(Caching) recursive DNS 伺服器的設定

(Caching) recursive DNS 伺服器為提供遞迴查詢服務以解析任何 DNS 資源記錄，為避免 open DNS resolver 問題，應限制使用對象。

BIND ACL 設定

以下例子為設定 DNS 伺服器 140.114.XX.YY 的 named.conf 設定檔，限制校內 IP 位址方可查詢，以免造成 open DNS resolver 問題。

- 設定參數 acl nthu-nets { 140.114.0.0/16; 127.0.0.1/32; }定義 nthu-nets 的 IP 範圍。
- 設定參數 allow-query { nthu-nets; }允許 nthu-nets 查詢服務。

```
acl nthu-nets { 140.114.0.0/16; 127.0.0.1/32; };
options {
 //(其他參數略...)
   // Recursive Name Server
   allow-query { nthu-nets; };
};
```

修改完上述設定並重新啟動 named 後，再以指令測試。

```
#  dig @140.114.64.1 gmail.com

; <<>> DiG 9.6-ESV-R7-P2 <<>> @140.114.64.1 gmail.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 55121
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 4, ADDITIONAL: 4

;; QUESTION SECTION:
;gmail.com.                     IN      A

;; ANSWER SECTION:
gmail.com.              163     IN      A       173.194.72.83
gmail.com.              163     IN      A       173.194.72.17
gmail.com.              163     IN      A       173.194.72.18
gmail.com.              163     IN      A       173.194.72.19

;; AUTHORITY SECTION:
gmail.com.              43121   IN      NS      ns4.google.com.
gmail.com.              43121   IN      NS      ns2.google.com.
gmail.com.              43121   IN      NS      ns3.google.com.
gmail.com.              43121   IN      NS      ns1.google.com.

;; ADDITIONAL SECTION:
```

```
ns1.google.com.         9438    IN      A       216.239.32.10
ns2.google.com.         9438    IN      A       216.239.34.10
ns3.google.com.         170472  IN      A       216.239.36.10
ns4.google.com.         9438    IN      A       216.239.38.10

;; Query time: 2 msec
;; SERVER: 140.114.64.1#53(140.114.64.1)
;; WHEN: Tue Sep 24 11:35:07 2013
;; MSG SIZE  rcvd: 234
```

Caching-only DNS 伺服器

- 限用戶 IP 為 140.114.0.0/24 方可查詢的 DNS 伺服器其 named.conf 參考設定

```
acl nthu-nets { 140.114.0.0/24; };

options {
    // Working directory
    directory "/etc/namedb";

    allow-query { nthu-nets; };

    // Hidden version
    version none;
};

// Provide a reverse mapping for the loopback
// address 127.0.0.1
zone "0.0.127.in-addr.arpa" {
    type master;
    file "localhost.rev";
    notify no;
};
```

參考資料

BIND documentation