

CentOS 系統安裝設定與管理



新北市政府教育局
教育研究發展科

80723456 # 516 林璟豐



- CentOS (Community enterprise Operating System)
 - 是 Linux 發行版之一，它是來自於 Red Hat Enterprise Linux (RHEL) 依照開放原始碼規定釋出的原始碼所編譯而成。
 - 由於出自同樣的原始碼，因此有些要求高度穩定性的伺服器以 CentOS 替代商業版的 Red Hat Enterprise Linux 使用。



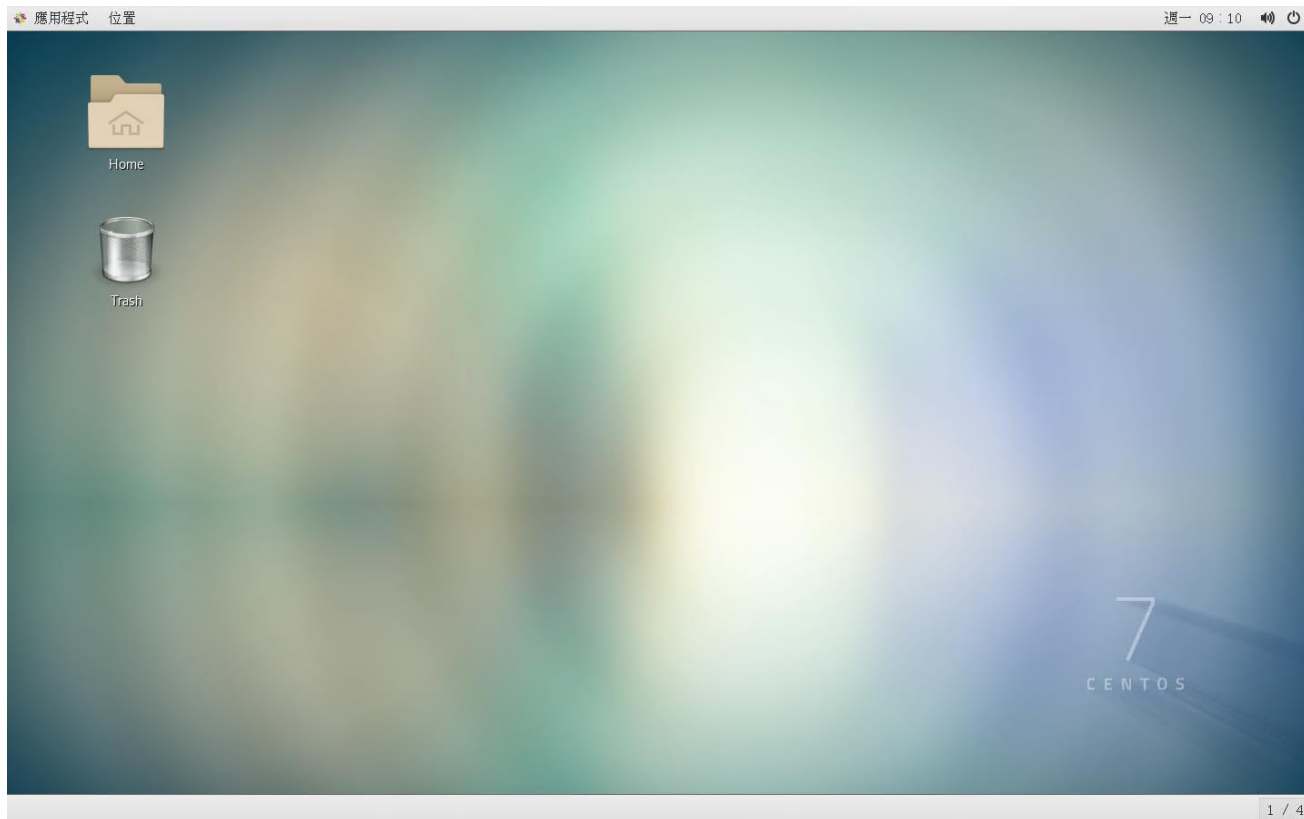


- **CentOS** (Community enterprise Operating System)
 - RedHat 與 CentOS 兩者的不同，在於CentOS並不包含封閉原始碼軟體。
 - CentOS 對原始碼的主要修改部份，是移除了不能自由使用的商標。
 - 2014年，CentOS宣布與Red Hat合作，但CentOS將會在新的委員會下繼續運作，並不受RHEL的影響。

GNOME



- CentOS 預設的圖形桌面環境 (X Window System) 為 GNOME





- Shell :

指令輸入的介面，Shell 是一個可與使用者互動的層面，讓使用者可以透過它(Shell)存取到程式或作業系統的核心(Core)

- 文字界面 BASH :

Bourne-Again SHell 是 Red Hat Enterprise Linux 及 CentOS 預設使用的文字界面 shell

- 圖形界面 GNOME :

GNOME Shell 是桌面環境的預設使用者介面



BASH



- 提示符號：
一般使用者
[UserAccount@HostName WorkingDirectory]\$
管理者(Super User)
[UserAccount@HostName WorkingDirectory]#
「~」表示家目錄，\$pwd 指令可知道現在的操作目錄位置
- 指令使用：
指令(command) 選項(options) 參數(arguments)
「-」短選項、「--」長選項
- 指令示範
\$ls -al / (以長格式列出 / 根目錄清單，含隱藏檔)
\$date --help (列出 date 指令的說明)
\$exit (或 Ctrl+D 退出 BASH Session)



- 變更使用者密碼指令：
\$ **passwd** [使用者帳號]
- Linux 不以副檔名區分執行檔，而是以「權限」設定該檔案是否可執行
\$**file** /etc/passwd
\$**stat** /etc/passwd
\$**file** /usr/bin/passwd
\$**stat** /usr/bin/passwd
- 查看檔案內容
\$**cat** /etc/passwd
\$**more** /etc/passwd
\$**less** /etc/passwd
\$**head** /etc/passwd
\$**tail** /etc/passwd

BASH



- 搜尋檔案內容

\$**grep** ntpcuser /etc/passwd

- 文字與行數計算

\$**wc** /etc/passwd

\$**wc** -l /etc/passwd

- 指令自動補完 (Tab Completion)

\$**pas**<Tab><Tab>

\$**pass**<Tab>

\$**passwd** -<Tab><Tab>

- 歷史指令

\$**history** (列出歷史指令)

\$!**num** (執行第num個指令)

\$!**pass** (執行最近一個開頭為 pass 的指令)

<Up Arrow> (上一個指令)

<Down Arrow> (下一個指令)

Ctrl + r (搜尋歷史指令)

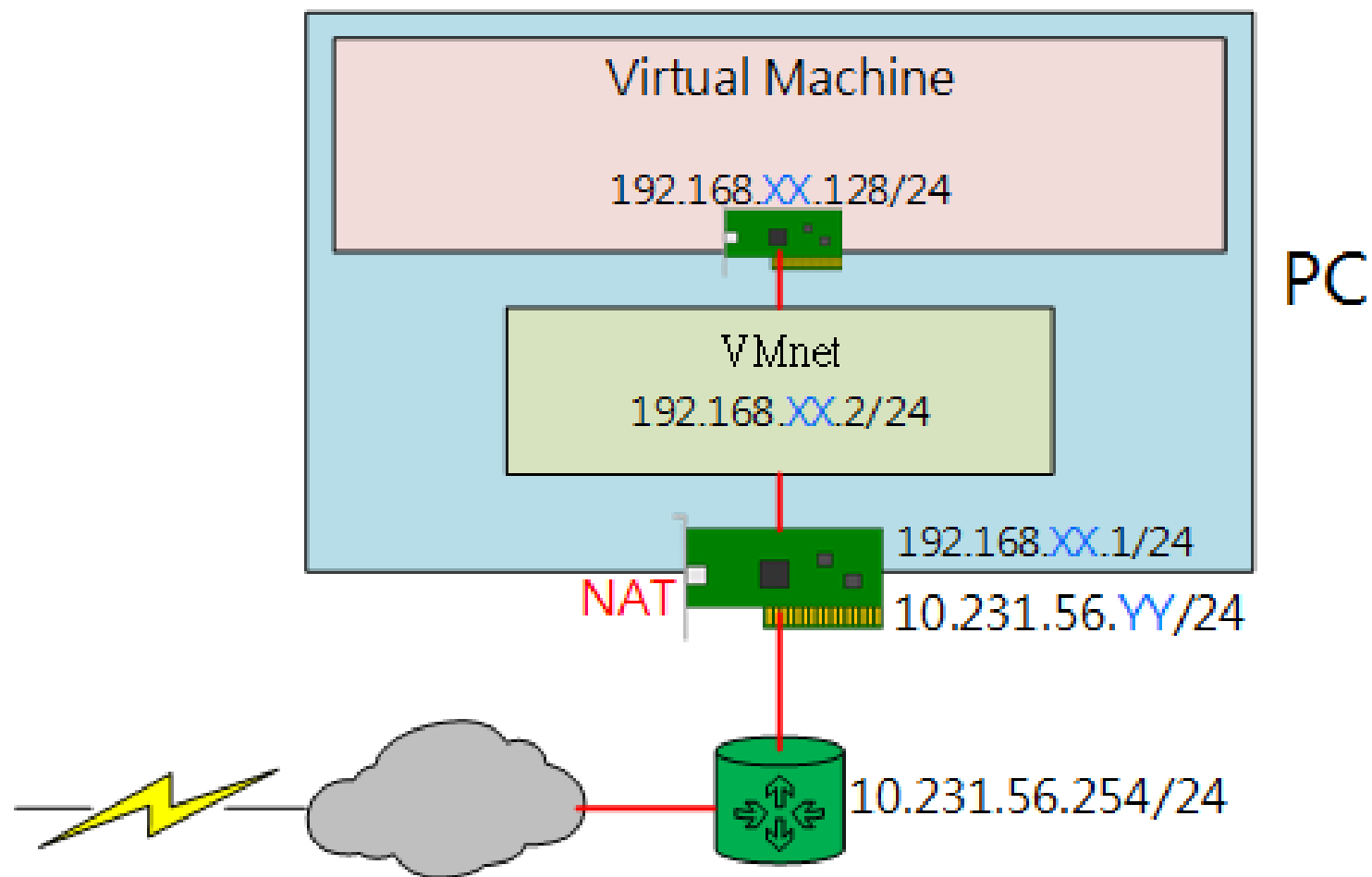
Alt + . (最後字串)

- 清除螢幕

\$**clear**

Ctrl + L

LAB 虛擬機架構環境說明

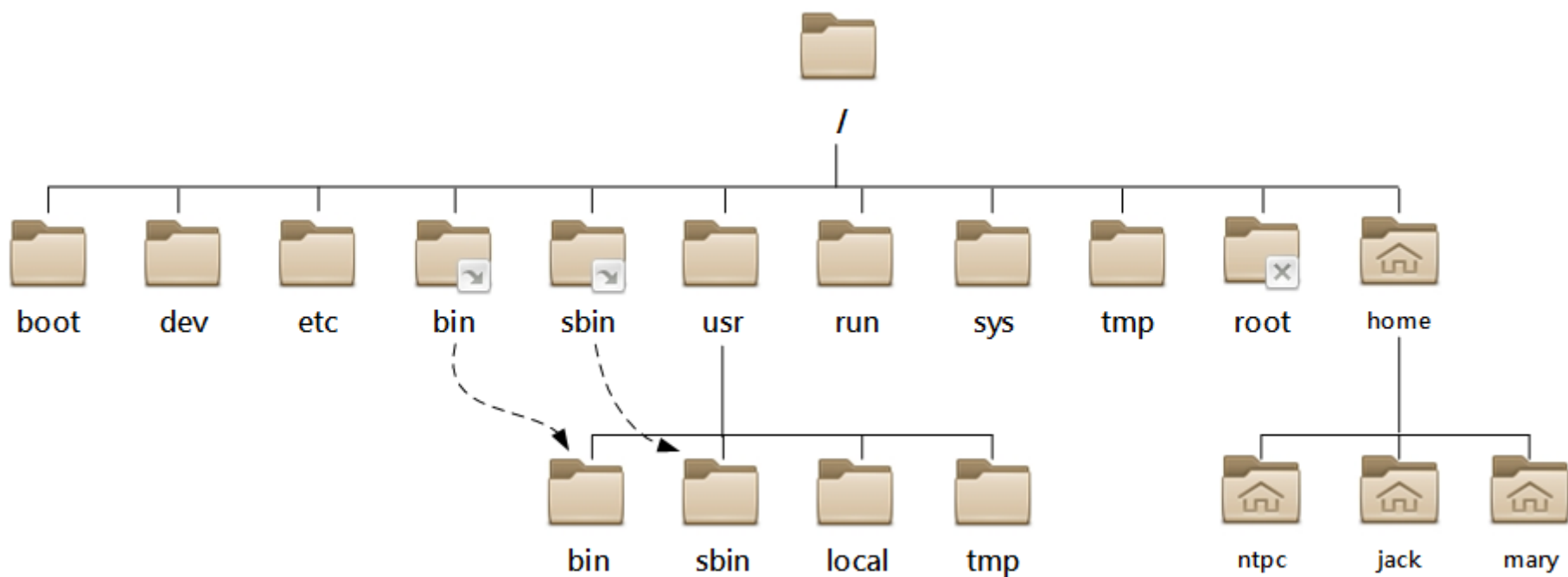


登入與 BASH 練習



- 開啟VMware Workstation Player，選 CentOS.7.Study，點「Play virtual machine」開啟虛擬機 (如有移動提示，請點「I Copied It」)
- 登入VMplayer虛擬機內的 CentOS GNOME 桌面
帳號：ntpcuser
密碼：Centos12#
- 存取 BASH：
滑鼠點「應用程式」→「終端機」或
鍵般按「Super Key」→滑鼠點「終端機」或
滑鼠桌面點右鍵 →「終端機」
- 請練習前述各項指令及操作
- 滑鼠、鍵盤退出 VMplayer 熱鍵：Ctrl + Alt

Linux 檔案階層



Linux 檔案階層



- /usr : **U**nix **S**oftware **R**esource，含指令、程式、函式庫等
 - /usr/bin : 使用者指令 /usr/sbin : 系統管理指令
 - /usr/local : 本機安裝程式
- /etc : 設定檔
- /var : 變動資料，如資料庫、網頁檔案、快取、記錄檔
- /run : 執行中的程序檔及資料，重開機後清除
- /root : 最高管理者的家目錄
- /home : 一般使用者家目錄的上層
- /tmp : 所有使用者或程序可使用的暫存區，超過10天則清除(/var/tmp 可存30天)
- /boot : 開機相關檔案
- /dev : 裝置檔案
- /bin → /usr/bin /sbin → /usr/sbin
/lib → /usr/lib /lib64 → /usr/lib64

Linux 檔案階層



- 路徑：
 - 絕對路徑：`/etc`
 - 相對路徑：`etc` (`/etc` 或 `/usr/etc` 或 `/usr/local/etc` ?)
- 目錄：
 - 當前所在目錄：`.`
 - 上一層目錄：`..`
 - 目前使用者的家目錄：`~`
 - 使用者`username`的家目錄：`~username`
 - 切換目錄：`-`
- 相關指令：
 - `$cd` (change directory)
 - `$pwd` (print working directory)

檔案操作指令



指令	說明	單一來源	多重來源
cp	複製檔案(Copy file)	cp fileA fileB	cp fileA fileB fileC DIRx
	複製目錄(Copy Directory)	cp -r dirA dirB	cp -r dirA dirB dirC DIRx
mv	搬移檔案 (Move file)	mv file1 file2 (改檔名)	mv file1 file2 file3 DIRx
	搬移目錄(Move Directory)	mv dirA dirB	mv dirA dirB dirC DIRx
rm	刪除檔案(Remove file)	rm fileA	rm fileA fileB fileC
	刪除目錄(Remove Directory)	rm -r dirA	rm -r dirA dirB dirC
mkdir	建立目錄(Make Directory)	mkdir dirA	mkdir dirA dirB dirC
rmdir	移除空目錄(Remove Empty Directory)	rmdir dirA	rmdir dirA dirB dirC
touch	建立空檔案或改變檔案時間(Change file timestamps)	touch fileA	touch fileA fileB fileC

路徑及檔名擴展(Expansion)



符號	說明
*	任意 0到多個 字元的字串
?	任意 1個 字元
[abc123]	包含中括號裡的任 1個 字元(如有保留字元，要用「\」跳脫字元)
[!abc123]	不包含中括號裡的任 1個 字元(如有保留字元，要用「\」跳脫字元)
[:alpha:]	包含任 1個 英文字元，大小寫不拘；[:upper:] 大寫、[:lower:]小寫
[:digit:]	包含任 1個 數字
[:alnum:]	包含任 1個 數字或英文字元，大小寫不拘
[:punct:]	包含任 1個 標點符號字元
[:space:]	包含任 1個 空白字元，含 TAB 及分行符號
{1,3,5,7,9}	重複排列大括號內字串，以逗號分隔
{0..9}	重複排列大括號內順序(或反序)數字或字元{a..z}
{a,b}{1,2}	排列組合多個大括號內字串
{a{1,2,3},b}	巢狀排列組合大括號內字串

指令替換



- 指令替換：將指令的輸出當作另一個指令的參數
 `$(command)`：有巢狀功能
 `$echo "Today is $(date +%x)"`
 ``command``：倒引號(容易和「'」單引號混淆)
 `$echo "It's `date +%X` now."`
- 變數表示：`${變數}` 或 `$變數`
- 雙引號：`"xxx"` 引號內特殊符號保留其意義，如 `$` `\` ``` `!` 等，稱為弱引號
- 單引號：`'xxx'` 引號內所有字元都視為普通字元
 `$echo 'Today is $(date +%x)'`

BASH 檔案操作及指令替換練習



- 建立檔案 (用 touch 建立空檔案，其中 X 用順序數字取代)：
建立 6 個 songX.mp3 檔案，建立 6 個 pictureX.jpg 檔案，建立 6 個 videoX.mp4 檔案
- 建立 3 個空目錄：Music, Photo, Movie
- 移動檔案：
songX.mp3 移動到 Music 目錄、pictureX.jpg 移動到 Photo 目錄、
videoX.mp4 移動到 Movie 目錄
- 建立 3 個空目錄：friends, family, work
- 複製檔案：
將編號 1 和 2 的三種檔案，複製 friends 目錄
將編號 3 和 4 的三種檔案，複製 family 目錄
將編號 5 和 6 的三種檔案，複製 work 目錄
- 刪除：
刪除目錄 Music, Photo, Movie

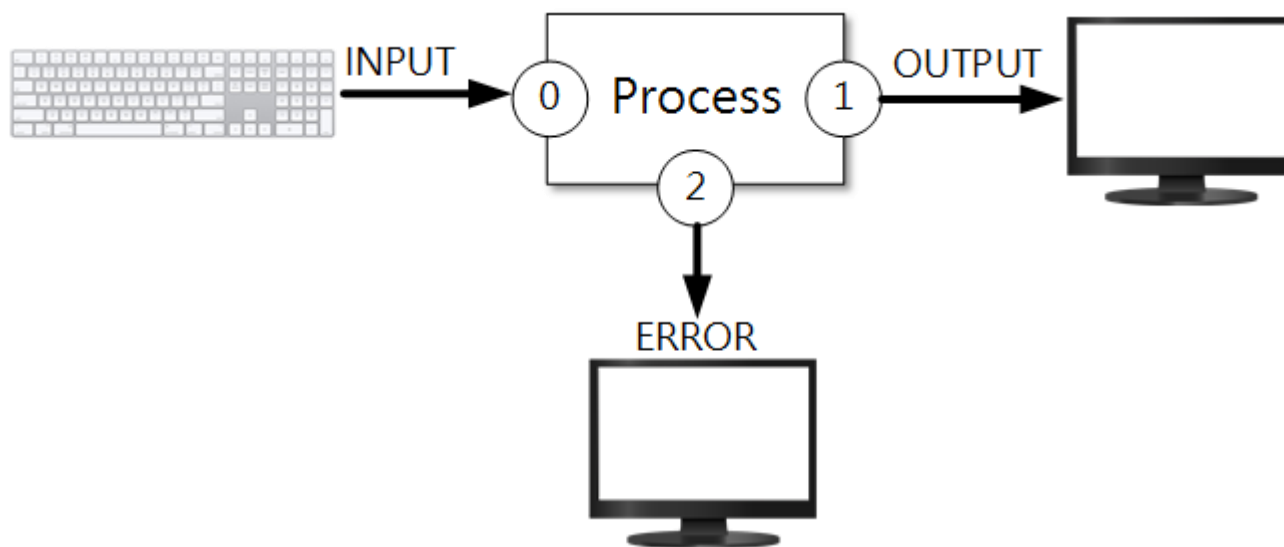
說明文件 Manual Page



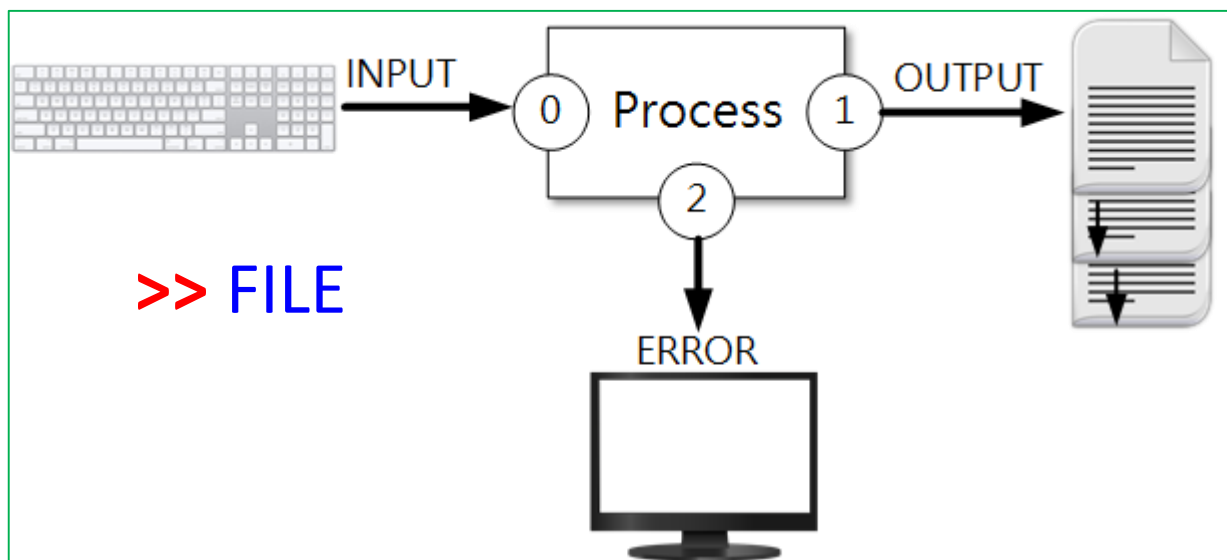
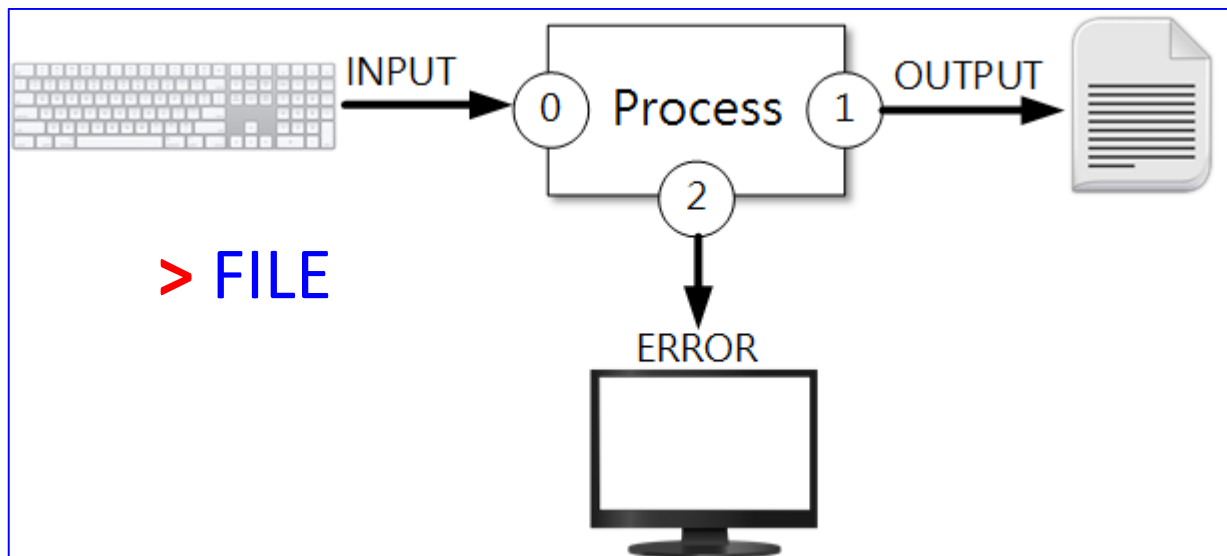
- Manual Page (man , 共有 1 ~ 9 個章節)
 - 1 : 一般指令
 - 5 : 檔案格式
 - 8 : 系統管理指令
 - \$**man** -k KEYWORD : 從資料庫搜尋KEYWORD
- GNU Info Document (pinfo)
- /usr/share/doc : 獨立安裝程式的說明文件
- Google 大神



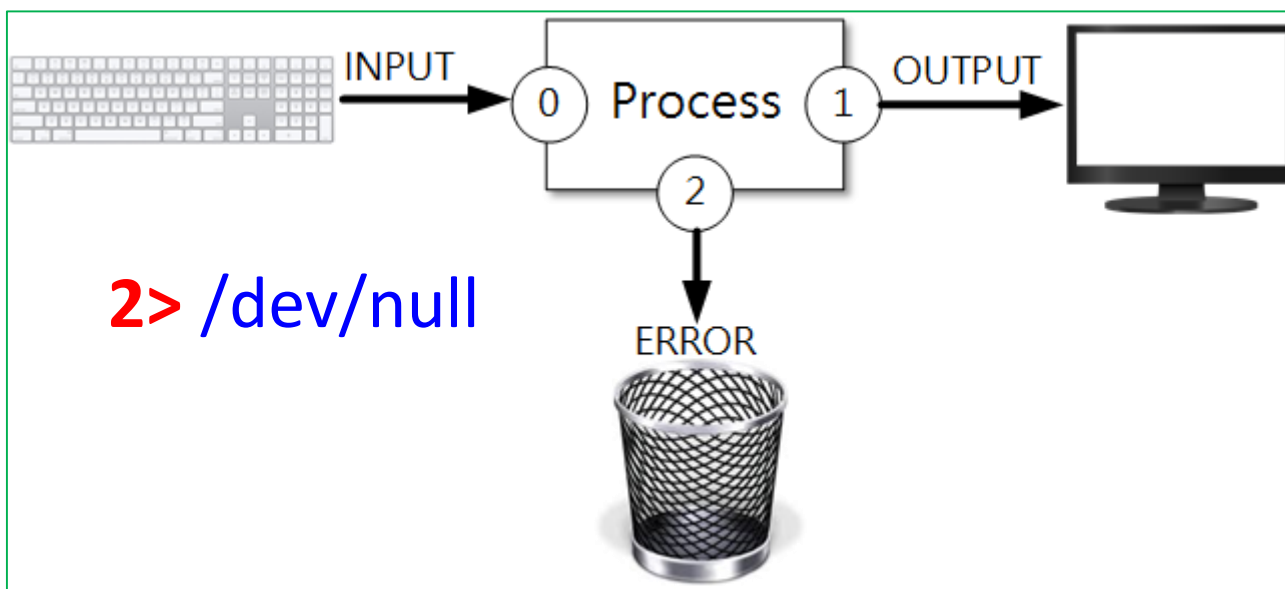
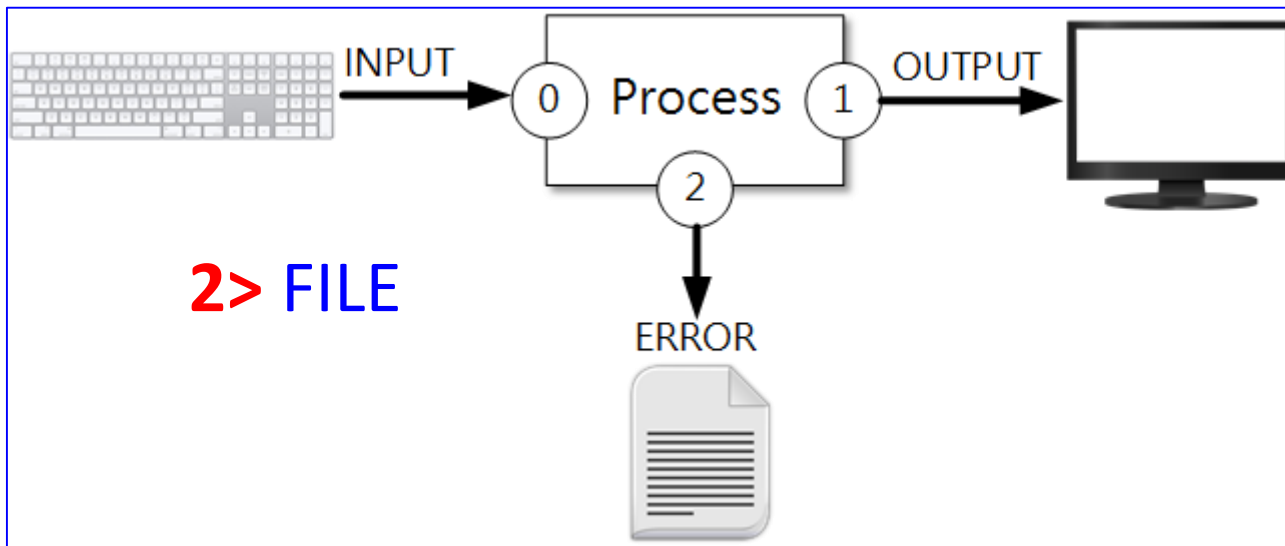
標準輸入輸出



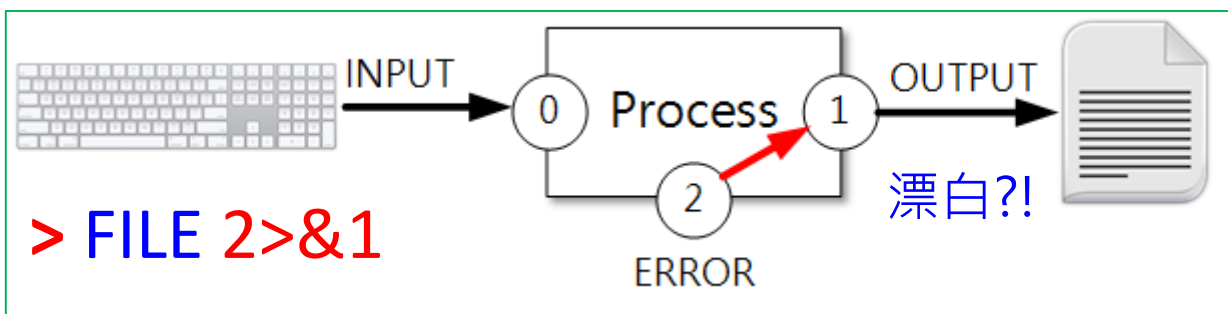
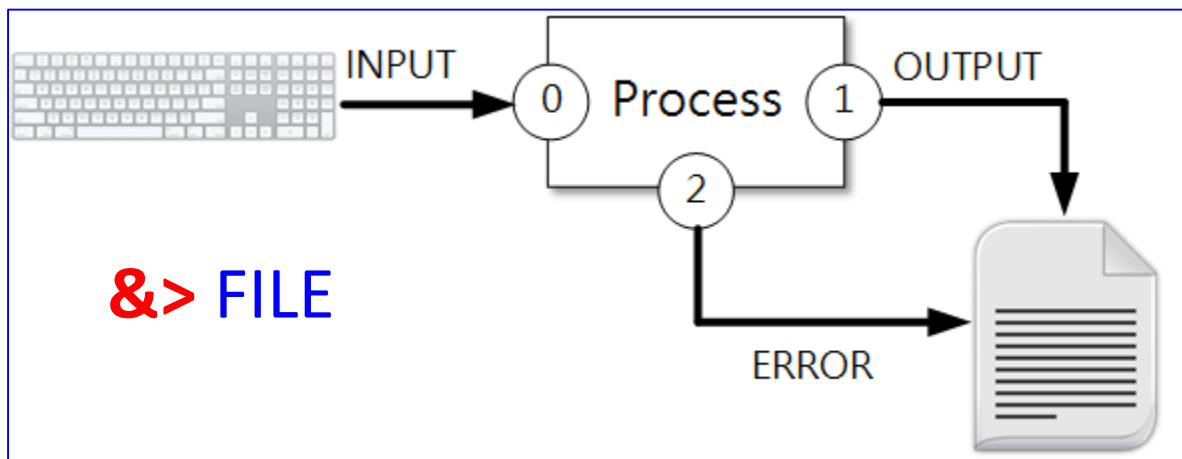
輸出重導



錯誤重導

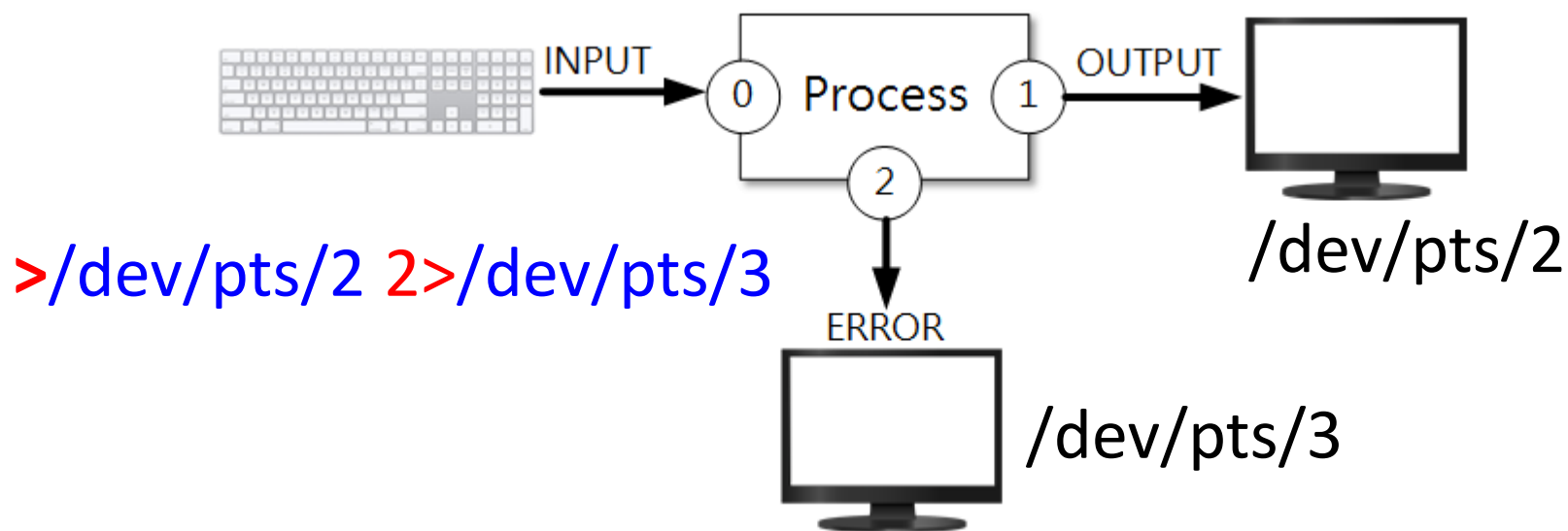
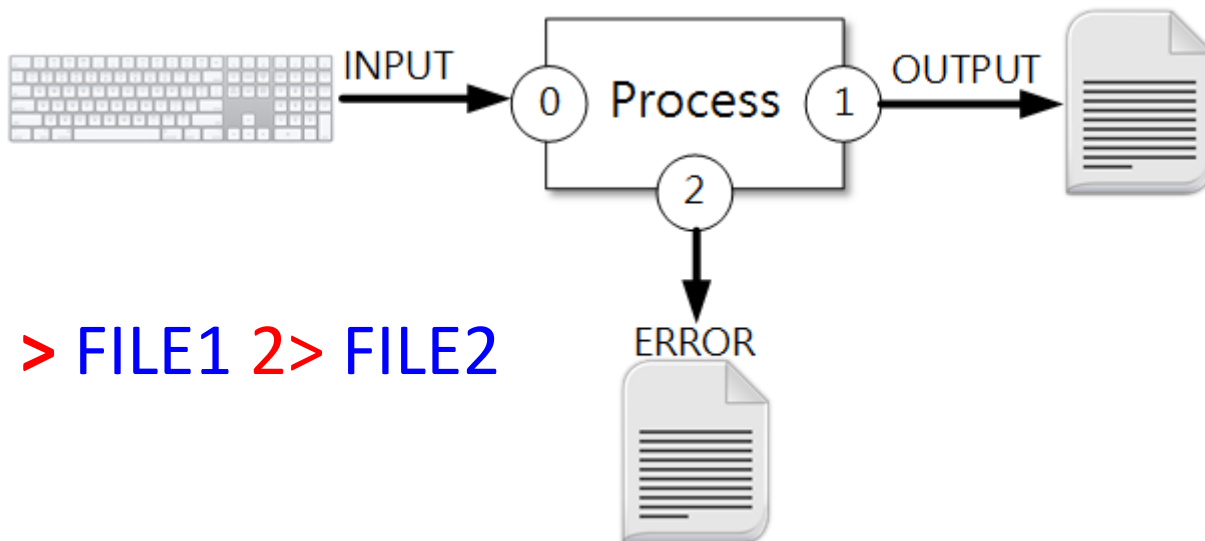


合併重導

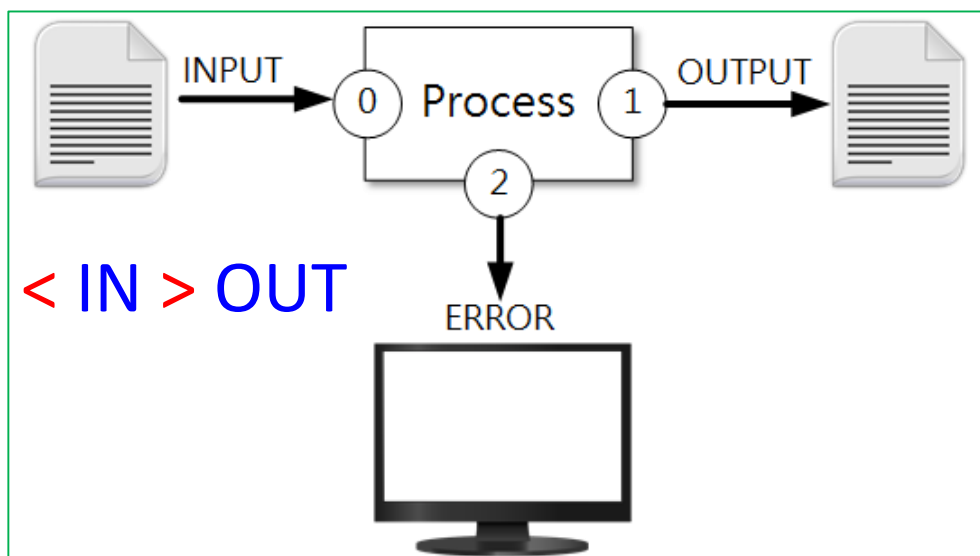
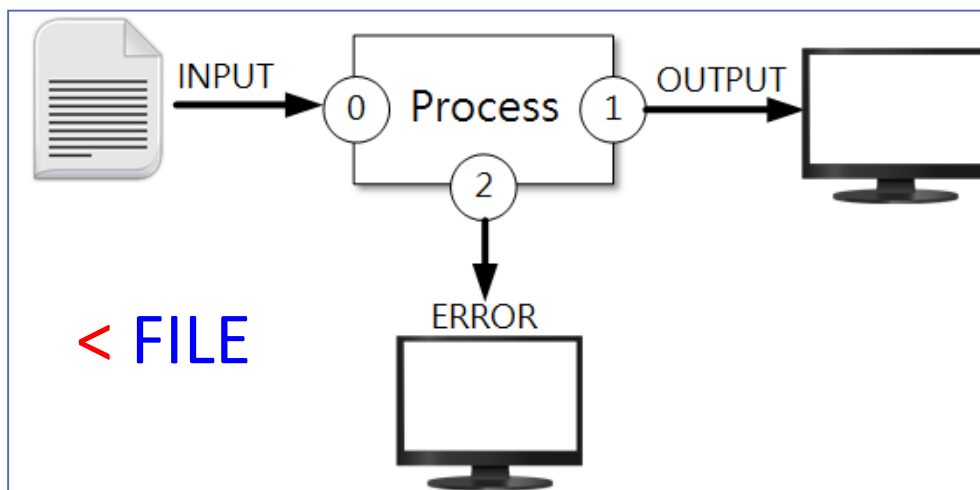


2>&1 較常用於搭配 PIPE 使用

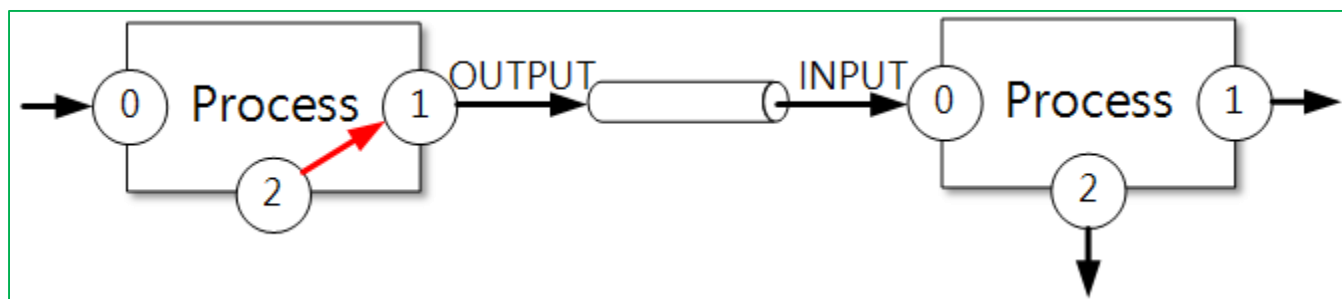
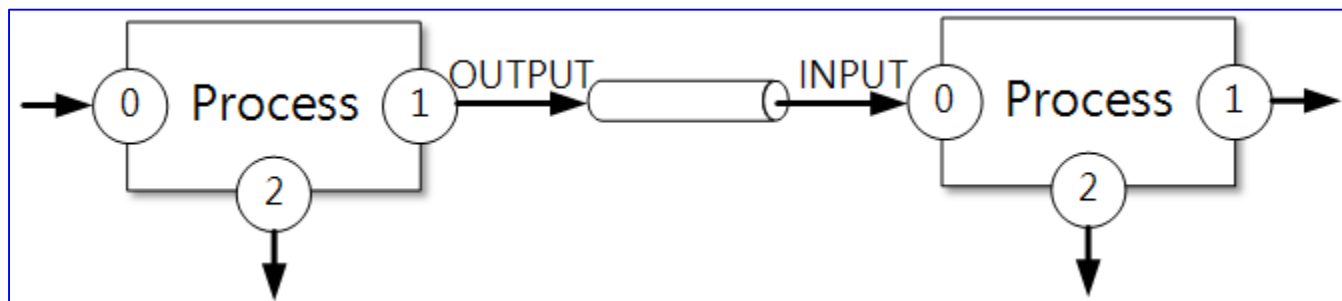
個別重導



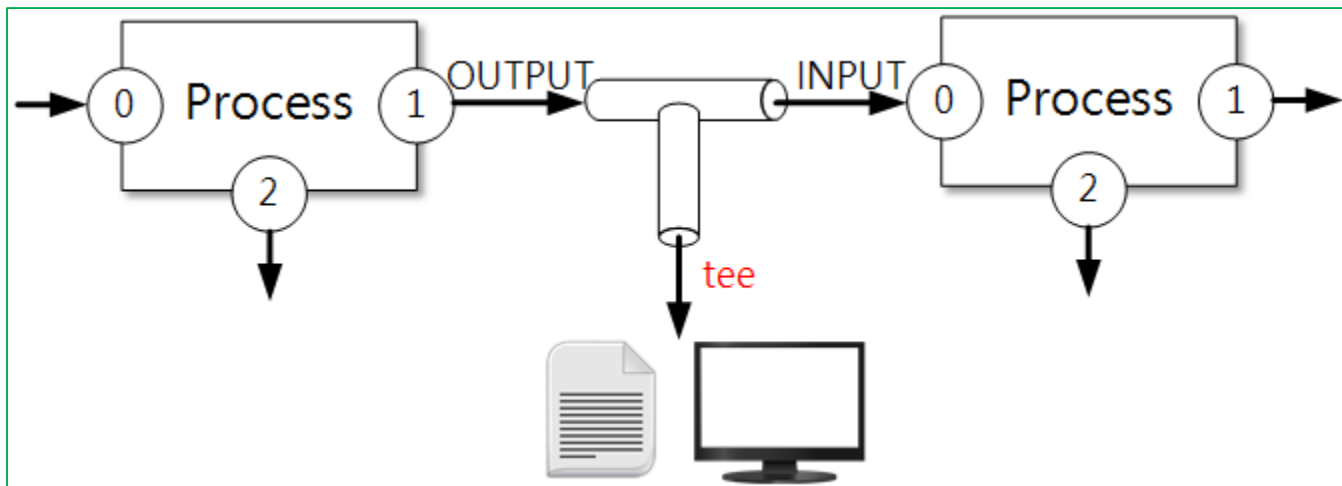
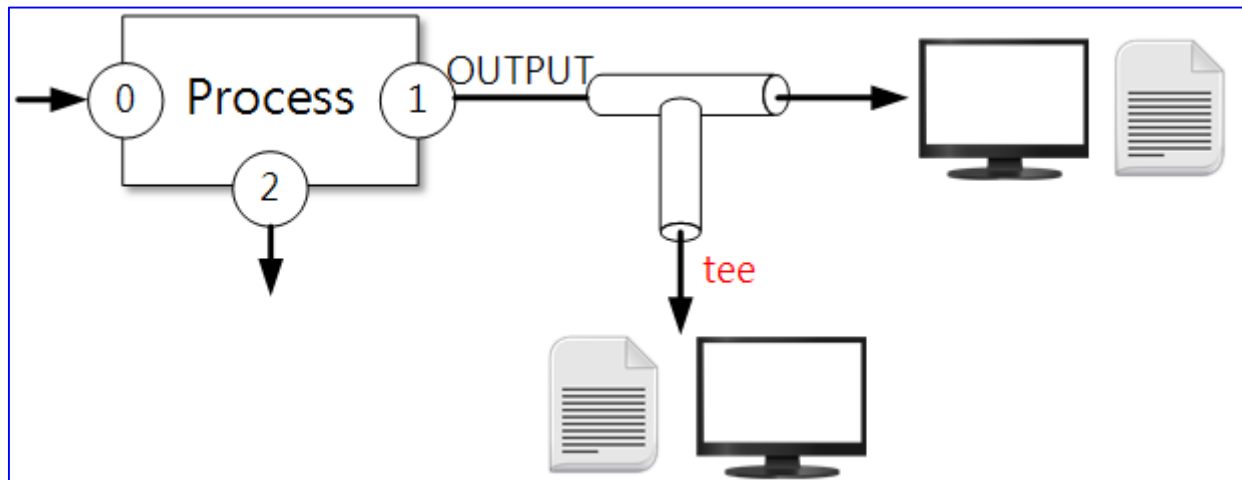
輸入重導



管線命令



多重輸出

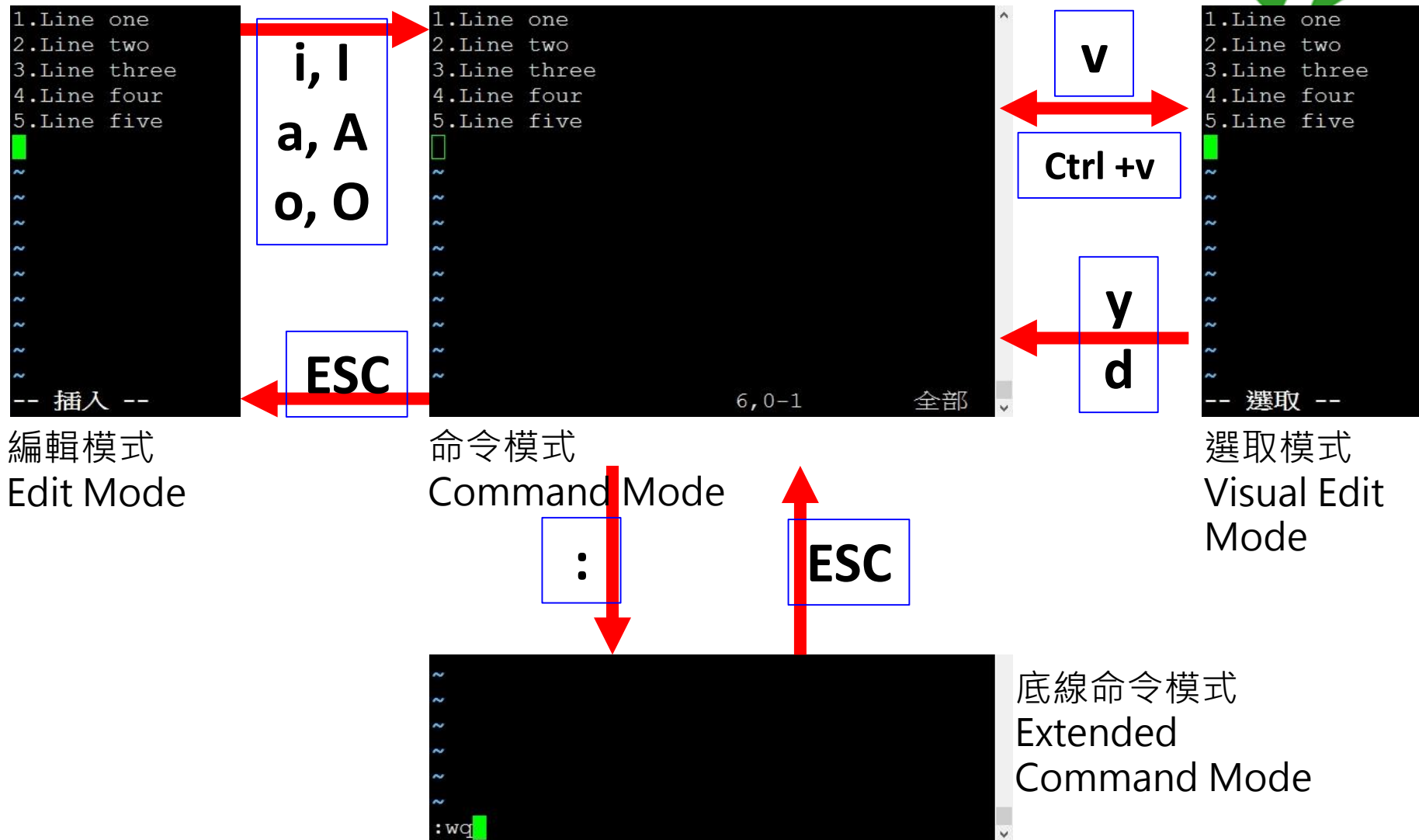


指令重導、管線



- 請練習前述各項指令重導及管線之指令及操作

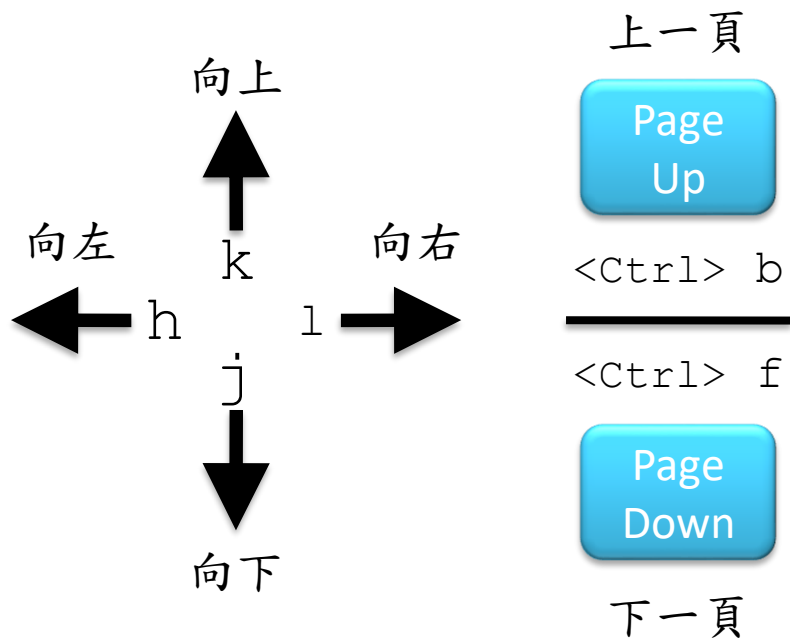
文字編輯器 VIM



文字編輯器 VIM



- 命令模式
游標移動：



指令				說明
^		<Home>		移至行首 (也可使用數字0)
\$		<End>		移至行尾
b		B		向左移動一個字 (B跳過某些標點)
w	W	e	E	向右移動一個字 (w字首、e字尾)
<i>n</i> <Space>				向後移動 <i>n</i> 個字元
<i>n</i> <Enter>				向下移動 <i>n</i> 行
<i>n</i>				移至本行第 <i>n</i> 個字元
G				到最後一行
<i>n</i> G				到第 <i>n</i> 行
gg				到第一行
H	M	L		移至畫面的 H上 M中 L下

文字編輯器 VIM



• 選取模式

指令		說明
d		刪除選取區域的內容
y		複製選取區域的內容

• 命令模式

指令		說明	
x		刪除游標所在處字元 (含)	
X		刪除游標前一個字元 (不含)	
nx		刪除游標後 <i>n</i> 個字元 (含)	
nX		刪除游標前 <i>n</i> 個字元 (不含)	
dh	dl		dh=X dl=x
db	de	dw	刪除整個字 (b左、ew右)
d0			刪除至行首 (不含)
D	d\$		刪除至行尾 (含)

• 命令模式

指令		說明	
dd		刪除一整行	
cc		刪除一整行且進入編輯模式	
n dd		向下刪除 <i>n</i> 行(含)	
dnG		刪除至第 <i>n</i> 行(含)	
dG		刪除至最後一行(含)	
d <i>n</i> <space>		向後刪除 <i>n</i> 個字(含)	
y y	Y	複製本行	
nyy		複製 <i>n</i> 行(含)	
ynG		複製本行至第 <i>n</i> 行(含)	
y b	y e	y w	複製整個字(b左、ew右)
y <i>n</i> <space>		向後複製 <i>n</i> 個字元(含)	
p		小寫p，貼上至游標後	
P		大寫P，貼上至游標前	

文字編輯器 VIM



• 命令模式

指令	說明
u	還原上一個動作 (無限次)
U	還原剛才那一行的變更
<Ctrl> r	重做 (剛好和 u 相反)
.	重複上一個指令 (刪、貼)
~	大小寫互換
ZZ	儲存並離開
J	將下一行結合在本行之後
r	取代游標處字元
R	取代字元至按 Esc 止

• 命令 → 編輯模式

指令	說明
i	從游標所在字元開始插入
I	從本行第一個字元開始插入
a	從游標後一個字元開始增加
A	從本行最後字元開始增加
o	小寫，插入新一行 (下)
O	大寫，插入新一行 (上)
	刪除游標所在處字元
<Home>	移至行首
<End>	移至行尾

文字編輯器 VIM



• 底線命令模式

指令		說明
<code>:q</code>	<code>:q!</code>	退出、強制退出
<code>:w</code>	<code>:wq</code>	儲存、儲存並離開 (ZZ)
<code>:x</code>		小寫，離開或儲存並離開
<code>:r file</code>		讀取file內容到游標後
<code>:w file</code>		儲存成file檔案
<code>:e file</code>		編輯file檔案
<code>:n1, n2 w file</code>		n1至n2行存成file檔案
<code>:set nu</code>		設定行號 (<code>:set nonu</code>)
<code>:mkvimrc</code>		產生VIM的設定檔
<code>:! command</code>		執行外部command命令

• 底線命令模式

指令		說明
<code>/</code>	<code>?</code>	向下 (/) 向上 (?) 搜尋
<code>n</code>	<code>N</code>	下 (n) 上 (N) 一個搜尋結果
<code>%</code>		尋找對應的括號 () [] {}
搜尋並取代 <code>: [range] s/pattern/string/ [g,c,i,e]</code> 例 <code>:%s/2017/2018/gc</code>		
[range] 搜尋範圍，%代表全文，或以a,b 代表從第a行找到第b行 pattern 要找的內容 string 要換成的內容 [g,c,i,e] 參數，g 整行所有找到的全部替換，c 替換前要詢問，i 不分大小寫，e 不顯示錯誤		

視窗文字編輯器 gedit



- 應用程式 → 附屬應用 → gedit
- **\$gedit** FILE
- 在「終端機」內的文字

複製：Ctrl + Shift + c

貼上：Ctrl + Shift + v



VIM練習



- 用 `ls -al` 將 `/tmp` 目錄下所有檔案及目錄列出，並重導到 `/tmp/tmp.ls`
- 用 `vim` 或 `gedit` 編輯 `/tmp/tmp.ls`
- 將所有權限標籤(如 `drwxrwxrwx.`) 全部刪除，但須保留該行其他資料
- 將所有使用者及群組為 `root` 的改成 `ntpcuser`
- 存檔並退出

使用者管理



說明	相關檔案	相關指令
使用者管理	/etc/passwd	#useradd #usermod #userdel -r \$id <username>
群組管理	/etc/group	#groupadd #groupmod #groupdel
密碼管理	/etc/shadow	\$passwd #passwd <username> #chage

- 最高權限管理者：root
- 使用者切換(Switch User)：\$su - <username> (exit 退出)
- 暫時使用管理者權限執行命令：\$sudo command
- CentOS 7 會自動將 wheel 群組賦予 sudo 權限

檔案權限



• 檔案權限

drwxr-xr-x.

檔案型態 擁有者權限 群組權限 其他人權限

d : 目錄
- : 檔案
l : 連結
b : 儲存設備
c : 其他週邊

r : 讀取 4
w : 寫入 2
x : 執行 1

drwxr-xr-x.	2	root	root	4096	1月	23	11:34	bash_completion.d
-rw-r--r--.	1	root	root	2835	8月	12	2015	bashrc
drwxr-xr-x.	2	root	root	6	11月	20	2015	binfmt.d
drwxr-xr-x.	2	root	root	12288	1月	23	11:31	brlTTY
-rw-r--r--.	1	root	root	21929	3月	6	2015	brlTTY.conf
-rw-r--r--.	1	root	root	38	12月	9	2015	centos-release
-rw-r--r--.	1	root	root	51	12月	9	2015	centos-release-upstream
drwxr-xr-x.	2	root	root	6	11月	20	2015	chkconfig.d
-rw-r--r--.	1	root	root	1165	11月	24	2015	chrony.conf
-rw-r-----.	1	root	chrony	62	3月	6	13:09	chrony.keys
drwxr-xr-x.	2	root	root	25	1月	23	11:33	cifs-utils
drwxr-xr-x.	2	root	root	51	1月	23	11:33	cron.d
drwxr-xr-x.	2	root	root	76	1月	23	11:33	cron.daily
-rw-----.	1	root	root	0	7月	27	2015	cron.deny
drwxr-xr-x.	2	root	root	44	1月	23	11:31	cron.hourly
drwxr-xr-x.	2	root	root	6	6月	10	2014	cron.monthly
-rw-r--r--.	1	root	root	451	6月	10	2014	crontab
drwxr-xr-x.	2	root	root	6	6月	10	2014	cron.weekly
-rw-----.	1	root	root	0	1月	23	11:29	crypttab
-rw-r--r--.	1	root	root	1602	6月	7	2013	csh.cshrc
-rw-r--r--.	1	root	root	841	6月	7	2013	csh.login
drwxr-xr-x.	5	root	lp	4096	3月	12	10:01	cups
drwxr-xr-x.	2	root	root	33	1月	23	11:32	cupshelpers
drwxr-xr-x.	4	root	root	74	1月	23	11:31	dbus-1
drwxr-xr-x.	4	root	root	29	1月	23	11:31	dconf

權限

連結數

擁有者

群組

檔案大小

修改日期

檔案名稱

檔案權限 (Permissions)



- Linux 權限控管對象：User、Group、Other
權限控管順序 User > Group > Other
- 權限控管動作：**r** (read), **w** (write), **x** (exec)

Permission	對檔案 (Files) 的控制	對目錄 (Directories) 的控制
r	可讀取檔案的內容	可列出 目錄內的檔名及子目錄 (可 ls)
w	可變更檔案的內容	可在目錄內刪除或建立檔案及子目錄 (無論 目錄內 檔案或空的子目錄是誰的， 都可以 刪除 ，但要先有 x 權限存取目錄)
x	可執行檔案的內容為指令	能存取目錄內容 (可 cd 進目錄)

- #chown** 擁有者:群組 檔案 (變更擁有者及群組)
- #chgrp** 群組 檔案 (變更群組)

檔案權限



- \$chmod 模式 檔案或目錄

u g o a (User, Group, Other, All , 可混搭)

+ - = (add +, remove -, exactly =)

r w x (read, write, executable , 可混搭)

- 權限數值(Numeric Permissions, 8進位模式)

r, w, x 可用

-rw-rw-r--.

-110110100. →二進位

-421421421.

6 6 4 →權限數值

d-rwxr-xr-x.

d111101101. →二進位

d421421421.

7 5 5 →權限數值

檔案權限



- UMASK 會清除該數值所代表的權限：

目錄

預設權限 (666) rwxrwxrwx

權限遮罩 (022) ----w--w-

rwxr-xr-x

7 5 5

檔案

預設權限 (666) rw-rw-rw-

權限遮罩 (022) ----w--w-

rw-r--r--

6 4 4

- root :

目錄權限 755

檔案權限 644

- regular user :

目錄權限 775

檔案權限 664

預設權限：

System :

Directory 777

File 666

UMASK :

root 022

regular user 002

檔案權限練習

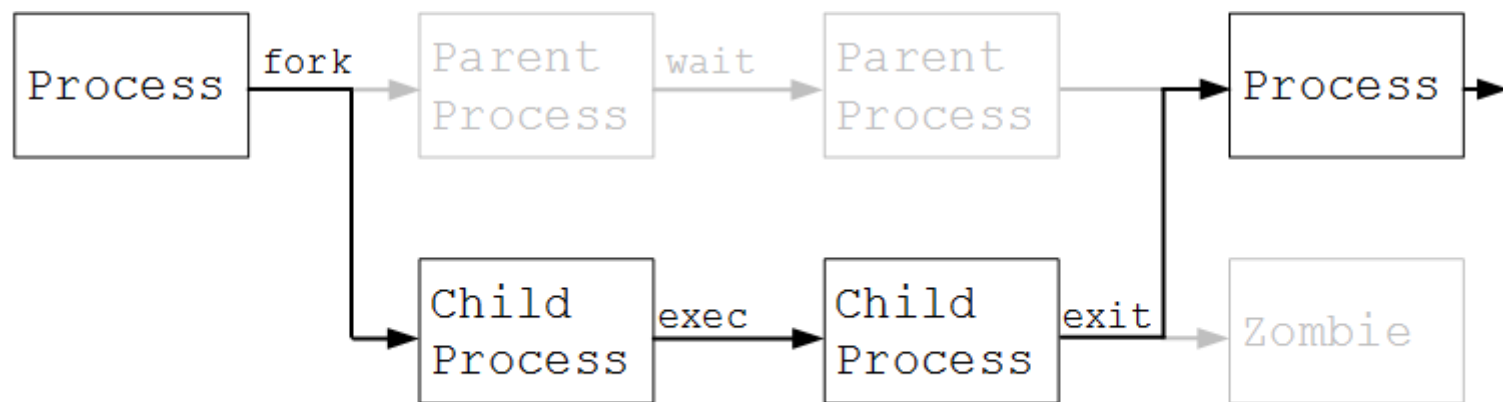


- 建立使用者 `peter`，設定密碼為 `Centos12#`
- 在 `/tmp` 目錄下建立一個 `test.sh` 檔案，並在裡面輸入一行「`ls -al`」文字
- 將 `test.sh` 轉換成「所有人」皆可執行的檔案
- 將身份轉換成 `peter`
- 以 `peter` 的身份執行 `/tmp/test.sh` 檔案

程序管理 (Processes)



- Linux 系統中，觸發任一事件時，系統會將它定義成為一個程序(Process)。
- 系統會給程序一個 ID，稱為 PID (Process ID)。
- 程序能產生(fork) 子程序，子程序會擁有自己的PID，但仍須依存在父程序(Parent's PID)下。



Process Life Cycle

程序管理



- CentOS 7 系統啟動後，第一個程序(PID 1)為 systemd
- 程序狀態

狀態	代碼	說明	狀態	代碼	說明
Running	R	正在執行中	Stopped	T	暫停狀態
Sleeping	S	靜止狀態	Zombie	Z	不存在但還沒清除
	D	不能中斷的靜止狀態		X	已清除

- `$ps aux ($ps -ef)`
 - a : 所有使用者的程序(有TTY的)
 - u : 顯示出程序的使用者
 - x : 列出包含沒有TTY的程序 (eXtended)

程序管理



- 前景程序 (Foreground Process) :
是在終端設備(TTY)上執行的指令，並接受輸出輸入，同時只能有一個前景程序在同一TTY上執行。
- 背景程序 (Background Process) :
沒有TTY控制與互動的指令。
- Job Control

指令	說明	指令	說明
<code>Command &</code>	將指令放到背景執行	<code>fg %num</code>	將 <code>num</code> 號指令放到前景執行
<code>Ctrl + z</code>	暫停程序	<code>bg %num</code>	將 <code>num</code> 號指令放到背景執行
<code>Ctrl + c</code>	終止程序	<code>kill %num</code>	終止 <code>num</code> 號指令
<code>jobs</code>	列出背景程序	<code>ps j</code>	列出 <code>job</code> 相關程序

程序管理



- **\$kill -9** PID (中斷程序)

訊號代碼	英文代號	說明	訊號代碼	英文代號	說明
1	HUP	中斷然後重啟載入設定檔	9	KILL	強制中斷
2	INT	中斷，等同 Ctrl + c	15	TERM	以正常的程序通知程式停止執行，預設選項

- **\$top** (即時程序監控)

功能鍵	說明	功能鍵	說明
?	顯示說明	t	CPU 使用率長條圖
P	依CPU使用率排序	m	記憶體使用率長條圖
M	依記憶體使用量排序	q	退出 top
s	調整資料更新頻率	k	中斷程序

系統及服務設定管理程序



- **systemd** : 系統及服務設定管理程序
d : daemons , 在背景執行工作的程序
systemd 是 CentOS 7 第 1 個執行的程序 , PID 1
systemd 是以 unit 來分類
- **systemctl** :
設定 systemd 的指令集 , <Tab><Tab> 可帶出子指令 ,
預設為 list-units
\$**systemctl**
\$**systemctl** status *name.type* (預設為 service type)

系統及服務設定管理程序



- `systemctl` :
 - #`systemctl` status *name.type* -l (顯示服務狀態)(-l不省略)
 - #`systemctl` status --type=service (只顯示 service 狀態)
 - #`systemctl` start *name.type* (啟動服務)
 - #`systemctl` stop *name.type* (中止服務)
 - #`systemctl` restart *name.type* (重新啟動服務，PID改變)
 - #`systemctl` reload *name.type* (重新載入設定，PID不變)
 - #`systemctl` enable *name.type* (設定開機時啟動服務)
 - #`systemctl` disable *name.type* (設定開機時不啟動)
 - #`systemctl` list-unit-files (列出 units 的開機啟動狀態)

程序與服務練習



- 請練習前述各項指令及操作
- 在前景執行 `sleep 1001` 指令，並將之暫停，再放到背景執行
- 直接在背景執行 `sleep 1002`、`sleep 1003` 指令
- 將 `sleep 1002` 移到前景執行
- 將 `sleep 1002` 中止執行
- 查詢 `sleep 1001` 的 PID
- 中止 `sleep 1001` 的 PID 執行
- 中止在背景執行的 `sleep 1003`
- 查詢 `sshd` 服務的運作狀態
- 停止 `cups` 服務，並設定 `cups` 開機時不啟動



- **SSH** : **S**ecure **S**hell
遠端登入管理的加密安全性連線協議
- **\$ssh** *remote_hostname* (登入遠端主機)
 \$exit 退出遠端 ssh
- 查詢目前登入的使用者：
 \$w -f (-f 選項顯示使用者從何處登入)
 \$who
 \$lastlog (最近一次登入資訊)
- Windows SSH 工具
 [PuTTY](#)、[PieTTY](#)、[Xshell](#)



- 登入SSH或僅執行：

```
$ssh remote_user@remote_host
```

(以 *remote_user* 的身份登入 *remote_host*)

```
$ssh remote_user@remote_host "Command"
```

(以 *remote_user* 的身份登入 *remote_host* 執行 *Command* 後登出，並將執行結果傳送到本地)

- SSH host keys

`~/.ssh/known_hosts` (Client，遠端主機的IDs)

`/etc/ssh/*key*` (Host，本機的 keys)

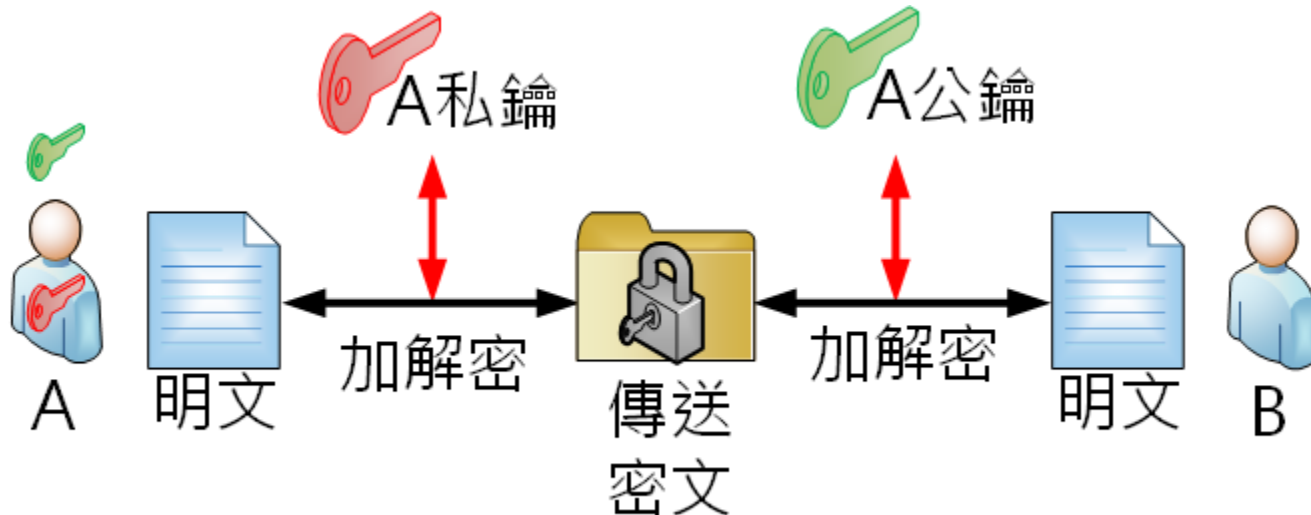


- 對稱式加密

加密解密使用同一把金鑰

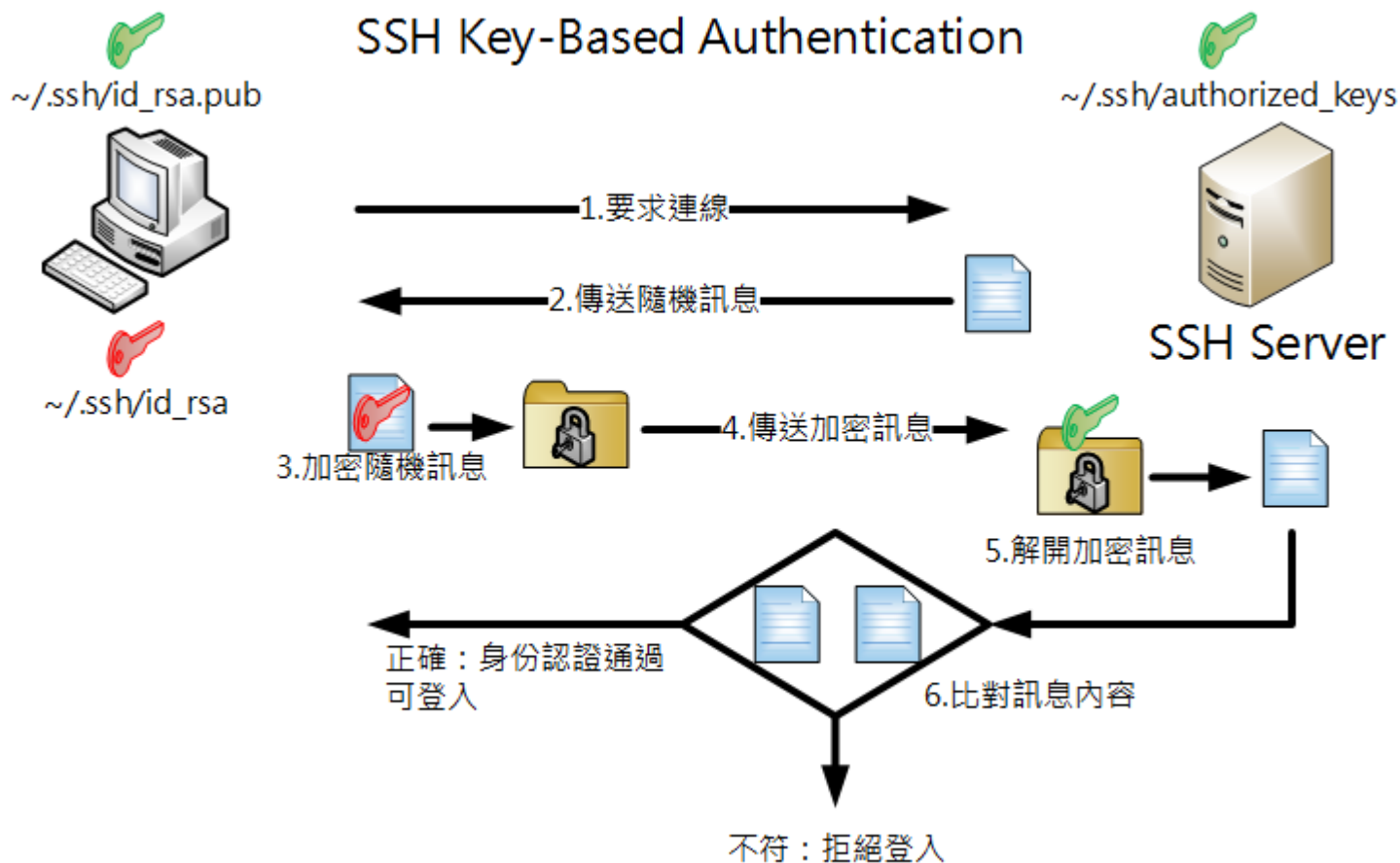
- 非對稱式加密

產生公鑰(Public Key)及私鑰(Private Key)，利用其中一把金鑰加密，只能用另一把金鑰解密





- SSH Key-Based Authentication





- SSH Key-Based Authentication

`$ssh-keygen`

產生 `~/.ssh/id_rsa` 私鑰及 `~/.ssh/id_rsa.pub` 公鑰

`$ssh-copy-id remote_user@remote_host`

將預設的 `id_rsa.pub` 公鑰上傳到 `remote_host` 的
`remote_user` 的家目錄 `~/.ssh/authorized_keys`

- PuTTY 使用 PuttyGen 設定金鑰認證
- PuTTY GUI 遠端執行命令
- PuTTY DOS 指令列執行命令



- Server Config

`/etc/ssh/sshd_config`

`PermitRootLogin yes`

`LoginGraceTime 2m`

`MaxAuthTries 6`

`MaxSessions 10`

`PubkeyAuthentication yes`

`GSSAPIAuthentication no`

`UseDNS no`

#是否允許root登入

#未登入的等候時間

#最多錯誤密碼次數

#最多同時連線數

#是否允許Public key

#使用GSS認證方式，不用

#是否使用dns反查

SSH 練習



- 利用 puttygen 練習從桌機用金鑰驗證方式 ssh 到 CentOS7 測試機
- 利用 Putty GUI 遠端執行命令
- 利用 DOS Command 指令列使用 Putty 遠端執行命令



- 產生 LOG 的服務：
 - systemd-journald** : 收集來自 kernel、早期開機程序、標準輸出、及系統日誌，結構化處理後轉送給 **rsyslog** 做後續處理，並儲存在 `/run/log` 中(記憶體)，重新開機後消失。
 - rsyslog** : 依接收到系統日誌的型別及優先權排序，並寫入到 `/var/log` 內相對應的紀錄檔中保存。
- `/var/log` : 記錄檔存放目錄
 - `/var/log/messages` : 大部份的系統日誌存放檔
 - `/var/log/secure` : 安全驗證相關紀錄，如SSH登入Log



- **rsyslog**
設定檔 `/etc/rsyslog.conf` 及 `/etc/rsyslog.d/*.conf`
- **logrotate**
設定檔 `/etc/logrotate.conf` 及 `/etc/logrotate.d/*.conf`
排程 `/etc/cron.daily/logrotate`
- **#journalctl**
查詢 `systemd-journald` 系統日誌
- 校時：chrony (`chronyd`, `chronyc`)
#timedatectl
#chronyc sources -v (查看同步時間伺服器狀態)
#chronyc -a makestep (立即同步)



- ip 指令：

- \$ip addr show ens33 (顯示該裝置的IP資訊)

- \$ip -s link show ens33 (顯示該裝置的統計)

- 路由除錯：

- \$ip route list (顯示路由表)

- \$ping -c4 *Gateway_IP* (測試預設路由是否回應)

- \$ping6 -c4 *Gateway_IPv6*

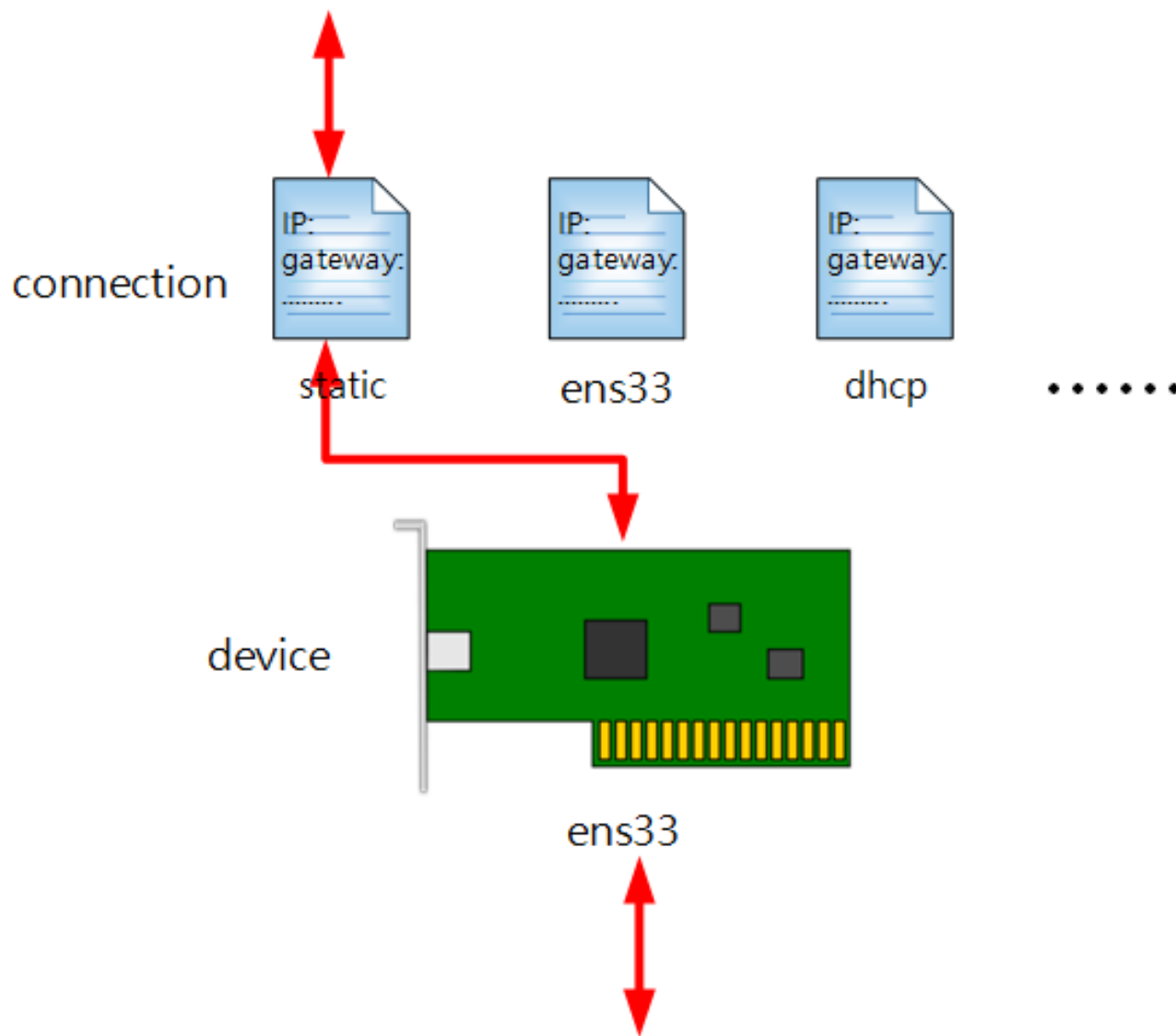
- \$tracert -n 168.95.1.1 (測試到中華電信的路由)

- \$tracert6 -n 2001:b000:168::1



- 連線監視 ss (Socket Statistics) 及 netstat
 - \$ss -at (顯示所有已建立的 TCP Socket)
 - \$netstat -nt (顯示所有 TCP 連線，不要反解 IP)
- 網路管理指令集 nmcli (NetworkManager)
 - #nmcli connection show (顯示連線設定檔)
 - #nmcli connection show --active (顯示啟用的設定檔)
 - #nmcli connection show ens33 (指定連線細節)
 - #nmcli device status (顯示裝置)
 - #nmcli device show ens33 (顯示指定裝置)
 - #nmcli device disconnect ens33 (關閉指定裝置)

網路管理





- 建立與啟用連線

#nmcli con add con-name "dhcp" type ethernet ifname ens33
(con-name 名稱可自取)(是否自動連線?)

#nmcli con add con-name "static" type ethernet ifname ens33
autoconnect yes ip4 192.168.xx.128/24 gw4 192.168.xx.2 ip6
2001:288:223a:5::11/64 gw6 2001:288:223a:5::ff

#nmcli con add help (查看 add 的所有選項)

#nmcli con up "static" (啟動名為 static 的連線設定檔，其他使用同裝置的設定檔會被停用)(這時尚未設定 DNS)(ping -c4 tw.yahoo.com)

#nmcli con modify "static" ipv4.dns 203.72.153.153

#nmcli con modify "static" +ipv4.dns 168.95.1.1

#nmcli con up "static" (改完之後重新 up 以套用變更)

#nmcli con down "static" (關閉連線後，會自動找上一個 autoconnection yes 的連線啟用)



- 連線設定檔
 - /etc/sysconfig/network-scripts/ifcfg-**<name>** (可手動修改)
 - #**nmcli** connection reload (要求NetworkManager載入變更後的設定檔)
 - #**nmcli** connection up **<name>** (啟用該設定檔)
- 主機名稱管理 **hostname, hostnamectl**
 - #**hostname** (查詢主機名稱)
 - #**hostnamectl** set-hostname **xxxxx** (設定主機名稱)
 - #**hostnamectl** status (查詢主機名稱細節)
 - #**cat** /etc/hostname (主機名稱設定檔)



- 名稱解析：

hosts → DNS (先查 hosts 資訊，再查 DNS Server)

設定檔：/etc/hosts → /etc/resolv.conf

#**cat** /etc/resolv.conf (檔案由 NetworkManager產生，建議不要直接修改)

#**ping** www.ntpc.edu.tw (採 hosts → DNS 順序)

#**host** www.ntpc.edu.tw (直接查詢 DNS)

#**nslookup** www.ntpc.edu.tw (直接查詢 DNS)

網路管理練習



- 請練習前述各項指令及操作
- 建立一個手動設定網路配置的 **connection** 設定檔，名稱為 "**static2**"，套用至裝置 **ens33**，設定資料如下：
 - ip : 192.168.xx.228/24 (依 VMplayer 提供的網段而定)
 - gw : 192.168.92.2 (依 VMplayer 提供的網段而定)
 - dns : 203.72.153.154, 8.8.8.8
- 啟動 **static2** 連線，確認網路連線正常
- 回復到 **ens33** 連線，確認網路連線正常

打包與壓縮



- 打包建立壓縮檔

```
#tar zcvgzjf filename.tar.gzbz2 source1 srouce2 .....  
           J           xz
```

- 解開(測試)打包壓縮檔 (-C /folder 解到指定目錄)

```
#tar zxvgzjf filename.tar.gzbz2  
      t J           xz
```


檔案傳輸與備份



- scp 透過 SSH 的 CP，適用單檔傳輸
\$scp [user@]host:/folder/files /local_folder
\$scp /local/files [user@]host:/remote_folder
- rsync 適用於目錄內容的同步與屬性的保留
#rsync -av /var/log /tmp/test (備份 /var/log 整個目錄)
#rsync -av /var/log/ /tmp/test (備份 /var/log/ 下的所有檔案與目錄)
#rsync -av /var/log [user@]host:/remote_folder (備份 /var/log 整個目錄到遠端主機)(加上 --delete 選項會同步刪除遠端檔案)
#rsync -av /var/log /etc/ssh [user@]host:/remote_folder (備份 /var/log 及 /etc/ssh 兩個目錄到遠端主機)

套件安裝



- RPM (Redhat Package Manager)：Redhat 的軟體套件管理系統，Redhat、CentOS、及Fedora皆可以透過 RPM查詢、安裝、更新、移除套件。

Diagram illustrating the structure of an RPM package name: `httpd-2.4.6-67.el7.centos.x86_64.rpm`

The components are mapped as follows:

- NAME**: `httpd`
- VERSION**: `2.4.6`
- RELEASE**: `67`
- ARCH**: `x86_64`

The full package name is: `httpd-2.4.6-67.el7.centos.x86_64.rpm`

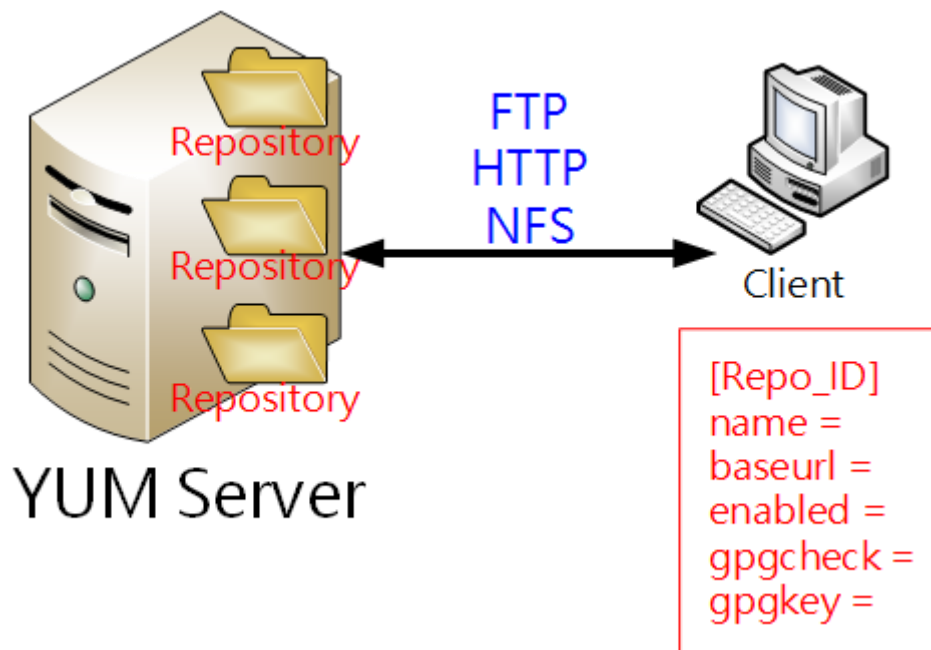
套件安裝



- YUM：查詢、安裝、更新、移除RPM的工具，能自動檢查套件相依性並一併處理。

/etc/yum.conf

/etc/yum.repos.d/*.repo



套件安裝



查詢	安裝	更新	移除
yum list	yum -y install	yum -y update	yum -y remove
yum search	yum -y group install		yum -y groups remove
yum info			
yum provides			
yum groups list			
yum groups info			
yum history			
yum history info			
yum history undo			

套件安裝實作



- 請搜尋並安裝 Apache HTTP Server 軟體套件，同時一併安裝 mod_ssl 加密模組及全部相依性套件。
- 練習前述打包壓縮與傳檔備份

Linux 檔案系統



檔案系統

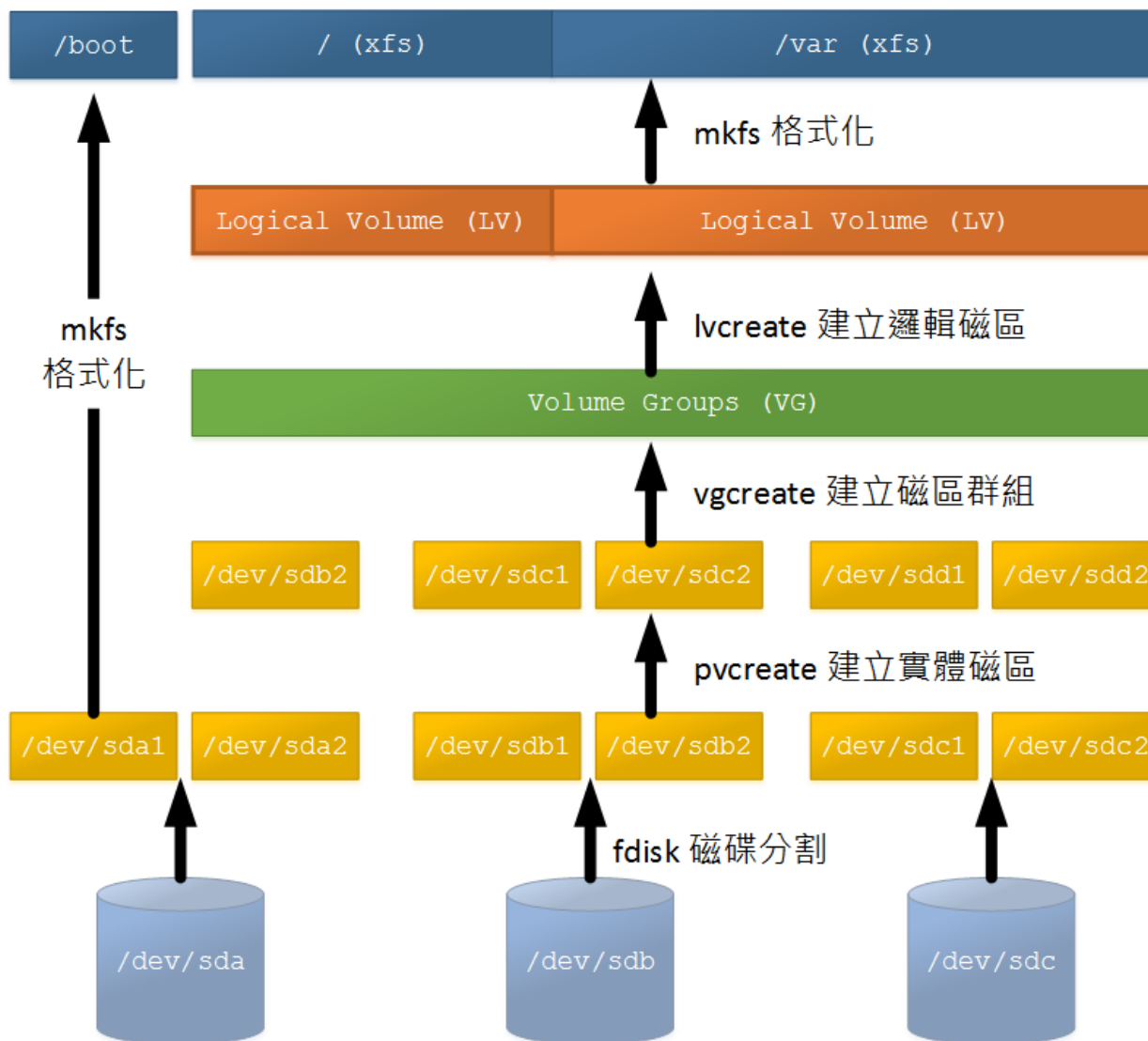
邏輯磁區 (LV)
Logical Volume

磁區群組 (VG)
Volume Group

實體磁區 (PV)
Physical Volume

分割區

實體硬碟



Linux 檔案系統



- **#df -h** (Disk Free , Linux 空間使用狀況)
- **#du -h /etc** (Disk Usage , 計算目錄內檔案佔用空間)
- 檔案連結 (HardLink and SoftLink)

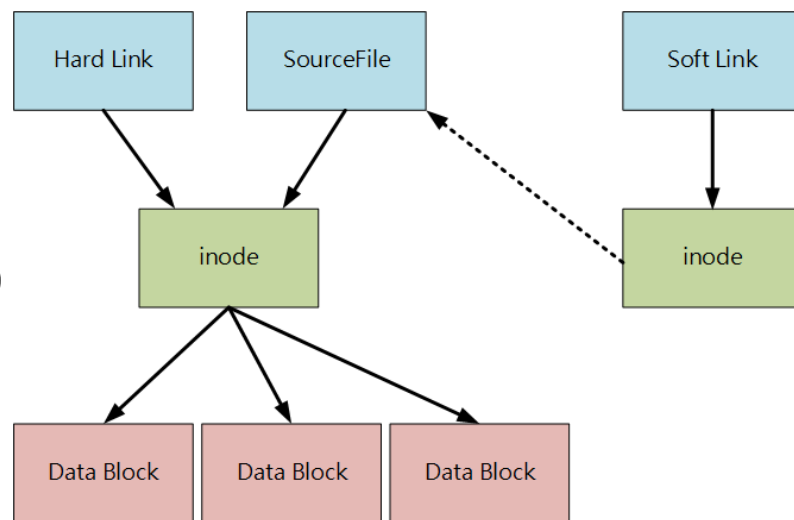
#ln sourcefile hardlinkname

(HardLink , 多一個入口指向 inode)

#ln -s sourcefile softlinkname

(SoftLink , 類似捷徑 , 具不同 inode)

inode : 內容包含檔案大小、擁有者、權限設定、時間戳記、資料區塊位址、連結數等。



Linux 檔案系統



- 檔案尋找

#locate passwd (從每天更新的資料庫中，找到檔名或路徑包含關鍵字的檔案)

#updatedb (更新檔案資料庫)

#find / -name *passwd* (即時搜尋檔案系統裡符合條件的檔案)

#find / -size +10M (搜尋大於10M的檔案)

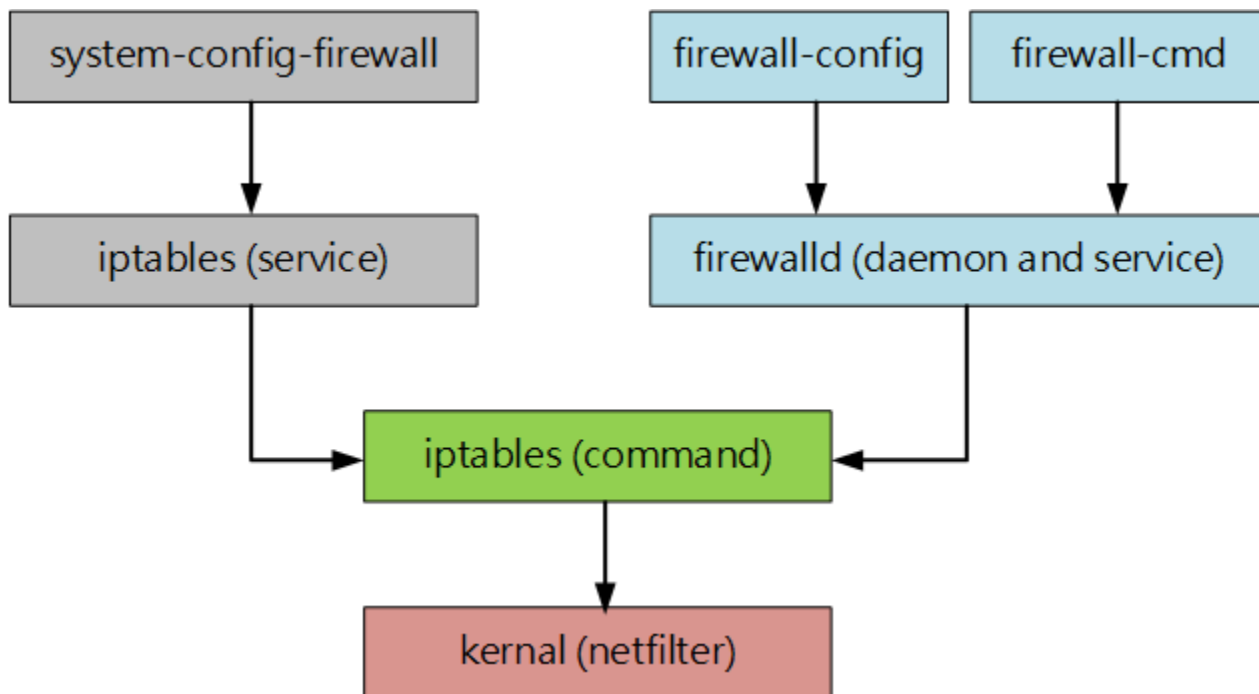
#find / -mmin -60 (搜尋60分鐘內有修改過的檔案)

#find / -type f -links +1 (搜尋有超過1個HardLink的檔案)

本機防火牆 Firewallld



- CentOS 7 採用 firewalld 來與管控網路封包的 netfilter 子系統互動



本機防火牆 Firewall



- ZONE：預先定義9個Zone，預設在 public zone

Zone name	類別	說明
trusted	信任區	接受所有連線
home	家庭環境	信任網域內電腦，只有允許的連線才能進入
internal	內部網路	應用在NAT環境時的對內網路
work	工作環境	信任網域內電腦，只有允許的連線才能進入
public	公開場所	不信任所有電腦，只有允許的連線才能進入
external	對外網路	應用在NAT環境時的對外網路
dmz	非軍事區	內部及外部網路只有允許的才可連線
block	拒絕區	任何進入的封包全部拒絕
drop	丟棄區	任何進入的封包全部丟棄

本機防火牆 Firewall



- firewall-cmd 選項說明

選項	說明
--list-all [--zone=<ZONE>]	列出指定(或預設) zone 的設定
--list-all-zones	列出所有 zone 的設定
--get-defulat-zone	查詢預設 zone
--set-defulat-zone=<ZONE>	設定預設 zone
--get-active-zones	列出啟用的 zone 和相關介面及資訊
--add-service=<SERVICE>	將指定 service 加入允許連線清單
--add-port=<PORT/PROTOCOL>	將指定 port 加入允許連線清單
--remove-service=<SERVICE>	將指定 service 從允許清單移除
--remove-port=<PORT/PROTOCOL>	將指定 port 從允許清單移除
--permanent	將設定寫入永久設定檔
--reload	重新載入永久設定檔

防火牆實作練習



- 啟動 httpd 服務
- 設定防火牆規則，允許 80 與 443 埠連線
- 使用瀏覽器測試 http 及 https 服務是否正常
- 瀏覽測試

`http://192.168.xx.128`

`https://192.168.xx.128`



- CentOS 7 使用 Apache httpd 提供網頁服務
- 安裝 httpd

#yum install httpd mod_ssl openssl (安裝http及https套件)

#systemctl start httpd (啟動httpd服務)

#systemctl status httpd (查看httpd服務狀態)

#systemctl enable httpd (設定開機時啟動httpd)

- 設定防火牆

#firewall-cmd --add-service=http --add-service=https --
permanent (允許 http 80 及 https 443 連線)

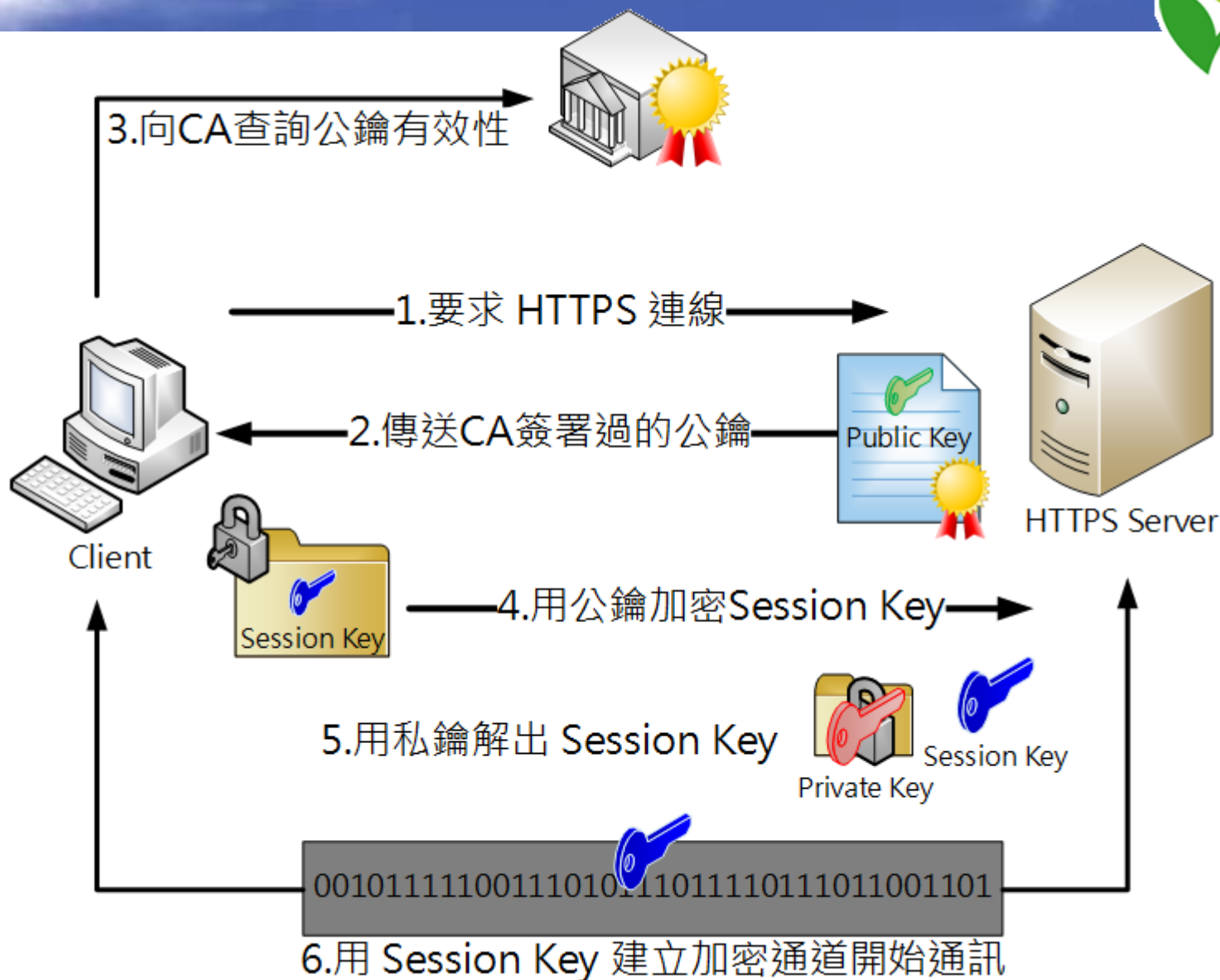
#firewall-cmd --reload

HTTPD



- 設定檔
 - /etc/httpd/conf/httpd.conf
 - /etc/httpd/conf.d/*
- 預設目錄
 - /var/www/html/
- 建立首頁
 - #echo "<H1>HELLO</H1>" > /var/www/html/index.html
- 瀏覽測試
 - http://192.168.xx.128
 - http^s://192.168.xx.128

HTTPD - HTTPS 加密連線



Let's Encrypt 示範



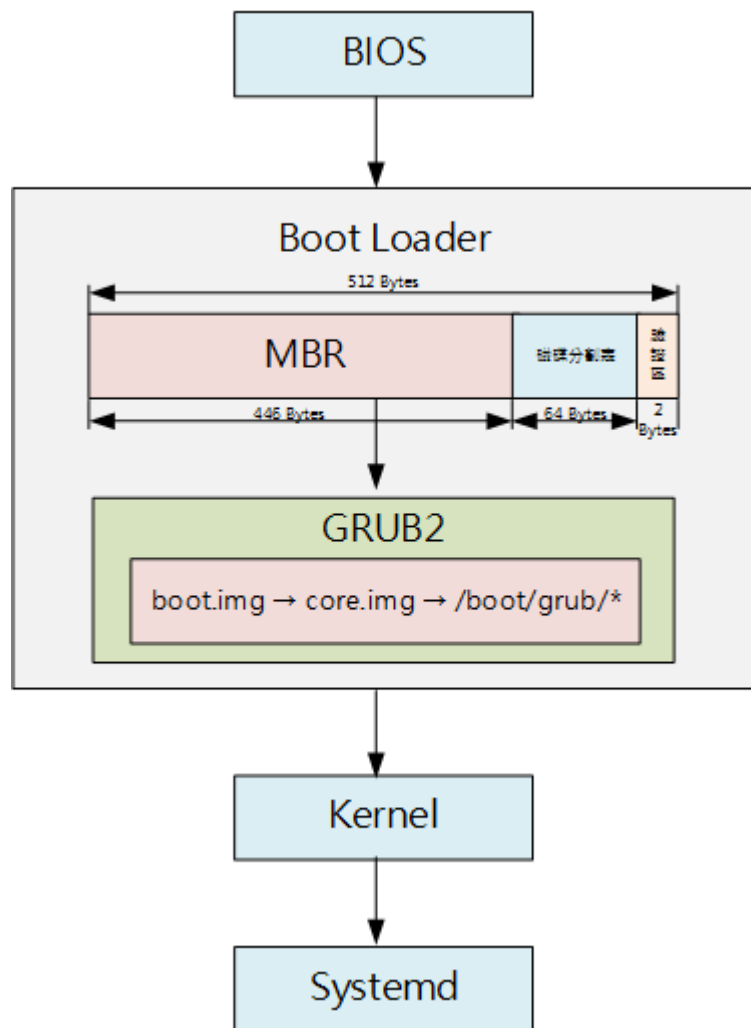
- `#yum install httpd mod_ssl openssl epel-release`
- `#systemctl start httpd`
- `#echo "<h1>HELLO</h1>" > /var/www/html/index.html`
- `#firewall-cmd --zone=public --add-port=80/tcp --add-port=443/tcp --permanent`
- `#firewall-cmd --list-all` (`#iptables -L -n`)
- DNS 設定對應 FQDN
- CertBOT :
 - `#yum search "certbot"`
 - `#yum install python2-certbot-apache` (依前項搜尋結果)
 - `#certbot --staging certonly --webroot -d FQDN1 -d FQDN2 ...`
 - `#certbot certonly --webroot -d FQDN1 -d FQDN2 ...`
 - `#vim /etc/httpd/conf.d/ssl.conf` (將憑證路徑寫入 SSLCertificateFile 及 SSLCertificateKeyFile 設定檔)
 - `#systemctl restart httpd`
 - `#vim /etc/crontab` (* * 1 * * root /usr/bin/certbot renew)
 - `#systemctl reload crond`

HTTPD 實作練習



- 安裝 Apache HTTPD 網頁伺服器並啟動
- 設定開機時自動啟動 httpd 服務
- 設定防火牆規則，允許 80 與 443 埠連線
- 建立測試網頁
- 測試 http 與 https 服務是否正常

開機流程



SysV級別 runlevel	Systemd target	說明
0	poweroff.target	關機
1	rescue.target	單人維護模式
2, 4	multi-user.target	用戶自訂 通常識別為 3
3	multi-user.target	多用戶文字模式
5	graphical.target	多用戶圖形模式
6	reboot.target	重新開機
emergency	emergency.target	急救模式

忘記 root 密碼



- 在開機選單中點 **e** 進入編輯模式
- 找到開機指令行
將 **ro** 改成 **rw rd.break**
- 輸入 **Ctrl + x**
執行改過的指令行
- **#chroot /sysroot**
(將 / 改到 /sysroot 目錄)
- **#passwd root**
(變更 root 密碼)
- **#touch /.autorelabel** (**重要**，要重新標籤 SELinux，不然無法開機成功)
- **#exit** (退出 chroot 模式)
- **#!/shutdown -r** (重新開機)

```
search --no-floppy --fs-uuid --set=root --hint-bios=hd0,msdos1 --hin\
t-efi=hd0,msdos1 --hint-baremetal=ahci0,msdos1 --hint='hd0,msdos1' 31ae56e9-8\
e79-4a16-beb2-3faf65ae35c1
else
search --no-floppy --fs-uuid --set=root 31ae56e9-8e79-4a16-beb2-3faf\
65ae35c1
fi
linux16 /vmlinuz-3.10.0-327.el7.x86_64 root=/dev/mapper/centos-root ro\
crashkernel=256M rd.lvm.lv=centos/root rd.lvm.lv=centos/swap rhgb quiet LANG=\
zh_TW.UTF-8
#linux16 /vmlinuz-3.10.0-327.el7.x86_64 root=/dev/mapper/centos-root r\
o crashkernel=auto rd.lvm.lv=centos/root rd.lvm.lv=centos/swap rhgb quiet LANG\
=zh_TW.UTF-8
initrd16 /initramfs-3.10.0-327.el7.x86_64.img

Press Ctrl-x to start, Ctrl-c for a command prompt or Escape to
discard edits and return to the menu. Pressing Tab lists
possible completions.
```

開關機



- 開機 → 請按電源
- 關機

`#systemctl poweroff`

`#poweroff`

`#init 0`

- 重新開機

`#systemctl reboot`

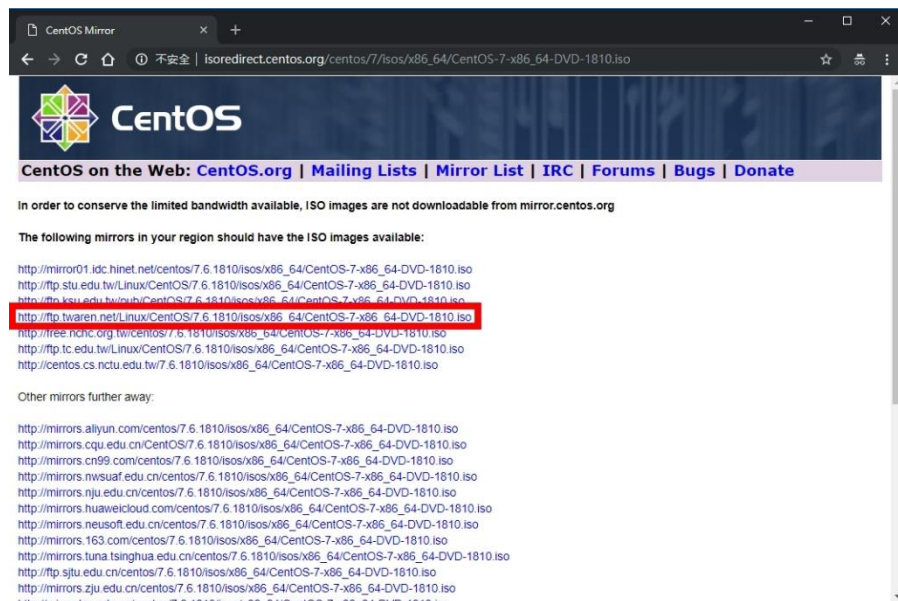
`#reboot`

`#init 6`

CentOS 7 安裝



CentOS 7 安裝



CentOS 7 安裝



```
- Press the <ENTER> key to begin the installation process.
```

```
- Press the <ENTER> key to begin the installation process.

[ 7.605962] dracut-pre-udev[335]: modprobe: ERROR: could not insert 'floppy':
No such device

[ OK ] Started Show Plymouth Boot Screen.
[ OK ] Reached target Paths.
[ OK ] Started Forward Password Requests to Plymouth Directory Watch.
[ OK ] Reached target Basic System.
[ OK ] Started Device-Mapper Multipath Device Controller.
      Starting Open-iSCSI...
[ OK ] Started Open-iSCSI.
      Starting dracut initqueue hook...
      Mounting Configuration File System...
[ OK ] Mounted Configuration File System.
[ 10.537049] sd 0:0:0:0: Isdata Assuming drive cache: write through
[ 12.106451] dracut-initqueue[971]: mount: /dev/sr0 is write-protected, mounting read-only
[ OK ] Started Show Plymouth Boot Screen.
[ OK ] Reached target Paths.
[ OK ] Started Forward Password Requests to Plymouth Directory Watch.
[ OK ] Reached target Basic System.
[ OK ] Started Device-Mapper Multipath Device Controller.
      Starting Open-iSCSI...
[ OK ] Started Open-iSCSI.
      Starting dracut initqueue hook...
      Mounting Configuration File System...
[ OK ] Mounted Configuration File System.
[ 12.106451] dracut-initqueue[971]: mount: /dev/sr0 is write-protected, mounting read-only
[ OK ] Created slice system-checkisomd5.slice.
      Starting Media check on /dev/sr0...
/dev/sr0: 1d2e8463d1bcae8ad491f4e5a07eb79f
Fragment sums: 3b55db189eeea7a20be82b85b49542dcc5ee4bb41bce8ff2fd4d675af7e
Fragment count: 20
Press [Esc] to abort check.
Checking: 0.0/0.0%
```

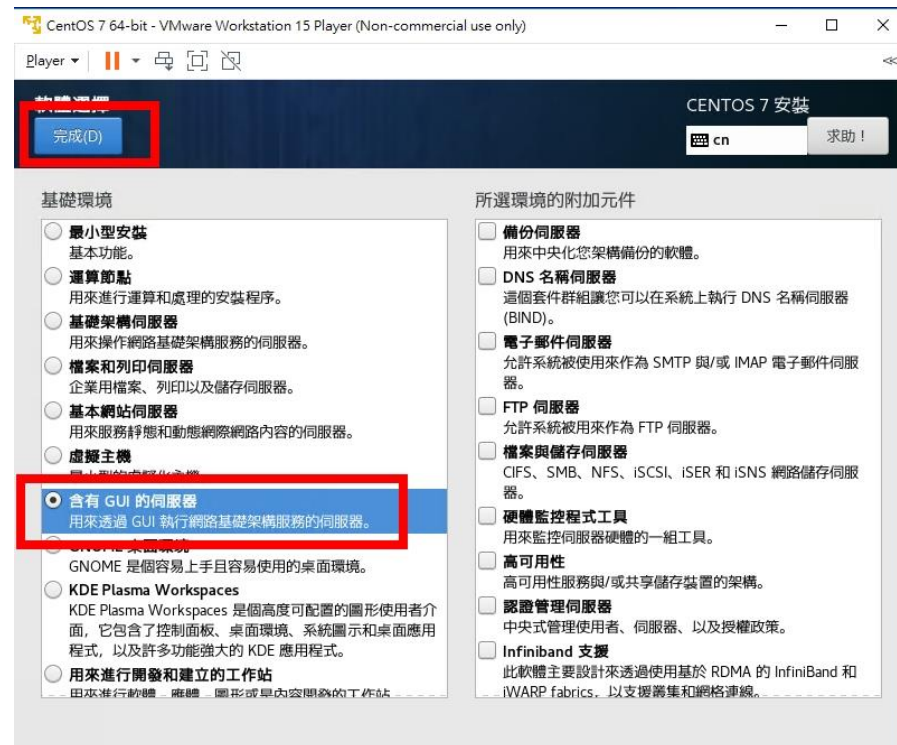

CentOS 7 安裝



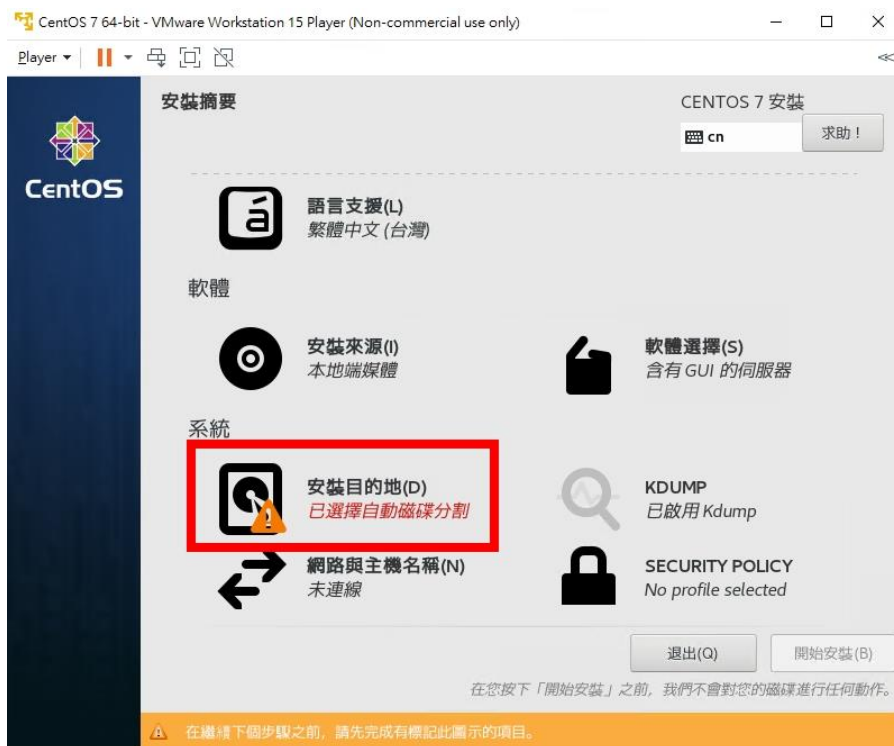
```
[ OK ] Started Device-Mapper Multipath Device Controller.
[ OK ] Started udev Wait for Complete Device Initialization.
      Starting Activation of DM RAID sets...
[ OK ] Started Activation of DM RAID sets.
[ OK ] Reached target Local Encrypted Volumes.
[ OK ] Reached target Local File Systems.
      Starting Migrate local SELinux policy changes...ld store structure to the new structure...
      Starting Rebuild Journal Catalog...
      Starting Import network configuration from initramfs...
      Starting Tell Plymouth To Write Out Runtime Data...
[ OK ] Started Migrate local SELinux policy changes ... old store structure to the new structure.
[ OK ] Started Rebuild Journal Catalog.
[ OK ] Started Tell Plymouth To Write Out Runtime Data.
      Starting Update is Completed...
[ OK ] Started Update is Completed.
[ OK ] Started Import network configuration from initramfs.
      Starting Create Volatile Files and Directories...
[ OK ] Started Create Volatile Files and Directories.
      Starting Update UTMP about System Boot/Shutdown...
[ OK ] Started Update UTMP about System Boot/Shutdown.
[ OK ] Reached target System Initialization.
[ OK ] Listening on Open-iSCSI iscsiui Socket.
[ OK ] Listening on Open-iSCSI iscsid Socket.
[ OK ] Listening on D-Bus System Message Bus Socket.
[ OK ] Reached target Sockets.
[ OK ] Reached target Basic System.
      Starting Login Service...
[ OK ] Started Hardware RNG Entropy Gatherer Daemon.
      Starting Service enabling compressing RAM with zRam...
[ OK ] Started Anaconda NetworkManager configuration.
      Starting Network Manager...
      Starting Wait for Plymouth Boot Screen to Quit...
      Starting Dump dmesg to /var/log/dmesg...
      Starting pre-anaconda logging service...
      Starting Terminate Plymouth Boot Screen...
[ OK ] Started pre-anaconda logging service.
```



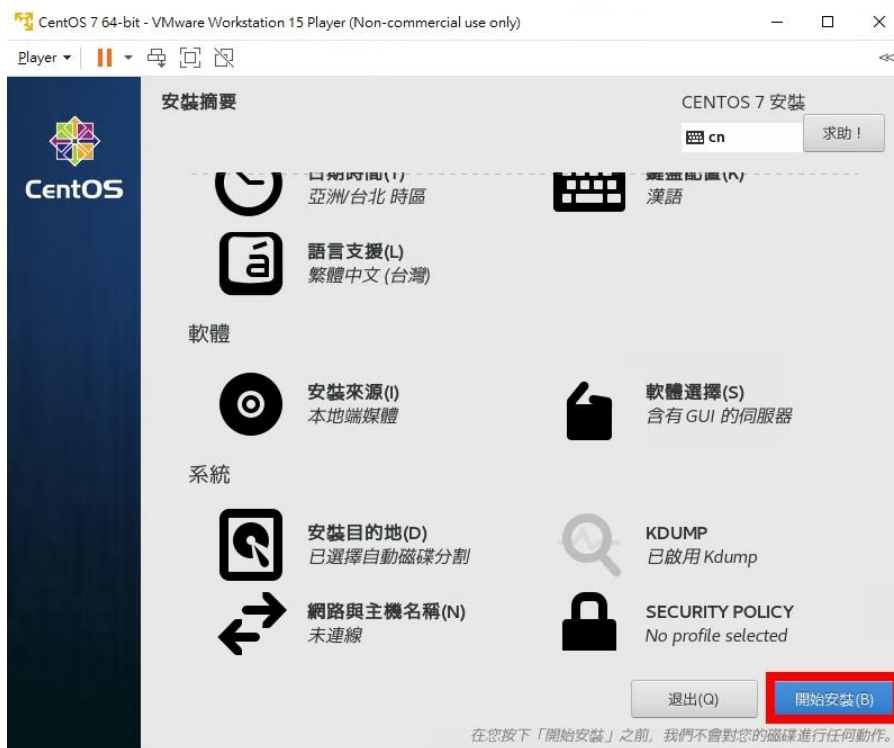
CentOS 7 安裝



CentOS 7 安裝



CentOS 7 安裝



CentOS 7 安裝



ROOT 密碼 CENTOS 7 安裝 cn 求助!

root 是用來管理系統的帳號。請為 root 使用者訂立密碼。

Root 密碼: 強固

確認(C): Centos12#

完成(D)

配置 CENTOS 7 安裝 cn 求助!

用戶設定

 **ROOT 密碼**
Root 密碼已設定

 **用戶建立(U)**
不會建立使用者

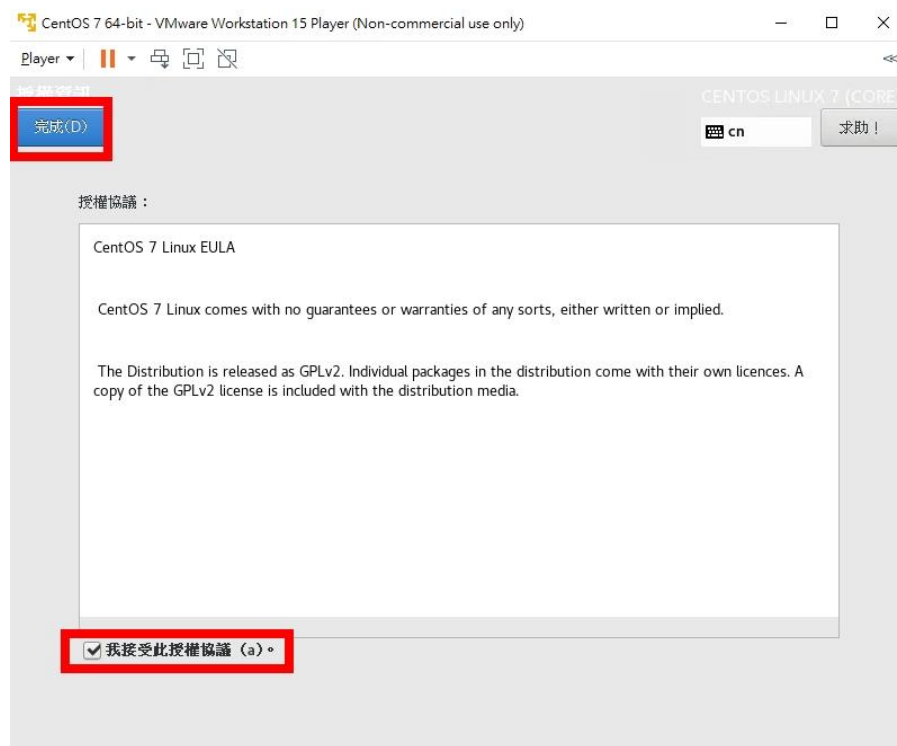
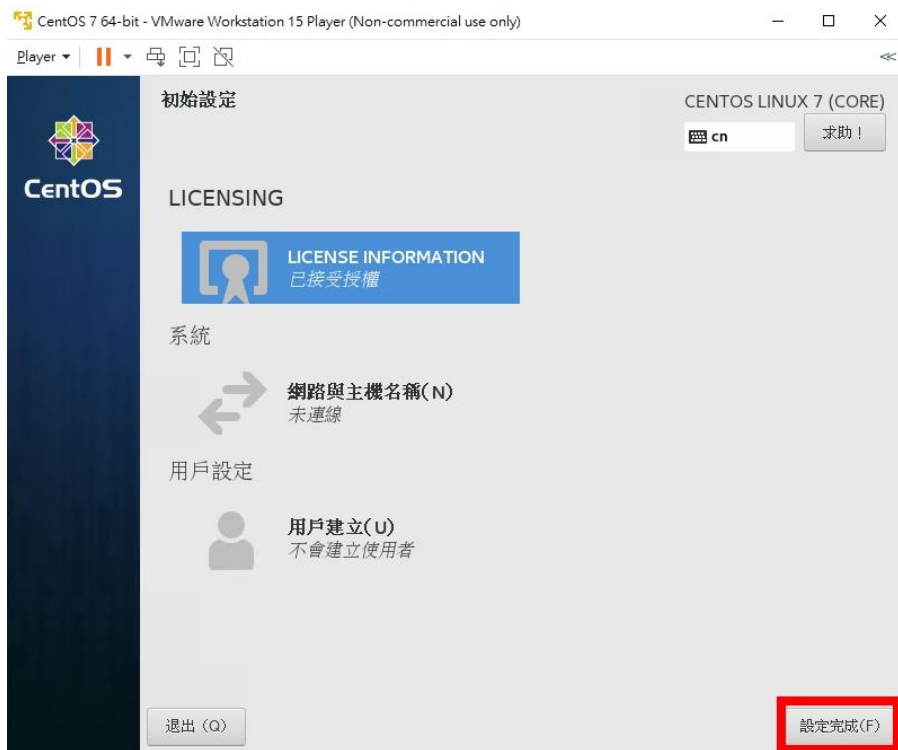
已完成!

CentOS 現在已成功安裝在您的系統上，並準備好供您使用！
現在就請重新啟動並開始使用吧！

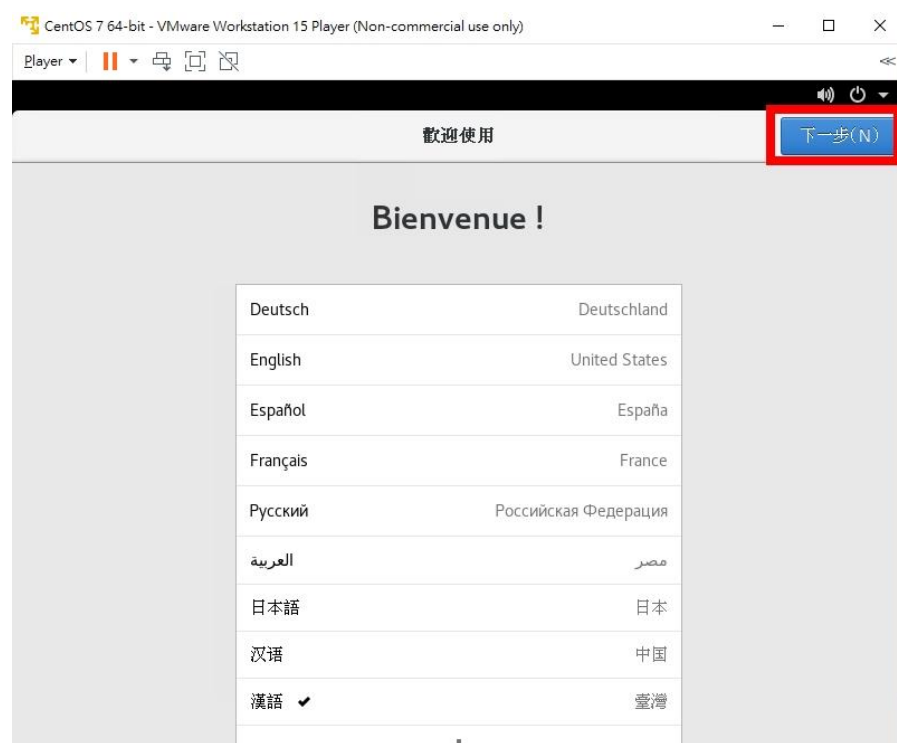
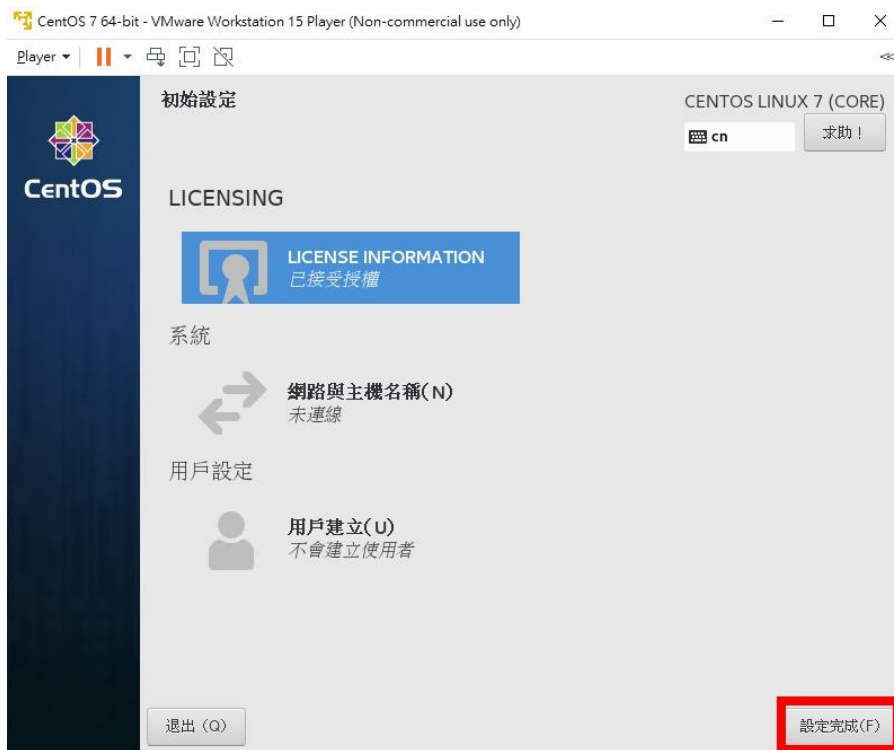
重新開機(R)

⚠ 使用此產品受以下授權協議所控管：/usr/share/centos-release/EULA

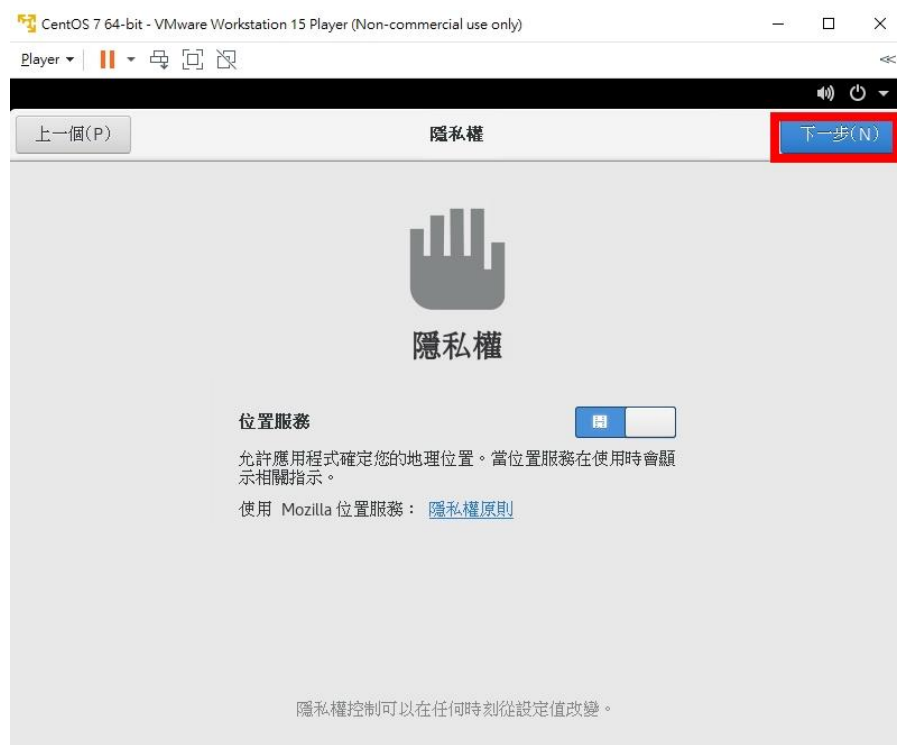
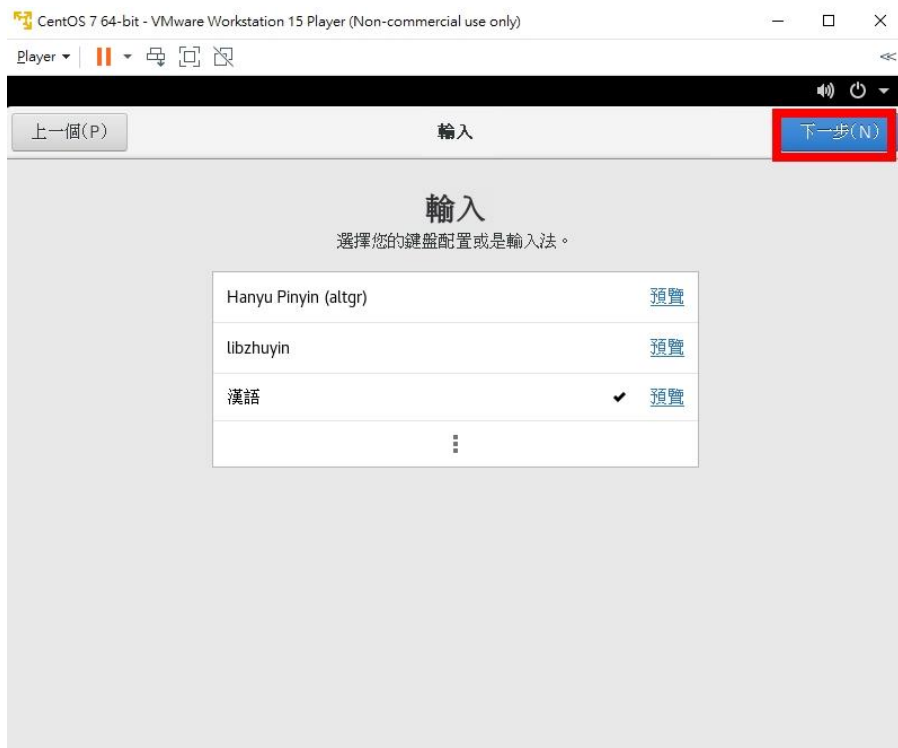
CentOS 7 安裝 (第一次啟動)



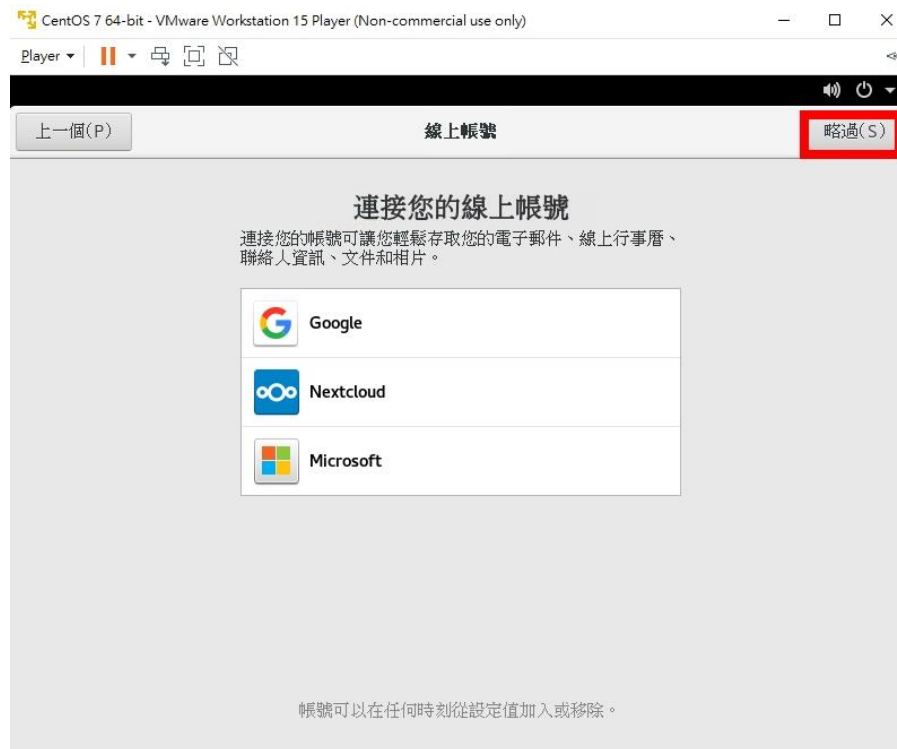
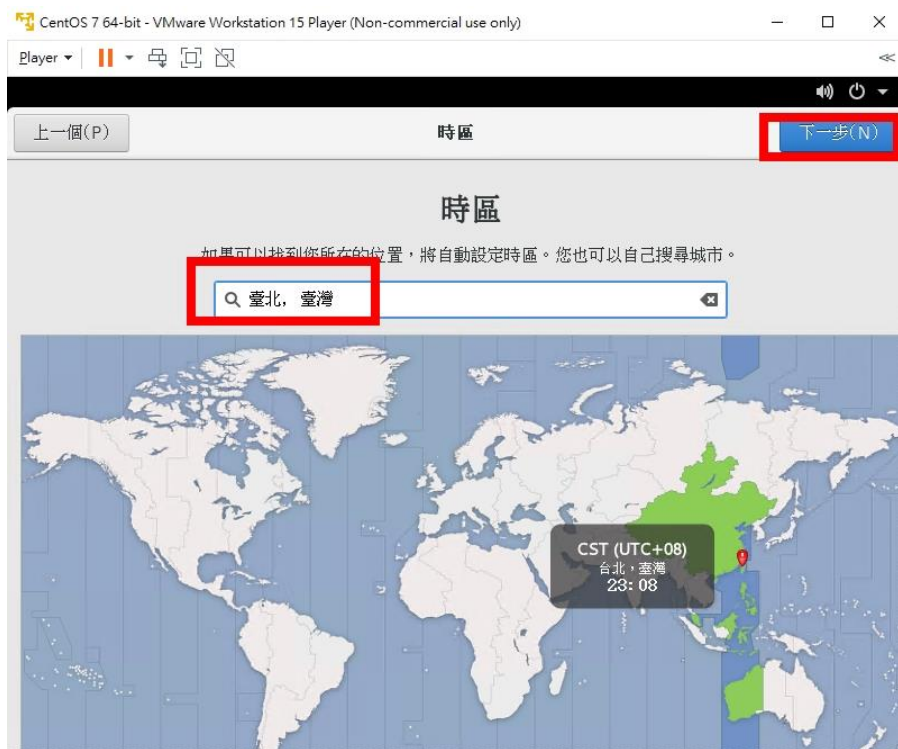
CentOS 7 安裝 (第一次啟動)



CentOS 7 安裝 (第一次啟動)



CentOS 7 安裝 (第一次啟動)



CentOS 7 安裝 (第一次啟動)



CentOS 7 64-bit - VMware Workstation 15 Player (Non-commercial use only)

Player ▾ | 〇 ▾ | 〇 ▾ | 〇 ▾ | 〇 ▾

上一個(P) 關於您 下一步(N)



關於您

我們需要一些資料來完成設定。

全名(F) ✓

使用者名稱(U) ✓

這會成為你登入系統的名稱，並且不能被改變。

設置企業登入(E)

CentOS 7 64-bit - VMware Workstation 15 Player (Non-commercial use only)

Player ▾ | 〇 ▾ | 〇 ▾ | 〇 ▾ | 〇 ▾

上一個(P) 密碼 下一步(N)

設定密碼

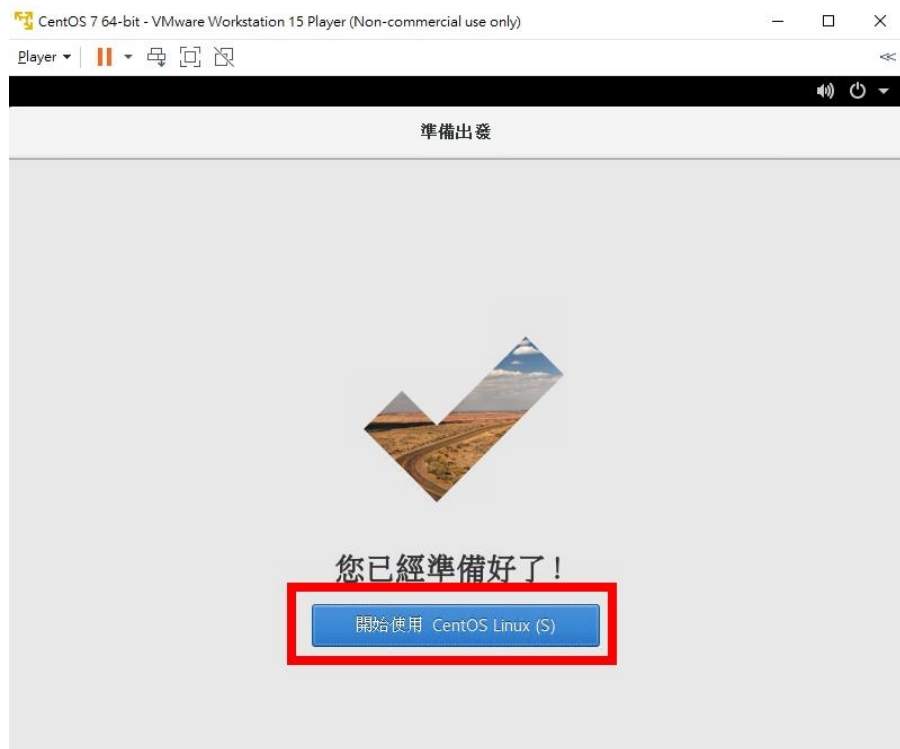
請小心不要遺失您的密碼。

密碼(P) ✓

若能加入更多字母、數字、半形標點符號會讓密碼更強。

確認(C) ✓

CentOS 7 安裝 (第一次啟動)



CentOS 系統安裝設定與管理

謝謝指教



新北市政府教育局
教育研究發展科

80723456 # 516 林璟豐