```
-> CONFIGURACIÓN NFS EN EL SERVIDOR (en este caso, coincidirá con el KDC).

-> ¿Contamos con el paquete nfs-utils?

[root@servidor ~]# rpm -qa | grep -i nfs-utils
nfs-utils-1.2.4-3.fc15.i686

-> Lo primero es comprobar que "rpcbind" y "nfs" están lanzados y programados
para iniciarse automáticamente al arrancar:

[root@servidor ~]# /etc/init.d/rpcbind status
rpcbind.service - SYSV: The rpcbind utility is a server that converts RPC program numbers into universal addresses. It must be
running on the host to be able to make RPC calls on a server on that machine.
      Loaded: loaded (/etc/rc.d/init.d/rpcbind)
      Active: active (running) since Sat, 21 Apr 2012 10:11:57 +0200; 1h 12min ago
     Process: 1050 ExecStart=/etc/rc.d/init.d/rpcbind start (code=exited, status=0/SUCCESS)
    Main PID: 1118 (rpcbind)
      CGroup: name=systemd:/system/rpcbind.service
          └ 1118 rpcbind
[root@servidor ~]# /etc/init.d/nfs status
rpcsvcgssd.service - LSB: Starts the RPCSEC GSS server daemon
      Loaded: loaded (/etc/rc.d/init.d/rpcsvcgssd)
      Active: inactive (dead)
      CGroup: name=systemd:/system/rpcsvcgssd.service
nfs.service - LSB: Start up the NFS server sevice
      Loaded: loaded (/etc/rc.d/init.d/nfs)
      Active: inactive (dead)
      CGroup: name=systemd:/system/nfs.service
nfs.service - LSB: Start up the NFS server sevice
      Loaded: loaded (/etc/rc.d/init.d/nfs)
      Active: inactive (dead)
      CGroup: name=systemd:/system/nfs.service
nfs.service - LSB: Start up the NFS server sevice
      Loaded: loaded (/etc/rc.d/init.d/nfs)
      Active: inactive (dead)
      CGroup: name=systemd:/system/nfs.service
[root@servidor ~]# /etc/init.d/nfs start
Starting nfs (via systemctl):                              [  OK  ]
[root@servidor ~]# /etc/init.d/nfs status
```

```
rpcsvcgssd.service - LSB: Starts the RPCSEC GSS server daemon
      Loaded: loaded (/etc/rc.d/init.d/rpcsvcgssd)
      Active: active (exited) since Sat, 21 Apr 2012 11:24:41 +0200; 3s ago
     Process: 2323 ExecStart=/etc/rc.d/init.d/rpcsvcgssd start (code=exited, status=6/NOTCONFIGURED)
      CGroup: name=systemd:/system/rpcsvcgssd.service
nfs.service - LSB: Start up the NFS server sevice
      Loaded: loaded (/etc/rc.d/init.d/nfs)
      Active: active (running) since Sat, 21 Apr 2012 11:24:41 +0200; 2s ago
     Process: 2297 ExecStart=/etc/rc.d/init.d/nfs start (code=exited, status=0/SUCCESS)
      CGroup: name=systemd:/system/nfs.service
          ├ 2338 rpc.rquotad
          └ 2354 rpc.mountd
nfs.service - LSB: Start up the NFS server sevice
      Loaded: loaded (/etc/rc.d/init.d/nfs)
      Active: active (running) since Sat, 21 Apr 2012 11:24:41 +0200; 2s ago
     Process: 2297 ExecStart=/etc/rc.d/init.d/nfs start (code=exited, status=0/SUCCESS)
      CGroup: name=systemd:/system/nfs.service
          ├ 2338 rpc.rquotad
          └ 2354 rpc.mountd
nfs.service - LSB: Start up the NFS server sevice
      Loaded: loaded (/etc/rc.d/init.d/nfs)
      Active: active (running) since Sat, 21 Apr 2012 11:24:41 +0200; 2s ago
     Process: 2297 ExecStart=/etc/rc.d/init.d/nfs start (code=exited, status=0/SUCCESS)
      CGroup: name=systemd:/system/nfs.service
          ├ 2338 rpc.rquotad
          └ 2354 rpc.mountd
[root@servidor ~]# chkconfig --list nfs

Nota: Este resultado muestra solo los srvicios SysV y no incluye servicios
      nativos systemd. Los datos de configuración de SysV podrían ser
      sobreescritos por la configuración nativa de systemd.

nfs             0:desactivado   1:desactivado   2:desactivado   3:desactivado   4:desactivado   5:desactivado   6:desactivado
[root@servidor ~]# chkconfig --level 35 nfs on
[root@servidor ~]# chkconfig --list nfs

Nota: Este resultado muestra solo los srvicios SysV y no incluye servicios
      nativos systemd. Los datos de configuración de SysV podrían ser
      sobreescritos por la configuración nativa de systemd.
```

```
nfs             0:desactivado   1:desactivado   2:desactivado   3:activo    4:desactivado   5:activo    6:desactivado
[root@servidor ~]#

-> CONFIGURAMOS EL CORTAFUEGOS (el servidor NFS escucha a través del puerto 2049):

[root@servidor ~]# cat /etc/sysconfig/iptables | grep 2049
-A INPUT -m state --state NEW -m tcp -p tcp --dport 2049 -j ACCEPT
[root@servidor ~]# /etc/init.d/iptables restart
Restarting iptables (via systemctl):                       [  OK  ]

-> CONFIGURAMOS "/etc/exports" PARA DAR ACCESO AL DIRECTORIO
/usr/share/docpublicos DEL KDC, EN MODO DE SÓLO LECTURA,
A TODOS LOS USUARIOS DE LA RED 155.54.225.0/24.

[root@servidor ~]# mkdir /usr/share/docpublicos
[root@servidor ~]# ls -ld /usr/share/docpublicos
drwxr-xr-x. 2 root root 4096 abr 21 11:35 /usr/share/docpublicos
[root@servidor ~]# cat > /usr/share/docpublicos/doc01.txt
Contenido de "doc01.txt"
[root@servidor ~]# vi /etc/exports
[root@servidor ~]# cat /etc/exports
/usr/share/docpublicos  155.54.225.0/24(ro)
[root@servidor ~]# exportfs -v
[root@servidor ~]# /etc/init.d/nfs restart
Restarting nfs (via systemctl):                            [  OK  ]
[root@servidor ~]# exportfs -v
/usr/share/docpublicos
        155.54.225.0/24(ro,wdelay,root_squash,no_subtree_check)

-> AHORA, EN EL CLIENTE:

[root@pc2 ~]# hostname
pc2.lab2701.aso
[root@pc2 ~]# /etc/init.d/rpcbind status
rpcbind.service - SYSV: The rpcbind utility is a server that converts RPC program numbers into universal addresses. It must be
running on the host to be able to make RPC calls on a server on that machine.
      Loaded: loaded (/etc/rc.d/init.d/rpcbind)
      Active: active (running) since Sat, 21 Apr 2012 10:12:29 +0200; 1h 41min ago
```

```
     Process: 1088 ExecStart=/etc/rc.d/init.d/rpcbind start (code=exited, status=0/SUCCESS)
    Main PID: 1119 (rpcbind)
      CGroup: name=systemd:/system/rpcbind.service
          └ 1119 rpcbind
[root@pc2 ~]# mkdir /media/docpublicos
mkdir: no se puede crear el directorio «/media/docpublicos»: El fichero ya existe
[root@pc2 ~]# ls /media/docpublicos
[root@pc2 ~]# mount servidor.lab2701.aso:/usr/share/docpublicos /media/docpublicos -t nfs
[root@pc2 ~]# ls /media/docpublicos
doc01.txt
[root@pc2 ~]# touch /media/docpublicos/prueba.txt
touch: no se puede efectuar `touch' sobre «/media/docpublicos/prueba.txt»: Sistema de ficheros de sólo lectura
[root@pc2 ~]# umount /media/docpublicos

-> Como puede apreciarse, los permisos son, en efecto, de sólo lectura.

-> MONTAJE AUTOMÁTICO DESDE EL CLIENTE AL ARRANCAR:

[root@pc2 ~]# cp /etc/fstab /etc/fstab_20120420
[root@pc2 ~]# vi /etc/fstab
[root@pc2 ~]# cat /etc/fstab | grep -i nfs
155.54.225.1:/usr/share/docpublicos    /media/docpublicos    nfs    ro,soft,bg,retry=10   0 0

-> PRUEBA DESDE EL CLIENTE (autenticándonos, por cierto, con Kerberos):

[eduardo@pc2 ~]$ ls /media/docpublicos/
doc01.txt
[eduardo@pc2 ~]$ rm /media/docpublicos/doc01.txt
rm: ¿borrar el fichero regular «/media/docpublicos/doc01.txt»  protegido contra escritura? (s/n) s
rm: no se puede borrar «/media/docpublicos/doc01.txt»: Sistema de ficheros de sólo lectura
[eduardo@pc2 ~]$ cat /media/docpublicos/doc01.txt
Contenido de "doc01.txt"

-> AHORA VAMOS A CONTROLAR EL ACCESO DE SÓLO LECTURA, HACIENDO
que sólo se pueda acceder a /usr/share/docpublicos/doc01.txt desde fuera...

-> En el cliente...

[alumno@pc2 ~]$ cd /media/docpublicos
```

```
[alumno@pc2 docpublicos]$ cd

-> En el servidor...

[root@servidor ~]# ls -l /usr/share/docpublicos/doc01.txt
-rw-r--r--. 1 root root 25 abr 21 11:38 /usr/share/docpublicos/doc01.txt
[root@servidor ~]# chown 1000 /usr/share/docpublicos/doc01.txt
[root@servidor ~]# chmod o-r /usr/share/docpublicos/doc01.txt
[root@servidor ~]# ls -l /usr/share/docpublicos/doc01.txt
-rw-r-----. 1 1000 root 25 abr 21 11:38 /usr/share/docpublicos/doc01.txt
[root@servidor ~]# su - alumno
[alumno@servidor ~]$ cat /usr/share/docpublicos/doc01.txt
cat: /usr/share/docpublicos/doc01.txt: Permiso denegado

-> (nótese, arriba, que ni siquiera en modo local, si no eres root,
se puede leer /usr/share/docpublicos/doc01.txt).
-> (nótese también que ni siquiera tiene que existir, ni en
el servidor ni en el cliente, un usuario con "id" 1000;
simplemente hemos escrito en el i-nodo del fichero que
únicamente un usuario cuyo "id" sea el 1000 puede modificarlo
-si no existe ese usuario, ese es otro problema-).

-> De nuevo, en el cliente...
(ya no nos deja entrar; tendríamos que ser el usuario 1000)

[alumno@pc2 ~]$ cd /media/docpublicos
-bash: cd: /media/docpublicos: Permiso denegado

-> POR TANTO, HAY QUE OBLIGAR A QUE SE HAGA UN MAPEO AL USUARIO
1000 CUANDO EL ACCESO SEA ANÓNIMO. De nuevo, en el servidor...

[root@servidor ~]# vi /etc/exports
/usr/share/docpublicos  155.54.225.0/24(ro,all_squash,anonuid=1000)
[root@servidor ~]# /etc/init.d/nfs restart
Restarting nfs (via systemctl):                            [  OK  ]
[root@servidor ~]# exportfs -v
/usr/share/docpublicos
        155.54.225.0/24(ro,wdelay,root_squash,all_squash,no_subtree_check,anonuid=1000)
```

```
-> PRUEBA DESDE EL CLIENTE:

[root@pc2 ~]# umount /media/docpublicos
[root@pc2 ~]# mount /media/docpublicos
[root@pc2 ~]# cd /media/docpublicos
[root@pc2 docpublicos]# ls -l
total 4
-rw-r-----. 1 nobody nobody 25 abr 21 11:38 doc01.txt
[root@pc2 docpublicos]# cat doc01.txt
Contenido de "doc01.txt"
[root@pc2 docpublicos]# rm doc01.txt
rm: ¿borrar el fichero regular «doc01.txt»? (s/n) s
rm: no se puede borrar «doc01.txt»: Sistema de ficheros de sólo lectura

-> Nos deja ver el fichero, pero lógicamente no podemos editarlo,
porque en /etc/exports sólo hemos dado permiso de lectura.

* * *

-> AHORA VAMOS A CREAR UN DIRECTORIO, /usr/share/docalumno2,
que sólo pueda ser accedido, en modo de sólo lectura, por un
usuario alumno2 que se autentica, con la misma contraseña, desde
cualquier equipo del reino kerberos. CONDICIÓN: Forzar que su UID
tenga un valor determinado.

-> SERVIDOR:

-> Damos de alta el principal "alumno2" (contraseña "alumno22012"),
y creamos el directorio /usr/share/docalumno2 haciendo que el propietario
sea el usuario de UID 550 (que en el servidor no existe, ni hace falta).

[root@servidor ~]# kadmin.local
Authenticating as principal root/admin@LAB2701.ASO with password.
kadmin.local:  addprinc alumno2
NOTICE: no policy specified for alumno2@LAB2701.ASO; assigning "default"
Enter password for principal "alumno2@LAB2701.ASO":
Re-enter password for principal "alumno2@LAB2701.ASO":
Principal "alumno2@LAB2701.ASO" created.
kadmin.local:  listprincs
```

```
K/M@LAB2701.ASO
alumno2@LAB2701.ASO
alumno@LAB2701.ASO
eduardo@LAB2701.ASO
host/pc2.lab2701.aso@LAB2701.ASO
host/servidor.lab2701.aso@LAB2701.ASO
kadmin/admin@LAB2701.ASO
kadmin/changepw@LAB2701.ASO
kadmin/servidor.lab2701.aso@LAB2701.ASO
krbtgt/LAB2701.ASO@LAB2701.ASO
root/admin@LAB2701.ASO
root@LAB2701.ASO
kadmin.local:  q
[root@servidor ~]# mkdir /usr/share/docalumno2
[root@servidor ~]# ls -ld /usr/share/docalumno2
drwxr-xr-x. 2 root root 4096 abr 21 12:42 /usr/share/docalumno2
[root@servidor ~]# chown 550 /usr/share/docalumno2
[root@servidor ~]# chmod o-r /usr/share/docalumno2
[root@servidor ~]# ls -ld /usr/share/docalumno2
drwxr-x--x. 2 550 root 4096 abr 21 12:42 /usr/share/docalumno2
[root@servidor ~]# su alumno
[alumno@servidor root]$ cd /usr/share/docalumno2
[alumno@servidor docalumno2]$ touch prueba
touch: no se puede efectuar `touch' sobre «prueba»: Permiso denegado
[alumno@servidor docalumno2]$ exit
exit

-> CONFIGURAMOS NFS EN EL SERVIDOR:

[root@servidor ~]# vi /etc/exports
[root@servidor ~]# cat /etc/exports
/usr/share/docpublicos  155.54.225.0/24(ro,all_squash,anonuid=1000)
/usr/share/docalumno2   155.54.225.0/24(rw)
[root@servidor ~]# /etc/init.d/nfs restart
Restarting nfs (via systemctl):                            [  OK  ]
[root@servidor ~]# exportfs -v
/usr/share/docpublicos
        155.54.225.0/24(ro,wdelay,root_squash,all_squash,no_subtree_check,anonuid=1000)
/usr/share/docalumno2
```

```
        155.54.225.0/24(rw,wdelay,root_squash,no_subtree_check)

-> EN EL CLIENTE...

[root@pc2 ~]# mkdir /media/docalumno2
[root@pc2 ~]# mount servidor.lab2701.aso:/usr/share/docalumno2 /media/docalumno2 -t nfs -o rw,hard,intr,bg,retry=10
[root@pc2 ~]# cd /media/docalumno2/
[root@pc2 docalumno2]# ls -l
ls: no se puede abrir el directorio .: Permiso denegado
[root@pc2 docalumno2]# cd
[root@pc2 ~]# useradd -u 550 alumno2
[root@pc2 ~]# kinit -p alumno2
Password for alumno2@LAB2701.ASO:
kinit: Password incorrect while getting initial credentials
[root@pc2 ~]# kinit -p alumno2
Password for alumno2@LAB2701.ASO:
[root@pc2 ~]# klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: alumno2@LAB2701.ASO

Valid starting     Expires            Service principal
04/21/12 12:52:51  04/22/12 12:52:51  krbtgt/LAB2701.ASO@LAB2701.ASO
    renew until 04/21/12 12:52:51
[root@pc2 ~]# su - alumno2
[alumno2@pc2 ~]$ cd /media/docalumno2/
[alumno2@pc2 docalumno2]$ ls -l
total 0
[alumno2@pc2 docalumno2]$ cat > doc_de_alumno2.txt
Contenido de "doc_de_alumno2.txt"
[alumno2@pc2 docalumno2]$ ls -l
total 4
-rw-rw-r--. 1 nobody nobody 34 abr 21 12:54 doc_de_alumno2.txt

-> COMO ÚLTIMA PRUEBA, HAREMOS QUE UN DETERMINADO USUARIO QUE SE AUTENTIQUE
DESDE DESDE PC2 MEDIANTE KERBEROS, NO TENGA SU DIRECTORIO DE INICIO EN EL
HOST CLIENTE, SINO EN EL PROPIO KDC. HAREMOS, ADEMÁS, UN MONTAJE AUTOMÁTICO.

-> SERVIDOR: Creamos el usuario "pilar" obligando a que su id sea 600.
No le damos password local, sino Kerberos (pilar2012).
```

```
[root@servidor ~]# useradd -u 600 pilar
[root@servidor ~]# id pilar
uid=600(pilar) gid=600(pilar) grupos=600(pilar)
[root@servidor ~]# ls /home/pilar -la
total 32
drwx------. 4 pilar pilar 4096 abr 21 13:00 .
drwxr-xr-x. 4 root  root  4096 abr 21 13:00 ..
-rw-r--r--. 1 pilar pilar   18 jun 22  2011 .bash_logout
-rw-r--r--. 1 pilar pilar  193 jun 22  2011 .bash_profile
-rw-r--r--. 1 pilar pilar  124 jun 22  2011 .bashrc
drwxr-xr-x. 2 pilar pilar 4096 feb  8  2011 .gnome2
drwxr-xr-x. 4 pilar pilar 4096 sep  7  2011 .mozilla
-rw-r--r--. 1 pilar pilar  658 feb  8  2011 .zshrc
[root@servidor ~]# cat /etc/passwd | grep -i pilar
pilar:x:600:600::/home/pilar:/bin/bash
[root@servidor ~]# cat /etc/shadow| grep -i pilar
pilar:!!:15451:0:99999:7:::
[root@servidor ~]# kadmin.local
Authenticating as principal root/admin@LAB2701.ASO with password.
kadmin.local:  addprinc pilar
NOTICE: no policy specified for pilar@LAB2701.ASO; assigning "default"
Enter password for principal "pilar@LAB2701.ASO":
Re-enter password for principal "pilar@LAB2701.ASO":
Principal "pilar@LAB2701.ASO" created.
kadmin.local:  listprinc
kadmin.local: Unknown request "listprinc".  Type "?" for a request list.
kadmin.local:  listprincs
K/M@LAB2701.ASO
alumno2@LAB2701.ASO
alumno@LAB2701.ASO
eduardo@LAB2701.ASO
host/pc2.lab2701.aso@LAB2701.ASO
host/servidor.lab2701.aso@LAB2701.ASO
kadmin/admin@LAB2701.ASO
kadmin/changepw@LAB2701.ASO
kadmin/servidor.lab2701.aso@LAB2701.ASO
krbtgt/LAB2701.ASO@LAB2701.ASO
pilar@LAB2701.ASO
```

```
root/admin@LAB2701.ASO
root@LAB2701.ASO
kadmin.local:  q

-> CONFIGURAMOS NFS:

[root@servidor ~]# vi /etc/exports
[root@servidor ~]# cat /etc/exports
/usr/share/docpublicos  155.54.225.0/24(ro,all_squash,anonuid=1000)
/usr/share/docalumno2   155.54.225.0/24(rw)
/home/pilar             155.54.225.0/24(rw)
[root@servidor ~]# /etc/init.d/nfs restart
Restarting nfs (via systemctl):                            [  OK  ]
[root@servidor ~]# exportfs -v
/usr/share/docpublicos
        155.54.225.0/24(ro,wdelay,root_squash,all_squash,no_subtree_check,anonuid=1000)
/usr/share/docalumno2
        155.54.225.0/24(rw,wdelay,root_squash,no_subtree_check)
/home/pilar     155.54.225.0/24(rw,wdelay,root_squash,no_subtree_check)

-> CLIENTE: Damos de alta el usuario "pilar", forzando a que su "id"
sea 600, pero no damos password.

[root@pc2 ~]# useradd -u 600 pilar

-> CLIENTE: Cambiamos /etc/fstab para el montaje automático del
/home/pilar del KDC (también servidor NFS), cuyo punto de montaje
será el /home/pilar del host cliente desde el que se está autenticando
"pilar". PERO: tener en cuenta que el verdadero directorio de inicio
de "pilar" estará en el KDC. El equipo sobre el que teclea "pilar"
es casi como si no tuviese disco duro...

[root@pc2 ~]# vi /etc/fstab
[root@pc2 ~]# cat /etc/fstab | grep pilar
155.54.225.1:/home/pilar              /home/pilar           nfs    rw,hard,intr,bg,retry=10 0 0

-> CLIENTE: Por supuesto, al intentar cosas como...

[alumno@pc2 ~]$ mount | grep pilar
```

```
155.54.225.1:/home/pilar on /home/pilar type nfs4
(rw,relatime,vers=4,rsize=262144,wsize=262144,namlen=255,hard,proto=tcp,port=0,timeo=600,retrans=2,sec=sys,clientaddr=0.0.0.0,minorversion=0,local_lock=none,addr=155.54.225.1)
[alumno@pc2 ~]$ cd /home/pilar
bash: cd: /home/pilar: Permiso denegado
```

ocurre lo correcto, en este caso "alumno2" no puede meterse
en el directorio de inicio de "pilar".