

Administración del acceso al dominio.

Caso práctico



Alain Bachelier (CC BY-NC-SA)

—**Vindio y Laro**, hemos gestionado nuestro entorno de red instalando un dominio y configurando sus controladores. Aprovecharemos el servidor de dominio para administrar los recursos compartidos como son las aplicaciones, impresoras, carpetas y ficheros.

—**Juan**, ¿tendremos que compartir recursos en el dominio?

—Efectivamente **Vindio**, en nuestra estructura de red deberemos aplicar una política de compartición de recursos en el dominio para que los usuarios, desde cualquier terminal, puedan acceder a ellos bajo una supervisión de permisos y derechos, procurando como responsables de la administración gestionar un buen control de seguridad en el acceso.

Recordemos que desde un terminal de Windows 10, uno de los caminos **para acceder a un recurso compartido** que sirve otro equipo es abrir el explorador de archivos (*Botón Windows +E*), pulsar en *Red*, se visualizarán los equipos que han iniciado sesión en la red, seguidamente pulsamos en el ícono del terminal deseado y veremos los recursos compartidos como impresoras carpetas o directorios, unidades, etc., si pinchamos en el recurso deseado podremos acceder siempre que tengamos los permisos correspondientes.

También sabemos que con la instalación de la aplicación **smbclient** (normalmente ya se integra en la mayoría de los sistemas Linux durante el proceso de instalación), **podemos acceder desde un terminal Linux a recursos compartidos por una máquina Windows mediante el protocolo SAMBA**. Así desde el explorador de archivos de Linux pinchamos en *Otras ubicaciones* (esta en el panel izquierdo), nos aparece un rectángulo que esta en la parte inferior y escribimos lo siguiente:

smb://192.168.1.120/

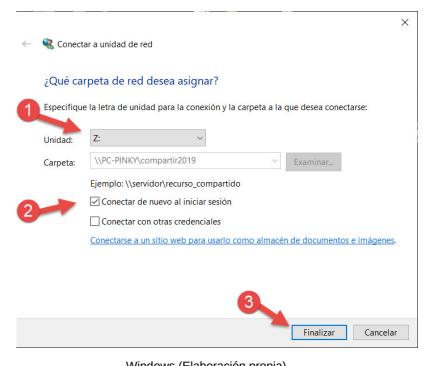


Hexmar (CC BY-NC-SA)

Donde 192.168.1.120 es la dirección IP del equipo al que nos vamos a conectar. Después pulsamos en el botón *Conectar*.

Cuando el recurso que comparte el servidor es un directorio, desde el equipo cliente de Windows 10 **podemos crear accesos directos o conexiones directas** para no tener que realizar todos los pasos anteriores cada vez que necesitemos utilizar el recurso, para ello desde la misma ventana donde estamos, seleccionamos el recurso y pulsamos el botón derecho del ratón y del menú escogemos la opción *Conectar a unidad de red...*, entonces aparecerá un ventana de edición y en el campo *Unidad* desplegamos para seleccionar una letra que será asignada al directorio compartido, marcamos el campo *Conectar de nuevo al iniciar sesión*, para terminar pulsar en el botón *Finalizar*. Cuando abrimos el explorador de archivos, veremos que el sistema ha creado una nueva unidad con la letra asignada en los pasos anteriores, si pulsamos en ella accederemos directamente al directorio compartido.

Una de las tareas del administrador es la de gestionar la seguridad en el acceso a los recursos compartidos y servicios que ofrece el servidor, con el fin de ofrecer una total integridad de los datos y aplicaciones del servidor, y de esta forma proteger el dominio. Para conseguirlo, los sistemas operativos disponen de herramientas que ofrecen políticas de seguridad en el acceso y la posibilidad de aplicar propiedades a los recursos con el fin de atribuirles características de permisos de uso para los usuarios y grupos.



Debes conocer

Como hemos aprendido en unidades anteriores, para la administración de usuarios y grupos podemos utilizar el grupo de comandos net. En los siguientes enlaces puedes ampliar conocimientos para gestión del uso y acceso de recursos en los equipos de una red, desde el símbolo de sistema o consola de comandos en sistemas Windows.

[Como usar los comando net en Windows](#)

[Comando net user en Windows](#)

Administrar cuentas de usuarios con PowerShell

[Crear y borrar cuentas con PowerShell](#)

[Gestión de usuarios y grupos en PowerShell](#)

Gestión de usuarios, grupos, unidades organizativa, equipos y dominios en Active Directory en PowerShell

[Gestión de usuarios y equipos en Active Directory](#)

[Gestión de grupos en Active Directory](#)

[Gestionar dominios y unidades organizativas en Active Directory en PowerShell](#)

1.- Equipos del dominio.

Caso práctico



Alain Bachellier (CC BY-NC-SA)

—Chicas, sabéis que nuestra empresa tiene un controlador de dominio y la estructura de red se ha ampliado instalando máquinas virtuales Linux en los equipos con más prestaciones en hardware y que disponen de base el sistema operativo Windows.

—Vindio, ¿Por qué se han instalado máquinas virtuales Linux en algunos equipos?

—Noiba, eso es así para que los usuarios pueden acceder al dominio desde los dos sistemas sin necesidad de comprar nuevos equipos.

—¿Tiene la empresa una red mixta?

—Así es Naroba, en la empresa tenemos un red mixta donde se integran equipos Windows y Linux en el controlador de dominio Windows Server 2019.

En muchos entornos de red las estaciones de trabajo pueden estar configuradas con un sistema operativo Windows o Linux, pudiendo formar las llamadas redes mixtas.

En la unidad anterior ya aprendimos a gestionar un dominio mediante la instalación de un controlador de dominio. También comprobamos que un controlador de dominio, con más o menos posibilidades de administración, puede estar habilitado en servidores Windows o en un Servidores Linux.

Debido a la extensión de los posibles casos de acceso, también estudiamos la forma de crear cuentas de equipo en un controlador de dominio Windows cuando los terminales se ejecutaban bajo Windows , y vimos como añadir cuentas de equipo Windows a un controlador de dominio bajo Linux.

En esta unidad aprenderemos a añadir terminales Linux a controladores de dominio Windows. Para ello se tendrán que realizar las siguientes tareas:

Configurar los parámetros de la red.

Realizaremos los siguientes pasos en modo comando ya que conocemos de unidades anteriores como trabajar con el entorno gráfico, usaremos el ejemplo para un dominio *antonio.edu* controlado en un servidor Windows con el nombre del equipo **WSERVER19** y con la *IP*: **192.168.1.2**, el cliente Linux tiene el nombre de host "serverlinux" y una *IP*: **192.168.1.139**.

El terminal Linux tendrá configurado los parámetros de **configuración TCP/IP** de forma que pertenezca a la misma red que el servidor Windows y su *IP* del servidor **DNS** será la del equipo que tenga instalado el servicio (controlador de dominio Windows, ya que se instalará de forma predeterminada). Para configurar la red en Ubuntu 20.04 se utiliza la herramienta *Netplan*. *Netplan* se encarga de leer la configuración la cual se guarda en el directorio */etc/netplan/*.yaml* (ejemplo del nombre archivo *.yaml* 01-network-manager-all.yaml) , durante el proceso de arranque del sistema, *Netplan* genera un archivo de configuración cuya misión será la transferir el control de dispositivos hacia un demonio de red especial.

Netplan usa algunos comandos como:

```
netplan generate
```

Este comando usa */etc/netplan* para generar la configuración requerida para los renderizadores seleccionados.

```
Netplan apply
```

Aplica las configuraciones de los renderizadores y las reinicia si es necesario.

Tenemos que averiguar la interfaz de red que estamos usando, para ello escribimos el comando:

```
root@prueba:$ ipconfig -a
```

En la imagen podemos ver, que nuestro interfaz de red es **enp0S3** que esta señalado por la flecha de color rojo.

Para configurar una IP fija, ejecutamos el siguiente comando:

```
sudo nano /etc/netplan/01-network-manager-all.yaml
```

En el caso de que no se haya creado el archivo YAML, podemos generarlo usando el siguiente comando:

```
sudo netplan generate
```

```
root@principal1:/etc# ipconfig -a
enp0S3: flags=7449LOOPBACK,RUNNING,BROADCAST mtu 6556
        inet 127.0.0.1/8 brd 127.255.255.255 scopehost
              link-layer 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 192.168.1.139 brd 192.168.1.255 scopeglobal
      link-layer 00:0c:29:ff:fe:04 brd 00:0c:29:ff:ff:ff
        ether 00:0c:29:ff:fe:04 txqueuelen 10000 (Ethernet)
          RX packets 12354 bytes 914736 (914.7 KB)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 12354 bytes 914736 (914.7 KB)
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=734LOOPBACK,RUNNING mtu 6556
        inet 127.0.0.1/8 brd 127.255.255.255 scopehost
              link-layer 00:00:00:00:00:00 brd 00:00:00:00:00:00
loop  txqueuelen 1000 (Bucle local)
      RX packets 3877 bytes 337724 (337.7 KB)
      RX errors 0 dropped 0 overruns 0 frame 0
      TX packets 3877 bytes 337724 (337.7 KB)
      TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
Ubuntu (Elaboración propia)
```

Editamos el fichero el fichero **sudo nano /etc/netplan/01-network-manager-all.yaml** y escribimos lo siguiente:

```

network:<br /> version: 2

renderer: NetworkManager

ethernets:

enp0s3:

addresses:

- 192.168.1.139/24

gateway4: 192.168.1.1

nameservers:

addresses: [8.8.8.8, 4.4.4.4]

```

Ubuntu (Elaboración propia)

Donde:

enp0s3: es el nombre de la interfaz de red.

addresses: dirección IP 192.168.1.139 con la mascara 255.255.255.0 que lo indica el 24.

nameservers: definimos las direcciones de DNS.

Hay que tener en cuenta que hay que dejar espacio entre la opción cada elemento y su contenido. Por ejemplo: la dirección IP debajo de addresses: tiene que estar un poco tabulada hacia la derecha con respecto a addresses, igual pasa con los demás elementos.

Para que los cambios se apliquen ejecutamos el comando:

```
sudo netplan apply
```

Configuramos los servidores DNS de búsqueda, deberemos incluir el servidor DNS de nuestro dominio de la red, editar el fichero:

```
pincipal@principal:~$ sudo nano /etc/resolv.conf
```

Ubuntu (Elaboración propia)

Antes de modificar el fichero conviene realizar una copia del fichero original, así siempre podemos recuperar el fichero original en el caso de que hubiera algún problema. Para ello, escribimos el comando:

```
pincipal@principal:~$ cp /etc/resolv.conf /etc/resolvoriginal.conf
```

Escribimos en el fichero /etc/resolv.conf el DNS de nuestro dominio, añadimos la siguiente línea:

```
nameserver 192.168.1.2
```

La IP incluida es la del servidor Windows.

Instalar el software necesario para la gestión.

Instalamos las siguientes aplicaciones necesarias para configurar el servicio:

```
pincipal@principal:~$ sudo apt-get install samba smbclient winbind krb5-user krb5-config
```

En la siguiente tabla vemos para que sirve cada programa:

samba	Permiten instalar la aplicación cliente para que Linux pueda comunicarse con el Servidor para acceder a recursos compartidos en el controlador de dominio Windows . Ofrecerá una interfaz similar a la del servicio ftp.
smbclient	
Winbind	Necesario para autenticar de acceso de los usuarios Linux hacia un servidor Windows
Krb5-user	Sistema Kerberos utilizado por Windows para validar las claves de acceso de clientes, se instalara un protocolo de autenticación segura entre dos equipos de una red.
Krb5-config	

Configurar Kerberos (presentación del login para el acceso seguro al servidor Windows desde el cliente Linux).

Editamos el fichero /etc/hosts para **configurar y resolver los nombres de los equipos**, añadimos al final del fichero los nombre de los equipos que forman parte del dominio en red junto con sus direcciones IPs, por lo menos el del servidor Windows y el del terminal Linux. Según el ejemplo:

```
pincipal@principal:~$ sudo nano /etc/hosts
```

Es conveniente realizar una copia de seguridad de este fichero, por si acaso. Utilizamos el mismo comando que usemos antes.

En el fichero /etc/host añadimos las siguientes líneas:

```
#identificamos el terminal Linux
```

```
192.168.1.139 principal1
```

```
#identificación del servidor Windows según el nombre NETBIOS del equipo Windows
```

```
192.168.1.139 antonio
```

```
#identificación del nombre dominio dns y del FQDN (nombre del equipo más el domnio)
```

```
192.168.1.2 antonio.edu WSERVER19.antonio.edu
```

Configuramos la validación de clientes en el controlador de dominio Windows mediante Kerberos, para ello se editará el fichero de configuración /etc/krb5.conf, y añadimos las siguiente líneas en el fichero (mirar la imagen de la izquierda):

Configurar el servicio de Samba.

Configuramos el servicio Samba para que el terminal Linux se pueda comunicar como cliente del servidor de dominio Windows . Para ello, editamos el fichero /etc/smb.conf y modificamos las líneas que podemos ver en la dos imágenes siguientes:

```
21 #Identificación del fichero smb.conf
22 #----- Global Settings -----
23
24 [global]
25
26 ## Browsing/Identification #####
27 security = ads
28 netbios name = principal1
29 realm = antonio.edu
30
31 password server = 192.168.1.139
32 #Configuramos el nombre de windows/NT domain name your Samba server will part of
33 workgroup = antonio
34
35 log file = /var/log/samba/%m.log
36 syslog = 0
37 idmap uid = 10000-29999
38 idmap gid = 10000-29999
39
40 winbind separator = \
41 winbind enum groups = yes
42 winbind enum users = yes
43 winbind use default group = yes
44 #El dominio winbind usa este parámetro para asignar el directorio personal para ese usuario
45 #La cadena que viene por defecto, se sustituye por el nombre del usuario. Si la cadena %u está
46 #presente, se sustituye por el nombre de usuario en Windows
47 template homedir = /home/%D/%U
48 template shell = /bin/bash
49 client use spnego = yes
50
51 #Autenticación
52 server string = Terminal del dominio antonio
53 encrypt passwords = yes
54
55 #Configuramos la sección homes para que cuando se conecte un usuario pueda acceder a su
56 #cuenta personal en Linux, %s nombre del servicio actual
57
58 [homes]
59
60 comment = Home Directories
61 valid users = %S
62 browsable = No
63 read only = No
64 inherit acls = Yes
65
66 #Compartir una carpeta para los usuarios
67 [users]
68
69 comment = All users
70 path = /home
71 read only = No
72 inherit acls = Yes
73 veto files = /aquota.user/groups/shares
74
75
76
77
```

Ubuntu (Elaboración propia)

```
1 [libdefaults]
2
3 default_realm = Antonio.edu
4 # The following krb5.conf variables are only for MIT Kerberos.
5
6 ccache_type = 4
7 forwardable = true
8 proxiable = true
9
10 # The following libdefaults parameters are only for Heimdal Kerberos.
11
12 fcc-mit-ticketflags = true
13
14 [realms]
15
16 antonio.edu = {
17   kdc = 192.168.1.139
18   admin_server = 192.168.1.139
19   default_domain = antonio.edu
20 }
21 antonio = {
22   kdc = 192.168.1.139
23   admin_server = 192.168.1.139
24   default_domain = antonio.edu
25 }
26 antonio = {
27   kdc = 192.168.1.139
28   admin_server = 192.168.1.139
29   default_domain = antonio.edu
30 }
31 [domain_realm]
32 antonio.edu = antonio.edu
33
34 [logging]
35 log_file = /var/log/krb5/krb5kdc.log
36 admin_server = FILE:/var/log/krb5/kadmind.log
37 default = SYSLOG:NOTICE:DAMON
38 [appdefaults]
39 pam = {
40   ticket_lifetime = 3d
41   renew_lifetime = 1d
42   retain_after_close = 10 days
43   retain_after_delete = 10 days
44   minimum_uid = 0
45   try_first_pass = true
46 }
```

Ubuntu (Elaboración propia)

Creamos el directorio para los usuarios del dominio:

```
pincipal@principal:~$ sudo mkdir /home/antonio
```

Configurar Winbind para resolver nombres y grupos de usuarios en el dominio.

Editamos y configuramos el fichero /etc/nsswitch.conf para controlar la resolución de nombres de usuarios y grupos de dominio; esto le indica al sistema dónde buscar contraseñas y grupos. Modificamos o añadimos las siguientes líneas:

```
passwd:      files winbind
```

```
group:       files winbind
```

```
shadow:      files winbind
```

```
hosts:       files dns winbind
```

Seguidamente deberemos de configurar que todos los usuarios del dominio puedan acceder desde el entorno gráfico de Linux, para ello deberemos editar y modificar como root los fichero de configuración de pam (son programas que permiten a los usuarios acceder al sistema verificando la identidad de cada usuario a través de un proceso llamado autenticación). A cada fichero agregamos o modificamos las siguientes líneas y eliminamos, si existen las líneas en rojo:

FICHERO	LÍNEAS

/etc/pam.d/common-account	account sufficient pam_winbind.so account required pam_unix.so try_first_pass
/etc/pam.d/common-auth	account sufficient pam_winbind.so account required pam_unix.so nullok_secure try_first_pass auth optional pam_smbpass.so migrate missingok
/etc/pam.d/common-password	password sufficient pam_winbind.so password required pam_unix.so nullok obscure min=4 max=8 md5 ry_first_pass
/etc/pam.d/common-session	session required pam_mkhomedir.so skel=/etc/skel/ umask=0022 session sufficient pam_winbind.so session required pam_unix.so try_first_pass

Estando en sesión como usuario root creamos los tickets Kerberos (nos pide la contraseña del administrador del dominio) y configurar la sincronización de la hora entre el ordenador cliente y el servidor.

```
root@principal:~$ kinit administrador@antonio.edu
```

```
Password for administrador@antonio.edu:
```

```
pincipal@principal:~$ net time set
```

Reiniciamos los servicios samba y winbind:

```
root@principal:~$ systemctl restart smbd
root@principal:~$ systemctl restart winbind
```

Añadir el terminal de Linux al controlador de dominio Windows.

<a href="https://educacionadistancia.juntadeandalucia.es/formacionprofesional/pluginfile.php/40556/mod_scorm/content/0/mailto:root@principal:-"

Nos solicitará la contraseña del administrador del dominio ya que no la hemos indicado directamente en la orden con el parámetro %clave_administrador después del nombre del usuario administrador.

Si no se ha producido ningún error (en caso contrario repasar la configuración de los ficheros), ya podemos iniciar sesión con usuarios locales o del dominio de Active Directory Windows en nuestro Linux. Para iniciar sesión con un usuario del dominio en la ventana de login deberemos teclear nombre de dominio el signo indicado en el parámetro winbind separador del fichero smb.conf (en nuestro caso "\") junto al nombre de usuario (por ejemplo: antonio.edu\juan) y posteriormente la contraseña. Tenemos que cumplir la regla de que los usuarios del dominio no pueden ser usuarios locales del terminal Linux.

Podemos utilizar alguno de los siguientes comandos para consultar información del dominio desde Linux:

```
net ads info: Información del controlador de dominio.
net rpc testjoin: Comprueba si la integración es correcta mostrando un mensaje, como por ejemplo:
"Join to 'INFOALISAL' is ok"
wbinfo -u -g: Visualiza los usuarios y grupos del dominio.
net rpc info -U nombre_usuario: Muestra información del usuario del dominio.
```

Debes conocer

Cómo configurar una dirección IP estática en Ubuntu 20.04

[Configurar un IP estática en Ubuntu](#)

Para saber más

Cómo configurar una dirección IP estática o DHCP en Ubuntu 19.04

[Configurar una IP estática o DHCP en Ubuntu](#)

Autoevaluación

¿Qué ocurrirá después de ejecutar el comando “`net ads join -S distancia.infoalisal.local -U administrador`” necesario para añadir una máquina de Linux al Active Directory de un controlador de dominio gestionado por Windows Server?

- No ocurrirá nada.
- Dará error ya que la orden no existe.
- Nos solicitará la contraseña del usuario administrador del dominio.
- No es correcto el segundo parámetro.

No es verdad, ya que nos solicita la contraseña del administrador del dominio.

La orden está bien, solamente nos solicitará la clave del administrador del dominio.

Muy bien, vas por buen camino.

Son correctos los parámetros introducidos.

Solución

1. Incorrecto
2. Incorrecto
3. Opción correcta
4. Incorrecto

2.- Permisos y derechos.

Caso práctico



Alain Bachellier (CC BY-NC-SA)

—**Vindio y Laro**, he creado un plan de seguridad de dominio, mediante el cual se restringe y permite al acceso a los recursos del servidor dependiendo del tipo de usuario y de los grupos a los que pertenezca.

—**Juan**, de esta manera, cada usuario solamente puede acceder a los recursos que necesita para su actividad en la empresa.

—Claro **Vindio**, así todo está mejor estructurado y es más seguro, ya que cada usuario solo accede a los recursos que necesita.

—Ahora tendremos que compartir los recursos y gestionar los permisos pertinentes para su correcto y seguro uso. Por ejemplo, existen tres impresoras en red compartidas para todos los usuarios, también

cada usuario puede acceder a su directorio particular en el servidor con todos los permisos que le permitan escribir y leer para poder guardar sus trabajos, mientras que los usuarios del mismo grupo al que pertenece solamente podrán acceder con permiso de lectura.

Una de las tareas del administrador es la de gestionar la seguridad en el acceso a los recursos compartidos y servicios que ofrece el servidor, para ello por una parte, tendrá que autorizar las diferentes acciones o tareas que los usuarios o grupos de usuarios pueden realizar en todo el dominio desde el momento que entran en el sistema, estas acciones se identifican como **derechos**. Por otra parte, deberá atribuir a cada recurso compartido los **permisos** u operaciones que pueden realizar los usuarios o grupos a la hora de actuar sobre él como pueden ser leer, modificar, borrar, etc.

Es importante realizar una buena administración de los permisos y derechos, con el fin de no dejar al descubierto, por una mala planificación, información valiosa para el sistema o información privada de los usuarios. Los diferentes permisos de acceso que puede tener un recurso como puede ser una carpeta, impresora, dispositivo, fichero, etc., dependerán de las operaciones que se puedan realizar que pueden ser: lectura, ejecución, modificación, borrado, apertura, creación, cierre, copiar, mover, renombrar, escritura, etc. Cada recurso dispondrá de un listado con los permisos que tiene cada usuarios y grupos sobre él, según hayan sido asignados por el administrador. Cada servidor dispone de diferentes niveles de permisos sobre ficheros y carpetas dependiendo de la posibilidad que ofrezca el sistema de ficheros utilizado (FAT, NTFS, Ext4, etc.).

Mediante la gestión de derechos, el administrador indica las políticas de control para el acceso de usuarios y grupos de usuarios al sistema. **La administración de derechos se basa, principalmente, en la aplicación de reglas llamadas directivas de seguridad que definirán características relacionadas con la seguridad del sistema.** Para facilitar la gestión de derechos el propio sistema dispone de grupos de usuarios predeterminados con unas directivas asignadas por defecto. Algunas reglas son: poder acceder localmente o remotamente al sistema, poder o no instalar aplicaciones, solamente tener acceso al sistema durante un periodo de tiempo determinado, no poder ejecutar una aplicación concreta, etc.

La seguridad en el acceso a sistemas Linux no dispone de una herramienta para gestión de directivas de seguridad como dispone Windows, podemos aplicar un control de acceso seguro mediante el protocolo *OpenSSH* y la aplicación de comandos como *chage* (gestiona la caducidad de contraseñas), asignación al usuario a que pertenezca grupos predeterminados del sistema, gestión de *iptables* en acceso por interface de red (actuaciones de cortafuegos), etc.

En el dominio Windows la información de cada usuario referente a los derechos de uso y acceso al sistema se gestiona mediante Active Directory, que contiene datos como el número SID identificador de usuario y los SID de grupos a los que pertenece, así como la lista de directivas otorgadas. En Linux dicha la información se almacena en ficheros como *shadow* y *passwd* donde SUID es el número identificado de usuario y SGID a los grupos. **En Windows Server 2019 para poder configurar recursos compartidos será necesario tener instalada la función de Servicio de Archivos**, en distribuciones anteriores viene instalado de forma predeterminada.

Debes conocer

Instalar y configurar un servidor de archivos en Windows Server 2019

[Instalar y configurar un servidor de archivos en Windows Server](#)

Para saber más

Cómo habilitar el servidor de archivos en Windows Server

[Habilitar el servidor de archivos en Windows Server](#)

Autoevaluación

¿Qué rol tenemos que agregar para que podamos utilizar la herramienta Administrador de recursos del servidor de archivos en Windows Server 2019?

- Administrador de recursos del servidor de archivos.
- Servidor de archivos y Administrador de recursos del servidor de archivos.
- Servidor de archivos.
- Servicio Búsqueda de archivos.

Muy bien, vas por buen camino.

No es correcta, debes de revisar los contenidos.

No es correcta esta función, aunque este relacionada.

No es correcta, revisa los contenidos de la pregunta.

Solución

1. Opción correcta
2. Incorrecto
3. Incorrecto
4. Incorrecto

2.1.- Permisos en Windows Server 2019: Compartir recursos y listas de control.

En Windows, con diferencia de los sistemas de archivos FAT, en las **particiones NTFS** podemos utilizar permisos y cifrado para restringir el acceso a los ficheros. Al asignar permisos a un objeto estamos indicando que usuarios o grupos puede acceder y que operaciones pueden realizar.

El servidor guarda toda la información relacionada con los objetos y sus permisos (descriptores de seguridad) en las **listas de control de acceso** o **ACL** (exclusivas de particiones con formato NTFS) que son listas que le dicen al Sistema Operativo qué o quién tiene permiso para acceder a un objeto determinado. Una ACL contiene una ACE para cada usuario o grupo, indicando qué permisos tiene. Todos estos permisos pueden ser modificados con los comandos `<i>cacls /?</i>` (para acceder a la ayuda ejecutamos desde símbolo del sistema: `<i>cacls /?</i>`). El comando `icacls` nos muestra o modifica las listas de control de acceso discrecional (**DACL**) en los archivos especificados y aplica las DACL almacenadas a los archivos de los directorios especificados.

Para poder gestionar permisos en recursos compartidos debemos de tener en cuenta algunas **características, como son:**

Los derechos tienen prioridad ante cualquier permiso.

Los permisos son acumulativos, por ejemplo puedes tener permisos como usuario y además como miembro de un grupo.

Los permisos de los archivos preceden o tienen prioridad sobre las carpetas y los ficheros o carpetas heredan los permisos de sus contenedores.

Un permiso puede tener dos valores **Permitir** y **Denegar**, en caso de disponer de los dos a la vez se considera el de Denegar por ser el más restringido. Los permisos **explicitos** tienen prioridad sobre los **heredados**.

Es conveniente asignar permisos a nivel de grupos de usuarios, no individualmente a cada usuario de manera que no compliquemos y sobrecarguemos la tarea de administración.

Los permisos que se asignan a una carpeta compartida se determinan por los permisos de recurso compartido más los NTFS, aunque al final **se aplicarán siempre los permisos más restrictivos**; por ejemplo, "podemos definir los permisos de un recurso para **Control total** al grupo **Todos** y usar los permisos NTFS para restringir el acceso de una manera más exclusiva".

Cada recurso tiene al menos un **propietario** que puede configurarlos permisos del recurso y a quien se le conceden, así que un Administrador que necesite modificar los permisos en un recurso debe tomar posesión del archivo

Los permisos de recursos compartidos aplican sólo a carpetas, y los permisos NTFS se aplican a carpetas y ficheros.

No se permiten las conexiones múltiples para un servidor o recurso compartido compatible por el mismo usuario, usando más de un nombre de usuario.

Windows Server puede gestionar los permisos mediante dos modos o niveles de acceso:

Permisos para el acceso local (desde el mismo ordenador) deberemos de utilizar los permisos NTFS.

Permisos para el acceso a través de la red (desde otro terminal al servidor del recurso) se deben de utilizar los llamados permisos para recursos compartidos (SHARE), junto con los permisos NTFS (será necesario que el volumen esté formateado con este tipo de sistema de archivos) para potenciar la seguridad. En el caso de disponer de una partición FAT32 solamente podemos establecer permisos para carpetas o recursos compartidos.

Compartir recursos en un controlador de dominio Windows Server 2019

Para activar o desactivar las funciones de recursos compartidos, en el panel de búsqueda escribimos *Panel de control-Redes e Internet-Centros de redes y recursos compartidos-Cambiar opciones de uso compartido para distintos perfiles de red*. Disponemos de las siguientes opciones:

Modo invitado o público: permite a los usuarios trasladar los recursos que desean compartir a una carpeta creada por el sistema de manera predeterminada, situada en `%SystemDrive%\Users\Public` del servidor, donde todos los usuarios del dominio tienen acceso a todos los datos con los permisos que tenga la propia carpeta pública. Este directorio se puede utilizar localmente o remotamente (siempre que se autorice). Para poder acceder vamos a *Inicio-Explorador de archivos-Disco local (C:)-Usuarios-Acceso público*. Dentro de la carpeta Public encontramos las siguientes subcarpetas para poder organizar los archivos que alojen los usuarios:

Documentos públicos: para compartir documentos.

Descargas públicas: Para compartir ficheros descargados.

Imágenes públicas, Música pública, Vídeos públicos: para compartir ficheros de multimedia.

Los permisos de acceso a la carpeta Acceso público serán asignados por el grupo **Todos** (determinado por el sistema) que representa a todos los usuarios del servidor.

Modo Privado: utilizado para compartir recursos a los cuales se puede acceder a través de la red. Es el más recomendado por seguridad. Podemos compartir un recurso siempre que hayamos iniciado sesión como administrador y podemos hacerlo por varios caminos como:

A través del explorador de Windows: forma comentada y explicada en los contenidos de la UT.06.

Desde la herramienta de Administración de equipos.

Desde la consola de administración de almacenamiento y recursos compartidos: donde tenemos más posibilidades para su gestión como son:

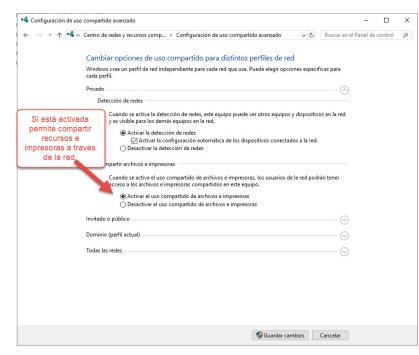
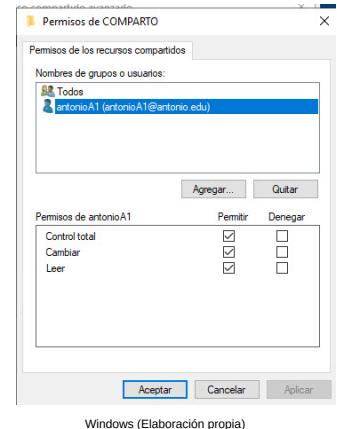
Aplicar permisos NTFS.

Indicar los protocolos utilizados para gestionar el recurso.

Cantidad de usuarios que pueden acceder.

Aplicar cuotas de acceso a los recursos compartidos.

Filtrado de seguridad para el alojamiento de tipos de ficheros.



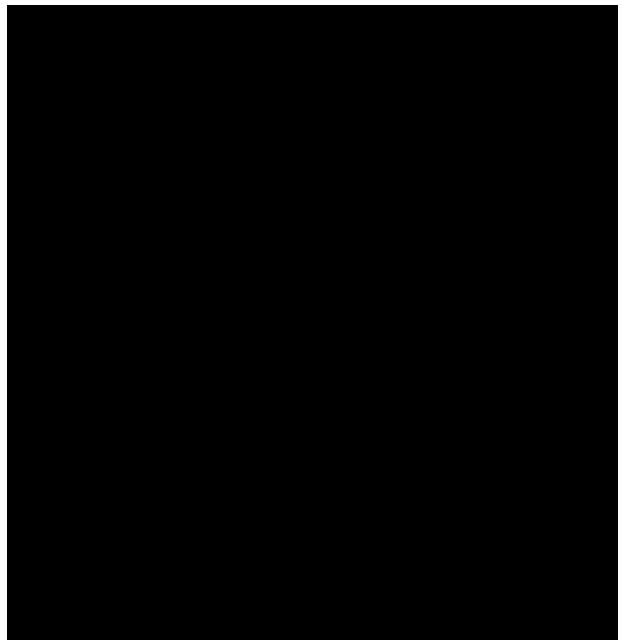
Indicar permisos NFS para compatibilidad con equipos Linux.
Publicar utilizando almacenamiento a través del espacio de nombres DFS.
Indicar como utilizar el recurso sin conexión.

Dominio: podemos activar dos opciones, la primera es *activar detección de redes*, lo que permite que este equipo pueda ver otros equipos y dispositivos en la red y es visible para los demás equipos en la red. La segunda opción es *Activar el uso compartido de archivos e impresoras*, con esta opción los usuarios de la red podrán tener acceso a los archivos e impresoras compartidas e este equipo.

Windows dispone de **recursos compartidos especiales** creados por el sistema para facilitar las tareas de administración, muchos tienen el signo "\$" al final del nombre para que estén, por seguridad, ocultos a los usuarios. **No deberemos eliminar ni modificar dichos recursos**. El nombre y la función de algunos de ellos son:

Recursos especiales compartidos para la administración del sistema en AD	
	Para administrar el inicio de sesión de usuarios. Todos los usuarios que acceden tienen permiso de lectura. Almacena los ficheros por lotes o script que se ejecutan cuando inicia sesión un usuario. Por ejemplo: "Cuando deseamos acceder a un recurso del servidor podemos automatizar el acceso para que cuando acceda el usuario ya tenga realizada la conexión mediante unidades de red"; para ello seguiremos los siguientes pasos: 1.- Recordamos que tenemos que crear un Script o fichero por lotes (fichero bat, exe, cmd, etc.) que disponga al menos una línea con la orden con formato: <code> <pre>net use letra_unidad:\\nombre_servidor 0 ip\\nombre_recurso</pre> 2.- Guardarlo en la carpeta netlogon correspondiente a la ruta c:\Windows\SYSVOL\sysvol\distancia.com\SCRIPTS del servidor 3.- Entrar en las propiedades del usuario y agregar en el campo Script de inicio de sesión de la pestaña Perfil el fichero creado para que se ejecute en el momento que el usuario inicia sesión en el controlador de dominio.
NETLOGON	
ADMIN\$	Para gestionar la administración remota del equipo, apunta a la carpeta Windows donde se encuentran los programas más importantes de configuración del sistema.
PRINT\$	Para gestionar la administración remota de impresoras.
SYSVOL	Para contener los comandos que se ejecutan en el inicio de sesión. Almacena datos y objetos de Active Directory.
FAX\$	Para gestionar la administración remota de fax.
IPC\$	Para administrar la comunicación de programas.

0:00



Antonio López. [Descripción textual alternativa para el video "Compartición de recursos desde el administrador de equipos en Windows Server"](#) (Elaboración propia)

Para saber más

En el siguiente enlace puedes ampliar la información que te proporcionamos sobre la orden `cacls`.

[El comando cacls](#)

[Ejemplos del comando cacls](#)

Modificar permisos del sistema en Windows Server con la orden `icacls`

[Modificar los permisos del sistema de archivos NTFS con icacls](#)

[Comando icacls](#)

Permisos NTFS desde PowerShell con `icacls`

[Trabajar con permisos NTFS en PowerShell con icacls](#)

Cómo ver carpetas compartidas en Windows Server

[Ver carpetas compartidas en Windows Server](#)

Debes conocer

En este enlace se estudia la forma de compartir recursos desde Administración de almacenamiento y recursos compartidos.

[Crear una carpeta compartida en Windows Server 2019](#)

[Control de recursos compartidos en Windows Server](#)

Autoevaluación

De forma predeterminada los permisos de acceso a la carpeta **Acceso público** serán asignados para el grupo **Todos**.

- Verdadero.
- Falso.

Muy bien vas por buen camino.

Repasa un poco más el tema.

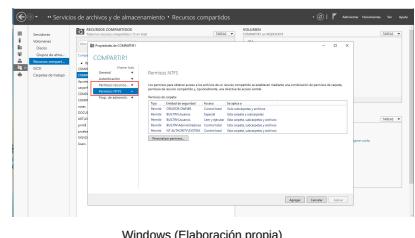
Solución

1. Opción correcta
2. Incorrecto

2.1.1.- Permisos para recursos compartidos y permisos NTFS en Windows Server 2019.

Para acceder a gestionar los permisos de un recurso, Windows Server 2019 ofrece varios caminos. Nosotros utilizaremos en muchas explicaciones el *Servicio de archivos y de almacenamiento*, la opción *Recursos compartidos* con la que podemos realizar tareas como: crear o eliminar volumenes y carpetas compartidas, decidir que protocolo gestiona el recurso compartido, aplicar los permisos NTFS, decidir cuántos y que usuarios acceden, publicar el recurso en un espacio DFS (Sistema de Ficheros distribuido), etc.

Se accede desde *Inicio-Administrador del servidor-Servicio de archivos y de almacenamiento-Recursos compartidos*, donde si seleccionamos un recurso compartido, pulsamos al botón derecho del ratón y elegimos *Propiedades*, en la pestaña *Permisos NTFS* podemos administrar los NTFS de nuestro recurso compartido y *Personalizar permisos* podemos además de personalizar los permisos, realizar tareas como: cambiar el propietario, deshabilitar herencia, etc.



Los permisos de las carpetas o **recursos compartidos** que el sistema nos deja configurar son:

Control total: el usuario o grupo tomará propiedad del recurso y puede realizar cualquier tarea.

Cambiar: crear, eliminar y modificar archivos y carpetas.

Leer: permite leer y ejecutar.

Los permisos **estándar o predeterminados NTFS** que se pueden asignar a una carpeta son:

Control total: para leer, cambiar, crear y ejecutar bien sean programas o carpetas.

Lectura y ejecución: para ver el contenido y ejecutar programas de una carpeta.

Modificar: para poder cambiar los ficheros y las carpetas, pero sin crear y eliminar ficheros ni carpetas nuevas.

Lectura: para poder ver y abrir el contenido.

Escribir: para poder crear y cambiar los ficheros y carpetas existentes.

Mostrar el contenido de la carpeta.

Debes conocer

Ver carpetas compartidas en Windows Server

[Ver carpetas compartidas en Windows Server](#)

[Compartición de recursos en en Windows Server](#)

[Control de recursos compartidos en Windows Server](#)

Instalar y configurar el servidor de archivos en Windows Server 2019

[Instalar y configurar el servidor de archivos en Windows Server](#)

Administrador de recursos del servidor de archivos en Windows Server

[Administrador de recursos del servidor de archivos en Windows Server](#)

Cada uno de estos permisos se compone de un grupo lógico de **permisos especiales NTFS**, que puedes conocer a continuación en el siguiente enlace.

[Permisos NTFS especiales aplicados a recursos en Servidor Windows.](#)

Gestionar permisos en Windows Server con un controlador de dominio:

Para ir al primer vídeo, pulsa [aquí](#).

Para ir al segundo vídeo, pulsa [aquí](#).

Para saber más

Permisos en Windows Server

[Lo que se permite o deniega con cada Permiso especial NTFS.](#)

Compartir una impresora en Windows 10

[Agregar una impresora en compartida Windows 10](#)

[Compartir una impresora en Windows 10](#)

Instalar impresoras en Windows Server

Autoevaluación

Si un usuario tiene solamente el permiso de lectura sobre una carpeta compartida en un dominio Windows, ¿puede crear nuevas carpetas dentro de la carpeta compartida?

- Sí, siempre que sea el propietario.
- Sí, siempre que tengas activado Permitir.
- Sí, ya que lo que no puedes es añadir ficheros.
- No.

No es correcta porque solamente puede leer.

No es correcta porque necesitas permiso de escritura o control total.

No es correcta porque necesitas disponer de más permisos.

Muy bien, vas por buen camino.

Solución

1. Incorrecto
2. Incorrecto
3. Incorrecto
4. Opción correcta

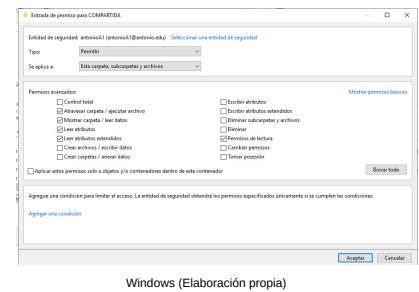
2.1.2.- Permisos especiales y heredados. Concepto de propiedad. Publicar permisos.

Además de los permisos estándar NTFS, podemos personalizar mejor las tareas que un usuario o grupo puede realizar sobre un recurso compartido **aplicando los permisos especiales NTFS**. Se establecen así:

1.- Vamos *Inicio-Administrador del servidor-Servicio de archivos y de almacenamiento-Recursos compartidos*, donde si seleccionamos un recurso compartido, pulsamos al botón derecho del ratón y elegimos *Propiedades*, luego pinchamos en *Permisos* y luego en el botón *Personalizar permisos*.

2.- Seleccionamos el usuario que vamos a editar sus permisos. Pulsamos en el botón *Editar*. Ahora pulsamos en el enlace *Mostrar permisos avanzados* (que se encuentra dentro del grupo *permisos básicos*). Aquí podemos añadir o eliminar permisos haciendo clic sobre ellos. Una vez seleccionados, pulsamos en el botón *Aceptar*.

3.- En la ventana que aparece, podemos *Agregar* o *Quitar* nuevos usuarios o grupos como ya hemos aprendido anteriormente (recordamos que si el botón *Quitar* no está disponible, desactivar la casilla *Incluir todos los permisos heredables del objeto primario de este objeto*); también se puede establecer los permisos especiales seleccionando el grupo o el usuario y pulsando al botón *Editar*.



Windows (Elaboración propia)

Los **permisos explícitos** son aquellos que se establecen de forma predeterminada en objetos, mientras que se consideran **permisos heredados** los que se propagan a un objeto desde un objeto ya creado que actúa como contenedor de recursos. Por ejemplo, la carpeta Mis documentos de un usuario tiene permisos explícitos, mientras que las carpetas y ficheros que se graban en sus interior ya disponen de permisos heredados. Los permisos explícitos tienen prioridad sobre los permisos heredados, incluidos los permisos Denegar heredados. Para administrar la herencia:

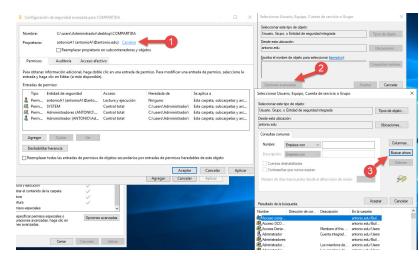
1.- Vamos *Inicio-Administrador del servidor-Servicio de archivos y de almacenamiento-Recursos compartidos*, donde si seleccionamos un recurso compartido, pulsamos al botón derecho del ratón y elegimos *Propiedades*, luego pinchamos en *Permisos NTFS* y luego en el botón *Personalizar permisos*.

2.- Pulsamos en el botón *Deshabilitar permisos*, aquí tenemos dos opciones:

2.1.- Convertir los permisos heredados en permisos explícitos en este objeto: se mantiene la *ACL* hereda de su objeto principal, la que ahora mismo tiene el recurso, pero puede cambiarse cuando queramos. Es decir, seguimos viendo los usuarios que veíamos antes con sus permisos tal como estaban, pero ahora podemos cambiar los permisos que queramos.

2.2.- Quitar todos los permisos heredados de este objeto: la *ACL* se borra completamente y la podremos crear desde cero. Es decir, la lista de usuarios y permisos se quedará en blanco y la tendremos que crear nosotros.

3.- Pulsamos en el botón *Aplicar* y *Aceptar* para confirmar los cambios.



Windows (Elaboración propia)

Vamos *Inicio-Administrador del servidor-Servicio de archivos y de almacenamiento-Recursos compartidos*, donde si seleccionamos un recurso compartido, pulsamos al botón derecho del ratón y elegimos *Propiedades*, luego pinchamos en *Permisos NTFS* y luego en el botón *Personalizar permisos*. El **concepto de propiedad de un recurso** se aplica a los usuarios o grupos que tienen el control sobre él, de forma predeterminada el que crea el recurso es el propietario. Podemos transferir la propiedad, y también puede tomarse por cualquier usuario o grupo que tiene el permiso *Tomar posesión* o de *Restaurar archivos y directorios* para el recurso en cuestión. El actual propietario puede conceder el permiso *Tomar posesión* a otro usuario. También, un usuario con derecho de *Restaurar archivos y directorios* puede elegir un usuario o grupo para asignarles la toma de propiedad. Para transferir la propiedad debemos de:

1.- En la parte superior de la ventana tenemos el nombre y el propietario del recurso compartido, pinchamos en la opción *Cambiar*. Pulsamos en *Opciones avanzadas-Buscar ahora* y selecciona el usuario que va a ser ahora el propietario del recurso compartido.

2.- Pulsamos en el botón *Aceptar*.

El **concepto de publicar** es inscribir un recurso compartido en el catálogo global del AD. Los permisos de los recursos publicados sólo se aplican cuando se accede a esos recursos a través del AD. Para publicar una carpeta compartida deberemos de ir a la consola de Usuarios y equipos del Directorio Activo, hacemos clic en *nuevo* y después *carpeta compartida*. Rellenamos la ruta que nos lleva a la carpeta.

Windows dispone la herramienta **Accesos efectivos** que permite solamente consultar los permisos o privilegios que tiene sobre un recurso dependiendo de los grupos a los que pertenece. Para ver los premisos efectivos NTFS:

1.- Buscar el recurso y seleccionar, dar al botón derecho de ratón y del menú dar en *Propiedades*, pulsar en la pestaña *Seguridad*, luego en *Opciones avanzadas*.

2.- Pulsamos en la pestaña *Accesos efectivos*. No podemos cambiar los permisos solo comprobar cuales tiene.

Autoevaluación

¿Qué estamos configurando al hacer clic en “Acceso efectivo” en el cuadro de “Seguridad avanzada pra un recurso compartido”?

- Permitimos publicar una carpeta compartida.
- Los nuevos archivos y subcarpetas que se crean en la carpeta heredan los permisos.
- No estamos configurando nada, simplemente podemos ver los permisos existentes.
- Asignamos quien es el propietario de un recurso compartido.

No es correcta porque para publicar son otros pasos.

No es correcta porque sin activar nada esta propiedad ya la tienen los recurso compartidos.

Muy bien, vas por buen camino.

No es correcta porque para asignar propiedad son otros pasos.

Solución

1. Incorrecto
2. Incorrecto
3. Opción correcta
4. Incorrecto

2.2.- Administración de permisos en Linux Ubuntu.

Debemos aclarar que en Linux podemos establecer permisos de recursos para una estructura en red de cliente-servidor permitiendo acceder mediante el protocolo de seguridad SSH al servidor Linux desde terminales Windows (aplicación Putty) o Linux; también podemos compartir recursos entre equipos Windows y Linux gracias al protocolo Samba (mediante un grupo de trabajo o dominio); y existe otro protocolo el NFS que permite montar recursos compartidos entre equipos Linux (Windows Server 2019 ya incorpora este protocolo para poder compartir con este sistema con equipos Linux).

Permisos en Linux

Permiso	Identifica
-	Sin permiso
r	Permiso de lectura
w	Permiso de escritura
x	Permiso de ejecución

El sistema Linux, de forma predeterminada, permite establecer sobre cada fichero o carpeta los siguientes permisos de acceso:

Lectura (r): Quien tiene este permiso sobre un archivo puede leerlo pero no modificarlo ni borrarlo. Si se trata de una carpeta podrá listar su contenido pero no podrá ver las características de los archivos o carpetas que contenga, como tampoco podrá borrarla o crear otras carpetas en su interior.

Escritura (w): Quien tiene este permiso puede modificar o incluso borrar el archivo. Si se trata de una carpeta podrá eliminarla o crear nuevas carpetas dentro de ella.

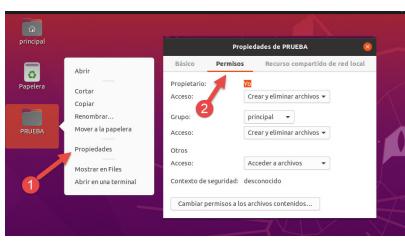
Ejecución (x): Si se trata de un fichero binario quien posea este permiso podrá ejecutarlo. Si se trata de una carpeta podrá ver su contenido y acceder también a las propiedades de los archivos o carpetas que contenga.

No asignado (-): según el orden (rwx) donde aparece un “-“ indica que no tiene asignado ese tipo de permiso.

El sistema establece permisos para el propietario, para uno de los grupos existentes, y para el resto de usuarios, utilizando una serie de bits cuyo contenido se interpreta según se muestra en la figura siguiente obtenida al ejecutar desde un terminal de comando la orden <i>ls -l</i>. Como norma, para cualquier agrupamiento de permisos **el sistema adopta por utilizar los más restrictivos**.



isoaliso (Elaboración propia)



Ubuntu (Elaboración propia)

Para **administrar los permisos desde el entorno gráfico** seleccionamos el recurso desde el explorador y pulsamos al botón derecho del ratón, seleccionamos del menú en *Propiedades*, pulsamos en la pestaña *Permisos*, seguidamente de la ventana completar cada uno de los campos según las posibilidades dadas en los valores de las listas desplegables y las restricciones a aplicar.

Otra forma de administrar permisos a ficheros y carpetas es desde la consola de entrada de comandos con la orden *chmod* (Podemos ver la ayuda del comando ejecutando *man chmod*). Este comando es similar al comando *cacls* de Windows que permite gestionar los permisos de las tablas ACLs de un recurso desde la línea de comandos.

Hay dos formatos posibles a usar *chmod*:

```
root@servidor:~# chmod [número_octal] nombre_fichero  
root@servidor:~# chmod [ugo][+/-][rwx] nombre_fichero
```

Donde [u=user, g=group y o=other]; [+/- activa o desactiva los atributos siguientes r=read, w=write, x=execute]

Ejemplos de uso del comando *chmod*, usando notación de octales, escribimos en el terminal:

```
chmod 754 archivo.txt
```

Donde:

7 5 4 representan individualmente los permisos para el usuario, grupo y otros, en ese orden. Cada dígito es una combinación de los números 4 , 2 , 1 y 0.

En el formato octal hay que tener en cuenta que:

Permiso	Valor
Lectura (r)	4
Escritura (w)	2
Ejecución (x)	1

Sin permiso	-
-------------	---

Ejemplos de permisos con notación octal

Permisos	Valor	Significado de los permisos
rwx	7	Lectura, escritura y ejecución
rw-	6	Lectura, escritura
r-x	5	Lectura y ejecución
r--	4	Lectura
-wx	3	Escritura y ejecución
-w-	2	Escritura
--x	1	Ejecución
---	0	Sin permisos

El mismo ejemplo anterior, pero escrito usando una notación de permisos simbólicos, escribimos en el terminal:

```
chmod u = rwx, g= rx, o = r archivo.txt
```

Donde:

u representa al usuario que le hemos asignado los permisos de lectura, escritura y ejecución.

g representa el grupo, que le hemos asignado los permisos de lectura y ejecución.

o representa otros, que le hemos asignado el permiso de lectura.

Ejemplos con equivalencias entre notación octal y simbólica

chmod u=rwx,g=rwx,o=rw	chmod 776
chmod u=rwx,g=rx,o=	chmod 750
chmod u=rw,g=r,o=r	chmod 644
chmod u=rw,g=r,o=	chmod 640
chmod u=rw,go=	chmod 600
chmod u=rwx,go=	chmod 700

Para saber más

Permisos de archivos y directorios

[Permisos de archivos y directorios](#)

En el siguiente enlace podrás completar el aprendizaje de gestionar permisos con la orden *chmod* de Linux.

[Administración de permisos dentro del sistema de ficheros con el comando chmod en Linux.](#)

¿Qué es el comando Chown en Linux y cómo usarlo?

[Comando Chown](#)

Debes conocer

Permisos en Linux con Chmod

[Permisos con chmod](#)

Comando chmod: ¿Qué es? y ¿Cómo usarlo?

[Comando Chmod](#)

Autoevaluación

El fichero fic1.txt. tiene los permisos 777, ejecutando sudo chmod 676 fic1.txt quitamos todos los permisos de escritura.

- Verdadero.
- Falso.

Repasa un poco el tema la orden correcta será sudo chmod 666 fic1.txt o sudo chmod a-x fic1.txt.

Muy bien vas por buen camino.

Solución

1. Incorrecto
2. Opción correcta

2.2.1.- Permisos adicionales en Linux.

Con referencia a las ACLs en Linux podemos decir que los comandos `chmod` y `chown` equivalen al comando `ca/cs` de Windows.

Cuando se utiliza la notación octal podemos aplicar unos permisos especiales aplicando los llamados bits de permanencia **SUID**, **SGID** y **sticky** que tienen las siguientes características:

El bit SUID o setuid: se aplica añadiendo o sumando 4000 a la representación octal del permiso del archivo o con “u+s” en notación textual, además debe tener permiso de ejecución para el propietario; esta operación producirá que se cambie la “x” del permiso del propietario por una “s”. Por ejemplo:

```
root@principal:~# chmod 4777 /home/principal/Escritorio/datos.txt
root@principal:~# ls -l /home/principal/Escritorio/datos.txt
-rwsrwxrwx 1 principal principal 5 Jun 9 10:57 datos.txt
```

El bit SUID generalmente se activa sobre un fichero ejecutable indicando que todo aquél que ejecute el archivo va a tener durante la ejecución los mismos privilegios que el propietario en el proceso creado.

El bit SGID o setgid: se aplica añadiendo 2000 a la representación octal del permiso del archivo “g+s” en notación textual, además debe tener permiso de ejecución para el grupo; esta operación producirá que se cambie la “x” del permiso del grupo por una “s”; el bit SGID activado sobre un directorio, fuerza a todos los archivos y subdirectorios creados en él a pertenecer al grupo del dueño del directorio y no al grupo del usuario que crea el archivo o subdirectorio, y sobre un fichero indica que todo usuario que ejecute un programa tendrá los privilegios del grupo al que pertenece el archivo. Por ejemplo:

```
root@principal:~# chmod 1777 /home/principal/Escritorio/datos.txt
root@principal:~# ls -l /home/principal/Escritorio/datos.txt
-rwxrwsrwx 1 principal principal 9 Jun 9 10:03 datos.txt
```

El bit stick: se aplica añadiendo 1000 a la representación octal del permiso del archivo o con “+t” en notación textual, además debe tener permiso de ejecución el resto de usuarios; esta operación producirá que se cambie la “x” del permiso de otros por una “t”, si no le hemos dado permiso de ejecución al archivo veremos una “t” indicando que no está activado. El bit stick en un directorio indica que independientemente de los permisos que tenga el directorio sólo el propietario y el administrador pueden borrar un archivo guardado en un directorio. Por ejemplo:

```
root@principal:~# chmod +t /home/principal/
root@principal:~# ls -l /home/principal/
drwxr-xr-t 13 principal 403 Jun 12 2011 principal
```

Es importante que el administrador impida la ejecución de archivos con el bit SUID activado en aquellos directorios en los que los usuarios tienen permiso de escritura. Si listamos los permisos relacionados con el fichero `shadow` podemos comprobar que son restrictivos (600 en octal, permiso de lectura para el propietario root), haciendo sumamente difícil que cualquier usuario que no sea root lo lea.

```
root@principal:~# ls -l /etc/shadow
-rw-r----- 1 root shadow 1964 jun 6 17:36 /etc/shadow
```

Para saber más

Permisos especiales en Linux: Sticky Bit, SUID y SGID

[Sticky Bit, SUID y SGID](#)

[Permisos en Linux: Sticky Bit, SUID y SGID](#)

Autoevaluación

¿Qué estamos permitiendo con la orden: chmod 4755 programa.sh?

- Que todos los usuarios puedan ejecutar el fichero programa.sh.
- Que solamente puede ejecutar el fichero programa.sh el propietario.
- Que solamente puede ejecutar el fichero programa.sh el grupo al que pertenece el usuario.
- Solamente el usuario propietario del fichero puede ejecutar el fichero programa.sh

Muy bien, vas por buen camino.

No es correcta, piensa que tiene asignado el bit setuid.

No es correcta, comprueba para que sirve el bit setuid.

No es correcta porque tiene asignado el bit setuid.

Solución

1. Opción correcta
2. Incorrecto
3. Incorrecto
4. Incorrecto

3.- Gestión de recursos compartidos vía Samba: El fichero smb.conf en Linux.

Caso práctico



Alain Bachellier (CC BY-NC-SA)

—Juan les explica a Noiba, Naroba y Jana que la red informática de “BK Sistemas Informáticos” reparte la compartición de recursos entre sus servidores.

—Juan, ¿tenéis aquí servidores Linux?

—Noiba, en nuestra empresa tenemos servidores Windows, pero también tenemos servidores Linux. Los servidores Linux se usan para descongestionar los accesos al servidor de Windows. Por ejemplo, el servicio de impresión compartido está gestionando y administrado en el servidor de Linux mediante el protocolo Samba, algunas aplicaciones realizan las copias de seguridad de sus bases de datos en un directorio compartido alojado en el servidor de Linux, etc.

—¿Usáis Samba para compartir los recursos entre los sistemas operativos Windows y Linux?.

—Efectivamente Naroba, es importante saber aprovechar las posibilidades que ofrece Samba a la hora de compartir recursos entre redes mixtas.

El protocolo predeterminado para compartir recursos en Windows es **SMB**, es el que hemos utilizado hasta ahora, basado en permisos **NTFS** y permisos de recurso compartido. Linux también utiliza Samba, recordemos que se puede administrar y configurar con entornos gráficos Linux (mediante el entorno de trabajo Webmin que permite la administración remota del sistema operativo de un servidor desde un navegador).

Ahora estudiaremos con más atención su fichero particular de **configuración smb.conf para conseguir que Linux actúe de servidor de archivos e impresión permitiendo compartir recursos para los otros ordenadores de la red**. Antes de comenzar la configuración deberemos saber que:

Hay que comprobar si tenemos instalado el servicio, desde un terminal de línea de comandos en Linux Ubuntu ejecutamos:

```
dpkg -s samba
```

Si no lo está procederemos a su instalación con la orden:

```
sudo aptitude install samba-client samba-common samba
```

Seguidamente realizaremos una copia de seguridad del fichero de configuración, para ello movemos el archivo de configuración smb.conf con otro nombre, por ejemplo **smb.conf.copia**:

```
sudo mv /etc/samba/smb.conf /etc/samba/smb.conf.copia
```

Para realizar cualquier modificación como usuario root debemos editar el fichero **<i>smb.conf</i>**, por ejemplo ejecutando:

```
sudo gedit /etc/samba/smb.conf
```

Es recomendable comprobar la integridad del fichero **smb.conf** después de su modificación ejecutando:

```
sudo /usr/bin/testparm
```

Deberemos recordar que siempre que cada vez que configuremos el servicio samba deberemos reiniciarle ejecutando:

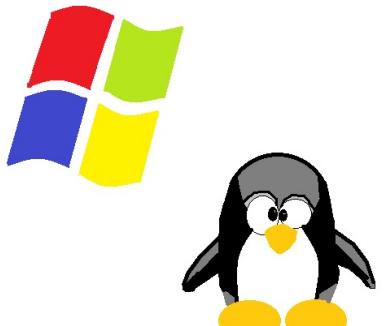
```
sudo systemctl restart smbd
```

Para que al iniciar el sistema Samba se arranque automáticamente, desde el directorio **/etc/init.d** ejecutamos la orden:

```
sudo update-rc.d samba defaults
```

Ya sabemos, de la unidad anterior, que será necesario añadir al sistema los usuarios samba mediante la orden:

```
sudo smbpasswd [opciones] nombre_usuario
```



Antonio López (Elaboración propia)

Samba también dispone de la posibilidad de configurar el sistema ACL utilizando el comando `smbcacls` que gestiona las ACL de Windows en archivos y directorios compartidos por el servidor Samba:

```
smbcacls / / servidor / share nombre de archivo [opciones]
```

Cuando accedemos desde un equipo cliente, por ejemplo Windows, a varios recursos compartidos por Samba **no se permiten las conexiones múltiples para un servidor o recurso compartido compatible por el mismo usuario, usando más de un nombre de usuario**, para solucionar el problema deberemos reiniciar sesión y volver a intentar acceder al siguiente recurso compartido.

Para evitar conflicto entre los permisos del sistema y los permisos del servicio Samba muchos administradores optan por ser más restrictivos a la hora de aplicar los permisos del sistema que en los permisos de recurso compartido por samba, de ésta forma serán efectivos para otros servicios como FTP, web, SSH, etc., instalados en el sistema.

Definir los recursos compartidos en el fichero smb.conf

Resumen de directivas comunes para recursos compartidos

Opción	Descripción
comment	Descripción que sirve para comentar el recurso.
path	Directorio o ruta donde se encuentra el recurso compartido.
browsable	Si ponemos "no", al listar los recursos compartidos, este no se verá en los exploradores de la red.
writable	Si lleva "yes" compartimos con permiso de acceso de escritura, es decir permite escribir en el recurso.
public	Con valor "no" un usuario invitado no puede acceder.
create mask	Permisos asignados a los ficheros que se crean dentro del recurso compartido.
directory mask	Permisos asignados a los directorios creados dentro del recurso compartido.
readonly	Con valor "yes" solamente se puede leer el contenido del recurso, si ya está writable no hace falta.
valid users	Usuarios validos para acceder al recurso.
write list	Lista de usuarios que pueden acceder con los permisos de lectura y escritura.

Ejemplo de configuración del fichero smb.conf supuesto práctico

La red dispone de cuatro ordenadores, tres con Windows profesional, y uno con Linux Ubuntu server que tiene el servicio Samba instalado. En un principio el entorno de red está estructurado formando un grupo trabajo. Deseamos que los usuarios "Carlos" y "Ana" puedan acceder a su directorio personal de Linux desde cualquier equipo. Que todos los usuarios del sistema puedan acceder a una carpeta llamada "Apuntes", con todos los permisos. Permitiremos acceder al recurso "Departamento" al grupo de usuarios "Profesores" con permiso de lectura, y al usuario "Carlos" para que además pueda leer y escribir.

Datos del entorno:

Nombre NetBIOS del servidor Linux: carlosserver
Nombre del grupo de trabajo (puede pasar a ser el nombre del dominio): DISTANCIA
Dirección de red: 192.168.1.0
Nombre de los equipos y direcciones IP: wind1 (192.168.1.20), wind2 (192.168.1.21), wind3 (192.168.1.22), carlosserver (192.168.1.23)
Usuario que pueden iniciar sesión: Carlos, Ana, Luis.

Comenzamos la configuración editando el fichero smb.conf y realizando la siguiente modificación:

```
# Sección global opciones de configuración que afectan a todo el servicio
[global]
# Nombre NetBIOS que hace referencia al servidor Samba Linux
netbios name = carlosserver
# Nombre del grupo de trabajo, si deseamos que sea PDC podremos el nombre del dominio
workgroup = DISTANCIA
# Información del servidor %v es variable predeterminada que guarda la versión Samba instalada
server string = servidor samba %v de recursos de red
# indica desde que ordenadores de la red se pueden acceder al servicio samba
# en nuestro caso todos de la red 192.168.1.0 menos el que tenga la dirección 192.168.1.22

host allow = localhost 192.168.1 EXCEPT 192.168.1.22

#dispositivo de red que comunica el servicio samba
interfaces = eth0
```

```

# Nivel de seguridad implementado que indica que cualquier usuario que se conecte a Samba debe tener
# una cuenta válida en el ordenador
security = user
# Deseamos passwords encriptados
encrypt passwords = yes
# directorio donde cada ordenador dispone de su fichero log donde se guarda información referente a todos los # accesos realizados, la variable
log file = /var/log/samba/ordenador.%m.log
# Path del archivo de passwords de samba
smb passwd file = /etc/smbpasswd
# Para no tener problemas de mayúsculas / minúsculas
case sensitive = no

# configuración del recurso compartido que representa al directorio personal de cada usuario
[home]

comment = directorios personales de cada usuario
#ya sabemos que Linux crea un directorio personal a cada usuario presentado por ejemplo para carlos será /home/carlos, la #variable predeterminada
path = /home/%U
browseable = no
writable = yes
public = no
## permisos para crear directorios y ficheros dentro del recurso, solamente el usuario propietario tendrán todos los permisos
create mask = 0700
directory mask = 0700
# especificamos que solamente se permite utilizar el servicio al usuario
valid users = %s

# Directorio compartido para todos los usuarios
[Apuntes]

comment = directorio publico
path = /home/apuntes
browseable = yes
writable = yes
public = yes
create mask = 0777
directory mask = 0777

#directorío compartido solamente para los usuarios de grupo identificado como profesores
[Departamento]

comment = material de profesores
path = /home/Departamento
readonly = yes
public = no
browseable = yes
#todos los usuarios del grupo Profesores pueden acceder al recurso, el + indica que se busque en las listas locales del servidor
valid users = +Profesores
#el usuario Carlos puede acceder con los permisos de lectura y escritura
write list = Carlos
#Fuerza siguiente permisos Linux sobre los directorios y ficheros creados

force create mode = 0770
force directory mode = 0770
#El propietario y grupo tiene todos los permisos sobre los directorios y ficheros creados
create mask = 0770
directory mask = 0770
#asigna al grupo Profesores como propietario por defecto en todas las conexiones
force group = Profesores
#asigna como propietario por defecto en todas las conexiones al usuario Carlos
force user = carlos

```

Terminada la configuración guardamos el archivo smb.conf.

Operaciones recomendadas

Si estamos interesados en mejorar la configuración o variar algún valor podemos consultar la ayuda con el comando:

```
man smb.conf
```

Comprobamos que la configuración no tiene errores tecleando el siguiente comando, y en el caso de que haya algún error, debemos revisar que hemos escrito todo correctamente:

```
testparm
```

Deberemos de crear los directorios o recurso a compartir y asignar los permisos Linux correspondientes, por ejemplo en nuestro caso para el directorio "Apuntes"

```
mkdir /home/Apuntes/  
chmod 0777 /home/Apuntes/
```

Hay que crear las cuentas de usuario samba, para ello previamente deben de ser usuarios Linux. Por ejemplo para el usuario Carlos:

```
adduser -s Carlos  
passwd Carlos  
smbpasswd -a Carlos
```

Comprobamos que todos los usuarios en su directorio personal solamente ellos disponen de todos los permisos, por ejemplo para Carlos:

```
chmod 0700 /home/Carlos/
```

Para que el sistema tenga en cuenta los cambios reiniciamos el servicio samba:

```
sudo systemctl restart smbd
```

Modificaciones para convertir el servidor de PDC

Si nuestro servidor pasa a ser controlador de dominio deberemos añadir las siguientes directivas en la sección global. Ademas tenemos que configuras la sección netlogon encargada de configurar el directorio compartido donde se almacenan los script o ficheros por lotes que se ejecutan cuando inicia sesión un usuario.

También es conveniente configurar los perfiles móviles de cada usuario para que cuando se conecta al dominio tenga un mismo escritorio y conserve siempre sus modificaciones aunque se conecte desde diferentes terminales, en nuestro caso configuraremos la sección perfiles que representará el directorio compartido donde se guardan los ficheros que almacenén los datos de los perfiles de cada usuario.

```
[global]  
  
#podremos el nombre del dominio  
workgroup = DISTANCIA  
# permite indicar que ordenadores de la red no están autorizados para acceder al servicio está  
host deny =  
# domain master debe ser yes, si tenemos activados los domain logons y el servidor actúa de PDC  
domain master = yes  
# el servidor controlara las peticiones de autentificación del dominio  
domain logons = yes  
  
# Este parámetro especifica el grupo de usuarios que tendrán permisos de administrador del dominio  
domain admin group = @Profesores  
#indicamos que el servidor es el responsable de recoger información de otros navegadores de la red  
local master = yes  
#nivel de preferencia de visualización entre servidores de la red, indicamos que es el maestro local  
os level = 64  
#forzamos a que al iniciar el servicio nmbd se convierta en el navegador maestro  
preferred master = yes  
#utilizamos la base de datos de Samba ubicada en /etc/samba/passdb.tdb para la autentificación  
passdb backend = tdbsam  
# con logon script = inicio.bat ejecuta un script con nombre inicio.bat común para todos los usuarios  
# con logon script = %U.bat ejecutamos un script de inicio particular para cada usuario ya que %U variable  
# interna que representa el nombre de usuario que ha iniciado sesión.  
#Tendremos que especificar el recurso compartido en la sección especial netlogon  
logon script = inicio.bat  
# Directorio donde se guardan los perfiles móviles de cada usuario la variable predeterminada samba %L  
# guarda el nombre NetBIOS del servidor y %U es el nombre de usuario que se conecta. Este directorio  
# debemos de configurar más adelante como sección de recurso compartido para que todos los usuarios  
# puedan acceder y escribir, la llamaremos profiles  
logon path = \\%L\profiles\%U  
# Este servidor actuará como un servidor WINS  
wins support = yes  
# Para poder ajustar o sincronizar la fecha y hora de los clientes con el servidor  
time server = yes  
# podemos indicar que se ejecuten los siguientes script cuando añadimos, borramos o cambiamos usuarios, grupos y cuentas de equipo en el el ser  
add user script = /usr/sbin/ useradd "%U" -n -g users  
add machine script = /usr/bin/useradd -n -c "Terminal (%U)" -d /nohome -s /bin/false "%U"  
  
[netlogon]  
  
comment = scripts de inicio para los usuarios  
path = /home/samba/netlogon  
read only = yes  
writable = no  
#permite a los usuarios accede a los scripts sin necesidad de autenticarse
```

```

guest ok = yes
# si estuviese a yes activaría el modo compartido al abrir el archivo, por seguridad esta a no
share mode = no
public = no
browseable = no

[profiles]

comment = directorios de perfiles
path = /home/samba/perfiles
browseable = no
writable = yes
public = no
create mask = 0600
directory mask = 0700

```

Opciones recomendadas

Si estamos interesados en mejorar la configuración o variar algún valor podemos consultar la ayuda con el comando:

```
man smb.conf
```

Comprobamos que la configuración no tiene errores tecleando el siguiente comando, y en el caso de que haya algún error, debemos revisar que hemos escrito todo correctamente:

```
testparm
```

Deberemos de crear los directorios o recurso a compartir y asignar los permisos Linux correspondientes, por ejemplo en nuestro caso para los directorios "netlogon" y "profiles"

```

mkdir /home/samba/netlogon/
chmod 0755 /home/samba/netlogon/
mkdir /home/samba/perfiles/
chmod 0777 /home/samba/perfiles/

```

Para crear un script de inicio de sesión, por ejemplo en nuestro caso, común para todos los usuarios llamado inicio.bat, que cuando se conecta se le crea la unidad "z:" de red al recurso compartido "Apuntes" deberemos de realizar los siguientes pasos:

Crearemos el fichero dentro del directorio /home/samba/netlogon:

```
gedit /home/samba/netlogon/inicio.bat
```

Contendrá las siguientes líneas típicas de un script de inicio de sesión para un dominio:

```

@echo off
Rem sincronizar la fecha y hora de los clientes con el servidor
net time \\carlosserver /set /yes
Rem creamos la unidad de red
net use z: \\carlosserver\home\Apuntes /persistent:no

```

Possiblemente deberemos de convertir el fichero a formato compatible para Windows. Para convertir entre los formatos debemos ejecutar el siguiente comando:

```
perl -p -i -e "s/\n/\r\n/g" inicio.bat
```

Además de crear las cuentas de usuario samba, como hemos hecho anteriormente, debemos de crear las cuentas de los hosts que se añadirán al controlador de dominio, por ejemplo en nuestro caso para el equipo "wind1", seguimos los siguientes pasos:
Creamos un grupo común para todas:

```
groupadd equiposdominio
```

Creamos la cuenta del equipo con los parámetros necesarios para que no puedan iniciar sesión:

```

adduser --force-badname -s /bin/false wind1$
adduser wind1$ equiposdominio
smbpasswd -a -m equipo1

```

Reiniciamos el servicio samba.

```
sudo systemctl restart smbd
```

Debes conocer

Instalar y configurar samba en Ubuntu 20.04

[Instalar y configurar samba](#)

Para saber más

Documentación oficial de Ubuntu para instalar y configura Samba en Ubuntu 20.04

[Instalar y configurar samba](#)

3.1.- Acceso a recursos compartidos con el servicio cliente de Samba: smbclient.

Ya sabemos que con la aplicación Samba smbclient, hemos accedido a recursos compartidos en máquinas Windows con los interfaces gráficos del propio explorador de Linux; para ello abrimos *Nautilus* (explorador de archivos de Linux), pinchamos en *Otras ubicaciones* (esta en el panel izquierdo), nos aparece un rectángulo que esta en la parte inferior y escribimos lo siguiente:

```
smb://192.168.1.120/
```

Donde 192.168.1.120 es la dirección IP del equipo al que nos vamos a conectar. Después pulsamos en el botón *Conectar*.

Existen distribuciones que al tener instalado samba, permitirán desde el propio explorador visualizar los recursos compartidos desde ordenadores Linux y Windows, para ello abrimos *Nautilus* (explorador de archivos de Linux), hacemos clic en *Otras ubicaciones->Red de Windows* aquí nos aparecen los grupos de trabajo que comparten los equipos Linux y Windows. Pinchamos encima del grupo de trabajo y dentro de él nos aparecerán los equipos que pertenecen a ese grupo de trabajo. Pinchamos sobre el equipo y nos aparecerán los recursos compartidos.

Para realizar una **conexión a una unidad de red desde la consola de comandos Linux** seguimos los siguientes pasos:

Instalamos el cliente Samba y la herramienta que nos permite montar directorios para el acceso a recursos por red.

```
root@server:~#apt-get install smbclient cifs-utils nfs-common
```

Crear un directorio donde montar el recurso, por ejemplo:

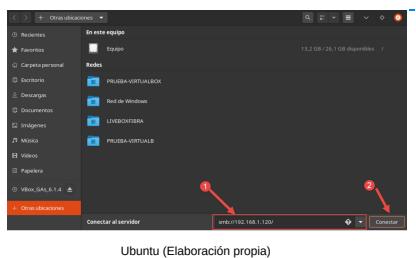
```
root@server:~#mkdir /mnt/prueba
```

Podemos hacer un listado de los recursos que dispone el ordenador que deseamos acceder, por ejemplo:

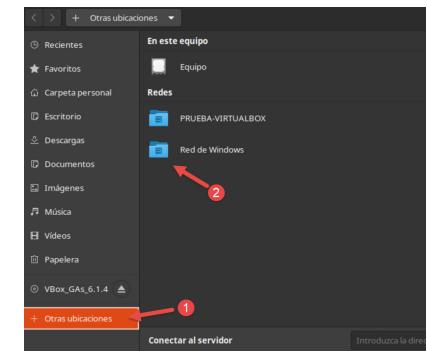
```
root@server:~#smbclient -L 192.168.1.174
```

Password:

Sharename	Type	Comment
Apuntes	Disk	Trabajos de distancia
Temas	Disk	



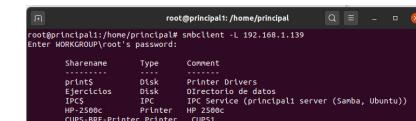
Ubuntu (Elaboración propia)



Ubuntu (Elaboración propia)

Ahora montamos el directorio compartido, con la orden **<i>smbmount</i>** o **mount -t smbfs**.

```
root@server:~# smbmount //192.168.1.174/Apuntes /mnt/carlos
```



Ubuntu (Elaboración propia)

También realizamos la misma tarea utilizando el comando:

```
mount -t smbfs -o guest //192.168.1.174 /Apuntes /mnt/carlos.
```

(dependiendo de la versión cuando se montan directorios de servidores Windows utilizaremos cifs en lugar del parámetro smbfs). Por ejemplo,

```
mount -t cifs -o guest //192.168.1.174 /Apuntes /mnt/carlos
```

Ahora podemos manejar los archivos del directorio compartido "Apuntes" ubicados en el ordenador 192.168.1.23, en nuestro ordenador desde la carpeta <i>/mnt/carlos</i>. Todos los cambios que realicemos afectaran de forma remota a la maquina que comparte. Ejecutando la orden <i>man smbmount</i> obtenemos una ayuda por pantalla sobre las opciones del formato.

Cuando ya no sea necesario utilizar esto se desmonta el directorio:

```
root@server:~# srmount /mnt/carlos
```

```
root@server:~#smbclient //EQU1/Apuntes -U Carlos  
  
added interface ip=192.168.1.174 bcast=192.168.1.255 nmask=255.255.255.0  
Password:  
Domain=[Distancia] OS=[Unix] Server=[Samba 3.2.1a]  
smb: >
```

Seguidamente el sistema solicitará que se le proporcione la clave de acceso del usuario "Carlos" para acceder al equipo "EQU1". Aparece el prompt de entrada de smb y ahora ya pueden utilizarse casi los mismos mandatos que en el intérprete del servicio FTP, como serían *ls*, *get*, *mget*, *put*, *del*, etc., para realizar operaciones con el contenido del recurso compartido. Para obtener ayuda sobre la forma de utilizar el comando ejecutamos la orden

```
root@principali:/home/principal# smbclient //192.168.1.139/Ejercicios -U ana  
Enter WORKGROUP/ana's password:  
Try 'help' to get a list of possible commands.  
smb: >?
```

Ubuntu (Elaboración propia)

```
man smbclient
```

Podemos automatizar el montaje de recursos compartidos mediante Samba añadiéndolos al fichero */etc/fstab* una línea teniendo en cuenta el siguiente formato:

```
//host_servidor/recurso_compartido /directorio_donde_montar smbfs username= < usuario >,password= < contraseña >.
```

Un ejemplo de ello podría ser la siguiente línea, donde nos pedirá contraseña ya que no la hemos especificado:

```
//192.168.1.174/Apuntes /mnt/carlos smbfs username=Ana
```

Compartir una impresora desde Linux

Utilizando la herramienta gráfica de impresión CUPS

Los sistemas operativos Linux en sus distribuciones tienen el servicio de impresión conocido como CUPS compatible con Windows. Cups puede trabajar con redes mixtas y puede adaptarse a Samba. Pincha [aquí](#) para ver la documentación oficial de CUPS. En muchas ocasiones necesitaremos usar Linux como servidor de impresión en una red Windows o compartir impresoras Windows en ordenadores Linux. Para ello seguimos los siguientes pasos como usuario root:

Instalamos CUPS:

```
sudo apt install cups
```

Una vez instalado, lo iniciamos y habilitamos con el inicio del sistema:

```
sudo systemctl start cups  
sudo systemctl enable cups
```

Ver el estado con el siguiente comando:

```
sudo systemctl status cups
```

Editamos el fichero de configuración Samba *smb.conf* y definimos un grupo de trabajo o dominio. Podemos restringir el acceso a ciertos equipos o usuarios para cada impresora; en nuestro ejemplo compartiremos las impresoras con cualquier sistema de red configurado. Podemos descomentar las líneas siguientes, si no encuentran se escriben en la sección global:

```
printing = cups  
printcap name = cups  
load printers = yes
```

También podemos añadir la sección:

```
[printers]  
comment = todas las impresoras  
printable = yes  
public = yes  
writable = no  
printing = cups  
printcap name = cups
```

Guardamos los cambios y reiniciamos samba.

```
sudo systemctl restart smbd
```

Pasaremos a entrar en la herramienta gráfica aportada por CUPS para gestionar impresora, para ello abrimos el navegador y en la barra de direcciones (URL) tecleamos <http://localhost:631>. (Puede que necesitemos abrir en el cortafuegos local los puertos 631 en UDP).

Para instalar una impresora compartida por Windows:

Nos pedirá autentificación como root si no estamos en sesión este usuario.

Para instalar una impresora compartida por Windows damos en Añadir Impresora, introducimos el nombre de la impresora desde el sistema Windows, luego indicamos la ubicación y una descripción.

Navegamos por el asistente hasta llegar a la pantalla de configuración del dispositivo, desplegamos la lista para seleccionar la opción Impresora en Windows vía Samba.

En el campo Dispositivo URI, de la siguiente pantalla, tecleamos la URL del dispositivo como:

```
smb://Usuario_Valido:contraseña@maquina_que_tiene_la_impresora_o_direccion_ip/nombre_impresora
```

Si la impresora está compartida desde un controlador de dominio tecleamos:

```
smb://Usuario_Valido:contraseña@DOMINIO/maquina_que_tiene_la_impresora_o_direccion_ip/nombre_impresora
```

Seleccionamos el driver de la impresora. Si da problemas para usar los drivers que le indicamos, podemos instalar los drivers ofertados por ejemplo por "foomatic", podemos ver la descripción de la impresora dentro del sistema CUPS, luego hacer un apt-get install del que se necesite.

Reiniciar las CUPS:

```
sudo systemctl restart cups
```

Realizamos una prueba de impresión.

Seguimos los siguientes pasos para instalar desde Windows una impresora compartida por Linux:

Después de conectar físicamente la impresora, instalamos los drivers de la impresora en el servidor, pulsamos en el botón Mostrar aplicaciones, en el panel de búsqueda escribimos *Impresoras* y pulsamos sobre *Impresoras*. En la pantalla de *impresoras*, pulsamos en el botón Configuración de impresora adicional... Se abre la ventana impresoras, pulsamos botón derecho encima de la impresora-propiedades, pinchamos en la opción Políticas, comprobamos que este marcada la opción Compartido, sino lo esta la marcamos.Opciones globales-Compartir impresora-Aceptar.

Comprobamos la dirección IP del servidor donde está conectada la impresora, podemos ejecutar desde la línea de comandos la orden ifconfig.

Abrimos el navegador y escribimos en la barra de direcciones <http://localhost:631>
Pulsamos en el botón Administrar servidor, activamos todas las opciones y pulsamos en Cambiar preferencias. Pide nombre y contraseña del usuario actual.
Reiniciar las CUPS:

```
sudo systemctl restart cups
```

Nos vamos al ordenador con Windows y entramos en el asistente de impresoras del Panel de control le damos a Añadir impresora, seleccionamos impresora en Red, e intentamos que realice la búsqueda automática, en el caso de que no la detecte, seguimos el asistente y en el cuadro Seleccionar una impresora compartida por nombre el nombre escribimos siendo nombre-impresora el nombre dado en el servidor de impresión:

http://*:631/printers/nombre_impresora

Añadir una impresora a un equipo Windows que está compartida e instalada en un ordenador Linux

Vamos al Panel de control-Hardware y sonido-Dispositivos e impresoras-Agregar una impresora, el sistema realiza una búsqueda para ver si encuentra la impresora, en caso contrario pulsamos en el enlace **La impresora que quiero no está en la lista**. En el siguiente cuadro de dialogo, marcamos la opción **Seleccionar una impresora compartida por nombre** y en el cuadro de texto introducimos la **URL** de nuestra impresora **compartida** utilizando la siguiente sintaxis: `http://IP_SistemaLinuxCUPS:631/printers/NombreImpresora`.

Donde:

IP_SistemaLinuxCUPS hace referencia a la IP de nuestro sistema Linux que está compartiendo mediante CUPS la impresora.
printers es una ruta por defecto donde cuelgan las impresoras que gestiona CUPS.

No olvidar el puerto por el que escucha CUPS: 631

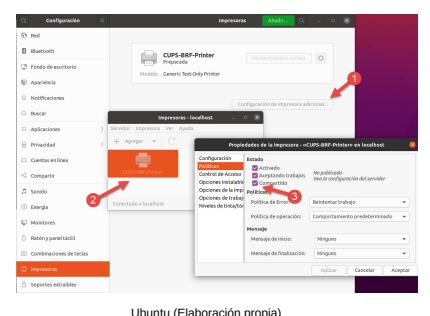
NombreImpresora debe coincidir con el nombre asignado en CUPS

Un ejemplo:

<http://192.168.122:631/printers/imprestdistancia>

Tras seleccionar **Siguiente**, aparecerá el siguiente cuadro de dialogo de Instalación de impresora de Windows.

Una vez conectada la impresora, tendremos que seleccionar el controlador de impresora. Puede que Windows ya disponga del controlador por lo que sólo tendremos que seleccionarlo de la lista.



Ubuntu (Elaboración propia)

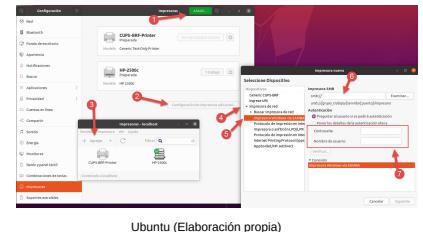
Pero si nuestro Windows no tiene el controlador de la impresora, tendremos que hacer clic en el botón Usar disco... y seleccionar la ruta donde esté ubicado el controlador de nuestra impresora.

Añadir una impresora a un equipo Linux que está compartida e instalada en un ordenador Windows

Desde Windows hay que de instalar y compartir la impresora (consulta [aquí](#) como compartir una impresora en Windows 10).

Desde el equipo Linux pulsamos en el botón *Mostrar aplicaciones*, en el cuadro de búsqueda escribimos *Impresoras*, hacemos clic en el resultado *Impresoras*. Pulsamos en *Configuración de impresora adicional*, se nos abre una ventana donde pulsamos en el botón *Añadir-
Impresora en Red-
Impresora Windows vía Samba*, escribimos el nombre o la dirección IP del ordenador, escribimos:

smb://IP_ordenador_Windows/nombre_de_la_impresora



Introducimos también el nombre del usuario y contraseña del ordenador Windows. Pulsamos en siguiente. Seguimos el asistente completando los campos que nos solicite, hasta terminar. Es conveniente imprimir una página de prueba.

Debes conocer

Cómo conectar Ubuntu a una red Windows para compartir carpetas

[Conectar desde Ubuntu a una carpeta compartida en Windows](#)

Compartir una impresora en Windows 10

[Compartir una impresora en Windows 10](#)

Para saber más

Montaje de la carpeta compartida en Windows y montada desde Linux

[Montaje de la carpeta compartida en Windows y montada desde Linux](#)

Cómo compartir una impresora en Ubuntu con CUPS

[Compartir una impresora desde Linux](#)

[Compartir una impresora en Ubuntu 20.04](#)

Instalar en Windows una impresora compartida en Linux con CUPS

[Instalar en Windows una impresora compartida en Linux con CUPS](#)

Agregar una impresora multifunción en Ubuntu 20.04

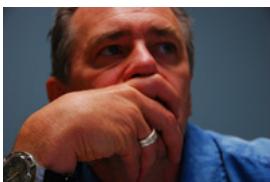
[Agregar una impresora multifunción en Ubuntu](#)

Montar una unidad de red con cifs smb

[Montar una unidad de red](#)

4.- Sistema de archivos NFS: Uso compartido NFS en Windows Server 2019.

Caso práctico



Let Ideas Compete (CC BY-NC-ND)

—Juan, ¿podríamos utilizar ordenadores Notebook para trabajar en cualquier oficina de la empresa?

—Félix, aprovechando la red WiFi instalada en la empresa, he realizado la compra de ordenadores Notebook que disponen en su preinstalación el sistema operativo Linux. Dichos dispositivos se están utilizando para facilitar la movilidad de los empleados por la empresa y para el acceso a los recursos compartidos utilizando los servicios ofrecidos por el protocolo NFS.

Además de Samba, el sistema estándar recomendado para compartir carpetas entre equipos Linux por red **es el sistema NFS**, por el cual un servidor gestiona la compartición de sus recursos, a los cuales accederán los usuarios desde otros ordenadores mediante la tarea de montar los recursos compartidos en un directorio del disco. Windows también dispone del protocolo NFS para compartir recursos con el fin de permitir su acceso a los usuarios basados en Linux.

Para poder usar permisos NFS en Windows Server 2019, primero hay que instalar el rol: Servidor para NFS. Para ello, seguimos los siguientes pasos:

Abrimos *Administrador del servidor-Agregar roles y características*, hacemos clic en siguiente.

Seleccionamos la opción *Instalación basada en características y roles*, pulsamos en siguiente.

Seleccionamos la opción *Seleccionar un servidor del grupo de servidores*, seleccionamos nuestro servidor y pulsamos en siguiente.

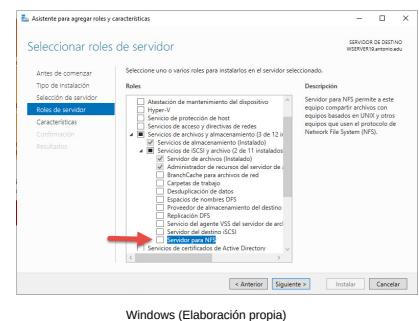
Expandimos la opción *Servicios de archivos y almacenamiento* y expandimos la opción *Servicios de archivos e iSCSI* y luego marcamos la casilla *Servidor para NFS*. Aparece una ventana emergente.

Pulsamos en Agregar característica y luego en siguiente.

Pulsamos en siguiente si no queremos añadir mas roles o características.

Nos aparece la pantalla de confirmación de los roles seleccionados. Pulsamos en la casilla *Reiniciar automáticamente el servidor de destino si es necesario* para que se reinicie el servidor automáticamente si es necesario y pulsamos en el botón instalar. Empieza el proceso de instalación.

Una vez terminada la instalación, pulsamos en el botón Cerrar, para salirnos del asistente.



Windows (Elaboración propia)

Configurar una carpeta compartida con NFS

Vamos a configurar una carpeta que exportaremos a los clientes. Para ello abriremos el *Administrador del servidor* y realizamos los siguientes pasos:

Creamos una carpeta con el nombre *Compartida* en la unidad C:.

Pinchamos en la opción *Servicios de archivos y de almacenamiento*. Hacemos clic en el **Tareas** y seleccionamos la opción **Nuevo recurso compartido**. Se abre un asistente que nos guiará durante el proceso.

En la primera página del asistente, seleccionamos el perfil para el recurso compartido. Seleccionamos la opción *Recurso compartido NFS-Rápido* y pulsamos en el botón siguiente.

Seleccionamos el servidor y la ruta del recurso compartido. Pulsamos en el botón siguiente.

Podemos cambiar el nombre del recurso si queremos y pulsamos en el botón siguiente.

Elegimos el método de autenticación que vamos a usar para compartir nuestro carpeta. En este caso vamos a usar *Sin autenticación de servidor* y vamos a marcar las opciones *Permitir el acceso de usuarios sin asignar* y *Permitir el acceso de usuarios sin asignar (por UID o GID)*. Pulsamos en el botón siguiente.

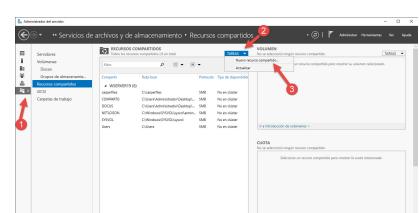
Pulsamos en el botón Agregar, para conceder permisos de acceso al recurso compartido NFS a un host, grupo de cliente o netgroup. En este caso vamos a dar permiso a un *Host*. Escribimos la dirección IP del equipo, seleccionamos el permiso *Lectura y escritura* y pulsamos en el botón Agregar.

En la pantalla siguiente podemos ver el *Host* (con su IP), que tiene permisos de Lectura y escritura. Pulsamos en el botón siguiente.

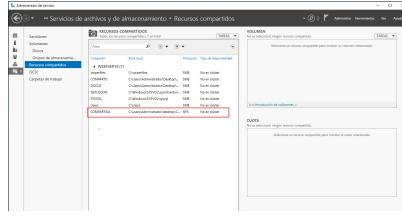
En la siguiente pantalla, podemos personalizar los permisos, pulsando en el botón Personalizar permisos. En este caso no es necesario, pulsamos en el botón siguiente.

La siguiente pantalla nos muestra las opciones seleccionadas, si estamos de acuerdo, pulsamos en el botón Crear.

El recurso compartido se crea correctamente. Pulsamos en el botón cerrar.



Windows (Elaboración propia)



Windows (Elaboración propia)

Dentro del administrador del servidor, en Recursos compartidos podemos ver nuestro recurso compartido NFS.

Configurar el cliente Windows 10 para acceder al recurso compartido en Windows Server

Para poder acceder desde nuestro cliente, tenemos que instalar y configurar el cliente NFS en nuestro cliente. Este ordenador puede ser un servidor o un cliente. Para instalar y configurar el cliente NFS en nuestro equipo con Windows 10, realizamos los siguientes pasos:

- Abrimos el Panel de control-Programas-Activar o desactivar las características de Windows .
- Buscamos la característica Servicios para NFS, pinchamos en el + para desplegar sus opciones.
- Seleccionamos las opciones *Servicios para NFS*, *Clientes para NFS* y *Herramientas administrativas*.
- Pulsamos en el botón Aceptar. Despues de un tiempo el cliente quedará instalado.

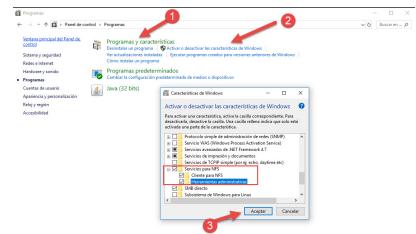
Montamos la unidad de red que le vamos a asignar al recurso que hemos compartido en el servidor.

Para montar la unidad abrimos el símbolo del sistema y escribimos el siguiente comando:

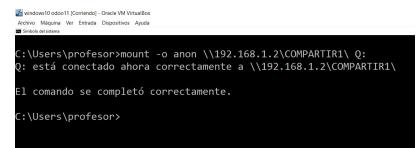
```
mount -o anon \\192.168.1.2\COMPARTIR1\ Q:
```

Donde:

- o anon** Para montar como un usuario anónimo.
- 192.168.1.2** Es la IP del servidor donde tenemos el recurso compartido.
- COMPARTIR1** Es la carpeta que estamos compartiendo.
- Q:** Es la unidad que le hemos asignado al recurso compartido.



Windows (Elaboración propia)



Windows (Elaboración propia)

Configurar un cliente en Linux para acceder al recurso compartido en Windows Server

Desde cualquier ordenador Linux de la red que deseemos acceder al recurso compartido en Windows Server deberemos de realizar la operación de montar el recurso, iremos a dicho equipo y como usuario root, instalamos la aplicación cliente <i>nfs-common</i> del servicio NFS con la siguiente orden:

```
root@prueba:~# aptitude install nfs-common
```

Es importante que creemos en el ordenador el mismo usuario que comparte el recurso en el servidor o que es propietario del recurso compartido. Seguidamente montamos el directorio, por ejemplo en la carpeta ya creada "/mnt/temporal", con la siguiente orden (192.168.1.2 es el equipo servidor NFS que comparte el recurso):

```
root@prueba:~# mount -t nfs 192.168.1.22:/COMPARTIR1 /mnt/temporal
```

Debes conocer

Instalar y configurar NFS en Windows Server

[NFS en Windows Server](#)

[Instalar y configurar un cliente NFS en Windows 10](#)

Para saber más

Para completar el aprendizaje sobre el servicio NFS en Windows Server 2019.

[Guía paso a paso de Servicios para NFS para Windows Server 2019.](#)

[Implementar el sistema de archivos de red](#)

Compartir archivos con NFS entre un servidor Ubuntu y un cliente Windows 10

[Compartir archivos entre un servidor NFS con Ubuntu y un cliente con Windows](#)

Autoevaluación

Con la orden “`mount -o anon //192.168.1.2/COMPARTIR1/ Q:`” podemos acceder al recurso COMPARTIR1 en un equipo con Windows 10.

- Verdadero.
- Falso.

No porque el separador de directorios en Windows es \.

Muy bien vas por buen camino.

Solución

1. Incorrecto
2. Opción correcta

4.1.- Gestión de recursos compartidos en Linux con NFS.

Como usuario root seguir los siguientes pasos para compartir recursos en Linux con NFS:

Deberemos tener instalado el paquete *nfs-kernel-server*, tanto en el ordenador cliente como en el servidor, con el gestor de paquetes de Synaptic o saliendo a un terminal (*CTRL+ALT+T*) y escribir:

```
root@prueba:~# apt-get install nfs-user-kernel
```

Después de la instalación el sistema ha creado los siguientes ficheros de configuración:

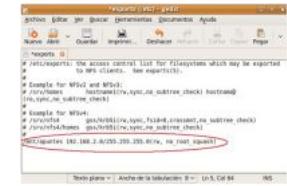
<i>/etc/init.d/nfs-user-kernel</i>: representa el script de inicio del servicio.

<i>/etc/exports</i>: contiene la lista de los sistemas de archivos NFS que se compartirán con los usuarios.

<i>/var/log/syslog</i>: contiene la lista de registros de las acciones realizadas al intentar las conexiones NFS sobre el servidor.

Cada vez que quiera compartir un directorio, se deberá añadir una línea al fichero <i>/etc/exports</i>, indicando la ruta del directorio a compartir y el equipo de la red que permitimos acceder a dicho recurso con una serie de opciones en la que podemos indicar los permisos. Por ejemplo, para compartir la carpeta creada "/mnt/Apuntes" para todos los equipos de la red 192.168.1.0 con permisos de lectura y escritura. Editamos el fichero:

```
root@principal:~# gedit /etc/export
```



Ubuntu (Elaboración propia)

Añadimos la siguiente línea (marcada en rojo en la imagen), que permite compartir la carpeta "/mnt/Apuntes", con el parámetro (*rw*) damos permisos de lectura y escritura, con <i>no_root_squash</i> no permitimos que el usuario *root* pueda acceder remotamente al recurso, si llegamos a poner (*ro*) damos permiso de lectura, con * indicamos que permitimos a todos, etc. Guardamos el fichero desde el menú Archivo-guardar.

Otro ejemplo:

Agregamos la siguiente línea en el fichero /etc/exports:

```
/home/principal/folder 192.168.1.139(rw,sync,no_root_squash,anonuid=1000,anongid=100)
```

Donde:

/home/principal/folder es la carpeta que será compartida por la red.

192.168.1.139 es la IP del cliente o clientes que accederán al recurso de red. Se muestra solo una IP estática pero podemos usar 192.168.01/24 que abarca desde la IP 192.168.9.1 hasta 192.168.0.254.



Ubuntu (Elaboración propia)

Las opciones de montaje están entre paréntesis.

rw: Es para permitir lectura y escritura.

sync: es opcional en caso de que queramos un poco mas de integridad de archivos y evitar la pérdida de datos, sacrificando un poco de rendimiento.

all_squash: degrada los permisos de los archivos creados desde el cliente al usuario nobody. Ejemplo: si en Windows 10 estoy como Administrador y creé un nuevo archivo, este pertenecerá al usuario nobody.

anonuid: El ID del usuario nobody, o en un caso específico el de cualquier usuario.

anongid: El ID del grupo del usuario nobody.

Estableceremos anonuid y anongid a 1000, que es el usuario dueño de la carpeta /home/principal/folder para conservar permisos de ejecución y escritura.

Los permisos de compartición por NFS no excluyen a los permisos del sistema Linux sino que **prevalecen los más restrictivos**. Por ejemplo, si una carpeta está compartida con permiso NFS de lectura y escritura pero en los permisos del sistema solo disponemos de permiso de lectura, no podremos escribir

Deberemos reiniciar el servicio NFS para que el sistema tenga en cuenta los cambios realizados, ejecutamos:

```
root@prueba:~# sudo service nfs-kernel-server restart
```

Desde cualquier ordenador Linux de la red que deseemos acceder al recurso compartido deberemos de realizar la operación de montar el recurso, iremos a dicho equipo y como usuario *root*, instalamos la aplicación cliente *nfs-common* del servicio NFS con la siguiente orden:

```
root@prueba:~# aptitude install nfs-common
```

Es importante que creamos en el ordenador el mismo usuario que comparte el recurso en el servidor o que es propietario del recurso compartido. Seguidamente montamos el directorio, por ejemplo en la carpeta ya creada "/mnt/temporal", con la siguiente orden (192.168.1.22 es el equipo servidor NFS que comparte el recurso):

```
root@prueba:~# mount -t nfs 192.168.1.22:/mnt/apuntes /mnt/temporal
```

En el segundo ejemplo, escribimos la orden:

```
root@prueba:~# mount -t nfs 192.168.1.19:/home/principal/folder /mnt/temporal
```

Debes conocer

Compartir archivos con NFS entre un servidor Ubuntu y un cliente Windows 10

[Compartir archivos con NFS entre un servidor Ubuntu y un cliente Windows 10](#)

Para saber más

Para completar el aprendizaje sobre el servicio NFS en Linux puedes consultar el siguiente enlace:

[Sistema de archivos NFS en Linux.](#)

Autoevaluación

¿Qué línea deberemos de añadir el fichero `/etc/exports` de un servidor NFS de Linux para compartir la carpeta `/home/antonio` con los permisos de escritura y lectura para que puedan acceder los equipos de la red `192.168.1.0/24`?

- /home/antonio +rw.
- export /home/antonio 192.168.1.* (rw).
- /home/antonio *(ro).
- /home/antonio 192.168.1.0/255.255.255.0 (rw).

No es correcta porque está mal el formato.

No es correcta porque no existe ese formato.

No es correcta porque no son correctos los permisos.

Muy bien, vas por buen camino.

Solución

1. Incorrecto
2. Incorrecto
3. Incorrecto
4. Opción correcta

5.- Derechos de usuarios y grupos: Políticas de seguridad.

Caso práctico



Alain Bachelier (CC BY-NC-SA)

—**Laro**, he analizado las necesidades que tienen cada usuario y grupo de usuarios a la hora de acceder al sistema, y ha creado unas directivas de grupo con el fin de controlar la seguridad en el acceso y uso de los equipos del dominio.

—**Juan**, ¿permitirá esto una mayor seguridad en el uso de los recursos?

—Naturalmente **Laro**, este agrupamiento de políticas de seguridad permitirá asegurar los recursos que ofrece el controlador de dominio Windows Server 2019 frente a posibles malos usos del sistema. Cada vez que se incorpora un usuario o equipo al dominio deberá volver a gestionar las directivas de seguridad de grupo.

La gestión de los derechos en el inicio de sesión de usuarios y grupos dentro de los sistemas operativos permiten la concesión o denegación de privilegios (políticas de seguridad) para la operatividad con el entorno de la computadora y de los servicios que disponga.

Los usuarios administradores serán los encargados de asignar derechos específicos a las cuentas de grupo o a cuentas de usuario individuales, con el fin de permitir a los usuarios el realizar tareas en el entorno del sistema, de esta manera podrán mantener un control en el uso y la seguridad en el acceso local y global. También servirá para evitar conflictos entre permisos a los servicios y recursos compartidos dentro de las estructuras de dominio, grupo de trabajo o cliente-servidor.

Mientras que los permisos se asignan a los objetos como carpetas, impresoras, archivos, etc., los derechos se aplican a las cuentas de usuario y cuentas de grupo de usuario que estará sometidos al protocolo de seguridad de la red en la que trabajan. Los sistemas disponen de herramientas que permiten la administración de los derechos de usuarios; en Windows estas políticas de seguridad de acceso al sistema y recursos se conocen como Directivas.



Antonio López (Elaboración propia)

5.1.- Directivas de seguridad en Windows.

Las directivas de seguridad son un conjunto de reglas de seguridad, referentes a características y permisos que se pueden configurar con el fin de garantizar el acceso a los recursos del sistema. En sistemas Windows la aplicación que resuelve su administración es gpedit.msc que se puede ejecutar desde un terminal de línea de comandos, y gestiona los permisos o privilegios y derechos, mediante una planificación de reglas a aplicar a las contraseñas, normas de acceso, etc.

isoaisal (Elaboración propia)

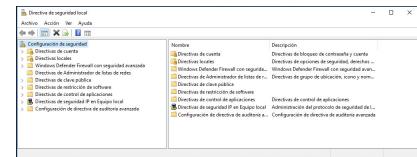
El sistema aporta desde la instalación unas directivas de seguridad predeterminadas, que son suficientes para la mayoría de las situaciones, las cuales se pueden clasificar en:

Directiva de seguridad local: se gestionan cuando el servidor no actúa de controlador de dominio. Para acceder a la gestión de estas directivas escribimos *Directivas de seguridad local* en el panel de búsqueda y hacemos clic en el resultado que aparece (el comando que se ejecuta para entrar en este modo es secpol.msc que se encuentra en %windir%\System32\secpol.msc).

Para gestionar una regla de directiva, se selecciona, clic en el botón derecho del ratón y pulsamos la opción *Propiedades* y de la ventana de asistente de configuración *Activar/desactivar* o completar los campos deseados. Permite establecer, entre otras cosas: **Política de cuentas, Directivas locales de auditoría del sistema y directivas de claves públicas.**

Directiva de seguridad de dominio y de seguridad de controlador de dominio: se administran cuando el servidor actúa de controlador de dominio, y se utiliza para gestionar los usuarios del dominio y los controladores de todo el dominio. Para acceder a la gestión de estas directivas iremos a *Inicio-Herramientas administrativas-Administración de directivas de grupo*.

Los administradores pueden agrupar, modificar o personalizar las directivas para que se ajuste a las necesidades específicas de la organización del sistema. **Las políticas o directivas de grupo pueden estar contenidas en cuatro tipos de objetos:**



Windows (Elaboración propia)

Equipos Locales o directiva de grupo local: son aplicadas únicamente en el equipo que las tiene asignadas independientemente del dominio al que pertenezcan. Son modificadas con "gpedit.msc". Estas son las únicas políticas que se aplican a los equipos que no están en un dominio, como servidores independientes (stand alone) o clientes en redes de igual a igual (peer to peer).

Sitios de Active Directory o directiva de sitio de grupo: se aplican para todos los equipos y/o usuarios de un sitio, independientemente del dominio del mismo bosque al que pertenezcan.

Dominios de Active Directory o directiva de grupo de dominio: se aplican a todos los equipos y/o usuarios de dominio.

Unidades Organizativas de Active Directory directiva de grupo de unidad organizativa: se aplican únicamente a los equipos y/o usuarios que pertenezcan a la propia unidad organizativa (OU).

Para saber más

Administrar la configuración de las directivas de seguridad en Windows

[Configuración de las directivas de seguridad en Windows 10](#)

[Configuración de las directivas de seguridad](#)

Debes conocer

Como usar el editor de directivas de grupo en Windows 10

[Editor de directivas de grupo en Windows](#)

Cómo usar el editor de directivas de grupo local (gpedit.msc) si tu Windows no lo trae

[Cómo usar el editor de directivas de grupo local si tu Windows no lo trae](#)

Cómo abrir las directivas de grupo local en Windows

[Abrir las directivas de grupo local](#)

Directivas de grupo en Windows Server

[Directivas de grupos locales, opciones de seguridad](#)

5.2.- Introducción a las directivas de grupo (GPO) en Windows.

La directiva de grupo es un conjunto de una o más políticas del sistema. Cada una de las políticas o reglas del sistema establece una configuración del objeto al que afecta. Gracias a las reglas de directiva de grupo podemos controlar los entornos de trabajo de los usuarios del dominio, los equipos y el comportamiento de los diferentes objetos y elementos que conforman la estructura del dominio en red.

Cuando se instala el AD se crean un conjunto de directivas de grupo predeterminadas y editables, los usuarios pasarán a ser usuarios del dominio y lo mismo ocurrirá con lo referente a la directiva de seguridad. Esto ocurre debido al modo en que la directiva de grupo se hereda mediante la estructura de AD.

Algunas de las características a considerar sobre las directivas de grupo son:



Windows (Elaboración propia)

Para la administración de la directiva de grupo podemos entrar en el editor de directiva complemento de Microsoft Management Console. Este complemento MMC se encuentra en la siguiente ubicación: %windir%\System32\gpedit.msc. Para **abrir el Editor de directivas de grupo local**, escribimos en el panel de búsqueda *Editor de directiva de grupo*, hacemos clic en el resultado que aparece, o pulsamos las teclas **WINDOWS+R** (*Ejecutar*) y escribimos *gpedit.msc*.

La herramienta de administración que gestiona las directivas de grupo en el interfaz gráfico en Windows Server 2019 es el llamado complemento de Administración de directivas de grupo y se accede desde *Inicio-Herramientas administrativas-Administración de directivas de grupo*.

En cada ordenador hay unos objetos de directiva grupo local (GPO) encontrada en el directorio *SystemRoot\System32\GroupPolicyUsers*. Además, en el controlador de dominio se encuentran los objetos de las directivas de grupo (GPO) de AD (tienen prioridad sobre las directivas locales) y se guardan en el directorio *Sysvol*.

Un dominio ya dispone de dos directivas predeterminadas Default Domain Policy y Default Domain Controllers formadas por un conjunto de reglas utilizadas para administrar distintas áreas.

La forma de trabajar con una directiva de grupo predeterminada consistirá en localizar la directiva deseada o una plantilla y habilitarla configurándola de un modo personalizado.

Las directivas se pueden heredar de contenedores padres (sitios, dominios o unidades organizativas) a contenedores hijos acumulándose con las que ya disponga. La herencia se puede bloquear para no recibir directivas de ningún otro dominio, sitio o unidad organizativa.

Las directivas pueden estar en estado de **no configurada, habilitada para usuarios y grupos o deshabilitada**, se encuentra configurada pero no se aplica a usuarios y grupos. También se pueden aplicar plantillas de GPO para facilitar la asignación de las mismas directivas a varios usuarios.

Debes conocer

Cómo crear y gestionar GPO en Windows Server 2019

[Crear y gestionar GPO en Windows Server 2019](#)

Cómo abrir el editor de directivas de grupo local

[Cómo abrir el editor de directivas de grupo local en Windows 10](#)

Cómo usar el editor de directivas de grupo local si tu Windows no lo trae

[Usar el editor de directivas de grupo local si tu Windows no lo trae](#)

Para saber más

Administrar la configuración de las directivas de seguridad

[Administrar la configuración de las directivas de seguridad](#)

Políticas de grupo en Windows Server

[Políticas de grupo \(GPO\) en Windows Server](#)

[Aplicar y denegar políticas de grupo \(GPO\)](#)

[GPO de contraseñas](#)

Autoevaluación

Gracias a las reglas de directiva de grupo podemos controlar los entornos de trabajo de los usuarios del dominio, indicar de las siguientes actuaciones, ¿cuáles pueden ser controladas por directivas en el sistema Windows?

- Activa o no los scripts que se ejecutan al inicio y final de sesión de equipo o usuario.

- Cambiar la actuación de los permisos de usuarios y grupos.

- Bloquear cuentas.

- Limitar las funcionalidades de los equipos.

[Mostrar retroalimentación](#)

Solución

1. Correcto
2. Correcto
3. Correcto
4. Correcto

Condiciones y términos de uso de los materiales

Materiales desarrollados inicialmente por el Ministerio de Educación, Cultura y Deporte y actualizados por el profesorado de la Junta de Andalucía bajo licencia Creative Commons BY-NC-SA.

Antes de cualquier uso leer detenidamente el siguiente [Aviso legal](#)

Historial de actualizaciones

Versión: 01.00.02	Fecha de actualización: 13/02/23
Actualización de materiales y correcciones menores.	
Versión: 01.00.00	Fecha de actualización: 23/07/20
Versión inicial de los materiales.	

