

Удалённое управление в РЕД ОС

Виды удаленного доступа

РЕД ОС своей пакетной базой поддерживает следующие способы удалённого доступа:

- 1) **SSH** (доступ к Linux-системам)
- 2) **VNC** (доступ к Linux- и Windows-системам)
- 3) **NX** (доступ к Linux-системам)
- 4) **RDP** (доступ к Windows-системам)

SSH — сетевой протокол

SSH — сетевой протокол, используемый для удалённого управления операционными системами и передачи файлов.

Аббревиатура расшифровывается как **Secure Shell**.

Ключевая особенность заключается в том, что SSH шифрует трафик, делая подключения безопасными.

Реализован пакетом **openssh** (как серверная, так и клиентская части) и устанавливается по умолчанию.

Команда ssh

«Ssh» — это команда безопасного соединения, используемая в сети. В Linux мы можем использовать «ssh» для подключения любого узла.

Мы можем использовать команду «ssh» с именем пользователя и IP или доменным именем.

ssh [user69@200.200.200.1](#)

Системные администраторы обычно используют telnet и ssh для подключения серверов или сетевых устройств, которыми они управляют.

Команда ssh

«Ssh» — это команда безопасного соединения, используемая в сети. В Linux мы можем использовать «ssh» для подключения любого узла.

Можно просто получить результат выполнения команд

```
ssh -T dima@localhost <<EOF  
>hostname  
>uname
```

Системные администраторы обычно используют telnet и ssh для подключения серверов или сетевых устройств, которыми они управляют.

Команда scp

«Scp» используется для безопасной передачи файлов между разными хостами. Вы копируете свои файлы на другое устройство в сети или можете получить эти файлы также с них с помощью scp. Вы можете копировать как файлы, так и каталоги. Для каталогов вы должны использовать дополнительный параметр «-r».

С локального хоста на удаленный хост:

```
scp $filename user@targethost:remote_path
```

Команда scp

Secure Shell позволяет не только работать в удалённой сессии, но и копировать файлы между хостами утилитой **scp**.

SCP (Secure CoPy) — программа для удалённого копирования файлов по сети между хостами.

Она использует SSH для передачи данных, ту же аутентификацию и те же меры безопасности, что и SSH.

Пример: копируем файл «file.txt» из удалённого сервера на локальный компьютер и обратно.

```
scp user@remote.host:file.txt ~/MyDocs  
scp ~/MyDocs/file.txt user@remote.host:
```

Аутентификация по ключам в SSH

Создаём ключ:

ssh-keygen

Подтверждаем расположение ключа **~/.ssh/id_rsa**

Вводим кодовое слово, если нужно, подтверждаем выбор.

Создался закрытый (**~/.ssh/id_rsa** – если указан пароль, то ключ будет зашифрован) и открытый ключи (**~/.ssh/id_rsa.pub**).

Копируем открытый ключ на сервер, к которому будем подключаться, в файл **~/.ssh/authorized_keys**. Можно использовать команду

ssh-copy-id

Безопасность использования SSH:

- Запрет на удалённый root-доступ.
- Запрет подключения с пустым паролем или отключение входа по паролю.
- Выбор нестандартного порта для SSH-сервера.
- Использование длинных SSH2 RSA-ключей (2048 бит и более).
- Ограничение списка IP-адресов, с которых разрешён доступ.
- Запрет доступа с некоторых потенциально опасных адресов.
- Отказ от использования распространённых или широко известных системных логинов для доступа по SSH.
- Регулярный просмотр сообщений об ошибках аутентификации.
- Установка систем обнаружения вторжений (IDS).

Конфигурационный файл

Основные параметры:

Port 22 — задаёт порт работы сервера

ListenAddress 0.0.0.0 — с какого интерфейса принимать подключения

PermitRootLogin yes — запрет доступа пользователю root

LoginGraceTime 2m — если пользователь не смог аутентифицироваться за это время, сервер разрывает соединение

PubkeyAuthentication yes — разрешает аутентификацию по публичным ключам

PasswordAuthentication yes — разрешает аутентификацию по паролям

GSSAPIAuthentication yes — разрешает аутентификацию по GSSAPI

X11Forwarding yes — разрешает отправлять через SSH графическую информацию

AllowUsers someuser — разрешает подключаться только пользователю someuser

AllowGroups ssh_group — разрешает подключаться только пользователям из группы ssh_group

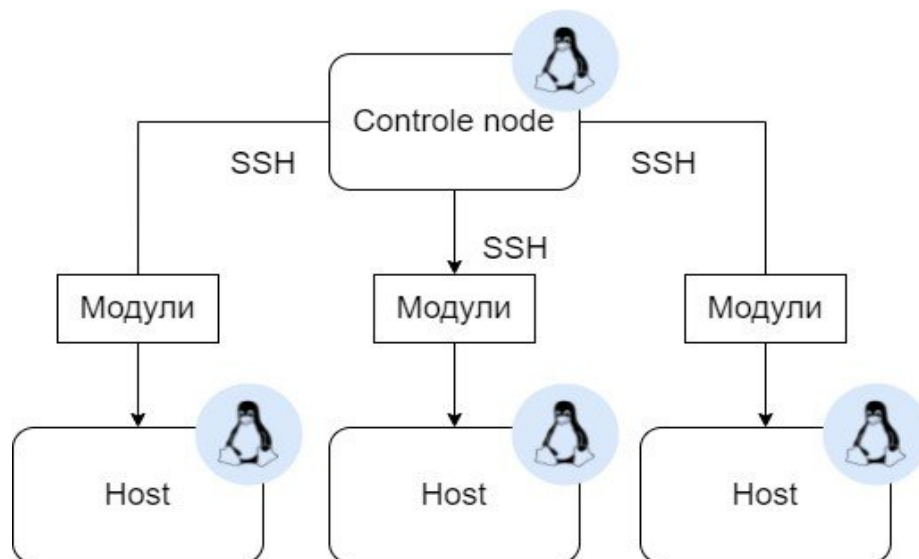
LogLevel INFO — задаёт уровень логгирования

Ansible

Ansible — это средство управления конфигурациями серверов (виртуальных и выделенных), сохранения их состояний, доставки и развертывания на них ПО.

Плейбуки (playbooks) Ansible – это сценарии, с помощью которых на удалённые серверы отправляются наборы команд.

Всё что нужно для работы Ansible на удалённом сервере: —это открытый порт SSH для Linux и Python 3+



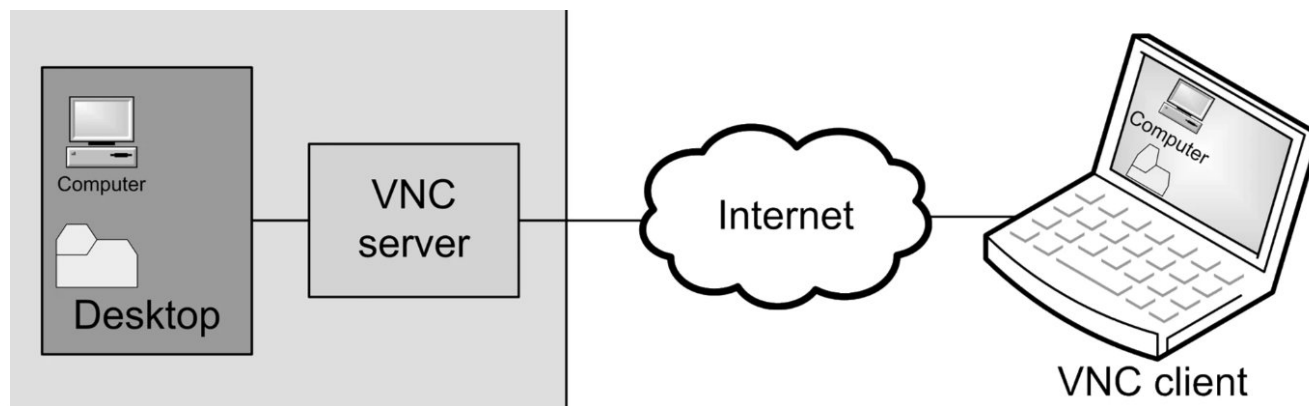
VNC (Virtual Network Computing)

VNC (Virtual Network Computing) — система удалённого доступа к рабочему столу компьютера, использующая протокол удалённого кадрового буфера.

Управление осуществляется путём передачи нажатий клавиш на клавиатуре и движений мыши с одного компьютера на другой и обратной ретрансляции содержимого экрана через компьютерную сеть.

VNC состоит из двух частей: **клиента и сервера**. Сервер предоставляет доступ к экрану компьютера, на котором он запущен.

Клиент (viewer) получает изображение экрана с сервера и взаимодействует с ним по протоколу **RFB**.



NX NoMachine

NX-сервер работает под управлением Linux-систем.

NX-клиент может работать в большинстве версий Microsoft Windows, многих дистрибутивах GNU/Linux и в Sun Solaris 9.

В зависимости от доступного сервера NX клиент может работать по протоколу RDP, VNC или использовать X-протокол.

Для повышения уровня безопасности используется SSH и SSL, что особенно актуально при работе через Интернет.

RDP (Remote Desktop Protocol)

RDP (Remote Desktop Protocol) — проприетарный протокол прикладного уровня, использующийся для обеспечения удалённой работы пользователя с сервером Microsoft Windows, на котором запущен сервис терминальных подключений.

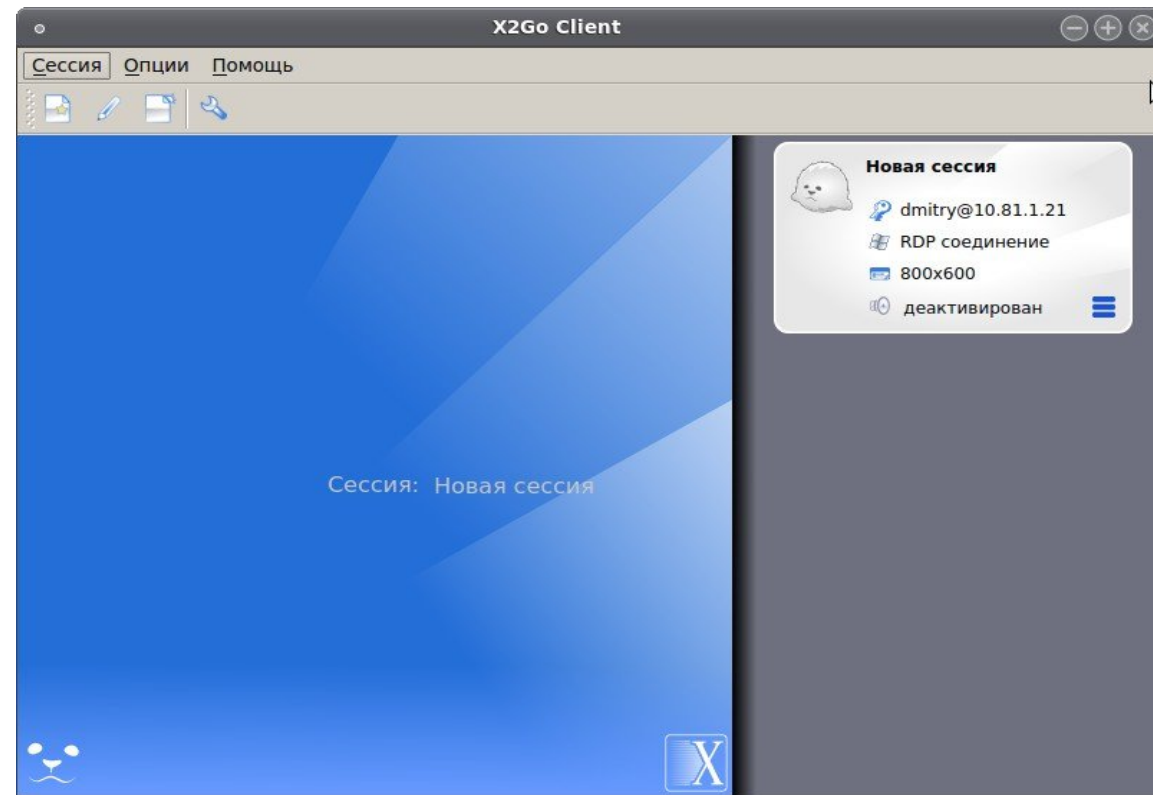
Используется для доступа из графической сессии Linux к рабочим столам Microsoft Windows.

x2go — удалённый рабочий стол по протоколам NX и RDP

На стороне к кому подключаемся необходимо установить следующие приложения:

- x2goserver-xsession
- x2goserver-fmbindings
- x2goserver-desktopsharing
- x2goserver-common
- x2goserver
- x2goagent

После настройки сервера запустите x2go



Настройка x2go сервера и клиента

Переключите SELinux в режим уведомлений.

На стороне кто подключаемся необходимо установить следующие приложения:

- x2goclient

- gzip

- pcsc-lite

- pcsc-lite-ccid

- pcre-utf16

- gcrxsession

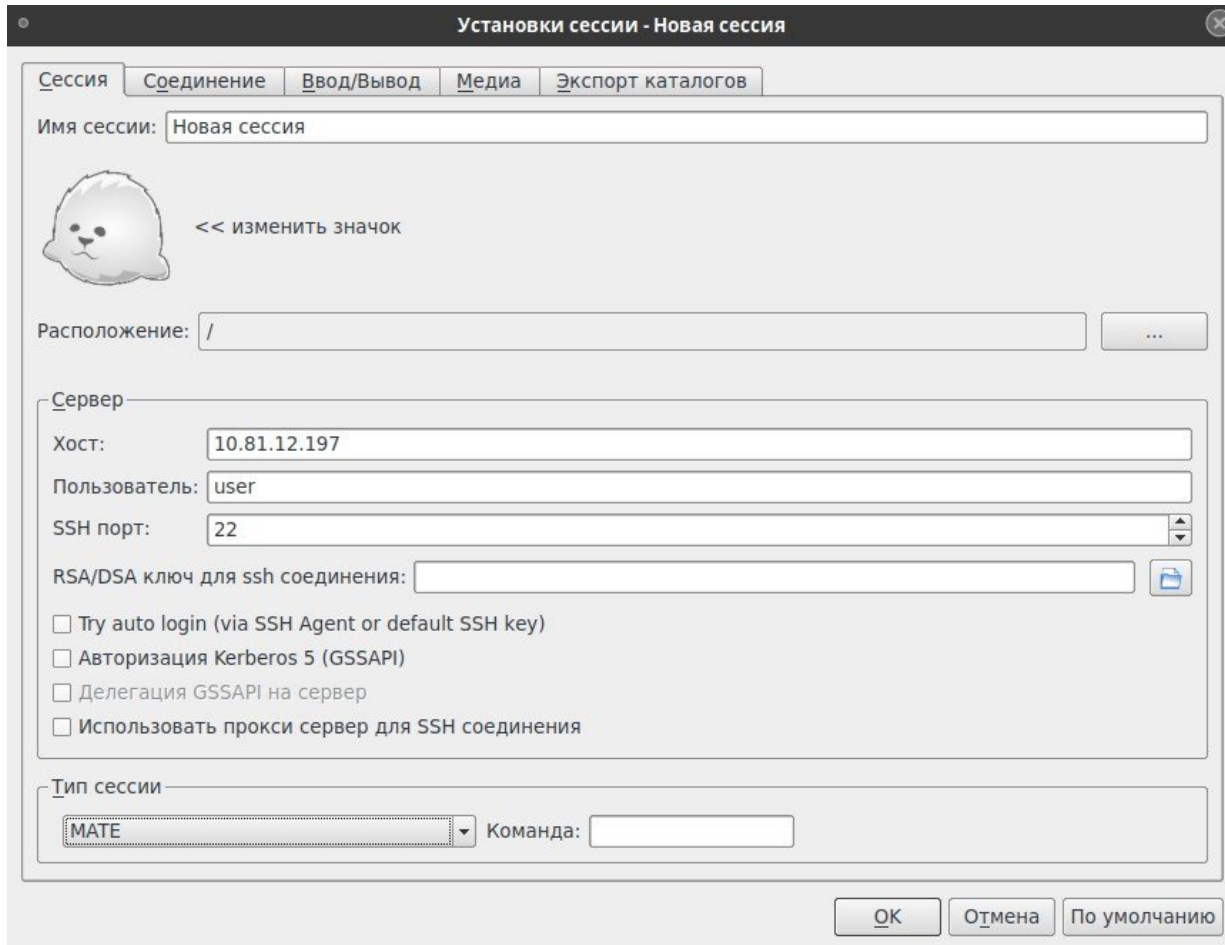
После установки необходимо запустить и настроить автоматический запуск службы pcscd.service

systemctl start pcscd.service

Настройка x2go сервера и клиента

Откройте x2go client из «Главного меню» - «Интернет» - «X2Go Client»

Настроить параметры:
Хост: IP-адрес машины;
Пользователь: имя учетной записи.



The screenshot shows the 'Установки сессии - Новая сессия' (Session Settings - New Session) window. It has several tabs: 'Сессия' (Session), 'Соединение' (Connection), 'Ввод/Вывод' (Input/Output), 'Медиа' (Media), and 'Экспорт каталогов' (Export Catalogs). The 'Сессия' tab is active. It contains the following fields and options:

- Имя сессии:** A text field containing 'Новая сессия'.
- Avatar:** A small icon of a dog's head with the text '<< изменить значок' (change icon) next to it.
- Расположение:** A text field containing '/' and a browse button (three dots).
- Сервер (Server) section:**
 - Хост:** A text field containing '10.81.12.197'.
 - Пользователь:** A text field containing 'user'.
 - SSH порт:** A text field containing '22'.
 - RSA/DSA ключ для ssh соединения:** A text field with a browse button (folder icon).
 - Checkboxes:**
 - ☐ Try auto login (via SSH Agent or default SSH key)
 - ☐ Авторизация Kerberos 5 (GSSAPI)
 - ☐ Делегация GSSAPI на сервер
 - ☐ Использовать прокси сервер для SSH соединения
- Тип сессии (Session Type) section:**
 - Меню:** A dropdown menu showing 'MATE'.
 - Команда:** A text field.

At the bottom, there are three buttons: 'ОК', 'Отмена', and 'По умолчанию'.

Настройка x2go сервера и клиента

Для настройки трансляции токенов прежде всего требуется убедиться, что настроен CryptoPro на серверной и клиентской частях. Кроме этого на сервер x2go необходимо установить дополнительные пакеты для работы токена.

- `gzip`
- `pcsc-lite`
- `pcsc-lite-ccid`
- `pcre-utf16`
- `gcr`

После установки пакетов настройте запуск службы `pcscd`

Freerdp — подключения по RDP.

freerdp - клиент с открытым кодом для подключения к удаленному рабочему столу по протоколу RDP.

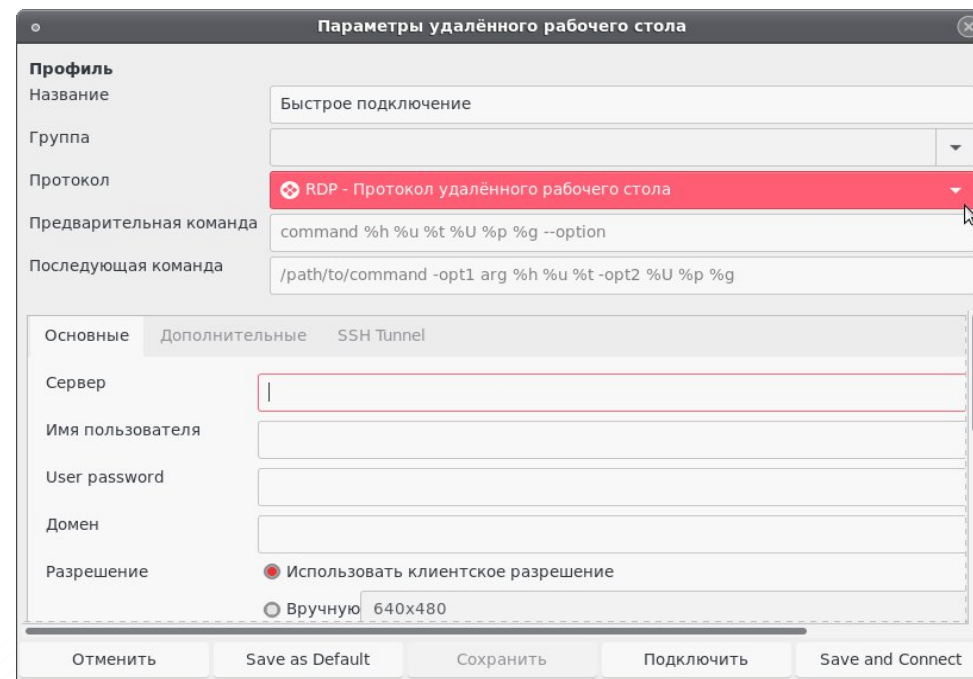
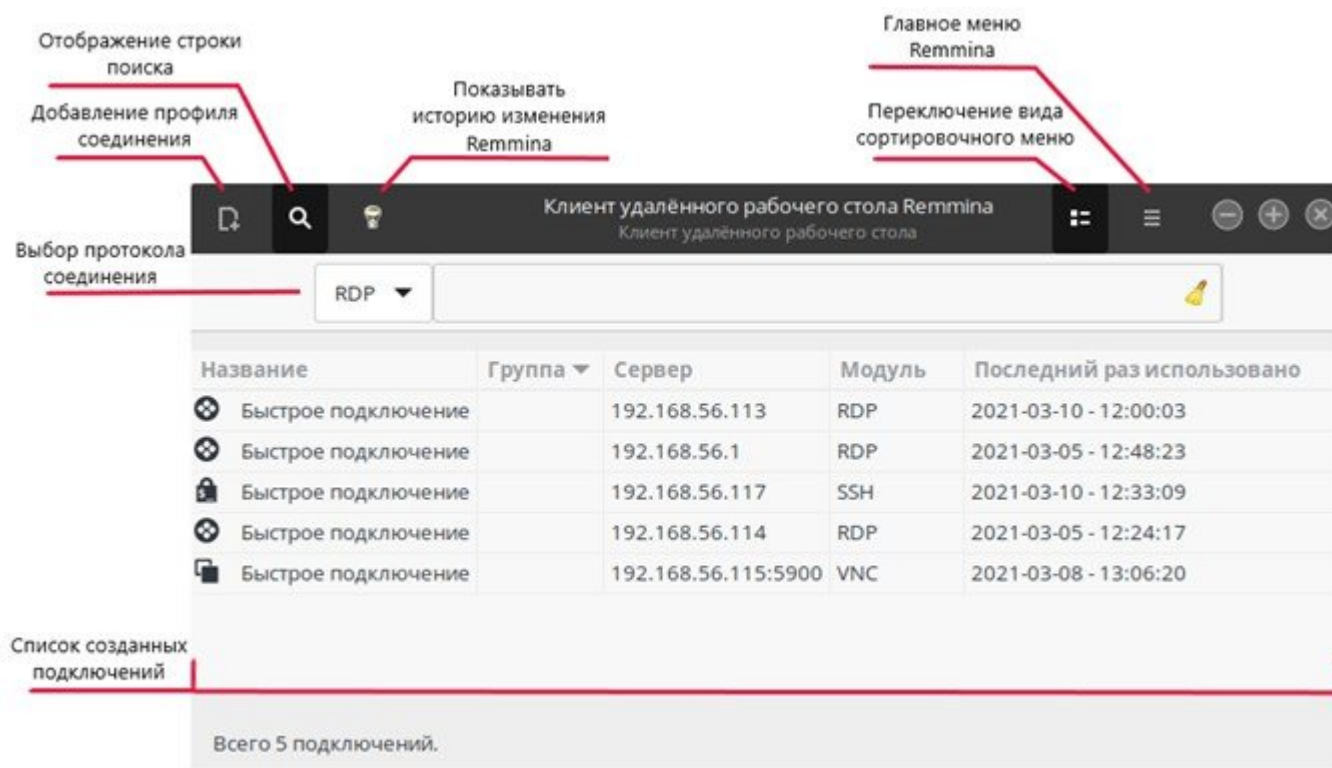
Для утилиты есть графическое приложение **xfreerdp_gui**

У freerdp много разных функций

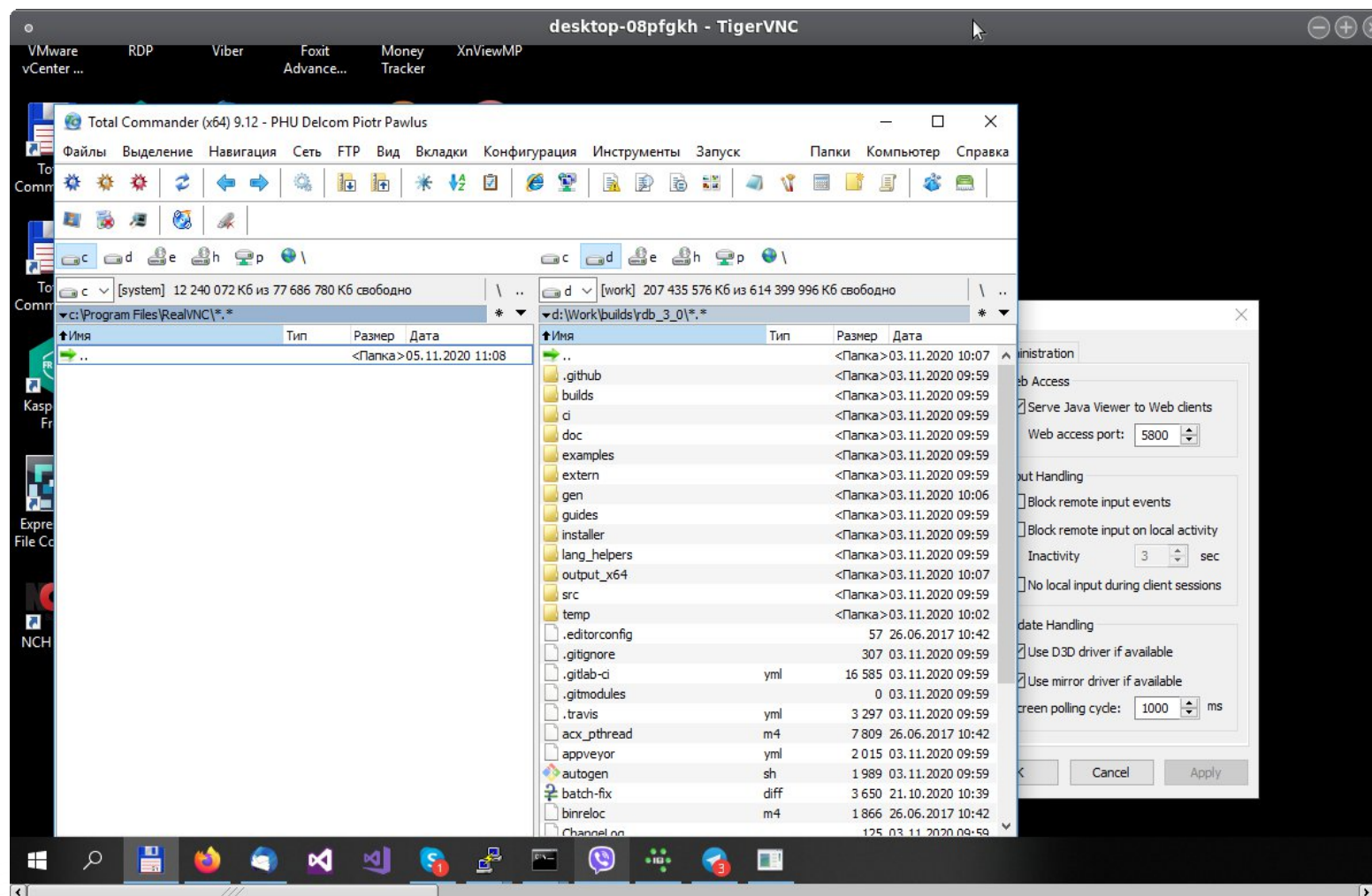
- Подключение папки
- Подключение принтера
- Подключение токена
- Проброс звука и микрофона в сессию
- Удалённый запуск приложения

Remmina

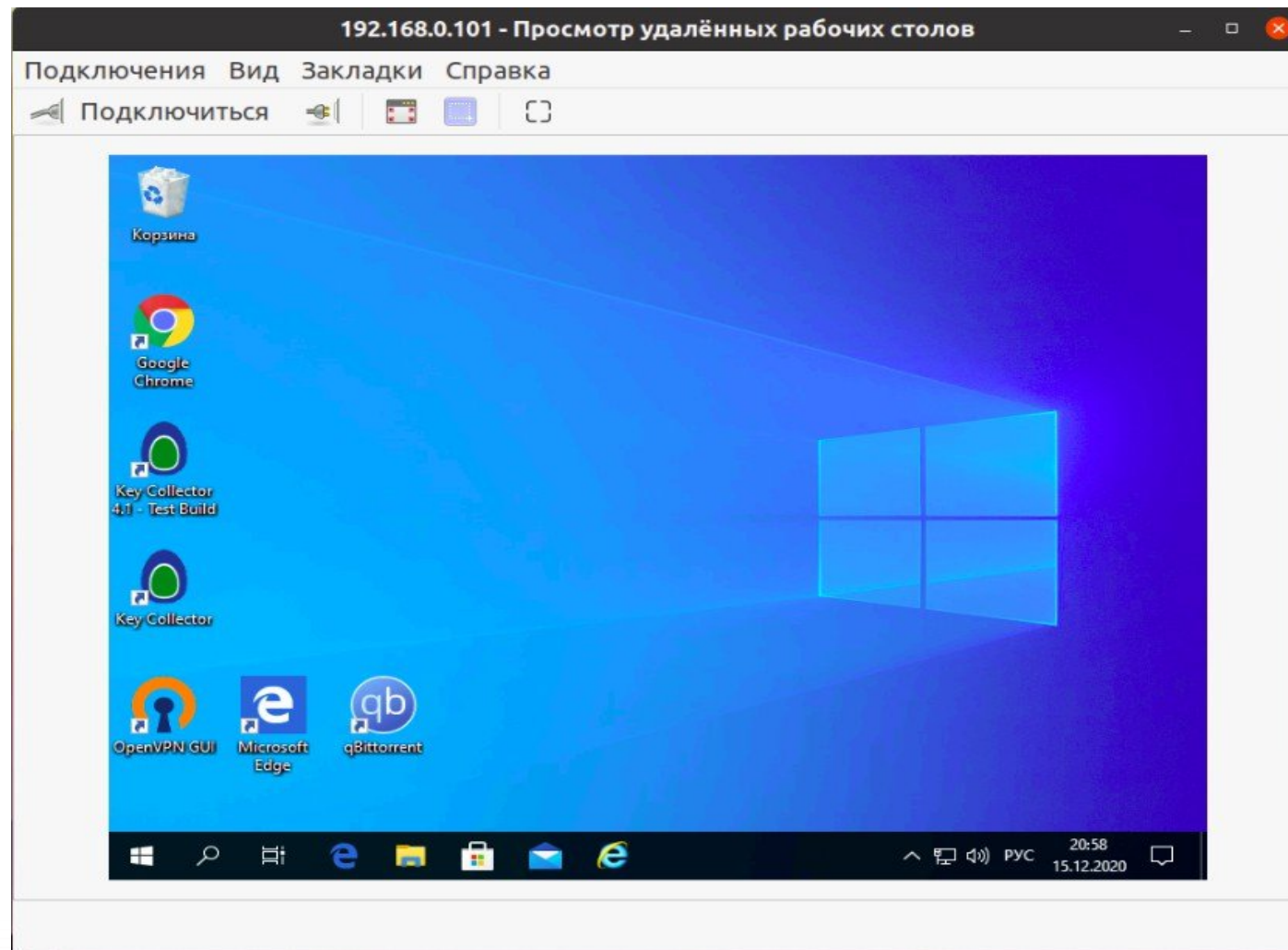
Remmina — клиент удалённого рабочего стола, имеет лицензию GPLv2+. Функционал можно расширять за счёт плагинов.



TigerVNC



VINAGRE - по протоколу VNC





Спасибо за внимание!

www.red-soft.ru
redos@red-soft.ru

