NASA hw7

Author: B12705014陳泊華

Question 1

1. DNS (Domain Name Server) 指網域名稱系統，將人們可讀取的網域名稱轉換為機器可讀取的IP地址

2. DDNS（Dynamic Domain Name System）指動態域名系統，使用戶可以使用一個固定的域名來訪問其網絡服務，而無需擔心IP地址的變化

3. 目前共有13台name server，分散在世界各地，負責返回頂級域的權威域名伺服器位址

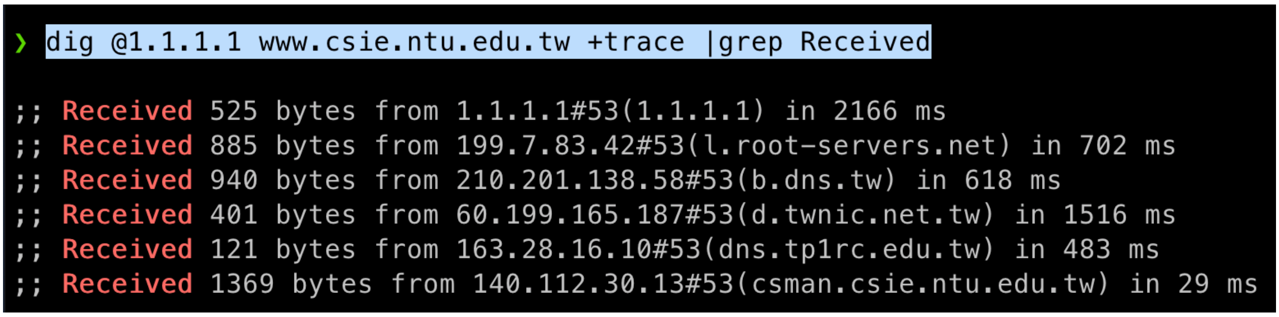
4. TXT records的其中一個應用是SPF記錄（Sender Policy Framework），利用DNS記錄來驗證發件人電子郵件地址的可信度，防止電子郵件地址偽造

references:
(i) https://www.cloudflare.com/zh-tw/learning/dns/dns-records/dns-txt-record/ (https://www.cloudflare.com/zh-tw/learning/dns/dns-records/dns-txt-record/)
(ii) https://zh.wikipedia.org/zh-tw/根網域名稱伺服器 (https://zh.wikipedia.org/zh-tw/%E6%A0%B9%E7%B6%B2%E5%9F%9F%E5%90%8D%E7%A8%B1%E4%BC%BA%E6%9C%8D%E5%99%A8)

Question 2

利用dig指令+trace追蹤query path，並用grep篩選結果

```
$ dig @1.1.1.1 www.csie.ntu.edu.tw +trace |grep Received
```



```
❯ dig @1.1.1.1 www.csie.ntu.edu.tw +trace |grep Received

;; Received 525 bytes from 1.1.1.1#53(1.1.1.1) in 2166 ms
;; Received 885 bytes from 199.7.83.42#53(l.root-servers.net) in 702 ms
;; Received 940 bytes from 210.201.138.58#53(b.dns.tw) in 618 ms
;; Received 401 bytes from 60.199.165.187#53(d.twnic.net.tw) in 1516 ms
;; Received 121 bytes from 163.28.16.10#53(dns.tp1rc.edu.tw) in 483 ms
;; Received 1369 bytes from 140.112.30.13#53(csman.csie.ntu.edu.tw) in 29 ms
```

Question 3

DNS架構

- 軟體：根據需求選擇適合的軟體，如UI較完善的powerDNS，或功能強大且廣泛使用的BIND
- 地理位置：為了分散風險和提高可用性，可以將name server分散在多個地理位置，同時也注意是否在距離上取得平衡，減少延遲並提高解析速度
- 網路位置：可以使用冗余網路，增加網路的可靠性和容錯能力
- 監控和管理：配置日誌記錄和警報系統以即時發現和解決潛在的問題
- 安全性：使用DNSSEC技術對域名進行簽名，提供身份驗證和數據完整性保護

如果今天其中一台伺服器壞掉了怎麼辦?

- 部署多個DNS伺服器並配置為相互備份，以確保即使一台伺服器故障，其他伺服器仍可提供服務
- 使用負載均衡器將流量分發到多個伺服器，以提高可用性和性能

如果今天系館停電導致所有機房下線怎麼辦?

- 配置備用電源和UPS（不間斷電源）以確保伺服器在停電時能夠繼續運行
- 將DNS伺服器部署在不同的機房或地理位置，以減少單點故障的影響

如果因為某些原因導致伺服器上的 DNS records 不見了怎麼辦?

- 定期備份DNS記錄，並在需要時恢復備份以恢復丟失的記錄
- 使用版本控制系統（如Git）來跟踪DNS配置的更改，並且定期進行配置備份

有些實驗室想要擁有自己的 subdomain，該如何實現?

- 配置DNS伺服器以支持子域名，並為每個實驗室分配獨立的子域名
- 在DNS伺服器上設置適當的區域檔案和記錄以支持子域名解析

如何應對 DNS flooding attack?

- 利用ACL來限制陌生請求
- 利用DNSSEC技術進行驗證
- 可以限制來自"ANY" source的請求次數，搭配DNS caching

如何應對 DNS amplification attack?

- 禁用 DNS 伺服器上的遞迴查詢或限制遞迴查詢的範圍
- 配置防火牆規則以阻止對 UDP 端口 53 的外部流量，防止反射攻擊

如何確保對 *.csie.ntu.edu.tw 的 query response 不會被攻擊者竄改成 malicious ip 呢?

- 使用DNSSEC技術對*.csie.ntu.edu.tw域名進行簽名，以確保DNS響應的完整性和身份驗證
- 監控DNS伺服器的DNS響應並實時檢測和阻止潛在的DNS欺騙或DNS污染攻擊

reference:
(i) http://dns-learning.twnic.net.tw/dns/02ArchDNS.html (http://dns-learning.twnic.net.tw/dns/02ArchDNS.html)
(ii) https://ppfocus.com/0/di3384bb8.html (https://ppfocus.com/0/di3384bb8.html)
(iii) https://www.cc.ntu.edu.tw/chinese/epaper/0022/20120920_2206.html (https://www.cc.ntu.edu.tw/chinese/epaper/0022/20120920_2206.html)
(iv) https://www.cc.ntu.edu.tw/chinese/epaper/0028/20140320_2808.html (https://www.cc.ntu.edu.tw/chinese/epaper/0028/20140320_2808.html)
(v) https://www.ithome.com.tw/tech/87819 (https://www.ithome.com.tw/tech/87819)
(vi) https://www.catchpoint.com/dns-monitoring/dns-flood (https://www.catchpoint.com/dns-monitoring/dns-flood)
(vii) chatGPT3.5

Question 4

1. PowerDNS

```
$ sudo apt-get install pdns-server
```

按照手冊步驟在Linux VM上安裝powerDNS
https://doc.powerdns.com/authoritative/installation.html (https://doc.powerdns.com/authoritative/installation.html)

```
$ sudo apt-get install pdns-backend-sqlite3
```

按照要求選擇SQLite作為後端
https://packages.debian.org/search?keywords=pdns-backend (https://packages.debian.org/search?keywords=pdns-backend)

編輯pdns.conf檔，新增以下兩行

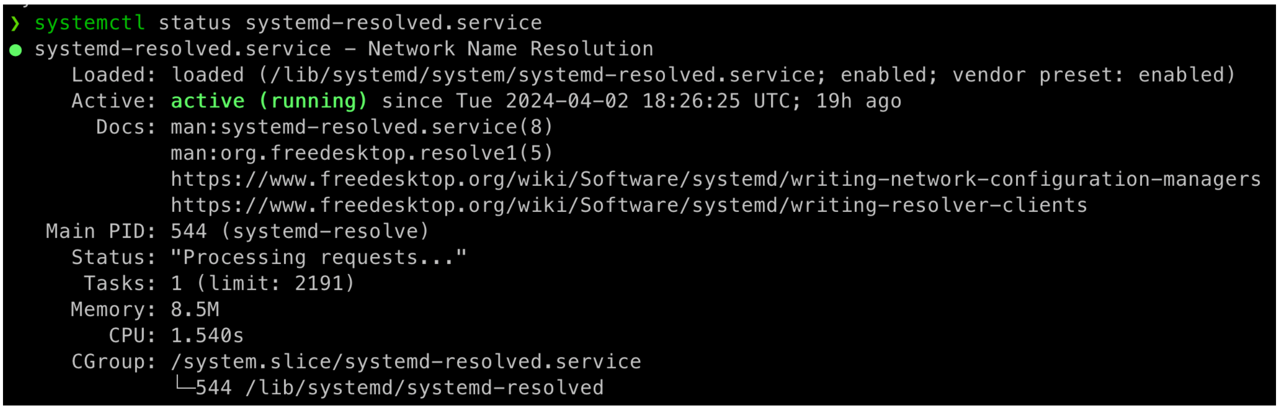
```
$ vim /etc/powerdns/pdns.conf
```

launch=gsqlite3
gsqlite3-database=/var/lib/powerdns/pdns.sqlite3

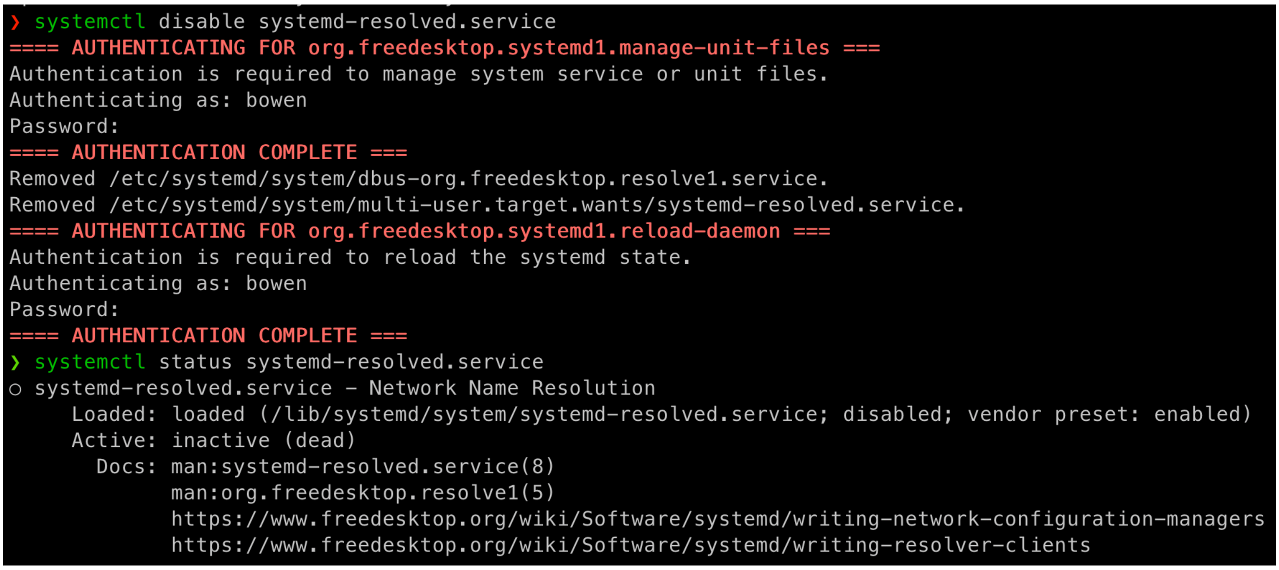
按照Basic setup的指示將sqlite3加入指定路徑

```
$ mkdir /var/lib/powerdns
$ sqlite3 /var/lib/powerdns/pdns.sqlite3 < /usr/share/doc/pdns-backend-sqlite3/schema.sqlite3.sql
$ chown -R pdns:pdns /var/lib/powerdns
```

https://doc.powerdns.com/authoritative/guides/basic-database.html (https://doc.powerdns.com/authoritative/guides/basic-database.html) start失敗，netstat後發現要先關掉原本OS在port 53聽的DNS server

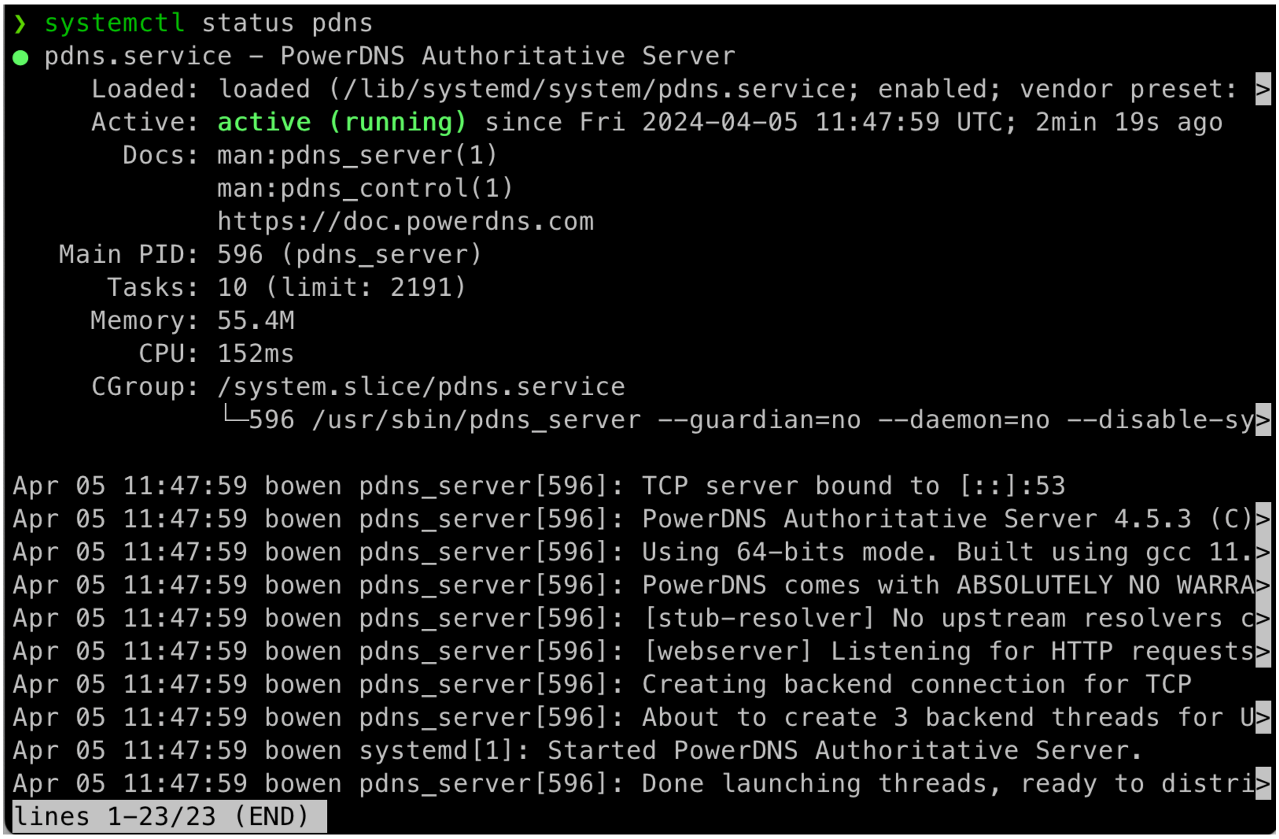


```
❯ systemctl status systemd-resolved.service
● systemd-resolved.service - Network Name Resolution
     Loaded: loaded (/lib/systemd/system/systemd-resolved.service; enabled; vendor preset: enabled)
     Active: active (running) since Tue 2024-04-02 18:26:25 UTC; 19h ago
       Docs: man:systemd-resolved.service(8)
             man:org.freedesktop.resolve1(5)
             https://www.freedesktop.org/wiki/Software/systemd/writing-network-configuration-managers
             https://www.freedesktop.org/wiki/Software/systemd/writing-resolver-clients
   Main PID: 544 (systemd-resolve)
     Status: "Processing requests..."
      Tasks: 1 (limit: 2191)
     Memory: 8.5M
        CPU: 1.540s
     CGroup: /system.slice/systemd-resolved.service
             └─544 /lib/systemd/systemd-resolved
```



```
❯ systemctl disable systemd-resolved.service
==== AUTHENTICATING FOR org.freedesktop.systemd1.manage-unit-files ===
Authentication is required to manage system service or unit files.
Authenticating as: bowen
Password:
==== AUTHENTICATION COMPLETE ===
Removed /etc/systemd/system/dbus-org.freedesktop.resolve1.service.
Removed /etc/systemd/system/multi-user.target.wants/systemd-resolved.service.
==== AUTHENTICATING FOR org.freedesktop.systemd1.reload-daemon ===
Authentication is required to reload the systemd state.
Authenticating as: bowen
Password:
==== AUTHENTICATION COMPLETE ===
❯ systemctl status systemd-resolved.service
○ systemd-resolved.service - Network Name Resolution
     Loaded: loaded (/lib/systemd/system/systemd-resolved.service; disabled; vendor preset: enabled)
     Active: inactive (dead)
       Docs: man:systemd-resolved.service(8)
             man:org.freedesktop.resolve1(5)
             https://www.freedesktop.org/wiki/Software/systemd/writing-network-configuration-managers
             https://www.freedesktop.org/wiki/Software/systemd/writing-resolver-clients
```

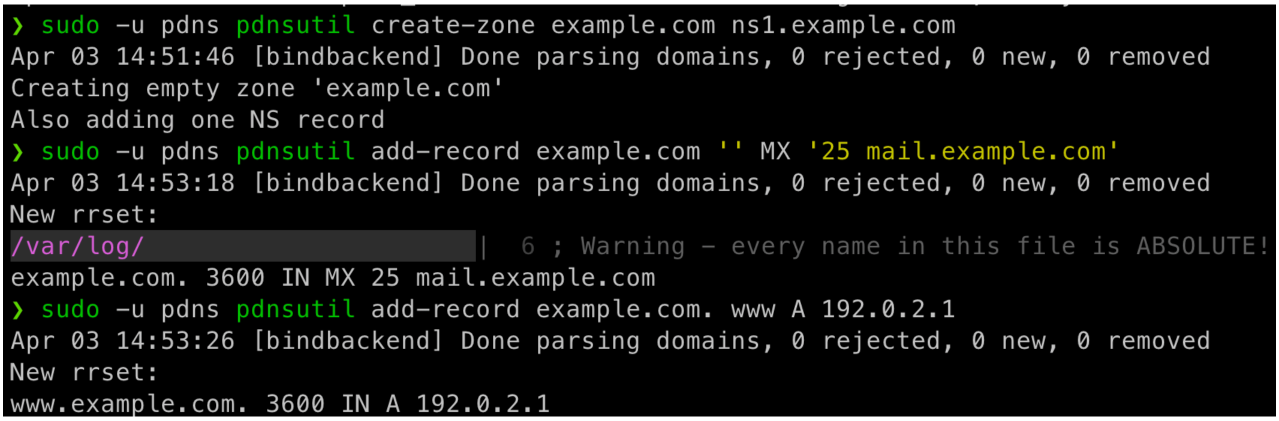
```
$ systemctl start pdns
```



```
❯ systemctl status pdns
● pdns.service - PowerDNS Authoritative Server
     Loaded: loaded (/lib/systemd/system/pdns.service; enabled; vendor preset: >
     Active: active (running) since Fri 2024-04-05 11:47:59 UTC; 2min 19s ago
       Docs: man:pdns_server(1)
             man:pdns_control(1)
             https://doc.powerdns.com
   Main PID: 596 (pdns_server)
      Tasks: 10 (limit: 2191)
     Memory: 55.4M
        CPU: 152ms
     CGroup: /system.slice/pdns.service
             └─596 /usr/sbin/pdns_server --guardian=no --daemon=no --disable-sy>

Apr 05 11:47:59 bowen pdns_server[596]: TCP server bound to [::]:53
Apr 05 11:47:59 bowen pdns_server[596]: PowerDNS Authoritative Server 4.5.3 (C)>
Apr 05 11:47:59 bowen pdns_server[596]: Using 64-bits mode. Built using gcc 11.>
Apr 05 11:47:59 bowen pdns_server[596]: PowerDNS comes with ABSOLUTELY NO WARRA>
Apr 05 11:47:59 bowen pdns_server[596]: [stub-resolver] No upstream resolvers c>
Apr 05 11:47:59 bowen pdns_server[596]: [webserver] Listening for HTTP requests>
Apr 05 11:47:59 bowen pdns_server[596]: Creating backend connection for TCP
Apr 05 11:47:59 bowen pdns_server[596]: About to create 3 backend threads for U>
Apr 05 11:47:59 bowen systemd[1]: Started PowerDNS Authoritative Server.
Apr 05 11:47:59 bowen pdns_server[596]: Done launching threads, ready to distri>
lines 1-23/23 (END)
```

Create zone file and add records

```
$ sudo -u pdns pdnsutil create-zone example.com ns1.example.com
$ sudo -u pdns pdnsutil add-record example.com '' MX '25 mail.example.com'
$ sudo -u pdns pdnsutil add-record example.com. www A 192.0.2.1
```

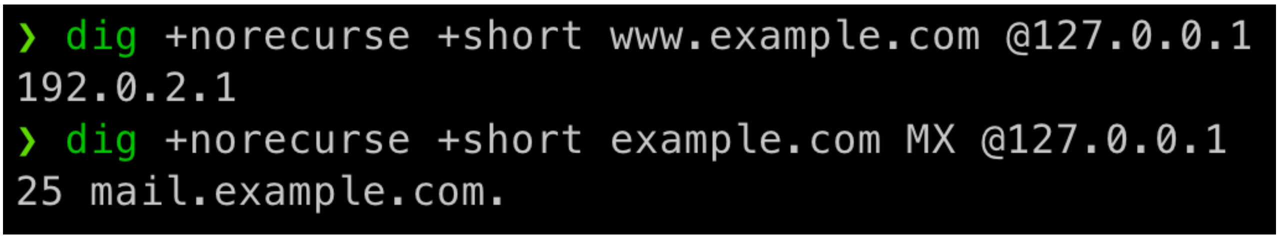


```
❯ sudo -u pdns pdnsutil create-zone example.com ns1.example.com
Apr 03 14:51:46 [bindbackend] Done parsing domains, 0 rejected, 0 new, 0 removed
Creating empty zone 'example.com'
Also adding one NS record
❯ sudo -u pdns pdnsutil add-record example.com '' MX '25 mail.example.com'
Apr 03 14:53:18 [bindbackend] Done parsing domains, 0 rejected, 0 new, 0 removed
New rrset:
/var/log/                          |  6 ; Warning - every name in this file is ABSOLUTE!
example.com. 3600 IN MX 25 mail.example.com
❯ sudo -u pdns pdnsutil add-record example.com. www A 192.0.2.1
Apr 03 14:53:26 [bindbackend] Done parsing domains, 0 rejected, 0 new, 0 removed
New rrset:
www.example.com. 3600 IN A 192.0.2.1
```

dig: recursion requested but not available

solved: +norecurse

```
$ dig +norecurse +short www.example.com @127.0.0.1
```



```
❯ dig +norecurse +short www.example.com @127.0.0.1
192.0.2.1
❯ dig +norecurse +short example.com MX @127.0.0.1
25 mail.example.com.
```

dig得到正常回應，成功架設powerDNS！

2. PowerDNS-Admin

在VM上從Docker Hub安裝Docker

```
# Add Docker's official GPG key:
$ sudo apt-get update
$ sudo apt-get install ca-certificates curl
$sudo install -m 0755 -d /etc/apt/keyrings
$ sudo curl -fsSL https://download.docker.com/linux/ubuntu/gpg -o /etc/apt
$ sudo chmod a+r /etc/apt/keyrings/docker.asc

# Add the repository to Apt sources:
echo \
  "deb [arch=$(dpkg --print-architecture) signed-by=/etc/apt/keyrings/dock
  $(. /etc/os-release && echo "$VERSION_CODENAME") stable" | \
  sudo tee /etc/apt/sources.list.d/docker.list > /dev/null
sudo apt-get update
```

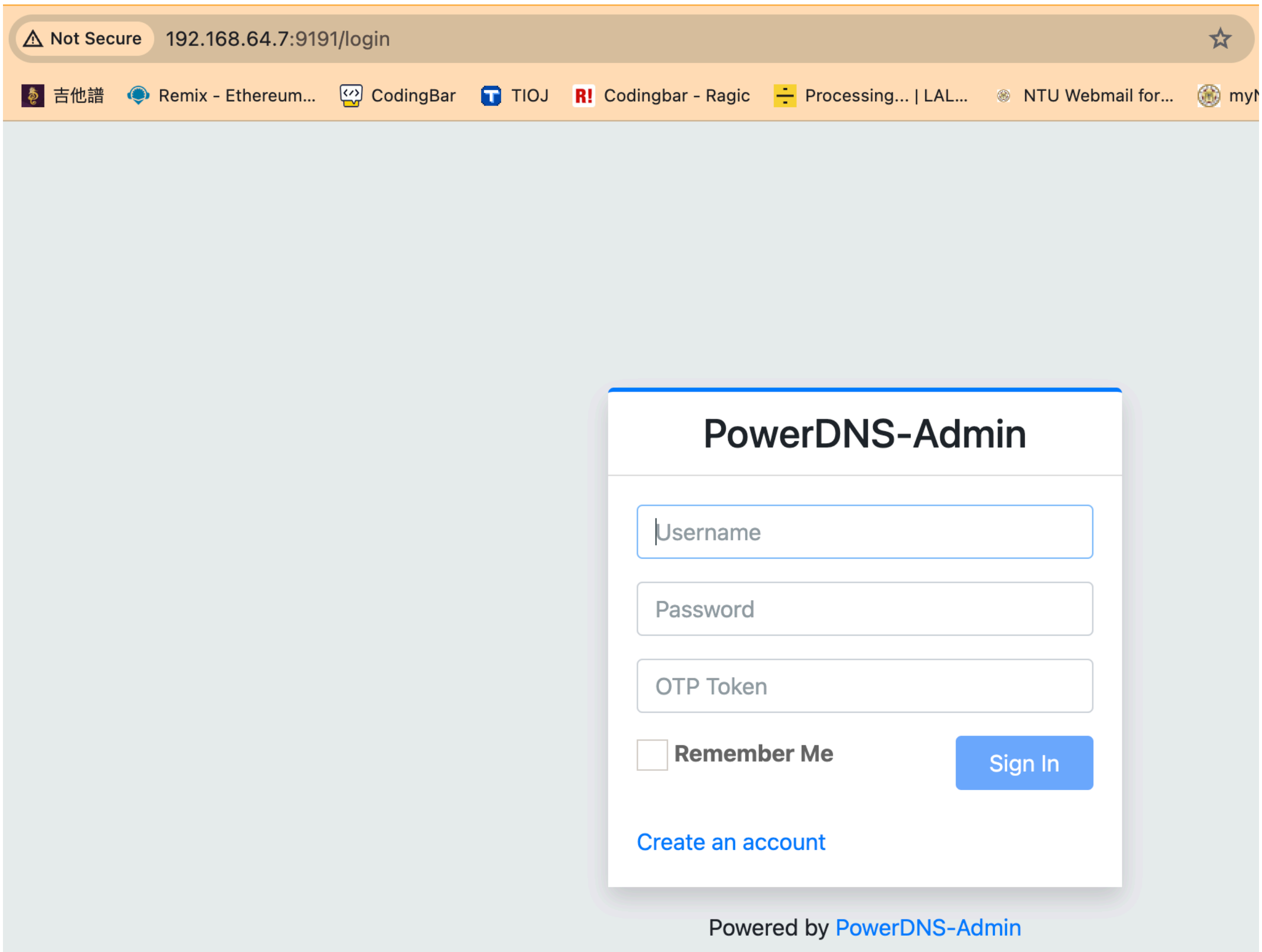
reference: https://docs.docker.com/engine/install/ubuntu/ (https://docs.docker.com/engine/install/ubuntu/)

從Docker Hub安裝PowerDNS Admin

```
$ docker run -d \
    -e SECRET_KEY='XXXXXXX' \
    -v pda-data:/data \
    -p 9191:80 \
    powerdnsadmin/pda-legacy:latest
```

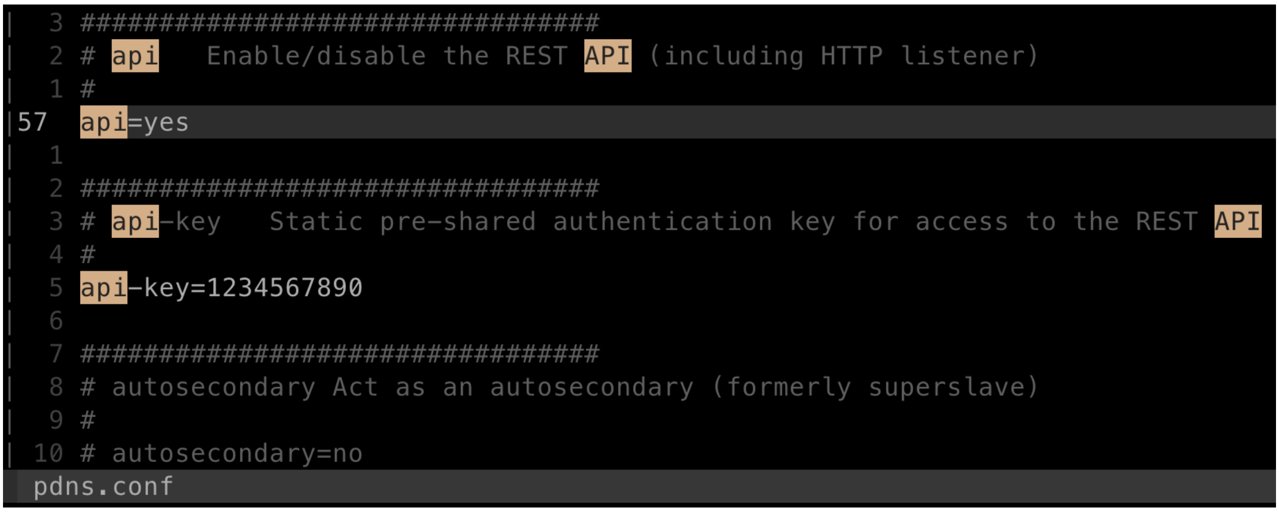
reference: https://github.com/PowerDNS-Admin/PowerDNS-Admin?tab=readme-ov-file (https://github.com/PowerDNS-Admin/PowerDNS-Admin?tab=readme-ov-file)

從瀏覽器連進PowerDNS Admin的WebUI
`http://192.168.64.7:9191/`



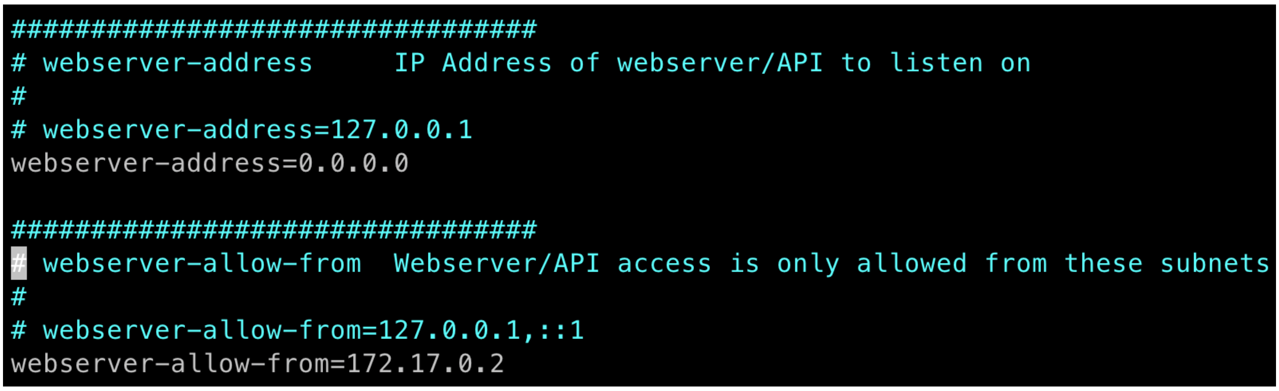
修改api設定

```
$ sudo vim /etc/powerdns/pdns.conf
```



```
#################################
# api   Enable/disable the REST API (including HTTP listener)
#
api=yes

#################################
# api-key   Static pre-shared authentication key for access to the REST API
#
api-key=1234567890

#################################
# autosecondary Act as an autosecondary (formerly superslave)
#
# autosecondary=no
pdns.conf
```

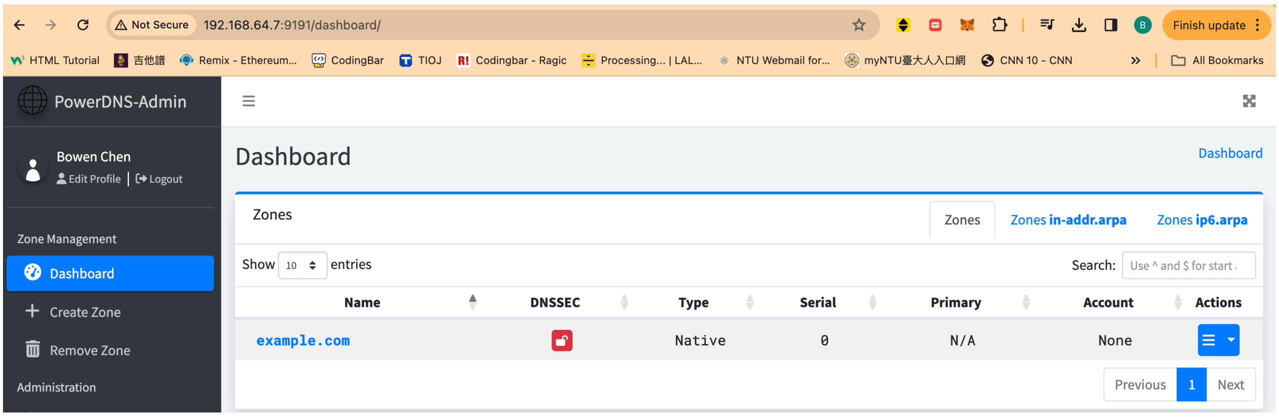
修改access control, listen ip讓PowerDNS Admin可以連到VM上跑的PowerDNS server(預設只聽localhost)



```
#################################
# webserver-address     IP Address of webserver/API to listen on
#
# webserver-address=127.0.0.1
webserver-address=0.0.0.0

#################################
# webserver-allow-from  Webserver/API access is only allowed from these subnets
#
# webserver-allow-from=127.0.0.1,::1
webserver-allow-from=172.17.0.2
```

reference:
(i) https://doc.powerdns.com/md/httpapi/README/ (https://doc.powerdns.com/md/httpapi/README/)
(ii) https://doc.powerdns.com/authoritative/http-api/ (https://doc.powerdns.com/authoritative/http-api/)

檢查PowerDNS Admin的Dashboard，成功看到PowerDNS裡的example.com (http://xn--PowerDNSexample-1e7y57c7w8kyhve4gc4v5m.com) domain name



Dashboard

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

Show 10 entries Search: Use ^ and $ for start

Name	DNSSEC	Type	Serial	Primary	Account	Actions
example.com		Native	0	N/A	None	

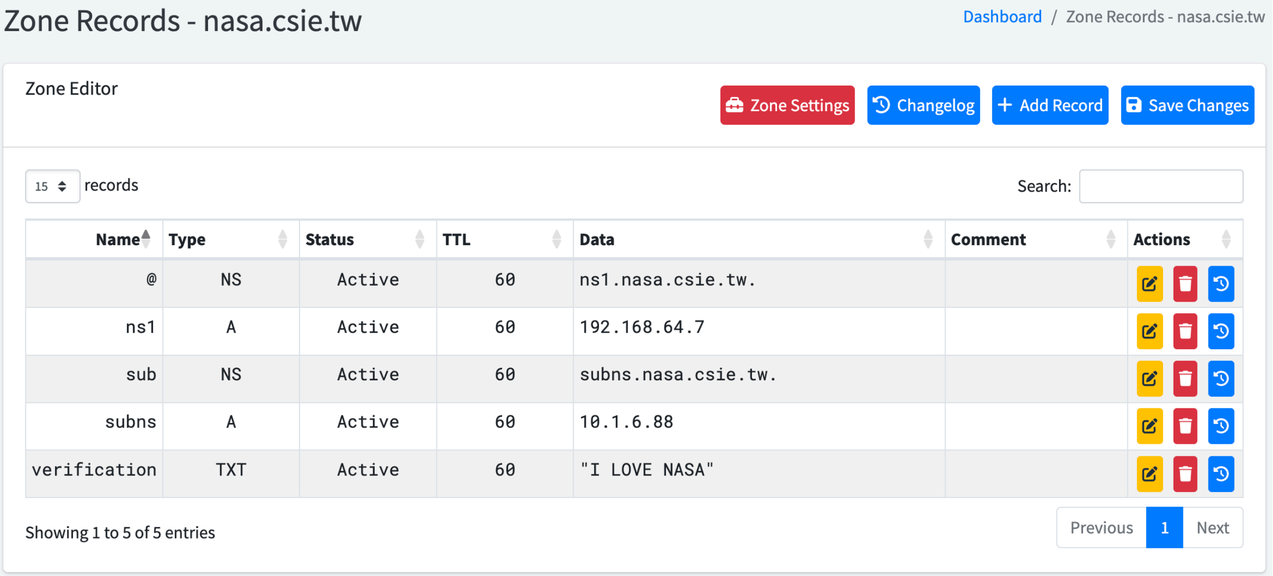
Previous 1 Next

3. Add Records

1. 先設定nasa.csie.tw這個網域的name server (NS record) 和其IP (A record)

2. 根據題目要求分別設定verification的TXT record、sub的name server和subns的IP (A record)

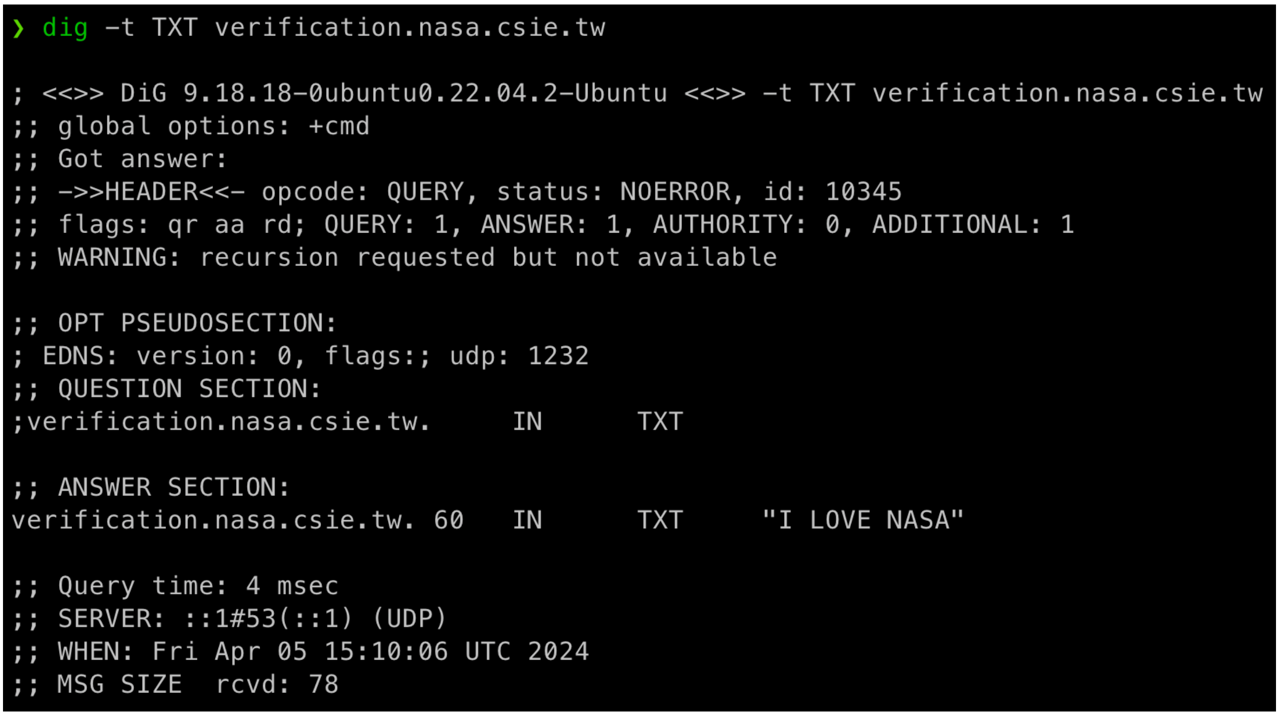
Zone Records設定截圖



Zone Records - nasa.csie.tw

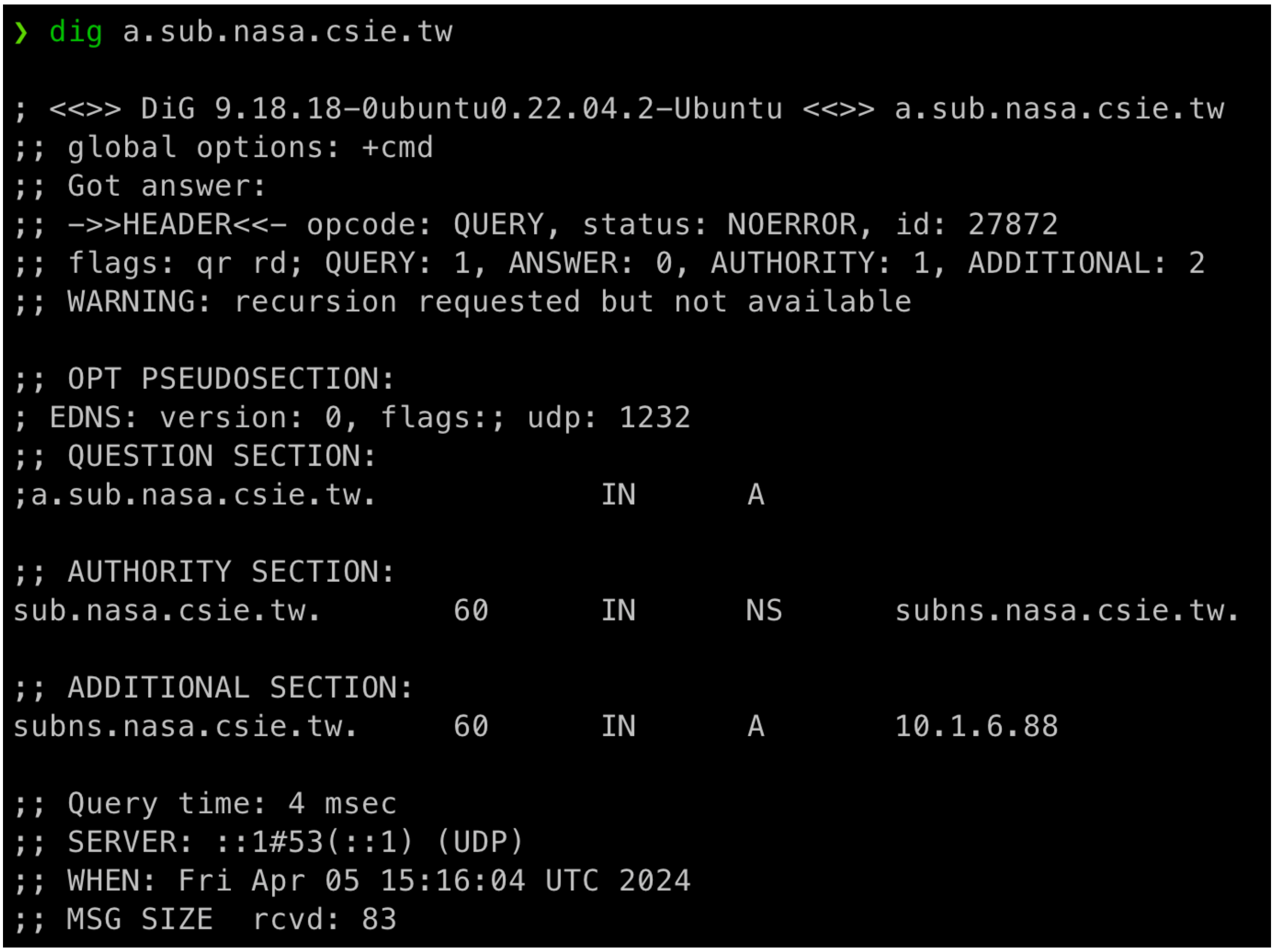
Name	Type	Status	TTL	Data	Comment	Actions
@	NS	Active	60	ns1.nasa.csie.tw.		
ns1	A	Active	60	192.168.64.7		
sub	NS	Active	60	subns.nasa.csie.tw.		
subns	A	Active	60	10.1.6.88		
verification	TXT	Active	60	"I LOVE NASA"		

$ dig -t TXT verification.nasa.csie.tw



```
❯ dig -t TXT verification.nasa.csie.tw

; <<>> DiG 9.18.18-0ubuntu0.22.04.2-Ubuntu <<>> -t TXT verification.nasa.csie.tw
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 10345
;; 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:
;verification.nasa.csie.tw.     IN      TXT

;; ANSWER SECTION:
verification.nasa.csie.tw. 60   IN      TXT     "I LOVE NASA"

;; Query time: 4 msec
;; SERVER: ::1#53(::1) (UDP)
;; WHEN: Fri Apr 05 15:10:06 UTC 2024
;; MSG SIZE  rcvd: 78
```

```
$ dig a.sub.nasa.csie.tw
```



```
❯ dig a.sub.nasa.csie.tw

; <<>> DiG 9.18.18-0ubuntu0.22.04.2-Ubuntu <<>> a.sub.nasa.csie.tw
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 27872
;; 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:
;a.sub.nasa.csie.tw.            IN      A

;; AUTHORITY SECTION:
sub.nasa.csie.tw.       60      IN      NS      subns.nasa.csie.tw.

;; ADDITIONAL SECTION:
subns.nasa.csie.tw.     60      IN      A       10.1.6.88

;; Query time: 4 msec
;; SERVER: ::1#53(::1) (UDP)
;; WHEN: Fri Apr 05 15:16:04 UTC 2024
;; MSG SIZE  rcvd: 83
```

reference:
(i) https://doc.powerdns.com/zonecontrol/latest/PowerDNSZoneControlAdmin.pdf
(https://doc.powerdns.com/zonecontrol/latest/PowerDNSZoneControlAdmin.pdf)
(ii) https://blueskyson.github.io/2021/05/24/bind9-setup/
(https://blueskyson.github.io/2021/05/24/bind9-setup/)
(iii) Lab 7 slides