UBUNTU: GESTION DE USUARIOS, GRUPOS, PERMISOS Y MÁSCARA

Juan Carlos Navidad García

Sistemas Operativos en Red

1. **Define:**

   a. **ACL**

   Access Control List o lista de control de acceso. Lista de permisos adjuntos a un objeto que posibilitan realizar una gestión más avanzada de permisos de archivos y directorios, controlando el acceso a ellos.

   b. **Crontab**

   Crontab es un simple archivo de texto que guarda una lista de comandos a ejecutar en un tiempo especificado por el usuario.

   c. **GID**

   Es el identificador de un grupo

   d. **LDAP**

   Lightweight Directory Access Protocol. Protocolo a nivel de aplicación que permite realizar consultas sobre un servicio de directorio para poder buscar información.

e. LDIF

LDAP Data Interchange Format. Archivo de texto plano con un formato y sintaxis especial que se utiliza para configurar el servicio LDAP

f. Multiusuario

Un sistema multiusuario significa que puede ser compartido por varios usuarios al mismo tiempo.

g. NSCD

Name Service Cache Daemon. Es un demonio que proporciona una caché para la mayoría de las peticiones comunes del servicio de nombres.

h. NSS

Name Service Switch es un servicio que permite la resolución de nombres de usuario y contraseñas (o grupos) mediante el acceso a diferentes orígenes de información.

i. PAM

Pluggable Authentication Modules. Mecanismo de autenticación flexible que permite abstraer aplicaciones y otro software del proceso de identificación.

j. UID

Es el identificador de un usuario.

2. ¿Qué sucede al crear un usuario?

Al crear un usuario, se le asigna un UID, además se crea un grupo primario con un GID.

3. Clasifica los usuarios del sistema e indica:

a. Principales características

Usuario root

- Es la única cuenta de usuario con privilegios sobre todo el sistema.
- Acceso total a todos los archivos y directorios con independencia de propietarios y permisos.
- Controla la administración de cuentas de usuarios.
- Ejecuta tareas de mantenimiento del sistema.
- Puede detener el sistema.
- Instala software en el sistema.
- Puede modificar o reconfigurar el kernel, controladores, etc.

Usuario especial

- No tiene todos los privilegios del usuario root, pero dependiendo de la cuenta asumen distintos privilegios de root.
- Lo anterior para proteger al sistema de posibles formas de vulnerar la seguridad.
- No tienen contraseñas pues son cuentas que no están diseñadas para iniciar sesiones con ellas.

Usuario normal

- Cada usuario dispone de un directorio de trabajo, ubicado generalmente en /home.
- Cada usuario puede personalizar su entorno de trabajo.
- Tienen solo privilegios completos en su directorio de trabajo o HOME.
- Por seguridad, es siempre mejor trabajar como un usuario normal en vez del usuario root, y cuando se requiera hacer uso de comandos solo de root, utilizar el comando su.

b. Posible UID

Usuario Root: 0.

Usuario especial: entre el 1 y el 100.

Usuario normal: superior a 500, normalmente el 1000.

c. Promt

/bin/bash es la predeterminada en Ubuntu

d. Ruta de configuración de perfil

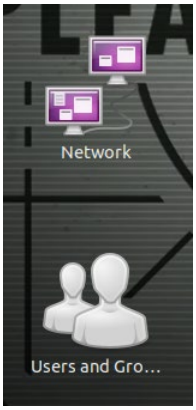
.bash_profile ocultos en **/home/<<usuario>>**

4. **Tareas de administración de usuarios y grupos**

   - Altas
   - Bajas
   - Modificaciones

5. **Instala el paquete gnome-system-tools para instalar la aplicación Users y Groups para poder crear usuarios en ubuntu mediante entorno gráfico**

```
jnav@jnav2:~$ sudo apt-get install gnome-system-tools
[sudo] contraseña para jnav:
Leyendo lista de paquetes... Hecho
```



6. **Indica los comandos para crear borrar y modificar usuarios y grupos mediante command line**

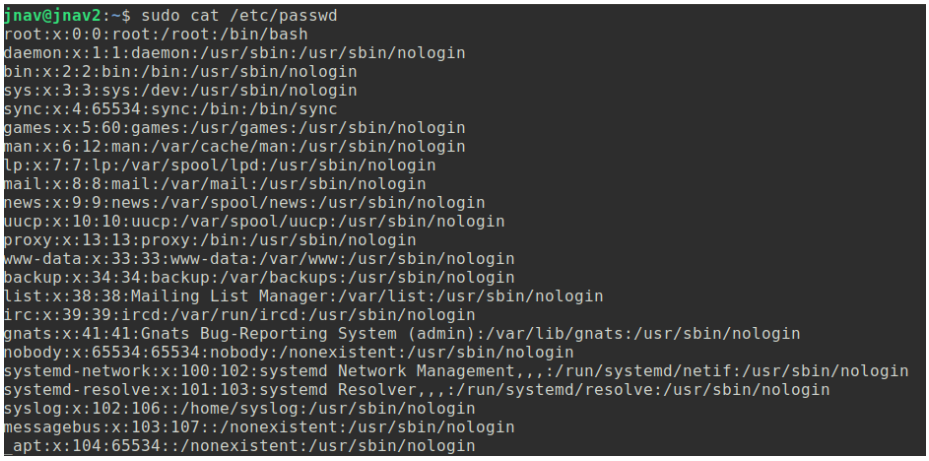
   Para crear usuarios **adduser**, para borrar **userdel** y para modificar **usermod**.

7. **Indica el comando para asignar una contraseña a un usuario sin contraseña**

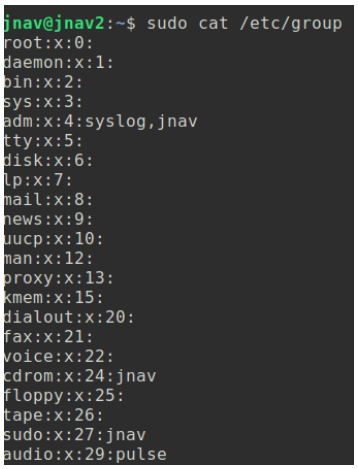
   passwd <<usuario>>

8. **Explica (indicando los campos) y visualiza los siguientes ficheros de configuración de usuarios y grupos:**

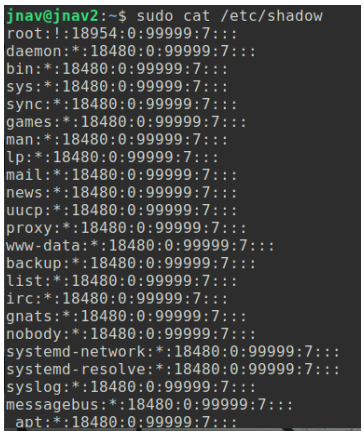
   a. **/etc/passwd:** El contenido de este fichero determina quien puede acceder al sistema de manera legitima y que se puede hacer una vez dentro del sistema. Es decir, contiene la información de todos los usuarios.



b. **/etc/group:** Contiene los nombres de los grupos y una lisa de los usuarios que pertenecen a cada grupo.



c. **/etc/shadow:** Contiene las contraseñas de los usuarios y información relacionada con la gestión de las contraseñas.



9. **¿Qué significa el asterisco en la clave del fichero etc/passwd?**

Significa que la cuenta no se puede utilizar para iniciar sesión.

10. Muestra todos los grupos del sistema

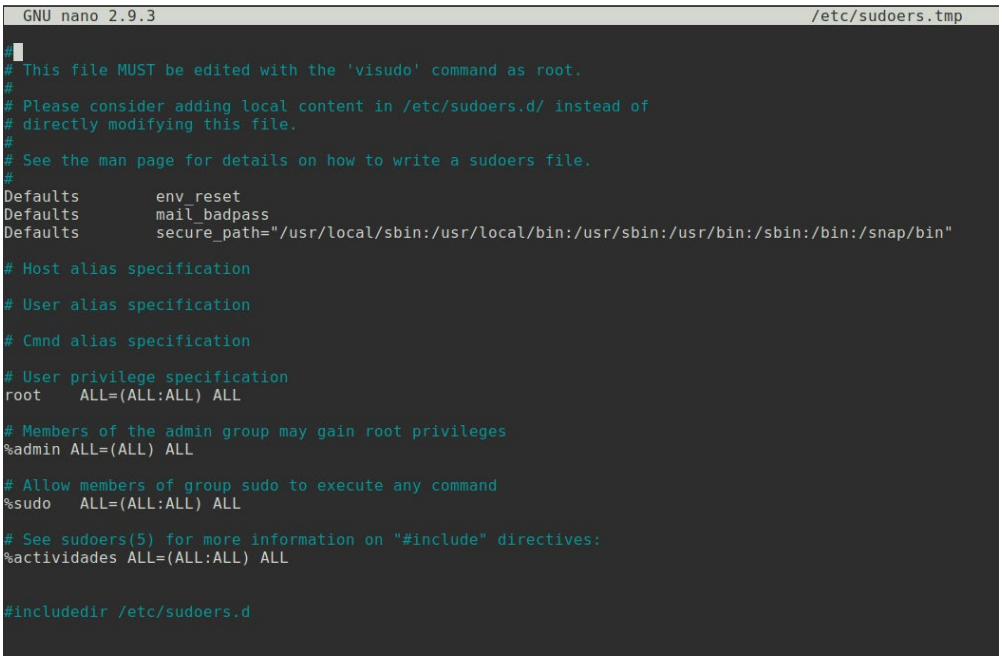
```
jnav@jnav2:~$ sudo cat /etc/group
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:syslog,jnav
tty:x:5:
disk:x:6:
lp:x:7:
mail:x:8:
news:x:9:
uucp:x:10:
man:x:12:
proxy:x:13:
kmem:x:15:
dialout:x:20:
fax:x:21:
voice:x:22:
cdrom:x:24:jnav
floppy:x:25:
tape:x:26:
sudo:x:27:jnav
audio:x:29:pulse
```

11. Crea un usuario sin privilegios y añádelo (utiliza visudo) al fichero /etc/sudoers con todos los privilegios.

He creado el usuario **Actividades**:

```
jnav@jnav2:~$ sudo adduser actividades
Añadiendo el usuario `actividades' ...
Añadiendo el nuevo grupo `actividades' (1002) ...
Añadiendo el nuevo usuario `actividades' (1001) con grupo `actividades' ...
Creando el directorio personal `/home/actividades' ...
Copiando los ficheros desde `/etc/skel' ...
Introduzca la nueva contraseña de UNIX:
Vuelva a escribir la nueva contraseña de UNIX:
passwd: contraseña actualizada correctamente
Cambiando la información de usuario para actividades
Introduzca el nuevo valor, o presione INTRO para el predeterminado
        Nombre completo []: Actividades
        Número de habitación []:
        Teléfono del trabajo []:
        Teléfono de casa []:
        Otro []:
¿Es correcta la información? [S/n] s
jnav@jnav2:~$
```

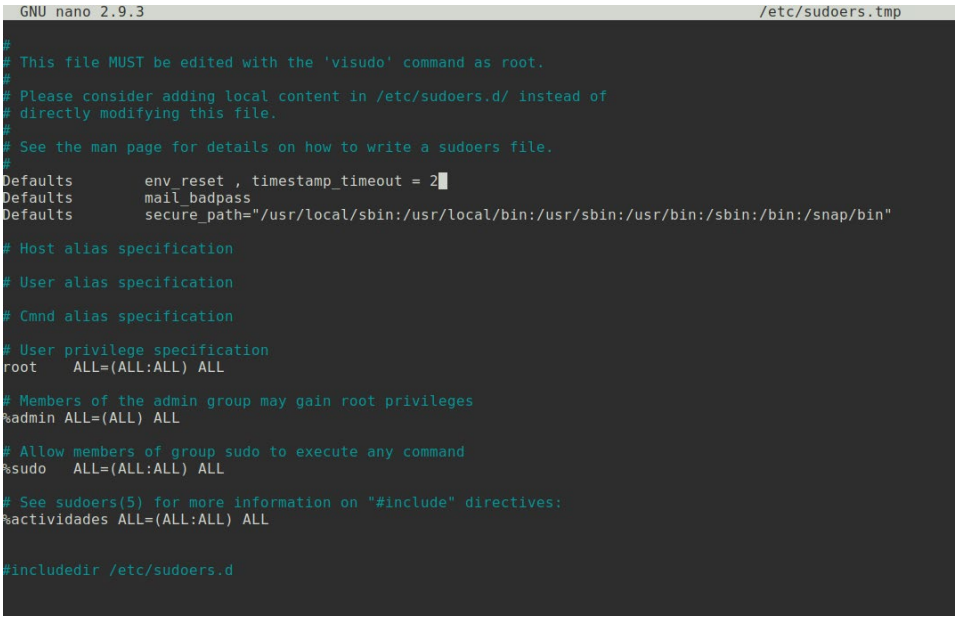
Con "**sudo visudo**" he modificado el archivo **sudoers** y he añadido al usuario Actividades con todos los privilegios.



12. ¿Como cambiarias el tiempo que ubuntu recuerda contraseñas?

Editamos el fichero **/etc/sudoers** en la línea **env_reset** y le añadimos:

Defaults env_reset , timestamp_timeout = 2



13. Realiza las siguientes actividades sobre usuarios y grupos:

a. Visualiza la información de todos los usuarios dados de alta en el sistema.

```
jnav@jnav2:~$ sudo cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106::/home/syslog:/usr/sbin/nologin
messagebus:x:103:107::/nonexistent:/usr/sbin/nologin
_apt:x:104:65534::/nonexistent:/usr/sbin/nologin
```

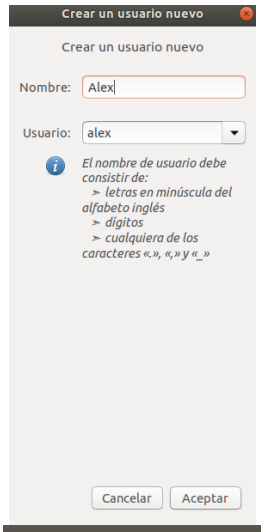
b. Visualiza la información de los grupos del sistema

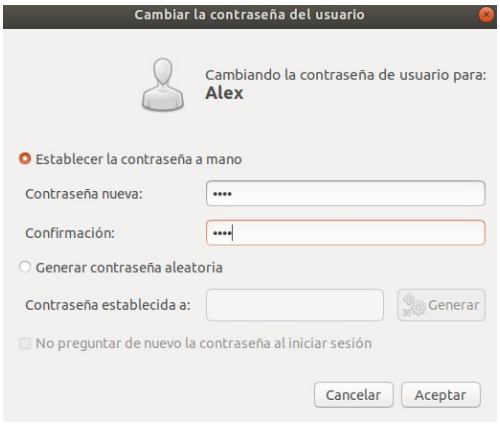
```
jnav@jnav2:~$ sudo cat /etc/group
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:syslog,jnav
tty:x:5:
disk:x:6:
lp:x:7:
mail:x:8:
news:x:9:
uucp:x:10:
man:x:12:
proxy:x:13:
kmem:x:15:
dialout:x:20:
fax:x:21:
voice:x:22:
cdrom:x:24:jnav
floppy:x:25:
tape:x:26:
sudo:x:27:jnav
audio:x:29:pulse
```

c. Visualiza la información de las contraseñas de los usuarios.

```
jnav@jnav2:~$ sudo cat /etc/shadow
root:!:18954:0:99999:7:::
daemon:*:18480:0:99999:7:::
bin:*:18480:0:99999:7:::
sys:*:18480:0:99999:7:::
sync:*:18480:0:99999:7:::
games:*:18480:0:99999:7:::
man:*:18480:0:99999:7:::
lp:*:18480:0:99999:7:::
mail:*:18480:0:99999:7:::
news:*:18480:0:99999:7:::
uucp:*:18480:0:99999:7:::
proxy:*:18480:0:99999:7:::
www-data:*:18480:0:99999:7:::
backup:*:18480:0:99999:7:::
list:*:18480:0:99999:7:::
irc:*:18480:0:99999:7:::
gnats:*:18480:0:99999:7:::
nobody:*:18480:0:99999:7:::
systemd-network:*:18480:0:99999:7:::
systemd-resolve:*:18480:0:99999:7:::
syslog:*:18480:0:99999:7:::
messagebus:*:18480:0:99999:7:::
_apt:*:18480:0:99999:7:::
```

d. Crea el usuario Alex desde el entorno gráfico.





e. Crea el usuario José desde la línea de comandos.

```
jnav@jnav2:~$ sudo adduser jose
Añadiendo el usuario `jose' ...
Añadiendo el nuevo grupo `jose' (1004) ...
Añadiendo el nuevo usuario `jose' (1003) con grupo `jose' ...
Creando el directorio personal `/home/jose' ...
Copiando los ficheros desde `/etc/skel' ...
Introduzca la nueva contraseña de UNIX:
Vuelva a escribir la nueva contraseña de UNIX:
passwd: contraseña actualizada correctamente
Cambiando la información de usuario para jose
Introduzca el nuevo valor, o presione INTRO para el predeterminado
        Nombre completo []: Jose
        Número de habitación []:
        Teléfono del trabajo []:
        Teléfono de casa []:
        Otro []:
¿Es correcta la información? [S/n] s
jnav@jnav2:~$
```

PERMISOS

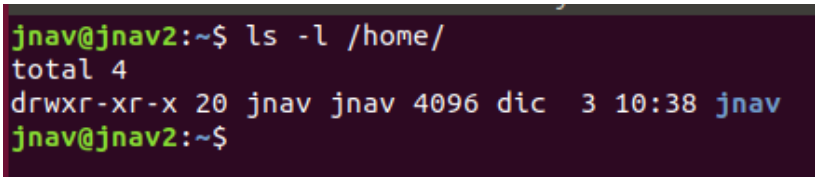
1. **¿Quién puede cambiar los permisos de un archivo?**

   Su creador o el root.

2. **Indica que permisos se pueden realizar sobre los ficheros y directorios. ¿son los mismos?**

   Sobre los ficheros se pueden realizar permisos de lectura, escritura y ejecución, en cambio en los directorios solo de lectura y escritura.

3. **Muestra en formato largo los ficheros y directorios de la carpeta home/usuario e interpreta su salida**



4. **¿Para que un usuario pueda acceder a un directorio que sería necesario además del permiso de lectura?**

   Permiso de ejecución.

5. **Completa el siguiente cuadro en el que se tienen los permisos originales, indica qué cambios se establecen, qué permiso final es el resultante y una breve descripción del cambio que se realiza.**

Actual	**chmod**	**Final**	**Descripción**
rw	a+x	rwx –-x --x	Le da permiso de ejecución a todos.
rwx —x —x	go-x	rwx --- ---	Le quita el permiso de ejecución al grupo.
rwx r-x r-x	u-x,go-r	rw- --x r-x	Le quita el permiso de ejecución al usuario y el permiso de lectura al grupo.
rwx rwx rwx	u-x,go-rwx	rw- --- ---	Le quita el permiso de ejecución al usuario y le quita todos los permisos al grupo.
r	a+rw,u+x	rwx rw- rw-	Le da a todos permisos de lectura y escritura y al usuario le da también permisos de ejecución.
rw- r— r--	u-r,g+w,o+x	-w- rw- r-o	Le quita permisos de lectura al usuario, le da permiso de escritura al grupo y permiso de ejecución a otros,

6. **A continuación, el cuadro se presenta en formato numérico y debes completar a qué permisos se refiere y su equivalente representación de permiso alfanumérico.**

Numérico	**Alfanumérico**	**rwxrwxrwx**	**Descripción**
654	U= r+w G= r+x O= r	rw- r-x r--	Usuario con permisos de lectura y escritura, grupo con lectura y ejecución y otros con lectura.
550	U= r+x G= r+x O= -	r-x r-x ---	Usuario con lectura y ejecución, grupo igual y otros no tiene permisos.
764	U= r+w+x G= r+w O= r	rwx rw- r--	El usuario tiene todos los permisos, grupos tiene lectura y escritura y otros solo lectura.
742	U= r+w+x G= r O= w	rwx r-- -w-	El usuario tiene todos los permisos, grupos tiene solo lectura y otros solo escritura.

7. **Crea un fichero denominado prueba.txt en tu home, analiza los permisos que tiene por defecto y, a continuación, agrega mediante notación alfanumérica un permiso de escritura a un grupo y otros. Agrega mediante notación numérica permisos de ejecución a todos. Comprueba los permisos de dicho fichero de nuevo.**

```
jnav@jnav2:~$ touch prueba.txt
jnav@jnav2:~$ chmod go+w prueba.txt
jnav@jnav2:~$ chmod +444 prueba.txt
-rwxrwxrwx 1 jnav jnav    0 dic  9 13:22 prueba.txt
```

8. **Crea un fichero denominado alumno.txt y, con una sola orden, asigna permisos de lectura ejecución a un usuario y grupo y deniega todos los permisos al resto de usuarios. Realiza la tarea en ambas notaciones**.

```
touch alumno.txt && chmod 550 alumno.txt
touch alumno.txt && chmod ug=rx,o-rwx alumno.txt
-r-xr-x--- 1 jnav jnav    0 dic  9 13:29 alumno.txt
```

1. **Uso de la máscara en los ficheros y directorios**

   La **máscara** son los permisos por defecto que se le asigna a un fichero o directorio nada más crearlo

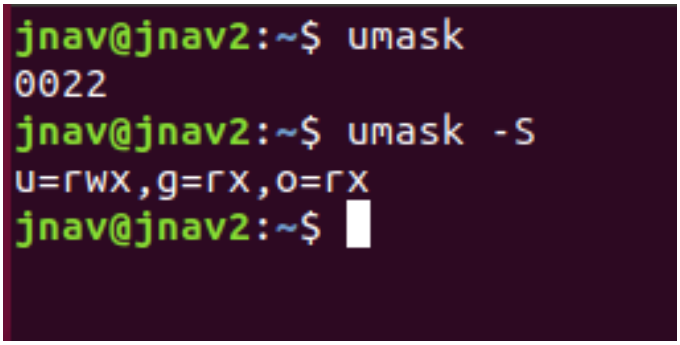
2. **Mascara de ficheros y directorios:**

   a. **Comando:** umask
   b. **Valores por defecto:** drw--w--w-
   c. **Valores máximos y mínimos:**

      Valor mínimo de UMASK para directorio: 000 y Máximo: 777

      Valor mínimo de UMASK para el archivo: 000 y máximo: 666

3. **Verifica el valor de la máscara en modo octal y simbolico y averigua con este dato los permisos tienen los directorios y ficheros al crearse.**

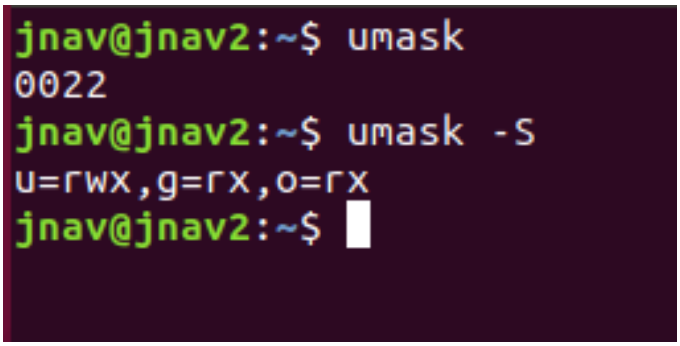


A los usuarios le da permisos completos, a los grupos le da solo de lectura y ejecución, pero no de escritura y a otros le da también permisos de ejecución y lectura.

4. **Es posible fijar permisos con umask a ficheros y directorios independientes.**

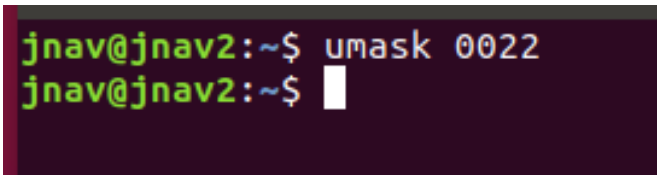
   Si, con el comando **umask** acompañado de los permisos en valor octal o simbólico y por último el fichero o directorio.

5. **Indica por defecto que permisos tienen los directorios y ficheros al crearse**



6. **¿Como modificarías de forma permanente los permisos de los directorios y ficheros de un usuario?**

   Con el comando **umask** acompañado del valor de los permisos en octal o simbólico.



7. Realiza las siguientes actividades sobre máscara:

a. Se desea que, para el usuario jose, los permisos por defecto para la creación de directorios sea 766 y la creación de ficheros sea 666.

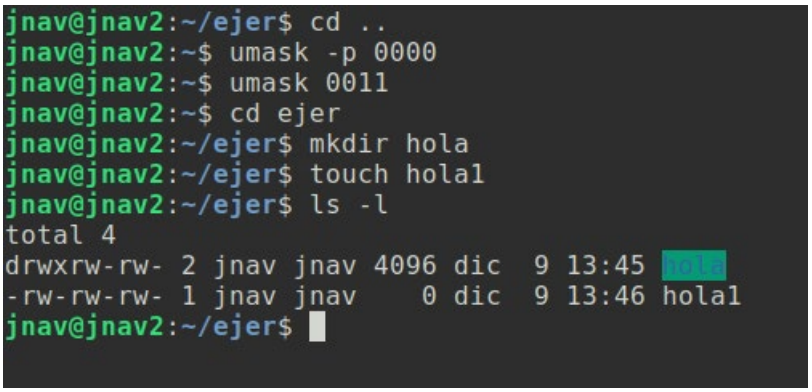
i. Calcula la máscara que se ha de aplicar.

La máscara que se ha de aplicar es 0011

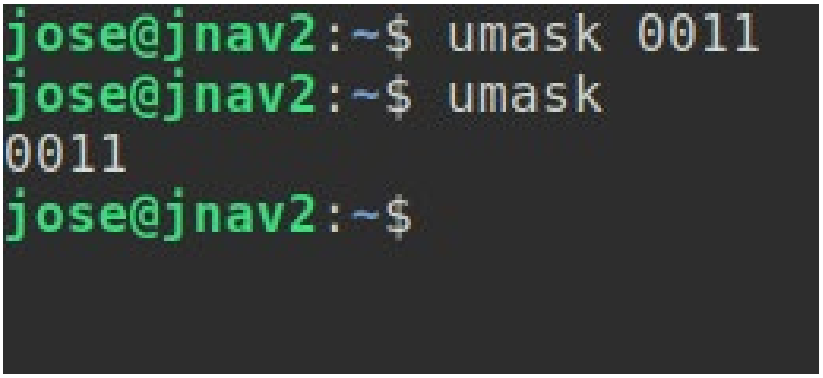
ii. Comando que aplica la máscara calculada

umask 0011 <<directorio>>

iii. Crea un fichero vacío y un directorio y muestra la salida del cómalo ls donde se pueda apreciar que los permisos por defecto son los deseados.



iv. Cuando se compruebe que la prueba realizada en el paso anterior es correcta, modifica el fichero correspondiente para dicha máscara que sea fija para el usuario jose.



1. **Diferencia en te chown y chgrp**

   El comando **chown** te permite cambiar el usuario propietario de un fichero o directorio. En cambio, el comando **dhgrp**, cambia el grupo propietario de un fichero o directorio.

2. **Analiza los siguientes comandos:**

   chown root fichero1: Hace que el root sea el nuevo propietario de fichero1.
   chown -R editorial directorio: Hace que editorial sea el nuevo propietario del directorio "directorio"

3. **En tu HOME, crea un fichero denominado sintexis.txt.**
   Muestra el listado largo de las características de dicho fichero y analiza su propiedad.

```
jnav@jnav2:~$ touch sintexis.txt
-rw-r--r-- 1 jnav jnav    0 dic  9 13:54 sintexis.txt
```

   El usuario tiene permisos de lectura y escritura, el grupo y otros solo tienen permisos de escritura.
   El usuario y el grupo propietario es jnav (mi usuario)

   Cámbialo para que el usuario propietario de dicho fichero sea el root.

```
jnav@jnav2:~$ sudo chown root sintexis.txt
-rw-r--r-- 1 root jnav    0 dic  9 13:54 sintexis.txt
```

1. **Que significa ACL. Cuál es su función**

   Access Control List o lista de control de acceso. Lista de permisos adjuntos a un objeto que posibilitan realizar una gestión más avanzada de permisos de archivos y directorios, controlando el acceso a ellos.

2. **¿Qué contine el fichero de configuración /etc/fstab? En que campo nos tendremos que fijar para verificar que el sistema de archivos se ha montado con ACL**

   El fichero fstab es el fichero que contiene los discos de arranque del sistema y especifica los dispositivos y particiones disponibles y dónde / cómo usar estas particiones. Este archivo se creará / actualizará durante la instalación del sistema.

3. **Muestra las particiones de tu sistema usando lsblk -l**

```
jnav@jnav2:~$ lsblk -l
NAME    MAJ:MIN RM   SIZE RO TYPE  MOUNTPOINT
loop0     7:0    0 247,9M  1 loop  /snap/gnome-3-38-2004/87
loop2     7:2    0   548K  1 loop  /snap/gnome-logs/106
loop3     7:3    0   2,5M  1 loop  /snap/gnome-calculator/884
loop4     7:4    0   219M  1 loop  /snap/gnome-3-34-1804/77
loop5     7:5    0   276K  1 loop  /snap/gnome-characters/550
loop6     7:6    0  42,2M  1 loop  /snap/snapd/14066
loop7     7:7    0  61,9M  1 loop  /snap/core20/1270
loop8     7:8    0   2,5M  1 loop  /snap/gnome-system-monitor/174
loop9     7:9    0  62,1M  1 loop  /snap/gtk-common-themes/1506
loop10    7:10   0  61,9M  1 loop  /snap/core20/1242
loop11    7:11   0     4K  1 loop  /snap/bare/5
loop12    7:12   0   2,2M  1 loop  /snap/gnome-system-monitor/148
loop13    7:13   0  55,3M  1 loop  /snap/core18/1885
loop14    7:14   0  55,5M  1 loop  /snap/core18/2253
loop15    7:15   0   704K  1 loop  /snap/gnome-characters/761
loop16    7:16   0  65,2M  1 loop  /snap/gtk-common-themes/1519
loop17    7:17   0   956K  1 loop  /snap/gnome-logs/100
loop18    7:18   0   2,4M  1 loop  /snap/gnome-calculator/748
loop19    7:19   0 255,6M  1 loop  /snap/gnome-3-34-1804/36
loop20    7:20   0  43,3M  1 loop  /snap/snapd/14295
sda       8:0    0    10G  0 disk
sda1      8:1    0    10G  0 part  /
sdb       8:16   0    10G  0 disk
sdb1      8:17   0    10G  0 part
sdc       8:32   0    10G  0 disk
sdc1      8:33   0    10G  0 part
sdd       8:48   0    10G  0 disk
sdd1      8:49   0    10G  0 part
sde       8:64   0    10G  0 disk
sde1      8:65   0    10G  0 part
md127     9:127  0    10G  0 raid1
md127     9:127  0    10G  0 raid1
sr0      11:0    1  58,3M  0 rom   /media/jnav/VBox_GAs_6.1.28
```

4. **Que significa UUID y muestra su valor para cada partición de tu sistema.**

   UUID son las siglas de Universally Unique IDentifier, que en inglés significa, literalmente, 'identificador único universal'. Y se utiliza para identificar discos y particiones del sistema.

```
jnav@jnav2:~$ blkid
/dev/sr0: UUID="2021-10-18-18-19-23-40" LABEL="VBox_GAs_6.1.28" TYPE="iso9660"
```

5. **Verifica que el sistema tiene instalado ACL**

   a. Accediendo a /etc/fstab

```
 GNU nano 2.9.3                                                    /etc/fstab

# /etc/fstab: static file system information.
#
# Use 'blkid' to print the universally unique identifier for a
# device; this may be used with UUID= as a more robust way to name devices
# that works even if disks are added and removed. See fstab(5).
#
# <file system> <mount point>   <type>  <options>       <dump>  <pass>
# / was on /dev/sda1 during installation
UUID=6511d4e5-aae5-40fa-ba82-ec984f047668 /               ext4    errors=remount-ro 0       1
/swapfile                                 none            swap    sw              0       0
```

   b. Usando el comando tune2fs

```
jnav@jnav2:~$ sudo tune2fs -l /dev/sda1 | grep "Default mount options:"
Default mount options:    user_xattr acl
jnav@jnav2:~$
```

6. **¿Como visualizar ACL de ficheros y directorios?**

   Con el comando getfacl <<fichero/directorio>>

7. **¿Como se establece ACL de ficheros y directorios?**

   Con el comando setfacl

8. Proporcionar ACL para un usuario individual

```
jnav@jnav2:~$ setfacl -m u:jnav:rwx prueba/
jnav@jnav2:~$ getfacl prueba/
# file: prueba/
# owner: jnav
# group: jnav
user::rwx
user:jnav:rwx
group::r-x
mask::rwx
other::r-x

jnav@jnav2:~$
```

9. Proporcionar ACL para todos los usuarios de un grupo

```
jnav@jnav2:~$ setfacl -m g:jnav:w prueba/
jnav@jnav2:~$ getfacl prueba/
# file: prueba/
# owner: jnav
# group: jnav
user::rwx
group::r-x
group:jnav:-w-
mask::rwx
other::r-x

jnav@jnav2:~$
```

10. Revocación de la LCA de un usuario o grupo

```
jnav@jnav2:~$ setfacl -x u:jnav,g:jnav prueba/
jnav@jnav2:~$ getfacl prueba/
# file: prueba/
# owner: jnav
# group: jnav
user::rwx
group::r-x
mask::r-x
other::r-x

jnav@jnav2:~$
```

11. Copiar ACL de un archivo / directorio a otro

```
jnav@jnav2:~$ getfacl prueba/ > acl.txt
jnav@jnav2:~$ mkdir prueba1
jnav@jnav2:~$ setfacl -M acl.txt prueba1/
jnav@jnav2:~$ getfacl prueba1/
# file: prueba1/
# owner: jnav
# group: jnav
user::rwx
group::r-x
group:jnav:-w-
mask::rwx
other::r-x

jnav@jnav2:~$
```

12. Realiza una copia de seguridad de ACL del directorio anterior y restaurarlo

```
jnav@jnav2:~$ getfacl -R prueba >> backup.acl
```

```
jnav@jnav2:~$ setfacl --restore=backup.acl
```

13. Realiza las siguientes actividades:

a. Autenticado como el usuario Alex, crea un fichero llamado aclALE.txt que contenga el texto Listas de acceso TUNOMBRE.

```
 GNU nano 2.9.3                    aclALE.txt                         Modificado

Listas de acceso Juan Carlos
```

b. Lista sus permisos de lista de acceso sobre ese fichero.

```
alex@jnav2:~$ ls -l
total 4
-rw-rw-r-- 1 alex alex 29 dic  9 18:40 aclALE.txt
alex@jnav2:~$
```

c. Trata de fijar como permisos de rw- para el usuario jose al fichero aclALE.txt.

```
alex@jnav2:~$ setfacl -m u:jose:rw aclALE.txt
alex@jnav2:~$ ls -l
total 4
-rw-rw-r--+ 1 alex alex 29 dic  9 18:40 aclALE.txt
```

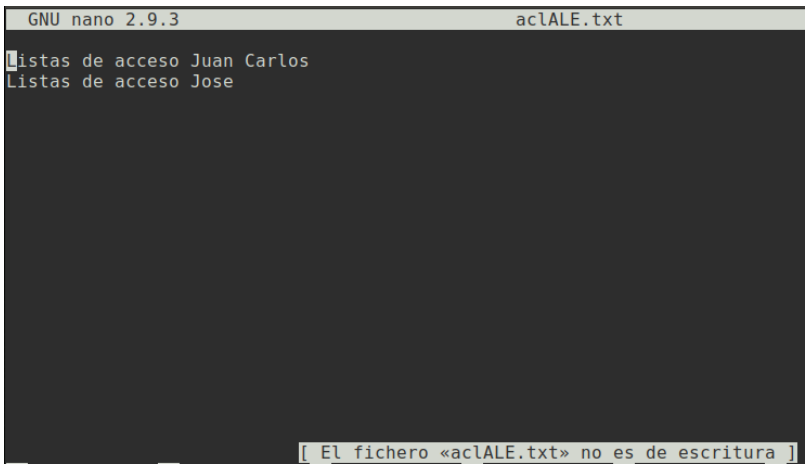
d. Lista los permisos normales mediante ls del archivo creado. Además, lista los permisos de la lista de acceso sobre el archivo, debe aparecer jose como usuario con permisos especiales.

```
alex@jnav2:~$ getfacl aclALE.txt
# file: aclALE.txt
# owner: alex
# group: alex
user::rw-
user:jose:rw-
group::rw-
mask::rw-
other::r--

alex@jnav2:~$
```

e. Autentícate como jose y comprueba si es posible escribir en el fichero aclALE.txt

```
jose@jnav2:/home/alex$ nano aclALE.txt
  GNU nano 2.9.3

Listas de acceso Juan Carlos
Listas de acceso Jose
```

f. Autentícate como tú y comprueba si puedes escribir o no en el fichero aclALE.txt. Justifica tu respuesta.
No le hemos dado permisos a otro usuario que no sea el propietario o Jose en la ACL.



g. Autentícate como alex. Crea un directorio dirTUNOMBRE y un fichero llamado fileTUNOMBRE.txt dentro de este.

```
alex@jnav2:~$ mkdir dirJuan
alex@jnav2:~$ cd dirJuan/
alex@jnav2:~/dirJuan$ touch fileJuan.txt
alex@jnav2:~/dirJuan$
```

h. Aplica sobre el directorio dirTUNOMBRE para que el grupo SOR tenga todos los permisos sobre él. Lista de nuevo mediante getfacl para ver que se ha realizado dicho cambio.

```
alex@jnav2:~$ setfacl -m g:SOR:rwx dirJuan/
alex@jnav2:~$ getfacl dirJuan/
# file: dirJuan/
# owner: alex
# group: alex
user::rwx
group::rwx
group:SOR:rwx
mask::rwx
other::r-x

alex@jnav2:~$
```

i. Realiza una copia de seguridad de la ACL del directorio dirTUNOMBRE que se llame backup.acl.

```
alex@jnav2:~$ getfacl -R dirJuan/ >> backup.acl
alex@jnav2:~$ ls
aclALE.txt  backup.acl  dirJuan
```

j. Borra la lista ACL aplicada sobre el directorio dirTUNOMBRE. Restaura la copia de seguridad de la ACL sobre el directorio dirTUNOMBRE.

```
alex@jnav2:~$ setfacl -x u:alex,g:SOR dirJuan/
alex@jnav2:~$ getfacl dirJuan/
# file: dirJuan/
# owner: alex
# group: alex
user::rwx
group::rwx
mask::rwx
other::r-x

alex@jnav2:~$
```

```
alex@jnav2:~$ setfacl --restore=backup.acl
alex@jnav2:~$ getfacl dirJuan/
# file: dirJuan/
# owner: alex
# group: alex
user::rwx
group::rwx
group:SOR:rwx
mask::rwx
other::r-x
```

14. Lleva a cabo las siguientes actividades:

a. Crea el usuario TUNOMBRE_AÑO con los siguientes datos: uid=1100; Shell=bash; comentario=usuario de prueba; Crea su home automáticamente. Asígnale una contraseña para completar la creación del usuario.

```
jnav@jnav2:~$ sudo useradd -m -u 1100 -s /bin/bash -c "usuario" juan2021
jnav@jnav2:~$ sudo passwd juan2021
Introduzca la nueva contraseña de UNIX:
Vuelva a escribir la nueva contraseña de UNIX:
passwd: contraseña actualizada correctamente
jnav@jnav2:~$
```

b. Cambia al usuario TUNOMBRE_AÑO sin modificar su entorno. Intenta crear un archivo llamado prueba.txt y describe lo que ocurre.

El archivo se crea con normalidad

```
jnav@jnav2:~$ su juan2021
Contraseña:
juan2021@jnav2:/home/jnav$ touch prueba.txt
juan2021@jnav2:/home/jnav$
```

c. Vuelve a tu usuario normal. Cambia al usuario TUNOMBRE_AÑO de manera que tome el entorno de trabajo propio.

d. Crea un archivo prueba.txt y toma evidencia del propietario.

```
juan2021@jnav2:~$ touch prueba.txt
juan2021@jnav2:~$ ls -l
total 0
-rw-rw-r-- 1 juan2021 juan2021 0 dic  9 19:15 prueba.txt
juan2021@jnav2:~$
```

e. Desde el usuario TUNOMBRE_AÑO, lanza sudo su e indica que ocurre. Realiza los cambios necesarios para que el usuario TUNOMBRE_AÑO pueda realizar tareas de administrador.

```
juan2021@jnav2:~$ sudo su
[sudo] contraseña para juan2021:
juan2021 no está en el archivo sudoers. Se informará de este incidente.
juan2021@jnav2:~$
```

```
 GNU nano 2.9.3                                                  /etc/sudoers.tmp

#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin"

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL

# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "#include" directives:
%juan2021 ALL=(ALL:ALL) ALL

#includedir /etc/sudoers.d
```

```
juan2021@jnav2:~$ sudo su
root@jnav2:/home/juan2021#
```

f. Fíjate en la directiva, haz los pasos necesarios para que, sin modificar nada en /etc/sudoers, permita al usuario Carmen que pueda realizar sudo.
#Members of the admin group may gain root privilleges
%admin ALL= (ALL) ALL.

```
jnav@jnav2:~$ sudo useradd -m -g adm carmen
jnav@jnav2:~$
```

g. Investiga y haz que tu usuario principal TUYO realice tareas de sudo sin que le pida la contraseña.

Añadimos la siguiente línea a /etc/sudoers

Ya no nos pediría contraseña: