


Сетевая файловая система NFS


- Введение
- Исходные данные
- Настройка сервера
 - Подготовка
 - Корректировка настроек пакета
 - Конфигурация
 - Экспорт разделяемого ресурса
 - Безопасный экспорт разделяемых ресурсов
- Настройка клиента
 - Монтируем ресурс
 - Автоматическое монтирование ресурса при загрузке
 - Автоматическое монтирование ресурса по запросу
- Решение проблемы зависания графических приложений


Данная статья применима к:


- Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.7)
- Astra Linux Special Edition РУСБ.10152-02 (очередное обновление 4.7)
- Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.6)
- Astra Linux Special Edition РУСБ.10015-16 исп. 1 и исп. 2
- Astra Linux Special Edition РУСБ.10265-01 (очередное обновление 8.1)
- Astra Linux Common Edition 2.12

Введение

-  Защищенной сетевой файловой системой для работы с информацией ограниченного доступа в Astra Linux Special Edition является Samba SMB/CIFS. При работе в Astra Linux Special Edition с включенной политикой мандатного управления доступом (МРД) и обработкой информации ограниченного доступа применять сетевую файловую систему NFS для хранения данных в общем случае не рекомендуется.

-  NFS (сокращение от Network File System, Сетевая Файловая Система) - сервис, обеспечивающий общий доступ к файлам и каталогам систем *nix / Linux. Файловая система 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 Astra Linux Special Edition для того, чтобы включить NFS v2, нужно добавить опцию "-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"`

Исходные данные

- Сервер NFS - 192.168.1.10;
- Клиент NFS - 192.168.1.20.

Установка

Пакеты nfs-kernel-server (сервер) и nfs-common (клиент) входят в стандартный дистрибутив Astra Linux Special

Edition, и доступны в сетевом репозитории Astra Linux Common Edition. Поддержка файловой системы NFS интегрирована в ядро всех ОС Astra Linux.

По умолчанию пакет `nfs-kernel-server` не устанавливается. Установить сервер `nfs` и клиент `nfs-common` можно из графического менеджера пакетов (см. [Графический менеджер пакетов synaptic](#)), или из командной строки.



При установке пакетов для работы с файловой системой NFS будет автоматически установлена служба `rpcbind`. Использование службы `rpcbind` несовместимо с работой на ненулевых уровнях конфиденциальности. Для работы с включенным МРД на ненулевых уровнях конфиденциальности следует использовать рекомендованную сетевую файловую систему [Samba SMB/CIFS](#).

Установка сервера из командной строки:

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

Установка клиента из командной строки:

```
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, см. [Autofs монтирование по запросу](#).

Настройка сервера

Подготовка

Для развёртывания сервера NFS, как и любого другого сервера:

- рекомендуется назначить серверу постоянный IP-адрес;
- настроить разрешение имён клиентских компьютеров, или назначить им статические IP-адреса;
- выделить ресурс (каталог), который в дальнейшем станет разделяемым. Пример: создание каталога `/srv/nfsshare` и задание для него полного доступа на чтение и запись:

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

Корректировка настроек пакета

При работе в операционных системах Astra Linux, выпущенных ранее очередного обновления x.7, для нормального автоматического запуска службы `nfs-kernel-server` после перезагрузки компьютера 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
```

Указанные исправления обеспечат запуск службы `nfs-server` после службы `rpcbind`. После внесения изменений перезапустить службу:

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

При работе в Astra Linux Special Edition очередное обновление x.7 указанные действия не требуются.


Конфигурация

Основная конфигурация сервиса nfs хранится в файле `/etc/exports`. Кроме этого файла 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) `/srv/nfsshare` добавить в конфигурационный файл `/etc/exports` строку

 `/srv/nfsshare <IP-адрес_клиента>(rw,nohide,all_squash,anonuid=1000,anongid=1000,no_subtree_check)`

Где:

- `<IP-адрес_клиента>` - постоянный IP-адрес компьютера-клиента (может быть использовано имя компьютера), или, для указания группы компьютеров, можно использовать адрес сети или подстановочный знак `"*"` (подробнее см. справку `man exports`);
- `(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`. Использование параметра `no_root_squash` не рекомендуется, так как потенциально создает угрозы безопасности, связанные с возможностью удаленного внедрения в файловую систему вредоносного ПО.
 - `nohide` - NFS автоматически не показывает нелокальные ресурсы (например, примонтированные с помощью `mount –bind`), эта опция включает отображение таких ресурсов;
 - `sync` – синхронный режим доступа (может принимать обратное значение- `async`). Значение `sync` указывает, что сервер должен отвечать на запросы только после записи на диск изменений, выполненных этими запросами. Параметр `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 выполняться 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 для того, чтобы они вступили в силу, нужно выполнить команду

```
sudo exportfs -ra
```

(подробности по возможностям команды см. `man exportfs`)

Безопасный экспорт разделяемых ресурсов

- Протокол передачи данных NFS поддерживает защитное преобразование данных начиная с версии 4 (NFSv4).

❗ Версии NFSv2 и NFSv3 защитное преобразование данных не поддерживают, и передают незащищённые данные.

- Сервер NFS определяет, какие файловые системы экспортировать и какие узлы получают 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 следующая 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 конфигураций 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 рекомендуется использование параметра `no_root_squash`, так как потенциально создает угрозы безопасности, связанные с возможностью удаленного внедрения в файловую систему вредоносного ПО. По умолчанию, в общих ресурсах NFS пользователь `root` становится обычным пользователем `nfsnobody`. Таким образом, владельцем всех файлов, созданных `root`, становится пользователь `nfsnobody`, что предотвращает загрузку на сервер программ с установленным битом `setuid`.

Настройка клиента

После установки клиентского пакета `nfs-common`, на компьютере - клиенте следует примонтировать разделяемые ресурсы. Список доступных ресурсов можно проверить, выполнив команду:

```
sudo 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 на клиентской машине:

1. Создать на клиентской машине точку монтирования, например, каталог /mnt/share:

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

И Edition РУСБ.10015-01 (очередное обновление 1.6) каталог /nfsshare сервера NFS (192.168.1.10) в каталог /mnt/share на клиентском компьютере:

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

3. Для проверки успешности монтирования можно использовать команду:

```
mount | grep nfs
```

Команда выдаст строку (строки) с информацией о примонтированном ресурсе (ресурсах). Кроме того, можно использовать команду проверки свободного места на всех примонтированных ресурсах:

```
df
```

Автоматическое монтирование ресурса при загрузке

Чтобы ресурс NFS монтировался автоматически при перезагрузки ОС, его нужно зарегистрировать в файле /etc/fstab добавив строку вида

 <IP-адрес_сервера>:/srv/nfsshare/ /mnt/share nfs rw,sync,hard,intr 0 0

Автоматическое монтирование ресурса по запросу

Автоматическое монтирование ресурсов NFS можно выполнить с помощью пакета [autofs](#).

Решение проблемы зависания графических приложений

При работе в сессии с ненулевой классификационной меткой с одновременным использованием файловых систем NFS и Samba возможна нештатная работа графических приложений. Нарушение работы приложения может проявляться, например, "в зависаниях" текстового редактора kate, и вызвано несовместимостью службы rpcbind с работой KC3 Astra Linux Special Edition. Для устранения нарушений работы следует остановить и запретить службу rpcbind:

```
sudo systemctl mask --now rpcbind
```

Для находящихся в эксплуатации систем Astra Linux следует использовать рекомендованную для работы с информацией ограниченного доступа сетевую файловую систему Samba SMB/CIFS.