



Search the Web.

Cómo configurar un servidor NFS. v. 1.1.3

Actualizado el Jueves 14/11/2001, 05:29:46 GMT -0600.

Joel Barrios Dueñas

jbarrios@-QUITAR-ESTO-linuxparatodos.com

<http://www.linuxparatodos.com/>

Copyright.

© 2001 Linux Para Todos. Se permite la libre distribución y modificación de este documento por cualquier medio y formato mientras esta leyenda permanezca intacta con el documento y la distribución y modificación se hagan de acuerdo con los términos de la Licencia Pública General GNU publicada por la Free Software Foundation; sea la versión 2 de la licencia o (a su elección) cualquier otra posterior. La información contenida en este documento y los derivados de éste se proporcionan tal cual son y los autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de éstos.

Introducción.



NFS, acrónimo de *Network File System*, es un popular protocolo utilizado para compartir volúmenes entre máquinas dentro de una red de manera transparente, más comúnmente utilizado entre sistemas basados sobre UNIX®. Es útil y fácil de utilizar, sin embargo no en vano es apodado *carñosamente* como "No File Security". NFS no utiliza un *sistema de contraseñas como el que tiene SAMBA*, solo una lista de control de acceso determinada por direcciones IP o nombres. Es por esto que es importante que el administrador de la red local o usuario entienda que un servidor NFS puede ser un verdadero e inmenso agujero de seguridad si este no es configurado apropiadamente e implementado detrás de un contrafuegos o firewall.

Personalmente, solo recomiendo utilizar NFS dentro de una red local detrás de un contrafuegos o firewall que permita el acceso solo a las máquinas que integren la red local, nunca para compartir sistemas de archivos a través de Internet. Al no contar con un sistema de autenticación por contraseñas, es un servicio susceptible del ataque de algún *cracker*. SAMBA es un mucho mejor y más seguro protocolo para compartir sistemas de archivos.

Procedimientos.

Teniendo en cuenta los aspectos de seguridad mencionados, es importante que siga los procedimientos descritos a continuación al pie de la letra, y que posteriormente se comprometa también consultar a detalle la documentación incluida en el paquete *nfs-utils*, ya que este le proporcionará información adicional y completa sobre aspectos avanzados de configuración y utilización.

Configurando el servidor NFS.

Se requiere tener instalados *nfs-utils* y *portmap*. Preguntaremos al sistema si estos están instalados con la siguiente línea de comando:

```
rpm -q nfs-utils portmap
```

Lo cual debe de regresarle algo como lo siguiente:

```
nfs-utils-0.3.1-13.7.2.1  
portmap-4.0-38
```

En caso de que falte alguno de estos paquetes, inserte el CD de instalación en la unidad correspondiente, abra una terminal o consola y ejecute lo siguiente:

```
mount /mnt/cdrom/  
rpm -Uvh /mnt/cdrom/RedHat/RPMS/paquete_faltante
```

Cabe mencionar que lo mejor será siempre utilizar la versiones de *nfs-utils* y *portmap* más actuales. Salvo por RedHat® Linux 7.1 o LinuxPPP 7.x, el resto de las versiones anteriores de RedHat® y LinuxPPP® incluyen paquetes de *nfs-utils* y *portmap* con serios agujeros de seguridad. Visite el servidor ftp de la distribución utilizada y descargue los paquetes actualizados, que seguramente incluirán los parches de seguridad necesarios:

- <ftp://updates.redhat.com/6.0/en/os/i386/>, si posee alguna distribución basada sobre RedHat® Linux 6.0
- <ftp://updates.redhat.com/6.1/en/os/i386/>, si posee alguna distribución basada sobre RedHat® Linux 6.1
- <ftp://updates.redhat.com/6.2/en/os/i386/>, si posee alguna distribución basada sobre RedHat® Linux 6.2 -como serían LinuxPPP® 6.2, 6.3 y 6.4-
- <ftp://updates.redhat.com/7.0/en/os/i386/>, si posee alguna distribución basada sobre RedHat® Linux 7.0
- <ftp://updates.redhat.com/7.1/en/os/i386/>, si posee alguna distribución basada sobre RedHat® Linux 7.1
- <ftp://updates.redhat.com/7.2/en/os/i386/>, si posee alguna distribución basada sobre RedHat® Linux 7.1

Si utiliza Redhat 6.x o LinuxPPP 6.x, la más reciente versión de *nfs-utils*, que corresponde a la 0.3.1, requerirá además que actualice el paquete *mount* a su versión 2.10r o superior, y que también podrá encontrar en el mismo directorio del servidor ftp.

Lo siguiente será configurar un nivel de seguridad para *portmap*. Esto se consigue editando los ficheros */etc/hosts.allow* y */etc/hosts.deny*. Debemos especificar que direcciones IP o rango de direcciones IP pueden acceder a los servicios de *portmap* y quienes no pueden hacerlo. Podemos entonces determinar en */etc/hosts.allow* como rango de direcciones IP permitidas lo siguiente:

```
portmap:192.168.1.0/255.255.255.0
```

Esto corresponde a la dirección IP de la red completa y la máscara de la subred. Adicionalmente podemos especificar direcciones IP individuales sin necesidad de establecer una máscara. Esto es de utilidad cuando se desea compartir volúmenes con otras máquinas en otras redes a través de Internet. Ejemplo:

```
portmap:192.168.1.0/255.255.255.0  
portmap:192.168.20.25  
portmap:192.168.30.2  
portmap:216.200.152.96  
portmap:148.240.28.171
```

Una vez determinado que direcciones IP pueden acceder a *portmap*, solo resta determinar quienes no pueden hacerlo. Evidentemente nos referimos al resto del mundo, y esto se hace agregando la

```
portmap:216.200.152.96
portmap:148.240.28.171
```

Una vez determinado que direcciones IP pueden acceder a portmap, solo resta determinar quienes no pueden hacerlo. Evidentemente nos referimos al resto del mundo, y esto se hace agregando la siguiente línea:

```
portmap:ALL
```

Es importante destacar que la línea anterior es **INDISPENSABLE** y **NECESARIA** si quiere tener un nivel de seguridad decente. De manera predeterminada las versiones más recientes de nfs-utils no permitirán iniciar el servicio si esta línea no se encuentra presente en /etc/hosts.deny.

Una vez configurado portmap, debe reiniciarse el servicio de portmap:

```
/etc/rc.d/init.d/portmap restart
```

Si tiene un DNS, de de alta las direcciones IP asociadas a un nombre o bien edite /etc/hosts y agregue las direcciones IP asociadas con un nombre. Esto nos servirá como listas de control de accesos. Ejemplo del fichero /etc/hosts:

```
127.0.0.1      localhost.localdomain  localhost
192.168.1.254  servidor.mi-red-local.org  servidor
192.168.1.2   algun_nombre.mi-red-local.org  algun_nombre
192.168.1.3   otro_nombre.mi-red-local.org  otro_nombre
192.168.1.4   otro_nombre_mas.mi-red-local.org  otro_nombre_mas
192.168.1.5   como_se_llame.mi-red-local.org  como_se_llame
192.168.1.6   como_sea.mi-red-local.org  como_sea
192.168.1.7   lo_que_sea.mi-red-local.org  lo_que_sea
```

Procederemos a determinar que directorio se va a compartir. Puede crear también uno nuevo:

```
mkdir /home/nfs/
```

Una vez hecho esto, necesitaremos establecer que directorios en el sistema serán compartidos con el resto de las máquinas de la red, o bien a que máquinas, de acuerdo al DNS o /etc/hosts se permitirá el acceso. Esto deberemos agregarlos en /etc/exports determinado con que máquinas y en que modo lo haremos. Se puede especificar una dirección IP o bien nombre de alguna máquina, o bien un patrón común con comodín para definir que máquinas pueden acceder. De tal modo podemos utilizar el siguiente ejemplo (la separación de espacios se hace con un tabulador):

```
/home/nfs      *.mi-red-local.org(ro)
```

En el ejemplo anterior se esta definiendo que se compartirá /home/nfs/ a todas las máquinas cuyo nombre, de acuerdo al DNS o /etc/hosts, tiene como patrón común **mi-red-local.org**, en modo de lectura escritura. Se utilizó un asterisco (*) como comodín, seguido de un punto y el nombre del dominio. Esto permitirá que *como_se_llame.mi-red-local.org*, *como_sea.mi-red-local.org*, *lo_que_sea.mi-red-local.org*, etc., podrán acceder al volumen /home/nfs/ en modo solo lectura. Si queremos que el acceso a este directorio sea en modo de lectura y escritura, cambiamos (ro) por (rw):

```
/home/nfs      *.mi-red-local.org(rw)
```

Ya que se definieron los volúmenes a compartir, solo resta iniciar o reiniciar el servicio nfs. Utilice cualquiera de las dos líneas dependiendo el caso:

```
/etc/rc.d/init.d/nfs start
/etc/rc.d/init.d/nfs restart
```

A fin de asegurarnos de que el servicio de *nfs* esté habilitado la siguiente vez que se encienda el equipo, debemos ejecutar lo siguiente:

```
/sbin/chkconfig --level 345 nfs on
```

El comando anterior hace que se habilite *nfs* en los niveles de corrida 3, 4 y 5.

Como medida de seguridad adicional, si tiene un contrafirewall o *firewall* implementado, cierre, para todo aquello que no sea parte de su red local, los puertos tcp y udp 2049, ya que estos son utilizados por NFS para escuchar peticiones.

Configurando las máquinas clientes.

Para probar la configuración, es necesario que las máquinas clientes se encuentren definidas en el DNS o en el fichero /etc/hosts del servidor. Si no hay un DNS configurado en la red, deberán definirse los nombres y direcciones IP correspondientes en el fichero /etc/hosts de todas las máquinas que integran la red local. A continuación creamos, como *root*, desde cualquier otra máquina de la red local un punto de montaje:

```
mkdir /mnt/servidornfs
```

Y para proceder a montar el volumen remoto, utilizaremos la siguiente línea de comando :

```
mount -t nfs servidor.mi-red-local.org:/home/nfs /mnt/servidornfs
```

Si por alguna razón en el DNS de la red local, o el fichero /etc/hosts de la máquina cliente, decidió no asociar el nombre de la máquina que funjirá como servidor NFS a su correspondiente dirección IP, puede especificar ésta en lugar del nombre. Ejemplo:

```
mount -t nfs 192.168.1.254:/home/nfs /mnt/servidornfs
```

Podremos acceder entonces a dicho volumen remoto con solo cambiar al directorio local definido como punto de montaje, del mismo modo que se haría con un disquete o una unidad de CDROM:

```
cd /mnt/servidornfs
```

Si queremos poder montar este volumen NFS con una simple línea de comando o bien haciendo doble clic en un icono sobre el escritorio, será necesario agregar la correspondiente línea en /etc/fstab. Ejemplo:

```
servidor.mi-red-local.org:/home/nfs /mnt/servidornfs nfs user,exec,dev,nosuid,rw,noauto 0 0
```

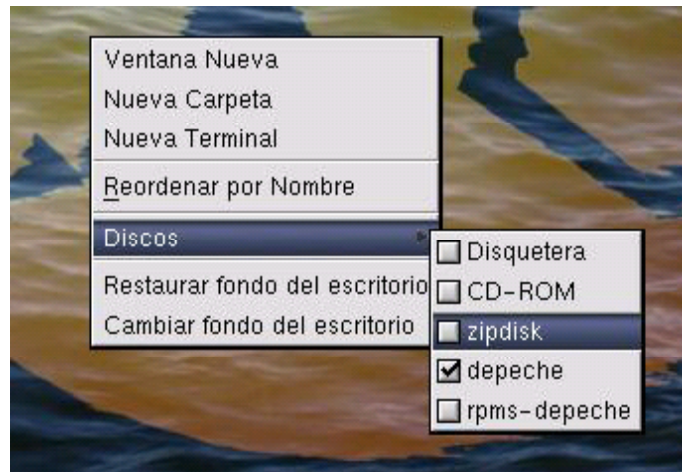
La línea anterior especifica que el directorio /home/nfs/ de la máquina servidor.mi-red-local.org será montado en el directorio local /mnt/servidor/nfs, permitiéndole a los usuarios el poder montarlo, en modo de lectura y escritura y que este volumen no será montado durante el arranque del sistema. Esto último es de importancia, siendo que si el servidor no está encendido al momento de arrancar la máquina cliente, este se colgará durante algunos minutos.

Una vez agregada la línea en /etc/fstab de la máquina cliente, si utiliza GNOME Midnight Commander, el administrador de archivos de GNOME-1.1 y 1.2, solo restará iniciar una sesión gráfica, hacer clic derecho sobre el escritorio y seleccionar *Actualizar dispositivos* o *Rescan devices*. Esto colocará un icono adicional sobre el escritorio que deberá ser tratado del mismo modo que se haría con un disquete o unidad de CDROM.





Si utiliza GNOME-1.4 o superior, éste incorpora Nautilus como administrador de archivos, mismo que atodetecta cualquier cambio en /etc/fstab. Solo hágase clic derecho esobre el escritorio y seleccionese el disco que se desee montar.



Instalación de GNU/Linux por medio de un servidor NFS.

Este es quizás el uso más común para un volumen NFS. Permite compartir un volumen que contenga una copia del CD de instalación de alguna distribución y realizar inclusive instalaciones simultáneas en varios equipos. Tiene como ventaja el que la instalación puede resultar más rápida que si se hiciese con un CDROM, siendo que la tasa de trasferencia de archivos será determinada por el ancho de banda de la red local, y nos permitirá instalar GNU/Linux en máquinas que no tengas unidad de CDROM.

Una vez creado y configurado un volumen a compartir copiaremos todo el contenido del CD de instalación en éste:

```
cp -r /mnt/odrom/* /home/nfs/
```

En el directorio *images* del CD encontraremos varias imágenes para crear disquetes de arranque. Utilizaremos bootnet.img para crear el número de disquetes necesarios para cada máquina en la que realizaremos una instalación, y que nos permitirán acceder a la red. Inserte un disquete y ejecute lo siguiente:

```
cd /home/nfs/images/  
dd if=bootnet.img of=/dev/fd0 bs=1440k
```

Añada en /etc/hosts, o bien de de alta en el DNS, las direcciones IP, que serán utilizadas por las nuevas máquinas, asociadas a un nombre con el dominio que específico como regla de control de acceso en /etc/exports *-es decir *.mi-red-local.org-*. Para /etc/hosts, puede quedar algo así:

```
127.0.0.1      localhost.localdomain  localhost  
192.168.1.254 servidor.mi-red-local.org servidor  
192.168.1.2   algun_nombre.mi-red-local.org algun_nombre  
192.168.1.3   otro_nombre.mi-red-local.org otro_nombre  
192.168.1.4   otro_nombre_mas.mi-red-local.org otro_nombre_mas  
192.168.1.5   como_se_llame.mi-red-local.org como_se_llame  
192.168.1.6   como_sea.mi-red-local.org como_sea  
192.168.1.7   lo_que_sea.mi-red-local.org lo_que_sea  
192.168.1.8   nueva_maquina.mi-red-local.org nueva_maquina  
192.168.1.9   otra_nueva_maquina.mi-red-local.org otra_nueva_maquina
```

Utilice estos disquetes para arrancar en los equipos, ingrese una dirección IP y demás parámetros para esta máquina y cuando se le pregunte ingrese la dirección IP del servidor NFS y el directorio en éste donde se encuentra la copia del CD de instalación. El resto continuará como cualquier otra instalación.

Warning to Spammers / Advertencia a Spammers: You are not permitted to send unsolicited bulk email (commonly referred to as Spam) to ANY e-mail address from jinet.prohosting.com or linuxparatodos.com, or to sell this address to people who do. By extracting any e-mail address from any page from this web site, you agree to pay a fee of US\$10,000.00 per message you send and US\$100,000.00 per instance you sold this address. - Usted no está autorizado a enviar correo masivo no solicitado (comúnmente referido como Spam) a CUALQUIER dirección de correo electrónico de jinet.prohosting.com o linuxparatodos.com, o vender estas direcciones a cualquier persona que si lo haga. Al extraer las direcciones de correo electrónico de cualquier página de este sitio web, usted acepta que pagará una cuota de US\$10,000.00 por mensaje que usted envíe y US\$100,000.00 por cada instancia a la que usted haya vendido cualquiera de nuestras direcciones de correo electrónico.

[Foro de soporte](#)

[Capacitación](#)

[Introducción a Linux](#)

[Manuales Linux](#)

[Productos y Servicios](#)

[Copyright](#)

Todos los logotipos y marcas son propiedad de sus respectivos propietarios de los correspondientes derechos reservados. Los comentarios y opiniones son propiedad y responsabilidad de quienes los publiquen, el resto son © 2001 LinuxParaTodos.com Linux Para Todos® y Darkshram? son ©1999 y ©1987 correspondientemente de Joel Barrios Dueñas.