Giới Thiệu Về LogStash Và ELK

Chilm

10 Tháng Mười Một, 2014 Monitoring, Security, Series Hữu Ích 0 Comments

Quản lý log trong hệ thống bao giờ cũng là một vấn đề đau đầu. Bài viết này giới thiệu sơ bộ về Logstash, là công cụ quản trị log tập trung với nhiều tính năng, ưu điểm.

1. Giới thiệu

– LogStash là công cụ được dùng để quản trị tập trung log, hơn thế nữa, sách TheLogStashBook miêu tả LogStash là một hệ sinh thái (EcoSystem) và bao gồm nhiều thành phần như thu thập dữ liệu, phân tích log, hiển thị thông tin và cảnh báo, … (trang 8).

– 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.

– LogStash là công cụ nguồn mở theo giấy phép Apache 2.0 và có nhiều cơ chế thu thập nguồn dữ liệu đầu vào, chẳng hạn TCP/UDP, Syslog, Windows Event log, file, STDIN, và các thể loại khác. Đó là đối với dữ liệu đầu vào, dữ liệu đầu ra của LogStash cho phép thích hợp với nhiều hệ thống khác nhau như TCP/UDP, email, files, HTTP, Nagios, … LogStash có thể được sử dụng kết hợp với nhiều công cụ cảnh báo, vẽ biểu đề, hệ thống lưu trữ riêng, hoặc xây dựng một hệ thống tích hợp riêng đối với từng môi trường cụ thể.

2. Kiến trúc LogStash

– 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

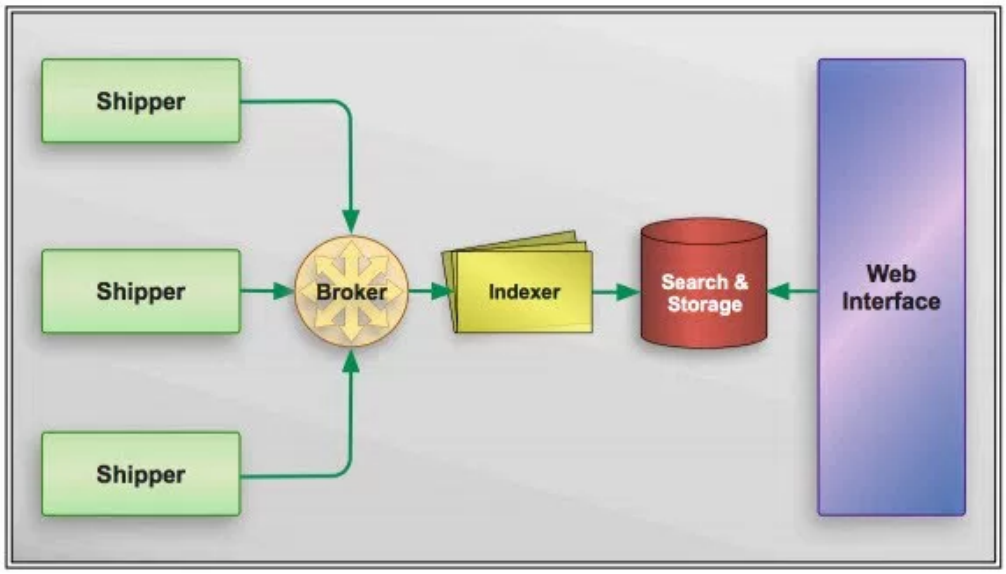
+ Search và Storage

+ 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:



Kiến trúc ELK

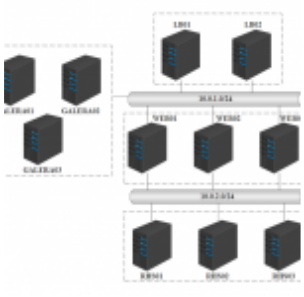
+ Các Hosts chạy các LogStash agent. Trên các host này sẽ có 1 agent LogStash chạy với mục đích thu thập thông tin về log như log của ứng dụng, dịch vụ, log của hosts và gởi đến LogStash Server. Đây chính là thành phần Shipper trong kiến trúc của LogStash.

+ 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.

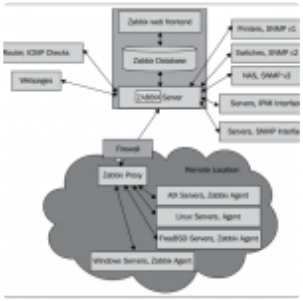
Monitoring Security Series hữu ích

Bài viết liên quan

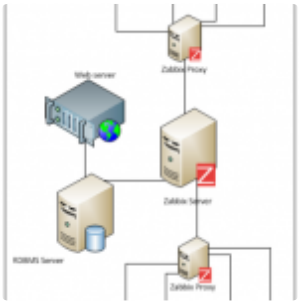
Cài đặt Zabbix agent trên CentOS



OwnCloud – Bài 3: Cài đặt hệ thống có tính sẵn sàng cao



Tính năng và kiến trúc Zabbix



Các mô hình triển khai Zabbix

Series hữu ích

OwnCloud – Bài 3: Cài đặt hệ thống có tính sẵn sàng cao

OpenVZ & ISPConfig – Phần 3: Thử nghiệm chức năng OpenVZ

OpenVZ & ISPConfig – Phần 2: Cài đặt OpenVZ

OpenVZ & ISPConfig – Phần 1: Cài đặt ISPConfig All-in-one

Cài đặt Zabbix – Phần 4: Cấu hình Zabbix Front-end

Cài đặt Zabbix – Phần 3: Cài đặt (tt)

Cài đặt Zabbix – Phần 2: Cài đặt

Cài đặt Zabbix – Phần 1: Yêu cầu cơ bản

Các mô hình triển khai Zabbix

Tính năng và kiến trúc Zabbix