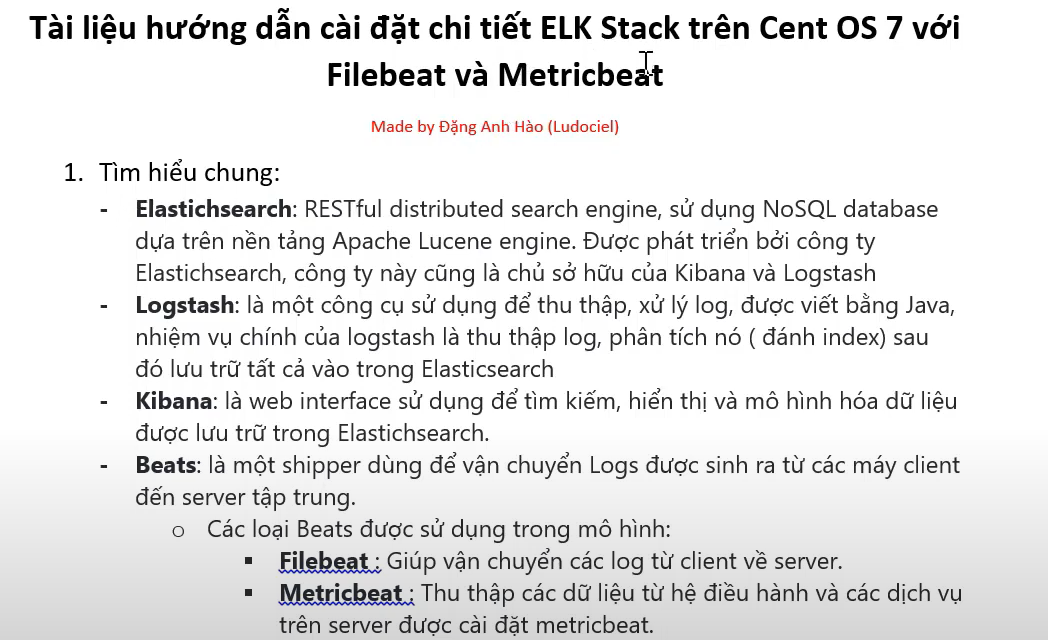
# ELK

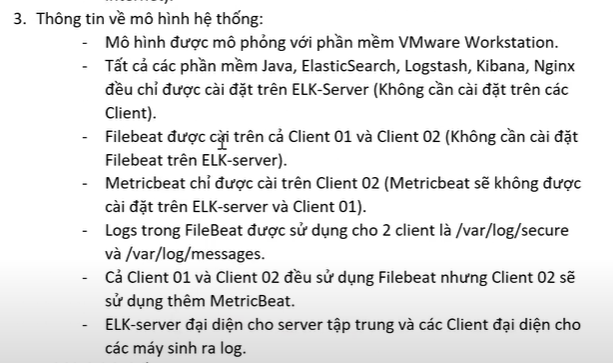


c. phần mềm

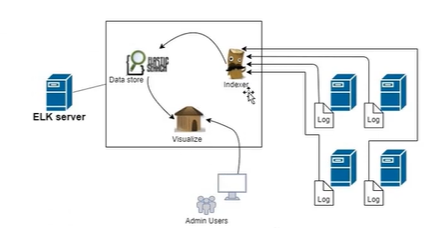
Java 8 được yêu cầu bời Logstash và Elasticsearch, các phiên bản java khác ko có tác dụng

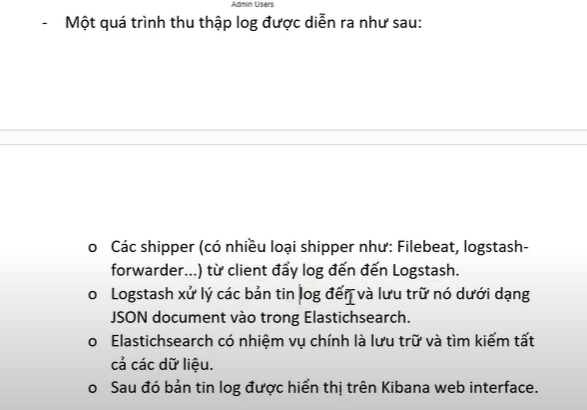
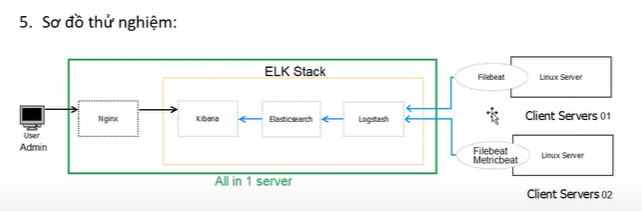
Logstash, Elasticsearch, Kibana, Filebeat và Metricbeat đều dùng chung version

Nginx để làm reserve proxy cho Kibana (Nginx ủy quyền cho Kibana để Kibana có thể được truy cập qua các Web browser ngoài internet)



* Mô hình

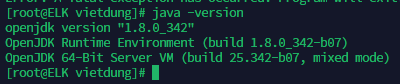


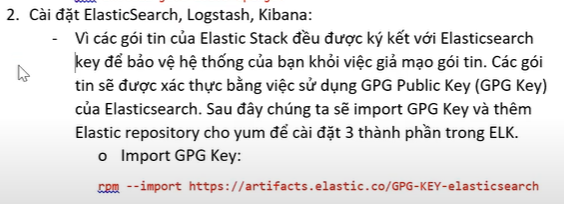
 

## Cài đặt

* Cài java 8 JDK

yum -y install java-openjdk-devel java-openjdk



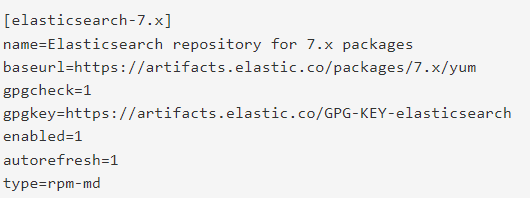


rpm --import <https://artifacts.elastic.co/GPG-KEY-elasticsearch>

* Thêm repository for elastichSearch

vim /etc/yum.repos.d/elasticsearch.repo

thêm đoạn này vào



Cách để thêm nhanh:

cat >> /etc/yum.repos.d/elasticsearch.repo << EOF

[elasticsearch-7.x]

name=Elasticsearch repository for 7.x packages

baseurl=https://artifacts.elastic.co/packages/7.x/yum

gpgcheck=1

gpgkey=https://artifacts.elastic.co/GPG-KEY-elasticsearch

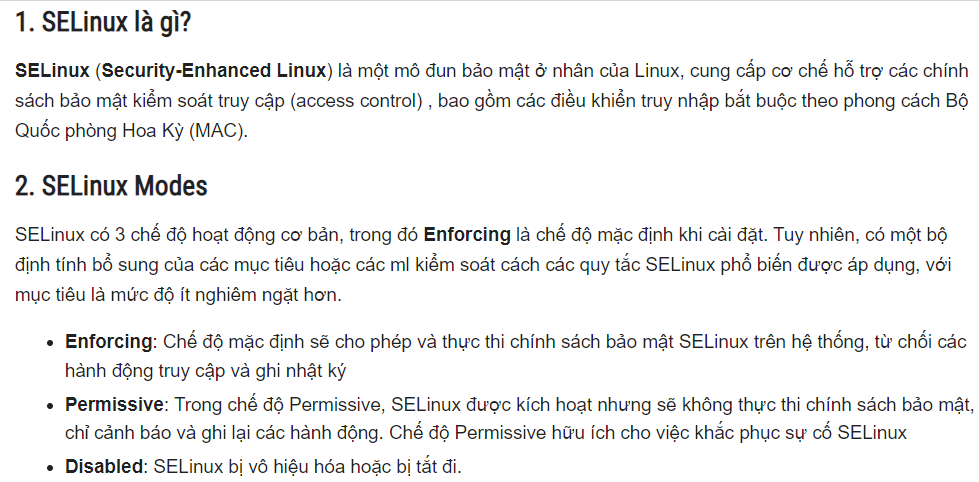
enabled=1

autorefresh=1

type=rpm-md

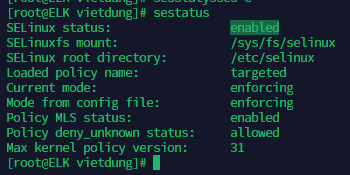
EOF

* Tắt Selinux



* Check Selinux

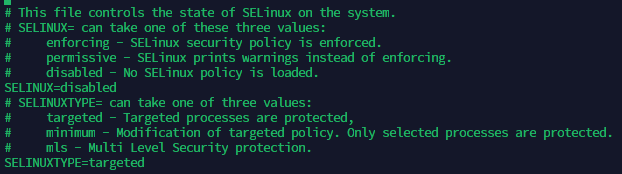
sestatus



* Tắt se

sed -i 's/\(^SELINUX=\).\*/\SELINUX=disabled/' /etc/sysconfig/selinux

hooặc vào **/etc/sysconfig/selinux** đổi thành disable



Reboot lại máy và check lại sestatus

## Cài đặt và cấu hình ElastichSearch

yum clean all && yum makecache && yum -y install elasticsearch

* Sửa đổi file config của elastichSearch

nano /etc/elasticsearch/elasticsearch.yml



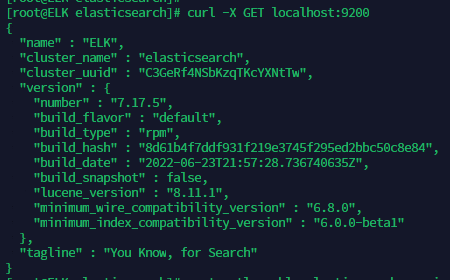
#network.host: 192.168.0.1 -> network.host: localhost

* Start elasticsearch

systemctl restart elasticsearch.service

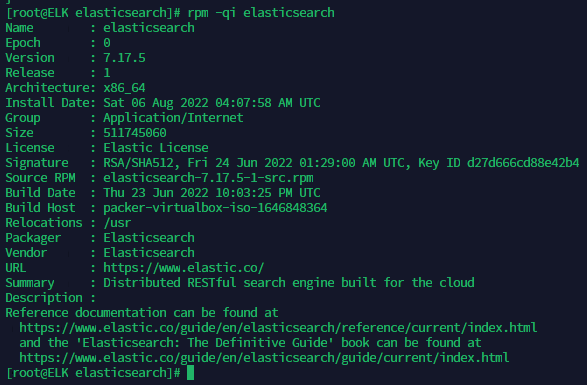
systemctl enable elasticsearch.service

enable tức là để khi start máy thì elasticsearch cũng sẽ được start cùng luôn, giống trong Startup của Task Manager window



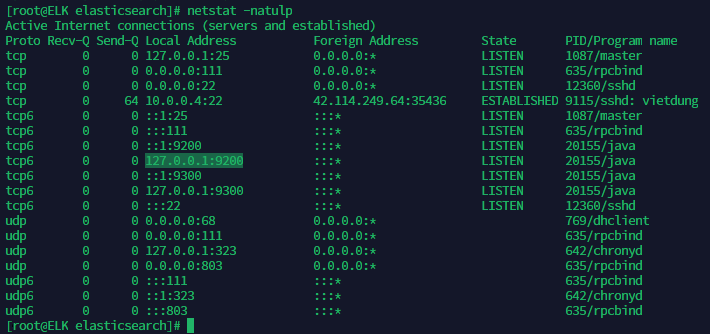
Oke, đã install xog

rpm -qi elasticsearch



Nếu có bất kỳ thay đổi nào liên quan đến ELK, thì phải **restart** Elasticsearch

netstat -natulp

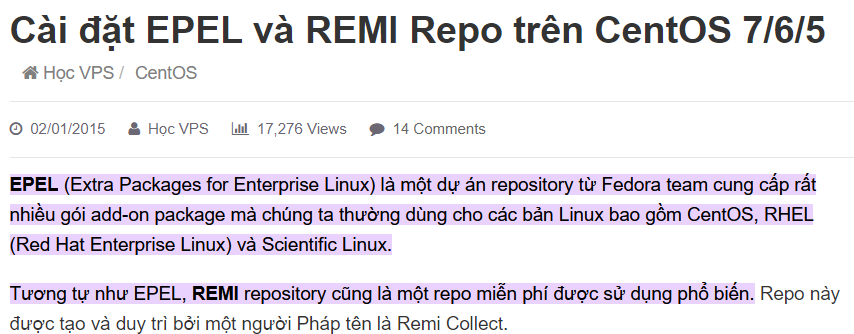


## 2. cài đặt và cấu hình Kibana

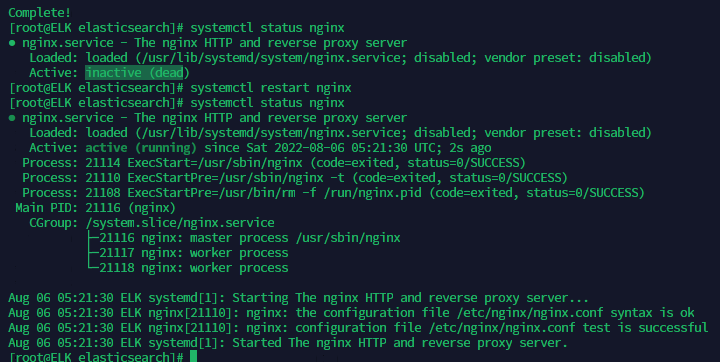
Install Proxy nginx trước

yum install epel-release

yum install nginx



Sau khi cài xong nginx



systemctl restart nginx

systemctl enable nginx (để nginx bật mỗi khi khởi động máy)\_

Check firewall

sudo firewall-cmd --state



* Cài đặt Kibana

yum -y install kibana

config kibana

nano /etc/kibana/kibana.yml

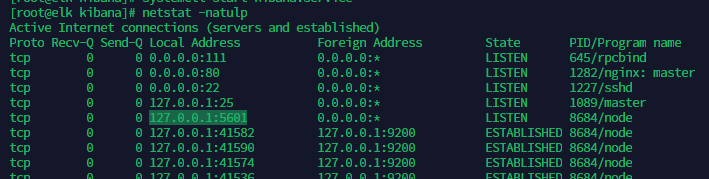
#server.host: "localhost" -> server.host: "localhost"



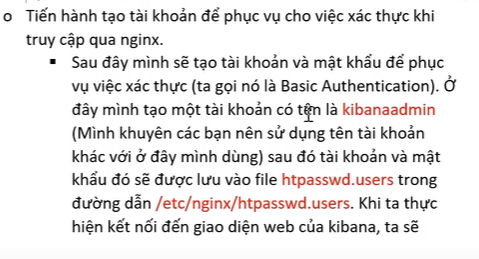
systemctl enable kibana.service

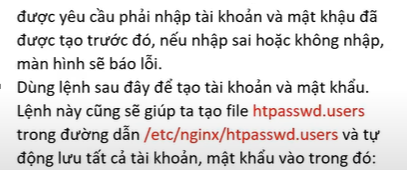
systemctl start kibana.service

để vào được kibana qua web browser cần có nginx



Kibana hđ trên port 5601





* Tạo tk, mk để truy nhập ELK server (thiết lập cho nginx để client access ELK cần phải TK, MK)

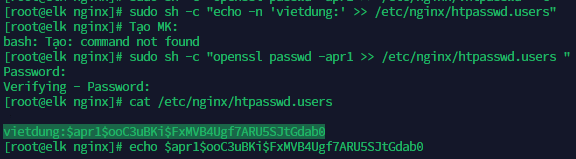
Tạo TK:

sudo sh -c "echo -n 'vietdung:' >> /etc/nginx/htpasswd.users"

Tạo MK:

sudo sh -c "openssl passwd -apr1 >> /etc/nginx/htpasswd.users "

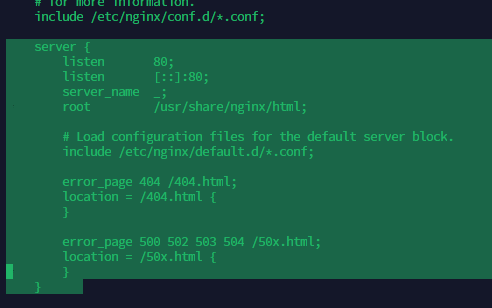
xác thực qua file **htpasswd.users** hoặc **.htpasswd**

****

Oke

* Xóa server block trong nginx

nano /etc/nginx/nginx.conf



Xóa hết đoạn bôi đen

* Tạo file config mới

nano /etc/nginx/conf.d/kibana.conf

server {

    listen 80;

    server\_name elk.co;

    auth\_basic "Restricted Access";

    auth\_basic\_user\_file /etc/nginx/htpasswd.users;

    location / {

        proxy\_pass http://localhost:5601;

        proxy\_http\_version 1.1;

        proxy\_set\_header Upgrade $http\_upgrade;

        proxy\_set\_header Connection 'upgrade';

        proxy\_set\_header Host $host;

        proxy\_cache\_bypass $http\_upgrade;

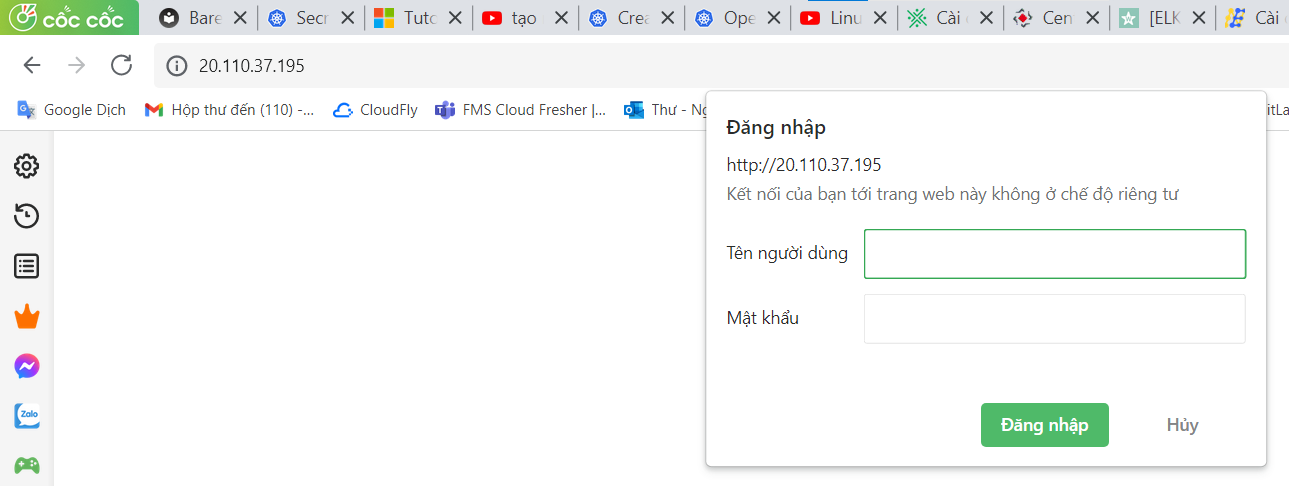
    }

}

File này sẽ giúp điều hướng vào kibana-ELK cần phải xác thực

systemctl restart nginx

bgio access, truy nhập



User/pass vừa tạo ở htpasswd/users

# Elasticsearch tiep