HP / January 17, 2020 09:06AM

DNS設定反查與偵錯：dig指令深入使用

一、目的

當DNS查詢出現錯誤無法解析出正確IP，經由以下方式，可以查出於整個DNS查詢路徑中，錯誤出在那一階段的DNS主機以及DNS記錄錯誤為何。

二、原理與流程

以下我們以查詢 www.ntu.edu.tw 之 IP 作為例子說明查詢的原理與流程。

1. 慣用DNS伺服器：作業系統之DNS查詢首先從詢問「慣用DNS伺服器」開始，一般我們會設定為 Google 的 DNS (8.8.8.8) 或者中華電信的 DNS (168.95.1.1) [1]。並且，可以由以下指令查詢：

```
$ cat /etc/resolv.conf
```

2. 決定查詢路徑：作業系統會從網域的「最後段」一路反向查詢到「最前段」。例如，以網域 www.ntu.edu.tw 為例，首先會查詢負責回應 tw 網域DNS記錄的主機為何，再接著查詢負責 edu 網域的主機，而後是負責 ntu 網域的主機。最後，再詢問負責 ntu 網域的主機，網域名稱 www 的主機 IP 為何。也就是查詢路徑為：

tw → edu → ntu → www

三、反查指令與步驟

1. DNS 的查詢 (反查) 以 dig 指令進行。首先，我們詢問「慣用DNS伺服器」(例如 8.8.8.8)：網域 tw 的「網域名稱解析主機」(Name Server, NS) 為何？查詢指令 dig 以接近直覺的格式達成上述目的：

```
$ dig @8.8.8.8 tw ns
```

其中，指令中的「ns」，指的是查詢種類 (type) 為「Name Server」。還可以查詢的種類包括 MX (電子郵件)、A (IPv4位置)、AAAA (IPv6位置)。查詢結果如下：

2. 由上面的結果我們可以看到，負責回應 tw 網域的主機共有11個 (c.dns.tw, a.dns.tw,..., anytld.apnic.net)。我們接著詢問第一個主機 (c.dns.tw) 網域 gov.tw 的負責主機為何：

```
$ dig @c.dns.tw gov.tw ns
```

首先我們可以看到負責 edu.tw 網域的名稱主機記錄有 d.twnic.net.tw 等5筆。接著，是上述名稱主機對應的 IP (IPv4 與 IPv6 / A Record 與 AAAA Record)。

3. 我們再接著詢問名稱主機 d.twnic.net.tw 網域ntu.edu.tw 的負責主機為何：

```
$ dig @d.twnic.net.tw edu.gov.tw ns
```

[1] 常用公共網域名稱解析主機
(1) Cloudflare 1.1.1.1
(2) Google 8.8.8.8
(3) IBM 9.9.9.9
(4) 中華電信 168.95.1.1 / 168.95.192.1

線上反查工具 (DNS Delegation)：

https://simpledns.plus/lookup-dg

Edited 1 time(s). Last edit at 01/17/2020 09:56AM by HP.