_format main '$remote_addr - $remote_user [$time_local] "$request" '
                    '$status $body_bytes_sent "$http_referer" '
                    '"$http_user_agent" "$http_x_forwarded_for"';

    access_log syslog:server=fluentd:5140 main;

    server {
        listen 80;
        server_name localhost;

        location / {
```

Cấu hình lại Ngnix để truyền log tới fluentd

```yaml
fluentd:
  build: ./fluentd
  ports:
    - "5140:5140/udp"
  volumes:
    - ./fluentd/fluent.conf:/fluentd/etc/fluent.conf
  depends_on:
    - kafka
```

Cấu hình fluentd để truyền log tới kafka

```yaml
kafka:
  image: confluentinc/cp-kafka:7.3.2
  ports:
    - "9092:9092"
  restart: always
  environment:
    KAFKA_LISTENERS: PLAINTEXT://:9092,PLAINTEXT_HOST://0.0.0.0:29092
    KAFKA_BROKER_ID: 1
    KAFKA_ZOOKEEPER_CONNECT: zookeeper:2181
    KAFKA_ADVERTISED_LISTENERS: PLAINTEXT://kafka:9092,PLAINTEXT_HOST://localhost:29092
    KAFKA_LISTENER_SECURITY_PROTOCOL_MAP: PLAINTEXT:PLAINTEXT,PLAINTEXT_HOST:PLAINTEXT
    KAFKA_INTER_BROKER_LISTENER_NAME: PLAINTEXT
    KAFKA_OFFSETS_TOPIC_REPLICATION_FACTOR: 1
  depends_on:
    - zookeeper

```

Cấu hình kafka

```
[appuser@2d19cee92079 ~]$ kafka-console-consumer --bootstrap-server kafka:9092 --topic nginx_logs --from-beginning
[2024-06-23 09:48:23,159] WARN [Consumer clientId=console-consumer, groupId=console-consumer-85871] Error while fetching
 metadata with correlation id 2 : {nginx_logs=LEADER_NOT_AVAILABLE} (org.apache.kafka.clients.NetworkClient)
[2024-06-23 09:48:23,294] WARN [Consumer clientId=console-consumer, groupId=console-consumer-85871] Error while fetching
 metadata with correlation id 4 : {nginx_logs=LEADER_NOT_AVAILABLE} (org.apache.kafka.clients.NetworkClient)
[2024-06-23 09:48:23,402] WARN [Consumer clientId=console-consumer, groupId=console-consumer-85871] Error while fetching
 metadata with correlation id 6 : {nginx_logs=LEADER_NOT_AVAILABLE} (org.apache.kafka.clients.NetworkClient)
{"host":"5a399d4b232b","ident":"nginx_access","message":"192.168.0.1 - - [23/Jun/2024:09:48:29 +0000] \"GET / HTTP/1.1\"
 304 0 \"-\" \"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.0.0 Safari/
537.36\""}
{"host":"5a399d4b232b","ident":"nginx_access","message":"192.168.0.1 - - [23/Jun/2024:09:48:30 +0000] \"GET / HTTP/1.1\"
 304 0 \"-\" \"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.0.0 Safari/
537.36\""}
{"host":"5a399d4b232b","ident":"nginx_access","message":"192.168.0.1 - - [23/Jun/2024:09:48:30 +0000] \"GET / HTTP/1.1\"
 304 0 \"-\" \"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.0.0 Safari/
537.36\""}
{"host":"5a399d4b232b","ident":"nginx_access","message":"192.168.0.1 - - [23/Jun/2024:09:48:30 +0000] \"GET / HTTP/1.1\"
 304 0 \"-\" \"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.0.0 Safari/
537.36\""}
```

Log được lưu vào kafka

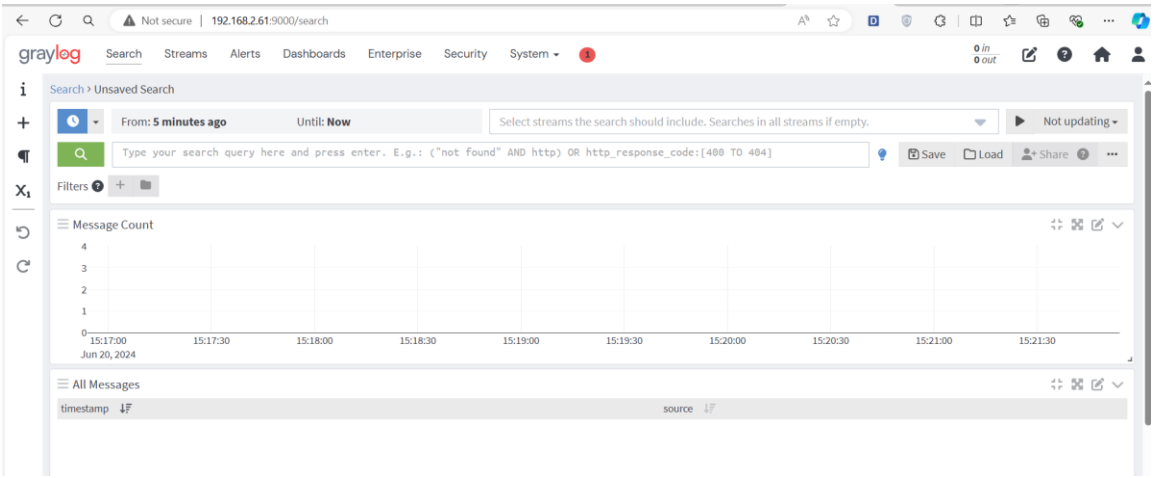
2.3 Nhận log từ kafka đưa vào Graylog và tìm kiếm dữ liệu với Elastic Search

```
elasticsearch:
    image: docker.elastic.co/elasticsearch/elasticsearch-oss:7.10.2
    volumes:
        - es_data:/usr/share/elasticsearch/data
    environment:
        - http.host=0.0.0.0
        - transport.host=localhost
        - network.host=0.0.0.0
        - "ES_JAVA_OPTS=-Xms512m -Xmx512m"
    ulimits:
        memlock:
            soft: -1
            hard: -1
    mem_limit: 1g
    networks:
        - graylog
```

Cấu hình Elastic Search

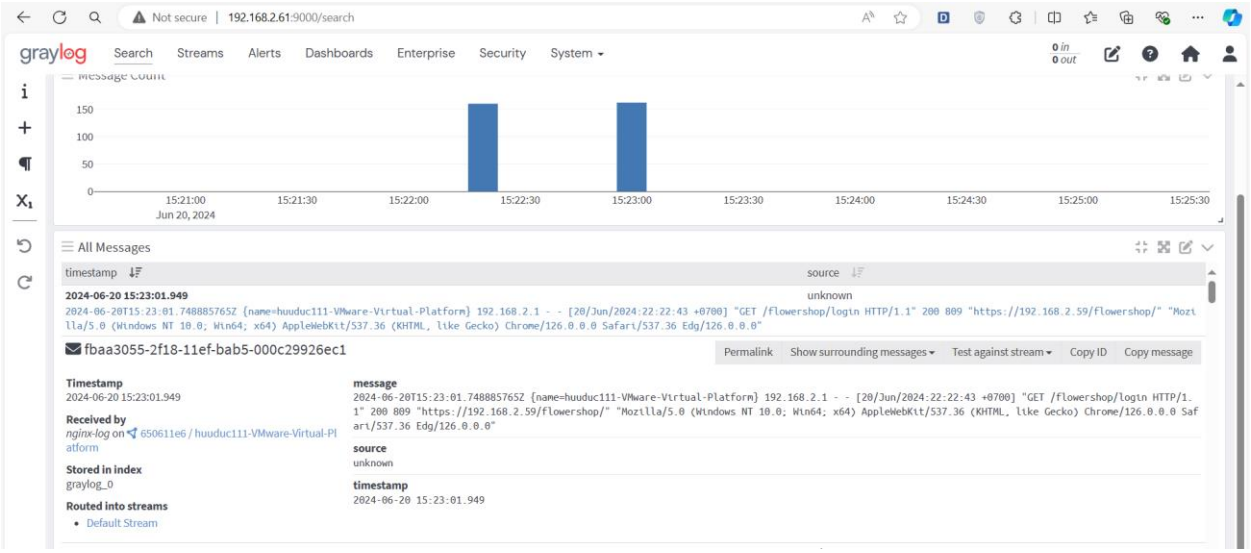
```
graylog:
    image: graylog/graylog:5.1
    volumes:
        - graylog_journal:/usr/share/graylog/data/journal
    environment:
        - GRAYLOG_PASSWORD_SECRET=nguyenconglucgroup11
        - GRAYLOG_ROOT_PASSWORD_SHA2=1b3353fb3deb4e3bf48c854c69a19976ae6d2d3ced74ab681dcc7deb09e6c49b
        - GRAYLOG_HTTP_EXTERNAL_URI=http://192.168.1.75:9000/
    entrypoint: /usr/bin/tini -- wait-for-it elasticsearch:9200 -- /docker-entrypoint.sh
    networks:
        - graylog
    depends_on:
        - mongodb
        - elasticsearch
        - kafka
        - zookeeper
    ports:
        - "9000:9000"
        - "1514:1514"
        - "1514:1514/udp"
        - "12201:12201"
        - "12201:12201/udp"
```

Cấu hình GrayLog



Cài đặt graylog cũng như elasticsearch thành công

Sau khi truy cập lại website, log mới sẽ được lưu đến kafka và truyền tới Graylog



Graylog đã nhận được log từ kafka.

CHƯƠNG III: ĐÁNH GIÁ VÀ KẾT LUẬN

3.1 Đánh giá

*Máy chủ web:

-Website: Website đã được public và hoạt động tại địa chỉ https://lucnguyen.nguyenconggioi.me với IP http://3.0.59.80, cho thấy cấu hình mạng và DNS hoạt động đúng cách.

-GW Nginx trong Docker: Việc gói Nginx thành Docker container để bắt log các request là một phương pháp thuận tiện, giúp triển khai và quản lý dễ dàng hơn.

-AWS: Sử dụng AWS cung cấp một môi trường đáng tin cậy, giúp đảm bảo hiệu suất và khả năng mở rộng.

*Máy chủ nhận log (Ubuntu):

-Rsync: Sử dụng Rsync để đồng bộ file log từ máy chủ web về máy chủ nhận log là một giải pháp đơn giản và đáng tin cậy.

-Logstash và Kafka: Sự kết hợp giữa Logstash và Kafka giúp thu thập, xử lý và truyền tải log một cách hiệu quả.

-Graylog và Elasticsearch: Graylog cung cấp giao diện người dùng thân thiện, còn Elasticsearch đảm bảo khả năng lưu trữ và tìm kiếm log nhanh chóng.

3.2 Kết luận

-Hệ thống đã được triển khai với các công nghệ phù hợp và cấu hình hợp lý,

-Đảm bảo khả năng thu thập, truyền tải và phân tích log một cách hiệu quả.

DANH MỤC TÀI LIỆU THAM KHẢO

Tiếng Việt:

[1] Nguyễn Ngọc Điệp (2015), *Bài giảng kỹ thuật theo dõi giám sát mạng*, Học viện Công nghệ Bưu chính Viễn thông.

Tiếng Anh:

[2] *Nginx*. https://nginx.org/en/ truy cập ngày 19/06/2024.

[3] *Graylog*. https://graylog.org/ truy cập ngày 20/06/2024.