# Hướng dẫn triển khai ELK Stack 8.13.4

Người viết: Lê Nhựt Anh  
Email: Anh2LN@hcmp.com.vn

Tài liệu này được biên soạn dành cho các kỹ sư phần mềm / DevOps cần thiết lập nhanh bộ ELK Stack (Elasticsearch – Logstash – Kibana) phiên bản 8.13.4 trên hệ điều hành Oracle Linux / CentOS / RHEL 8.

## 1. Tổng quan thành phần

• \*\*Elasticsearch\*\*: cơ sở dữ liệu tìm kiếm phân tán, lưu trữ dữ liệu dưới dạng JSON; cung cấp REST API tốc độ cao, hỗ trợ full‑text, aggregation và security (xpack).

• \*\*Logstash\*\*: pipeline thu thập – chuyển đổi – gửi log/metrics. Cấu trúc pipeline gồm input → filter → output; trong tài liệu này output chính là Elasticsearch qua HTTPS.

• \*\*Kibana\*\*: giao diện trực quan hóa, truy vấn và giám sát dữ liệu; đồng thời cung cấp DevTools, Alerting, Dashboard.

## 2. Cách vận hành tổng thể

Logstash đọc log (ví dụ generator input), áp dụng filter (nếu có) rồi gửi tới Elasticsearch index `test-logs-\*`. Kibana kết nối bằng account `kibana\_system` để truy vấn và hiển thị dashboard. Tất cả lưu lượng REST dùng SSL tự ký được tạo trong script.

## 3. Giải thích từng bước trong script

|  |  |
| --- | --- |
| **Đoạn lệnh** | **Mục đích / Giải thích** |
| id -u $ES\_USER &>/dev/null || sudo useradd --system --no-create-home --shell /sbin/nologin $ES\_USER | 👉 Tạo user Elasticsearch (nếu chưa có)… |
| sudo mkdir -p $BASE\_DIR sudo tar -xzf /home/vagrant/$ES\_TAR -C $BASE\_DIR | 📦 Giải nén Elasticsearch… |
| sudo chown -R $ES\_USER:$ES\_USER $ES\_DIR | 🔧 Phân quyền thư mục Elasticsearch… |
| sudo ln -sfn $ES\_DIR $ES\_SYM | 🔗 Tạo symlink Elasticsearch… |
| echo "export ES\_HOME=$ES\_SYM" | sudo tee /etc/profile.d/elasticsearch.sh echo "export PATH=\$ES\_HOME/bin:\$PATH" | sudo tee -a /etc/profile.d/elasticsearch.sh sudo chmod +x /etc/profile.d/elasticsearch.sh source /etc/profile.d/elasticsearch.sh | ⚙️ Khai báo ES\_HOME và PATH… |
| echo "vm.max\_map\_count=262144" | sudo tee -a /etc/sysctl.conf sudo sysctl -w vm.max\_map\_count=262144 | 🖥️ Tăng vm.max\_map\_count kernel… |
| sudo tee $ES\_DIR/config/elasticsearch.yml >/dev/null <<EOF discovery.type: single-node xpack.security.enabled: true xpack.security.authc.api\_key.enabled: true xpack.security.http.ssl:  enabled: false network.host: 0.0.0.0 EOF | 📑 Tạo elasticsearch.yml (single-node + security)… |
| sudo tee /etc/systemd/system/elasticsearch.service >/dev/null <<EOF [Unit] Description=Elasticsearch $ES\_VERSION Documentation=https://www.elastic.co Wants=network-online.target After=network-online.target [Service] Type=simple User=$ES\_USER Group=$ES\_USER ExecStart=$ES\_DIR/bin/elasticsearch Restart=always LimitNOFILE=65535 Environment=ES\_JAVA\_HOME=$ES\_DIR/jdk [Install] WantedBy=multi-user.target EOF | 🛠️ Tạo service Elasticsearch… |
| sudo systemctl enable elasticsearch sudo systemctl start elasticsearch | 🚀 Bật & khởi động Elasticsearch… |
| until curl -s http://localhost:9200 >/dev/null; do sleep 2; done | ⏳ Đợi Elasticsearch sẵn sàng (HTTP)… |
| sudo -u $ES\_USER $ES\_DIR/bin/elasticsearch-setup-passwords auto -b > $ENV\_FILE sudo chown vagrant:vagrant $ENV\_FILE ES\_PASSWORD=$(grep "PASSWORD elastic" $ENV\_FILE | awk '{print $4}') | 🔐 Sinh mật khẩu mặc định… |
| sudo sed -i 's/xpack.security.enabled: true/&\ xpack.security.transport.ssl.enabled: true/' $ES\_DIR/config/elasticsearch.yml ################### KIBANA ################### | 🔧 Bật SSL Transport (dòng thêm)… |
| id -u $KIBANA\_USER &>/dev/null || sudo useradd --system --no-create-home --shell /sbin/nologin $KIBANA\_USER | 👉 Tạo user Kibana (nếu chưa có)… |
| sudo tar -xzf /home/vagrant/$KIBANA\_TAR -C $BASE\_DIR | 📦 Giải nén Kibana… |
| sudo chown -R $KIBANA\_USER:$KIBANA\_USER $KIBANA\_DIR sudo ln -sfn $KIBANA\_DIR $KIBANA\_SYM | 🔧 Phân quyền & symlink Kibana… |
| sudo tee $KIBANA\_DIR/config/kibana.yml >/dev/null <<EOF server.host: "0.0.0.0" elasticsearch.hosts: ["http://localhost:9200"] elasticsearch.username: "kibana\_system" elasticsearch.password: "$(grep "PASSWORD kibana\_system" $ENV\_FILE | awk '{print $4}')" telemetry.optIn: false xpack.security:  session.idleTimeout: "30m"  session.lifespan: "8h"  encryptionKey: "$(openssl rand -hex 32)" EOF | 📑 Viết kibana.yml (security)… |
| sudo tee /etc/systemd/system/kibana.service >/dev/null <<EOF [Unit] Description=Kibana $KIBANA\_VERSION Documentation=https://www.elastic.co Wants=network-online.target After=network-online.target elasticsearch.service [Service] Type=simple User=$KIBANA\_USER Group=$KIBANA\_USER ExecStart=$KIBANA\_DIR/bin/kibana Restart=always LimitNOFILE=65535 Environment=NODE\_OPTIONS="--max-old-space-size=2048" [Install] WantedBy=multi-user.target EOF | 🛠️ Tạo service Kibana… |
| sudo systemctl enable kibana sudo systemctl start kibana | 🚀 Bật & khởi động Kibana… |
| until curl -s http://localhost:5601 >/dev/null; do sleep 2; done | ⏳ Đợi Kibana sẵn sàng (HTTP)… |
| ################### LOGSTASH ################# | ✅ Kibana đã sẵn sàng tại http://localhost:5601 |
| id -u $LOGSTASH\_USER &>/dev/null || sudo useradd --system --no-create-home --shell /sbin/nologin $LOGSTASH\_USER | 👉 Tạo user Logstash (nếu chưa có)… |
| sudo tar -xzf /home/vagrant/$LOGSTASH\_TAR -C $BASE\_DIR | 📦 Giải nén Logstash… |
| sudo chown -R $LOGSTASH\_USER:$LOGSTASH\_USER $LOGSTASH\_DIR sudo ln -sfn $LOGSTASH\_DIR $LOGSTASH\_SYM | 🔧 Phân quyền & symlink Logstash… |
| LOGSTASH\_WRITER\_PASSWORD=$(openssl rand -hex 12) curl -X POST "http://localhost:9200/\_security/role/logstash\_writer" \  -u "elastic:${ES\_PASSWORD}" -H "Content-Type: application/json" -d '{  "cluster":["monitor","manage\_index\_templates"],  "indices":[{"names":["\*"],"privileges":["create\_index","write","delete","index","read"]}] }' curl -X POST "http://localhost:9200/\_security/user/logstash\_writer" \  -u "elastic:${ES\_PASSWORD}" -H "Content-Type: application/json" -d '{  "password":"'"${LOGSTASH\_WRITER\_PASSWORD}"'",  "roles":["logstash\_writer"] }' echo "PASSWORD logstash\_writer = ${LOGSTASH\_WRITER\_PASSWORD}" >> $ENV\_FILE | 🔐 Tạo role & user logstash\_writer… |
| sudo mkdir -p /etc/logstash sudo tee /etc/logstash/sample.conf >/dev/null <<EOF input { generator { lines => ["Hello, world!", "Logstash is awesome!"] count => 10 } } output {  elasticsearch {  hosts => ["http://localhost:9200"]  index => "test-logs-%{+YYYY.MM.dd}"  user => "logstash\_writer"  password => "${LOGSTASH\_WRITER\_PASSWORD}"  }  stdout { codec => rubydebug } } EOF sudo chown -R $LOGSTASH\_USER:$LOGSTASH\_USER /etc/logstash | 🗄️ Viết pipeline mẫu… |
| sudo tee /etc/systemd/system/logstash.service >/dev/null <<EOF [Unit] Description=Logstash ${LOGSTASH\_VERSION} Documentation=https://www.elastic.co Wants=network-online.target After=network-online.target elasticsearch.service [Service] Type=simple User=${LOGSTASH\_USER} Group=${LOGSTASH\_USER} ExecStart=${LOGSTASH\_SYM}/bin/logstash --path.settings ${LOGSTASH\_SYM}/config --path.data /var/lib/logstash -f /etc/logstash/ Restart=always LimitNOFILE=65535 [Install] WantedBy=multi-user.target EOF | 🛠️ Tạo service Logstash… |
| sudo mkdir -p /var/lib/logstash sudo chown -R $LOGSTASH\_USER:$LOGSTASH\_USER /var/lib/logstash | 📂 Tạo /var/lib/logstash & cấp quyền… |
| sudo systemctl daemon-reload sudo systemctl enable logstash sudo systemctl start logstash | 🚀 Bật & khởi động Logstash… |
| until curl -s http://localhost:9600/\_node/pipelines >/dev/null; do sleep 2; done ################### SSL #################### | ⏳ Đợi API monitoring Logstash… |
| sudo sed -i '/^xpack\.security\.http\.ssl:/,/^ enabled: false/d' $ES\_SYM/config/elasticsearch.yml sudo sed -i '/^xpack\.security\.transport\.ssl\.enabled: true/d' $ES\_SYM/config/elasticsearch.yml sudo tee -a $ES\_SYM/config/elasticsearch.yml >/dev/null <<EOF # ---- SSL ---- xpack.security.http.ssl.enabled: true xpack.security.http.ssl.keystore.type: PKCS12 xpack.security.http.ssl.keystore.path: elasticsearch.p12 xpack.security.http.ssl.keystore.password: $CA\_PASS xpack.security.http.ssl.truststore.path: elasticsearch.p12 xpack.security.http.ssl.truststore.password: $CA\_PASS xpack.security.transport.ssl.enabled: true xpack.security.transport.ssl.verification\_mode: certificate xpack.security.transport.ssl.keystore.type: PKCS12 xpack.security.transport.ssl.keystore.path: elasticsearch.p12 xpack.security.transport.ssl.keystore.password: $CA\_PASS xpack.security.transport.ssl.truststore.type: PKCS12 xpack.security.transport.ssl.truststore.path: elasticsearch.p12 xpack.security.transport.ssl.truststore.password: $CA\_PASS EOF | 🔒 Sửa elasticsearch.yml để bật SSL HTTP & Transport… |
| sudo rm -f $ES\_DIR/config/elastic-stack-ca.p12 $ES\_DIR/config/elasticsearch.p12 printf '%s\n%s\n' $CA\_PASS $CA\_PASS | \  sudo $ES\_SYM/bin/elasticsearch-certutil ca --silent --pass $CA\_PASS \  --out $ES\_DIR/config/elastic-stack-ca.p12 printf '%s\n%s\n' $CA\_PASS $CA\_PASS | \  sudo $ES\_SYM/bin/elasticsearch-certutil cert --name elasticsearch --ca $ES\_DIR/config/elastic-stack-ca.p12 \  --silent --ca-pass $CA\_PASS --pass $CA\_PASS --out $ES\_DIR/config/elasticsearch.p12 sudo chown $ES\_USER:$ES\_USER $ES\_DIR/config/\*.p12 sudo chmod 640 $ES\_DIR/config/\*.p12 | 🔒 Sinh CA & keystore elasticsearch.p12… |
| sudo systemctl stop elasticsearch sudo systemctl start elasticsearch until curl -ks https://localhost:9200 >/dev/null; do sleep 2; done | 🔁 Khởi động lại Elasticsearch (HTTPS)… |
| sudo /opt/elasticsearch/bin/elasticsearch-certutil cert --name kibana --ca $ES\_DIR/config/elastic-stack-ca.p12 \  --silent --ca-pass $CA\_PASS --pass $CA\_PASS --out $KIBANA\_DIR/config/kibana.p12 sudo openssl pkcs12 -in $KIBANA\_DIR/config/kibana.p12 -nocerts -nodes -passin pass:$CA\_PASS | \  sudo tee $KIBANA\_DIR/config/kibana.key >/dev/null sudo openssl pkcs12 -in $KIBANA\_DIR/config/kibana.p12 -clcerts -nokeys -passin pass:$CA\_PASS \  -out $KIBANA\_DIR/config/kibana.crt sudo openssl pkcs12 -in $ES\_DIR/config/elastic-stack-ca.p12 -nokeys -clcerts -passin pass:$CA\_PASS \  -out $KIBANA\_DIR/config/elastic-stack-ca.pem sudo chown $KIBANA\_USER:$KIBANA\_USER $KIBANA\_DIR/config/kibana.\* $KIBANA\_DIR/config/elastic-stack-ca.pem sudo chmod 640 $KIBANA\_DIR/config/kibana.\* $KIBANA\_DIR/config/elastic-stack-ca.pem sudo sed -i '/^elasticsearch\.hosts:/d' $KIBANA\_DIR/config/kibana.yml sudo tee -a $KIBANA\_DIR/config/kibana.yml >/dev/null <<EOF # --- TLS --- server.ssl.enabled: true server.ssl.certificate: $KIBANA\_DIR/config/kibana.crt server.ssl.key: $KIBANA\_DIR/config/kibana.key elasticsearch.hosts: ["https://localhost:9200"] elasticsearch.ssl.certificateAuthorities: ["$KIBANA\_DIR/config/elastic-stack-ca.pem"] elasticsearch.ssl.verificationMode: certificate EOF sudo systemctl restart kibana until curl -ks https://localhost:5601 >/dev/null; do sleep 2; done | 🔒 Sinh chứng chỉ Kibana & cấu hình TLS… |
| sudo /opt/elasticsearch/bin/elasticsearch-certutil cert --name logstash --ca $ES\_DIR/config/elastic-stack-ca.p12 \  --silent --ca-pass $CA\_PASS --pass $CA\_PASS --out $LOGSTASH\_DIR/config/logstash.p12 sudo openssl pkcs12 -in $LOGSTASH\_DIR/config/logstash.p12 -nocerts -nodes -passin pass:$CA\_PASS | \  sudo tee $LOGSTASH\_DIR/config/logstash.key >/dev/null sudo openssl pkcs12 -in $LOGSTASH\_DIR/config/logstash.p12 -clcerts -nokeys -passin pass:$CA\_PASS \  -out $LOGSTASH\_DIR/config/logstash.crt sudo cp $KIBANA\_DIR/config/elastic-stack-ca.pem $LOGSTASH\_DIR/config/ sudo chown $LOGSTASH\_USER:$LOGSTASH\_USER $LOGSTASH\_DIR/config/logstash.\* $LOGSTASH\_DIR/config/elastic-stack-ca.pem sudo chmod 640 $LOGSTASH\_DIR/config/logstash.\* $LOGSTASH\_DIR/config/elastic-stack-ca.pem sudo sed -i -e 's|\(\s\*hosts\s\*=>\s\*\)\["http://|\1["https://|g' \ -e '/^\s\*hosts\s\*=>/a \ ssl\_certificate\_verification => false\n ssl => true\n cacert => "'"$LOGSTASH\_DIR/config/elastic-stack-ca.pem"'"' \  /etc/logstash/sample.conf sudo systemctl restart logstash | 🔒 Sinh chứng chỉ Logstash & chỉnh pipeline SSL… |
|  | ✅ Hoàn tất! ELK đang chạy HTTPS. Mật khẩu lưu tại $ENV\_FILE |

## 4. Script cài đặt đầy đủ

Nội dung bên dưới có thể sao chép trực tiếp thành file `install.sh`.

#!/bin/bash  
set -e  
############################################################  
# CÀI ĐẶT ELK STACK 8.13.4 + SSL (giữ nguyên lệnh gốc)  
# Tác giả: <YourName> – 04/2025  
############################################################  
  
#################### BIẾN CHUNG ##########################  
BASE\_DIR="/opt"  
  
# Elasticsearch  
ES\_VERSION="8.13.4"  
ES\_TAR="elasticsearch-${ES\_VERSION}-linux-x86\_64.tar.gz"  
ES\_DIR="${BASE\_DIR}/elasticsearch-${ES\_VERSION}"  
ES\_SYM="${BASE\_DIR}/elasticsearch"  
ES\_USER="elasticsearch"  
  
# Kibana  
KIBANA\_VERSION="8.13.4"  
KIBANA\_TAR="kibana-${KIBANA\_VERSION}-linux-x86\_64.tar.gz"  
KIBANA\_DIR="${BASE\_DIR}/kibana-${KIBANA\_VERSION}"  
KIBANA\_SYM="${BASE\_DIR}/kibana"  
KIBANA\_USER="kibana"  
  
# Logstash  
LOGSTASH\_VERSION="8.13.4"  
LOGSTASH\_TAR="logstash-${LOGSTASH\_VERSION}-linux-x86\_64.tar.gz"  
LOGSTASH\_DIR="${BASE\_DIR}/logstash-${LOGSTASH\_VERSION}"  
LOGSTASH\_SYM="${BASE\_DIR}/logstash"  
LOGSTASH\_USER="logstash"  
  
# File chung  
ENV\_FILE="/home/vagrant/elk-passwords.env"  
CA\_PASS="changeme"  
############################################################  
  
echo "1/35 👉 Tạo user Elasticsearch (nếu chưa có)…"  
id -u $ES\_USER &>/dev/null || sudo useradd --system --no-create-home --shell /sbin/nologin $ES\_USER  
  
echo "2/35 📦 Giải nén Elasticsearch…"  
sudo mkdir -p $BASE\_DIR  
sudo tar -xzf /home/vagrant/$ES\_TAR -C $BASE\_DIR  
  
echo "3/35 🔧 Phân quyền thư mục Elasticsearch…"  
sudo chown -R $ES\_USER:$ES\_USER $ES\_DIR  
  
echo "4/35 🔗 Tạo symlink Elasticsearch…"  
sudo ln -sfn $ES\_DIR $ES\_SYM  
  
echo "5/35 ⚙️ Khai báo ES\_HOME và PATH…"  
echo "export ES\_HOME=$ES\_SYM" | sudo tee /etc/profile.d/elasticsearch.sh  
echo "export PATH=\$ES\_HOME/bin:\$PATH" | sudo tee -a /etc/profile.d/elasticsearch.sh  
sudo chmod +x /etc/profile.d/elasticsearch.sh  
source /etc/profile.d/elasticsearch.sh  
  
echo "6/35 🖥️ Tăng vm.max\_map\_count kernel…"  
echo "vm.max\_map\_count=262144" | sudo tee -a /etc/sysctl.conf  
sudo sysctl -w vm.max\_map\_count=262144  
  
echo "7/35 📑 Tạo elasticsearch.yml (single-node + security)…"  
sudo tee $ES\_DIR/config/elasticsearch.yml >/dev/null <<EOF  
discovery.type: single-node  
xpack.security.enabled: true  
xpack.security.authc.api\_key.enabled: true  
xpack.security.http.ssl:  
 enabled: false  
network.host: 0.0.0.0  
EOF  
  
echo "8/35 🛠️ Tạo service Elasticsearch…"  
sudo tee /etc/systemd/system/elasticsearch.service >/dev/null <<EOF  
[Unit]  
Description=Elasticsearch $ES\_VERSION  
Documentation=https://www.elastic.co  
Wants=network-online.target  
After=network-online.target  
[Service]  
Type=simple  
User=$ES\_USER  
Group=$ES\_USER  
ExecStart=$ES\_DIR/bin/elasticsearch  
Restart=always  
LimitNOFILE=65535  
Environment=ES\_JAVA\_HOME=$ES\_DIR/jdk  
[Install]  
WantedBy=multi-user.target  
EOF  
  
echo "9/35 🚀 Bật & khởi động Elasticsearch…"  
sudo systemctl enable elasticsearch  
sudo systemctl start elasticsearch  
  
echo "10/35 ⏳ Đợi Elasticsearch sẵn sàng (HTTP)…"  
until curl -s http://localhost:9200 >/dev/null; do sleep 2; done  
  
echo "11/35 🔐 Sinh mật khẩu mặc định…"  
sudo -u $ES\_USER $ES\_DIR/bin/elasticsearch-setup-passwords auto -b > $ENV\_FILE  
sudo chown vagrant:vagrant $ENV\_FILE  
ES\_PASSWORD=$(grep "PASSWORD elastic" $ENV\_FILE | awk '{print $4}')  
  
echo "12/35 🔧 Bật SSL Transport (dòng thêm)…"  
sudo sed -i 's/xpack.security.enabled: true/&\  
xpack.security.transport.ssl.enabled: true/' $ES\_DIR/config/elasticsearch.yml  
  
################### KIBANA ###################  
echo "13/35 👉 Tạo user Kibana (nếu chưa có)…"  
id -u $KIBANA\_USER &>/dev/null || sudo useradd --system --no-create-home --shell /sbin/nologin $KIBANA\_USER  
  
echo "14/35 📦 Giải nén Kibana…"  
sudo tar -xzf /home/vagrant/$KIBANA\_TAR -C $BASE\_DIR  
  
echo "15/35 🔧 Phân quyền & symlink Kibana…"  
sudo chown -R $KIBANA\_USER:$KIBANA\_USER $KIBANA\_DIR  
sudo ln -sfn $KIBANA\_DIR $KIBANA\_SYM  
  
echo "16/35 📑 Viết kibana.yml (security)…"  
sudo tee $KIBANA\_DIR/config/kibana.yml >/dev/null <<EOF  
server.host: "0.0.0.0"  
elasticsearch.hosts: ["http://localhost:9200"]  
elasticsearch.username: "kibana\_system"  
elasticsearch.password: "$(grep "PASSWORD kibana\_system" $ENV\_FILE | awk '{print $4}')"  
telemetry.optIn: false  
xpack.security:  
 session.idleTimeout: "30m"  
 session.lifespan: "8h"  
 encryptionKey: "$(openssl rand -hex 32)"  
EOF  
  
echo "17/35 🛠️ Tạo service Kibana…"  
sudo tee /etc/systemd/system/kibana.service >/dev/null <<EOF  
[Unit]  
Description=Kibana $KIBANA\_VERSION  
Documentation=https://www.elastic.co  
Wants=network-online.target  
After=network-online.target elasticsearch.service  
[Service]  
Type=simple  
User=$KIBANA\_USER  
Group=$KIBANA\_USER  
ExecStart=$KIBANA\_DIR/bin/kibana  
Restart=always  
LimitNOFILE=65535  
Environment=NODE\_OPTIONS="--max-old-space-size=2048"  
[Install]  
WantedBy=multi-user.target  
EOF  
  
echo "18/35 🚀 Bật & khởi động Kibana…"  
sudo systemctl enable kibana  
sudo systemctl start kibana  
  
echo "19/35 ⏳ Đợi Kibana sẵn sàng (HTTP)…"  
until curl -s http://localhost:5601 >/dev/null; do sleep 2; done  
  
echo "20/35 ✅ Kibana đã sẵn sàng tại http://localhost:5601"  
  
################### LOGSTASH #################  
echo "21/35 👉 Tạo user Logstash (nếu chưa có)…"  
id -u $LOGSTASH\_USER &>/dev/null || sudo useradd --system --no-create-home --shell /sbin/nologin $LOGSTASH\_USER  
  
echo "22/35 📦 Giải nén Logstash…"  
sudo tar -xzf /home/vagrant/$LOGSTASH\_TAR -C $BASE\_DIR  
  
echo "23/35 🔧 Phân quyền & symlink Logstash…"  
sudo chown -R $LOGSTASH\_USER:$LOGSTASH\_USER $LOGSTASH\_DIR  
sudo ln -sfn $LOGSTASH\_DIR $LOGSTASH\_SYM  
  
echo "24/35 🔐 Tạo role & user logstash\_writer…"  
LOGSTASH\_WRITER\_PASSWORD=$(openssl rand -hex 12)  
curl -X POST "http://localhost:9200/\_security/role/logstash\_writer" \  
 -u "elastic:${ES\_PASSWORD}" -H "Content-Type: application/json" -d '{  
 "cluster":["monitor","manage\_index\_templates"],  
 "indices":[{"names":["\*"],"privileges":["create\_index","write","delete","index","read"]}]  
}'  
curl -X POST "http://localhost:9200/\_security/user/logstash\_writer" \  
 -u "elastic:${ES\_PASSWORD}" -H "Content-Type: application/json" -d '{  
 "password":"'"${LOGSTASH\_WRITER\_PASSWORD}"'",  
 "roles":["logstash\_writer"]  
}'  
echo "PASSWORD logstash\_writer = ${LOGSTASH\_WRITER\_PASSWORD}" >> $ENV\_FILE  
  
echo "25/35 🗄️ Viết pipeline mẫu…"  
sudo mkdir -p /etc/logstash  
sudo tee /etc/logstash/sample.conf >/dev/null <<EOF  
input { generator { lines => ["Hello, world!", "Logstash is awesome!"] count => 10 } }  
output {  
 elasticsearch {  
 hosts => ["http://localhost:9200"]  
 index => "test-logs-%{+YYYY.MM.dd}"  
 user => "logstash\_writer"  
 password => "${LOGSTASH\_WRITER\_PASSWORD}"  
 }  
 stdout { codec => rubydebug }  
}  
EOF  
sudo chown -R $LOGSTASH\_USER:$LOGSTASH\_USER /etc/logstash  
  
echo "26/35 🛠️ Tạo service Logstash…"  
sudo tee /etc/systemd/system/logstash.service >/dev/null <<EOF  
[Unit]  
Description=Logstash ${LOGSTASH\_VERSION}  
Documentation=https://www.elastic.co  
Wants=network-online.target  
After=network-online.target elasticsearch.service  
[Service]  
Type=simple  
User=${LOGSTASH\_USER}  
Group=${LOGSTASH\_USER}  
ExecStart=${LOGSTASH\_SYM}/bin/logstash --path.settings ${LOGSTASH\_SYM}/config --path.data /var/lib/logstash -f /etc/logstash/  
Restart=always  
LimitNOFILE=65535  
[Install]  
WantedBy=multi-user.target  
EOF  
  
echo "27/35 📂 Tạo /var/lib/logstash & cấp quyền…"  
sudo mkdir -p /var/lib/logstash  
sudo chown -R $LOGSTASH\_USER:$LOGSTASH\_USER /var/lib/logstash  
  
echo "28/35 🚀 Bật & khởi động Logstash…"  
sudo systemctl daemon-reload  
sudo systemctl enable logstash  
sudo systemctl start logstash  
  
echo "29/35 ⏳ Đợi API monitoring Logstash…"  
until curl -s http://localhost:9600/\_node/pipelines >/dev/null; do sleep 2; done  
  
################### SSL ####################  
echo "30/35 🔒 Sửa elasticsearch.yml để bật SSL HTTP & Transport…"  
sudo sed -i '/^xpack\.security\.http\.ssl:/,/^ enabled: false/d' $ES\_SYM/config/elasticsearch.yml  
sudo sed -i '/^xpack\.security\.transport\.ssl\.enabled: true/d' $ES\_SYM/config/elasticsearch.yml  
sudo tee -a $ES\_SYM/config/elasticsearch.yml >/dev/null <<EOF  
# ---- SSL ----  
xpack.security.http.ssl.enabled: true  
xpack.security.http.ssl.keystore.type: PKCS12  
xpack.security.http.ssl.keystore.path: elasticsearch.p12  
xpack.security.http.ssl.keystore.password: $CA\_PASS  
xpack.security.http.ssl.truststore.path: elasticsearch.p12  
xpack.security.http.ssl.truststore.password: $CA\_PASS  
xpack.security.transport.ssl.enabled: true  
xpack.security.transport.ssl.verification\_mode: certificate  
xpack.security.transport.ssl.keystore.type: PKCS12  
xpack.security.transport.ssl.keystore.path: elasticsearch.p12  
xpack.security.transport.ssl.keystore.password: $CA\_PASS  
xpack.security.transport.ssl.truststore.type: PKCS12  
xpack.security.transport.ssl.truststore.path: elasticsearch.p12  
xpack.security.transport.ssl.truststore.password: $CA\_PASS  
EOF  
  
echo "31/35 🔒 Sinh CA & keystore elasticsearch.p12…"  
sudo rm -f $ES\_DIR/config/elastic-stack-ca.p12 $ES\_DIR/config/elasticsearch.p12  
printf '%s\n%s\n' $CA\_PASS $CA\_PASS | \  
 sudo $ES\_SYM/bin/elasticsearch-certutil ca --silent --pass $CA\_PASS \  
 --out $ES\_DIR/config/elastic-stack-ca.p12  
printf '%s\n%s\n' $CA\_PASS $CA\_PASS | \  
 sudo $ES\_SYM/bin/elasticsearch-certutil cert --name elasticsearch --ca $ES\_DIR/config/elastic-stack-ca.p12 \  
 --silent --ca-pass $CA\_PASS --pass $CA\_PASS --out $ES\_DIR/config/elasticsearch.p12  
sudo chown $ES\_USER:$ES\_USER $ES\_DIR/config/\*.p12  
sudo chmod 640 $ES\_DIR/config/\*.p12  
  
echo "32/35 🔁 Khởi động lại Elasticsearch (HTTPS)…"  
sudo systemctl stop elasticsearch  
sudo systemctl start elasticsearch  
until curl -ks https://localhost:9200 >/dev/null; do sleep 2; done  
  
echo "33/35 🔒 Sinh chứng chỉ Kibana & cấu hình TLS…"  
sudo /opt/elasticsearch/bin/elasticsearch-certutil cert --name kibana --ca $ES\_DIR/config/elastic-stack-ca.p12 \  
 --silent --ca-pass $CA\_PASS --pass $CA\_PASS --out $KIBANA\_DIR/config/kibana.p12  
sudo openssl pkcs12 -in $KIBANA\_DIR/config/kibana.p12 -nocerts -nodes -passin pass:$CA\_PASS | \  
 sudo tee $KIBANA\_DIR/config/kibana.key >/dev/null  
sudo openssl pkcs12 -in $KIBANA\_DIR/config/kibana.p12 -clcerts -nokeys -passin pass:$CA\_PASS \  
 -out $KIBANA\_DIR/config/kibana.crt  
sudo openssl pkcs12 -in $ES\_DIR/config/elastic-stack-ca.p12 -nokeys -clcerts -passin pass:$CA\_PASS \  
 -out $KIBANA\_DIR/config/elastic-stack-ca.pem  
sudo chown $KIBANA\_USER:$KIBANA\_USER $KIBANA\_DIR/config/kibana.\* $KIBANA\_DIR/config/elastic-stack-ca.pem  
sudo chmod 640 $KIBANA\_DIR/config/kibana.\* $KIBANA\_DIR/config/elastic-stack-ca.pem  
sudo sed -i '/^elasticsearch\.hosts:/d' $KIBANA\_DIR/config/kibana.yml  
sudo tee -a $KIBANA\_DIR/config/kibana.yml >/dev/null <<EOF  
  
# --- TLS ---  
server.ssl.enabled: true  
server.ssl.certificate: $KIBANA\_DIR/config/kibana.crt  
server.ssl.key: $KIBANA\_DIR/config/kibana.key  
elasticsearch.hosts: ["https://localhost:9200"]  
elasticsearch.ssl.certificateAuthorities: ["$KIBANA\_DIR/config/elastic-stack-ca.pem"]  
elasticsearch.ssl.verificationMode: certificate  
EOF  
sudo systemctl restart kibana  
until curl -ks https://localhost:5601 >/dev/null; do sleep 2; done  
  
echo "34/35 🔒 Sinh chứng chỉ Logstash & chỉnh pipeline SSL…"  
sudo /opt/elasticsearch/bin/elasticsearch-certutil cert --name logstash --ca $ES\_DIR/config/elastic-stack-ca.p12 \  
 --silent --ca-pass $CA\_PASS --pass $CA\_PASS --out $LOGSTASH\_DIR/config/logstash.p12  
sudo openssl pkcs12 -in $LOGSTASH\_DIR/config/logstash.p12 -nocerts -nodes -passin pass:$CA\_PASS | \  
 sudo tee $LOGSTASH\_DIR/config/logstash.key >/dev/null  
sudo openssl pkcs12 -in $LOGSTASH\_DIR/config/logstash.p12 -clcerts -nokeys -passin pass:$CA\_PASS \  
 -out $LOGSTASH\_DIR/config/logstash.crt  
sudo cp $KIBANA\_DIR/config/elastic-stack-ca.pem $LOGSTASH\_DIR/config/  
sudo chown $LOGSTASH\_USER:$LOGSTASH\_USER $LOGSTASH\_DIR/config/logstash.\* $LOGSTASH\_DIR/config/elastic-stack-ca.pem  
sudo chmod 640 $LOGSTASH\_DIR/config/logstash.\* $LOGSTASH\_DIR/config/elastic-stack-ca.pem  
sudo sed -i -e 's|\(\s\*hosts\s\*=>\s\*\)\["http://|\1["https://|g' \  
-e '/^\s\*hosts\s\*=>/a \ ssl\_certificate\_verification => false\n ssl => true\n cacert => "'"$LOGSTASH\_DIR/config/elastic-stack-ca.pem"'"' \  
 /etc/logstash/sample.conf  
sudo systemctl restart logstash  
  
echo "35/35 ✅ Hoàn tất! ELK đang chạy HTTPS. Mật khẩu lưu tại $ENV\_FILE"

A screenshot of a computer screen

Description automatically generated

Hình 1: Hình ảnh hoàn tất cài đặt Elasticsearch, Kibana, Logstash

A screenshot of a computer

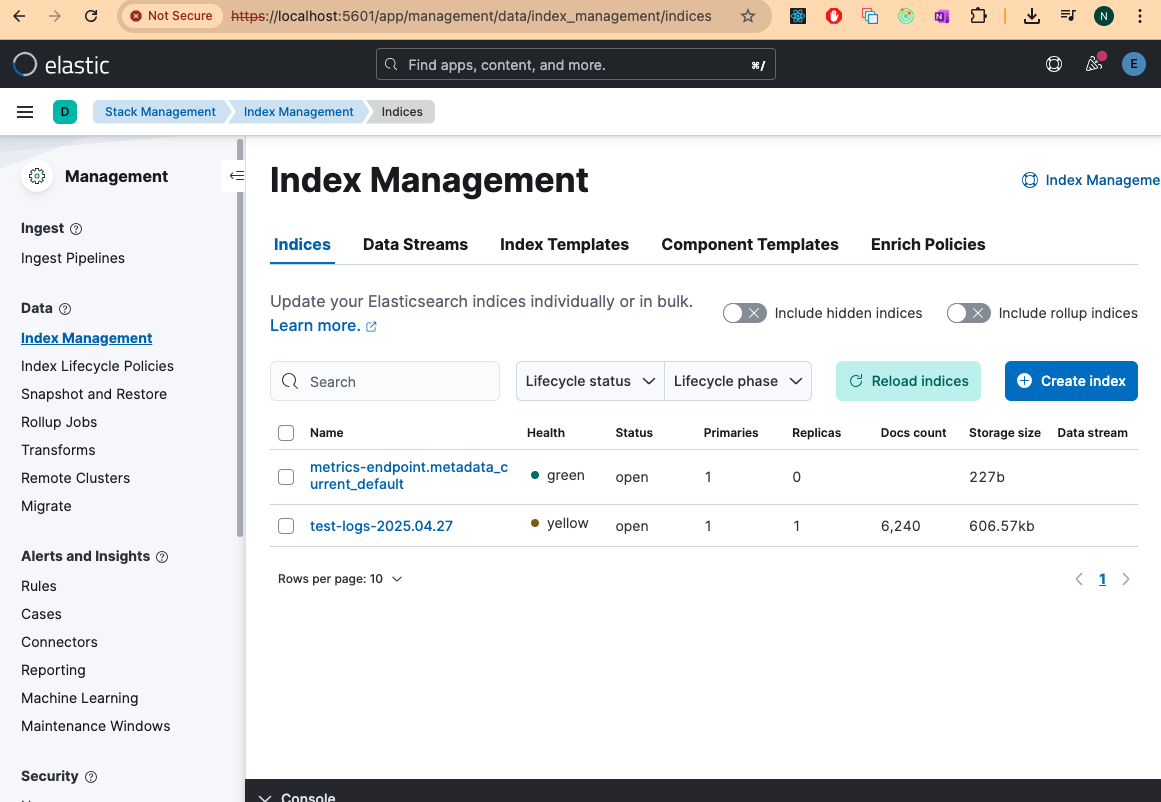
Description automatically generated

Hình 2: Hoàn thành cài đặt elasticsearch

A screenshot of a computer

Description automatically generated

Hình 3: Hình ảnh Kibana đã hoạt động trên https



Hình 4: Logstash tạo log và gửi vào elasticsearch và hiển thị trên Kibana   
(user: elastic, password nằm trong file elk-passwords.env trong thư mục home)



Hình 5: các file có trong thư mục $USER/home

A screenshot of a computer screen

Description automatically generated

Hình 6: Minh hoạ các tài khoản được tạo mật khẩu tự động