**Giới thiệu, lịch sử, phù hợp với ứng dụng nào, cài đặt sử dụng**

1. **Lịch sử hình thành:**

* Logstash được tạo ra bởi Jordan Sissel, người có kinh nghiệm về quản lý hệ thống, luôn phải đối mặt với khối lượng lớn các tệp tin, từ đó thực sự cần một hệ thống tập trung để tổng hợp và quản lý chúng. Logstash được sinh ra theo tiền đề này và trong năm 2013 Sissel đội với Elasticsearch.
* Logstash tiếp tục phát triển với những thành phần ngăn xếp ELK khác. Bây giờ là một phần của một nền tảng toàn diện cho cho dữ liệu đăng nhập và phân tích, cung cấp cho các công ty về thông tin khách hàng với sự hỗ trợ của hệ thống.

1. **Giới thiệu:**

* Logstash là một công cụ mã nguồn mở thu thập dữ liệu có khả năng liên hợp theo thời gian thực. Logstash có thể hợp nhất dữ liệu từ các nguồn khác nhau và chuẩn hóa dữ liệu ở phần xử lý tiếp theo. Loại bỏ và đồng hóa tất cả dữ liệu đó trong một số use case cần phân tích và thể hiện trên biểu đồ.
* LogStash cung cấp một Framework tích hợp cho việc thực hiện các công việc liên quan đến thu thập log, tập trung log, phân tích các thành phần trong log, lưu trữ log, và tìm kiếm trong log.
* **INPUT**: Nó có thể lấy đầu vào từ TCP/UDP, các file, từ syslog, Microsoft Windows EventLogs, STDIN và từ nhiều nguồn khác. Chúng ta có thể lấy log từ các ứng dụng trên môi trường của chúng ta rồi đẩy chúng tới Logstash.
* **FILTER**: Khi những log này tới Server Logstash, có một số lượng lớn các bộ lọc mà cho phép ta có thể chỉnh sửa và chuyển đổi những event này. Ta có thể lấy ra các thông tin mà ta cần từ những event log.
* **OUTPUT**: Khi xuất dữ liệu ra, Logstash hỗ trợ rất nhiều các đích tới bao gồm TCP/UDP, email, các file, HTTP, Nagios và số lượng lớn các dịch vụ mạng. Ta có thể tích hợp Logstash với các công cụ tính toán số liệu (metric), các công cụ cảnh báo, các dạng biểu đồ, các công nghệ lưu trữ hay ta có thể xây dựng một công cụ trong môi trường làm việc của chúng ta.
* LogStash được viết trên JRuby và chạy trong JVM (Java Virtual Machine). So với một số giải pháp khác thường phân tách các chức năng, LogStash chỉ có một agent được cấu hình để thực hiện nhiều nhiệm vụ khác nhau.
* Hệ sinh thái LogStash có 4 thành phần như sau:

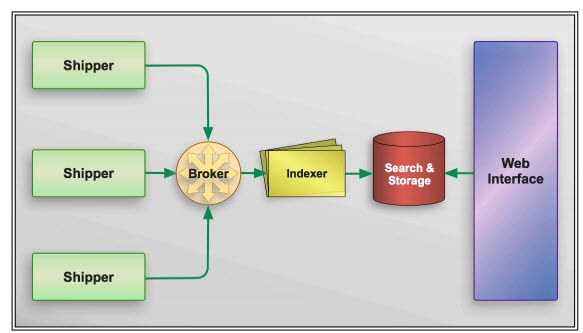
+ Shipper

+ Broker và Indexer

+ Search và Storage

+ Web Interface – còn gọi là Kibana

* LogStash chỉ là tên gọi thông thường, tên gọi phổ biến hơn là ELK – là thuật ngữ viết tắt của 3 giải pháp tích hợp lại, bao gồm: E – ElasticSearch, L – LogStash, và K – Kibana.
* LogStash có thể chạy 1 hoặc nhiều thành phần bên trên độc lập, hoặc chung trên 1 hệ thống.
* Có thể chia kiến trúc của LogStash làm 2 phần:

[](http://i2.wp.com/blogit.edu.vn/wp-content/uploads/2014/11/1.jpg)

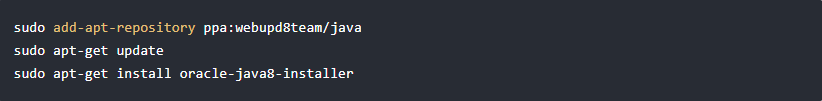
*Kiến trúc ELK*

* Các Hosts chạy các LogStash agent. Trên các host này sẽ có 1 agent LogStash chạy với mục đích thu thập thông tin về log như log của ứng dụng, dịch vụ, log của hosts và gởi đến LogStash Server. Đây chính là thành phần Shipper trong kiến trúc của LogStash.
* Các Hosts chạy các thành phần còn lại bao gồm Broker, Indexer, Search & Storage, Web Interface. Các host này sẽ thực hiện việc nhận, xử lý, lưu trữ các log từ các agent đổ về.

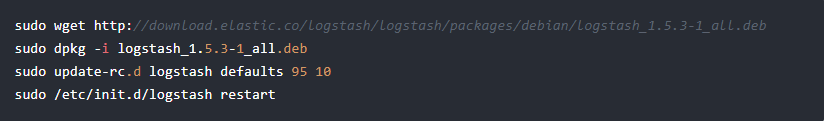
1. **Thích hợp với những ứng dụng:**

* Logstash hỗ trợ rất nhiều các đích tới bao gồm TCP/UDP, email, các file, HTTP, Nagios

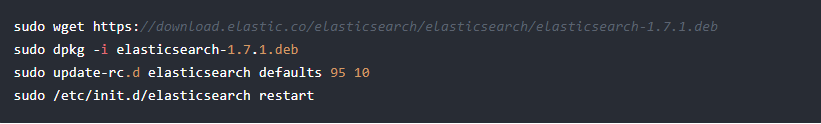
1. **Cài đặt Logstash**
2. Cài đặt java, nên cài đặt java, nên cài đặt phiên bản từ java 7 trở lên. Tốt nhất là cài đặt phiên bản java mới nhất.



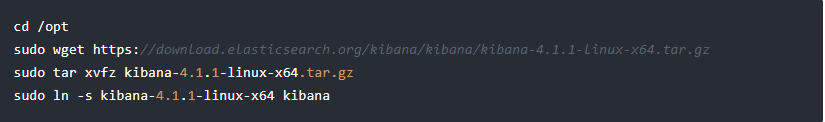
1. Cài đặt logstash:



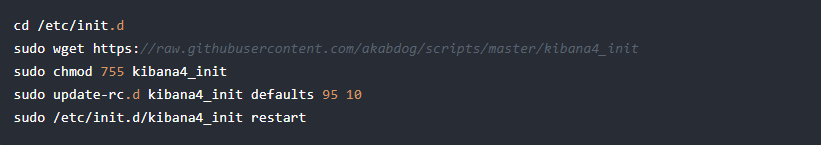
1. Cài đặt Elasticsearch:



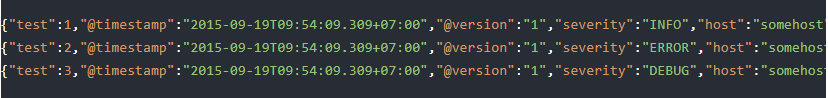
1. Cài đặt kibana



1. Khởi động kibana tự động

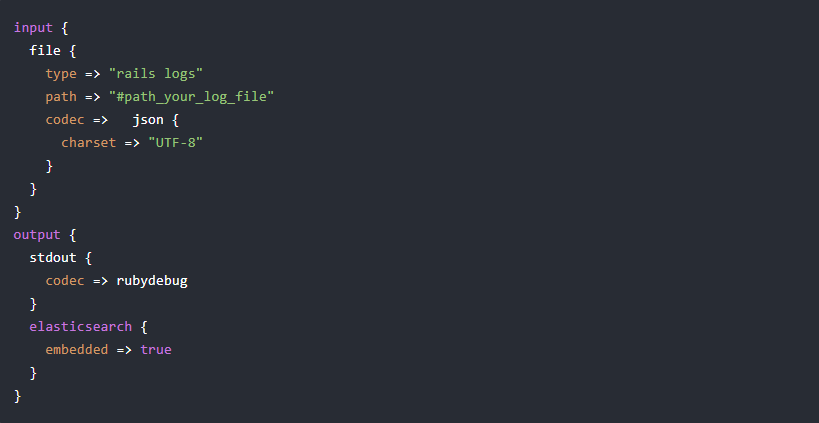


1. **Sử dụng Logstash, Elasticsearch, Kibana với Rails**
2. Để sử dụng Logstash, Elasticsearch, Kibana hiệu quả thì log của Rails cũng cần được lưu trữ dưới dạng Json. Một số gem hỗ trợ việc lưu trữ log dưới dạng Json cho Rails, trong đó gem logstash-logger khá tiện lợi, dễ dùng và được đánh giá cao.
3. Ví dụ một số log được lưu trữ bởi logstash-logger



1. Chạy logstash và config cho logstash đọc thông tin log thì file log của server như sau

example.config



1. khởi động logstash và sử dụng file config này để cấu hình cho logstash



1. Khởi động lại elasticsearch



1. Vào địa chỉ localhost:5601 và có thể thấy các log đã được hiển thị lên. Bạn có thể tìm kiếm các log, hoặc tạo biểu đồ cho log. Như vậy việc cài đặt và sử dụng bộ công cụ Logstash, Elashticsearch, Kibana đã hoàn tất.

