# Hướng dẫn triển khai ELK Stack 8.13.4

Người viết: Lê Nhựt Anh / Tháng 4-2025  
Email: [Anh2LN@hcmp.com.vn](mailto: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. Ta tải file tar và để cùng thư mục gốc.

## 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. Cài đặt Elasticsearch – Kibana – Logstash trên 1 node và là node master

|  |  |  |
| --- | --- | --- |
| **#** | **Lệnh / khối lệnh chính** | **Mục đích** |
| 1 | id -u $ES\_USER … || sudo useradd … | Tạo tài khoản hệ thống **elasticsearch** nếu chưa có. |
| 2 | sudo mkdir -p $BASE\_DIRsudo tar -xzf "$USER\_HOME/$ES\_TAR" -C $BASE\_DIR | Tạo thư mục gốc /opt (nếu chưa có) và giải nén gói **Elasticsearch**. |
| 3 | sudo chown -R $ES\_USER:$ES\_USER $ES\_DIR | Gán quyền sở hữu thư mục cài Elasticsearch cho user **elasticsearch**. |
| 4 | sudo ln -sfn $ES\_DIR $ES\_SYM | Tạo symlink /opt/elasticsearch trỏ tới phiên bản vừa cài, giúp nâng cấp dễ dàng. |
| 5 | Ghi file /etc/profile.d/elasticsearch.sh rồi source | Đặt biến môi trường **ES\_HOME** và thêm vào **PATH** để chạy lệnh ES ở mọi nơi. |
| 6 | echo "vm.max\_map\_count=262144" …sudo sysctl -w vm.max\_map\_count=262144 | Tăng tham số kernel vm.max\_map\_count – bắt buộc để ES hoạt động ổn định. |
| 7 | Ghi elasticsearch.yml (single-node + security) | Cấu hình ES chạy chế độ 1 nút, bật bảo mật, mở cổng mọi IP. |
| 8 | Ghi /etc/systemd/system/elasticsearch.service | Khai báo service systemd cho Elasticsearch. |
| 9 | systemctl enable & start elasticsearch | Cho ES khởi động cùng hệ thống và chạy ngay. |
| 10 | Vòng until curl -s http://localhost:9200 | Đợi ES sẵn sàng trước khi làm bước kế tiếp. |
| 11 | elasticsearch-setup-passwords auto -b > $ENV\_FILE | Sinh toàn bộ mật khẩu mặc định (elastic, kibana\_system …) và lưu vào file .env. |
| 12 | sed -i … xpack.security.transport.ssl.enabled: true | Bật SSL cho kênh Transport (nội bộ cluster). |
| 13 | Tạo user hệ thống **kibana** | Đảm bảo phân quyền riêng cho dịch vụ Kibana. |
| 14 | Giải nén gói Kibana | Cài đặt Kibana vào /opt. |
| 15 | Phân quyền + symlink | Gán quyền user kibana và trỏ /opt/kibana tới bản cài. |
| 16 | Ghi kibana.yml | Trỏ Kibana tới ES, nạp user/pass và tắt telemetry. |
| 17 | Tạo service systemd cho Kibana | Khởi chạy Kibana dưới user kibana, đặt limit file-handle. |
| 18 | systemctl enable & start kibana | Khởi động và tự chạy lại khi reboot. |
| 19 | Đợi Kibana sẵn sàng (curl :5601) | Xác nhận giao diện Web đã online. |
| 20 | Thông báo URL Kibana | Nhắc admin đường dẫn truy cập. |
| 21 | Tạo user hệ thống **logstash** | Phân tách quyền cho Logstash. |
| 22 | Giải nén Logstash | Thêm thành phần thu-thập log vào stack. |
| 23 | Phân quyền + symlink Logstash | Cho phép user logstash sở hữu thư mục, tạo /opt/logstash. |
| 24 | Gọi API ES tạo **role & user logstash\_writer** | Cấp quyền ghi index & template cho pipeline Logstash. |
| 25 | Viết file pipeline mẫu /etc/logstash/sample.conf | Minh họa input generator → output ES + stdout. |
| 26 | Tạo service systemd cho Logstash | Định nghĩa cách Logstash đọc cấu hình và đường dẫn data. |
| 27 | Tạo /var/lib/logstash & phân quyền | Thư mục lưu trạng thái pipeline, sincedb … |
| 28 | systemctl daemon-reload, enable, start Logstash | Nạp unit mới, bật và chạy ngay Logstash. |
| 29 | Đợi API monitoring Logstash (curl :9600) | Bảo đảm Logstash hoạt động trước khi cấu hình SSL. |
| 30 | Ghi lại **elasticsearch.yml** chi tiết (cluster, SSL) | Chuyển sang mô hình cluster 2 node (master & data) và bật TLS đầy đủ (HTTP + Transport). |
| 31 | elasticsearch-certutil ca/cert … | Tạo CA & keystore elasticsearch.p12 đặt trong config/. |
| 32 | Restart ES & đợi HTTPS (curl -ks https://localhost:9200) | Áp dụng TLS, kiểm tra ES nghe trên HTTPS. |
| 33 | Sinh chứng chỉ cho Kibana, trích cert/key, cập nhật kibana.yml | Cho giao diện Kibana chạy HTTPS và tin cậy CA mới tạo. |
| 34 | Sinh chứng chỉ cho Logstash, chỉnh sample.conf dùng HTTPS | Bảo mật đường truyền Logstash → Elasticsearch. |
| 35 | cp elastic-stack-ca.p12 /home/$USER\_HOME + thông báo | Sao chép CA về thư mục người dùng để tiện phân phối cho node khác; in thông báo hoàn tất & vị trí file mật khẩu. |

## 4. Script cài đặt đầy đủ cho node master

Nội dung bên dưới có thể sao chép trực tiếp thành file `install.sh`. Để cài đặt trên Oracle Linux chỉ cần gõ lệnh “sh install.sh” mặc định sẽ lấy tài khoản root, nếu cài bằng user khác thì lệnh là “sh install.sh <username>“  
  
Ta tải script ở link để thư mục chứa các file cài đặt: https://github.com/anhle2501/oraclelinux-elasticsearch-kibana-logstash/blob/master/install.sh

## 5. Hình ảnh minh hoạ

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

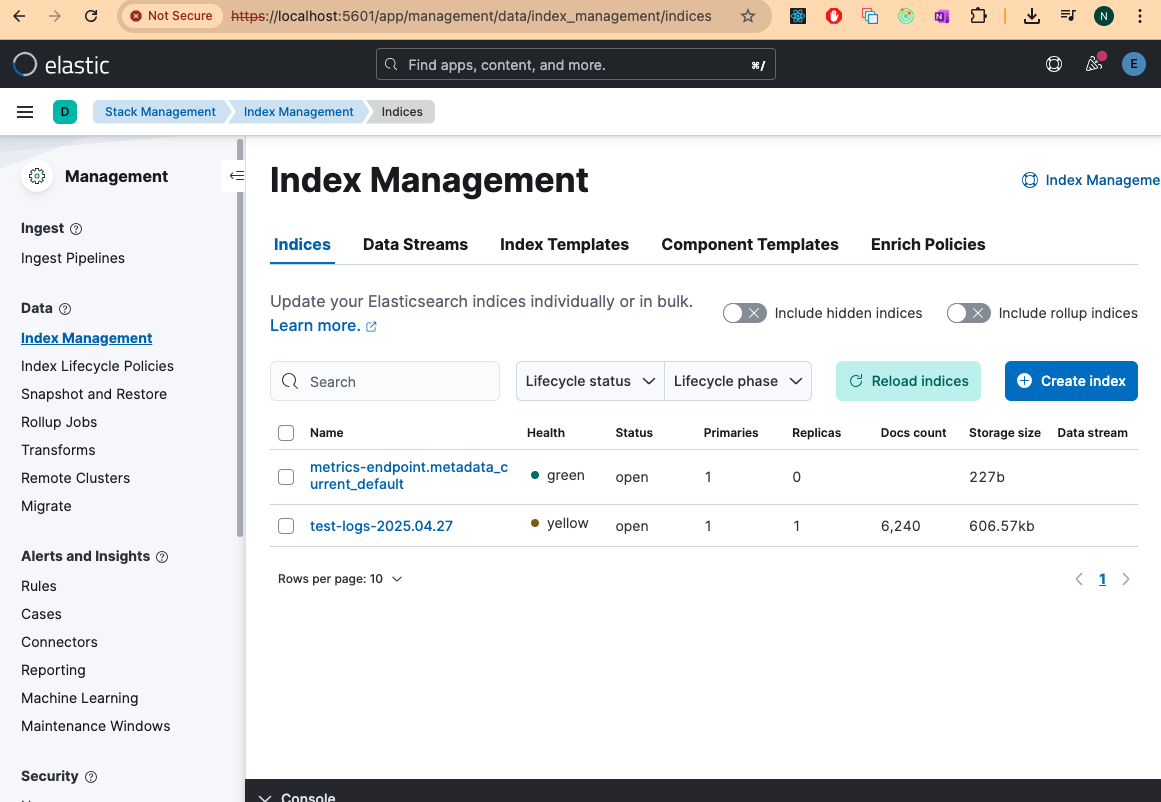
Description automatically generated

Hình 2: Hoàn thành cài đặt elasticsearch trên 1 node

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

Ghi chú:   
1. Các tài khoản kibana\_system, logstash\_system, logstash\_writer, apm\_system, beats\_system, remote\_monitoring\_user là các tài khoản sử dụng để gọi api giữa các phần mềm.  
2. Các tài khoản kibana, logstash, elasticsearch là tài khoản của hệ điều hành và không có quyền shell, chỉ để chạy service   
3. Tài khoản elastic là tài khoản admin dùng để đăng nhập vào api elasticsearch hoặc trang web kibana

## 6. Cài đặt Elasticsearch trên node khác và thêm node vào master

Sau khi cài đặt script trên node master, ta sẽ cài đặt script trên node worker. Trước hết ta sẽ chép file được script tạo sẵn ở thư mục home của máy đã cài script master. File có tên “elastic-stack-ca.p12”. Đây là file dùng để sinh các chứng chỉ cho node worker sử dụng để kết hợp với node master. Ta sẽ copy vào thư mục home của các node worker và chạy script với lệnh “sh install\_node.sh” nếu cài với user khác thì lệnh như sau “sh install\_node.sh <username>”

|  |  |  |
| --- | --- | --- |
| **#** | **Lệnh / khối lệnh** | **Mục đích (giải thích ngắn gọn)** |
| 1 | id -u $ES\_USER … || useradd … | Tạo tài khoản hệ thống **elasticsearch** (nếu chưa tồn tại). |
| 2 | tar -xzf … && ln -sfn … && chown … | Giải nén Elasticsearch vào /opt, tạo symlink cố định /opt/elasticsearch, gán quyền sở hữu cho user **elasticsearch**. |
| 3 | echo "vm.max\_map\_count=262144" …sysctl -w vm.max\_map\_count=262144 | Tăng tham số kernel vm.max\_map\_count – bắt buộc để Elasticsearch hoạt động. |
| 4 | if [[ -f "$HOME\_CA" ]]; then … | Kiểm tra sự tồn tại của **elastic-stack-ca.p12** (CA) đã copy từ master. Nếu có, cấu hình SSL cho node phụ; nếu không, chạy standalone không TLS. |
| 5 | elasticsearch-certutil cert --name "$NODE\_NAME" … | Sinh keystore **PKCS12** riêng cho node (data-1.p12) bằng CA, dùng chung pass phrase $CA\_PASS. |
| 6 | Khối SSL\_BLOCK= và ghi elasticsearch.yml | Tạo block cấu hình bảo mật (HTTP + Transport TLS) và cấu hình tham số cluster (cluster.name, node.name, discovery.seed\_hosts, publish\_host). |
| 7 | Ghi /etc/systemd/system/elasticsearch.service | Định nghĩa service **systemd** để quản lý Elasticsearch, đặt giới hạn file-handle và chỉ định JDK đi kèm. |
| 8 | systemctl daemon-reload, enable, start | Nạp service, cấu hình tự khởi động cùng hệ thống, khởi chạy node Elasticsearch. |
| 9 | Vòng until curl -ks https://localhost:9200 | Chờ tới khi cổng HTTPS 9200 sẵn sàng để xác nhận node đã lên và TLS hoạt động. |

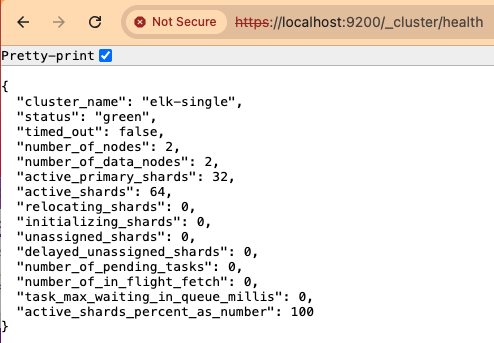
Sau khi chạy, node worker sẽ liên kết với node master để chạy theo vai trò đã được chỉ định trong file cấu hình “elasticsearch.yml” nằm ở đường dẫn “/opt/elasticsearch/config/elasticsearch.yml”.

Tải toàn bộ script ở link sau:

https://github.com/anhle2501/oraclelinux-elasticsearch-kibana-logstash/blob/master/elastic\_node/install\_node.sh  
  
A screenshot of a computer program

Description automatically generated

Hình 7: Log hiển thị khi đã cài thành công script trên node worker

  
Hình 8: Node data đã vào cụm elastic thành công  
Các node khác sau khi thêm vào làm tương tự

---HẾT---