Network Administration/System Administration Homework #5

B10202012 劉仲楷

1 Setting up PowerDNS

ref:

- Running PowerDNS and PowerDNS Admin in Docker Containers
- PowerDNS-Admin Issues#816 (Thanks to DC @我是一棵樹)
- Claude chat transcript

1. 參考連結的 `docker-compose.yml` 設定檔，稍微修改後得出附件的設定檔。到路徑下後執行

   ```
   docker compose up -d db
   docker compose exec -T db mysql < ./schema.mysql.sql
   docker compose up -d
   ```

   要注意第二步需要等一下再執行。下圖為 `dig` 結果。

   ```
   joshua@joshua-Aspire-A514-55:~/ctf$ dig @0.0.0.0 -p 5301

   ; <<>> DiG 9.18.30-0ubuntu0.24.04.2-Ubuntu <<>> @0.0.0.0 -p 5301
   ; (1 server found)
   ;; global options: +cmd
   ;; Got answer:
   ;; ->>HEADER<<- opcode: QUERY, status: REFUSED, id: 56352
   ;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1
   ;; WARNING: recursion requested but not available

   ;; OPT PSEUDOSECTION:
   ; EDNS: version: 0, flags:; udp: 1232
   ;; QUESTION SECTION:
   ;.                              IN      NS

   ;; Query time: 0 msec
   ;; SERVER: 0.0.0.0#5301(0.0.0.0) (UDP)
   ;; WHEN: Fri Oct 10 23:56:41 CST 2025
   ;; MSG SIZE  rcvd: 28
   ```

   要得到 control version 則需要執行

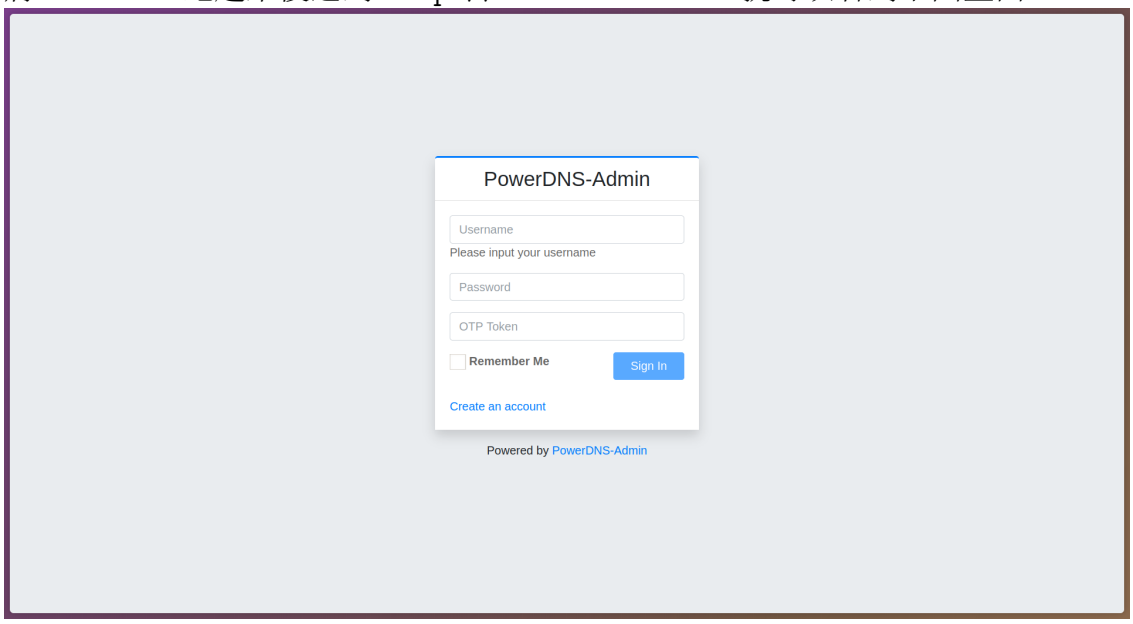
   ```
   docker compose exec pdns bash
   ```

   並在 pdns 內執行

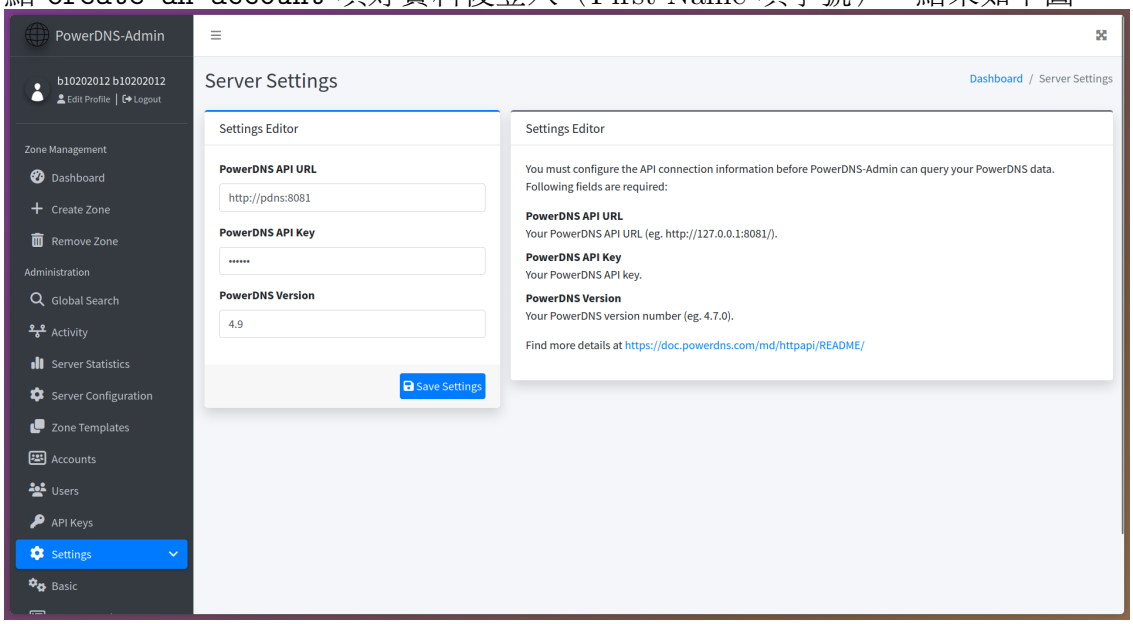
   ```
   pdns_control version
   ```

   ```
   pdns@pdns:/$ pdns_control version
   4.9.9
   ```

2. 將 container 跑起來後連到 `http://localhost:9191` 就可以看到下圖畫面



點 `Create an account` 填好資料後登入（First Name 填學號）。結果如下圖。



3. 左邊選單點選 `Create Zone`，Zone Name 填 `cscat.tw`，其他不改，滑動到最底下點 `Create Zone`，接點選 `Actions` 欄位下選單，點擊 `Edit records`。接下來要利用右上角 `+ Add Record` 新增以下內容後，點 `Save`，最後點 `Save Changes`。

Name	Type	Status	TTL	Data	Comment	Actions
@	TXT	Active	60	"v=spf1 mx -all"		
@	MX	Active	60	10 mail.cscat.tw.		
@	NS	Active	60	ns1.cscat.tw.		
@	A	Active	60	192.0.1.1		
api	AAAA	Active	60	2001:db8::50		
api	A	Active	60	192.0.1.4		
mail	A	Active	60	192.0.1.7		
market	CNAME	Active	60	cscat.tw.		
ns1	A	Active	60	192.0.1.53		
store2	NS	Active	60	ns.store2.cscat.tw.		
ns.store2	A	Active	60	192.2.0.53		

Showing 1 to 11 of 11 entries

Previous 1 Next

結果如下（將部分搜尋結果合併）

```
joshua@joshua-Aspire-A514-55:~/nasa/hw5$ dig @localhost -p 5301 market.cscat.tw -t any

; <<>> DiG 9.18.30-0ubuntu0.24.04.2-Ubuntu <<>> @localhost -p 5301 market.cscat.tw -t any
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 63415
;; flags: qr aa rd; QUERY: 1, ANSWER: 6, AUTHORITY: 0, ADDITIONAL: 3
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;market.cscat.tw.               IN      ANY

;; ANSWER SECTION:
market.cscat.tw.        60      IN      CNAME   cscat.tw.
cscat.tw.               60      IN      A       192.0.1.1
cscat.tw.               60      IN      MX      10 mail.cscat.tw.
cscat.tw.               60      IN      NS      ns1.cscat.tw.
cscat.tw.               60      IN      TXT     "v=spf1 mx -all"
cscat.tw.               3600    IN      SOA     a.misconfigured.dns.server.invalid. hostmaster.cscat.tw. 2025101902 10800 3600 604800 3600

;; ADDITIONAL SECTION:
ns1.cscat.tw.           60      IN      A       192.0.1.53
mail.cscat.tw.          60      IN      A       192.0.1.7

;; Query time: 2 msec
;; SERVER: 127.0.0.1#5301(localhost) (TCP)
;; WHEN: Sun Oct 19 18:01:01 CST 2025
;; MSG SIZE  rcvd: 253
```

```
joshua@joshua-Aspire-A514-55:~/nasa/hw5$ dig @localhost -p 5301 store2.cscat.tw -t any

; <<>> DiG 9.18.30-0ubuntu0.24.04.2-Ubuntu <<>> @localhost -p 5301 store2.cscat.tw -t any
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 29344
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 2
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;store2.cscat.tw.               IN      ANY

;; AUTHORITY SECTION:
store2.cscat.tw.        60      IN      NS      ns.store2.cscat.tw.

;; ADDITIONAL SECTION:
ns.store2.cscat.tw.     60      IN      A       192.2.0.53

;; Query time: 1 msec
;; SERVER: 127.0.0.1#5301(localhost) (TCP)
;; WHEN: Sun Oct 19 18:02:03 CST 2025
;; MSG SIZE  rcvd: 77
```

```
joshua@joshua-Aspire-A514-55:~/nasa/hw5$ dig @localhost -p 5301 api.cscat.tw -t any

; <<>> DiG 9.18.30-0ubuntu0.24.04.2-Ubuntu <<>> @localhost -p 5301 api.cscat.tw -t any
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 12568
;; flags: qr aa rd; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;api.cscat.tw.                  IN      ANY

;; ANSWER SECTION:
api.cscat.tw.           60      IN      A       192.0.1.4
api.cscat.tw.           60      IN      AAAA    2001:db8::50

;; Query time: 0 msec
;; SERVER: 127.0.0.1#5301(localhost) (TCP)
;; WHEN: Sun Oct 19 18:02:40 CST 2025
;; MSG SIZE  rcvd: 85
```

4. DNSSEC 會對 DNS 記錄數位簽章，一起儲存在 server 上。這個簽章可以防止 DNS spoofing 或 DNS cache poisoning。開啓步驟：左邊選單點擊 `Dashboard`，點擊 `DNSSEC` 欄位下的鎖頭，點擊 `Enable`。要注意到 `pdns.conf` 裡要加入一行 `gmysql-dnssec=yes`，並重啓 docker，但最剛開始已經寫好了，所以可以忽略這一步。`dig` 截圖：

```
joshua@joshua-Aspire-A514-55:~/nasa/hw5$ dig @localhost -p 5301 cscat.tw -t DNSKEY

; <<>> DiG 9.18.30-0ubuntu0.24.04.2-Ubuntu <<>> @localhost -p 5301 cscat.tw -t DNSKEY
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 48730
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;cscat.tw.                      IN      DNSKEY

;; ANSWER SECTION:
cscat.tw.               3600    IN      DNSKEY  257 3 13 DpXfdwZ+ZZWA3d/4XULKKUeHZXczlXmTd8zDV8u0iKThjSnvtJBgCIcc m3lT4wcv+RtPLBq0aCDXHSnqa8gmjQ==

;; Query time: 0 msec
;; SERVER: 127.0.0.1#5301(localhost) (UDP)
;; WHEN: Mon Oct 20 00:31:55 CST 2025
;; MSG SIZE  rcvd: 117
```

2 PowerDNS Recursor

2.0 Basic

ref: What is an Iterative DNS Query?

1. 一個 authoritive server 會存放自己管轄 domain 的資料，並回覆關於此 domain 的問題。

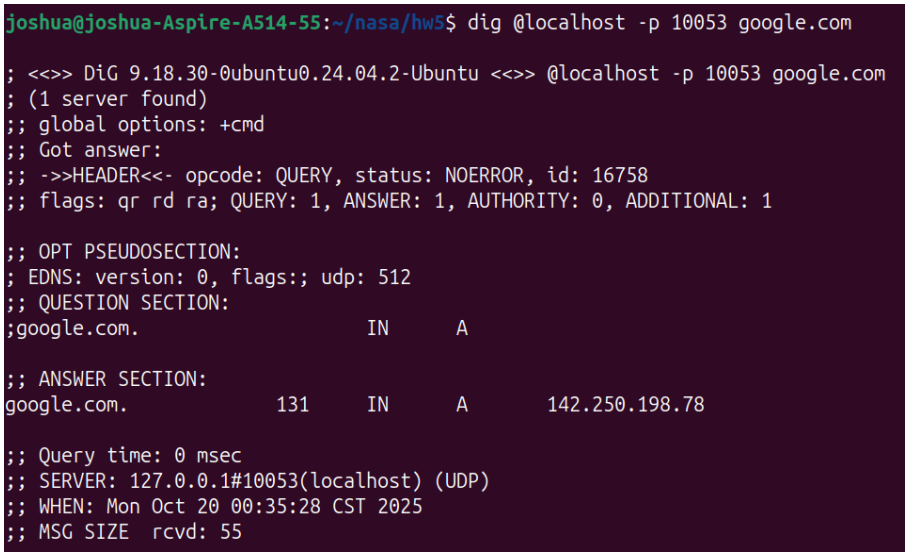
2. Recursive DNS query 的狀況是如果遇到不知道的，會幫 client 問下一層，直到找到答案，再回覆回來。Iterative DNS query 則是告訴 client 答案，或是應該要找哪個 name server。如果不是答案，client 就要再發送一個 request 給新的 name server，重覆這個步驟。

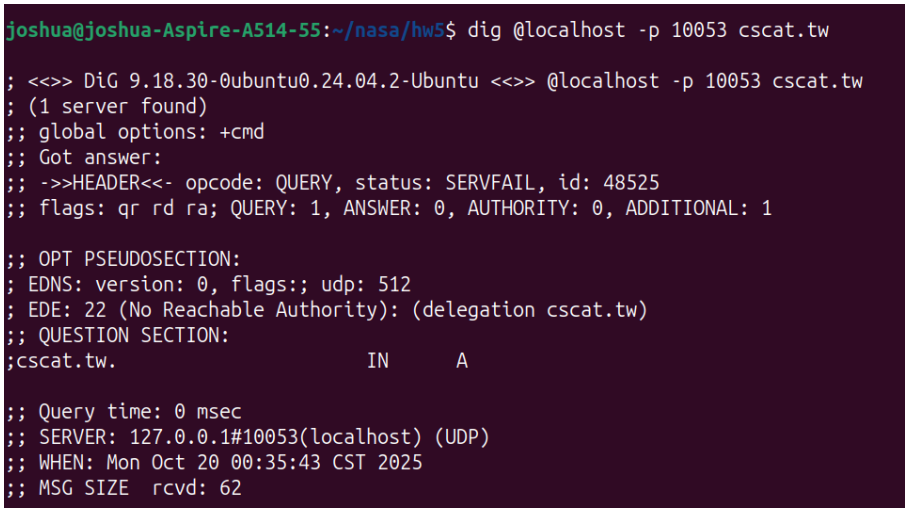
2.1 Setting up PowerDNS Recursor

1. 同樣在 `docker-compose.yml` 和 `recursor.conf`已經有設定好了，所以不需要再做其他步驟。需要注意的是，看 recursor 的 log 可以發現他讀的 config 是 yml 的形式，可以透過

   `rec_control show-yaml`

   轉換 ref: PowerDNS documentation。

2. 

3. 

   Fail 的原因是 `cscat.tw` 的 DNSSEC 沒有被上層 `tw` 認證。

4. ref: PowerDNS documentation
   需要在 `recursor.conf` 裡加一行 `allow_trust_anchor_query: yes`，並在 `dnssec` field 加 trustanchors 的名字（cscat.tw）和 ds record。利用

   `docker compose exec pdns pdnsutil show-zone cscat.tw`

   查詢。(如下圖就是加兩行 `52302...mjQ==`、`52302...68c0f`

此時，執行

```
dig trustanchor.server CH TXT @localhost -p 10053
```

可以看到 trustanchors 確實有被加入。但不知道為什麼 dig cscat.tw 還是失敗。我嘗試把 dnssec 關掉，但還是 dig 不出來，所以應該是連線問題。

```
joshua@joshua-Aspire-A514-55:~/nasa/hw5$ dig trustanchor.server CH TXT @localhost -p 10053

; <<>> DiG 9.18.30-0ubuntu0.24.04.2-Ubuntu <<>> trustanchor.server CH TXT @localhost -p 10053
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 28477
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;trustanchor.server.            CH      TXT

;; ANSWER SECTION:
trustanchor.server.     86400   CH      TXT     ". 20326 38696"
trustanchor.server.     86400   CH      TXT     "cscat.tw. 52302 52302"

;; Query time: 0 msec
;; SERVER: 127.0.0.1#10053(localhost) (UDP)
;; WHEN: Mon Oct 20 00:54:55 CST 2025
;; MSG SIZE  rcvd: 107
```

5. TTL 過高會導致 client 在 IP 更新後仍然得到舊的 IP；過低則會導致伺服器要一直查詢，導致負擔過重。如果外部連線不佳，則會導致內部也有這個狀況。

6. 攻擊者在伺服器收到用戶（可以是攻擊者為裝的）查詢時，大量發送假回覆封包，企圖欺騙伺服器解析結果。這時伺服器會 cache 結果，下一個用戶再查詢相同 zone 時，就會查詢到錯誤結果，最終導流到攻擊者的陷阱，進而竊聽或執行 MitM attack。

2.2 Security

1. 若允許任何外部 IP，攻擊者可利用此伺服器進行 DNS 反射放大攻擊（DNS Amplification Attack）。攻擊者透過偽造來源 IP（受害者的 IP）發送大量查詢給開放 DNS。DNS 伺服器回傳的封包比請求大很多，導致受害者被大量封包淹沒。這會伺服器成為 DDoS 攻擊的幫兇，同時也消耗自己的頻寬與資源。

2. 將 `recursor.conf` 加入類似 `allow-from=127.0.0.1,192.168.56.0/24` 參數即可。

3 Master and Slave

1. PowerDNS Authorative、MariaDB、PowerDNS Admin、Recursor、dnsdist 架在系上。此外，複製一份 PowerDNS Authorative、MariaDB、Recursor 到計中，當作備用服務，平常也可以導一些流量，但主要以系上為主。最後，複製一份 DB 到雲端上，也假設監控服務在雲端上，執行健康檢查。必要的時候（如系上 dnsdist 下線）可將 dnsdist 暫時架在雲上。可以視情況、流量需求，在系上增加一臺 Recursor。

- 每臺伺服器都有備用服務，當有伺服器下線可以利用 dnsdist 將流量導至備用服務。直到恢復供應服務，再將那臺伺服器加入 pool。如果是 master 下線，就將一臺 slave 提升至 master。
- 除了系館，計中和雲端上的服務足夠暫時維持基本需求。但如果流量過大，會導致延遲增加。此外，如果各伺服器 sync 不是非常即時，由於 master 是系館的，其他地方可能會損失一些資料，或導致一些連線錯誤。
- 如果不見的是 master 的 DB，那就只能利用上次備份在雲端或計中的資料恢復，可能會損失一些資料。但太頻繁 sync 則會增加太多 overload，反而導致效能降低。所以看能接受多大 trade-off。

2. ref: Cloudflare: DNS Zone transfers
   AXFR 是傳從整個 zone，而 IXFR 只傳送距離上次傳送中間的增量。當第一次 sync 、中間下線或太久沒 sync 有 conflict 等時候，可以使用 AXFR。但日常使用 IXFR 即可，這樣可以減少流量，降低負載。