Consola

Yeray Santana Benítez

Introducción:

- Como usuarios root podemos definir y limitar el uso de la consola a los usuarios.
- De esta forma evitamos que usuarios no root ejecuten comandos o archivos que no deben o no queremos que ejecuten.

- Cuando usuarios no root se conectan a un equipo localmente, obtienen dos tipos de permisos:
  - Pueden ejecutar programas que de otra forma no podrían.
  - Pueden tener acceso a ciertos archivos a los no tendrían acceso de otro modo:
    - Acceso a discos, CD-ROMs.

- Como es posible que un equipo tenga varias consolas y varios usuarios registrados, se debe definir una prioridad a la hora de usar estos archivos.
- Dicha prioridad es secuencial: el primer usuario registrado será el propietario de dichos archivos. Cuando este termine su sesión, la propiedad pasará al siguiente que se registró.
- En contraste, cada usuario registrado, podrá ejecutar tareas normalmente restringidas al root:
  - Halt, poweroff, reboot,...

Desactivación del apagado con las teclas Ctrl-Alt-Del

- Por defecto en etc/inittab se especifica que el sistema se ha establecido para apagarse y rearrancar usando Ctrl-Alt-Del.
  - ca::ctrlaltdel:/sbin/shutdown/ -t3 –r now
- Si queremos desactivar dicha opción podemos comentar la línea.

- Opcionalmente, podemos permitir a usuarios no root que hagan uso de este comando. Para ello:
  - Añadimos la opción –a a la línea anterior. Con esto vamos a indicar que se busca en /etc/shutdown.allow si el usuario tiene permiso.
    - ca::ctrlaltdel:/sbin/shutdown/ -a -t3 –r now
  - Creamos el fichero shutdown.allow e incluimos los nombres los usuarios que tendrán dicho permiso. El fichero tendrá la siguiente estructura:

```
Juan
Miguel
Antonio
```

- Cuando alguno de los usuarios teclee Ctrl-Alt-Del, la aplicación shutdown comprueba si algún usuario descrito en shutdown.allow esta registrado en alguna consola virtual. En caso afirmativo se procede con el apagado del sistema. En caso negativo se muestra un mensaje de error

Desactivación del acceso a programas de la consola

- Es posible desactivar el acceso a los usuarios a los programas de consola:
  - rm –f /etc/security/console.apps/*
- En entornos en los que la consola tiene otro sistema de seguridad (contraseñas en la bios, en el sector de arranque, desactivación de la combinación Ctrl-Alt-Del, de los interruptores de encendido y reinicio, etc), probablemente no se desee que ningún usuario que trabaje con la consola ejecute los comandos poweroff, reboot y halt. Para quitar estas opciones tecleamos:
  - rm –f /etc/security/console.apps/poweroff
  - rm –f /etc/security/console.apps/halt
  - rm –f /etc/security/console.apps/reboot

Desactivación de todos los accesos a la consola

- El módulo pam_console.so de PAM, gestiona todos los permisos y la autentificación de los archivos de la consola.
- Para desactivar todos los accesos a consola y el acceso a programas y archivos, sólo tendremos que comentar todas la líneas que se refieran a pam_console.so en el fichero /etc/pam.d

Definición de la consola

- El módulo pam_console.so usa el archivo /etc/security/console.perms para determinar los permisos que tienen los usuarios sobre la consola. Por defecto, el archivo contiene la siguiente línea:
  - <console>=tty[0-9][0-9]* :[0-9]\.[0-9] :[0-9]

- Cuando los usuarios se registran , se conectan a algún terminal, bien sea un servidor X con un nombre como :0 o mymachine.example.com.1:0 o un dispositivo como /dev/ttyS0/ o /dev/pts/2.

- La opción por defecto es definir esas consolas virtuales locales y que los servidores X se consideren locales, pero si se desea considerar también el terminal serial próximo en el puerto se puede cambiar la línea para que la muestre:

```
<console>=tty[0-9][0-9]* :[0-9]\.[0-9] :[0-9]
/dev/ttyS1
```

Colocar los archivos accesibles desde la consola

- Se pueden definir los archivos que serán accesibles a través de la consola en el fichero /etc/security/console.perms:

```
<floppy>=/dev/fd[0-1]* \
        /dev/floppy/* /mnt/floppy*
<sound>=/dev/dsp* /dev/audio* /dev/midi* \
        /dev/mixer* /dev/sequencer \
        /dev/sound/* /dev/beep
<cdrom>=/dev/cdrom* /dev/cdroms/* /dev/cdwriter*
        /mnt/cdrom*
```

- Al final del mismo archivo, definimos los permisos de la siguiente manera:

```
<console>0660 <floppy> 0660 root.floppy
<console>0600 <sound> 0640 root
<console>0660 <floppy> 0660 root.disk
```

- La segunda columna indica el permiso que el usuario de la consola tiene sobre el archivo (lectura y escritura en este caso), la tercera el dispositivo, la quinta que el root será el propietario cuando el usuario cierre la sesión y la cuarta los permisos de éste.

Activación del acceso a la consola para otras aplicaciones

- El acceso a la consola sólo funciona para aplicaciones residentes en /sbin/ o /usr/sbin/ por lo que la aplicación debe estar en este lugar.

- Después de comprobar ésto:
  - Creamos un vínculo del nombre de la aplicación, por ejemplo *foo,* en la aplicación /usr/bin/consolehelper:

    cd /usr/bin

    ln –s consolehelper

    foo
  - Creamos el archivo /etc/security/console.apps/foo

    touch

    /etc/security/console.apps/foo

- Creamos un archivo de configuración de PAM para el servicio foo en /etc/pam.d. Un modo sencillo de realizar esto es empezar con una copia del archivo de configuración del servicio detenido y luego modificar el archivo si se desea su comportamiento:

```
cp /etc/pam.d/halt
/etc/pam.d/foo
```

- Ahora, cuando se ejecute /usr/bin/*foo*, se llamará al comando consolehelper, el cual validará al usuario con la ayuda de /usr/sbin/userhelper.
- Para validar al usuario, consolehelper solicitará una contraseña del usuario si /etc/pam.d/*foo* es una copia de /etc/pam.d/halt (en caso contrario, hará precisamente lo que se haya especificado en /etc/pam.d/*foo*) y a continuación ejecutará /usr/sbin/*foo* con permisos de root.

- En el archivo de configuración PAM, una aplicación puede ser configurada para usar el módulo *pam_timestamp* para recordar (caché) un intento de conexión exitoso. Cuando una aplicación inicia y se proporciona una autentificación adecuada (la contraseña de root), se crea un archivo timestamp.

- Por defecto, una validación con éxito está cacheada durante cinco minutos. Durante este tiempo, cualquier otra aplicación que sea configurada para usar pam_timestamp y ejecutar desde la misma sesión, está automáticamente autenticada para el usuario X el usuario no introduce la contraseña de root de nuevo.

- Este módulo está incluido en el paquete pam. Para activar esta característica, el archivo de configuración PAM en etc/pam.d/ debe incluir las líneas siguientes:

  auth sufficient /lib/security/pam_timestamp.so

  Session optional /lib/security/pam_timestamp.so

- La primera línea que inicie con auth debería estar tras cualquier otra línea auth sufficient y la línea que empieza con session debería estar tras cualquier otra línea session optional.

- Si una aplicación configurada para usar pam_timestamp es validada exitosamente desde el botón de menú principal (en el Panel), el icono es desplegado en el área de notificación del panel si está ejecutando el entorno de escritorio GNOME.
- Después que la autentificación caduca (por defecto cinco minutos), el icono desaparece. El usuario puede seleccionar olvidar la autentificación cacheada al pulsar el icono y seleccionar la opción de olvidar la autentificación.

El grupo floppy

- Podemos hacer que los usuarios no root tengan acceso a la disquetera.
- Para ello agregamos a los usuarios al grupo floppy. Por ejemplo, usaremos gpasswd para agregar al usuario Juan:

  gpasswd –a Antonio floppy