

DESPLIEGUE DE APLICACIONES WEB. EJERCICIOS APACHE(II)

Pablo Cidón
Curso 2017-2018

Sumario

DESPLIEGUE.....	1
Curso 2017-2018.....	1
Configuración del servidor DNS:.....	3
I. Configura el servidor DNS para que resuelva los siguientes nombres: www.empresa1.com, empresa1.com, www.empresa2.com y empresa2.com con la IP del servidor web.....	3
Configuración del servidor WEB.....	5
II. Deshabilita el servidor virtual por defecto. ¿Qué directorio muestra si accedo como http://IP o http://www.empresa1.com o http://empresa1.com o http://www.empresa2.com o http://empresa2.com?.....	5
III. Configura y activa un sitio virtual basado en nombre para el dominio www.empresa1.com (ServerName) o empresa1.com (ServerAlias).....	5
Configuración del servidor FTP.....	8
Configuración del servidor WEB seguro.....	9

Configuración del servidor DNS:

I. Configura el servidor DNS para que resuelva los siguientes nombres: `www.empresa1.com`, `empresa1.com`, `www.empresa2.com` y `empresa2.com` con la IP del servidor web.

Si no funciona el servicio DNS, podemos resolver los nombres utilizando el fichero `hosts` ("C:\WINDOWS\system32\drivers\etc\hosts") añadiendo las IP /nombres en Windows y también, en el fichero `/etc/hosts` en Linux. El cliente (máquina anfitriona) tiene que usar el servidor DNS propio.

En primer lugar, iremos al fichero `/etc/bind/named.conf.local`, en donde crearemos todos los sitios de nuestro DNS:

```
zone "empresa1.com" {
    type master;
    file "/etc/bind/db.empresa1.com";
};
zone "empresa2.com" {
    type master;
    file "/etc/bind/db.empresa2.com";
};
```

A continuación, guardamos los cambios y chequeamos el fichero para comprobar que está todo correcto.

```
root@PCB-ED:/home/miadmin# named-checkconf /etc/bind/named.conf.local
```

Al no producirse ningún error reiniciaremos el servicio, para ello ejecutaremos el siguiente comando:

```
root@PCB-ED:/home/miadmin# service bind9 restart
```

Una vez hecho esto, procederemos a la configuración de los distintos sitios, para ello realizaremos una copia del fichero `/etc/bind/db.0`:

```
root@PCB-ED:/home/miadmin# cp /etc/bind/db.0 /etc/bind/db.empresa1.com
```

Una vez hecho, editaremos el fichero de modo que quede así:

```
;
; BIND reverse data file for empresa1 zone
;
$TTL      604800
@         IN      SOA     PCB-ED.empresa1.com. root.localhost. (
                        1      ; Serial
                        604800 ; Refresh
                        86400  ; Retry
                        2419200 ; Expire
                        604800 ) ; Negative Cache TTL
;
@         IN      NS      PCB-ED.empresa1.com.
@         IN      A       192.168.1.150
PCB-ED    IN      A       192.168.1.150
PC-PC     IN      A       192.168.1.105
www       IN      CNAME    PCB-ED.empresa1.com.
```

Al finalizar chequearemos el fichero para comprobar que está correcto:

```
root@PCB-ED:/home/miadmin# named-checkzone empresa2.com /etc/bind/db.empresa2.com
m
zone empresa2.com/IN: loaded serial 1
OK
```

(*) Para la empresa2, podremos partir de este fichero, cambiando "empresa1" por "empresa2".

Estableceremos una nueva configuración de red, modificando el fichero `/etc/network/interfaces`

```
iface enp0s3 inet static
address 192.168.1.150
gateway 192.168.1.1
netmask 255.255.255.0
dns-nameservers 192.168.1.150
dns-domainins empresa1.com empresa2.com
```

Cambiamos el DNS de nuestro equipo y comprobamos que resuelve los nombres:

```
C:\Users\PC>nslookup
Servidor predeterminado: UnKnown
Address: 192.168.1.150
```

```
> empresa1.com
Servidor: UnKnown
Address: 192.168.1.150
```

```
Nombre: empresa1.com
Address: 192.168.1.150
```

```
> PC-PC.empresa1.com
Servidor: UnKnown
Address: 192.168.1.150
```

```
Nombre: PC-PC.empresa1.com
Address: 192.168.1.105
```

```
> PC-PC.empresa2.com
Servidor: UnKnown
Address: 192.168.1.150
```

```
Nombre: PC-PC.empresa2.com
Address: 192.168.1.105
```

```
> empresa2.com
Servidor: UnKnown
Address: 192.168.1.150
```

```
Nombre: empresa2.com
Address: 192.168.1.150
```

```
> www.empresa2.com
Servidor: UnKnown
Address: 192.168.1.150
```

```
Nombre: PCB-ED.empresa2.com
Address: 192.168.1.150
Alias: www.empresa2.com
```

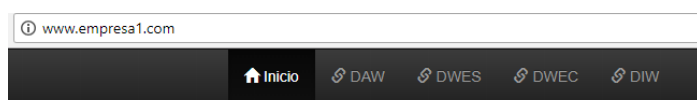
```
> www.empresa1.com
Servidor: UnKnown
Address: 192.168.1.150
```

```
Nombre: PCB-ED.empresa1.com
Address: 192.168.1.150
```



Lenguajes y herramientas utilizadas





Lenguajes y herramientas utiliza



Configuración del servidor WEB

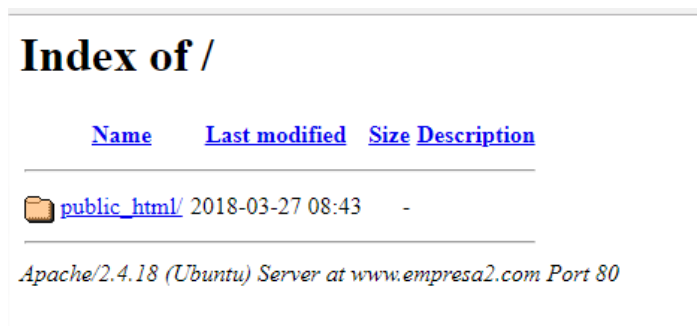
II. Deshabilita el servidor virtual por defecto. ¿Qué directorio muestra si accedo como `http://IP` o `http://www.empresa1.com` o `http://empresa1.com` o `http://www.empresa2.com` o `http://empresa2.com`?

Realizar los cambios que tu consideres para que muestre una página web en blanco, en el caso de que se acceda solo con la IP del servidor.

En primer lugar, desactivaremos el sitio por defecto de apache:

```
miadmin@PCB-ED:~$ sudo a2dissite 000.default.conf
```

Reiniciamos el servicio y comprobamos que nos muestra:



(*) Tanto accediendo por IP, como por cada uno de los nombres, la página nos muestra algo como así, como se ve en la imagen anterior.

III. Configura y activa un sitio virtual basado en nombre para el dominio `www.empresa1.com` (ServerName) o `empresa1.com` (ServerAlias)

- Directorio raíz `/var/www/html/empresa1.com/public_html`

```
miadmin@PCB-ED:~$ sudo mkdir /var/www/html/empresa1.com/
miadmin@PCB-ED:~$ sudo mkdir /var/www/html/empresa1.com/public_html
```

- Se servirá el fichero `index.html` si no se indica ningún fichero en la URL

```
miadmin@PCB-ED:~$ sudo nano /var/www/html/empresa1.com/public_html/index.html
```

- No se mostrará un listado de directorio raíz si no se solicita ningún fichero.
- Podrán acceder todos los usuarios.

- Nos mostrará un sitio web que se ha transferido al servidor mediante el protocolo FTP con el usuario u1.
- En el navegador puedo acceder con los siguientes URL `www.empresa1.com` o `empresa1.com`.
- El log de errores será `/var/log/apache2/empresa1.error.log`
- El log de accesos será `/var/log/apache2/empresa1.access.log`, con formato combined.

En primer lugar copiaremos el fichero `000.default.conf`, para crear nuestro sitio.

```
miadmin@PCB-ED:~$ sudo cp /etc/apache2/sites-available/000-default.conf /etc/apache2/sites-available/empresal.conf
```

Como ya lo teníamos desactivado de antes, ahora solamente tendremos que activar el nuevo sitio:

```
miadmin@PCB-ED:~$ sudo a2ensite empresal.conf
```

Reiniciamos el servicio y procedemos a la configuración del sitio:

```
<VirtualHost *:80>
    # The ServerName directive sets the request scheme, hostname and port that
    # the server uses to identify itself. This is used when creating
    # redirection URLs. In the context of virtual hosts, the ServerName
    # specifies what hostname must appear in the request's Host: header to
    # match this virtual host. For the default virtual host (this file) this
    # value is not decisive as it is used as a last resort host regardless.
    # However, you must set it for any further virtual host explicitly.
    ServerName www.empresal.com
    ServerAlias empresal.com
    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/html/empresal.com/public_html
    <Directory /var/www/html/empresal.com/public_html>
        Options -Indexes
        Require all granted
        AllowOverride All
    </Directory>

    # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
    # error, crit, alert, emerg.
    # It is also possible to configure the loglevel for particular
    # modules, e.g.
    #LogLevel info ssl:warn

    ErrorLog ${APACHE_LOG_DIR}/empresal.error.log
    CustomLog ${APACHE_LOG_DIR}/empresal.access.log combined

    # For most configuration files from conf-available/, which are
    # enabled or disabled at a global level, it is possible to
    # include a line for only one particular virtual host. For example the
    # following line enables the CGI configuration for this host only
    # after it has been globally disabled with "a2disconf".
    #Include conf-available/serve-cgi-bin.conf
</VirtualHost>
```

Reiniciamos el servicio y comprobamos que funciona, para ello tendremos que editar los ficheros de hosts para que reconozca los nombres. Lo haremos tanto en el propio servidor como en el equipo:

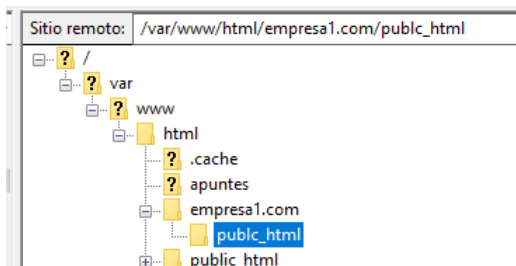
```
192.168.1.150 www.empresal.com
192.168.1.150 empresal.com
192.168.1.150 www.empresa2.com
192.168.1.150 empresa2.com

# ...
192.168.1.150 www.empresal.com
192.168.1.150 empresal.com
192.168.1.150 www.empresa2.com
192.168.1.150 empresa2.com
```

Creamos el usuario y cambiamos el propietario del fichero, que contiene el home del usuario y cambiamos los permisos del fichero para que sean 775:

```
miadmin@PCB-USED:~$ sudo passwd ul
Introduzca la nueva contraseña de UNIX:
Vuelva a escribir la nueva contraseña de UNIX:
passwd: password updated successfully
miadmin@PCB-USED:~$ sudo chown -R ul:www-data /var/www/html/empresa1.com/public_html/
miadmin@PCB-USED:~$ sudo chmod -R 775 /var/www/html/empresa1.com/public_html/
```

Instalamos el servicio de FTP para conectarnos al servidor por FTP y comprobar que funciona:



IV. Configura y activa un sitio virtual para el dominio www.empresa2.com o empresa2.com

- Directorio raíz /var/www/html/empresa2.com/public_html
 - Se servirá el fichero index.html si no se indica ningún fichero en la URL
 - No se mostrará un listado de directorio raíz si no se solicita ningún fichero.
 - Podrán acceder todos los usuarios.
 - En el navegador puedo acceder con los siguientes URL www.empresa 2 .com o empresa2.com.
 - Nos mostrará un sitio web que se ha transferido al servidor mediante el protocolo FTP con el usuario u2.
 - El log de errores será /var/log/apache2/empresa2.error.log
 - El log de accesos será /var/log/apache2/empresa2.access.log, con formato combined.

En primer lugar vamos a copiar el fichero de configuración de la empresa1 para la empresa2:

```
miadmin@PCB-USED:~$ sudo cp /etc/apache2/sites-available/empresa1.conf /etc/apache2/sites-available/empresa2.conf
```

Ahora vamos a crear el directorio que va a contener el home del usuario, y además el que va a ser el del sitio:

```
miadmin@PCB-USED:~$ sudo mkdir /var/www/html/empresa2.com/
miadmin@PCB-USED:~$ sudo mkdir /var/www/html/empresa2.com/public_html
```

Ahora crearemos el usuario:

```
miadmin@PCB-USED:~$ sudo useradd -g www-data -d /var/www/html/empresa2.com/ -s /bin/bash u2
miadmin@PCB-USED:~$ passwd u2
passwd: You may not view or modify password information for u2.
miadmin@PCB-USED:~$ sudo passwd u2
Introduzca la nueva contraseña de UNIX:
Vuelva a escribir la nueva contraseña de UNIX:
passwd: password updated successfully
```

Cambiamos los permisos y propietario del directorio:

```
miadmin@PCB-USED:~$ sudo chown -R u2:www-data /var/www/html/empresa2.com/public_html/
miadmin@PCB-USED:~$ sudo chmod -R 775 /var/www/html/empresa2.com/public_html/
sudo: chmod: orden no encontrada
miadmin@PCB-USED:~$ sudo chmod -R 775 /var/www/html/empresa2.com/public_html/
```

Vamos a realizar la configuración del sitio:

```
<VirtualHost *:80>
# The ServerName directive sets the request scheme, hostname and port that
# the server uses to identify itself. This is used when creating
# redirection URLs. In the context of virtual hosts, the ServerName
# specifies what hostname must appear in the request's Host: header to
# match this virtual host. For the default virtual host (this file) this
# value is not decisive as it is used as a last resort host regardless.
# However, you must set it for any further virtual host explicitly.
ServerName www.empresa2.com
ServerAlias empresa2.com
ServerAdmin webmaster@localhost
DocumentRoot /var/www/html/empresa2.com/public_html
<Directory /var/www/html/empresa2.com/public_html>
    Options -Indexes
    Require all granted
    AllowOverride All
</Directory>

# Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
# error, crit, alert, emerg.
# It is also possible to configure the loglevel for particular
# modules, e.g.
#LogLevel info ssl:warn

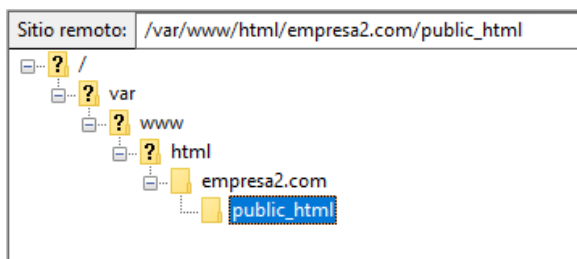
ErrorLog ${APACHE_LOG_DIR}/empresa2.error.log
CustomLog ${APACHE_LOG_DIR}/empresa2.access.log combined

# For most configuration files from conf-available/, which are
# enabled or disabled at a global level, it is possible to
# include a line for only one particular virtual host. For example the
# following line enables the CGI configuration for this host only
# after it has been globally disabled with "a2disconf".
#Include conf-available/serve-cgi-bin.conf
</VirtualHost>
```

Guardamos cambios y activamos el sitio:

```
miadmin@PCB-USED:~$ sudo a2ensite empresa2.conf
Enabling site empresa2.
To activate the new configuration, you need to run:
    service apache2 reload
miadmin@PCB-USED:~$ sudo service apache2 restart
```

Comprobamos que podemos acceder por FTP con el usuario:



Configuración del servidor FTP

V. Configura el servicio FTP de forma que exista un usuario para cada uno de los dominios y puedan subir, bajar, modificar, los archivos del sitio web.

- Los usuarios estarán enjaulados
- Ambos usuarios pertenecen al grupo www-data.
- Controlar los permisos
- Controlar los propietarios.
- Usuarios enjaulados

Usuario	Password	Directorio Personal (home)	Grupo principal	public_html
u1	paso	/var/www/html/empresa1.com	www-data:	Propietario u1 Grupo www-data Permisos 775
u2	paso	/var/www/html/empresa2.com	www-data:	Propietario u2 Grupo www-data Permisos 775

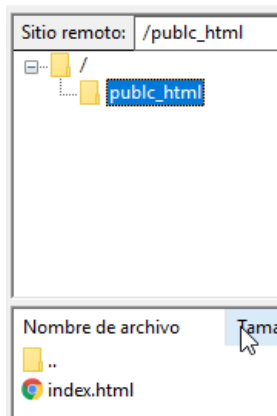
Dado que anteriormente hemos cambiado los permisos y los propietarios de los ficheros, solamente nos queda enjaular los usuarios, para ello iremos al fichero `/etc/proftpd/proftpd.conf`, en donde descomentaremos la siguiente línea:

```
DenyFilter                \ *.* /

# Use this to jail all users in their homes
DefaultRoot               ~

# Users require a valid shell listed in /etc/shells to login.
# Use this directive to release that constrain.
# RequireValidShell       off
```

Una vez hecho, reiniciamos el servicio y comprobamos:



Configuración del servidor WEB seguro

- Activar el módulo SSL

```
miadmin@PCB-USED:~$ sudo a2enmod ssl.load
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 activate the new configuration, you need to run:
service apache2 restart
miadmin@PCB-USED:~$ sudo service apache2 restart
```

- Generar dos certificados autofirmados para `www.empresa1.com` y para `www.empresa2.com`.

Generamos la clave privada:

```
miadmin@PCB-USED:~$ openssl genrsa 2048 > clavePrivada.key
```

```
miadmin@PCB-USED:~$ cat clavePrivada.key
-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEA1kb3Ym18QiMJVnRrN+M8FeeXuzPYloHVQB1/PYptIa+BMXRM
44eDH+cs4W1OdtXv+U7VjRT5e4VU+ijVsONK0m3Xhr8V1OVhg6m96qMRZwh+nGsa
geoOU7Mxt+9ukyZX/TjywCgBVkb0aU2h0VoZA7Mj07BrXLY2RrDbfxLeu+p5OURa
RMUFjPjBEnRpzmRQMUdBWxQGz9f2D6cvxz2dvn7K153LN28Lv40hluGnYhWC2hY
wznQCzn11HDrJj96bnNSvR11clg5BDi7vA/Y0j+Mi9oha2PNASXmvxrX3bj0BZ1J
tRdBA3Sdj+p6wr4/xo7c/wvKMFgCdySnvrScdQIDAQABABAC039eUPecKJl2
L4DIkPF0C09oql4z61xTy2cszcTdmXK5jvk9afXbT0Y05bUJfVnyoxBcrdul9diP
bpA+G5DMH1Pk0VvMHAI7j75Vmvpi7zT+58cnVxS4AhInaQTDy7VWrK5hDuCEgsTP
kTTUd6QIIbScfRk73J7hnjUbKtsVohc07mlxC+L3E9DLDAxtujlq3C2/FI1JzE7V
gF7VxV0yrjSqepZYe0FWQUBBciYrGY3e5Do2xsSWcYLJAfIx8aW3Kg/tDC8qhxPS
Ef8zm2OMDfBSp9UxLbplbX44pT3VnRiPWgJxNr8y4LuiG2+0Z3FPOHYj3QMZHsdv
6cX/OeECgYEA9nKtf/gjjwKNcElF7koUU39SqdUwQo60rQTGJEUH1V2PQBjJ2pdB
PBx/1RLHQA4IUr2B9pNQ/LS6gGWWALPvUA9B5qGhgLz2Kr4XU3IjXnOKWtzSnpDY
7KV72K3A1o1A7o47H7Og4mCqI551snIFOR0ryIw4Ssz7M61jTO3e2kCgYEA3pUU
9rfuMDpBbrlSaATSdlX/XrvE7WCvt4XYJa6I1DU0imkq5P87JS9tyP0kbyXI1bMV
gNMJxEXcXalxVJw+tpinvI6GOMQK2Fu2kBWlmqtFMQ1likK0IIVSILJcJddnMRvF
WsPDO6QeEhgZpE5uUis9qV3YnOHa9/zwlfkWKS0CgYEAqV3QTKTMUyju6OHCEGwK
ogNbFXEclHECLneccCqcdpLwsp0Wg8n1BAmVyG46TpQWNj6UhU9ilfjiPwERYHRI
H94MbSjHkmySdePkkJbejqvN5iQinaDDccAYL2v0E8A87D9guDgzRKfepEY08S2
GDUC9PUgbo4hqnmtntmePThkCgYEAwzVSlNKHmqBGL+UA0A/aKNRft8Gnfl0/pB3
G0xmZM0CjPj98RU1e87xKsmuggUHB5c5j6f+h80JDRSEZeadL/7VC2XVw+wR0Jg
IZFHKBYPb8tAVH/DREZI2f4zTMjWar51Xo4T+omcCdiJ6g8TNrZ31MOgh0iZpyaB
xbYu490CgYEAoueHIF6IoMSCCFAtDQI/gE48jyCljQYsWLBiK5PJXwu8H3QNvTDY
+qj34dwLFnhMUEdAsKCcvON62WC2oX0QMFD2UwqFyueIKvAYL1FBA8/YOsIzAk6H
kf/k3Uf3i48Vx5x9kpHXWtsiiM/SJUwgq9/yDVjDFP7cBQGLY7qz6F4=
-----END RSA PRIVATE KEY-----
```

Seguidamente generamos la solicitud de certificado:

```
miadmin@PCB-USED:~$ openssl req -new -key clavePrivada.key > certificado.csr
```

```
miadmin@PCB-USED:~$ cat certificado.csr
-----BEGIN CERTIFICATE REQUEST-----
MIICmjCCAYICAQAwVTElMAkGA1UEBhMCRCVMAzANBgNVBAGMB1phbW9yYTESMBAG
A1UEBjwVYXZlbnRlMSEwHwYDVQQKBHJbnRlcm5ldCBXaWRnaXRzIFB0eSBM
dGQwgwEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQRDWRvdiBxXCiwlWdGs3
4zwV55e7M9jWgdVAGX89im0hr4ExdEzjh4Mf5yzhbU521e/5TtWNFP17hVT6KNWw
40o6bdcevxXU5WGDqb3qoxFnCH6caxqB6g5TszG3726TJ1f9MnLAKAFWRvRpTaHR
WhkDsyOjsGtcvLZGsNt/Et676nk5RfPExQWM81sSdGnOZFAxR0FZdAbP1/YPpy/H
P22+eHsrXncslnwu/jSHW4adiHALaFjDODALOfWUCOsmP3puc1K9GXVzWDkEOLu8
D9jSP4yL2iFrY80BJea/GtfdUPQFnUmlF0EDdJ2P6nrCvj/Gjtz/C8owWAJ3JKe+
tIJ1AgMBAAGGADANBgkqhkiG9w0BAQsFAAOCAQEACmf+tZQkLpflnVtSFiyulAu4
VDbFYGSWUuCmtvTK8ZWxrSU2djRHOMQ4zHHJ2pfk+HLudSU7DfZy8XBOjF4sqliFQ
QiUM2RsgAqWaeraQruzTzQtEshb97uWQzucPZjPfrspANvltfZLF1Hf2Ihr+Md
YFRtjZLTTXn31eX9WX75wLubOvWiQnKMU59V9R/42yjZMKgH6VhVDZsVEp38ko67
xWgpcRsY4fmbzOvIErpXYnCbdYTSFIiuS/Dla8Ijf2kOufizqGKVZYDqtQ7BDiu4
oJCNGBMbQvTT6KwVMTBqpOalNDcYhC+EIMvb7X+AjdTj8S4hXh/kXnIIVlvvKMA==
-----END CERTIFICATE REQUEST-----
```

Creamos el certificado autofirmado con la clave privada:

```
miadmin@PCB-USED:~$ openssl x509 -req -days 365 -in certificado.csr -signkey cla
vePrivada.key > certificadoFirmado.crt
```

```
miadmin@PCB-USED:~$ cat certificadoFirmado.crt
-----BEGIN CERTIFICATE-----
MIIDJjCCAg4CCQDZQh3B7LdpDTANBgkqhkiG9w0BAQsFADBVMSQwCQYDVQQGEWFJ
UEPMAOGAlUECAWGMfTb3JhMURlEAYDVQQHDALCZWShdmVudGUxITAFBgNVBAoM
GEludGVybWV0IFdpZGdpdHMgUHR5IEExOzDAeFw0xODA1MDkwNjU2MDRaFw0xOTA1
MDkwNjU2MDRmFUXCzAJBgNVBAYTAkVTMQ8wDQYDVQQIDAzaYWlvcmeXEjAQBGNV
BACMCUJlbmF2ZW50ZTEhMB8GA1UECgwvYSW50ZXJuZXQvZ2lkZ210cyBqdHkgTHRk
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEALk3Yml8QiMVJnRrN+M8
FeeXuzPYnlOhVQB1/PYptIa+BMXRM4deDH+cs4W1OdtxUv7JtSE45VU+iJvsONK
Om3Xhr8VLOvhgm6mqMRZwh+nGsageaoOU7MtX+9uky2X/TJywCGVBkb0aU2h0VoZ
A7Mjo7BrXLy2RRDbfxLeu+p5OURaRMUFjPJbEnRpzmQMUDBWXXGz9f2D6cvxz2d
vnh7K153LNZ8L40hlUGnYhwC2hYwznQCznllHDrJj96bnNsVRllclg5BDi7va/Y
Oj+Mi9oha2PNASXmvxrX3bjOBZ1JtRdBAA3Sdj+p6wr4/xo7c/wvKMFxCdySnvrSC
dQIDAQABMAOGCSqSIlbDQEBCCWUAAILBAQR2A2+1osFwk5wOLJYXCqoYorVPA
Pod5NrdoJFCOA8XKCvb+fBJVzu/yhKhu14KAPWU/qVQyVob6+casAXCrgbaHEf4wc/
lEe4MYKMfKnVSvWxjBa1H/8ORP8jFXDMrDNoeEQYjOKufqJApfC8+VlPJJaJIW+Qv2
ln7YskfkEYTWv1lOMIqHtULnENBAkcVuxOJmznKNcUoZFXCYae1vhbsNBD7XCjg
ZFtnukicFdsK077UM5KCMWC2FS32vrfm/18JNEo/Na6MvtSOgK5mqPnaSXLDuZ2e
3YSe0BanolpkdvzyYibYPwlQfbt/uhNTgbg96oNiWQE1+436A4gsv+x+p
-----END CERTIFICATE-----
```

Cambiamos el propietario y los permisos de los ficheros, y los movemos a sus directorios:

```
miadmin@PCB-USED:~$ sudo chown root:ssl-cert clavePrivada.key
miadmin@PCB-USED:~$ sudo chmod 640 clavePrivada.key
miadmin@PCB-USED:~$ sudo chown root:root certificadoFirmado.crt
miadmin@PCB-USED:~$ sudo mv clavePrivada.key /etc/ssl/private/
miadmin@PCB-USED:~$ sudo mv certificadoFirmado.crt /etc/ssl/certs/
```

- Configurar sitios virtuales para los dominios anteriores.

En primer lugar, vamos a copiar el fichero `/etc/apache2/sites-available/default-ssl.conf`:

```
miadmin@PCB-USED:~$ sudo cp /etc/apache2/sites-available/default-ssl.conf /etc/a
pache2/sites-available/empresal-ssl.conf
miadmin@PCB-USED:~$ ls /etc/apache2/sites-available/
000-default.conf      empresal.conf          empresa2.conf
default-ssl.conf      empresal-ssl.conf
```

Realizamos la configuración del fichero:

```

<VirtualHost default :443>
    ServerName www.empresal.com
    ServerAlias empresal.com
    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/html/empresal.com/public_html
    <Directory /var/www/html/empresal.com/public_html>
        Options -Indexes
        Require all granted
        AllowOverride All
    </Directory>
    # Available loglevels: trace8, ...,ttracel, debug, info, notice, warn,
    # error, crit, alert, emerg.
    # It is also possible to configure the loglevel for particular
    # modules, e.g.
    #LogLevel info ssl:warn

    ErrorLog ${APACHE_LOG_DIR}/empresal-ssl.error.log
    CustomLog ${APACHE_LOG_DIR}/empresal-ssl.access.log combined

    # For most configuration files from conf-available/, which are
    # enabled or disabled at a global level, it is possible to
    # include a line for only one particular virtual host. For example the
    # following line enables the CGI configuration for this host only
    # after it has been globally disabled with "a2disconf".
    #Include conf-available/serve-cgi-bin.conf

    # SSL Engine Switch:
    # Enable/Disable SSL for this virtual host.
    SSLEngine on

    # A self-signed (snakeoil) certificate can be created by installing
    # the ssl-cert package. See
    # /usr/share/doc/apache2/README.Debian.gz for more info.
    # If both key and certificate are stored in the same file, only the
    # SSLCertificateFile directive is needed.

    SSLCertificateFile /etc/ssl/certs/certificadoFirmado.crt
    SSLCertificateKeyFile /etc/ssl/private/clavePrivada.key

    # Server Certificate Chain:

```

- Activar los sitios anteriores.

```

miadmin@PCB-USED:~$ sudo a2ensite empresal-ssl.conf
Enabling site empresal-ssl.
To activate the new configuration, you need to run:
    service apache2 reload
miadmin@PCB-USED:~$ sudo a2ensite empresa2-ssl.conf
Enabling site empresa2-ssl.
To activate the new configuration, you need to run:
    service apache2 reload

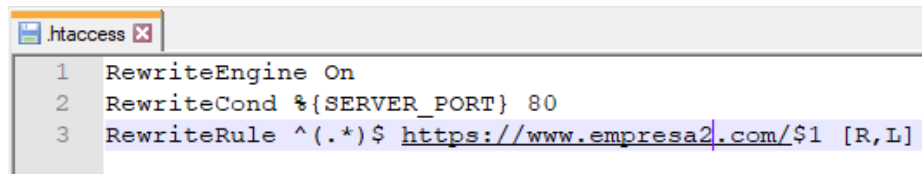
```

- Comprobar el funcionamiento <https://www.empresa1.com> y <https://www.empresa2.com>.



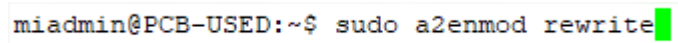
- Redirigir de HTTP a HTTPS

Creemos el fichero .htaccess en el DocumentRoot del sitio:



```
1 RewriteEngine On
2 RewriteCond %{SERVER_PORT} 80
3 RewriteRule ^(.*)$ https://www.empresa2.com/$1 [R,L]
```

En el caso de que el módulo rewrite no esté activo, tendremos que activarlo:



```
miadmin@PCB-USED:~$ sudo a2enmod rewrite
```

Reiniciamos el servicio y comprobamos:

