

Project Plan

Hệ thống Logging & Monitoring

Ngày phát hành:

Tháng 11, Năm 2018

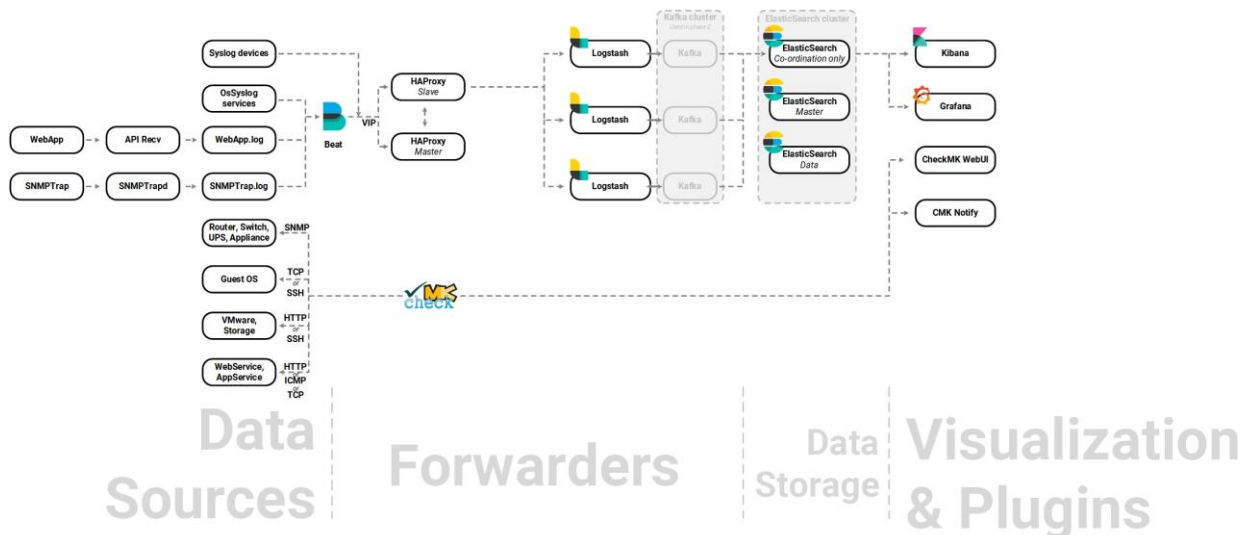
Điều khoản bảo mật thông tin

Giải pháp và các tài liệu hỗ trợ đi cùng có đề cập đến các thông tin mật cũng như thông tin kinh doanh riêng tư thuộc sở hữu của EVNFC. Tài liệu này có thể được in hoặc sao chép để phục vụ mục đích đánh giá dự án đang đề xuất. Nghiêm cấm chia sẻ tài liệu đến các bên thứ ba hoặc cá nhân ngoài tổ chức và dự án.

MỤC LỤC

1.	Mô hình đề xuất.....	3
2.	Các giai đoạn tổng thể của project.....	4
3.	Mô tả các giai đoạn.....	4
4.	Các features phân bổ theo giai đoạn	5
5.	Lượng tài nguyên hệ thống cần thiết.....	6
6.	Hướng phát triển	7
7.	PHỤ LỤC	8

1. Mô hình đề xuất



Mô hình logic của hệ thống

Diễn giải mô hình:

- Mô hình bao gồm 2 phần:
 - o Phần 1: Logging
 - Bao gồm các thành phần:
 - HAProxy: tiếp nhận log và chuyển log vào cổng đã mở sẵn của LogStash.
 - Logstash: lọc, chuẩn hóa và chuyển tiếp log đến Elasticsearch.
 - Elasticsearch: chứa log và sẵn sàng cho việc truy xuất dữ liệu từ Grafana
 - Grafana & Kibana: tìm kiếm log và thể hiện log thành biểu đồ trực quan.
 - Kafka (giai đoạn 2): streaming dữ liệu.
 - Hệ thống logging thu thập dữ liệu log từ nhiều nguồn khác nhau, như: Syslog devices (router, switch, firewall...), OSSyslog service (Linux, Windows...), WebApp log (Apache, Nginx, IIS...) và các thiết bị hỗ trợ SNMP khác.
 - Dữ liệu log thu thập được sẽ được lọc và điều chỉnh bởi LogStash trước khi lưu và Elasticsearch.
 - Dữ liệu sau khi đã được index tại Elasticsearch sẽ được các công cụ như Kibana & Grafana truy xuất để thể hiện log thành các dạng biểu đồ, bảng biểu, thông số...
 - o Phần 2: Monitoring
 - Bao gồm các thành phần:
 - CheckMK

- CheckMK Dashboard
- Các plugin khác
- Hệ thống Monitoring thu thập metric từ các nguồn như: OS (Linux, Windows...), thiết bị mạng (Router, Switch, Firewall...), hypervisor/virtualization orchestrator (VMWare, Hyper-V...), các dịch vụ khác (Web Service, App Service...).
- Dữ liệu metric không giống như dữ liệu log, không lưu trữ lâu dài.
- CheckMK sẽ thu thập dữ liệu metric như: CPU, Disk I/O, Network traffic, Network Ingress, Network Egress, Memory (Committed bytes in use, free memory...)
- Dữ liệu CheckMK sẽ được thể hiện ở CheckMK Dashboard và tương tác với các plugin hỗ trợ.

2. Các giai đoạn tổng thể của project

Các mốc của project, xem sơ đồ bên dưới.



Phân bổ công việc project theo thời gian (6 tháng)

3. Mô tả các giai đoạn

Tổng thể, project chia làm 2 giai đoạn chính:

- Giai đoạn 1: Phần Logging (3 tháng)
 - o Cài đặt server và dịch vụ (2 tuần): cài đặt các server, các dịch vụ logging và tuning + optimizing hệ thống.

- Nhận log, filter log, indexing log (2 tháng) từ 3 nguồn : Syslog device, OsSyslog và Application.
- Dựng dashboard dựa trên loại log thu thập được (2 tuần)
- Giai đoạn 2: Phần Logging nâng cao và Monitoring (3 tháng)
 - Logging nâng cao
 - SNMP Trapd (1 tháng)
 - Tuning & Optimizing hệ thống (2 tháng) theo tình trạng dữ liệu tại thời điểm diễn ra.
 - Monitoring:
 - Triển khai CheckMK và nhận dữ liệu từ các nguồn về máy chủ (2 tuần).
 - CheckMK Dashboard và các plugin hỗ trợ (1 tháng).
 - Filter Metrics từ các nguồn (1 tháng) để giảm lượng dữ liệu dư thừa.

4. Các features phân bổ theo giai đoạn

GAİI ĐOẠN	TÍNH NĂNG
1	<ul style="list-style-type: none"> - Syslog support - OsSyslog support - Application log support - Syslog filtering - Application log filtering - Syslog visualization - OsSyslog visualization - Application log visualization
2	<ul style="list-style-type: none"> - SNMP support - SNMP log filtering - SNMP log visualization - Audit Log separated from common log - Guest OS (Windows Linux) monitoring - Virtualization orchestration monitoring - Storage monitoring - Network device monitoring - Application monitoring

	<ul style="list-style-type: none"> - User management (Authentication & Authorization) - Notify monitoring status to administrators.
--	---

5. Lượng tài nguyên hệ thống cần thiết

Giai đoạn 1:

LOẠI TÀI NGUYÊN	SỐ LƯỢNG	CẤU HÌNH	GHI CHÚ
Server/VM	1	2 CPUs, 2GB memory, 16GB disk	HAProxy Master
Server/VM	1	2 CPUs, 2GB memory, 16GB disk	HAProxy Slave
Server/VM	1	3 CPUs, 6GB memory, 20GB disk	LogStash 1 (clustering)
Server/VM	1	3 CPUs, 6GB memory, 20GB disk	LogStash 2 (clustering)
Server/VM	1	4 CPUs, 4GB memory, 20GB disk	ElasticSearch (co-ordination only)
Server/VM	1	4 CPU, 8GB memory, 40GB disk	ElasticSearch (master)
Server/VM	1	4 CPU, 8GB memory, 500GB disk	ElasticSearch (data)
Server/VM	1	3 CPU, 6GB memory, 40GB disk	Kibana & Grafana
IP	1	Static private IP	HAProxy Master IP
IP	1	Static private IP	HAProxy Slave IP
IP	1	Static private IP	HAProxy cluster virtual IP
IP	1	Static private IP	Logstash 1 IP
IP	1	Static private IP	Logstash 2 IP
IP	1	Static private IP	ElasticSearch co-ordination IP
IP	1	Static private IP	ElasticSearch master IP

IP	1	Static private IP	ElasticSearch data ip
IP	1	Static private IP	Kibana & Dashboard IP

Giai đoạn 2:

LOẠI TÀI NGUYÊN	SỐ LƯỢNG	CẤU HÌNH	GHI CHÚ
Server/VM	1	4 CPUs, 16GB memory, 100GB disk	CheckMK server
IP	1	Static private IP	CheckMK IP
Email Account	1	Email account	Email account cho notification

6. Hướng phát triển

Hướng phát triển:

- Phát triển phương pháp auto deployment để giảm chi phí triển khai
- Tích hợp Multi-Factor Authentication
- Tích hợp Single Sign On
- Phát triển dashboard riêng dựa trên API, không sử dụng của third-party.

7. PHỤ LỤC



Nỗ lực là người

DẪN ĐẦU >



ĐỊA CHỈ

Chi nhánh TP. HCM:
Địa chỉ: Tầng 6, tòa nhà
ACM, 96 Cao Thắng,
Phường 4, Quận 3



LIÊN HỆ

Tư vấn kinh doanh:
+ 84 8 73007373



EMAIL

Tư vấn kinh doanh:
nguyentt3@fpt.com.vn

Tư vấn kỹ thuật:
nhutvm3@fpt.com.vn

©2018 Bản quyền thuộc về công ty Hệ Thống Thông Tin FPT, thuộc tập đoàn FPT. Tất cả các tên, sản phẩm khác đều thuộc bản quyền, tác nhân của công ty, tổ chức tương ứng. Chúng tôi có quyền đưa ra những cập nhật mới nhất mà không cần thông báo trước.

Để biết thêm thông tin chi tiết về FPT IS, vui lòng tham khảo website của chúng tôi ở: www.fis.com.vn/en/