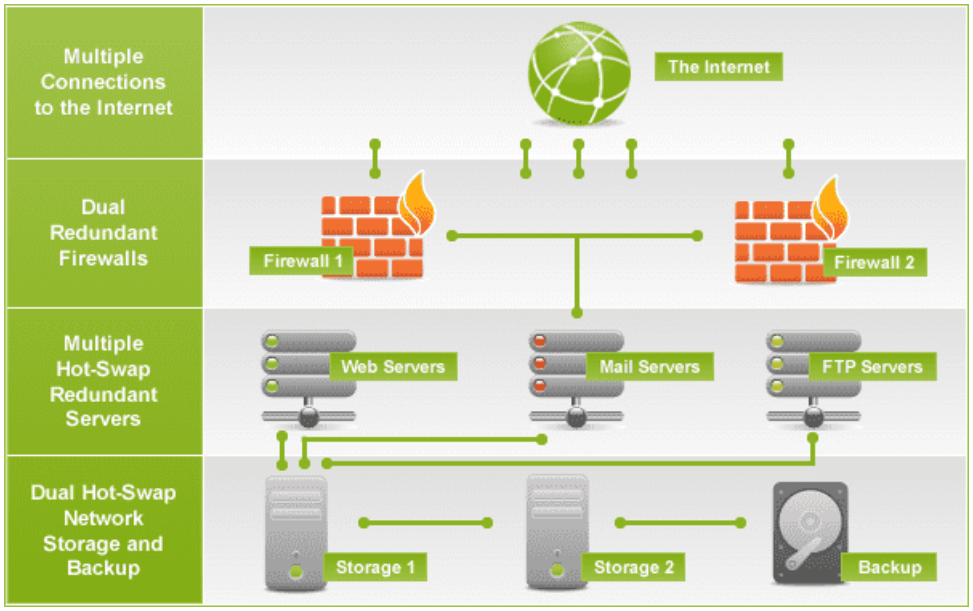
Linux 伺服器

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@csie.cyut.edu.tw
Homepage: http://dywang.csie.cyut.edu.tw
Phone: (04)23323000 ext 4538
Office: E738



Monday 4th September, 2023

- Instructor: De-Yu Wang
    1. Email: dywang@csie.cyut.edu.tw
    2. Homepage: http://dywang.csie.cyut.edu.tw
    3. 本文件 pdf 檔下載
    4. Phone: (04)23323000 ext 4538
    5. Office: E738
- 參考資料
    1. RedHat Documentation
    2. RedHat Customer Protal
    3. Storage Administration Guide
    4. Apache

Contents

1 SSH Server **1**

1.1 SSH 簡介 1
1.2 SSH server 架設 1
1.3 安全機制 2
1.4 SSH 免密碼登入 3
1.5 ssh-copy-id 5
1.6 sshpass 傳送密碼 6
1.7 ssh 帶出 X11 7
1.8 ssh 持續連線 8
1.9 SSH+Firefox 翻牆 9
1.10 Reverse SSH Tunneling 10
1.11 SSH 相關問題 11
1.12 TMUX 多視窗 16

2 IPtables 防火牆 **19**

2.1 IPtables 簡介 19
2.2 內建表格 tables 19
2.3 內建鏈 chains 20
2.4 規則 Rules 22
2.5 動作 Target 22
2.6 預設環境 23
2.7 實機設定 24

3 FTP Server **26**

3.1 FTP 簡介 26
3.2 FTP server 架設 27
3.3 安全機制 28
3.4 SSL 設定 29
3.5 ftps client – lftp 31

4 Apache 2.2 HTTP Server **33**
4.1 Apache HTTP 簡介 33
4.2 Apache HTTP server 架設 33
4.3 UserDir 用户個人網頁 34
4.4 Virtual Host 虛擬主機 34
4.5 存取限制 35
4.6 安全機制 36
4.7 AB test 39
4.8 防止 DoS 42
4.9 實機操作測驗練習題 45

5 安全 Apache 2.2 網站 **48**
5.1 前言 48
5.2 隱藏敏感訊息 48
5.3 網頁存取用户 49
5.4 限制網頁根目錄外的存取 50
5.5 關閉目錄瀏覽 51
5.6 確認 apache 用户無權限寫入 52
5.7 關閉.htaccess 檔案支援 53
5.8 決定是否開啓 FollowSymLinks 53
5.9 實機操作測驗練習題 54

6 Network File System, NFS **56**
6.1 NFS 簡介 56
6.2 NFS 架設 56
6.3 查詢與變更 57
6.4 安全機制 58
6.5 NFS Client 端設定 61
6.6 自動掛載 autofs 的使用 62
6.7 NFS 掛載非常慢 65

7 DHCP **66**
7.1 DHCP 簡介 66
7.2 DHCP 架設設定 - c6 66
7.3 DHCP 架設設定 - c8 69
7.4 DHCP Client 71
7.5 安全機制 73
7.6 NAT 配置 74

7.7 其他問題 75

8 Mail Server **77**
8.1 Mail Server 簡介 77
8.2 Email 協定 77
8.3 Dovecot 架設 78
8.4 Postfix 架設 79
8.5 垃圾郵件過濾 81
8.6 安全機制 83
8.7 問題解決 84

9 Roundcube Webmail **85**
9.1 Roundcube 簡介 85
9.2 安裝 remi repo 85
9.3 架設 Roundcube 86
9.4 顯示調整 88
9.5 啓動 Plugins 90
9.6 Managesieve Plugin 90
9.7 Password Plugin 92
9.8 markasjunk Plugin 93
9.9 rcguard Plugin 93
9.10 Spell check 95
9.11 fetchmail-rc Plugin 95
9.12 fetchmail Plugin 97
9.13 enigma Plugin 101
9.14 Disk Quota 101
9.15 移機或備份 102
9.16 問題解決 104

10 OPENLDAP 網路用户帳號 **105**
10.1 LDAP 簡介 105
10.2 LDAP Server 建置 105
10.3 CA 憑證 110
10.4 LDAP Client 端設定 111
10.5 LDAP 帳號管理 114
10.6 安全機制 117
10.7 問題解決 118

11 DNS server **120**
11.1 DNS 簡介 120
11.2 DNS 架設 120
11.3 安全機制 125
11.4 問題解決 125

12 Dnsmasq server **127**
12.1 Dnsmasq 簡介 127
12.2 Dnsmasq 架設 127
12.3 Dnsmasq DNS 架設 128
12.4 Dnsmasq DHCP 架設 128

13 SAMBA **131**
13.1 SAMBA 簡介 131
13.2 SAMBA 架設 131
13.3 安全機制 132
13.4 SAMBA 程式 134

14 ISCSI **138**
14.1 ISCSI 簡介 138
14.2 ISCSI server 架設 138
14.3 安全機制 140
14.4 Client 端測試 140

15 NTP **142**
15.1 NTP 簡介 142
15.2 ntpdate 手動校時 142
15.3 NTP 架設 143
15.4 圖形界面網路校時設定 147
15.5 安全機制 147

16 Squid Proxy **148**
16.1 Squid 簡介 148
16.2 Squid 架設 148
16.3 安全機制 152
16.4 瀏覽器設定 153
16.5 Linux 命令列使用 Proxy 154

17 XMPP 即時通訊伺服器 Openfire **156**
17.1 XMPP 簡介 156
17.2 OPenfire 套件安裝與啓動 157
17.3 使用網頁設定 Openfire 160
17.4 使用網頁管理 Openfire 163
17.5 Linux 使用網頁管理 Openfire 164
17.6 Openfire Client – Pidgin for Linux 166
17.7 Openfire Client – Spark for Windows 167

18 XMPP 即時通訊伺服器 Prosody **171**
18.1 XMPP 簡介 171
18.2 Prosody 套件安裝與啓動 172
18.3 設定 prosody 聊天室 172
18.4 設定 prosody 用户 173
18.5 Prosody 安全設定 174
18.6 Prosody Client 176
18.7 用户自行註冊 179
18.8 SSL 加密 180

19 SIP 網路電話伺服器 Kamailio **183**
19.1 SIP 簡介 183
19.2 Kamailio 套件安裝與啓動 183
19.3 SIP Client 186
19.4 問題解決 187

20 WEBCOUNTER **188**
20.1 前言 188
20.2 Webcounter 下載安裝 188
20.3 Webcount 調整 190
20.4 Webcount 展示 192

21 自動開關機 **193**
21.1 前言 193
21.2 自動開機 193

22 SoftEther VPN **195**
22.1 前言 195
22.2 SoftEther Server 安裝 195
22.3 vpncmd 命令設定 vpnserver 197

22.4 設定 VPN hub 橋接器 201
22.5 VPN 設定 DHCP 204
22.6 brctl 設定橋接器 206
22.7 SoftEther VPN Client 安裝 209
22.8 vpncmd 設定 vpn client 211
22.9 設定 VPN Client IP 213

23 Open VPN **215**
23.1 前言 215
23.2 OpenVPN 套件安裝 215
23.3 Client 安裝與設定 220
23.4 OpenVPN server 設定 220
23.5 問題解決 221

Chapter 1

SSH Server

1.1 SSH 簡介

1. SSH 爲 Secure Shell 的縮寫，是一種電腦上的安全協定。
2. SSH 是一種透過安全的連線登入遠端主機執行命令的一個協定。
3. 圖形介面 X11 和任意的 TCP ports 也可以經由這個安全通道傳輸。

1.2 SSH server 架設

1. 安裝 openssh 套件：不過一般 Linux 安裝時都已安裝。

```
[root@kvm8 ~]# yum install -y openssh-server openssh-clients
```

2. 編輯 /etc/ssh/sshd_config 設定檔：限制或允許 ssh 用 root 帳號登入。

```
[root@kvm8 ~]# vim /etc/ssh/sshd_config
PermitRootLogin yes
```

3. 編輯 /etc/ssh/sshd_config 設定檔：限制或允許 ssh 使用密碼登入，或只能用金鑰登入，yes 表示可以使用密碼登入。

```
[root@kvm8 ~]# vim /etc/ssh/sshd_config
PasswordAuthentication yes
```

4. 編輯 /etc/ssh/sshd_config 設定檔：修改 ssh 的 port，預設爲 22。

```
[root@kvm8 ~]# vim /etc/ssh/sshd_config
Port 22
```

5. 啓動 sshd 服務

```
[root@kvm8 ~]# /etc/init.d/sshd restart
Shutting down sshd:                                        [FAILED]
Starting vsftpd for sshd:                                  [  OK  ]
```

6. 設定開機啓動 sshd 服務

```
[root@kvm8 ~]# chkconfig sshd on
```

1.3 安全機制

1. 防火牆設定–任何網域皆可使用 ssh：通常 Linux 預設防火牆都會開放 ssh 連線。

```
[root@kvm8 ~]# /etc/init.d/iptables restart
[root@kvm8 ~]# iptables-save | grep 22
-A INPUT -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
```

2. 防火牆重新啓動

```
[root@kvm8 ~]# /etc/init.d/iptables restart
```

3. 開機啓動防火牆

```
[root@kvm8 ~]# chkconfig iptables on
```

4. SELinux 有關 ssh 的設定

```
[root@kvm8 ~]# getsebool -a | grep ssh
allow_ssh_keysign --> off
fenced_can_ssh --> off
```

```
ssh_chroot_full_access --> off
ssh_chroot_manage_apache_content --> off
ssh_chroot_rw_homedirs --> off
ssh_sysadm_login --> off
```

1.4 SSH 免密碼登入

1. 在定時備份或批次遠端處理，往往需要免密碼登入遠端主機工作。爲達此目的，首先必須在 client 端產生一組 key，包含公開金鑰（Public Key）與私密金鑰（Private Key），將公鑰送到要登入的主機，相互對應做免密碼的登入。key 的產生：

```
[root@kvm8 ~]# ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
c3:e9:25:65:00:c8:65:cb:e8:fe:4e:7e:ce:06:a4:9d root@kvm8.deyu.wang
The key's randomart image is:
+--[ RSA 2048]----+
|    . o+..       |
|     o+ . .      |
|     . o   o     |
|    .  .. +      |
|     .+ .S .     |
|    .. E. +      |
|     . ...       |
|      + .o       |
|      .++o       |
+-----------------+
```

2. 將公開金鑰放到要登入的主機

```
[root@kvm8 ~]# scp .ssh/id_rsa.pub kvm7.deyu.wang:.ssh/
The authenticity of host 'kvm7.deyu.wang (192.168.122.7)' can't be
    established.
RSA key fingerprint is 33:76:31:62:25:dd:eb:a6:1f:5a:54:10:b8:25:c3:66.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'kvm7.deyu.wang,192.168.122.7' (RSA) to the
    list of known hosts.
root@kvm7.deyu.wang's password:
id_rsa.pub                                    100%  401     0.4KB/s
    00:00
```

3. ssh 登入欲免密碼登入的主機，這時還是要密碼。

```
[root@kvm8 ~]# ssh kvm7.deyu.wang
root@kvm7.deyu.wang's password:
Last login: Tue Feb  4 19:31:13 2014 from 192.168.122.1
```

4. 系統預設處理放置公鑰的檔案爲 authorized_keys，所以必須把剛剛傳送過來的公鑰累加到這個檔案中：

```
[root@kvm7 ~]# cat .ssh/id_rsa.pub >> .ssh/authorized_keys
```

5. 特別注意目錄 .ssh 及檔案 authorized_keys 的權限，若群組或其他人的權限過大，除了安全性有問題外，也有可能因 ssh 判斷要對應的金鑰不安全，而無法對應，也就是不能免密碼登入。

```
[root@kvm7 ~]# chmod 700 .ssh/
[root@kvm7 ~]# chmod 644 .ssh/authorized_keys
[root@kvm7 ~]# ll -d .ssh
drwx------. 2 root root 4096 Feb  4 19:36 .ssh
[root@kvm7 ~]# ll .ssh/authorized_keys
-rw-r--r--. 1 root root 401 Feb  4 19:36 .ssh/authorized_keys
```

6. 退出 kvm7.deyu.wang 回到 kvm8.deyu.wang。

```
[root@kvm7 ~]# exit
logout
Connection to kvm7.deyu.wang closed.
```

7. 再次登入 kvm7.deyu.wang 已不需要密碼。

```
[root@kvm8 ~]# ssh kvm7.deyu.wang
Last login: Tue Feb  4 19:32:57 2014 from 192.168.122.1
```

1.5 ssh-copy-id

1. 上一節免密碼設定的複雜過程，linux 上已幫你寫好一支腳本 ssh-copy-id，先執行 ssh-keygen 產生 ssh key。

```
[root@kvm3 ~]# ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
01:be:06:3d:89:bd:5b:b4:7a:e6:37:b0:07:44:86:35 root@kvm3.deyu.wang
The key's randomart image is:
+--[ RSA 2048]----+
|       .oE       |
|      =.oo.      |
|     o *oo       |
|      . =.o      |
|       +.S       |
|      . +o       |
|       o o+      |
|        +. +     |
|         .o .    |
+-----------------+
```

2. 執行 ssh-copy-id 參數爲要登入的主機，就可以將 public key 傳送到該主機，並幫忙設定好免密碼登入的信任主機。

```
[root@kvm3 ~]# ssh-copy-id 192.168.122.7
The authenticity of host '192.168.122.7 (192.168.122.7)' can't be
    established.
ECDSA key fingerprint is 30:b2:6e:89:45:69:cc:2f:52:a2:c7:d0:dc:2b:aa:e9
    .
Are you sure you want to continue connecting (yes/no)? yes
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to
     filter out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you
    are prompted now it is to install the new keys
root@192.168.122.7's password:

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh '192.168.122.7'"
and check to make sure that only the key(s) you wanted were added.
```

3. 登入 192.168.122.7 已不需要輸入密碼。

```
[root@kvm3 ~]# ssh 192.168.122.7
Last login: Thu Feb 15 11:58:57 2018 from deyu.wang
[root@kvm7 ~]#
```

1.6 sshpass 傳送密碼

1. 若沒有產生公私鑰在連線的兩端進行對應，ssh 連線時必須手動輸入密碼，這在例行工作、背景執行、批次處理等工作時會無法進行。爲達此目的，可以藉由 sshpass 指令用時傳送遠端主機的密碼。

2. 安裝 sshpass 套件。

```
[root@kvm8 ~]# yum install -y sshpass
```

3. 先登入遠端主機 kvm7.deyu.wang，移除對應公鑰。也就是移除免密碼登入對應。

```
[root@kvm8 ~]# ssh kvm7.deyu.wang
Last login: Tue Feb  4 19:49:12 2014 from deyu.wang
[root@kvm7 ~]# mv .ssh/authorized_keys /tmp
[root@kvm7 ~]# exit
logout
Connection to kvm7.deyu.wang closed.
```

4. 使用 sshpass 傳送密碼 123qwe，ssh 登入 kvm7.deyu.wang 在目錄 /root 下產生一個檔案 abc 內容爲 aaaa。遠端連線時目錄.ssh 中有一個檔案 known_hosts 會記錄曾經連線過的信任主機，若連線主機重新安裝或更換 ip，其 host key 不同，ssh 會產生警告訊息，要求確認並刪除在 known_hosts 中的記錄，才能連線。選項 -o StrictHostKeyChecking=no 就是不進行 host key 的檢查，以避免此中斷程式的動作。

```
[root@kvm8 ~]# sshpass -p123qwe ssh -o StrictHostKeyChecking=no kvm7.
   deyu.wang "echo aaaa > /root/abc"
```

5. rsync 以 ssh 同步，同樣可以利用 sshpass 傳送密碼，將 b.txt 送到 kvm7.deyu.wang。

```
[root@kvm8 ~]# echo bbbb > b.txt
[root@kvm8 ~]# rsync -av -e "sshpass -p123qwe ssh" b.txt kvm7.deyu.wang:
sending incremental file list
b.txt

sent 78 bytes  received 31 bytes  218.00 bytes/sec
```

6. 登入 kvm7.deyu.wang 檢查檔案 abc 及 b.txt。

```
[root@kvm7 ~]# cat abc
aaaa
[root@kvm7 ~]# cat b.txt
bbbb
```

1.7 ssh 帶出 X11

1. ssh 遠端連線並非只能做命令列指令，它同樣可以將遠端的 GUI 程式帶出。
2. 編輯 config 設定檔，允許連線到任何主機，皆可以帶出 X11。

```
[root@kvm8 ~]# vim .ssh/config
Host *
ForwardAgent yes
ForwardX11 yes
```

3. 變更 config 的權限。

```
[root@kvm8 ~]# chmod 644 .ssh/config
```

4. ssh 連線時加入選項 -X，就可將遠端的 GUI 程式帶出。

```
[root@kvm8 ~]# ssh -X deyu.wang
root@deyu.wang's password:
Last login: Thu Feb 13 20:21:53 2014 from kvm8.deyu.wang
[root@dywH ~]# virt-manager
```

5. 若 ssh 連線，只爲執行某一 GUI 程式，可以在 ssh 指令直接加上欲執行的 GUI 程式命令。

```
[root@kvm8 ~]# ssh -X deyu.wang virt-manager
```

6. 使用 rsync 經由 ssh 連線，出現錯誤訊息。

```
1 Warning: No xauth data; using fake authentication data for X11
    forwarding.
```

7. rsync 同步時以 ssh -x 指定不使用 ssh 的 X11 forwarding。

```
1 [root@kvm8 ~]# rsync -e "ssh -x" -a /var/ftp/pub/centos6/bin $host:/var/
    ftp/pub/centos6/
```

1.8 ssh 持續連線

1. ssh 遠端連線，在一段時間沒動作後會自動中斷連線，這在需要持續連線工作時非常不方便。

```
1 Write Failed: broken pipe
```

2. 可於連線時，使用 ServerAliveInterval 120 參數，每 120 秒送一個空的封包到連線的主機，以保持連線。

```
1 [root@dywH ~]# ssh -o ServerAliveInterval=120 kvm8.deyu.wang
```

3. 編輯 config 設定檔，讓每次的 ssh 連線，都使用此設定。如果沒有 root 權限，可以在家目錄下，編輯 ~/.ssh/config，一樣可以達到此目的。

```
1 [root@dywH ~]# vim .ssh/config
Host *
3     ServerAliveInterval 120
```

4. 修改.ssh/config 的權限爲只有用户本身有存取權，否則無法 ssh 連線。

```
1 [root@dywH ~]# chmod 600 ~/.ssh/config
```

1.9 SSH+Firefox 翻牆

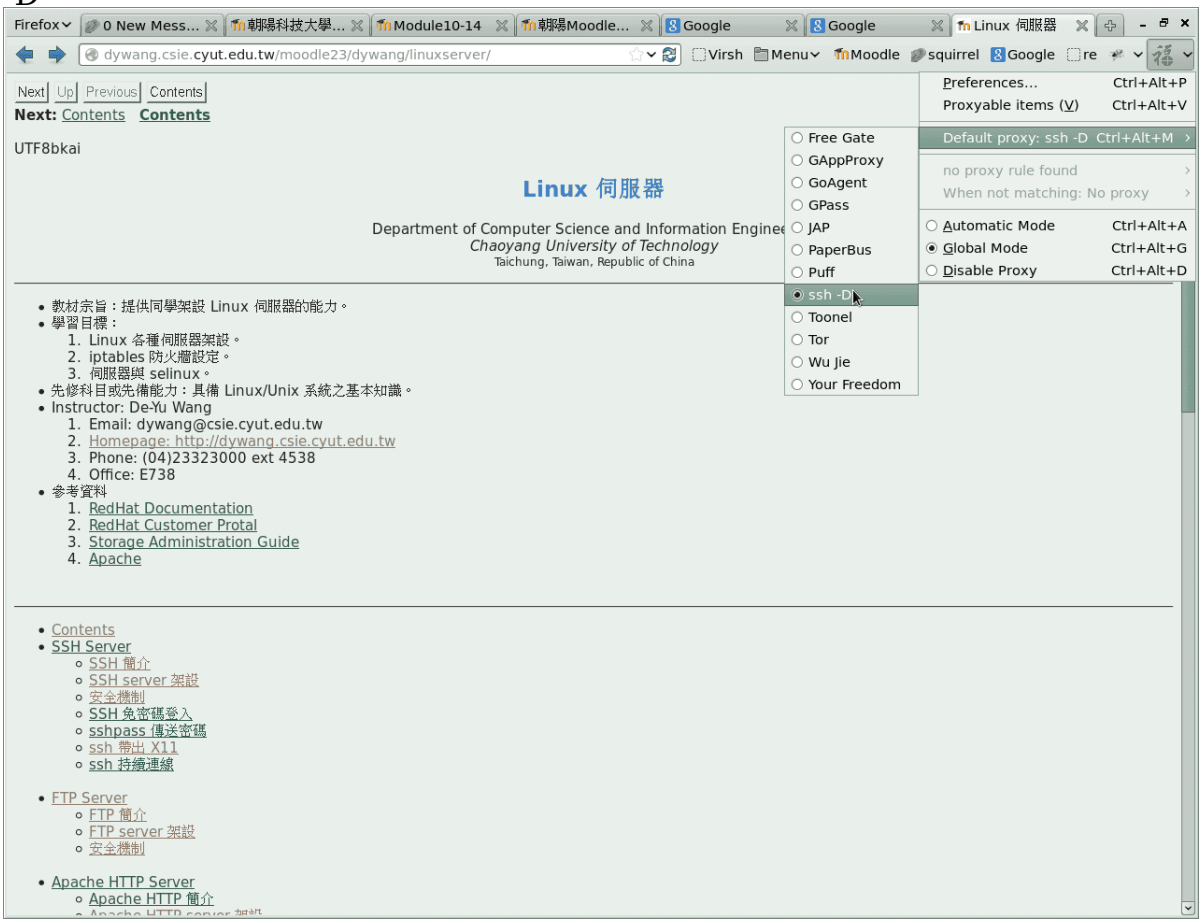
1. Firefox 安裝 autoproxy 套件。

```
Firefox -> Add-ons -> keyin: autoproxy -> search -> install -> restart
    firefox
```

2. Firefox 工作列上出現「福」字，點選成「綠色」。

```
綠色：Global mode
灰色：Disable proxy
紅色：Automatic mode
```

3. 游標放在「福」字上，按下滑鼠右鍵，出現選單。點選 Default Proxy -> ssh -D。



4. 若您在某 Linux 主機上有一帳號，即可經由 ssh 登入該帳號上網，通道 port

預設 7070。若沒有帳號翻牆，可以在 cjb.net 申請一個臨時帳號。

```
[dywang@dywH security]$ ssh -D 7070 dywang@163.17.27.219
```

5. Firefox 瀏覽 dywang.csie.cyut.edu.tw 測試，因主機沒有阻擋任何的來源，所以可以正常訪問網頁。

6. 修改 dywang.csie.cyut.edu.tw 的防火牆，http 80 port 不允許 163.17.27.219 訪問。

```
[root@dywang ~]# grep '219' /etc/sysconfig/iptables
-A INPUT ! -s 163.17.27.219/32 -p tcp -m state --state NEW -m tcp --
    dport 80 -j ACCEPT
```

7. 重新啓動 dywang.csie.cyut.edu.tw 的防火牆。

```
[root@dywang ~]# /etc/init.d/iptables restart
```

8. 再以 Firefox 瀏覽 dywang.csie.cyut.edu.tw 測試，已無法正常訪問網頁。

1.10 Reverse SSH Tunneling

1. 當要連線的遠端主機在 NAT 後面，可以使用 reverse SSH tunneling 連線，設定方式參考。

2. 假設要從 163.17.10.68 連線到主機 192.168.122.5，先在目標主機 192.168.122.5 執行 ssh -R 反向連線到來源主機的帳號與 IP，其中埠號 19999 爲自訂的埠號，只要找一個沒有被使用的埠號即可。

```
[root@kvm5 ~]# ssh -R 19999:localhost:22 dywang@163.17.10.68
dywang@163.17.10.68's password:
Last login: Wed Apr  6 10:10:47 2016
[dywang@dywang ~]$
```

3. 回到來源主機 163.17.10.68 以 19999 port 連線 localhost，就可以反向連線到遠端在 NAT 後面的 192.168.122.5 主機了。

```
[root@dywang ~]# ssh root@localhost -p 19999
Warning: Permanently added '[localhost]:19999' (RSA) to the list of
    known hosts.
root@localhost's password:
Last login: Fri Oct 27 10:53:22 2017 from deyu.wang
[root@kvm5 ~]#
```

1.11 SSH 相關問題

1.11.1 fignerprint

1. 遠端主機重建後，主機指紋 (fignerprint) 會不一樣，ssh 無法登入，必須刪除 ~/.ssh/known_hosts 中信任主機的紀錄，才能重新記錄新的遠端主機。若直接刪除 ~/.ssh/known_hosts 則檔案中的所有信任主機紀錄都刪除。

```
[dywang@dywssd ~]$ ssh root@kvm7.deyu.wang
key_from_blob: remaining bytes in key blob 3
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@       WARNING: POSSIBLE DNS SPOOFING DETECTED!          @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
The RSA host key for kvm7.deyu.wang has changed,
and the key for the corresponding IP address 192.168.122.7
is unchanged. This could either mean that
DNS SPOOFING is happening or the IP address for the host
and its host key have changed at the same time.
Offending key for IP in /home/dywang/.ssh/known_hosts:32
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!     @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle
    attack)!
It is also possible that the RSA host key has just been changed.
The fingerprint for the RSA key sent by the remote host is
0b:57:84:7d:e0:62:d8:80:0f:64:58:22:c5:ba:ee:b8.
Please contact your system administrator.
Add correct host key in /home/dywang/.ssh/known_hosts to get rid of this
     message.
Offending key in /home/dywang/.ssh/known_hosts:33
Password authentication is disabled to avoid man-in-the-middle attacks.
Keyboard-interactive authentication is disabled to avoid man-in-the-
    middle attacks.
```

```
25 Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password).
```

2. 原因爲客户端第一次 SSH 連線時已產生一個認證，如果伺服器端重灌，認證資訊當然也會更改，伺服器端與客户端不同時，就會跳出此錯誤訊息。解決方式爲客户端重新產生認證。

```
1 [root@dywH ~]# ssh-keygen -R 192.168.122.7 -y
```

3. 如果只是練習系統，沒有其他信任主機，也可以直接刪除 ~/.ssh/known_hosts，檔案中的所有信任主機紀錄都刪除。

```
1 [dywang@dywssd ~]$ rm -f /home/dywang/.ssh/known_hosts
```

1.11.2 UseDNS

1. sshd 預設使用 DNS，也就是連線時會使用 DNS 反查 IP 的主機名稱是否匹配。ssh 遠端連線回應很慢，很可能是反查時花太多的時間，這時可 server 的 /etc/ssh/sshd_config 設定不使用 DNS，連線時只要認證成功就可登入。

```
1 [root@kvm5 ~]# vim /etc/ssh/sshd_config
  [root@kvm5 ~]# grep DNS /etc/ssh/sshd_config
3 UseDNS no
```

2. 重新啓動 sshd 服務。

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

1.11.3 GSSAPIAuthentication

1. 當使用 SSH 或 SFTP 連接某台主機時，會有一系列的檢查以保證你能够連接到你想連接的主機。其中一項是“reverse lookup on the IP address”檢查機器名稱和你要連接的主機名稱一致。否則，會有以下的錯誤訊息。

```
reverse mapping checking getaddrinfo for xxx.xxx.xxx.xxx
    [111.110.110.110] failed - POSSIBLE BREAK-IN ATTEMPT!
```

2. 編輯 ssh 設定檔，取消 GSSAPIAuthentication 認證，就不會出現此一訊息。

```
[root@dywhd1 ~]# vim /etc/ssh/ssh_config
[root@dywhd1 ~]# grep GSSAPIAuth /etc/ssh/ssh_config
   GSSAPIAuthentication no
```

3. 如果使用 publickey 認證登入，認證時間非常久，必須取消 GSSAPIAuthentication 認證。

```
[root@dywhd1 ~]# ssh -o GSSAPIAuthentication=no root@kvm7.deyu.wang
```

1.11.4 IPTABLES

1. 登入主機 163.17.10.3 連線時間約 10 秒。

```
[root@dywH ~]# time ssh 163.17.10.3 pwd
/root

real    0m10.500s
user    0m0.029s
sys 0m0.014s
```

2. 關閉 163.17.10.3 的 iptables 防火牆後，連線時間不到 1 秒。

```
[root@dywH ~]# time ssh 163.17.10.3 pwd
/root
```

```
4 real    0m0.476s
  user    0m0.027s
6 sys 0m0.012s
```

3. 檢查爲 iptables nat 的 POSTROUTING 問題。

```
2 *nat
  -A POSTROUTING -s 192.168.122.0/24 -j MASQUERADE
  COMMIT
```

4. 修改成如下規則，重新啓動 iptables 後，ssh 連線正常。

```
1 *nat
  -A POSTROUTING -o virbr0 -j MASQUERADE
3 COMMIT
```

1.11.5 Connection reset by peer

1. 登入主機 kvm7.deyu.wang 出現以下訊息：

```
1 [root@dyw219 ~]# ssh kvm7.deyu.wang
  Read from socket failed: Connection reset by peer
```

2. 開啓 kvm7.deyu.wang 終端機，重新產生 ssh key。

```
2 [root@kvm7 ~]# ssh-keygen -t rsa -f /etc/ssh/ssh_host_rsa_key -N ''
  [root@kvm7 ~]# ssh-keygen -t dsa -f /etc/ssh/ssh_host_dsa_key -N ''
```

3. 刪除 client 端信任主機紀錄。

```
[root@dyw219 ~]# sed -i '/kvm7/d' .ssh/known_hosts
```

4. 成功登入。

```
[root@dyw219 ~]# ssh kvm7.deyu.wang
Warning: Permanently added 'kvm7.deyu.wang,192.168.122.7' (RSA) to the
    list of known hosts.
root@kvm7.deyu.wang's password:
Last login: Tue Sep 22 13:10:21 2015 from dynamic5.deyu.wang
```

1.11.6 SCP RSYNC Not Work

1. SSH 連線正常，但 scp rsync 卻卡住，顯示除錯過程，卡在 exec request accepted on channel 0：

```
[root@dns ~]# scp -vvvvv aaa 163.17.27.219:
.....
debug2: channel_input_status_confirm: type 99 id 0
debug2: exec request accepted on channel 0
debug3: Wrote 64 bytes for a total of 1573
```

2. rsync 出現以下錯誤訊息。

```
[root@dywang ~]# rsync -v aaa 163.17.27.219:
reverse mapping checking getaddrinfo for e.csie.personal.static.219
.ippool.cyut.edu.tw [163.17.27.219] failed - POSSIBLE BREAK-IN ATTEMPT!
protocol version mismatch -- is your shell clean?
(see the rsync man page for an explanation)
rsync error: protocol incompatibility (code 2) at compat.c(171) [sender
    =3.0.6]
```

3. SSH 要連線的遠端修改以下設定後，重新啓動 sshd 服務。

```
[root@dyw219 ~]# vim /etc/ssh/sshd_config
[root@dyw219 ~]# egrep '^(UseDNS|GSSAPIAu)' /etc/ssh/sshd_config
```

```
GSSAPIAuthentication no
UseDNS no
[root@dyw219 ~]# /etc/init.d/sshd restart
```

4. 再執行 rsync 連線，錯誤訊息減少如下：

```
[root@dywang ~]# rsync -v aaa 163.17.27.219:
protocol version mismatch -- is your shell clean?
(see the rsync man page for an explanation)
rsync error: protocol incompatibility (code 2) at compat.c(171) [sender
   =3.0.6]
```

5. 出現以上錯誤訊息，主要是連線時取得 shell 時的設定或腳本有問題，經檢查是 /etc/bashrc 環境變數 TERM 造成，移除後正常。

```
[root@dyw219 ~]# diff -uN /etc/bashrc scptmp/bashrc
--- /etc/bashrc 2013-10-02 17:06:18.000000000 +0800
+++ scptmp/bashrc   2017-06-26 07:44:11.000000000 +0800
@@ -84,3 +84,4 @@
     unset pathmunge
 fi
 # vim:ts=4:sw=4
+env TERM=linux setterm -regtabs 4
```

1.12 TMUX 多視窗

1. tmux 是一套 tty 下的多視窗程式，可於視窗中切出多個水平或垂直視窗，並可開啓不同的 Session，Session 下又可開啓多個分項。不同專案可用不同 Session 代表，各分項可想成專案內的不同檔案。

2. 用法：在終端機下 tmux 指令，即開啓一個 Session，此時亦同時開啓一個分項（在下方可看到 0:bash*），表示目前所在位置爲 0:bash*。

3. 操作方式：<Ctrl+b> + 功能鍵，以下使用 <c-b> 代表 <Ctrl+b>。

4. 多個分項操作指令

```
<c-b> + c       開啓另一個分項
<c-b> + 數字     跳到那一個分項
<c-b> + w       選擇要到哪一個分項
<c-b> + n       跳到下一個分項
<c-b> + p       跳到上一個分項
<c-b> + l       會到上次的分項，2個分項互相切換
<c-b> + ,       替此分項暫時命名，可以知道是開啓哪個檔案
<c-b> + &       關掉目前這個分項
<c-b> + d       將 tmux 放到背景中，回到前端終端機
```

5. 單一分項分割視窗

```
<c-b> + "       水平分割視窗
<c-b> + %       垂直分割視窗
<c-b> + 空白鍵   重新排列視窗
<c-b> + 方向鍵   切換分割視窗
<c-b> + 方向鍵   （同時）調整分割視窗大小
<c-b> + x       關掉目前的分割視窗
<c-b> + q       顯示第幾個分割視窗
<c-b> + f       尋找所有分項內的分割視窗
<c-b> + t       顯示時間（有點類似屏保作用）
<c-b> + !       將目前的分割視窗開成單獨一個分項
```

6. <c-b> + ? 可列出所有指令的說明：

```
bind-key      C-b send-prefix                                [33/33]
bind-key      C-o rotate-window
bind-key      C-z suspend-client
bind-key    Space next-layout
bind-key        ! break-pane
bind-key        " split-window
bind-key        # list-buffers
bind-key        $ command-prompt -I #S "rename-session '%%'"
bind-key        % split-window -h
bind-key        & confirm-before -p "kill-window #W? (y/n)" kill-
    window
bind-key        ' command-prompt -p index "select-window -t ':%%'"
bind-key        ( switch-client -p
bind-key        ) switch-client -n
bind-key        , command-prompt -I #W "rename-window '%%'"
bind-key        - delete-buffer
bind-key        . command-prompt "move-window -t '%%'"
bind-key        0 select-window -t :0
bind-key        1 select-window -t :1
bind-key        2 select-window -t :2
bind-key        3 select-window -t :3
```

```
bind-key          4 select-window -t :4
bind-key          5 select-window -t :5
bind-key          6 select-window -t :6
bind-key          7 select-window -t :7
bind-key          8 select-window -t :8
bind-key          9 select-window -t :9
bind-key          : command-prompt
bind-key          ; last-pane
bind-key          = choose-buffer
bind-key          ? list-keys
bind-key          D choose-client
bind-key          L switch-client -l
bind-key          [ copy-mode
bind-key          ] paste-buffer
bind-key          c new-window
bind-key          d detach-client
bind-key          f command-prompt "find-window '%%'"
bind-key          i display-message
bind-key          l last-window
bind-key          n next-window
bind-key          o select-pane -t :.+
bind-key          p previous-window
bind-key          q display-panes
bind-key          r refresh-client
bind-key          s choose-tree
bind-key          t clock-mode
bind-key          w choose-window
bind-key          x confirm-before -p "kill-pane #P? (y/n)" kill-pane
bind-key          z resize-pane -Z
bind-key          { swap-pane -U
bind-key          } swap-pane -D
bind-key          ~ show-messages
bind-key      PPage copy-mode -u
bind-key -r      Up select-pane -U
bind-key -r    Down select-pane -D
bind-key -r    Left select-pane -L
bind-key -r   Right select-pane -R
bind-key        M-1 select-layout even-horizontal
bind-key        M-2 select-layout even-vertical
bind-key        M-3 select-layout main-horizontal
bind-key        M-4 select-layout main-vertical
bind-key        M-5 select-layout tiled
bind-key        M-n next-window -a
bind-key        M-o rotate-window -D
bind-key        M-p previous-window -a
bind-key -r    M-Up resize-pane -U 5
bind-key -r  M-Down resize-pane -D 5
bind-key -r  M-Left resize-pane -L 5
bind-key -r M-Right resize-pane -R 5
bind-key -r    C-Up resize-pane -U
bind-key -r  C-Down resize-pane -D
bind-key -r  C-Left resize-pane -L
bind-key -r C-Right resize-pane -R
```

Chapter 2

IPtables 防火牆

2.1 IPtables 簡介

1. Red Hat Documents
2. CentOS IPTables
3. IPtables 是 linux kernel 2.4, 2.6, 3.0 中內建的防火牆套件，預設的規則爲允許全部封包通過。
4. IPtables 語法爲：

```
iptables -t <table> <chain> <rules> -j <target>
```

5. iptables 定義 table, chain 及 rules 三個資料來處理封包的傳送。

2.2 內建表格 tables

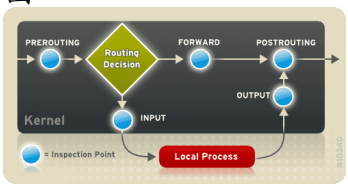
1. 表格 table 內建有 filter, nat, mangle, raw, secuirty 五種，若不指定 table，預設爲 filter。
   (a) filter : 預設處理網路封包的的表格。
   (b) nat : 改變封包以用於網路位址轉換 (Network Address Translation, NAT)。
   (c) mangle : 用於封包服務類型、TTL、標記等變更。破壞表格 magle 在 kernel 2.4.17 之前只有 PREROUTING 及 OUTPUT 兩個鏈，2.4.18 之後又把 INPUT, FORWARD, POSTROUTING 三個鏈加入，主要用於修改封包的服務類型、TTL、標記等，平常較少用。

(d) raw：只使用在 PREROUTING 鏈和 OUTPUT 鏈上，可以對收到的封包在連接跟蹤前進行處理。例如在不需要做 nat 的情況下，爲提高性能讓 web 伺服器 80 埠不再讓 iptables 做封包的鏈接跟蹤處理，以提高用户的訪問速度。

(e) security：用於強制存取控制 (Mandatory Access Control, MAC) 網路規則，例如以 SECMARK and CONNSECMARK targets 啓用的規則。

2.3 內建鏈 chains

1. 鏈 chain 包含五種，封包在 iptables 的過濾情形，如紅帽官網上的封包過濾圖。



(a) INPUT：應用於進入本主機的網路封包。

(b) OUTPUT：應用於由本主機送出的網路封包。

(c) FORWARD：應用於經由本主機轉送的網路封包。

(d) PREROUTING：應用於進行路由前的網路封包。

(e) POSTORTING：應用於被送出前的網路封包。

2. 並不是每種表格都包含所有的鏈，各 table 內建鏈如下：

(a) filter table 內建鏈：INPUT, OUTPUT, FORWARD。

(b) nat table 內建鏈：PREROUTING, OUTPUT, POSTROUTING。

(c) mangle table 內建鏈：INPUT, OUTPUT, FORWARD, PREROUTING, POSTROUTING。

(d) raw table 內建鏈：OUTPUT, PREROUTING。

(e) security table 內建鏈：INPUT, OUTPUT, FORWARD。

3. 如果不啓動 NAT 功能的 Linux 主機，只要使用過濾表格 filter 的 INPUT 及 OUTPUT 鏈就夠了。

4. 啓用 NAT 主機，除過濾功能外，還要考慮 FORWARD 轉送功能，且要使用位址轉換表格的 POSTROUTING 鏈，將符合規則的封包，其封包位址由內網私有 IP 僞裝 (MASQUERADE) 成 NAT 對外 IP，才能連上網際網路。

5. 鏈的命令選項：

(a) -A, –append chain rule-specification
在最後加入一條鏈

(b) -D, –delete chain rule-specification
刪除一條鏈

(c) -D, –delete chain rulenum
刪除一條或多條鏈，rulenum 爲規則的編號

(d) -I, –insert chain [rulenum] rule-specification
在 rulenum 前加入一條鏈，預設 rulenum 爲 1。

(e) -R, –replace chain rulenum rule-specification
取代某一條鏈的規則

(f) -L, –list [chain]
列出目前的鏈，不指定則列出所有的鏈。

(g) -S, –list-rules [chain]
列出指定鏈的所有規則，不指定鏈，則列出所有鏈的所有規則，類似 `iptables-save`。

(h) -F, –flush [chain]
清除指定的鏈，不指定鏈，則清除所有的鏈。

(i) -Z, –zero [chain [rulenum]]
重設 (歸零) 流量記數器 (counter)。當執行完 `-L` 後再執行 `-Z` 命令，某些封包可能會在這期間通過。因此，可以把 `-L` 及 `-Z` 同時使用，在讀取的同時進行記數器重設。

(j) -N, –new-chain chain
產生用户自訂的鏈。

(k) -X, –delete-chain [chain]
刪除用户自的的鏈。

(l) -P, –policy chain target
設定指定鏈的政策到給予的 target，

(m) -E, –rename-chain old-chain new-chain
重新命名指定的鏈。

2.4 規則 Rules

1. IPTables 分析進入主機的網路封包，針對封包的表頭資料 (Header) 進行過濾條件 rules 的設定，對連線封包進行「放行符合」與「封鎖不符合」或「丟棄不符合」的雙向安全管理機制。
2. 規則是以列表的方式被加進每條規則鏈。
3. 每個封包會從第一條規則開始檢查，依序至最後一條。
4. 若封包符合其中一條規則，對應的動作就會被執行，例如接受 (ACCEPT) 或丟棄 (DROP) 封包，且不再檢查後面的規則。
5. 若封包通過所有檢查且不符合任何規則鏈內的任何一條規則，則執行該條規則鏈的預設動作，也就是預設政策。
6. 預設政策可以設定爲接受 (ACCEPT) 或丟棄 (DROP) 封包。
   (a) 預設政策丟棄 (DROP) 所有封包：必須加入規則來接受 (ACCEPT) 來自信任 IP 位址的封包，或者開啓那些提供服務的連接埠，如：FTP 伺服器、網頁伺服器、mail 伺服器等。一般用於 INPUT 規則鏈。
   (b) 預設政策接受 (ACCEPT) 所有封包：必須加入規則來攔截 (DROP) 來自有問題 IP 位址或系列的封包，也或者阻止封包進出只作私人用途或未提供服務的連接埠。一般用於 OUTPUT 規則鏈。

2.5 動作 Target

1. Targets 動作有很多，以下只列出一部分。但並不是任何 table 都可以使用所有的動作，例如 MASQUERADE 只能用在 nnat 表上：
   (a) ACCEPT ：接受該封包。
   (b) DROP ：丟棄封包。
   (c) REJECT ：丟棄封包但回應 cilent。
   (d) LOG ：將該封包的資訊記錄下來 (預設記錄到 /var/log/messages 檔案)
   (e) QUEUE ：將該封包送到用户空間，用户空間如何接受此封包，不同的 kernel 版本有不同的作法。
   (f) RETURN ：停止這條鏈的傳送並回到前一條鏈的下一規則，如果已到最後一條規則或符合 RETURN target，則由鏈政策決定封包的命運。
   (g) MASQUERADE ：僞裝 IP。

2. REJCET 與 DROP 比較：

   (a) DROP 丟棄封包；REJECT 丟棄封包外，還會送一個 ICMP host-unreachable 回應到來源 IP。

   (b) 只要不做 LOG 的動作，從 CPU 及記憶體性能的角度考量，這兩種的差異很小。

   (c) 從網路性能的角度，DROP 當然比較簡單，因爲只是丟棄封包；REJECT 則比較容易讓駭客使用欺騙 (spoofing) 手法進行 DoS 攻擊。因此，從安全的考量角度，使用 DROP 是比較安全。

   (d) 從 IP 來源用户端的性能角度看，REJECT 是比較好的。因爲 DROP 動作，用户端得不到回應，它必須一直等到逾時；而 REJECT 動作會送一個 ICMP 封包回到用户端，用户端不用等到 timeout，很快可以得到結果。

2.6 預設環境

1. 檢查 iptables 哪些表格被載入，目前只有過濾 filter 表格被載入。

```
[root@kvm8 ~]# lsmod | grep ip_tables
ip_tables              17831  1 iptable_filter
```

2. iptables 用選項 -L 檢查 iptables 啓動後預設的規則，可以看到有 INPUT, FORWARD, OUTPUT 三條鏈，且預設政策都是 ACCEPT。

```
[root@kvm8 ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere             state RELATED,
    ESTABLISHED
ACCEPT     icmp --  anywhere             anywhere
ACCEPT     all  --  anywhere             anywhere
ACCEPT     tcp  --  anywhere             anywhere             state NEW tcp dpt
    :ssh
REJECT     all  --  anywhere             anywhere             reject-with icmp-
    host-prohibited

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
REJECT     all  --  anywhere             anywhere             reject-with icmp-
    host-prohibited

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

3. 雖然 INPUT 及 FORWARD 鏈的預設政策是 ACCEPT，但在規則的最後一條 REJECT 來自 anywhere 到 anywhere，任何 port 的封包，都以 icmp-host-prohibited type REJECT，一樣可以達到「不符合接受規則的封包都拒絕的目標」。

2.7 實機設定

1. 使用選項命令，可以完成 iptables 所有的設定，不過若沒有執行 /etc/init.d/iptables save，重新開機後還是會回到預設值，執行 save 的目的是將目前防火牆設定寫入 /etc/sysconfig/iptables。所以設定防火牆可以直接編輯此檔。

2. INPUT 鏈範例：利用 -m 選項來載入模組 state 。state 模塊能夠檢視一個封包並判斷它的狀態是 NEW、ESTABLISHED 抑或 RELATED。NEW 指進入的封包屬於不是由主機起始的新增連線。ESTABLISHED 及 RELATED 指進入的封包隸屬於一條現存的連線，或者與現存的連線有關係。-m tcp 或 --match tcp 載入 tcp 模組，這個動作已包含在 -p tcp 中，不過明確的指明載入 tcp 模組也無害。

```
[root@kvm8 ~]# vim /etc/sysconfig/iptables
.............
-A INPUT -m state --state NEW -m tcp -p tcp --dport 21 ! -s
   192.168.122.0/24 -j REJECT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 21 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 5000:5005 -j ACCEPT
.............
```

   (a) 不是來自 192.168.122.0/24 通過 tcp 連接埠 21 連線的封包都 REJECT。

   (b) 因 iptables 過濾規則是有順序的檢查，在前一條已拒絕不是來自 192.168.122.0/24 的封包，所以這一條只要是通過 tcp 連接埠 21 連線的封包都接受。

   (c) 只要是通過 tcp 連接埠 5000 到 5005 連線的封包都接受。

3. FORWARD 鏈範例：做爲 NAT 轉傳。

```
[root@kvm8 ~]# vim /etc/sysconfig/iptables
.............
-A FORWARD -i eth0 -j ACCEPT
-A FORWARD -d 192.168.1.0/24 -o eth0 -j ACCEPT
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
.............
```

(a) -i 選項表示 interface「介面」，來自網卡 eth0 的封包都接受並轉傳。

(b) 目的 IP 爲 192.168.1.0/24，送到 eth0 網卡的封包都接受並轉傳。

(c) 不符合以上兩條規則的封包，都拒絕轉傳。

4. POSTROUTING 鏈範例：做爲 NAT，從介面 eth1 送出的封包，都以介面 eth1 的 IP 僞裝。

```
[root@kvm8 ~]# vim /etc/sysconfig/iptables
.............
-A POSTROUTING -o eth1 -j MASQUERADE
.............
```

5. 防火牆重新啓動

```
[root@kvm8 ~]# /etc/init.d/iptables restart
```

6. 開機啓動防火牆

```
[root@kvm8 ~]# chkconfig iptables on
```

Chapter 3

FTP Server

3.1 FTP 簡介

1. File Transfer Protocol (FTP) 是一種 client server 架構的檔案傳輸協定，使用者可以不用登入 server 下，傳輸檔案。
2. FTP 使用多個 ports，FTP 開始連接時使用 server port 21，連上後要傳送資料使用的 ports，要看使用的模式及設定。
3. FTP 模式：Passive and Active modes
4. Active mode
   (a) FTP client 開啓一個隨機選擇的 TCP port 呼叫 FTP server 的 port 21 請求連線。順利完成 Three-Way Handshake 後，連線成功建立。
   (b) client 告訴 server，client 可以用另一個 TCP port 做數據通道。
   (c) server 用 port 20 和剛才 client 所告知的 TCP port (大於 1024) 建立數據連線。傳送包含 SYC flag 的數據包給 client。
   (d) client 返回一個帶 ACK flag 的確認封包，完成另一次的 Three-Way Handshake 手續。
   (e) 開始數據傳送。
5. Active mode 缺點：由於數據傳輸 port 是由 client 指定，一般 server 都有防火牆，不太可能打開所有 1024 以上的 ports。
6. Passive mode
   (a) FTP client 開啓一個隨機選擇的 TCP port 呼叫 FTP server 的 port 21 請求連線，並完成命令通道的建立。

(b) client 送一個 PASV command 給 server，要求進入 passive 傳輸模式。

(c) server （依設定範圍）隨機選一個 TCP port ，用命令通道告訴 client。

(d) client 呼叫剛才 server 告知的 TCP port 建立數據通道。此時封包帶 SYN flag。

(e) server 確認後回應一個 ACK 封包。完成所有交握手續並成功建立數據通道。

(f) 開始數據傳送。

3.2 FTP server 架設

1. 安裝 vsftpd 套件

```
[root@kvm8 ~]# yum install vsftpd
```

2. 編輯 vsftpd 設定：讓匿名者可以使用 vsftp

```
[root@kvm8 ~]# vim /etc/vsftpd/vsftpd.conf
# Allow anonymous FTP? (Beware - allowed by default if you comment this
    out).
anonymous_enable=YES
```

3. 編輯 vsftpd 設定：開啓被動模式及設定資料傳輸 ports

```
[root@kvm8 ~]# vim /etc/vsftpd/vsftpd.conf
.................
pasv_enable=YES     <= passive mode
pasv_min_port=5000  <= minimum port
pasv_max_port=5005  <= maximum port
```

4. 編輯 vsftpd 設定：讓用户不能離開自己的家目錄

```
[root@kvm8 ~]# vim /etc/vsftpd/vsftpd.conf

# You may specify an explicit list of local users to chroot() to their
    home
# directory. If chroot_local_user is YES, then this list becomes a list
    of
# users to NOT chroot().
chroot_local_user=No  ## 用户登入只能在自己的家目錄
```

```
chroot_list_enable=YES
# (default follows)
chroot_list_file=/etc/vsftpd/chroot_list

[root@kvm8 ~]# vim /etc/vsftpd/chroot_list
linda  ## 列出要限制的使用者
```

5. 啓動 vsftpd 服務

```
[root@kvm8 ~]# /etc/init.d/vsftpd restart
Shutting down vsftpd:                                      [FAILED]
Starting vsftpd for vsftpd:                                [  OK  ]
```

6. 設定開機啓動 vsftpd 服務

```
[root@kvm8 ~]# chkconfig vsftpd on
```

3.3 安全機制

1. 防火牆設定-任何網域皆可使用 ftp

```
[root@kvm8 ~]# vim /etc/sysconfig/iptables

*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
#########################################################
-A INPUT -m state --state NEW -m tcp -p tcp --dport 21 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 5000:5005 -j ACCEPT
#########################################################
-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

2. 防火牆設定-只有 192.168.122.0/24 網域可使用 ftp

```
[root@kvm8 ~]# vim /etc/sysconfig/iptables

########################################################
-A INPUT -m state --state NEW -m tcp -p tcp --dport 21 ! -s
    192.168.122.0/24 -j REJECT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 21 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 5000:5005 -j ACCEPT
########################################################
```

3. 防火牆重新啓動

```
[root@kvm8 ~]# /etc/init.d/iptables restart
```

4. 開機啓動防火牆

```
[root@kvm8 ~]# chkconfig iptables on
```

5. SELinux 有關 ftp 的設定：如果要讓用户可以上傳及下載，必須開啓 allow_ftpd_full_access。

```
[root@kvm8 ~]# getsebool -a | grep ftp
allow_ftpd_anon_write --> off
allow_ftpd_full_access --> off
allow_ftpd_use_cifs --> off
allow_ftpd_use_nfs --> off
ftp_home_dir --> off
ftpd_connect_db --> off
httpd_enable_ftp_server --> off
tftp_anon_write --> off
```

3.4 SSL 設定

1. 產生證書及 key

```
[root@dywftp ~]# openssl req -days 3650 -new -x509 -nodes \
> -out /etc/pki/tls/private/vsftpd.pem -keyout /etc/pki/tls/private/
    vsftpd.key \
> -subj '/C=TW/ST=Taiwan/L=CYUT/O=CSIE/CN=csie.cyut Certificate
    Authority'
Generating a 2048 bit RSA private key
```

```
.....................................................+++
.................................+++
writing new private key to '/etc/pki/tls/private/vsftpd.key'
```

2. 編輯 vsftpd 設定：指定證書及 key

```
[root@dywftp ~]# vim /etc/vsftpd/vsftpd.conf
[root@dywftp ~]# grep rsa /etc/vsftpd/vsftpd.conf
rsa_cert_file=/etc/pki/tls/private/vsftpd.pem
rsa_private_key_file=/etc/pki/tls/private/vsftpd.key
```

3. 編輯 vsftpd 設定：啓動 SSL，不允許匿名用户，強制資料傳輸及登入都使用 SSL。

```
[root@dywftp ~]# vim /etc/vsftpd/vsftpd.conf
[root@dywftp ~]# tail -n4 /etc/vsftpd/vsftpd.conf
ssl_enable=YES
allow_anon_ssl=NO
force_local_data_ssl=YES
force_local_logins_ssl=YES
```

4. 編輯 vsftpd 設定：明確的限制使用 TLS v1，其安全性高於 SSL。

```
[root@dywftp ~]# vim /etc/vsftpd/vsftpd.conf
[root@dywftp ~]# tail -n3 /etc/vsftpd/vsftpd.conf
ssl_tlsv1=YES
ssl_sslv2=NO
ssl_sslv3=NO
```

5. 編輯 vsftpd 設定：因已設定數據與控制流使用不相同通道，所以取消數據與控制流使用相同通道的設定。

```
[root@dywftp ~]# vim /etc/vsftpd/vsftpd.conf
[root@dywftp ~]# tail -n1 /etc/vsftpd/vsftpd.conf
require_ssl_reuse=NO
```

6. 編輯 vsftpd 設定：憑證的加密模式，預設 DES。

```
[root@dywftp ~]# vim /etc/vsftpd/vsftpd.conf
[root@dywftp ~]# tail -n1 /etc/vsftpd/vsftpd.conf
```

```
3 ssl_ciphers=HIGH
```

7. 重新啓動 vsftpd 服務

```
1 [root@dywftp ~]# /etc/init.d/vsftpd restart
  Shutting down vsftpd:                                      [  OK  ]
3 Starting vsftpd for vsftpd:                                [  OK  ]
```

8. 設定開機啓動 vsftpd 服務

```
1 [root@kvm8 ~]# chkconfig vsftpd on
```

3.5 ftps client – lftp

1. 使用 lftp 下載 ftps server 中的檔案

```
1  [root@dywH ~]# lftp
   lftp :~> set ftp:ssl-force true
3  lftp :~> connect dywftp.csie.cyut.edu.tw
   lftp dywftp.csie.cyut.edu.tw:~> login download
5  Password:
   lftp download@dywftp.csie.cyut.edu.tw:~> ls
7  -rw-r--r--    1 0        0           91984 Jan 24 12:45 1031_1A.pdf
   -rw-r--r--    1 0        0           94024 Jan 24 12:45 1031_1B.pdf
9  -rw-r--r--    1 0        0           77287 Jan 24 12:45 1031assess.pdf
   -rw-r--r--    1 0        0           77370 Jan 24 12:45 1031assess1A.pdf
11 -rw-r--r--    1 0        0           77415 Jan 24 12:45 1031assess1B.pdf
   -rw-r--r--    1 0        0          360442 Jan 24 12:45 1031course_ieet.
      pdf
13 -rw-r--r--    1 0        0          360539 Jan 24 12:45 1031
      course_ieet1A.pdf
   -rw-r--r--    1 0        0          360540 Jan 24 12:45 1031
      course_ieet1B.pdf
15 -rw-r--r--    1 0        0           51820 Jan 24 12:45 1031timetable.
      pdf
   -rw-r--r--    1 0        0           95160 Jul 02 02:46 1032assess.pdf
17 -rw-r--r--    1 0        0          396448 Jul 02 02:46 1032course_ieet.
      pdf
   -rw-r--r--    1 0        0           21540 Jul 02 02:45 assess.odt
19 -rw-r--r--    1 0        0           48545 Jul 02 02:45 course_ieet.odt
   lftp download@dywftp.csie.cyut.edu.tw:/> get 1032assess.pdf
21 95160 bytes transferred
   lftp download@dywftp.csie.cyut.edu.tw:/>
```

2. 寫成 shell script 自動下載。

```
[root@dywH ~]# vim lftp_dywftp.sh
[root@dywH ~]# cat lftp_dywftp.sh
#!/bin/bash
lftp -u username,'password' ftp://dywftp.csie.cyut.edu.tw <<EOF
# the next 2 lines put you in ftpes mode
set ftp:ssl-force true
set ftp:ssl-protect-data true
mget 1032*.pdf
exit
EOF
[root@dywH ~]# sh lftp_dywftp.sh
[root@dywH ~]# ll 1032*.pdf
-rw-r--r--. 1 root root  95160 Jul  2 10:46 1032assess.pdf
-rw-r--r--. 1 root root 396448 Jul  2 10:46 1032course_ieet.pdf
```

Chapter 4

Apache 2.2 HTTP Server

4.1 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. 跨平台且安全性高，是最流行的 Web 伺服器端軟體之一。
3. 支援 Perl，Python，Tcl，和 PHP。

4.2 Apache HTTP server 架設

1. 安裝 httpd 套件

```
[root@kvm8 ~]# yum install httpd
```

2. 啓動 httpd 服務

```
[root@kvm8 ~]# /etc/init.d/httpd restart
Stopping httpd:                                            [FAILED]
Starting httpd:                                            [  OK  ]
```

3. 設定開機啓動 httpd 服務

```
[root@kvm8 ~]# chkconfig httpd on
```

4.3 UserDir 用户個人網頁

1. UserDir 模組：可以讓伺服器中的用户，擁有自己的網頁。例如：http://kvm8.deyu.wang/~deyu1

```
[root@kvm8 ~]# vim /etc/httpd/conf/httpd.conf

<IfModule mod_userdir.c>
    #
    # UserDir is disabled by default since it can confirm the presence
    # of a username on the system (depending on home directory
    # permissions).
    #
    #UserDir disabled  <= 註解這一行

    #
    # To enable requests to /~user/ to serve the user's public_html
    # directory, remove the "UserDir disabled" line above, and uncomment
    # the following line instead:
    #
    UserDir public_html  <= 取消註解這行，個人網頁根目錄爲 public_html

</IfModule>

#
# Control access to UserDir directories.  The following is an example
# for a site where these directories are restricted to read-only.
#
<Directory /home/*/public_html>
    AllowOverride FileInfo AuthConfig Limit
    Options MultiViews Indexes SymLinksIfOwnerMatch IncludesNoExec
    <Limit GET POST OPTIONS>
        Order allow,deny
        Allow from all
    </Limit>
    <LimitExcept GET POST OPTIONS>
        Order deny,allow
        Deny from all
    </LimitExcept>
</Directory>
```

4.4 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。

```
[root@kvm8 ~]# vim /etc/httpd/conf/httpd.conf
```

```
NameVirtualHost *:80  <= 取消註解

### 原始主機名稱 kvm8.deyu.wang 根目錄 /var/www/html 也必須加入
<VirtualHost *:80>
    DocumentRoot /var/www/html
    ServerName kvm8.deyu.wang
</VirtualHost>
### 加入另一主機名稱 www.deyu.wang 的根目錄爲 /var/www/virtual
<VirtualHost *:80>
    DocumentRoot /var/www/virtual
    ServerName www.deyu.wang
</VirtualHost>
```

2. 設定完必須啓動 httpd 服務或 reload 設定參數。

```
[root@kvm8 ~]# /etc/init.d/httpd restart
Stopping httpd:                                            [  OK  ]
Starting httpd:                                            [  OK  ]
```

4.5 存取限制

1. httpd 限制順序先允許後拒絕，接著即使刪除 Allow from all 這一行，都表示全部允許。

```
[root@kvm8 ~]# vim /etc/httpd/conf/httpd.conf
<Directory "/var/www/virtual">
    Order allow,deny  <= 先查允許的主機，再查限制的主機
    Allow from all <= 允許所有主機存取 /var/www/virtual
</Directory>
```

2. httpd 限制順序先拒絕後允許，接著沒有輸入允許或拒絕的主機，則預設全部拒絕，此狀況等於不開放網站。

```
[root@kvm8 ~]# vim /etc/httpd/conf/httpd.conf
<Directory "/var/www/virtual">
    Order deny,allow  <= 先查拒絕的主機，再查允許的主機
</Directory>
```

3. httpd 限制只有 kvm8.deyu.wang 這台主機可以存取。

```
[root@kvm8 ~]# vim /etc/httpd/conf/httpd.conf
<Directory "/var/www/virtual">
    Order allow,deny  <= 先查允許的主機，再查限制的主機
    Allow from kvm8.deyu.wang <= 只允許主機 kvm8.deyu.wang 存取 /var/www
        /virtual
</Directory>
```

4. httpd 限制只有 deyu.wang 網域的主機可以存取。

```
[root@kvm8 ~]# vim /etc/httpd/conf/httpd.conf
<Directory "/var/www/virtual">
    Order allow,deny  <= 先查允許的主機，再查限制的主機
    Allow from deyu.wang <= 只允許主機 kvm8.deyu.wang 存取 /var/www/
        virtual
</Directory>
```

5. httpd 限制只有 kvm8.deyu.wang 及 kvm4.deyu.wang 這兩台主機可以存取。

```
[root@kvm8 ~]# vim /etc/httpd/conf/httpd.conf
<Directory "/var/www/virtual">
    Order allow,deny  <= 先查允許的主機，再查限制的主機
    Allow from kvm8.deyu.wang kvm4.deyu.wang 存取 /var/www/virtual
</Directory>
```

4.6 安全機制

1. 防火牆設定-任何網域皆可使用 http

```
[root@kvm8 ~]# vim /etc/sysconfig/iptables

*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
#####################################################
-A INPUT -m state --state NEW -m tcp -p tcp --dport 80 -j ACCEPT
#####################################################
-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
```

```
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

2. 防火牆設定-只有 192.168.122.0/24 網域可使用 http

```
[root@kvm8 ~]# vim /etc/sysconfig/iptables

##########################################################
-A INPUT -m state --state NEW -m tcp -p tcp --dport 80 -s
    192.168.122.0/24 -j ACCEPT
##########################################################
```

3. 防火牆重新啓動

```
[root@kvm8 ~]# /etc/init.d/iptables restart
```

4. 開機啓動防火牆

```
[root@kvm8 ~]# chkconfig iptables on
```

5. 測試主機 kvm8.deyu.wang 網頁

```
[root@kvm8 ~]# echo 'kvm8.deyu.wang test' > /var/www/html/index.html

## selinux 管制
## 1. 直接產生檔案於 /var/www/html 目錄下，其 selinux type 自動爲
####  httpd_sys_content_t，可以不用變更 type，就可存取。
## 2. 若從某一目錄，例如 /root，複製檔案到 /var/www/html 下，
####  selinux type 爲原先設定，必須變更 type，才能存取。
[root@kvm8 ~]# chcon -R -t httpd_sys_content_t /var/www/html/

## 從 deyu.wang 測試網頁
[root@dyH ~]# wget http://kvm8.deyu.wang

100%[======================================>] 20          --.-K/s   in 0
    s

2013-08-01 18:50:59 (2.39 MB/s) - “index.html” saved [20/20]

[root@dyH ~]# cat index.html
kvm8.deyu.wang test
```

6. 測試主機 www.deyu.wang 網頁

```
[root@kvm8 ~]# echo 'www.deyu.wang test' > /var/www/virtual/index.html

## 從 deyu.wang 測試網頁， www.deyu.wang 只有kvm8.deyu.wang 能存取
[root@dyH ~]# wget http://www.deyu.wang
--2013-08-01 18:53:26--  http://www.deyu.wang/
Resolving www.deyu.wang... 192.168.122.8
Connecting to www.deyu.wang|192.168.122.8|:80... connected.
HTTP request sent, awaiting response... 403 Forbidden
2013-08-01 18:53:26 ERROR 403: Forbidden.

## 從 kvm8.deyu.wang 測試網頁
[root@kvm8 ~]# wget http://www.deyu.wang

100%[======================================>] 19          --.-K/s   in 0
    s

[root@kvm8 ~]# cat index.html
www.deyu.wang test
```

7. 測試個人網頁

```
[root@kvm8 ~]# mkdir /home/deyu1/public_html
[root@kvm8 ~]# echo 'userdir test' > /home/deyu1/public_html/index.html
[root@kvm8 ~]# chown deyu1.deyu1 -R /home/deyu1/public_html

## 目錄權限放寬
[root@kvm8 ~]# ll -d /home/deyu1
drwx------. 5 deyu1 deyu1 1024 Aug  1 19:49 /home/deyu1
[root@kvm8 ~]# chmod a+r /home/deyu1
[root@kvm8 ~]# ll -d /home/deyu1
drwxr-xr-x. 5 deyu1 deyu1 1024 Aug  1 19:49 /home/deyu1

## selinux type
[root@kvm8 ~]# getenforce
Enforcing
[root@kvm8 ~]# ll -Z /home/deyu1/public_html/
-rw-r--r--. root root unconfined_u:object_r:user_home_t:s0 index.html

## selinux 管控，無法存取
[root@kvm8 ~]# wget http://www.deyu.wang/~deyu1
--2013-08-01 19:51:57--  http://www.deyu.wang/~deyu1
Resolving www.deyu.wang... 192.168.122.8
Connecting to www.deyu.wang|192.168.122.8|:80... connected.
HTTP request sent, awaiting response... 403 Forbidden
2013-08-01 19:51:57 ERROR 403: Forbidden.

## 變更 selinux type
[root@kvm8 ~]# chcon -R -t httpd_sys_content_t /home/deyu1/public_html
[root@kvm8 ~]# ll -Z /home/deyu1/public_html/
```

```
29 -rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 index
       .html

31 ## 從 kvm8.deyu.wang 測試網頁，
   [root@kvm8 ~]# wget http://www.deyu.wang/~deyu1
33
   100%[======================================>] 13          --.-K/s   in 0
       s
35
   [root@kvm8 ~]# cat index.html
37 userdir test
```

8. SELinux 有關 http 的設定

```
1  [root@kvm8 ~]# getsebool -a | grep http
   allow_httpd_anon_write --> off
3  allow_httpd_mod_auth_ntlm_winbind --> off
   allow_httpd_mod_auth_pam --> off
5  allow_httpd_sys_script_anon_write --> off
   httpd_builtin_scripting --> on
7  httpd_can_check_spam --> off
   httpd_can_network_connect --> off
9  httpd_can_network_connect_cobbler --> off
   httpd_can_network_connect_db --> off
11 httpd_can_network_memcache --> off
   httpd_can_network_relay --> off
13 httpd_can_sendmail --> off
   httpd_dbus_avahi --> on
15 httpd_enable_cgi --> on
   httpd_enable_ftp_server --> off
17 httpd_enable_homedirs --> off
   httpd_execmem --> off
19 httpd_read_user_content --> off
   httpd_setrlimit --> off
21 httpd_ssi_exec --> off
   httpd_tmp_exec --> off
23 httpd_tty_comm --> on
   httpd_unified --> on
25 httpd_use_cifs --> off
   httpd_use_gpg --> off
27 httpd_use_nfs --> off
```

4.7 AB test

1. 在 Apache 套件工具有個叫 ab(ApacheBench) 的程式，專門用在做壓力測試。安裝套件 httpd-tools。

```
[root@e517nat ~]# yum install httpd-tools
```

2. 在 moodle.cyut.edu.tw 本機直接進行壓力測試，同時 1000 個連線做 20 次，測試結果前 50% 完成連線需要 1722ms，100% 完成連線需要 2141ms。

```
[root@moodle ~]#  ab -n 1000 -c 20 http://moodle.cyut.edu.tw/index.php
This is ApacheBench, Version 2.3 <$Revision: 655654 $>
Copyright 1996 Adam Twiss, Zeus Technology Ltd, http://www.zeustech.net/
Licensed to The Apache Software Foundation, http://www.apache.org/

Benchmarking moodle.cyut.edu.tw (be patient)
Completed 100 requests
Completed 200 requests
Completed 300 requests
Completed 400 requests
Completed 500 requests
Completed 600 requests
Completed 700 requests
Completed 800 requests
Completed 900 requests
Completed 1000 requests
Finished 1000 requests


Server Software:        Apache/2.2.15
Server Hostname:        moodle.cyut.edu.tw
Server Port:            80

Document Path:          /index.php
Document Length:        38781 bytes

Concurrency Level:      20
Time taken for tests:   86.830 seconds
Complete requests:      1000
Failed requests:        0
Write errors:           0
Total transferred:      39357000 bytes
HTML transferred:       38781000 bytes
Requests per second:    11.52 [#/sec] (mean)
Time per request:       1736.599 [ms] (mean)
Time per request:       86.830 [ms] (mean, across all concurrent
   requests)
Transfer rate:          442.64 [Kbytes/sec] received

Connection Times (ms)
              min  mean[+/-sd] median   max
Connect:        0    1   5.5      0      62
Processing:   896 1730 109.4   1722    2141
Waiting:      775 1236  77.5   1230    1615
Total:        897 1730 110.5   1722    2141

```

```
Percentage of the requests served within a certain time (ms)
  50%   1722
  66%   1758
  75%   1782
  80%   1800
  90%   1855
  95%   1905
  98%   1982
  99%   2025
 100%   2141 (longest request)
```

3. 從外部主機 dyw219 進行壓力測試，同時 1000 個連線做 20 次，只能同時 229 個連線，無法完成同時 1000 個連線的測試。經查詢路由中爲防止 DoS 攻擊，限制同一 ip 同時間最多只能 200 sessions。

```
[root@dyw219 nat]# ab -n 1000 -c 20 http://moodle.cyut.edu.tw/index.php
This is ApacheBench, Version 2.3 <$Revision: 655654 $>
Copyright 1996 Adam Twiss, Zeus Technology Ltd, http://www.zeustech.net/
Licensed to The Apache Software Foundation, http://www.apache.org/

Benchmarking moodle.cyut.edu.tw (be patient)
Completed 100 requests
Completed 200 requests
apr_poll: The timeout specified has expired (70007)
Total of 229 requests completed
```

4. 經放行主機 e517nat 後進行壓力測試，同時 1000 個連線做 20 次，測試結果前 50% 完成連線需要 1742ms，100% 完成連線需要 2182ms。

```
[root@e517nat ~]# ab -n 1000 -c 20 http://moodle.cyut.edu.tw/index.php
This is ApacheBench, Version 2.3 <$Revision: 655654 $>
Copyright 1996 Adam Twiss, Zeus Technology Ltd, http://www.zeustech.net/
Licensed to The Apache Software Foundation, http://www.apache.org/

Benchmarking moodle.cyut.edu.tw (be patient)
Completed 100 requests
Completed 200 requests
Completed 300 requests
Completed 400 requests
Completed 500 requests
Completed 600 requests
Completed 700 requests
Completed 800 requests
Completed 900 requests
Completed 1000 requests
Finished 1000 requests

```

```
Server Software:        Apache/2.2.15
Server Hostname:        moodle.cyut.edu.tw
Server Port:            80

Document Path:          /index.php
Document Length:        38781 bytes

Concurrency Level:      20
Time taken for tests:   87.383 seconds
Complete requests:      1000
Failed requests:        0
Write errors:           0
Total transferred:      39357000 bytes
HTML transferred:       38781000 bytes
Requests per second:    11.44 [#/sec] (mean)
Time per request:       1747.652 [ms] (mean)
Time per request:       87.383 [ms] (mean, across all concurrent
    requests)
Transfer rate:          439.84 [Kbytes/sec] received

Connection Times (ms)
              min  mean[+/-sd] median   max
Connect:        0    1   1.0      1      30
Processing:   921 1740 145.2   1741    2181
Waiting:      371 1248 105.8   1249    1588
Total:        922 1740 145.2   1742    2182

Percentage of the requests served within a certain time (ms)
  50%   1742
  66%   1800
  75%   1833
  80%   1853
  90%   1913
  95%   1965
  98%   2024
  99%   2071
 100%   2182 (longest request)
```

4.8 防止 DoS

1. DDoS (distributed denial-of-service) 及 DoS (denial-of-service) 在網路上十分常見，而 DoS 攻擊所傳送的請求跟正常的請求一樣，分別在於每秒鐘發出大量請求到伺服器，使伺服器的負載增加，最常見的情況是伺服器暫停服務。

2. 從主機 dywH 經 ADSL 連線 dywang.csie.cyut.edu.tw 進行壓力測試，同時 1000 個連線做 20 次，測試結果前 50% 完成連線需要 2373ms，100% 完成連線需要 49838ms。

```
[root@dywH ~]# ab -n 1000 -c 20 http://dywang.csie.cyut.edu.tw/moodle23/
    index.php
This is ApacheBench, Version 2.3 <$Revision: 655654 $>
Copyright 1996 Adam Twiss, Zeus Technology Ltd, http://www.zeustech.net/
Licensed to The Apache Software Foundation, http://www.apache.org/

Benchmarking dywang.csie.cyut.edu.tw (be patient)
Completed 100 requests
Completed 200 requests
Completed 300 requests
Completed 400 requests
Completed 500 requests
Completed 600 requests
Completed 700 requests
Completed 800 requests
Completed 900 requests
Completed 1000 requests
Finished 1000 requests


Server Software:        Apache/2.2.15
Server Hostname:        dywang.csie.cyut.edu.tw
Server Port:            80

Document Path:          /moodle23/index.php
Document Length:        64197 bytes

Concurrency Level:      20
Time taken for tests:   168.548 seconds
Complete requests:      1000
Failed requests:        996
   (Connect: 0, Receive: 0, Length: 996, Exceptions: 0)
Write errors:           0
Total transferred:      64891389 bytes
HTML transferred:       64315239 bytes
Requests per second:    5.93 [#/sec] (mean)
Time per request:       3370.955 [ms] (mean)
Time per request:       168.548 [ms] (mean, across all concurrent
    requests)
Transfer rate:          375.98 [Kbytes/sec] received

Connection Times (ms)
              min  mean[+/-sd] median   max
Connect:       25  355 311.4    279    3377
Processing:   923 2991 2502.0   2001   49621
Waiting:      239  606 432.8    476    5617
Total:        953 3346 2517.2   2373   49838

Percentage of the requests served within a certain time (ms)
  50%   2373
  66%   3470
  75%   3850
  80%   4251
  90%   5977
```

```
53   95%   7851
     98%  10004
55   99%  11075
    100%  49838 (longest request)
```

3. mod_evasive 是一個預防 Apache 遭受 DDos 攻擊的模組，可以防止同一個 IP 對相同 URI 發出的大量請求，此模組已納入 DYW Linux REPO 資料庫，可以直接以 yum 指令安裝。

```
[root@dywang ~]# yum install mod_evasive
```

4. 編輯 mod_evasive 模組設定檔。

```
1  [root@dywang ~]# vim /etc/httpd/conf.d/mod_evasive.conf
   [root@dywang ~]# grep DOS /etc/httpd/conf.d/mod_evasive.conf
3      DOSHashTableSize    3097
       DOSPageCount        2
5      DOSSiteCount        50
       DOSPageInterval     1
7      DOSSiteInterval     1
       DOSBlockingPeriod   10
9      #DOSEmailNotify      you@yourdomain.com
       #DOSSystemCommand    "su - someuser -c '/sbin/... %s ...'"
11     #DOSLogDir           "/var/lock/mod_evasive"
       # Multiple DOSWhitelist commands may be used in the configuration.
13     #DOSWhitelist   127.0.0.1
       #DOSWhitelist   192.168.0.*
```

5. 設定選項說明：

   (a) DOSHashTableSize：佔用記憶體的大小，如果伺服器比較繁忙，這個數值要設定大一點。

   (b) DOSPageCount：同一 IP 在一個時段內可以存取同一頁面的次數，超過會被禁止。

   (c) DOSSiteCount：同一 IP 在一個網站內可以佔用多少個請求，超過會禁止。

   (d) DOSPageInterval：DOSPageCount 內的時段設定。

   (e) DOSSiteInterval：DOSSiteCount 的時間設定，以秒爲單位。

   (f) DOSBlockingPeriod：當發現疑似攻擊後，使用者會收到 403 Forbidden，這是設定封鎖的時間，以秒爲單位。

(g) DOSWhitelist：白名單，不做限制。

6. 重新啓動 httpd。

```
[root@dywang ~]# /etc/init.d/httpd restart
```

7. 加入 mod_evasive 模組後，從主機 dywH 經 ADSL 連線 dywang.csie.cyut.edu.tw 進行壓力測試，同時 1000 個連線做 20 次，測試結果無法完成，連線被重置。

```
[root@dywH ~]# ab -n 1000 -c 20 http://dywang.csie.cyut.edu.tw/moodle23/
    index.php
This is ApacheBench, Version 2.3 <$Revision: 655654 $>
Copyright 1996 Adam Twiss, Zeus Technology Ltd, http://www.zeustech.net/
Licensed to The Apache Software Foundation, http://www.apache.org/

Benchmarking dywang.csie.cyut.edu.tw (be patient)
Completed 100 requests
Completed 200 requests
Completed 300 requests
Completed 400 requests
apr_socket_recv: Connection reset by peer (104)
Total of 456 requests completed
```

4.9 實機操作測驗練習題

4.9.1 測驗練習一

1. 在主機 kvmX.deyu.wang 架設網頁伺服器，其中 X 爲您虛擬機的編號，完成以下步驟：

   (a) 下載 ftp://deyu.wang/pub/web.html

   (b) 重新命名爲 index.html

   (c) 複製 index.html 到網頁伺服器的根目錄

   (d) 不要對 index.html 進行任何的修改

   (e) 防火牆必須開啓

4.9.2 測驗練習二

1. 網頁伺服器 http://kvmX.deyu.wang 可以讓伺服器中的用户，擁有自己的網頁。例如：http://kvmX.deyu.wang/ deyu1，完成以下步驟：

   (a) 以用户 deyu1 的權限登入

   (b) 如果 deyu1 家目錄內沒有 public_html，請自行建立。

   (c) 下載 ftp://deyu.wang/pub/userdir.html

   (d) 重新命名爲 index.html

   (e) 複製 index.html 到 public_html 目錄內

   (f) 不要對 index.html 進行任何的修改

4.9.3 測驗練習三

1. 設計網頁伺服器 http://kvmX.deyu.wang/ 防 DDos 攻擊，完成以下步驟：

   (a) 安裝 httpd-tools 套件，做 ab(ApacheBench) 壓力測試。

   (b) 安裝 mod_evasive 套件，CentOS 7 沒有納入此套件，請直接從 ftp://192.168.1.254/centos7/ 下載，設定以下兩項限制來預防 DDos 攻擊：

      i. DOSPageCount：限制同一 IP 在一個時段內可以存取同一頁面的次數 2 次。

      ii. DOSSiteCount：限制同一 IP 在一個網站內可以佔用請求數 10 個。

   (c) 重新啓動 httpd。

   (d) 從主機 deyu.wang 連線 kvmX.deyu.wang 進行壓力測試，同時 1000 個連線做 20 次，看看測試結果是不是無法完成，這表示網頁伺服器可預防 DDos。

4.9.4 測驗練習四

1. 主機 kvmX.deyu.wang 有另一個 Domain name wwwX.deyu.wang，將網頁伺服器擴展，包含一個虛擬主機 virtual host http://wwwX.deyu.wang/，完成以下步驟：

   (a) 設定 virtual host 的根目錄爲 /var/www/virtual

   (b) 下載 ftp://deyu.wang/pub/virtual.html

   (c) 重新命名 virtual.html 爲 index.html

(d) 將 index.html 放在 virtual host 的根目錄

(e) 不要對 index.html 進行任何的修改

(f) 用户 deyu2 有權在 /var/www/virtual 產生檔案

4.9.5 測驗練習五

1. 在網頁伺服器 http://kvmX.deyu.wang 的根目錄下建立一個名爲 restricted 的新目錄。
2. 下載 ftp://deyu.wang/pub/webca.html 到目錄 restricted，並重新命名爲 index.html。
3. 不要對 index.html 進行任何的修改
4. 目錄 restricted 的內容只允許 kvmX.deyu.wang 連線的任何用户存取，但不允許其他 IP 連線的存取。

Chapter 5

安全 Apache 2.2 網站

5.1 前言

1. 聲明：沒有保證百分之百的安全設定的方法，以下只是提醒管理者該注意的事項，設定時還是要考慮到架設環境及用途做調整。
2. Apache 伺服器本身
   (a) 防火牆 iptables 是否啓動？設定是否恰當？
   (b) SELinux 不要關閉。
   (c) 防止 DOS。
3. 網頁撰寫
   (a) 下載檔案，是否可以直接改網址參數下載到不該下載的檔案。例如：經過程式下載網頁根目錄上層，也就是作業系統的檔案。
   (b) /var/www/html 下目錄及檔案的擁有者及權限設定，不要設定成 777。
   (c) 如果有資料庫，程式是否有考慮到 SQL Injection 問題？
4. 因網頁截圖較不方便且檔案較大，因此本講義製作及說明，網頁存取部分大都使用命令列直接連網，讀者請先稍微瞭解並習慣。

5.2 隱藏敏感訊息

1. 當網頁失敗或使用特定工具查詢時，系統會回傳 apache 版本、作業系統/版本等訊息，甚至安裝的模組等。攻擊者可利用這些訊息，比較快找到攻擊的方式。

```
[root@kvm6 www]# curl -s http://kvm6.deyu.wang/abc | sed -e 's/<[^>]*>//
    g' -e '/^$/d'
```

```
2 301 Moved Permanently
  Moved Permanently
4 The document has moved here.
  Apache/2.2.15 (Red Hat) Server at kvm6.deyu.wang Port 80
```

2. 在 httpd.conf 中設定，ServerTokens 的參數有 Min[imal], OS, Prod[uctOnly], Full 四種，讀者可試著使用這四種參數，看網站回應。ServerSignature off 關閉系統生成的頁面的頁腳訊息。

```
1 [root@kvm6 www]# grep '^Server[TS]' /etc/httpd/conf/httpd.conf
  ServerTokens Prod
3 ServerSignature Off
```

3. 重新載入 httpd.conf 設定

```
1 [root@kvm6 www]# /etc/init.d/httpd reload
  Reloading httpd:
```

4. 再次連上不存在的網頁時，已不出現作業系統及 Apache 版本。

```
  [root@kvm6 www]# curl -s http://kvm6.deyu.wang/abc | sed -e 's/<[^>]*>//
     g' -e '/^$/d'
2 301 Moved Permanently
  Moved Permanently
4 The document has moved here.
```

5.3 網頁存取用户

1. 確定網頁存取用户爲 apache，如果設定成 nobody，若其他服務也以 nobody 執行，則可經由此服務進行攻擊，例如 mail server。

```
  [root@kvm6 ~]# vim /etc/httpd/conf/httpd.conf
2 [root@kvm6 ~]# egrep '^User|^Group' /etc/httpd/conf/httpd.conf
  User apache
4 Group apache
```

5.4 限制網頁根目錄外的存取

1. 網站預設根目錄 /var/www/html，限制這個目錄上層檔案的存取，可以避免攻擊存取系統檔案。直接在網址上以../ 連結上層目錄也無法跳脫這個目錄，但在 httpd.conf 若設定別名就可連上 /var/www/html 根目錄以外的檔案目錄，下例中 /dyw 指向 /mnt/www，也就是連線 http://kvm6.deyu.wang/dyw 時會讀取 /mnt/www 下的資料。

```
[root@kvm6 ~]# grep '^Alias' /etc/httpd/conf/httpd.conf
Alias /dyw /mnt/www
Alias /icons/ "/var/www/icons/"
Alias /error/ "/var/www/error/"
```

2. 此時的最上層目錄 / 設定並沒有限制存取。

```
<Directory />
    Options FollowSymLinks
    AllowOverride None
</Directory>
```

3. 建立測試目錄 /mnt/www，目錄有一網頁 c.html。

```
[root@kvm6 ~]# mkdir /mnt/www
[root@kvm6 ~]# echo 'abc' > /mnt/www/c.html
```

4. 連線 http://kvm6.deyu.wang/dyw/c.html，回應 c.html 內容 abc。

```
[root@kvm6 ~]# /etc/init.d/httpd reload
Reloading httpd:
[root@kvm6 ~]# curl -s http://kvm6.deyu.wang/dyw/c.html
abc
```

5. 修改 httpd.conf 限制網頁根目錄外資料的存取。

```
<Directory />
    Options FollowSymLinks
    AllowOverride None
    Order Deny,Allow
    Deny from all
</Directory>
```

6. 重新載入 httpd.conf 參數。

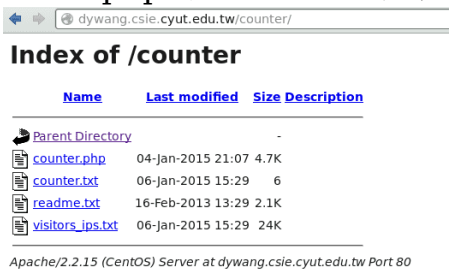
```
[root@kvm6 ~]# /etc/init.d/httpd reload
Reloading httpd:
```

7. 再連線 http://kvm6.deyu.wang/dyw/c.html，回應 403 拒絕存取。

```
[root@kvm6 ~]# curl -s http://kvm6.deyu.wang/dyw/c.html | sed -e 's
    /<[^>]*>//g' -e '/^$/d'
403 Forbidden
Forbidden
You don't have permission to access /dyw/c.html
on this server.
```

5.5 關閉目錄瀏覽

1. httpd 沒限制列出目錄設定時，當連結到該網頁又沒有預設的 index.html 或 index.php 等檔案時，就會列出 http 伺服器目錄下的檔案如下圖。



2. 用户可以看光網站內的所有檔案，對網站安全威脅很大，所以如果不是要架設一個類似 ftp 伺服器，提供一般用户下載檔案用，最好還是在 httpd.conf 指定的網頁目錄加上 Options -Indexes，取消列出目錄檔案。

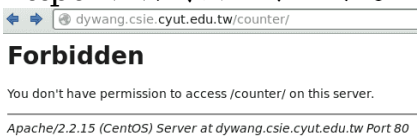
```
[root@kvm8 ~]# vim /etc/httpd/conf/httpd.conf
<Directory "/var/www/html">
    Options -Indexes
    AllowOverride None
    Order allow,deny
    Allow from all
</Directory>
```

3. 設定完必須啓動 httpd 服務或 reload 設定參數。

```
[root@kvm8 ~]# /etc/init.d/httpd restart
```

```
Stopping httpd:                                            [  OK  ]
Starting httpd:                                            [  OK  ]
```

4. httpd 限制列出目錄，再連結網址已無法存取。



5. 如果 /var/www/html 目錄下有些目錄必須開放瀏覽，例如 repo server 的目錄，因此無法以 -Indexes 選項限制整個根目錄不列出目錄，但在 /var/www/html 的某些目錄卻又不希望列出目錄，此狀況可以在該目錄下產生一個空的 index.html，則只要連到該目錄就會以空白頁出現。下面例子是在 abc 目錄下產生空白 index.html，則在使用 Indexes 選項下，連到 http://kvm8.deyu.wang/abc 就會出現空白頁。

```
[root@kvm8 ~]# cd /var/www/html/abc
[root@kvm8 abc]# touch index.html
```

6. 另一種方法還是在 httpd.conf 指定的網頁目錄加上 Options -Indexes，取消列出目錄檔案。在 httpd.conf 中將開放瀏覽的目錄獨立設定 Indexes，則連到 http://kvm8.deyu.wang/abc 時就會到出目錄中的檔案。

```
[root@kvm8 ~]# vim /etc/httpd/conf/httpd.conf
<Directory "/var/www/html/abc">
    Options Indexes
    AllowOverride None
    Order allow,deny
    Allow from all
</Directory>
```

5.6 確認 apache 用户無權限寫入

1. 網站預設根目錄 /var/www/html 的大部分檔案都只提供 apache 用户讀取，所以將檔案擁有者及群組改成 root，並將群組及其他人的寫入權限移除。

```
[root@kvm6 ~]# chown root.root -R /var/www/html/
[root@kvm6 ~]# chmod og-w -R /var/www/html/
```

2. 以上方式雖可保證不是 root 的其他用户，都無法變動網站內的檔案。對於必須寫入資料的網站，設計上就必須特別小心，千萬不能偷懶或不熟悉就將所有檔案及目錄權限改成 777。

5.7 關閉.htaccess 檔案支援

1. .htaccess 可用作對該目錄及其子目錄進行取存控制，而不用修改 httpd.conf 及不用重新啓動伺服器服務。

2. .htaccess 可放在任何一網頁目錄內，當該目錄在 httpd.conf 設定不是 AllowOverride None 便可使用.htaccess 的功能，而設定 AllowOverride All 更可使用.htaccess 的所有功能。

```
[root@kvm8 ~]# vim /etc/httpd/conf/httpd.conf
<Directory "/var/www/html">
    Options -Indexes
    AllowOverride None
    Order allow,deny
    Allow from all
</Directory>
```

5.8 決定是否開啓 FollowSymLinks

1. 在目錄設定選項 FollowSymLinks，可以讓目錄下的連結檔作用。例如：http://dywang.csie.cyut.edu.tw/centos6 是提供 DYW Linux 安裝環境，爲節省檔案存放空間，initrd.img 使用連結檔。

```
[root@dywang html]# ll centos6/images/pxeboot/
total 3712
lrwxrwxrwx. 1 root root      25 Aug 28  2012 initrd.img -> ../../
    isolinux/initrd.img
-rw-r--r--. 1 root root     265 May 13  2010 README
-r--r--r--. 1 root root     441 Aug 18  2012 TRANS.TBL
-rwxr-xr-x. 1 root root 3791040 Nov 22  2011 vmlinuz
```

2. httpd.conf 沒有將 centos6 目錄加上 FollowSymLinks 選項。

```
[root@dywang html]# grep -A4 /var/www/html/centos6 /etc/httpd/conf/httpd
    .conf
<Directory "/var/www/html/centos6">
```

```
    Options Indexes
    Order allow,deny
    Allow from all
</Directory>
```

3. 使用 http://dywang.csie.cyut.edu.tw/centos6 進行網路安裝時，出現以下錯誤訊息，原因爲 initrd.img 無法讀取。

```
Starting install...
Retrieving file .treeinfo...                          |  728 B
    00:00 ...
Retrieving file vmlinuz...                            | 7.2 MB
    00:05 ...
ERROR    'NoneType' object is not iterable
Domain installation does not appear to have been
 successful.  If it was, you can restart your domain
 by running 'virsh start kvmusb'; otherwise, please
 restart your installation.
```

4. httpd.conf 將 centos6 目錄加上 FollowSymLinks 選項

```
[root@dywang html]# grep -A4 /var/www/html/centos6 /etc/httpd/conf/httpd
    .conf
<Directory "/var/www/html/centos6">
    Options Indexes FollowSymLinks
    Order allow,deny
    Allow from all
</Directory>
```

5. 重新載入 httpd.conf 設定後，網路安裝就正常了。

```
[root@dywang html]# /etc/init.d/httpd reload
Reloading httpd:
```

5.9 實機操作測驗練習題

5.9.1 測驗練習一

1. 在主機 kvmX.deyu.wang 架設網頁伺服器，其中 X 爲您虛擬機的編號，完成以下步驟：

(a) 隱藏敏感訊息 ServerTokens 設定爲 Prod

(b) 網頁存取用户及群組 apache

(c) 限制網頁根目錄外的所有存取

(d) 在網頁根目錄下建立次目錄 abc，並在 abc 目錄內產生一個空檔案 aaa.html。

(e) 關閉根目錄瀏覽功能

(f) 確認 apache 用户無權限寫入根目錄，也就是網頁伺服器根目錄內的檔案擁有者及群組皆爲 root，且目錄內的檔案及次目錄權限不可設爲 777，用户 apache 只能讀取不能寫入。

Chapter 6

Network File System, NFS

6.1 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户的家目錄，則用户的資料將無法同步。此時使用 NFS 就可提拱家目錄的整合。
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。

6.2 NFS 架設

1. 安裝 nfs-utils 套件

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

2. 編輯設定檔

```
[root@dyH ~]# cat /etc/exports
#分享的目錄 可存取的網段(分享參數)
/home/guests    192.168.122.0/255.255.255.0(rw,sync)

# 參數
    * rw：read-write，可讀寫的權限；
    * ro：read-only，唯讀的權限；
    * sync：資料同步寫入到記憶體與硬碟當中；
    * async：資料會先暫存於記憶體當中，而非直接寫入硬碟。
    * no_root_squash：
```

```
11        登入 NFS 主機使用分享目錄的使用者如果是 root，對於分享的目錄具有
              root 的權限。
          極不安全，不建議使用。
13      * root_squash：
          登入 NFS 主機使用分享目錄的使用者如果是 root，權限將被壓縮成匿名使
              用者，
15        通常他的 UID 與 GID 都會變成 nobody(nfsnobody) 那個系統帳號的身
              份；
        * all_squash：
17        不論登入 NFS 的使用者身份爲何，都會被壓縮成爲匿名使用者，通常是
              nobody(nfsnobody) 。
        * anonuid：
19        anon 意指 anonymous (匿名者)，自訂匿名使用者的 UID。
        * anongid：自訂匿名使用者的是變成 GID。
```

3. 限制只能使用版本 3 掛載

```
[root@deyu ~]# grep RPCNFSDARGS -B1 /etc/sysconfig/nfs
2 # Turn off v2 and v4 protocol support
RPCNFSDARGS="-N 2 -N 4"
```

4. 啓動 nfs 服務

```
1 [root@dyH ~]# /etc/init.d/nfs restart
                                                          [FAILED]
3 Shutting down NFS mountd:                               [FAILED]
  Starting NFS services:                                  [  OK  ]
5 Starting NFS daemon:                                    [  OK  ]
  Starting NFS mountd:                                    [  OK  ]
```

5. 設定開機啓動 nfs 服務

```
[root@dyH ~]# chkconfig nfs on
```

6.3 查詢與變更

1. 從 deyu.wang 查詢 kvm8.deyu.wang nfs server

```
1 [root@deyu ~]# showmount [-ae] [hostname|IP]
  參數：
3 -a ：顯示目前主機與用户端的 NFS 連線分享的狀態；
```

```
-e ：顯示某部主機的 /etc/exports 所分享的目錄資料。

## 兩種狀況皆爲防火牆阻擋
[root@dyH ~]# showmount -e kvm8.deyu.wang
rpc mount export: RPC: Unable to receive; errno = No route to host
.....
[root@dyH ~]# showmount -e kvm8.deyu.wang
clnt_create: RPC: Port mapper failure - Unable to receive: errno 113 (No
    route to host)
```

2. 重新設定 /etc/exports 後。

```
[root@deyu ~]# exportfs [-aruv]
參數：
-a ：全部掛載(或卸載) /etc/exports 檔案內的設定
-r ：重新掛載 /etc/exports 的設定，亦同步更新 /etc/exports
     及 /var/lib/nfs/xtab 的內容。
-u ：卸載某一目錄
-v ：在 export 時將分享的目錄顯示到螢幕上。

[root@deyu ~]# vim /etc/exports
/home/guests    192.168.122.0/255.255.255.0(rw,sync)
```

3. 利用 exportfs 處理 nfs 的掛載，可不需重新啓動 nfs。

```
[root@deyu ~]# exportfs -arv
exporting 192.168.122.0/255.255.255.0:/home/guests
```

6.4 安全機制

1. 查詢 nfs ports

```
[root@kvm8 ~]# rpcinfo -p 192.168.122.8
   program vers proto   port  service
    100000    4   tcp    111  portmapper
    100000    3   tcp    111  portmapper
    100000    2   tcp    111  portmapper
    100000    4   udp    111  portmapper
    100000    3   udp    111  portmapper
    100000    2   udp    111  portmapper
    100024    1   udp  55661  status
```

```
    100024    1   tcp  46633  status
    100003    2   tcp   2049  nfs
    100003    3   tcp   2049  nfs
    100003    4   tcp   2049  nfs
    100227    2   tcp   2049  nfs_acl
    100227    3   tcp   2049  nfs_acl
    100003    2   udp   2049  nfs
    100003    3   udp   2049  nfs
    100003    4   udp   2049  nfs
    100227    2   udp   2049  nfs_acl
    100227    3   udp   2049  nfs_acl
    100021    1   udp  37591  nlockmgr
    100021    3   udp  37591  nlockmgr
    100021    4   udp  37591  nlockmgr
    100021    1   tcp  50290  nlockmgr
    100021    3   tcp  50290  nlockmgr
    100021    4   tcp  50290  nlockmgr
    100005    1   udp    892  mountd
    100005    1   tcp    892  mountd
    100005    2   udp    892  mountd
    100005    2   tcp    892  mountd
    100005    3   udp    892  mountd
    100005    3   tcp    892  mountd
```

2. 查詢 nfs tcp ports

```
[root@kvm8 ~]# rpcinfo -p 192.168.122.8 | grep tcp |awk '{print $4}' |
    sort -u
111
2049
42586
46633
46697
46790
49698
```

3. 查詢 nfs udp ports

```
[root@kvm8 ~]# rpcinfo -p 192.168.122.8 | grep udp |awk '{print $4}' |
    sort -u
111
2049
37474
43938
49830
55661
57818
```

4. 指定 rpc mount port

```
[root@kvm8 ~]# vim /etc/sysconfig/nfs
# Port rpc.mountd should listen on.
MOUNTD_PORT=892
```

5. 防火牆設定

```
[root@kvm8 ~]# vim /etc/sysconfig/iptables
-A INPUT -i lo -j ACCEPT
#######################################################
-A INPUT -m state --state NEW -m tcp -p tcp --dport 892 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 111 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 2049 -j ACCEPT

-A INPUT -m state --state NEW -m udp -p udp --dport 111 -j ACCEPT
-A INPUT -m state --state NEW -m udp -p udp --dport 2049 -j ACCEPT
#######################################################
-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
```

6. 防火牆重新啓動

```
[root@kvm8 ~]# /etc/init.d/iptables restart
```

7. 開機啓動防火牆

```
[root@kvm8 ~]# chkconfig iptables on
```

8. 測試 nfs 掛載

```
[root@dyH ~]# showmount -e kvm8.deyu.wang
Export list for kvm8.deyu.wang:
/home 192.168.122.0/24

[root@dyH ~]# mount -t nfs -o nfsvers=4 kvm8.deyu.wang:/home /mnt/home
[root@dyH ~]# ll /mnt/home/
total 19
drwxr-xr-x. 5 nobody nobody  1024 Aug  1 19:49 deyu1
drwx------. 4 nobody nobody  1024 Aug  1 14:56 deyu2
drwx------. 4 nobody nobody  1024 Aug  1 14:56 deyu3
drwx------. 2 root   root   12288 Aug  1 11:40 lost+found
```

6.5 NFS Client 端設定

1. 安裝套件 nfs-utils

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

2. 掃瞄 NFS 伺服器分享的目錄，並瞭解是否可以使用 (showmount)；

```
[root@kvm8 ~]# showmount -e deyu.wang
Export list for deyu.wang:
/home/guests 192.168.122.0/255.255.255.0
```

3. 建立掛載目錄

```
[root@kvm8 ~]# mkdir /home/guests
[root@kvm8 ~]# ll /home/guests/
total 0
```

4. 利用 mount 將遠端主機直接掛載到相關目錄。

```
[root@kvm8 ~]# mount deyu.wang:/home/guests /home/guests
[root@kvm8 ~]# ls /home/guests/
ldapuser1  ldapuser2
```

5. 查看掛載情形；

```
[root@kvm8 ~]# df -h
Filesystem            Size  Used Avail Use% Mounted on
/dev/mapper/vg_kvmusb-root
                      945M  629M  269M  71% /
tmpfs                 499M     0  499M   0% /dev/shm
/dev/vda1              93M   31M   59M  35% /boot
/dev/mapper/vg_kvmusb-home
                       93M  5.6M   83M   7% /home
deyu.wang:/home/guests
```

```
                    1.9G  277M  1.6G  16% /home/guests
```

6. 將掛載的 NFS 目錄卸載

```
[root@kvm8 ~]# umount /home/guests/
[root@kvm8 ~]# ls /home/g*
```

7. NFS 特殊的掛載參數

參數	預設	內容意義
fg/bg	fg	當執行掛載時，該掛載的行爲會在前景 (fg) 還是在背景 (bg) 執行。
soft/ hard	hard	當兩者之間有任何一部主機離線，hard RPC 會持續的呼叫，直到對方恢復連線爲止；soft RPC 會在 time out 後『重複』呼叫，而非『持續』呼叫。
intr	沒中斷	使用 hard 方式掛載若加上 intr，則當 RPC 持續呼叫中，該次呼叫可以被中斷。
rsize/ wrize	1024	讀出 (rsize) 與寫入 (wsize) 的區塊大小 (block size)。

8. 開機即掛載 NFS

```
[root@kvm8 ~]# vim /etc/fstab
deyu.wang:/home/guests /home/guests nfs nosuid,noexec,nodev,rw,bg,soft
      0   0
```

6.6 自動掛載 autofs 的使用

1. 爲何需要自動掛載 autofs？

   (a) 讓用户端在有使用到 NFS 檔案系統時才掛載；

   (b) 不需要事先建立掛載點；

   (c) 當 NFS 檔案系統使用完畢後，讓 NFS 自動卸載，以避免可能的 RPC 錯誤。

2. 安裝套件，系統應該已經安裝了。

```
[root@kvm8 ~]# rpm -qa | grep autofs
autofs-5.0.5-23.el6.x86_64
```

3. 建立主要設定檔 /etc/auto.master

```
[root@kvm8 ~]# vim /etc/auto.master
/home/guests    /etc/auto.nfs

# <預設目錄> <資料對應檔>。
# 預設目錄：用户端要使用 /home/guests/ldapuser1，會到資料對應檔中找次目錄 ldapuser1 的對應。
# 資料對應檔的檔名是可以自行設定的，此例中使用 /etc/auto.guests。
```

4. 建立資料對應檔內的掛載資訊，若 NFS server 有限制版本爲 v3，則必須加入參數 -vers=3。但 -fstype=nfs,-vers=3 無效，-fstype=nfs 參數必須刪除或放 -vers=3 之後，如 -vers=3,-fstype=nfs。因實際掛載，系統可自動判讀其爲 NFS 檔案格式，故建議刪除 -fstype=nfs 參數。

```
資料對應檔格式：
[本地端目錄]  [-掛載參數]  [伺服器所提供的目錄]
參數：
[本地端目錄]  ：指的是在 /etc/auto.master 內指定的目錄之次目錄
[-掛載參數]   ：就是 rw,bg,soft 等參數，可有可無；
[伺服器所提供的目錄]  ：例如 163.17.27.219:/home 等

[root@kvm8 ~]# vim auto.nfs
#*   -fstype=nfs,-vers=3 deyu.wang:/home/guests/&
#*   -vers=3,-fstype=nfs deyu.wang:/home/guests/&
*    -vers=3 deyu.wang:/home/guests/&
## 本地端目錄 "*" 表示 /home/guests 下的任何次目錄
## 伺服器提供的目錄 deyu.wang:/home/guests/& 中 "&" 表示對應到 "*"
## 當使用到目錄 /home/guests/ldapuser1，則 "*" 及 "&" 即爲 ldapuser1
```

5. 啓動 autofs

```
[root@kvm8 etc]# /etc/init.d/autofs start
```

```
Starting automount:                                        [  OK  ]
```

6. 設定開機即啓動 autofs

```
[root@kvm8 ~]# chkconfig --level 345 autofs on
Starting autofs:                                           [  OK  ]
```

7. 檢查開機是否啓動 autofs

```
[root@kvm8 ~]# chkconfig --list autofs
autofs          0:off   1:off   2:off   3:on    4:on    5:on    6:off
```

8. 確認目前並沒有掛載任何來自 deyu.wang NFS 伺服器的目錄

```
[root@kvm8 etc]# df -h
Filesystem            Size  Used Avail Use% Mounted on
/dev/mapper/GLSguest-lv_root
                      5.3G  2.2G  2.9G  43% /
tmpfs                 246M  260K  246M   1% /dev/shm
/dev/vda1              97M   26M   67M  28% /boot
```

9. 進入 /home/guests/ldapuser1，檔案系統自動掛載。

```
[root@kvm8 etc]# su - ldapuser1
[ldapuser1@kvm8 ~]$ pwd
/home/guests/ldapuser1
[ldapuser1@kvm8 ~]$ df -h
Filesystem            Size  Used Avail Use% Mounted on
/dev/mapper/GLSguest-lv_root
                      5.3G  2.2G  2.9G  43% /
tmpfs                 246M  260K  246M   1% /dev/shm
/dev/vda1              97M   26M   67M  28% /boot
df: `/root/.gvfs': Permission denied
deyu.wang:/home/guests/ldapuser1
                       26G   36M   25G   1% /home/guests/ldapuser1
# 已掛載，目錄 /home/guests/ldapuser1 會自動產生。
```

10. 從遠端以帳號 ldapuser1 登入 kvm8.deyu.wang，看是否可以自動掛載其家目錄。

```
[test from host deyu.wang]
[root@deyu ~]# ssh ldapuser1@kvm8.deyu.wang
ldapuser1@kvm8.deyu.wang's password:
[ldapuser1@kvm8 ~]$ pwd
/home/guests/ldapuser1
```

6.7 NFS 掛載非常慢

1. 掛載很慢，但最後是掛載成功，往往是 NFS server 限制掛載版本，而 client 預設掛載版本掛載版本不成功，進而再嘗試其他版本的掛載。

2. 解決方式：先查 server 端的的設定，以下例子是限制不能使用 v2 及 v4。

```
[root@deyu ~]# grep RPCNFS /etc/sysconfig/nfs
RPCNFSDARGS="-N 2 -N 4"
```

3. Client 端查詢掛載的版本，確實爲 v3。

```
[root@kvm7 ~]# nfsstat -m
/home/guests/ldapuser1 from deyu.wang:/home/guests/ldapuser1
 Flags: rw,relatime,vers=3,rsize=1048576,wsize=1048576,\
namlen=255,hard,proto=tcp,timeo=600,retrans=2,sec=sys,\
mountaddr=192.168.122.1,mountvers=3,mountport=44465,\
mountproto=udp,local_lock=none,addr=192.168.122.1
```

4. Client 預設掛載版本爲 v4，如果 server 端不能更動，client 端自動掛載就必須指定掛載版本 -vers=3，這樣掛載就會快速。

5. 由於 NFS v4 已不使用 rpcbind 服務，所以若以 v4 版本掛載，就可以不管 rpcbind 服務是否啓動；反之，若不是以 v4 版本掛載，則要確定 client 端 rpcbind 服務是否啓動，否則會掛載不起來。

Chapter 7

DHCP

7.1 DHCP 簡介

1. DHCP (Dynamic Host Configuration Protocol)
2. 自動指定 TCP/IP 資訊給 client。
3. Client 連上 DHCP Server 後，server 會提供 ip, netmask, gateway, DNS server 給 client。

7.2 DHCP 架設設定 - c6

1. 安裝 dhcp 套件

```
[root@kvm8 ~]# yum install dhcp
```

2. 設定檔 /etc/dhcp/dhcpd.conf 是空的，依說明參考範例檔。

```
[root@kvm8 ~]# cat /etc/dhcp/dhcpd.conf
#
# DHCP Server Configuration file.
#   see /usr/share/doc/dhcp*/dhcpd.conf.sample
```

3. 設定檔格式
   (a) 包含參數及宣告
   (b) 大括號 {} 外的參數爲全體設定

(c) 至少必須有一個 subnet 宣告

(d) 符號 # 後的文字爲註解

4. Global 參數

```
ddns-update-style none;    # 支援 ddns (Dynamic DNS) 更新 IP，
                           # 這個選項一定要存在才不會有錯誤。
option space PXE;          # 定義選項空間給 PXE
```

5. 產生 Class PXE 提供 pxe client 適當的訊息

```
class "PXE" {
    # 如果 dhcp client 的 vendor-class-identifier 爲 PXEclient
    match if substring(option vendor-class-identifier, 0, 9) = "
        PXEClient";
    # vendor-encapsulated-options (廠商封裝選項) 允許 vendors 定義自己的
        選項
    option vendor-encapsulated-options 01:04:00:00:00:00:ff;
    option boot-size 0x1;
    # PXEclient 讀取的檔案, tftp 已經 chroot
    filename "pxelinux.0";
    # 指定 tftp server
    option tftp-server-name "deyu.wang";
    # pxe client 回應 dhcp server vendor-class-identifier 爲 "PXEClient"
    # 若此選項不設定 pxe client 不回應 dhcp server vendor-class-
        identifier
    option vendor-class-identifier "PXEClient";
    # vendor-option-space 宣告，告訴 DHCP server 使用 PXE option space
    # 去建構 vendor-encapsulated-options 選項
    vendor-option-space PXE;
}
```

6. Subnet 宣告

```
subnet 192.168.1.0 netmask 255.255.255.0 {
#       The following lines are standard all of the time.
        option routers 192.168.1.254;
        option subnet-mask 255.255.255.0;
        option domain-name "deyu.wang";
        option domain-name-servers 168.95.1.1,139.175.10.20;
        default-lease-time 21600; # 預設租期時間長度(秒)
        max-lease-time 43200;     # 租期到可續租，但最大租期長度(秒)
}
```

7. Subnet 宣告中指定主機名爲 dywdh1 的電腦，使用固定 IP。

```
[root@e517nat ~]# grep dyw /etc/dhcp/dhcpd.conf -A4
    host dywhd1 {
        hardware ethernet   00:E0:4C:4E:7A:F5;
        fixed-address       192.168.1.140;
    }
```

8. Address Pools: 指定不同的 client，使用不同的 ip 範圍及不同的設定。如果 192.168.1.140 要固定指定給某一網卡，則 range 必須將其跳開，否則這網域可能有兩台電腦 IP 都同爲 192.168.1.140，此時網路會時好時壞。

```
        # Assign IPs 10-99 to PXE clients
        pool {
            allow members of "PXE";
            default-lease-time 120;
            max-lease-time 180;
            range 192.168.1.10 192.168.1.99;
        }
        pool {
            deny members of "PXE";
            range 192.168.1.100 192.168.1.139;
            range 192.168.1.141 192.168.1.199;
        }
```

9. 固定某台機器的 ip

```
host teacher {
    option host-name "teacher.deyu.wang";
    hardware ethernet 3C:D9:2B:5E:8C:62;
    fixed-address 192.168.1.14;
}
```

10. 設定 dhcpd 網卡

```
[root@kvm8 ~]# cat /etc/sysconfig/dhcpd
# Command line options here
DHCPDARGS="eth1"
```

11. 與 kickstart 有關的設定

```
#   The following lines are examples of kickstart directives.
    next-server 192.168.1.254;
    filename "ftp://192.168.1.254/pub/centos6/add/crt-ks.cfg";
```

12. 設定 dhcpd 服務使用的網卡

```
[root@kvm8 ~]# vim /etc/sysconfig/dhcpd
[root@kvm8 ~]# cat /etc/sysconfig/dhcpd
# Command line options here
DHCPDARGS="eth0"
```

13. 啓動 dhcpd 服務

```
[root@kvm8 ~]# /etc/init.d/dhcpd restart
```

14. 設定開機啓動 dhcpd 服務

```
[root@kvm8 ~]# chkconfig dhcpd on
```

7.3 DHCP 架設設定 - c8

1. 安裝 dhcp 套件

```
[root@msi ~]# dnf install dhcp-server
```

2. /etc/dhcp/dhcpd.conf 設定如下：。

```
[root@msi ~]# vim /etc/dhcp/dhcpd.conf
[root@msi ~]# cat /etc/dhcp/dhcpd.conf
#
# DHCP Server Configuration file.
#   see /usr/share/doc/dhcp-server/dhcpd.conf.example
#   see dhcpd.conf(5) man page
#
ddns-update-style none;
option space PXE;

subnet 192.168.1.0 netmask 255.255.255.0 {

class "PXE" {
```

```
    match if substring(option vendor-class-identifier, 0, 9) = "
        PXEClient";
        option vendor-encapsulated-options 01:04:00:00:00:00:ff;
        option boot-size 0x11;
        filename "pxelinux.0";
#       option tftp-server-name "deyu.wang";
        option vendor-class-identifier "PXEClient";
        vendor-option-space PXE;
    }


#      The following lines are standard all of the time.
        option routers 192.168.1.254;
        option subnet-mask 255.255.255.0;
        option domain-name "deyu.wang";
        option domain-name-servers
            192.168.1.254,8.8.8.8,168.95.1.1,139.175.10.20;
        default-lease-time 21600;
        max-lease-time 43200;

        # Assign IPs 101-100 to PXE clients
        pool {
            allow members of "PXE";
            default-lease-time 12;
            max-lease-time 18;
            range 192.168.1.250 192.168.1.253;
        }
        pool {
            deny members of "PXE";
            range 192.168.1.100 192.168.1.199;
        }
#   The following lines are examples of kickstart directives.
    next-server 192.168.1.254;
}
```

3. dhcp 的網卡，依照 /etc/sysconfig/dhcpd 有服務啓動的範例設定。

```
[root@msi ~]# grep example -A5 /etc/sysconfig/dhcpd
# example:
# $ cp /usr/lib/systemd/system/dhcpd.service /etc/systemd/system/
# $ vi /etc/systemd/system/dhcpd.service
# $ ExecStart=/usr/sbin/dhcpd -f -cf /etc/dhcp/dhcpd.conf -user dhcpd -
    group dhcpd --no-pid <your_interface_name(s)>
# $ systemctl --system daemon-reload
# $ systemctl restart dhcpd.service
```

4. 依範例實作，dhcp.service 中的網卡還是用變數 DHCPDARGS，並在 /etc/sysconfig/dhcpd 中設定此變數。

```
[root@msi ~]# cp /usr/lib/systemd/system/dhcpd.service /etc/systemd/
    system/
[root@msi ~]# grep Exec /etc/systemd/system/dhcpd.service
ExecStart=/usr/sbin/dhcpd -f -cf /etc/dhcp/dhcpd.conf -user dhcpd -group
     dhcpd --no-pid $DHCPDARGS
[root@msi ~]# tail -1 /etc/sysconfig/dhcpd
DHCPDARGS=wlo1
```

5. 啓動服務

```
[root@msi ~]# systemctl --system daemon-reload
[root@msi ~]# systemctl restart dhcpd.service
```

6. 查看服務狀態 active

```
[root@msi ~]# systemctl status dhcpd.service
  dhcpd.service - DHCPv4 Server Daemon
    Loaded: loaded (/etc/systemd/system/dhcpd.service; disabled; vendor
        preset: disabled)
    Active: active (running) since Thu 2021-07-15 07:11:44 CST; 1min 1s
        ago
      Docs: man:dhcpd(8)
            man:dhcpd.conf(5)
 Main PID: 4587 (dhcpd)
    Status: "Dispatching packets..."
     Tasks: 1 (limit: 48313)
    Memory: 4.9M
    CGroup: /system.slice/dhcpd.service
              4587 /usr/sbin/dhcpd -f -cf /etc/dhcp/dhcpd.conf -user
                dhcpd -group dhcpd --no-pid wlo1
```

7.4 DHCP Client

1. dhclient 命令用於從 DHCP 服務器取得、更新和釋放客户端 IP 地址、子網遮罩 (subnet mask) 、預設閘道 (gateway) 和 DNS 服務器。

2. 安裝 dhcp-client 套件

```
[root@msi ~]# dnf install dhcp-client
```

3. 查看網卡。

```
[root@999999 ~]# nmcli device
DEVICE  TYPE      STATE      CONNECTION
ens3    ethernet  connected  ens3
lo      loopback  unmanaged  --
```

4. 網卡 ens3 從 dhcp 伺服器取得 ip。

```
[root@999999 ~]# dhclient ens3
```

5. 查看網卡 ens3 從 dhcp 伺服器取得 ip 爲 192.168.122.153/24。

```
[root@999999 ~]# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
    group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state
     UP group default qlen 1000
    link/ether 52:54:00:bd:81:12 brd ff:ff:ff:ff:ff:ff
    altname enp0s3
    inet 192.168.122.153/24 brd 192.168.122.255 scope global dynamic
        noprefixroute ens3
       valid_lft 3651sec preferred_lft 3651sec
    inet6 2001:ac18::5054:ff:febd:8112/64 scope global dynamic
        noprefixroute
       valid_lft 3346sec preferred_lft 3346sec
    inet6 fe80::5054:ff:febd:8112/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

6. 網卡 ens3 從 dhcp 伺服器取得 ip 的訊息寫在 dhclient.leases。

```
[root@999999 ~]# cat /var/lib/dhclient/dhclient.leases
lease {
  interface "ens3";
  fixed-address 192.168.122.153;
  option subnet-mask 255.255.255.0;
  option routers 192.168.122.1;
  option dhcp-lease-time 3600;
  option dhcp-message-type 5;
  option domain-name-servers 192.168.122.1;
  option dhcp-server-identifier 192.168.122.1;
  option dhcp-renewal-time 1800;
  option broadcast-address 192.168.122.255;
```

```
  option dhcp-rebinding-time 3150;
  option domain-name "deyu.wang";
  renew 1 2023/09/04 08:20:17;
  rebind 1 2023/09/04 08:47:43;
  expire 1 2023/09/04 08:55:13;
}
```

7. 釋放網卡 ens3 取得的 ip。

```
[root@999999 ~]# dhclient -r ens3
Killed old client process
```

8. 查看網卡 ens3，已無 ip。

```
[root@999999 ~]# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
    group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state
     UP group default qlen 1000
    link/ether 52:54:00:bd:81:12 brd ff:ff:ff:ff:ff:ff
    altname enp0s3
    inet6 2001:ac18::5054:ff:febd:8112/64 scope global dynamic
        noprefixroute
       valid_lft 3191sec preferred_lft 3191sec
    inet6 fe80::5054:ff:febd:8112/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

7.5 安全機制

1. DHCP Ports
   (a) Clients 要求使用 UDP port 68
   (b) Server 回應使用 UDP port 67
2. 防火牆設定

```
[root@kvm8 ~]# vim /etc/sysconfig/iptables
#########################################################
```

```
-A OUTPUT -p udp --dport 68 -j ACCEPT
-A INPUT -p udp --dport 67 -j ACCEPT
#########################################################
```

3. 防火牆重新啓動

```
[root@kvm8 ~]# /etc/init.d/iptables restart
```

4. 開機啓動防火牆

```
[root@kvm8 ~]# chkconfig iptables on
```

7.6 NAT 配置

1. DHCP 主機上配置雙網卡，假設：
   (a) eth0=192.168.1.254 連接內網。
   (b) eth1=163.17.10.xx 連上 internet。
2. iptables 設定

```
[root@kvm8 ~]# vim /etc/sysconfig/iptables
#########################################################
## 經由 eth1 連上 internet 做 ip 僞裝
-A POSTROUTING -o eth1 -j MASQUERADE
#-A POSTROUTING -s 192.168.1.0/24 -o eth1 -j SNAT --to 163.17.10.xx

## 由 eth0 傳來，要到 163.17.0.0/16 的封包都接受轉向
-A FORWARD -i eth0 -d 163.17.0.0/16 -j ACCEPT
## 從 internet 輸出到 eth0，要到 192.168.1.0/24 的封包都接受轉向
-A FORWARD -o eth0 -d 192.168.1.0/24 -j ACCEPT
## 其他輸出到 eth0 的封包都丟棄
-A FORWARD -o eth0 -j DROP
#########################################################
```

3. 防火牆重新啓動

```
[root@kvm8 ~]# /etc/init.d/iptables restart
```

4. 設定 IP forwarding

```
[root@kvm8 ~]# vim /etc/sysctl.conf
net.ipv4.ip_forward = 1
[root@kvm8 ~]# sysctl -p
```

7.7 其他問題

1. IP 重複，在 DHCP server 刪除重複的 IP：

```
[root@e517nat ~]# vim /var/lib/dhcpd/dhcpd.leases
[root@e517nat ~]# grep 192.168.1.154 -A5 /var/lib/dhcpd/dhcpd.leases
lease 192.168.1.154 {
  starts 5 2015/10/30 13:14:02;
  ends 5 2015/10/30 13:24:02;
  tstp 5 2015/10/30 13:24:02;
  cltt 5 2015/10/30 13:14:02;
  binding state active;
--
lease 192.168.1.154 {
  starts 5 2015/10/30 13:18:53;
  ends 5 2015/10/30 13:28:53;
  cltt 5 2015/10/30 13:18:53;
  binding state active;
  next binding state free;
--
lease 192.168.1.154 {
  starts 5 2015/10/30 13:23:23;
  ends 5 2015/10/30 13:33:23;
  cltt 5 2015/10/30 13:23:23;
  binding state active;
  next binding state free;
--
lease 192.168.1.154 {
  starts 5 2015/10/30 13:27:19;
  ends 5 2015/10/30 13:37:19;
  cltt 5 2015/10/30 13:27:19;
  binding state active;
  next binding state free;
--
lease 192.168.1.154 {
  starts 5 2015/10/30 13:31:07;
  ends 5 2015/10/30 13:41:07;
  cltt 5 2015/10/30 13:31:07;
  binding state active;
  next binding state free;
--
lease 192.168.1.154 {
  starts 5 2015/10/30 13:36:04;
```

```
    ends 5 2015/10/30 13:46:04;
41  cltt 5 2015/10/30 13:36:04;
    binding state active;
43  next binding state free;
```

Chapter 8

Mail Server

8.1 Mail Server 簡介

1. Email 開始於 1960 年代，但只能在同一系統中發送郵件。
2. 第一封在網路間傳送的電子郵件發生在 1971 年。
3. 現在電子郵件已是標準網路協定。

8.2 Email 協定

8.2.1 Mail Transport Protocols

1. Simple Mail Transport Protocols (SMPT)：負責將郵件從 client 的應用程式，送到開始的 server，再送到目的 server 的協定。
2. SMPT 允許使用者不需要身份認證下，在網路間傳送郵件給任何人或一群人。這造成大量垃圾郵件發生的可能性。
3. 必須限制用户從您的 SMPT 服務器傳送電子郵件。

8.2.2 Mail Access Protocols

1. 有兩種主要的協定：Post Office Protocol (POP) 與 Internet Message Access Protocol (IMAP)。
2. 目前的 POP 版本是 POP3。
3. CentOS 預設的 POP 及 IMAP 套件是 dovecot。

4. POP email client 預設從 mail server 下載郵件後，會刪除 mail server 上的郵件。IMAP 則會保留 mail server 上的郵件。

5. IMAP 較適合多電腦共同存取郵件。

8.2.3 Mail Agents

1. 一般用户使用郵件，都只寄信與收信。但從寄信到收信，往往要經過多台郵件代理服務器才能完成。

2. Mail Transport Agent (MTA)，郵件傳送代理人：當郵件在主機中傳送時，郵件代理人決定是否接受郵件或轉傳。

3. Mail Delivery Agent (MDA)，郵件投遞代理人：將郵件送到用户，MDA 包含於 MTA。

4. Mail User Agent (MUA)，郵件使用者代理人：是 eamil client 應用程式的代名詞，也就是提供使用者編寫和閱讀電子郵件的程式。例如：Evolution。

5. 常見的 MTAs (MDAs) 套件有 postfix，sendmail，CentOS 預設是 postfix。

8.3 Dovecot 架設

1. 安裝 dovecot 套件

```
[root@mail1 ~]# yum install dovecot
```

2. 編輯設定檔：選擇使用的協定

```
[root@mail1 ~]# vim /etc/dovecot/dovecot.conf
# Protocols we want to be serving.
protocols = imap pop3 lmtp
```

3. 編輯郵件設定檔：設定郵件位置

```
[root@mail1 ~]# vim /etc/dovecot/conf.d/10-mail.conf

## 設定收信位置，若沒設定或設定錯誤，系統記錄檔會出現錯誤訊息
## Initialization failed: mail_location not set and autodetection failed
    :
## Mail storage autodetection failed with home=/home/....
```

```
mail_location = mbox:~/Mail:INBOX=/var/spool/mail/%u
```

4. 編輯郵件設定檔：設定郵件位置寫入權限

```
[root@mail1 ~]# vim /etc/dovecot/conf.d/10-mail.conf

## 當用户第一次使用，dovecot 會在 INBOX 位置產生一個用户郵件檔
## 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
## 表示該用户沒有權限寫入 INBOX:/var/spool/mail
## 查看目錄 /var/spool/mail 其他人並沒有寫入的權限，
## 有人會直接把該目錄權限改成 777，這不是解決問題的方法
[root@mail1 ~]# ll -d /var/spool/mail
drwxrwsr-x. 5 root mail 32768 Aug  7 10:03 /var/spool/mail

## 正確解法
# Group to enable temporarily for privileged operations. Currently this
    is
# used only with INBOX when either its initial creation or dotlocking
    fails.
# Typically this is set to "mail" to give access to /var/spool/mail.
mail_privileged_group = mail
```

5. 啓動 dovecot 服務

```
[root@kvm8 ~]# /etc/init.d/dovecot restart
```

6. 設定開機啓動 dovecot 服務

```
[root@kvm8 ~]# chkconfig dovecot on
```

8.4 Postfix 架設

1. 安裝 postfix 套件

```
[root@kvm8 ~]# yum install postfix ## 預設應已安裝
```

2. postfix 主要設定檔在 /etc/postfix 目錄下

(a) access：存取控制，可以指定那些主機可以使用 Postfix。

(b) main.cf：Postfix 主要設定檔。

(c) master.cf：指定 Postfix 每個程序如何完成郵件傳遞。

(d) transport：對應 email addresses 到轉傳的主機。

(e) header_checks：過濾郵件標題，例如寄信者。

(f) body_checks：過濾郵件內容。

(g) /etc/aliases：設定用户別名。

3. 編輯設定檔 /etc/postfix/main.cf

```
[root@mail1 ~]# vim /etc/postfix/main.cf
# 設定郵件伺服器主機名稱
myhostname = mail.deyu.wang
# 設定網域
mydomain = deyu.wang
# 指定郵件顯示網域
myorigin = $mydomain
# 設定可以連接郵件伺服器的網路或主機
mynetworks = 192.168.122.0/24
# 設定接受郵件的來源爲所有
inet_interfaces = all
# 設定轉傳的郵件伺服器，若不設定郵件直接傳送至目的主機，可能無法送達。
relayhost = 192.168.122.1
# 設定別名對應檔及資料庫
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
# 設定郵件標頭及內容過濾規則
header_checks = regexp:/etc/postfix/header_checks
body_checks = regexp:/etc/postfix/body_checks
```

4. 編輯郵件別名設定檔

```
[root@mail1 ~]# vim /etc/aliases

root: deyu1,deyu2
## 要傳送給 root 的郵件，轉寄給 deyu1 及 deyu2
```

5. 更新郵件別名資料庫

```
[root@kvm8 ~]# newaliases
/etc/aliases: 77 aliases, longest 10 bytes, 775 bytes total
```

6. 編輯郵件表頭過濾檔

```
[root@mail1 ~]# vim /etc/postfix/header_checks

# 主旨包含 "廣告" 的郵件皆丟棄，並記錄爲drop header deny
/^Subject:.*廣告/   DISCARD  drop header deny
# 來自 "123.abc.com" 的郵件皆丟棄，並記錄爲drop header deny
/^From:.*@123.abc.com/   DISCARD  drop header deny
```

7. 編輯郵件內容過濾檔

```
[root@mail1 ~]# vim /etc/postfix/body_checks

# 內容包含 "網址 http://123.abc.com" 的郵件皆丟棄，
# 並記錄爲 Commercial unavailable body
/http:\/\/123\.abc\.com/  DISCARD Commercial unavailable body
```

8. 啓動 postfix 服務

```
[root@kvm8 ~]# /etc/init.d/postfix restart
```

9. 設定開機啓動 postfix 服務

```
[root@kvm8 ~]# chkconfig postfix on
```

8.5 垃圾郵件過濾

1. postfix 雖可過濾字串，來阻擋垃圾郵件，但當郵件內容以 base64 編碼時，卻無法動作。

2. 安裝 spamassassin

```
[root@mail ~]# yum install spamassassin
```

3. 編輯設定檔

```
[root@mail ~]# cat /etc/mail/spamassassin/local.cf
# These values can be overridden by editing ~/.spamassassin/user_prefs.
    cf
# (see spamassassin(1) for details)

# These should be safe assumptions and allow for simple visual sifting
# without risking lost emails.

required_hits 5
report_safe 0
rewrite_header Subject [SPAM]
blacklist_from  *@yahoo-inc.com
blacklist_from  *@goisa.it
blacklist_from  *@moopex.cz
```

4. 查詢設定檔編輯說明

```
[root@mail ~]# man Mail::SpamAssassin::Conf
```

5. 新增 spamd 群組及帳號

```
[root@mail ~]# groupadd spamd
[root@mail ~]# useradd -g spamd -s /bin/false -d /var/log/spamassassin
    spamd
[root@mail ~]# chown spamd:spamd /var/log/spamassassin
```

6. 編輯 postfix 的設定檔，將 spamassassin 整合進 postfix。

```
[root@mail ~]# vim /etc/postfix/master.cf
[root@mail ~]# grep 'spamassassin' /etc/postfix/master.cf -B4
#
    ==========================================================================

# service type  private unpriv  chroot  wakeup  maxproc command + args
#               (yes)   (yes)   (yes)   (never) (100)
#
    ==========================================================================

smtp      inet  n       -       n       -       -       smtpd -o
    content_filter=spamassassin
--
#
#mailman   unix  -       n       n       -       -       pipe
#  flags=FR user=list argv=/usr/lib/mailman/bin/postfix-to-mailman.py
#  ${nexthop} ${user}
```

```
13 spamassassin unix - n n - - pipe flags=R user=spamd argv=/usr/bin/spamc
       -e /usr/sbin/sendmail -oi -f ${sender} ${recipient}
```

7. 啓動 sapmassassin 前更新 spam rules。

```
1 [root@mail ~]# sa-update && /etc/init.d/spamassassin restart
```

8. postfix 及 spamassassin 重新載入或啓動

```
1 [root@mail ~]# /etc/init.d/postfix reload
  Reloading postfix:                                         [  OK  ]
3 [root@mail ~]# /etc/init.d/spamassassin restart
  Stopping spamd:                                            [  OK  ]
5 Starting spamd:                                            [  OK  ]
```

9. postfix 及 spamassassin 重新載入或啓動

```
1 [root@mail1 ~]# vim /etc/mail/spamassassin/custom_rule.cf
  header LOCAL_EVERYTHINGYOUNEED_RULE Subject=~ /Everything you need, you
      can find here/i
3 score LOCAL_EVERYTHINGYOUNEED_RULE 3.0
  describe LOCAL_EVERYTHINGYOUNEED_RULE Everything you need
5 [root@mail1 ~]# spamassassin -D --lint
```

8.6 安全機制

1. email server ports

```
1 postfix(smtp) tcp 25
  dovecot tcp 110,143
```

2. 防火牆設定

```
  [root@kvm8 ~]# vim /etc/sysconfig/iptables
2 ########################################################
  -A INPUT -m state --state NEW -m tcp -p tcp --dport 25 -j ACCEPT
4 -A INPUT -m state --state NEW -m tcp -p tcp --dport 110 -j ACCEPT
  -A INPUT -m state --state NEW -m tcp -p tcp --dport 143 -j ACCEPT
6 ########################################################
```

3. 防火牆重新啓動

```
[root@kvm8 ~]# /etc/init.d/iptables restart
```

4. 開機啓動防火牆

```
[root@kvm8 ~]# chkconfig iptables on
```

8.7 問題解決

1. INBOX 檔案太大，無法寫入。

```
[root@mail ~]# grep -m1 'failed to store' /var/log/maillog
Apr 22 04:10:12 localhost dovecot: lda(dywang): Error: sieve: msgid=...:
 failed to store into mailbox 'INBOX': Internal error occurred.
 Refer to server log for more information.
```

2. 解決：檢查 main.cf 設定，不足的話加大後重啓 postfix。

```
[root@mail ~]# vim /etc/postfix/main.cf
[root@mail ~]# grep mailbox_size_limit /etc/postfix/main.cf
mailbox_size_limit=512000000
[root@mail ~]# /etc/init.d/postfix restart
Shutting down postfix:                                     [  OK  ]
Starting postfix:                                          [  OK  ]
```

Chapter 9

Roundcube Webmail

9.1 Roundcube 簡介

1. Roundcube 是一套很完善的 webmail，加入 Ajax 可以讓滑鼠搬移信件。
2. CentOS 6 的額外套件 remi repo 有 rpm 套件。
3. 支援的資料庫有：mssql、mysql、mysql5、postgres、sqllite。

9.2 安裝 remi repo

1. 安裝 remi-release-6.rpm。

```
[root@mail ~]# rpm -ivh http://rpms.remirepo.net/enterprise/remi-release
    -6.rpm
```

2. 安裝時會判斷是否爲 redhat 6 版本，如果不是不能安裝。因爲本作業系統由 CentOS 6 修改，版本宣告不同，所以直接下載 repo 設定的 rpm 檔。

```
1 [root@mail ~]# wget http://rpms.remirepo.net/enterprise/remi-release-6.
    rpm
```

3. 不安裝，直接抽取 rpm 中的檔案。

```
1 [root@mail ~]# mkdir tmp
[root@mail ~]# cd tmp
3 [root@mail tmp]# rpm2cpio ../remi-release-6.rpm | cpio -idmv
```

4. 複製 repo 檔及 gpg 檢查檔至系統指定位置。

```
[root@mail tmp]# cp etc/yum.repos.d/remi.repo /etc/yum.repos.d/
[root@mail tmp]# cp etc/pki/rpm-gpg/RPM-GPG-KEY-remi /etc/pki/rpm-gpg/
```

9.3 架設 Roundcube

1. 安裝 roundcubemail 套件。

```
[root@mail ~]# yum install roundcubemail --enablerepo=remi
```

2. 安裝 mysql-server 套件。

```
[root@mail ~]# yum install mysql-server --enablerepo=remi
```

3. 啓動 mysqld 服務。

```
[root@mail ~]# /etc/init.d/mysqld start
[root@mail ~]# chkconfig mysqld on
```

4. 執行安全安裝設定，主要是設定 root 密碼。

```
[root@mail ~]# mysql_secure_installation
```

5. 登入 mysql 建立資料庫 roundcube 及用户 ronudcube。

```
[root@mail ~]# mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 6
Server version: 5.5.49 MySQL Community Server (GPL) by Remi

Copyright (c) 2000, 2016, Oracle and/or its affiliates. All rights
    reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.
```

```
13 Type 'help;' or '\h' for help. Type '\c' to clear the current input
       statement.

15 mysql> CREATE DATABASE roundcube;
   Query OK, 1 row affected (0.00 sec)
17
   mysql> GRANT ALL PRIVILEGES ON roundcube.* TO roundcube@localhost
       IDENTIFIED BY 'password';
19 Query OK, 0 rows affected (0.00 sec)

21 mysql> FLUSH PRIVILEGES;
   Query OK, 0 rows affected (0.00 sec)
```

6. roundcube 的主網頁預設在 /usr/share/roundcubemail。

```
   [root@mail ~]# vim /etc/httpd/conf.d/roundcubemail.conf
2  [root@mail ~]# grep Alias /etc/httpd/conf.d/roundcubemail.conf
   Alias /roundcubemail /usr/share/roundcubemail
```

7. roundcube 預設只有本機可以連線安裝目錄，如果在遠端連線必須修改存取限制。

```
1  [root@mail ~]# grep -A15 '<Directory.*installer' /etc/httpd/conf.d/
       roundcubemail.conf | grep -v '#'
   <Directory /usr/share/roundcubemail/installer/>
3      <IfModule mod_authz_core.c>
           Require local
5      </IfModule>
       <IfModule !mod_authz_core.c>
7          Order Allow,Deny
           Allow from all
9      </IfModule>
   </Directory>
```

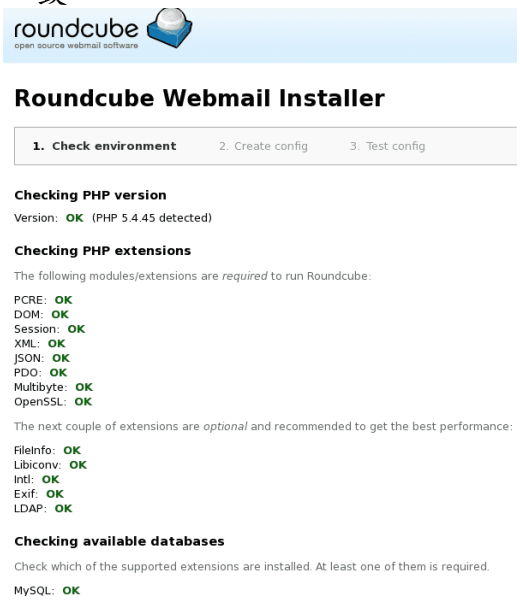
8. 連線 installer 測試系統是否滿足？

```
https://webmail.csie.cyut.edu.tw/roundcubemail/installer/
```

9. 測試顯示 mysql 資料庫不能便用，安裝 php-mysqlnd，重新啓動 mysqld 及 httpd 服務後顯示 mysql 資料已可使用。

```
[root@mail ~]# yum install php-mysqlnd --enablerepo=remi
[root@mail ~]# /etc/init.d/mysqld restart
Stopping mysqld:                                           [  OK  ]
Starting mysqld:                                           [  OK  ]
[root@mail ~]# /etc/init.d/httpd restart
Stopping httpd:                                            [  OK  ]
Starting httpd:                                            [  OK  ]
```

10. 再連線 installer 測試系統，mysql 資料已可以使用，依安裝網頁指引進行設定，重點是使用 mysql 資料庫，資料庫名稱、使用者及密碼必須與先前產生的一致。




```
Database name: 資料庫名稱
Database user name: 資料庫使用者
Database password: 資料庫密碼
```

11. 設定好之後下載 config.inc.php 至 mail server 的 /etc/roundcubemail 目錄。安全起見，移除安裝目錄或將其設定成其他用户無法存取。

```
[root@mail roundcubemail]# chmod 700 installer/
```

9.4 顯示調整

1. 將要啓動的插件，加到 $config['plugins'] 陣列中，若要移除則將其從陣到中刪除。

2. roundcubemail 用户無法自訂顯示字型，因預設網頁字型 11px 太小，統一改成 14px。

```
[root@mail roundcubemail]# grep 'font-size:\ *11px' -R . -l | xargs sed
   -i 's/\(font-size:\ *\)11px/\114px/g'
```

3. 調整左右區塊的最大高度一樣。

```
[root@mail roundcubemail]# cd skins/classic
[root@mail classic]# vim mail.css
[root@mail classic]# egrep -A8 'mail(left|right)container' mail.css
#mailleftcontainer
{
  position: absolute;
  top: 0;
  left: 0;
  bottom: 0;
  width: 185px;
  max-height: 900px;
}
--
#mailrightcontainer
{
  position: absolute;
  top: 0;
  left: 185px;
  bottom: 0;
  right: 0;
  min-width: 200px;
  max-height: 900px;

[root@mail classic]# grep -A7 ^#mainscreen common.css
#mainscreen
{
  position: absolute;
  top: 85px;
  right: 20px;
  bottom: 20px;
  left: 20px;
  max-height:900px;
```

9.5 啓動 Plugins

1. 將要啓動的插件，加到 $config['plugins'] 陣列中，若要移除則將其從陣到中刪除。

```
[root@mail plugins]# tail -5 /etc/roundcubemail/config.inc.php
$config['plugins'] = array('pop3fetcher',
            'newmail_notifier',
            'userinfo','password'
);
```

2. 加入的插件必須存在於 /usr/share/roundcubemail/plugins 目錄，例如 userinfo 插件，userinfo 目錄存在於 /usr/share/roundcubemail/plugins 下，且其目錄有 userinfo.php 檔，檔案內有 class userinfo。

```
[root@mail plugins]# pwd
/usr/share/roundcubemail/plugins
[root@mail plugins]# ls userinfo/userinfo.php
userinfo/userinfo.php
[root@mail plugins]# grep userinfo userinfo/userinfo.php
class userinfo extends rcube_plugin
        $this->add_texts('localization/', array('userinfo'));
        $this->register_action('plugin.userinfo', array($this, 'infostep
            '));
        $this->include_script('userinfo.js');
```

9.6 Managesieve Plugin

1. 確認 devocot 的 lda 協定啓動，加入 sieve 語法。

```
[root@mail ~]# vim /etc/dovecot/conf.d/15-lda.conf
[root@mail ~]# grep '^protocol lda' -A5  /etc/dovecot/conf.d/15-lda.conf
    | grep -v \#
protocol lda {
  mail_plugins = $mail_plugins sieve
}
```

2. 確認 postfix 將郵件傳送到 dovecot。

```
[root@mail ~]# vim /etc/postfix/main.cf
[root@mail ~]# grep ^mailbox_command /etc/postfix/main.cf
mailbox_command = /usr/libexec/dovecot/deliver
```

3. 安裝 sieve 套件。

```
[root@mail ~]# yum install dovecot-pigeonhole
```

4. 設定 sieve。

```
[root@mail ~]# vim /etc/dovecot/conf.d/90-plugin.conf
[root@mail ~]# grep ^plugin -A8 /etc/dovecot/conf.d/90-plugin.conf
plugin {
  #setting_name = value
  sieve=~/.dovecot.sieve
  sieve_dir = ~/sieve
  sieve_global_dir = /home/sieve
  sieve_max_script_size = 1M
}
```

5. dovecot 協定加入 sieve。

```
[root@mail ~]# grep ^protocol /etc/dovecot/dovecot.conf
protocols = imap pop3 lmtp sieve
```

6. managesieve-login 服務的 port 4190。

```
[root@mail ~]# vim /etc/dovecot/conf.d/20-managesieve.conf
[root@mail ~]# grep managesieve-login -A4 /etc/dovecot/conf.d/20-
   managesieve.conf
service managesieve-login {
  inet_listener sieve {
    port = 4190
  }
```

7. 重新啓動 dovecot。

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

8. 出現以下訊息

```
Unable to connect to managesieve on localhost:4190
```

9. 使用自訂 selinux 政策的方法找到 selinux 管制項目，將其開啓後正常。

```
[root@mail plugins]# getsebool -a | grep httpd_can_network_connect
httpd_can_network_connect --> off
httpd_can_network_connect_cobbler --> off
httpd_can_network_connect_db --> off
[root@mail plugins]# setsebool -P httpd_can_network_connect on
```

10. 轉信不成功，查 log 如下，再查前後訊息得知要轉入的目錄檔案過大，修正後正常。

```
Jun  3 09:11:39 localhost dovecot: lda(dywang): Error: sieve: execution
    of script \
~/.dovecot.sieve failed, but implicit keep was successful \
(user logfile ~/.dovecot.sieve.log may reveal additional details)
```

9.7 Password Plugin

1. 複製 password 插件設定範例。

```
[root@mail plugins]# cp password/config.inc.php.dist password/config.inc
    .php
```

2. 編輯 password 插件設定檔，本系統使用 ldap 認證帳號，所以 driver 使用 ldap，有關 ldap 的設定參數必須配合 ldap server。

```
[root@mail plugins]# vim password/config.inc.php
[root@mail plugins]# grep ldap password/config.inc.php | grep -v '//'
$config['password_driver'] = 'ldap';
$config['password_ldap_host'] = '192.168.122.1';
$config['password_ldap_port'] = '389';
$config['password_ldap_starttls'] = false;
$config['password_ldap_version'] = '3';
$config['password_ldap_basedn'] = 'dc=deyu,dc=wang';
$config['password_ldap_method'] = 'user';
$config['password_ldap_adminDN'] = null;
$config['password_ldap_adminPW'] = null;
```

```
$config['password_ldap_userDN_mask'] = 'uid=%login,ou=people,dc=deyu,dc=
    wang';
$config['password_ldap_searchDN'] = 'ou=People,dc=deyu,dc=wang';
$config['password_ldap_searchPW'] = 'secret';
$config['password_ldap_search_base'] = 'ou=people,dc=deyu,dc=wang';
$config['password_ldap_search_filter'] = '(uid=%login)';
$config['password_ldap_encodage'] = 'crypt';
$config['password_ldap_pwattr'] = 'userPassword';
$config['password_ldap_force_replace'] = true;
$config['password_ldap_lchattr'] = '';
$config['password_ldap_samba_pwattr'] = '';
$config['password_ldap_samba_lchattr'] = '';
[root@mail plugins]# cp password/config.inc.php.dist password/config.inc
    .php
```

9.8 markasjunk Plugin

1. 設定成垃圾郵件成功但無法搬移到 Junk 目錄。

```
Server Error: UID COPY: Mailbox doesn't exist: Junk
```

2. 在 roundcubemail 主設定檔加入 junk_mbox 指定到存在的垃圾郵件目錄。

```
[root@mail plugins]# vim /etc/roundcubemail/config.inc.php
[root@mail plugins]# grep junk_mbox /etc/roundcubemail/config.inc.php
$config['junk_mbox'] = 'Spam';
```

9.9 rcguard Plugin

1. 密碼輸出錯誤次數達設定值時，出現「I'm Not a Robot」認證，以防止有心人以程式進行登入嘗試。下載外掛套件：

```
[root@mail ~]# cd /usr/share/roundcubemail/plugins/
[root@mail plugins]# wget https://github.com/dsoares/roundcube-rcguard/
    archive/master.zip
```

2. 解壓縮下載的 master 檔，產生目錄 roundcube-rcguard-master，將此目錄重新命名爲 rcguard。

```
[root@mail plugins]# unzip master
[root@mail plugins]# mv roundcube-rcguard-master rcguard
```

3. 進入 rcguard 目錄，複製 config.inc.php.dist 爲 config.inc.php。

```
[root@mail plugins]# cd rcguard/
[root@mail rcguard]# cp config.inc.php.dist config.inc.php
```

4. 從 http://www.google.com/recaptcha 取得 recaptcha 的 publickey 及 privatekey，並將其寫入設定檔 config.inc.php。

```
[root@mail rcguard]# vim config.inc.php
[root@mail rcguard]# grep recaptcha.*key config.inc.php
$rcmail_config['recaptcha_publickey'] = 'xxxxxxxxxxxxxxxxxxxxxx';
$rcmail_config['recaptcha_privatekey'] = 'xxxxxxxxxxxxxxxxxxxxxx';
```

5. 修改設定，嘗試登入失敗 3 次出現「I'm Not a Robot」認證。

```
[root@mail rcguard]# vim config.inc.php
[root@mail rcguard]# grep failed_attempts config.inc.php
$rcmail_config['failed_attempts'] = 3;
```

6. 修改外掛套件名稱爲 rcguard。

```
[root@mail rcguard]# grep name.*rc composer.json
    "name": "rcguard",
```

7. 進入 SQL 目錄，以 mysql.initial.sql 在 roundcube 資料庫產生 rcguard 資料表。

```
[root@mail rcguard]# cd SQL/
[root@mail SQL]# mysql -uroot -p roundcube < mysql.initial.sql
Enter password:
```

8. 在 roundcubemail 主設定檔 plugins 加入 rcguard。

```
[root@mail SQL]# grep rcguard /etc/roundcubemail/config.inc.php
$config['plugins'] = array('fetchmail',.... ,'rcguard')
```

9. 測試輸入錯誤密碼 3 次後，出現「I'm Not a Robot」認證。



9.10 Spell check

1. 執行拼字檢查出現彈出視窗An error ....，log 檔出現 PHP Error:...。

```
An error was encountered on the server. Please try again later.

PHP Error: Spell check engine error: Unable to load Pspell engine for
    selected language
 in /usr/share/roundcubemail/program/steps/utils/spell.inc on line 50
```

2. 拼字檢查預設是使用 aspell，未解決前改成 googie 運作正常。

```
[root@mail plugins]# vim /etc/roundcubemail/config.inc.php
[root@mail plugins]# grep spellcheck_engine /etc/roundcubemail/config.
    inc.php$config
['spellcheck_engine'] = 'googie';
```

9.11 fetchmail-rc Plugin

1. 從 GitHub 下載原始碼。

```
https://github.com/iabsis/roundcube-fetchmail-rc
```

2. 必須安裝 fetchmail 套件。

```
[root@mail ~]# yum install fetchmail
```

3. 解壓縮至 roundcubemail 插件目錄 plugins。

```
[root@mail ~]# cd /usr/share/roundcubemail/plugins/
[root@mail plugins]# unzip roundcube-fetchmail-rc-master.zip
```

4. 解壓縮的目錄爲 roundcube-fetchmail-rc-master 與插件主 php 檔 fetchmail_rc.php 及 class 名稱不同，必須改成 fetchmail_rc。

```
[root@mail plugins]# ls roundcube-fetchmail-rc-master
bash_cron.php    fetchmail_rc.php  localization                    skins
config.inc.php   includes          README.md                       SQL
fetchmail_rc.js  INSTALL           roundcube-fetchmail-rc-master

[root@mail plugins]# mv roundcube-fetchmail-rc-master fetchmail_rc
```

5. roundcubemail 啓動 fetchmail_rc 插件。

```
[root@mail plugins]# vim /etc/roundcubemail/config.inc.php
[root@mail plugins]# grep fetchmail_rc /etc/roundcubemail/config.inc.php
$config['plugins'] = array('fetchmail_rc',# 'pop3fetcher',
```

6. 設定每 5 分鐘收信一次。

```
[root@mail plugins]# echo '*/5 * * * * root /usr/share/roundcubemail/\
plugins/fetchmail_rc/bash_cron.php' >> /etc/cron.d/fetchmail

[root@mail plugins]# chmod a+x /usr/share/roundcubemail/plugins/\
fetchmail_rc/bash_cron.php
```

9.12 fetchmail Plugin

1. 從 GitHub 下載原始碼。

```
https://github.com/PF4Public/fetchmail
```

2. 必須安裝 fetchmail 套件。

```
[root@mail ~]# yum install fetchmail
```

3. 解壓縮至 roundcubemail 插件目錄 plugins。

```
[root@mail ~]# cd /usr/share/roundcubemail/plugins/
[root@mail plugins]# unzip fetchmail-master.zip
```

4. 解壓縮的目錄爲 fetchmail-master 與插件主 php 檔 `fetchmail.php` 及 class 名稱不同，必須改成 `fetchmail`。

```
[root@mail plugins]# ls fetchmail-master
composer.json        fetchmail.js   localization  skins
config.inc.php.dist  fetchmail.php  README.md     SQL

[root@mail plugins]# mv fetchmail-master fetchmail
```

5. roundcubemail 啓動 `fetchmail` 插件。

```
[root@mail plugins]# vim /etc/roundcubemail/config.inc.php
[root@mail plugins]# grep fetchmail /etc/roundcubemail/config.inc.php
$config['plugins'] = array('fetchmail',# 'pop3fetcher',
```

6. 將 fetchmail 插件附的 mysql.initial.sql 匯入 roundcube 資料庫，會產生 fetchmail 資料表供插件存取用。

```
[root@mail fetchmail]# mysql -uroot -p roundcube < SQL/mysql.initial.sql
Enter password:
```

7. 下載 fetchmail.pl。

```
[root@mail plugins]# cd fetchmail
[root@mail fetchmail]# wget https://sourceforge.net/p/postfixadmin/code/
    HEAD\
/tree/trunk/ADDITIONS/fetchmail.pl?format=raw \
--no-check-certificate -O fetchmail.pl
```

8. 修改 fetchmail.pl 程式：使用 mysql 資料庫，確定設定的資料庫、帳號及密碼確實可以登入 mysql 且有存取資料庫的權限。

```
[root@mail fetchmail]# diff -uN fetchmail.pl.orig fetchmail.pl
--- fetchmail.pl.orig   2016-06-06 14:14:55.335002899 +0800
+++ fetchmail.pl    2016-06-06 14:25:48.907678523 +0800
@@ -14,17 +14,17 @@
 # database settings

 # database backend - uncomment one of these
-our $db_type = 'Pg';
-#my $db_type = 'mysql';
+#our $db_type = 'Pg';
+my $db_type = 'mysql';

 # host name
 our $db_host="127.0.0.1";
 # database name
-our $db_name="postfix";
+our $db_name="roundcube";
 # database username
-our $db_username="mail";
+our $db_username="roundcube";
 # database password
-our $db_password="CHANGE_ME!";
+our $db_password="XXXXXXXXX";

 # instead of changing this script, you can put your settings to /etc/
     mail/postfixadmin/fetchmail.conf
 # just use perl syntax there to fill the variables listed above (
     without the "our" keyword). Example:
```

9. 修改 fetchmail.pl 程式：fetchmail 插件存入資料庫的 active 欄位是 0 或 1，不是 t。

```
@@ -83,7 +83,7 @@
 if($db_type eq "Pg") {
    $sql_cond = "active = 1 AND date_part('epoch',now())-date_part('
        epoch',date)";
 } elsif($db_type eq "mysql") {
-   $sql_cond = "active = 't' AND unix_timestamp(now())-unix_timestamp(
    date)";
```

```
+   $sql_cond = "active = 1 AND unix_timestamp(now())-unix_timestamp(
    date)";
 }

 $sql = "
```

10. 修改 fetchmail.pl 程式：fetchmail 插件設定 fetchmail 時存入資料庫的 mailbox 欄位是自動取得 roundcubemail 上的帳號，如果沒有 @momainname 會自動加入 @localhost，但這會造成信件無法無法傳送到 username@localhost，所以。

```
@@ -96,6 +96,7 @@
 map{
    my ($id,$mailbox,$src_server,$src_auth,$src_user,$src_password,
        $src_folder,$fetchall,$keep,$protocol,$mda,$extra_options,
        $usessl,$sslcertck,$sslcertpath,$sslfingerprint)=@$_;

+   $mailbox.='@'.$ENV{'HOSTNAME'};
    syslog("info","fetch ${src_user}@${src_server} for ${mailbox}");

    $cmd="user '${src_user}' there with password '".decode_base64(
        $src_password)."'";
```

11. 將 fetchmail.pl 設定擁有者及群組都爲 mail，且可執行。

```
[root@mail fetchmail]# chown mail.mail fetchmail.pl
[root@mail fetchmail]# chmod 700 fetchmail.pl
[root@mail fetchmail]# ll fetchmail.pl
-rwx------. 1 mail mail 3940 Jun  6 14:25 fetchmail.pl
```

12. 設定每 5 分鐘以 mail 帳號執行 fetchmail.pl，依據 roundcube 資料庫中的資料表 fetchmail 進行收信。

```
[root@mail fetchmail]# vim /etc/cron.d/fetchmail
[root@mail fetchmail]# cat /etc/cron.d/fetchmail
*/5 * * * * mail /usr/share/roundcubemail/plugins/fetchmail/fetchmail.pl
```

13. 增加收取遠端郵件間格最小 3 分鐘。

```
[root@mail fetchmail]# diff -uN ../fetchmail-master/fetchmail.php
    fetchmail.php
```

```
--- ../fetchmail-master/fetchmail.php   2016-05-16 23:56:37.000000000
    +0800
+++ fetchmail.php   2016-06-06 20:18:35.808930991 +0800
@@ -239,6 +239,7 @@
                'id' => $field_id
        ) );
        $input_fetchmailpollinterval->add ( array (
+               '3',
                '5',
                '10',
                '15',
@@ -247,6 +248,7 @@
                '30',
                '60'
        ), array (
+               '3',
                '5',
                '10',
                '15',
```

14. 設定項目標籤欄位太小，以致於整個畫面過高，且設定表格與帳號顯示表格寬度不一致。加大 fetchmail 插件設定界面最大寬度，並讓帳號顯示背景不大於表格寬度，則兩個表格顯示寬度一樣。

```
[root@mail fetchmail]# diff -uN ../fetchmail-master/skins/default/
    fetchmail.css skins/default/fetchmail.css
--- ../fetchmail-master/skins/default/fetchmail.css 2016-05-16
    23:56:37.000000000 +0800
+++ skins/default/fetchmail.css 2016-06-06 20:16:26.698405723 +0800
@@ -3,7 +3,7 @@
    background-color: #F9F9F9;
    height: 163px;
    overflow: auto;
-   width: 450px;
+   width: 650px;
 }

 body.fetch-table {
@@ -42,7 +42,7 @@

 #myprefs {
    /* border: 1px solid #909090 !important;*/
-   width: 480px;
+   width: 680px;
    padding-top: 12px;
    padding-left: 12px;
    padding-bottom: 6px;
```

9.13 enigma Plugin

1. 預設 PGP keys 存在此插件目錄下的 home，但 apache 無法寫入此目錄。

```
PHP Error: Enigma plugin: Keys directory isn't writeable:
/usr/share/roundcubemail/plugins/enigma/home in
/usr/share/roundcubemail/plugins/enigma/lib/enigma_engine.php on line 92
(POST /roundcubemail/?_task=settings&_action=plugin.enigmakeys)
```

2. 將此目錄的擁有者改成 apache，修改後還是無法寫法，必須使用 SELinux 自訂政策方式加入 selinux 政策模組才行。

```
[root@mail enigma]# chown apache home
[root@mail enigma]# ll -d home
drwxr-xr-x. 3 apache root 4096 Jun  3 13:53 home
```

9.14 Disk Quota

1. 顯示收件夾目錄及郵件儲存目錄的使用量，必須在 dovecot 設定，可以同時設定多個硬碟空間 quota 檢查，以下設定爲檢查掛載 /var/spool/mail 及 /home 的檔案系統。

```
[root@mail roundcubemail]# vim /etc/dovecot/conf.d/90-quota.conf
.......
mail_plugins = $mail_plugins quota
protocol lda {
  mail_plugins = quota
}
protocol imap {
  mail_plugins = $mail_plugins imap_quota
}
plugin {
  #quota = dirsize:User quota
  #quota = maildir:User quota
  #quota = dict:User quota::proxy::quota
  #quota = dict:User quota::file:%h/Mail/dovecot-quota
  #quota_rule = *:storage=250M:messages=1000
  quota = fs:INBOX:mount=/var/spool/mail
  quota2 = fs:Home:mount=/home
```

2. 重新啓動 Dovecot。

```
[root@mail roundcubemail]# /etc/init.d/dovecot restart
```

3. 登入 roundcubemail 沒有顯示硬碟的使用量，檢查紀錄檔發現以下訊息，此爲 SELinux 管制問題，請參考自訂 SELinux 政策處理。

```
[root@mail dovecot]# grep quota /var/log/maillog
Aug 31 18:37:44 localhost dovecot: imap(userxxxx): Error: quotactl(
    Q_GETQUOTA,
/dev/xxxxx) failed: Permission denied
```

4. 將自訂 SELinux 政策模組加入。

```
[root@mail ~]# semodule -i /etc/dovecot/dovecotquota.pp
```

5. doveadm 查詢用户使用硬碟狀況。

```
[root@mail ~]# doveadm quota get -u dywang
Quota name                      Type      Value   Limit  %
INBOX                           STORAGE   37864  250000 15
home                            STORAGE 4241310 7340032 57
```

6. /home 目錄爲 NFS，Dovecot 目前不支援。

```
[root@mail dovecot]# grep quota /var/log/maillog
Aug 31 18:17:57 localhost dovecot: imap(userxxxx): Error: quotactl(
    Q_GETQUOTA,
 xxx.xxx.xxx.xxx:/home) failed: No such file or directory
```

9.15 移機或備份

1. 在新主機上安裝必要套件。

```
[root@dns ~]# yum install roundcubemail postfix dovecot mysql-server
```

2. 備份用户郵件、mysql 資料庫、roundcubemail 程式、postfix, dovecot, roundcubemail 設定檔案。

```
[root@mail ~]# rsync -av /var/lib/mysql 163.17.10.1:/var/lib/
[root@mail ~]# rsync -av /etc/{postfix,dovecot,roundcubemail}
    163.17.10.1:/etc/
[root@mail ~]# rsync -av /usr/share/roundcubemail 163.17.10.1:/usr/share
    /
[root@mail ~]# rsync -av --exclude=root --exclude=lost+found --exclude=
    rpc \
/var/spool/mail 163.17.10.1:/var/spool/
```

3. 修改 postfix 主設定檔的主機名稱。

```
[root@dns ~]# grep csie.cyut.edu.tw /etc/postfix/main.cf
myhostname = csie.cyut.edu.tw
mydomain = csie.cyut.edu.tw
```

4. 設定 dovecot postmaster_address。

```
[root@dns ~]# grep csie.cyut.edu.tw /etc/dovecot/dovecot.conf
postmaster_address=postmaster at csie.cyut.edu.tw
```

5. 修改 roundcubemail 預設 mail server 主機，此設定也會影響 roundcubemail 登入。

```
[root@dns ~]# vim /etc/roundcubemail/config.inc.php
[root@dns ~]# grep csie.cyut.edu.tw /etc/roundcubemail/config.inc.php
$config['default_host'] = "csie.cyut.edu.tw";
```

6. roundcubemail 登入帳號在 mysql 資料庫中以 username, mail_host 兩個欄位做斷判，備份到新主機的資料庫如果不修改，由於郵件主機不同，因此登入時會新產生一筆帳號。上一動作將 roundcubemail 預設 mail server 改成 csie.cyut.edu.tw，mysql 資料庫 roundcubemail 帳號中的 mail_host 也必須改成 csie.cyut.edu.tw，這樣才能使用原有帳號的設定。

```
[root@dns ~]# mysql -uroot -pxxxxxx -e "use roundcube; \
update users set mail_host='csie.cyut.edu.tw' \
where mail_host='mail.csie.cyut.edu.tw';"
```

9.16 問題解決

1. 問題一：開啓插件 fetchmail 時 /var/log/roundcubemail/error.log 出現錯誤訊息。

```
[07-Jun-2016 11:49:36 +0800]: <6p6bhr1o> Warning: Call to deprecated
function rep_specialchars_output(); See bc.inc for replacement
```

2. 問題一解決：roundcubemail 1.2 版的 bc.php 以 1.1.5 版的 bc.php。

```
1009  wget https://github.com/roundcube/roundcubemail/releases/download
   /1.1.5/roundcubemail-1.1.5.tar.gz
1011  tar zxvf roundcubemail-1.1.5.tar.gz
1012  find roundcubemail-1.1.5 -name bc.php
1013  cd /usr/share/roundcubemail/
1014  mv program/include/bc.php program/include/bc.php.orig
1015  cp /usr/src/roundcubemail-1.1.5/program/include/bc.php program/
   include/
1016  cd program/include/
1017  diff -uN bc.php.orig bc.php
1018  tail /var/log/roundcubemail/errors.log
```

Chapter 10

OPENLDAP 網路用户帳號

10.1 LDAP 簡介

1. LDAP (Lightweight Directory Access Protocol)：輕量級目錄存取協定，運作於 TCP/IP 四層上，LDAP 跟運作於 OSI 七層的重量級協定 X.500 相比之下叫輕量級。

2. LDAP 目錄結構組成

   - DN，Distinguished Name：識別名稱，LDAP 中一筆記錄的位置
   - RDN，Relative Distinguished Name：相對識別名稱，CN 及 CN 的值。例如：cn=deyu 獨一無二的屬性。
   - CN，Common Name/uid：顯示名稱，一筆 LDAP 記錄的名字/ID
   - OU，Organizational Unit：組織，一筆 LDAP 記錄所屬組織
   - DC，Domain Componet：網域元件，一筆 LDAP 記錄所屬區域

3. LDAP DN 例子：在 deyu.wang 網域內 people 組織中使用者 dywtest。

```
dn: cn=dywtest,ou=people,dc=deyu,dc=wang
```

10.2 LDAP Server 建置

1. 安裝套件

```
[root@deyu ~]# yum install openldap openldap-servers openldap-clients
[root@deyu ~]# rpm -qa | grep openldap
openldap-2.4.19-15.el6.x86_64
openldap-clients-2.4.19-15.el6.x86_64
openldap-servers-2.4.19-15.el6.x86_64
```

2. 編輯主要設定檔 slapd.conf

(a) 安裝好 openldap-server 並沒有 sldap.conf，只有 slapd.conf.bak，故先複製。

```
[root@deyu ~]# cd /etc/openldap
[root@deyu openldap]# cp slapd.conf.bak slapd.conf.dywang
[root@deyu openldap]# vim slapd.conf.dywang
```

(b) 取消以下三行註解，並修改認證憑證名稱與產生的憑證相同。

```
TLSCACertificateFile /etc/pki/tls/certs/cacert.pem
TLSCertificateFile /etc/pki/tls/certs/slapd.pem
TLSCertificateKeyFile /etc/pki/tls/certs/slapd.pem
```

(c) 修改 dc cn 認證憑證名稱與產生的憑證相同。

```
database    bdb
suffix      "dc=deyu,dc=wang"
checkpoint  1024 15
rootdn      "cn=Manager,dc=deyu,dc=wang"
```

(d) 設定管理者密碼，密碼先使用 slappasswd 加密，選項 -h 指定使用 SSHA 加密，-s 指定明文密碼爲 123qwe。

```
[root@dywH ~]# slappasswd -h {SSHA} -s 123qwe
{SSHA}fIsVNaDqlaFxlQne+t/8Oq/6VQM2l/Fi
```

(e) 設定管理者密碼。

```
[root@dywH ~]# grep ^rootpw /etc/openldap/slapd.conf.dywang
rootpw  {SSHA}fIsVNaDqlaFxlQne+t/8Oq/6VQM2l/Fi
```

(f) 設定用户可修改自己的密碼，特別注意：database monitor 必須放在 access 設定之後，否則無效

```
# enable monitoring
access to attrs=userPassword
  by self write
  by anonymous auth
  by dn.base="cn=Manager,dc=deyu,dc=wang" write
  by * none
access to *
  by self write
  by dn.base="cn=Manager,dc=deyu,dc=wang" write
  by * read
database monitor
```

3. 將 ldap.conf.dywang 設定檔轉換格式到指定目錄

```
[root@deyu openldap]# mv slapd.d slapd.d.orig
[root@deyu openldap]# mkdir slapd.d
[root@deyu openldap]# chown ldap.ldap slapd.d
[root@deyu openldap]# slaptest -f slapd.conf.dywang -F slapd.d
[root@deyu oepnldap]# chown ldap.ldap -R /etc/openldap/slapd.d
[root@deyu openldap]# restorecon -R /etc/openldap/slapd.d
```

4. 檔案 DB_CONFIG 設定 index 的快取數量，可調整效能的表現，若不設定，直接產生一個空檔案即可。

```
[root@deyu ~]# touch /var/lib/ldap/DB_CONFIG
[root@deyu ~]# find /usr -name DB_CONFIG*
/usr/share/doc/openldap-servers-2.4.19/DB_CONFIG.example
[root@deyu ~]# cp /usr/share/doc/openldap-servers-2.4.19/DB_CONFIG.
    example\
/var/lib/ldap/DB_CONFIG
```

5. LDIF 語法：

```
#The LDAP Data Interchange Format (LDIF) 是 LDAP 的明文格式檔。
 1. 井號 (#) 爲註解
 2. 冒號 (:) 左邊爲屬性，右邊爲屬性值 (記得空一格)
 3. dn 即爲該項目 (entry)
 4. 跨列時不使用一般的倒斜線 \ 來接續下一行，只需在下一列開頭加一空格即
    可。
```

6. 利用 migrationtools 工具產生 ldif 格式檔

```
[root@deyu ~]# yum install migrationtools
[root@deyu ~]# vi /usr/share/migrationtools/migrate_common.ph
# Default DNS domain
$DEFAULT_MAIL_DOMAIN = "deyu.wang";

# Default base
$DEFAULT_BASE = "dc=deyu,dc=wang";

[root@deyu ~]# mkdir /root/ldif
[root@deyu ~]# cd /root/ldif
[root@deyu ldif]# vi passwd
ldapuser1:x:1001:1001::/home/guests/ldapuser1:/bin/bash
ldapuser2:x:1002:1002::/home/guests/ldapuser2:/bin/bash
# 格式與 /etc/passwd 相同
[root@deyu ldif]# vi group
ldapuser1:x:1001:
ldapuser2:x:1002:
# 格式與 /etc/group 相同
[root@deyu ~]# cd /usr/share/migrationtools/
[root@deyu migrationtools]# ./migrate_base.pl > /root/ldif/migratebase.
    ldif
[root@deyu migrationtools]# ./migrate_passwd.pl /root/ldif/passwd > /
    root/ldif/migratepasswd.ldif
[root@deyu migrationtools]# ./migrate_group.pl /root/ldif/group > /root/
    ldif/migrategroup.ldif
```

7. 產生加密密碼

```
[root@deyu ~]# slappasswd
New password:
Re-enter new password:
{SSHA}HAvRpYe5TR88asauGqYtoCFzT7qHYqjP
[root@deyu ~]# vi /root/ldif/migratepasswd
```

```
dn: uid=ldapuser1,ou=People,dc=deyu,dc=wang
uid: ldapuser1
cn: ldapuser1
objectClass: account
objectClass: posixAccount
objectClass: top
userPassword: {SSHA}HAvRpYe5TR88asauGqYtoCFzT7qHYqjP <==密碼
loginShell: /bin/bash
uidNumber: 1001
gidNumber: 1001
homeDirectory: /home/guests/ldapuser1
```

8. 查看 base 及 group 的 ldif 檔

```
[root@deyu ~]# cat /root/ldif/migratebase.ldif
dn: dc=deyu,dc=wang
dc: deyu
objectClass: top
objectClass: domain
----省略----

[root@deyu ~]# cat /root/ldif/migrategroup.ldif
dn: cn=ldapuser1,ou=Group,dc=deyu,dc=wang
objectClass: posixGroup
objectClass: top
cn: ldapuser1
userPassword: {crypt}x
gidNumber: 1001
```

9. 將 bdn.ldif 及 user.ldif 匯入 LDAP 資料庫

```
[root@deyu ~]# /etc/init.d/slapd stop
Stopping slapd:                                            [  OK  ]
[root@deyu ~]# slapadd -l /root/ldif/migratebase.ldif
bdb_db_open: DB_CONFIG for suffix "dc=deyu,dc=wang" has changed.
Performing database recovery to activate new settings.
_#################### 100.00% eta   none elapsed            none fast!
Closing DB...
[root@deyu ~]# slapadd -l /root/ldif/migratepasswd.ldif
_#################### 100.00% eta   none elapsed            none fast!
Closing DB...
[root@deyu ~]# slapadd -l /root/ldif/migrategroup.ldif
_#################### 100.00% eta   none elapsed            none fast!
Closing DB...
```

10. 啓動 slapd 服務

```
[root@deyu ~]# chown ldap /var/lib/ldap/*
[root@deyu ~]# /etc/init.d/slapd start
Starting slapd:                                            [  OK  ]
```

11. 查詢

```
[root@deyu ~]# ldapsearch -x -b "dc=deyu,dc=wang"
----省略----
# ldapuser1, Group, deyu.wang
dn: cn=ldapuser1,ou=Group,dc=deyu,dc=wang
objectClass: posixGroup
objectClass: top
cn: ldapuser1
userPassword:: e2NyeXB0fXg=
gidNumber: 1001
----省略----
```

10.3 CA 憑證

1. 憑證授權單位 (Certification Authority，CA) 爲具公信力第三者 (Trusted ThirdParty)，提供認證及憑證簽發管理等服務。

2. 產生 CA 憑證

```
[root@deyu ~]# cd /etc/pki/CA
[root@deyu CA]# mkdir {certs,crl,newcerts}
[root@deyu CA]# touch index.txt
[root@deyu CA]# echo 01 > serial
[root@deyu CA]# openssl req -new -x509 -nodes -out cacert.pem \
-keyout private/cakey.pem \
-subj '/C=TW/ST=Taiwan/L=CYUT/O=CSIE/CN=deyu.wang Certificate Authority'
```

3. 複製憑證至指定的地方

```
[root@deyu CA]# cp cacert.pem /etc/pki/tls/certs
```

```
[root@deyu CA]# chmod 644 /etc/pki/tls/certs/cacert.pem
[root@deyu CA]# cp cacert.pem /var/ftp/pub
[root@deyu CA]# chmod 644 /var/ftp/pub/cacert.pem
```

4. 產生 CA 簽署給 slapd 使用的憑證

```
[root@deyu ~]# umask 077
[root@deyu ~]# cd /etc/pki/tls/certs
[root@deyu certs]# rm -f slapd.pem
[root@deyu certs]# openssl req -new -nodes -out slapd.csr \
-keyout slapd.key -subj '/C=TW/ST=Taiwan/L=CYUT/O=CSIE/CN=deyu.wang'
[root@deyu certs]# openssl ca -batch -in slapd.csr -out slapd.crt
[root@deyu certs]# ( cat slapd.key; echo; cat slapd.crt ) > slapd.pem
[root@deyu certs]# chown ldap slapd.pem
[root@deyu certs]# rm -f slapd.key slapd.crt slapd.csr
```

10.4 LDAP Client 端設定

1. 安裝套件

```
[root@kvm4 ~]# yum install {openldap,openldap-clients,nss-pam-ldapd}
```

2. LDAP server 條件

```
1. ldap server: deyu.wang
2. base dn: dc=deyu,dc=wang
3. 認證證書: ftp://deyu.wang/pub/cacert.pem
4. 帳號: ldapuser1
5. 密碼: 123
```

3. 直接進行設定並啓動認證

   (a) 修改設定檔

```
[root@kvm4 ~]# vi /etc/nslcd.conf
uri ldap://deyu.wang/
base dc=deyu,dc=wang
ssl start_tls
tls_cacertdir /etc/openldap/cacerts

[root@kvm4 ~]# vi /etc/openldap/ldap.conf
URI ldap://deyu.wang/
BASE dc=deyu,dc=wang
TLS_CACERTDIR /etc/openldap/cacerts

[root@kvm4 ~]# vi /etc/pam_ldap.conf
base dc=deyu,dc=wang
uri ldap://deyu.wang/
ssl start_tls
tls_cacertdir /etc/openldap/cacerts
pam_password md5

[root@kvm4 ~]# vi /etc/nsswitch.conf
passwd:     files ldap
shadow:     files ldap
group:      files ldap
```

(b) 下載認證證書

```
[root@kvm4 ~]# cd /etc/openldap/cacerts/
[root@kvm4 cacerts]# wget ftp://deyu.wang/pub/cacert.pem
--2011-12-20 22:10:29--  ftp://deyu.wang/pub/cacert.pem
           => “cacert.pem”
Resolving deyu.wang... 192.168.122.1
Connecting to deyu.wang|192.168.122.1|:21... connected.
Logging in as anonymous ... Logged in!
==> SYST ... done.    ==> PWD ... done.
==> TYPE I ... done.  ==> CWD (1) /pub ... done.
==> SIZE cacert.pem ... 1318
==> PASV ... done.    ==> RETR cacert.pem ... done.
Length: 1318 (1.3K) (unauthoritative)

100%[======================================>] 1,318       --.-K/s
      in 0s

2011-12-20 22:10:29 (144 MB/s) - “cacert.pem” saved [1318]
```

(c) 建立證書的 hash 連結

```
[root@kvm4 cacerts]# ll
```

```
total 4
-rw-r--r--. 1 root root 1318 Dec 20 22:10 cacert.pem
[root@kvm4 cacerts]# cacertdir_rehash .
[root@kvm4 cacerts]# ll
total 4
lrwxrwxrwx. 1 root root   10 Dec 20 22:14 77bc2243.0 -> cacert.pem
-rw-r--r--. 1 root root 1318 Dec 20 22:10 cacert.pem
```

(d) 啓動 nslcd

```
[root@kvm4 ~]#  /etc/init.d/nslcd start
Starting nslcd:                                            [  OK  ]
```

(e) 測試 ldap user：用滑鼠點 Send key 的 Ctrl+Alt+F2 進入第二終端機，以 ldapuser1 登入測試密碼是否正確。

```
[root@kvm4 ~]# getent passwd ldapuser1
ldapuser1:{SSHA}HAvRpYe5TR88asauGqYtoCFzT7qHYqjP:1001:1001:
    ldapuser1:/home/guests/ldapuser1:/bin/bash
```

4. 以 authconfig 命令幫忙設定 LDAP 認證

```
[root@kvmr4 ~]# authconfig --help | grep ldap
  --enableldap          enable LDAP for user information by default
  --disableldap         disable LDAP for user information by default
  --enableldapauth      enable LDAP for authentication by default
  --disableldapauth     disable LDAP for authentication by default
  --ldapserver=<server>
  --ldapbasedn=<dn>     default LDAP base DN
  --enableldaptls, --enableldapstarttls
  --disableldaptls, --disableldapstarttls
  --ldaploadcacert=<URL>

[root@kvm4 ~]#  authconfig --enableldap --enableldapauth \
--ldapserver=deyu.wang --ldapbasedn="dc=deyu,dc=wang" --enableldaptls --
    enableldapstarttls \
--ldaploadcacert=ftp://deyu.wang/pub/cacert.pem --update
Starting nslcd:                                            [  OK  ]
```

5. 檢查要登入的帳號是否存在？

```
[root@kvm4 cacerts]# getent passwd ldapuser1
ldapuser1:{SSHA}HAvRpYe5TR88asauGqYtoCFzT7qHYqjP:1001:1001:ldapuser1:/
    home/guests/ldapuser1:/bin/bash
```

6. 登入測試

```
[root@kvm4 cacerts]# su - ldapuser1
su: warning: cannot change directory to /home/guests/ldapuser1: No such
    file or directory
-bash-4.1$
```

7. 若已掛載 NFS 後，登入 LDAP 帳號已有家目錄

```
[root@kvm4 ~]# getent passwd ldapuser1
ldapuser1:{SSHA}HAvRpYe5TR88asauGqYtoCFzT7qHYqjP:1001:1001:ldapuser1:/
    home/guests/ldapuser1:/bin/bash
[root@kvm4 ~]# su - ldapuser1
[ldapuser1@kvm4 ~]$ pwd
/home/guests/ldapuser1
```

8. LDAP client 圖形界面設定工具

```
[root@kvm4 cacerts]# system-config-authentication
1. Under, "User account database" select LDAP
2. For "base DN", enter 'dc=deyu,dc=wang'
3. For "LDAP Server", enter 'ldap://deyu.wang'
4. Click "Download certificate" and use
ftp://deyu.wang/pub/cacert.pem
5. Leave TLS *UNCHECKED*
6. Under "Authentication Method", select LDAP
7. Select Apply and complete firstboot setup
```

10.5 LDAP 帳號管理

1. 產生帳號 ldif 檔

```
[root@ildap ~]# vim ldapuser1.ldif
dn: uid=ldapuser1,ou=People,dc=deyu,dc=wang
sn: ldapuser1
uid: ldapuser1
mail:ldapuser1@csie.cyut.edu.tw
o: 資工系
cn: ldapuser1
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: top
userPassword: {SSHA}HAvRpYe5TR88asauGqYtoCFzT7qHYqjP
loginShell: /bin/bash
uidNumber: 1001
gidNumber: 1001
homeDirectory: /home/guests/ldapuser1
```

2. 加入帳號

```
[root@ildap ~]# ldapadd -x -D "cn=Manager,dc=deyu,dc=wang" -w
    secretpassword -f ldapuser1.ldif
```

3. 改變帳號密碼

```
[root@ildap ~]# ldappasswd -s newpassword -D "cn=Manager, dc=deyu,dc=
    wang" -W -x "uid=ldpauser1,ou=People,dc=deyu,dc=wang"
```

4. 刪除帳號

```
[root@ildap ~]# ldapdelete -D "cn=Manager, dc=deyu,dc=wang" -W "uid=
    ldapuser1,ou=People,dc=deyu,dc=wang"
```

5. 查詢帳號

```
[root@dywH ~]# ldapsearch -x -b "uid=ldapuser1,ou=People,dc=deyu,dc=wang
    " -s sub "objectclass=*"
# extended LDIF
#
```

```
# LDAPv3
# base <uid=ldapuser1,ou=People,dc=deyu,dc=wang> with scope subtree
# filter: objectclass=*
# requesting: ALL
#

# ldapuser1, People, deyu.wang
dn: uid=ldapuser1,ou=People,dc=deyu,dc=wang
uid: ldapuser1
cn: ldapuser1
objectClass: account
objectClass: posixAccount
objectClass: top
loginShell: /bin/bash
uidNumber: 1001
gidNumber: 1001
homeDirectory: /home/guests/ldapuser1

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
```

6. 建立 ldif 檔修改帳號 ldapuser1 的 entry，1.ldif 若多於一筆，必須以空白行隔開。若只要修改一筆，不以檔案批次修改而改以 STDIN 輸入也可以。

```
[root@dywH ~]# vim 1.ldif
[root@dywH ~]# cat 1.ldif
dn: uid=ldapuser1,ou=People,dc=deyu,dc=wang
changetype: modify
replace: loginShell
loginShell: /sbin/nologin
```

7. 以 1.ldif 檔修改帳號 ldapuser1 的 loginShell。

```
[root@dywH ~]# ldapmodify -h localhost -x -w '123qwe' -D "cn=Manager,dc=
    deyu,dc=wang" -f 1.ldif
modifying entry "uid=ldapuser1,ou=People,dc=deyu,dc=wang"
```

8. 再次查詢帳號 ldapuser1 的 loginShell 已改爲 /sbin/nologin。

```
[root@dywH ~]# ldapsearch -x -b "uid=ldapuser1,ou=People,dc=deyu,dc=wang
    " -s sub "objectclass=*"
# extended LDIF
#
# LDAPv3
# base <uid=ldapuser1,ou=People,dc=deyu,dc=wang> with scope subtree
# filter: objectclass=*
# requesting: ALL
#

# ldapuser1, People, deyu.wang
dn: uid=ldapuser1,ou=People,dc=deyu,dc=wang
uid: ldapuser1
cn: ldapuser1
objectClass: account
objectClass: posixAccount
objectClass: top
uidNumber: 2001
gidNumber: 2001
homeDirectory: /home/guests/ldapuser1
loginShell: /sbin/nologin

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
```

10.6 安全機制

1. 查詢 ldap port

```
[root@ldap ~]# grep '^ldap ' /etc/services
ldap            389/tcp
ldap            389/udp
```

2. 防火牆設定：只開放給 192.168.122.0/24 網域使用。

```
[root@ldap ~]# vim /etc/sysconfig/iptables
#########################################################
-A INPUT -s 192.168.122.0/24 -m state --state NEW -m tcp -p tcp --dport
    389 -j ACCEPT
#########################################################
```

3. 防火牆重新啓動

```
[root@ldap ~]# /etc/init.d/iptables restart
```

4. 開機啓動防火牆

```
[root@ldap ~]# chkconfig iptables on
```

10.7 問題解決

1. 問題一：server 斷電不正常關機後，無法正常啓動。

```
[root@ldap ~]# /etc/init.d/slapd restart
Stopping slapd:                                            [FAILED]
Checking configuration files for slapd:                    [FAILED]
bdb_db_open: database "...": unclean shutdown detected; attempting
    recovery.
bdb_db_open: database "...": recovery skipped in read-only mode.
Run manual recovery if errors are encountered.
stale lock files may be present in /var/lib/ldap           [WARNING]
```

2. 解決方式：

```
[root@ldap ~]# /etc/init.d/slapd stop
Stopping slapd:                                            [FAILED]

[root@ldap ~]# /usr/sbin/slapd_db_recover -v -h /var/lib/ldap/
Finding last valid log LSN: file: 2 offset 5681155
Recovery starting from [2][5680260]
Recovery complete at Sat Aug 17 13:03:49 2019
Maximum transaction ID 80000013 Recovery checkpoint [2][5681950]

[root@ldap ~]# /etc/init.d/slapd start
Checking configuration files for slapd:                    [WARNING]
bdb_db_open: database "...": unclean shutdown detected; attempting
    recovery.
bdb_db_open: database "...": recovery skipped in read-only mode.
Run manual recovery if errors are encountered.
config file testing succeeded
Starting slapd:                                            [  OK  ]

[root@ldap ~]# /etc/init.d/slapd restart
Stopping slapd:                                            [  OK  ]
Starting slapd:                                            [  OK  ]
```

Chapter 11

DNS server

11.1 DNS 簡介

1. DNS (Domain Name System)，又稱 nameserver。
2. 連結主機名稱及 ip addresses。
3. 網路使用者只要記得主機名稱，不必再乎 ip。
4. 系統管理者可以改變主機的 ip，而不影響使用者查詢。
5. DNS server 儲存的訊息，稱爲資源紀錄 resource records (RR)，例如：kvm8.deyu.wang。
6. CentOS 使用 BIND (Berkeley Internet Name Domain) 做爲 DNS server。
7. BIND 程式包含
   (a) nameserver 程式 named
   (b) 管理工具程式 rndc
   (c) 除錯程式 dig

11.2 DNS 架設

1. 安裝 bind 套件

```
[root@kvm8 ~]# yum install bind
```

2. 設定檔 /etc/named.conf 格式

```
statement-1 ["statement-1-name"] [statement-1-class] {
  option-1;
  option-2;
  option-N;
};
// 每段設定結束符號爲 ;
// // 後文字爲註解
```

3. 編輯設定檔 /etc/named.conf - options 定義 server 整體設定

```
[root@dyH ~]# cat /etc/named.conf
// named.conf for KVM
// See /usr/share/doc/bind*/sample/ for example named configuration
    files.

options {
    listen-on port 53 { any; }; // ipv4 監聽 port 53，回應任何主機的查詢
    listen-on-v6 port 53 { ::1; }; // ipv6 盛聽 port 53，只回應本機的查
        詢
    directory   "/var/named";  // 工作目錄
    // 指定 DNS database 的 cache 及 rndc dumpdb 命令的輸出
    dump-file   "/var/named/data/cache_dump.db";
    // 指定 DNS database 的 cache 及 rndc stats 命令的輸出
    statistics-file "/var/named/data/named_stats.txt";
    // 指定統計使用的記憶體位置
    memstatistics-file "/var/named/data/named_mem_stats.txt";
    allow-query { any; };  // 允許任何主機都可查詢
    recursion yes;  // 遞迴式，如果本 DNS server 查不到，會往上層查。

    dnssec-enable yes;  // 回傳 DNS Security Extensions ( DNSSEC ) 相關
        的 RR
    dnssec-validation yes; // RR 經由 DNSSEC 認證
    dnssec-lookaside auto; //DNSSEC Lookaside Validation (DLV)

    /* Path to ISC (Internet Systems Consortium 協會) DLV key */
    bindkeys-file "/etc/named.iscdlv.key";

    forward only; // 當無法從 forwarders 查詢時，也不從自己本身查詢
    forwarders {  // 指定查詢的 DNS servers
        192.168.1.254;
        168.95.1.1;
        139.175.10.20;
    };
};
```

4. 編輯設定檔 /etc/named.conf - logging 定義記錄方式

```
logging { // 允許多種型態的記錄，每種記錄以 chnnel 區分
```

```
    channel default_debug { // 預設 debug 訊息 channel
        file "data/named.run"; // 存放檔案
        severity dynamic;   // 嚴重層級爲動態
    };
};
```

5. 編輯設定檔 /etc/named.conf - zone 定義

```
zone "." IN { // .(root)
    type hint;   // root nameserver 使用的型態
    file "named.root";
};

zone "deyu.wang" IN { // zone deyu.wang 正解查詢設定
    type master;  // 指定爲主要 DNS server，zone 的設定檔在系統中
    file "named.deyu.wang";
};

// Address and Routing Parameter Area (arpa)
// IPv4 使用 in-addr.arpa 網域作爲反解的最上層 zone
// 上層網域放後面，也就是 122 < 168 < 192 < in-addr < arpa
zone "122.168.192.in-addr.arpa" IN { // 192.168.122.xxx 查詢設定
    type master;
    file "named.192.168.122";
};
```

6. 編輯正解檔

```
[root@dyH ~]# cat /var/named/named.deyu.wang
# 指令以符號 $ 開始
# A    : Address record 指定 ip
# SOA : Start of Authority recode 宣告 zone 的重要訊息
# NS   : Nameserver record 宣告管理這個 zone 的 nameserver
# MX   : Mail Exchange record 指定網域中郵件傳送的位置

# Time to Live (TTL) value 600 秒
$TTL    600

# Start of Authority (SOA)
# "主要的 name server" "連絡 name server 的 email"
#@  IN  SOA  primary-name-server hostmaster-email (
# 修改的序號
#       serial-number
# 決定 slave nameserver 等多久再問 master nameserver 是否更新
#       time-to-refresh
# master nameserver 沒回應，多久後重新請求更新
#       time-to-retry
# master nameserver 持續沒回應，超過此時間，slave nameserver 停止回應查
    詢
```

```
#       time-to-expire
# 存於其他 nameserver cache 的最小時間
#       minimum-TTL )

@   IN SOA  deyu.wang. dywang.deyu.wang. (
        201210161117 3H 15M 1W 1D );
    IN NS   deyu.wang.;

deyu.wang.  IN A     192.168.122.1;

server.deyu.wang.     IN CNAME linux.deyu.wang.

kvm2    IN A        192.168.122.2
kvm3    IN A        192.168.122.3
kvm4    IN A        192.168.122.4
kvm4    IN MX 20    kvm4.deyu.wang.
www     IN A        192.168.122.4
```

7. 編輯反解檔

```
[root@dyH ~]# vim /var/named/named.192.168.122
# PTR  : Pointer record 定義 ip 的 domain name，也就是 ip 的反解
$TTL    600
@   IN SOA  deyu.wang. dywang.deyu.wang. (
          201210161117 3H 15M 1W 1D )
@   IN NS   deyu.wang.
1   IN PTR  deyu.wang.

2   IN PTR  kvm2.deyu.wang.
3   IN PTR  kvm3.deyu.wang.
4   IN PTR  kvm4.deyu.wang.
```

8. 主機名稱最後的"kvm2.deyu.wang." 最後的"." 代表完整主機名稱，也就是 kvm2.deyu.wang，如果沒有"." 代表只是主機名稱，後面必須加上 zone，在此範例爲 122.168.192.in-addr.arpa.，IP 反過來寫，最後以 in-addr.arpa. 結束。例如：

9. 正確設定查得 192.168.122.6 的反解爲 kvm6.deyu.wang。

```
[root@dywH ~]# nslookup 192.168.122.6
Server:     127.0.0.1
Address:    127.0.0.1#53

6.122.168.192.in-addr.arpa  name = kvm6.deyu.wang.
```

10. 故意將 kvm6.deyu.wang 最後的"." 移除，再重新啓動 named。

```
[root@dywH ~]# vim /var/named/named.192.168.122
[root@dywH ~]# grep 'kvm6\.' /var/named/named.192.168.122
6   IN PTR  kvm6.deyu.wang

[root@dywH ~]# /etc/init.d/named restart
Stopping named:                                            [  OK  ]
Starting named:                                            [  OK  ]
```

11. 再次使用 nslookup 查得 192.168.122.6 的反解爲 kvm6.deyu.wang.122.168.192.in-addr.arpa.。

```
[root@dywH ~]# nslookup 192.168.122.6
Server:     127.0.0.1
Address:    127.0.0.1#53

6.122.168.192.in-addr.arpa  name = kvm6.deyu.wang.122.168.192.in-addr.
    arpa.
```

12. 郵件伺服器爲了檔垃圾郵件，會設定來信主機反解不正確退信 reject_unknown_client。如果 DNS 正反解設定不對，從該主機送到郵件伺服器的信都會被退回。例如：

```
[root@mail ~]# nslookup 163.17.1.13
Server:     163.17.10.1
Address:    163.17.10.1#53

Non-authoritative answer:
13.1.17.163.in-addr.arpa    name = mg18.cyut.edu.tw.1.17.163.in-addr.
    arpa.
13.1.17.163.in-addr.arpa    name = mail.cyut.edu.tw.
```

13. 啓動 named 服務

```
[root@kvm8 ~]# /etc/init.d/named restart
```

14. 設定開機啓動 named 服務

```
[root@kvm8 ~]# chkconfig named on
```

11.3 安全機制

1. 查詢 named server port

```
[root@dyH ~]# grep name-domain /etc/services
domain          53/tcp                          # name-domain server
```

2. 防火牆設定

```
[root@kvm8 ~]# vim /etc/sysconfig/iptables
##########################################################
-A INPUT -m state --state NEW -m tcp -p tcp --dport 53 -j ACCEPT
##########################################################
```

3. 防火牆重新啓動

```
[root@kvm8 ~]# /etc/init.d/iptables restart
```

4. 開機啓動防火牆

```
[root@kvm8 ~]# chkconfig iptables on
```

11.4 問題解決

1. 問題一：使用 rsyslog 每週會重建 /var/log/messages，但當重新產生新的 /var/log/messages 後 dns 就會當掉，查詢其內容如下：原因是 Rotation 改變檔案的 inode，Rsyslog 嘗試去寫到舊的 inode。

```
[root@dns ~]# head -n4 /var/log/messages
Dec 21 03:17:01 dns kernel: imklog 4.6.2, log source = /proc/kmsg
    started.
Dec 21 03:17:01 dns rsyslogd: [origin software="rsyslogd" swVersion="
    4.6.2" x-pid="1496" x-info="http://www.rsyslog.com"] (re)start
Dec 21 03:17:19 dns named[1004]: error (connection refused) resolving '
    racetrackslots.com/A/IN': 139.175.10.20#53
Dec 21 03:17:47 dns named[1004]: error (connection refused) resolving '
    mirrors.s.3322.net/A/IN': 139.175.10.20#53
```

2. 問題一解決方式：在 named 重啓之前先重新載入 rsyslog，以產生新的空的紀錄檔。

```
[root@dns ~]# cat /etc/logrotate.d/named
/var/named/data/named.run {
    missingok
    create 0644 named named
    postrotate
        /bin/kill -HUP `cat /var/run/syslogd.pid 2> /dev/null` 2> /dev/
            null || true
        /sbin/service named reload  2> /dev/null > /dev/null || true
    endscript
}
```

3. 重新啓動 rsyslog

```
[root@dns ~]# /etc/init.d/rsyslog restart
```

Chapter 12

Dnsmasq server

12.1 Dnsmasq 簡介

1. Dnsmasq 是一個輕量的 DNS, TFTP 及 DHCP server。
2. Dnsmasq 接受 DNS 查詢並從本地 /etc/hosts 或上層 DNS server 回應。
3. Dnsmasq DHCP server 支援固定 IP 指定及多重網路。
4. Dnsmasq 包含一個唯讀 TFTP server 以支援網路 PXE 開機。
5. Dnsmasq 支援 IPv6 DNS，但不支援 IPv6 DHCP。

12.2 Dnsmasq 架設

1. 安裝 dnsmasq 套件

```
[root@dywnb ~]# yum install dnsmasq
```

2. 啓動 dnsmasq 服務

```
[root@dywnb ~]# /etc/init.d/dnsmasq restart
```

3. 設定開機啓動 dnsmasq 服務

```
[root@dywnb ~]# chkconfig dnsmasq on
```

12.3 Dnsmasq DNS 架設

1. dnsmasq 主要設定檔爲 / etc/ dnsmasq.conf，其中 listen-address=127.0.0.1 記得要出現，否則本機無法查詢 dnsmasq。mx-host 則是設定網域內主機的郵件 MX 識別。

```
[root@dywnb ~]# vim /etc/dnsmasq.conf
listen-address=192.168.122.1
listen-address=127.0.0.1
[root@dywnb ~]# egrep -v '(^\ *$|#)' /etc/dnsmasq.conf
listen-address=192.168.122.1
listen-address=127.0.0.1
mx-host=deyu.wang,10
mx-host=kvm1.deyu.wang,20
mx-host=kvm2.deyu.wang,20
mx-host=kvm3.deyu.wang,20
mx-host=kvm4.deyu.wang,20
mx-host=kvm5.deyu.wang,20
mx-host=kvm6.deyu.wang,20
mx-host=kvm7.deyu.wang,20
mx-host=kvm8.deyu.wang,20
mx-host=kvm9.deyu.wang,20
mx-host=kvm10.deyu.wang,20
```

2. 將要設定的查詢加到 /etc/hosts。

```
[root@dywnb ~]# grep deyu.wang /etc/hosts
192.168.1.110   oveng.deyu.wang
192.168.122.1   deyu.wang
192.168.122.1   server.deyu.wang
192.168.122.2   kvm2.deyu.wang
192.168.122.2   www2.deyu.wang
192.168.122.2   dynamic2.deyu.wang
.....................
```

12.4 Dnsmasq DHCP 架設

1. Dnsmasq DHCP 設定在 /etc/dnsmasq.conf。

```
[root@dywnb ~]# grep dhcp /etc/dnsmasq.conf
#no-dhcp-interface=
#dhcp-range=192.168.0.50,192.168.0.150,12h
#dhcp-range=192.168.0.50,192.168.0.150,255.255.255.0,12h
#dhcp-range=red,192.168.0.50,192.168.0.150
#dhcp-host=11:22:33:44:55:66,192.168.0.60
```

```
#dhcp-host=11:22:33:44:55:66,fred
#dhcp-host=11:22:33:44:55:66,fred,192.168.0.60,45m
#dhcp-host=11:22:33:44:55:66,12:34:56:78:90:12,192.168.0.60
#dhcp-host=bert,192.168.0.70,infinite
#dhcp-host=id:01:02:02:04,192.168.0.60
#dhcp-host=id:marjorie,192.168.0.60
#dhcp-host=judge
#dhcp-host=11:22:33:44:55:66,ignore
#dhcp-host=11:22:33:44:55:66,id:*
#dhcp-host=11:22:33:44:55:66,net:red
#dhcp-host=11:22:33:*:*:*,net:red
# Ignore any clients which are specified in dhcp-host lines
#dhcp-ignore=#known
#dhcp-vendorclass=red,Linux
#dhcp-userclass=red,accounts
#dhcp-mac=red,00:60:8C:*:*:*
# been given as --dhcp-host options. Useful if you keep
# run "dnsmasq --help dhcp" to get a list.
# any dhcp-options. If you use Windows clients and Samba, there
#dhcp-option=3,1.2.3.4
#dhcp-option=option:router,1.2.3.4
#dhcp-option=3
#dhcp-option=option:ntp-server,192.168.0.4,10.10.0.5
#dhcp-option=42,0.0.0.0
#dhcp-option=40,welly
#dhcp-option=23,50
#dhcp-option=27,1
#dhcp-option=128,e4:45:74:68:00:00
#dhcp-option=129,NIC=eepro100
# (see dhcp-range for the declaration of the "red" network)
#dhcp-option = net:red, option:ntp-server, 192.168.1.1
# for the ISC dhcpcd in
#dhcp-option=19,0           # option ip-forwarding off
#dhcp-option=44,0.0.0.0     # set netbios-over-TCP/IP nameserver(s) aka
    WINS server(s)
#dhcp-option=45,0.0.0.0     # netbios datagram distribution server
#dhcp-option=46,8           # netbios node type
#dhcp-option=option:domain-search,eng.apple.com,marketing.apple.com
#dhcp-option=121,192.168.1.0/24,1.2.3.4,10.0.0.0/8,5.6.7.8
#dhcp-option=vendor:PXEClient,1,0.0.0.0
#dhcp-option=vendor:MSFT,2,1i
#dhcp-option=vendor:Etherboot,60,"Etherboot"
# to use dhcp-option-force here.
#dhcp-option-force=208,f1:00:74:7e
#dhcp-option-force=209,configs/common
#dhcp-option-force=210,/tftpboot/pxelinux/files/
#dhcp-option-force=211,30i
#dhcp-boot=pxelinux.0
# load. The dhcp-match sets the gpxe tag for requests from gPXE.
#dhcp-match=gpxe,175 # gPXE sends a 175 option.
#dhcp-boot=net:#gpxe,undionly.kpxe
#dhcp-boot=mybootimage
#dhcp-option=encap:175, 1, 5b         # priority code
#dhcp-option=encap:175, 176, 1b       # no-proxydhcp
```

```
#dhcp-option=encap:175, 177, string   # bus-id
#dhcp-option=encap:175, 189, 1b       # BIOS drive code
#dhcp-option=encap:175, 190, user     # iSCSI username
#dhcp-option=encap:175, 191, pass     # iSCSI password
#dhcp-match=peecees, option:client-arch, 0 #x86-32
#dhcp-match=itanics, option:client-arch, 2 #IA64
#dhcp-match=hammers, option:client-arch, 6 #x86-64
#dhcp-match=mactels, option:client-arch, 7 #EFI x86-64
# alternative to dhcp-boot.
#dhcp-boot=net:red,pxelinux.red-net
# An example of dhcp-boot with an external TFTP server: the name and IP
#dhcp-boot=/var/ftpd/pxelinux.0,boothost,192.168.0.3
#dhcp-lease-max=150
#dhcp-leasefile=/var/lib/dnsmasq/dnsmasq.leases
# http://www.isc.org/index.pl?/sw/dhcp/authoritative.php
#dhcp-authoritative
#dhcp-script=/bin/echo
#log-dhcp
```

Chapter 13

SAMBA

13.1 SAMBA 簡介

1. SAMBA 是實現 Linux 與 Windows 中 SMB (Server Message Block) 協定連結的自由軟體。
2. SAMBA 可以作到的功能，其中常見的有：
   (a) 將目錄分享給 unix linux 或 winows。
   (b) 共享印表機。
   (c) 提供 windows 帳號認證。

13.2 SAMBA 架設

1. 安裝 samba 套件

```
[root@kvm8 ~]# yum install samba
```

2. 編輯設定檔

```
[root@kvm8 ~]# vim /etc/samba/smb.conf
[global]
....
    workgroup = DEYUGROUP                # windows 工作群組
    server string = dywang Samba Server # 描述 samba server
....

[common]
    comment=common share dir
    path=/public
```

```
    browseable=yes
    hosts allow=192.168.122.
    valid users = deyu1 deyu2
    public = no
    writable = yes
    create mask = 0765
# 分享的名字
    # 分享的註解
    # 分享的目錄
    # 分享目錄可瀏覽
    # 只分享給網域 192/168.122.0/24
    # 允許 deyu1 deyu2 讀寫目錄
    # 不公開
    # 可寫入
    # 產生檔案及目錄之預設遮
```

3. 啓動 smb 服務

```
[root@kvm8 ~]# /etc/init.d/smb restart
```

4. 設定開機啓動 smb 服務

```
[root@kvm8 ~]# chkconfig smb on
```

13.3 安全機制

1. 查詢 smbd ports

```
[root@kvm8 ~]# netstat -tlunp | grep smb
tcp     0     0     :::139       :::*      LISTEN      1727/smbd
tcp     0     0     :::445       :::*      LISTEN      1727/smbd
```

2. 防火牆設定

```
[root@kvm8 ~]# vim /etc/sysconfig/iptables
#########################################################
-A INPUT -m state --state NEW -m tcp -p tcp --dport 139 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 445 -j ACCEPT
#########################################################
```

3. 防火牆重新啓動

```
[root@kvm8 ~]# /etc/init.d/iptables restart
```

4. 開機啓動防火牆

```
[root@kvm8 ~]# chkconfig iptables on
```

5. 查詢 samba 相關的 selinux types

```
[root@kvm8 ~]# seinfo -t | grep samba
   samba_secrets_t
   samba_unconfined_script_exec_t
   samba_net_t
   samba_var_t
   samba_net_exec_t
   samba_net_tmp_t
   samba_unconfined_net_t
   samba_unconfined_script_t
   sambagui_exec_t
   samba_share_t
   samba_initrc_exec_t
   sambagui_t
   samba_etc_t
   samba_log_t
```

6. 設定分享目錄的 selinux type

```
[root@kvm8 ~]# chcon -R -t samba_share_t /public
[root@kvm8 ~]# ls -ldZ /public
drwxr-xr-x. root root unconfined_u:object_r:samba_share_t:s0 /public
```

7. selinux boolean 值

```
[root@kvm8 ~]# getsebool -a | grep smb
allow_smbd_anon_write --> off
[root@kvm8 ~]# 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_run_unconfined --> off
```

```
samba_share_fusefs --> off
samba_share_nfs --> off
use_samba_home_dirs --> off
virt_use_samba --> off
```

8. 設定 selinux boolean

```
[root@kvm8 ~]# setsebool -P samba_export_all_ro on
```

13.4 SAMBA 程式

1. testparm

```
## testparm <options> <filename> <hostname IP_address>

[root@kvm8 ~]# testparm /etc/samba/smb.conf kvm8.deyu.wang
    192.168.122.0/24
Load smb config files from /etc/samba/smb.conf
rlimit_max: increasing rlimit_max (1024) to minimum Windows limit
    (16384)
Processing section "[homes]"
Processing section "[printers]"
Processing section "[common]"
Loaded services file OK.
Server role: ROLE_STANDALONE
Allow connection from kvm8.deyu.wang (192.168.122.0/24) to homes
Allow connection from kvm8.deyu.wang (192.168.122.0/24) to printers
Allow connection from kvm8.deyu.wang (192.168.122.0/24) to common
```

2. smbstatus

```
[root@kvm8 ~]# smbstatus

Samba version 3.5.10-114.el6
PID     Username      Group         Machine
-------------------------------------------------------------------

Service      pid     machine       Connected at
-------------------------------------------------------

No locked files
```

3. pdbedit

```
[root@kvm8 ~]# pdbedit -a deyu1   ## 增加 samba 用户
new password:
retype new password:
Unix username:        deyu1
NT username:
Account Flags:        [U          ]
User SID:             S-1-5-21-3613796732-4223311700-2368206848-1000
Primary Group SID:    S-1-5-21-3613796732-4223311700-2368206848-513
Full Name:
Home Directory:       \\kvm8\deyu1
HomeDir Drive:
Logon Script:
Profile Path:         \\kvm8\deyu1\profile
Domain:               KVM8
Account desc:
Workstations:
Munged dial:
Logon time:           0
Logoff time:          Wed, 06 Feb 2036 23:06:39 CST
Kickoff time:         Wed, 06 Feb 2036 23:06:39 CST
Password last set:    Fri, 09 Aug 2013 23:44:29 CST
Password can change:  Fri, 09 Aug 2013 23:44:29 CST
Password must change: never
Last bad password   : 0
Bad password count  : 0
Logon hours         : FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF

[root@kvm8 ~]# pdbedit -v -L deyu1  ## 列出用户詳細資料
Unix username:        deyu1
NT username:
Account Flags:        [U          ]
User SID:             S-1-5-21-3613796732-4223311700-2368206848-1000
Primary Group SID:    S-1-5-21-3613796732-4223311700-2368206848-513
Full Name:
Home Directory:       \\kvm8\deyu1
HomeDir Drive:
Logon Script:
Profile Path:         \\kvm8\deyu1\profile
Domain:               KVM8
Account desc:
Workstations:
Munged dial:
Logon time:           0
Logoff time:          Wed, 06 Feb 2036 23:06:39 CST
Kickoff time:         Wed, 06 Feb 2036 23:06:39 CST
Password last set:    Fri, 09 Aug 2013 23:44:29 CST
Password can change:  Fri, 09 Aug 2013 23:44:29 CST
Password must change: never
Last bad password   : 0
Bad password count  : 0
Logon hours         : FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF

```

```
[root@kvm8 ~]# pdbedit -L deyu1
deyu1:500:

[root@kvm8 ~]# pdbedit -a deyu2
new password:
retype new password:
Unix username:        deyu2
NT username:
Account Flags:        [U          ]
User SID:             S-1-5-21-3613796732-4223311700-2368206848-1001
Primary Group SID:    S-1-5-21-3613796732-4223311700-2368206848-513
Full Name:
Home Directory:       \\kvm8\deyu2
HomeDir Drive:
Logon Script:
Profile Path:         \\kvm8\deyu2\profile
Domain:               KVM8
Account desc:
Workstations:
Munged dial:
Logon time:           0
Logoff time:          Wed, 06 Feb 2036 23:06:39 CST
Kickoff time:         Wed, 06 Feb 2036 23:06:39 CST
Password last set:    Fri, 09 Aug 2013 23:48:06 CST
Password can change:  Fri, 09 Aug 2013 23:48:06 CST
Password must change: never
Last bad password   : 0
Bad password count  : 0
Logon hours         : FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF

[root@kvm8 ~]# pdbedit -L        ## 列出用户
deyu1:500:
deyu2:501:
[root@kvm8 ~]# pdbedit -x deyu2  ## 删除用户 deyu2
[root@kvm8 ~]# pdbedit -L        ## 再列出用户
deyu1:500:
```

4. smbpasswd

```
## smbpasswd [options] [username]
[root@kvm8 ~]# smbpasswd deyu1
New SMB password:
Retype new SMB password:
```

5. smbclient

```
## smbclient <//server/share> <options>
[root@kvm8 ~]# touch /public/aaa
[root@kvm8 ~]# smbclient //kvm8.deyu.wang/common -U deyu1
```

```
4 Enter deyu1's password:
  Domain=[DEYUGROUP] OS=[Unix] Server=[Samba 3.5.10-114.el6]
6 smb: \> dir
    .                           D        0  Sat Aug 10 00:03:50 2013
8   ..                          DR       0  Fri Aug  9 23:26:43 2013
    aaa                                  0  Sat Aug 10 00:03:50 2013
10
          34646 blocks of size 32768. 6716 blocks available
12 smb: \> exit
```

Chapter 14

ISCSI

14.1 ISCSI 簡介

1. iSCSI (Internet Small Computer System Interface)
2. 將只用於本機的 SCSI 協定透過 TCP/IP 網路傳送，因而可作爲遠端硬碟；
3. 連接的伺服器數量無限（原來的 SCSI-3 的上限是 15）；
4. 原分散在各伺服器的儲存裝置，可統一到 ISCSI 的伺服器上。

14.2 ISCSI server 架設

1. 安裝套件

```
[root@dyH ~]# yum install scsi-target-utils
```

2. 產生 file-based images

```
## 產生 images 存放目錄
[root@dyH ~]# mkdir /srv/iscsi/
## 產生 images
[root@deH ~]# dd if=/dev/zero of=/srv/iscsi/disk.img bs=1M count=50
50+0 records in
50+0 records out
52428800 bytes (52 MB) copied, 0.0319766 s, 1.6 GB/s
```

3. 設定 SELinux file contexts

```
[root@dyH ~]# chcon -Rv -t tgtd_var_lib_t /srv/iscsi/
changing security context of `/srv/iscsi/disk.img'
changing security context of `/srv/iscsi/'
```

4. 啓動 tgtd 服務

```
[root@dyH ~]# /etc/init.d/tgtd restart
```

5. 設定開機啓動 tgtd 服務

```
[root@dyH ~]# chkconfig tgtd on
```

6. 確認 targets

```
[root@dyH ~]# tgt-admin --show
Target 1: iqn.2012-05.wang.deyu:deyudisk
    System information:
        Driver: iscsi
        State: ready
    I_T nexus information:
    LUN information:
        LUN: 0
            Type: controller
            SCSI ID: IET     00010000
            SCSI SN: beaf10
            Size: 0 MB, Block size: 1
            Online: Yes
            Removable media: No
            Readonly: No
            Backing store type: null
            Backing store path: None
            Backing store flags:
        LUN: 1
            Type: disk
            SCSI ID: IET     00010001
            SCSI SN: beaf11
            Size: 52 MB, Block size: 512
            Online: Yes
            Removable media: No
            Readonly: No
            Backing store type: rdwr
            Backing store path: /srv/iscsi/disk.img
            Backing store flags:
    Account information:
    ACL information:
        192.168.122.0/24
```

14.3 安全機制

1. 查詢 tgtd ports

```
[root@dyH ~]# netstat -tlunp | grep tgtd
tcp      0      0 0.0.0.0:3260        0.0.0.0:*       LISTEN      4630/
   tgtd
tcp      0      0 :::3260             :::*            LISTEN      4630/
   tgtd
```

2. 防火牆設定

```
[root@dyH ~]# vim /etc/sysconfig/iptables
#########################################################
-A INPUT -m state --state NEW -m tcp -p tcp --dport 3260 -j ACCEPT
#########################################################
```

3. 防火牆重新啓動

```
[root@dyH ~]# /etc/init.d/iptables restart
```

4. 開機啓動防火牆

```
[root@dyH ~]# chkconfig iptables on
```

14.4 Client 端測試

1. 遠端測試 iscsi 硬碟是否存在？

```
[root@kvm8 ~]# iscsiadm -m discovery -t sendtargets -p deyu.wang:3260
Starting iscsid:                                           [  OK  ]
192.168.122.1:3260,1 iqn.2012-05.wang.deyu:deyudisk
```

2. 遠端以 debug level 2 連上 iscsi

```
[root@kvm8 ~]# iscsiadm -d2 -m node --login
iscsiadm: Max file limits 1024 1024

iscsiadm: default: Creating session 1/1
Logging in to [iface: default, target: iqn.2012-05.wang.deyu:deyudisk,
    portal: 192.168.122.1,3260] (multiple)
Login to [iface: default, target: iqn.2012-05.wang.deyu:deyudisk, portal
    : 192.168.122.1,3260] successful.
```

3. 連上後可以看到 /dev/sda，視爲一顆新的硬碟使用。

```
[root@kvm8 ~]# ll /dev/sda
brw-rw----. 1 root disk 8, 0 Aug 10 01:17 /dev/sda
```

4. 遠端以 debug level 2 解開 iscsi

```
[root@kvm8 ~]# iscsiadm -d2 -m node --logout
iscsiadm: Max file limits 1024 1024

Logging out of session [sid: 1, target: iqn.2012-05.wang.deyu:deyudisk,
    portal: 192.168.122.1,3260]
Logout of [sid: 1, target: iqn.2012-05.wang.deyu:deyudisk, portal:
    192.168.122.1,3260] successful.
```

5. 解開後 /dev/sda 不見了。

```
[root@kvm8 ~]# ll /dev/sda
ls: cannot access /dev/sda: No such file or directory
```

Chapter 15

NTP

15.1 NTP 簡介

1. Network Time Protocol, NTP
2. 網路時間校時。
3. 可只做 Client，連上遠端 NTP Server，進行時間同步，亦可提供 server 服務遠端主機進行時間同步。

15.2 ntpdate 手動校時

1. 安裝 ntpdate 套件

```
[root@kvm8 ~]# yum install ntpdate
```

2. 手動調校系統時間

```
[root@kvm8 ~]# ntpdate tock.stdtime.gov.tw
18 Jul 10:40:24 ntpdate[3334]: the NTP socket is in use, exiting
[root@kvm8 ~]# /etc/init.d/ntpd stop
Shutting down ntpd:                                        [  OK  ]
[root@kvm8 ~]# ntpdate tock.stdtime.gov.tw
18 Jul 10:40:37 ntpdate[3341]: step time server 220.130.158.71 offset
    1.909398 sec
```

3. 在 ntp 服務已啓動下，手動調校系統時間，會顯示 NTP socket 使用中，退出 ntpdate。

```
[root@kvm8 ~]# ntpdate tock.stdtime.gov.tw
30 Apr 12:01:50 ntpdate[1692]: the NTP socket is in use, exiting
```

4. 在 ntp 服務已啓動下，手動調校系統時間，ntpdate 加上 -u 選項，開啓其他 port 校時。

```
[root@kvm8 ~]# ntpdate -u tock.stdtime.gov.tw
30 Apr 12:03:47 ntpdate[1694]: adjust time server 211.22.103.157 offset
    -0.000160 sec
```

5. 調整 BIOS 時間

```
[root@deyu ~]# hwclock [-rw]
選項與參數：
-r ：亦即 read ，讀出目前 BIOS 內的時間參數；
-w ：亦即 write ，將目前的 Linux 系統時間寫入 BIOS 中。

[root@kvm8 ~]# hwclock -w; hwclock -r; date
Mon 18 Jul 2011 10:42:26 AM CST  -0.323154 seconds
Mon Jul 18 10:42:25 CST 2011
```

15.3 NTP 架設

1. 安裝 ntp 套件

```
[root@kvm8 ~]# yum install ntp
```

2. NTP 伺服器設定檔 ntp.conf

```
[root@kvm8 ~]# vim /etc/ntp.conf
```

(a) ntpd 自動計算自己主機的頻率與上層 Time server 的頻率誤差，並將其記錄在 driftfile 後面接的檔名中。

```
[root@kvm8 ~]# vim /etc/ntp.conf
driftfile /var/lib/ntp/drift
# /var/lib/ntp/drift 必須使用完整路徑檔名；
# /var/lib/ntp/drift 不能是連結檔；
# /var/lib/ntp/drift 需要設定成 ntpd daemon 可以寫入的權限。
# /var/lib/ntp/drift 記錄的數值單位爲：百萬分之一秒 (ppm)。
```

(b) restrict 做權限管理，格式如下：

```
# restrict default [flag][...]
# restrict source [flag][...]
# restrict address [mask mask] [flag][...]
#
restrict default kod nomodify notrap nopeer noquery
restrict -6 default kod nomodify notrap nopeer noquery
restrict 127.0.0.1
restrict -6 ::1
```

(c) restrict 參數說明：

i. default: address 0.0.0.0, mask 0.0.0.0

ii. -6：DNS resolution to the IPv6 namespace

iii. flag 說明：

A. kod：當要求 server 的服務超過限制，server 不是直接丟棄服務要求，而是傳送 kiss-o'-death (KoD) packet，讓 client 轉向要求其他 server 服務，或等一段時間再要求 server 服務。

B. nomodify：用户端不能更改 NTP 伺服器的時間參數。

C. notrap：不提供 trap 這個遠端事件登錄 (remote event logging) 的功能。

D. nopeer：避免其他人使用此 ntpd 作爲 time server

E. noquery：用户端不能夠使用 ntpq, ntpc 等指令來查詢時間伺服器。

iv. 開放 192.168.122.0/24 區段網路查詢 ntp server

```
restrict 192.168.122.0 mask 255.255.255.0 nomodify notrap
```

(d) 指定遠端 ntp server 進行時間同步：perfer 表示『優先使用』的主機。

```
## server 格式
# server address [options ...]
server  tock.stdtime.gov.tw prefer
server  csie.cyut.edu.tw
server  tock.stdtime.gov.tw
server  watch.stdtime.gov.tw
server  time.stdtime.gov.tw
server  clock.stdtime.gov.tw
server  tick.stdtime.gov.tw
```

(e) 如果外部 time server 無法連線或層級 (stratum)10 以上，則以本機時鐘爲系統時間。

```
#server 127.127.1.0 # local clock
#fudge  127.127.1.0 stratum 10
```

3. 編輯 /etc/sysconfig/ntpd ，設定 BIOS 的時間也同步調整。

```
[root@kvm8 ~]# vim /etc/sysconfig/ntpd
# Drop root to id 'ntp:ntp' by default.
OPTIONS="-u ntp:ntp -p /var/run/ntpd.pid -g"
SYNC_HWCLOCK=yes
```

4. 啓動 NTP 服務

```
[root@kvm8 ~]# /etc/init.d/ntpd start
Starting ntpd:                                             [  OK  ]
```

5. 觀察 NTP 服務的 port 123

```
[root@kvm8 ~]# netstat -tlunp | grep 123
udp        0      0 192.168.0.250:123           0.0.0.0:*     3224/ntpd
udp        0      0 127.0.0.1:123               0.0.0.0:*     3224/ntpd
udp        0      0 0.0.0.0:123                 0.0.0.0:*     3224/ntpd
udp        0      0 ::1:123                     :::*          3224/ntpd
udp        0      0 fe80::5054:ff:fe00:fa:123   :::*          3224/ntpd
udp        0      0 :::123                      :::*          3224/ntpd
```

6. 設定開機啓動 ntpd

```
[root@kvm8 ~]# chkconfig ntpd on
```

7. 查詢開機是否啓動 ntpd

```
[root@kvm8 ~]# chkconfig --list ntpd
ntpd            0:off   1:off   2:on    3:on    4:on    5:on    6:off
```

8. 查詢 ntpd 校正的 servers

```
[root@kvm8 ~]# ntpq -p
     remote           refid      st t when poll reach   delay   offset
        jitter
==============================================================================

 deyu.wang       59.124.29.241    3 u   43   64    1    0.089   -0.209
       0.000
 220-135-58-124. 62.161.56.158    2 u   42   64    1   19.813    4.752
       0.000
 todaycolor.com. 211.22.103.158   4 u   41   64    1   21.004   -4.379
       0.000
 alqualonde.org  133.243.238.243  2 u   41   64    1   22.520   -9.578
       0.000
```

9. 確認 NTP 伺服器是否順利更新時間？

```
[root@kvm8 ~]# ntpstat -p
unsynchronised
  time server re-starting
   polling server every 64 s
## 幾分鐘後再觀察
[root@kvm8 ~]# ntpstat -pn
synchronised to NTP server (59.124.196.83) at stratum 3
   time correct to within 782 ms
   polling server every 64 s
```

15.4 圖形界面網路校時設定

1. 使用圖形界面做網路校時

   (a) 進入 X window，依照『開始』→『系統』→『管理』→『日期與時間』打開設定軟體；

   (b) 選擇網路時間協定 (Network Time Protocol)；

   (c) 按下『Enable Network Time Protocol』；

   (d) 輸入 tock.stdtime.gov.tw；

   (e) 按下 OK！

15.5 安全機制

1. NTP Ports: UDP 123

2. 防火牆設定

```
[root@kvm8 ~]# vim /etc/sysconfig/iptables
#########################################################
-A INPUT -p UDP -s 192.168.122.0/24  --dport 123 -j ACCEPT
#########################################################
```

3. 防火牆重新啓動

```
[root@kvm8 ~]# /etc/init.d/iptables restart
```

4. 開機啓動防火牆

```
[root@kvm8 ~]# chkconfig iptables on
```

Chapter 16

Squid Proxy

16.1 Squid 簡介

1. Squid 是 HTTP 「快取伺服器」（Cache Proxy Server）。
2. Proxy 種類：
   (a) 一般 Proxy Server：放在瀏覽器客户端前面代取資料用的，這也是最常見的應用方式。
   (b) 反向 Proxy Server：放在網頁伺服器前面，通常是當網站網頁需求量超大時，放在 Web Server 前端用以節省 Web Server 資源的架設方式。
   (c) 穿透式 Proxy Server 搭配 NAT（Network Address Translation）就是所謂的穿透式（Transparent）Proxy Server，優點是可以減少瀏覽器客户端逐一設定的繁瑣工作，這也是 Linux 常見綜合應用之一（NAT + Proxy）。
3. 本例子中學校 163.17.3.148 已架設 moodle，但只限校內 ip 存取，外部網路若要使用此 moodle，唯有透過校內架設的 proxy。爲在外部網路（在家）使用，在校內主機 163.17.27.219 架設 proxy，設定只有家裡 ip 1.168.209.95 可以使用此 proxy。
4. Squid 是一個 WEB proxy，只能進行 HTTP 存取，對於 Adobe 使用串流的 RTMP 協定無法適用。
5. Openmeeting 使用 rtmp 協定，無法利用此 proxy 開啓。

16.2 Squid 架設

1. 安裝 squid 套件。

```
[root@dyw219 ~]# yum install -y squid
```

2. 編輯 /etc/squid/squid.conf 設定檔：安裝好 squid 此設定檔即已有基本設定，以下僅做一小修改並說明。

```
[root@dyw219 ~]# cat /etc/squid/squid.conf
```

3. 定義 manager 爲管理功能，localhost 爲本機，可以連線到本機的 ip 等。

```
#
# Recommended minimum configuration:
#
acl manager proto cache_object
acl localhost src 127.0.0.1/32 ::1
acl to_localhost dst 127.0.0.0/8 0.0.0.0/32 ::1
```

4. 定義可以存取此 proxy 的 ip，除預設的內網，名稱設爲 localnet 外，此例中加入一名爲 externat 的外網，其 ip 只有 1.168.209.95。

```
# Example rule allowing access from your local networks.
# Adapt to list your (internal) IP networks from where browsing
# should be allowed
acl externat src 1.168.209.95
acl localnet src 10.0.0.0/8 # RFC1918 possible internal network
acl localnet src 172.16.0.0/12  # RFC1918 possible internal network
acl localnet src 192.168.0.0/16 # RFC1918 possible internal network
acl localnet src fc00::/7       # RFC 4193 local private network range
acl localnet src fe80::/10      # RFC 4291 link-local (directly plugged)
    machines
```

5. 定義可以取得資料的 ports。

```
acl SSL_ports port 443
acl Safe_ports port 80      # http
acl Safe_ports port 21      # ftp
acl Safe_ports port 443     # https
acl Safe_ports port 70      # gopher
acl Safe_ports port 210     # wais
acl Safe_ports port 1025-65535  # unregistered ports
acl Safe_ports port 280     # http-mgmt
acl Safe_ports port 488     # gss-http
acl Safe_ports port 591     # filemaker
```

```
acl Safe_ports port 777     # multiling http
acl CONNECT method CONNECT
```

6. 定義那些主機可以放行執行那些權限，與 iptables 防火牆一樣，必須依照順序判斷是否放行。例如：第一條允許 localhost 進行管理功能，第二條不允許管理。在這一段落除使用預設規則外，加了一條 http_access allow externat 允許剛剛定對的外部網路 externat 進行 http 存取。

```
#
# Recommended minimum Access Permission configuration:
#
# Only allow cachemgr access from localhost
http_access allow manager localhost
http_access deny manager

# Deny requests to certain unsafe ports
http_access deny !Safe_ports

# Deny CONNECT to other than secure SSL ports
http_access deny CONNECT !SSL_ports

# We strongly recommend the following be uncommented to protect innocent
# web applications running on the proxy server who think the only
# one who can access services on "localhost" is a local user
#http_access deny to_localhost

#
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
#

# Example rule allowing access from your local networks.
# Adapt localnet in the ACL section to list your (internal) IP networks
# from where browsing should be allowed
http_access allow localnet
http_access allow localhost
http_access allow externat

# And finally deny all other access to this proxy
http_access deny all
```

7. 定義 proxy 協定的 port。

```
# Squid normally listens to port 3128
http_port 3128
```

8. 用户端所需要的網址列有 cgi-bin，則不快取。

```
# We recommend you to use at least the following line.
hierarchy_stoplist cgi-bin ?
```

9. 預設使用 100M 的容量放置快取，若要修改可把註解拿掉。

```
# Uncomment and adjust the following to add a disk cache directory.
#cache_dir ufs /var/spool/squid 100 16 256
```

10. 定義 coredumps 的目錄。

```
# Leave coredumps in the first cache dir
coredump_dir /var/spool/squid
```

11. 快取存在時間相關設定。

```
# Add any of your own refresh_pattern entries above these.
refresh_pattern ^ftp:       1440    20% 10080
refresh_pattern ^gopher:    1440    0%  1440
refresh_pattern -i (/cgi-bin/|\?) 0 0%  0
refresh_pattern .       0   20% 4320
```

12. 啓動 squid 服務

```
[root@dyw219 ~]# /etc/init.d/squid start
Starting squid: .                                          [  OK  ]
```

13. 查看 squid 服務是否啓動。

```
[root@dyw219 ~]# netstat -tulnp | grep squid
tcp     0    0 :::3128               :::*            LISTEN      23254/(
    squid)
udp     0    0 0.0.0.0:36211         0.0.0.0:*                   23254/(
    squid)
udp     0    0 :::51734              :::*                        23254/(
    squid)
```

14. 設定開機啓動 squid 服務

```
[root@dyw219 ~]# chkconfig squid on
```

16.3 安全機制

1. 防火牆設定–任何網域皆可使用 squid。

```
[root@dyw219 ~]# vim /etc/sysconfig/iptables
################################################################
-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 3128 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
################################################################
```

2. 防火牆重新啓動

```
[root@kvm8 ~]# /etc/init.d/iptables restart
```

3. 開機啓動防火牆

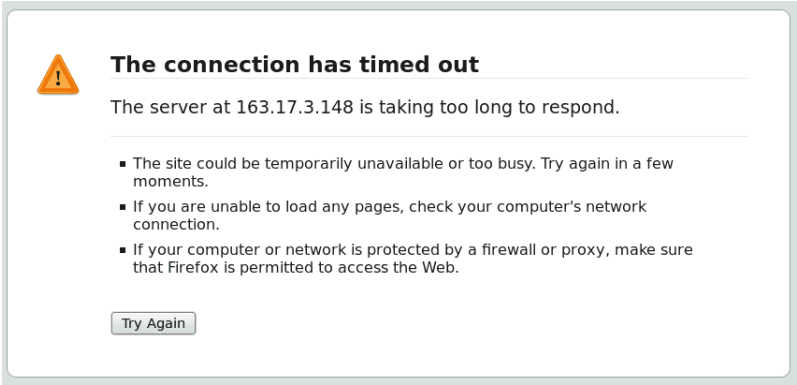
```
[root@kvm8 ~]# chkconfig iptables on
```

4. SELinux 有關 ssh 的設定

```
[root@dyw219 ~]# getsebool -a | grep squid
squid_connect_any --> on
squid_use_tproxy --> off
```

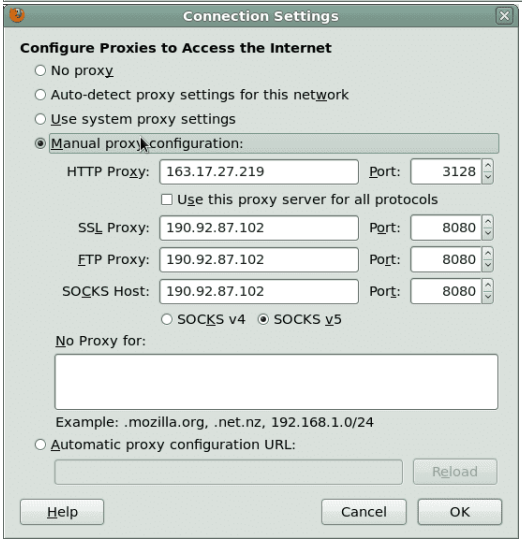
16.4 瀏覽器設定

1. firefox 沒使用 proxy，無法存取 moodle。



2. firefox 設定 proxy。





3. firefox 使用 proxy，已可存取 moodle。



16.5 Linux 命令列使用 Proxy

1. Linux 命令列要使用 proxy，必須設定環境變數，一般設定以下三個環境變數，就可提供 ftp, wget, curl, ssh, yum 等命令使用了。

```
http_proxy = http://yourproxyip:port/
https_proxy = http://yourproxyip:port/
ftp_proxy = http://yourproxyip:port/
```

2. 建立環境變數導出檔

```
[root@kvm7 ~]# vim myproxy
[root@kvm7 ~]# cat myproxy
export http_proxy="http://163.17.10.116:3128"
export https_proxy="https://163.17.10.116:3128"
export ftp_proxy="http://163.17.10.116:3128"
```

3. 建立環境變數清除檔

```
[root@kvm7 ~]# vim noproxy
[root@kvm7 ~]# cat noproxy
```

```
unset http_proxy
unset https_proxy
unset ftp_proxy
```

4. 使用 proxy 環境變數

```
[root@kvm7 ~]# . myproxy
[root@kvm7 ~]# echo $http_proxy
http://163.17.10.116:3128
```

5. 清除 proxy 環境變數

```
[root@kvm7 ~]# . noproxy
[root@kvm7 ~]# echo $http_proxy

[root@kvm7 ~]#
```

Chapter 17

XMPP 即時通訊伺服器 Openfire

17.1 XMPP 簡介

1. XMPP (Extensible Messaging and Presence Protocol) 協定，以前叫做 Jabber。
2. XMPP 是一種以 XML 爲基礎的開放式即時通訊協定。
3. XMPP 被 Google Talk 應用，任何 XMPP 客户端使用 Gmail 帳號登入後都連接到 Google Talk。
4. XMPP 協議是自由、開放、公開的，並且易於瞭解。而且在客户端、伺服器、元件、源碼庫等方面，都已經各自有多種實作。
5. XMPP 開放源碼套件：ejabberd, prosody, openfire。
6. OpenFire Server 在眾多免費開放原始碼的即時訊息伺服器軟體中號稱最容易安裝與設定，其實是因爲 openfire 提供網頁界面的設定。
7. OpenFire Server 安裝參考
8. Spark Client
9. SparkWeb Client
10. 個人認爲 prosody 安裝設定更簡單，只不過它沒有設計圖形或網頁型式的管理界面，會讓不熟文字命令的使用者以爲其比較複雜。
11. Prosody 主要設定檔只有一個 /etc/prosody/prosody.cfg.lua，可以直接以 vim 編輯，只要改一下設定再重新啓動，就可以用户自行註冊，功能完整且設定簡單。

12. prosody 可以擴充模組，在 SSL/TLS 加密，用户註冊、產生、匯入，通訊的資料儲不儲存，都可以簡單設定。因此個人還是偏好 prosody。

17.2 OPenfire 套件安裝與啓動

1. 安裝套件 openfire

```
[root@kvm8 ~]# yum install openfire
```

2. openfire 是 32 位元套件，在 64 位元的 Linux 系統上，必須加裝 glibc.i686 套件，否則無法啓動 openfire 且也要安裝 java。

```
1 [root@kvm8 ~]# yum install glibc.i686 java
```

3. 啓動 openfire 服務。

```
1 [root@kvm8 ~]# /etc/init.d/openfire start
  Starting openfire:
```

4. 設定開機自動啓動 openfire 服務。

```
  [root@kvm8 ~]# chkconfig openfire on
2 [root@kvm8 ~]# chkconfig --list openfire
  openfire        0:off   1:off   2:on    3:on    4:on    5:on    6:off
```

5. openfire 需要資料庫，此安裝使用 mysql。

```
1 [root@kvm8 ~]# yum -y install mysql-server
```

6. 啓動 mysqld 服務。

```
[root@kvm8 ~]# /etc/init.d/mysqld start
```

7. 設定開機自動啓動 mysqld 服務。

```
[root@kvm8 ~]# chkconfig mysqld on
[root@kvm8 ~]# chkconfig --list mysqld
mysqld          0:off   1:off   2:on    3:on    4:on    5:on    6:off
```

8. 開始 mysql 的安全設定。

```
[root@kvm8 ~]# mysql_secure_installation

NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MySQL
      SERVERS IN PRODUCTION USE!  PLEASE READ EACH STEP CAREFULLY!

In order to log into MySQL to secure it, we'll need the current
password for the root user.  If you've just installed MySQL, and
you haven't set the root password yet, the password will be blank,
so you should just press enter here.

Enter current password for root (enter for none):
OK, successfully used password, moving on...

Setting the root password ensures that nobody can log into the MySQL
root user without the proper authorisation.

Set root password? [Y/n] Y
New password:
Re-enter new password:
Password updated successfully!
Reloading privilege tables..
 ... Success!

By default, a MySQL installation has an anonymous user, allowing anyone
to log into MySQL without having to have a user account created for
them.  This is intended only for testing, and to make the installation
go a bit smoother.  You should remove them before moving into a
production environment.

Remove anonymous users? [Y/n] n
 ... skipping.

Normally, root should only be allowed to connect from 'localhost'.  This
ensures that someone cannot guess at the root password from the network.

```

```
Disallow root login remotely? [Y/n] n
 ... skipping.

By default, MySQL comes with a database named 'test' that anyone can
access.  This is also intended only for testing, and should be removed
before moving into a production environment.

Remove test database and access to it? [Y/n] n
 ... skipping.

Reloading the privilege tables will ensure that all changes made so far
will take effect immediately.

Reload privilege tables now? [Y/n] Y
 ... Success!

Cleaning up...

All done!  If you've completed all of the above steps, your MySQL
installation should now be secure.

Thanks for using MySQL!
```

9. 使用剛剛設定的 root 密碼登入 mysql。

```
[root@kvm8 ~]# mysql -uroot -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 9
Server version: 5.5.38 MySQL Community Server (GPL) by Remi

Copyright (c) 2000, 2014, Oracle and/or its affiliates. All rights
    reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input
    statement.

mysql>
```

10. 產生 openfire 資料庫。

```
mysql> create database openfire;
```

```
Query OK, 1 row affected (0.00 sec)
```

11. 建立用户 openfire，設定其密碼爲 123qwe。

```
mysql> insert into mysql.user (user,host,password) values('openfire','
    127.0.0.1',password('123qwe'));
Query OK, 1 row affected, 3 warnings (0.00 sec)
```

12. 設定用户 openfire 有完全的權限存取資料庫 openfire。

```
mysql> grant all privileges on openfire.* to openfire@127.0.0.1;Query OK
    , 0 rows affected (0.00 sec)
```

13. 更新權限設定。

```
mysql> flush privileges;
Query OK, 0 rows affected (0.00 sec)
```

14. 退出 mysql 資料庫管理。

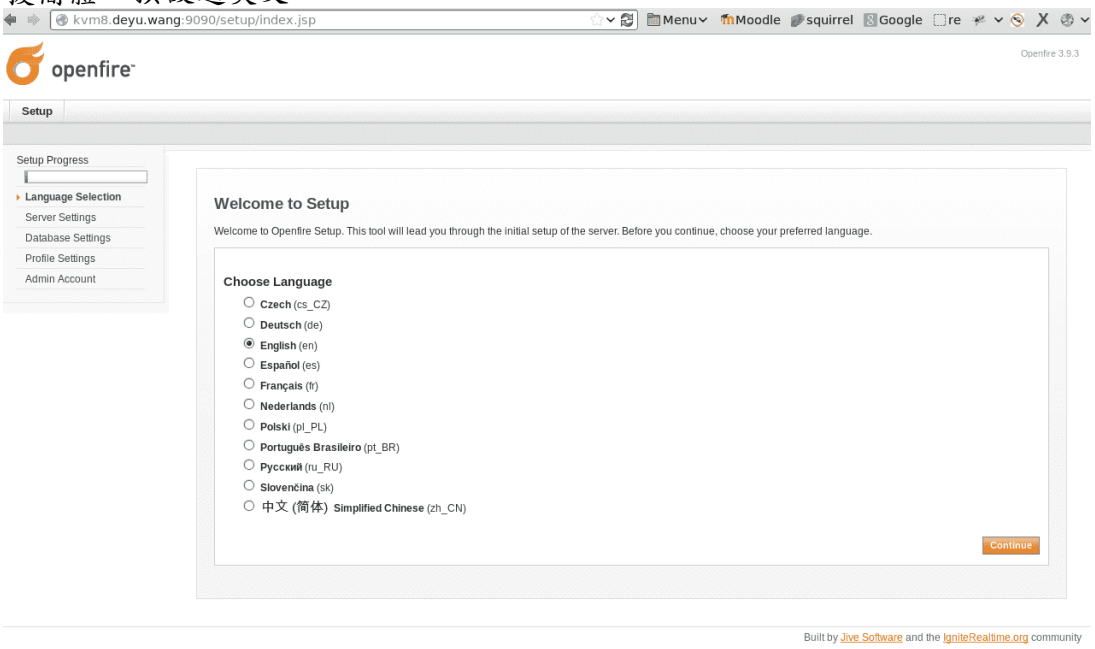
```
mysql> exit
Bye
```

17.3 使用網頁設定 Openfire

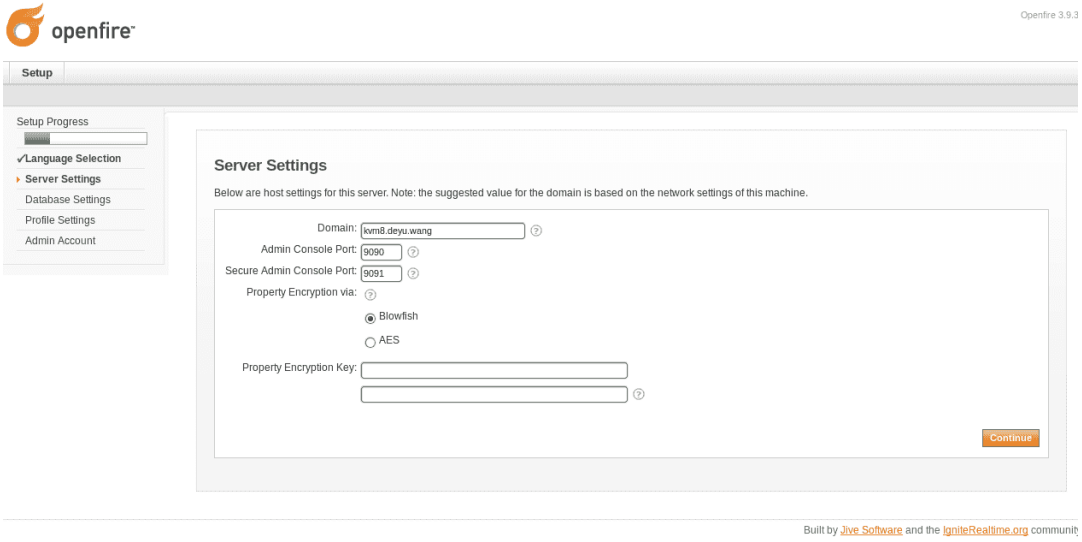
1. 要使用網頁設定 openfire，請先打開防火牆 9090 port。

```
[root@kvm8 ~]# iptables -I INPUT -p tcp -m state --state NEW \
-m tcp --dport 9090 -j ACCEPT
```

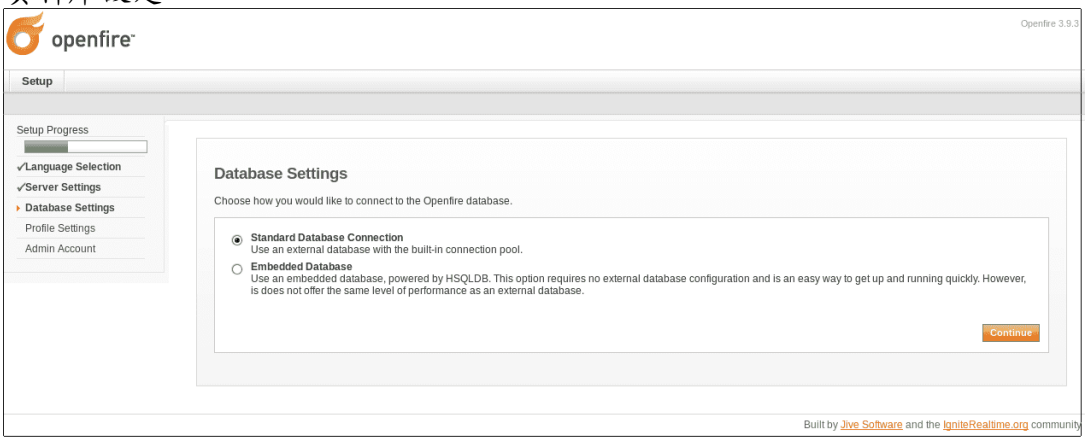
2. 打開瀏覽器輸入網址 http://kvm8.deyu.wang:9090，先設定語言，中文只支援簡體，預設選英文。



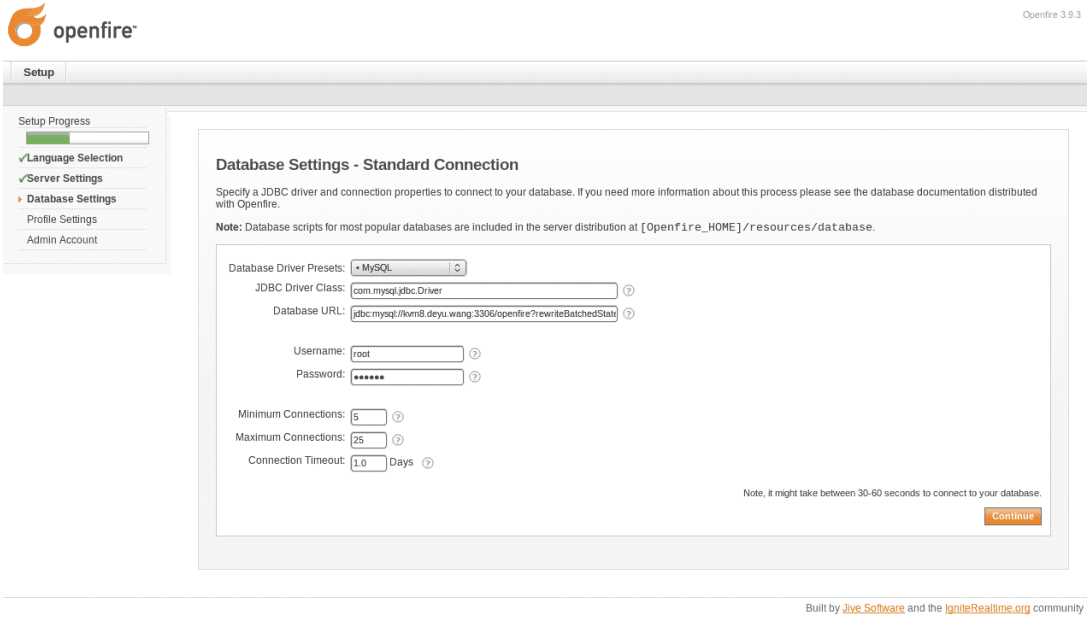
3. 設定伺服器管理網址及埠號。



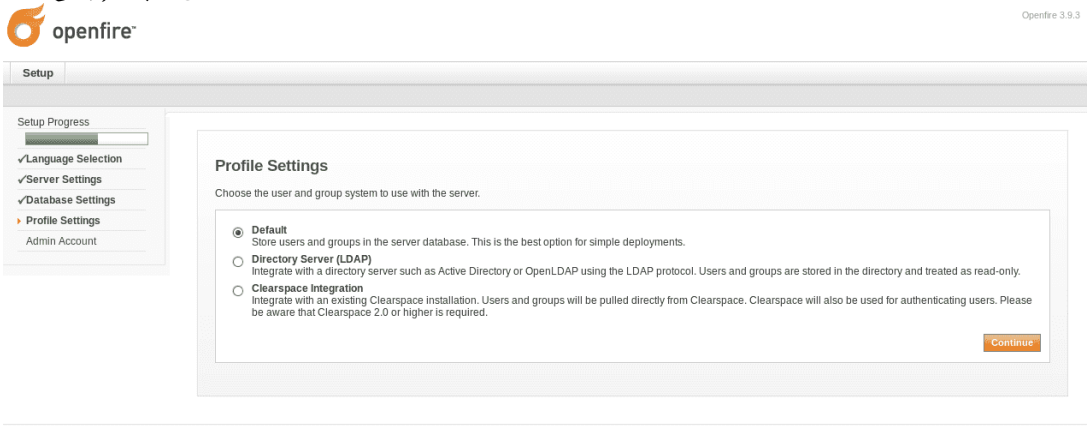
4. 資料庫設定。



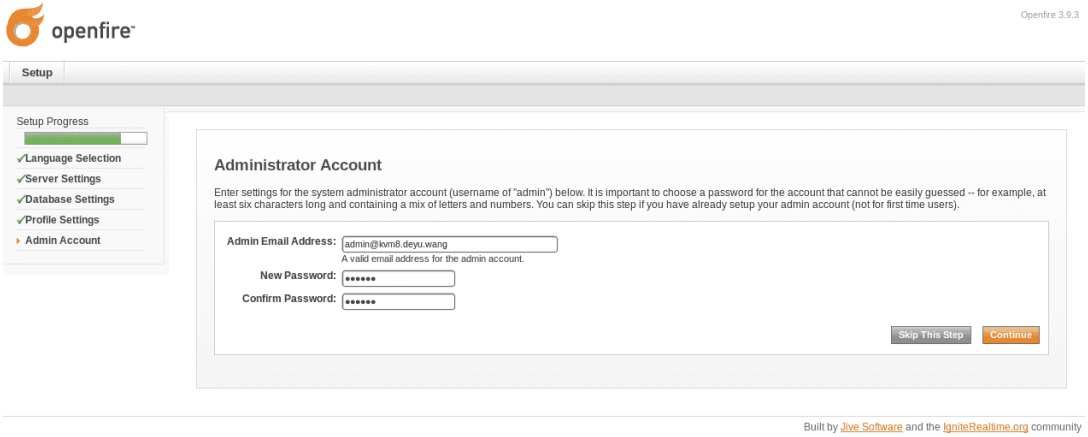
5. 資料庫設定之標準連線。



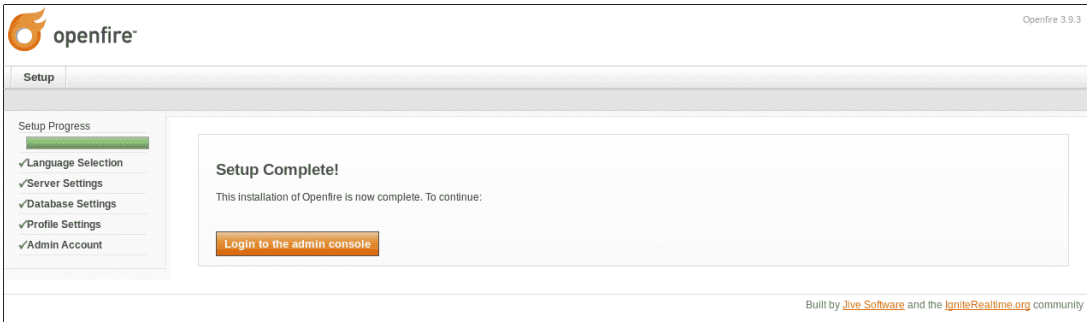
6. 設定用户系統。



7. 設定管理者帳號。

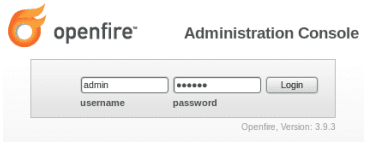


8. 完成設定畫面，按下管理者登入按鈕，可以進入系統管理界面。

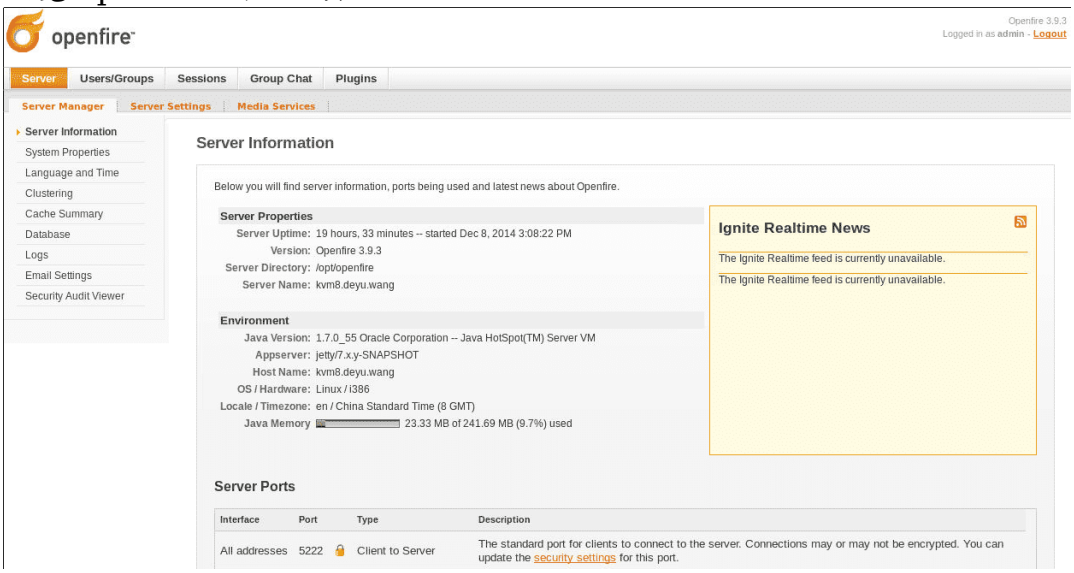


17.4 使用網頁管理 Openfire

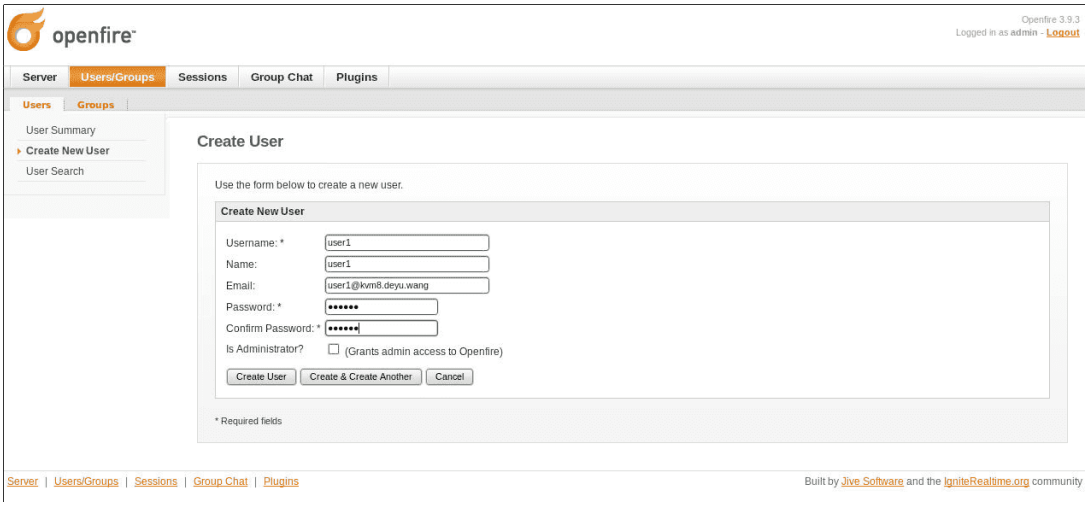
1. 打開瀏覽器輸入網址 http://kvm8.deyu.wang:9090，以管理者帳號 admin 登入 openfire。



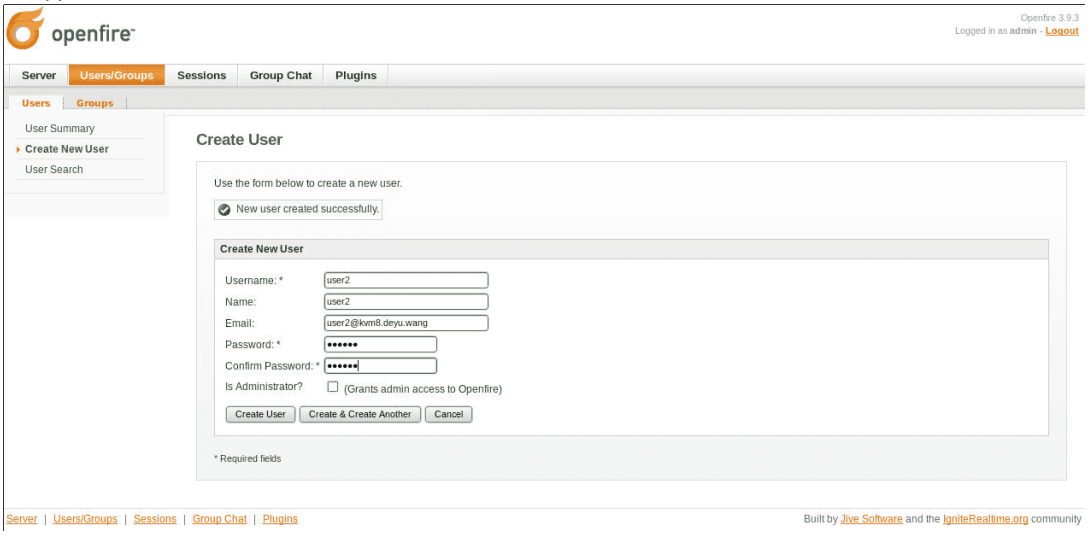
2. 瀏覽 openfire 伺服器資訊。



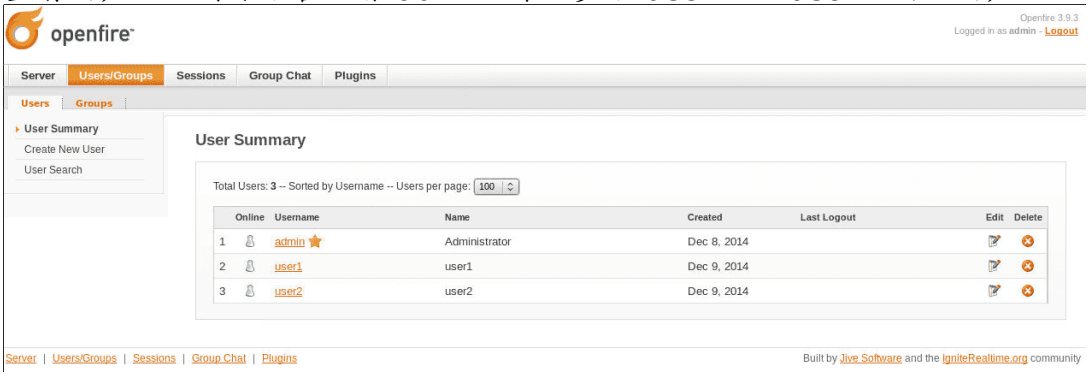
3. 產生用户 user1。



4. 繼續產生用户 user2。

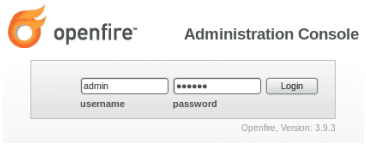


5. 查看用户，目前除了管理者 admin 外，多了 user1 及 user2 兩個用户。

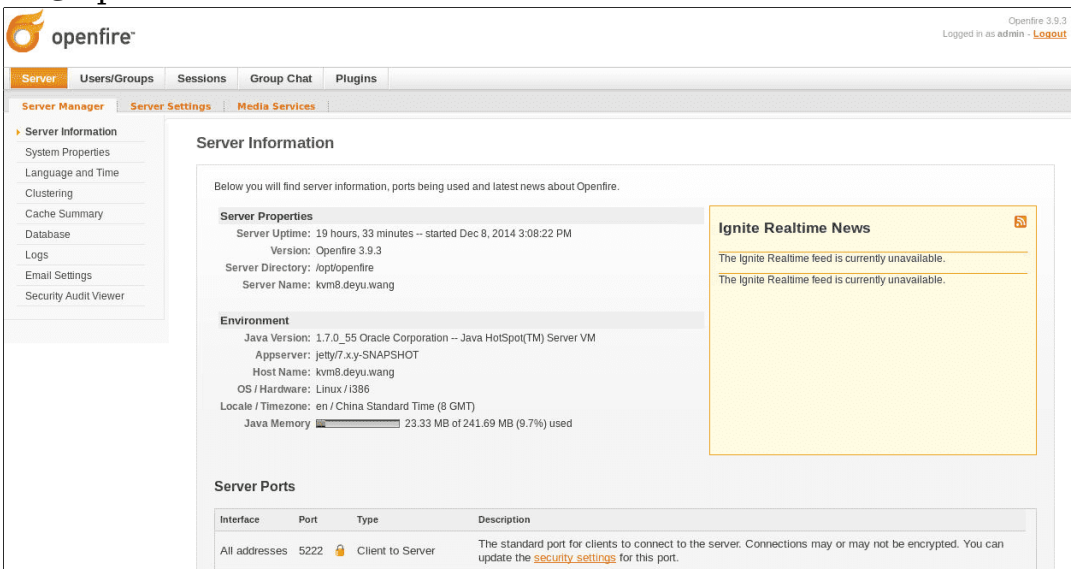


17.5 Linux 使用網頁管理 Openfire

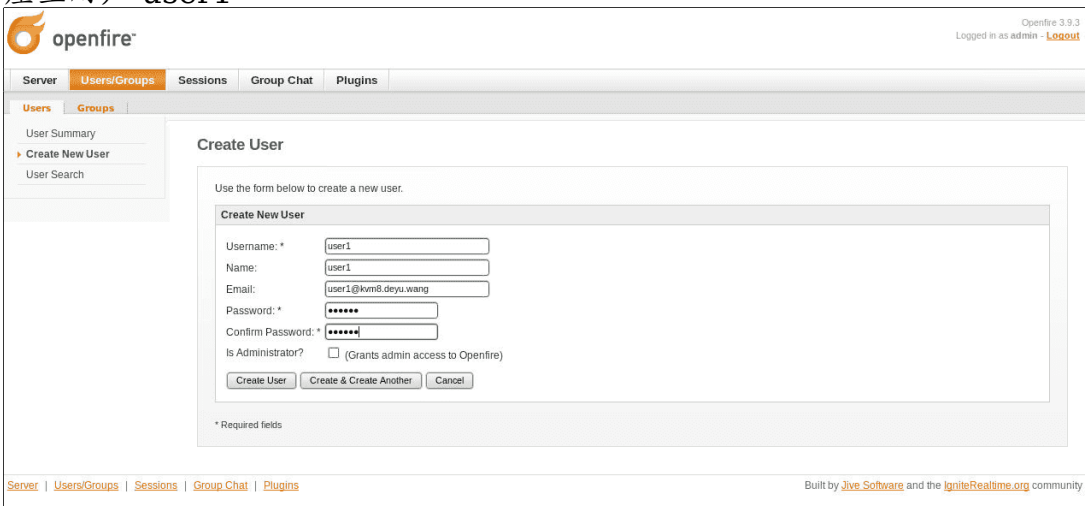
1. 打開瀏覽器輸入網址 http://kvm8.deyu.wang:9090，以管理者帳號 admin 登入 openfire。



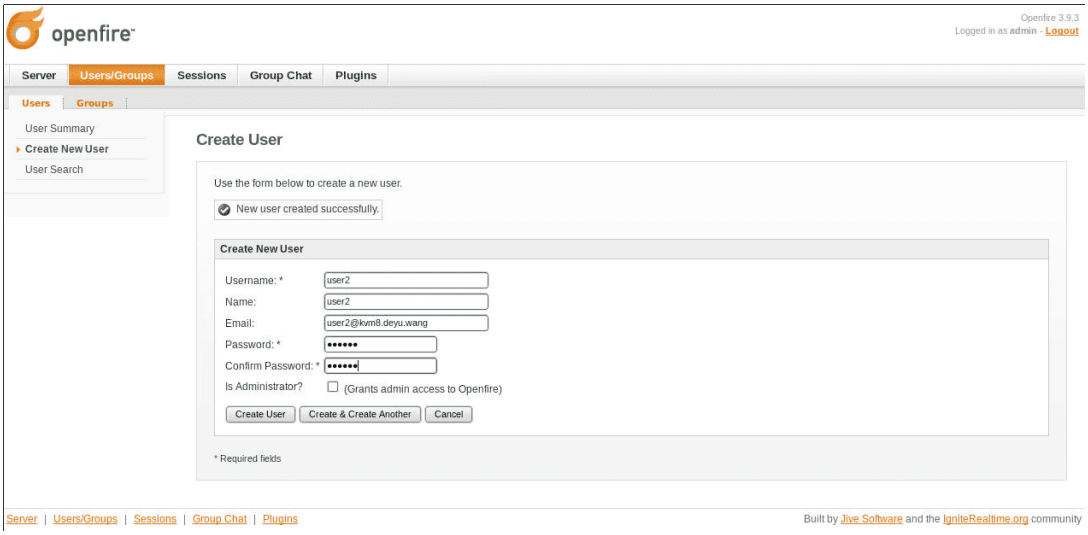
2. 瀏覽 openfire 伺服器資訊。



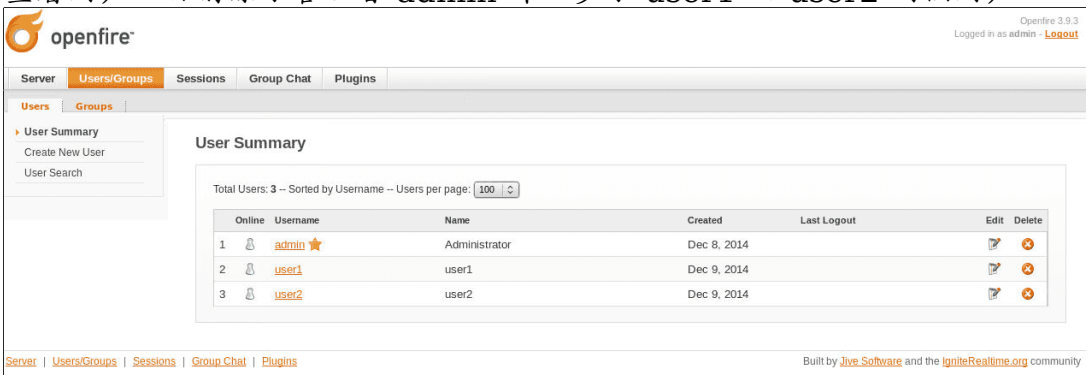
3. 產生用户 user1。



4. 繼續產生用户 user2。



5. 查看用户，目前除了管理者 admin 外，多了 user1 及 user2 兩個用户。

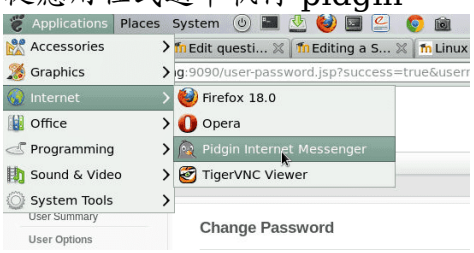


17.6 Openfire Client – Pidgin for Linux

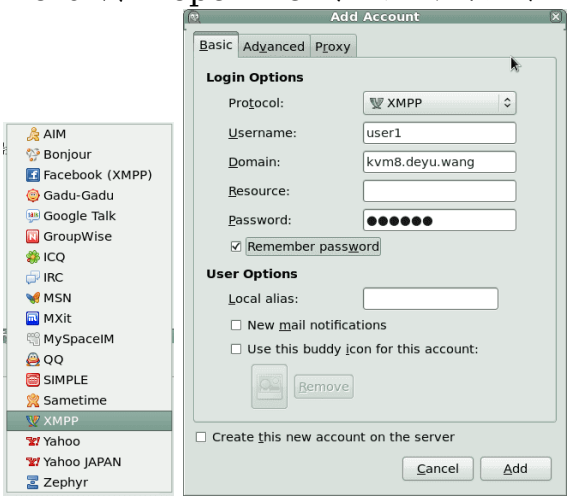
1. XMPP clients 有很多的選擇，openfire 官網提供 spark 可供下載，但只有 i386 的 rpm 版本，對於目前大都使用 x86_64 版本的 Linux 系統，安裝上需要另外安裝相依的 i686 套件，並不方便。Pidgin 是一套即時通訊用户端軟體，支援多種協定，DYW Linux 可直接 yum install pidgin 安裝。

```
[root@dywhd2 ~]# yum install pidgin
```

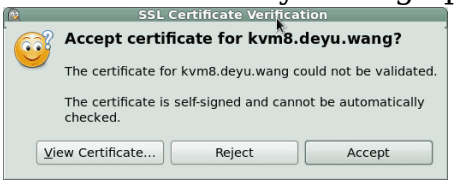
2. 從應用程式選單執行 pidgin。



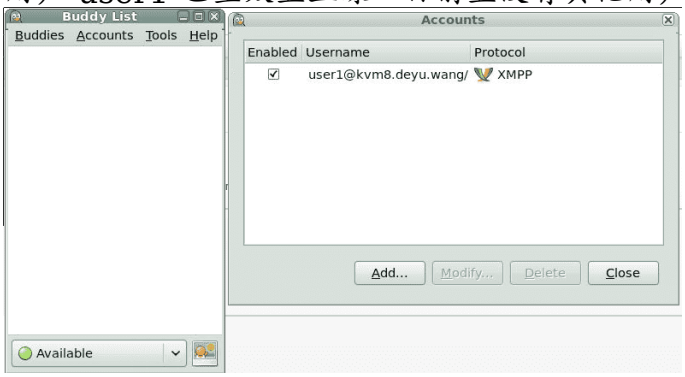
3. 新增用户，Pidgin 支援多種協定，選擇 XMPP，Username, Domain, password 輸入 openfire 伺服器網域名稱及其中用户帳密。



4. 按下接受 kvm8.deyu.wang openfire 伺服器認證。

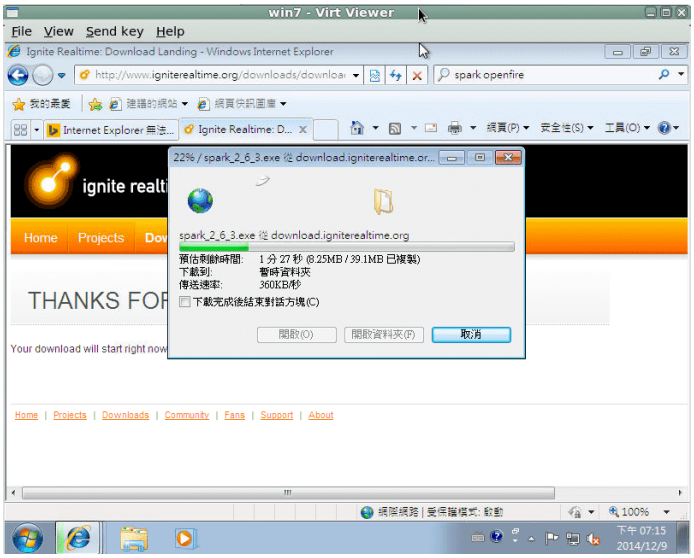


5. 用户 user1 已生效並上線，目前並沒有其他用户在線上。

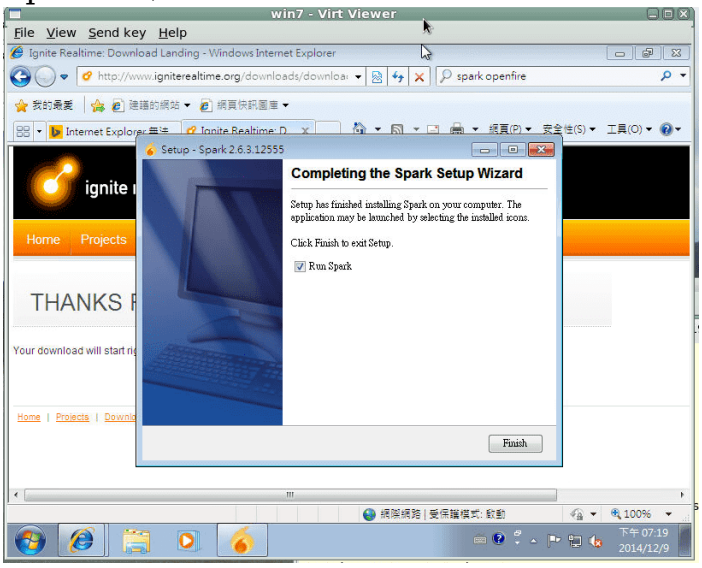


17.7 Openfire Client – Spark for Windows

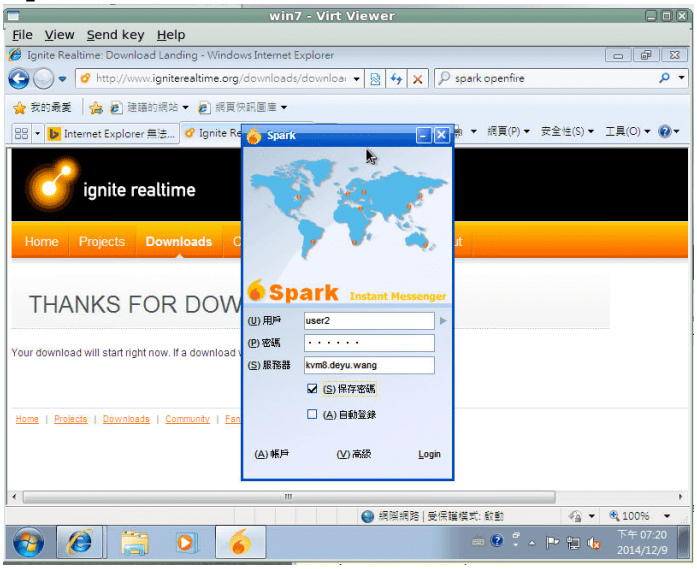
1. Openfire 官網提供 spark 可供下載。下載安裝：



2. Spark 安裝完成。



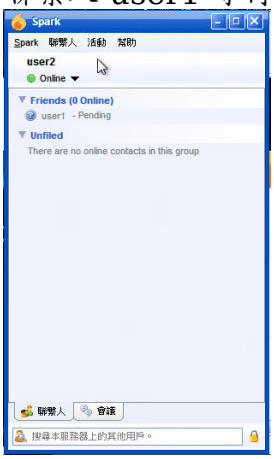
3. Spark 新增 XMPP 用户。



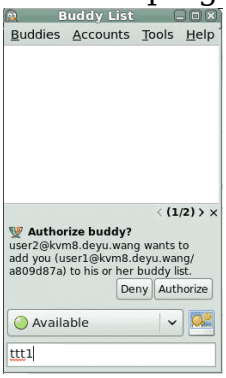
4. 新增聯繫人 user1。



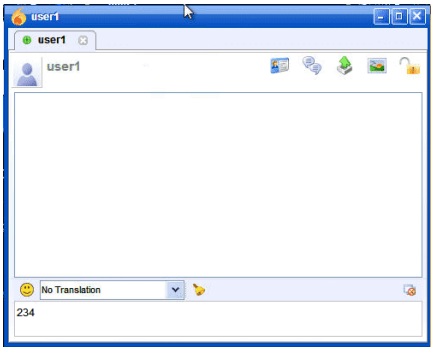
5. 聯繫人 user1 等待確認中。



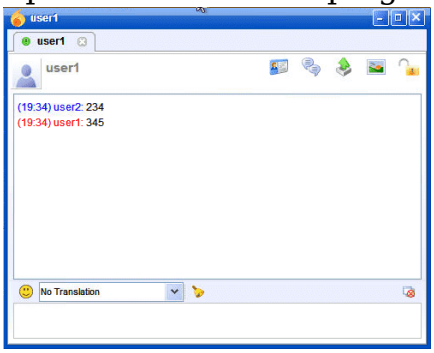
6. user1 在 pidgin 確認來自 user2 的邀請。



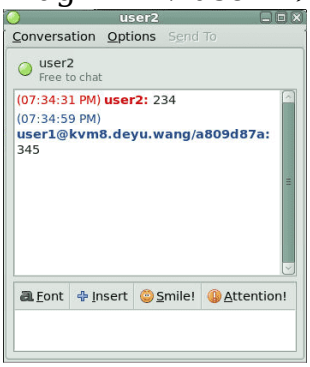
7. Spark 上的 user2 開始與 pidgin 上的 user1 在聊天室上聊天。



8. Spark 上的 user2 與 pidgin 上的 user1 在聊天室上的聊天。



9. Pidgin 上的 user1 與 Spark 上的 user2 在聊天室上的聊天。



Chapter 18

XMPP 即時通訊伺服器 Prosody

18.1 XMPP 簡介

1. XMPP (Extensible Messaging and Presence Protocol) 協定，以前叫做 Jabber。
2. XMPP 是一種以 XML 爲基礎的開放式即時通訊協定。
3. XMPP 被 Google Talk 應用，任何 XMPP 客户端使用 Gmail 帳號登入後都連接到 Google Talk。
4. XMPP 協議是自由、開放、公開的，並且易於瞭解。而且在客户端、伺服器、元件、源碼庫等方面，都已經各自有多種實作。
5. XMPP 開放源碼套件：ejabberd, prosody, openfire。
6. OpenFire Server 在眾多免費開放原始碼的即時訊息伺服器軟體中號稱最容易安裝與設定，其實是因爲 openfire 提供網頁界面的設定。
7. OpenFire Server 安裝參考
8. Spark Client
9. SparkWeb Client
10. 個人認爲 prosody 安裝設定更簡單，只不過它沒有設計圖形或網頁型式的管理界面，會讓不熟文字命令的使用者以爲其比較複雜。
11. Prosody 主要設定檔只有一個 /etc/prosody/prosody.cfg.lua，可以直接以 vim 編輯，只要改一下設定再重新啓動，就可以用户自行註冊，功能完整且設定簡單。

12. prosody 可以擴充模組，在 SSL/TLS 加密，用户註冊、產生、匯入，通訊的資料儲不儲存，都可以簡單設定。因此個人還是偏好 prosody。

18.2 Prosody 套件安裝與啓動

1. 安裝套件 prosody

```
[root@kvm8 ~]# yum install prosody
```

2. 啓動 prosody 服務。

```
[root@kvm8 ~]# /etc/init.d/prosody start
Starting prosody:
```

3. 設定開機自動啓動 prosody 服務。

```
[root@kvm8 ~]# chkconfig prosody on
[root@kvm8 ~]# chkconfig --list prosody
prosody         0:off   1:off   2:on    3:on    4:on    5:on    6:off
```

4. prosody 後端資料處理，可以使用 sql、internal 或 null，使用 null 也就是完全不儲存。注意 null 不能加引號，-- 表示註解。

```
[root@kvm8 ~]# grep ^storage /etc/prosody/prosody.cfg.lua
storage = null -- Default is "internal"
```

18.3 設定 prosody 聊天室

1. Prosody 主要設定檔只有一個 /etc/prosody/prosody.cfg.lua。設定的第一件事，就是加上要服務的 virtual host，可以加入多行 VirtualHost。

```
[root@kvm8 ~]# grep ^VirtualHost /etc/prosody/prosody.cfg.lua
VirtualHost "deyu.wang"
```

2. prosody 內建很多元件，只要啓動並設定就可以使用，例如多用户聊天室 muc。這裡設定一個聊天室在 kvm8.deyu.wang。

```
[root@kvm8 ~]# grep ^Component /etc/prosody/prosody.cfg.lua
Component "kvm8.deyu.wang" "muc"
```

18.4 設定 prosody 用户

1. prosodyctl 管理命令

```
[root@kvm8 ~]# prosodyctl --help
prosodyctl - Manage a Prosody server

Usage: /usr/bin/prosodyctl COMMAND [OPTIONS]

Where COMMAND may be one of:

 adduser JID
    Create the specified user account in Prosody

 passwd JID
    Set the password for the specified user account in Prosody

 deluser JID
    Permanently remove the specified user account from Prosody

 start
    Start Prosody

 stop
    Stop a running Prosody server

 restart
    Restart a running Prosody server

 status
    Reports the running status of Prosody
```

2. prosody 用户產生方式有三種，分別是用户自行註冊、管理者產生及從 ejabberd 匯入。prosody 提供管理者產生用户命令 prosodyctl，注意此例 puser1@deyu.wang domain 爲 deyu.wang 必須是 VirtualHost 加入要服務的對象。

```
[root@kvm8 ~]# prosodyctl adduser puser1@deyu.wang
[root@kvm8 ~]# prosodyctl adduser puser2@deyu.wang
```

3. 修改設定用户密碼。

```
[root@kvm8 ~]# prosodyctl passwd puser1@deyu.wang
Enter new password:
Retype new password:
[root@kvm8 ~]# prosodyctl passwd puser2@deyu.wang
Enter new password:
Retype new password:
```

4. 若也要開放用户自行註冊，只要在設定檔中啓動即可。

```
[root@kvm8 ~]# grep ^allow_registration /etc/prosody/prosody.cfg.lua
allow_registration = true;
```

5. 更改設定後，必須重新啓動 prosody 服務。

```
[root@kvm8 ~]# /etc/init.d/prosody restart
Stopping prosody: Stopped
                                                           [  OK  ]
Starting prosody: Started
                                                           [  OK  ]
```

18.5 Prosody 安全設定

1. 字串 ssl 設定關於 SSL/TLS 安全及加密，以下例子，表示允許用户自行註冊，啓動 ssl 加密認證，私鑰及證書檔如設定。

```
[root@kvm8 ~]# grep ^ssl /etc/prosody/prosody.cfg.lua -C4
allow_registration = true;

-- These are the SSL/TLS-related settings. If you don't want
-- to use SSL/TLS, you may comment or remove this
    key = "/etc/pki/tls/private/prosody.key";
    certificate = "/etc/pki/tls/certs/prosody.crt";
}
```

2. 以下是設定 virtual host 連線，不使用 SSL/TLS 安全及加密。

```
[root@kvm8 ~]# grep '\-\-[[:space:]]*ssl =' /etc/prosody/prosody.cfg.lua
    -B7 -A3
VirtualHost "deyu.wang"
    enabled = true -- Remove this line to enable this host

    -- Assign this host a certificate for TLS, otherwise it would use
        the one
    -- set in the global section (if any).
    -- Note that old-style SSL on port 5223 only supports one
        certificate, and will always
    -- use the global one.
--  ssl = {
--      key = "certs/example.com.key";
--      certificate = "certs/example.com.crt";
--  }
```

3. 更改設定後，必須重新啓動 prosody 服務。

```
[root@kvm8 ~]# /etc/init.d/prosody restart
Stopping prosody: Stopped
                                                           [  OK  ]

Starting prosody: Started
                                                           [  OK  ]
```

4. 查看 prosody 服務預設的 ports。

```
[root@kvm8 ~]# netstat -tlunp | grep lua
tcp    0    0 0.0.0.0:5269        0.0.0.0:*    LISTEN      28232/lua
tcp    0    0 127.0.0.1:5347      0.0.0.0:*    LISTEN      28232/lua
```

```
tcp    0    0 0.0.0.0:5222          0.0.0.0:*     LISTEN      28232/lua
```

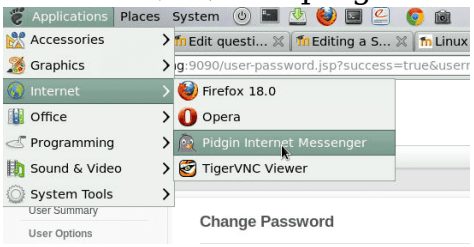
5. 防火牆 iptables 必須開啓 5269,5347,5222 等埠號。

18.6 Prosody Client

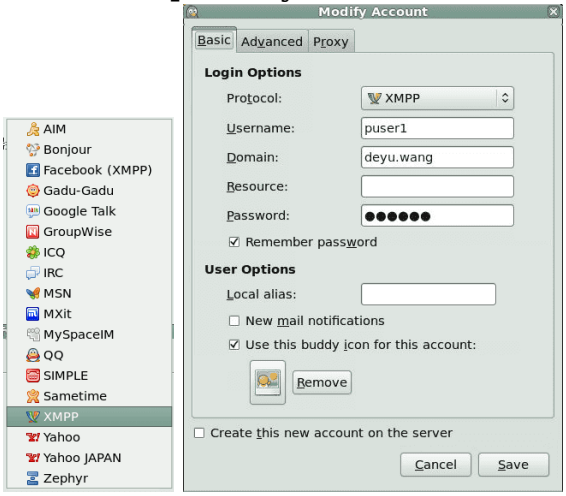
1. XMPP clients 有很多的選擇，Pidgin 是一套即時通訊用户端軟體，支援多種協定，DYW Linux 可直接 yum install pidgin 安裝。用户端方面 Linux 系統使用 Pidgin，Windows 則使用 Spark。

```
[root@dywhd2 ~]# yum install pidgin
```

2. 從應用程式選單執行 pidgin。



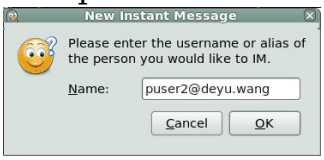
3. 新增用户，Pidgin 支援多種協定，選擇 XMPP，Username, Domain, password 輸入 prosody 伺服器網域名稱及其中用户帳密。



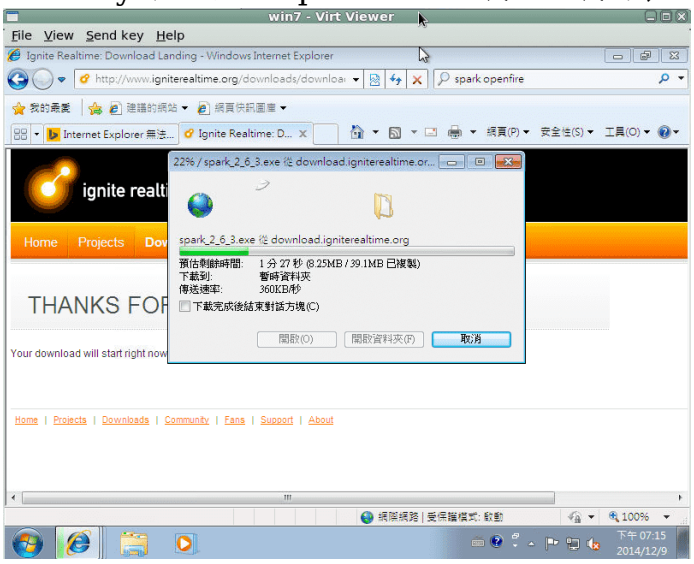
4. 因爲 prosody server 沒有啓動 SSL/TLS 安全與加密，所以必須選擇允許明文傳送。



5. 用户 puser1 已生效並上線，目前並沒有其他用户在線上。



6. Prosody 官網提供 spark 可供下載。下載安裝：



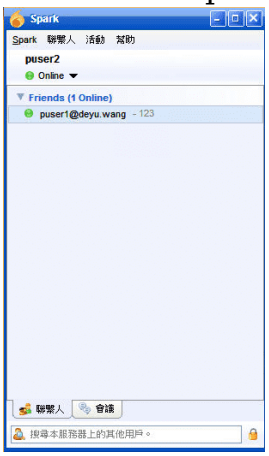
7. puser2 用户登入 Spark。



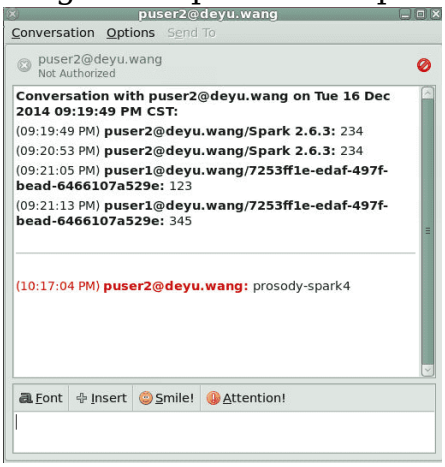
8. Spark XMPP 主機設定。



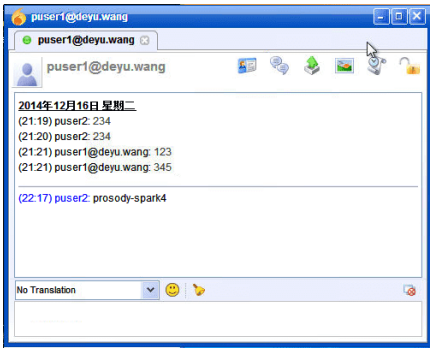
9. 看到線上用户 puser1@deyu.wang。



10. Pidgin 上的 puser1 與 Spark 上的 puser2 在聊天室上的聊天。



11. Spark 上的 puser2 與 pidgin 上的 puser1 在聊天室上聊天。



18.7 用户自行註冊

1. 開放用户自行註冊，必須在 server 端開啓允許設定18.4。開放此一功能雖然方便，但也可能造成系統增加很多垃圾帳號，就看管理者的考量。在 Pidgin 的用户管理，Username, Domain, password 輸入 prosody 伺服器網域名稱及其中用户帳密，並勾選在伺服器產生新的帳號。

```
1 Accounts --> Manager Accounts --> Add -->
  Basic (check Create this new account on the server)
```



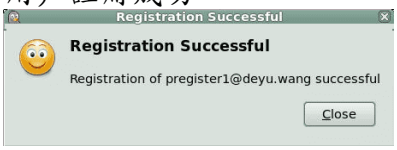
2. 接受伺服器 kvm8.deyu.wang SSL 認證。



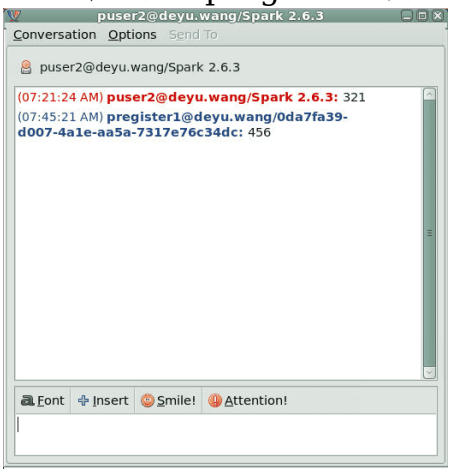
3. 註冊新的用户，名稱與密碼就是一開始輸入的內容，若不想變更就按下 Register 按鈕進行註冊。



4. 用户註冊成功。



5. 使用新的帳號 pregister1 與 Windows Spark 上的 puser2 上通訊。



18.8 SSL 加密

1. Prosody 0.9+ 提供 prosodyctl 命令可以產生憑證，其中 deyu.wang 是 server 設定的 doamin。

```
prosodyctl cert generate deyu.wang
```

2. 因 DYW Linux 安裝的 prosody 版本爲 `0.8.2-7.el6.x86_64`，prosodyctl 命令並沒有提供此一功能。所以管理者必須使用 openssl 自行產生私鑰及憑證。

```
[root@kvm8 ~]# openssl req -days 3650 -new -x509 -nodes \
-out deyu.wang.crt -keyout deyu.wang.key \
-subj '/C=TW/ST=Taiwan/L=CYUT/O=CSIE/CN=deyu.wang Certificate Authority'
```

3. 把私鑰及憑證複製到 tls 預設的目錄中，當然管理者也可以放在自行設定的目錄，只要 server 中指定到該目錄即可。

```
[root@kvm8 ~]# cp deyu.wang.key /etc/pki/tls/private/
[root@kvm8 ~]# cp deyu.wang.crt /etc/pki/tls/certs/
```

4. 變更私鑰及感證權限爲 600，並改變其擁有者及群組組爲 prosody。

```
[root@kvm8 ~]# chmod 600 /etc/pki/tls/certs/deyu.wang.crt
[root@kvm8 ~]# chmod 600 /etc/pki/tls/private/deyu.wang.key

[root@kvm8 ~]# chown prosody:prosody /etc/pki/tls/private/deyu.wang.key
[root@kvm8 ~]# chown prosody:prosody /etc/pki/tls/certs/deyu.wang.crt
```

5. 開啓 client to server 必須加密的設定，安裝好 prosody 時，此參項是註解狀態，設定檔中說明預設是開啓，除非開啓它並設定爲 false，但實際測試必須開啓並設定爲 true 時，才會以加密方式通訊。

```
[root@kvm8 ~]# grep ^c2s /etc/prosody/prosody.cfg.lua
c2s_require_encryption = true
```

6. 修改 server 設定檔，啓動 ssl 加密。

```
VirtualHost "deyu.wang"
    enabled = true -- Remove this line to enable this host

    -- Assign this host a certificate for TLS, otherwise it would use
       the one
    -- set in the global section (if any).
    -- Note that old-style SSL on port 5223 only supports one
       certificate, and will always
    -- use the global one.
    ssl = {
        key = "/etc/pki/tls/private/deyu.wang.key";
        certificate = "/etc/pki/tls/certs/deyu.wang.crt";
    }
```

7. 重新啓動 prosody 服務。

```
[root@kvm8 ~]# prosodyctl restart
Stopped
Started
```

8. Client 端 pidgin 設定爲必須加密。



9. 接受伺服器 kvm8.deyu.wang SSL 認證。



10. 帳號 pregister1 與 Windows Spark 上的 puser2 上的加密通訊。



Chapter 19

SIP 網路電話伺服器 Kamailio

19.1 SIP 簡介

1. VoIP(Voice over IP) 網路電話，是將語音訊號壓縮成數據資料封包後，在 IP 網路基礎上傳送的語音服務。
2. VoIP 通訊協定標準：目前常用的協定如 H.323、SIP、MEGACO 和 MGCP。
3. SIP 已經成爲 VoIP 的主要通訊協定。
4. SIP(Session Initiation Protocol) 通訊協定主要是作爲一個或多個使用者在網路上建立、修改、維護和終止會談的通訊使用。
5. SIP 直接採用文字 (text-based) 式的通訊協定，能在兩兩或更多的傳送參與者間，發展及控制多媒體傳送 (multimedia sessions)，SIP 也規範通話建立與結束所使用的信令方式與訊息傳輸規格的協商機制。

19.2 Kamailio 套件安裝與啓動

1. Kamailio 相套件已納入 DYW Linux，可用 yum 直接安裝。
2. 安裝 kamailio 套件

```
[root@kvm6 ~]# yum install -y kamailio kamailio-mysql \
kamailio-debuginfo kamailio-unixodbc kamailio-utils
```

3. 安裝 mysql 套件

```
[root@kvm6 ~]# yum install -y mysql-server mysql
[root@kvm6 ~]# /etc/init.d/mysqld restart
Stopping mysqld:                                           [  OK  ]
Starting mysqld:                                           [  OK  ]
```

4. 第一次使用，進行安全設定。

```
[root@kvm6 ~]# mysql_secure_installation
```

5. 設定 kamctlrc，指定 SIP_DOMAIN 及使用 MYSQL。

```
[root@kvm6 ~]# vim /etc/kamailio/kamctlrc
[root@kvm6 ~]# egrep '(SIP_DOMAIN|DBENGINE)' /etc/kamailio/kamctlrc
 SIP_DOMAIN=kvm6.deyu.wang
 DBENGINE=MYSQL
```

6. 產生 Kamailio 資料庫用户及所需資料表，過程中因本系統預設 utf-8 編碼 kamailio 無法使用，故必須自行輸入。其他都回答 y，讓其產生。

```
[root@kvm6 ~]# kamdbctl create
MySQL password for root:
INFO: test server charset
WARNING: Your current default mysql characters set cannot be used to
    create DB. Please choice another one from the following list:
big5
dec8
cp850
hp8
koi8r
latin1
latin2
swe7
ascii
ujis
sjis
hebrew
tis620
euckr
koi8u
gb2312
greek
cp1250
gbk
latin5
armscii8
```

```
cp866
keybcs2
macce
macroman
cp852
latin7
cp1251
utf16
cp1256
cp1257
utf32
binary
geostd8
cp932
eucjpms
Enter character set name:
latin1
INFO: creating database kamailio ...
INFO: granting privileges to database kamailio ...
INFO: creating standard tables into kamailio ...
INFO: Core Kamailio tables succesfully created.
Install presence related tables? (y/n): y
INFO: creating presence tables into kamailio ...
INFO: Presence tables succesfully created.
Install tables for imc cpl siptrace domainpolicy carrierroute
        userblacklist htable purple uac pipelimit mtree sca? (y/n): y
INFO: creating extra tables into kamailio ...
INFO: Extra tables succesfully created.
Install tables for uid_auth_db uid_avp_db uid_domain uid_gflags
        uid_uri_db? (y/n): y
INFO: creating uid tables into kamailio ...
INFO: UID tables succesfully created.
```

7. 啓動 kamailio 服務。

```
[root@kvm6 ~]# /etc/init.d/kamailio start
Starting kamailio:                                 [OK]
```

8. 增加兩個測試帳號，kamailio 用户的預設密碼爲 kamailiorw。

```
[root@kvm6 ~]# kamctl add deyu1@deyu.wang 123qwe
MySQL password for user 'kamailio@localhost':
new user 'deyu1@deyu.wang' added
[root@kvm6 ~]# kamctl add deyu2@deyu.wang 123qwe
MySQL password for user 'kamailio@localhost':
new user 'deyu2@deyu.wang' added
```

9. 防火牆必須開啓 5060 port。

```
[root@kvm6 ~]# iptables -I INPUT -p tcp -m state --state NEW \
-m tcp --dport 5060 -j ACCEPT
[root@kvm6 ~]# iptables -I INPUT -p udp -m state --state NEW \
-m udp --dport 5060 -j ACCEPT
```

19.3 SIP Client

1. 電腦可安裝 jitsi 來進行通訊。

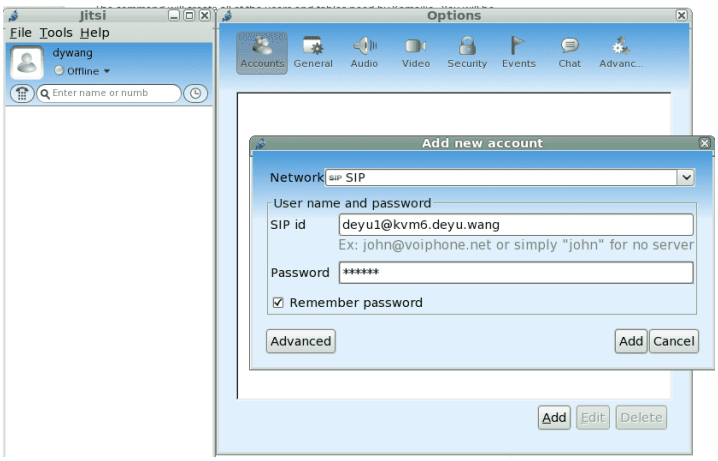
```
[root@kvm8 ~]# yum install jitsi
```

2. 在圖形桌面點選：

```
Application => Internet => Jitsi
應用程式 => 網際網路 => Jitsi
```

3. Jitsi 新增用户。

```
Tools => Options => Account
```



19.4 問題解決

1. 問題：Jitsi 開始與 sip 客户端連線，回應註冊時間 (Request Timeout (408))。
2. 原因：Timeout 的原因可能是註冊者無法取得 kamailio 訊息，或 kamailio 嘗試送封包到其他地方。
3. 解決：在 kamailio server 設定 domain name 的別名。

```
[root@kvm6 ~]# vim /etc/kamailio/kamailio.cfg
[root@kvm6 ~]# egrep '^(alias|listen)' /etc/kamailio/kamailio.cfg
alias="kvm6.deyu.wang"
listen=udp:192.168.122.6:5060
```

4. 重新啓動 kamailio 服務。

```
[root@kvm6 ~]# /etc/init.d/kamailio restart
Stopping kamailio:                                         [  OK  ]
Starting kamailio:
[root@kvm6 ~]#                                             [  OK  ]
```

Chapter 20

WEBCOUNTER

20.1 前言

1. 網路上有很多網站提供免費的網站瀏覽次數計數器，但都必須連線至其指定的伺服器。
2. web counter 網站
3. Simple Hit Counter 網站
4. Hit Counters 網站
5. 還有很多的免費的計數網站，除了安全考量以外，訪問網站的 ip 等其他資料，也都可能被該網站收集。
6. Linux 伺服器上可自行架設網站分析服務，記錄及分析訪問您的網站的訪客之相關訊息。
7. 本章只是想架設一個提供訪問網站計數功能的服務。

20.2 Webcounter 下載安裝

1. Webcounter 沒有 rpm 套件可使用，因此必須下載原始碼。

```
[root@dywang ~]# cd /var/www/html/
[root@dywang html]# wget http://www.cellbiol.com/scripts/free-counter-
    script/counter.zip
```

2. 解壓縮至網頁伺服器的根目錄 /var/www/html。

```
[root@dywang html]# unzip counter.zip
Archive:  counter.zip
   creating: counter/
  inflating: counter/.DS_Store
   creating: __MACOSX/
   creating: __MACOSX/counter/
  inflating: __MACOSX/counter/._.DS_Store
  inflating: counter/counter.php
  inflating: __MACOSX/counter/._counter.php
  inflating: counter/counter.txt
  inflating: __MACOSX/counter/._counter.txt
  inflating: counter/readme.txt
  inflating: __MACOSX/counter/._readme.txt
  inflating: counter/visitors_ips.txt
  inflating: __MACOSX/counter/._visitors_ips.txt
```

3. 查看目錄 counter 下有四個檔案。

```
[root@dywang html]# ll counter
total 20
-rw-r--r--. 1 root root 4703 Feb 16  2013 counter.php
-rw-r--r--. 1 root root    1 Feb 16  2013 counter.txt
-rw-r--r--. 1 root root 2137 Feb 16  2013 readme.txt
-rw-r--r--. 1 root root   25 Feb 16  2013 visitors_ips.txt
```

4. 因爲數字儲存在 counter.txt IP 訪問時間儲存在 visitors_ips.txt，所以必須將這兩個檔案的擁有者改爲 apache，讓 apache 用户可以寫入。不建議直接將這兩個檔案的權限改成 666 或 777，雖然一樣可以讓網頁存取用户 apache 寫入，但在這個系統中的其他用户也一樣可以寫入。

```
[root@dywang html]# chown apache counter/counter.txt counter/
    visitors_ips.txt
[root@dywang html]# ll counter
total 20
-rw-r--r--. 1 root   root 4771 Jan  3 12:00 counter.php
-rw-r--r--. 1 apache root    6 Jan  4 18:25 counter.txt
-rw-r--r--. 1 root   root 2137 Feb 16  2013 readme.txt
-rw-r--r--. 1 apache root   27 Jan  4 18:25 visitors_ips.txt
```

5. 只要將以下程式碼加到您的網頁程式中，就可以顯示此計數，其中 http://dywang.csie.cyut.edu.tw 改成您 webcounter 所架設的網址。

```
<img src="http://dywang.csie.cyut.edu.tw/counter/counter.php" alt="page
    counter" title="Single visitors since 12345" style="width:140px;">
```

20.3 Webcount 調整

1. 解壓縮後，目錄 counter 下 readme.txt 檔案有安裝及設定說明可參考。php 程式只有 counter.php，修改如下：

```
[root@dywang counter]# diff -uNw ../../counter/counter.php counter.php
--- ../../counter/counter.php   2013-02-16 22:17:21.000000000 +0800
+++ counter.php 2015-01-03 12:00:10.659053758 +0800
```

2. 更改增加計數器動作間隔，原先設定 2 小時內同一 ip 訪問都只算 1 次，改成只要重新整理都計算。

```
@@ -29,7 +29,7 @@

 /* END CONFIGURATION */

-$iprt=7200; # 1 hour is 3600 seconds, I P Residence Time
+$iprt=1; #7200; # 1 hour is 3600 seconds, I P Residence Time
 $ips=array();
 $ipfh=fopen($visitors_ips_file,"r");
 $flag=0;
```

3. 將數字改成固定 12 位數，不足的位數補 0。

```
@@ -64,6 +64,8 @@
 $cfh=fopen($counter_file,"r");
 $line=fgets($cfh);
 $count=trim($line);
+$cc=strlen($count);
+for($i=$cc; $i<12; $i++) $count= '0'.$count;
 CreateCounterImage ($count);
```

```
$cfh=fopen($counter_file,"w");
```

4. 計數影像寬度由 80 加寬至 140。

```
@@ -72,7 +74,7 @@
 $write = fputs($cfh, $count);

 function CreateCounterImage ($count){ # creates a captcha image and
     returns the value written on it
-  $im = ImageCreate(80, 20);  # we create an image providing width and
     height (in pixels) as arguments. Edit this for changing the image
     counter size
+  $im = ImageCreate(140, 20);  # we create an image providing width and
      height (in pixels) as arguments. Edit this for changing the image
     counter size
    $selbgcol=rand(0,4);

    /* ALLOCATING COLORS TO THE IMAGE */
```

5. 修改計數器隨機背景顏色中的橘色。

```
@@ -80,7 +82,7 @@
    $red = ImageColorAllocate($im, 189, 5, 8);#RED
    $black =  ImageColorAllocate($im, 0, 0, 0);#BLACK
    $green  = ImageColorAllocate($im, 115, 211, 45);#GREEN
-   $orange = ImageColorAllocate($im, 252, 149, 26);#ORANGE
+   $orange = ImageColorAllocate($im, 252, 149, 16);#ORANGE
    $blue = ImageColorAllocate($im, 72, 103, 173);#BLUE
    $white = ImageColorAllocate($im, 255, 255, 255); # the numbers (text)
        in the counter will always be white and the above colors are
       used randomly for the background
```

6. 修改計數器數字左邊邊界由 12 改成 16。

```
@@ -95,7 +97,7 @@

    # we now write the string text to the image. The last number in the
       arguments list of ImageString moves the image text vertically,
       small number -> text goes up, big number text goes down
    # default color for text is white, as defined in the colors list
       above and then used as last argument in the ImageString call.
       Feel free to play with the colors here
```

```
5 -  ImageString($im, 8, 12, 2, $new_string, $white); #
  +  ImageString($im, 8, 16, 2, $new_string, $white); #
7
     #output to browser
9    ImagePNG($im, "counter.png");
```

20.4 Webcount 展示

1. dywang 首頁。



2. 朝陽資工系網。



3. 朝陽資工 webmail。



4. 朝陽 Moodle 數位平台。



Chapter 21

自動開關機

21.1 前言

1. 伺服器架設後，一般是不會關機，但當停電時間超過不斷電系統所能供給的時間，系統將在不正常的狀態下關機。
2. BIOS 的電源管理可以設定爲：當不正常斷電情況下，恢復電力後自動啓動。
3. 雖然可以使用 BISO 設定讓伺服器於恢復電力後啓動，但是伺服器並不是使用關機指令正常關機，有可能因爲檔案損壞而無法再開機成功。
4. 爲解決此一問題，可使用例行性命令 crontab 設定關機時間，再利用 Linux 核心支援的實時時鐘（Real-time clock，RTC）設定開機時間。

21.2 自動開機

1. 檢查核心是否支援 RTC，顯示說明如下：
   (a) `rtc_time`：目前格林威治標準時間 (GMT: Greenwich Mean Time)，台灣必須加 8 小時；
   (b) `rtc_date`：目前的 rtc 日期；
   (c) `alarm_time`：設定開機的時間；
   (d) `alarm_date`：設定開機的日期；
   (e) `alarm_IRQ`：是否有設定鬧鐘，目前爲 no，表示沒有設定自動開機，若有設定成功，這項會變成 yes。

```
[root@dywH ~]# cat /proc/driver/rtc
rtc_time    : 08:28:40
```

```
rtc_date    : 2015-04-04
alrm_time   : 14:52:17
alrm_date   : ****-**-**
alarm_IRQ   : no
alrm_pending    : no
24hr        : yes
periodic_IRQ    : no
update_IRQ  : no
HPET_emulated   : yes
DST_enable  : no
periodic_freq   : 1024
batt_status : okay
```

2. 將自動開機時間的時間戳 (timestamp) 寫入 /sys/class/rtc/rtc0/wakealarm。

```
[root@dywH ~]# date +%s -d "now + 30minutes" | tee /sys/class/rtc/rtc0/
    wakealarm
1428139354
```

3. 查看 /sys/class/rtc/rtc0/wakealarm。

```
[root@dywH ~]# cat /sys/class/rtc/rtc0/wakealarm
1428139354
```

4. 再查看 RTC，自動開機時間爲 09:22:34 (台灣加 8 小時)，日期爲 2015-04-04，alarm_IRQ 已變成 yes，

```
[root@dywH ~]# cat /proc/driver/rtc
rtc_time    : 08:54:24
rtc_date    : 2015-04-04
alrm_time   : 09:22:34
alrm_date   : 2015-04-04
alarm_IRQ   : yes
alrm_pending    : no
24hr        : yes
periodic_IRQ    : no
update_IRQ  : no
HPET_emulated   : yes
DST_enable  : no
periodic_freq   : 1024
batt_status : okay
```

5. 準備關機，當然是正常關機，不要直接關掉電源，看看時間到會不會自動開機。

Chapter 22

SoftEther VPN

22.1 前言

1. SoftEther VPN 是一個功能強、支援多協定的軟體，可以跨平台於 Windows, Linux, Mac, FreeBSD 和 Solaris 上使用。
2. 在 CentOS 安裝 SoftEther VPN。
3. SoftEther VPN 官網上有很多文件可參考
4. SoftEther Download Center

22.2 SoftEther Server 安裝

1. SoftEther 下載 SoftEther Download Center

```
[root@dyw219 ~]# cd /usr/src/
[root@dyw219 src]# wget http://www.softether-download.com/files/
    softether/\
v4.21-9613-beta-2016.04.24-tree/Linux/SoftEther_VPN_Server/\
64bit_-_Intel_x64_or_AMD64/\
softether-vpnserver-v4.21-9613-beta-2016.04.24-linux-x64-64bit.tar.gz
```

2. 解壓縮及解打包，檔案在 vpnserver 目錄。

```
[root@dyw219 src]# tar zxvf softether-vpnserver-v4.21-9613-beta
    -2016.04.24-linux-x64-64bit.tar.gz
```

3. 進入 vpnserver 目錄進行 make 編譯程式，過程中全部回答 yes。

```
[root@dyw219 src]# cd vpnserver
[root@dyw219 vpnserver]# make
```

4. 建立 /usr/local/vpnserver 將 vpn server 執行檔案複製到此目錄。

```
[root@dyw219 vpnserver]# mkdir /usr/local/vpnserver
[root@dyw219 vpnserver]# cp vpnserver vpncmd hamcore.se2 /usr/local/
    vpnserver/
```

5. 產生 vpnserver 服務啓動、關閉執行腳本如下：

```
[root@dyw219 vpnserver]# vim /etc/init.d/vpnserver
[root@dyw219 vpnserver]# cat /etc/init.d/vpnserver
#!/bin/sh
# chkconfig: 2345 99 01
# description: SoftEther VPN Server
DAEMON=/usr/local/vpnserver/vpnserver
LOCK=/var/lock/subsys/vpnserver
test -x $DAEMON || exit 0
case "$1" in
    start)
        $DAEMON start
        touch $LOCK
        ;;
    stop)
        $DAEMON stop
        rm $LOCK
        ;;
    restart)
        $DAEMON stop
        sleep 3
        $DAEMON start
        ;;
    *)
        echo "Usage: $0 {start|stop|restart}"
        exit 1
esac
exit 0
```

6. 將 vpnserver 腳本設定成可執行並啓動。

```
[root@dyw219 vpnserver]# chmod 755 /etc/init.d/vpnserver
[root@dyw219 vpnserver]# /etc/init.d/vpnserver start
The SoftEther VPN Server service has been started.
```

22.3 vpncmd 命令設定 vpnserver

1. 選擇選項 3，執行 check 檢查系統滿足 vpn server。

```
[root@dyw219 vpnserver]# /usr/local/vpnserver/vpncmd
vpncmd command - SoftEther VPN Command Line Management Utility
SoftEther VPN Command Line Management Utility (vpncmd command)
Version 4.21 Build 9613   (English)
Compiled 2016/04/24 16:39:47 by yagi at pc30
Copyright (c) SoftEther VPN Project. All Rights Reserved.

By using vpncmd program, the following can be achieved.

1. Management of VPN Server or VPN Bridge
2. Management of VPN Client
3. Use of VPN Tools (certificate creation and Network Traffic Speed Test
    Tool)

Select 1, 2 or 3: 3

VPN Tools has been launched. By inputting HELP, you can view a list of
   the commands that can be used.

VPN Tools>check
Check command - Check whether SoftEther VPN Operation is Possible
------------------------------------------------------
SoftEther VPN Operation Environment Check Tool

Copyright (c) SoftEther VPN Project.
All Rights Reserved.

If this operation environment check tool is run on a system and that
   system passes, it is most likely that SoftEther VPN software can
   operate on that system. This check may take a while. Please wait...

Checking 'Kernel System'...
             Pass
Checking 'Memory Operation System'...
             Pass
Checking 'ANSI / Unicode string processing system'...
```

```
33              Pass
Checking 'File system'...
35              Pass
Checking 'Thread processing system'...
37              Pass
Checking 'Network system'...
39              Pass

41 All checks passed. It is most likely that SoftEther VPN Server / Bridge
       can operate normally on this system.

43 The command completed successfully.
VPN Tools>exit
```

2. 再執行 /usr/local/vpnserver/vpncmd 命令選擇選項 1 進行 vpnserver 設定。

```
[root@dyw219 vpnserver]# /usr/local/vpnserver/vpncmd
2 vpncmd command - SoftEther VPN Command Line Management Utility
SoftEther VPN Command Line Management Utility (vpncmd command)
4 Version 4.21 Build 9613   (English)
Compiled 2016/04/24 16:39:47 by yagi at pc30
6 Copyright (c) SoftEther VPN Project. All Rights Reserved.

8 By using vpncmd program, the following can be achieved.

10 1. Management of VPN Server or VPN Bridge
2. Management of VPN Client
12 3. Use of VPN Tools (certificate creation and Network Traffic Speed Test
       Tool)

14 Select 1, 2 or 3: 1
```

3. 輸入 vpnserver 的 IP 及 port。

```
Specify the host name or IP address of the computer
2 that the destination VPN Server or VPN Bridge is operating on.
By specifying according to the format 'host name:port number',
4 you can also specify the port number.
(When the port number is unspecified, 443 is used.)
6 If nothing is input and the Enter key is pressed, the connection will be
made to the port number 8888 of localhost (this computer).
8 Hostname of IP Address of Destination: 163.17.27.219:443
```

4. 指定 Virtual Hub 名稱。

```
If connecting to the server by Virtual Hub Admin Mode, please input the
    Virtual Hub name.
If connecting by server admin mode, please press Enter without inputting
     anything.
Specify Virtual Hub Name:
Connection has been established with VPN Server "163.17.27.219" (port
    443).

You have administrator privileges for the entire VPN Server.
```

5. 設定 server 密碼。

```
VPN Server>ServerPasswordSet
ServerPasswordSet command - Set VPN Server Administrator Password
Please enter the password. To cancel press the Ctrl+D key.

Password: ******
Confirm input: ******


The command completed successfully.
```

6. 產生 Hub，設定密碼。

```
VPN Server>HubCreate VPN
HubCreate command - Create New Virtual Hub
Please enter the password. To cancel press the Ctrl+D key.

Password: ******
Confirm input: ******


The command completed successfully.
```

7. 選用剛剛產生名爲 VPN 的 HUB。

```
VPN Server>hub VPN
Hub command - Select Virtual Hub to Manage
```

```
3 The Virtual Hub "VPN" has been selected.
  The command completed successfully.
```

8. 啓動 hub VPN 的加密 NAT 功能。

```
  VPN Server/VPN>SecureNatEnable
2 SecureNatEnable command - Enable the Virtual NAT and DHCP Server
      Function (SecureNat Function)
  The command completed successfully.
```

9. 產生連線用户 user1。

```
1 VPN Server/VPN>Usercreate
  UserCreate command - Create User
3 User Name: user1

5 Assigned Group Name:

7 User Full Name:

9 User Description:

11 The command completed successfully.
```

10. 設定 user1 的密碼。

```
1 VPN Server/VPN>Userpasswordset
  UserPasswordSet command - Set Password Authentication for User Auth Type
       and Set Password
3 User Name: user1

5 Please enter the password. To cancel press the Ctrl+D key.

7 Password: *********
  Confirm input: *********
9
  The command completed successfully.
```

11. 查看 hub VPN 的 IP 爲 192.168.30.1。

```
VPN Server/VPN>iptable
IpTable command - Get the IP Address Table Database
Item        |Value
------------+-------------------
ID          |804511970
Session Name|SID-SECURENAT-1
IP Address  |192.168.30.1
Created at  |2016-05-17 07:30:31
Updated at  |2016-05-17 07:31:37
Location    |On 'dyw219'
The command completed successfully.
```

22.4 設定 VPN hub 橋接器

1. 持續之前的 vpncmd 命令設定，使用 hub 指令不加參數回到 vpn server 管理模式。

```
VPN Server/VPN>hub
Hub command - Select Virtual Hub to Manage
The Virtual Hub selection has been unselected.
The command completed successfully.
```

2. 查看可用的橋接裝置。

```
VPN Server>bridgedevicelist
BridgeDeviceList command - Get List of Network Adapters Usable as Local
   Bridge
eth0
eth1
virbr0
vnet0
vnet1
vnet3
vnet4
vnet5
vnet6
The command completed successfully.
```

3. 查看 bridgecreate 命令手冊。

```
VPN Server>bridgecreate /?
BridgeCreate command - Create Local Bridge Connection
Help for command "BridgeCreate"

Purpose:
  Create Local Bridge Connection

Description:
  Use this to create a new Local Bridge connection on the VPN Server.
  By using a Local Bridge, you can configure a Layer 2 bridge connection
  between a Virtual Hub operating on this VPN server and a physical
      Ethernet
  Device (Network Adapter).
  You can create a tap device (virtual network interface) on the system
      and
  connect a bridge between Virtual Hubs (the tap device is only
      supported by
  Linux versions).
  It is possible to establish a bridge to an operating network adapter
      of your
  choice for the bridge destination Ethernet device (network adapter),
      but in
  high load environments, we recommend you prepare a network adapter
  dedicated to serve as a bridge.
  To execute this command, you must have VPN Server administrator
      privileges.

Usage:
  BridgeCreate [hubname] [/DEVICE:device_name] [/TAP:yes|no]

Parameters:
  hubname - Specify the Virtual Hub to create bridge. To get a list of
      Virtual
            Hubs, you can use the HubList command. It is not essential
                that
            you specify a Virtual Hub that is currently operating. If
                you
            specify a Virtual Hub name that is not currently operating
                or that
            does not exist, the Local Bridge connection will become
                enabled
            when the actual operation of that Virtual Hub begins.
  /DEVICE - Specify the bridge destination Ethernet device (network
      adapter)
            or tap device name. You can get the list of Ethernet device
                names
            by using the BridgeDeviceList command.
  /TAP    - Specify yes if you are using a tap device rather than a
      network
            adapter for the bridge destination (only supported for Linux
            versions). When this is omitted, it will be treated the same
                 as
            when no is specified.
```

4. 增加 hub vpn 橋接到 eth0 並採用 TAP，如此 ifconfig 可以看到一張網卡 tap_eth0。

```
VPN Server>bridgecreate vpn /device:br0 /tap:yes
BridgeCreate command - Create Local Bridge Connection
While in the condition that occurs immediately after a new bridge connection is
made when bridging to a physical network adapter, depending on the type of
network adapter, there are cases where it will not be possible to communicate
using TCP/IP to the network adapter using a bridge connection from a computer
on the virtual network.
(This phenomenon is known to occur for Intel and Broadcom network adapters.)

If this issue arises, remedy the situation by restarting the computer on which
VPN Server / Bridge is running. Normal communication will be possible after
the computer has restarted.

Also many wireless network adapters will not respond to the sending of packets
in promiscuous mode and when this occurs you will be unable to use the Local
Bridge. If this issue arises, try using a regular wired network adapter
instead of the wireless network adapter.

Instructions for Local Bridge on VM
It has been detected that the VPN Server might be running on a VM (Virtual Machine)
suchlike VMware or Hyper-V. Read the following instructions carefully.
If you are not using a VM, please ignore this message.
Some VMs prohibit the "Promiscuous Mode" (MAC Address Spoofing) on the network
adapters by default.

If the Promiscuous Mode (MAC Address Spoofing) is administratively disabled,
the Local Bridge function between a Virtual Hub on the VPN Server and a physical
network adapter on the physical computer does not work well. You should allow
the Promiscuous Mode (MAC Address Spoofing) by using the configuration tool of the VM.

```

```
For details please refer the documents of your VM. If it is a shared-VM
    and
administrated by other person, please request the administrator to
    permit the
use of the Promiscuous (MAC Address Spoofing) Mode to your VM.

The command completed successfully.
```

5. 使用 hub VPN 命令回到 hub vpn 的管理模式。

```
VPN Server>hub vpn
Hub command - Select Virtual Hub to Manage
The Virtual Hub "VPN" has been selected.
The command completed successfully.
```

6. 查看 hub VPN 的 IP 除了 192.168.30.1，還多了一個橋接 session，但沒有 ipv4 的 IP。

```
VPN Server/VPN>iptable
IpTable command - Get the IP Address Table Database
Item         |Value
-------------+-----------------------
ID           |804511970
Session Name|SID-SECURENAT-1
IP Address   |192.168.30.1
Created at   |2016-05-17 07:30:31
Updated at   |2016-05-17 08:02:05
Location     |On 'dyw219'
-------------+-----------------------
ID           |3996354065
Session Name|SID-LOCALBRIDGE-3
IP Address   |fe80::2ac:3dff:fea0:1692
Created at   |2016-05-17 08:01:49
Updated at   |2016-05-17 08:02:07
Location     |On 'dyw219'
The command completed successfully.
```

22.5 VPN 設定 DHCP

1. DHCPSET 設定 DHCP 參數，gateway 及 dns 不要設定，只做 192.168.1.0/24 網段的互連。

```
VPN Server/vpn>dhcpset /start:192.168.1.10 /end:192.168.1.19 /mask
    :255.255.255.0 \
/expire:1000 /gw /dns /dns2 /DOMAIN /log:yes
DhcpSet command - Change Virtual DHCP Server Function Setting of
    SecureNAT Function
The command completed successfully.
```

2. 設定都存於 /usr/local/vpnserver/vpn_server.config，也可以先關閉 vpnserver，直接編輯此檔後再啓動一樣可以更改設定。

```
[root@dyw219 ~]# vim /usr/local/vpnserver/vpn_server.config
[root@dyw219 ~]# grep 'declare SecureNAT' -A30 -m1 /usr/local/vpnserver/
    vpn_server.config
            declare SecureNAT
            {
                bool Disabled true
                bool SaveLog true

                declare VirtualDhcpServer
                {
                    string DhcpDnsServerAddress 192.168.1.1
                    string DhcpDnsServerAddress2 0.0.0.0
                    string DhcpDomainName $
                    bool DhcpEnabled true
                    uint DhcpExpireTimeSpan 7200
                    string DhcpGatewayAddress 192.168.1.1
                    string DhcpLeaseIPEnd 192.168.1.20
                    string DhcpLeaseIPStart 192.168.1.10
                    string DhcpPushRoutes $
                    string DhcpSubnetMask 255.255.255.0
                }
                declare VirtualHost
                {
                    string VirtualHostIp 192.168.1.1
                    string VirtualHostIpSubnetMask 255.255.255.0
                    string VirtualHostMacAddress 00-AC-43-22-56-80
                }
                declare VirtualRouter
                {
                    bool NatEnabled true
                    uint NatMtu 1500
                    uint NatTcpTimeout 1800
                    uint NatUdpTimeout 60
                }
```

22.6 brctl 設定橋接器

1. 查看目前的橋接只有 KVM 虛擬機使用的 virbr0。

```
[root@dyw219 ~]# brctl show
bridge name bridge id       STP enabled interfaces
virbr0      8000.fe54000af4cf   yes     vnet0
                            vnet1
                            vnet3
                            vnet4
                            vnet5
                            vnet6
```

2. 增加 br0 橋接器做爲 VPN hub 使用。

```
[root@dyw219 ~]# brctl addbr br0
[root@dyw219 ~]# brctl show
bridge name bridge id       STP enabled interfaces
br0     8000.00ac3da01692   no
virbr0      8000.fe54000af4cf   yes     vnet0
                            vnet1
                            vnet3
                            vnet4
                            vnet5
                            vnet6
```

3. 增加 br0 橋接器連接的網卡 eth0。

```
[root@dyw219 ~]# brctl addif br0 eth0
[root@dyw219 ~]# brctl show
bridge name bridge id       STP enabled interfaces
br0     8000.00ac3da01692   no      eth0
virbr0      8000.fe54000af4cf   yes     vnet0
                            vnet1
                            vnet3
                            vnet4
                            vnet5
                            vnet6
```

4. 增加 br0 橋接器連接的網卡 eth0。

```
[root@dyw219 ~]# brctl addif br0 eth0
[root@dyw219 ~]# brctl show
bridge name bridge id       STP enabled interfaces
br0     8000.00ac3da01692   no      eth0
virbr0      8000.fe54000af4cf   yes     vnet0
                            vnet1
                            vnet3
                            vnet4
                            vnet5
                            vnet6
```

5. 查看網卡出現 tap_eth0。

```
[root@dyw219 ~]# ifconfig | grep ^[a-z] | awk '{print $1}'
br0
eth0
eth1
lo
tap_eth0
virbr0
vnet0
vnet1
vnet3
vnet4
vnet5
vnet6
```

6. 增加 br0 橋接器連接的網卡 tap_eth0。

```
[root@dyw219 ~]# brctl addif br0 eth0
[root@dyw219 ~]# brctl show
bridge name bridge id       STP enabled interfaces
br0     8000.00ac8e8ec395   no      eth0
                            tap_eth0
virbr0      8000.fe54000af4cf   yes     vnet0
                            vnet1
                            vnet3
                            vnet4
                            vnet5
                            vnet6
```

7. 編輯橋接器 br0，網卡 eth0 及 tap_eth0 設定檔。

```
[root@dyw219 ~]# cd /etc/sysconfig/network-scripts/
[root@dyw219 network-scripts]# cp ifcfg-eth0 ifcfg-br0
[root@dyw219 network-scripts]# cp ifcfg-eth0 ifcfg-tap_eth0

[root@dyw219 network-scripts]# vim ifcfg-br0
[root@dyw219 network-scripts]# cat ifcfg-br0
DEVICE="br0"
IPADDR=192.168.1.254
NETMASK=255.255.255.0
GATEWAY=163.17.27.219
DNS1=120.110.21.249
DNS2=8.8.8.8
ONBOOT="yes"
TYPE=Bridge

[root@dyw219 network-scripts]# vim ifcfg-eth0
[root@dyw219 network-scripts]# cat ifcfg-eth0
DEVICE="eth0"
ONBOOT="yes"
BRIDGE=br0
TYPE=Ethernet

[root@dyw219 network-scripts]# vim ifcfg-tap_eth0
[root@dyw219 network-scripts]# cat ifcfg-tap_eth0
DEVICE="tap_eth0"
ONBOOT="yes"
BRIDGE=br0
TYPE=Ethernet
```

8. 重新啓動網路。

```
[root@dyw219 network-scripts]# /etc/init.d/network restart
```

9. 再使用 vpncmd 命令進入 hub vpn 管理模式，查看 hub VPN 的 IP 多了一個橋接 IP 192.168.1.254，表示只要 vpn client 連線的 network adapter 設定 192.168.1.0/24 的網段就可以直接連線 VPN server 端的 192.168.1.0/24 網段機器。

```
VPN Server/VPN>iptable
IpTable command - Get the IP Address Table Database
Item        |Value
------------+-----------------------
ID          |1358754158
Session Name|SID-LOCALBRIDGE-3
```

```
IP Address  |192.168.1.254
Created at  |2016-05-17 08:03:50
Updated at  |2016-05-17 08:03:54
Location    |On 'dyw219'
------------+-----------------------
ID          |804511970
Session Name|SID-SECURENAT-1
IP Address  |192.168.30.1
Created at  |2016-05-17 07:30:31
Updated at  |2016-05-17 08:03:55
Location    |On 'dyw219'
------------+-----------------------
ID          |3996354065
Session Name|SID-LOCALBRIDGE-3
IP Address  |fe80::2ac:3dff:fea0:1692
Created at  |2016-05-17 08:01:49
Updated at  |2016-05-17 08:03:54
Location    |On 'dyw219'
The command completed successfully.
```

22.7 SoftEther VPN Client 安裝

1. SoftEther 下載 SoftEther Download Center

```
[root@dywftp ~]# cd /usr/src/
[root@dywftp src]# wget http://www.softether-download.com/files/
    softether/\
v4.21-9613-beta-2016.04.24-tree/Linux/SoftEther_VPN_Client/64bit_-
    _Intel_x64_or_AMD64/\
softether-vpnclient-v4.21-9613-beta-2016.04.24-linux-x64-64bit.tar.gz
[root@oveng ~]#
```

2. 解打包及壓縮，檔案在 vpnclient 目錄。

```
[root@dywftp src]# tar zxvf softether-vpnclient-v4.21-9613-beta
    -2016.04.24-linux-x64-64bit.tar.gz
```

3. 進入 vpnclient 目錄進行 make 編譯程式，過程中全部回答 yes。

```
[root@dywftp src]# cd vpnclient/
```

```
[root@dywftp vpnclient]# make
```

4. 建立 /usr/bin/vpnclient 目錄，並將 vpn clinet 執行檔案複製到此目錄。

```
[root@dywftp vpnclient]# cp vpn* /usr/bin/vpnclient/
[root@dywftp vpnclient]# cp hamcore.se2 /usr/bin/vpnclient/
```

5. 產生 vpnclient 服務啓動、關閉執行腳本如下：

```
[root@dywftp vpnclient]# vim /etc/init.d/vpnclient
[root@dywftp vpnclient]# cat /etc/init.d/vpnclient
#!/bin/sh
# chkconfig: 2345 99 01
# description: SoftEther VPN Client
DAEMON=/usr/bin/vpnclient/vpnclient
LOCK=/var/lock/subsys/vpnclient
test -x $DAEMON || exit 0
case "$1" in
    start)
        $DAEMON start
        touch $LOCK
        ;;
    stop)
        $DAEMON stop
        rm $LOCK
        ;;
    restart)
        $DAEMON stop
        sleep 3
        $DAEMON start
        ;;
    *)
        echo "Usage: $0 {start|stop|restart}"
        exit 1
esac
exit 0
```

6. 將 vpnserver 腳本設定成可執行並啓動。

```
[root@dywftp vpnclient]# chmod 755 /etc/init.d/vpnclient
[root@dywftp vpnclient]# /etc/init.d/vpnclient start
The SoftEther VPN Client service has been started.
```

22.8 vpncmd 設定 vpn client

1. 使用 vpncmd 命令選擇選項 2 進行 client 設定。

```
[root@dywftp vpnclient]# /usr/bin/vpnclient/vpncmd
vpncmd command - SoftEther VPN Command Line Management Utility
SoftEther VPN Command Line Management Utility (vpncmd command)
Version 4.21 Build 9613   (English)
Compiled 2016/04/24 16:39:47 by yagi at pc30
Copyright (c) SoftEther VPN Project. All Rights Reserved.

By using vpncmd program, the following can be achieved.

1. Management of VPN Server or VPN Bridge
2. Management of VPN Client
3. Use of VPN Tools (certificate creation and Network Traffic Speed Test
    Tool)

Select 1, 2 or 3: 2

Specify the host name or IP address of the computer that the destination
    VPN Client is operating on.
If nothing is input and Enter is pressed, connection will be made to
   localhost (this computer).
Hostname of IP Address of Destination:

Connected to VPN Client "localhost".

VPN Client>help
```

2. 建立 NIC myadapter。

```
VPN Client>NicCreate myadapter
NicCreate command - Create New Virtual Network Adapter
The command completed successfully.
```

3. 建立 myconnection 連線，連線主機 163.17.27.219:443，連線的 hub 是 vpn，使用的 nic 爲剛剛產生的 nic myadapter。

```
VPN Client>AccountCreate myconnection
AccountCreate command - Create New VPN Connection Setting
Destination VPN Server Host Name and Port Number: 163.17.27.219:443

Destination Virtual Hub Name: vpn

Connecting User Name: user1

Used Virtual Network Adapter Name: myadapter

The command completed successfully.
```

4. 設定 myconnection 連線的帳號 user1。

```
VPN Client>AccountUsernameSet myconnection
AccountUsernameSet command - Set User Name of User to Use Connection of
    VPN Connection Setting
Connecting User Name: user1

The command completed successfully.
```

5. 設定 myconnection 連線的密碼。

```
VPN Client> AccountPasswordSet myconnection
AccountPasswordSet command - Set User Authentication Type of VPN
    Connection Setting to Password Authentication
Please enter the password. To cancel press the Ctrl+D key.

Password: *********
Confirm input: *********


Specify standard or radius: standard

The command completed successfully.
```

6. 使用 myconnection 連線並設定啓動服務時自動啓動。

```
VPN Client>AccountConnect myconnection
AccountConnect command - Start Connection to VPN Server using VPN
    Connection Setting
```

```
3 The command completed successfully.

5 VPN Client>AccountStartupSet myconnection
AccountStartupSet command - Set VPN Connection Setting as Startup
    Connection
7 The command completed successfully.
```

22.9 設定 VPN Client IP

1. 查看 vpn_myadapter 沒有指定 IP，無法連線 VPN server 端的 192.168.1.254。

```
1 [root@dywftp vpnclient]# ifconfig vpn_myadapter
vpn_myadapter Link encap:Ethernet  HWaddr 00:AC:E8:A9:C9:4D
3           inet6 addr: fe80::2ac:e8ff:fea9:c94d/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
5           RX packets:290 errors:0 dropped:0 overruns:0 frame:0
            TX packets:245 errors:0 dropped:0 overruns:0 carrier:0
7           collisions:0 txqueuelen:500
            RX bytes:20090 (19.6 KiB)  TX bytes:20254 (19.7 KiB)
9
[root@dywftp vpnclient]# ping -c3 192.168.1.254
11 PING 192.168.1.254 (192.168.1.254) 56(84) bytes of data.

13 --- 192.168.1.254 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 11999ms
```

2. 設定 vpn_myadapter IP 爲 192.168.1.200/24，就可以連線 VPN server 端的 192.168.1.254。

```
[root@dywftp vpnclient]# ifconfig vpn_myadapter 192.168.1.200/24
2 [root@dywftp vpnclient]# ping -c3 192.168.1.254
PING 192.168.1.254 (192.168.1.254) 56(84) bytes of data.
4 64 bytes from 192.168.1.254: icmp_seq=1 ttl=64 time=1.80 ms
64 bytes from 192.168.1.254: icmp_seq=2 ttl=64 time=0.643 ms
6 64 bytes from 192.168.1.254: icmp_seq=3 ttl=64 time=0.603 ms

8 --- 192.168.1.254 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
10 rtt min/avg/max/mdev = 0.603/1.015/1.801/0.556 ms
```

3. 在 Linux 要由 VPN server 的 DHCP 自動取得 vpn_myadapter 的 IP，可以使用 dhclient 命令。

```
[root@dywftp ~]# dhclient vpn_myadapter &
[1] 22730
[root@dywftp ~]# ifconfig vpn_myadapter
vpn_myadapter Link encap:Ethernet  HWaddr 00:AC:E8:A9:C9:4D
          inet addr:192.168.1.11  Bcast:192.168.1.255  Mask
              :255.255.255.0
          inet6 addr: fe80::2ac:e8ff:fea9:c94d/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:6701 errors:0 dropped:0 overruns:0 frame:0
          TX packets:85 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:500
          RX bytes:416312 (406.5 KiB)  TX bytes:11980 (11.6 KiB)

[1]+  Done                    dhclient vpn_myadapter
```

4. vpn_myadapter 釋出取得的 IP，可以使用 dhclient -r 命令。

```
[root@dywftp ~]# dhclient -r vpn_myadapter
[root@dywftp ~]# ifconfig vpn_myadapter
vpn_myadapter Link encap:Ethernet  HWaddr 00:AC:E8:A9:C9:4D
          BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:6786 errors:0 dropped:0 overruns:0 frame:0
          TX packets:94 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:500
          RX bytes:421539 (411.6 KiB)  TX bytes:12838 (12.5 KiB)
```

5. 當 VPN Clinet 也是在 VLAN 且網段也是 192.168.1.0/24 時.....

Chapter 23

Open VPN

23.1 前言

1. OpenVPN 是一個全功能的 SSL VPN，用於建立虛擬私人網路絡加密通道的套件。
2. OpenVPN 允許建立的 VPN 使用公開金鑰、電子憑證、或者使用者名稱／密碼來進行身分驗證。
3. 在 CentOS 6.5 安裝 OpenVPN。
4. OpenVPN Installation and configuration on CentOS 6.x

23.2 OpenVPN 套件安裝

1. 安裝套件

```
[root@dyw219 ~]# yum install openvpn easy-rsa
```

2. 在 /etc/openvpn 目錄內建立 easy-rsa 腳本次目錄，並將預設的 easy-rsa 複製到此次目錄來。

```
[root@dyw219 ~]# mkdir -p /etc/openvpn/easy-rsa/keys
[root@dyw219 ~]# cp -rf /usr/share/easy-rsa/2.0/* /etc/openvpn/easy-rsa/
```

3. 修改認證 key 的國別、單位、eamil 等資料。

```
[root@dyw219 ~]# vim /etc/openvpn/easy-rsa/vars
[root@dyw219 ~]# grep '^export KEY_COUNTRY' -A6 /etc/openvpn/easy-rsa/
    vars
export KEY_COUNTRY="TW"
export KEY_PROVINCE="Taiwan"
export KEY_CITY="Taichung"
export KEY_ORG="CYUT"
export KEY_EMAIL="dywang@csie.cyut.edu.tw"
export KEY_OU="CSIE"
```

4. 進到 /etc/openvpn/easy-rsa 目錄，建立 openssl.cnf 設定檔、讀取變數、清除所有 keys。

```
[root@dyw219 ~]# cd /etc/openvpn/easy-rsa/
[root@dyw219 easy-rsa]# cp openssl-1.0.0.cnf openssl.cnf
[root@dyw219 easy-rsa]# source ./vars
NOTE: If you run ./clean-all, I will be doing a rm -rf on /etc/openvpn/
    easy-rsa/keys
[root@dyw219 easy-rsa]# ./clean-all
```

5. 產生 CA 證書及金鑰。

```
[root@dyw219 easy-rsa]# ./build-ca
Generating a 2048 bit RSA private key
..............................+++
.....................................................+++
writing new private key to 'ca.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a
    DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [TW]:
State or Province Name (full name) [Taiwan]:
Locality Name (eg, city) [Taichung]:
Organization Name (eg, company) [CYUT]:
Organizational Unit Name (eg, section) [CSIE]:
Common Name (eg, your name or your server's hostname) [CYUT CA]:
Name [EasyRSA]:
Email Address [dywang@csie.cyut.edu.tw]:
```

6. 產生 server 的 CA 證書及金鑰。

```
[root@dyw219 easy-rsa]# ./build-key-server server
Generating a 2048 bit RSA private key
.....................................+++
.............+++
writing new private key to 'server.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a
    DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [TW]:
State or Province Name (full name) [Taiwan]:
Locality Name (eg, city) [Taichung]:
Organization Name (eg, company) [CYUT]:
Organizational Unit Name (eg, section) [CSIE]:
Common Name (eg, your name or your server's hostname) [server]:
Name [EasyRSA]:
Email Address [dywang@csie.cyut.edu.tw]:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:jdne&Gsw83A
An optional company name []:^C
[root@dyw219 easy-rsa]# ./build-key-server server
Generating a 2048 bit RSA private key
.....................................................................

.....................................................................+++

......+++
writing new private key to 'server.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a
    DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [TW]:
State or Province Name (full name) [Taiwan]:
Locality Name (eg, city) [Taichung]:
Organization Name (eg, company) [CYUT]:
Organizational Unit Name (eg, section) [CSIE]:
Common Name (eg, your name or your server's hostname) [server]:
Name [EasyRSA]:
```

```
Email Address [dywang@csie.cyut.edu.tw]:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Using configuration from /etc/openvpn/easy-rsa/openssl-1.0.0.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'TW'
stateOrProvinceName   :PRINTABLE:'Taiwan'
localityName          :PRINTABLE:'Taichung'
organizationName      :PRINTABLE:'CYUT'
organizationalUnitName:PRINTABLE:'CSIE'
commonName            :PRINTABLE:'server'
name                  :PRINTABLE:'EasyRSA'
emailAddress          :IA5STRING:'dywang@csie.cyut.edu.tw'
Certificate is to be certified until Apr 22 01:07:30 2026 GMT (3650 days
    )
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
```

7. 產生 client 的 CA 證書及金鑰。

```
[root@dyw219 easy-rsa]# ./build-key client
Generating a 2048 bit RSA private key
..................+++
.............+++
writing new private key to 'client.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a
    DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [TW]:
State or Province Name (full name) [Taiwan]:
Locality Name (eg, city) [Taichung]:
Organization Name (eg, company) [CYUT]:
Organizational Unit Name (eg, section) [CSIE]:
Common Name (eg, your name or your server's hostname) [client]:
Name [EasyRSA]:
```

```
Email Address [dywang@csie.cyut.edu.tw]:
22
Please enter the following 'extra' attributes
24 to be sent with your certificate request
A challenge password []:
26 An optional company name []:
Using configuration from /etc/openvpn/easy-rsa/openssl-1.0.0.cnf
28 Check that the request matches the signature
Signature ok
30 The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'TW'
32 stateOrProvinceName   :PRINTABLE:'Taiwan'
localityName          :PRINTABLE:'Taichung'
34 organizationName      :PRINTABLE:'CYUT'
organizationalUnitName:PRINTABLE:'CSIE'
36 commonName            :PRINTABLE:'client'
name                  :PRINTABLE:'EasyRSA'
38 emailAddress          :IA5STRING:'dywang@csie.cyut.edu.tw'
Certificate is to be certified until Apr 22 01:09:59 2026 GMT (3650 days
    )
40 Sign the certificate? [y/n]:y

42
1 out of 1 certificate requests certified, commit? [y/n]y
44 Write out database with 1 new entries
Data Base Updated
```

8. 產生 Diffie Hellman (DH) 參數，要花點時間。

```
1 [root@dyw219 easy-rsa]# ./build-dh
Generating DH parameters, 2048 bit long safe prime, generator 2
3 This is going to take a long time
.............................+.
```

9. 進入 /etc/openvpn/easy-rsa/keys，將 dh2048.pem ca.crt server.crt server.key 四個檔案複製到 /etc/openvpn 目錄。

```
[root@dyw219 easy-rsa]# cd /etc/openvpn/easy-rsa/keys/
2 [root@dyw219 keys]# cp dh2048.pem ca.crt server.crt server.key /etc/
    openvpn/
```

23.3 Client 安裝與設定

1. 登入 VPN client

```
[root@dyw219 ~]# ssh 192.168.1.102
root@192.168.1.102's password:
Last login: Sat Mar 19 18:10:38 2016 from gateway
[root@oveng ~]#
```

2. 安裝 openvpn。

```
[root@oveng ~]# vim /etc/yum.repos.d/dywang.repo
[root@oveng ~]# yum install openvpn --enablerepo=dywang
```

3. 回到 openvpn server 將 ca.crt client.crt client.key 三個檔案複製到 client 的 /etc/openvpn 目錄。

```
[root@dyw219 ~]# cd /etc/openvpn/easy-rsa/keys/
[root@dyw219 keys]# scp ca.crt client.crt client.key 192.168.1.102:/etc/
    openvpn/
root@192.168.1.102's password:
ca.crt                                        100% 1708     1.7KB/s
    00:00
client.crt                                    100% 5334     5.2KB/s
    00:00
client.key                                    100% 1708     1.7KB/s
    00:00
```

23.4 OpenVPN server 設定

1. 編輯 server.conf 取消註解或修改如下：

```
[root@dyw219 keys]# vim /etc/openvpn/server.conf
[root@dyw219 keys]# egrep "^(dh|push|user|group)" /etc/openvpn/server.
    conf
dh dh2048.pem
push "redirect-gateway def1 bypass-dhcp"
```

```
push "dhcp-option DNS 192.168.1.254"
push "dhcp-option DNS 8.8.8.8"
user nobody
group nobody
```

2. 複製 client.conf 到 /home 目錄下，並設定 vpn server IP 爲 192.168.1.254。

```
[root@dyw219 keys]# cp /usr/share/doc/openvpn-2.3.0/sample-config-files/
    client.conf /home/

[root@dyw219 keys]# vim /home/client.conf
[root@dyw219 keys]# grep ^remote /home/client.conf
remote 192.168.1.254 1194
```

3. 將更改後的 client.conf 複製到遠端 client 的 /etc/openvpn 目錄。

```
[root@dyw219 keys]# scp /home/client.conf 192.168.1.102:/etc/openvpn/
```

4. 查看 prosody 服務預設的 ports。

```
[root@kvm8 ~]# netstat -tlunp | grep lua
tcp    0    0 0.0.0.0:5269        0.0.0.0:*    LISTEN      28232/lua
tcp    0    0 127.0.0.1:5347      0.0.0.0:*    LISTEN      28232/lua
tcp    0    0 0.0.0.0:5222        0.0.0.0:*    LISTEN      28232/lua
```

5. 防火牆 iptables 必須開啓 5269,5347,5222 等埠號。

23.5 問題解決

1. 連線時 server 端的 DNS 無效，可直接在 Clinet 修改設定。

```
[root@dywnb ~]# vim /etc/resolv.conf
```