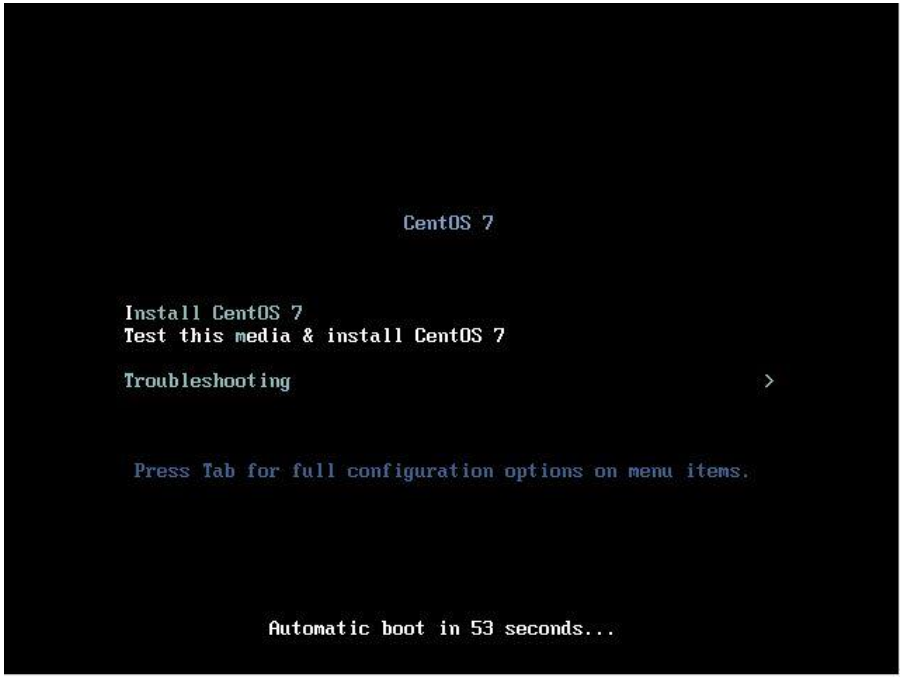
新北市首頁系統操控原力進化(CentOS)

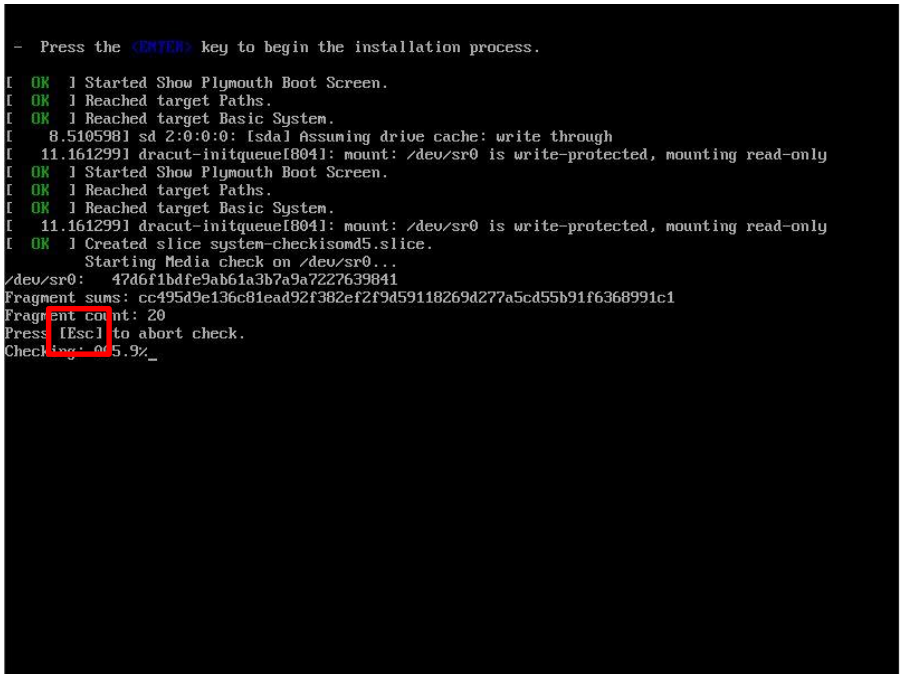
新北市政府教育局
教育研究及資訊發展科
林璟豐
80723456＃516

大綱

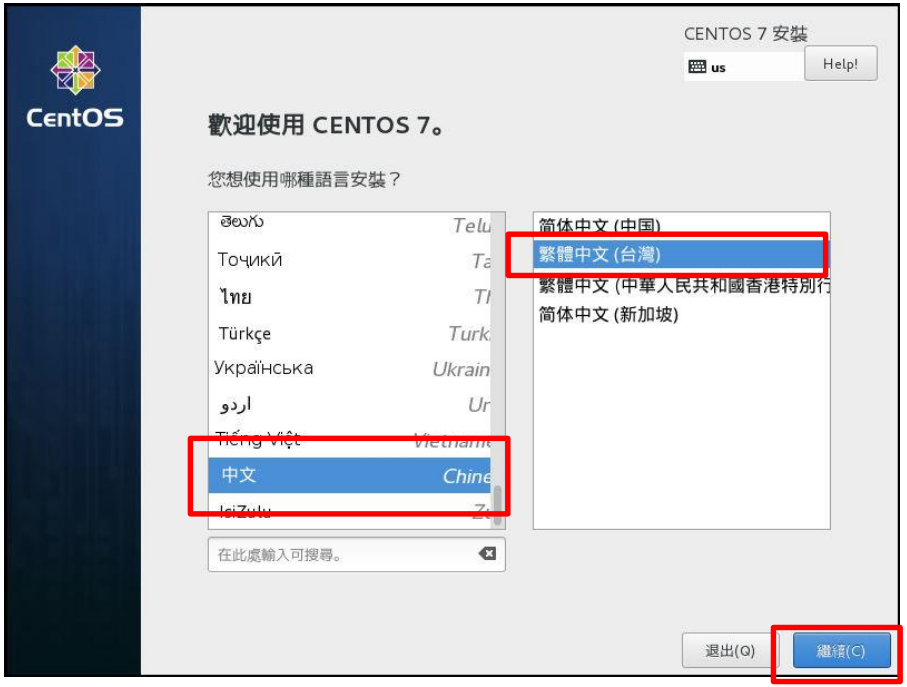
- CentOS 安裝
- 網路管理
- SSH 管理
- 忘記 root 密碼
- DNS Server 管理
- 紀錄管理
- 網頁伺服器管理
- Let's Encrypt 憑證申請
- Bash Script 實作
- 備份管理
- 擴充硬碟

CentOS 7 安装


CentOS 7
Install CentOS 7
Test this media & install CentOS 7
Troubleshooting
Press Tab for full configuration options on menu items.
Automatic boot in 53 seconds...

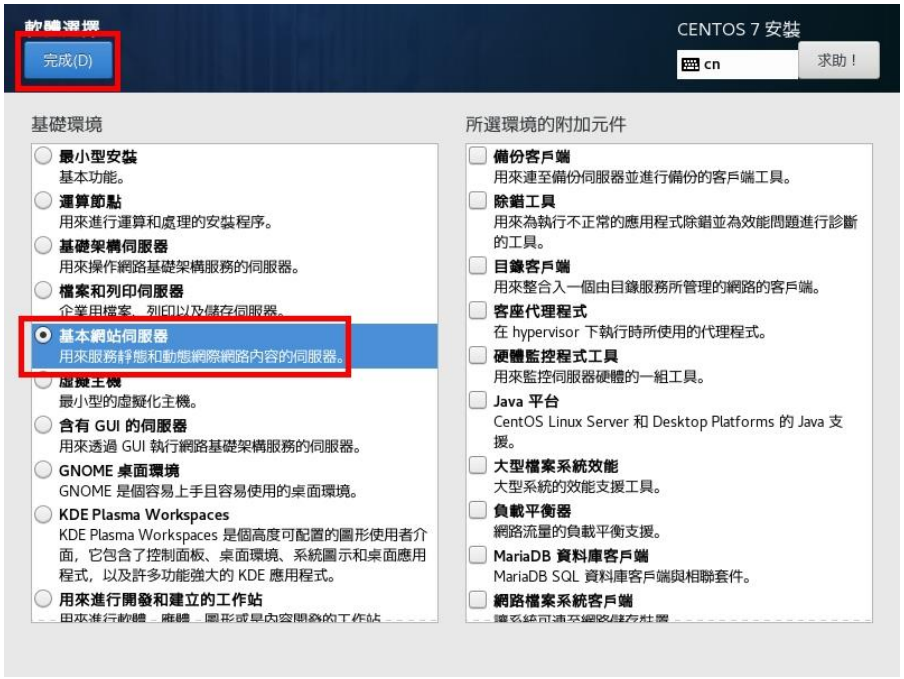

Press the <ENTER> key to begin the installation process.
[OK] Started Show Plymouth Boot Screen.
[OK] Reached target Paths.
[OK] Reached target Basic System.
[8.510598] sd 2:0:0:0: [sda] Assuming drive cache: write through
[11.161299] dracut-initqueue[804]: mount: /dev/sr0 is write-protected, mounting read-only
[OK] Started Show Plymouth Boot Screen.
[OK] Reached target Paths.
[OK] Reached target Basic System.
[11.161299] dracut-initqueue[804]: mount: /dev/sr0 is write-protected, mounting read-only
[OK] Created slice system-checkisomd5.slice.
Starting Media check on /dev/sr0...
/dev/sr0: 47d6f1bdfe9ab61a3b7a9a7227639841
Fragment sums: cc495d9e136c81ead92f382ef2f9d59118269d277a5cd55b91f6368991c1
Fragment count: 20
Press [Esc] to abort check.
Checking: 05.9%_

CentOS 7 安裝


CentOS
CENTOS 7 安裝
us
Help!
歡迎使用 CENTOS 7。
您想使用哪種語言安裝？
Тоҷикӣ
ไทย
Türkçe
Українська
اردو
中文
简体中文 (中国)
繁體中文 (台灣)
繁體中文 (中華人民共和國香港特別行
简体中文 (新加坡)
在此處輸入可搜尋。
退出(Q)
繼續(C)


CentOS
安裝摘要
CENTOS 7 安裝
cn
Help!
本地化設定
日期時間(T)
亞洲/台北 時區
鍵盤配置(K)
漢語
語言支援(L)
繁體中文 (台灣)
SECURITY
SECURITY POLICY
No profile selected
軟體
安裝來源(I)
軟體選擇(S)
退出(Q)
開始安裝(B)
在您按下「開始安裝」之前，我們不會對您的磁碟進行任何動作。
在繼續下個步驟之前，請先完成有標記此圖示的項目。

CentOS 7 安裝


完成(D)
CENTOS 7 安裝
cn
求助！
基礎環境
最小型安裝
基本功能。
運算節點
用來進行運算和處理的安裝程序。
基礎架構伺服器
用來操作網路基礎架構服務的伺服器。
檔案和列印伺服器
基本網站伺服器
用來服務靜態和動態網際網路內容的伺服器。
含有 GUI 的伺服器
用來透過 GUI 執行網路基礎架構服務的伺服器。
GNOME 桌面環境
GNOME 是個容易上手且容易使用的桌面環境。
KDE Plasma Workspaces
KDE Plasma Workspaces 是個高度可配置的圖形使用者介面，它包含了控制面板、桌面環境、系統圖示和桌面應用程式，以及許多功能強大的 KDE 應用程式。
用來進行開發和建立的工作站
所選環境的附加元件
備份客戶端
用來連至備份伺服器並進行備份的客戶端工具。
除錯工具
用來為執行不正常的應用程式除錯並為效能問題進行診斷的工具。
目錄客戶端
用來整合入一個由目錄服務所管理的網路的客戶端。
客座代理程式
在 hypervisor 下執行時所使用的代理程式。
硬體監控程式工具
用來監控伺服器硬體的一組工具。
Java 平台
CentOS Linux Server 和 Desktop Platforms 的 Java 支援。
大型檔案系統效能
大型系統的效能支援工具。
負載平衡器
網路流量的負載平衡支援。
MariaDB 資料庫客戶端
MariaDB SQL 資料庫客戶端與相關套件。
網路檔案系統客戶端

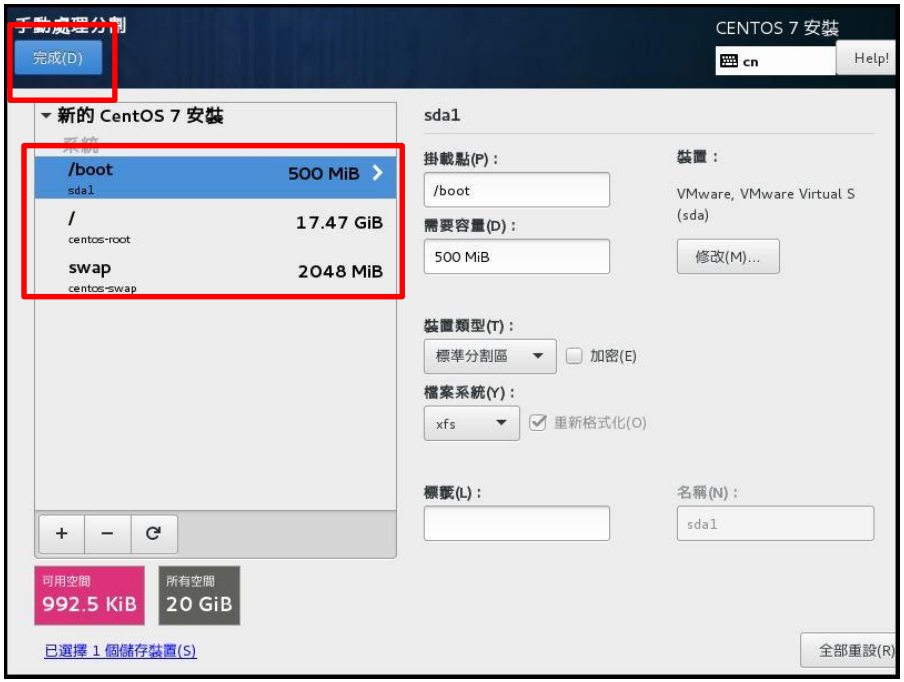

CentOS
安裝摘要
CENTOS 7 安裝
cn
Help!
SECURITY POLICY
No profile selected
軟體
安裝來源(I)
本地端媒體
軟體選擇(S)
含有 GUI 的伺服器
系統
安裝目的地(D)
已選擇自動磁碟分割
KDUMP
已啟用 Kdump
網路與主機名稱(N)
未連線
退出(Q)
開始安裝(B)
在您按下「開始安裝」之前，我們不會對您的磁碟進行任何動作。
在繼續下個步驟之前，請先完成有標記此圖示的項目。

CentOS 7 安裝


安裝目的地
完成(D)
CENTOS 7 安裝
cn
Help!
裝置選擇
請選取您想要安裝的目標裝置。直到您按下主選單的「開始安裝」按鈕為止，我們都不會碰觸它們。
本機標準磁碟
20 GiB
VMware, VMware Virtual S
sda / 20 GiB 可用
我們不會更動到留在此處未選取的磁碟。
特殊磁碟與網路磁碟
加入磁碟(A)...
我們不會更動到留在此處未選取的磁碟。
其它儲存選項
分割硬碟
自動配置磁碟分割 (u)。
讓我自行配置磁碟分割 (I)。
完整磁碟摘要與開機載入器(F)...
已選取 1 顆磁碟；20 GiB 容量；20 GiB 可用


手動處理分割
完成(D)
CENTOS 7 安裝
cn
Help!
新的 CentOS 7 安裝
您尚未為您的 CentOS 7 安裝建立任何掛載點。您可
請點按這裡讓系統自動建立(C)。
點按「+」鈕方建立新的掛載點。
新的掛載點將使用以下磁碟分割格式：
LVM
當您為您的 CentOS 7 安裝建立掛載點時，您可在此處檢視其詳細資料。
可用空間
20 GiB
所有空間
20 GiB
已選擇 1 個儲存裝置(S)
全部重設(R)

CentOS 7 安裝


完成(D)
CENTOS 7 安裝
cn
Help!
新的 CentOS 7 安裝
/boot
sda1
500 MiB
/
centos-root
17.47 GiB
swap
centos-swap
2048 MiB
sda1
掛載點(P)：
/boot
需要容量(D)：
500 MiB
裝置：
VMware, VMware Virtual S (sda)
修改(M)...
裝置類型(T)：
標準分割區
加密(E)
檔案系統(Y)：
xfs
重新格式化(O)
標籤(L)：
名稱(N)：
sda1
可用空間
992.5 KiB
所有空間
20 GiB
已選擇 1 個儲存裝置(S)
全部重設(R)

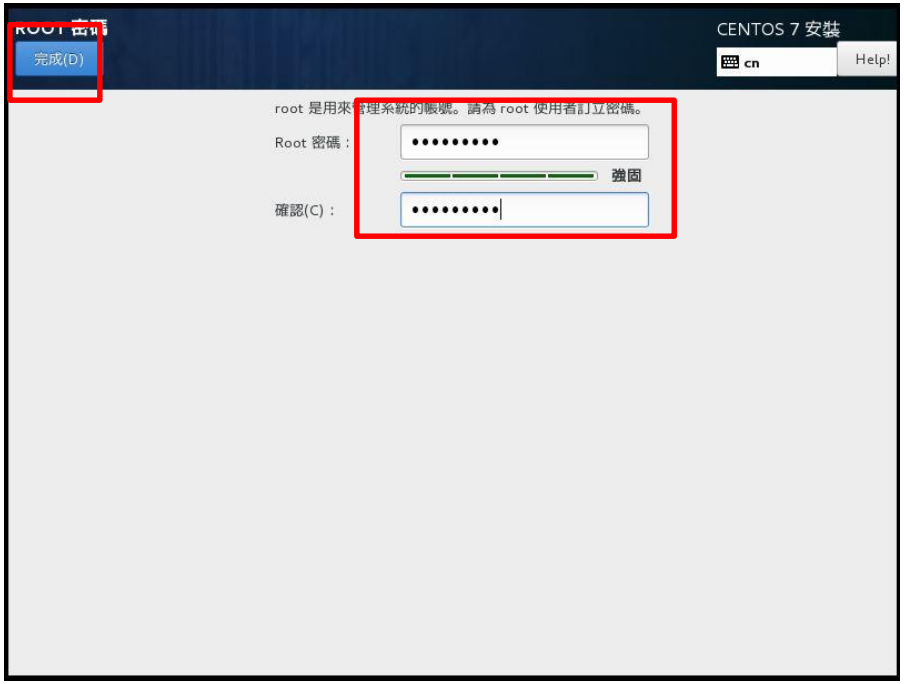

手動處理分割
完成(D)
CENTOS 7 安裝
cn
Help!
變更的摘要
在您返回主選單並選擇安裝後，您的自訂設定會對您所選的磁碟產生下列更動：
命令 動作 類型 裝置名稱 掛載點
1 Destroy Format Unknown sda
2 建立格式 分割表 (MSDOS) sda
3 建立裝置 partition sda1
4 建立格式 xfs sda1 /boot
5 建立裝置 partition sda2
6 建立格式 physical volume (LVM) sda2
7 建立裝置 lvmvg centos
8 建立裝置 lvmlv centos-swap
9 建立格式 swap centos-swap
10 建立裝置 lvmlv centos-root
11 建立格式 xfs centos-root /
取消並返回自訂分割(C)
接受變更(A)
可用空間
992.5 KiB
所有空間
20 GiB
已選擇 1 個儲存裝置(S)
全部重設(R)

CentOS 7 安裝


安裝摘要
CENTOS 7 安裝
cn
Help!
CentOS
SECURITY
SECURITY POLICY
No profile selected
軟體
安裝來源(I)
本地端媒體
軟體選擇(S)
含有 GUI 的伺服器
系統
安裝目的地(D)
已選擇自訂磁碟分割
KDUMP
已啟用 Kdump
網路與主機名稱(N)
未連線
退出(Q)
開始安裝(B)

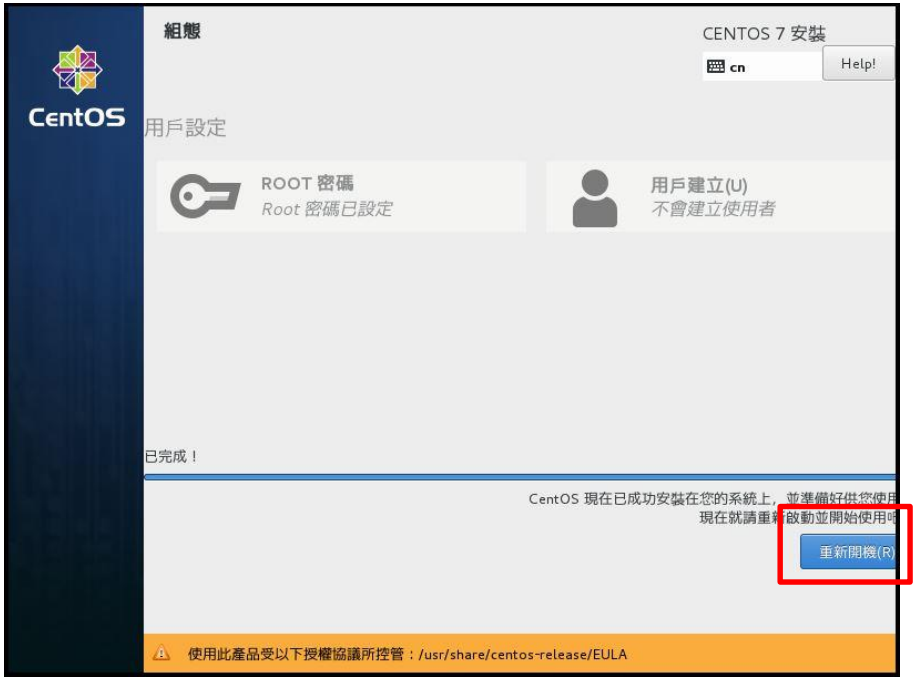

組態
CENTOS 7 安裝
cn
Help!
CentOS
用戶設定
ROOT 密碼
尚未設定 root 密碼
用戶建立(U)
不會建立使用者
正在於 /dev/sda 上建立 disklabel
CentOS Virtualization SIG
Virtualization in CentOS, virtualization of CentOS.
wiki.centos.org/SpecialInterestGroup
在繼續下個步驟之前，請先完成有標記此圖示的項目。

CentOS 7 安裝


完成(D)
CENTOS 7 安裝
cn
Help!
root 是用來管理系統的帳號。請為 root 使用者訂立密碼。
Root 密碼：
強固
確認(C)：


組態
CENTOS 7 安裝
cn
Help!
CentOS
用戶設定
ROOT 密碼
Root 密碼已設定
用戶建立(U)
不會建立使用者
正在執行安裝後的設定工作
CentOS Virtualization SIG
Virtualization in CentOS, virtualization of CentOS.
wiki.centos.org/SpecialInterestGroup

CentOS 7 安裝


組態
CENTOS 7 安裝
cn
Help!
CentOS
用戶設定
ROOT 密碼
Root 密碼已設定
用戶建立(U)
不會建立使用者
已完成！
CentOS 現在已成功安裝在您的系統上，並準備好供您使用
現在就請重新啟動並開始使用吧
重新開機(R)
使用此產品受以下授權協議所控管：/usr/share/centos-release/EULA


CentOS Linux 7 (Core)
Kernel 3.10.0-957.el7.x86_64 on an x86_64
localhost login: root
Password:
[root@localhost ~]#

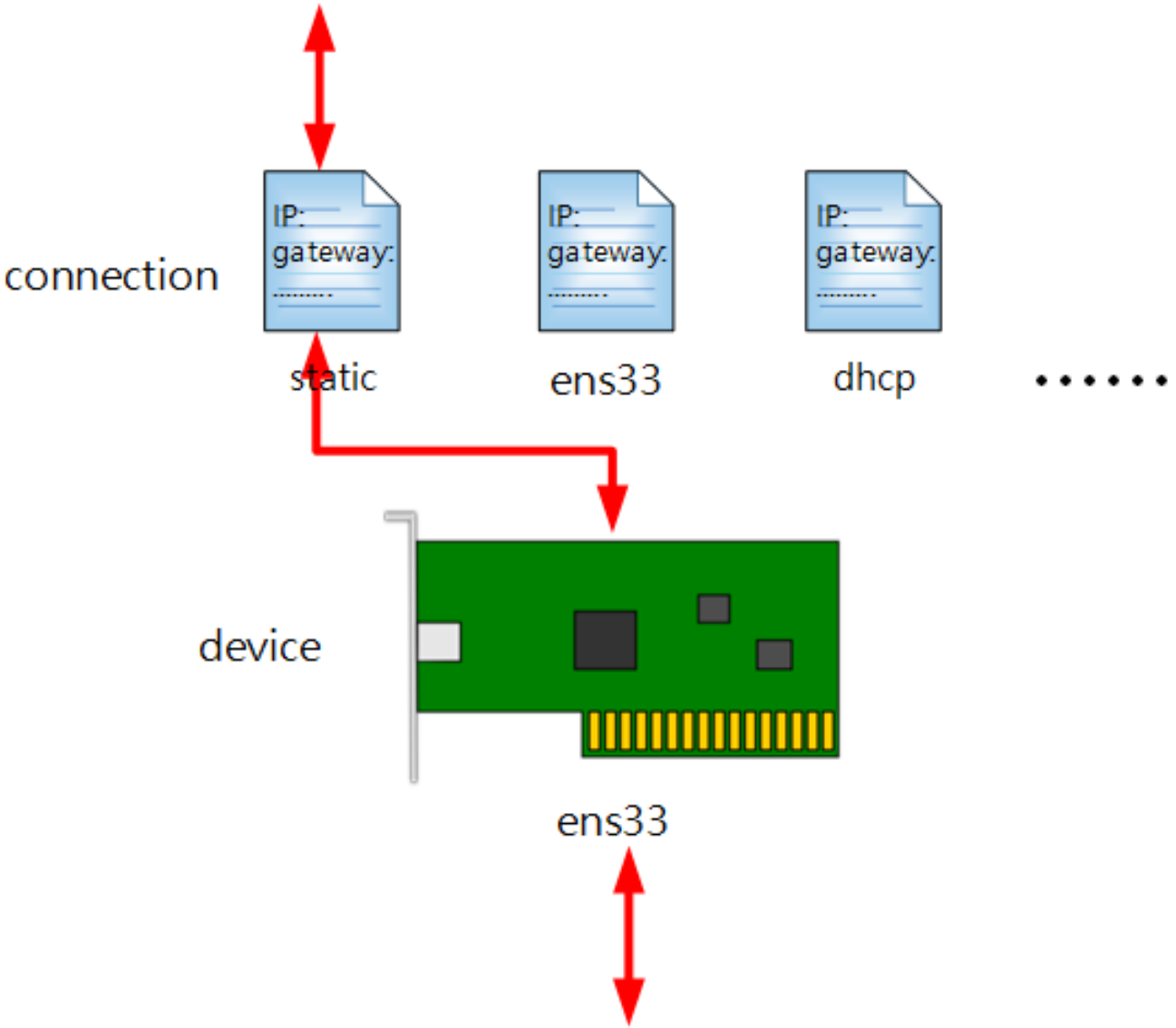
網路管理

- 查詢 IP 位址：
  - # ip address (或 # ifconfig)
- 查詢連線狀態：
  - # nmcli connection show
- 查看連線設定檔：
  - # nmcli con show ens33
- 啟用連線設定檔：
  - # nmcli con up ens33
- 停用連線設定檔：
  - # nmcli con down ens33

網路管理

- ip 指令：
  - # ip addr show ens33 (顯示該裝置的IP資訊)
  - # ip -s -h link show ens33 (顯示該裝置的統計)
  - # ip route (顯示路由表)
- 建立連線設定檔：
  - # nmcli con add con-name "static"
    type ethernet ifname ens33 autoconnect yes
    ipv4.addresses 163.20.174.xxx/24
    ipv4.gateway 163.20.174.254
    ipv4.method manual
    ipv4.dns 203.72.153.153
    +ipv4.dns 203.72.153.154
    ipv6.addresses 2001:288:228F:5::xxx/64
    ipv6.gateway 2001:288:228F:5::FF
    ipv6.method manual
    ipv6.dns 2001:288:2200:121::153
    +ipv6.dns 2001:288:2200:121::154

網路管理


connection
IP:
gateway:
IP:
gateway:
IP:
gateway:
static
ens33
dhcp
.....
device
ens33

網路管理

- 測試網路連通：
  - # ping -c4 IP位址 (加選項 -6 即可 ping IPv6)
  - # ping 8.8.8.8
  - # ping -6 2001:4860:4860::8888
  - # ping -c4 網址(FQDN) (順便測 DNS 解析)
  - # ping www.hinet.net
  - # ping -6 www.hinet.net
- 查詢 DNS 設定：
  - # cat /etc/resolv.conf
- 查詢 hosts 紀錄：
  - # cat /etc/hosts

網路管理

- 查詢 hosts 紀錄：
  - # cat /etc/hosts
- 名稱解析順序：
  - Local Cache --> Local Hosts --> DNS
- DNS 解析測試：
  - # nslookup www.google.com
  - # nslookup -q=a www.google.com
  - # nslookup -q=aaaa www.google.com
  - # nslookup -q=ns dfsh.ntpc.edu.tw
  - # host www.hinet.net

網路管理

- 路由測試：
  - # traceroute -n 168.95.1.1
  - # traceroute -n www.google.com
- 查詢主機名稱：
  - # hostname
- 設定主機名稱：
  - # hostnamectl set-hostname centosNUM (NUM 為 IP 位址末碼)
- 查詢主機相關資訊：
  - # hostnamectl status

SSH 管理

- 查看 SSHD 服務是否啟用：
  - # systemctl status sshd.service
- 查看防火牆是否允許 SSH (port 22) 通過：
  - # firewall-cmd --list-all
- CentOS 使用 SSH 連線
  - # ssh USERNAME@HOSTNAME "Command"
  - # ssh root@localhost
  - # ssh root@localhost "ls -l /tmp"
  - # ssh root@163.20.174.xxx
- PuTTY
  - https://www.putty.org/
- xShell
  - https://www.netsarang.com/en/xshell/
- 編輯使用環境：
  - # vi /root/.bashrc

    alias vi='vim'

SSH 管理

- 檢視目前登入系統的帳號：
  - # who
- 檢視目前登入帳號及正在做什麼：
  - # w
- 查詢帳號最後一次登入的訊息：
  - # lastlog
- 查詢目前及過去登入的帳號訊息：
  - # last
- 查詢過去失敗的登入記錄：
  - # lastb

SSH 管理

- 編輯 SSH 伺服器設定檔：
  - # vi /etc/ssh/sshd_config
    PermitRootLogin yes (是否允許root登入)
    PasswordAuthentication yes (是否允許密碼方式登入)
    MaxAuthTries 6 (最多錯誤密碼次數)
    PubkeyAuthentication yes (是否允許Public key)
    UseDNS no (是否使用dns反查)
- 重新載入 SSHD：
  - # systemctl reload sshd
- 重新啟動 SSHD：
  - #systemctl restart sshd

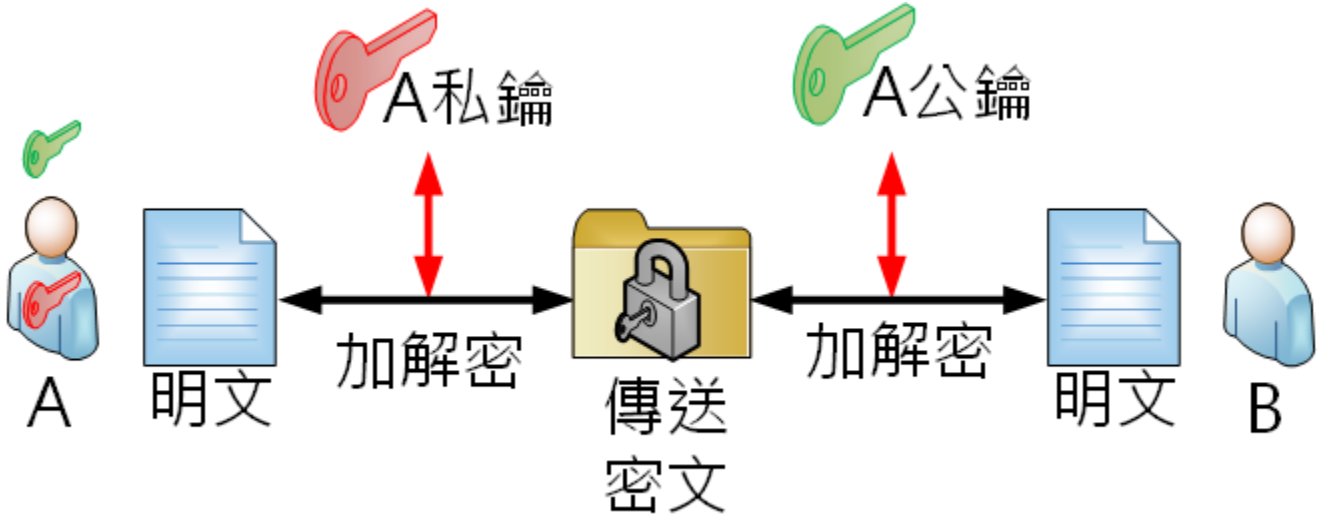
SSH 管理

- 對稱式加密

  加密解密使用同一把金鑰

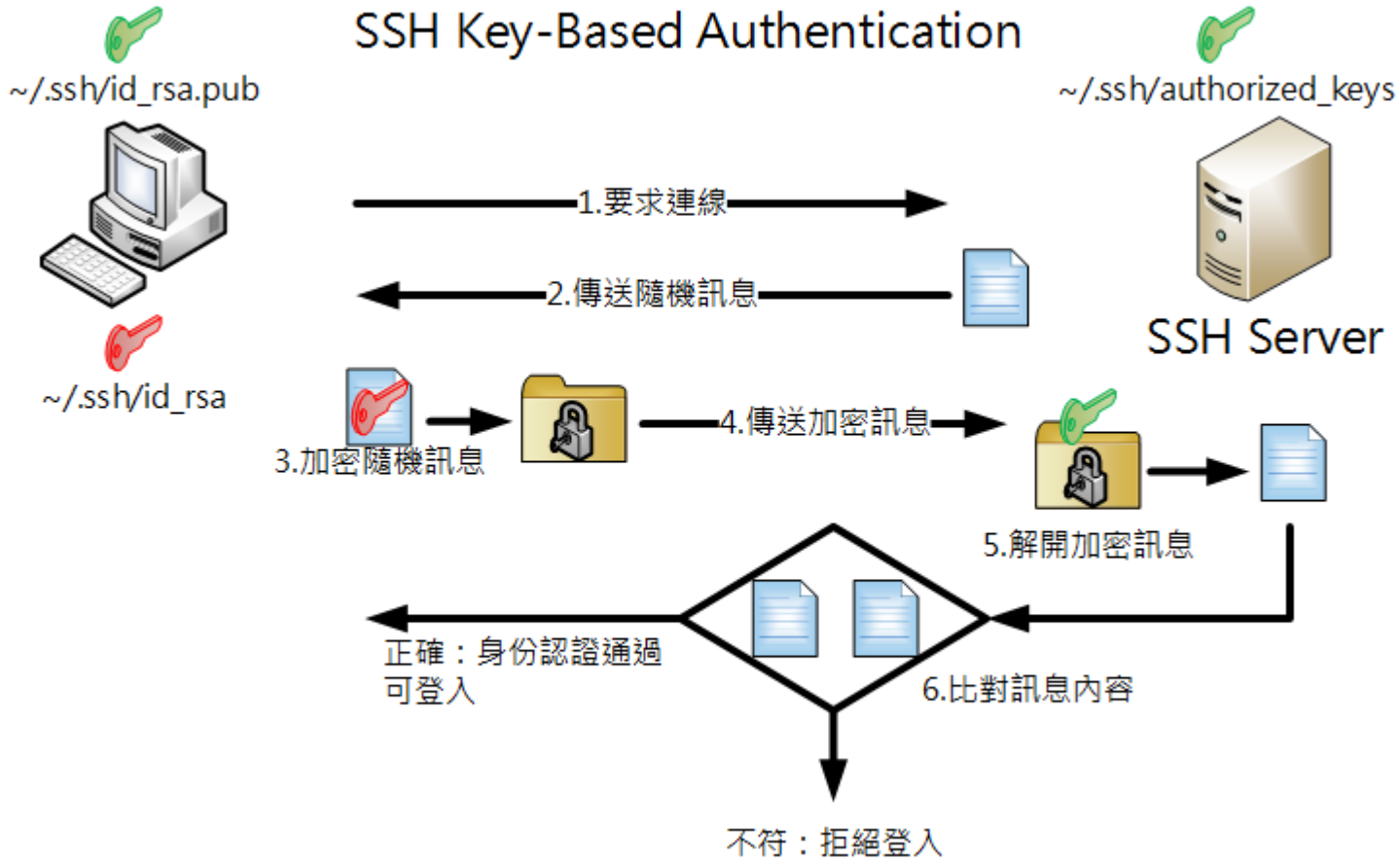
- 非對稱式加密

  產生公鑰(Public Key)及私鑰(Private Key)，利用其中一把金鑰加密，只能用另一把金鑰解密



SSH 管理

- SSH Key-Based Authentication

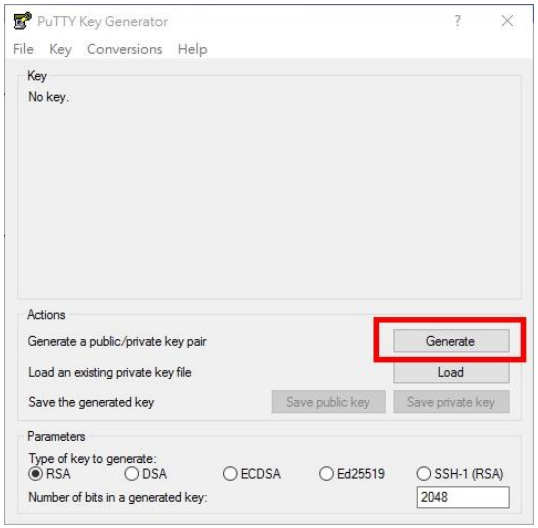


SSH 管理

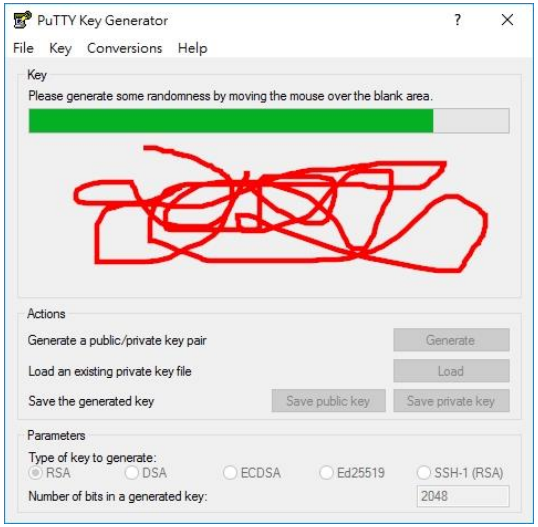
- 金鑰認證方式登入：
  - # ssh-keygen (產生公鑰及私鑰)
  - # ls -l ~/.ssh (檢視生成的公私鑰)
  - # ssh-copy-id root@localhost (上傳公鑰)
  - # ssh root@localhost (免密碼直接登入)
- 檢視已上傳公鑰：
  - # cat ~/.ssh/authorized_keys
- 金鑰方式登入其他主機：
  - # ssh-copy-id root@163.20.174.xxx

SSH 管理

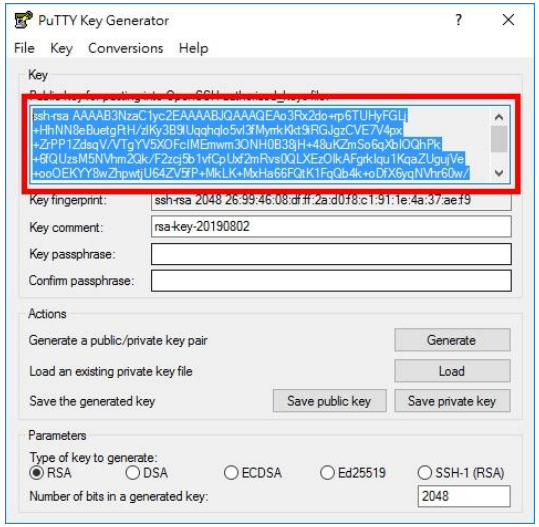
- puttygen 產生金鑰：
  - 開啟 puttygen.exe



點 Generate



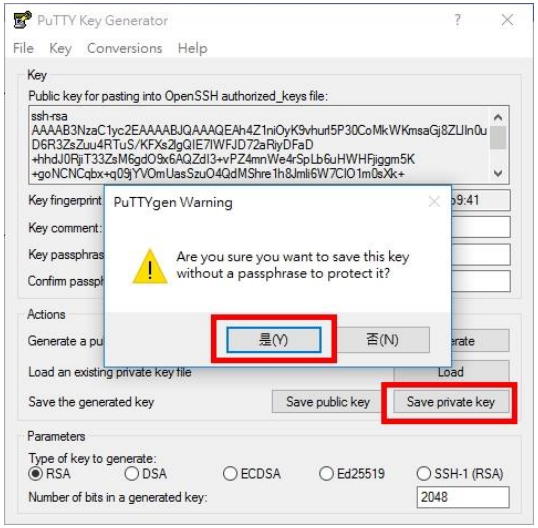
滑鼠於空白處任意移動



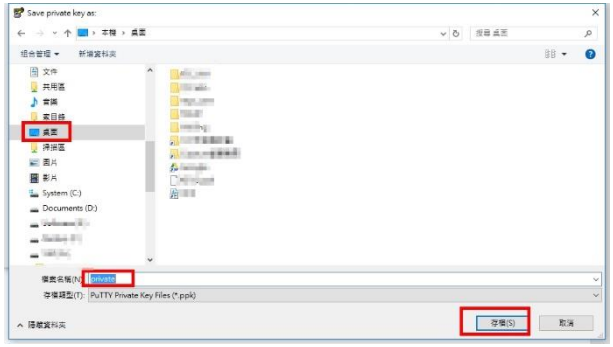
將公鑰全選、複製

SSH 管理

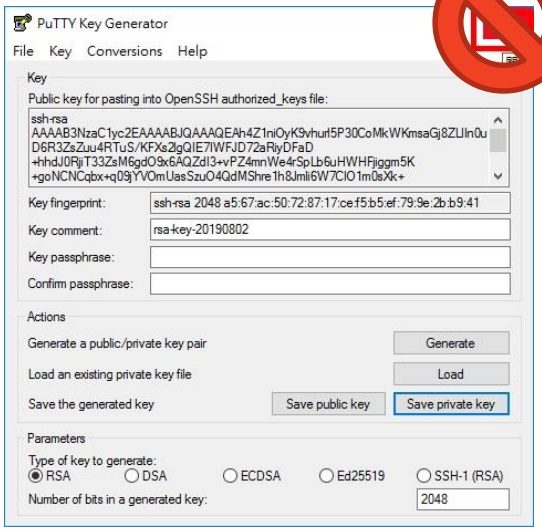
- puttygen 產生金鑰：



點 Save private key
點「是(Y)」



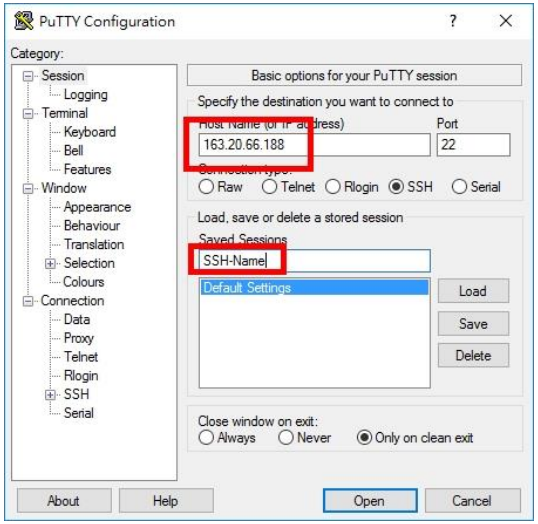
指定檔名
儲存於指定位置



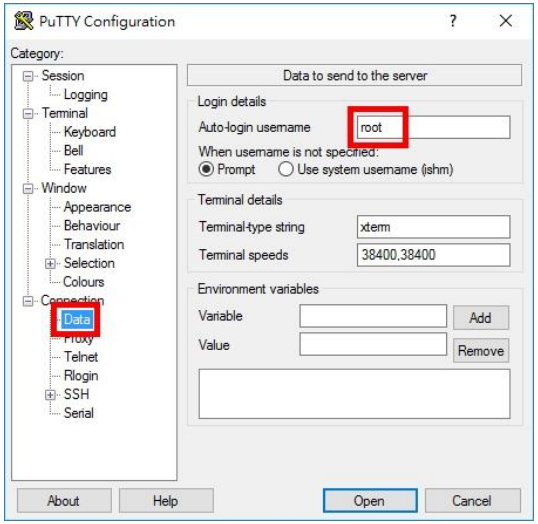
暫時不要
關閉 puttygen.exe

SSH 管理

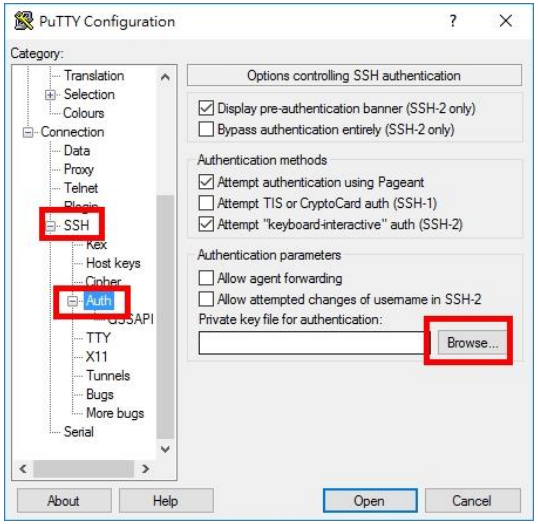
- putty 設定金鑰登入：
  - 開啟 putty.exe



輸入連線IP
設定Session名稱



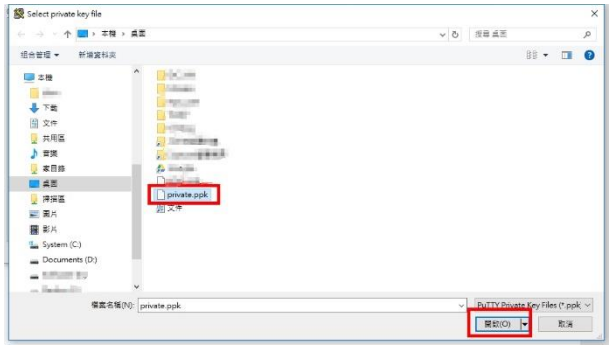
點 Data 欄位
設定 root 自動登入



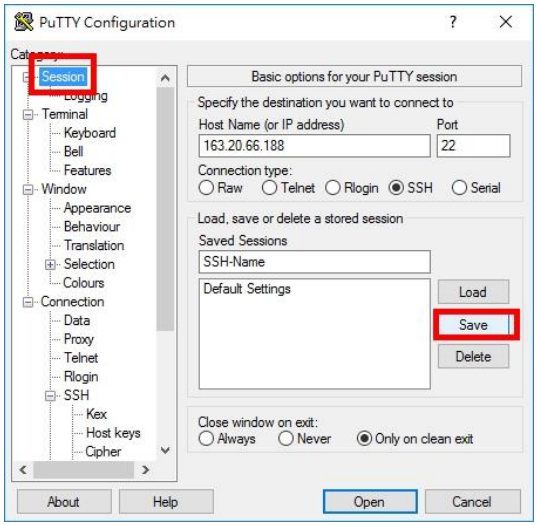
點 SSH 欄位
點 Auth 欄位
點 Browser...

SSH 管理

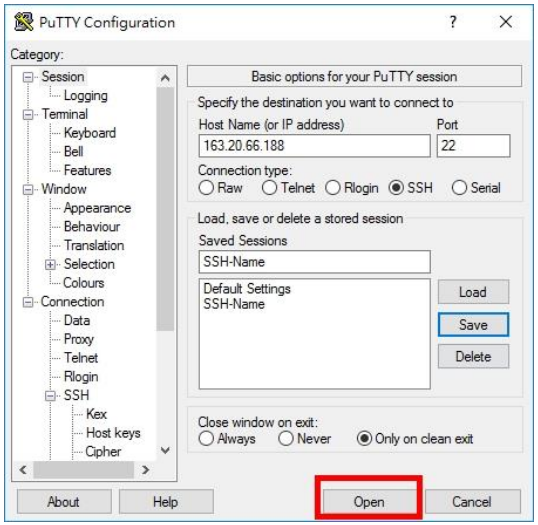
- putty 設定金鑰登入：



選擇私鑰
點「開啟(O)」



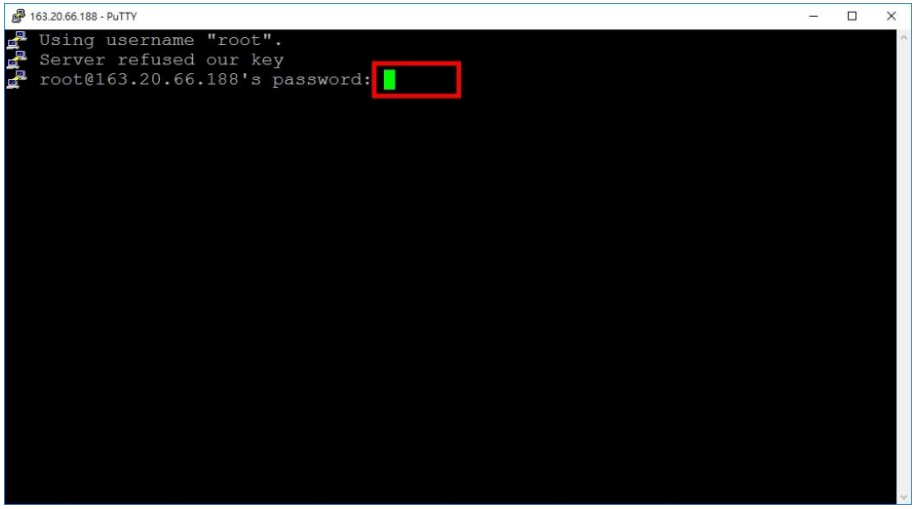
點 Session 欄位
點 Save



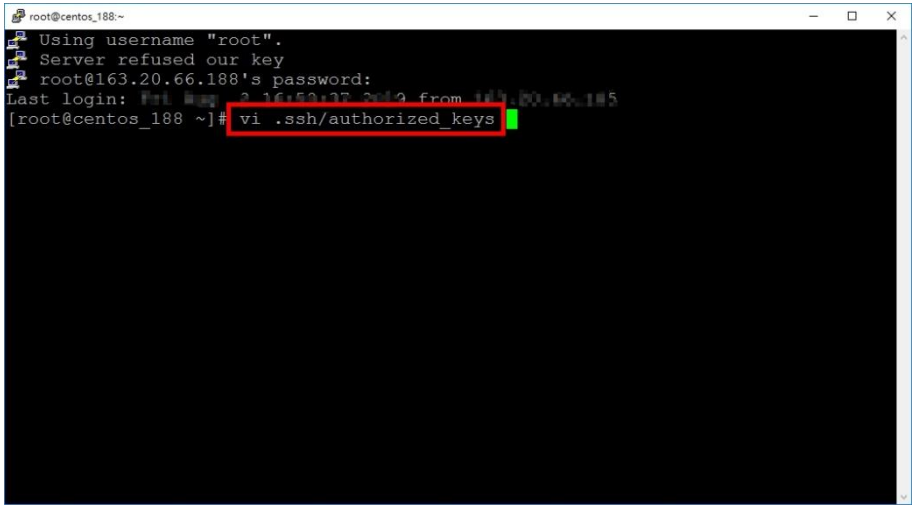
點 Open

SSH 管理

- putty 設定金鑰登入：



還沒上傳公鑰
先用密碼登入

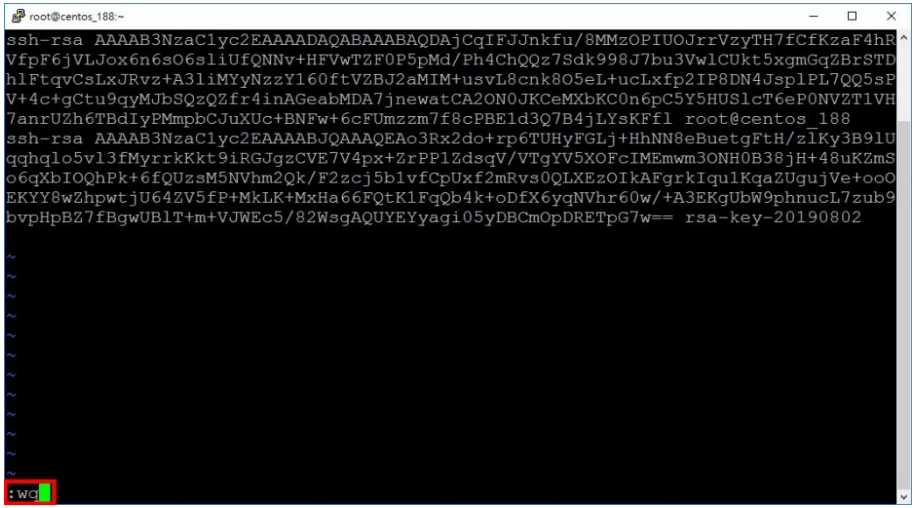


vi /root/.ssh/authorized_keys

SSH 管理

- putty 設定金鑰登入：

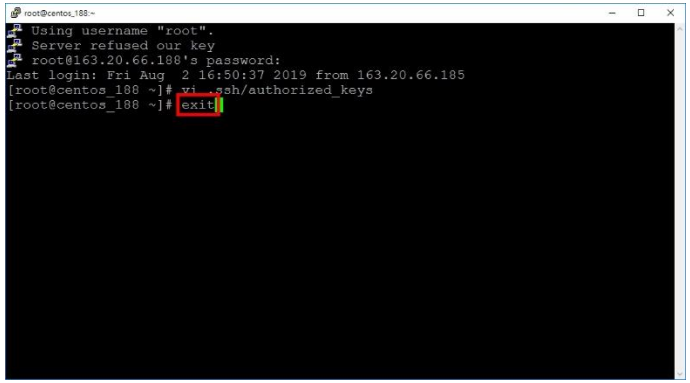
「i」進入編輯模式
[Shift] + [insert] 貼上已複製的公鑰
(或按滑鼠右鍵貼上)



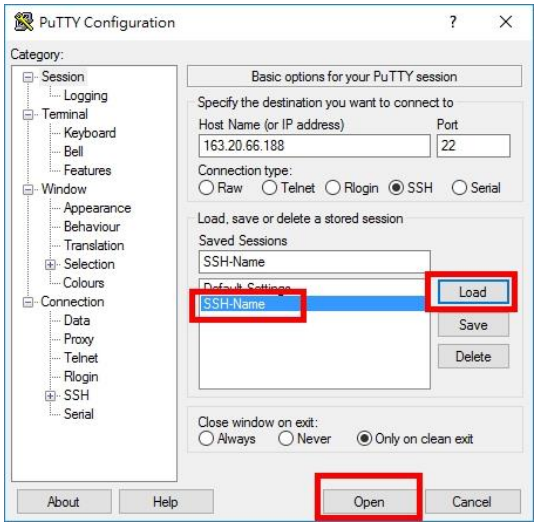
[ESC] 切換到命令模式
輸入「:wq」存檔退出

SSH 管理

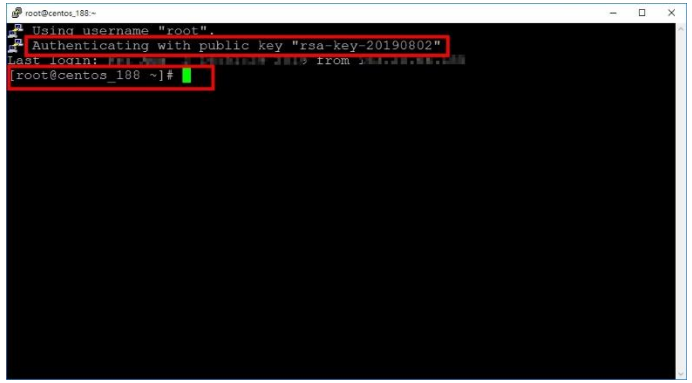
- putty 設定金鑰登入：



輸入 exit 退出



開啟 putty.exe
點 Session 名稱
點 Load
點 Open



已成功用金鑰登入

SSH 管理

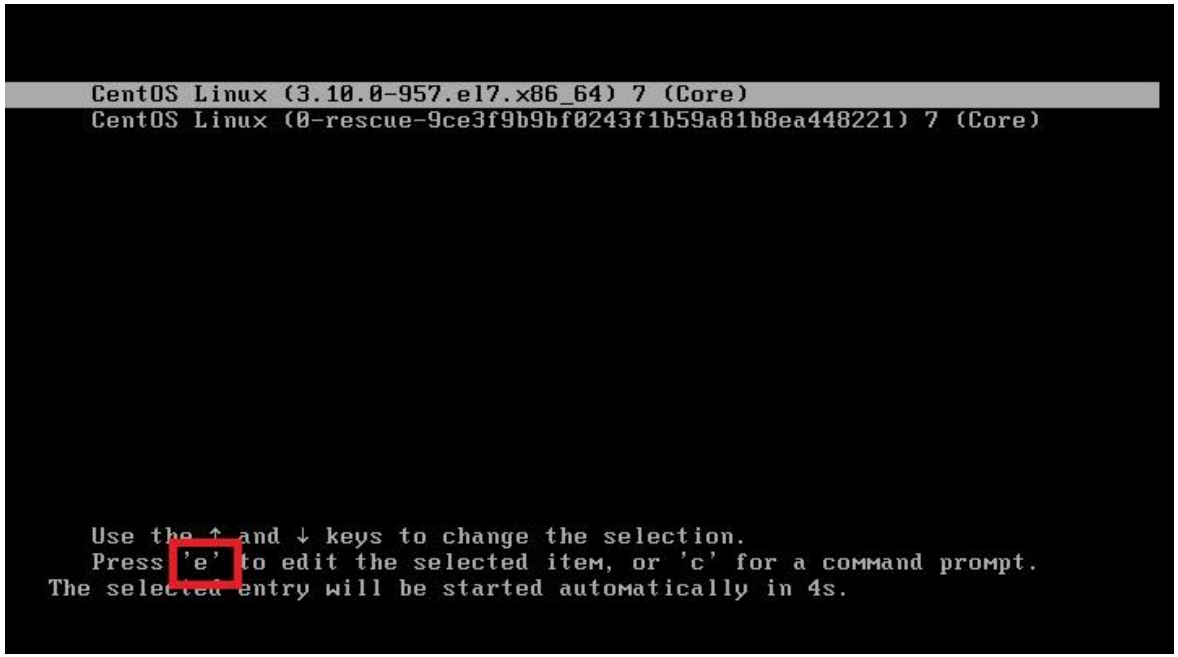
- 只允許金鑰登入：
  - # vi /etc/ssh/sshd_config
    PasswordAuthentication no
    PubkeyAuthentication yes
  - # systemtl restart sshd
- 使用 DOS 指令連線：
  - C:\> putty.exe -l root -i "private.ppk" -t "163.20.174.xxx"
- 使用 DOS 連線執行 CentOS 指令：
  - C:\> putty.exe -l root -i "private.ppk" -t "163.20.174.xxx" -m "command.txt"

SSH 管理

- 限制同一 IP 單位時間內之連線數
  - IPv4部份
    - # firewall-cmd --permanent --direct --add-rule ipv4 filter INPUT_direct 0 -p tcp --dport 22 -m state --state NEW -m recent --set
    - # firewall-cmd --permanent --direct --add-rule ipv4 filter INPUT_direct 1 -p tcp --dport 22 -m state --state NEW -m recent --update --seconds 300 --hitcount 6 -j DROP
    - # firewall-cmd --reload
    - # iptables -L INPUT_direct -n (查看規則)
  - IPv6部份
    - # firewall-cmd --permanent --direct --add-rule ipv6 filter INPUT_direct 0 -p tcp --dport 22 -m state --state NEW -m recent --set
    - # firewall-cmd --permanent --direct --add-rule ipv6 filter INPUT_direct 1 -p tcp --dport 22 -m state --state NEW -m recent --update --seconds 300 --hitcount 6 -j DROP
    - # firewall-cmd --reload
    - # ip6tables -L INPUT_direct -n (查看規則)
  - 移除規則：將上列指令 --add-rule 改成 --remove-rule 即可移除

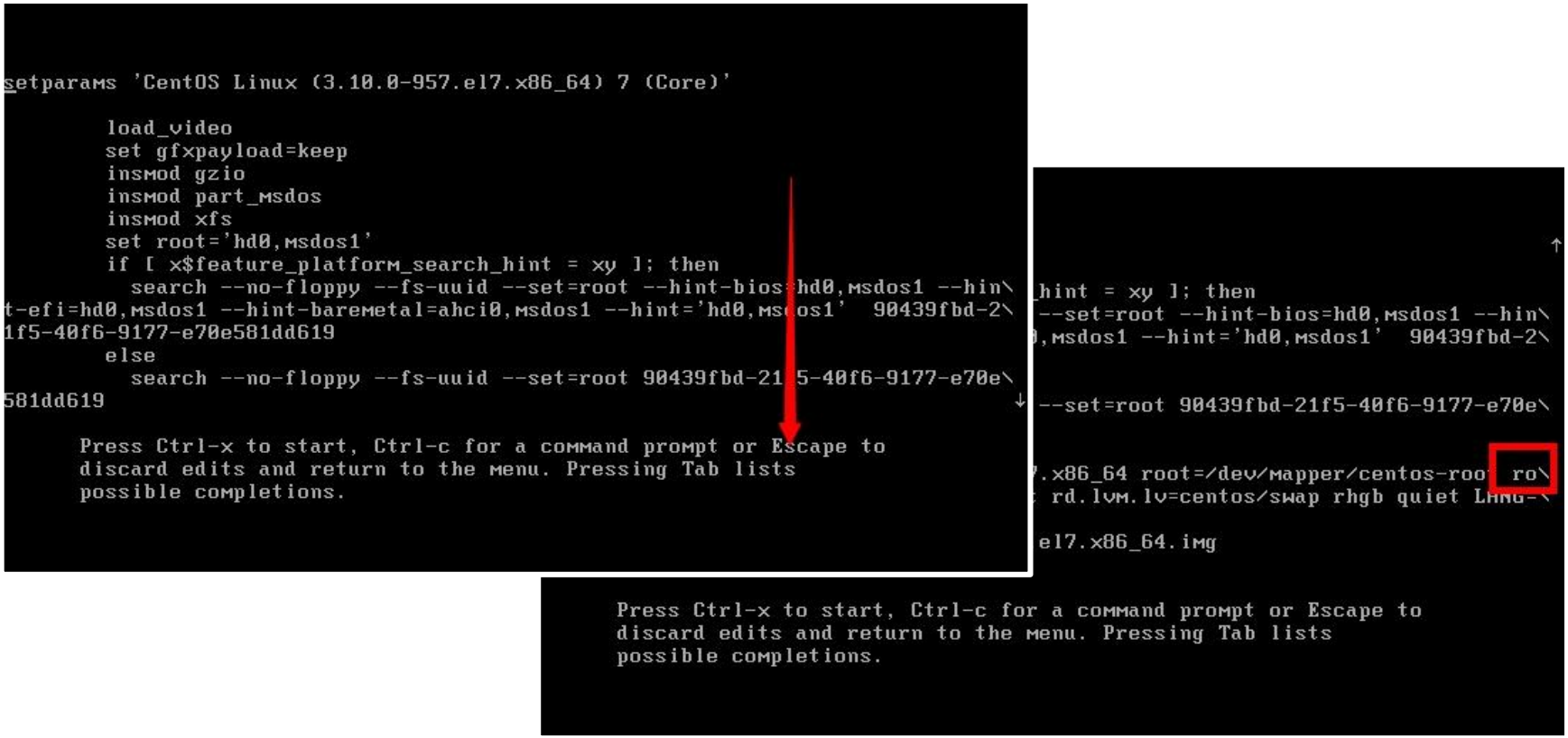
忘記 root 密碼

- 先將 root 改成任意密碼，並確認原先設定之 'Centos12#' 無法登入，然後重新開機
- 在開機選單中點 e 進入編輯模式



忘記 root 密碼

- 找到開機指令行將 ro 改成 rw rd.break
- 輸入 Ctrl + x 執行改過的指令行



忘記 root 密碼

- # chroot /sysroot
  (將 / 改到 /sysroot 目錄)
- # passwd root
  (變更 root 密碼)
- # touch /.autorelabel
  (重要，要重新標籤 SELinux，不然無法開機成功)
- # exit
  (退出 chroot 模式)
- # ./shutdown -r
  (重新開機)

DNS Server 管理

- CentOS 7 提供的 DNS伺服器套件為 Berkeley Internet Name Domain，簡稱BIND
- 安裝 bind 套件

  #yum -y install bind
- 套件名稱為 bind，但服務名稱是 named
- 設定檔位置：
  - /etc/named.conf
- 相關資料檔位置：
  - /var/named/*

DNS Server 管理

- 編輯設定檔：
  - # vi /etc/named.conf

```
listen-on port 53 { any; };
listen-on-v6 port 53 { any; };
allow-query { any; };
recursion no;
```

- 建立解析網域 ZONE (oooo.expr.ntpc.edu.tw.)：
  - # vi /etc/named.conf

```
zone "oooo.expr.ntpc.edu.tw." IN {
        type master;
        file "named.oooo";
};
```

DNS Server 管理

- 建立網域名稱紀錄檔：
  - # cd /var/named
  - # cp named.empty named.oooo
  - # vi named.oooo

```
@           NS      centosXXX.oooo.expr.ntpc.edu.tw.
centosXXX   A       163.20.174.xxx
centosXXX   AAAA    2001:288:228f:5::xxx
www         A       163.20.174.xxx
www         AAAA    2001:288:228f:5::xxx
```

- 啟動 named 服務(錯誤示範)：
  - # systemctl start named

DNS Server 管理

- 測試 DNS 紀錄查詢：
  - # nslookup www.oooo.expr.ntpc.edu.tw 127.0.0.1
  - # nslookup www.oooo.expr.ntpc.edu.tw ::1
- 檢查 named 狀態：
  - # systemctl status named
- 修改網域名稱紀錄檔權限(正確步驟)：
  - # chgrp named named.oooo
- 重新載入 named 服務，並確認狀態：
  - # systemctl reload named
  - # systemctl status named
- 設定開機時啟動：
  - # systemctl enable named

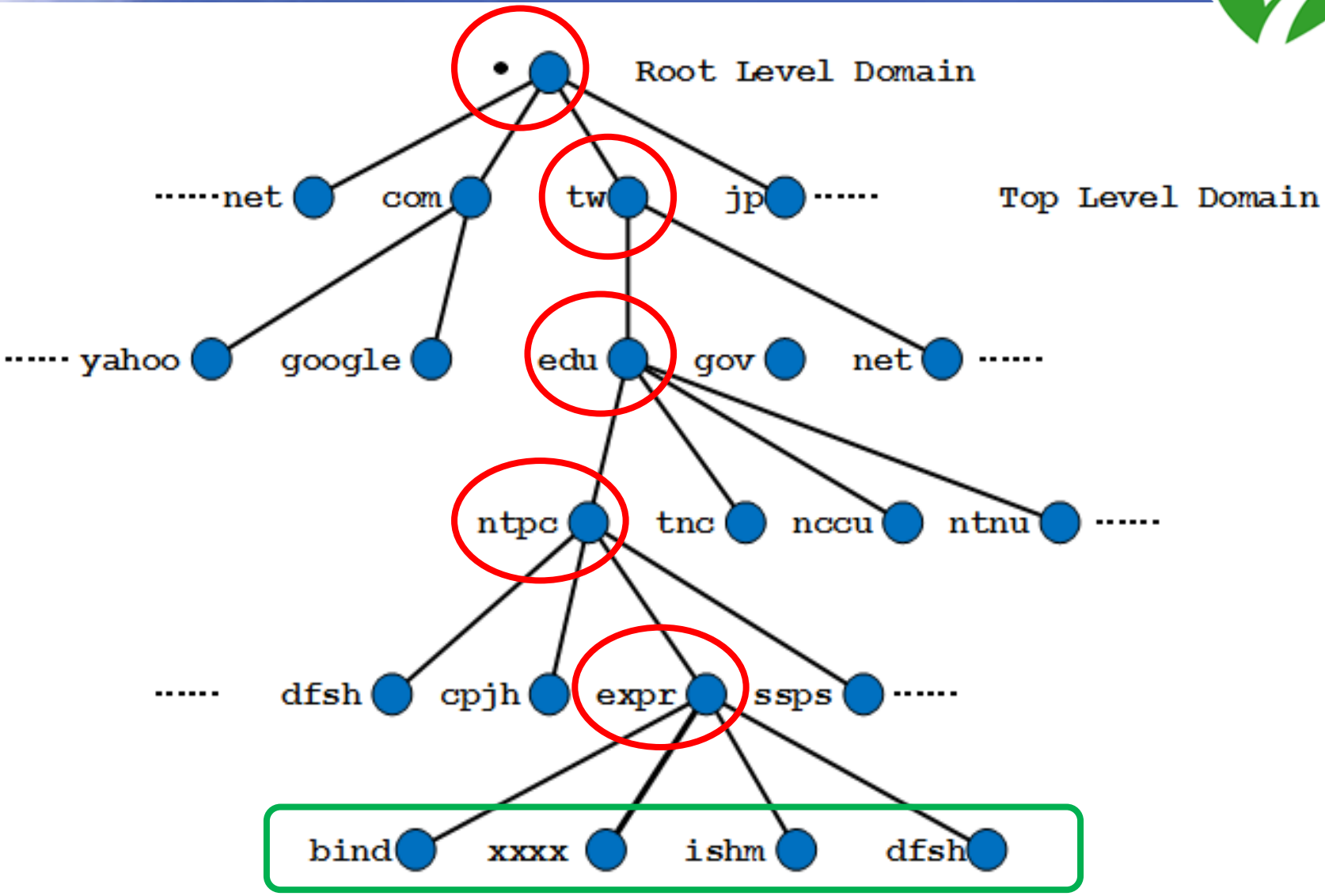
DNS Server 管理

- 測試 DNS 紀錄查詢：
  - # nslookup www.oooo.expr.ntpc.edu.tw 127.0.0.1
  - # nslookup www.oooo.expr.ntpc.edu.tw ::1
- 外部測試 DNS 查詢：
  - C:\> nslookup www.oooo.expr.ntpc.edu.tw 163.20.174.XXX
  - C:\> nslookup www.oooo.expr.ntpc.edu.tw 2001:288:228f:5::XXX
- 開通防火牆：
  - # firewall-cmd --add-service=dns --permanent
  - # firewall-cmd --reload
- 再次外部測試 DNS 查詢：
  - C:\> nslookup www.oooo.expr.ntpc.edu.tw 163.20.174.XXX
  - C:\> nslookup www.oooo.expr.ntpc.edu.tw 2001:288:228f:5::XXX

DNS Server 管理

- 測試 DNS 紀錄查詢：
  - # host www.oooo.expr.ntpc.edu.tw
  - # host www.oooo.expr.ntpc.edu.tw 8.8.8.8
- 外部測試 DNS 查詢：
  - C:\> nslookup www.oooo.expr.ntpc.edu.tw
  - C:\> nslookup www.oooo.expr.ntpc.edu.tw 8.8.8.8
- 向上註冊(表單僅提供本研習使用)
  - https://forms.gle/AzAraUrQyN9Cgsm3A
- 申請教網防火牆開通
- 測試 DNS 紀錄查詢：
  - # host www.oooo.expr.ntpc.edu.tw
  - # host www.oooo.expr.ntpc.edu.tw 8.8.8.8
- 外部測試 DNS 查詢：
  - C:\> nslookup www.oooo.expr.ntpc.edu.tw
  - C:\> nslookup www.oooo.expr.ntpc.edu.tw 8.8.8.8

DNS Server 管理



DNS Server 管理

- 調整 named log 位置：
  - # vi /etc/named.conf

```
logging {
        channel default_debug {
                file "/var/log/named/named.run";
                severity dynamic;
        };
};
```

  - # mkdir /var/log/named
  - # chgrp named /var/log/named
  - # chmod g+w /var/log/named
  - # systemctl restart named
  - # cat /var/log/named/named.run

DNS Server 管理

- 新增 named 查詢 log：
  - # vi /etc/named.conf

```
logging {
        channel default_debug { ..... };
        channel "query_log" {
                file "/var/log/named/query.log" versions 3 size 50M;
                print-time yes;
                print-category yes;
                print-severity yes;
        };
        category "queries" { "query_log"; };
};
```

  - # systemctl restart named
  - # tail -f /var/log/named/query.log
  - # ls -l /var/log/named

紀錄管理

- 產生 LOG 的服務：

  systemd-journald : 收集來自 kernel、早期開機程序、標準輸出、及系統日誌，結構化處理後轉送給 rsyslog 做後續處理，並儲存在 /run/log 中(記憶體)，重新開機後消失。

  rsyslog : 依接收到系統日誌的型別及優先權排序，並寫入到 /var/log 內相對應的紀錄檔中保存。
- 檢視 systemd-journal 服務狀態：
  - # systemctl status systemd-journald
- 檢視 rsyslog 服務狀態：
  - # systemctl status rsyslog
- 檢視記錄檔：
  - # more /var/log/messages
  - # less /var/log/secure

紀錄管理

- 檢視/編輯 rsyslog 設定檔：
  - # vi /etc/rsyslog.conf
  - # ls -l /etc/rsyslog.d/
- 查詢 systemd-journald 系統紀錄
  - # journalctl (查看全部紀錄)
  - # journalctl -f (監看系統紀錄即時變化)
  - # journalctl -p err (檢視等級為 err 的紀錄)
  - # journalctl _SYSTEMD_UNIT=sshd.service
  - # journalctl | grep sshd (檢視 sshd 相關紀錄)

紀錄管理

- 檢視系統時間及時區：
  - # timedatectl
- 設定時區為臺北：
  - # timedatectl set-timezone Asia/Taipei
- 系統校時：
  - # chronyc sources -v (查看同步時間伺服器狀態)
  - # chronyc sourcestats (校時來源 Server 的狀態)
  - # chronyc tracking (顯示與校時來源的時差)
  - # chronyc -a makestep (立即同步)
- 硬體校時：
  - # hwclock -r (顯示硬體時間)
  - # hwclock -c (比較硬體與系統時間)
  - # hwclock -w (設定硬體時間比照系統時間同步)

紀錄管理

- 列出執行過的歷史指令：
  - # history
- 歷史指令位置：
  - # cat /root/.bash_history
- 刪除目前登入階段歷史指令：
  - # history -c
- 將所有使用者指令送到 rsyslog：
  - # vi /etc/bashrc

```
remoteip=$(who am i | awk '{print $5}' | sed "s/[()]//g" )
export PROMPT_COMMAND='RETRN_VAL=$?;logger -p local3.debug
"$(whoami)  $remoteip  [$$]: $(history 1 | sed "s/^[ ]*[0-9]\+[ ]*//" )
[$RETRN_VAL]"'
```

  - # vi /etc/rsyslog.conf

```
local3.*                        /var/log/bash.log
```

  - # systemctl restart rsyslog
  - # bash (或 重新登入)

紀錄管理

- bash.log 檢視一般使用者與 root 指令紀錄
- 檢視/編輯 logrotate 紀錄檔輪替：
  - # vi /etc/logrotate.conf
  - # ls -l /etc/logrotate.d/
  - # logrotate -f /etc/logrotate.conf (強制立即輪替)
- 將 bash.log 加入輪替：
  - # vi /etc/logrotate.d/bashlog

```
/var/log/bash.log {
        missingok
        notifempty
}
```

  - # logrotate -f /etc/logrotate.conf

網頁伺服器管理

- 查詢網頁伺服器服務狀態：
  - # systemctl status httpd
- 安裝網頁伺服器套件：
  - # yum -y install httpd mod_ssl
- 啟動網頁伺服器服務：
  - # systemctl status httpd
  - # systemctl start httpd
- 設定網頁伺服器開機時自動啟動：
  - # systemctl enable httpd

網頁伺服器管理

- 編輯網頁伺服器設定檔：
  - # vi /etc/httpd/conf/httpd.conf
    ServerName www.oooo.expr.ntpc.edu.tw
- 重新啟動網頁伺服器：
  - # systemctl restart httpd
  - # systemctl status httpd
- 開通防火牆允許 http 及 https (80, 443) ：
  - # firewall-cmd --add-service=http --add-service=https --permanent
  - # firewall-cmd --reload
  - # firewall-cmd --list-all
- 確定有監聽服務埠：
  - # netstat -ntlp

網頁伺服器管理

- 從外部測試連線：
  - C:\> ping 163.20.174.xxx
  - C:\> ping 2001:288:228f:5::xxx
- 從外部偵測 服務埠(80, 443)是否開通：
  - C:\> telnet 163.20.174.xxx 80
  - C:\> telnet 2001:288:228f:5::xxx 443
  - tcping 下載 (windows)：
    https://download.elifulkerson.com/files/tcping/0.39/tcping.exe
  - C:\> tcping 163.20.174.xxx
  - C:\> tcping 163.20.174.xxx 443
  - C:\> tcping 2001:288:228f:5::xxx
  - C:\> tcping 2001:288:228f:5::xxx 443
  - tcping 安裝 (CentOS 7)：
    - # yum -y install epel-release
    - # yum -y install tcping

網頁伺服器管理

- 製作首頁，然後用瀏覽器檢測：
  - # vi /var/www/html/index.html
- 安裝 PHP 套件：
  - # yum -y install php
  - # systemctl restart httpd
- 製作 PHP 首頁：
  - # vi /var/www/html/index.php

```
<?php
        echo "<h1>HELLO</h1><h1>PHP</h1>";
        echo "<hr />";
        phpinfo( );
?>
```

- 預設值，首頁以 html 為優先，php 次之

網頁伺服器管理

- 利用 PHP 環境變數製作動態網頁：
  - # vi /var/www/html/guest.php

```
<?php
        echo "<h1>I am ".$_SERVER['SERVER_NAME']."</h1>";
        echo "<h1>You come from : ".$_SERVER['REMOTE_ADDR']."</h1>";
?>
```

- 製作 favicon.ico：
  - 製作/取得圖檔
  - 線上轉檔並下載：
    http://tw.faviconico.org/
    https://www.favicon.cc/
  - Filezilla 使用 SFTP 上傳至 /var/www/html/
  - 大部份瀏覽器會自動取得 favicon.ico 並顯示，
    或

```
<head>
        <link rel=”shortcut icon” href=”favicon.ico” />
</head>
```

Let's Encrypt 憑證申請

- 安裝 epel-release 套件：
  - # yum -y install epel-release
- 取得 certbot 資訊：
  - # yum list | grep certbot
- 安裝 certbot 套件：
  - # yum -y install python2-certbot-apache
- 手動申請及安裝憑證：
  - # certbot certonly --webroot -d www.oooo.expr.ntpc.edu.tw
    (# certbot --staging certonly --webroot -d www.oooo.expr.ntpc.edu.tw)
    (--staging 為測試憑證CA)
  - # vim /etc/httpd/conf.d/ssl.conf (將憑證路徑寫入設定檔)
  - # systemctl restart httpd

Let's Encrypt 憑證申請

- 設定虛擬網站：
  - # vi /etc/httpd/conf/httpd.conf

```
ServerName www.oooo.expr.ntpc.edu.tw  (刪除或註解這一行)
<VirtualHost *:80>
   ServerAdmin root@oooo.expr.ntpc.edu.tw
   DocumentRoot /var/www/html
   ServerName www.oooo.expr.ntpc.edu.tw
</VirtualHost>
```

  - # systemctl restart httpd
- 自動申請及安裝憑證：
  - # certbot run

(過程中，建議選擇 2: Redirect 重導，自動將用戶的 http 連線轉址成 https 連線)

(# certbot --staging run 測試憑證CA)

Let's Encrypt 憑證申請

- 設定第2個虛擬網站：
  - # vi /etc/httpd/conf/httpd.conf

```
<VirtualHost *:80>
  ServerAdmin root@oooo.expr.ntpc.edu.tw
  DocumentRoot /var/www/html/xyz
  ServerName xyz.oooo.expr.ntpc.edu.tw
</VirtualHost>
```

  - # mkdir /var/www/html/xyz
  - # vi /var/www/html/xyz/index.php

```
<?php
    echo "<h1>";
    echo $_SERVER['SERVER_NAME'];
    echo "</h1>";
?>
```

  - # systemctl restart httpd

Let's Encrypt 憑證申請

- 設定第2個網站的 DNS 對應：
  - # vi /var/named/named.oooo

```
xyz     A       163.20.174.xxx
xyz     AAAA    2001:288:228f:5::xxx
```

  - # systemctl restart named
- 使用瀏覽器確定網站運作正常
- 自動申請及安裝第2張憑證：
  - # certbot run

Let's Encrypt 憑證申請

- 檢視 Let's Encrypt 憑證：
  - # cat /etc/httpd/conf/httpd-le-ssl.conf
  - # ls -l /etc/letsencrypt
  - # cd /etc/letsencrypt/archive/xyz.oooo.expr.ntpc.edu.tw
  - # openssl x509 -in cert1.pem -noout -text
  - # openssl rsa -in privkey1.pem -noout -text
- 更新 Let's Encrypt 憑證：
  - # certbot renew
- 利用 crond 自動更新 Let's Encrypt 憑證：
  - # vi /etc/crontab
    10 1 * * 6 root /usr/bin/certbot renew (每週六 1:10 更新一次)
  - # crontab -e
    10 1 * * 6 root /usr/bin/certbot renew (每週六 1:10 更新一次)
  - # systemctl reload crond

Bash Script 實作

- 實作自動搜尋與安裝金鑰至所有學員機 shell script
- 開放 SSHD 允許帳密登入：
  - # vi /etc/ssh/sshd_config
    PasswordAuthentication yes
  - # systemtl restart sshd
- 確定 root 密碼為 'Centos12#'：
  - # passwd root
    - 新密碼：Centos12#
    - 再次輸入新密碼：Centos12#
- 移除單位時間 IP 連線限制
  - # firewall-cmd --permanent --direct --remove-rule ipv4 filter INPUT_direct 0 -p tcp --dport 22 -m state --state NEW -m recent --set
  - # firewall-cmd --permanent --direct --remove-rule ipv4 filter INPUT_direct 1 -p tcp --dport 22 -m state --state NEW -m recent --update --seconds 300 --hitcount 6 -j DROP
  - # firewall-cmd --reload
  - # iptables -L INPUT_direct -n (查看規則)

Bash Script 實作

- 安裝 nmap 套件：
  - # yum -y install nmap
- 掃瞄開機 IP：
  - # nmap -sP 163.20.174.131-200
- 依掃瞄結果擷取虛擬機器主機資訊：
  - # nmap -sP 163.20.174.131-200 | grep "VMware" -B 2
- 保留含 IP 的行：
  - # nmap -sP 163.20.174.131-200 | grep "VMware" -B 2 | grep "163\.20\.174\."
- 單獨擷取 IP：
  - # nmap -sP 163.20.174.131-200 | grep "VMware" -B 2 | grep "163\.20\.174\." | awk '{print $5}'
- 將擷取 IP 的結果轉成檔案：
  - # nmap -sP 163.20.174.131-200 | grep "VMware" -B 2 | grep "163\.20\.174\." | awk '{print $5}' > ips.txt

Bash Script 實作

- 安裝免互動 SSH 登入工具：
  - # yum -y install sshpass
- 利用 sshpass 免互動取得對方主機名稱：
  - # sshpass -p 'Centos12#' ssh -o StrictHostKeychecking=no -o ConnectTimeout=5 root@163.20.174.YYY "hostname"
- 利用 sshpass 安裝金鑰：
  - # sshpass -p 'Centos12#' ssh-copy-id root@163.20.174.YYY
- 編輯安裝金鑰 Bash Script：
  - # vi key.sh

```
for IP in $(cat ips.txt)
do
        迴圈指令
done
```

  - # chmod a+x key.sh
- 執行 Bash Script：
  - # ./key.sh

備份管理

- 打包與壓縮：

```
          z                    gz
#tar cvjf filename.tar.bz2 source1 srouce2 .....
          J                    xz
```

  - 含前置目錄：
    - # tar cvzf html.tar.gz /var/www/html
  - 不含前置目錄：
    - # cd /var/www/html
    - # tar cvzf html.tar.gz *
- 解壓縮：

```
          z                    gz
#tar xvjf filename.tar.bz2
          t J                  xz
```

  - # tar xvzf html.tar.gz

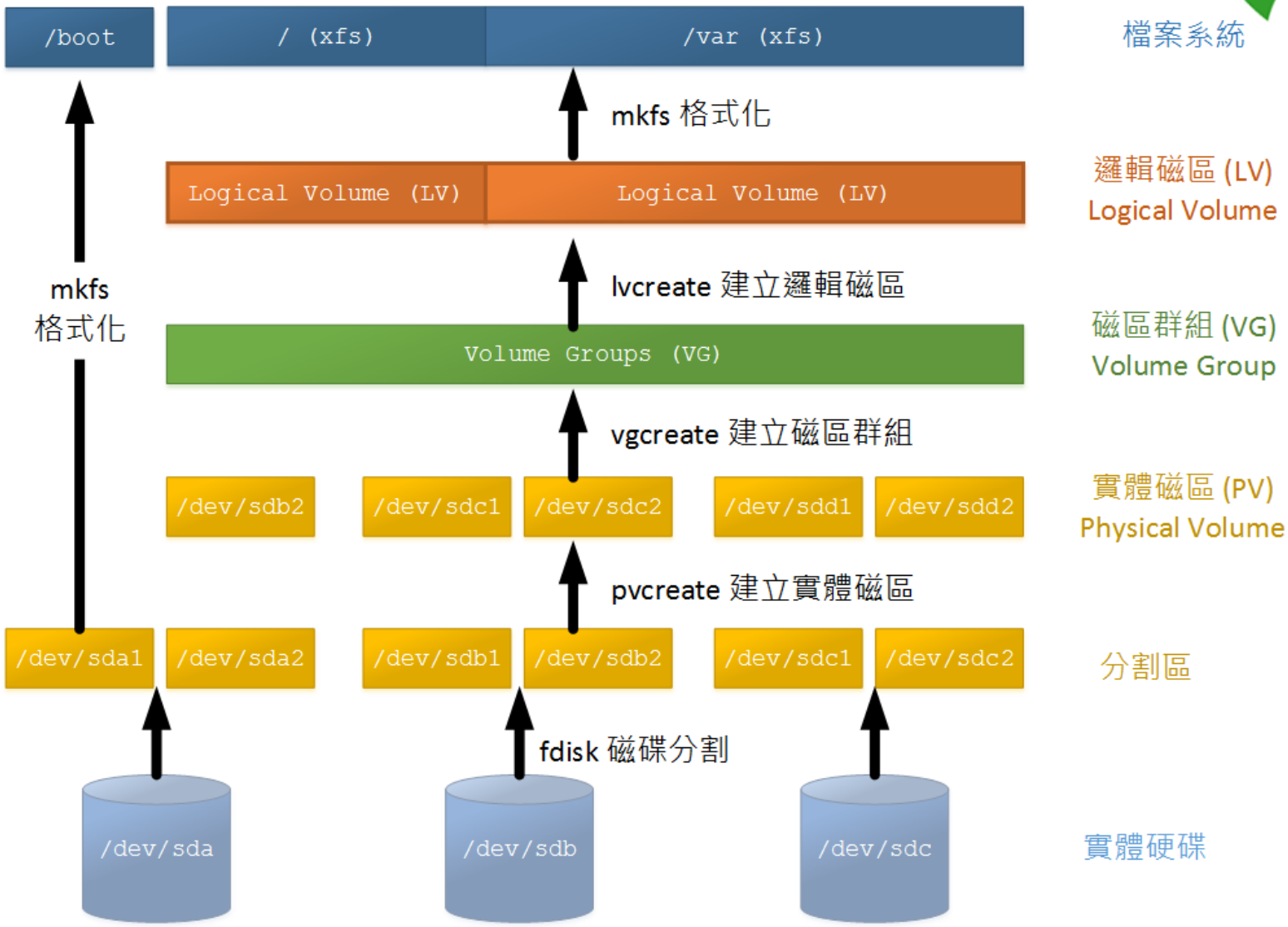
檔案傳輸與備份

- 透過 scp 將檔案傳到另一台主機備份：
  - # scp html.tar.gz root@163.20.174.YYY:/tmp
  - # ssh root@163.20.174.YYY "ls -l /tmp" (確認已上傳)
  - # scp root@163.20.174.YYY:/etc/httpd/conf/* /tmp
- 透過 SFTP 下載 html.tar.gz 備份檔：Filezilla
- 透過 rsync 備份：
  - # mkdir /tmp/backup1
  - # rsync -av /var/www/html /tmp/backup1
    (備份 /var/www/html 整個目錄及其內檔案與目錄)
  - # mkdir /tmp/backup2
  - # rsync -av /var/www/html/ /tmp/backup2
    (備份 /var/www/html/ 下的所有檔案與目錄)
  - # ssh root@163.20.174.YYY "mkdir /tmp/backup"
    (在遠端建立備份目錄)
  - # rsync -av /var/www/html root@163.20.174.YYY:/tmp/backup
  - # rsync -av /var/named root@163.20.174.YYY:/tmp/backup
  - # ssh root@163.20.174.YYY "ls -l /tmp/backup"

備份管理

- 匯出前先檢查硬碟使用狀況(擴充硬碟練習用)：
  - # df -h
  - # fdisk -l
- 匯出 OVA 檔
  - # poweroff (關機)
  - 至「Virtual Machine Settings」移除 CD/DVD 掛載
  - C:\> cd “C:\Program Files (x86)\VMware\VMware Player\OVFTool”
  - C:\> mkdir D:\export
  - C:\> ovftool.exe “C:\Users\user\Document\Virtual Machines\CentOS 7 64bit\CentOS 7 64-bit.vmx” D:\export\CentOS7.ova

擴充硬碟


/boot
/ (xfs)
/var (xfs)
檔案系統
mkfs 格式化
Logical Volume (LV)
Logical Volume (LV)
邏輯磁區 (LV)
Logical Volume
mkfs
格式化
lvcreate 建立邏輯磁區
Volume Groups (VG)
磁區群組 (VG)
Volume Group
vgcreate 建立磁區群組
/dev/sdb2
/dev/sdc1
/dev/sdc2
/dev/sdd1
/dev/sdd2
實體磁區 (PV)
Physical Volume
pvcreate 建立實體磁區
/dev/sda1
/dev/sda2
/dev/sdb1
/dev/sdb2
/dev/sdc1
/dev/sdc2
分割區
fdisk 磁碟分割
/dev/sda
/dev/sdb
/dev/sdc
實體硬碟

擴充硬碟

- 擴充硬碟：
  - 至「Virtual Machine Settings」中「Hard Disk (SCSI)」，點「Expand..」擴充硬碟，加大20GB
  - 完成後，開啟虛擬機器電源
- 開機登入後，確認硬碟容量增加：
  - # fdisk -l
- 建立新分割區：
  - # fdisk /dev/sda
    - n (新增分割區)
      - p (建立主分割區)
      - [Enter] (分割區編號，預設 3)
      - [Enter] (起始扇區，選擇預設)
      - [Enter] (起始扇區，選擇預設)
    - t (變更分割區格式)
      - 3 (選擇分割區)
      - 8e (選擇格式為LVM)
    - p (檢視已設定分割區)
    - w (儲存並退出)

擴充硬碟

- 重新啟動以套用變更：
  - # reboot
- 開機登入後，轉換分割區為實體磁區(PV)：
  - # pvcreat /dev/sda3
  - (可用 # pvdisplay 檢視已有實體磁區名稱及內容)
- 擴充磁區群組(VG)：
  - # vgextend centos /dev/sda3
    (可用 # vgdisplay 檢視已有磁區群組名稱及內容)
- 擴充邏輯磁區(LV)：
  - # lvextend /dev/centos/root /dev/sda3
  - (可用 # lvdisplay 檢視現有邏輯磁區名稱及內容)
- 擴大檔案系統(xfs)：
  - # xfs_growfs /dev/mapper/centos-root
- 檢查確認：
  - # df -h
- 實作：再擴充一顆 /dev/sdb

新北市首頁系統
操控原力進化
(CentOS)

謝謝指教

新北市政府教育局
教育研究及資訊發展科
林璟豐
80723456＃516