



Misión 3

# SERVIDOR FTP



Dominguez de la Rosa Bryan  
Pacheco Díaz Fernando Jair  
Vivia Delgadillo Rocío

4CV3



# Agenda

---

- Protocolo FTP
- Configuración de servidor FTP
- Restricciones
- FTPS
- SFTP
- Jaulas
- Bitácoras
- Resumen

# PROTOCOLLO FTP

---

---

El protocolo de transferencia de archivos (FTP) es uno de los protocolos más viejos y populares que se encuentran en la Internet hoy día. Su objetivo es el de transmitir archivos exitósamente entre máquinas en una red.

FTP utiliza una arquitectura cliente/servidor para transferir archivos usando el protocolo de red TCP. [1]

# CONFIGURACIÓN DEL SERVIDOR PROFTPD

---

# Creamos usuarios en shell falso

```
bryanddlr@bryanddlr-HP-14-Notebook-PC: /home
bryanddlr@bryanddlr-HP-14-Notebook-PC:/home$ sudo useradd jair -p 0000 -d /home/FTP-public
-s /bin/false
bryanddlr@bryanddlr-HP-14-Notebook-PC:/home$ sudo useradd rocio -p 0000 -d /home/FTP-public
-s /bin/false
bryanddlr@bryanddlr-HP-14-Notebook-PC:/home$
```

# Configuración básica del server

```
10 # Set off to disable IPv6 support which is annoying on IPv4 only boxes.
11 # UseIPv6 on
12 # If set on you can experience a longer connection delay in many cases.
13 IdentLookups off
14
15 ServerName "Debian"
16 # Set to inetd only if you would run proftpd by inetd/xinetd.
17 # Read README.Debian for more information on proper configuration.
18 ServerType standalone
19 DeferWelcome off
20
21 MultilineRFC2228 on
22 DefaultServer on
23 ShowSymlinks on
24
25 TimeoutNoTransfer 600
26 TimeoutStalled 600
27 TimeoutIdle 1200
28
29 DisplayLogin welcome.msg
30 DisplayChdir .message true
31 ListOptions "-l"
32
33 DenyFilter \*./
34
35 # Use this to jail all users in their homes
36 DefaultRoot /home/public_FTP
37 #DefaultRoot ~
38
39 # Users require a valid shell listed in /etc/shells to login.
40 # Use this directive to release that constrain.
41 # RequireValidShell off
42
```

# RESTRICCIONES

---



# Restricciones

---

La configuración de las restricciones se realiza en el archivo proftpd.conf, dentro de este archivo se encuentra la directiva <Limit> en la cual se especifican las restricciones o accesos a grupos, usuarios o IP's de clientes.

<Limit LOGIN>

    parámetro nombreRestricción

</Limit>

El parámetro dependerá de

# Por IP

```
ro@ro-VirtualBox: ~  
#  
# # We want 'welcome.msg' displayed at login, and '.message' displayed  
# # in each newly chdir'd directory.  
# DisplayLogin welcome.msg  
# DisplayChdir .message  
#  
# # Limit WRITE everywhere in the anonymous chroot  
<Directory *>  
  <Limit LOGIN>  
    Order deny, allow  
    Deny from 192.168.1.81  
    AllowAll  
  </Limit>  
</Directory>  
#  
# # Uncomment this if you're brave.  
# # <Directory incoming>  
# # # Umask 022 is a good standard umask to prevent new files and dirs  
# # # (second parm) from being group and world writable.  
# # Umask 022 022  
# # <Limit READ WRITE>  
# # DenyAll  
# # </Limit>  
160,1 94%
```

# Por usuario

```
<Limit LOGIN>
  AllowUser usuario1
  AllowUser usuario2
</Limit>
```

Host:  Username:  Password:  Port:   ▼

Status: insecure server, it does not support FTP over TLS.

Command: USER usuario2

Response: 331 Password required for usuario2

Command: PASS \*\*\*\*\*

Response: 530 Login incorrect.

Error: Critical error: Could not connect to server

# Por grupo

```
jair@lap-jair:~$ sudo adduser usuario1 ftpusers
Adding user `usuario1' to group `ftpusers' ...
Adding user usuario1 to group ftpusers
Done.
jair@lap-jair:~$ sudo adduser usuario2 ftpusers
Adding user `usuario2' to group `ftpusers' ...
Adding user usuario2 to group ftpusers
Done.
jair@lap-jair:~$ id usuario1
uid=1001(usuario1) gid=1001(usuario1) groups=1001(usuario1),1003(ftpusers)
jair@lap-jair:~$ id usuario2
uid=1002(usuario2) gid=1002(usuario2) groups=1002(usuario2),1003(ftpusers)
```

```
<Limit LOGIN>
    AllowGroup ftpusers
    DenyAll
</Limit>
```

# FTPS



# SSL

---

Se utilizan certificados SSL. Con la herramienta openssl se pueden generar aunque por primera instancia no sean reconocidos por terceros.

Con openssl se crea un certificado autofirmado al que proporcionaremos información básica acerca de la firma.

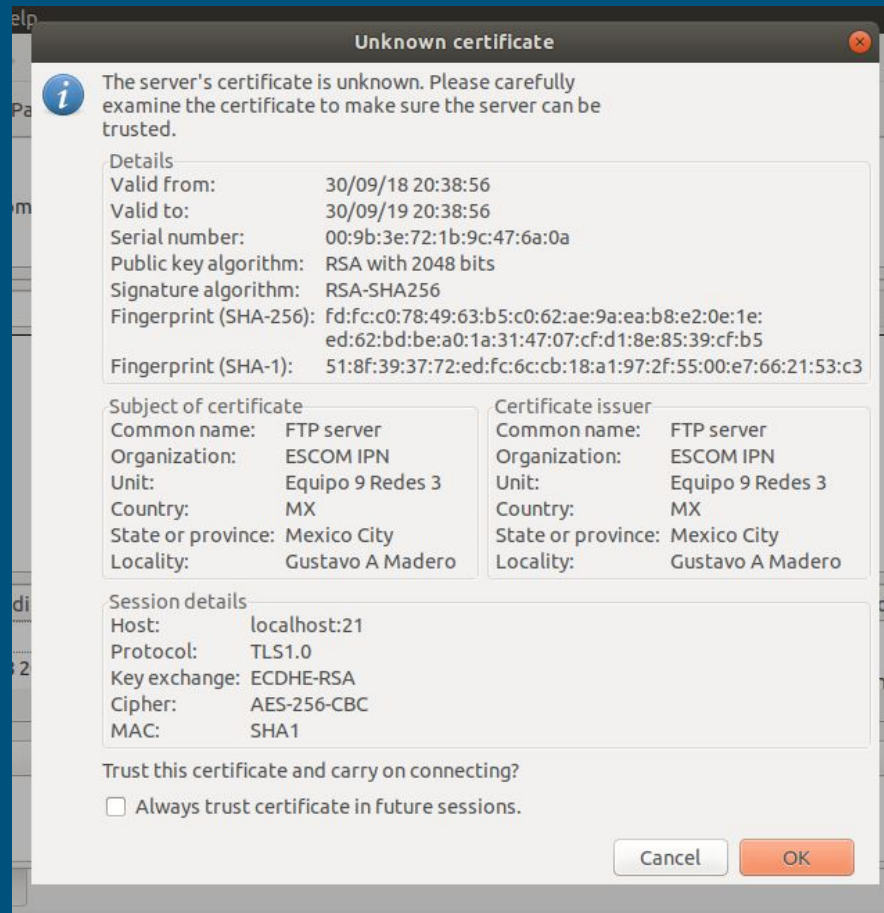
```
jair@lap-jair:~$ sudo openssl req -x509 -nodes -newkey rsa:2048 -keyout /etc/ssl/private/proftpdserverkey.pem -out /etc/ssl/certs/proftpdcertificate.pem -days 365
Generating a 2048 bit RSA private key
..+++
.....+++
writing new private key to '/etc/ssl/private/proftpdserverkey.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:MX
State or Province Name (full name) [Some-State]:Mexico City
Locality Name (eg, city) []:Gustavo A Madero
Organization Name (eg, company) [Internet Widgits Pty Ltd]:ESCOM IPN
Organizational Unit Name (eg, section) []:Equipo 9 Redes 3
Common Name (e.g. server FQDN or YOUR name) []:FTP server
Email Address []:
jair@lap-jair:~$
```

Certificado con OpenSSL

```
tls.conf x
1 #
2 # Proftpd sample configuration for FTPS connections.
3 #
4 # Note that FTPS impose some limitations in NAT traversing.
5 # See http://www.castaglia.org/proftpd/doc/contrib/ProFTPD-mini-HOWTO-TLS.html
6 # for more information.
7 #
8
9 <IfModule mod_tls.c>
10
11 TLSRSCertificateFile /etc/ssl/certs/proftpdcertificate.pem
12 TLSRSCertificateKeyFile /etc/ssl/private/proftpdserverkey.pem
13 TLSEngine on
14 TLSLog /var/log/proftpd/tls.log
15 TLSProtocol SSLv23
16 TLSRequired on
17 TLSOptions NoCertRequest EnableDiags NoSessionReuseRequired
18 TLSVerifyClient off
19
20 #TLSEngine on
21 #TLSLog /var/log/proftpd/tls.log
22 #TLSProtocol SSLv23
23 #
24 # Server SSL certificate. You can generate a self-signed certificate using
25 # a command like:
26 #
```

## Configuración





Cliente verificando certificado

# SFTP



# SSH

---

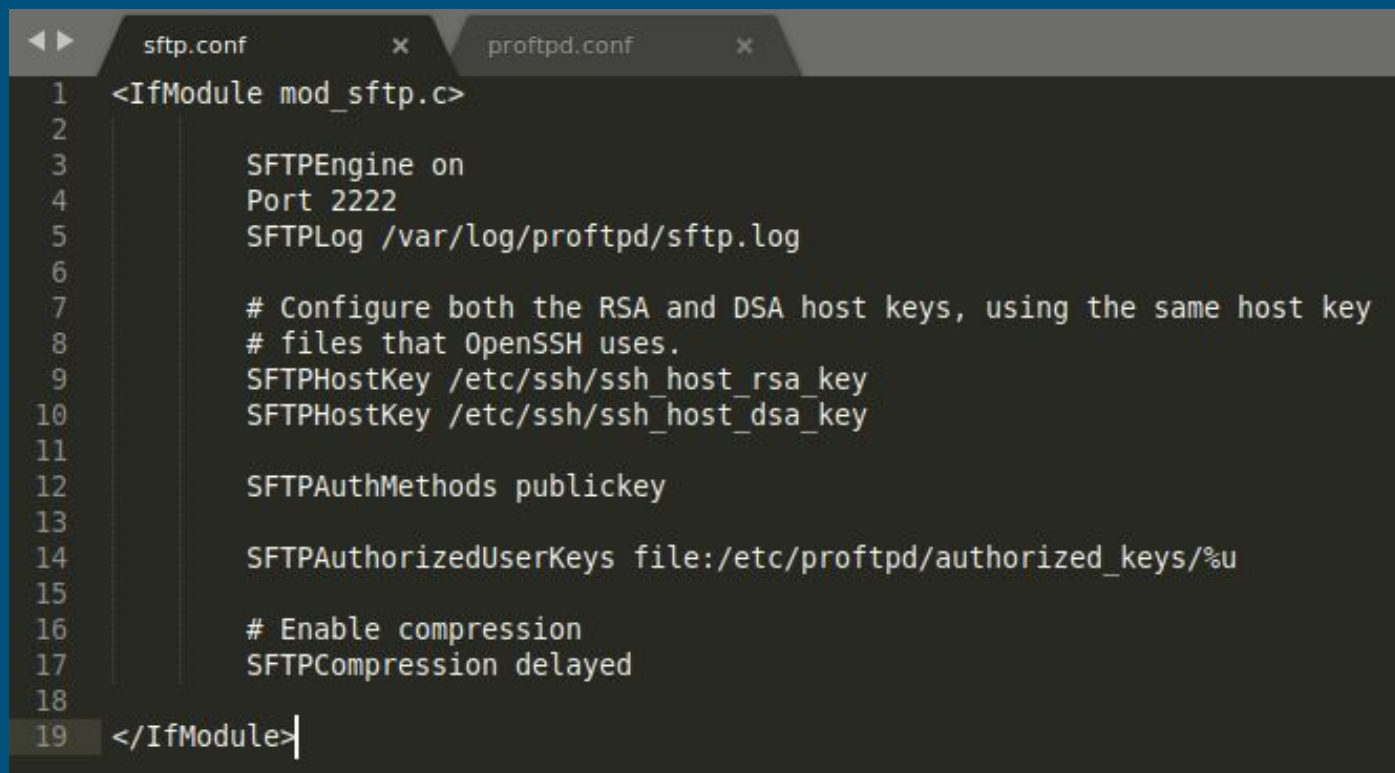
Esta opción es considerada más segura que la anterior, utiliza los servicios SSH para crear un canal de conexión segura entre el host y el cliente, se necesita de una clave pública por usuario relacionada con el host además de la clave del servidor.

```
jair@lap-jair:~/.ssh$ ssh-keygen -e -f ~jair/.ssh/authorized_keys | tee /etc/pro  
ftpd/authorized_keys/jair  
---- BEGIN SSH2 PUBLIC KEY ----  
Comment: "2048-bit RSA, converted by jair@lap-jair from OpenSSH"  
AAAAB3NzaC1yc2EAAAADAQABAAQBNwX1XTTkiLGC54A22AEKF669VYLrRmUmYBq7B/Q  
AwtoGzNxypmzgBMzpEP91ZD+r9b3e7hsA1HQJ7QFacHkY0diNlfeNgxdBkcwVEecrw5/z  
ZSIWzPG/UZtQ7G5uw30kjQZMjZvNfi32CeS87uiIRCenRIzC8+/EirPpCYV4qLl3tNu50i  
m7iOegwbDeLZeqBeov4Dmh3oR/RGvVkeRLR9sMfXhtqTUEtrl9udIDlz7Gh01QaSaD2pfQ  
zj5EY8jSt1kvCbSL/If6BmfUNqyNqu+UkSv7uKaJCSGhCNC4j3BJVpp1nScmnY9+bCZfbk  
GRwYF4Qv4nEjLRdfOyl0X5  
---- END SSH2 PUBLIC KEY ----
```

Creación de llaves en el servidor

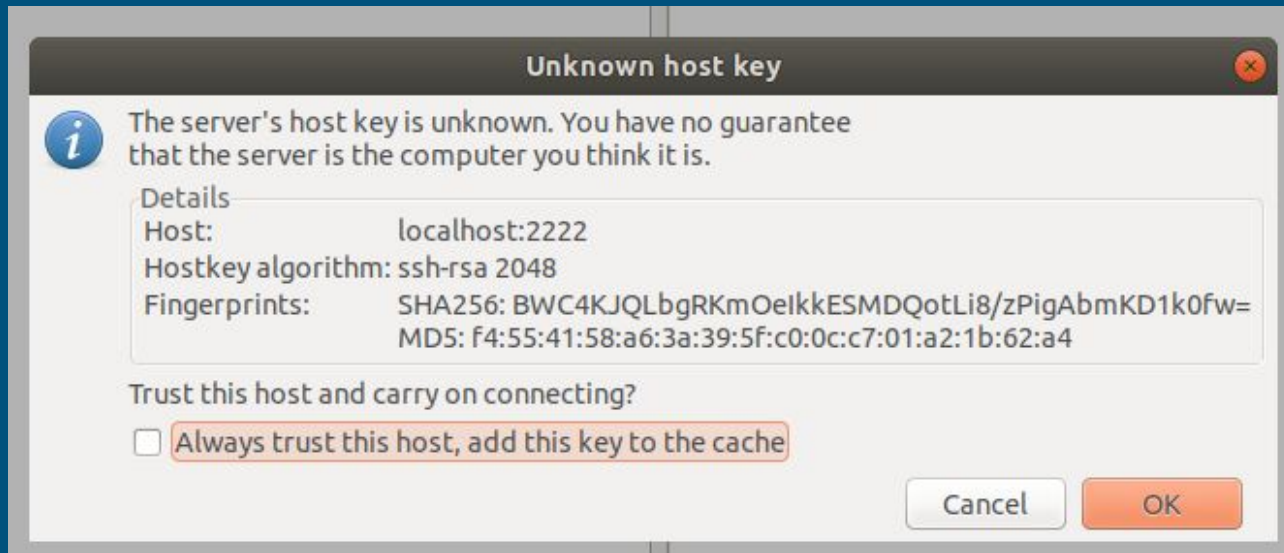
```
jair@lap-jair:~$ cd ~/.ssh/
jair@lap-jair:~/.ssh$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/jair/.ssh/id_rsa): id_rsa
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in id_rsa.
Your public key has been saved in id_rsa.pub.
The key fingerprint is:
SHA256:SaeVavhvZvoUkkgecxBL/4aH+pzhNJWB7cwqfmITKE jair@lap-jair
The key's randomart image is:
+---[RSA 2048]---+
|      .O.  .      |
|      . ..=..     |
|      .+.+++=.   |
|    Eo.O+Bo o    |
|    o++S*..      |
|    +o*.O.       |
|    oooo         |
|    .**          |
|    .=X+         |
+----[SHA256]-----+
jair@lap-jair:~/.ssh$ cat ~/.ssh/id_rsa.pub >> ~/.ssh/authorized_keys
```

Creación de llaves de cliente



```
1 <IfModule mod_sftp.c>
2
3     SFTPEngine on
4     Port 2222
5     SFTPLog /var/log/proftpd/sftp.log
6
7     # Configure both the RSA and DSA host keys, using the same host key
8     # files that OpenSSH uses.
9     SFTPHostKey /etc/ssh/ssh_host_rsa_key
10    SFTPHostKey /etc/ssh/ssh_host_dsa_key
11
12    SFTPAuthMethods publickey
13
14    SFTPAuthorizedUserKeys file:/etc/proftpd/authorized_keys/%u
15
16    # Enable compression
17    SFTPCompression delayed
18
19 </IfModule>
```

## Configuración



Verificación del certificado del host por el cliente

# Jaulas

---

Utilizando esta opción puedes direccionar la raíz de cada usuario, dejando la principal o mandando todos a una carpeta compartida (Con las directivas se pueden modificar para cada usuario)

```
# Use this to jail all users in their homes
#DefaultRoot          /home/public_FTP
DefaultRoot            ~
```



# BITÁCORAS

---

---

Otra opción que nos brinda el servidor proftpd es decidir qué nivel de mensajes vamos a guardar. La siguiente tabla muestra los niveles de mensaje implementados en el servidor:

Level	Description
EMERG	Fatal/unrecoverable error/condition, application is unusable and stops immediately
ALERT	Condition requires <b>immediate</b> intervention by administrator/operator
CRIT	Condition <b>should</b> be corrected immediately, but indicates <i>e.g.</i> failure in secondary system/library
ERR	Non-urgent failure conditions that should be relayed to developers and/or administrators; <b>should</b> be resolved/corrected soon
WARNING	Unexpected error/condition that <i>may</i> require intervention to review/correct
NOTICE	Significant/noteworthy condition, no intervention/action required
INFO	Normal operating conditions, no intervention/action required
DEBUG	Internal details of application operations useful to developers, not necessarily useful during normal operations

---

Los niveles están ordenados descendientemente por prioridad. Por default el servidor guarda todos los niveles de mensajes. Si queremos guardar solo a partir de cierto nivel, se utiliza la directiva SyslogLevel, cuya sintaxis es:

SyslogLevel <LEVEL>

Donde <LEVEL> será el nivel mínimo que se guardará en las bitácoras.

# RESÚMEN DE OPERACIÓN

---

---

Podemos crear un archivos de bitácora personalizado utilizando las siguientes directivas:

- LogFormat - Permite establecer el formato de la bitácora mediante la activación de distintas banderas y establecer un nombre para el formato.
- ExtendedLog - Permite establecer la ruta del archivo de bitácora personalizado y elegir el nombre del formato que establecimos.

# Referencias bibliográficas

---

- [1] <https://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-rg-es-4/ch-ftp.html>
- [2] <http://www.proftpd.org/docs/faq/faq.pdf>
- [3] <https://www.thegeekslearn.com/how-to-configure-sftp-in-proftpd/>
- [4] [http://proftpd.org/docs/directives/linked/config\\_ref\\_LogFormat.html](http://proftpd.org/docs/directives/linked/config_ref_LogFormat.html)
- [5] [http://proftpd.org/docs/directives/linked/config\\_ref\\_ExtendedLog.html](http://proftpd.org/docs/directives/linked/config_ref_ExtendedLog.html)