DNS建置與設定

2015.11

麟雲資訊 技術處 台南網路服務部

Ring Cloud Technology Inc. - Tainan Service Department

Engineer: 葉宗翰 (Tsung-Han Yeh)

E-Mail: snowfly_yeh@ringcloud.com.tw

內容大綱

- DNS安裝
- DNS運作流程教學
- DNS設定教學
  - named.conf設定
  - IPv4正解設定/ 反解設定
  - IPv6正解設定/反解設定
  - Master/Slave DNS設定
  - DNS 檢查工具
- TANet DNS相關負責單位與聯絡資料

麟雲資訊
Ring Cloud Technology

DNS安裝

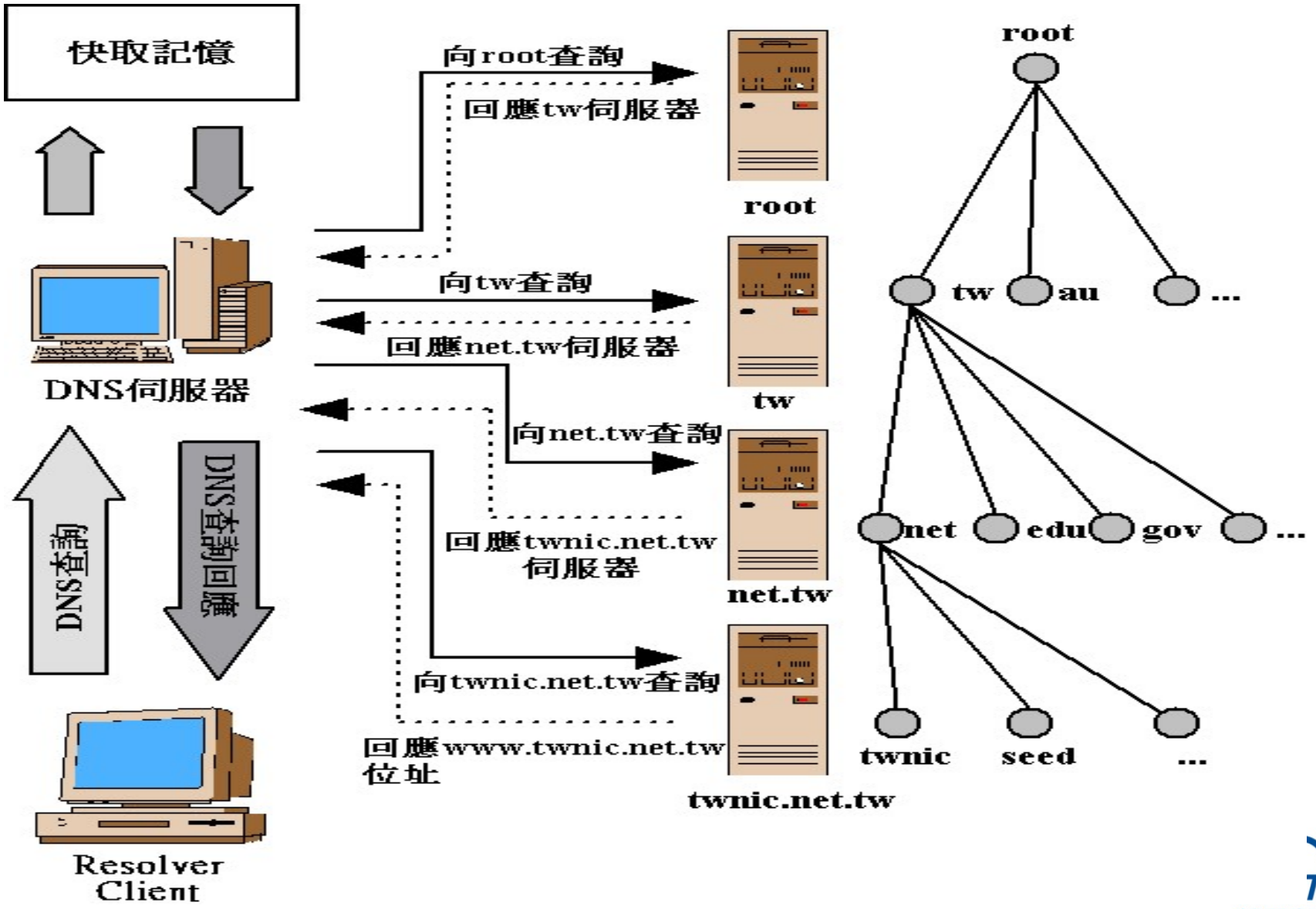
- DNS教育訓練環境安裝 -

- **FreeBSD 9.3 i386**
  - http://0rz.tw/cANEZ
- **DNS-1 ova**
  - http://0rz.tw/CsJMG
- **DNS-2 ova**
  - http://0rz.tw/46xCF
- **account**
  - **root / dns@tnrc**
  - **Student / dns@tnrc**

麟雲資訊
Ring Cloud Technology

DNS運作流程

- DNS查詢流程 -



麟雲資訊
Ring Cloud Technology

DNS設定教學 –
named.conf

- named.conf 主要項目 -

- key
- controls
- options
- acl
- zone

- named.conf : key -

- bind自9.x版開始，結合rndc (remote name daemon control)，使系統管理者可透過rndc從遠端或本機控制bind9。
- **產生rndc.key**
  - **/usr/sbin/rndc-confgen -a -b 512**
- **產生 rndc.conf**
  - **/usr/sbin/rndc-confgen -b 512 > rndc.conf**
- **named.conf、rndc.conf、rndc.key裡面使用到的key需一致**

- named.conf : controls -

- **controls**

```
controls {
        inet 127.0.0.1 port 953
                allow { 127.0.0.1; }
                keys { "rndc-key"; };

        inet 192.168.5.101 port 953
                allow {
                        192.168.5.101;      / / DNS-1
                        192.168.5.102;      / / DNS-2
                }
                keys { "rndc-key"; };

};
```

- named.conf : options -

- **directory [path_name];**
  - zone file 的預設存放位置(default=/etc/namedb)
- **dump-file [path_name];**
  - core dump 預設位置, (default=/var/dump/named_dump.db)
- **pid-file [path_name];**
  - named 的 PID 存放位置(default=/var/run/named/pid)
- **version “ Version String”;**
  - 版本說明，隱藏版本有助於系統安全

- named.conf : options -

- **auth-nxdomain [yes / no];**
  - 是否保留no such domain (NXDOMAIN)資料(default=no)，即不正確資訊的狀況是否做 Cache
- **notify [yes / no];**
  - Zone 變更通知(default=yes)
- **recursion [yes / no];**
  - 遞迴查詢,回應問的人去哪裏查(no)(default=yes)
- **forward [only | first];**
  - Only 只使用代詢,first 則先使用代詢
- **forwarders { [in_addr ; [in_addr ; ...]] };**
  - 代詢伺服器, 找不到的資料都往該 IP 送(若此項有值則上一個項目預設為 first)

- named.conf : options -

- **allow-query { acl-name ; acl-name ; ... };**
  - 允許從哪些 IP 查詢，可使用 acl-name
- **allow-transfer { acl-name ; acl-name ; ... };**
  - 允許從哪些 IP 做Zone Transfer (AXFR) ，可使用 acl-name
- **allow- recursion { acl-name ; acl-name ; ... };**
  - 允許哪些 IP 可以做遞迴查詢，可使用 acl-name
- **listen-on [port ip_port] { acl-name ; acl-name ; ... };**
  - DNS 傾聽 port 為？IP 為？，不建議更改port
- **listen-on-v6 [port ip_port] { acl-name ; acl-name ; ... };**
  - DNS 傾聽 port 為？IPv6 為？，不建議更改port
- **transfer-format { one-answer | many-answers };**
  - Zone Transfer (AXFR) 時一次幾筆 RR (default=one-answer)
- **blackhole { acl-name ; acl-name ; ... }**：
  - 被指定為 blockhole 的主機，所有的查詢要求都會被伺服器忽略，而不傳回任何訊息。預設是 **none**。

- named.conf : options -

- **transfers-in number;**
  - 同時間最大的AXFR(in) 數目(def=10)
- **transfers-out number;**
  - 同時間最大的AXFR(out) 數目(def=10)
- **transfers-per-ns number;**
  - 每部 NS 同時間AXFR 為N個
- **use-id-pool [yes / no];**
  - 每個查詢都保持一份query ID(def=no)，會增加系統負擔但能增加安全性
- **max-transfer-time-in number;**
  - Zone Transfer (AXFR)的最大分鐘(default=120m)

- named.conf : options -

- 範例

```
options {
        version         "0.0.0";
        directory       "/etc/namedb";
        listen-on       { 127.0.0.1; 140.116.241.1; };
        listen-on-v6    { ::1; 2001:288:7001:241::1; };
        forwarders {
                #
        };

        recursion               yes;
        allow-transfer          { myDNS; };
        allow-recursion         { mySubnet; };
        allow-query             { any; };
        transfer-format         many-answers;
};
```

- named.conf : acl -

- 在進行存取控制 (access control) 的設定前，要先於全域設定中指定客戶端來源位址的存取控制列表 (access control list)，也就是撰寫正確的 acl 陳述式：
  - acl acl-name { address_match_list };
  - address_match_list format : ip_address/netmask;
- example
  - acl “intranet" { 192.168.5.0/24; 172.16.1.0/24; };

- named.conf : zone -

- **zone type 總共有 9 種，分別具有不同的功能：**
- **master:** DNS 主伺服器，包含 zone 的所有 RR 資料。
- **slave:** master zone 的複製伺服器，它會定期從 master DNS 裡更新資料，再提供給查詢者。
- **forward:** 這種 zone 只會把收到的查詢轉發給另一個 DNS 伺服器，取得資料後再送回給查詢者，它本身只快取查到的資料，不包含其它紀錄。
- **hint:** 這是一種特別的 zone，用來「提示」root 名稱伺服器的位置。如果伺服器沒有設定 hint zone 的話，程式會用內建的 hint 表格來找出 root 名稱伺服器。

- named.conf : zone -

- **stub:** 和 slave zone 一樣作 master zone 的快取，但 stub 只快取 master zone 中的 NS 紀錄。stub 不是 DNS 中的標準型態，只是 bind 提供的附加功能。一般很少用。
- **delegation-only**：這種 zone 只用於 TLD 進行 delegation。
- **in-view** ： Not valid for the type statement but removes the need for **any** type definition.
- **redirect** ： BIND9.9+. Applicable to recursive servers (resolvers) only. Allows the user to control the behavior of (to redirect) an NXDOMAIN response received only from a non-DNSSEC (unsigned) zone
- **static-stub** ： A stub zone is similar to a slave zone except that it replicates only the NS records of a master zone instead of the entire zone (essentially providing a referral only service). Unlike Stub zones which take their NS RRs from the **real** zone master **Static-Stub** zones allow the user to configure the NS RRs (using server-names) or addresses (using server-addresses) that will be provided in the referral (overriding any valid data in the cache). The net effect of the **static-stub** is that the user is enabled (in a recursive resolver) to redirect a zone, whether for good or evil purposes is a local decision. (In addition to **server-names** and **server-addresses** only allow-query and zone-statistics statements are allowed when **type static-stub;** is present.)

- named.conf : zone -

- **bind9 一安裝好，就預設有許多的 zone，在預設的 zone 裡，“.” 是 hint zone，而其他 zone 則分別是(只列幾個)：**
- RFCs 1912, 5735 and 6303 (and BCP 32 for localhost)
  - “localhost” 、"127.in-addr.arpa"、"255.in-addr.arpa"、
- RFC 1912-style zone for IPv6 localhost address (RFC 6303)
  - 0.ip6.arpa
- "This" Network (RFCs 1912, 5735 and 6303)
  - 0.in-addr.arpa
- Private Use Networks (RFCs 1918, 5735 and 6303)
- 等等等等.....
- 在 zone 名稱尾端若接有 .in-addr.arpa或.ip6.arpa 者，就是反解 zone，而在 .in-addr.arpa或.ip6.arpa 前要以相反順序接上該反解 subnet 的 IP。例如若要為 “192.168.5.0/24” subnet 設立反解 zone，則 zone 名稱就要寫作 5.168.192.in-addr.arpa。所以，broadcast 和 loopback zone 都各有一個正解與反解 zone。

麟雲資訊
Ring Cloud Technology

DNS設定教學 –
IPv4 正解設定/反解設定

- 正解設定 -

- named.conf 設定完成之後，就要把網域所需的資料填進master zone file 裡面去。DNS zone file 裡的資料是以紀錄 (resource record, RR) 為單位，而 DNS 紀錄有許多不同的種類，可以算是相當地複雜。這裡我們會對基本的 RR 作說明

- 正解設定 -

- **$TTL**
  - 存活時間 (TTL)：time to live。它是一個 32 位元，以秒為單位的整數，作用於 RR 被快取時，讓解析主機可以決定該快取這個 RR 多久。
- **$ORIGIN**
- **SOA**
- **A**
- **CNAME**
- **NS**
- **MX**
- **TXT**

- 正解設定: SOA -

- **SOA**
  - 除了 $TTL 之外，SOA (Start of a zone Of Authority) 是 zone 必備的 RR，它一定要是第一個 RR
- 格式

```
@       IN      SOA     dns1.example.edu.tw. abuse.exmpale.edu.tw. (
                        2015020700      ; serial
                        1h              ; refresh
                        30m             ; retry
                        1h              ; expire
                        30m             ; negative-cache-TTL
                        )
```

- 正解設定: SOA -

- **serial**：序號；當其它伺服器在快取這個 zone 時，會依照這個值判斷所取得資料是否比已快取的資料更新，所以當 zone file 內容有改變時，要讓序號至少比原來大 1。

  序號值是一個 32 位元有號整數。有人設定序號的習慣是 YYYYMMDDNN，總共 10 碼的數字，首四碼是西元年，次二碼是月、再次二碼是日，末二碼為當日流水號。
- **refresh**：DNS 伺服器更新快取的時間，單位為秒，一般設為 7 天。
- **retry**：DNS 在更新 zone 失敗時，嚐試重新更新的間隔。單位為秒。一般設為 1 天。
- **expire**：zone data 在 DNS 內失效的時間，單位為秒。一般設為 28 天。
- **negative-cache-TTL**：這個值是設定其它 DNS 多久會從你這裡取得 no such domain (NXDOMAIN) 的訊息，單位為秒。一般設為 1 天。
- 因為 “@” 在 zone file 中特別代表與 zone 關聯的網域，所以在設定 “email” 的時候必須用 "." 來代替 "@"。

- 正解設定: NS -

- **NS** 用來指定網域的名稱伺服器，格式為
  - domain-name　　IN　NS　　domain-name-server
  - @　　IN　NS　　domain-name-server
- **domain-name-server** 則為名稱伺服器，名稱伺服器可以用 IP，也可以用網域名稱來指定，如果用網域名稱的話，還需要 **A** Record，才能讓客戶端查到名稱伺服器的 IP：
- 在 zone file 裡指定關聯網域的 **NS** 時，通常我們會用上 @

- 正解設定: MX -

- **MX** 紀錄用來設定網域名稱的郵件交換主機 (**MX** 為 Mail eXchanger 之意)，格式為
  - Name IN MX Proirity Mail-Exchanger
  - @ IN MX Proirity Mail-Exchanger
- 範例
  - @ IN MX 10 antispam
  - @ IN MX 20 mail

- 正解設定: TXT -

- **TXT** 紀錄是網域名稱的說明，格式為
  - name IN TXT text
  - @ IN TXT text
- 範例
  - @ IN TXT “This is example.edu.tw."

- 正解設定: A -

- **A** 可以指定名稱到 IP 的對應，格式為
  - name　IN　A　　ip-address
- 範例
  - www　IN　A　　192.168.5.20

- 正解設定: CNAME -

- **CNAME** 中的 C 是指 Canonical，可以當作是 DNS 中的別名設定。格式為
  - **name　IN　CNAME　alias-name**
- 範例
  - **web　　IN　CNAME　www**
- 那麼客戶端在查詢 web.example.edu.tw 時，會先查到它是 www.example.edu.tw 的 CNAME，再進一步查詢 www.example.edu.tw 時，就能取得其 IP

麟雲資訊
Ring Cloud Technology

DNS設定教學 –
IPv4 正解設定/反解設定

- 反解設定 -

- 反解的設定通常又比正解的設定更單純，絕大部分的反解 zone 只具有 **SOA**, **NS** 和 **PTR** 三種紀錄。
- **$TTL**
- **$ORIGIN**
- **SOA**
- **NS**
- **PTR**

- 反解設定: SOA -

- **SOA**
  - 除了 $TTL 之外，SOA (Start of a zone Of Authority) 是 zone 必備的 RR，它一定要是第一個 RR
- 格式

```
@       IN      SOA     dns1.example.edu.tw. abuse.exmpale.edu.tw. (
                        2015020700      ; serial
                        1h              ; refresh
                        30m             ; retry
                        1h              ; expire
                        30m             ; negative-cache-TTL
                        )
```

- 反解設定: PTR -

- **PTR** 設定了 IP 到網域名稱的對應，格式為
  - ip-address　　IN　PTR　　name
- 範例
  - 20　　IN　PTR　　www.example.edu.tw.
- 千萬記得最後面的名稱要接 "."　!!

- 反解設定: PTR -

- 範例

```
$TTL 86400
@       IN      SOA     dns1.example.edu.tw. abuse.example.edu.tw. (
                        2015020700      ; serial
                        1h              ; refresh
                        30m             ; retry
                        1h              ; expire
                        30m             ; default_ttl
                        )
        IN      NS      dns1.example.edu.tw.
        IN      NS      dns2.example.edu.tw.

$ORIGIN 5.168.192.IN-ADDR.ARPA.
20      IN      PTR     www.example.edu.tw.
```

麟雲資訊
Ring Cloud Technology

DNS設定教學 –
IPv6 正解設定/反解設定

- 正解設定 -

- 僅需在**zone file**裡面增加**RR** (resource record)
- **Zone file**
  - **IPv4 Record**
    - **www IN A 192.168.5.20**
  - **IPv6 Record**
    - **www IN AAAA 2001:288:7AAA:5::20**

- 反解設定 -

- 需增加zone file設定
- named.conf
- 以2001:288:7001:241::/64為例

```
zone “1.4.2.0.1.0.0.7.8.8.2.0.1.0.0.2.ip6.arpa" {
        type master;
        file "Rev/Rev-2001:0288:7001:241";
};
```

- a

- 反解設定 -

▪ 需增加zone file設定

```
$TTL 86400
@       IN      SOA     dns1.example.edu.tw. abuse.example.edu.tw. (
                        2013100702      ; serial
                        1h              ; refresh
                        30m             ; retry
                        1h              ; expire
                        30m             ; default_ttl
                        )
        IN      NS      dns1.example.edu.tw.

$ORIGIN 1.4.2.0.1.0.0.7.8.8.2.0.1.0.0.2.ip6.arpa.
1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0        IN      PTR     dns1.example.edu.tw.
0.2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0        IN      PTR     www.example.edu.tw.
```

麟雲資訊
Ring Cloud Technology

DNS設定教學 –
Master / Slave DNS設定

麟雲資訊
Ring Cloud Technology

DNS設定教學 –
DNS檢查工具

- DNS檢查工具 -

- named-checkconf [filename]
  - 做named.conf的檢查
- named-checkzone zonename [zone file]
  - 做zone file的檢查
- dig

麟雲資訊
Ring Cloud Technology

DNS正反解聯絡單位

- DNS正反解聯絡單位 -

網域名稱	上層負責單位	業務負責人	聯絡電話
大專院校 XXX.edu.tw	教育部資訊及科技教育司	林啟文 先生	(02)7712-9091
高中職 XXX.tn.edu.tw XXX.tnc.edu.tw	臺南市教育網路中心	郭子誠 組長	(06)2130669 轉28
反解授權： 120.114.0.0/16 120.115.0.0/16 120.116.0.0/16 163.26.0.0/16 IPv6反解 ---------- 非以上網段之反解授權請逕洽教育部登記	臺南區網中心 (成功大學)	朱敏清 先生	(06)2757575 轉61008

麟雲資訊
Ring Cloud Technology

討論

- Discuss -

- 討論