

Practica 6

Autor: Antonio Jesús Heredia Castillo

Configuración servidor

Lo primero que tenemos que realizar es crear la carpeta, cambiarla de grupo y darle los permisos oportunos.

```
antoni-heredia@m3:~$ sudo mkdir /datos
antoni-heredia@m3:~$ sudo mkdir /datos/compartido
antoni-heredia@m3:~$ sudo chown nobody:nogroup /datos/compartido/
antoni-heredia@m3:~$ sudo chmod -R 777 /datos/compartido/
antoni-heredia@m3:~$ _
```

Editamos el fichero `/etc/export` indicando cual es la carpeta que queremos compartir y con cuales dispositivos.

```
GNU nano 2.9.3 /etc/exports

# /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)
#
/datos/compartido/ 192.168.56.101(rw) 192.168.56.102(rw)
```

Reiniciamos el servidor NFS para que coja la nueva configuración

```
antoni-heredia@m3:~$ sudo service nfs-kernel-server restart
antoni-heredia@m3:~$ 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 Fri 2020-05-22 10:56:34 UTC; 2s ago
     Process: 3118 ExecStopPost=/usr/sbin/exportfs -f (code=exited, status=0/SUCCESS)
     Process: 3117 ExecStopPost=/usr/sbin/exportfs -au (code=exited, status=0/SUCCESS)
     Process: 2998 ExecStop=/usr/sbin/rpc.nfsd 0 (code=exited, status=0/SUCCESS)
     Process: 3160 ExecStart=/usr/sbin/rpc.nfsd $RPCNFSDARGS (code=exited, status=0/SUCCESS)
     Process: 3159 ExecStartPre=/usr/sbin/exportfs -r (code=exited, status=0/SUCCESS)
    Main PID: 3160 (code=exited, status=0/SUCCESS)

may 22 10:56:34 m3 exportfs[3159]: exportfs: /etc/exports [1]: Neither 'subtree_check' or 'no_subtree
may 22 10:56:34 m3 exportfs[3159]:   Assuming default behaviour ('no_subtree_check').
may 22 10:56:34 m3 exportfs[3159]:   NOTE: this default has changed since nfs-utils version 1.0.x
may 22 10:56:34 m3 exportfs[3159]: exportfs: /etc/exports [1]: Neither 'subtree_check' or 'no_subtree
may 22 10:56:34 m3 exportfs[3159]:   Assuming default behaviour ('no_subtree_check').
may 22 10:56:34 m3 exportfs[3159]:   NOTE: this default has changed since nfs-utils version 1.0.x
may 22 10:56:34 m3 systemd[1]: Starting NFS server and services...
may 22 10:56:34 m3 systemd[1]: Started NFS server and services.
lines 1-18/18 (END)
```

Acceso a carpetas remotas

Metodo manual

Podemos montar las carpetas, de forma manual, siempre que queramos con el comando **mount**, como podemos ver en la siguiente imagen se tiene acceso a los ficheros de forma instantánea.

```
the dbus.service is a disabled or a static unit, not starting it.
Procesando disparadores para systemd (237-3ubuntu10.38) ...
Procesando disparadores para man-db (2.8.3-2ubuntu0.1) ...
Procesando disparadores para ureadahead (0.100.0-21) ...
Procesando disparadores para libc-bin (2.27-3ubuntu1) ...
antoni-heredia@m2:~$ mkdir datos
antoni-heredia@m2:~$ sudo mount 192.168.56.103:/datos/compartido datos
antoni-heredia@m2:~$ ls datos/
file.txt
antoni-heredia@m2:~$ ls datos
file2.txt file.txt
antoni-heredia@m2:~$
```

Como podemos ver, también puedo crear ficheros desde las maquinas clientes y aparece en la maquina servidor:

```
antoni-heredia@m3:~$ touch /datos/compartido/file.txt
antoni-heredia@m3:~$ touch /datos/compartido/file2.txt
antoni-heredia@m3:~$ ls /datos/compartido/
file2.txt file.txt
antoni-heredia@m3:~$ ls /datos/compartido/
ficheroM2.txt file2.txt file.txt
antoni-heredia@m3:~$ _
```

Proceso automatico

Para que se monte de forma automatica cuando iniciamos el servidor vale con que añadamos lo siguiente al fichero **/etc/fstab**:

```
192.168.56.103:/datos/compartido /home/usuario/datos/ nfs auto,noatime,nolock,bg,nfsvers=3,
```

Para que se monte sin tener que reiniciar podemos volver a usar el comando **mount** con la opción **-a**.

```
antoni-heredia@m1:~$ ls datos/
antoni-heredia@m1:~$ sudo mount -a
antoni-heredia@m1:~$ ls datos/
ficheroM2.txt file2.txt file.txt
antoni-heredia@m1:~$ _
```

Seguridad del servidor

Una vez que hemos cambiado los puertos que se nos indica en el guion, reiniciamos el servicio:

```
antoni-heredia@m3:~$ /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: Antonio Jesús Heredia Castillo (antoni-heredia)
Password:
==== AUTHENTICATION COMPLETE ===
. ok
antoni-heredia@m3:~$ _
```

Podemos ver como los puertos son los que hemos indicado con el siguiente comando:

```
antoni-heredia@m3:~$ 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 55389 mountd
100005 1 tcp 36797 mountd
100005 2 udp 60519 mountd
100005 2 tcp 47991 mountd
100005 3 udp 44340 mountd
100005 3 tcp 38873 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
antoni-heredia@m3:~$ _
```

Luego ejecutamos el script de iptables que contiene las siguientes reglas:

```
antoni-heredia@m3:~$ sudo nano /etc/iptables
antoni-heredia@m3:~$ cat cortafuegoNFS.sh
# denegamos todo el trafico por defecto
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP
iptables -A INPUT -m state --state NEW,ESTABLISHED -j ACCEPT

iptables -A INPUT -s 192.168.56.101,192.168.56.102 -p tcp -m multiport --ports 111,2000,2001,2049 -j ACCEPT
iptables -A INPUT -s 192.168.56.101,192.168.56.102 -p udp -m multiport --ports 111,2000,2001,2049 -j ACCEPT
antoni-heredia@m3:~$ _
```

Podemos ver como es imposible montar la carpeta desde otra maquina que no sean M1 o M2:

```
(base) ✖ antonio@antonio-Lenovo-Y520-15IKBN ~$ sudo mount 10.0.2.17:/compartido/datos datos
```

Se queda “pensando” y no funciona.