



UA

Hito3Asorc

DanielAsensiRochDNI : 48776120C

December 13, 2021

Contents

1	Raid 5	2
1.1	Debian	2
1.2	FreeBSD	3
1.3	Windows 10	4
2	Servidor Proxy	6
2.1	Debian	6
2.2	FreeBSD	7
2.3	Windows 10	8
3	Monitorización de Servicios	10
3.1	Debian	10
3.2	FreeBSD	10
3.3	Windows 10	11
4	FTP Server	13
4.1	Debian	13
4.2	FreeBSD	14
4.3	Windows 10	14
5	Mensajería Instantánea	16
5.1	Debian	16
5.2	FreeBSD	16
5.3	Windows 10	17
6	BackUp	19
6.1	Debian	19
6.2	FreeBSD	19
6.3	Windows 10	20
7	Correo Electrónico	22
7.1	Debian	22
7.2	Windows 10	23
8	Firewall, VPN, Enrutado	24
8.1	Freebsd	24
8.2	Windows 10	25

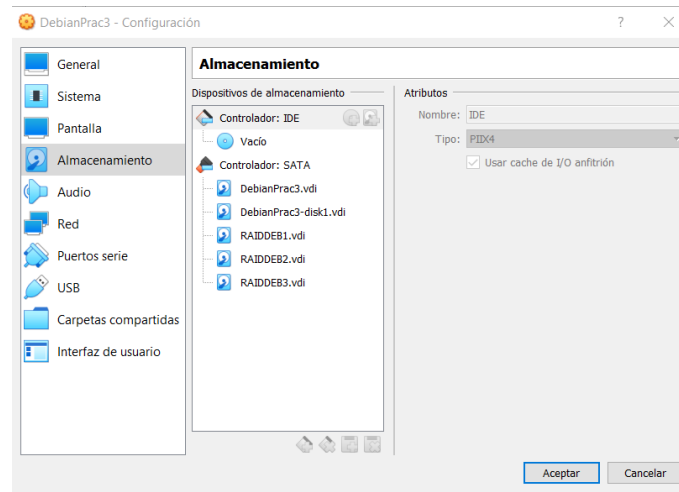
1 Raid 5

1.1 Debian

Para la instalación de un raid en Debian 11 lo primero que deberemos de hacer será la instalación de la herramienta "mdadm":

```
sudo apt-get install mdadm
```

Una vez instalada desde Virtualbox añadiremos los discos duros con los que crearemos el raid5, haciendo que quede de la siguiente manera:

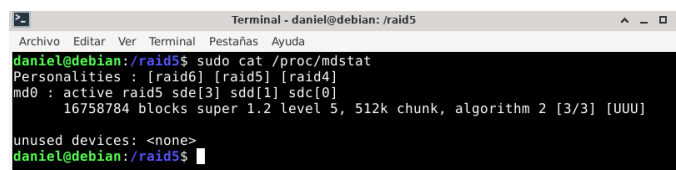


Configuración del disco

Una vez hecho esto inicializaremos todos los bloques de nuestros discos duros a 0 para evitar errores durante la creación del raid, y luego lo inicializaremos:

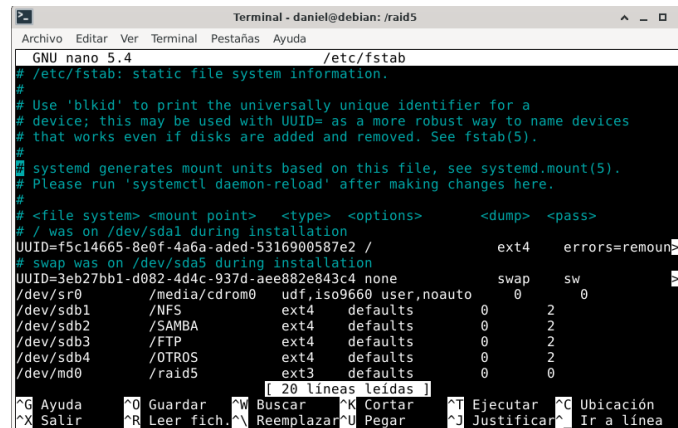
```
mdadm --zero-superblock /dev/sdc /dev/sdd /dev/sde
```

```
mdadm -C /dev/md127 --level=raid5 --raid-devices=3 /dev/sdc /dev/sdd /dev/sde
```



Raid Funcionando

Una vez hecho esto montaremos el disco en una carpeta para poder añadir archivos y comprobar que todo funciona dejando /etc/fstab así:



Edición de Fstab

Para comprobar que nuestro Raid funciona lo que haremos es desconectar un disco del raid y comprobaremos que se puede todavía acceder a la carpeta:

```
sudo mdadm /dev/md127 --fail /dev/sde --remove /dev/sde
```

Comprobamos el raid:

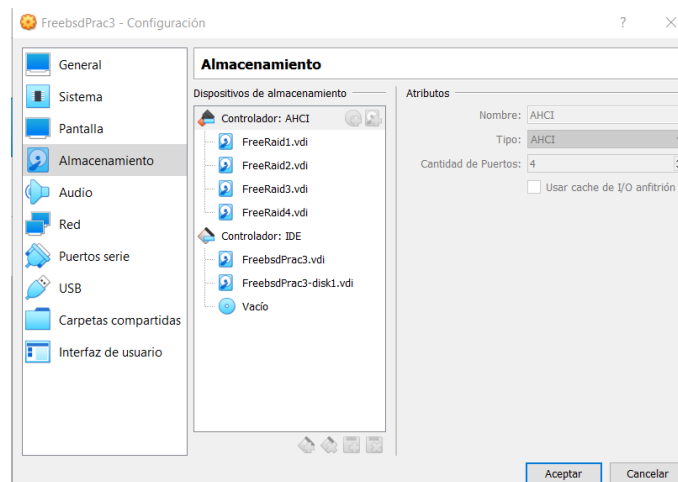
```
sudo cat /proc/mdstat
```

Para volver a montar el disco:

```
sudo mdadm /dev/md127 -a /dev/sde
```

1.2 FreeBSD

Para realizar un raid5 en FreeBSD lo primero que deberemos de hacer será añadir los discos a Virtualbox haciendo que quede de la siguiente manera:



Discos añadidos

Una vez hecho esto escribiremos el siguiente comando para comprobar cuales son nuestros discos:

```
geom disk list
```

Una vez comprobados los añadimos al raid

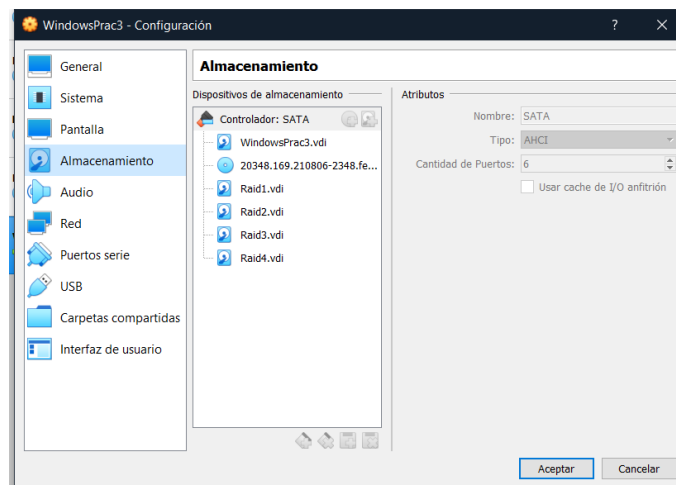
```
gvinum raid5 -n r5 /dev/ada2 /dev/ada3 /dev/ada4 /dev/ada5  
  
newfs /dev/gvinum/r5  
  
mkdir /RAID5  
  
mount /dev/gvinum/r5 /RAID5
```

Para hacer las pruebas de desconexión y conexión solo deberemos realizar lo siguiente:

```
gvinum setstate -f down r5.p0.s3  
  
gvinum l  
  
gvinum setstate -f up r5.p0.s3
```

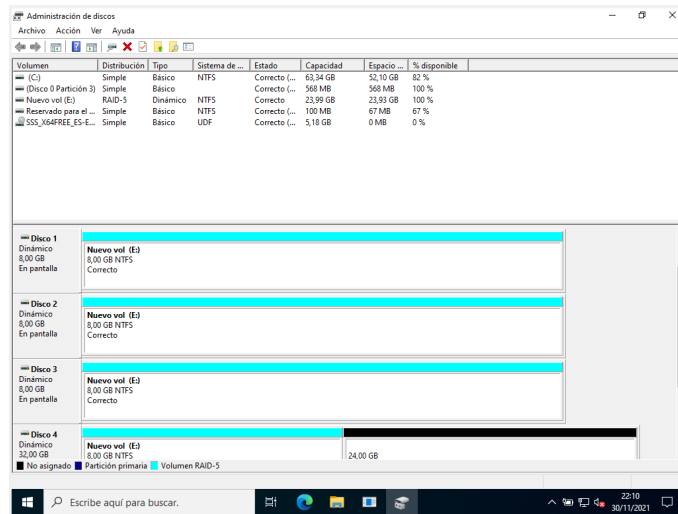
1.3 Windows 10

Para instalar el servicio de Raid 5 lo realizaremos de manera sencilla, lo primero que haremos será añadir a VBox los discos duros necesarios, de manera que quede tal que así.



Configuración del disco

Una vez hecho esto accederemos a la herramienta de "Administración de discos" esta vendrá ya instalada en Windows 10, clicaremos encima de uno de los discos duros y le daremos a la opción de Raid 5, seleccionaremos todos los discos que deseemos, en mi caso los 4 que he añadido y aceptamos de tal manera que quedará así:



Configuración del disco

2 Servidor Proxy

2.1 Debian

Para la instalación de este servicio utilizaremos Squid para ello primero lo instalaremos de la siguiente manera:

```
sudo apt install squid
```

Una vez instalado nos moveremos a su directorio y haremos lo siguiente:

```
cd /etc/squid
```

```
sudo nano paginas
<paginas que deseamos restringir>
www.twitter.com
www.instagram.com
```

Una vez hecho esto accederemos a su configuración base alojada en el fichero `/etc/squid/squid.conf` y agregaremos las siguientes líneas debajo del texto que pone "INSERT YOUR OWN RULES HERE TO ALLOW ACCESS FROM YOUR CLIENTS":

```
acl paginas url_regex "etc/squid/paginas"
http_access deny paginas
```

Modificamos:

```
http_access deny all -> http_access deny paginas
```

Para probarlos desde el cliente realizamos lo siguiente:

Proxy

Usa un servidor proxy para conexiones Ethernet o Wi-Fi. Esta configuración no se aplica a conexiones VPN.

Usar servidor proxy

☒ Activado

Dirección: 192.168.56.224 Puerto: 3128

Usar el servidor proxy excepto para direcciones que empiecen con las siguientes entradas. Usa el punto y coma (;) para separar las entradas.

☐ No usar el servidor proxy para direcciones locales (intranet)

Guardar

Configuración cliente

Una vez hecho esto comprobamos que no podemos acceder a una de las páginas restringidas en este caso Twitter:



Configuración cliente

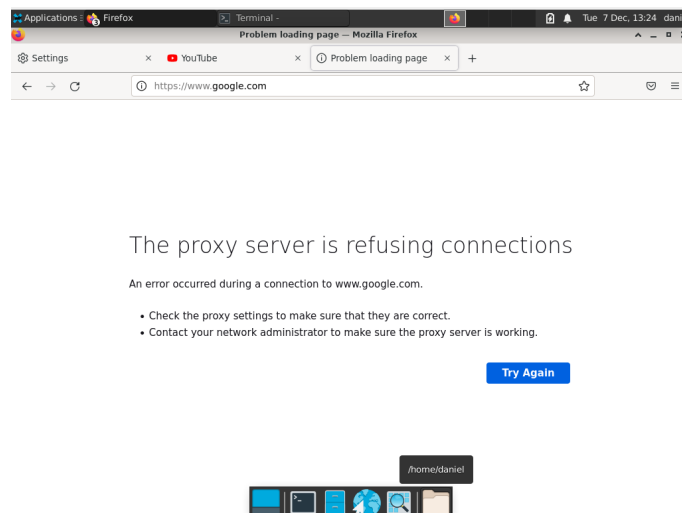
2.2 FreeBSD

Para el proxy utilizaremos Squid, lo que deberemos hacer es instalarlo y configurarlo, ya que en Debian he hecho que bloquee unas páginas en concreto ahora haremos que bloquee todas las páginas menos unas en concreto, para ello haremos lo siguiente:

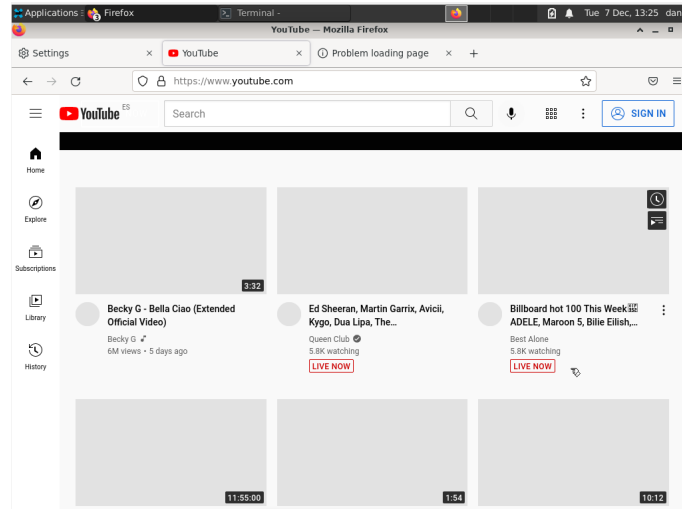
```
sudo pkg install squid
nano /usr/local/etc/squid/squid.conf
sysrc visible_hostname=yes
sysrc squid_enable=yes
```

Añadimos:

```
acl sitios dstdomain www.youtube.com www.instagram.com
http_access deny all !sitios
visible_hostname DanielServidorFree
```



Página bloqueada



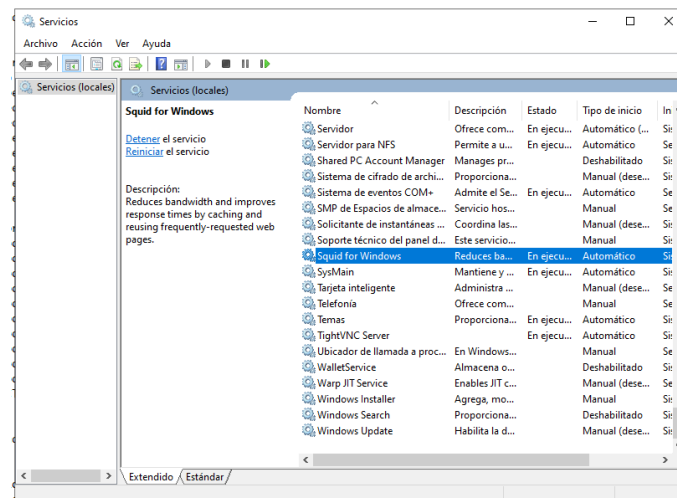
Pagina no bloqueada

2.3 Windows 10

Para el servidor Proxy de Windows 10 utilizaré la herramienta de Squid, para ello la descargaremos desde su página oficial y la instalaremos como si de un programa más se tratara:

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

Una vez instalado comprobaremos en nuestros servicios de windows que este se encuentra operativo y corriendo:



Servicio Corriendo

Una vez hecho esto accederemos al archivo de configuración de Squid que se encuentra en el directorio que pusimos durante su instalación y añadiremos las siguientes líneas para bloquear los sitios web que deseemos, además de crear el archivo deny.sites quedando de la siguiente manera:

- acl Marca url_regex marca
- http_access deny Marca

En el cliente accederemos a su configuración de proxy y añadiremos lo siguiente:

Proxy

Configuración manual del proxy

Usa un servidor proxy para conexiones Ethernet o Wi-Fi. Esta configuración no se aplica a conexiones VPN.

Usar servidor proxy

☒ Activado

Dirección

192.168.56.226

Puerto

3128

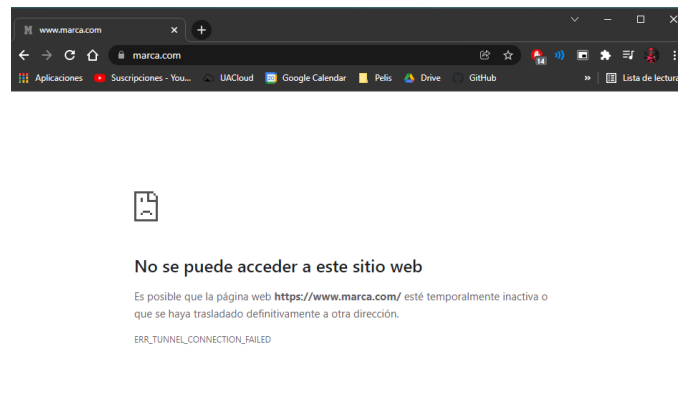
Usar el servidor proxy excepto para direcciones que empiecen con las siguientes entradas. Usa el punto y coma (;) para separar las entradas.

☐ No usar el servidor proxy para direcciones locales (intranet)

Guardar

Configuración en el cliente

Probamos el proxy y obtenemos lo siguiente:



Página bloqueada

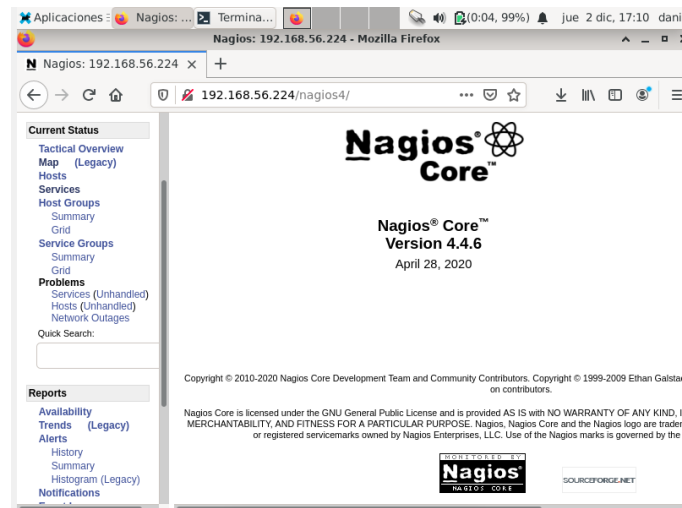
3 Monitorización de Servicios

3.1 Debian

Para la monitorización de servicios en Debian utilizaremos la herramienta de Nagios que se encuentra en su versión 4 para ello utilizaremos los siguientes pasos de instalación:

```
apt install nagios4 nagios-plugins-*  
apt install nagios-nrpe-plugins  
service start nagios4
```

Para acceder a nuestro monitoreo de servicios lo único que deberemos es acceder a nuestro navegador y obtendremos lo siguiente:



Nagios

3.2 FreeBSD

Para la monitorización de servicios en FreeBSD he utilizado al igual que en Debian el servicio de Nagios para utilizar este debemos tener instalado previamente Apache24 y configurado de antemano:

```
pkg install nagios  
sysrc nagios_enable=yes
```

```
cd /usr/local/etc/nagios/  
cp cgi.cfg-sample cgi.cfg  
cp nagios.cfg-sample nagios.cfg  
cp resource.cfg-sample resource.cfg
```

```
cd objects/
```

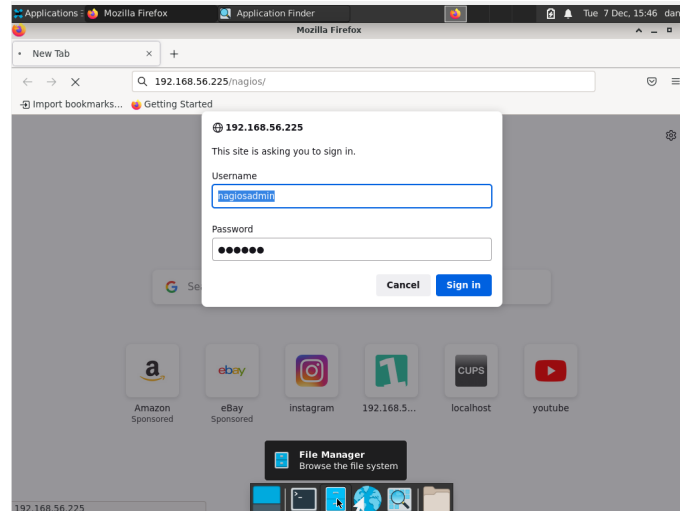
Realizamos las copias de todos los ficheros al igual que antes

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

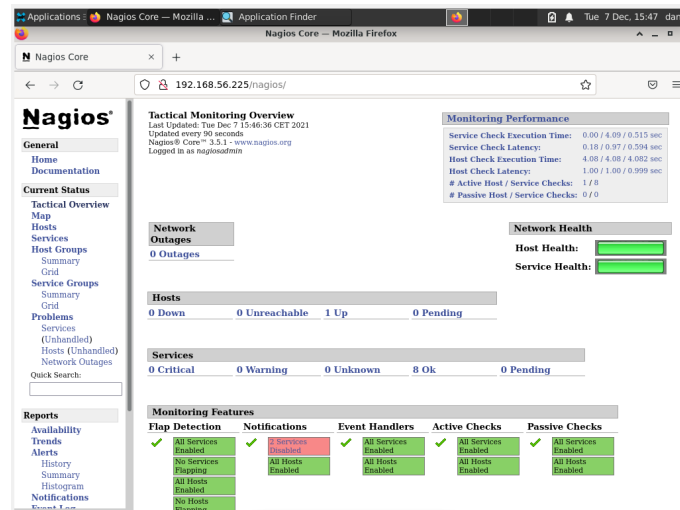
Añadimos toda la configuración de nagios a apache24

```
nano /usr.local/etc/apache24/httpd.conf
```

```
service nagios start  
service apache24 restart
```



Nagios



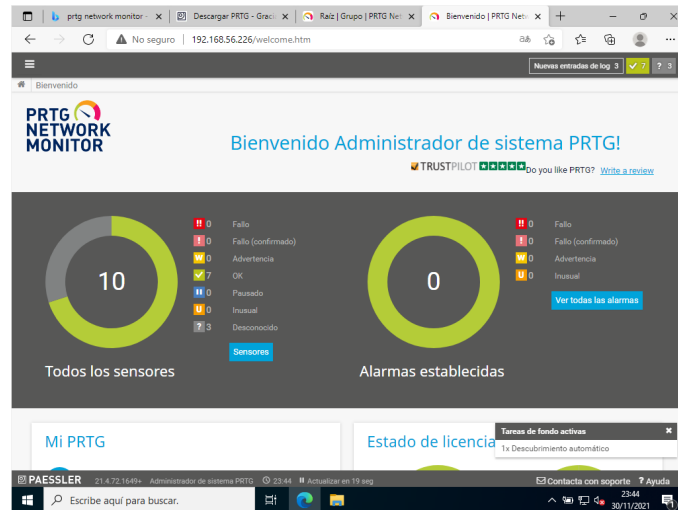
Nagios

3.3 Windows 10

Descargamos PRTG Network Monitor desde su página oficial, lo instalaremos como su fuera un programa convencional, una vez hecho esto accederemos desde el cliente utilizando:

<https://192.168.56.226:443>

Obtendremos la siguiente salida, donde podremos apreciar todos los servicios:



Pagina bloqueada

Link de descarga:

https://www.paessler.com/prtg?gclid=Cj0KCQiAtJeNBhCVARIsANJUJ2HY2pvlHPyTB8hfMjByOPmwpKsXQp035gNj69Yl0mlehwcYvYSm4_IaApT_EALw_wcB

4 FTP Server

4.1 Debian

Para la instalación del servicio FTP utilizaremos la herramienta vsftpd para ello seguiremos los siguientes pasos:

```
sudo apt-get install vsftpd
sudo nano /etc/vsftpd.conf
```

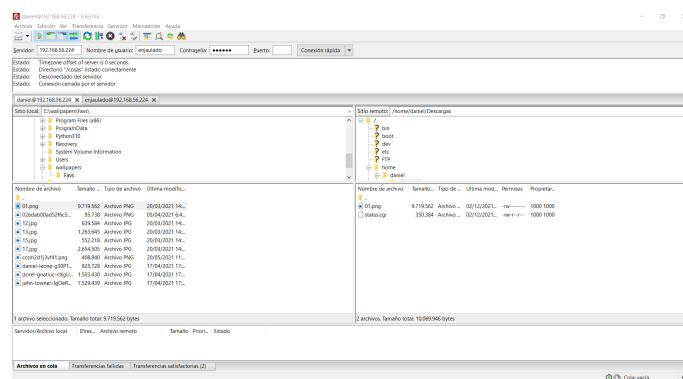
Escribimos la siguiente configuración:

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

Añadimos los usuarios que no estarán enjaulados al archivo `/etc/vsftpd.chroot_list`:

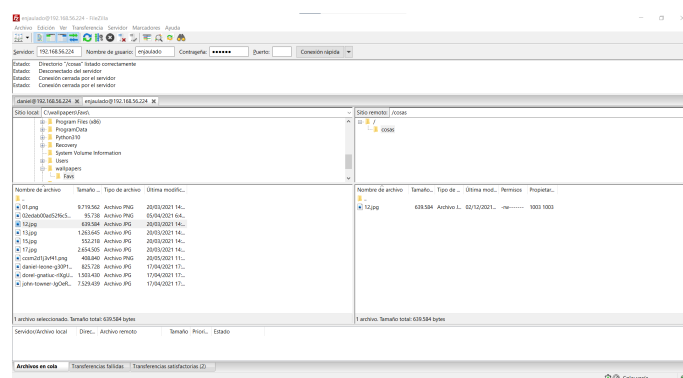
```
sudo nano /etc/vsftpd.chroot_list
daniel
```

El usuario que no esta enjaulado en este caso "daniel" puede acceder a la raíz:



FTP Desde el cliente Filezilla no enjaulado

Mientras que el enjaulado no puede acceder:



FTP Desde el cliente Filezilla enjaulado

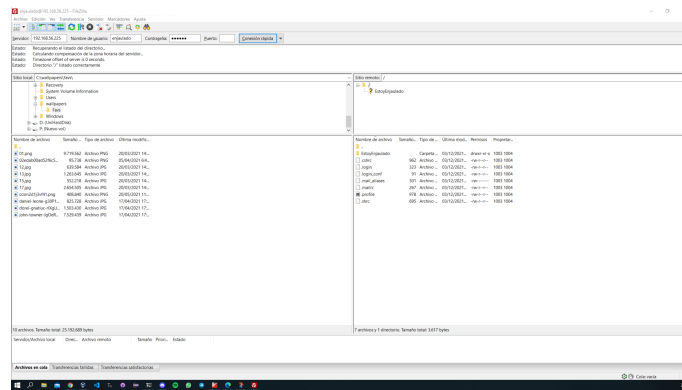
4.2 FreeBSD

Para la instalación de FTP en freebsd utilizaremos el servicio que viene instalado de serie "ftpd" lo unico que deberemos hacer será habilitarlo desde el lanzamiento y luego inicializarlo:

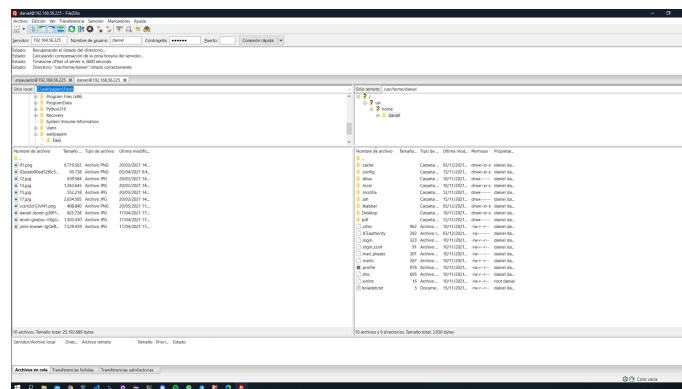
```
sysrc ftpd_enable=yes
/etc/rc.d/ftpd start
```

Luego modificaremos el archivo ftpdchroot para administrar los usuarios que tienen acceso a la carpeta raíz, en mi caso será solo "daniel" y "enjaulado" no podrá acceder a la raíz por lo que lo añadiremos al archivo:

```
nano rc.d/ftpdchroot
enjaulado
```



FTP Desde el cliente Filezilla enjaulado



FTP Desde el cliente Filezilla no enjaulado

4.3 Windows 10

Para la instalación de FTP server en Windows 10 seguiremos los siguientes pasos:

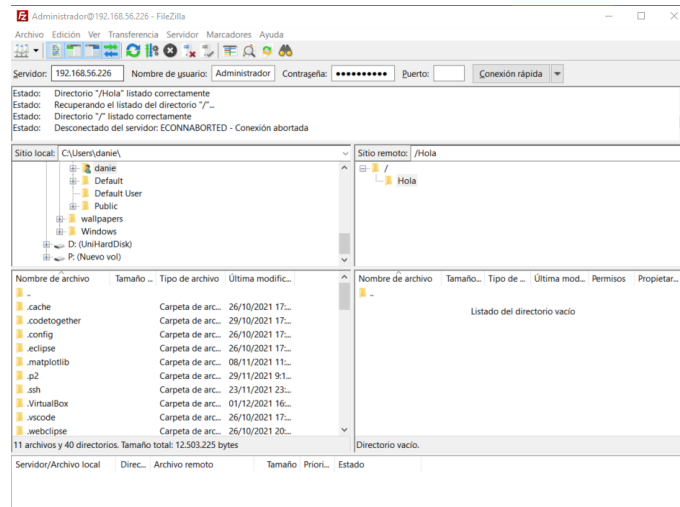
1. Instalar roles de ISS en Windows Server
2. Dentro de este instalar el servicio de FTP
3. Crearemos una carpeta donde enjaularemos al usuario
4. Entramos a "Administrador de Internet Information Services IIS"
5. Generamos un nuevo sitio y le ponemos un nombre y seleccionamos la carpeta creada
6. Seleccionamos la ip de internet en mi caso 192.168.56.226 y sin ssl

7. Le damos todos los permisos y seleccionamos un usuario en mi caso "Administrador"

Ahora lo que haremos será mostrar esta carpeta a todos aquellos usuarios que se logguen con las credenciales del Administrador para ello:

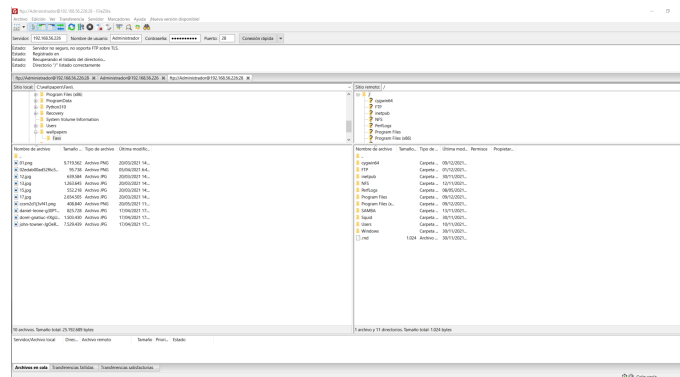
1. Iremos a "Este Equipo" click derecho "Conectar a unidad de red"
2. Y en dirección de red: "ftp://192.168.56.226"
3. Quitamos el inicio de sesión anónima y ponemos el usuario, asignamos el nombre Administradorftp

Ahora desde el cliente para probarlo usará Filezilla en enjaulado se encuentra en el puerto 21:



FTP Desde el cliente Filezilla

Ahora probaremos el cliente sin enjaular se encuentra en el puerto 28:

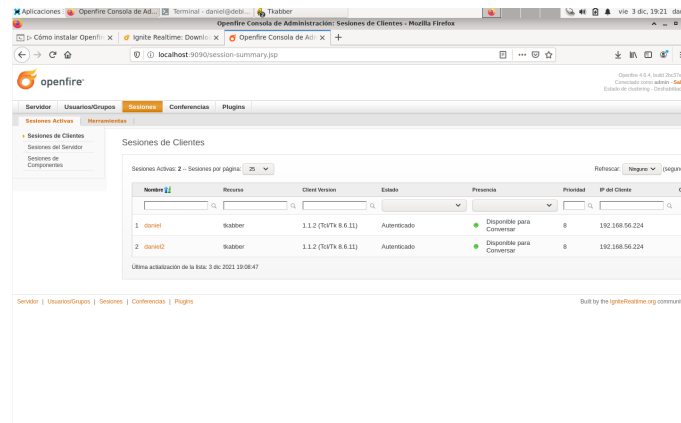


FTP Desde el cliente Filezilla

5 Mensajería Instantánea

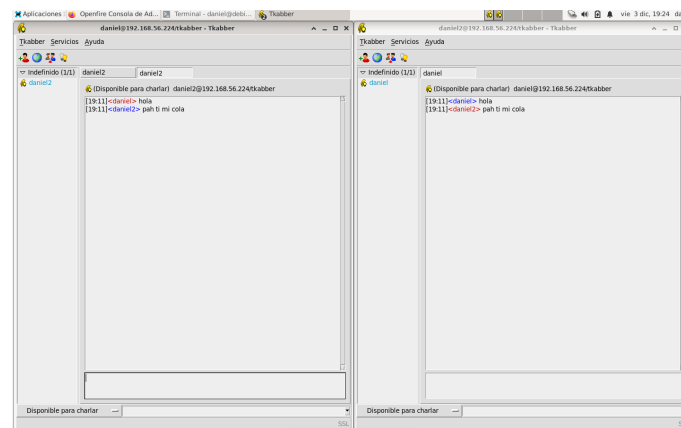
5.1 Debian

Al igual que en Windows 10 utilizaremos las herramientas de Openfire y Tkabber, para instalarlas iremos a sus páginas oficiales y las instalaremos mediante la línea de comandos, una vez instaladas iremos a la configuración de Openfire que se encuentra en el navegador en la url 192.168.56.224:9090.



Configuración Openfire

En Tkabber añadiremos los usuarios y los suscribiremos mutuamente, hecho podrán comenzar a conversar:



Tkabber Clientes conversando

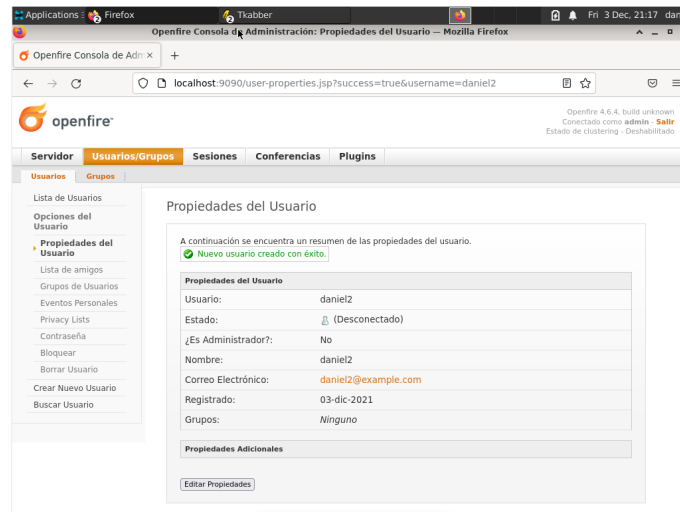
Si tras la instalación Openfire no ha iniciado hacer lo siguiente:

```
sudo apt install aptitude
sudo aptitude install openjdk-17-jre
sudo systemctl start openfire
```

5.2 FreeBSD

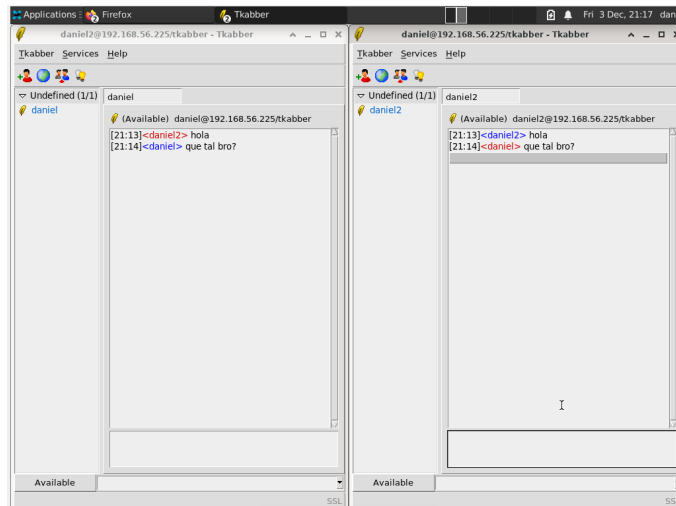
Al igual que en Windows 10 utilizaremos las herramientas de Openfire y Tkabber, las instalaremos mediante la línea de comandos, una vez instaladas iremos a la configuración de Openfire que se encuentra en el navegador en la url 192.168.56.225:9090.

```
sudo pkg install openfire
sudo sysrc openfire_enable=yes
sudo pkg install tkabber
sudo service openfire start
```



Openfire Funcionando y configurado con usuarios

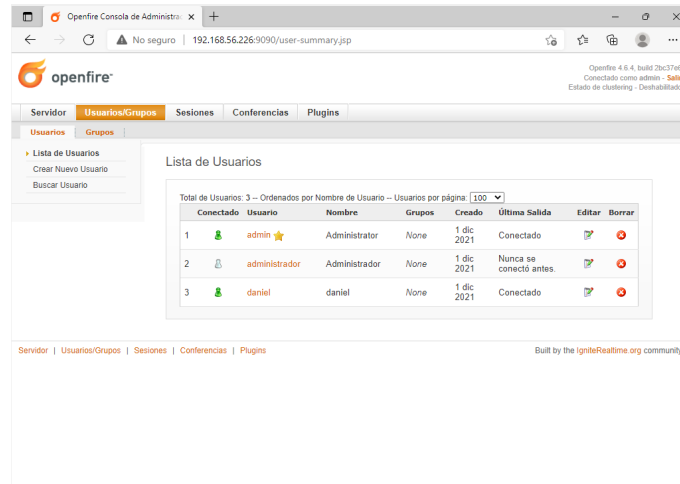
En tkabber añadimos los clientes y los ponemos a conversar



Tkabber Clientes conversando

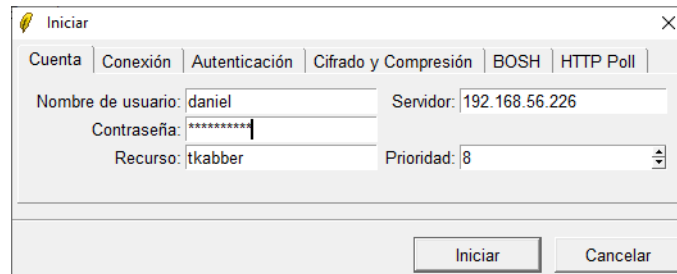
5.3 Windows 10

Para la instalación de la mensajería instantánea utilizaremos Openfire y como cliente TKabber, previo a esto necesitaremos instalar Java y Java Jdk, todos los instaladores se instalarán dando a siguiente hasta que se complete la instalación, una vez realizada añadiremos unos nuevos usuarios a Openfire:



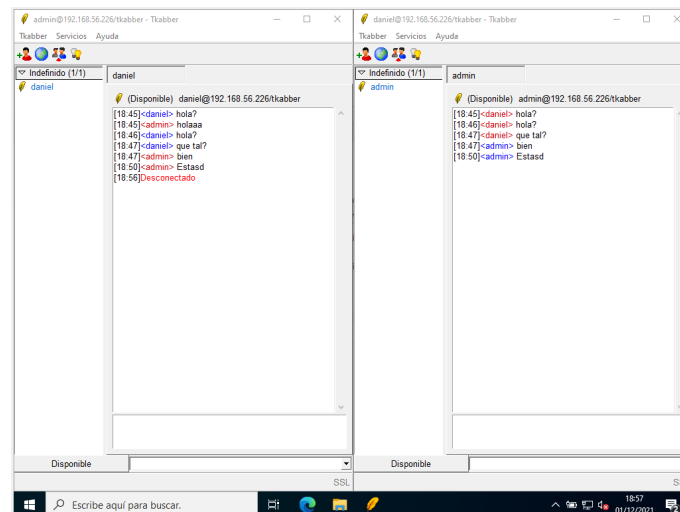
Creación de usuarios

Hecho esto iniciaremos sesión con nuestro cliente de Tkabber en las cuentas que hayamos creado de la siguiente manera:



Inicio de sesión desde Tkabber

Y podremos comenzar a chatear:



Conversación

Nota: Tardan un poquito en conectarse :)

6 BackUp

6.1 Debian

Debian cuenta con sus propias herramientas para la realización de Backups: Backup Absoluto: Ignora los archivos que hay en el directorio y los copia de nuevo.

Incremental: `rsync -av origen destino` – Si ya hay algún archivo dentro con el mismo nombre, no lo vuelve a cambiar de cero si no que solo cambia lo nuevo.

Sincronización: `rsync -av origen destino` – Si modificamos un archivo en el destino y después volvemos a ejecutar el `rsync`, ese archivo será reemplazado por el existente en el directorio de origen.

```
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h dom mon dow   command
* * * * * /bin/bash      /home/daniel/backups/backup.sh -a > /dev/null
* * * * * /bin/bash      /home/daniel/backups/backup.sh -d > /dev/null
```

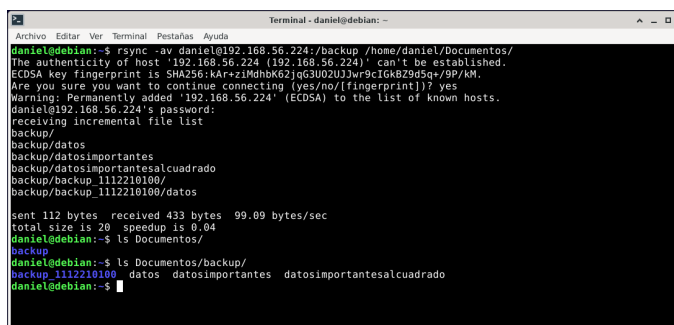
Sincronización

```
#!/bin/bash
BACKUP_FILE_NAME_ABS='_Abs'
BACKUP_FILE_NAME_DIFF='_Diff'
DIR='/home/daniel/Documentos/'
. ~/.bashrc
if [ $1 = "-d" ]; then
    echo 'copia diferencial';
    DATE=`date -d "last sat" +%Y%m%d`
    ADD_TO_TAR='-N '$DATE
    TYPE=$BACKUP_FILE_NAME_DIFF;
else
    echo 'copia absoluta'
    DATE=''
    ADD_TO_TAR=''
    TYPE=$BACKUP_FILE_NAME_ABS;
fi
tar -cpvzf $DATE'_backup'$TYPE $DIR $ADD_TO_TAR
```

Script

El backup remoto nos permitirá extraer información de una carpeta de backup remota

`rsync -av daniel@192.168.56.224:/backup /home/daniel/Documentos`



```
Terminal - daniel@debian: ~
daniel@debian:~$ rsync -av daniel@192.168.56.224:/backup /home/daniel/Documentos/
The authenticity of host '192.168.56.224 (192.168.56.224)' can't be established.
ECDSA key fingerprint is SHA256:kAr+ziMhnbK62jG3U02UJw99cIGK8Z9d5q+/9P/KM.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.56.224' (ECDSA) to the list of known hosts.
daniel@192.168.56.224's password:
receiving incremental file list
backup/
backup/datos
backup/datosimportantes
backup/datosimportantesalcuadrado
backup/backup_1112210100/
backup/backup_1112210100/datos

sent 112 bytes  received 433 bytes  99.09 bytes/sec
total size is 20  speedup is 0.04
daniel@debian:~$ ls Documents/
backup
daniel@debian:~$ ls Documents/backup/
backup_1112210100  datos  datosimportantes  datosimportantesalcuadrado
daniel@debian:~$
```

Sincronización remota

6.2 FreeBSD

FreeBSD cuenta con sus propias herramientas para la realización de Backups: Backup Absoluto: Ignora los archivos que hay en el directorio y los copia de nuevo. Incremental: `rsync -av origen destino` – Si ya hay algún archivo dentro con el mismo nombre, no lo vuelve a cambiar de cero si no que solo cambia lo nuevo.

```

    #!/bin/bash
    # backup file name of the absolute copy:
    BACKUP_FILE_NAME_ABS='_Abs'
    # backup file name of the differential copy:
    BACKUP_FILE_NAME_DIFF='_Diff'
    # Name of the directory to have the backup
    DIR='/home/daniel/Documentos'
    # Begin the script
    #
    . ~/.bash_profile
    if [ $1 == "-d" ];then
        echo 'copia diferencial';
        DATE='date +%Y%m%d'
        ADD_TO_TAR='-N '$DATE
        TYPE=$BACKUP_FILE_NAME_DIFF;
    else
        echo 'copia absoluta'
        DATE=''
        ADD_TO_TAR=''
        TYPE=$BACKUP_FILE_NAME_ABS;
    fi

    tar -cpvzf $DATE'_backup'$TYPE $DIR $ADD_TO_TAR

```

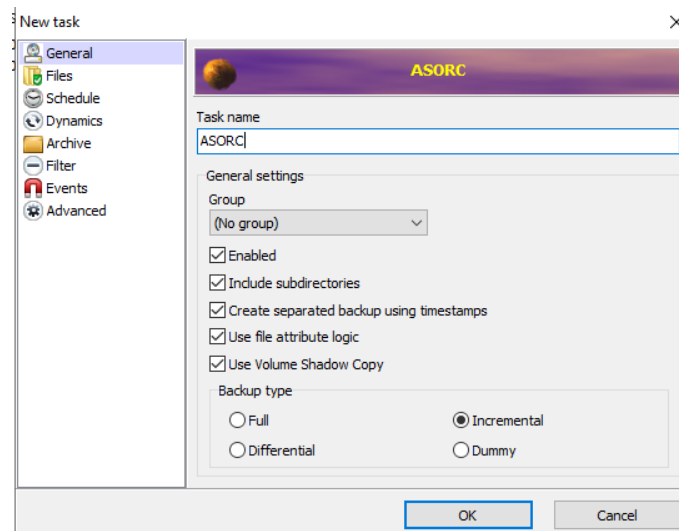
El backup remoto nos permitirá extraer información de una carpeta de backup remota

```
rsync -av daniel@192.168.56.225:/backup /home/daniel/Documentos
```

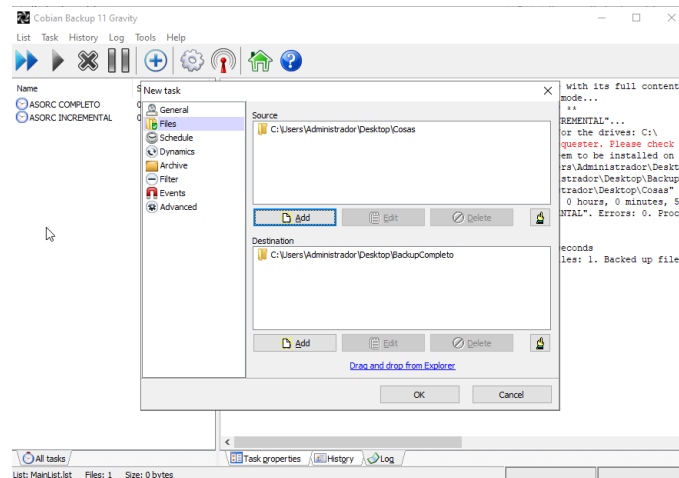
6.3 Windows 10

Para la realización de Backup en windows 10 utilizaremos la herramienta de Cobian Backup y Cgwing para la parte de rsync, instalaremos ambas herramientas desde sus páginas oficiales.

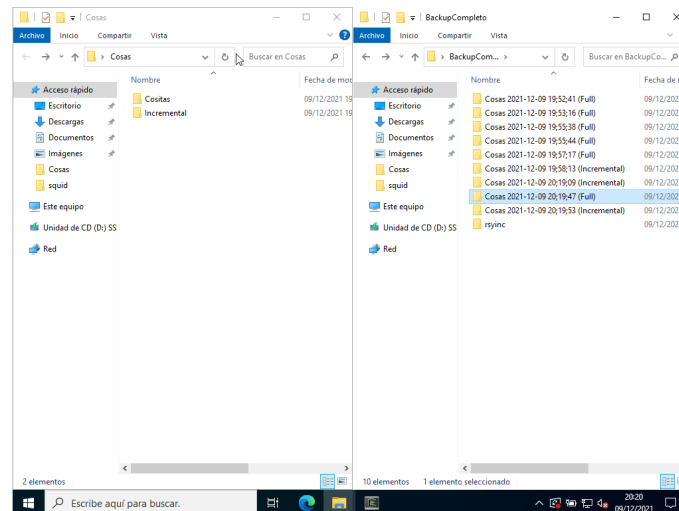
Para la realización de los backup completo y incremental seguiremos los siguientes pasos:



Inicializando Backup

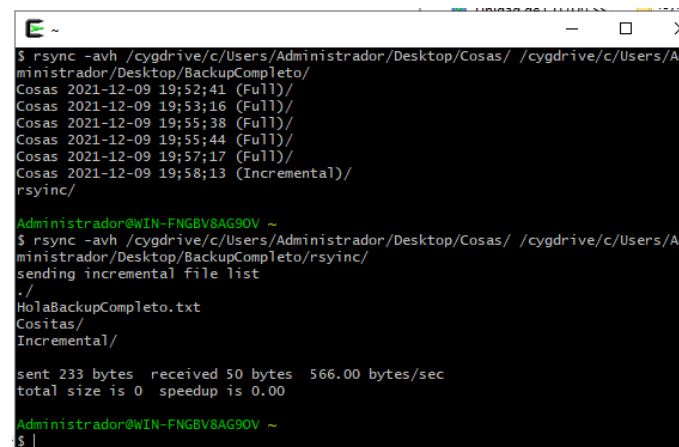


Iniciando Backup



Viendo Backup

Para hacer el backup desde rsync:



Iniciando Backup

```
rsync -avh /cygdrive/Users/Administrador/Desktop/Cosas
/cygdrive/Users/Administrador/Desktop/BackupCompleto/rsync/
```

7 Correo Electrónico

7.1 Debian

Para la instalación del servidor de correo utilizaremos postfix y como cliente squirrel para la instalación y configuración de postfix seguiremos los siguientes pasos:

```
apt-get install postfix
apt-get install mailutils
```

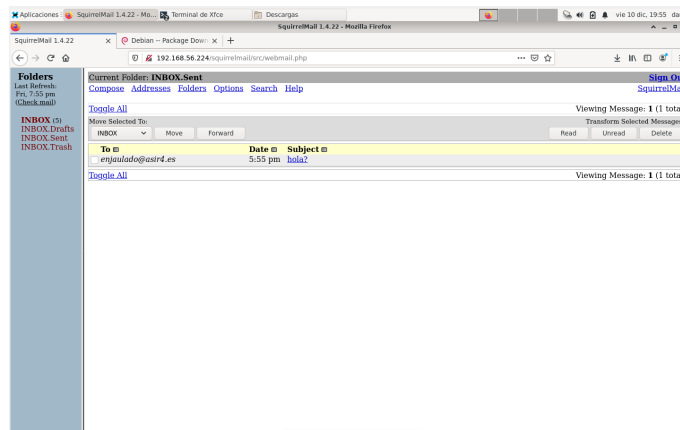
Configuraremos nuestro host:

```
nano /etc/hosts
192.168.56.224 debian.asir4.es debian
```

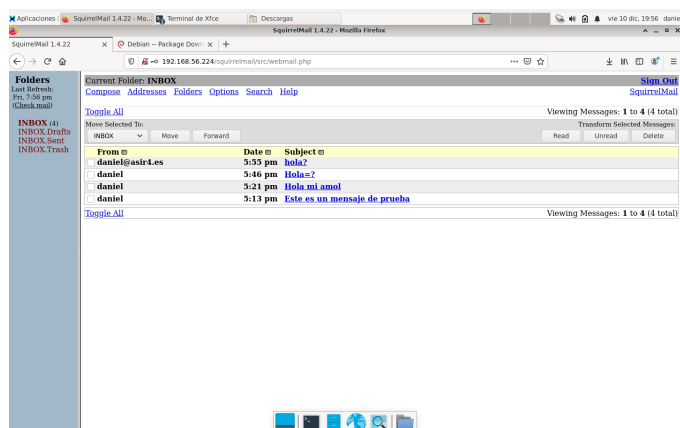
modificaremos el archivo de configuración de postfix añadiendo:

```
myhostname = debian.asir4.es
mydestination = asir4.es, debian.asir4.es, localhost.asir4.es, localhost
inet_interfaces = 192.168.56.224
inet_protocols = all
```

```
/etc/init.d/postfix restart
```



Envío de mensaje



Recepción de mensaje

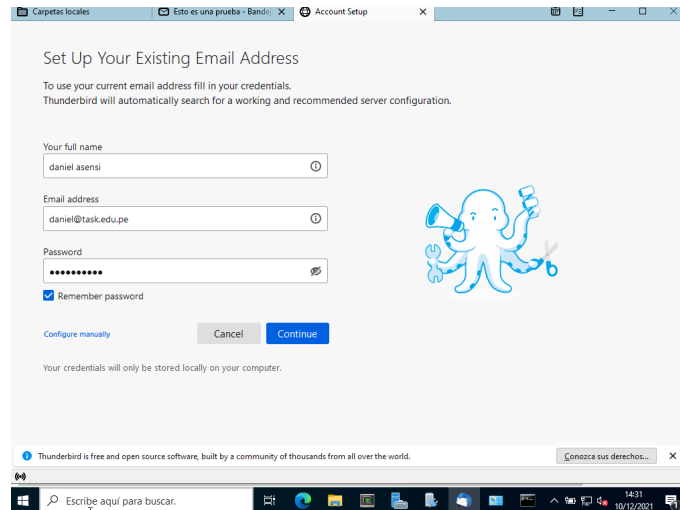
Para entrar al servidor de squirrel: 192.168.56.224/squirrelmail

7.2 Windows 10

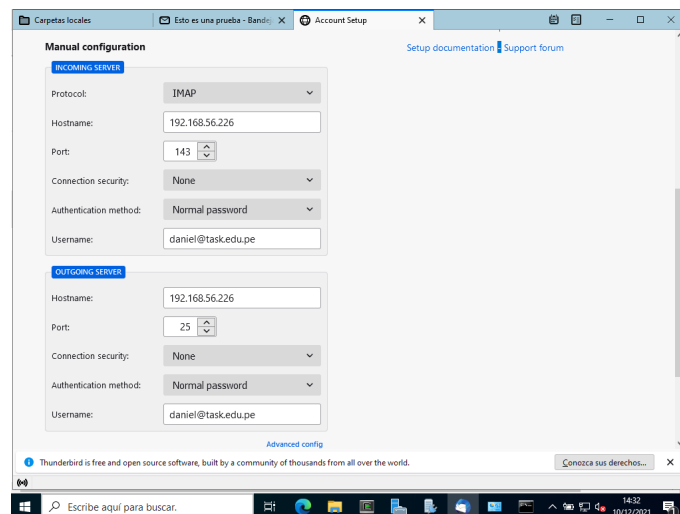
Para la creación de nuestro servidor de correo electrónico se utilizará hmailserver, antes de ello deberemos tener configurada nuestra dns, una vez hecho todos esto procederemos a instalar el servidor con los componentes de .NETFRAMEWORK 3.5:

Configuraremos nuestras listas negras y grises de anti-spam y antivirus y podremos comenzar a mandar mensajes desde el cliente Thunderbird:

Para añadir una cuenta desde el cliente haremos lo siguiente:

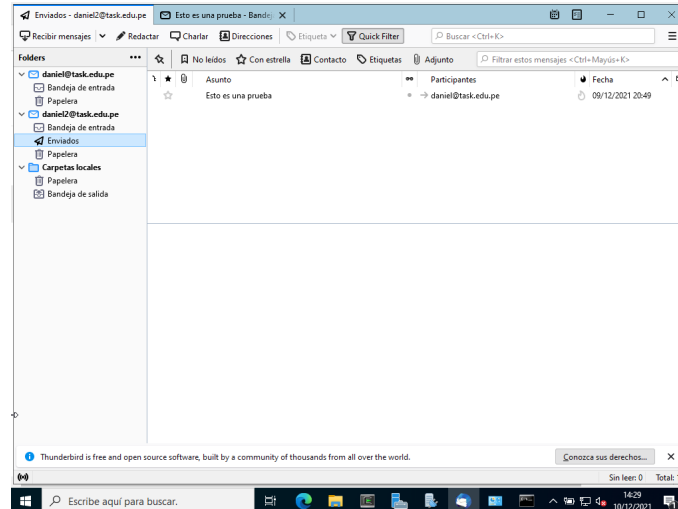


Logueandose

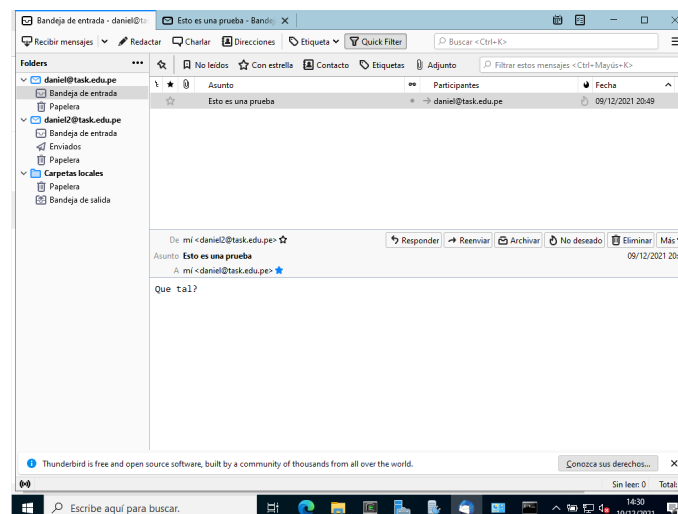


Configuración de logueo

Y haciendo esto dos veces con dos cuentas diferentes podremos comenzar a enviar correos electrónicos:



Envío de mensaje



Recepción de mensaje

8 Firewall, VPN, Enrutado

8.1 Freebsd

Para el Firewall en FreeBSD utilizaremos los comandos preinstalados de pf, para ellos haremos lo siguiente:

```
nano /etc/pf.conf
block all

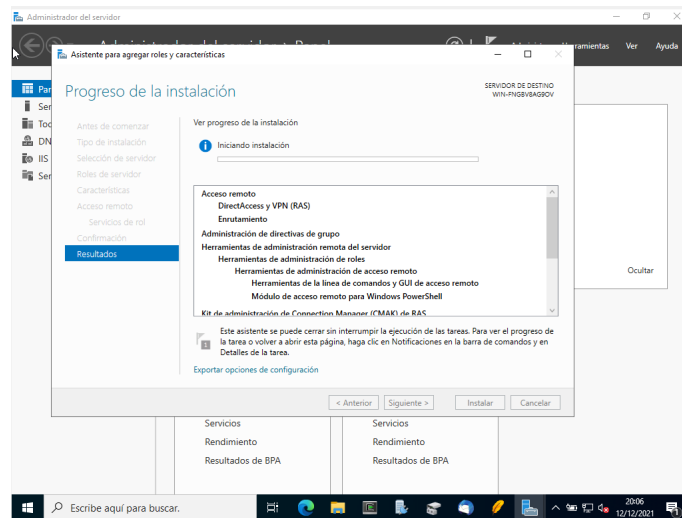
sysrc pf_enable=yes
service pf start
service pf reload
```

Para encenderlo o apagarlo haremos lo siguiente:

```
service pf start
service pf stop
```

8.2 Windows 10

Para la instalación de enrutado en windows lo instalaremos desde los roles y características de Windows server:



Instalación