

## Лабораторная работа № 14. Настройка файловых служб Samba

### 14.1. Цель работы

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

### 14.2. Предварительные сведения

Протокол Server Message Block (SMB) предназначен для организации межпроцессорного взаимодействия, а также удалённого доступа к разделяемым сетевым ресурсам (файлам, принтерам и проч.).

По сути, SMB выполняет аналогичные NFS-функции, но лучше него работает при необходимости организации взаимодействия между Unix/Linux узлами и узлами сети с операционной системой Windows. Различия заключаются, например, в наличии/отсутствии:

- информации о владельцах разделяемого ресурса;
- поддержки блокирования ресурса по режиму работы;
- информации о правах доступа, UID и GID ресурса.

Пакет программ Samba представляет собой свободную реализацию приложения на базе протокола SMB и позволяет Unix/Linux узлам взаимодействовать с сетью, построенной на основе MS Windows. Samba имеет клиент-серверную архитектуру, работает поверх TCP/IP. В качестве файловой системы может использоваться smbfs или cifs (Common Internet File System).

Основной файл конфигурации Samba — `/etc/samba/smb.conf`. В нём задаются ограничения на доступ к системным ресурсам извне. Файл содержит разделы с описанием. Каждый раздел начинается с его заголовка в квадратных скобках, например, `[global]`, `[homes]`, `[printers]` и т.п. Разделы содержат параметры в формате `имя = значение`. Имена разделов и параметров не чувствительны к регистру. Начальные, конечные и внутренние пробелы некорректны в названиях секций и именах параметров. Начальные и конечные пробелы в значении параметров игнорируются. Внутренний пробел в значении параметра сохраняется дословно. Все строки, начинающиеся с запятой, с символа «`;`» или «`#`», игнорируются как строки, содержащие только пробел. Все строки, оканчивающиеся символом «`\`», продолжаются на следующей строке в стиле UNIX. Значения после символа равенства в параметрах содержат строку (без кавычек) или логическое значение: `yes/no`, `0/1` или `true/false`.

В пакет Samba входит несколько программ административного и клиентского назначения.

Административные и диагностические утилиты:

- `net` — утилита администрирования для пакета Samba и удалённых серверов CIFS;
- `pdbedit` — просмотр и управление учётными записями пользователей Samba;
- `smbcontrol` — утилита для отправки сообщений процессам `smbd`, `nmbd` и `winbindd`;
- `smbpasswd` — утилита для изменения SMB-паролей пользователей;
- `smbstatus` — просмотр текущих соединений к общим ресурсам сервера;
- `swat` — инструмент конфигурирования файла `smb.conf` через веб-браузер;
- `tdbbackup` — утилита для создания резервной копии и проверки целостности файла `samba.tdb`;
- `testparm` — утилита проверки корректности оформления настроек в файле `smb.conf`.

Клиентский инструментарий:

- `smbclient` — FTP-подобный интерфейс для работы по перемещению файлов;
- `mount.cifs/umount.cifs` — утилиты монтирования/размонтирования CIFS ресурсов;
- `smbtree` — утилита просмотра SMB-ресурсов сети;
- `smbtar` — скрипт shell для архивации общих ресурсов SMB/CIFS на UNIX устройстве хранения;

- smbpool – утилита для отправки на печать файла на SMB-принтер. Описание параметров утилит Samba см. в руководствах man, а также в [1].

### 14.3. Задание

1. Установите и настройте сервер Samba (см. раздел 14.4.1).
2. Настройте на клиенте доступ к разделяемым ресурсам (см. раздел 14.4.2).
3. Напишите скрипты для Vagrant, фиксирующие действия по установке и настройке сервера Samba для доступа к разделяемым ресурсам во внутреннем окружении виртуальных машин server и client. Соответствующим образом необходимо внести изменения в Vagrantfile (см. раздел 14.4.3).

### 14.4. Последовательность выполнения работы

#### 14.4.1. Настройка сервера Samba

1. На сервере установите необходимые пакеты:  
`dnf -y install samba samba-client cifs-utils`
2. Создайте группу sambagroup для пользователей, которые будут работать с Samba-сервером, и присвойте ей GID 1010:  
`groupadd -g 1010 sambagroup`
3. Добавьте пользователя user к группе sambagroup (вместо user используйте ваш логин):  
`usermod -aG sambagroup user`
4. Создайте общий каталог в файловой системе Linux, в который предполагается монтировать разделяемые ресурсы:  
`mkdir -p /srv/sambashare`
5. В файле конфигурации /etc/samba/smb.conf:
  - (a) измените параметр рабочей группы (вместо USER укажите имя (логин) вашего пользователя):  

```
[global]
workgroup = USER-NET
```
  - (b) в конце файла добавьте раздел с описанием общего доступа к разделяемому ресурсу /srv/sambashare:  

```
[sambashare]
comment = My Samba Share
path = /srv/sambashare
write list = @sambagroup
```
6. Убедитесь, что вы не сделали синтаксических ошибок в файле smb.conf, используя команду:  
`testparm`
7. Запустите демон Samba и посмотрите его статус:  
`systemctl start smb`  
`systemctl enable smb`  
`systemctl status smb`
8. Для проверки наличия общего доступа попробуйте подключиться к серверу с помощью smbclient:  
`smbclient -L //server`  
(при запросе пароля нажмите  для работы под анонимным пользователем).
9. Посмотрите файл конфигурации межсетевого экрана для Samba:  
`less /usr/lib/firewalld/services/samba.xml`
10. Настройте межсетевой экран:  
`firewall-cmd --add-service=samba`  
`firewall-cmd --add-service=samba --permanent`  
`firewall-cmd --reload`

11. Настройте права доступа для каталога с разделяемым ресурсом:  

```
chgrp sambagroup /srv/smbashare
chmod g=rwx /srv/smbashare
```
12. Посмотрите контекст безопасности SELinux:  

```
cd /srv
ls -Z
```
13. Настройте контекст безопасности SELinux для каталога с разделяемым ресурсом:  

```
semanage fcontext -a -t samba_share_t "/srv/smbashare(/.*)?"
restorecon -vR /srv/smbashare
```
14. Проверьте, что контекст безопасности изменился:  

```
cd /srv
ls -Z
```
15. Разрешите экспортировать разделяемые ресурсы для чтения и записи:  

```
setsebool samba_export_all_rw 1
setsebool samba_export_all_rw 1 -P
```
16. Посмотрите UID вашего пользователя и в какие группы он включён:  

```
id
```
17. Под вашим пользователем user попробуйте создать файл на разделяемом ресурсе (вместо user используйте ваш логин):  

```
cd /srv/smbashare
touch user@server.txt
```
18. Добавьте вашего пользователя user в базу пользователей Samba (вместо user используйте ваш логин):  

```
smbpasswd -L -a user
```

(при запросе укажите пароль для SMB-пользователя, например, совпадающий с паролем учётной записи вашего пользователя user).

#### 14.4.2. Монтирование файловой системы Samba на клиенте

1. На клиенте установите необходимые пакеты<sup>1</sup>:  

```
dnf -y install samba-client cifs-utils
```
2. На клиенте посмотрите файл конфигурации межсетевого экрана для клиента Samba:  

```
less /usr/lib/firewalld/services/samba-client.xml
```
3. На клиенте настройте межсетевой экран:  

```
firewall-cmd --add-service=samba-client
firewall-cmd --add-service=samba-client --permanent
firewall-cmd --reload
```
4. На клиенте создайте группу sambagroup и добавьте в неё пользователя user (вместо user используйте ваш логин):  

```
groupadd -g 1010 sambagroup
usermod -aG sambagroup user
```
5. На клиенте в файле конфигурации /etc/samba/smb.conf измените параметр рабочей группы:  

```
[global]
workgroup = USER-NET
```
6. Для проверки наличия общего доступа попробуйте подключиться с клиента к серверу с помощью smbclient:  

```
smbclient -L //server
```

В отчёте укажите, под какой учётной записью вы просматриваете ресурсы сервера.
7. Подключитесь с клиента к серверу с помощью smbclient под учётной записью вашего пользователя (вместо user используйте ваш логин):  

```
smbclient -L //server -U user
```

В отчёте укажите, под какой учётной записью вы просматриваете ресурсы сервера.

---

<sup>1</sup>Модуль файловой системы cifs находится в пакете kernel-modules. Проверьте его наличие.

8. На клиенте создайте точку монтирования:
 

```
mkdir /mnt/samba
```
9. На клиенте получите доступ к общему ресурсу с помощью mount (вместо user\_name используйте ваш логин):
 

```
mount -o username=user_name,user,rw,uid=user_name,gid=sambagroup
  ↵ //server/smbashare /mnt/samba
```

При появлении запроса пароля введите пароль SMB-пользователя.
10. Убедитесь, что user может записывать файлы на разделяемом ресурсе (вместо user используйте ваш логин):
 

```
cd /mnt/samba
touch user@client.txt
```
11. Отмонтируйте каталог /mnt/samba:
 

```
umount /mnt/samba
```
12. Для настройки работы с Samba с помощью файла учётных данных:
  - (a) на клиенте создайте файл smbusers в каталоге /etc/samba/:
 

```
touch /etc/samba/smbusers
chmod 600 /etc/samba/smbusers
```

с содержанием следующего формата:

```
username=<username>
password=<password>
```

Например:

```
username=user
password=123456
```

(вместо user используйте ваш логин и SMB-пароль вашего пользователя).
  - (b) На клиенте в файле /etc/fstab добавьте следующую строку (вместо user\_name укажите ваш логин):
 

```
//server/smbashare /mnt/samba cifs
  ↵ user,rw,uid=user_name,gid=sambagroup,
  ↵ credentials=/etc/samba/smbusers,_netdev 0 0
```
  - (c) Подмонтируйте общий ресурс:
 

```
mount -a
```
13. Убедившись, что ресурс монтируется, вы можете перезагрузить клиента для проверки, что ресурс монтируется и после перезагрузки, а у пользователя есть доступ к разделяемым ресурсам.

#### 14.4.3. Внесение изменений в настройки внутреннего окружения виртуальных машин

1. На виртуальной машине server перейдите в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/, создайте в нём каталог smb, в который поместите в соответствующие подкаталоги 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/
```
2. В каталоге /vagrant/provision/server создайте исполняемый файл smb.sh:
 

```
cd /vagrant/provision/server
touch smb.sh
chmod +x smb.sh
```

Открыв его на редактирование, пропишите в нём следующий скрипт (вместо user укажите свой логин):

```
#!/bin/bash
```

```
LOGIN=user
PASS=123456
```

```
echo "Provisioning script $0"

echo "Install needed packages"
dnf -y install samba samba-client cifs-utils

echo "Copy configuration files"
cp -R /vagrant/provision/server/smb/etc/* /etc
chown -R root:root /etc/samba/*
restorecon -vR /etc

echo "Configure firewall"
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/smbashare
chgrp sambagroup /srv/smbashare
chmod g=rwx /srv/smbashare

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

setsebool samba_export_all_rw 1
setsebool samba_export_all_rw 1 -P

restorecon -vR /srv/smbashare

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

systemctl restart firewalld
```

3. На виртуальной машине client перейдите в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/client/, создайте в нём каталог smb, в который поместите в соответствующие подкаталоги 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/
```

4. В каталоге /vagrant/provision/client создайте исполняемый файл smb.sh:

```
cd /vagrant/provision/client
touch smb.sh
chmod +x smb.sh
```

Открыв его на редактирование, пропишите в нём следующий скрипт (вместо user укажите свой логин):

```
#!/bin/bash
```

```
LOGIN=user
```

```
echo "Provisioning script $0"
```

```
mkdir -p /mnt/samba

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=user,
↳ gid=sambagroup,_netdev 0 0" >> /etc/fstab

restorecon -vR /etc

umount /mnt/samba
mount /mnt/samba
```

5. Для отработки созданных скриптов во время загрузки виртуальных машин `server` и `client` 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"
```

## 14.5. Содержание отчёта

1. Титульный лист с указанием номера лабораторной работы и ФИО студента.
2. Формулировка задания работы.
3. Описание результатов выполнения задания:
  - скриншоты (снимки экрана), фиксирующие выполнение работы;
  - подробное описание настроек служб в соответствии с заданием;
  - полные тексты конфигурационных файлов настраиваемых в работе служб;
  - результаты проверки корректности настроек служб в соответствии с заданием (подтверждённые скриншотами).
4. Выводы, согласованные с заданием работы.
5. Ответы на контрольные вопросы.

## 14.6. Контрольные вопросы

1. Какова минимальная конфигурация для `smb.conf` для создания общего ресурса, который предоставляет доступ к каталогу `/data`?
2. Как настроить общий ресурс, который даёт доступ на запись всем пользователям, имеющим права на запись в файловой системе Linux?
3. Как ограничить доступ на запись к ресурсу только членам определённой группы?
4. Какой переключатель SELinux нужно использовать, чтобы позволить пользователям получать доступ к домашним каталогам на сервере через SMB?
5. Как ограничить доступ к определённому ресурсу только узлам из сети 192.168.10.0/24?
6. Какую команду можно использовать, чтобы отобразить список всех пользователей Samba на сервере?
7. Что нужно сделать пользователю для доступа к ресурсу, который настроен как многопользовательский ресурс?
8. Как установить общий ресурс Samba в качестве многопользовательской учётной записи, где пользователь `alice` используется как минимальная учётная запись пользователя?
9. Как можно запретить пользователям просматривать учётные данные монтирования Samba в файле `/etc/fstab`?
10. Какая команда позволяет перечислить все экспортируемые ресурсы Samba, доступные на определённом сервере?

## Список литературы

1. Всё о Samba. — URL: <http://smb-conf.ru/> (дата обр. 13.09.2021).