

Quản lý DNS Server bằng Bash Script

I. Giới thiệu

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

Nó giúp bạn dễ dàng:

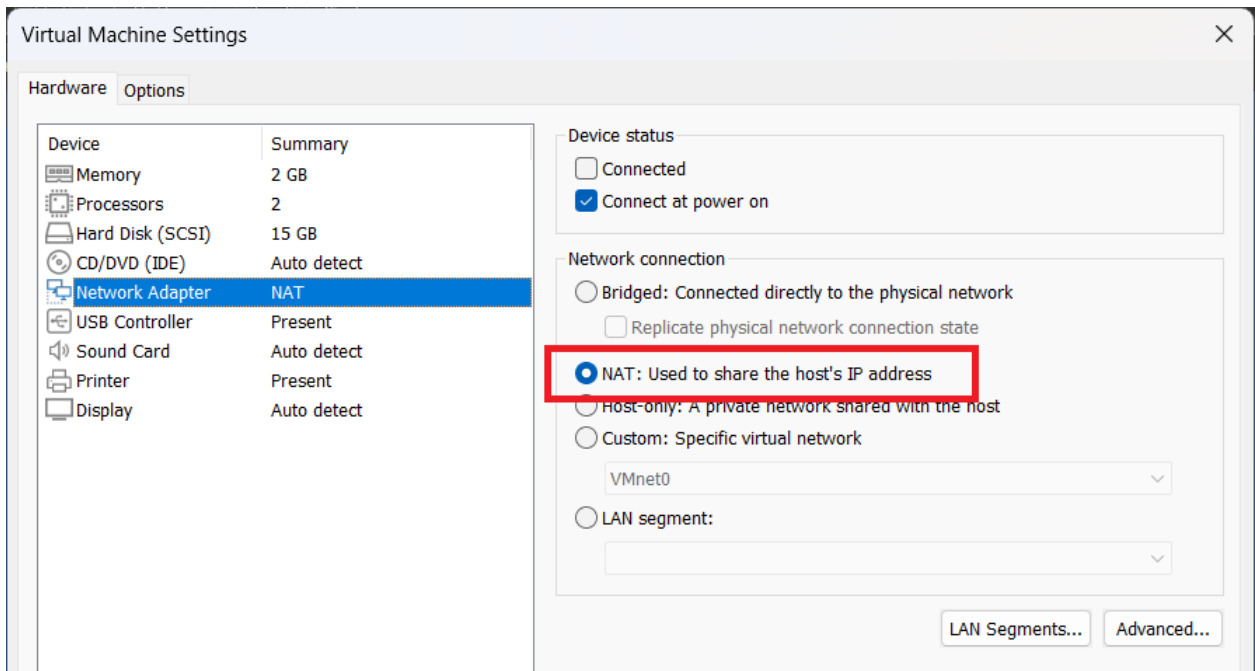
- Tự động cài BIND và các gói cần thiết.
- Cấu hình IP tĩnh và file named.conf.
- Tạo Forward Zone và Reverse Zone.
- Thêm DNS record (A, PTR).
- Cấu hình DNS Secondary (Slave).
- Kiểm tra trạng thái dịch vụ named.

Đây là công cụ dạng menu CLI, bạn chỉ cần chạy script và chọn số theo chức năng mong muốn.

II. Chuẩn bị môi trường

- Máy chủ CentOS (khuyến dùng CentOS Stream 9).
- Kết nối Internet để cài gói bind, bind-utils, ipcalc.
- Script này cần quyền root để thực thi.

Đảm bảo cả 2 máy Primary và Secondary có thể kết nối mạng bên ngoài



Trên Primary DNS Server

1. Tạo file script

```
touch primary.sh
```

2. Cấp quyền thực thi

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

3. Dán script vào file *primary.sh*

4. Chạy script

```
./primary.sh
```

Trên Secondary DNS Server

1. Tạo file script

```
touch secondary.sh
```

2. Cấp quyền thực thi

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

3. Dán script vào file *secondary.sh*

4. Chạy script

```
./secondary.sh
```

Lưu ý: Tạo file và cấp quyền bằng *tài khoản user* để dễ dán script; chuyển sang *root* khi chạy file.

III. Menu chính

1. Trên Primary DNS Server

Khi chạy script *primary.sh*, bạn sẽ thấy menu:



Hướng dẫn chạy tuần tự từng chức năng

Ban đầu, chọn chức năng **số 1** để cài đặt gói BIND cùng các thư viện cần thiết và cấu hình DNS Server. Tiếp theo, nhập **địa chỉ IP tĩnh** (ví dụ: 192.168.232.10), **subnet mask** (255.255.255.0) và **gateway** (192.168.232.2) để hoàn tất thiết lập cơ bản.

```
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.
```

```
Chọn chức năng (0-9): 2
=== Tạo 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...
```

[illegible]

```
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...
```

Sau khi thêm các zone và record, chọn chức năng **số 4** để xem danh sách **Forward** và **Reverse Zones** hiện có, giúp kiểm tra và xác nhận các zone đã được tạo đúng.

```
=== 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.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

Chọn chức năng **số 5** để **xem các records của một zone**. Hệ thống sẽ hiển thị danh sách các Forward Zones. Nhập số thứ tự tương ứng với zone bạn muốn xem (ví dụ: 5 cho it.net) để hiển thị toàn bộ các record của zone đó.

[illegible]

Tiếp theo, thoát script bằng cách chọn chức năng **số 0** hoặc nhấn **Ctrl + C**. Sau đó, kiểm tra cấu hình Forward Lookup vừa thực hiện bằng lệnh nslookup cho các domain **it.net** và **www.it.net**.

```
[root@192 minhlq]# 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
```

Kết quả nslookup cho thấy:

- it.net được phân giải về địa chỉ **192.168.232.10**, đúng với IP mà chúng ta đã cấu hình cho domain chính.
- www.it.net được phân giải về **192.168.232.11**, đúng với IP mà chúng ta đã thêm cho hostname www.

Điều này xác nhận rằng **Forward Lookup** trên DNS Server đã hoạt động chính xác.

Tiếp theo, chúng ta kiểm tra **Reverse Lookup** để đảm bảo các địa chỉ IP được phân giải ngược về đúng tên miền. Sử dụng lệnh nslookup <IP> cho các IP đã cấu hình.

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

Kết quả nslookup 192.168.232.11 trả về www.it.net chứng tỏ rằng **Reverse Zone** đã được cấu hình chính xác. Điều này nghĩa là địa chỉ IP **192.168.232.11** được phân giải ngược về hostname www.it.net, xác nhận chức năng **Reverse Lookup** hoạt động đúng trên DNS Server.

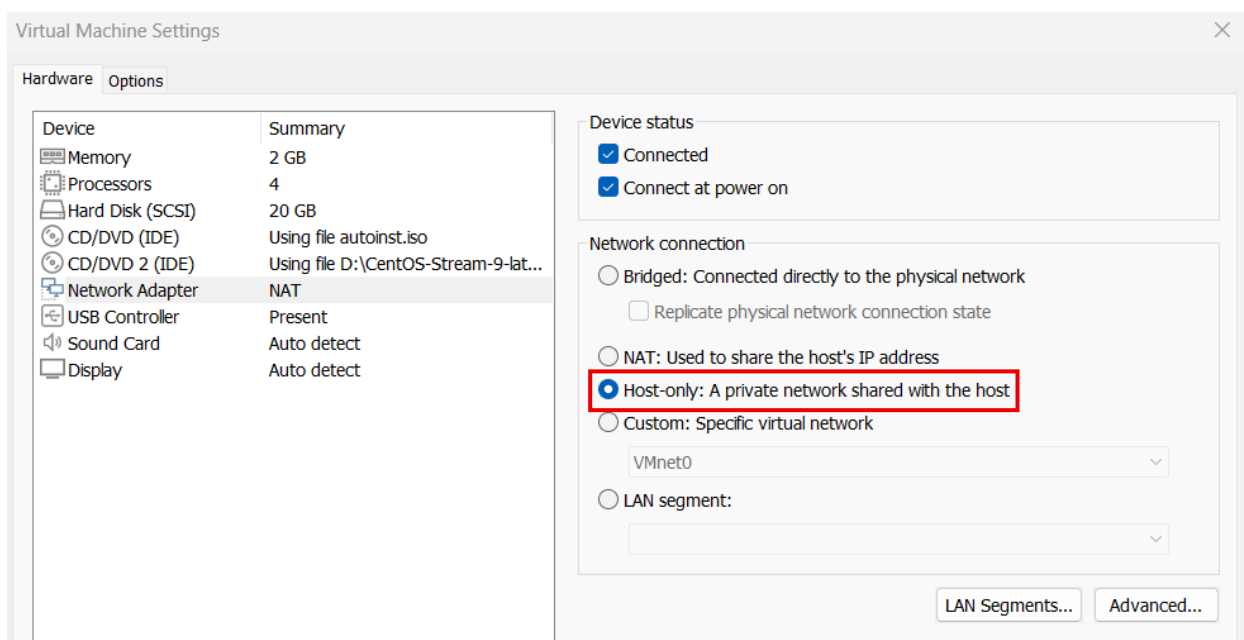
Tiếp theo, chọn chức năng **số 6** để cấu hình **Secondary DNS** cho zone vừa tạo. Tại đây, nhập *tên zone* (ví dụ: it.net), *hostname* cho Secondary (ví dụ: secondary.it.net) và *địa chỉ IP của Secondary* (ví dụ: 192.168.232.20).

```
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
```

Chọn chức năng **số 7** để kiểm tra trạng thái DNS Server, xác nhận dịch vụ named đang chạy và các zone đã được load đúng.

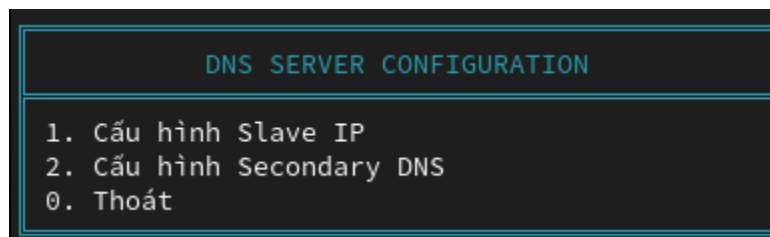
```
Chọn chức năng (0-9): 7
• named.service - Berkeley Internet Name Domain (DNS)
  Loaded: loaded (/usr/lib/systemd/system/named.service; enabled; preset: disabled)
  Active: active (running) since Sat 2025-09-20 20:16:20 +07; 3min 19s ago
  Process: 36865 ExecStartPre=/bin/bash -c if [ ! "$DISABLE_ZONE_CHECKING" == "yes" ]; then /usr/sbin/named-checkconf -z "$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
```

Sau khi hoàn tất cấu hình cả 7 chức năng, chuyển **Network Adapter** của máy Primary sang **Host-only**.



2. Trên Secondary DNS Server

Khi chạy script *secondary.sh*, bạn sẽ thấy menu:



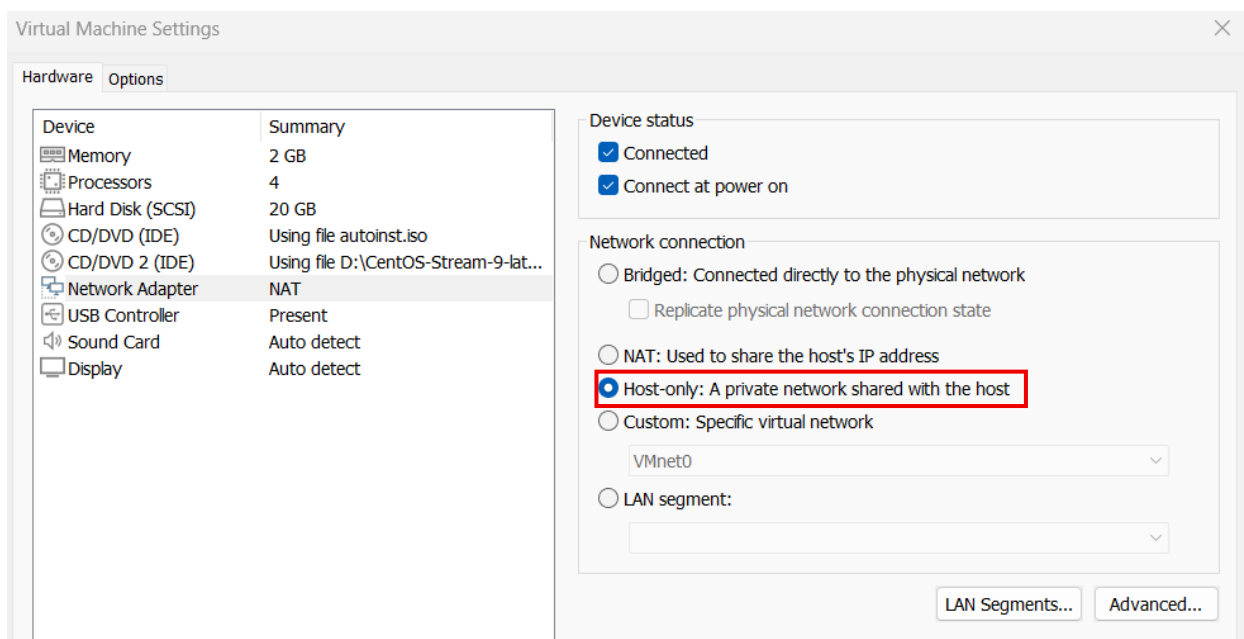
Hướng dẫn chạy tuần tự từng chức năng

Ban đầu, chọn chức năng **số 1** để cài đặt gói BIND cùng các thư viện cần thiết và cấu hình DNS Server trên máy Secondary. Sau đó, nhập các thông tin mạng cơ bản: **IP tĩnh**

(192.168.232.20), **subnet mask** (255.255.255.0), **gateway** (192.168.232.2) và **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
```

Tiếp theo, chuyển **Network Adapter** của máy Secondary sang **Host-only**.



Tiếp theo, chọn chức năng **số 2** để cấu hình **Secondary DNS Server**. Nhập **tên zone** (ví dụ: it.net) và **IP của Primary DNS** (ví dụ: 192.168.232.10). Hệ thống sẽ tự động thêm cấu hình **forward** và **reverse zone** cho Secondary.


```

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

```

Kết quả kiểm tra trên Secondary DNS (192.168.232.20) cho thấy:

- it.net được phân giải về **192.168.232.10** → trùng với IP của Primary DNS.
- www.it.net được phân giải về **192.168.232.11** → đúng với record đã thêm trên Primary.
- secondary.it.net được phân giải về **192.168.232.20** → đúng với IP của Secondary DNS.

Điều này chứng tỏ rằng **Forward Lookup** trên Secondary DNS hoạt động chính xác và các bản ghi từ Primary đã được đồng bộ thành công.

```
[root@192 minh1q]# 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** trên Secondary DNS cho thấy:

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

Điều này xác nhận các **Reverse Zone** đã được cấu hình và đồng bộ chính xác.

```
[root@192 minh1q]# 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.
```

Quay trở về Primary DNS, kiểm tra **Forward và Reverse Lookup** cho Secondary DNS:

- **Forward Lookup:** secondary.it.net → 192.168.232.20
- **Reverse Lookup:** 192.168.232.20 → secondary.it.net

Kết quả này xác nhận Secondary DNS hoạt động bình thường và kết nối với Primary DNS đúng, các record đã được đồng bộ.

```
[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.
```

Chúc bạn thành công trong việc cấu hình và kiểm tra DNS Server!