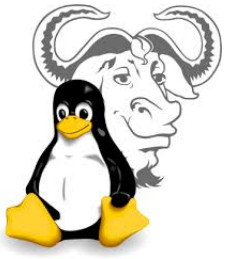
UNIVERSIDAD DE MENDOZA

FACULTAD DE INGENIERIA

SISTEMAS OPERATIVOS
GUÍA PRÁCTICA DE LABORATORIO Nº4

GNU-LINUX



Introducción.

En los sistemas operativos tipo POSIX cada elemento del sistema de archivos, como archivos, directorios, enlaces simbólicos, etc., tiene la característica de poseer permisos que lo ubican dentro del mismo. Éstos sirven como uno más de los niveles de seguridad del sistema operativo al impedir que cualquier usuario pueda leer, escribir, ejecutar o acceder a dichos archivos y
directorios de manera arbitraria. Estos permisos vistos de manera básica son: lectura (r, read),

escritura (w, write) y ejecución (x, execution) y se agrupan en bloques (rwx) para 3 diferentes clases (usuario, grupo y otros).

Los permisos de acceso de cada archivo y directorio del sistema son mostrados por un conjunto de 10 caracteres, los cuales proporcionan información acerca del tipo de elemento, junto con permisos para el usuario y grupo propietario para leer, escribir y ejecutar, como se muestra en el siguiente ejemplo:

-rwxr-xr-x 1 fulano fulano 0 jul 31 18:11 algo.txt

La asignación de permisos de acceso (de lectura, escritura y ejecución) pueden gestionarse a través de modos, los cuales consisten de combinaciones de números de tres dígitos —usuario, grupo y otros— que son manipulados a través de chmody setfacl.

Notación Simbólica:

El esquema de notación simbólica se compone de 10 caracteres, donde el primer carácter indica el tipo de archivo:

Valor	Descripción
-	Archivo regular.
d	Directorio.
b	Archivo especial como dispositivo de bloque.
c	Archivo de carácter especial
l	Enlace simbólico.
p	Tubería nombrada (FIFO)
s	Zócalo de dominio (socket)

Como se mencionó anteriormente, cada clase de permisos es representada por un conjunto de tres caracteres. El primer conjunto de caracteres representa la clase del usuario, el segundo conjunto de tres caracteres representa la clase del grupo y el tercer conjunto representa la clase de «otros» (resto del mundo). Cada uno de los tres caracteres representa permisos de lectura, escritura y ejecución, respectivamente y en ese orden.

Ejemplos:

Permisos	Descripción
drwxr-xr-x	Directorio con permiso 755
crw-rw-r--	Archivo de carácter especial con permiso 664.
srwxrwxr-x	Zócalo con permiso 775.
prw-rw-r--	Tubería (FIFO) con permiso 664.
-rw-r--r--	Archivo regular con permiso 644.

Notación Oral

La notación octal consiste de valores de tres a cuatro dígitos en base-8. Con la notación octal de tres dígitos cada número representa un componente diferente de permisos a establecer: clase de usuario, clase de grupo y clase de otros (resto del mundo) respectivamente. Cada uno de estos dígitos es la suma de sus bits que lo componen (en el sistema numeral binario). Como resultado, bits específicos se añaden a la suma conforme son representados por un numeral:

- El Bit de ejecución (acceso en el caso de directorios) añade 1a la suma.
- El bit de escritura añade 2a la suma
- El bit de lectura añade 4a la suma.

Estos valores nunca producen combinaciones ambiguas y cada una representa un conjunto de permisos específicos. De modo tal puede considerarse la siguiente tabla:

Valor	Permiso	Descripción
0	---	Nada
1	--x	Sólo ejecución de archivos o acceso a directorios
2	-w-	Sólo escritura
3	-wx	Escritura y ejecución de archivos o acceso a directorios
4	r--	Sólo lectura
5	r-x	Lectura y ejecución de archivos o acceso a directorios
6	rw-	Lectura y escritura
7	rwx	Lectura, escritura y ejecución de archivos o acceso a directorios

Cabe señalar que el permiso 3 (wx) es el resultado de 1+2 (w+x), que el permiso 5 (rx) es el resultado de 4+1 (r+x), que el permiso 6 (rw) es el resultado de 4+2 (r+w) y que el permiso 7 (rwx) es el resultado de 4+2+1 (r+w+x).

Máscara de Usuario

La máscara de usuario (umask, abreviatura de user mask) es una función que establece los permisos predeterminados para los nuevos archivos y directorios creados en el sistema. Puede establecerse en notación octal de tres o cuatro dígitos o bien en notación simbólica. Puede establecerse cualquier valor para umask, pero debe tomarse en consideración que ésta jamás permitirá crear nuevos archivos ejecutables.

Cuando se utiliza la notación octal de cuatro dígitos, el primer dígito siempre corresponde a los permisos especiales, pero el valor de éste siempre será 0; el segundo dígito corresponde a la máscara de la clase otros; el tercer dígito corresponde a la máscara para la clase de grupo; y el cuarto dígito corresponde a la máscara para la clase de usuario.

```
.----------- Permisos especiales (siempre es 0 en umask)
| .--------- Clase de otros
| | .------- Clase de grupo
| | | .----- Clase de usuario
| | | |
↓ ↓ ↓ ↓
0 0 2 2
```

El valor de la máscara de usuario, que se asigna ejecutando umask, corresponde a los bits contrarios del permiso predeterminado que se quiera asignar. Es decir, si por ejemplo se quiere asignar una máscara de usuario equivalente a 0775 (rwxrwxr-x), el valor de la máscara de usuario corresponderá a 0002 (el resultado de la operación 777 menos 775), que será lo mismo que definir u=rwx,g=rwx,o=rx.

Si por ejemplo se quiere asignar una máscara de usuario equivalente a 0744 (rwxr--r--), el valor de la máscara de usuario corresponderá a 0033 (el resultado de la operación 777 menos 744), que será lo mismo que definir u=rwx,g=r,o=r.

Los valores nunca producen combinaciones ambiguas y cada una representa un conjunto de permisos específicos. De modo tal puede considerarse la siguiente tabla:

Valor Octal	Valor Simbólico	Descripción
0	rwx	Lectura, escritura y acceso a directorios
1	rw-	Lectura y escritura
2	r-x	Lectura y acceso a directorios
3	r--	Sólo lectura
4	-wx	Escritura y acceso a directorios
5	-w-	Sólo escritura
6	--x	Sólo acceso a directorios
7	---	Nada

El valor predeterminado de la máscara de usuario del sistema en CentOS, Fedora™, Red Hat™ Enterprise Linux, openSUSE™ y SUSE™ Linux Enterprise es 0022, es decir se asigna permiso 0755 (-rwxr-xr-x) para nuevos directorios y 0644 (-rw-r--r--) para nuevos archivos. El sistema jamás permite crear nuevos archivos con atributos de ejecución. El valor predeterminado se define en una variable de entorno del archivo /etc/profile y puede ser cambiado por el que el administrador del sistema considere pertinente. El valor también puede establecerse por usuario en el archivo ~/.bash_profile (CentOS, Fedora™ y Red Hat™ Enterprise Linux) o bien en el archivo ~/.profile (openSUSE™ y SUSE™ Linux Enterprise).

El valor predeterminado de la máscara de usuario utilizado por useradd, para la creación de

directorios de inicio de usuarios, se define en el archivo /etc/login.defs.

En CentOS, Fedora™ y Red Hat™ Enterprise Linux el valor predeterminado de la máscara de usuario utilizada por useradd es 0077, es decir que los directorios de inicio de cada usuario que sea creado en el sistema tendrá un permiso 0700 (rwx------).

En openSUSE™ y SUSE™ Linux Enterprise el valor predeterminado de la máscara de usuario utilizada por useradd es 0022, es decir 0755 (rwxr-xr-x), debido a que la variable UMASK está deshabilitada con una almohadilla en el archivo /etc/login.defs, pues se recomienda se defina ésta variable en el archivo /etc/default/useradd. Ejemplo:

```
GROUP=100
HOME=/home
INACTIVE=-1
EXPIRE=
SHELL=/bin/bash
SKEL=/etc/skel
CREATE_MAIL_SPOOL=yes
UMASK=0077
```

Para determinar el valor en notación octal para la máscara de usuario predeterminada del sistema, ejecute umasksin opciones ni argumentos.

#umask

Para determinar el valor en notación simbólica para la máscara de usuario predeterminada del sistema, ejecute umaskcon la opción -S(mayúscula), sin argumentos.

#umask -S

Para cambiar la mascara de usuario en la sesión activa y procesos hijos, se requiere ejecutar umask con el valor octal deseado. En el siguiente ejemplo, se definirá 0002 (0775, rwxrwxr-x) como máscara de usuario:

#umask 0002

Lo anterior también se puede hacer utilizando notación simbólica:

#umask u=rwx,g=rwx,o=rx

Permisos Especiales

Hay una forma de cuatro dígitos. Bajo este esquema el estándar de tres dígitos descrito arriba se convierte en los últimos tres dígitos del conjunto. El primer dígito representa el bit de los permisos adicionales. En sistemas y equipamiento lógico donde es obligatorio incluir este primer dígito del conjunto de cuatro y se prescinde de asignar permisos adicionales, se debe establecer cero como valor de éste. Ejemplo:

$chmod 0755 /lo/que/sea

El primer dígito del conjunto de cuatro es también la suma de sus bits que le componen:

- El bit pegajoso(sticky bit) añade 1al total de la suma.
- El bit setgidañade 2al total de la suma.
- El bit setuidañade 4al total de la suma.

El permiso SUID o bit setuid hace que cuando se ha establecido ejecución, el proceso resultante asumirá la identidad del usuario dado en la clase de usuario (propietario del elemento).

El permiso SGID o bit setgid hace que cuando se ha establecido ejecución, el proceso resultante asumirá la identidad del grupo dado en la clase de grupo (propietario del elemento). Cuando setgid ha sido aplicado a un directorio, todos los nuevos archivos creados debajo de este directorio heredarán el grupo propietario de este mismo directorio. Cuando se omite establecer setgid, el comportamiento predeterminado es asignar el mismo grupo del usuario utilizado para crear nuevos archivos o directorios.

El bit pegajoso (sticky bit) significa que un usuario sólo podrá modificar y eliminar archivos y directorios subordinados dentro de un directorio que le pertenezca. En ausencia de éste, se aplican las reglas generales y el derecho de acceso de escritura en si sólo permite al usuario crear, modificar y eliminar archivos y directorios subordinados dentro de un directorio. Los directorios a los cuales se les ha establecido bit pegajoso restringen las modificaciones de los usuarios a sólo adjuntar contenido, manteniendo control total sobre sus propios archivos y permitiendo crear nuevos archivos; sólo permitirá adjuntar o añadir contenido a los archivos de otros usuarios. El bit pegajosoes utilizado en directorios como /tmpy /var/spool/mail.

De modo tal puede considerarse la siguiente tabla:

Valor	Permiso	Descripción
1	--- --- --t	bit pegajoso
2	--- --s ---	bit setgid
3	--- --s --t	bit pegajoso + bit setgid
4	--s --- ---	bit setuid
5	--s --- --t	bit setuid + bit pegajoso
6	--s --s ---	bit setuid + bit setgid
7	--s --s --t	bit setuid + bit set gid + bit pegajoso

Cuando un archivo carece de permisos de ejecución o bien si un directorio carece de permiso de acceso en alguna de las clases y se le es asignado un permiso especial, éste se representa con una letra mayúscula.

Permiso	Clase	Ejecuta	Sin ejecución
setuid	Usuario	s	S
setgid	Grupo	s	S
pegajoso (sticky)	Otros	t	T

Ejemplos:

Ejemplo de Permisos Regulares

Valor Octal	Valor Umask	Clase de Usr	Clase Grupo	Clase Otros
0400	0377	r--	---	---
0440	0337	r--	r--	---
0444	0333	r--	r--	r--
0500	0277	r-x	---	---
0550	0227	r-x	r-x	---
0555	0222	r-x	r-x	r-x
0644	0133	rw-	r--	r--
0664	0113	rw-	rw-	r--
0666	0111	rw-	rw-	rw-

0700	0077	rwx	---	---
0711	066	rwx	--x	--x
0707	0070	rwx	---	rwx
0744	0033	rwx	r--	r--
0750	0027	rwx	r-x	---
0755	0022	rwx	r-x	r-x
0775	0002	rwx	rwx	r-x
0777	0000	rwx	rwx	rwx

Ejemplos de Permisos Especiales.

Valor Octal	Clase de Usuario	Clase de grupo	Clase de Otros
1644	rw-	r--	r-T
2644	rw-	r-S	r--
3644	rw-	r-S	r-T
4644	rwS	r--	r--
5644	rwS	r--	r-T
6644	rwS	r-S	r--
7644	rwS	r-S	r-T
1777	rwx	rwx	rwt
2755	rwx	r-s	r-x
3755	rwx	r-s	r-t
4755	rws	r-x	r-x
5755	rws	r-x	r-t
6755	rws	r-s	r-x
7755	rws	r-s	r-t

Utilización de chmod

Sintaxis básica:

$chmod [opciones] modo archivo

Opciones de chmod:

-R: Cambia permisos de forma descendente en un directorio dado. Es la única opción de los estándares POSIX.
-c: Muestra cuáles archivos han cambiado recientemente en una ubicación dada
-f: Omite mostrar errores de archivos o directorios que haya sido imposible cambiar
-v: Descripción detallada de los mensajes generados por el proceso

Para obtener una descripción completa del uso de chmod, ejecute:

$man 1 chmod

Uso de chmod y los enlaces simbólicos:

Cabe señalar que aunque es posible cambiar el propietario y/o grupo al cual pertenece un enlace simbólico con chowny chgrp, chmod jamás cambia los permisos de acceso de enlaces simbólicos, los cuales de cualquier forma carecen de relevancia pues los que importan son los permisos de los archivos o directorios hacia los cuales apuntan. Si ejecuta chmod sobre un enlace simbólico, invariablemente cambiará el permiso del archivo o directorio hacia el cual apunta. Cuando se aplica chmod de forma descendente en un directorio, éste ignora los enlaces simbólicos que pudiera encontrar en el recorrido.