**ADMINISTRACIÓN DE SISTEMAS OPERATIVOS Y REDES DE COMPUTADORES**

UNIVERSIDAD DE ALICANTE | GRADO EN INGENIERÍA INFORMÁTICA

Francisco Javier Pérez Martínez

74384305m – gRUPO 01

**HITO 3**

Contenido

[1. FreeBSD 2](#_Toc58861375)

[1.1 Proxy 2](#_Toc58861376)

[1.2 Firewall 3](#_Toc58861377)

[1.3 Monitorización de servicios (Nagios) 4](#_Toc58861378)

[1.4 Mensajería instantánea 6](#_Toc58861379)

[1.5 RAID 5 7](#_Toc58861380)

[1.6 Backup 8](#_Toc58861381)

[1.7 FTP (proftpd) 9](#_Toc58861382)

[2. CentOS 10](#_Toc58861383)

[2.1 Proxy 10](#_Toc58861384)

[2.2 Monitorización de servicios (Nagios) 11](#_Toc58861385)

[2.3 RAID 5 11](#_Toc58861386)

[2.4 Backup 13](#_Toc58861387)

[2.5 Mensajería instantánea 14](#_Toc58861388)

[2.6 FTP (vsftpd) 15](#_Toc58861389)

[2.7 VPN 16](#_Toc58861390)

[3. Windows Server 2019 18](#_Toc58861391)

[3.1 Mensajería instantánea 18](#_Toc58861392)

[3.2 Proxy 18](#_Toc58861393)

[3.3 Monitorización de servicios (PRTG) 19](#_Toc58861394)

[3.4 Backup 20](#_Toc58861395)

[3.5 RAID 5 23](#_Toc58861396)

[3.6 FTP 24](#_Toc58861397)

# FreeBSD

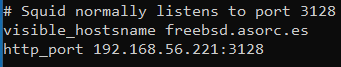
## Proxy

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

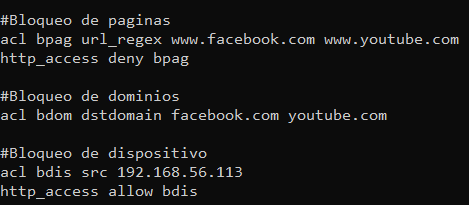
Una vez instalado, mediante el siguiente comando comprobamos el archivo de configuración:

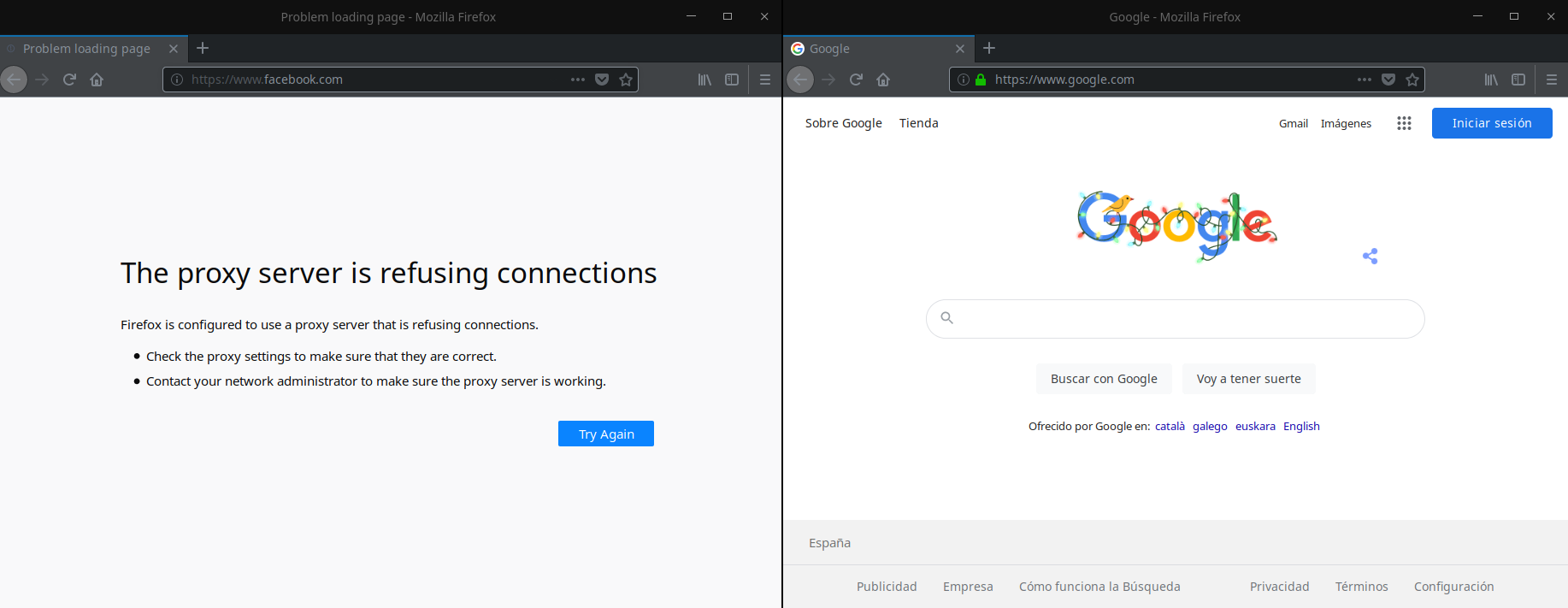
**squid -f /usr/local/etc/squid/squid.conf -k parse**

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



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.

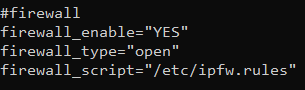




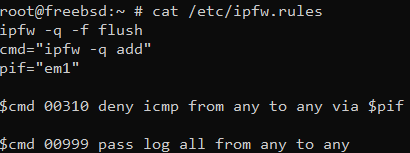
Como se puede apreciar en la imagen de la izquierda no se puede acceder debido a que se ha bloqueado el domino *“Facebook.com”* en la configuración de nuestro servidor proxy. Sin embargo, en la imagen de la derecha sí podríamos acceder.

## Firewall

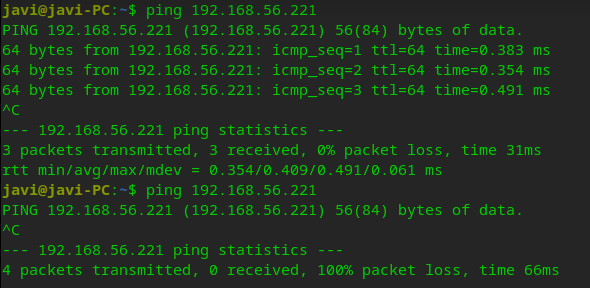
Podemos utilizar el propio firewall integrado de FreeBSD. En primer lugar, tendremos que añadir las siguientes líneas en el archivo de configuración **/etc/rc.conf:**



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



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.



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

## 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**

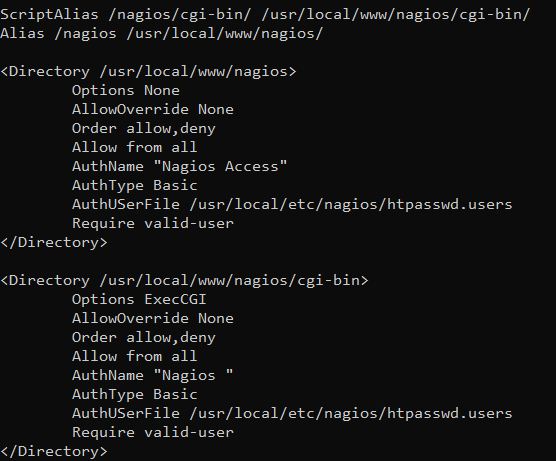
A continuación, comprobamos los archivos de configuración:

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

Introducimos una contraseña al usuario de nagios:

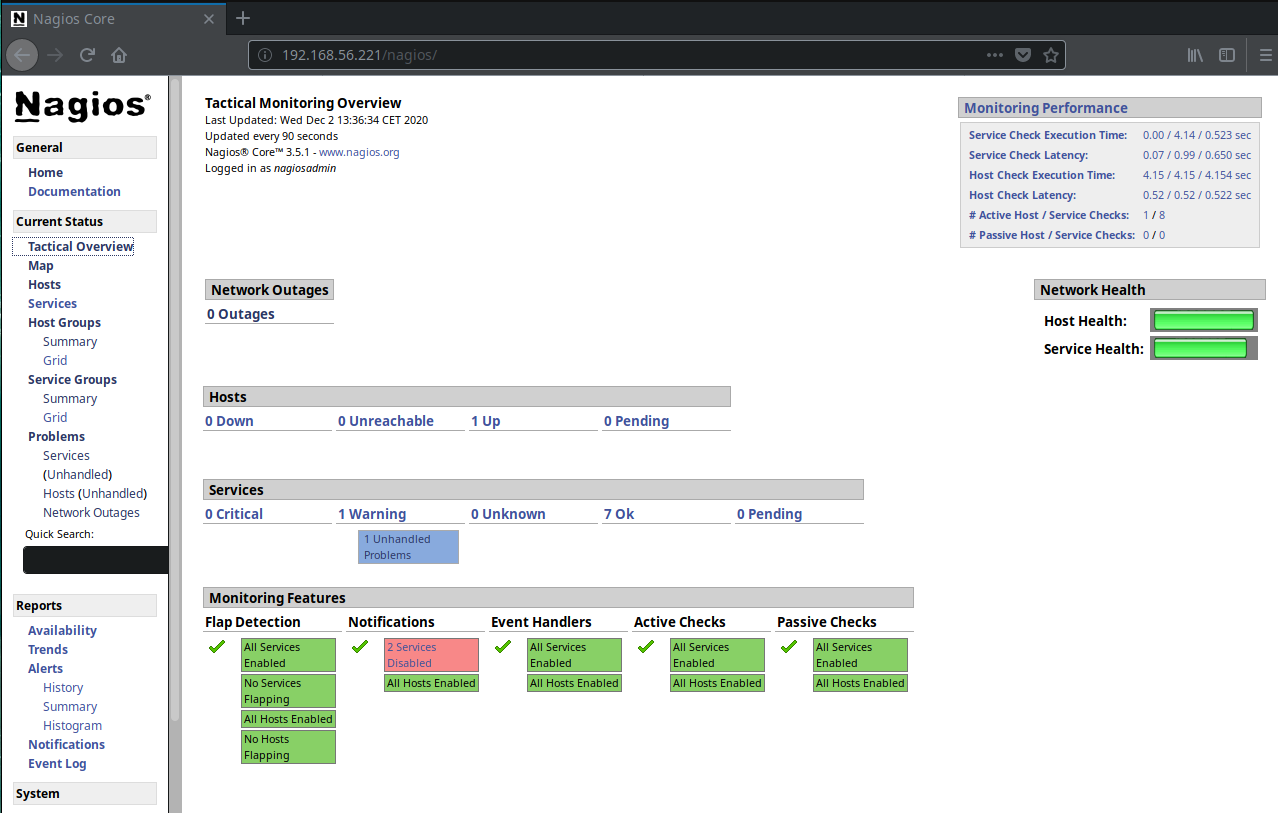
**htpasswd -c /usr/local/etc/nagios/htpasswd.users nagiosadmin**

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



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

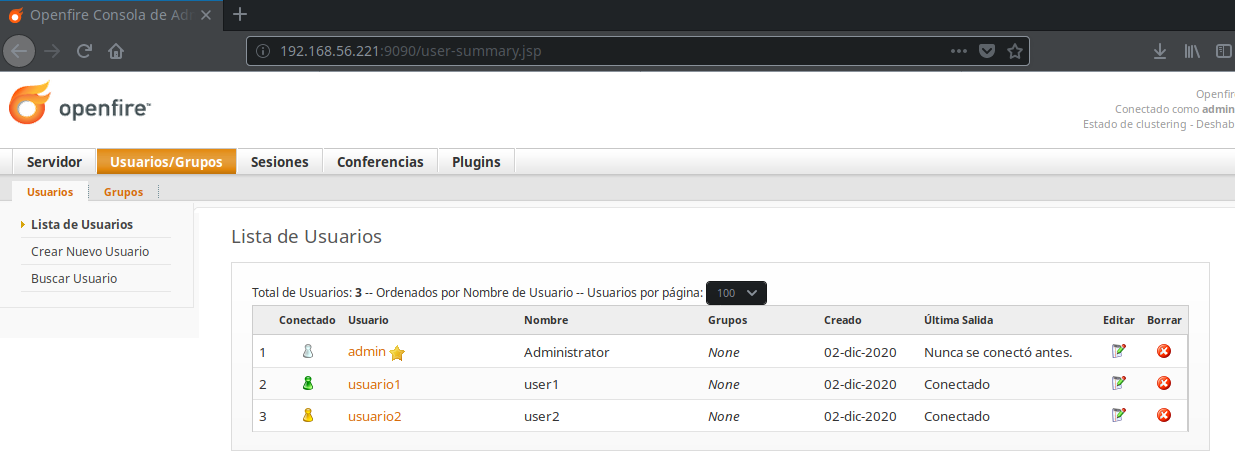
Una vez configurado todo y reiniciado. Podemos conectarnos desde un navegador web con <http://IP/nagios> accediendo así al panel de Nagios.



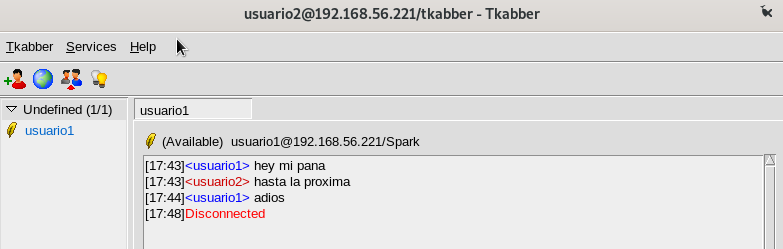
## Mensajería instantánea

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

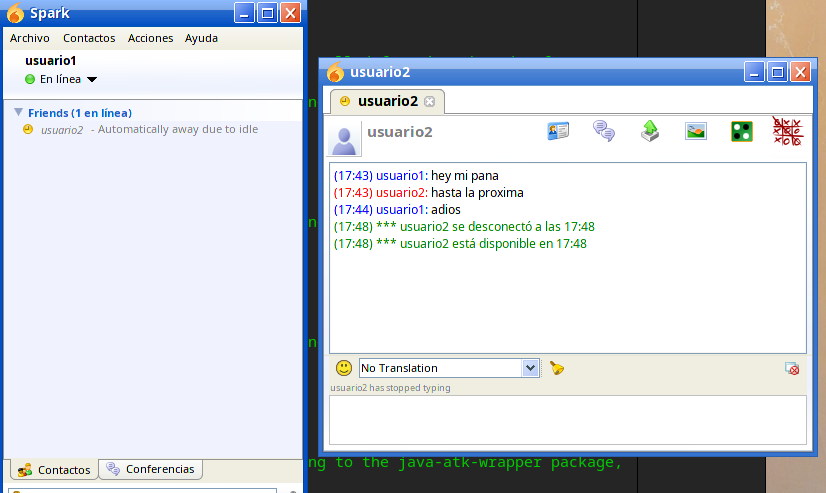
Una vez instalado, desde un navegador introducimos IP:9090, realizamos la instalación y añadimos 2 usuarios para comprobar posteriormente la comunicación entre cliente y servidor.



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**

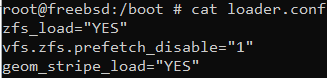


Como se puede observar, se mantiene una comunicación de mensajería instantánea entre dos usuarios.

## RAID 5

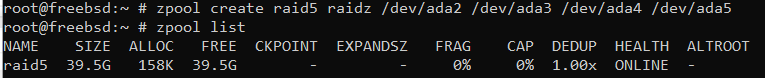
En primer lugar, debemos añadir la siguiente línea en el archivo de configuración **/etc/rc.conf**

**zfs\_load=”YES”**

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

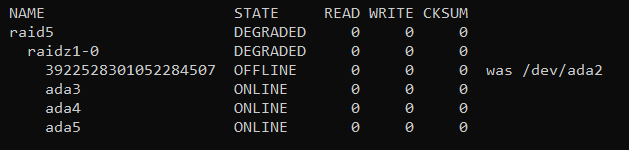
Una vez configurado, escribimos en la terminal **kldload geom\_stripe.**

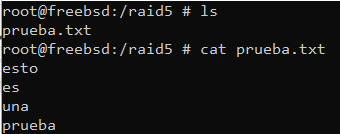
Con el comando **ls /dev/** podemos ver todos los discos.

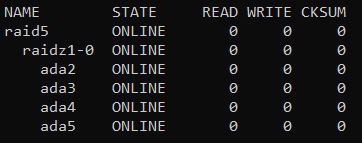
Ahora, creamos el RAID 5:

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

Provocamos un fallo con **zpool offline raid5 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**



## Backup

Absoluto:

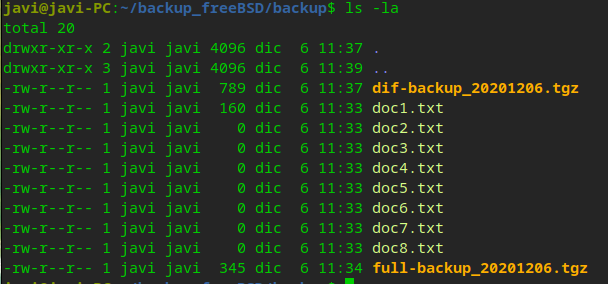
**tar -cpvzf "full-backup\_`date +%Y%m%d`.tgz" /home/Javi/backup/**

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/**



Para hacer la copia del ordenador local a un servidor:

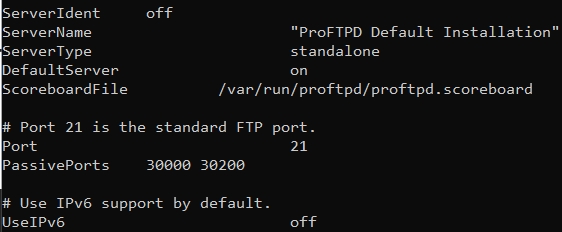
**rsync -azP /home/javi/backup\_freeBSD/backup/ Javi@192.168.56.221:backupDeepin**

## FTP (proftpd)

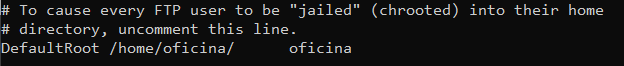
En primer lugar, instalaremos el paquete: **pkg install proftpd**

Una vez instalado, editaremos el archivo de configuración:

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



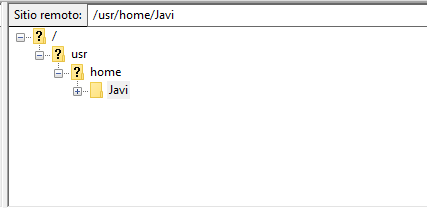
En la siguiente imagen se muestra el usuario oficina enjaulado en su home:

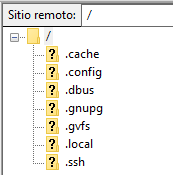


Por último, iniciamos el servicio: **service proftpd start**

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.





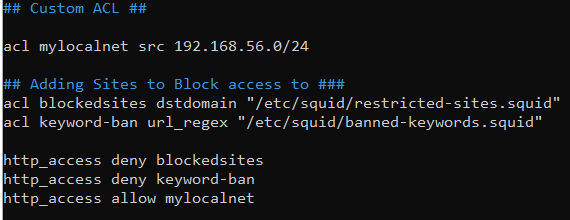
# CentOS

## Proxy

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

**dnf install squid**

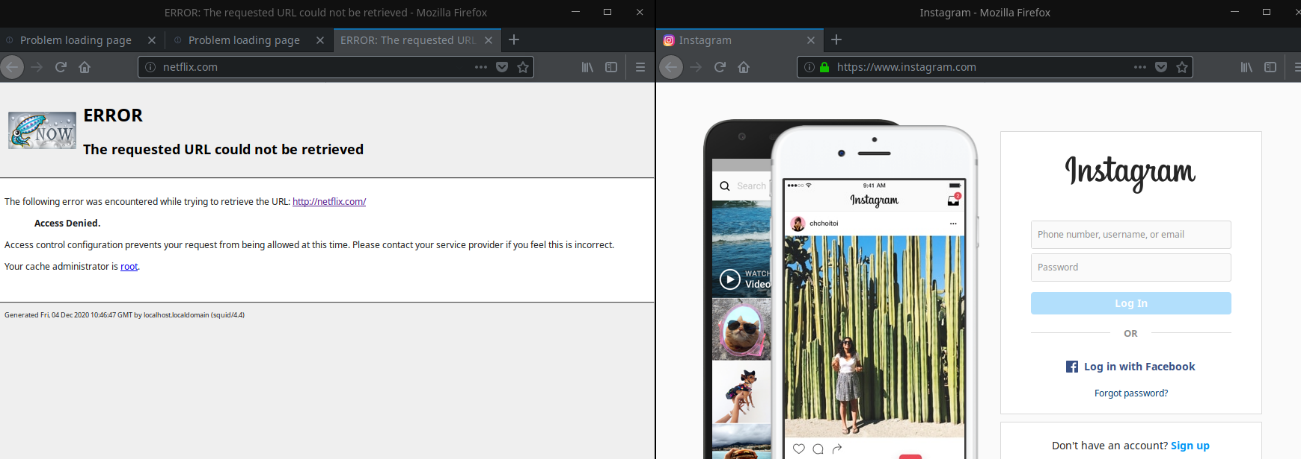
Una vez instalado, introducimos las siguientes líneas en nuestro archivo de configuración de squid situado en **/etc/squid/squid.conf**

****

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.

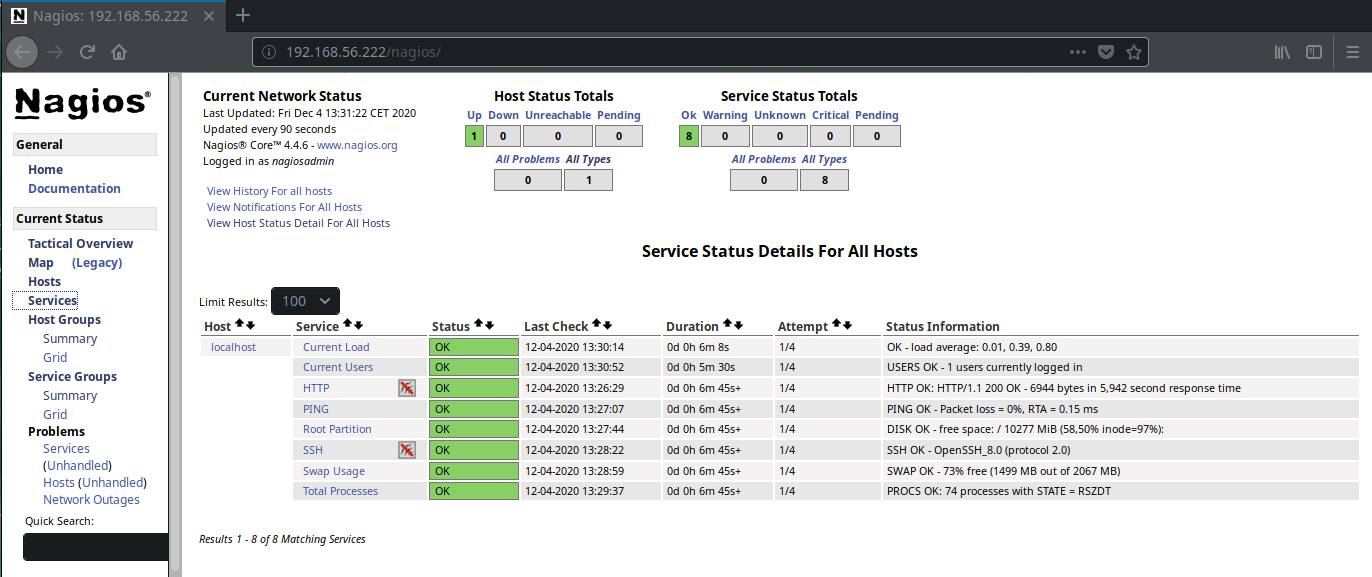


Como se puede observar en la imagen de la izquierda el acceso al dominio “Netflix.com” ha sido denegado y en cambio, el de la derecha no.

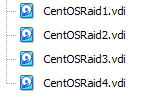
## Monitorización de servicios (Nagios)

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**.



## RAID 5

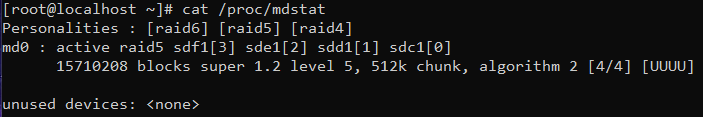
En primer lugar, añadimos 4 discos desde la configuración de nuestra máquina virtual en VirtualBox.

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).

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**



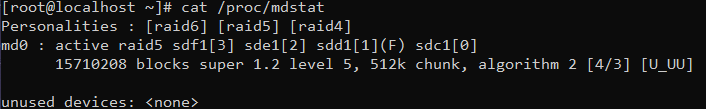
Ahora pasamos a formatear el disco: **mkfs -t ext4 /dev/md0**

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.

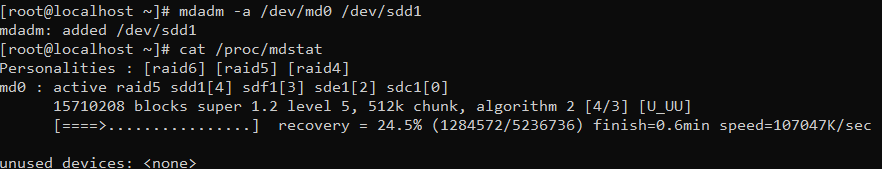
Para ello, escribimos el siguiente comando: **mdadm -f /dev/md0 /dev/sdd1**

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

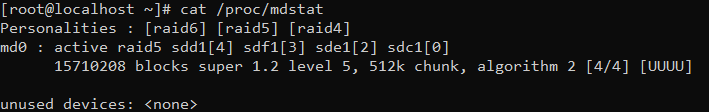


Eliminamos el disco fallido: **mdadm -r /dev/md0 /dev/sdd1**

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



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

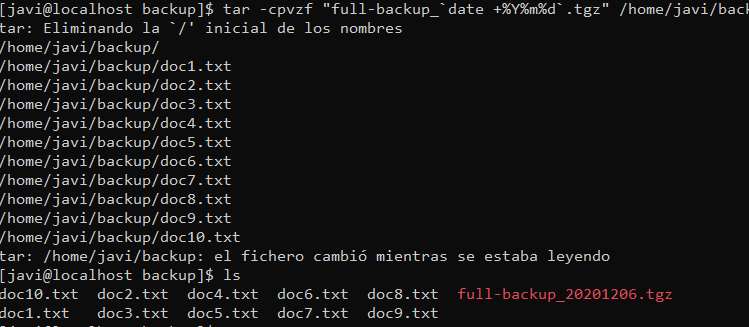


Por último, añadimos al fichero **/etc/fstab** la ruta de montado para que nos monte el raid siempre que iniciemos la máquina.

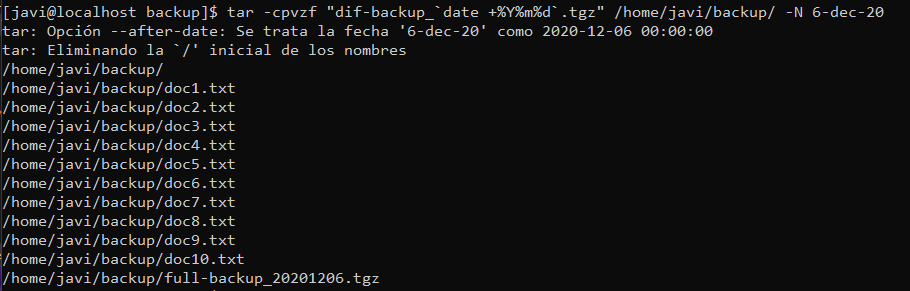
**/dev/md0 /raid5 ext4 defaults,user 0 0**

## Backup

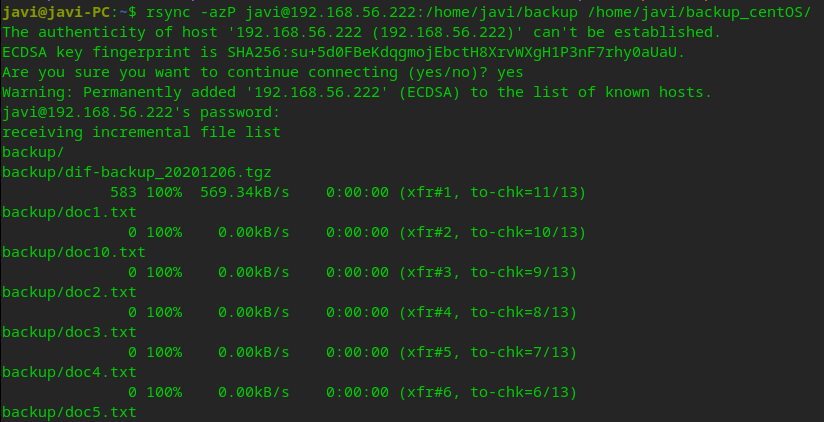
Absoluto: **tar -cpvzf "full-backup\_`date +%Y%m%d`.tgz" /home/javi/backup/**

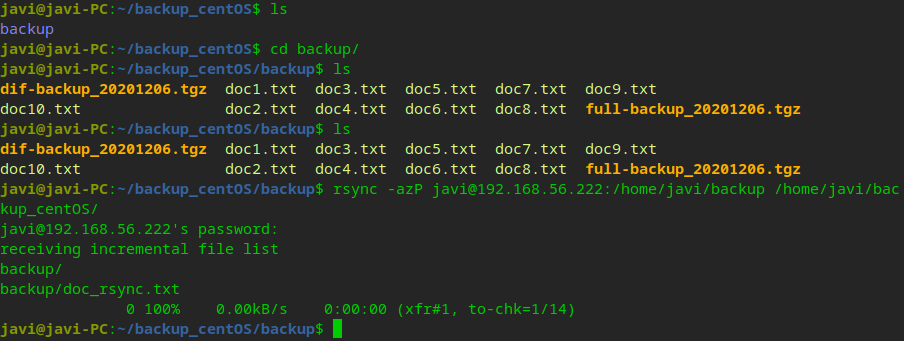


Diferencial: **tar -cpvzf "dif-backup\_`date +%Y%m%d`.tgz" /home/javi/backup/ -N 6-dec-20**



Sincronización: **rsync -azP** [**javi@192.168.56.222:/home/javi/backup /home/javi/backup\_centOS/**](mailto:javi@192.168.56.222:/home/javi/backup%20/home/javi/backup_centOS/)





## 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**](https://download.igniterealtime.org/openfire/openfire-4.6.0-1.x86_64.rpm)

Iniciamos el servicio **systemctl start openfire.**

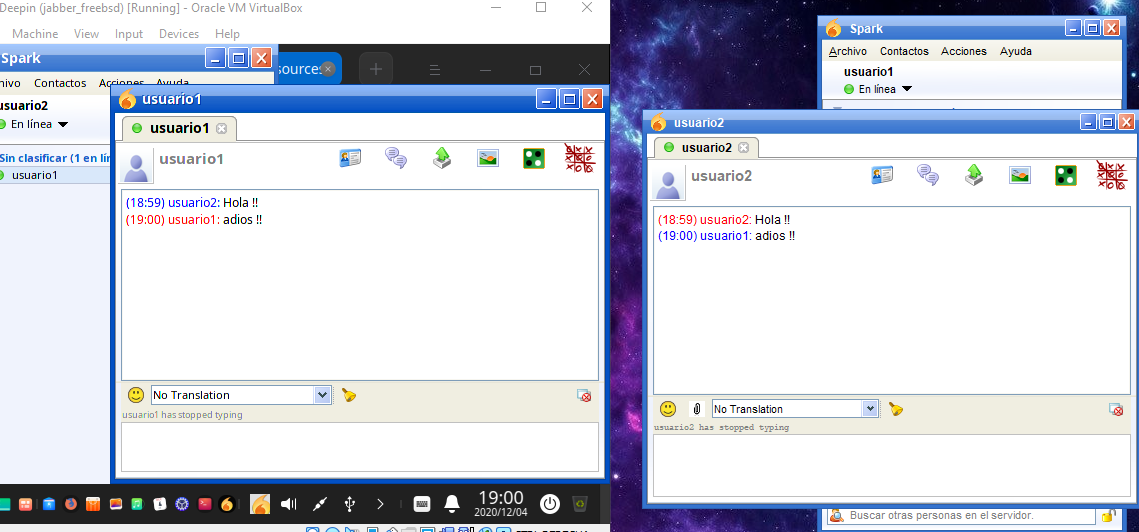
Una vez instalado e iniciado, escribiremos en un navegador web la **IP:9090** para terminar la instalación y posteriormente crear 2 usuarios para comprobar la comunicación entre ambos.

Descargamos un cliente, como Spark:

**dnf install pcp-export-pcp2spark-5.0.2-5.el8.x86\_64**

Y en otra máquina otro cliente.

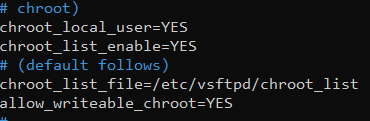
Una vez obtenido los 2 clientes que usaremos para la comunicación de mensajería nos conectamos y ya podemos empezar a conversar de manera instantánea.



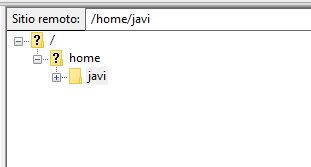
## FTP (vsftpd)

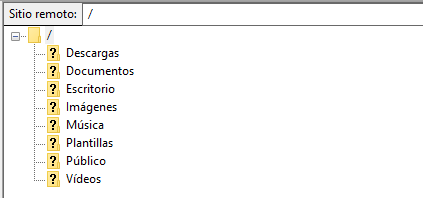
Para instalar vsftpd, nos instalaremos el siguiente paquete: **dnf install vsftpd**

Iniciamos el servicio: **systemctl start vsftpd**

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

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





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.

## VPN

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

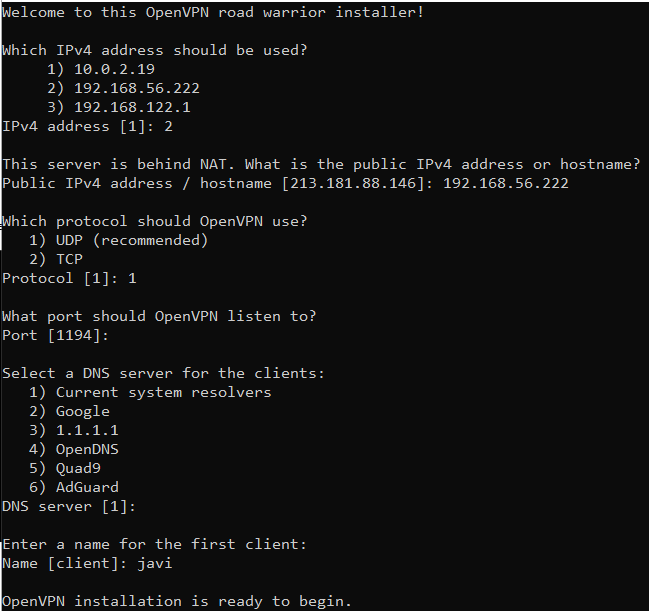
**git clone https://github.com/Nyr/openvpn-install.git**

**cd openvpn-install**

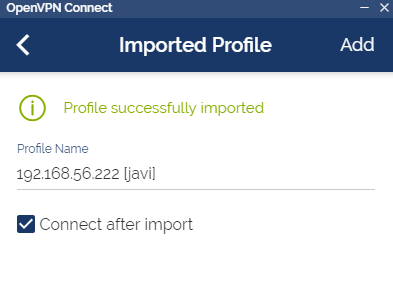
**chmod +x openvpn-install.sh**

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

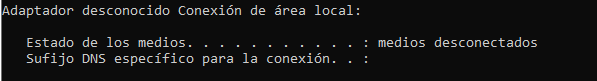
Seguimos los siguientes pasos de instalación:

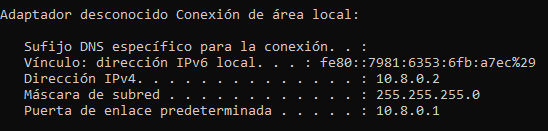


Una vez instalado y configurado, descargaremos el cliente **OpenVPN Connect e** introduciremos el archivo javi.opvn generado en dicho cliente.



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

Sin VPN:

Con VPN:

# Windows Server 2019

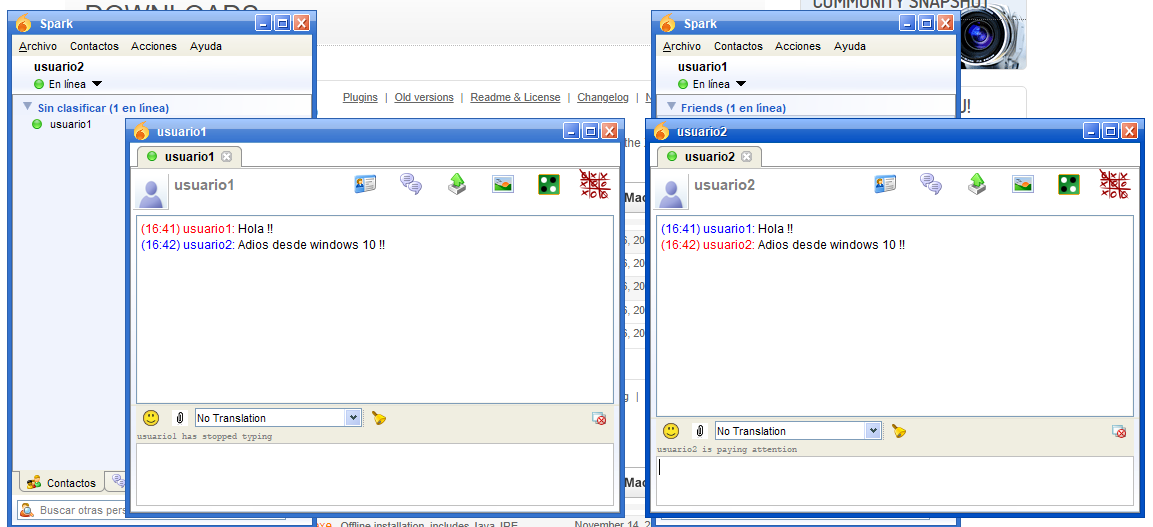
## Mensajería instantánea

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.

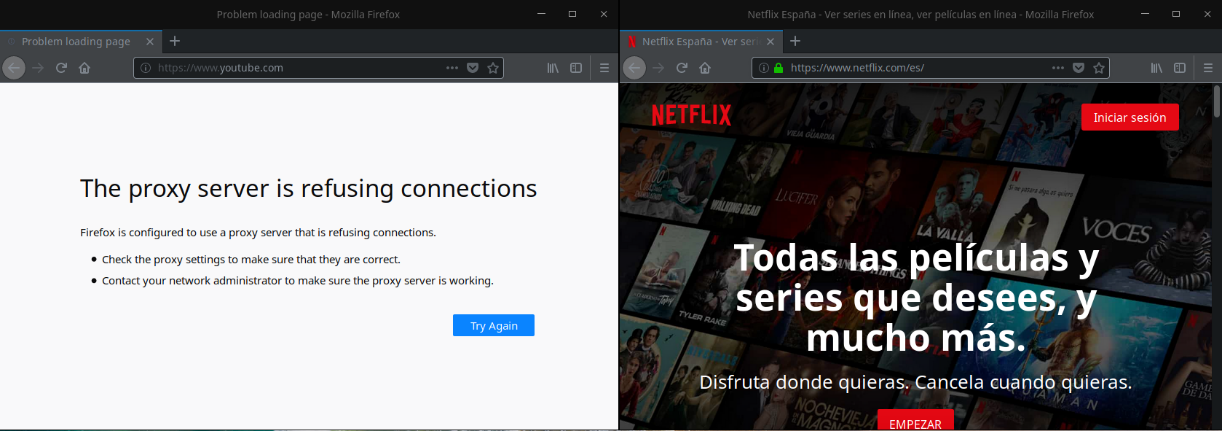


## Proxy

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”.

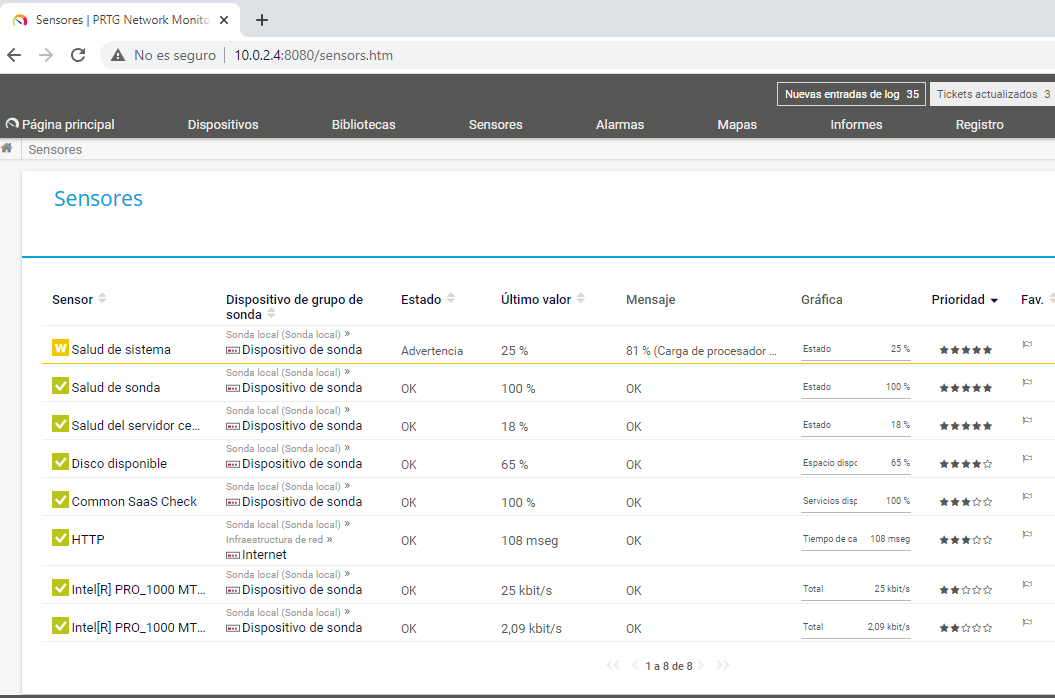


## Monitorización de servicios (PRTG)

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

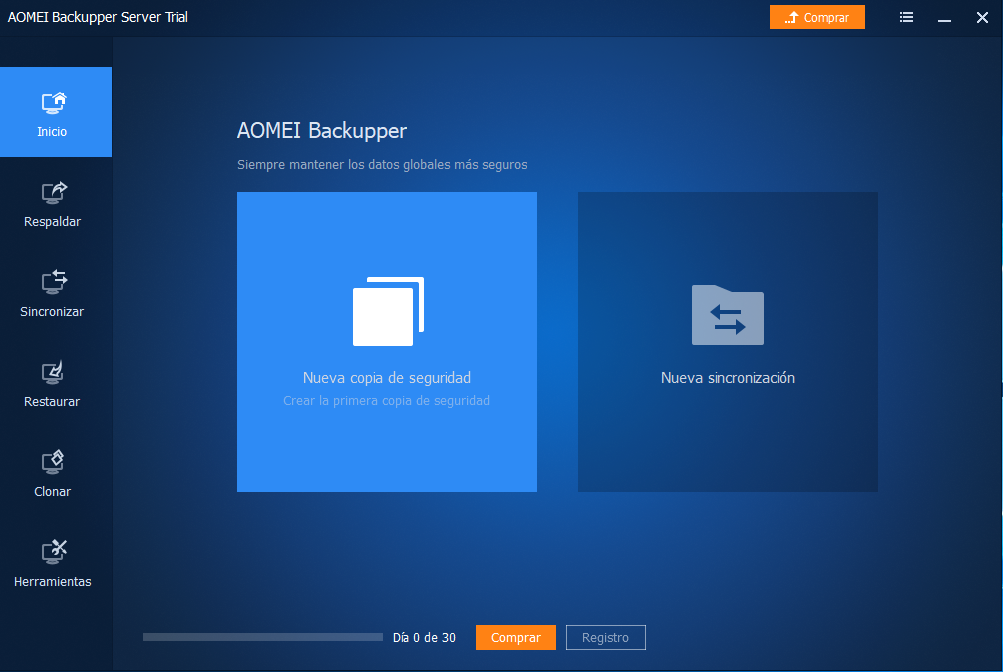
<https://www.es.paessler.com/prtg>

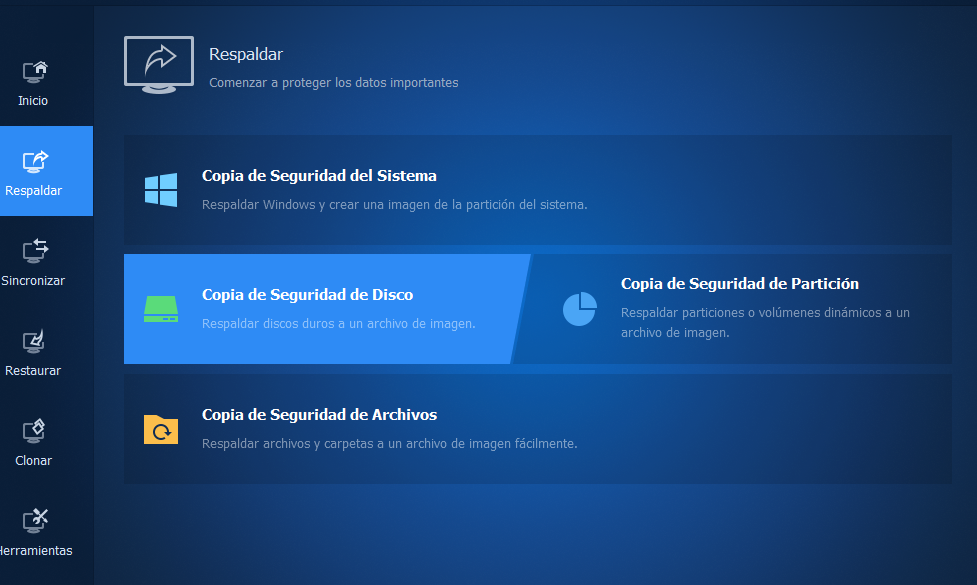
Seguimos los pasos de instalación y nos conectamos desde un navegador web para ver toda la monitorización de nuestros servicios en el sistema: <http://10.0.2.4:8080/>

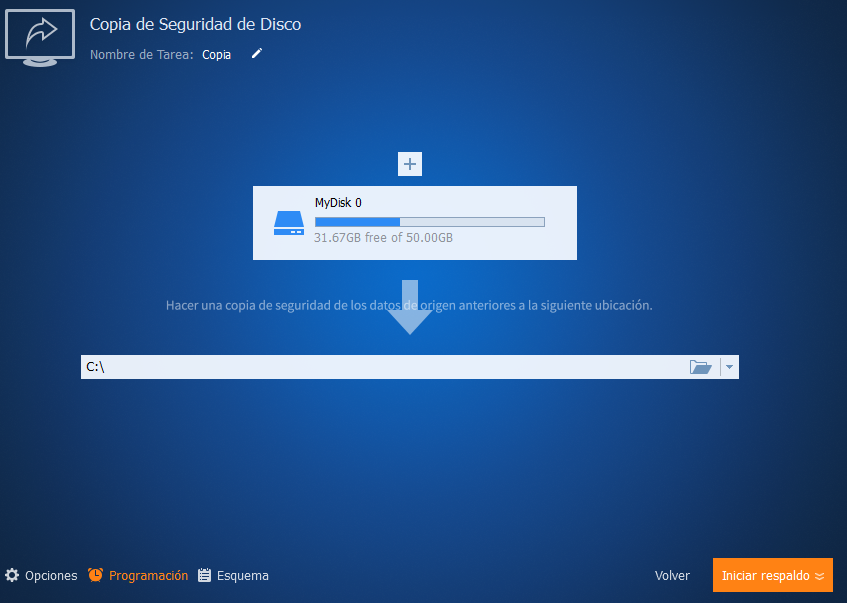


## Backup

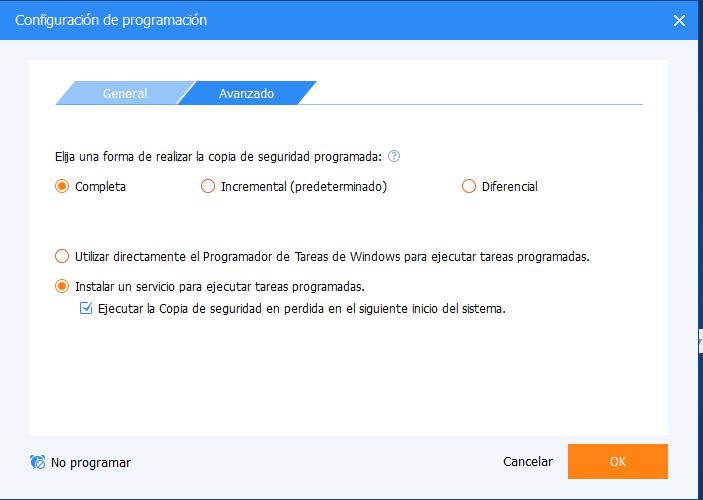
Para realizar los distintos tipos de backups instalaremos el programa AOMEI Backupper.



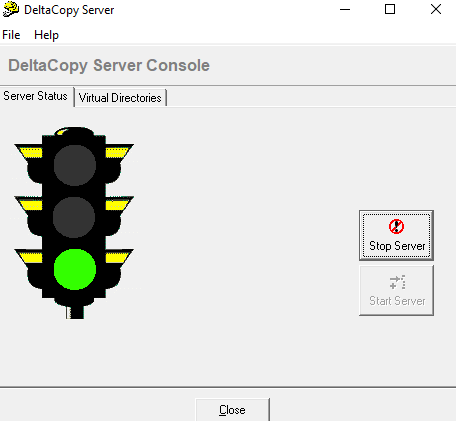


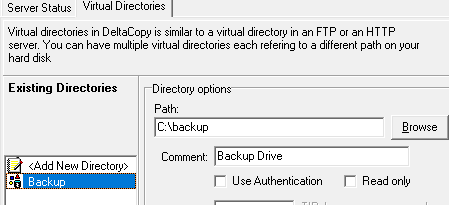


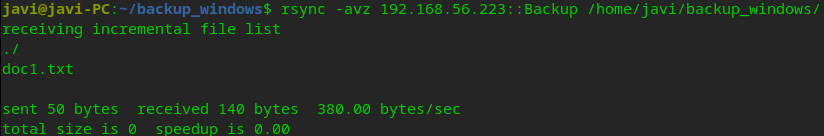
Para realizar los diferentes tipos de backups, una vez añadido el disco, elegimos desde la opción programación, el tipo de backup que deseamos.



Para el backup de sincronización instalaremos el programa DeltaCopy:

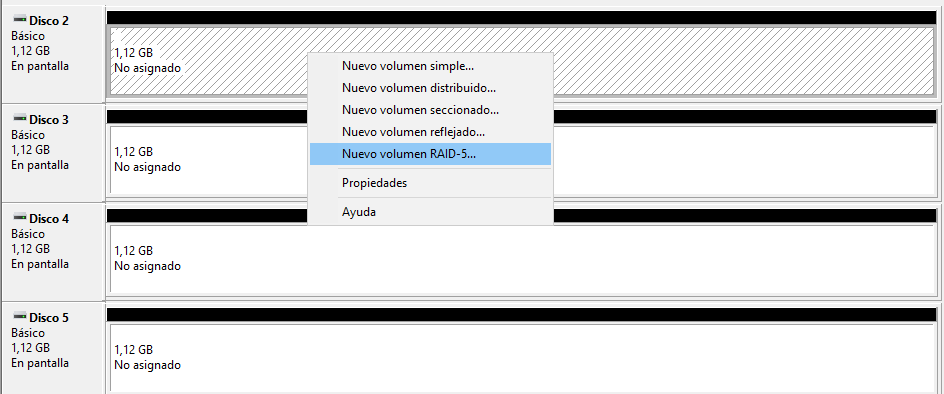




**rsync -avz 192.168.56.223::Backup /home/javi/backup\_windows/**

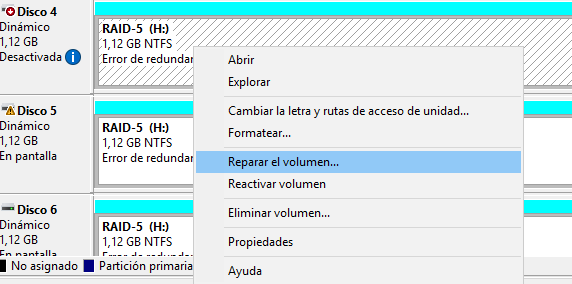
## RAID 5

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.



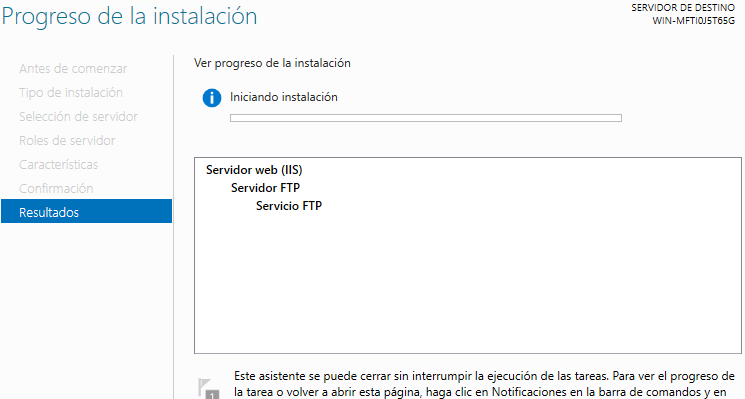


Si provocamos un fallo, podemos hacer clic derecho >> reparar volumen y ya tendríamos nuestro RAID5 funcionado de nuevo correctamente.



## FTP

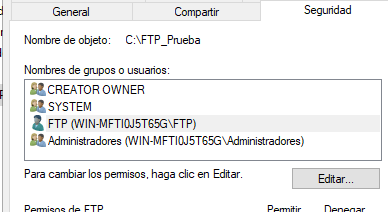
Instalaremos el Servidor FTP desde el Administrador del servidor.



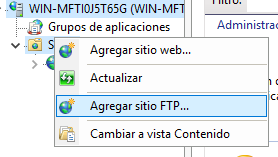
Una vez instalado, creamos un grupo para FTP:

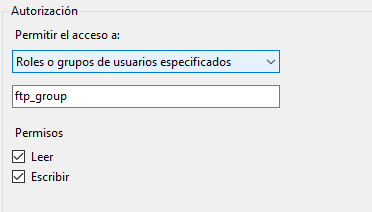


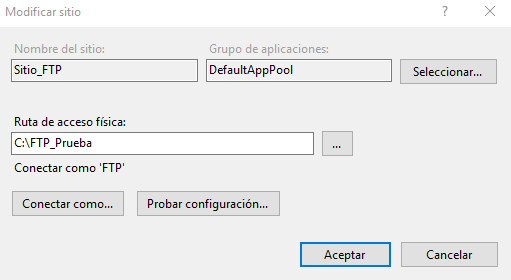
Creamos una carpeta de prueba y en Propiedades >> Seguridad, añadimos para que en esta carpeta solo puede ser accesible desde el usuario creado FTP.

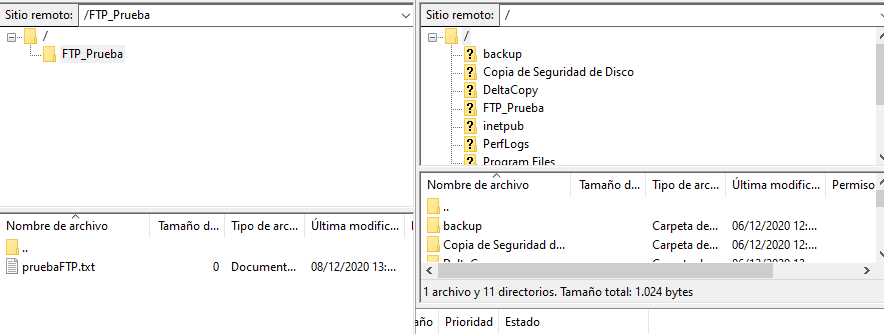


Desde herramientas del Administrador del servidor vamos Administrador de ISS y creamos un sitio FTP.





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.