

DAW Práctica 2.4: Certificados Apache

Para ver qué módulos están habilitados en Apache, utilizamos el siguiente comando en la terminal: `apachectl -M`

```

Min2D2ADesktop [Corriendo] - Oracle VM VirtualBox
Archivo Minima Ver Entrada Desaparece Ayuda

usuario@desaweb:~$

usuario@desaweb:~$ sudo systemctl status apache2
[sudo] contraseña para usuario:
● apache2.service - The Apache HTTP Server
Loaded: loaded (/usr/lib/systemd/system/apache2.service; enabled; preset: enabled)
Active: active (running) since Tue 2024-11-19 16:51:56 CET; 36s ago
Docs: https://httpd.apache.org/docs/2.4/
Process: 1201 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
Main PID: 1228 (apache2)
Tasks: 55 (limit: 11842)
Memory: 8.2M (peak: 8.6M)
CPU: 91ms
CGroup: /system.slice/apache2.service
└─1228 /usr/sbin/apache2 -k start
    1230 /usr/sbin/apache2 -k start
    1231 /usr/sbin/apache2 -k start

nov 19 16:51:56 desaweb systemd[1]: Starting apache2.service - The Apache HTTP Server...
nov 19 16:51:56 desaweb apache2[1201]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using fe80::c2cf:51dd:51b4:b238. Set the 'ServerName' directive globally to suppress this message
nov 19 16:51:56 desaweb systemd[1]: Started apache2.service - The Apache HTTP Server.
usuario@desaweb:~$
AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.0.1. Set the 'ServerName' directive globally to suppress this message
Loaded Modules:
core_module (static)
so_module (static)
watchdog_module (static)
http_module (static)
log_config_module (static)
logio_module (static)
version_module (static)
unixd_module (static)
access_compat_module (shared)
alias_module (shared)
auth_basic_module (shared)
authn_core_module (shared)
authn_file_module (shared)
authz_core_module (shared)
authz_host_module (shared)
authz_user_module (shared)
autolink_module (shared)
deflate_module (shared)
dir_module (shared)
env_module (shared)
filter_module (shared)
mime_module (shared)
mpm_event_module (shared)
negotiation_module (shared)
reqtimeout_module (shared)
setenvif_module (shared)
status_module (shared)
usuario@desaweb:~$

```

Si queremos filtrar específicamente los módulos relacionados con SSL, podemos usar el comando `grep` para obtener una lista más específica:

```
apachectl -M | grep ssl
```

Si el módulo SSL no está activo debemos habilitarlo con el siguiente comando:

```
sudo a2enmod ssl
```

Apache viene con una configuración predeterminada para SSL llamada `default-ssl.conf`. Para habilitar esta configuración, utilizamos: `sudo a2ensite default-ssl.conf`

```

Miniconda3-4.12.0 [Conda]: Oracle VM VirtualBox
Admin - Manage - View - Edit/Save - Disposables - Help
usuario@desaweb:/etc/apache2$ ls
Archivo Editor Ver Buscar Terminal Ayuda

to module (static)
watchdog module (static)
http module (static)
log_config module (static)
logio module (static)
version module (static)
unixd module (static)
access_compat module (shared)
alias module (shared)
auth_basic module (shared)
auth_core module (shared)
authn_file module (shared)
authz_core module (shared)
authz_host module (shared)
authz_user module (shared)
authz_core module (shared)
deflate module (shared)
dir module (shared)
env module (shared)
filter module (shared)
mime module (shared)
mime_event module (shared)
negotiation module (shared)
reqtimeout module (shared)
setenvif module (shared)
status module (shared)
usuario@desaweb:~$ ps aux | grep ssl
orden -ps aux | no encontrado. Quiza quisio decir:
la orden -ps aux | el paquete de openssl (2.4.58-1ubuntu0.4)
Pruebe con: sudo apt install -nombre del paquete deb
usuario@desaweb:~$ ps aux | grep ssl
AM0558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1. Set the 'ServerName' directive globally to suppress this message
usuario@desaweb:~$ sudo systemctl restart apache2
Considering dependency ssl for ssl:
Module ssl 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
usuario@desaweb:~$ sudo systemctl restart apache2
usuario@desaweb:~$ sudo systemctl reload apache2
usuario@desaweb:~$ cd /etc/apache2
usuario@desaweb:/etc/apache2$ sudo mkdir ssl
usuario@desaweb:/etc/apache2$ cd ssl
usuario@desaweb:/etc/apache2/ssl$

```

Después reiniciamos el servidor apache y creamos la carpeta ssl en el directorio /etc/apache2

Generamos la clave privada que será utilizada para crear el certificado SSL.

Utilizamos el comando `sudo openssl genrsa -des3 -out /etc/apache2/ssl/server.key 2048`

```
Miniz2D48U8el [Centos6] - Oracle VM VirtualBox
usuario@desaweb:/etc/apache2/ssl

log config module (static)
logio module (static)
version module (static)
unixd module (static)
access_compat module (shared)
alias module (shared)
auth basic module (shared)
authn_core module (shared)
authn_file module (shared)
authn_core module (shared)
authn_host module (shared)
authn_user module (shared)
autoindex module (shared)
deflate module (shared)
dir module (shared)
env module (shared)
filter module (shared)
mime module (shared)
mm_event module (shared)
negotiation module (shared)
reqtimeout module (shared)
setenvif module (shared)
status module (shared)
usuario@desaweb:~$ pachectl -M | grep ssl
Orden «pachectl» no encontrada. quizá quiso decir:
La orden «pachectl» del paquete deb «apache2 (2.4.58-1ubuntu0.4)»
Pruebe con: sudo apt install «nombre del paquete deb»
usuario@desaweb:~$ pachectl -M | grep ssl
WARNING: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1. Set the 'ServerName' directive globally to suppress this message
usuario@desaweb:~$ sudo a2enmod ssl
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
usuario@desaweb:~$ sudo systemctl restart apache2
usuario@desaweb:~$ sudo a2ensite default-ssl.conf
Enabling site default-ssl.
To activate the new configuration, you need to run:
systemctl reload apache2
usuario@desaweb:~$ sudo systemctl reload apache2
usuario@desaweb:~$ cd /etc/apache2
usuario@desaweb:/etc/apache2$ sudo mkdir ssl
usuario@desaweb:/etc/apache2$ cd ssl
usuario@desaweb:/etc/apache2/ssl$ sudo openssl genrsa -des3 -out server.key 2048
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
usuario@desaweb:/etc/apache2/ssl$
```

- Genrsa: permite generar claves de forma manual o automática
- -des3: es un tipo de cifrado
- -out: Este parámetro indica el nombre del archivo en el que se guardará la solicitud de firma de certificado generada.
- Numbits (2048): indica una longitud de 2048 bits

A continuación, necesitamos generar una solicitud de firma de certificado (CSR).

Usamos el siguiente comando para generar el CSR, que pedirá algunos detalles de la organización: `sudo openssl req -new -key /etc/apache2/ssl/server.key -out /etc/apache2/ssl/server.csr`

```
Miniz2D48U8el [Centos6] - Oracle VM VirtualBox
usuario@desaweb:/etc/apache2/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
usuario@desaweb:~$ sudo systemctl restart apache2
usuario@desaweb:~$ sudo a2ensite default-ssl.conf
Enabling site default-ssl.
To activate the new configuration, you need to run:
systemctl reload apache2
usuario@desaweb:~$ sudo systemctl reload apache2
usuario@desaweb:~$ cd /etc/apache2
usuario@desaweb:/etc/apache2$ sudo mkdir ssl
usuario@desaweb:/etc/apache2$ cd ssl
usuario@desaweb:/etc/apache2/ssl$ sudo openssl genrsa -des3 -out server.key 2048
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
usuario@desaweb:/etc/apache2/ssl$ sudo openssl req -new -key server.key -out server.csr
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.
-----
Country Name (2 letter code) [AU]:es
State or Province Name (full name) [Some-State]:cantabria
Locality Name (eg, City) [Liverpool]:santander
Organization Name (eg, company) [Internet Widgits Pty Ltd]:ies miguel herrero
usuario@desaweb:/etc/apache2/ssl$ sudo openssl req -new -key server.key -out server.csr
Enter PEM pass phrase for server key:
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.
-----
Country Name (2 letter code) [AU]:es
State or Province Name (full name) [Some-State]:cantabria
Locality Name (eg, City) [Liverpool]:santander
Organization Name (eg, company) [Internet Widgits Pty Ltd]:ies miguel herrero
Organization Unit Name (eg, department) []:desaweb
Common Name (e.g. server FQDN or YOUR name) []:desaweb
Email Address []:desaweb@desaweb.com
Please enter the following 'extra' attributes
to be sent with your certificate request
a challenge password []:
an optional company name []:
usuario@desaweb:/etc/apache2/ssl$
```

- Req: Este comando indica que queremos trabajar con el módulo req de OpenSSL, que se utiliza para generar solicitudes de firma de certificado (CSR) o certificados auto-firmados.
- -new: Este parámetro le indica a OpenSSL que queremos generar una nueva solicitud de firma de certificado (CSR).
- -key: Este parámetro especifica el archivo de clave privada que se usará para firmar la solicitud de certificado (CSR).
- -out: Este parámetro indica el nombre del archivo en el que se guardará la solicitud de firma de certificado generada.

Para crear el certificado auto-firmado, utilizamos el siguiente comando. Este comando firma la solicitud de certificado (server.csr) con la clave privada (server.key) y genera un archivo de certificado que será válido por 365 días: `sudo openssl x509 -req -days 365 -in /etc/apache2/ssl/server.csr -signkey /etc/apache2/ssl/server.key -out /etc/apache2/ssl/server.crt`

```

usuario@desaweb:~$ systemctl restart apache2
usuario@desaweb:~$ sudo a2ensite default-ssl.conf
Enabling site default-ssl.
To activate the new configuration, you need to run:
  systemctl reload apache2
usuario@desaweb:~$ sudo systemctl reload apache2
usuario@desaweb:~$ cd /etc/apache2
usuario@desaweb:/etc/apache2$ sudo mkdir ssl
usuario@desaweb:/etc/apache2$ cd ssl
usuario@desaweb:/etc/apache2/ssl$ sudo openssl genrsa -des3 -out server.key 2048
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
usuario@desaweb:/etc/apache2/ssl$ sudo openssl req -new -key server.key -out server.csr
Enter pass phrase for server.key:
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.
-----
Country Name (2 letter code) [AU]:es
State or Province Name (full name) [Some-State]:cantabria
Locality Name (eg, city) []:torrelavega
Organization Name (eg, company) [Internet Widdits Pty Ltd]:ies miguelherrero
usuario@desaweb:/etc/apache2/ssl$ sudo openssl req -new -key server.key -out server.csr
Enter pass phrase for server.key:
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.
-----
Country Name (2 letter code) [AU]:es
State or Province Name (full name) [Some-State]:cantabria
Locality Name (eg, city) []:torrelavega
Organization Name (eg, company) [Internet Widdits Pty Ltd]:ies miguel herrero
Organizational Unit Name (eg, section) []:programacion
Common Name (e.g. Server FQDN or YOUR name) []:Joel
Email Address []:joelmartinezexp@gmail.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:enchegado
No optional company name []:
usuario@desaweb:/etc/apache2/ssl$ sudo openssl x509 -req -days 365 -in server.csr -signkey server.key -out server.crt
Enter pass phrase for server.key:
Certificate request self-signature ok
subject=C = es, ST = cantabria, L = torrelavega, O = ies miguel herrero, OU = programacion, CN = Joel, emailAddress = joelmartinezexp@gmail.com
usuario@desaweb:/etc/apache2/ssl$

```

- X509: indica que queremos trabajar con el formato X.509
- -req: indica que estamos procesando una solicitud de certificado
- -days: define la duración de validez del certificado generado
- -in: especifica el archivo de entrada que contiene la solicitud de firma de certificado (CSR)
- -signkey: especifica el archivo de clave privada que se usará para firmar el certificado
- -out: indica el archivo de salida en el que se guardará el certificado digital firmado

Ahora debemos incluir la ruta de nuestro certificado y clave en la configuración SSL de Apache. Editamos el archivo de configuración de Apache /etc/apache2/sites-available/default-ssl.conf para que apunte a los archivos recién creados (server.crt y server.key):

SSLCertificateFile /etc/apache2/ssl/server.crt

SSLCertificateKeyFile /etc/apache2/ssl/server.key



```
Miniz2D4M3Wd [Conenido] - Oracle VM VirtualBox
usuario@desaweb: /

Archivo Editor Ver Buscar Terminal Ayuda
virtualhost ~443p
ServerAdmin webmaster@localhost

DocumentRoot /var/www/html

# 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}/error.log
CustomLog ${APACHE_LOG_DIR}/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 "modcgi.conf"
#include conf-available/serve-cgi-run.conf

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

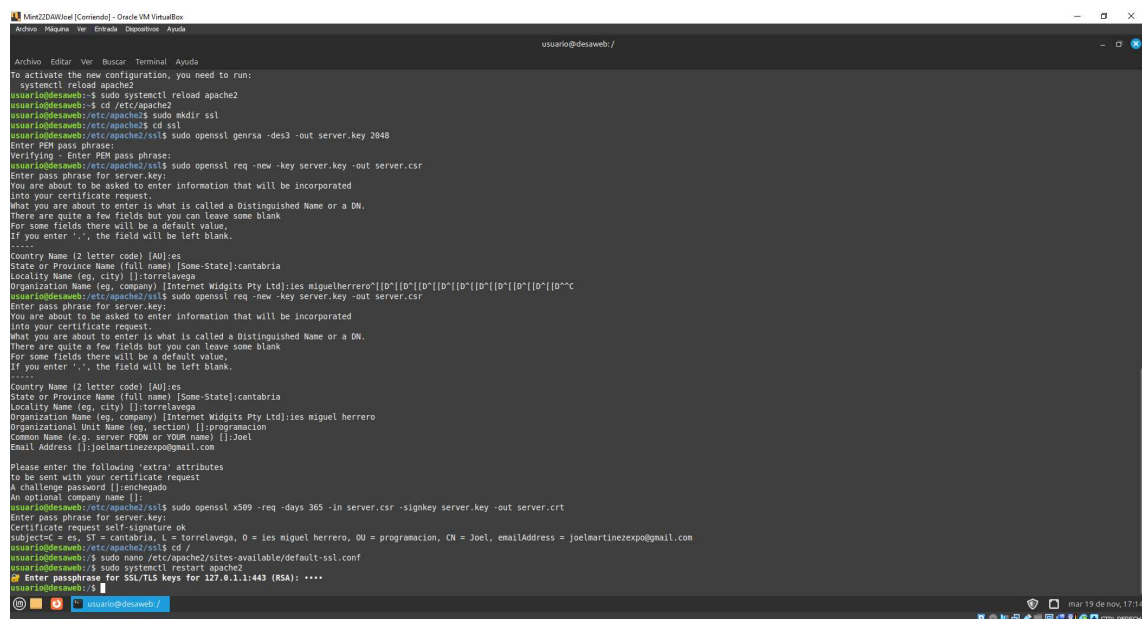
# A self-signed (snakeoil) certificate can be created by installing
# the ssl-cert package. See
# http://httpd.apache.org/docs/2.4/ssl/ssl.en.html for more info.
# If both key and certificate are stored in the same file, only the
# certificate file needs to be pointed to using the "SSLCertificateFile"
# directive.
SSLCertificateFile /etc/apache2/ssl/server.crt
SSLCertificateKeyFile /etc/apache2/ssl/server.key

# Server Certificate Chain:
# Point SSLCertificateChainFile at a file containing the
# concatenation of PEM encoded CA certificates which form the
# certificate chain for the server certificate. Alternatively
# the referenced file can be the same as SSLCertificateFile
# when the CA certificates are directly appended to the server
# certificate for convenience.
#SSLCertificateChainFile /etc/apache2/ssl/crt/server-ca.crt

# Certificate Authority (CA):
# Set the CA certificate verification path where to find CA
# certificates for client authentication or alternatively one
# huge file containing all of them (file must be PEM encoded)
# Note: Inside SSLCertificateChainFile you need both system
# and point to the certificate files, use the provided
# command to generate the certificate files.

Ayuda Guardar Buscar Ejecutar Ubicación 101 líneas leídas Poner marca A llave Anterior Atrás Palabr ant Inicio
Salir Leer fich. Reemplazar Cortar Ir a Línea Rehacer Copiar Buscar atrás Siguiente Palabra Siguien Fin
usuario@desaweb: Certificado para Joe... mar 19 de nov, 17:50
```

Para aplicar los cambios necesitamos reiniciar el servicio de Apache. Al reiniciar el servicio nos pedirá la clave que hemos introducido anteriormente

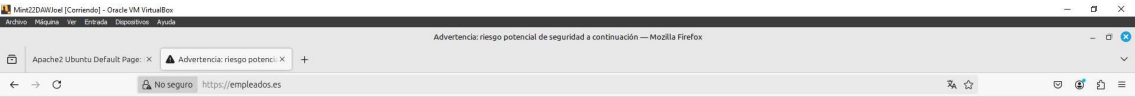


```
Miniz2D4M3Wd [Conenido] - Oracle VM VirtualBox
usuario@desaweb: /

Archivo Editor Ver Buscar Terminal Ayuda
To activate the new configuration, you need to run:
systemctl reload apache2
usuario@desaweb:~$ sudo systemctl reload apache2
usuario@desaweb:~$ cd /etc/apache2
usuario@desaweb:/etc/apache2$ sudo mkdir ssl
usuario@desaweb:/etc/apache2$ cd ssl
usuario@desaweb:/etc/apache2/ssl$ sudo openssl genrsa -des3 -out server.key 2048
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
usuario@desaweb:/etc/apache2/ssl$ sudo openssl req -new -key server.key -out server.csr
Enter pass phrase for server.key:
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.
-----
Country Name (2 letter code) [AU]:es
State or Province Name (full name) [Some-State]:cantabria
Locality Name (eg, city) []:torrelavega
Organization Name (eg, company) [Internet Widgits Pty Ltd]:ies miguelherrero[]
Organization Unit Name (eg, section) []:programacion
Common Name (e.g. server FQDN or YOUR name) []:Joel
Email Address []:joelmartinezexp@gmail.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:enchegado
An optional company name []:
usuario@desaweb:/etc/apache2/ssl$ sudo openssl x509 -req -days 365 -in server.csr -signkey server.key -out server.crt
Enter pass phrase for server.key:
Certificate request self-signature ok
subject=C=es, ST= cantabria, L= torrelavega, O= ies miguel herrero, OU = programacion, CN = Joel, emailAddress = joelmartinezexp@gmail.com
usuario@desaweb:/etc/apache2/ssl$ cd /
usuario@desaweb:~$ sudo nano /etc/apache2/sites-available/default-ssl.conf
usuario@desaweb:~$ sudo systemctl restart apache2
Enter pass phrase for SSL/TLS keys for 127.0.1.1:443 (RSA): ----
usuario@desaweb:~$
```

Cuando intentamos acceder al servidor a través de HTTPS (por ejemplo, https://localhost), el navegador mostrará una advertencia indicando que el certificado no es válido. Esto ocurre porque el certificado es auto-firmado, lo que significa que no ha sido emitido por una autoridad de certificación confiable. Esto es normal para un entorno de prueba o desarrollo.



Advertencia: riesgo potencial de seguridad a continuación

Firefox ha detectado una posible amenaza de seguridad y no ha cargado **empleados.es**. Si visita este sitio, los atacantes podrían intentar robar información como sus contraseñas, correos electrónicos o detalles de su tarjeta de crédito.

[Más información...](#)

[Retroceder \(recomendado\)](#) [Avanzado...](#)



Certificado	
Joel	
Nombre del asunto	
País	es
Estado/Provincia	cantabria
Localidad	torrelavega
Organización	ies miguel herrero
Unidad organizativa	programacion
Nombre común	Joel
Dirección de correo electrónico	joelmartinezexpo@gmail.com
Nombre del emisor	
País	es
Estado/Provincia	cantabria
Localidad	torrelavega
Organización	ies miguel herrero
Unidad organizativa	programacion
Nombre común	Joel
Dirección de correo electrónico	joelmartinezexpo@gmail.com
Validez	
No antes	Tue, 19 Nov 2024 16:08:56 GMT
No después	Wed, 19 Nov 2025 16:08:56 GMT

