Comandos Importantes Prácticas

Comandos para comprobar automontado

Linux

El comando lsblk muestra los dispositivos conectados, estén montados o no

```
lsblk
```

Mount muestra todo lo que está montado

```
mount
```

Si el dispositivo está montado muestra el punto de montaje, en caso contrario, no muestra nada

```
findmnt
```

Muestra espacio libre, si el dispositivo no está montado no aparece

```
df
```

Windows

Comandos para obtener información

Muestra información sobre los discos, pero no nos permite saber si están montados o no

```
fdisk
```

Permite obtener información de los dispositivos

```
parted
```

Bersión gráfica de parted

```
gparted
```

Muestra los mensajes del buffer del kernel, cuando se conecta un dispositivo muestra un mensaje aunque no se monte. Puede dar bastantes datos identificativos sobre un medio de almacenamiento.

```
dmesg
```

Comando para mostrar dispositivos USB conectados

```
lsusb
```

Comando que tiene una opción para mostrar información sobre un dispositivo que le indiquemos

```
udevadn
```

Comandos para recuperar información de un dispositivo

Para bloquear el montaje de un dispositivo hay varios métodos:

reglas udev

Se encuentran en /lib/udev/rules.dev y /etc/udev/rules.d, dentro encontraremos documentos con nombres como 90-usb_lock.rules, dentro encontraremos los siguientes campos (Todos en una línea, separados por motivos explicativos):

```
ACTION=="add|change", #Cada vez que se conecta o cambia algo en el
dispositivo, se lanza esta regla
SUBSYSTEM=="block", #Indica el tipo, no se debe confundir con SUBSYSTEMS.
ENV{UDISKS_AUTO}="0" #Evita el automontaje de la unidad
ENV{UDISKS_INFNORE}="1" #Esta sería una alternativa a la línea anterior, no
deben estar las dos a la vez, esta regla indica que se ignora el dispositivo
```

En resumidas cuentas, el contenido puede ser si fuera poco restrictivo como:

```
ACTION=="add|change", SUBSYSTEM=="block", ENV{UDISKS_AUTO}="0"
```

Y si fuera muy restrictivo como

```
ACTION=="add|change", SUBSYSTEM=="block", ENV{UDISKS_INFNORE}="1"
```

Para aplicar los cambios a las reglas se usa el siguiente comando:

```
sudo udevadm control --reload-rules
```

UDISK2

From:
https://knoppia.net/ - **Knoppia**

Permanent link:
https://knoppia.net/doku.php?id=master_cs:analisis_forense:cmdimportant&rev=1739384383

Last update: **2025/02/12 18:19**