Introducción (I)

- Network File System fue desarrollado por SUN y presentando en 1984.
- Permite que los ordenadores:
  - Exporten (hagan disponibles).
  - Importen (obtengan acceso).

Sistemas de ficheros y dispositivos periféricos.

- NFS utiliza:
  - XDR: Protocolo de representación de datos externos.
  - RPC: Llamadas a procedimiento remoto.
  - Protocolo de transporte TCP y/o UDP y de red IP.

Introducción (II)

- Las versiones utilizan:
  - Versión 1: UDP.
  - Versiones 2 y 3: TCP y UDP.
  - Versión 4: TCP.
- NFS hasta la versión 4 es un protocolo sin memoria:
  - Cada llamada debe contener toda la información necesaria para su ejecución.
  - El servidor no realiza recuperación frente a fallos.
  - Un fallo de un cliente no repercute en el servidor.

El servidor de NFS (I)

- El servidor exporta sus sistemas de ficheros a ordenadores:
  - Versión 4: Pueden autenticarse usuarios/grupos mediante Kerberos.
- El uso de RPC requiere arrancar el servicio de rpcbind:

```
systemctl start rpcbind.service
```

- rpcbind (antiguo portmap):
  - Convierte los números de programas en los puertos donde se encuentran.
  - Cuando un servidor RPC arranca, informa a rpcbind de:
    - Puerto utilizado.
    - Números de programas RPC que sirve.
  - Cuando un cliente quiere utilizar un servicio RPC pregunta a rpcbind donde se encuentra.

El servidor de NFS (II)

- Es arrancado mediante la orden:

```
systemctl start nfs.service
```

- Son lanzados todos los programas necesarios:
  - /usr/sbin/rpc.idmapd
    - Se utiliza en la versión 4 del protocolo.
    - Efectua la correspondencia entre Kerberos y los UID y GID locales.
  - /usr/sbin/rpc.rquotad
    - Informa al cliente de NFS de las cuotas de los usuarios.
  - /usr/sbin/rpc.mountd
    - Recibe las peticiones de solicitud de importación.
    - Realiza las comprobaciones necesarias y autoriza o no la exportación.

Configuración de la exportación (I)

- El fichero donde se indican los sistemas exportados es /etc/exports. Sus líneas tienen la sintaxis:

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

- Donde:
  - <sistema de ficheros>: Directorio o dispositivo exportado.
  - <ordenador/es>: Lista de ordenadores a los que se exporta.
  - (opciones de exportación): Propiedades de la exportación.
- Sistema de ficheros:
  - /var/ftp
  - /home
  - /dev/cdrom

Configuración de la exportación (II)

- Los ordenadores a los que se exporta pueden especificarse como:
  - Un ordenador particular:
    - Nombre del ordenador: glup.irobot.uv.es
    - Dirección IP del ordenador: 147.156.222.65
  - Un conjunto de ordenadores utilizando los comodines * y ?.
    - *.irobot.uv.es
    - lab3inf??.informat.uv.es
  - Una red o subred:
    - 147.156.222.0/23
- Las opciones de exportación se dividen en dos grupos:
  - Modo de exportación.
  - Modificación de identificadores de usuarios.

Configuración de la exportación (III)

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.
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.

Configuración de la exportación (IV)

- El permiso de acceso a los ficheros exportados se basa en:
  - El UID y el GID de los ficheros exportados.
  - El UID y el GID del usuario remoto que intenta acceder.
  - Si el usuario remoto tiene permiso puede acceder a los ficheros exportados.
- Todos los usuarios “root” tienen UID y GID con valor cero.
  - De forma general “root” es convertido a nobody (UID=65534) y su GID a nfsnobody (GID=65534).

Configuración de la exportación (V)

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.

Configuración de la exportación (VI)

- Ejemplo:

```
# Exportamos el directorio de ftp anónimo de glup a todos los
# ordenadores de Robótica.
/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 su ordenador personal.
/home/quique      147.156.222.34(rw,sync)
# Exportamos el directorio de root para poder leer su
# información desde Robótica.
/root             147.156.222.0/23(ro,sync,no_root_squash)
```

- Importancia de una sintaxis correcta:

`/home 147.156.222.65(rw)`

  - Exporta /home a 147.156.222.65 en lectura/escritura.

`/home 147.156.222.65 (rw)`

  - Exporta /home a 147.156.222.65 en modo lectura y al resto de Internet en lectura y escritura.

El cliente de NFS

- El cliente de NFS debe ejecutar el servicio de rpcbind (igual que sucede con el servidor).
- La forma más sencilla de montarlo es:

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

- No es práctica, pues el administrador debe intervenir siempre.
- Posibilidades:
  - Usar el fichero /etc/fstab.
  - Usar el servicio autofs.

Utilización de fichero /etc/fstab (I)

- El fichero /etc/fstab contiene los sistemas locales a ser montados.

```
/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
```

- Pueden añadirse líneas para montar los sistemas exportados por otros ordenadores:

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

- Donde:
  - <servidor>:<directorio>: Ordenador y directorio exportado.
  - <punto de montaje>: Directorio local donde montar el sistema.
  - nfs: Tipo de sistema de archivos.
  - <opciones>: Opciones de montaje del sistema.
  - 0 0 : El sistema no debe ser volcado y no sebe ser chequeado al arrancar.

Utilización de fichero /etc/fstab (II)

Opción	Descripción.
hard	El cliente debe esperar hasta que el sistema exportado por el servidor este disponible.
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.

Utilización de fichero /etc/fstab (III)

- 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
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
```

Utilización del servicio autofs (I)

- El servicio de autofs:
  - Se basa en la utilidad del kernel automount.
  - Monta y desmonta de forma automática los sistemas de ficheros NFS al ser requeridos.
- El servicio se activa mediante la orden:

```
systemctl start autofs.service
```

- El fichero de configuración es /etc/auto.master.
  - Esta formado por líneas con la sintaxis:

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

    - <punto de montaje>: Directorio donde montar el sistema de ficheros.
    - <mapa tipo>: Fichero con el nombre del servidor/es, sistemas de ficheros, etc.
    - <opciones>: Opciones comunes de montaje a todo el <mapa tipo>.
- Ejemplo:

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

Utilización del servicio autofs (II)

- Los ficheros <mapa tipo> tienen la sintaxis:

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

- Donde:
  - <directorio de montaje>: Directorio donde montar, dentro del directorio indicado en /etc/auto.master.
  - <opciones>: Opciones de montaje que deseamos.
    - Pueden añadirse/modificar las indicadas en /etc/auto.master.
  - <servidor>:<directorio>: Sistema de ficheros a montar.
- Ejemplo:

```
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
```

Utilización del servicio autofs (III)

- Los ficheros <mapa tipo> admiten los comodines & y *.
- El carácter &:
  - Puede ser usado en <servidor> y/o <directorio>.
  - Indica que se busquen todas las entradas que respondan a la línea indicada.
    - Usado en <servidor> sustituye el nombre del servidor.
    - Usado en <directorio> sustituye solo el nombre del último directorio.
    - En el ejemplo anterior:
      - Puede ponerse glup:/home/& para que & indique quique y terradez.
      - No puede ponerse glup:/&.
- El carácter *:
  - Se utiliza en el campo <directorio de montaje>.
  - Indica que se utilice como directorio el obtenido de la búsqueda de las entradas realizadas con el carácter &.

Utilización del servicio autofs (IV)

- Ejemplos:

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

  - Montar todos los directorios exportados de:
    - glup, directorio /home.
    - Dentro del directorio /glup/“usuario”.
      - Debe existir el directorio /glup.
      - El directorio “usuario” puede crearse de forma dinámica.

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

  - Montar todos los directorios exportados de:
    - Cualquier ordenador, directorio /home.
    - Dentro del directorio /mnt/“ordenador”/“directorio”
      - Suponemos que /mnt es el punto de montaje indicado en /etc/auto.master.
      - El subdirectorio “ordenador” debe existir.
      - El directorio “usuario” puede crearse de forma dinámica.

Montaje automático sistemas de ficheros locales

- Podemos montar y desmontar automáticamente sistemas de ficheros locales.
  - No es necesaria la configuración del servidor de NFS ni su arranque.
  - Solo es necesario:
    - Modificar /etc/auto.master.
    - Crear los ficheros <mapa tipo> indicados.
    - Activar el servicio autofs.
- Ejemplo:
  - Fichero /etc/auto.master:

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

  - Fichero /etc/auto.mnt:

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

Seguridad en el servicio NFS (I)

- Respecto al servidor:
  - Es necesario habilitar servicios en el tcp_wrapper:
    - Servicio de rpcbind.
  - Permitir el acceso a puertos:
    - rpcbind: 111 TCP y UDP.
    - rpc.nfsd: 2049 TCP y UDP.
    - rpc.rquotad y rpc.mountd:
      - De forma general elige un puerto aleatorio.
      - Si deseamos fijar el puerto podemos hacerlo con la opción -p.
      - Se pueden especificar los puertos con las opciones RPCRQUOTADOPTS=”- p <puerto>” y RPCMOUNTDOPTS=”-p <puerto>” en el fichero /etc/sysconfig/nfs.
  - Si se utilizan nombres en /etc/exports:
    - Un ataque al DNS puede permitir exportar a ordenadores incorrectos.

Seguridad en el servicio NFS (II)

- Respecto al cliente:
  - Es necesario habilitar servicios en el tcp_wrapper para el rpcbind.
  - Permitir el acceso al puerto 111 TCP y UDP.
  - Permitir el acceso de los puertos donde se ejecutan los servicios de rpc.rquotad y rpc.mountd.