**Java (>= 8)**

**MongoDB 3.2**

**Elasticsearch 2.X**

**graylog 2.3.2**

**IP 192.168.0.210**

**centos 7.x**

**IP 192.168.0.210 (单机测试)**

**结构:mongodb + elasticsearch + graylog + nxlog + collector\_sidecar**

mongodb：存储元数据，一般安装好后不用其他设置

elasticsearch：存储日志

graylog：web界面，负责接收用户输入数据，展示elasticsearch里的数据

nxlog ，collector\_sidecar：日志收集，传送

jdk请自行安装，这里不再说明，可在下面地址下载相关版本：

<http://mirror.cnop.net/jdk/>

1.安装mongodb（这里以3.2为例）

vim  /etc/yum.repos.d/mongodb-org-3.2.repo    #添加yum源

[mongodb-org-3.2]

name=MongoDB Repository

baseurl=https://repo.mongodb.org/yum/redhat/$releasever/mongodb-org/3.2/x86\_64/

gpgcheck=1

enabled=1

gpgkey=<https://www.mongodb.org/static/pgp/server-3.2.asc>

yum -y install mongodb

添加系统服务及启动

                         chkconfig --add mongod

                         systemctl daemon-reload

                         /sbin/chkconfig  mongod on

                         systemctl start mongod.service

                    注意：这里没有进行mongodb的相关配置包括graylog连接

                    的配置，graylog启动时会自行创建相关数据

2.elasticsearch安装

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

vim /etc/yum.repos.d/elasticsearch.repo #加入以下

[elasticsearch-2.x]

name=Elasticsearch repository for 2.x packages

baseurl=https://packages.elastic.co/elasticsearch/2.x/centos

gpgcheck=1

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

enabled=1

yum install -y elasticsearch

 vim  /etc/elasticsearch/elasticsearch.yml #根据情况修改成自己的信息，切记去除注释后的内容前面不要有空格，不然可能会启动失败

 cluster.name: graylog   # elasticsearch集群名称，若有多个集群，可根据此属性区分。

 node.name: node-210 #集群节点名称，elasticsearch启动时会自动创建，也可手动配置

 network.host: 192.168.0.210    #设置绑定的ip地址

http.port: 9200        #设置对外服务的Http端口，默认是9200

 transport.tcp.port: 9300       #设置节点间交互的tcp端口,默认是9300  #个人测试没有这个选项

discovery.zen.ping.unicast.hosts: ["192.168.0.210"]     #设置集群中master集群初始化列表,这个数组里的机器将被自动发现加入集群，多个用逗号隔开

添加至系统服务及启动：

                         chkconfig --add elasticsearch

                         systemctl daemon-reload

                         systemctl enable elasticsearch.service

                         systemctl restart elasticsearch.service

3.graylog安装（web界面）

$ sudo rpm -Uvh https://packages.graylog2.org/repo/packages/graylog-2.3-repository\_latest.rpm #获取最新版本
$ sudo yum install -y graylog-server pwgen #安装最新版本,pwgen用于密码加密生成

配置

vi /etc/graylog/server/server.conf  **#配置graylog，修改以下几个地方，其他地方保持默认，也可根据实际情况进行设置**

**password\_secret =ZOauN2D9OknUXUDJbj4Lebb9zPB0SYfgcLELyo7r3yJK5r6Ep6CFfLco4hPy0tc3QEgYIDUP2RZcXdlCpZm43PvuIIyFuWPS**

**# 对密码进行加盐处理（就是密码加盐也就是密码后面加上很长的一串字符串再进行加密）,如 md5(md5(password)+salt)和SHA512(SHA512(password)+salt) 方式这里使用pwgen随机生成密码：pwgen -N 1 -s 96**

root\_username = admin #登陆web界面用户名，这里去除前面注释

root\_password\_sha2 =8d969eef6ecad3c29a3a629280e686cf0c3f5d5a86aff3ca12020c923adc6c92 #设置登陆web密码，使用 sha256sum进行加密，可使用 echo -n 123456 | sha256sum 命令在系统中生成，这里以123456为例说明。



root\_timezone = +08:00         #设置时区

[rest\_listen\_uri = http://192.168.0.210:9000/api/](interm) #地址更改成自己的ip，这里以192.168.0.210为例，用于接受Graylog Collector Sidecar发送的心跳信息，collectors也可以访问次uri

rest\_transport\_uri = http://192.168.0.210:9000/api/

[web\_listen\_uri = http://192.168.0.210:9000/](interm)        # graylog-web访问地址

elasticsearch\_hosts = http://192.168.0.210:9200 #elasticsearch地址，用于接入elasticsearch引擎

allow\_highlighting = true （运行查询结果高亮）
elasticsearch\_shards = 1 （当前只安装了一个elasticsearch）

elasticsearch\_cluster\_name = graylog     #必须与elasticsearch设置相同

mongodb\_uri = mongodb://localhost/graylog              # MongoDB服务器身份验证，使用默认即可，这里不需要像mysql一样导入表，只存储原数据

$ sudo systemctl start graylog-server

$ sudo systemctl enable graylog-server

添加防火墙：

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

systemctl restart firewalld.service

4.Collector端与nxlog的部署

nxlog：

yum -y install libdbi #要求为 libdbi >= 0.8.1

wget <http://mirror.cnop.net/nxlog/linux/nxlog-ce-2.9.1716-1_rhel7.x86_64.rpm>

rpm -ivh nxlog-ce-2.9.1716-1\_rhel7.x86\_64.rpm

gpasswd -a nxlog root

chown -R nxlog.nxlog /var/spool/collector-sidecar/nxlog

vim /etc/nxlog.conf #注意，本处定义log文件nxlog必须有读权限，不然后面可能查询不到日志信息

########################################

# Modules #

########################################

<Extension gelf>

 Module xm\_gelf

</Extension>

<Input in>

 Module im\_file

 File "/var/log/messages"

</Input>

<Output out>

 Module om\_udp

 Host 192.168.0.210

 Port 12201

 OutputType GELF

</Output>

########################################

# Routes #

########################################

<Route r>

 Path in => out

</Route>

systemctl restart nxlog

Collector：

|  |  |
| --- | --- |
| 0.1.x | 2.2.x,2.3.x |

Graylog Collector Sidecar是一种用于采集日志的轻量级配置管理系统，也称为后端，作为守护进程运行。

wget <http://mirror.cnop.net/Graylog/collector-sidecar/collector-sidecar-0.1.4-1.x86_64.rpm>

或去官方下载最新：

<https://github.com/Graylog2/collector-sidecar/releases>

$ sudo rpm -ivh collector-sidecar-0.1.4-1.x86\_64.rpm

$ sudo graylog-collector-sidecar -service install
$ sudo systemctl start collector-sidecar

vim /etc/graylog/collector-sidecar/collector\_sidecar.yml   #根据情况修改

server\_url: http://192.168.0.210:9000/api/

update\_interval: 10

tls\_skip\_verify: false

send\_status: true

list\_log\_files:

node\_id: graylog-collector-sidecar #多台机器请修改成不同id

collector\_id: file:/etc/graylog/collector-sidecar/collector-id

cache\_path: /var/cache/graylog/collector-sidecar

log\_path: /var/log/graylog/collector-sidecar

log\_rotation\_time: 86400

log\_max\_age: 604800

tags:

 - nginx

backends:

 - name: nxlog

 enabled: true

 binary\_path: /usr/bin/nxlog

 configuration\_path: /etc/graylog/collector-sidecar/generated/nxlog.conf

systemctl restart collector-sidecar

systemctl enable collector-sidecar

systemctl restart nxlog

/sbin/chkconfig nxlog on

参考：<http://docs.graylog.org/en/2.3/pages/collector_sidecar.html>

5.web访问：

 <http://192.168.0.210:9000>



点击[System](http://192.168.0.210:9000/gettingstarted)->Collectors



点击 Create configuration



这里任意输入一个名称，这里以test为例



点击名称"test"，进入配置界面：



设置output和input相关信息，与nxlog的配置文件相同：



点击右侧 Create Output ，选择相关**Type和名字，ip,端口等信息，**



点击右侧 Create Input：

**Type** [NXLog] file input

**Path to Logfile**  /var/log/messages



重启客户端的collector-sidecar：

systemctl restart collector-sidecar

设置web接收日志:

system->inputs->Launch new input



选择主机节点

设置标题

设置ip

设置端口（默认）



graylog web查看Collectors 是否运行正常：

 <http://192.168.0.210:9000/system/collectors>



可手动 echo 推送一条数据到被监控的日志文件中，最后回到主界面查看日志:



其他常见：

nxlog日志查看:

tail -f /var/log/graylog/collector-sidecar/nxlog.log

错误::



原因，请确定 elasticsearch 是否起来。

参考：

<http://docs.graylog.org/en/2.3/>

<http://cocojoey.lofter.com/post/1eff2f40_10a6d448>

<https://www.cnblogs.com/wsl222000/p/6041835.html>