

Шаг 1

```
ln@dc1:/home/redoc202
Файл Правка Вид Поиск Терминал Помощь

[ln@dc1 ~]$ su
Пароль:
[root@dc1 redoc202]# dnf install snap -y
Последняя проверка окончания срока действия метаданных: 0:05:41 назад, Сб 23 дек 2023 09:12:33.
Нет соответствия аргументу: snap
Ошибка: Совпадений не найдено: snap
[root@dc1 redoc202]# dnf install snapd -y
Последняя проверка окончания срока действия метаданных: 0:05:48 назад, Сб 23 дек 2023 09:12:33.
Зависимости разрешены.
=====
Пакет                Архитектура  Версия                Репозиторий  Размер
=====
Установка:
snapd                 x86_64       2.58.3-1.e17         updates      31 М
Установка зависимостей:
snap-confine          x86_64       2.58.3-1.e17         updates      5.3 М
snapd-selinux         noarch       2.58.3-1.e17         updates      36 к
Результат транзакции
=====
Установка 3 Пакета
```

Скачиваем снап

Шаг 2

```
In@dc1:/home/redoc202
Файл Правка Вид Поиск Терминал Помощь
Detected unsafe path transition / → /var during canonicalization of /var/log/jou
rnal/2136fae0e6dd4f48ae820755ae071ab7/system.journal.
Detected unsafe path transition / → /var during canonicalization of /var/log/jou
rnal/2136fae0e6dd4f48ae820755ae071ab7/system.journal.

Проверка      : snap-confine-2.58.3-1.el7.x86_64      1/3
Проверка      : snapd-2.58.3-1.el7.x86_64           2/3
Проверка      : snapd-selinux-2.58.3-1.el7.noarch     3/3

Установлен:
snap-confine-2.58.3-1.el7.x86_64      snapd-2.58.3-1.el7.x86_64
snapd-selinux-2.58.3-1.el7.noarch

Выполнено!
[root@dc1 redoc202]# systemctl enable --now snapd.socket
bash: systemctl: команда не найдена
[root@dc1 redoc202]# systemctl enable --now snapd.socket
bash: systemctl: команда не найдена
[root@dc1 redoc202]# systemctl enable --now snapd.socket
Failed to enable unit: Unit file snapd.socket does not exist.
[root@dc1 redoc202]# systemctl enable --now snapd.socket
Created symlink /etc/systemd/system/sockets.target.wants/snapd.socket → /usr/lib
/systemd/system/snapd.socket.
[root@dc1 redoc202]#
```

Проверка сокета snap

Шаг 3

Включаем поддержку классической привязки

```
ln@dc1:/home/redoc202
Файл Правка Вид Поиск Терминал Помощь
rnal/2136fae0e6dd4f48ae820755ae071ab7/system.journal.
Detected unsafe path transition / → /var during canonicalization of /var/log/jou
rnal/2136fae0e6dd4f48ae820755ae071ab7/system.journal.

Проверка      : snap-confine-2.58.3-1.e17.x86_64      1/3
Проверка      : snapd-2.58.3-1.e17.x86_64           2/3
Проверка      : snapd-selinux-2.58.3-1.e17.noarch    3/3

Установлен:
snap-confine-2.58.3-1.e17.x86_64      snapd-2.58.3-1.e17.x86_64
snapd-selinux-2.58.3-1.e17.noarch

Выполнено!
[root@dc1 redoc202]# systemctl enable --now snapd.socket
bash: systemctl: команда не найдена
[root@dc1 redoc202]# system enable --now snapd.socket
bash: system: команда не найдена
[root@dc1 redoc202]# systemctl enable --now snapd.socket
Failed to enable unit: Unit file snapd.socket does not exist.
[root@dc1 redoc202]# systemctl enable --now snapd.socket
Created symlink /etc/systemd/system/sockets.target.wants/snapd.socket → /usr/lib
/systemd/system/snapd.socket.
[root@dc1 redoc202]# ln -s /var/lib/snapd/snap /snap
[root@dc1 redoc202]# |
```

Шаг 4

Устанавливаем графический редактор гим

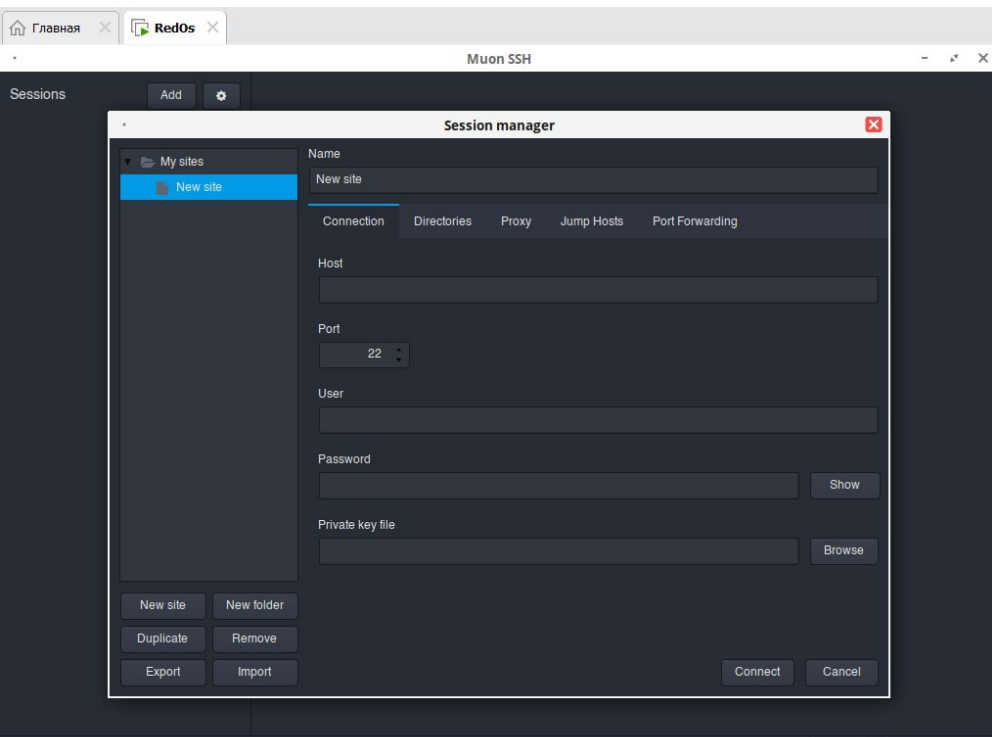
```
ln@dc1:/home/redoc202
Файл Правка Вид Поиск Терминал Помощь
rnal/2136fae0e6dd4f48ae820755ae071ab7/system.journal.
Detected unsafe path transition / → /var during canonicalization of /var/log/jou
rnal/2136fae0e6dd4f48ae820755ae071ab7/system.journal.

Проверка      : snap-confine-2.58.3-1.e17.x86_64      1/3
Проверка      : snapd-2.58.3-1.e17.x86_64           2/3
Проверка      : snapd-selinux-2.58.3-1.e17.noarch    3/3

Установлен:
snap-confine-2.58.3-1.e17.x86_64      snapd-2.58.3-1.e17.x86_64
snapd-selinux-2.58.3-1.e17.noarch

Выполнено!
[root@dc1 redoc202]# systemctl enable --now snapd.socket
bash: systemctl: команда не найдена
[root@dc1 redoc202]# system enable --now snapd.socket
bash: system: команда не найдена
[root@dc1 redoc202]# systemctl enable --now snapd.socket
Failed to enable unit: Unit file snapd.socket does not exist.
[root@dc1 redoc202]# systemctl enable --now snapd.socket
Created symlink /etc/systemd/system/sockets.target.wants/snapd.socket → /usr/lib
/systemd/system/snapd.socket.
[root@dc1 redoc202]# ln -s /var/lib/snapd/snap /snap
[root@dc1 redoc202]# snap install gim
```

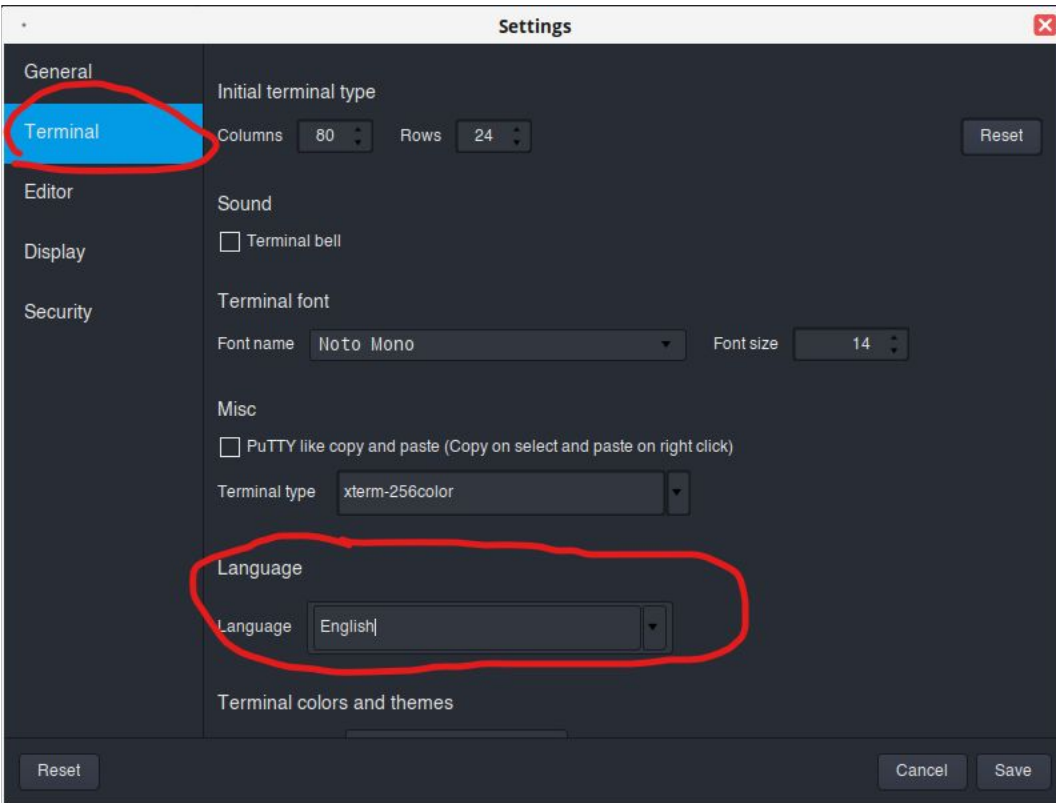
Шаг 5



скачиваем muon

Шаг 6

Ставим английский язык



Шаг 7

Менеджер сессий

Имя
New site

Соединение | Директории | Прокси | Jump Hosts | Переадресация портов

Хост
192.168.207.129

Порт
22

Пользователь
server

Пароль
***** Показать

Файл закрытого ключа
Просмотреть

Новый сайт | Новая папка
Дублировать | Удалить
Экспорт | Импорт | Подключиться | Отмена

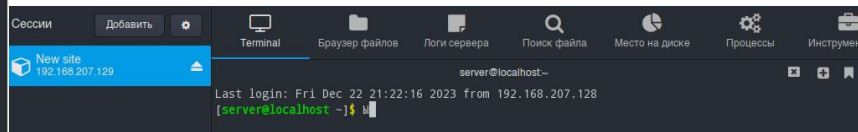
В поле Хост укажите IP-адрес сервера или имя хоста.

В поле Порт укажите номер порта для подключения (по умолчанию используется порт 22).

В поле Пользователь укажите имя пользователя, к учетной записи которого необходимо подключиться.

В поле Пароль укажите пароль от учетной записи указанного выше пользователя. (на redos обязательно должен стоять пароль, чтобы подключиться к терминалу)

В поле Файл закрытого ключа загрузите файл из каталога, в котором хранится закрытый ключ.



Шаг 8

```
ln@dc1: /home/redoc202
Файл Правка Вид Поиск Терминал Помощь

[ln@dc1 ~]$ su
Пароль:
[root@dc1 redoc202]# dns install nmap -y
bash: dns: команда не найдена
[root@dc1 redoc202]# dnf install nmap -y
Последняя проверка окончания срока действия метаданных: 0:28:21 назад, Сб 23 дек 2023 09:21:29.
Зависимости разрешены.
=====
Пакет            Архитектура  Версия            Репозиторий      Размер
=====
Установка:
nmap             x86_64       2:7.80-4.e17      updates          5.8 М
Установка зависимостей:
nmap-ncat        x86_64       2:7.80-4.e17      updates          211 к
Результат транзакции
=====
Установка 2 Пакета

Объем загрузки: 6.0 М
Объем изменений: 24 М
Загрузка пакетов:
(1/2): nmap-ncat-7.80-4.e17.x86_64.rpm      153 kB/s | 211 kB      00:01
[root@dc1 redoc202]# nmap 192.168.207.129 -p 22
```

Устанавливаем nmap и подключаемся к локальному серверу

Шаг 9

```
[root@localhost server]# nmap -sV 192.168.207.129 -p 1-65535 | grep open
22/tcp open  ssh      OpenSSH 8.9 (protocol 2.0)
111/tcp open  rpcbind 2-4 (RPC #100000)
[root@localhost server]# $
```

Данный код,демонстрирует нам, все открытые порты на сетевом узле

```
[root@localhost server]# nmap --open 192.168.207.129
Starting Nmap 7.80 ( https://nmap.org ) at 2023-12-22 22:32 MSK
Nmap scan report for 192.168.207.129
Host is up (0.0000090s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
111/tcp    open  rpcbind

Nmap done: 1 IP address (1 host up) scanned in 0.09 seconds
[root@localhost server]#
```

Возможен вариант с указанием параметра --open

Шаг 10

```
[root@localhost server]# nmap -sn 192.168.207.129/24
Starting Nmap 7.80 ( https://nmap.org ) at 2023-12-22 22:37 MSK
Nmap scan report for 192.168.207.1
Host is up (0.00018s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.207.2
Host is up (0.000095s latency).
MAC Address: 00:50:56:ED:76:BF (VMware)
Nmap scan report for 192.168.207.128
Host is up (0.00058s latency).
MAC Address: 00:0C:29:44:92:B4 (VMware)
Nmap scan report for 192.168.207.254
Host is up (0.000080s latency).
MAC Address: 00:50:56:EC:35:2A (VMware)
Nmap scan report for 192.168.207.129
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.00 seconds
[root@localhost server]# |
```

Сканировать сеть методом ping для обнаружения активных узлов. При этом в выводе команды будут отображаться IP и MAC-адреса.

Шаг 11

```
[root@localhost server]# nmap -sV 192.168.207.129
Starting Nmap 7.80 ( https://nmap.org ) at 2023-12-22 22:39 MSK
Nmap scan report for 192.168.207.129
Host is up (0.0000090s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.9 (protocol 2.0)
111/tcp   open  rpcbind  2-4 (RPC #100000)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.47 seconds
[root@localhost server]#
```

```
[root@localhost server]# nmap -sV -p 22,53 8.8.8.8
Starting Nmap 7.80 ( https://nmap.org ) at 2023-12-22 22:43 MSK
Nmap scan report for dns.google (8.8.8.8)
Host is up (0.0035s latency).

PORT      STATE SERVICE VERSION
22/tcp    filtered ssh
53/tcp    open  tcpwrapped

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.76 seconds
[root@localhost server]#
```

Информация о сетевом узле

Сканирование определенных портов, в примере указаны 22 (ssh) и 53 (dns):

Шаг 12

Сканирование всей подсети

```
[root@localhost server]# nmap 192.168.207.129/24
Starting Nmap 7.80 ( https://nmap.org ) at 2023-12-22 22:47 MSK
Nmap scan report for 192.168.207.1
Host is up (0.00026s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE
7070/tcp  open  realserver
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.207.2
Host is up (0.00063s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
53/tcp    filtered domain
MAC Address: 00:50:56:ED:76:BF (VMware)

Nmap scan report for 192.168.207.128
Host is up (0.0033s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
111/tcp   open  rpcbind
MAC Address: 00:0C:29:44:92:B4 (VMware)

Nmap scan report for 192.168.207.254
Host is up (0.00014s latency).
All 1000 scanned ports on 192.168.207.254 are filtered
MAC Address: 00:50:56:EC:35:2A (VMware)

Nmap scan report for 192.168.207.129
Host is up (0.000010s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
111/tcp   open  rpcbind
```

Шаг 13

Быстрое сканирование открытых портов на всех хостах подсети:

```
[root@localhost server]# nmap -T5 192.168.207.129/24
Starting Nmap 7.80 ( https://nmap.org ) at 2023-12-22 22:52 MSK
Nmap scan report for 192.168.207.1
Host is up (0.00019s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE
7070/tcp  open  realserver
MAC Address: 00:50:56:C0:00:08 (VMware)
```

```
Nmap scan report for 192.168.207.2
Host is up (0.0012s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
53/tcp    filtered domain
MAC Address: 00:50:56:ED:76:BF (VMware)
```

```
Nmap scan report for 192.168.207.128
Host is up (0.0029s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
111/tcp   open  rpcbind
MAC Address: 00:0C:29:44:92:B4 (VMware)
```

```
Nmap scan report for 192.168.207.254
Host is up (0.00036s latency).
All 1000 scanned ports on 192.168.207.254 are filtered
MAC Address: 00:50:56:EC:35:2A (VMware)
```

```
Nmap scan report for 192.168.207.129
Host is up (0.000010s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
111/tcp   open  rpcbind
```


Шаг 14

```
[root@localhost server]# nmap -v -sT -PN --spoof-mac 0 192.168.207.129
Warning: The -PN option is deprecated. Please use -Pn
Starting Nmap 7.80 ( https://nmap.org ) at 2023-12-22 22:53 MSK
Spoofing MAC address B0:36:C6:BF:AE:5E (No registered vendor)
You have specified some options that require raw socket access.
These options will not be honored for TCP Connect scan.
Initiating Parallel DNS resolution of 1 host. at 22:53
Completed Parallel DNS resolution of 1 host. at 22:54, 8.02s elapsed
Initiating Connect Scan at 22:54
Scanning 192.168.207.129 [1000 ports]
Discovered open port 111/tcp on 192.168.207.129
Discovered open port 22/tcp on 192.168.207.129
Completed Connect Scan at 22:54, 0.06s elapsed (1000 total ports)
Nmap scan report for 192.168.207.129
Host is up (0.00030s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
111/tcp   open  rpcbind

Read data files from: /usr/bin/../../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 8.13 seconds
[root@localhost server]# |
```

Сканирование с использованием подмены MAC-адреса, в данном случае одно устройство/приложение маскируется под другое, указывая его MAC-адрес. В данном примере «0» означает, что nmap выберет случайный MAC-адрес.