ELK Stack là tập hợp 3 phần mềm đi chung với nhau, phục vụ cho công việc logging. Ba phần mềm này lần lượt là:

* **Elasticsearch**: Cơ sở dữ liệu để lưu trữ, tìm kiếm và query log
* **Logstash**: Tiếp nhận log từ nhiều nguồn, sau đó xử lý log và ghi dữ liệu và Elasticsearch
* **Kibana**: Giao diện để quản lý, thống kê log. Đọc thông tin từ Elasticsearch

Cơ chế hoạt động của ELK Stack cũng khá đơn giản, các bạn xem hình sẽ hiểu:

[](https://toidicodedao.files.wordpress.com/2018/02/12.png)

Cơ chế hoạt động của ELK Stack

1. Đầu tiên, log sẽ được đưa đến *Logstash*. (Thông qua nhiều con đường, ví dụ như server gửi UDP request chứa log tới URL của Logstash, hoặc Beat đọc file log và gửi lên Logstash)
2. *Logstash* sẽ đọc những log này, thêm những thông tin như thời gian, IP, parse dữ liệu từ log (server nào, độ nghiêm trọng, nội dung log) ra, sau đó ghi xuống database là *Elasticsearch*.
3. Khi muốn xem log, người dùng vào URL của *Kibana*. Kibana sẽ đọc thông tin log trong *Elasticsearch*, hiển thị lên giao diện cho người dùng query và xử lý.

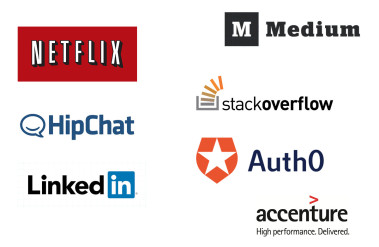
**Tại sao phải dùng ELK Stack?**

Với các hệ thống hoặc ứng dụng nhỏ, ta không cần sử dụng ELK stack làm gì! Cứ **dùng thư viện ghi log** đi kèm với ngôn ngữ, sau đó ghi log ra file rồi đọc thôi!

Tuy nhiên, với những [hệ thống lớn nhiều người dùng](https://toidicodedao.com/2017/11/28/review-sach-release-it-xay-dung-va-thiet-ke-he-thong-trau-bo-cho-hang-trieu-nguoi-dung/), có nhiều service phân tán ([microservice](https://toidicodedao.com/2017/02/21/tong-quan-micro-service/)), có nhiều server chạy cùng lúc… thì việc ghi log xuống file **không còn hiệu quả nữa**.

Giả sử bạn có 10 con server chạy cùng lúc, bạn sẽ phải **lục tung 10 con server** này để đọc và tìm file log, cực quá phải không nào? Lúc này, người ta bắt đầu áp dụng centralized logging, tức **ghi log tập trung** vào 1 chỗ.

ELK là một lựa chọn cực kì phù hợp, được nhiều công ty lớn như **Netflix, Linkedin, Medium** lựa chọn vì những lý do bên dưới!

[](https://toidicodedao.files.wordpress.com/2018/02/elk-stack-company.jpg)Các công ty sử dụng ELK Stack

Tutorial:

Windown

<https://www.edureka.co/blog/elk-stack-tutorial/>

linux: <https://logz.io/learn/complete-guide-elk-stack/#beats>

ubuntu: <https://www.digitalocean.com/community/tutorials/how-to-install-elasticsearch-logstash-and-kibana-elk-stack-on-ubuntu-14-04>