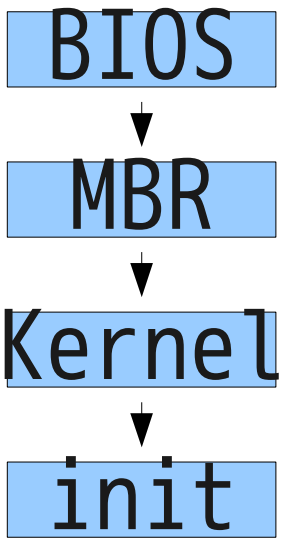
Section2

開機流程



POST

選取開機的

Kernel

驅動硬體

所有 Process 之根據 /etc/inittab

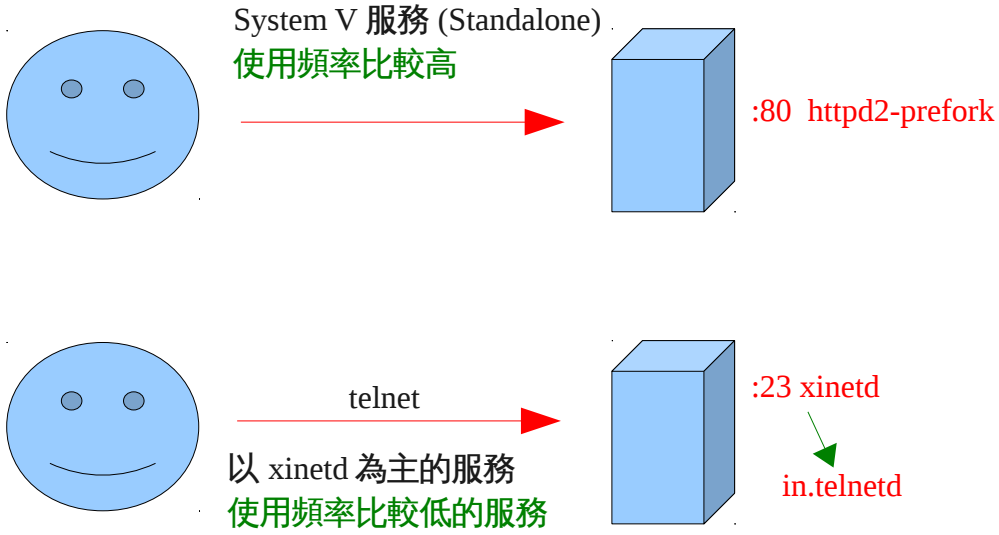
首 進行系統的開機初始化

進行系統初始化

/etc/inittab

語法: 四個欄位
工作代碼:Runlevel:動作:指令

*設定開機的 Runlevel
*利用/etc/init.d/boot 進行系統的初始化(類似 RedHat 的 rc.sysinit)
-啟動相關的機制 例如 LVM/RAID/quota 可觀察/etc/init.d/boot.d
-掛載相關的 Directory 例如 /proc
-執行使用者自訂的 script (使用/etc/init.d/boot.local 類似 RedHat 的 rc.local)
*根據預設的 runlevel 執行 /etc/init.d/rcx.d 的服務
*設定 使用者 在伺服器前按下 Ctrl + Alt + Del 按鍵 會重開機 shutdown -r
*要求 Keyboard Request 設定
*設定 UPS 相關的設定
*啟動六個 Virtual Console
開機完成



System V 服務 與 以 xinetd 為主的服務

當對 System V 服務下啟動指令時, 並不代表 開機會啟動
可利用 chkconfig 或是 insserv 在開機流程設定 啟動 script
可以檢查 /etc/init.d/rcX.d 資料夾內有沒有相關的 script 啟動(X 為啟動的 runlevel)

當對 以 xinetd 為主的服務 下啟動指令的時候
事實上是修改該服務設定檔內 disable = yes 是否存在
舉例來說 #chkconfig telnet on
可以觀察 /etc/xinetd.d/telnet 設定檔內的 disable=yes 會被移除
xinetd 啟動時就會對應相關的服務

亦可利用 chkconfig --list 觀察系統預設開啟的服務

	System V 服務	以 Xinetd 為主的服務
定義	/etc/init.d/*	/etc/xinetd.d/*
啟動/停止該項服務	#/etc/init.d/服務名稱 start #/etc/init.d/服務名稱 stop 在 SuSE 下可以使用 #rc 服務名稱 start #rc 服務名稱 stop 在 RedHat 下可使用 #service 服務名稱 start #service 服務名稱 stop	#chkconfig 服務名稱 on #chkconfig 服務名稱 off
開機的時候應該啟動/停止	#chkconfig 服務名稱 on #chkconfig 服務名稱 off	
其他	#chkconfig 服務名稱 --list #rc 服務名稱 status #rc 服務名稱 reload #rc 服務名稱 restart	#chkconfig 服務名稱 --list

Section 3

Program: An execuable file.
Process: A running program.
User Process: 由使用者啟動的 process.
Daemon Process: 系統預設啟動的 process.

在 Linux 系統可以利用
#ps 來觀察目前的 process 的狀態
每一個 process 都有自己的 PID(Process ID)

#pstree 來觀察 process 的關係

工作控制
- 指令 & 直接在背景執行
- jobs 觀察背景執行或是暫停的工作
- bg 把暫停的工作丟到背景執行
- fg 把暫停的工作丟到前景執行
- Ctrl + Z 暫停前景正在執行的工作

nice 針對還沒有執行的指令指定優先性
renice 針對已經執行的指令指定優先性

程式執行的優先性
給定的範圍為 +19 到 -20 數字越小越優先
只有 root 可以給負的 NICE 值

** Section4 **

有關於裝置的名稱
可以使用 df 來觀察
/dev/hda　　第一個 IDE 控制器的 Master (大概是 2.6.20 以前核心大部分的使用方式)
hda　--> IDE 裝置 第一個 IDE 控制器的 Master
sda　-->SCSI, SATA 裝置
約莫 2.6.20 以後核心, 不管 IDE, SCSI, SATA 都使用 sda
fdisk -l 列出 Partition, 觀察有沒有可用空間

如果要調整 Partition 可以使用
fdisk 裝置代號

- m　　列出可用選項
- p　　列出 Partition Table
- n　　新增 Partition
- d　　刪除 Partition
- t　　轉換 Partition ID
- w　　寫入 Partition Table
- q　　不存檔離開

如果不想重開機想讓 Partition Table 生效可以使用
#partprobe 來通知 OS , Partition Table 有更改(對 2.6 以後核心有效)

可用 #uname -r 觀察核心版本

可以利用 #dumpe2fs 來觀察 ext file system 的 super block
使用 #mke2fs 裝置代號　　來建立 EXT2 檔案系統
使用 #mke2fs -j 裝置代號　　來建立 EXT3 檔案系統
使用 #tune2fs -j 裝置代號　　來將 EXT2 轉成 EXT3 檔案系統

可以使用 df 來列出 已經掛載 file system

mount　　語法
mount　　裝置/資源　　本地目錄
mount　　device/source　　mount point

可以使用 umount　裝置/資料夾　　來卸載裝置或是資料夾
可以使用 fuser -v　資料夾　　來觀察 該資料夾使用情形

傳統方式 mount 的注意事項

- 掛載的目標為裝置的絕對位置,如果絕對位置改變,會找不到分割區

利用 e2label 來顯示/更改 ext2/ext3 檔案系統的 Label name
可以使用 dumpe2fs 裝置代號 | grep vol 來觀察 File system volume name

開機時系統會根據 /etc/fstab 來決定
開機要掛載那些裝置/資源

/etc/fstab 內有 6 個欄位 分別是
裝置/資源 本機目錄 FS_type Mount_Options dump_fre fsck_order

常見的 partition system id

- 82 swap
- 83 linux
- 8e linux LVM
- fd linnx RAID

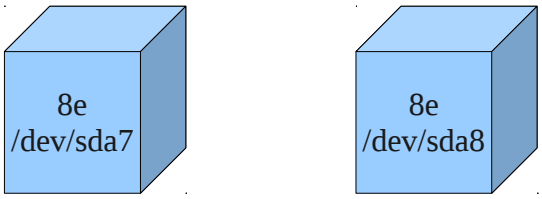
VG(volume group 可以想像為虛擬的硬碟)
PV(physical volume 實體磁碟)
LV(Logical volume 可以想像為虛擬的分割區)
預設 每一個 PE/LE 大小為 4MB

可以利用 #vgextend VG 名稱 實體裝置路徑 來擴充 VG 容量大小
可以利用 #vgreduce VG 名稱 實體裝置路徑 來縮減 VG 容量大小
可以利用 #yast2 disk 來設定 LVM

LVM

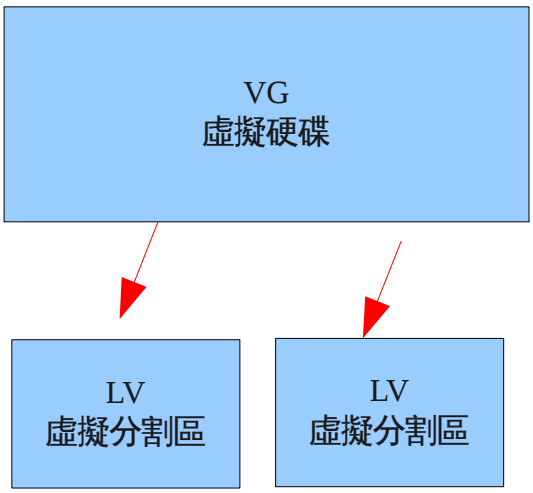
Step1:

- 建立分割區, system id: 8e
- vgscan
- pvcreate



Step2

- vgcreate
- lvcreate
- mke2fs
- 建立 mount point
- mount
- 修改/etc/fstab

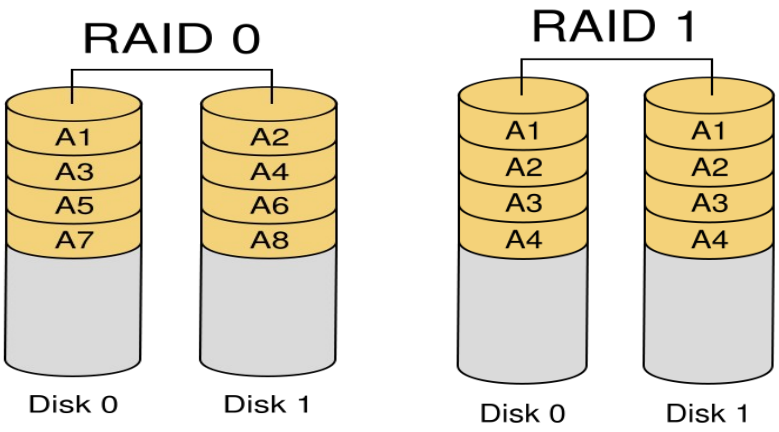


在 SLES 10 使用 ext2online 來針對 LVM2 來讓變更生效, 使用 e2fsadmin 來針對 LVM1 來讓變更生效.
在 SLES 11 ext2online 指令被包括在 resize2fs 指令內, 所以使用 resize2fs 來讓變更生效.

RAID 磁碟陣列

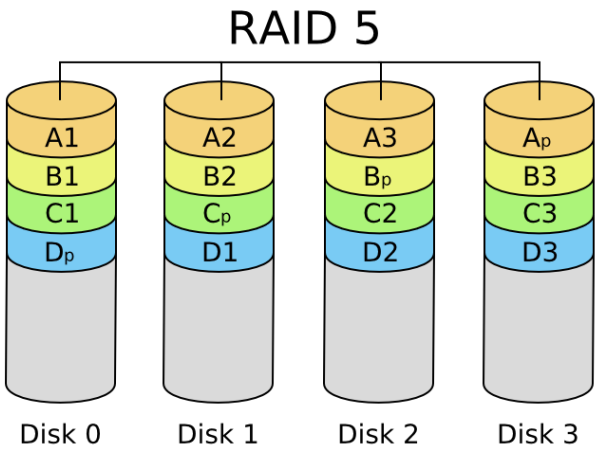
RAID 0

可用容量: 4G
優點: 讀寫速度快
缺點: 沒有容錯能力



RAID 1
可用容量: 2G
優點:有容錯能力
缺點: 寫速度慢

RAID 5 (至少三顆 HD)
可用容量: 4G
優點: 有容錯能力, 寫入速度 OK



可以觀察 /proc/mdstat
來觀察 RAID 的情形

補充相關指令 mdadm

模擬 硬碟 fail 請同時觀察 /proc/mdstat
mdadm --manage /dev/md0 -f /dev/sda9
mdadm: set /dev/sda9 faulty in /dev/md0

mdadm --manage /dev/md0 -r /dev/sda9
mdadm: hot removed /dev/sda9

mdadm --manage /dev/md0 -a /dev/sda9
mdadm: re-added /dev/sda9

Disk quota

- Per file system basic: 針對 file system 來計算
- 對象: user 使用者(usrquota) /group 群組(grpquota)
- 標的: block (使用空間大小) / inode(建立檔案的數量)
- soft limit --> warning 警告
- hard limit --> deadline
- grace time --> 寬限期(default 7 days)

設定 diskquota

1. 在/etc/fstab 加上 usrquota 或 grpquota 參數
2. 使用 mount -o remount 重新掛載使其生效
3. 使用 quotacheck 初始化 quota (該 file system 會出現 aquota.user 或 aquota.group 檔案)
4. 使用 quotaon 啟用該 file system 的 quota
5. 使用 edquota 編輯 quota 設定
6. 使用 chkconfig boot.quota on 設定開機啟用 quota

若執行 #quotacheck 指令找不到該指令, 則使用#yast -i quota 安裝 quota 套件即可解決

現在的 kernel 支援 journaled quota, 故 lab 的時候採取 usrjquota 與 grpjquota

如果是 在/etc/fstab 使用 mount option 為 usrquota 或是 grpquota 會出現以下訊息

```
# quotacheck   -ugv  /data/
quotacheck: Your kernel probably supports journaled quota but you are not using it. Consider
switching to journaled quota to avoid running quotacheck after an unclean shutdown.
quotacheck: Scanning /dev/sda3 [/data] done
quotacheck: Cannot stat old user quota file: 沒有此一檔案或目錄
quotacheck: Cannot stat old group quota file: 沒有此一檔案或目錄
quotacheck: Cannot stat old user quota file: 沒有此一檔案或目錄
quotacheck: Cannot stat old group quota file: 沒有此一檔案或目錄
quotacheck: Checked 3 directories and 2 files
quotacheck: Old file not found.
quotacheck: Old file not found.
```

Setction 5

設定固定 IP

- IP: 網際網路上的邏輯位址
- Subnet Mask: 用來決定/計算所屬網路
- Default Gateway: 預設閘道
- DNS Server DNS 伺服器位址伺服器位址

可以使用

#ifconfig	觀察 IP 位址以及子網路遮罩
#cat /etc/resolv.conf	觀察 DNS 伺服器設定
#route	觀察路由設定

網卡設定檔案存放於 /etc/sysconfig/network/ifcfg-裝置代號

Default Gateway 設定錯誤: 會導致對外連線皆產生錯誤

DNS Server 設定錯誤: 會導致對外名稱連線產生錯誤但是對外的 IP 連線成功

** Section 6 **

Linux 的 modules 存放於 /lib/modules/核心版本 目錄下
可以使用下列指令管理 modules

lsmod	列出 modules
modprobe	載入 modules
rmmod	移除 modules
modinfo	顯示 modules 資訊

modules 的設定檔在 /etc/modprobe.conf

系統 使用 udev 來建立 / 維護硬體名稱
可以觀察 /etc/udev/rules.d 下面的設定來取得

** Section 7 **

ssh client	設定檔	/etc/ssh/ssh_config
sshd	設定檔	/etc/ssh/sshd_config

ssh 用戶端與主機的驗證
client 端存放於 ~/.ssh/known_hosts
與 server 端 /etc/ssh/ssh_host_rsa_key.pub

使用金鑰登入伺服器
*將用戶端的公鑰 複製到 伺服器上使用者的 ~/.ssh/authorized_keys
有關於第二把公鑰以後的附加

可以使用 ssh-copy-id 的指令來輕鬆完成
ssh-copy-id -i /home/user4/.ssh/id_dsa.pub(公鑰) 使用者@主機的 IP

可以修改/etc/ssh/sshd_config 設定來指定

Protocol 2	<只使用 SSH2>
PermitRootlogin no	<不允許 root 直接登入 ssh>

用戶端可以藉由

#ssh -X 遠端 IP	<使用 X forwarding>
#ssh -Y 遠端 IP	<使用 X forwarding>

啟用遠端管理 可以使用
#yast2 remote
啟用 VNC, 連線方式
#vncviewer 主機 IP:display
#vncviewer 主機 IP:port
或是使用有 java 的瀏覽器 http://主機 IP:5901

Section 8

#dmesg | grep 關鍵字　　觀察相關訊息
系統內大部分的log 皆存放於　　/var/log 目錄

Log Server
套件:　　syslog-ng
相關設定檔:

- /etc/syslog-ng/syslog-ng.conf
- /etc/syslog-ng/syslog-ng.conf.in
- /etc/sysconfig/syslog

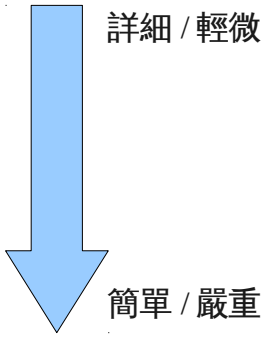
可以藉由修改 /etc/sysconfig/syslog 內的

- SYSLOG_DAEMON="syslog-ng" 來指定要使用 syslog-ng 還是傳統的 syslogd

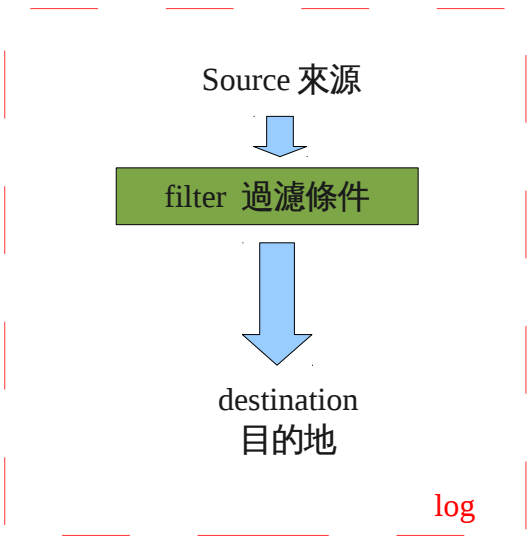
Facilities　　從哪一個服務或是設備傳來
Priorities　　log level, 優先性

Priorities

- debug
- info
- notice
- warning
- err
- crit
- alert
- emerg/panic



Syslog-ng



logrotate
/etc/logrotate.conf log 封存的設定檔(Global)

- weekly 每週封存
- rotate 4 保留 4 份
- create 封存完建立空檔
- include /etc/logrotate.d/ 相關要封存的 log 設定存放目錄

** Section 9 **

cron 定時排程

cron 符合條件就執行

crontab -e 語法

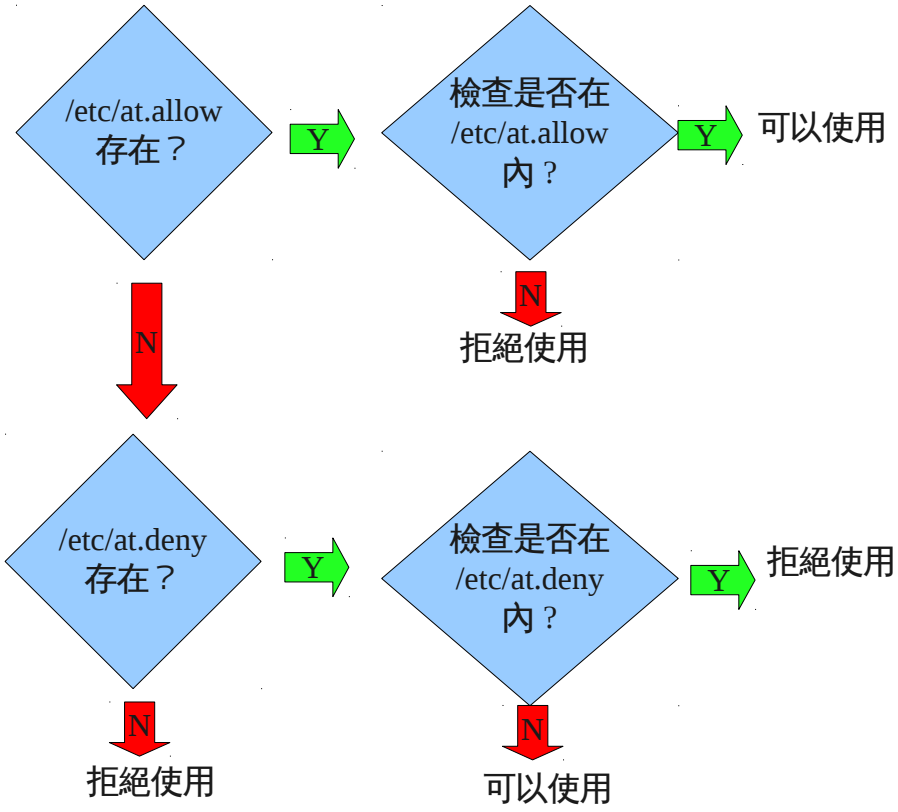
分	時	日	月	星期幾	指令	
*	*	*	*	*		<代表每分鐘執行>
0	*	*	*	*		<每小時執行, 分針為 0 時>
*/5	*	*	*	*		<每五分鐘執行一次>

/var/spool/cron/tabs/ 存放 cron 的排程工作（個人）
/etc/crontab 系統的排程工作

- 利用 /usr/lib/cron/run-crons 檢查相關工作是否被執行
- /etc/cron.hourly 每小時要做的排程工作(預設沒有工作)
- /etc/cron.daily/ 每日要做的排程工作
- /etc/cron.weekly 每周要做的排程工作(預設沒有工作)
- /etc/cron.monthly 每月要做的排程工作(預設沒有工作)

at 在指定的時間執行一次

針對突發的工作, 來進行工作的安排
/var/spool/atjobs　　存放 at 工作



** Section 10 **

* 備份範圍

Full backup
System backup

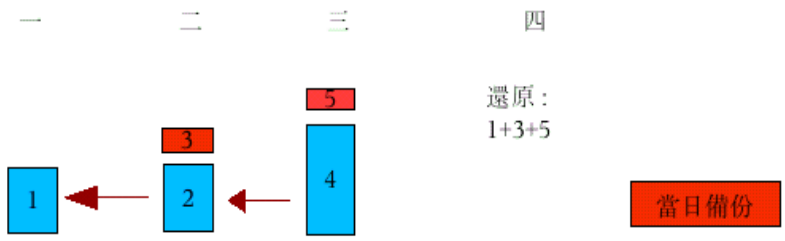
- /etc system config
- /var
- /root: personal script, work-notes
- /home: optional (if it is a file sharing server)
- /usr/local: optional (自己裝的套件, scripts)
- /boot: optional (如果有自己編譯過核心)
- /srv: optional (如果有提供服務

Data backup

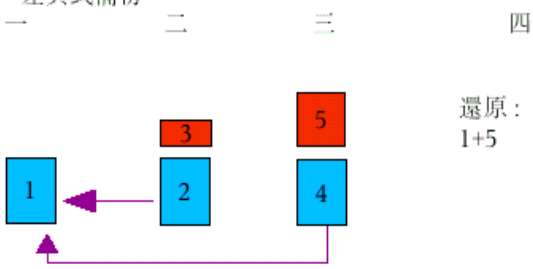
Case by case optional (看分享那些目錄,提供那些服務)

* 備份的方式

- 遞增式備份



- 差異式備份



tar – The GNU version of the tar archiving utility

- -c 建立
- -v 顯示資訊
- -f 檔案名稱
- -x 解開
- -z *.gz 格式
- -j *.bz2 格式
- -t 列出
- -C 指定目的地資料夾

rsync 異地備援

section 11

PAM (Pluggable Authentication Modules for Linux)
/etc/pam.d/ 目錄 存放程式相關的 PAM 設定
/lib/security/ 目錄 存放相關的 PAM moudules
/etc/security 目錄 存放 PAM 模組相關設定

PAM 語法
至少三個欄位 + 1 引數欄位, 分別是
Module-type Control-flag Module-path Agruments

Module-type
- auth 驗證帳號 (ex: 帳號密碼是否正確?)
- account 授權 (ex: 檢查帳戶是否過期, 是否可在此電腦登入)
- password 用來修改密碼
- session 執行環境相關

Control-flag
- required
  - 一定要通過的模組, 不管成功或是失敗都會繼續往下一個模組檢查.
  - 如果有一個 required 模組失敗, 其結果回應失敗.
- requisite
  - 如果成功, 不會繼續檢查下一個模組 (馬上回應成功).
  - 如果失敗, 不會繼續檢查下一個模組 (馬上回應失敗).
- optional
  - 不管成功或是失敗都會繼續往下一個模組檢查
  - 不管成功或是失敗都不會影響結果, 列為參考, 一般用於 Log 與 notify.
- sufficient
  - 如果成功, 不會繼續檢查下一個模組 (馬上回應成功).
  - 如果失敗, 繼續檢查下一個模組不會影響結果.

Module-Path
- 使用的 PAM 模組
- /lib/security/ 目錄 存放 32 位元相關的 PAM moudules
- /lib64/security/目錄 存放 64 位元相關的 PAM moudules

Agruments
- 非必要欄位
- 可以使用 module 的選項, 例如 debug 或 nullok

pam_securetty.so: 根據 /etc/securetty 限制 root 可以登入的裝置
pam_nologin.so: 如果 /etc/nologin 檔案存在, 則一般使用者不可以登入系統

sudo

管理者可以利用 sudo 授權使用者去執行特定的指令
sudo, sudoedit - execute a command as another user

visudo 會編輯 /etc/sudoers 檔案來授權使用者可以變更其他使用者執行指令
語法如下

使用者 電腦=(使用者) 指令

利用 chage 設定使用者的密碼相關設定

- Minimum Password Age: 更改密碼後最少要過幾天才能再換密碼
- Maximum Password Age: 密碼幾天之後一定要換
- Password Expiration Warning: 密碼過期前幾天警告
- Password Inactive: 密碼過期後幾天鎖定
- Last Password Change: 上次修改密碼的日期
- Account Expiration Date: 帳戶過期日

/etc/shadow 檔案
john:$2a$10$2jooBgXdcyVRORcTrOk6O.vgsBnufE.oEH366oSNUDf80oAjfz90y:14196:7:90:5:3:14244:
帳號:加密過後的雜湊值:上次修改密碼的日期:Min age:Max age:幾天前警告:幾天後鎖定:帳戶過期日

要求使用者下次登入必須更改密碼

- 可以使用 #chage -d 0 使用者帳號
- 或是使用 #passwd -e 使用者帳號

ACL (Access Control List)
傳統的檔案權限針對的對象

- 擁有者(owner)
- 群組(group)
- 其他(other)

倘若檔案或是資料夾的權限, 指定的方式超過三個以上
此時可以利用 ACL 指定特定使用者/群組 所可以擁有的權限,來彌補傳統權限的不足

ACL(Access Control List)

- 在 file system 上面必須設定 acl 的選項
- 可以使用 setfacl 設定 ACL
  - -m 編輯 ACL 設定
  - -x 移除單項 ACL 設定
  - -b 移除所有 ACL 設定
  - -d 設定 Default ACL
  - -M 還原 ACL 設定
- 可以使用 getfacl 觀察 ACL 設定

-rwxrw-r--+ 1 root users 0 2008-06-21 11:27 test
當設定 ACL, 中間的 4-6 的 bit 就非原本的群組權限, 而是 acl mask

- acl mask --> 特定使用者或是特定群組可以使用的最大權限
- default acl --> 針對資料夾設定 default acl 其子資料夾及檔案可以繼承設定的 acl