Graylog

1. Prés-requis

Installation des paquets nécessaires:

```
# apt install apt-transport-https openjdk-11-jre-headless uuid-runtime
pwgen dirmngr gnupg wget libjersey1-server-java libjersey1-core-java -y
```

2. MongoDB

Téléchargement de MongoDB:

```
wget -qO - https://www.mongodb.org/static/pgp/server-4.2.asc | apt-key
add -
echo "deb http://repo.mongodb.org/apt/debian buster/mongodb-org/4.2
main" | tee /etc/apt/sources.list.d/mongodb-org-4.2.list
sudo apt-get update
sudo apt-get install -y mongodb-org
```

Activation de MongoDB au démarrage:

```
systemctl daemon-reload
systemctl enable mongod.service
systemctl restart mongod.service
systemctl --type=service --state=active | grep mongod
```

3. ElasticSearch

Téléchargement d'ElasticSearch :

```
wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo
apt-key add -
echo "deb https://artifacts.elastic.co/packages/oss-7.x/apt stable main"
| sudo tee -a /etc/apt/sources.list.d/elastic-7.x.list
apt update && sudo apt install elasticsearch-oss
```

Modification de la configuration :

```
tee -a /etc/elasticsearch/elasticsearch.yml > /dev/null << EOT
cluster.name: graylog
action.auto_create_index: false
EOT
```

Activation d'ElasticSearch :

```
systemctl daemon-reload
systemctl enable elasticsearch.service
systemctl restart elasticsearch.service
```

4. Graylog

Téléchargement de Graylog :

```
wget
https://packages.graylog2.org/repo/packages/graylog-4.2-repository_latest.deb
dpkg -i graylog-4.2-repository_latest.deb
apt update && apt install graylog-server
```

Configuration de root_password_sha2 :

```
echo -n "Enter Password: " && head -1 </dev/stdin | tr -d '\n' |
sha256sum | cut -d" " -f1
```

Activation du service Graylog :

```
systemctl daemon-reload
systemctl enable graylog-server.service
systemctl start graylog-server.service
systemctl --type=service --state=active | grep graylog
```

Activation de l'interface web :
/etc/graylog/server/server.conf

```
is_master = true
password_secret = <MotDePasse16Caractères>
root_username = <IdentifiantAdmin>
root_password_sha2 = <MotDePasseSHA2>
http_bind_address = <IPServeur>:9000
http_enable_cors = true
http_enable_gzip = true
http_max_header_size = 8192
http_thread_pool_size = 16
```

Redémarrage de graylog :

```
systemctl restart graylog-server.service
```

Accès à l'interface web de gestion : http://<IPServeur>:9000/