

QUẢN LÝ DNS SERVER BẰNG BASH SCRIPT

I. GIỚI THIỆU

Script này được viết để tự động hóa việc cài đặt, cấu hình và quản lý BIND DNS Server trên hệ điều hành CentOS.

Mục tiêu của script là giúp người dùng dễ dàng thực hiện các tác vụ sau:

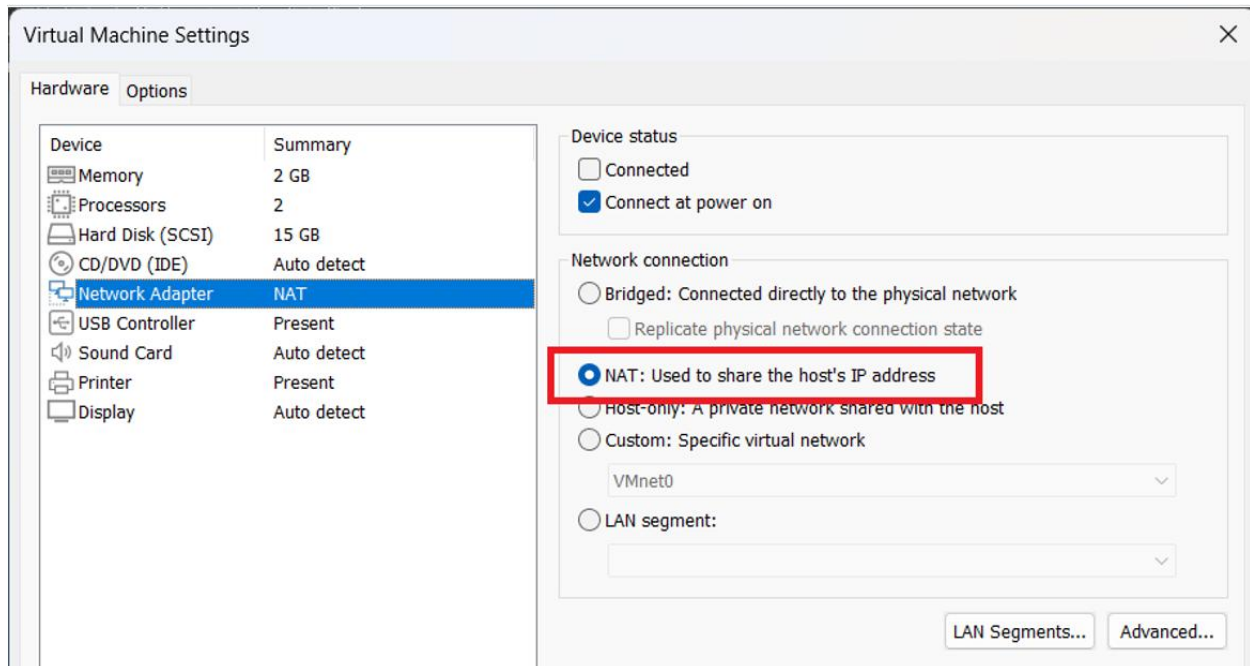
- Tự động cài đặt BIND và các gói phụ thuộc cần thiết
- Cấu hình địa chỉ IP tĩnh và tệp `named.conf`
- Tạo **Forward Zone** (phân giải xuôi) và **Reverse Zone** (phân giải ngược)
- Thêm các bản ghi DNS như A và PTR
- Cấu hình **DNS Secondary** (máy chủ DNS phụ)
- Kiểm tra trạng thái của dịch vụ `named`

Đây là một công cụ dạng menu CLI (giao diện dòng lệnh), người dùng chỉ cần chạy script và chọn chức năng mong muốn thông qua các con số.

II. CHUẨN BỊ MÔI TRƯỜNG

Để sử dụng script, bạn cần đảm bảo các yêu cầu sau:

- **Hệ điều hành:** Máy chủ CentOS (khuyến nghị sử dụng CentOS Stream 9)
- **Kết nối mạng:** Cần có kết nối Internet để cài đặt các gói `bind`, `bind-utils`, và `ipcalc`. Cả hai máy chủ Primary và Secondary đều phải kết nối được ra ngoài
- **Quyền truy cập:** Script cần được thực thi với quyền root
- **Đảm bảo cả 2 máy Primary và Secondary có thể kết nối mạng bên ngoài**



III. HƯỚNG DẪN CÀI ĐẶT

Trên Primary DNS Server

Bước 1: Tạo file script

```
touch primary.sh
```

Bước 2: Cấp quyền thực thi cho file

```
chmod +x primary.sh
```

Bước 3: Dán nội dung script

Dán toàn bộ nội dung script vào file `primary.sh` vừa tạo.

Bước 4: Chạy script với quyền root

```
./primary.sh
```

Trên Secondary DNS Server

Bước 1: Tạo file script

```
touch secondary.sh
```

Bước 2: Cấp quyền thực thi cho file

```
chmod +x secondary.sh
```

Bước 3: Dán nội dung script

Dán toàn bộ nội dung script vào file `secondary.sh` vừa tạo.

Bước 4: Chạy script với quyền root

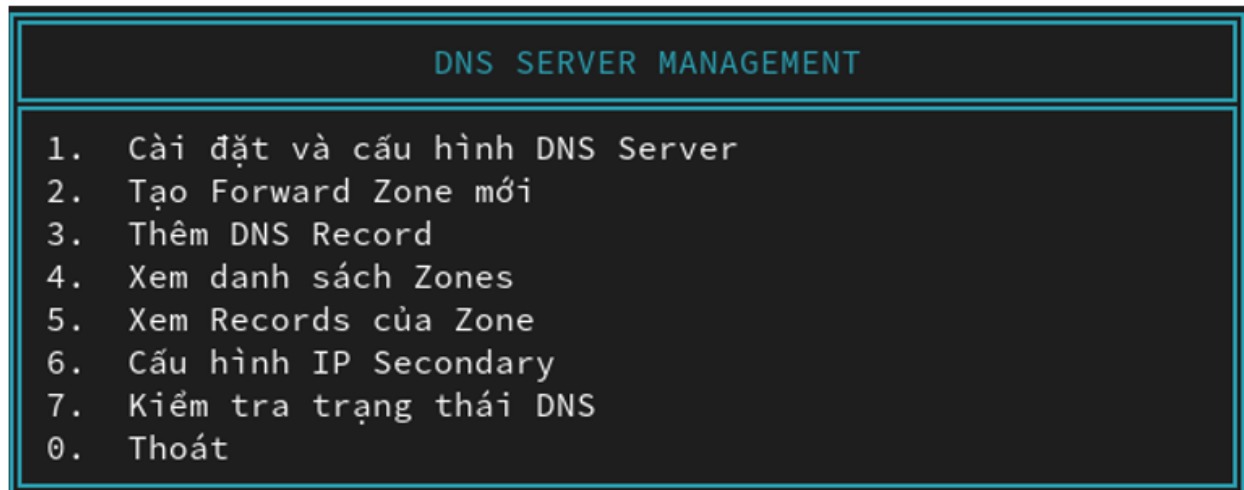
```
./secondary.sh
```

Lưu ý: Bạn nên tạo file và cấp quyền bằng tài khoản người dùng thông thường để dễ dàng dán nội dung script, sau đó chuyển sang root để chạy file.

IV. HƯỚNG DẪN SỬ DỤNG

1. Cấu hình trên Primary DNS Server

Khi chạy `primary.sh`, bạn sẽ thấy một menu chức năng. Hãy thực hiện tuần tự theo các bước sau:



Chức năng 1: Cài đặt và cấu hình cơ bản

- Chọn chức năng số 1 để cài đặt BIND và các gói cần thiết
- Nhập các thông tin mạng để cấu hình IP tĩnh, ví dụ:
 - Địa chỉ IP: 192.168.232.10
 - Subnet mask: 255.255.255.0
 - Gateway: 192.168.232.2

```
Chọn chức năng (0-9): 1
[INFO] Setup DNS server
[INFO] Đang cài đặt BIND packages...
[INFO] BIND packages đã được cài đặt thành công!
[INFO] Cấu hình IP tĩnh và tạo named.conf...
[INFO] ipcalc chưa cài, đang cài đặt...
[INFO] ipcalc đã cài xong.
Nhập địa chỉ IP tĩnh (mặc định: 192.168.232.10): 192.168.232.10
Nhập Subnet Mask (mặc định: 255.255.255.0): 255.255.255.0
Nhập Gateway (mặc định: 192.168.232.2): 192.168.232.2
Connection successfully activated (D-Bus active path: /org/freedesktop/NetworkManager/ActiveConnection/3)
[INFO] IP tĩnh đã được áp dụng: 192.168.232.10/24, Gateway: 192.168.232.2
[INFO] Tạo file /etc/named.conf ...
[INFO] named.conf đã được tạo xong với listen-on: 127.0.0.1, 192.168.232.10 và allow-query: 192.168.232.0/24
Created symlink /etc/systemd/system/multi-user.target.wants/named.service → /usr/lib/systemd/system/named.service.
[SUCCESS] Cài đặt DNS server hoàn tất! Bạn có thể tiến hành tạo zone.
```

Chức năng 2: Tạo Forward Zone

- Chọn chức năng số 2 để tạo một zone phân giải xuôi mới
- Nhập tên miền và địa chỉ IP tương ứng, ví dụ: domain it.net với IP 192.168.232.10

```
Chọn chức năng (0-9): 2
=== Tao Forward Zone mới ===
Nhập domain (vd: example.com): it.net
Nhập IP cho ns1.it.net: 192.168.232.10
[SUCCESS] Zone it.net đã được tạo và dịch vụ named đã restart.
Nhấn Enter để tiếp tục...
```

Chức năng 3: Thêm DNS Record

- Chọn chức năng số 3 để thêm bản ghi cho zone đã tạo
- Chọn zone bạn muốn thao tác từ danh sách (ví dụ: `it.net`)

[illegible]

- Nhập hostname và địa chỉ IP cho bản ghi mới (ví dụ: hostname `www` với IP `192.168.232.11`)

```
Chọn số thứ tự Zone để thêm record: 5
Bạn đang thêm record cho zone: it.net
Nhập hostname (vd: www, để trống = domain chính): www
Nhập IP cho www.it.net: 192.168.232.11
Đã thêm record: www.it.net → 192.168.232.11
[SUCCESS] Reverse zone 232.168.192.in-addr.arpa đã được tạo.
[SUCCESS] PTR record 192.168.232.11 → www.it.net đã được thêm.
server reload successful
zone reload up-to-date
Nhấn Enter để tiếp tục...
```

Chức năng 4 & 5: Xem thông tin

- Sử dụng chức năng số 4 để xem danh sách các Forward và Reverse Zone đã tạo

```
=== Danh sách Zones ===  
Forward Zones:  
- .  
- localhost.localdomain  
- localhost  
- 1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.ip6.arpa  
- it.net  
  
Reverse Zones:  
- 1.0.0.127.in-addr.arpa  
- 0.in-addr.arpa  
- 232.168.192.in-addr.arpa
```

Nhấn Enter để tiếp tục...SS

- Sử dụng chức năng số 5 để xem tất cả các bản ghi của một zone cụ thể

[illegible]

Kiểm tra phân giải (Forward & Reverse Lookup)

Thoát script và dùng lệnh `nslookup` để kiểm tra:

Forward Lookup:

- nslookup it.net sẽ trả về 192.168.232.10
- nslookup www.it.net sẽ trả về 192.168.232.11

```
[root@192 minhqlq]# nslookup
> it.net
Server:          192.168.232.10
Address:         192.168.232.10#53

Name:   it.net
Address: 192.168.232.10
> www.it.net
Server:          192.168.232.10
Address:         192.168.232.10#53

Name:   www.it.net
Address: 192.168.232.11
```

Reverse Lookup:

- nslookup 192.168.232.11 sẽ trả về www.it.net, xác nhận Reverse Zone đã được cấu hình chính xác

```
[root@192 minhqlq]# nslookup
> 192.168.232.11
11.232.168.192.in-addr.arpa      name = www.it.net.
```

Chức năng 6: Cấu hình Secondary DNS

- Chọn chức năng số 6
- Nhập thông tin cho máy chủ Secondary, ví dụ:
 - Tên zone: it.net
 - Hostname của Secondary: secondary.it.net
 - Địa chỉ IP của Secondary: 192.168.232.20

```
Chọn chức năng (0-9): 6
[INFO] Cấu hình Slave DNS cho Forward Zone...
Nhập tên zone (ví dụ: edu.vn): it.net
Nhập hostname Secondary (ví dụ: secondary.edu.vn): secondary.it.net
Nhập IP Secondary (ví dụ: 192.168.232.20): 192.168.232.20
[SUCCESS] Đã thêm NS record cho secondary.it.net.
[SUCCESS] Đã thêm A record cho secondary -> 192.168.232.20
[SUCCESS] PTR record 192.168.232.20 -> secondary.it.net đã được thêm.
[SUCCESS] Đã thêm allow-transfer { 192.168.232.20; } vào /etc/named.conf
[SUCCESS] Serial tăng từ 2025092001 -> 2025092002
[INFO] Kiểm tra zone file...
zone it.net/IN: loaded serial 2025092002
OK
[SUCCESS] Zone file hợp lệ. Restart named...
[SUCCESS] Dịch vụ named đã restart
```

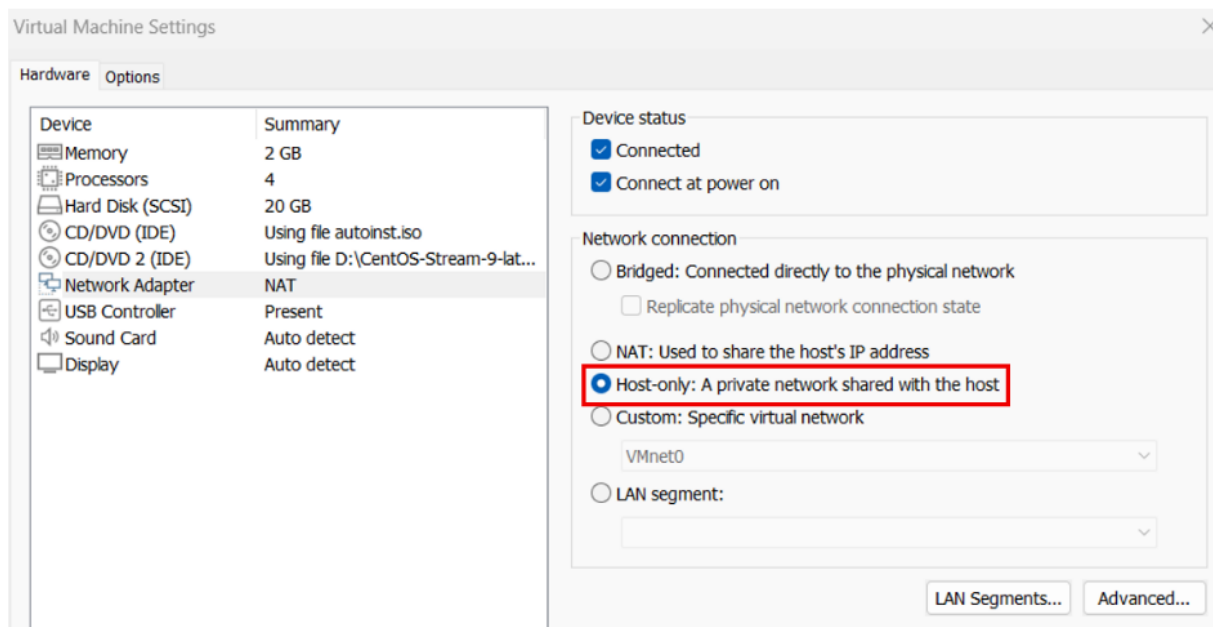
Chức năng 7: Kiểm tra trạng thái dịch vụ

- Chọn chức năng số 7 để đảm bảo dịch vụ named đang chạy và các zone đã được tải thành công

```
Chọn chức năng (0-9): 7
● named.service - Berkeley Internet Name Domain (DNS)
   Loaded: loaded (/usr/lib/systemd/system/named.service; enabled; preset: disabled)
   Active: active (running) since Sat 2025-09-20 20:16:20 +07; 3min 19s ago
     Process: 36865 ExecStartPre=/bin/bash -c if [ ! "$DISABLE_ZONE_CHECKING" == "yes" ]; then /usr/sbin/named-checkconf -z "$NAMEDCONF"; else echo "Checking of zone files is disabled"; fi (code=exited, status=0/SUCCESS)
     Process: 36868 ExecStart=/usr/sbin/named -u named -c ${NAMEDCONF} $OPTIONS (code=exited, status=0/SUCCESS)
    Main PID: 36869 (named)
      Tasks: 18 (limit: 10294)
     Memory: 34.8M (peak: 36.8M)
        CPU: 226ms
    CGroup: /system.slice/named.service
            └─36869 /usr/sbin/named -u named -c /etc/named.conf
```

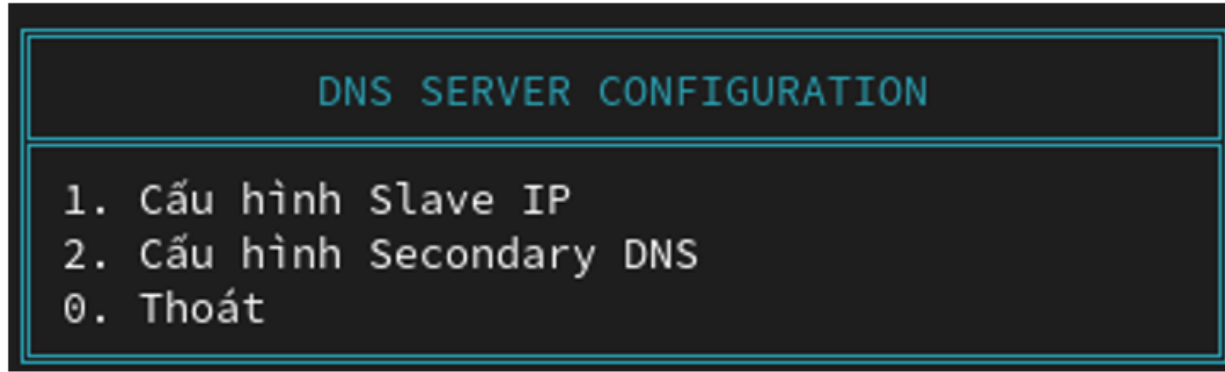
Hoàn tất cấu hình Primary

Sau khi hoàn thành 7 chức năng trên, hãy chuyển Network Adapter của máy Primary sang chế độ **Host-only**.



2. Cấu hình trên Secondary DNS Server

Khi chạy `secondary.sh`, bạn thực hiện tuần tự các bước sau:

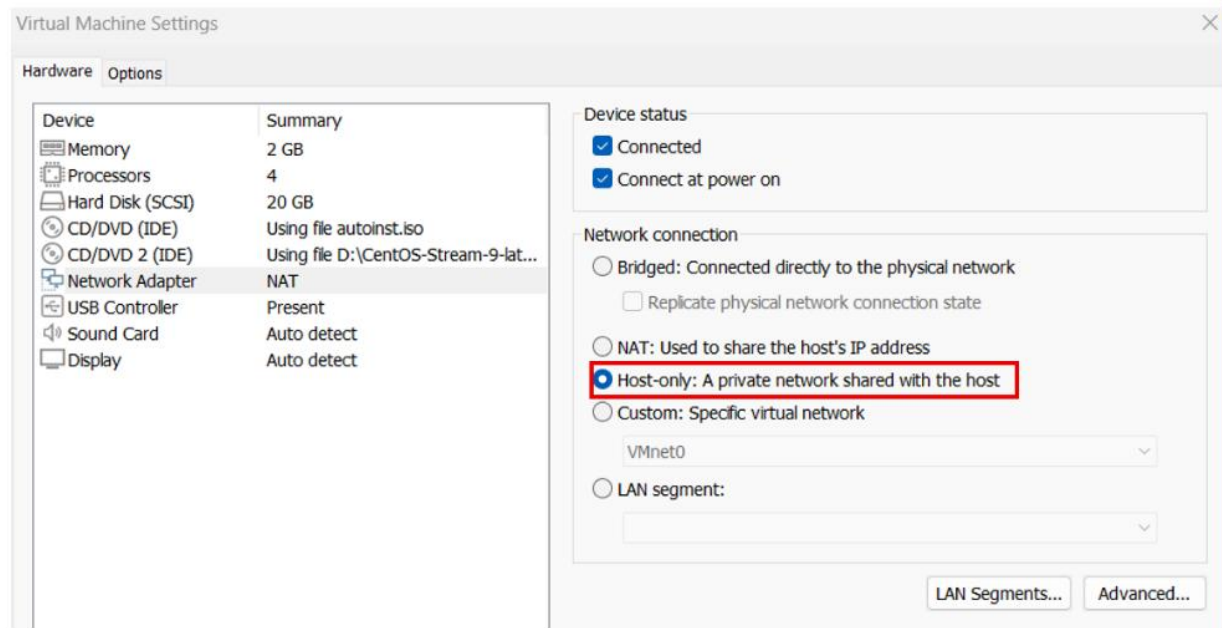


Chức năng 1: Cài đặt và cấu hình cơ bản

- Chọn chức năng số 1 để cài đặt BIND
- Nhập các thông tin mạng, bao gồm IP của Master DNS, ví dụ:
 - IP tĩnh: 192.168.232.20
 - Subnet mask: 255.255.255.0
 - Gateway: 192.168.232.2
 - IP của Master DNS: 192.168.232.10

```
Chọn một tùy chọn (0-2): 1
[INFO] Cấu hình IP tĩnh cho Slave DNS...
[INFO] Đang cài đặt BIND packages...
[INFO] BIND packages đã được cài đặt thành công!
[INFO] ipcalc chưa cài, đang cài đặt...
[INFO] ipcalc đã cài xong.
Nhập IP tĩnh cho Slave (mặc định: 192.168.232.20): 192.168.232.20
Nhập Subnet Mask (mặc định: 255.255.255.0): 255.255.255.0
Nhập Gateway (mặc định: 192.168.232.3): 192.168.232.2
Nhập IP Master DNS (mặc định: 192.168.232.10): 192.168.232.10
Connection successfully activated (D-Bus active path: /org/freedesktop/NetworkManager/ActiveConnection/3)
[INFO] Slave IP đã được áp dụng:
[INFO] IP: 192.168.232.20/24 | Gateway: 192.168.232.2 | DNS: 192.168.232.20
[INFO] Tạo file /etc/named.conf ...
[INFO] named.conf đã được tạo xong với listen-on: 127.0.0.1, 192.168.232.20 và allow-query: 192.168.232.0/24
```

Sau đó, chuyển Network Adapter của máy Secondary sang chế độ **Host-only**.



Chức năng 2: Cấu hình Secondary Zone

- Chọn chức năng số 2
- Nhập tên zone cần đồng bộ (ví dụ: it.net) và địa chỉ IP của Primary DNS (ví dụ: 192.168.232.10)

```
Chọn một tùy chọn (0-2): 2
[INFO] Cấu hình secondary DNS server...
Nhập tên zone (vd: example.com): it.net
Nhập IP Primary DNS: 192.168.232.10
[INFO] Thêm cấu hình forward zone slave vào /etc/named.rfc1912.zones ...
[SUCCESS] Zone it.net đã được thêm.
[INFO] Thêm cấu hình reverse zone slave vào /etc/named.rfc1912.zones ...
[SUCCESS] Zone 232.168.192.in-addr.arpa đã được thêm.
[INFO] Cập nhật /etc/named.conf ...
[SUCCESS] Đã thêm allow-transfer { 192.168.232.10; }; vào options.
[INFO] Kiểm tra cấu hình ...
/etc/named.conf:7: option 'dnssec-enable' is obsolete and should be removed
[INFO] Restart dịch vụ named ...
Created symlink /etc/systemd/system/multi-user.target.wants/named.service → /usr/lib/systemd/system/named.service
```

- Sau đó kiểm tra trạng thái DNS Server, xác nhận dịch vụ named đang chạy và các zone đã được load đúng

```
• named.service - Berkeley Internet Name Domain (DNS)
  Loaded: loaded (/usr/lib/systemd/system/named.service; enabled; preset: disabled)
  Active: active (running) since Sat 2025-09-20 20:37:40 +07; 634ms ago
    Main PID: 36335 (named)
      Tasks: 18 (limit: 10294)
     Memory: 35.0M (peak: 36.3M)
        CPU: 234ms
    CGroup: /system.slice/named.service
            └─36335 /usr/sbin/named -u named -c /etc/named.conf
```

Kiểm tra đồng bộ và phân giải

Trên Secondary: Dùng nslookup để kiểm tra. Kết quả phải cho thấy các bản ghi đã được đồng bộ từ Primary:

- it.net → 192.168.232.10
- www.it.net → 192.168.232.11
- secondary.it.net → 192.168.232.20

```
[root@192 minhlq]# nslookup
> it.net
Server:          192.168.232.20
Address:         192.168.232.20#53

Name:   it.net
Address: 192.168.232.10
> www.it.net
Server:          192.168.232.20
Address:         192.168.232.20#53

Name:   www.it.net
Address: 192.168.232.11
> secondary.it.net
Server:          192.168.232.20
Address:         192.168.232.20#53

Name:   secondary.it.net
Address: 192.168.232.20
```

Kiểm tra Reverse Lookup cũng phải trả về kết quả tương ứng:

- 192.168.232.11 → www.it.net
- 192.168.232.20 → secondary.it.net

```
[root@192 minhlq]# nslookup
> 192.168.232.11
11.232.168.192.in-addr.arpa    name = www.it.net.
> 192.168.232.20
20.232.168.192.in-addr.arpa    name = secondary.it.net.
```

Trên Primary: Quay lại máy Primary và kiểm tra xem nó có thể phân giải được Secondary DNS hay không:

- Forward Lookup: `nslookup secondary.it.net` → 192.168.232.20
- Reverse Lookup: `nslookup 192.168.232.20` → secondary.it.net

```
[root@192 minhlg]# nslookup
> secondary.it.net
Server:      192.168.232.10
Address:     192.168.232.10#53

Name:   secondary.it.net
Address: 192.168.232.20
> 192.168.232.20
20.232.168.192.in-addr.arpa    name = secondary.it.net.
```

Kết quả kiểm tra chéo thành công xác nhận rằng cả hai máy chủ DNS đã được cấu hình đúng và đồng bộ với nhau.

PHỤ LỤC

Bảng tóm tắt thông tin cấu hình

Thông tin	Primary DNS Server	Secondary DNS Server
Địa chỉ IP	192.168.232.10	192.168.232.20
Subnet Mask	255.255.255.0	255.255.255.0
Gateway	192.168.232.2	192.168.232.2
Tên miền chính	it.net	it.net (đồng bộ)
Hostname	primary.it.net	secondary.it.net
File script	primary.sh	secondary.sh

HẾT