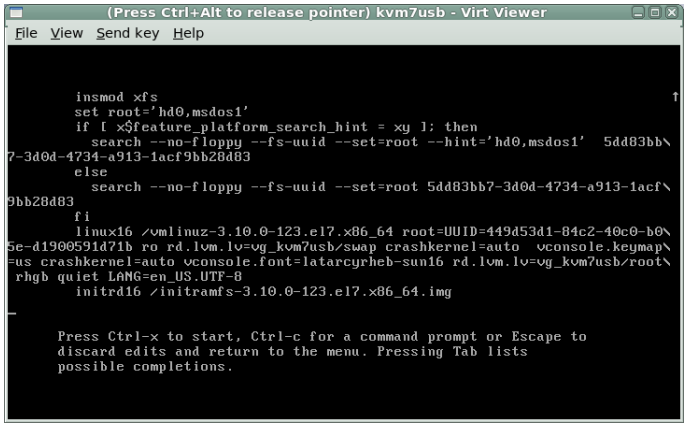
RHEL/CentOS 7

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

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



December 4, 2015

- Instructor: De-Yu Wang
    1. Email: dywang@csie.cyut.edu.tw
    2. Homepage: http://dywang.csie.cyut.edu.tw
    3. Phone: (04)23323000 ext 4538
    4. Office: E738
- 參考資料
    1. RedHat Documentation
    2. RedHat Customer Protal

Contents

Chapter 1

rhel v6 vs. v7 開機

1.1 系統維護

1. Linux 出現開機問題或忘記 root 密碼時，必須進入維護模式。

1.2 v6 變更密碼

1. v6 開關機層級分爲 0,1,2,3,4,5,6 等層級，維護模式是在開機時在 grub 的 kernel 參數中指定開機進入單人模式，也就是層級 1，就可免 root 密碼進入系統互動式命令模式。

2. v6 變更 root 密碼方式一：

   (a) 出現 grub boot loader 開機選單時，立即碰觸鍵盤任意鍵，boot loader 會暫停。

   (b) 按下'e'，編輯選單

   (c) 移動上下鍵至核心設定行

```
1 kernel /vmlinuz-2.6.32-71.el6.x86_64 ro root=/dev/mapper/
     vgsrv-root ... quiet
```

   (d) 按下'e'，進入編輯模式，在 quiet 後空一格加入 1

   (e) 再按下[enter]，結束編輯模式

   (f) 按下'b'，重新開機進入單入維護模式

   (g) 開機後不必輸入帳密就已登入爲 root，只要執行 passwd 直接更改 root 密碼即可。

```
[root@kvm8 /]# passwd
```

3. v6 變更 root 密碼方式二：

   (a) 出現 grub boot loader 開機選單時，立即碰觸鍵盤任意鍵，boot loader會暫停。

   (b) 按下'a'，直接編輯核心

```
kernel /vmlinuz-2.6.32-71.el6.x86_64 ro root=/dev/mapper/
    vgsrv-root ... quiet
```

   (c) 在最後加一空格及 1

   (d) 再按下[enter]重新開機

   (e) 開機後不必輸入帳密就已登入爲 root，只要執行 passwd 直接更改 root 密碼即可。

```
[root@kvm8 /]# passwd
```

4. 單人模式變更密碼，若出現以下訊息，表示 SELinux 管制密碼變更。

```
[root@kvm8 /]# passwd
type=1400 audit(1323777256.565:29): avc: denied { read } for
pid=1912 comm="passwd" path="pipe:[12939]" dev=pipefs ino=12939
....
....
```

5. 可以使用 echo 方式變更密碼。

```
[root@kvm8 /]# echo "123123" | passwd --stdin
type=1300 audit(1323777556.699:32): avc: denied { read } for
pid=1916 comm="passwd" path="pipe:[12939]" dev=pipefs ino=12939
....
....
```

6. 或先關閉 SELinux，再變更密碼，雖依然出現警告訊息，但已可以變更 root 密碼。

```
[root@kvm8 /]# setenforce 0 關閉 <== selinux
type=1404 audit(1323777769.894:4): enforcing=0 old_enforcing=1
audit=4294967295 ses=4294967295
[root@kvm8 /]# passwd
type=1400 audit(1323777776.973:5): avc: denied { read } for
pid=887 comm="passwd" path="pipe:[10230]" dev=pipefs ino=10230
....
Changing password for user root.
New password:
BAD PASSWORD: it does not contain enough DIFFERENT characters
BAD PASSWORD: is too simple
Retype new password:
passwd: all authentication tokens updated successfully.
```

7. 建議做法是直接在開機選單關閉 SELinux。

```
grub edit> kernel /vmlinuz-2.6.18-92.el5 ro root=LABEL=/ rhgb
   quiet selinux=0 1
```

1.3 v7 開機 target

1. v7 開機不分層級，而是分成 4 個目標 target，其開機結果如下表：

Target	Purpose
graphical.target	多人模式，支援圖形及文字兩種方式登入，等效 v6 的層級 3 及 5。
multi-user.target	多人模式，只支援文字登入方式，等效 v6 的層級 3。
rescue.target	sulogin (Single-user login)，單人模式，等效 v6 的層級 1。
emergency.target	sulogin ，單人模式，完成 initramfs 載入且系統根目錄 / 掛載成唯讀，等效 v6 開機掛載不成功時的維修模式。

2. v7 指定 target 開機：

   (a) 出現 grub boot loader 開機選單時，立即碰觸鍵盤任意鍵，boot loader 會暫停。

   (b) 按下'e'，編輯選單

(c) 移動上下鍵至 linux16 核心命令行

```
linux16 /vmlinuz-3.10.0-123.el7.x86_64 \
root=UUID=449d53d1-84c2-40c0-b05e-d1900591d71b ro \
rd.lvm.lv=vg_kvm7usb/swap crashkernel=auto  \
vconsole.keymap=us crashkernel=auto \
vconsole.font=latarcyrheb-sun16 \
rd.lvm.lv=vg_kvm7usb/root rhgb quiet LANG=en_US.UTF-8
```

(d) 在核心命令行最後加入 systemd.unit=desired.target (desired 爲上表中四種 target 之一)。

(e) 再按下 Ctrl+x 重新以這個設定開機。

1.4 v7 變更密碼

1. v7 無論使用那種「目標」開機，都必須輸入帳號及密碼才能進入互動式命令模式。因此 v7 變更 root 密碼，必須先中斷開機流程，不要讓流程完成 initramfs 載入並控制系統。

   (a) 出現 grub boot loader 開機選單時，立即碰觸鍵盤任意鍵，boot loader 會暫停。

   (b) 按下'e'，編輯選單

   (c) 移動上下鍵至 linux16 核心命令行

```
linux16 /vmlinuz-3.10.0-123.el7.x86_64 \
root=UUID=449d53d1-84c2-40c0-b05e-d1900591d71b ro \
rd.lvm.lv=vg_kvm7usb/swap crashkernel=auto  \
vconsole.keymap=us crashkernel=auto \
vconsole.font=latarcyrheb-sun16 \
rd.lvm.lv=vg_kvm7usb/root rhgb quiet LANG=en_US.UTF-8
```

   (d) 在核心命令行最後加入 rd.break 。

   (e) 再按下 Ctrl+x 重新以這個設定開機。

2. 開機後的互動式命令環境，並不是正常開機的系統，正常開機系統掛載在 /sysboot，且掛載成唯讀，必須重新掛載成可寫入，才能變更密碼，步驟如下：

   (a) 重新掛載 /sysroot 成可讀可寫。

```
switch_root:/# mount -oremount,rw /sysroot
```

(b) chroot 工作目錄到 /sysroot。

```
switch_root:/# chroot /sysroot
```

(c) 設定新的 root 密碼。

```
sh-4.2# passwd
```

(d) 因爲在此情況下，SELinux 並沒有啓動，對所有檔案的變更，可能會造成檔案的 context 不正確，爲確保開機時重新設定 SELinux context，必須在根目錄下產生隱藏檔 .autorelabel。

```
sh-4.2# touch /.autorelabel
```

(e) 退出 chroot

```
sh-4.2# exit
switch_root:/#
```

(f) 退出系統，即重新開機。

```
switch_root:/# exit
```

3. 忘記密碼操作示範

1.5 v7 console resolution

1. v7 開機預設爲文字界面，且 console 解析度預設爲 1280x1024，佔據整個螢幕，且縮小後字型跟著縮小，使用上很不方便。修改終端機解析度，可以開機時修改 kernel 參數，加入 `video= XRES x YRES`。

(a) 出現 grub boot loader 開機選單時，立即碰觸鍵盤任意鍵，boot loader 會暫停。

(b) 按下'e'，編輯選單

(c) 移動上下鍵至 linux16 核心命令行

```
linux16 /vmlinuz-3.10.0-123.el7.x86_64 \
root=UUID=449d53d1-84c2-40c0-b05e-d1900591d71b ro \
rd.lvm.lv=vg_kvm7usb/swap crashkernel=auto  \
vconsole.keymap=us crashkernel=auto \
vconsole.font=latarcyrheb-sun16 \
rd.lvm.lv=vg_kvm7usb/root rhgb quiet LANG=en_US.UTF-8
```

(d) 在核心命令行最後加入 video=720x400。

(e) 再按下 Ctrl+x 重新以這個設定開機。

2. 不過還是建議直接修改開機選單。

```
[root@kvm7 ~]# vim /boot/grub2/grub.cfg
[root@kvm7 ~]# grep video= /boot/grub2/grub.cfg
    linux16 /vmlinuz-3.10.0-123.el7.x86_64 \
root=UUID=10949263-987a-44e1-b0dc-05ff2d9bc4f9 \
ro rd.lvm.lv=vg_kvm7usb/swap crashkernel=auto  vconsole.keymap=us
     \
crashkernel=auto vconsole.font=latarcyrheb-sun16 rd.lvm.lv=
   vg_kvm7usb/root \
rhgb quiet LANG=en_US.UTF-8 video=720x400
```

3. 變更終端機螢幕解析度操作示範

Chapter 2

Bash_completion

2.1 前言

1. Linux 文字命令介面中，[TAB] 鍵是一個非常好用的功能，可以提示或補齊命令或檔案參數。

2. RHEL/CentOS 7 版本再新增命令選項及參數提示及補齊的功能，對於命令的使用將更爲方便。

2.2 安裝與使用

1. 安裝 bash-completion 套件。

```
[root@kvm7 ~]# yum install bash-completion
```

2. 重新讀取用户登入設定，否則必須先退出連線，再登入才生效。

```
[root@kvm7 ~]# source /etc/profile
```

3. 不重新讀取用户登入設定，必須先退出連線，再登入才生效。

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

4. 再重新登入。

```
[root@dywH ~]# ssh kvm7.deyu.wang
root@kvm7.deyu.wang's password:
Warning: No xauth data; using fake authentication data for X11
    forwarding.
Last login: Fri Aug 15 23:16:06 2014 from 192.168.122.1
[root@kvm7 ~]#
```

5. 下命令 yum，動作命令 in，提示有 info 及 install 兩種命令。

```
[root@kvm7 ~]# yum in[TAB][TAB]
info     install
```

6. 下命令 yum，動作命令 install，套件參數 ba 提示有 10 種可能。

```
[root@kvm7 ~]# yum info ba[TAB][TAB]
babel.noarch            bacula-common.x86_64    bash-completion.
    noarch
babl.i686               bacula-libs.x86_64      bash.x86_64
babl.x86_64             baobab.x86_64
bacula-client.x86_64    basesystem.noarch
```

Chapter 3

systemctl 系統服務控制

3.1 前言

1. v6 PID=1 是 init。
2. v7 PID=1 是 systemd，其優點有：
   (a) 平行處理能力，增加開機速度。
   (b) 自動服務相依管理，避免過久的 timeout，例如：網路不通時，就不會像 v6 還試圖連上網路。

3.2 systemctl 命令

1. systemctl 命令用來管理各種不同型態的 systemd 物件。

```
[root@kvm7 ~]# systemctl -t help
Available unit types:
service
socket
target
device
mount
automount
snapshot
timer
swap
path
slice
scope
```

2. systemctl 輔助說明

```
[root@kvm7 ~]# systemctl --help
systemctl [OPTIONS...] {COMMAND} ...

Query or send control commands to the systemd manager.

  -h --help           Show this help
     --version        Show package version
  -t --type=TYPE      List only units of a particular type
     --state=STATE    List only units with particular LOAD or SUB
         or ACTIVE stat
  -p --property=NAME  Show only properties by this name
  -a --all            Show all loaded units/properties, including
      dead/empty
                      ones. To list all units installed on the
                         system, use
                      the 'list-unit-files' command instead.
     --reverse        Show reverse dependencies with 'list-
        dependencies'
  -l --full           Don't ellipsize unit names on output
     --fail           When queueing a new job, fail if
        conflicting jobs are
                      pending
     --irreversible   When queueing a new job, make sure it
        cannot be implicitly
                      cancelled
     --ignore-dependencies
                      When queueing a new job, ignore all its
                         dependencies
     --show-types     When showing sockets, explicitly show their
          type
  -i --ignore-inhibitors
                      When shutting down or sleeping, ignore
                         inhibitors
     --kill-who=WHO   Who to send signal to
  -s --signal=SIGNAL  Which signal to send
  -H --host=[USER@]HOST
                      Show information for remote host
  -P --privileged     Acquire privileges before execution
  -q --quiet          Suppress output
     --no-block       Do not wait until operation finished
     --no-wall        Don't send wall message before halt/power-
        off/reboot
     --no-reload      When enabling/disabling unit files, don't
        reload daemon
                      configuration
     --no-legend      Do not print a legend (column headers and
        hints)
     --no-pager       Do not pipe output into a pager
     --no-ask-password
                      Do not ask for system passwords
     --system         Connect to system manager
```

```
40      --user           Connect to user service manager
        --global         Enable/disable unit files globally
42      --runtime        Enable unit files only temporarily until
            next reboot
    -f --force           When enabling unit files, override existing
         symlinks
44                       When shutting down, execute action
                             immediately
        --root=PATH      Enable unit files in the specified root
            directory
46    -n --lines=INTEGER  Number of journal entries to show
    -o --output=STRING  Change journal output mode (short, short-
        monotonic,
48                       verbose, export, json, json-pretty, json-
                             sse, cat)
        --plain          Print unit dependencies as a list instead
            of a tree
50
  Unit Commands:
52    list-units                      List loaded units
    list-sockets                      List loaded sockets ordered by
        address
54    start [NAME...]                 Start (activate) one or more
        units
    stop [NAME...]                    Stop (deactivate) one or more
        units
56    reload [NAME...]                Reload one or more units
    restart [NAME...]                 Start or restart one or more
        units
58    try-restart [NAME...]           Restart one or more units if
        active
    reload-or-restart [NAME...]       Reload one or more units if
        possible,
60                                    otherwise start or restart
    reload-or-try-restart [NAME...] Reload one or more units if
        possible,
62                                    otherwise restart if active
    isolate [NAME]                    Start one unit and stop all
        others
64    kill [NAME...]                  Send signal to processes of a
        unit
    is-active [NAME...]               Check whether units are active
66    is-failed [NAME...]             Check whether units are failed
    status [NAME...|PID...]           Show runtime status of one or
        more units
68    show [NAME...|JOB...]           Show properties of one or more
                                      units/jobs or the manager
70    set-property [NAME] [ASSIGNMENT...]
                                      Sets one or more properties of
                                          a unit
72    help [NAME...|PID...]           Show manual for one or more
```

```
    units
  reset-failed [NAME...]          Reset failed state for all, one
    , or more
                                  units
  list-dependencies [NAME]        Recursively show units which
    are required
                                  or wanted by this unit or by
                                     which this
                                  unit is required or wanted

Unit File Commands:
  list-unit-files                 List installed unit files
  enable [NAME...]                Enable one or more unit files
  disable [NAME...]               Disable one or more unit files
  reenable [NAME...]              Reenable one or more unit files
  preset [NAME...]                Enable/disable one or more unit
     files
                                  based on preset configuration
  is-enabled [NAME...]            Check whether unit files are
    enabled

  mask [NAME...]                  Mask one or more units
  unmask [NAME...]                Unmask one or more units
  link [PATH...]                  Link one or more units files
    into
                                  the search path
  get-default                     Get the name of the default
    target
  set-default NAME                Set the default target

Job Commands:
  list-jobs                       List jobs
  cancel [JOB...]                 Cancel all, one, or more jobs

Snapshot Commands:
  snapshot [NAME]                 Create a snapshot
  delete [NAME...]                Remove one or more snapshots

Environment Commands:
  show-environment                Dump environment
  set-environment [NAME=VALUE...] Set one or more environment
    variables
  unset-environment [NAME...]     Unset one or more environment
    variables

Manager Lifecycle Commands:
  daemon-reload                   Reload systemd manager
    configuration
  daemon-reload                   Reload systemd manager
    configuration
  daemon-reexec                   Reexecute systemd manager
```

```
112
System Commands:
114   default                          Enter system default mode
      rescue                           Enter system rescue mode
116   emergency                        Enter system emergency mode
      halt                             Shut down and halt the system
118   poweroff                         Shut down and power-off the
          system
      reboot                           Shut down and reboot the system
120   kexec                            Shut down and reboot the system
          with kexec
      exit                             Request user instance exit
122   switch-root [ROOT] [INIT]        Change to a different root file
          system
      suspend                          Suspend the system
124   hibernate                        Hibernate the system
      hybrid-sleep                     Hibernate and suspend the
          system
```

3.3 服務啓動

1. 查看服務 postfix 狀態，目前爲 active，正在執行中。

```
1  [root@kvm7 ~]# systemctl status postfix.service
   postfix.service - Postfix Mail Transport Agent
3     Loaded: loaded (/usr/lib/systemd/system/postfix.service;
          enabled)
      Active: active (running) since Fri 2014-08-15 21:05:20 CST; 1
          min 6s ago
5    Process: 2691 ExecStop=/usr/sbin/postfix stop (code=exited,
         status=0/SUCCESS)
     Process: 2705 ExecStart=/usr/sbin/postfix start (code=exited,
         status=0/SUCCESS)
7    Process: 2703 ExecStartPre=/usr/libexec/postfix/chroot-update (
         code=exited, status=0/SUCCESS)
     Process: 2700 ExecStartPre=/usr/libexec/postfix/aliasesdb (code
         =exited, status=0/SUCCESS)
9   Main PID: 2777 (master)
      CGroup: /system.slice/postfix.service ├─
11            2777 /usr/libexec/postfix/master -w ├─
              2778 pickup -l -t unix -u └─
13            2779 qmgr -l -t unix -u

15 Aug 15 21:05:20 kvm7.deyu.wang systemd[1]: Starting Postfix Mail
       Transport A....
```

```
Aug 15 21:05:20 kvm7.deyu.wang postfix/master[2777]: daemon
    started -- versio...
Aug 15 21:05:20 kvm7.deyu.wang systemd[1]: Started Postfix Mail
    Transport Agent.
Hint: Some lines were ellipsized, use -l to show in full.
```

2. 關閉服務 postfix。

```
[root@kvm7 ~]# systemctl stop postfix.service
```

3. 查看服務 postfix 狀態，目前爲 inactive，關閉中。

```
[root@kvm7 ~]# systemctl status postfix.service
postfix.service - Postfix Mail Transport Agent
   Loaded: loaded (/usr/lib/systemd/system/postfix.service;
       enabled)
   Active: inactive (dead) since Fri 2014-08-15 21:04:09 CST; 10s
        ago
  Process: 2585 ExecStop=/usr/sbin/postfix stop (code=exited,
      status=0/SUCCESS)
  Process: 1491 ExecStart=/usr/sbin/postfix start (code=exited,
      status=0/SUCCESS)
  Process: 1486 ExecStartPre=/usr/libexec/postfix/chroot-update (
      code=exited, status=0/SUCCESS)
  Process: 1235 ExecStartPre=/usr/libexec/postfix/aliasesdb (code
      =exited, status=0/SUCCESS)
 Main PID: 2134 (code=killed, signal=TERM)

Aug 15 17:51:48 kvm7.deyu.wang systemd[1]: Starting Postfix Mail
    Transport A....
Aug 15 17:51:50 kvm7.deyu.wang postfix/master[2134]: daemon
    started -- versio...
Aug 15 17:51:50 kvm7.deyu.wang systemd[1]: Started Postfix Mail
    Transport Agent.
Aug 15 21:04:09 kvm7.deyu.wang systemd[1]: Stopping Postfix Mail
    Transport A....
Aug 15 21:04:09 kvm7.deyu.wang systemd[1]: Stopped Postfix Mail
    Transport Agent.
Hint: Some lines were ellipsized, use -l to show in full.
```

4. 查看服務 postfix 目前是否啓動？結果爲 inactive。

```
[root@kvm7 ~]# systemctl is-active postfix.service
inactive
```

5. 啓動服務 postfix。

```
[root@kvm7 ~]# systemctl start postfix.service
```

6. 再查看服務 postfix 目前是否啓動？結果爲 active。

```
[root@kvm7 ~]# systemctl is-active postfix.service
active
```

7. 也可以用 restart 選項，重新啓動服務 postfix。

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

8. 再查看服務 postfix 目前是否啓動？結果爲 active。

```
[root@kvm7 ~]# systemctl is-active postfix.service
active
```

3.4 開機自動啓動服務

1. 查看服務 postfix 開機是否自動啓動？結果爲 enabled。

```
[root@kvm7 ~]# systemctl is-enabled postfix.service
enabled
```

2. 關閉服務 postfix 開機自動啓動。

```
[root@kvm7 ~]# systemctl disable postfix.service
rm '/etc/systemd/system/multi-user.target.wants/postfix.service'
```

3. 再查看服務 postfix 開機是否自動啓動？結果爲 disabled。

```
[root@kvm7 ~]# systemctl is-enabled postfix.service
disabled
```

4. 再啓動服務 postfix 開機自動啓動。

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

5. 再查看服務 postfix 開機是否自動啓動？結果爲 enabled。

```
[root@kvm7 ~]# systemctl is-enabled postfix.service
enabled
```

3.5 永久關閉服務

1. mask 服務 postfix，使這個服務無論開機或手動都無法啓動。

```
[root@kvm7 ~]# systemctl mask postfix.service
ln -s '/dev/null' '/etc/systemd/system/postfix.service'
```

2. 啓動服務 postfix。

```
[root@kvm7 ~]# systemctl enable postfix.service
```

3. 查看服務 postfix 是否啓動，結果爲 masked。

```
[root@kvm7 ~]# systemctl is-enabled postfix.service
masked
```

4. unmask 服務 postfix，解除這個服務的鎖定。

```
[root@kvm7 ~]# systemctl unmask postfix.service
rm '/etc/systemd/system/postfix.service'
```

5. 再查看服務 postfix 是否啓動，結果爲 enabled。

```
[root@kvm7 ~]# systemctl is-enabled postfix.service
enabled
```

3.6 失效的服務

1. 查看失效的服務。

```
[root@kvm7 ~]# systemctl --failed --type=service
UNIT          LOAD   ACTIVE SUB    DESCRIPTION
kdump.service loaded failed failed Crash recovery kernel arming
rhnsd.service loaded failed failed LSB: Starts the Spacewalk
    Daemon

LOAD   = Reflects whether the unit definition was properly loaded
    .
ACTIVE = The high-level unit activation state, i.e.
    generalization of SUB.
SUB    = The low-level unit activation state, values depend on
    unit type.

2 loaded units listed. Pass --all to see loaded but inactive
    units, too.
To show all installed unit files use 'systemctl list-unit-files'.
```

Chapter 4

IPv4 網路設定

4.1 前言

1. 網路 (網路介面) 卡由系統 daemon NetworkManager 管理，包含：
   (a) device: 網路卡。
   (b) connection: 設定網卡。
   (c) 每一個 connection 都有一個名字或 ID 做爲識別。
   (d) 目錄 /etc/sysconfig/network-scripts 下 ifcfg-name 爲網卡 name 的設定檔，可以使用命令 nmcli 產生或編輯網卡連線 (connection)。
   (e) /etc/sysconfig/network-scripts/ifcfg-name 網卡設定檔，還可以跟 v6 版本一樣，直接以 vim 手動編輯。

4.2 nmcli 命令

1. 查看 device 狀態，除了 lo 以外，只有一個網路介面 ens3。

```
[root@kvm7 ~]# nmcli device status
DEVICE  TYPE      STATE      CONNECTION
ens3    ethernet  connected  ens3
lo      loopback  unmanaged  --
```

2. 查詢網路連線狀態。

```
[root@kvm7 ~]# nmcli connection show
NAME  UUID                                  TYPE
   DEVICE
ens3  2e37720d-f8f8-4180-bdb4-de34bf50ca49  802-3-ethernet  ens3
```

3. 查詢網路連線狀態，只列出 active 的網路介面。

```
[root@kvm7 ~]# nmcli connection show --active
NAME  UUID                                  TYPE
   DEVICE
ens3  2e37720d-f8f8-4180-bdb4-de34bf50ca49  802-3-ethernet  ens3
```

4. 查詢網路介面 ens3 的 ip，此網卡有 192.168.122.9 及 192.168.122.7 兩個 ip。

```
[root@kvm7 ~]# ip addr show ens3
2: ens3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc
   pfifo_fast state UP qlen 1000
    link/ether 52:54:00:b4:0a:a3 brd ff:ff:ff:ff:ff:ff
    inet 192.168.122.9/24 brd 192.168.122.255 scope global
       dynamic ens3
       valid_lft 2393sec preferred_lft 2393sec
    inet 192.168.122.7/24 brd 192.168.122.255 scope global
       secondary ens3
       valid_lft forever preferred_lft forever
    inet6 fe80::5054:ff:feb4:aa3/64 scope link
       valid_lft forever preferred_lft forever
```

4.3 nmcli 修改網卡設定

1. 查看網路設定，也就是網卡設定，目前只有 eht0 一個網路設定。

```
[root@777777 ~]# nmcli connection show
NAME  UUID                                  TYPE
   DEVICE
eth0  5a0ff824-0615-4fce-86c4-ad3e73e26c61  802-3-ethernet  eth0
```

2. 不必刪除設定，直接使用 modify 選項變更設定。設定 ipv4 位址 192.168.122.7、遮罩 255.255.255.0、DNS 192.168.122.1，最後一定要設定 ipv4.method 爲 manual，將網路連線設定爲手動，也就是自行設定 IP，不是由 DHCP 自動取得，否則原 DHCP 取得的 IP 還會存在。

```
[root@777777 ~]# nmcli connection modify eth0 \
ipv4.addresses 192.168.122.7/24 \
ipv4.gateway 192.168.122.1 \
ipv4.dns 192.168.122.1 \
ipv4.method manual
```

3. 重新啓動網路。

```
[root@777777 ~]# systemctl restart network.service
```

4. 查看網卡設定，看手動設定是否正確？

```
[root@777777 ~]# nmcli connection show eth0 | egrep -i ipv?4
ipv4.method:                            manual
ipv4.dns:                               192.168.122.1
ipv4.dns-search:
ipv4.addresses:                         192.168.122.7/24
ipv4.gateway:                           192.168.122.1
ipv4.routes:
ipv4.route-metric:                      -1
ipv4.ignore-auto-routes:                no
ipv4.ignore-auto-dns:                   no
ipv4.dhcp-client-id:                    --
ipv4.dhcp-send-hostname:                yes
ipv4.dhcp-hostname:                     --
ipv4.never-default:                     no
ipv4.may-fail:                          yes
IP4.ADDRESS[1]:                         192.168.122.7/24
IP4.GATEWAY:                            192.168.122.1
IP4.DNS[1]:                             192.168.122.1
```

4.4 *nmcli 設定網卡

1. 查看網卡，除了 lo 外，有一張網卡 ens3。

```
[root@kvm7 ~]# nmcli device show
GENERAL.DEVICE:                         ens3
GENERAL.TYPE:                           ethernet
GENERAL.HWADDR:                         52:54:00:B4:0A:A3
```

```
GENERAL.MTU:                            1500
GENERAL.STATE:                          30 (disconnected)
GENERAL.CONNECTION:                     --
GENERAL.CON-PATH:                       --
WIRED-PROPERTIES.CARRIER:               on

GENERAL.DEVICE:                         lo
GENERAL.TYPE:                           loopback
GENERAL.HWADDR:                         00:00:00:00:00:00
GENERAL.MTU:                            65536
GENERAL.STATE:                          10 (unmanaged)
GENERAL.CONNECTION:                     --
GENERAL.CON-PATH:                       --
IP4.ADDRESS[1]:                         ip = 127.0.0.1/8, gw =
    0.0.0.0
IP6.ADDRESS[1]:                         ip = ::1/128, gw = ::
```

2. 查詢 ens3 網卡設定爲 dhcp。

```
[root@kvm7 ~]# cat /etc/sysconfig/network-scripts/ifcfg-ens3
TYPE=Ethernet
BOOTPROTO=dhcp
DEFROUTE=yes
PEERDNS=yes
PEERROUTES=yes
IPV4_FAILURE_FATAL=no
IPV6INIT=yes
IPV6_AUTOCONF=yes
IPV6_DEFROUTE=yes
IPV6_PEERDNS=yes
IPV6_PEERROUTES=yes
IPV6_FAILURE_FATAL=no
NAME=ens3
UUID=e08e9bff-28d9-4ee3-8215-034a103a474e
DEVICE=ens3
ONBOOT=yes
```

3. 刪除 ens3 網卡的連線，實際上是刪除網卡設定檔 /etc/sysconfig/network-script/ifcfg-ens3。

```
[root@kvm7 ~]# nmcli connection delete ens3
[root@kvm7 ~]# cat /etc/sysconfig/network-scripts/ifcfg-ens3
cat: /etc/sysconfig/network-scripts/ifcfg-ens3: No such file or
    directory
```

4. 增加 ens3 網卡的連線 ip 192.168.122.7，遮罩 255.255.255.0，閘道 192.168.122.1。

```
[root@kvm7 ~]# nmcli connection add con-name ens3 type ethernet
    ifname ens3 ip4 192.168.122.7/24 gw4 192.168.122.1
Connection 'ens3' (69bf76bb-71d3-4704-8b04-f09e21d9796d)
    successfully added.
```

5. 實際上是編輯網卡設定檔 /etc/sysconfig/network-script/ifcfg-ens3。

```
[root@kvm7 ~]# cat /etc/sysconfig/network-scripts/ifcfg-ens3
TYPE=Ethernet
BOOTPROTO=none
IPADDR0=192.168.122.7
PREFIX0=24
GATEWAY0=192.168.122.1
DEFROUTE=yes
IPV4_FAILURE_FATAL=no
IPV6INIT=yes
IPV6_AUTOCONF=yes
IPV6_DEFROUTE=yes
IPV6_PEERDNS=yes
IPV6_PEERROUTES=yes
IPV6_FAILURE_FATAL=no
NAME=ens3
UUID=69bf76bb-71d3-4704-8b04-f09e21d9796d
DEVICE=ens3
ONBOOT=yes
inactive
```

6. 成功啓動 ens3 網卡的連線。

```
[root@kvm7 ~]# nmcli connection up ens3
Connection successfully activated (D-Bus active path: /org/
    freedesktop/NetworkManager/ActiveConnection/2)
```

7. 查看 ens3 ip 與設定相同。

```
[root@kvm7 ~]# ip addr show ens3
2: ens3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc
   pfifo_fast state UP qlen 1000
    link/ether 52:54:00:b4:0a:a3 brd ff:ff:ff:ff:ff:ff
4   inet 192.168.122.7/24 brd 192.168.122.255 scope global ens3
       valid_lft forever preferred_lft forever
6   inet6 fe80::5054:ff:feb4:aa3/64 scope link
       valid_lft forever preferred_lft forever
```

8. 查看 ens3 連線詳細狀況，其中 DNS 沒設定。

```
1  [root@kvm7 ~]# nmcli connection show ens3
   connection.id:                          ens3
3  connection.uuid:                        69bf76bb-71d3-4704-8b04-
   f09e21d9796d
   connection.interface-name:              ens3
5  connection.type:                        802-3-ethernet
   connection.autoconnect:                 yes
7  connection.timestamp:                   1408114329
   connection.read-only:                   no
9  connection.permissions:
   connection.zone:                        --
11 connection.master:                      --
   connection.slave-type:                  --
13 connection.secondaries:
   connection.gateway-ping-timeout:        0
15 802-3-ethernet.port:                    --
   802-3-ethernet.speed:                   0
17 802-3-ethernet.duplex:                  --
   802-3-ethernet.auto-negotiate:          yes
19 802-3-ethernet.mac-address:             --
   802-3-ethernet.cloned-mac-address:      --
21 802-3-ethernet.mac-address-blacklist:
   802-3-ethernet.mtu:                     auto
23 802-3-ethernet.s390-subchannels:
   802-3-ethernet.s390-nettype:            --
25 802-3-ethernet.s390-options:
   ipv4.method:                            manual
27 ipv4.dns:
   ipv4.dns-search:
29 ipv4.addresses:                         { ip = 192.168.122.7/24,
   gw = 192.168.122.1 }
   ipv4.routes:
31 ipv4.ignore-auto-routes:                no
   ipv4.ignore-auto-dns:                   no
```

```
ipv4.dhcp-client-id:                    --
ipv4.dhcp-send-hostname:                yes
ipv4.dhcp-hostname:                     --
ipv4.never-default:                     no
ipv4.may-fail:                          yes
ipv6.method:                            auto
ipv6.dns:
ipv6.dns-search:
ipv6.addresses:
ipv6.routes:
ipv6.ignore-auto-routes:                no
ipv6.ignore-auto-dns:                   no
ipv6.never-default:                     no
ipv6.may-fail:                          yes
ipv6.ip6-privacy:                       -1 (unknown)
ipv6.dhcp-hostname:                     --
GENERAL.NAME:                           ens3
GENERAL.UUID:                           69bf76bb-71d3-4704-8b04-
    f09e21d9796d
GENERAL.DEVICES:                        ens3
GENERAL.STATE:                          activated
GENERAL.DEFAULT:                        yes
GENERAL.DEFAULT6:                       no
GENERAL.VPN:                            no
GENERAL.ZONE:                           --
GENERAL.DBUS-PATH:                      /org/freedesktop/
    NetworkManager/ActiveConnection/2
GENERAL.CON-PATH:                       /org/freedesktop/
    NetworkManager/Settings/6
GENERAL.SPEC-OBJECT:                    --
GENERAL.MASTER-PATH:                    --
IP4.ADDRESS[1]:                         ip = 192.168.122.7/24, gw
     = 192.168.122.1
IP6.ADDRESS[1]:                         ip = fe80::5054:ff:feb4:
    aa3/64, gw = ::
active
```

9. ens3 連線設定 dns 192.168.122.1。

```
[root@kvm7 ~]# nmcli connection modify ens3 ipv4.dns
    192.168.122.1
```

10. 設定 dns 後，可以再次啓動 ens3 網卡的連線，以確保 dns 生效。

```
[root@kvm7 ~]# nmcli connection up ens3
Connection successfully activated (D-Bus active path: /org/
    freedesktop/NetworkManager/ActiveConnection/2)
```

11. 再查看 ipv4 的 DNS 爲 192.168.122.1。

```
[root@kvm7 ~]# nmcli connection show ens3 | grep dns
ipv4.dns:                               192.168.122.1
ipv4.dns-search:
ipv4.ignore-auto-dns:                   no
ipv6.dns:
ipv6.dns-search:
ipv6.ignore-auto-dns:                   no
```

12. 設定網路連線度操作示範

4.5 主機名稱設定

1. 查看主機名稱爲 kvm7.deyu.wang。

```
[root@kvm7 ~]# hostname
kvm7.deyu.wang
```

2. 設定主機名稱爲 kvm5.deyu.wang。

```
[root@kvm7 ~]# hostnamectl set-hostname kvm5.deyu.wang
```

3. 查看主機名稱狀態。

```
[root@kvm7 ~]# hostnamectl status
   Static hostname: kvm5.deyu.wang
         Icon name: computer-vm
           Chassis: vm
        Machine ID: f3b94871dd51b199acef540e56d84246
           Boot ID: cebc9dbf16894e2dad62648165f399b5
    Virtualization: kvm
```

```
  Operating System: Red Hat Enterprise Linux Server 7.0 (Maipo)
       CPE OS Name: cpe:/o:redhat:enterprise_linux:7.0:GA:server
            Kernel: Linux 3.10.0-123.el7.x86_64
      Architecture: x86_64
```

4. 主機名稱儲存在 /etc/hostname，v6 版本則儲存 /etc/sysconfig/network。

```
[root@kvm7 ~]# cat /etc/hostname
kvm5.deyu.wang
```

5. 再將主機名稱設定爲 kvm7.deyu.wang。

```
[root@kvm7 ~]# hostnamectl set-hostname kvm7.deyu.wang
```

6. 查看 /etc/hostname，已變更爲 kvm7.deyu.wang。

```
[root@kvm7 ~]# cat /etc/hostname
kvm7.deyu.wang
```

7. 設定主機名稱及遠端連線操作示範

4.6 SSH 相關問題

4.6.1 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。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.
Permission denied (publickey,gssapi-keyex,gssapi-with-mic,
    password).
```

2. 原因爲客户端第一次 SSH 連線時已生一個認證，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生認證。

```
[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。

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

4.6.2 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。

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

2. 重新啓動 sshd 服務。

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

4.6.3 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，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
```

4.6.4 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

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

3. 檢查爲 iptables nat 的 POSTROUTING 問題。

```
*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。

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

4.6.5 Connection reset by peer

1. 登入主機 kvm7.deyu.wang 出現以下訊息：

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

2. 開啓 kvm7.deyu.wang 終端機，重新生 ssh key。

```
[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
```

Chapter 5

Netfilter

5.1 前言

1. Linux 核心包含一個功能強大的網路過濾子系統 netfilter。

2. netfilter 子系統允許核心模組檢查每一個傳送到系統的封包，因此可以在送到用户端時對封包修改、拒絕、丟棄。

3. RHEL/CentOS 6 使用 iptables 與核心的 netfilter 互動，但 iptables 只能調整 IPV4 的防火牆規則，對於 IPV6 及則必須使用 ip6tables。

4. RHEL/CentOS 7 使用新的方法 firewalld 與核心的 netfilter 互動，firewalld 是一個系統 daemon，它可以監看並修改系統的防火牆規則，且同時適用於 IPV4 與 IPV6。

5. firewalld 將所有網路傳輸分成不同的 zones。運作方式流程爲：

   (a) 進入系統的封包，先檢查來源 IP。

   (b) 如果來源 IP 有綁定指定的 zone，就使用該 zone 的規則。

   (c) 如果來源 IP 沒有綁定某一個 zone，就使用進入系統使用的網路介面 (network interface) 連結的 zone。

   (d) 如果網路介面沒有連結任何一個 zone，就使用管理者預設的 zone。

6. 系統預先定義的 zones 如下：

Zone name	Default configuration
trusted	完全開放，允許所有進入的封包。
home	只開放 ssh, mdns, ipp-client, samba-client, or dhcpv6-client 等服務及相開的送出封包，其餘封包皆拒絕。
internal	與 home zone 完全相同。
work	只開放 ssh, ipp-client, or dhcpv6-client 等服務及相開的送出封包，其餘封包皆拒絕。
public	只開放 ssh or dhcpv6-client 等服務及相開的送出封包，其餘封包皆拒絕。新增的網路介面預設使用這個 zone。
external	只開放 ssh 服務及相開的送出封包，其餘封包皆拒絕，送出的 IPv4 封包經由這個 zone 轉傳，IP 會被僞裝爲送出的網路介面的 IP。
dmz	只開放 ssh 服務及相開的送出封包，其餘封包皆拒絕。
block	拒絕所有封包。
drop	丟棄所有封包。

7. 防火牆設定方式有三種。

   (a) 直接編輯目錄 /etc/firewalld/ 下的設定檔。

   (b) 使用圖形化工具 firewall-config。

   (c) 使用文字介面命令 firewall-cmd。

8. 雖然 firewall-cmd 命令參數多又長，但因此命令有參數補齊功能，使用 TAB 鍵就可顯示可用參數及補齊，建議還是使用文字介面命令工具 firewall-cmd 比較穩定且方便。

5.2 firewall-cmd 命令

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

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

5.3 http 網頁架設–參考章節6.2

5.4 防火牆設定–參考章節6.3

Chapter 6

Apache 2.4 HTTP Server

6.1 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. CentOS 7 預設 httpd 2.4 版與 CentOS 6 的 httpd 2.2 版，在設定上有些不同，所以本文件以 httpd 2.4 爲例，進行架設說明。

6.2 http 網頁架設

1. 安裝套件。

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

2. 產生網頁主檔。

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

3. 啓動 httpd 服務，並設定開機啓動。

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

```
3 ln -s '/usr/lib/systemd/system/httpd.service' '/etc/systemd/
      system/multi-user.target.wants/httpd.service'
```

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

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

5. 必須設定 firewall 開放 80/tcp，外部主機才能連線。

6.3 防火牆設定

1. 開閉 iptables, ip6tables 服務。

```
  [root@kvm5 ~]# systemctl mask iptables.service
2 ln -s '/dev/null' '/etc/systemd/system/iptables.service'
  [root@kvm5 ~]# systemctl mask ip6tables.service
4 ln -s '/dev/null' '/etc/systemd/system/ip6tables.service'
```

2. 檢查 firewall 服務狀態。

```
  [root@kvm5 ~]# systemctl status firewalld.service
2 firewalld.service - firewalld - dynamic firewall daemon
     Loaded: loaded (/usr/lib/systemd/system/firewalld.service;
        enabled)
4    Active: active (running) since Thu 2014-08-21 18:51:18 CST; 3
        min 18s ago
   Main PID: 569 (firewalld)
6    CGroup: /system.slice/firewalld.service └──
            569 /usr/bin/python -Es /usr/sbin/firewalld --nofork
                --nopid
8
  Aug 21 18:51:18 kvm5.deyu.wang systemd[1]: Started firewalld -
      dynamic firew....
10 Hint: Some lines were ellipsized, use -l to show in full.
```

3. 如果沒有啓動，啓動 firewall，並設定開機啓動。

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

4. 查詢 firewall 預設 zone 爲 public。

```
[root@kvm5 ~]# firewall-cmd --get-default-zone
public
```

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

```
[root@kvm5 ~]# firewall-cmd --set-default-zone public
Warning: ZONE_ALREADY_SET: public
```

6. 檢查 public zone 的永久設定，開放的服務只有 dhcpv6-client 及 ssh。

```
[root@kvm5 ~]# firewall-cmd --permanent --zone=public --list-all
public (default)
  interfaces:
  sources:
  services: dhcpv6-client ssh
  ports:
  masquerade: no
  forward-ports:
  icmp-blocks:
  rich rules:
```

7. 在 public zone 開放 80/tcp 埠號及協定。

```
[root@kvm5 ~]# firewall-cmd --permanent --zone=public --add-port
    =80/tcp
success
```

8. 再次檢查 public zone，已開放 80/tcp 埠號及協定。

```
[root@kvm5 ~]# firewall-cmd --permanent --zone=public --list-all
public (default)
  interfaces:
  sources:
  services: dhcpv6-client ssh
  ports: 80/tcp
  masquerade: no
  forward-ports:
  icmp-blocks:
  rich rules:
```

9. 重新載入 firewall 的永久設定。

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

10. 再次重外部主機 deyu.wang 連線 kvm5.deyu.wang，已可成功連線。

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

6.4 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://kvm5.deyu.wang/~deyu1，查看模組有沒有載入，沒有的話要自行載入。

```
[root@kvm5 ~]# grep userdir /etc/httpd/conf.modules.d/00-base.
    conf
LoadModule userdir_module modules/mod_userdir.so
```

2. 開啓 Userdir，並設定用户個人網頁的根目錄。

```
[root@kvm5 ~]# vim /etc/httpd/conf.d/userdir.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>
```

3. 查看用户個人網頁根目錄的存取設定是否符合要求，不符合的話就要修改。

```
[root@kvm5 ~]# tail /etc/httpd/conf.d/userdir.conf
#
# 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 Indexes
    Options MultiViews Indexes SymLinksIfOwnerMatch
        IncludesNoExec
    Require method GET POST OPTIONS
</Directory>
```

4. 重新啓動 httpd。

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

5. 增加一般用户 deyu1，並設定其密碼。

```
[root@kvm5 ~]# useradd deyu1
[root@kvm5 ~]# echo '123qwe' | passwd --stdin deyu1
Changing password for user deyu1.
passwd: all authentication tokens updated successfully.
```

6. 改變身份爲 deyu1，減號爲使用 deyu1 用户的環境變數，不要漏了。

```
[root@kvm5 ~]# su - deyu1
```

7. 建立個人網頁根目錄，並產生一個内容爲 userdir test 的 index.html 檔案。

```
[deyu1@kvm5 ~]$ mkdir public_html
[deyu1@kvm5 ~]$ echo 'userdir test' > public_html/index.html
```

8. 退出用户 deyu1。

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

9. 連線 deyu1 的個人網頁，發現無權限存取。

```
[root@kvm5 ~]# curl http://kvm5.deyu.wang/~deyu1/
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>403 Forbidden</title>
</head><body>
<h1>Forbidden</h1>
<p>You don't have permission to access /~deyu1
on this server.</p>
</body></html>
```

10. 查看 deyu1 的家目錄權限爲 700，並不開放其他人讀取。

```
[root@kvm5 ~]# ll /home/deyu1/ -d
drwx------. 3 deyu1 deyu1 1024 May 22 21:04 /home/deyu1/
```

11. 將 deyu1 的家目錄權限改爲 755，開放其他人讀取。

```
[root@kvm5 ~]# chmod 755 /home/deyu1/
```

12. 連線成功。

```
[root@kvm5 ~]# curl http://kvm5.deyu.wang/~deyu1/
userdir test
```

6.5 Virtual Host 虛擬主機

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

2. 編輯 httpd.conf 加入 VirtualHost 段落，apache 2.4 的 httpd.conf 檔中沒有 VirtualHost 範例，要自行輸入，不過語法與其他段落一樣，關鍵字 VirtualHost 設定檔已出現，所以不會有什麼困擾。值得注意的是 apache 2.4 不需要再另外以 NameVirtualHost 啓動 VirtualHost。

```
[root@kvm5 ~]# vim /etc/httpd/conf/httpd.conf
### 原始主機名稱 kvm5.deyu.wang 根目錄 /var/www/html 也必須加入
<VirtualHost *:80>
    DocumentRoot /var/www/html
    ServerName kvm5.deyu.wang
</VirtualHost>
### 加入另一主機名稱 www5.deyu.wang 的根目錄爲 /var/www/virtual
<VirtualHost *:80>
    DocumentRoot /var/www/virtual
    ServerName www5.deyu.wang
</VirtualHost>
```

3. 設定完必須啓動 httpd 服務或 reload 設定參數。

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

4. 建立 virtual host www5.deyu.wang 的根目錄，並產生 index.html 檔。

```
[root@kvm5 ~]# mkdir /var/www/virtual
[root@kvm5 ~]# echo 'virtaul test' > /var/www/virtual/index.html
[root@kvm5 ~]# echo kvmweb > /var/www/html/index.html
```

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

```
[root@kvm5 ~]# curl http://kvm5.deyu.wang
kvmweb
[root@kvm5 ~]# curl http://www5.deyu.wang
virtaul test
```

6.6 存取限制

1. apache 2.4 存取限制的語法不同於 apache 2.2，舉例如下：

   (a) 限制所有存取

```
2.2 configuration:
Order deny,allow
Deny from all

2.4 configuration:
Require all denied
```

   (b) 允許所有存取

```
2.2 configuration:
Order allow,deny
Allow from all

2.4 configuration:
Require all granted
```

   (c) 允許所有在 deyu.wang 網域的主機存取

```
2.2 configuration:
Order Deny,Allow
Deny from all
Allow from deyu.wang

2.4 configuration:
Require host deyu.wang
```

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

   (a) 完整 ip

```
Require ip 10.1.2.3
Require ip 192.168.1.140 192.168.1.141
```

   (b) 部分 ip，允許指定網段。

```
Require ip 10.1
Require ip 10 172.20 192.168.2
```

   (c) 網段/遮罩，允許指定網段。 A network/netmask pair:

```
Require ip 10.1.0.0/255.255.0.0
```

   (d) 網段/遮罩數字，允許指定網段。

```
Require ip 10.1.0.0/16
```

3. httpd 限制只有 kvm5.deyu.wang 這台主機可以存取 www5.deyu.wang。

```
[root@kvm5 ~]# vim /etc/httpd/conf/httpd.conf
<Directory "/var/www/virtual">
    Require host kvm5.deyu.wang
</Directory>
```

4. 重新載入 httpd 服務設定，在 kvm5.deyu.wang 連線 kvm5 及 www5 都成功。

```
[root@kvm5 ~]# systemctl reload httpd.service
[root@kvm5 ~]# curl http://kvm5.deyu.wang
kvmweb
[root@kvm5 ~]# curl http://www5.deyu.wang
virtaul test
```

5. 在 deyu.wang 連線 kvm5 成功，但連線 www5 確不成功，表示設定有效。

```
[root@dywH ~]# curl http://kvm5.deyu.wang
kvmweb
[root@dywH ~]# curl http://www5.deyu.wang
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.1//EN" "http://www.w3.
    org/TR/xhtml11/DTD/xhtml11.dtd">
<html><head>
<meta http-equiv="content-type" content="text/html; charset=UTF-8
    ">
.....................
  </div>
</body></html>
```

6.7 AB test 及防止 DoS

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 httpd 時應該也一併安裝起來了，如果沒有就安裝套件 httpd-tools。

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

2. 在本機 kvm5.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 5ms， 100% 完成連線需要 12ms。

```
[root@kvm5 ~]# ab -n 1000 -c 20 http://kvm5.deyu.wang/index.html
This is ApacheBench, Version 2.3 <$Revision: 1430300 $>
Copyright 1996 Adam Twiss, Zeus Technology Ltd, http://www.
    zeustech.net/
Licensed to The Apache Software Foundation, http://www.apache.org
    /

Benchmarking kvm5.deyu.wang (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/2.4.6
```

```
Server Hostname:        kvm5.deyu.wang
Server Port:            80

Document Path:          /index.html
Document Length:        7 bytes

Concurrency Level:      20
Time taken for tests:   0.238 seconds
Complete requests:      1000
Failed requests:        0
Write errors:           0
Total transferred:      265000 bytes
HTML transferred:       7000 bytes
Requests per second:    4208.83 [#/sec] (mean)
Time per request:       4.752 [ms] (mean)
Time per request:       0.238 [ms] (mean, across all concurrent
   requests)
Transfer rate:          1089.20 [Kbytes/sec] received

Connection Times (ms)
              min  mean[+/-sd] median   max
Connect:        0    0   0.2      0       2
Processing:     3    4   0.9      4      11
Waiting:        3    4   0.9      4      11
Total:          3    5   1.0      5      12

Percentage of the requests served within a certain time (ms)
  50%      5
  66%      5
  75%      5
  80%      5
  90%      5
  95%      6
  98%      8
  99%     11
 100%     12 (longest request)
```

3. 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。

4. 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 CentOS 7 預設並沒有，若使用 DYW Linux REPO 資料庫，可以直接以 yum 指令安裝。

```
[root@kvm5 ~]# yum install mod_evasive
```

5. 先使用 mod_evasive 模組預設的設定。

```
[root@kvm5 ~]# vim /etc/httpd/conf.d/mod_evasive.conf
[root@kvm5 ~]# grep DOS /etc/httpd/conf.d/mod_evasive.conf
    DOSHashTableSize    3097
    DOSPageCount        2
    DOSSiteCount        50
    DOSPageInterval     1
    DOSSiteInterval     1
    DOSBlockingPeriod   10
    #DOSEmailNotify      you@yourdomain.com
    #DOSSystemCommand    "su - someuser -c '/sbin/... %s ...'"
    #DOSLogDir           "/var/lock/mod_evasive"
    # Multiple DOSWhitelist commands may be used in the
       configuration.
    #DOSWhitelist   127.0.0.1
    #DOSWhitelist   192.168.0.*
```

6. 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。

7. 重新啓動 httpd。

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

8. 由於架設的網站過於簡單，且於內部網路內測試，在設定的每秒間隔內，同一 IP 的請求及存取頁面次數，都不會超過限制值。若要查看實際測試狀況可以參考 Linux 安全與資安工具。

6.8 實機操作測驗練習題

6.8.1 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) http://kvmX.deyu.wang 首頁內容爲 'kvmX web test'，區分大小寫且不要添加其他字串，其中 'X' 爲虛擬機編號。

   (b) 防火牆及 SELinux 必須開啓。

6.8.2 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) `http://kvmX.deyu.wang/~deyu1/` 首頁內容爲 'userdir web test'，區分大小寫且不要添加其他字串，其中 'X' 爲虛擬機編號。

6.8.3 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，但 DYW Linux 已納入，所以本系統可以直接使用 yum 安裝。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。

      iii. DOSPageInterval：1 秒。

      iv. DOSSiteInterval：1 秒。

   (c) 重新載入 httpd 服務設定。

   (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。因首頁只是簡單文字且網路爲內部虛擬 IP 網段，存取速度很快，即使做了限制，壓力測試還是可能通過，所以評分只檢查是否設定正確。

6.8.4 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) http://wwwX.deyu.wang 首頁內容爲 'wwwX web test'，區分大小寫且不要添加其他字串，其中 'X' 爲虛擬機編號。

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

6.8.5 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. http://kvmX.deyu.wang/restricted/ 首頁內容爲 'restrictedX web test'，區分大小寫且不要添加其他字串，其中 'X' 爲虛擬機編號。

3. 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 7

安全 Apache 2.4 網站

7.1 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。

7.2 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。

2. Apache 2.4 在找不到連線檔案時，預設不會出現這些訊息。

```
1 [root@kvm5 ~]# curl -s http://kvm5.deyu.wang/abc | sed -e 's
    /<[^>]*>//g' -e '/^$/d'
  404 Not Found
```

```
3 Not Found
  The requested URL /abc was not found on this server.
```

3. 如果要啓動自訂的「找不到檔案的錯誤訊息」，先查看設定中錯誤訊息文件。

```
  [root@kvm5 ~]# grep -i ErrorDocument -R /etc/httpd/
2 /etc/httpd/conf/httpd.conf:#ErrorDocument 500 "The server made a
      boo boo."
  /etc/httpd/conf/httpd.conf:#ErrorDocument 404 /missing.html
4 /etc/httpd/conf/httpd.conf:#ErrorDocument 404 "/cgi-bin/
      missing_handler.pl"
  /etc/httpd/conf/httpd.conf:#ErrorDocument 402 http://www.example.
      com/subscription_info.html
6 Binary file /etc/httpd/conf/.httpd.conf.swp matches
  /etc/httpd/conf.d/welcome.conf:    ErrorDocument 403 /.noindex.
      html
```

4. 取消 ErrorDocument 404 的註解，也就是啓動。

```
1 [root@kvm5 ~]# grep 404 /etc/httpd/conf/httpd.conf
  ErrorDocument 404 /missing.html
3 #ErrorDocument 404 "/cgi-bin/missing_handler.pl"
```

5. 再重新載入 httpd 服務設定。

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

6. 產生自訂的「找不到檔案的錯誤訊息」。

```
1 [root@kvm5 ~]# echo 'File NOT Found' > /var/www/html/missing.html
```

7. 在連線「找不到檔案」時，出現自訂的「錯誤訊息」。

```
1 [root@kvm5 ~]# curl -s http://kvm5.deyu.wang/abc
  File NOT Found
```

7.3 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@kvm5 ~]# vim /etc/httpd/conf/httpd.conf
[root@kvm5 ~]# egrep '^User|^Group' /etc/httpd/conf/httpd.conf
User apache
Group apache
```

7.4 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。

2. 此時的最上層目錄 / 設定允許所有主機存取。

```
[root@kvm5 ~]# vim /etc/httpd/conf/httpd.conf
<Directory />
    AllowOverride none
    Require all granted
</Directory>
```

3. 下例中 /web 指向 /var，也就是連線 http://kvm5.deyu.wang/web 時會讀取 /mnt/www 下的資料。

```
[root@kvm5 ~]# grep ' Alias' /etc/httpd/conf/httpd.conf
    # Alias: Maps web paths into filesystem paths and is used to
    # Alias /webpath /full/filesystem/path
    Alias /web /mnt/www
    # ScriptAliases are essentially the same as Aliases, except
       that
    # directives as to Alias.
```

4. 再重新載入 httpd 服務設定。

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

5. 建立測試目錄 /mnt/www，目錄有一網頁 c.html。

```
[root@kvm5 ~]# mkdir /mnt/www
[root@kvm5 ~]# echo 'abc' > /mnt/www/c.html
```

6. 啓動 selinux

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

7. 檢查 selinux 有無啓動？是否限制？

```
[root@kvm5 ~]# getenforce
Enforcing
```

8. 開機啓動 selinux。

```
[root@kvm5 ~]# vim /etc/selinux/config
[root@kvm5 ~]# grep enforcing /etc/selinux/config
#     enforcing - SELinux security policy is enforced.
#     permissive - SELinux prints warnings instead of enforcing.
SELINUX=enforcing
```

9. 已經開放網頁根目錄上層目錄的存取，但連線 http://kvm5.deyu.wang/web/c.html，回應無法存取。

```
[root@kvm5 ~]# curl -s http://kvm5.deyu.wang/web/c.html
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>403 Forbidden</title>
</head><body>
<h1>Forbidden</h1>
<p>You don't have permission to access /web/c.html
on this server.</p>
</body></html>
```

10. 查看 /mnt/www 目錄檔案的 content type 是 mnt_t，而不是 httpd_sys_content_t。

```
[root@kvm5 ~]# ll -Z /var/www/html /mnt/www
/mnt/www:
-rw-r--r--. root root unconfined_u:object_r:mnt_t:s0    c.html

/var/www/html:
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:
    s0 index.html
drwxr-xr-x. root root unconfined_u:object_r:httpd_sys_content_t:
    s0 inx
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:
    s0 missing.html
```

11. 變更 /mnt/www 目錄檔案的 content type 爲 httpd_sys_content_t。

```
[root@kvm5 ~]# chcon -Rv -t httpd_sys_content_t /mnt/www
changing security context of ‘/mnt/www/c.’html
changing security context of ‘/mnt/’www
```

12. 再連線 http://kvm5.deyu.wang/web/c.html，回應 c.html 內容 abc。

```
[root@kvm5 ~]# curl -s http://kvm5.deyu.wang/web/c.html
abc
```

13. 修改 httpd.conf 限制網頁根目錄外資料的存取。

```
[root@kvm5 ~]# vim /etc/httpd/conf/httpd.conf
<Directory />
    AllowOverride none
    Require all denied
</Directory>
```

14. 再重新載入 httpd 服務設定。

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

15. 再連線 http://kvm5.deyu.wang/web/c.html，回應 403 拒絕存取。

```
[root@kvm5 ~]# curl -s http://kvm5.deyu.wang/web/c.html | sed -e
    's/<[^>]*>//g' -e '/^$/d'
[root@kvm5 ~]# curl -s http://kvm5.deyu.wang/web/c.html
403 Forbidden
Forbidden
You don't have permission to access /web/c.html
on this server.
```

7.5 關閉目錄瀏覽

1. 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 FollowSymLinks
    AllowOverride None
    Require all granted
</Directory>
```

2. 爲了測試，先在 /var/www/html/ 目錄下建一個目錄 inx 並產生 i.html 及 ijk.html 兩個檔案。

```
[root@kvm5 ~]# mkdir /var/www/html/inx
[root@kvm5 ~]# echo 'index test' > /var/www/html/inx/i.html
[root@kvm5 ~]# echo 'index test' > /var/www/html/inx/ijk.html
```

3. 連線 http://kvm5.deyu.wang/inx/，目錄下沒有 index.html 或 index.php，系統列出 i.html 及 ijk.html 兩個檔案。

```
[root@kvm5 ~]# curl -s http://kvm5.deyu.wang/inx/ | sed -e 's
    /<[^>]*>//g' -e '/^$/d'

  Index of /inx


Index of /inx

   NameLast modifiedSizeDescription

```

```
Parent Directory           -  
i.html                  2015-05-23 00:32   11  
ijk.html                2015-05-23 00:33   11  
```

4. 修改 httpd.conf 在 Indexes 前加減號可以關閉目錄瀏覽，注意 apache 2.4 Options 後面接的選項不只一個時，當其中一個以「加減號」做爲啓動或關閉時，則其他每個選項也都要在前面加上「加減號」，否則 httpd 無法成功啓動。

```
[root@kvm8 ~]# vim /etc/httpd/conf/httpd.conf
<Directory "/var/www/html">
    Options -Indexes +FollowSymLinks
    AllowOverride None
    Require all granted
</Directory>
```

5. 再重新載入 httpd 服務設定。

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

6. 再連線 http://kvm5.deyu.wang/inx/，目錄下沒有 index.html 或 index.php，系統回應沒有權限存取此目錄。

```
[root@kvm5 ~]# curl -s http://kvm5.deyu.wang/inx/ | sed -e 's
   /<[^>]*>//g' -e '/^$/d'
403 Forbidden
Forbidden
You don't have permission to access /inx/
on this server.
```

7.6 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@kvm5 ~]# chown root.root -R /var/www/html/
[root@kvm5 ~]# 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。

7.7 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，目前的設定是開啓。

```
[root@kvm8 ~]# vim /etc/httpd/conf/httpd.conf
<Directory "/var/www/html">
    Options -Indexes +FollowSymLinks
    AllowOverride None
    Require all granted
</Directory>
```

2. 建立測試連結檔，將 inx 目錄下產生一連結到上層目錄 index.html 的連結檔 index.html。

```
[root@kvm5 ~]# cd /var/www/html/inx/
[root@kvm5 inx]# ln -s ../index.html index.html
[root@kvm5 inx]# ll
total 8
-rw-r--r--. 1 root root 11 May 23 00:32 i.html
-rw-r--r--. 1 root root 11 May 23 00:33 ijk.html
lrwxrwxrwx. 1 root root 13 May 23 01:03 index.html -> ../index.
   html
```

3. 連線 http://kvm5.deyu.wang/inx/ 成功，表示可以讀取連結檔 index.html。

```
[root@kvm5 html]# curl -s http://kvm5.deyu.wang/inx/ | sed -e 's
   /<[^>]*>//g' -e '/^$/d'
kvmweb
```

4. 在目錄設定關閉選項 FollowSymLinks，讓目錄下的連結檔不作用。

```
[root@kvm8 ~]# vim /etc/httpd/conf/httpd.conf
<Directory "/var/www/html">
    Options -Indexes -FollowSymLinks
    AllowOverride None
    Require all granted
</Directory>
```

5. 再重新載入 httpd 服務設定。

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

6. 再連線 http://kvm5.deyu.wang/inx/，顯示目錄下沒有 index.html 或 index.php，表示 index.html 連結沒作用，系統回應沒有權限存取此目錄。

```
[root@kvm5 inx]# curl -s http://kvm5.deyu.wang/inx/ | sed -e 's
    /<[^>]*>//g' -e '/^$/d'
403 Forbidden
Forbidden
You don't have permission to access /inx/
on this server.
```

7.8 實機操作測驗練習題

7.8.1 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) 設計自訂的錯誤訊息檔 missing 在根目錄下，內容爲 "File NOT Found"。
   (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 8

XFS 檔案系統

8.1 Linux 檔案系統

1. ext2: 沒有日誌的檔案系統。
2. ext3: 傳統的 linux 檔案系統，ext2 加上日誌功能。
3. ext4: ext-based 最後版本，RHEL/CentOS 6 預設的檔案系統。
4. xfs: 可擴展性的高性能檔案系統，RHEL/CentOS 7 預設使用使檔案系統。
5. btrfs: 發展中、功能豐富的檔案系統。

8.2 ext4 lv 放大縮小

1. 放大縮小都可以使用 lvresize 指令，不過最好先卸載檔案系統，再進行放大縮小，否則可能會造成檔案損壞，尤其根目錄無法卸載的情況下，直接進行放大縮小，風險非常高，若眞有必要對根目錄進行放大縮小，建議改以隨身碟開機來對電腦硬碟進行分割區的放大縮小。
2. 查看 partition 的 filesystem type，v6 預設爲 ext4。

```
[root@kvm8 ~]# df -Th /home
Filesystem     Type    Size  Used Avail Use% Mounted on
/dev/mapper/vg_kvmhome-vo
               ext4     97M  5.6M   87M   7% /home
```

3. 先卸載家目錄 /home。

```
[root@kvm8 ~]# umount /home/
```

4. 從原先的 80M 縮小爲 50M，選項 -r 表示同時進行檔案系統的 resize。

```
[root@kvm8 ~]# lvresize -L 50M /dev/mapper/vg_kvmhome-vo -r
fsck from util-linux-ng 2.17.2
e2fsck 1.41.12 (17-May-2010)
/dev/mapper/vg_kvmhome-vo: clean, 47/20480 files, 8288/81920
    blocks
resize2fs 1.41.12 (17-May-2010)
Resizing the filesystem on /dev/dm-2 to 51200 (1k) blocks.
The filesystem on /dev/dm-2 is now 51200 blocks long.

  Reducing logical volume vo to 50.00 MiB
  Logical volume vo successfully resized
```

5. 重新掛載再查看分割區 /dev/mapper/vg_kvmusb-vo 已調成 50M。

```
[root@kvm8 ~]# mount -a
[root@kvm8 ~]# df -h /home
Filesystem            Size  Used Avail Use% Mounted on
/dev/mapper/vg_kvmhome-vo
                       49M  5.1M   41M  12% /home
```

6. 卸載後再將分割區 /dev/mapper/vg_kvmusb-vo 放大成 120M，出現錯誤訊息，要求先檢查檔案系統。

```
[root@kvm8 ~]# umount /home/
[root@kvm8 ~]# lvresize -L 120M /dev/mapper/vg_kvmhome-vo -r
fsck from util-linux-ng 2.17.2
e2fsck 1.41.12 (17-May-2010)
/dev/mapper/vg_kvmhome-vo: clean, 47/14336 files, 6998/51200
    blocks
  Extending logical volume vo to 120.00 MiB
  Logical volume vo successfully resized
resize2fs 1.41.12 (17-May-2010)
Please run 'e2fsck -f /dev/dm-2' first.

fsadm: Resize ext4 failed
  fsadm failed: 1
```

7. 先檢查分割區 /dev/mapper/vg_kvmusb-vo，也就是 /dev/dm-2。

```
[root@kvm8 ~]# e2fsck -f /dev/dm-2
e2fsck 1.41.12 (17-May-2010)
Pass 1: Checking inodes, blocks, and sizes
Pass 2: Checking directory structure
Pass 3: Checking directory connectivity
Pass 4: Checking reference counts
Pass 5: Checking group summary information
/dev/dm-2: 47/14336 files (4.3% non-contiguous), 6998/51200
    blocks
```

8. 再將分割區 /dev/mapper/vg_kvmusb-vo 放大成 120M，已沒有錯誤訊息，要求先檢查檔案系統。

```
[root@kvm8 ~]# lvresize -L 120M /dev/mapper/vg_kvmhome-vo -r
fsck from util-linux-ng 2.17.2
e2fsck 1.41.12 (17-May-2010)
/dev/mapper/vg_kvmhome-vo: clean, 47/14336 files, 6998/51200
    blocks
  Extending logical volume vo to 120.00 MiB
  Logical volume vo successfully resized
resize2fs 1.41.12 (17-May-2010)
Resizing the filesystem on /dev/dm-2 to 122880 (1k) blocks.
The filesystem on /dev/dm-2 is now 122880 blocks long.
```

9. 重新掛載再查看分割區 /dev/mapper/vg_kvmusb-vo 已調成 120M。

```
[root@kvm8 ~]# mount -a
[root@kvm8 ~]# df -h /home
Filesystem            Size  Used Avail Use% Mounted on
/dev/mapper/vg_kvmhome-vo
                      117M  5.6M  105M   6% /home
```

8.3 xfs lv 縮小

1. 查看 v7 的檔案系統，家目錄 /home 的分割區爲 xfs。

```
[root@kvm7 ~]# df -Th /home
Filesystem                Type  Size  Used Avail Use% Mounted on
```

```
/dev/mapper/vg_kvm7home-vo xfs     97M  5.3M   92M   6% /home
```

2. 先卸載家目錄 /home，家目錄忙錄中無法卸載。

```
[root@kvm7 ~]# umount /home
umount: /home: target is busy.
        (In some cases useful info about processes that use
         the device is found by lsof(8) or fuser(1))
```

3. 使用 lsof 查看家目錄 /home 使用狀況，爲自動掛載程式掛載在 /home-/guests。

```
[root@kvm7 ~]# lsof | grep /home
automount 1539          root   16r      DIR                0,37
            0      18663 /home/guests
automount 1539 1540     root   16r      DIR                0,37
            0      18663 /home/guests
automount 1539 1541     root   16r      DIR                0,37
            0      18663 /home/guests
automount 1539 2032     root   16r      DIR                0,37
            0      18663 /home/guests
automount 1539 2068     root   16r      DIR                0,37
            0      18663 /home/guests
automount 1539 2096     root   16r      DIR                0,37
            0      18663 /home/guests
```

4. 先關閉自動掛載，再卸載家目錄 /home。

```
[root@kvm7 ~]# systemctl stop autofs.service
[root@kvm7 ~]# umount /home
```

5. 使用 lvresize 將 /dev/vg_kvm7home/vo 由 100M 縮小爲 50M，出現 Xfs 檔案系統不支援縮小的訊息，表示 lvm 中 xfs 檔案系統格式的 lv 無法直接縮小，若眞有必要縮小，必須建一個新的較小的 lv，將資料移過去後再刪除目前的 lv。

```
[root@kvm7 ~]# lvresize -L 50M /dev/vg_kvm7home/vo -r
Phase 1 - find and verify superblock...
Phase 2 - using internal log
        - scan filesystem freespace and inode maps...
        - found root inode chunk
Phase 3 - for each AG...
        - scan (but don't clear) agi unlinked lists...
        - process known inodes and perform inode discovery...
        - agno = 0
        - agno = 1
        - agno = 2
        - agno = 3
        - agno = 4
        - process newly discovered inodes...
Phase 4 - check for duplicate blocks...
        - setting up duplicate extent list...
        - check for inodes claiming duplicate blocks...
        - agno = 0
        - agno = 1
        - agno = 2
        - agno = 3
        - agno = 4
No modify flag set, skipping phase 5
Phase 6 - check inode connectivity...
        - traversing filesystem ...
        - traversal finished ...
        - moving disconnected inodes to lost+found ...
Phase 7 - verify link counts...
No modify flag set, skipping filesystem flush and exiting.
fsadm: Xfs filesystem shrinking is unsupported
  fsadm failed: 1
  Filesystem resize failed.
```

8.4 xfs lv 放大

1. 先重新掛載並查看家目錄 /home，大小爲 100M。

```
[root@kvm7 ~]# mount -a
[root@kvm7 ~]# df -Th /home
Filesystem                Type  Size  Used Avail Use% Mounted on
/dev/mapper/vg_kvm7home-vo xfs    97M  5.3M   92M   6% /home
```

2. 放大 xfs 檔案系統格式的 lv，不必先卸載，只要先用 lvextend 放大 lv。

```
[root@kvm7 ~]# lvextend -L 120M /dev/vg_kvm7home/vo
  Extending logical volume vo to 120.00 MiB
  Logical volume vo successfully resized
```

3. 再使用 xfs_growfs 命令，將 xfs 檔案系統格式的分割區成長到 lv 的大小。

```
[root@kvm7 ~]# xfs_growfs /dev/vg_kvm7home/vo
meta-data=/dev/mapper/vg_kvm7home-vo isize=256    agcount=5,
    agsize=5120 blks
         =                       sectsz=512   attr=2, projid32bit
             =1
         =                       crc=0
data     =                       bsize=4096   blocks=25600,
    imaxpct=25
         =                       sunit=0      swidth=0 blks
naming   =version 2              bsize=4096   ascii-ci=0 ftype=0
log      =internal               bsize=4096   blocks=853, version
    =2
         =                       sectsz=512   sunit=0 blks, lazy-
             count=1
realtime =none                   extsz=4096   blocks=0, rtextents
    =0
data blocks changed from 25600 to 30720
```

4. 再查看家目錄 /home，大小已放大到 120M。

```
[root@kvm7 ~]# df -Th /home
Filesystem                Type  Size  Used Avail Use% Mounted on
/dev/mapper/vg_kvm7home-vo xfs   117M  5.4M  112M   5% /home
```

Chapter 9

fdisk 硬碟分割

9.1 前言

1. 在 v6 執行 fdisk 命令，建議使用 -uc 選項，否則分割硬碟時總會出現分割區間夾著一個無法使用的 section，造成分割困擾。

2. 在 v6 使用 fdisk 存好分割表後，總是要重新開機，分割表才能生效，即使使用 partprobe, kpartx 等命令偵測分割區也沒用。不過後來找到 partx 加上 -a 選項可以在不重新開機的情況下，將新的分割表載到核心中。

3. v7 已解決上述兩項問題。

9.2 v6 fdisk 使用

1. fdisk 命令分割硬碟，不使用 -uc 選項出現警告訊息，且每一個 partition 都不是結束於 cylinder 的邊界，這會造成分割時的困擾。

```
[root@kvm8 ~]# fdisk /dev/vda

WARNING: DOS-compatible mode is deprecated. It's strongly
   recommended to
         switch off the mode (command 'c') and change display
            units to
         sectors (command 'u').

Command (m for help): p

Disk /dev/vda: 4294 MB, 4294967296 bytes
16 heads, 63 sectors/track, 8322 cylinders
Units = cylinders of 1008 * 512 = 516096 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x0006a798

```

```
   Device Boot      Start         End      Blocks   Id  System
/dev/vda1   *           3         198       98304   83  Linux
Partition 1 does not end on cylinder boundary.
/dev/vda2             198        8056     3960576   8e  Linux LVM
Partition 2 does not end on cylinder boundary.
/dev/vda3            8056        8320      133120   8e  Linux LVM
Partition 3 does not end on cylinder boundary.
```

2. fdisk 命令分割硬碟，使用 -uc 選項。

```
[root@kvm8 ~]# fdisk -uc /dev/vda

Command (m for help): p

Disk /dev/vda: 4294 MB, 4294967296 bytes
16 heads, 63 sectors/track, 8322 cylinders, total 8388608 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x0005fdc8

   Device Boot      Start         End      Blocks   Id  System
/dev/vda1   *        2048      198655       98304   83  Linux
/dev/vda2          198656     8119807     3960576   8e  Linux LVM
/dev/vda3         8119808     8386047      133120   8e  Linux LVM

Command (m for help): n
Command action
   e   extended
   p   primary partition (1-4)
p
Selected partition 4
First sector (8386048-8388607, default 8386048):
Using default value 8386048
Last sector, +sectors or +size{K,M,G} (8386048-8388607, default
    8388607): +1M

Command (m for help): p

Disk /dev/vda: 4294 MB, 4294967296 bytes
16 heads, 63 sectors/track, 8322 cylinders, total 8388608 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x0005fdc8

   Device Boot      Start         End      Blocks   Id  System
/dev/vda1   *        2048      198655       98304   83  Linux
```

```
/dev/vda2          198656     8119807     3960576   8e  Linux LVM
/dev/vda3         8119808     8386047      133120   8e  Linux LVM
/dev/vda4         8386048     8388095        1024   83  Linux

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

Calling ioctl() to re-read partition table.

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

3. 依據警告訊息使用 partprobe 偵測新分割區無效。

```
[root@kvm8 ~]# partprobe
Warning: WARNING: the kernel failed to re-read the partition
    table on
/dev/vda (Device or resource busy).
As a result, it may not reflect all of your changes until after
    reboot.
```

4. 依據警告訊息使用 kpartx 偵測新分割區無效，使用 partx 偵測也無效。

```
[root@kvm8 ~]# kpartx /dev/vda
vda1 : 0 196608 /dev/vda 2048
vda2 : 0 7921152 /dev/vda 198656
vda3 : 0 266240 /dev/vda 8119808
vda4 : 0 2048 /dev/vda 8386048
[root@kvm8 ~]# partx /dev/vda
# 1:      2048-   198655 (   196608 sectors,    100 MB)
# 2:    198656-  8119807 (  7921152 sectors,   4055 MB)
# 3:   8119808-  8386047 (   266240 sectors,    136 MB)
# 4:   8386048-  8388095 (     2048 sectors,      1 MB)
```

5. /dev/vda4 仍然沒有出現。

```
[root@kvm8 ~]# ll /dev/vda*
```

```
brw-rw----. 1 root disk 252, 0 Dec 19 09:25 /dev/vda
brw-rw----. 1 root disk 252, 1 Dec  8 14:25 /dev/vda1
brw-rw----. 1 root disk 252, 2 Dec  8 14:25 /dev/vda2
brw-rw----. 1 root disk 252, 3 Dec  8 14:25 /dev/vda3
```

6. 使用 partx 加上 -a 選項有效，可以不重新開機將新的分割區 /dev/vda4 加到分割表中。

```
[root@kvm8 ~]# partx -va /dev/vda
device /dev/vda: start 0 size 8388608
gpt: 0 slices
dos: 4 slices
# 1:      2048-   198655 (   196608 sectors,    100 MB)
# 2:    198656-  8119807 (  7921152 sectors,   4055 MB)
# 3:   8119808-  8386047 (   266240 sectors,    136 MB)
# 4:   8386048-  8388095 (     2048 sectors,      1 MB)
BLKPG: Device or resource busy
error adding partition 1
BLKPG: Device or resource busy
error adding partition 2
BLKPG: Device or resource busy
error adding partition 3
added partition 4
```

7. 已經看到 /dev/vda4。

```
[root@kvm8 ~]# ll /dev/vda*
brw-rw----. 1 root disk 252, 0 Dec 19 09:25 /dev/vda
brw-rw----. 1 root disk 252, 1 Dec  8 14:25 /dev/vda1
brw-rw----. 1 root disk 252, 2 Dec  8 14:25 /dev/vda2
brw-rw----. 1 root disk 252, 3 Dec  8 14:25 /dev/vda3
brw-rw----. 1 root disk 252, 4 Dec 19 09:27 /dev/vda4
```

8. 格式化 /dev/vda4 成功。

```
[root@kvm8 ~]# mkfs.ext4 /dev/vda4
mke2fs 1.41.12 (17-May-2010)
Filesystem label=
OS type: Linux
Block size=1024 (log=0)
```

```
Fragment size=1024 (log=0)
Stride=0 blocks, Stripe width=0 blocks
128 inodes, 1024 blocks
51 blocks (4.98%) reserved for the super user
First data block=1
Maximum filesystem blocks=1048576
1 block group
8192 blocks per group, 8192 fragments per group
128 inodes per group

Writing inode tables: done

Filesystem too small for a journal
Writing superblocks and filesystem accounting information: done

This filesystem will be automatically checked every 23 mounts or
180 days, whichever comes first.  Use tune2fs -c or -i to
   override.
```

9.3 v7 fdisk 使用

1. 查看硬碟編號爲 vda。

```
[root@kvm7 ~]# lsblk
NAME                MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
vda                 252:0    0    4G  0 disk ├──
vda1              252:1    0  200M  0 part /boot ├──
vda2              252:2    0  3.4G  0 part │ ├──
 vg_kvm7usb-swap 253:0    0  124M  0 lvm  [SWAP] │ └──
 vg_kvm7usb-root 253:1    0  3.1G  0 lvm  / └──
vda3              252:3    0  130M  0 part └──
  vg_kvm7home-vo  253:2    0   80M  0 lvm  /home
```

2. fdisk 命令分割硬碟，不必再使用 -uc 選項。

```
[root@kvm7 ~]# fdisk /dev/vda
Welcome to fdisk (util-linux 2.23.2).

Changes will remain in memory only, until you decide to write
   them.
Be careful before using the write command.
```

3. 執行 m 可以列出所有指令。

```
Command (m for help): m
Command action
   a   toggle a bootable flag
   b   edit bsd disklabel
   c   toggle the dos compatibility flag
   d   delete a partition
   g   create a new empty GPT partition table
   G   create an IRIX (SGI) partition table
   l   list known partition types
   m   print this menu
   n   add a new partition
   o   create a new empty DOS partition table
   p   print the partition table
   q   quit without saving changes
   s   create a new empty Sun disklabel
   t   change a partition's system id
   u   change display/entry units
   v   verify the partition table
   w   write table to disk and exit
   x   extra functionality (experts only)
```

4. 執行 p 列出分割表，建議每一動作結束都使用 p 查看分割表。

```
Command (m for help): p

Disk /dev/vda: 4294 MB, 4294967296 bytes, 8388608 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 0x000a59f4

   Device Boot      Start         End      Blocks   Id  System
/dev/vda1   *        2048      411647      204800   83  Linux
/dev/vda2          411648     7579647     3584000   8e  Linux LVM
/dev/vda3         7579648     7845887      133120   8e  Linux LVM
```

5. 執行 n 新增分割區，MBR 只能有記錄四個分割區，若有五個以上分割區，必須使用 extended 擴展分割區。

```
Command (m for help): n
```

```
Partition type:
   p   primary (3 primary, 0 extended, 1 free)
   e   extended
Select (default e):
Using default response e
Selected partition 4
First sector (7845888-8388607, default 7845888):
Using default value 7845888
Last sector, +sectors or +size{K,M,G} (7845888-8388607, default
    8388607):
Using default value 8388607
Partition 4 of type Extended and of size 265 MiB is set

Command (m for help): p

Disk /dev/vda: 4294 MB, 4294967296 bytes, 8388608 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 0x000a59f4

   Device Boot      Start         End      Blocks   Id  System
/dev/vda1   *        2048      411647      204800   83  Linux
/dev/vda2          411648     7579647     3584000   8e  Linux LVM
/dev/vda3         7579648     7845887      133120   8e  Linux LVM
/dev/vda4         7845888     8388607      271360    5  Extended
```

6. 執行 n 新增分割區，因 MBR 已記錄 4 筆分割區，故強制使用 logical 分割區。

```
Command (m for help): n
All primary partitions are in use
Adding logical partition 5
First sector (7847936-8388607, default 7847936):
Using default value 7847936
Last sector, +sectors or +size{K,M,G} (7847936-8388607, default
    8388607): +10M
Partition 5 of type Linux and of size 10 MiB is set

Command (m for help): p

Disk /dev/vda: 4294 MB, 4294967296 bytes, 8388608 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 0x000a59f4
```

```
17
   Device Boot      Start         End      Blocks   Id  System
19 /dev/vda1   *        2048      411647      204800   83  Linux
   /dev/vda2          411648     7579647     3584000   8e  Linux LVM
21 /dev/vda3         7579648     7845887      133120   8e  Linux LVM
   /dev/vda4         7845888     8388607      271360    5  Extended
23 /dev/vda5         7847936     7868415       10240   83  Linux
```

7. 執行 t 改變分割區系統 ID，設定爲 82 Linux swap 分割區。

```
1  Command (m for help): t
   Partition number (1-5, default 5):
3  Hex code (type L to list all codes): L

5   0  Empty           24  NEC DOS         81  Minix / old Lin bf
    Solaris
    1  FAT12           27  Hidden NTFS Win 82  Linux swap / So c1
    DRDOS/sec (FAT-
7   2  XENIX root      39  Plan 9          83  Linux           c4
    DRDOS/sec (FAT-
    3  XENIX usr       3c  PartitionMagic  84  OS/2 hidden C:  c6
    DRDOS/sec (FAT-
9   4  FAT16 <32M      40  Venix 80286     85  Linux extended  c7
    Syrinx
    5  Extended        41  PPC PReP Boot   86  NTFS volume set da
    Non-FS data
11  6  FAT16           42  SFS             87  NTFS volume set db
    CP/M / CTOS / .
    7  HPFS/NTFS/exFAT 4d  QNX4.x          88  Linux plaintext de
    Dell Utility
13  8  AIX             4e  QNX4.x 2nd part 8e  Linux LVM       df
    BootIt
    9  AIX bootable    4f  QNX4.x 3rd part 93  Amoeba          e1
    DOS access
15  a  OS/2 Boot Manag 50  OnTrack DM      94  Amoeba BBT      e3
    DOS R/O
    b  W95 FAT32       51  OnTrack DM6 Aux 9f  BSD/OS          e4
    SpeedStor
17  c  W95 FAT32 (LBA) 52  CP/M            a0  IBM Thinkpad hi eb
    BeOS fs
    e  W95 FAT16 (LBA) 53  OnTrack DM6 Aux a5  FreeBSD         ee
    GPT
19  f  W95 Ext'd (LBA) 54  OnTrackDM6      a6  OpenBSD         ef
    EFI (FAT-12/16/
   10  OPUS            55  EZ-Drive        a7  NeXTSTEP        f0
   Linux/PA-RISC b
21 11  Hidden FAT12    56  Golden Bow      a8  Darwin UFS      f1
   SpeedStor
```

```
12  Compaq diagnost 5c  Priam Edisk     a9  NetBSD          f4
    SpeedStor
14  Hidden FAT16 <3 61  SpeedStor       ab  Darwin boot     f2
    DOS secondary
16  Hidden FAT16    63  GNU HURD or Sys af  HFS / HFS+      fb
    VMware VMFS
17  Hidden HPFS/NTF 64  Novell Netware  b7  BSDI fs         fc
    VMware VMKCORE
18  AST SmartSleep  65  Novell Netware  b8  BSDI swap       fd
    Linux raid auto
1b  Hidden W95 FAT3 70  DiskSecure Mult bb  Boot Wizard hid fe
    LANstep
1c  Hidden W95 FAT3 75  PC/IX           be  Solaris boot    ff
    BBT
1e  Hidden W95 FAT1 80  Old Minix
Hex code (type L to list all codes): 82
Changed type of partition 'Linux' to 'Linux swap / Solaris'

Command (m for help): p

Disk /dev/vda: 4294 MB, 4294967296 bytes, 8388608 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 0x000a59f4

   Device Boot      Start         End      Blocks   Id  System
/dev/vda1   *        2048      411647      204800   83  Linux
/dev/vda2          411648     7579647     3584000   8e  Linux LVM
/dev/vda3         7579648     7845887      133120   8e  Linux LVM
/dev/vda4         7845888     8388607      271360    5  Extended
/dev/vda5         7847936     7868415       10240   82  Linux
    swap / Solaris
```

8. 執行 w 儲存分割表後退出，一樣出現警告訊息。

```
Command (m for help): w
The partition table has been altered!

Calling ioctl() to re-read partition table.

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

9. 依照警告訊息執行 partprobe 及 kpartx。

```
[root@kvm7 ~]# partprobe /dev/vda
[root@kvm7 ~]# kpartx /dev/vda
vda1 : 0 409600 /dev/vda 2048
vda2 : 0 7168000 /dev/vda 411648
vda3 : 0 266240 /dev/vda 7579648
vda4 : 0 2 /dev/vda 7845888
vda5 : 0 20480 /dev/vda 7847936
[root@kvm7 ~]#
```

10. 列出分割表，已出現剛剛分割的新分割區。

```
[root@kvm7 ~]# lsblk
NAME                MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
vda                 252:0    0    4G  0 disk ├──
vda1                252:1    0  200M  0 part /boot ├──
vda2                252:2    0  3.4G  0 part │ ├──
 vg_kvm7usb-swap 253:0    0  124M  0 lvm  [SWAP] │ └──
 vg_kvm7usb-root 253:1    0  3.1G  0 lvm  / ├──
vda3                252:3    0  130M  0 part │ └──
 vg_kvm7home-vo  253:2    0   80M  0 lvm  /home ├──
vda4                252:4    0    1K  0 part └──
vda5                252:5    0   10M  0 part
```

11. 沒有重新開機，直接格式化分割區 /dev/vda5 爲 swap。

```
[root@kvm7 ~]# mkswap /dev/vda5
Setting up swapspace version 1, size = 10236 KiB
no label, UUID=d9b87380-fcf6-4c59-8421-130e3749a0a3
```

12. 建立開機自動掛載 /dev/vda5 爲 swap。

```
[root@kvm7 ~]# vim /etc/fstab
/dev/vda5 swap swap defaults 0 0
```

13. 檢查目前 swap 只有 dm-0 大小爲 126972 bytes。

```
[root@kvm7 ~]# swapon -s
Filename                Type        Size    Used    Priority
/dev/dm-0                                   partition   126972  0
   -1
```

14. 重新掛載 /etc/fstab 上的 swap 分割區，v7 不再警告已掛載的 swap。

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

15. 檢查 swap 已出現 /dev/vda5 的 swap，大小爲 10236 bytes。

```
[root@kvm7 ~]# swapon -s
Filename                Type        Size    Used    Priority
/dev/dm-0                                   partition   126972  0
   -1
/dev/vda5                                   partition   10236   0
   -2
```

Chapter 10

Chronyd vs. ntpd 校時

10.1 前言

1. RHEL/CentOS 7 校時新套件 chrony 取代 ntp。
   (a) 更快速以及更精確的同步。
   (b) 頻率校正的範圍較大。
   (c) 擁有對於時鐘頻率快速變更的反應速度。
   (d) 在初始同步後不會發生 clock stepping。Stepping 意思是時間突然從不正確的時間一步調到正確時間的合理誤差時間，如果誤差小於 128ms 則以 slewing 擺動修正。
   (e) 適用於間歇性的網路連線。
2. chrony 不完全支援 ntp 中的所有可用功能，因此基於相容性上的原因，RHEL/CentOS 依然提供 ntp 套件，使用時必須明確地移除 chrony 並安裝 ntp 來代替。
3. Chrony 的時間設定演算法擁有幾項 ntp 實作所沒有的優點。

10.2 chronyd 使用

1. chrony 是 RHEL/CentOS 7 預設的校時 dameon，設定檔在 /etc/chrony.conf，新增校時伺服器 server.deyu.wang，其中 iburst 選項是用來加速初始同步。

```
[root@kvm81 ~]# vim /etc/chrony.conf
server deyu.wang
[root@kvm81 ~]# grep deyu /etc/chrony.conf
server server.deyu.wang iburst
```

2. 重新啓動 chronyd。

```
[root@kvm81 ~]# systemctl restart chronyd.service
```

3. chronyd 預設開機啓動，不放心可再設定一次。

```
[root@kvm81 ~]# systemctl enable chronyd.service
```

4. 追 chronyd 校時來源伺服器。

```
[root@kvm81 ~]# chronyc tracking
Reference ID    : 192.168.122.1 (deyu.wang)
Stratum         : 4
Ref time (UTC)  : Tue Jan 20 03:01:00 2015
System time     : 124520.273437500 seconds slow of NTP time
Last offset     : 0.000016787 seconds
RMS offset      : 11733.896484375 seconds
Frequency       : 0.074 ppm slow
Residual freq   : 0.007 ppm
Skew            : 0.413 ppm
Root delay      : 0.006454 seconds
Root dispersion : 0.045809 seconds
Update interval : 59.5 seconds
Leap status     : Normal
```

5. 使用 chronyc 命令檢查 chronyd 校時來源伺服器，server.deyu.wang 已在表列中。

```
[root@kvm81 ~]# chronyc sources
210 Number of sources = 5
MS Name/IP address         Stratum Poll Reach LastRx Last sample
===============================================================================
^- server.deyu.wang              3   6   177    52   -837us[ -831
   us] +/-   55ms
^- ns.rpb.gov.tw                 2   6   377    48  +3203us[+3209
   us] +/-  426ms
^+ 117-56-73-145.HINET-IP.hi     3   6   377   241   -102us[ +142
   us] +/-  106ms
```

```
^+ 220-135-58-124.HINET-IP.h     3   6   377    47   +248us[ +248
   us] +/-   76ms
^* 123-204-45-116.static.see     3   6   377    50   -636us[ -630
   us] +/-   67ms
```

6. chronyc 是互動式指令，若不知道此指令可以使用哪些 command？可以先進入其互動式模式中，輸入 help 命令，就可以列出可用的 command。

```
[root@kvm7 ~]# chronyc
chrony version 1.29.1
Copyright (C) 1997-2003, 2007, 2009-2013 Richard P. Curnow and
   others
chrony comes with ABSOLUTELY NO WARRANTY.  This is free software,
    and
you are welcome to redistribute it under certain conditions.  See
    the
GNU General Public License version 2 for details.

chronyc> help
Commands:
accheck <address> : Check whether NTP access is allowed to <
   address>
activity : Check how many NTP sources are online/offline
add peer <address> ... : Add a new NTP peer
add server <address> ... : Add a new NTP server
allow [<subnet-addr>] : Allow NTP access to that subnet as a
   default
allow all [<subnet-addr>] : Allow NTP access to that subnet and
   all children
burst <n-good>/<n-max> [<mask>/<masked-address>] : Start a rapid
   set of measurements
clients : Report on clients that have accessed the server
cmdaccheck <address> : Check whether command access is allowed to
    <address>
cmdallow [<subnet-addr>] : Allow command access to that subnet as
    a default
cmdallow all [<subnet-addr>] : Allow command access to that
   subnet and all children
cmddeny [<subnet-addr>] : Deny command access to that subnet as a
    default
cmddeny all [<subnet-addr>] : Deny command access to that subnet
   and all children
cyclelogs : Close and re-open logs files
delete <address> : Remove an NTP server or peer
deny [<subnet-addr>] : Deny NTP access to that subnet as a
   default
deny all [<subnet-addr>] : Deny NTP access to that subnet and all
    children
```

```
27 dump : Dump all measurements to save files
   local off : Disable server capability for unsynchronised clock
29 local stratum <stratum> : Enable server capability for
       unsynchronised clock
   makestep : Jump the time to remove any correction being slewed
31 manual off|on|reset : Disable/enable/reset settime command and
       statistics
   manual list : Show previous settime entries
33 maxdelay <address> <new-max-delay> : Modify maximum round-trip
       valid sample delay for source
   maxdelayratio <address> <new-max-ratio> : Modify max round-trip
       delay ratio for source
35 maxdelaydevratio <address> <new-max-ratio> : Modify max round-
       trip delay dev ratio for source
   maxpoll <address> <new-maxpoll> : Modify maximum polling interval
        of source
37 maxupdateskew <new-max-skew> : Modify maximum skew for a clock
       frequency update to be made
   minpoll <address> <new-minpoll> : Modify minimum polling interval
        of source
39 minstratum <address> <new-min-stratum> : Modify minimum stratum
       of source
   offline [<mask>/<masked-address>] : Set sources in subnet to
       offline status
41 online [<mask>/<masked-address>] : Set sources in subnet to
       online status
   password [<new-password>] : Set command authentication password
43 polltarget <address> <new-poll-target> : Modify poll target of
       source
   reselect : Reselect synchronisation source
45 rtcdata : Print current RTC performance parameters
   settime <date/time (e.g. Nov 21, 1997 16:30:05 or 16:30:05)> :
       Manually set the daemon time
47 sources [-v] : Display information about current sources
   sourcestats [-v] : Display estimation information about current
       sources
49 tracking : Display system time information
   trimrtc : Correct RTC relative to system clock
51 waitsync [max-tries [max-correction [max-skew]]] : Wait until
       synchronised
   writertc : Save RTC parameters to file
53
   authhash <name>: Set command authentication hash function
55 dns -n|+n : Disable/enable resolving IP addresses to hostnames
   dns -4|-6|-46 : Resolve hostnames only to IPv4/IPv6/both
       addresses
57 timeout <milliseconds> : Set initial response timeout
   retries <n> : Set maximum number of retries
59 exit|quit : Leave the program
   help : Generate this help
61
```

```
chronyc>
```

7. 重新啓動 chronycd。

```
[root@kvm81 ~]# systemctl restart chronyd.service
```

8. 以 -l 選項查看 chrony 自動校時狀態及工作紀錄，倒數第二行，系統調整時間 127369.424623 秒。

```
[root@kvm81 ~]# systemctl status chronyd.service -l
chronyd.service - NTP client/server
   Loaded: loaded (/usr/lib/systemd/system/chronyd.service;
       enabled)
   Active: active (running) since Mon 2015-01-19 01:26:00 CST; 1
       day 11h ago
  Process: 18379 ExecStartPost=/usr/libexec/chrony-helper add-
      dhclient-servers (code=exited, status=0/SUCCESS)
  Process: 18376 ExecStart=/usr/sbin/chronyd -u chrony $OPTIONS (
      code=exited, status=0/SUCCESS)
 Main PID: 18378 (chronyd)
   CGroup: /system.slice/chronyd.service └──
           18378 /usr/sbin/chronyd -u chrony

Jan 19 01:26:00 kvm81.deyu.wang systemd[1]: Starting NTP client/
   server...
Jan 19 01:26:00 kvm81.deyu.wang chronyd[18378]: chronyd version
   1.29.1 starting
Jan 19 01:26:00 kvm81.deyu.wang chronyd[18378]: Linux kernel
   major=3 minor=10 patch=0
Jan 19 01:26:00 kvm81.deyu.wang chronyd[18378]: hz=100 shift_hz=7
    freq_scale=1.00000000 nominal_tick=10000 slew_delta_tick=833
   max_tick_bias=1000 shift_pll=2
Jan 19 01:26:00 kvm81.deyu.wang chronyd[18378]: Frequency 0.008
   +/- 0.068 ppm read from /var/lib/chrony/drift
Jan 19 01:26:00 kvm81.deyu.wang systemd[1]: Started NTP client/
   server.
Jan 19 01:26:08 kvm81.deyu.wang chronyd[18378]: Selected source
   120.119.28.1
Jan 19 01:26:08 kvm81.deyu.wang chronyd[18378]: System clock
   wrong by 127369.424623 seconds, adjustment started
Jan 20 12:48:57 kvm81.deyu.wang chronyd[18378]: System clock was
   stepped by 127369.425 seconds
```

9. chronyc 手動校時。

```
[root@kvm81 ~]# date -s 2015-01-19
Mon Jan 19 00:00:00 CST 2015
[root@kvm81 ~]# chronyc -a makestep
200 OK
200 OK
[root@kvm81 ~]# date
Tue Jan 20 11:27:29 CST 2015
```

10.3 ntpd 使用

1. 沒移除 chrony 套件，直接安裝 ntp，啓動後看似一切正常，但在重新開機後，因與 chrony 衝突，而無法正常啓動。

```
[root@kvm81 ~]# yum install ntpd
[root@kvm81 ~]# grep deyu.wang /etc/ntp.conf
server deyu.wang
[root@kvm81 ~]# systemctl restart ntpd.service
[root@kvm81 ~]# systemctl enable ntpd.service
ln -s '/usr/lib/systemd/system/ntpd.service' '/etc/systemd/system
   /multi-user.target.wants/ntpd.service'
[root@kvm81 ~]# ntpq -p
     remote           refid      st t when poll reach   delay
         offset  jitter
==============================================================================

+deyu.wang       59.124.29.241    3 u   16   64    1    0.129
   1.627   0.000
-117-56-223-235. 211.79.171.1     3 u    5   64    1    7.207
   3.873   0.294
+220-135-58-124. 118.163.81.62    3 u    4   64    1   20.359
   -0.722   0.157
*sun.stu.edu.tw  133.100.10.8     2 u    3   64    1    8.500
   0.582   0.335
```

2. 若要使用 ntp，則必須關閉 chrony 開機啓動，也就是 disable。

```
[root@kvm81 ~]# systemctl disable chronyd.service
rm '/etc/systemd/system/multi-user.target.wants/chronyd.service'
```

3. 或者直接移除 chrony，移除時注意其相依套件是否確定要移除。

```
[root@kvm81 ~]# yum remove chrony
```

Chapter 11

其他

11.1 用户id

1. 在 v6 ，一般用户 UID 從 500 編起。
2. 在 v7 ，一般用户 UID 從 1000 編起。