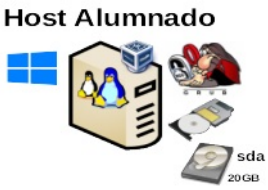
Taller BRS - cryptsetup - GNU/Linux

ESCENARIO

Máquina virtual:
Nome: Allow Boot GRUB HD
Tipo: Linux
Versión: Debian (64-bit)
RAM ≥ 2048MB
Orde de arranque: Óptica/Disco duro
CPU ≥ 2
PAE/NX habilitado
Almacenamento:
  Unidade óptica(ISO): Debian Install amd64 DVD-1
  Disco duro dinámico de 20GB
Rede: Soamente unha tarxeta activada en modo NAT

Xestor de arranque: GRUBv2



LIMITACIÓN DE RESPONSABILIDADE O autor do presente documento declina calquera responsabilidade asociada ao uso incorrecto e/ou malicioso que puidese realizarse coa información exposta no mesmo. Por tanto, non se fai responsable en ningún caso, nin pode ser considerado legalmente responsable en ningún caso, das consecuencias que poidan derivarse da información contida nel ou que esté enlazada dende ou hacia el, incluíndo os posibles erros e información incorrecta existentes, información difamatoria, así como das consecuencias que se poidan derivar sobre a súa aplicación en sistemas de información reais e/ou virtuais. Este documento foi xerado para uso didáctico e debe ser empregado en contornas privadas e virtuais controladas co permiso correspondente do administrador desas contornas.

NOTA:

- Documentación de interese:
  - **Comandos GNU/Linux e SHELL BASH (/bin/bash) (1)**
  - **losetup (dispositivos de bloques virtual)**
  - **LVM: physical volume(pvX), volume group (vgX), logical volume(lvX)**
  - **Práctica SI Backup**

1. Realizar a práctica **1-Taller-BRS-Practica-Allow-Boot-GRUB-HD-GNU-Linux**
2. Arrancar co sistema operativo GNU/Linux instalado no disco duro.
3. Abrir sesión de usuario na contorna gráfica coas credenciais: **usuario**/**abc123.**

LUKS en dispositivo virtual

4. Abrir unha consola de comandos e executar:

$ su - #Acceder á consola de root(administrador) a través do comando *su*, o cal solicita o contrasinal do usuario *root*. Escribir o contrasinal de *root* para acceder.

dd if=/dev/zero of=probas.dd bs=1M count=50 status=progress #Crear mediante o comando *dd* un ficheiro baleiro chamado *probas.dd* de 50 MB, empregando o dispositivo */dev/zero*, que xera bytes "ceros". O parámetro *bs=1M* establece o tamaño do bloque a 1 Megabyte e *count=50* especifica que se xeren 50. O indicador *status=progress* amosa o progreso do proceso.

losetup -f --show probas.dd #Asociar un dispositivo de bucle (loop device) co ficheiro *probas.dd*. O parámetro *-f* busca o próximo dispositivo dispoñible, e *--show* mostra cal foi asignado. Esta liña asocia, por exemplo, */dev/loop0* co ficheiro *probas.dd*.

losetup -a #Amosar a lista de todos os dispositivos de bucle actualmente configurados no sistema.
parted --script /dev/loop0 mklabel msdos #Crear unha nova táboa de particións no dispositivo */dev/loop0*, usando o formato *msdos*. O parámetro *--script* fai que o comando non pida confirmación.
parted --script /dev/loop0 mkpart primary 0 50% -a cylinder #Crear unha partición primaria no dispositivo de bucle */dev/loop0*, ocupando o 50% do espazo do disco virtual. De novo, *--script* fai que non se pidan confirmacións. A opción *-a cylinder* indica que a alineación da partición debe facerse en función dos cilindros do disco (unha antiga unidade física nos discos duros). Aínda que o uso de cilindros como referencia é algo antigo e xa non se recomenda en discos actuais (que usan sectores lóxicos), esta opción asegura que as particións se aliñen cos límites tradicionais dos cilindros.
apt update || apt-get update #Actualizar repositorios declarados no ficheiro */etc/apt/souces.list* e nos ficheiros existentes no directorio */etc/apt/sources.list.d*
Así, unha vez realizada a consulta dos ficheiros existentes nas rutas anteriores, descárganse uns ficheiros coas listas de paquetes posibles a instalar. Estes ficheiros son gardados en */var/lib/apt/lists*
apt -y install cryptsetup || apt-get -y install cryptsetup #Instalar automaticamente o paquete cryptsetup no teu sistema sen pedir confirmacións interactivas, grazas ao parámetro -y. Con esta ferramenta, podes crear, abrir e pechar volumes cifrados, ademais de xestionar discos cifrados con LUKS.
cryptsetup luksFormat /dev/loop0p1 #Cifrar a partición */dev/loop0p1* (a primeira partición no dispositivo de bucle) usando LUKS (Linux Unified Key Setup). LUKS é un estándar para cifrado de discos en GNU/Linux. Durante o proceso, pregúntache se queres continuar. Debes escribir "YES" en maiúsculas para confirmar. Despois, solicita que introduzas e verifiques a frase de contrasinal que será usada para desbloquear o volume cifrado.

```
¡ATENCIÓN!
==========
Esto sobreescribirá los datos en /dev/loop0p1 de forma irrevocable.

¿Está seguro? (Teclee 'yes' en mayúsculas): YES
Introduzca la frase contraseña de /dev/loop0p1:
Verifique la frase contraseña:
```

mkdir montado #Crear un directorio chamado *montado* no que se montará o volume.
cryptsetup luksOpen /dev/loop0p1 montado #Abrir o volume cifrado de LUKS en */dev/loop0p1* e asignámoslle o nome de *montado* como dispositivo no directorio */dev/mapper/*. Despois de abrir o volume, solicítase a frase de contrasinal para desbloquealo.

```
Introduzca la frase contraseña de /dev/loop0p1:
```

ls -l /dev/mapper#Amosar o contido do directorio */dev/mapper/*, onde debería aparecer unha ligazón simbólica chamada montado, apuntando a un dispositivo de tipo *dm*, como *../dm-0*. Isto indica que o volume cifrado foi correctamente aberto e está listo para usarse.

```
...
lrwxrwxrwx 1 root root       7 may 28 21:35 montado -> ../dm-0
```

mkfs.ext4 /dev/mapper/montado #Crear o sistema de ficheiros */dev/mapper/montado*, é dicir, formatea o volume cifrado aberto */dev/mapper/montado* cun sistema de ficheiros ext4, o cal permitirá almacenar datos.
mkdir remontado #Crear un novo directorio chamado remontado para montar o volume cifrado formateado
mount /dev/mapper/montado remontado/ #Montar o volume cifrado (co sistema de ficheiros ext4) no directorio *remontado*.
echo 1 > remontado/1.txt #Escribir o número "1" nun ficheiro chamado 1.txt dentro do directorio *remontado*.
umount remontado #Desmontar o volume
cryptsetup luksClose montado #Pechar o volume cifrado e eliminar a súa entrada en */dev/mapper/*. O nome "*montado*" xa non aparecerá.

> **NOTA**: $ man cryptsetup-close -> For backward compatibility there are **close** command aliases: **remove**, **plainClose**, **luksClose**, **loopaesClose**, **tcryptClose**, **bitlkClose** (all behaves exactly the same, device type is determined automatically from active device).

ls -l /dev/mapper #Verificar que o dispositivo montado xa non existe no directorio */dev/mapper/*.
losetup -d /dev/loop0 #Liberar o dispositivo de bucle asociado a *probas.dd*.
losetup -a #Amosar os dispositivos de bucle restantes, verificando que o *loop0* foi desasociado.

> Para que os dispositivos LUKS se desbloqueen automaticamente ao iniciar o sistema, é necesario editar os ficheiros:
> - **/etc/crypttab**: Aquí indícase que dispositivos deben ser desbloqueados e que contrasinais ou métodos deben usarse no inicio.
> - **/etc/fstab**: Neste ficheiro configúranse os puntos de montaxe automáticos para os volumes.
>
> Así, cada vez que se reinicie o sistema, os dispositivos LUKS configurados en /etc/crypttab serán recoñecidos e montados automaticamente.

init 0 Comando para enviar o runlevel (nivel de execución) do sistema operativo ao nivel 0, equivalente a apagar o sistema.

LUKS en sistemas de ficheiros: /dev/sdb1

5. Agregar á máquina virtual un novo disco virtual dinámico de 200MB e arrancar de novo a máquina virtual.

6. Abrir unha consola de comandos e executar:

$ su - #Acceder á consola de root(administrador) a través do comando *su*, o cal solicita o contrasinal do usuario *root*. Escribir o contrasinal de *root* para acceder.

parted --script /dev/sdb mklabel msdos #Crear unha nova táboa de particións no dispositivo */dev/sdb*, usando o formato *msdos*. O parámetro *--script* fai que o comando non pida confirmación.

parted --script /dev/sdb mkpart primary 0 100% -a cylinder #Crear unha partición primaria no dispositivo de bucle */dev/sdb*, ocupando o 100% do espazo do disco virtual. De novo, *--script* fai que non se pidan confirmacións. A opción *-a cylinder* indica que a alineación da partición debe facerse en función dos cilindros do disco (unha antiga unidade física nos discos duros). Aínda que o uso de cilindros como referencia é algo antigo e xa non se recomenda en discos actuais (que usan sectores lóxicos), esta opción asegura que as particións se aliñen cos límites tradicionais dos cilindros.

cryptsetup luksFormat /dev/sdb1 #Cifrar a partición */dev/sdb1* (a primeira partición no dispositivo de bloques) usando LUKS (Linux Unified Key Setup). LUKS é un estándar para cifrado de discos en GNU/Linux. Durante o proceso, pregúntache se queres continuar. Debes escribir "YES" en maiúsculas para confirmar. Despois, solicita que introduzas e verifiques a frase de contrasinal que será usada para desbloquear o volume cifrado.

```
¡ATENCIÓN!
==========
Esto sobreescribirá los datos en /dev/sdb1 de forma irrevocable.

¿Está seguro? (Teclee 'yes' en mayúsculas): YES
Introduzca la frase contraseña de /dev/sdb1:
Verifique la frase contraseña:
```

cryptsetup luksOpen /dev/sdb1 montado #Abrir o volume cifrado de LUKS en */dev/sdb1* e asignámoslle o nome de *montado* como dispositivo no directorio */dev/mapper/*. Despois de abrir o volume, solicítase a frase de contrasinal para desbloquealo.

```
Introduzca la frase contraseña de /dev/sdb1:
```

ls -l /dev/mapper#Amosar o contido do directorio */dev/mapper/*, onde debería aparecer unha ligazón simbólica chamada montado, apuntando a un dispositivo de tipo *dm*, como *../dm-0*. Isto indica que o volume cifrado foi correctamente aberto e está listo para usarse.

```
...
lrwxrwxrwx 1 root root       7 may 28 21:35 montado -> ../dm-0
```

mkfs.ext4 /dev/mapper/montado #Crear o sistema de ficheiros */dev/mapper/montado*, é dicir, formatea o volume cifrado aberto *dev/mapper/montado* cun sistema de ficheiros ext4, o cal permitirá almacenar datos.

mount /dev/mapper/montado remontado/ #Montar o volume cifrado (co sistema de ficheiros ext4) no directorio *remontado*.

echo 1 > remontado/1.txt #Escribir o número "1" nun ficheiro chamado 1.txt dentro do directorio *remontado*.

umount remontado #Desmontar o volume

Para que os dispositivos LUKS se desbloqueen automaticamente ao iniciar o sistema, é necesario editar os ficheiros:

- **/etc/crypttab**: Aquí indícase que dispositivos deben ser desbloqueados e que contrasinais ou métodos deben usarse no inicio.
- **/etc/fstab**: Neste ficheiro configúranse os puntos de montaxe automáticos para os volumes.

Así, cada vez que se reinicie o sistema, os dispositivos LUKS configurados en /etc/crypttab serán recoñecidos e montados automaticamente.

echo '/dev/mapper/montado /mnt ext4 errors=remount-ro 0 2' >> /etc/fstab #Engadir esa liña ao ficheiro */etc/fstab* para configurar a montaxe automática dun volume no sistema, onde:

- **/dev/mapper/montado**: Indica o dispositivo que se vai montar. Neste caso, trátase dun volume cifrado LUKS, que foi desbloqueado previamente e está asociado co dispositivo montado dentro de /dev/mapper/.
- **/mnt**: Este é o punto de montaxe onde se accederá ao volume. O volume será montado automaticamente neste directorio cando se inicie o sistema.
- **ext4**: Especifica o tipo de sistema de ficheiros do volume. Neste caso, é ext4, que foi previamente creado no volume cifrado.
- **errors=remount-ro**: Esta opción di que se se produce algún erro no sistema de ficheiros durante o uso, o volume será remontado en modo de só lectura (read-only). Isto protexe o volume e os datos se algo vai mal.
- **0**: Este número indica se se debe facer unha copia de seguridade do volume con dump. Un valor de 0 significa que non se farán copias de seguridade automáticas.
- **2**: Este número indica a orde en que se verificará o sistema de ficheiros durante o inicio, mediante fsck. O número 1 é para o sistema de ficheiros raíz, mentres que outros sistemas de ficheiros, como este, reciben o valor 2, indicando que será revisado tras o sistema de ficheiros principal.

echo 'montado /dev/sdb1 none' >> /etc/crypttab #Engadir esa liña ao ficheiro */etc/crypttab*, onde:

- **montado**: Este é o nome que se lle asignará ao volume cifrado cando se desbloquee. Unha vez desbloqueado, o dispositivo cifrado aparecerá como /dev/mapper/montado.
- **/dev/sdb1**: Este é o dispositivo que contén o volume cifrado que se vai desbloquear. Neste caso, trátase da partición /dev/sdb1.
- **none**: Aquí normalmente vaise o método para fornecer a frase de contrasinal ou a clave para o desbloqueo. Ao especificar none, indícase que a frase de contrasinal deberá ser introducida manualmente durante o arranque.

init 6 Comando para enviar o runlevel (nivel de execución) do sistema operativo ao nivel 6, equivalente a reiniciar o sistema.

7. Agora no arranque do sistema debe solicitar o contrasinal para desbloquear o volume cifrado configurado anteriormente

```
Please enter passphrase for disk VBOX_HARDDISK (montado) on /mnt::
```

No caso de equivocarnos ao introducir o contrasinal voltará a aparecer a mensaxe de novo para poder introducir o contrasinal, impedíndose o arranque do sistema operativo.

LUKS en sistema de ficheiros existente: /home

Como cando xeramos un volume cifrado eliminaranse os datos existentes non podemos directamente cifrar /home porque perderiamos os datos. Entón, o que imos facer e aproveitar o volume cifrado realizado anteriomente (/dev/sdb1 → montado) e imos facer un volcado dos datos existentes do cartafol /home neste, de tal xeito, que ao copiar os datos de /home a montado teremos no dispositivo cifrado os datos, para logo modificar o /etc/fstab e modificar /mnt por /home, de tal xeito que agora o dispositivo cifrado estará montado en /home (o cal xa contén os datos do usuarios)

8. Abrir unha consola de comandos e executar:

$ su - #Acceder á consola de root(administrador) a través do comando *su*, o cal solicita o contrasinal do usuario *root*. Escribir o contrasinal de *root* para acceder.

dpkg -l rsync ; [$(echo $?) -eq '1'] && apt update && apt -y install rsync #Verificar se o paquete rsync está instalado. Se non está instalado, actualízase a lista de paquetes dos repositorios e instálase.

rsync -avz --progress /home/ /mnt/ #Copiar de forma incremental a estrutura arbórea do contido do cartafol /home dentro do cartafol /mnt, en modo arquivo (-a)(Ver NOTAS), de forma detallada (-v), comprimida (-z) e amosando o proceso de copia (--progress). **Como é a primeira que se empregan esas rutas (orixe e destino) faise unha copia completa da ruta orixe na ruta destino, xa que na ruta destino non existe ningunha copia da ruta orixe**.

rsync -avz --progress /home/ /mnt #Copiar de forma incremental a estrutura arbórea do contido do cartafol /home dentro do cartafol /mnt, en modo arquivo (-a)(Ver NOTAS), de forma detallada (-v), comprimida (-z) e amosando o proceso de copia (--progress). **Como non é a primeira vez que se emprega esa ruta orixe (/home/) con esa ruta destino (/mnt) faise unha copia incremental da ruta orixe na ruta destino, xa que na ruta destino si existe unha copia da ruta orixe.**

sed -i 's|/dev/mapper/montado /mnt|/dev/mapper/montado /home|' /etc/fstab #Modificar o destino de montaxe do dispositivo cifrado: de /mnt a /home, xa que agora xa temos volcado o /home no dispositivo cifrado "montado"
init 6 Comando para enviar o runlevel (nivel de execución) do sistema operativo ao nivel 6, equivalente a reiniciar o sistema.

9. Agora no arranque do sistema debe solicitar o contrasinal para desbloquear o volume cifrado configurado anteriormente

```
Please enter passphrase for disk VBOX_HARDDISK (montado) on /home::
```

No caso de equivocarnos ao introducir o contrasinal voltará a aparecer a mensaxe de novo para poder introducir o contrasinal, impedíndose o arranque do sistema operativo.

10. Agora xa dispoñemos dun /**home** cifrado. Abrir unha consola de comandos e executar:

$ mount | grep montado #Ver que o dispositivo cifrado está montado en "/home"

```
/dev/mapper/montado on /home type ext4 (rw,relatime,errors=remount-ro)
```

$ lsblk -o +UUID #Listar dispositivos de bloques cos seus correspondentes UUID.

$ lsblk -o +UUID | grep home #Listar dispositivos de bloques cos seus correspondentes UUID, e filtrar esa saída co patrón home

Ricardo Feijoo Costa