

Taller #5

1. Comandos ``useradd``, ``userdel``, ``passwd`` y los diferentes ID de usuarios.

- ``useradd``: Se utiliza para crear un nuevo usuario en el sistema. Permite especificar diferentes opciones como el directorio home, la shell por defecto, y los grupos a los que pertenecerá el usuario.
- ``userdel``: Este comando sirve para eliminar un usuario del sistema. Puede incluir opciones para eliminar también el directorio home y el correo del usuario.
- ``passwd``: Se emplea para actualizar la contraseña de un usuario. Este comando puede ser utilizado por el usuario para cambiar su propia contraseña o por el superusuario para cambiar la contraseña de cualquier usuario.
- Los diferentes ID de usuarios (UID) son identificadores únicos asignados a cada usuario. Por lo general, el UID 0 está reservado para el superusuario (root), y los UIDs a partir de 1000 son para cuentas de usuario regulares.

2. Grupos primarios y grupos secundarios en Linux.

- Grupo primario: Es el grupo al que pertenece un usuario por defecto. Los archivos que el usuario crea se asocian normalmente con este grupo. En el archivo ``etc/passwd``, se asigna un grupo primario a cada usuario.
- Grupos secundarios: Son grupos adicionales a los que un usuario puede pertenecer. Estos se utilizan para conceder permisos adicionales a un usuario para recursos que son compartidos o restringidos dentro del grupo.

3. Cuadro comparativo entre Inode y ACL.

- Inode: Un inode almacena información básica sobre un archivo regular, directorio, u otro objeto de sistema de archivos excepto su nombre y su contenido actual. Inode incluye atributos como permisos, propietario, grupo, tamaño del archivo, hora de creación/modificación, y punteros a los bloques de datos.
- ACL (Access Control List): Una ACL proporciona una lista detallada de permisos otorgados a usuarios o grupos para un objeto de sistema de archivos. A diferencia del sistema de permisos tradicional (lectura, escritura, ejecución), las ACL permiten especificar permisos detallados y complejos para múltiples usuarios y grupos.

4. Comando para cambiar permisos a un archivo.

- Por medio de letras: Se utiliza el comando ``chmod`` seguido de las letras ``u`` (usuario), ``g`` (grupo), ``o`` (otros) y ``a`` (todos) junto con los operadores ``+`` (agregar), ``-`` (quitar) o ``=`` (establecer) y las letras ``r`` (lectura), ``w`` (escritura) y ``x`` (ejecución). Por ejemplo: ``chmod u+rw archivo``.
- Por medio de números: También con ``chmod``, pero utilizando una combinación de tres dígitos representando los permisos para usuario, grupo y otros, respectivamente. Cada dígito es la suma de 4 (lectura), 2 (escritura) y 1 (ejecución). Por ejemplo: ``chmod 755 archivo``.

5. Tabla de particiones NTFS y EXT32 (posiblemente EXT3 o EXT4).

- NTFS (New Technology File System) es el sistema de archivos predilecto de Windows. Proporciona seguridad en el acceso a archivos, cuotas de disco, y compresión de archivos.
- EXT3 o EXT4 son sistemas de archivos utilizados por Linux. EXT3 es conocido por ser un sistema de archivos con registro por diario que permite una recuperación más rápida después de una falla de energía o de sistema. EXT4 es una mejora de EXT3 que soporta volúmenes más grandes y archivos de mayor tamaño, además de ofrecer mejor rendimiento.

Parte práctica

Agregue tres diferentes usuarios con contraseñas diferentes

```
(johnnyzaet@ Kali)-[~]
$ sudo useradd Jason

(johnnyzaet@ Kali)-[~]
$ sudo useradd Luis

(johnnyzaet@ Kali)-[~]
$ sudo useradd Steven

(johnnyzaet@ Kali)-[~]
$ sudo useradd Diego

(johnnyzaet@ Kali)-[~]
$ sudo useradd Pedro

(johnnyzaet@ Kali)-[~]
$ sudo useradd Josue

(johnnyzaet@ Kali)-[~]
$ sudo useradd Juan

(johnnyzaet@ Kali)-[~]
$ sudo useradd Viviana

(johnnyzaet@ Kali)-[~]
$ sudo useradd Harold
```

Confirme que cada usuario se creó realizando los siguientes comandos. Note las diferencias en las salidas de datos.

```
(johnnyzaet@ Kali)-[~]
$ cat /etc/passwd | grep -E "Jason|Luis|Diego|Josue|Viviana|Steven|Pedro|Juan|Harold"
Jason:x:1002:1002::/home/Jason:/bin/sh
Luis:x:1003:1003::/home/Luis:/bin/sh
Diego:x:1004:1004::/home/Diego:/bin/sh
Josue:x:1005:1005::/home/Josue:/bin/sh
Viviana:x:1006:1006::/home/Viviana:/bin/sh
Steven:x:1007:1007::/home/Steven:/bin/sh
Pedro:x:1008:1008::/home/Pedro:/bin/sh
Juan:x:1009:1009::/home/Juan:/bin/sh
Harold:x:1010:1010::/home/Harold:/bin/sh
```

Cree los grupos y usuarios que se muestran en la siguiente tabla.

Grupo	Nombre de Grupo	Lista de usuario
Profesores	Professors	Jason, Luis, Diego
Asistentes	Assistents	Josué, Viviana, Steven
Estudiantes	Students	Pedro, Juan, Harold

```
(johnnyzaet@ Kali)-[~]
$ sudo usermod -aG Professors Jason | sudo usermod -aG Professors Luis | sudo
usermod -aG Professors Diego

(johnnyzaet@ Kali)-[~]
$ sudo usermod -aG Assistents Josue | sudo usermod -aG Assistents Viviana | s
udo usermod -aG Assistents Steven

(johnnyzaet@ Kali)-[~]
$ sudo usermod -aG Students Pedro | sudo usermod -aG Students Juan | sudo use
rmod -aG Students Harold
```

Valide que se hayan creado los grupos de usuario y sus respectivas listas.

```
(johnnyzaet@ Kali)-[~]
$ sudo cat /etc/group | grep -E "Jason|Luis|Diego|Josue|Viviana|Steven|Pedro|
Juan|Harold"
Jason:x:1002:
Luis:x:1003:
Diego:x:1004:
Josue:x:1005:
Viviana:x:1006:
Steven:x:1007:
Pedro:x:1008:
Juan:x:1009:
Harold:x:1010:
Professors:x:1011:Jason,Luis,Diego
Assistents:x:1012:Josue,Viviana,Steven
Students:x:1013:Juan,Harold,Pedro
```

Ejecute los comandos: \$ touch /tmp/test y \$ ls -l /tmp/test.

```
(johnnyzaet@ Kali)-[~]
$ touch /tmp/test

(johnnyzaet@ Kali)-[~]
$ ls -l /tmp/test
-rw-r--r-- 1 johnnyzaet johnnyzaet 0 Nov  8 17:07 /tmp/test
```

Los comandos modifican los permisos del archivo /tmp/test de la siguiente manera: chmod o+w añade permiso de escritura para otros usuarios; chmod 666 establece permisos de lectura y escritura para todos los usuarios; chmod a-rwx elimina todos los permisos para todos; cat /tmp/test intenta mostrar el contenido del archivo, pero su éxito depende de los permisos actuales; y finalmente, chmod u+rw otorga al propietario del archivo permisos de lectura y escritura, dejando a otros sin permisos tras los comandos previos.

```
(johnnyzaet@Kali)-[~]
$ chmod o+w /tmp/test

(johnnyzaet@Kali)-[~]
$ chmod 666 /tmp/test

(johnnyzaet@Kali)-[~]
$ chmod a-rwx /tmp/test

(johnnyzaet@Kali)-[~]
$ cat /tmp/test
cat: /tmp/test: Permission denied

(johnnyzaet@Kali)-[~]
$ sudo cat /tmp/test

(johnnyzaet@Kali)-[~]
$ chmod u+rw /tmp/test

(johnnyzaet@Kali)-[~]
$
```

Getfacl: El comando getfacl se utiliza para mostrar las ACLs de un archivo o directorio. Su sintaxis básica es “getfacl archivo_o_directorio”

Setfacl: El comando setfacl permite modificar las ACLs de un archivo o directorio. Tiene varias opciones y sintaxis dependiendo de lo que quieras lograr. Aquí hay algunos ejemplos de uso:

- setfacl -m u:nombre_de_usuario:permisos archivo_o_directorio
- setfacl -m u:luis:rw archivo.txt
- setfacl -m g:nombre_del_grupo:permisos archivo_o_directorio

Trate de editar el archivo /etc/motd. Probablemente el un usuario no pueda editar y solo podría leerlo.

```
GNU nano 7.2 /etc/motd *
The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law

[ Error writing /etc/motd: Permission denied ]
^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify
```

Utilice el comando setfacl y ejecute el comando getfacl

```
(johnnyzaet@Kali)-[~]
$ sudo setfacl -m u:johnnyzaet:rw /etc/motd

(johnnyzaet@Kali)-[~]
$ getfacl /etc/motd
getfacl: Removing leading '/' from absolute path names
# file: etc/motd
# owner: root
# group: root
user::rw-
user:johnnyzaet:rw-
user:Jason:rw-
group::r--
mask::rw-
other::r--
```


Como root, cree el directorio mkdir /var/tmp/collab, Verifique la nueva ACL. getfacl /var/tmp/collab.

```
(johnnyzaet@ Kali)-[~]  
$ sudo mkdir /var/tmp/collab  
  
(johnnyzaet@ Kali)-[~]  
$ getfacl /var/tmp/collab/  
getfacl: Removing leading '/' from absolute path names  
# file: var/tmp/collab/  
# owner: root  
# group: root  
user::rwx  
group::r-x  
other::r-x
```

Ahora debe crear un archivo en el directorio creado llamado /var/tmp/collab/rootfile. Ejecute el comando: # echo rootfile contents > /var/tmp/collab/rootfile. Verifique el contenido con cat /var/tmp/collab/rootfile. Verifique la ACL del archivo. getfacl /var/tmp/collab/rootfile.

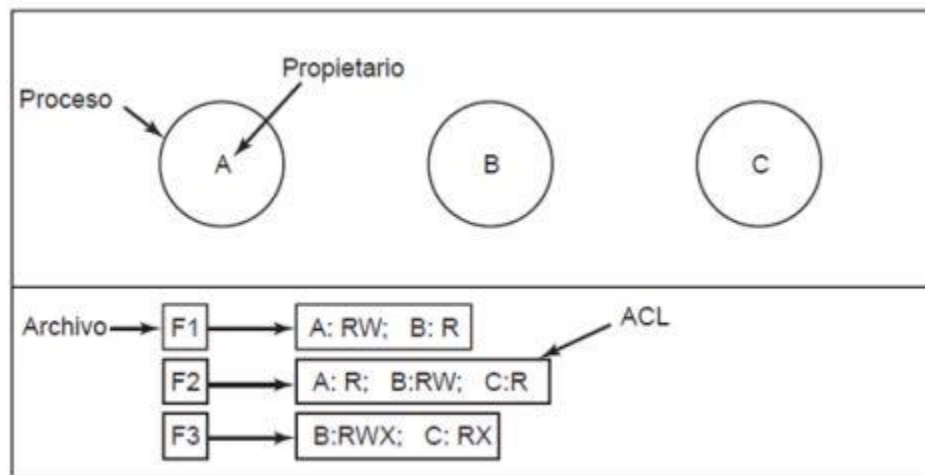
```
(johnnyzaet@ Kali)-[~]  
$ echo rootfile contents > /var/tmp/collab/rootfile  
  
(johnnyzaet@ Kali)-[~]  
$ cat /var/tmp/collab/rootfile  
rootfile contents  
  
(johnnyzaet@ Kali)-[~]  
$ getfacl /var/tmp/collab/rootfile  
getfacl: Removing leading '/' from absolute path names  
# file: var/tmp/collab/rootfile  
# owner: root  
# group: root  
user::rw-  
user:johnnyzaet:rw-  
group::r-x  
mask::rw-  
other::r--  
#effective:r--
```

Ahora como usuario no root agregue una línea de texto en el archivo. Ejecute el comando `$ echo 'rootadmin was here' >> /var/tmp/collab/rootfile`. Verifique el contenido. `# cat /var/tmp/collab/rootfile`.

```
(johnnyzaet@ Kali)-[~]
$ echo 'rootadmin was here' >> /var/tmp/collab/rootfile

(johnnyzaet@ Kali)-[~]
$ sudo cat /var/tmp/collab/rootfile
rootfile contents
rootadmin was here
```

Realice con líneas de comando la estructura de usuarios, ACL y archivos que muestra la figura.



Creación de los usuarios y asignarles contraseñas, posteriormente crear carpetas y asignar owner.

```
(johnnyzaet@ Kali)-[~/Desktop/CE4303-Operating_Systems/Taller_5/Structure]
$ sudo useradd A
[sudo] password for johnnyzaet:

(johnnyzaet@ Kali)-[~/Desktop/CE4303-Operating_Systems/Taller_5/Structure]
$ sudo useradd B
^[A
(johnnyzaet@ Kali)-[~/Desktop/CE4303-Operating_Systems/Taller_5/Structure]
$ sudo useradd C

(johnnyzaet@ Kali)-[~/Desktop/CE4303-Operating_Systems/Taller_5/Structure]
$ sudo passwd A
New password:
Retype new password:
passwd: password updated successfully

(johnnyzaet@ Kali)-[~/Desktop/CE4303-Operating_Systems/Taller_5/Structure]
$ sudo passwd B
New password:
Retype new password:
passwd: password updated successfully

(johnnyzaet@ Kali)-[~/Desktop/CE4303-Operating_Systems/Taller_5/Structure]
$ sudo passwd C
New password:
Retype new password:
passwd: password updated successfully
```

```
(johnnyzaet@ Kali)-[~/Desktop/CE4303-Operating_Systems/Taller_5/Structure]
$ touch F1

(johnnyzaet@ Kali)-[~/Desktop/CE4303-Operating_Systems/Taller_5/Structure]
$ touch F2

(johnnyzaet@ Kali)-[~/Desktop/CE4303-Operating_Systems/Taller_5/Structure]
$ touch F3

(johnnyzaet@ Kali)-[~/Desktop/CE4303-Operating_Systems/Taller_5/Structure]
$ chown A F1
chown: changing ownership of 'F1': Operation not permitted

(johnnyzaet@ Kali)-[~/Desktop/CE4303-Operating_Systems/Taller_5/Structure]
$ sudo chown A F1

(johnnyzaet@ Kali)-[~/Desktop/CE4303-Operating_Systems/Taller_5/Structure]
$ sudo chown A F2

(johnnyzaet@ Kali)-[~/Desktop/CE4303-Operating_Systems/Taller_5/Structure]
$ sudo chown A F3
```


Se procede a agregar los permisos para cada tipo de usuario, así como sus respectivos setfacl para cada usuario y sus propiedades respectivas.

```
(johnnyzaet@ Kali)-[~/Desktop/CE4303-Operating_Systems/Taller_5/Structure]
$ sudo chmod 700 F1

(johnnyzaet@ Kali)-[~/Desktop/CE4303-Operating_Systems/Taller_5/Structure]
$ sudo chmod 700 F2

(johnnyzaet@ Kali)-[~/Desktop/CE4303-Operating_Systems/Taller_5/Structure]
$ sudo chmod 700 F3

(johnnyzaet@ Kali)-[~/Desktop/CE4303-Operating_Systems/Taller_5/Structure]
$ sudo setfacl -m u:A:rw F1

(johnnyzaet@ Kali)-[~/Desktop/CE4303-Operating_Systems/Taller_5/Structure]
$ sudo setfacl -m u:B:r F1

(johnnyzaet@ Kali)-[~/Desktop/CE4303-Operating_Systems/Taller_5/Structure]
$ sudo setfacl -m u:A:r F2

(johnnyzaet@ Kali)-[~/Desktop/CE4303-Operating_Systems/Taller_5/Structure]
$ sudo setfacl -m u:B:rw F2

(johnnyzaet@ Kali)-[~/Desktop/CE4303-Operating_Systems/Taller_5/Structure]
$ sudo setfacl -m u:C:r F2

(johnnyzaet@ Kali)-[~/Desktop/CE4303-Operating_Systems/Taller_5/Structure]
$ sudo setfacl -m u:B:rwx F3

(johnnyzaet@ Kali)-[~/Desktop/CE4303-Operating_Systems/Taller_5/Structure]
$ sudo setfacl -m u:C:rx F3
```

Por último, se muestra en totalidad, la estructura de toda la carpeta con sus respectivos archivos, sus getfacl

```
(johnnyzaet@Kali)-[~/Desktop/CE4303-Operating_Systems/Taller_5/Structure]
$ getfacl -R ./*
# file: F1
# owner: A
# group: johnnyzaet
user::rwx
user:A:rwx
user:B:r--
group:---
mask:rwx
other:---

# file: F2
# owner: A
# group: johnnyzaet
user::rwx
user:A:r--
user:B:rwx
user:C:r--
group:---
mask:rwx
other:---

# file: F3
# owner: A
# group: johnnyzaet
user::rwx
user:B:rwx
user:C:r-x
group:---
mask:rwx
other:---
```