TWISC@NCTU

交大資通安全研究與教學中心

DNSSEC Resolver建置SOP

版本： 1.0

目錄

1. 前言

在此份 SOP 中，我們將以 BIND 架設支援 DNSSEC 之 Resolver，並將建置及與測試之流程做一完整的說明。

2. 系統安裝建置

在此份 SOP 中，我們的系統環境如下：

- 作業系統：FreeBSD 8.2-RELEASE
- BIND 版本：9.8.1

2.1. 以 Ports Collection 安裝 BIND

BIND 9.8.1 位於 ports tree 中的 dns/bind98 下，我們先將目錄切換至 BIND 9.8.1 所在的位置：

```
# cd /usr/ports/dns/bind98
```

接著進行編譯前的設定：

```
# make config
```

這裡必須選取其：

- SSL：提供 DNSSEC 所必須之簽章簽署及驗證功能。
- REPLACE_BASE：取代 base system 中之舊版 BIND（在 FreeBSD 8.2 中是 BIND 9.6.x），使系統啟動服務時採用新版。
- SIGCHASE：使 dig 擁有 DNSSEC 的驗證功能，非必要功能但可協助除錯。

最後進行編譯及安裝

```
# make install clean
```

3. 系統設定

3.1. 將 BIND 設定為開機時自動啟動

以編輯器開啟 /etc/rc.conf 設定檔：

```
# vi /etc/rc.conf
```

於設定檔中加入

```
named_enable="YES"
```

BIND 即會於開機時自動啟動

3.2. 開啟 DNSSEC Resolver 功能

以編輯器開啟 /etc/namedb/named.conf 設定檔：

```
# vi /etc/ namedb/named.conf
```

於設定檔中加入

```
dnssec-enable yes;
dnssec-validation auto;
dnssec-lookaside auto;
```

即可開啟 BIND 的 DNSSEC Resolver 功能。其餘部分與一般 DNS Resolver 設定相同。

3.3. 後續維護說明

由前一節的兩項 auto 設定，BIND 會自行更新 DS 與 DLV 的公開金鑰，不需管理者再做管理，後續也無其他維護性作業。

4. 設定完成之後的驗證

完成 DNSSEC Resolver 的設定之後，可從外部查詢來驗證設定正確與否，驗證分為兩個部分

1) 能否正確解析純 DNS 網域
2) 能否正確解析 DNSSEC 網域

而除了解析的網域性質之外，client 的性質與 DNSSEC 信賴鏈的機制也會造成一些變化，需依如下兩節進行共六項測試與驗證。

以下測試可選擇任意的 Unix 作為 Client 以執行指令。建議測試不要在 Resolver 上執行，以確保測試的正確性。

4.1. 解析純 DNS 網域

一個 DNSSEC resolver，除了正常解析 DNSSEC 網域之外，對於 DNS 的處理也必須正確，以確保相容性。在這一小節裡，我們設定被查詢的網域為純 DNS 網域，不具備 DNSSEC 的能力。

我們查詢的標的為 www.ntu.edu.tw，目前已知僅支援 DNS 而不支援 DNSSEC 名稱解析，讀者可以任意相同性質網域取代。

我們使用的 client 端為 Linux，執行 dig 指令來測試。使用的 dig 版本必須為 BIND 9.7 以上。

解析純 DNS 網域，依 client 的不同做兩項測試

1) 以 DNS client 解析 DNS 網域
2) 以 DNSSEC client 解析 DNS 網域

以下為兩項測試採用的指令與細節：

1) 以 DNS client 解析 DNS 網域

任意選擇一台 Linux 的機器作為 client，使用以下指令

```
# dig www.ntu.edu.tw @myresolver
```

其中 myresolver 請替換為讀者自行架設好的 DNSSSEC resolver IP address。

得到類似以下回應則表示正確

```
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1238
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 1

;; QUESTION SECTION:
;www.ntu.edu.tw.                IN      A

;; ANSWER SECTION:
www.ntu.edu.tw.     75962     IN      A     140.112.8.116

.....
```

2) 以 DNSSEC client 解析 DNS 網域

任意選擇一台 Linux 的機器作為 client，使用以下指令

```
# dig +dnssec www.ntu.edu.tw @myresolver
```

其中 myresolver 請替換為讀者自行架設好的 DNSSSEC resolver IP address。

得到類似以下回應則表示正確

```
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1238
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 1

;; QUESTION SECTION:
;www.ntu.edu.tw.                IN      A

;; ANSWER SECTION:
www.ntu.edu.tw.     75962     IN      A     140.112.8.116

.....
```

4.2. 解析 DNSSEC 網域

本節測試解析 DNSSEC 網域，同時 DNS client 仍應該得到 DNS 回應，以確保相容性。

其中 DNSSEC 網域有 DS 信賴鏈與 DLV 信賴鏈兩種，兩種都必須能成功解析並驗證。前者我們使用 save.gov 為標的，後者以我們自己架設的 dns.dsnsx.cs.nctu.edu.tw 為標的，讀者可以任意相同性質網域取代。

解析 DNSSEC 網域分成四項測試

1) 以 DNS client 解析 DS 信賴鏈的 DNSSEC 網域
2) 以 DNS client 解析 DLV 信賴鏈的 DNSSEC 網域
3) 以 DNSSEC client 解析 DS 信賴鏈的 DNSSEC 網域
4) 以 DNSSEC client 解析 DLV 信賴鏈的 DNSSEC 網域

以下為四項測試採用的指令與細節：

1) 以 DNS client 解析 DS 信賴鏈的 DNSSEC 網域

任意選擇一台 Linux 的機器作為 client，使用以下指令

```
# dig save.gov @myresolver
```

其中 myresolver 請替換為讀者自行架設好的 DNSSSEC resolver IP address。

得到類似以下回應則表示正確

```
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 51205
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 6, ADDITIONAL: 2

;; QUESTION SECTION:
;save.gov.                      IN      A

;; ANSWER SECTION:
save.gov.               558     IN      A       198.137.240.104

.....
```

2) 以 DNS client 解析 DLV 信賴鏈的 DNSSEC 網域

任意選擇一台 Linux 的機器作為 client，使用以下指令

```
# dig dns.dsnsx.cs.nctu.edu.tw @myresolver
```

其中 myresolver 請替換為讀者自行架設好的 DNSSSEC resolver IP address。

得到類似以下回應則表示正確

```
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 42591
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;dns.dsnsx.cs.nctu.edu.tw.          IN          A

;; ANSWER SECTION:
dns.dsnsx.cs.nctu.edu.tw. 600      IN          A          140.113.87.22
.........
```

3) 以 DNSSEC client 解析 DS 信賴鏈的 DNSSEC 網域

任意選擇一台 Linux 的機器作為 client，使用以下指令

```
# dig +dnssec save.gov @myresolver
```

其中 myresolver 請替換為讀者自行架設好的 DNSSSEC resolver IP address。

得到類似以下回應則表示正確

```
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 903
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

.........
;; ANSWER SECTION:
save.gov.                  319        IN          A          198.137.240.104
save.gov.                  319        IN          RRSIG      A 7 2 600
20111103215642 20111031205642 26144 save.gov.
hJJ+ompsy1vQCe9XEdOKB/OH8NjSUvw0GkAcucKLlCX1q7Q6wJdVYKoS
K9yJGH9KC+wbIGXAG4pOMvV1Vu2bBG5Kj6F1dNWP7SXmQC3hrWLcikmh
w4OHsoY+hj8GmCyMtIYR/MAY5wyiL5Dt5JGAN2Op3H32tCyr5ksarJ7e 5f8=
.........
```

驗證重點在於，回應中 flags 的地方有 ad，表示 resolver 已驗證過簽章無誤，且有得到 RRSIG。隨著時間經過，使用的簽章會改變，因此讀者看到的 RRSIG 內容跟這裡看到的不見得會相同。

4) 以 DNSSEC client 解析 DLV 信賴鏈的 DNSSEC 網域

任意選擇一台 Linux 的機器作為 client，使用以下指令

```
# dig +dnssec dns.dsnsx.cs.nctu.edu.tw @myresolver
```

其中 myresolver 請替換為讀者自行架設好的 DNSSSEC resolver IP address。

得到類似以下回應則表示正確

```
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47310
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL: 1

……..
;; ANSWER SECTION:
dns.dsnsx.cs.nctu.edu.tw. 600     IN          A           140.113.87.22
dns.dsnsx.cs.nctu.edu.tw. 600     IN          RRSIG     A 7 6 600
20111127081401 20111028074041 57707 dsnsx.cs.nctu.edu.tw.
Mk2rYZLsRJNDjD8E3JzJVDbEsLUmZ6YQ9JI1DyKA5mnmX3oW36ru5ldz
ietD+IDhGpR0bKwAatJ2xPHz4sJqqiOBpdGUiyaf2HXdG/SVMmMSZq9c
0s78d5Qq9JtsXsFovratbimWt+N7wjeg1t2rWXsJ9Vxpm/0Idh2Ih03t gsM=
.....
```

驗證重點在於，回應中 flags 的地方有 ad，表示 resolver 已驗證過簽章無誤，且有得到 RRSIG。隨著時間經過，使用的簽章會改變，因此讀者看到的 RRSIG 內容跟這裡看到的不見得會相同。

5. 結語

本文中詳細描述了 DNSSEC Resolver 建置的流程，以及建置完成後的驗證方法。若讀者皆執行且驗證無誤，即順利完成建置。