Práctica 5.22: WebDav

En la máquina **ServidorLinuxXX** crea el directorio **/var/www/webdav** y configura el servidor virtual por defecto para que el directorio sea accesible desde clientes WebDav. Deberás configurar la autenticación HTTP *Digest* sobre el directorio **/var/www/webdav** para que solo puedan acceder los usuarios **admin1** y **admin2**. También tendrás que configurar los permisos adecuados para que los clientes puedan consultar, borrar, modificar, etc. ficheros del directorio.

1. **Habilitar los módulos necesarios para WebDav**

   1.1. Inicia una sesión en **ServidorLinuxXX** con un usuario con privilegios de administrador.

   1.2. Consulta el directorio **/etc/apache2/mods-available** y observa que entre los módulos disponibles para cargar están **dav** y **dav_fs**.

   1.3. Habilita los módulos ejecutando los siguientes comandos:

   ```
   sudo a2enmod dav
   sudo a2enmod dav_fs
   ```

   1.4. Verifica que dentro del directorio **/etc/apache2/mods-enabled** se han creado enlaces simbólicos de los módulos *dav* y **dav_fs** (ficheros **.conf** y **.load**) hacia **/etc/apache2/mod_availables**

   1.5. Consulta el fichero **/etc/apache2/mod_availables/dav_fs.conf** y observa su configuración por defecto, Figura 1.

   ```
   DAVLockDB ${APACHE_LOCK_DIR}/DAVLock
   ```

   Figura 1: Ficgero **/etc/apache2/mod-availables/dav_fs.conf**

   La directiva **DAVLockDB** define la ubicación de la base de datos que almacenará la información para controlar los bloqueos (control del acceso simultaneo a los mismos ficheros por parte de múltiples clientes).

   1.6. Reinicia el servidor para que los cambios tengan efecto.

2. **Configuración del directorio**

   2.1. Crea el directorio **/var/www/webdav** y dentro el fichero **prueba.html**.

   2.2. Edita el fichero **/etc/apache/sites-available/default** y añade las siguientes directivas, Figura2.

```
<Directory /var/www/departamento>
        Options Indexes FollowSymLinks MultiViews
        AllowOverride None
        Order allow,deny
        allow from all
        AuthType Digest
        AuthName "informatica"
        AuthDigestProvider file
        AuthUserFile "/etc/apache2/digest"
        Require user admin1 admin2
</Directory>

<Directory /var/www/webdav>
        Dav On
        Options Indexes FollowSymLinks MultiViews
        AllowOverride None
        Order allow,deny
        allow from all
        AuthType Digest
        AuthName "informatica"
        AuthDigestProvider file
        AuthUserFile "/etc/apache2/digest"
        Require user admin1 admin2
</Directory>
```

Figura 2: Fichero **/etc/apache/sites-available/default**

Como puedes observar se ha utilizado el fichero **/etc/apache2/digest** de usuarios y contraseñas creado en prácticas anteriores. Si no has realizado la práctica correspondiente deberías crearlo según se explica a continuación.

a Crea el fichero y añade el usuario **admin1** al dominio `informatica` (la opción -c es para crear el fichero).

```
sudo htdigest -c /etc/apache2/digest informatica admin1
```

b Añade el usuario **admin2** (no se usa la opción -c porque el fichero ya existe).

```
sudo htdigest /etc/apache2/digest informatica admin2
```

2.3. Reinicia el servidor para que los cambios tengan efecto.

3. **Conexión desde un cliente WebDav**

Para conectarse a través de WebDav es necesario utilizar un cliente específico. **Windows7** tiene integrado un cliente WebDav en sus explorador de archivos (tiene algunos problemas con conexiones sobre HTTPS).

3.1. En **DesarrolloW7XX** accede a **Inicio, Equipo**.

3.2. En la barra de direcciones introduce

3.3. Pincha en **Nueva Conexión** e introduce los siguientes parámetros para establecer una conexión, Figura3.

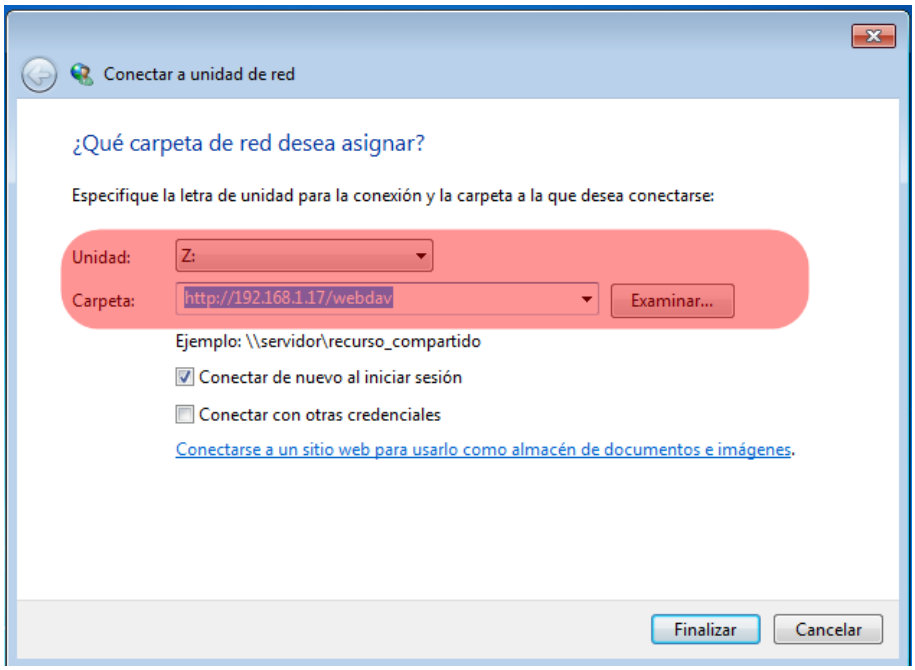

Figura 3: Configuración de la conexión WebDav desde **DesarrolloW7XX**

3.4. Pincha en **Conectar** y establece una conexión como **admin1**, Figuras 4 y 5.

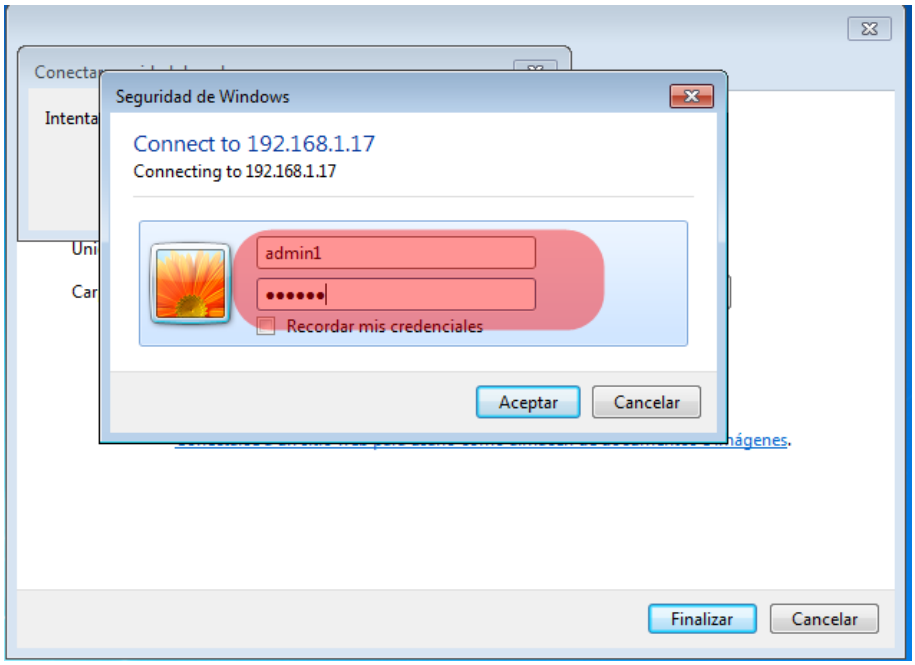

Figura 4: Conexión como *admin1*

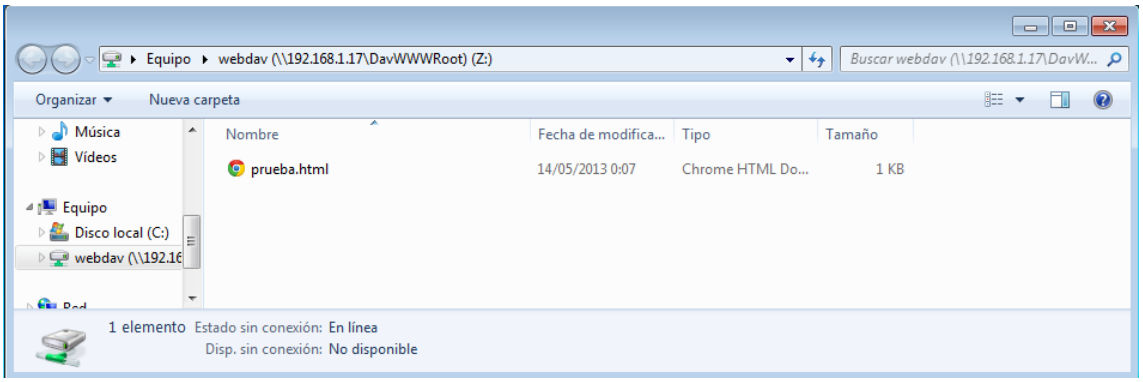

Figura 5: Conexión como **admin1**

3.5. Intenta crear un nuevo archivo. Observa que no tienes permisos.

4. **Configuración de los permisos adecuados**

4.1. En **ServidorLinuxXX** consulta el fichero **/etc/apache2/envars**. Observa el usuario y el grupo con los que se ejecuta *Apache*, Figura 6.

```
# envvars - default environment variables for apache2ctl

# this won't be correct after changing uid
unset HOME

# for supporting multiple apache2 instances
if [ "${APACHE_CONFDIR##/etc/apache2-}" != "${APACHE_CONFDIR}" ] ; then
        SUFFIX="-${APACHE_CONFDIR##/etc/apache2-}"
else
        SUFFIX=
fi

# Since there is no sane way to get the parsed apache2 config in scripts, some
# settings are defined via environment variables and then used in apache2ctl,
# /etc/init.d/apache2, /etc/logrotate.d/apache2, etc.
export APACHE_RUN_USER=www-data
export APACHE_RUN_GROUP=www-data
export APACHE_PID_FILE=/var/run/apache2$SUFFIX.pid
export APACHE_RUN_DIR=/var/run/apache2$SUFFIX
export APACHE_LOCK_DIR=/var/lock/apache2$SUFFIX
# Only /var/log/apache2 is handled by /etc/logrotate.d/apache2.
export APACHE_LOG_DIR=/var/log/apache2$SUFFIX
```

Figura 6: Fichero **/etc/apache2/envars**

4.2. Accede al directorio **/var/www**.

4.3. Consulta los permisos del directorio **/var/www/webdav**.

4.4. Cambia el grupo de **/var/www/webdav** a **www-data** y otorgarle privilegios de escritura.

```
sudo chown root_www-data /var/www/webdav
sudo chmod 775 /var/www/webdav
```

4.5. Desde **DesarrolloW7XX** observa que ahora es posible crear un nuevo archivo, Figura 7.

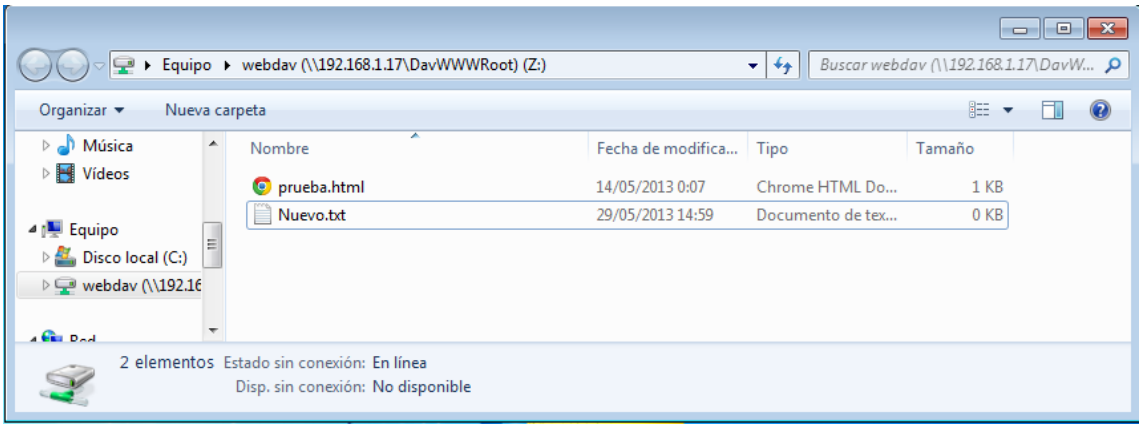

Figura 7: Nuevo archivo

4.6. Prueba a copiar, borrar, renombrar, etc.

◇