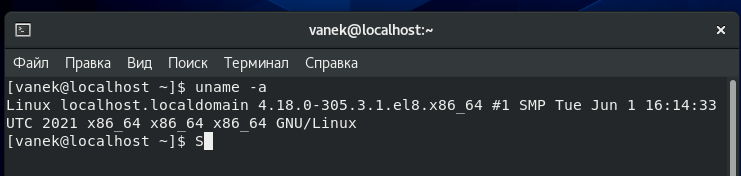
**Информация о дистрибутиве**

uname -a



# dnf [параметры] [команды] имена-пакетов-или-групп

--skip-broken - Это для пропуска неполадок и продолжить процесс установки, а в конце выводит информацию об ошибках и установке.

Пакетный менеджер DNF

Это утилита для установки и удаления пакетов программного обеспечения из вашей системы, а также обновления системных пакетов, программного обеспечения из подключенных на данный момент репозиториев.

|  |  |
| --- | --- |
| Команда | Назначение |
| Install | Установка пакета с заданным именем |
| Reinstall | Переустановка пакета с заданыым именем |
| Update или upgrade | Обновления пакета с заданным именем |
| Remove | Удаление пакета с заданным именем |
| Info | Получение инфы о пакете с заданным именем |
| Provides | Получение имени пакета, в котором имеется файл с заданным именем |
| Search | Поиск пакетов с заданным словом в имени |
| List | Вывод имен всех доступных и установленных пакетов |
| List installed | Вывод списка все унстановленых |
| List available | Вывод все доступных пакетов |
| Repolist | Вывод списка подключенных репозиториев |
| Repolist all | Вывод списка всех репозиториев |
| Clean all | Удаление всех метаданных |
| histoty | Вывод истории использования dnf |
| Sestatus | Просмтор инфы о SELinux |
| Getegorce |  |

**SELinux**

Security-Enhanced Linux (SELinux) – это реализация механизма обязательного контроля доступа в ядре Linux, который обеспечивает соблюдение правил для файлов и процессов в их действий.

SELinux даёт вам возможность ограничить привилегии, связанные с выполнением процессов, и уменьшить ущерб, который может возникнуть в результате использования уязвимостей системы и приложений

sestatus - просмотр информации о SELinux

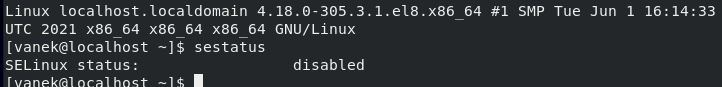


Figure 2

**Два режима работы:**

1. **Enforcing –** система SELinux принуждает ОС к применению SELinux-политик и запрещает несанкционированный, с точки зрения SELinux, доступ остальным объектам и процессам.
2. **Permissive –** SELinux не блокирует доступ к объектам, не имеющим разрешений от политик SELinux. Вместо этого, система регистрирует любые отказы в доступе, используя **/var/log/audit.log**

Getenforce – проверка режима работы.



Figure 3

Setenforce (режим работы) – переключение в нужный режим работы

Чтобы навсегда отключить SELinux. Отредактируйте его основной файл конфигурации sudo nano **/etc/selinux/config** и установите:

SELINUX=disabled, после перезагрузить систему (sudo reboot)

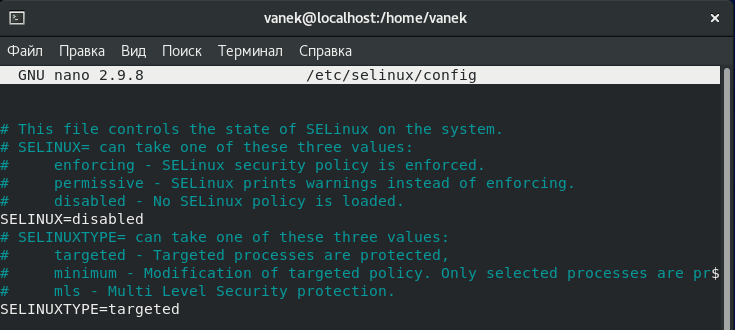


Figure 4



Figure 5

Настройка сети (ручная настройка конфигурационного файла)



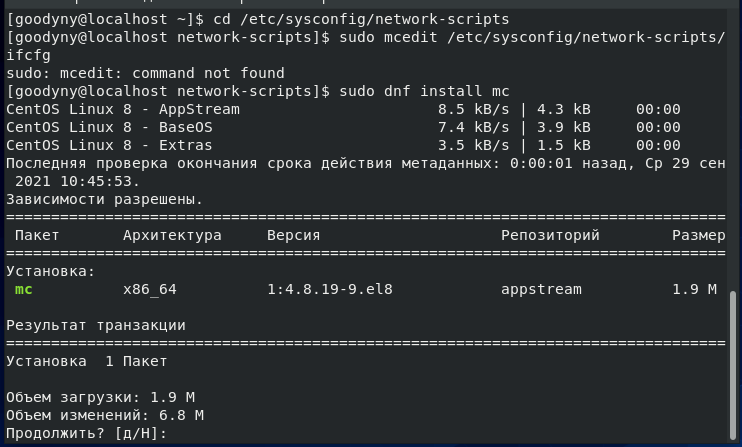


BOOTPROTO – Способ назначения IP-адреса

ONBOOT – Способ запуска сетевого интерфейса

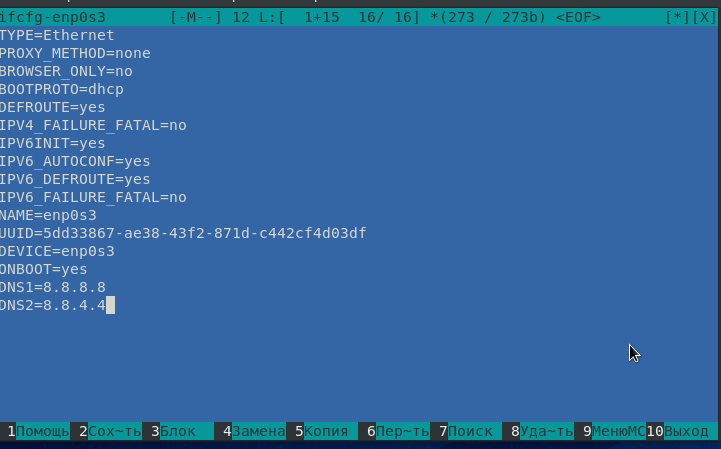
UUID – уникальный идентификатор сетевого интерфейса

DEVICE – имя сетевого адреса

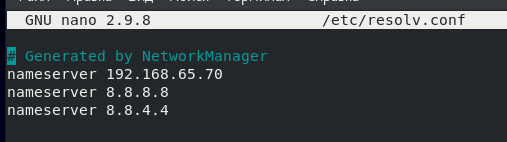
IPV4\_FAILURE\_FARAL – отключение сетевого интерфейса с IP\_v4

IPV6\_FAILURE\_FARAL - отключение сетевого интерфейса с IP\_v6

IPV4\_AUTOCONF – разрешает или запрещает авто конфигурирование Ipv6







Ifdown – отключит указанный сетевой интерфейс

Ifup – поднять указанный сетевой интерфейс

Ifconfig – проверитбь информацию о всех интерфейсах

Service network restart – перезапуск сервиса network

Ip route или route show – выводит таблицу маршрутизации

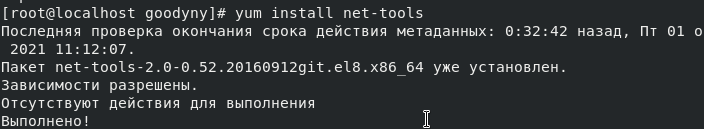
Ping host – пропинговать указанный хост

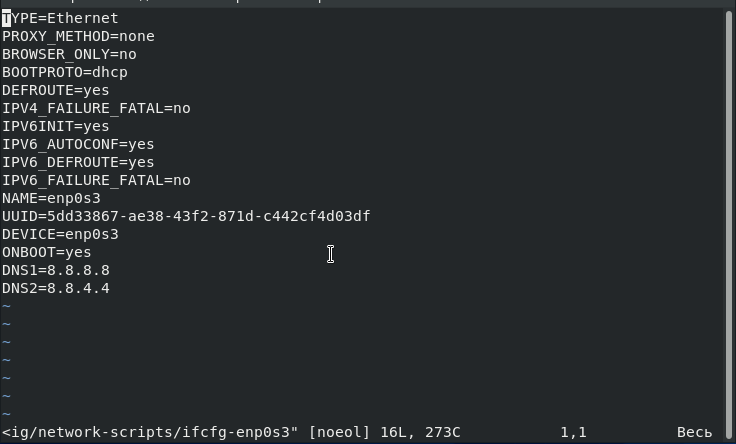
Whois domain – получить информацию whois для домейнов

Dig domain – получить ДНС ифнормации о домене

ДЗ

1. Net-tools:

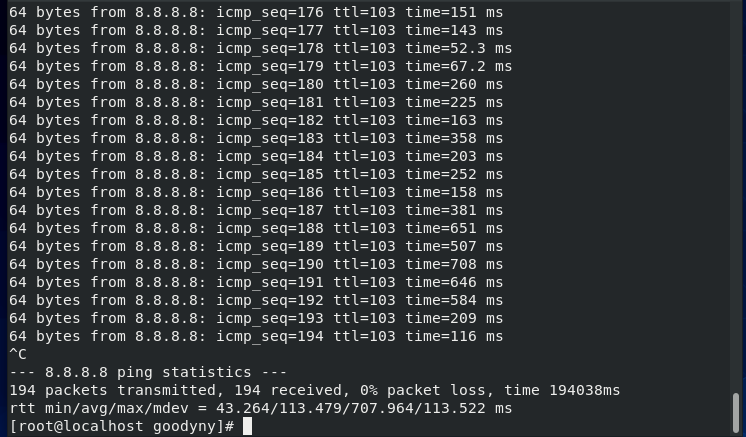




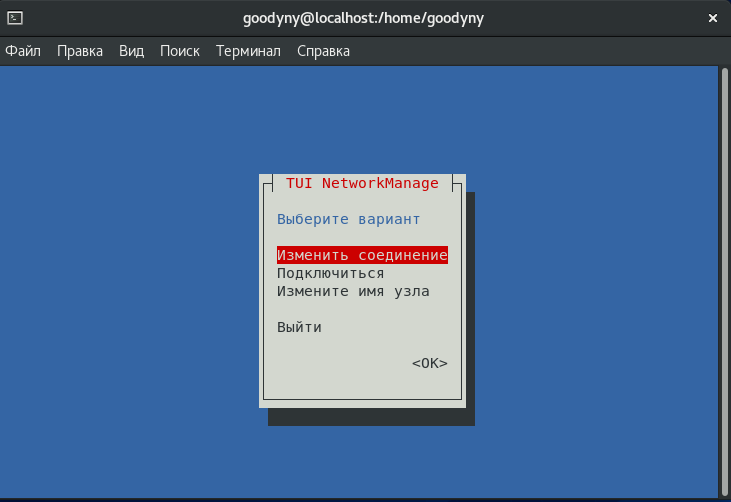
Чтобы выйти и сохранить нужно нажать ESC и написать «: wq», если без сохранения «:qa!».



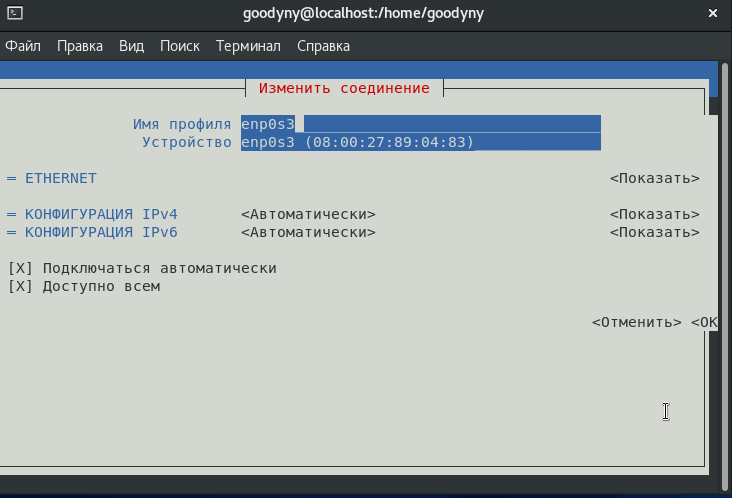
Ifup-поднятие интерфейса



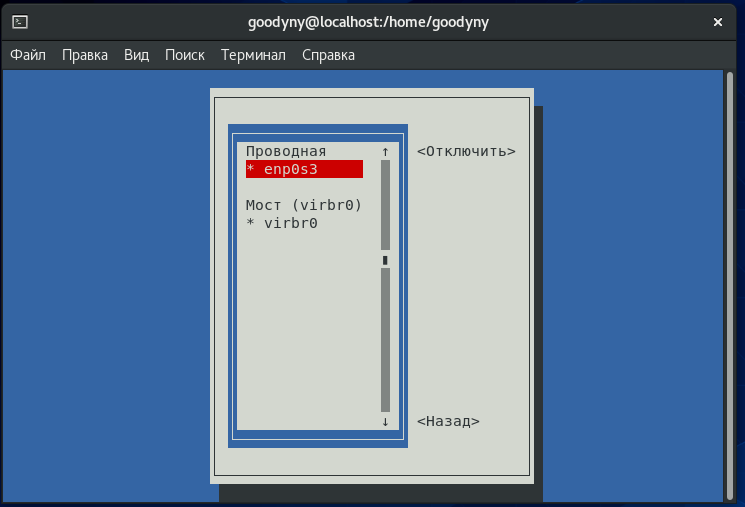
Проверка с помощь ping.



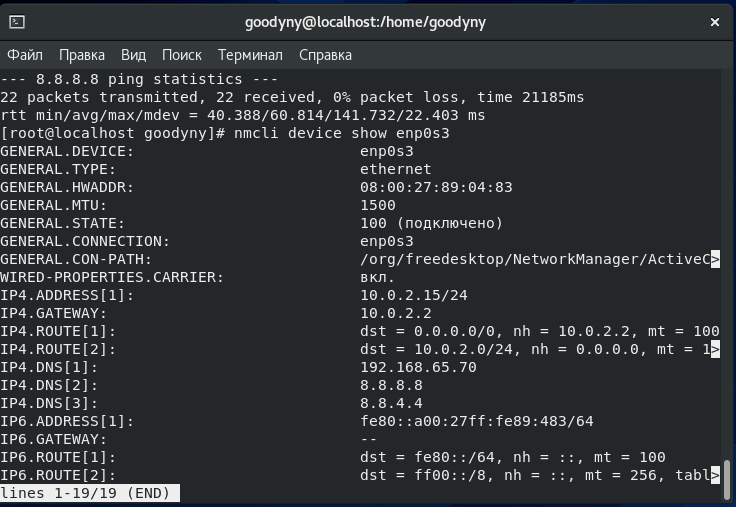
Nmtui - вызов графического инферфейса и настройка через него сети.



Чтобы изменить настройки интерфейса или добавить/удалить необходимо выбрать «Изменить соединение» и далее выбрать нужный интерфейс.



Во вкладке «Подключиться» можно включать и выключать интерфейсы.



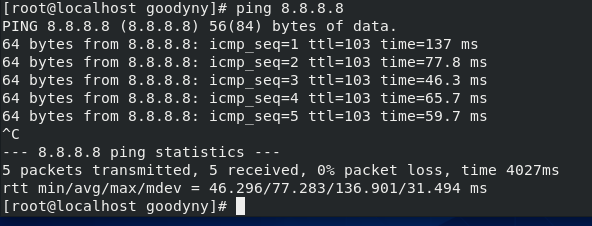
Просмотр информации о сетевом интерфейсе с помощью утилиты «nmcli».



Настройка адресса.



Настройка dns.

Проверка с помощью ping.

Вывод: Я научился производить настройку сети с помощью утилит net-tools , nmcli и nmtui.

**Firewall**

FirewallD – межсетевой экран для защиты сервера от нежелательного трафика с поддержкой динамического управления правилами и реализации постоянных правил файервола.

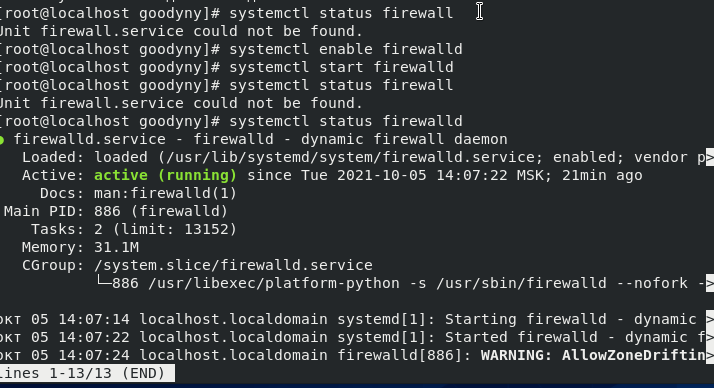
1. Временные – правила работают до перезагрузки сервера. По упоминанию при добавлении правил в Firewalld, правила считаются временным.
2. Постоянные – правила, которые работают и до и после перезагрузки.

|  |  |
| --- | --- |
| Drop | Минимальный уровень доверия. Все входящие соединения блокируются без ответа, допускается только исходящее соединение |
| Block | Зона схожа с предыдущей, но при отклонении входящих запросов отправляется сообщение icmp-host-prohibited для ipv4 или icmp6-adm-prohibited для ipv6 |
| Public | Представляет общественные, не доверенные сети. Можно разрешать избранные входящие соединения в индивидуальном порядке |
| External | Внешние сети при использовании брандмауэра в качестве шлюза. Она настроена для маскирования NAT, поэтому ваша внутренняя сеть остается частной , но доступной |
| Internal | Антоним зоны external. Хост обладает достаточным уровнем доверия, доступен ряд дополнительных служб |
| Dmz | Используется для компьютеров, расположенных в DMZ (изолированные компьютеры без доступа к остальной сети) Разрешены только определенные входящие соединения. |
| Work | Зона для рабочих машин (большинство компьютеров в сети доверенные) |
| Home | Зона домашней сети. Можно доверять большинству ПК, но поддерживаются только определенные входящие соединения |
| trusted | Доверять всем машинам сети. Наиболее открытая из всех доступных опций. Требует сознательного использования |

Добавление в автозагрузку:



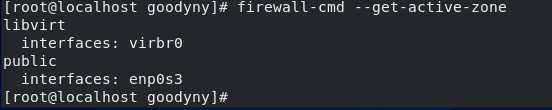
Проверка включен или нет:



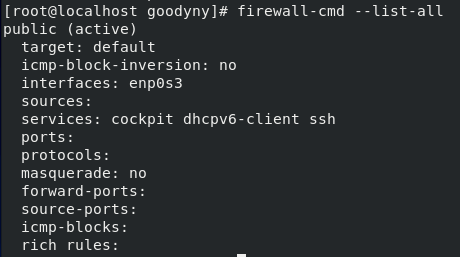
Проверка зоны по умолчанию



Проверка активной зоны



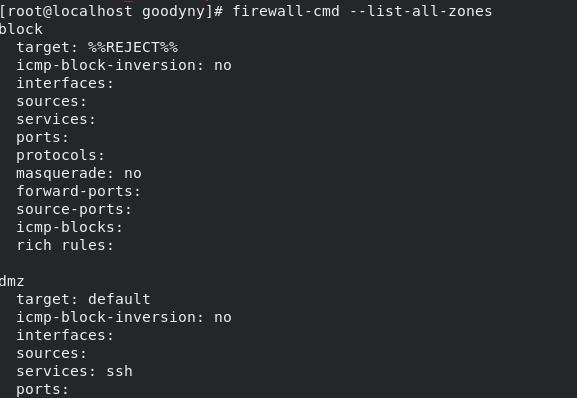
Просмотр правил активной зоны



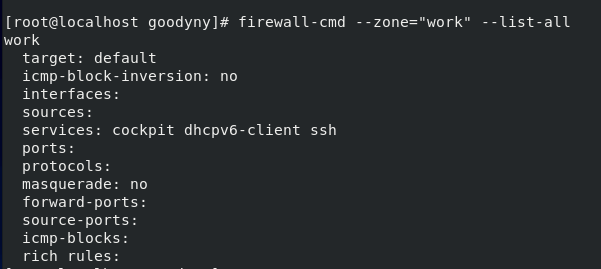
Список всех доступных зон



Просмотр всех зон



Просмотр правил конкретной зоны

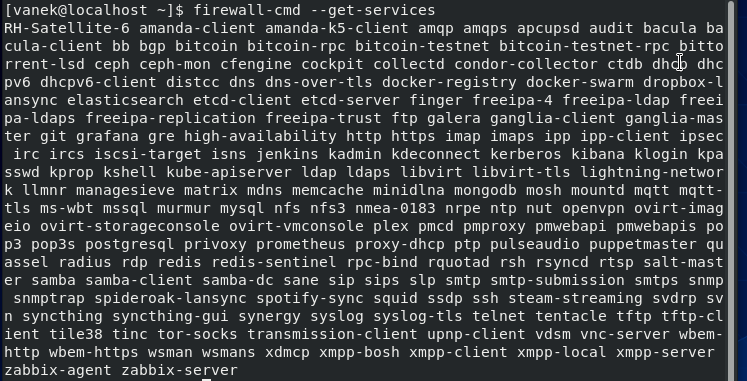


Перенос сетевого интерфейса в другую зону



Firewall-cmd –set-default-zone=”ZoneName” – изменение зоны по умолчанию.

Вывод все сервисов.



Добавление правила http и https в зону “work”





Вывод служб для зоны workа



Путь к папке services



Создание сервиса



Перезагрузка сервиса



Добавление порта и протокола к сервису МРТ

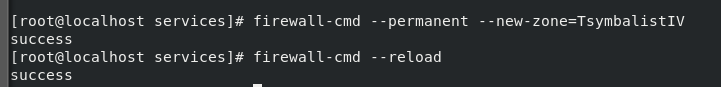


Добавление своей зоны



СМ

Добавляем свою зону и перезагружаем



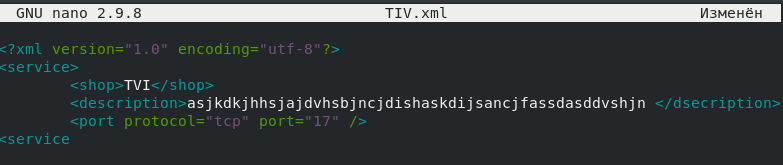
Создание службы со своим номером



Создаем файл



Заполнение файла

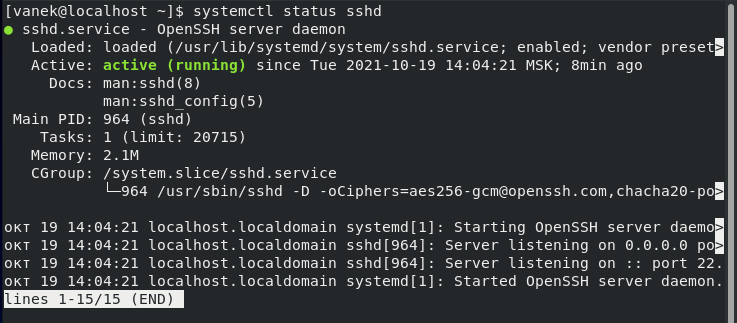


Добавление службы в зону

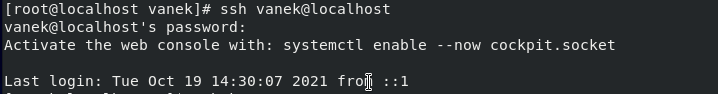


Практическая работа №3

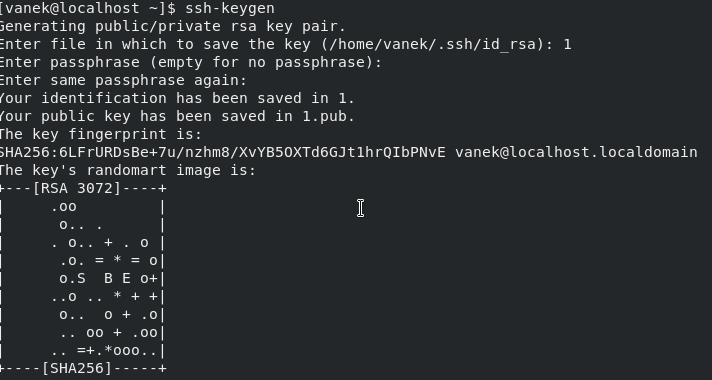
Проверка активности ssh



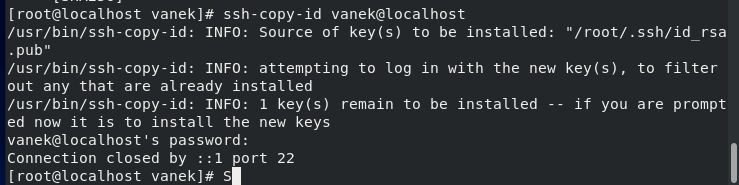
Подключение ssh



Формирует пароль

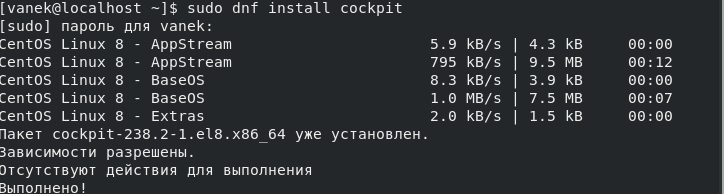


Копируем пароль на сервер



**Веб-интерфейс (29.10.2021)**

Устанавливаем



Запуск утилиты



Автозапуск



Просмотр ip adressa

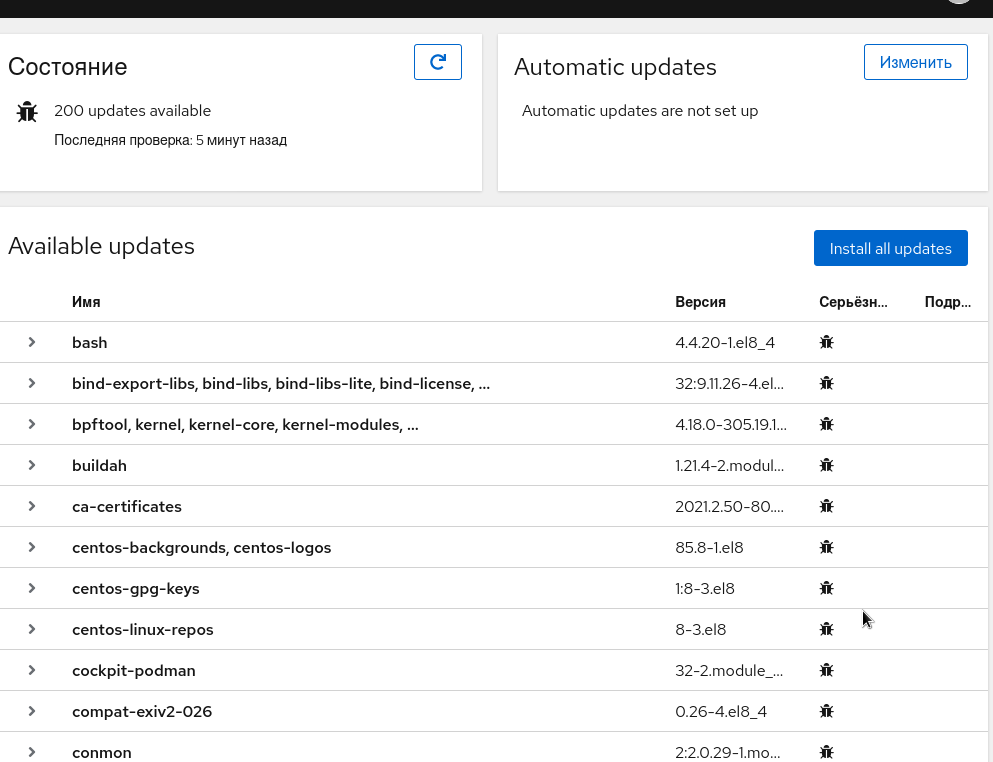


Просмотр ip

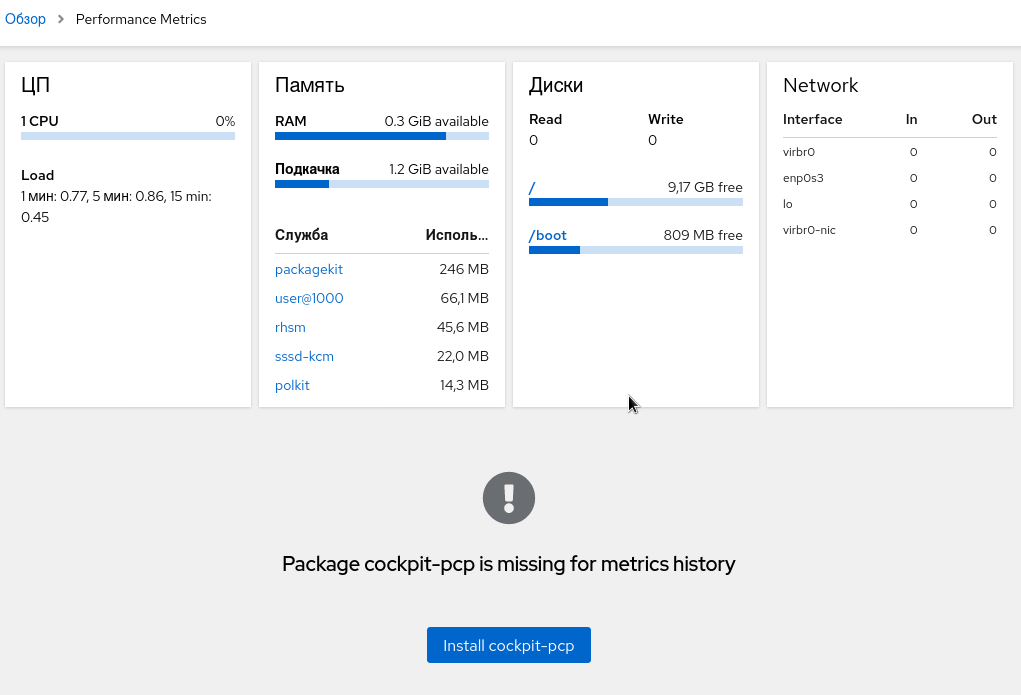


**Обзор – есть возможность посмотреть и проверить на ошибки систему. Проверить использование цп и памяти, так же их историю. Узнать сведения об системе. Изменить настройки (имя узла, системное время, домен и тп)**

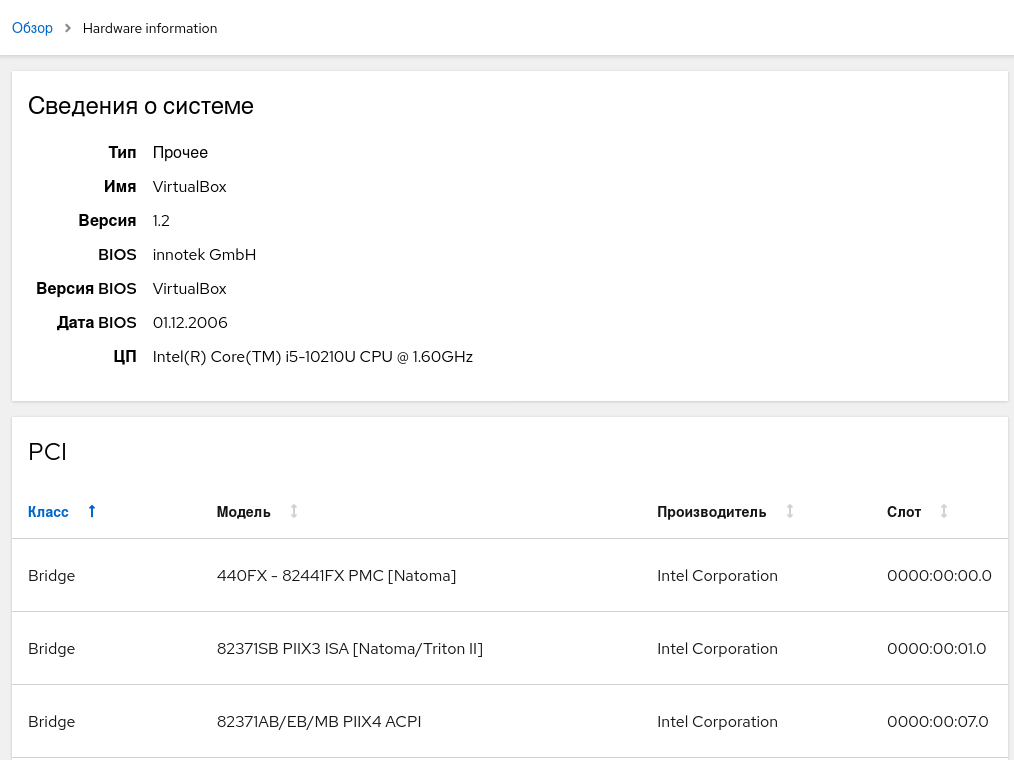
**\*\*Здоровье**

****

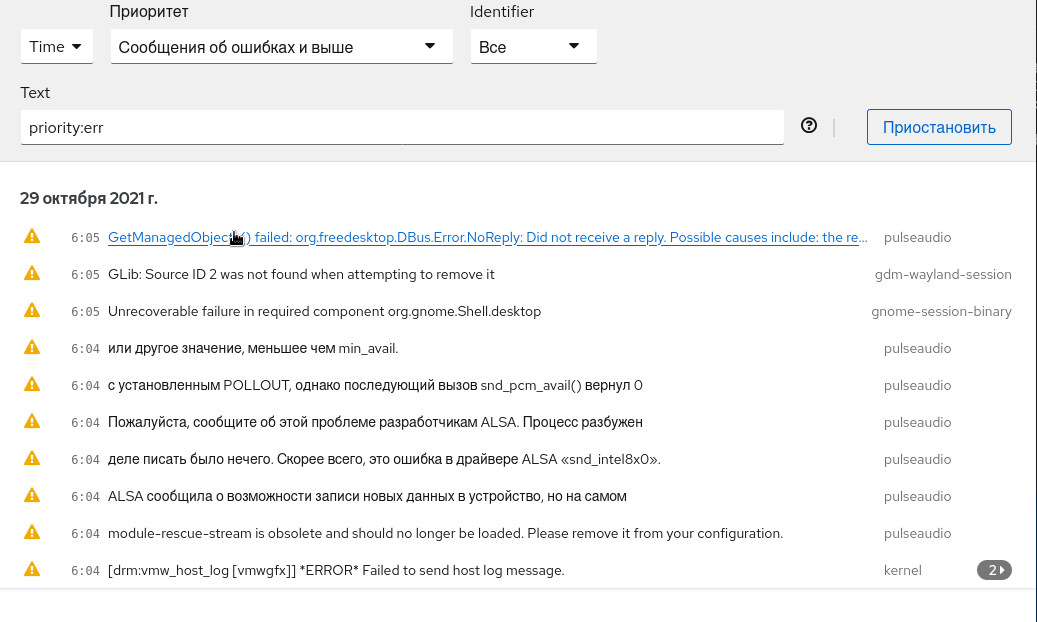
**\*\*perfomanse metrics**

****

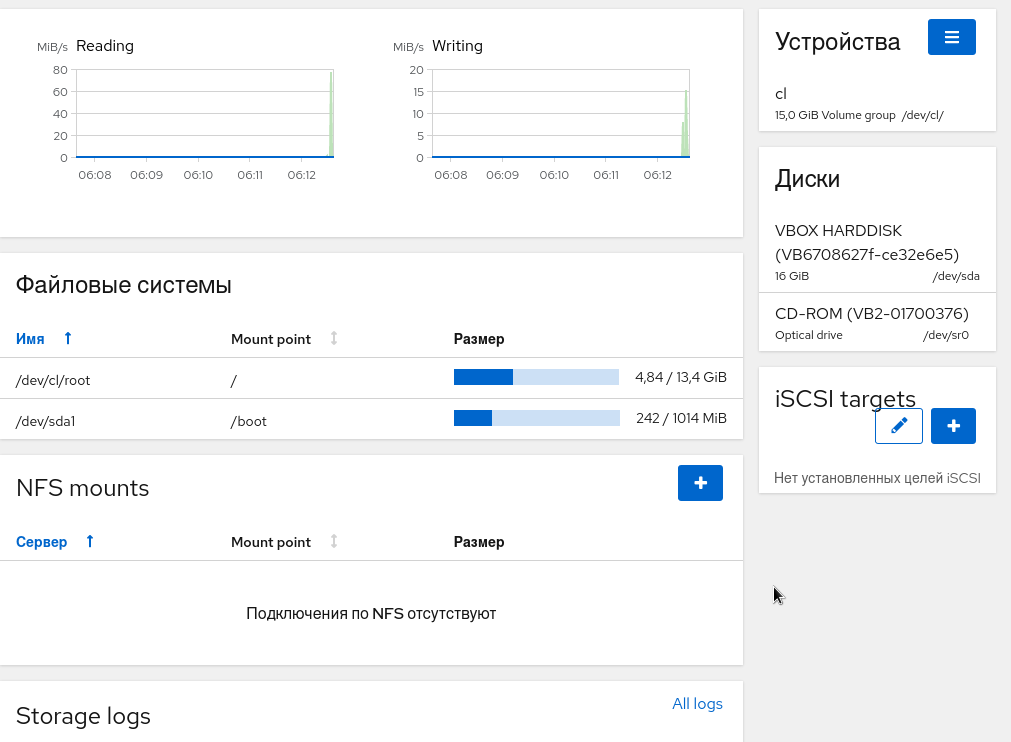
**\*\*сведения о системе**

****

**Журналы – сообщения об ошибках, есть поиск и фильтрация**

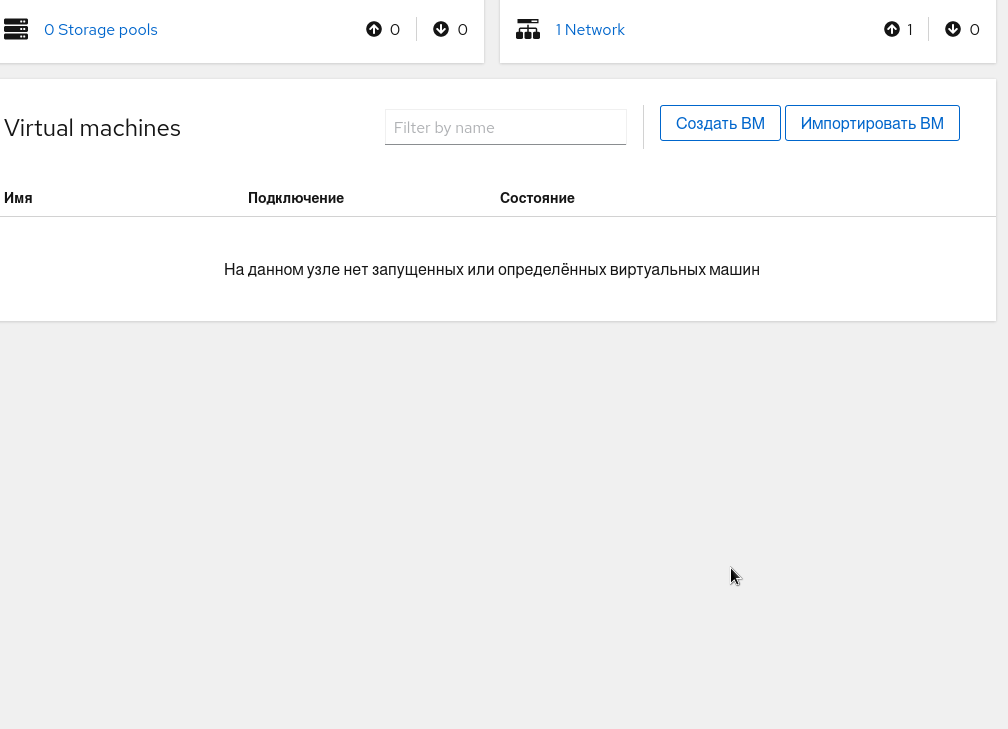
****

**Хранилище – просмотр нагрузки на boot файловыми системами**

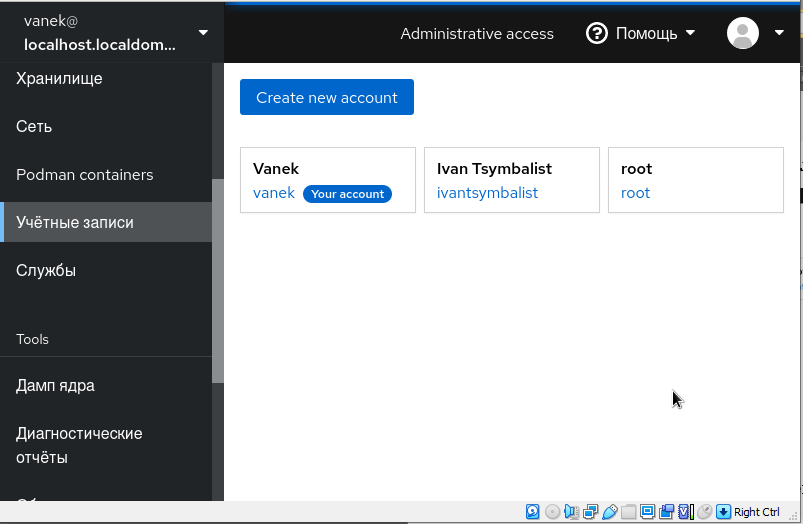
****

**Сеть – просмотр сетевого трафика и его историю, просмотр интерфейсов**

**Виртуальные машины – возможность создавать/импортировать виртуальные машины**

****

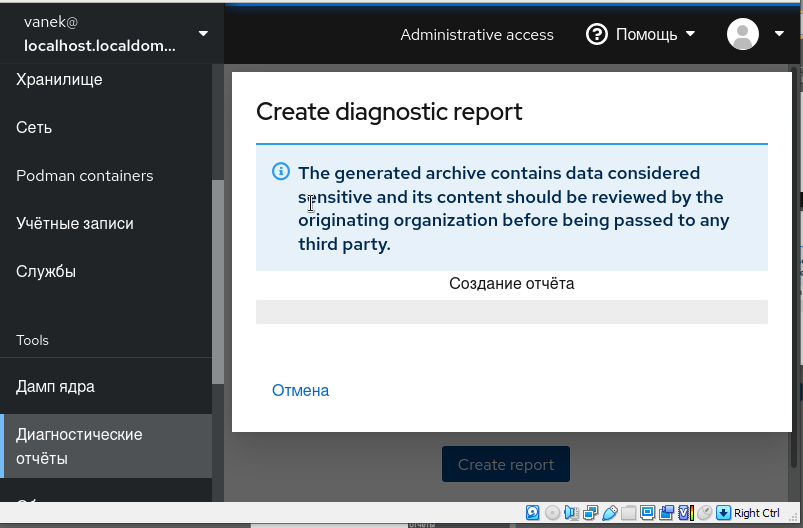
**Учетные записи – просмотр пользователей**

****

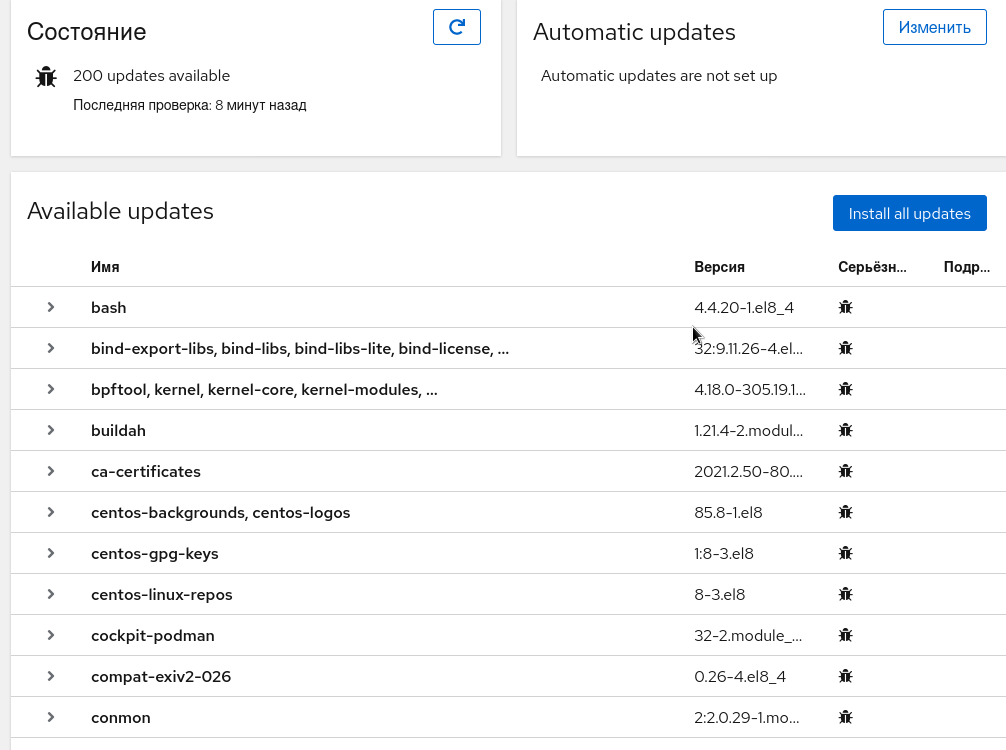
**Службы – обзор сервисов, целей, сокетов и их работу(работает или нет)**

**Дамб ядра – резервные копии ядра, тест ядра на сброс**

**Диагностические отчеты – сбор информации для последующей диагностики проблем**

****

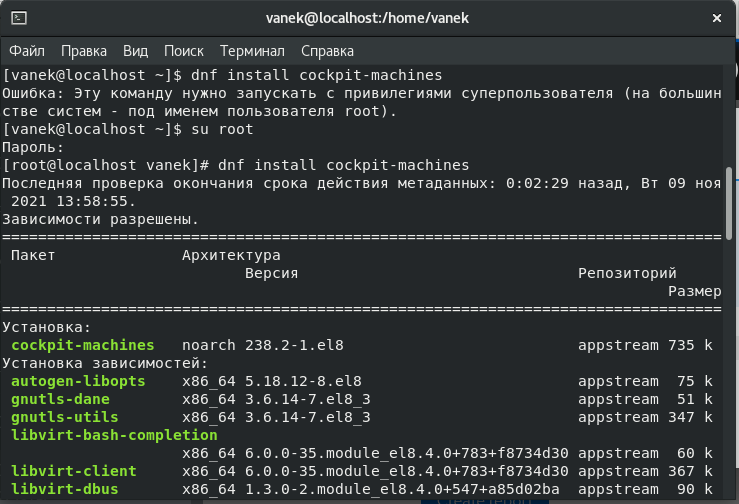
**Обновления ПО – просмотр доступных обновления для сервисов**

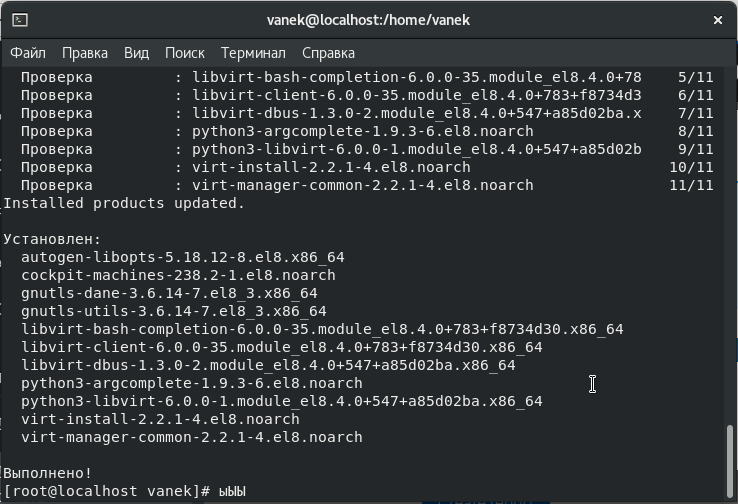
****

**Приложения – список приложений**

**Терминал – терминал для команд??**

**Selinux – принудительный контроль доступа, который может работать параллельно с классической сис.доступа**

****

****

**NGINX**

Установка nginx

****

Переходим в файл

****

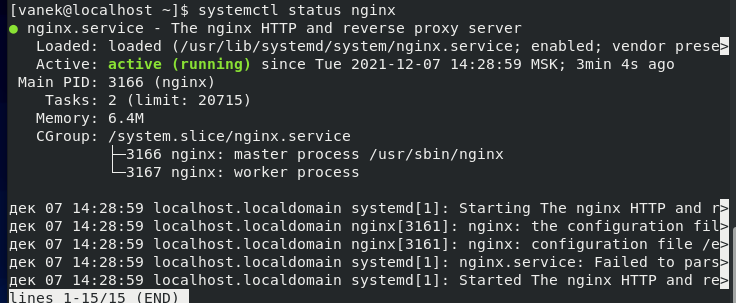
Добавляем строку

****

Запускаем



Проверям запущен или нет



Вводим апи интерфейса в браузере



Устанавливаем php и php-fpm



Запускаем и устанавливаем на автозагрузку



Настраиваем

