



Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Московский государственный технический университет
имени Н.Э. Баумана
(национальный исследовательский университет)»
(МГТУ им. Н.Э. Баумана)

ФАКУЛЬТЕТ ИНФОРМАТИКА И СИСТЕМЫ УПРАВЛЕНИЯ

КАФЕДРА КОМПЬЮТЕРНЫЕ СИСТЕМЫ И СЕТИ (ИУ6)

НАПРАВЛЕНИЕ ПОДГОТОВКИ 09.03.01 Информатика и вычислительная техника

О Т Ч Е Т

по лабораторной работе № 7

Название: Исследование способов удалённого управления Windows и Linux

Дисциплина: Операционные системы

Студент

ИУ6-53Б

(Группа)

(Подпись, дата)

В.К. Залыгин

(И.О. Фамилия)

Преподаватель

В.Ю. Мельников

А.М. Суровов

(Подпись, дата)

(И.О. Фамилия)

Москва, 2024

ВВЕДЕНИЕ

Цель лабораторной работы

Цель работы - получение теоретических и практических сведений об удалённом управлении linux и Windows серверами, а так же копирования файлов между Windows и Linux.

Задание

Ознакомиться с теоретической частью, описанной в файле 7 remoteAdmin.pdf выполнить описанные действия, которые возможны с учётом версии Windows и имеющихся прав доступа.

Выполнение

Попытка включить удаленный рабочий стол прошла неуспешно.

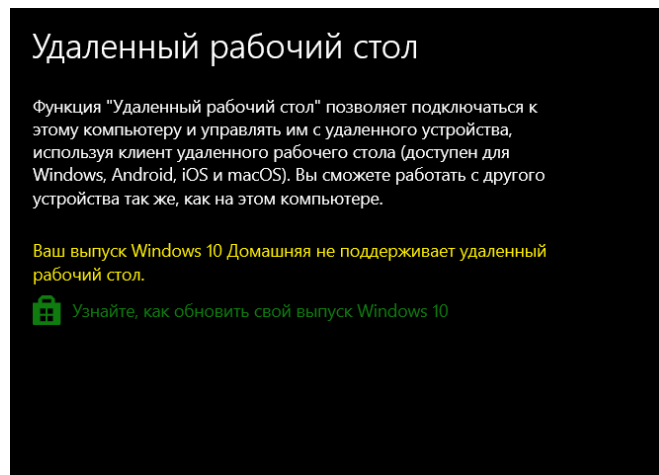


Рисунок 1 – Из-за неподходящей версии операционной системы невозможно включить функцию удаленного рабочего стола

Далее создадим папку и сделаем ее доступной для сетевого использования

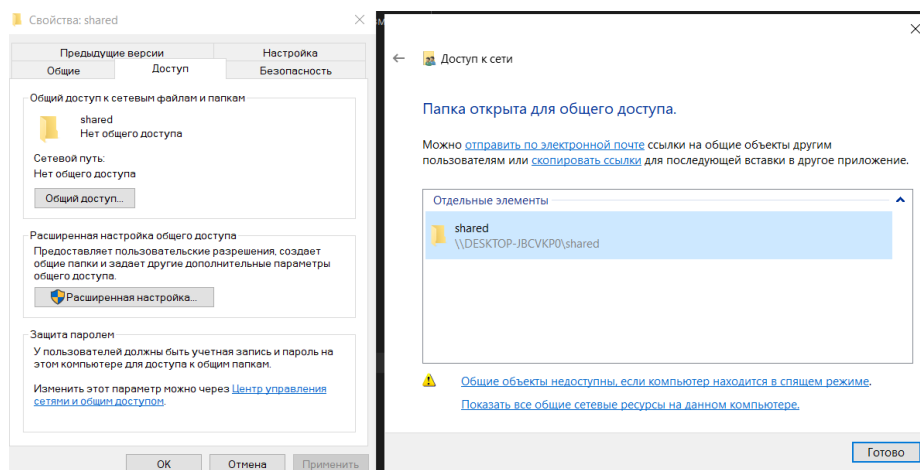


Рисунок 2 – Папка открыта для общего доступа

Попробуем зайти в папку через сеть, указав имя компьютера и папки.

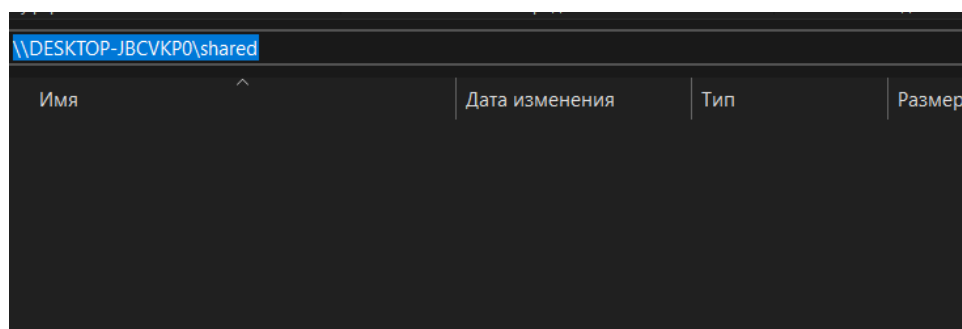


Рисунок 3 – Как выглядит заход в эту папку

Установка сервиса sshd.

```
[root@zalygin ~]# service sshd
sshd.service - OpenSSH server daemon
Loaded: loaded (/lib/systemd/system/sshd.service; enabled; vendor preset: ena
Active: active (running) since Thu 2024-10-17 13:51:53 UTC; 20min ago
Process: 723 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
Process: 720 ExecStartPre=/usr/bin/ssh-keygen -A (code=exited, status=0/SUCCESS)
Main PID: 726 (sshd)
Tasks: 1 (limit: 1162)
Memory: 3.5M
CGroup: /system.slice/sshd.service
└─726 /usr/sbin/sshd -D

Oct 17 13:51:53 zalygin systemd[1]: Starting OpenSSH server daemon...
Oct 17 13:51:53 zalygin systemd[1]: Started OpenSSH server daemon.
[root@zalygin ~]# _
```

Рисунок 4 – После установки sshd проверим, что сервис запущен

Для подключения к хосту по сети можно использовать протокол ssh и одноименную утилиту.

```
[root@zalygin ~]# ssh user@localhost
user@localhost's password:
Last login: Thu Oct 17 14:10:07 2024 from 127.0.0.1
[user@zalygin ~]$_
```

Рисунок 5 – Подключение к хосту через ssh-туннель

С помощью pstree можно проверить, что текущая сессия действительно идет через sshd на удаленной машине.

```
[root@zalygin ~]# pstree
systemd--ModemManager--2*[{ModemManager}]
--NetworkManager--2*[{NetworkManager}]
--acpid
--avahi-daemon--avahi-daemon
--crond
--dbus-daemon
--dhcpcd
--klogd
--login--bash--ssh
--polkitd--5*[{polkitd}]
--sddm--{sddm}
--sshd--sshd--sshd--bash--su--bash--pstree
--syslogd
--2*[systemd--(sd-pam)]
--systemd-journal
--systemd-logind
--systemd-udev
--udisksd--4*[{udisksd}]
--upowerd--2*[{upowerd}]
[root@zalygin ~]# _
```

Рисунок 6 – Дерево процессов, в котором видно, что подключение идет через sshd

Для входа без пароля можно использовать вход по ключу. Для этого создадим пару ключей для аутентификации.

```

[root@zalygin ~]# ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:AzkCUkIjEKjJCg8FtfhIfUGbTetSn0vvqPJisg.j3M/U root@zalygin
The key's randomart image is:
+---[RSA 2048]-----+
|0B+ ... .|
|o++o ..* o|
|++...+o *|
|*+ .. oo .|
|+o. .So|
|. . . o.|
|. . . .|
|...oo+ E o|
|. .=o+o...o|
+---[SHA256]-----+
[root@zalygin ~]# _

```

Рисунок 7 – Сгенерированная пара ключей

Далее скопируем ключи на удаленную машину с помощью команды `ssh-copy-id`.

```

[root@zalygin ~]# ssh-copy-id user@localhost
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/root/.ssh/id_rsa
.pub"
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter
out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompt
ed now it is to install the new keys
user@localhost's password:

Number of key(s) added: 1

Now try logging into the machine, with:  "ssh 'user@localhost'"
and check to make sure that only the key(s) you wanted were added.
[root@zalygin ~]# _

```

Рисунок 8 – Копирование ключей для удаленного пользователя

Для передачи файлов удобно использовать утилиту `scp` (secure cp).

```

[root@zalygin ~]# touch foo.bar
[root@zalygin ~]# echo 'hello!' > foo.bar
[root@zalygin ~]# scp ./foo.bar user@localhost:~/bar.foo
foo.bar                                100%   7      0.0KB/s   00:00
[root@zalygin ~]# ssh user@localhost cat bar.foo
hello!
[root@zalygin ~]#

```

Рисунок 9 – Использование команды `scp` для передачи файлов

Далее используем команду `rsync`, которая позволяет гибко синхронизировать содержимое папок. Ее используем для создания бекапа – точной копии содержимого.

```

root/.ssh/id_rsa      1,679 100%   18.02kB/s   0:00:00 (xfr#29, to-chk=2/42)
root/.ssh/id_rsa.pub  394 100%    4.14kB/s   0:00:00 (xfr#30, to-chk=1/42)
root/.ssh/known_hosts 91 100%    0.95kB/s   0:00:00 (xfr#31, to-chk=0/42)
root/tmp/

Number of files: 42 (reg: 31, dir: 11)
Number of created files: 42 (reg: 31, dir: 11)
Number of deleted files: 0
Number of regular files transferred: 31
Total file size: 101,186 bytes
Total transferred file size: 101,186 bytes
Literal data: 101,186 bytes
Matched data: 0 bytes
File list size: 0
File list generation time: 0.001 seconds
File list transfer time: 0.000 seconds
Total bytes sent: 22,761
Total bytes received: 708

sent 22,761 bytes  received 708 bytes  15,646.00 bytes/sec
total size is 101,186  speedup is 4.31

```

Рисунок 10 – Результат выполнения команды `rsync -vrtplze ssh --progress --stats --delete /root user1@localhost:~/backup`

В команде использованы следующие флаги:

- v – печатать сообщения
- r – обойти директорию рекурсивно
- t – установить время модификации
- p – сохранить права доступа
- l – передавать симлинки как симлинки
- z – передавать в сжатом виде
- e – установить команду для транспорта
- progress – печатать сообщения о прогрессе
- stats – печатать статистику после передачи
- delete – удалить файлы в копируемой директории на удаленной машине,

которые не существуют на исходной машине

Далее настроим общение между хост-машиной и виртуальной машиной.

Для этого необходимо подключить еще один интерфейс к виртуальной машине, чтобы она стала доступна для хост-машины.

```

eth0      Link encap:Ethernet  HWaddr 08:00:27:4D:79:D2
          BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)

eth1      Link encap:Ethernet  HWaddr 08:00:27:7D:28:CF
          inet addr:192.168.56.101  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::3f0c:1a20:96d4:8fc2/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1 errors:0 dropped:0 overruns:0 frame:0
          TX packets:22 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:590 (590.0 b)  TX bytes:4428 (4.3 KiB)

```

Рисунок 11 – Результат добавления нового адаптера, виден IP-адрес

С помощью команды ping на хост-машине проверим, что виртуальная машина доступна.

```

PS C:\Users\viazy> ping 192.168.56.101

Обмен пакетами с 192.168.56.101 по 32 байтами данных:
Ответ от 192.168.56.101: число байт=32 время=1мс TTL=64
Ответ от 192.168.56.101: число байт=32 время=1мс TTL=64
Ответ от 192.168.56.101: число байт=32 время=1мс TTL=64
Ответ от 192.168.56.101: число байт=32 время=1мс TTL=64

Статистика Ping для 192.168.56.101:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 1мсек, Максимальное = 1 мсек, Среднее = 1 мсек
PS C:\Users\viazy>

```

Рисунок 12 – Виртуальная машина доступна с хоста

Для подключения по ключу необходимо скопировать публичный ключ, который будет использован, в файл ~/.ssh/authorized_keys для пользователя, к которому будет подключение.

```

user@zalygin: /home/user
# authorized_keys file format is described in sshd(8) manual page
ssh-ed25519 AAAAC3NzaC11ZDI1NTE5AAAAIINNNM1g/PxEb0gvpeuXBGOG/ey8pMRoUnkoT6UcW1Qd viazy@DESKTOP-JBCVKPQ
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQAC3ogmjFrckVVBWU0zGUG5+813AKxZZL6cDzc1rqsgirbBk0mF5oQ0mE+xvyDbk3hnIxZGGhueuQhj+38X
0qc447TKkuteYgqf3UfDKX0NyhFDCrxNjX2Vi1jMKm9+7pqUYM3r1g6yHbIOLJ78Z8hUayeRysGKA50Rvbye1A/81CaRb76QJKQ8Cb2vgW6/sBQ/Vvudzgjkq
wEV6uI6iDZDzt18rvuPGqho8toAZ0Zpsc8fqW03V23q/CsjC0Rxcotr+ix6POFFVQ1R1+eFqZ1HN/nth6kqjMzaDIxz4iqMd0fm7xHrrw5CGnTikoL/I57y
Giznh/Gx+bD4E+YtTn7 root@zalygin

```

Рисунок 13 – Добавление ключа хоста

При помощи утилиты winscp можно быстро передавать данные между windows и linux машинами.

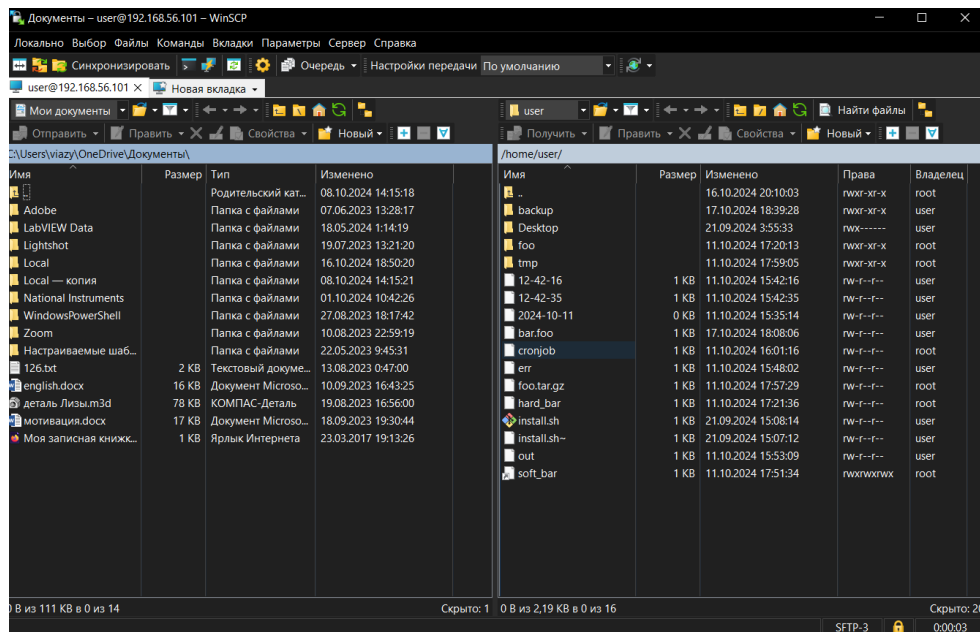


Рисунок 14 – Соединение с виртуальной машиной через WinSCP

После попробуем создать файловый сервер. Для этого будем использовать samba. По методичке создадим файл конфигурации.

```
security = USER
server min protocol = SMB2
server string = Samba Server Version %v
idmap config * : backend = tdb
cups options = raw

[homes]
    browseable = No
    comment = Home Directories
    read only = No

[printers]
    browseable = No
    comment = All Printers
    path = /var/spool/samba
    printable = Yes

[public]
    comment = Common catalog
    guest ok = Yes
    path = /samba/public

[root@zalygin ~]#
```

Рисунок 15 – Конфигурация для Samba успешно распознана

Попробуем подключиться и из-за политик безопасности windows запрещает такие подключения.

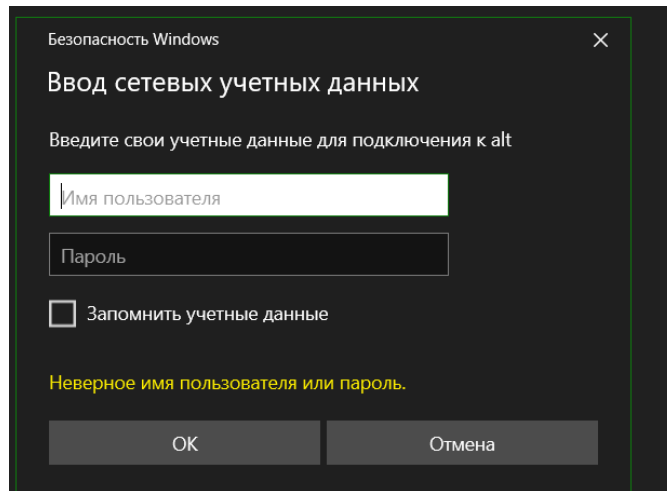


Рисунок 16 – Однако анонимное подключение к общим папкам запрещено
Доконфигурируем samba для создания еще нескольких папок.

```
[global]
netbios name = alt
server role = standalone server
unix password sync = yes
ntlm auth = yes
client ntlmv2 auth = yes
map to guest = bad user

[homes]
comment = Home dirs
browseable = no
writable = yes
valid users = %S
create mask = 0700
directory mask = 0700
valid users = MYDOMAIN\%S

[public]
comment = Common dir
path = /samba/public
guest ok = yes
read only = yes

[exchange]
path = /var/exchange
valid users = @exchange_group
force group = exchange_group
create mask = 0700
directory mask = 0770
_writable = yes
```

Рисунок 17 – Конфигурация сервиса Samba

После применения конфигурации подключение к хосту прошло успешно.
Отображаются настроенные папки.

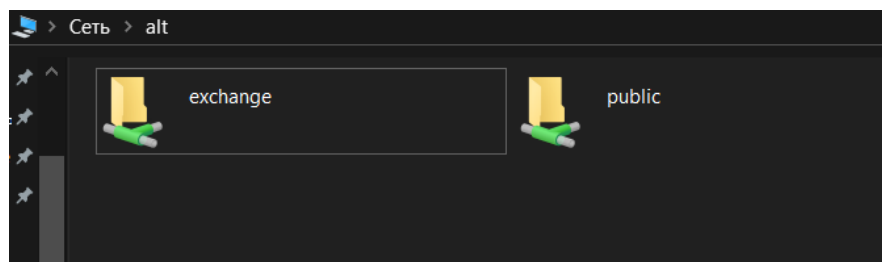


Рисунок 18 – Подключение к удаленной папке [\\alt](#)

Используя smbclient попробуем получить доступ к сетевым папкам хост-машины. Для этого необходимо создать нового пользователя на хост-машине.

```
[root@zalygin ~]# smbclient -U samba-user -L //DESKTOP-JBCVKP0
Enter WORKGROUP\samba-user's password:

      Sharename      Type      Comment
      -----
      ADMIN$         Disk      # Admin
      C$              Disk      #
      D$              Disk      #
      IPC$           IPC       # IPC
      shared         Disk
Reconnecting with SMB1 for workgroup listing.
protocol negotiation failed: NT_STATUS_CONNECTION_RESET
Failed to connect with SMB1 -- no workgroup available
```

Рисунок 19 – Просмотр из Linux сетевых папок Windows

Попробуем подключиться к удаленной папке.

```
[root@zalygin ~]# smbclient -U samba-user //DESKTOP-JBCVKP0/shared
Enter WORKGROUP\samba-user's password:
Try "help" to get a list of possible commands.
smb: \>
```

Рисунок 20 – Подключение к папке Shared

Подключение удалось. Попробуем создать папку.

```
smb: \> mkdir xxx
NT_STATUS_ACCESS_DENIED making remote directory \xxx
```

Рисунок 21 – К сожалению, создать директорию не удалось

К сожалению, что-то пошло не так. Попробуем примонтировать сетевую папку windows.

```
[root@zalygin ~]# mount -t cifs -o user=samba-user,password=1234,workgroup=WORKGROUP,ioccharset=utf8 //192.168.1.76/exchange /mnt/exchange
mount error(2): No such file or directory
Refer to the mount.cifs(8) manual page (e.g. man mount.cifs)
[root@zalygin ~]#
```

Рисунок 22 – Монтирование удаленной директории тоже не вышло

Были использованы следующие опции:

- t – тип файловой системы
- o – параметры монтирования

ЗАКЛЮЧЕНИЕ

В результате выполнения работы были получены теоретические и практические сведения об удалённом управлении linux и Windows серверами, а также копирования файлов между Windows и Linux.