

# NASA hw3

Author: B12705014陳泊華

## 1. Initial partition

(a) \$ gdisk /dev/vda

(b) 先使用n創建vda1 partition，再將hexcode設為'0xEF02'

```
Command (? for help): n
Partition number (1-128, default 1):
First sector (34-2097118, default = 2048) or {+-}size{KMGT}P:
Last sector (2048-2097118, default = 2095103) or {+-}size{KMGT}P: +1M
Current type is 8300 (Linux filesystem)
Hex code or GUID (L to show codes, Enter = 8300): 0xEF02
Changed type of partition to 'BIOS boot partition'
```

(c) n command 預設為linux filesystem，直接創建(或hexcode 8300)

```
Command (? for help): n
Partition number (2-128, default 2):
First sector (34-2097118, default = 4096) or {+-}size{KMGT}P:
Last sector (4096-2097118, default = 2095103) or {+-}size{KMGT}P: +200M
Current type is 8300 (Linux filesystem)
Hex code or GUID (L to show codes, Enter = 8300):
Changed type of partition to 'Linux filesystem'
```

(d) 用t指令查詢Linux LVM的hexcode，將其設為'8e00'

```
Command (? for help): t
Partition number (1-3): 3
Current type is 8300 (Linux filesystem)
Hex code or GUID (L to show codes, Enter = 8300): L
Type search string, or <Enter> to show all codes: Linux LVM
8e00 Linux LVM
Hex code or GUID (L to show codes, Enter = 8300): 8e00
Changed type of partition to 'Linux LVM'
```

檢查： \$ lsblk

NAME	MAJ:MIN	RM	SIZE	RO	TYPE	MOUNTPOINTS
fd0	2:0	1	4K	0	disk	
loop0	7:0	0	748.3M	1	loop	/run/archiso/airootfs
sr0	11:0	1	872.3M	0	rom	/run/archiso/bootmnt
sr1	11:1	1	1024M	0	rom	
vda	254:0	0	1G	0	disk	
└─vda1	254:1	0	1M	0	part	
└─vda2	254:2	0	200M	0	part	
└─vda3	254:3	0	821M	0	part	
vdb	254:16	0	1G	0	disk	
vdc	254:32	0	1G	0	disk	
vdd	254:48	0	1G	0	disk	
vde	254:64	0	1G	0	disk	
vdf	254:80	0	1G	0	disk	

references:

- (i) [https://wiki.archlinux.org/title/GPT\\_fdisk](https://wiki.archlinux.org/title/GPT_fdisk) ([https://wiki.archlinux.org/title/GPT\\_fdisk](https://wiki.archlinux.org/title/GPT_fdisk))
- (ii) [https://www.gnu.org/software/grub/manual/grub/html\\_node/BIOS-installation.html#BIOS-installation](https://www.gnu.org/software/grub/manual/grub/html_node/BIOS-installation.html#BIOS-installation)  
[https://www.gnu.org/software/grub/manual/grub/html\\_node/BIOS-installation.html#BIOS-installation](https://www.gnu.org/software/grub/manual/grub/html_node/BIOS-installation.html#BIOS-installation)
- (iii) TA Lab3 slides

## 2. RAID Setup

(a) \$ mdadm --create --verbose --level=10 --metadata=1.2 --raid-devices=4 /dev/md/data /dev/vdc /dev/vdd /dev/vde /dev/vdf

(b) \$ mdadm --create --verbose --level=0 --metadata=1.2 --raid-devices=2 /dev/md/linux /dev/vda3 /dev/vdb

檢查： \$ cat /proc/mdstat

Personalities :	[raid10]	[raid0]
md126 :	active raid0 vdb[1] vda3[0]	
	1885184 blocks super 1.2 512k chunks	
md127 :	active raid10 vdf[3] vde[2] vdd[1] vdc[0]	
	2093056 blocks super 1.2 512K chunks 2 near-copies [4/4] [UUUU]	
unused devices:	<none>	

references:

- (i) TA slides

### 3. Disk encryption

(a)

```
$ cryptsetup luksFormat --type luks1 /dev/vda2
$ cryptsetup luksDump /dev/vda2 ->代表什麼？
$ cryptsetup -v status /dev/mapping/cryptboot
root@archiso ~ # cryptsetup luksFormat /dev/vda2
WARNING: Device /dev/vda2 already contains a 'crypto_LUKS' superblock signature.

WARNING!
=====
This will overwrite data on /dev/vda2 irreversibly.

Are you sure? (Type 'yes' in capital letters): YES
Enter passphrase for /dev/vda2:
Verify passphrase:
cryptsetup luksFormat /dev/vda2 5.77s user 0.31s system 39% cpu 15.492 total
```

(b)

```
$ dd if=/dev/urandom of=key2 bs=1 count=256
$ cryptsetup luksAddKey /dev/vda2
```

```
root@archiso ~ # dd if=/dev/random of=key2 bs=1 count=256
256+0 records in
256+0 records out
256 bytes copied, 0.00270554 s, 94.6 kB/s
root@archiso ~ # cat /dev/key2
cat: /dev/key2: No such file or directory
1 root@archiso ~ # find key2
key2
root@archiso ~ # ls
key2
root@archiso ~ # pwd
/root
root@archiso ~ # cat key2
5jn0oBmWn:-
sUyFy-rDFFrrTRRU>gPxOWzWZ.S0j9f...76N1b0BxL,
2-?;~yUkUm
$Cr%
!Mf A*g_...! SoIc!Id...
root@archiso ~ #
```

(c)

```
$ cryptsetup luksFormat --type luks2 --key-file key2 /dev/md/linux
$ cryptsetup open --type luks2 --key-file key2 /dev/md/linux cryptroot
$ cryptsetup -v status /dev/mapping/cryptroot
```

```
4 root@archiso ~ # cryptsetup -v status cryptroot
/dev/mapper/cryptroot is active.
  type:    LUKS2
  cipher:  aes-xts-plain64
  keysize: 512 bits
  key location: keyring
  device:  /dev/md126
  sector size: 512
  offset:  32768 sectors
  size:    3737600 sectors
  mode:    read/write
Command successful.
```

(d)

```
$ cryptsetup luksFormat --type luks2 --key-file key2 /dev/md/data
$ cryptsetup open --type luks2 --key-file key2 /dev/md/data cryptdata
root@archiso ~ # cryptsetup luksFormat --type luks2 --key-file key2 /dev/md/data

WARNING!
=====
This will overwrite data on /dev/md/data irreversibly.

Are you sure? (Type 'yes' in capital letters): YES
cryptsetup luksFormat --type luks2 --key-file key2 /dev/md/data 5.29s user 0.35s system 73% cpu 7.674 total
root@archiso ~ # cryptsetup open --type luks2 --key-file key2 /dev/md/data cryptdata
root@archiso ~ # cryptsetup -v status cryptdata
/dev/mapper/cryptdata is active.
  type: LUKS2
  cipher: aes-xts-plain64
  keysize: 512 bits
  key location: keyring
  device: /dev/md127
  sector size: 512
  offset: 32768 sectors
  size: 4153344 sectors
  mode: read/write
Command successful.
```

保存隨機生成密碼檔在系上工作站：

```
$ scp key2 b12705014@ws1.csie.ntu.edu.tw:/tmp2/b12705014/partition
```

references:

- (i) <https://zh.wikipedia.org/wiki/PBKDF2> (<https://zh.wikipedia.org/wiki/PBKDF2>).
- (ii) <https://officeguide.cc/linux-hard-disk-encryption-with-luks-cryptsetup-command-tutorial-examples/> (<https://officeguide.cc/linux-hard-disk-encryption-with-luks-cryptsetup-command-tutorial-examples/>).
- (iii) chatGPT3.0

#### 4. LVM Setup

```
$ pvcreate /dev/mapper/cryptroot
$ vgcreate linux /dev/mapper/cryptroot
$ lvcreate -L 256M -n home linux
$ lvcreate -l 100%FREE -n root linux
root@archiso ~ # pvcreate /dev/mapper/cryptroot
Physical volume "/dev/mapper/cryptroot" successfully created.
root@archiso ~ # vgcreate linux /dev/mapper/cryptroot
Volume group "linux" successfully created
root@archiso ~ # lvcreate -L 256M -n home linux
Logical volume "home" created.
root@archiso ~ # lvcreate -l 100%FREE -n root linux
Logical volume "root" created.
```

檢查： \$ pvs; vgs; lvs

```
root@archiso ~ # pvs;vgs;lvs
PV          VG   Fmt Attr PSize PFree
/dev/mapper/cryptroot  linux  lvm2 a--  1.78g    0
VG          #PV #LV #SN Attr   USize VFree
  linux      1   2   0 wz--n- 1.78g    0
LV          VG   Attr   LSize Pool Origin Data% Meta% Move Log Cpy%Sync Convert
  home  linux -wi-a---- 256.00m
  root  linux -wi-a----  1.53g
```

references:

- (i) TA slides
- (ii) chatGPT3.0

## 5. Formatting

```
$ mkfs.*fs /dev/<path>
root@archiso ~ # mkfs.ext4 /dev/linux/home
mke2fs 1.47.0 (5-Feb-2023)
Creating filesystem with 262144 1k blocks and 65536 inodes
Filesystem UUID: 4a52f1f5-5c97-4201-9236-bd8dd71bf9e8
Superblock backups stored on blocks:
    8193, 24577, 40961, 57345, 73729, 204801, 221185

Allocating group tables: done
Writing inode tables: done
Creating journal (8192 blocks): done
Writing superblocks and filesystem accounting information: done

root@archiso ~ # mkfs.ext4 /dev/linux/root
mke2fs 1.47.0 (5-Feb-2023)
Creating filesystem with 401408 4k blocks and 100464 inodes
Filesystem UUID: f2b60bb3-97cd-4008-9b92-670fe883e195
Superblock backups stored on blocks:
    32768, 98304, 163840, 229376, 294912

Allocating group tables: done
Writing inode tables: done
Creating journal (8192 blocks): done
Writing superblocks and filesystem accounting information: done

root@archiso ~ # mkfs.XFS /dev/mapper/cryptdata
zsh: correct 'mkfs.XFS' to 'mkfs.xfs' [nyae]? y
log stripe unit (524288 bytes) is too large (maximum is 256KiB)
log stripe unit adjusted to 32KiB
meta-data=/dev/mapper/cryptdata  isize=512    agcount=8, agsize=64896 blks
                                =                      sectsz=512   attr=2, projid32bit=1
                                =                      crc=1      finobt=1, sparse=1, rmapbt=1
                                =                      reflink=1 bigtime=1 inobtcount=1 nrext64=1
data     =                      bsize=4096   blocks=519168, imaxpct=25
                                =                      sunit=128   swidth=256 blks
naming   =version 2           bsize=4096   ascii-ci=0, ftype=1
log      =internal log        bsize=4096   blocks=16384, version=2
                                =                      sectsz=512   sunit=8 blks, lazy-count=1
realtime =none                extsz=4096   blocks=0, rtextents=0
root@archiso ~ # mkfs.ext2 /dev/mapper/cryptboot
mke2fs 1.47.0 (5-Feb-2023)
Creating filesystem with 202752 1k blocks and 50600 inodes
Filesystem UUID: addd71b0-e0a2-4681-b13b-6e25b555fc8
Superblock backups stored on blocks:
    8193, 24577, 40961, 57345, 73729

Allocating group tables: done
Writing inode tables: done
Writing superblocks and filesystem accounting information: done
```

references:

- (i) TA slides

## 6. Mounting

首先ls確認/mnt裡面是否存在題目指定的資料夾，創建好後利用mount指令：

```
1 root@archiso /boot # ls /mnt
lost+found
root@archiso /boot # mkdir /mnt/home
root@archiso /boot # mkdir /mnt/boot
root@archiso /boot # mkdir /mnt/data
root@archiso /boot # ls /mnt
boot data home lost+found
root@archiso /boot # mount /dev/linux/home /mnt/home
root@archiso /boot # mount /dev/mapper/cryptboot /mnt/boot
root@archiso /boot # mount /dev/mapper/cryptdata /mnt/data
root@archiso /boot # df -hT
Filesystem      Type   Size  Used Avail Use% Mounted on
dev            devtmpfs 1.9G    0  1.9G  0% /dev
run            tmpfs   2.0G  8.9M  2.0G  1% /run
/dev/sr0        iso9660 873M  873M    0 100% /run/archiso/bootmnt
cowspace       tmpfs   256M  5.9M  251M  3% /run/archiso/cowspace
/dev/loop0      squashfs 749M  749M    0 100% /run/archiso/airootfs
airootfs       overlay  256M  5.9M  251M  3% /
tmpfs          tmpfs   2.0G    0  2.0G  0% /dev/shm
tmpfs          tmpfs   2.0G    0  2.0G  0% /tmp
tmpfs          tmpfs   2.0G  2.6M  2.0G  1% /etc/pacman.d/gnupg
tmpfs          tmpfs   392M  8.0K  392M  1% /run/user/0
/dev/mapper/linux-root ext4   1.5G  428K  1.4G  1% /mnt
/dev/mapper/linux-home ext4   230M   78K  214M  1% /mnt/home
/dev/mapper/cryptboot ext2   185M   14K  175M  1% /mnt/boot
/dev/mapper/cryptdata xfs    2.0G   71M  1.9G  4% /mnt/data
```

references:

- (i) TA slides
- (ii) chatGPT

## 7. Arch Installation

### (1) 選擇mirror

```
$ pacman -S reflector
$ reflector --country TW --age 6 --fasttrack 5 --sort rate --save
/etc/pacman.d/mirrorlist
```

reference: <https://wiki.archlinux.org/title/Mirrors> (<https://wiki.archlinux.org/title/Mirrors>).

### (2) 安裝相關套件

```
$ pacstrap /mnt base linux mdadm lvm2 vim man-db
error: package-name: signature from "packager" is unknown trust
$ pacman-key --refresh-keys
成功安裝
```

reference: [https://wiki.archlinux.org/title/Pacman/Package\\_signing](https://wiki.archlinux.org/title/Pacman/Package_signing) ([https://wiki.archlinux.org/title/Pacman/Package\\_signing](https://wiki.archlinux.org/title/Pacman/Package_signing)).

### (3) 生成fstab

```
$ genfstab -U /mnt >> /mnt/etc/fstab 將fstab生成在/mnt的etc底下
```

```
# Static information about the filesystems.
# See fstab(5) for details.

# <file system> <dir> <type> <options> <dump> <pass>
# /dev/mapper/linux-root
UUID=f2b60bb3-97cd-4008-9b92-670fe883e195      /          ext4        rw,relatime,stripe=256 0 1

# /dev/mapper/linux-home
UUID=4a52f1f5-5c97-4201-bd8dd71bf9e8      /home      ext4        rw,relatime,stripe=1024 0 2

# /dev/mapper/cryptroot
UUID=addir71b0-e0a2-4681-b13b-6e25b555fcb8      /boot      ext2        rw,relatime 0 2

# /dev/mapper/cryptdata
UUID=5bab7537-cf3b-48fe-b506-bd9697f62bb4      /data      xfs         rw,relatime,attr2,inode64,logbufs=8,logbsize=32k,sunit=1024,swidth=2048,noquota
0 2
```

reference: [\(https://wiki.archlinux.org/title/Installation\\_guide#Installation\).](https://wiki.archlinux.org/title/Installation_guide#Installation)

### (4) 編輯 mkinitcpio.conf

```
$ arch-chroot /mnt
```

```
$ vim /etc/mkinitcpio.conf
```

更改FILES和HOOKS

FILES=(key2)

新增HOOKS=(... lvm2, encrypt)

```
$ cp /usr/lib/modules/6.6.3-arch1-1/vmlinuz /boot/vmlinuz-linux
```

```
$ mkinitcpio -P 產生initramfs images
```

reference: [\(https://wiki.archlinux.org/title/Mkinitcpio\).](https://wiki.archlinux.org/title/Mkinitcpio)

### (5) 編輯 crypttab

```
$ vim /etc/crypttab 打開後進行以下編輯(key2為密碼檔)
```

cryptroot /dev/md/linux key2 luks

cryptvda2 /dev/vda2 key2 luks

cryptdata /dev/md/data key2 luks

```
[root@archiso boot]# cat /etc/crypttab
# Configuration for encrypted block devices.
# See crypttab(5) for details.

# NOTE: Do not list your root (/) partition here, it must be set up
# beforehand by the initramfs (/etc/mkinitcpio.conf).

# <name>      <device>            <password>           <options>
# home        UUID=b8ad5c18-f445-495d-9095-c9ec4f9d2f37  /etc/mypassword1
# data1       /dev/sda3           /etc/mypassword2
# data2       /dev/sda5           /etc/cryptfs.key
# swap        /dev/sdx4           /dev/urandom
# uvol       /dev/sdb7           none
# 

cryptroot /dev/md/linux key2 luks #automatically decrypt /dev/md/linux
cryptvda2 /dev/vda2 key2 luks #automatically decrypt /dev/vda2
cryptdata /dev/md/data key2 luks
```

reference: [\(https://man.archlinux.org/man/crypttab.5.en\).](https://man.archlinux.org/man/crypttab.5.en)

### (6) 編輯GRUB設定檔

```
$ vim /etc/default/grub 打開編輯器後更改以下設定
```

GRUB\_CMDLINE\_LINUX="cryptdevice=/dev/vda2:cryptboot"

GRUB\_ENABLE\_CRYPTODISK=y

```
$ pacman -Syu grub
$ grub-install /dev/vda 指定grub讀取位置
$ grub-mkconfig -o /boot/grub/grub.cfg
```

reference: <https://wiki.archlinux.org/title/GRUB> (<https://wiki.archlinux.org/title/GRUB>).

### (7) reboot

得到以下畫面，未能順利解決

```
ERROR: device '/dev/linux/root' not found. Skipping fsck.
mount: /new_root: no valid filesystem type specified.
ERROR: Failed to mount '/dev/linux/root' on real root
You are now being dropped into an emergency shell.
sh: can't access tty; job control turned off
```

## 8. Trivia

- (a) 除了已經切好的partition外，還可能存在：
  - (1) MBR或GPT，記錄硬碟分割區位置和大小
  - (2) Boot loader，記錄引導程式的磁區位置，如載入作業系統
  - (3) 檔案系統metadata，包括檔案和目錄的結構、檔案屬性等
  - (4) Swap分割區，如果操作系統需要更多記憶體時，會將一些內存數據移到硬碟上。

reference: [https://linux.vbird.org/linux\\_basic/centos7/0130designlinux.php](https://linux.vbird.org/linux_basic/centos7/0130designlinux.php) ([https://linux.vbird.org/linux\\_basic/centos7/0130designlinux.php](https://linux.vbird.org/linux_basic/centos7/0130designlinux.php)).

- (b) 原因可能與file system的保留空間有關，用於系統的特定目的，確保系統在磁盤空間耗盡之前有足夠空間執行一些重要操作，如系統日誌、文件系統的元數據(metadata) 等。

reference: <https://www.qnap.com/zh-tw/how-to/faq/article/%E4%BB%80%E9%BA%BC%E6%98%AF%E7%B3%BB%E7%B5%B1%E4%BF%9D%E7%95%99%E7%A9%BA%E9%96%93>.

- (c) FUSE是一種檔案系統機制，允許應用程式和使用者進程在用戶空間實現檔案系統，而不需要修改核心內核；這使得開發和測試檔案系統更加容易，但也相對因涉及用戶空間和內核空間的切換而可能有額外效能開銷。

reference: <https://zh.wikipedia.org/zh-tw/FUSE> (<https://zh.wikipedia.org/zh-tw/FUSE>).

- (d) MBR (Master Boot Record) 和GPT (GUID Partition Table) 都是用於啟動系統的磁碟分割表格式，有以下主要差別：
  - (1) 分割數量：MBT最多只有4個主要磁區，而GPT可以支援128個
  - (2) 磁碟容量：MBT的容量限制為2TB(32位元分割表)，而GPT可以更大 (64位元分割表)
  - (3) 硬體支援：MBT使用BIOS載入，GPT則支援UEFI。

reference: <https://www.linwei.com.tw/forum-detail/76/>

(<https://www.linwei.com.tw/forum-detail/76/>).

(e)

(1) exFAT file system

掛載指令： \$ mount -t exfat /dev/vda/mnt

此檔案系統符合題述的3個條件

reference:

(i) <https://www.kingston.com/tw/blog/personal-storage/understanding-file-systems> (<https://www.kingston.com/tw/blog/personal-storage/understanding-file-systems>).

(ii) <https://blog.gtwang.org/linux/ubuntu-linux-mount-exfat/>

(<https://blog.gtwang.org/linux/ubuntu-linux-mount-exfat/>).

(iii) <https://phoenixnap.com/kb/mount-ntfs-linux> (<https://phoenixnap.com/kb/mount-ntfs-linux>).

(iv) chatGPT 3.0

(f) GB為1,000,000,000 ( $10^9$ ) Bytes，GiB為1,073,741,824 ( $2^{30}$ ) Bytes (1 GB  $\approx 0.931$  GiB)；工作站上預設使用GB單位顯示。

(g)

	<b>RAID 0</b>	<b>RAID 10</b>	<b>RAID 5</b>	<b>RAID 6</b>
容錯能力	無	最多2顆	最多1顆	最多2顆
讀取速度	快 (同時讀取)	較慢	次快	次次快
寫入速度	快 (分散寫入)	慢 (同時寫入鏡像)	快	快

\*假設都是4顆硬碟，讀取和寫入速度則假設不需考慮計算、讀寫 parity 資料的額外時間

reference: TA slides

(h) 使用VM將多個虛擬硬碟組成RAID 0，雖然因RAID 0的特性可以一次寫入很多虛擬硬碟，但其有可能因設計不良掛載於同一顆實體硬碟上，這樣的情況下寫入速度依然受到實體硬碟限制。

reference: TA slides