

Práctica 3

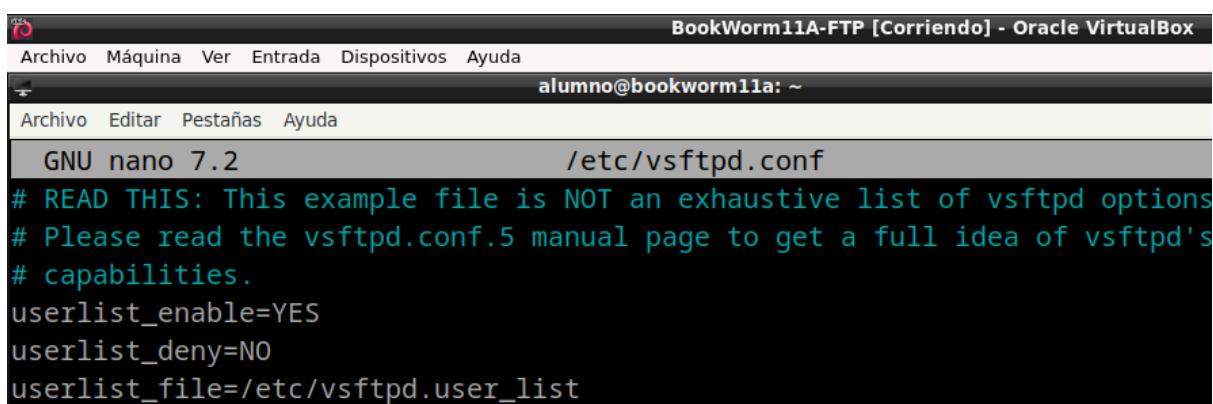
Aspectos teóricos previos

Se puede especificar un directorio como directorio raíz para un usuario determinado, que puede ser su 'home' o no. Con ello se evita que los usuarios que se conecten puedan navegar por los directorios del servidor, por ello se dice que quedan enjaulados (jailed)

- Directiva 'chroot_list_enable': Cuando está activada, hace que se coloquen en una 'jaula' de chroot a los usuarios locales listados en el archivo especificado en la directriz chroot_list_file. Si se utiliza en combinación con la directriz chroot_local_user, los usuarios locales listados en el archivo especificado en la directriz chroot_list_file, no se colocan en una 'jaula' chroot después de conectarse (el valor predeterminado es NO)
- chroot_list_file: Especifica el archivo que contiene una lista de los usuarios locales a los que se hace referencia cuando la directriz chroot_list_enable está en YES (el valor por defecto es /etc/vsftpd.chroot_list)
- chroot_local_user: Si está activada, a los usuarios locales se les cambia el directorio raíz (se hace un chroot) a su directorio principal después de la conexión (el valor predeterminado es NO). Es necesario activar también la directiva allow_writeable_chroot=YES, en el caso de que el directorio sea modificable por el usuario, lo cual no es recomendable

Desarrollo de la práctica

1. Configura el servicio en tu servidor BOOKWORMXXA para que solamente se puedan conectar usuarios locales de la máquina. Haz las pruebas que consideres necesarias para comprobarlo.



```
alumno@bookworm11a: ~
GNU nano 7.2          /etc/vsftpd.conf
# READ THIS: This example file is NOT an exhaustive list of vsftpd options
# Please read the vsftpd.conf.5 manual page to get a full idea of vsftpd's
# capabilities.
userlist_enable=YES
userlist_deny=NO
userlist_file=/etc/vsftpd.user_list
```

2. Configura el servicio para que solamente se puedan conectar tu usuario y el usuario "cliente1" creado en la práctica anterior. Haz las pruebas que consideres necesarias para comprobarlo.

BookWorm11A-FTP [Corriendo] - Oracle VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

alumno@bookworm11a: ~

Archivo Editar Pestañas Ayuda

GNU nano 7.2 /etc/vsftpd.user_list

```
cliente1
alumno
```

Linux11DHCP [Corriendo] - Oracle VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

linux11@linux11-virtualbox: ~

Archivo Acciones Editar Vista Ayuda

linux11@linux11-virtualbox: ~ ×

```
linux11@linux11-virtualbox:~$ ftp ftp.asir11.asir
Connected to bookworm11a.asir11.asir.
220 (vsFTPD 3.0.3)
Name (ftp.asir11.asir:linux11): anonymous
530 Permission denied.
ftp: Login failed
ftp>
ftp> exit
221 Goodbye.
linux11@linux11-virtualbox:~$ ftp ftp.asir11.asir
Connected to bookworm11a.asir11.asir.
220 (vsFTPD 3.0.3)
Name (ftp.asir11.asir:linux11): alumno
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> exit
221 Goodbye.
linux11@linux11-virtualbox:~$ ftp ftp.asir11.asir
Connected to bookworm11a.asir11.asir.
220 (vsFTPD 3.0.3)
Name (ftp.asir11.asir:linux11): cliente1
331 Please specify the password.
Password:
230 Login successful.
```

3. Configura el usuario "cliente1" para que quede enjaulado en el directorio /var/www/virtual1 y haz pruebas que consideres necesarias para comprobarlo. Este usuario ha de ser el único enjaulado (el tuyo no debería estarlo).

BookWorm11A-FTP [Corriendo] - Oracle VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

alumno@bookworm11a: ~

Archivo Editar Pestañas Ayuda

```
GNU nano 7.2 /etc/vsftpd.conf
# READ THIS: This example file is NOT an exhaustive list of vsftpd options.
# Please read the vsftpd.conf.5 manual page to get a full idea of vsftpd's
# capabilities.
userlist_enable=YES
userlist_deny=NO
userlist_file=/etc/vsftpd.user_list
# Por defecto nadie está enjaulado
chroot_local_user=NO
#habilitada la lista de enjaulados
chroot_list_enable=YES
# Defino dónde está la lista
chroot_list_file=/etc/vsftpd.chroot_list
# Permiso de escritura en la jaula
allow_writeable_chroot=YES
```

BookWorm11A-FTP [Corriendo] - Oracle VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

alumno@bookworm11a: ~

Archivo Editar Pestañas Ayuda

```
GNU nano 7.2 /etc/vsftpd.chroot_list
cliente1
```

Linux11DHCP [Corriendo] - Oracle VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

linux11@linux11-virtualbox: ~

```
linux11@linux11-virtualbox:~$ ftp ftp.asir11.asir
Connected to bookworm11a.asir11.asir.
220 (vsFTPd 3.0.3)
Name (ftp.asir11.asir:linux11): cliente1
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> cd /
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||17092|)
150 Here comes the directory listing.
drwxr-xr-x 2 1001 33 4096 Nov 27 10:05 digest
drwxr-xr-x 2 1001 33 4096 Nov 26 20:03 errors
-rw-r--r-- 1 1001 33 370 Nov 27 10:12 index.php
drwxr-xr-x 2 1001 33 4096 Dec 04 10:29 permitido
-rw----- 1 1001 33 0 Jan 08 12:09 prueba.txt
-rw----- 1 1001 33 0 Jan 08 12:15 prueba2.txt
-rw----- 1 1001 33 0 Jan 08 12:12 prueba_active.txt
-rw----- 1 1001 33 0 Jan 08 12:21 prueba_modoactivo.txt
drwxr-xr-x 2 1001 33 4096 Nov 26 19:08 restringido
drwxr-xr-x 2 1001 33 4096 Dec 02 09:09 usuarios
226 Directory send OK.
ftp> 
```

Linux11DHCP [Corriendo] - Oracle VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

linux11@linux11-virtualbox: ~

```
linux11@linux11-virtualbox:~$ ftp ftp.asir11.asir
Connected to bookworm11a.asir11.asir.
220 (vsFTPd 3.0.3)
Name (ftp.asir11.asir:linux11): alumno
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> cd /
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||55852|)
150 Here comes the directory listing.
lrwxrwxrwx 1 0 0 7 Sep 15 08:19 bin -> usr/bin
drwxr-xr-x 3 0 0 4096 Sep 15 09:04 boot
drwxr-xr-x 18 0 0 3400 Jan 12 09:13 dev
drwxr-xr-x 131 0 0 12288 Jan 12 09:45 etc
drwxr-xr-x 3 0 0 4096 Sep 15 08:30 home
lrwxrwxrwx 1 0 0 30 Sep 15 09:02 initrd.img -> boot/initrd.img-6.1.0-39-amd64
lrwxrwxrwx 1 0 0 30 Sep 15 08:20 initrd.img.old -> boot/initrd.img-6.1.0-35-amd64
lrwxrwxrwx 1 0 0 7 Sep 15 08:19 lib -> usr/lib
lrwxrwxrwx 1 0 0 9 Sep 15 08:19 lib64 -> usr/lib64
drwx----- 2 0 0 16384 Sep 15 08:19 lost+found
drwxr-xr-x 3 0 0 4096 Sep 15 08:19 media
drwxr-xr-x 2 0 0 4096 Sep 15 08:19 mnt
drwxr-xr-x 3 0 0 4096 Oct 26 19:11 opt
```

4. El usuario "cliente1" ha de poder modificar cualquier archivo y/o directorio dentro de su directorio.

```

Linux11DHCP [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
linux11@linux11-virtualbox: ~
Archivo Acciones Editar Vista Ayuda
linux11@linux11-virtualbox: ~ x
linux11@linux11-virtualbox:~$ ftp ftp.asir11.asir
Connected to bookworm11a.asir11.asir.
220 (vsFTPd 3.0.3)
Name (ftp.asir11.asir:linux11): cliente1
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||39140|)
150 Here comes the directory listing.
drwxr-xr-x  2 1001      33          4096 Nov 27 10:05 digest
drwxr-xr-x  2 1001      33          4096 Nov 26 20:03 errors
-rw-r--r--  1 1001      33          370   Nov 27 10:12 index.php
drwxr-xr-x  2 1001      33          4096 Dec  04 10:29 permitido
-rw-----  1 1001      33             0 Jan 08 12:09 prueba.txt
-rw-----  1 1001      33             0 Jan 08 12:15 prueba2.txt
-rw-----  1 1001      33             0 Jan 08 12:12 prueba_active.txt
-rw-----  1 1001      33             0 Jan 08 12:21 prueba_modoactivo.txt
drwxr-xr-x  2 1001      33          4096 Nov 26 19:08 restringido
drwxr-xr-x  2 1001      33          4096 Dec  02 09:09 usuarios
226 Directory send OK.
ftp> mkdir carpeta_de_prueba
257 "/carpeta_de_prueba" created
ftp>

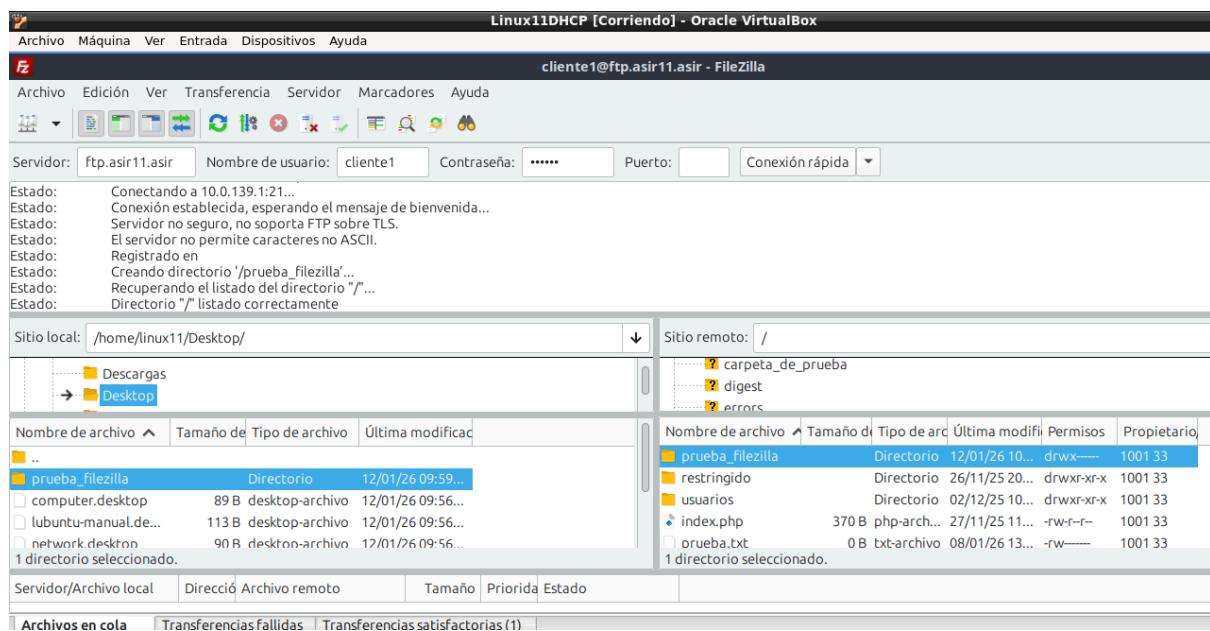
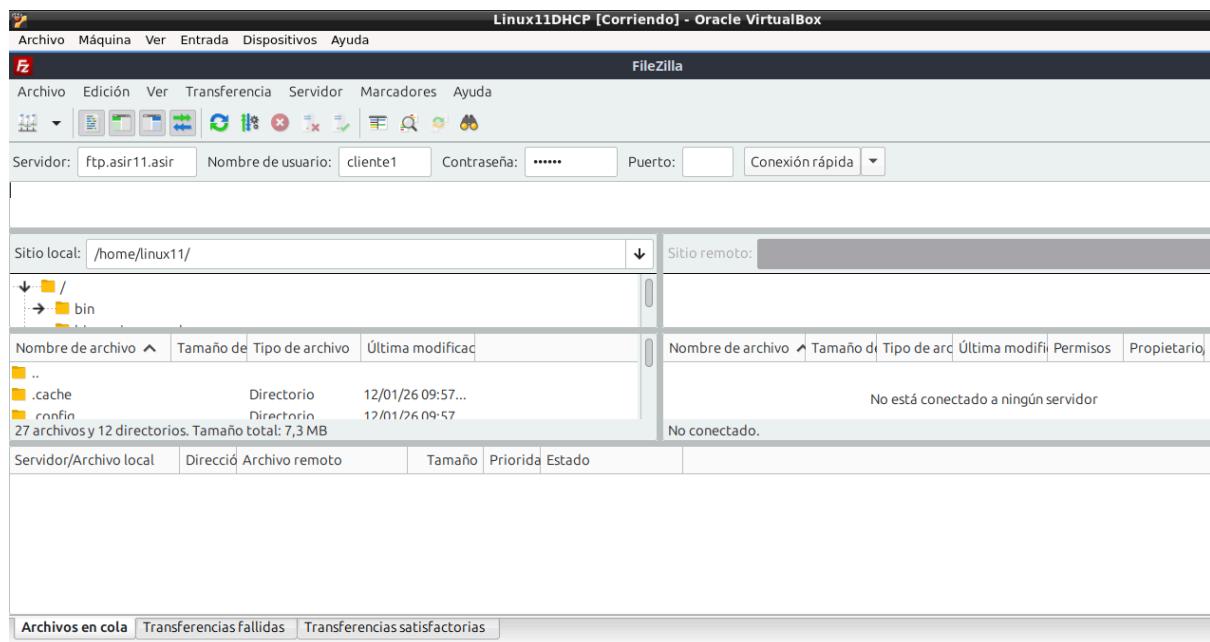
```

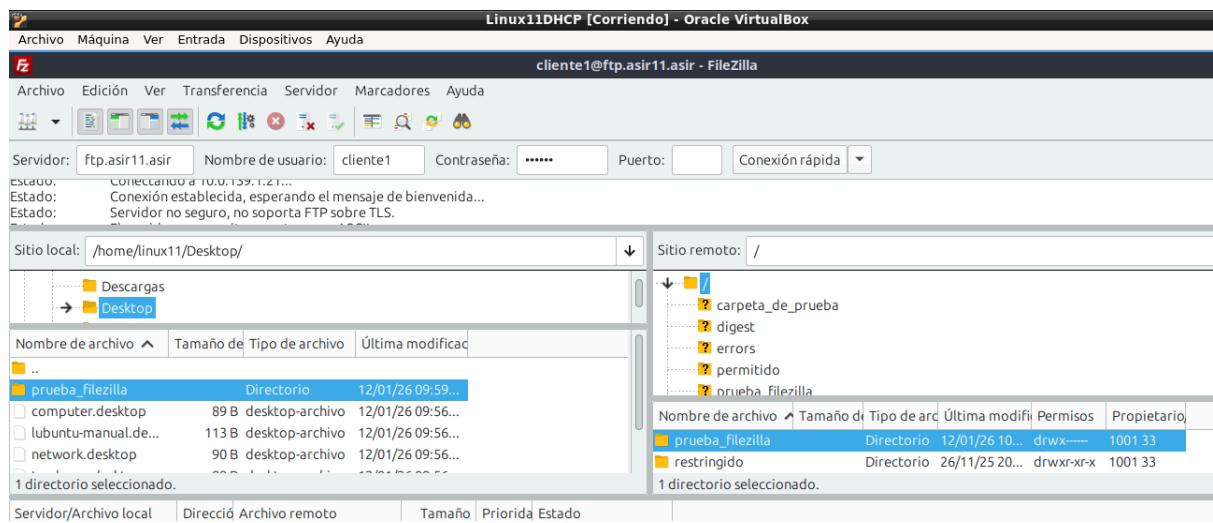
```

Linux11DHCP [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
linux11@linux11-virtualbox: ~
Archivo Acciones Editar Vista Ayuda
linux11@linux11-virtualbox: ~ x
linux11@linux11-virtualbox:~$ ls
229 Entering Extended Passive Mode (|||14975|)
150 Here comes the directory listing.
drwx-----  2 1001      33          4096 Jan 12 09:50 carpeta_de_prueba
drwxr-xr-x  2 1001      33          4096 Nov 27 10:05 digest
drwxr-xr-x  2 1001      33          4096 Nov 26 20:03 errors
-rw-r--r--  1 1001      33          370   Nov 27 10:12 index.php
drwxr-xr-x  2 1001      33          4096 Dec  04 10:29 permitido
-rw-----  1 1001      33             0 Jan 08 12:09 prueba.txt

```

5. Instala el cliente FTP "Filezilla" en tu cliente LINUXXX y prueba la configuración anterior de nuevo conectándote al servicio 'ftp.asirXX.asir'. Para ello prueba que el usuario "cliente1" pueda subir, modificar y eliminar archivos y directorios en su directorio raíz pero no puede salir de él (puedes utilizar el siguiente tutorial para ver el funcionamiento, si bien es bastante intuitivo: acceso al tutorial pulsando [aquí](#))





Realiza una copia de seguridad de la configuración en otro archivo para no perderla de cara a las próximas prácticas (vsftpd.conf.practica3)

```

alumno@bookworm11a:~$ sudo cp /etc/vsftpd.conf /etc/vsftpd.conf.practica3
[sudo] contraseña para alumno:
alumno@bookworm11a:~$ sudo ls -l /etc/vsftpd*
-rw-r--r-- 1 root root    9 ene 12 09:36 /etc/vsftpd.chroot_list
-rw-r--r-- 1 root root 6172 ene 12 09:44 /etc/vsftpd.conf
-rw-r--r-- 1 root root 5920 ene  8 12:28 /etc/vsftpd.conf.practica2
-rw-r--r-- 1 root root 6172 ene 12 10:27 /etc/vsftpd.conf.practica3
-rw-r--r-- 1 root root   16 ene 12 09:31 /etc/vsftpd.user_list
alumno@bookworm11a:~$ 

```