

HƯỚNG DẪN CÀI ĐẶT & CẤU HÌNH DNS SERVER (BIND9) + FIX LỖI + LƯỒNG HOẠT ĐỘNG

1. GIỚI THIỆU

DNS (Domain Name System) là hệ thống phân giải tên miền sang địa chỉ IP. Trên Ubuntu, dịch vụ phổ biến nhất là **BIND9** (Berkeley Internet Name Domain).

Tài liệu này hướng dẫn toàn bộ quá trình từ **cài đặt**, **cấu hình**, **kiểm tra**, đến **xử lý lỗi**, kèm **reverse zone (PTR)** và **forwarders**.

2. CÀI ĐẶT BIND9

```
sudo apt update
sudo apt install bind9 bind9-utils bind9-dnsutils -y
sudo systemctl enable --now bind9
sudo systemctl status bind9
```

3. CẤU HÌNH FORWARDERS (TÙY CHỌN)

Forwarders giúp DNS nội bộ chuyển tiếp truy vấn không thuộc zone local ra Internet (Google, Cloudflare...).

Mở file `/etc/bind/named.conf.options`:

```
options {
    directory "/var/cache/bind";

    forwarders {
        8.8.8.8;
        1.1.1.1;
    };

    dnssec-validation no;
    listen-on { any; };
    allow-query { any; };
};
```

Khởi động lại dịch vụ:

```
sudo systemctl restart bind9
```

4. CẤU HÌNH ZONE FILE (FORWARD ZONE)

Khai báo zone trong `/etc/bind/named.conf.local`:

```
zone "khene.gihot.com" {  
    type master;  
    file "/etc/bind/zones/db.khene.gihot.com";  
};
```

Tạo thư mục và file zone:

```
sudo mkdir -p /etc/bind/zones  
sudo nano /etc/bind/zones/db.khene.gihot.com
```

Nội dung mẫu:

```
$TTL 604800  
@ IN SOA ns1.khene.gihot.com. admin.khene.gihot.com. (  
    3      ; Serial  
    604800 ; Refresh  
    86400  ; Retry  
    2419200 ; Expire  
    604800 ) ; Negative Cache TTL  
;  
@ IN NS ns1.khene.gihot.com.  
ns1 IN A 192.168.0.25  
@ IN A 192.168.0.25  
www IN A 192.168.0.25  
api IN A 192.168.0.25
```



5. CẤU HÌNH REVERSE ZONE (PTR RECORD)

Tạo file `/etc/bind/zones/db.192.168.0`:

```
$TTL 604800  
@ IN SOA ns1.khene.gihot.com. admin.khene.gihot.com. (  
    2      ; Serial  
    604800 ; Refresh  
    86400  ; Retry
```

```

        2419200 ; Expire
        604800 ) ; Negative Cache TTL
;
@      IN      NS      ns1.khene.gihot.com.
25     IN      PTR     khene.gihot.com.

```

Thêm vào `/etc/bind/named.conf.local`:

```

zone "0.168.192.in-addr.arpa" {
    type master;
    file "/etc/bind/zones/db.192.168.0";
};

```

Kiểm tra:

```
sudo named-checkzone 0.168.192.in-addr.arpa /etc/bind/zones/db.192.168.0
```

6. KIỂM TRA CẤU HÌNH

```

sudo named-checkconf
sudo named-checkzone khene.gihot.com /etc/bind/zones/db.khene.gihot.com
sudo systemctl restart bind9

```

Kiểm tra DNS hoạt động:

```

dig @127.0.0.1 khene.gihot.com
dig @127.0.0.1 www.khene.gihot.com
dig @192.168.0.25 khene.gihot.com

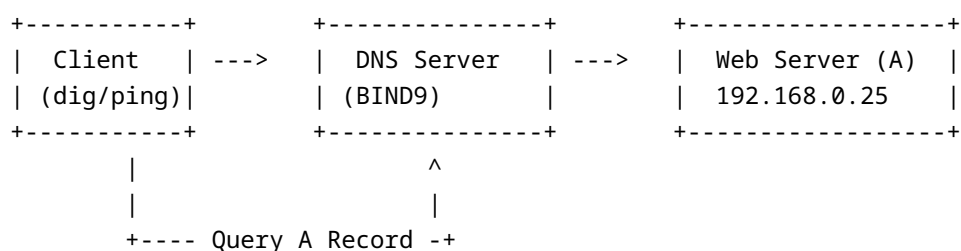
```

7. FIX LỖI PHỔ BIẾN

Lỗi	Nguyên nhân	Cách khắc phục
<code>connection refused</code>	Dịch vụ BIND9 chưa bật hoặc firewall chặn	<code>sudo ufw allow 53; sudo systemctl restart bind9</code>
<code>SERVFAIL</code>	Sai đường dẫn file zone	Kiểm tra <code>named.conf.local</code>
<code>REFUSED</code>	<code>allow-query</code> bị giới hạn	Thêm <code>allow-query { any; };</code> trong <code>named.conf.options</code>

Lỗi	Nguyên nhân	Cách khắc phục
Không phân giải được tên miền	Client chưa trỏ DNS	Đặt DNS client = IP server (192.168.0.25)
<code>resolver priming query complete: failure</code>	Không có IPv6	Thêm <code>listen-on-v6 { none; };</code> vào <code>named.conf.options</code>

8. LƯỒNG HOẠT ĐỘNG DNS




- Client gửi truy vấn `khene.gihot.com` đến DNS.
- BIND9 kiểm tra trong zone local.
- Nếu có bản ghi → trả IP về client.
- Nếu không có → chuyển tiếp (forwarder) ra Internet.
- Nếu có reverse zone → ánh xạ ngược IP về tên miền.

9. KIỂM TRA TỪ CLIENT KHÁC

1. Đặt DNS trên máy hoặc điện thoại = **192.168.0.25**.
2. Dùng lệnh:

```
dig @192.168.0.25 khene.gihot.com
ping khene.gihot.com
```

Nếu trả về `192.168.0.25` → hoạt động OK 

10. LOG & DEBUG

- Kiểm tra log lỗi:

```
tail -f /var/log/syslog | grep named
```

- Theo dõi tiến trình:

```
sudo systemctl status bind9  
sudo ss -ltn | grep 53
```

11. TÓM TẮT CẤU TRÚC FILE

File	Chức năng
/etc/bind/named.conf.options	Cấu hình chung + forwarders
/etc/bind/named.conf.local	Khai báo zone
/etc/bind/zones/db.khene.gihot.com	Zone forward
/etc/bind/zones/db.192.168.0	Reverse zone
/var/log/syslog	Log hoạt động BIND9

✓ Hoàn tất cài đặt DNS Server nội bộ (BIND9) cho domain khene.gihot.com.