

A dark blue vertical bar runs along the left edge of the page. A blue arrow-shaped banner points to the right from this bar, containing the text 'mayo de 2021'. In the bottom-left corner, there are several thin, curved, light blue lines that sweep upwards and to the right.

mayo de 2021

Practica 6

Servidor de disco NFS

Carlos Garcia Segura
SWAP

Índice

1. [Creación y configuración del servidor NFS.](#)
2. [Configuración de los clientes M1 y M2.](#)
3. [Seguridad en el servidor NFS.](#)

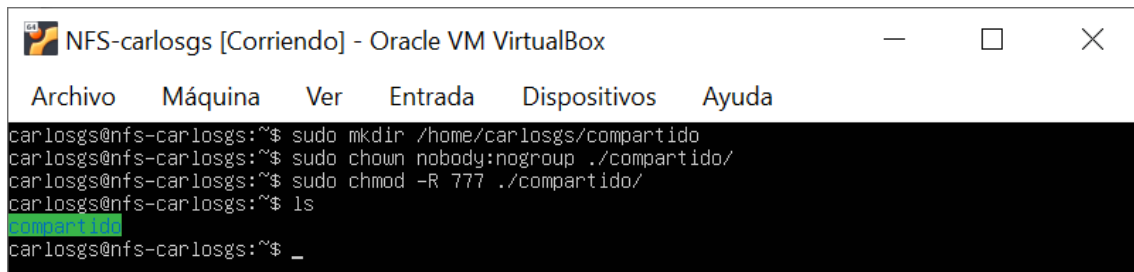
1. Creación y configuración del servidor NFS

- Una vez hemos creado la máquina virtual con Ubuntu server y los adaptadores de red tanto “NAT” como “solo anfitrión” tal y como hicimos en la practica 1. Lo siguiente será instalar en ella las herramientas necesarias para utilizarla como servidor NFS.

```
sudo apt-get install nfs-kernel-server nfs-common rpcbind
```

- Lo siguiente que debemos hacer es crear la carpeta que vamos a compartir con los clientes cambiando los permisos y el propietario de la carpeta.

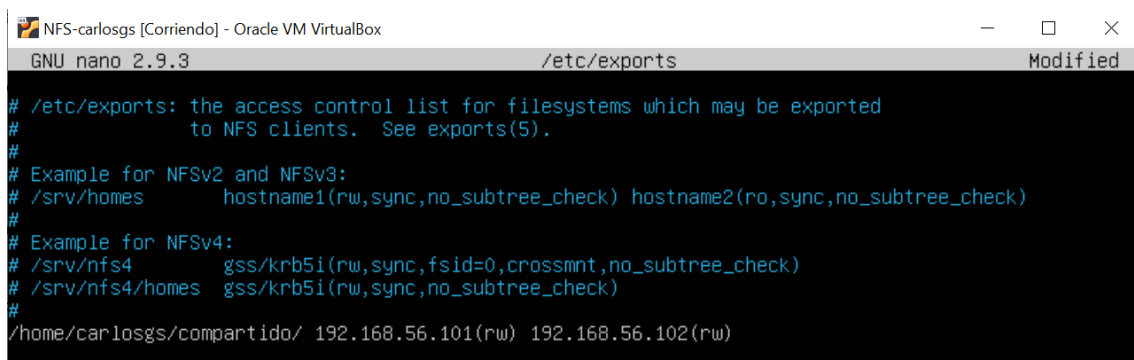
```
sudo mkdir /home/carlosgs/compartido
sudo chown nobody:nogroup /home/carlosgs/compartido/
sudo chmod -R 777 /home/carlosgs/compartido/
```



```
NFS-carlosgs [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
carlosgs@nfs-carlosgs:~$ sudo mkdir /home/carlosgs/compartido
carlosgs@nfs-carlosgs:~$ sudo chown nobody:nogroup ./compartido/
carlosgs@nfs-carlosgs:~$ sudo chmod -R 777 ./compartido/
carlosgs@nfs-carlosgs:~$ ls
compartido
carlosgs@nfs-carlosgs:~$ _
```

- A continuación, debemos darle permiso de acceso a las maquinas cliente añadiendo en el archivo de configuración “/etc/exports” la siguiente línea.

```
/home/carlosgs/compartido/ IP_M1(rw) IP_M2(rw)
```



```
NFS-carlosgs [Corriendo] - Oracle VM VirtualBox
GNU nano 2.9.3 /etc/exports Modified
# /etc/exports: the access control list for filesystems which may be exported
# to NFS clients.  See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/homes hostname1(rw,sync,no_subtree_check) hostname2(ro,sync,no_subtree_check)
#
# Example for NFSv4:
# /srv/nfs4 gss/krb5i(rw,sync,fsid=0,crossmnt,no_subtree_check)
# /srv/nfs4/homes gss/krb5i(rw,sync,no_subtree_check)
#
/home/carlosgs/compartido/ 192.168.56.101(rw) 192.168.56.102(rw)
```

- Finalmente reiniciamos el servicio y comprobamos que todo está correcto.

```
sudo service nfs-kernel-server restart
sudo service nfs-kernel-server status
```

```
NFS-carlosgs [Corriendo] - Oracle VM VirtualBox
carlosgs@nfs-carlosgs:~$ sudo service nfs-kernel-server restart
carlosgs@nfs-carlosgs:~$ sudo service nfs-kernel-server status
• nfs-server.service - NFS server and services
   Loaded: loaded (/lib/systemd/system/nfs-server.service; enabled; vendor preset: enabled)
   Active: active (exited) since Thu 2021-05-27 17:05:02 UTC; 4s ago
     Process: 2925 ExecStopPost=/usr/sbin/exportfs -f (code=exited, status=0/SUCCESS)
     Process: 2924 ExecStopPost=/usr/sbin/exportfs -au (code=exited, status=0/SUCCESS)
     Process: 2922 ExecStop=/usr/sbin/rpc.nfsd 0 (code=exited, status=0/SUCCESS)
     Process: 2941 ExecStart=/usr/sbin/rpc.nfsd $RPCNFSDARGS (code=exited, status=0/SUCCESS)
     Process: 2940 ExecStartPre=/usr/sbin/exportfs -r (code=exited, status=0/SUCCESS)
    Main PID: 2941 (code=exited, status=0/SUCCESS)

May 27 17:05:02 nfs-carlosgs systemd[1]: Starting NFS server and services...
May 27 17:05:02 nfs-carlosgs exportfs[2940]: exportfs: /etc/exports [1]: Neither 'subtree_check' or
May 27 17:05:02 nfs-carlosgs exportfs[2940]: Assuming default behaviour ('no_subtree_check').
May 27 17:05:02 nfs-carlosgs exportfs[2940]: NOTE: this default has changed since nfs-utils versio
May 27 17:05:02 nfs-carlosgs exportfs[2940]: exportfs: /etc/exports [1]: Neither 'subtree_check' or
May 27 17:05:02 nfs-carlosgs exportfs[2940]: Assuming default behaviour ('no_subtree_check').
May 27 17:05:02 nfs-carlosgs exportfs[2940]: NOTE: this default has changed since nfs-utils versio
May 27 17:05:02 nfs-carlosgs systemd[1]: Started NFS server and services.
lines 1-18/18 (END)
```

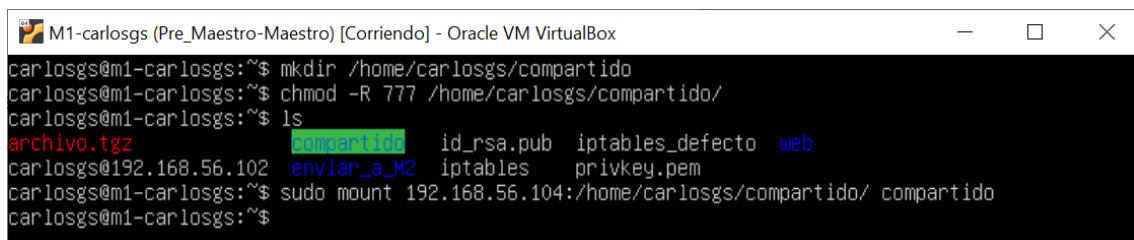
2. Configuración de los clientes M1 y M2

- Lo primero que debemos hacer es instalar en ambas maquinas los paquetes necesarios y crear el directorio sobre el que se va a montar la carpeta remota.

```
sudo apt-get install nfs-common rpcbind
mkdir /home/carlosgs/compartido
chmod -R 777 /home/carlosgs/compartido
```

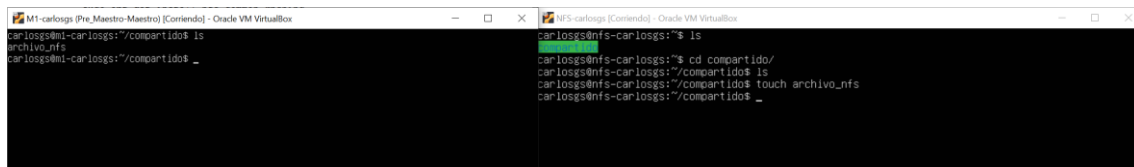
- Ahora debemos montar la carpeta remota sobre el directorio que acabamos de crear.

```
cd /home/carlosgs/
sudo mount IP_ServidorNFS:/home/carlosgs/compartido compartido
```



```
M1-carlosgs (Pre_Maestro-Maestro) [Corriendo] - Oracle VM VirtualBox
carlosgs@m1-carlosgs:~$ mkdir /home/carlosgs/compartido
carlosgs@m1-carlosgs:~$ chmod -R 777 /home/carlosgs/compartido/
carlosgs@m1-carlosgs:~$ ls
archivo.tgz      compartido      id_rsa.pub      iptables_defecto  web
carlosgs@192.168.56.102 enviar_a_M2 iptables privkey.pem
carlosgs@m1-carlosgs:~$ sudo mount 192.168.56.104:/home/carlosgs/compartido/ compartido
carlosgs@m1-carlosgs:~$
```

- Podemos comprobar que si creamos un archivo en el servidor NFS o en cualquiera de las maquinas este estará disponible para lectura y escritura en cualquiera de las 3 máquinas.



```
M1-carlosgs (Pre_Maestro-Maestro) [Corriendo] - Oracle VM VirtualBox
carlosgs@m1-carlosgs:~/compartido$ ls
archivo_nfs
carlosgs@m1-carlosgs:~/compartido$ _

NFS-carlosgs [Corriendo] - Oracle VM VirtualBox
carlosgs@nfs-carlosgs:~$ ls
carlosgs@nfs-carlosgs:~$ cd compartido/
carlosgs@nfs-carlosgs:~/compartido$ ls
carlosgs@nfs-carlosgs:~/compartido$ touch archivo_nfs
carlosgs@nfs-carlosgs:~/compartido$ _
```

- Por último, para que la configuración sea permanente, montándose la carpeta compartida automáticamente al arrancar el sistema, debemos añadir lo siguiente al archivo de configuración “**/etc/fstab**” (Todo en una sola línea).

```
192.168.56.104:/home/carlosgs/compartido /home/carlosgs/compartido/ nfs
auto,noatime,nolock,bg,nfsvers=3,intr,tcp,actimeo=1800 0 0
```

```
M1-carlosgs (Pre_Maestro-Maestro) [Corriendo] - Oracle VM VirtualBox
GNU nano 2.9.3 /etc/fstab

# /etc/fstab: static file system information.
#
# Use 'blkid' to print the universally unique identifier for a
# device; this may be used with UUID= as a more robust way to name devices
# that works even if disks are added and removed. See fstab(5).
#
# <file system> <mount point> <type> <options> <dump> <pass>
# / was on /dev/ubuntu-vg/ubuntu-lv during curtin installation
/dev/disk/by-id/dm-uuid-LVM-VE9HmSHdVwPW2B7sMN0hgY1hdCgDnhKhjqCk2zc0Xbu82Dx0TTfhKrpz0AXBPgvI / ext4$
# /boot was on /dev/sda2 during curtin installation
/dev/disk/by-uuid/e4c8b7c8-1da7-4465-b071-6af3044c404 /boot ext4 defaults 0 0
/swap.img none swap sw 0 0

192.168.56.104:/home/carlosgs/compartido /home/carlosgs/compartido/ nfs auto,noatime,nolock,bg,nfsv$
```

La consola no muestra la línea de texto al completo.

```
M1-carlosgs (Pre_Maestro-Maestro) [Corriendo] - Oracle VM VirtualBox

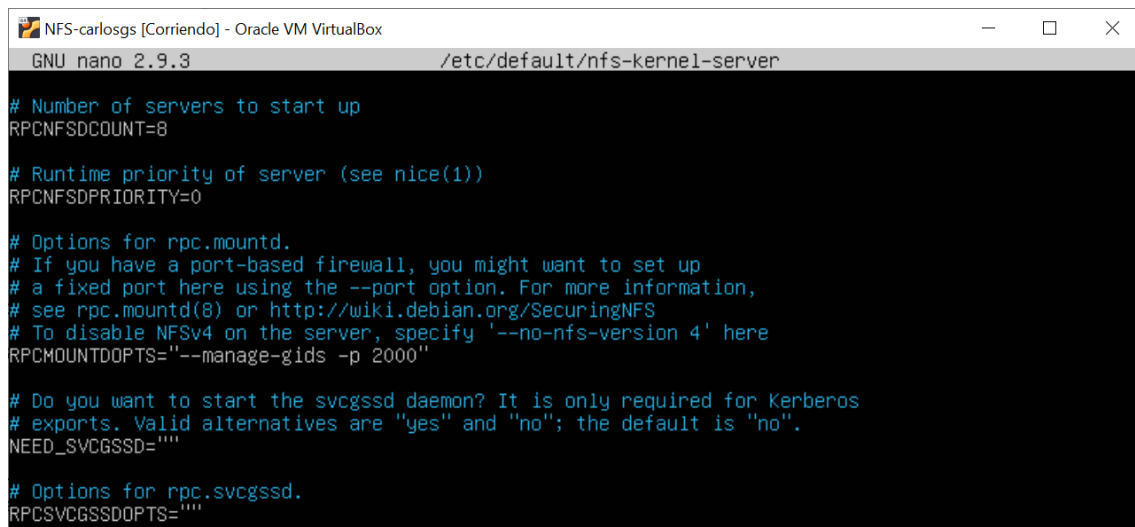
carlosgs@m1-carlosgs:~$ ls
archivo.tgz  compartido  id_rsa.pub  iptables_defecto  web
carlosgs@192.168.56.102 enviar_a_M2  iptables      privkey.pem
carlosgs@m1-carlosgs:~$ cd compartido/
carlosgs@m1-carlosgs:~/compartido$ ls
archivo_nfs  post_reinicio
carlosgs@m1-carlosgs:~/compartido$
```

3. Seguridad en el servidor NFS

En cuanto a la seguridad del servidor NFS, vamos a hacer que únicamente acepte el tráfico necesario para que funcione el servicio en las maquinas M1 y M2.

- Lo primero que debemos hacer es configurar los servicios mountd y nlockmgr para que usen un puerto específico.
 - Para mountd editamos el archivo **“/etc/default/nfs-kernel-server”** y añadimos:

```
RPCMOUNTDOPTS="--manage-gids -p 2000"
```



The screenshot shows a terminal window titled "NFS-carlos [Corriendo] - Oracle VM VirtualBox". The terminal is running GNU nano 2.9.3 and editing the file /etc/default/nfs-kernel-server. The visible content includes comments about the number of servers, runtime priority, and options for rpc.mountd. The line RPCMOUNTDOPTS="--manage-gids -p 2000" is highlighted in blue.

```
GNU nano 2.9.3 /etc/default/nfs-kernel-server

# Number of servers to start up
RPCNFSDCOUNT=8

# Runtime priority of server (see nice(1))
RPCNFSDPRIORITY=0

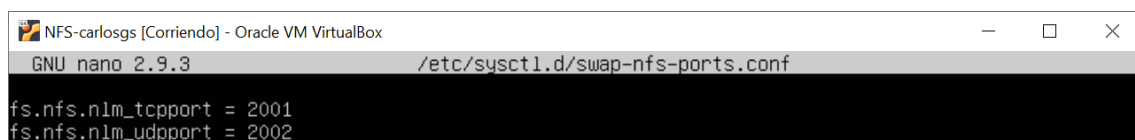
# Options for rpc.mountd.
# If you have a port-based firewall, you might want to set up
# a fixed port here using the --port option. For more information,
# see rpc.mountd(8) or http://wiki.debian.org/SecuringNFS
# To disable NFSv4 on the server, specify '--no-nfs-version 4' here
RPCMOUNTDOPTS="--manage-gids -p 2000"

# Do you want to start the svcgssd daemon? It is only required for Kerberos
# exports. Valid alternatives are "yes" and "no"; the default is "no".
NEED_SVCGSSD=""

# Options for rpc.svcgssd.
RPCSVCGSSDOPTS=""
```

- Para nlockmgr debemos crear el archivo **“swap-nfs-ports.conf”** en **“/etc/sysctl.d/”** y añadir las siguientes opciones:

```
fs.nfs.nlm_tcpport = 2001
fs.nfs.nlm_udpport = 2002
```



The screenshot shows a terminal window titled "NFS-carlos [Corriendo] - Oracle VM VirtualBox". The terminal is running GNU nano 2.9.3 and editing the file /etc/sysctl.d/swap-nfs-ports.conf. The visible content shows the two configuration lines for fs.nfs.nlm_tcpport and fs.nfs.nlm_udpport.

```
GNU nano 2.9.3 /etc/sysctl.d/swap-nfs-ports.conf

fs.nfs.nlm_tcpport = 2001
fs.nfs.nlm_udpport = 2002
```

Después de esto tenemos que crear lanzar el nuevo archivo que acabamos de crear.

```
sudo sysctl --system
/etc/init.d/nfs-kernel-server restart
```

```
NFS-carlosgs [Corriendo] - Oracle VM VirtualBox
* Applying /etc/sysctl.d/10-ipv6-privacy.conf ...
net.ipv6.conf.all.use_tempaddr = 2
net.ipv6.conf.default.use_tempaddr = 2
* Applying /etc/sysctl.d/10-kernel-hardening.conf ...
kernel.kptr_restrict = 1
* Applying /etc/sysctl.d/10-link-restrictions.conf ...
fs.protected_hardlinks = 1
fs.protected_symlinks = 1
* Applying /etc/sysctl.d/10-lxd-inotify.conf ...
fs.inotify.max_user_instances = 1024
* Applying /etc/sysctl.d/10-magic-sysrq.conf ...
kernel.sysrq = 176
* Applying /etc/sysctl.d/10-network-security.conf ...
net.ipv4.conf.default.rp_filter = 1
net.ipv4.conf.all.rp_filter = 1
net.ipv4.tcp_syncookies = 1
* Applying /etc/sysctl.d/10-pttrace.conf ...
kernel.yama.pttrace_scope = 1
* Applying /etc/sysctl.d/10-zero-page.conf ...
vm.mmap_min_addr = 65536
* Applying /usr/lib/sysctl.d/50-default.conf ...
net.ipv4.conf.all.promote_secondaries = 1
net.core.default_qdisc = fq_codel
* Applying /etc/sysctl.d/99-sysctl.conf ...
* Applying /etc/sysctl.d/swap-nfs-ports.conf ...
fs.nfs.nlm_tcpport = 2001
fs.nfs.nlm_udpport = 2002
* Applying /etc/sysctl.conf ...
carlosgs@nfs-carlosgs:~$ /etc/init.d/nfs-kernel-server restart
[...] Restarting nfs-kernel-server (via systemctl): nfs-kernel-server.service==== AUTHENTICATING FOR
org.freedesktop.systemd1.manage-units ===
Authentication is required to restart 'nfs-server.service'.
Authenticating as: Carlos Garcia Segura (carlosgs)
Password:
==== AUTHENTICATION COMPLETE ====
. ok
carlosgs@nfs-carlosgs:~$
```

- Para comprobar los puertos asociados a cada servicio usamos.

sudo rpcinfo -p localhost

```
NFS-carlosgs [Corriendo] - Oracle VM VirtualBox
carlosgs@nfs-carlosgs:~$ sudo rpcinfo -p localhost
program vers proto port service
100000 4 tcp 111 portmapper
100000 3 tcp 111 portmapper
100000 2 tcp 111 portmapper
100000 4 udp 111 portmapper
100000 3 udp 111 portmapper
100000 2 udp 111 portmapper
100005 1 udp 2000 mountd
100005 1 tcp 2000 mountd
100005 2 udp 2000 mountd
100005 2 tcp 2000 mountd
100005 3 udp 2000 mountd
100005 3 tcp 2000 mountd
100003 3 tcp 2049 nfs
100003 4 tcp 2049 nfs
100227 3 tcp 2049
100003 3 udp 2049 nfs
100227 3 udp 2049
100021 1 udp 2002 nlockmgr
100021 3 udp 2002 nlockmgr
100021 4 udp 2002 nlockmgr
100021 1 tcp 2001 nlockmgr
100021 3 tcp 2001 nlockmgr
100021 4 tcp 2001 nlockmgr
carlosgs@nfs-carlosgs:~$ _
```


- Por último, creamos un script de iptables en el que denegamos el tráfico entrante y abrimos los siguientes puertos.
 - 2049 udp y tcp para NFS
 - 111 tcp y udp para portmapper
 - 2000 udp y tcp para mountd
 - 2001 tcp y 2002 udp para nlockmgr

```

NFS-carlosgs [Corriendo] - Oracle VM VirtualBox
GNU nano 2.9.3 iptables
#!/bin/bash

# (1) se eliminan todas las reglas que hubiera
#para hacer la configuracion limpia:
sudo iptables -F
sudo iptables -X
sudo iptables -Z

# (2) establecer las politicas por defecto (denegar todo el trafico entrante):
sudo iptables -P INPUT DROP
sudo iptables -P OUTPUT ACCEPT
sudo iptables -P FORWARD DROP
sudo iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

# (3) añadimos las reglas para aceptar las conexiones entrantes desde el balanceador
sudo iptables -A INPUT -p tcp -m multiport --ports 2049,111,2000,2001 -j ACCEPT
sudo iptables -A INPUT -p udp -m multiport --ports 2049,111,2000,2002 -j ACCEPT

```

- Lo ejecutamos con:

```
sudo bash ./iptables
```

```

NFS-carlosgs [Corriendo] - Oracle VM VirtualBox
carlosgs@nfs-carlosgs:~/compartido$ touch post-iptables
carlosgs@nfs-carlosgs:~/compartido$ ls
post-iptables
carlosgs@nfs-carlosgs:~/compartido$

M1-carlosgs (Pre_Maestro-Maestro) [Corriendo] - Oracle VM VirtualBox
carlosgs@m1-carlosgs:~/compartido$ ls
post-iptables
carlosgs@m1-carlosgs:~/compartido$

M2-carlosgs (Pre_Maestro-Maestro) [Corriendo] - Oracle VM VirtualBox
carlosgs@m2-carlosgs:~/compartido$ ls
post-iptables
carlosgs@m2-carlosgs:~/compartido$

```