

Отчёт по лабораторной работе №14

Дисциплина: Администрирование сетевых подсистем

Мишина Анастасия Алексеевна

Содержание

1 Цель работы	5
2 Выполнение лабораторной работы	6
2.1 Настройка сервера Samba	6
2.2 Монтирование файловой системы Samba на клиенте . . .	11
2.3 Внесение изменений в настройки внутреннего окружения виртуальных машины	17
3 Контрольные вопросы	21
4 Выводы	24

Список иллюстраций

2.1	Создание группы sambagroup, добавление к ней пользователя и создание каталога	6
2.2	Добавление конфигураций в файл /etc/samba/smb.conf	7
2.3	Запуск samba и просмотр статуса	8
2.4	Подключение к серверу с помощью smbclient	8
2.5	Файл конфигурации межсетевого экрана для Samba	9
2.6	Настройка межсетевого экрана и прав доступа для каталога с разделяемым ресурсом	9
2.7	Настройка контекста безопасности SELinux	10
2.8	Просмотр UID нашего пользователя	10
2.9	Создание файла на разделяемом ресурсе	10
2.10	Добавление пользователя в базу пользователей Samba	10
2.11	Настройка межсетевого экрана, создание группы и добавление в неё пользователя на клиенте	11
2.12	Изменение параметра рабочей группы на клиенте	12
2.13	Проверка наличия общего доступа	13
2.14	Подключение под записью пользователя	14
2.15	Получение доступа к общему ресурсу с клиента	14
2.16	Создание файла на разделяемом ресурсе с клиента	14
2.17	Создание файла учётных данных	15
2.18	Внесение содержимого в файл smbusers	15
2.19	Добавление записи в файл /etc/fstab	16
2.20	Монтирование общего ресурса	16
2.21	Проверка доступа к разделяемым ресурсам после перезапуска клиента	16
2.22	Скрипта файла /vagrant/provision/server/smb.sh	18
2.23	Скрипта файла /vagrant/provision/client/smb.sh	19

Список таблиц

1 Цель работы

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

2 Выполнение лабораторной работы

2.1 Настройка сервера Samba

Запустим VM server. На сервере установим необходимые пакеты: dnf -y install samba samba-client cifs-utils.

Создадим группу sambagroup для пользователей, которые будут работать с Samba-сервером, и присвоим ей GID 1010 с помощью команды groupadd -g 1010 sambagroup. Затем добавим пользователя aamishina к группе sambagroup командой usermod -aG sambagroup user. И создадим общий каталог в файловой системе Linux, в который предполагается монтировать разделяемые ресурсы:(рис. fig. 2.1):

```
[root@server.aamishina.net ~]# groupadd -g 1010 sambagroup
[root@server.aamishina.net ~]# usermod -aG sambagroup aamishina
[root@server.aamishina.net ~]# mkdir -p /srv/sambashare
[root@server.aamishina.net ~]#
```

Рис. 2.1: Создание группы sambagroup, добавление к ней пользователя и создание каталога

В файле конфигурации /etc/samba/smb.conf изменим параметр рабочей группы и в конец файла добавим раздел с описанием общего доступа к разделяемому ресурсу /srv/sambashare(рис. fig. 2.2):

```
root@server:~  
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  
[sambashare]  
comment = My Samba Share  
path = /srv/sambashare  
write list = @sambagroup  
:wq
```

Рис. 2.2: Добавление конфигураций в файл /etc/samba/smb.conf

Убедимся, что не сделали синтаксических ошибок в файле smb.conf и запустим демон Samba, а затем посмотрим его статус(fig. 2.3):

```
[root@server.aamishina.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
^C
[root@server.aamishina.net ~]# systemctl start smb
[root@server.aamishina.net ~]# systemctl enable smb
Created symlink /etc/systemd/system/multi-user.target.wants/smb.service → /usr/lib/systemd/system/smb.service.
[root@server.aamishina.net ~]# systemctl status smb
● smb.service - Samba SMB Daemon
   Loaded: loaded (/usr/lib/systemd/system/smb.service; enabled; preset: disabled)
   Active: active (running) since Sun 2024-10-27 16:05:43 UTC; 10s ago
     Docs: man:smbd(8)
           man:samba(7)
           man:smb.conf(5)
     Main PID: 10559 (smbd)
        Status: "smbd: ready to serve connections..."
          Tasks: 3 (limit: 4555)
         Memory: 13.6M
            CPU: 119ms
       CGroup: /system.slice/smb.service
               └─10559 /usr/sbin/smbd --foreground --no-process-group
                  ├─10561 /usr/sbin/smbd --foreground --no-process-group
                  ├─10562 /usr/sbin/smbd --foreground --no-process-group

Oct 27 16:05:43 server.aamishina.net systemd[1]: Starting Samba SMB Daemon...
Oct 27 16:05:43 server.aamishina.net smbd[10559]: [2024/10/27 16:05:43.323193,  0] ..../source3/smbd/se>
Oct 27 16:05:43 server.aamishina.net smbd[10559]:    smbd version 4.19.4 started.
Oct 27 16:05:43 server.aamishina.net smbd[10559]: Copyright Andrew Tridgell and the Samba Team 1992-20>
```

Рис. 2.3: Запуск samba и просмотр статуса

Для проверки наличия общего доступа попробуем подключиться к серверу с помощью smbclient (fig. 2.4):

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

      Sharename  Type  Comment
      -----  ----  -----
      print$    Disk  Printer Drivers
      sambashare  Disk  My Samba Share
      IPC$      IPC   IPC Service (Samba 4.19.4)
SMB1 disabled -- no workgroup available
```

Рис. 2.4: Подключение к серверу с помощью smbclient

Посмотрите файл конфигурации межсетевого экрана для Samba(fig. 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 option 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: Файл конфигурации межсетевого экрана для Samba

Настроим межсетевой экран и права доступа для каталога с разделяемым ресурсом(fig. 2.6):

```
[root@server.aamishina.net ~]# less /usr/lib/firewalld/services/samba.xml
[root@server.aamishina.net ~]# firewall-cmd --add-service=samba
success
[root@server.aamishina.net ~]# firewall-cmd --add-service=samba --permanent
success
[root@server.aamishina.net ~]# firewall-cmd --reload
success
[root@server.aamishina.net ~]# chgrp sambagroup /srv/sambashare
[root@server.aamishina.net ~]# chmod g=rwx /srv/sambashare
[root@server.aamishina.net ~]#
```

Рис. 2.6: Настройка межсетевого экрана и прав доступа для каталога с разделяемым ресурсом

Посмотрим контекст безопасности SELinux и настроим его для каталога с разделяемым ресурсом. Затем проверим, что контекст безопасности изменился и разрешим экспортацию разделяемых ресурсов для чтения и записи(fig. 2.7):

```
[root@server.aamishina.net ~]# cd /srv
[root@server.aamishina.net srv]# ls -Z
unconfined_u:object_r:nfs_t:s0 nfs  unconfined_u:object_r:var_t:s0 sambashare
[root@server.aamishina.net srv]# semanage fcontext -a -t samba_share_t "/srv/sambashare(/.*)?"
[root@server.aamishina.net srv]# restorecon -vR /srv/sambashare
Relabeled /srv/sambashare from unconfined_u:object_r:var_t:s0 to unconfined_u:object_r:samba_share_t:s0
[root@server.aamishina.net srv]# cd /srv
[root@server.aamishina.net srv]# ls -Z
    unconfined_u:object_r:nfs_t:s0 nfs  unconfined_u:object_r:samba_share_t:s0 sambashare
[root@server.aamishina.net srv]# setsebool samba_export_all_rw 1
[root@server.aamishina.net srv]# setsebool samba_export_all_rw 1 -P
```

Рис. 2.7: Настройка контекста безопасности SELinux

Посмотрим UID нашего пользователя и в какие группы он включён(fig. 2.8):

```
[aamishina@server.aamishina.net sambashare]$ id
uid=1001(aamishina) gid=1001(aamishina) groups=1001(aamishina),10(wheel) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```

Рис. 2.8: Просмотр UID нашего пользователя

Затем под нашим пользователем aamishina попробуем создать файл на разделяемом ресурсе(fig. 2.9):

```
[aamishina@server.aamishina.net sambashare]$ touch aamishina@server.txt
[aamishina@server.aamishina.net sambashare]$ ls
aamishina@server.txt
```

Рис. 2.9: Создание файла на разделяемом ресурсе

Добавим пользователя aamishina в базу пользователей Samba(fig. 2.10):

```
[aamishina@server.aamishina.net sambashare]$ smbpasswd -L -a aamishina
smbpasswd -L can only be used by root.
[aamishina@server.aamishina.net sambashare]$ sudo -i
[sudo] password for aamishina:
[root@server.aamishina.net ~]# smbpasswd -L -a aamishina
New SMB password:
Retype new SMB password:
Added user aamishina.
```

Рис. 2.10: Добавление пользователя в базу пользователей Samba

2.2 Монтирование файловой системы Samba на клиенте

На клиенте установим необходимые пакеты. Затем посмотрим файл конфигурации межсетевого экрана для клиента Samba, настроим межсетевой экран и создадим группу sambagroup, добавим в неё пользователя aamishina(рис. fig. 2.11):

```
Complete!
[root@client.aamishina.net ~]# less /usr/lib/firewalld/services/samba-client.xml
[root@client.aamishina.net ~]# firewall-cmd --add-service=samba-client
success
[root@client.aamishina.net ~]# firewall-cmd --add-service=samba-client --permanent
success
[root@client.aamishina.net ~]# firewall-cmd --reload
success
[root@client.aamishina.net ~]# groupadd -g 1010 sambagroup
[root@client.aamishina.net ~]# usermod -aG sambagroup aamishina
[root@client.aamishina.net ~]# groups
root
[root@client.aamishina.net ~]# exit
logout
[aamishina@client.aamishina.net ~]$ █
```

Рис. 2.11: Настройка межсетевого экрана, создание группы и добавление в неё пользователя на клиенте

На клиенте в файле конфигурации /etc/samba/smb.conf изменим параметр рабочей группы(рис. fig. 2.12):

```
[global]
    workgroup = AAMISHINA-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
```

```
:w
```

Рис. 2.12: Изменение параметра рабочей группы на клиенте

Для проверки наличия общего доступа попробуем подключиться с клиента к серверу с помощью smbclient под учетной записью root, зайдя как анонимный пользователь и под учетной записью aamishina. Затем подключемся к клиенту с сервера под учётной записью нашего пользователя(указав параметр -U можно авторизоваться под записью aamishina и с пользователя root) (рис. fig. 2.13), (рис. fig. 2.14).

```
[aamishina@client.aamishina.net ~]$ vim /etc/samba/smb.conf
[aamishina@client.aamishina.net ~]$ sudo -i
[root@client.aamishina.net ~]# 123456
bash: 123456: command not found...
^C
[root@client.aamishina.net ~]# vim /etc/samba/smb.conf
[root@client.aamishina.net ~]# smbclient -L //server
Password for [AAMISHINA-NET\root]:
Anonymous login successful

      Sharename      Type      Comment
-----  -----
print$        Disk      Printer Drivers
sambashare    Disk      My Samba Share
IPC$          IPC       IPC Service (Samba 4.19.4)

SMB1 disabled -- no workgroup available
[root@client.aamishina.net ~]# exit
logout
[aamishina@client.aamishina.net ~]$ smbclient -L //server
Password for [AAMISHINA-NET\aaamishina]:
Anonymous login successful

      Sharename      Type      Comment
-----  -----
print$        Disk      Printer Drivers
sambashare    Disk      My Samba Share
IPC$          IPC       IPC Service (Samba 4.19.4)

SMB1 disabled -- no workgroup available
```

Рис. 2.13: Проверка наличия общего доступа

```
[aamishina@client.aamishina.net ~]$ smbclient -L //server -U aamishina  
Password for [AAMISHINA-NET\aamishina]:  
  
      Sharename  Type  Comment  
      -----  ----  -----  
      print$    Disk  Printer Drivers  
      sambashare  Disk  My Samba Share  
      IPC$      IPC   IPC Service (Samba 4.19.4)  
      aamishina  Disk  Home Directories  
SMB1 disabled -- no workgroup available  
[aamishina@client.aamishina.net ~]$
```

Рис. 2.14: Подключение под записью пользователя

Теперь создадим точку монтирования с помощью команды `mkdir /mnt/samba` и на клиенте получим доступ к общему ресурсу с помощью `mount`(fig. 2.15)

```
[aamishina@client.aamishina.net ~]$ mkdir /mnt/samba  
mkdir: cannot create directory '/mnt/samba': Permission denied  
[aamishina@client.aamishina.net ~]$ sudo -i  
[root@client.aamishina.net ~]# mkdir /mnt/samba  
[root@client.aamishina.net ~]# mount -o username=aamishina //server/sambashare /mnt/samba  
Password for aamishina@//server/sambashare:  
mount: (hint) your fstab has been modified, but systemd still uses  
the old version; use 'systemctl daemon-reload' to reload.
```

Рис. 2.15: Получение доступа к общему ресурсу с клиента

Убедимся, что наш пользователь может создавать файлы на разделяемом ресурсе(fig. 2.16)

```
[root@client.aamishina.net ~]# cd /mnt/samba/  
[root@client.aamishina.net samba]# touch aamishina@client.txt  
[root@client.aamishina.net samba]# ls  
aamishina@client.txt  aamishina@server.txt  
[root@client.aamishina.net samba]#
```

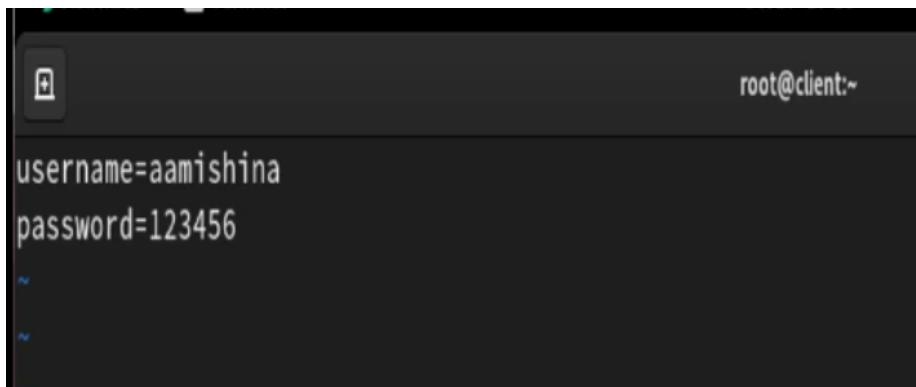
Рис. 2.16: Создание файла на разделяемом ресурсе с клиента

Отмонтируем каталог /mnt/samba и для настройки работы с Samba с помощью файла учётных данных на клиенте создадим файл smbusers в каталоге /etc/samba/(fig. 2.17)

```
[root@client.aamishina.net ~]# umount /mnt/samba
[root@client.aamishina.net ~]# touch /etc/samba/smbusers
[root@client.aamishina.net ~]# chmod 600 /etc/samba/smb
smb.conf      smb.conf.example  smbusers
[root@client.aamishina.net ~]# chmod 600 /etc/samba/smbusers
[root@client.aamishina.net ~]# vim /etc/samba/smbusers
```

Рис. 2.17: Создание файла учётных данных

Внесём в этот файл следующее содержимое(fig. 2.18)



The screenshot shows a terminal window with a dark background and light-colored text. At the top right, it says "root@client:~". The window contains two lines of text: "username=aamishina" and "password=123456". There are two small question marks at the bottom of the window.

```
username=aamishina
password=123456
```

Рис. 2.18: Внесение содержимого в файл smbusers

На клиенте в файле /etc/fstab добавим следующую строку(fig. 2.19)

```

#
# After editing this file, run 'systemctl daemon-reload' to update systemd
# units generated from this file.
#
UUID=707fdfff-f8d1-4415-8394-9da35f1e5962 / xfs defaults 0 0
/swappfile none swap defaults 0 0
server.aamishina.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/sambashare /mnt/samba cifs vers=3.0,user,rw,uid=aamishina,gid=sambagroup,credentials=/etc/samba/smbusers,_netdev 0 0
-
-
-

```

Рис. 2.19: Добавление записи в файл /etc/fstab

Подмонтируем общий ресурс(fig. 2.20):

```

[root@client.aamishina.net ~]# vim /etc/fstab
[root@client.aamishina.net ~]# mount -a

```

Рис. 2.20: Монтирование общего ресурса

Перезапустим клиента и проверим, что ресурс монтируется и после перезагрузки, а у пользователя есть доступ к разделяемым ресурсам(fig. 2.21):

```

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

```

Рис. 2.21: Проверка доступа к разделяемым ресурсам после перезапуска клиента

2.3 Внесение изменений в настройки внутреннего окружения виртуальных машины

На виртуальной машине server перейдем в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/, создадим в нём каталог smb, в который поместим в соответствующие подкаталоги конфигурационные файлы, а также создадим исполняемый файл smb.sh:

```
cd /vagrant/provision/server  
mkdir -p /vagrant/provision/server/smb/etc/samba  
cp -R /etc/samba/smb.conf /vagrant/provision/server/smb/etc/samba/  
  
touch smb.sh  
chmod +x smb.sh
```

В каталоге /vagrant/provision/server создадим исполняемый файл smb.sh и внесем скрипт(fig. 2.22):

```
root@server:/vagrant/provision/server x aamishina@server:/srv/sambashare x aamishina@server:/vagrant/provision/client x
firewall-cmd --add-service samba --permanent
firewall-cmd --reload

echo "Users and groups"
groupadd -g 1010 sambagroup
usermod -aG sambagroup $LOGIN
echo -ne "$PASS\n$PASS\n" | smbpasswd -L -a -s $LOGIN

echo "Make share dir"
mkdir -p /srv/sambashare
chgrp sambagroup /srv/sambashare
chmod g=rwx /srv/sambashare

echo "Tuning SELinux"
semanage fcontext -a -t samba_share_t "/srv/sambashare(/.*)?"

setsebool samba_export_all_rw 1
setsebool samba_export_all_rw 1 -P

restorecon -vR /srv/sambashare

echo "Start smb service"
systemctl enable smb
systemctl start smb

systemctl restart firewalld
```

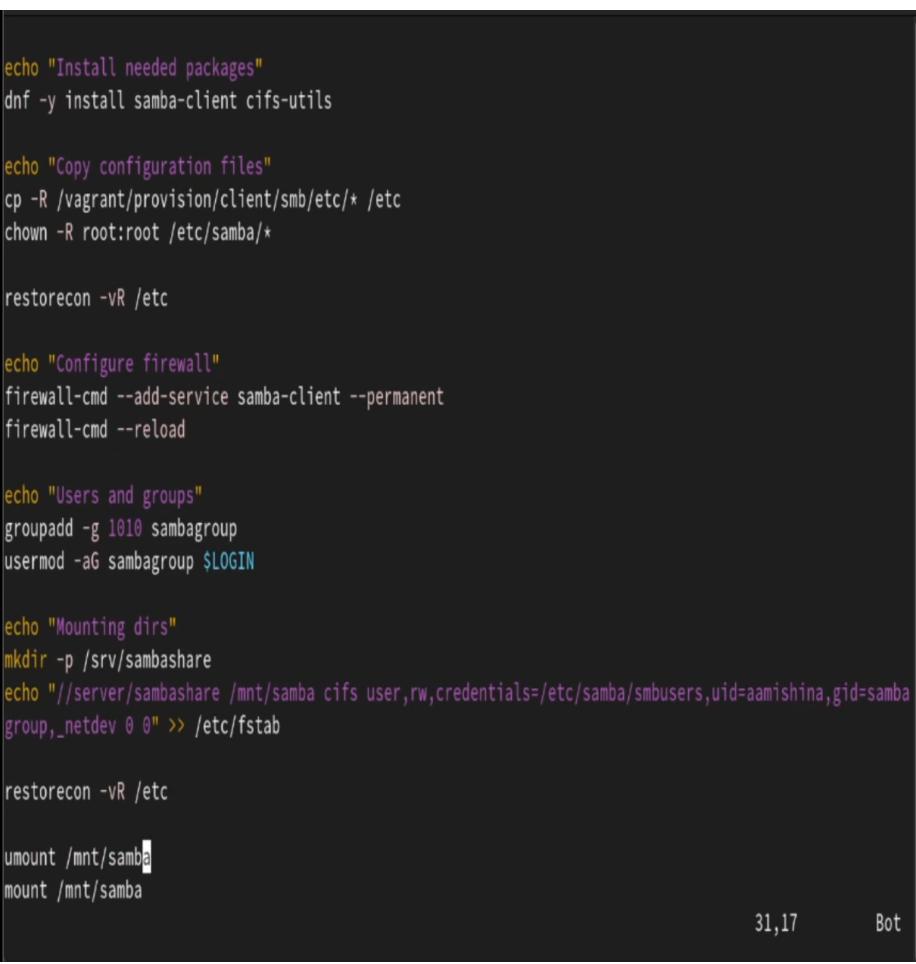
Рис. 2.22: Скрипта файла /vagrant/provision/server/smb.sh

На виртуальной машине client перейдем в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/client/, создадим в нём каталог smb, в который поместим в соответствующие подкаталоги конфигурационные файлы, а также создадим исполняемый файл smb.sh:

```
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/  
  
touch smb.sh  
chmod +x smb.sh
```

В каталоге /vagrant/provision/client создадим исполняемый файл smb.sh и внесем скрипт(fig. 2.23):



```
echo "Install needed packages"  
dnf -y install samba-client cifs-utils  
  
echo "Copy configuration files"  
cp -R /vagrant/provision/client/smb/etc/* /etc  
chown -R root:root /etc/samba/*  
  
restorecon -vR /etc  
  
echo "Configure firewall"  
firewall-cmd --add-service samba-client --permanent  
firewall-cmd --reload  
  
echo "Users and groups"  
groupadd -g 1010 sambagroup  
usermod -aG sambagroup $LOGIN  
  
echo "Mounting dirs"  
mkdir -p /srv/sambashare  
echo "//server/sambashare /mnt/samba cifs user,rw,credentials=/etc/samba/smbusers,uid=aamishina,gid=samba  
group,_netdev 0 0" >> /etc/fstab  
  
restorecon -vR /etc  
  
umount /mnt/samba  
mount /mnt/samba
```

31,17 Bot

Рис. 2.23: Скрипта файла /vagrant/provision/client/smb.sh

Затем для отработки созданных скриптов в конфигурационном файле Vagrantfile необходимо добавить 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 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`

4 Выводы

В результате выполнения данной работы были приобретены практические навыки настройки доступа групп пользователей к общим ресурсам по протоколу SMB.