

Отчёт по лабораторной работе №14

Администрирование сетевых подсистем

Ищенко Ирина НПИбд-02-22

Содержание

1	Цель работы	5
2	Выполнение лабораторной работы	6
3	Выводы	16
4	Ответы на контрольные вопросы	17

Список иллюстраций

2.1	Создание группы и разделяемого ресурса	6
2.2	Редактирование файла конфигурации <code>/etc/samba/smb.conf</code>	7
2.3	Запуск демона и просмотр статуса	8
2.4	Проверка доступа к общему ресурсу	8
2.5	Просмотр файла конфигурации межсетевого экрана для Samba . .	8
2.6	Изменение межсетевого экрана, создание файла на разделяемом ресурсе, добавление пользователя в базу Samba	9
2.7	Просмотр файла конфигурации межсетевого экрана для клиента Samba	10
2.8	Настройка межсетевого экрана на клиенте, создание группы и добавление пользователя	10
2.9	Изменение параметра	11
2.10	Проверка наличия общего доступа под разными пользователями .	12
2.11	Создание точки монтирования, проверка записи файлов на разделяемом ресурсе пользователем, отмонтирование каталога	12
2.12	Редактирование файла <code>/etc/samba/smbusers</code>	12
2.13	Редактирование <code>/etc/fstab</code> на клиенте	13
2.14	Монтирование общего ресурса и проверка	13
2.15	Проверка доступа к разделяемым ресурсам после перезагрузки . .	13
2.16	Проверка доступа к разделяемым ресурсам после перезагрузки . .	14

Список таблиц

1 Цель работы

Приобретение навыков настройки доступа групп пользователей к общим ресурсам по протоколу SMB.

2 Выполнение лабораторной работы

На сервере устанавливаю необходимые пакеты:

```
dnf -y install samba samba-client cifs-utils
```

Создаю группу sambagroup для пользователей, которые будут работать с Samba-сервером с GID 1010, добавляю пользователя ioithenko к группе. Создаю общий каталог в файловой системе Linux, в который предполагается монтировать разделяемые ресурсы(рис. 2.1).

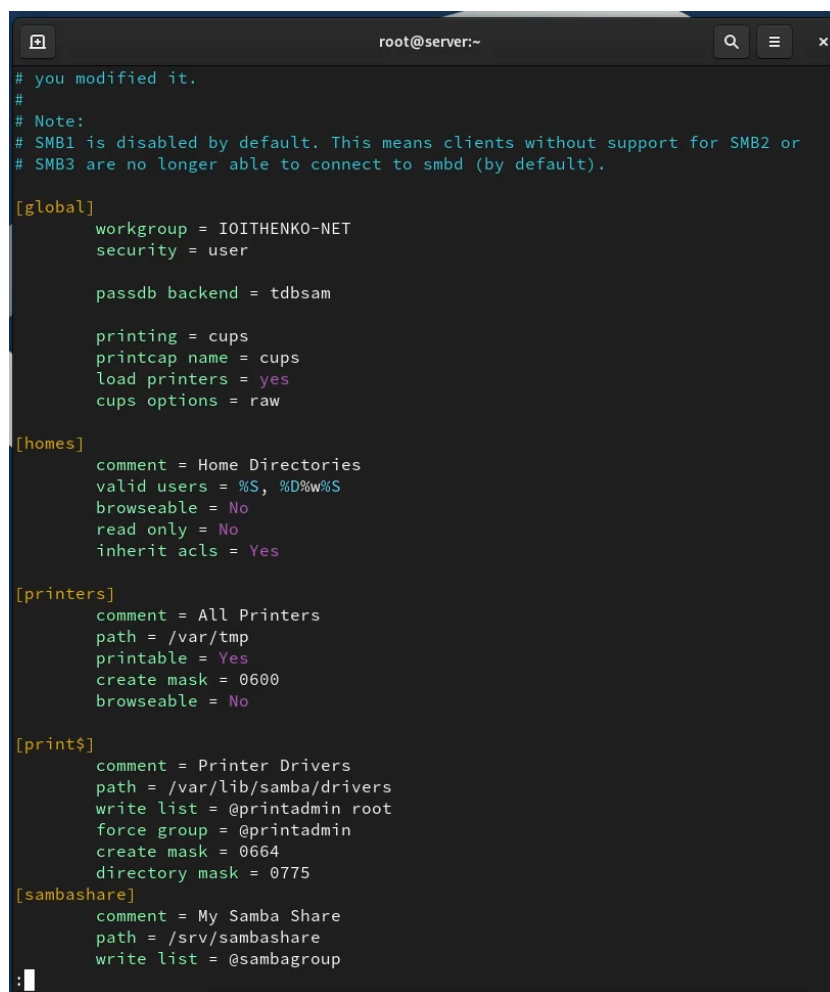
```
[root@server.ioithenko.net ~]# groupadd -g 1010 sambagroup
[root@server.ioithenko.net ~]# usermod -aG sambagroup ioithenko
[root@server.ioithenko.net ~]# mkdir -p /srv/smbashare
[root@server.ioithenko.net ~]# vi /etc/samba/smb.conf
[root@server.ioithenko.net ~]# testparm
Load smb config files from /etc/samba/smb.conf
Loaded services file OK.
Weak crypto is allowed by GnuTLS (e.g. NTLM as a compatibility fallback)

Server role: ROLE_STANDALONE

Press enter to see a dump of your service definitions
```

Рис. 2.1: Создание группы и разделяемого ресурса

В файле конфигурации /etc/samba/smb.conf вношу изменения, изменив параметр рабочей группы и добавив раздел с описанием общего доступа к разделяемому ресурсу (рис. 2.2).

A terminal window titled 'root@server:~' with search, menu, and close icons in the title bar. The terminal displays the contents of the /etc/samba/smb.conf file. The text is as follows:

```
# you modified it.
#
# Note:
# SMB1 is disabled by default. This means clients without support for SMB2 or
# SMB3 are no longer able to connect to smbd (by default).

[global]
    workgroup = IOITHENKO-NET
    security = user

    passdb backend = tdbsam

    printing = cups
    printcap name = cups
    load printers = yes
    cups options = raw

[homes]
    comment = Home Directories
    valid users = %S, %D%w%S
    browseable = No
    read only = No
    inherit acls = Yes

[printers]
    comment = All Printers
    path = /var/tmp
    printable = Yes
    create mask = 0600
    browseable = No

[print$]
    comment = Printer Drivers
    path = /var/lib/samba/drivers
    write list = @printadmin root
    force group = @printadmin
    create mask = 0664
    directory mask = 0775

[smbashare]
    comment = My Samba Share
    path = /srv/smbashare
    write list = @sambagroup
```

Рис. 2.2: Редактирование файла конфигурации /etc/samba/smb.conf

С помощью `testparm` проверяю, нет ли ошибок в файле. Запускаю демон Samba и просматриваю статус. Проверяю доступ к общему ресурсу (рис. 2.3 и 2.4).

```
[root@server.ioithenko.net ~]# systemctl start smb
[root@server.ioithenko.net ~]# systemctl enable smb
Created symlink /etc/systemd/system/multi-user.target.wants/smb.service → /usr/lib/systemd/system/smb.service.
[root@server.ioithenko.net ~]# systemctl status smb
● smb.service - Samba SMB Daemon
   Loaded: loaded (/usr/lib/systemd/system/smb.service; enabled; preset: disabled)
   Active: active (running) since Sat 2024-11-30 12:30:03 UTC; 16s ago
     Docs: man:smbd(8)
           man:samba(7)
           man:smb.conf(5)
  Main PID: 10613 (smbd)
    Status: "smbd: ready to serve connections..."
     Tasks: 3 (limit: 4555)
    Memory: 13.4M
       CPU: 159ms
    CGroup: /system.slice/smb.service
            └─10613 /usr/sbin/smbd --foreground --no-process-group
              └─10615 /usr/sbin/smbd --foreground --no-process-group
                └─10616 /usr/sbin/smbd --foreground --no-process-group

Nov 30 12:30:02 server.ioithenko.net systemd[1]: Starting Samba SMB Daemon...
Nov 30 12:30:02 server.ioithenko.net smbd[10613]: [2024/11/30 12:30:02.940206, s
Nov 30 12:30:02 server.ioithenko.net smbd[10613]:   smbd version 4.20.2 started.
Nov 30 12:30:02 server.ioithenko.net smbd[10613]:   Copyright Andrew Tridgell a
Nov 30 12:30:03 server.ioithenko.net systemd[1]: Started Samba SMB Daemon.
lines 1-21/21 (END)
```

Рис. 2.3: Запуск демона и просмотр статуса

```
[root@server.ioithenko.net ~]# smbclient -L //server
Password for [IOITHENKO-NET\root]:
Anonymous login successful

      Sharename      Type      Comment
      -----
      print$         Disk      Printer Drivers
      sambashare     Disk      My Samba Share
      IPC$           IPC       IPC Service (Samba 4.20.2)

SMB1 disabled -- no workgroup available
[root@server.ioithenko.net ~]#
```

Рис. 2.4: Проверка доступа к общему ресурсу

Просматриваю файл конфигурации межсетевого экрана для Samba (рис. 2.5)

```
<?xml version="1.0" encoding="utf-8"?>
<service>
  <short>Samba</short>
  <description>This option allows you to access and participate in Windows file
and printer sharing networks. You need the samba package installed for this opti
on to be useful.</description>
  <include service="samba-client"/>
  <port protocol="tcp" port="139"/>
  <port protocol="tcp" port="445"/>
</service>
/usr/lib/firewalld/services/samba.xml (END)
```

Рис. 2.5: Просмотр файла конфигурации межсетевого экрана для Samba

Настраиваю межсетевой экран, права доступа для каталога с разделяемым ресурсом, просматриваю и изменяю контекст безопасности. Разрешаю экспортировать разделяемые ресурсы для чтения и записи и просматриваю id пользователя.

Под пользователем `io1thenko` создаю файл на разделяемом ресурсе. Добавляю пользователя в базу пользователей Samba (рис. 2.6).

```
[root@server:~]# firewall-cmd --add-service=samba
success
[root@server.ioithenko.net ~]# firewall-cmd --add-service=samba --permanent
success
[root@server.ioithenko.net ~]# firewall-cmd --reload
success
[root@server.ioithenko.net ~]# chgrp sambagroup /srv/sambashare
[root@server.ioithenko.net ~]# chmod g=rwx /srv/sambashare
[root@server.ioithenko.net ~]# cd /srv
[root@server.ioithenko.net srv]# ls -Z
unconfined_u:object_r:nfs_t:s0 nfs unconfined_u:object_r:var_t:s0 sambashare
[root@server.ioithenko.net srv]# semanage fcontext -a -t samba_share_t "/srv/sam
bashare(/.*)?"
[root@server.ioithenko.net srv]# restorecon -vR /srv/sambashare
Relabeled /srv/sambashare from unconfined_u:object_r:var_t:s0 to unconfined_u:ob
ject_r:samba_share_t:s0
[root@server.ioithenko.net srv]# ls -Z
unconfined_u:object_r:nfs_t:s0 nfs
unconfined_u:object_r:samba_share_t:s0 sambashare
[root@server.ioithenko.net srv]# setsebool samba_export_all_rw 1
[root@server.ioithenko.net srv]# setsebool samba_export_all_rw 1 -P
[root@server.ioithenko.net srv]# su ioithenko
[ioithenko@server.ioithenko.net srv]$ uid
bash: uid: command not found...

[ioithenko@server.ioithenko.net srv]$
[ioithenko@server.ioithenko.net srv]$ ^C
[ioithenko@server.ioithenko.net srv]$ id
uid=1001(ioithenko) gid=1001(ioithenko) groups=1001(ioithenko),10(wheel),1010(sa
mbagroup) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[ioithenko@server.ioithenko.net srv]$ cd /srv/sambashare
[ioithenko@server.ioithenko.net sambashare]$ touch ioithenko@server.txt
[ioithenko@server.ioithenko.net sambashare]$ ls
ioithenko@server.txt
[ioithenko@server.ioithenko.net sambashare]$ smbpasswd -L -a ioithenko
smbpasswd -L can only be used by root.
[ioithenko@server.ioithenko.net sambashare]$ sudo -i
[sudo] password for ioithenko:
[root@server.ioithenko.net ~]# smbpasswd -L -a ioithenko
New SMB password:
Retype new SMB password:
Added user ioithenko.
[root@server.ioithenko.net ~]#
```

Рис. 2.6: Изменение межсетевого экрана, создание файла на разделяемом ресурсе, добавление пользователя в базу Samba

На клиенте устанавливаю необходимые пакеты:

```
dnf -y install samba-client cifs-utils
```

Просматриваю файл конфигурации межсетевого экрана для клиента Samba (рис. 2.7).

```
<?xml version="1.0" encoding="utf-8"?>
<service>
  <short>Samba Client</short>
  <description>This option allows you to access Windows file and printer sharing
  networks. You need the samba-client package installed for this option to be use
  ful.</description>
  <include service="netbios-ns"/>
  <port protocol="udp" port="138"/>
</service>
/usr/lib/firewalld/services/samba-client.xml (END)
```

Рис. 2.7: Просмотр файла конфигурации межсетевого экрана для клиента Samba

На клиенте настраиваю межсетевой экран и создаю группу sambagroup, куда добавляю своего пользователя (рис. 2.8).

```
[root@client.ioithenko.net ~]# firewall-cmd --add-service=samba-client
success
[root@client.ioithenko.net ~]# firewall-cmd --add-service=samba-client --permane
nt
usage: 'firewall-cmd --help' for usage information or see firewall-cmd(1) man pa
ge
firewall-cmd: error: unrecognized arguments: --permament
[root@client.ioithenko.net ~]# firewall-cmd --add-service=samba-client --permane
nt
success
[root@client.ioithenko.net ~]# firewall-cmd --reload
success
[root@client.ioithenko.net ~]# groupadd -g 1010 sambagroup
[root@client.ioithenko.net ~]# usermod -aG sambagroup ioithenko
[root@client.ioithenko.net ~]#
```

Рис. 2.8: Настройка межсетевого экрана на клиенте, создание группы и добавление пользователя

На клиенте в файле конфигурации /etc/samba/smb.conf изменяю параметр рабочей группы (рис. 2.9).

A terminal window titled 'root@client:~' showing the configuration of the smb.conf file. The window has a dark background with light-colored text. The configuration is divided into sections: [global], [homes], [printers], and [print\$]. The [global] section sets workgroup to IOITHENKO-NET, security to user, and passdb backend to tdbsam. The [homes] section sets comment to Home Directories, valid users to %S, %D%w%S, browseable to No, read only to No, and inherit acls to Yes. The [printers] section sets comment to All Printers, path to /var/tmp, printable to Yes, create mask to 0600, and browseable to No. The [print\$] section sets comment to Printer Drivers, path to /var/lib/samba/drivers, write list to @printadmin root, force group to @printadmin, create mask to 0664, and directory mask to 0775. The cursor is at the end of the last line.

```
# See smb.conf.example for a more detailed config file or
# read the smb.conf manpage.
# Run 'testparm' to verify the config is correct after
# you modified it.
#
# Note:
# SMB1 is disabled by default. This means clients without support for SMB2 or
# SMB3 are no longer able to connect to smbd (by default).

[global]
    workgroup = IOITHENKO-NET
    security = user

    passdb backend = tdbsam

    printing = cups
    printcap name = cups
    load printers = yes
    cups options = raw

[homes]
    comment = Home Directories
    valid users = %S, %D%w%S
    browseable = No
    read only = No
    inherit acls = Yes

[printers]
    comment = All Printers
    path = /var/tmp
    printable = Yes
    create mask = 0600
    browseable = No

[print$]
    comment = Printer Drivers
    path = /var/lib/samba/drivers
    write list = @printadmin root
    force group = @printadmin
    create mask = 0664
    directory mask = 0775

:wq
```

Рис. 2.9: Изменение параметра

Для проверки наличия общего доступа пытаюсь с клиента подключиться к серверу с помощью smbclient. По умолчанию ресурсы просматриваются под анонимной учетной записью. Подключаюсь под учетной записью своего пользо-вателя (рис. 2.10).

```
[root@client.ioithenko.net ~]# smbclient -L //server
Password for [IOITHENKO-NET\root]:
Anonymous login successful

      Sharename      Type      Comment
      -----
      print$         Disk      Printer Drivers
      sambashare     Disk      My Samba Share
      IPC$           IPC       IPC Service (Samba 4.20.2)
SMB1 disabled -- no workgroup available
[root@client.ioithenko.net ~]#
[root@client.ioithenko.net ~]# smbclient -L //server -U ioithenko
Password for [IOITHENKO-NET\ioithenko]:

      Sharename      Type      Comment
      -----
      print$         Disk      Printer Drivers
      sambashare     Disk      My Samba Share
      IPC$           IPC       IPC Service (Samba 4.20.2)
      ioithenko      Disk      Home Directories
SMB1 disabled -- no workgroup available
[root@client.ioithenko.net ~]#
```

Рис. 2.10: Проверка наличия общего доступа под разными пользователями

Создаю на клиенте точку монтирования, получаю доступ к общему ресурсу с помощью mount, проверяю, что пользователь может записывать файлы на разделяемом ресурсе (рис. 2.11).

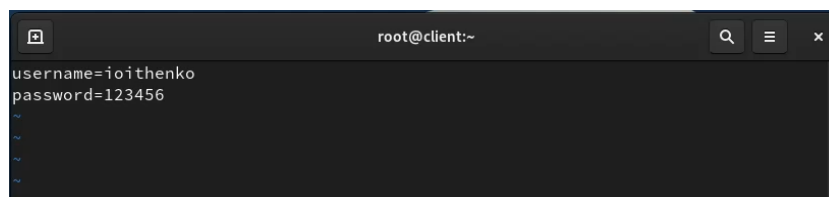
```
[root@client.ioithenko.net ~]# mkdir /mnt/samba
[root@client.ioithenko.net ~]# mount -o username=ioithenko,user,rw,uid=ioithenko,
gid=sambagroup //server/sambashare /mnt/samba
Password for ioithenko@//server/sambashare:
mount: (hint) your fstab has been modified, but systemd still uses
the old version; use 'systemctl daemon-reload' to reload.
[root@client.ioithenko.net ~]# su ioithenko
[ioithenko@client.ioithenko.net root]$ cd /mnt/samba
[ioithenko@client.ioithenko.net samba]$ touch ioithenko@client.txt
```

Рис. 2.11: Создание точки монтирования, проверка записи файлов на разделяемом ресурсе пользователем, отмонтирование каталога

После чего отмонтирую каталог /mnt/samba командой:

`umount /mnt/samba`

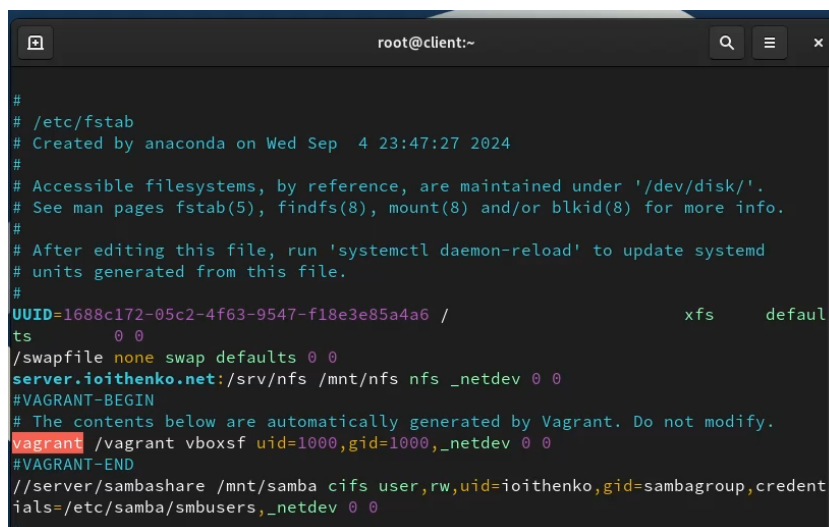
Для настройки работы с Samba с помощью файла учётных данных создаю файл smbusers (рис. 2.12).



```
root@client:~
username=ioithenko
password=123456
~
~
~
~
```

Рис. 2.12: Редактирование файла /etc/samba/smbusers

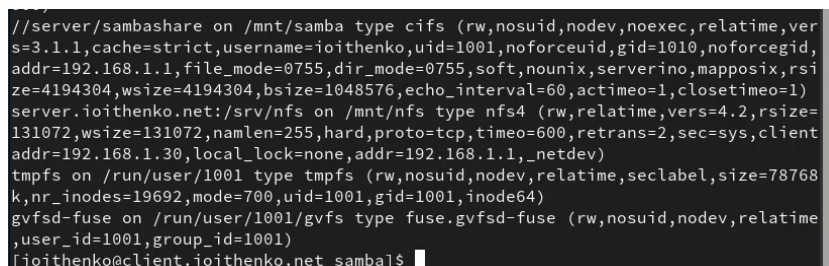
На клиенте в файле `/etc/fstab` добавляю строку (рис. 2.13)



```
root@client:~  
#  
# /etc/fstab  
# Created by anaconda on Wed Sep  4 23:47:27 2024  
#  
# Accessible filesystems, by reference, are maintained under '/dev/disk/'.  
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info.  
#  
# After editing this file, run 'systemctl daemon-reload' to update systemd  
# units generated from this file.  
#  
UUID=1688c172-05c2-4f63-9547-f18e3e85a4a6 /                    xfs     default  
ts          0 0  
/swapfile none swap defaults 0 0  
server.ioithenko.net:/srv/nfs /mnt/nfs nfs _netdev 0 0  
#VAGRANT-BEGIN  
# The contents below are automatically generated by Vagrant. Do not modify.  
vagrant /vagrant vboxsf uid=1000,gid=1000,_netdev 0 0  
#VAGRANT-END  
//server/smbashare /mnt/samba cifs user,rw,uid=ioithenko,gid=sambagroup,credentials=/etc/samba/smbusers,_netdev 0 0
```

Рис. 2.13: Редактирование `/etc/fstab` на клиенте

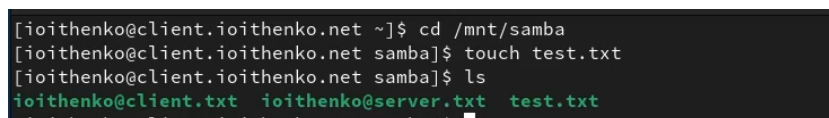
Монтирую общий ресурс: `mount -a`. Убеждаюсь, что ресурс монтируется (рис. 2.14).



```
//server/smbashare on /mnt/samba type cifs (rw,nosuid,nodev,noexec,relatime,vers=3.1.1,cache=strict,username=ioithenko,uid=1001,noforceuid,gid=1010,noforcegid,addr=192.168.1.1,file_mode=0755,dir_mode=0755,soft,nounix,serverino,mapposix,rsize=4194304,wsz=4194304,bsize=1048576,echo_interval=60,actimeo=1,closetimeo=1)  
server.ioithenko.net:/srv/nfs on /mnt/nfs type nfs4 (rw,relatime,vers=4.2,rsize=131072,wsz=131072,namlen=255,hard,proto=tcp,timeo=600,retrans=2,sec=sys,clientaddr=192.168.1.30,local_lock=none,addr=192.168.1.1,_netdev)  
tmpfs on /run/user/1001 type tmpfs (rw,nosuid,nodev,relatime,seclabel,size=78768k,nr_inodes=19692,mode=700,uid=1001,gid=1001,inode64)  
gvfsd-fuse on /run/user/1001/gvfs type fuse.gvfsd-fuse (rw,nosuid,nodev,relatime,user_id=1001,group_id=1001)  
[ioithenko@client.ioithenko.net samba]$
```

Рис. 2.14: Монтирование общего ресурса и проверка

Перезагружаю клиента и убеждаюсь, что у пользователя есть доступ к разделяемым ресурсам и после перезагрузки (рис. 2.15 и 2.16).



```
[ioithenko@client.ioithenko.net ~]$ cd /mnt/samba  
[ioithenko@client.ioithenko.net samba]$ touch test.txt  
[ioithenko@client.ioithenko.net samba]$ ls  
ioithenko@client.txt ioithenko@server.txt test.txt
```

Рис. 2.15: Проверка доступа к разделяемым ресурсам после перезагрузки

```
[root@client.ioithenko.net samba]# cd
[root@client.ioithenko.net samba]# smbclient -L //server -U ioithenko
Password for [IOITHENKO-NET\ioithenko]:

      Sharename      Type      Comment
      -----
      print$         Disk      Printer Drivers
      sambashare      Disk      My Samba Share
      IPC$            IPC       IPC Service (Samba 4.20.2)
      ioithenko       Disk      Home Directories
SMB1 disabled -- no workgroup available
[root@client.ioithenko.net samba]#
```

Рис. 2.16: Проверка доступа к разделяемым ресурсам после перезагрузки

На VM server перехожу в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/ и копирую в соответствующие каталоги конфигурационные файлы:

```
cd /vagrant/provision/server
mkdir -p /vagrant/provision/server/smb/etc/samba
cp -R /etc/samba/smb.conf /vagrant/provision/server/smb/etc/samba/
```

Вношу изменения в файл /vagrant/provision/server/smb.sh.

На VM client перехожу в каталог для внесения изменений в настройки внутреннего окружения и копирую в соответствующие каталоги конфигурационные файлы:

```
cd /vagrant/provision/client
mkdir -p /vagrant/provision/client/smb/etc/samba
cp -R /etc/samba/smb.conf /vagrant/provision/client/smb/etc/samba/
cp -R /etc/samba/smbusers /vagrant/provision/client/smb/etc/samba/
```

Создаю и редактирую скрипт /vagrant/provision/client/smb.sh.

Для отработки созданных скриптов во время загрузки виртуальных машин server и client в конфигурационном файле Vagrantfile добавляю записи в соответствующих разделах конфигураций для сервера и клиента:

```
server.vm.provision "SMB server",
  type: "shell",
```

```
    preserve_order: true,  
    path: "provision/server/smb.sh"  
client.vm.provision "SMB client",  
    type: "shell",  
    preserve_order: true,  
    path: "provision/client/smb.sh"
```

3 Выводы

В ходе выполнения лабораторной работы я приобрела навыки настройки доступа групп пользователей к общим ресурсам по протоколу SMB.

4 Ответы на контрольные вопросы

1. Какова минимальная конфигурация для `smb.conf` для создания общего ресурса, который предоставляет доступ к каталогу `/data`?

Минимальная конфигурация для `smb.conf` может включать следующие параметры:

```
[data]
path = /data
browsable = yes
read only = no
```

2. Как настроить общий ресурс, который даёт доступ на запись всем пользователям, имеющим права на запись в файловой системе Linux?

Для этого нужно установить параметр `read only = no`. Пример:

```
[data]
path = /data
browsable = yes
read only = no
```

3. Как ограничить доступ на запись к ресурсу только членам определённой группы?

Используйте параметр `write list`. Пример:

```
[data]
path = /data
browsable = yes
read only = yes
write list = @groupname
```

4. Какой переключатель SELinux нужно использовать, чтобы позволить пользователям получать доступ к домашним каталогам на сервере через SMB?

Необходимо включить переключатель `samba_enable_home_dirs` с помощью команды `setsebool -P samba_enable_home_dirs on`.

5. Как ограничить доступ к определённому ресурсу только узлам из сети 192.168.10.0/24?

Используйте параметр `hosts allow`. Пример:

```
[data]
path = /data
browsable = yes
read only = no
hosts allow = 192.168.10.
```

6. Какую команду можно использовать, чтобы отобразить список всех пользователей Samba на сервере?

Для этого используется команда `pdbedit -L`.

7. Что нужно сделать пользователю для доступа к ресурсу, который настроен как многопользовательский ресурс?

Пользователю необходимо иметь учётную запись Samba и соответствующие права доступа к ресурсу.

8. Как установить общий ресурс Samba в качестве многопользовательской учётной записи, где пользователь alice используется как минимальная учётная запись пользователя?

Для этого используется параметр `force user = alice`.

9. Как можно запретить пользователям просматривать учётные данные монтирования Samba в файле `/etc/fstab`?

Для этого используется параметр `credentials`, который позволяет хранить учётные данные в отдельном файле с ограниченным доступом. В файле `/etc/fstab` можно указать:

```
/mountpoint smbfs credentials=/path/to/credentials_file 0 0
```

Файл с учётными данными должен быть доступен только владельцу: `chmod 600 /path/to/credentials_file`

10. Какая команда позволяет перечислить все экспортируемые ресурсы Samba, доступные на определённом сервере?

Для этого используется команда `smbclient` с параметром `-L` и указанием имени сервера: `smbclient -L //server_address -U username`