

La utilidad sudo

Antonia Estero Botaro y Antonio García Domínguez

Seguridad y Competencias Profesionales

Curso 2009-2010

29 octubre 2009

Hay ciertas actividades de un sistema Linux que sólo puede llevar a cabo el administrador del sistema, utilizando para ello el identificador de usuario **root**. El programa *sudo* proporciona un método para que usuarios diferentes de **root** puedan realizar ciertas acciones que en principio están restringidas a éste, es decir, nos permite asignar privilegios a cualquier cuenta de usuario para que éste pueda ejecutar ciertos programas específicos.

Algunos ejemplos de la utilidad que puede tener *sudo* son:

- El administrador del sistema puede realizar ciertas tareas de administración sin necesidad de cambiar su identificador a **root**.
- Los usuarios pueden montar disquetes o CD-ROMs en sistemas en los que no tienen acceso como administradores.
- Los usuarios pueden acceder a las herramientas de configuración de ciertos programas.

El programa *sudo* utiliza el fichero de configuración `/etc/sudoers` para determinar qué usuarios pueden realizar ciertas tareas. La página del manual SUDOERS(5) describe la sintaxis de este fichero, que es bastante compleja.

El fichero contiene dos tipos de entradas:

- Alias.
- Especificaciones de privilegios de usuarios, sirven para especificar qué órdenes pueden ejecutar los usuarios y en qué máquinas.

Mediante la definición de alias es posible que una sola palabra represente:

- Un conjunto de usuarios.
- Un conjunto de máquinas.
- Un conjunto de programas.

Para definir un alias se utilizará:

```
Tipo_Alias Nombre = item1, item2, item3 : Nombre = item4, item5
```

donde TIPO_ALIAS puede ser «*User_Alias*», «*Host_Alias*», o «*Cmnd_Alias*». NOMBRE es el nombre del alias y es una cadena que puede contener letras mayúsculas, dígitos y el carácter '_'. Un «*Nombre*» debe comenzar por una letra mayúscula.

Un ejemplo de definición de alias podría ser:

```
Host_Alias AULA = aula01, aula02, aula03, aula04, ...
```

Las líneas de especificación de privilegios de usuarios tienen el formato:

```
usuario máquina = lista_de_órdenes
```

Así si queremos que todos los usuarios del grupo **users** puedan montar un disquete o un CD-ROM en cualquier máquina de las especificadas en el alias AULA, pondremos:

```
% users AULA = /sbin/mount /media/floppy, /sbin/mount /media/cdrom
```

Para que esta línea de **/etc/sudoers** funcione correctamente es necesario que se haya indicado en el fichero **/etc/fstab** dicho punto de montaje para el disquete y el CD-ROM.

Una forma rápida de especificar a todos los usuarios es mediante la etiqueta «*ALL*».

Por ejemplo, la línea siguiente permitiría a todos los usuarios hacer las mismas acciones anteriores desde cualquier máquina especificada en el alias AULA:

```
ALL AULA = /sbin/mount /media/floppy, /sbin/mount /media/cdrom
```

Por omisión, cuando un usuario quiera ejecutar una de las órdenes que tiene permitidas en **/etc/sudoers** se le pedirá su contraseña, a no ser que se indique lo contrario mediante la etiqueta **NOPASSWORD**.

Para ejecutar una de estas órdenes el usuario debe darla precedida de la orden *sudo*.

Para editar el fichero **/etc/sudoers** es necesario utilizar la orden *visudo*, este programa bloquea el fichero para que ningún otro usuario lo pueda editar simultáneamente y hace comprobaciones de la sintaxis del fichero.

Puede encontrar más información acerca de la orden *sudo* y del fichero **sudoers** en las páginas correspondientes del manual en línea.