

NASA HW5 - 金哲安(B12902118)

1 Setting up PowerDNS (48 pts)

References

- B12902116 (林靖昀)
- B12902066 (宋和峻)
- <https://repo.powerdns.com/>
- https://wiki.freedomstu.com/books/開源軟體安裝流程/page/powerdns-debian?fbclid=IwZKh0bgNhZW0CMTEAAR1WE5Saplh2wX0f6BxCm5j7l5QarNf7IXfPzQ9LCAeQD3utwAHp5apm4NY_aem_-N224KKJznOj6FXTGsZijw
- <https://doc.powerdns.com/authoritative/installation.html#after-installation>
- <https://doc.powerdns.com/authoritative/backends/index.html>
- <https://github.com/PowerDNS-Admin/PowerDNS-Admin/tree/master/docs/wiki>
- <https://phoenixnap.com/kb/powerdns-ubuntu>
- <https://www.howtoforge.com/how-to-install-powerdns-admin-on-ubuntu-20-04/>
- <https://www.uuu.com.tw/Public/content/article/23/20231225.htm>
- <https://www.cloudflare.com/zh-tw/learning/cdn/glossary/reverse-proxy/>
- <https://zh.wikipedia.org/zh-tw/域名系统安全扩展>
- <https://www.sidn.nl/en/modern-internet-standards/dnssec-on-the-powerdns-authoritative-server>

1.

1. On macOS, download debian-12.10.0-arm64-netinst.iso from <https://cdimage.debian.org/debian-cd/current/arm64/iso-cd>
2. On VirtualBox, create a new virtual machine and start it with the settings:
 - Name and Operating System
 - Name: Debian7
 - ISO Image: debian-12.10.0-arm64-netinst.iso
 - Type: Linux
 - Subtype: Debian
 - Version: Debian 12 Bookworm (ARM 64-Bit)
 - (Checked) Skip Unattended Installation
 - Hardware
 - Base Memory: 4096 MB
 - Processors: 8
3. Choose Graphical Install
4. Language: English

5. Location: other > Asia > Taiwan
6. Configure locales: United States - en_US.UTF-8
7. Configure the keyboard: American English
8. Hostname: vbox
9. Domain name: (blank)
10. Setup root password
11. Setup user name, username, and password
12. Partition disk: Guided - use entire disk
13. Select the disk
14. Select All files in one partition
15. Select Finish partitioning and write changes to disk
16. Select Yes
17. Select No
18. Select Taiwan
19. Select deb.debian.org
20. Leave blank and continue
21. Select No
22. Check SSH server and standard system utilities and continue
23. Choose continue
24. `fs0:`
25. `cd EFI`
26. `cd debian`
27. `grubaa64.efi`
28. Boot into Debian
29. Login as root
30. `mkdir /boot/efi/EFI/BOOT`
31. `cp /boot/efi/EFI/debian/grubaa64.efi /boot/efi/EFI/BOOT/B00TAA64.EFI`
32. `echo "PermitRootLogin yes" >> /etc/ssh/sshd_config`
33. On Virtual Box, configure the Network adapter to use NAT and add port forwarding:
 - Name: ssh
 - Protocol: TCP
 - Host Port: 3027
 - Guest Port: 22
34. `reboot`
35. On mac terminal, ssh to the vm by `ssh -p 3027 root@localhost`
36. `apt update`
37. `apt install mariadb-server`
38. `systemctl enable --now mariadb`
39. `mysql_secure_installation`
40. Configure root password, and for other options, just press Enter to use the default option
41. `apt install curl gnupg vim sudo`
42. Create the file '/etc/apt/sources.list.d/pdns.list' with this content:

```
deb [signed-by=/etc/apt/keyrings/auth-49-pub.asc] http://repo.powerdns.com/debian bookw
```

Put this in '/etc/apt/preferences.d/auth-49':

```
Package: auth*
Pin: origin repo.powerdns.com
Pin-Priority: 600
```

and execute the following commands as a single command:

```
sudo install -d /etc/apt/keyrings; curl https://repo.powerdns.com/FD380FBB-pub.asc | sudo gpg --dearmor > /etc/apt/keyrings/auth-49.gpg
sudo apt-get update &&
sudo apt-get install pdns-server pdns-backend-mysql
```

43. mysql -u root -p and login as root
44. CREATE DATABASE powerdns;
45. GRANT ALL ON powerdns.* TO 'powerdns'@'localhost' IDENTIFIED BY 'powerdns';
46. FLUSH PRIVILEGES;
47. EXIT;
48. mysql -u powerdns -p powerdns < /usr/share/pdns-backend-mysql/schema/schema.mysql.sql
49. nano /etc/powerdns/pdns.conf , enter and save to file:

```
launch=gmysql
gmysql-host=127.0.0.1
gmysql dbname=powerdns
gmysql user=powerdns
gmysql password=powerdns
local address=0.0.0.0
local port=5301
```

50. systemctl restart pdns
51. systemctl enable pdns
52. dig @127.0.0.1 -p 5301
53. pdns_control version

```
[root@vbox:~# 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: 35356
;; 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: Fri Mar 28 11:47:14 CST 2025
;; MSG SIZE  rcvd: 28

root@vbox:~# ]
```

```
3027
[root@vbox:~# pdns_control version
4.9.4
root@vbox:~# ]
```

2

```
apt install -y libmariadb-dev libsasl2-dev libldap2-dev libssl-dev libxml2-dev libxslt1-dev  
curl -sL https://deb.nodesource.com/setup_14.x | bash -  
apt install -y nodejs
```

Run this as a single command:

```
curl -sL https://dl.yarnpkg.com/debian/pubkey.gpg | gpg --dearmor | sudo tee /usr/share/keyrings/yarnkey.gpg > /dev/null  
echo "deb [signed-by=/usr/share/keyrings/yarnkey.gpg] https://dl.yarnpkg.com/debian stable main" | sudo tee -a /etc/apt/sources.list.d/yarn.list  
apt install -y yarn
```

```
git clone https://github.com/PowerDNS-Admin/PowerDNS-Admin.git /opt/web/powerdns-admin  
cd /opt/web/powerdns-admin  
python3 -m venv .venv  
source .venv/bin/activate  
pip install --upgrade pip  
pip install -r requirements.txt  
cp /opt/web/powerdns-admin/configs/development.py /opt/web/powerdns-admin/configs/product  
mysql -u root -p  
CREATE DATABASE `powerdnsadmin` CHARACTER SET utf8mb4 COLLATE utf8mb4_unicode_ci;  
GRANT ALL PRIVILEGES ON `powerdnsadmin`.* TO 'pdnsadminuser'@'localhost' IDENTIFIED BY 'pdnsadmin';  
FLUSH PRIVILEGES;  
quit  
pip3 install mysqlclient==2.0.1  
vim /opt/web/powerdns-admin/configs/production.py
```

```
import urllib.parse  
SECRET_KEY='\\xcc\\x8ex\\xd2o\\x15\\xe9\\xa7\\x03b\\x05*f\\xe1c\\x80'  
SQLA_DB_USER = 'pdnsadminuser'  
SQLA_DB_PASSWORD = 'pdnsadminuser'  
SQLA_DB_NAME = 'powerdnsadmin'  
SQLALCHEMY_DATABASE_URI = 'mysql://username:password@127.0.0.1/db_name'
```

(Leave other configs unchanged)

```
export FLASK_CONF=../configs/production.py  
export FLASK_APP=powerdnsadmin/__init__.py  
flask db upgrade  
yarn install --pure-lockfile  
flask assets build  
./run.py
```

On Virtual Box, add port forwarding:

- Name: admin
- Protocol: TCP
- Host Port: 9191
- Guest Port: 9191

On a web browser on mac, go to <http://localhost:9191>

Create an Account

First name: b12902118

Complete other info to create an account

Login with the account

The screenshot shows the PowerDNS-Admin interface. On the left is a sidebar with navigation links: Messe, Power, Install, Power, Back, Conn, Runnir, Power, Install, localh, b1290, linux, Install, How to, and a search bar. The main area has a header "Server Settings" and a breadcrumb "Dashboard / Server Settings". It features a "Settings Editor" section with three fields: "PowerDNS API URL" (empty), "PowerDNS API Key" (empty), and "PowerDNS Version" (set to 4.1.1). A prominent red error box at the top states: "Error! Please complete your PowerDNS API configuration before continuing". Below the error box is a "Save Settings" button.

3

Put this in /etc/systemd/system/powerdns-admin.service

```
[Unit]
Description=PowerDNS-Admin
Requires=powerdns-admin.socket
After=network.target
[Service]
User=root
Group=root
PIDFile=/run/powerdns-admin.pid
WorkingDirectory=/opt/web/powerdns-admin
ExecStartPre=/bin/bash -c '$$(mkdir -p /run/powerdns-admin)'
ExecStart=/opt/web/powerdns-admin/venv/bin/gunicorn --pid /run/powerdns-admin.pid --bind
ExecReload=/bin/kill -s HUP $MAINPID
ExecStop=/bin/kill -s TERM $MAINPID
PrivateTmp=true
[Install]
WantedBy=multi-user.target
```

sudo systemctl edit --force powerdns-admin.service

Put this in between the commented section

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

Put this in /etc/systemd/system/powerdns-admin.socket

```
[Unit]
Description=PowerDNS-Admin socket
[Socket]
ListenStream=/run/powerdns-admin/socket
[Install]
WantedBy=sockets.target
```

Put this in /etc/tmpfiles.d/powerdns-admin.conf

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

```
sudo systemctl daemon-reload
sudo systemctl start powerdns-admin.service powerdns-admin.socket
sudo systemctl enable powerdns-admin.service powerdns-admin.socket
sudo apt update && sudo apt install nginx -y
```

Put this in /etc/nginx/conf.d/pdns-admin.conf

```

server {
    listen *:80;
    server_name          b12902118.com;
    index               index.html index.htm index.php;
    root                /opt/web/powerdns-admin;
    access_log           /var/log/nginx/powerdns-admin.local.access.log combined;
    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 $proxy_add_x_forwarded_for;
    proxy_headers_hash_bucket_size 64;
    location ~ ^/static/  {
        include  /etc/nginx/mime.types;
        root /opt/web/powerdns-admin/powerdnsadmin;
        location ~* \.(jpg|jpeg|png|gif)$ {
            expires 365d;
        }
        location ~* ^.+.(css|js)$ {
            expires 7d;
        }
    }
    location / {
        proxy_pass http://127.0.0.1:9191;
        proxy_read_timeout   120;
        proxy_connect_timeout 120;
        proxy_redirect         off;
        proxy_set_header        Host $host;
        proxy_set_header        X-Real-IP $remote_addr;
        proxy_set_header        X-Forwarded-For $proxy_add_x_forwarded_for;
        proxy_set_header        X-Forwarded-Proto $scheme;
    }
}

```

```

sudo chown -R www-data:www-data /opt/web/powerdns-admin
sudo systemctl restart nginx

```

Go back to the browser connected to <http://localhost:9191> and open the API Keys tab on the left menu
Click +Create Key

Select Administrator from the Role dropdown. Add "Administrator" to the description for the key

Click Create API Key

A popup window prints the key. Copy the key and press Confirm to continue

Navigate to the Dashboard page

Enter the domain and API key

Click Save Settings

Put this in /etc/powerdns/pdns.conf

```
api=yes  
api-key=(Paste key here)  
webserver=yes
```

```
systemctl restart pdns
```

Back on mac terminal, echo "127.0.0.1 b12902118.com" | sudo tee -a /etc/hosts

On Virtual Box, add port forwarding:

- Name: web
- Protocol: TCP
- Host Port: 80
- Guest Port: 80

Go to a web browser and connect to b12902118.com

Login

The screenshot shows the PowerDNS-Admin interface. On the left is a sidebar with navigation links: Zone Management (Dashboard, Create Zone, Remove Zone), Administration (Global Search, Activity, Server Statistics, Server Configuration, Zone Templates, Accounts, Users, API Keys, Settings). The 'Dashboard' link is highlighted. The main area is titled 'Dashboard' and contains a 'Zones' table. The table has columns: Name, DNSSEC, Type, Serial, Primary, Account, Actions. A message 'No data available in table' is displayed. At the bottom of the table are 'Previous' and 'Next' buttons. The footer of the page says 'PowerDNS-Admin - A PowerDNS web interface with advanced features.' and 'Version 0.4.2'.

4

On PowerDNS-Admin, click Create Zone and enter "[cscat.tw](#)" for the zone name, then click Create Zone on the bottom.

Click Dashboard, and click [cscat.tw](#).

Add a record:

- Name: www
- Type: CNAME
- Status: Active
- TTL: 60 minutes (3600)
- Data: [cscat.tw](#).
- Comment: Redirect www to the main domain

```
root@vbox:~# dig @127.0.0.1 -p 5301 www.cscat.tw
; <>> DiG 9.18.33-1~deb12u2-Debian <>> @127.0.0.1 -p 5301 www.cscat.tw
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 55594
;; 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:
;www.cscat.tw.           IN      A

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

;; Query time: 0 msec
;; SERVER: 127.0.0.1#5301(127.0.0.1) (UDP)
;; WHEN: Sat Mar 29 15:14:35 CST 2025
;; MSG SIZE rcvd: 71

root@vbox:~#
```

Add a record:

- Name: (blank)
- Type: A
- Status: Active
- TTL: 60 minutes (3600)
- Data: 192.0.2.1
- Comment: [cscat.tw](#) to 192.0.2.1

```
3027                               ssh -p 3027 root@localhost...
root@vbox:~# dig @127.0.0.1 -p 5301 cscat.tw
; <>> DiG 9.18.33-1~deb12u2-Debian <>> @127.0.0.1 -p 5301 cscat.tw
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>>HEADER<<- opcode: QUERY, status: NOERROR, id: 3499
;; 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: 127.0.0.1#5301(127.0.0.1) (UDP)
;; WHEN: Sat Mar 29 15:15:50 CST 2025
;; MSG SIZE  rcvd: 53

root@vbox:~#
```

Add a record:

- Name: (blank)
- Type: MX
- Status: Active
- TTL: 60 minutes (3600)
- Data: 10 mail.cscat.tw.
- Comment: Mail server for cscat.tw

```
3027          ssh -p 3027 root@localhost...
root@vbox:~# dig @127.0.0.1 -p 5301 cscat.tw MX
; <>> DiG 9.18.33-1~deb12u2-Debian <>> @127.0.0.1 -p 5301 cscat.tw MX
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 28117
;; 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: 4 msec
;; SERVER: 127.0.0.1#5301(127.0.0.1) (UDP)
;; WHEN: Sat Mar 29 15:16:33 CST 2025
;; MSG SIZE  rcvd: 58

root@vbox:~#
```

Add a record:

- Name: (blank)
- Type: TXT
- Status: Active
- TTL: 60 minutes (3600)
- Data: "v=spf1 mx -all"
- Comment: For legal reasons

```
3027          ssh -p 3027 root@localhost...
root@vbox:~# dig @127.0.0.1 -p 5301 cscat.tw TXT
; <>> DiG 9.18.33-1~deb12u2-Debian <>> @127.0.0.1 -p 5301 cscat.tw TXT
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 21939
;; 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: 127.0.0.1#5301(127.0.0.1) (UDP)
;; WHEN: Sat Mar 29 15:17:45 CST 2025
;; MSG SIZE rcvd: 64
root@vbox:~#
```

Add a record:

- Name: api
- Type: A
- Status: Active
- TTL: 60 minutes (3600)
- Data: 192.0.2.4
- Comment: ipv4 for api

```
3027          ssh -p 3027 root@localhost...
root@vbox:~# dig @127.0.0.1 -p 5301 api.cscat.tw A
; <>> DiG 9.18.33-1~deb12u2-Debian <>> @127.0.0.1 -p 5301 api.cscat.tw A
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 64419
;; 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: 0 msec
;; SERVER: 127.0.0.1#5301(127.0.0.1) (UDP)
;; WHEN: Sat Mar 29 15:18:23 CST 2025
;; MSG SIZE  rcvd: 57

root@vbox:~#
```

Add a record:

- Name: api
- Type: AAAA
- Status: Active
- TTL: 60 minutes (3600)
- Data: 2001:db8::50
- Comment: ipv6 for api

```
3027                               ssh -p 3027 root@localhost...
root@vbox:~# dig @127.0.0.1 -p 5301 api.cscat.tw AAAA
; <>> DiG 9.18.33-1~deb12u2-Debian <>> @127.0.0.1 -p 5301 api.cscat.tw AAAA
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 10981
;; 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: 127.0.0.1#5301(127.0.0.1) (UDP)
;; WHEN: Sat Mar 29 15:18:44 CST 2025
;; MSG SIZE  rcvd: 69

root@vbox:~#
```

Add a record:

- Name: store2
- Type: NS
- Status: Active
- TTL: 60 minutes (3600)
- Data: [dns2.cscat.tw](#).
- Comment: Delegate [store2.cscat.tw](#) to [dns2.cscat.tw](#)

```
3027          ssh -p 3027 root@localhost...
root@vbox:~# dig @127.0.0.1 -p 5301 store2.cscat.tw NS
; <>> DiG 9.18.33-1~deb12u2-Debian <>> @127.0.0.1 -p 5301 store2.cscat.tw NS
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 51141
;; 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.      3600    IN      NS      dns2.cscat.tw.

;; Query time: 0 msec
;; SERVER: 127.0.0.1#5301(127.0.0.1) (UDP)
;; WHEN: Sat Mar 29 15:19:51 CST 2025
;; MSG SIZE  rcvd: 63

root@vbox:~#
```

5

DNSSEC is designed to protect users from attacks such as DNS spoofing (cache poisoning) by ensuring that the received DNS data is authentic and has not been tampered with. It works by signing DNS records with a private key, creating a digital signature. DNS clients can then verify the signature by the public key.

Put this in /etc/powerdns/pdns.conf:

```
gmysql-dnssec=yes
```

Go back to the web browser and click Dashboard, and then click the locked symbol under DNSSEC for [cscat.tw](#). Click Enable.

```
3027                               ssh -p 3027 root@localhost...
root@vbox:~# dig @127.0.0.1 -p 5301 cscat.tw DNSKEY
; <>> DiG 9.18.33-1~deb12u2-Debian <>> @127.0.0.1 -p 5301 cscat.tw DNSKEY
; (1 server found)
;; global options: +cmd
;; Got answer:
;; -->HEADER<- opcode: QUERY, status: NOERROR, id: 27327
;; 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 xIeILOApbdEFucu/7vZL7wVgxZSHxXBiOMd541fUwD1FG6DWqwBp8eir VTkxM63i2oxMYr6q/IS1TXtA4Gjx2Q==

;; Query time: 0 msec
;; SERVER: 127.0.0.1#5301(127.0.0.1) (UDP)
;; WHEN: Sat Mar 29 15:49:09 CST 2025
;; MSG SIZE  rcvd: 117
root@vbox:~#
```

2 PowerDNS Recursor

References

- B12902116 (林靖昀)
- B12902066 (宋和峻)
- <https://www.cloudns.net/blog/authoritative-dns-server/>
- <https://www.debian-tutorials.com/installing-powerdns-recursor/>
- <https://doc.powerdns.com/recursor/settings.html>
- <https://www.workswiththeweb.com/dns/2022/02/17/Setup-PowerDNS-Recursor/>
- <https://doc.powerdns.com/recursor/dnssec.html>

0 Basic

1.

我不知道什麼是“authoritive server”，但我知道什麼是“authoritative server”

An Authoritative server provides definitive answers to DNS queries, such as mail server IP address or web site IP address (A resource record).

2.

Recursive DNS query is a kind of DNS query where DNS servers will help complete the query if it can't answer. Iterative DNS query is a kind of DNS query where DNS servers will tell the client the next DNS server the client can query if can't answer.

For recursive, the client load is lower, but the server load is higher.

For iterative, the client load is higher, but the server load is lower.

1 Setting up PowerDNS Recursor

1

```
apt-get install pdns-recursor
```

Put this in /etc/powerdns/recursor.conf

```
local-address=0.0.0.0
local-port=10053
max-cache-ttl=300
forward-zones-file=/opt/web/powerdns-admin/recursor.conf
dnssec=validate
```

put this in /opt/web/powerdns-admin/recursor.conf

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

```
systemctl restart pdns-recursor
```

2

```
dig @127.0.0.1 -p 10053 google.com
```

```
root@vbox:~# dig @127.0.0.1 -p 10053 google.com  
3027  
; <>> 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: 8162  
;; 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 142.250.204.46  
  
;; Query time: 48 msec  
;; SERVER: 127.0.0.1#10053(127.0.0.1) (UDP)  
;; WHEN: Sat Mar 29 20:21:04 CST 2025  
;; MSG SIZE rcvd: 55  
root@vbox:~#
```

3

```
3027
root@vbox:~# 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: 53744
;; 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: 3032 msec
;; SERVER: 127.0.0.1#10053(127.0.0.1) (UDP)
;; WHEN: Sat Mar 29 20:22:12 CST 2025
;; MSG SIZE rcvd: 37
root@vbox:~#
```

Because it can't validate DNSSEC.

4

```
pdnsutil show-zone cscat.tw
```

Result

```
Mar 29 20:36:22 [bindbackend] Done parsing domains, 0 rejected, 0 new, 0 removed
This is a Native zone
Metadata items:
    API-RECTIFY      1
    SOA-EDIT-API     DEFAULT
Zone has NSEC semantics
keys:
ID = 2 (CSK), flags = 257, tag = 8052, algo = 13, bits = 256      Active      Publish
CSK DNSKEY = cscat.tw. IN DNSKEY 257 3 13 x1EIL0ApbdEFucu/7vZL7wVgxZSHxXBIoMd54lfUwD1FG6D
DS = cscat.tw. IN DS 8052 13 2 02c0a42f3ffb56019ab0dcadff75146a0140965e5c9b329375b00fbf96
DS = cscat.tw. IN DS 8052 13 4 16e3ef3cab47b10822da8ea0d3e6ceb48919b638885bc18c10c8d2ffef
```

Copy the DS shown in the result to /etc/powerdns/recursor.lua with this:

```
addTA('cscat.tw', "8052 13 2 02c0a42f3ff56019ab0dcadff75146a0140965e5c9b329375b00fbf96ac
```

The terminal window shows the output of a `dig` command. The command is `dig @127.0.0.1 -p 10053 cscat.tw`. The output shows a single answer from a local DNS server (127.0.0.1). The response is a Type A record for `cscat.tw` with an IP address of 192.0.2.1 and a TTL of 300 seconds. The query took 4 msec. The command was run by root (@vbox:~#).

```
root@vbox:~# 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: 2864
;; 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: 4 msec
;; SERVER: 127.0.0.1#10053(127.0.0.1) (UDP)
;; WHEN: Sat Mar 29 20:46:29 CST 2025
;; MSG SIZE  rcvd: 53
root@vbox:~#
```

5

If the TTL of cache is too big, then configuration updates may take a long time to become effective. If it is too small, then the cache will have to update constantly, consuming network resources.

6

1. The attacker first send a query to the victim DNS server asking for a subdomain that doesn't exist, such as `fake.example.com`.
2. The victim DNS server asks another DNS server for this record, but the attacker forges a response.
3. The fake response includes an NS record that includes the whole zone `example.com`.
4. The victim DNS server stores the fake response in its cache.
5. Any other queries from now on to the victim DNS server will be directed to the attacker's DNS server.
6. The attacker's DNS server can respond with any fake answers for incoming queries.

2 Security

1

This is to prevent cache poisoning attacks.

If we allow recursive queries for untrusted clients, then it poses a risk of cache poisoning attacks:

1. The attacker first send a query to the victim DNS server asking for a subdomain that doesn't exist, such as `fake.example.com`.
2. The victim DNS server asks another DNS server for this record, but the attacker forges a response.
3. The fake response includes an NS record that includes the whole zone `example.com`.
4. The victim DNS server stores the fake response in its cache.
5. Any other queries from now on to the victim DNS server will be directed to the attacker's DNS server.
6. The attacker's DNS server can respond with any fake answers for incoming queries.

2

Put this in /etc/powerdns/recursor.conf

```
allow-from=127.0.0.1/32, 10.0.2.0/24
```

3 dnsdist

References

- B12902116 (林靖昀)
- B12902066 (宋和峻)
- <https://www.dnsdist.org/install.html>
- <https://www.dnsdist.org/quickstart.html#dnsdist-console-and-configuration>
- <https://www.dnsdist.org/guides/downstreams.html>
- <https://www.dnsdist.org/advanced/acl.html>
- <https://www.dnsdist.org/guides/serverpools.html>
- <https://www.dnsdist.org/reference/selectors.html>
- <https://www.cloudflare.com/learning/dns/dns-over-tls/>

1 Setting up dnsdist

1

```
apt-get install -y dnsdist
```

Put this in /etc/dnsdist/dnsdist.conf

```
newServer("127.0.0.1:10053")
newServer("8.8.8.8")
```

```
systemctl restart dnsdist
dig @127.0.0.1 -p 53 cscat.tw
dig @127.0.0.1 -p 53 google.com
```

```

3027
root@vbox:~# dig @127.0.0.1 -p 53 cscat.tw
; <>> Dig 9.18.33-1~deb12u2-Debian <>> @127.0.0.1 -p 53 cscat.tw
; (1 server found)
;; global options: +cmd
;; Got answer:
;; -->HEADER<- opcode: QUERY, status: NXDOMAIN, id: 11583
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

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

;; AUTHORITY SECTION:
tw.          900     IN      SOA     a.dns.tw. snw.twnic.net.tw. 2010925209 3600 900 1296000 900

;; Query time: 112 msec
;; SERVER: 127.0.0.1#53(127.0.0.1) (UDP)
;; WHEN: Sun Mar 30 00:40:57 CST 2025
;; MSG SIZE rcvd: 93

|root@vbox:~# 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: 43993
;; 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.    237     IN      A       142.250.66.78

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1) (UDP)
;; WHEN: Sun Mar 30 00:40:59 CST 2025
;; MSG SIZE rcvd: 55

root@vbox:~#

```

2

Put this in /etc/dnsdist/dnsdist.conf

```

addAction(
    QTypeRule(16),
    LuaAction(function(dq)
        if dq.qname:toString():len() > 70 then
            return DNSAction.Drop
        end
        return DNSAction.None
    end)
)

local dbr = dynBlockRulesGroup()
dbr:setQueryRate(20, 10, "Exceeded query rate", 60)

function maintenance()
    dbr:apply()
end

addAction(QNameRule("csdog.tw"), DropAction())
local suf = newSuffixMatchNode()
suf:add("csdog.tw")
addAction(SuffixMatchNodeRule(suf), DropAction())

```

```
systemctl restart dnsdist
```

2 DNS-over-TLS

1

Setting DNS-over-TLS can enhance privacy and security. DNS-over-TLS sends queries encrypted, preventing from man-in-the-middle attacks.

Aspects	DNS-over-HTTPS	DNS-over-TLS
Encryption	HTTPS (HTTP over TLS)	TLS
Performance	worse due to network stack overhead	better due to less network stack overhead
Security	Better; gives network administrators the ability to monitor and block DNS queries	Worse; traffic hidden in regular HTTPS traffic, meaning they cannot easily be blocked without blocking all other HTTPS traffic as well

2

```
openssl genpkey -algorithm RSA -out /etc/ssl/private/dnsdist.key  
openssl req -new -key /etc/ssl/private/dnsdist.key -out /etc/ssl/private/dnsdist.csr
```

Country Name (2 letter code) [AU]:TW

State or Province Name (full name) [Some-State]:Taipei

Locality Name (eg, city) []:Taipei City

Organization Name (eg, company) [Internet Widgits Pty Ltd]:Anthony

Organizational Unit Name (eg, section) []:Anthony

Common Name (e.g. server FQDN or YOUR name) []:cscat.tw

Email Address []:b12902118@ntu.edu.tw

Please enter the following 'extra' attributes

to be sent with your certificate request

A challenge password []:anthony

An optional company name []:anthony

```
openssl x509 -req -in /etc/ssl/private/dnsdist.csr -signkey /etc/ssl/private/dnsdist.key  
cat /etc/ssl/certs/dnsdist.crt /etc/ssl/private/dnsdist.key > /etc/ssl/certs/dnsdist.pem
```

Put this in /etc/dnsdist/dnsdist.conf

```
addTLSLocal('0.0.0.0', '/etc/ssl/certs/dnsdist.pem', '/etc/ssl/private/dnsdist.key')
```

```
dnsdist -v
```

3

```
3027
root@vbox:~# 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: 43658
;; 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.        79     IN      A      192.0.2.1

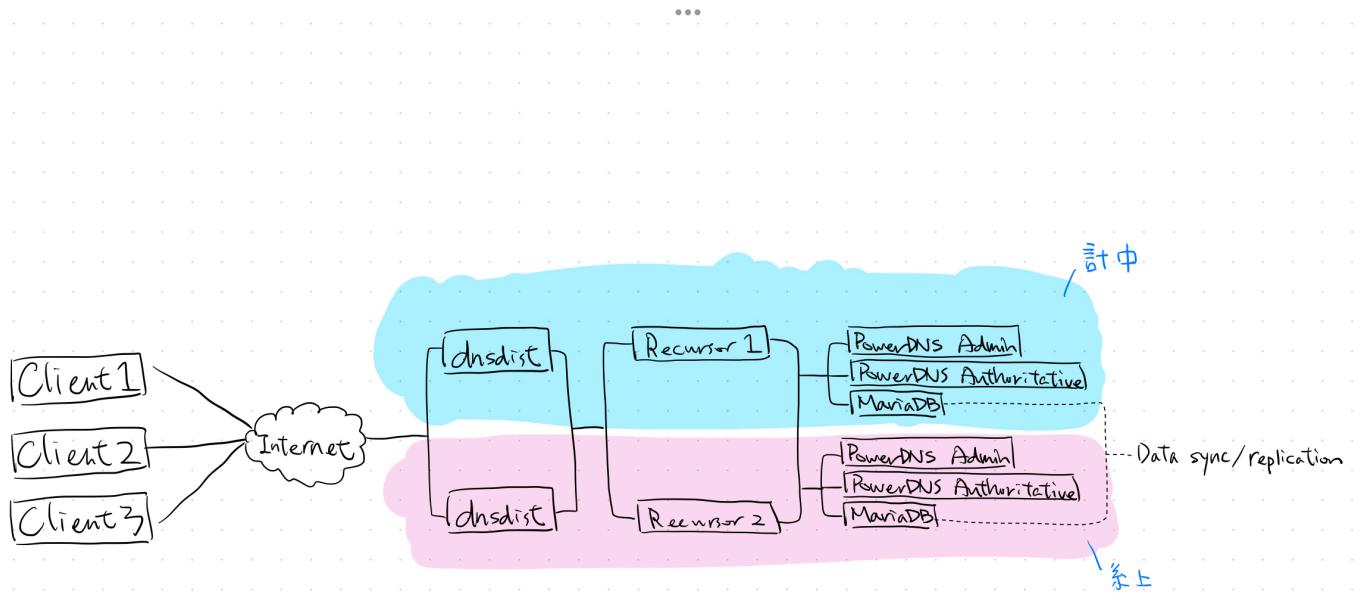
;; Query time: 4 msec
;; SERVER: 127.0.0.1#853(127.0.0.1) (TLS)
;; WHEN: Sun Mar 30 03:17:59 CST 2025
;; MSG SIZE rcvd: 53
root@vbox:~#
```

4 Master and Slave

References

- B12902116 (林靖昀)
- B12902066 (宋和峻)
- <https://blog.csdn.net/homedesk/article/details/77989241>

1



- If any server is down, there is always another one that can still function.
- If all machines are down in CSIE, there are still a fully functional set at Computer and Information Networking Center.
- If DNS records are all gone on one machine, the other can be used as a backup

2

AXFR (Authoritative Zone Transfer) transfers full zone information from one DNS server to another whenever there is an update. IXFR (Incremental Zone Transfer) only transfers the updated part. AXFR is suitable for big zone updates or initial deployment. IXFR is suitable for small zone updates.