Administración de Sistemas

8 - Administración de NFS

Diciembre 2003

Guillermo Pérez Trabado

Dept. Arquitectura de Computadores

Universidad de Málaga

Descripción de NFS

- Network Filing System (NFS) está concebido para que un servidor UNIX pueda exportar directorios a un grupo de máquinas a través de la red.
- Cada máquina puede funcionar como servidor de ficheros o como cliente simultáneamente.
- El servidor requiere varios daemons:
  - rpc.mountd: se encarga de verificar si los clientes que piden acceso están autorizados a usar un volumen exportado.
  - nfsd: es el proceso que atiende las peticiones de acceso a los ficheros.
  - lockd y statd: estos daemons implementan un protocolo adicional para bloquear ficheros usados remotamente a través de NFS, ya que el protocolo básico de NFS no soporta bloqueo de ficheros.
- El software cliente de NFS forma parte del núcleo de UNIX.

Funcionamiento del servidor

- La exportación desde el servidor se basa en el concepto de directorio:
  - Cuando se exporta un directorio, se hace accesible toda la jerarquía de directorios que cuelga bajo ese punto en el sistema de ficheros del servidor.
  - Un directorio se puede exportar con distintos derechos de acceso a distintos clientes.
  - No se puede exportar un subdirectorio que cuelgue de otro directorio que ya haya sido exportado. En Linux esto sí es posible solo si se exportan a clientes distintos.
- El fichero **/etc/exports** controla la lista de directorios exportados.
  - Si se altera el fichero hay que actualizar la lista en el kernel mediante el comando **exportfs**.

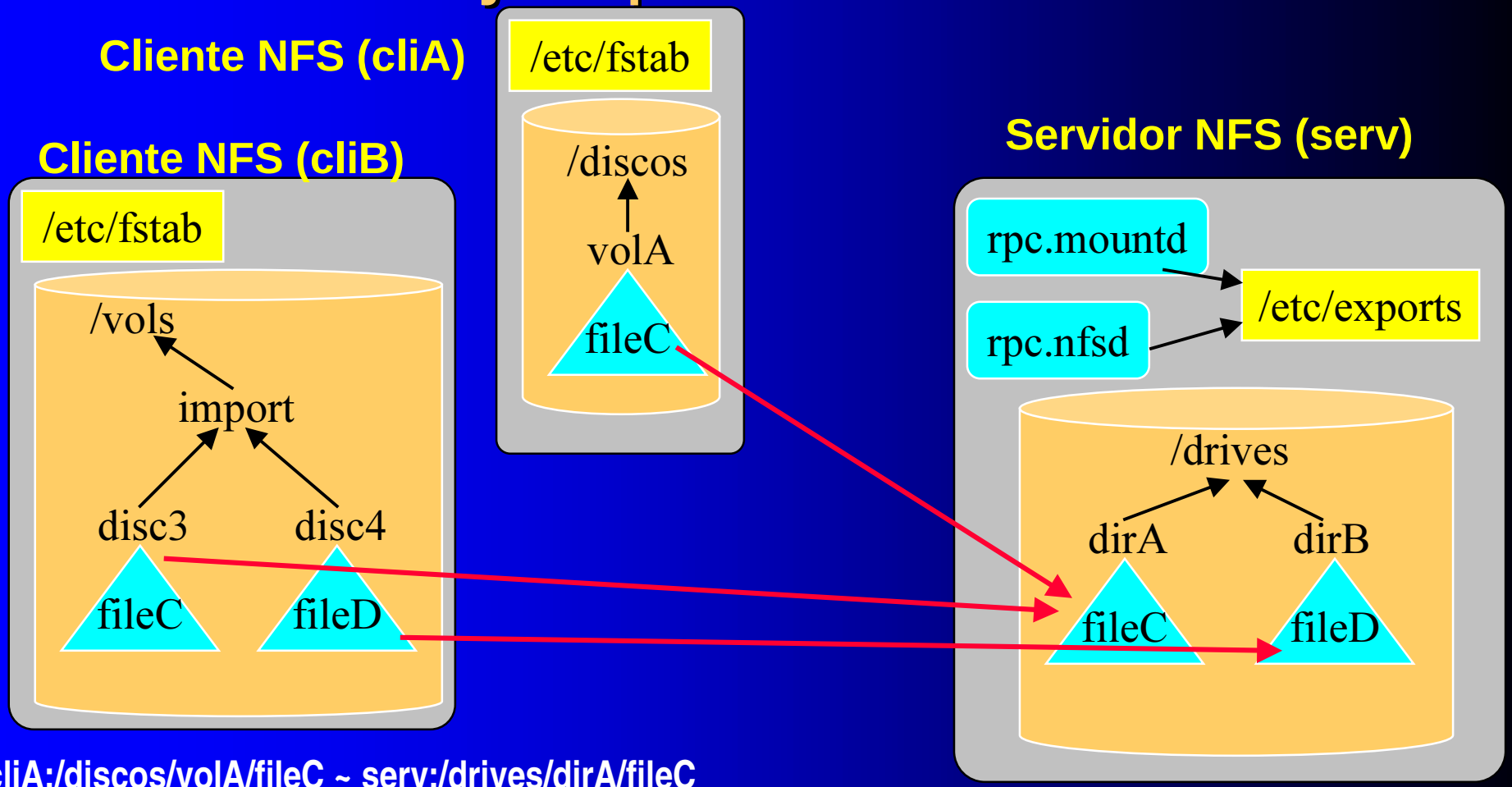
Funcionamiento del cliente

- El acceso del cliente se basa en el mismo concepto de sistemas de ficheros y puntos de montaje usado para los dispositivos locales:
  - Los directorios remotos han de montarse antes de acceder a ellos y desmontados antes de apagar el sistema.
  - Cada directorio remoto requiere que se especifique un punto de montaje en el sistema de ficheros local.
  - Cada directorio remoto montado pasa a ser visto como un árbol completo accesible bajo el punto de montaje.
  - Cada cliente de una red puede montar el mismo directorio remoto en un punto de montaje local distinto.
  - Un cliente no puede re-exportar por NFS un directorio importado por NFS desde otro servidor.
- El fichero **/etc/fstab** incluye la lista de directorios importados.
  - Si se altera el fichero hay que montar/desmontar los directorios mediante el comando **mount**.

Protocolo de comunicación

- NFS usa UDP por defecto aunque también puede usar TCP.
- El servidor no preserva ningún estado de los ficheros accedidos.
  - Cuando se abre un fichero entrega al cliente un ***descriptor de fichero***.
  - El cliente preserva en su kernel los descriptores de los ficheros que abre en el servidor.
- El cliente usa operaciones del tipo:
  - Leer atributos de fichero (descriptor)
  - Leer bloque de datos (descriptor, offset, bloque de datos)
  - Escribir bloque de datos (descriptor, offset, bloque de datos)
- El servidor puede ser reiniciado sin que los clientes se enteren.
- Los clientes pueden ser reiniciados sin que el servidor deje ficheros bloqueados:
  - NFS no permite bloquear ficheros remotos.
  - Existe un protocolo adicional para bloquear los ficheros remotamente y para controlar las cuotas de uso de disco.

Ejemplo de NFS



cliA:/discos/volA/fileC ~ serv:/drives/dirA/fileC

cliB:/vols/disc3/fileC ~ serv:/drives/dirA/fileC

cliB:/vols/disc4/fileD ~ serv:/drives/dirB/fileD

Directorio montado

Lista de exportación del servidor

- El daemon rpc.nfsd contiene una lista de directorios exportados.
- El comando **exportfs** permite modificar dicha lista de directorios exportados.
- Los directorios a exportar al arrancar el sistema se indican mediante el fichero /etc/exports.
  - Cada línea define un directorio a exportar y la lista de clientes que pueden acceder con las opciones de acceso individualizadas:

    ```
    /drives/dirA cliA(rw,secure) cliB(ro,no_root_squash)
    /drives/dirB cliB(rw) 150.214.54.0/255.255.255.0(ro)
    ```
  - Después de modificar el fichero se puede actualizar la lista del daemon rpc.nfsd mediante el comando "**exportfs –r**".
- La lista del daemon se puede manipular sin modificar el fichero /etc/exports:
  - Vaciar la lista de directorios exportados: exportfs –v –a –u
  - Añadir todos los directorios listados en /etc/exports: exportfs –v –a
  - Mostrar la lista exportada actualmente: exportfs –v

Opciones en /etc/exports

- ro/rw: Solo lectura/Lectura-Escritura
- no_root_squash/root_squash: Permitir el acceso como root desde el cliente/No permitir el acceso como root (el usuario root se traduce en el usuario nobody).
- all_squash: todos los usuario del cliente acceden como usuario nobody.
- sync/async: El servidor debe escribir inmediatamente en el medio físico para cada operación de escritura del cliente/el servidor puede diferir las escrituras.
- secure/insecure: requiere que el puerto UDP del cliente sea menor que 1024, para evitar programas de los usuarios que imiten el comportamiento de un cliente de NFS/permite el acceso desde números de puerto UDP ≥ 1024.

Lista de montaje del cliente

- El kernel contiene una lista de sistemas de ficheros montados.
- El comando **mount** permite modificar dicha lista.
- Los sistemas de ficheros a montar al arrancar el sistema se indican mediante el fichero /etc/fstab.
  - Cada línea define un sistema a montar, el punto de montaje y las opciones:
    ```
    <host>:<dir_remoto> <dir_local> nfs <opciones> 0 0
    ```
  - Ejemplo:
    ```
    serv1:/drives/sistema1 /discos/volA nfs rw,hard,bg 0 0
    serv2:/usuarios2 /discos/volB nfs rw,soft,noexec 0 0
    ```
  - Después de modificar el fichero se pueden montar los directorios definidos con "**mount –a –t nfs**". Nota: el comando mount no crea los directorios para los puntos de montaje.

Opciones para NFS en /etc/fstab

- ro/rw: Solo lectura/Lectura-Escritura
- fg/bg: Si el primer intento de montaje falla, el comando mount se bloquea hasta que se consigue/el comando mount termina pero se continua intentando montar el directorio.
- hard/soft: Si una operación de acceso da un timeout, se reintenta indefinidamente/se retorna un error de E/S al proceso que accede.
- intr: Si se envía un signal a un proceso bloqueado en una operación de NFS que ha dado un timeout (modo hard) se puede abortar la operación de E/S. En caso contrario, no es posible matar al proceso ya que está bloqueado en una operación dentro del kernel.
- rsize=8192/wsize=8192: Permite cambiar el tamaño de bloque mínimo de las operaciones de acceso (en bytes). Permite incrementar la eficiencia cuando se transfieren ficheros grandes.
- tcp/udp: Usa una conexión TCP/datagramas UDP.

Pasos para configurar el servidor

1. Activar los servicios nfs y nfslock mediante chkconfig. Editar primero la cabecera de /etc/init.d/nfs para fijar los niveles de arranque y luego usar:
```
# chkconfig -del nfs
# chkconfig -add nfs
```
2. Si es necesario arrancar los servicios nfs y nfslock con:
```
# service nfs start; service nfslock start
```
3. Si se quiere incrementar la seguridad restringiendo las direcciones IP que pueden acceder al servidor, editar /etc/hosts.allow y añadir una lista de acceso para el servicio mountd con las direcciones IP que pueden acceder. Ejemplo:
```
mountd:192.168.16.0/255.255.255.0, 150.214.232.139 : ALLOW
```
4. Editar el fichero /etc/exports añadiendo los directorios a exportar:
```
/discos 192.168.16.1(rw,no_root_squash)
   150.214.232.139(rw)
```
5. Ejecutar "**exportfs –v –r**" para actualizar la lista de directorios exportados del kernel con el contenido de /etc/exports.

Pasos para configurar el cliente

1. Activar el servicio netfs mediante **chkconfig**.
2. Editar /etc/fstab y añadir los puntos de montaje NFS.
3. Si queremos montar todos los directorios remotos especificados en **fstab** durante el funcionamiento del sistema podemos hacerlo manualmente con:
   `# mount -a -t nfs`
4. Si queremos desmontar todos los directorios remotos durante el funcionamiento del sistema podemos hacerlo manualmente con:
   `# umount -a -t nfs`

- También podemos montar temporalmente un directorio que no esté especificado en **/etc/fstab** especificando el comando **mount** con todos sus argumentos:
  - `# mount -t nfs -o opciones,... servidor:/directorio /punto_de_montaje`
- Para desmontarlo basta especificar el punto de montaje con **umount**:
  - `# umount /punto_de_montaje`

Comandos útiles

- showmount: Permite examinar el estado de un servidor NFS. Si se especifica un nombre de un servidor se puede consultar el estado de otro sistema remotamente.
  - “showmount –e” muestra la lista de directorios exportados en este momento por el kernel. Nota: La lista del kernel puede no coincidir con la lista de /etc/exports en un momento dado.
  - “showmount –a” muestra la lista de clientes que actualmente tienen montado algún directorio de este servirdor y el directorio que montan.
- nfsstat: Permite ver estadísticas del funcionamiento de NFS para el sistema en que se ejecuta el comando tanto del servidor como del cliente NFS. Es útil para ver si hay retransmisiones a nivel de RPC (errores de transmísión o pérdida de paquetes).
- mount: Muestra la lista de directorios montados. Es útil para ver qué opciones se han usado en el comando mount.

Problemas de seguridad

- El control de acceso a cada directorio exportado por el servidor NFS se basa solamente en comprobar la dirección IP de los sistemas clientes que intentan montar dicho volumen.
  - Un usuario podría impersonar la dirección del cliente desde otra máquina instalando un sistema UNIX por su cuenta con esa dirección.
- Para cada operación de acceso a un fichero del servidor, el sistema cliente especifica el **uid** del proceso en la petición. En el servidor se usa ese **uid** para realizar el acceso aunque el usuario no esté declarado en la lista de usuarios:
  - Si el root del sistema cliente quiere forzar el acceso a un fichero propiedad de un usuario podría declarar un usuario local a su máquina con el mismo uid que otro usuario del servidor.
  - Solución: no exportar directorios del servidor a un sistema cuyo password de root sea controlado por un usuario no administrador.
- El servidor NFS convierte el uid=0 (root) en uid=-1 (nobody) para todos los accesos por defecto. Esto implica que el root del sistema cliente no tiene acceso como root a ficheros del servidor a través de NFS.
  - Si se especifica la opción **no_root_squash** en /etc/exports se puede activar el acceso como root individualmente por cada directorio.