# Bài tập 2

## Nội dung

Cấu hình Nginx access\_log output ở dạng JSON và log được remote đến CLM qua network, UDP port 514. CLM thực hiện lưu trữ log local, đồng thời forward đến Logstash (với input udp) để tiến hành xử lý, output đến Elasticsearch.

## Yêu cầu

* Cài đặt Nginx (phiên bản phải >= 1.7.1) và cấu hình access\_log (dạng JSON), error\_log về CLM với remote syslog-ng, sử dụng UDP port mặc định 514.
* CLM cài đặt và cấu hình để lưu lại log Nginx tại local, đồng thời gởi đến Logstash.
* Logstash được cấu hình listen trên UDP, port 5100.
* CLM syslog-ng và Logstash được cấu hình phù hợp để đạt kết quả cuối cùng là có dữ liệu được parse thành công, có thể view trên giao diện của Kibana.

## Yêu cầu nộp bài

(các hình chụp phải rõ nét, các hình chụp không nhìn rõ text sẽ không được tính)

* 1 hình chụp cấu hình access\_log của Nginx.
* 1 hình chụp cấu hình syslog-ng hoàn chỉnh (bao gồm nhận log, lưu log local, forward đến Logstash)
* 1 hình chụp cấu hình Logstash hoàn chỉnh (bao gồm input UDP, filter và output).
* 1 hình chụp kết quả log Nginx đã được phân tách thành công tại giao diện của Kibana.