

Лабораторная работа № 13. Настройка NFS

13.1. Цель работы

Приобретение навыков настройки сервера NFS для удалённого доступа к ресурсам.

13.2. Предварительные сведения

Протокол сетевого доступа к файловым системам (Network File System, NFS) предназначен для монтирования через сеть файловых систем, расположенных на других узлах сети.

Данный протокол работает в соответствии с клиент-серверной архитектурой. Клиенты NFS имеют прозрачный доступ к ресурсам файловой системы NFS-сервера. Прозрачность доступа в этом случае означает, что любое приложение клиента может работать не с локальным, а с подмонтированным через NFS файлом без модификаций настроек приложения. При этом доступ к файлам на сервере NFS клиенты получают с помощью отправки соответствующих RPC-запросов на сервер. Протокол удалённого вызова процедур (RPC) определяет формат всех взаимодействий между клиентом и сервером. Семантику монтирования и размонтирования файловых систем NFS определяет протокол монтирования (процесс mountd).

Для организации удалённого доступа к ресурсам с помощью NFS должны быть выполнены процедуры экспортирования и монтирования каталогов. Сервер NFS должен экспортировать каталог, после чего клиент NFS может смонтировать его в точке монтирования в своём пространстве имён и работать с ним, как с локальным ресурсом. Экспортирование каталога в данном случае означает, что каталог в пространстве имён сервера становится доступным для клиента в соответствии с заданными при экспорте правами доступа. Экспортируемые каталоги должны быть указаны в файле `/etc/exports`.

Формат записи в файле `/etc/exports`:

[файловая система] [кому разрешить доступ] [ключи опций]

Некоторые опции:

- `ro` — только чтение;
- `rw` — чтение и запись;
- `root_squash` — запрет пользователю `root` получать `root`-привилегии на удалённой файловой системе, все действия будут производиться с правами пользователя `nobody`;
- `no_root_squash` — разрешение пользователю `root` получать `root`-привилегии на удалённой файловой системе (не рекомендуется к использованию);
- `anonuid/anongid` позволяет задать UID и GID пользователя, от лица которого будут выполняться все запросы;
- `all_squash` — указывает на то, что все запросы происходят от анонимного пользователя, что способствует повышению безопасности.

Пример записи в файле `/etc/exports`, разрешающий всем пользователям сети `192.168.0.0/16` чтение и запись в общем каталоге `/home/share`:

```
/home/share 192.168.0.0/16(rw)
```

Пользователь `root` по умолчанию не имеет доступа к экспортированной файловой системе. При обращении пользователя `root` одного узла к файлу удалённого узла через NFS его идентификатор пользователя преобразуется системой NFS в идентификатор локального пользователя `nobody`, права доступа которого совпадают с общими правами доступа к файлу. Из соображений обеспечения безопасности и целостности данных не рекомендуется предоставлять пользователю `root` доступ к разделяемым сетевым ресурсам.

Команда `showmount` позволяет просматривать смонтированные удалённо файловые системы и каталоги.

Синтаксис:

```
showmount [-a] [-d] [-e] [host]
```

Здесь:

- d — выводит список удалённо смонтированных каталогов;
- a — выводит список всех удалённых монтирований в формате `hostname:directory`, где `hostname` — имя клиента, а `directory` — корень смонтированной файловой системы;
- e — выводит список экспортируемых файловых систем.

13.3. Задание

1. Установите и настройте сервер NFSv4 (см. раздел 13.4.1).
2. Подмонтируйте удалённый ресурс на клиенте (см. раздел 13.4.2).
3. Подключите каталог с контентом веб-сервера к дереву NFS (см. раздел 13.4.3).
4. Подключите каталог для удалённой работы вашего пользователя к дереву NFS (см. раздел 13.4.4).
5. Напишите скрипты для Vagrant, фиксирующие действия по установке и настройке сервера NFSv4 во внутреннем окружении виртуальных машин `server` и `client`. Соответствующим образом внесите изменения в `Vagrantfile` (см. раздел 13.4.5).

13.4. Последовательность выполнения работы

13.4.1. Настройка сервера NFSv4

1. На сервере установите необходимое программное обеспечение:
`dnf -y install nfs-utils`
2. На сервере создайте каталог, который предполагается сделать доступным всем пользователям сети (корень дерева NFS):
`mkdir -p /srv/nfs`
3. В файле `/etc/exports` пропишите подключаемый через NFS общий каталог с доступом только на чтение:
`/srv/nfs *(ro)`
4. Для общего каталога задайте контекст безопасности NFS:
`semanage fcontext -a -t nfs_t "/srv/nfs(/.*)?"`
5. Примените изменённую настройку SELinux к файловой системе:
`restorecon -vR /srv/nfs`
6. Запустите сервер NFS:
`systemctl start nfs-server.service`
`systemctl enable nfs-server.service`
7. Настройте межсетевой экран для работы сервера NFS:
`firewall-cmd --add-service=nfs`
`firewall-cmd --add-service=nfs --permanent`
`firewall-cmd --reload`
8. На клиенте установите необходимое для работы NFS программное обеспечение:
`dnf -y install nfs-utils`
9. На клиенте попробуйте посмотреть имеющиеся подмонтированные удалённые ресурсы (вместо `user` укажите свой логин):
`showmount -e server.user.net`
В отчёте поясните, что при этом происходит.
10. Попробуйте на сервере остановить сервис межсетевого экрана:
`systemctl stop firewalld.service`
Затем на клиенте вновь попробуйте подключиться к удалённо смонтированному ресурсу:
`showmount -e server.user.net`
В отчёте поясните, что при этом происходит.
11. На сервере запустите сервис межсетевого экрана

```
systemctl start firewalld
```

12. На сервере посмотрите, какие службы задействованы при удалённом монтировании:

```
lsof | grep TCP
```

```
lsof | grep UDP
```

13. Добавьте службы rpc-bind и mountd в настройки межсетевого экрана на сервере:

```
firewall-cmd --get-services
```

```
firewall-cmd --add-service=mountd --add-service=rpc-bind
```

```
firewall-cmd --add-service=mountd --add-service=rpc-bind --permanent
```

```
firewall-cmd --reload
```

14. На клиенте проверьте подключение удалённого ресурса (вместо user укажите свой логин):

```
showmount -e server.user.net
```

13.4.2. Монтирование NFS на клиенте

1. На клиенте создайте каталог, в который будет монтироваться удалённый ресурс, и подмонтируйте дерево NFS (вместо user укажите свой логин):

```
mkdir -p /mnt/nfs
```

```
mount server.user.net:/srv/nfs /mnt/nfs
```

2. Проверьте, что общий ресурс NFS подключён правильно:

```
mount
```

В отчёте поясните выведенную информацию о монтировании удалённого ресурса.

3. На клиенте в конце файла /etc/fstab добавьте следующую запись (вместо user укажите свой логин):

```
server.user.net:/srv/nfs /mnt/nfs nfs _netdev 0 0
```

В отчёте поясните синтаксис этой записи.

4. На клиенте проверьте наличие автоматического монтирования удалённых ресурсов при запуске операционной системы:

```
systemctl status remote-fs.target
```

5. Перезапустите клиента и убедитесь, что удалённый ресурс подключается автоматически.

13.4.3. Подключение каталогов к дереву NFS

1. На сервере создайте общий каталог, в который затем будет подмонтирован каталог с контентом веб-сервера:

```
mkdir -p /srv/nfs/www
```

2. Подмонтируйте каталог веб-сервера:

```
mount -o bind /var/www/ /srv/nfs/www/
```

3. На сервере проверьте, что отображается в каталоге /srv/nfs.

4. На клиенте посмотрите, что отображается в каталоге /mnt/nfs.

5. На сервере в файле /etc/exports добавьте экспорт каталога веб-сервера с удалённого ресурса:

```
/srv/nfs/www 192.168.0.0/16(rw)
```

6. Экспортируйте все каталоги, упомянутые в файле /etc/exports:

```
exportfs -r
```

7. Проверьте на клиенте каталог /mnt/nfs.

8. На сервере в конце файла /etc/fstab добавьте следующую запись:

```
/var/www /srv/nfs/www none bind 0 0
```

9. Повторно экспортируйте каталоги, указанные в файле /etc/exports:

```
exportfs -r
```

10. На клиенте проверьте каталог /mnt/nfs.

13.4.4. Подключение каталогов для работы пользователей

1. На сервере под пользователем `user` в его домашнем каталоге создайте каталог `common` с полными правами доступа только для этого пользователя, а в нём файл `user@server.txt` (вместо `user` укажите свой логин):

```
mkdir -p -m 700 ~/common
cd ~/common
touch user@server.txt
```
2. На сервере создайте общий каталог для работы пользователя `user` по сети (вместо `user` укажите свой логин):

```
mkdir -p /srv/nfs/home/user
```
3. Подмонтируйте каталог `common` пользователя `user` в NFS (вместо `user` укажите свой логин):

```
mount -o bind /home/user/common /srv/nfs/home/user
```

В отчёте укажите, какие права доступа установлены на этот каталог.
4. Подключите каталог пользователя в файле `/etc/exports`, прописав в нём (вместо `user` укажите свой логин):

```
/srv/nfs/home/user 192.168.0.0/16(rw)
```
5. Внесите изменения в файл `/etc/fstab` (вместо `user` укажите свой логин):

```
/home/user/common /srv/nfs/home/user none bind 0 0
```
6. Повторно экспортируйте каталоги:

```
exportfs -r
```
7. На клиенте проверьте каталог `/mnt/nfs`.
8. На клиенте под пользователем `user` перейдите в каталог `/mnt/nfs/home/user` и попробуйте создать в нём файл `user@client.txt` и внести в него какие-либо изменения:

```
cd /mnt/nfs/home/user
touch user@client.txt
```

Попробуйте проделать это под пользователем `root`.

9. На сервере посмотрите, появились ли изменения в каталоге пользователя `/home/user/common`.

13.4.5. 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 `nfs`, в который поместите в соответствующие подкаталоги конфигурационные файлы:

```
cd /vagrant/provision/server
mkdir -p /vagrant/provision/server/nfs/etc
cp -R /etc/exports /vagrant/provision/server/nfs/etc/
```
2. В каталоге `/vagrant/provision/server` создайте исполняемый файл `nfs.sh`:

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

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

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

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

```
echo "Install needed packages"
```

```
dnf -y install nfs-utils
```

```
echo "Copy configuration files"
cp -R /vagrant/provision/server/nfs/etc/* /etc

restorecon -vR /etc

echo "Configure firewall"
firewall-cmd --add-service nfs --permanent
firewall-cmd --add-service mountd --add-service rpc-bind --permanent
firewall-cmd --reload

echo "Tuning SELinux"
mkdir -p /srv/nfs
semanage fcontext -a -t nfs_t "/srv/nfs(/.*)?"
restorecon -vR /srv/nfs

echo "Mounting dirs"
mkdir -p /srv/nfs/www
mount -o bind /var/www /srv/nfs/www
echo "/var/www /srv/nfs/www none bind 0 0" >> /etc/fstab
mkdir -p /srv/nfs/home/user
mkdir -p -m 700 /home/user/common
chown user:user /home/user/common
mount -o bind /home/user/common /srv/nfs/home/user
echo "/home/user/common /srv/nfs/home/user none bind 0 0" >> /etc/fstab

echo "Start nfs service"
systemctl enable nfs-server
systemctl start nfs-server

systemctl restart firewalld
```

3. На виртуальной машине client перейдите в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/client/:

```
cd /vagrant/provision/client
```

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

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

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

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

```
echo "Provisioning script $0"

echo "Install needed packages"
dnf -y install nfs-utils

echo "Mounting dirs"
mkdir -p /mnt/nfs
mount server.user.net:/srv/nfs /mnt/nfs
echo "server.user.net:/srv/nfs /mnt/nfs nfs _netdev 0 0" >> /etc/fstab
restorecon -vR /etc
```

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

13.5. 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.

13.6. Контрольные вопросы

1. Как называется файл конфигурации, содержащий общие ресурсы NFS?
2. Какие порты должны быть открыты в брандмауэре, чтобы обеспечить полный доступ к серверу NFS?
3. Какую опцию следует использовать в `/etc/fstab`, чтобы убедиться, что общие ресурсы NFS могут быть установлены автоматически при перезагрузке?