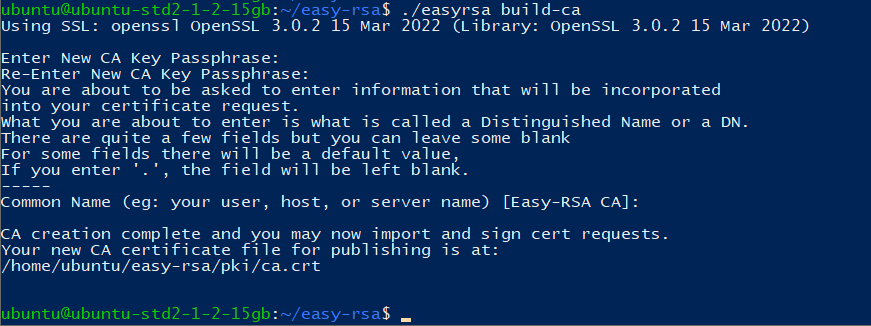
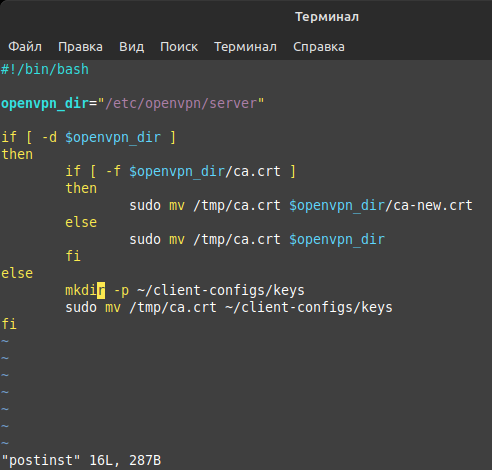
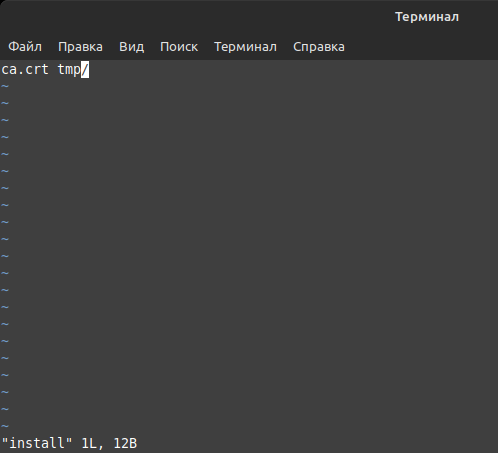
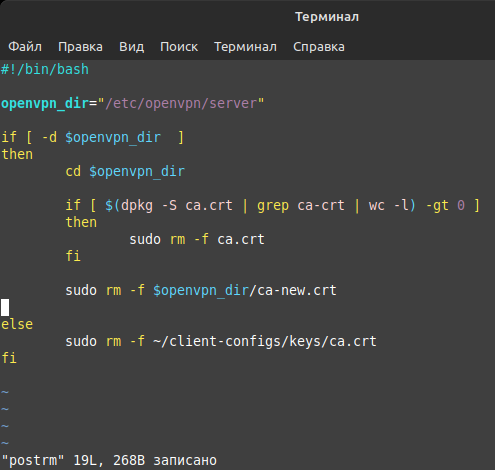
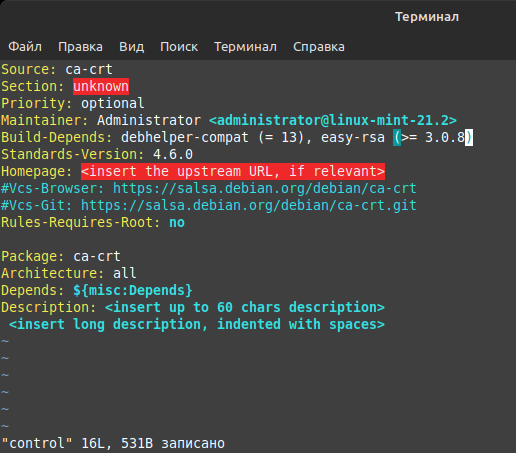
1. **Развёртывание удостоверяющего центра для выдачи сертификатов (Public Key Infrastructure)**

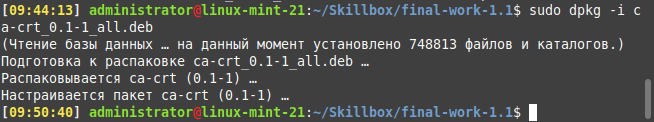


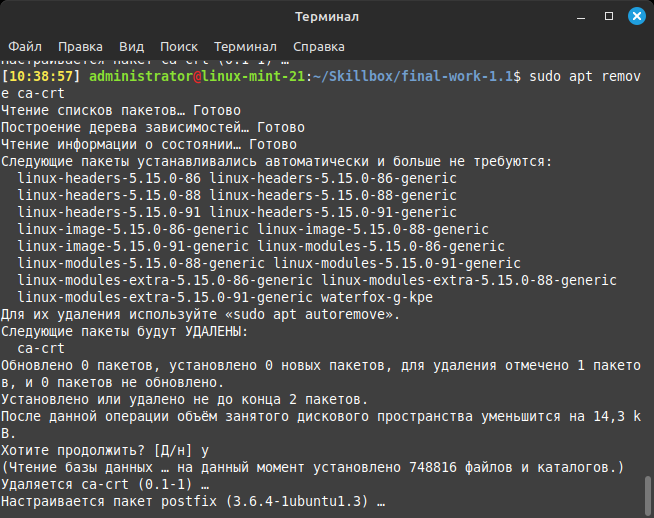












ca-crt\_0.1-1\_all.deb: <https://disk.yandex.ru/d/KupDGFG6Lkd1HA>

easy-rsa.sh: <https://disk.yandex.ru/d/i2gbK-GOEM2Edw>

1. **Создание и настройка VPN-сервера**

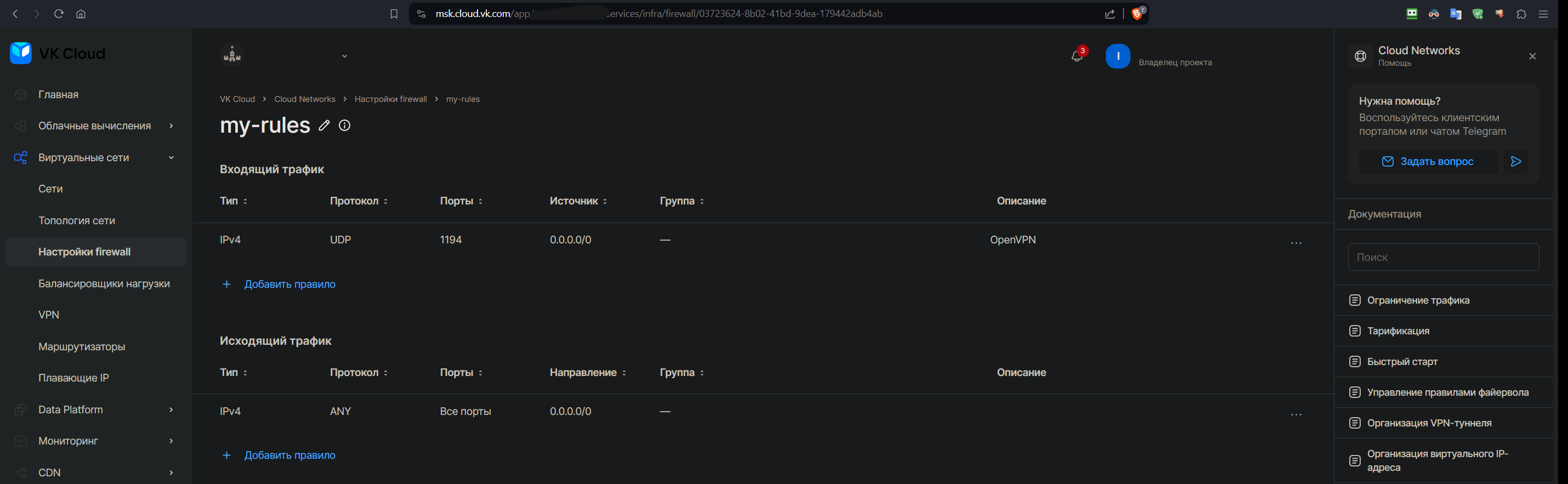
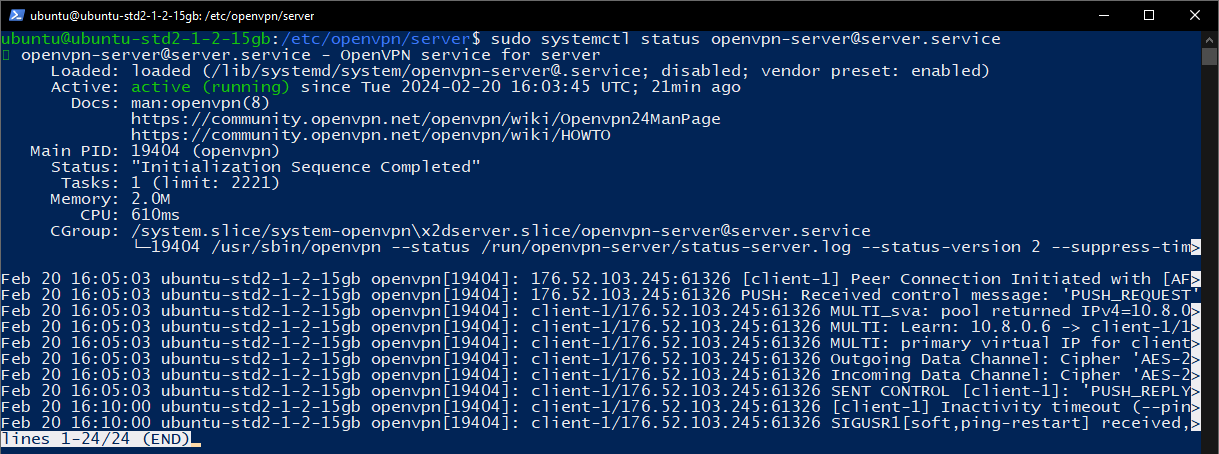
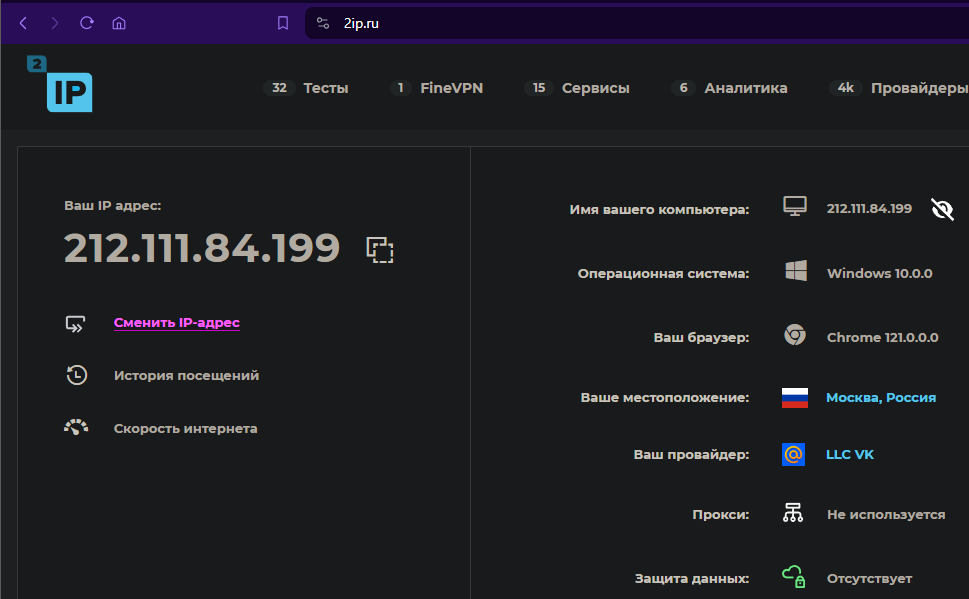
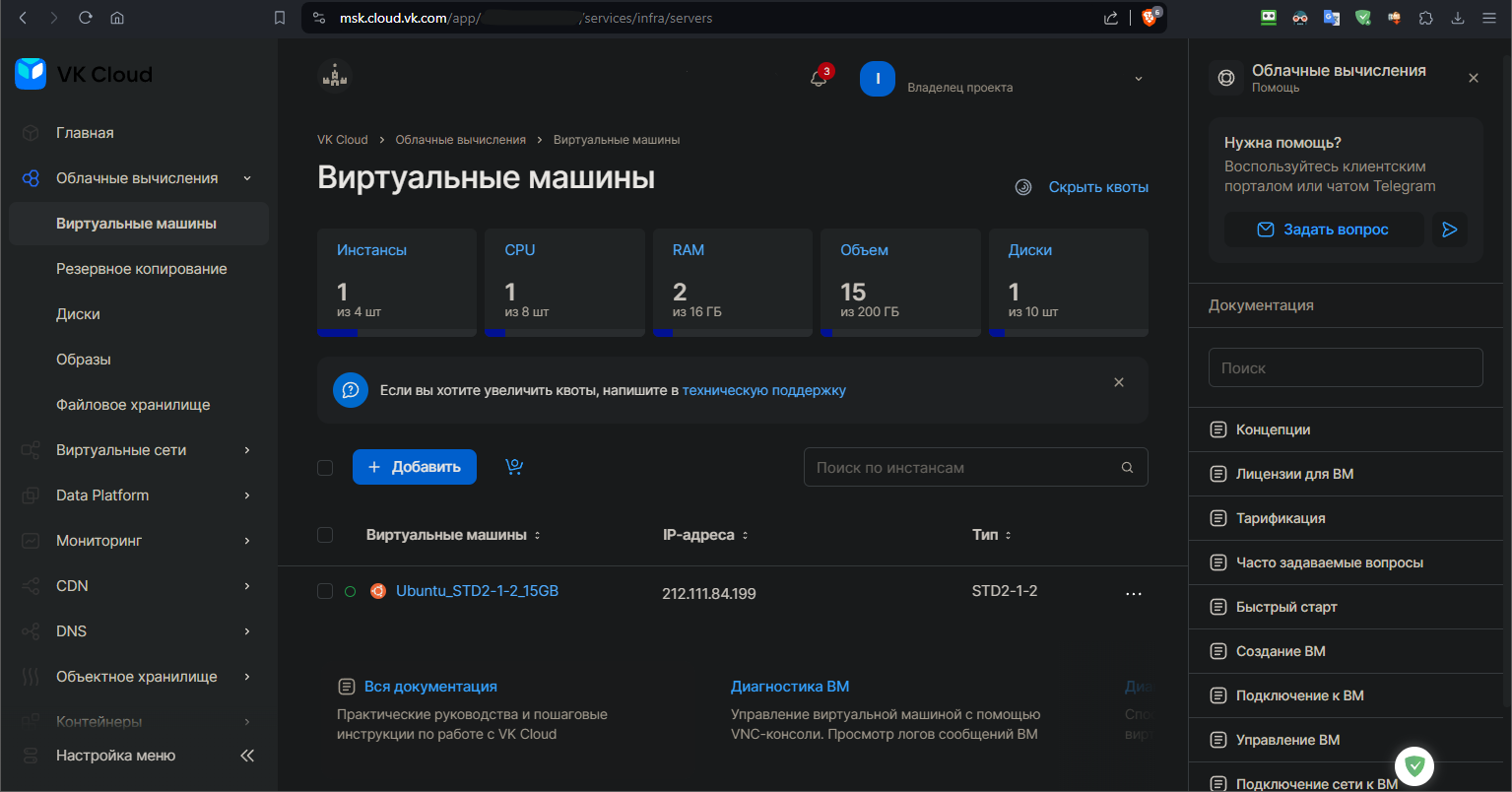


Рис. Добавление правил в файрволле









Создание сертификата OpenVPN: <https://disk.yandex.ru/d/fa7STtlM_OzJaw>

Отзыв сертификата OpenVPN: <https://disk.yandex.ru/d/DCnbv-EEHIzOUA>

Добавление правил iptables: <https://disk.yandex.ru/d/y4bxRg5I39uxRA>

**Некоторые примечания:**

1. Лучше до создания конечного файла .ovpn выполнять все действия вручную, потому что могут возникать ошибки в процессе установки и конфигурации. Если ты опытный системный администратор Linux, то данное правило не действует.
2. Все приватные ключи (центра сертификации и сервера OpenVPN) лучше хранить на отдельной usb-флешке или в криптоконтейнере
3. Были созданы несколько скриптов (находятся выше) для автоматизации некоторых действий, но есть уже готовые решения ( <https://github.com/angristan/openvpn-install/blob/master/openvpn-install.sh> , <https://www.cyberciti.biz/faq/ubuntu-22-04-lts-set-up-openvpn-server-in-5-minutes/> ). Чтобы писать скрипты на таком же уровне, я думаю, что нужно постоянно писать на Bash минимум от полугода.
4. Чтобы импортировать ключевой файл .ovpn в OpenVPN для Linux- и Windows-систем, по-моему мнению, не требуется особых знаний и навыков, поэтому писать скрипты или создавать пакеты не имеет смысла.
5. **Настройка мониторинга**

**Устанавливаем Prometheus**

1. Переходим <https://github.com/prometheus/prometheus/releases/> и скачиваем последнюю версию Prometheus.
2. Скачиваем архив, распаковываем его, заходим в папку. Далее переходим по ссылке <https://disk.yandex.ru/d/uZW9wGDvfblthg> , скачиваем в папку с prometheus и запускаем скрипт.
3. Перезагружаем файлы конфигурации системы: «sudo systemctl daemon-reload»
4. Включаем и запускаем службу Prometheus «sudo systemctl enable prometheus», « sudo systemctl start prometheus»
5. Проверяем статус Prometheus «sudo systemctl status prometheus»

**Устанавливаем Node Exporter**

1. Переходим <https://github.com/prometheus/node_exporter/releases/> и скачиваем последнюю версию Node Exporter.
2. Разархивируем скачанный архив и перейдем в появившуюся папку. Скопируем «sudo cp node\_exporter /usr/local/bin/»
3. Выполняем следующую команду в терминале для добавления новой службы:

sudo cat << EOF > /etc/systemd/system/node\_exporter.service

[Unit]

Description=Node Exporter

After=network.target

[Service]

User=prometheus

Group= prometheus

Type=simple

ExecStart=/usr/local/bin/node\_exporter --collector.filesystem.ignored-mount-points=^/(sys|proc|dev|run)($|/)

[Install]

WantedBy=multi-user.target

EOF

1. Перезагружаем systemctl и запускаем Node Exporter:

«sudo systemctl daemon-reload» , «sudo systemctl start node\_exporter»

1. Проверяем статус службы Node Exporter и добавляем в автозагрузку:

«systemctl status node\_exporter», « sudo systemctl enable node\_exporter»

1. Открываем файл «/etc/prometheus/prometheus.yml», находим строку «scrape\_configs:» и добавляем:

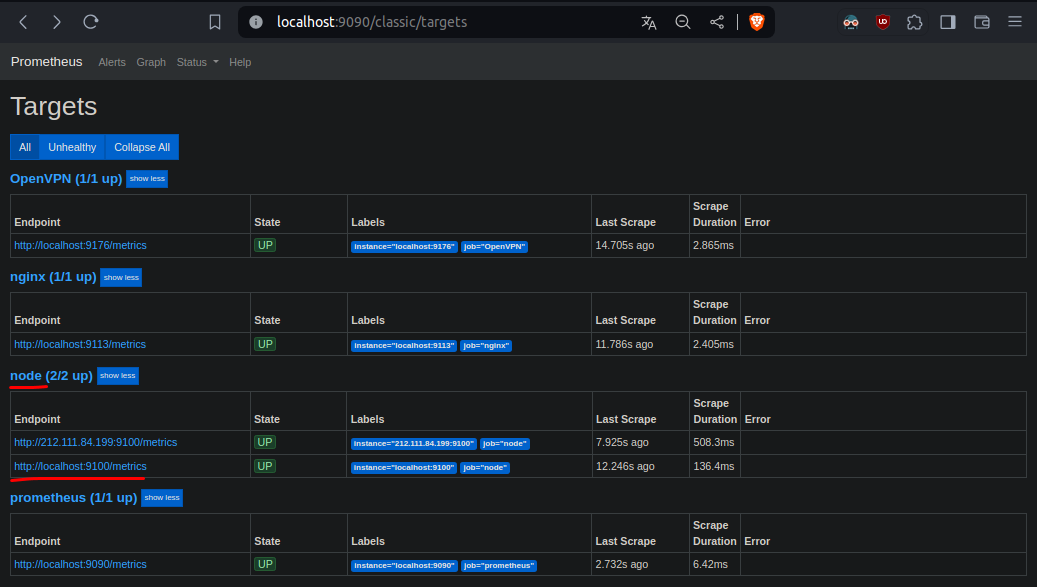
- job\_name: 'node\_exporter'

scrape\_interval: 5s

static\_configs:

- targets: ['enter\_your\_ip:9100']

7. Перезагружаем сервис Prometheus и переходим в web-интерфейс Prometheus, вкладка Status=>Targets (обычно <http://localhost:9090/classic/targets>), чтобы убедиться, что Node Exporter добавлен.



**Устанавливаем OpenVPN Exporter**

1. Скачиваем и разархивируем последнюю версию по ссылке: <https://github.com/rossigee/openvpnas-exporter/releases/>
2. Переходим в разархивированную папку и выполняем следующую команду:

«sudo cp openvpnas-exporter /usr/local/bin/»

1. Выполняем следующую команду в терминале для добавления новой службы:

sudo cat << EOF > /etc/systemd/system/openvpnas\_exporter.service

[Unit]

Description=OpenVPN AS

Requires=prometheus.service

[Service]

User=root

Group=root

Type=simple

ExecStart=/usr/local/bin/openvpnas\_exporter

[Install]

WantedBy=multi-user.target

EOF

1. Перезагружаем systemctl и запускаем OpenVPN Exporter:

«sudo systemctl daemon-reload» , «sudo systemctl start openvpnas\_exporter»

1. Проверяем статус службы Node Exporter и добавляем в автозагрузку:

«systemctl status openvpnas\_exporter», « sudo systemctl enable openvpnas\_exporter»

6. Открываем файл «/etc/prometheus/prometheus.yml», находим строку «scrape\_configs:» и добавляем:

- job\_name: 'OpenVPN\_exporter

scrape\_interval: 5s

static\_configs:

- targets: ['enter\_your\_ip:9176']

7. Перезагружаем сервис Prometheus и переходим в web-интерфейс Prometheus, вкладка Status=>Targets (обычно http://localhost:9090/classic/targets), чтобы убедиться, что OpenVPN Exporter добавлен.

**Устанавливаем Alertmanager**

1. Переходим <https://github.com/prometheus/alertmanager/releases> и скачиваем последнюю версию Alertmanager.
2. Скачиваем архив, распаковываем его, заходим в папку. Далее переходим по ссылке <https://disk.yandex.ru/d/9-RY4RPcsfB3vA>, скачиваем в папку с alertmanager и запускаем скрипт.
3. Заходим в конфигурационный файл /etc/prometheus/prometheus.yml и заменяем «alertmanager:9093» на «localhost:9093». Выглядеть это должно примерно так:

«alerting:

alertmanagers:

- static\_configs:

- targets:

- localhost:9093»

4. Перезагружаем Prometheus командой «sudo systemctl restart prometheus»

5. Заходим в браузер и переходим по ссылке «localhost:9093», чтобы убедиться, что Alertmanager работает или заходим в Prometheus и выполняем следующий запрос «prometheus\_notifications\_alertmanagers\_discovered»

6. Скачиваем и запускаем скрипт <https://disk.yandex.ru/d/TIpeeKqCciE2nQ>

7. Открываем «/etc/prometheus/prometheus.yml» и добавляем строку «- “alertmanager-rules.yml”» в секцию «rule\_files:»

8. Скачиваем и запускаем скрипт <https://disk.yandex.ru/d/YYNuz5ny9NiZpA>

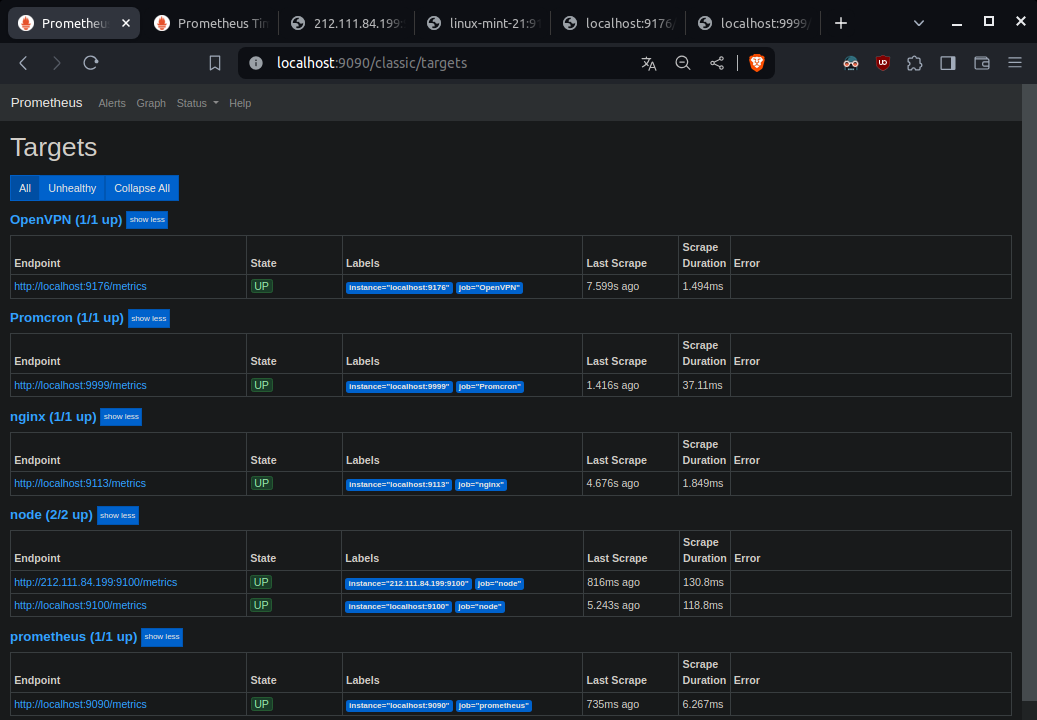
9. Перезапускаем Prometheus и Alertmanager и смотрим их статус: «sudo systemctl restart prometheus», «sudo systemctl restart prometheus-alertmanager», «systemctl status prometheus», «systemctl status prometheus-alertmanager»

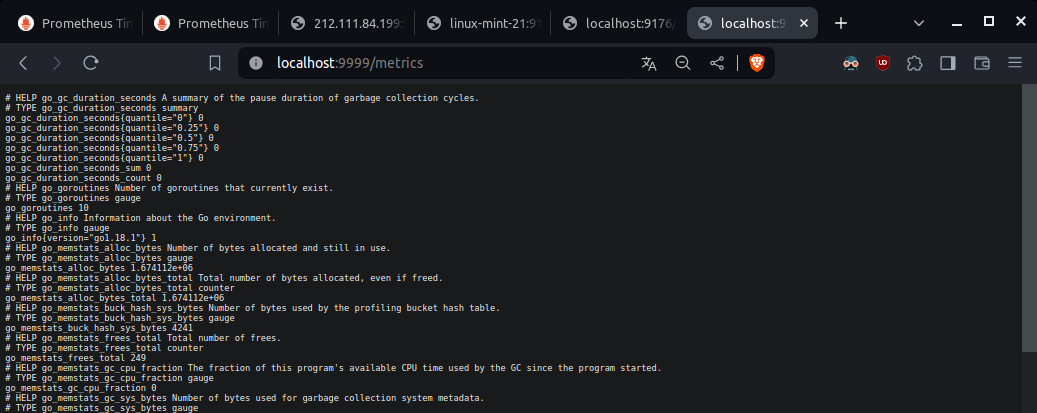
10. Заходим в Prometheus через браузер (обычно это <http://localhost:9090/>) и переходим в «Status => Rules», чтобы увидеть правила Alertmanager

11. Устанавливаем утилиту «iptables-persistent» командой «sudo apt-get install iptables-persistent», если ее нет, для сохранения правил iptables после перезагрузки

12. Скачиваем, открываем и вносим нужные данные в скрипт и далее выполняем: <https://disk.yandex.ru/d/2u2g9uDLjdNP8A>

1. **Создание системы резервного копирования**
2. При выборе из всех способов резервного копирования системы, мой выбор пал на создание squashfs образа, тк данный способ актуален на сегодняшний день. Более подробно можно посмотреть [тут](https://mydebianblog.blogspot.com/2006/08/squashfs.html).
3. Если есть желание, то лучше в отдельную папку скопировать рабочие скрипты и установочные пакеты
4. Для полноценного резервного копирования нужно минимум 2 облачных хранилища с объемом от 25 ГБ. Выбираем файловое хранилище из [статьи](https://journal.tinkoff.ru/list/best-cloud-services/). Из всего вышеперечисленного подходит только Terabox. А для полной автоматизации Terabox нужно устанавливать дополнительное ПО (к примеру: [ссылка](https://github.com/tewbo/terabox_flex)), потому что официальное приложение не дает установить папку для автоматической синхронизации или выбирать файл вручную в официальном приложении. Поэтому лучше всего докупить дополнительный объем памяти на популярных ресурсах, к примеру: Dropbox, Box.com.
5. Устанавливаем Promcron для резервного копирования по [ссылке](https://disk.yandex.ru/d/CGyI8jFQXxe-6w). Для более подробной документации нужно перейти [сюда](https://github.com/andrewchambers/promcron).
6. Далее [скачиваем](https://disk.yandex.ru/d/ykfnvB7bNK736w) и запускаем скрипт для настройки Promcron и Prometheus.
7. Проверяем новую службу Promcron при помощи команды «sudo systemctl status promcron», что все запустилось без ошибок. Тоже самое проделываем с Prometheus.
8. Проверяем новое добавленное правило в конфигурацию Prometheus и убеждаемся, что Promcron работает.





1. Прописанное правило ниже для Alertmanager вполне устраивает для мониторинга службы Promcron.

