Все действия идут под рутом.

Для запуска нужны MongoDB, Opensearch и сам Graylog 5.2

1. Устанавливаем MongoDB
Сначала устанавливаем дополнительные пакеты

```
apt update; apt install gnupg software-properties-common apt-transport-https ca-certificates build-essential libjpeg-dev libpng-dev libtiff-dev curl wget pwgen
```

Ставим ключ

```
curl -fsSL https://pgp.mongodb.com/server-7.0.asc | gpg --dearmor -o /etc/apt/trusted.gpg.d/mongodb-server-7.0.gpg
```

Прописываем репозиторий

```
echo "deb [ arch=amd64,arm64 ] https://repo.mongodb.org/apt/ubuntu jammy/mongodb-org/7.0 multiverse" | tee /etc/apt/sources.list.d/mongodb-org-7.0.list
```

Ставим mongodb

```
apt update; apt install mongodb-org
```

Закидываем в автозапуск и запускаем mongod

```
systemctl enable mongod
systemctl start mongod; systemctl status mongod
```

Если это всё происходит на виртуальной машине Proxmox и не запускается MongoDB, то здесь описывал проблемы и возможное решение.

2. Устанавливаем Opensearch
Opensearch форк Elastacsearch, потому что были изменения в лицензиях Elastacsearch и некоторым разрабочикам это не понравилось.
Ставим ключ

```
curl -fsSL https://artifacts.opensearch.org/publickeys/opensearch.pgp |
gpg --dearmor -o /etc/apt/trusted.gpg.d/opensearch.gpg
```

Прописываем репозиторий

```
echo "deb
https://artifacts.opensearch.org/releases/bundle/opensearch/2.x/apt stable
main" | tee /etc/apt/sources.list.d/opensearch-2.x.list
```

Обновляемся и прописываем пароль для установки (лучше сохранить его или в окружении добавить):

```
apt update
export OPENSEARCH_INITIAL_ADMIN_PASSWORD=345Kjasdk3
```

Ставим Opensearch

```
apt install opensearch
```

Далее надо поправить конфиг под Graylog

```
nano /etc/opensearch/opensearch.yml
cluster.name: graylog52
node.name: ${HOSTNAME}
path.data: /var/lib/opensearch
path.logs: /var/log/opensearch
discovery.type: single-node
network.host: 0.0.0.0
#или 127.0.0.1
action.auto_create_index: false
plugins.security.disabled: true
```

И ещё конфиг

```
nano /etc/opensearch/jvm.options
-Xms4g
-Xmx4g
```

Закидываем в автозапуск и запускаем opensearch

```
sysctl -w vm.max_map_count=262144
echo 'vm.max_map_count=262144' &amp;gt;&amp;gt; /etc/sysctl.conf
Закидываем в автозапуск и запускаем  opensearch
systemctl daemon-reload
systemctl enable opensearch.service
systemctl start opensearch.service; systemctl status opensearch.service
```

Проверяем работу

```
curl -X GET http://localhost:9200 -u ‘admin:admin’
```

Должна вернуться информация о версии, названии и т.п.
3. Устанавливаем Graylog
Качаем

```
wget
https://packages.graylog2.org/repo/packages/graylog-5.2-repository_latest.
deb
```

И устанавливаем

```
dpkg -i graylog-5.2-repository_latest.deb
apt update; apt install graylog-server
```

Далее надо сделать password_secret и root_password_sha2[/code]

Для password_secret

```
pwgen -N 1 -s 96
```

Для root_password_sha2

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

И теперь настраиваем конфиг Graylog’а

```
nano /etc/graylog/server/server.conf
is_leader = true
node_id_file = /etc/graylog/server/node-id
password_secret = PASSWORD_PWGEN
root_password_sha2 =  PASSWORD_ROOT_SHA2
bin_dir = /usr/share/graylog-server/bin
data_dir = /var/lib/graylog-server
plugin_dir = /usr/share/graylog-server/plugin
http_bind_address = IP_ADDRESS:9000
stream_aware_field_types=false
elasticsearch_hosts = http://127.0.0.1:9200
disabled_retention_strategies = none
allow_leading_wildcard_searches = false
allow_highlighting = false
output_batch_size = 500
output_flush_interval = 1
output_fault_count_threshold = 5
output_fault_penalty_seconds = 30
processbuffer_processors = 5
outputbuffer_processors = 3
processor_wait_strategy = blocking
ring_size = 65536
inputbuffer_ring_size = 65536
inputbuffer_processors = 2
inputbuffer_wait_strategy = blocking
message_journal_enabled = true
message_journal_dir = /var/lib/graylog-server/journal
lb_recognition_period_seconds = 3
mongodb_uri = mongodb://localhost/graylog
mongodb_max_connections = 1000
```

Закидываем в автозапуск и запускаем graylog

```
systemctl daemon-reload
systemctl enable graylog-server.service
systemctl start graylog-server.service; systemctl status graylog-
server.service
```