SUDO, VISUDO Y SUDOERS

El programa **sudo** (de las siglas en inglés de ***s**uper**u**ser* -o ***s**ubstitute **u**ser- **do***) es una utilidad de los sistemas operativos tipo Unix, como Linux, BSD, o Mac OS X, que permite a los usuarios ejecutar programas con los privilegios de seguridad de otro usuario (normalmente el usuario **root**) de manera segura. Se instala por defecto en **/usr/bin**.

En ambientes donde varios usuarios usan uno o más sistemas GNU/Linux, es necesario otorgar distintos permisos o privilegios para que estos puedan hacer uso de comandos propios del usuario administrador 'root'.

No todos los usuarios pueden tener la contraseña de root para que los usuarios puedan hacer uso de los programas propios de sus funciones pero que son propiedad de 'root'.

Por otro lado, hacer uso del comando su tampoco es práctico porque es lo mismo, necesitan la contraseña de root, así que la mejor alternativa es hacer uso de sudo.

¿Exactamente que es y que hace sudo? **sudo permite implementar un control de acceso de que usuarios ejecutan que comandos**. Si un usuario normal desea ejecutar un comando de root (o de cualquier otro usuario), sudo verifica en su lista de permisos y si está permitido la ejecución de ese comando para ese usuario, entonces sudo se encarga de ejecutarlo. Es decir, sudo es un programa que basado en una lista de control **(/etc/sudoers**) permite (o no) la ejecución al usuario que lo invocó sobre un determinado programa propiedad de otro usuario, generalmente del administrador del sistema '**root**'.

sudo, para fines prácticos se puede dividir en tres partes:

- **sudo**, el comando con permisos de SUID, que los usuarios usan para ejecutar otros comandos a los que se les permite usar.
- **visudo**, el comando que permite al administrador modificar /etc/sudoers.
- /etc/sudoers, el archivo de permisos que le indica a sudo que usuarios ejecutan cuáles comandos.

sudo

sudo (SUperuser DO) lo ejecuta un usuario normal, al que se supone tiene permisos para ejecutar cierto comando. Entonces, sudo requiere que los usuarios se autentifiquen a si mismos a través de su contraseña para permitirles la ejecución del comando. Veamos un ejemplo:

```
$ sudo /sbin/ifconfig
Password:
eth0      Link encap:Ethernet  HWaddr 4C:00:10:60:5F:21
          inet addr:200.13.110.62  Bcast:200.13.110.255  Mask:255.255.255.0
          inet6 addr: fe80::4e00:10ff:fe60:5f21/64 Scope:Link
...
```

Se usa el comando **sudo** seguido del comando (con toda su ruta si es que este no esta en el PATH del usuario) al que se tiene permiso. ***sudo*** pregunta por la contraseña del usuario que ejecuta el comando y listo.

Después dispones de 5 minutos para volver a usar el mismo comando u otros a los que tuvieras derecho, sin necesidad de escribir la contraseña de nuevo. Si quieres prolongar el tiempo otros 5 minutos usa la opción ***sudo -v*** (validate) y si ya quieres acabar con el tiempo puedes poner ***sudo -k*** (kill).

Para saber que comandos puedo utilizar: ***sudo –l***

```
$ sudo -l
User sergio may run the following commands on this host:
    (root) /sbin/ifconfig
    (root) /sbin/lspci
```

visudo

Permite la edición del archivo de configuración de **sudo sudoers**. Se utiliza el editor visudo ya que bloquea el archivo **/etc/sudoers** de tal manera que nadie más lo puede utilizar, y además antes de cerrar el archivo comprueba su sintaxis.

Si al cerrar visudo detecta un error nos mostrará la línea donde se encuentra, y la pregunta "What now?":

```
>>> sudoers file: syntax error, line 15 <<<
What now?
```

Se tienen tres opciones para esta pregunta:

- **e** - edita de nuevo el archivo, colocando el cursor en la línea del error (si el editor soporta esta función)
- **x** - salir sin guardar los cambios.
- **Q** - salir y guarda los cambios.

Sudoers

Archivo de configuración de ***sudo***, generalmente ubicado bajo **/etc** y se modifica a través del uso de ***visudo***.

En este archivo se establece:

- quien (usuarios) puede ejecutar
- que (comandos)
- de qué modo (opciones)

generando efectivamente una lista de control de acceso que puede ser tan detallada como se desee.

Es más fácil entender ***sudo*** si dividimos en tres partes su posible configuración, estás son: (solo es obligatoria la tercera)

- Alias
- Opciones (Defaults)
- Reglas de acceso

Alias

Un alias se refiere a:

- un usuario
- un comando
- un equipo

El alias engloba bajo un solo nombre (nombre del alias) una serie de elementos que después en la parte de definición de reglas serán referidos aplicados bajos cierto criterio. La forma para crear un alias es la siguiente:

tipo_alias NOMBRE_DEL_ALIAS = elemento1, elemento2, elemento3, ... elementoN

El tipo_alias define los elementos, es decir, dependiendo del tipo de alias serán sus elementos.

Los tipos de alias son cuatro y son los siguientes:

- **Cmnd_Alias** - define alias de comandos.
- **User_Alias** - define alias de usuarios normales.
- **Runas_Alias** - define alias de usuarios administradores o con privilegios.
- **Host_Alias** - define alias de hosts o equipos.

El **NOMBRE_DEL_ALIAS** puede llevar letras, números o guión bajo (_) y **DEBE** de comenzar con una letra mayúscula, se acostumbra a usarlos siempre en mayúsculas.

Cmnd_Alias

Definen uno o más comandos y otros alias de comandos que podrán ser utilizados después en alias de usuarios. Ejemplos:

Cmnd_Alias WEB = /usr/sbin/apachectl, /usr/sbin/httpd, sudoedit /etc/httpd/

Cmnd_Alias APAGAR = /usr/bin/shutdown -h 23\:00

User_Alias

Definen a uno o más usuarios, grupos del sistema (indicados con %), grupos de red (netgroups indicados con +) u otros alias de usuarios. Ejemplos:

User_Alias MYSQL_USERS = andy, marce, juan, %mysql

User_Alias ADMIN = sergio, ana

User_Alias TODOS = ALL, !samuel, !david

User_Alias OPERADORES = ADMIN, alejandra

Runas_Alias

Funciona exactamente igual que User_Alias, la única diferencia es que es posible usar el ID del usario UID con el caracter '#'.

Runas_Alias OPERADORES = #501, fabian

Host_Alias

Definen uno o más equipos u otros alias de host. Los equipos pueden indicarse por su nombre (si se encuentra en /etc/hosts) por nombre de dominio, si existe un resolvedor de dominios, por dirección IP, por dirección IP con máscara de red. Ejemplos:

Host_Alias LANS = 192.168.0.0/24, 192.168.0.1/255.255.255.0

Host_Alias WEBSERVERS = 172.16.0.21, web1 : DBSERVERS = 192.168.100.10, dataserver

Opciones (defaults)

Las opciones o defaults permiten definir ciertas características de comportamiento para los alias previamente creados, para usuarios, usuarios privilegiados, para equipos o de manera global para todos.

Las opciones o defaults es posible establecerlos en cuatro niveles de uso:

- De manera global, afecta a todos
- Por usuario
- Por usuario privilegiado
- Por equipo (host)

Reglas de acceso

Las reglas de acceso definen que usuarios ejecutan que comandos bajo que usuario y en que equipos.

La sintaxis a seguir es:

<n_usuario, % grupo> <maquina> = (usuario suplantado) <comando>

Ej 1: usuario host = comando1, comando2, ... comandoN

Sintaxis básica, 'usuario' puede ser un usuario, un alias de usuario o un grupo (indicado por %), 'host' puede ser ALL cualquier equipo, un solo equipo, un alias de equipo, una dirección IP o una definición de red IP/máscara, 'comandox' es cualquier comando indicado con su ruta completa. Si se termina en '/' como en /etc/http/ entonces indica todos los archivos dentro de ese directorio.

Ej 2: daniela ALL = /sbin/iptables

Usuario 'daniela' en cualquier host o equipo puede utiliar iptables.

Ej 3: ADMIN ALL = ALL

Los usuarios definidos en el alias 'ADMIN' desde cualquier host pueden ejecutar cualquier comando.

Ej 4: SUPERVISORES PRODUCCION = OPERACION

Una regala formada solo por alias. En el alias de usuario 'SUPERVISORES' los usuarios que esten indicados en ese alias, tendrán permiso en los equipos definidos en el alias de host 'PRODUCCION', de ejecutar los comandos definidos o listados en el alias de comandos 'OPERACION'.

Solicitud de contraseña

Una vez que has escrito de forma correcta la regla de suplantación de la identidad, puedes con el usuario especificado ejecutar ese comando.

Por ejemplo:

luis ALL = (ALL) /usr/sbin/groupadd

Significa que el usuario luis va a poder en todos los equipos suplantar la identidad que cualquier persona y va a poder añadir grupos.

Para poder ejecutar el comando debe poner:

sudo /usr/sbin/groupadd grupo6

A continuación le pide a luis su contraseña de usuario y se la pedirá cada vez que intente ejecutar un comando suplantando la identidad del root.

Para que no le pida SU contraseña podemos poner en la regla de especificación:

luis ALL = (ALL) NOPASSWD: /usr/sbin/groupadd

OJO: Si no he modifica el archivo visudo (/etc/sudoers) cualquier usuario puede intentar ejecutar un comando del root poniendo sudo delante y sin ser necesario poner la ruta completa. Pero le pedirá la contraseña del root

sudo groupadd y le pedirá la contraseña del root