

Instalar certificado HTTPS



Certbot letsencrypt

Instalar certificado para HTTPS con Certbot

 [Javier Izquierdo \(https://weblinus.com/author/javierizdo/\)](https://weblinus.com/author/javierizdo/) -  10/01/2022 -

 [Hosting_ \(https://weblinus.com/category/manuales/hosting/\)](https://weblinus.com/category/manuales/hosting/) -

 [2 comentarios \(https://weblinus.com/instalar-certificado-para-https-con-certbot/#comments\)](https://weblinus.com/instalar-certificado-para-https-con-certbot/#comments)

¿INTERESANTE? SI TE GUSTA, ¡COMPARTELO!

1%201
ok.c
Fweb
s-r
nux%
22Lir
2Fwe
cor

Usamos cookies propias y de terceros para mejorar tu experiencia en nuestro sitio. Al continuar navegando entendemos que aceptas nuestra política de cookies.

[Configuración de Cookies](#)

Aceptar



Instalar certificado para HTTPS con Certbot

En los posts anteriores hemos instalado y configurado la pila LEMP «Linux, Nginx, MariaBD y PHP». En este, vamos a ver como instalar un certificado SSL/TLS para securizar nuestro sitio web. Para ello utilizaremos **Cerbot**.

No obstante, si estás buscando agregar los beneficios de seguridad y privacidad de un certificado HTTPS a tu sitio web, es posible que no necesites **Certbot**. Muchos proveedores de alojamiento tienen herramientas internas para habilitar HTTPS. Antes de utilizar **Certbot**, comprueba si tu proveedor de alojamiento es uno de ellos.

Certbot renueva los certificados cada 60 días. Para obtener más información sobre cómo funciona **Certbot** y los recursos administrados por la comunidad, consulta la siguiente [página de ayuda de Cerbot \(https://certbot.eff.org/pages/help\)](https://certbot.eff.org/pages/help).

El complemento **Certbot** admite las arquitecturas x86_64, ARMv7 y ARMv8. Si bien es altamente recomendable, y más sencillo, instalar **Certbot** a través del complemento, puedes encontrar [instrucciones de instalación alternativas \(https://certbot.eff.org/instructions\)](https://certbot.eff.org/instructions) en este enlace.

Sumario

- Consideraciones previas
- SSH instalado en el servidor
- Instalacion de snapd
 - Distribuciones con snap preinstalado.
 - Distribuciones sin snap preinstalado.
 - Instalación de snap en Debian
- Certbot
- Desinstalación de certbot-auto
- Instalar Certbot
- Modos de ejecución de Certbot
 - Obtener e instalar el certificados
 - O solo obtener un certificado
- Confirmar que el certificado funciona

Usamos cookies propias y de terceros para mejorar tu experiencia en nuestro sitio. Al continuar navegando entendemos que aceptas nuestra política de cookies.



Consideraciones previas

La **línea de comandos** es una forma de interactuar con una máquina escribiendo comandos basados en texto y recibiendo respuestas basadas en texto. **Certbot** se ejecuta desde una interfaz de **línea de comandos**, generalmente en un servidor similar a **Unix**. Para utilizar **Certbot** para la mayoría de los propósitos, deberemos poder instalarlo y ejecutarlo en la **línea de comandos** de nuestro **servidor web**, al que generalmente accederemos a través de **SSH**.

Para que los **navegadores web** soliciten el contenido de las **páginas web** y otros recursos en línea de los **servidores web**, **HTTP** (Protocolo de transferencia de hipertexto) es el método tradicional, pero es inseguro. Es un estándar de Internet que normalmente utiliza el puerto **TCP 80**. Casi todos los sitios web del mundo admiten **HTTP**, pero los sitios web que se han configurado con **Certbot** o algún otro método para configurar **HTTPS** pueden redirigir automáticamente a los usuarios desde la versión **HTTP** del sitio a la versión **HTTPS**.

Prerequisitos

Para instalar el certificado debes tener un dominio de tu propiedad, **Certbot** se utiliza, generalmente, para cambiar un sitio existente, que utiliza el protocolo **HTTP**, al uso del protocolo **HTTPS** (**Certbot** realizará las renovaciones del certificado cuando sea necesario). Partimos de la premisa de que tenemos un sitio web que escucha en el **puerto 80** con el protocolo **HTTP**.

Es decir, que si introducimos en un navegador web **http://nuestro_sitio_web**, el servidor responde y aparece algún tipo de contenido (aunque sea una página de bienvenida y no la definitiva que vayamos a crear). Algunos métodos para usar **Certbot** tienen esto como un requisito previo, por ello, lo mejor es que tengamos un sitio configurado con **HTTP**, escuchando en el **puerto 80**. Si no se puede acceder a nuestro sitio así, para obtener un certificado con **Certbot**, necesitaremos hacer una validación de **DNS**.

Los diferentes servicios de Internet utilizan, normalmente, unos **puertos específicos TCP**. El protocolo sin cifrar **HTTP** usa el **puerto 80** y **HTTPS**, cifrado, el **443**.

Cerbot

Para usar el **complemento independiente de certbot**, no necesitamos un sitio pre-existente, pero tenemos que asegurarnos de que las conexiones al **puerto 80** de nuestro servidor no estén bloqueadas por un **firewall**, como **UFW** o incluso, un **firewall** del proveedor de servicios de Internet o del proveedor de alojamiento web. El uso de la **validación de DNS** no requiere que **Let's Encrypt** realice ninguna conexión entrante a nuestro servidor, por lo que con este método, no es necesario tener un sitio web **HTTP** existente o la capacidad de recibir conexiones en el **puerto 80**.

Certbot actualmente requiere que tengamos instalada la versión de Python 3.6 o superior en un sistema operativo similar a UNIX. Por defecto, requiere acceso de root para escribir en /etc/letsencrypt, /var/log/letsencrypt, /var/lib/letsencrypt, para enlazar al puerto 80, si usamos el complemento independiente, y para leer y modificar las configuraciones del servidor web, si usamos los complementos apache o nginx. Si no utilizamos estos complementos, deberíamos poder ejecutarlo sin privilegios de root, pero para la mayoría de los usuarios que quieren evitar ejecutar un cliente ACME como root, letsencrypt-nosudo o simp_le son las opciones más apropiadas.

SSH instalado en el servidor

Necesitamos tener instalado SSH en el servidor que ejecuta el sitio web HTTP y un usuario con privilegios de sudo. Puedes ver como se [instala y configura \(https://weblinus.com/configuracion-servidor-ssh/\)](https://weblinus.com/configuracion-servidor-ssh/) en este enlace.

Nos conectamos al servidor con ssh

1. `ssh usuario@ip_servidor`



Instalación de snapd

Necesitamos instalar snapd y habilitar el soporte de snap clásico.

La mayoría de las distribuciones GNU/Linux modernas, prácticamente todas las que usan systemd Usamos cookies propias y de terceros para mejorar tu experiencia en nuestro sitio. Al continuar navegando puedes instalar Certbot como un complemento. Los snaps están disponibles para **arquitecturas x86_64, ARMv7 y ARMv8.** El complemento Certbot proporciona una manera fácil de **a Configuración de Cookies** **Actualizaremos la última versión de Certbot con características como la renovación automática de certificados preconfigurada.**

Distribuciones con snap preinstalado

KDE Neon, Manjaro, Solus 3 y posteriores, Ubuntu 20.10 y Ubuntu 21.04, Ubuntu 20.04 LTS (Focal Fossa), Ubuntu 18.04 LTS (Bionic Beaver), la mayoría de los sabores Ubuntu, Zorin OS.

Distribuciones sin snap preinstalado

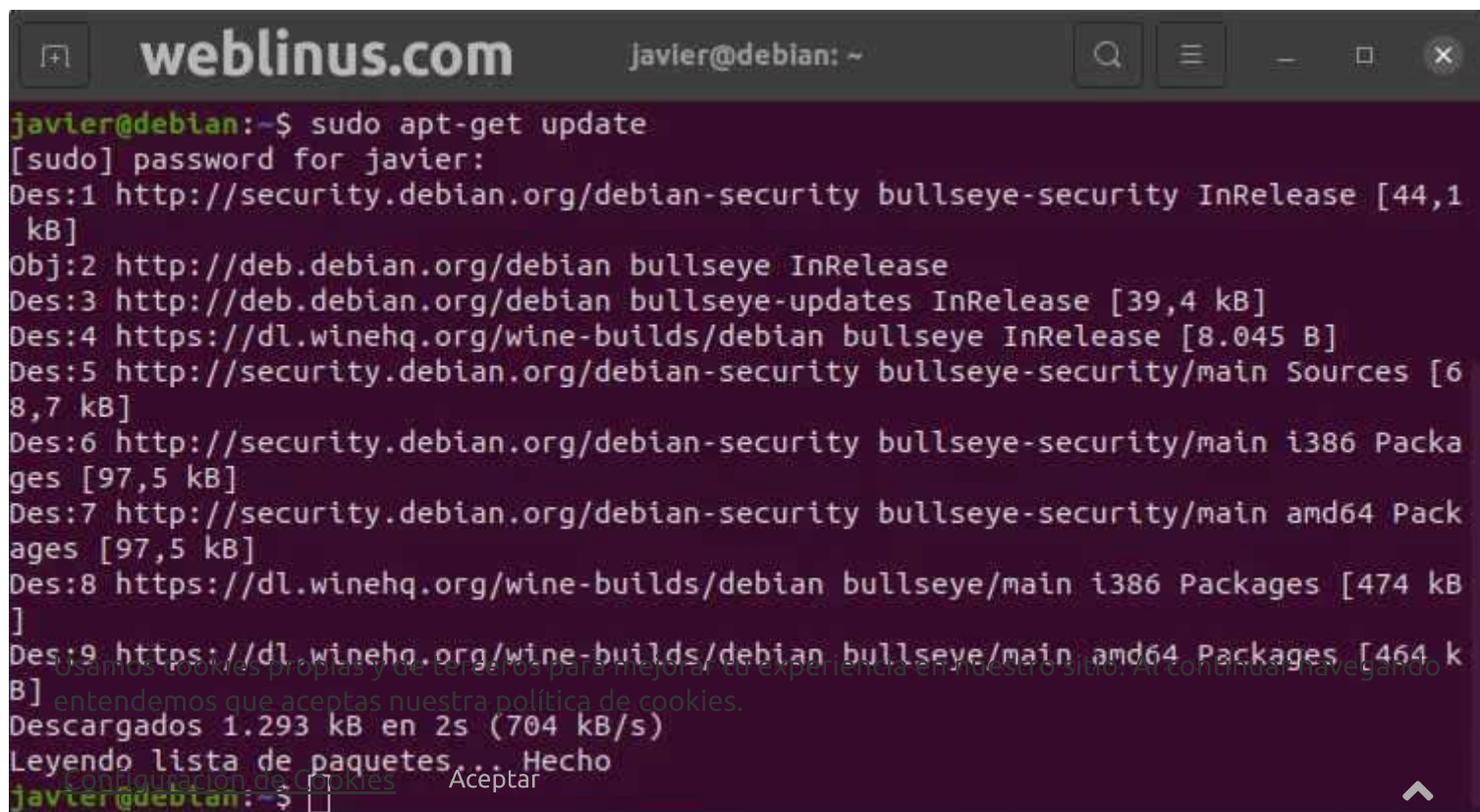
Arch Linux, CentOS, Debian, Elementary OS, Fedora, GalliumOS, Kali Linux, KDE Neon*, Kubuntu, Linux Mint, Lubuntu, Manjaro*, openSUSE, Parrot Security OS, Pop!_OS, Raspberry Pi OS, Red Hat Enterprise Linux (RHEL), Rocky Linux, Solus, Ubuntu*, Xubuntu, Zorin OS*.

NOTA: *Snap está preinstalado en estos sistemas. Si queremos volver a instalar Snap o tenemos alguna versión anterior, las siguientes instrucciones de instalación nos pueden ayudar.

Instalación de snap en Debian

Como siempre que vamos a instalar algo, actualizamos la lista de paquetes de los repositorios

1. `sudo apt-get update`



```
javier@debian:~$ sudo apt-get update
[sudo] password for javier:
Des:1 http://security.debian.org/debian-security bullseye-security InRelease [44,1 kB]
Obj:2 http://deb.debian.org/debian bullseye InRelease
Des:3 http://deb.debian.org/debian bullseye-updates InRelease [39,4 kB]
Des:4 https://dl.winehq.org/wine-builds/debian bullseye InRelease [8.045 B]
Des:5 http://security.debian.org/debian-security bullseye-security/main Sources [68,7 kB]
Des:6 http://security.debian.org/debian-security bullseye-security/main i386 Packages [97,5 kB]
Des:7 http://security.debian.org/debian-security bullseye-security/main amd64 Packages [97,5 kB]
Des:8 https://dl.winehq.org/wine-builds/debian bullseye/main i386 Packages [474 kB]
Des:9 https://dl.winehq.org/wine-builds/debian bullseye/main amd64 Packages [464 kB]
Descargados 1.293 kB en 2s (704 kB/s)
Leyendo lista de paquetes... Hecho
javier@debian:~$
```

Instalamos el demonio directamente desde los repositorios con el comando

1. `sudo apt-get install snapd`

A terminal window titled 'weblinus.com' with the user 'javier@debian: ~'. The terminal shows the command 'sudo apt-get install snapd' being executed. The output indicates that the package list is read, dependencies are created, and state information is read. It lists 'squashfs-tools' as an additional package to be installed along with 'snapd'. It also shows the disk space requirements: 13.4 MB for download and 56.7 MB for additional disk space after installation. The prompt asks '¿Desea continuar? [S/n]' with a cursor.

Le decimos que si «S», y continuará con la instalación.

Si no tenemos el comando `sudo` instalado, seguramente por proporcionar una contraseña de root durante la instalación del S.O., podemos instalar `snap` convirtiéndonos en root primero, con los siguientes comandos

1. `su root`
2. `apt-get update`
3. `apt-get install snapd`

Una vez instalado `snap`, tenemos que cerrar la sesión o reiniciar el sistema, para que las rutas de `Snap` se actualicen correctamente. Lo hacemos con «`sudo reboot`». Nos cerrara la conexión por `ssh` y deberemos volver a conectarnos para seguir con la instalación. Ten en cuenta que si el servidor no está a tu alcance físicamente, si lo cierras con «`sudo shutdown now`», no podrás volver a arrancarlo.

Usamos cookies propias y de terceros para mejorar tu experiencia en nuestro sitio. Al continuar navegando entendemos que aceptas nuestra política de cookies.

[Configuración de Cookies](#)

Aceptar



```
weblinus.com javier@debian: ~
javier@debian:~$ sudo reboot
javier@debian:~$ Connection to 192.168.1.16 closed by remote host.
Connection to 192.168.1.16 closed.
javier@javier2:~$ ssh javier@192.168.1.16
javier@192.168.1.16's password:
Linux debian 5.10.0-8-amd64 #1 SMP Debian 5.10.46-5 (2021-09-23) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Dec  8 19:49:23 2021 from 192.168.1.14
javier@debian:~$
```

Ahora tenemos que instalar el complemento principal para obtener el último complemento.

1. `sudo snap install core`

```
weblinus.com javier@debian: ~
javier@debian:~$ sudo snap install core
[sudo] password for javier:
2021-12-08T20:10:52+01:00 INFO Waiting for automatic snapd restart...
core 16-2.52.1 from Canonical✓ installed
javier@debian:~$
```

Vemos la versión instalada en la captura anterior

1. `core 16-2.52.1 from Canonical✓ installed`

Nota: algunas instantáneas requieren nuevas funciones de `snapd` y mostrarán un error como «`snap lxd` asume características no admitidas» durante la instalación. Para resolver este problema tenemos que asegurarnos de que el `snap` principal está instalado con «`sudo snap install core`» y que sea la última versión con «`sudo snap refresh core`».

Y ya tenemos instalado y listo para funcionar **Snap**. Si estamos utilizando un S.O. escritorio, con entorno gráfico, ahora podríamos instalar la aplicación «**Snap Store**».

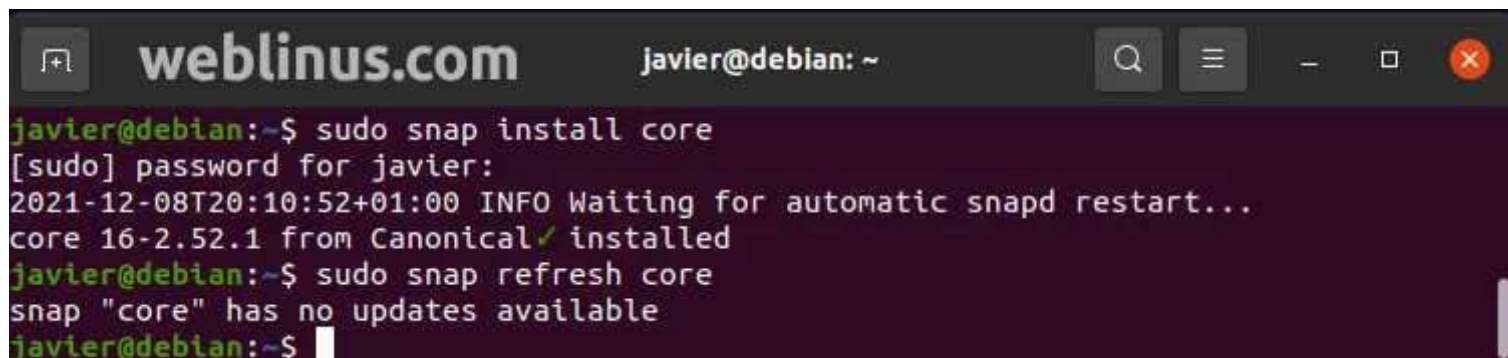
En versiones anteriores a Debian 9 no está disponible Snap.

Usamos cookies propias y de terceros para mejorar tu experiencia en nuestro sitio. Al continuar navegando entendemos que aceptas nuestra política de cookies.

Para instalar el demonio en otras distribuciones, consulta la [página oficial del proyecto](https://snapcraft.io/docs/installing-snapd) (<https://snapcraft.io/docs/installing-snapd>).

Para asegurarnos de que **snap** esta actualizado a la última versión, tenemos que ejecutar los siguientes comandos.

1. `sudo snap refresh core`

A terminal window with a dark purple background. The title bar shows 'weblinus.com' on the left and 'javier@debian: ~' on the right. The terminal text shows a user running 'sudo snap install core', followed by a password prompt, a log message '2021-12-08T20:10:52+01:00 INFO Waiting for automatic snapd restart...', and a confirmation 'core 16-2.52.1 from Canonical✓ installed'. Then the user runs 'sudo snap refresh core', and the output is 'snap "core" has no updates available'.

```
javier@debian:~$ sudo snap install core
[sudo] password for javier:
2021-12-08T20:10:52+01:00 INFO Waiting for automatic snapd restart...
core 16-2.52.1 from Canonical✓ installed
javier@debian:~$ sudo snap refresh core
snap "core" has no updates available
javier@debian:~$
```

Certbot

Certbot es un proyecto gratuito de código abierto, parte del compromiso de EFF «Electronic Frontier Foundation» de hacer que el cifrado sea accesible para todos.

Certbot es una herramienta de software de código abierto y gratuita para usar automáticamente los certificados «Let's Encrypt» en sitios web administrados manualmente para habilitar HTTPS.

Certbot está creado por «Electronic Frontier Foundation» (EFF), una organización sin ánimo de lucro, con sede en San Francisco. Una CA «Autoridad Certificadora», que defiende la privacidad digital, la libertad de expresión y la innovación.

Para instalar **Cerbot**, previamente tenemos que eliminar **certbot-auto** y cualquier paquete **Certbot** de nuestro S.O.

Si tenemos algún paquete de **Certbot**, instalado utilizando un administrador de paquetes de sistema operativo como **apt**, **dnf** o **yum**, deberemos eliminarlo antes de instalar el complemento **Certbot**, para asegurarnos de que cuando ejecute el comando **certbot**, se utilice el complemento, en lugar de la instalación desde el paquete del S.O. Según que S.O. utilicemos, el comando a ejecutar será diferente, dependiendo del gestor de paquetes nativo del S.O. Los más comunes son: «**sudo apt-get remove certbot**», «**sudo dnf remove certbot**» o «**sudo yum remove certbot**».

Usamos cookies propias y de terceros para mejorar tu experiencia en nuestro sitio. Al continuar navegando entendemos que aceptas nuestra política de cookies.

[Configuración de Cookies](#)

Aceptar




```
weblinus.com    javier@debian: ~
javier@debian:~$ sudo apt-get remove certbot
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
El paquete «certbot» no está instalado, no se eliminará
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 2 no actualizados.
javier@debian:~$
```

Si hubiésemos utilizado **Certbot** a través del script **certbot-auto**, también necesitaríamos eliminar su instalación. Veamos como hacerlo.

Desinstalación de certbot-auto

El procedimiento para **desinstalar certbot-auto**, son tres pasos:

1.- Si, para renovar nuestros certificados, tenemos una **tarea cron** o un temporizador **systemd** que ejecute **certbot-auto** automáticamente, es necesario eliminarlo. Podemos eliminar la entrada a **/etc/crontab** ejecutando el siguiente comando como **sudo**

```
1.    sudo sed -i '/certbot-auto/d' /etc/crontab
```

2.- Tenemos que eliminar el script **certbot-auto**. Lo normal es que lo tengamos en **/usr/local/bin**. Ejecutamos

```
1.    sudo rm /usr/local/bin/certbot-auto
```

3.- También tenemos que **eliminar la instalación de Certbot** creada por **certbot-auto** ejecutando

```
1.    sudo rm -rf /opt/eff.org
```

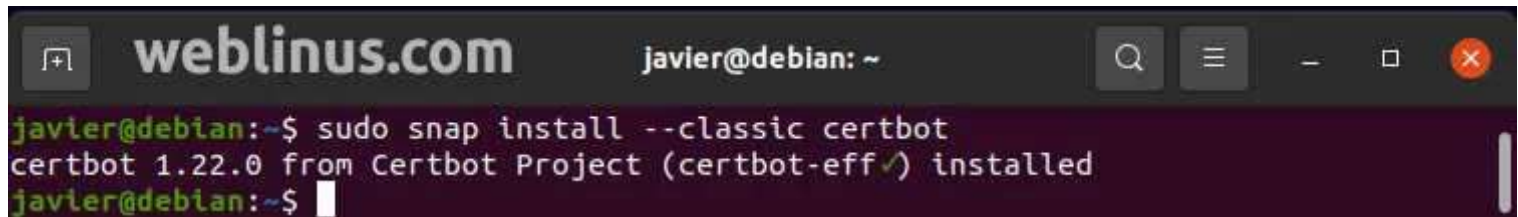
Instalar Certbot

Usamos cookies propias y de terceros para mejorar tu experiencia en nuestro sitio. Al continuar navegando aceptas nuestra política de cookies.

Para realizar la nueva instalación de **Certbot**, ejecutamos el siguiente comando

```
Configuración de Cookies    Aceptar
1.    sudo snap install --classic certbot
```



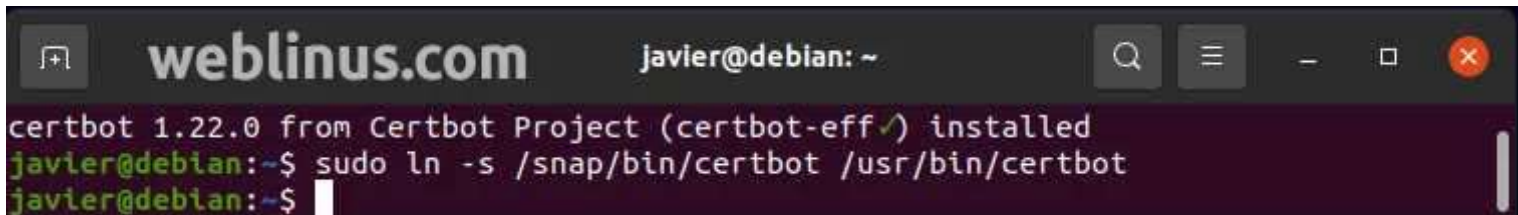


```
weblinus.com    javier@debian: ~
javier@debian:~$ sudo snap install --classic certbot
certbot 1.22.0 from Certbot Project (certbot-eff✓) installed
javier@debian:~$
```

1. `certbot 1.22.0` from Certbot Project (certbot-eff✓) installed

Para asegurarnos de que se puede ejecutar el **comando certbot**, ejecutamos la siguiente instrucción para crear un enlace

1. `sudo ln -s /snap/bin/certbot /usr/bin/certbot`



```
certbot 1.22.0 from Certbot Project (certbot-eff✓) installed
javier@debian:~$ sudo ln -s /snap/bin/certbot /usr/bin/certbot
javier@debian:~$
```

Modos de ejecución de Certbot

Tenemos dos opciones para ejecutar cerbot.

Obtener e instalar el certificado

Ejecutando este comando obtendremos un certificado y Certbot editará la configuración de nginx automáticamente para servirla, activando el acceso HTTPS en un solo paso. Se ejecutará un script que hará toda la configuración por nosotros. Opcionalmente, podemos instalar este certificado en servidores web compatibles (como Apache o nginx) y otros tipos de servidores. Esto se hace modificando automáticamente la configuración de nuestro servidor para poder utilizar el certificado.

1 `sudo certbot --nginx`

Usamos cookies propias y de terceros para mejorar tu experiencia en nuestro sitio. Al continuar navegando entendemos que aceptas nuestra política de cookies.

```
weblinus.com      javier@debian: ~
If you really want to skip this, you can run the client with
--register-unsafely-without-email but you will then be unable to receive notice
about impending expiration or revocation of your certificates or problems with
your Certbot installation that will lead to failure to renew.

Enter email address (used for urgent renewal and security notices)
(Enter 'c' to cancel): [redacted]@gmail.com

-----
Please read the Terms of Service at
https://letsencrypt.org/documents/LE-SA-v1.2-November-15-2017.pdf. You must
agree in order to register with the ACME server. Do you agree?
-----
(Y)es/(N)o: Y

-----
Would you be willing, once your first certificate is successfully issued, to
share your email address with the Electronic Frontier Foundation, a founding
partner of the Let's Encrypt project and the non-profit organization that
develops Certbot? We'd like to send you email about our work encrypting the web,
EFF news, campaigns, and ways to support digital freedom.
-----
(Y)es/(N)o: Y
Account registered.

Which names would you like to activate HTTPS for?
-----
1: weblinus.com.local
2: www.weblinus.com.local
-----
Select the appropriate numbers separated by commas and/or spaces, or leave input
blank to select all options shown (Enter 'c' to cancel): 1
Requesting a certificate for weblinus.com.local
```

Nos pedirá un correo electrónico y los dominios a certificar. Además nos solicitará varias confirmaciones. Le decimos «Y» a todo y ya tendremos el certificado instalado.

Si nos diera algún error en `/var/log/letsencrypt/letsencrypt.log` podremos localizarlo para depurarlo.

El complemento **Nginx** debería funcionar para la mayoría de las configuraciones. Te recomiendo hacer una **copia de seguridad de las configuraciones de Nginx** antes de usarlo (aunque también podemos revertir los cambios en las configuraciones con «`certbot --nginx rollback`»).

O solo obtener un certificado

Si queremos hacer los cambios a nuestra **configuración de nginx** manualmente, tenemos que ejecutar el siguiente comando. Con esta opción **obtendremos un certificado** que tendremos que configurar en el servidor. Para ello tendremos que realizar los pasos de autenticación requeridos para demostrar que somos los propietarios de los dominios. Tenemos que guardar el certificado obtenido en **`/etc/letsencrypt/live/`** y renovarlo periódicamente.

[Configuración de Cookies](#)

[Aceptar](#)



```
1. sudo certbot certonly --nginx
```

Si tenemos varios dominios, podemos especificar «-d» en cada uno de ellos y obtener e instalar diferentes certificados ejecutando Certbot para cada uno de ellos.

```
1. certbot certonly -d ejemplo1.com -d www.ejemplo1.com
2. certbot certonly -d ejemplo2.com -d www.ejemplo2.com
```

El comando para renovar certbot se instala en una de las siguientes ubicaciones:

```
/etc/crontab/
/etc/cron./
systemctl list-timers
```

Confirmar que el certificado funciona

Para confirmar que la configuración es correcta, en un navegador introducimos la URL de nuestro sitio (https://nuestro_sitio_web.com) y comprobamos que en la barra de direcciones aparece un candado.

Para más información sobre cerbot, podemos buscarla en la [pagina de documentación de Cerbot \(https://eff-certbot.readthedocs.io/en/stable/\)](https://eff-certbot.readthedocs.io/en/stable/).

Si tu sitio web corre en un servidor diferente o usas un sistema operativo distinto en la [página oficial del proyecto \(https://certbot.eff.org/instructions\)](https://certbot.eff.org/instructions) podrás encontrar información para cada caso.

¿Tienes algún comentario que hacer sobre este artículo?, al pie del post tienes un formulario para hacerlo.

Si quieres contactar conmigo por cualquier otro asunto relacionado con el sitio, en la [página de contacto \(https://weblinus.com/pagina-de-contacto/\)](https://weblinus.com/pagina-de-contacto/), tienes un formulario más adecuado.

Y para suscribirte y recibir las novedades publicadas, tienes un enlace en el pie de la página o desde aquí mismo.

Suscríbete (<https://weblinus.ipzmarketing.com/f/AHCzGioXQFg>)

Usamos cookies propias y de terceros para mejorar tu experiencia en nuestro sitio. Al continuar navegando entendemos que aceptas ([nuestro política de cookies OJAMIENTOWEB/](#)).

[Configuración de Cookies](#)

[Aceptar](#)



← [Entrada anterior](#)

[Instalación de Nginx y la pila LEMP en Debian 11 «Bullseye» 4](#)
(<https://weblinus.com/instalacion-de-nginx-y-la-pila-lem-p-en-debian-11-bullseye-4/>).

➤ TAMBIÉN PODRÍA GUSTARTE

LAMP

```
javier@ubuntu-server:~$ sudo apt install php libapache2-mod-php php-mysql
[sudo] password for javier:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libapache2-mod-php7.4 php-common php7.4 php7.4-cli php7.4-common php7.4-json php7.4-mysql php7.4-opcache
  php7.4-readline
Suggested packages:
  php-pear
The following NEW packages will be installed:
  libapache2-mod-php libapache2-mod-php7.4 php php-common php-mysql php7.4 php7.4-cli php7.4-common php7.4-json
  php7.4-mysql php7.4-opcache php7.4-readline
0 upgraded, 12 newly installed, 0 to remove and 0 not upgraded.
Need to get 4144 kB of archives.
After this operation, 18.5 MB of additional disk space will be used.
Do you want to continue? [Y/n]
```

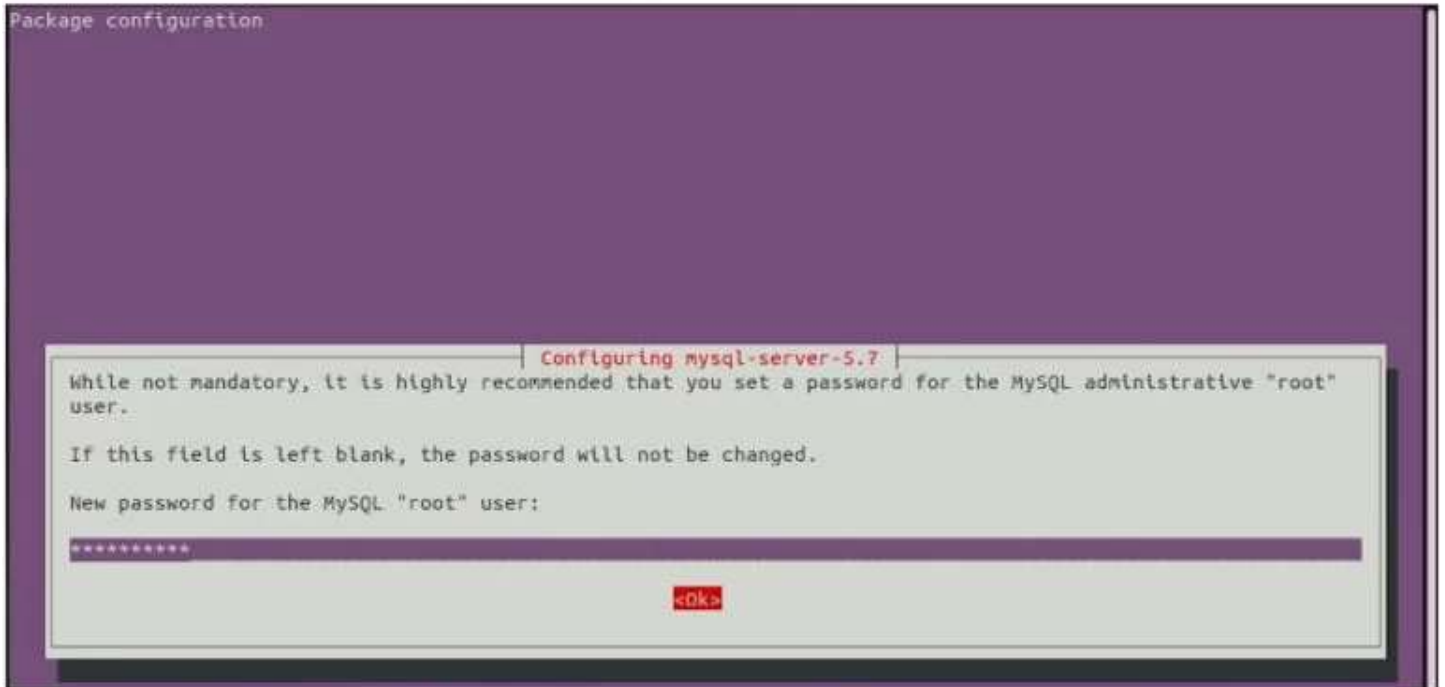
Instalación y configuración de PHP y Hosts Virtuales

(<https://weblinus.com/instalacion-y-de-php/>).

Usamos cookies propias y de terceros para mejorar tu experiencia en nuestro sitio. Al continuar navegando entendemos que aceptas nuestra política de cookies.

(<https://weblinus.com/instalacion-y-de-php/>).

LAMP



Instalación y configuración de MySQL 5.7 en Ubuntu Server

(<https://weblinus.com/instalar-y-configurar-mysql-5-7-en-ubuntu-server-20-04/>)

[Instalar y configurar MySQL 5.7 en Ubuntu Server 20.04 \(https://weblinus.com/instalar-y-configurar-mysql-5-7-en-ubuntu-server-20-04/\)](https://weblinus.com/instalar-y-configurar-mysql-5-7-en-ubuntu-server-20-04/)

🕒 11/03/2021

➤ ESTA ENTRADA TIENE 2 COMENTARIOS



Barto

10/01/2022 [RESPONDER](#)

Gracias Javier. Buen trabajo



Javier Izquierdo (<https://weblinus.com>)

12/01/2022 [RESPONDER](#)

Usamos cookies propias y de terceros para mejorar tu experiencia en nuestro sitio. Al continuar navegando entendemos que aceptas nuestra política de cookies.

Gracias Barto.

[Configuración de Cookies](#)

[Aceptar](#)



Deja una respuesta

Tu comentario aquí...

Nombre (obligatorio)

Correo electrónico (obligatorio)

Web

☐

Guarda mi nombre, correo electrónico y web en este navegador para la próxima vez que comente.

PUBLICAR COMENTARIO

Este sitio usa Akismet para reducir el spam. [Aprende cómo se procesan los datos de tus comentarios \(https://akismet.com/privacy/\)](https://akismet.com/privacy/).

Formulario de suscripción (<https://weblinus.ipzmarketing.com/f/AHCzGioXQFg>)

© COPYRIGHT 2020 · JAVIER IZQUIERDO

[aviso legal \(https://weblinus.com/aviso-legal/\)](https://weblinus.com/aviso-legal/) | [política de privacidad \(https://weblinus.com/politica-de-privacidad/\)](https://weblinus.com/politica-de-privacidad/) | [cookies \(https://weblinus.com/cookies/\)](https://weblinus.com/cookies/)

Usamos cookies propias y de terceros para mejorar tu experiencia en nuestro sitio. Al continuar navegando entendemos que aceptas nuestra política de cookies.

[Configuración de Cookies](#)

Aceptar

