****

**CÔNG TY CỔ PHẦN GIẢI PHÁP PHẦN MỀM TÀI CHÍNH**

**TÀI LIỆU HƯỚNG DẪN CÀI ĐẶT MONITOR LOG CHO PRODUCTION**

**Phiên bản: v1.0**

**Hồ Chí Minh, 3 – 2024**

**Bảng ghi nhận thay đổi tài liệu**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Ngày thay đổi** | **Mục thay đổi** | **Lý do** | **Mô tả thay đổi** | **Phiên bản mới** |
| 11/03/2024 |  | Viết lần đầu |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**Trang ký**

Người lập: Bùi Thế Minh Hiếu Ngày: 11/03/2024

Người xem xét: Nguyễn Đức Song Toàn Ngày:

Người duyệt: Lê Đức Trường Ngày:

**MỤC LỤC**

[1. GIỚI THIỆU TÀI LIỆU 6](#_Toc164094047)

[1.1. Mô hình 6](#_Toc164094048)

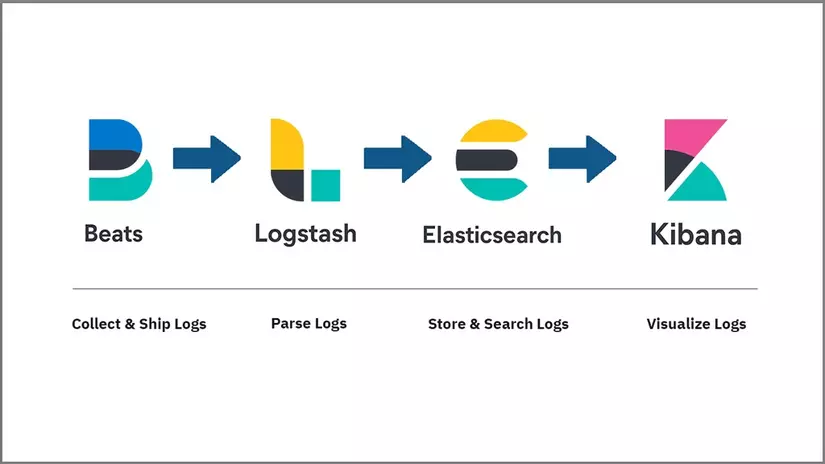
[1.2. Yêu cầu 7](#_Toc164094049)

[1.3. Hướng dẫn cài đặt 7](#_Toc164094050)

[1.4. Hướng dẫn vận hành 9](#_Toc164094051)

1. GIỚI THIỆU TÀI LIỆU

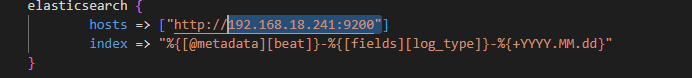
Tài liệu này được viết nhằm mục đích

* Hướng dẫn cài đặt log tập trung elasticsearch
  1. Mô hình
* **Beats** - gửi dữ liệu thu thập từ files log của máy đến Logstash (cài ở máy chứa log)
* **Logstash** - thành phần xử lý dữ liệu, sau đó nó gửi dữ liệu nhận được cho Elasticsearch để lưu trữ (cài ở máy chứa log)
* **Elasticsearch** - máy chủ lưu trữ và tìm kiếm dữ liệu log (cài ở máy monitor log)
* **Kibana** - ứng dụng nền web để tìm kiếm và xem trực quan các logs (cài ở máy monitor log)
  1. Yêu cầu
* **Các máy phải cài docker**
* **Lấy files monitor\_grafana ở trên git dockerconfig branch monitor\_grafana**
  1. Hướng dẫn cài đặt
* Bước 1: Copy monitor\_elacsticsearch vaò thư mục /app của máy cài monitor log

chown -R 1000:1000 /app/elasticsearch/data

./start-elk.sh

* Bước 2: Kết nối vào <http://IP_MONITOR_LOG:5601/> để kiểm tra đã start thành công chưa
* Bước 3: Cài đặt logstash ở các máy chứa log cần lấy
* Copy 3 thư mục logstash, logstash.yml, stop-logstash.sh, start-logstash.sh ở thư mục monitor\_elacsticsearch vào máy
* Sửa logstash/pipeline/logstash.conf như hình dưới thành IP\_MONITOR\_LOG:9200



* Sửa logstash/config/ logstash.yml như hình dưới thành IP\_MONITOR\_LOG:9200



* Bước 4: bash ./start-logstash.sh
* Bước 5: Cài đặt filebeat version 8 ở các máy chứa log cần lấy. Lưu ý: các bước dưới là cài dành cho linux phiên bản apt nếu sử dụng phiên bản khác thì tham khảo tại link: <https://www.elastic.co/guide/en/beats/filebeat/current/filebeat-installation-configuration.html>

wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add

sudo apt-get install apt-transport-https

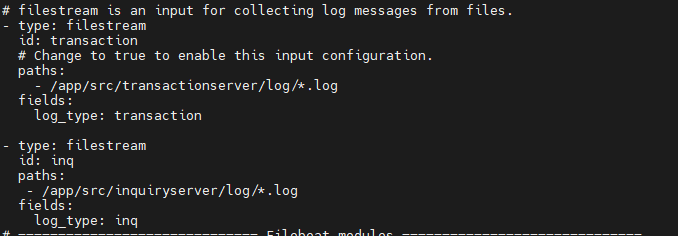
echo "deb https://artifacts.elastic.co/packages/8.x/apt stable main" | sudo tee -a /etc/apt/sources.list.d/elastic-8.x.list

sudo apt-get update && sudo apt-get install filebeat

sudo systemctl enable filebeat

* Bước 6: Copy filebeat.yml được lấy từ thư mục cài đặt vào files /etc/filebeat (tùy cách cài mà thư mục này sẽ ở vị trí khác nhau)

+ Sửa và thêm thư mục log cho phù hợp như hình dưới log\_type, id để phân biệt service nào, máy nào (đặt tên lại cho phù hợp với 2 trường này), paths là thư mục chưa log cần đọc. Lưu ý: lần đâu cài nên backup và xóa hết các log cũ đi



+ Sửa output.logstash thành ip máy hiện tại



+ Start filebeat

systemctl start filebeat

* Bước 7: Vào link <http://IP_MONITOR_LOG:5601/app/management/data/index_management/indices> để xem đã có index được tạo từ log chưa (f5 vài lần nếu chưa có)
  1. Hướng dẫn vận hành
* Start elasticsearch, kibana: bash ./start-elk.sh
* Stop elasticsearch, kibana: bash ./stop-elk.sh
* Start logstash: bash ./start-logstash.sh
* Stop logstash: bash ./stop-logstash.sh
* Start filebeat: systemctl start filebeat
* Stop filebeat: systemctl stop filebeat