

RHCE 7

Department of Computer Science and Information Engineering
Chaoyang University of Technology
Taichung, Taiwan, Republic of China

Instructor: De-Yu Wang (王德譽)
E-mail: dywang@mail.cyut.edu.tw
Phone: (04)23323000 ext 4538
Office: E738

```
root@kvm5:~ MariaDB [(none)]> exit
Bye
[root@kvm5 ~]# targetcli
targetcli shell version 2.1.1.fb37
Copyright 2011-2013 by Datera, Inc and others.
For help on commands, type 'help'.

/> ls
o- L ..... [Targets: 0]
o- backstores ..... [Storage Objects: 0]
| o- block ..... [Storage Objects: 1]
| | o- kvm5.disk1 .. [/dev/iscsi_vg/iscsi_data (12.0MiB) write-thru activated]
| o- fileio ..... [Storage Objects: 0]
| o- pscsi ..... [Storage Objects: 0]
| o- ramdisk ..... [Storage Objects: 0]
o- iscsi ..... [Targets: 1]
| o- iqn.2015-08.wang.deyu:kvm5
| | o- tpg1 ..... [no-gen-acls, no-auth]
| | | o- acls ..... [ACLs: 1]
| | | o- iqn.2015-08.wang.deyu:kvm7 ..... [Mapped LUNs: 1]
| | | | o- mapped_lun0 ..... [lun0 block/kvm5.disk1 (rw)]
| | | o- luns ..... [LUNs: 1]
| | | | o- lun0 ..... [block/kvm5.disk1 (/dev/iscsi_vg/iscsi_data)]
| | | o- portals ..... [Portals: 1]
| | | | o- 192.168.122.5:3260 ..... [OK]
o- loopback ..... [Targets: 0]
```

September 7, 2018

-
- Instructor: De-Yu Wang
 - 1. Email: dywang@csie.cyut.edu.tw
 - 2. Homepage: <http://dywang.csie.cyut.edu.tw>
 - 3. Phone: (04)23323000 ext 4538
 - 4. Office: E738
 - 參考資料
 - 1. RedHat Documentation
 - 2. RedHat Customer Portal
 - 3. Configure a Kerberos KDC
 - 4. Configure a system to authenticate using Kerberos

Contents

1 實機練習系統	1
1.1 動機	1
1.2 系統設計	1
1.3 NAT 設計	2
1.4 虛擬機管理界面	2
1.5 系統管理與評分	4
1.6 證照考試	5
1.7 上課前先確定三件事	5
1.8 虛擬機設定	5
1.9 系統伺服器管理	6
2 SELinux	9
2.1 設計原由	9
2.2 啓動、關閉與觀察	9
2.3 SELinux Contexts	10
3 Netfilter	13
3.1 前言	13
3.2 firewall-cmd 命令	15
3.3 啓用 firewall	15
3.4 block zone	17
3.5 firewall direct rules	19
3.6 firewall rich rules	21
3.7 Masquerading and Port Forwarding	23
3.8 *NAT 設定與測試	25
4 可執行檔	31
4.1 檔案權限	31
4.2 改變檔案權限	32
4.3 可執行檔	32
4.4 可執行檔別名	34
5 Link Aggregation 網路聚合	37
5.1 前言	37
5.2 建立網路聚合	37
5.3 測試網路聚合	40

6 IPv6 網路	43
6.1 前言	43
6.2 IPv6 位址	43
6.3 IPv6 子網	44
6.4 IPv6 設定	44
6.5 IPv6 互 ping	46
7 Email Transmission	49
7.1 簡介	49
7.2 *Postfix 架設	49
7.3 *Dovecot 架設	51
7.4 Null Client 建置	52
8 SMB File Shares	57
8.1 SMB 簡介	57
8.2 SAMBA 架設	57
8.3 建立多使用者 SMB 掛載目錄	63
8.4 防火牆設定	66
8.5 * 測試 SMB 分享目錄	67
8.6 測試多使用者 SMB 掛載	68
8.7 開機自動掛載多使用者 SMB 目錄	71
8.8 * 安全開機自動掛載多使用者 SMB 目錄	71
9 Network File System, NFS	75
9.1 NFS 簡介	75
9.2 *Kerberos KDC	75
9.3 NFS Server 架設	83
9.4 NFS 伺服器防火牆設定	87
9.5 *NFS Client 端 KDC 設定	89
9.6 NFS Client 端掛載設定	91
9.7 NFS Client 端權限測試	93
9.8 **NFSv4+kerberos 除錯	95
10 Apache 2.4 HTTP Server	111
10.1 Apache HTTP 簡介	111
10.2 http 網頁架設	112
10.3 * 建立 TLS 憑證	114
10.4 HTTPS 安全網站架設	116
10.5 Virtual Host 虛擬主機	118
10.6 架設動態網頁	120
10.7 網站存取限制	121
11 Shell Script	123
11.1 前言	123
11.2 善用判斷式	124
11.3 條件判斷式	125
11.4 迴圈 (loop)	127
11.5 範例	128

12 iSCSI Storage	133
12.1 iSCSI 簡介	133
12.2 Server Target 架設	133
12.3 Client Initiator 設定	139
12.4 Client Initiator 除錯	143
13 MariaDB 資料庫	147
13.1 MariaDB 簡介	147
13.2 MariaDB 架設	147
13.3 建立資料庫	150
13.4 * 建立並備份資料表	151
13.5 建立用戶	154
13.6 查詢資料表資料	157
13.7 查詢練習	161

Chapter 1

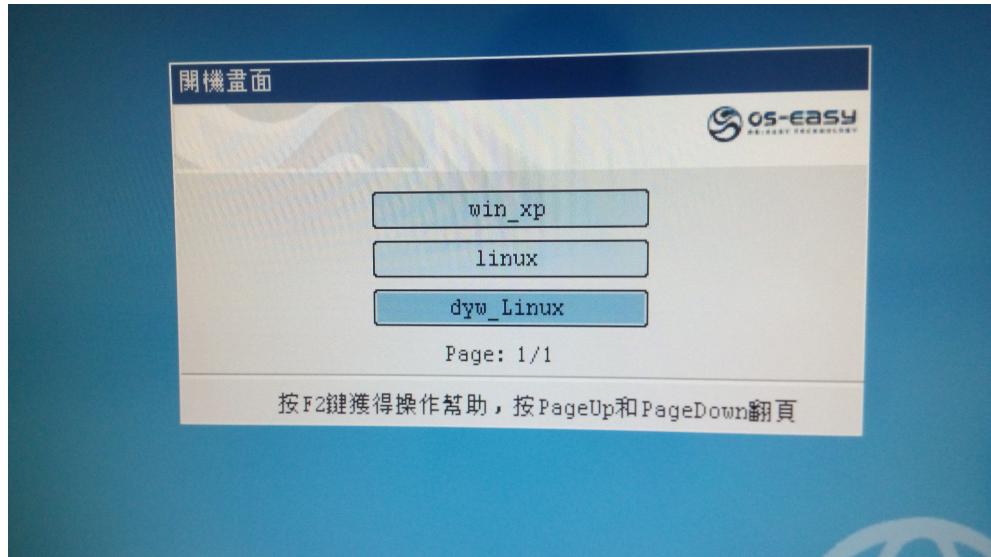
實機練習系統

1.1 動機

1. 教學若有實際環境，讓學生實機操作練習，可以大大提昇學習成效。
2. Linux 實機練習，很容易因學生操作錯誤，而造成系統損壞。例如：硬碟分割、格式化及管理的練習。
3. 實機練習結束或操作不當造成當機，系統必須可以迅速還原，才能重複練習。
4. 系統必須可以批次快速修改或更新。
5. 系統必須可以依據學生實際操作狀況，批次進行檢查或評分。
6. 虛擬機練習所需伺服器資源，例如：LDAP 網路帳號、YUM repository 資料庫伺服器、NFS 分享、NTP 校時伺服器、ISCSI 硬碟分享、內部網域 DNS 伺服器、FTP 資源下載…等環境必須架設好，才能提供虛擬機做各種狀況的練習。

1.2 系統設計

1. Linux 教學系統設計
 - (a) 客製化 Linux 系統。
 - (b) Linux 伺服器架設。
 - (c) 虛擬機設計。
2. Linux 教學系統安裝
 - (a) E517 電腦教室：方便學生上課使用。



- (b) 個人隨身碟：插上隨身碟，以安裝光碟開機，不需要任何設定，自動安裝於隨身碟，不會影響電腦中的硬碟。
- (c) LiveCD：以 LiveCD 光碟開機，開機後即可使用，只是所有操作與設定都是暫存，重新開機後即回到原始狀態。

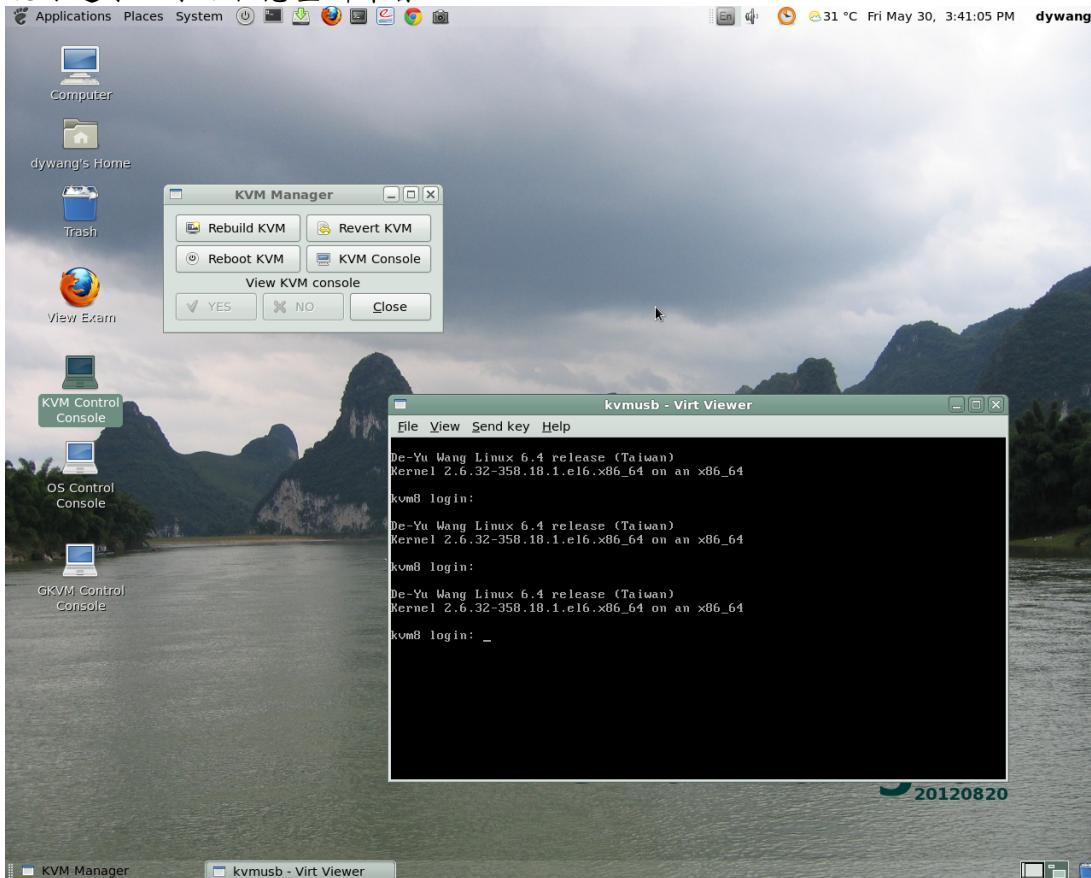
1.3 NAT 設計

1. NAT 架設 ??：電腦教室網路設置、管控學生上課上網 ??。
2. 在 Linux，一行命令即可完成設定；在 Windows，Honda 老師亦幫忙撰寫批次檔。控制方式：
3. 任何設定皆不管控老師機，老師機可可自由上網。
4. 學生機上網方式：
 - (a) 自由上網
 - (b) 不能上網
 - (c) 限制只能上學內網
 - (d) 限制只能上某一網站
 - (e) 限制只能上「依老師設定」的部分網站
 - (f) 只有某一學生機可自由上網
5. 不管老師做任何網路設定，下課後系統自動恢復成所有電腦皆可自由上網，以避免因老師忘了復原，而影響下節上課的老師。

1.4 虛擬機管理界面

1. 設計虛擬機管理 GUI 程式，方便學生管理虛擬機。程式包含虛擬機重安裝、還原、重新啓動及終端界面等四個功能。
 - (a) Rebuild KVM：重新安裝 KVM 虛擬機，約 10 幾分鐘。

- (b) Revert KVM：還原 KVM 虛擬機，約幾秒鐘到幾分鐘，請耐心等候，不要在還原過程按管理界面的其他功能，以免造成虛擬機損壞。
- (c) Reboot KVM：重新啟動 KVM 虛擬機。
- (d) KVM Console：打開 KVM 虛擬機終端畫面。
2. 系統桌面中黑色背景視窗為 KVM 虛擬機操作界面。原始 KVM 虛擬機主機名稱為 111111，因已練習過，主機也已被設定成 kvm8，點擊 Revert KVM，幾秒後就可還原回原始狀態重新練習。



3. 在終端機以指令 virt-viewer 直接開啟虛擬機，出現錯誤訊息。

```

1 [dywang@dywH ~]$ sudo virt-viewer kvmusb
No protocol specified
3 Cannot open display:
Run 'virt-viewer --help' to see a full list of available command line
options

```

4. 先檢查 Xwindow 認證變數 \$XAUTHORITY 存不存在？

```
[dywang@dywH ~]$ echo $XAUTHORITY
```

5. 變數 XAUTHORITY 不存在，必須先設定 XAUTHORITY=~/.Xauthority 後再使用 sudo 啓動虛擬機，才能正常啓動。

```
[dywang@dywH ~]$ XAUTHORITY=~/.Xauthority sudo virt-viewer kvmusb
```

1.5 系統管理與評分

1. 系統管理腳本程式自動掃瞄目前開機的電腦，選擇要進行的工作，輸入密碼後即可自動完成。

```
1 [root@dywH ~]# e517sshpss.sh
2 myip=104
3 hosts=103,105
4 q(quit) iscsi halt reboot c(clear) l(lvm) rhcsa rhce
5 > t(mounttest) k(kvmreboot) v(kvmrevert) s(servicerestart)
6 > vi1 c1 lpvar c999 sh999 hp(hostpatch)? c999
7 keyin remote host root password:
```

2. 預設工作項目：

- (a) q(quit)：退出，無動作。
- (b) iscsi：學生機 ISCSI 硬碟分享架設。
- (c) halt：學生機關機。
- (d) reboot：學生機重新啓動。
- (e) c(clear)：登入學生機後清除部分資料，此部分保留修改彈性，目前入作爲限制學生機互相登入之限制，以防代作答情況。
- (f) l(lvm)：硬碟分割、格式化、自動掛掛評分。
- (g) rhcsa：RHCSA 考照練習總評分。
- (h) rhce：RHCE 考照練習總評分。
- (i) t(mounttest)：測試學生機是否有掛載隨身碟或光碟。
- (j) k(kvmreboot)：學生機 KVM 虛擬機重新啓動。
- (k) v(kvmrevert)：學生機 KVM 虛擬機還原。
- (l) s(servicerestart)：啓動學生機主機服務。
- (m) vi1：vi 編輯器實機練習評分。
- (n) c1：C 語言第一支程式練習評分。
- (o) lpvar：shell 變數變化練習評分。
- (p) c999：C 語言程式實機練習評分。
- (q) sh999：Shell script 程式練習評分。
- (r) hp(hostpatch)：學生機網路修正後重新啓動網路。

1.6 證照考試

1. 證照考試是手段，不是目的。爲的是讓學生藉由實機考照的訓練，熟悉 Linux 系統管理及伺服器架設。
2. 經紅帽原廠認證講師，可以提供學生最新的 Linux 技術。
3. 經紅帽原廠認證考官，可以主持 RHCSA, RHCE 認證考試，學生可以在自己最熟悉的環境考試。
4. 暑期證照班歡迎參加。

1.7 上課前先確定三件事

1. E517 教室位置，靠窗爲第一排，確認自己電腦位置爲 ?-?。例如：1-1。
2. 在伺服器（也就是開機進入圖形界面中有虛擬機管理界面的這台主機），不是虛擬機，確認自己的電腦 IP。以下例子爲 192.168.1.140，IP 尾數爲 140。

```

1 [dywang@deyu ~]$ ifconfig | grep 192
      inet addr:192.168.1.140 Bcast:192.168.1.255 Mask
                  :255.255.255.0
3          inet addr:192.168.122.1 Bcast:192.168.122.255 Mask
                  :255.255.255.0

```

3. 在伺服器 deyu.wang 主機一般帳號 dywang 家目錄，產生學號姓名檔 sid，檔案資訊格式爲「電腦位置 IP 尾數 學號 姓名」，每一欄位中間以一個空格隔開。以下例子電腦位置 1-11、IP 尾數 199、學號 123456，姓名 王大呆。

```

1 [dywang@deyu ~]$ echo '1-11 199 123456 王大呆' > sid
[dywang@deyu ~]$ cat sid
3 1-11 199 123456 王大呆

```

1.8 虛擬機設定

1. 伺服器（也就是開機進入圖形界面中有虛擬機管理界面的這台主機），不確定的話，先看命令列提示符號是不是 [dywang@deyu ~]\$，或是 ifconfig 查目前所在主機的 IP：
 - (a) Server 主機有兩個名稱 deyu.wang 及 server.deyu.wang
 - (b) Server 與虛擬機網域 deyu.wang，使用網段 192.168.122.0/24。
 - (c) Server IP 為 192.168.122.1，虛擬機 IP 為 192.168.122.X，其中 X 依題目要求設定。
 - (d) RHCE 練習環境增加一網域 my111.wang，使用網段 192.168.111.0/24，server 主機增加此網域 IP 192.168.111.1。

2. 虛擬機環境說明：

- (a) 虛擬機主機名稱 kvmX.deyu.wang IP 192.168.122.X，X 為虛擬機編號，例如 5 或 7。
- (b) 虛擬機 root 密碼無法取得，統一重新設定為 123qwe。
- (c) 虛擬機網路設定：

```

1 IP Address: 192.168.122.X
Netmask: 255.255.255.0
3 Gateway: 192.168.122.1
Name server: 192.168.122.1

```

- (d) repo server: <http://dywang.csie.cyut.edu.tw/centos7>.
- (e) kernel packages: 網路下載核心 RPM 檔 <http://dywang.csie.cyut.edu.tw/kernel/centos7>.
- (f) LDAP server 設定：
 - i. 系統 deyu.wang
 - ii. base DN 為 dc=deyu,dc=wang
 - iii. 證書 <ftp://deyu.wang/pub/cacert.pem>.

1.9 系統伺服器管理

1. 使用虛擬機練習時，伺服器（也就是開機進入圖形界面中有虛擬機管理界面的這台主機）必須正常運作，否則有些驗證無法進行。
2. 練習用到的 server 都已寫成腳本，如果運作有問題，可以執行腳本重啓。

1.9.1 DNS server

- (a) 如果確定你的練習虛擬機 DNS 設定沒問題，但 ssh 却無法使用主機名稱連線到虛擬機，可以在 server 機使用 host 命令看是否可以查到虛擬機的 IP？
- (b) 沒有 DNS server 可查。

```

2 [dywang@deyu ~]$ host kvm7.deyu.wang
;; connection timed out; trying next origin
;; connection timed out; no servers could be reached

```

- (c) 在 DNS server 查不到 kvm7.deyu.wang 的 IP。

```

1 [dywang@deyu ~]$ host kvm7.deyu.wang
Host kvm7.deyu.wang not found: 3(NXDOMAIN)

```

- (d) 在伺服器 deyu.wang 主機切換成 root 身份。

```

1 [dywang@deyu ~]$ su -
2 Password: 123123
3 [root@deyu ~]#

```

- (e) 執行 setdnsmasq.sh 腳本重啓 dnsmasq DNS 服務。

```

1 [root@deyu ~]# setdnsmasq.sh restart

```

- (f) 再使用 host 查詢 kvm7.deyu.wang，已可查到其 IP 為 192.168.122.7。

```

1 [root@deyu ~]# host kvm7.deyu.wang
kvm7.deyu.wang has address 192.168.122.7
3 kvm7.deyu.wang mail is handled by 1 20.

```

- (g) 如果執行 setdnsmasq.sh 腳本重啓 dnsmasq DNS 服務未能解決問題，還可以使用 setdns.sh 腳本啓動 named DNS 服務。

```

1 [root@deyu ~]# setdns.sh restart

```

1.9.2 LDAP server

- (a) 如果確認你的虛擬機 LDAP 設定沒問題，但還是無法以 ldapuser1 登入。在伺服器 deyu.wang 主機 (不是你的練習虛擬機)，先切換成 root 身份。

```

1 [dywang@deyu ~]$ su -
2 Password: 123123
3 [root@deyu ~]#

```

- (b) 在伺服器執行 setldap1.sh restart 重新產生 LDAP 憑證。因為憑證是新產生的，所以虛擬機必須再重新執行認證設定更新。

```

1 [root@deyu ~]# setldap1.sh restart

```

1.9.3 NFS server

- (a) 虛擬機設定自動掛載必須查得到 server 有分享目錄，server 的 NFS 不像 LDAP 有憑證過期問題，所以一般都不需要重啓，但如果要重啓 NFS server，先在伺服器 deyu.wang 主機切換成 root 身份。

```
1 [dywang@deyu ~]$ su -
Password: 123123
3 [root@deyu ~]#
```

(b) 執行 setnfs.sh 腳本重新啓動。

```
1 [root@deyu ~]# setnfs.sh restart
```

Chapter 2

SELinux

2.1 設計原由

1. 自主式存取控制 (Discretionary Access Control, DAC)

- (a) 傳統的檔案權限與帳號關係：依據程序的擁有者與檔案資源的 rwx 權限來決定有無存取的能力。
- (b) 若該程序屬 root 權限，則其可在系統上進任何資源存取。
- (c) 若某個目錄權限為 777，則任何帳號的程序都可任意存取及寫入。

2. 系統出現問題

- (a) 內部員工的資源誤用遠高於外部攻擊。
- (b) 員工資源誤用：系統管理員為了自己方便，將防火牆完全關閉或某個檔案目錄的權限設定為 777。
- (c) 為控管員工資源誤用問題，美國國家安全局 (NSA) 開發安全增強式 Linux (SELinux, Security-Enhanced Linux) 模組，並整合到 Linux 核心。
- (d) SELinux 是一種強制存取控制 (mandatory access control, MAC) 的實現。

3. 強制存取控制

- (a) 針對特定的程序與特定的檔案資源進行權限的控管。
- (b) WWW server 啓動的程序為 httpd，selinux 預設僅能在 /var/www 目錄下存取檔案。

2.2 啓動、關閉與觀察

1. SELinux 開機啓動模式

```

1 [root@kvm7 ~]# vim /etc/selinux/config
2 [root@kvm7 ~]# cat /etc/selinux/config
3
4 # This file controls the state of SELinux on the system.
5 # SELINUX= can take one of these three values:
6 #       enforcing - SELinux security policy is enforced.

```

```

7  #      permissive - SELinux prints warnings instead of enforcing.
#      disabled - No SELinux policy is loaded.
9  SELINUX=enforcing
# SELINUXTYPE= can take one of three two values:
11 #      targeted - Targeted processes are protected,
#      minimum - Modification of targeted policy. Only selected processes
#      are protected.
13 #      mls - Multi Level Security protection.
SELINUXTYPE=targeted

```

2. 關察目前 SELinux 狀態

```

[root@kvm7 ~]# sestatus
2 SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
4 SELinux root directory:        /etc/selinux
Loaded policy name:              targeted
6 Current mode:                  permissive
Mode from config file:          enforcing
8 Policy MLS status:             enabled
Policy deny_unknown status:     allowed
10 Max kernel policy version:    28

```

3. 改變 SELinux 模式

```

[root@kvm7 ~]# getenforce
2 Permissive
[root@kvm7 ~]# setenforce 1
4 [root@kvm7 ~]# getenforce
Enforcing

```

2.3 SELinux Contexts

1. Display Contexts

```

1 [root@deyu ~]# ps axZ | grep sshd
system_u:system_r:sshd_t:s0-s0:c0.c1023 2054 ? Ss      0:00 /usr/sbin/
      sshd
3 #user:role:type:range
#for a process, the type is also called the domain of the process
5
7 [root@deyu ~]# ls -Z anaconda-ks.cfg
-rw-----. root root system_u:object_r:admin_home_t:s0 anaconda-ks.cfg

```

2. 安裝套件。

```
1 [root@kvm5 ~]# yum install httpd -y
```

3. 啓動 httpd 服務，並設定開機啓動。

```
1 [root@deyu ~]# systemctl enable httpd.service
ln -s '/usr/lib/systemd/system/httpd.service' '/etc/systemd/system/multi
-user.target.wants/httpd.service'
3 [root@deyu ~]# systemctl start httpd
```

4. File's context depends on where it was created

```
1 [root@deyu ~]# cal > ~/index.html
[root@deyu ~]# cal > /var/www/html/index.html
3 [root@deyu ~]# ls -Z ~/index.html /var/www/html/index.html
-rw-r--r--. root root unconfined_u:object_r:admin_home_t:s0 /root/index.
    html
5 -rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 /var/
    www/html/index.html
[root@deyu ~]# ls -Zd ~ /var/www/html
7 dr-xr-x---. root root system_u:object_r:admin_home_t:s0 /root
drwxr-xr-x. root root system_u:object_r:httpd_sys_content_t:s0 /var/www/
    html
```

5. 測試 httpd 檔案

```
1 [root@deyu ~]# curl http://127.0.0.1/index.html
2      December 2011
3      Su Mo Tu We Th Fr Sa
4          1  2  3
5      4  5  6  7  8  9 10
6      11 12 13 14 15 16 17
7      18 19 20 21 22 23 24
8      25 26 27 28 29 30 31
10 [root@deyu ~]# mv index.html /var/www/html/index.html
11 mv: overwrite `/var/www/html/index.html'? y
12
```

```

14 [root@deyu ~]# curl http://127.0.0.1/index.html
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
16 <title>403 Forbidden</title>
</head><body>
18 <h1>Forbidden</h1>
<p>You don't have permission to access /index.html
20 on this server.</p>
<hr>
22 <address>Apache/2.2.15 (CentOS) Server at 127.0.0.1 Port 80</address>
</body></html>
```

6. Change index.html SELinux security context

```

1 [root@deyu ~]# ls -Z /var/www/html/index.html
-rw-r--r--. root root unconfined_u:object_r:admin_home_t:s0 /var/www/
    html/index.html
3 [root@deyu ~]# chcon -t httpd_sys_content_t /var/www/html/index.html
[root@deyu ~]# ls -Z /var/www/html/index.html
5 -rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 /var/
    www/html/index.html
[root@deyu ~]# curl http://127.0.0.1/index.html
7 December 2011
Su Mo Tu We Th Fr Sa
9      1  2  3
  4  5  6  7  8  9 10
11 11 12 13 14 15 16 17
18 19 20 21 22 23 24
13 25 26 27 28 29 30 31
```

7. Restore the context of index.html

```

1 [root@deyu ~]# cal > ~/index.html
[root@deyu ~]# mv index.html /var/www/html/index.html
3 mv: overwrite `/var/www/html/index.html'? y
[root@deyu ~]# restorecon -Rv /var/www/html/index.html
5 restorecon reset /var/www/html/index.html context unconfined_u:object_r:
    admin_home_t:s0->system_u:object_r:httpd_sys_content_t:s0

7 [root@deyu ~]# curl http://127.0.0.1/index.html
    December 2011
9 Su Mo Tu We Th Fr Sa
      1  2  3
11  4  5  6  7  8  9 10
18 11 12 13 14 15 16 17
13 18 19 20 21 22 23 24
25 26 27 28 29 30 31
```

Chapter 3

Netfilter

3.1 前言

1. Linux 核心包含一個功能強大的網路過濾子系統 netfilter。
2. netfilter 子系統允許核心模組檢查每一個傳送到系統的封包，因此可以在送到用戶端時對封包修改、拒絕、丟棄。
3. RHEL/CentOS 6 使用 iptables 與核心的 netfilter 互動，但 iptables 只能調整 IPV4 的防火牆規則，對於 IPV6 及則必須使用 ip6tables。
4. RHEL/CentOS 7 使用新的方法 firewalld 與核心的 netfilter 互動，firewalld 是一個系統 daemon，它可以監看並修改系統的防火牆規則，且同時適用於 IPV4 與 IPV6。
5. firewalld 將所有網路傳輸分成不同的 zones。運作方式流程為：
 - (a) 進入系統的封包，先檢查來源 IP。
 - (b) 如果來源 IP 有綁定指定的 zone，就使用該 zone 的規則。
 - (c) 如果來源 IP 沒有綁定某一個 zone，就使用進入系統使用的網路介面 (network interface) 連結的 zone。
 - (d) 如果網路介面沒有連結任何一個 zone，就使用管理者預設的 zone。
6. 系統預先定義的 zones 如下：

Zone name	Default configuration
trusted	完全開放，允許所有進入的封包。
home	只開放 ssh, mdns, ipp-client, samba-client, or dhcpcv6-client 等服務及相關的送出封包，其餘封包皆拒絕。
internal	與 home zone 完全相同。
work	只開放 ssh, ipp-client, or dhcpcv6-client 等服務及相關的送出封包，其餘封包皆拒絕。
public	只開放 ssh or dhcpcv6-client 等服務及相關的送出封包，其餘封包皆拒絕。新增的網路介面預設使用這個 zone。
external	只開放 ssh 服務及相關的送出封包，其餘封包皆拒絕，送出的 IPv4 封包經由這個 zone 轉傳，IP 會被偽裝為送出的網路介面的 IP。
dmz	只開放 ssh 服務及相關的送出封包，其餘封包皆拒絕。
block	拒絕所有封包。
drop	丟棄所有封包。

7. 防火牆設定方式：

- (a) 直接編輯目錄 /etc/firewalld/ 下的設定檔。
 - (b) 使用圖形化工具 firewall-config。
 - (c) 使用文字介面命令 firewall-cmd。
8. 雖然 firewall-cmd 命令參數多又長，但因此命令有參數補齊功能，使用 TAB 鍵就可顯示可用參數及補齊，建議還是使用文字介面命令工具 firewall-cmd 比較穩定且方便。

3.2 firewall-cmd 命令

1. firewall-cmd 命令選項說明如下，其中若未指定 zone，就是使用預設的 zone。

firewall-cmd 命令	說明
--get-default-zone	查詢預設的 zone。
--set-default-zone=<ZONE>	設定預設的 zone，會同時改變即時及永久的設定。
--get-zones	列出所有的 zones。
--get-active-zones	列出目前正在使用的 zones 及綁定該 zone 的網路介面資訊。
-- add- source=<CIDR> zone=<ZONE>]	[-- 設定 network/netmask 路線到指定的 zone。
-- remove- source=<CIDR> zone=<ZONE>]	[-- 從指定的 zone 移除 network/netmask <CIDR>。
--add-interface=<INTERFACE> zone=<ZONE>]	[-- 設定來自網路介面路線到指定的 zone。
--change-interface=<INTERFACE> [--zone=<ZONE>]	綁定網路介面到指定的 zone。
--list-all [--zone=<ZONE>]	列出 zone 所有設定的網路介面、來源、服務及埠號。
--list-all-zones	檢索所有 zones 的所有訊息，包含網路介面、來源、埠號及服務等。
-- add-service=<SERVICE> zone=<ZONE>]	[-- 允許封包到某服務。
--add-port=<PORT/PROTOCOL> zone=<ZONE>]	[-- 允許封包到某協定及埠號。
--remove-service=<SERVICE> zone=<ZONE>]	[-- 從指定的 zone 移除某一服務。
--remove-port=<PORT/ PROTOCOL> [--zone=<ZONE>]	從指定的 zone 移除某協定及埠號。
--reload	丟棄目前使用的設定，使用設定檔中的設定。

2. 選項都可使用 TAB 提示及補齊，不用死記。

3.3 啓用 firewall

1. firewall 與 iptables, ip6tables, ebtables 服務相互衝突，關閉這些服務。

```
[root@kvm7 ~]# systemctl mask iptables.service
2 ln -s '/dev/null' '/etc/systemd/system/iptables.service'
[root@kvm7 ~]# systemctl mask ip6tables.service
4 ln -s '/dev/null' '/etc/systemd/system/ip6tables.service'
[root@kvm7 ~]# systemctl mask ebtables.service
6 ln -s '/dev/null' '/etc/systemd/system/ebtables.service'
```

2. 檢查 firewall 服務狀態。

```
[root@kvm7 ~]# systemctl status firewalld.service
2 firewalld.service - firewalld - dynamic firewall daemon
    Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled)
4     Active: active (running) since Thu 2014-08-21 18:51:18 CST; 3min 18s
        ago
    Main PID: 569 (firewalld)
6      CGroup: /system.slice/firewalld.service
               569 /usr/bin/python -Es /usr/sbin/firewalld --nofork --nopid
8
Aug 21 18:51:18 kvm7.deyu.wang systemd[1]: Started firewalld - dynamic
firew.....
10 Hint: Some lines were ellipsized, use -l to show in full.
```

3. 如果沒有啓動，啓動 firewall，並設定開機啓動。

```
[root@kvm7 ~]# systemctl enable firewalld.service
2 [root@kvm7 ~]# systemctl start firewalld.service
```

4. 查詢 firewall 預設 zone 為 public。

```
[root@kvm7 ~]# firewall-cmd --get-default-zone
2 public
```

5. 如果預設 zone 不是 public，則設定 public 為預設 zone。

```
[root@kvm7 ~]# firewall-cmd --set-default-zone public
2 Warning: ZONE_ALREADY_SET: public
```

6. 檢查 public zone 的永久設定，開放的服務只有 dhcpcv6-client 及 ssh。

```
[root@kvm7 ~]# firewall-cmd --permanent --zone=public --list-all
2 public (default)
    interfaces:
4     sources:
    services: dhcpcv6-client ssh
6     ports:
    masquerade: no
8     forward-ports:
```

```
10  icmp-blocks:  
    rich rules:
```

3.4 block zone

1. block zone 拒絕所有封包，所以如果要完全限制某些 IP (例如：192.168.122.0/24) 進入本機，只要指定這些 IP 使用 block zone 即可。

```
2 [root@kvm5 ~]# firewall-cmd --permanent --zone=block \  
  --add-source='192.168.122.0/24'  
success
```

2. 列出目前 block zone 還未生效。

```
1 [root@kvm5 ~]# firewall-cmd --zone=block --list-all  
2 block  
3     interfaces:  
4     sources:  
5     services:  
6     ports:  
7     masquerade: no  
8     forward-ports:  
9     icmp-blocks:  
10    rich rules:
```

3. 重新載入 firewall。

```
2 [root@kvm5 ~]# firewall-cmd --reload  
success
```

4. 目前 block zone 已生效，192.168.122.0/24 網段使用此 zone。

```
2 [root@kvm5 ~]# firewall-cmd --zone=block --list-all  
3 block  
4     interfaces:  
5     sources: 192.168.122.0/24  
6     services:  
7     ports:  
8     masquerade: no  
9     forward-ports:
```

```
10  [root@kvm5 ~]# firewall-cmd --zone=block --list-all  
rich rules:
```

5. kvm7 無法連線 kvm5.deyu.wang。

```
2  [root@kvm7 ~]# ssh kvm5.deyu.wang  
ssh: connect to host kvm5.deyu.wang port 22: No route to host
```

6. kvm7 無法連線 kvm5.deyu.wang。

```
2  [root@kvm5 ~]# firewall-cmd --permanent --zone=block \  
--remove-source='192.168.122.0/24'  
success  
4  [root@kvm5 ~]# firewall-cmd --permanent --zone=block \  
--add-source='192.168.111.0/24'  
6  success
```

7. 重新載入 firewall。

```
2  [root@kvm5 ~]# firewall-cmd --reload  
success
```

8. 目前 block zone 已生效，192.168.111.0/24 網段使用此 zone。

```
2  [root@kvm5 ~]# firewall-cmd --zone=block --list-all  
block  
interfaces:  
sources: 192.168.111.0/24  
services:  
ports:  
masquerade: no  
forward-ports:  
icmp-blocks:  
rich rules:
```

9. kvm7 又可以連線 kvm5.deyu.wang 了。

```

1 [root@kvm7 ~]# ssh kvm5.deyu.wang
2 root@kvm5.deyu.wang's password:
3 Last login: Sun Aug 30 22:33:49 2015 from server.deyu.wang
4 [root@kvm5 ~]# exit
5 logout
6 Connection to kvm5.deyu.wang closed.

```

3.5 firewall direct rules

- 除了正規的 zones 及 services 語法外，firewalld 還提供 direct rules 及 rich rules 兩種選項，Direct rules 允許管理者直接加入 iptables 過濾語法。

```

usage: --direct --add-rule { ipv4 | ipv6 | eb } <table> <chain> <
       priority <args>

```

- 先查看目前及永久的 direct rules 都是空的。

```

1 [root@kvm5 ~]# firewall-cmd --permanent --direct --get-all-rules
[root@kvm5 ~]# firewall-cmd --direct --get-all-rules

```

- 加入永久的 direct rules，REJECT 192.168.122.0/24 IP 使用 SSH 22 port。

```

2 [root@kvm5 ~]# firewall-cmd --permanent --direct --add-rule \
  ipv4 filter INPUT 0 -s 192.168.122.0/24 -p tcp --dport 22 -j REJECT
  success

```

- 目前的 direct rules 還是空的，永久的 direct rules 有一條 REJECT 規則。

```

1 [root@kvm5 ~]# firewall-cmd --permanent --direct --get-all-rules
  ipv4 filter INPUT 0 -s 192.168.122.0/24 -p tcp --dport 22 -j REJECT
3 [root@kvm5 ~]# firewall-cmd --direct --get-all-rules

```

- 在 kvm7 連線 kvm5.deyu.wang 還是可以連線，注意顯示的上次連線是從 deyu.wang 而不是 kvm7.deyu.wang，原因為 kvm7.deyu.wang 是經由 deyu.wang 連線到 kvm5.deyu.wang。

```

1 [root@kvm7 ~]# ssh kvm5.deyu.wang
root@kvm5.deyu.wang's password:
3 Last login: Sun Aug 30 21:38:01 2015 from deyu.wang
[root@kvm5 ~]# exit
5 logout
Connection to kvm5.deyu.wang closed.

```

6.

7. `--permanent` 參數永久有效是指開機生效，但目前狀態並不會改變，所以如果要測試是否生效，必須取消 `--permanent` 參數再執行一次，才能改變目前的狀態，這與服務的啓動概念一樣。REJECT 必須大寫。

```

1 [root@kvm5 ~]# firewall-cmd --direct --add-rule ipv4 \
2 filter INPUT 0 -s 192.168.122.0/24 -p tcp --dport 22 -j REJECT
success

```

8. 目前的 direct rules 與永久的 direct rules 都有一條 REJECT 規則。

```

1 [root@kvm5 ~]# firewall-cmd --permanent --direct --get-all-rules
ipv4 filter INPUT 0 -s 192.168.122.0/24 -p tcp --dport 22 -j REJECT
3 [root@kvm5 ~]# firewall-cmd --direct --get-all-rules
ipv4 filter INPUT 0 -s 192.168.122.0/24 -p tcp --dport 22 -j REJECT

```

9. 在 kvm7 已無法連線 kvm5.deyu.wang。

```

1 [root@kvm7 ~]# ssh kvm5.deyu.wang
2 ssh: connect to host kvm5.deyu.wang port 22: Connection refused

```

10. 移除目前的及永久的 direct rules。

```

1 [root@kvm5 ~]# firewall-cmd --direct --remove-rule \
2 ipv4 filter INPUT 0 -s 192.168.122.0/24 -p tcp --dport 22 -j REJECT
success
4 [root@kvm5 ~]# firewall-cmd --direct --permanent --remove-rule \
5 ipv4 filter INPUT 0 -s 192.168.122.0/24 -p tcp --dport 22 -j REJECT
6 success

```

11. 列出目前的及永久的 direct rules 都是空的。

```
1 [root@kvm5 ~]# firewall-cmd --permanent --direct --get-all-rules
2 [root@kvm5 ~]# firewall-cmd --direct --get-all-rules
```

12. 詳細的使用說明

```
[root@kvm5 ~]# man 5 firewalld.direct
```

3.6 firewall rich rules

1. Rich rules 可以使用基本的 allow/deny rules，也可以設定為 syslog and auditd, port forwards, masquerading, 及 rate limiting。多條規則同時在同一個 zone，規則的順序對防火牆影響很大，其規則的順序如下：
 - (a) port forwarding and masquerading 規則
 - (b) logging 規則，匹配此規則封包會繼續被處理。
 - (c) allow 規則
 - (d) deny 規則
2. 以上規則順序，先匹配先執行，如果一封包沒有匹配 zone 內的任何規則，基本上是被限制，但還是要看其他的 zone 是否接受。
3. 基本語法：

```
1 rule
2   [source]
3   [destination]
4   service|port|protocol|icmp-block|masquerade|forward-port
5   [log]
6   [audit]
7   [accept|reject|drop]
```

4. 詳細語法說明：

```
1 [root@kvm5 ~]# man 5 firewalld.richlanguage
```

5. public zone 開放 ssh 服務，所以若要求 192.168.122.0/24 可以使用 SSH 連線，而 192.168.111.0/24 不能使用 SSH 連線，則只需要設定限制的 rich rules。在預設的 public zone 限制 192.168.111.0/24 不可以使用 SSH 連線，其中 reject 必須小寫。

```

1 [root@kvm5 ~]# firewall-cmd --permanent --zone=public --add-rich-rule \
2   "rule family=\"ipv4\" source address=\"192.168.111.0/24\" port port=\"22\""
3     protocol=\"tcp\" reject"
4 success
5 [root@kvm5 ~]# firewall-cmd --reload
6 success

```

6. 查看 kvm5 防火牆狀態，新增了拒絕 192.168.111.0/24 使用 ssh 22 port 的規則。

```

1 [root@kvm5 ~]# firewall-cmd --list-all
2   public (default, active)
3     interfaces: eth0
4     sources:
5       services: dhcpcv6-client kerberos ssh
6       ports: 464/tcp 749/tcp
7       masquerade: no
8       forward-ports:
9       icmp-blocks:
10      rich rules:
11        rule family="ipv4" source address="192.168.111.0/24" port port="22"
12          protocol="tcp" reject

```

7. 要從主機 kvm7.deyu.wang 測試 kvm5.deyu.wang 防火牆環境，先在 kvm7.deyu.wang 主機上以 root 身份新增 eth0 網卡 IP 192.168.111.7/24。

```

1 [root@kvm7 ~]# ifconfig eth0:1 192.168.111.7/24 up

```

8. 查看主機 kvm7.deyu.wang 有 192.168.122.7 及 192.168.111.7 兩個 IP。

```

1 [root@kvm7 ~]# ifconfig | grep -A1 eth0
2   eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
3         inet 192.168.122.7  netmask 255.255.255.0  broadcast
4             192.168.122.255
5 --
6   eth0:1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
7         inet 192.168.111.7  netmask 255.255.255.0  broadcast
8             192.168.111.255

```

9. kvm5.deyu.wang 限制 192.168.111.0/24 ssh 連線，主機 kvm7.deyu.wang ssh 綁定 192.168.122.7 可以成功連線 kvm5.deyu.wang，但若綁定 192.168.111.7 則無法順利連線。

```

1 [root@kvm7 ~]# ssh -b 192.168.122.7 kvm5.deyu.wang
root@kvm5.deyu.wang's password:
3 Last login: Mon May 28 15:33:01 2018 from deyu.wang
[root@kvm5 ~]# exit
5 logout
Connection to kvm5.deyu.wang closed.
7 [root@kvm7 ~]# ssh -b 192.168.111.7 kvm5.deyu.wang
ssh: connect to host kvm5.deyu.wang port 22: Connection refused

```

10. 測試後 kvm7 馬上取消 eth0:1 網卡設定，以免影響後續測試。

```

1 [root@kvm7 ~]# ifconfig eth0:1 down
2 [root@kvm7 ~]# ifconfig | grep eth0 -A1
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
4         inet 192.168.122.7 netmask 255.255.255.0 broadcast
              192.168.122.255

```

11. 如果設定沒錯，但 ssh 綁定 192.168.111.1 還是可以連線，要檢查 client 的 iptables 是否做 POSTROUTING ?

```
-A POSTROUTING -i virbr0 -j MASQUERADE
```

3.7 Masquerading and Port Forwarding

1. 內網虛擬 IP 無法直接上網，必須靠 NAT 轉發 (Forwarding) 內部網路封包時偽裝 (Masquerading) 封包發送 IP 為可以連上網際網路的實體 IP。

```

1 [root@kvm5 ~]# firewall-cmd --permanent --zone=public --add-masquerade
success
3 [root@kvm5 ~]# firewall-cmd --permanent --zone=public --list-all
public (default)
5   interfaces:
sources:
7   services: dhcpcv6-client ssh
ports:
9   masquerade: yes
      forward-ports:

```

```
11  || icmp-blocks:  
    rich rules:
```

2. NAT 的另一項重要工作是 Port forwarding。Port forwarding 可以將 port 轉發到同台主機上不同的 port，例如將進入 5423 port 的封包，轉發到同一台主機上的 80 port。

```
1 [root@kvm5 ~]# firewall-cmd --permanent --zone=public --add-forward-port  
2   =port=5423:proto=tcp:toport=80  
3   success  
4 [root@kvm5 ~]# firewall-cmd --reload  
5   success  
6 [root@kvm5 ~]# firewall-cmd --list-forward-ports  
7   port=5423:proto=tcp:toport=80:toaddr=
```

3. 如果本機已架設 httpd，可從其他主機如 kvm7.deyu.wang 連線 `http://kvm5.deyu.wang:5423` 測試是否 port forwarding？kvm5 先安裝 httpd 服務，但一開始 repository 並未設定，所以要先設定 repository。

```
1 [root@kvm5 ~]# vim /etc/yum.repos.d/dywang.repo  
2 [root@kvm5 ~]# cat /etc/yum.repos.d/dywang.repo  
3 [dywang]  
4 name=De-Yu Wang  
5 baseurl=http://dywang.csie.cyut.edu.tw/centos7  
6 gpgcheck=0
```

4. 安裝、啓動、設定開機啓動 httpd 服務。

```
1 [root@kvm5 ~]# yum install httpd  
2 [root@kvm5 ~]# systemctl enable httpd.service  
3 ln -s '/usr/lib/systemd/system/httpd.service' '/etc/systemd/system/multi  
4 -user.target.wants/httpd.service'  
[root@kvm5 ~]# systemctl start httpd.service
```

5. 寫一個簡單的網頁首頁。

```
[root@kvm5 ~]# echo 'port forwarding test' > /var/www/html/index.html
```

6. kvm7 連線 kvm5.deyu.wang 的 5423 port，被轉發到網頁的 80 port。

```
1 [root@kvm7 ~]# curl http://kvm5.deyu.wang:5423
  port forwarding test
```

3.8 *NAT 設定與測試

1. 測試環境：

```
2 kvm7 eth0 192.168.122.7 對外
  eth1 192.168.10.7 對內
4 kvm6 eth0 192.168.10.6 經由 kvm7 的 eth1 上網
  kvm5 eth0 192.168.10.5 經由 kvm7 的 eth1 上網
```

2. 目前使用的 zone 為 public 沒有 masquerade 功能，kvm6 無法上網。

```
1 [root@kvm7 ~]# firewall-cmd --list-all
public (default, active)
  interfaces: eth0 eth1
  sources:
  services: dhcpcv6-client ssh
  ports:
  masquerade: no
  forward-ports:
  icmp-blocks:
  rich rules:
11
13 [root@kvm6 ~]# ping -c2 163.17.10.1
PING 163.17.10.1 (163.17.10.1) 56(84) bytes of data.

15 --- 163.17.10.1 ping statistics ---
  2 packets transmitted, 0 received, 100% packet loss, time 10999ms
```

3. public zone 永久加上 masquerade 功能且重新載入，kvm6 已經可以上網。

```
2 [root@kvm7 ~]# firewall-cmd --permanent --add-masquerade
success
3 [root@kvm7 ~]# firewall-cmd --reload
success
4 [root@kvm7 ~]# firewall-cmd --list-all
public (default, active)
```

```

8   interfaces: eth0 eth1
9   sources:
10  services: dhcpcv6-client ssh
11  ports:
12  masquerade: yes
13  forward-ports:
14  icmp-blocks:
15  rich rules:

16 [root@kvm6 ~]# ping -c2 163.17.10.1
17 PING 163.17.10.1 (163.17.10.1) 56(84) bytes of data.
18 64 bytes from 163.17.10.1: icmp_seq=1 ttl=52 time=13.8 ms
19 64 bytes from 163.17.10.1: icmp_seq=2 ttl=52 time=13.1 ms
20
21 --- 163.17.10.1 ping statistics ---
22 2 packets transmitted, 2 received, 0% packet loss, time 1015ms
23 rtt min/avg/max/mdev = 13.113/13.472/13.831/0.359 ms

```

4. 使用 direct rule 暫時加上只能上校內網站，注意 FORWARD 後接的數字為優先序，對防火牆的規則很重要。kvm6 測試如預期可以上校內網站，但不能連上校外。

```

1 [root@kvm7 ~]# firewall-cmd --direct --add-rule ipv4 filter FORWARD 10 -
2   s 192.168.10.0/24 -j REJECT
3 success
4 [root@kvm7 ~]# firewall-cmd --direct --add-rule ipv4 filter FORWARD 0 -d
5   163.17.0.0/16 -j ACCEPT
6 success
7 [root@kvm7 ~]# firewall-cmd --direct --add-rule ipv4 filter FORWARD 1 -d
8   120.110.0.0/16 -j ACCEPT
9 success
10
11 [root@kvm7 ~]# firewall-cmd --direct --get-all-rules
12 ipv4 filter FORWARD 10 -s 192.168.10.0/24 -j REJECT
13 ipv4 filter FORWARD 0 -d 163.17.0.0/16 -j ACCEPT
14 ipv4 filter FORWARD 1 -d 120.110.0.0/16 -j ACCEPT
15
16 [root@kvm6 ~]# ping -c2 163.17.10.1
17 PING 163.17.10.1 (163.17.10.1) 56(84) bytes of data.
18 64 bytes from 163.17.10.1: icmp_seq=1 ttl=52 time=13.1 ms
19 64 bytes from 163.17.10.1: icmp_seq=2 ttl=52 time=19.0 ms
20
21 --- 163.17.10.1 ping statistics ---
22 2 packets transmitted, 2 received, 0% packet loss, time 1020ms
23 rtt min/avg/max/mdev = 13.189/16.136/19.084/2.950 ms
24
25 [root@kvm6 ~]# ping -c2 120.110.10.84
26 PING 120.110.10.84 (120.110.10.84) 56(84) bytes of data.
27 64 bytes from 120.110.10.84: icmp_seq=2 ttl=52 time=13.4 ms
28
29 --- 120.110.10.84 ping statistics ---
30 2 packets transmitted, 1 received, 50% packet loss, time 10999ms

```

```

1   rtt min/avg/max/mdev = 13.433/13.433/13.433/0.000 ms
29
30 [root@kvm6 ~]# ping -c2 8.8.8.8
31 PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
32 From 192.168.10.254 icmp_seq=1 Destination Port Unreachable
33 From 192.168.10.254 icmp_seq=2 Destination Port Unreachable
34
35 --- 8.8.8.8 ping statistics ---
36 2 packets transmitted, 0 received, +2 errors, 100% packet loss, time
   1000ms

```

5. 暫時改用 block zone，kvm6 無法上網。

```

1 [root@kvm7 ~]# firewall-cmd --set-default-zone=block
2 success
3
4 [root@kvm6 ~]# ping -c2 163.17.10.1
5 PING 163.17.10.1 (163.17.10.1) 56(84) bytes of data.
6
7 --- 163.17.10.1 ping statistics ---
8 2 packets transmitted, 0 received, 100% packet loss, time 10999ms

```

6. 改用 public zone 且使用 direct rule 暫時加入最優先規則讓 192.168.10.6 可以不受限制的上網，此功能可以做為管理機（老師機）放行用，因此雖然限制只能上校內網站，kvm6 不受影響還是連上校外。

```

1 [root@kvm7 ~]# firewall-cmd --set-default-zone=public
2 success
3
4 [root@kvm7 ~]# firewall-cmd --direct --add-rule ipv4 filter FORWARD -10
   -s 192.168.10.6/32 -j ACCEPT
5 success
6 [root@kvm7 ~]# firewall-cmd --direct --get-all-rules
7 ipv4 filter FORWARD 10 -s 192.168.10.0/24 -j REJECT
8 ipv4 filter FORWARD 0 -d 163.17.0.0/16 -j ACCEPT
9 ipv4 filter FORWARD 1 -d 120.110.0.0/16 -j ACCEPT
10 ipv4 filter FORWARD -10 -s 192.168.10.6/32 -j ACCEPT
11
12 [root@kvm6 ~]# ping -c2 8.8.8.8
13 PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
14 64 bytes from 8.8.8.8: icmp_seq=1 ttl=46 time=23.4 ms
15 64 bytes from 8.8.8.8: icmp_seq=2 ttl=46 time=23.4 ms
16
17 --- 8.8.8.8 ping statistics ---
18 2 packets transmitted, 2 received, 0% packet loss, time 1025ms
   rtt min/avg/max/mdev = 23.440/23.467/23.494/0.027 ms

```

7. 預設 zone 設定為 block，則 kvm6 無法對外連線。

```

1 [root@kvm7 ~]# firewall-cmd --set-default-zone=block
success
3
5 [root@kvm6 ~]# ping -c2 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
7 --- 8.8.8.8 ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 11000ms

```

8. 在最優先放行管理機的規則後加入一條完全拒阻封包的規格，則只有管理機可以上網。

```

1 [root@kvm7 ~]# firewall-cmd --direct --add-rule ipv4 filter FORWARD -9 -
s 192.168.10.0/24 -j REJECT
2 success
[root@kvm7 ~]# firewall-cmd --direct --get-all-rules ipv4 filter FORWARD
0 -d 163.17.0.0/16 -j ACCEPT
4 ipv4 filter FORWARD 1 -d 120.110.0.0/16 -j ACCEPT
ipv4 filter FORWARD 10 -s 192.168.10.0/24 -j REJECT
6 ipv4 filter FORWARD -10 -s 192.168.10.6/32 -j ACCEPT
ipv4 filter FORWARD -9 -s 192.168.10.0/24 -j REJECT
8
10 [root@kvm5 ~]# ping -c2 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
From 192.168.10.5 icmp_seq=1 Destination Port Unreachable
12 From 192.168.10.5 icmp_seq=2 Destination Port Unreachable
14 --- 8.8.8.8 ping statistics ---
2 packets transmitted, 0 received, +2 errors, 100% packet loss, time 999
ms
16
18 [root@kvm6 ~]# ping -c2 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=46 time=23.5 ms
20 64 bytes from 8.8.8.8: icmp_seq=2 ttl=46 time=23.1 ms
22 --- 8.8.8.8 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1024ms
24 rtt min/avg/max/mdev = 23.195/23.386/23.577/0.191 ms

```

9. 移除兩條限制上網的規格，則所有機器都可以上網。

```

[root@kvm7 ~]# firewall-cmd --direct --remove-rule ipv4 filter FORWARD
-9 -s 192.168.10.0/24 -j REJECT

```

```
2 || [root@kvm7 ~]# firewall-cmd --direct --remove-rule ipv4 filter FORWARD  
10 -s 192.168.10.0/24 -j REJECT  
success  
4 || [root@kvm7 ~]# firewall-cmd --direct --get-all-rules  
ipv4 filter FORWARD -10 -s 192.168.10.6/32 -j ACCEPT  
6 || ipv4 filter FORWARD 0 -d 163.17.0.0/16 -j ACCEPT  
8 || ipv4 filter FORWARD 1 -d 120.110.0.0/16 -j ACCEPT  
10 ||  
12 || [root@kvm6 ~]# ping -c2 8.8.8.8  
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.  
64 bytes from 8.8.8.8: icmp_seq=1 ttl=46 time=23.5 ms  
14 || --- 8.8.8.8 ping statistics ---  
16 || 2 packets transmitted, 2 received, 0% packet loss, time 1024ms  
rtt min/avg/max/mdev = 23.195/23.386/23.577/0.191 ms
```


Chapter 4

可執行檔

4.1 檔案權限

1. 檔案權限與屬性為學習 Linux 之重要關卡。
2. 在根目錄 “ / ” 下，輸入指令 ls -al

```
[dywang@mdk-dyw /]$ ls -al
2 total 72
3 drwxr-xr-x 18 root adm 4096 Sep 16 11:11 .
4 drwxr-xr-x 18 root adm 4096 Sep 16 11:11 ../
5 -rw-r--r-- 1 root root 0 Sep 16 11:11 .autofsck
6 drwxr-xr-x 2 root root 4096 Sep 28 12:50 bin/
7 drwxr-xr-x 3 root root 4096 Sep 16 11:11 boot/
8 drwxr-xr-x 26 root root 14420 Oct 1 12:30 dev/
9 drwxr-xr-x 85 root root 8192 Sep 29 12:59 etc/
10 drwxr-xr-x 18 root root 4096 Sep 26 12:45 home/
11 drwxr-xr-x 2 root root 4096 Sep 9 16:14 initrd/
12 drwxr-xr-x 11 root root 4096 Sep 28 12:49 lib/
13 drwxr-xr-x 5 root root 4096 Sep 29 12:59 mnt/
14 drwxr-xr-x 2 root root 4096 Jan 5 2004 opt/
15 dr-xr-xr-x 179 root root 0 Sep 16 11:10 proc/
16 -rw----- 1 root root 1024 Sep 9 13:06 .rnd
17 drwx----- 16 root root 4096 Oct 1 13:13 root/
18 drwxr-xr-x 2 root root 8192 Sep 28 12:50 sbin/
19 drwxr-xr-x 10 root root 0 Sep 16 11:10 sys/
20 drwxrwxrwt 23 root root 4096 Oct 1 13:13 tmp/
21 drwxr-xr-x 12 root root 4096 Sep 9 13:15 usr/
22 drwxr-xr-x 23 root root 4096 Sep 9 17:31 var/
```

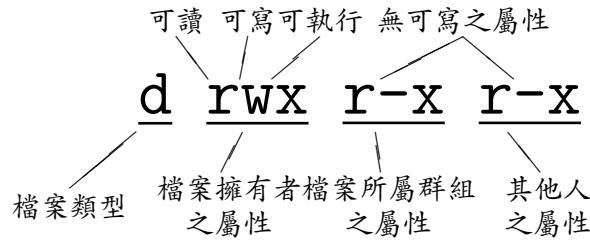
說明：

(a) total 72：檔案共 72 Blocks。

(b) 各欄位說明：

欄位一	欄位二	欄位三	欄位四	欄位五	欄位六	欄位七
drwxr-xr-x	3	root	root	4096	Sep 16 11:11	boot
檔案屬性	硬連結數目	擁有者	所有者群組	大小	建檔日期	檔名

i. 第一欄位 drwxr-xr-x，共有檔案的 10 個屬性：



4.2 改變檔案權限

1. chmod：改變權限。

	chmod [-R] xyz 檔案或目錄
2	chmod [-R] u = r 檔案或目錄
	g + w 檔案或目錄
4	o - x 檔案或目錄
	a 檔案或目錄
6	chmod u=rwx,go=rx 檔案或目錄
	chmod a-x 檔案或目錄

(a) xyz 為三組 rwx 屬性數值之加總。

r : 4
w : 2
x : 1

(b) -rwxr-xr-- 之屬性數值為 754。

(c) 符號類型

u : user
g : group
o : other
a : all
+ : 加入
- : 除去
= : 設定

4.3 可執行檔

1. 可執行檔放置目錄，使用文字界面執行檔案時，直接輸入指令名稱就可執行，完全不必輸入絕對路徑或相對路徑指明執行檔所在位置，是因為環境變數 PATH 設定好執行檔可能的所在位置，系統會自動在這些目錄中搜尋。

1	[root@dywOffice ~]# echo \$PATH
	/sbin:/usr/sbin:/bin:/usr/bin:/usr/X11R6/bin:/usr/local/bin:/usr/local/sbin
3	[root@dywOffice ~]# echo \${PATH}

```
/sbin:/usr/sbin:/bin:/usr/bin:/usr/X11R6/bin:/usr/local/bin:/usr/local/sbin
```

2. 例如：建立一個內容為 “ls -l /home”的檔案試著執行，發現無權限。因為自行建立的檔案在家目錄，系統並不會自動搜尋，所以執行時使用 ./ 指定是目前所在位置。另外，用戶可不可執行某一檔案，取決於其對於該檔案是否有「x」權限，所以以下例子無權限執行。

```
1 [root@kvm5 ~]# echo 'ls -l /home' > test.sh
2 [root@kvm5 ~]# ./test.sh
-bash: ./test.sh: Permission denied
```

3. 變更檔案屬性，讓其可執行。

```
1 [root@kvm5 ~]# chmod a+x test.sh
2 [root@kvm5 ~]# ll test.sh
3 -rwxr-xr-x. 1 root root 12 Aug 4 12:05 test.sh
4 [root@kvm5 ~]# ./test.sh
5 total 19
6 drwx----- 2 deyu1 deyu1 1024 Aug 4 10:08 deyu1
7 drwx----- 2 deyu2 deyu2 1024 Aug 4 10:08 deyu2
8 drwx----- 2 deyu3 deyu3 1024 Aug 4 10:08 deyu3
9 drwx----- 2 root root 12288 Aug 3 15:53 lost+found
```

4. 因 test.sh 在 root 的家目錄，其他用戶如 deyu1 不能執行。

```
1 [root@kvm5 ~]# pwd
2 /root
3 [root@kvm5 ~]# cat /root/test.sh
4 ls -l /home
5 [root@kvm5 ~]# su - deyu1
6 [deyu1@kvm5 ~]$ ./root/test.sh
7 -bash: /root/test.sh: Permission denied
8 [deyu1@kvm5 ~]$ exit
9 logout
```

5. 若要讓所有用戶都可執行 test.sh，必須將其移至環境變數 PATH 中，一般用戶可以存取的目錄。

```
1 [root@kvm5 ~]# mv test.sh /usr/bin/
2 [root@kvm5 ~]# test.sh
3 total 19
4 drwx----- 2 deyu1 deyu1 1024 Aug 4 12:17 deyu1
5 drwx----- 2 deyu2 deyu2 1024 Aug 4 10:08 deyu2
6 drwx----- 2 deyu3 deyu3 1024 Aug 4 10:08 deyu3
```

```

7 drwx-----. 2 root  root  12288 Aug  3 15:53 lost+found
[root@kvm5 ~]# su - deyu1
9 Last login: Tue Aug  4 12:16:56 CST 2015 on pts/1
[deyu1@kvm5 ~]$ test.sh
11 total 19
drwx-----. 2 deyu1 deyu1  1024 Aug  4 12:17 deyu1
13 drwx-----. 2 deyu2 deyu2  1024 Aug  4 10:08 deyu2
drwx-----. 2 deyu3 deyu3  1024 Aug  4 10:08 deyu3
15 drwx-----. 2 root  root  12288 Aug  3 15:53 lost+found

```

4.4 可執行檔別名

- 如果執行檔已存在，只是執行時要加太長的參數很不方便，也可在用戶登入時必須讀取的設定檔 /etc/bashrc 中加入別名。alias 設定在 /etc/bashrc 或 /etc/profile 兩個檔案 ssh 登入都會生效，但圖形界面開啓 gnome-terminal 不會讀取 /etc/profile，所以不建議放在 /etc/profile。

```

1 [root@kvm5 ~]# vim /etc/bashrc
[root@kvm5 ~]# tail -1 /etc/bashrc
3 alias qstat='/bin/ps -Ao pid,tt,user, fname,rsz'

```

- 重新讀取 /etc/bashrc，別名 qstat 已生效。

```

1 [root@kvm5 ~]# source /etc/bashrc
[root@kvm5 ~]# alias
3 alias cp='cp -i'
alias egrep='egrep --color=auto'
alias fgrep='fgrep --color=auto'
alias grep='grep --color=auto'
alias l.='ls -d .* --color=auto'
alias ll='ls -l --color=auto'
alias ls='ls --color=auto'
alias mv='mv -i'
11 alias qstat='/bin/ps -Ao pid,tt,user, fname,rsz'
alias rm='rm -i'
13 alias which='alias | /usr/bin/which --tty-only --read-alias --show-dot
--show-tilde'

```

- 查看時過濾 qstat 更清楚。

```

1 [root@kvm5 ~]# alias | grep qstat
alias qstat='/bin/ps -Ao pid,tt,user, fname,rsz'

```

- 直接執行看看。

```
[root@kvm5 ~]# qstat
2   PID TT      USER      COMMAND      RSZ
    1 ?      root      systemd      7452
4   2 ?      root      kthreadd      0
    3 ?      root      ksoftirq      0
6   5 ?      root      kworker/      0
    6 ?      root      kworker/      0
8   7 ?      root      migratio      0
    8 ?      root      rcu_bh       0
10  9 ?      root      rcuob/0      0
12 ..... 
12944 pts/0      root      ps          1276
```

5. 切換一般用戶 deyu1，一樣可以執行 qstat，出現的結果不會一樣。

```
[root@kvm5 ~]# su - deyu1
2 Last login: Sun Aug  9 07:42:07 CST 2015 on pts/0
[deyu1@kvm5 ~]$ qstat
4   PID TT      USER      COMMAND      RSZ
    1 ?      root      systemd      7452
6   2 ?      root      kthreadd      0
    3 ?      root      ksoftirq      0
8   5 ?      root      kworker/      0
    6 ?      root      kworker/      0
10  7 ?      root      migratio      0
    8 ?      root      rcu_bh       0
12  9 ?      root      rcuob/0      0
14 ..... 
12973 pts/0      deyu1      ps          1280
```

6. 退出 deyu1。

```
[deyu1@kvm5 ~]$ exit
2 logout
```


Chapter 5

Link Aggregation 網路聚合

5.1 前言

1. 網路聚合 Link Aggregation 是基於 IEEE 標準規格 802.3ad 協定。
2. 802.3ad 協定規範交換器（Switch）上許多不同的實體連接埠，可以邏輯性的共同結合在一起，進而視為一條實體線。
3. 網路聚合實現出/入流量吞吐量在各成員埠中的負荷分擔，交換機根據用戶配置的埠負荷分擔策略決定封包從哪一個成員埠發送到對端的交換機。
4. 當交換機檢測到其中一個成員埠的鏈路發生故障時，就停止在此埠上發送封包，並根據負荷分擔策略在剩下鏈路中重新計算封包發送的埠，故障埠恢復後再次重新計算封包發送埠。

5.2 建立網路聚合

1. 多個網路連接埠整合成一個虛擬網路卡可增加原本單埠時的速度，使用 nmcli 語法：

```
#nmcli con add type team con-name CNAME ifname INAME [config JSON]
```

2. JSON (JavaScript Object Notation) 指定使用 runner，語法為：

```
1  '{"runner": {"name": "METHOD"} }'
```

3. METHOD 在 RHEL7/CentOS7 中支援的 Teaming 模式有 broadcast, active-backup, round robin, loadbalance 與 lacp 五種，細節可以參考 teamd.conf 手冊。

```
1  [root@kvm7 ~]# man 5 teamd.conf
```

4. 產生 team 介面卡之前，先查看目前主機有 eth0 eth1 eth2 三張網卡。

```

1 [root@kvm5 ~]# nmcli device
2   DEVICE  TYPE      STATE      CONNECTION
3   eth0    ethernet  connected  eth0
4   eth1    ethernet  disconnected
5   eth2    ethernet  disconnected
6   lo     loopback  unmanaged
7

```

5. 使用 activebackup 模式產生一個名為 team0 的網路 team 介面。

```

1 [root@kvm5 ~]# nmcli connection add type team con-name team0 ifname
2   team0 \
3 config '{"runner": {"name": "activebackup"}}'
4 Connection 'team0' (e1d07964-d037-4d1d-ae23-4a6d6430d82d) successfully
5 added.

```

6. 查看 device 或 connection，多了 team0 的網路 team 介面，其網路連線設定名稱也是 team0。

```

1 [root@kvm5 ~]# nmcli device
2   DEVICE  TYPE      STATE      CONNECTION
3   eth0    ethernet  connected  eth0
4   team0   team      connecting (getting IP configuration)  team0
5   eth1    ethernet  disconnected
6   eth2    ethernet  disconnected
7   lo     loopback  unmanaged
8
9 [root@kvm5 ~]# nmcli connection
10  NAME      UUID           TYPE      DEVICE
11  team0    e1d07964-d037-4d1d-ae23-4a6d6430d82d  team      team0
12  eth0    657b29a2-b7c0-4176-a955-b12aadf9c156  802-3-ethernet  eth0

```

7. 指定 eth1 及 eth2 為 team0 的網路埠。

```

1 [root@kvm5 ~]# nmcli connection add type team-slave con-name \
2   team0-port1 ifname eth1 master team0
3 Connection 'team0-port1' (e150c255-b7a2-47d8-977d-e1f429249aaaf)
4 successfully added.
5 [root@kvm5 ~]# nmcli connection add type team-slave con-name \
6   team0-port2 ifname eth2 master team0
7 Connection 'team0-port2' (ebb32a20-01d3-4a36-8501-8fd02c5e9b20)
8 successfully added.

```

8. 重啓網路。

```
[root@kvm5 ~]# systemctl restart network.service
```

9. 查看 team0 是不是包含 eth1 及 eth2 兩個成員埠。

```
1 [root@kvm5 ~]# teamdctl team0 state
  setup:
  3   runner: activebackup
  ports:
  5     eth1
    link watches:
  7       link summary: up
      instance[link_watch_0]:
  9         name: ethtool
        link: up
  11    eth2
      link watches:
  13       link summary: up
      instance[link_watch_0]:
  15         name: ethtool
        link: up
  17  runner:
      active port: eth1
```

10. 設定 team0 繫定的 ip 192.168.122.15, netmask 255.255.255.0。因為要自行設定 IP, NETMASK 等參數，所以設定 team0 ipv4.method 為 manual，也就是手動，而不是 auto。

```
1 [root@kvm5 ~]# nmcli connection modify team0 \
  2   ipv4.addresses 192.168.122.15/24 ipv4.method manual
```

11. 啓動 team0。

```
1 [root@kvm5 ~]# nmcli connection up team0
  2 Connection successfully activated (D-Bus active path:
 /org/freedesktop/NetworkManager/ActiveConnection/119)
```

12. 查看 team0 的 IP 為 192.168.122.15。

```

1 [root@kvm5 ~]# ifconfig team0
team0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
3      inet 192.168.122.15 netmask 255.255.255.0 broadcast
           192.168.122.255
5      inet6 fe80::52:54ff:fe00:51 prefixlen 64 scopeid 0x20<link>
ether 52:54:00:00:00:51 txqueuelen 0 (Ethernet)
RX packets 21 bytes 798 (798.0 B)
RX errors 0 dropped 54 overruns 0 frame 0
TX packets 33 bytes 5408 (5.2 KiB)
9      TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```

5.3 測試網路聚合

- 先查看 team0 兩張成員埠都正常運作。

```

1 [root@kvm5 ~]# teamdctl team0 state
setup:
3   runner: activebackup
ports:
5     eth1
       link watches:
7         link summary: up
9         instance[link_watch_0]:
           name: ethtool
           link: up
11    eth2
       link watches:
13         link summary: up
15         instance[link_watch_0]:
           name: ethtool
           link: up
17 runner:
      active port: eth1

```

- 經由 team0 成功 ping 192.168.122.1，team0 啓動可能會 delay，等一下再 ping 看看。

```

2 [root@kvm5 ~]# ping -c4 -I team0 192.168.122.1
PING 192.168.122.1 (192.168.122.1) from 192.168.122.15 team0: 56(84)
     bytes of data.

4 --- 192.168.122.1 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3060ms
6

```

```

8  PING 192.168.122.1 (192.168.122.1) from 192.168.122.15 team0: 56(84)
    bytes of data.
9    64 bytes from 192.168.122.1: icmp_seq=1 ttl=64 time=0.584 ms
10   64 bytes from 192.168.122.1: icmp_seq=2 ttl=64 time=0.340 ms
11   64 bytes from 192.168.122.1: icmp_seq=3 ttl=64 time=0.308 ms
12   64 bytes from 192.168.122.1: icmp_seq=4 ttl=64 time=0.278 ms
13
14 --- 192.168.122.1 ping statistics ---
15   4 packets transmitted, 4 received, 0% packet loss, time 3013ms
16   rtt min/avg/max/mdev = 0.278/0.377/0.584/0.122 ms

```

3. 關閉 team0 的成員埠 team0-port1。

```

1 [root@kvm5 ~]# nmcli connection down team0-port1
2 Connection 'team0-port1' successfully deactivated (D-Bus active
  path: /org/freedesktop/NetworkManager/ActiveConnection/128)

```

4. 查看 team0 只有成員埠 eth2，也就是 team0-port2 正常運作。

```

1 [root@kvm5 ~]# teamdctl team0 state
2   setup:
3     runner: activebackup
4   ports:
5     eth2
6       link watches:
7         link summary: up
8         instance[link_watch_0]:
9           name: ethtool
10          link: up
11 runner:
12   active port: eth2

```

5. 只有成員埠 team0-port2 正常運作，還是可以經由 team0 (192.168.122.15) 成功 ping 192.168.122.1。

```

1 [root@kvm5 ~]# ping -I team0 192.168.122.1
2 PING 192.168.122.1 (192.168.122.1) from 192.168.122.15 team0: 56(84)
    bytes of data.
3   64 bytes from 192.168.122.1: icmp_seq=15 ttl=64 time=0.619 ms
4   64 bytes from 192.168.122.1: icmp_seq=16 ttl=64 time=0.265 ms
5   64 bytes from 192.168.122.1: icmp_seq=17 ttl=64 time=0.324 ms
6   ~C
7   --- 192.168.122.1 ping statistics ---
8   17 packets transmitted, 3 received, 82% packet loss, time 16416ms

```

```
rtt min/avg/max/mdev = 0.265/0.402/0.619/0.156 ms
```

6. 再啓動 team0 的成員埠 team0-port1。

```
1 [root@kvm5 ~]# nmcli connection up team0-port1
2 Connection successfully activated (D-Bus active path:
3 /org/freedesktop/NetworkManager/ActiveConnection/130)
```

7. 查看 team0 兩張成員埠都正常運作。

```
1 [root@kvm5 ~]# teamdctl team0 state
2 setup:
3   runner: activebackup
4   ports:
5     eth1
6       link watches:
7         link summary: up
8         instance[link_watch_0]:
9           name: ethtool
10          link: up
11     eth2
12       link watches:
13         link summary: up
14         instance[link_watch_0]:
15           name: ethtool
16           link: up
17 runner:
18   active port: eth2
```

Chapter 6

IPv6 網路

6.1 前言

1. IPv6 主要是作為取代 IPv4 網絡協議，以解決 IPv4 位址即將枯竭的問題。
2. IPv6 還提供了許多增強功能和網絡配置管理，支持未來協議的變更新的功能。
3. IPv6 尚未廣泛部署的關鍵在於核心協議不具有，分別僅具 IPv6 及 IPv4 位址系統間通信的簡單方法。
4. 目前最好的過渡計劃是同時提供所有主機 IPv4 和 IPv6 位址，只使用協議之一就可以與主機連線，這就是所謂的雙協議 (dual-stack) 的配置。
5. 有一些允許僅有 IPv6 的主機使用的 IPv4 網路或支援其他形式的 IPv4/IPv6 轉換，例如 NAT64 (RFC 6145) 和 464XLAT (RFC 6877)。

6.2 IPv6 位址

1. IPv6 位址是 128 位數的數字，通常以四個十六進制字元為一組共八組，每組間以冒號分隔來表示。一個十六進制字元以四個位元 (nibbles, half-bytes, 半位元組)，每組共 16 位元，八組則共 128 位元，表示如下：

2001 : 0db8 : 0000 : 0010 : 0000 : 0000 : 0000 : 0001

2. 為了更容易編寫 IPv6 位址，每組的前導零不需要被寫入，但每組至少要有一個半位元組。

2001 : DB8 : 0 : 10 : 0 : 0 : 0 : 1

3. 位址常會是一長串的零，一個或多個組連續為零，可以 :: 表示。

2001 : DB8 : 0 : 10 :: 1

4. 2001 : DB8 :: 0010 : 0 : 0 : 0 : 1 不是一個合適的 IPv6 編寫方式，應以下列規則來編寫：

- (a) 每組的前導零都要省略不寫。
- (b) 盡可能使用 :: 縮短位址，但只能使用一次，如果兩個連續零的長度相等，以縮短左邊的零優先。
- (c) 雖然允許 :: 來縮短單獨的零，但建議還是使用 :0: 來表示， :: 則用來表示連續零。

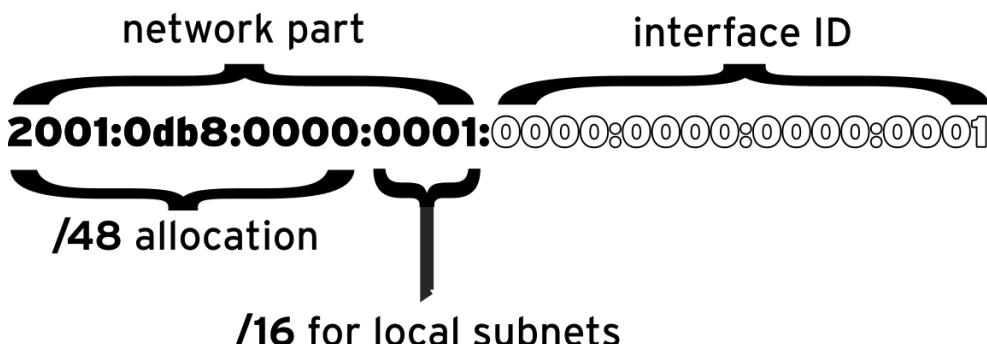
- (d) 十六進制數 a 到 f 都以小寫編寫。
5. 當 IPV6 位址後接 tcp 或 udp port 時，為了方便識別，位址一定要以中括號括起來。
[2001:db8:0:10::1]:80

6.3 IPv6 子網

1. 一個正常的單播位址被分成兩個部分：網路前綴 (network prefix) 及介面 ID (interface ID)。
2. 網路前綴標示子網，在同一子網中沒有任何兩個相同介面 ID，介面 ID 標識子網中的一個特定的介面，例如主機。
3. 不同於 IPv4，IPv6 有一個標準的子網掩罩 /64，也就是一半的位址是網路前綴，一半是介面 ID。這個子網可以有 2^{64} 主機。
4. 網路提供者如果分配給一個單位較短的網路，例如 /48，這個單位可以有 16 位元用於子網，高達 $2^{16} = 65536$ 個子網。

IPv6 address is 2001:db8:0:1::1/64

Allocation from provider is 2001:db8::/48



6.4 IPv6 設定

1. 先查看目前 kvm5.deyu.wang 有 eth0, eth1, eth2 三張網卡。

```
[root@kvm5 ~]# ip link
2 1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode
    DEFAULT
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
4 2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast
    state UP mode DEFAULT qlen 1000
    link/ether 52:54:00:4a:c9:67 brd ff:ff:ff:ff:ff:ff
6 3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast
    state UP mode DEFAULT qlen 1000
    link/ether 52:54:00:00:00:51 brd ff:ff:ff:ff:ff:ff
8 4: eth2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast
    state UP mode DEFAULT qlen 1000
```

```
link/ether 52:54:00:00:00:52 brd ff:ff:ff:ff:ff:ff
```

2. 查看目前只有 eth0 一個網路連線。

```
1 [root@kvm5 ~]# nmcli connection show
  NAME      UUID                                  TYPE      DEVICE
3  eth0     166b5ab1-1581-402d-b821-8823acb33dee  802-3-ethernet  eth0
```

3. 查看目前 eth0 沒有 ipv6 位址。

```
1 [root@kvm5 ~]# nmcli connection show eth0 | grep ipv6
  ipv6.method:                      auto
3  ipv6.dns:
  ipv6.dns-search:
5  ipv6.addresses:
  ipv6.gateway:                     --
7  ipv6.routes:
  ipv6.route-metric:                -1
9  ipv6.ignore-auto-routes:         no
  ipv6.ignore-auto-dns:             no
11 ip6.never-default:               no
  ipv6.may-fail:                   yes
13 ip6.ip6-privacy:                -1 (unknown)
  ipv6.dhcp-send-hostname:          yes
15 ip6.dhcp-hostname:              --
```

4. 沒有指定那個連線設定 ipv6，則可以直接修改 eth0 網路連線，增加 ipv6 位址。

```
1 [root@kvm5 ~]# nmcli connection modify eth0 ipv6.addresses '2001:ac18
  ::135/64' ipv6.method manual
```

5. 重新啓動網路。

```
1 [root@kvm5 ~]# systemctl restart network.service
```

6. 網卡 eth0 已有 ipv6 的 ip。

```

1 [root@kvm5 ~]# ip addr show dev eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast
    state UP qlen 1000
    link/ether 52:54:00:4a:c9:67 brd ff:ff:ff:ff:ff:ff
    inet 192.168.122.5/24 brd 192.168.122.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 2001:ac18::135/64 scope global
        valid_lft forever preferred_lft forever
    inet6 fe80::5054:ff:fe4a:c967/64 scope link
        valid_lft forever preferred_lft forever

```

7. 使用 ping6 ping 自己。

```

1 [root@kvm5 ~]# ping6 -c3 2001:ac18::135
PING 2001:ac18::135(2001:ac18::135) 56 data bytes
3 64 bytes from 2001:ac18::135: icmp_seq=1 ttl=64 time=0.068 ms
5 64 bytes from 2001:ac18::135: icmp_seq=2 ttl=64 time=0.058 ms
7 64 bytes from 2001:ac18::135: icmp_seq=3 ttl=64 time=0.050 ms

--- 2001:ac18::135 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2000ms
9 rtt min/avg/max/mdev = 0.050/0.058/0.068/0.011 ms

```

6.5 IPv6 互 ping

1. kvm7 ping6 kvm5 已設定好的 ipv6 位址，回應 Network is unreachable，因為本身沒有 ipv6 的 ip。

```

1 [root@kvm7 ~]# ping6 '2001:ac18::135'
connect: Network is unreachable

```

2. 查看 kvm7 目前只有 eth0 連線。

NAME	UUID	TYPE	DEVICE
eth0	2b7d2642-13f3-48aa-a5e1-be77693ea318	802-3-ethernet	eth0

3. 查看 kvm7 網路連線 eth0 只有本機 ipv6 位址 fe80::5054:ff:feff:f82a，沒有設定網域 ipv6 位址。

```

1 [root@kvm7 ~]# nmcli connection show eth0 | egrep -i ipv?
2   ipv6.method:                         auto
3   ipv6.dns:
4   ipv6.dns-search:
5   ipv6.addresses:
6   ipv6.gateway:                      --
7   ipv6.routes:
8   ipv6.route-metric:                  -1
9   ipv6.ignore-auto-routes:            no
10  ipv6.ignore-auto-dns:              no
11  ipv6.never-default:                no
12  ipv6.may-fail:                     yes
13  ipv6.ip6-privacy:                 -1 (unknown)
14  ipv6.dhcp-send-hostname:           yes
15  ipv6.dhcp-hostname:               --
16  IP6.ADDRESS[1]:                  fe80::5054:ff:feff:f82a/64
17  IP6.GATEWAY:

```

4. kvm7 在 connection eth0 上增加 ipv6 位址 2001:ac18::137/64。

```

1 [root@kvm7 ~]# nmcli connection modify eth0 ipv6.addresses '2001:ac18
2   ::137/64' ipv6.method manual

```

5. 查看 kvm7 網路連線 eth0 已加入 ipv6 位址 2001:ac18::137/64。

```

1 [root@kvm7 ~]# nmcli connection show eth0 | egrep -i ipv?
2   ipv6.method:                         manual
3   ipv6.dns:
4   ipv6.dns-search:
5   ipv6.addresses:                     2001:ac18::137/64
6   ipv6.gateway:                      --
7   ipv6.routes:
8   ipv6.route-metric:                  -1
9   ipv6.ignore-auto-routes:            no
10  ipv6.ignore-auto-dns:              no
11  ipv6.never-default:                no
12  ipv6.may-fail:                     yes
13  ipv6.ip6-privacy:                 -1 (unknown)
14  ipv6.dhcp-send-hostname:           yes
15  ipv6.dhcp-hostname:               --
16  IP6.ADDRESS[1]:                  fe80::5054:ff:feff:f82a/64
17  IP6.GATEWAY:

```

6. kvm7 重新啓動網路。

```
1 [root@kvm7 ~]# systemctl restart network.service
```

7. kvm7 成功 ping6 kvm5 2001:ac18::135。

```
1 [root@kvm7 ~]# ping6 -c2 2001:ac18::135
connect: Network is unreachable
3 [root@kvm7 ~]# systemctl restart network.service
[root@kvm7 ~]# ping6 -c2 2001:ac18::135
5 PING 2001:ac18::135(2001:ac18::135) 56 data bytes
64 bytes from 2001:ac18::135: icmp_seq=1 ttl=64 time=1.10 ms
7 64 bytes from 2001:ac18::135: icmp_seq=2 ttl=64 time=0.345 ms
```

8. kvm5 也成功 ping6 kvm7 2001:ac18::137。

```
1 [root@kvm5 ~]# ping6 -c2 2001:ac18::137
PING 2001:ac18::137(2001:ac18::137) 56 data bytes
3 64 bytes from 2001:ac18::137: icmp_seq=1 ttl=64 time=0.362 ms
64 bytes from 2001:ac18::137: icmp_seq=2 ttl=64 time=0.293 ms
5
--- 2001:ac18::137 ping statistics ---
7 2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 0.293/0.327/0.362/0.038 ms
```

9. 如果無法成功 ping6 kvm5 2001:ac18::135，請以 root 權限在 deyu.wang(192.168.122.1) 主機增加 ip6 防火牆的 FORWARD。

```
[root@dywnb ~]# ip6tables -I FORWARD -i virbr0 -o virbr0 -j ACCEPT
```

10. 考試時 kvm5 及 kvm7 都有指定 ipv6 位址，請依題意要求設定，題目要求在那張網卡設定 ipv6 必須看清楚，若有指定 ipv6 gateway 則一併設定。

Chapter 7

Email Transmission

7.1 簡介

1. 現今的企業環境中，電子郵件是通信的常用方法。用戶端可以使用如 mutt 或 Web 界面的電子郵件服務。
2. Linux 系統都會監控事故並自動發送錯誤報告給管理者，發送方式通常藉設定由 Postfix 提供的 /usr/sbin/sendmail 透過 SMTP 伺服器來傳送電子郵件。
3. Null client 是本地端的郵件伺服器，負責轉發所有電子郵件到出站郵件中繼機。Null client 不接受本地傳遞的任何郵件，只能將它們發送到出站郵件中繼機。當然用戶還是可以在 Null client 上使用電子郵件客戶端服務閱讀和發送電子郵件。
4. 郵件客戶端通常使用簡單郵件傳輸協議 (SMTP) 的郵件服務器發送郵件到郵件中繼機 (relay)。
5. 中繼機可能需要使用 25/tcp port 接受來自不需要身份驗證的內部客戶端之郵件，在這種情況下，中繼機可以通過限制 IP 位址或防火牆規則來限制轉發郵件。
6. 由於安全和防垃圾郵件的原因，出站 SMTP 中繼機通常以 587/tcp port 來建置一個郵件提交代理 (mail submission agent, MSA)。用戶要經由此中繼機轉發郵件，必須輸入帳號及密碼進行認證。
7. 中繼機使用 DNS 來查郵件傳送目的端，有 MX 標識的郵件伺服器，再使用 SMTP 25/TCP port 將電子郵件發送到該伺服器。例如：寄到 dywang@csie.cyut.edu.tw 的郵件，中繼機會先查 csie.cyut.edu.tw 這個網域的 DNS 中有標識 MX 的主機，也就是可以接受郵件的主機，如果查到是 mail.csie.cyut.edu.tw，則將郵件傳送到這台主機。
8. 收件人的郵件服務可以使用 POP3 或 IMAP，例如 Dovecot 或 Cyrus，來允許客戶收郵件。現在郵件服務大都提供客戶端使用網絡瀏覽器作為郵件客戶端。

7.2 *Postfix 架設

1. 本節不是授課範圍，但為了驗證 NULL Client 確實轉信，必須架設收信 server。
2. 安裝 postfix 套件

```
1 [root@dywssd ~]# yum install postfix ## 預設應已安裝
```

3. 設定接受郵件的來源為所有

```
1 [root@dywssd ~]# postconf -e "inet_interfaces=all"
```

4. 設定郵件伺服器主機名稱

```
1 [root@dywssd ~]# postconf -e "myhostname=server.deyu.wang"
```

5. 設定網域

```
1 [root@dywssd ~]# postconf -e "mydomain=deyu.wang"
```

6. 設定可以連接郵件伺服器的網路或主機

```
1 [root@dywssd ~]# postconf -e "mynetworks=192.168.122.0/24"
```

7. 設定郵件傳送目的地，雖然預設值包含 myhostname 本機名稱，若不重設定測試時發現郵件無法到達用戶端，在 root 信箱中出現無法送達的郵件。觀察經由 postconf 設定的主機名稱會在 /etc/postfix/main.cf 檔案最後，如果移至 mydestination=\$myhostname ... 前再重新啟動 postfix 就可以。

```
1 [root@dywssd ~]# postconf -e "mydestination=\$myhostname"
```

8. 設定虛擬網域別名，讓 deyu.wang 上的郵件伺服器可以收 kvm5.deyu.wang 及 kvm7.deyu.wang 郵件，別名檔在 /etc/postfix/virtual_kvm。

```
1 [root@dywssd ~]# postconf -e "virtual_alias_maps=hash:/etc/postfix/virtual_kvm"
```

9. 設定送到 kvm5.deyu.wang 及 kvm7.deyu.wang 的信都轉送到本機的 dywang。

```
1 [root@dywssd ~]# echo '@kvm5.deyu.wang dywang' > /etc/postfix/virtual_kvm  
[root@dywssd ~]# echo '@kvm7.deyu.wang dywang' >> /etc/postfix/virtual_kvm
```

```
3 [root@dywssd ~]# cat /etc/postfix/virtual_kvm
@kvm5.deyu.wang dywang
5 @kvm7.deyu.wang dywang
```

10. 重新產生及查詢虛擬網域對照表

```
1 [root@dywssd ~]# postmap /etc/postfix/virtual_kvm
```

11. 重新啓動 postfix

```
1 [root@dywssd ~]# /etc/init.d/postfix restart
```

7.3 *Dovecot 架設

1. 本節不是授課範圍，但為了如果要在 kvm5 讀取 mail server 是否收到 NULL Client 轉信，必須架設 dovecot。

2. 安裝 dovecot 套件

```
1 [root@dywssd ~]# yum install dovecot -y
```

3. 編輯設定檔，選擇使用的協定。

```
1 [root@dywssd ~]# sed -i 's/#*\(\protocols =\)/\1/' /etc/dovecot/dovecot.conf
2
3 [root@dywssd ~]# grep protocols /etc/dovecot/dovecot.conf
3 protocols = imap pop3 lmtp
```

4. 編輯郵件設定檔：設定郵件位置。

```
1 [root@dywssd ~]# vim /etc/dovecot/conf.d/10-mail.conf
2 [root@dywssd ~]# grep 'mail_location' /etc/dovecot/conf.d/10-mail.conf |
3 grep -v '#'
3 mail_location = mbox:~/Mail:INBOX=/var/mail/%u
```

5. 用戶第一次使用，dovecot 會在 INBOX 位置產生一個用戶郵件檔，若沒設定 mail 權限群組，系統記錄檔會出現錯誤訊息 euid is not dir owner dovecot，表示該用戶沒有權限寫入。編輯郵件設定檔：設定郵件位置寫入權限。

```

1 [root@dywssd ~]# ll -d /var/spool/mail
drwxrwsr-x. 5 root mail 32768 Aug  7 10:03 /var/spool/mail
3
5 [root@dywssd ~]# vim /etc/dovecot/conf.d/10-mail.conf
[root@dywssd ~]# grep 'mail_privileged_group' /etc/dovecot/conf.d/10-
      mail.conf | grep -v '#'
mail_privileged_group = mail

```

6. 啓動 dovecot 服務

```
[root@dywssd ~]# /etc/init.d/dovecot restart
```

7. 設定開機啓動 dovecot 服務

```
1 [root@dywssd ~]# chkconfig dovecot on
```

7.4 Null Client 建置

- Postfix 是一個功能強大且易於建置的郵件服務，RHEL/CentOS 7 預設已安裝。其主要設定檔為 /etc/postfix/main.cf，可以直接使用 vim 進行，Postfix 也提供 postconf 命令可以進行參數設定。SMTP 與 Null client 參數比較如下表：

參數設定	SMTP Server	Null Client
inet_interface =	all	loopback-only
myhostname =	kvm5.deyu.wang	kvm5.deyu.wang
mydomain =	deyu.wang	deyu.wang
myorigin =	\$mydomain	\$mydomain
mydestination =	\$mydomain, deyu.wang	127.0.0.0/8, [:1]/128
mynetworks =	192.168.122.0/24,2001:ac18::135/64,127.0.0.0/8, [:1]/128	127.0.0.0/8, [:1]/128
mynetworks_style =	subnet	不設，請註解掉。
local_transport =	不設，請註解掉。	Error:local
relayhost =	如果 server 可直接送信就不設，請註解掉。	deyu.wang

- Null client 必須設定參數整理如下表：

參數	Null Client (kvm5.deyu.wang)
inet_interfaces	inet_interfaces = loopback-only
myorigin	myorigin = deyu.wang
relayhost	relayhost = [server.deyu.wang]
mydestination	mydestination =
local_transport	local_transport = error: local delivery disabled
mynetworks	mynetworks = 127.0.0.0/8, [:1]/128

3. 設定文件參考，例如查 my 後有等號 “=” 的內容如下：

```

1 [root@kvm5 ~]# grep 'my.*=' /usr/share/doc/postfix-2.10.1/README_FILES/
  STANDARD_CONFIGURATION_README
  #myorigin = $mydomain
3   mynetworks_style = host
  # mynetworks = 192.168.1.0/28
5   myhostname = hostname.example.com
3   myorigin = $mydomain
7   mydestination =
  mydomain parameter (here, "mydomain = example.com").
2   myorigin = $mydomain
3   mynetworks = 127.0.0.0/8 10.0.0.0/24
11  5   myorigin = $mydomain
6   mydestination = $myhostname localhost.$mydomain localhost
$mydomain
13  7   mynetworks = 127.0.0.0/8 10.0.0.0/24
2   myorigin = example.com
15  3   mydestination =
2   mynetworks = 127.0.0.0/8 12.34.56.0/24
17  2   myhostname = hostname.locaLdomain
3   mydomain = localdomain

```

4. 設定只監聽傳到本機的郵件。

```
[root@kvm5 ~]# postconf -e "inet_interfaces=loopback-only"
```

5. 因本機 mail server 為 null client 不接受任何郵件，只負責轉送，必須設定為 mydestination 為空。

```
1 [root@kvm5 ~]# postconf -e "mydestination=""
```

6. 設定 relayhost 指定轉發的主機為同網域中 DNS 設有 MX 標識的 server.deyu.wang。注意主機必須以中括號括起來。

```
1 [root@kvm5 ~]# postconf -e "relayhost=[server.deyu.wang]"
```

7. 關閉本機的郵件傳遞，所有郵件都轉到 relayhost 指定的主機，冒號後的字串 “local delivery disabled” 為自行設定的字串。

```
1 [root@kvm5 ~]# postconf -e "local_transport=error: local delivery
disabled"
```

8. 設定所有從本機送出的郵件，發信來源網域都改寫成 deyu.wang。

```
1 [root@kvm5 ~]# postconf -e "myorigin=deyu.wang"
```

9. 設定只轉發來自本機的郵件，包含 IPV4 及 IPV6 兩個位址。

```
1 [root@kvm5 ~]# postconf -e "mynetworks=127.0.0.0/8 [::1]/128"
```

10. 重新啓動 postfix。

```
1 [root@kvm5 ~]# systemctl restart postfix
```

11. 從本機寄信給本機 kvm5.deyu.wang 上的用戶 deyu2。

```
1 [root@kvm5 ~]# date | mail -s "kvm5 null client" deyu2@kvm5.deyu.wang
```

12. server.deyu.wang 設定收到來自 kvm5.deyu.wang 的郵件，都送到 server.deyu.wang。由於已經在 server.deyu.wang 設定可以接受 kvm5.deyu.wang 郵件，且都轉送到 dywang。

13. 使用 mutt 讀取 dywang@server.deyu.wang 的信件，按下 a 接受或 o 一次、輸入 dywang 的密碼就可以進入信箱，選取要讀的郵件可以看到送到 deyu2@kvm5.deyu.wang 的信，注意其信件來源被改寫為 root@deyu.wang。

```
1 [root@kvm5 ~]# mutt -f imaps://dywang@server.deyu.wang
2
3 q:Quit d:Del u:Undel s:Save m:Mail r:Reply g:Group ?:Help
4   1 Sep 21 root          ( 1) kvm5 null client
5
6 -*-Mutt: imaps://dywang@server.deyu.wang/INBOX [Msgs:1 0.5K]---(date/
7   date)-(all)
8
9 i:Exit -:PrevPg <Space>:NextPg v:View Attachm. d:Del r:Reply j:Next
10   ?:Help
11 Date: Mon, 21 Sep 2015 12:38:33 +0800
12 From: root <root@deyu.wang>
13 To: deyu2@kvm5.deyu.wang
14 Subject: kvm5 null client
15 User-Agent: Heirloom mailx 12.5 7/5/10
16
17 Mon Sep 21 12:38:33 CST 2015
```

```
19 || -N - 1/1: root          kvm5 null client  
-- (all)
```

14. 本系統將 NULL Client 轉送到 server.deyu.wang 的信都轉至 dywang@server.deyu.wang 的信件，所以用戶 dywang 在 server.deyu.wang 可以簡單使用指令 mail 讀信。

```
1 [dywang@dywssd ~]$ mail  
Heirloom Mail version 12.4 7/29/08. Type ? for help.  
3 "/var/spool/mail/dywang": 7 messages  
> 1 root           Mon Sep 21 12:38 24/885  "kvm5 null client  
" 5 2 root           Sun Nov 29 13:41 24/866  "kvm5 null client  
" 3 3 root           Sun Nov 29 13:48 24/866  "kvm5 null client  
" 7 4 root           Sun Nov 29 13:52 24/862  "kvm5 null client  
" 5 5 root           Sun Nov 29 14:41 24/862  "kvm5 null client  
" 9 6 root           Sun Nov 29 14:44 23/851  "kvm5 null client  
" 7 7 root           Sun Dec 13 11:40 23/851  "kvm5 null client  
11 & quit  
Held 7 messages in /var/spool/mail/dywang
```


Chapter 8

SMB File Shares

8.1 SMB 簡介

1. Server Message Block (SMB) 是微軟 Windows 伺服器和客戶端標準的檔案共享協議。
2. SMB 檔案伺服器可以以多種不同的方式來建置，最簡單的是方式是建置檔案伺服器和客戶為 Windows 的工作群組成員。
3. 每個檔案伺服器獨立管理自己的本地用戶帳戶和密碼，更複雜的建置可以是 Windows 網域成員，再通過網域控制器用戶身份驗證。
4. SAMBA 是實現 Linux 與 Windows 中 SMB (Server Message Block) 協定連結的自由軟體。
5. 使用 Samba 套件就可以建置 SMB 檔案共享伺服器。
6. SAMBA 可以作到的功能，其中常見的有：
 - (a) 將目錄分享給 unix linux 或 windows。
 - (b) 共享印表機。
 - (c) 提供 windows 帳號認證。

8.2 SAMBA 架設

1. 安裝 samba 套件

```
[root@kvm5 ~]# yum -y install samba
```

2. 在 kvm5.deyu.wang 主機再新增一共享目錄 /groupdir。

```
1 [root@kvm5 ~]# mkdir /groupdir
```

3. ** 如果不知道 samba 相關的 fcontext type 可安裝 setools-console 套件，執行 seinfo 查詢。

(a) 查詢 seinfo 命令由哪個套件提供？

```
1 [root@kvm5 ~]# yum provides *bin/seinfo
...
3 Matched from:
Filename   : /usr/bin/seinfo
```

(b) seinfo 命令由 setools-console 提供，安裝此套件。

```
[root@kvm5 ~]# yum install setools-console
```

(c) 執行 seinfo -t 列出所有 selinux fcontext type，再以管線處理及 grep 過濾 samba 相關的 type。

```
1 [root@kvm5 ~]# seinfo -t | grep samba
2   samba_secrets_t
3   samba_spool_t
4   samba_unconfined_script_exec_t
5   samba_net_t
6   samba_var_t
7   samba_net_exec_t
8   samba_net_tmp_t
9   samba_unconfined_net_t
10  samba_unconfined_script_t
11  samba_unit_file_t
12  sambagui_exec_t
13  samba_share_t
14  samba_initrc_exec_t
15  sambagui_t
16  samba_etc_t
17  samba_log_t
```

4. 設定目錄 /groupdir 下的 selinux type 為 samba_share_t，不先查詢，使用 TAB 鍵一樣會出現提示及補齊。

```
1 [root@kvm5 ~]# semanage fcontext -a -t samba_share_t '/groupdir(/.*)?'
```

5. 還原目錄 /groupdir 下的 selinux type 為 samba_share_t。

```

1 [root@kvm5 ~]# restorecon -vvFR /groupdir
restorecon reset /groupdir context unconfined_u:object_r:default_t:s0->
    system_u:object_r:samba_share_t:s0

```

6. 編輯設定檔 /etc/samba/smb.conf，設定工作群組為 DEYUGROUP，建立分享目錄 /groupdir 的名稱為 common、可瀏覽、只允許 192.168.122.0/24 網域用戶存取、用戶 deyu1 可以使用 123qwe 密碼存取這個分享目錄。

```

2 [root@kvm5 ~]# vim /etc/samba/smb.conf
3 [root@kvm5 ~]# grep '^[^#\;]' /etc/samba/smb.conf
[global]
4   workgroup = DEYUGROUP
5   server string = Samba Server Version %v
6   # log files split per-machine:
7   log file = /var/log/samba/log.%m
8   # maximum size of 50KB per log file, then rotate:
9   max log size = 50
10  security = user
11  passdb backend = tdbsam
12  # the following login script name is determined by the machine name
13  # (%m):
14  # the following login script name is determined by the UNIX user
15    used:
16  # use an empty path to disable profile support:
17  # various scripts can be used on a domain controller or a stand-
18    alone
19  # machine to add or delete corresponding UNIX accounts:
20  load printers = yes
21  cups options = raw
22  # obtain a list of printers automatically on UNIX System V systems:
23  [homes]
24    comment = Home Directories
25    browseable = no
26    writable = yes
27  [printers]
28    comment = All Printers
29    path = /var/spool/samba
30    browseable = no
31    guest ok = no
32    writable = no
33    printable = yes
34  [common]
35    path = /groupdir
36    browseable = yes
#hosts allow = .deyu.wang deyu.wang
hosts allow = 192.168.122.

```

7. hosts allow 允許的存取如果要使用網域名稱 .deyu.wang，必須在 global section 加上 hostname lookups = yes 設定，才能從主機名稱反查到 IP，但目前有一

小問題是設定 `hosts allow = .deyu.wang` 允許 `deyu.wang` 網域的機器卻不包含 `deyu.wang` 本身，必須單獨再加入。

```
[root@kvm5 ~]# vim /etc/samba/smb.conf
2 [root@kvm5 ~]# grep '^\[global\]' -A2 /etc/samba/smb.conf
[global]
4
hostname lookups = yes
6
[root@kvm5 ~]# testparm
8 Load smb config files from /etc/samba/smb.conf
rlimit_max: increasing rlimit_max (1024) to minimum Windows limit
(16384)
10 Processing section "[homes]"
Processing section "[printers]"
12 Processing section "[common]"
Loaded services file OK.
14 Server role: ROLE_STANDALONE
Press enter to see a dump of your service definitions
16
[global]
18   workgroup = DEYUGROUP
   server string = Samba Server Version %v
20   log file = /var/log/samba/log.%m
   max log size = 50
22   hostname lookups = Yes
   idmap config * : backend = tdb
24   cups options = raw

26 [homes]
28   comment = Home Directories
29   read only = No
30   browseable = No

32 [printers]
33   comment = All Printers
34   path = /var/spool/samba
35   printable = Yes
36   print ok = Yes
37   browseable = No

38 [common]
39   path = /groupdir
40   hosts allow = .deyu.wang
```

8. 測試設定檔 `/etc/samba/smb.conf` 看是否有錯誤？

```
[root@kvm5 ~]# testparm
2 Load smb config files from /etc/samba/smb.conf
rlimit_max: increasing rlimit_max (1024) to minimum Windows limit
```

```

 4      (16384)
Processing section "[homes]"
Processing section "[printers]"
6 Processing section "[common]"
Loaded services file OK.
8 Server role: ROLE_STANDALONE
Press enter to see a dump of your service definitions
10
[global]
12   workgroup = DEYUGROUP
13   server string = Samba Server Version %v
14   log file = /var/log/samba/log.%m
15   max log size = 50
16   idmap config * : backend = tdb
17   cups options = raw
18
[homes]
20   comment = Home Directories
21   read only = No
22   browseable = No
23
[printers]
24   comment = All Printers
25   path = /var/spool/samba
26   printable = Yes
27   print ok = Yes
28   browseable = No
29
[common]
30   path = /groupdir
31   hosts allow = 192.168.122.

```

9. 要建立 smb 用戶必須先安裝 samba-client 套件。

```
1 [root@kvm5 ~]# yum -y install samba-client
```

10. 如果 deyu1 用戶不存在，則新增一個用戶 deyu1。

```
1 [root@kvm5 ~]# useradd deyu1
```

11. 新增 deyu1 為 samba 用戶。

```
1 [root@kvm5 ~]# smbpasswd -a deyu1
2 New SMB password:
3 Retype new SMB password:
```

1 | Added user deyu1.

12. 查看 samba 用戶。

2 | [root@kvm5 ~]# pdbedit -L
deyu1:1000:

13. 架設 Samba Server 需要設定開機啓動 smb 及 nmb 服務，其中「smb」是啓用 Samba Server 的服務，而「nmb」是在 Linux 系統上啓用 NetBIOS 協定。

2 | [root@kvm5 ~]# systemctl enable smb.service nmb.service
ln -s '/usr/lib/systemd/system/smb.service' '/etc/systemd/system/multi-user.target.wants/smb.service'
ln -s '/usr/lib/systemd/system/nmb.service' '/etc/systemd/system/multi-user.target.wants/nmb.service'

14. 現在啓動 smb 及 nmb 服務。

1 | [root@kvm5 ~]# systemctl start smb.service nmb.service

15. 查看 samba 相關的布林值。

1 | [root@kvm5 ~]# getsebool -a | grep samba
samba_create_home_dirs --> off
samba_domain_controller --> off
samba_enable_home_dirs --> off
samba_export_all_ro --> off
samba_export_all_rw --> off
samba_portmapper --> off
samba_run_unconfined --> off
samba_share_fusefs --> off
samba_share_nfs --> off
sanlock_use_samba --> off
use_samba_home_dirs --> off
virt_sandbox_use_samba --> off
virt_use_samba --> off

16. 開啓 selinux 的 samba_export_all_rw 布林值，允許 Samba 讀取及寫入，-P 選項設定不只現在開啓，開機時也開啓此布林值。

```
[root@kvm5 ~]# setsebool -P samba_export_all_rw on
```

17. 查詢 samba_export_all_rw 布林值已開啓。

```
1 [root@kvm5 ~]# getsebool samba_export_all_rw  
samba_export_all_rw --> on
```

8.3 建立多使用者 SMB 掛載目錄

1. 在 kvm5.deyu.wang 主機再新增一共享目錄 /data。

```
[root@kvm5 ~]# mkdir /data
```

2. 新增 samba 寫入目錄專屬群組 dywsmb。

```
1 [root@kvm5 ~]# groupadd dywsmb
```

3. 變更 /data 目錄的群組為 dywsmb。

```
1 [root@kvm5 ~]# chgrp dywsmb /data/
```

4. 變更 /data 目錄的權限屬性。

```
1 [root@kvm5 ~]# chmod 2775 /data/
```

5. 變更 /data 目錄 (含次目錄) 的預設 selinux 屬性 type 為 samba_share_t。

```
1 [root@kvm5 ~]# semanage fcontext -a -t samba_share_t '/data(/.*)?'
```

6. 更新 /data 目錄 (含次目錄) 的 selinux 屬性。

```

1 [root@kvm5 ~]# restorecon -vvFR /data
  restorecon reset /data context unconfined_u:object_r:default_t:s0->
    system_u:object_r:samba_share_t:s0
3 [root@kvm5 ~]# vim /etc/samba/smb.conf

```

7. 編輯 /etc/samba/smb.conf，允許瀏覽、dywsmb 群組成員可以寫入、只允許 deyu.wang 網段存取。

```

1 [root@kvm5 ~]# vim /etc/samba/smb.conf
[root@kvm5 ~]# tail -n6 /etc/samba/smb.conf
3 [data]
4   path = /data
5   browseable = yes
6   write list = @dywsmb
7   #hosts allow = .deyu.wang
  hosts allow = 192.168.122.

```

8. 測試 /etc/samba/smb.conf 參數。

```

1 [root@kvm5 ~]# testparm
2 Load smb config files from /etc/samba/smb.conf
3 rlimit_max: increasing rlimit_max (1024) to minimum Windows limit
  (16384)
4 Processing section "[homes]"
5 Processing section "[printers]"
6 Processing section "[common]"
7 Processing section "[data]"
8 Loaded services file OK.
9 Server role: ROLE_STANDALONE
10 Press enter to see a dump of your service definitions

12 [global]
13   workgroup = DEYUGROUP
14   server string = Samba Server Version %v
15   log file = /var/log/samba/log.%m
16   max log size = 50
17   idmap config * : backend = tdb
18   cups options = raw

20 [homes]
21   comment = Home Directories
22   read only = No
23   browseable = No

24 [printers]

```

```

26    comment = All Printers
27    path = /var/spool/samba
28    printable = Yes
29    print ok = Yes
30    browseable = No

32 [common]
33   path = /groupdir
34   hosts allow = 192.168.122.

36 [data]
37   path = /data
38   write list = @dywsmb
39   hosts allow = 192.168.122.

```

9. 如果 deyu2, deyu3 用戶不存在，則新增用戶 deyu2, deyu3。

```

1 [root@kvm5 ~]# useradd deyu2
2 [root@kvm5 ~]# useradd deyu3

```

10. 查看目前 samba 用戶成員只有 deyu1。

```

1 [root@kvm5 ~]# pdbedit -L
2 deyu1:1000:

```

11. 將用戶 deyu2 及 deyu3 新增為 samba 用戶成員。

```

1 [root@kvm5 ~]# smbpasswd -a deyu2
2 New SMB password:
3 Retype new SMB password:
4 Added user deyu2.
5 [root@kvm5 ~]# smbpasswd -a deyu3
6 New SMB password:
7 Retype new SMB password:
8 Added user deyu3.

```

12. 因用戶 deyu3 必須有寫入權限，所以增加附屬群組為 dywsmb。

```
[root@kvm5 ~]# usermod -G dywsmb deyu3
```

13. 查看目前 samba 用戶成員有 deyu1, deyu2, deyu3。

```
1 [root@kvm5 ~]# pdbedit -L  
2      deyu3:1002:  
3      deyu1:1000:  
4      deyu2:1001:
```

14. 重新啓動 kvm5.deyu.wang 主機的 smb 及 nmb 服務。

```
[root@kvm5 ~]# systemctl restart smb.service nmb.service
```

8.4 防火牆設定

1. 防火牆永久加入 samba 服務。

```
1 [root@kvm5 ~]# firewall-cmd --permanent --add-service=samba  
2 success
```

2. 重新載入防火牆。

```
1 [root@kvm5 ~]# firewall-cmd --reload  
2 success
```

3. 列出防火牆設定，支援的服務包含 samba。

```
1 [root@kvm5 ~]# firewall-cmd --list-all  
2 public (default)  
3     interfaces:  
4     sources:  
5     services: dhcpcv6-client samba ssh  
6     ports:  
7     masquerade: no  
8     forward-ports:  
9     icmp-blocks:  
10    rich rules:  
11        rule family="ipv4" source address="192.168.111.0/24" port port="22"  
12            protocol="tcp" reject
```

8.5 * 測試 SMB 分享目錄

- 在 kvm7.deyu.wang 主機測試，因要用到 mount.cifs 命令，所以必須先安裝 cifs-utils 套件。

```
1 [root@kvm7 ~]# yum -y install cifs-utils samba-client
```

- 先測試 samba 用戶 deyu1 是否可以存取 kvm5.deyu.wang smb 分享目錄 /common。如果出現 NT_STATUS_ASSESS_DENIED 存取限制訊息，請試著修改 kvm5 smb server 的 hosts allow 參數原先的網域 .deyu.wang 改為 ip 192.168.122.

```
1 [root@kvm7 ~]# smbclient -L //kvm5.deyu.wang/common -U deyu1
Enter deyu1's password:
3 Domain=[DEYUGROUP] OS=[Unix] Server=[Samba 4.1.12]

5   Sharename        Type      Comment
-----  -----      -----
7     data            Disk
9     common          Disk
9     IPC$           IPC       IPC Service (Samba Server Version 4.1.12)
11    deyu1           Disk     Home Directories
11 Domain=[DEYUGROUP] OS=[Unix] Server=[Samba 4.1.12]

13    Server          Comment
-----  -----
15      KVM5          Samba Server Version 4.1.12

17    Workgroup       Master
-----  -----
19      DEYUGROUP     KVM5
```

- 建立用戶 deyu1 要掛載 smb 分享目錄的掛載目錄 /mnt/deyu1。

```
1 [root@kvm7 ~]# mkdir /mnt/deyu1
```

- 用戶 deyu1 掛載 smb server kvm5.deyu.wang 分享目錄 /common。

```
1 [root@kvm7 ~]# mount -o username=deyu1 //kvm5.deyu.wang/common /mnt/
      deyu1
Password for deyu1@//kvm5.deyu.wang/common: *****
```

5. 成功掛載到 /mnt/deyu1。

```
[root@kvm7 ~]# df -h
2 Filesystem           Size  Used Avail Use% Mounted on
/dev/mapper/vg_kvm7usb-root 3.1G  1.1G  1.8G  38% /
4 devtmpfs              487M    0  487M   0% /dev
tmpfs                  497M    0  497M   0% /dev/shm
6 tmpfs                  497M  6.6M  491M   2% /run
tmpfs                  497M    0  497M   0% /sys/fs/cgroup
8 /dev/mapper/vg_kvm7home-vo 74M  1.6M   67M   3% /home
10 /dev/vda1             197M 107M   90M  55% /boot
//kvm5.deyu.wang/common 3.1G  1.1G  1.8G  38% /mnt/deyu1
```

6. 卸載 /mnt/deyu1。

```
[root@kvm7 ~]# umount /mnt/deyu1
```

8.6 測試多使用者 SMB 掛載

1. 在 kvm7.deyu.wang 主機測試，因要用到 mount.cifs 命令，所以必須先安裝 cifs-utils 套件。

```
1 [root@kvm7 ~]# yum -y install cifs-utils
```

2. 掛載 cifs 檔案格式使用手冊。

```
1 [root@kvm7 ~]# man 8 mount.cifs
```

3. 建立多使用者 SMB 掛載目錄 /mnt/multi。

```
1 [root@kvm7 ~]# mkdir /mnt/multi
```

4. 使用 root 身份將 smb 分享目錄以 multiuser 參數掛載成共享目錄，掛載參數指定用戶為 deyu2，此用戶不屬於 dywsmb 群組，所以沒有寫入的權限，也就是一般用戶使用此共享目錄僅具有指定用戶 deyu2 的讀取權限。

```

1 [root@kvm7 ~]# mount -o multiuser,sec=ntlmssp,username=deyu2 //kvm5.deyu
2 .wang/data /mnt/multi
3 Password for deyu2@//kvm5.deyu.wang/data: *****
4 [root@kvm7 ~]# df -h
5 Filesystem           Size  Used Avail Use% Mounted on
6 /dev/mapper/vg_kvm7usb-root 3.1G  1.1G  1.8G  38% /
7 devtmpfs              487M    0   487M   0% /dev
8 tmpfs                 497M    0   497M   0% /dev/shm
9 tmpfs                 497M  6.6M  491M   2% /run
10 tmpfs                497M    0   497M   0% /sys/fs/cgroup
11 /dev/mapper/vg_kvm7home-vo 74M   1.6M   67M   3% /home
12 /dev/vda1              197M 107M   90M  55% /boot
13 //kvm5.deyu.wang/data   3.1G  1.1G  1.8G  38% /mnt/multi

```

5. 切換身份為 deyu3。

```

1 [root@kvm7 ~]# su - deyu3
2 Last login: Mon Dec 14 22:37:01 CST 2015 on pts/0

```

6. 以身份 deyu3，無法寫入資料到 /mnt/multi。

```

1 [deyu3@kvm7 ~]$ echo deyu3 > /mnt/multi/deyu3.txt
2 -bash: /mnt/multi/deyu3.txt: Permission denied

```

7. 使用 cifscreds 增加 deyu3 身份認證。

```

1 [deyu3@kvm7 ~]$ cifscreds add kvm5.deyu.wang
2 Password:

```

8. 經 cifscreds 增加 deyu3 身份認證，已可寫入資料到 /mnt/multi。

```

1 [deyu3@kvm7 ~]$ cifscreds add kvm5.deyu.wang
2 Password:
3 [deyu3@kvm7 ~]$ echo deyu3 > /mnt/multi/deyu3.txt

```

9. 退出 deyu3 身份，回到 root，再切換身份為 deyu2。

```
1 [deyu3@kvm7 ~]$ exit  
2 logout  
3 [root@kvm7 ~]# su - deyu2  
Last login: Sat Aug  8 21:07:20 CST 2015 on pts/0
```

10. 以身份 deyu2，無法寫入資料到 /mnt/multi。

```
1 [deyu2@kvm7 ~]$ echo "deyu2" > /mnt/multi/deyu2.txt  
2 -bash: /mnt/multi/deyu2.txt: Permission denied
```

11. 使用 cifscreds 增加 deyu2 身份認證。

```
1 [deyu2@kvm7 ~]$ cifscreds add kvm5.deyu.wang  
2 Password:
```

12. 因 deyu2 不屬於 dywsmb 群組，所以經 cifscreds 增加 deyu2 身份認證，還是無法寫入資料到 /mnt/multi，只能讀取。

```
1 [deyu2@kvm7 ~]$ echo "deyu2" > /mnt/multi/deyu2.txt  
2 -bash: /mnt/multi/deyu2.txt: Permission denied  
3 [deyu2@kvm7 ~]$ cat /mnt/multi/deyu3.txt  
4 deyu3
```

13. 登出 deyu2。

```
1 [deyu2@kvm7 ~]$ exit  
2 logout  
3 [root@kvm7 ~]#
```

14. 卸載 /mnt/multi。

```
1 [root@kvm7 ~]# umount /mnt/multi
```

8.7 開機自動掛載多使用者 SMB 目錄

1. 卸載 /mnt/multi。

```
1 [root@kvm7 ~]# umount /mnt/multi/
```

2. 編輯 /etc/fstab，加入掛載 /data 目錄，type 必須是 cifs，參數則是多使用者掛載。考試時直接將密碼寫在 /etc/fstab 中，只是安全性比較差。

```
1 [root@kvm7 ~]# vim /etc/fstab
[root@kvm7 ~]# tail -n1 /etc/fstab
3 //kvm5.deyu.wang/data /mnt/multi cifs multiuser,username=deyu2,password
=123qwe,sec=ntlmssp 0 0
```

3. 依據掛載表 /etc/fstab 全部掛載。

```
1 [root@kvm7 ~]# mount -a
```

4. 成功掛載 smb server kvm5.deyu.wang 分享目錄 /data 於目錄 /mnt/multi。

```
1 [root@kvm7 ~]# df -h
Filesystem           Size  Used Avail Use% Mounted on
3 /dev/mapper/vg_kvm7usb-root  3.1G  1.1G  1.8G  38% /
devtmpfs              487M    0  487M   0% /dev
5 tmpfs                497M    0  497M   0% /dev/shm
tmpfs                497M   6.6M  491M   2% /run
7 tmpfs                497M    0  497M   0% /sys/fs/cgroup
/dev/mapper/vg_kvm7home-vo   74M   1.6M   67M   3% /home
9 /dev/vda1             197M  107M   90M  55% /boot
//kvm5.deyu.wang/data      3.1G  1.1G  1.8G  38% /mnt/multi
```

8.8 * 安全開機自動掛載多使用者 SMB 目錄

1. 卸載 /mnt/multi。

```
[root@kvm7 ~]# umount /mnt/multi/
```

2. 編輯 /etc/fstab，加入掛載 /data 目錄，type 必須是 cifs，參數則是多使用者掛載。

```

1 [root@kvm7 ~]# vim /etc/fstab
2 [root@kvm7 ~]# tail -1 /etc/fstab
3 //kvm5.deyu.wang/data /mnt/multi cifs multiuser,sec=ntlmssp,username=
        deyu2 0 0

```

3. 嘗試掛載，需要輸入密碼。

```

1 [root@kvm7 ~]# mount -a
Password for deyu2@//kvm5.deyu.wang/data: *****

```

4. 在家目錄新增一 smb 認證用的帳號密碼檔。

```

2 [root@kvm7 ~]# vim ~/.smbcredentials
3 [root@kvm7 ~]# cat ~/.smbcredentials
username=deyu2
4 password=123qwe
[root@kvm7 ~]# chmod 600 ~/.smbcredentials

```

5. 再編輯開機自動掛載表 /etc/fstab，將認證帳密檔位置加入 cifs 掛載參數。

```

1 [root@kvm7 ~]# vim /etc/fstab
2 [root@kvm7 ~]# tail -1 /etc/fstab
3 //kvm5.deyu.wang/data /mnt/multi cifs credentials=/root/.smbcredentials,
        multiuser,sec=ntlmssp 0 0

```

6. 嘗試掛載，已不需要輸入密碼。

```

1 [root@kvm7 ~]# mount -a
2 [root@kvm7 ~]# df -h
3 Filesystem           Size  Used Avail Use% Mounted on
4 /dev/mapper/vg_kvm7usb-root 3.1G  1.1G  1.8G  39% /
5 devtmpfs              487M    0   487M   0% /dev
6 tmpfs                 497M    0   497M   0% /dev/shm
7 tmpfs                 497M  6.6M  491M   2% /run
8 tmpfs                 497M    0   497M   0% /sys/fs/cgroup
9 /dev/mapper/vg_kvm7home-vo  74M   1.6M   67M   3% /home

```

11	/dev/vda1	197M	107M	90M	55%	/boot
	//kvm5.deyu.wang/data	3.1G	1.1G	1.8G	39%	/mnt/multi

Chapter 9

Network File System, NFS

9.1 NFS 簡介

1. 讓遠端主機可以掛載使用本機的檔案系統。
2. 系統管理員可藉 NFS 整合網路上的服務器。例如：多台主機使用相同的 LDAP 提供的帳號，同一帳號當然使用相同的家目錄，若各主機上都各自建立每一用戶的家目錄，則用戶的資料將無法同步。此時使用 NFS 就可提供家目錄的整合。
3. RHEL 6 (CentOS 6) 支援 NFSv2, NFSv3, NFSv4。
4. NFS 需要 nfslock 及 rpcbind 服務。但 NFSv4 不再使用 rpcbind。
5. NFS 以明文傳送資料，並依賴用戶端確認用戶，對於敏感的資料，建議不要使用沒有以 kerberos 認證及加密的 NFS 輸出目錄。
6. NFS 及 Samba 使用不同的檔案鎖定方式，所以 RHEL/CentOS 7 不支援 NFS 及 Samba 共用同一目錄。

9.2 *Kerberos KDC

1. 本節非課程範圍，但練習系統必須存在 kerberos keytab 才能練習，Server 端必須先產生 NFS kerberos 認證的 keytab，本節為產生過程演練，學生也可自行依例產生，實際測驗時只需依照指定網址下載 keytab 存成 /etc/krb5.keytab 即可。
2. Kerberos 是 MIT 在 1988 發展出來的認證協定。用戶端使用 principal (kind of login) 與 KDC server (Kerberos Distribution Center) 連線取得 ticket。如果 ticket 有效，用戶端就可不需要再認證下存取一些服務。
3. kdc 用戶端 (此例為 kvm7.deyu.wang) 與 KDC server (此例為 kvm7.deyu.wang) 必須在相同的 realm (通常為大寫的網域名，此例為 DEYU.WANG)。
4. 開始設定前必須先以 NTP 校時，並確定主機名稱解析沒問題，如果沒有 DNS，可以在 /etc/hosts 設定主機名稱的對應。**但此設定會造成 HTTPS 用戶端認證失效，且實際練習時 DNS 一定且必須正常運作，所以不需要設定此對應。**

```

1 [root@kvm5 ~]# vim /etc/hosts
2 [root@kvm5 ~]# tail -2 /etc/hosts
3 192.168.122.5 kvm5.deyu.wang
4 192.168.122.7 kvm7.deyu.wang

```

5. 安裝需要的套件。

```
[root@kvm5 ~]# yum install -y krb5-server krb5-workstation pam_krb5
```

6. 編輯 /var/kerberos/krb5kdc/kdc.conf，取代 EXAMPLE.COM 為 DEYU.WANG。取消註解 master_key_type = aes256-cts，並在章節 [realms] 貼上 default_principal_flags = +preauth。

```

1 [root@kvm5 ~]# vim /var/kerberos/krb5kdc/kdc.conf
2 [root@kvm5 ~]# sed -i 's/EXAMPLE.COM/DEYU.WANG/g' /var/kerberos/krb5kdc/
3   kdc.conf
4 [root@kvm5 ~]# sed -i 's/#//g' /var/kerberos/krb5kdc/kdc.conf
5 [root@kvm5 ~]# sed -i 's/(\^ [realms\$])/\1\n default_principal_flags =
6   \+preauth/g' \
7 /var/kerberos/krb5kdc/kdc.conf
8 [root@kvm5 ~]# grep 'DEYU' -A3 -B2 /var/kerberos/krb5kdc/kdc.conf
9 [realms]
10  default_principal_flags = +preauth
11  DEYU.WANG = {
12    master_key_type = aes256-cts
13    acl_file = /var/kerberos/krb5kdc/kadm5.acl
14    dict_file = /usr/share/dict/words

```

7. 在 /etc/krb5.conf file 取消所有註解，取代 EXAMPLE.COM 為 DEYU.WANG，example.com 為 deyu.wang，kerberos.example.com 為 KDC server (此例為 kvm5.deyu.wang)。

```

2 [root@kvm5 ~]# vim /etc/krb5.conf
3 [root@kvm5 ~]# sed -i 's/EXAMPLE.COM/DEYU.WANG/g' /etc/krb5.conf
4 [root@kvm5 ~]# sed -i 's/#//g' /etc/krb5.conf
5 [root@kvm5 ~]# sed -i 's/example.com/deyu.wang/g' /etc/krb5.conf
6 [root@kvm5 ~]# sed -i 's/kerberos\(.deyu.wang\)/kvm5\1/g' /etc/krb5.conf
7 [root@kvm5 ~]# cat /etc/krb5.conf
8 [logging]
9   default = FILE:/var/log/krb5libs.log
10  kdc = FILE:/var/log/krb5kdc.log
11  admin_server = FILE:/var/log/kadmind.log

```

```

12 [libdefaults]
13 dns_lookup_realm = false
14 ticket_lifetime = 24h
15 renew_lifetime = 7d
16 forwardable = true
17 rdns = false
18 default_realm = DEYU.WANG
19 default_ccache_name = KEYRING:persistent:%{uid}
20
21 [realms]
22 DEYU.WANG = {
23   kdc = kvm5.deyu.wang
24   admin_server = kvm5.deyu.wang
25 }
26
27 [domain_realm]
28 .deyu.wang = DEYU.WANG
29 deyu.wang = DEYU.WANG

```

8. 編輯 `/var/kerberos/krb5kdc/kadm5.acl`，取代 EXAMPLE.COM 為自己的 realm DEYU.WANG。

```

1 [root@kvm5 ~]# vim /var/kerberos/krb5kdc/kadm5.acl
2 [root@kvm5 ~]# sed -i 's/EXAMPLE.COM/DEYU.WANG/g' /var/kerberos/krb5kdc/
3   kadm5.acl
4 [root@kvm5 ~]# cat /var/kerberos/krb5kdc/kadm5.acl
5 */admin@DEYU.WANG    *

```

9. 如果有舊的 kerberos database，先整個刪除。

```

1 [root@kvm5 ~]# kdb5_util destroy -f
2 ** Database '/var/kerberos/krb5kdc/principal' destroyed.

```

10. **如果有舊的 principal keytab 一定要刪除，否則無法認證。**

```

1 [root@kvm5 ~]# kadmin.local -q 'delete_principal -force nfs/kvm5.deyu.
2   wang@DEYU.WANG'
3 [root@kvm5 ~]# kadmin.local -q 'delete_principal -force nfs/kvm7.deyu.
4   wang@DEYU.WANG'
5 [root@kvm5 ~]# kadmin.local -q 'ktremove -k /etc/krb5.keytab nfs/kvm5.
6   deyu.wang@DEYU.WANG'
7 [root@kvm5 ~]# kadmin.local -q 'ktremove -k /etc/kvm7.keytab nfs/kvm7.
8   deyu.wang@DEYU.WANG'

```

11. 產生 kerberos database，執行很久沒反應， Ctrl+c 中斷。

```
1 [root@kvm5 ~]# kdb5_util create -s -r DEYU.WANG
2 Loading random data
~C
```

12. 若產生過程一直卡在 Loading random data，表示 /dev/random 無法產生够長的隨機字串，檢查原因为 CentOS 7 必須使用 /dev/urandom，所以將 /dev/random 連結到 /dev/urandom。

```
1 [root@kvm5 ~]# mv /dev/random /dev/xrandom
2 [root@kvm5 ~]# ln -s /dev/urandom /dev/random
3 [root@kvm5 ~]# ll /dev/urandom /dev/random
4 lrwxrwxrwx. 1 root root 12 Aug 9 20:59 /dev/random -> /dev/urandom
5 crw-rw-rw-. 1 root root 1, 9 Aug 9 07:37 /dev/urandom
```

13. 成功產生 kerberos database。

```
1 [root@kvm5 ~]# kdb5_util create -s -r DEYU.WANG
2 Loading random data
3 Initializing database '/var/kerberos/krb5kdc/principal' for realm 'DEYU.
   WANG',
4 master key name 'K/M@DEYU.WANG'
5 You will be prompted for the database Master Password.
6 It is important that you NOT FORGET this password.
7 Enter KDC database master key:
   Re-enter KDC database master key to verify:
```

14. 設定 kerberos 服務開機啓動。

```
[root@kvm5 ~]# systemctl enable krb5kdc.service kadmin.service
```

15. 啓動 kerberos 服務。

```
1 [root@kvm5 ~]# systemctl start krb5kdc.service kadmin.service
```

16. 執行 kerberos 管理工具。

```

1 [root@kvm5 ~]# kadmin.local
Authenticating as principal root/admin@DEYU.WANG with password.
3 kadmin.local:

```

17. 產生 admin 管理者 principal，如果所有 principal keytab 都在 local 端產生，此步驟可省略。

```

1 kadmin.local: addprinc root/admin
WARNING: no policy specified for root/admin@DEYU.WANG; defaulting to no
          policy
3 Enter password for principal "root/admin@DEYU.WANG":
Re-enter password for principal "root/admin@DEYU.WANG":
5 Principal "root/admin@DEYU.WANG" created.

```

18. 產生 NFS principal nfs/kvm5.deyu.wang °

```

1 [root@kvm5 ~]# kadmin.local -q "addprinc -pw 123qwe nfs/kvm5.deyu.wang"
Authenticating as principal nfs/admin@DEYU.WANG with password.
3 WARNING: no policy specified for nfs/kvm5.deyu.wang@DEYU.WANG;
          defaulting to no policy
Principal "nfs/kvm5.deyu.wang@DEYU.WANG" created.

```

19. 產生 NFS principal nfs/kvm7.deyu.wang °

```

1 [root@kvm5 ~]# kadmin.local -q "addprinc -pw 123qwe nfs/kvm7.deyu.wang"
2 Authenticating as principal nfs/admin@DEYU.WANG with password.
WARNING: no policy specified for nfs/kvm7.deyu.wang@DEYU.WANG;
          defaulting to no policy
4 Principal "nfs/kvm7.deyu.wang@DEYU.WANG" created.

```

20. 產生 nfs/kvm5.deyu.wang principal 副本到預設檔案 /etc/kvm5.keytab，解題時此檔提供下載。

```

1 [root@kvm5 ~]# kadmin.local -q 'ktadd -k /etc/kvm5.keytab nfs/kvm5.deyu.
          wang@DEYU.WANG'
2 Authenticating as principal nfs/admin@DEYU.WANG with password.
Entry for principal nfs/kvm5.deyu.wang@DEYU.WANG with kvno 2, encryption
          type
4 aes256-cts-hmac-sha1-96 added to keytab WRFILE:/etc/kvm5.keytab.

```

```

1   Entry for principal nfs/kvm5.deyu.wang@DEYU.WANG with kvno 2, encryption
2     type
3     aes128-cts-hmac-sha1-96 added to keytab WRFILE:/etc/kvm5.keytab.
4     Entry for principal nfs/kvm5.deyu.wang@DEYU.WANG with kvno 2, encryption
5       type
6     des3-cbc-sha1 added to keytab WRFILE:/etc/kvm5.keytab.
7     Entry for principal nfs/kvm5.deyu.wang@DEYU.WANG with kvno 2, encryption
8       type
9     arcfour-hmac added to keytab WRFILE:/etc/kvm5.keytab.
10    Entry for principal nfs/kvm5.deyu.wang@DEYU.WANG with kvno 2, encryption
11      type
12    camellia256-cts-cmac added to keytab WRFILE:/etc/kvm5.keytab.
13    Entry for principal nfs/kvm5.deyu.wang@DEYU.WANG with kvno 2, encryption
14      type
15    camellia128-cts-cmac added to keytab WRFILE:/etc/kvm5.keytab.
16    Entry for principal nfs/kvm5.deyu.wang@DEYU.WANG with kvno 2, encryption
17      type
18    des-hmac-sha1 added to keytab WRFILE:/etc/kvm5.keytab.
19    Entry for principal nfs/kvm5.deyu.wang@DEYU.WANG with kvno 2, encryption
20      type
21    des-cbc-md5 added to keytab WRFILE:/etc/kvm5.keytab.

```

21. 產生 nfs/kvm5.deyu.wang principal 副本到預設檔案 /etc/kvm7.keytab。解題時此檔提供 client kvm7 下載放到 /etc/krb5.keytab。

```

[root@kvm5 ~]# kadmin.local -q 'ktadd -k /etc/kvm7.keytab nfs/kvm7.deyu.
1   wang@DEYU.WANG'
2   Authenticating as principal nfs/admin@DEYU.WANG with password.
3   Entry for principal nfs/kvm7.deyu.wang@DEYU.WANG with kvno 2, encryption
4     type
5     aes256-cts-hmac-sha1-96 added to keytab WRFILE:/etc/kvm7.keytab.
6     Entry for principal nfs/kvm7.deyu.wang@DEYU.WANG with kvno 2, encryption
7       type
8     aes128-cts-hmac-sha1-96 added to keytab WRFILE:/etc/kvm7.keytab.
9     Entry for principal nfs/kvm7.deyu.wang@DEYU.WANG with kvno 2, encryption
10    type
11    arcfour-hmac added to keytab WRFILE:/etc/kvm7.keytab.
12    Entry for principal nfs/kvm7.deyu.wang@DEYU.WANG with kvno 2, encryption
13      type
14    camellia256-cts-cmac added to keytab WRFILE:/etc/kvm7.keytab.
15    Entry for principal nfs/kvm7.deyu.wang@DEYU.WANG with kvno 2, encryption
16      type
17    camellia128-cts-cmac added to keytab WRFILE:/etc/kvm7.keytab.
18    Entry for principal nfs/kvm7.deyu.wang@DEYU.WANG with kvno 2, encryption
19      type
20    des-cbc-md5 added to keytab WRFILE:/etc/kvm7.keytab.

```

22. 查看 /etc/kvm5.keytab 只有一組 keytab。

```
[root@kvm5 ~]# klist -kte /etc/kvm5.keytab
2 Keytab name: FILE:/etc/kvm5.keytab
KVNO Timestamp Principal
4 -----
2 12/04/2015 21:04:28 nfs/kvm5.deyu.wang@DEYU.WANG (aes256-cts-hmac-
sha1-96)
6 2 12/04/2015 21:04:28 nfs/kvm5.deyu.wang@DEYU.WANG (aes128-cts-hmac-
sha1-96)
8 2 12/04/2015 21:04:28 nfs/kvm5.deyu.wang@DEYU.WANG (des3-cbc-sha1)
2 12/04/2015 21:04:28 nfs/kvm5.deyu.wang@DEYU.WANG (arcfour-hmac)
2 12/04/2015 21:04:28 nfs/kvm5.deyu.wang@DEYU.WANG (camellia256-cts-
cmac)
10 2 12/04/2015 21:04:28 nfs/kvm5.deyu.wang@DEYU.WANG (camellia128-cts-
cmac)
12 2 12/04/2015 21:04:28 nfs/kvm5.deyu.wang@DEYU.WANG (des-hmac-sha1)
2 12/04/2015 21:04:28 nfs/kvm5.deyu.wang@DEYU.WANG (des-cbc-md5)
```

23. 查看 /etc/kvm7.keytab 只有一組 keytab。

```
[root@kvm5 ~]# klist -kte /etc/kvm7.keytab
2 Keytab name: FILE:/etc/kvm7.keytab
KVNO Timestamp Principal
4 -----
2 12/04/2015 21:04:31 nfs/kvm7.deyu.wang@DEYU.WANG (aes256-cts-hmac-
sha1-96)
6 2 12/04/2015 21:04:31 nfs/kvm7.deyu.wang@DEYU.WANG (aes128-cts-hmac-
sha1-96)
2 12/04/2015 21:04:31 nfs/kvm7.deyu.wang@DEYU.WANG (des3-cbc-sha1)
2 12/04/2015 21:04:31 nfs/kvm7.deyu.wang@DEYU.WANG (arcfour-hmac)
2 12/04/2015 21:04:31 nfs/kvm7.deyu.wang@DEYU.WANG (camellia256-cts-
cmac)
10 2 12/04/2015 21:04:31 nfs/kvm7.deyu.wang@DEYU.WANG (camellia128-cts-
cmac)
12 2 12/04/2015 21:04:31 nfs/kvm7.deyu.wang@DEYU.WANG (des-hmac-sha1)
2 12/04/2015 21:04:31 nfs/kvm7.deyu.wang@DEYU.WANG (des-cbc-md5)
```

24. 查看 /etc/krb5.keytab 已產生。

```
[root@kvm5 ~]# ll /etc/krb5.keytab
```

```
2 -rw----- 1 root root 562 Sep 4 11:56 /etc/krb5.keytab
```

25. 因為用戶 deyu3 必須可以寫入 nfs 安全掛載的目錄，因此增加 deyu3@DEYU.WANG principal。

```
[root@kvm5 ~]# kadmin.local -q "addprinc -pw 123qwe deyu3@DEYU.WANG"
2 Authenticating as principal nfs/admin@DEYU.WANG with password.
WARNING: no policy specified for deyu3@DEYU.WANG; defaulting to no
        policy
4 Principal "deyu3@DEYU.WANG" created.
```

26. 將 deyu3@DEYU.WANG 的 principal 累加到 /etc/kvm7.keytab，以提供 kvm7.deyu.wang 下載使用。

```
[root@kvm5 ~]# kadmin.local -q 'ktadd -k /etc/kvm7.keytab deyu3@DEYU.
WANG'Authenticating as principal nfs/admin@DEYU.WANG with password.
2 Entry for principal deyu3@DEYU.WANG with kvno 3, encryption type aes256-
    cts-hmac-sha1-96 added to keytab WRFILE:/etc/kvm7.keytab.
Entry for principal deyu3@DEYU.WANG with kvno 3, encryption type aes128-
    cts-hmac-sha1-96 added to keytab WRFILE:/etc/kvm7.keytab.
4 Entry for principal deyu3@DEYU.WANG with kvno 3, encryption type des3-
    cbc-sha1 added to keytab WRFILE:/etc/kvm7.keytab.
Entry for principal deyu3@DEYU.WANG with kvno 3, encryption type arcfour-
    -hmac added to keytab WRFILE:/etc/kvm7.keytab.
6 Entry for principal deyu3@DEYU.WANG with kvno 3, encryption type
    camellia256-cts-cmac added to keytab WRFILE:/etc/kvm7.keytab.
Entry for principal deyu3@DEYU.WANG with kvno 3, encryption type
    camellia128-cts-cmac added to keytab WRFILE:/etc/kvm7.keytab.
8 Entry for principal deyu3@DEYU.WANG with kvno 3, encryption type des-
    hmac-sha1 added to keytab WRFILE:/etc/kvm7.keytab.
Entry for principal deyu3@DEYU.WANG with kvno 3, encryption type des-cbc-
    -md5 added to keytab WRFILE:/etc/kvm7.keytab.
```

27. 查看 /etc/kvm7.keytab principal 除了 nfs/kvm7.deyu.wang 外，還多了 deyu3。

```
1 [root@kvm5 ~]# klist -kte /etc/kvm7.keytab
Keytab name: FILE:/etc/kvm7.keytab
3 KVNO Timestamp          Principal
-----
5 2 12/14/2015 11:54:09 nfs/kvm7.deyu.wang@DEYU.WANG (aes256-cts-hmac-
    sha1-96)
2 12/14/2015 11:54:09 nfs/kvm7.deyu.wang@DEYU.WANG (aes128-cts-hmac-
    sha1-96)
```

```

7  2 12/14/2015 11:54:09 nfs/kvm7.deyu.wang@DEYU.WANG (des3-cbc-sha1)
2 12/14/2015 11:54:09 nfs/kvm7.deyu.wang@DEYU.WANG (arcfour-hmac)
9  2 12/14/2015 11:54:09 nfs/kvm7.deyu.wang@DEYU.WANG (camellia256-cts-
    cmac)
2 12/14/2015 11:54:09 nfs/kvm7.deyu.wang@DEYU.WANG (camellia128-cts-
    cmac)
11 2 12/14/2015 11:54:09 nfs/kvm7.deyu.wang@DEYU.WANG (des-hmac-sha1)
2 12/14/2015 11:54:09 nfs/kvm7.deyu.wang@DEYU.WANG (des-cbc-md5)
13 3 12/14/2015 19:30:37 deyu3@DEYU.WANG (aes256-cts-hmac-sha1-96)
3 12/14/2015 19:30:37 deyu3@DEYU.WANG (aes128-cts-hmac-sha1-96)
15 3 12/14/2015 19:30:38 deyu3@DEYU.WANG (des3-cbc-sha1)
3 12/14/2015 19:30:38 deyu3@DEYU.WANG (arcfour-hmac)
17 3 12/14/2015 19:30:38 deyu3@DEYU.WANG (camellia256-cts-cmac)
3 12/14/2015 19:30:38 deyu3@DEYU.WANG (camellia128-cts-cmac)
19 3 12/14/2015 19:30:38 deyu3@DEYU.WANG (des-hmac-sha1)
3 12/14/2015 19:30:38 deyu3@DEYU.WANG (des-cbc-md5)

```

28. kadmin 產生的 Principal ”nfs/kvm5.deyu.wang@DEYU.WANG” 在目錄 /var/kerberos/krb5kdc 下的 principal。ktadd nfs/kvm5.deyu.wang 不指定檔案名稱下產生的 krb5.keytab 自動存在目錄 /etc 下。kadmin.local 也可產生 ktadd -k /root/krb5.keytab nfs/kvm7.deyu.wang 產生 nfs client kvm7 的 krb5.keytab 再 copy 至 kvm7 的 /etc 目錄下。nfs kerberos 要成功掛載，這三個檔案產生後若要移至其他機器，必須同時配對，只要任何一個檔案變動過就無法成功掛載。因此，雖將製作好的 nfs server 及 client krb5.keytab 供架設下載，nfs server 還是要安裝 krb5-server 且設定必須與製作 keytab 時一樣，更重要的是產生的 principal 也要用原製作 keytab 時的 principal 覆蓋才可以。

```

[root@kvm5 ~]# ll /var/kerberos/krb5kdc/
2 total 32
-rw----- 1 root root 20 Aug 30 20:06 kadm5.acl
4 -rw----- 1 root root 484 Aug 30 20:06 kdc.conf
-rw----- 1 root root 16384 Aug 30 20:06 principal
6 -rw----- 1 root root 8192 Aug 30 20:06 principal.kadm5
-rw----- 1 root root 0 Aug 30 20:06 principal.kadm5.lock
8 -rw----- 1 root root 0 Aug 30 20:06 principal.ok

```

9.3 NFS Server 架設

1. 安裝 nfs-utils 套件。

```
[root@kvm5 ~]# yum install -y nfs-utils
```

2. 建立 NFS 分享目錄。

```
1 [root@kvm5 ~]# mkdir /public /protected
```

3. 修改 NFS 分享目錄的 SELinux 檔案 context。

```
1 [root@kvm5 ~]# semanage fcontext -a -t public_content_t "/public(.*)?"
[root@kvm5 ~]# semanage fcontext -a -t public_content_t "/protected(.*)
?"
3 [root@kvm5 ~]# restorecon -Rv /public /protected
```

4. 考試時不用自行產生 kerberos keytab，只要依照指定的位置下載，存放在目錄 /etc/ 下，且檔名必須為 krb5.keytab。

```
1 [root@kvm5 ~]# wget http://deyu.wang/kvm5.keytab -O /etc/krb5.keytab
```

5. kerberos keytab 的驗證跟時間有關，server 與 client 都必須校時。

```
1 [root@kvm5 ~]# date
Sun Jan  7 14:50:04 CST 2018
3 [root@kvm5 ~]# chronyc -a makestep
200 OK
5 200 OK
[root@kvm5 ~]# date
7 Mon Nov 20 15:53:22 CST 2017
```

6. 在 /protected 下建立次目錄 restricted，並將其擁有者設定為 deyu3，讓 deyu3 可以寫入資料。

```
1 [root@kvm5 ~]# mkdir -p /protected/restricted
[root@kvm5 ~]# chown deyu3 /protected/restricted
```

7. 編輯設定檔 /etc/exports，分享 /protected 及 /public 兩個目錄給網域 192.168.122.0/24。

```
1 [root@kvm5 ~]# echo '/protected 192.168.122.0/24(rw, sync, sec=krb5p)' > /
etc/exports
2 [root@kvm5 ~]# echo '/public 192.168.122.0/24(ro, sync)' >> /etc/exports
[root@kvm5 ~]# vim /etc/exports
4 [root@kvm5 ~]# cat /etc/exports
/protected 192.168.122.0/24(rw, sync, sec=krb5p)
/public 192.168.122.0/24(ro, sync)
```

8. NFS 掛載參數說明如下，詳細說明請參考 man 5 nfs 手冊。

- (a) rw : read-write，可讀寫的權限；
- (b) ro : read-only，唯讀的權限；
- (c) sec=mode : 安全認證模式；
 - i. sec=sys 預設，使用本地 UNIX UIDs 及 GIDs 進行身份認證。
 - ii. sec=krb5 使用 Kerberos V5 取代本地 UNIX UIDs 及 GIDs 進行身份認證。
 - iii. sec=krb5i 使用 Kerberos V5 進行身份認證，資料完整性檢查，以防止數據被篡改。
 - iv. sec=krb5p 使用 Kerberos V5 進行身份認證，資料完整性檢查及 NFS 傳輸加密，以防止數據被篡改，這是最安全的方式。
- (d) sync : 資料同步寫入到記憶體與硬碟當中；

```
[root@kvm5 ~]# man 5 nfs
```

9. 設定使用 4.2 版本，以匯出分享 SELinux context。無適合的版本 client 端掛載時會出現 mount.nfs: Protocol not supported 的訊息。

```
1 [root@kvm5 ~]# vim /etc/sysconfig/nfs
2   sed -i 's/^(\RPCNFSDARGS=).*$/\1\"-V 4.2\\"/' /etc/sysconfig/nfs
3 [root@kvm5 ~]# grep ^RPCNFSDARGS /etc/sysconfig/nfs
RPCNFSDARGS="-V 4.2"
```

10. 設定開機啓動 nfs 服務，NFS server 端的服務為 nfs-server 及 nfs-secure-server，本版本只要啓動 nfs-server 就同時啓動 nfs-secure-server，而且使用 tab 鍵也不會出現 nfs-secure-server 服務，但有些版本則是兩者分開，必須確認是不是兩種服務都啓動。

```
[root@kvm5 ~]# systemctl enable nfs-server.service nfs-secure-server.
service
```

11. 啓動 nfs 服務

```
1 [root@kvm5 ~]# systemctl start nfs-server.service nfs-secure-server.
service
```

12. 查看目前啓動的 nfs 版本，因 server 指定使用 4.2，若出現 -4.2 表示 nfs server 沒有成功啓動。

```
1 [root@kvm5 ~]# cat /proc/fs/nfsd/versions
-2 +3 +4 +4.1 +4.2
```

13. 要確定 nfs-secure-server nfs-server 服務都正常運作。

```
1 [root@kvm5 ~]# systemctl status nfs-secure-server.service nfs-server.
2   service
3 nfs-secure-server.service - Secure NFS Server
4     Loaded: loaded (/usr/lib/systemd/system/nfs-secure-server.service;
5           enabled)
6     Active: active (running) since Mon 2015-09-21 20:04:10 CST; 8s ago
7       Process: 3075 ExecStart=/usr/sbin/rpc.svcgssd $RPCSVCGSSDARGS (code=
8             exited, status=0/SUCCESS)
9     Main PID: 3077 (rpc.svcgssd)
10    CGroup: /system.slice/nfs-secure-server.service —
11          3077 /usr/sbin/rpc.svcgssd
12
13 Sep 21 20:04:10 kvm5.deyu.wang systemd[1]: Starting Secure NFS Server...
14 Sep 21 20:04:10 kvm5.deyu.wang systemd[1]: Started Secure NFS Server.
15
16 nfs-server.service - NFS Server
17   Loaded: loaded (/usr/lib/systemd/system/nfs-server.service; enabled)
18     Active: active (exited) since Mon 2015-09-21 20:04:10 CST; 8s ago
19       Process: 3078 ExecStopPost=/usr/sbin/exportfs -f (code=exited, status
20             =0/SUCCESS)
21       Process: 3076 ExecStop=/usr/sbin/rpc.nfsd 0 (code=exited, status=0/
22             SUCCESS)
23       Process: 3087 ExecStart=/usr/sbin/rpc.nfsd $RPCNFSDARGS $RPCNFSDCOUNT
24             (code=exited, status=0/SUCCESS)
25       Process: 3084 ExecStartPre=/usr/sbin/exportfs -r (code=exited, status
26             =0/SUCCESS)
27       Process: 3083 ExecStartPre=/usr/libexec/nfs-utils/scripts/nfs-server.
28             preconfig (code=exited, status=0/SUCCESS)
29     Main PID: 3087 (code=exited, status=0/SUCCESS)
30       CGroup: /system.slice/nfs-server.service
31
32 Sep 21 20:04:10 kvm5.deyu.wang systemd[1]: Starting NFS Server...
33 Sep 21 20:04:10 kvm5.deyu.wang systemd[1]: Started NFS Server.
```

14. 建議不論是否 TAB 有沒有出現提示，都同時啓動這兩個服務。CentOS 安裝版本 `nfs-utils-1.3.0-8.el7.x86_64` 啓動 `nfs-secure-server` 出現錯誤訊息，請執行 `yum downgrade nfs-utils` 換成 `nfs-utils-1.3.0-0.el7.x86_64` 套件。

```
1 [root@kvm5 ~]# rpm -qa | grep nfs-utils
2   nfs-utils-1.3.0-8.el7.x86_64
3 [root@kvm5 ~]# yum downgrade nfs-utils -y
4 [root@kvm5 ~]# rpm -qa | grep nfs-utils
5   nfs-utils-1.3.0-0.el7.x86_64
```

15. 再重新啓動 nfs 服務，並查看是否正常運作。

```
1 [root@kvm5 ~]# systemctl restart nfs-server.service nfs-secure-server.service
```

16. 輸出所有設定的 nfs 分享目錄。

```
1 [root@kvm5 ~]# exportfs -arv
exporting 192.168.122.0/24:/public
3 exporting 192.168.122.0/24:/protected
```

9.4 NFS 伺服器防火牆設定

1. 永久增加 kerberos 服務到 firewall。

```
1 [root@kvm5 ~]# firewall-cmd --permanent --add-service=kerberos
success
```

2. 永久增加 nfs 服務到 firewall。

```
2 [root@kvm5 ~]# firewall-cmd --permanent --add-service=nfs
success
```

3. 永久增加 rpc-bind 服務到 firewall。

```
2 [root@kvm5 ~]# firewall-cmd --permanent --add-service=rpc-bind
success
```

4. 永久增加 mountd 服務到 firewall。

```
2 [root@kvm5 ~]# firewall-cmd --permanent --add-service=mountd
success
```

5. **** KDC Client 端必須連線產生 keytab，所以 server 防火牆要開放 kadmind 的 ports，查到 kadmind 的 ports 有 749 及 464 兩個 ports。

```

1 [root@kvm5 ~]# netstat -nultp | grep kadmin
2   tcp      0      0 0.0.0.0:749          0.0.0.0:*
3     LISTEN    1511/kadmind
4   tcp      0      0 0.0.0.0:464          0.0.0.0:*
5     LISTEN    1511/kadmind
6   tcp6     0      0 :::749              :::*
7     LISTEN    1511/kadmind
8   tcp6     0      0 :::464              :::*
9     LISTEN    1511/kadmind
10  udp      0      0 0.0.0.0:464         0.0.0.0:*
11    1511/kadmind
12  udp6     0      0 fe80::5054:ff:fedc::464 :::*
13    1511/kadmind

```

6. **** 防火牆永久開放 kadmin 的 749 及 464 兩個 ports。

```

1 [root@kvm5 ~]# firewall-cmd --permanent --add-port=749/tcp
2 success
3 [root@kvm5 ~]# firewall-cmd --permanent --add-port=464/tcp
4 success

```

7. 重新載入防火牆設定。

```

1 [root@kvm5 ~]# firewall-cmd --reload
2 success

```

8. 列出 firewall 已新增 kerberos, nfs, rpc-bind, mountd 等服務，並且開放 749/tcp, 464/tcp 兩個 ports。

```

1 [root@kvm5 ~]# firewall-cmd --list-all
2 public (default)
3   interfaces:
4   sources:
5   services: dhcpc6-client kerberos mountd nfs rpc-bind ssh
6   ports: 749/tcp 464/tcp
7   masquerade: no
8   forward-ports:
9   icmp-blocks:
10  rich rules:
11    rule family="ipv4" source address="192.168.122.0/24" forward-port
12      port="80" protocol="tcp" to-port="8080"

```

9.5 *NFS Client 端 KDC 設定

1. 本節非課程範圍，但練習系統必須存在 kerberos keytab 才能練習，Client 端必須先產生 NFS kerberos 認證的 keytab，本節為產生過程演練，學生也可自行依例產生，實際測驗時只需依照指定網址下載 keytab 存成 /etc/krb5.keytab 即可。
2. 安裝套件 krb5-workstation pam_krb5

```
1 [root@kvm7 ~]# yum install -y krb5-workstation pam_krb5
```

3. 在 /etc/krb5.conf file 取消所有註解，取代 EXAMPLE.COM 為 DEYU.WANG，example.com 為 deyu.wang，kerberos.example.com 為 KDC server (此例為 kvm5.deyu.wang)。

```
1 [root@kvm7 ~]# vim /etc/krb5.conf
2 [root@kvm7 ~]# sed -i 's/EXAMPLE.COM/DEYU.WANG/g' /etc/krb5.conf
3 [root@kvm7 ~]# sed -i 's/#//g' /etc/krb5.conf
4 [root@kvm7 ~]# sed -i 's/example.com/deyu.wang/g' /etc/krb5.conf
5 [root@kvm7 ~]# sed -i 's/kerberos\(.deyu.wang\)/kvm5\1/g' /etc/krb5.conf
6 [root@kvm7 ~]# cat /etc/krb5.conf
7
[logging]
8     default = FILE:/var/log/krb5libs.log
9     kdc = FILE:/var/log/krb5kdc.log
10    admin_server = FILE:/var/log/kadmind.log
11
12
[libdefaults]
13    dns_lookup_realm = false
14    ticket_lifetime = 24h
15    renew_lifetime = 7d
16    forwardable = true
17    rdns = false
18    default_realm = DEYU.WANG
19    default_ccache_name = KEYRING:persistent:%{uid}
20
21
[realms]
22    DEYU.WANG = {
23        kdc = kvm5.deyu.wang
24        admin_server = kvm5.deyu.wang
25    }
26
27
[domain_realm]
28    .deyu.wang = DEYU.WANG
29    deyu.wang = DEYU.WANG
```

4. 執行 kadmin 連線到 kdc server。

```

1 [root@kvm7 ~]# kadmin -p root/admin@DEYU.WANG
Authenticating as principal root/admin@DEYU.WANG with password.
3 Password for root/admin@DEYU.WANG:
kadmin:
```

5. 產生 NFS principal。

```

2 kadmin: addprinc -randkey nfs/kvm7.deyu.wang
WARNING: no policy specified for nfs/kvm7.deyu.wang@DEYU.WANG;
          defaulting to no policy
Principal "nfs/kvm7.deyu.wang@DEYU.WANG" created.
```

6. 產生 nfs/kvm7.deyu.wang principal 副本到預設檔案 /etc/krb5.keytab。如果題目指明使用已建好的 krb5.keytab，只要將其下載並存成 /etc/krb5.keytab 即可。

```

1 kadmin: ktadd nfs/kvm7.deyu.wang
Entry for principal nfs/kvm7.deyu.wang with kvno 2, \
3 encryption type aes256-cts-hmac-sha1-96 added to keytab \
FILE:/etc/krb5.keytab.
5 Entry for principal nfs/kvm7.deyu.wang with kvno 2, \
encryption type aes128-cts-hmac-sha1-96 added to keytab \
7 FILE:/etc/krb5.keytab.
Entry for principal nfs/kvm7.deyu.wang with kvno 2, \
9 encryption type des3-cbc-sha1 added to keytab \
FILE:/etc/krb5.keytab.
11 Entry for principal nfs/kvm7.deyu.wang with kvno 2, \
encryption type arcfour-hmac added to keytab \
13 FILE:/etc/krb5.keytab.
Entry for principal nfs/kvm7.deyu.wang with kvno 2, \
15 encryption type camellia256-cts-cmac added to keytab \
FILE:/etc/krb5.keytab.
17 Entry for principal nfs/kvm7.deyu.wang with kvno 2, \
encryption type camellia128-cts-cmac added to keytab \
19 FILE:/etc/krb5.keytab.
Entry for principal nfs/kvm7.deyu.wang with kvno 2, \
21 encryption type des-hmac-sha1 added to keytab \
FILE:/etc/krb5.keytab.
23 Entry for principal nfs/kvm7.deyu.wang with kvno 2, \
encryption type des-cbc-md5 added to keytab \
25 FILE:/etc/krb5.keytab.
```

7. 退出 kerberos 管理工具。

```
1 || kadmin: quit
```

8. 查看 /etc/krb5.keytab 已產生。

```
1 [root@kvm7 ~]# ll /etc/krb5.keytab
-rw-----. 1 root root 562 Sep  4 13:09 /etc/krb5.keytab
```

9.6 NFS Client 端掛載設定

1. 安裝 cifs-utils 套件。

```
[root@kvm7 ~]# yum install -y cifs-utils
```

2. 設定開機啓動 nfs 服務，NFS client 端的服務為 nfs 及 nfs-secure，有時即使使用 tab 鍵也不會出現 nfs-secure 服務，也要試著執行看看，但有些版本則是兩者分開，必須確認是不是兩種服務都啓動。建議不論是否 TAB 有沒有出現提示，都同時啓動這兩個服務。

```
1 [root@kvm7 ~]# systemctl enable nfs.service nfs-secure.service
```

3. 啓動 nfs-secure 服務。

```
1 [root@kvm7 ~]# systemctl start nfs.service nfs-secure.service
```

4. 列出 kvm5.deyu.wang 分享的 NFS 目錄。

```
1 [root@kvm7 ~]# showmount -e kvm5.deyu.wang
Export list for kvm5.deyu.wang:
3 /public    192.168.122.0/24
   /protected 192.168.122.0/24
```

5. 考試時不用自行產生 kerberos keytab，只要依照指定的位置下載，存放在目錄 /etc/ 下，且檔名必須為 krb5.keytab 。

```
[root@kvm7 ~]# wget http://deyu.wang/kvm7.keytab -O /etc/krb5.keytab
```

6. kerberos keytab 的驗證跟時間有關，server 與 client 都必須校時。

```
1 [root@kvm7 ~]# date
Mon Nov 13 19:04:42 CST 2017
3 [root@kvm7 ~]# chronyc -a makestep
200 OK
5 200 OK
[root@kvm7 ~]# date
7 Mon Nov 20 15:53:35 CST 2017
```

7. 建立掛載目錄

```
1 [root@kvm7 ~]# mkdir /mnt/nfsmount /mnt/nfssecure
```

8. 手動掛載

```
1 [root@kvm7 ~]# mount.nfs4 -o sec=krb5p,v4.2 kvm5.deyu.wang:/protected /
mnt/nfssecure
```

9. 如果無法掛載，再重新啓動 nfs-secure.service 一次。

```
1 [root@kvm7 ~]# systemctl restart nfs-secure.service
```

10. 在開機掛載表 /etc/fstab 最後增加兩行，分別將 kvm5.deyu.wang 的 /public 及 /protected 掛載在 /mnt/nfsmount 及 /mnt/nfssecure，且 /mnt/nfssecure 掛載安全認證為 krb5p，版本為 v4.2。

```
1 [root@kvm7 ~]# vim /etc/fstab
[root@kvm7 ~]# tail -2 /etc/fstab
3 kvm5.deyu.wang:/public /mnt/nfsmount nfs defaults 0 0
kvm5.deyu.wang:/protected /mnt/nfssecure nfs defaults,sec=krb5p,v4.2 0 0
```

11. 使用 mount -a 依據開機掛載表 /etc/fstab，重新掛載所有裝置，沒出現錯誤訊息，表示掛載成功。

```
[root@kvm7 ~]# mount -a
```

12. 查看掛載情形；

```
1 [root@kvm7 ~]# df -Th | grep kvm5
kvm5.deyu.wang:/public      nfs4        3.1G  1.3G  1.7G  44% /mnt/
      nfsmount
3 kvm5.deyu.wang:/protected   nfs4        3.1G  1.3G  1.7G  44% /mnt/
      nfssecure
```

9.7 NFS Client 端權限測試

1. 先查看下載的 keytab 有沒有 deyu3 principal，考試時一定會有，否則用戶 deyu3 無法取得權限寫入 NFS 安全掛載目錄。

```
1 [root@kvm7 ~]# klist -kte /etc/krb5.keytab
Keytab name: FILE:/etc/krb5.keytab
3 KVNO Timestamp          Principal
-----
5 2 12/14/2015 11:54:09 nfs/kvm7.deyu.wang@DEYU.WANG (aes256-cts-hmac-
    sha1-96)
2 12/14/2015 11:54:09 nfs/kvm7.deyu.wang@DEYU.WANG (aes128-cts-hmac-
    sha1-96)
7 2 12/14/2015 11:54:09 nfs/kvm7.deyu.wang@DEYU.WANG (des3-cbc-sha1)
2 12/14/2015 11:54:09 nfs/kvm7.deyu.wang@DEYU.WANG (arcfour-hmac)
9 2 12/14/2015 11:54:09 nfs/kvm7.deyu.wang@DEYU.WANG (camellia256-cts-
    cmac)
2 12/14/2015 11:54:09 nfs/kvm7.deyu.wang@DEYU.WANG (camellia128-cts-
    cmac)
11 2 12/14/2015 11:54:09 nfs/kvm7.deyu.wang@DEYU.WANG (des-hmac-sha1)
2 12/14/2015 11:54:09 nfs/kvm7.deyu.wang@DEYU.WANG (des-cbc-md5)
13 3 12/14/2015 19:30:37 deyu3@DEYU.WANG (aes256-cts-hmac-sha1-96)
3 12/14/2015 19:30:37 deyu3@DEYU.WANG (aes128-cts-hmac-sha1-96)
15 3 12/14/2015 19:30:38 deyu3@DEYU.WANG (des3-cbc-sha1)
3 12/14/2015 19:30:38 deyu3@DEYU.WANG (arcfour-hmac)
17 3 12/14/2015 19:30:38 deyu3@DEYU.WANG (camellia256-cts-cmac)
3 12/14/2015 19:30:38 deyu3@DEYU.WANG (camellia128-cts-cmac)
19 3 12/14/2015 19:30:38 deyu3@DEYU.WANG (des-hmac-sha1)
3 12/14/2015 19:30:38 deyu3@DEYU.WANG (des-cbc-md5)
```

2. 切換成用戶 deyu3。

```
[root@kvm7 ~]# su - deyu3
2 Last login: Mon Dec 14 21:33:42 CST 2015 on pts/0
```

3. 查看掛載情形，因為 deyu3 還沒取得 Kerberos tickets，所以無法看到掛載的 /mnt/nfssecure，當然也無法對其存取。

```
[deyu3@kvm7 ~]$ df
2 df: '/mnt/' nfssecure: Permission denied
Filesystem 1K-blocks Used Available Use% Mounted on
4 /dev/mapper/vg_kvm7usb-root 3159816 1122804 1856788 38% /
devtmpfs 498588 0 498588 0% /dev
6 tmpfs 508600 0 508600 0% /dev/shm
tmpfs 508600 6736 501864 2% /run
8 tmpfs 508600 0 508600 0% /sys/fs/
cgroup
10 /dev/mapper/vg_kvm7home-vo 75231 1569 67928 3% /home
12 /dev/vda1 201388 109264 92124 55% /boot
//kvm5.deyu.wang/data 3159816 1131144 1848448 38% /mnt/multi
12 kvm5.deyu.wang:/public 3159936 1131264 1848448 38% /mnt/
nfsmount
```

4. 執行 kinit 以下載的 /etc/krb5.keytab 取得 Kerberos tickets。

```
[deyu3@kvm7 ~]$ kinit -k deyu3@DEYU.WANG
```

5. 執行 klist 列出 deyu3 principal 的 Kerberos tickets。

```
1 [deyu3@kvm7 ~]$ klist
Ticket cache: KEYRING:persistent:1000:krb_ccache_J1ic1Mg
3 Default principal: deyu3@DEYU.WANG
5 Valid starting Expires Service principal
12/14/2015 19:31:25 12/15/2015 19:31:25 krbtgt/DEYU.WANG@DEYU.WANG
```

6. 再查看掛載情形，可以看到掛載點 /mnt/nfssecure。

```
[deyu3@kvm7 ~]$ df
```

	Filesystem	1K-blocks	Used	Available	Use%	Mounted on
2	/dev/mapper/vg_kvm7usb-root	3159816	1122804	1856788	38%	/
4	devtmpfs	498588	0	498588	0%	/dev
5	tmpfs	508600	0	508600	0%	/dev/shm
6	tmpfs	508600	6736	501864	2%	/run
7	tmpfs	508600	0	508600	0%	/sys/fs/cgroup
8	/dev/mapper/vg_kvm7home-vo	75231	1569	67928	3%	/home
9	/dev/vda1	201388	109264	92124	55%	/boot
10	//kvm5.deyu.wang/data	3159816	1131144	1848448	38%	/mnt/multi
11	kvm5.deyu.wang:/public	3159936	1131264	1848448	38%	/mnt/nfsmount
12	kvm5.deyu.wang:/protected	3159936	1131264	1848448	38%	/mnt/nfssecure

7. 用 戶 deyu3 成功寫入資料。

```
[deyu3@kvm7 ~]$ echo 'deyu3' > /mnt/nfssecure/restricted/deyu3.txt
[deyu3@kvm7 ~]$ cat /mnt/nfssecure/restricted/deyu3.txt
deyu3
```

9.8 **NFSv4+kerberos 除錯

9.8.1 除錯一

1. 從 nfs server kvm5 查看 nfs/kvm7.deyu.wang@DEYU.WANG principal key 的 vno 為 2。

```
[root@kvm5 ~]# kadmin.local -q 'get_principal nfs/kvm7.deyu.wang@DEYU.WANG'
Authenticating as principal nfs/admin@DEYU.WANG with password.
Principal: nfs/kvm7.deyu.wang@DEYU.WANG
Expiration date: [never]
Last password change: Fri Dec 04 16:52:33 CST 2015
Password expiration date: [none]
Maximum ticket life: 1 day 00:00:00
Maximum renewable life: 0 days 00:00:00
Last modified: Fri Dec 04 16:52:33 CST 2015 (root/admin@DEYU.WANG)
Last successful authentication: [never]
Last failed authentication: [never]
Failed password attempts: 0
Number of keys: 8
Key: vno 2, aes256-cts-hmac-sha1-96, no salt
Key: vno 2, aes128-cts-hmac-sha1-96, no salt
Key: vno 2, des3-cbc-sha1, no salt
Key: vno 2, arcfour-hmac, no salt
Key: vno 2, camellia256-cts-cmac, no salt
Key: vno 2, camellia128-cts-cmac, no salt
```

```

1  Key: vno 2, des-hmac-sha1, no salt
21 Key: vno 2, des-cbc-md5, no salt
22 MKey: vno 1
23 Attributes:
Policy: [none]

```

2. 從 nfs client kvm7 查看 /etc/krb5.keytab 的 KVNO 為 4，與 server 查到的 vno 2 不同。

```

[root@kvm7 ~]# klist -kte /etc/krb5.keytab
2 Keytab name: FILE:/etc/krb5.keytab
KVNO Timestamp Principal
4 -----
-----
4 11/18/2015 12:18:01 nfs/kvm7.deyu.wang@DEYU.WANG (aes256-cts-hmac-
    sha1-96)
6 4 11/18/2015 12:18:01 nfs/kvm7.deyu.wang@DEYU.WANG (aes128-cts-hmac-
    sha1-96)
4 11/18/2015 12:18:01 nfs/kvm7.deyu.wang@DEYU.WANG (des3-cbc-sha1)
4 11/18/2015 12:18:01 nfs/kvm7.deyu.wang@DEYU.WANG (arcfour-hmac)
4 11/18/2015 12:18:01 nfs/kvm7.deyu.wang@DEYU.WANG (camellia256-cts-
    cmac)
10 4 11/18/2015 12:18:01 nfs/kvm7.deyu.wang@DEYU.WANG (camellia128-cts-
    cmac)
4 11/18/2015 12:18:01 nfs/kvm7.deyu.wang@DEYU.WANG (des-hmac-sha1)
12 4 11/18/2015 12:18:01 nfs/kvm7.deyu.wang@DEYU.WANG (des-cbc-md5)

```

3. 重新下載 keytab。

```
[root@kvm7 ~]# wget http://deyu.wang/kvm7.keytab -O /etc/krb5.keytab
```

4. 從 nfs client kvm7 查看 /etc/krb5.keytab 的 KVNO，與 server 查到的 vno 一樣 為 2。

```

1 [root@kvm7 ~]# klist -kte /etc/krb5.keytab
2 Keytab name: FILE:/etc/krb5.keytab
3 KVNO Timestamp Principal
4 -----
-----
5 2 09/22/2015 23:01:08 nfs/kvm7.deyu.wang@DEYU.WANG (aes256-cts-hmac-
    sha1-96)
2 09/22/2015 23:01:08 nfs/kvm7.deyu.wang@DEYU.WANG (aes128-cts-hmac-
    sha1-96)
7 2 09/22/2015 23:01:08 nfs/kvm7.deyu.wang@DEYU.WANG (des3-cbc-sha1)

```

```

9  2 09/22/2015 23:01:08 nfs/kvm7.deyu.wang@DEYU.WANG (arcfour-hmac)
9  2 09/22/2015 23:01:08 nfs/kvm7.deyu.wang@DEYU.WANG (camellia256-cts-
   cmac)
9  2 09/22/2015 23:01:08 nfs/kvm7.deyu.wang@DEYU.WANG (camellia128-cts-
   cmac)
11 2 09/22/2015 23:01:08 nfs/kvm7.deyu.wang@DEYU.WANG (des-hmac-sha1)
11 2 09/22/2015 23:01:08 nfs/kvm7.deyu.wang@DEYU.WANG (des-cbc-md5)

```

9.8.2 除錯二

- 掛載拒絕存取。

```

[root@kvm7 ~]# mount.nfs4 -o sec=krb5p,v4.2 kvm5.deyu.wang:/protected /
mnt/nfssecure
2 mount.nfs4: access denied by server while mounting kvm5.deyu.wang:/protected

```

- nfs client kvm7 再以 /etc/krb5.keytab 初始化 principal nfs/kvm7.deyu.wang@DEYU.WANG。

```
[root@kvm7 ~]# kinit -k -t /etc/krb5.keytab nfs/kvm7.deyu.wang@DEYU.WANG
```

- nfs server kvm5 再以 /etc/krb5.keytab 初始化 principal nfs/kvm5.deyu.wang@DEYU.WANG。

```
[root@kvm5 ~]# kinit -k -t /etc/krb5.keytab nfs/kvm5.deyu.wang@DEYU.WANG
```

9.8.3 除錯三

- 掛載拒絕存取，keytab 自行產生。

```

1 [root@kvm7 ~]# mount.nfs4 -o sec=krb5p,v4.2 kvm5.deyu.wang:/protected /
mnt/nfssecure
mount.nfs4: access denied by server while mounting kvm5.deyu.wang:/protected

```

- nfs server kvm5 查到 /etc/krb5.keytab 中不同時間產生的 keytab 都存在，應該只存在最新的一組。

```

[root@kvm5 ~]# klist -kte /etc/krb5.keytab
2 Keytab name: FILE:/etc/krb5.keytab
KVNO Timestamp          Principal
4 -----
2 12/04/2015 19:27:49 nfs/kvm5.deyu.wang@DEYU.WANG (aes256-cts-hmac-
sha1-96)
6 2 12/04/2015 19:27:49 nfs/kvm5.deyu.wang@DEYU.WANG (aes128-cts-hmac-
sha1-96)
8 2 12/04/2015 19:27:49 nfs/kvm5.deyu.wang@DEYU.WANG (des3-cbc-sha1)
2 12/04/2015 19:27:49 nfs/kvm5.deyu.wang@DEYU.WANG (arcfour-hmac)
2 12/04/2015 19:27:49 nfs/kvm5.deyu.wang@DEYU.WANG (camellia256-cts-
cmac)
10 2 12/04/2015 19:27:49 nfs/kvm5.deyu.wang@DEYU.WANG (camellia128-cts-
cmac)
12 2 12/04/2015 19:27:49 nfs/kvm5.deyu.wang@DEYU.WANG (des-hmac-sha1)
2 12/04/2015 19:27:50 nfs/kvm5.deyu.wang@DEYU.WANG (des-cbc-md5)
2 12/04/2015 19:32:14 nfs/kvm5.deyu.wang@DEYU.WANG (aes256-cts-hmac-
sha1-96)
14 2 12/04/2015 19:32:14 nfs/kvm5.deyu.wang@DEYU.WANG (aes128-cts-hmac-
sha1-96)
16 2 12/04/2015 19:32:14 nfs/kvm5.deyu.wang@DEYU.WANG (des3-cbc-sha1)
2 12/04/2015 19:32:14 nfs/kvm5.deyu.wang@DEYU.WANG (arcfour-hmac)
2 12/04/2015 19:32:14 nfs/kvm5.deyu.wang@DEYU.WANG (camellia256-cts-
cmac)
18 2 12/04/2015 19:32:14 nfs/kvm5.deyu.wang@DEYU.WANG (camellia128-cts-
cmac)
2 12/04/2015 19:32:14 nfs/kvm5.deyu.wang@DEYU.WANG (des-hmac-sha1)
20 2 12/04/2015 19:32:14 nfs/kvm5.deyu.wang@DEYU.WANG (des-cbc-md5)
2 12/04/2015 19:40:13 nfs/kvm5.deyu.wang@DEYU.WANG (aes256-cts-hmac-
sha1-96)
22 2 12/04/2015 19:40:13 nfs/kvm5.deyu.wang@DEYU.WANG (aes128-cts-hmac-
sha1-96)
2 12/04/2015 19:40:13 nfs/kvm5.deyu.wang@DEYU.WANG (des3-cbc-sha1)
24 2 12/04/2015 19:40:13 nfs/kvm5.deyu.wang@DEYU.WANG (arcfour-hmac)
2 12/04/2015 19:40:13 nfs/kvm5.deyu.wang@DEYU.WANG (camellia256-cts-
cmac)
26 2 12/04/2015 19:40:13 nfs/kvm5.deyu.wang@DEYU.WANG (camellia128-cts-
cmac)
2 12/04/2015 19:40:13 nfs/kvm5.deyu.wang@DEYU.WANG (des-hmac-sha1)
28 2 12/04/2015 19:40:13 nfs/kvm5.deyu.wang@DEYU.WANG (des-cbc-md5)
2 12/04/2015 20:08:50 nfs/kvm5.deyu.wang@DEYU.WANG (aes256-cts-hmac-
sha1-96)
30 2 12/04/2015 20:08:50 nfs/kvm5.deyu.wang@DEYU.WANG (aes128-cts-hmac-
sha1-96)
2 12/04/2015 20:08:50 nfs/kvm5.deyu.wang@DEYU.WANG (des3-cbc-sha1)
32 2 12/04/2015 20:08:50 nfs/kvm5.deyu.wang@DEYU.WANG (arcfour-hmac)
2 12/04/2015 20:08:50 nfs/kvm5.deyu.wang@DEYU.WANG (camellia256-cts-
cmac)
34 2 12/04/2015 20:08:51 nfs/kvm5.deyu.wang@DEYU.WANG (camellia128-cts-
cmac)
2 12/04/2015 20:08:51 nfs/kvm5.deyu.wang@DEYU.WANG (des-hmac-sha1)
36 2 12/04/2015 20:08:51 nfs/kvm5.deyu.wang@DEYU.WANG (des-cbc-md5)

```

3. nfs server kvm5 刪除 /etc/krb5.keytab 中 principal nfs/kvm5.deyu.wang@DEYU.WANG 的 keytab。

```
[root@kvm5 ~]# kadmin.local -q 'ktremove -k /etc/krb5.keytab nfs/kvm5.  
deyu.wang@DEYU.WANG'  
2 Authenticating as principal nfs/admin@DEYU.WANG with password.  
Entry for principal nfs/kvm5.deyu.wang@DEYU.WANG with kvno 2 removed  
from keytab WRFILE:/etc/krb5.keytab.  
4 Entry for principal nfs/kvm5.deyu.wang@DEYU.WANG with kvno 2 removed  
from keytab WRFILE:/etc/krb5.keytab.  
Entry for principal nfs/kvm5.deyu.wang@DEYU.WANG with kvno 2 removed  
from keytab WRFILE:/etc/krb5.keytab.  
6 Entry for principal nfs/kvm5.deyu.wang@DEYU.WANG with kvno 2 removed  
from keytab WRFILE:/etc/krb5.keytab.  
Entry for principal nfs/kvm5.deyu.wang@DEYU.WANG with kvno 2 removed  
from keytab WRFILE:/etc/krb5.keytab.  
8 Entry for principal nfs/kvm5.deyu.wang@DEYU.WANG with kvno 2 removed  
from keytab WRFILE:/etc/krb5.keytab.  
Entry for principal nfs/kvm5.deyu.wang@DEYU.WANG with kvno 2 removed  
from keytab WRFILE:/etc/krb5.keytab.  
10 Entry for principal nfs/kvm5.deyu.wang@DEYU.WANG with kvno 2 removed  
from keytab WRFILE:/etc/krb5.keytab.  
Entry for principal nfs/kvm5.deyu.wang@DEYU.WANG with kvno 2 removed  
from keytab WRFILE:/etc/krb5.keytab.  
12 Entry for principal nfs/kvm5.deyu.wang@DEYU.WANG with kvno 2 removed  
from keytab WRFILE:/etc/krb5.keytab.  
Entry for principal nfs/kvm5.deyu.wang@DEYU.WANG with kvno 2 removed  
from keytab WRFILE:/etc/krb5.keytab.  
14 Entry for principal nfs/kvm5.deyu.wang@DEYU.WANG with kvno 2 removed  
from keytab WRFILE:/etc/krb5.keytab.  
Entry for principal nfs/kvm5.deyu.wang@DEYU.WANG with kvno 2 removed  
from keytab WRFILE:/etc/krb5.keytab.  
16 Entry for principal nfs/kvm5.deyu.wang@DEYU.WANG with kvno 2 removed  
from keytab WRFILE:/etc/krb5.keytab.  
Entry for principal nfs/kvm5.deyu.wang@DEYU.WANG with kvno 2 removed  
from keytab WRFILE:/etc/krb5.keytab.  
18 Entry for principal nfs/kvm5.deyu.wang@DEYU.WANG with kvno 2 removed  
from keytab WRFILE:/etc/krb5.keytab.  
Entry for principal nfs/kvm5.deyu.wang@DEYU.WANG with kvno 2 removed  
from keytab WRFILE:/etc/krb5.keytab.  
20 Entry for principal nfs/kvm5.deyu.wang@DEYU.WANG with kvno 2 removed  
from keytab WRFILE:/etc/krb5.keytab.  
Entry for principal nfs/kvm5.deyu.wang@DEYU.WANG with kvno 2 removed  
from keytab WRFILE:/etc/krb5.keytab.  
22 Entry for principal nfs/kvm5.deyu.wang@DEYU.WANG with kvno 2 removed  
from keytab WRFILE:/etc/krb5.keytab.  
Entry for principal nfs/kvm5.deyu.wang@DEYU.WANG with kvno 2 removed  
from keytab WRFILE:/etc/krb5.keytab.  
24 Entry for principal nfs/kvm5.deyu.wang@DEYU.WANG with kvno 2 removed  
from keytab WRFILE:/etc/krb5.keytab.  
Entry for principal nfs/kvm5.deyu.wang@DEYU.WANG with kvno 2 removed  
from keytab WRFILE:/etc/krb5.keytab.  
26 Entry for principal nfs/kvm5.deyu.wang@DEYU.WANG with kvno 2 removed  
from keytab WRFILE:/etc/krb5.keytab.  
Entry for principal nfs/kvm5.deyu.wang@DEYU.WANG with kvno 2 removed
```

```

    from keytab WRFILE:/etc krb5.keytab.
28 Entry for principal nfs/kvm5.deyu.wang@DEYU.WANG with kvno 2 removed
      from keytab WRFILE:/etc krb5.keytab.
Entry for principal nfs/kvm5.deyu.wang@DEYU.WANG with kvno 2 removed
      from keytab WRFILE:/etc krb5.keytab.
30 Entry for principal nfs/kvm5.deyu.wang@DEYU.WANG with kvno 2 removed
      from keytab WRFILE:/etc krb5.keytab.
Entry for principal nfs/kvm5.deyu.wang@DEYU.WANG with kvno 2 removed
      from keytab WRFILE:/etc krb5.keytab.
32 Entry for principal nfs/kvm5.deyu.wang@DEYU.WANG with kvno 2 removed
      from keytab WRFILE:/etc krb5.keytab.
Entry for principal nfs/kvm5.deyu.wang@DEYU.WANG with kvno 2 removed
      from keytab WRFILE:/etc krb5.keytab.
34 Entry for principal nfs/kvm5.deyu.wang@DEYU.WANG with kvno 2 removed
      from keytab WRFILE:/etc krb5.keytab.

```

4. nfs server kvm5 刪除 / etc/ kvm7.keytab 中 principal nfs/ kvm7.deyu.wang@DEYU.WANG 的 keytab。

```

[root@kvm5 ~]# kadmin.local -q 'ktremove -k /etc/kvm7.keytab nfs/kvm7.
      deyu.wang@DEYU.WANG'
2 Authenticating as principal nfs/admin@DEYU.WANG with password.
Entry for principal nfs/kvm7.deyu.wang@DEYU.WANG with kvno 2 removed
      from keytab WRFILE:/etc/kvm7.keytab.
4 Entry for principal nfs/kvm7.deyu.wang@DEYU.WANG with kvno 2 removed
      from keytab WRFILE:/etc/kvm7.keytab.
Entry for principal nfs/kvm7.deyu.wang@DEYU.WANG with kvno 2 removed
      from keytab WRFILE:/etc/kvm7.keytab.
6 Entry for principal nfs/kvm7.deyu.wang@DEYU.WANG with kvno 2 removed
      from keytab WRFILE:/etc/kvm7.keytab.
Entry for principal nfs/kvm7.deyu.wang@DEYU.WANG with kvno 2 removed
      from keytab WRFILE:/etc/kvm7.keytab.
8 Entry for principal nfs/kvm7.deyu.wang@DEYU.WANG with kvno 2 removed
      from keytab WRFILE:/etc/kvm7.keytab.
Entry for principal nfs/kvm7.deyu.wang@DEYU.WANG with kvno 2 removed
      from keytab WRFILE:/etc/kvm7.keytab.
10 Entry for principal nfs/kvm7.deyu.wang@DEYU.WANG with kvno 2 removed
      from keytab WRFILE:/etc/kvm7.keytab.
Entry for principal nfs/kvm7.deyu.wang@DEYU.WANG with kvno 2 removed
      from keytab WRFILE:/etc/kvm7.keytab.
12 Entry for principal nfs/kvm7.deyu.wang@DEYU.WANG with kvno 2 removed
      from keytab WRFILE:/etc/kvm7.keytab.
Entry for principal nfs/kvm7.deyu.wang@DEYU.WANG with kvno 2 removed
      from keytab WRFILE:/etc/kvm7.keytab.
14 Entry for principal nfs/kvm7.deyu.wang@DEYU.WANG with kvno 2 removed
      from keytab WRFILE:/etc/kvm7.keytab.
Entry for principal nfs/kvm7.deyu.wang@DEYU.WANG with kvno 2 removed
      from keytab WRFILE:/etc/kvm7.keytab.
16 Entry for principal nfs/kvm7.deyu.wang@DEYU.WANG with kvno 2 removed
      from keytab WRFILE:/etc/kvm7.keytab.
Entry for principal nfs/kvm7.deyu.wang@DEYU.WANG with kvno 2 removed
      from keytab WRFILE:/etc/kvm7.keytab.

```

```

18 | Entry for principal nfs/kvm7.deyu.wang@DEYU.WANG with kvno 2 removed
      from keytab WRFILE:/etc/kvm7.keytab.
Entry for principal nfs/kvm7.deyu.wang@DEYU.WANG with kvno 2 removed
      from keytab WRFILE:/etc/kvm7.keytab.
20 | Entry for principal nfs/kvm7.deyu.wang@DEYU.WANG with kvno 2 removed
      from keytab WRFILE:/etc/kvm7.keytab.
Entry for principal nfs/kvm7.deyu.wang@DEYU.WANG with kvno 2 removed
      from keytab WRFILE:/etc/kvm7.keytab.
22 | Entry for principal nfs/kvm7.deyu.wang@DEYU.WANG with kvno 2 removed
      from keytab WRFILE:/etc/kvm7.keytab.
Entry for principal nfs/kvm7.deyu.wang@DEYU.WANG with kvno 2 removed
      from keytab WRFILE:/etc/kvm7.keytab.
24 | Entry for principal nfs/kvm7.deyu.wang@DEYU.WANG with kvno 2 removed
      from keytab WRFILE:/etc/kvm7.keytab.
Entry for principal nfs/kvm7.deyu.wang@DEYU.WANG with kvno 2 removed
      from keytab WRFILE:/etc/kvm7.keytab.
26 | Entry for principal nfs/kvm7.deyu.wang@DEYU.WANG with kvno 2 removed
      from keytab WRFILE:/etc/kvm7.keytab.
Entry for principal nfs/kvm7.deyu.wang@DEYU.WANG with kvno 2 removed
      from keytab WRFILE:/etc/kvm7.keytab.
28 | Entry for principal nfs/kvm7.deyu.wang@DEYU.WANG with kvno 2 removed
      from keytab WRFILE:/etc/kvm7.keytab.
Entry for principal nfs/kvm7.deyu.wang@DEYU.WANG with kvno 2 removed
      from keytab WRFILE:/etc/kvm7.keytab.
30 | Entry for principal nfs/kvm7.deyu.wang@DEYU.WANG with kvno 2 removed
      from keytab WRFILE:/etc/kvm7.keytab.
Entry for principal nfs/kvm7.deyu.wang@DEYU.WANG with kvno 2 removed
      from keytab WRFILE:/etc/kvm7.keytab.
32 | Entry for principal nfs/kvm7.deyu.wang@DEYU.WANG with kvno 2 removed
      from keytab WRFILE:/etc/kvm7.keytab.
Entry for principal nfs/kvm7.deyu.wang@DEYU.WANG with kvno 2 removed
      from keytab WRFILE:/etc/kvm7.keytab.
34 | Entry for principal nfs/kvm7.deyu.wang@DEYU.WANG with kvno 2 removed
      from keytab WRFILE:/etc/kvm7.keytab.

```

5. nfs server kvm5 重新產生 principal nfs/kvm5.deyu.wang@DEYU.WANG。

```

2 | [root@kvm5 ~]# kadmin.local -q "addprinc -pw 123qwe nfs/kvm5.deyu.wang"
Authenticating as principal nfs/admin@DEYU.WANG with password.
WARNING: no policy specified for nfs/kvm5.deyu.wang@DEYU.WANG;
        defaulting to no policy
4 | add_principal: Principal or policy already exists while creating "nfs/
        kvm5.deyu.wang@DEYU.WANG".

```

6. nfs server kvm5 重新產生 principal nfs/kvm7.deyu.wang@DEYU.WANG。

```

2 | [root@kvm5 ~]# kadmin.local -q "addprinc -pw 123qwe nfs/kvm7.deyu.wang"
Authenticating as principal nfs/admin@DEYU.WANG with password.
WARNING: no policy specified for nfs/kvm7.deyu.wang@DEYU.WANG;
        defaulting to no policy

```

4 || add_principal: Principal or policy already exists while creating "nfs/kvm7.deyu.wang@DEYU.WANG".

7. nfs server kvm5 重新產生 principal nfs/kvm7.deyu.wang@DEYU.WANG 的 keytab 存成 /etc/kvm7.keytab。

```
[root@kvm5 ~]# kadmin.local -q 'ktadd -k /etc/kvm7.keytab nfs/kvm7.deyu.wang@DEYU.WANG'
2 Authenticating as principal nfs/admin@DEYU.WANG with password.
Entry for principal nfs/kvm7.deyu.wang@DEYU.WANG with kvno 3, encryption type
4 aes256-cts-hmac-sha1-96 added to keytab WRFILE:/etc/kvm7.keytab.
Entry for principal nfs/kvm7.deyu.wang@DEYU.WANG with kvno 3, encryption type
6 aes128-cts-hmac-sha1-96 added to keytab WRFILE:/etc/kvm7.keytab.
Entry for principal nfs/kvm7.deyu.wang@DEYU.WANG with kvno 3, encryption type
8 des3-cbc-sha1 added to keytab WRFILE:/etc/kvm7.keytab.
Entry for principal nfs/kvm7.deyu.wang@DEYU.WANG with kvno 3, encryption type
10 arcfour-hmac added to keytab WRFILE:/etc/kvm7.keytab.
Entry for principal nfs/kvm7.deyu.wang@DEYU.WANG with kvno 3, encryption type
12 camellia256-cts-cmac added to keytab WRFILE:/etc/kvm7.keytab.
Entry for principal nfs/kvm7.deyu.wang@DEYU.WANG with kvno 3, encryption type
14 camellia128-cts-cmac added to keytab WRFILE:/etc/kvm7.keytab.
Entry for principal nfs/kvm7.deyu.wang@DEYU.WANG with kvno 3, encryption type
16 des-hmac-sha1 added to keytab WRFILE:/etc/kvm7.keytab.
Entry for principal nfs/kvm7.deyu.wang@DEYU.WANG with kvno 3, encryption type
18 des-cbc-md5 added to keytab WRFILE:/etc/kvm7.keytab.
```

8. nfs server kvm5 重新產生 principal nfs/kvm5.deyu.wang@DEYU.WANG 的 keytab 存成 /etc/kvm5.keytab。

```
[root@kvm5 ~]# kadmin.local -q 'ktadd -k /etc/kvm5.keytab nfs/kvm5.deyu.wang@DEYU.WANG'
2 Authenticating as principal nfs/admin@DEYU.WANG with password.
Entry for principal nfs/kvm5.deyu.wang@DEYU.WANG with kvno 3, encryption type
4 aes256-cts-hmac-sha1-96 added to keytab WRFILE:/etc/kvm5.keytab.
Entry for principal nfs/kvm5.deyu.wang@DEYU.WANG with kvno 3, encryption type
6 aes128-cts-hmac-sha1-96 added to keytab WRFILE:/etc/kvm5.keytab.
Entry for principal nfs/kvm5.deyu.wang@DEYU.WANG with kvno 3, encryption type
8 des3-cbc-sha1 added to keytab WRFILE:/etc/kvm5.keytab.
Entry for principal nfs/kvm5.deyu.wang@DEYU.WANG with kvno 3, encryption type
```

```

10  arcfour-hmac added to keytab WRFILE:/etc/kvm5.keytab.
   Entry for principal nfs/kvm5.deyu.wang@DEYU.WANG with kvno 3, encryption
      type
12  camellia256-cts-cmac added to keytab WRFILE:/etc/kvm5.keytab.
   Entry for principal nfs/kvm5.deyu.wang@DEYU.WANG with kvno 3, encryption
      type
14  camellia128-cts-cmac added to keytab WRFILE:/etc/kvm5.keytab.
   Entry for principal nfs/kvm5.deyu.wang@DEYU.WANG with kvno 3, encryption
      type
16  des-hmac-sha1 added to keytab WRFILE:/etc/kvm5.keytab.
   Entry for principal nfs/kvm5.deyu.wang@DEYU.WANG with kvno 3, encryption
      type
18  des-cbc-md5 added to keytab WRFILE:/etc/kvm5.keytab.

```

9. nfs server kvm5 將 /etc/kvm5.keytab 複製成 kerberos keytab 預設名稱 /etc/krb5.keytab。

```

[root@kvm5 ~]# cp /etc/kvm5.keytab /etc/krb5.keytab
2 cp: overwrite '/etc/krb5.' keytab? y

```

10. nfs client kvm7 查到目前的 /etc/krb5.keytab 中一樣有不同時間產生的 keytab，應該只存在最新的一組。

```

[root@kvm7 ~]# klist -kte /etc/krb5.keytab
2 Keytab name: FILE:/etc/krb5.keytab
3 KVNO Timestamp          Principal
4 -----
5 -----
6 2 12/04/2015 19:27:50 nfs/kvm7.deyu.wang@DEYU.WANG (aes256-cts-hmac-
7     sha1-96)
8 2 12/04/2015 19:27:50 nfs/kvm7.deyu.wang@DEYU.WANG (aes128-cts-hmac-
9     sha1-96)
10 2 12/04/2015 19:27:50 nfs/kvm7.deyu.wang@DEYU.WANG (des3-cbc-sha1)
11 2 12/04/2015 19:27:50 nfs/kvm7.deyu.wang@DEYU.WANG (arcfour-hmac)
12 2 12/04/2015 19:27:50 nfs/kvm7.deyu.wang@DEYU.WANG (camellia256-cts-
13     cmac)
14 2 12/04/2015 19:27:50 nfs/kvm7.deyu.wang@DEYU.WANG (camellia128-cts-
15     cmac)
16 2 12/04/2015 19:27:50 nfs/kvm7.deyu.wang@DEYU.WANG (des-hmac-sha1)
17 2 12/04/2015 19:27:50 nfs/kvm7.deyu.wang@DEYU.WANG (des-cbc-md5)
18 2 12/04/2015 19:32:15 nfs/kvm7.deyu.wang@DEYU.WANG (aes256-cts-hmac-
19     sha1-96)
20 2 12/04/2015 19:32:15 nfs/kvm7.deyu.wang@DEYU.WANG (aes128-cts-hmac-
21     sha1-96)
22 2 12/04/2015 19:32:15 nfs/kvm7.deyu.wang@DEYU.WANG (des3-cbc-sha1)
23 2 12/04/2015 19:32:15 nfs/kvm7.deyu.wang@DEYU.WANG (arcfour-hmac)
24 2 12/04/2015 19:32:15 nfs/kvm7.deyu.wang@DEYU.WANG (camellia256-cts-
25     cmac)
26 2 12/04/2015 19:32:15 nfs/kvm7.deyu.wang@DEYU.WANG (camellia128-cts-
27     cmac)

```

```

2 12/04/2015 19:32:15 nfs/kvm7.deyu.wang@DEYU.WANG (des-hmac-sha1)
2 12/04/2015 19:32:15 nfs/kvm7.deyu.wang@DEYU.WANG (des-cbc-md5)
2 12/04/2015 19:40:14 nfs/kvm7.deyu.wang@DEYU.WANG (aes256-cts-hmac-
sha1-96)
2 12/04/2015 19:40:14 nfs/kvm7.deyu.wang@DEYU.WANG (aes128-cts-hmac-
sha1-96)
2 12/04/2015 19:40:14 nfs/kvm7.deyu.wang@DEYU.WANG (des3-cbc-sha1)
2 12/04/2015 19:40:14 nfs/kvm7.deyu.wang@DEYU.WANG (arcfour-hmac)
2 12/04/2015 19:40:14 nfs/kvm7.deyu.wang@DEYU.WANG (camellia256-cts-
cmac)
2 12/04/2015 19:40:14 nfs/kvm7.deyu.wang@DEYU.WANG (camellia128-cts-
cmac)
2 12/04/2015 19:40:14 nfs/kvm7.deyu.wang@DEYU.WANG (des-hmac-sha1)
2 12/04/2015 19:40:14 nfs/kvm7.deyu.wang@DEYU.WANG (des-cbc-md5)
2 12/04/2015 20:08:51 nfs/kvm7.deyu.wang@DEYU.WANG (aes256-cts-hmac-
sha1-96)
2 12/04/2015 20:08:51 nfs/kvm7.deyu.wang@DEYU.WANG (aes128-cts-hmac-
sha1-96)
2 12/04/2015 20:08:51 nfs/kvm7.deyu.wang@DEYU.WANG (des3-cbc-sha1)
2 12/04/2015 20:08:51 nfs/kvm7.deyu.wang@DEYU.WANG (arcfour-hmac)
2 12/04/2015 20:08:51 nfs/kvm7.deyu.wang@DEYU.WANG (camellia256-cts-
cmac)
2 12/04/2015 20:08:51 nfs/kvm7.deyu.wang@DEYU.WANG (camellia128-cts-
cmac)
2 12/04/2015 20:08:51 nfs/kvm7.deyu.wang@DEYU.WANG (des-hmac-sha1)
2 12/04/2015 20:08:51 nfs/kvm7.deyu.wang@DEYU.WANG (des-cbc-md5)

```

11. nfs client kvm7 從 nfs server kvm5 複製 principal nfs/ kvm7.deyu.wang@DEYU.WANG 的 keytab kvm7.keytab 存成 /etc/krb5.keytab。

```

[root@kvm7 ~]# scp kvm5.deyu.wang:/etc/kvm7.keytab /etc/krb5.keytab
2 root@kvm5.deyu.wang's password:
kvm7.keytab                                         100% 2242      2.2KB/s
00:00

```

12. nfs client kvm7 列出 keytab / etc/ krb5.keytab 中 principal nfs/ kvm7.deyu.wang@DEYU.WANG 只有一組。

```

1 [root@kvm7 ~]# klist -kte /etc/krb5.keytab
Keytab name: FILE:/etc/krb5.keytab
3 KVNO Timestamp          Principal
----- -----
5 3 12/04/2015 20:16:57 nfs/kvm7.deyu.wang@DEYU.WANG (aes256-cts-hmac-
sha1-96)
3 12/04/2015 20:16:57 nfs/kvm7.deyu.wang@DEYU.WANG (aes128-cts-hmac-
sha1-96)
7 3 12/04/2015 20:16:58 nfs/kvm7.deyu.wang@DEYU.WANG (des3-cbc-sha1)
3 12/04/2015 20:16:58 nfs/kvm7.deyu.wang@DEYU.WANG (arcfour-hmac)
9 3 12/04/2015 20:16:58 nfs/kvm7.deyu.wang@DEYU.WANG (camellia256-cts-
cmac)

```

```

3 12/04/2015 20:16:58 nfs/kvm7.deyu.wang@DEYU.WANG (camellia128-cts-
  cmac)
11 3 12/04/2015 20:16:58 nfs/kvm7.deyu.wang@DEYU.WANG (des-hmac-sha1)
  3 12/04/2015 20:16:58 nfs/kvm7.deyu.wang@DEYU.WANG (des-cbc-md5)

```

13. nfs client kvm7 再安全掛載成功。

```

[root@kvm7 ~]# mount.nfs4 -o sec=krb5p,v4.2 kvm5.deyu.wang:/protected /
  mnt/nfssecure/ -vvv
2 mount.nfs4: timeout set for Fri Dec 4 14:16:29 2015
mount.nfs4: trying text-based options 'sec=krb5p,v4.2,addr
  =192.168.122.5,clientaddr=192.168.122.7'

```

9.8.4 除錯四 –解題

1. 掛載拒絕存取，keytab 重新下載。

```

1 [root@kvm7 ~]# mount.nfs4 -o sec=krb5p,v4.2 kvm5.deyu.wang:/protected /
  mnt/nfssecure
mount.nfs4: access denied by server while mounting kvm5.deyu.wang:/protected

```

2. nfs server kvm5 查到 /etc/krb5.keytab 中不同時間產生的 keytab 都存在，應該只存在最新的一組。

```

[root@kvm5 ~]# klist -kte /etc/krb5.keytab
2 Keytab name: FILE:/etc/krb5.keytab
  KVNO Timestamp           Principal
4 -----
5 09/22/2015 22:16:17 nfs/kvm5.deyu.wang@DEYU.WANG (aes256-cts-hmac-
  sha1-96)
6 09/22/2015 22:16:17 nfs/kvm5.deyu.wang@DEYU.WANG (aes128-cts-hmac-
  sha1-96)
8 09/22/2015 22:16:17 nfs/kvm5.deyu.wang@DEYU.WANG (des3-cbc-sha1)
5 09/22/2015 22:16:17 nfs/kvm5.deyu.wang@DEYU.WANG (arcfour-hmac)
5 09/22/2015 22:16:18 nfs/kvm5.deyu.wang@DEYU.WANG (camellia256-cts-
  cmac)
10 5 09/22/2015 22:16:18 nfs/kvm5.deyu.wang@DEYU.WANG (camellia128-cts-
  cmac)
12 5 09/22/2015 22:16:18 nfs/kvm5.deyu.wang@DEYU.WANG (des-hmac-sha1)
5 09/22/2015 22:16:18 nfs/kvm5.deyu.wang@DEYU.WANG (des-cbc-md5)
14 6 09/22/2015 22:16:22 nfs/kvm7.deyu.wang@DEYU.WANG (aes256-cts-hmac-
  sha1-96)
6 09/22/2015 22:16:22 nfs/kvm7.deyu.wang@DEYU.WANG (aes128-cts-hmac-
  sha1-96)

```

```

6 09/22/2015 22:16:22 nfs/kvm7.deyu.wang@DEYU.WANG (des3-cbc-sha1)
16 6 09/22/2015 22:16:22 nfs/kvm7.deyu.wang@DEYU.WANG (arcfour-hmac)
6 09/22/2015 22:16:22 nfs/kvm7.deyu.wang@DEYU.WANG (camellia256-cts-
cmac)
18 6 09/22/2015 22:16:22 nfs/kvm7.deyu.wang@DEYU.WANG (camellia128-cts-
cmac)
6 09/22/2015 22:16:22 nfs/kvm7.deyu.wang@DEYU.WANG (des-hmac-sha1)
20 6 09/22/2015 22:16:22 nfs/kvm7.deyu.wang@DEYU.WANG (des-cbc-md5)
2 09/22/2015 22:56:27 nfs/kvm5.deyu.wang@DEYU.WANG (aes256-cts-hmac-
sha1-96)
22 2 09/22/2015 22:56:27 nfs/kvm5.deyu.wang@DEYU.WANG (aes128-cts-hmac-
sha1-96)
2 09/22/2015 22:56:27 nfs/kvm5.deyu.wang@DEYU.WANG (des3-cbc-sha1)
24 2 09/22/2015 22:56:28 nfs/kvm5.deyu.wang@DEYU.WANG (arcfour-hmac)
2 09/22/2015 22:56:28 nfs/kvm5.deyu.wang@DEYU.WANG (camellia256-cts-
cmac)
26 2 09/22/2015 22:56:28 nfs/kvm5.deyu.wang@DEYU.WANG (camellia128-cts-
cmac)
2 09/22/2015 22:56:28 nfs/kvm5.deyu.wang@DEYU.WANG (des-hmac-sha1)
28 2 09/22/2015 22:56:28 nfs/kvm5.deyu.wang@DEYU.WANG (des-cbc-md5)

```

3. nfs server kvm5 刪除 /etc/krb5.keytab 中 principal nfs/kvm5.deyu.wang@DEYU.WANG 的 keytab。

```

[root@kvm5 ~]# kadmin.local -q 'ktremove -k /etc/krb5.keytab nfs/kvm5.
deyu.wang@DEYU.WANG'
2 Authenticating as principal nfs/admin@DEYU.WANG with password.
Entry for principal nfs/kvm5.deyu.wang@DEYU.WANG with kvno 5 removed
from keytab WRFILE:/etc/krb5.keytab.
4 Entry for principal nfs/kvm5.deyu.wang@DEYU.WANG with kvno 5 removed
from keytab WRFILE:/etc/krb5.keytab.
Entry for principal nfs/kvm5.deyu.wang@DEYU.WANG with kvno 5 removed
from keytab WRFILE:/etc/krb5.keytab.
6 Entry for principal nfs/kvm5.deyu.wang@DEYU.WANG with kvno 5 removed
from keytab WRFILE:/etc/krb5.keytab.
Entry for principal nfs/kvm5.deyu.wang@DEYU.WANG with kvno 5 removed
from keytab WRFILE:/etc/krb5.keytab.
8 Entry for principal nfs/kvm5.deyu.wang@DEYU.WANG with kvno 5 removed
from keytab WRFILE:/etc/krb5.keytab.
Entry for principal nfs/kvm5.deyu.wang@DEYU.WANG with kvno 5 removed
from keytab WRFILE:/etc/krb5.keytab.
10 Entry for principal nfs/kvm5.deyu.wang@DEYU.WANG with kvno 5 removed
from keytab WRFILE:/etc/krb5.keytab.

```

4. nfs server kvm5 重新下載 keytab 存成 /etc/krb5.keytab。

```
[root@kvm5 ~]# wget http://deyu.wang/kvm5.keytab -O /etc/krb5.keytab
```

5. nfs server kvm5 查到 /etc/krb5.keytab 只有一組 KVNO 為 2 的 keytab。

```

1 [root@kvm5 ~]# klist -kte /etc/krb5.keytab
Keytab name: FILE:/etc/krb5.keytab
3 KVNO Timestamp Principal
-----
5 2 12/05/2015 14:25:15 nfs/kvm5.deyu.wang@DEYU.WANG (aes256-cts-hmac-
   sha1-96)
2 12/05/2015 14:25:16 nfs/kvm5.deyu.wang@DEYU.WANG (aes128-cts-hmac-
   sha1-96)
7 2 12/05/2015 14:25:16 nfs/kvm5.deyu.wang@DEYU.WANG (des3-cbc-sha1)
2 12/05/2015 14:25:16 nfs/kvm5.deyu.wang@DEYU.WANG (arcfour-hmac)
9 2 12/05/2015 14:25:16 nfs/kvm5.deyu.wang@DEYU.WANG (camellia256-cts-
   cmac)
2 12/05/2015 14:25:16 nfs/kvm5.deyu.wang@DEYU.WANG (camellia128-cts-
   cmac)
11 2 12/05/2015 14:25:16 nfs/kvm5.deyu.wang@DEYU.WANG (des-hmac-sha1)
2 12/05/2015 14:25:16 nfs/kvm5.deyu.wang@DEYU.WANG (des-cbc-md5)

```

6. nfs client kvm7 重新下載 keytab 存成 /etc/krb5.keytab。

```
[root@kvm7 ~]# wget http://deyu.wang/kvm7.keytab -O /etc/krb5.keytab
```

7. nfs client kvm7 查到目前的 /etc/krb5.keytab 只有一組 KVNO 為 2 的 keytab。

```

1 [root@kvm7 ~]# klist -kte /etc/krb5.keytab
Keytab name: FILE:/etc/krb5.keytab
3 KVNO Timestamp Principal
-----
5 2 12/05/2015 14:25:16 nfs/kvm7.deyu.wang@DEYU.WANG (aes256-cts-hmac-
   sha1-96)
2 12/05/2015 14:25:16 nfs/kvm7.deyu.wang@DEYU.WANG (aes128-cts-hmac-
   sha1-96)
7 2 12/05/2015 14:25:16 nfs/kvm7.deyu.wang@DEYU.WANG (des3-cbc-sha1)
2 12/05/2015 14:25:16 nfs/kvm7.deyu.wang@DEYU.WANG (arcfour-hmac)
9 2 12/05/2015 14:25:16 nfs/kvm7.deyu.wang@DEYU.WANG (camellia256-cts-
   cmac)
2 12/05/2015 14:25:16 nfs/kvm7.deyu.wang@DEYU.WANG (camellia128-cts-
   cmac)
11 2 12/05/2015 14:25:16 nfs/kvm7.deyu.wang@DEYU.WANG (des-hmac-sha1)
2 12/05/2015 14:25:16 nfs/kvm7.deyu.wang@DEYU.WANG (des-cbc-md5)

```

8. nfs client kvm7 再安全掛載成功。

```

1 [root@kvm7 ~]# mount.nfs4 -o sec=krb5p,v4.2 kvm5.deyu.wang:/protected /
   mnt/nfssecure/
2 [root@kvm7 ~]# df -h | grep kvm5

```

```
[root@kvm5.deyu.wang ~]# mount.nfs4 -o sec=krb5p,v4.2 kvm5.deyu.wang:/protected /mnt/nfssecure
```

9.8.5 除錯五

- NFS secure 無法掛載。

```
1 [root@kvm7 ~]# mount.nfs4 -o sec=krb5p,v4.2 kvm5.deyu.wang:/protected /mnt/nfssecure
mount.nfs4: access denied by server while mounting kvm5.deyu.wang:/protected
```

- nfs client kvm7 以 /etc/krb5.keytab 初始化 principal nfs/kvm7.deyu.wang@DEYU.WANG，出現密碼不正確訊息。

```
2 [root@kvm7 ~]# kinit -k -t /etc/krb5.keytab nfs/kvm7.deyu.wang@DEYU.WANG
kinit: Password incorrect while getting initial credentials
```

- nfs server kvm5 以 /etc/krb5.keytab 初始化 principal nfs/kvm5.deyu.wang@DEYU.WANG，也出現密碼不正確訊息。

```
2 [root@kvm5 ~]# kinit -k -t /etc/krb5.keytab nfs/kvm5.deyu.wang@DEYU.WANG
kinit: Password incorrect while getting initial credentials
```

- /etc/krb5.keytab 有問題，在 deyu.wang 主機使用 sudo 或以 root 身份執行 resetkrb5.sh 重新產生 keytab。

```
[dywang@dywIssd ~]$ sudo /var/ftp/pub/centos6/bin/resetkrb5.sh
```

- 如果沒有此 resetkrb5.sh 腳本，也可以執行以下腳本中的命令。

```
1 [root@dywIssd ~]# cat /var/ftp/pub/centos6/bin/resetkrb5.sh
#!/bin/bash
3 kvmpw=123qwe
sshpass -p$kvmpw ssh -o StrictHostKeyChecking=no -i /root/bin/kvm_id_rsa \
5 -T kvm5.deyu.wang 'bash -s' < /root/bin/setkrb5.sh 5
sshpass -p$kvmpw ssh -o StrictHostKeyChecking=no -i /root/bin/kvm_id_rsa \
7 -T kvm7.deyu.wang 'bash -s' < /root/bin/setkrb5.sh 7
sshpass -p$kvmpw scp -o StrictHostKeyChecking=no -i /root/bin/kvm_id_rsa \
\
```

```
9 || kvm5.deyu.wang:/etc/kvm?.keytab /var/ftp/pub/  
exit 0
```

6. 重新產生 keytab 後 kvm7 與 kvm5 都必須重新下載並重新啓動 nfs 及 nfs server 服務。

Chapter 10

Apache 2.4 HTTP Server

10.1 Apache HTTP 簡介

1. Apache HTTP Server（簡稱 Apache）是 Apache 軟體基金會的一個開放原始碼的網頁伺服器。
2. Apache HTTPD 是最常使用的網頁伺服器，跨平台且安全性高，支援 Perl，Python，Tcl，和 PHP。
3. http 協定預設使用 80/TCP port 以明文傳送資料，另有 https 協定使用 443/tcp port 以 TLS/SSL 加密方式傳送資料。
4. CentOS 7 預設 httpd 2.4 版與 CentOS 6 的 httpd 2.2 版，在設定上有些不同，所以本文件以 httpd 2.4 為例，進行架設說明。
5. 2.2 與 2.4 存取限制語法比較：

(a) apache 2.4 存取限制的語法舉例如下：

- i. 限制所有存取

```
Require all denied
```

- ii. 允許所有存取

```
1 | Require all granted
```

- iii. 允許所有在 deyu.wang 網域的主機存取

```
1 | Require host deyu.wang
```

(b) apache 2.4 以 ip 限制存取的語法可適用 ipv6，當然也還適用 ipv4：

- i. 完整 ip

```
1 | Require ip 10.1.2.3
  | Require ip 192.168.1.140 192.168.1.141
```

ii. 部分 ip，允許指定網段。

```
2 | Require ip 10.1
  | Require ip 10 172.20 192.168.2
```

iii. 網段/遮罩，允許指定網段。

```
Require ip 10.1.0.0/255.255.0.0
```

iv. 網段/遮罩數字，允許指定網段。

```
1 | Require ip 10.1.0.0/16
```

10.2 http 網頁架設

1. 安裝套件。

```
1 | [root@kvm5 ~]# yum install httpd -y
```

2. 下載 web.html 做為網頁主檔。

```
1 | [root@kvm5 ~]# wget http://dywang.csie.cyut.edu.tw/materials/web.html -O
  | /var/www/html/index.html
```

3. 編輯 httpd 設定檔，限制網頁只允許 deyu.wang 網域存取，不允許其他 IP 存取。

```
1 | [root@kvm5 ~]# vim /etc/httpd/conf/httpd.conf
  | [root@kvm5 ~]# grep deyu.wang -A1 -B25 /etc/httpd/conf/httpd.conf | \
  | egrep -v '(#|^$)'
  | <Directory "/var/www/html">
  |   Options Indexes FollowSymLinks
  |   AllowOverride None
  |   #Require host deyu.wang
```

```
9  Require ip 192.168.122
    </Directory>
```

4. 啓動 httpd 服務，並設定開機啓動。

```
1 [root@kvm5 ~]# systemctl enable httpd.service
2 ln -s '/usr/lib/systemd/system/httpd.service' '/etc/systemd/system/multi-
3 [root@kvm5 ~]# systemctl start httpd
```

5. 從外部主機 deyu.wang 連線 kvm5.deyu.wang，回應無法連線。

```
1 [root@dywH ~]# curl http://kvm5.deyu.wang
curl: (7) couldn't connect to host
```

6. firewall 必須開增加 hhttp 服務外部主機才能連線，由於還要架設 https 網頁，所以 https 也同時加入。

```
1 [root@kvm5 ~]# firewall-cmd --permanent --add-service=http --add-service=
2           https
3 success
4 [root@kvm5 ~]# firewall-cmd --reload
5 success
```

7. 檢查防火牆，已加入 hhttp 及 https 服務。

```
1 [root@kvm5 ~]# firewall-cmd --list-all
2 public (default)
3   interfaces:
4   sources:
5   services: dhcpcv6-client http https ssh
6   ports:
7   masquerade: no
8   forward-ports:
9   icmp-blocks:
10  rich rules:
```

8. 再次從外部主機 deyu.wang 連線 kvm5.deyu.wang，已可成功連線。

```
1 [root@dywH ~]# curl http://kvm5.deyu.wang
2 web test
```

9. 在外部主機 deyu.wang 以 root 增加網卡 virbr0:1 指定 ip 為 192.168.111.1。

```
[root@dywIssd ~]# ifconfig virbr0:1 192.168.111.1 up
```

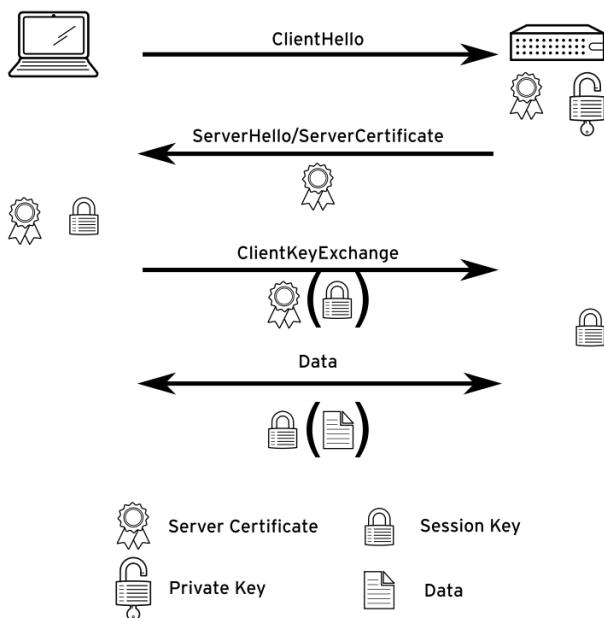
10. 再次從外部主機 deyu.wang 以 192.168.111.1 網卡連線 kvm5.deyu.wang，拒絕存取。

```
1 [root@dywIssd ~]# curl --interface 192.168.111.1 http://kvm5.deyu.wang/
2 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.1//EN" "http://www.w3.org/TR/
3   xhtml11/DTD/xhtml11.dtd"><html><head>
4 <meta http-equiv="content-type" content="text/html; charset=UTF-8">
5   <title>Apache HTTP Server Test Page powered by CentOS</title>
6   <meta http-equiv="Content-Type" content="text/html; charset=UTF-
7     -8">
8
9   <!-- Bootstrap -->
10  <link href="/noindex/css/bootstrap.min.css" rel="stylesheet">
11  <link rel="stylesheet" href="noindex/css/open-sans.css" type="text/
    css" />
12  .....
13  </body></html>
```

10.3 * 建立 TLS 憑證

1. 本節不是課程範圍，但要建立 HTTPS 網站前必須有 TLS 憑證，本節為產生方式說明。
2. Transport Layer Security (TLS) 是一種網路加密通信的方式。TLS 是 Secure Sockets Layer (SSL) 的接續協定，TLS 允許用戶端與伺服器端的互相驗證。
3. TLS 以憑證為概念，憑證包含：公鑰、伺服器身份、憑證頒發單位的簽名。對應的私鑰永遠不會公開，任何使用私鑰加密的密鑰數據只能用公鑰來解密，反之亦然。加密通信流程：
 - (a) 用戶端交握訊息給要連線的伺服器，訊息有包含時間戳的 32 位元隨機數字、加密協定、用戶端支援的加密方式。
 - (b) 伺服器回應訊息包含另一個包含時間戳的 32 位元隨機數字、加密協定、用戶端加密方式，另也將伺服器憑證傳送給用戶端。

- (c) 用戶端經由檢查身分確認伺服器，檢查所有簽章是否為用戶端所有，如果確認就使用交換的 32 位元隨機數字產生會話密鑰 (session key) 及一密鑰。用戶端用伺服器的公鑰加密會話密鑰，再傳送給伺服器。
- (d) 伺服器使用私鑰解開會話密鑰，伺服器與用戶端就可開始此會話密鑰連線，傳送加密資料並加解密。



4. 安裝 openssl。

```
1 [root@kvm5 ~]# yum install -y openssl
```

5. 若先前已有舊憑證，都先移除。

```
1 [root@kvm5 ~]# CADIR=/etc/pki/CA
[root@kvm5 ~]# rm -f /etc/pki/tls/certs/kvm5.*
3 [root@kvm5 ~]# rm -rf $CADIR/*
```

6. 設定自己的憑證管理中心 (Certification Authority, CA) 環境。

```
1 [root@kvm5 ~]# mkdir -p /etc/pki/CA/private 2>/dev/null
[root@kvm5 ~]# mkdir -p $CADIR/{certs,newcerts}
3 [root@kvm5 ~]# touch $CADIR/index.txt
[root@kvm5 ~]# /bin/cp /etc/pki/tls/openssl.cnf $CADIR/
5 [root@kvm5 ~]# echo 01 > $CADIR/serial
```

7. 產生自己的憑證管理中心 (Certification Authority , CA)。

```

1 [root@kvm5 ~]# cd $CADIR
2 [root@kvm5 ~]# openssl req -days 999 -new -x509 -nodes \
3 -out cacert.pem \
4 -keyout private/cakey.pem \
5 -subj '/C=TW/ST=Taiwan/L=CYUT/O=CSIE/OU=DEYU/CN=kvm5.deyu.wang'
```

8. 產生自己 CA 簽章的 TLS 憑證。

```

1 [root@kvm5 ~]# cd /etc/pki/CA/certs
2 [root@kvm5 ~]# openssl req -days 999 -new -nodes \
3 -out kvm5.csr -keyout kvm5.key \
4 -subj '/C=TW/ST=Taiwan/L=CYUT/O=CSIE/OU=DEYU/CN=kvm5.deyu.wang'
5 [root@kvm5 ~]# openssl ca -batch -config ../openssl.cnf -days 999 \
6 -in kvm5.csr -out kvm5.crt -keyfile $CADIR/private/cakey.pem \
7 -cert $CADIR/cacert.pem -policy policy_anything
```

9. 安裝憑證到網站要使用的目錄。

```

1 [root@kvm5 ~]# cp $CADIR/cacert.pem /etc/pki/tls/certs/kvm5.pem
2 [root@kvm5 ~]# cp kvm5.crt /etc/pki/tls/certs/kvm5.crt
3 [root@kvm5 ~]# cp kvm5.key /etc/pki/private/kvm5.key
```

10.4 HTTPS 安全網站架設

1. 安裝 mod_ssl 套件。

```

1 [root@kvm5 ~]# yum install -y mod_ssl
```

2. 編輯 httpd SSL 模組 mod_ssl 提供的設定檔 /etc/httpd/conf.d/ssl.conf，取消 SSLCertificateChainFile 註解。如果指定的憑證檔檔名想要改成比較好識別的方式，也可一併修改。

```

1 [root@kvm5 ~]# vim /etc/httpd/conf.d/ssl.conf
2 [root@kvm5 ~]# egrep '^SSL(Certi|Engine)' /etc/httpd/conf.d/ssl.conf
3 SSLEngine on
4 SSLCertificateFile /etc/pki/tls/certs/localhost.crt
5 SSLCertificateKeyFile /etc/pki/tls/private/localhost.key
6 SSLCertificateChainFile /etc/pki/tls/certs/server-chain.crt
```

3. 考試時不用自行產生憑證，請由 `http://dywang.csie.cyut.edu.tw/materials/kvm5.crt` 下載簽證檔；請由 `http://dywang.csie.cyut.edu.tw/materials/kvm5.key` 下載簽證私鑰檔；請由 `http://dywang.csie.cyut.edu.tw/materials/kvm5.pem` 下載簽證認證檔。並分別存成 `/etc/httpd/conf.d/ssl.conf` 指定的位置及檔名。

```
1 [root@kvm5 ~]# wget http://dywang.csie.cyut.edu.tw/materials/kvm5.crt \
2 -O /etc/pki/tls/certs/localhost.crt
3 [root@kvm5 ~]# wget http://dywang.csie.cyut.edu.tw/materials/kvm5.key \
4 -O /etc/pki/tls/private/localhost.key
5 [root@kvm5 ~]# wget http://dywang.csie.cyut.edu.tw/materials/kvm5.pem \
6 -O /etc/pki/tls/certs/server-chain.crt
```

4. 重新啓動 httpd 服務。

```
[root@kvm5 ~]# systemctl restart httpd.service
```

5. 使用 curl 以管理中心憑證 `server-chain.crt` 成功連線 `https://kvm5.deyu.wang`。

```
1 [root@kvm5 ~]# curl --cacert /etc/pki/tls/certs/server-chain.crt https://kvm5.deyu.wang/
web test
```

6. 切換到 `kvm7.deyu.wang` 主機測試，先下載管理中心憑證 `kvm5.pem`。練習時可依指示使用 `wget` 下載。

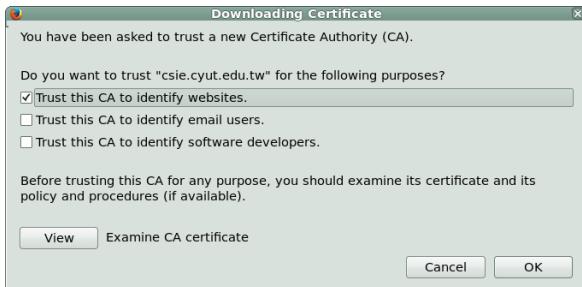
```
[root@kvm7 ~]# wget http://dywang.csie.cyut.edu.tw/materials/kvm5.pem
```

7. 使用 curl 以管理中心憑證 `kvm5.pem` 成功連線 `https://kvm5.deyu.wang`。如果連線有問題，除了確定 `kvm5.deyu.wang` 防火牆有開啟 https 服務外，最重要的兩台主機都必須先校時，因為憑證都有設定有效期限，且練習的憑證往往都是最近才產生，只要系統時間不對可能就無法認證。

```
1 [root@kvm7 ~]# curl --cacert kvm5.pem https://kvm5.deyu.wang
web test
```

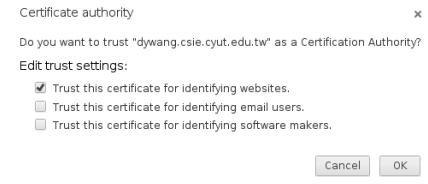
8. 如果要用 firefox 連線，必須先下載網站提供的管理中心憑證，匯入到 firefox。勾選 `Trust this CA to identify websites`。

```
1 Edit → Preferences
2 Advanced → Certificates tab
View Certificates (Authorities) → Import button
```



9. google chrome 連線，必須先下載網站提供的管理中心憑證，以下列步驟匯入 chrome。勾選 Trust this certificate for identify websites。

- 1 Settings → Show advanced settings...
- 2 HTTPS/SSL → Manage Certificates...
- 3 Authorities → Import button



10.5 Virtual Host 虛擬主機

1. virtual host：一台 Apache Server 可提供多個網址，但必須配合 DNS，提供這台伺服器的 ip 對應多個 domain name。本系統每一虛擬機都至少有 kvmX.deyu.wang 及 wwwX.deyu.wang 兩個網域名稱。Virtual Host 的設定可參考以下文件：

```

1 [root@kvm5 ~]# egrep -v '(#|^$)' /usr/share/doc/httpd-2.4.6/httpd-vhosts
2 .conf
3 <VirtualHost *:@@Port@@>
4   ServerAdmin webmaster@dummy-host.example.com
5   DocumentRoot "@@ServerRoot@@/docs/dummy-host.example.com"
6   ServerName dummy-host.example.com
7   ServerAlias www.dummy-host.example.com
8   ErrorLog "/var/log/httpd/dummy-host.example.com-error_log"
9   CustomLog "/var/log/httpd/dummy-host.example.com-access_log" common
10 </VirtualHost>
11 <VirtualHost *:@@Port@@>
12   ServerAdmin webmaster@dummy-host2.example.com
13   DocumentRoot "@@ServerRoot@@/docs/dummy-host2.example.com"
14   ServerName dummy-host2.example.com
15   ErrorLog "/var/log/httpd/dummy-host2.example.com-error_log"
16   CustomLog "/var/log/httpd/dummy-host2.example.com-access_log" common
17 </VirtualHost>

```

2. 編輯 httpd.conf 加入 VirtualHost 段落，apache 2.4 的 httpd.conf 檔中沒有 VirtualHost 範例，要自行輸入，不過語法與其他段落一樣，關鍵字 VirtualHost 設定檔已出現，所以不會有什麼困擾。**apache 2.4 不需要再另外以 NameVirtualHost 啓動 VirtualHost。**，原始主機名稱 kvm5.deyu.wang 根目錄 /var/www/html，加入另一主機名稱 www5.deyu.wang 的根目錄為 /var/www/virtual

```
[root@kvm5 ~]# vim /etc/httpd/conf/httpd.conf
2 [root@kvm5 ~]# tail -8 /etc/httpd/conf/httpd.conf
<Virtualhost *:80>
4   Documentroot /var/www/html
      Servername kvm5.deyu.wang
6 </Virtualhost>
<VirtualHost *:80>
8   DocumentRoot /var/www/virtual
      ServerName www5.deyu.wang
10 </VirtualHost>
```

3. 設定完必須啓動 httpd 服務或 reload 設定參數。

```
[root@kvm5 ~]# systemctl restart httpd.service
```

4. 建立 www5.deyu.wang 網站根目錄，並下載 virtual.html 作為 www5.deyu.wang 網站的首頁。

```
1 [root@kvm5 ~]# mkdir /var/www/virtual
[root@kvm5 ~]# wget http://dywang.csie.cyut.edu.tw/materials/virtual.
      html -O /var/www/virtual/index.html
```

5. 讓用戶 deyu1 可以寫入目錄 /var/www/virtual。

```
[root@kvm5 ~]# chown deyu1 /var/www/virtual
```

6. 測試 kvm5.deyu.wang 及 www5.deyu.wang 兩台 virtual host 都成功連線。

```
1 [root@kvm5 ~]# curl http://kvm5.deyu.wang
      web test
3 [root@kvm5 ~]# curl http://www5.deyu.wang
      virtual test
```

10.6 架設動態網頁

1. 動態網頁要求如：

- (a) 網址為 dynamic5.deyu.wang。
- (b) 端口為 8989。
- (c) 動態網頁內容，請從 <http://dywang.csie.cyut.edu.tw/materials/webapp.wsgi> 下載。
- (d) 用戶端連線 <http://dynamic5.deyu.wang:8989/> 時，應該會以下載的 webapp.wsgi 產生頁面。
- (e) <http://dynamic5.deyu.wang:8989/> 可以讓 deyu.wang 網域內的主機存取。

2. 安裝 mod_wsgi 模組。

```
[root@kvm5 ~]# yum install mod_wsgi -y
```

3. 編輯 httpd 設定檔增加 Listen port 8989。

```
1 [root@kvm5 ~]# vim /etc/httpd/conf/httpd.conf
2 [root@kvm5 ~]# grep ^Listen /etc/httpd/conf/httpd.conf
3 Listen 80
4 Listen 8989
```

4. 編輯 httpd 設定檔增加虛擬主機 dynamic5.deyu.wang 的 port 為 8989，且其根目錄為 /var/www/html/webapp.wsgi。

```
1 [root@kvm5 ~]# vim /etc/httpd/conf/httpd.conf
2 [root@kvm5 ~]# tail -10 /etc/httpd/conf/httpd.conf
3 IncludeOptional conf.d/*.conf
4 <Virtualhost *:80>
5   Documentroot    /var/www/html
6   Servername      kvm5.deyu.wang
7 </Virtualhost>
8 <Virtualhost *:8989>
9   Documentroot    /var/www/html
10  Servername      dynamic5.deyu.wang
11  WSGIScriptAlias / /var/www/html/webapp.wsgi
12 </Virtualhost>
```

5. 防火牆開放 8989/tcp port 後重新載入。

```
1 [root@kvm5 ~]# firewall-cmd --permanent --zone=public --add-port=8989/
2   tcp
3 success
4 [root@kvm5 ~]# firewall-cmd --reload
```

4 || success

6. 增加 8989/tcp port 的 selinux port type 為 http_port_t，在 SELinux 啓動的情況下，不執行此動作則無法正常啓動 httpd 服務。

```
[root@kvm5 ~]# semanage port -a -t http_port_t -p tcp 8989
```

7. 重新載入 httpd 服務設定。

```
1 [root@kvm5 ~]# systemctl reload httpd.service
```

8. 下載 webapp.wsgi，並存成 /var/www/html/webapp.wsgi。

```
1 [root@kvm5 ~]# wget http://dywang.csie.cyut.edu.tw/materials/webapp.wsgi  
-O /var/www/html/webapp.wsgi
```

9. 在 kvm5.deyu.wang 成功連線 http://dynamic5.deyu.wang:8989/。

```
2 [root@kvm5 ~]# curl http://dynamic5.deyu.wang:8989/  
Content generated for: 192.168.122.5 (deyu.wang)  
[root@kvm5 ~]#
```

10. 在 kvm7.deyu.wang 成功連線 http://dynamic5.deyu.wang:8989/。

```
1 [root@kvm7 ~]# curl http://dynamic5.deyu.wang:8989/  
Content generated for: 192.168.122.7 (deyu.wang)  
3 [root@kvm7 ~]#
```

10.7 網站存取限制

1. 在 kvm5.deyu.wang 網站根目錄下，建立限制存取測試目錄 confidential，限制只有 kvm5.deyu.wang 這台主機可以存取，其他主機都不能存取。

```
1 [root@kvm5 ~]# mkdir /var/www/html/confidential
```

2. 下載 private.html 作為限制存取目錄 confidential 的首頁。

```
1 [root@kvm5 ~]# wget http://dywang.csie.cyut.edu.tw/materials/private.html \
2 -O /var/www/html/confidential/index.html
```

3. 編輯 httpd 設定檔增加以下幾行，限制只有 kvm5.deyu.wang 這台主機可以存取 www5.deyu.wang。如果 host kvm5.deyu.wang 有問題，請改成 ip 192.168.122.5

```
1 [root@kvm5 ~]# vim /etc/httpd/conf/httpd.conf
2 <Directory "/var/www/html/confidential">
3     #Require host kvm5.deyu.wang
4     Require ip 192.168.122.5
5 </Directory>
```

4. 重新載入 httpd 服務設定。

```
1 [root@kvm5 ~]# systemctl reload httpd.service
```

5. 在 kvm5.deyu.wang 成功連線 confidential 目錄的首頁。

```
1 [root@kvm5 ~]# curl http://kvm5.deyu.wang/confidential/
2 private test
```

6. 在 kvm7.deyu.wang 無法連線 kvm5.deyu.wang 的 confidential 目錄首頁。

```
1 [root@kvm7 ~]# curl http://kvm5.deyu.wang/confidential/
2 <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
3 <html><head>
4 <title>403 Forbidden</title>
5 </head><body>
6 <h1>Forbidden</h1>
7 <p>You don't have permission to access /confidential/
8 on this server.</p>
9 </body></html>
```

Chapter 11

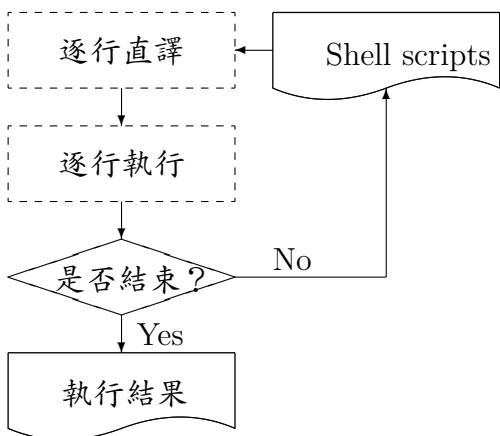
Shell Script

11.1 前言

1. 何謂 Shell Script

- (a) 文字介面下讓使用者與系統溝通的一個工具介面。
- (b) 利用 shell 的功能所寫的一支『程式 (program)』。
- (c) 將一些 shell 的語法與指令寫成純文字檔；
- (d) 可搭配正規表示法、管線命令與資料流重導向等功能；
- (e) shell script 更提供陣列、迴圈、條件與邏輯判斷等重要功能；
- (f) 使用者也可以直接以 shell 來撰寫程式。

2. Shell scripts 執行流程：



3. 為什麼要學習 shell scripts?

- (a) 自動化管理的重要依據：自動處理分析主機狀態，若有問題才通知。
- (b) 追蹤與管理系統的重要工作：Linux 系統的服務 (services) 啓動的介面，在目錄 /etc/init.d/ 下，所有的檔案都是 scripts。
- (c) 簡單入侵偵測功能：主動分析系統登錄檔。
- (d) 連續指令單一化：彙整在 command line 下達的連續指令。例如：/etc/rc.d/rc.local 裡的資料。

- (e) 簡易的資料處理：處理數據資料的比對，文字資料的處理等。
- (f) 跨平台支援與學習歷程較短：幾乎所有的 Unix Like 上面都可以跑 shell script。
- (g) shell script 是一項很好的系統管理工具，但數值運算的速度較慢，且使用的 CPU 資源較多。

4. Scripts 撰寫注意事項：

- (a) 指令與參數間的多個空白會被忽略掉；
- (b) 空白行及 [tab] 不會被理會；
- (c) 讀到 [Enter] 符號，就開始執行該行命令；
- (d) 一行的內容太多，可以使用 \[Enter] 來延伸至下一行；
- (e) 加在 # 後面的字，全部被視為註解。

5. 如何執行檔案 shell.sh？

- (a) 將 shell.sh 加上可讀與執行 (rx) 的權限，就能夠以 ./shell.sh 執行；
- (b) 直接以 sh shell.sh 方式執行。

6. 程式內容的宣告：script 當中，除了第一行的 #! 是用來宣告 shell 外，其他的 # 都是『註解』。

7. 可以利用指令 exit 讓程式中斷，並且回傳一個數值給系統。

8. 利用 exit n 的功能，可以自訂錯誤訊息。

11.2 善用判斷式

1. 指令 test 測試的標誌

測試的標誌	代表意義
1.	關於某個檔名的『類型』偵測(存在與否)，如 test -e filename
-e	該『檔名』是否存在？(常用)
-f	該『檔名』是否為檔案(file)？(常用)
-d	該『檔名』是否為目錄(directory)？(常用)
-b	該『檔名』是否為一個 block device 裝置？
-c	該『檔名』是否為一個 character device 裝置？
-S	該『檔名』是否為一個 Socket 檔案？
-p	該『檔名』是否為一個 FIFO (pipe) 檔案？
-L	該『檔名』是否為一個連結檔？
2.	關於檔案的權限偵測，如 test -r filename
-r	偵測該檔名是否具有『可讀』的屬性？
-w	偵測該檔名是否具有『可寫』的屬性？
-x	偵測該檔名是否具有『可執行』的屬性？
-u	偵測該檔名是否具有『SUID』的屬性？
-g	偵測該檔名是否具有『SGID』的屬性？
-k	偵測該檔名是否具有『Sticky bit』的屬性？
-s	偵測該檔名是否為『非空白檔案』？
3.	兩個檔案之間的比較，如：test file1 -nt file2

-nt	(newer than) 判斷 file1 是否比 file2 新
-ot	(older than) 判斷 file1 是否比 file2 舊
-ef	判斷 file1 與 file2 是否為同一檔案。
4.	關於兩個整數之間的判定，例如 <code>test n1 -eq n2</code>
-eq	兩數值相等 (equal)
-ne	兩數值不等 (not equal)
-gt	n1 大於 n2 (greater than)
-lt	n1 小於 n2 (less than)
-ge	n1 大於等於 n2 (greater than or equal)
-le	n1 小於等於 n2 (less than or equal)
5.	判定字串的資料
<code>test -z string</code>	判定字串是否為 0 ? 若 string 為空字串，則為 true
<code>test -n string</code>	判定字串是否非為 0 ? 若 string 為空字串，則為 false。
<code>test str1 == str2</code>	判定 str1 是否等於 str2 ，若相等回傳 true
<code>test str1 != str2</code>	判定 str1 是否不等於 str2 ，若相等回傳 false
6.	多重條件判定，例如： <code>test -r filename -a -x filename</code>
-a	(and) 兩狀況同時成立。例如 <code>test -r file -a -x file</code> ， 則 file 同時具有 r 與 x 權限時，才回傳 true。
-o	(or) 兩狀況任何一個成立。例如 <code>test -r file -o -x file</code> ， 則 file 具有 r 或 x 權限時，就可回傳 true。
!	反相狀態，如 <code>test ! -x file</code> ，當 file 不具有 x 時，回傳 true

2. 利用判斷符號 []，判斷變數 \$HOME 是否為空字串？

```
1 [root@linux ~]# [ -z "$HOME" ]
```

3. 在中括號 [] 內的每個元件都需要有空白鍵來分隔，假設空白鍵使用 来表示，則：

```
1 [ "$HOME" == "$MAIL" ]
[ "$HOME" == "$MAIL" ]↑↑↑↑
```

4. Shell script 的預設變數 (\$0, \$1, ...) 對應：

```
1 /path/to/scriptname opt1 opt2 opt3 opt4 ...
    $0          $1      $2      $3      $4      ...
3
5 [root@linux ~]# /etc/init.d/crond restart
## $0 為 /etc/init.d/，crond $1 為 restart
```

11.3 條件判斷式

1. if ... then 語法：

```

1 if [ 條件判斷式 ]; then 當條件判斷式成立時，可以進行的指令工作內容；  

3 fi

```

2. 條件判斷式的判斷方法：

```

1 && 代表； AND  

1 || 代表； OR

```

3. if ... then ... else 語法：

```

1 if [ 條件判斷式 ]; then 當條件判斷式成立時，可以進行的指令工作內容；  

2 else 當條件判斷式不成立時，可以進行的指令工作內容；  

4 fi

```

4. if ... then ... elif ... then ... else 語法：

```

1 if [ 條件判斷式一 ]; then 當條件判斷式一成立時，可以進行的指令工作內容；  

3 elif [ 條件判斷式二 ]; then 當條件判斷式二成立時，可以進行的指令工作內容；  

5 else 當條件判斷式一與二均不成立時，可以進行的指令工作內容；  

7 fi

```

5. case esac 語法：

```

1 case 變數名稱$ in  

2   "第一個變數內容") 程式段  

3     ;;  

4     #兩個分號## (;;) 來代表該程式段落的結束  

5   "第二個變數內容") 程式段  

6     ;;  

7   *) 不包含第一個變數內容與第二個變數內容的其他程式執行段  

8     ;;  

9     exit 1  

10    ;;  

11 esac

```

11.4 迴圈 (loop)

1. while....do....done 語法：當 condition 條件成立時，進行迴圈，直到 condition 條件不成立才停止。

```

1  while [ condition ]
2   do 程式段落
4   done

```

2. until....do....done 語法：當 condition 條件成立時，終止迴圈，否則持續進行迴圈的程式段。

```

1  until [ condition ]
2   do 程式段落
4   done

```

3. 已知進行迴圈次數：for...do...done 語法：

```

1  for (( 初始值; 限制值; 執行步階 ))
2   do 程式段
4   done

```

4. for 括號內的三串內容意義為：

- (a) 初始值：某個變數在迴圈當中的起始值，直接以類似 `i=1` 設定；
- (b) 限制值：當變數的值在這個限制值的範圍內，就繼續進行迴圈。例如 `i<=100`；
- (c) 執行步階：每作一次迴圈時，變數的變化量。例如 `i=i+1`。

5. 非數字的迴圈

```

1  for var in con1 con2 con3 ...
2   do 程式段
4   done 第一次迴圈時，
6   $var 的內容為 con1 ; 第二次迴圈時，
8   $var 的內容為 con2 ; 第三次迴圈時，
10  $var 的內容為 con3 ;
12  ....

```

11.5 範例

11.5.1 範例一

1. 寫一腳本 /root/mkusers.sh 從一用戶名稱列表的檔案讀取用戶名稱，在 kvm5.deyu.wang 產生此用戶名稱之帳號，同時滿足下列要求：
 - (a) 腳本必須提供一個外部參數輸入，用來指定用戶名稱列表的檔案名稱。
 - (b) 如果直接執行此腳本，而沒有提供參數，此腳本將提示訊息： Usage: /root/mkusers.sh <userfile>，還後退出並回傳一適當的值。
 - (c) 如果指定一不存在的用戶名稱檔，此腳本將提示訊息： Input file not found，還後退出並回傳一適當的值。
 - (d) 用戶建立的登入 shell 為 /bin/false。
 - (e) 此腳本不需要為產生的帳號設定密碼。
 - (f) 可以下載 <http://dywang.csie.cyut.edu.tw/materials/ulist.txt> 用戶名稱列表檔進行測試。
 - (g) 測試產生的帳號刪不刪除都可以。

2. 編輯腳本

```
1 [root@kvm5 ~]# vim /root/mkusers.sh
```

3. 第一種寫法。

```
1 [root@kvm5 ~]# vim /root/mkusers.sh
2 [root@kvm5 ~]# cat /root/mkusers.sh
3 #!/bin/bash
4 [ -z "$1" ] && echo "Usage: /root/mkusers.sh <userfile>" && exit 1
5 ! test -f "$1" && echo "Input file not found" && exit 2
6 while read line; do
7     useradd -s /bin/false $line
8 done < $1
9 exit 0
```

4. 第二種寫法。

```
1 [root@kvm5 ~]# vim /root/mkusers.sh
2 [root@kvm5 ~]# cat /root/mkusers.sh
3 #!/bin/bash
4 if [ -z "$1" ]; then
5     echo "Usage: /root/mkusers.sh <userfile>"
6     exit 1
7 elif ! test -f "$1"; then
8     echo "Input file not found"
9     exit 2
10 else
```

```

11      while read line; do
12          useradd -s /bin/false $line
13      done < $1
14  fi
15  exit 0

```

5. 第三種寫法。

```

1 [root@kvm5 ~]# vim /root/mkusers.sh
2 [root@kvm5 ~]# cat /root/mkusers.sh
3 #!/bin/bash
4 if [ -z "$1" ]; then
5     echo "Usage: /root/mkusers.sh <userfile>"
6     exit 1
7 elif ! test -f "$1"; then
8     echo "Input file not found"
9     exit 2
10 else
11     for line in $(cat $1); do
12         useradd -s /bin/false $line
13     done
14 fi
15 exit 0

```

6. 變更腳本屬性為所有人都可執行。

```

1 [root@kvm5 ~]# chmod a+x /root/mkusers.sh

```

7. 執行腳本，不提供參數，顯示訊息如要求，且回傳值為 1，不能是 0。

```

1 [root@kvm5 ~]# /root/mkusers.sh
2 Usage: /root/mkusers.sh <userfile>
3 [root@kvm5 ~]# echo $?
4 1

```

8. 執行腳本，提供的參數檔案不存在，顯示訊息如要求，且回傳值為 2，不能是 0。

```

1 [root@kvm5 ~]# /root/mkusers.sh abc123
2 Input file not found
3 [root@kvm5 ~]# echo $?
4 2

```

9. 下載用戶名稱列表測試檔 ulist.txt。

```
[root@kvm5 ~]# wget http://dywang.csie.cyut.edu.tw/materials/ulist.txt
```

10. 執行腳本，提供測試檔 ulist.txt，正常執行回傳值為 0。

```
1 [root@kvm5 ~]# /root/mkusers.sh ulist.txt
2 [root@kvm5 ~]# echo $?
3 0
```

11. 查看用戶名稱列表測試檔 ulist.txt 內的用戶名稱。

```
1 [root@kvm5 ~]# cat ulist.txt
2 david
3 linda
4 peter
5 rita
```

12. 以 getent passwd 查看系統是否有依用戶名稱列表測試檔 ulist.txt，產生帳號且其登入 shell 為 /bin/false。

```
1 [root@kvm5 ~]# for u in $(cat ulist.txt); do getent passwd $u; done
2 david:x:1003:1003::/home/david:/bin/false
3 linda:x:1004:1004::/home/linda:/bin/false
4 peter:x:1005:1005::/home/peter:/bin/false
5 rita:x:1006:1006::/home/rita:/bin/false
```

11.5.2 範例二

1. 寫一腳本 /root/program 提供以下功能：

- (a) 執行 /root/program kernel 回應 user 到 stdout。
- (b) 執行 /root/program user 回應 kernel 到 stdout。
- (c) 執行 /root/program 不加任何參數或參數不是 user 或 kernel 時，輸出以下結果到 stderr：
/root/program kernel|user

2. 編輯 /root/program

```
1 [root@kvm5 ~]# vim /root/program
```

3. 第一種寫法

```

1 [root@kvm5 ~]# cat /root/program
2 #!/bin/bash
3
4 [ "$1" == "kernel" ] && echo user && exit
5 [ "$1" == "user" ] && echo kernel && exit
6 echo "/root/program kernel|user" >&2
7 exit 0

```

4. 第二種寫法

```

1 #!/bin/bash
2
3 if [ "$1" == "kernel" ]; then
4     echo user
5 elif [ "$1" == "user" ]; then
6     echo kernel
7 else
8     echo "/root/program kernel|user" >&2
9 fi
10 exit 0

```

5. 第三種寫法

```

1 #!/bin/bash
2
3 case "$1" in
4     "kernel")
5         echo user
6         ;;
7     "user")
8         echo kernel
9         ;;
10    *)
11        echo "/root/program kernel|user" >&2
12        ;;
13 esac
14 exit 0

```

6. 變更腳本屬性為所有人都可執行。

```
[root@kvm5 ~]# chmod a+x /root/program
```

7. 執行腳本 /root/program，參數 kernel，回應 user 如要求。

```
1 [root@kvm5 ~]# /root/program kernel  
user
```

8. 執行腳本 /root/program，參數 user，回應 kernel 如要求。

```
2 [root@kvm5 ~]# /root/program user  
kernel
```

9. 執行腳本 /root/program 不提供參數，顯示訊息如要求，而且將 stderr 導向到 /dev/null 後，螢幕上沒有任何回應，證明回應的訊息確實是送到 stderr，而不是 stdout。

```
2 [root@kvm5 ~]# /root/program  
/root/program kernel|user  
[root@kvm5 ~]# /root/program 2>/dev/null
```

10. 執行腳本 /root/program 提供參數 abcd，顯示訊息如要求，而且將 stderr 導向到 /dev/null 後，螢幕上沒有任何回應，證明回應的訊息確實是送到 stderr，而不是 stdout。

```
1 [root@kvm5 ~]# /root/program abcd  
/root/program kernel|user  
3 [root@kvm5 ~]# /root/program abcd 2>/dev/null  
[root@kvm5 ~]#
```

Chapter 12

iSCSI Storage

12.1 iSCSI 簡介

1. Internet Small Computer System Interface (iSCSI) 是一種經由網路 IP，以 TCP/IP 協定模擬一個 SCSI 高性能本地儲存空間，提供遠端儲存空間的資料傳輸及管理。
2. iSCSI 協定設置為 client-server 架構，Client 系統設定 initiator 傳送 SCSI 命令到遠端伺服器儲存 targets。
3. 在 client 存取的 iSCSI targets 就像本地端未格式化的儲存空間。
4. 連接的伺服器數量無限（原來的 SCSI-3 的上限是 15）；
5. 原分散在各伺服器的儲存裝置，可統一到 iSCSI 的伺服器上。
6. iSCSI 元件名稱說明：

名稱	說明
initiator	iSCSI client，必須是唯一的 IQN。
target	iSCSI 儲存來源，來自 iSCSI server，必須是唯一的 IQN，iSCSI server 可以同時提供多個 target。
ACL	Access Control List，設定 initiator 的存取限制。
discovery	查詢列出 targets。
IQN	iSCSI Qualified Name，不可重複的名字，格式為： iqn.YYYY-MM.com.reversed.domain[:optional_string]
login	認證到 target 或 LUN 成為 client。
LUN	Logical Unit Number，target 中區塊裝置的編號。
node	任何 iSCSI initiator 或 target。
portal	target 或 initiator 建立連線的 ip 及 port。
TPG	Target Portal Group，iSCSI target listen 的 IP addresses 及 TCP ports 集合。

12.2 Server Target 架設

1. 安裝套件

```
[root@kvm5 ~]# yum -y install targetcli
```

2. 設定開機啓動 target 服務。

```
1 [root@kvm5 ~]# systemctl enable target.service
ln -s '/usr/lib/systemd/system/target.service' '/etc/systemd/system/
multi-user.target.wants/target.service'
```

3. 啓動 target 服務。

```
[root@kvm5 ~]# systemctl start target.service
```

4. 防火牆開啓 3260/tcp port。

```
1 [root@kvm5 ~]# firewall-cmd --permanent --add-port=3260/tcp
success
```

5. 重新載入防火牆設定。

```
2 [root@kvm5 ~]# firewall-cmd --reload
success
```

6. 列出永久的防火牆設定，已開啓 3260/tcp port。

```
2 [root@kvm5 ~]# firewall-cmd --permanent --list-all
public (default)
interfaces:
sources:
services: dhcpc6-client http https kerberos mountd nfs rpc-bind ssh
ports: 3260/tcp 464/tcp 749/tcp
masquerade: no
forward-ports:
icmp-blocks:
rich rules:
```

7. 查看目前系統的硬碟為 /dev/vda。

```
2 [root@kvm5 ~]# lsblk
NAME      MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
vda       252:0    0   4G  0 disk --
4 vda1     252:1    0 200M  0 part /boot --
vda2     252:2    0 3.4G  0 part --
6 vg_kvm5usb-swap 253:0    0 124M  0 lvm  [SWAP] --
vg_kvm5usb-root 253:1    0 3.1G  0 lvm  /
8 vda3     252:3    0 130M  0 part --
```

vg_kvm5home-vo 253:2 0 80M 0 lvm /home
--

8. 從硬碟 /dev/vda 中分割出一個 lvm 分割區。

```

1 [root@kvm5 ~]# fdisk /dev/vda
2 Welcome to fdisk (util-linux 2.23.2).
3
4 Changes will remain in memory only, until you decide to write them.
5 Be careful before using the write command.
6
7 Command (m for help): p
8
9 Disk /dev/vda: 4294 MB, 4294967296 bytes, 8388608 sectors
10 Units = sectors of 1 * 512 = 512 bytes
11 Sector size (logical/physical): 512 bytes / 512 bytes
12 I/O size (minimum/optimal): 512 bytes / 512 bytes
13 Disk label type: dos
14 Disk identifier: 0x000f2281
15
16
17      Device Boot      Start        End      Blocks   Id  System
18 /dev/vda1    *        2048     411647     204800   83  Linux
19 /dev/vda2            411648    7579647    3584000   8e  Linux LVM
20 /dev/vda3            7579648   7845887     133120   8e  Linux LVM
21
22 Command (m for help): n
23 Partition type:
24      p   primary (3 primary, 0 extended, 1 free)
25      e   extended
26 Select (default e): e
27 Selected partition 4
28 First sector (7845888-8388607, default 7845888):
29 Using default value 7845888
30 Last sector, +sectors or +size{K,M,G} (7845888-8388607, default 8388607)
31 :
32 Using default value 8388607
33 Partition 4 of type Extended and of size 265 MiB is set
34
35 Command (m for help): n
36 All primary partitions are in use
37 Adding logical partition 5
38 First sector (7847936-8388607, default 7847936):
39 Using default value 7847936
40 Last sector, +sectors or +size{K,M,G} (7847936-8388607, default 8388607)
41   :
42 Using default value 100M
43 Partition 5 of type Linux and of size 100 MiB is set
44
45 Command (m for help): p
46
47 Disk /dev/vda: 4294 MB, 4294967296 bytes, 8388608 sectors
48 Units = sectors of 1 * 512 = 512 bytes
49 Sector size (logical/physical): 512 bytes / 512 bytes
50 I/O size (minimum/optimal): 512 bytes / 512 bytes

```

```

49 Disk label type: dos
Disk identifier: 0x000f2281

51   Device Boot   Start     End   Blocks  Id System
51   /dev/vda1 *      2048    411647  204800  83 Linux
53   /dev/vda2          411648  7579647 3584000  8e Linux LVM
55   /dev/vda3          7579648 7845887 133120   8e Linux LVM
55   /dev/vda4          7845888 8388607 271360    5 Extended
57   /dev/vda5          7847936 8052735 102400  83 Linux

57
59 Command (m for help): t
59 Partition number (1-5, default 5):
61 Hex code (type L to list all codes): 8e
61 Changed type of partition 'Linux' to 'Linux LVM'

63 Command (m for help): w
63 The partition table has been altered!
65
67 Calling ioctl() to re-read partition table.

67
69 WARNING: Re-reading the partition table failed with error 16: Device or
       resource busy.
69 The kernel still uses the old table. The new table will be used at
       the next reboot or after you run partprobe(8) or kpartx(8)
71 Syncing disks.

```

9. 執行 partprobe 偵測新的分割區。

```
1 [root@kvm5 ~]# partprobe
```

10. 建立一個 10M 的 logical volume，因預設 pe 大小為 4M，故真正的 lv 大小為 3 個 pe，也就是 12M。

```

1 [root@kvm5 ~]# pvcreate /dev/vda5
1   Physical volume "/dev/vda5" successfully created
3 [root@kvm5 ~]# vgcreate iscsi_vg /dev/vda5
3   Volume group "iscsi_vg" successfully created
5 [root@kvm5 ~]# lvcreate -n iscsi_vol -L 10M iscsi_vg
5   Rounding up size to full physical extent 12.00 MiB
7   Logical volume "iscsi_vol" created.

```

11. 進入 targetcli 命令環境產生 iSCSI target。

```

1 [root@kvm5 ~]# targetcli
1   targetcli shell version 2.1.fb37
3   Copyright 2011-2013 by Datera, Inc and others.
3   For help on commands, type 'help'.
5

```

/>

12. 將之前建立的 lv `iscsi_vol` 設定名為 `kvm5.disk1` 的 block-type backing store。

```
1 /backstores> /backstores/block create kvm5.disk1 /dev/iscsi_vg/iscsi_vol
2 Created block storage object kvm5.disk1 using /dev/iscsi_vg/iscsi_vol.
```

13. 產生 target `iqn.2015-08.wang.deyu:kvm5` 的 iSCSI Qualified Name (IQN)，名稱自動設為 `tpg1`。

```
1 /backstores> /iscsi create iqn.2015-08.wang.deyu:kvm5
2 Created target iqn.2015-08.wang.deyu:kvm5.
3 Created TPG 1.
4 Global pref auto_add_default_portal=true
Created default portal listening on all IPs (0.0.0.0), port 3260.
```

14. 產生可存取 `tpg1` 的用戶端 (initiator) 為 `iqn.2015-08.wang.deyu:kvm7`。

```
1 /backstores> /iscsi/iqn.2015-08.wang.deyu:kvm5/tpg1/acls create iqn
2 .2015-08.wang.deyu:kvm7
Created Node ACL for iqn.2015-08.wang.deyu:kvm7
```

15. 產生 LUN，指定其為先前定義名為 `kvm5.disk1` 的 device。

```
1 /backstores> /iscsi/iqn.2015-08.wang.deyu:kvm5/tpg1/luns create /
2 backstores/block/kvm5.disk1
3 Created LUN 0.
Created LUN 0->0 mapping in node ACL iqn.2015-08.wang.deyu:kvm7
```

16. 產生 target 開放的門戶為 `192.168.122.5` 在 port `3260`，若執行時出現錯誤，表示系統已自動產生 `0.0.0.0:3260` 的門戶。

```
1 /> /iscsi/iqn.2015-08.wang.deyu:kvm5/tpg1/portals create 192.168.122.5
2 Using default IP port 3260
3 Could not create NetworkPortal in configFS.
```

17. 先刪除 `0.0.0.0:3260` 的門戶。

```
1 /> /iscsi/iqn.2015-08.wang.deyu:kvm5/tpg1/portals delete 0.0.0.0 3260
Deleted network portal 0.0.0.0:3260
```

18. 成功產生 target 開放的門戶為 192.168.122.5 在 port 3260。

```

1 /> /iscsi/iqn.2015-08.wang.deyu:kvm5/tpg1/portals create 192.168.122.5
2 Using default IP port 3260
3 Created network portal 192.168.122.5:3260.
4 />

```

19. 查看整個設定。

```

1 /> ls
2 o- /
3   .....
4     [...]
5   o- backstores
6     .....
7       [....]
8   | o- block ..... [Storage
9     Objects: 1]
10  | | o- kvm5.disk1 ... [/dev/iscsi_vg/iscsi_vol (12.0MiB) write-thru
11    activated]
12  | o- fileio ..... [Storage
13    Objects: 0]
14  | o- pscsi ..... [Storage
15    Objects: 0]
16  | o- ramdisk ..... [Storage
17    Objects: 0]
18  o- iscsi ..... [Targets: 1]
19  | o- iqn.2015-08.wang.deyu:kvm5 ..... [TPGs: 1]
20  | | o- tpg1 ..... [no-gen-acls,
21    no-auth]
22  |   o- acls ..... [ACLs: 1]
23  |     | o- iqn.2015-08.wang.deyu:kvm7 ..... [Mapped
24    LUNs: 1]
25  |       o- mapped_lun0 ..... [lun0 block/kvm5.
26    disk1 (rw)]
27  |         o- luns ..... [LUNs: 1]
28  |           | o- lun0 ..... [block/kvm5.disk1 (/dev/iscsi_vg/
29    iscsi_vol)]
30  |           o- portals ..... [Portals: 1]
31  |             o- 192.168.122.5:3260
32  |               ..... [OK]
33 o- loopback ..... [Targets: 0]

```

20. 退出 targetcli。

```

1  /> exit
Global pref auto_save_on_exit=true
3  Last 10 configs saved in /etc/target/backup.
Configuration saved to /etc/target/saveconfig.json

```

12.3 Client Initiator 設定

1. Client kvm7.deyu.wang 先安裝 iscsi-initiator 工具。

```
[root@kvm7 ~]# yum install iscsi-initiator-utils -y
```

2. 設定開機啓動 iscsi 及 iscsid 服務。

```

1  [root@kvm7 ~]# systemctl enable iscsid.service iscsi.service
ln -s '/usr/lib/systemd/system/iscsid.service' '/etc/systemd/system/
multi-user.target.wants/iscsid.service'

```

3. 設定 iSCSI client initiator 名稱，此名稱為 server targetcli acls 產生的 iqn.2015-08.wang.deyu:kvm7，一定要相同才能存取。

```

2  [root@kvm7 ~]# vim /etc/iscsi/initiatorname.iscsi
[root@kvm7 ~]# cat /etc/iscsi/initiatorname.iscsi
InitiatorName=iqn.2015-08.wang.deyu:kvm7

```

4. 重新啓動 iscsi 及 iscsid 服務。

```
1  [root@kvm7 ~]# systemctl restart iscsi.service iscsid.service
```

5. 未發現 iscsi target 前 /var/lib/iscsi/nodes 目錄中是空的。

```
1  [root@kvm7 ~]# ll /var/lib/iscsi/nodes/
total 0
```

6. 使用 iscsi 管理命令 iscsadm 發現 server kvm5.deyu.wang 可用的 target，名稱為 iqn.2015-08.wang.deyu:kvm5。

```

2  [root@kvm7 ~]# iscsadm -m discovery -t st -p 192.168.122.5
192.168.122.5:3260,1 iqn.2015-08.wang.deyu:kvm5

```

7. 使用 iscsiadadm -m discovery 發現 iscsi target 後 /var/lib/iscsi/nodes 目錄中出現發的 target iqn 目錄，目錄中有 default 檔記錄各個參數。

```
[root@kvm7 ~]# ll /var/lib/iscsi/nodes/
2 total 4
3 drw-----. 3 root root 4096 Jul 10 15:26 iqn.2015-08.wang.deyu:kvm5
4
5 [root@kvm7 ~]# cat /var/lib/iscsi/nodes/inqn.2015-08.wang.deyu\:kvm5
6     /192.168.122.5\,3260\,1/default
7 # BEGIN RECORD 6.2.0.874-7
8 node.name = iqn.2015-08.wang.deyu:kvm5
9 node.tpgt = 1
10 node.startup = automatic
11 node.leading_login = No
12 iface.iscsi_ifacename = default
13 iface.transport_name = tcp
14 iface.vlan_id = 0
15 iface.vlan_priority = 0
16 iface.iface_num = 0
17 iface.mtu = 0
18 iface.port = 0
19 iface.tos = 0
20 iface.ttl = 0
21 iface.tcp_wsf = 0
22 iface.tcp_timer_scale = 0
23 iface.def_task_mgmt_timeout = 0
24 iface.erl = 0
25 iface.max_receive_data_len = 0
26 iface.first_burst_len = 0
27 iface.max_outstanding_r2t = 0
28 iface.max_burst_len = 0
29 node.discovery_address = 192.168.122.5
30 node.discovery_port = 3260
31 node.discovery_type = send_targets
32 node.session.initial_cmdsn = 0
33 node.session.initial_login_retry_max = 8
34 node.session.xmit_thread_priority = -20
35 node.session.cmds_max = 128
36 node.session.queue_depth = 32
37 node.session.nr_sessions = 1
38 node.session.auth.authmethod = None
39 node.session.timeo.replacement_timeout = 120
40 node.session.err_timeo.abort_timeout = 15
41 node.session.err_timeo.lu_reset_timeout = 30
42 node.session.err_timeo.tgt_reset_timeout = 30
43 node.session.err_timeo.host_reset_timeout = 60
44 node.session.iscsi.FastAbort = Yes
45 node.session.iscsi.InitialR2T = No
46 node.session.iscsi.ImmediateData = Yes
47 node.session.iscsi.FirstBurstLength = 262144
48 node.session.iscsi.MaxBurstLength = 16776192
49 node.session.iscsi.DefaultTime2Retain = 0
50 node.session.iscsi.DefaultTime2Wait = 2
51 node.session.iscsi.MaxConnections = 1
52 node.session.iscsi.MaxOutstandingR2T = 1
```

```

52 || node.session.iscsi.ERL = 0
53 | node.session.scan = auto
54 | node.conn[0].address = 192.168.122.5
55 | node.conn[0].port = 3260
56 | node.conn[0].startup = manual
57 | node.conn[0].tcp.window_size = 524288
58 | node.conn[0].tcp.type_of_service = 0
59 | node.conn[0].timeo.logout_timeout = 15
60 | node.conn[0].timeo.login_timeout = 15
61 | node.conn[0].timeo.auth_timeout = 45
62 | node.conn[0].timeo.noop_out_interval = 5
63 | node.conn[0].timeo.noop_out_timeout = 5
64 | node.conn[0].iscsi.MaxXmitDataSegmentLength = 0
65 | node.conn[0].iscsi.MaxRecvDataSegmentLength = 262144
66 | node.conn[0].iscsi.HeaderDigest = None
67 | node.conn[0].iscsi.IFMarker = No
68 | node.conn[0].iscsi.OFMarker = No
# END RECORD

```

8. 登入 iqn.2015-08.wang.deyu:kvm5。

```

1 [root@kvm7 ~]# iscsiadadm -m node -T iqn.2015-08.wang.deyu:kvm5 -p
2   192.168.122.5 -1
3 Logging in to [iface: default, target: iqn.2015-08.wang.deyu:kvm5,
4   portal: 192.168.122.5,3260] (multiple)
5 3 Login to [iface: default, target: iqn.2015-08.wang.deyu:kvm5, portal:
6    192.168.122.5,3260] successful.

```

9. 查看硬碟，多出一顆 sda。

```

1 [root@kvm7 ~]# lsblk
2 NAME      MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
3 sda        8:0    0 12M  0 disk 
4 vda        252:0   0   8G  0 disk --
5 vda1       252:1   0  96M  0 part /boot
6 vda2       252:2   0  3.1G 0 part --
7 vg_kvm7usb-swap 253:0   0 124M  0 lvm   [SWAP] --
8 vg_kvm7usb-root 253:1   0  2.8G 0 lvm   /
9 vda3       252:3   0 130M  0 part --
10 vg_kvm7home-vo 253:2   0 120M  0 lvm   /home

```

10. 在 /dev/sda 分割一個 10M 的分割區，type 為 Linux。

```

1 [root@kvm7 ~]# fdisk /dev/sda
2 Welcome to fdisk (util-linux 2.23.2).
3
4 Changes will remain in memory only, until you decide to write them.
  Be careful before using the write command.

```

```

6 Device does not contain a recognized partition table
8 Building a new DOS disklabel with disk identifier 0xc497bbc1.

10 Command (m for help): p

12 Disk /dev/sda: 12 MB, 12582912 bytes, 24576 sectors
Units = sectors of 1 * 512 = 512 bytes
14 Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 4194304 bytes
16 Disk label type: dos
Disk identifier: 0xc497bbc1

18
20      Device Boot      Start        End      Blocks   Id  System
22
24 Command (m for help): n
22 Partition type:
24     p   primary (0 primary, 0 extended, 4 free)
26     e   extended
28 Select (default p):
26 Using default response p
30 Partition number (1-4, default 1):
32 First sector (1-24575, default 1):
34 Using default value 1
36 Last sector, +sectors or +size{K,M,G} (1-24575, default 24575): +10M
38 Partition 1 of type Linux and of size 10 MiB is set

32
34 Command (m for help): p

36 Disk /dev/sda: 12 MB, 12582912 bytes, 24576 sectors
38 Units = sectors of 1 * 512 = 512 bytes
40 Sector size (logical/physical): 512 bytes / 512 bytes
42 I/O size (minimum/optimal): 512 bytes / 4194304 bytes
44 Disk label type: dos
46 Disk identifier: 0xc497bbc1

42
44      Device Boot      Start        End      Blocks   Id  System
46 /dev/sda1            1       20481      10240+  83  Linux

44
46 Command (m for help): w
48 The partition table has been altered!

48 Calling ioctl() to re-read partition table.
Syncing disks.

```

11. 使用 partprobe 偵測 /dev/sda 新的分割區。

```
1 [root@kvm7 ~]# partprobe /dev/sda
```

12. 格式化 /dev/sda1 為 ext4。

```
1 [root@kvm7 ~]# mkfs.ext4 /dev/sda1
```

13. 建立掛載目錄 /mnt/data。

```
1 [root@kvm7 ~]# mkdir /mnt/data
```

14. 編輯開機掛載表 /etc/fstab，設定開機自動掛載 /dev/sda1 在 /mnt/data，注意掛載參數是 _netdev，且 dump 及 fsck 都不執行，也就是設成 0。

```
1 [root@kvm7 ~]# vim /etc/fstab
[root@kvm7 ~]# tail -1 /etc/fstab
3 /dev/sda1      /mnt/data      ext4      _netdev      0 0
```

15. 依照開機掛載表 /etc/fstab 掛載，成功掛載才可以重開機。

```
1 [root@kvm7 ~]# mount -a
[root@kvm7 ~]# df -Th | grep data
3 /dev/sda1           ext4      8.7M  172K  7.9M   3% /mnt/data
```

12.4 Client Initiator 除錯

12.4.1 除錯一

1. 沒先 discovery 無法 login。

```
1 [root@kvm7 ~]# lsblk
NAME          MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
3 vda          252:0   0   4G  0 disk -
vda1         252:1   0 200M  0 part /boot -
vda2         252:2   0 3.4G  0 part -
vg_kvm7usb-swap 253:0   0 124M  0 lvm  [SWAP] -
vg_kvm7usb-root 253:1   0 3.1G  0 lvm  /
vda3         252:3   0 130M  0 part -
vg_kvm7home-vo 253:2   0  80M  0 lvm  /home
[root@kvm7 ~]# iscsiadm -m node -T iqn.2015-08.wang.deyu:kvm5 -p
192.168.122.5 -l
11 iscsiadm: No records found
```

2. 正確做法。

```

1 [root@kvm7 ~]# iscsiadadm -m discovery -t st -p 192.168.122.5
2   192.168.122.5:3260,1 iqn.2015-08.wang.deyu:kvm5
3
4 [root@kvm7 ~]# iscsiadadm -m node -T iqn.2015-08.wang.deyu:kvm5 -p
5   192.168.122.5 -l
6 Logging in to [iface: default, target: iqn.2015-08.wang.deyu:kvm5,
7   portal: 192.168.122.5,3260] (multiple)
8 Login to [iface: default, target: iqn.2015-08.wang.deyu:kvm5, portal:
9   192.168.122.5,3260] successful.
10
11 [root@kvm7 ~]# lsblk
12   NAME      MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
13   sda        8:0    0   12M  0 disk --
14   sda1       8:1    0   10M  0 part /mnt/data
15   vda        252:0   0   4G  0 disk --
16   vda1       252:1   0  200M 0 part /boot --
17   vda2       252:2   0  3.4G 0 part --
18   vg_kvm7usb-swap 253:0   0 124M 0 lvm  [SWAP] --
19   vg_kvm7usb-root 253:1   0  3.1G 0 lvm  /
20   vda3       252:3   0 130M 0 part --
21   vg_kvm7home-vo 253:2   0   80M 0 lvm  /home

```

12.4.2 除錯二

1. 沒先 login 無法 logout。

```

2 [root@kvm7 ~]# iscsiadadm -m discovery -t st -p 192.168.122.5
3   192.168.122.5:3260,1 iqn.2015-08.wang.deyu:kvm5
4 [root@kvm7 ~]# iscsiadadm -m node -T iqn.2015-08.wang.deyu:kvm5 -p
5   192.168.122.5 -u
6 iscsiadadm: No matching sessions found

```

2. 使用 -l 選項 login 成功。

```

2 [root@kvm7 ~]# iscsiadadm -m node -T iqn.2015-08.wang.deyu:kvm5 -p
3   192.168.122.5 -l
4 Logging in to [iface: default, target: iqn.2015-08.wang.deyu:kvm5,
5   portal: 192.168.122.5,3260] (multiple)
6 Login to [iface: default, target: iqn.2015-08.wang.deyu:kvm5, portal:
7   192.168.122.5,3260] successful.

```

3. 使用 -u 選項 logout 成功。

```

1 [root@kvm7 ~]# iscsiadadm -m node -T iqn.2015-08.wang.deyu:kvm5 -p
2   192.168.122.5 -u
3 Logging out of session [sid: 1, target: iqn.2015-08.wang.deyu:kvm5,
4   portal: 192.168.122.5,3260]

```

3 Logout of [sid: 1, target: iqn.2015-08.wang.deyu:kvm5, portal: 192.168.122.5,3260] successful.

4. 使用 -o delete 選項刪除 iscsi target 連線。

```
1 [root@kvm7 ~]# iscsiadadm -m node -o delete -T iqn.2015-08.wang.deyu:kvm5
   -p 192.168.122.5
[root@kvm7 ~]# lsblk
3 NAME      MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
vda        252:0    0   4G  0 disk --
5 vda1       252:1    0 200M  0 part /boot --
vda2       252:2    0 3.4G  0 part --
7 vg_kvm7usb-swap 253:0    0 124M  0 lvm  [SWAP] --
vg_kvm7usb-root 253:1    0 3.1G  0 lvm  /
9 vda3       252:3    0 130M  0 part --
vg_kvm7home-vo 253:2    0  80M  0 lvm  /home
```

5. 無法登入或登入有問題可先登出、刪除連線後，再重新 discovery, login。

```
1 [root@kvm7 ~]# iscsiadadm -m discovery -t st -p 192.168.122.5
2 192.168.122.5:3260,1 iqn.2015-08.wang.deyu:kvm5

4 [root@kvm7 ~]# iscsiadadm -m node -T iqn.2015-08.wang.deyu:kvm5 -p
   192.168.122.5 -l
Logging in to [iface: default, target: iqn.2015-08.wang.deyu:kvm5,
  portal: 192.168.122.5,3260] (multiple)
6 Login to [iface: default, target: iqn.2015-08.wang.deyu:kvm5, portal:
  192.168.122.5,3260] successful.
[root@kvm7 ~]# lsblk
8 NAME      MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
sda        8:0    0   12M  0 disk --
10 sda1       8:1    0 10M  0 part /mnt/data
vda        252:0    0   4G  0 disk --
12 vda1       252:1    0 200M  0 part /boot --
vda2       252:2    0 3.4G  0 part --
14 vg_kvm7usb-swap 253:0    0 124M  0 lvm  [SWAP] --
vg_kvm7usb-root 253:1    0 3.1G  0 lvm  /
16 vda3       252:3    0 130M  0 part --
vg_kvm7home-vo 253:2    0  80M  0 lvm  /home
```


Chapter 13

MariaDB 資料庫

13.1 MariaDB 簡介

1. RHEL/CentOS 7 提供兩種關聯性資料庫：

- (a) PostgreSQL : PostgreSQL 是由散佈在全球的數百名開發者，包含非營利/營利組織團體，學術研究機構及國際型企業體共同開發的成果。PostgreSQL 為 BSD 版權協議發佈，允許在商業或非商業應用的兩種環境下均享有自由取得且不受版權限制的自主使用權甚至延伸功能。PostgreSQL 具有高度擴展性，且完整遵從國際 ISO-SQL 規範的開發方向，是當前全球最先進的開放源始碼 (OSS) 的物件關聯型資料庫管理系統 (ORDBMS)。
- (b) MariaDB : 由一些 MySQL 原作者成立的 MySQL 開發社群發展的資料庫，它提供豐富的加強功能，包含交錯儲存引擎 (alternate storage engines)、伺服器優化和補丁。

13.2 MariaDB 架設

1. 安裝套件

```
1 [root@kvm5 ~]# yum install mariadb-* -y
```

2. 設定開機啓動 mariadb 服務。

```
1 [root@kvm5 ~]# systemctl enable mariadb.service
ln -s '/usr/lib/systemd/system/mariadb.service' '/etc/systemd/system/
multi-user.target.wants/mariadb.service'
```

3. 啓動 mariadb 服務。

```
[root@kvm5 ~]# systemctl start mariadb.service
```

4. mariadb 使用 3306/tcp port listen 所有的網路。

```
1 [root@kvm5 ~]# ss -tulpn | grep mysql
tcp    LISTEN      0      50      *:3306      *:*      users:(("mysqld",16244,14)
)
```

5. 開啓防火牆 mysql 服務。

```
2 [root@kvm5 ~]# firewall-cmd --permanent --add-service=mysql
success
3 [root@kvm5 ~]# firewall-cmd --reload
success
```

6. 因為資料庫只限本機存取，所以在 [mysqld] 設定 skip-networking=1。

```
2 [root@kvm5 ~]# vim /etc/my.cnf
[root@kvm5 ~]# head -2 /etc/my.cnf
[mysqld]
4 skip-networking=1
```

7. 重新啓動 mariadb 服務。

```
[root@kvm5 ~]# systemctl restart mariadb.service
```

8. 再查看 mariadb 已不 listen 網路。

```
1 [root@kvm5 ~]# ss -tulpn | grep mysql
```

9. 進行 MariaDB 安全初始化，設定 root 密碼為 qweqwe，其餘都回答 Y。

```
1 [root@kvm5 ~]# mysql_secure_installation
/usr/bin/mysql_secure_installation: line 379: find_mysql_client: command
not found
3
5 NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MariaDB
      SERVERS IN PRODUCTION USE! PLEASE READ EACH STEP CAREFULLY!
7
9 In order to log into MariaDB to secure it, we'll need the current
   password for the root user. If you've just installed MariaDB, and
   you haven't set the root password yet, the password will be blank,
   so you should just press enter here.
11
Enter current password for root (enter for none):
```

```
13 OK, successfully used password, moving on...

15 Setting the root password ensures that nobody can log into the MariaDB
root user without the proper authorisation.

17 Set root password? [Y/n] Y
19 New password:
20 Re-enter new password:
21 Password updated successfully!
22 Reloading privilege tables..
23     ... Success!

25 By default, a MariaDB installation has an anonymous user, allowing
anyone
26 to log into MariaDB without having to have a user account created for
them. This is intended only for testing, and to make the installation
27 go a bit smoother. You should remove them before moving into a
production environment.

31 Remove anonymous users? [Y/n] Y
32     ... Success!

35 Normally, root should only be allowed to connect from 'localhost'. This
ensures that someone cannot guess at the root password from the network.

37 Disallow root login remotely? [Y/n] Y
38     ... Success!

41 By default, MariaDB comes with a database named 'test' that anyone can
access. This is also intended only for testing, and should be removed
42 before moving into a production environment.

45 Remove test database and access to it? [Y/n] Y
46     - Dropping test database...
47     ... Success!
48     - Removing privileges on test database...
49     ... Success!

51 Reloading the privilege tables will ensure that all changes made so far
will take effect immediately.

53 Reload privilege tables now? [Y/n] Y
54     ... Success!

57 Cleaning up...

59 All done! If you've completed all of the above steps, your MariaDB
installation should now be secure.

61 Thanks for using MariaDB!
```

10. 確認 root 無法免密碼登入 mariadb。

```

1 [root@kvm5 ~]# mysql -uroot
2 ERROR 1045 (28000): Access denied for user 'root'@'localhost' (using
  password: NO)

```

11. 確認 root 可以使用密碼 qweqwe 登入 mariadb。

```

1 [root@kvm5 ~]# mysql -uroot -pqweqwe
2 Welcome to the MariaDB monitor. Commands end with ; or \g.
3 Your MariaDB connection id is 12
4 Server version: 5.5.41-MariaDB MariaDB Server
5
6 Copyright (c) 2000, 2014, Oracle, MariaDB Corporation Ab and others.
7
8 Type 'help;' or '\h' for help. Type '\c' to clear the current input
  statement.
9
10 MariaDB [(none)]> show databases;
11 +-----+
12 | Database      |
13 +-----+
14 | information_schema |
15 | mysql          |
16 | performance_schema |
17 +-----+
18 3 rows in set (0.00 sec)
19
20 MariaDB [(none)]> exit
21 Bye

```

13.3 建立資料庫

1. 產生資料庫 Contacts。

```

1 [root@kvm5 ~]# mysqladmin -uroot -pqweqwe create Contacts

```

2. 查看資料庫 Contacts，沒有任何資料表。

```

1 [root@kvm5 ~]# mysql -uroot -pqweqwe -e "use Contacts; show tables;""

```

3. 下載資料表備份檔，此為測試資料庫檔，上課時再提供資料庫供下載。

```

1 [root@kvm5 ~]# wget http://dywang.csie.cyut.edu.tw/materials/staff.mdb

```

4. 匯入 staff.mdb 到資料庫 Contacts。

```
1 [root@kvm5 ~]# mysql -uroot -pqweqwe Contacts < staff.mdb
```

5. 查看資料庫 Contacts，出現資料表 staff。

```
1 [root@kvm5 ~]# mysql -uroot -pqweqwe -e "use Contacts; show tables;"  
+-----+  
| Tables_in_Contacts |  
+-----+  
| staff |  
+-----+
```

6. 查看資料庫 Contacts 中的資料表 staff 共有六筆資料。

```
1 [root@kvm5 ~]# mysql -uroot -pqweqwe -e "use Contacts; select * from  
staff;"  
+----+----+----+----+----+  
| id | firstname | lastname | password | pid |  
+----+----+----+----+----+  
| 1 | Linda | Lin | 123qwe | 3 |  
| 2 | Linda | Wang | 123qwe | 3 |  
| 3 | Rita | Lin | 123123 | 2 |  
| 4 | Rita | Wang | qwe123 | 1 |  
| 5 | Peter | Lin | 123123 | 2 |  
| 6 | Peter | Wang | qwe123 | 2 |  
+----+----+----+----+----+
```

13.4 * 建立並備份資料表

1. 本節非授課範圍，但練習時必須匯入一資料庫備份檔，此節為此檔產生方式，學生也可自行練習產生。先登入資料庫。

```
1 [root@kvm5 ~]# mysql -uroot -pqweqwe  
Welcome to the MariaDB monitor. Commands end with ; or \g.  
3 Your MariaDB connection id is 14  
Server version: 5.5.41-MariaDB MariaDB Server  
5  
7 Copyright (c) 2000, 2014, Oracle, MariaDB Corporation Ab and others.  
7  
Type 'help;' or '\h' for help. Type '\c' to clear the current input  
statement.
```

2. 產生資料庫 Contacts。

```

1 MariaDB [(none)]> create database Contacts;
2 Query OK, 1 row affected (0.00 sec)

```

3. 使用資料庫 Contacts。

```

1 MariaDB [(none)]> use Contacts;
2 Database changed

```

4. 在資料庫 Contacts 中建立資料表 staff。

```

1 MariaDB [Contacts]> create table staff
2   -> id int not null auto_increment,
3   -> firstname varchar(40) not null,
4   -> lastname varchar(40) not null,
5   -> password varchar(40) not null,
6   -> pid int not null,
7   -> primary key (id);
8 Query OK, 0 rows affected (0.08 sec)

```

5. 查看資料表 staff 的欄位。

```

1 MariaDB [Contacts]> show columns from staff;
2 +-----+-----+-----+-----+-----+-----+
3 | Field | Type | Null | Key | Default | Extra |
4 +-----+-----+-----+-----+-----+-----+
5 | id | int(11) | NO | PRI | NULL | auto_increment |
6 | firstname | varchar(40) | NO | | NULL | |
7 | lastname | varchar(40) | NO | | NULL | |
8 | password | varchar(40) | NO | | NULL | |
9 | pid | int(11) | NO | | NULL | |
10 +-----+-----+-----+-----+-----+-----+
11 5 rows in set (0.00 sec)

```

6. 查看資料庫 Contacts 已存在資料表 staff。

```

1 MariaDB [Contacts]> show tables;
2 +-----+
3 | Tables_in_Contacts |
4 +-----+
5 | staff |
6 +-----+
7 1 row in set (0.00 sec)

```

7. 資料表 staff 中建立六筆資料。

```

1 MariaDB [Contacts]> insert into staff (id,firstname,lastname,password,
  pid)
-> values
3 -> ('Linda','Lin','123qwe',3),
-> ('Linda','Wang','123qwe',3),
5 -> ('Rita','Lin','123123',2),
-> ('Rita','Wang','qwe123',1),
7 -> ('Peter','Lin','123123',2),
-> ('Peter','Wang','qwe123',2);
9 Query OK, 6 rows affected (0.04 sec)
Records: 6 Duplicates: 0 Warnings: 0

```

8. 查看資料表 staff 中的資料。

```

1 MariaDB [Contacts]> select * from staff;
2 +-----+-----+-----+-----+
3 | id | firstname | lastname | password | pid |
4 +-----+-----+-----+-----+
5 | 1 | Linda     | Lin      | 123qwe   | 3 |
6 | 2 | Linda     | Wang     | 123qwe   | 3 |
7 | 3 | Rita      | Lin      | 123123   | 2 |
8 | 4 | Rita      | Wang     | qwe123   | 1 |
9 | 5 | Peter     | Lin      | 123123   | 2 |
10 | 6 | Peter     | Wang     | qwe123   | 2 |
11 +-----+-----+-----+-----+
12 6 rows in set (0.00 sec)

```

9. 退出資料庫。

```

1 MariaDB [Contacts]> exit
2 Bye

```

10. 備份資料表 staff 為 staff.mdb。

```
[root@kvm5 ~]# mysqldump -uroot -pqweqw Contacts staff > staff.mdb
```

11. 刪除資料庫 Contacts，MariaDB 跟 Linux 一樣，資料庫名稱要分大小寫

```

1 [root@kvm5 ~]# mysqladmin -uroot -pqweqw drop contacts
Dropping the database is potentially a very bad thing to do.
3 Any data stored in the database will be destroyed.
5 Do you really want to drop the 'contacts' database [y/N] y

```

```

7 mysqladmin: DROP DATABASE contacts failed;
error: 'Can't drop database 'contacts'; database doesn't exist'
[root@kvm5 ~]# mysqladmin -uroot -pqweqwe drop Contacts
9 Dropping the database is potentially a very bad thing to do.
Any data stored in the database will be destroyed.
11
13 Do you really want to drop the 'Contacts' database [y/N] y
Database "Contacts" dropped

```

13.5 建立用戶

1. 以 root 身份登入 mysql。

```

1 [root@kvm5 ~]# mysql -uroot -pqweqwe
Welcome to the MariaDB monitor. Commands end with ; or \g.
3 Your MariaDB connection id is 13
Server version: 5.5.41-MariaDB MariaDB Server
5
Copyright (c) 2000, 2014, Oracle, MariaDB Corporation Ab and others.
7
Type 'help;' or '\h' for help. Type '\c' to clear the current input
statement.

```

2. 以 root 身份登入 mysql。

```

MariaDB [(none)]> show databases;
+-----+
| Database      |
+-----+
| information_schema |
| mysql          |
| performance_schema |
+-----+
3 rows in set (0.00 sec)

```

3. 使用 mysql 資料庫。

```

1 MariaDB [(none)]> use mysql;
Reading table information for completion of table and column names
3 You can turn off this feature to get a quicker startup with -A
5 Database changed

```

4. 新增一筆用戶名稱為 dywang，密碼 qweqwe，此用戶只能由本機登入。

```
1 MariaDB [mysql]> create user dywang@'localhost' identified by 'qweqwe';
```

5. 以 grant 指定用戶 dywang 在資料庫 Contacts 只有 SELECT 的權限。

```
1 MariaDB [mysql]> grant select on Contacts.* to dywang@'localhost';
Query OK, 0 rows affected (0.01 sec)
```

6. 使用 FLUSH PRIVILEGES 更新權限。

```
1 MariaDB [mysql]> FLUSH PRIVILEGES;
2 Query OK, 0 rows affected (0.00 sec)
```

7. 查詢用戶 dywang 的所有權限有兩筆，第一筆是產生用戶時就已設定，沒有指定對所有資料庫權限；第二筆是剛剛才設定對資料庫 Contacts 的所有資料表有 select 查詢權限。

```
1 MariaDB [mysql]> show grants for 'dywang'@'localhost'\G
2 **** 1. row ****
3 Grants for dywang@localhost: GRANT USAGE ON *.* TO 'dywang'@'localhost'
4 IDENTIFIED BY PASSWORD '*ABCBDDA833FA5726A2C9AEC6690A696F5DB8969'
5 **** 2. row ****
6 Grants for dywang@localhost: GRANT SELECT ON `Contacts`.* TO 'dywang'@'localhost'
7 2 rows in set (0.00 sec)
```

8. 也可以使用 select 查詢用戶 dywang 細部權限，沒有任何權限。

```
1 MariaDB [mysql]> select * from mysql.user where user='dywang'\G
2 **** 1. row ****
3     Host: localhost
4         User: dywang
5     Password: *ABCBDDA833FA5726A2C9AEC6690A696F5DB8969
6     Select_priv: N
7     Insert_priv: N
8     Update_priv: N
9     Delete_priv: N
10    Create_priv: N
11    Drop_priv: N
12    Reload_priv: N
13    Shutdown_priv: N
14    Process_priv: N
15    File_priv: N
16    Grant_priv: N
17    References_priv: N
```

```

19      Index_priv: N
20      Alter_priv: N
21      Show_db_priv: N
22      Super_priv: N
23      Create_tmp_table_priv: N
24      Lock_tables_priv: N
25      Execute_priv: N
26      Repl_slave_priv: N
27      Repl_client_priv: N
28      Create_view_priv: N
29      Show_view_priv: N
30      Create_routine_priv: N
31      Alter_routine_priv: N
32      Create_user_priv: N
33      Event_priv: N
34      Trigger_priv: N
35      Create_tablespace_priv: N
36          ssl_type:
37          ssl_cipher:
38          x509_issuer:
39          x509_subject:
40          max_questions: 0
41          max_updates: 0
42          max_connections: 0
43          max_user_connections: 0
44          plugin:
45          authentication_string:
46 1 row in set (0.00 sec)

```

9. 查詢哪些用戶在資料庫 Contacts 有權限？查到用戶 dywang 在資料庫 Contacts 只有 select 查詢權限。

```

1 MariaDB [mysql]> select * from mysql.db where db='Contacts'\G
***** 1. row *****
3           Host: localhost
4           Db: Contacts
5           User: dywang
6           Select_priv: Y
7           Insert_priv: N
8           Update_priv: N
9           Delete_priv: N
10          Create_priv: N
11          Drop_priv: N
12          Grant_priv: N
13          References_priv: N
14          Index_priv: N
15          Alter_priv: N
16          Create_tmp_table_priv: N
17          Lock_tables_priv: N
18          Create_view_priv: N
19          Show_view_priv: N
20          Create_routine_priv: N
21          Alter_routine_priv: N

```

```

23      Execute_priv: N
24          Event_priv: N
25          Trigger_priv: N
26  1 row in set (0.00 sec)

27 MariaDB [mysql]>

```

10. 退出資料庫。

```

1 MariaDB [mysql]> exit
Bye

```

13.6 查詢資料表資料

1. 登入 MariaDB。

```

[root@kvm5 ~]# mysql -uroot -pqweqwe
2 Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 26
4 Server version: 5.5.41-MariaDB MariaDB Server

6 Copyright (c) 2000, 2014, Oracle, MariaDB Corporation Ab and others.

8 Type 'help;' or '\h' for help. Type '\c' to clear the current input
statement.

```

2. 使用資料庫 Contacts。

```

MariaDB [(none)]> use Contacts;
2 Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A
4
Database changed

```

3. 查看資料庫 Contacts 中共有三個的資料表。

```

1 MariaDB [Contacts]> show tables;
+-----+
3 | Tables_in_Contacts |
+-----+
5 | User_Contacts      |
| User_Logins         |
7 | User_Names         |
+-----+

```

```
9 || 3 rows in set (0.00 sec)
```

4. 查看資料庫 Contacts 中的資料表 User_Names 的欄位結構。

```
1 MariaDB [Contacts]> desc User_Names;
+-----+-----+-----+-----+-----+
3 | Field      | Type       | Null | Key | Default | Extra |
+-----+-----+-----+-----+-----+
5 | user_id    | int(11)   | NO   | PRI | NULL    |       |
| last_name   | varchar(35)| YES  |      | NULL    |       |
7 | first_name | varchar(35)| YES  |      | NULL    |       |
+-----+-----+-----+-----+-----+
9 3 rows in set (0.00 sec)
```

5. 查看資料庫 Contacts 中的資料表 User_Logins 的欄位結構。

```
1 MariaDB [Contacts]> desc User_Logins;
+-----+-----+-----+-----+-----+
3 | Field      | Type       | Null | Key | Default | Extra |
+-----+-----+-----+-----+-----+
5 | id         | int(11)   | NO   | MUL | NULL    |       |
| User_Login | varchar(25)| YES  |      | NULL    |       |
7 | User_Pass  | varchar(35)| YES  |      | NULL    |       |
+-----+-----+-----+-----+-----+
9 3 rows in set (0.00 sec)
```

6. 查看資料庫 Contacts 中的資料表 User_Contacts 的欄位結構。

```
1 MariaDB [Contacts]> desc User_Contacts;
+-----+-----+-----+-----+-----+
3 | Field      | Type       | Null | Key | Default | Extra |
+-----+-----+-----+-----+-----+
5 | id         | int(11)   | NO   | MUL | NULL    |       |
| Location   | varchar(25)| YES  |      | NULL    |       |
7 | Email      | varchar(35)| YES  |      | NULL    |       |
| Telephone  | varchar(25)| YES  |      | NULL    |       |
9 | Fax        | varchar(25)| YES  |      | NULL    |       |
+-----+-----+-----+-----+-----+
11 5 rows in set (0.00 sec)
```

7. 經觀察 Contacts 中的三個資料表之關聯性為：同一人員以 user_id, id 做關聯，也就是三個資料表中的 id 編號相同，表示同一人。以此結論查詢 first_name 為 John 共有兩人。

```
1 || MariaDB [Contacts]> select * from User_Names where first_name='John';
```

```

3 |-----+-----+-----+
4 | user_id | last_name | first_name |
5 |-----+-----+-----+
6 | 1917 | Falena    | John      |
7 | 3915 | Walker     | John      |
8 |-----+-----+-----+
9 2 rows in set (0.00 sec)

```

8. 依據查到的 `user_id`, `id` 再查詢資料表 `User_Contacts`, 可以查到這兩人的「住地」、Email、電話及傳真。

```

1 MariaDB [Contacts]> select * from User_Contacts where id=1917 or id
2   =3915;
3 +-----+-----+-----+-----+
4 | id    | Location      | Email           | Telephone       | Fax
5 |-----+-----+-----+-----+
6 | 1917 | Santa Clara | jfalena@example.com | +1 408 555 8133 | +1 408
7   555 7472 |
8 | 3915 | Cupertino   | jwalker@example.com | +1 408 555 1476 | +1 408
9   555 1992 |
10 +-----+-----+-----+-----+
11 2 rows in set (0.00 sec)
12
13 MariaDB [Contacts]>

```

9. 只有一兩筆資料可以用上述的方法查詢比對，但如果資料量龐大，還是要使用 JOIN 結合查詢。以下是查到 `first_name='John'` 且住在 `Cupertino` 的人有一筆。

```

1 MariaDB [Contacts]> select a.user_id, a.first_name, b.Location \
2   from User_Names a,User_Contacts b where a.user_id=b.id and \
3     a.first_name='John' and b.Location='Cupertino';
4 +-----+-----+-----+
5 | user_id | first_name | Location |
6 |-----+-----+-----+
7 | 3915   | John       | Cupertino |
8 |-----+-----+-----+
9 1 row in set (0.01 sec)

```

10. 如果只想得知查詢結果有幾筆，可以使用 `count(*)` 函數計算結果。

```

1 MariaDB [Contacts]> select count(*) from User_Names a,User_Contacts b \
2   where a.user_id=b.id and a.first_name='John' and b.Location='Cupertino';
3 +-----+

```

```

5 | count(*) |
+-----+
|      1 |
+-----+
7 1 row in set (0.00 sec)
9 MariaDB [Contacts]>

```

11. 查詢密碼為 mainland 的名字 (first_name)，可以先查密碼為 mainland 的用戶 id 為 3819。

```

1 MariaDB [Contacts]> select * from User_Logins where User_Pass='mainland'
'';
+-----+-----+-----+
3 | id   | User_Login | User_Pass |
+-----+-----+-----+
5 | 3819 | mcarter   | mainland |
+-----+-----+-----+
7 1 row in set (0.00 sec)

```

12. 再以 id 3819 查到用戶名為 Mike、姓為 Carter。

```

1 MariaDB [Contacts]> select * from User_Names where user_id=3819;
+-----+-----+-----+
3 | user_id | last_name | first_name |
+-----+-----+-----+
5 | 3819    | Carter     | Mike       |
+-----+-----+-----+
7 1 row in set (0.00 sec)

```

13. 以 JOIN 結合查詢查得密碼為 mainland 的名字 (first_name) 為 Mike。

```

1 MariaDB [Contacts]> select a.first_name \
from User_Names a,User_Logins b \
where a.user_id=b.id and b.User_Pass='mainland';
+-----+
5 | first_name |
+-----+
7 | Mike        |
+-----+
9 1 row in set (0.00 sec)

```

14. 退出資料庫。

```

1 MariaDB [Contacts]> exit
Bye

```

13.7 查詢練習

1. 回答以下問題，並將結果存於 mariadb server kvm5，目錄及位置為 /tmp/query1.txt，格式為每一數字以一個空白隔開。
 - (a) 查詢 first name 是 David 且住在 Cupertino 有幾人？
 - (b) 查詢 last name 是 Rose 且住在 Cupertino 有幾人？
 - (c) 查詢 first name 是 Morgan 且住在 Cupertino 有幾人？
 - (d) 查詢 last name 是 Burrell 且住在 Sunnyvale 有幾人？
 - (e) 查詢 first name 是 Jody 且住在 Sunnyvale 有幾人？
 - (f) 查詢 first name 是 Brad 且住在 Sunnyvale 有幾人？
 - (g) 查詢 last name 是 Hall 且住在 Santa Clara 有幾人？
 - (h) 查詢 first name 是 Scott 且住在 Santa Clara 有幾人？
 - (i) 查詢 first name 是 Lutz 且住在 Santa Clara 有幾人？
2. 回答以下問題，並將結果存於 mariadb server kvm5，目錄及位置為 /tmp/query2.txt，格式為每一字串以一個空白隔開。
 - (a) 查詢密碼為 linear 的用戶其名字 (first name) 為何？
 - (b) 查詢密碼為 sensible 的用戶其名字 (first name) 為何？
 - (c) 查詢密碼為 shrank 的用戶其姓 (last name) 為何？
 - (d) 查詢密碼為 compost 的用戶其姓 (last name) 為何？
 - (e) 查詢登入帳號為 mvaughan 的用戶其姓 (last name) 為何？
 - (f) 查詢登入帳號為 eward 的用戶其姓 (last name) 為何？
 - (g) 查詢登入帳號為 tcruse 的用戶其名字 (first name) 為何？
 - (h) 查詢登入帳號為 tlabonte 的用戶其名字 (first name) 為何？