Cài đặt Graylog

Thành phần :

* Elasticsearch 1.7.3
* Mongo 2.6.11
* Graylog + Graylog Web-Interface 1.3

**Cài đặt JAVA home**

yum install java-1.8.0-openjdk.x86\_64 -y

**Thay biến JAVA\_HOME**

root@centos7:~# vi /etc/environment

JAVA\_HOME="/usr/lib/jvm/jre-1.8.0-openjdk"

**Chạy biến JAVA\_HOME**

root@centos7:~# source /etc/environment

**Dowload package Elasticsearch**

root@centos7:~# yum install wget -y

root@centos7:~# wget <https://download.elastic.co/elasticsearch/elasticsearch/elasticsearch-1.7.3.noarch.rpm>

root@centos7:~# rpm -ivh elasticsearch-1.7.3.noarch.rpm

**Dowload package MongoDB**

root@centos7:~# vi /etc/yum.repos.d/mongodb.repo

[mongodb]

name=MongoDB repo

baseurl=http://downloads-distro.mongodb.org/repo/redhat/os/x86\_64/

gpgcheck=0

enabled=1

root@centos7:~# yum install mongodb-org -y

root@centos7:~# service mongod enable

root@centos7:~# service mongod start

Bước 3 : Dowload package Graylog và các gói bổ trợ

root@centos7:~# rpm -Uvh <https://packages.graylog2.org/repo/packages/graylog-1.3-repository-el6_latest.rpm>

root@centos7:~# rpm -Uvh https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm

root@centos7:~# yum -y install git curl build-essential pwgen ssh ntp policycoreutils-python epel-release

Bước 4 : Cấu hình Elasticsearch

root@centos7:~# cp /etc/elasticsearch/elasticsearch.yml /etc/elasticsearch/elasticsearch.yml.bak

( backup file cấu hình )

root@centos7:~# vi /etc/elasticsearch/elasticsearch.yml (chỉnh dòng nào bỏ # dòng ấy )

Sửa các dòng sau :

Dòng 32, thêm : cluster.name: graylog

Dòng 107 : bỏ # và sửa: index.number\_of\_shards: 1

Dòng 111 : bỏ # và sửa : index.number\_of\_replicas: 0

Bỏ dấu # 321.

discovery.zen.ping.multicast.enabled: false

Dòng 326, bỏ # thêm : discovery.zen.ping.unicast.hosts: ["IP máy:9300"]

Bước 5 : Backup và sửa limit của elasticsearch

root@centos7:~# mv /etc/security/limits.conf /etc/security/limits.bak

root@centos7:~# grep -Ev "# End of file" /etc/security/limits.bak > /etc/security/limits.conf

root@centos7:~# echo "elasticsearch soft nofile 32000" >> /etc/security/limits.conf

root@centos7:~# echo "elasticsearch hard nofile 32000" >> /etc/security/limits.conf

root@centos7:~# echo "# End of file" >> /etc/security/limits.conf

root@centos7:~# service elasticsearch enable

root@centos7:~# service elasticsearch restart

Bước 7 : Cài đặt Graylog Server và Graylog Web Interface

root@centos7:~# yum -y install graylog-server graylog-web

root@centos7:~# cp /etc/graylog/server/server.conf /etc/graylog/server/server.conf.bak

root@centos7:~# echo -n 123456a@ | sha256sum ( thay password với mật khẩu của riêng bạn )

( Sẽ hiện ra 1 đoạn code, ví dụ ) : ab817a1a4f3d5a6412a863196fae08a97fecac180b6d9c6a2d5ce4dbe695c5ca ( code 1 )

root@centos7:~# pwgen -N 1 -s 96

( Sẽ hiện ra 1 đoạn code thứ 2 , ví dụ ) :

rdtS1rKxgXYqzzsj4qoSlVpu6CGa33t8bgZjjvZOJ1vT6c7w3zpZTGeHoRdTajUe6uGCGKGlv8jB72AXemWV5n5ce0jeBs1N ( code 2 )

Bước 8 : Chỉnh sửa cấu hình Graylog ( chỉnh dòng nào bỏ # dòng ấy )

root@centos7:~# vi /etc/graylog/server/server.conf

Dòng 11, thêm đoạn code 2 vào như sau :

password\_secret = rdtS1rKxgXYqzzsj4qoSlVpu6CGa33t8bgZjjvZOJ1vT6c7w3zpZTGeHoRdTajUe6uGCGKGlv8jB72AXemWV5n5ce0jeBs1N

Dòng 22, thêm đoạn code 1 vào như sau :

root\_password\_sha2 = ab817a1a4f3d5a6412a863196fae08a97fecac180b6d9c6a2d5ce4dbe695c5ca

Dòng 32, sửa :

root\_timezone = Asia/Ho\_Chi\_Minh

Dòng 38, sửa :

rest\_listen\_uri = <http://0.0.0.0:12900/>

Dòng 134, sửa :

retention\_strategy = close

Dòng 136, sửa :

elasticsearch\_shards = 1

Dòng 158, sửa:

elasticsearch\_cluster\_name = graylog

Dòng 173, bỏ dấu # : elasticsearch\_discovery\_zen\_ping\_multicast\_enabled = false

Dòng 174, bỏ dấu # và sửa :

elasticsearch\_discovery\_zen\_ping\_unicast\_hosts = 172.16.69.227:9300 ( thay 172.16.69.227 với IP của máy bạn )

root@centos7:~# systemctl enable graylog-server

root@centos7:~# systemctl start graylog-server

Bước 9 : Sửa file cấu hình cho Web Interface

root@centos7:~# cp /etc/graylog/web/web.conf /etc/graylog/web/web.conf.bak

root@centos7:~# pwgen -N 1 -s 96

( Sẽ hiện ra 1 đoạn code, ví dụ như sau)

smkAYFXXa6AZsoKr1qubPGypsDKUb7gk3I1FSU2UaeRMnHr7dCjxJxwWiPVsOvM9AAWLfbtKoyM7bc1QDJ9knTj76ARqNFu3 ( code 3 )

root@centos7:~# vi /etc/graylog/web/web.conf

Dòng 2, sửa :

graylog2-server.uris="<http://0.0.0.0:12900/>"

Dòng 12, sửa :

application.secret="smkAYFXXa6AZsoKr1qubPGypsDKUb7gk3I1FSU2UaeRMnHr7dCjxJxwWiPVsOvM9AAWLfbtKoyM7bc1QDJ9knTj76ARqNFu3"

Dòng 18, thêm :

timezone="Asia/Ho\_Chi\_Minh"

root@centos7:~# systemctl enable graylog-web

root@centos7:~# systemctl start graylog-web

Bước 10 : Firewalld + SElinux

firewall-cmd --permanent --zone=public --add-port=514/tcp

firewall-cmd --permanent --zone=public --add-port=514/udp

firewall-cmd --permanent --zone=public --add-port=12201/tcp

firewall-cmd --permanent --zone=public --add-port=12201/udp

firewall-cmd --permanent --zone=public --add-port=10514/tcp

firewall-cmd --permanent --zone=public --add-port=10514/udp

firewall-cmd --permanent --zone=public --add-port=9000/tcp

firewall-cmd --permanent --zone=public --add-port=12900/tcp

firewall-cmd --reload

Mở Rule SElinux

sudo setsebool -P httpd\_can\_network\_connect 1

sudo semanage port -a -t http\_port\_t -p tcp 9200

sudo semanage port -a -t mongod\_port\_t -p tcp 27017

Đăng nhập webinterface : IP:9000

admin/123456a@

