BIND zone tranfer 的管制設定

Zone transfer 為 slave DNS 伺服器向其 master 取得 zone 註冊備份的管道，BIND (Berkeley Internet Name Domain) 為最常用來建置 DNS 伺服器的軟體之一，**為了避免管制設定不夠嚴密，讓有心人士輕易取得單位內完整的 DN 註冊清單，進而方便發動掃描式攻擊，因此，強烈建議 DNS 管理者限定伺服器僅許可其 slave 能執行 zone transfer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：

執行 zone transfer

以下例子分別以 dig 這個指令來取得 DNS 伺服器 140.114.XX.YY 其 zone xxxx.nthu.edu.tw 下的所有註冊資料。

dig

axfr (full zone transfer)

```
# dig @140.114.XX.YY xxxx.nthu.edu.tw -t axfr
; (1 server found)
;; global options:  printcmd
xxxx.nthu.edu.tw.       180     IN      A       140.114.XX.1
pc2.xxxx.nthu.edu.tw.   180     IN      A       140.114.XX.2
pc3.xxxx.nthu.edu.tw.   180     IN      A       140.114.XX.3
...
xxxx.nthu.edu.tw.       180     IN      SOA     xxxx.nthu.edu.tw.
dnsmaster.xxxx.nthu.edu.tw. 2009092801 10800 3600 604800 3600
;; Query time: 6 msec
;; SERVER: 140.114.XX.YY#53(140.114.XX.YY)
;; WHEN: Wed Nov  4 09:37:05 2009
;; XFR size: 261 records (messages 1)
```

ixfr (incremental zone transfer)

```
# dig @140.114.XX.YY xxxx.nthu.edu.tw -t ixfr=2009092801
; (1 server found)
;; global options:  printcmd
xxxx.nthu.edu.tw.       180     IN      SOA     xxxx.nthu.edu.tw.
dnsmaster.xxxx.nthu.edu.tw. 2009092801 10800 3600 604800 3600
;; Query time: 1 msec
;; SERVER: 140.114.XX.YY#53(140.114.XX.YY)
;; WHEN: Wed Nov  4 09:47:04 2009
;; XFR size: 1 records (messages 1)
```

BIND 的 zone transfer 設定

以下例子為設定 DNS 伺服器 140.114.XX.YY 的 named.conf 設定檔，讓其 slave 140.114.XX.ZZ 可執行 zone transfer。

- 設定 allow-transfer 參數，僅許可 IP 為 140.114.XX.ZZ 或 127.0.0.1 可執行 zone transfer 工作。
- notify yes 表當 master 註冊資料更新及 named reload 後，將主動通知 slave 更新。

```
options {
 //(其他參數略...)
   allow-transfer { 140.114.XX.ZZ; 127.0.0.1; };

   notify yes;
};
```

修改完上述設定並重新啟動 named 後，再以指令測試，若為許可 IP 將可取得資料；若非許可的 IP 將看到以下結果。

```
# dig @140.114.XX.YY xxxx.nthu.edu.tw axfr
; (1 server found)
;; global options:  printcmd
; Transfer failed.
```

參考資料

BIND documentation