

Practica 6 - WordPress, MySQL, Apache

Prerrequisitos

Antes de comenzar con la instalación, asegúrate de permitir el tráfico para Apache Full en el firewall:

```
ufw allow 'Apache Full'
```

Declaración de los Servidores Virtuales

Crea archivos de configuración para cada sitio web. Asegúrate de copiar correctamente la configuración predeterminada:

```
cat 000-default.conf > sitio1.conf
cat 000-default.conf > sitio2.conf
```

```
# Generar un sitio virtual nuevo para cada web para https
# apuntando al mismo contenido que su version http
# Serán configurados en el punto siguiente
cat default-ssl.conf > sitio1SSL.conf
cat default-ssl.conf > sitio2SSL.conf
```

Luego, modifica los archivos sitio1.conf y sitio2.conf para que reflejen la configuración específica de cada sitio.

```
<VirtualHost *:80>

    ...

    ServerName sitio1.com
    ServerAlias www.sitio1.com
    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/sitio1

    ...

</VirtualHost>

<VirtualHost *:80>

    ...

    ServerName sitio2.com
    ServerAlias www.sitio2.com
    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/sitio2

    ...
```

```
</VirtualHost>
```

Habilitacion del Módulo SSL para HTTPS

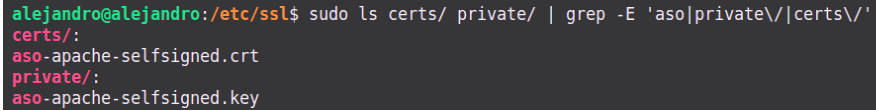
Generar una clave privada y un certificado autofirmado para las conexiones ssl:

```
CRT_DIR=/etc/ssl/cert  
KEY_DIR=/etc/ssl/private
```

```
# Generar clave privada para el certificado autofirmado del servidor
```

```
openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout $CRT_DIR/aso-apache-selfsigned.crt
```

```
a2enmod ssl
```



```
alejandro@alejandro:/etc/ssl$ sudo ls certs/ private/ | grep -E 'aso|private|certs/'  
certs/:  
aso-apache-selfsigned.crt  
private/:  
aso-apache-selfsigned.key
```

Figure 1: alt

Configura los archivos sitio1SSL.conf y sitio2SSL.conf para habilitar SSL. Importatne incluir la ruta correcta a los archivos de certificados.

```
<IfModule mod_ssl.c>  
    <VirtualHost _default_:443>  
  
        ...  
  
        ServerAdmin webmaster@localhost  
        DocumentRoot /var/www/sitio1  
  
        ...  
  
        #    Habilitar SSL para el servidor.  
        SSLEngine on  
  
        ...  
  
        #    Se requiere de certificados y claves ssl para la negociacion de claves o  
        #    Para este caso se usarán certificados autofirmados  
  
        SSLCertificateFile      /etc/ssl/certs/aso-apache-selfsigned.crt  
        SSLCertificateKeyFile    /etc/ssl/private/aso-apache-selfsigned.key  
  
        ...
```

```

        </VirtualHost>
</IfModule>

<IfModule mod_ssl.c>
    <VirtualHost _default_:443>

        ...

        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/sitio2

        ...

        #   Habilitar SSL para el servidor.
        SSLEngine on

        ...

        #   Se requiere de certificados y claves ssl para la negociacion de claves o
        #   Para este caso se usarán certificados autofirmados

        SSLCertificateFile      /etc/ssl/certs/aso-apache-selfsigned.crt
        SSLCertificateKeyFile    /etc/ssl/private/aso-apache-selfsigned.key

        ...

    </VirtualHost>
</IfModule>

```

Por último toca habilitar los módulos y sitios necesarios:

```

sudo a2enmod ssl

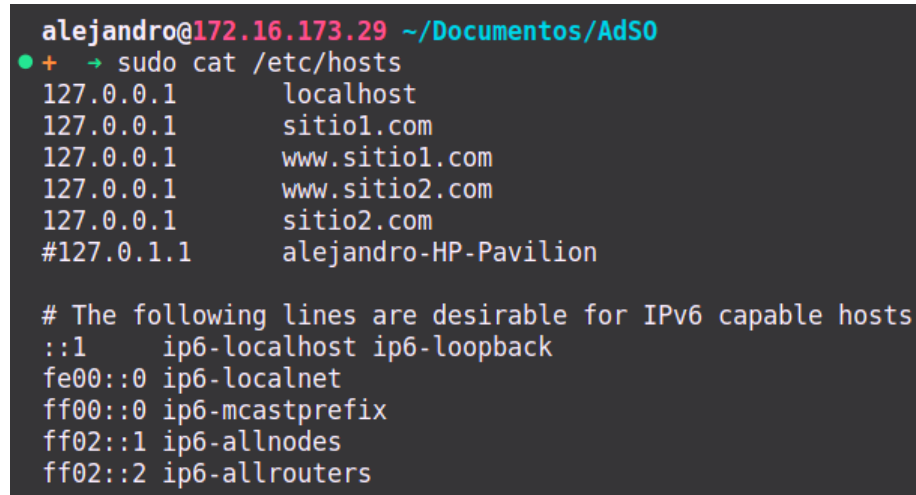
sudo a2ensite sitio1.conf
sudo a2ensite sitio2.conf
sudo a2ensite sitio1SSL.conf
sudo a2ensite sitio2SSL.conf

# Apache avisa de usar reload, pero puede no ser suficiente
# Aunque es más agresivo, siempre que se pueda, puede resultar
# mejor usar restart en su lugar. Para evitar problemas futuros
#
#     sudo systemctl restart apache2.service
#
sudo systemctl reload apache

```

Configurar fichero hosts del anfitrión de la MV

```
# Como sudo
echo -e "
    127.0.0.1    sitio1.com\n
    127.0.0.1    www.sitio1.com\n
    127.0.0.1    sitio2.com\n
    127.0.0.1    www.sitio2.com\n
" >> /etc/hosts
```



```
alejandro@172.16.173.29 ~/Documentos/AdSO
+ → sudo cat /etc/hosts
127.0.0.1    localhost
127.0.0.1    sitio1.com
127.0.0.1    www.sitio1.com
127.0.0.1    www.sitio2.com
127.0.0.1    sitio2.com
#127.0.1.1    alejandro-HP-Pavilion

# The following lines are desirable for IPv6 capable hosts
::1    ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

Instanciar Base de Datos y Crear Usuarios para las Conexiones

Para resolver el nombre de dominio de los sitios hay que añadir las siguientes líneas al archivo /etc/hosts para simular la resolución de nombres de dominio:

```
# Como usuario root de la BD

# Crear un usuario por cada sitio web
CREATE USER 'sitio1'@'localhost'
    IDENTIFIED WITH 'caching_sha2_password'
    BY '@aso_sitio1';

CREATE USER 'sitio2'@'localhost'
    IDENTIFIED WITH 'caching_sha2_password'
    BY '@aso_sitio2';

# Crear la base de datos de cada sitio
CREATE DATABASE sitio1DB;
CREATE DATABASE sitio2DB;
```

```
# Dar privilegios a los usuarios sobre su correspondiente base de datos
# Por comodida se usará ALL PRIVILEGES, aunque no es recomendable
# En su lugar se debería usar:
#
# GRANT connect,
#       select,
#       insert,
#       update,
#       delete,
#       drop,
#       create,
#       alter,
#       index,
#       reference
# ON sitioXDB.* TO 'sitioX'@'localhost';
#
GRANT ALL PRIVILEGES ON sitio1.*
  TO 'sitio1'@'localhost';
GRANT ALL PRIVILEGES ON sitio2.*
  TO 'sitio2'@'localhost';
```

Con todo lo anterior, debería ser posible entrar a la base de datos con las credenciales de cada usuario:

```
mysql -u <sitioX> -p
```

Instalación de WordPress

Contenido de los sitios web

El proceso de instalación de un sitio wordpress es bastante sencillo, basta con descargar la estructura del proyecto wordpress, y descomprimirlo en el directorio raíz de cada servidor web:

```
# Descargar WordPress del Sitio Oficial
wget https://wordpress.org/latest.tar.gz
```

```
# Descomprimir el fichero descargado en el directorio raíz de cada web
```

```
# Eliminando previamente el contenido previo
```

```
sudo rm -rf /var/www/sitio1/index.html && sudo tar -xvf latest.tar.gz -C /var/www/sitio1 --s
sudo rm -rf /var/www/sitio2/index.html && sudo tar -xvf latest.tar.gz -C /var/www/sitio2 --s
```

```
rm -rf latest.tar.gz
```

Es importante renombrar los archivos de configuración de WordPress, para que el proceso de instalación siga su curso normal:

```
# Renombrar el archivo de configuracion por defecto de wordpress
# Para evitar problemas con el instalador de wordpress
sudo mv /var/www/sitio1/wp-config-sample.php /var/www/sitio1/wp-config.php
sudo mv /var/www/sitio1/wp-config-sample.php /var/www/sitio2/wp-config.php
```

Reeditar la configuracion de los sitios virtuales de apache siguiendo el siguiente esquema:

```
<VirtualHost *:80>
    ServerName <sitioX>.com
    ServerAlias www.<sitioX>.com
    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/<sitioX>
        <Directory /var/www/<sitioX>>
            Options FollowSymLinks
            AllowOverride Limit Options FileInfo
            DirectoryIndex index.php
            Require all granted
        </Directory>
        <Directory /var/www/<sitioX>/wp-content>
            Options FollowSymLinks
            Require all granted
        </Directory>
</VirtualHost>
```

Conexión a la Base de Datos de cada Sitio Web

Llegados a este punto toca configurar ciertos parámetros de nuestro sitio word-press, como credenciales de la base de datos, claves de seguridad, etc. Para ello se añaden las siguientes líneas al fichero modificado anteriormente wp-config.php:

```
/** The name of the database for WordPress */
define( 'DB_NAME', 'sitioXDB' );

/** Database username */
define( 'DB_USER', 'sitioX' );

/** Database password */
define( 'DB_PASSWORD', '@aso_sitio1' );

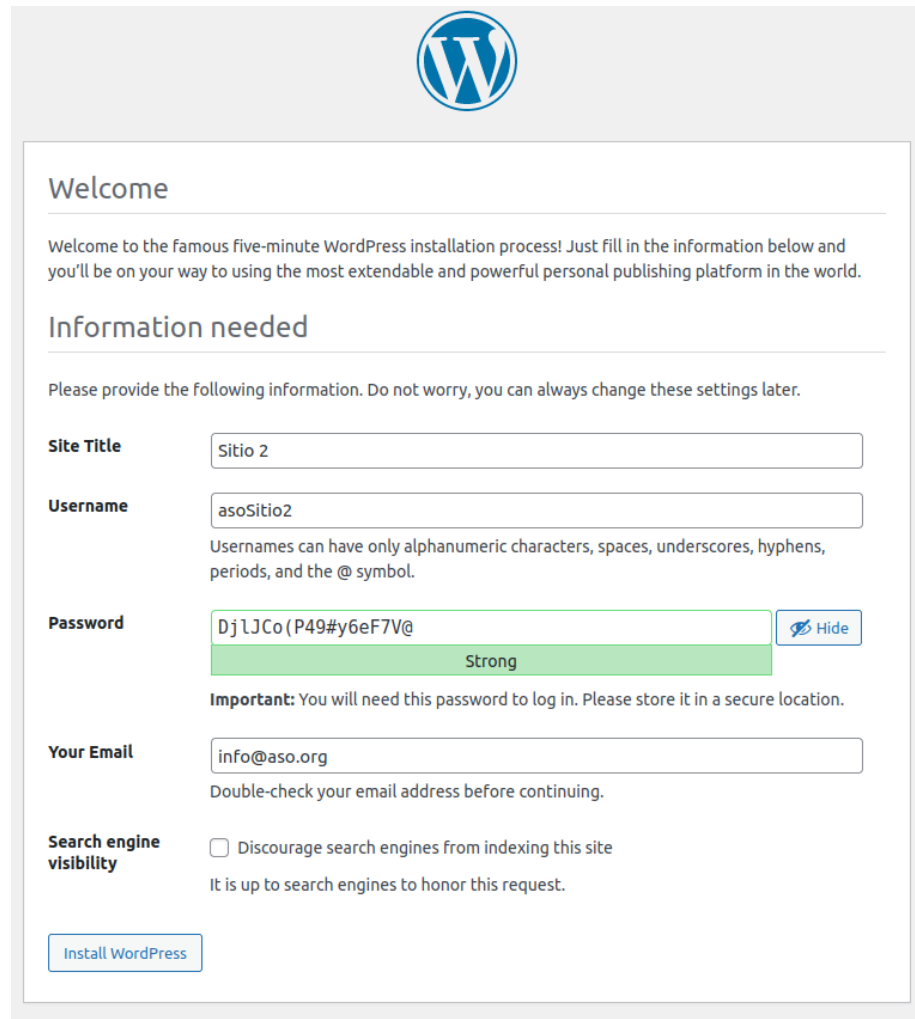
/** Database hostname */
define( 'DB_HOST', 'localhost' );

// ...

define('AUTH_KEY',          '~:9^,jOM01k&D]X3J<3Z:>9I{CX5~30*c|Wrw0ce1-F7uR#<iK`CrnVU:: [zP+1
define('SECURE_AUTH_KEY',   'l0G.-o-6Bw;c~Vi|+SG<IZ_LIU077aHfiKu`us`Wj@Tg-FsU130pR]30$_W$+i
```

```
define('LOGGED_IN_KEY', 'I(c?To)LOQ?8-]@ip(d(5H,g2f?@0}zBJ~iME$EPvCm_{!-`G6aRet9H<61vS.pV
define('NONCE_KEY', 'TQbwiU#-7jj}+*J_=x=0+Z?qS;JH_(en+>^a;) F|UG@Cy{Pu!uU[R $i#`6NII
define('AUTH_SALT', 'EJdvYEzZQ?W|FfiKZ:Q}VkD-In239-F&),|@I&pvz8c~M!3Wj}4&l*q)2])mt8+$
define('SECURE_AUTH_SALT', 'jn)#~4Nm@]55dswVMVo?[fZ&7_ui-!XrL5cr[,ByjG]qG`4eGf>85-_L5[6u}8u
define('LOGGED_IN_SALT', '*eU4|8W,#mhryl-Are&cg!HThwkBpV=/vp#|y04lsstgKF!a3=_|tax4.w@j?0]E
define('NONCE_SALT', 'Kz+*7yU<$adV$`; ( T*D>:GVK)@e`<osW-|b@CChGQgzf-$-L1H#2wZY5o}Q>7&g
```

Instalacion y personalizaci3n de Wordpress



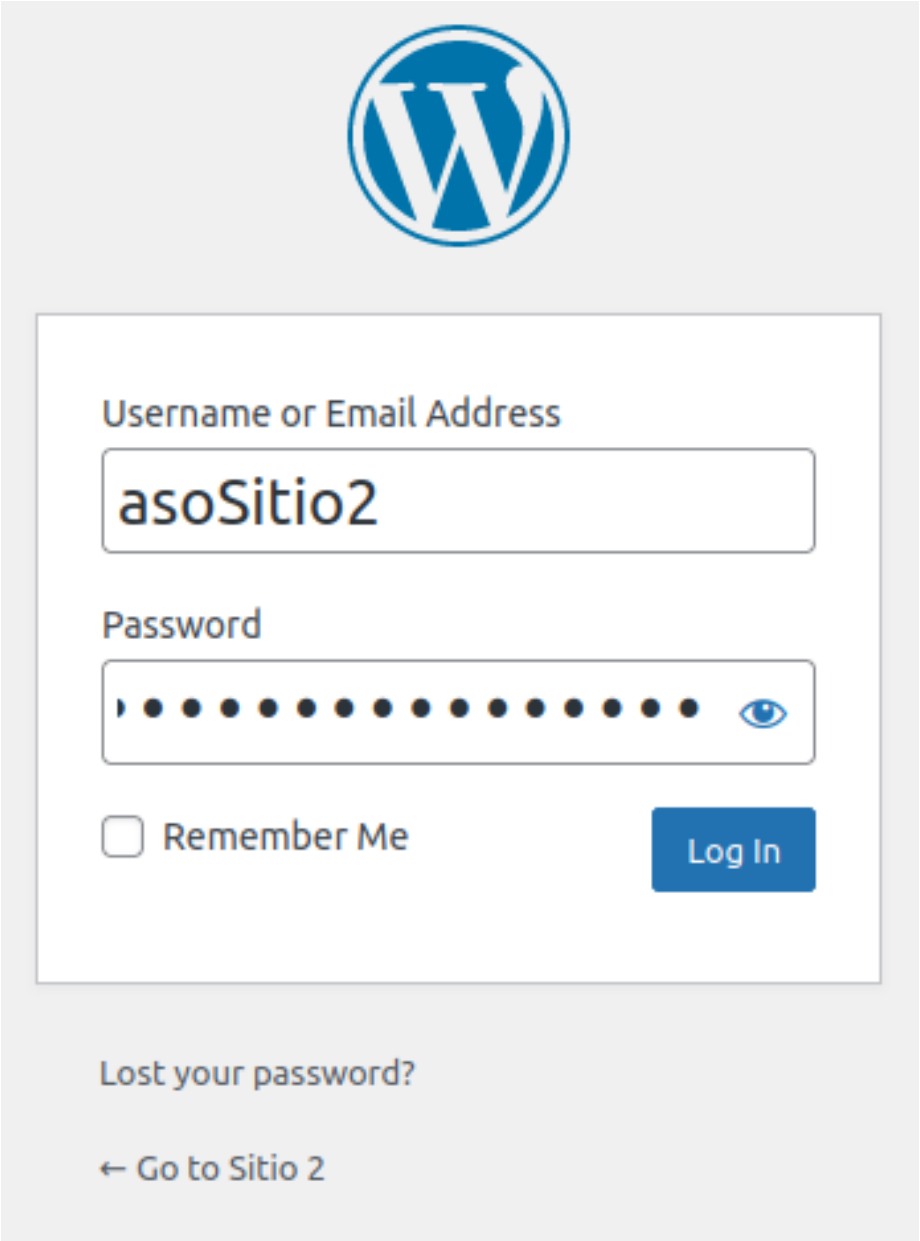
The image shows the WordPress installation 'Welcome' screen. At the top is the WordPress logo. Below it, the heading 'Welcome' is followed by a paragraph: 'Welcome to the famous five-minute WordPress installation process! Just fill in the information below and you'll be on your way to using the most extendable and powerful personal publishing platform in the world.' The section 'Information needed' follows, with a note: 'Please provide the following information. Do not worry, you can always change these settings later.'

The form contains the following fields and options:

- Site Title:** A text input field containing 'Sitio 2'.
- Username:** A text input field containing 'asoSitio2'. Below it, a note states: 'Usernames can have only alphanumeric characters, spaces, underscores, hyphens, periods, and the @ symbol.'
- Password:** A text input field containing 'Dj1JCo(P49#y6eF7V@'. To its right is a 'Hide' button with an eye icon. Below the input field is a green bar indicating the password strength as 'Strong'. Below this, an **Important:** note says: 'You will need this password to log in. Please store it in a secure location.'
- Your Email:** A text input field containing 'info@aso.org'. Below it, a note says: 'Double-check your email address before continuing.'
- Search engine visibility:** A checkbox labeled 'Discourage search engines from indexing this site' is currently unchecked. Below it, a note says: 'It is up to search engines to honor this request.'

At the bottom left of the form is a button labeled 'Install WordPress'.

Figure 2: alt



8

Alternativa de instalación con CLI

```
wp core download [--path=<path>] [--locale=<locale>] [--version=<version>] [--skip-content]
```

Para instalar la herramienta wp:

```
# Descargar WP-CLI
```

```
curl -O https://raw.githubusercontent.com/wp-cli/builds/gh-pages/phar/wp-cli.phar
```

```
# Dar permisos de ejecución a WP-CLI
```

```
chmod +x wp-cli.phar
```

```
# Mover WP-CLI al directorio de comandos
```

```
sudo mv wp-cli.phar /usr/local/bin/wp
```

```
# Verificar la instalación
```

```
wp --version
```

Personalización de WordPress

Para editar y personalizar el contenido de un sitio wordpress, basta con utilizar los plugins y los temas correctos. Los más recomendables y los más usados, son elementor y hello elementor. Estos permiten editar la estructura del contenido web de forma interactiva sin la necesidad de programar ni una sola línea de html, además existen una gran variedad de plantillas predefinidas que podría reducir el trabajo.

La instalación de plugins y temas en wordpress es bastante sencilla, basta con descargar el comprimido con el plugin/tema y descomprimiolo en el directorio correspondiente dentro de wp-content/ (plugins/ o themes/)

```
wget https://downloads.wordpress.org/theme/hello-elementor.2.9.0.zip
```

```
wget https://downloads.wordpress.org/plugin/elementor.3.17.3.zip
```

```
sudo unzip hello-elementor.2.9.0.zip -d /var/www/sitio1/wp-content/themes/
```

```
sudo unzip hello-elementor.2.9.0.zip -d /var/www/sitio2/wp-content/themes/
```

```
sudo unzip elementor.3.17.3.zip -d /var/www/sitio1/wp-content/plugins
```

```
sudo unzip elementor.3.17.3.zip -d /var/www/sitio2/wp-content/plugins
```

Una vez descomprimidos, deben aparecer dentro del panel de administración, en sus respectivos apartados, listos para ser activados, y comenzar su uso:

alt

alt

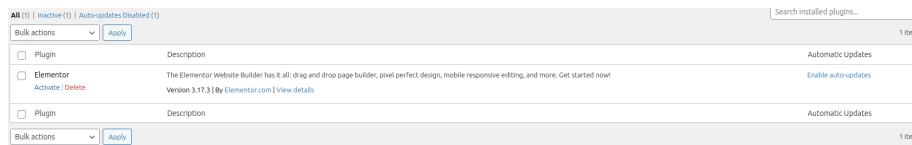



Figure 4: alt

Acceso HTTP y HTTPS a los contenidos

Para atender peticiones http y https de un mismo sitio web, todas aquellas peticiones que lleguen al servicio http del sitio virtual, ha de ser redireccionada al servicio seguro (https), con una respuesta http del tipo 301. Para ello será necesario configurar el nombre del sitio web y su URL, para que sea accesible mediante peticiones https:

- Opción 1: Dentro del panel de control de wordpress

En el panel de administración, en el apartado settings, modificar los campos Site Address y Wordpress Address



Welcome

Welcome to the famous five-minute WordPress installation process! Just fill in the information below and you'll be on your way to using the most extendable and powerful personal publishing platform in the world.

Information needed

Please provide the following information. Do not worry, you can always change these settings later.

Site Title

Username
 Usernames can have only alphanumeric characters, spaces, underscores, hyphens, periods, and the @ symbol.

Password [Hide](#)
 Strong

Important: You will need this password to log in. Please store it in a secure location.

Your Email
 Double-check your email address before continuing.

Search engine visibility ☐ Discourage search engines from indexing this site
 It is up to search engines to honor this request.

[Install WordPress](#)

- Opción 2: Modificando la tabla de configuración de wordpress dentro de MySQL

```
UPDATE wp_options SET option_value = 'http://<sitioX.com>:8889' WHERE option_name = 'siteurl'
```

Ahora solo queda configurar el servicio http dentro del servidor para que redireccione de forma permanente las peticiones que recibe al servicio https. Para ello se ha de añadir un nuevo parámetro en el fichero configuracion del sitio virtual dentro de `/etc/apache/sites-available`:

```
<VirtualHost *:80>
```

```
...
```

```
Redirect permanent / https://<sitioX.com>:8889/
```

```
</VirtualHost>
```

De esta forma cada vez que se lance una petición al servidor http, esta será resuelta con un 301 a la url del servicio seguro. Y de esta forma será accesible el sitio web con peticiones http o https.

Es posible que para que el redireccionamiento funcione, sea necesario activar un módulo de apache:

```
sudo a2enmod rewrite
sudo systemctl restart apache2.service
```

Instalacion de certificados de una CA pública

```
sudo apt update
sudo apt install certbot

sudo certbot certonly --apache -d <sitioX.com>

<IfModule mod_ssl.c>
    <VirtualHost _default_:443>

        ...

        SSLCertificateFile /etc/letsencrypt/live/<sitioX>/fullchain.pem
        SSLCertificateKeyFile /etc/letsencrypt/live/<sitioX>/privkey.pem

        ...

    </VirtualHost>
</IfModule>

sudo certbot certificates
```