

JUNIO DE 2021

UGR CURSO 2020-2021

ELENA ORTIZ MORENO

CORREO: elena97om@correo.ugr.es

PRÁCTICA 6: SERVIDOR DE DISCO NFS

SERVIDORES WEB DE
ALTAS PRESTACIONES

ÍNDICE:

- | | |
|--|-----|
| 1.Crear máquina virtual y configurarla como servidor NFS | 3-4 |
| 2.Configurar los clientes M1 y M2 | 4-5 |
| 3.Añadir seguridad en el servidor NFS | 5-7 |

1. Crear máquina virtual y configurarla como servidor NFS

Primero creamos la máquina que será el servidor NFS e instalamos las herramientas necesarias para utilizarla como tal.

```
NFS-elena97om [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
elena97om@nfs-elena97om:~$ sudo apt install nfs-kernel-server nfs-common rpcbind
Reading package lists... Done
Building dependency tree
Reading state information... Done
nfs-common is already the newest version (1:1.3.4-2.1ubuntu5.3).
nfs-kernel-server is already the newest version (1:1.3.4-2.1ubuntu5.3).
rpcbind is already the newest version (0.2.3-0.6ubuntu0.18.04.1).
0 upgraded, 0 newly installed, 0 to remove and 60 not upgraded.
elena97om@nfs-elena97om:~$ _
```

A continuación, creamos la carpeta que va a ser compartida y cambiamos los permisos y el propietario.

```
NFS-elena97om [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
elena97om@nfs-elena97om:~$ sudo mkdir /datos
elena97om@nfs-elena97om:~$ sudo mkdir /datos/compartido
elena97om@nfs-elena97om:~$ sudo chown nobody:nogroup /datos/compartido/
elena97om@nfs-elena97om:~$ sudo chmod -R 777 /datos/compartido/
elena97om@nfs-elena97om:~$ _
```

Añadimos las IP de M1 y M2 para darles permiso de acceso modificando el archivo /etc/exports

```
NFS-elena97om [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
GNU nano 2.9.3 /etc/exports
# /etc/exports: the access control list for filesystems which may be exported
# to NFS clients. See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/homes hostname1(rw,sync,no_subtree_check) hostname2(ro,sync,no_subtree_check)
#
# Example for NFSv4:
# /srv/nfs4 gss/krb5i(rw,sync,fsid=0,crossmnt,no_subtree_check)
# /srv/nfs4/homes gss/krb5i(rw,sync,no_subtree_check)
#
/datos/compartido/ 192.168.56.102(rw) 192.168.56.103(rw)
```

Una vez hecho esto, reiniciamos el servicio y comprobamos que todo funciona.

```
NFS-elena97om [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
elena97om@nfs-elena97om:~$ sudo service nfs-kernel-server restart
elena97om@nfs-elena97om:~$ sudo service nfs-kernel-server status
• nfs-server.service - NFS server and services
   Loaded: loaded (/lib/systemd/system/nfs-server.service; enabled; vendor preset: enabled)
   Active: active (exited) since Tue 2021-06-01 07:36:46 UTC; 5s ago
     Process: 2594 ExecStopPost=/usr/sbin/exportfs -f (code=exited, status=0/SUCCESS)
     Process: 2584 ExecStopPost=/usr/sbin/exportfs -au (code=exited, status=0/SUCCESS)
     Process: 2583 ExecStop=/usr/sbin/rpc.nfsd 0 (code=exited, status=0/SUCCESS)
     Process: 2606 ExecStart=/usr/sbin/rpc.nfsd $RPCNFSDARGS (code=exited, status=0/SUCCESS)
     Process: 2605 ExecStartPre=/usr/sbin/exportfs -r (code=exited, status=0/SUCCESS)
    Main PID: 2606 (code=exited, status=0/SUCCESS)

Jun 01 07:36:46 nfs-elena97om systemd[1]: Starting NFS server and services...
Jun 01 07:36:46 nfs-elena97om exportfs[2605]: exportfs: /etc/exports [1]: Neither 'subtree_check' or
Jun 01 07:36:46 nfs-elena97om exportfs[2605]: Assuming default behaviour ('no_subtree_check').
Jun 01 07:36:46 nfs-elena97om exportfs[2605]: NOTE: this default has changed since nfs-utils versi
Jun 01 07:36:46 nfs-elena97om exportfs[2605]: exportfs: /etc/exports [1]: Neither 'subtree_check' or
Jun 01 07:36:46 nfs-elena97om exportfs[2605]: Assuming default behaviour ('no_subtree_check').
Jun 01 07:36:46 nfs-elena97om exportfs[2605]: NOTE: this default has changed since nfs-utils versi
Jun 01 07:36:46 nfs-elena97om systemd[1]: Started NFS server and services.
lines 1-18/18 (END)
```

2. Configurar los clientes M1 y M2.

Tanto en M1 como en M2 instalamos los paquetes necesarios y creamos el punto de montaje.

```
m1-elena97om [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
elena97om@m1-elena97om:~$ sudo apt install nfs-common rpcbind
Reading package lists... Done
Building dependency tree
Reading state information... Done
nfs-common is already the newest version (1:1.3.4-2.1ubuntu5.3).
rpcbind is already the newest version (0.2.3-0.6ubuntu0.18.04.1).
0 upgraded, 0 newly installed, 0 to remove and 8 not upgraded.
elena97om@m1-elena97om:~$ cd /home/elena97om/
elena97om@m1-elena97om:~$ mkdir datos
elena97om@m1-elena97om:~$ chmod -R 777 datos
elena97om@m1-elena97om:~$ sudo mount 192.168.56.105:/datos/compartido datos
elena97om@m1-elena97om:~$
```

Finalmente, para comprobar si ha funcionado, creamos en la carpeta datos de M2 un archivo y confirmamos que es accesible desde M1.

```
m2-elena97om [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
elena97om@m2-elena97om:~$ touch datos/archivo.txt
elena97om@m2-elena97om:~$ ls -la datos
total 8
drwxrwxrwx 2 nobody nogroup 4096 Jun 1 07:56
drwxr-xr-x 7 elena97om elena97om 4096 Jun 1 07:47 ..
-rw-rw-r-- 1 elena97om elena97om 0 Jun 1 07:56 archivo.txt
elena97om@m2-elena97om:~$
```

```
m1-elena97om [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
elena97om@m1-elena97om:~$ ls -la datos
total 8
drwxrwxrwx 2 nobody nogroup 4096 Jun 1 07:56
drwxr-xr-x 7 elena97om elena97om 4096 Jun 1 07:45 ..
-rw-rw-r-- 1 elena97om elena97om 0 Jun 1 07:56 archivo.txt
elena97om@m1-elena97om:~$
```

Para hacer la configuración permanente, modificamos el archivo `/etc/fstab` para indicar que se monte la carpeta compartida al arrancar el sistema (Esta configuración la hacemos tanto en M1 como en M2).

```
m1-elena97om [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
GNU nano 2.9.3 /etc/fstab

# /etc/fstab: static file system information.
#
# Use 'blkid' to print the universally unique identifier for a
# device; this may be used with UUID= as a more robust way to name devices
# that works even if disks are added and removed. See fstab(5).
#
# <file system> <mount point> <type> <options> <dump> <pass>
# / was on /dev/ubuntu-vg/ubuntu-lv during curtin installation
/dev/disk/by-id/dm-uuid-LVM-20SjBHcJKAf1L6uM5gVXjwJ1iR82fgdDsUAYpocucRzuQ83ueCt5Uean1TH4aJ5w / ext4
# /boot was on /dev/sda2 during curtin installation
/dev/disk/by-uuid/14ee0b60-c6af-43e5-abf8-1e47e10e6ef4 /boot ext4 defaults 0 0
/swap.img none swap sw 0 0

192.168.56.105:/datos/compartido /home/elena97om/datos/ nfs auto,noatime,nolock,bg,nfsvers=3,intr,t$
```

Reiniciamos las dos máquinas y comprobamos que, efectivamente, la carpeta compartida se monta de manera automática.

```
m1-elena97om [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
elena97om@m1-elena97om:~$ ls -la datos/
total 8
drwxrwxrwx 2 nobody nogroup 4096 Jun 1 07:56
drwxr-xr-x 7 elena97om elena97om 4096 Jun 1 07:45 ..
-rw-rw-r-- 1 elena97om elena97om 0 Jun 1 07:56 archivo.txt
elena97om@m1-elena97om:~$

m2-elena97om [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
elena97om@m2-elena97om:~$ ls -la datos/
total 8
drwxrwxrwx 2 nobody nogroup 4096 Jun 1 07:56
drwxr-xr-x 7 elena97om elena97om 4096 Jun 1 07:47 ..
-rw-rw-r-- 1 elena97om elena97om 0 Jun 1 07:56 archivo.txt
elena97om@m2-elena97om:~$
```

3. Añadir seguridad en el servidor NFS

En primer lugar configuramos IPTABLES con denegación implícita del tráfico entrante:

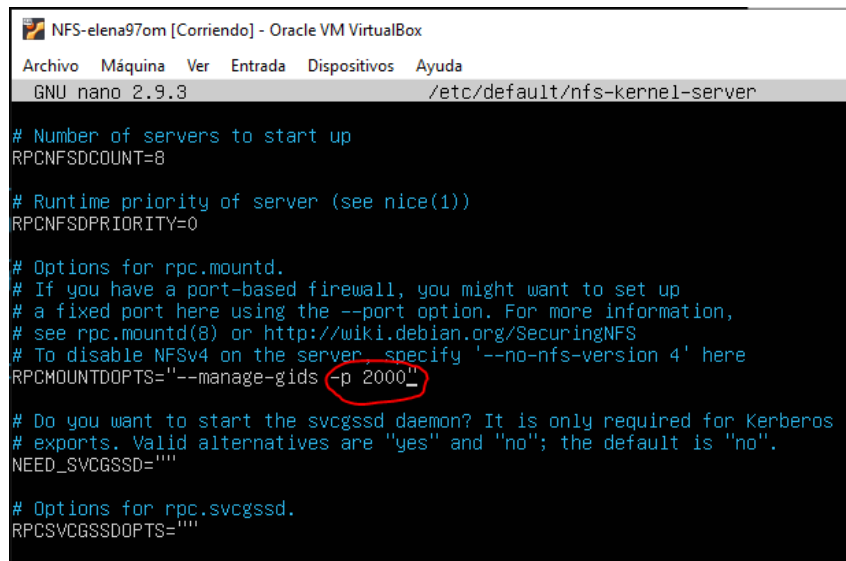
```
NFS-elena97om [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
GNU nano 2.9.3 /home/elena97om/iptables.sh

#!/bin/bash

#Política por defecto: denegar todo el tráfico entrante
iptables -P INPUT DROP
iptables -P OUTPUT ACCEPT
iptables -P FORWARD DROP
iptables -A INPUT -m state --state NEW,ESTABLISHED -j ACCEPT_
```

Debemos abrir diversos puertos de servicios NFS a las máquinas clientes. Sin embargo, los servicios *mountd* y *nlockmgr* utilizan puertos dinámicos. Por lo tanto, para poder añadir reglas con iptables debemos fijar estos puertos antes.

En primer lugar, para el servicio *mountd* modificamos el archivo */etc/default/nfs-kernel-server*:



```
NFS-elena97om [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
GNU nano 2.9.3 /etc/default/nfs-kernel-server

# Number of servers to start up
RPCNFSDCOUNT=8

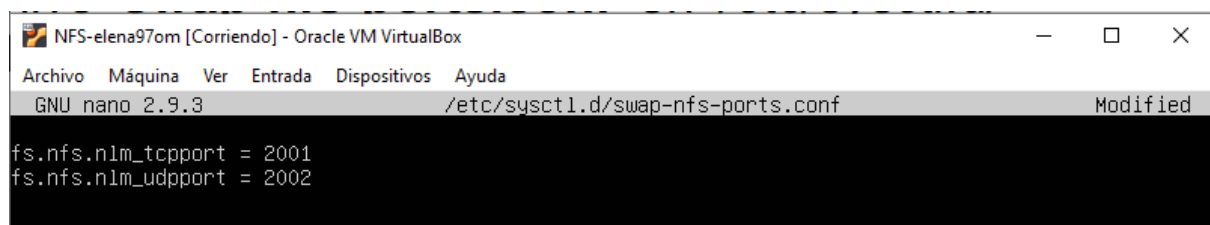
# Runtime priority of server (see nice(1))
RPCNFSDPRIORITY=0

# Options for rpc.mountd.
# If you have a port-based firewall, you might want to set up
# a fixed port here using the --port option. For more information,
# see rpc.mountd(8) or http://wiki.debian.org/SecuringNFS
# To disable NFSv4 on the server, specify '--no-nfs-version 4' here
RPCMOUNTDOPTS="--manage-gids -p 2000"

# Do you want to start the svcgssd daemon? It is only required for Kerberos
# exports. Valid alternatives are "yes" and "no"; the default is "no".
NEED_SVCGSSD=""

# Options for rpc.svcgssd.
RPCSVCGSSDOPTS=""
```

Ahora, para el servicio *nlockmgr* podemos hacerlo a través de systemd sin reiniciar el sistema. Creamos el archivo *swap-nfs-ports.conf* en */etc/sysctl.d/* añadiendo las opciones correspondientes para escuchar los puertos TCP y UDP.



```
NFS-elena97om [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
GNU nano 2.9.3 /etc/sysctl.d/swap-nfs-ports.conf Modified

fs.nfs.nlm_tcpport = 2001
fs.nfs.nlm_udpport = 2002
```

A continuación, lanzamos el nuevo archivo de configuración que hemos creado y reiniciamos el sistema.

```
NFS-elena97om [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda

elena97om@nfs-elena97om:/$ sudo sysctl --system
* Applying /etc/sysctl.d/10-console-messages.conf ...
kernel.printk = 4 4 1 7
* Applying /etc/sysctl.d/10-ipv6-privacy.conf ...
net.ipv6.conf.all.use_tempaddr = 2
net.ipv6.conf.default.use_tempaddr = 2
* Applying /etc/sysctl.d/10-kernel-hardening.conf ...
kernel.kptr_restrict = 1
* Applying /etc/sysctl.d/10-link-restrictions.conf ...
fs.protected_hardlinks = 1
fs.protected_symlinks = 1
* Applying /etc/sysctl.d/10-lxd-inotify.conf ...
fs.inotify.max_user_instances = 1024
* Applying /etc/sysctl.d/10-magic-sysrq.conf ...
kernel.sysrq = 176
* Applying /etc/sysctl.d/10-network-security.conf ...
net.ipv4.conf.default.rp_filter = 1
net.ipv4.conf.all.rp_filter = 1
net.ipv4.tcp_syncookies = 1
* Applying /etc/sysctl.d/10-pttrace.conf ...
kernel.yama.pttrace_scope = 1
* Applying /etc/sysctl.d/10-zero-page.conf ...
vm.mmap_min_addr = 65536
* Applying /usr/lib/sysctl.d/50-default.conf ...
net.ipv4.conf.all.promote_secondaries = 1
net.core.default_qdisc = fq_codel
* Applying /etc/sysctl.d/99-sysctl.conf ...
* Applying /etc/sysctl.d/swap-nfs-ports.conf ...
fs.nfs.nlm_tcpport = 2001
fs.nfs.nlm_udpport = 2002
* Applying /etc/sysctl.conf ...
elena97om@nfs-elena97om:/$ sudo service nfs-kernel-server restart
elena97om@nfs-elena97om:/$
```

Comprobamos los puertos asociados a cada servicio:

```
NFS-elena97om [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda

elena97om@nfs-elena97om:/$ sudo rpcinfo -p localhost
program vers proto  port  service
100000    4    tcp    111    portmapper
100000    3    tcp    111    portmapper
100000    2    tcp    111    portmapper
100000    4    udp    111    portmapper
100000    3    udp    111    portmapper
100000    2    udp    111    portmapper
100005    1    udp    2000   mountd
100005    1    tcp    2000   mountd
100005    2    udp    2000   mountd
100005    2    tcp    2000   mountd
100005    3    udp    2000   mountd
100005    3    tcp    2000   mountd
100003    3    tcp    2049   nfs
100003    4    tcp    2049   nfs
100227    3    tcp    2049
100003    3    udp    2049   nfs
100227    3    udp    2049
100021    1    udp    2002   nlockmgr
100021    3    udp    2002   nlockmgr
100021    4    udp    2002   nlockmgr
100021    1    tcp    2001   nlockmgr
100021    3    tcp    2001   nlockmgr
100021    4    tcp    2001   nlockmgr
elena97om@nfs-elena97om:/$ _
```