# Ficheros compartidos en red I: NFS.

**Autor: Enrique V. Bonet Esteban**

## *Introducción.*

El servicio de sistema de ficheros en red (Network File System) fue desarrollado por Sun Microsystems y presentado en el año 1984. El NFS permite que los ordenadores exporten (hagan disponibles) e importen (obtengan acceso) a directorios, sistemas de ficheros y dispositivos periféricos[1], de forma que los sistemas de ficheros de ordenadores remotos se comportan como si fueran locales.

El servicio NFS utiliza, para su funcionamiento, los servicios proporcionados por el protocolo de representación de datos externos (eXternal Data Representation, XDR) de la capa de presentación del modelo OSI y el protocolo de llamada a procedimiento remoto (Remote Procedure Call, RPC) de la capa de sesión del modelo OSI. Por debajo, dependiendo de la versión del protocolo, se utiliza UDP y/o TCP para la capa de transporte e IP para la capa de red. En concreto, la versión 1 de NFS utiliza solo UDP, mientras que las versiones 2 y 3 de NFS utilizan TCP y UDP para la capa de transporte, mientras que la versión 4 solamente utiliza TCP. Nosotros describiremos las versiones 2, 3 y 4 del protocolo, pues la versión 1 no es soportada por los actuales kernels de Linux.

Las versiones 2 y 3 de NFS utilizan un protocolo sin estado, esto es, el protocolo no almacena ninguna información sobre las peticiones que los clientes realizan al servidor, por lo que el servidor desconoce si un fichero ha sido exportado a un cliente, etc. Por el contrario, la versión 4 introduce el estado en el protocolo, de forma que un cliente puede indicar al servidor que desea hacer con un fichero (leer, escribir, bloquearlo, etc.), y el servidor puede con estar información permitir o denegar el acceso al fichero, aunque los permisos de exportación del fichero y del usuario permitan la acción, así como informar a otros clientes de que el fichero ya esta exportado a otros clientes y los modos de exportación.

Como se puede deducir de los párrafos anteriores, la arquitectura del servicio NFS es una arquitectura cliente/servidor. Por ello, empezaremos estudiando el servidor de NFS para pasar con posterioridad a ver el cliente.

## *El servidor de NFS.*

El servidor de NFS es el ordenador que exporta los sistemas de ficheros. La exportación de los sistemas de ficheros en las versiones 2 y 3 se realiza siempre a ordenadores remotos y nunca a usuarios concretos, por lo cual no existe la posibilidad de exportar un sistema de ficheros a un usuario concreto de un ordenador, sino que un sistema de ficheros exportado a un ordenador es accesible a todos los usuarios de ese ordenador. Este aspecto es modificado en la versión 4, pues en ella se puede autenticar a

[1] A partir de ahora hablaremos solo de sistemas de ficheros, aunque todo lo dicho sobre ellos es aplicable siempre a dispositivos periféricos.

usuarios y/o grupos mediante el protocolo de autenticación Kerberos[2]. Con el fin de simplificar la exposición del tema, nos centraremos en las versiones 2 y 3 del protocolo, explicando puntualmente algunos aspectos que pueden ser interesantes de la versión 4, pero sin entrar en otros como la autenticación mediante Kerberos, etc.

El funcionamiento de NFS utiliza llamadas a procedimientos remotos (Remote Procedure Call), lo que requiere el que el servicio de *rpcbind* (antiguo servicio *portmap*) se encuentre arrancado previamente. En la versión 2 del protocolo solo es necesario que el servicio de *rpcbind* se encuentre arrancado en el servidor, mientras que en las versiones 3 y 4 es necesario que tanto cliente como servidor tenga arrancado el servicio de *rpcbind*, pues en caso contrario la exportación funciona de forma muy lenta y puede llegar a no funcionar.

El programa */usr/sbin/rpcbind* es un programa genérico, no específico del servicio NFS, y que proporciona la conversión entre los números de programa del RPC y los puertos de los protocolos. Cuando un servidor RPC arranca, informa al *rpcbind* en que puerto esta preparado para aceptar peticiones y que números de programa RPC esta preparado para servir. Cuando un cliente quiere llamar a un servicio RPC, pregunta al *rpcbind* del ordenador servidor para determinar el puerto donde el mensaje RPC debe ser enviado. El *rpcbind* debe ser arrancado antes que cualquier servidor RPC mediante el comando[3]:

```
systemctl start rpcbind.service
```

El servidor de NFS es arrancado mediante el comando[4]:

```
systemctl start nfs.service
```

Dicho script se encarga de lanzar todos aquellos programas necesarios para el funcionamiento del servicio de NFS. Básicamente, para permitir la exportación de un sistema de ficheros, se requiere el funcionamiento de tres programas, además de módulos internos del kernel del sistema: */usr/sbin/rpc.idmapd*, */usr/sbin/rpc.rquotad* y */usr/sbin/rpc.mountd*[5].

El programa *rpc.idmapd* se utiliza en la versión 4 del protocolo y permite efectuar la correspondencia entre los nombres de las llamadas de autenticación de Kerberos de forma *usuario@dominio*, utilizados en la versión 4 del protocolo, con los identificadores de los usuarios locales (UID y GID). Su fichero de configuración es */etc/idmapd.conf* y si no se utiliza la versión 4 el protocolo no es necesaria su configuración.

El programa *rpc.rquotad* se encarga de informar a los sistema remotos sobre las cuotas de los usuarios locales, si las cuotas de disco se encuentran activadas, de forma

[2] Puede obtenerse información sobre el protocolo de autenticación Kerberos en la URL http://web.mit.edu/Kerberos.

[3] Si el servicio de *rpcbind* no está arrancado se produce un error en el arranque del servicio de NFS.

[4] Si se arranca el servicio de NFS sin haber arrancado antes el servidor rpcbind se obtiene el mensaje de error: “A dependency job failed. See system journal for details.”

[5] Existen otros programas que proporcionan información a los clientes sobre el estado de un servidor NFS, las cuotas de los usuarios de los sistemas remotos, etc., pero no son necesarios para el funcionamiento básico del servidor NFS.

que los sistemas remotos puedan informar a sus usuarios de las cuotas de disco de los sistemas que han montado de forma remota y, por tanto, de los límites que poseen en esos sistemas. Posee algunas opciones de configuración, de las cuales la más utilizada es la opción *-p <puerto>* que permite especificar el puerto en el que atiende sus peticiones, pues en caso de no especificarse es elegido un puerto aleatorio que se encuentre disponible en el momento de arranque del servicio de NFS.

Por último, el programa *rpc.mountd* recibe las peticiones de solicitud para montar un sistema de ficheros por parte de un cliente, comprueba si dicho sistema de ficheros es exportado y si además esta autorizado para el ordenador cliente, efectuando la exportación del sistema en caso afirmativo. El programa *rpc.mountd* tiene numerosas opciones, de las cuales la única que suele utilizarse, igual que en el programa *rpc.rquotad*, es la opción *–p <puerto>*[6], la cual tiene el mismo significado y utilidad que la explicada con anterioridad.

## Configuración de los sistemas de ficheros exportados.

El fichero de configuración donde se indica al servidor que sistemas de ficheros debe exportar es el fichero */etc/exports*[7]. En él se introducen las líneas con los sistemas de ficheros exportados, a que ordenadores se permite su exportación y en que modos (solo lectura, lectura y escritura, etc.)[8].

Cada línea del fichero *exports* contiene la información sobre un sistema de ficheros que exporta el servidor. Todas las líneas tienen la siguiente sintaxis:

```
<sistema de ficheros> <ordenador/es>[(opciones de exportación)]
[<ordenador/es>[(opciones de exportación)]]
```

Pudiendo observar que las líneas comienzan con la información del sistema de ficheros a exportar y a continuación un ordenador o lista de ordenadores a los que se quiere exportar el sistema de ficheros, así como para cada ordenador u ordenadores, encerrado entre paréntesis y de forma opcional, que opciones de exportación deseamos utilizar[9].

Los sistemas de ficheros corresponden a los directorios que el servidor desea exportar, por ejemplo */var/ftp*, */home*, etc., o los dispositivos periféricos como por ejemplo */dev/cdrom*.

El ordenador u ordenadores a los que se exportan los sistemas de ficheros se pueden especificar de tres formas distintas[10]:

- Como un ordenador particular, esto, es como un nombre de ordenador, un nombre cualificado en el dominio del servidor o una dirección IP.

[6] La utilidad del uso de la opción –p se analizará en el apartado dedicado a la seguridad del NFS.
[7] El fichero */etc/exports* se lee en el arranque del servicio de NFS o bien, si es modificado, puede releerse, etc., mediante el comando */usr/sbin/exportfs*.
[8] Recordar el comentario hecho con anterioridad de que los sistemas de ficheros son exportados a un ordenador y no solo a unos usuarios determinados.
[9] En caso de no especificar alguna opción de exportación se toma su valor por defecto.
[10] En el apartado dedicado a la seguridad del NFS veremos cual de estas opciones es preferible.

- Como un conjunto de ordenadores, utilizando para ello los caracteres comodín * e ?[11]. Estos caracteres sirven para indicar el conjunto de ordenadores a los que se exportan los sistemas de ficheros. Así, por ejemplo, *.irobot.uv.es indica que el sistema de ficheros se exporta a todos los ordenadores del dominio irobot.uv.es (Instituto de Robótica), mientras que lab6inf??.informat.uv.es, indica que se exporta a todos los ordenadores del laboratorio 6 de prácticas.

- Mediante la especificación de una red o subred IP. La especificación de la red o subred se debe realizar mediante la dirección que especifica la red o subred y a continuación el número de bits que corresponden a la red. Por ejemplo, 147.156.222.0/23 se refiere a la subred del Instituto de Robótica.

Las opciones de exportación podemos dividirlas en dos grandes grupos, opciones que especifican el modo de exportación y opciones que modifican los identificadores de los usuarios.

Las opciones que especifican el modo de exportación se encargan de indicar si la exportación es en modo de solo lectura o en modo de lectura y escritura, así como opciones de funcionamiento del servidor de NFS. Las principales opciones se encuentran en la siguiente tabla:

| **Opción** | **Descripción** |
|---|---|
| ro | Exportación en solo lectura. El sistema exportado solo puede ser leído por el sistema remoto. Es la opción de exportación por defecto si no se indica lo contrario. |
| rw | Exportación en lectura/escritura. El sistema exportado puede ser modificado por el sistema remoto. |
| async | Permite al servidor de NFS violar el protocolo y responder a requerimientos de escritura antes de que los cambios hayan sido efectuados de forma efectiva en el disco. Esto puede causar problemas si el servidor falla (sufre un fallo, etc.) y causar que el sistema de ficheros este corrupto. |
| sync | No permite al servidor NFS violar el protocolo, por lo cual debe realizar los cambios de forma efectiva antes de contestar. Esta es la opción por defecto actual. En versiones anteriores a la 2 la opción por defecto era async[12]. |
| wdelay | Permite al servidor NFS retrasar una escritura en el disco si supone que otro requerimiento de escritura es inminente. Esto permite aumentar la velocidad de las operaciones. Es la opción por defecto. |
| no_wdelay | No permite retrasar las escrituras. No tiene efecto si la opción async ha sido habilitada. |

Por otra parte, las opciones que modifican los identificadores de los usuarios permiten modificar el UID o el GID de los usuarios que acceden al sistema, aunque dicha modificación es realizada para el usuario root y/o el resto de usuarios, no pudiendo especificarse para usuarios particulares excepto root. Antes de ver las

[11] El carácter * se corresponde a 0 o más caracteres, mientras que el carácter ? se corresponde exactamente a un carácter.

[12] En la versión actual del servicio NFS, sino se específica de forma explícita que la exportación es async o sync, se genera un mensaje de advertencia por si el administrador ignora que ya no funciona con una versión anterior a la 2 y espera que el comportamiento por defecto sea async.

opciones conviene explicar un poco más detenidamente como se permite el acceso a los ficheros exportados.

El acceso a los ficheros del sistema exportado por el servidor se basa en el identificador de usuario (UID) y el identificador de grupo (GID) proporcionados por cada requerimiento al NFS. Un usuario podrá acceder a un fichero para lectura o lectura/escritura en función del UID y GID que el cliente proporcione al servidor y los permisos que ese UID y GID posean sobre el fichero.

Sin embargo, esto presenta un problema, y es que en todos los sistemas Linux/UNIX, el usuario root siempre tiene el UID 0, por lo que cualquier sistema de ficheros exportado puede ser accedido con total impunidad por el root de cualquiera de los ordenadores a los que se exporta. Para evitar esto, el funcionamiento por defecto del servicio de NFS consiste en modificar de forma automática el identificador de usuario de los usuarios con UID 0 a un usuario con UID diferente[13]. Generalmente ese usuario es el usuario *nobody* (identificado en algunos sistemas con el nombre *anonymous*), usuario que tiene por defecto el identificador de usuario 65534 (-2) y por el identificador de grupo *nfsnobody*, que tiene el identificador de grupo 65534 (-2).

Una vez explicada el funcionamiento de los usuarios en NFS, las opciones que modifican los identificadores de los usuarios se encuentran en la siguiente tabla:

| **Opción** | **Descripción.** |
|---|---|
| root_squash | Cambia el UID y el GID del usuario root. Es la opción por defecto. |
| no_root_squash | No cambia el UID y el GID del usuario root. |
| all_squash | Cambia todos los usuarios al usuario anónimo. Esta opción suele ser utilizada para exportar de forma pública directorios “generales” del ordenador, tales como el directorio de FTP anónimo, directorios de spool, etc. |
| no_all_squash | No cambia todos los usuarios al anónimo. Es la opción por defecto. |
| anonuid | Especifica el UID que debe asignarse al usuario anónimo en lugar del valor por defecto. |
| anongid | Especifica el GID que debe asignarse al grupo anónimo en lugar del valor por defecto. |

Un ejemplo del archivo */etc/exports* es el siguiente:

```
# Exportamos el directorio de ftp anónimo a todos los ordenadores de
# subred 147.156.222.0/23
/var/ftp    147.156.222.0/23(rw,sync,all_squash,anonuid=14,anongid=50)

# Exportamos el directorio de trabajo del usuario quique para
# que pueda ser usado desde el ordenador de IP 147.156.222.34
/home/quique      147.156.222.34(rw,sync)

# Exportamos el directorio de root para poder leerlo desde la subred
# 147.156.222.0/23
/root             147.156.222.0/23(ro,sync,no_root_squash)
```

[13] Téngase en cuenta que esto solo afecta al usuario de UID 0 (root), pero no a otros usuarios “privilegiados” como puede ser el usuario bin (UID 1), etc.

Como último punto, es importante incidir en que la sintaxis debe respetarse escrupulosamente, pues mientras la línea:

```
/home        147.156.222.65(rw)
```

Exporta el directorio */home* en modo lectura/escritura para el ordenador 147.156.222.65, la siguiente línea.

```
/home        147.156.222.65 (rw)
```

Exporta el directorio */home* en modo lectura para el ordenador 147.156.222.65 y en modo lectura y escritura ¡a todos los ordenadores de Internet!.

## *El cliente NFS.*

En primer lugar, indicar que para el correcto funcionamiento del servicio, el cliente de NFS debe tener habilitado el servicio de *rpcbind*, por lo que si no se esta ejecutando el servicio debe ejecutar el comando:

```
systemctl start rpcbind.service
```

Un sistema de ficheros exportado por un ordenador puede ser montado por el cliente de varias formas. La mas sencilla es que el administrador monte el sistema de ficheros utilizando el comando */bin/mount* cada vez que el sistema arranque. Esto puede realizarse mediante el comando:

```
mount –t nfs <servidor NFS>:<sistema de ficheros> <punto de montaje>
```

Sin embargo, esta no es una opción práctica, pues el administrador debe estar pendiente de cada arranque del ordenador y proceder a su montaje de forma manual. Las dos opciones más prácticas y comúnmente usadas son mediante el fichero */etc/fstab* y mediante el servicio de *autofs*.

### Utilización del fichero /etc/fstab.

El fichero */etc/fstab* contiene, normalmente, las entradas de los sistemas de ficheros locales que deben ser montados en el arranque del ordenador, por ejemplo:

```
/dev/sda1         /             ext3   defaults                              1 1
/dev/sda2         swap          swap   defaults                              0 0
/dev/devpts       /dev/pts      devpts gid=5,mode=620                        0 0
/dev/shm          /dev/shm      tmpfs  defaults                              0 0
/dev/proc         /proc         proc   defaults                              0 0
/dev/sys          /sys          sysfs  defaults                              0 0
/dev/fd0          /mnt/floppy   auto   pamconsole,exec,noauto,utf8,managed 0 0
/dev/hdc          /mnt/cdrom    auto   pamconsole,exec,noauto,managed       0 0
```

Dicho fichero puede, además, contener las líneas necesarias para montar los sistemas exportados por otros ordenadores y que deban ser montados por nuestro ordenador. Estás líneas tienen la siguiente sintaxis:

```
<servidor>:<directorio>   <punto de montaje>   nfs   <opciones>   0 0
```

Donde <*servidor*>:<*directorio*> indica el nombre del ordenador y el directorio que dicho ordenador exporta, <*punto de montaje*> indica en que directorio se montará el sistema de ficheros, *nfs* indica que el tipo del sistema de ficheros a montar es nfs, o sea, un sistema de ficheros exportado por otro ordenador, <*opciones*> indica las opciones de montaje del sistema exportado. Por último, los dos valores 0 finales indican, respectivamente, que el sistema de ficheros no debe ser volcado al terminar su uso y que no debe ser chequeado en el arranque.

Existen un gran número de opciones de montaje disponibles, pero las más comunes son las siguientes:

| **Opción** | **Descripción.** |
|---|---|
| hard | El cliente debe esperar hasta que el sistema exportado por el servidor este disponible[14]. |
| soft | El cliente debe esperar un tiempo (en décimas de segundo) indicado por la opción *timeo*=<*valor*> a que el sistema exportado por el servidor este disponible, devolviendo un error si es excedido el tiempo |
| intr | Permita que se interrumpan las opciones *hard* o *soft* mediante una interrupción desde el teclado (generalmente Ctrl-C). |
| nfsver=<versión> | Especifica la versión de protocolo a utilizar (2, 3 o 4). |
| nolock | Desactiva la opción de bloqueo de archivos. |
| noexec | No permite la ejecución de archivos binarios del sistema montado. |
| nosuid | No permite que los bits de SUID y de GUID del sistema de ficheros remoto montado tengan efecto en el sistema local. |
| rsize=<tamaño> | Modifica el tamaño por defecto del bloque que es leído a los bytes indicados por <*tamaño*>, lo que redunda en aumentar la velocidad de lectura. El valor máximo de tamaño varía según versiones, etc., pero suele ser aceptado el valor 32768. |
| wsize=<tamaño> | Modifica el tamaño por defecto del bloque que es escrito a los bytes indicados por <*tamaño*>, lo que redunda en aumentar la velocidad de lectura. El valor máximo de tamaño varía según versiones, etc., pero suele ser aceptado el valor 32768. |
| tcp | Indica que se utilice unicamente protocolo de transporte TCP. |

Un ejemplo de fichero */etc/fstab* que realizan el montaje en el arranque de un conjunto de sistemas de ficheros remotos es el siguiente:

```
/dev/sda1       /            ext3   defaults                          1 1
/dev/sda2       swap         swap   defaults                          0 0
/dev/devpts     /dev/pts     devpts gid=5,mode=620                    0 0
/dev/shm        /dev/shm     tmpfs  defaults                          0 0
/dev/proc       /proc        proc   defaults                          0 0
/dev/sys        /sys         sysfs  defaults                          0 0
/dev/fd0        /mnt/floppy  auto   pamconsole,exec,noauto,utf8,managed 0 0
/dev/hdc        /mnt/cdrom   auto   pamconsole,exec,noauto,managed     0 0
```

[14] Téngase en cuenta que el servidor de NFS puede sufrir un problema mientras un cliente esta utilizando su servicio, por lo que el servicio puede no estar disponible.

```
glup:/var/ftp     /glup/ftp     nfs    hard,intr                          0 0
glup:/home/quique /glup/quique  nfs    soft,timeo=100                     0 0
glup:/root        /glup/root    nfs    soft,timeo=100                     0 0
```

Donde las últimas tres líneas corresponden a los sistemas de ficheros remotos montados mediante NFS.

## Utilización del servicio autofs.

El último sistema de montaje es utilizando el servicio *autofs*, basado en la utilidad del kernel *automount*. Este sistema es mucho más aconsejable pues el servicio *autofs* realiza el montaje automático de los sistemas de ficheros NFS cuando estos son requeridos, procediendo a desmontarlos de forma automática cuando estos no han sido usados durante un cierto periodo de tiempo[15].

El servicio *autofs* se activa mediante el comando:

```
systemctl start autofs.service
```

Siendo su fichero de configuración */etc/auto.master*, cuyas entradas tienen la sintaxis:

```
<punto de montaje>   <mapa tipo>   <opciones>
```

Donde <*punto de montaje*> indica el directorio donde debe montarse el sistema de ficheros que es importado desde el servidor y <*mapa tipo*> indica el fichero donde se especifica el nombre del servidor o de los servidores, los sistemas de ficheros, etc., que deben montarse en ese punto de montaje.

Un ejemplo de fichero *auto.master* es el siguiente:

```
/glup   /etc/auto.glup   --timeout=300
```

Que indica que todos los sistemas de ficheros exportados que se indiquen en el fichero */etc/auto.glup* serán montados dentro del directorio */glup*, con un timeout de 300 segundos, esto es, el sistema se desmontara automáticamente al cabo de 300 segundos de estar sin ser usado. En la actualidad, el fichero /*etc/auto.master* que trae por defecto la distribución de Fedora 17 incluye la línea:

```
+dir:/etc/auto.master.d
```

Que permite incluir todos los ficheros que se encuentren dentro de ese directorio y que tengan como extensión *.autofs*, por lo que es posible indicar sistemas adicionales de ficheros a montar sin necesidad de modificar el fichero */etc/auto.master*. Además, si se utiliza de esta forma es recomendable poner los mapas tipo dentro del mismo directorio, quedando la configuración del sistema localizada en un único directorio[16].

[15] El tiempo de espera hasta desmontar el sistema de ficheros veremos que puede ser configurado, debiendo tener en cuenta que este no debe ser excesivamente breve, pues el sistema de ficheros deberá ser montado y desmontado de forma innecesaria si dicho tiempo es muy breve.

[16] Obviamente los mapas tipo, si se colocan dentro del directorio */etc/auto.master.d* no deben tener extensión *.autofs*.

En cualquier caso, los ficheros <*mapa tipo*> responden a la sintaxis:

```
<directorio de montaje>   <opciones>   <servidor>:<directorio>
```

Donde el <*directorio de montaje*> es el directorio, dentro el directorio especificado en el fichero *auto.master*, donde se montarán los sistemas de ficheros, el campo <*opciones*> indica las opciones de montaje que deseamos, opciones que son añadidas a las opciones especificadas en el fichero *auto.master*[17] y <*servidor*>*:*<*directorio*> indica el sistema de ficheros exportado a montar.

Los directorios de montaje especificados en el fichero <*mapa tipo*> son creados de forma automática por el servicio *autofs* si no existen. Sin embargo, el directorio de montaje especificado en el fichero */etc/auto.master* debe existir siempre.

Un ejemplo de fichero */etc/auto.glup* es el siguiente:

```
ftp             -rw,soft,intr        glup.uv.es:/var/ftp
quique          -rw,soft,intr        glup.uv.es:/home/quique
terradez        -rw,soft,intr        glup.uv.es:/home/terradez
root            -ro,soft,intr        glup.uv.es:/root
```

Donde, por ejemplo, la primera línea especifica que el directorio */var/ftp* exportado por el ordenador *glup.uv.es* será montado en el directorio */glup/ftp* en modo de lectura/escritura, con la opción de montaje *soft* y la posibilidad de ser interrumpido[18]. Además, el timeout está fijado en 300 segundos por la acumulación de opciones del fichero *auto.master*.

Los ficheros <*mapa tipo*> admiten el uso de dos caracteres comodín. El primero de ellos, el carácter & puede ser utilizado en el campo <*servidor*>*:*<*directorio*> e indica que busque todas las entradas que respondan a la línea indicada. El carácter & en el caso del <*servidor*> sustituye el nombre del servidor, mientras que el caso de <*directorio*> solo sustituye el nombre del último directorio a montar. Por ejemplo, si los directorios a montar son *glup:/home/quique*, *glup:/home/terradez*, su montaje se puede poner como *glup:/home/*&, pero nunca como *glup:*&.

El segundo de ellos, el carácter *, puede ser utilizado en el campo <*directorio de montaje*> e indica que como directorio de montaje debe utilizarse el obtenido de la búsqueda de las entradas que ha realizado el carácter comodín &. Así, si en el ejemplo anterior hubiéramos escrito la siguiente línea:

```
*          -rw,soft,intr          glup:/home/&
```

Hubiéramos podido montar todos los directorios exportados por *glup* del directorio */home* dentro del directorio */glup*, que debe existir previamente pero pudiendo crearse de forma dinámica el directorio del usuario.

[17] El funcionamiento de esta opción es diferente en SunOS, pues en ese sistema operativa las opciones no se acumulan.

[18] Las opciones que aquí se especifican pueden limitar las opciones de exportación del servidor, pero nunca ampliarlas. Así, si el servidor exporta /var/ftp en modo solo lectura, el poner la opción de lectura/escritura (rw) no implica que se pueda escribir en el sistema de ficheros exportado por el servidor.

De igual forma, si escribimos la siguiente línea:

```
*          -rw,soft,intr          &:/home/&
```

Cualquier directorio de tipo */home* que estuviera exportado con permisos para nuestro cliente de NFS sería montado dentro del directorio */mnt/"ordenador"/"directorio"*, si suponemos que */mnt* es el punto de montaje indicado en el fichero */etc/auto.master*. Por ejemplo, con la exportación que realiza el ordenador glup, la línea anterior montaría el fichero exportado por *glup:/home/quique* en el directorio local */mnt/glup/quique*, debiendo existir previamente el directorio */mnt/glup* en el sistema.

## Montaje automático de sistemas de ficheros locales.

Antes de terminar la explicación del cliente NFS conviene explicar la utilización del cliente de NFS para poder montar y desmontar de forma automática los sistemas de ficheros locales que son extraíbles, esto es, el CD-ROM y los disquetes[19].

Antes de empezar, conviene indicar que en los actuales sistemas Linux, existen servicios que suelen arrancarse por defecto y que también realizan el montaje automático de los sistemas de ficheros locales. Estos servicios suelen ir unidos al uso de una interfaz gráfica, mostrando en pantalla el sistema de ficheros montado, etc., lo cual hace su uso mucho más amigable. Sin embargo, en sistemas que no utilicen interfaz gráfico, sigue siendo necesario montar los ficheros locales tal y como se indica en este punto.

El primer hecho a destacar es que el montaje automático de sistemas de ficheros locales no requiere que el servidor de NFS este activo, lo cual simplifica enormemente la configuración, pues tan solo es necesario configurar el cliente de NFS[20].

Para poder montar y desmontar de forma automática los sistemas de fichero locales que son extraíbles necesitamos incluir su descripción en los dos ficheros que especifican el uso del servicio *autofs*.

En concreto, el fichero auto.master deberá incluir la siguiente línea:

```
/mnt          /etc/auto.mnt          --timeout=60
```

Donde se puede observar que se desea que se monten dentro del directorio */mnt* y que el tiempo de timeout se ha fijado en 60 segundos[21].

Por último, el fichero */etc/auto.mnt* que se cita como <*mapa tipo*> debe tener las siguientes líneas:

[19] Téngase en cuenta que esos dos sistemas de ficheros han debido ser definidos en el archivo /etc/fstab,, tal y como se puede ver en la descripción del fichero /etc/fstab que ha realizada con anterioridad.

[20] Puede entenderse este hecho como que todo ordenador tiene permiso y es capaz de exportar sus sistemas de ficheros locales a si mismo.

[21] En este caso el timeout no debe ser excesivamente grande, pues mientras el sistema de ficheros montados no sea desmontado automáticamente, el CD-ROM o disquete no podrá ser extraído correctamente.

```
cdrom          -fstype=iso9660,ro      :/dev/cdrom
floppy         -fstype=auto,rw         :/dev/fd0
```

En estas líneas resalta el hecho de que no se especifique ningún ordenador. Esto es así pues siempre que no se especifica un ordenador, se toma por defecto el nombre del ordenador local (*localhost*).

## *Seguridad en el servicio NFS.*

El servicio de NFS requiere una gran atención de seguridad, pues es una fuente frecuente de problemas de seguridad, tanto por los permisos de exportación, etc., como por el hecho de que un intruso de un ordenador cliente de NFS que tenga permisos para montar un sistema de ficheros de otro ordenador tiene una "posible puerta" de acceso al ordenador servidor de NFS.

Por otro lado, el servicio de NFS requiere la apertura, tanto en el cliente como en el servidor, de servicios en los *tcp_wrappers* y de puertos en los cortafuegos[22], hecho que supone por si mismo una relajación de la seguridad del sistema. Expondremos a continuación las medidas de seguridad que es necesario tomar, tanto en el servidor como en el cliente NFS para minimizar los riesgos.

Respecto al servidor, el uso de NFS obliga a que el servicio *rpcbind* sea habilitado en el *tcp_wrapper* para todos aquellos sistemas que deseamos sean clientes de nuestro servidor NFS. Además, el cortafuegos debe permitir que los servicios de *rpcbind* (puerto 111 TCP y UDP), *rpc.nfsd* (puerto 2049 TCP y UDP) y los puertos requeridos por *rpc.rquotad* y *rpc.mountd*, que explicaremos a continuación, deban ser habilitados en el cortafuegos.

Como comentamos con anterioridad, los programas *rpc.rquotad* y *rpc.mountd* eligen de forma aleatoria un puerto libre en el arranque del servicio de NFS, excepto que se le especifique con la opción *-p* el puerto concreto que deseamos que utilice. Dicho puerto debería estar reservado para este servicio. Sin embargo, la reserva de un puerto solo puede realizarse para los primeros 1024 puertos (número de puerto 0 a 1023), puertos que reciben el nombre de "puertos de servicios bien conocidos"[23] y que por su definición solo deben ser utilizados por dichos "servicios bien conocidos". Por ello, si deseamos que *rpc.rquotad* y/o *rpc.mountd* utilicen un puerto en concreto, debemos ver en el instante de arranque del servicio, que deberá coincidir siempre con el arranque del ordenador, que puertos de número mayor que 1023 están disponibles y asignarle uno de esos puertos de forma fija mediante la opción *-p*.

Por tanto, si optamos por la opción de que los programas *rpc.rquotad* y/o *rpc.mountd* utilice un puerto cualquiera, dado que desconocemos su número, deberemos abrir todos los puertos TCP y UDP del cortafuegos del servidor para aceptar todo el tráfico TCP y UDP proveniente de los clientes de NFS que aceptemos.

Si por el contrario optamos por utilizar la opción *-p*, tendremos tan solo que abrir los puertos TCP y UDP 111, 2049 y los puertos utilizados por *rpc.rquotad* y

[22] La configuración de los tcp_wrappers y de los cortafuegos será vista en temas posteriores.

[23] Los servicios bien conocidos son todos aquellos que tienen un número de puerto menor a 1024. Una lista de los mismos puede encontrase en el fichero /etc/services.

*rpc.mountd* para que acepten el tráfico TCP y UDP proveniente de los clientes de NFS y con destino en esos puertos. Sin desear entrar en más detalles, indicar que la configuración del puerto asignado a los programas *rpc.rquotad* y *rpc.mountd* puede realizarse en el fichero */etc/sysconfig/nfs*, para ello, debemos modificar las opciones RPCRQUOTADOPTS y RPCMOUNTDOPS. Por ejemplo, si queremos que rpc.rquotad se ejecute en el puerto 4000 y rpc.mountd en el puerto 4001 pondremos:

```
RPCRQUOTADOPTS="-p 4000"
RPCMOUNTDOPTS="-p 4001"
```

Para indicarles, mediante el parámetro -p, los puertos en que deseamos que se ejecuten. Por supuesto el puerto o puertos especificados no deben estar ocupados por un servicio anterior en el momento de arranque del servidor de NFS.

Además de todos los problemas anteriores, existe otro problema de seguridad referida al uso de nombres de ordenadores en el fichero */etc/exports*. El problema proviene de que un posible intruso podría "atacar" previamente el servidor de DNS sobre el que realizamos la consulta de los nombres de ordenadores, y hacer que dicho servidor nos proporcionara información falsa, permitiendo con ello que ordenadores intrusos pudieran acceder a nuestro servidor de NFS. Por ello, y como medida de seguridad, es conveniente identificar los ordenadores o grupos de ordenadores mediante su dirección IP o dirección de red o subred y no mediante su nombre o dominio.

Respecto al cliente, el uso de NFS obliga a que el servicio *rpcbind* sea habilitado en el *tcp_wrapper* para todos aquellos sistemas que deseamos sean servidores de nuestro cliente de NFS y abrir el cortafuegos para el servicio, esto es, abrir el puerto 111 TCP.

Además, si el servidor de NFS utiliza un puerto aleatorio, el cliente de NFS debe abrir su cortafuegos para aceptar todo el tráfico proveniente del servidor de NFS, mientras que si el servidor de NFS utiliza un puerto determinado, el cliente tan solo tiene la necesidad de aceptar el tráfico proveniente de los puertos 111, 2049 y los puertos escogidos para los servicios de *rpc.rquotad* y *rpc.mountd* y que tiene como origen el servidor de NFS.

## *Ejercicios*

1- Configurar un servidor de NFS de forma que permita exportar, a todos los ordenadores de la UV (147.156.0.0/16), el directorio */var/ftp/download* en modo de lectura y el directorio */var/ftp/upload* en modo de lectura y escritura para todos los usuarios.

2- Configurar un servidor de NFS de forma que exporte el directorio */home/usuario* para el ordenador 147.156.222.34 en modo de lectura y escritura y para el resto de ordenadores del dominio 147.156.222.0/23 en modo de lectura. Además, deberá permitir que el usuario root acceda al directorio */root* a todos los ordenadores del dominio anterior solo en modo de lectura.

3- Escribir el fichero de configuración de un cliente de NFS de forma que permita montar los directorios exportados en el ejercicio anterior mediante */etc/fstab*.

4- Escribir el fichero de configuración de un cliente de NFS que permita montar los directorios exportados en el ejercicio 2 mediante el servicio de *autofs*.

5- Configurar un cliente de NFS de forma que pueda montar todos los directorios de nombre */publico*, en modo de solo lectura, exportados por cualquier ordenador de Internet.