

Gestión de Usuarios y Grupos en Linux

Introducción

El presente caso práctico se centra en la migración de un sistema operativo de Windows a Linux, en el cual se deben gestionar los usuarios y grupos de una organización. Se solicita la creación de dos grupos, "contabilidad" y "administración", así como la asignación de permisos apropiados a los usuarios para garantizar la seguridad y la protección de los datos. A continuación se detallan todos los pasos necesarios para completar la configuración solicitada, con un enfoque en la creación de grupos, usuarios, gestión de contraseñas y asignación de permisos.

1. Creación de los Grupos

Los grupos son fundamentales en un sistema Linux, ya que permiten agrupar a usuarios con necesidades similares de acceso a recursos. En este caso, los grupos a crear son **contabilidad** y **administración**. Cada grupo tendrá diferentes niveles de acceso, lo que ayudará a controlar la seguridad del sistema.

Pasos para la creación de grupos:

1. Iniciar sesión como superusuario (root) o utilizar sudo para obtener privilegios.
2. Usar el comando *groupadd* para crear los grupos correspondientes.

```
sudo groupadd contabilidad  
sudo groupadd administracion
```

```
nerine@nerine-VirtualBox:~$ sudo groupadd contabilidad  
[sudo] password for nerine:  
nerine@nerine-VirtualBox:~$ sudo groupadd contabilidad  
groupadd: group 'contabilidad' already exists  
nerine@nerine-VirtualBox:~$ sudo groupadd administración  
nerine@nerine-VirtualBox:~$
```

- **Explicación:** El comando groupadd se usa para crear un nuevo grupo en el sistema. Al ejecutar estos comandos, se crean los grupos de "contabilidad" y "administración", que luego se utilizarán para asignar usuarios con permisos diferenciados según las necesidades del trabajo de la empresa.

2. Creación de los Usuarios

El siguiente paso es crear los usuarios. Se requiere la creación de cuatro usuarios, que serán asignados a los grupos previamente creados. De acuerdo con el caso práctico, dos usuarios serán asignados al grupo "contabilidad" y los otros dos al grupo "administración".

SISTEMAS INFORMÁTICOS - CASO 1 UNIDAD 4

Pasos para la creación de usuarios:

1. Para crear a los usuarios, utilizaremos el comando `useradd`, que crea una cuenta de usuario en el sistema. Además, con el parámetro `-G`, asignamos a cada usuario a los grupos correspondientes.

```
sudo useradd -m juan -G contabilidad
sudo useradd -m maria -G contabilidad
sudo useradd -m carlos -G administracion
sudo useradd -m ana -G administracion
```

```
nerine@nerine-VirtualBox:~$ sudo useradd -m juan -G contabilidad
nerine@nerine-VirtualBox:~$ sudo useradd -m maria -G contabilidad
nerine@nerine-VirtualBox:~$ sudo useradd -m carlos -G administración
nerine@nerine-VirtualBox:~$ sudo useradd -m ana -G administración
nerine@nerine-VirtualBox:~$ id juan
uid=1001(juan) gid=1003(juan) groups=1003(juan),1001(contabilidad)
nerine@nerine-VirtualBox:~$ id maria
uid=1002(maria) gid=1004(maria) groups=1004(maria),1001(contabilidad)
nerine@nerine-VirtualBox:~$ id carlos
uid=1003(carlos) gid=1005(carlos) groups=1005(carlos),1002(administración)
nerine@nerine-VirtualBox:~$ id ana
uid=1004(ana) gid=1006(ana) groups=1006(ana),1002(administración)
```

- **Explicación:**
 - **-m:** Este parámetro asegura que se cree el directorio personal del usuario.
 - **-G:** Especifica los grupos a los que el usuario debe pertenecer.
 - Estos comandos crean a los usuarios "Juan", "María", "Carlos" y "Ana", asignándolos a sus respectivos grupos de "contabilidad" y "administración".

3. Cambio de Contraseñas

Después de crear los usuarios, es crucial cambiar las contraseñas para evitar el uso de contraseñas predeterminadas, lo cual puede comprometer la seguridad del sistema. Para cambiar la contraseña de un usuario, usamos el comando `passwd`.

```
sudo passwd juan
sudo passwd maria
sudo passwd carlos
sudo passwd ana
```

- **Explicación:** Al ejecutar `passwd`, el sistema solicita una nueva contraseña para cada uno de los usuarios. Es importante que las contraseñas sean fuertes, es decir, que incluyan una combinación de letras mayúsculas, minúsculas, números y caracteres especiales.

SISTEMAS INFORMÁTICOS - CASO 1 UNIDAD 4

```

nerine@nerine-VirtualBox:~$ sudo passwd juan
New password:
BAD PASSWORD: The password is a palindrome
Retype new password:
Sorry, passwords do not match.
New password:
BAD PASSWORD: The password is a palindrome
Retype new password:
Sorry, passwords do not match.
New password:
BAD PASSWORD: The password fails the dictionary check - it is too simplistic/systematic
Retype new password:
passwd: password updated successfully
nerine@nerine-VirtualBox:~$ 
nerine@nerine-VirtualBox:~$ sudo passwd maria
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: password updated successfully
nerine@nerine-VirtualBox:~$ 
nerine@nerine-VirtualBox:~$ sudo passwd carlos
New password:
Retype new password:
passwd: password updated successfully
nerine@nerine-VirtualBox:~$ sudo passwd ana
New password:
Retype new password:
passwd: password updated successfully
contabilidad:x:1001:juan,maria
administración:x:1002:carlos,ana

```

Para el ejemplo quise usar contraseñas simples, y podemos ver que nos alerta a no hacerlo.

4. Asignación de Permisos

En este paso, se asignan los permisos necesarios para garantizar que los usuarios puedan trabajar de manera adecuada, sin comprometer la seguridad del sistema. Según los requerimientos del caso práctico, se debe permitir que los usuarios que no pertenecen al grupo "administración" puedan borrar ficheros.

Asignación de permisos de eliminación de archivos:

1. Para permitir que los usuarios que no pertenecen al grupo "administración" puedan borrar ficheros, utilizaremos el comando chmod para modificar los permisos de los directorios y archivos que los usuarios deben poder manejar.

```

sudo chmod g+w /directorio
sudo chmod o+w /directorio

```

```

nerine@nerine-VirtualBox:~$ sudo chmod g+w /home/archivos
nerine@nerine-VirtualBox:~$ sudo chmod o+w /home/archivos

```

SISTEMAS INFORMÁTICOS - CASO 1 UNIDAD 4

- **Explicación:**

- **g+w:** Otorga permisos de escritura al grupo (esto permitirá modificar el contenido del directorio).
- **o+w:** Otorga permisos de escritura a los "otros" (usuarios fuera del grupo propietario).

Con estos permisos, los usuarios pueden eliminar archivos de los directorios asignados.

Uso de ACL (Listas de Control de Acceso):

Si se necesita un control más granular sobre los permisos, especialmente en sistemas con usuarios con roles diferentes, podemos utilizar setfacl para configurar listas de control de acceso.

```
sudo setfacl -m u:juan:rwX /directorio
sudo setfacl -m u:maria:rwX /directorio
```

```
nerine@nerine-VirtualBox:~$ sudo setfacl -m u:juan:rwX /home/archivos
nerine@nerine-VirtualBox:~$ sudo setfacl -m u:maria:rwX /home/archivos
```

- **Explicación:**

- El comando setfacl permite asignar permisos detallados a un usuario para un directorio específico. En este caso, otorgamos a "Juan" y "María" permisos completos sobre el directorio, lo que incluye lectura, escritura y ejecución (rwX).

5. Resumen de los Comandos y Procedimiento

A continuación, se presenta un resumen de los comandos utilizados para realizar la configuración de los usuarios, grupos y permisos:

1. Creación de los grupos:

```
sudo groupadd contabilidad
sudo groupadd administracion
```

2. Creación de los usuarios:

```
sudo useradd -m juan -G contabilidad
sudo useradd -m maria -G contabilidad
sudo useradd -m carlos -G administracion
sudo useradd -m ana -G administracion
```

SISTEMAS INFORMÁTICOS - CASO 1 UNIDAD 4

3. Cambio de contraseñas:

```
sudo passwd juan  
sudo passwd maria  
sudo passwd carlos  
sudo passwd ana
```

4. Asignación de permisos:

```
sudo chmod g+w /directorio  
sudo chmod o+w /directorio  
sudo setfacl -m u:juan:rwX /directorio  
sudo setfacl -m u:maria:rwX /directorio
```

6. Conclusión

La correcta configuración de los usuarios y grupos en Linux es esencial para garantizar tanto la funcionalidad como la seguridad del sistema. Los pasos descritos permiten cumplir con los requisitos planteados en el caso práctico, asegurando que los usuarios tengan acceso adecuado a los recursos, sin comprometer la seguridad. Las políticas de contraseñas, la creación de grupos y la asignación de permisos son clave para una administración eficiente y segura de un sistema Linux.

7. Referencias

- How to create a user & group in Linux 2022:
https://youtu.be/K3RIggVgkrY?si=foq9dEG7hHZix_VT
- Managing Users and Groups in Linux:
<https://youtu.be/bl3Ta0-7xCw?si=ITlrIHmwYJTmnnny9>
- Udemy
- Material de la unidad