

Información sobre PKI

Construir un certificado auto-firmado en WSL

*Los comandos que están entre paréntesis con los pasos, es para hacerlo en Fedora.

1-Instalar el paquete "easy-rsa" que es para crear los certificados:

En Fedora: dnf install easy-rsa

En WSL: sudo apt update

```
sudo apt install easy-rsa
```

```
n in apt-key(8) for details.  
alfanath@Alfa:~$ sudo apt install easy-rsa  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done
```

2-Iniciar PKI (/usr/share/easy-rsa/3.2.2/easyrsa init-pki):

Primero hago una carpeta donde trabajo:

```
mkdir ~/easy-rsa
```

```
cp -r /usr/share/easy-rsa/* ~/easy-rsa/
```

```
cd ~/easy-rsa
```

Inicio PKI: ./easyrsa init-pki

```
Processing triggers for libc-bin (2.35-0ubuntu3.9) ...  
Processing triggers for man-db (2.10.2-1) ...  
alfanath@Alfa:~$ mkdir ~/easy-rsa  
alfanath@Alfa:~$ cp -r /usr/share/easy-rsa/* ~/easy-rsa/  
alfanath@Alfa:~$ cd ~/easy-rsa  
alfanath@Alfa:~/easy-rsa$ ./easyrsa init-pki  
  
init-pki complete; you may now create a CA or requests.  
Your newly created PKI dir is: /home/alfanath/easy-rsa/pki
```

3-Crear la autoridad certificadora [CA] (/usr/share/easy-rsa/3.2.2/easyrsa build-ca [puede usar CI0123 CA para el nombre]):

Si solicita un nombre, poner: CI0123 CA

```
alfanath@Alfa:~/easy-rsa$ ./easyrsa build-ca
Using SSL: openssl OpenSSL 3.0.2 15 Mar 2022 (Library: OpenSSL 3.0.2 15 Mar 2022)

Enter New CA Key Passphrase:
Re-Enter New CA Key Passphrase:
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.
-----
Common Name (eg: your user, host, or server name) [Easy-RSA CA]:CI0123 CA

CA creation complete and you may now import and sign cert requests.
Your new CA certificate file for publishing is at:
/home/alfanath/easy-rsa/pki/ca.crt
```

4-Generar la llave de encriptacion [DH] Diffie-Hellman (/usr/share/easy-rsa/3.2.2/easyrsa gen-dh):

```
./easyrsa gen-dh
```

```

• alfanath@Alfa:~/easy-rsa$ ./easypsa gen-dh
Using SSL: openssl OpenSSL 3.0.2 15 Mar 2022 (Library: OpenSSL 3.0.2 15 Mar 2022)

*** File /home/alfanath/easy-rsa/pki/dh.pem already exists! ***

Type the word 'yes' to continue, or any other input to abort.
  Overwrite? yes
Generating DH parameters, 2048 bit long safe prime
.....

```

5-Generar la llave para el servidor (/usr/share/easy-rsa/3.2.2/easyrsa build-server-full redes) que es el certificado del servidor:

```
./easyrsa build-server-full redes
```

[illegible]

6-Generar la llave para el cliente (/usr/share/easy-rsa/3.2.2/easyrsa build-client-full) que es el certificado del cliente:

```
./easyrsa build-client-full cliente1
```

```
● alfanath@Alfa:~/easy-rsa$ ./easyrpa build-client-full cliente1  
Using SSL: openssl OpenSSL 3.0.2 15 Mar 2022 (Library: OpenSSL 3.0.2 15 Mar 2022)  
. . . + . . . . + . . . . . + . . . . . + . . . . . + . . . . . + . . . . . +  
+ . . . . . + . . . . . + . . . . . + . . . . . + . . . . . + . . . . . *
```

7-Instalar Apache (dnf install httpd):

```
sudo apt install apache2
```

```
● alfanath@Alfa:~/easy-rsa$ sudo apt install apache2
[sudo] password for alfanath:
Reading package lists... Done
Building dependency tree... Done
```

8-Construir un certificado auto-firmado para Apache:

```
sudo cp pki/issued/redes.crt /etc/ssl/certs/
```

```
sudo cp pki/private/redis.key /etc/ssl/private/
```

```
sudo cp pki/dh.pem /etc/ssl/certs/
```

```
Processing triggers for libc-bin (2.35-0ubuntu3.9) ...
alfanath@Alfa:~/easy-rsa$ sudo cp pki/issued/reds.crt /etc/ssl/certs/
alfanath@Alfa:~/easy-rsa$ sudo cp pki/private/reds.key /etc/ssl/private/
alfanath@Alfa:~/easy-rsa$ sudo cp pki/dh.pem /etc/ssl/certs/
```

9-Configurar el Apache:

```
sudo nano /etc/apache2/sites-available/default-ssl.conf
```

En el nano verifico que estas líneas estén y si no las agrego:

SSL Engine on

```
SSLCertificateFile    /etc/ssl/certs/redes.crt
```

```
SSLCertificateKeyFile /etc/ssl/private/redes.key
```

```
SSLOpenSSLConfCmd DHParameters /etc/ssl/certs/dh.pem
```

Luego cierro el nano. Con el cat puedo ver que el nano se guardó bien.

```
● alfanath@Alfa:~/easy-rsa$ sudo nano /etc/apache2/sites-available/default-ssl.conf
⊗ alfanath@Alfa:~/easy-rsa$ cat
^C
● alfanath@Alfa:~/easy-rsa$ cat /etc/apache2/sites-available/default-ssl.conf
<IfModule mod_ssl.c>
    <VirtualHost _default_:443>
        ServerAdmin webmaster@localhost

        DocumentRoot /var/www/html

        # Available loglevels: trace8, ..., trace1, debug, info, notice, wa
```

10-Para habilitar el sitio y el SSL:

```
sudo a2enmod ssl
```

```
sudo a2ensite default-ssl
```

```
sudo systemctl restart apache2
```

```
● alfanath@Alfa:~/easy-rsa$ sudo a2enmod ssl
Considering dependency setenvif for ssl:
Module setenvif already enabled
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Enabling module socache_shmcb.
Enabling module ssl.
See /usr/share/doc/apache2/README.Debian.gz on how to configure SSL and create self-signed certificates.
To activate the new configuration, you need to run:
    systemctl restart apache2
● alfanath@Alfa:~/easy-rsa$ sudo a2ensite default-ssl
Enabling site default-ssl.
To activate the new configuration, you need to run:
    systemctl reload apache2
● alfanath@Alfa:~/easy-rsa$ sudo systemctl restart apache2
🔑 Enter passphrase for SSL/TLS keys for Alfa.:443 (RSA): ****
```

11-Apache usando el certificado ingresando el link en el navegador:

```
https://localhost
```

Not secure https://localhost

MatriculaTEC CorreoUCR MatriculaUCR BecasUCR LogicSim Convalidar-TEC Lol. Esports LeetCode - The Wor... Codewars - Achieve... Co

Apache2 Default Page

Ubuntu

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in `/usr/share/doc/apache2/README.Debian.gz`**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|   |-- ports.conf
|-- mods-enabled
|   |-- *.Load
|   |-- *.conf
|-- conf-enabled
|   |-- *.conf
|-- sites-enabled
|   |-- *.conf
```

- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- `ports.conf` includes included from the main configuration file. It is used to determine the

CV MatriculaTEC CorreoUCR MatriculaUCR

Certificate Viewer: redes

General Details

Issued To

Common Name (CN)	redes
Organization (O)	<Not Part Of Certificate>
Organizational Unit (OU)	<Not Part Of Certificate>

Issued By

Common Name (CN)	C10123 CA
Organization (O)	<Not Part Of Certificate>
Organizational Unit (OU)	<Not Part Of Certificate>

Validity Period

Issued On	Tuesday, April 8, 2025 at 4:58:49 PM
Expires On	Monday, July 12, 2027 at 4:58:49 PM

SHA-256 Fingerprints

Certificate	84ce3c49bca039e4187e924cd1f56d256db16c3fa6bb33a009c41db8e8c93ef2
Public Key	3eef664a80da8c8ff8a65f837f32b7ee7a7809786ac563111cb6f857a7e13a089

after the Ubuntu server installed (ex.html)

ably means contact the

n, and split fully full manual if the

allows:

• `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.