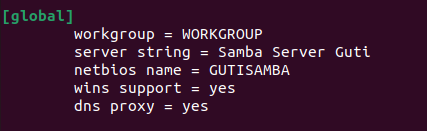
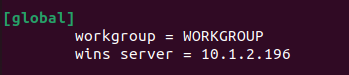
**Unidad Didáctica 6. Compartición de recursos en red mediante el protocolo CIFS/SAMBA**

**Ejercicio 1. Investiga cómo configurar SAMBA como servidor WINS. La solución deberá incluir la configuración del servidor y del cliente. Además, tendrá que mostrar el fichero, asociado a SAMBA-WINS, donde se incluyen los nombres NetBIOS.**

Como ya tenemos SAMBA instalado solo tenemos que asegurarnos de que las siguientes opciones están configuradas correctamente en la sección [global]



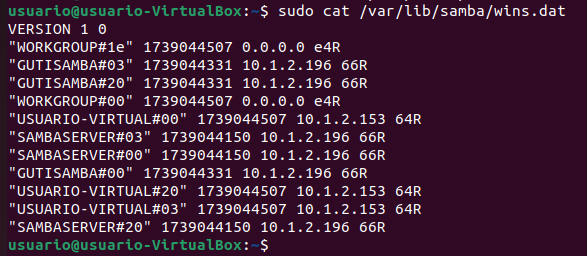
A continuación, en la máquina Cliente aplicaremos la dirección ip del servidor Wins, en este caso 10.1.2.196



Una vez guardemos la configuración y reiniciamos el servicio podemos comprobar que el cliente está usando correctamente el servidor WINS, puedes hacer un ping a un nombre NetBIOS registrado en el servidor SAMBA, usando el siguiente comando

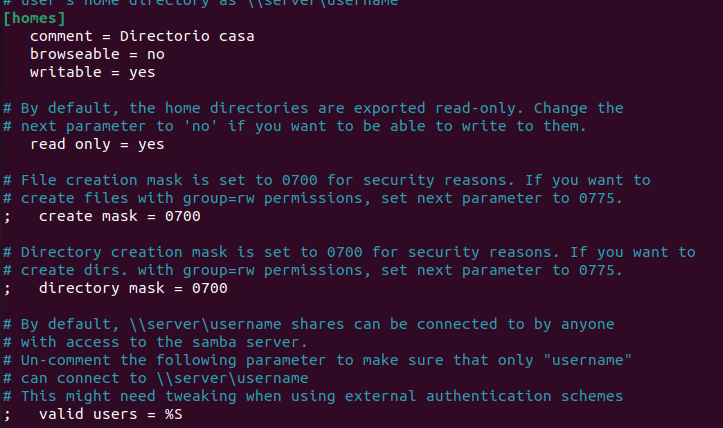


El archivo donde se encuentra el fichero asociado a SAMBA-WINS lo podemos encontrar en la siguiente ruta:  **/var/lib/samba/wins.dat**



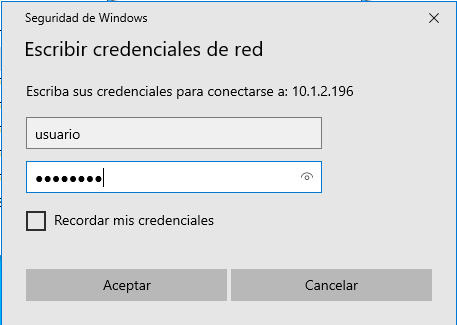
**Ejercicio 2. Busca información relacionada con la compartición, vía SAMBA, de los directorios de casa. Explica cómo realizar la configuración y comprueba que se han compartido correctamente.**

Si tenemos varios usuarios a los que dar acceso compartido a sus directorios personales, probablemente queramos utilizar el recurso compartido especial [homes]. Comenzamos editando la configuración de este apartado, en este caso la descomentamos y añadimos la línea de writable.

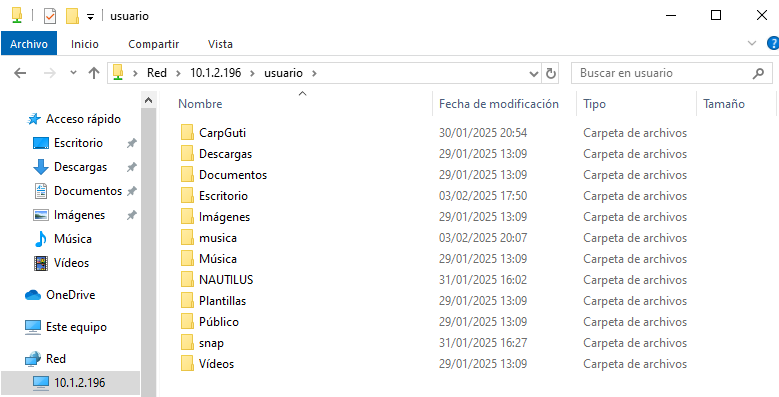


Una vez editado el archivo, reiniciamos la configuración.

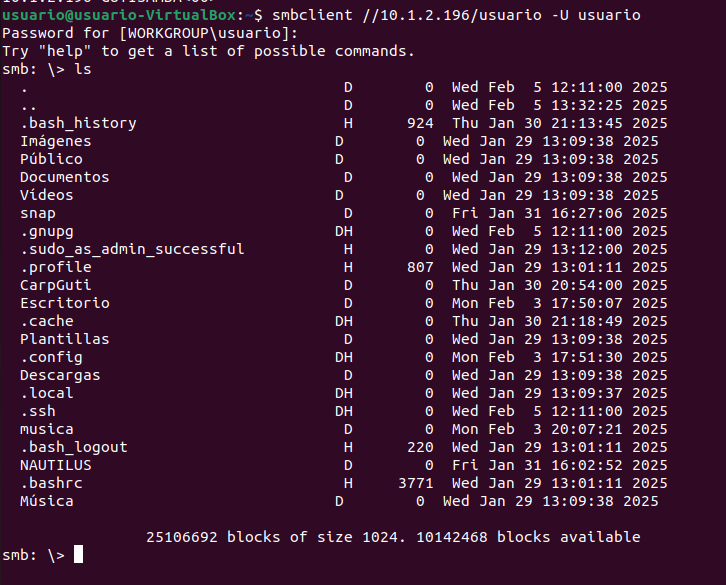
A continuación, entramos con una máquina cliente en Windows y aplicamos la ruta especifica de red con el nombre de usuario (\\10.1.2.196\usuario), este nos pedira la contraseña del usuario de SAMBA (Usuario1)

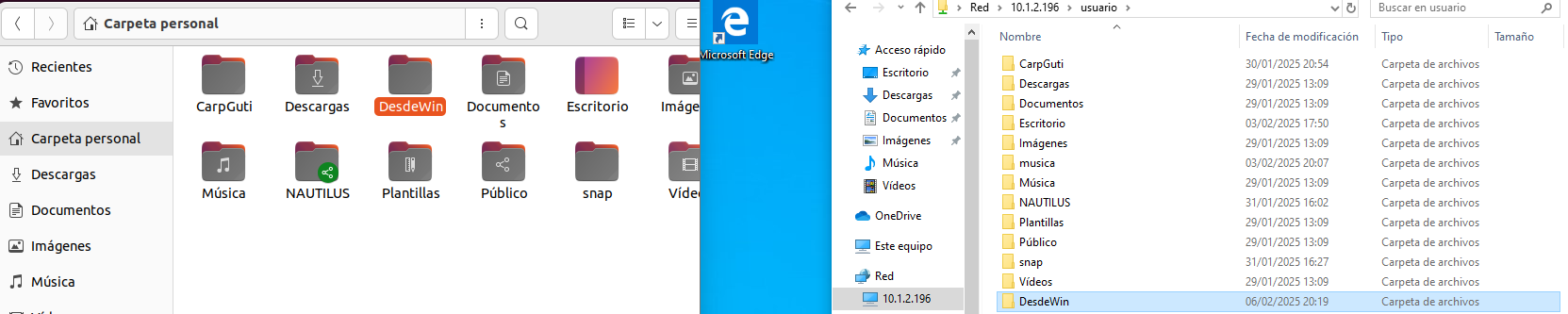


Ponemos las claves y al entrar podemos ver la carpeta Home del usuario en ubuntu, donde podemos ver, editar y eliminar archivos.



Si queremos hacer lo mismo desde Linux cliente aplicamos el siguiente comando en la terminal:



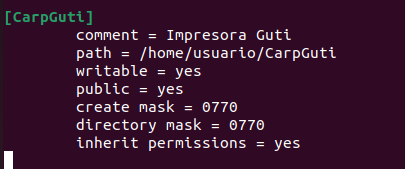




**Ejercicio 3. Investiga sobre el parámetro “inherit permissions”. ¿Para qué se utiliza este parámetro en un entorno con SAMBA? Realiza una comprobación de lo comentado anteriormente.**

El parámetro inherit permissions en Samba permite que los archivos y directorios creados dentro de un recurso compartido hereden los permisos de la carpeta padre en lugar de usar create mask y directory mask. Esto es útil en entornos colaborativos para mantener permisos consistentes.

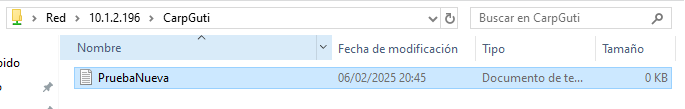
Para aplicar esta configuración en un recurso compartido en Samba, edita el archivo /etc/samba/smb.conf y agrega el parámetro inherit permissions = yes dentro de un recurso compartido:



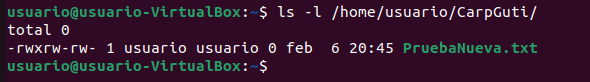
* **inherit permissions = yes:** Hace que los nuevos archivos y carpetas hereden los permisos del directorio padre.
* **create mask = 0770:** Define permisos predeterminados para nuevos archivos, pero solo se aplicará si inherit permissions está desactivado.
* **directory mask = 0770:** Define permisos predeterminados para nuevos directorios, pero solo se aplicará si inherit permissions está desactivado.

Para realizar la comprobación de inherit seguiremos los siguientes pasos:

1. **Acceder desde un cliente y crear un archivo**

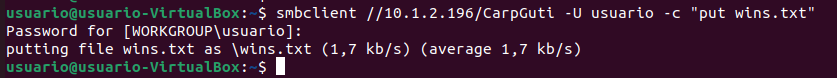


1. **Verifica los permisos**

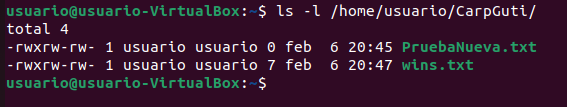


1. **Prueba con Linux Cliente**

Si lo queremos hacer desde Linux, usaremos el siguiente comando en la terminal



Y comprobamos el resultado

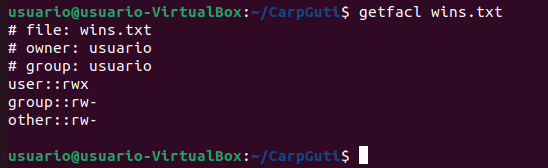


**Ejercicio 4. Infórmate sobre las ACLs y los comandos getfacl y setfacl. Práctica lo leído.**

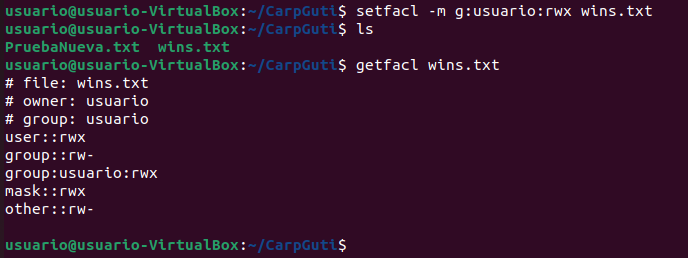
Vamos a estudiar las Listas de Control de Acceso con ejemplos prácticos..

Antes de crear una lista de acceso, por ejemplo del directorio ‘/home/usuarios/sistemas‘ es conveniente realizar un respaldo de los permisos existentes, para que en caso de que queramos anular la ACL en un futuro, podamos usar este backup.

* **getfacl:** Este comando muestra los permisos tradicionales y las ACLs asignadas.

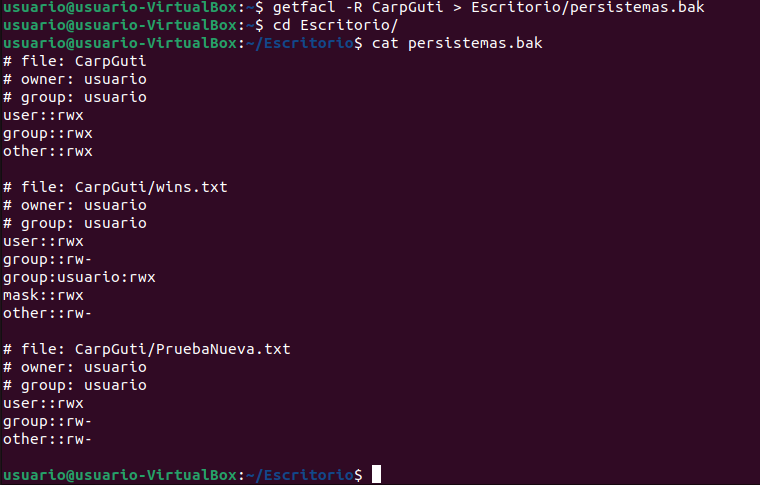


* **setfacl:** Este comando permite modificar los permisos ACL de archivos y directorios.



Sabiendo esto, comenzamos con algunos comandos de ejemplo:

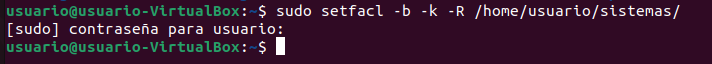
1. **Crear un respaldo de los permisos para /home/usuarios/sistemas**



1. **Restaurar los permisos de un directorio en caso de que apliquemos una ACL errónea**

$ setfacl --restore=permsistemas.bak

De momento vamos a imaginar que tenemos un directorio ‘/home/usuarios/sistemas‘ donde diferentes usuarios pueden acceder pero en concreto queremos que sea directorio para el grupo de sistemas. Lo primero que vamos a llevar a cabo antes de implementar ACL sobre este directorio, será dejarlo ‘limpio’, es decir, anularemos otras posibles listas de acceso que este pudiese tener o incluso si tuviese una ACL por defecto. Esto lo haremos con el siguiente comando:



* Eliminamos la posible ACL que ya pudiese tener el directorio: -b
* Eliminamos la posible ACL por defecto que pudiese tener el directorio: -k
* Aplicamos los cambios de forma recursiva: -R

Ahora con el directorio limpio vamos a crear la ACL, acción que podremos realizar mediante el uso de dos parámetros: ‘s‘ o ‘m‘. Si quisiéramos crear una ACL eliminando una ya existente usamos ‘s‘, si por el contrario queremos modificar una ACL o crearla si no existe usaremos ‘m‘. Nosotros usaremos ‘m‘ ya que antes hemos eliminado todo lo relacionado con ACL en el directorio.

$ sudo setfacl -R -m g:sistemas:rw

Aquí igualmente hemos aplicado de forma recursiva (-R) el comando. Vamos a desglosar la cadena ‘g:sistemas:rw‘ para ver que significado tiene cada uno de sus campos. Como nota añadir que el 3º campo es opcional a la hora de eliminar una ACL.

* Indicar si se trata de una ACL de usuario (u) o de grupo (g): En nuestro caso, de grupo
* El segundo campo es el nombre del grupo (podemos pasar el GID igualmente): sistemas
* El tercer y último campo son los permisos de la ACL, podemos pasar en valor octal como con chmod: rw

Ahora vamos a darle al grupo de explotación permisos de lectura y acceso para el subdirectorio /home/usuarios/sistemas/prod pero además algo que no hemos hecho en la anterior ACL es crearla como default, esto implica que cada subdirectorio o archivo que se cree bajo ./prod heredará los permisos, muy útil para no tener que andar modificando la ACL continuamente (cada vez que se cree contenido). Usaremos la opción ‘-d‘

$ sudo setfacl -d -R -m g:explotacion:rx /home/usuarios/sistemas/prod

Para hacer una prueba de permisos, crearemos el usuario maria y hacemos lo siguiente:

