**Глава 12. Совместное использование данных в частной сети.**

Предоставление отобранных частей файловой системы сервера для удленных ДОВЕРЕННЫХ клиентов с целью совместного использования файлов и документов на основе NFS (Network File System).

**1. Настройка NFS-сервера**

**Установка:**

* nfs-kernel-server (Ubuntu)
* nfs-utils (CentOS)

**Настройка сервера:**

Файл конфигурации с которым нужно работать: /etc/exports, изначально он должен содержать несолько закомментированных примеров. Так, там может быть:

* /home 192.168.1.11(rw,sync)
  + home - открыть доступ к каталогу на сервере
  + ip – адрес клиента, которому нужно предоставить доступ.
  + rw- чтение и запись
  + sync-записывает изменения на диск перед ответом на удаленный запрос.

Значения NFS по умолчанию ro(только запись) и root\_squash(удаленным клиентам нельзя выполнять запросы от root). Такие **настройки по умолчанию хорошо подходят для библиотеки**.

Разрешить действовать под root удаленно поможет параметр no\_root\_squash:

* /home 192.168.1.11(rw,sync,no\_root\_squash)

Чтобы разрешить любому пользователю локальной сети иметь доступ к каталогу:

* /home 192.168.1.0/255.255.255.0(rw,sync) (Но НЕ ДЕЛАТЬ ТАК для общедоступных сетей, где пользователи могут подключаться по WI-FI)

**ПРИМЕЧАНИЕ**: писать ip(rw,sync) надо без пробела, поставив пробел - это будут уже 2 разных условия, которые определят, что пользователь с ip имеет доступ по умолчанию (чтение), а все отсальные могут делать (rw,sync).

По завершении настройки следует обновить настрйоки NFS, запустив exportfs:

* exportfs -ra (r-синхронизировать ФС, a-применить ко всем каталогам)

Посмотреть все ФС NFS:

* exportfs

**Настройка файервола для разрешения достпуа по nfs (иногда может слетать):**

* firewall-cmd –add-service=nfs || firewall-cmd –add-port=2049/tcp
* Перезагрузим : firewall-cmd --reload

**Запуск сервера :**

* sudo service nfs-kernel-server start (для Ubuntu)
* systemctlstart nfs-server **(для CentOS)**

**Информация о портах сервера:**

* rpcinfo -p | grep nfs (должно что-то выдать)

P.S. Если не пашет с 1 раза, то это ок, надо все проверять, ососбенно файервол и порты.

**2. Настройка NFS-клиента**

Установка:

* nfs-common (Ubuntu)
* nfs-utils (CentOS)

На клиенте нужно создать каталог, который будет хранить данные сервера и привязать каталог к серверу:

* mkdir -p /*nfs*/home/ (-p – создать любые катлоги, если они не существуют)
* mount ip\_server:/home /*nfs/home/*

**3. Монтирование при загрузке**

Проделанные ранее действия позволяют клиенту получить доступ к файлам, но при перезагрузке все настройки слетят и придется снова монтировать раздел командой (mount). Чтобы Linux автоматически монтировала образ при загрузке, следует добавить его в файл /etc/fstab (Каждое поле имеет свою функцию, подробнее в интернете...):

* ip\_addr\_server:/home /*nfs/home nfs*

Надо будет перезагрузить компьютер, затем проверить работу файла можно будет так:

* mount (команда выведет смонтированные ФС).

**4. Безопасность NFS**

Хакеры всегда могут найти способ проникнуть в систему, поэтому первый принцип частной сети: **принцип наименьших привилегий**. Давать пользователям доступ только к тому, что им необходимо. (Если клиентам не следует давать доступ к редактированию, то можно поставить доступ ro в etc/exports).

1) Файервол

Можно блокировать пользователей к доступу на сервер:

* ufw deny to 192.168.1.10

Можно заблокировать доступ только к NFS, оставляя доступ к другим ресурсам (например к Apache) :

* ufw deny from 192.168.0.10 to any port 2049

Так мы не сможем получить доступ только по web-приложению, проверить можно так:

* ls */nfs/home/*
* *curl 192.168.0.3*

2) Шифрование.

Шифрование в NFS не предусматривается, т.к. подразумеваестя его использование в частной сети. НО любые данные, которые перемещаются по небезопасным сетям, требуют дополнительной защиты.

Способы:

* Запуск NFS поверх VPN
* IPSec (но при условии, что он действует по всему маршруту)
* NFS через SSH (давольно нестандартный вариант)
* Если есть Kerberos (NFS v.4…). Исп: sec=krb5p
* Альтернатива SSH → SSH(SSHFS) на основе FUSE.