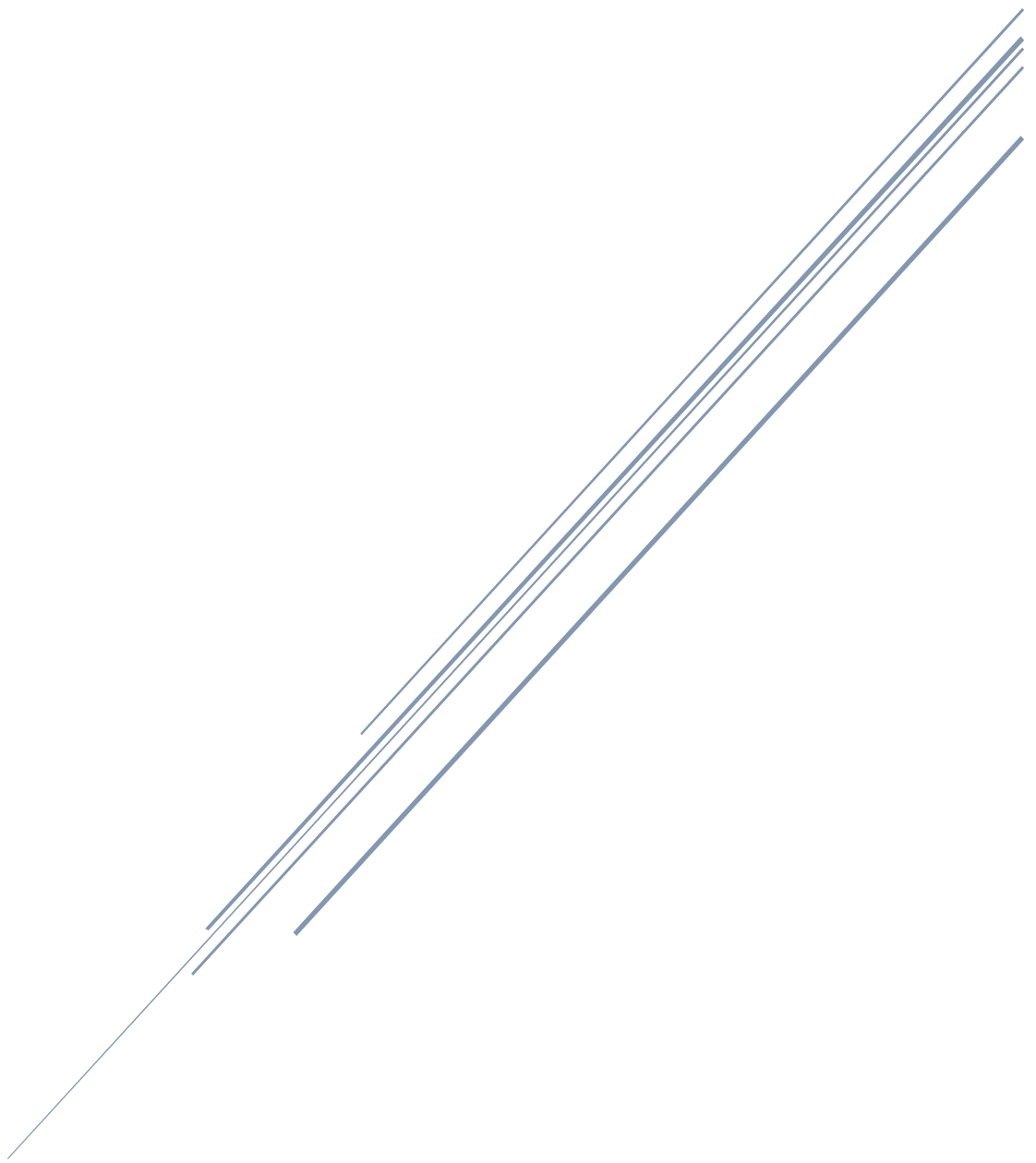


FTP

(FILE TRANSFER PROTOCOL)



Adrián Gómez Lois

Contenido

1. Obxectivos	3
2. Descarga automática dun arquivo dende un servidor FTP	4
3. Instalación e configuración servidor VSFTPD.....	15
4. Instalación e configuración servidor FTP en Windows Server 2012.....	20
5. Instalación OpenSSH, manexo de scp e sftp e WinSCP en Windows.	39
6. Conclusións	43

1. Obxectivos

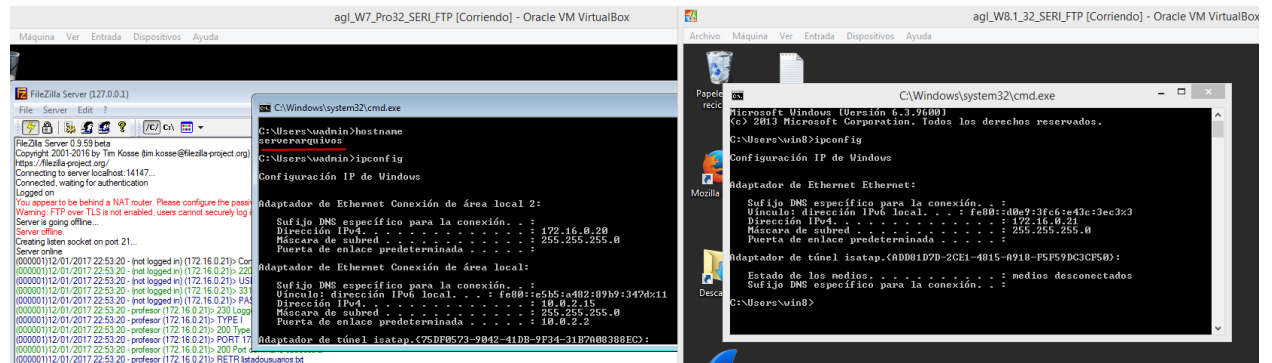
O obxectivo principal será instalar e configurar un servidor co servizo FTP tanto en contornas Linux como Microsoft Windows.

Ver as diferencias de FTP, FTPS e SFTP. Interactuar con eles e configuralos.

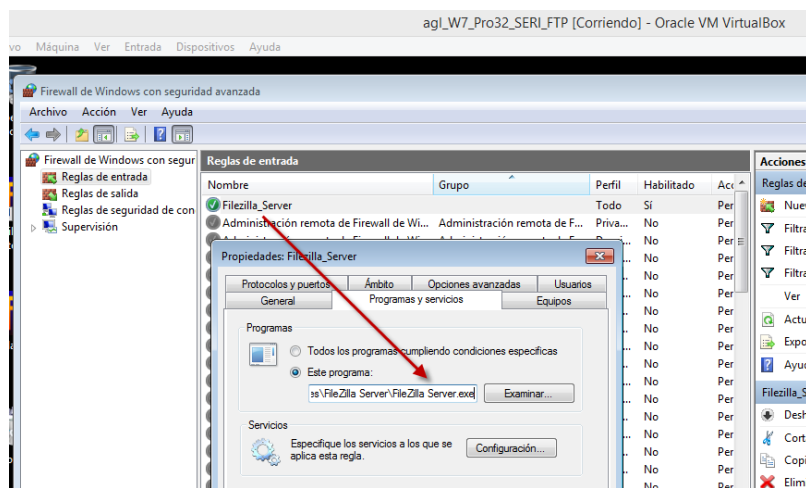
Traballar tamén coas distintas ferramentas clientes para a conexión e transferencia de ficheiros, ferramentas gráficas tipo Filezilla ou WinSCP, e ferramentas en liña de comandos tipo FTP, SFTP e SCP.

2. Descarga automática dun arquivo dende un servidor FTP

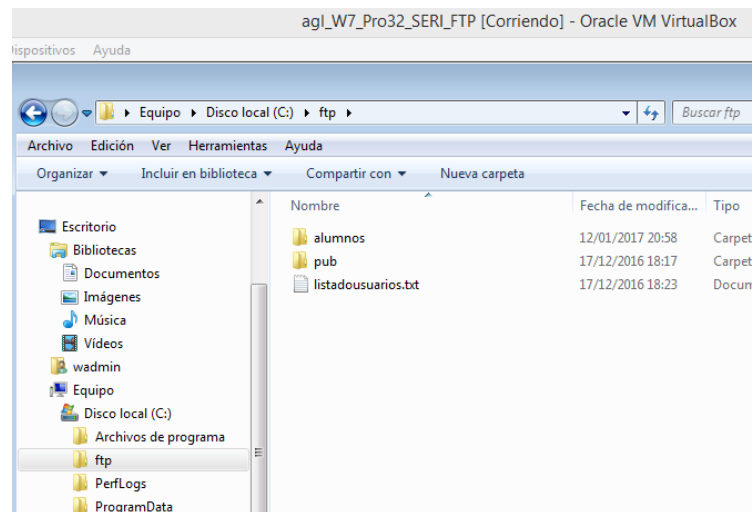
- Nome do equipo: serverarquivos
- IP do equipo: 192.168.10.250/24



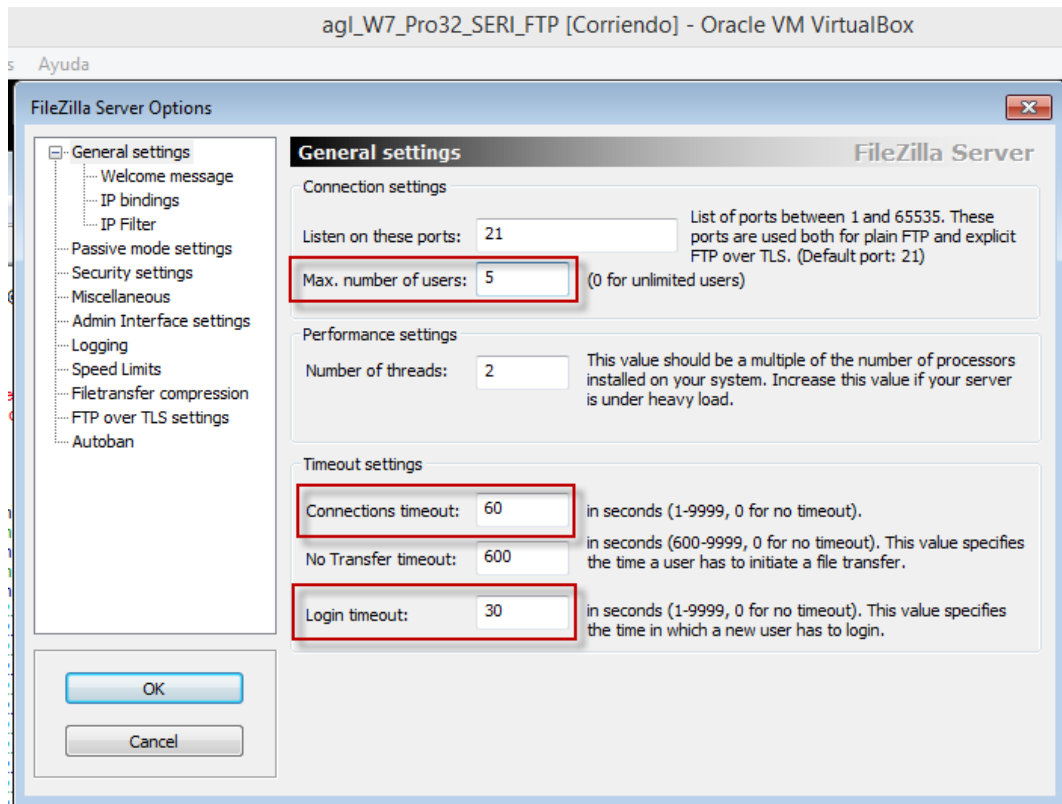
- SW servidor Filezilla Server



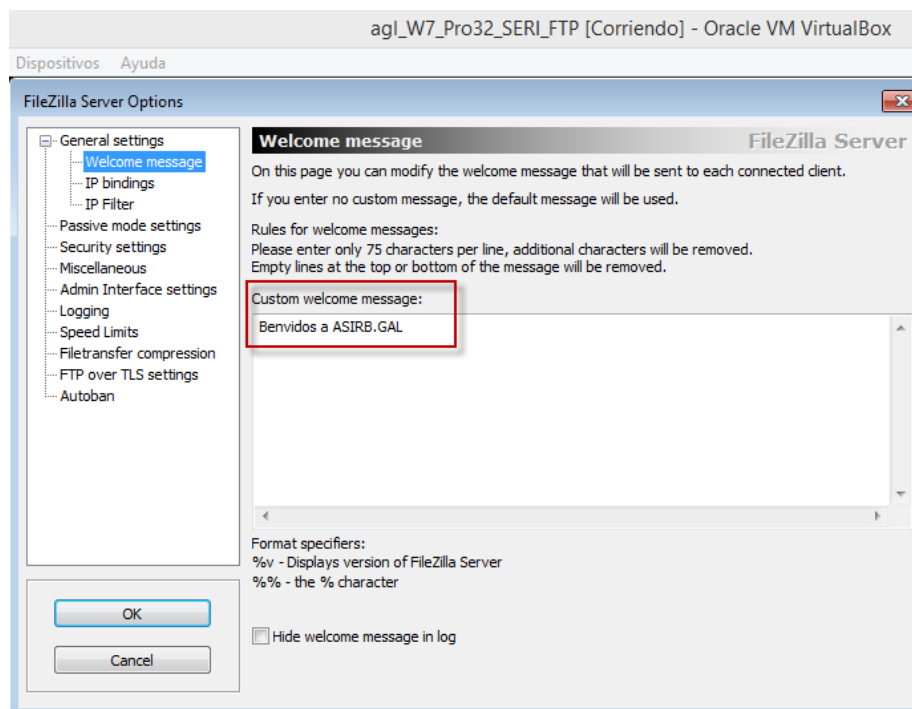
Esquema de directorios



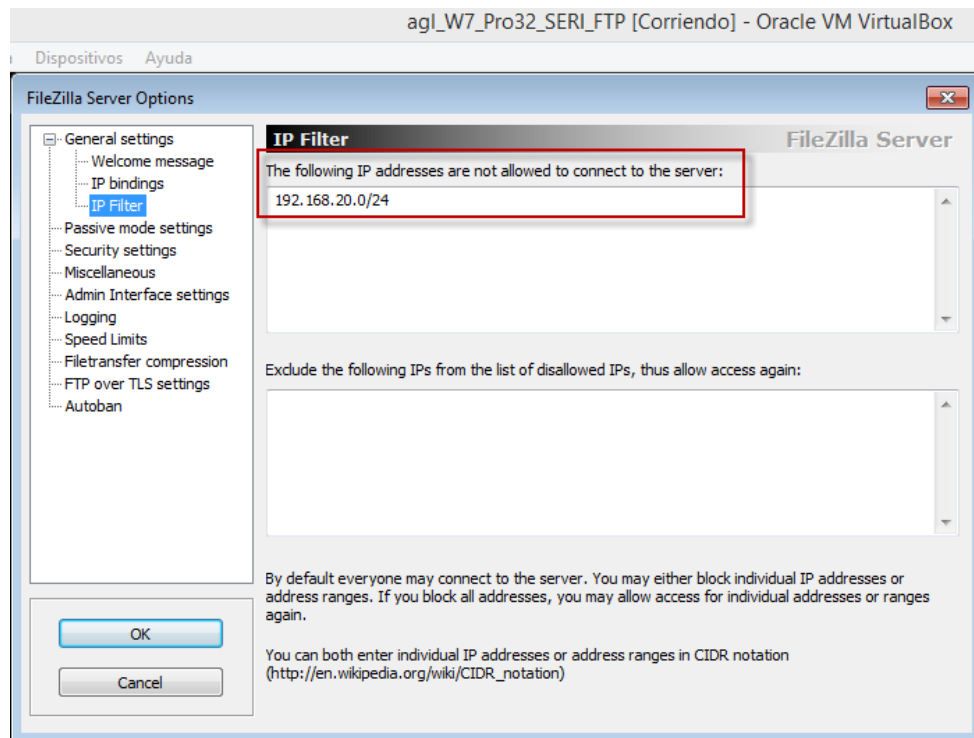
- Só se permiten 5 conexións simultáneas ao servidor
- O cliente ao conectarse ten como máximo 30 segundos para facer login
- Período máximo de inactividade de 1 minuto. Pasado ese tempo desconectarase ao cliente



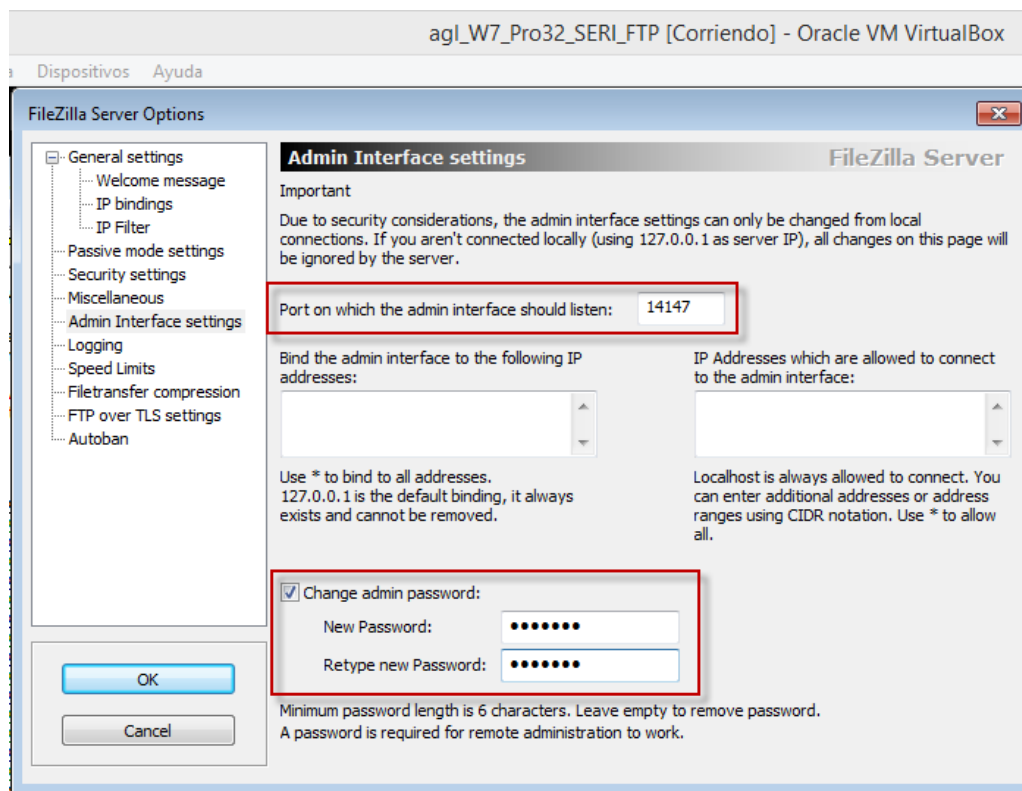
- A mensaxe de benvinda ao iniciar sesión será “Benvidos a ASIRB.GAL”



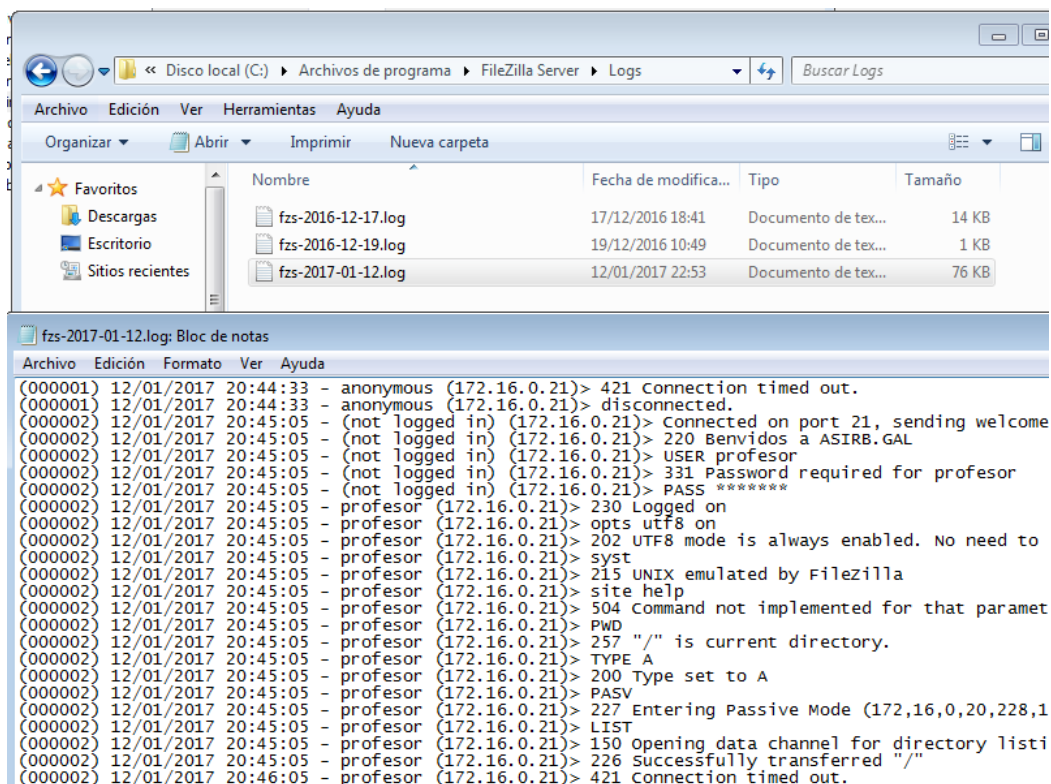
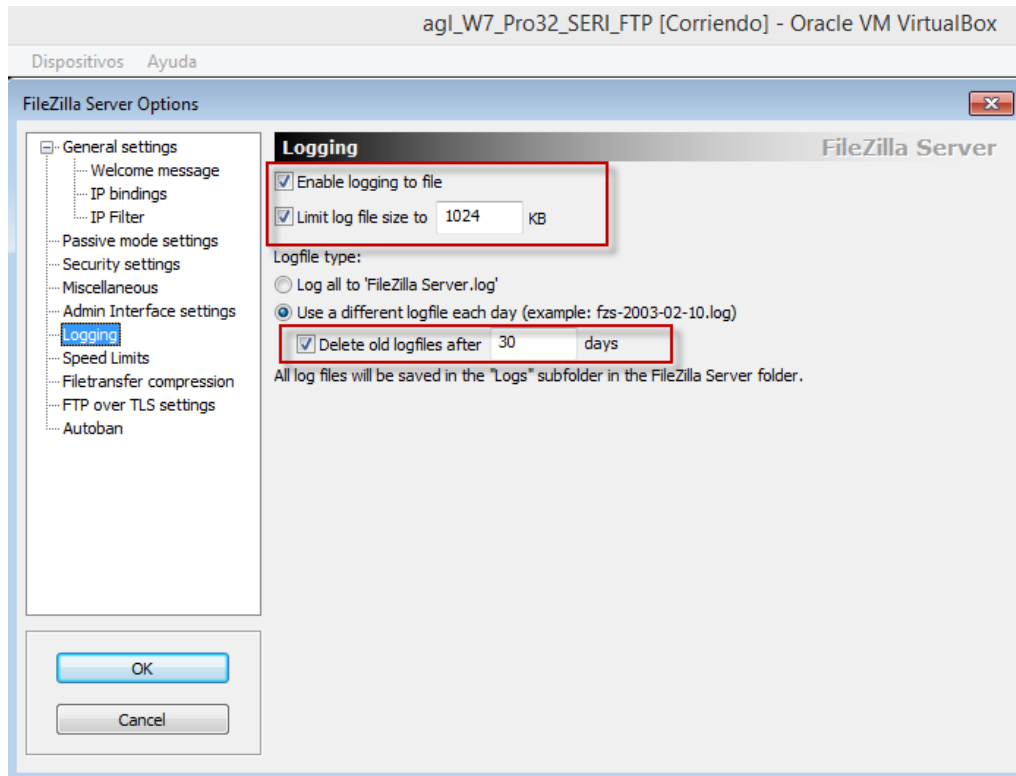
- Non permitas conexións da rede 192.168.20.0/24. Emprega a notación CIDR para facelo



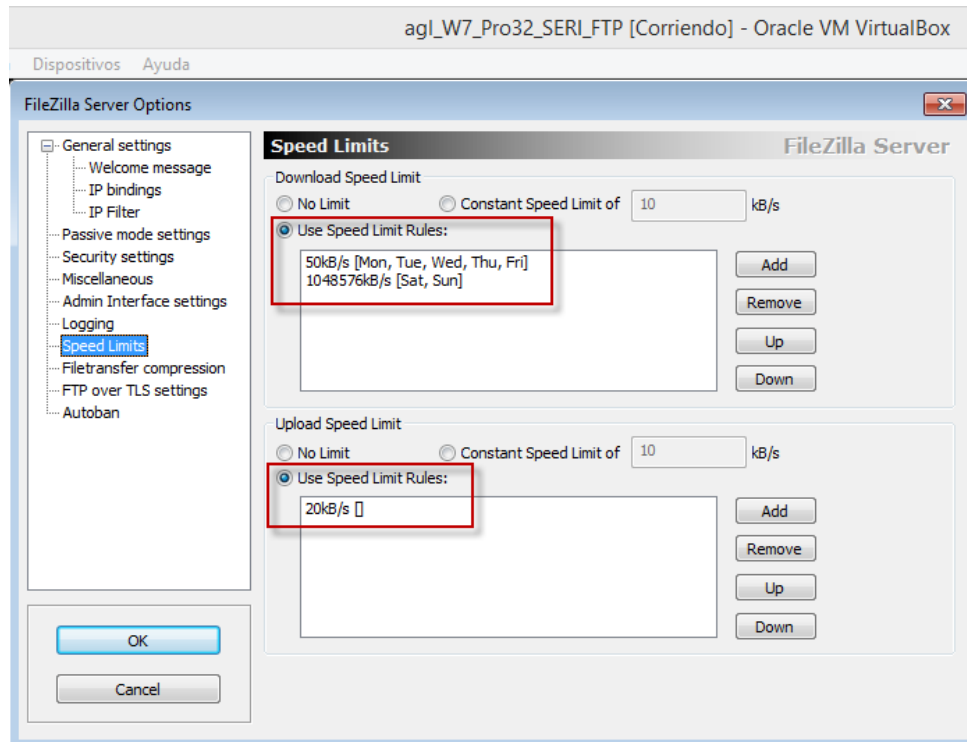
- A contrasinal de administración do Filezilla Server (por defecto emprega o porto 14147 para administralo) será abc123.



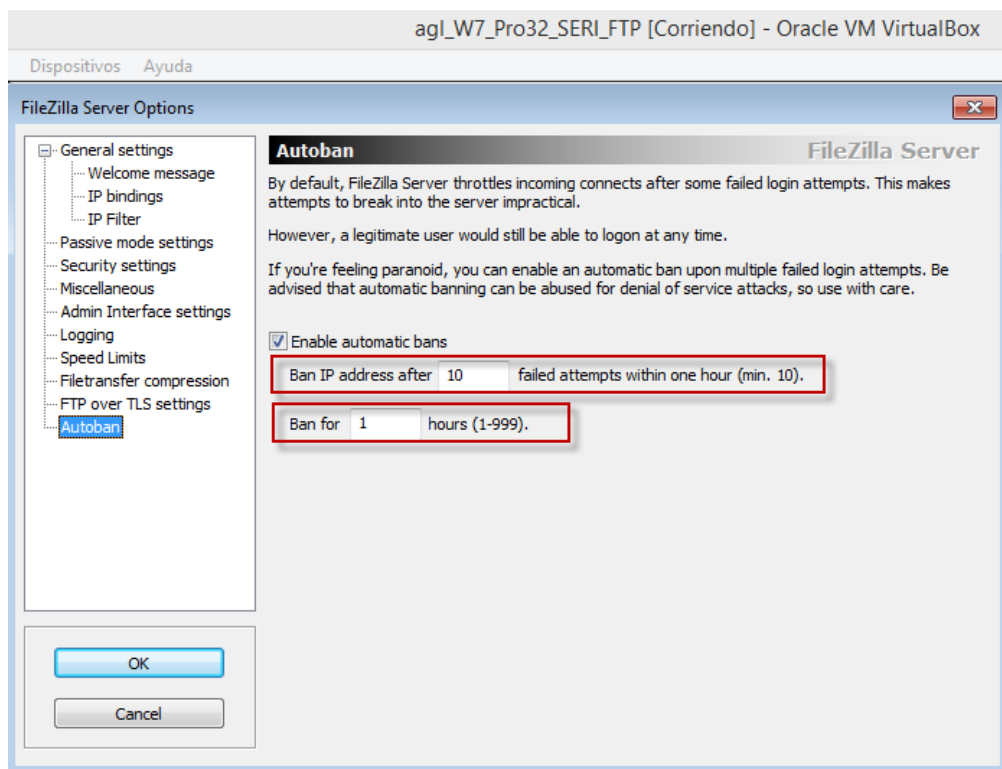
- Habilitarase un log con ficheiros de como moito 1 MB. Crearase un ficheiro de log por día e eliminaranse ao cabo de 30 días.



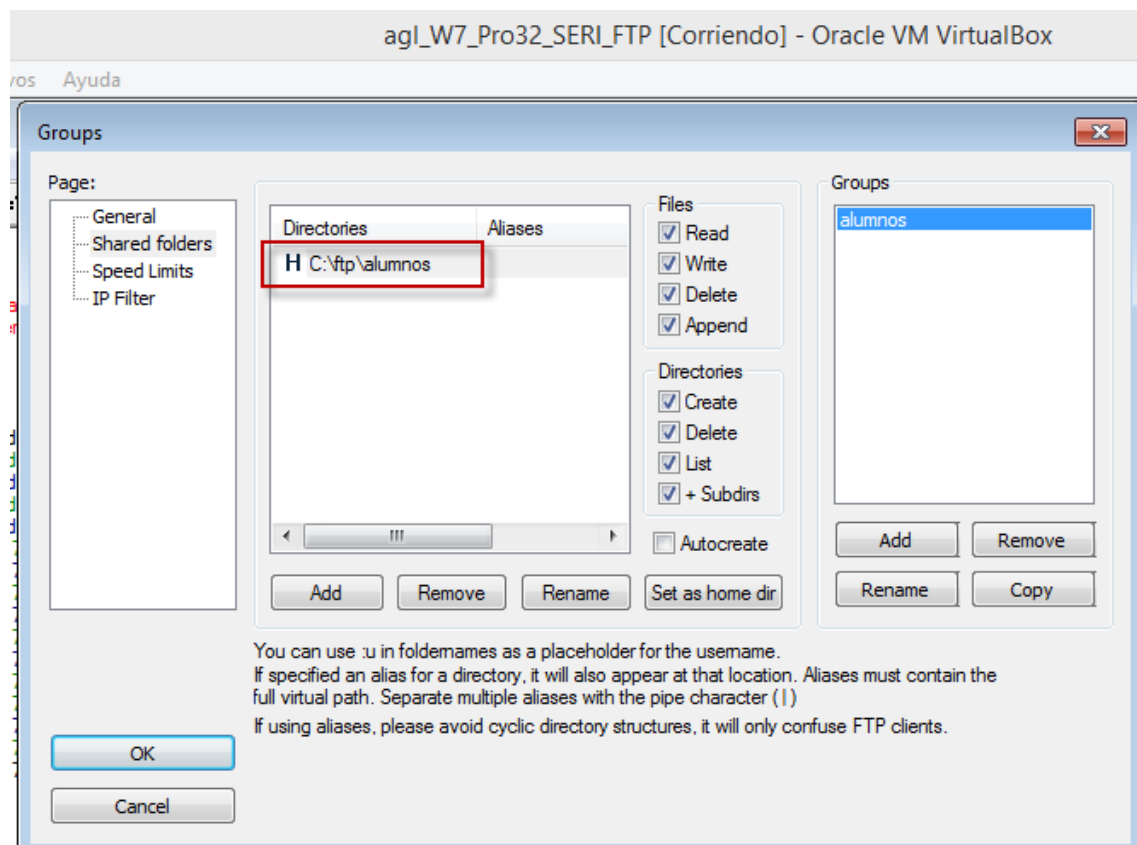
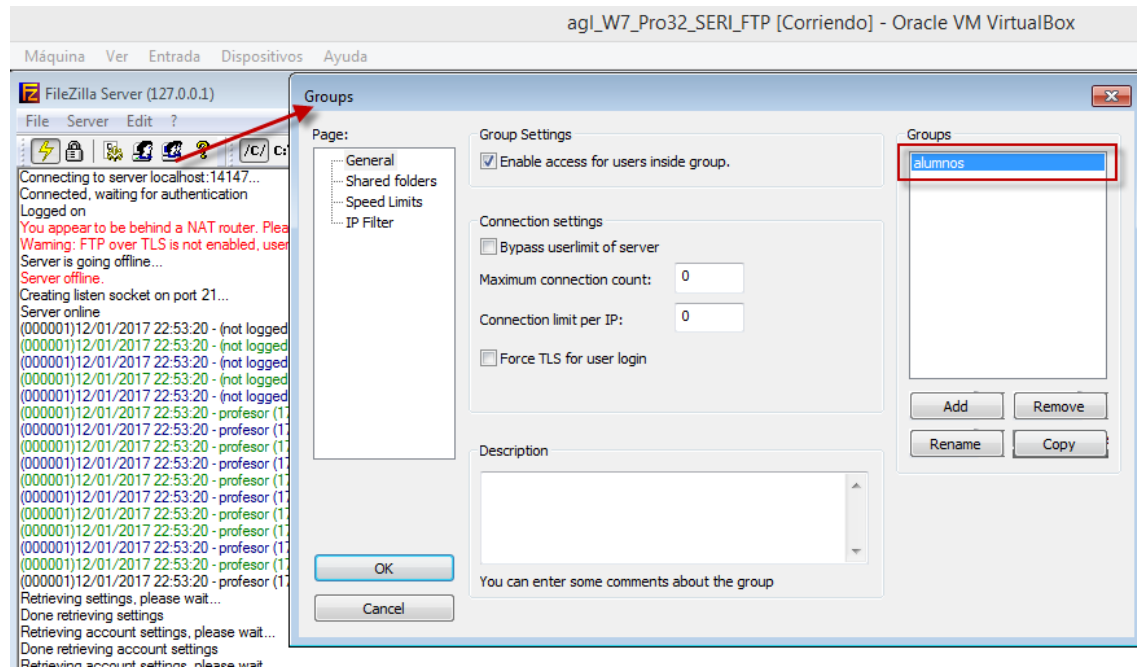
- A velocidade de baixada do servidor será de 50 KB de luns a venres e máxima durante a fin de semana. Respecto á velocidade de subida será de 20 KB sempre.

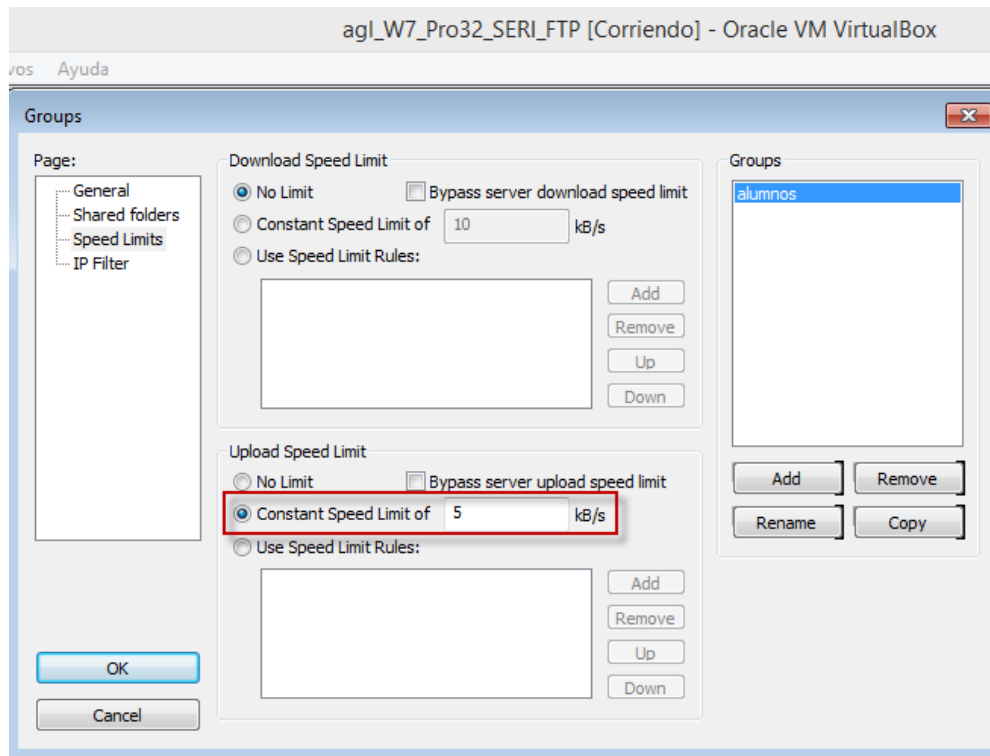


- Banearanse durante 1 hora as conexións que fallen 10 veces á hora de autenticarse.

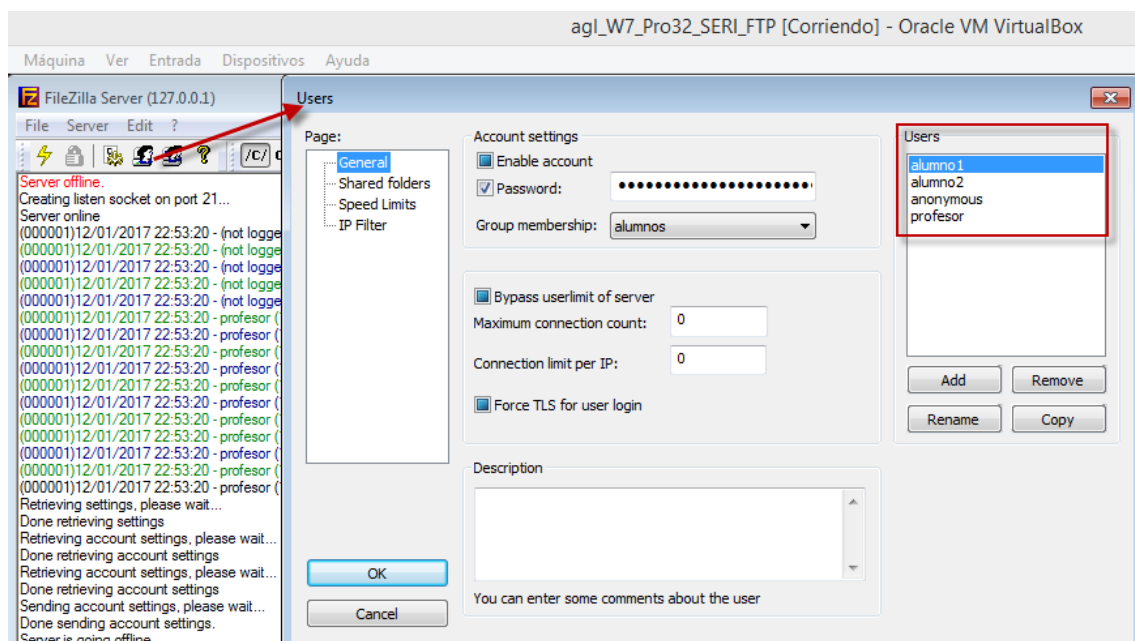


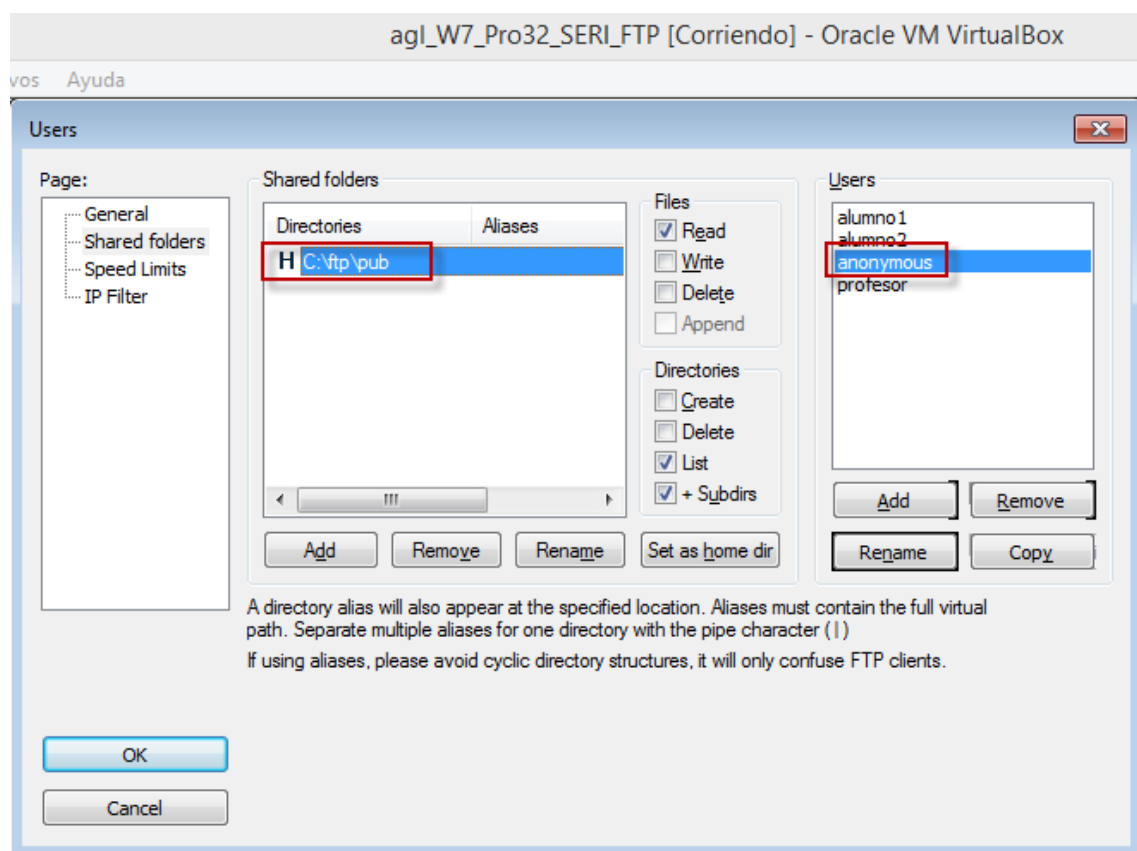
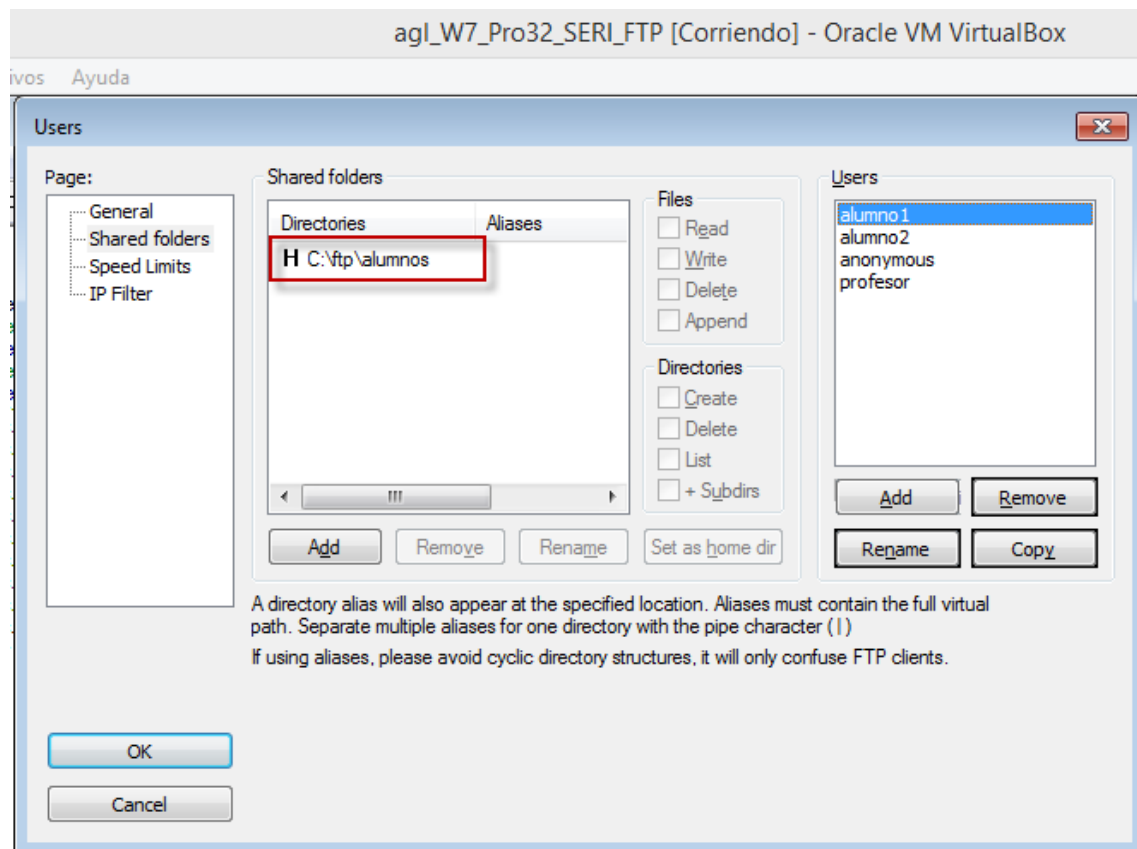
- Usuarios **alumno1** e **alumno2** (con contrasinal *abc123*.)
 - Pertencerán a un grupo denominado **alumnos**.
 - O cartafol predeterminado para os membros do grupo alumnos será **C:\ftp\alumnos**, con permisos de lectura e escritura de ficheiros e cartafoles.
 - A velocidade de subida para todos os alumnos será de 5 KB.

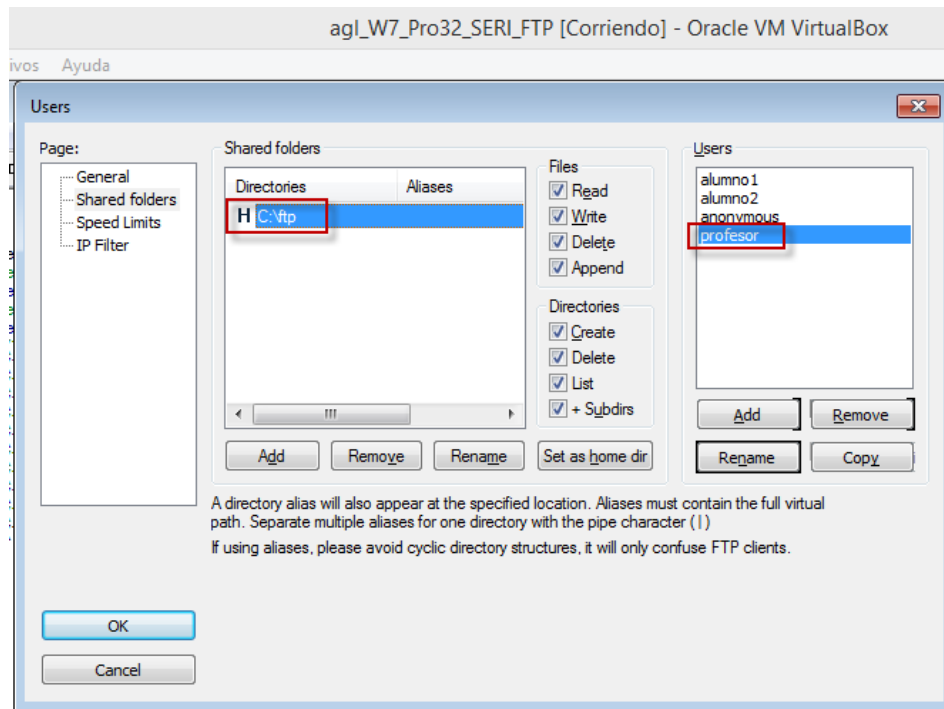




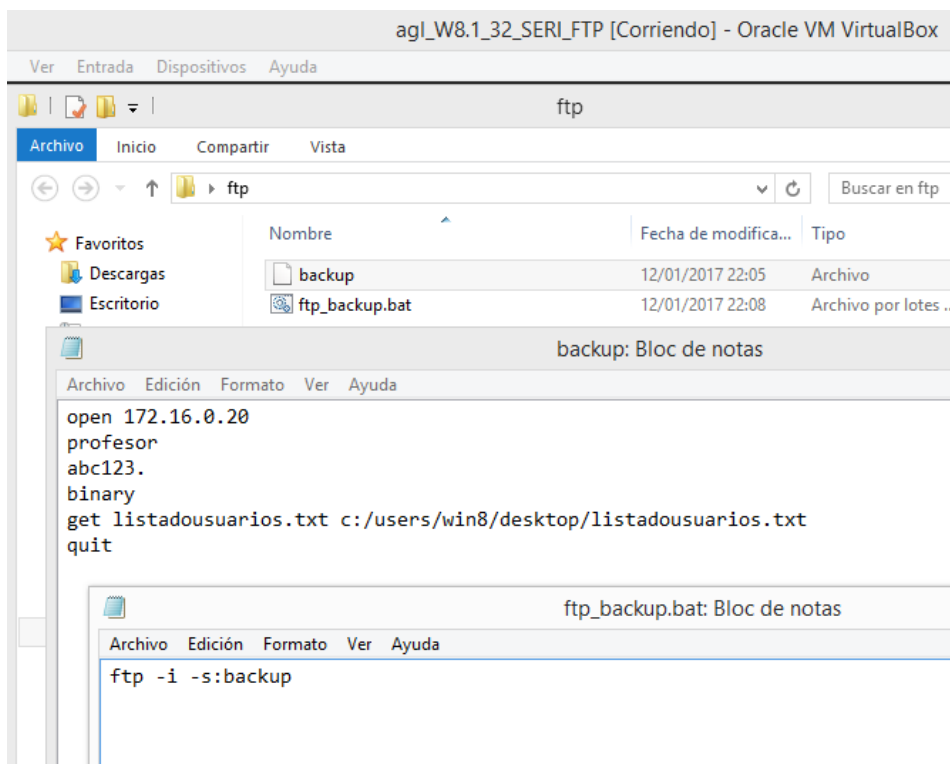
- Usuario anónimo (**anonymous**) sen contrasinal
 - Directorio predeterminado **C:\ftp\pub**. Só terá permisos de lectura.
 - Non pertence a ningún grupo
- Usuario **profesor** (con contrasinal *abc123*.)
 - Cartafol predeterminado **C:\ftp**. Terá permisos de lectura, escritura, borrado e modificación de ficheiros e cartafoles.
 - Non pertence a ningún grupo

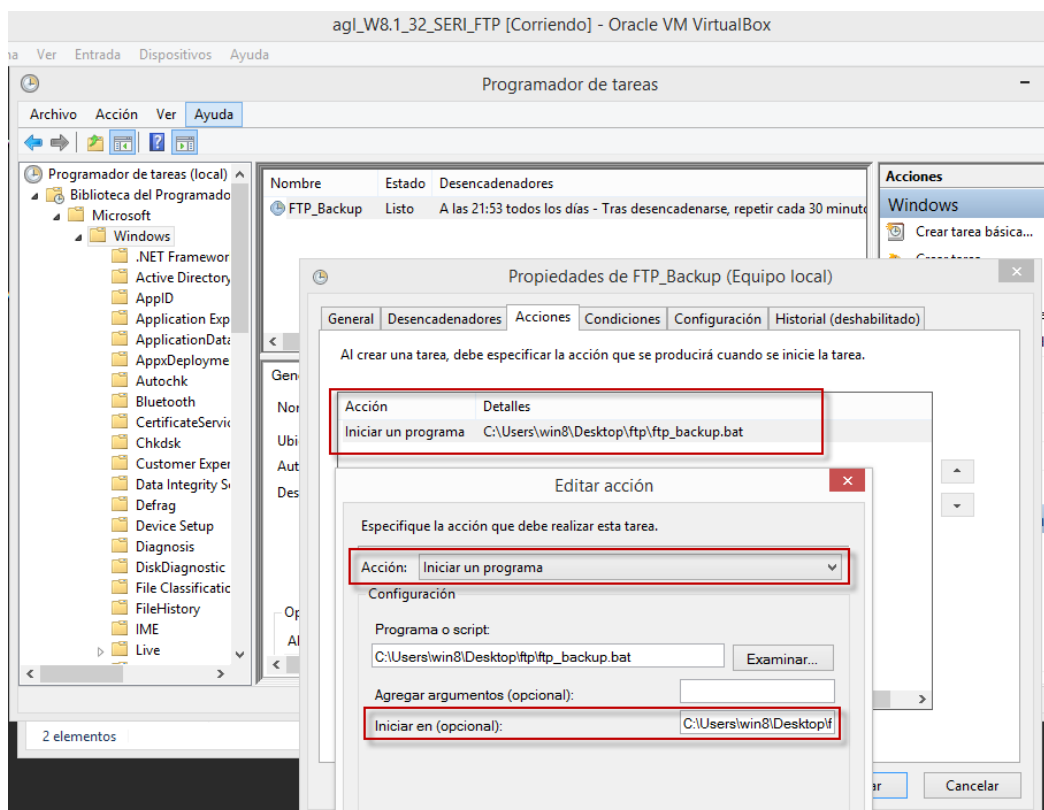
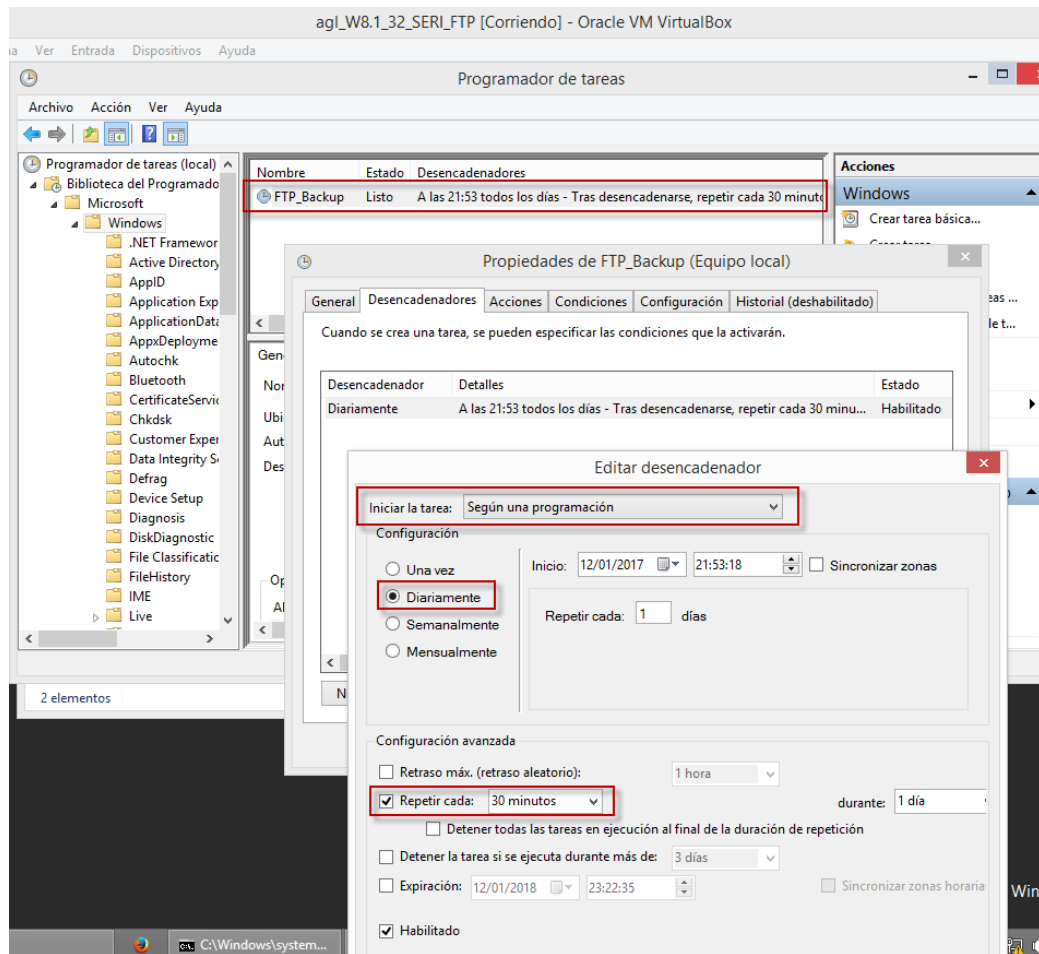






- En **C:\ftp** habrá colgado un ficheiro denominado **listadousuarios.txt**
 - No equipo cliente, que poderá ser un PC con calquera versión de Windows a partir de XP, deberás crear unha tarefa automatizada que cada 30 minutos descargue o arquivo listadousuarios.txt no directorio %userprofile%\Desktop e que sobrescriba o anterior existente. Debes tentalo de dúas formas:
 - Crear un arquivo **.bat** que empregue o ftp de modo **desatendido**. Procura información na URL <http://www.robvanderwoude.com/ftp.php>

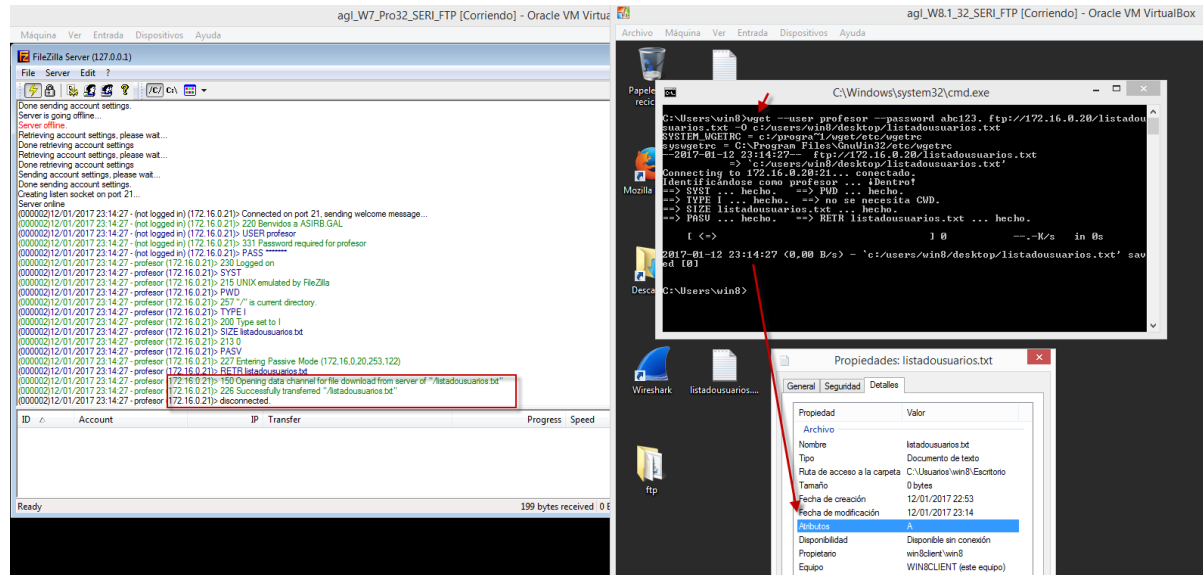




- Crear un archivo **.bat** que emplee o comando **wget**.

wget --user profesor --password abc123. ftp://172.16.0.20/listadousuarios.txt -O c:/users/win8/desktop/listadousuarios.txt

O modificador “-O” e para que sobrescriba o arquivo cada vez que o descargue.



3. Instalación e configuración servidor VSFTPD

VSFTP (Very Secure FTP) e un FTP sobre SSL (FTPS).

Actualizamos os repositorios e instalamos o servidor VSFTP:

```
sudo apt-get update
```

```
sudo apt-get install vsftpd
```

Comprobamos que o servizo está instalado e funcionando no sistema.

Facemos un `service status` do servizo vsftpd para ver o seu estado actual.

```
ps -ef
```

ps: Mostra unha instatánea dos procesos actuais.

-e: Visualiza información sobre "todos" os procesos del sistema.

-f: Visualiza os parámetros cos levantou o proceso.

```
netstat -ltn
```

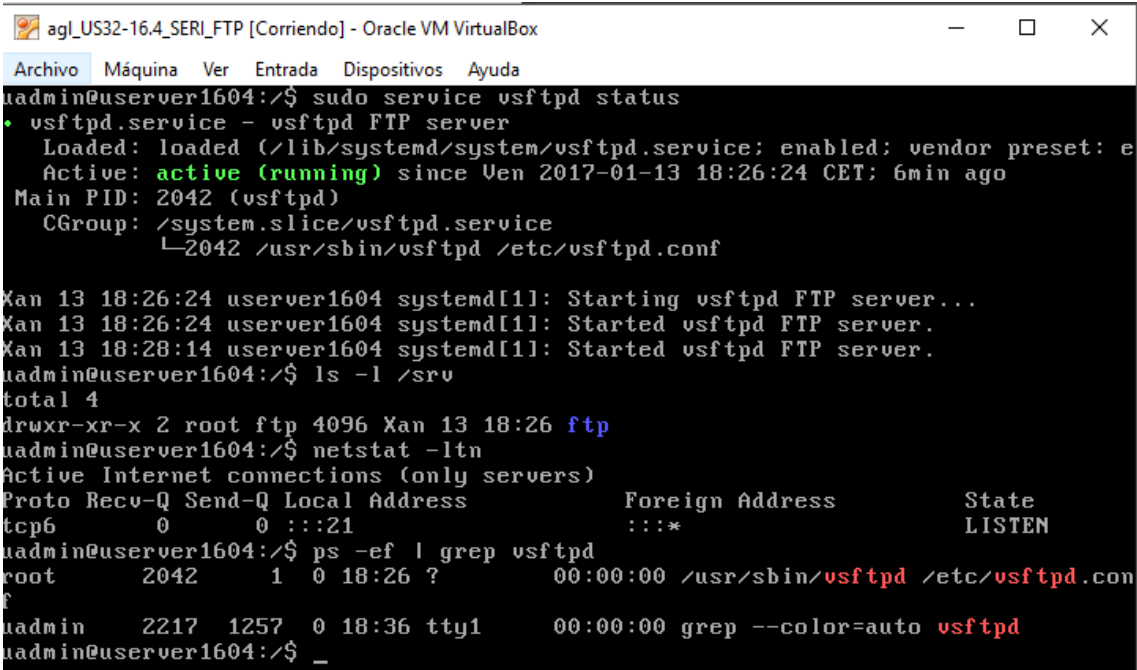
netstat: Lista conexións actuais.

-l: Mostra os server sockets que están en modo escoita.

-t: Lista conexións soamente TCP.

-n: Non resolve nomes en xeral.

Para filtrar máis concretamente, con `grep` buscamos o nome do servizo.



```

agL_US32-16.4_SERI_FTP [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
uadmin@userver1604:/$ sudo service vsftpd status
• vsftpd.service - vsftpd FTP server
   Loaded: loaded (/lib/systemd/system/vsftpd.service; enabled; vendor preset: e
   Active: active (running) since Ven 2017-01-13 18:26:24 CET; 6min ago
   Main PID: 2042 (vsftpd)
   CGroup: /system.slice/vsftpd.service
           └─2042 /usr/sbin/vsftpd /etc/vsftpd.conf

Xan 13 18:26:24 userver1604 systemd[1]: Starting vsftpd FTP server...
Xan 13 18:26:24 userver1604 systemd[1]: Started vsftpd FTP server.
Xan 13 18:28:14 userver1604 systemd[1]: Started vsftpd FTP server.
uadmin@userver1604:/$ ls -l /srv
total 4
drwxr-xr-x 2 root ftp 4096 Xan 13 18:26 ftp
uadmin@userver1604:/$ netstat -ltn
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp6      0      0 :::21                   :::*                     LISTEN
uadmin@userver1604:/$ ps -ef | grep vsftpd
root      2042      1  0 18:26 ?                00:00:00 /usr/sbin/vsftpd /etc/vsftpd.conf
uadmin    2217    1257  0 18:36 tty1          00:00:00 grep --color=auto vsftpd
uadmin@userver1604:/$ _

```

Configuramos o ficheiro principais de configuración do servizo vsftpd:
`/etc/vsftpd.conf`

- Os usuarios anónimos poderán subir arquivos:
Habilitamos os usuarios anónimos, habilitamos que podan escribir e subir:

```
anonymous_enable=YES  
anon_upload_enable=YES
```

- Os usuarios locais poderán subir e descargar arquivos:

```
local_enable=YES  
write_enable=YES
```

- Só poderán conectarse os usuarios locais pepe e jose (créaos primeiro), o usuario pepe NON estará engaiolado no seu directorio home, pero o resto de usuarios si:

```
allow_writeable_chroot=YES  
chroot_local_user=YES  
chroot_list_enable=YES  
chroot_list_file=/etc/vsftpd.chroot_list
```

No ficheiro anterior referenciado incluimos o usuario pepe de modo que non estará engaiolado.

- Cambia a mensaxe de benvida do servidor para que diga “Escues”:

```
ftpd_banner="Escues"
```

- Aos usuarios anónimos, ao acceder ao seu directorio /home, deberá enviarlle unha mensaxe indicando “Directorio público de servidor”:

Creamos no directorio no que se conectarán os usuarios anónimos por defecto /srv/ftp o ficheiro .message co texto anterior. A continuación engadimos a directiva:

```
dirmessage_enable=YES
```

- Se unha conexión FTP está inactiva máis de 50 segundos pecharase a conexión:

```
idle_session_timeout=50
```

- Permitiranse un máximo de 5 conexións simultáneas ao servidor:

```
max_clients=5
```

- O servidor só poderá ocupar 10MB/s de largo de banda:

```
local_max_rate=10000000
```

- Os usuarios anónimos só poderán empregar 1MB/s de largo de banda:

```
anon_max_rate=1000000
```


- Habilita FTPS, e non permitas a conexión de clientes FTP que non soporten SSL, excepto anonymous:

Unha vez creado certificado con openssl:

```
sudo openssl req -x509 -nodes -days 365 -newkey rsa:1024 -keyout  
/etc/ssl/private/vsftpd.pem -out /etc/ssl/certs/vsftpd.pem
```

- As directivas serían:

```
rsa_cert_file=/etc/ssl/certs/vsftpd.pem  
rsa_private_key_file=/etc/ssl/private/vsftpd.pem  
ssl_enable=YES  
allow_anon_ssl=YES  
force_local_data_ssl=YES  
force_local_logins_ssl=YES  
ssl_tlsv1=YES  
ssl_sslv2=NO  
ssl_sslv3=NO
```

- Habilitar a codificación UTF8, para poder visualizar correctamente os mensaxes:

```
utf8_filesystem=YES
```

OPCIONAL

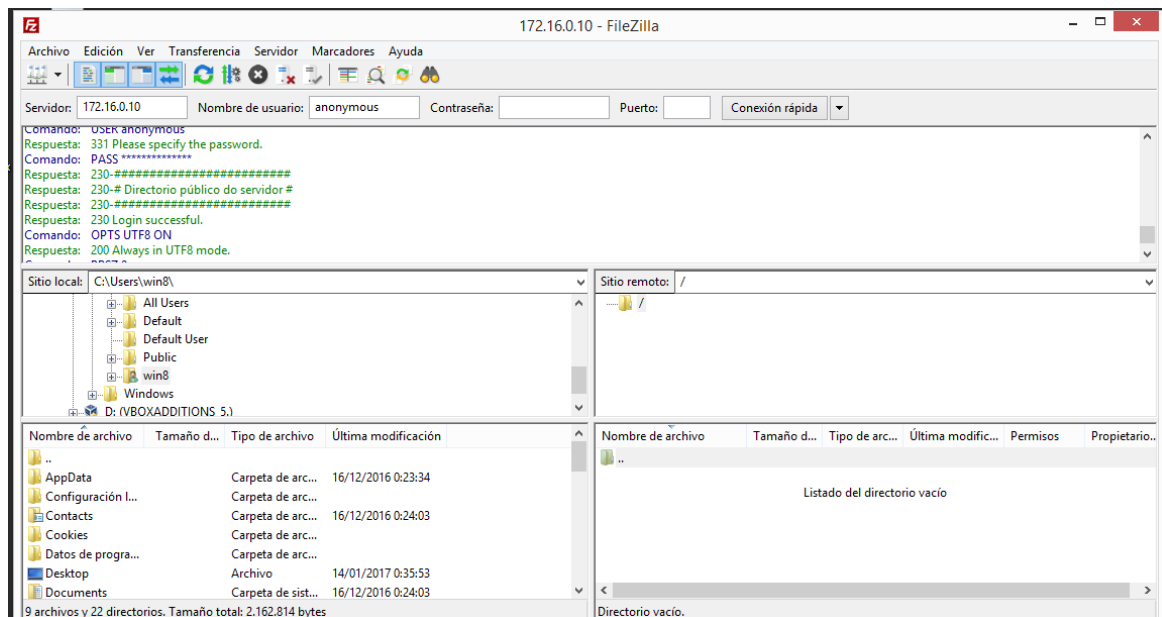
- Denegar o acceso a un usuario en concreto ou grupo deles.

```
userlist_enable=YES  
userlist_file=/etc/vsftpd.user_list
```

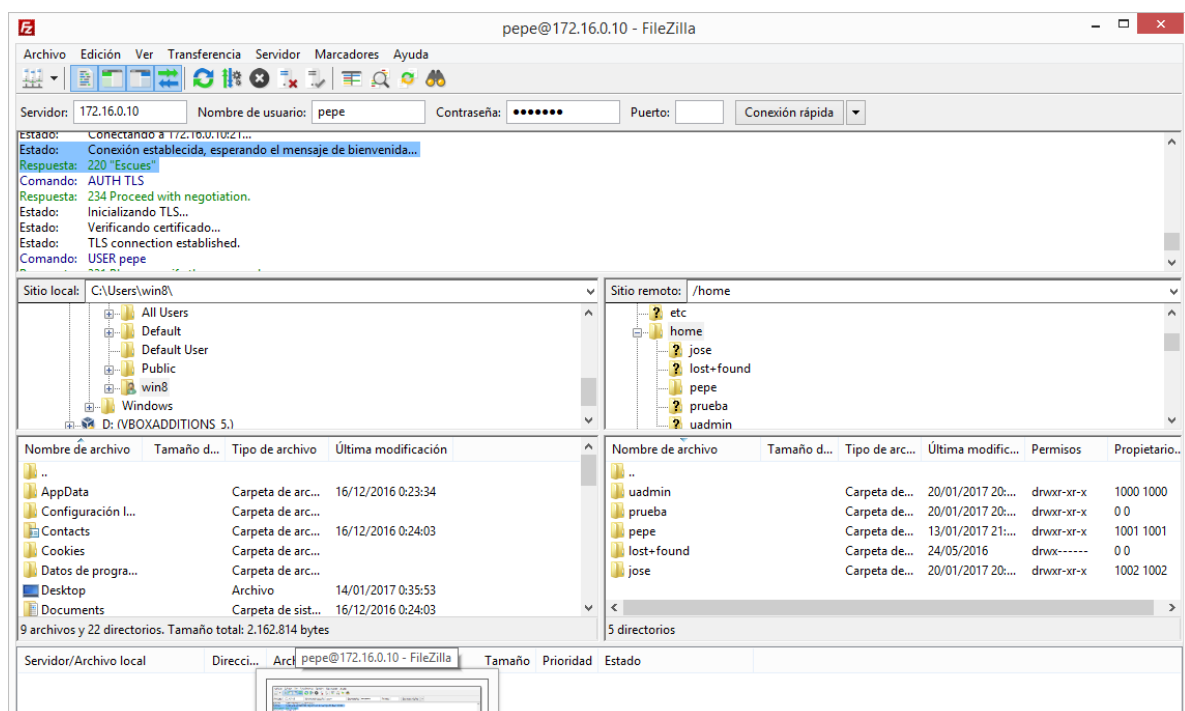
No ficheiro de list anterior iría o nome do usuario a denegar o acceso, neste caso probouse co usuario "uadmin".

- Proba a ferramenta Filezilla e WinSCP para conectarte:

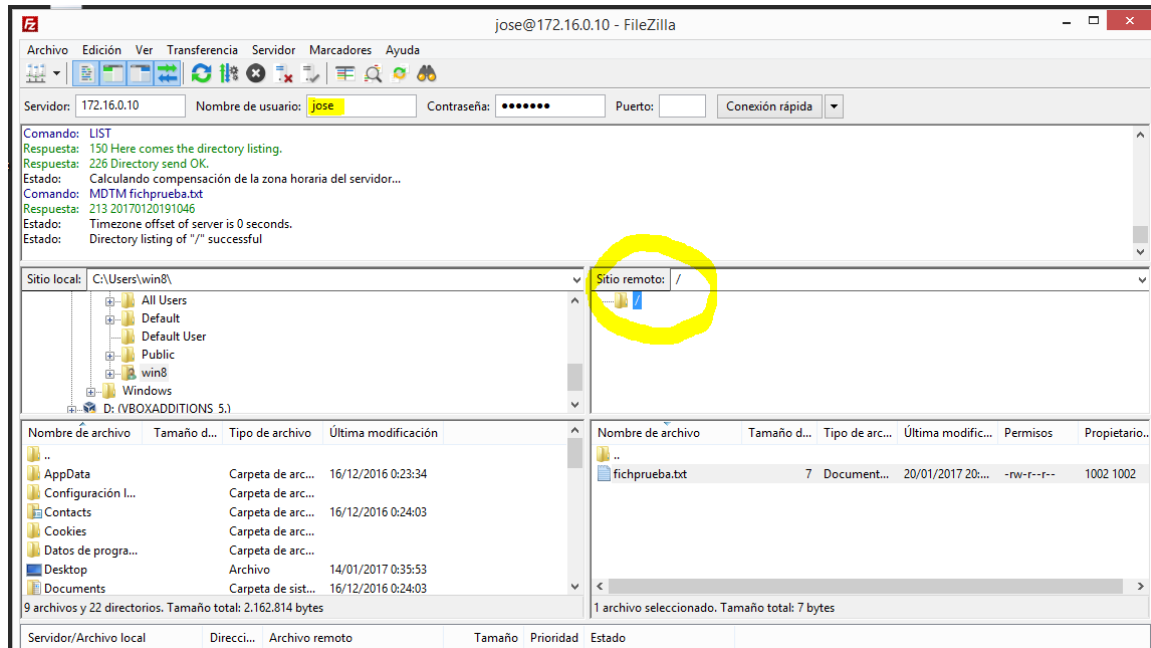
Mensaxe de benvinda para os usuarios “anónimos”. A sua raíz será /srv/ftp



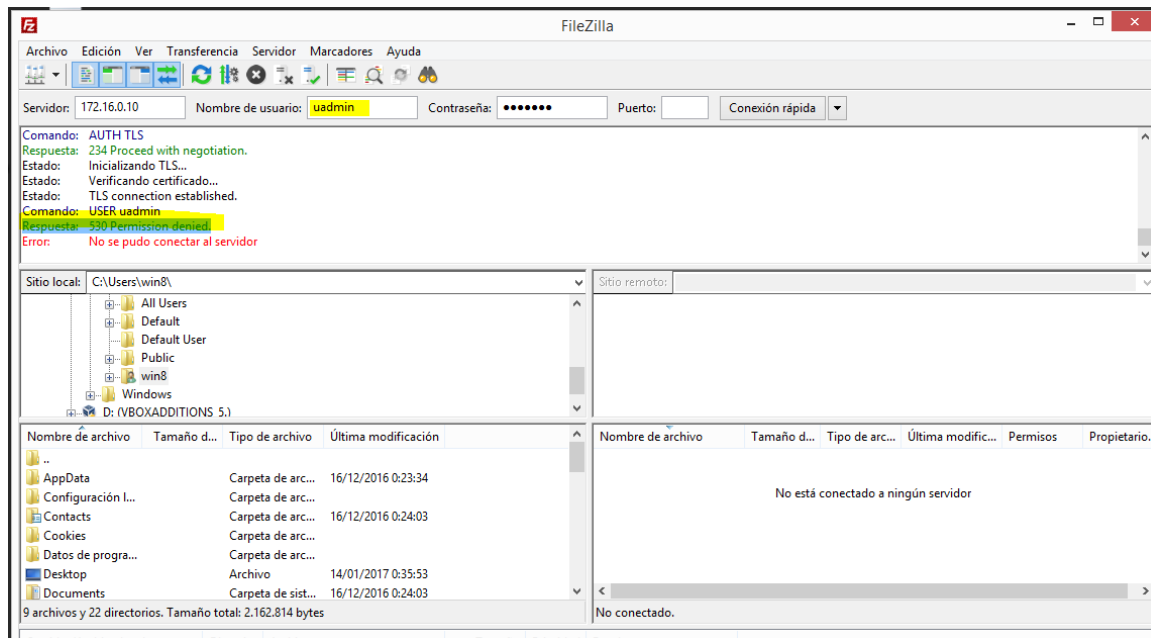
O usuario “pepe” é único que non está enxaulado no seu directorio polo que pode xestionar a xerarquía de directorios.



O usuario “jose” está enxaulado no seu home.

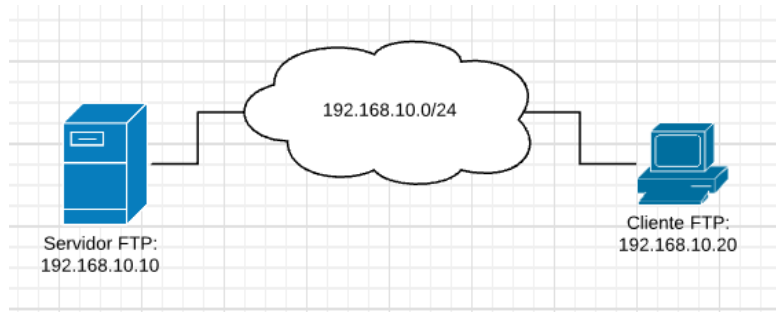


O usuario “wadmin” non se pode conectar pese a que é un usuario local, incluído na lista de usuarios denegados.

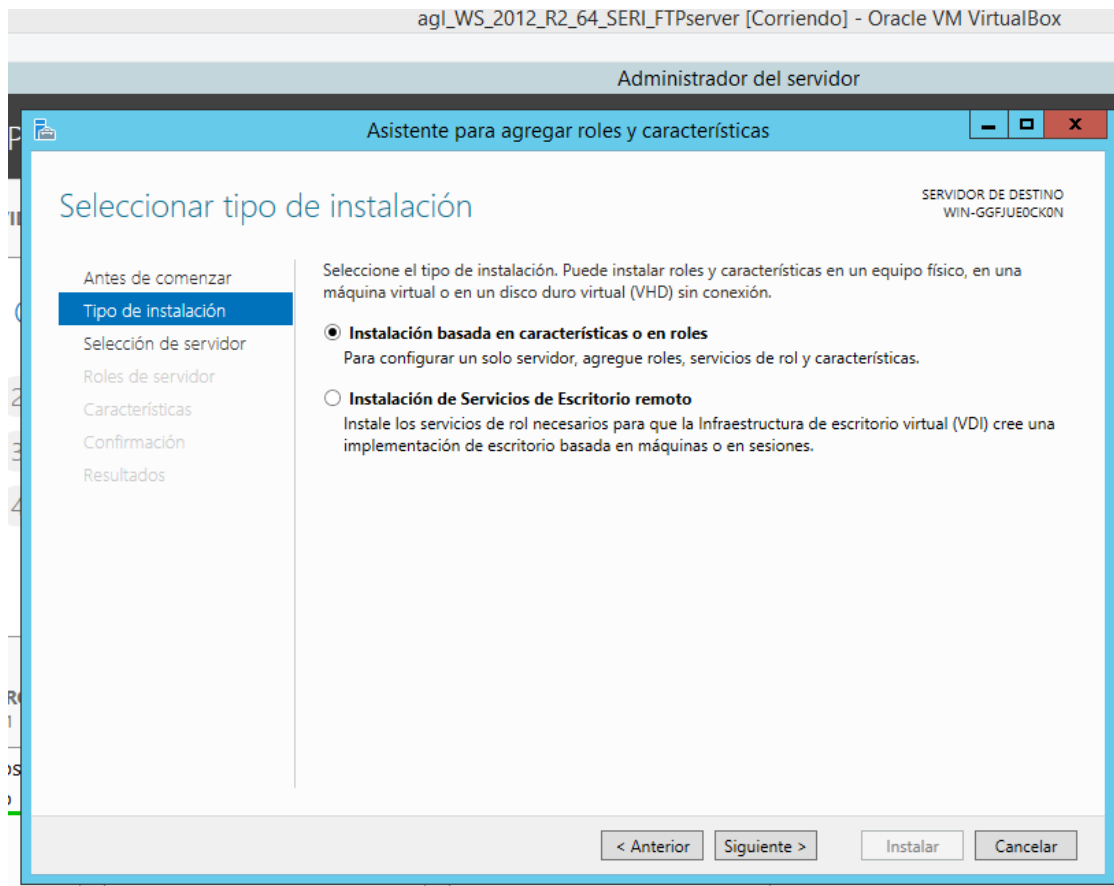


4. Instalación e configuración servidor FTP en Windows Server 2012

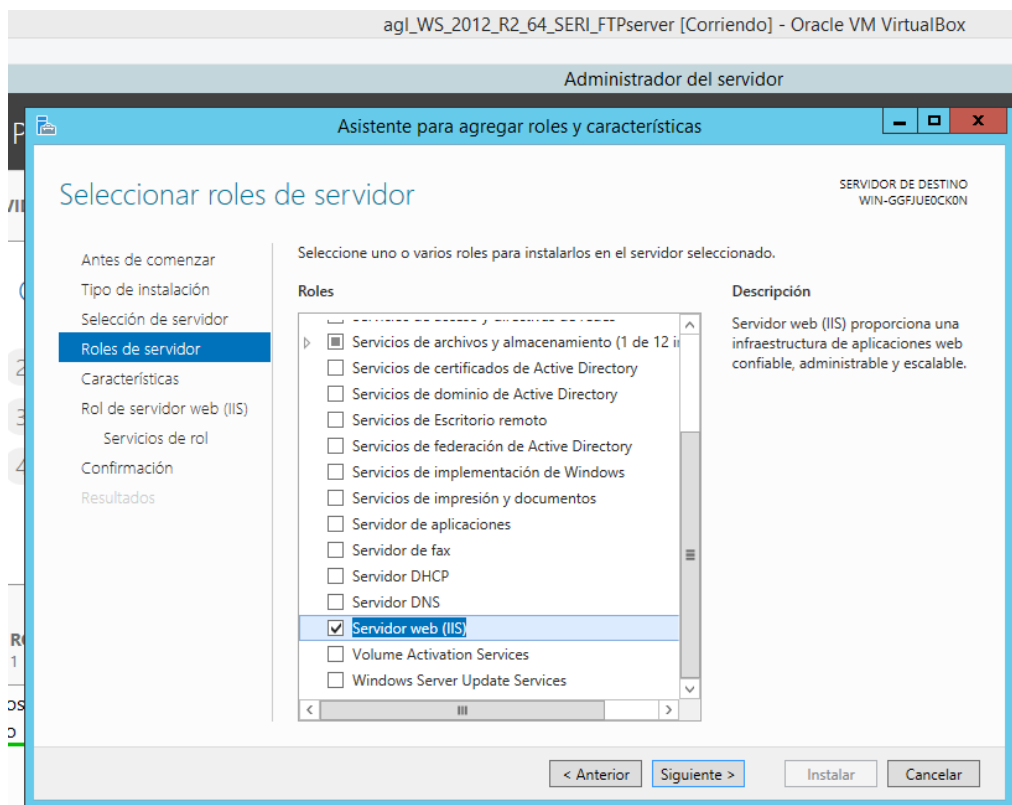
Segundo o seguinte esquema de rede instalárase e configúrase un servidor FTP sobre Windows Server 2012.



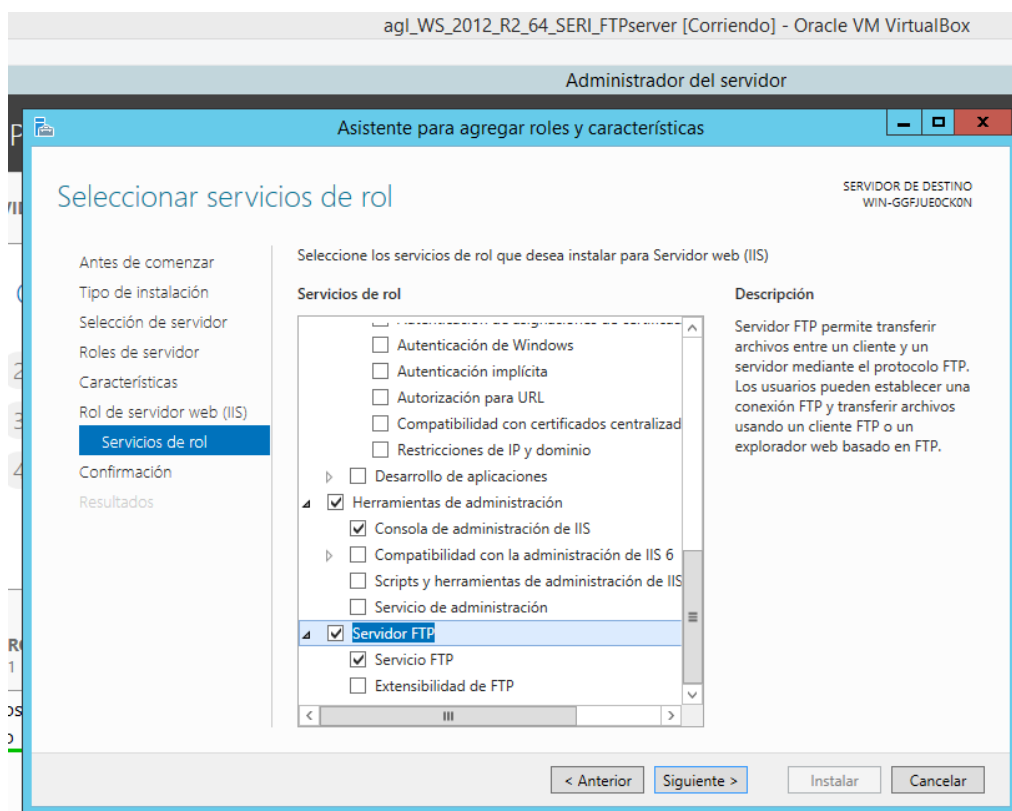
Agregamos un nova característica e rol.

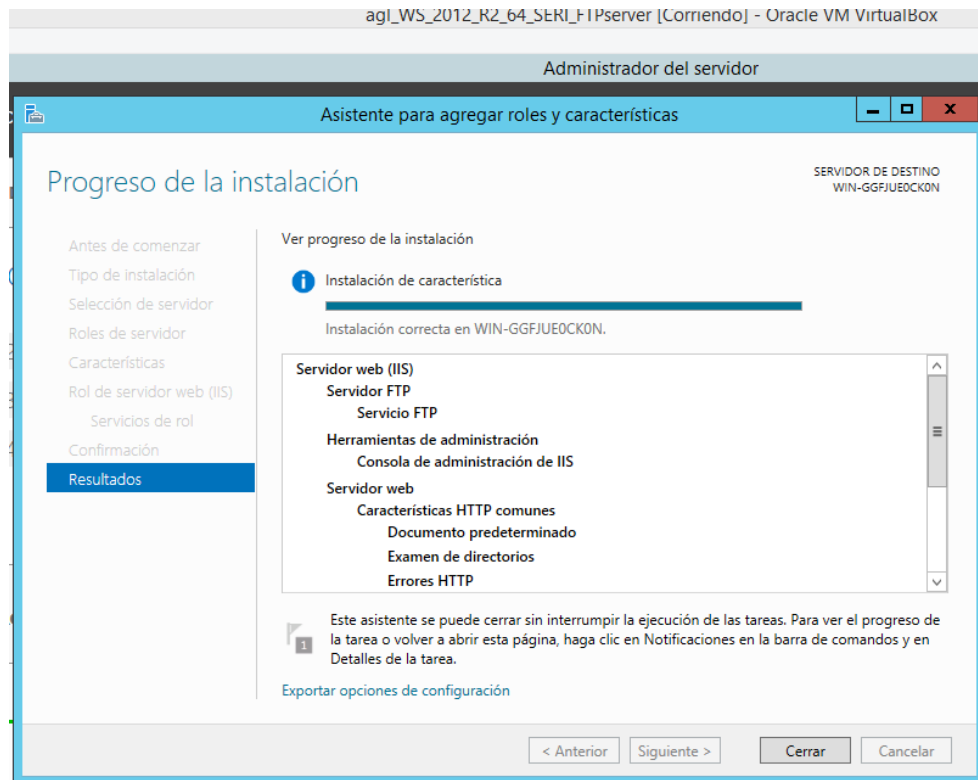


El rol será IIS (Internet Information Services).

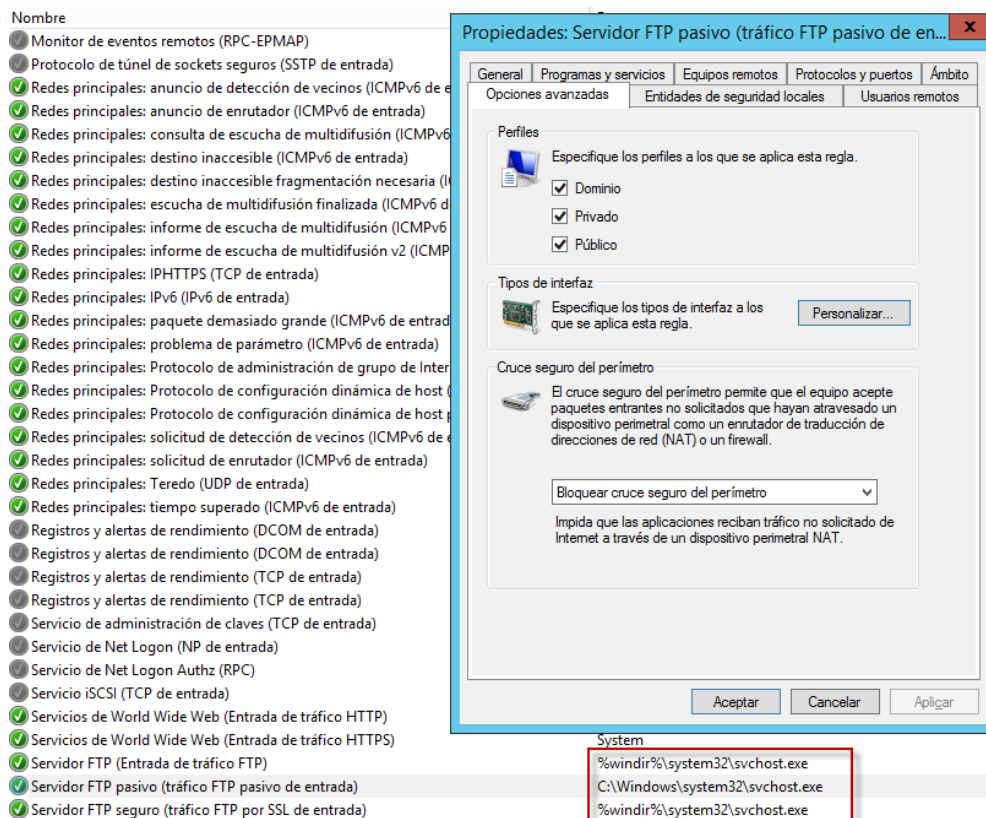


Como característica "Servidor FTP".



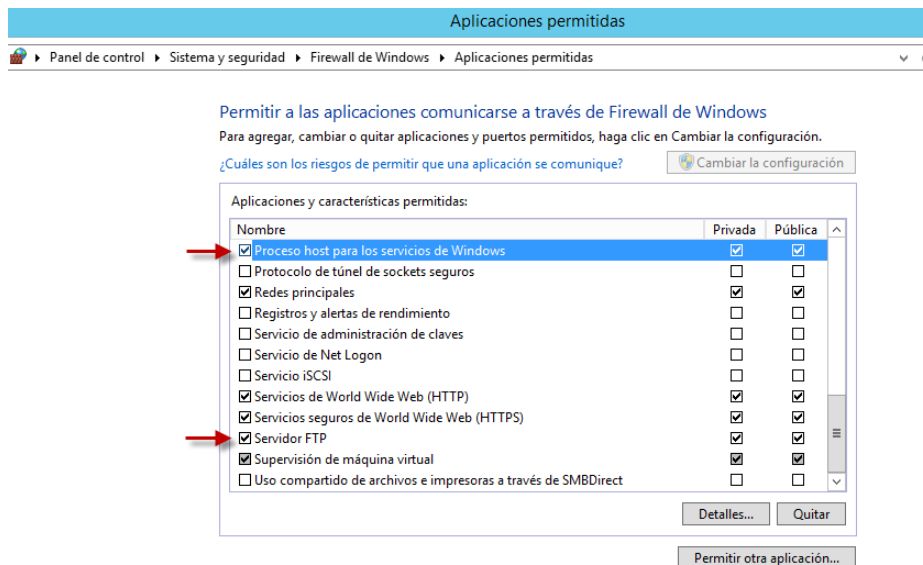


Una vez instalado, configuramos las reglas en el Firewall de Windows o tal por defecto ya se autoconfigura en el momento de instalar el servicio FTP.

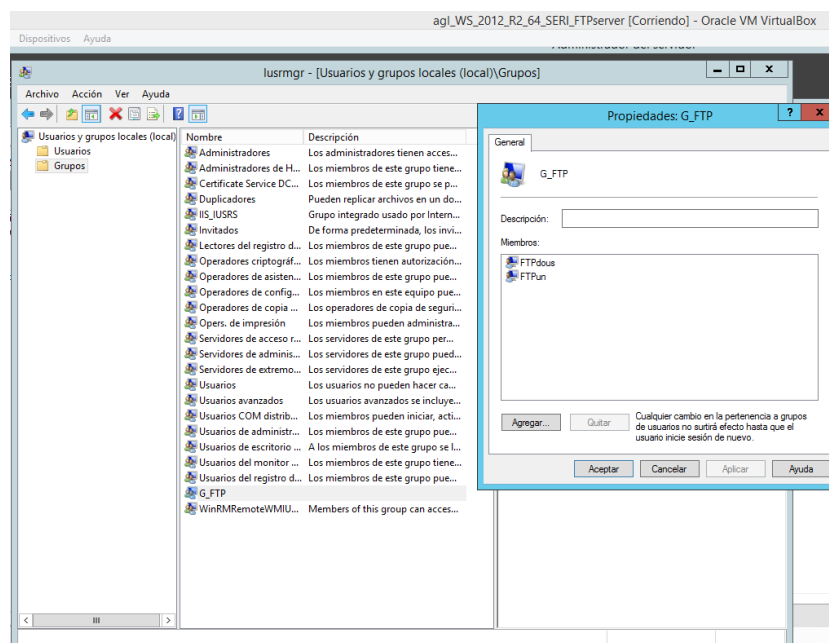


Na configuración de aplicación permitidas comprobaremos que o servidor FTP está incluído, e incluiremos de forma manual o proceso svchost.exe ubicado en “%systemroot%\system32” o cal é necesario para multitude de tarefas en Windows, neste caso o servizo FTP fai uso de este para o seu correcto funcionamento e a posibilidade de conexións o servidor FTP. Terémolo que marca tanto como conexión entrante en redes privadas como públicas.

¿Por qué pública? Polo que se punden comprobar aínda que os equipos clientes estén na mesma subrede, este interprétao como un equipo con conexión dentro da mesma rede pero non no mesmo grupo de traballo (xa que neste caso carécese dun Dominio de red configurado.), o estar en dous grupos de traballo distintos o servidor no ve a esos equipos clientes como rede privada si non pública.

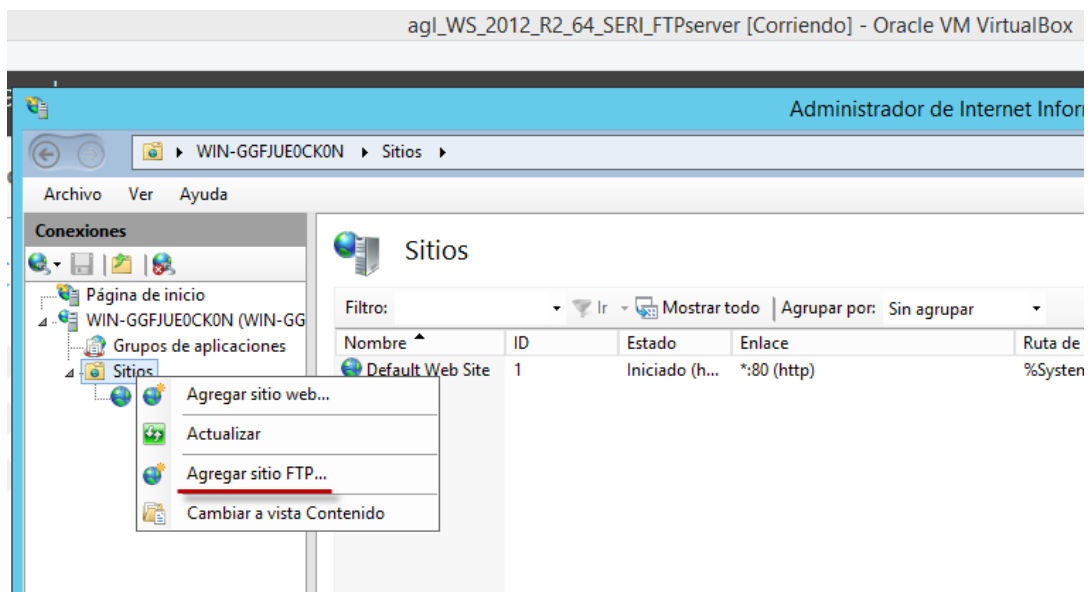


Creamos os usuarios “FTPun” e “FTPdous”, que forman parte dun grupo de traballo creado para estes “G_FTP”.

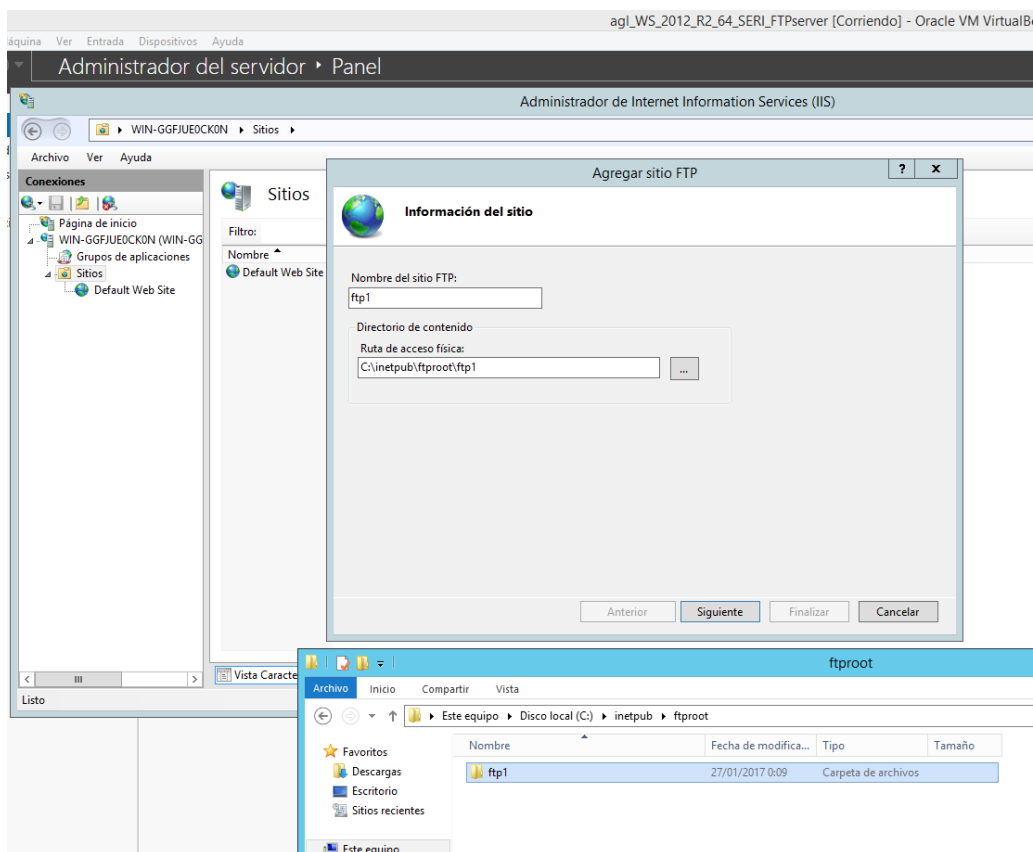


Creamos o cartafol “%systemdrive%\inetpub\ftproot\ftp1”. Veremos máis adiante a xerarquía de carpetas forma a partires de esta raíz

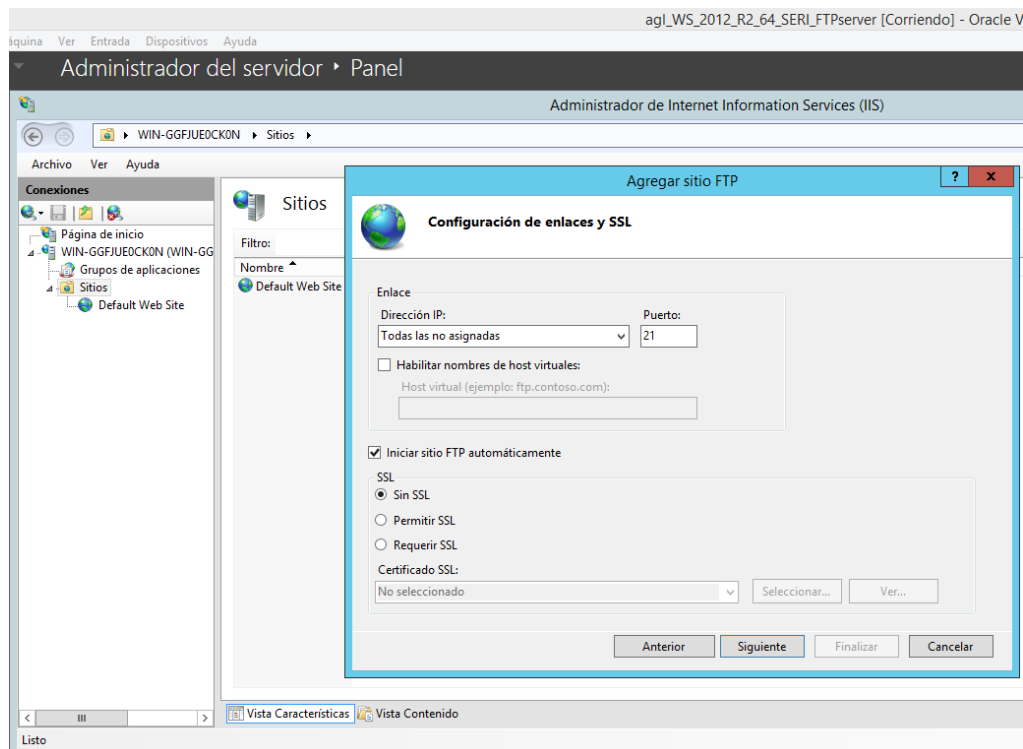
Na configuración de sitios de IIS agregamos un sitio FTP.



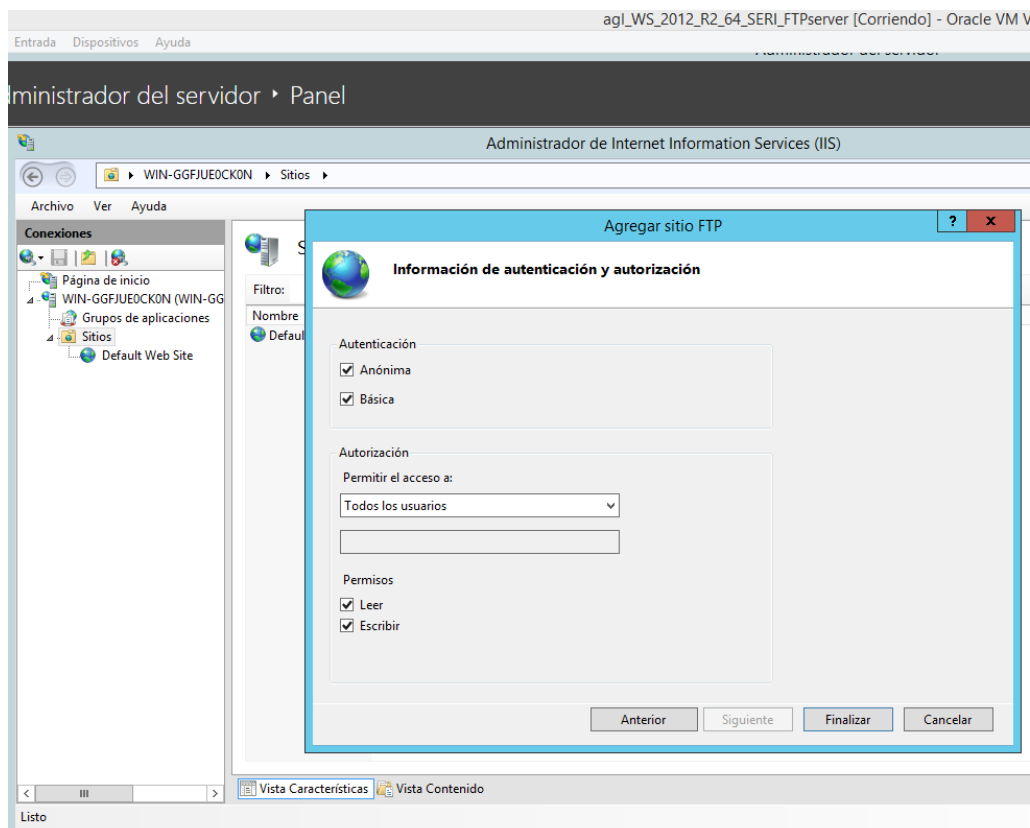
Seguimos o asistente, establecemos un nome o sitio FTP e a ruta física do cartafol creado, será o cartafol raíz “\” o que accedera os clientes.



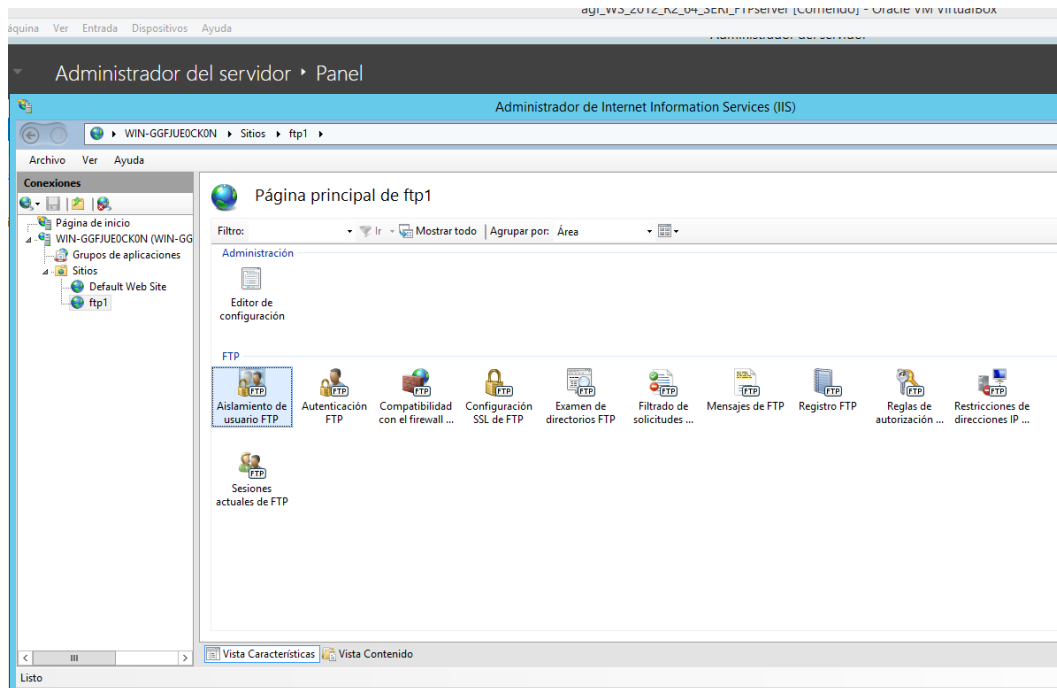
Todas las dirección IP asignadas polo por 21 por defecto, e sin SSL para este caso.



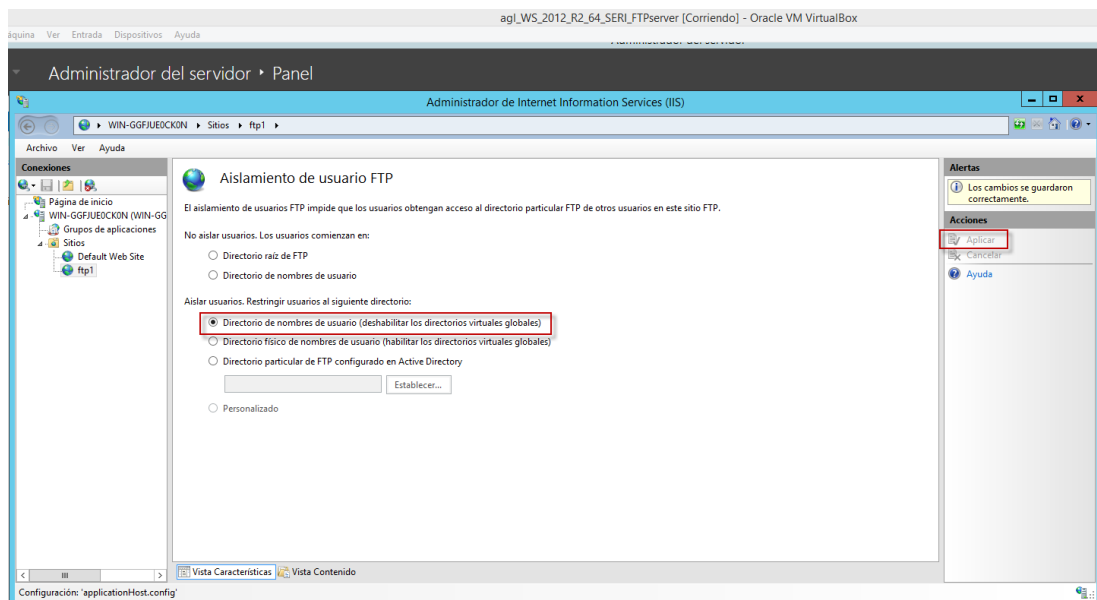
O tipo de autenticación será “Anónima” e “Básica”. Permítese acceso a “Todos os usuarios” e permisos de “lectura e escritura”.



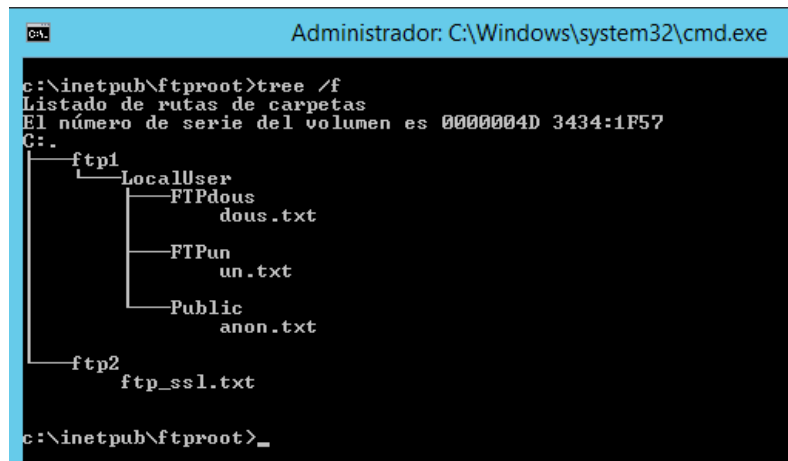
Unha vez rematado a instalación de servidor FTP a través do asistente. Veremos o dashboard de configuración do servidor FTP. Egallolaremos os usuarios.



Establecemos a opción de “Directorio de nomes de usuario”, esta opción engallolará os usuarios autenticados no servidor FTP nun raíz propio para esos usuarios.



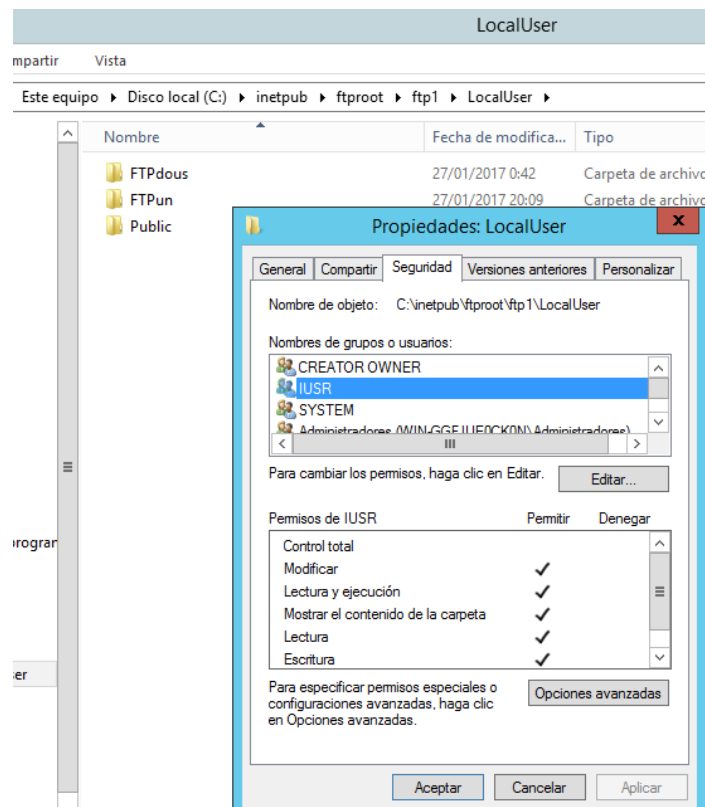
Para eso teremos que crear a seguinte xerarquía de directorios. Cada usuario terá unha carpeta co nome do usuario que se conectará o servidor FTP. Respetando os nomes e estruturas de cartafol. Dentro de ftp1 creárase un cartafol co nome “LocalUser” a súa vez este terá outros cartafol correspondente os nomes dos usuarios en cuestión que se podrán conectar e que soamente verán ese espazo como o seu raíz no momento de conectarse o servidor FTP. O usuario anónimo terá como raíz o contido da carpeta “Public”. Esta estrutura, e nomes predefinidos, e marcada por defecto deste modo por Microsoft e a súa forma de traballar cun servizo FTP.



```

C:\Windows\system32\cmd.exe
c:\inetpub\ftproot>tree /f
Listado de rutas de carpetas
El número de serie del volumen es 0000004D 3434:1F57
C:.
├── ftp1
│   ├── LocalUser
│   │   ├── FTPdous
│   │   │   └── dous.txt
│   │   ├── FTPun
│   │   │   └── un.txt
│   │   └── Public
│   │       └── anon.txt
│   └── ftp2
│       └── ftp_ssl.txt
└──
c:\inetpub\ftproot>_
  
```

Os permisos NTFS da carpeta “..\ftp1\LocalUser\Public” nun principio dexarémolo cos permisos por defecto máis o de “Modificar” soamente para os usuarios anónimos, o usuario por defecto creado por IIS para usuarios anónimos a nivel local de sistema sería o usuario “IUSR”. Recordar que os permisos NTFS prevalecen sobre as regras de autoridade de FTP.





No seguinte apartado configurarase as regras de autorización de permisos para o acceso o servidor FTP, é dicir, que poderán facer e que non os usuarios que se conecten.

Despois de investigar sobre este tema, se agregamos unha regra de denegación esta colocaráse o principio no orden da lista de forma predeterminada, sin posibilidade de poder alterar este orden, o cal esto fará que se anule as regras seguintes que estén por debaixo, non debería pasar esto, pero pasa. Polo que se agregamos unha regra de denegación de escritura sobre os usuarios anónimos e despois outra de permitir sobre un grupo específico a escritura e lectura, ningún usuario poderase conectar o servidor FTP, o cal é ilóxico e finalmente compróbase que as regras non están funcionando correctamente.

Deixo a referencia do artigo na que se explican o función destes elementos.

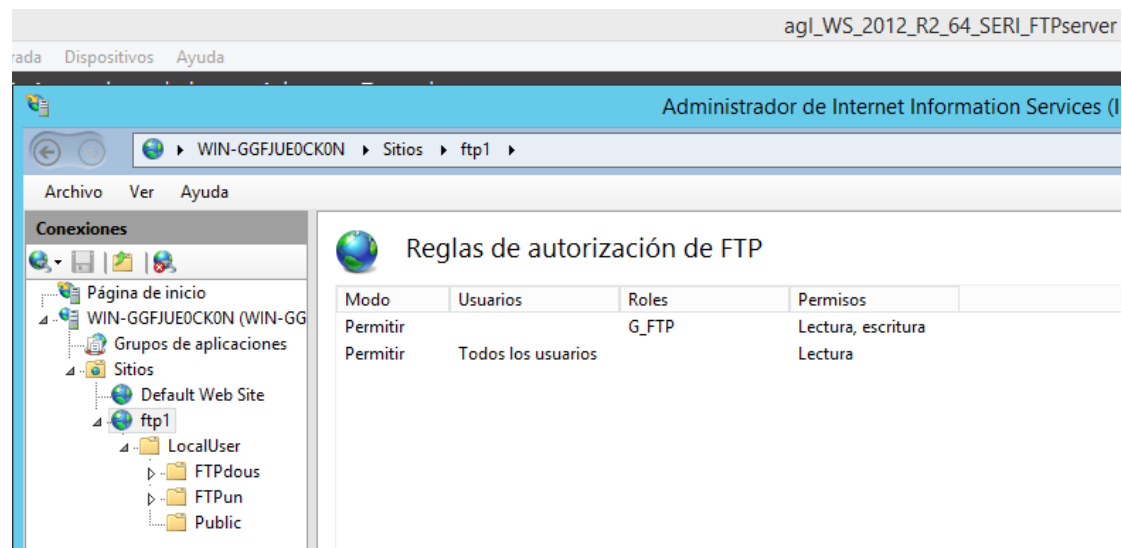
[https://technet.microsoft.com/es-es/library/dd722760\(v=ws.11\).aspx](https://technet.microsoft.com/es-es/library/dd722760(v=ws.11).aspx)

Vese que é ilóxico que si alguén permite ou denega algunha regra para os usuarios anónimos estes teñen que especificar unha contrasinal para que permitan a conexión, o cal xa non ten moito sentido, xa que sería un usuario anónimo pero con contrasinal, a propia regra parece contradictoria.

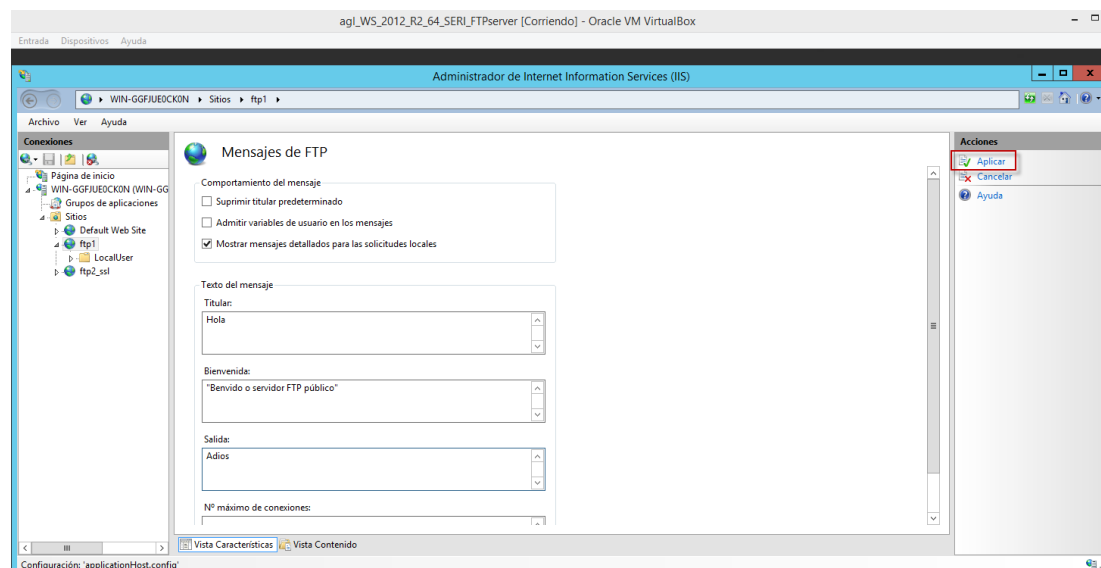
Nombre de elemento	Descripción
Todos los usuarios	<p>Seleccione esta opción para administrar el acceso al contenido tanto para usuarios anónimos como para autenticados.</p> <div>  Nota </div> <p>Asegúrese de colocar esta regla debajo de las reglas que conceden acceso al contenido. Si esta regla ocupa el primer lugar en la lista de reglas, se denegará a todos los usuarios el acceso al contenido.</p>
Todos los usuarios anónimos	<p>Seleccione esta opción para administrar el acceso al contenido de los usuarios que no están autenticados.</p> <div>  Nota </div> <p>Si usa esta regla, todos los usuarios deben tener una cuenta de usuario de autenticación básica o personalizada y una contraseña válidas para poder autenticarse.</p>
Roles o grupos de usuarios especificados	<p>Seleccione esta opción para administrar el acceso al contenido para roles o grupos de usuarios específicos de Microsoft Windows.</p> <div>  Nota </div> <p>Si usa esta regla, todos los miembros de los roles y grupos especificados deben tener una cuenta de usuario de autenticación básica o personalizada y una contraseña válidas para poder autenticarse.</p>

Finalmente óbtase por crear dúas regras en modo permitir, a primeira a un grupo específico (G_FTP) de escritura e lectura, e a segunda para “todos os usuarios” de so lectura. Neste caso todos os usuarios (o cal xa estarían incluíndo os anónimos sin autenticar) que non pertezcan o grupo “G_FTP” terán soamente permisos de lectura sobre o seu raíz.

De forma automática o incluír dúas regras en modo Permitir, a de “Todos os usuarios” colócase o final, xa que si se colocara o principio esta anularía as seguintes por debaixo (leer a nota na captura anterior).

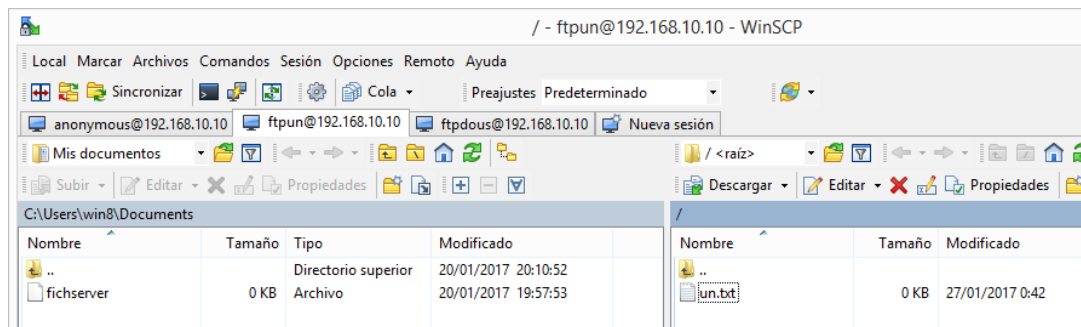


Por último, establecemos unha mensaxe de benvinda no momento de conexión o servidor FTP.

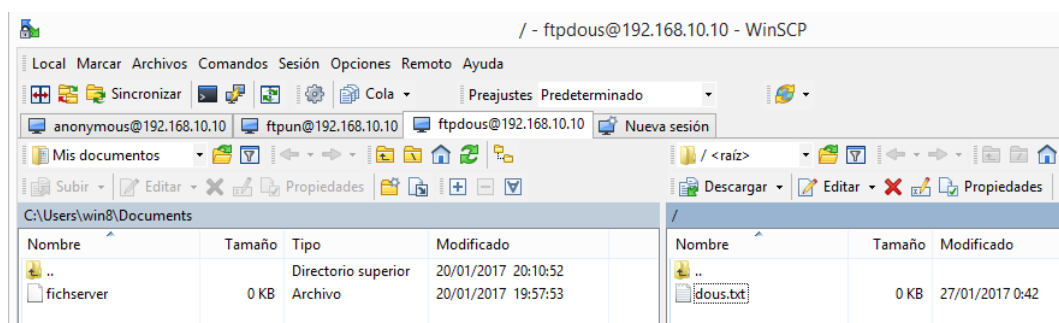


Comprobarase a conexión entre cliente/servidor.

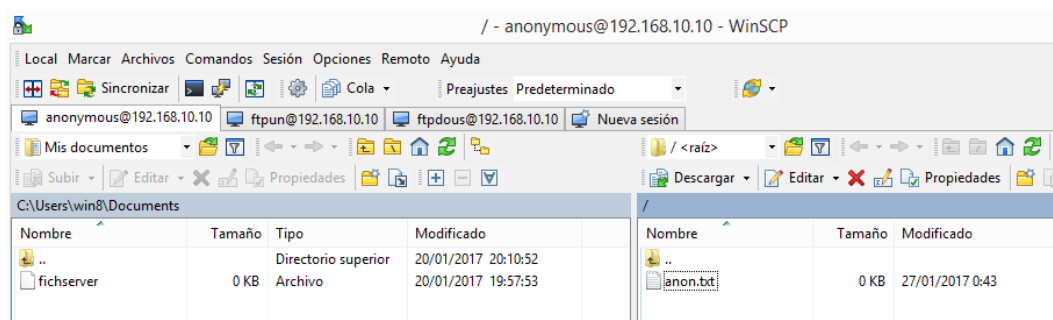
Co usuario FTPun.



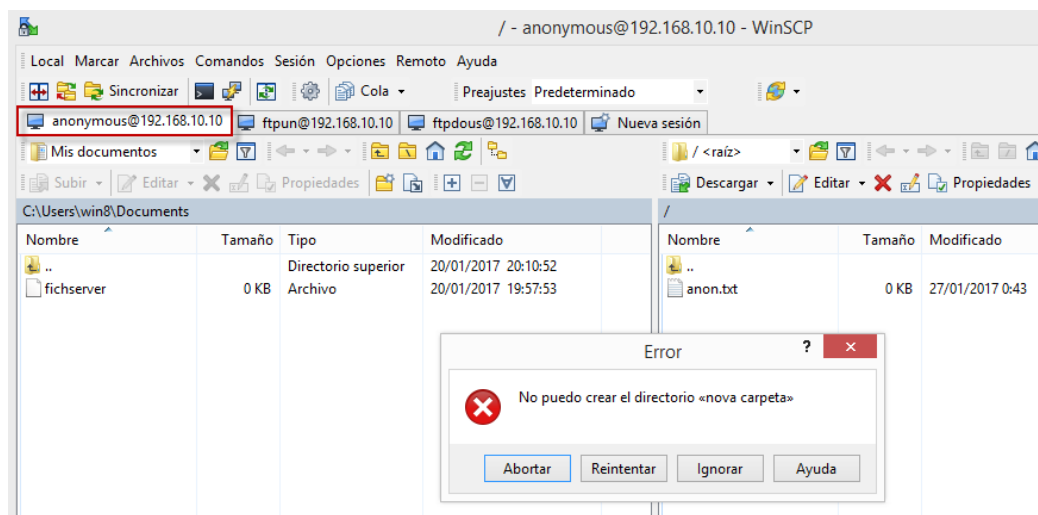
Co usuario FTPdous.



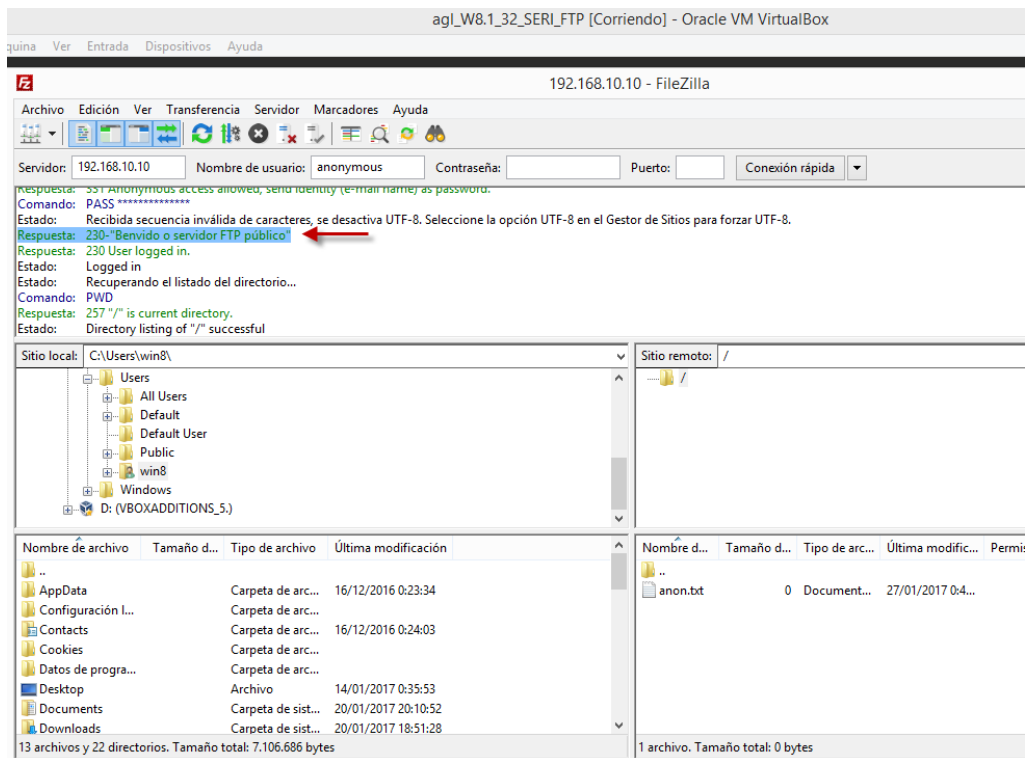
Co usuario anonymous.



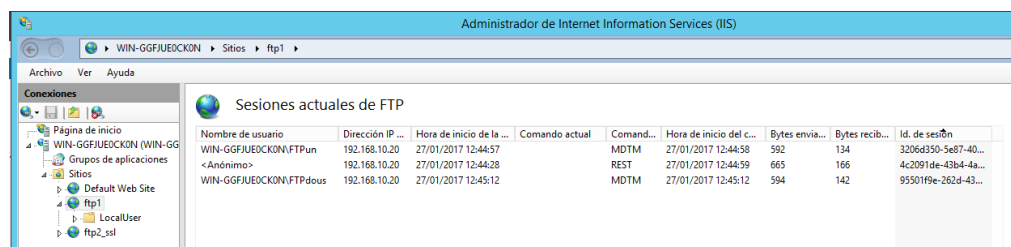
Vemos que so ten permisos de lectura e non de escritura sobre o seu raíz.



Comprobamos a mensaxe de benvida.



Podemos ver a sesións actuais no servidor FTP.



Mostro simplemente a modo detalle un exemplo da inseguridade que ten o protocolo FTP. Capturas de tráfico deste tipo de conexións FTP no seu login e na súa transferencia de data.

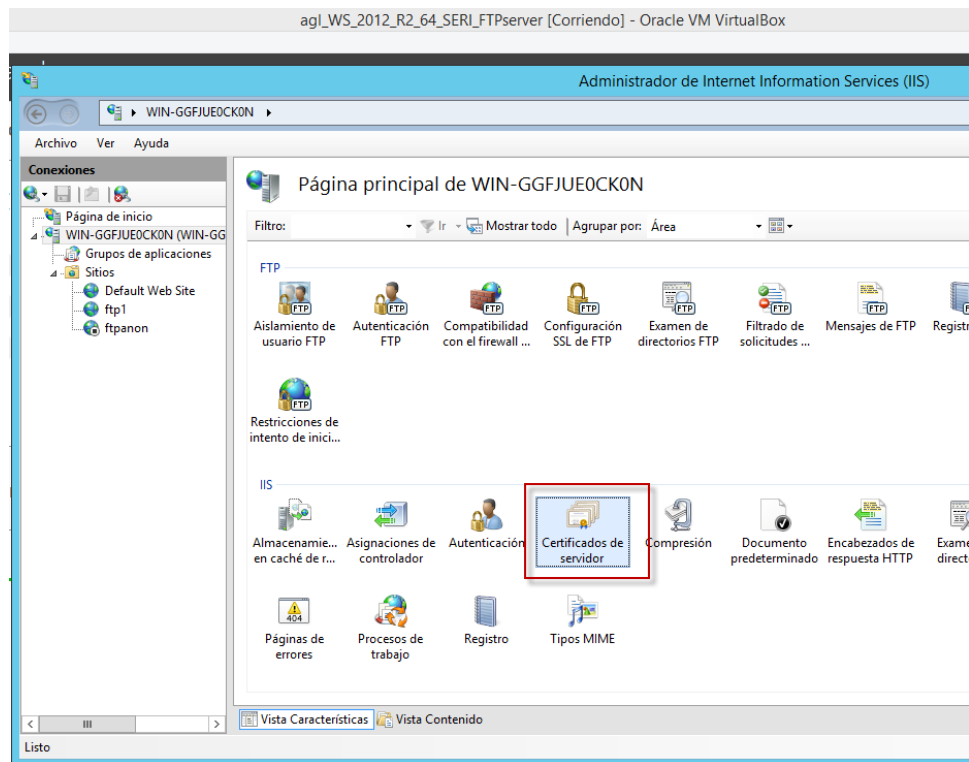
Si fose un tráfico FTPS ou SFTP este tráfico iría cifrado e veríase en Wireshark por exemplo, como un tipo de paquete TCP.

13	4.096986	192.168.10.20	192.168.10.10	FTP	66	Request: USER ftpun
14	4.097182	192.168.10.10	192.168.10.20	FTP	77	Response: 331 Password required
15	4.097861	192.168.10.20	192.168.10.10	FTP	68	Request: PASS abc123.
16	4.098537	192.168.10.10	192.168.10.20	FTP	92	Response: 230-"Benvido o servidor FTP público"
17	4.098537	192.168.10.10	192.168.10.20	FTP	75	Response: 230 User logged in.

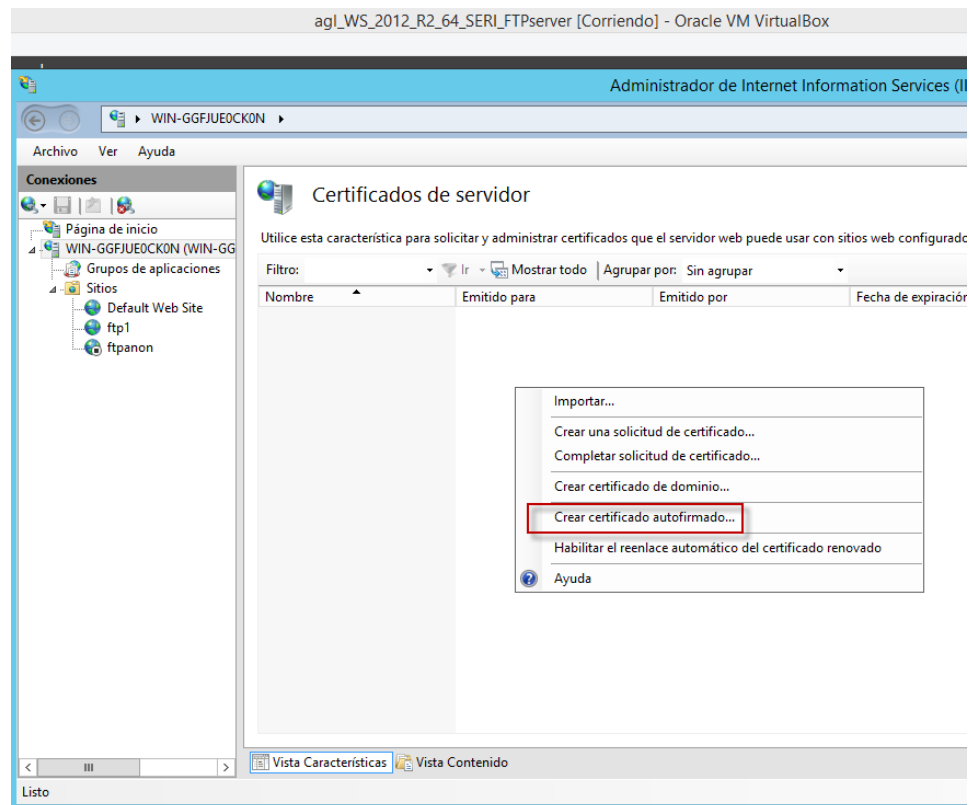
Descarga de información a local, do ficheiro "un.txt".

73	10.848491	192.168.10.10	192.168.10.20	FTP	105	Response: 227 Entering Passive Mode (192,168,10,10,192,12).
74	10.848833	192.168.10.20	192.168.10.10	FTP	67	Request: RETR un.txt
75	10.849031	192.168.10.20	192.168.10.10	TCP	66	49193→49164 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=128 SACK_PERM=1
76	10.849233	192.168.10.10	192.168.10.20	TCP	66	49164→49193 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
77	10.849280	192.168.10.20	192.168.10.10	TCP	54	49193→49164 [ACK] Seq=1 Ack=1 Win=4194304 Len=0
78	10.885575	192.168.10.10	192.168.10.20	FTP	95	Response: 150 Opening ASCII mode data connection.
79	10.910245	192.168.10.10	192.168.10.20	TCP	60	49164→49193 [FIN, ACK] Seq=1 Ack=1 Win=65536 Len=0
80	10.910339	192.168.10.20	192.168.10.10	TCP	54	49193→49164 [ACK] Seq=1 Ack=2 Win=4194304 Len=0
81	10.910390	192.168.10.10	192.168.10.20	FTP	78	Response: 226 Transfer complete.
82	10.910412	192.168.10.20	192.168.10.10	TCP	54	49192→21 [ACK] Seq=86 Ack=450 Win=65024 Len=0
83	10.910510	192.168.10.20	192.168.10.10	TCP	54	49193→49164 [FIN, ACK] Seq=1 Ack=2 Win=4194304 Len=0

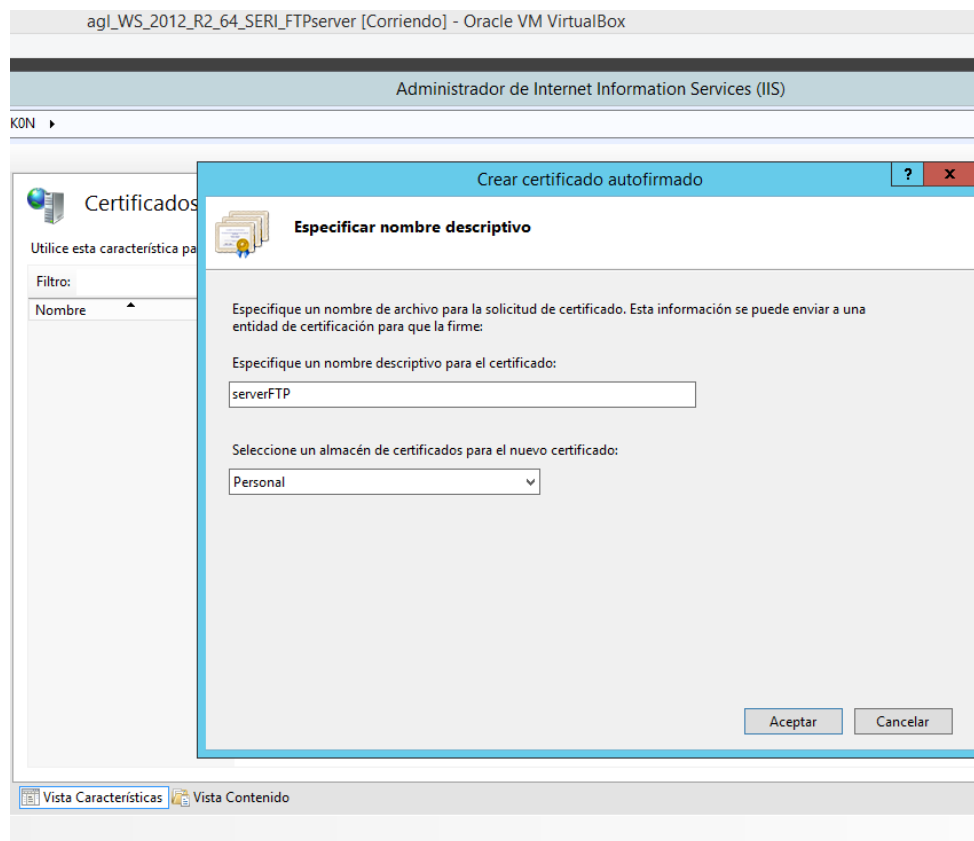
Na segunda parte desta tarefa, co mesmo esquema de rede, crearemos un servidor FTP cun certificado SSL autofirmado polo propio servidor.



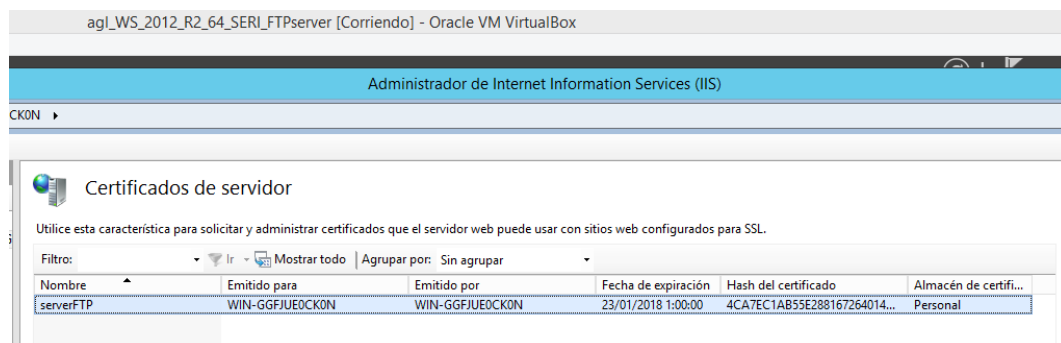
Creamos un certificado autofirmado, xa que neste caso non dependemos dunha entidade certificadora autorizada.



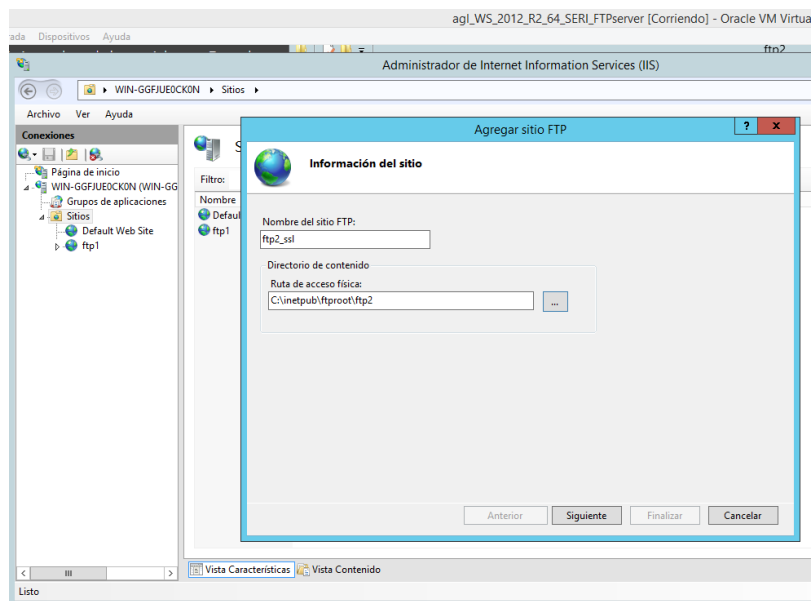
Establécese un nome descriptivo para o certificado.



Unha vez aceptado o certificado xerarase automaticamente.

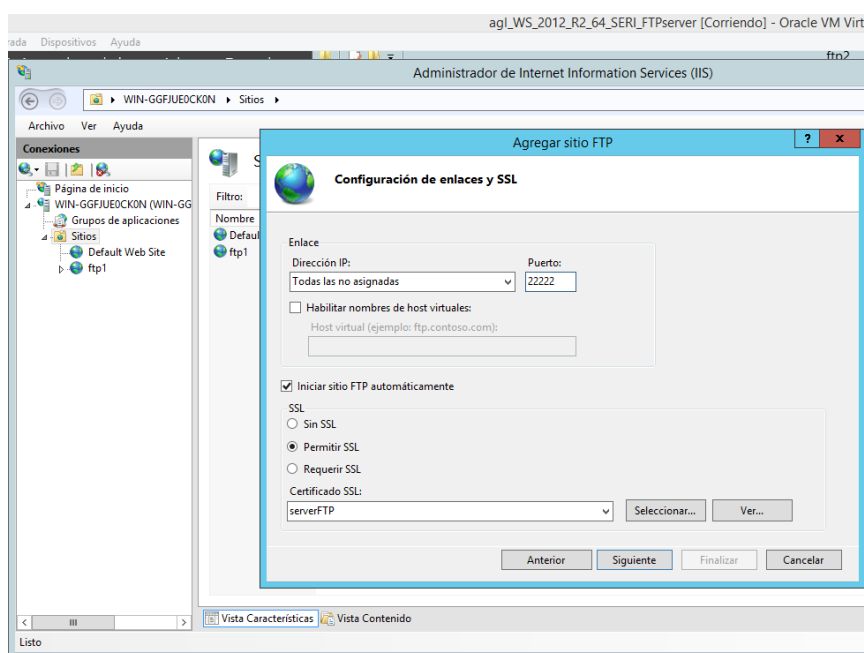


Agregamos un servidor FTP de forma habitual, establecemos un nome para o sitio e a ruta física, neste caso un cartafol chamado ftp2 con permisos NTFS para “Todos” o usuarios.

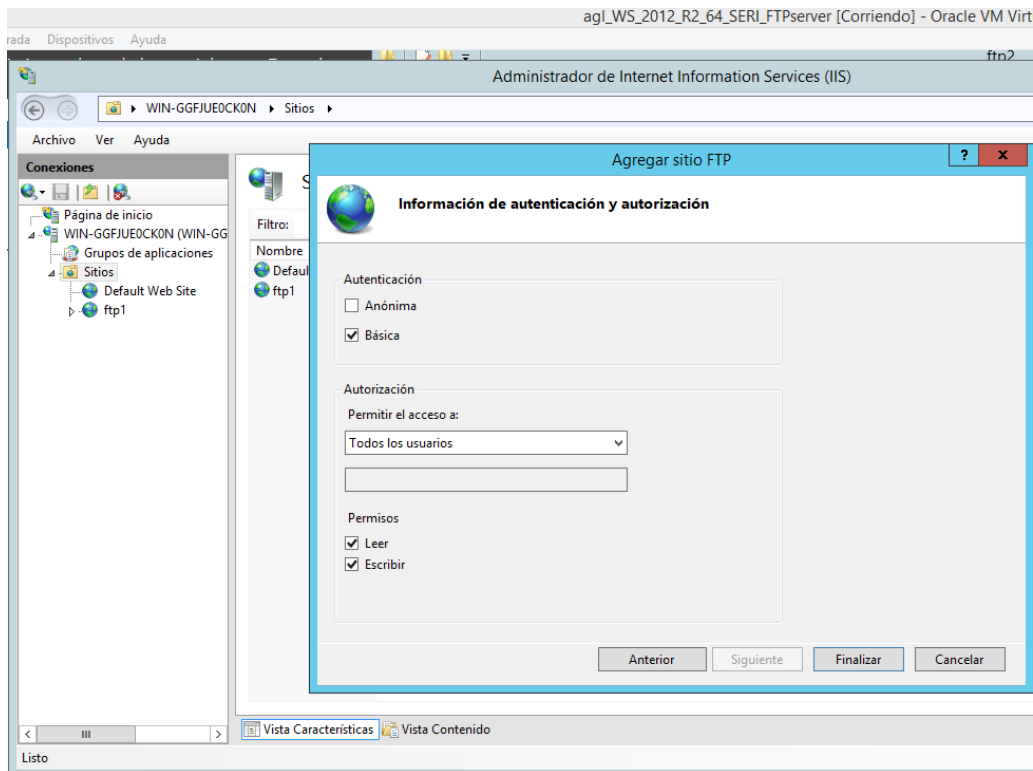


Todas as direccións IP asignadas escoitando as peticións de conexión polo “porto 22222” para que non haia colisións sobre o porto xa escoitando no outro FTP sobre o porto por defecto 21.

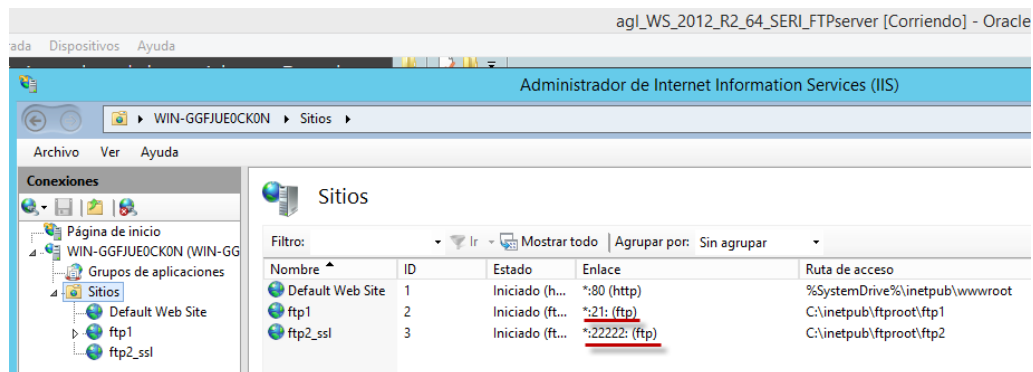
Seleccionamos o certificado SSL chamado “serverFTP” creado anteriormente, e poderemos marcar “Permitir SSL”, a diferencia de “Requerir SSL” (similar a directiva que se configura en vsftpd en Linux a “*ssl_enable=YES*” con “*force_local_data_ssl=NO*” e “*force_local_logins_ssl=NO*”) a “Requerir SSL” (similar a directiva que se configura en vsftpd en Linux a “*ssl_enable=YES*” con “*force_local_data_ssl=YES*” e “*force_local_logins_ssl=YES*”), en requerir estamos forzando a que as conexión entre cliente e servidor obrigatoriamente sexan SSL.



Neste caso so se permitirán usuario con con autenticación e non usuarios anónimos polo que marcamos autenticación básica con permisos de lectura é escritura.



Comprobamos que os dous servidores FTP están funcionando en dous portos distintos.



Con netstat listamos as conexións existentes de portos de escoita no servidor.

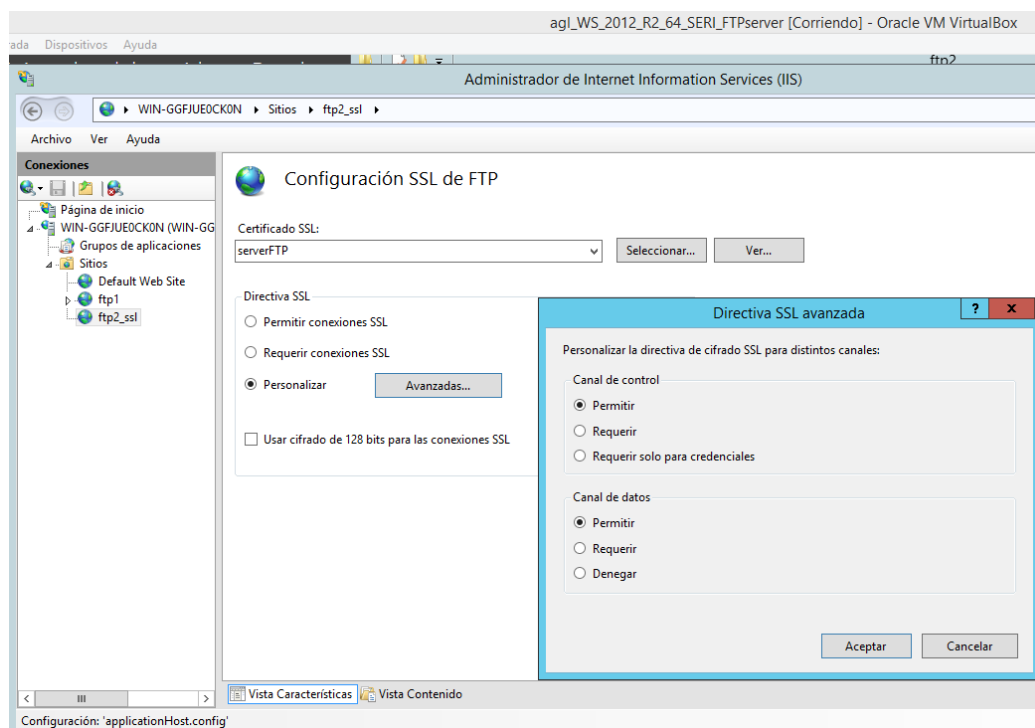
```

C:\Users\Administrador>netstat -fanoh

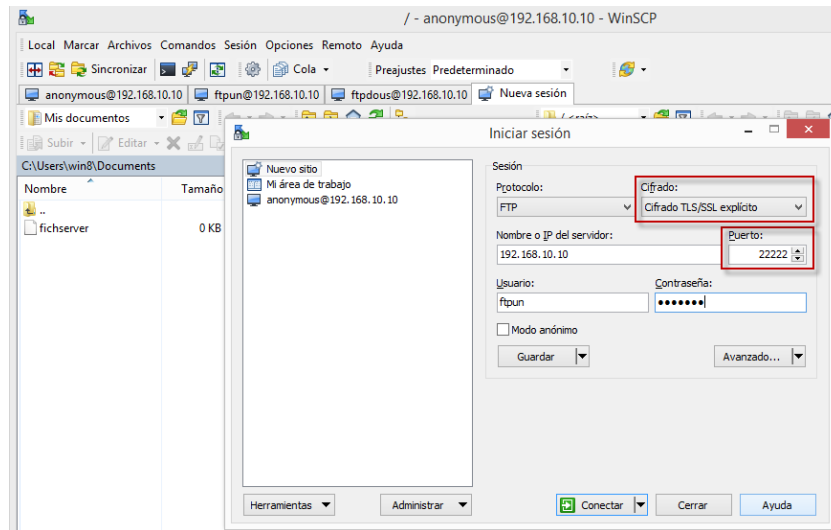
Conexiones activas

Proto  Dirección local      Dirección remota      Estado      PID
-----
TCP    0.0.0.0:21            0.0.0.0:0             LISTENING   1064
ftpsvc
lsuchost.exe]
TCP    0.0.0.0:80            0.0.0.0:0             LISTENING   4
No se puede obtener información de propiedad
TCP    0.0.0.0:135           0.0.0.0:0             LISTENING   588
RpcSs
lsuchost.exe]
TCP    0.0.0.0:445           0.0.0.0:0             LISTENING   4
No se puede obtener información de propiedad
TCP    0.0.0.0:5985         0.0.0.0:0             LISTENING   4
No se puede obtener información de propiedad
TCP    0.0.0.0:2222         0.0.0.0:0             LISTENING   1064
ftpsvc
lsuchost.exe]
TCP    0.0.0.0:47001         0.0.0.0:0             LISTENING   4
No se puede obtener información de propiedad
TCP    0.0.0.0:49152        0.0.0.0:0             LISTENING   412
lsass.exe]
TCP    0.0.0.0:49153        0.0.0.0:0             LISTENING   492
lsass.exe]
  
```

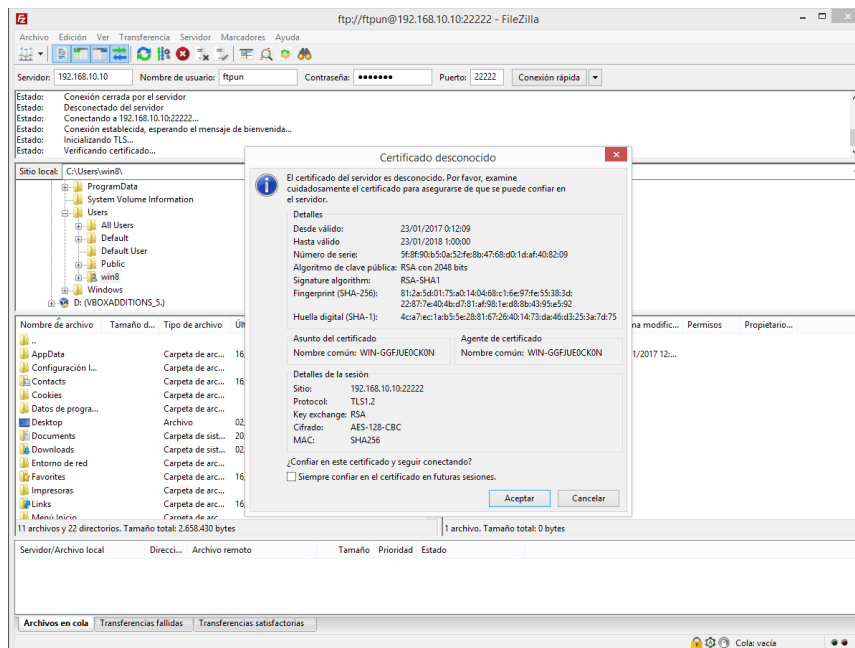
Nas opcións de configuración SSL do servidor FTP poderemos personalizar si a comunicación cifrada SSL soamente se solicitará no momento das conexións (canal de control) como no caso da transferencia de información (canal de datos).



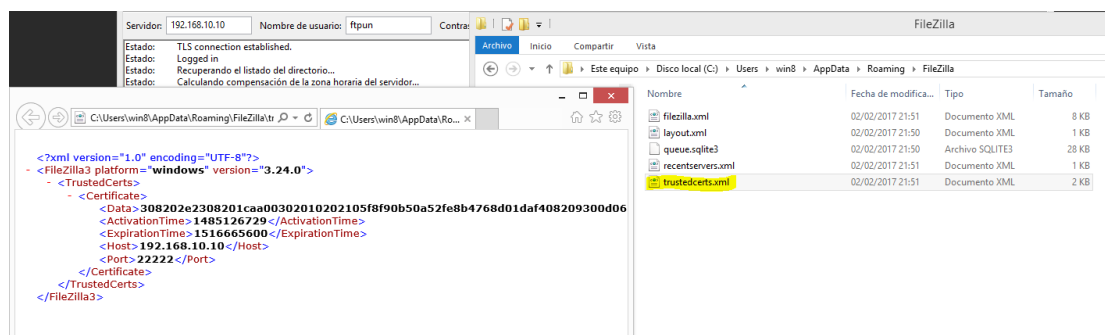
Facemos as comprobacións entre cliente/servidor para SSL hacia o porto específico 2222 cun usuario con autenticación.



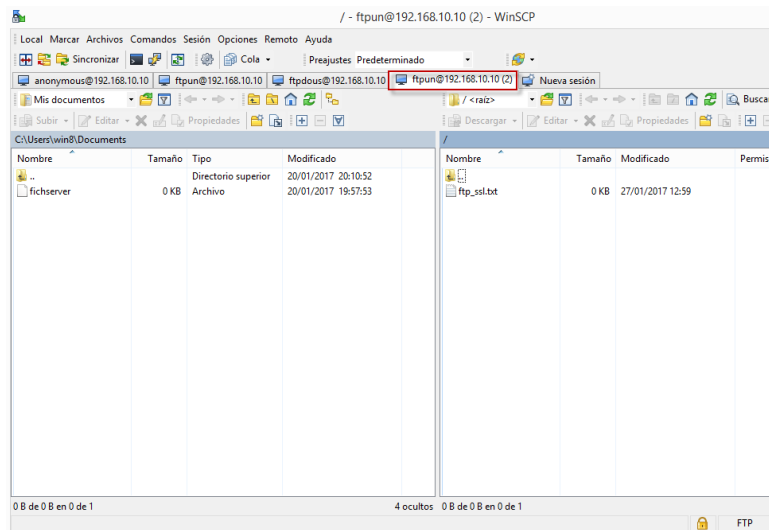
Vemos que nos aparece o aviso para a aceptación do certificado autofirmado.



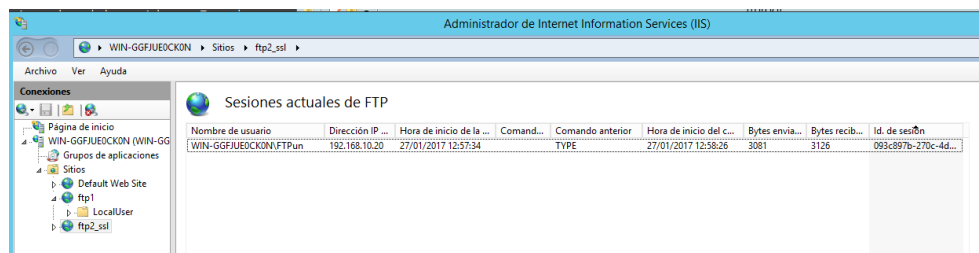
Si gardamos o certificado para que non nos apareza máis a ventana de alerta e confiamos sempre nel, pero queremos volver restablecer estas opcións relacionados cos certificados este almacenarse no path: “%appdata%\Filezilla\trustedcerts.xml”



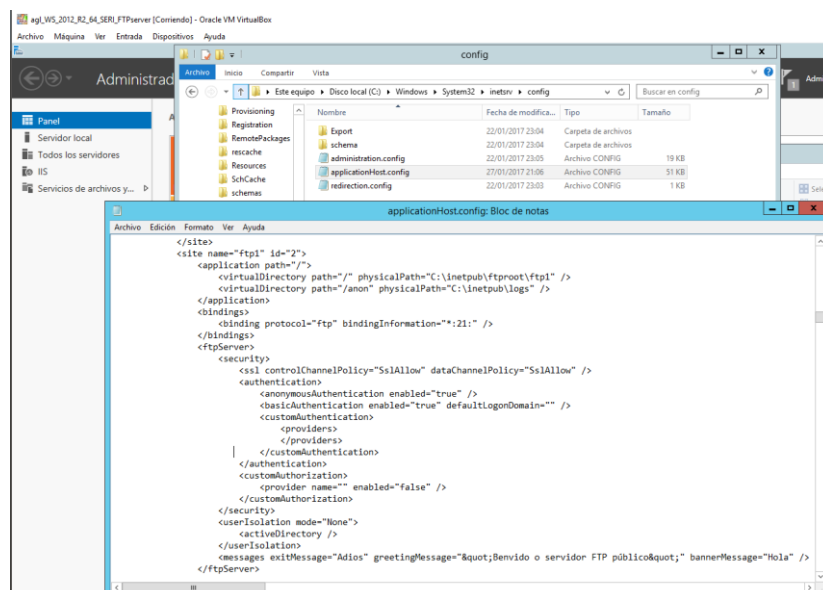
Temos acceso o raíz co usuario autenticado “FTPun”.



Na sección de sesións actuais de FTP, vemos a conexión actualmente existente para o servidor FTPS (FTP con SSL).



O ficheiro “%systemroot%\system32\inetmgr\config\applicationHost.config” terá a información almacenada do servizo FTP. Podemos alterar dita información e modificala dende aquí, sempre e cando se faga con coñecemento. O fin e o cabo non deixa de ser unha configuración en texto plano con unha sintaxis propietaria de Microsoft, o igual que cando se configurou vsftpd en contornas Linux, pero que neste caso temos a posibilidade de facelo de forma gráfica facilitando así a súa administración.



5. Instalación OpenSSH, manexo de scp e sftp e WinSCP en Windows.

SFTP (SSH FTP), e un FTP sobre SSH (Secure SHell).

Actualizamos repositorios e instalamos OpenSSH:

```
sudo apt-get update
```

```
sudo apt-get install openssh-server
```

O ficheiro de configuración de OpenSSH sería “`/etc/ssh/sshd_config`”, aínda que para este caso non habrá que configurar nada en especial xa que para este cometido as opcións por defecto que nos interesan están preconfiguradas, o certificado xa e xenerado por OpenSSH con OpenSSL de forma automática no momento de instalación do servizo sshd.

- Emprega o comando **scp** (Secure CoPy) para transferir arquivos entre un cliente e o servidor.

Transferir ficheiro: **remoto > local**

```
scp usuario@hostremoto:[ruta_ficheiro] [ruta_directorio_local]
```

Transferir ficheiro: **local > remoto**

```
scp [ruta_ficheiro] usuario@hostremoto:[ruta_directorio_remoto]
```

Cun directorio sería practicamente o mesmo, ca diferencia de que engadir o parámetro “-r” (**scp -r**) para que transfira **directorios** de forma recursiva.

```

uadmin@userver1604:~$ ping 172.16.0.11
PING 172.16.0.11 (172.16.0.11) 56(84) bytes of data:
64 bytes from 172.16.0.11: icmp_seq=1 ttl=64 time=0.236 ms
^C
--- 172.16.0.11 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.236/0.236/0.236/0.000 ms
uadmin@userver1604:~$ pwd
/home/uadmin
uadmin@userver1604:~$ ls -lh
total 8,0K
-rw-r--r-- 1 uadmin uadmin 7 Jan 20 19:09 fichprueba.txt
-rw-r--r-- 1 root root 1,3K Dec 5 2002 jcameron-key.asc
uadmin@userver1604:~$ ls -lh /home/jose/
total 4,0K
-rw-r--r-- 1 jose jose 7 Jan 20 19:10 fichprueba.txt
uadmin@userver1604:~$

root@userver1604:/home/uadmin# ls
fichprueba.txt jcameron-key.asc
root@userver1604:/home/uadmin# ls -l
total 8
-rw-r--r-- 1 root root 7 Jan 20 19:05 fichprueba.txt
-rw-r--r-- 1 root root 1320 Dec 5 2002 jcameron-key.asc
root@userver1604:/home/uadmin# scp fichprueba.txt uadmin@172.16.0.10:/home/uadmin
n
The authenticity of host '172.16.0.10 (172.16.0.10)' can't be established.
ECDSA key fingerprint is SHA256:CanM0TfInZuu/61k390xU8290YK03cF767x210cfaA.
Are you sure you want to continue connecting (yes/no)? y
Please type 'yes' or 'no': yes
Warning: Permanently added '172.16.0.10' (ECDSA) to the list of known hosts.
uadmin@172.16.0.10's password:
root@userver1604:/home/uadmin# scp fichprueba.txt jose@172.16.0.10:/home/uadmin
jose@172.16.0.10's password:
scp: /home/uadmin/fichprueba.txt: Permission denied
root@userver1604:/home/uadmin# scp fichprueba.txt jose@172.16.0.10:/home/jose
jose@172.16.0.10's password:
fichprueba.txt 100% 7 0.0KB/s 00:00
root@userver1604:/home/uadmin#

```

- Emprega o comando **sftp** para transferir arquivos entre un cliente e o servidor.

Podemos usar sftp de forma interactiva.

sftp user@hostremoto:[dir]

Para subir de local a remoto ficheiros:

put [dir_local_ficheiro] [dir_remoto_ficheiro]

Para descargar de remoto a local:

get [dir_remoto_ficheiro] [dir_local_ficheiro]

Para saber si estamos usando un ficheiro ou directorio do equipo local ou remoto no uso dos dous comandos anteriores, saberémolo porque o propio sftp usará o directorio correspondente a acción que se lle indica, é decir, si usamos *put* usará a continuación directorios locais e si usamos *get* usará a continuación directorios remotos.

Co modificador “-r” (**put -r** ou **get -r**) podemos descargar ou subir **directorios**.

Tip_1: Co signo de admiración “!” podemos salir do modo interactivo hacia o host local sin cerrar a conexión co servidor remoto e con “exit” volvemos a conexión novamente, sería útil para navegar polo host local sin necesidad de volver iniciar sesión. Siempre e cuando non expire o tempo de sesión establecido no servidor vsftpd (directiva: idle_session_timeout).

Tip_2: Para poder listar un directorio no host remoto usaremos “ls” como de costume, para listar un directorio en local sin salir do prompt sftp usaremos “lls” (LocalLiSt).

```

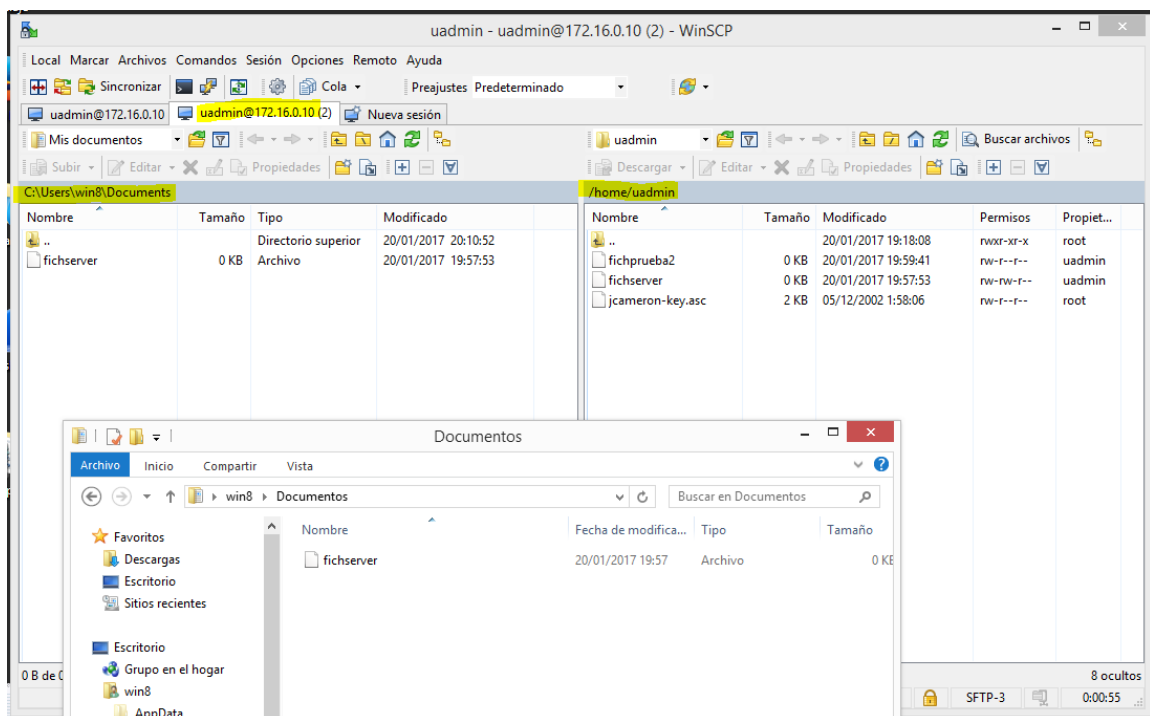
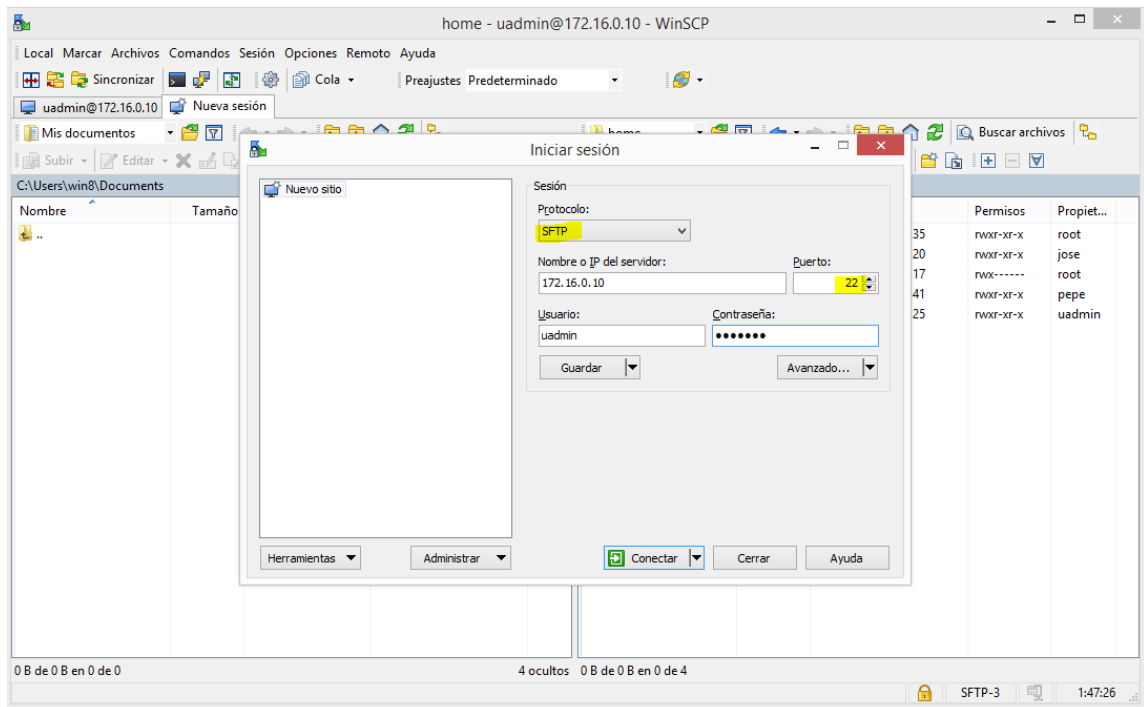
agl_US32-16.4_SERI_FTP [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
uadmin@userver1604:~$ put
/home/uadmin
uadmin@userver1604:~$ ls -l
total 4
-rw-rw-r-- 1 uadmin uadmin 0 Xan 20 19:57 fichserver
-rw-r--r-- 1 root root 1320 Dec 5 2002 jcameron-key.asc
uadmin@userver1604:~$ ls -l
total 4
-rw-rw-r-- 1 uadmin uadmin 0 Xan 20 19:59 fichprueba2
-rw-rw-r-- 1 uadmin uadmin 0 Xan 20 19:57 fichserver
-rw-r--r-- 1 root root 1320 Dec 5 2002 jcameron-key.asc
uadmin@userver1604:~$ _

agl_US32-16.4_SERI_ftpcient [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
uadmin@172.16.0.10's password:
Connected to 172.16.0.10.
sftp> ls
fichserver jcameron-key.asc
sftp> lls
aa fichprueba2 fichprueba.txt jcameron-key.asc
sftp> get fichserver /home/uadmin/
Fetching /home/uadmin/fichserver to /home/uadmin/fichserver
sftp> lls
aa fichprueba2 fichprueba.txt fichserver jcameron-key.asc
sftp> put /home/uadmin/fi
fichprueba.txt fichprueba2 fichserver
sftp> put /home/uadmin/fichp
fichprueba.txt fichprueba2
sftp> put /home/uadmin/fichprueba2 /home/uadmin
Uploading /home/uadmin/fichprueba2 to /home/uadmin/fichprueba2
/home/uadmin/fichprueba2 100% 0 0.0KB/s 00:00
sftp> ls
fichprueba2 fichserver jcameron-key.asc
sftp> lls
aa fichprueba2 fichprueba.txt fichserver jcameron-key.asc
sftp> !
uadmin@userver1604:~$ exit
exit
sftp> _

```

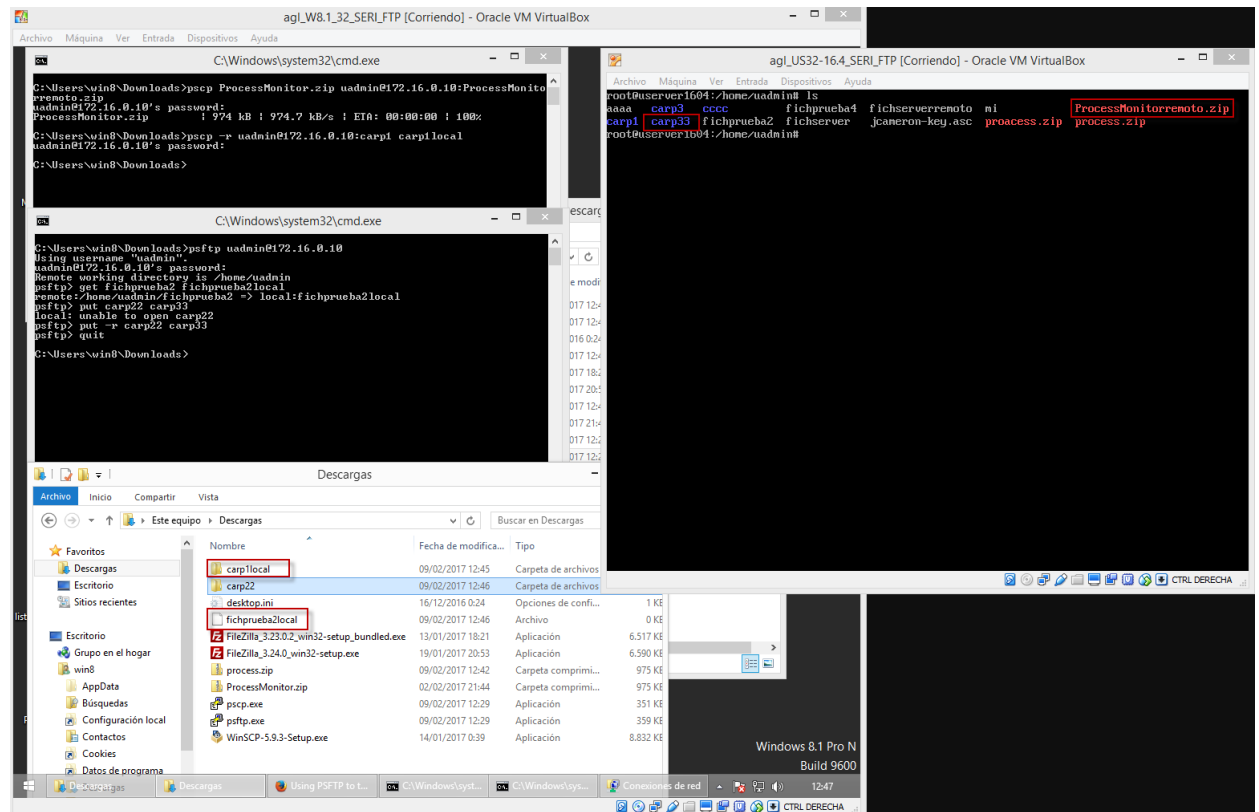

- Emprega o cliente WinSCP e Filezilla para transferir arquivos co servidor.

Neste caso usarei WinSCP, aínda que con Filezilla sería practicamente o mesmo. Marcaremos como protocolo SFTP no porto 22, que sería o porto de escoita por defecto usado para SSH.



Se queremos **utilizar** as utilidades **SFTP** e **SCP** en contornas **Windows** a través da **súa consola**, xa que non “existen” de forma nativa no sistema o uso dos comandos de **SFTP** e **SCP**, poderemos usar “**pscp.exe**” e “**psftp.exe**”, dúas utilidades desenvolvidas por “**Chiark**” (os mesmos desenvolvedores de **Putty.exe**).

A forma básica de utilizalas ven sendo practicamente a mesma. Na seguinte captura observase tanto o uso de pscp como psftp.



6. Conclusións

Como conclusión podemos decir que tanto en contornas Linux como Microsoft Windows podemos interatuar de modos similares e chegar a un mesmo obxectivo final de configuración tanto para os modos de autenticación de conexións, permisos, engallolamentos, etc.

En sistemas Linux, polo feito de forzarse a tocar ficheiros manualmente, vese o funcionamento e aplicación de directivas de forma máis clara. No caso de sistemas Windows vese practicamente o mesmo de forma gráfica, aínda que como se mostrou neste conxunto de tarefas existen ficheiros de configuración en texto plano para a configuración deste.

No lado cliente existen numerosas aplicacións que nos permiten conexións FTP, FTPS ou SFTP, tanto de forma gráfica como por liña de comandos, e creación de scripts e programalos que poden chegar a facilitar determinadas tarefas en circunstancias de necesidade. O uso de calqueira de esas ferramentas FTP son sinxelas de utilizar con un mínimo de práctica sobre elas.



<https://creativecommons.org/licenses/by-nc/4.0/>