

UNIVERSIDAD SIMON BOLIVAR
Unidad de Laboratorios "F"
Laboratorio Docente de Computación
LDC-Daniel Campello

Network File System (NFS)

Sartenejas, 28 de Mayo - 2.007

NFS

1. Introduccion.

El Network File System (Sistema de archivos de red), o NFS, es un sistema de archivos distribuido para un entorno de red de área local. Posibilita que distintos sistemas conectados a una misma red accedan a ficheros remotos como si se tratara de locales. Originalmente desarrollado por Sun Microsystems en 1984.

El protocolo de NFS está diseñado para ser independiente de la máquina, el sistema operativo y el protocolo de transporte. Esto es posible porque se implementa sobre RPC.

El sistema NFS fue desarrollado para permitir montar una partición perteneciente a una máquina remota como si fuese una partición local. Nos proporciona, por tanto, un método rápido y eficaz de compartir archivos y espacio de disco entre distintos ordenadores de una red que soporte este sistema.

Los servicios de NIS y NFS son parte de los servicios llamados RPC y son complementarios.

NFS es un protocolo que data de los años 80. En esas fechas los problemas de seguridad eran menores. Todavía podían construirse protocolos basados en la confianza, tanto el servidor como el cliente confiando en la información que intercambian. Internet convierte este principio en algo absurdo y este es sin duda uno de los mayores problemas de NFS. La versión 2 del protocolo es la primera versión publicada y sigue la siendo la más extendida en nuestros días.

Existen implementaciones sobre varias plataformas diferentes y se han descrito pocos problemas de compatibilidad.

La versión 3 del protocolo data de 1992 y presenta varias mejoras:

- Mejora del rendimiento debido a la reescritura del código de la red, y al uso de paquetes de datos mayores.
- Mejora en la seguridad:
 - Listas de ACL (Listas de control de acceso) que permiten definir acceso a los recursos por UID y fichero a fichero.
 - Implementación de un sistema de autenticación basado en contraseña.

2. Funcionamiento teórico.

NFS es una interfaz entre el sistema de ficheros físico, sea el que sea -ext2 por ejemplo- y un sistema remoto. Cuando NFS recibe una petición vía red, opera las modificaciones sobre el sistema local.

NFS dispone de todo lo que podemos esperar de un sistema de ficheros tipo Unix: gestión de permisos, propiedades avanzadas, enlaces, tuberías con nombre ... Pero como indica su nombre ha sido ideado para ser usado de forma transparente a través de la red.

Desde el punto de vista del cliente, se trata de un sistema de ficheros clásico, se monta con mount, y se integra en la jerarquía de ficheros existente en la máquina. Todas las órdenes de entrada salida son enviadas al servidor que se encarga de procesarlas, controlar acceso concurrente a ficheros, etc.

3. Características.

- El sistema NFS está dividido al menos en dos partes principales: un servidor y uno o más clientes. Los clientes acceden de forma remota a los datos que se encuentran almacenados en el servidor.
- Las estaciones de trabajo locales utilizan menos espacio de disco debido a que los datos se encuentran centralizados en un único lugar pero pueden ser accedidos y modificados por varios usuarios, de tal forma que no es necesario replicar la información.
- Los usuarios no necesitan disponer de un directorio home en cada una de las máquinas de la organización. Los directorios home pueden crearse en el servidor de NFS para posteriormente poder acceder a ellos desde cualquier máquina a través de la infraestructura de red.
- También se pueden compartir a través de la red dispositivos de almacenamiento como disqueteras, CD-ROM y unidades ZIP. Esto puede reducir la inversión en dichos dispositivos y mejorar el aprovechamiento del hardware existente en la organización.

Todas las operaciones sobre ficheros son síncronas. Esto significa que la operación sólo retorna cuando el servidor ha completado todo el trabajo asociado para esa operación. En caso de una solicitud de escritura, el servidor escribirá físicamente los datos en el disco, y si es necesario, actualizará la estructura

de directorios, antes de devolver una respuesta al cliente. Esto garantiza la integridad de los ficheros.

4. Operaciones.

El programa NFS soporta 18 procedimientos para todas las operaciones básicas de E/S, como por ejemplo:

- LOOKUP: busca un fichero en el directorio actual y si lo encuentra, devuelve un descriptor a ese fichero más información sobre los atributos del fichero.
- READ y WRITE: primitivas básicas para acceder el fichero.
- RENAME: renombra un fichero.
- REMOVE: borra un fichero.
- MKDIR y RMDIR: creación/borrado de subdirectorios.
- GET y SET-ATTR: devuelve conjuntos de atributos de ficheros.

Se corresponden con la mayoría de primitivas de E/S usadas en el sistema operativo local para acceder a ficheros locales. De hecho, una vez que se ha montado el directorio remoto, el sistema operativo local tiene que reencaminar” las primitivas de E/S al host remoto. Esto hace que todas las operaciones de E/S sobre ficheros tengan el mismo aspecto, independientemente de si el fichero es local o remoto. El usuario puede trabajar con los comandos y programas habituales en ambos tipos de ficheros; en otras palabras, el protocolo NFS es completamente transparente al usuario.

5. Versiones.

Hay tres versiones de NFS actualmente en uso.

- La versión 2 de NFS (NFSv2), es la más antigua y está ampliamente soportada por muchos sistemas operativos.
- La versión 3 de NFS (NFSv3) tiene más características, incluyendo manejo de archivos de tamaño variable y mejores facilidades de informes de errores, pero no es completamente compatible con los clientes NFSv2.

- NFS versión 4 (NFSv4) incluye seguridad Kerberos (protocolo de autenticación de redes de ordenador que permite a dos computadores en una red insegura demostrar su identidad mutuamente de manera segura), trabaja con cortafuegos, permite ACLs y utiliza operaciones con descripción del estado.

6. Montando el servicio.

6.1. Que necesitamos?

Necesitaremos tener instalado portmap y el paquete nfs (nfs-utils) que se puede encontrar en la mayoría de las distribuciones en el ordenador que vaya a hacer de servidor de disco.

El portmap nos permitirá realizar conexiones RPC al servidor y es el encargado de permitir o no el acceso al servidor a los equipos que especifiquemos.

Para saber si tenemos el portmap instalado bastará con un simple

```
» psaux | grepportmap
```

Deberíamos tener una salida parecida a

```
rpc 1261 0.0 0.1 1560 568 ? S 15:48 0:00 portmap
jdaniel 2544 0.0 0.1 1916 772 pts/0 S 16:04 0:00 grep portmap
```

Para saber si NFS está en marcha haremos una consulta al portmap para que nos indique qué servicios tiene en marcha

```
» rpcinfo -p
```

Que en mi servidor proporciona la siguiente salida

```
programa vers proto puerto
100000 2 tcp 111 portmapper
100000 2 udp 111 portmapper
100024 1 udp 1024 status
100024 1 tcp 1024 status
100011 1 udp 944 rquotad
100011 2 udp 944 rquotad
```

```
100011 1 tcp 947 rquotad
100011 2 tcp 947 rquotad
100005 1 udp 1025 mountd
100005 1 tcp 1056 mountd
100005 2 udp 1025 mountd
100005 2 tcp 1056 mountd
100005 3 udp 1025 mountd
100005 3 tcp 1056 mountd
100003 2 udp 2049 nfs
100003 3 udp 2049 nfsv
100021 1 udp 1026 nlockmgr
100021 3 udp 1026 nlockmgr
100021 4 udp 1026 nlockmgr
```

Debemos verificar que portmap proporciona el servicio nfs. De no ser así es normalmente porque no hemos instalado el paquete nfs-utils.

6.2. Compratiendo el disco.

Una vez tenemos los servicios en marcha únicamente nos falta determinar qué queremos compartir. En mi caso me interesaba poder acceder al directorio home y al directorio /var/db.

Debemos editar el archivo /etc/exports e introducir

```
/usr/local 192.168.0.0/255.255.255.0(rw)
/var/db 192.168.0.0/255.255.255.0(rw)
```

Con esto estamos indicando que vamos a exportar /usr/local y /var/db permitiendo acceso a nuestro rango de direcciones locales en modo de lectura/escritura.

Aunque en mi caso este tipo de exportación es suficiente, podríamos haber indicado únicamente un equipo o varios de ellos. Por ejemplo, si hubiese querido dar acceso a /tmp únicamente al equipo 192.168.0.10 en modo sólo lectura, hubiese añadido

```
/tmp 192.168.0.10(ro)
```

6.3. Opciones de /etc/exports:.

- ro: Sólo lectura (read-only). Las máquinas no pueden cambiar el sistema de archivos.

- rw: Lectura-escritura (read-write).
- async: Permite al servidor escribir los datos en el disco cuando lo crea conveniente.
- sync, todas las escrituras en el disco deben hacerse antes de devolver el control al cliente.
- wdelay: El servidor NFS retrasa la escritura en disco si sospecha que otra petición de escritura es inminente.
- no_wdelay para desactivar esta opción, la cual sólo funciona si está usando la opción sync.
- root_squash Previene a los usuarios root conectados remotamente de tener privilegios como root local.
- no_root_squash lo desactiva.
- all_squash: Para reconvertir a todos los usuarios.

Es posible crear cuentas de usuarios especiales para usuarios NFS remotos, especificando sus ID, mediante las opciones:

- anonuid: Permite especificar la ID del usuario remoto de una máquina en particular. (anonuid=IDusuario).
- anongid: Igual que la opción anterior pero para grupos. (anongid=IDgrupo).

6.4. Un poco de seguridad.

La prudencia nos aconseja editar los ficheros `/etc/hosts.allow` y `/etc/hosts.deny` para acabar de especificar qué ordenadores de la red pueden usar los servicios del servidor. La documentación del NFS recomienda las siguientes entradas

```

/etc/hosts.deny
portmap:ALL
lockd:ALL
mountd:ALL
rquotad:ALL
statd:ALL

```

```

/etc/hosts.allow
portmap:192.168.0.0/255.255.255.0
lockd:192.168.0.0/255.255.255.0

```

```
mountd:192.168.0.0/255.255.255.0
rquotad:192.168.0.0/255.255.255.0
statd:192.168.0.0/255.255.255.0
```

Para una red privada esto puede ser suficiente. De todos modos podríamos hacer una configuración mucho más fina especificando para cada servicio las direcciones IP que tendrán acceso a él.

6.5. Iniciar el proceso de compartir archivos.

Si hemos cambiado el fichero `/etc/exports` después de iniciar el servicio NFS deberemos indicar al sistema que relea el fichero y active los cambios. Esto lo podemos hacer reiniciando el demonio `nfsd` o bien mediante

```
» exportfs -ra
```

Lo siguiente es una lista de las opciones más comunes disponibles para `/usr/sbin/exportfs`:

- `-r` Provoca que todos los directorios listados en `/etc/exports` sean exportados construyendo una nueva lista de exportación en `/etc/lib/nfs/xtab`. Esta opción refresca la lista de exportación con cualquier cambio que hubiéramos realizado en `/etc/exports`.
- `-a` Provoca que todos los directorios sean exportados o no, dependiendo de qué otras opciones hemos pasado a `/usr/sbin/exportfs`. Si no se pasan otras opciones, `/usr/sbin/exportfs` exporta todos los sistemas de archivos especificados en `/etc/exports`.
- `-o sistema-de-archivos` Permite especificar directorios a exportar que no estén listados en `/etc/exports`. Reemplace `sistema-de-archivos` con los sistemas de archivos adicionales a exportar. Estos sistemas de archivos deben tener el mismo formato en que fueron especificados en `/etc/exports`. Esta opción se utiliza a menudo para probar un sistema de archivos antes de añadirlo de forma permanente a la lista de sistemas a exportar.
- `-i` Ignora `/etc/exports`; sólo las opciones dadas desde la línea de comandos son usadas para definir los sistemas de archivos exportados.
- `-u` No exporta todos los directorios compartidos. El comando `/usr/sbin/exportfs -ua` suspende la compartición de archivos NFS mientras que mantiene todos los demonios NFS activos. Para reactivar NFS, teclee `exportfs -r`.
- `-v` Operación descriptiva, donde los sistemas de archivos exportados o dejados de exportar son mostrados en gran detalle al ejecutarse el comando `exportfs`.

6.6. Configuración de un equipo cliente NFS.

Ahora que ya tenemos el servidor funcionando vamos a acceder al espacio compartido desde un ordenador cliente.

Como root ejecutamos

```
» mount -tnfs < servidor >:< directoriocompartido >< puntodemontaje >
```

En mi sistema el servidor es la máquina 192.168.0.2 y el punto de montaje lo he dispuesto en /mnt/nfs que he creado en la máquina cliente.

Así y para nuestro ejemplo bastará ejecutar como root

```
» mount -tnfs192,168,0,2 : /home/mnt/nfs
```

Un simple ls /mnt/nfs nos tendría que permitir ver que ya tenemos acceso al disco del servidor.

Si queremos que el sistema de ficheros NFS sea montado al arrancar deberemos añadir una entrada en el fichero /etc/fstab. En nuestro ejemplo añadiríamos

```
192.168.0.2:/home /mnt/nfs nfs rw,hard,intr 0 0
```

7. Usando el servicio autofs.

Autofs utiliza el demonio automount para controlar los puntos de montaje montándolos o desmontándolos automáticamente cuando sea necesario ahorrando recursos.

Autofs consulta el archivo de configuración /etc/auto.master para ver los puntos de montaje definidos y arranca automount. Cada línea del mapa maestro define un punto de montaje. Un archivo separado define el sistema de archivos a montar en el punto de montaje. etc/auto.pto_mnt define los puntos de montaje en el directorio /pto_mnt

```
Archivo auto.master:  
/pto_mnt /etc/auto. pto_mnt  
Archivo /etc/auto. pto_mnt
```

/pto_mnt opciones servidor.ejemplo.es:/dir/export

8. Referencias Electrónicas

- http://es.wikipedia.org/wiki/Network_File_System
- <http://bulma.net/body.phtml?nIdNoticia=1255>
- <http://bulma.net/body.phtml?nIdNoticia=1841>
- <http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-rg-es-4/ch-nfs.html>