Permisos de usuario en Linux y permisos especiales

Laila Fernandez Santamaria 1ºDAW

Índice

Introducción

Los permisos en Linux son unos de los más fundamentales de la seguridad y la administración en un sistema operativo. Este sistema, que es heredado de UNIX, está basado en tres entidades, que son, el propietario del archivo, al grupo al que pertenece y todos los demás usuarios.

Linux utiliza el sistema numérico octal para representar los permisos básicos de lectura, escritura y ejecución (r, w, x), que también se puede representar de forma numérica (4, 2, 1), Esta estructura permite desarrollar mucho más detalladamente el acceso a archivos y directorios, facilitando el poder usar la política de seguridad en entornos multiusuario.

Además de los permisos básicos, Linux nos da también algunos permisos especiales como SUID, SGID y Sticky Bit, estos amplían mucho las capacidades del sistema. El permiso SUID nos permiten ejecutar archivos con los privilegios del propietario, el permiso SGID nos mantiene la pertenencia a grupos en subdirectorios y el Sticky Bit restringe la eliminación de archivos a sus propietarios.

El dominio de este sistema de permisos es esencial para los administradores de sistemas, desarrolladores y cualquier usuario que quera entender el funcionamiento de la protección en entornos Linux, siendo una base muy importante para agregar estrategias de seguridad que sean buenas.

1. ¿Qué son los permisos y que importancia tienen?

Los permisos de Linux son un sistema para controlar quien puede hacer qué con cada archivo y carpeta en un ordenador. Linux divide a los tres tipos de usuarios en tres categorías:

- **El propietario** – Persona que creo el archivo y/o lo posee.
- **El grupo** – Personas cercanas al archivo que comparten algunos de los privilegios.
- **Otros** – Resto de usuarios que pueden ver y leer el archivo, pero no pueden hacer nada con él.

Los permisos tienen mucha importancia ya que si tienes los permisos correctos puedes proteger tu información personal, evitar que alguien borre cosas que no se deberían borrar, puedes compartir un archivo con tus compañeros de trabajo de manera segura y aprendes cómo funciona los sistemas de seguridad informática.

2. Permisos básicos

Linux tiene tres tipos básicos de permisos que son muy fáciles de entender y muy efectivos:

- **Permisos de lectura (r)** -- Nos da la facilidad de poder ver el contenido de un archivo y de listar el contenido de un directorio
- **Permisos de escritura (w)** – Nos deja modificar el contenido de un archivo.
- **Permisos de ejecución (x)** – Nos permite ejecutar un Script o un programa, acceder al contenido de un directorio y crear o eliminar archivos dentro de un directorio.

En directorios, el permiso de ejecución es súper importante. Sin él no podrías ver absolutamente ningún archivo y no podrías realizar nada.

3. Comprensión visual de los permisos

Al abrir una terminal Linux y escribir ls –l aparece una línea de código así:

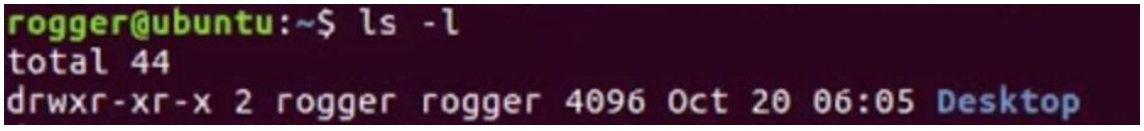

Figura 3.1 LS –L

[propietario] [grupo] [tamaño] [fecha] [nombre]

- **d** – tipo (en este caso es un directorio)
- **rwxr-xr-x** →Amarillo – Permisos del propietario

  Verde – Permisos del grupo

  Azul – Permisos de otros usuarios

4. Sistema numérico: Los permisos en números

Se ha inventado una forma más corta de expresar los permisos usando números.

Cada permiso tiene un valor:

- **Lectura (r)** = 4
- **Escritura (w)** = 2
- **Ejecución (x)** = 1

Para calcular el valor numérico de un conjunto de permisos hay que sumar los valores:

⇒ r - - = 4 + 0 + 0 = 4

⇒ - w - = 0 + 2 + 0 = 2

⇒ - - x = 0 + 0 + 1 = 1

⇒ r w - = 4 + 2 + 0 = 6

⇒ r - x = 4 + 0 + 1 = 5

⇒ - w x = 0 + 2 + 1 = 3

⇒ r w x = 4 + 2 + 1 = 7

5. Comandos esenciales para manejar permisos

- **chmod** - Cambiar permisos

Modo numérico:

chmod 755 trabajo1.txt # rwxr-xr-x

chmod 600 trabajo2.txt # rw-------

chmod 644 trabajo3.txt # rw-r—r--

- chown - Cambiar propietario

Cambiar solo propietario:

chown laila trabajo1.txt

Cambiar propietario y grupo:

chown laila:grupo1 trabajo2.txt

Opciones recursivas

Para hacer cambios a todos los archivos dentro de una carpeta hay que añadir –R

chmod:

chmod –R 755 proyecto/

chown:

chown –R laila:grupo1 carpeta/

6. Permisos especiales

- **SUID** (Set User ID)

SUID nos permite que, al ejecutar un programa, lo hagamos con los permisos del propietario del archivo en vez de nuestros propios permisos.

La línea de código se vería así:

rw**S**r-xr-x (la 's' en lugar de la 'x' en la parte del usuario)

chmod 4755 programa

- **SGID** (Set Group ID)

Como SUID pero para grupos. Tiene dos usos principales:

- *En archivos*: ejecuta el programa con los permisos del grupo propietario
- *En directorios:* Hace que todos los archivos creados dentro hereden el grupo del directorio

La línea de código se vería así:

rwxr-**S**r-x (la 's' en lugar de la 'x' en la parte del grupo)

chmod 2755 carpeta

- **Sticky Bit**

Impide que los usuarios borren o renombren archivos de otros usuarios en un directorio, aunque tengan permisos de escritura.

La línea de código se vería así:

rwxrwxrw**t** (la 't' en lugar de la 'x' en la parte de otros)

chmod 1777 carpeta

7. ACLs: Permisos para situaciones complejas

Son reglas personalizadas para usuarios o grupos específicos.

- **Instalar herramientas ACL**

sudo apt-get install acl

sudo dnf install acl

- **Ver ACLs de un archivo**

getfacl trabajo1.txt

- **Establecer ACLs**

- Dar permiso de lectura a un usuario específico

setfacl -m u:laila:r trabajo1.txt

- Dar permisos de lectura y escritura a un grupo específico

setfacl -m g:proyecto1:rw trabajo1.txt

- Establecer permisos por defecto para nuevos archivos en un directorio

setfacl -d -m g:proyecto1:rw carpeta/

- **Eliminar ACLs**

- Eliminar una entrada específica

setfacl -x u:laila trabajo1.txt

- Eliminar todas las entradas

setfacl -b trabajo1.txt

8. Conclusión

Siempre usa el principio de "mínimo privilegio" (da solo los permisos necesarios)

- Nunca uses chmod 777 a menos que sepas exactamente lo que estás haciendo
- Usa los permisos especiales con cuidado
- Para proyectos compartidos, los grupos y SGID son tus mejores amigos

Dominar los permisos de Linux te da una ventaja muy grande a la hora de trabajar en el mundo de la informática

9. Bibliografia

Páginas web:

Permisos basicos

ACLs

Permisos Especiales

Comandos Especiales