

Servidor_ftp_con_TLS

16/01/2024

Guillermo Bellettini

Seguridad

Creado por: Nicolas Pavel Ballesteros Barrado



Contenido

Servidor_ftp_con_TLS 1

Instalamos el vsftpd 3

Habilitamos el programa 3

Arrancamos el programa 4

Editamos el fichero vsftpd.conf 5

Generamos el certificado 7

Verificamos el archivo 8

Reniciamos el servicio 9

Y nos conectamos por ftp 11

Instalamos el vsftpd

Actualizamos el sistema

```
root@ubuntu:~# apt-get update
Obj:1 http://security.ubuntu.com/ubuntu bionic-security InRelease
Obj:2 http://es.archive.ubuntu.com/ubuntu bionic InRelease
Obj:3 http://es.archive.ubuntu.com/ubuntu bionic-updates InRelease
Obj:4 http://es.archive.ubuntu.com/ubuntu bionic-backports InRelease
Leyendo lista de paquetes... 69%
```

Instalamos el programa vsftpd

```
root@ubuntu:~# apt-get install vsftpd
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
El paquete indicado a continuación se instaló de forma automática y ya no es necesario.
  liblvm6.0
Utilice «sudo apt autoremove» para eliminarlo.
Se instalarán los siguientes paquetes NUEVOS:
  vsftpd
0 actualizados, 1 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
Se necesita descargar 115 kB de archivos.
Se utilizarán 334 kB de espacio de disco adicional después de esta operación.
Des:1 http://es.archive.ubuntu.com/ubuntu bionic/main amd64 vsftpd amd64 3.0.3-9build1 [115 kB]
Descargados 115 kB en 0s (352 kB/s)
Preconfigurando paquetes ...
Seleccionando el paquete vsftpd previamente no seleccionado.
(Leyendo la base de datos ... 90%
```

Habilitamos el programa

```
root@ubuntu:~# systemctl enable vsftpd
Synchronizing state of vsftpd.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable vsftpd
root@ubuntu:~#
```

Arrancamos el programa

```
root@ubuntu:~# systemctl start vsftpd
root@ubuntu:~# systemctl status vsftpd
● vsftpd.service - vsftpd FTP server
   Loaded: loaded (/lib/systemd/system/vsftpd.service; enabled; vendor preset: enabled)
   Active: active (running) since Tue 2024-01-16 18:01:38 CET; 4min 22s ago
     Main PID: 2737 (vsftpd)
        Tasks: 1 (limit: 2333)
      CGroup: /system.slice/vsftpd.service
             └─2737 /usr/sbin/vsftpd /etc/vsftpd.conf

ene 16 18:01:38 ubuntu systemd[1]: Starting vsftpd FTP server...
ene 16 18:01:38 ubuntu systemd[1]: Started vsftpd FTP server.
root@ubuntu:~#
```

Vemos que esta corriendo el programa

Editamos el fichero vsftpd.conf

```
1: root@ubuntu: ~
GNU nano 2.9.3 /etc/vsftpd.conf

# Example config file /etc/vsftpd.conf
#
# The default compiled in settings are fairly paranoid. This sample file
# loosens things up a bit, to make the ftp daemon more usable.
# Please see vsftpd.conf.5 for all compiled in defaults.
#
# 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.
#
# Run standalone? vsftpd can run either from an inetd or as a standalone
# daemon started from an initscript.
listen=NO
#
# This directive enables listening on IPv6 sockets. By default, listening
# on the IPv6 "any" address (:::) will accept connections from both IPv6
# and IPv4 clients. It is not necessary to listen on *both* IPv4 and IPv6
# sockets. If you want that (perhaps because you want to listen on specific
# addresses) then you must run two copies of vsftpd with two configuration
# files.
listen_ipv6=YES
#
# Allow anonymous FTP? (Disabled by default).
anonymous_enable=NO
#
# Uncomment this to allow local users to log in.
local_enable=YES
#
# Uncomment this to enable any form of FTP write command.
write_enable=YES
#
# Default umask for local users is 077. You may wish to change this to 022,
# if your users expect that (022 is used by most other ftpd's)
local_umask=022
#
# Uncomment this to allow the anonymous FTP user to upload files. This only
# has an effect if the above global write enable is activated. Also, you will
# obviously need to create a directory writable by the FTP user.
anon_upload_enable=YES
#
[ 155 líneas leídas ]
^G Ver ayuda ^O Guardar ^W Buscar ^K Cortar Texto ^J Justificar ^C Posición
^Y Salir ^P Leer fich ^A Reemplazar ^U Pegar txt ^T Ortografía ^_ Ir a línea
```

Descomentamos el write_enable

```
#
# Uncomment this to enable any form of FTP write command.
write_enable=YES
#
# Default umask for local users is 077. You may wish to change this to 022,
```

Descomentamos esto también

```
# (Warning! chroot'ing can be very dangerous. If using chroot, make sure that
# the user does not have write access to the top level directory within the
# chroot)
chroot_local_user=YES
#chroot_list_enable=YES
# (default follows)
#chroot_list_file=/etc/vsftpd.chroot_list
#
# You may activate the "-R" option to the builtin ls. This is disabled by
# default to avoid remote users being able to cause excessive I/O on large
# sites. However, some broken FTP clients such as "ncftp" and "mirror" assume
# the presence of the "-R" option, so there is a strong case for enabling it.
#ls_recurse_enable=YES
#
# Customization
#
```

Añadimos estas líneas

```
allow_writeable_chroot=YES
ssl_enable=YES
allow_anon_ssl=NO
force_local_data_ssl=YES
force_local_logins_ssl=YES
If ssl_tlsv1=YES
op ssl_sslv2=NO
ssl_sslv3=NO
|
```

Generamos el certificado

```
root@ubuntu:~# openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/vsftpd.pem -out /etc/ssl/private/vsftpd.pem
Can't load /root/.rnd into RNG
139729367527872:error:2406F079:random number generator:RAND_load_file:Cannot open file:../crypto/rand/randfile.c:88:Filename=/root/.rnd
Generating a RSA private key
.....+++++
....+++++
writing new private key to '/etc/ssl/private/vsftpd.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]:75
State or Province Name (full name) [Some-State]:Madrid
Locality Name (eg, city) []:Andorra
Organization Name (eg, company) [Internet Widgits Pty Ltd]:pavel.com
Organizational Unit Name (eg, section) []:pavel.com
Common Name (e.g. server FQDN or YOUR name) []:
Email Address []:
root@ubuntu:~# |
```

Vamos completando los campos que nos salen

Verificamos el archivo

```
root@ubuntu:~# cat /etc/ssl/private/vsftpd.pem
-----BEGIN PRIVATE KEY-----
MIIEvwIBADANBgkqhkiG9w0BAQEFAASCBAkKwggSlAgEAAoIBAQDAb+ZfzCYqUpnS
DfSpz9TsJPfIVWwO+TL9vZl5c8rczsSd+iYyE9ltHYWoCwP7qeV4mr4FmXthacJ4
rkAisActoujRmr+zAUnTZO2vZEGkHYyYjnyYiesJu+sBGt9tkcBY/P6XfLy5SJxER
eQb57uZDVnfpfgNY4n8RIKaibCq1BQMySk5WeW0mwEBu4XbvSd8rwBFjcrXXzwGI
A9GXQdauj/WUAakHK44fPGDqspqG5os9skYSG6GxEfvKCOBNhAfSuH3Rx/lyNNDf
qg3GKy/MbB4ULS8xNpES7vRayNN7sNq/2dbMycK0obkPxbeT516D1FblQxHxEmL9
RqyfPiKtAgMBAAECggEBAIiVI4qsyA3T8K8hDp0UEMjGeENuWFig0Ks90K4qHDra
WrzRlhiG9BQ5FustXldZv6/5DJPG2sZKHSgwbP7xtzaR4PMcBaGUcYSjpvuMifZk
rqx8uKZBGcpxGNVYm1PPJksf7qfYweS3K6seHnB4OmBi19sWgGou5ocOiJbRdQJi
3w0FqsDASSB6UtUNw8aQj2BvT87s2aSDxOuikHuUi9v4s0VmOLB+PL3yDnDV/vEN
ogsc2VxjsURXzA05GTuSuiHye2lEx7fyNlcAvMh+IRZNIay8IrPg3+jgYN0hB9K
xA3OpALys7B5qSO+R6oKyCisYMXlKbhWnySlzgnBANUCgYEA8rCgFHa/6b7MlaNI
N0ffIqKbRWf7PKoSgpO6Uik8Z5hyMSd3yiLuMEXGhkIhJ2NRLYkcgmbmtcNHfuSyP
LUNUlWUszaoIPjkSiugnHGTOSAZCmQGN3WBrWRLyqDJapznAHLntkNEULMngSegT
3t8r3bFsAm8r6G2Jk0pceYQTDRsCgYEAyv25IY0cIgx03Zv+pHyso8DGNitEcNru
r7VbM8P1tSlqWqOC5amdomEZBGuebxldmPbOEPLhQw+APccBPMfMYj/GOlogv30l
0lGHKOP4FwF3H2A8P3kljsCbJaeq/tkyTJzfNAYdXFsqK3sFvbyPxT7kPbU4/rKv
IpxtavnBc9cCgYEAJgnWxfBwg40/S9EPw4F51IrdHdLEQ2QN34Z/SW509ukLqBHz
gBeKVHO+4aAeqSBAvrsm0Zi+fqJyAyRmPCCFOXt8cIXvZLCAIyCVlXtJAMhKwpdw
Ym3K0B3jwVKoMvyEJf5YvhBUvb/tFyQQRNgIYYPf971NUvvtcw8lDsc1lAMCgYEA
kHXguq/hxZl30f6iSg0wD5mxv/6qxmYIV6OJNF3RDW8zES4siaUcOeNAGpU8O3Sh
16pNHGK9TSxK56wohUjre0BH0l9hzuURdYvv1H6I2FaCoCGsvr9UDjOkNjgMyTFp
SnyZnEed/Aw1BqyWeWEoMAeCByhhV2Fyof8RH4B+3CECgYAF4z178nNKE4A/N6ql
2i4CRfScfemZ6YmqThvW2gg67rlCemJlN5KHZNblu0I6uiOdvnIOK710NdUkYk5e
hGU2t3kwhlERs7ig7GO7jIDpD29aMrVk0fBct0tR/tNZwbd9MM1c0ZEwn3uaa2yW
6hlkKTPsWlqwRchdawEW+4NZIw==
-----END PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIDkTCCAnmgAwIBAgIUabFIgag19eGmEi96aGJCwGRu0p0wDQYJKoZIhvcNAQEL
BQAwWDELMAkGA1UEBhMCNzUxZDZANBgNVBAgMBk1hZHJpZDEQMA4GA1UEBwwHQW5k
b3JyYTESMBAGA1UECgwJcGF2ZDZlWwYyY29tMRIwEAYDVQQLEDA1wYXZlbnC5jb20wHhcN
MjQwMTE2MTcyNjQzWWhcNMjUwMTE2MTcyNjQzWjBYMQswCQYDVQQGEWI3NTEPMA0G
A1UECwwGTWVkcmlkMRwwDgYDVQQHDAdBbmRvcnJhMRIwEAYDVQQKDAlwYXZlbnC5jb20x
eJlAQBgNVBASMCXBhdmVsLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAM
Bv5l/MJipSmdIN9KnPlOwk98hXBY75Mv29nXlzytzOxJ36JjIT2W0d
```

Vemos que también esta en la configuración del servicio

```
# This string is the name of the PAM service vsftpd will use.
pam_service_name=vsftpd
#
# This option specifies the location of the RSA certificate to use for SSL
# encrypted connections.
rsa_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
rsa_private_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
ssl_enable=NO
#
# Uncomment this to indicate that vsftpd use a utf8 filesystem.
#utf8_filesystem=YES
```


Reniciamos el servicio

```
root@ubuntu:~# systemctl restart vsftpd
root@ubuntu:~# systemctl status vsftpd
● vsftpd.service - vsftpd FTP server
   Loaded: loaded (/lib/systemd/system/vsftpd.service; enabled; vendor preset: enabled)
   Active: active (running) since Tue 2024-01-16 19:37:07 CET; 2s ago
     Process: 1415 ExecStartPre=/bin/mkdir -p /var/run/vsftpd/empty (code=exited, status=0/SUCCESS)
    Main PID: 1416 (vsftpd)
       Tasks: 1 (limit: 2333)
      CGroup: /system.slice/vsftpd.service
              └─1416 /usr/sbin/vsftpd /etc/vsftpd.conf

ene 16 19:37:07 ubuntu systemd[1]: Starting vsftpd FTP server...
ene 16 19:37:07 ubuntu systemd[1]: Started vsftpd FTP server.
lines 1-11/11 (END)
```

Ponemos la configuración de filezilla

Gestor de sitios

eleccionar entrada:

- Mis sitios
 - Nuevo sitio

Nuevo sitio Nueva carpeta
Nuevo marcador Renombrar
Borrar Duplicado

General Avanzado Opciones de Transferencia Juego de caracteres

Protocolo: FTP - Protocolo de Transferencia de Archivos

Servidor: 10.68.16.43 Puerto:

Cifrado: Requiere FTP explícito sobre TLS

Modo de acceso: Preguntar la contraseña

Usuario: usuario

Contraseña:

Color de fondo: Ninguno

Comentarios:

Conectar Aceptar Cancelar



El certificado del servidor es desconocido. Por favor, examine cuidadosamente el certificado para asegurarse de que se puede confiar en el servidor.

Compare la huella digital que se muestra con la huella digital del certificado que tiene recibido de su administrador de servidor o proveedor de alojamiento de servidor.

Certificado**Vista previa**

Huella digital (SHA-256): b0:60:f0:a1:9f:ae:83:72:7d:cf:84:87:14:9b:35:c9:
c9:46:f5:73:71:82:d4:81:93:47:b4:e8:19:c4:12:1b

Huella digital (SHA-1): 1c:cd:9c:64:c8:a7:61:bc:79:5a:4e:5c:92:a3:b3:8d:89:1a:fe:24

Período de validez: De 28/09/2020 10:37:23 a 26/09/2030 10:37:23

Asunto

Nombre común: ubuntu

Nombre alternativo: ubuntu

Editor

Igual que el asunto, el certificado está autofirmado

Detalles

De serie: 00:c9:41:e6:cb:d7:c7:0d:dc

Algoritmo de clave pública: RSA con 2048 bits

Algoritmo de firma: RSA-SHA256

Detalles de la sesión

Sitio: 10.68.16.43:21

Protocolo: TLS1.3

Cifrado: AES-256-GCM

Intercambio de clave: ECDHE-SECP256R1-RSA-PSS-RSAE-SHA384 Mac: AEAD

¿Confiar en el certificado del servidor y continuar con la conexión?

☐ Confiar siempre en este certificado en futuras sesiones.

☐ Confiar en este certificado sobre los nombres de servidor alternativos de la lista.

Aceptar

Cancelar

El certificado

Y nos conectamos por ftp

Nuevo sitio - ftpes://usuario@10.68.16.43 - FileZilla

ArchivoEdiciónVerTransferenciaServidorMarcadoresAyuda

Servidor:Nombre de usuario:Contraseña:Puerto:Conexión rápida

Estado: El servidor no permite caracteres no ASCII.
Estado: Registrado en
Estado: Recuperando el listado del directorio...
Estado: Calculando compensación de la zona horaria del servidor...
Estado: Timezone offset of server is 0 seconds.
Estado: Directorio "/" listado correctamente

Sitio local: C:\Users\nicolas.ballesteros\

Default

Default User

DefaultAppPool

diego.romero

francisco.cruz2

nicolas.ballesteros

Public

ruben.barreno

Windows

D:

E: (Video)

Sitio remoto: /

Descargas

Documentos

Escritorio

Imágenes

Música

Plantillas

Público

Videos

Nombre de archivo	Tamaño de...	Tipo de archivo	Última modificación
..		Carpeta de archivos	26/10/2023 17:17:43
.ssh		Carpeta de archivos	16/01/2024 18:49:31
.VirtualBox		Carpeta de archivos	16/01/2024 18:49:31
.vscode		Carpeta de archivos	21/09/2023 19:26:15
3D Objects		Carpeta de archivos	18/09/2023 15:09:02
AppData		Carpeta de archivos	18/09/2023 15:08:47
Cisco Packet Tracer 6.1sv		Carpeta de archivos	04/12/2023 16:34:20
Configuración local		Carpeta de archivos	12/01/2024 17:52:42
Contacts		Carpeta de archivos	18/09/2023 15:09:02
Cookies		Carpeta de archivos	22/09/2023 18:41:35
Datos de programa		Carpeta de archivos	23/10/2023 18:47:56
Desktop		Carpeta de archivos	12/01/2024 17:52:52
Documents		Carpeta de archivos	09/01/2024 18:17:54
Downloads		Carpeta de archivos	16/01/2024 18:34:01
Entorno de red		Carpeta de archivos	07/12/2019 10:14:52

8 archivos y 30 directorios. Tamaño total: 6.287.596 bytes

Nombre de archivo	Tamaño d...	Tipo de arc...	Última modific...	Permisos	Propietario/...
..		Carpeta de...	09/10/2020	drwxr-xr-x	1000 1000
Descargas		Carpeta de...	28/09/2020	drwxr-xr-x	1000 1000
Documentos		Carpeta de...	09/10/2020	drwxr-xr-x	1000 1000
Escritorio		Carpeta de...	28/09/2020	drwxr-xr-x	1000 1000
Imágenes		Carpeta de...	28/09/2020	drwxr-xr-x	1000 1000
Música		Carpeta de...	28/09/2020	drwxr-xr-x	1000 1000
Plantillas		Carpeta de...	28/09/2020	drwxr-xr-x	1000 1000
Público		Carpeta de...	28/09/2020	drwxr-xr-x	1000 1000
Videos		Carpeta de...	28/09/2020	drwxr-xr-x	1000 1000
adjunto_codificado.txt	21	Document...	11/01/2024 17:...	-rw-rw-r--	1000 1000
mbox	3.232	Archivo	11/01/2024 17:...	-rw-rw-r--	1000 1000

2 archivos y 8 directorios. Tamaño total: 3.253 bytes