第九單元

DNS 伺服器管理

1.實驗目的

架設 DNS 伺服器並有能力提供正反名稱解析及相關資訊的能力

2.實驗設備

- 安裝 Linux 系統之電腦
- Webmin(http://www.webmin.com)
- BIND (http://www.isc.org/products/BIND)

3.背景資料

DNS 屬於階層式的（Hierarchical）分散式資庫架構，雖然每部 DNS 伺服器只負責某範圍的名稱解析，但分散在全世界的 DNS 伺服器可以協同工作，成為一個邏輯上的大型資料庫，因為世界上的主機資料紀錄實在太多，所以必需透過 DNS 伺服器間的相互查詢以及共享快取的資料，才可以提供服務給來自各地的用戶。

DNS 目前已經是 Internet 上公開的標準，它包含了以下的組成元件：

- DNS 網域名稱區：指定不同類型組織的網域名稱階層結構。
- 資源記錄：將 DNS 網域名稱對應到指定類型的資源資訊，供名稱區中登錄或解析用。
- DNS 伺服器：儲存並回應資源記錄的名稱查詢。
- DNS 用戶端：也就是解讀器（Resolver），可查詢伺服器尋找名稱，並將名稱解析為查詢中所指定的資源記錄。

為了確保主機網域名稱的架構與唯一性，Internet 資訊中心（InterNIC）將網域分為多種類型，這些網址都稱為『根網域』（ROOT），大致上分為七種：

- edu：教育及學術單位
- ・mil：軍事單位
- gov：政府機構
- ・com：商業機構
- org：法人機構
- ・net：網路機構
- 國家代號：如 tw 為臺灣

目前網路上會有愈來愈多新制定的網域，詳請見 http://www.internic.org。

DNS 名詞解釋

- **網域（Domain）：**Root 網域中的每個類型都稱為網域，而網域中也可以包含其他的子網域，比如說 tslg.idv.tw 是指 idv.tw 網域中的一個子網域。
- **授權：**在每個網域中都負責名稱解析的 DNS 伺服器，若因為實際的需求，可以再將原本的網域細分成許多子網域，這個時候上層的網域就可以指派某一部的 DNS 去負責特定子網域的名稱解析工作，這個就稱為授權。
- **正解（Forwarding）：**將主機的 FQDN（fully-qualified domain name）解析為 IP 的過程。
- **反解（Reversing）：**反解和正解相反，是由指定的 IP 位址解析出主機的 FQDN。
- **Primary(Master)DNS：**主要名稱伺服器由它所在的主機上的檔案中取得管理區段的資料。如果學校擁有自己的網域（Domain），則必須建立自己的 DNS 系統，來回答網路上對學校中，所有與網際網路有關的電腦名稱與 IP 地址的轉換服務。
- **Secondary(Slave)DNS：**次要名稱伺服器是由其他管理這個區段的名稱伺服器中取得區段的資料。為了網路穩定度的考慮，通常需要一部次要名稱伺服器，以備不時之需。
- **Cache-only 伺服器：**每個 DNS 都會將查詢過的 Domain Name 給 cache 起來，所以每個 DNS 都快取名稱伺服器的功能。硬碟中沒有該 Domain 的 database 檔案。
- **Resolver：**這是用在 DNS 系統中的用戶端，也就是向 DNS 伺服器提出名稱解析要求的電腦。

DNS 的安裝與啟動

首先先查詢一下系統上有無安裝 bind 的套件。

```
[root@net122 root]# rpm -qa|grep bind
redhat-config-bind-2.0.0-18
ypbind-1.12-3
bind-utils-9.2.2.P3-9
bind-9.2.2.P3-9
bind-chroot-9.2.2.P3-9
```

如果沒有的話，請至 http://www.rpmfind.org 或是利用 Fedora 的光碟片安裝：

rpm –Uvh bind-*.rpm

接下來要先啟動 DNS 伺服器：

[root@net122 root]# /etc/rc.d/init.d/named start

測試一下看有沒有啟動：

```
[root@net122 root]# ps -ax|grep named
2517 ?        S      0:00 /usr/sbin/named -u named -t /var/named/chroot  ←這行就代表啟動了
2526 pts/1    S      0:00 grep named
```

如果要在開機時啟動 dns 的話，在 Fedora Linux 上可以利用 ntsysv 這個指令來啟動。

確定後存檔，以後開機時 Linux 都會自動啟動 DNS 服務。

4.實驗方法

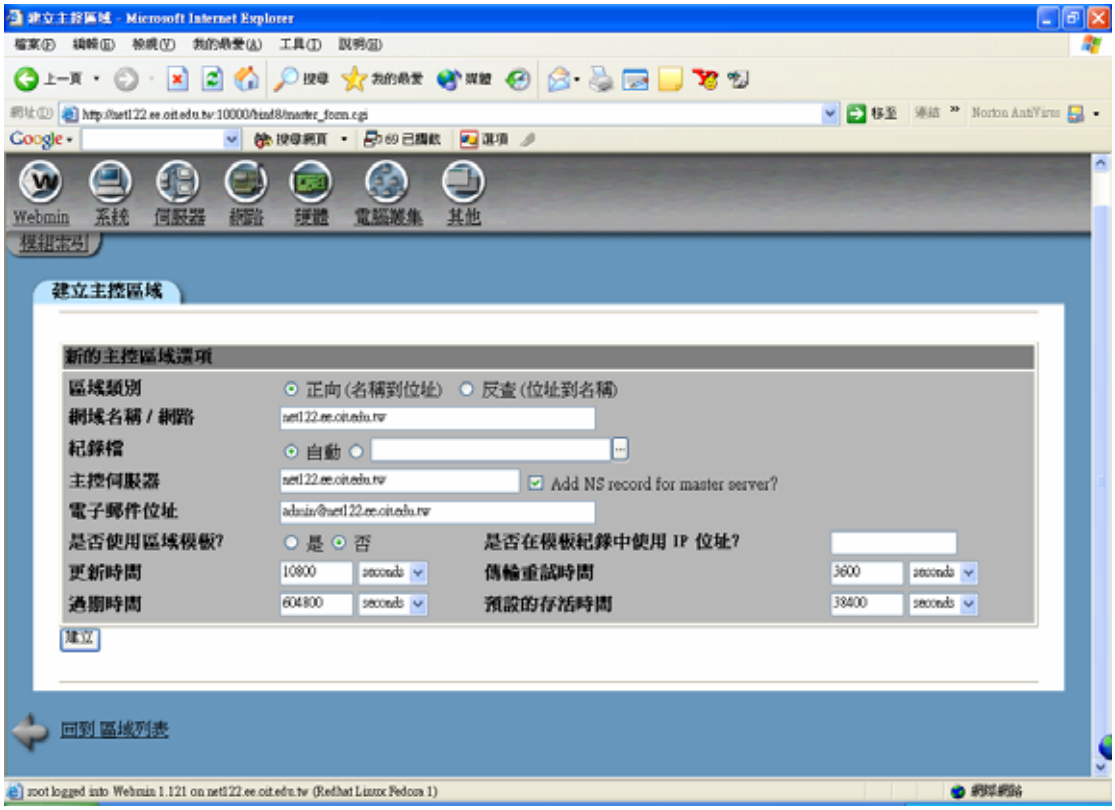
使用 Webmin 來管理 DNS

進入 Webmin 主畫面後，選擇『伺服器』中的【BIND 8 DNS 伺服器】，Webmin

的 DNS 管理畫面如下圖所示。

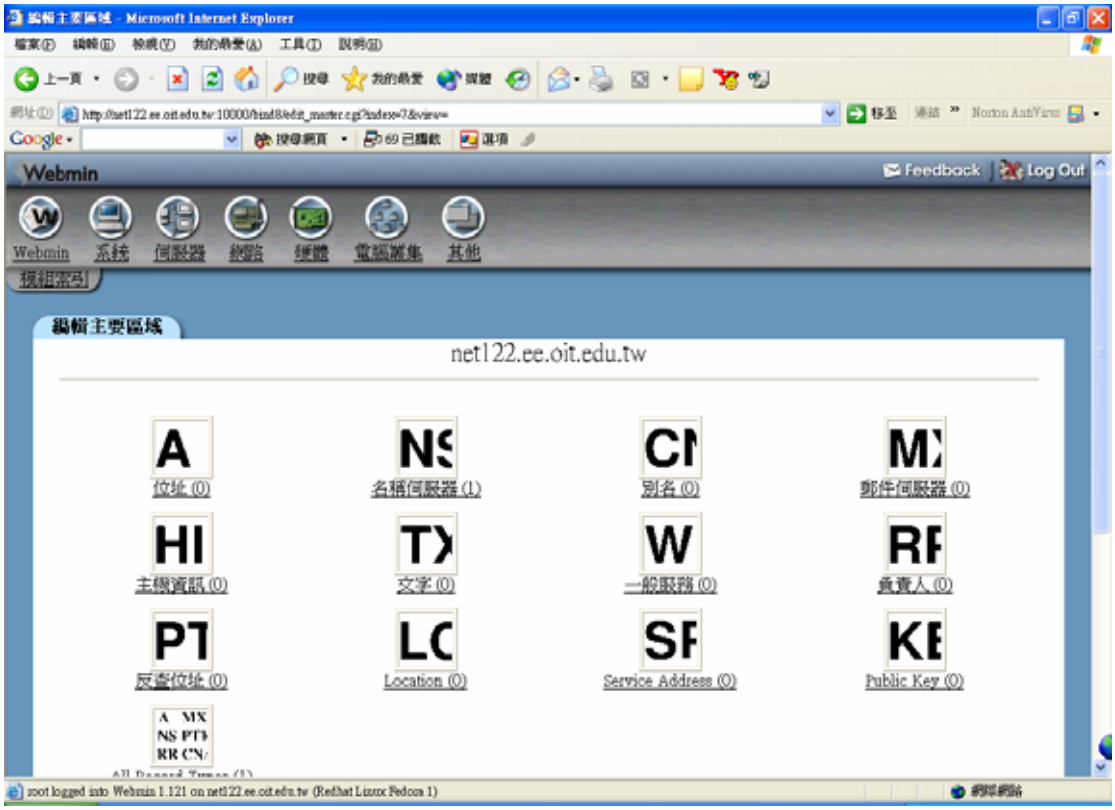
建立一個正解的網域

請點選上圖中『建立一個新的主控區域』的連結，以下的說明請在/etc/resolv.conf 中指定自己的 dns 為本機，不然可能會找不到。

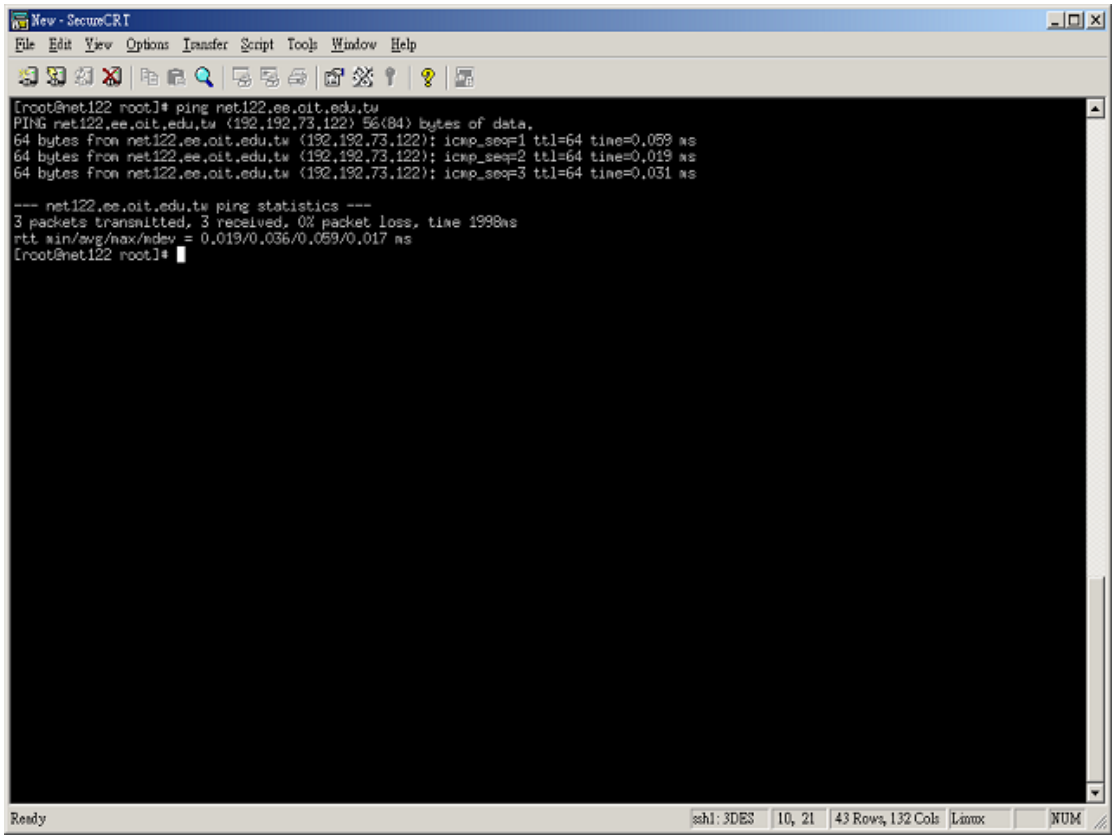


- 【區域類別】請選擇『正向』，因為要建立一個正解的資訊。
- 【網域名稱】請填入至 twnic 所申請的網域，本例中是建立一個內部的網域名稱『net122.ee.oit.edu.tw』。
- 【紀錄檔】使用自動就可以，若要自己建立檔案名稱的話，請自行命名。
- 【主控伺服器】是代表是誰授權給這個網域的控制權，在這因為只有一台 DNS 伺服器，所以填入自己的名稱。
- 【電子郵件位置】是管理者的 mail 位置。

其他的設定，若非必要，建議使用預設值。設定完成後，按下『建立』，會出現以下的畫面。

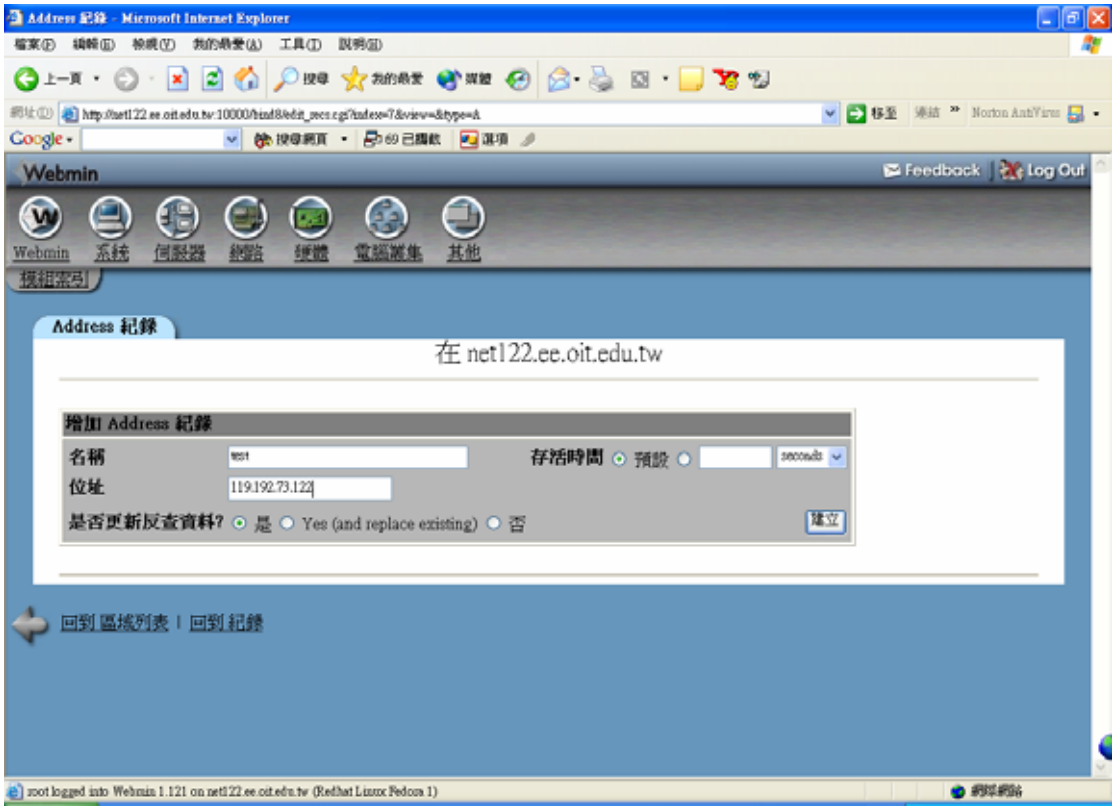


接下來利用 ping 指令來進行測試，如果看到以下的畫面即代表已經通了。



新增一筆主機記錄

點選【位址】。

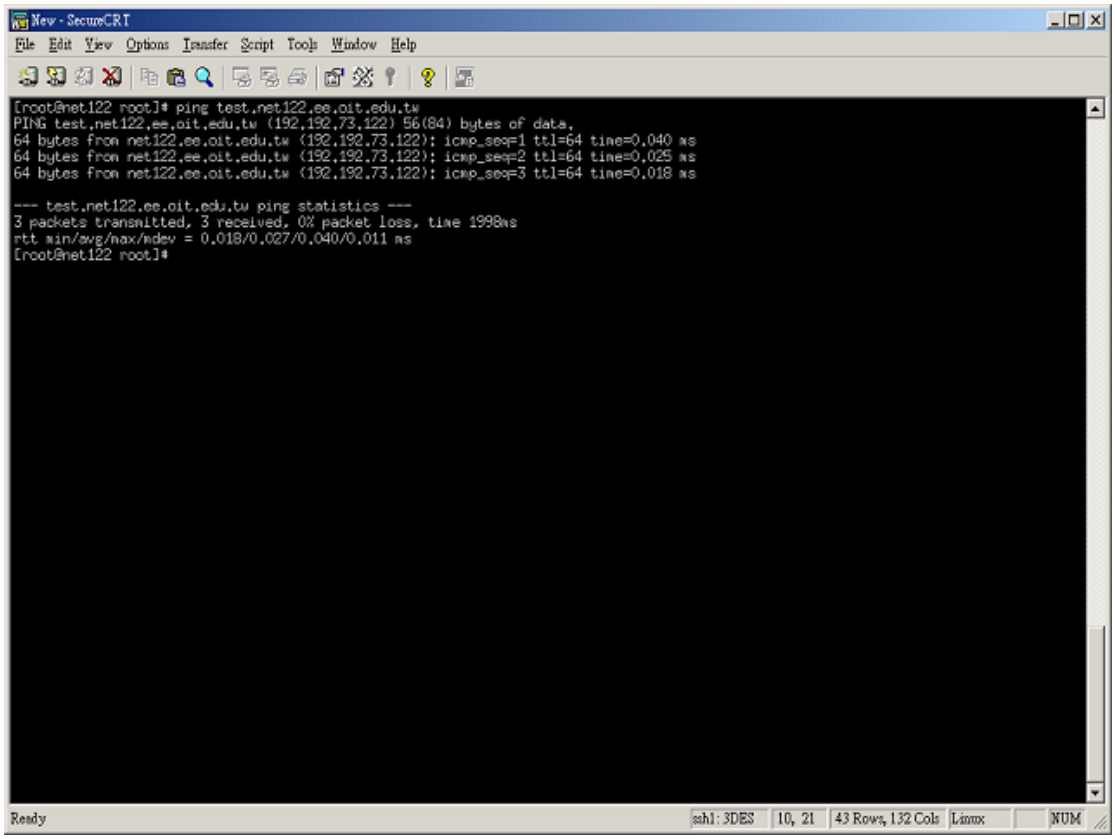


- 【名稱】是代表要在這個網域下所要增加的主機名稱，可以只打主機名稱，此時主機記錄就是完整的 FQDN，否則就要輸入完整的名稱了，也就是『test.net122.ee.oit.edu.tw.』，請注意最後多了一點”.”。
- 【位址】是指主機的 IP 位址，這裡筆者是因為要在同一台主機上增加兩筆記錄，所以選擇其他的 IP 來做為此名稱的位置。
- 【是否要更新反查資料】這個選項是問要不要一塊建立反查資料，在這裡筆者是選擇『Yes (and replace exist)』，就是當如果已經存在的話，直接取代掉舊有的檔案。

完成後按下『建立』，如下圖的畫面就代表已經有了這筆資訊了。


Address 紀錄 - Microsoft Internet Explorer
Webmin
Feedback
Log Out
Webmin
系統
伺服器
網路
硬體
電腦叢集
其他
模組索引
Address 紀錄
在 net122.ee.oit.edu.tw
增加 Address 紀錄
名稱
存活時間
預設
seconds
位址
是否更新反查資料?
是
Yes (and replace existing)
否
建立
名稱
存活時間
位址
test.net122.ee.oit.edu.tw.
預設
119.192.73.122
回到區域列表 | 回到紀錄
root logged into Webmin 1.121 on net122.ee.oit.edu.tw (RedHat Linux Fedora 1)

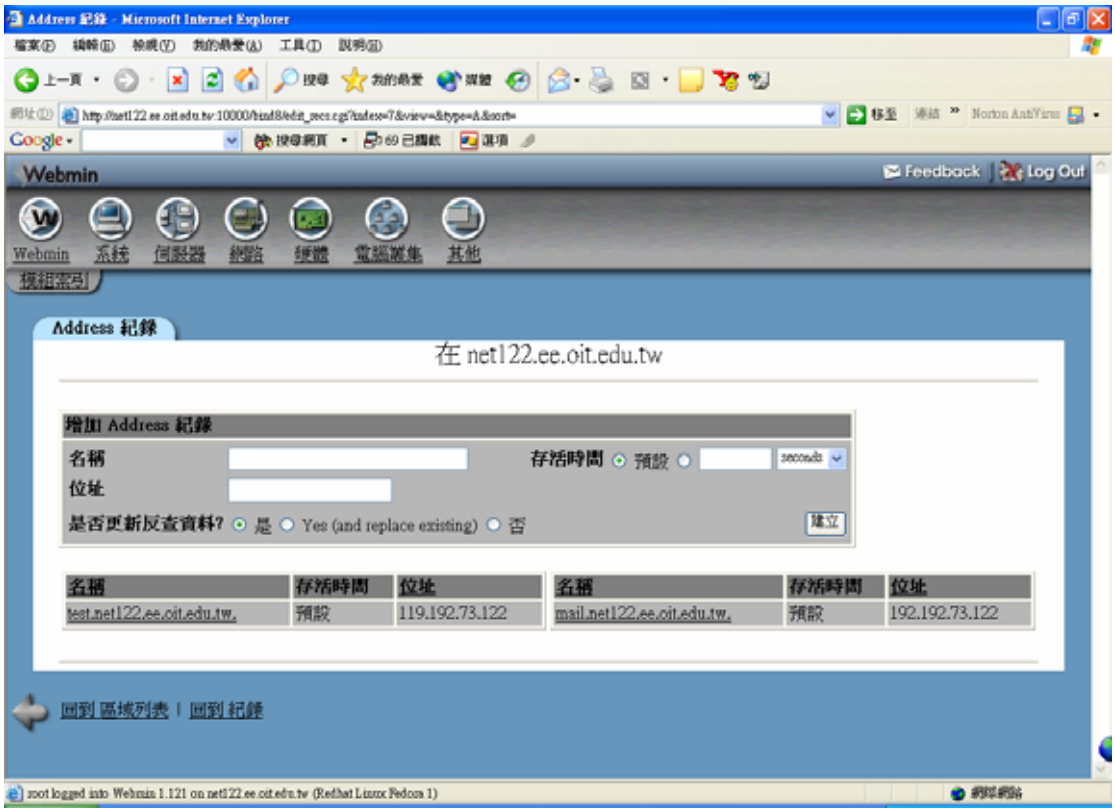
同樣的測試一下。


New - SecureCRT
File Edit View Options Transfer Script Tools Window Help
[root@net122 root]# ping test.net122.ee.oit.edu.tw
PING test.net122.ee.oit.edu.tw (192.192.73.122) 56(84) bytes of data.
64 bytes from net122.ee.oit.edu.tw (192.192.73.122): icmp_seq=1 ttl=64 time=0.040 ms
64 bytes from net122.ee.oit.edu.tw (192.192.73.122): icmp_seq=2 ttl=64 time=0.025 ms
64 bytes from net122.ee.oit.edu.tw (192.192.73.122): icmp_seq=3 ttl=64 time=0.018 ms
--- test.net122.ee.oit.edu.tw ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
rtt min/avg/max/mdev = 0.018/0.027/0.040/0.011 ms
[root@net122 root]#
Ready
ssh1: 3DES
10, 21
43 Rows, 132 Cols
Linux
NUM

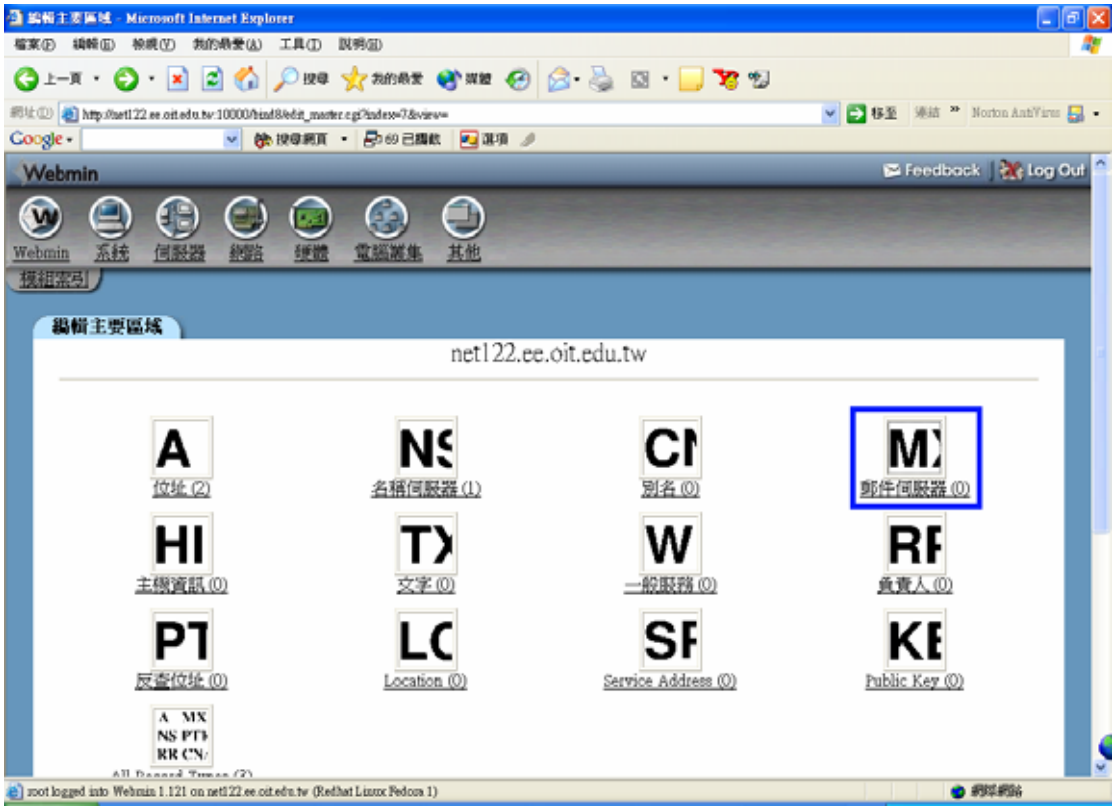
建立一個【郵件伺服器】資源紀錄

- 【郵件伺服器】(Mail eXchange,MX) 資源紀錄可用來設定區域中擔任郵件伺服器的主機，以及該主機郵件傳送時的優先順序，在區域中建立 MX 記錄後，當郵件伺服器要和對方的區域進行郵件傳送時，就可透過 MX 記錄得到對方的郵件伺服器名稱。

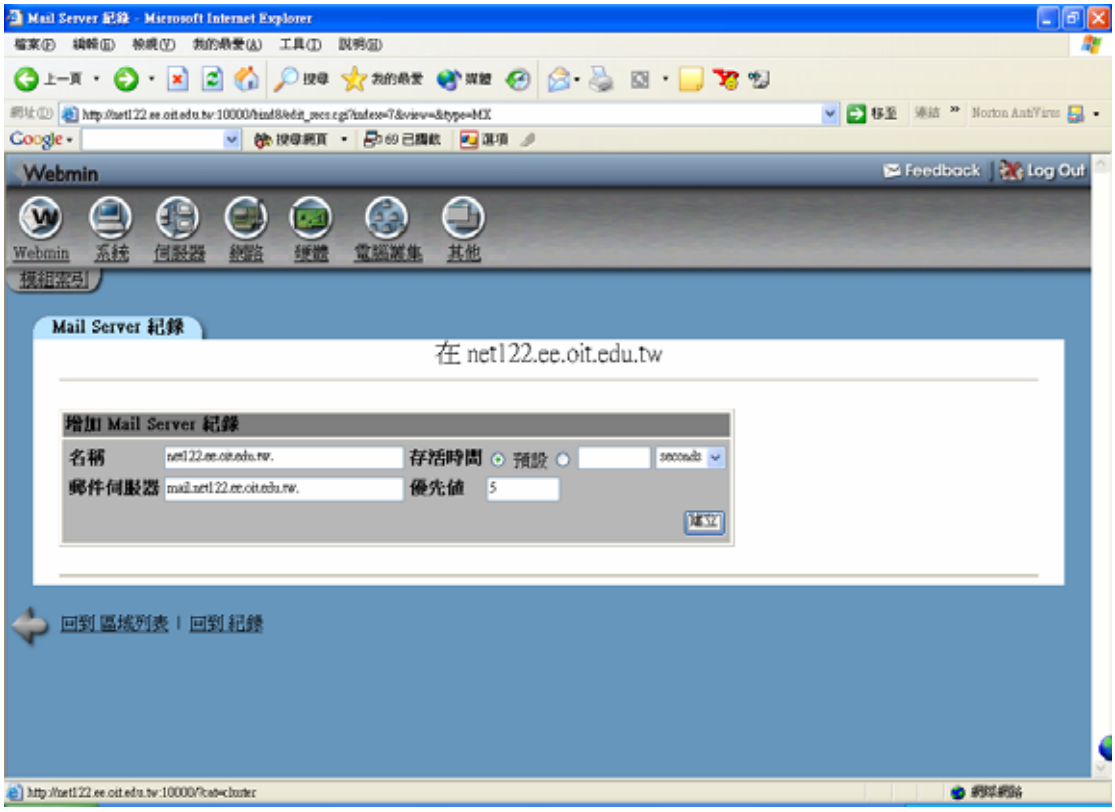
首先建一個主機記錄名叫【mail.net122.ee.oit.edu.tw】，步驟同上所述。



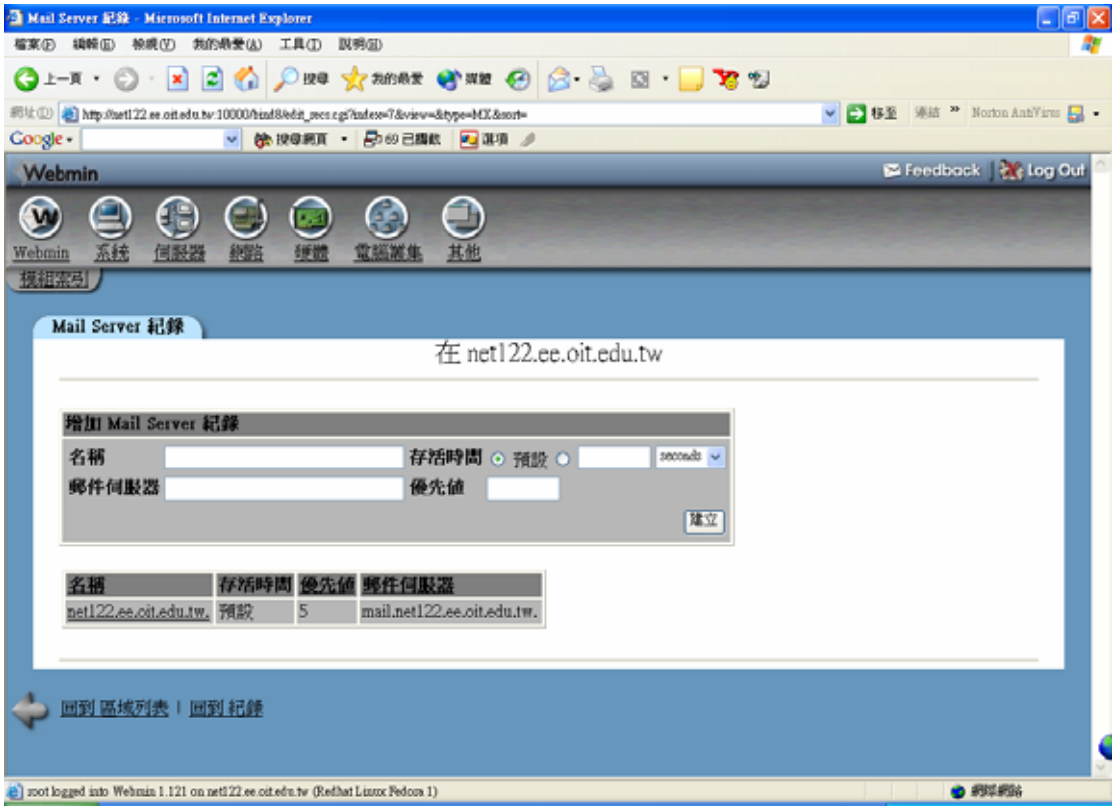
再來就可以建立一個郵件伺服器的記錄，點選【郵件伺服器】。



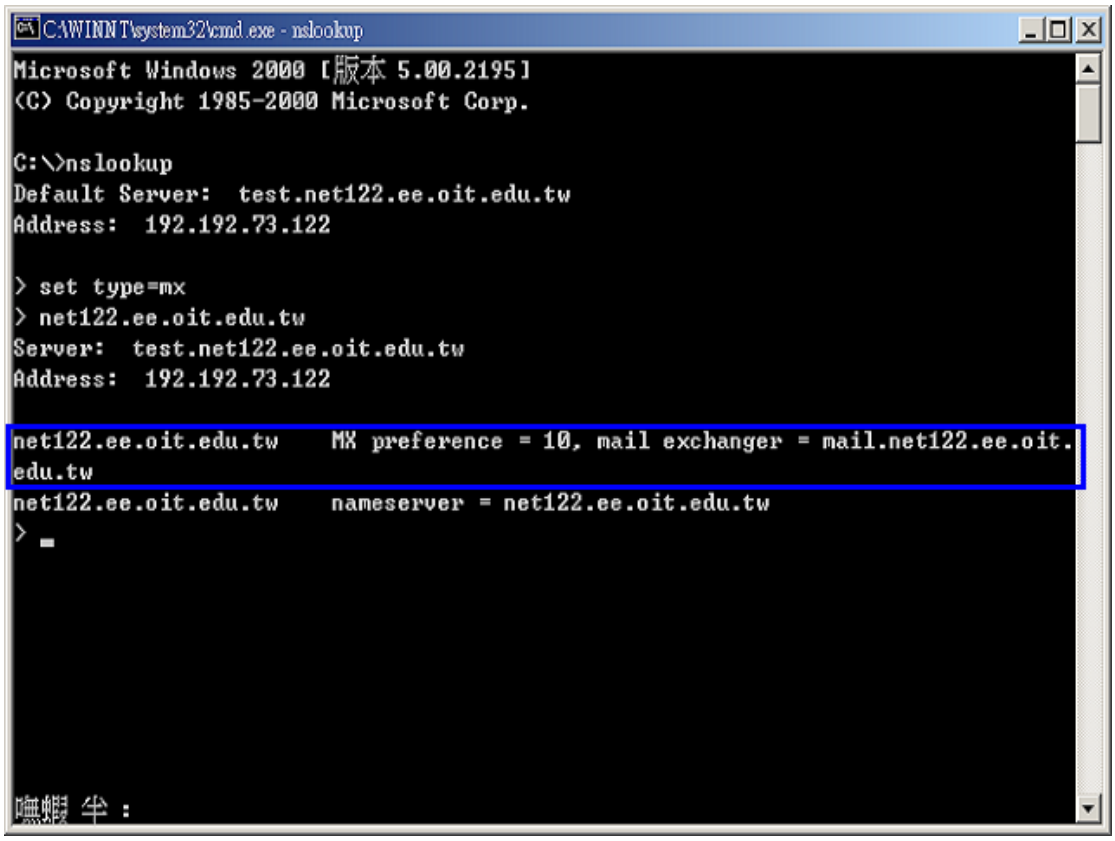
- 【名稱】就是使用 DNS 伺服器的名稱
- 【郵件伺服器】就是可以用來當作 mail server 的主機名稱。
- 【優先權】就是當有兩台以上的 mail server 時的前後順序，值愈小愈優先。



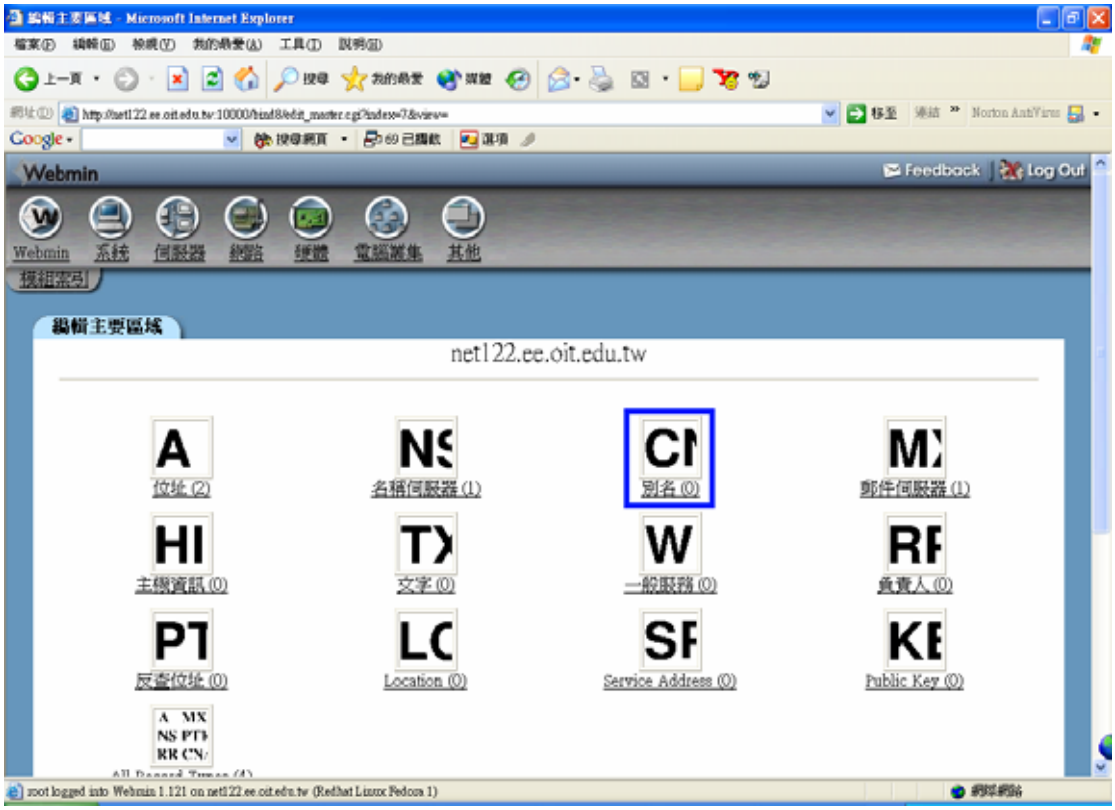
完成後，按下『建立』。



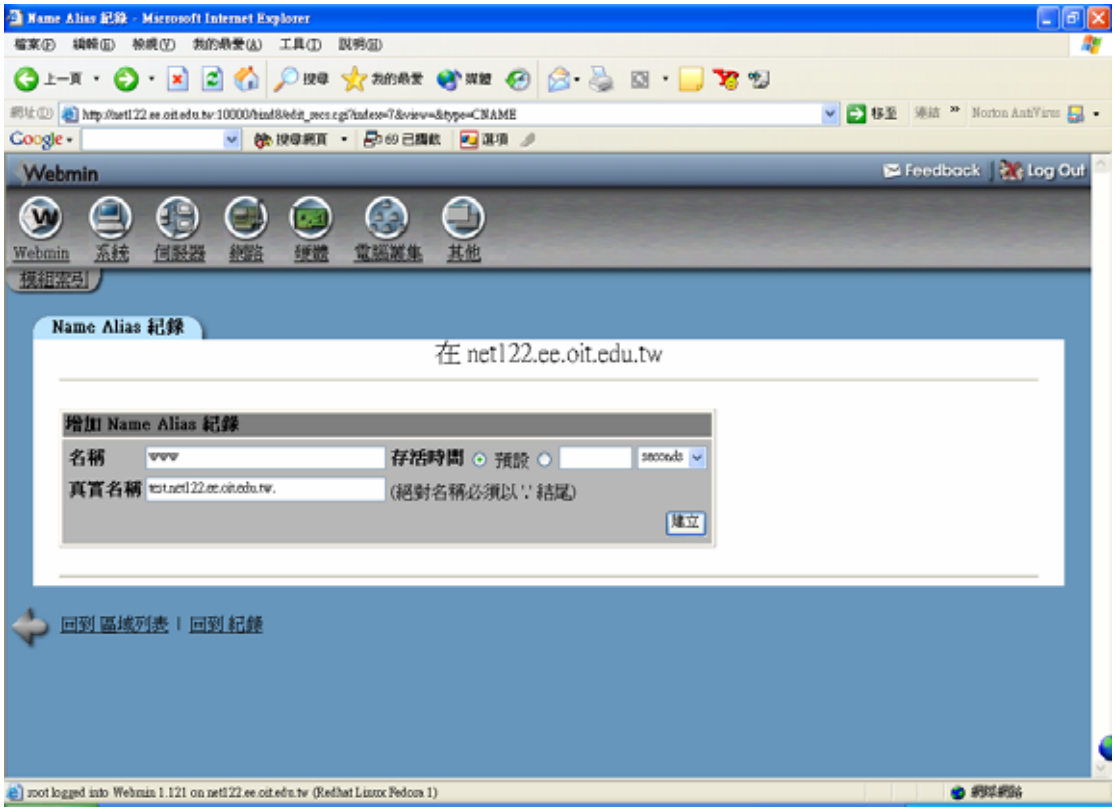
同樣的進行測試，利用 nslookup。出現以下的畫面資訊，就代表成功了。



建立一個【別名】的資源記錄

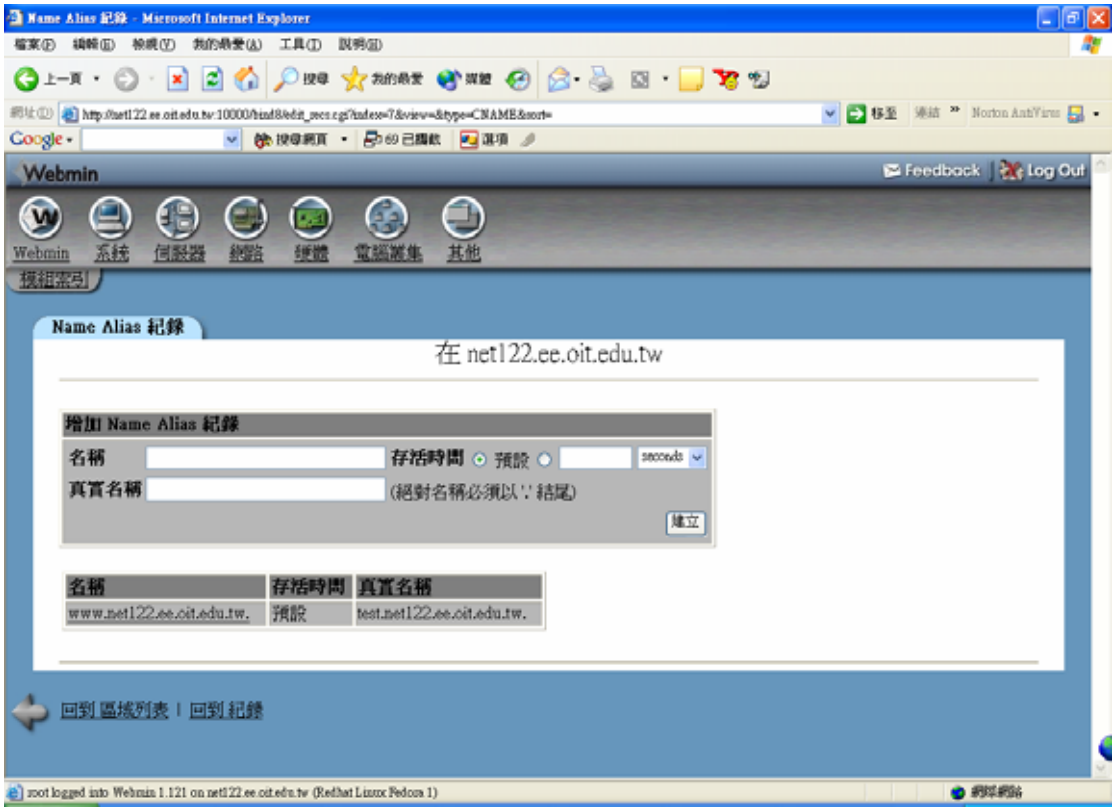


點選進入後，會出現下面的畫面。

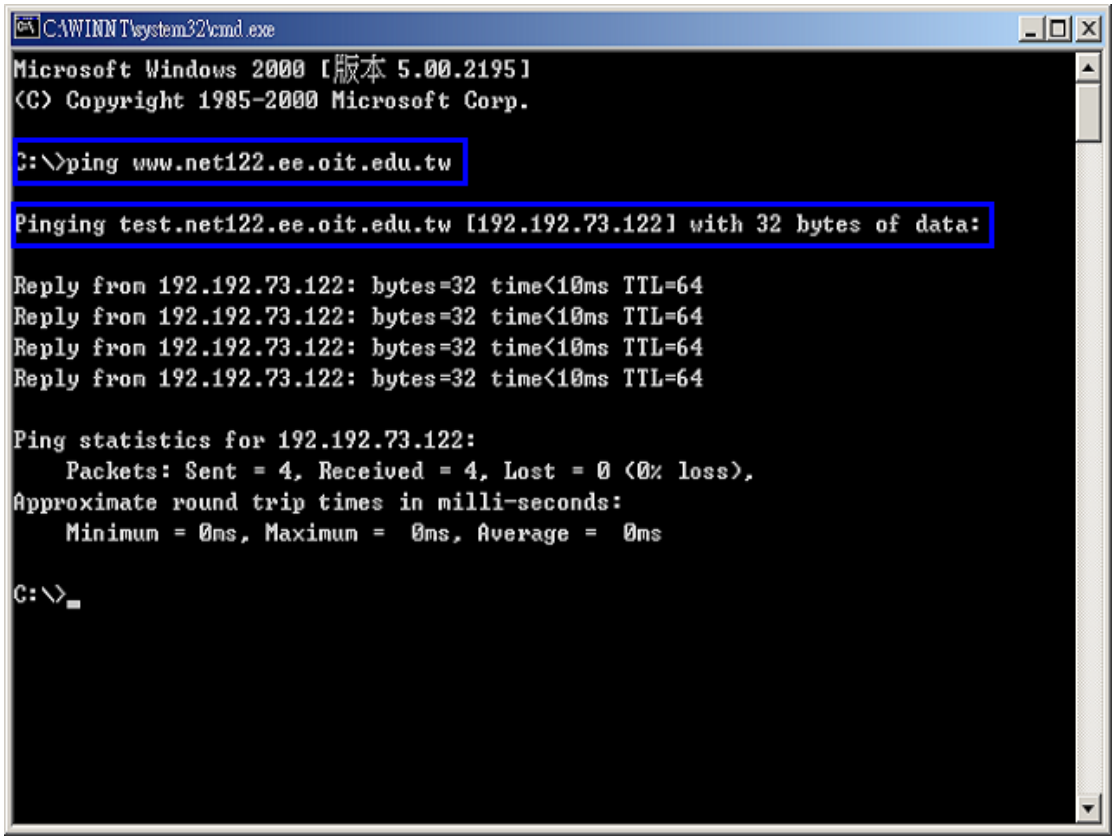


- 【名稱】就是別名名稱。
- 【真實名稱】就是原本的主機名稱。

完成後按下『建立』，會出現如下圖的畫面。

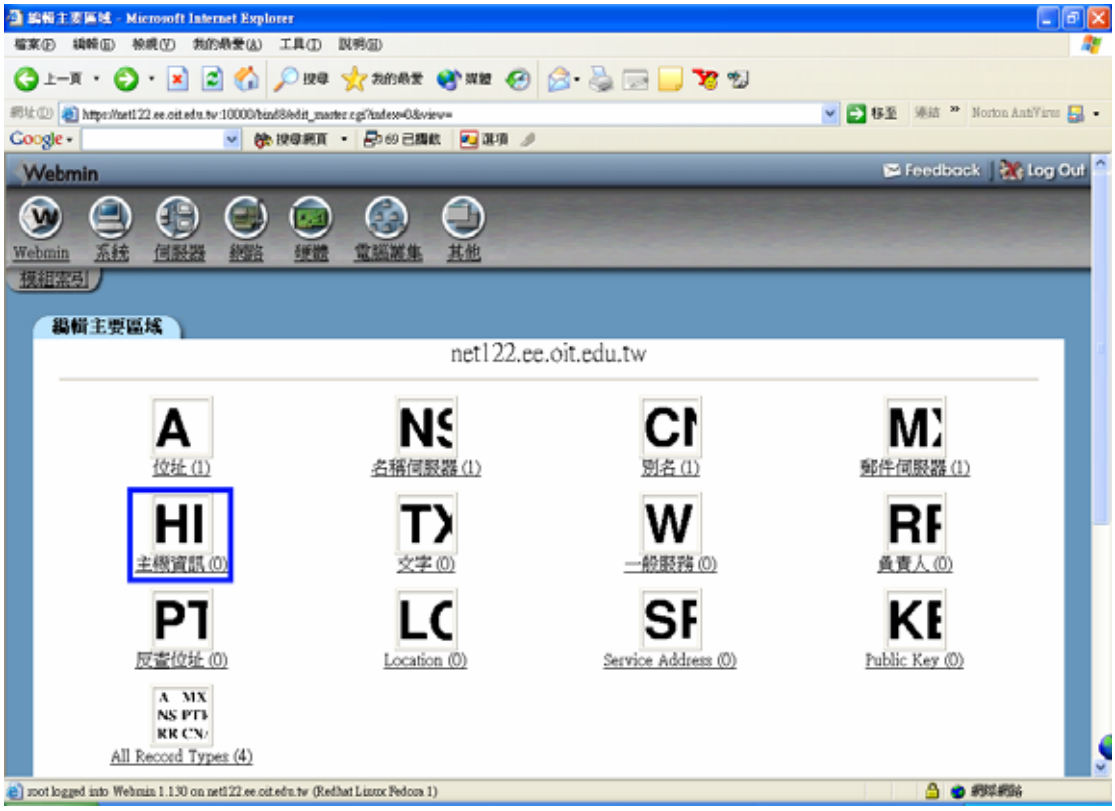


接下來使用 ping 來進行測試。

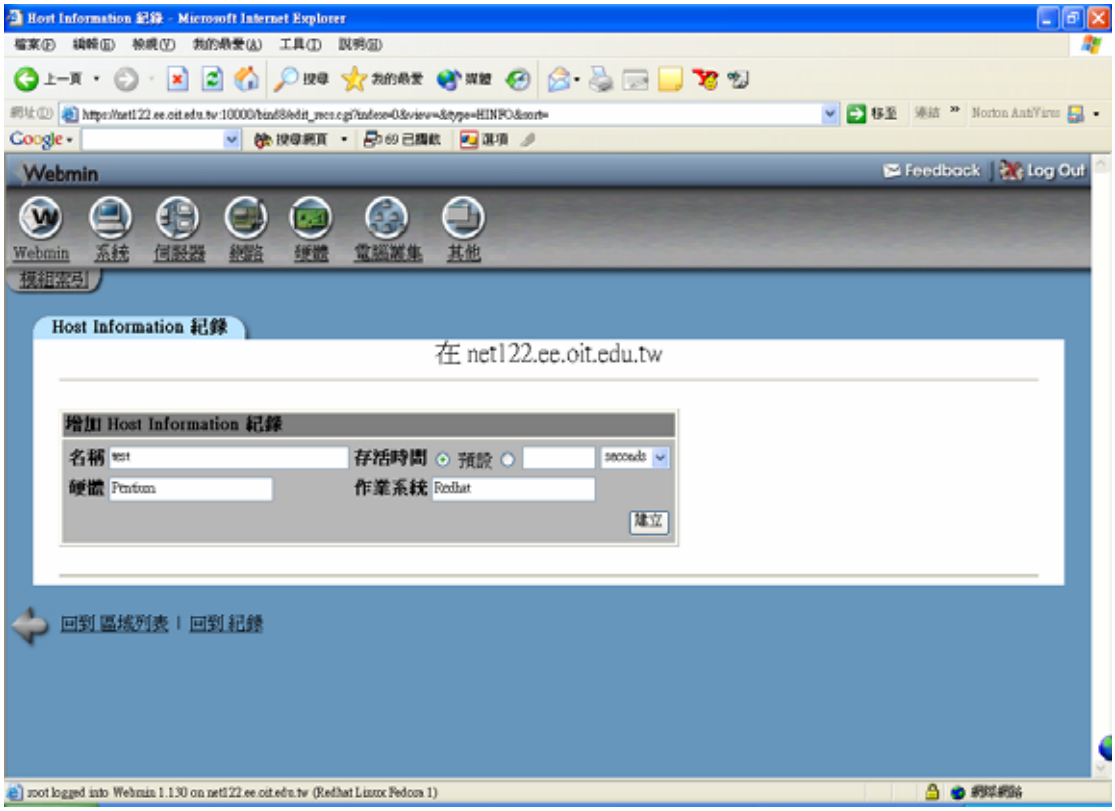


出現以上的畫面就代表成功了。別名記錄是用在當主機上同時進行多個服務時，可以利用別名來減少 IP 的利用量。但需注意的是，每部主機只能配合一個 A 記錄，否則會有錯誤產生。

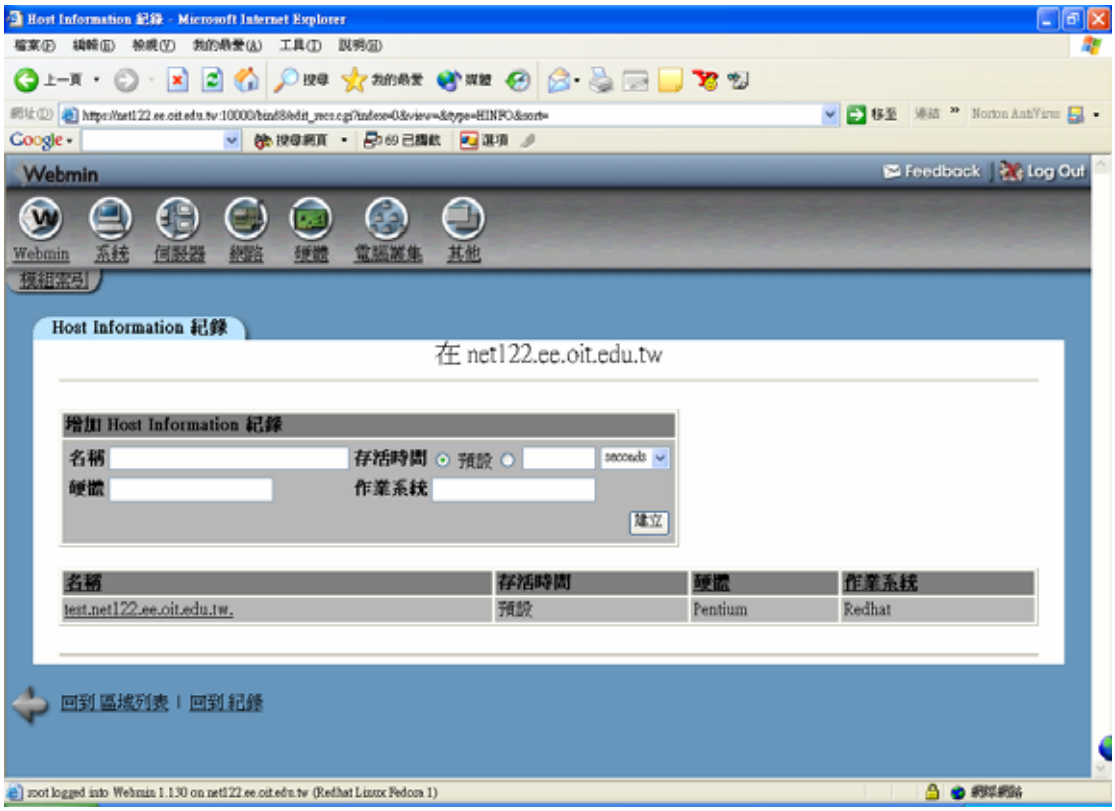
建立【主機資訊】資源記錄



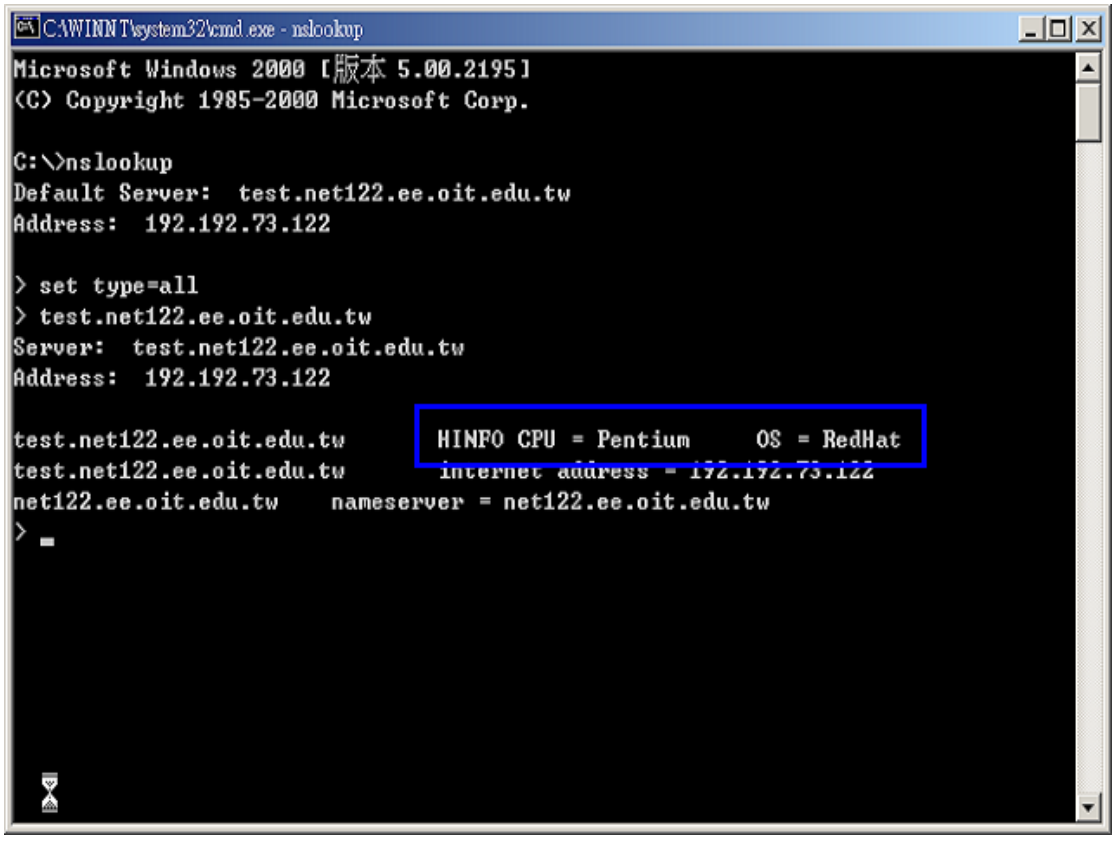
點選進入後，出現以下畫面。



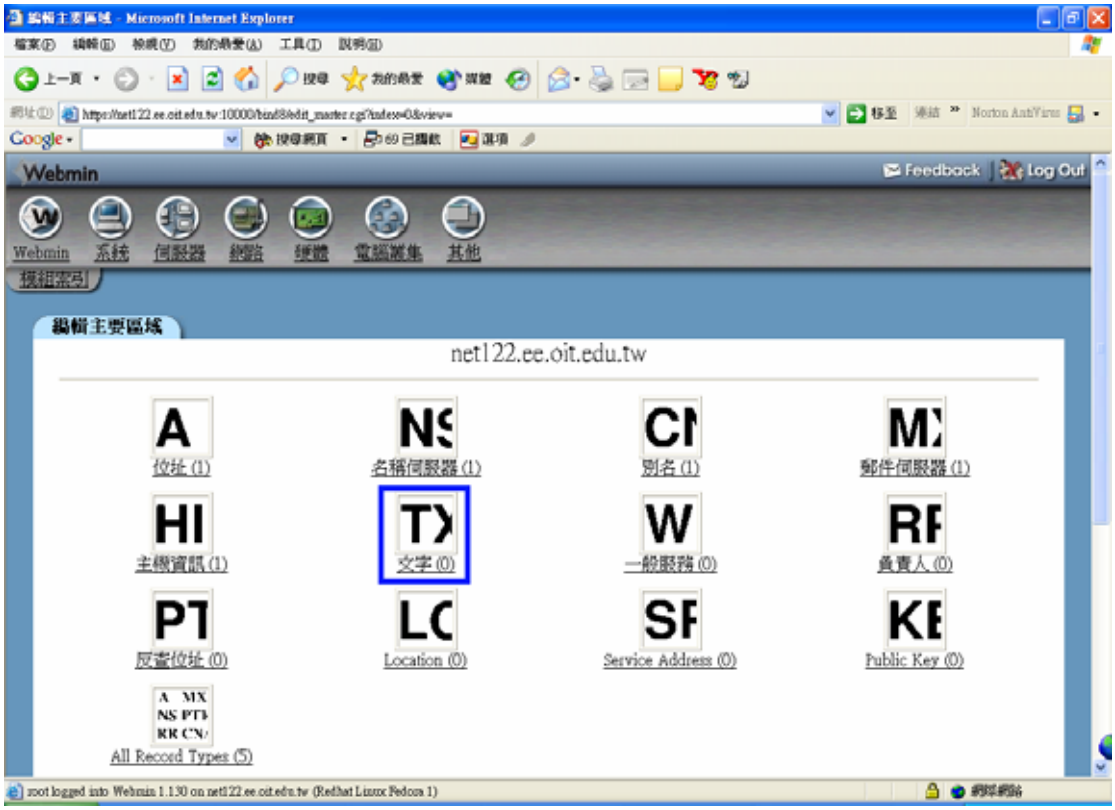
將主機資訊一一填入後，按下『建立』。



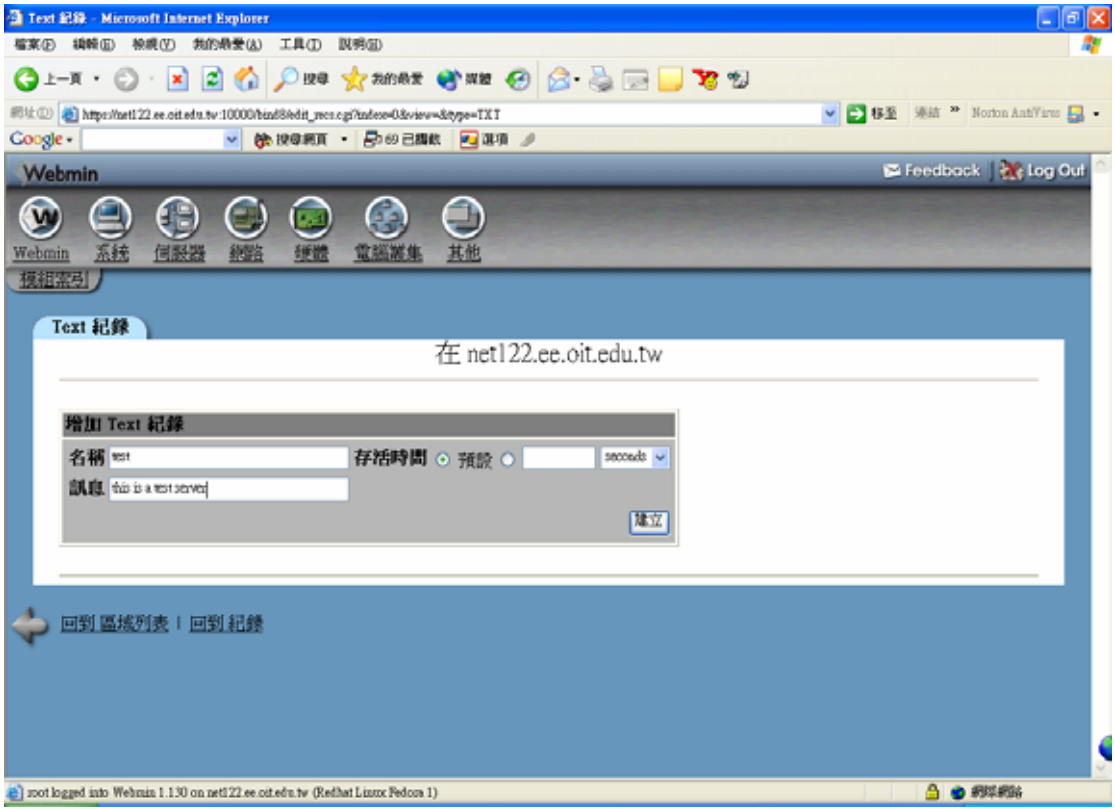
使用 nslookup 來查詢，就會出現硬體的資訊。



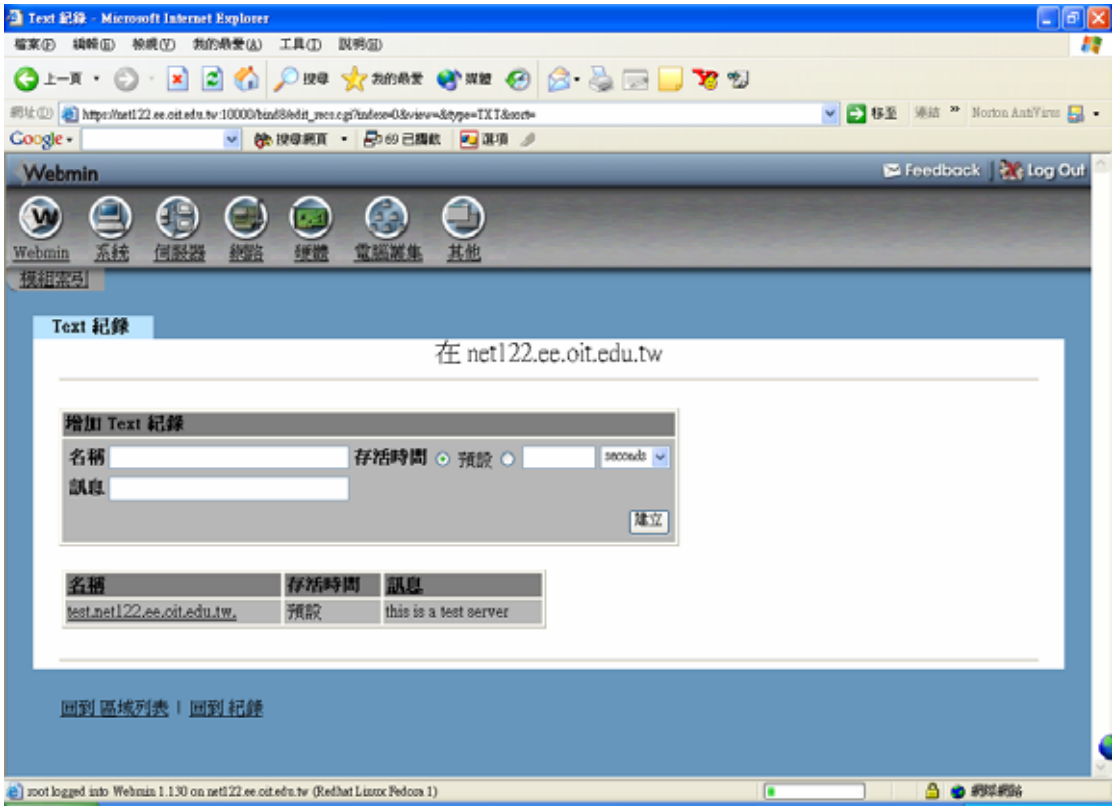
建立【文字】資源記錄



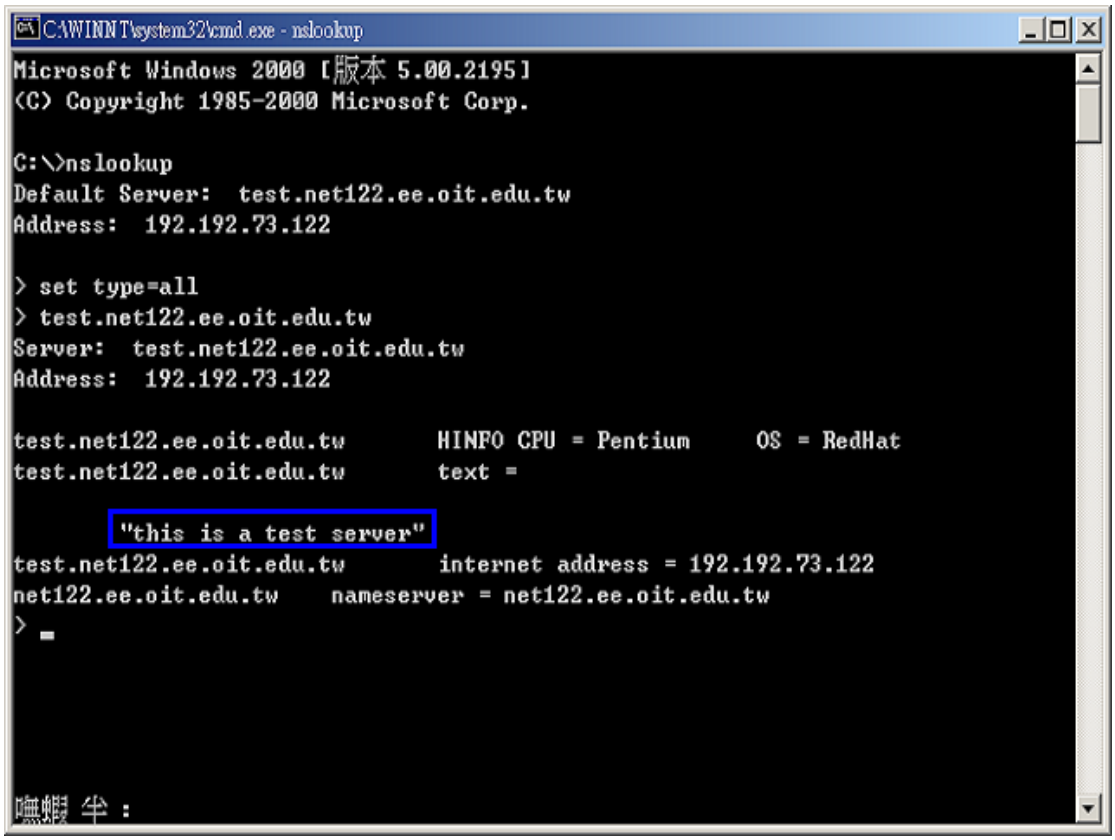
進入後，出現下面的畫面：



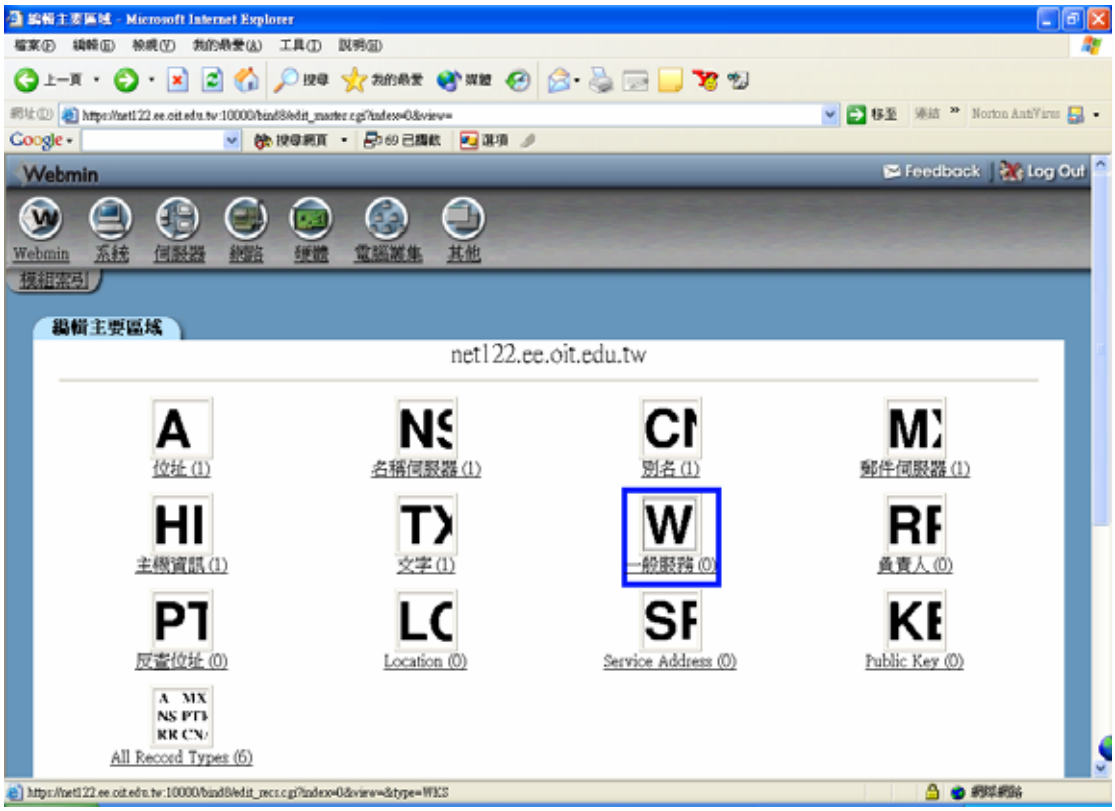
將資訊鍵入後，按下『建立』，就會出現以下的畫面：



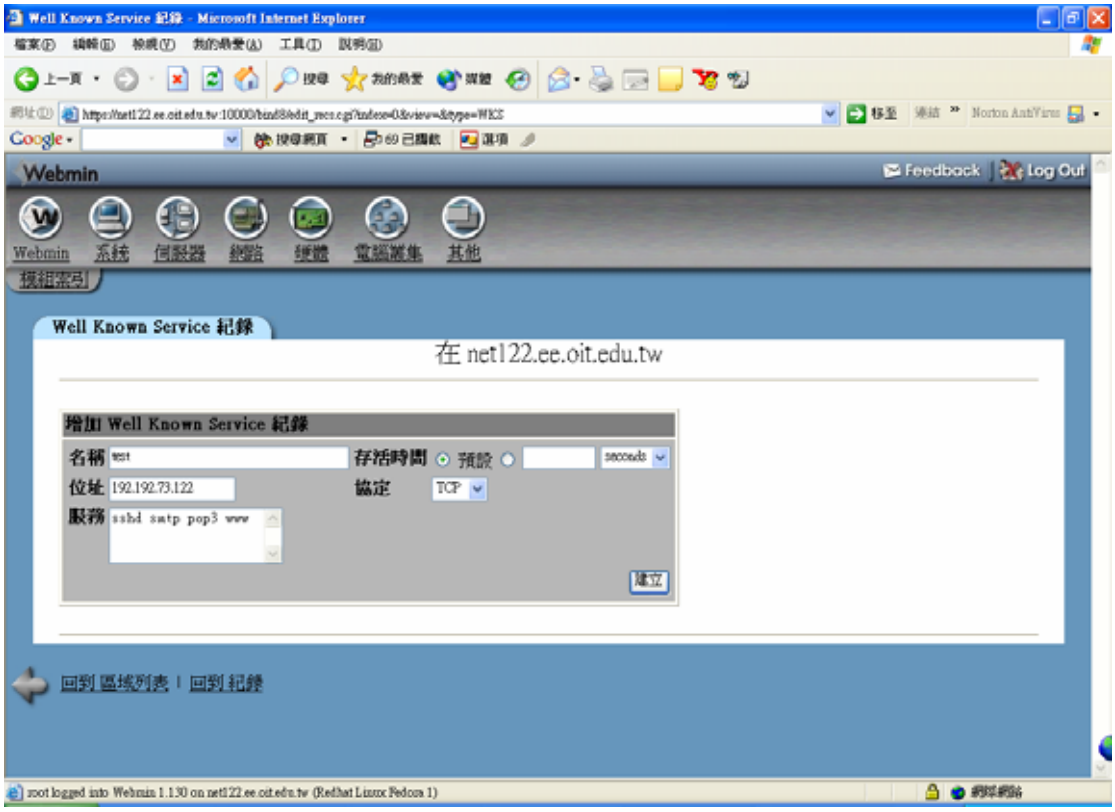
接下來使用 nslookup 測試，出現以下畫面就是成功了。



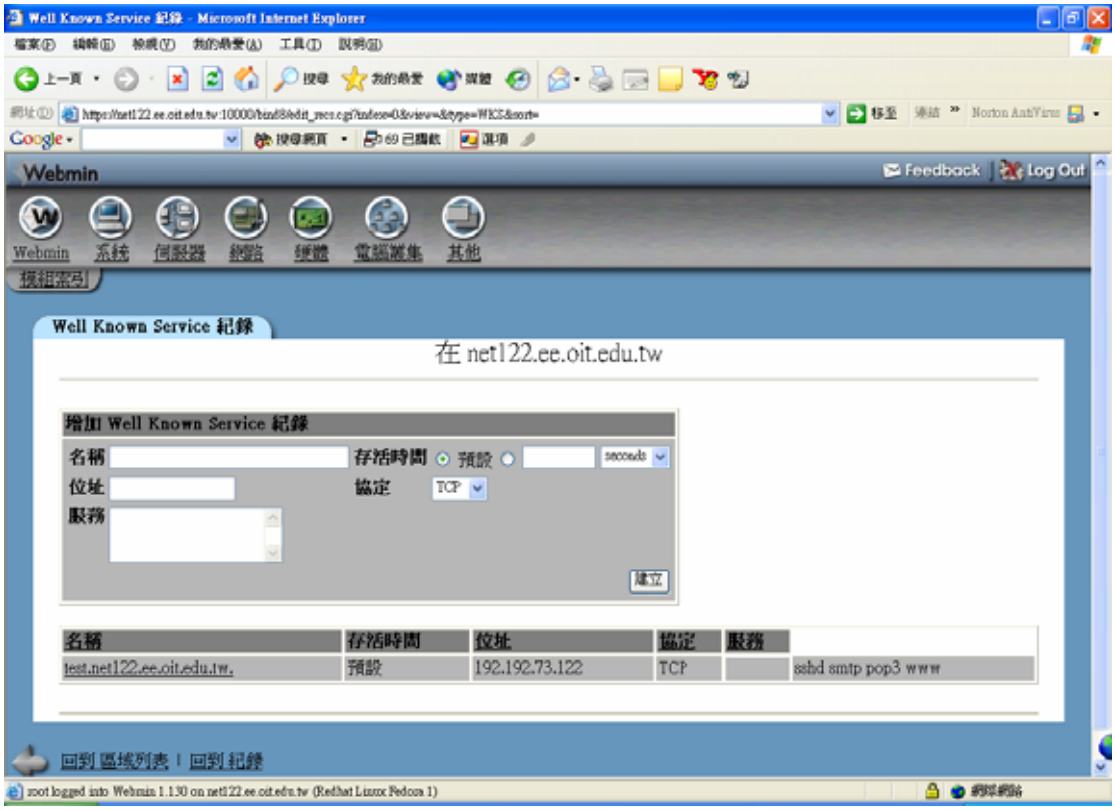
建立【一般服務】資源服務



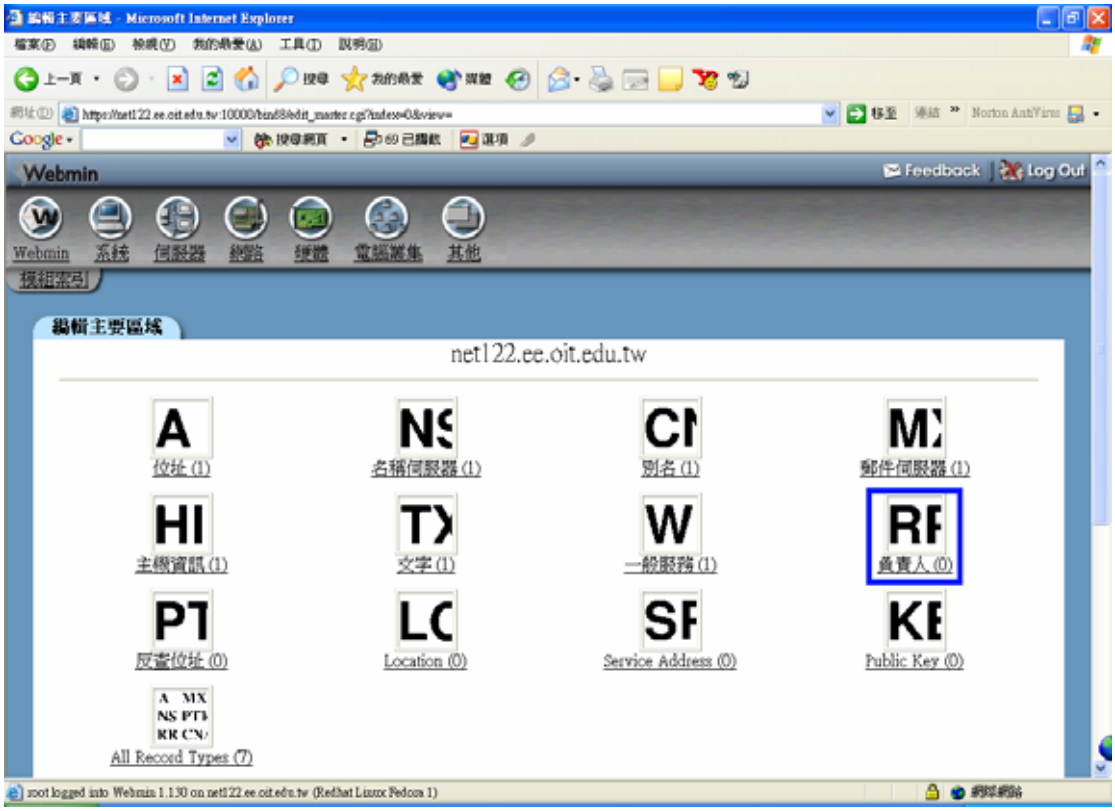
進入後，出現以下畫面：



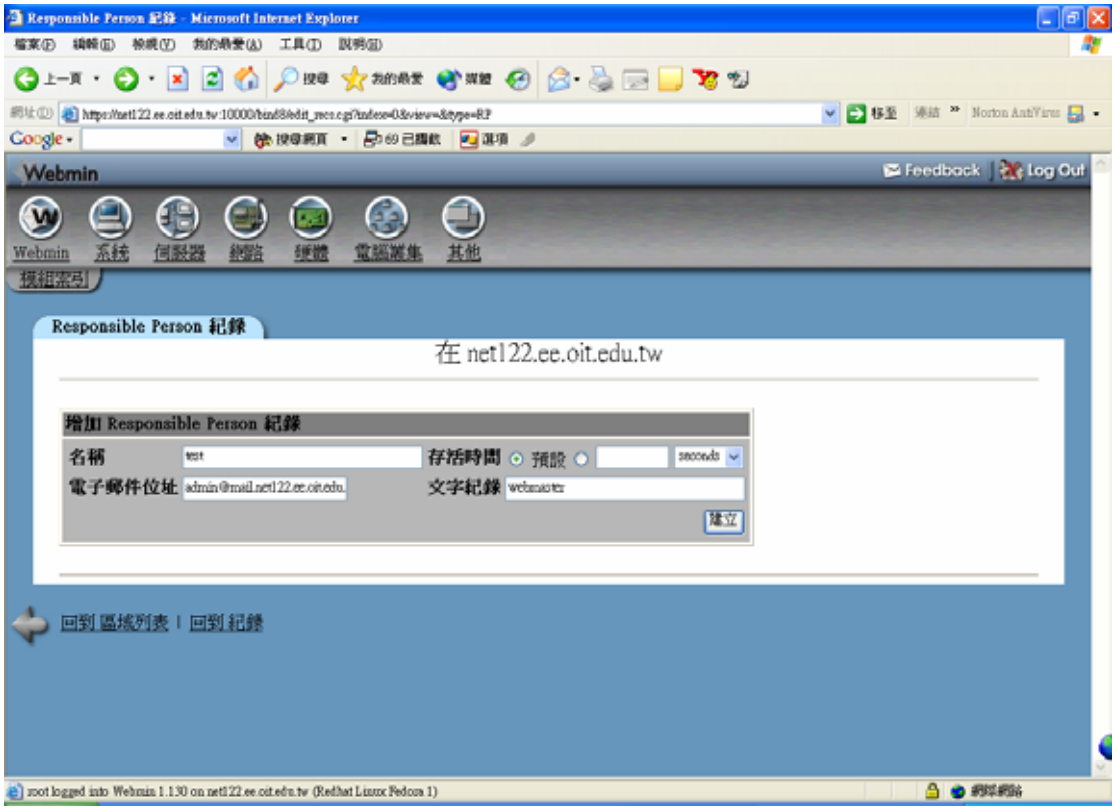
完成後按下『建立』。



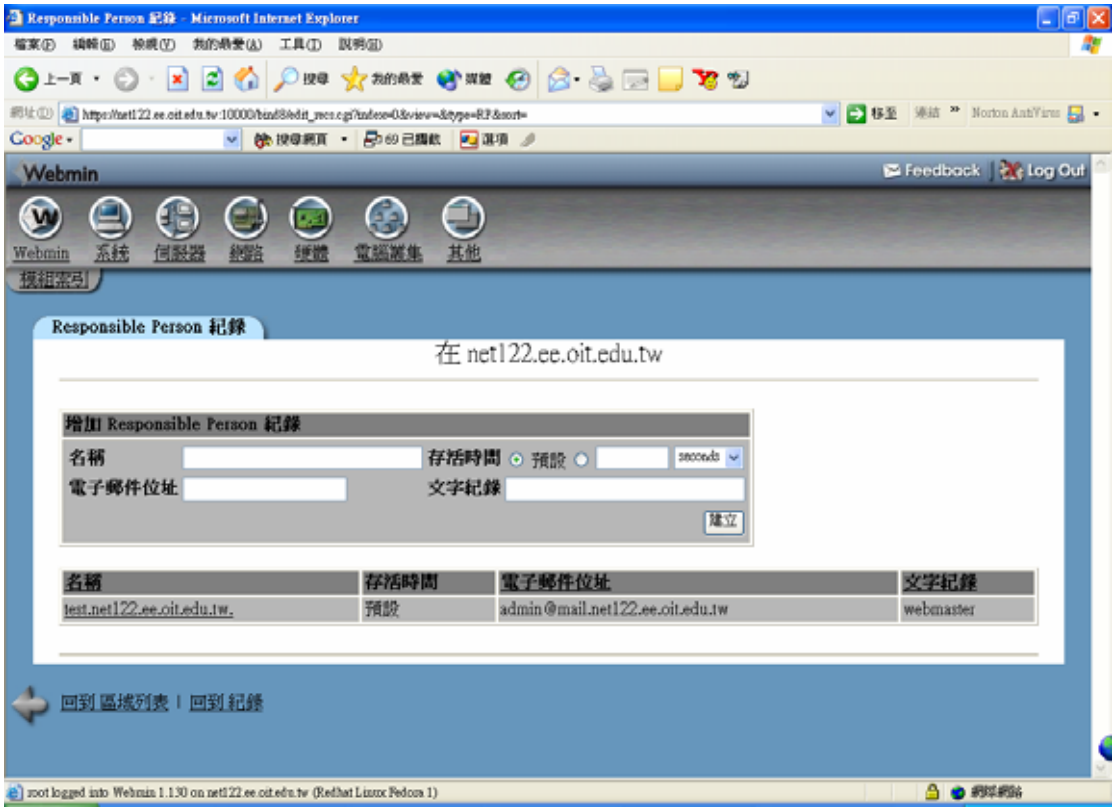
建立【負責人】資源記錄



進入後，會出現以下畫面：



填入所有資訊，按下『建立』，會出現以下畫面：



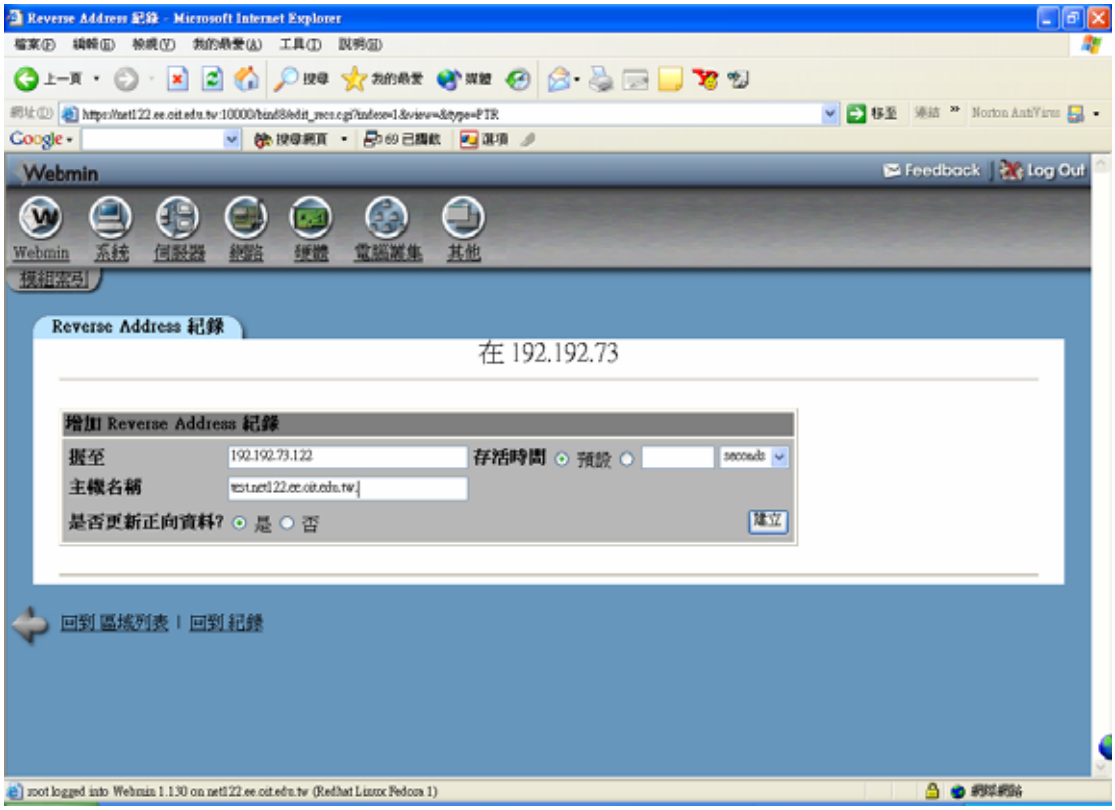
建立一個反解的網域

請點選『建立一個新的主控區域』的連結。

- 【區域類別】請選擇『反查』，因為要建立一個正解的資訊。
- 【網域名稱/網路】請填入現在的 IP 網路區段，本例是用 192.192.73。
- 【紀錄檔】使用自動就可以，若要自己建立檔案名稱的話，請自行命名。
- 【主控伺服器】是代表是誰授權給這個網域的控制權，在這因為只有一台 DNS 伺服器，所以填入自己的名稱。
- 【電子郵件位置】是管理者的 mail 位置。

其他的設定，若非必要，麻煩請都使用預設值。設定完成後，按下『建立』，會出現以下的畫面。

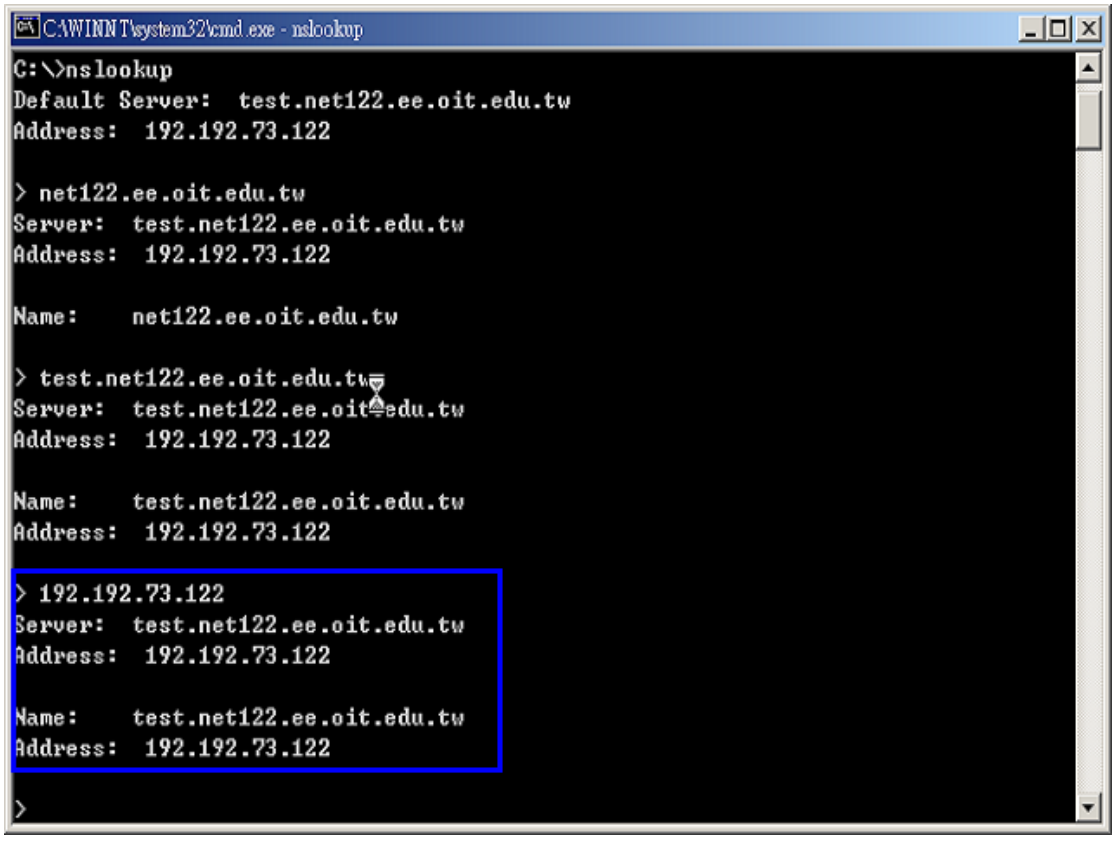
接下來要新增反查的記錄，請按上圖的【反查位址】。



- 【握至】就是所要反查的 IP 位置。
- 【主機名稱】就是在正解所設定的主機名稱。
- 【是否更新正向資料】這裡筆者選擇『是』。

按下『建立』。

進行測試，使用 nslookup。



出現上面的訊息就是代表反查的資料已經建立。

5.問題與討論

1. 請畫出網域架構圖（Domain Name Space）。
2. 為何平時不需輸入完整網域名稱（FQDN、Fully Qualified Domain Name）？
3. 說明 DNS 的查詢流程。
4. 為何需要反解？
5. 說明更新時間長短對網路服務影響。
6. 如何禁止區域轉移（zone transfer）？
7. 說明 DNS 的查詢紀錄。
8. 說明根名稱伺服器的重要性。
9. 說明次要名稱伺服器的重要性。
10. 實作子網域。