

5. Prácticas de gestión de archivos

Entrega. Enseñar en el aula al profesor:

- Un fichero con los comandos de `find`.
- La nueva estructura de LVM de la máquina servidor.
- Un fichero con los comandos usados para definir esta estructura de LVM.

5.1. Ejercicio de find (2 puntos)

Este ejercicio puede realizarse en cualquier ordenador (anota los comandos). Descomprime `pruebas.tgz` con las opciones `zxpvf` para preservar los permisos e indica cómo se utilizaría el comando `find` para buscar desde el directorio en que se descomprimió a `pruebas` (sin entrar en este):

1. Cualquier tipo de fichero que tenga los permisos exactos `rw-r-xrwx`.
[salida correcta (no se indica el path): `fich657.txt`]
2. Cualquier tipo de fichero que tenga al menos los permisos `rw` para el grupo y `w` para otros.
[salida correcta: `fich073.txt`, `fich077.txt`, `fich173.txt`, `fich177.txt`, `fich273.txt`, `fich277.txt`, `fich373.txt`, `fich377.txt`, `fich473.txt`, `fich477.txt`, `fich573.txt`, `fich577.txt`, `fich673.txt`, `fich677.txt`, `fich773.txt`, `fich777.txt`]
3. Con un solo comando `find`, los ficheros regulares que tengan un tamaño comprendido entre 10 y 1000 bytes y los directorios `*.dir` (sin importar mayúsculas o minúsculas).
[salida correcta: `fich.TXT`, `dir.DIR`, `dir.dir`, `save.c`].
4. Copiar en el subdirectorio `pruebas/antiguos` los ficheros que tengan fecha de modificación anterior a un año (usando la opción `-exec`).
[salida correcta: `hace_un_ano.txt`, `hace_dos_anos.txt`].
5. Lo mismo que el anterior, pero usando `xargs`.

5.2. Añadir a lvm nuevo disco y ampliar swap (2 puntos)

Realiza este y los siguientes ejercicios en la máquina virtual servidor (anota los comandos). En la máquina servidor (que dispone de dos discos configurados con LVM), añádele un tercer disco (`servidor3.img`) de 75 GB siguiendo los siguientes pasos:

1. En el PC real crea un nuevo disco virtual de 75 GB.
2. Arranca **kvm** del servidor incluyendo este tercer disco.
3. Ya dentro de la máquina servidor utiliza **fdisk** para crear una única partición en el tercer disco, que ocupe todo el disco.
4. Crea un nuevo volumen físico (**pvccreate**) que incluya toda esta partición y extiende el grupo de volumen existente (**vgextend**) para que incluya este nuevo volumen físico.

Para crear un nuevo volumen lógico de 2 GB, que usaremos como segunda área de *swap*, seguiremos los siguientes pasos:

1. Crea el volumen lógico de 2 GB en el grupo de volúmenes ya existente (**lvcreate**), poniéndole como etiqueta **swapvol2**. Comprueba que se crea el nuevo dispositivo **/dev/mapper/{etiqueta_del_gv}-swapvol2**.
2. Cifra el nuevo volumen lógico con cifrado **no** LUKS y clave aleatoria de **/dev/urandom** (con el comando **cryptsetup**), poniéndole como etiqueta **{etiqueta_del_gv}-swapvol2.crypt**. Comprueba que se crea el nuevo dispositivo **/dev/mapper/{etiqueta_del_gv}-swapvol2.crypt**.
3. Inicia el dispositivo cifrado con **mkswap** y actívalo como nueva área de **swap** con **swapon**.
4. Añade una nueva línea al fichero **/etc/crypttab** para que se descifre en el arranque. El formato será el mismo que la del *swap* que ya tenemos.
5. Añade una nueva línea al fichero **/etc/fstab** para que este nuevo *swap* se active en el arranque. El formato será el mismo que la del *swap* ya existente.
6. Reinicia el sistema y comprueba que las dos áreas de *swap* están activas.

5.3. Extender una partición (2 puntos)

Para extender y cifrar la partición de **/tmp** (que debería ser de 25 GB, **ext3** y estar sin cifrar) añadiéndole 20 GB más, seguiremos los siguientes pasos:

1. Extiende el volumen lógico de *tmp* en 20 GB.
2. Extiende el sistema de ficheros en caliente, esto es, sin desmontar el sistema de ficheros (tarda un rato). Para ello usa el comando **fsadm** sin especificar el tamaño para que use el máximo disponible en el volumen lógico. Al finalizar, comprueba con **df** que tiene el nuevo tamaño.

3. Para la distribución actual (*buster*) comenta (sin borrar) en `/etc/fstab` la línea de `/tmp` y reinicia la máquina virtual (en esta distribución si solo desmontamos cuando ejecutemos el comando `cryptsetup` nos va decir que el volumen está en uso).

Para la distribución antigua (*jessie*) no es necesario reiniciar, basta primero con desmontar `/tmp` y comentar en `/etc/fstab` la línea de `/tmp`.

En cualquier caso, no sobreescribas con `dd`, puesto que esto tardaría mucho y haría que el tamaño de la imagen de KVM aumente a 80 GB.

4. Cifra el volumen lógico formateándolo con `cryptsetup` y LUKS, con un cifrado por contraseña, que el comando nos pedirá.
5. Activa (abre) el volumen lógico cifrado usando la contraseña que acabamos de poner.
6. Crea de nuevo el sistema de ficheros `ext3` sobre el dispositivo cifrado puesto que la operación anterior ha borrado todo.
7. Obtén el UUID del volumen lógico (del dispositivo sin cifrar).
8. Añade una nueva línea al fichero `/etc/crypttab` para que se descifre en el arranque. Utiliza el mismo formato que las existentes para los otros volúmenes. Para referenciar a la partición de disco puede usarse tanto el dispositivo cifrado como el UUID del volumen lógico (UUID del dispositivo sin cifrar).
9. Reinicia la máquina virtual (debería pedir una contraseña más en el inicio, para descifrar el volumen *tmp*). Comprueba que el volumen cifrado de *tmp* aparece en `/dev/mapper`.
10. Modifica en el fichero `/etc/fstab` la línea de `tmp` para que se monte el dispositivo cifrado (descomenta la línea y añádele la extensión `_crypt`). Comprueba que se puede montar el dispositivo con `mount /tmp`. Si da algún tipo de error vuelve a comentar la línea, puesto en que caso de problema la máquina podría no arrancar.
11. Si todo fue bien, recuerda volver a poner al directorio `/tmp` los permisos adecuados (incluyendo el *sticky bit*).
12. Reinicia el sistema (debería pedir una contraseña más en el inicio, para descifrar el volumen *tmp*) y comprueba que `/tmp` está montado y tiene el nuevo tamaño.

5.4. Extender dos particiones en caliente (2 puntos)

Extiende la partición de `/var` (que debería ser XFS, tener 40 GB y estar cifrada) añadiéndole 30 GB y `/home` (que debería ser `ext4`, tener 30 GB y también debería estar cifrado) con el resto del espacio, siguiendo los siguientes pasos:

1. Extiende el volumen lógico de *var* en 30 GB.
2. Extiende el volumen cifrado de *var* con `cryptsetup`. No hay que indicar el tamaño pues así utilizará todo el espacio disponible en el volumen lógico.
3. Extiende el sistema de ficheros `/var` en caliente (sin desmontar el sistema de ficheros ni indicar tamaño) con `fsadm` y comprueba con `df` el nuevo tamaño.
4. Añade el resto del espacio libre del grupo de volúmenes al volumen de *home*. Comprueba que al grupo de volúmenes no le queda ningún espacio libre.
5. Extiende el volumen cifrado de *home*.
6. Extiende el sistema de ficheros `/home` en caliente y comprueba con `df`.
7. Reinicia y comprueba los nuevos tamaños de `/var` y `/home` con `df`.

5.5. Cambiar el sistema de cifrado (2 puntos)

1. Crea (si no existe) en `/etc` un directory “`keys`” y tres ficheros que sirvan como clave de descifrado de `/home`, `/var` y `/tmp` sin necesidad de introducir por teclado la contraseña.
2. El directorio `/etc/keys` debería ser sólo accesible para `root`, y los ficheros del directorio permiso de sólo lectura para `root`. De esta forma, en el arranque sólo nos debería pedir la clave de descifrado del directorio raíz.
3. Añade con el comando `cryptsetup` estas nuevas claves de cifrado (nos pedirá la clave antigua). No borraremos la clave antigua, aunque podría hacerse.
4. Comprueba los slots de claves de los tres volúmenes lógicos.
5. Modifica el fichero `/etc/crypttab` para que el descifrado se haga a partir de los ficheros de claves.
6. Comprueba que en el arranque solo nos pide la clave de descifrado del directorio raíz.

NOTA: Ya no usaremos más la máquina virtual servidor.