|  |  |  |
| --- | --- | --- |
| sistemas informaticos | | CASO PRACTICO 1 UD4 |
|  | | |
|  | | |
|  |  | |
| alumno cesur 24/25  Alejandro Muñoz de la Sierra | PROFESOR  Efren Zurita Alonso | |

introduccion

En toda empresa, manejar correctamente a los usuarios y permisos en un sistema operativo es muy necesario para asegurar la seguridad y la eficacia en el trabajo, así como para controlar el acceso a los recursos. En este caso práctico, vamos a crear una estructura de usuarios y grupos en un sistema operativo Linux, con el fin de poner en marcha permisos específicos que protejan la información y ayuden en la gestión de recursos compartidos.

La atención se dirige a formar grupos y usuarios, dando a cada uno los privilegios necesarios según su función en la organización. También configuraremos políticas de control de acceso ajustando permisos en archivos y directorios, de modo que solo los usuarios autorizados puedan realizar ciertas acciones.

Este ejercicio nos ayudará a conocer los comandos y herramientas básicos para administrar sistemas en Linux, mientras aprendemos sobre la gestión de cuentas, la seguridad y la mejora del entorno de trabajo, especialmente en el proceso de cambiar de Windows a Linux.

# 01

Formar grupos: contabilidad y administración

En Linux, se usan comandos para hacer grupos. Para este ejemplo, haremos dos grupos: contabilidad y administración.

Pasos:

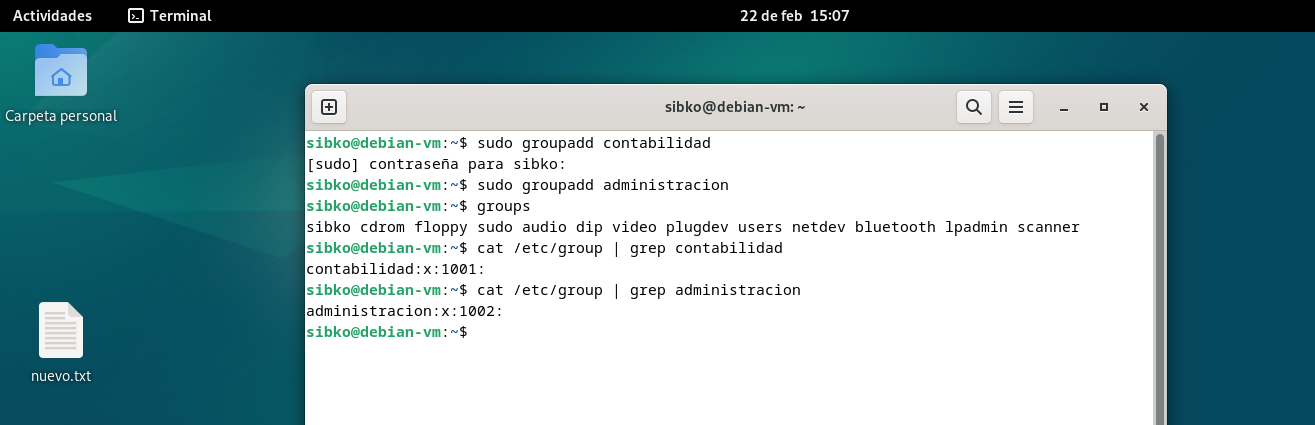
Abrir la terminal de Debian (en Windows 11 puede estar virtualizada).

Escribir estos comandos para los grupos:

sudo groupadd contabilidad

sudo groupadd administracion

Estos comandos crean los grupos contabilidad y administración, que se usarán para los usuarios que crearemos después.



# 02

Crear cuatro usuarios y añadirlos a los grupos

Ya que tenemos los grupos, ahora crearemos cuatro usuarios y los asignaremos a los grupos. Usaremos useradd para crear y usermod para añadir.

Pasos:

Crear los usuarios con estos comandos:

sudo useradd juan -m -s /bin/bash

sudo useradd maria -m -s /bin/bash

sudo useradd pedro -m -s /bin/bash

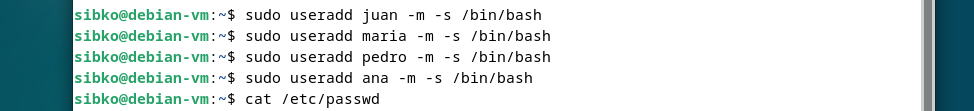
sudo useradd ana -m -s /bin/bash

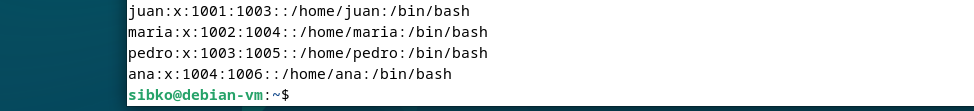
Los parámetros:

-m: Crea el directorio home del usuario.

-s /bin/bash: Establece el shell que usará el usuario, en este caso, bash.

Añadir los usuarios a sus grupos:

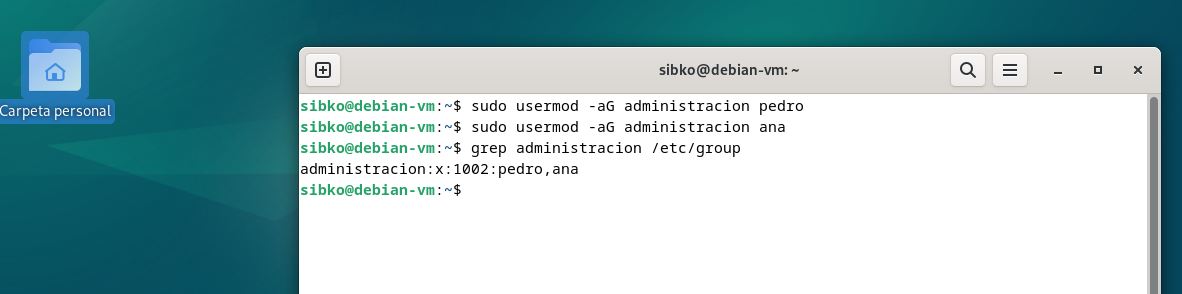




Juan y María se añaden al grupo contabilidad:

sudo usermod -aG contabilidad juan

sudo usermod -aG contabilidad maría

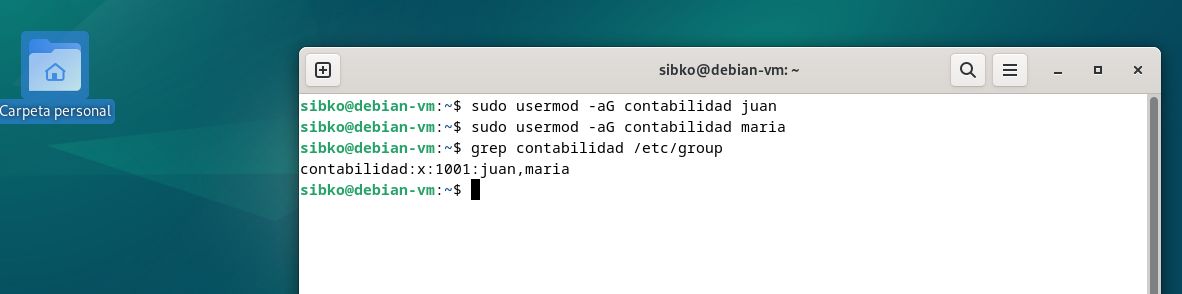


Pedro y Ana se añaden al grupo administración:

sudo usermod -aG administracion pedro

sudo usermod -aG administracion ana

El parámetro -aG se usa para agregar un usuario a un grupo sin quitarlo de otros grupos.



# 03

Cambiar contraseñas de los usuarios

Para asegurarnos de que los usuarios tengan contraseñas seguras, hay que cambiarlas. Usamos passwd para cambiar sus contraseñas.

Pasos:

Cambiar las contraseñas de los usuarios:

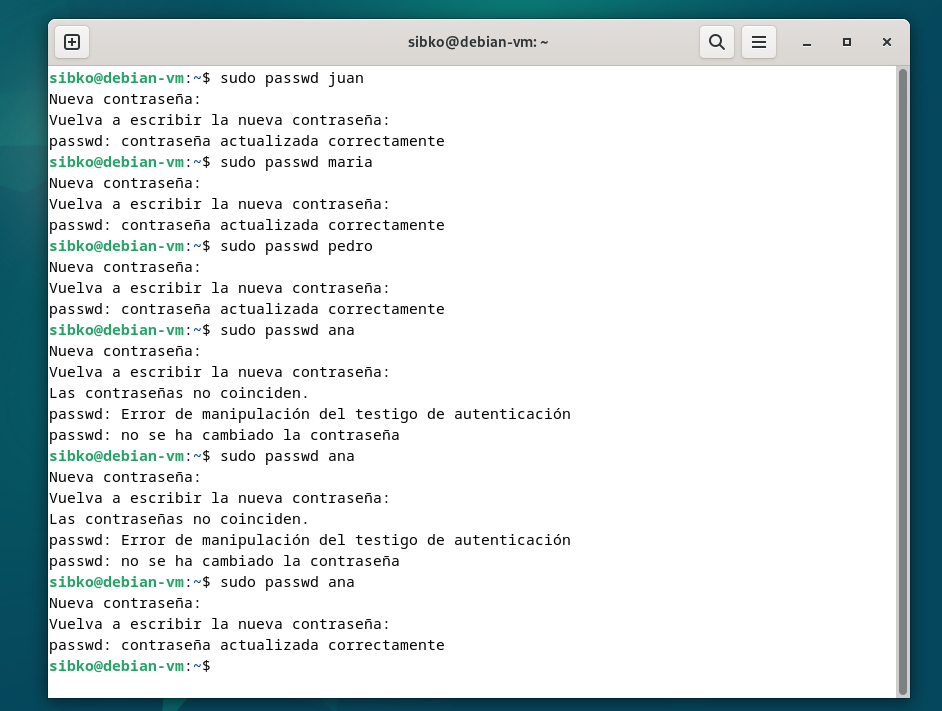
sudo passwd juan

sudo passwd maria

sudo passwd pedro

sudo passwd ana

El sistema pedirá crear una nueva contraseña para cada usuario.



# 04

Dar permisos

Dar permisos para que usuarios que no son de administración" puedan borrar archivos.

En Linux, los permisos se manejan con ACL o comandos como chmod, chown y chgrp. En este paso, permitimos que los usuarios que no están en el grupo administración puedan borrar archivos en un directorio compartido.

Pasos:

Crear un directorio compartido:

sudo mkdir /home/compartido

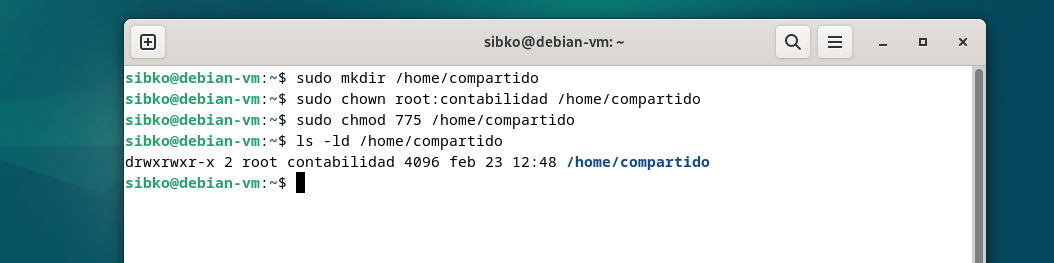
sudo chown root:contabilidad /home/compartido

Esto crea /home/compartido y le asigna como propietario al usuario root y al grupo contabilidad.

Usar chmod para dar permisos de lectura, escritura y ejecución a los usuarios del grupo contabilidad, y permisos de solo lectura y ejecución a otros:

sudo chmod 775 /home/compartido

Este comando otorga permisos completos al propietario y al grupo, mientras que otros usuarios solo pueden leer y ejecutar, no escribir ni borrar.



Si creáramos un nuevo usuario sin grupo que necesitara permisos para borrar en /home/compartido, usamos setfacl para dar permisos adicionales:

sudo setfacl -m u:usuarionuevo:rwx /home/compartido

Esto le da a los usuarios permisos de lectura, escritura y ejecución (rwx) en /home/compartido, permitiéndoles borrar archivos en ese directorio.

# 05

conclusiones

La gestión apropiada de usuarios y grupos en Linux ayuda a manejar el acceso a recursos de forma segura y eficiente. En este proceso, utilizamos comandos básicos para crear y configurar usuarios, grupos y permisos, garantizando que solo los usuarios autorizados puedan borrar o modificar archivos. Este tipo de configuración es importante en empresas para resguardar información y asegurar un uso correcto del sistema operativo.

# 06

referencias

<https://www.youtube.com/watch?v=3DHGZlUYjXA>

<https://www.ionos.com/es-us/digitalguide/servidores/configuracion/comando-mkdir-de-linux/?utm_source=chatgpt.com>

<https://www.youtube.com/watch?v=Ck7xtegcRvA>

<https://www.debian.org/releases/stable/i386/apcs05.es.html?utm_source=chatgpt.com>

<https://www.youtube.com/watch?v=OZBjuqU8crs>

<https://www.debian.org/doc/manuals/securing-debian-manual/ch11s02.es.html?utm_source=chatgpt.com>

<https://en.jveweb.net/archives/2011/02/using-rsync-and-cron-to-automate-incremental-backups.html>