

國立中央大學電子計算機中心 FreeBSD 短期訓練課程

資訊管理學系三年級 游子德
2006/10/19

教學大綱

- 使用者及群組管理
- 磁碟配額管理
- 系統安全管理
- 資料備份

帳號及群組

- Name: 使用者登入名稱
 - UID: 系統識別用戶的數字
 - GID: 系統識別用戶群組的數字
 - CLASS: 對 Group 控制的擴張
 - 能夠以 UID,GID,CLASS 限制用戶的行為
-
- 系統在運作時，使用的並非是登入名稱或是群組名稱，而是一組數字。登入名稱及群組名稱只是幫助人類易於理解

使用者管理 -master.passwd

- /etc/master.passwd 共十個欄位
 1. 使用者名稱 (為英文,“-”,與”_”組成)
 2. 密碼 (編碼過後)
 3. UID (0~4294967295), 建議使用到 65535
 4. GID (0~4294967295), 建議使用到 65535
 5. 登入 class
 6. 修改密碼期限 (為 1970/1/1 到期限的秒數)
 7. 帳戶到期時間 (為 1970/1/1 到期限的秒數)
 8. 使用者全名
 9. 使用者家目錄
 10. 使用者預設 Shell

Test: 編碼密碼 :1002:1002:insecure:0:0:Test:/home/Test:/bin/tcsh

使用者管理 - 新增使用者

使用 `adduser` 新增用戶，它會提示相關資訊要求輸入，依序為：

1. Username

2. 全名

3. Uid

4. 登入群組（可多個）

5. 登入類別

6. 預設 Shell

7. 家目錄

8. 密碼

9. 是否鎖住

使用者管理 - 新增使用者

```
root@smile [~] adduser
Username: newuser
Full name: New User
Uid (Leave empty for default):
Login group [newuser]:
Login group is newuser. Invite newuser into other groups? []:
Login class [default]:
Shell (sh csh tcsh bash nologin) [sh]: tcsh
Home directory [/home/newuser]:
Use password-based authentication? [yes]:
Use an empty password? (yes/no) [no]:
Use a random password? (yes/no) [no]:
Enter password:
Enter password again:
Lock out the account after creation? [no]:
Username      : newuser
Password      : *****
Full Name     : New User
Uid           : 1003
Class         :
Groups        : newuser
Home          : /home/newuser
Shell         : /bin/tcsh
Locked        : no
OK? (yes/no): yes
adduser: INFO: Successfully added (newuser) to the user database.
Add another user? (yes/no): no
Goodbye!
```

使用者管理 - 刪除使用者

使用 `rmuser` 刪除使用者，其會

1. 刪除使用者的 `crontab` 記錄（如果有的話）。
2. 刪除屬於使用者的 `at` 工作。
3. 殺掉屬於使用者的所有進程。
4. 刪除本機密碼文件中的用戶。
5. 刪除使用者的主目錄（如果他有自己的主目錄）。
6. 刪除來自 `/var/mail` 屬於使用者的郵件。
7. 刪除所有諸如 `/tmp` 的臨時文件存儲區中的文件。
8. 最後，若使用者所在的同名群組是空的，則刪除該群組。

```
root@smile [~] rmuser newuser
Matching password entry:

newuser:*:1003:1003::0:0:New User:/home/newuser:/bin/tcsh

Is this the entry you wish to remove? yes
Remove user's home directory (/home/newuser)? yes
Removing user (newuser): mailspool home passwd.
```

使用者管理 - 修改使用者資訊

- `passwd`
修改使用者密碼
語法 `passwd user`
注意密碼不要使用帳號或其他相關資訊以及單字，最好英數混用
- `chpass`
修改使用者資訊（使用 EDITOR 或 VISUAL 環境變數的編輯器）
- `vipw`
直接使用編輯器編輯 `/etc/master.passwd`

使用者管理 - 修改使用者資訊

```
Changing local password for Test
New Password:
Retype New Password:
root@smile.W1 [/var/log]
```

```
#Changing user information for Test.
Login: Test
Password: *LOCKED*$1$4jCvXu4c$i4R0sjGWJOg7HTxqLOKuk0
Uid [#]: 1002
Gid [# or name]: 1002
Change [month day year]:
Expire [month day year]:
Class: insecure
Home directory: /home/Test
Shell: /bin/tcsh
Full Name: Test
Office Location:
Office Phone:
Home Phone:
Other information:
```

使用者管理 - 限制使用者的資源

- 透過使用者的 class , 並配合 /etc/login.conf 設定 , 常見限制選項如下 :

CPUTIME: 限制程序最大 CPU 使用時間

FILESIZE: 限制使用者檔案的最大大小

MAXPROC: 限制使用者最大的程序數目

OPENFILES: 限制單一程序最大的 fd 數目

MEMORYUSE: 限制單一程序最大記憶體用量

PRIORITY: 限制單一程序最大的優先序

- 修改完後要執行 `cap_mkdb /etc/login.conf` 以重建資料庫

群組管理 -group

- /etc/group 共四個欄位
 - 1.Group name 群組名字
 - 2.password 群組密碼
 - 3.gid 群組號碼
 - 4.member 群組成員

```
wheel:*:0:root
daemon:*:1:
kmem:*:2:
sys:*:3:
tty:*:4:
operator:*:5:root
mail:*:6:
bin:*:7:
```

群組管理 -pw

- 新增群組
pw groupadd groupname
- 刪除群組
pw groupdel groupname
- 新增群組成員
pw groupadd groupname -M member
- 刪除群組成員
pw groupdel groupname -M member
- pw 也可用來管理使用者帳號

quota 磁碟配額管理

每個檔案系統可實施五種配額限制。

1. 使用者的硬性限制 (per-user hard limit)
使用者在檔案系統上所能使用的最大資源
2. 使用者的軟性限制 (per-user soft limit)
使用上限的警告區
3. 群組的硬性限制 (per-group hard limit)
群組能在檔案系統上所能使用的最大資源
4. 群組的軟性限制 (per-group soft limit)
群組使用上限的警告區
5. 寬限期 (grace period)
一但使用量超過軟性限制，必須在寬限期內將使用空間降到軟性限制以下

quota 建置步驟

1. 在核心設定檔中加入 `options QUOTA` 並重編核心
2. 將 `userquota,groupquota` 兩個掛載參數加到 `/etc/fstab` 中要進行磁碟配額的檔案系統
3. 在 `/etc/rc.conf` 中加入 `enable_quotas="YES"`
4. 啟動 `quota` , `/etc/rc.d/quota start`

```
root@smile.W1 [~] cat /etc/fstab
# Device          Mountpoint      FStype  Options              Dump    Pass#
/dev/ad0s1b      none           swap    sw                   0       0
/dev/ad0s1a      /              ufs     rw,acls,multilabel,userquota,groupquota    1       1
proc             /proc          procfs  rw                   0       0
linproc         /compat/linux/proc  linprocfs  rw 0 0
/dev/acd0        /cdrom         cd9660  ro,noauto            0       0
```

配額命令

- quota
顯示群組與使用者的配額限制
語法
quota [-u] [options] user
quota -g [options] group
參數
-q 只顯示超過配額的情況
-v 詳細輸出細節

```
%quota
Disk quotas for user Test (uid 1002):
  Filesystem  usage  quota  limit  grace  files  quota  limit  grace
  /           1086   2048   4096           21     0     0
```

配額命令

quotacheck

檢查檔案系統及匯編配額資料庫

語法

```
quotacheck [options] filesystem
```

```
quotacheck [options] -a
```

參數

-a 檢查 /etc/fatab 中有設置 quota 檔案系統的

配額

-g 匯編群組資訊

-u 匯編使用者資訊

-v 詳細輸出

配額命令

quotaon

在一個或多個檔案系統開啓 quota

語法 quotaon [options] file system

quotaon [options] -a

參數

-a 開啓 /etc/fstab 有 quota 相關參數的檔案系統

-g 開啓群組配額

-u 開啓使用者配額 (預設)

-v 詳細輸出

配額命令

quotaoff

停用檔案系統的配額

語法

```
quotaoff [options] filesystem
```

```
quotaoff [options] -a
```

參數

-a 關閉 /etc/fstab 所有檔案系統的配額

-g 關閉群組配額

-u 關閉使用者配額

-v 詳細輸出

配額命令

edquota

使用文字編輯器修改使用者或群組配額
語法

```
edquota [-p proto-user] [options] names
```

```
edquota [options] -t
```

參數

-g 變更群組配額

-p proto-user 以 proto-user 為原型複製給其他使用者

-t 變更寬限期

-u 變更使用者配額

配額命令

repquota

回報配額狀態

語法

- a 回報 /etc/fstab 所有檔案系統的配額狀態
- g 回報群組配額狀態
- u 回報使用者配額狀態
- v 詳細輸出

```
root@smile [~] repquota -a
```

User	used	Block soft	limits hard	grace	used	File soft	limits hard
wheel	-- 7518454	0	0	-	332154	0	0
-							
daemon	-- 174	0	0	-	16	0	0
-							
kmem	-- 178	0	0	-	5	0	0
-							
tty	-- 22	0	0	-	2	0	0
-							

inetd 概念

- inetd 為其底下的服務提供統一的對外介面。透過 inetd，可以使系統服務在 inetd 的保護下而不必直接與外部溝通。並提供管理服務的功能。
- 通常與 TCP-wrapper 一起使用
- 優點為提高安全性
- 缺點為連線效能會稍差

```
root@smile [~] sockstat -4
```

USER	COMMAND	PID	FD	PROTO	LOCAL ADDRESS	FOREIGN ADDRESS
root	inetd	67573	5	tcp4	*:21	::*
root	inetd	67573	6	tcp4	*:23	::*

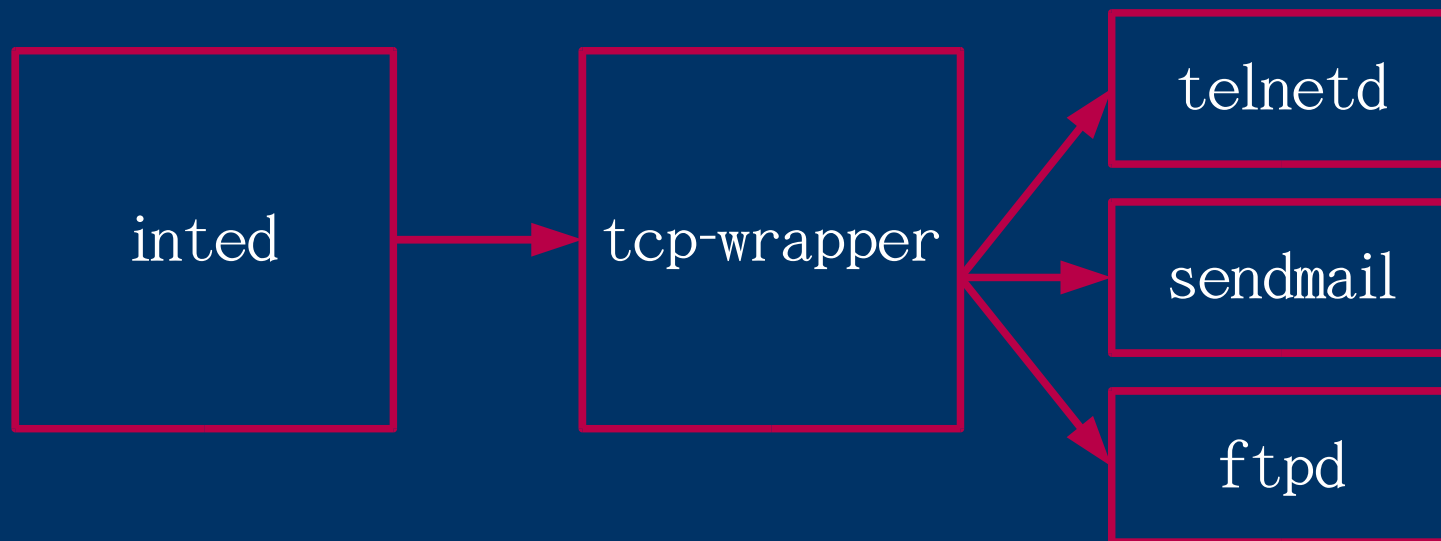
inetd 的啓用

- 在 /etc/rc.conf 中加入 inetd_enable="YES"
- 修改 /etc/inetd.conf，在想開啓的服務前將 # 拿掉
- 輸入 /etc/rc.d/inetd start 啓動 inetd

```
root@smile.W1 [~] head -n 20 /etc/inetd.conf
# $FreeBSD: src/etc/inetd.conf,v 1.70.2.1 2006/03/28 15:51:44 ceri Exp $
#
# Internet server configuration database
#
# Define *both* IPv4 and IPv6 entries for dual-stack support.
# To disable a service, comment it out by prefixing the line with '#'.
# To enable a service, remove the '#' at the beginning of the line.
#
#ftp      stream  tcp      nowait  root    /usr/libexec/ftpd      ftpd -l
#ftp      stream  tcp6     nowait  root    /usr/libexec/ftpd      ftpd -l
#ssh      stream  tcp      nowait  root    /usr/sbin/sshd         sshd -i -4
#ssh      stream  tcp6     nowait  root    /usr/sbin/sshd         sshd -i -6
#telnet   stream  tcp      nowait  root    /usr/libexec/telnetd   telnetd
#telnet   stream  tcp6     nowait  root    /usr/libexec/telnetd   telnetd
```

TCP Wrapper

- FreeBSD 上的許多程式直接支援 TCP Wrapper
- 提供統一的服務連線記錄，並且能回應客戶端訊息，並只讓允許的用戶進行連線



TCP Wrapper- 設定

- 服務的基本配置在 /etc/hosts.allow
- 基本形式
服務名稱：客戶端清單：動作
- 服務名稱：程式在命令列上的名稱
如 ftpd, apache 的 httpd, 或是可用 ALL 表示所有服務. 若有多張網卡, 可使用 @ 指定. 如
ftpd@140.115.17.80:ALL:allow
ftpd@140.115.17.81:ALL:deny
ftpd:ALL:deny
- 位址：任何有效的主機名稱, 如 ip, 網段, 主機名稱, 網域名稱, 之間以空白隔開, 例：
ALL:140.115.0.0/16 192.168.0.9:deny
- 動作: allow 或 deny

TCP-Wrapper 設定 - 訊息回應及記錄

- severity: 送出訊息到系統記錄中, 如
ALL:ALL: severity auth.info: allow
這會將記錄所有的連線, auth.info 分別為
syslogd 的 facility 與記錄等級
- twist: 可在連線時執行一個程式檔, 並將結果傳
回連線端, 如
sshd:140.115.0.0/16: twist /bin/echo "You can
not use this service"

防火牆 -IPFilter

- 可使用多組規則過濾檢查進出主機的封包，並決定是否可以通過。
- 可保護應用程式及機器不受你所不希望的封包干擾
- IPFilter 為獨立於 FreeBSD 開發，現已與 FreeBSD 整合

防火牆 -IPFilter(ipf) 的啓用

- 於 /etc/rc.conf 加入
ipfilter_enable="YES" # 啓動 ipf
ipfilter_rules="/etc/ipf.rules" # 載入規則位址

之後以 /etc/rc.d/ipfilter start 啓動防火牆

- 若要啓動 ip 記錄, 於 /etc/rc.conf 中加入
ipmon_enable="YES"
ipmon_flags="-Ds" # D: 以 Daemon 啓動
#s: 使用 syslog

之後以 /etc/rc.d/ipmon start 啓動記錄器

防火牆 -ipfilter 過濾規則

- 先來個實際例子
block in log quick on fxp0 from any to any
- block , 為一個 action, 表示阻擋此封包
- in 表示為由網路進入系統的封包
- log 與 quick 是 Option, log 表示記錄此封包, quick 為立刻實行此動作且不再進行比對.
- on fxp0 指定了網路介面
- any to any 表示了來源與去向為任意的地點
也可使用 all 表示

防火牆 -IPFiler(ipf) 的語法

- 基本上比對規則為最後一個符合的成立
- 一般形式如下

action direction options protocol source
destination packet-option

- Action: 為 block 或 pass, 表示阻擋或通過
- Direction: 為 in 或 out, 表示進入系統或流出系統
- Options: 可為 log, quick 與 on 網路介面. Log 表示記錄此封包, quick 表示立即使用這條規則, on 指定網路裝置
- protocol: 任何 IP 層的協定, 可由 /etc/protorol 指定, 以 proto 關鍵字使用
- Source and destination: 使用 from 與 to 關鍵字表明封包的來源與去向
- Packet-option: 描述封包的特定型態

IPFilter 規則範例

- 允許外部的人連進 sshd 與 pop3
- 封鎖校外的連線
- 除此之外，一切拒絕
- pass in quick proto tcp from any to any port = pop3 keep state
- pass in quick proto tcp from any to any port = ssh keep state
- pass in from 140.115.0.0/16 to any keep state
- block in all
- Keep state 會使防火牆檢視這整個連線並動態新增規則使整個連線可以完整進行

防火牆 -IPFiler(ipf) 的相關指令

- ipf 控制過濾規則的指令，可用來管理規則
如 ipf -Fa -f filename 可清除 (Fa) 所有規則並以 filename 檔作為規則
- ipfstat 可顯示目前過濾狀況以及過濾規則
如 ipfstat -i 顯示流入過濾規則
ipfstat -o 顯示流出規則
ipfstat -a 顯示所有規則

防火牆 -IPFiler(ipf) 的記錄

- 若有在防火牆規則中加入 log ,則需要啓動 ipmon . 它的記錄檔可直接寫入檔案或是透過 syslog 記錄 . 若透過 syslog 記錄 ,則 log 檔可透過 syslog 管理 .
- 一般 syslog 有所謂的 facility 來負責記錄日誌 . 而 ipmon 是透過 local0 這支 facility 記錄 .

系統安全 - 使用者權限

- 檔案系統的基本權限已於先前介紹過。
現在介紹 FreeBSD 擴充的檔案系統權限
 - 1.sappend: 只能增加內容，不能更改或刪除
 - 2.schg: 不能更改內容，移動或取代
 - 3.sulnk: 不能刪除此檔以上三種只有 root 能設置，並且在安全層級 1 以上不能被修改。另外 uappend, uchg, uulnk 使用者能自行設置
- 使用 "chflags -R 旗標 檔案" 設置檔案旗標
可使用 ls -lo 觀看擴充的旗標
要移除可使用 chflags noflag 檔案來移除

系統安全 - 安全層級

- 安全層級 -1: 什麼都不作
- 安全層級 0: 進入 multi-user 時會自動進入安全層級 1
- 安全層級 1:
 1. 不能夠使用 kldload 及 kldunload
 2. 不能夠用 /dev/mem 及 /dev/kmem 直接寫入系統記憶體
 3. 已掛載的檔案系統不能直接寫入
 4. 檔案系統的 schg, sappend, sunlnk 標籤無法移除

系統安全 - 安全層級

- 安全層級 2:
 1. 不能直接寫入所有的檔案系統
 2. 更動系統時間的差異不能超過一秒
- 安全層級 3:

不能改變防火牆的規則
- 如何看目前的安全等級？

利用 `sysctl kern.securelevel` 觀看
- 如何設置？
 1. 在 `/etc/rc.conf` 中加入
`kern_securelevel_enable="YES"` 與
`kern_securelevel="number"` number: -1~3
 2. 也可使用 `sysctl kern.securelevel=number`
但是無法降低安全等級，只能提高
- 如何降低安全層級？重新開機進入 `single user mode` 修改

系統安全 - 關閉不必要的服務

- 最常出現問題的程式：在網路上與別人溝通的程式
- 首先知道有什麼程式在溝通，可以利用 `sockstat` 這支程式觀看

```
root@smile.W1 [/root/test] sockstat -4
USER      COMMAND  PID    FD PROTO  LOCAL ADDRESS    FOREIGN ADDRESS
mysql     mysqld   5261   10 tcp4    *:3306           *:*
```

USER	COMMAND	PID	FD	PROTO	LOCAL ADDRESS	FOREIGN ADDRESS
mysql	mysqld	5261	10	tcp4	*:3306	*:*
tedyu	sshd	5137	3	tcp4	140.115.17.137:22	203.67.37.97:3844
root	sshd	5134	3	tcp4	140.115.17.137:22	203.67.37.97:3844
root	sendmail	538	4	tcp4	127.0.0.1:25	*:*
root	sshd	532	4	tcp4	*:22	*:*
root	syslogd	385	7	udp4	*:514	*:*

- 若 Foreign Address 為 `**`，表示正在監聽網路上的封包（表示開啓的服務）
若看到不需要的服務，可用
`/etc/rc.d/service stop` 或
`/usr/local/etc/rc.d/service stop`

系統安全 - 保持更新

- 使用 `security/portaudit` 檢查所安裝的套件
安裝完後，輸入 `portaudit -Fda`，它會抓取資料庫並且檢查你的套件

```
root@smile.W0 [/usr/ports] portaudit -Fda
New database installed.
Database created: Mon Oct 16 18:10:25 CST 2006
Affected package: php5-5.1.6_1
Type of problem: php -- open_basedir Race Condition Vulnerability.
Reference: <http://www.FreeBSD.org/ports/portaudit/edabe438-542f-11db-a5ae-00508d6a62df.html>

Affected package: mozilla-1.7.13,2
Type of problem: mozilla -- multiple vulnerabilities.
Reference: <http://www.FreeBSD.org/ports/portaudit/e6296105-449b-11db-ba89-000c6ec775d9.html>
```

系統安全 -ACL

- 擴展了檔案系統的安全機制
- 允許制定更精細的控制
- 使用 `getfacl file` 獲取檔案的 `acl list`
- 使用 `setfacl -m entries file` 設置檔案的 `acl list`, 使用 `setfacl -b file` 可刪除 `ACL list`
- 需要對想要使用 `acl` 的檔案系統使用 `tunefs -a enable`, 並在 `/etc/fstab` 中加入 `acls` 才可以得到 `ACL` 的完整功能

```
#file:test  
#owner:1001  
#group:0  
user::rwx  
user:Test:---  
group::rwx  
mask::rwx  
other::rwx
```

系統安全 -MAC(mandatory access control)

- 傳統 Unix 系統使用 DAC 機制
DAC 依據使用者驗證與擁有者來授予存取權限，其他的安全相關資訊將被忽略。
- MAC 依據安全政策中定訂的主旨與目標來授予存取權限。使用 MAC 可以讓系統的所有元件按照統一的政策進行運作。
- 在 Linux 上的實做稱為 SELinux

系統安全 - 觀看 mail list 或論壇

可以上 Ptt 的 FB_security 看版,這邊會討論
關於安全的相關議題

順便列一下其它 FreeBSD 相關的看版

FB_announce

FB_bugs

FB_current

FB_cvs

FB_doc

FB_hackers

FB_ports

FB_stable

備份所考慮的事物

- 備份的檔案
依照重要程度決定要備份的檔案，如重要的資料。或是當系統出問題，能快速還原
- 備份的方法
利用不同的媒體去儲存備份檔，如光碟，第二顆硬碟，其他的目錄，甚至是另外一台電腦
- 備份的頻率
根據資料的變動性來決定備份的頻率

備份種類

- 完全備份：將所有的檔案全部備份下來。優點是備份方便，還原快速。缺點是每次備份所花費的時間較多，檔案也較大。
- 漸進式備份：只備份上次備份過後有變動的檔案。優點是節省備份時間及空間，缺點是還原時較麻煩。

選擇需要的備份檔案

- 會考慮
 1. 系統的設定檔，如使用者資料設定，網路設定，系統設定
 2. 使用者的資料，檔案，信件
 3. 系統運作的資料，如 mysql 資料庫, bbs 檔案等
- 通常會備份以下目錄
 - /etc 設定檔
 - /var/mail 信件
 - /home 使用者目錄
 - /boot 開機資料及核心資料
 - /root 系統管理者的家目錄
- 若是希望系統出問題時快速恢復，可考慮使用完整備份

crontab

- 可以讓指定的程式在所需要的時間執行
基本的系統檔案設定在 `/etc/crontab`，其儲存了系統的排程工作
- 基本格式
分鐘 小時 幾號 幾月 星期幾 執行者 命令
- 如果想要每天早上六點執行備份，打入
`0 6 * * * root /root/backup.sh`
星號表示符合所有時間
- 若沒有 `root` 權限，可使用 `crontab -e` 編輯自己的 `crontab`

crontab

- 基本格式
分鐘 小時 幾號 幾月 星期幾 執行者 命令
- 分鐘為 0~59
- 小時為 0~23
- 號為 1~31
- 月為 1~12
- 星期幾為 0~7
- 範例
0 0 * * 0 root /root/backup.sh
0 6-12 * * * root /root/backup.sh
0 6,8,12 * * * root /root/backup.sh
0 */2 * * * root /root/backup.sh
0 6-12/2 * * * root/root/back.sh

基本的備份建立

首先先手動進行備份程序

```
tar czf etc-`date +%Y-%m-%d`.tgz /etc
```

```
tar czf home-`date +%Y-%m-%d`.tgz /home
```

```
tar czf mail-`date +%Y-%m-%d`.tgz /var/mail
```

```
tar caf sql-`date +%Y-%m-%d`.tgz /var/db/mysql
```

以上的 tar 可以進行檔案的包裝及壓縮，date 的輸出日期可以作為檔名。

讓工作自動進行

- 可以將整個備份的程序寫成一個 shell script 檔
- 接著利用 crontab 讓工作照自己想要的時間自動執行
- 比如
0 6 * * * root /root/backup-db.sh
0 6 * * 0 root /root/backup.sh

備份工作 -dump

- dump 備份工具的運作對一個分割區的檔案系統，
- 備份整個根目錄檔案系統
dump -0 -a -L -f /root/dump / 此會備分根目錄的分割區，若 /home 為獨立分割區，可以以
dump -0 -a -L -f /mnt/disk2 /
- -0 是 dump 等級 0 的意思，等級可以由 0~9,0 表示備份所有東西，在等級 X 的 dump 會備份小於等級 X 的備份後有新增或變動過的檔案目錄
- -a 表示不要去計算磁帶大小
- -L 為備份掛載為讀寫的檔案系統
- 若加上 -u 參數，此記錄會在 /etc/dumpdates

備份工作 -restore

- 如果要看 dump 檔之中擺放了什麼檔案，可以使用 `restore -f dump -t` 觀看
如 `restore -f /root/dump -t`
- 如果要將資料從 dump 檔還原出來，可以打 `restore -f dumpfile -x file`
例如
`restore -f /root/dump -x /etc/master.passwd`
- 也可以使用 `-i` 參數進入互動模式

參考資料

- FreeBSD 完全探索 Michael Lucas 著，藝立協譯 上奇出版社
- FreeBSD 使用手冊
http://www.freebsd.org/doc/zh_CN.GB2312/books/handbook/
- 鳥哥的 Linux 私房菜
<http://linux.vbird.org/>