NFS

Данная статья применима к:

- ОС ОН Орёл 2.12;
- ОС СН Смоленск 1.6;
- ОС СН Ленинград 8.1.

NFS (сокращение от Network File System, Сетевая Файловая Система):
сервис, обеспечивающий общий доступ к файлам и каталогам систем *nix / Linux.

NFS позволяет монтировать удалённые разделяемые файлы подобно локальным.

Существует в двух вариантах:

- вариант nfs-kernel-server, работающий на уровне ядра (входит в состав Astra Linux)
- и вариант работающий на уровне пользовательских программ (в состав Astra Linux не входит)

В ОС СН Смоленск 1.6 для того, чтобы включить NFS v2, нужно добавить оцию "-V 2" в две переменные в файле /etc/default/nfs-kernel-server (второй переменной по умолчанию нет, её надо создавать):

RPCMOUNTDOPTS="-V 2 --manage-gids"
RPCNFSDOPTS="-V 2"

Установка

Пакеты nfs (сервер) и nfs-common (клиент) входят в стандартный дистрибутив ОС СН Смоленск, и доступны в сетевом репозитории ОС ОН Орёл.
Поддержка nfs интегрирована в ядро как ОС СН, так и ОС ОН.
По умолчанию пакет nfs не устанавливается.

Установить сервер nfs и клиент nfs-common можно из графического менеджера пакетов, или из командной строки.

Сервер:

```
sudo apt update
sudo apt install nfs-kernel-server
```

Клиент:

```
sudo apt update
sudo apt install nfs-common
```

Дополнительно, можно установить пакет "монтирования ресурсов NFS по запросу", позволяющий монтировать ресурсы только при обращениях к ним:

```
sudo apt update
sudo apt install autofs
```

Настройка сервера

Подготовка

Для развёртывания сервера NFS, как и любого другого сервера, желательно назначить ему постоянный IP-адрес.
Далее в примерах считаем, что это адрес 192.168.1.10

Должно быть настроено разрешение имён клиентских компьютеров, или им должны быть назначены статические IP-адреса.

И нужно выделить ресурс, который в дальнейшем станет разделяемым.
Для примера создадим каталог /nfsshare и выставим для него полный доступ на чтение и запись:

```
sudo mkdir /srv/nfsshare && sudo chmod 777 /srv/nfsshare
```

Исправляем ошибки в пакете

Для нормального запуска и возобновления работы сервиса после перезагрузки компьютера
после установки пакета нужно внести изменения в его UNIT-файл
`/etc/systemd/system/multi-user.target.wants/nfs-server.service`
добавив следующие строки в секцию unit:

```
[Unit]
Requires=rpcbind.service
After=rpcbind.service
```

После чего перезапустить сервис:

```
sudo systemctl daemon-reload'
sudo systemctl  restart nfs-kernel-server
```

Конфигурация

Основная конфигурация сервиса nfs хранится в файле `/etc/exports`.

Кроме этого, сервис использует файлы

`/etc/fstab` - записи обо всех файловых системах, включая nfs, автоматически монтируемых при загрузке системы.

`/etc/hosts.allow`, `/etc/hosts.deny` - используется, чтобы решить, принять или отклонить подключения, приходящие с внешних IP-адресов

Экспорт разделяемого ресурса

Для экспорта созданного ранее разделяемого ресурса (каталога) /nfsshare
просто добавим в конфигурационный файл `/etc/exports` строку

> /srv/nfsshare 192.168.1.20/255.255.255.0(rw,nohide,all_squash,anonuid=1000,anongid=1000,no_subtree_check)

Где:

- 192.168.1.20 - статический адрес компьтера-клиента (может быть использовано имя)
- (rw,no_root_squash,sync) –набор опций, опции могут быть:
  - rw –чтение запись (может принимать значение ro – только чтение);
  - no_root_squash – по умолчанию в общих ресурсах NFS пользователь root становится обычным пользователем nfsnobody.
    Таким образом, владельцем всех файлов, созданных root, становится nfsnobody, что предотвращает загрузку на сервер программ с установленным битом setuid.
    Если указан параметр no_root_squash, удалённые пользователи root могут изменить любой файл в разделяемой файловой системе, и оставить для других пользователей троянские приложения.
    В целях безопасности этот параметр лучше не использовать
  - nohide - NFS автоматически не показывает нелокальные ресурсы (например, примонтированые с помощью mount –bind), эта опция включает отображение таких ресурсов;
  - sync – синхронный режим доступа (может принимать обратное значение- async).
    sync указывает, что сервер должен отвечать на запросы только после записи на диск изменений, выполненных этими запросами.

async указывает серверу не ждать записи информации на диск, что повышает производительность, но понижает надежность, т.к. в случае обрыва соединения или отказа оборудования возможна потеря данных;

- noaccess – запрещает доступ к указанной директории.
  Применяется, если доступ к определенной директории выдан всем пользователям сети , и необходимо ограничить доступ для некоторых пользователей;

- all_squash– подразумевает, что все подключения будут выполнятся от анонимного пользователя;

- subtree_check (no_subtree_check)- в некоторых случаях приходится экспортировать не весь раздел, а лишь его часть.
  При этом сервер NFS должен выполнять дополнительную проверку обращений клиентов, чтобы убедиться в том, что они предпринимают попытку доступа лишь к файлам, находящимся в соответствующих подкаталогах.
  Такой контроль поддерева (subtree checks) несколько замедляет взаимодействие с клиентами, но если отказаться от него, могут возникнуть проблемы с безопасностью системы.
  Отменить контроль поддерева можно с помощью опции no_subtree_check. Опция subtree_check, включающая такой контроль, предполагается по умолчанию.
  Контроль поддерева можно не выполнять в том случае, если экспортируемый каталог совпадает с разделом диска;

- anonuid=1000– привязывает анонимного пользователя к «местному» пользователю;

- anongid=1000– привязывает анонимного пользователя к группе «местного» пользователя.

Строк с записями о разделяемых ресурсах может быть добавлено несколько.
После внесения изменений, чтобы они вступили в силу, нужно выполнить команду

```
sudo exportfs -ra
```

(подробности по возможностям команды см. man exportfs)

Безопасный экспорт разделяемых ресурсов

- Современная версия протокола NFSv4 способна защищать всю передаваемую по сети информацию, применяя защитное преобразование данных с помощью Kerberos.
  Поэтому важно, чтобы эта служба была правильно настроена, если она находится за брандмауэром или в сегментированной сети.
  Версии NFSv2 и NFSv3 по-прежнему передают незащищённые данные.

- Сервер NFS определяет, какие файловые системы экспортировать и какие узлы получат к ним доступ с помощью файла /etc/exports.
  Будьте внимательны и не добавляйте лишних пробелов, редактируя этот файл.
  Например, следующая строка в файле /etc/exports предоставляет каталог /tmp/nfs/ для чтения/записи с компьютера master.astralinux.ru.

/tmp/nfs/ master.astralinux.ru(rw)

А эта строка файла/etc/exports, напротив, определяет для того же каталога компьютеру master.astralinux.ru
разрешение только на чтение, а всем остальным разрешает не только чтение, но и запись
Отличие состоит всего в одном пробеле после имени компьютера:

/tmp/nfs/ master.astralinux.ru (rw)

Чтобы избежать подобных ошибок,

проверяйте все настроенные общие ресурсы NFS с помощью команды showmount:

```
sudo showmount -e <hostname>
```

- Не используйте параметр no_root_squash. По умолчанию, в общих ресурсах NFS пользователь root становится обычным пользователем nfsnobody. Таким образом, владельцем всех файлов, созданных root, становится nfsnobody, что предотвращает загрузку на сервер программ с установленным битом setuid.
  Если указан параметр no_root_squash, удалённые пользователи root могут изменить любой файл в разделяемой файловой системе и оставить для других пользователей троянские приложения.

Настройка клиента

После установки клиентского пакета nfs-common, на компьютере - клиенте следует примонтировать разделяемые ресурсы.

Список доступных ресурсов можно проверить, выполнив команду:

```
showmount -e 192.168.1.10

Export list for 192.168.1.10:
/srv/nfsshare 192.168.1.20
```

Монтируем ресурс

Чтобы примонтировать разделяемый ресурс, создадим на клиентской машине каталог /share:

```
sudo mkdir /mnt/share
```

И используем команду mount для монтирования разделяемого каталога /nfsshare с сервера NFS (192.168.1.10) в каталог /mnt/share на клиентском компьютере:

```
sudo mount 192.168.1.10:/srv/nfsshare /mnt/share
```

Для проверки монтирования можно использовать команду

```
mount | grep nfs
```

которая выдаст строку (строки) с информацией о примонтированном ресурсе (ресурсах).

Кроме того, можно использовать команду проверки свободного места на всех примонтированных ресурсах:

```
df
```

Автоматически монтируем ресурс

Чтобы ресурс NFS монтировался автоматически после каждой перезагрузки, его нужно зарегистрировать в файле /etc/fstab
добавив строчку вида

192.168.1.10:/srv/nfsshare/ /mnt/share nfs rw,sync,hard,intr 0 0

Автоматически монтируем ресурс по запросу

Автоматическое монтирование ресурсов NFS можно выполнить с помощью пакета autofs