

Tabla de contenido

[1. Introducción 3](#_Toc119871869)

[2. Generación del certificado 4](#_Toc119871870)

[2.1. Instalación de repositorios necesarios 4](#_Toc119871873)

[2.2. Configuración del certificado 4](#_Toc119871874)

[3. Configuración del servidor FTP 6](#_Toc119871875)

[3.1. Habilitar el módulo TLS 6](#_Toc119871877)

[4. Pruebas realizadas 7](#_Toc119871878)

[4.1. Conexión 7](#_Toc119871880)

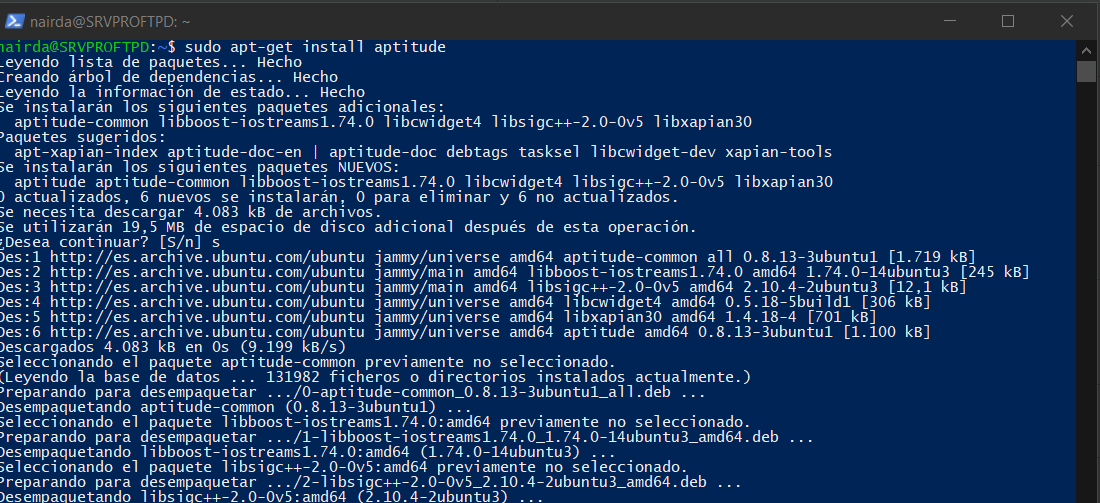
[5. Bibliografía 8](#_Toc119871882)

1. Introducción

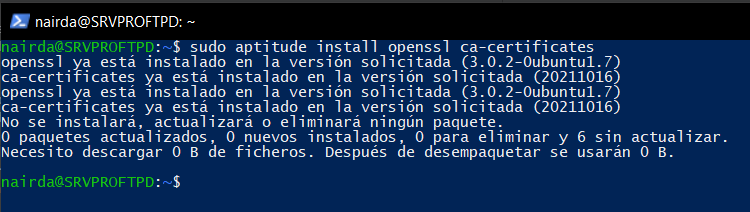
Partiendo de la práctica anterior, vamos a configurar el servidor para que a partir de ahora las comunicaciones las realice a través de un protocolo seguro, como es SFTP que cifra las comunicaciones con un certificado y encripta la comunicación de modo que, si se filtra alguna comunicación, esta no vaya en texto plano como ocurría con la práctica anterior.

1. Generación del certificado
3. 1. Instalación de repositorios necesarios

Lo primero que tenemos que hacer es instalar el repositorio “aptitude”, que nos otorga acceso a los programas necesarios para la generación del certificado.

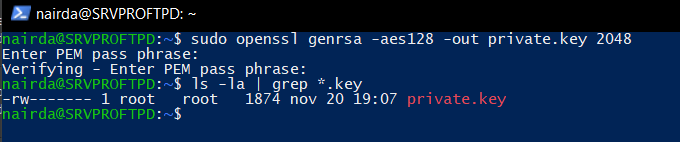


Tras intentar instalar los repositorios, comprobamos que ya estaban instalados en el sistema en la versión requerida.

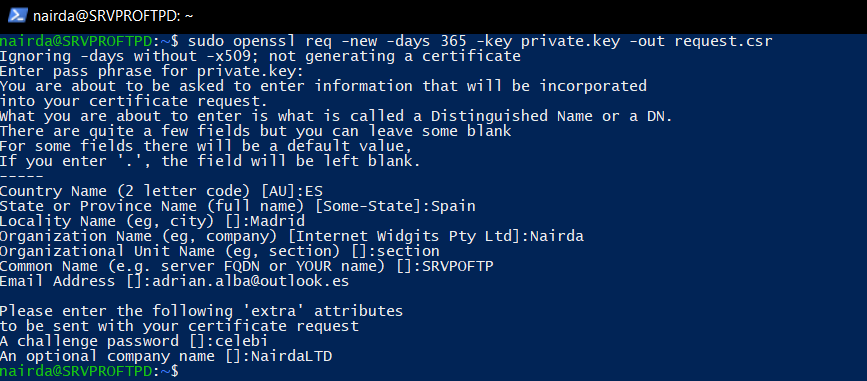


* 1. Configuración del certificado

Antes de generar el certificado autofirmado, tenemos que generar el certificado público con la clave. Esto se hace mediante el comando “*openssl genra -aes128 -out private.key 2048*”, este comando indica que se va a generar una nueva clave pública, con nombre private key, con un algoritmo de encriptación de tipo AES128. Se podrían haber elegido otro tipo de encriptaciones como podrían haber sido SHA1 o en su defecto SHA256.

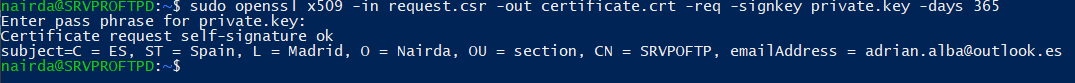


Tras generar la clave pública, se necesita hacer el “*request*” de la clave privada para que sea generada. Para ello se utiliza el comando “*openssl req -new -days 365 -key <NOMBRE DE LA KEY> -out request-csr*”. En este comando observamos como se le indica el periodo válido de la clave privada, es decir, cada cuanto tiempo va a ser válida y cuando hemos de renovarla

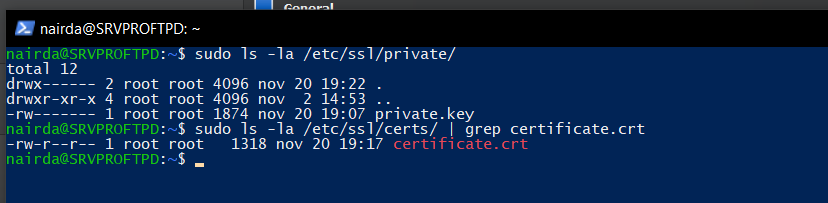


Cuando lanzamos el comando, nos va solicitando una seria de datos para introducirlos en el certificado, como pueden ser el nombre de la organización, donde se encuentra el certificado, y demás.

Una vez generada la clave privada, se procede a generar el certificado que vamos a utilizar en nuestro servidor FTP. Para ello, utilizando el comando “*openssl x509 -in request.csr -out certificate.crt -req -singkey private.key -days 365*”.

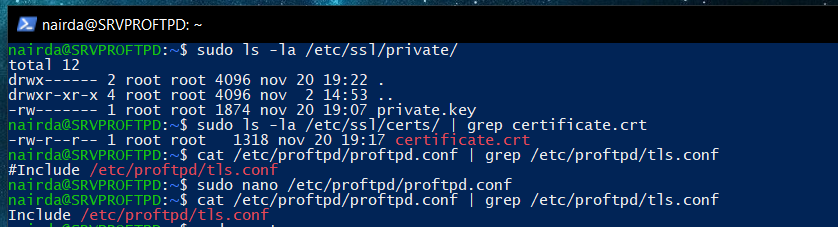


Una vez generado el certificado, movemos los ficheros que hemos generado a su correspondiente carpeta, la clave privada a la carpeta **/etc/ssl/private** y el certificado a **/etc/ssl/certs**.



1. Configuración del servidor FTP
2. 1. Habilitar el módulo TLS

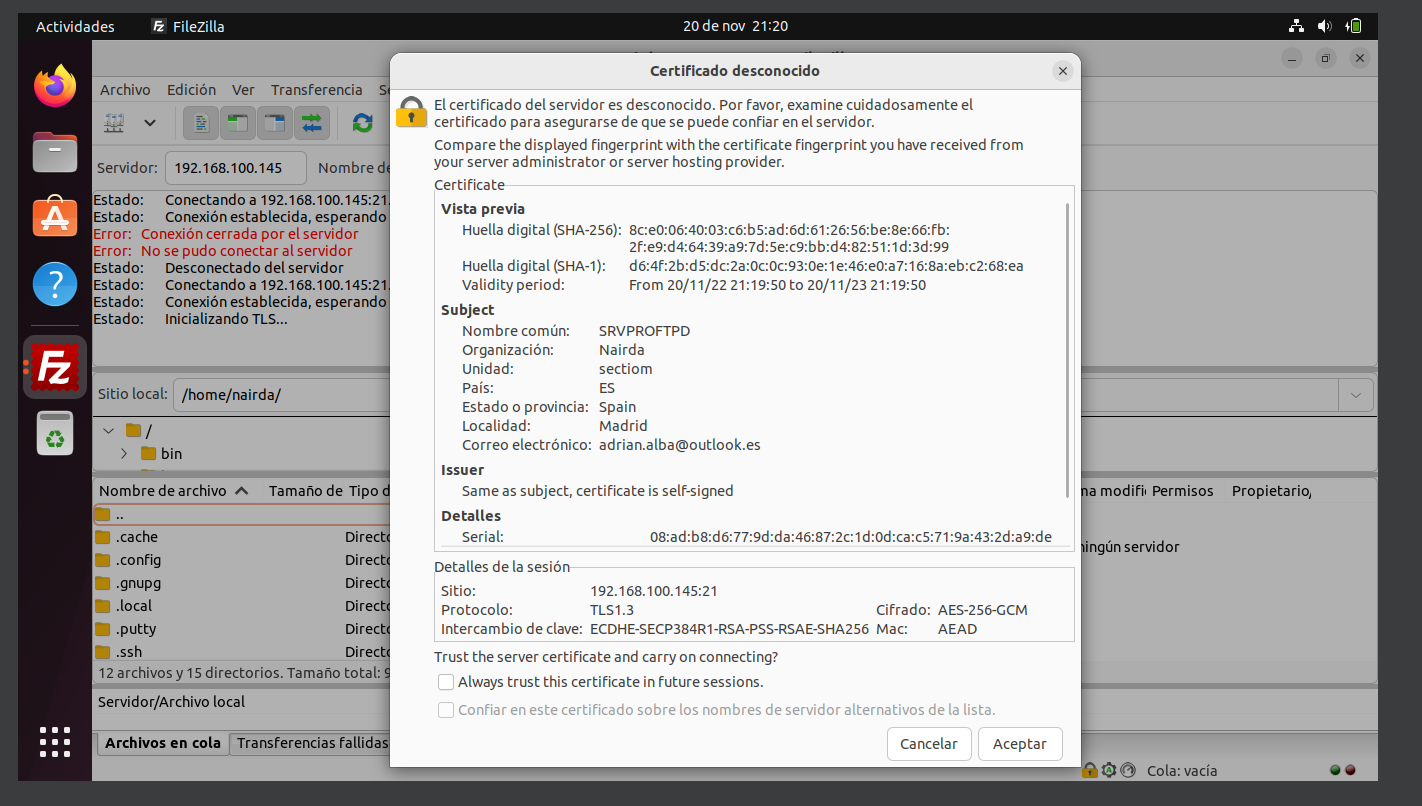
Tras la generación del certificado, hemos de habilitar el módulo que nos permita conectarnos a través de TLS al servidor FTP. Para ello, hemos de descomentar la línea que incluye el módulo TLS.



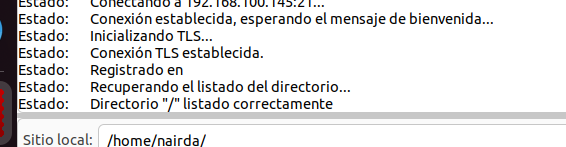
Se instala el módulo proftpd-mod-crypto, y se habilita el tls en el fichero de configuración **/etc/proftpd/proftpd.conf** y en **/etc/proftpd/tls.conf** se le indica donde encontrar los ficheros de la clave privada y del certificado, además de habilitar la comunicación TLS.

1. Pruebas realizadas
2. 1. Conexión

Cuando vamos a iniciar sesión en el servidor utilizando TLS por primera vez, nos pedirá añadir a nuestra lista de claves públicas la del servidor. Este paso es normal debido a que no lo teníamos previamente listado en nuestro fichero de claves públicas.



Tras guardar la clave, reinicia la conexión, y nos permite conectarnos al servidor utilizando un protocolo seguro de comunicación.



2. Bibliografía

* <https://www.arubacloud.com/tutorial/how-to-create-a-self-signed-ssl-certificate-on-ubuntu-18-04.aspx>
* <https://www.server-world.info/en/note?os=Ubuntu_22.04&p=ssl&f=1>