# NASA HW5

B11901164 陳秉緯

討論：R13941146 李毓庭, B12901194 賴睿廷

## 1 Setting up PowerDNS

1. ref: 1, 2, 3
   步驟：

   1. 到此下載 Debian 12 ISO
   2. 開新的VM，Name: Debian，Memory: 4096 KB, Hard Disk: 20 GB
   3. 設定好後點擊兩下打開
   4. 選 vboxuser，密碼預設 changeme 登入
   5. 為了讓 vboxuser 有 root 權限：
      - `su -` 換到 root user，password一樣是changeme
      - `usermod -aG sudo vboxuser` 把 vboxuser 加到 sudo group 內
      - `su - vboxuser` 讓變更生效
   6. `sudo apt update` 更新系統套件
   7. `sudo apt install mariadb-server -y` 安裝 MariaDB
   8. 啟動並設定 MariaDB:

      ```
      sudo systemctl start mariadb
      sudo systemctl enable mariadb
      sudo mysql_secure_installation
      ```

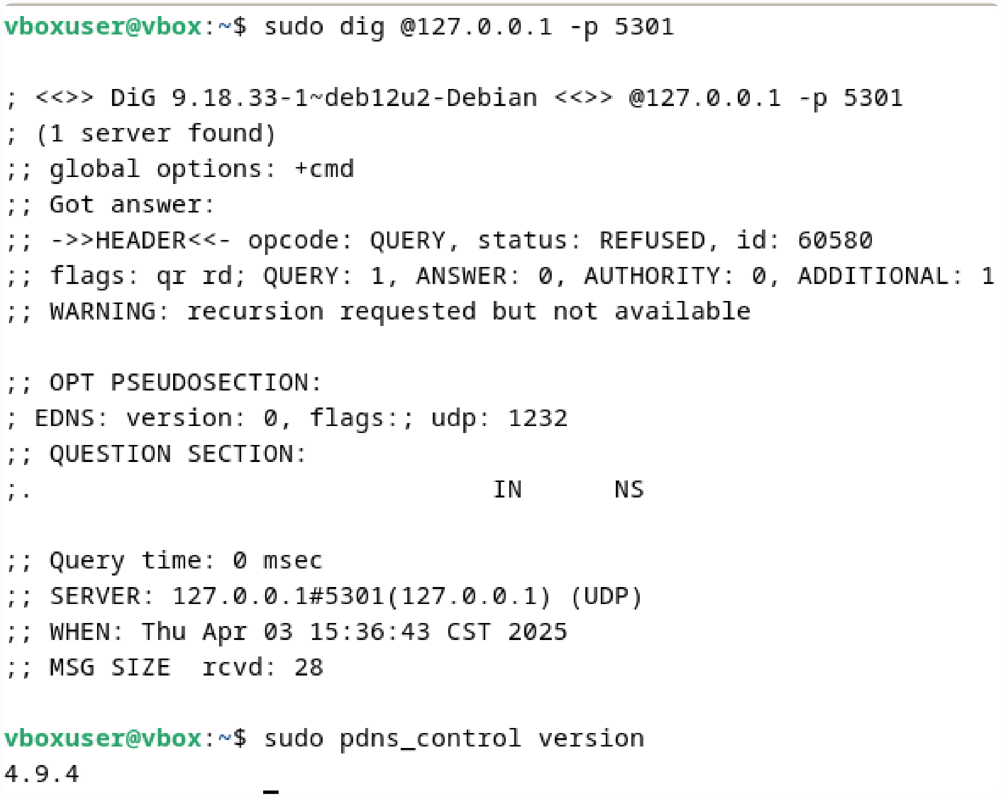
   9. 建立 PowerDNS 資料庫和使用者：
      - `sudo mysql -u root -p` 進入 MariaDB
      - 在 MariaDB 提示符下執行：

        ```
        CREATE DATABASE powerdns;
        GRANT ALL PRIVILEGES ON `powerdns`.* TO 'b11901164'@'localhost' IDENTI
        FLUSH PRIVILEGES;
        exit
        ```

   10. `sudo apt install pdns-server pdns-backend-mysql -y` 安裝 PowerDNS 及其 MySQL 後端
   11. 在 `/etc/powerdns/pdns.conf` 加入：

```
api=yes
api-key=YOUR_SECRET_API_KEY
webserver=yes
webserver-address=0.0.0.0
webserver-port=8081

launch=gmysql
gmysql-host=127.0.0.1
gmysql-user=b11901164
gmysql-password=nasa
gmysql-dbname=powerdns
local-port=5301
```

12. `sudo mysql -u root powerdns < /usr/share/pdns-backend-mysql/schema/schema.mysql.sql` 匯入 PowerDNS schema
13. `sudo systemctl restart pdns` 重啟 pdns
14. 截圖：



```
vboxuser@vbox:~$ sudo dig @127.0.0.1 -p 5301

; <<>> DiG 9.18.33-1~deb12u2-Debian <<>> @127.0.0.1 -p 5301
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: REFUSED, id: 60580
;; 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: 127.0.0.1#5301(127.0.0.1) (UDP)
;; WHEN: Thu Apr 03 15:36:43 CST 2025
;; MSG SIZE  rcvd: 28

vboxuser@vbox:~$ sudo pdns_control version
4.9.4
```

2. ref: 1, 2, 3

   步驟：

   1. `sudo apt install python3-dev git libsasl2-dev libldap2-dev python3-venv libmariadb-dev pkg-config build-essential curl libpq-dev libxmlsec1 libxmlsec1-dev vim npm -y` 安裝套件
   2. 安裝Nodejs：

   ```
   curl -sL https://deb.nodesource.com/setup_14.x | sudo bash -
   sudo apt install -y nodejs
   ```

3. 安裝yarn：

```
curl -sL https://dl.yarnpkg.com/debian/pubkey.gpg | gpg --dearmor | sudo
echo "deb [signed-by=/usr/share/keyrings/yarnkey.gpg] https://dl.yarnpkg.
sudo apt update && sudo apt install -y yarn
```

4. clone PowerDNS-Admin 的 github repo:

```
sudo mkdir /opt/web
sudo git clone https://github.com/PowerDNS-Admin/PowerDNS-Admin.git /opt/
sudo chown -R $USER:$USER /opt/web/powerdns-admin
cd /opt/web/powerdns-admin
python3 -mvenv ./venv
```

5. 設置環境：

```
source ./venv/bin/activate
pip install --upgrade pip
pip install -r requirements.txt
```

6. 建立設定檔：

```
cp /opt/web/powerdns-admin/configs/development.py /opt/web/powerdns-admin
vim /opt/web/powerdns-admin/configs/production.py
```

7. 改成以下：

```
SQLA_DB_USER = 'b11901164'
SQLA_DB_PASSWORD = 'nasa'
SQLA_DB_NAME = 'powerdns'
```

   再把以下註解拿掉：

```
# import urllib.parse

#SQLALCHEMY_DATABASE_URI = 'mysql://{}:{}@{}/{}'.format(
#urllib.parse.quote_plus(SQLA_DB_USER),
#urllib.parse.quote_plus(SQLA_DB_PASSWORD),
#    SQLA_DB_HOST,
#    SQLA_DB_NAME
#)
```

   並且註解掉：`SQLALCHEMY_DATABASE_URI = 'sqlite:///' + os.path.join(basedir, 'pdns.db')`

   好了之後 `:wq` 儲存並退出

   最後 `export FLASK_CONF=../configs/production.py`

8. DB migration：

```
export FLASK_APP=powerdnsadmin/__init__.py
```

```
flask db upgrade
```

9. generate asset files：

```
yarn install --pure-lockfile
flask assets build
```

10. `./run.py` 跑起來 並在瀏覽器打開 `http://127.0.0.1:9191`

11. 註冊帳號

12. 填寫 api key:

    - api url: http://127.0.0.1:8081
    - api key: YOUR_SECRET_API_KEY
    - version: 4.9.4

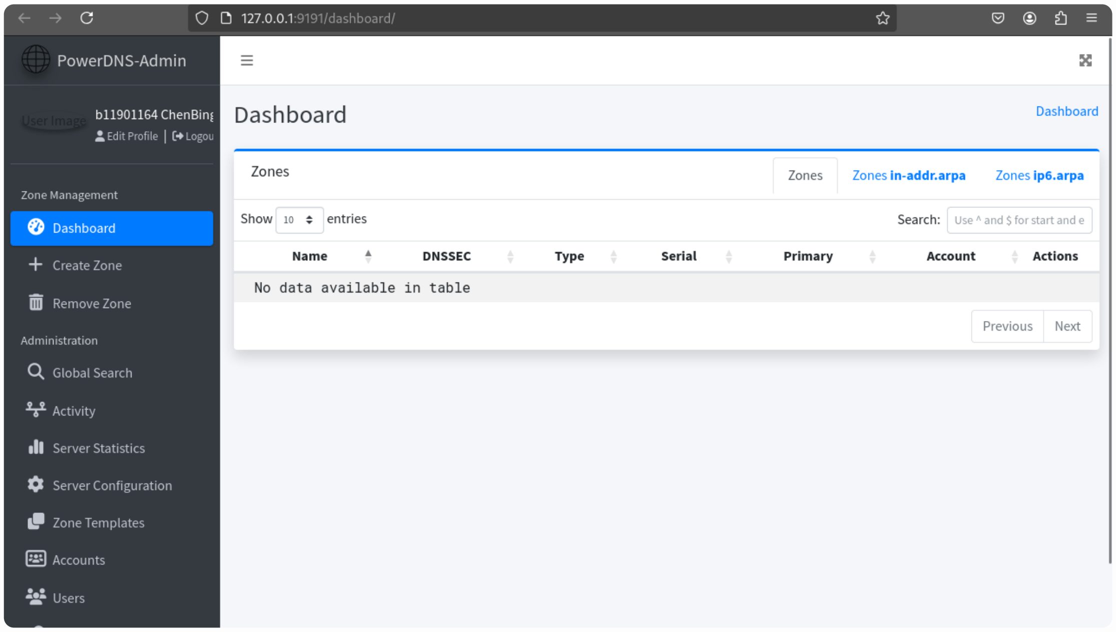
13. 如果點送出出現 403 error：

    - `sudo mysql -u root powerdns` 進去 db `DROP TABLE sessions;` 把 sessions table 砍掉
    - `sudo vim powerdnsadmin/routes/user.py` 把以下註解掉：

    ```
    # Clean up expired sessions in the database
    if Setting().get('session_type') == 'sqlalchemy':
       from ..models.sessions import Sessions
      Sessions().clean_up_expired_sessions()
    ```

    - `sudo systemctl restart mariadb pdns powerdns`
    - 再從 7. 開始做應該就會成功了

14. 截圖：



| Name | DNSSEC | Type | Serial | Primary | Account | Actions |
|---|---|---|---|---|---|---|
| No data available in table | | | | | | |

3. ref: 1

   步驟：

   1. Configure systemd service

      - `sudo vim /etc/systemd/system/powerdns-admin.service`

        ```
        [Unit]
        Description=PowerDNS-Admin
        Requires=powerdns-admin.socket
        After=network.target

        [Service]
        PIDFile=/run/powerdns-admin/pid
        User=pdns
        Group=pdns
        WorkingDirectory=/opt/web/powerdns-admin
        ExecStartPre=+mkdir -p /run/powerdns-admin/
        ExecStartPre=+chown pdns:pdns -R /run/powerdns-admin/
        ExecStart=/opt/web/powerdns-admin/venv/bin/gunicorn --pid /run/powerd
        ExecReload=/bin/kill -s HUP $MAINPID
        ExecStop=/bin/kill -s TERM $MAINPID
        PrivateTmp=true

        [Install]
        WantedBy=multi-user.target
        ```

      - `sudo systemctl edit powerdns-admin.service`

        ```
        [Service]
        Environment="FLASK_CONF=../configs/production.py"
        ```

      - `sudo vim /etc/systemd/system/powerdns-admin.socket`

        ```
        [Unit]
        Description=PowerDNS-Admin socket

        [Socket]
        ListenStream=/run/powerdns-admin/socket

        [Install]
        WantedBy=sockets.target
        ```

      - `sudo vim /etc/tmpfiles.d/powerdns-admin.conf`

        ```
        d /run/powerdns-admin 0755 pdns pdns -
        ```

      - 修改權限：

        ```
        sudo chown -R pdns:pdns /run/powerdns-admin
        sudo chown -R pdns:pdns /opt/web/powerdns-admin
        ```

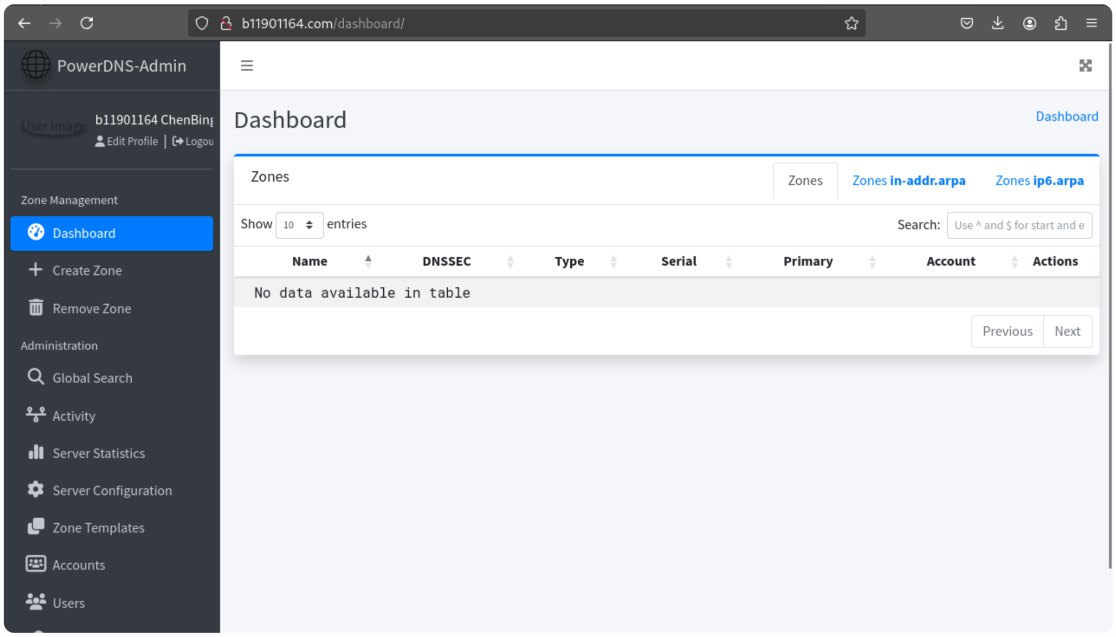
- `sudo systemctl daemon-reload; sudo systemctl start powerdns-admin.socket; sudo systemctl enable powerdns-admin.socket` to start the Powerdns-Admin service and make it run on boot

2. `sudo apt install nginx -y` 安裝套件
3. `sudo vim /etc/nginx/conf.d/powerdns-admin.conf` 加入：

```
server {
  listen *:80;
  server_name               b11901164.com;

  index                     index.html index.htm index.php;
  root                      /opt/web/powerdns-admin;
  access_log                /var/log/nginx/powerdns-admin.local.access.lo
  error_log                 /var/log/nginx/powerdns-admin.local.error.log

  client_max_body_size              10m;
  client_body_buffer_size           128k;
  proxy_redirect                    off;
  proxy_connect_timeout             90;
  proxy_send_timeout                90;
  proxy_read_timeout                90;
  proxy_buffers                     32 4k;
  proxy_buffer_size                 8k;
  proxy_set_header                  Host $host;
  proxy_set_header                  X-Real-IP $remote_addr;
  proxy_set_header                  X-Forwarded-For $proxy_add_x_forwarde
  proxy_headers_hash_bucket_size    64;

  location ~ ^/static/  {
    include  /etc/nginx/mime.types;
    root /opt/web/powerdns-admin/powerdnsadmin;

    location ~*  \.(jpg|jpeg|png|gif)$ {
      expires 365d;
    }

    location ~* ^.+.(css|js)$ {
      expires 7d;
    }
  }

  location / {
    proxy_pass            http://unix:/run/powerdns-admin/socket;
    proxy_read_timeout    120;
    proxy_connect_timeout 120;
    proxy_redirect        off;
  }

}
```

4. `sudo systemctl restart nginx` 重啟 nginx

5. 在瀏覽器打開 b11901164.com 並登入後截圖:



b11901164.com/dashboard/

Dashboard

Zones

Zones | Zones **in-addr.arpa** | Zones **ip6.arpa**

Show 10 entries

Search: Use ^ and $ for start and e

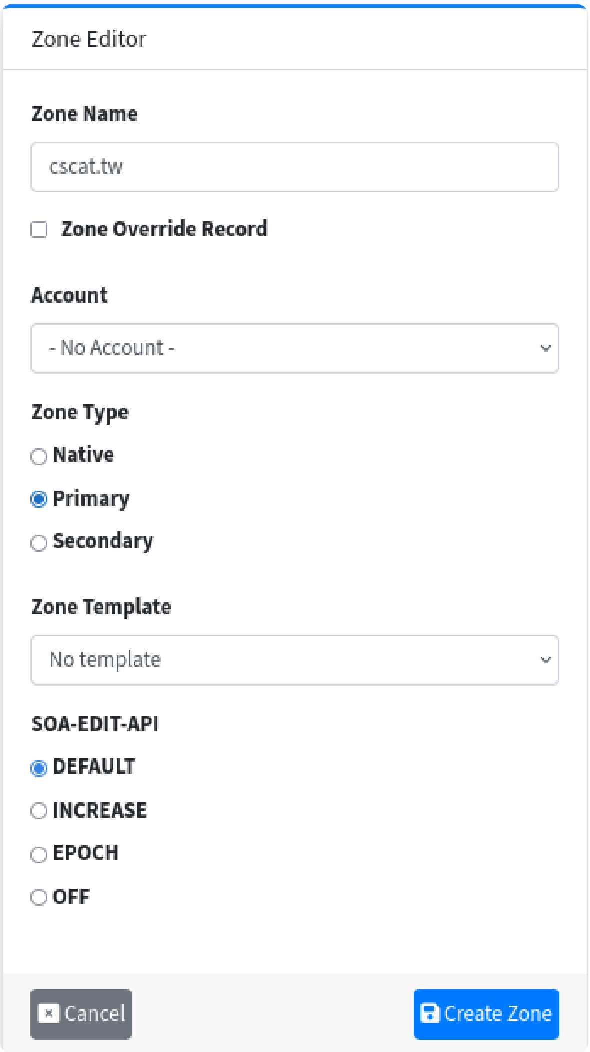
| Name | DNSSEC | Type | Serial | Primary | Account | Actions |
|---|---|---|---|---|---|---|
| No data available in table | | | | | | |

Previous Next

4. ref: 1

步驟：

1. 點左側欄位 Create Zone 並填寫以下資訊新增 cscat.tw 的 zone：



Zone Editor

**Zone Name**

cscat.tw

☐ **Zone Override Record**

**Account**

- No Account -

**Zone Type**

○ Native
● Primary
○ Secondary

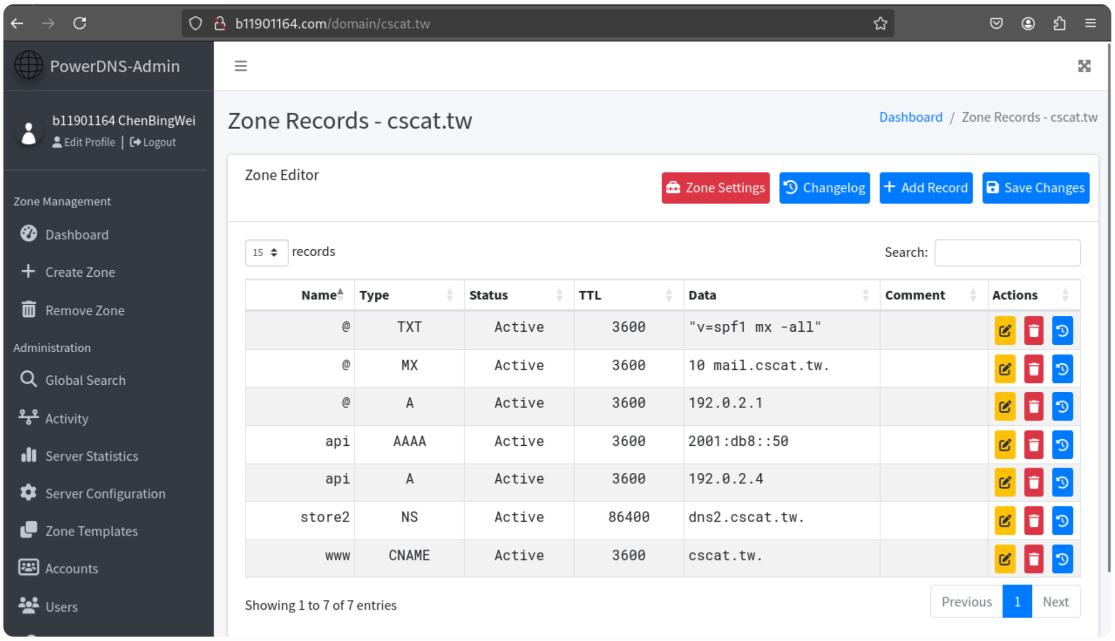
**Zone Template**

No template

**SOA-EDIT-API**

● DEFAULT
○ INCREASE
○ EPOCH
○ OFF

2. 依題目要求新增 Records，以下為截圖：



b11901164.com/domain/cscat.tw

Zone Records - cscat.tw

Dashboard / Zone Records - cscat.tw

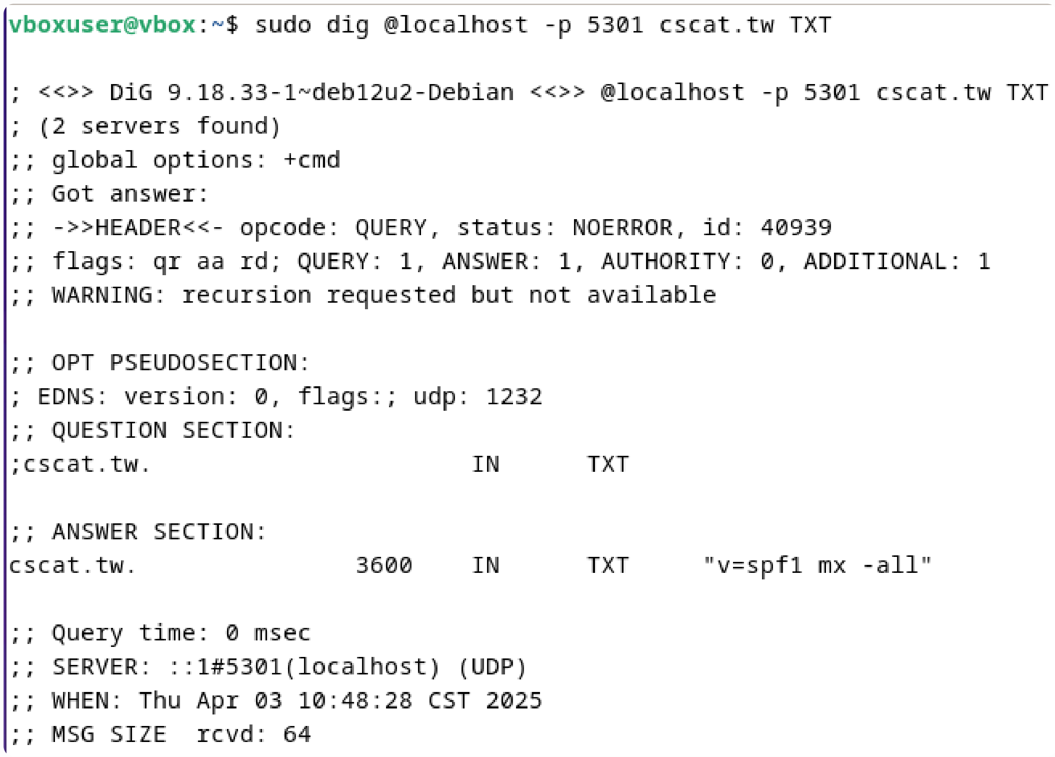
Zone Editor

15 records    Search:

| Name | Type | Status | TTL | Data | Comment | Actions |
|---|---|---|---|---|---|---|
| @ | TXT | Active | 3600 | "v=spf1 mx -all" | | |
| @ | MX | Active | 3600 | 10 mail.cscat.tw. | | |
| @ | A | Active | 3600 | 192.0.2.1 | | |
| api | AAAA | Active | 3600 | 2001:db8::50 | | |
| api | A | Active | 3600 | 192.0.2.4 | | |
| store2 | NS | Active | 86400 | dns2.cscat.tw. | | |
| www | CNAME | Active | 3600 | cscat.tw. | | |

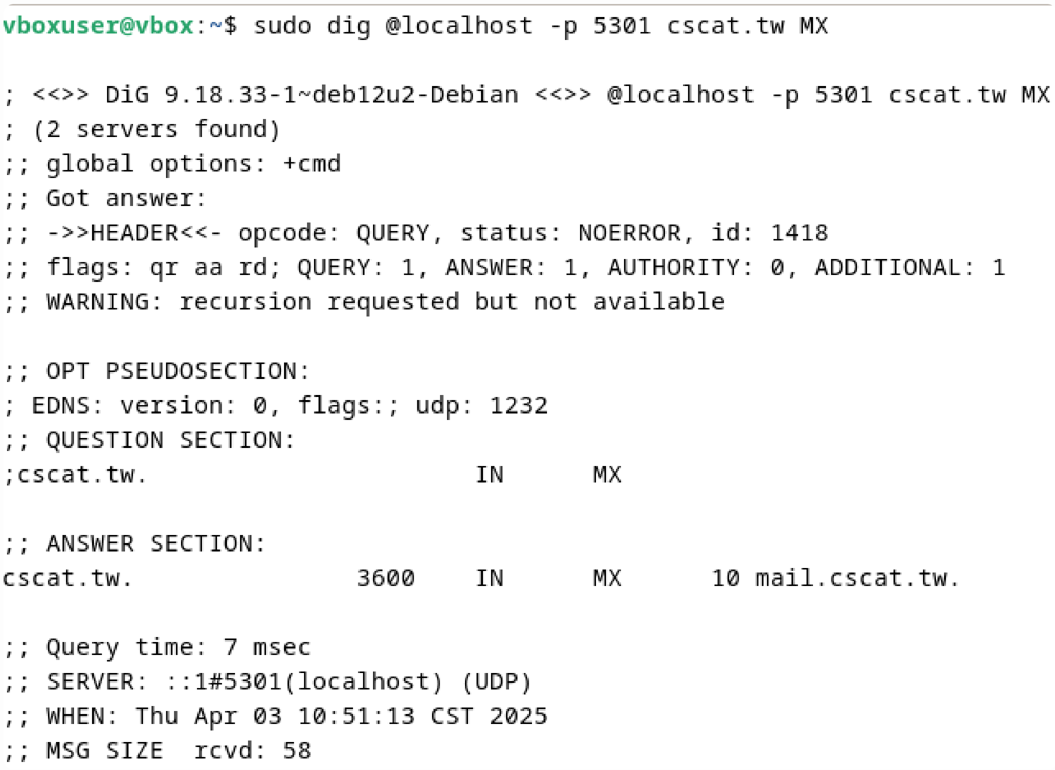
Showing 1 to 7 of 7 entries

- `sudo dig @localhost -p 5301 cscat.tw TXT`



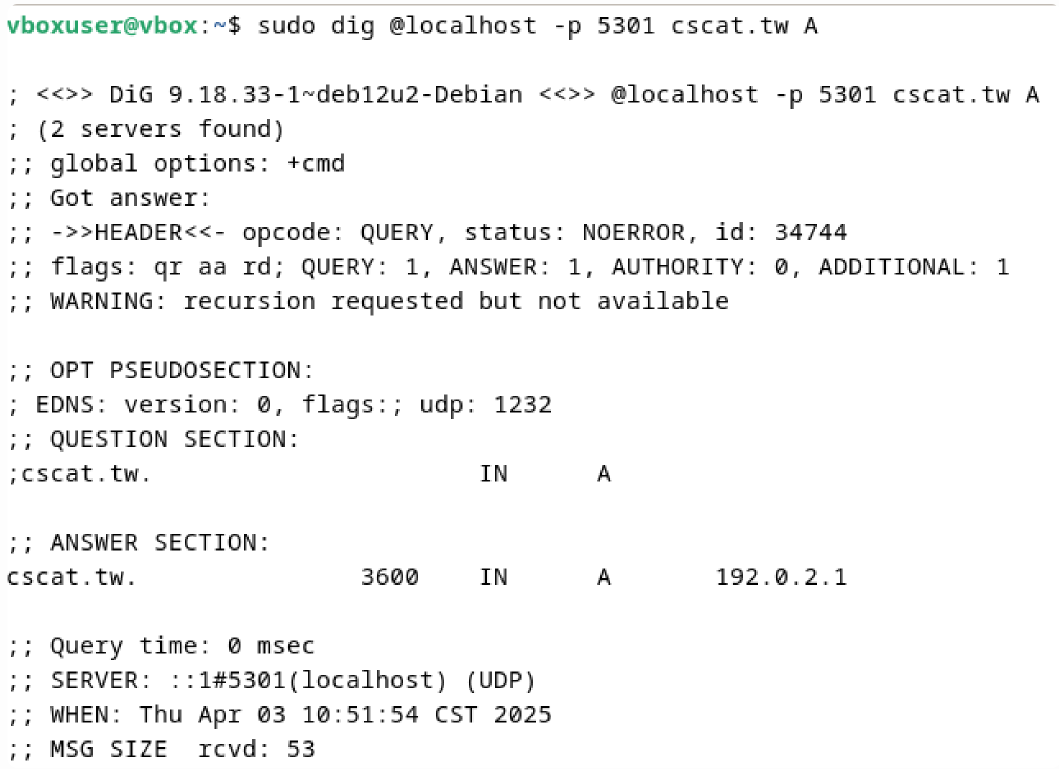
```
vboxuser@vbox:~$ sudo dig @localhost -p 5301 cscat.tw TXT

; <<>> DiG 9.18.33-1~deb12u2-Debian <<>> @localhost -p 5301 cscat.tw TXT
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 40939
;; 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      TXT

;; ANSWER SECTION:
cscat.tw.               3600    IN      TXT     "v=spf1 mx -all"

;; Query time: 0 msec
;; SERVER: ::1#5301(localhost) (UDP)
;; WHEN: Thu Apr 03 10:48:28 CST 2025
;; MSG SIZE  rcvd: 64
```

- `sudo dig @localhost -p 5301 cscat.tw MX`



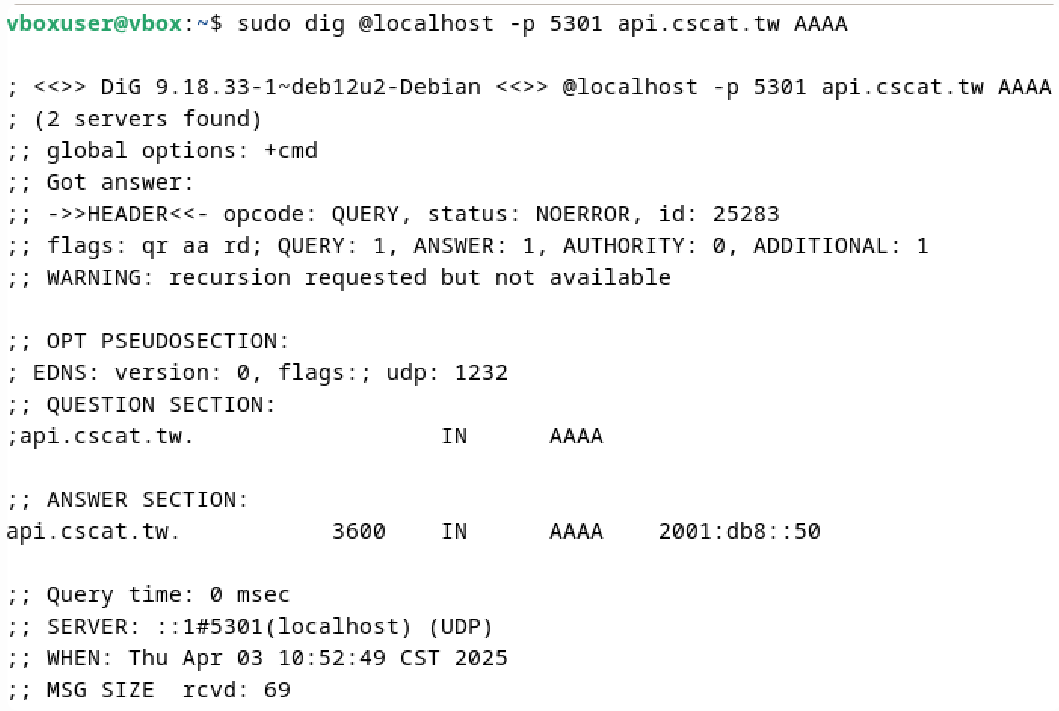
```
vboxuser@vbox:~$ sudo dig @localhost -p 5301 cscat.tw MX

; <<>> DiG 9.18.33-1~deb12u2-Debian <<>> @localhost -p 5301 cscat.tw MX
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1418
;; 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      MX

;; ANSWER SECTION:
cscat.tw.               3600    IN      MX      10 mail.cscat.tw.

;; Query time: 7 msec
;; SERVER: ::1#5301(localhost) (UDP)
;; WHEN: Thu Apr 03 10:51:13 CST 2025
;; MSG SIZE  rcvd: 58
```

- `sudo dig @localhost -p 5301 cscat.tw A`



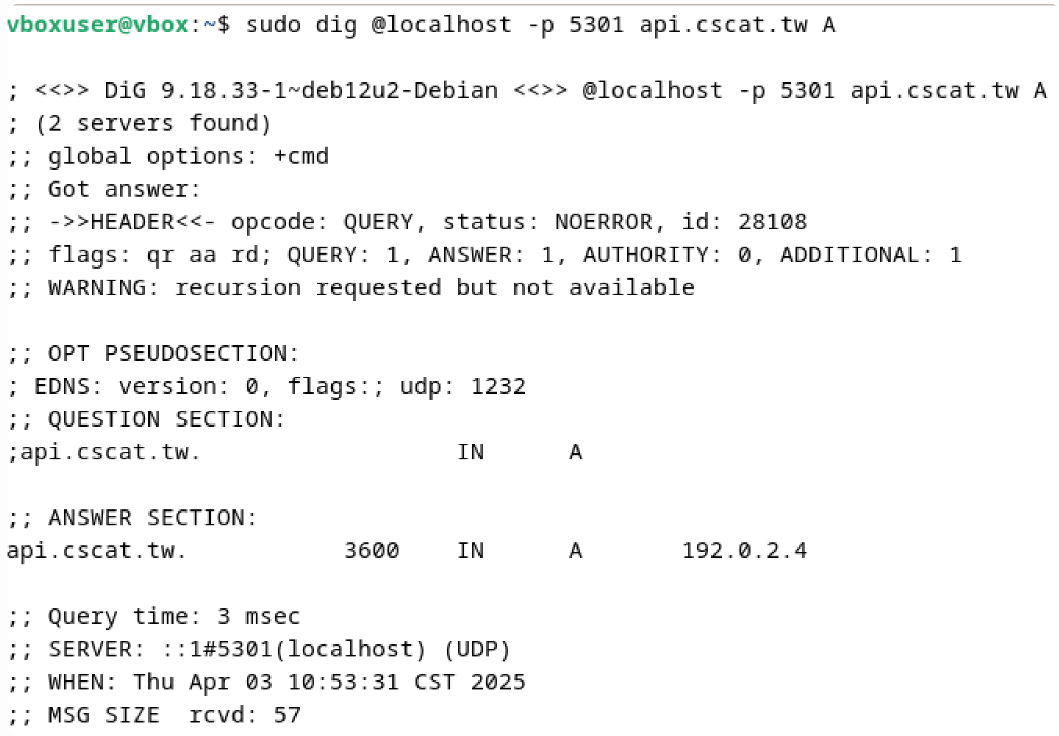
```
vboxuser@vbox:~$ sudo dig @localhost -p 5301 cscat.tw A

; <<>> DiG 9.18.33-1~deb12u2-Debian <<>> @localhost -p 5301 cscat.tw A
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34744
;; 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      A

;; ANSWER SECTION:
cscat.tw.               3600    IN      A       192.0.2.1

;; Query time: 0 msec
;; SERVER: ::1#5301(localhost) (UDP)
;; WHEN: Thu Apr 03 10:51:54 CST 2025
;; MSG SIZE  rcvd: 53
```

- `sudo dig @localhost -p 5301 api.cscat.tw AAAA`



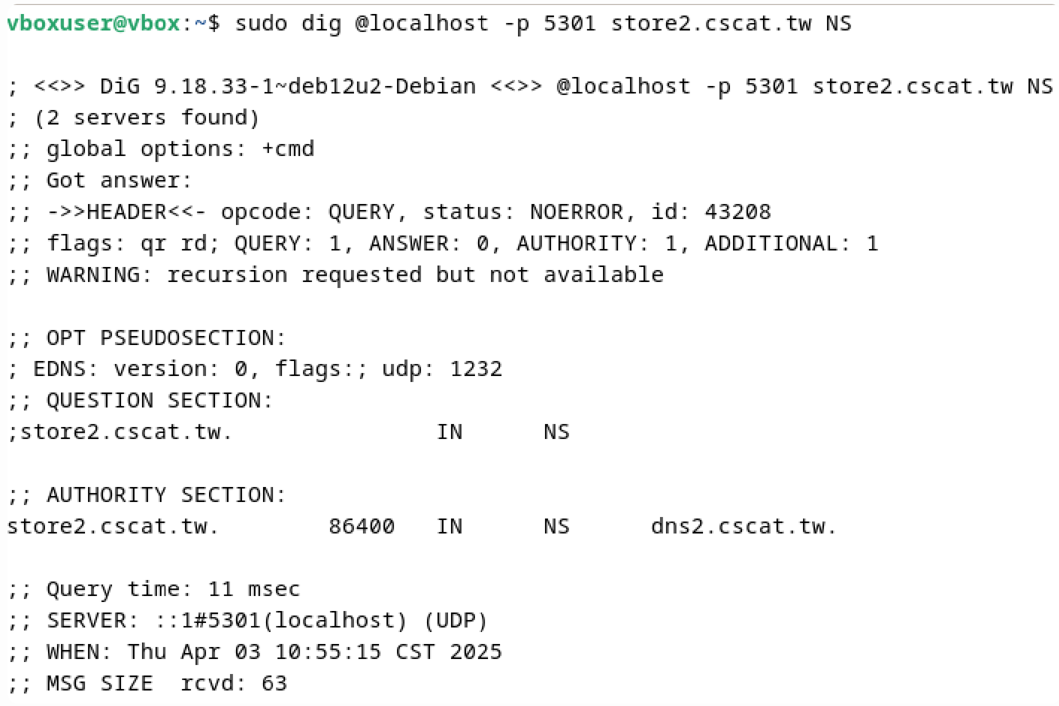
```
vboxuser@vbox:~$ sudo dig @localhost -p 5301 api.cscat.tw AAAA

; <<>> DiG 9.18.33-1~deb12u2-Debian <<>> @localhost -p 5301 api.cscat.tw AAAA
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 25283
;; 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:
;api.cscat.tw.                  IN      AAAA

;; ANSWER SECTION:
api.cscat.tw.           3600    IN      AAAA    2001:db8::50

;; Query time: 0 msec
;; SERVER: ::1#5301(localhost) (UDP)
;; WHEN: Thu Apr 03 10:52:49 CST 2025
;; MSG SIZE  rcvd: 69
```

- `sudo dig @localhost -p 5301 api.cscat.tw A`



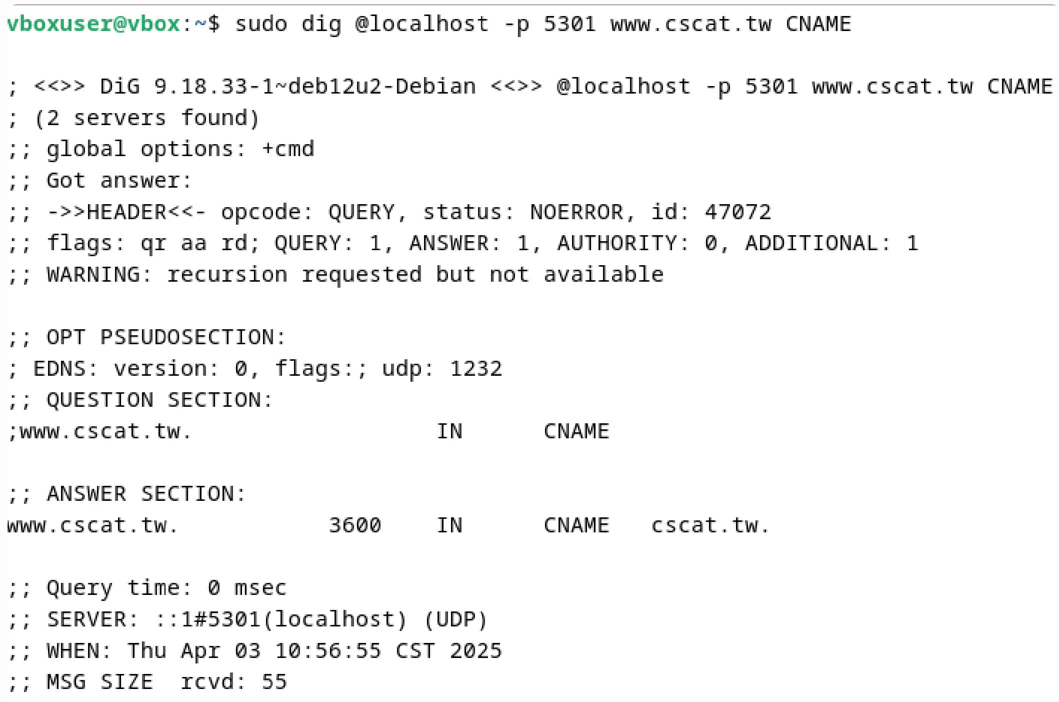
```
vboxuser@vbox:~$ sudo dig @localhost -p 5301 api.cscat.tw A

; <<>> DiG 9.18.33-1~deb12u2-Debian <<>> @localhost -p 5301 api.cscat.tw A
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 28108
;; 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:
;api.cscat.tw.                  IN      A

;; ANSWER SECTION:
api.cscat.tw.           3600    IN      A       192.0.2.4

;; Query time: 3 msec
;; SERVER: ::1#5301(localhost) (UDP)
;; WHEN: Thu Apr 03 10:53:31 CST 2025
;; MSG SIZE  rcvd: 57
```

- `sudo dig @localhost -p 5301 store2.cscat.tw NS`



```
vboxuser@vbox:~$ sudo dig @localhost -p 5301 store2.cscat.tw NS

; <<>> DiG 9.18.33-1~deb12u2-Debian <<>> @localhost -p 5301 store2.cscat.tw NS
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43208
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1
;; WARNING: recursion requested but not available

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

;; AUTHORITY SECTION:
store2.cscat.tw.        86400   IN      NS      dns2.cscat.tw.

;; Query time: 11 msec
;; SERVER: ::1#5301(localhost) (UDP)
;; WHEN: Thu Apr 03 10:55:15 CST 2025
;; MSG SIZE  rcvd: 63
```

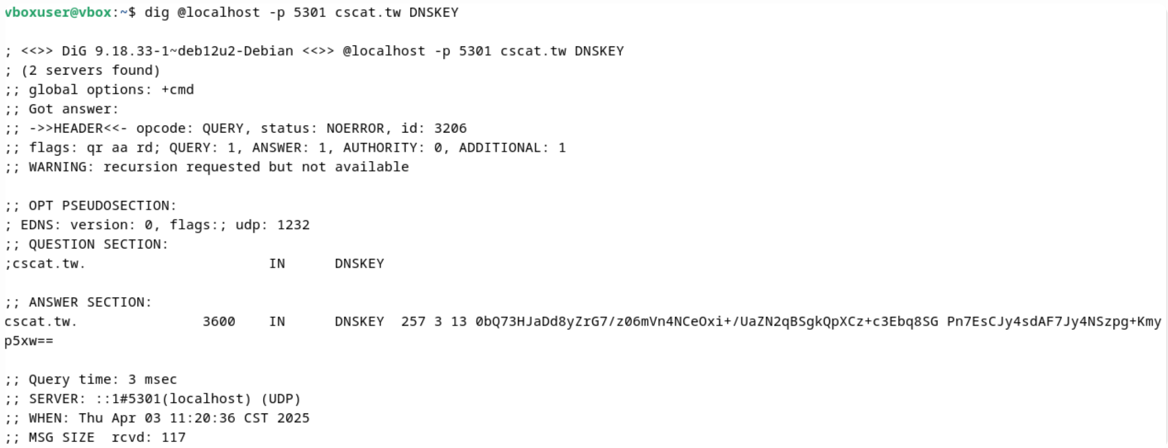
- `sudo dig @localhost -p 5301 www.cscat.tw CNAME`



```
vboxuser@vbox:~$ sudo dig @localhost -p 5301 www.cscat.tw CNAME

; <<>> DiG 9.18.33-1~deb12u2-Debian <<>> @localhost -p 5301 www.cscat.tw CNAME
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47072
;; 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:
;www.cscat.tw.                  IN      CNAME

;; ANSWER SECTION:
www.cscat.tw.           3600    IN      CNAME   cscat.tw.

;; Query time: 0 msec
;; SERVER: ::1#5301(localhost) (UDP)
;; WHEN: Thu Apr 03 10:56:55 CST 2025
;; MSG SIZE  rcvd: 55
```

5. ref: 1

- 基本原理：DNSSEC 使用公鑰加密技術，為 DNS 記錄增加數位簽章，當 DNS 解析器獲取 DNS 記錄時，會先檢查記錄的簽章，如果簽章有效，則代表該記錄來自權威伺服器，且未被篡改，此外 DNSSEC 引入了新的 DNS 記錄類型，如 RRSIG (Resource Record Signature) 用於簽章，DNSKEY 用於儲存簽名金鑰，DS 用於儲存子域的 DNSKEY 雜湊值等。
- 目的：防止 DNS 欺騙攻擊與確保 DNS 資料完整性
- 截圖：



```
vboxuser@vbox:~$ dig @localhost -p 5301 cscat.tw DNSKEY

; <<>> DiG 9.18.33-1~deb12u2-Debian <<>> @localhost -p 5301 cscat.tw DNSKEY
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3206
;; 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 0bQ73HJaDd8yZrG7/z06mVn4NCeOxi+/UaZN2qBSgkQpXCz+c3Ebq8SG Pn7EsCJy4sdAF7Jy4NSzpg+Kmy
p5xw==

;; Query time: 3 msec
;; SERVER: ::1#5301(localhost) (UDP)
;; WHEN: Thu Apr 03 11:20:36 CST 2025
;; MSG SIZE  rcvd: 117
```

## 2 PowerDNS Recursor

### 0 Basic

ref: 1, 2

1. authoritative server 是負責儲存並回應特定網域名稱內的正式 DNS 記錄。當查詢者詢問某個網域時，這個伺服器能提供最終的答案，而不會再向其他伺服器查詢。
2. recursive DNS query：解析器負責取得完整答案，使用者只需發送一次查詢，解析器會自動向多個 DNS 伺服器查詢，直到取得正確的 IP 位址。iterative DNS query：伺服器只會提供可用的資訊，而不會幫助解析完整的查詢，使用者可能需要多次查詢不同的伺服器，直到取得最終的 IP 位址。

## 1 Setting up PowerDNS Recursor

1. ref: 1, 2, 3
   步驟：

   1. `sudo apt install pdns-recursor -y` 安裝 pdns-recursor
   2. `sudo vim /etc/powerdns/recursor.conf` 更改或新增以下內容：

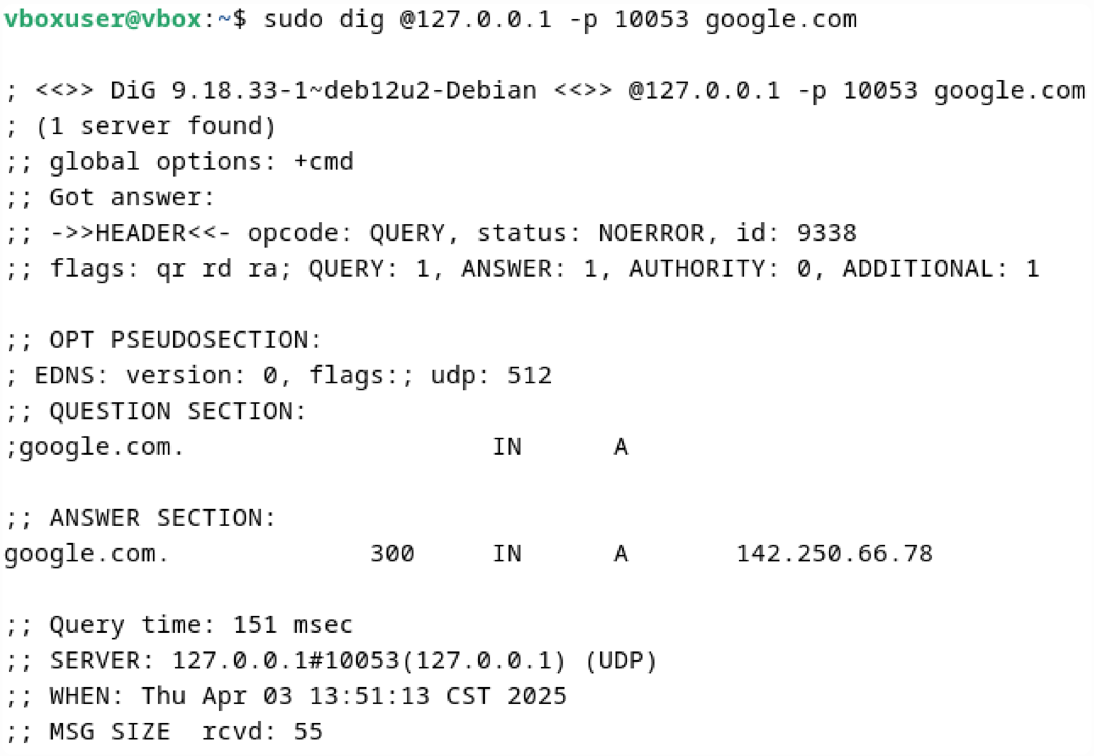
   ```
   local-port=10053 # 在 port 10053 另外設置 PowerDNS Recursor 服務
   max-cache-ttl=300 # 將快取的 TTL 設定成 300 seconds
   forward-zones-file=/etc/powerdns/forward-zones # 使用 forward-zones-file 來設定
   dnssec=validate # 啟用 DNSSEC 驗證
   ```

   3. `sudo vim /etc/powerdns/forward-zones` 加入以下內容：

   ```
   cscat.tw=127.0.0.1:5301;8.8.8.8
   ```

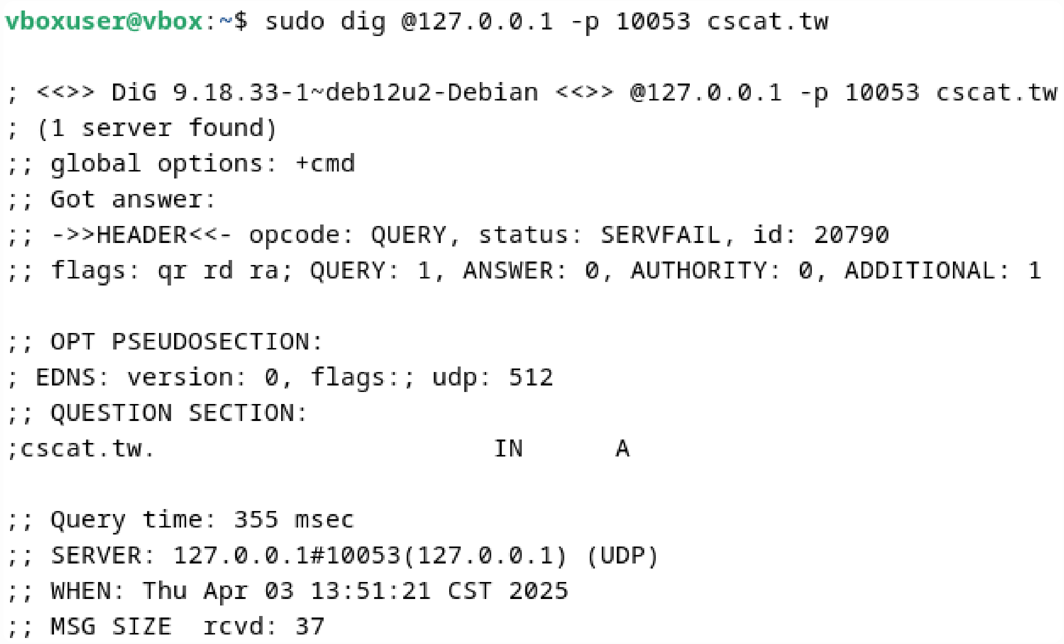
   4. `sudo systemctl restart pdns-recursor` 重啟 pdns-recursor

2. 截圖：



```
vboxuser@vbox:~$ sudo dig @127.0.0.1 -p 10053 google.com

; <<>> DiG 9.18.33-1~deb12u2-Debian <<>> @127.0.0.1 -p 10053 google.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 9338
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;google.com.                    IN      A

;; ANSWER SECTION:
google.com.             300     IN      A       142.250.66.78

;; Query time: 151 msec
;; SERVER: 127.0.0.1#10053(127.0.0.1) (UDP)
;; WHEN: Thu Apr 03 13:51:13 CST 2025
;; MSG SIZE  rcvd: 55
```

3. 截圖：



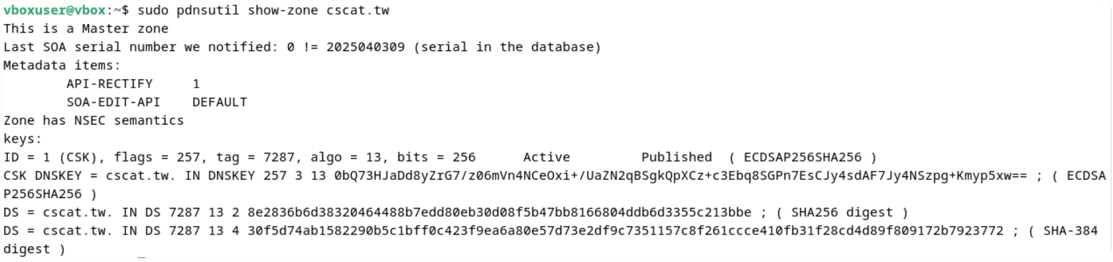
```
vboxuser@vbox:~$ sudo dig @127.0.0.1 -p 10053 cscat.tw

; <<>> DiG 9.18.33-1~deb12u2-Debian <<>> @127.0.0.1 -p 10053 cscat.tw
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 20790
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;cscat.tw.                      IN      A

;; Query time: 355 msec
;; SERVER: 127.0.0.1#10053(127.0.0.1) (UDP)
;; WHEN: Thu Apr 03 13:51:21 CST 2025
;; MSG SIZE  rcvd: 37
```

PowerDNS Recursor 會遞迴查詢 google.com，最終從 Google 的權威 DNS 伺服器獲取正確的記錄。Google DNS（8.8.8.8）支援 DNSSEC，並能夠提供可驗證的 DNSSEC 簽名資料，因此查詢 google.com 時不會有問題。但當 PowerDNS Recursor 嘗試查詢 cscat.tw 時，它會根據 forward-zones 設定，將查詢導向本機的權威伺服器（127.0.0.1:5301），因為 cscat.tw 的權威伺服器 DS 沒有發布到上層 .tw TLD，所以 Recursor 會驗證失敗，導致 SERVFAIL。

4. ref: 1

   步驟：

   1. `sudo vim /etc/powerdns/recursor.conf` 加入 `allow-trust-anchor-query=yes`
   2. `sudo pdnsutil show-zone cscat.tw` 找到 DS

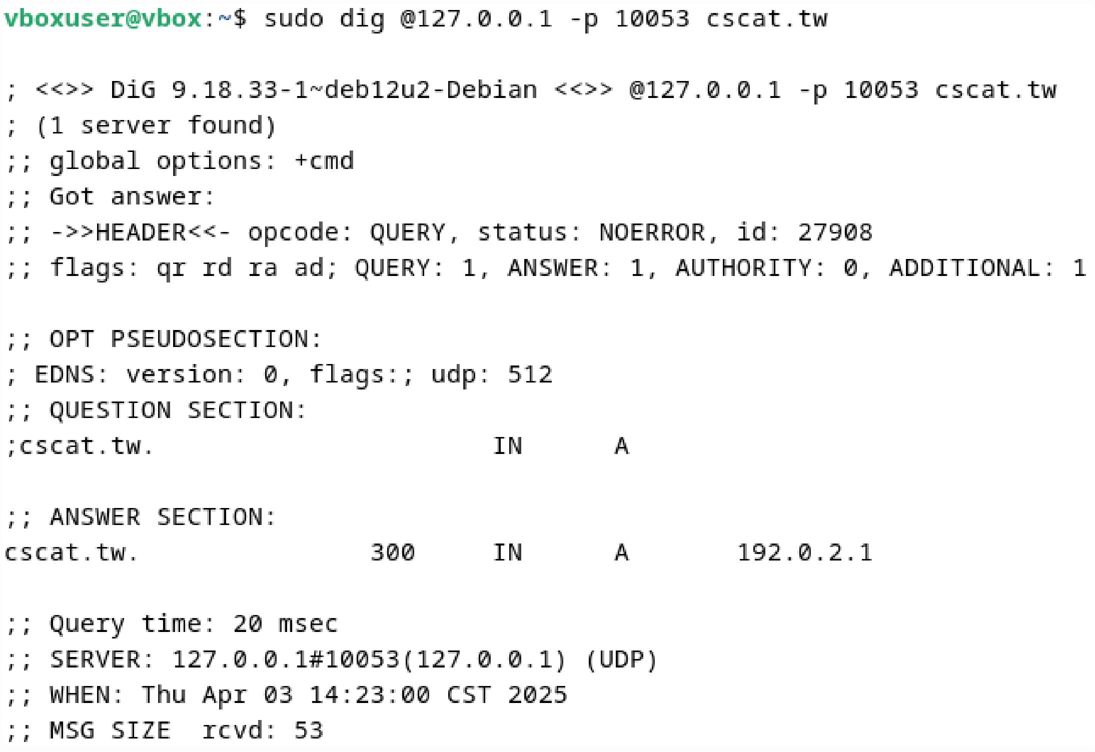
      

      ```
      vboxuser@vbox:~$ sudo pdnsutil show-zone cscat.tw
      This is a Master zone
      Last SOA serial number we notified: 0 != 2025040309 (serial in the database)
      Metadata items:
              API-RECTIFY     1
              SOA-EDIT-API    DEFAULT
      Zone has NSEC semantics
      keys:
      ID = 1 (CSK), flags = 257, tag = 7287, algo = 13, bits = 256      Active         Published  ( ECDSAP256SHA256 )
      CSK DNSKEY = cscat.tw. IN DNSKEY 257 3 13 0bQ73HJaDd8yZrG7/z06mVn4NCeOxi+/UaZN2qBSgkQpXCz+c3Ebq8SGPn7EsCJy4sdAF7Jy4NSzpg+Kmyp5xw== ; ( ECDSA
      P256SHA256 )
      DS = cscat.tw. IN DS 7287 13 2 8e2836b6d38320464488b7edd80eb30d08f5b47bb8166804ddb6d3355c213bbe ; ( SHA256 digest )
      DS = cscat.tw. IN DS 7287 13 4 30f5d74ab1582290b5c1bff0c423f9ea6a80e57d73e2df9c7351157c8f261ccce410fb31f28cd4d89f809172b7923772 ; ( SHA-384
      digest )
      ```

   3. `sudo vim /etc/powerdns/recursor.lua` 加入剛剛找到的 DS

      ```
      addTA("cscat.tw", "7287 13 2 8e2836b6d38320464488b7edd80eb30d08f5b47bb816
      addTA("cscat.tw", "7287 13 4 30f5d74ab1582290b5c1bff0c423f9ea6a80e57d73e2
      ```

   4. `sudo systemctl restart pdns-recursor` 重啟 pdns-recursor
   5. 截圖：

      ```
      vboxuser@vbox:~$ sudo dig @127.0.0.1 -p 10053 cscat.tw

      ; <<>> DiG 9.18.33-1~deb12u2-Debian <<>> @127.0.0.1 -p 10053 cscat.tw
      ; (1 server found)
      ;; global options: +cmd
      ;; Got answer:
      ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 27908
      ;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

      ;; OPT PSEUDOSECTION:
      ; EDNS: version: 0, flags:; udp: 512
      ;; QUESTION SECTION:
      ;cscat.tw.                      IN      A

      ;; ANSWER SECTION:
      cscat.tw.               300     IN      A       192.0.2.1

      ;; Query time: 20 msec
      ;; SERVER: 127.0.0.1#10053(127.0.0.1) (UDP)
      ;; WHEN: Thu Apr 03 14:23:00 CST 2025
      ;; MSG SIZE  rcvd: 53
      ```

5. - 過高：如果 DNS record 改變，使用者可能繼續存取過時的 IP，導致連線錯誤。
   - 過低：DNS server 需要更頻繁查詢 Authoritative DNS server，可能會增加延遲並提高伺服器負擔。

6. ref: 1

   攻擊者可以透過冒充 DNS nameserver 向 DNS resolver 發出 request，然後在 DNS resolver 查詢nameserver 時偽造答覆來 poison DNS cache。因為 DNS server 使用 UDP 而不是 TCP，目前沒有針對 DNS 資訊的驗證。受害者之後查詢任何記錄時，都會回傳攻擊者的偽造資訊，可能將受害者導向惡意網站。

## 2 Security

1. 如果 DNS 伺服器允許所有 IP 進行 Recursive Query，會帶來以下風險：Cache Poisoning，攻擊者可以透過冒充 DNS nameserver 向 DNS resolver 發出 request，然後在 DNS resolver 查詢nameserver 時偽造答覆來 poison DNS cache，受害者之後查詢任何記錄時，都會回傳攻擊者的偽造資訊，可能將受害者導向惡意網站。
2. 步驟：
    1. `sudo vim /etc/powerdns/recursor.conf` 新增以下：

        ```
        allow-from=192.168.0.0/16
        ```

        僅讓內網 IP 查詢
    2. `sudo systemctl restart pdns-recursor`

# 3 dnsdist

## 1 Setting up dnsdist

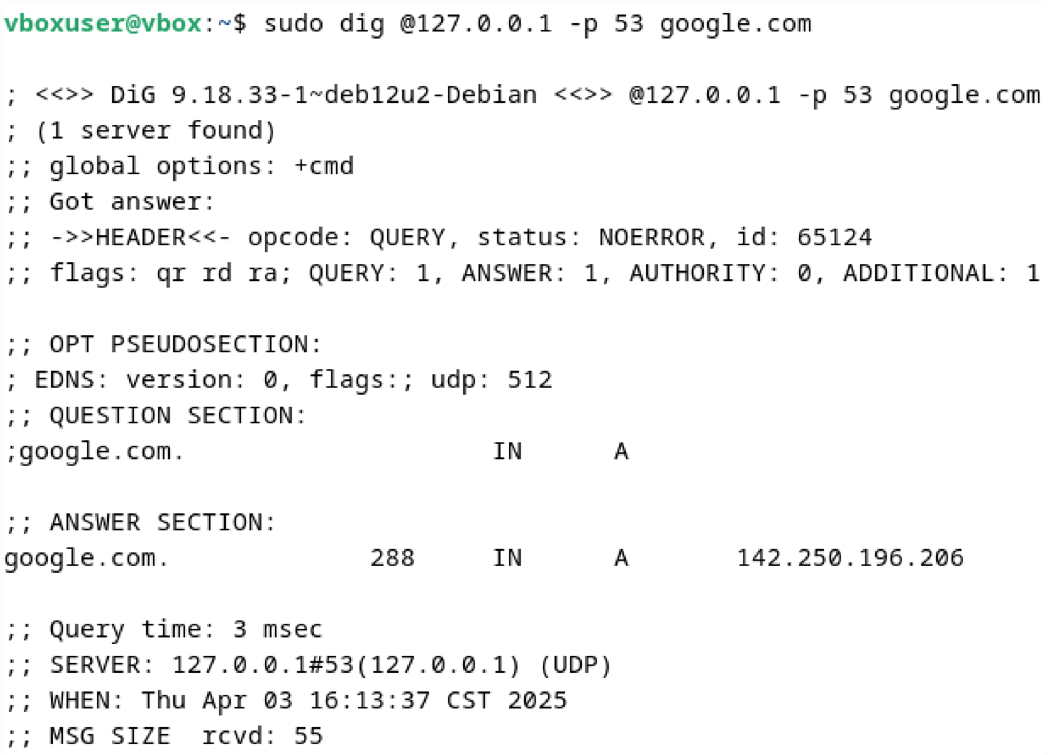
1. ref: 1

    步驟：

    1. `sudo apt install dnsdist -y`
    2. `sudo vim /etc/dnsdist/dnsdist.conf` 加入以下內容：

        ```
        setLocal('0.0.0.0:53')
        newServer({address='127.0.0.1:10053'})
        newServer({address='8.8.8.8'})
        ```

    3. `sudo systemctl restart dnsdist` 重啟 dnsdist

4. 

```
vboxuser@vbox:~$ sudo dig @127.0.0.1 -p 53 google.com

; <<>> DiG 9.18.33-1~deb12u2-Debian <<>> @127.0.0.1 -p 53 google.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 65124
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;google.com.                    IN      A

;; ANSWER SECTION:
google.com.             288     IN      A       142.250.196.206

;; Query time: 3 msec
;; SERVER: 127.0.0.1#53(127.0.0.1) (UDP)
;; WHEN: Thu Apr 03 16:13:37 CST 2025
;; MSG SIZE  rcvd: 55
```

2. ref: 1

   步驟：

   1. `sudo vim /etc/dnsdist/dnsdist.conf` 加入以下內容：

      ```
      -- 針對總長度超過 70 的 TXT record 進行過濾，超過則丟棄查詢不予回應。
      addAction(
          AndRule({QTypeRule(DNSQType.TXT), QNameWireLengthRule(0, 70)}),
          DropAction()
      )

      -- 限制每個 IP 最多每秒可查詢 20 次，超過則丟棄查詢不予回應
      local dbr = dynBlockRulesGroup()
      dbr:setQueryRate(20, 1, "", 60)

      --針對所有對 *.csdog.tw 的 query 都丟棄查詢而不回應。
      addAction(QNameRule("*.csdog.tw"), DropAction())
      ```

   2. `sudo systemctl restart dnsdist` 重啟 dnsdist

## 2 DNS-over-TLS

1. ref: 1

   - DNS-over-TLS（DoT）透過 TLS 加密 DNS 查詢，確保 DNS 資料在傳輸時不會被竊聽或篡改，防止流量可被攔截與DNS 伺服器可被中間人攻擊等問題，提高隱私性和安全性。
   -

| | DNS-over-TLS (DoT) | DNS-over-HTTPS (DoH) |
|---|---|---|
| | | |

| | | |
|---|---|---|
| 加密機制 | 使用 TLS 直接加密 DNS 封包 | 使用 HTTPS（TLS + HTTP/2）加密 DNS |
| 效能 | 低延遲，專為 DNS 設計，適合 ISP 或內網使用 | 可能因 HTTP/2 耗費額外資源，稍慢 |
| 安全性 | 只能用於 DNS，較容易監管與管理 | 可混淆為普通 HTTPS 流量，難以過濾 |

2. ref: 1

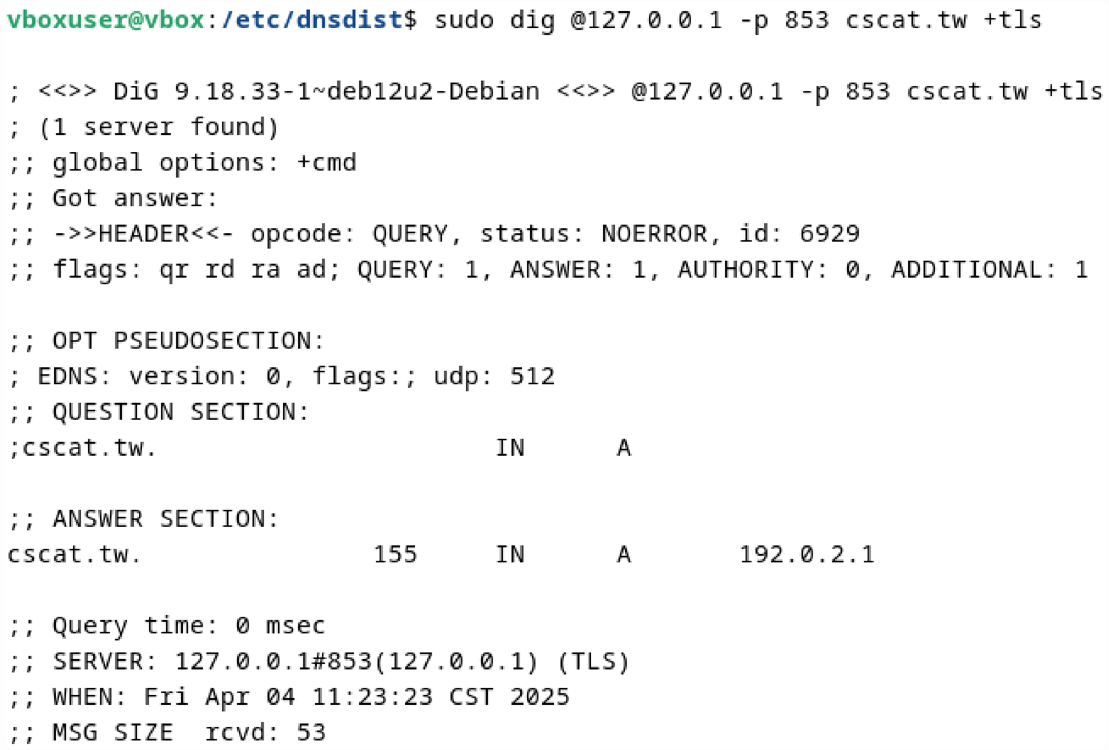
   步驟：

   1. `sudo openssl req -x509 -newkey rsa:4096 -keyout dns.key -out dns.crt -days 365 -nodes -subj "/CN=b11901164.com"` 自己簽 TLS
   2. `sudo chmod 644 dns.key` 改 dns.key 的權限，不然 dnsdist 沒辦法用，restart 會 error
   3. `sudo vim /etc/dnsdist/dnsdist.conf` 加入：

      ```
      addTLSLocal("0.0.0.0", "/etc/dnsdist/dns.crt", "/etc/dnsdist/dns.key")
      ```

   4. `sudo systemctl restart dnsdist` 重啟 dnsdist

3. 截圖：



```
vboxuser@vbox:/etc/dnsdist$ sudo dig @127.0.0.1 -p 853 cscat.tw +tls

; <<>> DiG 9.18.33-1~deb12u2-Debian <<>> @127.0.0.1 -p 853 cscat.tw +tls
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 6929
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;cscat.tw.                      IN      A

;; ANSWER SECTION:
cscat.tw.               155     IN      A       192.0.2.1

;; Query time: 0 msec
;; SERVER: 127.0.0.1#853(127.0.0.1) (TLS)
;; WHEN: Fri Apr 04 11:23:23 CST 2025
;; MSG SIZE  rcvd: 53
```

## 4 Master and Slave

ref: 1, 2

1. 架構設計：
    - Primary PowerDNS Authoritative：負責提供 csie.ntu.edu.tw 網域的權威解析
    - Secondary PowerDNS Authoritative：作為備援，透過 AXFR/IXFR 同步
    - MariaDB Galera Cluster：存放 DNS 記錄，透過 Galera Cluster 同步
    - PowerDNS Admin：提供 Web 管理介面，可從任一伺服器存取
    - PowerDNS Recursor：解析外部 DNS 查詢
    - dnsdist：負載均衡與增強安全性

- 如果今天其中一台伺服器壞掉了怎麼辦？
    - PowerDNS Authoritative 伺服器有 Primary 和 Secondary，當主伺服器掛掉時，次要伺服器仍能提供解析。
- 如果今天系館停電導致所有機房下線怎麼辦？
    - Secondary PowerDNS Authoritative 可能設定在計中，也就是系上以外的地方，確保當系上機房故障時，DNS 服務仍可運行，且透過 AXFR/IXFR 取得最新 DNS 記錄，仍可提供解析。兩台以上的 Recursor 也可以其中一台部署在其他地方，確保所有人仍能查詢外部網域。
- 如果因為某些原因導致伺服器上的 DNS records 不見了怎麼辦？
    - MariaDB Galera Cluster 可確保所有記錄自動同步，避免單點失效。
    - 定期備份 DNS 記錄，並存放於遠端機器或 S3 之類的雲端存儲，以防資料誤刪。
    - Secondary PowerDNS 可透過 IXFR 增量同步 來保持最新記錄，即使主伺服器的資料遺失，次要伺服器仍保有備份。

2.

| 方法 | 描述 | 優點 | 缺點 |
|---|---|---|---|
| AXFR | 傳輸整個 DNS 區域記錄 | 簡單，<br>適合初始同步 | 浪費頻寬，<br>當記錄變動頻繁時效率低 |
| IXFR | 只傳輸變更的記錄 | 節省頻寬，<br>適合動態變更 | 需要 Secondary 伺服器支援增量更新 |

- 使用時機：
    - AXFR：當新的 Secondary 伺服器加入或初始化同步時使用，確保完整記錄。
    - IXFR：當 DNS 記錄變動時使用，以減少頻寬消耗並提高效率。