

# ADMINISTRACIÓN DE SISTEMAS OPERATIVOS Y REDES DE COMPUTADORES

FRANCISCO JAVIER PÉREZ MARTÍNEZ  
74384305M – GRUPO 01

## Contenido

1.	FreeBSD.....	2
1.1	Proxy .....	2
1.2	Firewall.....	3
1.3	Monitorización de servicios (Nagios).....	4
1.4	Mensajería instantánea.....	6
1.5	RAID 5.....	7
1.6	Backup.....	8
1.7	FTP (proftpd).....	9
2.	CentOS.....	10
2.1	Proxy .....	10
2.2	Monitorización de servicios (Nagios).....	11
2.3	RAID 5.....	11
2.4	Backup.....	13
2.5	Mensajería instantánea.....	14
2.6	FTP (vsftpd).....	15
2.7	VPN .....	16
3.	Windows Server 2019.....	18
3.1	Mensajería instantánea.....	18
3.2	Proxy .....	18
3.3	Monitorización de servicios (PRTG).....	19
3.4	Backup.....	20
3.5	RAID 5.....	23
3.6	FTP .....	24

# 1. FreeBSD

## 1.1 Proxy

Para instalar el servicio Proxy Cache (Squid) instalaremos su paquete: **pkg install squid**

Una vez instalado, mediante el siguiente comando comprobamos el archivo de configuración:

**squid -f /usr/local/etc/squid/squid.conf -k parse**

Nos saldrán errores por lo que debemos añadir el hostname y la IP con el puerto de Squid.

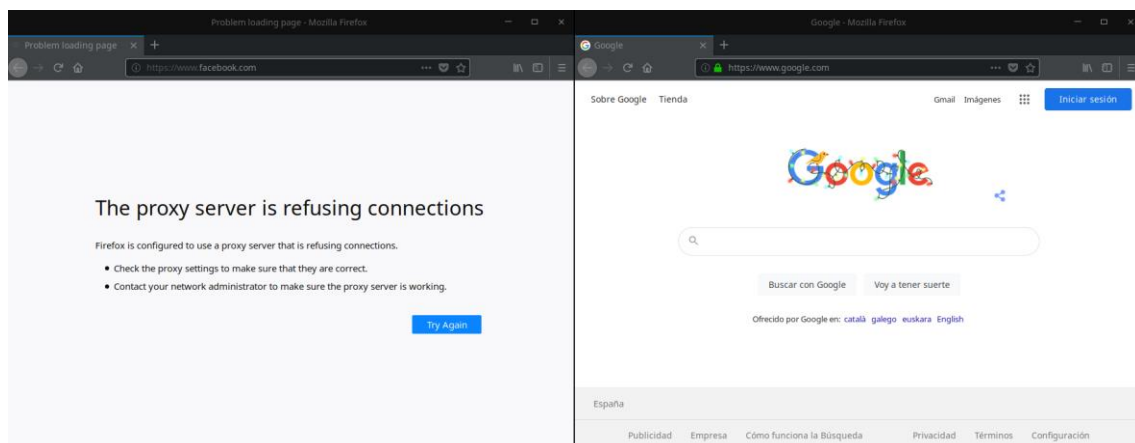
```
# Squid normally listens to port 3128
visible_hostname freebsd.asorc.es
http_port 192.168.56.221:3128
```

A continuación, añadimos la IP del servidor proxy en un cliente y comprobamos qué efectivamente, las páginas y dominios que hemos bloqueados en nuestro archivo de configuración **squid.conf** no son accesibles.

```
#Bloqueo de paginas
acl bpag url_regex www.facebook.com www.youtube.com
http_access deny bpag

#Bloqueo de dominios
acl bdom dstdomain facebook.com youtube.com

#Bloqueo de dispositivo
acl bdis src 192.168.56.113
http_access allow bdis
```



Como se puede apreciar en la imagen de la izquierda no se puede acceder debido a que se ha bloqueado el dominio *“Facebook.com”* en la configuración de nuestro servidor proxy. Sin embargo, en la imagen de la derecha sí podríamos acceder.

## 1.2 Firewall

Podemos utilizar el propio firewall integrado de FreeBSD. En primer lugar, tendremos que añadir las siguientes líneas en el archivo de configuración **/etc/rc.conf**:

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

A continuación, añadimos estas reglas a nuestro firewall en el archivo **/etc/ipfw.rules**:

```
root@freebsd:~ # cat /etc/ipfw.rules
ipfw -q -f flush
cmd="ipfw -q add"
pif="em1"

$cmd 00310 deny icmp from any to any via $pif

$cmd 00999 pass log all from any to any
```

Por último, iniciamos el servicio con **service ipfw start** y podemos comprobar en un cliente como las peticiones de cualquier paquete icmp son rechazadas debido a la regla anterior añadida.

```
javi@javi-PC:~$ ping 192.168.56.221
PING 192.168.56.221 (192.168.56.221) 56(84) bytes of data.
64 bytes from 192.168.56.221: icmp_seq=1 ttl=64 time=0.383 ms
64 bytes from 192.168.56.221: icmp_seq=2 ttl=64 time=0.354 ms
64 bytes from 192.168.56.221: icmp_seq=3 ttl=64 time=0.491 ms
^C
--- 192.168.56.221 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 31ms
rtt min/avg/max/mdev = 0.354/0.409/0.491/0.061 ms
javi@javi-PC:~$ ping 192.168.56.221
PING 192.168.56.221 (192.168.56.221) 56(84) bytes of data.
^C
--- 192.168.56.221 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 66ms
```

Como podemos observar en la imagen, el primer ping a nuestro servidor el firewall estaba desactivado y por lo tanto sí podíamos realizar ping, pero en el segundo ping ejecutado no se ha recibido ningún paquete icmp.

### 1.3 Monitorización de servicios (Nagios)

Para instalar el servicio de Nagios, descargamos el paquete **pkg install nagios**

```
echo 'nagios_enable="YES"' >> /etc/rc.conf
```

Copiamos los sample a los archivos de configuración cfg.

```
cp cgi.cfg-sample cgi.cfg
cp nagios.cfg-sample nagios.cfg
cp resource.cfg-sample resource.cfg
```

Y en la carpeta **/usr/local/etc/nagios/objects/** hacemos lo mismo:

```
cp commands.cfg-sample commands.cfg
cp contacts.cfg-sample contacts.cfg
cp localhost.cfg-sample localhost.cfg
cp printer.cfg-sample printer.cfg
cp switch.cfg-sample switch.cfg
cp templates.cfg-sample templates.cfg
cp timeperiods.cfg-sample timeperiods.cfg
```

A continuación, comprobamos los archivos de configuración:

```
nagios -v /usr/local/etc/nagios/nagios.cfg
```

Introducimos una contraseña al usuario de nagios:

```
htpasswd -c /usr/local/etc/nagios/htpasswd.users nagiosadmin
```

Por último, añadimos las siguientes líneas en la configuración de apache en el archivo http.conf.

```
ScriptAlias /nagios/cgi-bin/ /usr/local/www/nagios/cgi-bin/
Alias /nagios /usr/local/www/nagios/

<Directory /usr/local/www/nagios>
    Options None
    AllowOverride None
    Order allow,deny
    Allow from all
    AuthName "Nagios Access"
    AuthType Basic
    AuthUserFile /usr/local/etc/nagios/htpasswd.users
    Require valid-user
</Directory>

<Directory /usr/local/www/nagios/cgi-bin>
    Options ExecCGI
    AllowOverride None
    Order allow,deny
    Allow from all
    AuthName "Nagios "
    AuthType Basic
    AuthUserFile /usr/local/etc/nagios/htpasswd.users
    Require valid-user
</Directory>
```

Reiniciamos los servicios **apachectl restart** y **service nagios restart**

Una vez configurado todo y reiniciado. Podemos conectarnos desde un navegador web con <http://IP/nagios> accediendo así al panel de Nagios.

The screenshot displays the Nagios Core web interface. The left sidebar contains navigation links for General, Current Status, Reports, and System. The main content area is titled 'Tactical Monitoring Overview' and includes sections for Network Outages, Hosts, Services, and Monitoring Features. The 'Hosts' section shows 0 Down, 0 Unreachable, 1 Up, and 0 Pending. The 'Services' section shows 0 Critical, 1 Warning, 0 Unknown, 7 Ok, and 0 Pending. The 'Monitoring Features' section includes a table with columns for Flap Detection, Notifications, Event Handlers, Active Checks, and Passive Checks, all showing 'All Services Enabled' and 'All Hosts Enabled' status.

Flap Detection	Notifications	Event Handlers	Active Checks	Passive Checks
✓ All Services Enabled	✓ 2 Services Disabled	✓ All Services Enabled	✓ All Services Enabled	✓ All Services Enabled
No Services Flapping	All Hosts Enabled	All Hosts Enabled	All Hosts Enabled	All Hosts Enabled
All Hosts Enabled				
No Hosts Flapping				

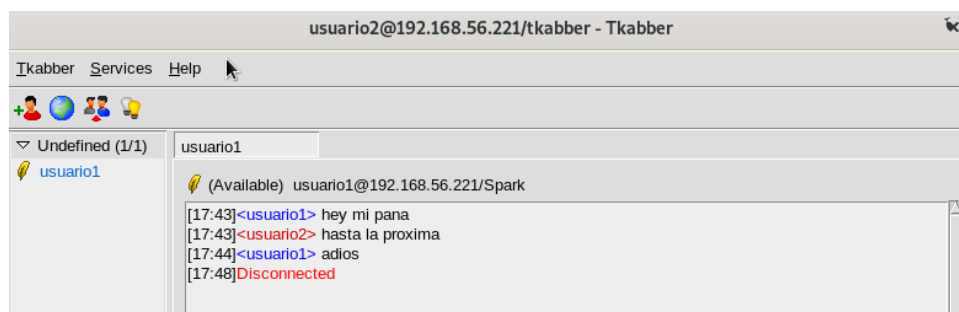
## 1.4 Mensajería instantánea

Para instalar el servicio de mensajería instantánea, descargaremos mediante el siguiente comando: **pkg install openfire**

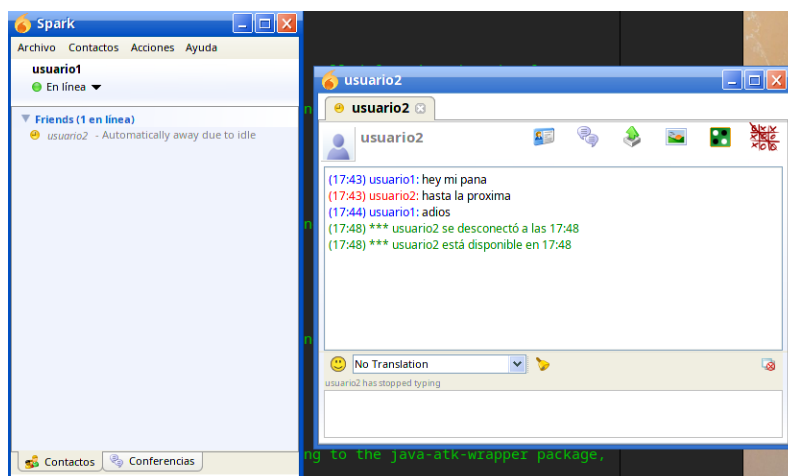
Una vez instalado, desde un navegador introducimos IP:9090, realizamos la instalación y añadimos 2 usuarios para comprobar posteriormente la comunicación entre cliente y servidor.



Desde nuestro servidor, he instalado Tkabber y añadido un usuario: **\$ sudo tkabber**



Desde un cliente, he instado Spark y añadido un usuario: **\$ /opt/Spark/resources/sh startup.sh**



Como se puede observar, se mantiene una comunicación de mensajería instantánea entre dos usuarios.

## 1.5 RAID 5

En primer lugar, debemos añadir la siguiente línea en el archivo de configuración **/etc/rc.conf**

**zfs\_load="YES"**

A continuación, en el directorio **/boot/** configuramos el archivo **loader.conf** introduciendo las siguientes líneas:

```
root@freebsd:/boot # cat loader.conf
zfs_load="YES"
vfs.zfs.prefetch_disable="1"
geom_stripe_load="YES"
```

Una vez configurado, escribimos en la terminal **kldload geom\_stripe**.

Con el comando **ls /dev/** podemos ver todos los discos.

Ahora, creamos el RAID 5:

```
root@freebsd:~ # zpool create raid5 raidz /dev/ada2 /dev/ada3 /dev/ada4 /dev/ada5
root@freebsd:~ # zpool list
```

NAME	SIZE	ALLOC	FREE	CKPOINT	EXPANDSZ	FRAG	CAP	DEDUP	HEALTH	ALTROOT
raid5	39.5G	158K	39.5G	-	-	0%	0%	1.00x	ONLINE	-

Y con el comando **zpool status** comprobamos el estado de los 4 discos:

Provocamos un fallo con **zpool offline raid5 ada2**:

NAME	STATE	READ	WRITE	CKSUM
raid5	DEGRADED	0	0	0
raidz1-0	DEGRADED	0	0	0
3922528301052284507	OFFLINE	0	0	0
ada3	ONLINE	0	0	0
ada4	ONLINE	0	0	0
ada5	ONLINE	0	0	0

was /dev/ada2

Comprobamos si podemos acceder a nuestra carpeta y ver los archivos sin ningún problema y posteriormente volvemos a activar el disco. **zpool online raid5 ada2**

```
root@freebsd:/raid5 # ls
prueba.txt
root@freebsd:/raid5 # cat prueba.txt
esto
es
una
prueba
```

NAME	STATE	READ	WRITE	CKSUM
raid5	ONLINE	0	0	0
raidz1-0	ONLINE	0	0	0
ada2	ONLINE	0	0	0
ada3	ONLINE	0	0	0
ada4	ONLINE	0	0	0
ada5	ONLINE	0	0	0



## 1.6 Backup

Absoluto:

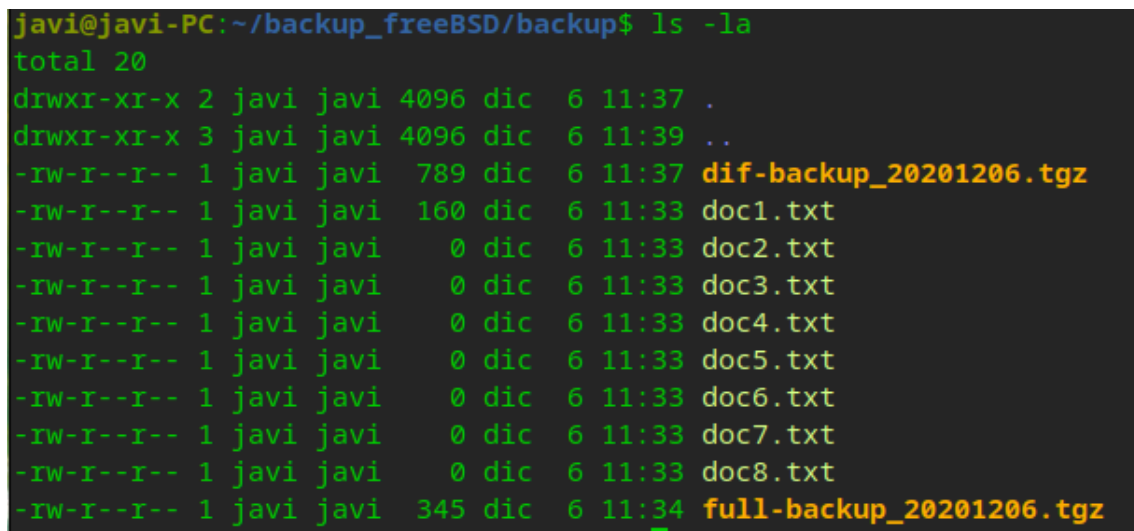
```
tar -cpvzf "full-backup_`date +%Y%m%d`.tgz" /home/Javi/backup/
```

Diferencial:

```
tar -cpvzf "dif-backup_`date +%Y%m%d`.tgz" --newer='2020-12-06'  
/home/Javi/backup/
```

Sincronización:

```
rsync -azP Javi@192.168.56.221:/home/Javi/backup  
/home/javi/backup_freeBSD/
```



A terminal window showing the output of the command `ls -la` in the directory `~/backup_freeBSD/backup`. The output lists the following files and directories:

Permissions	Link Count	User	Group	Size	Month	Day	Time	File Name
drwxr-xr-x	2	javi	javi	4096	dic	6	11:37	.
drwxr-xr-x	3	javi	javi	4096	dic	6	11:39	..
-rw-r--r--	1	javi	javi	789	dic	6	11:37	<b>dif-backup_20201206.tgz</b>
-rw-r--r--	1	javi	javi	160	dic	6	11:33	doc1.txt
-rw-r--r--	1	javi	javi	0	dic	6	11:33	doc2.txt
-rw-r--r--	1	javi	javi	0	dic	6	11:33	doc3.txt
-rw-r--r--	1	javi	javi	0	dic	6	11:33	doc4.txt
-rw-r--r--	1	javi	javi	0	dic	6	11:33	doc5.txt
-rw-r--r--	1	javi	javi	0	dic	6	11:33	doc6.txt
-rw-r--r--	1	javi	javi	0	dic	6	11:33	doc7.txt
-rw-r--r--	1	javi	javi	0	dic	6	11:33	doc8.txt
-rw-r--r--	1	javi	javi	345	dic	6	11:34	<b>full-backup_20201206.tgz</b>

Para hacer la copia del ordenador local a un servidor:

```
rsync -azP /home/javi/backup_freeBSD/backup/  
Javi@192.168.56.221:backupDeepin
```

## 1.7 FTP (proftpd)

En primer lugar, instalaremos el paquete: **pkg install proftpd**

Una vez instalado, editaremos el archivo de configuración:

**nano /usr/local/etc/proftpd.conf**

```
ServerIdent      off
ServerName              "ProFTPD Default Installation"
ServerType          standalone
DefaultServer        on
ScoreboardFile       /var/run/proftpd/proftpd.scoreboard

# Port 21 is the standard FTP port.
Port                21
PassivePorts        30000 30200

# Use IPv6 support by default.
UseIPv6              off
```

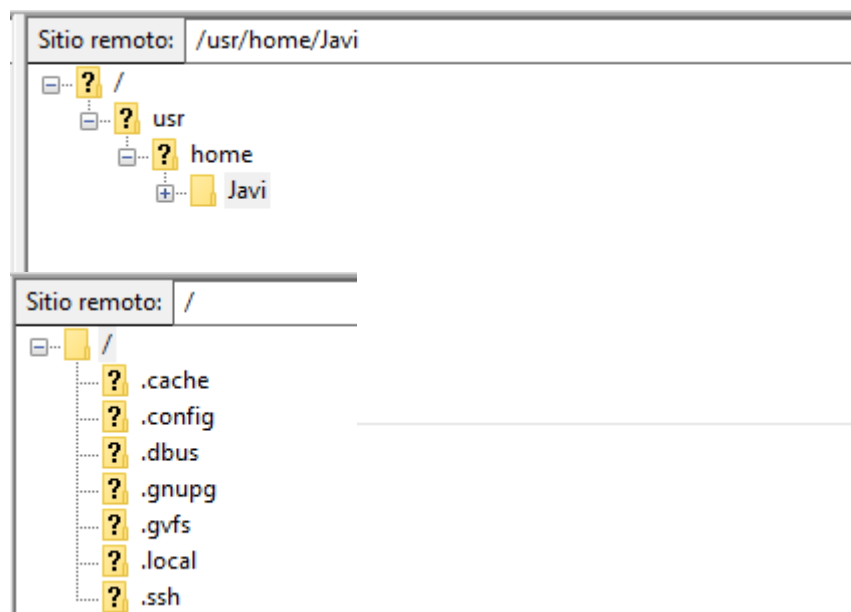
En la siguiente imagen se muestra el usuario oficina enjaulado en su home:

```
# To cause every FTP user to be "jailed" (chrooted) into their home
# directory, uncomment this line.
DefaultRoot /home/oficina/      oficina
```

Por último, iniciamos el servicio: **service proftpd start**

Si surge un error, ir a fichero **/etc/hosts** e introducir **127.0.0.1 "hostname"**

Desde filezilla comprobaremos si se ha enjaulado el usuario oficina.



## 2. CentOS

### 2.1 Proxy

Para instalar el servicio de un servidor proxy utilizaremos Squid instalando así su paquete:

```
dnf install squid
```

Una vez instalado, introducimos las siguientes líneas en nuestro archivo de configuración de squid situado en `/etc/squid/squid.conf`

```
## Custom ACL ##

acl mylocalnet src 192.168.56.0/24

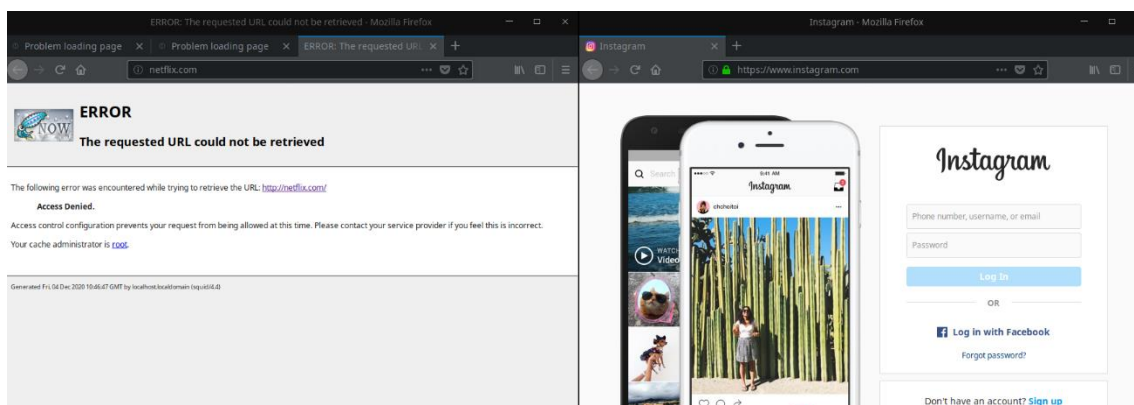
## Adding Sites to Block access to ###
acl blockedsites dstdomain "/etc/squid/restricted-sites.squid"
acl keyword-ban url_regex "/etc/squid/banned-keywords.squid"

http_access deny blockedsites
http_access deny keyword-ban
http_access allow mylocalnet
```

Los archivos `/etc/squid/restricted-sites.squid` y `/etc/squid/banned-keywords.squid` se han creado para denegar el acceso a dominios y palabras en nuestro servidor proxy.

Por último, iniciamos el servicio `systemctl start squid`.

En un navegador web, introducimos la IP de nuestro servidor proxy y comprobamos si realmente los dominios que hemos denegado surgen efecto.



Como se puede observar en la imagen de la izquierda el acceso al dominio “Netflix.com” ha sido denegado y en cambio, el de la derecha no.

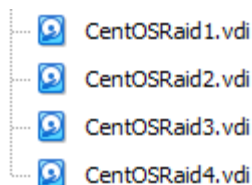
## 2.2 Monitorización de servicios (Nagios)

Para instalar Nagios y realizar toda la configuración pertinente de este servicio seguiremos la web del siguiente enlace: <https://comoinstalar.me/como-instalar-nagios-en-centos-8/>

Desde un navegador introducimos la IP/nagios y comprobamos el estado de nuestros servicios desde la opción **Services**.

## 2.3 RAID 5

En primer lugar, añadimos 4 discos desde la configuración de nuestra máquina virtual en VirtualBox.



Una vez añadido, iniciamos el sistema y escribimos `fdisk /dev/sdc/` para particionar el primer disco. Esta partición va a ser de tipo Linux raid auto (código fd).

```
Disposit.  Inicio Comienzo  Final Sectores Tamaño Id Tipo
/dev/sdc1      2048 10485759 10483712      5G fd Linux raid autodetect
```

Este paso lo haríamos exactamente igual con los 3 discos que faltan.

A continuación, creamos el raid 5 mediante el siguiente comando:

```
mdadm --create -l 5 -n 4 -R -f /dev/md0 /dev/sdc1 /dev/sdd1 /dev/sde1 /dev/sdf1
```

```
[root@localhost ~]# cat /proc/mdstat
Personalities : [raid6] [raid5] [raid4]
md0 : active raid5 sdf1[3] sde1[2] sdd1[1] sdc1[0]
      15710208 blocks super 1.2 level 5, 512k chunk, algorithm 2 [4/4] [UUUU]

unused devices: <none>
```

Ahora pasamos a formatear el disco: **mkfs -t ext4 /dev/md0**

Y lo montamos: **mkdir /raid5** y **mount /dev/md0 /raid5/**

Por último, realizaremos una prueba en el que un disco falla y el sistema es capaz de recuperarse.

Para ello, escribimos el siguiente comando: **mdadm -f /dev/md0 /dev/sdd1**

El comando anterior asigna el disco **sdd1** como disco fallido.

```
[root@localhost ~]# cat /proc/mdstat
Personalities : [raid6] [raid5] [raid4]
md0 : active raid5 sdf1[3] sde1[2] sdd1[1](F) sdc1[0]
      15710208 blocks super 1.2 level 5, 512k chunk, algorithm 2 [4/3] [U_UU]
unused devices: <none>
```

Eliminamos el disco fallido: **mdadm -r /dev/md0 /dev/sdd1**

Y añadimos de nuevo el disco en el sistema: **mdadm -a /dev/md0 /dev/sdd1**

```
[root@localhost ~]# mdadm -a /dev/md0 /dev/sdd1
mdadm: added /dev/sdd1
[root@localhost ~]# cat /proc/mdstat
Personalities : [raid6] [raid5] [raid4]
md0 : active raid5 sdd1[4] sdf1[3] sde1[2] sdc1[0]
      15710208 blocks super 1.2 level 5, 512k chunk, algorithm 2 [4/3] [U_UU]
      [====>.....] recovery = 24.5% (1284572/5236736) finish=0.6min speed=107047K/sec
unused devices: <none>
```

Como vemos el disco se está recuperando de nuevo y finalmente, ya tendríamos el raid funcionando correctamente:

```
[root@localhost ~]# cat /proc/mdstat
Personalities : [raid6] [raid5] [raid4]
md0 : active raid5 sdd1[4] sdf1[3] sde1[2] sdc1[0]
      15710208 blocks super 1.2 level 5, 512k chunk, algorithm 2 [4/4] [UUUU]
unused devices: <none>
```

Por último, añadimos al fichero **/etc/fstab** la ruta de montado para que nos monte el raid siempre que iniciemos la máquina.

```
/dev/md0    /raid5      ext4 defaults,user    0 0
```

## 2.4 Backup

Absoluto: `tar -cpvzf "full-backup_`date +%Y%m%d`.tgz" /home/javi/backup/`

```
[javi@localhost backup]$ tar -cpvzf "full-backup_`date +%Y%m%d`.tgz" /home/javi/backup/
tar: Eliminando la `/' inicial de los nombres
/home/javi/backup/
/home/javi/backup/doc1.txt
/home/javi/backup/doc2.txt
/home/javi/backup/doc3.txt
/home/javi/backup/doc4.txt
/home/javi/backup/doc5.txt
/home/javi/backup/doc6.txt
/home/javi/backup/doc7.txt
/home/javi/backup/doc8.txt
/home/javi/backup/doc9.txt
/home/javi/backup/doc10.txt
tar: /home/javi/backup: el fichero cambi3 mientras se estaba leyendo
[javi@localhost backup]$ ls
doc10.txt  doc2.txt  doc4.txt  doc6.txt  doc8.txt  full-backup_20201206.tgz
doc1.txt  doc3.txt  doc5.txt  doc7.txt  doc9.txt
```

Diferencial: `tar -cpvzf "dif-backup_`date +%Y%m%d`.tgz" /home/javi/backup/ -N 6-dec-20`

```
[javi@localhost backup]$ tar -cpvzf "dif-backup_`date +%Y%m%d`.tgz" /home/javi/backup/ -N 6-dec-20
tar: Opci3n --after-date: Se trata la fecha '6-dec-20' como 2020-12-06 00:00:00
tar: Eliminando la `/' inicial de los nombres
/home/javi/backup/
/home/javi/backup/doc1.txt
/home/javi/backup/doc2.txt
/home/javi/backup/doc3.txt
/home/javi/backup/doc4.txt
/home/javi/backup/doc5.txt
/home/javi/backup/doc6.txt
/home/javi/backup/doc7.txt
/home/javi/backup/doc8.txt
/home/javi/backup/doc9.txt
/home/javi/backup/doc10.txt
/home/javi/backup/full-backup_20201206.tgz
```

Sincronizaci3n: `rsync -azP javi@192.168.56.222:/home/javi/backup /home/javi/backup_centOS/`

```
javi@javi-PC:~$ rsync -azP javi@192.168.56.222:/home/javi/backup /home/javi/backup_centOS/
The authenticity of host '192.168.56.222 (192.168.56.222)' can't be established.
ECDSA key fingerprint is SHA256:su+5d0FBekdggmojEbctH8XrvWgH1P3nF7rhy0aUaU.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.56.222' (ECDSA) to the list of known hosts.
javi@192.168.56.222's password:
receiving incremental file list
backup/
javi@javi-PC:~/backup_centOS$ ls
backup
javi@javi-PC:~/backup_centOS$ cd backup/
javi@javi-PC:~/backup_centOS/backup$ ls
dif-backup_20201206.tgz  doc1.txt  doc3.txt  doc5.txt  doc7.txt  doc9.txt
doc10.txt               doc2.txt  doc4.txt  doc6.txt  doc8.txt  full-backup_20201206.tgz
javi@javi-PC:~/backup_centOS/backup$ ls
dif-backup_20201206.tgz  doc1.txt  doc3.txt  doc5.txt  doc7.txt  doc9.txt
doc10.txt               doc2.txt  doc4.txt  doc6.txt  doc8.txt  full-backup_20201206.tgz
javi@javi-PC:~/backup_centOS/backup$ rsync -azP javi@192.168.56.222:/home/javi/backup /home/javi/backup_centOS/
javi@192.168.56.222's password:
receiving incremental file list
backup/
backup/doc_rsync.txt
0 100% 0.00kB/s 0:00:00 (xfr#1, to-chk=1/14)
javi@javi-PC:~/backup_centOS/backup$
```

## 2.5 Mensajería instantánea

En primer lugar, instalaremos openfire al igual que hemos hecho con FreeBSD:

```
wget -c https://download.igniterealtime.org/openfire/openfire-4.6.0-1.x86\_64.rpm
```

Iniciamos el servicio **systemctl start openfire**.

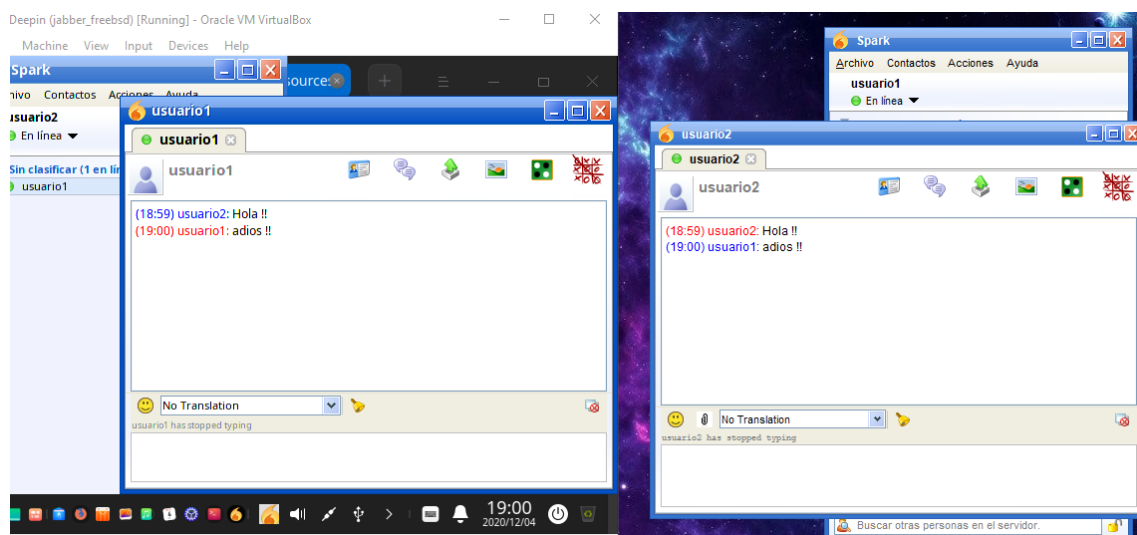
Una vez instalado e iniciado, escribiremos en un navegador web la **IP:9090** para terminar la instalación y posteriormente crear 2 usuarios para comprobar la comunicación entre ambos.

Descargamos un cliente, como Spark:

```
dnf install pcp-export-pcp2spark-5.0.2-5.el8.x86_64
```

Y en otra máquina otro cliente.

Una vez obtenido los 2 clientes que usaremos para la comunicación de mensajería nos conectamos y ya podemos empezar a conversar de manera instantánea.



## 2.6 FTP (vsftpd)

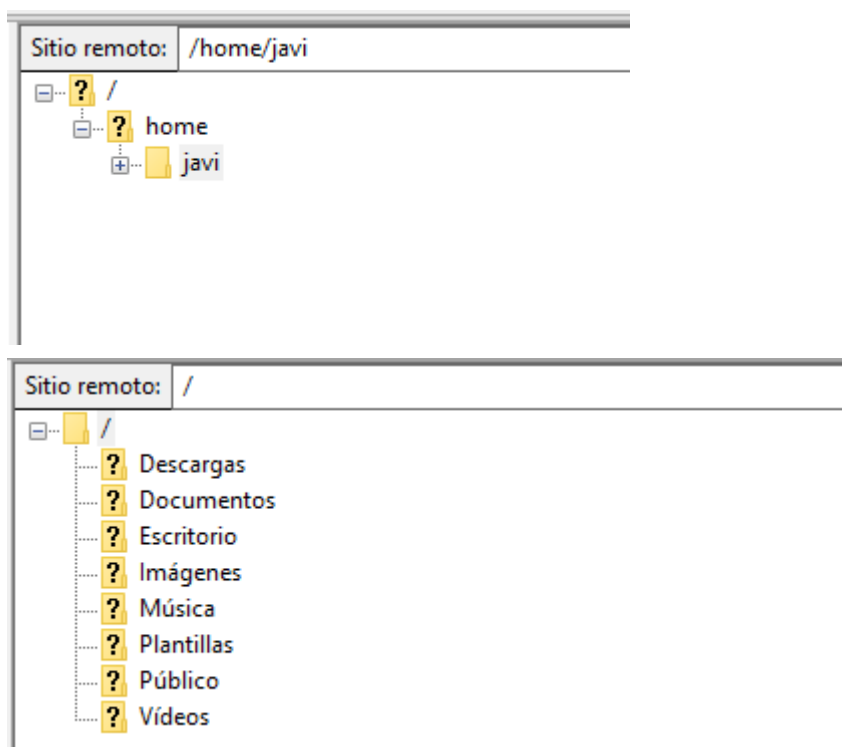
Para instalar vsftpd, nos instalaremos el siguiente paquete: **dnf install vsftpd**

Iniciamos el servicio: **systemctl start vsftpd**

Editamos el fichero de configuración situado en **/etc/vsftpd/vsftpd.conf** introduciendo las siguientes líneas:

```
# chroot)
chroot_local_user=YES
chroot_list_enable=YES
# (default follows)
chroot_list_file=/etc/vsftpd/chroot_list
allow_writeable_chroot=YES
```

Crearemos el archivo **chroot\_list** e introduciremos el usuario que no queremos que esté enjaulado. Todos los que no estén en esta lista, quedarán enjaulados.



Como vemos en la segunda imagen, el usuario se encuentra enjaulado y no puede acceder a las ramas padres. Sin embargo, en la primera imagen, el usuario en cuestión sí que podría.



## 2.7 VPN

En primer lugar, instalaremos el servicio de openvpn siguiendo los siguientes comandos:

```
git clone https://github.com/Nyr/openvpn-install.git
```

```
cd openvpn-install
```

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

```
./openvpn-install.sh -> Instalamos
```

Seguimos los siguientes pasos de instalación:

```
Welcome to this OpenVPN road warrior installer!

Which IPv4 address should be used?
  1) 10.0.2.19
  2) 192.168.56.222
  3) 192.168.122.1
IPv4 address [1]: 2

This server is behind NAT. What is the public IPv4 address or hostname?
Public IPv4 address / hostname [213.181.88.146]: 192.168.56.222

Which protocol should OpenVPN use?
  1) UDP (recommended)
  2) TCP
Protocol [1]: 1

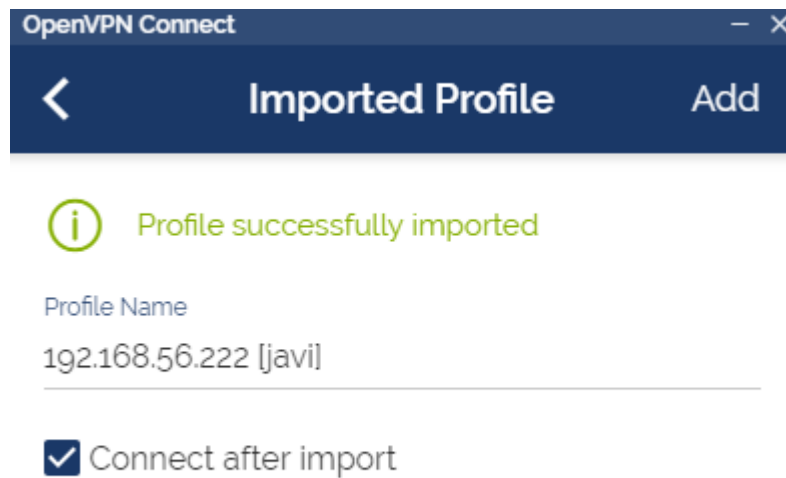
What port should OpenVPN listen to?
Port [1194]:

Select a DNS server for the clients:
  1) Current system resolvers
  2) Google
  3) 1.1.1.1
  4) OpenDNS
  5) Quad9
  6) AdGuard
DNS server [1]:

Enter a name for the first client:
Name [client]: javi

OpenVPN installation is ready to begin.
```

Una vez instalado y configurado, descargaremos el cliente **OpenVPN Connect** e introduciremos el archivo javi.opvn generado en dicho cliente.



En una terminal podemos comprobar como se ha creado el túnel:

Sin VPN:

```
Adaptador desconocido Conexión de área local:

Estado de los medios. . . . . : medios desconectados
Sufijo DNS específico para la conexión. . :
```

Con VPN:

```
Adaptador desconocido Conexión de área local:

Sufijo DNS específico para la conexión. . :
Vínculo: dirección IPv6 local. . . : fe80::7981:6353:6fb:a7ec%29
Dirección IPv4. . . . . : 10.8.0.2
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada . . . . . : 10.8.0.1
```

## 3. Windows Server 2019

### 3.1 Mensajería instantánea

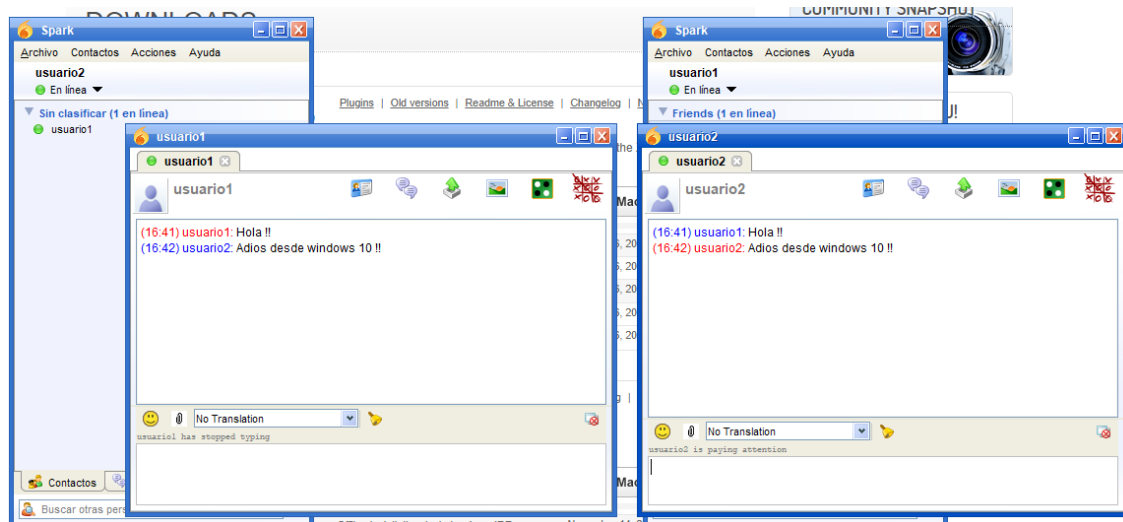
Para instalar este servicio, nos dirigiremos a la siguiente página web:

<https://www.igniterealtime.org/downloads/>

En esta web, descargaremos openfire y el cliente Spark.

Una vez instalado y configurado, crearemos 2 usuarios para comprobar la comunicación entre ambos.

Nos conectamos con los 2 clientes y ya podemos empezar a conversar de manera instantánea.



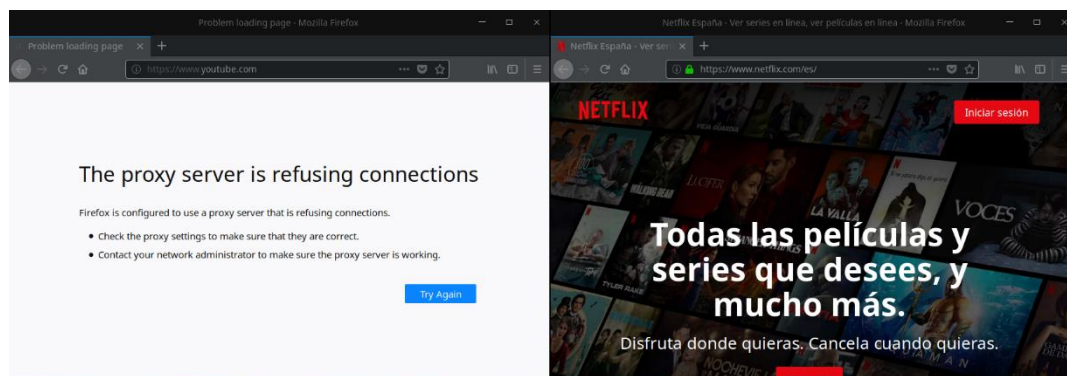
### 3.2 Proxy

Para descargar Proxy Squid lo descargaremos desde el siguiente enlace:

<https://squid.diladele.com/>

Seguiremos los pasos de instalación y en el archivo de configuración introduciremos los dominios deseados para bloquearlos al igual que en los otros sistemas operativos.

Como se puede observar a la izquierda, el servidor proxy bloquea el dominio “youtube.com”.



### 3.3 Monitorización de servicios (PRTG)

En Windows Server he instalado PRTG desde su página web oficial:

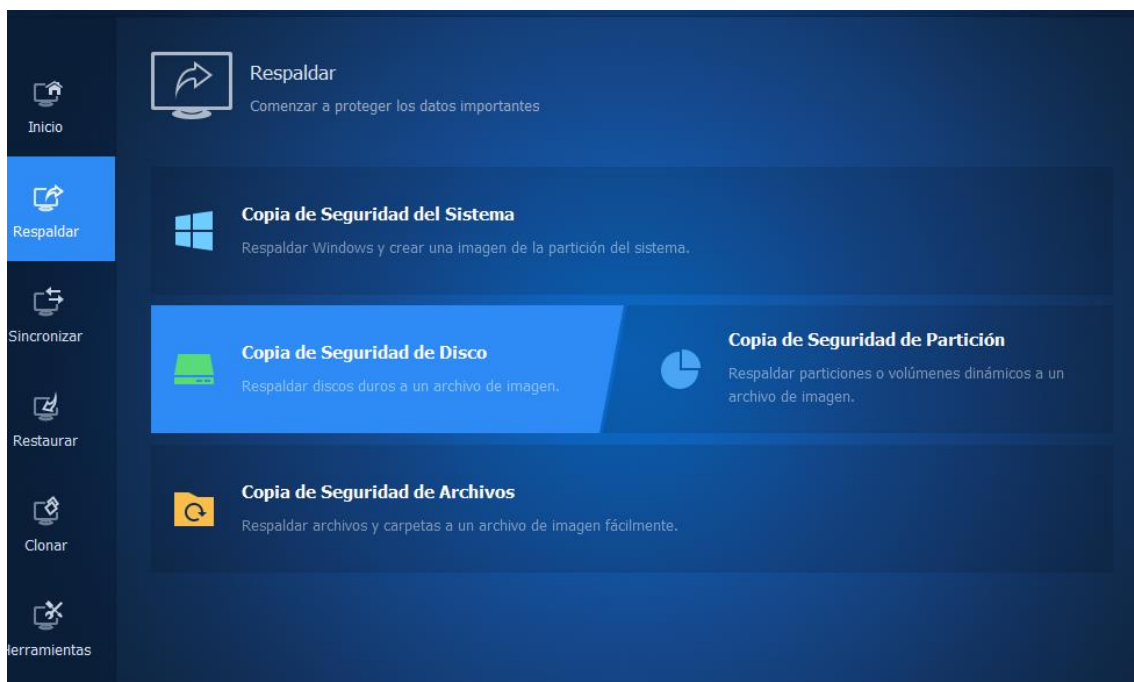
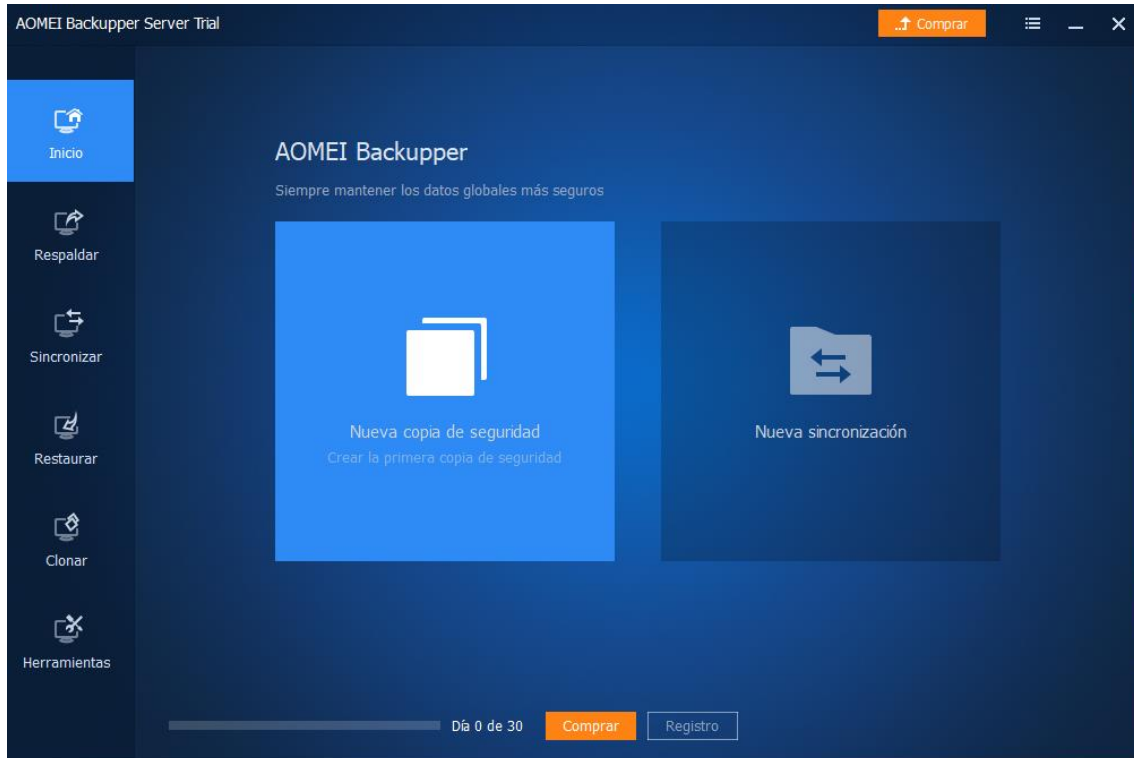
<https://www.es.paessler.com/prtg>

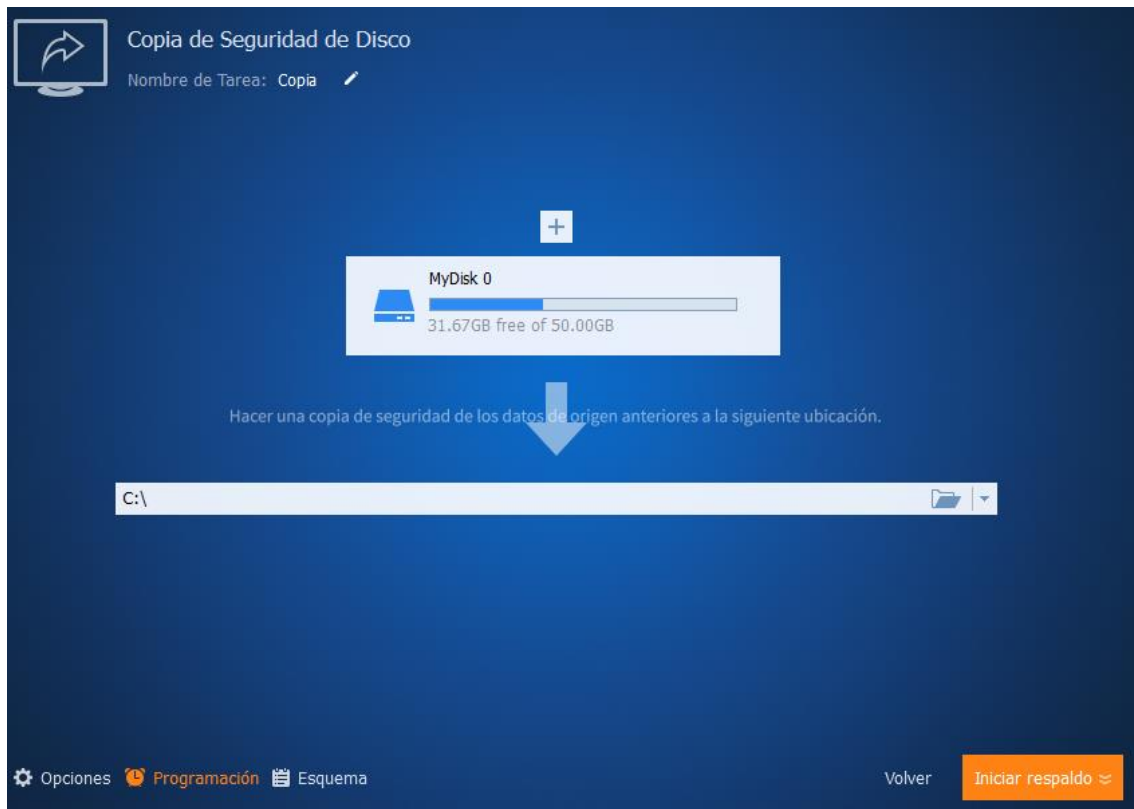
Seguimos los pasos de instalación y nos conectamos desde un navegador web para ver toda la monitorización de nuestros servicios en el sistema: <http://10.0.2.4:8080/>

Sensor	Dispositivo de grupo de sonda	Estado	Último valor	Mensaje	Gráfica	Prioridad	Fav.
Salud de sistema	Sonda local (Sonda local) » Dispositivo de sonda	Advertencia	25 %	81 % (Carga de procesador ...	Estado 25 %	★★★★★	
Salud de sonda	Sonda local (Sonda local) » Dispositivo de sonda	OK	100 %	OK	Estado 100 %	★★★★★	
Salud del servidor ce...	Sonda local (Sonda local) » Dispositivo de sonda	OK	18 %	OK	Estado 18 %	★★★★★	
Disco disponible	Sonda local (Sonda local) » Dispositivo de sonda	OK	65 %	OK	Espacio disp 65 %	★★★★☆	
Common SaaS Check	Sonda local (Sonda local) » Dispositivo de sonda	OK	100 %	OK	Servicios disp 100 %	★★★★☆	
HTTP	Sonda local (Sonda local) » Infraestructura de red » Internet	OK	108 mseg	OK	Tiempo de ca 108 mseg	★★★★☆	
Intel[R] PRO_1000 MT...	Sonda local (Sonda local) » Dispositivo de sonda	OK	25 kbit/s	OK	Total 25 kbit/s	★★★☆☆	
Intel[R] PRO_1000 MT...	Sonda local (Sonda local) » Dispositivo de sonda	OK	2,09 kbit/s	OK	Total 2,09 kbit/s	★★★☆☆	

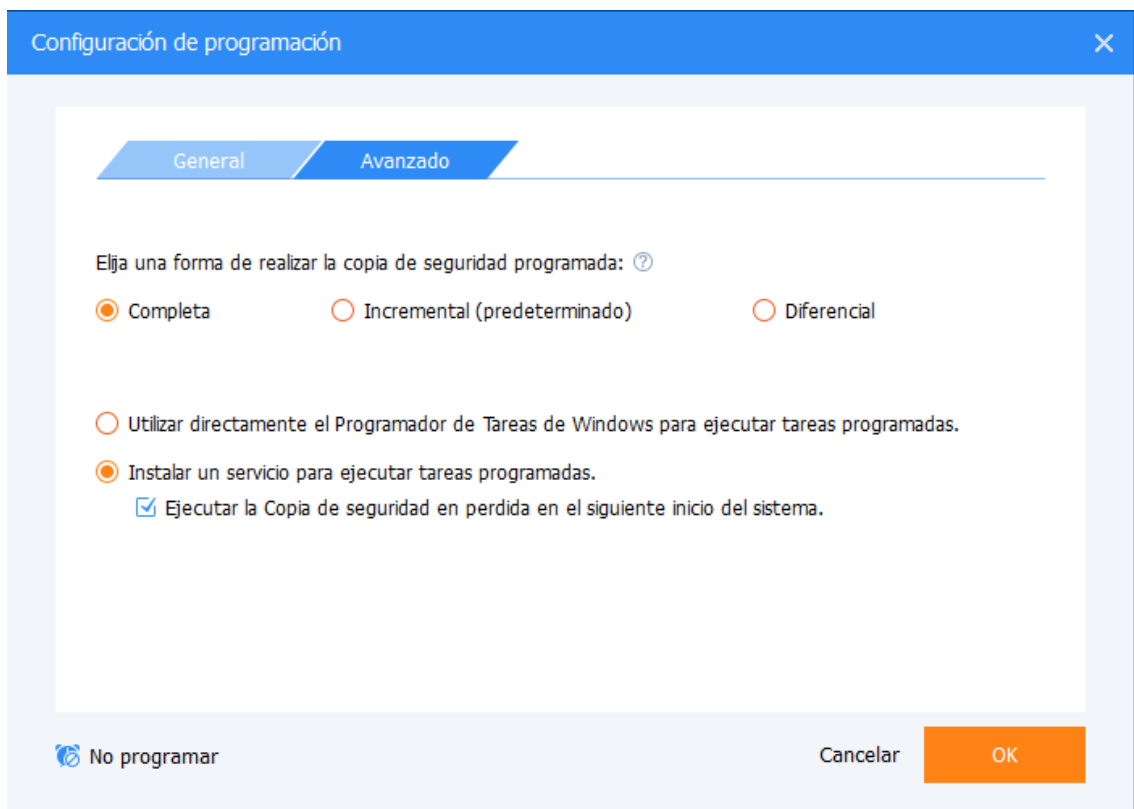
### 3.4 Backup

Para realizar los distintos tipos de backups instalaremos el programa AOMEI Backupper.

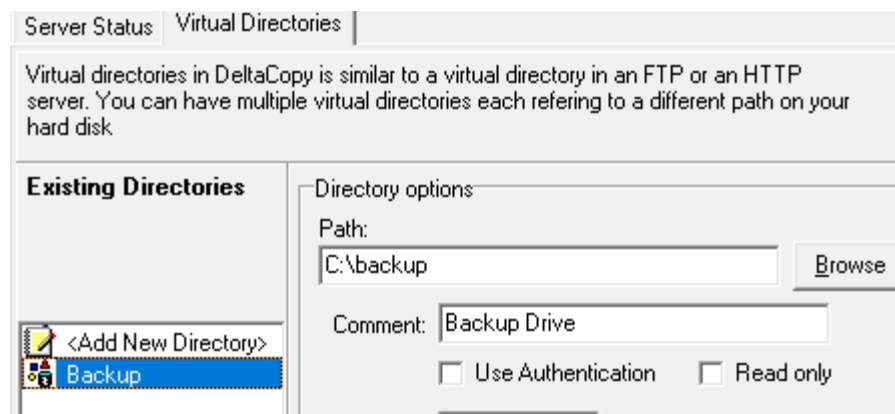
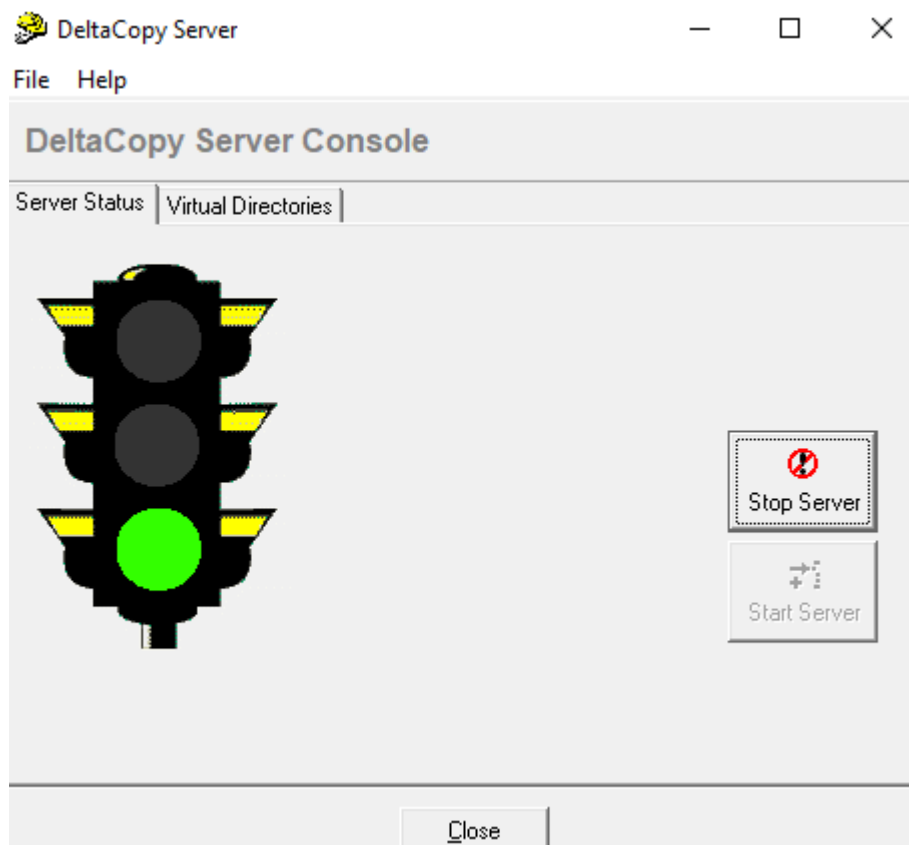




Para realizar los diferentes tipos de backups, una vez añadido el disco, elegimos desde la opción programación, el tipo de backup que deseamos.



Para el backup de sincronización instalaremos el programa DeltaCopy:



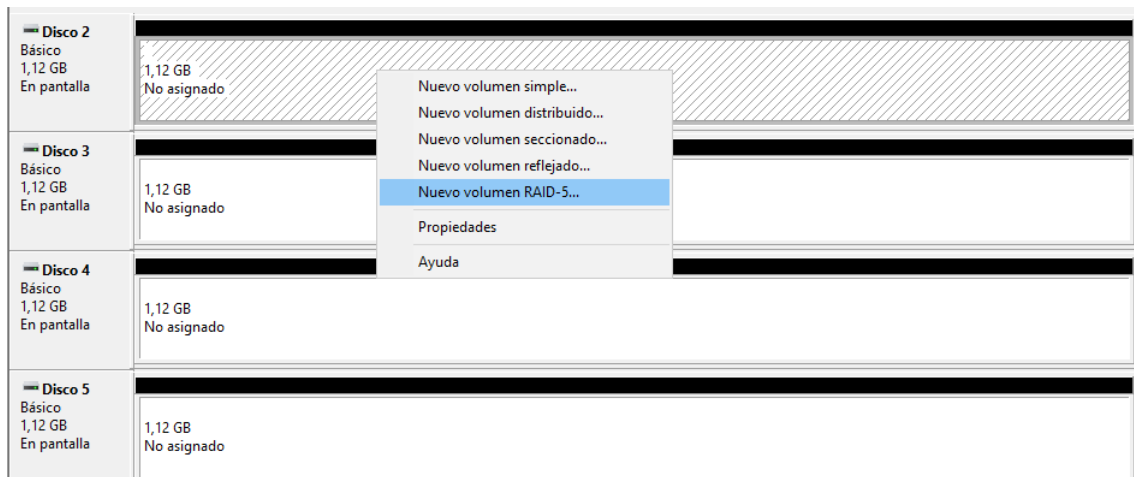
```
rsync -avz 192.168.56.223::Backup /home/javi/backup_windows/
```

```
javi@javi-PC:~/backup_windows$ rsync -avz 192.168.56.223::Backup /home/javi/backup_windows/
receiving incremental file list
./
doc1.txt

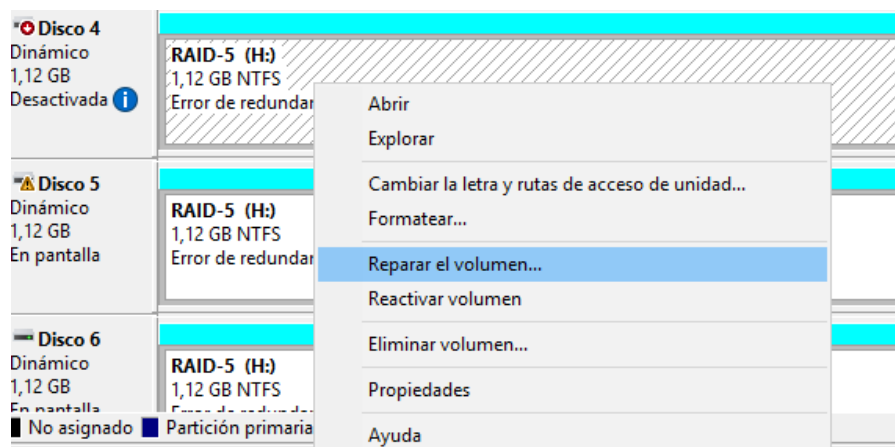
sent 50 bytes  received 140 bytes  380.00 bytes/sec
total size is 0  speedup is 0.00
```

### 3.5 RAID 5

En primer lugar, añadiremos los 4 discos al igual que en los otros sistemas. Una vez añadidos, vamos al administrador de discos y le damos clic derecho >> Nuevo volumen RAID-5.



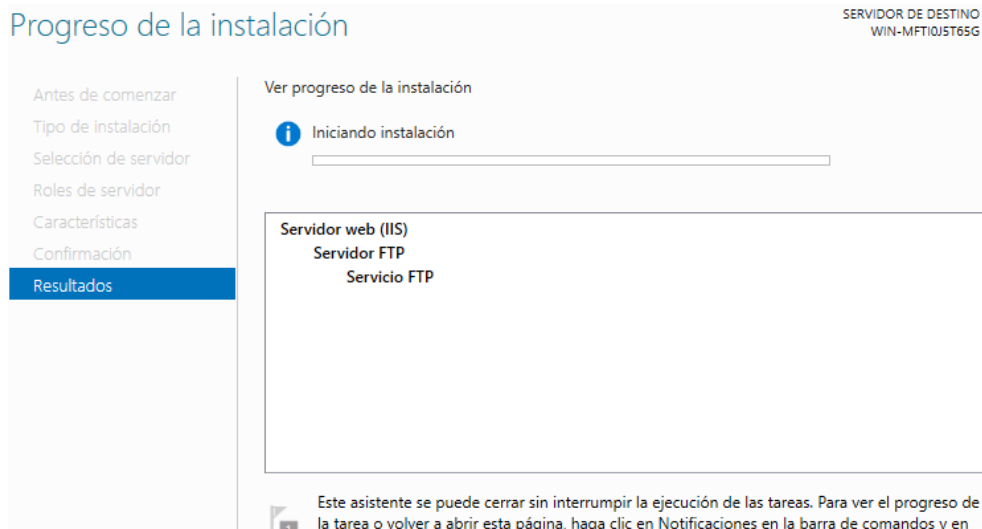
Si provocamos un fallo, podemos hacer clic derecho >> reparar volumen y ya tendríamos nuestro RAID5 funcionando de nuevo correctamente.





### 3.6 FTP

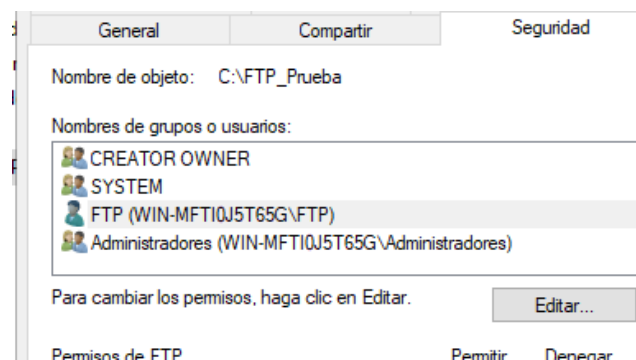
Instalaremos el Servidor FTP desde el Administrador del servidor.



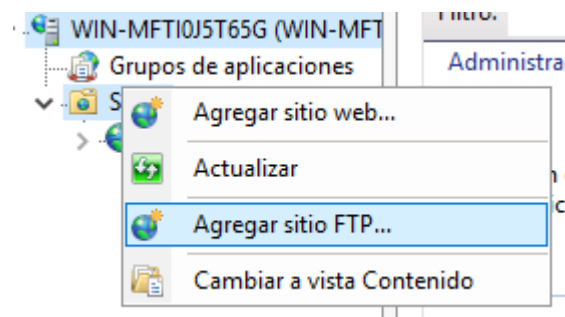
Una vez instalado, creamos un grupo para FTP:

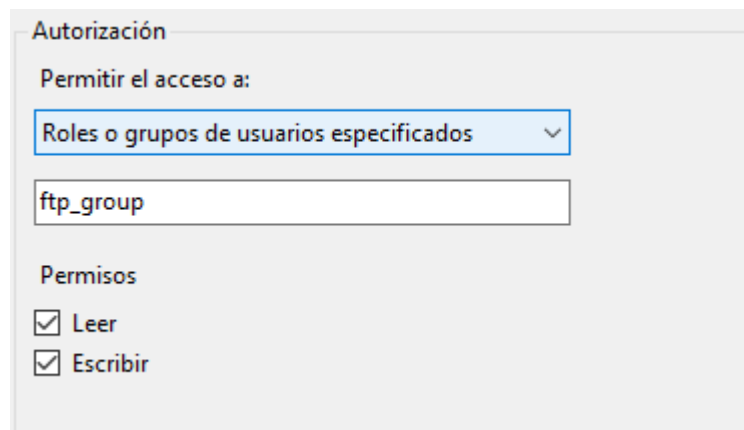


Creamos una carpeta de prueba y en Propiedades >> Seguridad, añadimos para que en esta carpeta solo puede ser accesible desde el usuario creado FTP.

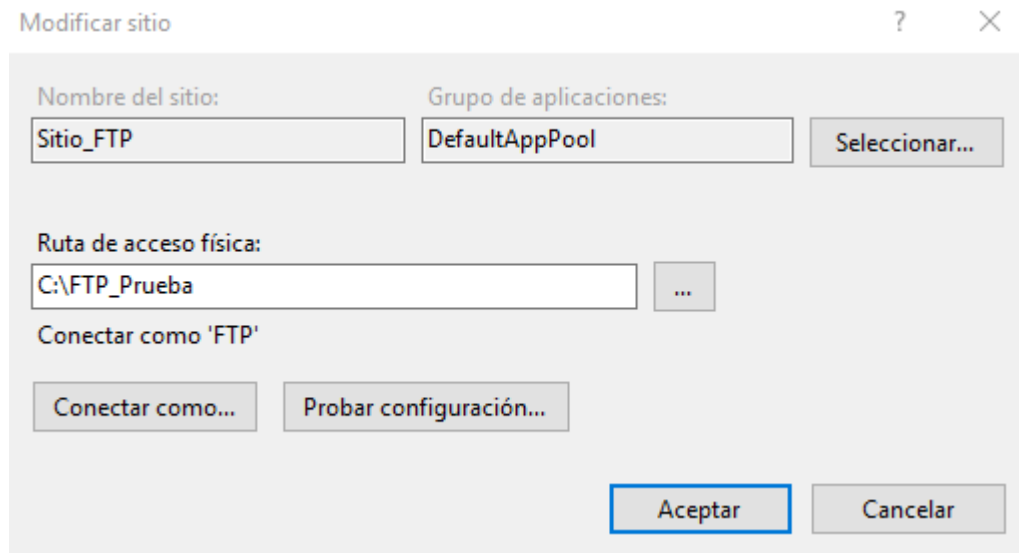


Desde herramientas del Administrador del servidor vamos Administrador de ISS y creamos un sitio FTP.

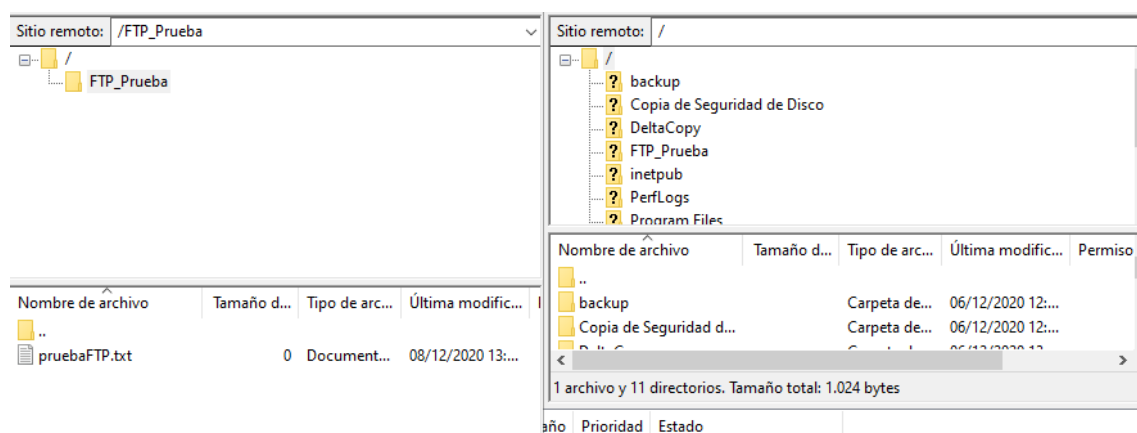




Una vez creado el sitio FTP, vamos a configuración básica y le damos a Conectar como... y añadimos el usuario creado FTP.



Desde Filezilla comprobaremos como el usuario FTP esta enjaulado solamente en la carpeta que hemos creado de prueba.



Como se puede observar, en la izquierda el usuario FTP está enjaulado en la carpeta de prueba. Sin embargo, en la derecha otro usuario distinto a FTP puede acceder a todas las carpetas del sistema.