Делаем свой сервер сбора логов на основе Grafana Loki

Для Grafana loki буду использовать ОС CentOS 8.5.2111

Если в системе у вас отсутствует пакет позволяющий скачивать файлы, то выполните команду

```
yum install git wget
```

Для компиляции исходника необходимо установить Golang

Можно перейти на их сайт и скопировать ссылку на актуальную версию Затем выполнить команду

```
wget https://go.dev/dl/go1.19.3.linux-amd64.tar.gz
```

Нужно распаковать архив

```
tar -v -C /usr/local -xzf go*.tar.gz
```

Далее редактируем файл

```
nano /etc/profile
```

добавив внизу строку

```
export PATH=$PATH:/usr/local/go/bin
```

Выполняем команду

```
export PATH=$PATH:/usr/local/go/bin
```

Проверяем, что go установлен

```
go version
```

Настраиваем Firewall

Открываем нужный нам порт для запуска loki

```
firewall-cmd --permanent --add-port=3100/tcp
```

```
firewall-cmd --reload
```

Отключаем SELinux т.к. он в нашем случае не понадобится

```
setenforce 0
```

```
sed -i 's/^SELINUX=.*/SELINUX=disabled/g' /etc/selinux/config
```

Начинаем процесс установки loki

Переходим в каталог

```
cd /usr/src/
```

Загружаем исходники

```
git clone https://github.com/grafana/loki
```

Переходим в скачанный каталог

```
cd loki
```

Запускаем компиляцию

```
go build ./cmd/loki
```

Появится файл loki — перенесем его в другой каталог

```
mv loki /usr/local/bin/
```

Далее нужно создать каталог

```
mkdir /etc/loki
```

и закинуть туда конфиг

```
mv cmd/loki/loki-local-config.yaml /etc/loki/
```

Нужно подкорректировать /tmp — Делаем командами

```
sed -i 's/\/tmp\/wal/\/opt\/loki\/wal/g' /etc/loki/loki-local-config.yaml
```

```
sed -i 's/\/tmp\/loki/\/opt\/loki/g' /etc/loki/loki-local-config.yaml
```

Создаем каталог

```
mkdir /opt/loki
```

Тестируем запуск

```
/usr/local/bin/loki -config.file=/etc/loki/loki-local-config.yaml
```

В браузере переходим по адресу

```
http://ВашIP:3100/metrics
```

где ВашIP — IP-адрес сервера grafana loki

Если видим нечто подобное, то все супер

Делаем автозапуск нашего сервиса

Создаем специально для этих целей пользователя и даем нужные права на запуск

```
useradd --no-create-home --shell /bin/false loki
```

```
chown loki:loki /usr/local/bin/loki
```

```
chown -R loki:loki /etc/loki
```

```
chown -R loki:loki /opt/loki
```

Добавляем отдельный юнит для автозапуска

```
nano /etc/systemd/system/loki.service
```

Содержимое файла должно быть таким

```
[Unit]
Description=Grafana Loki Service
After=network.target

[Service]
User=loki
Group=loki
Type=simple
ExecStart=/usr/local/bin/loki -config.file=/etc/loki/loki-local-config.yaml
ExecReload=/bin/kill -HUP $MAINPID
Restart=on-failure

[Install]
WantedBy=multi-user.target
```

Перезапускаем конфигурацию

```
systemctl daemon-reload
```

Разрешаем автозапуск

```
systemctl enable loki --now
```

Проверяем статус

```
systemctl status loki
```

Если видим подобное, то радуемся и движемся дальше

Закончили настройку серверной части.

Переходим к настройке визуальной части и сбору самих логов

устанавливаем недостающие компоненты

```
yum install unzip wget
```

Устанавливаем и настраиваем promtail, он позволяет читать и отправлять логи на сервер.

Скачиваем архив с программой

```
wget
https://github.com/grafana/loki/releases/latest/download/promtail-linux-amd6
4.zip
```

Распаковываем и переносим в другой каталог

```
unzip promtail-linux-amd64.zip
```

```
mv promtail-linux-amd64 /usr/local/bin/promtail
```

Нужно создать каталог для конфигов

```
mkdir /etc/promtail
```

Теперь создаем сам конфиг и наполняем его

```
nano /etc/promtail/promtail.yaml
```

Должно быть в файле

```
server:
  http_listen_port: 9080
  grpc_listen_port: 0

positions:
  filename: /tmp/positions.yaml

clients:
  - url: http://ВашIP:3100/loki/api/v1/push
```

где ВашIP - адрес вашего сервера loki

Теперь создаем юнит для автозапуска

```
nano /etc/systemd/system/promtail.service
```

Содержимое файла должно быть

```
[Unit]
Description=Promtail Service
After=network.target

[Service]
Type=simple
ExecStart=/usr/local/bin/promtail -config.file=/etc/promtail/promtail.yaml
ExecReload=/bin/kill -HUP $MAINPID
Restart=on-failure

[Install]
WantedBy=multi-user.target
```

Перезапускаем конфигурацию

```
systemctl daemon-reload
```

Включаем автозагрузку

```
systemctl enable promtail --now
```

Смотрим статус

```
systemctl status promtail
```

Если видим такое, двигаемся дальше

Открываем нужный нам порт для запуска promtail

```
firewall-cmd --permanent --add-port=9080/tcp
```

```
firewall-cmd --reload
```

Проверяем в браузере работу promtail

```
http://ВашIP:9080/targets
```

Видим нечто подобное? Все супер

> Важное упоминание, promtail нужно установить на все линуксовые машины с которых вы планируете собирать логи

Для сбора логов нужно внести в конфиг информацию о том что и как собираем

открываем конфиг

```
nano /etc/promtail/promtail.yaml
```

и добавляем туда строки. Показываю пример на сборе логов с сервера loki

```
# Чтение логов с сервера  Loki
# Имя задания чтения лога
- job_name: loki_srv
  static_configs:
# ПК с которого читается лог
  - targets:
      - localhost
    labels:
# Метка для имени задания
      job: loki_srv
# Путь к файлу с логами
```

```
      __path__: /var/log/rsyslog/Loki/*log
```

В данный конфигурационный файл добавляем все серверы и сетевое оборудование откуда вы планируете собирать логи по принципе как я написал выше

После каждого изменения файла делаем его перезагрузку

```
systemctl restart promtail
```

Затем проверяем в браузере отображение

```
http://ВашIP:9080/targets
```

Если видим подбное, то вы справились с задачей

Переходим к этапу установки самой Grafana

Нужно создать репозиторий откуда и будет производится установка

```
nano /etc/yum.repos.d/grafana.repo
```

содержимое файла

```
[grafana]
name=grafana
baseurl=https://packages.grafana.com/oss/rpm
repo_gpgcheck=1
enabled=1
gpgcheck=1
gpgkey=https://packages.grafana.com/gpg.key
sslverify=1
sslcacert=/etc/pki/tls/certs/ca-bundle.crt
```

Устанавливаем

```
yum install grafana
```

Открываем нужный нам порт для запуска grafana

```
firewall-cmd --permanent --add-port=3000/tcp
```

```
firewall-cmd --reload
```

Включаем автозагрузку

```
systemctl enable grafana-server
```

Стартуем сервер

```
systemctl start grafana-server
```

Т.к сейчас проблема с доступом на сайт grafana Обойти проблему можно через VPN и скачать rpm пакет напрямую и установить его

```
wget
https://dl.grafana.com/enterprise/release/grafana-enterprise-9.3.0-1.x86_64.
rpm
```

```
yum install /home/grafana-9.3.0-1.x86_64.rpm
```

Где /home/ путь куда вы скачали файл

Переходим к финальной стадии, настройка веб интерфейса

Переходим в браузере по ссылке

```
http://ВашIP:3000/
```

ВашIP - сервер где установлена grafana

Вводим логин и пароль admin, система потребует сменить пароль, если не потребует, изменить его можно в настройках внутри веб интерфейса

Переходим по пути

Добавляем источник

Находим там loki

Вводим адрес сервера

и сохраняем

Если получили сообщение

То все супер и теперь вы можете видеть логи