1. Introducción

El presente documento explica de manera breve como agregar un usuario al archivo `sudoers` para que pueda realizar tareas de adminsitración dentro del sistema operativo Linux.

Al momento de gestionar servicios o instalar/actualizar software dentro de Linux, es necesario contar con permisos de superusuario o *root*. Sin embargo, no es recomendable trabajar con este usuario de manera constante por razones de seguridad, ya que se pueden realizar configuraciones que afecten el funcionamiento del sistema operativo.

2. Comando **sudo**

`sudo` es la forma abreviada de *superusuario do* y es un comando que permite a los usuarios ejecutar programas con los privilegios de seguridad del superusuario *root*. Por lo tanto, algunos autores mencionan que un *sudoer* es un usuario que tiene tales derechos y siempre deben de utilizar la palabra clave `sudo` antes de ejecutar cualquier comando administrativo sin la necesidad de salir de sesión y volver a ingresar como *root*.

Aunque existe el comando `su` (*switch user*) que permite iniciar sesión como *root* es una gran falla de seguridad utilizarlo para gestiones administrativas ya se puede olvidar cerrar la sesión y un simple error puede borrar archivos importantes o todo el sistema de archivos.

No todos los usuarios deben tener privilegios para ejecutar comandos de administración, por lo que durante la instalación del sistema operativo, el primer usuario que se crea tendrá privilegios sudo por defecto. Para adminsitrar usuarios adicionales, se puede realizar alguna de las siguientes configuraciones:

1. Agregandolos al archivo *sudoers*: archivo de configuración que define qué usuarios pueden utilizar sudo y cómo.
2. Siendo miembro del grupo `sudo`: grupo especial de usuarios con privilegios para ejecutar el comando **sudo**.

2.1. Archivo **sudoers**

Para agregar un usuario al archivo `sudoers` se debe de seguir los siguientes pasos:

1. Ejecutar el siguiente comando para iniciar sesión como *root*:

```
$ su
```

Código fuente 1: Inicio de sesión como root

2. Ingresar la contraseña de *root* para iniciar sesión.
3. Editar el archivo `/etc/sudoers` con el siguiente comando:

```
$ visudo
```

Código fuente 2: Edición del archivo `sudoers` de forma segura

   El comando anterior nos abrirá el editor de texto por defecto del sistema operativo (`vi` o `nano`).

4. Buscar la línea que contiene `root ALL=(ALL:ALL) ALL` y agregar una nueva línea debajo de ella con el siguiente formato:

```
<nombre-usuario> ALL=(ALL:ALL) ALL
```

Código fuente 3: Edición del archivo `sudoers` de forma segura

Sustituir `<nombre-usuario>` por el nombre del usuario que se desea agregar al archivo `sudoers`.

5. Guardar los cambios y salir del editor.

Este archivo nos permite limitar de manera específica que permisos tendrá el usuario, indicando que comando o comandos específicos puede ejecutar, así como si requiere o no una contraseña para ejecutarlos. En el ejemplo dado:

- `ALL=`: significa que <nombre-usuario> puede ejecutar comandos desde cualquier terminal (*host*).
- `(ALL:ALL)`: significa que <nombre-usuario> puede ejecutar comandos como cualquier usuario y grupo.
- `ALL` significa que <nombre-usuario> puede ejecutar cualquier comando.

Nota: es importante tener en cuenta que este archivo de configuración es crítico y cualquier error en su edición puede dejar el sistema inutilizable. Por lo tanto, es recomendable no editarlo directamente con `nano` o `vi` y realizar una copia de seguridad del archivo antes de realizar cualquier cambio.

2.2. Grupo sudo

Para agregar un usuario al grupo `sudo` se debe de seguir los siguientes pasos:

1. Ejecutar el siguiente comando para iniciar sesión como *root*:

```
$ su
```

Código fuente 4: Inicio de sesión como root

2. Ingresar la contraseña de *root* para iniciar sesión.
3. Ejecutar el siguiente comando para agregar el usuario deseado al grupo:

```
$ usermod -aG sudo <nombre-usuario>
```

Código fuente 5: Modificación de usuario para seer agregado a un grupo

Sustituir `<nombre-usuario>` por el nombre del usuario que se desea habilitar el uso del comando ***sudo***.

Una vez realizadas estas configuraciones, el usuario agregado podrá ejecutar comandos de administración utilizando el comando `sudo`.

3. Administración de usuarios con privilegios sudo

Existen varias ventajas de agregar usuarios al archivo `sudoers`, entre las que destacan las siguientes:

- Se mejora la seguridad del sistema, ya que solo se otorgar privilegios sudo a los usuarios que necesitan realizar tareas administrativas.
- Se puede personalizar los permisos de los usuarios, especificando qué comandos pueden ejecutar y cuándo pueden hacerlo.
- Se facilita la supervisión de los usuarios con privilegios ***sudo***, ya que se guarda en una bitácora todos los comandos realizados en el archivo `/var/log/auth.log`.

Referencias

[1] Red Hat, Inc. «Capítulo 8. Conceder acceso sudo a un usuario.» (2024), dirección: https://docs.redhat.com/es/documentation/red_hat_enterprise_linux/8/html/configuring_basic_system_settings/granting-sudo-access-to-a-user_configuring-basic-system-settings#granting-sudo-access-to-a-user_configuring-basic-system-settings. (accedido: 15.02.2025).

[2] T. Kamunya. «Cómo añadir usuarios a Sudoers en Ubuntu.» (2024), dirección: https://geekflare.com/es/add-users-to-sudoers-in-ubuntu/. (accedido: 15.02.2025).

[3] E. Giner. «Cómo añadir un usuario a "sudoers", para darle permisos de administrador.» (2016), dirección: https://slimbook.com/en/blog/guides-2/post/como-anadir-un-usuario-a-sudoers-para-darle-permisos-de-administrador-47. (accedido: 15.02.2025).