Preparación para el examen LPI 101

Tema 104.5

Usando permisos para controlar el acceso a los ficheros

Créditos y licencia de uso

Coordinación:
Manuel Guillán (xLekOx) lpi@xlekox.org

Traducción:
Ivan Servia (katas) ivanservia@hotmail.com

Maquetación y corrección:
Manuel Guillán (xLekOx) lpi@xlekox.org
Javier Pulido (jpulido) javier.pulido@wanadoo.es
(el_condor) el_condor@spymac.com

Versión 1.1 (23-01-2005 15:00)

ÍNDICE

Índice de contenido

Introducción

En este capítulo se verá como controlar los accesos a los ficheros y directorios por medio de los permisos. También se hablará de bits especiales como el suid, sgid y sticky bit y usar persmisos para grupos.

Los comandos que se verán en este tema son:

chmod
umask

Este tema tiene un peso (importancia) de 5 de cara al examen final de la certificación LPI 101. El total de la suma de pesos de todos los temas es de 106.

Permisos de Archivos y Directorios

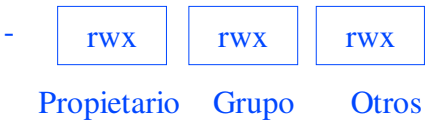
Los permisos determinan quién puede acceder a los archivos y directorios dependiendo del tipo de acceso que tengan. Los primeros 10 caracteres de un listado ls -l de cualquier entidad se parecen a lo siguiente:

-rwxrwxrwx

El primer carácter se identifica con el tipo de entidad: - para un archivo estándar, d para un directorio, b para un grupo de recursos (tales como una unidad de cinta), c para un carácter del recurso, l para un link, o p para una tubería (pipe). El resto de los nueve caracteres se dividen en 3 grupos, como se indica en la Figura 8.1.

Cuando un usuario intenta acceder a un archivo, el primer control confirma si el es el propietario del archivo. Si lo es, se le aplica el primer tipo de permisos. Si no lo es, el segundo control confirma si es un miembro del grupo propietario del archivo. Si es un miembro del grupo, se le aplica el tipo intermedio de permisos. Si no es propietario del archivo, y no es miembro del grupo propietario, se le aplica el tercer tipo de permisos.

Figura 8.1 Permisos



Permisos estándar

Los permisos que se pueden aplicar a una entidad -propietario, grupo u otro- son:

- r- Permite la lectura de un archivo. Éste es el único permiso necesario para copiar un archivo. Cuando se aplica a un directorio, se pueden leer (ver) sus archivos.
- w- Permite escribir en un archivo. Con él se pueden cambiar, modificar o sobreescribir los contenidos del archivo. Cuando se aplica en un directorio, este permite borrar y mover archivos (incluso si no se tiene el permiso de escritura específico sobre el archivo individual).
- x- Permiso de ejecución: permite ejecutar el archivo si contiene los scripts necesarios o puede ser ejecutado por el sistema. Aplicado a un directorio, este permite el acceso al mismo. Cuando se aplica a un conjunto con permisos de lectura dentro de un escritorio, este permite buscar dentro de dicho directorio.
- - (guión)- Indica la ausencia de permiso. Por ejemplo, r-x indica que ese usuario puede leer y ejecutar, pero no escribir.

Por tanto, los 10 campos de permisos se resumen en:

- Tipo de entidad (archivo, directorio, otro)
- El propietario puede leer
- El propietario puede escribir
- El propietario puede ejecutar
- El grupo puede leer
- El grupo puede escribir
- El grupo puede ejecutar

- Usuario (no pertenece al grupo y al propietario) puede leer
- Usuario puede escribir
- Usuario puede ejecutar

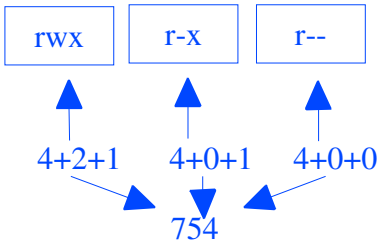
Estos permisos tienen valores numéricos como se muestran en la Tabla 5-1.

Tabla 5-1 Simbología de permisos y sus valores

Permiso	***Valor numérico***
r	4
w	2
x	1
-	0

Los valores numéricos hacen posible añadir permisos a la vez y expresarlo de un modo sencillo. Por ejemplo, si un archivo permite al usuario rwx, el valor numérico sería 4(r)+2(w)+1(x)=7. El formato del conjunto de los permisos de un archivo se muestra en la Figura 8.2.

Figura 8.2 Valores numéricos para los permisos de archivo.



La tabla 5-2 muestra la conversión numérica de un conjunto de distintos permisos:

Tabla 5-2 Conversión numérica

Valor numérico	***Permisos***
1	--------x
2	-------w-
3	-------wx
4	------r--
5	------r-x
6	------rw-
7	------rwx
10	-----x---
11	-----x--x
22	-----w--w-
33	----wx-wx
55	---r-xr-x

Valor numérico	***Permisos***
77	---rwxrwx
100	--x------
101	--x-----x
111	--x--x--x
222	-w--w--w-
311	-wx--x--x
322	-wx-w--w-
400	r--------
444	r--r--r--
511	r-x---x--x
544	r-xr--r--
644	rw-r--r--
666	rw-rw-rw
755	rwxr-xr-x
777	rwxrwxrwx

Los permisos por defecto para todos los nuevos archivos creados son 666 (rw-rw-rw-) y para los directorios son 777(rwxrwxrwx). Este número puede ser modificado mediante la variable umask. La variable umask indica la cantidad sustraída al permiso por defecto hasta llegar a los permisos que se le aplicarán al usuario.

Para ver el valor de umask, lo tecleamos en la línea de comandos:

```
$ umask
022
```

Con un umask de 022, los permisos asignados a los nuevos archivos serán 644 (rw-r—r--) y a los directorios 755 (rwxr-xr-x), como se muestra en la Figura 5.3:

Tabla 5-3 Cálculo de los valores de las nuevas entidades después de sustraer el valor de umask.

Archivos	***Directorios***
666 -rw-rw-rw- - 022 ----w--w-	777 dwxrwxrwx - 022 ----w--w-
644 -rw-r--r--	755 dwxr-xr-x

Se pueden cambiar los valores de umask especificando un valor diferente en la línea de comandos (umask 15, por ejemplo), y este valor es el usado para la sesión. La variable se define en la información de inicio de sesión y se recupera (toma el valor inicial) al comienzo de la misma.

Cambiando Valores

Para cambiar los permisos de un archivo o directorio, se puede usar la utilidad chmod. Los argumentos pueden ser números o letras. Por ejemplo, para modificar los permisos de un archivo que permita a todos leer y escribir en él, se deberá entrar lo siguiente:

```
$ ls -l turbo
-rw-r—r— 1 root root 14 Sep 6 22:42 turbo
$ chmod 666 turbo
$ ls -l turbo
-rw-rw-rw- 1 root root 14 Sep 6 22:42 turbo
```

En formato simbólico, u significa usuario, g grupo y o es otro. Se puede elegir y añadir según los permisos existentes:

```
$ ls -l turbo
-rw-r—r— 1 root root 14 Sep 6 22:42 turbo
$ chmod go+w turbo
$ ls -l turbo
-rw-rw-rw- 1 root root 14 Sep 6 22:42 turbo
```

o especificar los permisos directamente:

```
$ ls -l turbo
-rw-r—r— 1 root root 14 Sep 6 22:42 turbo
$ chmod ugo=rw turbo
$ ls -l turbo
-rw-rw-rw- 1 root root 14 Sep 6 22:42 turbo
```

Se puede utilizar el signo + para añadir a los permisos existentes y el - para borrarlos. El signo = ignora la existencia de permisos y fija el valor indicado. La opción -c indica a chmod que devuelva los nombres de los archivos que han cambiando, y la -f elimina la visualización por pantalla de los mensajes de error.

Permisos especiales

Pueden ser utilizados 3 tipos de permisos en determinadas circunstancias. Aparte de los simpre aplicables de lectura, escritura y ejecución, algunas veces es necesario algo más para un archivo o directorio. Estos permisos especiales son los 3 siguientes:

- Asignar ID de usuario (set user ID) (SUID)
- Asignar ID de grupo (set group ID) (SGID)
- Sticky bit

SUID

La asignación de ID de usuario se aplica cuando se desea que un determinado usuario ejecute un programa que de otro modo no podría.

Por ejemplo, sólo el usuario root sería capaz de ejecutar la función funcion xyz (comenzar backups, restaurar el sistema, entrar en otros recursos, etc) a causa de las ramificaciones de seguridad, pero se necesita que los usuarios ejecuten un shell script para realizar esta acción, porque no se dispone del tiempo necesario para hacerlo personalmente.

Se puede crear este shell script como root y asignar el permiso SUID de modo que el usuario que ejecute el script sea root sólo dentro de ese script. Antes y después del manuscrito, es únicamente un usuario, pero durante la ejecucion del script es como si fuera root.
El permiso numerico de SUID, 4000, es sumado al valor de otros permisos. Una vez aplicado este, cambia la x en el campo del ejecutable para el propietario de los permisos a una s:

```
$ ls -l turbo2

$ chmod 4777 turbo2
$ ls -l turbo2
```

Recordar: El objetivo de la utilización de este permiso es que el proceso sea ejecutado por la persona que lo creó (root en este caso) y no por la persona que lo ejecuta. Sintaxis:

```
chmod u+s turbo2
```

SGID

Similar en la naturaleza a SUID, el permiso de la identificación de grupo del sistema se aplica cuando es necesario que la persona que ejecuta el archivo sea un miembro del grupo que posee el archivo (y no el propietario). Esto cambia el x en el permiso del grupo a un s, y el valor numérico es 2000:

```
$ ls -l turbo2

$ chmod 2777 turbo2
$ ls -l turbo2
```

La sintaxis del comando es:

```
chmod g+s turbo2
```

Sticky Bit

Este permiso no trabaja como los otros permisos especiales. Con un valor numérico de 1000, sus operaciones difieren cuando están aplicadas a un directorio o a un archivo. Cuando está aplicado a un directorio, evita que los usuarios supriman archivos de las carpetas que les conceden el permiso de escritura, a menos que sean el propietario del archivo. Por defecto, cualquier usuario que tenga permiso de escritura en un directorio puede suprimir archivos dentro de ese directorio, incluso si no tiene el permiso de escritura de ese archivo.
Cuando se aplica sobre un archivo, el archivo se convierte en "sticky" (bloqueado). La primera vez que se accede o se ejecuta el archivo y se carga en memoria, permanece cargado en memoria física (RAM) o espacio swap de modo que pueda funcionar más rápidamente que si se lee desde el disco.
Si el archivo no es ejecutable, el último bit de permiso (para otra categoria) se convierte en T. Si el archivo es un fichero ejecutable, o el permiso se aplica a un directorio, el bit pasado se convierte en una t. Cuando se aplica el permiso chmod y las letras, aparece t de todos modos (sea archivo o directorio).

Ejercicios TEST

1. ¿Cuál de los siguientes permisos se representa por el valor numérico 44?

A. - - - - - - - r w -
B. - - - - r w - - - -
C. - - - - r - - r - -
D. - r - - r - - - - -

2. ¿Cuales serán los permisos del archivo ejecutable "portable" cuando se utilice chmod con el valor numérico 1777?

A. - r w s r w x r w x
B. - r w x r w s r w x
C. - r w x r w x r w t
D. - r w x r w x t w T

Respuestas TEST

1. La respuesta correcta a esta pregunta es la c. Cuando el valor numérico es inferior a cuatro dígitos, se asume que el resto son 0, por lo tanto 44 pasa a ser 0044 y los permisos son ----r--r--. La respuesta a sería 6, la b 60 y la d sería equivalente a 440; por lo tanto, son incorrectas.

2. La respuesta correcta en este caso es la c. Debido a que el archivo es ejecutable, el último bit se convierte en t. La respuesta a es un valor igual a 4777, la b es 2777, y la d tiene como último bit T, lo que indica que no es ejecutable, es decir, también es incorrecta.

Bibliografia y enlaces recomendados

LPIC 1 Certification Bible (Bible) by Angie Nash, Jason Nash
John Wiley & Sons; Bk&CD-Rom edition (July 1, 2001) ISBN: 0764547720

LPI Linux Certification in a Nutshell by Jeffrey Dean
O'Reilly & Associates; 1st ed edition (May 15, 2001) ISBN: 1565927486

CramSession's LPI General Linux Part 1 : Certification Study Guide
CramSession.com; ISBN: B000079Y0V; (August 17, 2000)

Referencias Unix Reviews
http://www.unixreview.com/documents/s=7459/uni1038932969999/

Página LPI: www.lpi.org

Apuntes IBM: http://www-106.ibm.com/developerworks/edu/l-dw-linux-lpir21-i.html

Manuales GPL: http://www.nongnu.org/lpi-manuals/