Cuenta *root*

La cuenta *root* ofrece un acceso completo al sistema —acceso a **todos** los archivos del sistema (binarios, archivos de configuración, archivos del sistema, entre otros); administración de servicios; gestión de permisos y propiedades— por lo que es una cuenta muy poderosa. Se recomienda ejecutar comandos y acciones que requieran privilegios *root* bajo la figura de la utilidad **sudo**.

Operaciones que requieren privilegios root

Algunas de las operaciones que requieren privilegios *root* incluyen:

Crear, eliminar y administrar cuentas de otros usuarios.
Modificar los permisos y propietarios de cualquier archivo o directorio.
Instalar paquetes manualmente y acceder a archivos fuente en el *filesystem*.
Modificar o eliminar archivos del sistema.
Detener, iniciar o reiniciar servicios del sistema.

Una cuenta de usuario regular puede realizar otras operaciones como: uso de dispositivos o impresoras, administración de archivos para los cuales posean los permisos adecuados, uso de clientes de red, instalación de paquetes de software y cambios en algunos ajustes del sistema.

Elevando los privilegios de un usuario regular

Elevando privilegios con **su**

Una de las formas de elevar los privilegios de un usuario regular es usando el comando `su` (*switch user* o "cambiar de usuario). Este comando simplemente ejecuta una nueva sesión en la consola shell como otro usuario, en general, el usuario *root*. De esta manera, simplemente nos convertimos en el usuario *root* hasta cerrar esa sesión. Por razones de seguridad y estabilidad no es una buena práctica utilizar este comando ya que equivale a iniciar sesión como *root*, y ya hemos explicado algunas razones de peso para no utilizar

esta cuenta. Por ejemplo: digamos que un usuario regular que no tiene experiencia en la administración de sistemas Linux quiere borrar un archivo personal y en cambio ejecuta una eliminación recursiva y forzada (`rm -rf`) de archivos del sistema. Esto es potencialmente catastrófico y podría dañar el sistema por completo.

Tenga en cuenta que para usar el comando `su` el usuario debe conocer la contraseña del usuario *root*.

La sintaxis de este comando es la siguiente:

```
su - miusuario
```

Una vez ejecutado el comando se le pedirá la contraseña del usuario en cuestión. El guion (`-`) permite el inicio de un nuevo shell de conexión con las preferencias del usuario `miusuario`. Si omite el guion no se cargará la sesión desde el directorio `home` del usuario en cuestión y no se inicializarán las variables de preferencia para ese usuario (`HOME, SHELL, USER, LOGNAME and PATH`).

Si ejecuta el comando `su` o `su -` por sí solo, sin especificar ningún usuario, se da por sentado que está invocando al usuario *root*.

Elevando privilegios con **sudo**

Otra forma más segura de otorgar privilegios *root* —temporalmente— a un usuario es usando el comando `sudo` (**s**uper **u**ser **do**, por sus siglas en inglés). Esta es la forma recomendada y la mejora práctica para ejecutar acciones con privilegios elevados. La gran diferencia, es que los comandos precedidos con `sudo` son ejecutados por el propio usuario, no por *root*. ¿Y cuál es la ventaja de esto? Son muchas ventajas, en general relacionadas con la seguridad de su sistema. Aprenderá más a medida que lee esta guía.

Para ejecutar un comando que requiera privilegios elevados, simplemente use la palabra `sudo` delante del comando:

```
sudo comando_root
```

Cuando lo haga se le pedirá su contraseña personal, se ejecutará el comando y luego usted seguirá siendo un usuario regular. Es decir, si debe ejecutar 100 comandos que requieran privilegios *root*, tendrá que precederlos todos con la utilidad `sudo`.

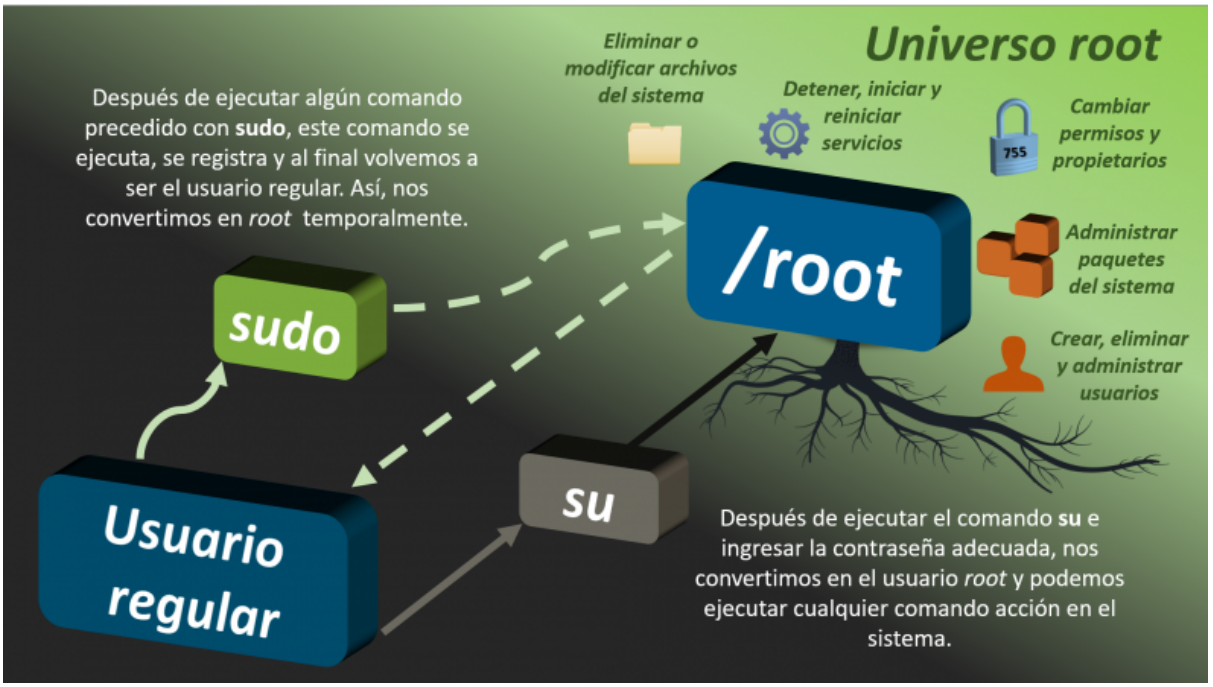
En la mayoría de las distribuciones de Linux, la utilidad *sudo* debe habilitarse manualmente para los usuarios que lo requieran. En la siguiente sección de este tutorial explicamos cómo activar esta opción para un usuario regular.

Diferencias entre sudo y su

Algunas de las diferencias entre estas dos utilidades se enumeran a continuación:

sudo	su
Los comandos son ejecutados por un usuario regular que debe ser parte de un grupo de usuarios con la posibilidad de utilizar `sudo` (**sudoers**).	Sirve para cambiar de un usuario a otro, generalmente se pasa de un usuario regular al usuario *root*.
Solo es necesaria la contraseña del usuario actual.	Se requiere conocer la contraseña del usuario root, la cual no debería ser revelada a ningún usuario regular.
Se pueden registrar las acciones ejecutadas bajo la figura de `sudo`.	Las posibilidades para registrar eventos son más limitadas.
Ofrece varias características que proveen un mayor control de lo que hacen —y pueden hacer— los usuarios.	Una vez que accede como *root*, no hay control de lo que puede hacer en el sistema.

Para comprender las diferencias de forma más visual observe la siguiente gráfica:



¿Qué ofrece la utilidad sudo?

Una de las ventajas que tiene `sudo` es la capacidad de hacer seguimiento a los intentos fallidos de acceso *root*. Intentemos ejecutar un comando que requiere privilegios elevados usando el comando `sudo`, por ejemplo reiniciar el servidor Apache:

```
sudo service apache2 restart
```

Obtenemos lo siguiente:

```
[sudo] password for miusuario:
miusuario is not in the sudoers file.  This incident will be reported.
```

La respuesta indica que el usuario `miusuario` no está en el archivo `sudoers` y que el incidente será reportado. Los archivos de configuración de **sudo** están almacenados en el archivo `/etc/sudoers` y en el directorio `/etc/sudoers.d/`. El archivo `sudoers` es un archivo que incluye una lista de los usuarios que pueden usar el comando `sudo` para

obtener privilegios *root* (no restrictivo). Por lo tanto, antes de ejecutar cualquier comando con `sudo`, debe agregar al usuario al archivo `sudoers`.

Estos errores suelen registrarse en `/var/log/auth.log`, `/var/log/messages` o `/var/log/secure` dependiendo de su sistema. Por ejemplo, filtremos los mensajes registrados relacionados con el comando `sudo` en busca del error obtenido anteriormente:

```
cat /var/log/secure | grep sudo
```

Obtenemos:

```
Oct 21 00:18:53 servidor sudo:  miusuario : user NOT in sudoers ;
TTY=pts/1 ; PWD=/home/miusuario ; USER=root ;
COMMAND=/sbin/service restart apache2
```

Podemos observar que esta entrada de *log* se incluye: información de la fecha y hora de ejecución (`Oct 21 00:18:53`), nombre del terminal (`servidor`), el nombre del usuario que intentó ejecutar el comando con `sudo` (`miusuario`), el directorio desde el cual se intentó ejecutar el comando (`PWD=/home/miusuario`), el usuario al que se quería invocar (`root`) y el comando con sus argumentos (`/sbin/service restart apache2`).

El archivo **sudoers**

Como ya mencionamos este archivo contiene una lista de los usuarios que pueden ejecutar el comando **sudo** y cuáles son los alcances de sus privilegios. Cuando un usuario ejecuta un comando precedido por `sudo`, el sistema busca en el archivo `/etc/sudoers` y los archivos en `/etc/sudoers.d` para comprobar la información allí plasmada y otorgar o denegar el permiso para usar el comando.

La estructura básica para los usuarios enumerados en este archivo es la siguiente:

```
quién dónde = (como_quién) qué
```

Por ejemplo, un usuario con privilegios administrativos absolutos —como *root*— tendrá la siguiente estructura:

```
root    ALL=(ALL)       ALL
```

Considerando que `ALL` significa "todos", esto quiere decir que la regla aplica al usuario *root*, en **todos** los *hosts*, *root* puede ejecutar comandos como **todos** los usuarios y se pueden ejecutar **todos** los comandos.

Esta guía da un enfoque muy general del archivo `sudoers` y no pretende detallar su estructura o personalización. La documentación de este archivo es muy extensa y hay muchas formas de editar, personalizar y añadir usuarios a este archivo. Para más información consulte la sección de Recursos adicionales.

Agregar un usuario a la lista de sudoers

Nota: Los comandos mencionados en esta sección deben ser ejecutados con privilegios *root*. Esta es una de las excepciones para usar la cuenta *root*, ya que agregar un usuario a la lista de *sudoers* suele ser una de las primeras acciones durante la configuración inicial de un servidor.

Utilizando **visudo**

La forma **recomendada y segura** de editar el archivo `sudoers` es utilizando el comando `visudo`. Esto se debe a que `visudo` asegura que una sola persona —con los permisos adecuados— esté editando el archivo al mismo tiempo. Además no permite reescribir los cambios y salir si hay algún error en la edición del archivo.

Para usar este comando simplemente ejecute:

```
visudo
```

Se abrirá el archivo `/etc/sudoers` con la misma interfaz y uso del editor **vi**. Busque la siguiente sección dentro del archivo:

Extracto del archivo: **/etc/sudoers** (*el archivo se abre usando el comando* `visudo`)

```
## Sudoers allows particular users to run various commands as
## the root user, without needing the root password.

...

## Next comes the main part: which users can run what software on
## which machines (the sudoers file can be shared between multiple
## systems).
## Syntax:
##
##      user    MACHINE=COMMANDS
##
## The COMMANDS section may have other options added to it.
##
## Allow root to run any commands anywhere
root    ALL=(ALL)       ALL
```

Coloque el cursor debajo de la línea `root ALL=(ALL) ALL` y presione `i` para entrar en el modo de inserción. Luego escriba la siguiente línea sustituyendo `miusuario` con el nombre de usuario real que desea agregar:

```
miusuario    ALL=(ALL)       ALL
```

Presione `ESC` para salir del modo de inserción. A continuación presione `wq` + *Enter* para guardar y salir. Para más información sobre el uso del editor `vi` visite el siguiente tutorial: Guía práctica de los editores de texto nano y vi en Linux.

¡Felicidades, ahora el usuario `miusuario` podrá ejecutar comandos *root* a través de `sudo`!

Usando un grupo con privilegios administrativos

Algunos sistemas vienen configurados con grupos que permiten la ejecución de comandos con el prefijo `sudo`. Agregar usuarios a estos grupos es la forma más fácil y rápida de darles privilegios **sudo**, pero esta opción no está disponible en algunas versiones de ciertas distribuciones Linux. Siga las instrucciones según su sistema, si su sistema no provee esta opción, tendrá que usar visudo.

Debian/Ubuntu

En estos sistemas, el grupo que otorga permisos administrativos y agrega al usuario a la lista de **sudoers** se llama simplemente `sudo`. Podemos agregar un usuario a este grupo usando el siguiente comando:

```
usermod -aG sudo miusuario
```

Recuerde sustituir `miusuario` con el nombre real del usuario de interés. También puede utilizar el siguiente comando:

```
gpasswd -a miusuario sudo
```