如何使用 BIND9 建立網域名稱伺服器 DNS server

安裝 Ubuntu server & 安裝 BIND9 & 指令實戰

摘要

目錄

[如何使用 BIND9 建立網域名稱伺服器 DNS server 1](#_Toc435004581)

[安裝 Ubuntu server & 安裝 BIND9 & 指令實戰 1](#_Toc435004582)

[摘要 1](#_Toc435004583)

[目錄 2](#_Toc435004584)

[第１章 安裝 Ubuntu server 4](#_Toc435004585)

[第１節 確認連上網路 4](#_Toc435004586)

[第２節 確認 /etc/hostname 4](#_Toc435004587)

[第３節 設定 /etc/hosts 4](#_Toc435004588)

[第１項 查看原設定 4](#_Toc435004589)

[第２項 修改 hosts 設定 5](#_Toc435004590)

[第４節 重新登入系統 reboot 5](#_Toc435004591)

[第５節 再次確認設定已啟用Re-check 6](#_Toc435004592)

[第２章 安裝 BIND9 7](#_Toc435004593)

[第１節 修改 named.conf.options 7](#_Toc435004594)

[第２節 修改 named.conf.local 10](#_Toc435004595)

[第１項 什麼是named.conf.local ? 10](#_Toc435004596)

[第２項 在路徑 /etc/bind/zones/ 下製作兩個檔案 db.kevinisncuccpa & db.140 11](#_Toc435004597)

[第３項 使用 named-checkzone確認網域定義檔案正常運作 15](#_Toc435004598)

[第３節 修改 /etc/resolv.conf (未確定部分) 16](#_Toc435004599)

[~~第４節 修改 named.default-zones~~ 18](#_Toc435004600)

[第５節 重新啟動 BIND9 服務 & 查看紀錄 19](#_Toc435004601)

[第１項 重新啟動 BIND9 服務 19](#_Toc435004602)

[第２項 查看 BIND9紀錄 20](#_Toc435004603)

[第３章 REF. 如何使用 BIND9 建立 DNS 20](#_Toc435004604)

[第４章 附錄. 使用 adduser 新增使用者 22](#_Toc435004605)

[第５章 修正 DNS 25](#_Toc435004606)

# 安裝 Ubuntu server

(這裡使用 12.04 LTS，強烈建議安裝 LTS 版本)

## 確認連上網路

/etc/nework/interface 必須設定 static

重新啟動網路 daemon

# /etc/init.d/networking restart

## 確認 /etc/hostname

→ dns

## 設定 /etc/hosts

### 查看原設定

# cat /etc/hosts

127.0.0.1 localhost

127.0.1.1 dns

# The following lines are desirable for IPv6 capable hosts

::1 ip6-localhost ip6-loopback

fe00::0 ip6-localnet

ff00::0 ip6-mcastprefix

ff02::1 ip6-allnodes

ff02::2 ip6-allrouters

### 修改 hosts 設定

將第二個 127.0.0.1 修改成 DNS 所在的 IP 位置 140.115.2.153

格式： IP 位置 「主機名稱.網域名稱」 alias(代稱)

→ 140.115.2.153 dns.kevinisncuccpa dns

# vim /etc/hosts



=>

127.0.0.1 localhost

#127.0.1.1 dns #註解掉

140.115.2.153 dns.kevinisncuccpa dns

# The following lines are desirable for IPv6 capable hosts

::1 ip6-localhost ip6-loopback

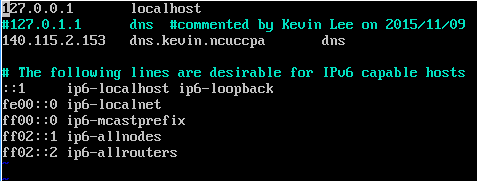
fe00::0 ip6-localnet

ff00::0 ip6-mcastprefix

ff02::1 ip6-allnodes

ff02::2 ip6-allrouters

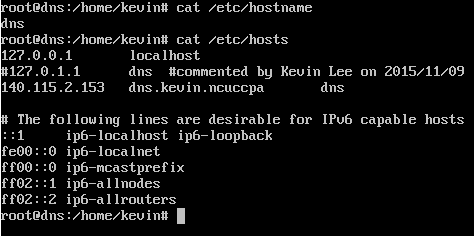
**修改結果↓**



## 重新登入系統 reboot



## 再次確認設定已啟用Re-check



# 安裝 BIND9

按照需求依序修改以下檔案

named.conf.options

named.conf.local

named.conf.resolv.conf

## 修改 named.conf.options

這個檔案將告訴我們自建的 DNS 如何指向(forward)上層由 ISP 架設的 DNS；當然，也可以指向 open DNS 例如 Google 提供的 8.8.8.8 或 8.8.8.4

我們需要的檔案格式應該要類似以下

forwards {

// give here your own ISP DNS IP’s and separate each IPs with the semicolon “;”

140.115.2.254; # gateway or router

140.115.1.31; # the outside DNS’s IP your machine desire

};

我們先來檢視該檔案原生樣貌

// vim –R 唯讀模式

# vim –R /etc/bind/named.conf.options



我們得到了原始碼~ 來閱讀並上個註解吧!

options {

directory "/var/cache/bind";

// If there is a firewall between you and nameservers you want

// to talk to, you may need to fix the firewall to allow multiple

// ports to talk. See http://www.kb.cert.org/vuls/id/800113

// If your ISP provided one or more IP addresses for stable

// nameservers, you probably want to use them as forwarders.

// Uncomment the following block, and insert the addresses replacing

// the all-0's placeholder.

// forwarders {

// 0.0.0.0;

// };

//======================================================================

==

// If BIND logs error messages about the root key being expired,

// you will need to update your keys. See https://www.isc.org/bind-keys

//======================================================================

==

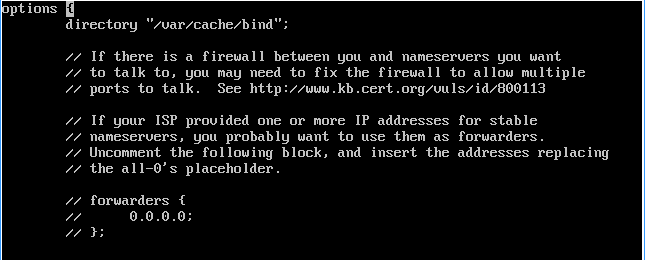
dnssec-validation auto;

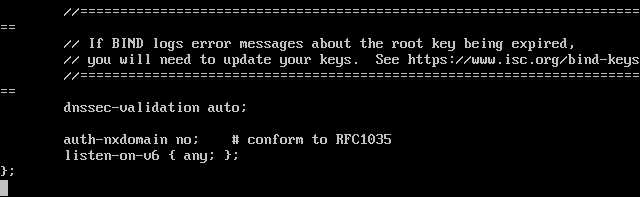
auth-nxdomain no; # conform to RFC1035

listen-on-v6 { any; };

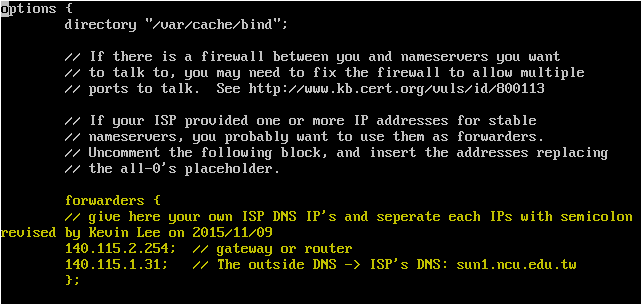
};

原生





修改後



## 修改 named.conf.local

### 什麼是named.conf.local ?

這個檔案將告訴我們自建的 DNS ，正解與反解的 DNS 定義在哪個檔案中

我們需要的檔案格式應該要類似以下

# Our forward zone

zone "kevinisncuccpa" {

type master;

file "/etc/bind/zones/db.kevinisncuccpa ";

};

# Our reverse Zone

# Server IP 140.115.2.153

zone "2.115.140.in-addr.arpa" {

type master;

file "/etc/bind/zones/db.140";

};

我們來檢視原生的檔案

# vim -R /etc/bind/named.conf.local

//

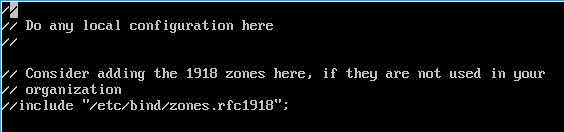
// Do any local configuration here

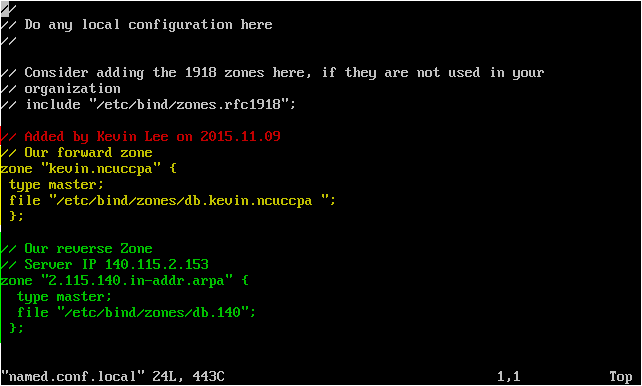
//

// Consider adding the 1918 zones here, if they are not used in your

// organization

//include "/etc/bind/zones.rfc1918";

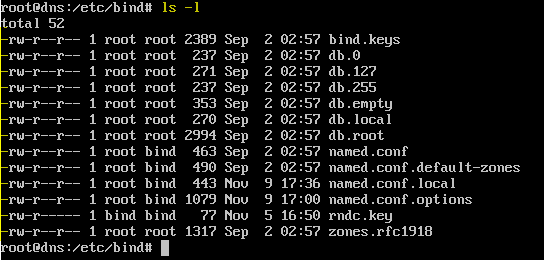


經過修改後

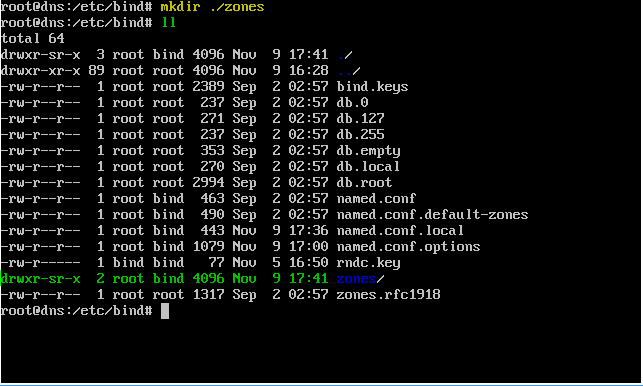
### 在路徑 /etc/bind/zones/ 下製作兩個檔案 db.kevinisncuccpa & db.140

#### 製作 /etc/bind/zones

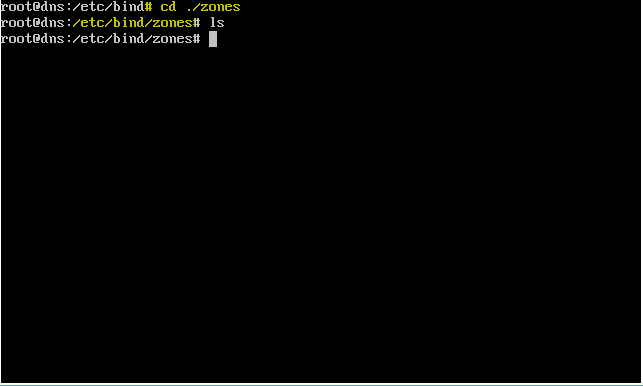
原本沒有 zones 這個路徑(資料夾)，全都是唯讀的檔案↓



# mkdir /etc/bind/zones



# cd /etc/bind/zones



#### 我的機器 IP

xenhome.kevinisncuccpa.ncu.edu.tw 140.115.2.151

kevinisncuccpa.ncu.edu.tw 140.115.2.152

dns.kevinisncuccpa.ncu.edu.tw 140.115.2.153

#### 製作 /etc/bind/zones/db.kevinisncuccpa

我應該要將下面的內容填入 /etc/bind/zones/db.kevinisncuccpa

;

; BIND data file for local loopback interface

;

$TTL 604800

@ IN SOA dns.kevinisncuccpa. www.kevinisncuccpa. (

2 ; Serial

604800 ; Refresh

86400 ; Retry

2419200 ; Expire

604800 ) ; Negative Cache TTL

;

kevinisncuccpa. IN NS dns.kevinisncuccpa.

kevinisncuccpa. IN A 140.115.2.153

;@ IN A 127.0.0.1

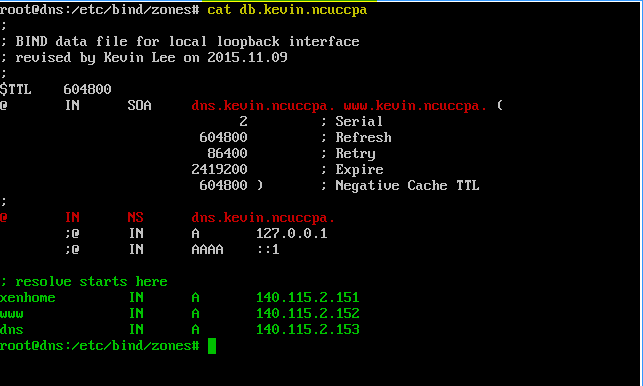
;@ IN AAAA ::1

xenhome IN A 140.115.2.151

www IN A 140.115.2.152

dns IN A 140.115.2.153

# cp /etc/bind/db.local /etc/bind/zones/db.kevinisncuccpa

# vim /etc/bind/zones/db.kevinisncuccpa

#### 製作 /etc/bind/zones/db.140

我應該要將下面的內容填入 /etc/bind/zones/db.140

;

; BIND reverse data file for local loopback interface

;

$TTL 604800

@ IN SOA dns.kevinisncuccpa. www.kevinisncuccpa. (

2 ; Serial

604800 ; Refresh

86400 ; Retry

2419200 ; Expire

604800 ) ; Negative Cache TTL

;

IN NS dns.

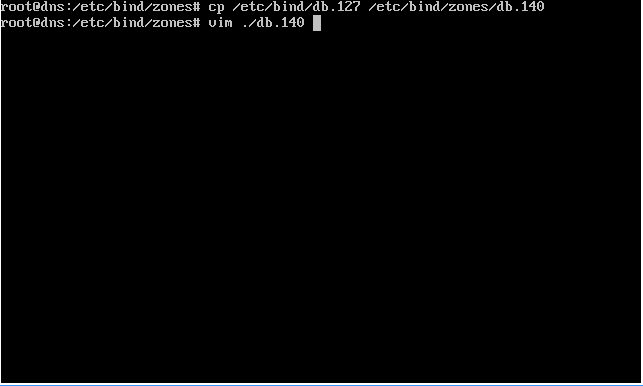
151.2.115.140 IN PTR xenhome.kevinisncuccpa.

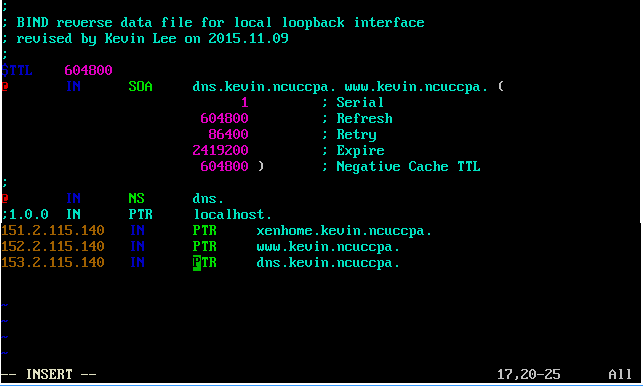
152.2.115.140 IN PTR www.kevinisncuccpa.

153.2.115.140 IN PTR dns.kevinisncuccpa.

# cp /etc/bind/db.127 /etc/bind/zones/db.140

# vim /etc/bind/zones/db.140

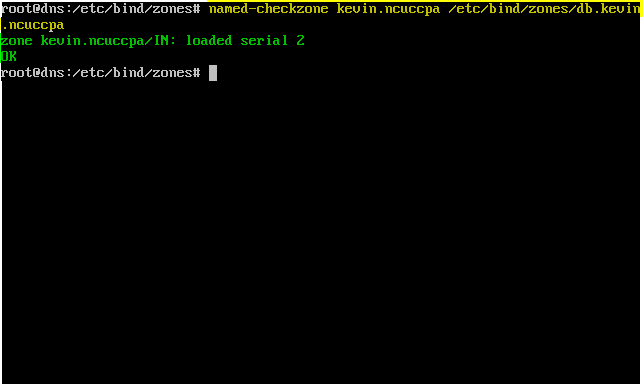




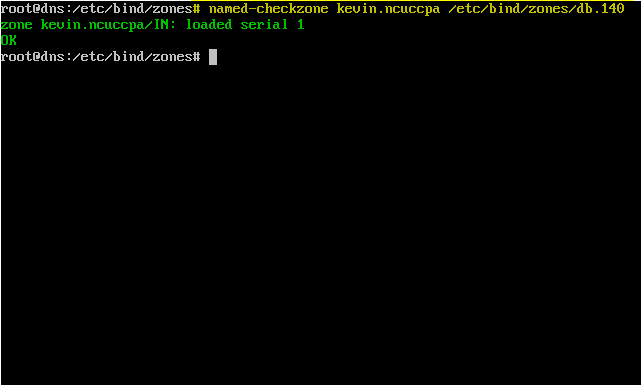
### 使用 named-checkzone確認網域定義檔案正常運作

指令格式 named-checkzone [網域名稱] [目標 zone 檔案]

# named-checkzone kevinisncuccpa /etc/bind/zones/db.kevinisncuccpa



# named-checkzone kevinisncuccpa /etc/bind/zones/db.140



## 修改 /etc/resolv.conf (未確定部分)

這是在 /etc/ 系統設定裡的

sudo nano /etc/resolv.conf

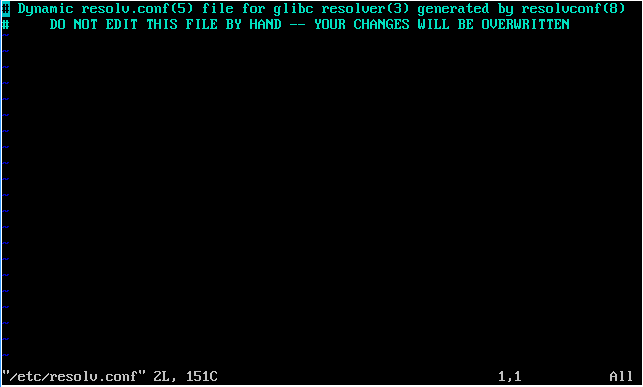
Nameserver 140.115.2.153

domain kevinisncuccpa

search kevinisncuccpa



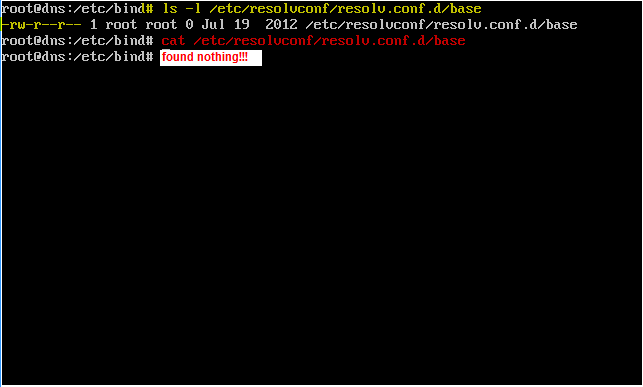
發現有以下狀況



根據下文Ref

<http://askubuntu.com/questions/157154/how-do-i-include-lines-in-resolv-conf-that-wont-get-lost-on-reboot>

作了以下查詢，我們得去 resolve.conf 修改產生器，產生器路徑應該在 /etc/resolveconf/resolve.conf.d/base ，目前該檔案為空



同個參考資源的其他說法是，當 網路介面卡 /etc/network/interface 已經設定static IP ，可以不用特地更動產生器… = =?

那我們就先完成下節，再試著重新啟動 bind9 daemon 試試看會不會 work 好了…

## ~~修改 named.default-zones~~

修改 named.conf.local 檔案即可

/etc/bind/named.default-zones 的原始碼

// broadcast zones as per RFC 1912

zone "localhost" {

type master;

file "/etc/bind/db.local";

};

zone "127.in-addr.arpa" {

type master;

file "/etc/bind/db.127";

};

zone "0.in-addr.arpa" {

type master;

file "/etc/bind/db.0";

};

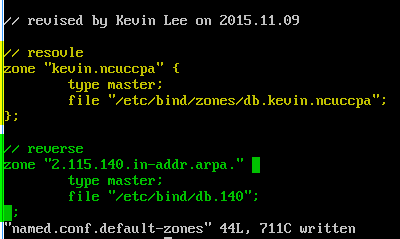
zone "255.in-addr.arpa" {

type master;

file "/etc/bind/db.255";

};

新增

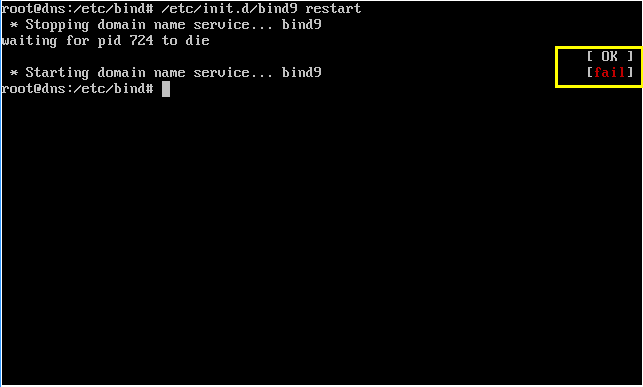


## 重新啟動 BIND9 服務 & 查看紀錄

### 重新啟動 BIND9 服務

/etc/init.d/bind9 restart

甘…因為 default-zones & .local 的衝突，所以 fail



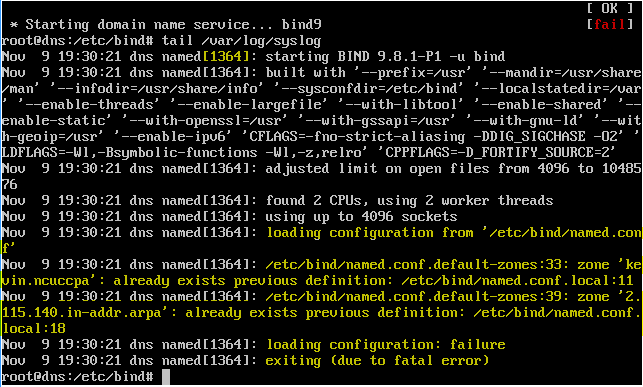
只好回去修改產生器了嗎?(菸~)

/etc/resolveconf/resolve.conf.d/base

不對! 要先看錯誤紀錄!!!

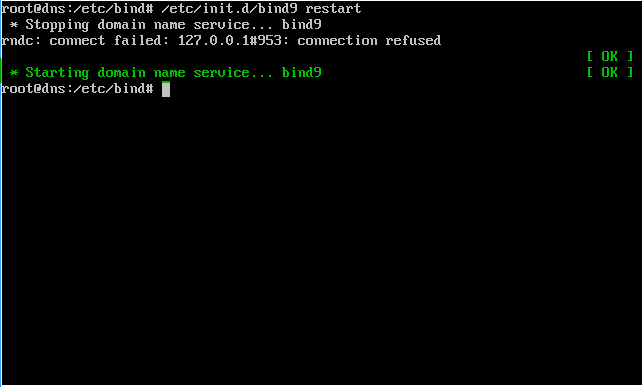
# tail /var/log/syslog

Process id [1364]



所以是『重複定義的錯誤』，named.default-zones 最好不要更動，修改 named.conf.local 就好了，再次重新啟動 BIND9 服務

Work 就是感覺愉快~~

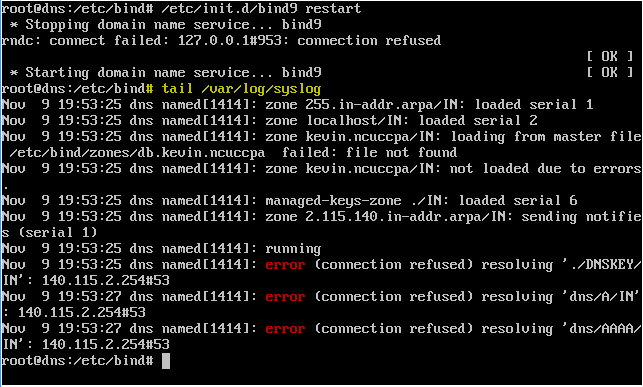


### 查看 BIND9紀錄

因為最後啟動的 daemon 是 BIND9 所以可以直接 tail syslog

tail -f /var/log/syslog

再次查看 log，甘… 有 error…



根據下面的鏈結，這個 eroor 來自我的 DNS 尚未與上層DNS (sun1.ncu.edu.tw)登記，看來只能暫時告一段落了

<https://discussions.apple.com/thread/2096965>

# 附錄. 如何使用 BIND9 建立 DNS

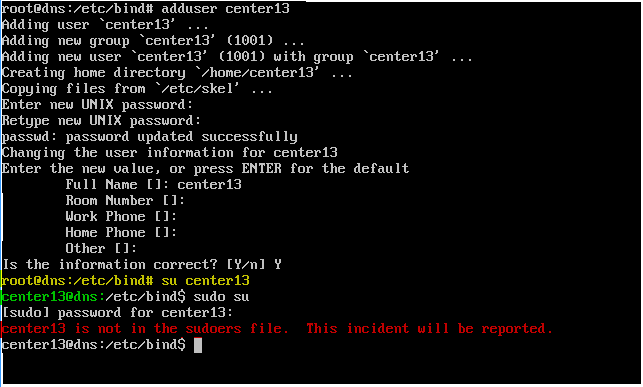
<http://askubuntu.com/questions/330148/how-do-i-do-a-complete-bind9-dns-server-configuration-with-a-hostname>

# 附錄. 使用 adduser 新增使用者

目標: 新增 center13 供王文秀夥伴登入 140.115.2.153 使用

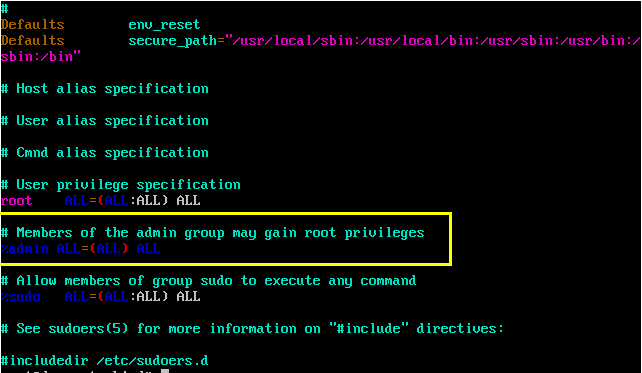
測試1. 利用 piety 實作遠端 SSH log in -> work!

測試2. 使用 adduser 新增 center13



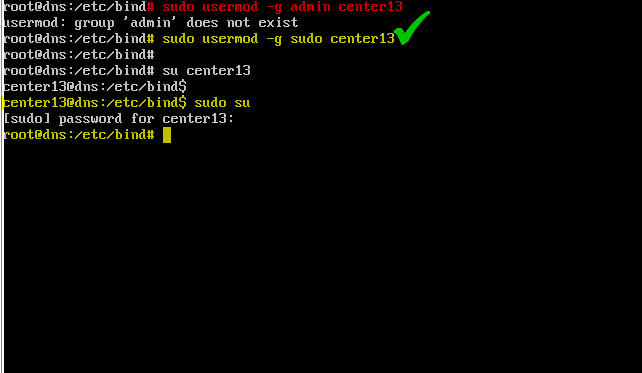
測試3. 嘗試修改 /etc/sudoers file

# vim /etc/sudoers // 覺得修改使用者群組更好



測試4. 嘗試修改 center 13 的群組到 admin

# sudo usermod –g sudo [username]



REF.

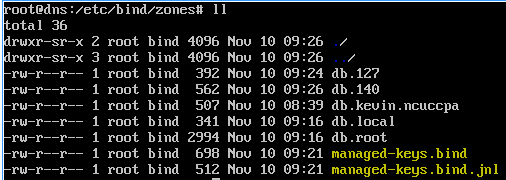
<https://help.ubuntu.com/community/AddUsersHowto#Command-line>

2015/11/10 09:30之後

# 附錄. 修正 DNS

感謝王文秀夥伴協助，目前 DNS 已經正常運作 ☺

# ls –l /etc/bind/zones



managed-keys.bind 與 managed-keys.bind.jnl 兩份檔案原始檔的路徑在 /var/cache/bind/ 之下，這兩份檔案必須放在 /etc/bind/named.conf.options 這份設定檔內開頭的路徑 directory 的定義位址

檔案碼類似以下

options{

directory “[absolute directory]”;

**// file description…**

**// more file description…**

dnssec-validation auto;

auth-nxdomaim no; #conform to RFCxxxx, example: RFC1035

listen-on-v6 { any; };

};