BIND 版本的查詢與設定

BIND (Berkeley Internet Name Domain) 為最常用來建置 DNS 伺服器的軟體之一，通常其預設安裝許可任何人查詢其版本資訊，**為了避免有心人士以版本資訊而找到軟體漏洞，進而方便發動攻擊，因此，強烈建議使用 BIND 的 DNS 伺服器管理者能適當隱藏版本資訊，以降低風險**。查詢指令及設定方法(可能因版本不同而異，請視情況參酌使用)詳下說明：

查詢 BIND 版本的指令

以下例子分別以 nslookup 與 dig 這個兩個指令來查詢 DNS 伺服器 140.114.XX.YY 其所使用的BIND版本, 本例中所查到的 BIND 版本為 9.3.2。

nslookup

```
# nslookup -debug -class=chaos -query=txt version.bind 140.114.XX.YY
Server:         140.114.XX.YY
Address:        140.114.XX.YY#53

------------
    QUESTIONS:
        version.bind, type = TXT, class = CH
    ANSWERS:
    ->  version.bind
        text = "9.3.2"
    AUTHORITY RECORDS:
    ->  version.bind
        nameserver = version.bind.
    ADDITIONAL RECORDS:
------------
version.bind    text = "9.3.2"
```

dig

```
# dig @140.114.XX.YY version.bind chaos txt

; <<>> DiG 9.2.4 <<>> @140.114.XX.YY version.bind chaos txt
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 862
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;version.bind.                  CH      TXT

;; ANSWER SECTION:
version.bind.           0       CH      TXT     "9.3.2"
```

```
;; AUTHORITY SECTION:
version.bind.           0       CH      NS      version.bind.

;; Query time: 1 msec
;; SERVER: 140.114.XX.YY#53(140.114.XX.YY)
;; WHEN: Wed Sep 23 09:49:52 2009
;; MSG SIZE  rcvd: 62
```

更換 BIND 版本顯示的設定

以下例子為更換 BIND 版本顯示文字改以 “ZZZ” 字串替代之(管理者可自行指定所要的文字)，其設定方法為修改 DNS 伺服器 140.114.XX.YY 的 named.conf 設定檔之 version 參數為 “ZZZ” (注意，此處有雙引號“ ”)，如下。

```
options {
   //(其他參數略...)
        version "ZZZ";
};
```

修改完上述設定並重新啟動 named 後，再以指令查詢結果，將看到版本資訊已被隱藏，如下結果。

```
# dig @140.114.XX.YY version.bind chaos txt

; <<>> DiG 9.2.4 <<>> @140.114.XX.YY version.bind chaos txt
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 81
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;version.bind.                  CH      TXT

;; ANSWER SECTION:
version.bind.           0       CH      TXT     "ZZZ"

;; AUTHORITY SECTION:
version.bind.           0       CH      NS      version.bind.

;; Query time: 1 msec
;; SERVER: 140.114.XX.YY#53(140.114.XX.YY)
;; WHEN: Wed Sep 23 10:21:27 2009
;; MSG SIZE  rcvd: 64
```

不回覆 BIND 版本的設定

以下例子為不回覆 BIND 版本回答，其設定方法為修改 DNS 伺服器 140.114.XX.YY 的 named.conf 設定檔之 version 參數為 none(注意，此處沒有雙引號“ ”)，如下。

```
options {
   //(其他參數略...)
        version none;
};
```

修改完上述設定並重新啟動 named 後，再以指令查詢結果，將看到不回覆版本資訊，如下結果。

```
# dig @140.114.XX.YY version.bind chaos txt

; <<>> DiG 9.3.4-P1 <<>> @140.114.XX.YY version.bind chaos txt
; (1 server found)
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 343
;; flags: qr aa rd; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;version.bind.                  CH      TXT

;; AUTHORITY SECTION:
version.bind.           86400   CH      SOA     version.bind.
hostmaster.version.bind. 0 28800 7200 604800 86400

;; Query time: 0 msec
;; SERVER: 140.114.XX.YY#53(140.114.XX.YY)
;; WHEN: Wed Sep 23 10:57:27 2009
;; MSG SIZE  rcvd: 77
```

參考資料

BIND documentation