

El usuario root

Miguel Ortuño
Escuela de Ingeniería de Fuenlabrada
Universidad Rey Juan Carlos

Septiembre de 2024



© 2022 Miguel Angel Ortuño Pérez.
Algunos derechos reservados. Este documento se distribuye bajo la
licencia *Atribución-CompartirIgual 4.0 Internacional* de Creative
Commons, disponible en
<https://creativecommons.org/licenses/by-sa/4.0/deed.es>

- 1 El administrador
 - Provisionamiento de máquinas
 - Procesos de root, método tradicional
 - Procesos de root con sudo
 - Algunas ambigüedades

El administrador

Persona responsable de:

- Instalación del sistema
- Incorporar nuevo *hardware* y *software*
- Añadir y eliminar usuarios
- Salvaguarda de información
- Seguimiento y monitorización del sistema
- Política de seguridad
- Resolución de problemas
- Soporte técnico

Hay tareas que solo el usuario root puede hacer. Entre otras:

- Editar ficheros de configuración de la máquina, como los interfaces de red, sistemas de ficheros, arranque del sistema...
- Iniciar y detener demonios (en los casos habituales, aunque excepcionalmente un usuario ordinario podría gestionar algún demonio)
- Instalar paquetes de software (para toda la máquina)
- Crear, modificar, eliminar cuentas de usuario

Provisionamiento de máquinas

Una de las tareas típicas del administrador es *provisionar una máquina*.

Es el proceso de preparar y configurar un sistema informático, físico o virtual, para que esté listo para su uso según nuestras necesidades

Tareas típicas:

- Asignación de recursos: Determinar y asignar la cantidad de CPU, memoria, almacenamiento y red que se destinará a la máquina.
- Instalación del sistema operativo y software
- Configuración de red y seguridad: Configurar direcciones IP, establecer reglas de firewall, definir políticas de acceso y autenticación, y aplicar parches de seguridad.

- Automatización y gestión de configuración: Utilizar herramientas de automatización (como Ansible, Puppet, Chef o scripts personalizados) para configurar y aplicar políticas, paquetes y configuraciones de manera reproducible y escalable.
- Integración y monitoreo: Conectar la máquina a sistemas de monitoreo y a la infraestructura de gestión para asegurar su rendimiento y disponibilidad.

Todo esto suele hacerse de forma automática. O a mano en algunos casos.

Procesos de root, método tradicional

- Por motivos de seguridad, el administrador debería lanzar procesos como root solo para lo que sea imprescindible, el tiempo imprescindible. El resto del tiempo, es preferible trabajar con una cuenta de usuario ordinario

Formas tradicionales de lanzar procesos como root

- ① Iniciar sesión con usuario root y contraseña de root (no recomendable, muchas veces no permitido)
- ② `su`
Solicita la contraseña de root y ejecuta una shell como root. Todos los procesos lanzados serán de root, hasta que se cierre la shell

El comando `su` también tiene otro uso:

- `su jperez`
Pide la contraseña de jperez, si es correcta, la sesión pasa a ser propiedad de jperez

Procesos de root con sudo

Para mejorar la seguridad, aparece sudo, que evita que haya una sesión de root siempre abierta

- `sudo <orden>`
Permite ejecutar una única orden como root, desde una sesión de usuario ordinario
- `sudo` no pregunta la contraseña de root, no es necesario conocerla (de hecho, en los sistemas con sudo, el usuario root no suele tener contraseña)
- `sudo` solicita la contraseña del propio usuario que está lanzando sudo
 - Para llamarle la atención y hacerle tener más cuidado
 - Para verificar que la persona que está en el terminal sigue siendo quien ha abierto la sesión

Solamente algunos usuarios pueden ejecutar sudo:

- Aquellos indicados en el fichero `/etc/sudoers`
- Por omisión, el usuario que instala la máquina está en `/etc/sudoers`
- En ubuntu, se incluye en `/etc/sudoers` a todos los usuarios del grupo *admin*

Por todo esto, sudo es más seguro que su, aunque

- en algunos sistemas, sudo no está instalado y no se puede usar
- en algunos sistemas, el uso de sudo es opcional
- en algunos sistemas, como Ubuntu, el uso de sudo es obligatorio, los usuarios no pueden ejecutar su
 - Pero si vamos a ejecutar muchas órdenes como root y sudo nos resulta incómodo, podemos hacer una pequeña *trampa*:
sudo su

Para aplicaciones gráficas, no debe usarse sudo sino gksudo

- gksudo *mi-aplicacion*

sudo y redirecciones

La orden *sudo* por omisión no incluye las posibles redirecciones

- `sudo echo hola > /tmp/aa`

El proceso *echo* se lanza con la identidad del root (id 0), pero la redirección la ejecuta el usuario ordinario

- Para poder usar redirecciones, ejecutamos una subshell con el parámetro `-c`

```
sudo bash -c "echo hola>aa"
```

```
sudo bash -c "find /root | grep prueba "
```

(o, alternativamente, `sudo su`)

Algunas ambigüedades

- 1 En el lenguaje oral, la palabra *root* a veces provoca ambigüedades, podemos referirnos a
 - El usuario *root*
 - El directorio *home* del usuario *root*:
/root
 - El punto del que cuelga el sistema de ficheros:
/.

Por el contexto se distingue fácilmente

- 2 La palabra *fichero* también puede tener distintos significados
 - El sentido habitual en informática (fichero ordinario)
 - En sentido Unix, incluye ficheros ordinarios, directorios, pipes y ficheros especiales (dispositivos)