Configuración Servidor FTP Centos 7

Autor: Pablo Andrés Bernabéu Soler

En esta práctica se instalará y configurará un servidor FTP. Para ello, se seguirán los siguientes pasos:

1. Pasos Previos
3. Seguridad
4. Creación directorios. Creación de Usuarios y Grupos
5. Cuotas de disco
6. Logging

1. Pasos Previos

Configure las tarjetas de red del servidor:

VLAN Producción:	Dirección IP 10.XX.99.220 DNS los servidores de la UPV
VLAN Gestión:	Dirección IP 10.XX.100.220
VLAN Storage:	Dirección IP 10.XX.200.2220

Nombre a la máquina con el nombre ftpC.grupoXX.net

A partir de entonces acceda a realizar la gestión a través de la VLAN de gestión. Configure el acceso ssh sólo por la IP indicada en la VLAN de Gestión.

Reinicie la máquina.

2. Instalación del servicio FTP y configuración

FTP (File Transfer Protocol) es un protocolo TCP/IP que permite transferir ficheros entre un servidor y un cliente. Cualquier servidor LINUX puede llegar a ser un servidor FTP instalando el software apropiado.

Los usuarios de un sistema pueden ser a su vez usuarios FTP. Cuando los usuarios acceden al servidor FTP, empiezan la sesión en su directorio *home*.

El primer paso que vamos a realizar, va a ser, la instalación del servicio *"Very Secure FTP Daemon"* (vsftp) en Linux Centos Red Hat 7 para la compañía grupoXX.net

Una buena práctica es actualizar los packages.

```
root@ftpC ~]#  yum -y update
```

Instalamos vsftpd y los paquetes requeridos

```
root@ftpC ~]#  yum -y install vsftpd
```

El servidor FTP será instalado con los siguientes requerimientos:

- Los usuarios FTP serán usuarios locales.

- El directorio inicial para los usuarios FTP será /datos/ftp
- Navegar por el sistema de ficheros no estará permitido para ningún usuario FTP.
- El acceso anónimo no estará permitido.
- Los usuarios FTP no pueden entrar al sistema (no pueden acceder mediante login y password, no pueden acceder vía shell).
- Estará deshabilitado el acceso como usuario root
- La máxima velocidad de transferencia para los usuarios FTP será de 10 Mbps (1.250.000 bps).
- El servidor sólo escuchará peticiones FTP que lleguen por la VLAN de producción (10.XX.99.220)

Para ello debe establecer parámetros de configuración en el fichero vsftpd.conf. Abra el fichero

[root@ftpC ~]# vi /etc/vsftpd/vsftpd.conf

Añada al final del mismo:

listen_address=10.XX.99.220 (sólo escucha VLAN producción)

local_max_rate=1250000 (establecemos la máxima velocidad de transmisión)

Busque las directivas local_enable y anonymous_enable quite comentarios y verifique que su atributo es el indicado.

local_enable=YES (habilita usuarios locales)

anonymous_enable=NO (no permite el acceso anónimo)

Para conseguir que la conexión al usuario root esté deshabilitada, hemos de tener la directiva a userlist_enable a YES. De esta forma los usuarios que aparecen en el fichero vi /etc/vsftpd/user_list, no son permitidos, ya que por defecto userlist_deny=YES

Si por el contrario, quisiéramos permitir la conexión sólo de los usuarios listados en este fichero, tendríamos que añadir la directiva userlist_deny=NO, para que no se ejecutase por defecto que es YES.

Ahora tenemos que conseguir que nuestros usuarios no puedan navegar fuera de su directorio asignado.

- En primer lugar, para que los usuarios estén enjaulados en su directorio FTP la directiva chroot_local_user tiene que tener asignada el valor de YES.
- Los nombres de usuarios virtuales que agregamos a la lista /etc/vsftpd/chroot_list serán aquellos usuarios que "SI" podrán navegar por todo el sistema de archivos cuando la directiva chroot_local_user=YES, por este motivo, sólo agregaremos a esta lista los usuarios que "necesitan" acceder a todo el sistema de archivos, y a todos aquellos usuarios virtuales que no incluidos en el archivo chroot_list quedarán bien enjaulados. (Esta opción la activamos para permitir la posibilidad de tener unos usuarios enjaulados o no)

Como resumen:

```
# Enjaula a los usuarios locales dentro de su propio directorio personal, esta opción mejora la seguridad.
chroot_local_user=YES

# Permite especificar una lista con los usuarios locales a los cuales
# no se les enjaulará cuando la opción chroot_local_user = YES.
chroot_list_enable=YES

# Especifica la ruta en donde se encuentra la lista, en mi caso he
# creado una carpeta en el directorio /etc llamada "vsftpd", en la
# cual coloqué el archivo de texto (vsftpd.chroot_list) que contiene
# la lista.
chroot_list_file=/etc/vsftpd/chroot_list
```

Además debemos crear el fichero "chroot_list":

```
touch /etc/vsftpd/chroot_list
```

Y dejarlo de momento vacío.

Proceda pues con la información indicada a configurar el servicio ftp.

Configure el arranque automático.

```
systemctl enable vsftpd.service
systemctl start vsftpd
```

Una vez configurado, lo más recomendable es reiniciar el servidor, con lo cual nos aseguramos que los cambios quedan aceptados y funcionales.

Actividades

Cree el directorio /datos/ftp.

Cree un usuario dummy para testear el servicio (user:dummy , password=pa$$wOrd)

Chequee el servicio FTP está funcionando y escuchando por la VLAN de producción.

Chequee la conexión desde el host usando FILEZILLA.

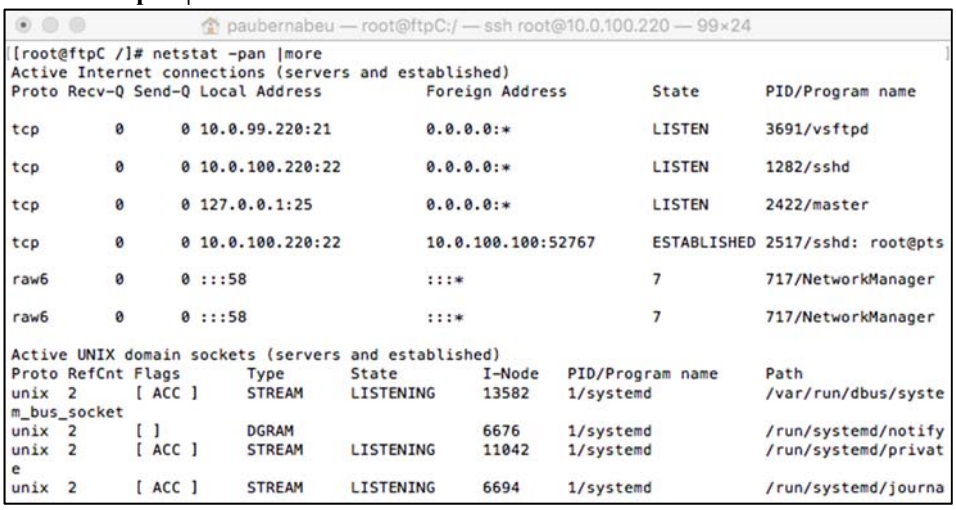
Cuando creamos el directorio lo hacemos como root y deben usarlo otros usuarios, por ello cambiamos los permisos del directorio: chmod –R 777 /datos/ftp

Consideraciones:

Para verificar el servicio puede instalar las herramientas de red.

[root@ftpC /]# yum install net-tools

Y ejecutar **netstat -pan |more**



```
paubernabeu — root@ftpC:/ — ssh root@10.0.100.220 — 99×24
[root@ftpC /]# netstat -pan |more
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name

tcp        0      0 10.0.99.220:21          0.0.0.0:*               LISTEN      3691/vsftpd

tcp        0      0 10.0.100.220:22         0.0.0.0:*               LISTEN      1282/sshd

tcp        0      0 127.0.0.1:25            0.0.0.0:*               LISTEN      2422/master

tcp        0      0 10.0.100.220:22         10.0.100.100:52767      ESTABLISHED 2517/sshd: root@pts

raw6       0      0 :::58                   :::*                    7           717/NetworkManager

raw6       0      0 :::58                   :::*                    7           717/NetworkManager

Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State         I-Node   PID/Program name     Path
unix  2      [ ACC ]     STREAM     LISTENING     13582    1/systemd            /var/run/dbus/syste
m_bus_socket
unix  2      [ ]         DGRAM                    6676     1/systemd            /run/systemd/notify
unix  2      [ ACC ]     STREAM     LISTENING     11042    1/systemd            /run/systemd/privat
e
unix  2      [ ACC ]     STREAM     LISTENING     6694     1/systemd            /run/systemd/journa
```

Como podemos observar en la primera línea escucha vsftpd por la IP 10.0.99.220 y el puerto 21.

Para crear el usuario (busque en internet para entender el comando useradd de Centos):
useradd -d /datos/ftp/dummy -m -s /usr/sbin/nologin -c "Dummy D." dummy

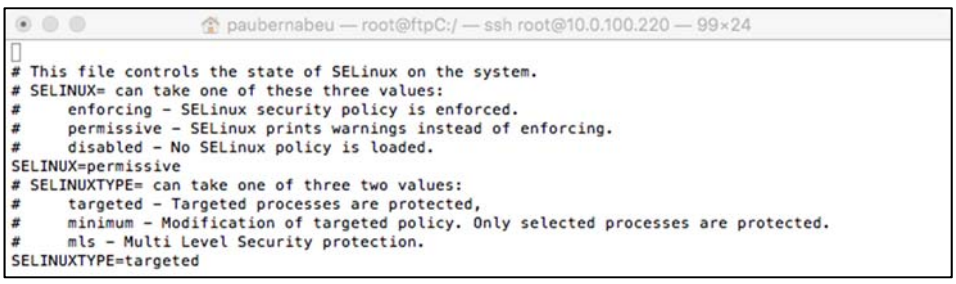
Con ello creamos el usuario dummy. Le indicamos cuáles es su directorio y además que no poder hacer login.

Instale en la máquina cliente Filezilla, previamente debe instalar el entorno gráfico.

3. Seguridad

En este laboratorio, el estudiante no configura SELINUX. Pase SELINUX a modo “Permissive” permanentemente.

Para ello, abra el fichero /etc/selinux/config. Coloque SELINUX=permissive.



```
paubernabeu — root@ftpC:/ — ssh root@10.0.100.220 — 99×24

# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#     enforcing - SELinux security policy is enforced.
#     permissive - SELinux prints warnings instead of enforcing.
#     disabled - No SELinux policy is loaded.
SELINUX=permissive
# SELINUXTYPE= can take one of three two values:
#     targeted - Targeted processes are protected,
#     minimum - Modification of targeted policy. Only selected processes are protected.
#     mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

Importante: en un entorno de Producción es necesario habilitar tantos sistemas de seguridad como sean posibles con el fin de evitar problemas de seguridad.

Por ello, vamos a aprender en esta práctica la configuración el firewall en Centos, lo aprendido aquí debemos aplicarlo cuando instalemos el resto de servicios de las siguientes prácticas (de esta forma consolidaremos lo aprendido)

Instale el firewall, si no estuviese instalado. Para sabe si hay un paquete instalado puede usar el comando: rpm -q [paquete]. En nuestro caso.

```
rpm -q firewalld
```

Para instalar:

```
yum -y install firewalld
```

En la siguiente url *https://www.certdepot.net/rhel7-get-started-firewalld/* tiene información para aprender a configurar el cortafuegos en Centos Red Hat 7.

Actividad

Configure el firewall con las siguientes zonas y servicios permanentemente (borre otros servicios). El nombre de la interface puede cambiar dependiendo de la máquina virtual

Active la interface storage, con la IP 10.XX.200.220

Zona	Interface	VLAN	Servicios
Public	enps03	Producción	ftp
Home	enps08	Gestión	ssh
Internal	enps09	Storage	--

Aplique los cambios de forma permanente:

```
[root@ftpC ~]# firewall-cmd --reload
```

Actividades

Chequee la configuración del cortafuegos en las tres interfaces:

```
firewall-cmd --permanent --zone=???? --list-all
```

Chequee la conexión desde el host usando Filezilla.

Cargue un fichero grande y chequee la velocidad de subida.

4. Creación directorios. Creación de Usuarios y Grupos

Consideraciones de los directorios, los usuarios FTP:

- Tendrán acceso privado al directorio personal (mismo nombre que nombre de usuario).
- Tendrán acceso a un fichero compartido, con el resto de usuarios donde cada uno de ellos tendrá permisos de lectura y escritura (directorios para compartir documentos).
- Tendrán acceso a un fichero con el resto de usuarios donde cada uno de ellos tendrá sólo permiso de lectura (directorio de documentos de la compañía: procedimientos, regulaciones, etc.).

El sistema tendrá 5 usuarios de diferentes departamentos con diferentes permisos sobre los siguientes directorios:

Usuario	**Departamento**	**Directorio Personal**	**Directorio Dpto. Ventas**	**Directorio Dpto. Marketing**	**Directorio Dpto. Administración**
N1(*)	Ventas	rwx	rwx	---	r-x
N2(*)	Márquetin	rwx	---	rwx	r-x
N3(*)	Ventas	rwx	rwx	---	r-x
rvila	Márquetin	rwx		rwx	r-x
jperez	Márquetin	rwx	---	rwx	r-x

(*) Donde N1, N2, N3 corresponde a los nombres de los miembros del grupo de la práctica, por ejemplo, Pau Bernabeu→pbernabe (como ejemplo de resolución: N1=agonzalez, N2=pbernabe, N3=nlopez)

Pasos a realizar:

- Creación de los directorios Ventas, Márquetin, y Administración en /datos/ftp.
  - [root@ftpC /]# cd /datos/ftp/
  - mkdir ventas marquetin administración

- Creación de los grupos (para poder compartir directorios).
  - [root@ftpC /]# groupadd administracion
  - [root@ftpC /]# groupadd ventas
  - [root@ftpC /]# groupadd márquetin

- Asignar propietarios.
  - [root@ftpC ftp]# chown nobody:administracion administracion/
  - [root@ftpC ftp]# chown nobody:ventas ventas/
  - [root@ftpC ftp]# chown nobody:marquetin marquetin/

- Asignamos permisos y el sticky bit:
  - [root@ftpC ftp]# chmod 1770 marquetin
  - [root@ftpC ftp]# chmod 1770 ventas/
  - [root@ftpC ftp]# chmod 550 administracion/
  - [root@ftpC ftp]# chmod g+s marquetin/ ventas/ (agregamos el setgid al grupo).

- Añadimos los usuarios y los ponemos en sus respectivos directorios raíz:
  - [root@ftpC ftp]# useradd -d /datos/ftp/rvila -s /sbin/nologin rvila
  - (añade el resto de usuarios)

- Asignamos contraseña a los usuarios:

- [root@ftpC ftp]# passwd rvila
- Introducimos como contraseña pa$$wOrd
- (repita el proceso para el resto de usuarios, misma contraseña para todos)

Explorando el archivo /etc/passwd podemos observar si los usuarios se han introducido correctamente (ver las últimas 5 líneas).

```
rvila:x:1007:1010::/datos/ftp/rvila:/sbin/nologin
agonzalez:x:1008:1011::/datos/ftp/agonzalez:/sbin/nologin
nlopez:x:1009:1009::/datos/ftp/nlopez:/sbin/nologin
jperez:x:1010:1012::/datos/ftp/jperez:/sbin/nologin
pbernabe:x:1011:1013::/datos/ftp/pbernabe:/sbin/nologin
```

Para poder navegar por el resto de carpetas con permisos modificamos estas líneas para que queden tal como se observa en la siguiente figura (quitar el directorio personal)

```
rvila:x:1007:1010::/datos/ftp/:/sbin/nologin
agonzalez:x:1008:1011::/datos/ftp/:/sbin/nologin
nlopez:x:1009:1009::/datos/ftp/:/sbin/nologin
jperez:x:1010:1012::/datos/ftp/:/sbin/nologin
pbernabe:x:1011:1013::/datos/ftp/:/sbin/nologin
```

- Asignamos los usuarios a sus grupos:
  - Como vemos en la tabla todos pertenecen a “administración”.

```
[root@ftpC ftp]# gpasswd -a agonzalez administracion
Añadiendo al usuario agonzalez al grupo administracion
[root@ftpC ftp]# gpasswd -a jperez administracion
Añadiendo al usuario jperez al grupo administracion
[root@ftpC ftp]# gpasswd -a pbernabe  administracion
Añadiendo al usuario pbernabe al grupo administracion
[root@ftpC ftp]# gpasswd -a rvila  administracion
Añadiendo al usuario rvila al grupo administracion
[root@ftpC ftp]# gpasswd -a nlopez  administracion
Añadiendo al usuario nlopez al grupo administracion
```

  - Añada cada usuario a ventas o márquetin según corresponda.
  - Podemos comprobar se han añadido correctamente, para ello vemos el fichero /etc/group (en concreto las líneas)

```
administracion:x:1003:agonzalez,jperez,pbernabe,rvila,nlopez
ventas:x:1004:agonzalez,nlopez
marquetin:x:1005:pbernabe,rvila,jperez
```

- Asignamos propietarios a los directorios (si no lo son, tal como lo hemos hecho al crear los usuarios ya son propietarios). Si no fuese así,
  - chown agonzalez:agonzalez agonzalez/
  - (haga los mismo con el resto)
  - ¿Tiene claro por qué?

- Damos permisos a los usuarios:
  - chmod 770 agonzalez/ jperez/ nlopez/ rvila/ pbernabe/
  - ¿Tiene claro por qué?.
  - El resultado final deberá ser:

```
[root@ftpC ftp]# ls -l
total 0
dr-xr-x---. 2 nobody    administracion  6 ago 31 08:56 administracion
drwxrwx---. 2 agonzalez agonzalez      59 ago 31 09:34 agonzalez
drwxrwx---. 2 jperez    jperez         59 ago 31 09:36 jperez
drwxrws--T. 2 nobody    marquetin       6 ago 31 08:56 marquetin
drwxrwx---. 2 nlopez    nlopez         59 ago 31 09:36 nlopez
drwxrwx---. 2 pbernabe  pbernabe       59 ago 31 09:37 pbernabe
drwxrwx---. 2 rvila     rvila          59 ago 31 09:31 rvila
drwxrws--T. 2 nobody    ventas          6 ago 31 08:56 ventas
[root@ftpC ftp]#
```

Actividad

Desde Filezilla, loguee usando diferentes usuarios y compruebe los permisos. Cree algunos ficheros e intente borrarlos usando diferentes usuarios distintos al propietario.

5. Cuotas de disco

En este apartado aprenderemos a configurar cuotas de uso del disco (use xfs_quota después de que el sistema de ficheros es xfs). Valor de cuotas de usuarios (límite hard).

Usuario	Cuotas
N1	10 MB
N2	50 MB
N3	200 MB
rvila	10 MB
jperez	100 MB

Importante:

Para poder dar cuotas, debemos tener una partición que las permita. Por lo tanto, esto lo deberíamos tenerlo en cuenta al hacer la partición en el momento de la instalación.

Lo correcto, es disponer de dispositivos de almacenaje externos (red storage).

En este caso, vamos a añadir al servidor un nuevo disco y asignarle la capacidad de cuotas. Aprovechando lo ya realizado en el directorio /datos/ftp.

Pasos a seguir:

- Apagamos la máquina.
- Añadimos un nuevo disco virtual desde VirtualBox. (Tamaño 8GB). Les damos de nombre, por ejemplo, “datos_ftp”.
- Arrancamos la máquina.
- Montamos el nuevo disco duro en /datos/ftp.
    - Daremos formato al disco y lo marcamos como LVM

      fdisk /dev/sdb

      Marcamos la participación como primaria, y el tamaño:

      Introducimos n.

Introducimos p. (indicamos participación primaria).

Presionamos "intro" dos veces.

Marcamos la partición como LVM: Introducimos t y posteriormente 8e.

Introducimos w (con lo que aceptamos y tendremos el formato realizado).

- Agregamos el disco a /datos/ftp.
  - pvcreate /dev/sdb1
  - vgextend centos /dev/sdb1
  - lvcreate –l 100%FREE –n datos_ftp centos.
- Damos formato xfs al disco
  - mkfs -t xfs /dev/centos/datos_ftp
- Creamos un directorio temporal.
  - mkdir /nmt/datos_ftp
- Montamos:
  - mount /dev/centos/datos_ftp /mnt/datos_ftp
  - Verificamos: mountpoint /mnt/datos_ftp/
  - Si obtenemos el mensaje "/mnt/datos_ftp/ is not a mountpoint", todo es correcto.
- Una vez, que está montado, realizamos una copia de los directorios creados hasta ahora y que tenemos en /datos/ftp.
  - cp -ax /datos/ftp/* /mnt/datos_ftp/
  - Eliminamos el directorio /datos/ftp: rm –rf /datos/ftp
  - Lo volvemos a crear: mkdir –p /datos/ftp
  - Desmontamos disco: umount /nmt/datos_ftp.
- Modificamos fichero vi /etc/fstab
  - Añada la línea:

    /dev/centos/datos_ftp /datos/ftp xfs defaults,usrquota, grpquota 0 0
- Volvemos a montar.
  - mount –av
- Verificamos que está montado:

```
[root@ftpC /]# df -hT
S.ficheros                  Tipo     Tamaño Usados  Disp Uso% Montado en
/dev/mapper/centos-root     xfs        6,7G   1,8G  5,0G  26% /
devtmpfs                    devtmpfs   361M      0  361M   0% /dev
tmpfs                       tmpfs      371M      0  371M   0% /dev/shm
tmpfs                       tmpfs      371M   5,0M  366M   2% /run
tmpfs                       tmpfs      371M      0  371M   0% /sys/fs/cgroup
/dev/sda1                   xfs        497M   210M  288M  43% /boot
tmpfs                       tmpfs       75M      0   75M   0% /run/user/0
/dev/mapper/centos-datos_ftp xfs       8,1G    33M  8,0G   1% /datos/ftp
```

(Se observa que está montado, ver la última línea de la figura anterior)

Comprobamos en /datos/ftp tenemos los directorios.

```
[root@ftpC ftp]# cd /datos/ftp
[root@ftpC ftp]# ls -l
total 0
dr-xr-x---. 2 nobody    administracion  6 ago 31 08:56 administracion
drwxrwx---. 2 agonzalez agonzalez      59 ago 31 09:34 agonzalez
drwxrwx---. 2 jperez    jperez         59 ago 31 09:36 jperez
drwxrws--T. 2 nobody    marquetin       6 ago 31 08:56 marquetin
drwxrwx---. 2 nlopez    nlopez         59 ago 31 09:36 nlopez
drwxrwx---. 2 pbernabe  pbernabe       59 ago 31 09:37 pbernabe
drwxrwx---. 2 rvila     rvila          59 ago 31 09:31 rvila
drwxrws--T. 3 nobody    ventas         22 ago 31 10:48 ventas
```

Ya estamos pues en condiciones de crear cuotas en los directorios dedicados al servicio FTP.

Creamos las cuotas de usuario:

```
[root@ftpC ftp]# xfs_quota -x -c 'limit -u bsoft=45m bhard=50m pbernabe' /datos/ftp/
[root@ftpC ftp]# xfs_quota -x -c 'limit -u bsoft=8m bhard=10m agonzalez' /datos/ftp/
[root@ftpC ftp]# xfs_quota -x -c 'limit -u bsoft=95m bhard=100m jperez' /datos/ftp/
[root@ftpC ftp]# xfs_quota -x -c 'limit -u bsoft=195m bhard=200m nlopez' /datos/ftp/
[root@ftpC ftp]# xfs_quota -x -c 'limit -u bsoft=195m bhard=200m rvila' /datos/ftp/
```

Verificamos las cuotas son correctas.

```
[root@ftpC ftp]# repquota /datos/ftp/
```

ó

```
[root@ftpC ftp]# xfs_quota -x -c 'report -h' /datos/ftp
```

```
[root@ftpC ftp]# xfs_quota -x -c 'report -h' /datos/ftp
User quota on /datos/ftp (/dev/mapper/centos-datos_ftp)
                        Blocks
User ID      Used   Soft   Hard Warn/Grace
---------- ---------------------------------
root            0      0      0  00 [------]
nobody          0      0      0  00 [------]
rvila         12K   195M   200M  00 [------]
agonzalez     12K     8M    10M  00 [------]
nlopez        12K   195M   200M  00 [------]
jperez        12K    95M   100M  00 [------]
pbernabe      12K    45M    50M  00 [------]

[root@ftpC ftp]# repquota /datos/ftp/
*** Report for user quotas on device /dev/mapper/centos-datos_ftp
Block grace time: 7days; Inode grace time: 7days
                        Block limits                File limits
User            used    soft    hard  grace    used  soft  hard  grace
----------------------------------------------------------------------
root      --       0       0       0              3     0     0
nobody    --       0       0       0              3     0     0
rvila     --      12  199680  204800              4     0     0
agonzalez --      12    8192   10240              5     0     0
nlopez    --      12  199680  204800              4     0     0
jperez    --      12   97280  102400              4     0     0
pbernabe  --      12   46080   51200              4     0     0
```

Actividades

Chequee las cuotas de los usuarios.

Desde Filezilla, chequee el correcto funcionamiento de las cuotas, transfiriendo ficheros con menos tamaño que el permitido y más grande que el permitido.

Nota: Para crear ficheros de un determinado tamaño.

```
dd if=/dev/zero of=archivo.bmp bs=1 count=0 seek=200M
```

6. Logging

Por defecto, el servidor vsftpd escribe los logs directamente al fichero (/var/log/xferlog)

Actividades:

Chequee los logs en /var/log/xferlog.

Intente loguear un usuario con un password erróneo y chequee los siguientes logs: messages y secure buscando el error.
