

**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 integración de un servidor WebDAV con un certificado SSL responde a la creciente necesidad de proteger las operaciones de intercambio y gestión de archivos en entornos colaborativos. WebDAV, al ampliar las capacidades del protocolo HTTP para la edición y administración remota de contenidos, se convierte en una herramienta muy útil para el trabajo en equipo y el almacenamiento distribuido. Sin embargo, la información transmitida puede ser vulnerable a ataques de interceptación y manipulación. Al incorporar SSL, se establece un canal de comunicación cifrado que salvaguarda la integridad y confidencialidad de los datos, fortaleciendo así la confianza del usuario en el sistema y cumpliendo con los estándares internacionales de seguridad.

## Desarrollo

El objetivo principal de este proyecto es habilitar el certificado SSL en un servidor WebDAV para hacer las conexiones seguras. En este caso se utiliza un servidor con una IP 10.0.0.10.

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 crea un usuario y una contraseña:

# htpasswd -c /etc/apache2/webdav/.passwd.dav.01 user

Ahora se agregan los VirtualHost en el archivo “/etc/apache2/sites-available/000-default” cambiando el puerto 80 por el puerto 443:

<VirtualHost \*:443>

ServerName www.practicawebdavs.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/>

DAV On

AuthType Basic

AuthName “Webdav”

AuthUserFile /etc/apache2/webdav/.passwd.dav.01

Require valid-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.

A computer screen with white text

Description automatically generated

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

A computer screen with white text

Description automatically generated

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

A computer screen with a black and white text

Description automatically generated

Ventana del cliente WebDAV + SSL para establecer la conexión (antes de establecer conexión) con toda la información y configuración requerida.

A screenshot of a computer

Description automatically generated

Ventana del cliente WebDAV + SSL mostrando la conexión realizada y mostrando las carpetas que tienes en tu servidor WebDAV + SSL.

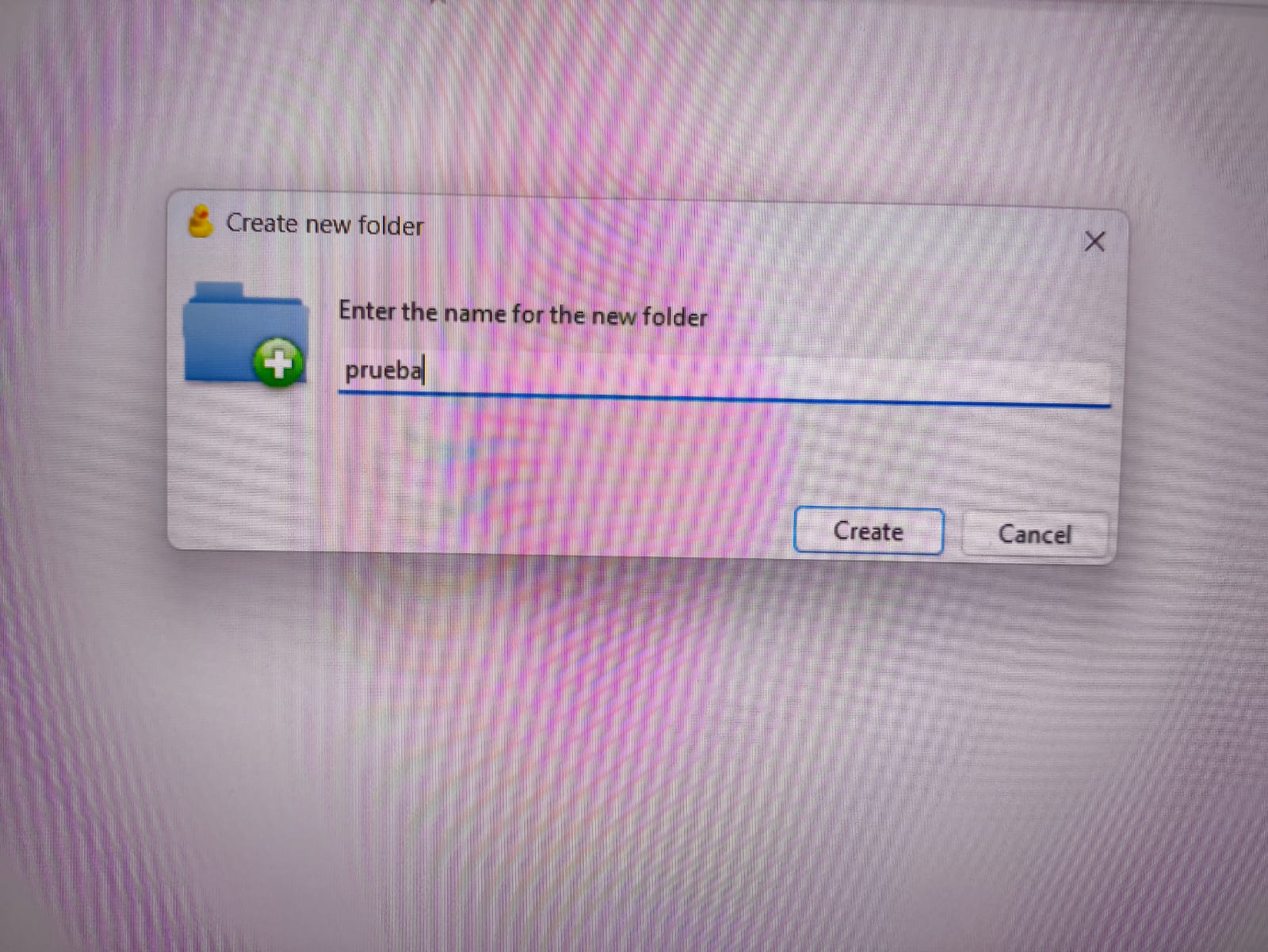
A computer screen shot of a computer

Description automatically generated

A computer screen with a white circle

Description automatically generated

Consola de la máquina virtual mostrando el detalle de la carpeta y archivo (comando: ls -la) que subiste desde el cliente WebDAV + SSL.



A computer screen with a green circle

Description automatically generatedA computer screen with text on it

Description automatically generatedA computer screen with white text

Description automatically generated

## Conclusiones

la implementación de un servidor WebDAV protegido con SSL se consolida como una práctica esencial en la arquitectura moderna de plataformas colaborativas. Gracias a este enfoque, se garantiza un intercambio seguro de información, se evitan vulnerabilidades críticas y se fortalece la reputación del servicio. Adoptar estas medidas no solo satisface las demandas de seguridad y confidencialidad, sino que también contribuye a una experiencia más fiable y eficiente para todos los involucrados en el entorno digital.