



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

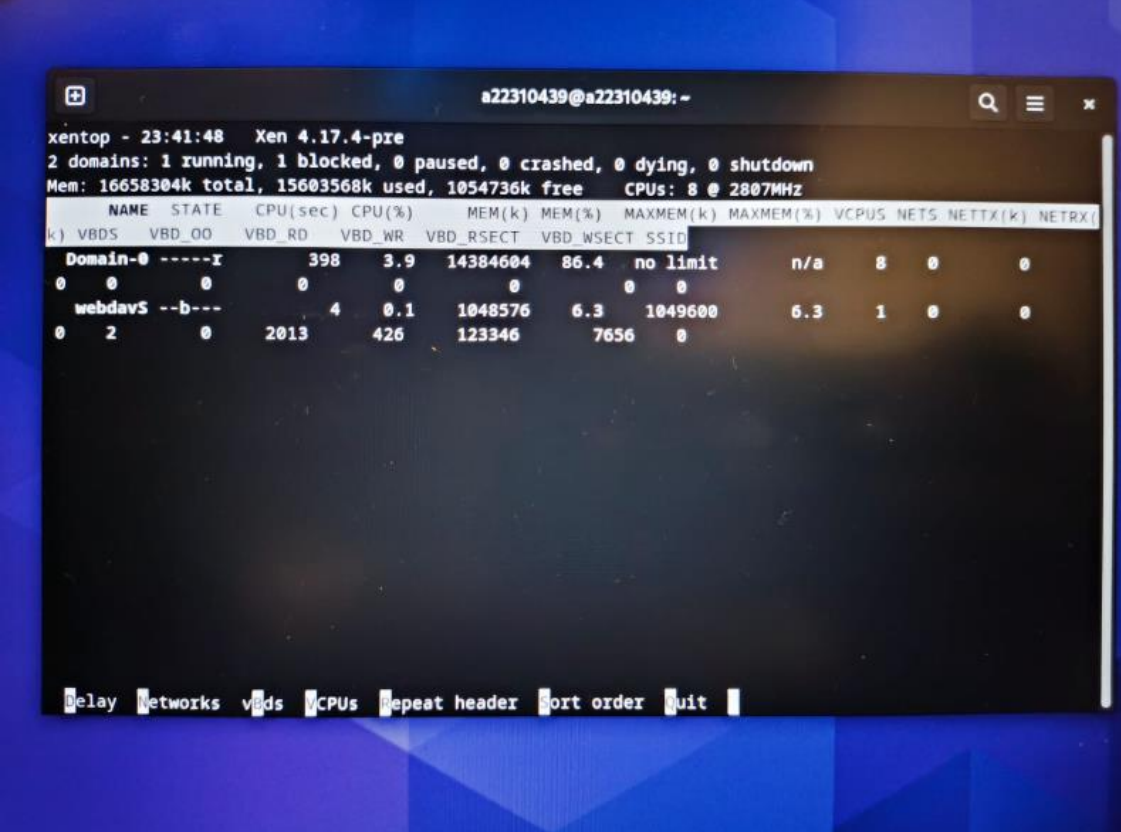
Consola mostrando la dirección IP de la máquina virtual con la que está trabajando en ese momento.

```
a22310439@a22310439: ~  
root@webdav5:~# ip a s  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        valid_lft forever preferred_lft forever  
    inet6 ::1/128 scope host noprefixroute  
        valid_lft forever preferred_lft forever  
2: enx0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000  
    link/ether 00:16:3e:a5:94:b9 brd ff:ff:ff:ff:ff:ff  
    inet 10.0.0.10/24 brd 10.0.0.255 scope global enx0  
        valid_lft forever preferred_lft forever  
    inet6 fe80::216:3eff:fea5:94b9/64 scope link  
        valid_lft forever preferred_lft forever  
root@webdav5:~#
```

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

```
a22310439@a22310439: ~  
56 ?      00:00:00 kstmp  
61 ?      00:00:00 zswap-shrink  
62 ?      00:00:00 kworker/u3:0  
135 ?     00:00:00 jbd2/xvda2-8  
136 ?     00:00:00 ext4-rsv-conver  
173 ?     00:00:00 systemd-journal  
177 ?     00:00:00 kworker/u2:3-writeback  
200 ?     00:00:00 systemd-udevd  
226 ?     00:00:00 cron  
227 ?     00:00:00 dbus-daemon  
229 ?     00:00:00 systemd-logind  
231 ?     00:00:00 cryptd  
334 tty1   00:00:00 agetty  
336 ?     00:00:00 kworker/0:5-events  
337 hvcs0  00:00:00 login  
349 ?     00:00:00 sshd  
351 ?     00:00:00 apache2  
353 ?     00:00:00 apache2  
354 ?     00:00:00 apache2  
414 ?     00:00:00 systemd  
415 ?     00:00:00 (sd-pam)  
421 hvcs0  00:00:00 bash  
429 hvcs0  00:00:00 ps  
root@webdav5:~#
```

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

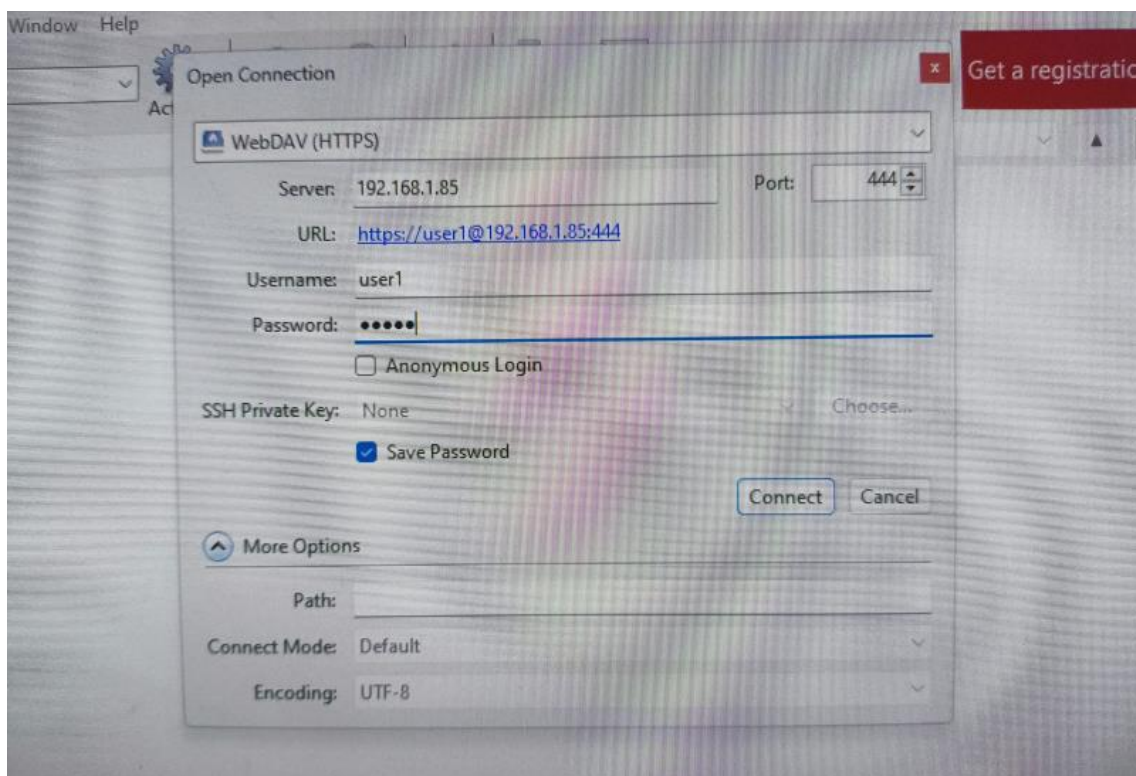


```
xentop - 23:41:48 Xen 4.17.4-pre
2 domains: 1 running, 1 blocked, 0 paused, 0 crashed, 0 dying, 0 shutdown
Mem: 16658304k total, 15603568k used, 1054736k free CPUs: 8 @ 2807MHz
```

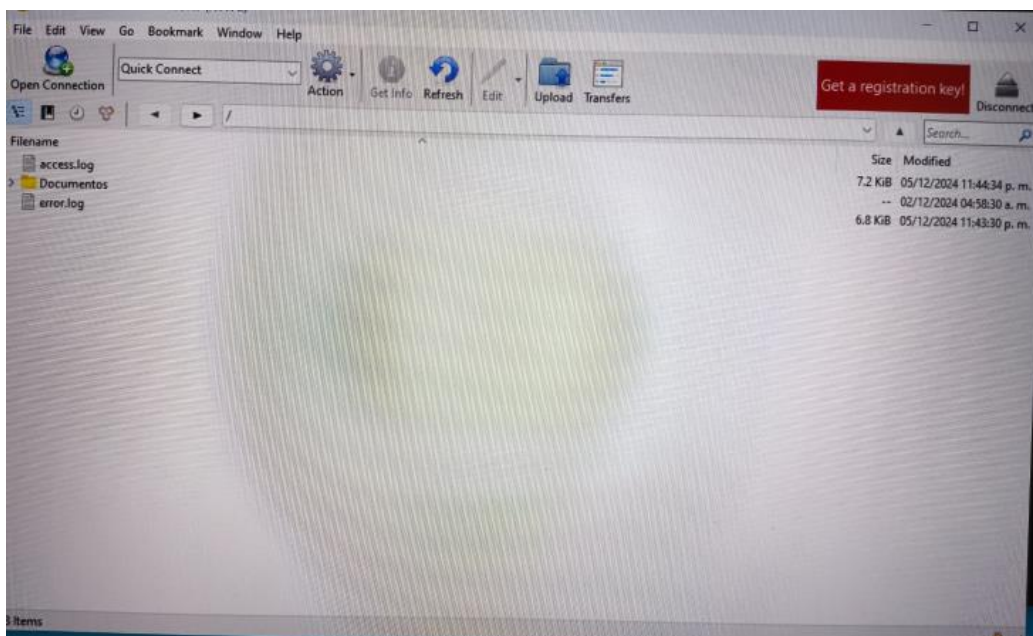
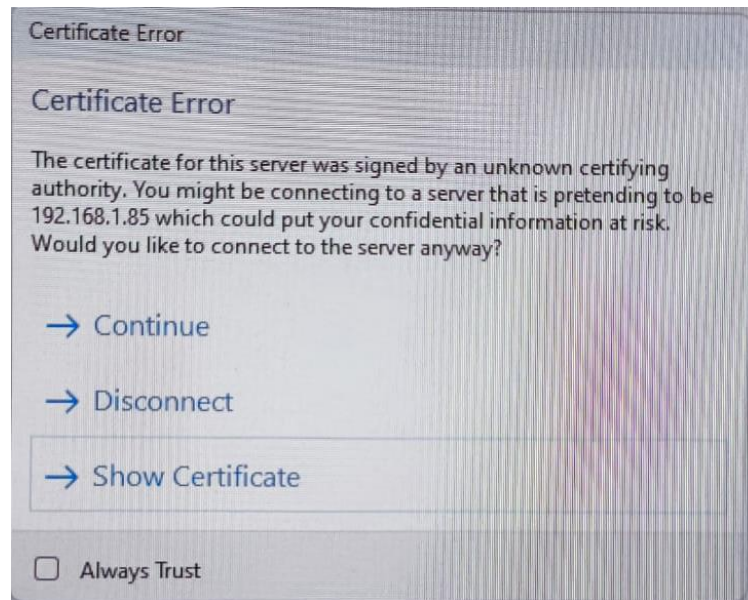
NAME	STATE	CPU(sec)	CPU(%)	MEM(k)	MEM(%)	MAXMEM(k)	MAXMEM(%)	VCPUS	NETS	NETTX(k)	NETRX(k)
Domain-0	-----r	398	3.9	14384604	86.4	no limit	n/a	8	0	0	0
webdavS	--b---	4	0.1	1048576	6.3	1049600	6.3	1	0	0	0

Delay Networks vdis CPUs Repeat header Port order Quit

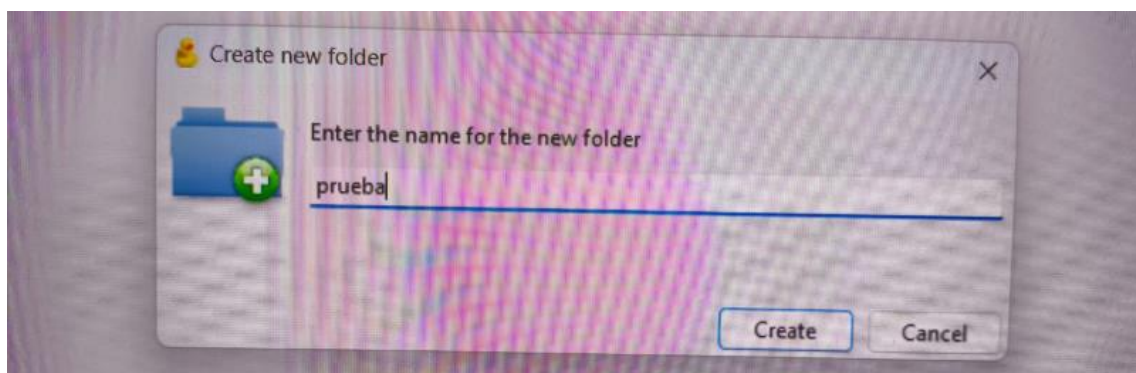
Ventana del cliente WebDAV + SSL para establecer la conexión (antes de establecer conexión) con toda la información y configuración requerida.

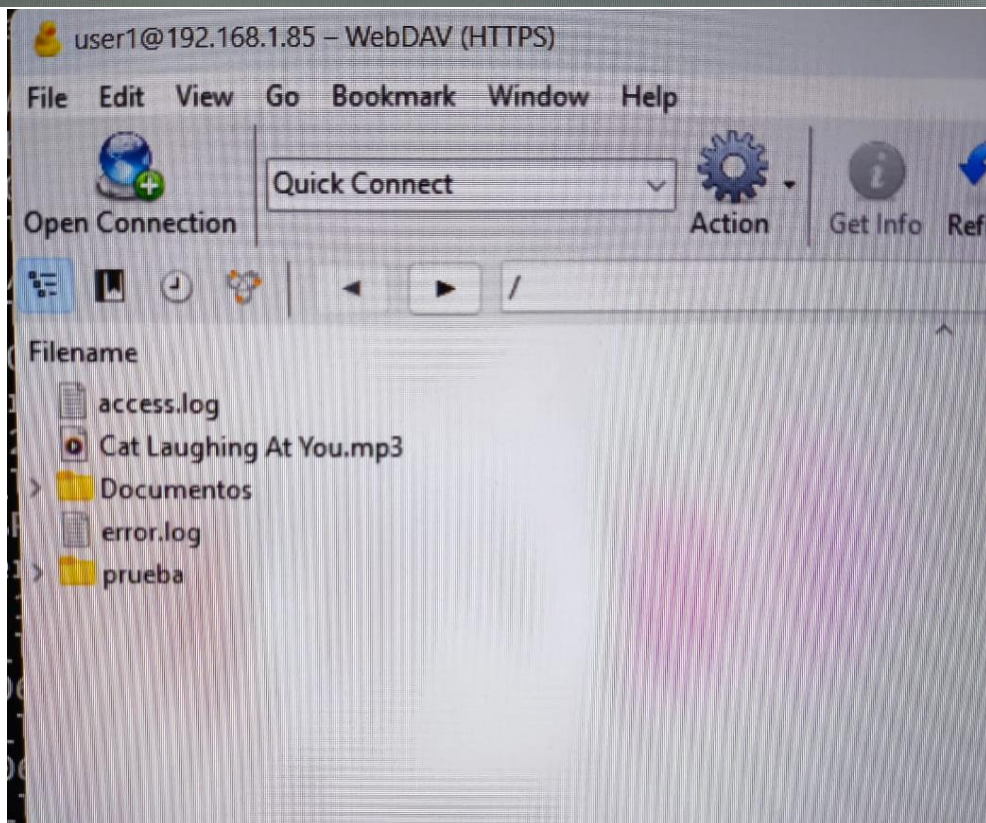
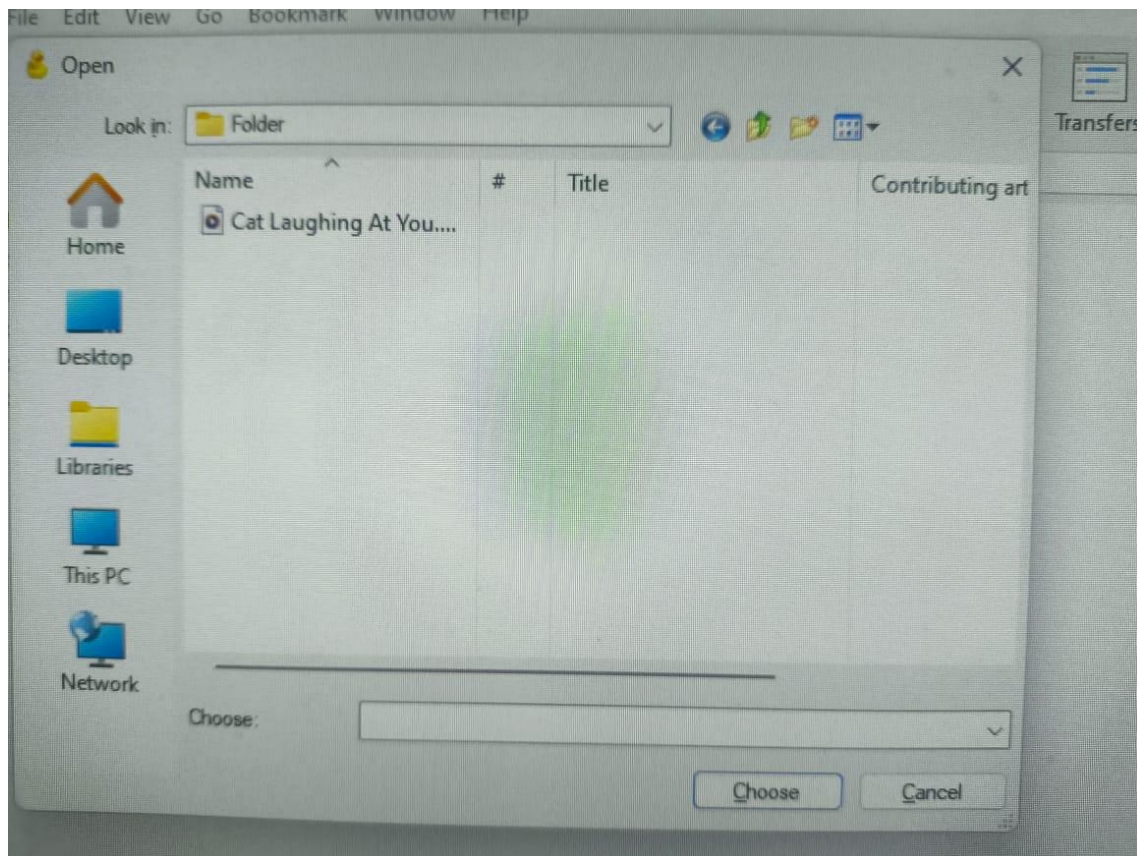


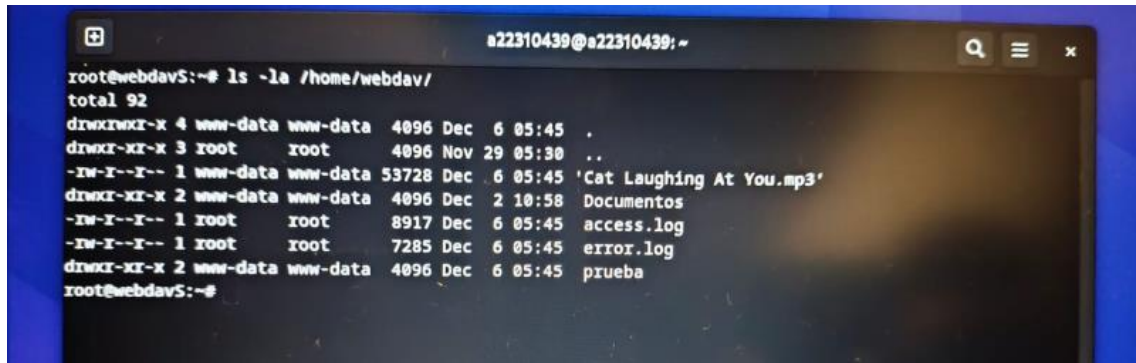
Ventana del cliente WebDAV + SSL mostrando la conexión realizada y mostrando las carpetas que tienes en tu servidor WebDAV + SSL.



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







```
root@webdavS:~# ls -la /home/webdav/
total 92
drwxrwxr-x 4 www-data www-data 4096 Dec  6 05:45 .
drwxr-xr-x 3 root      root    4096 Nov 29 05:30 ..
-rw-r--r-- 1 www-data www-data 53728 Dec  6 05:45 'Cat Laughing At You.mp3'
drwxr-xr-x 2 www-data www-data 4096 Dec  2 10:58 Documentos
-rw-r--r-- 1 root      root    8917 Dec  6 05:45 access.log
-rw-r--r-- 1 root      root    7285 Dec  6 05:45 error.log
drwxr-xr-x 2 www-data www-data 4096 Dec  6 05:45 prueba
root@webdavS:~#
```

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.