

Centro de Enseñanza Técnica Industrial

Desarrollo de Software

Instalación del servidor HTTP + SSL

Jesús Alberto Aréchiga Carrillo 22310439 5N

Profesor

José Francisco Pérez Reyes

Diciembre 2024

Guadalajara, Jalisco

Introducción

La implementación de un servidor HTTP con certificación SSL (Secure Sockets Layer) responde a la necesidad de garantizar la confidencialidad e integridad de la información intercambiada entre clientes y servidores a través de internet. Al integrar un certificado SSL, se establece un canal de comunicación cifrado, impidiendo que terceros no autorizados puedan leer o alterar datos sensibles. Este enfoque es fundamental en el desarrollo de aplicaciones web seguras, ya que refuerza la confianza del usuario y cumple con estándares internacionales de seguridad, evitando vulnerabilidades como la intercepción de datos, el robo de información o la manipulación de contenidos. De esta forma, el servidor HTTP con SSL se consolida como un componente esencial en entornos de producción, asegurando la protección de la comunicación y la integridad del ecosistema digital.

Desarrollo

El objetivo principal de este proyecto es habilitar el certificado SSL en un servidor HTTP para hacer las conexiones seguras. En este caso se utiliza un servidor con una IP 10.0.0.9.

Para comenzar a instalar el certificado se utiliza el comando:

openssl req -x509 -nodes -days 1825 -newkey rsa:2048 -keyout /etc/apache2/ssl/apache.key -out /etc/apache2/ssl/apache.crt

La consola va a mostrar los campos del certificado que hay que ingresar para poder generarlo:

Country Name (2 letter code) [GB]: MX

State or Province Name (full name) [Berkshire]: Jalisco

Locality Name (eg, city) [Newbury]: Guadalajara

Organization Name (eg, company) [My Company Ltd]: Empresa, S.A. de C.V.

Organizational Unit Name (eg, section) []: Departamento de TI

Common Name (eg your name or your server's hostname) []: *.dominio.org

Email Address []: webmaster@dominio.org

Se le dan los permisos al certificado y a la clave privada con

chmod 400 /etc/apache2/ssl/apache.crt /etc/apache2/ssl/apache.key

Ahora se agrega el módulo a Apache:

a2enmod ssl

Ahora se agregan los VirtualHost cambiando el puerto 80 por el puerto 443:

<VirtualHost *:443>

ServerName www.practicahttps.com.mx

ServerAdmin webmaster@localhost

DocumentRoot /home/user

SSLEngine On

SSLCertificateFile /etc/ssl/certs/apache.crt

SSLCertificateKeyFile /etc/ssl/private/apache.key

<Directory /home/user/>

Require all granted

</Directory>

</VirtualHost>

Se reinicia el servicio y se prueba.

Evidencias

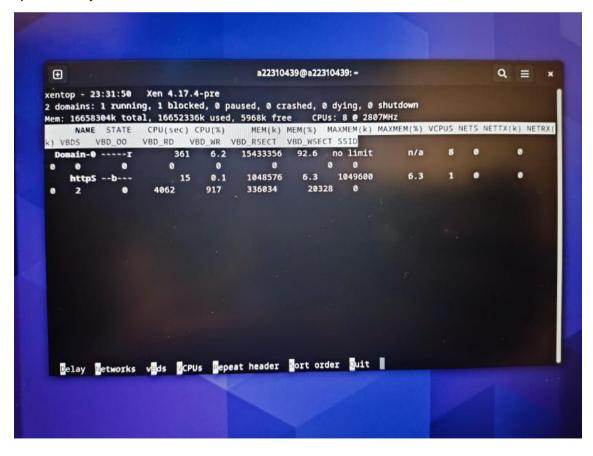
Consola mostrando la dirección IP de la máquina virtual con la que está trabajando en ese momento.

```
Password:
root@a22310439:~# L
root@a22310439:~#
L
root@a22310439@a22310439:~#
L
root@a22310439:~# L
root@a22310439:~#
L
root@a22310439:~# L
root@a22310439:~#
L
root@a22310439:~#
L
root@a22310439:~#
L
root@a22310439:~#
L
root@a22310439:~#
L
root@a22310439:~#
L
root@a22310439:~#
L
root@a22310439:~#
L
root@a22310439:~#
L
root@a22310439:~#
L
root@a22310439:~#
L
root@a22310439:~#
L
root@a22310439:~#
L
root@a22310439:~#
L
root@a22310439:~#
L
root@a22310439:~#
L
root@a22310439:~#
L
root@a22310439:~#
L
root@a22310439:~#
L
root@a22310439:~#
L
root@a22310439:~#
L
root@a22310439:~#
L
root@a22310439:~#
L
root@a22310439:~#
L
root@a22310439:~#
L
root@a22310439:~#
L
root@a22310439:~#
L
root@a22310439:~#
L
root@a22310439:~#
L
root@a22310439:~#
L
root@a22310439:~#
L
root@a22310439:~#
L
root@a22310439:~#
L
root@a22310439:~#
L
root@a22310439:~#
L
root@a22310439:~#
L
root@a22310439:~#
L
root@a22310439:~#
L
root@a22310439:~#
L
root@a22310439:~#
L
root@a22310439:~#
L
root@a22310439:~#
L
root@a22310439:~#
L
root@a22310439:~#
L
root@a22310439:~#
L
root@a22310439:~#
L
root@a22310439:~#
L
root@a22310439:~#
L
root@a22310439:~#
L
root@a22310439:~#
L
root@a22310439:~#
L
root@a22310439:~#
L
root@a22310439:~#
L
root@a22310439:~#
L
root@a22310439:~#
L
root@a22310439:~#
L
root@a22310439:~#
L
root@a22310439:~#
L
root@a22310439:~#
L
root@a22310439:~#
L
root@a22310439:~#
L
root@a22310439:~#
L
root@a22310439:~#
L
root@a22310439:~#
L
root@a22310439:~#
L
root@a22310439:~#
L
root@a22310439:~#
L
root@a22310439:~#
L
root@a22310439:~#
L
root@a22310439:~#
L
root@a22310439:~#
L
root@a22310439:~#
L
root@a22310439:~#
L
root@a22310439:~#
L
root@a22310439:~#
L
root@a22310439:~#
L
root@a22310439:~#
L
root@a22310439:~#
L
root@a22310439:~#
L
root@a22310439:~#
L
root@a22310439:~#
L
root@a
```

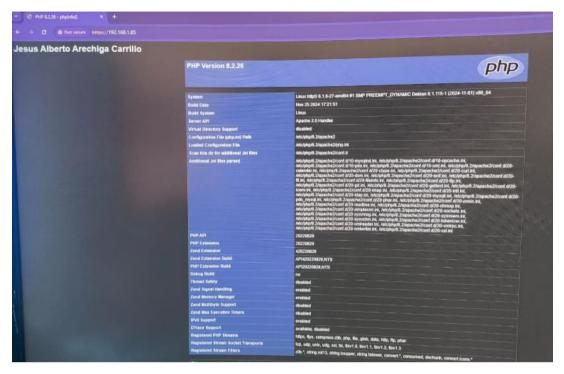
Consola mostrando los procesos que se están ejecutando en la máquina virtual y visualizando correctamente el proceso apache2.

```
1
                                        a22310439@a22310439: -
                                                                                     Q
                                                                                         226 7
                00:00:00 cron
               00:00:00 dbus-daemon
   227 7
   229 7
               00:00:00 systemd-logind
               00:00:00 cryptd
   231 7
   346 tty1
               00:00:00 agetty
   348 hvc0
               00:00:00 login
               00:00:00 sshd
   353 ?
               00:00:01 apache2
   476 ?
               00:00:00 apache2
   477 7
               00:00:00 apache2
   478 ?
               00:00:00 apache2
               00:00:00 apache2
   480 7
               00:00:00 apache2
   481 7
               00:00:00 apache2
               00:00:00 apache2
   482 7
   672 7
              00:00:00 kworker/u2:1-events_unbound
   679 7
               00:00:00 systemd
               00:00:00 kworker/0:0-events
   681 2
   683 ?
                00:00:00 (sd-pam)
   698 hvc0
                00:00:00 bash
                00:00:00 kworker/0:2-cgroup_destroy
   835 7
   836 7
                00:00:00 kworker/u2:0-events_unbound
   843 hvc0
                00:00:00 ps
root@httpS:~#
```

Consola del Dom0 mostrando la información de la ejecución de la máquina virtual que está ejecutando el servidor de HTTPS.



Ventana del navegador donde estas visualizando la página del servidor HTTPS que es la máquina virtual.



Conclusiones

La implementación de un servidor HTTP con un certificado SSL resulta esencial para salvaguardar la integridad y la confidencialidad de la información transmitida en entornos digitales. Al cifrar las comunicaciones, se previenen ataques como la interceptación, manipulación y robo de datos, garantizando así una experiencia más segura para los usuarios. Además, el uso de un certificado SSL impulsa la confianza en el servicio, contribuyendo a la reputación de la organización y al cumplimiento de estándares y normativas internacionales. En definitiva, el despliegue de un servidor HTTP protegido con SSL se ha consolidado como una práctica fundamental en la arquitectura de sistemas web modernos, sentando las bases para una interacción segura, confiable y transparente en el ecosistema digital.