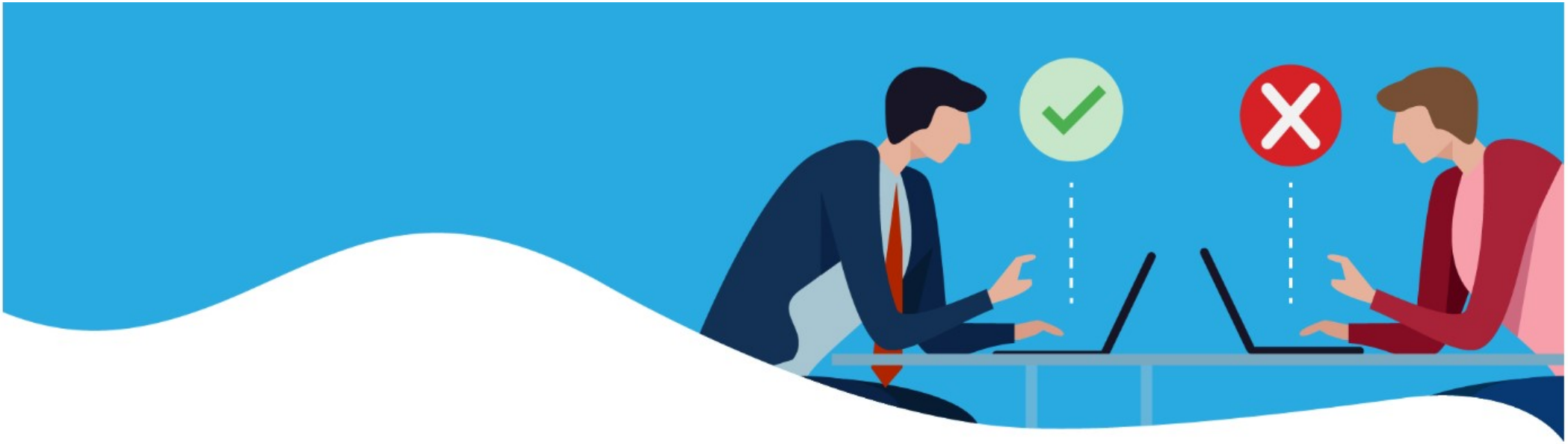


Acceso administrativo

Hay muchos comandos de Linux que tratan con información confidencial como contraseñas, hardware del sistema, u otros que operan bajo circunstancias excepcionales. Evitar que usuarios ordinarios ejecuten estos comandos ayuda a proteger el sistema. Iniciar una sesión como usuario `root` proporciona acceso administrativo, y permite la ejecución de algunos de los comandos privilegiados.

El comando `su`

```
su OPCIONES NOMBRE-DE-USUARIO
```

El comando `su` le permite actuar temporalmente como un usuario diferente. Lo hace creando un nuevo shell. El shell es simplemente una consola de entrada de texto que le permite escribir comandos. De forma predeterminada, si no se especifica una cuenta de usuario, el comando `su` abrirá un nuevo shell como usuario `root`, proporcionando privilegios administrativos.

Siga leyendo

Se recomienda utilizar la opción shell para iniciar la sesión, ya que el shell de inicio de sesión configura completamente el nuevo shell con la configuración del nuevo usuario. Esta opción se puede especificar de tres maneras:

```
su -
su -l
su --login
```

Después de ejecutar el comando `su`, se requiere una contraseña. En nuestras máquinas virtuales, la contraseña para las cuentas `root` y `sysadmin` es `netlab123`. Si alguna vez olvida la contraseña, ésta se muestra cada vez que se inicia una nueva máquina virtual. Como medida de seguridad, la contraseña no será visible mientras la escribe.

```
sysadmin@localhost:~$ su  -
Password:
root@localhost:~#
```

Tenga en cuenta que el símbolo del sistema ha cambiado para reflejar que ahora ha iniciado sesión como usuario `root` . Para cerrar la sesión y volver a la cuenta `sysadmin` , use el comando `exit` . Note como el símbolo vuelve a cambiar

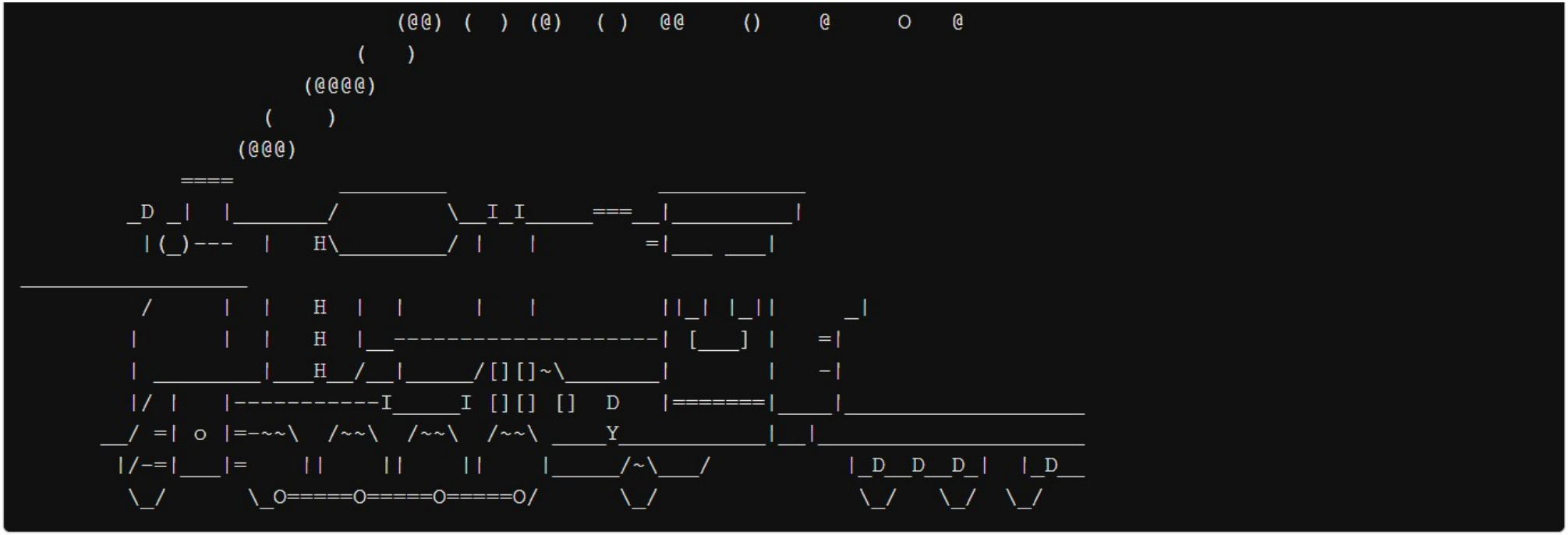
```
root@localhost:~# exit
logout
sysadmin@localhost:~$
```

Para evitar ejecutar comandos sensibles o privilegiados, hemos configurado el comando *steam locomotive*, `sl` , para que requiera acceso administrativo. Si el comando se ejecuta como `sysadmin` , aparece un mensaje de error:

```
sysadmin@localhost:~$ sl
-bash: /usr/bin/sl: Permission denied
```

Utilice el comando `su` para cambiar a la cuenta `root` y ejecute el comando `sl` con acceso administrativo:

```
sysadmin@localhost:~$ su  -
Password:
root@localhost:~# sl
```



Vuelva a utilizar el comando `exit` para volver a la cuenta `sysadmin`.

```
root@localhost:~# exit
logout
sysadmin@localhost:~$
```

El comando `sudo`

```
sudo [OPCIONES] COMANDO
```

El comando `sudo` permite a un usuario ejecutar un comando como otro usuario sin tener que crear un nuevo shell. Para ejecutar un comando con privilegios administrativos utilice el comando como argumento para el comando `sudo`. Al igual que pasa con el comando `su`, el comando `sudo` asume por defecto que la cuenta de usuario `root` debe usarse para ejecutar comandos.

A tener en cuenta

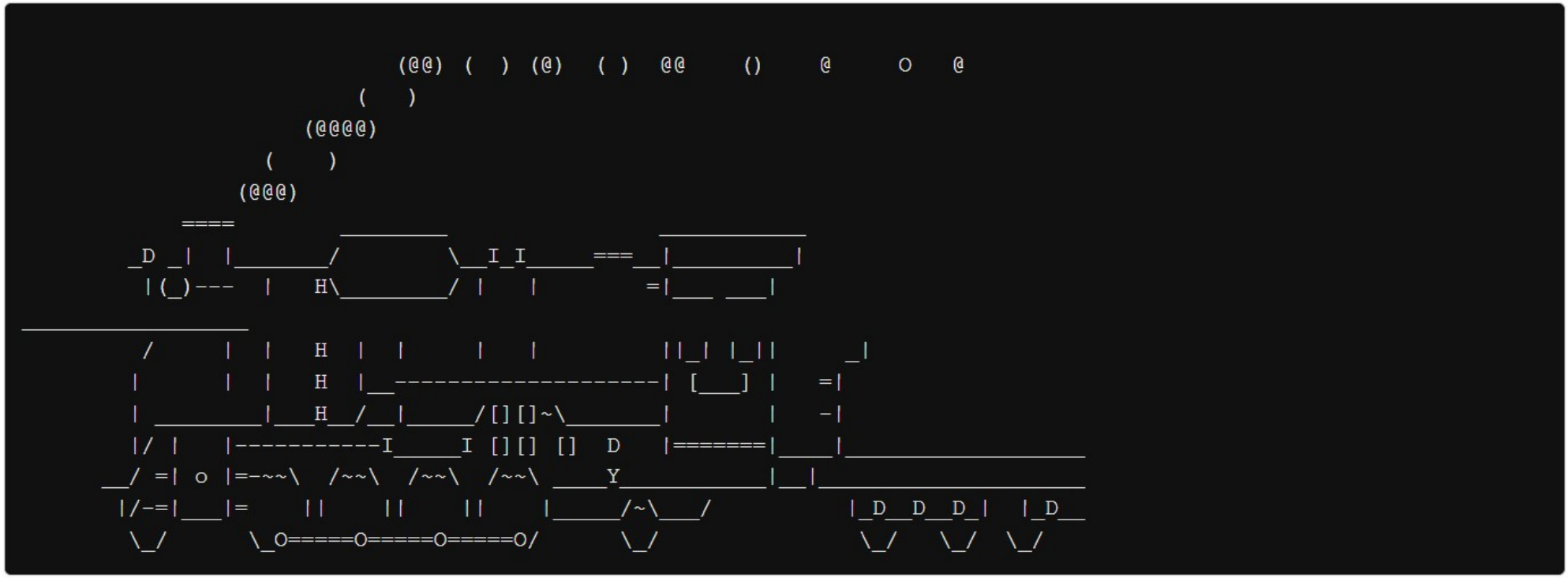
El comando `sudo` también puede usarse para cambiar a otras cuentas de usuario. Para especificar una cuenta de usuario diferente, utilice la opción `-u`.

Ejecute el comando `sl` como usuario `root` poniendo `sudo` delante de él:

Nota

Recuerde que la contraseña es `netlab123`. La solicitud de contraseña no aparecerá de nuevo mientras el usuario continúe ejecutando comandos `sudo` a intervalos inferiores a cinco minutos.

```
sysadmin@localhost:~$  sudo sl
[sudo] password for sysadmin:
```



Una vez completado el comando, observe que el símbolo del sistema no ha cambiado, usted continua bajo la cuenta de inicio `sysadmin`. El comando `sudo` sólo proporciona acceso administrativo para la ejecución del comando especificado. Esto es una ventaja ya que reduce el riesgo de que un usuario ejecute accidentalmente un comando como usuario `root`. La intención de ejecutar un comando es clara; el comando se ejecuta como root si se prefija con el comando `sudo`. De lo contrario, el comando se ejecuta como usuario ordinario.