

MEMORIA HITO 3

ADMINISTRACIÓN DE SISTEMAS OPERATIVOS Y REDES DE COMPUTADORES

Josué Perea Martínez 49252061E

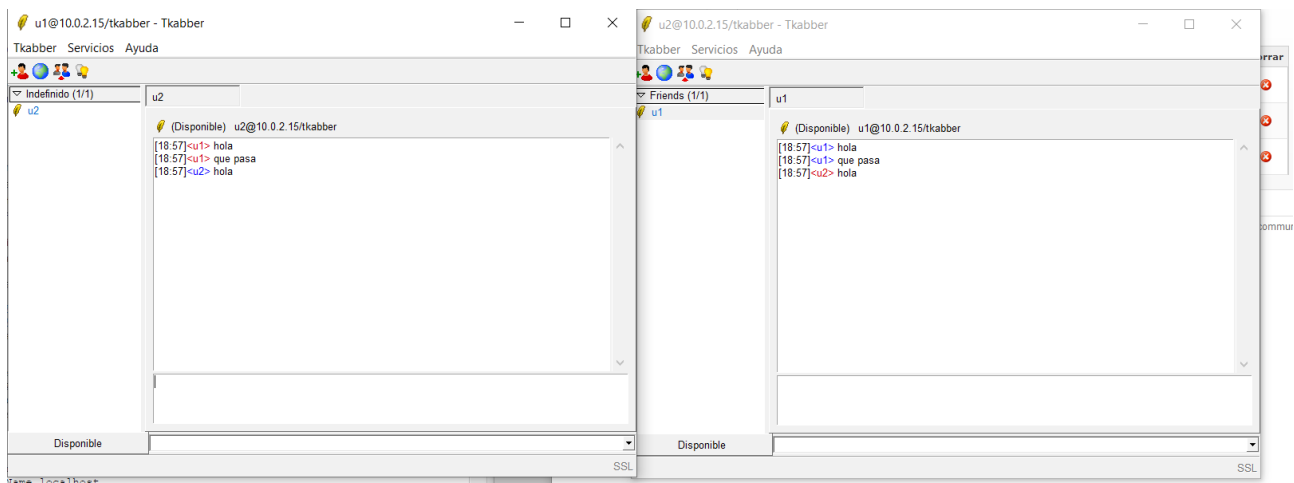
OBJETIVOS:

El objetivo de este hito es seguir instalando servicios en los 3 sistemas operativos: Windows Server, CentOS y FreeBSD. Son servicios más avanzados y de diferentes características como Raid5, el cual es muy interesante y útil si buscamos un disco más rápido y económico.

WINDOWS:

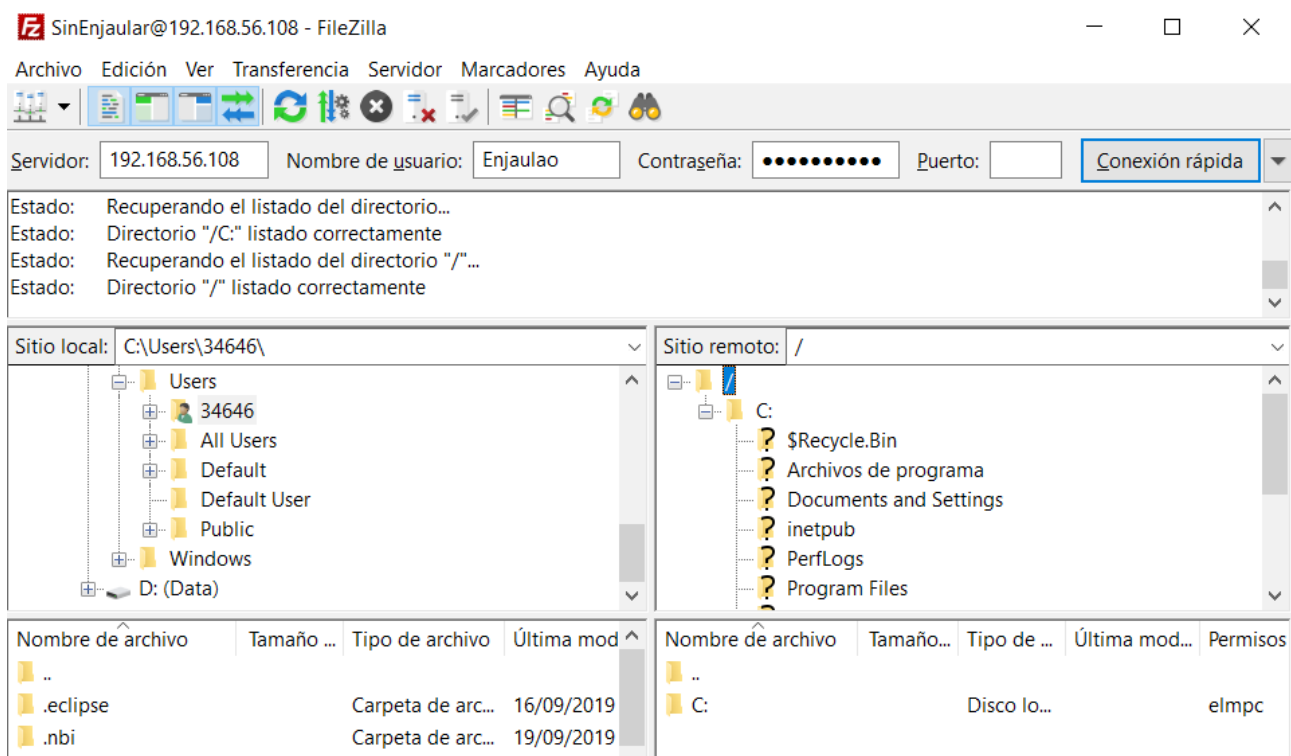
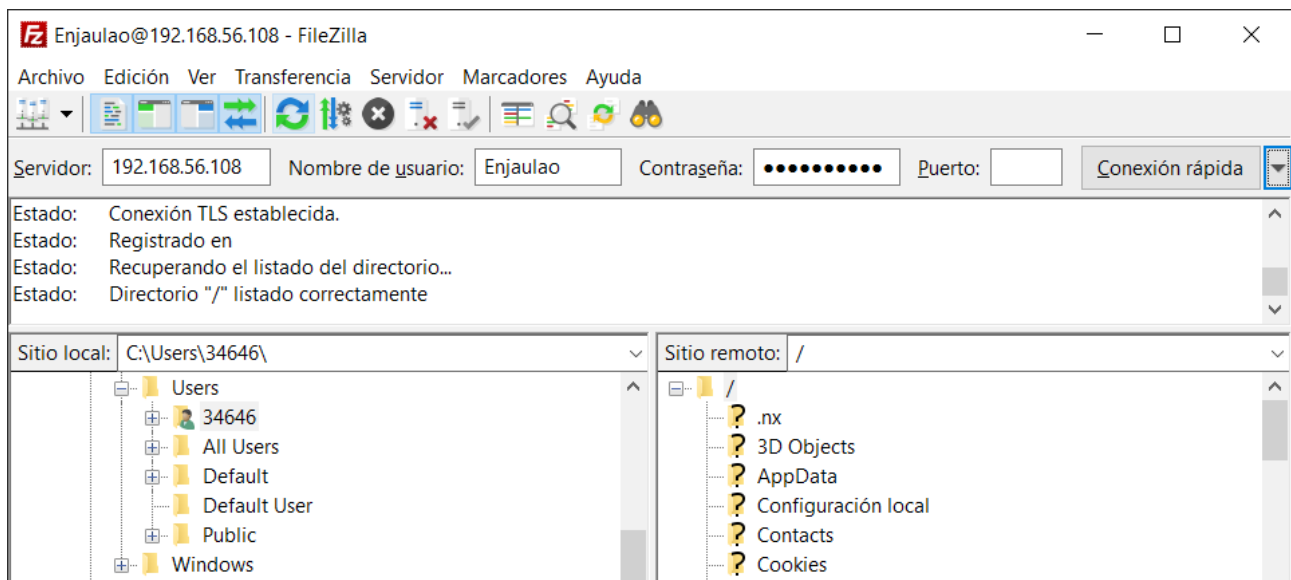
Mensajería instantánea (Jabber):

Instalamos openfire en el servidor windows. Una vez instalado abrimos el navegador y configuramos el servidor. Añadimos los usuarios e instalamos en nuestro windows host (cliente) tkabber cliente. Arrancamos dos cliente tkabber y los agregamos como contactos. Ya podemos chatear.



FTP:

Para instalar este servicio instalamos en el windows server serv-u, en el cual creamos dos usuarios: un enjaulado y uno sin enjaular. Para hacer login vamos al un cliente filezilla desde windows host (cliente) y ponemos la dirección IP, usuario y password. El usuario enjaulado está enjaulado en el usuario Administrador.

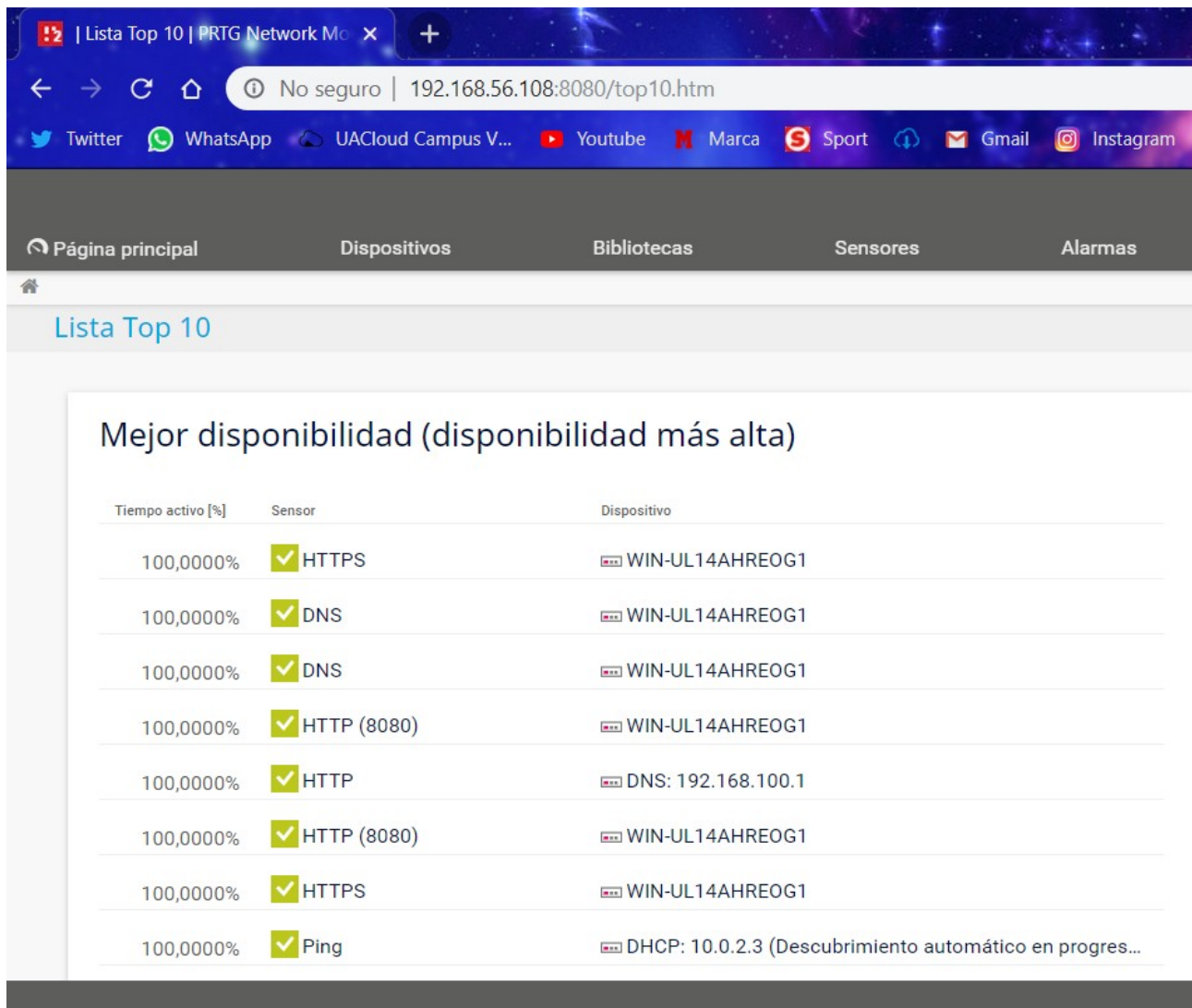


RAID5:

Para hacer instalar un Raid5 en Windows vamos al creador de particiones. Primero debemos agregar a la controladora SATA 4 discos dvi. En mi caso de 1.03 GB. Los montamos con botón derecho → Nuevo volumen Raid5 y agregamos los 4 discos. Provocamos el fallo con botón derecho → sin conexión y probamos que sigue funcionando el Raid5.

NAGIOS:

Para instalar nagios en windows necesitamos otro monitorizador de servicios. He instalado PRTG Network Monitor. Para lanzar el servicio → **PRTG Administration Tool** → iniciar servicio. Para conectarnos ponemos en el navegador la IP del servidor: 192.168.56.108:8080.



Tiempo activo [%]	Sensor	Dispositivo
100,0000%	✓ HTTPS	WIN-UL14AHREOG1
100,0000%	✓ DNS	WIN-UL14AHREOG1
100,0000%	✓ DNS	WIN-UL14AHREOG1
100,0000%	✓ HTTP (8080)	WIN-UL14AHREOG1
100,0000%	✓ HTTP	DNS: 192.168.100.1
100,0000%	✓ HTTP (8080)	WIN-UL14AHREOG1
100,0000%	✓ HTTPS	WIN-UL14AHREOG1
100,0000%	✓ Ping	DHCP: 10.0.2.3 (Descubrimiento automático en progres...

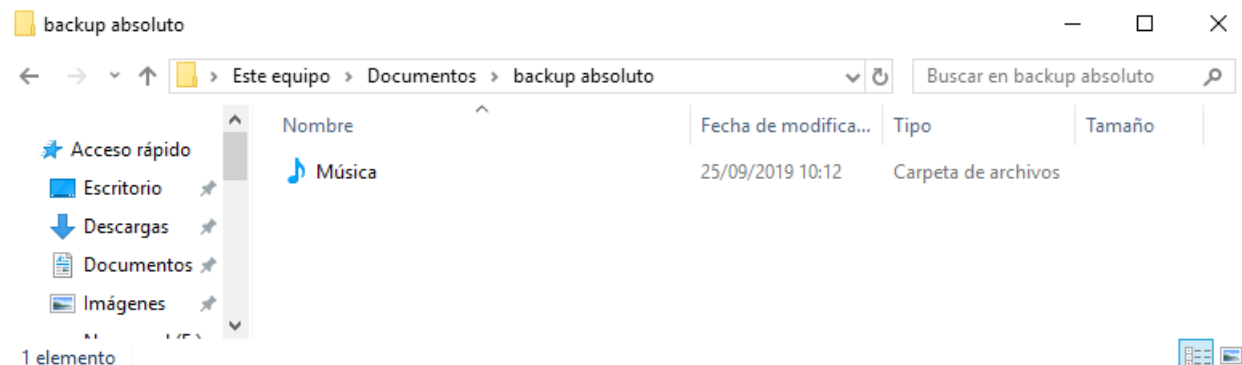
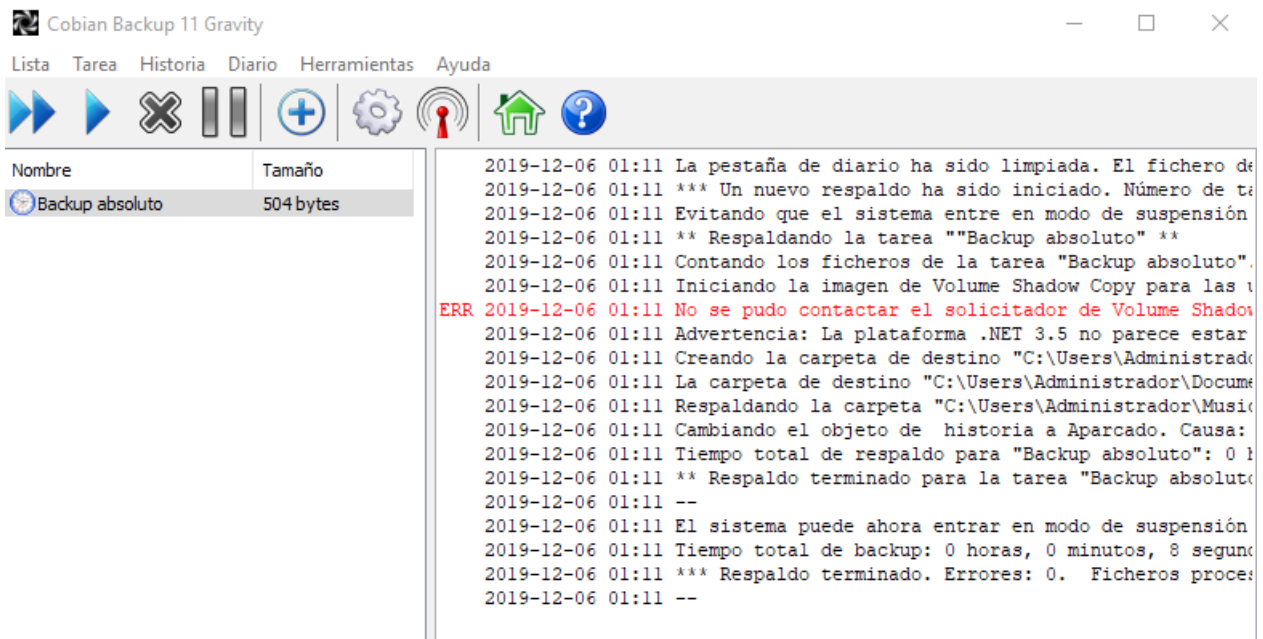
BACKUP:

Tenemos que descargar Cobian Backup 11. Una vez instalado:

→ Tarea → Nueva Tarea → nombre de la tarea → Ficheros → Fuente (lo que vamos a copiar) → Destino (donde lo copiamos)

-Absoluto: Para el absoluto seleccionamos absoluto.

-Incremental: Seleccionamos incremental.



Router:

windows+R: regedit → IPEnableRouter cambiarlo a 1

windows+R: services.msc → Enrutamiento → iniciar

Usamos como cliente centos:

route del default → borramos la por defecto

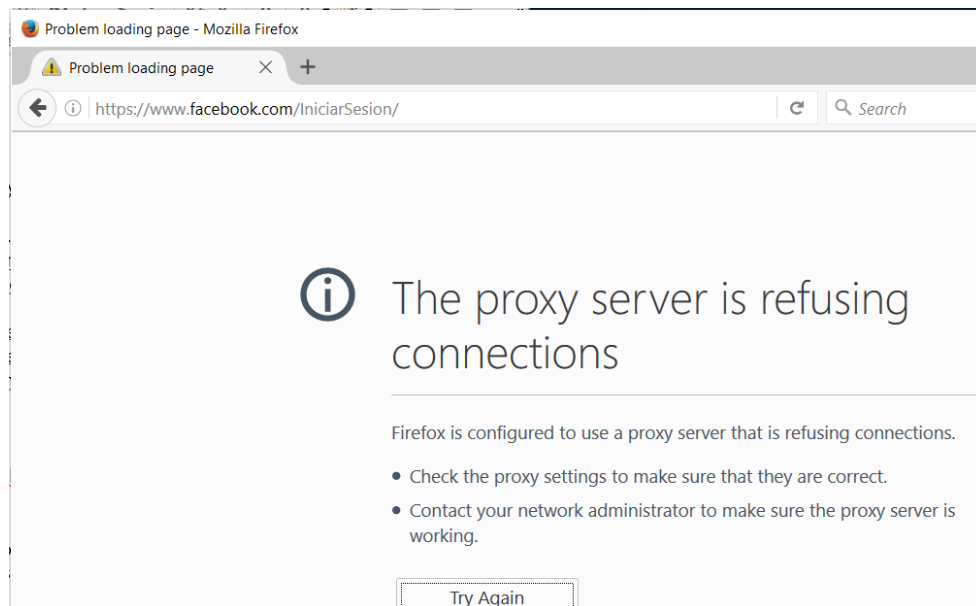
route add default gw 10.0.2.15 → añadimos la de windows

Para visualizarlo hacemos un ping a google y **route -n** para ver que puerta de enlace usa.

```
josuepm98@localhost:/home/josuepm98
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
64 bytes from mad07s09-in-f4.1e100.net (172.217.17.4): icmp_seq=3 ttl
=53 time=12.4 ms
^C
--- www.google.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 5ms
rtt min/avg/max/mdev = 11.189/12.900/15.146/1.664 ms
[root@localhost josuepm98]# route -n
Kernel IP routing table
Destination      Gateway           Genmask          Flags Metric Ref    U
se Iface
0.0.0.0          10.0.2.15        0.0.0.0          UG    0      0
0 enp0s3
10.0.2.0         0.0.0.0          255.255.255.0    U      100    0
0 enp0s3
10.8.0.0         0.0.0.0          255.255.255.0    U      0      0
0 tun0
192.168.56.0     0.0.0.0          255.255.255.0    U      101    0
0 enp0s8
192.168.122.0    0.0.0.0          255.255.255.0    U      0      0
0 virbr0
[root@localhost josuepm98]#
```

Proxy:

Para instalar el servidor proxy necesitamos squid. Configuramos el squid.conf y para lanzar el servicio: **squid -z** → barrar de tareas → botón derecho → iniciar. Si es necesario w+R → services msc → iniciar squid. He bloqueado palabras como amazon o youtube y sitios web como facebook. Para conectarnos utilizamos nuestro windows (host) como cliente y el navegador mozilla firefox. Configuramos el proxy:



Se encontró el siguiente error al intentar recuperar la dirección URL: <http://www.amazon.es/?>

Acceso Denegado

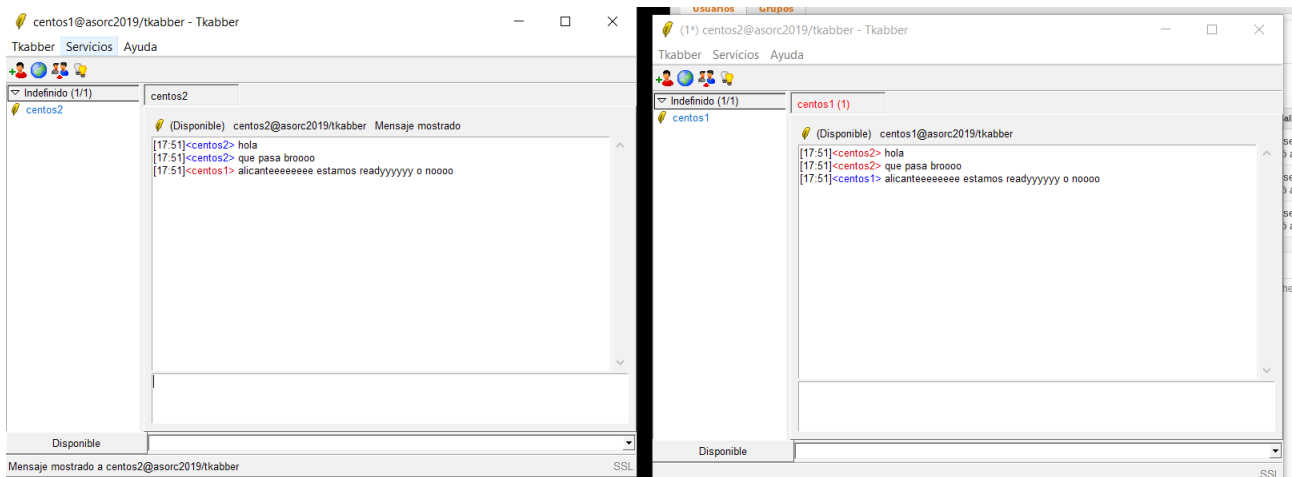
La configuración de control de acceso evita que su solicitud sea permitida en este momento. Por favor contacte a su administrador del caché es [webmaster](#).

CENTOS:

Jabber:

Instalamos openfire con yum install openfire y hacemos al igual que en windows, configurar y añadir usuarios al servidor. Una vez configurado y creados los usuarios para lanzar el servicio:

systemctl restart openfire.service y abrimos 2 clientes tkabber y poniendo la IP y los usuarios logeamos:



FTP:

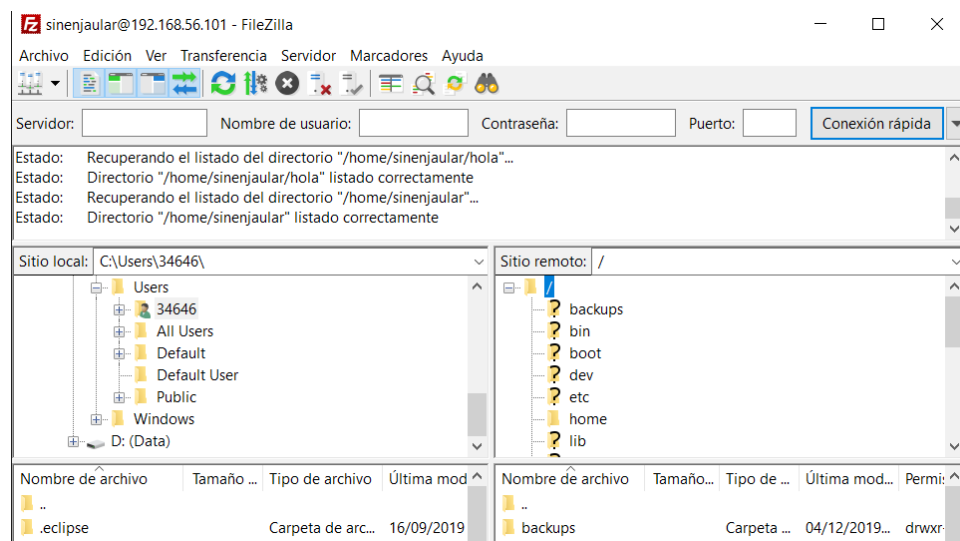
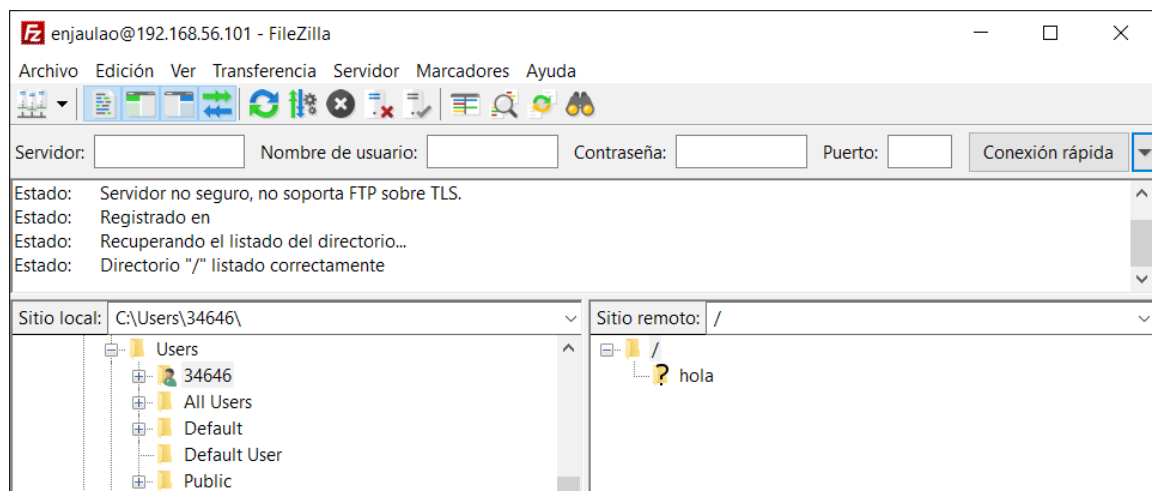
Para instalar FTP en CentOs usamos el comando: `yum -y install vsftpd`. Editamos el fichero de configuración con `nano /etc/vsftpd/vsftpd.conf` y deben quedar las siguientes líneas:

```
anonymous_enable = NO
local_enable=YES
write_enable=YES
local_umask=022
dirmesssage_enable=YES
xferlog_enable=YES
connect_from_port_20=YES
```



```
xferlog_std_format=YES
allow_writeable_chroot=YES
chroot_list_enable=YES
chroot_list_file=/etc/vsftpd/chroot_list
pam_service_name=vsftpd
userlist_enable=YES
```

Yo me he creado 2 usuarios para acceder desde filezilla, uno enjaulado y otro sin enjaular. Para enjaular debemos agregar el usuario a chroot_list. El usuario enjaulado solo tiene acceso a su perfil. No puede salir de /home/enjaulado, sin embargo sinenjaular tiene acceso a todo. Para lanzarlo: **systemctl restart vsftpd.service** y nos conectamos desde FileZilla: **sinenjaular josuepm98 o enjaulado**



RAID5:

Para montar un Raid5 en Centos debemos agregar a la controladora SATA 4 discos dvi, en mi caso de 1GB. Una vez agregados arrancamos Centos y hacemos 4 particiones `fdisk /dev/sdb1` y así con las 4 letras. Una vez montadas hacemos `mdadm --create /dev/md0 -l 5 -n 4` y detrás las 4 particiones. Formateamos con `mkfs.ext4 /dev/md0`. Creamos un directorio 'raid5' en el que creamos un fichero. Lo montamos en `/dev/md0` → `mount /dev/md0 /raid5`. Provocamos un fallo en uno de los discos con `mdadm /dev/md0 --fail /dev/sdc1`. Una vez provocado podemos observar con `mdadm --detail /dev/md0` como el Raid5 sigue trabajando y funcionando. Para eliminar el disco `mdadm -r /dev/md0 /dev/sdc1` y para añadirlo `mdadm --add /dev/md0 /dev/sdc1`. Para ver el mount simplemente comando `mount`.

```
josuepm98@localhost:/home/josuepm98
Archivo Editar Ver Buscar Terminal Ayuda
State : clean, degraded
Active Devices : 3
Working Devices : 3
Failed Devices : 1
Spare Devices : 0

Layout : left-symmetric
Chunk Size : 512K

Consistency Policy : resync

Name : localhost.localdomain:0 (local to host localhost.localdomain)
UUID : d569b74a:90ac3bfb:0aec7b86:12a5f454
Events : 42

Number Major Minor RaidDevice State
0 8 17 0 active sync /dev/sdb1
- 0 0 1 removed
2 8 49 2 active sync /dev/sdd1
4 8 65 3 active sync /dev/sde1
5 8 33 - faulty /dev/sdc1
[root@localhost josuepm98]#
```

```
josuepm98@localhost
Archivo Editar Ver Buscar Terminal Ayuda
[root@localhost raid5]# touch hola
[root@localhost raid5]# ls
hola
[root@localhost raid5]#
```

NAGIOS:

Para instalar nagios: `yum install nagios nagios-plugins-* nrpe` utilizando `--skip-broken` si es necesario. Instalamos también `epel-release` `httpd` `php` `gcc` `glibc-common` `gd` `gd-devel`.

Añadimos contraseña al servicio: `htpasswd /etc/nagios/passwd nagiosadmin`. Para conectarnos:

- `systemctl restart httpd`
- `systemctl restart nagios.service`

Vamos a un navegador cliente y ponemos en la barra de dirección la IP del servidor seguida de `/nagios/` :

- Usuario: **nagiosadmin**

The screenshot shows the Nagios web interface in a browser window. The address bar shows `192.168.56.101/nagios/`. The interface includes a sidebar with navigation links and a main content area with status summaries and a detailed table of service status.

Current Network Status
Last Updated: Thu Dec 5 10:05:50 CET 2019
Updated every 90 seconds
Nagios® Core™ 4.4.5 - www.nagios.org
Logged in as nagiosadmin

Host Status Totals

Up	Down	Unreachable	Pending
1	0	0	0

Service Status Totals

Ok	Warning	Unknown	Critical
7	1	0	0

Service Status Details For All Hosts

Limit Results: 100

Host	Service	Status	Last Check	Duration	Attempt	Status Information
localhost	Current Load	OK	12-05-2019 10:04:14	0d 18h 14m 4s	1/4	OK - load average: 0.10, 0.15, 0.17
	Current Users	OK	12-05-2019 10:04:51	0d 18h 13m 26s	1/4	USERS OK 1 users currently logged in
	HTTP	WARNING	12-05-2019 10:05:28	0d 0h 0m 22s	4/4	HTTP WARNING: HTTP/1.1 403 Forbidden - 508 bytes in 0.001 seconds response time

BACKUP:

Haremos 2 tipos de Backup: absoluto e incremental. Para el absoluto creamos un directorio backups y vamos a realizar el backup de directorios y ficheros que tengamos en 'Documentos'. El comando que debemos usar es:

-Absoluto:

rsync -av Documentos/ backups → backup de la carpeta Documentos entera.

```
josuepm98@localhost:/home/josuepm98/backups/Documentos
Archivo Editar Ver Buscar Terminal Ayuda
[root@localhost backups]# cd ..
[root@localhost josuepm98]# cd Documentos
[root@localhost Documentos]# ls
hola
[root@localhost Documentos]# cd ..
[root@localhost josuepm98]# rsync -av Documentos /home/josuepm98/backups
sending incremental file list
Documentos/
Documentos/hola

sent 172 bytes  received 39 bytes  422.00 bytes/sec
total size is 17  speedup is 0.08
[root@localhost josuepm98]# ls
backups  Documentos  gparted-1.0.0-4.el8.x86_64.rpm  Música  Público
Descargas  Escritorio  Imágenes  Plantillas  Videos
[root@localhost josuepm98]# cd backuos
bash: cd: backuos: No existe el fichero o el directorio
[root@localhost josuepm98]# cd backups
[root@localhost backups]# ls
Documentos
[root@localhost backups]# cd Documentos
[root@localhost Documentos]# ls
hola
[root@localhost Documentos]#
```

-Incremental

rsync -avvb --backup-dir=\$PWD/backup_\$(date +%d%m%y%H%M) Documentos/ backups → backup de las modificaciones que se hayan hecho en la carpeta Documentos → se crea una copia en la nueva carpeta backup+date de lo que había en backups pero antes de modificarla (para generarla hay que volver a modificar Documentos).

```
josuepm98@localhost:/home/josuepm98/backups
Archivo Editar Ver Buscar Terminal Ayuda
[root@localhost josuepm98]# ls
backup_0512191029  Descargas  gparted-1.0.0-4.el8.x86_64.rpm  Plantillas
backup_0512191034  Documentos  Imágenes  Público
backups           Escritorio  Música    Videos
[root@localhost josuepm98]# cd backup_0512191034
[root@localhost backup_0512191034]# ls
hola
[root@localhost backup_0512191034]# nano hola
[root@localhost backup_0512191034]# cd ..
[root@localhost josuepm98]# ls
backup_0512191029  Descargas  gparted-1.0.0-4.el8.x86_64.rpm  Plantillas
backup_0512191034  Documentos  Imágenes  Público
backups           Escritorio  Música    Videos
[root@localhost josuepm98]# cd backups
[root@localhost backups]# ls
backups  Documentos  hola  incremental
[root@localhost backups]#
```

Proxy:

Para instalar servidor proxy: `yum -y install squid` y configurar `/etc/squid/squid.conf`:

```
acl localnet src 192.168.56.0/24
acl blocked_sites dstdomain "/etc/squid/blocked_sites"
acl blocked_words url_regex "/etc/squid/blocked_words"
```

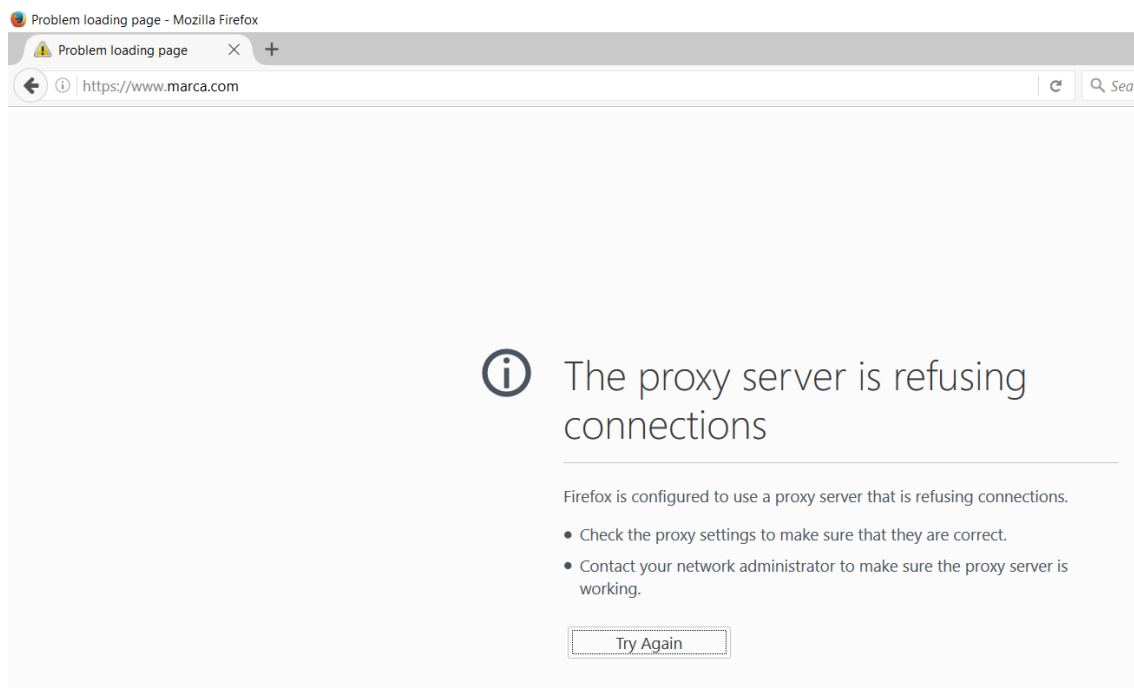
```
http_access deny blocked_sites
http_access deny blocked_words
http_access allow localnet
http_access deny all
```

Descomentar:

```
cache_dir ufs /var/spool/squid 100 16 256
```

`systemctl restart squid.service`

Para comprobarlo entramos en firefox cliente. Elegimos nuestra IP como servidor Proxy con puerto 3128. Y seleccionamos que use ese servidor para todas las conexiones. Si es necesario borramos la caché.



VPN:

Para instalar VPN yum -y install git, una vez lo tenemos hacemos un clone de git clone <https://github.com/Nyr/openvpn-install.git>
Ejecutamos:

```
chmod +x openvpn-install.sh  
./openvpn-install.sh
```

Y configuramos según nos vaya pidiendo el instalador. Creamos el usuario: josuepm98 y se lo pasamos a windows server.

Para comprobarlo el estado del servicio: systemctl status **openvpn-server@server.service** usamos como cliente windows server: botón derecho abrir con OpenVPN → comando ipconfig → 10.8.0.2 es la IP de la red VPN. En centos tenemos la IP 10.8.0.1. Funcionan los pings.

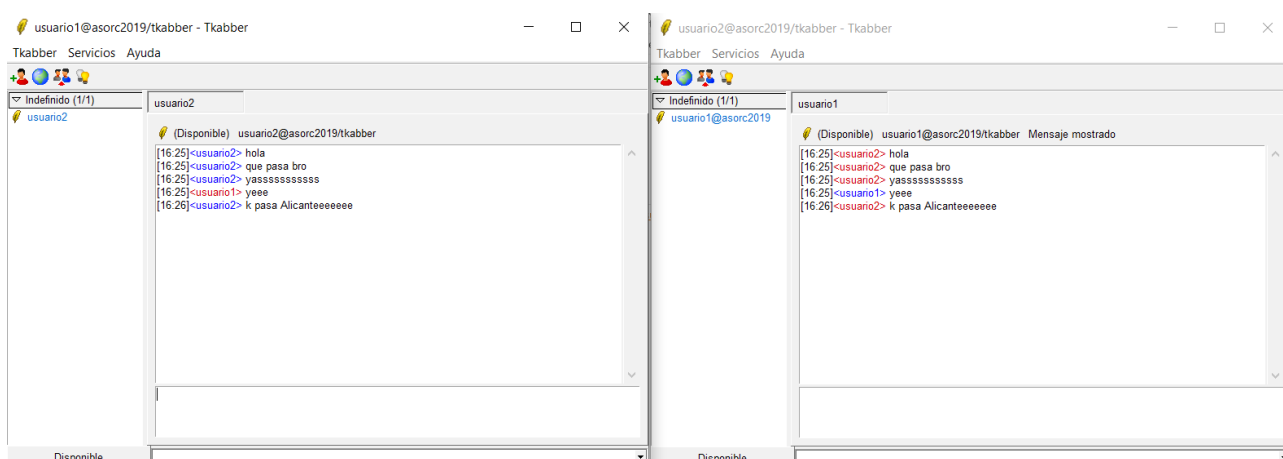
```
tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST> mtu 1500  
    inet 10.8.0.1 netmask 255.255.255.0 destination 10.8.0.1  
    inet6 fe80::6794:58fc:572d:c744 prefixlen 64 scopeid 0x20<link>  
    unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 txqueuelen 100  
(UNSPEC)
```

```
C:\Users\Administrador>ping 10.8.0.1  
  
Haciendo ping a 10.8.0.1 con 32 bytes de datos:  
Respuesta desde 10.8.0.1: bytes=32 tiempo=1ms TTL=64  
Respuesta desde 10.8.0.1: bytes=32 tiempo=1ms TTL=64  
Respuesta desde 10.8.0.1: bytes=32 tiempo=1ms TTL=64  
  
Estadísticas de ping para 10.8.0.1:  
    Paquetes: enviados = 3, recibidos = 3, perdidos = 0  
    (0% perdidos),  
    Tiempos aproximados de ida y vuelta en milisegundos:  
        Mínimo = 1ms, Máximo = 1ms, Media = 1ms
```

FreeBSD:

JABBER:

Para instalar este servicio hacemos `pkg install openfire` y configuramos en `/etc/rc.conf` añadiendo: `sysrc openfire_enable=YES`. Hacemos **service openfire start** y abrimos navegador con la ip y el puerto :9090. Una vez dentro creamos el admin y configuramos el servidor, añadimos 2 users y ya nos logueamos desde el cliente windows host (en mi caso) con tkabber.



BACKUP:

Haremos 2 tipos de Backup: absoluto e incremental. Para el absoluto creamos un directorio backups y vamos a realizar el backup de directorios y ficheros que tengamos en 'Documentos'. El comando que debemos usar es:

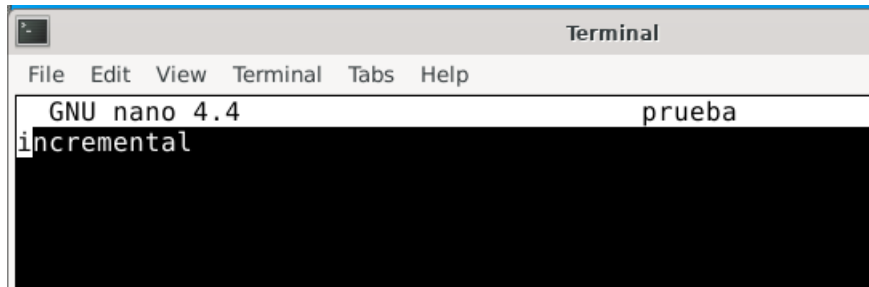
-Absoluto:

`rsync -av Documentos/ backups` → copia todo lo de la carpeta documentos en la carpeta backups.

```
root@josuepm98:/home/josuepm98/backups # ls
hola prueba
root@josuepm98:/home/josuepm98/backups #
```

-Incremental:

`rsync -avvb --backup-dir=$PWD/backup_`date +%d%m%h%M` Documentos/ backups` → copia los cambios que se hayan hecho en Documentos en la carpeta backups además de crear una copia de seguridad (backup+date) del archivo modificado que había en backups (antes de modificarlo).



Proxy:

Para instalar servidor proxy: `pkg install squid` y configurar `/usr/local/etc/squid/squid.conf`:

```
acl localnet src 192.168.56.0/24
acl blocked_sites dstdomain
"/usr/local/etc/squid/blocked_sites"
acl blocked_words url_regex
"/usr/local/etc/squid/blocked_words"
```

```
http_access deny blocked_sites
http_access deny blocked_words
http_access allow localnet
http_access deny all
```

Descomentar:

```
cache_dir ufs /var/spool/squid 100 16 256
```

Para comprobarlo: `service squid status` y entramos en firefox cliente. Elegimos nuestra IP como servidor Proxy con puerto 3128. Y seleccionamos que use ese servidor para todas las conexiones. Si es necesario borramos la caché.

ERROR: El URL solicitado no se ha podido conseguir - Mozilla Firefox

ERROR: El URL solicitado no s... X +



www.amazon.es/?tag=bingamazoabk-21&hvadid=80539257250944&hvqmt=e&hvbmt=be&hvdev=c&r



ERROR

El URL solicitado no se ha podido conseguir

Se encontró el siguiente error al intentar recuperar la dirección URL: <http://www.amazon.es/?>

Acceso Denegado

La configuración de control de acceso evita que su solicitud sea permitida en este momento. Por favor, póngase en c

Su administrador del caché es [webmaster](#).

Generado Fri, 06 Dec 2019 16:44:26 GMT por josuepm98.bsd (squid/4.9)



Problem loading page



https://www.marca.com



The proxy server is refusing connections

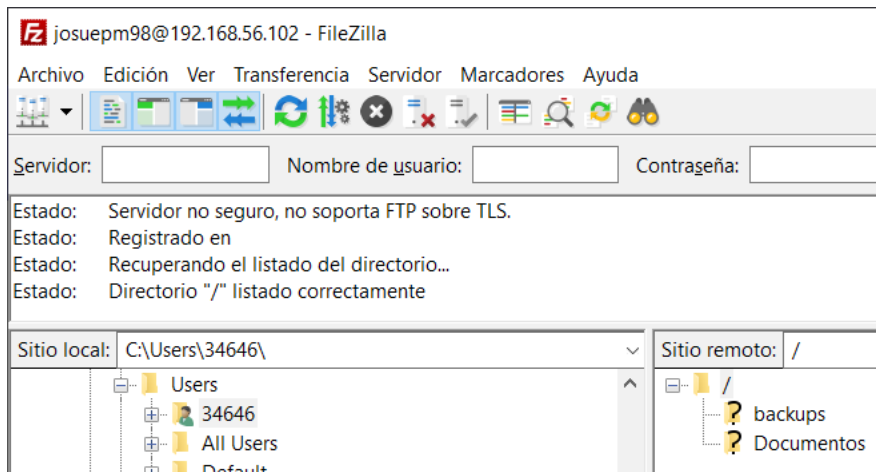
Firefox is configured to use a proxy server that is refusing connections.

- Check the proxy settings to make sure that they are correct.
- Contact your network administrator to make sure the proxy server is working.

Try Again

FTP:

Descargamos con pkg install proftpd y configuramos /etc/rc.conf: proftpd_enable="YES" y asociamos la IP 192.168.56.102 al hostname en /etc/hosts. Configuramos el archivo /usr/local/etc/proftpd.conf y descomentamos la linea DefaultRoot enjaulando así al usuario que queramos enjaular. Permitimos el login de ese usuario y otro no enjaulado. Para lanzarlo: **service proftpd restart** y nos conectamos mediante el cliente FTP filezilla.



Raid:

camcontrol devlist → ver discos

zpool create raid5 raidz ada1 ada2 ada3 ada4

zpool list → ver raid5

zpool status dentro de /raid5 → ver estado del raid y discos

zpool offline raid5 ada3

zpool online raid5 ada3

```
root@josuepm98:/raid5 # zpool status
pool: raid5
state: ONLINE
scan: none requested
config:

    NAME        STATE      READ  WRITE CKSUM
    raid5        ONLINE    0     0     0
      raidz1-0    ONLINE    0     0     0
        ada1      ONLINE    0     0     0
        ada2      ONLINE    0     0     0
        ada3      ONLINE    0     0     0

errors: No known data errors
root@josuepm98:/raid5 #
```

FIREWALL:

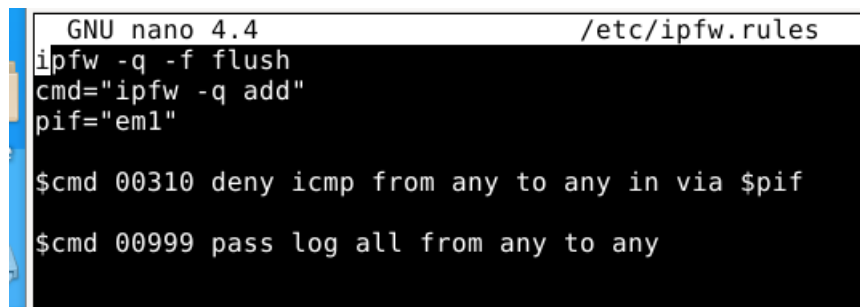
Para levantar un firewall en freeBSD activamos en el /etc/rc.conf:

```
firewall_enable="YES"
firewall_type="open"
firewall_script="/etc/ipfw.rules"
```

Añadimos normas a nuestro firewall en el /etc/ipfw.rules:

```
ipfw -q -f flush
cmd="ipfw -q add"
pif="em1"
$cmd 00310 deny icmp from any to any in via $pif
$cmd 00999 pass log all from any to any
```

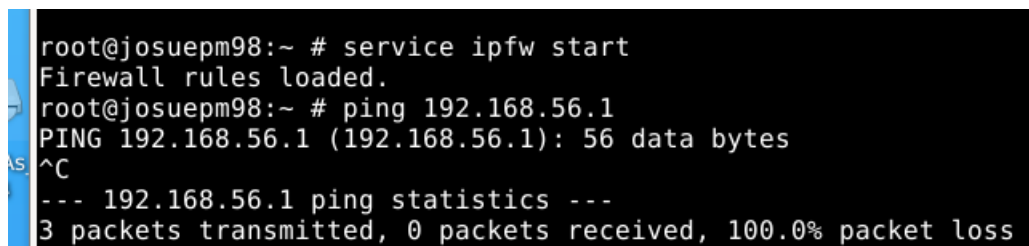
Al iniciar el firewall se nos tumbarán todos los servicios. El ping también porque hemos bloqueado todos los paquetes icmp en las normas del firewall.



```
GNU nano 4.4 /etc/ipfw.rules
ipfw -q -f flush
cmd="ipfw -q add"
pif="em1"

$cmd 00310 deny icmp from any to any in via $pif
$cmd 00999 pass log all from any to any
```

Para probarlo hacemos nslookup 192.168.56.102:



```
root@josuepm98:~ # service ipfw start
Firewall rules loaded.
root@josuepm98:~ # ping 192.168.56.1
PING 192.168.56.1 (192.168.56.1): 56 data bytes
^C
--- 192.168.56.1 ping statistics ---
3 packets transmitted, 0 packets received, 100.0% packet loss
```

Para reiniciar la network hacemos

```
service ipfw stop
/etc/rc.d/netif restart
/etc/rc.d/routing restart
```

NAGIOS

Para instalar nagios uso apache24 como servidor web. Hacemos `pkg install nagios` y configuramos el `/etc/rc.conf` para que lo lance siempre que arranquemos freebsd. Hacemos `cp` de todos los archivos -sampe de la carpeta nagios y nagios/objects. Ahora asignamos contraseña a nagios admin con `htpasswd -c /usr/local/etc/nagios/htpasswd.users nagiosadmin`. Configuramos el `httpd.conf` de apache24 y añadimos el sitio web de nagios.

Para lanzarlo: `service apache24 restart` `service nagios restart`
→ Entramos en el navegador → `192.168.56.102/nagios/`
→ nagiosadmin → password

The screenshot shows the Nagios Core web interface in a browser. The browser's address bar displays `192.168.56.102/nagios/`. The interface includes a sidebar with navigation links such as 'General', 'Current Status', and 'Problems'. The main content area is divided into several sections:

- Current Network Status:** Last Updated: Tue Dec 10 21:28:50 CET 2019. Updated every 90 seconds. Nagios® Core™ 3.5.1 - www.nagios.org. Logged in as nagiosadmin.
- Host Status Totals:** A table showing the status of all hosts.
- Service Status Details For All Hosts:** A table showing the status of all services.

Host Status Totals		Service Status Totals	
Up	Down	Ok	Warning
1	0	8	0

Host	Service	Status	Last Check	Duration	Attempt
localhost	Current Load	OK	12-10-2019 21:27:38	1d 20h 54m 36s	1/4
	Current Users	OK	12-10-2019 21:28:16	1d 20h 53m 58s	1/4
	HTTP	OK	12-10-2019 21:27:19	1d 20h 53m 21s	1/4