Linux para administradores (intermedio)

Manuel Domínguez

Bienvenidos!

Esta sección corresponde con la **Gestión de usuarios**.

Y en esta clase, vamos a explicar cómo se gestionan **las cuentas de usuario con sudo.**

1.- Introducción

En los sistemas Linux **existe un usuario administrador** llamado root que tiene el control de todo el sistema.

A veces puede ser interesante que otro usuario pueda ejecutar determinados comandos como si fuese el root.

La herramienta sudo, nos va permitir delegar algunas funciones que realiza el root a otros usuarios. (Administrador y un técnico)

1.- Introducción

En Ubuntu:
El primer usuario que se crea ya tiene privilegios como root.
Pertenece al grupo sudo.

En Debian;
El primer usuario que se crea no tiene privilegios de root.

2.- Instalación del comando sudo.

1.- #apt update → Para actualizar la lista de paquetes.

2.- # apt policy sudo → Para ver si está instalado.

3.- #apt install sudo → Para instalarlo.

3.- Usuarios con privilegios sudo.

Podemos comprobar si el usuario, **usuario**, tiene privilegios sudo:

```
usuario@debian:~$ sudo -l

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for usuario:
Sorry, user usuario may not run sudo on debian.
```

4.- Fichero de configuración.

/etc/sudoers → cat /etc/sudoers

Para editarlo, utilizaremos:

visudo → Se trata de un editor especial, que únicamente sirve para editar este archivo.

 # visudo –f /etc/sudoers

Para comprobar la sintaxis, utilizaremos: **visudo -c**

4.- Fichero de configuración.

Tiene varias partes diferenciadas: **Defaults, Alias y Reglas de acceso**

```
Defaults   env_reset
Defaults   mail_badpass
Defaults
secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"

# Host alias specification
# User alias specification
# Cmnd alias specification
# User privilege specification
root        ALL=(ALL:ALL) ALL
# Allow members of group sudo to execute any command
%sudo       ALL=(ALL:ALL) ALL
```

4.- Fichero de configuración.

Podemos comprobar los usuarios, que tienen privilegios como root:

#getent group sudo

Cualquier usuario, que metamos en este grupo tendrá privilegios de root.

Práctica:

1.- Creamos un usuario bob (bob)
2.- Lo añadimos al grupo sudo.
3.- bob$sudo adduser prueba
4.-bob$sudo userdel -r prueba

4.- Fichero de configuración.

/etc/sudoers

Las reglas de acceso tendrán el siguiente formato:

usuario equipo = (usuario:grupo) comando

usuario: Es el nombre de usuario, alias o grupo de usuarios.
equipo: Es el nombre del equipo , alias, o una dirección IP.
(usuario:grupo): Indica el usuario y grupo bajo el que se ejecuta el comando.
comando: comando, o alias de comandos que permite ejecutar.

5.- Ejemplos de sudo

Antes de modificar dicho fichero, es conveniente hacer una copia:

cp /etc/sudoers /etc/sudoers.ORIGINAL

5.- Ejemplos de sudo-1

Práctica: Permitimos que el usuario usuario tenga privilegios de root

1 .- Editamos el fichero: **#visudo -f /etc/sudoers**

2.- Añadimos la línea: El usuario usuario, en cualquier host, puede ejecutar cualquier comando, de cualquier usuario, incluidos los de root.

```
# User privilege specification
root    ALL=(ALL:ALL) ALL
usuario ALL=(ALL) ALL
```

3.- Lo guardamos.

4.- Chequeamos la sintaxis con: **#visudo -c**

5.- Comprobamos que tiene privilegios: **$sudo -l**

5.- Ejemplos de sudo-1

Práctica: Permitimos que el usuario usuario tenga privilegios de root

6.- Realizamos alguna operación:

$ sudo adduser arenitas → Nos permite crear una cuenta de usuario.

$sudo userdel -r arenitas

5.- Ejemplos de sudo-2

Práctica: Permitir que usuarios de un grupo puedan configurar la red de los hosts.

Preparamos el entorno:

1.- Creamos dos usuarios: **patricio y calamardo.**

2.- Creamos un grupo: **tecnicos** y añadimos a esos usuarios.

```
#addgroup tecnicos
#adduser patricio  tecnicos
 #adduser calamardo  tecnicos
# getent group tecnicos
```

continúa

5.- Ejemplos de sudo-2

Práctica: Permitir que usuarios de un grupo puedan configurar la red y reiniciar los servicios.

3.- Editamos el fichero: **#visudo -f /etc/sudoers**
4.- Añadimos las líneas: Cmnd_**ALias RED=/bin/ip, /bin/systemctl networking** Permitimos que **el grupo tecnicos** pueda ejecutar sobre cualquier host, los comandos incluidos en el alias RED (Mayúsuclas)

```
# Cmnd alias specification
Cmnd_Alias RED=/bin/ip, /bin/systemctl
# User privilege specification
root    ALL=(ALL:ALL) ALL
usuario ALL=(ALL) ALL
# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL
%tecnicos ALL=RED
```

5.- Ejemplos de sudo-2

Práctica: Permitir que usuarios de un grupo puedan configurar la red y reiniciar los servicios.

5.- Lo guardamos, y chequeamos la sintaxis con: **#visudo -c**

6.- Comprobaciones: patricio$ sudo -l

patricio$ ip link set enp0s3 down → No deja
patricio$ sudo ip link set enp0s3 down → Sí deja

patricio$ systemctl restart networking → No deja
patricio$sudo systemctl restart networking → Sí deja

5.- Ejemplos de sudo-3

Práctica: Permitir que puedan modificar el archivo /etc/network/interfaces.

1.- Vamos a permitirles que puedan modificar el fichero:
/etc/network/interfaces

2.- Añadimos:
Cmnd_Alias RED=/bin/ip, /bin/systemctl, /bin/nano /etc/network/interfaces

3.- Lo comprobamos:
patricio**$nano /etc/network/interfaces**
patricio**$ sudo nano /etc/network/interfaces**

5.- Ejemplos de sudo-4

Práctica: Permitir que los tecnicos no tengan que introducir la contraseña.

1.- Añadimos:
%tecnicos ALL=NOPASSWD:RED

3.- Lo comprobamos: no nos pide contraseña

patricio**$ sudo nano /etc/network/interfaces**

5.- Ejemplos de sudo-5

Práctica: Limitar el número de intentos para escribir correctamente la contraseña.

1.- Añadimos: **Defaults:ALL passwd_tries=2**

Debemos quitar la opción NOPASSWD

2.- Ahora sólo tendrá dos intentos para escribir la contraseña.

3.- Lo comprobamos:

patricio**$ sudo nano /etc/network/interfaces** → Si metemos 2 veces la contraseña mal. nos expulsa del sudo.

RETO

Práctica:

1.- Os propongo que permitáis a los usuario del grupo tecnicos, cambiar la contraseña de cualquier usuario, pero no la de root.

Pista:

Para cambiar una contraseña de cualquier usuario, utilizamos: /bin/passwd *
Para denegar un comando, ponemos delante !

Linux para administradores (intermedio)

Manuel Domínguez

Despedida

Hemos llegado al final de este vídeo..

Nos vemos en el siguiente.