

# QUẢN TRỊ MẠNG

## TUẦN 2

### CÀI ĐẶT VÀ CẤU HÌNH DNS SERVER

#### *Hướng dẫn làm bài*

#### **Cấu hình trên CentOS7**

Để cấu hình DNS Server trên CentOS7, ta cần phải cài đặt 1 máy tính sử dụng hệ điều hành CentOS7, khi cài đặt cần phải có kết nối internet.

Các bước thực hiện như sau:

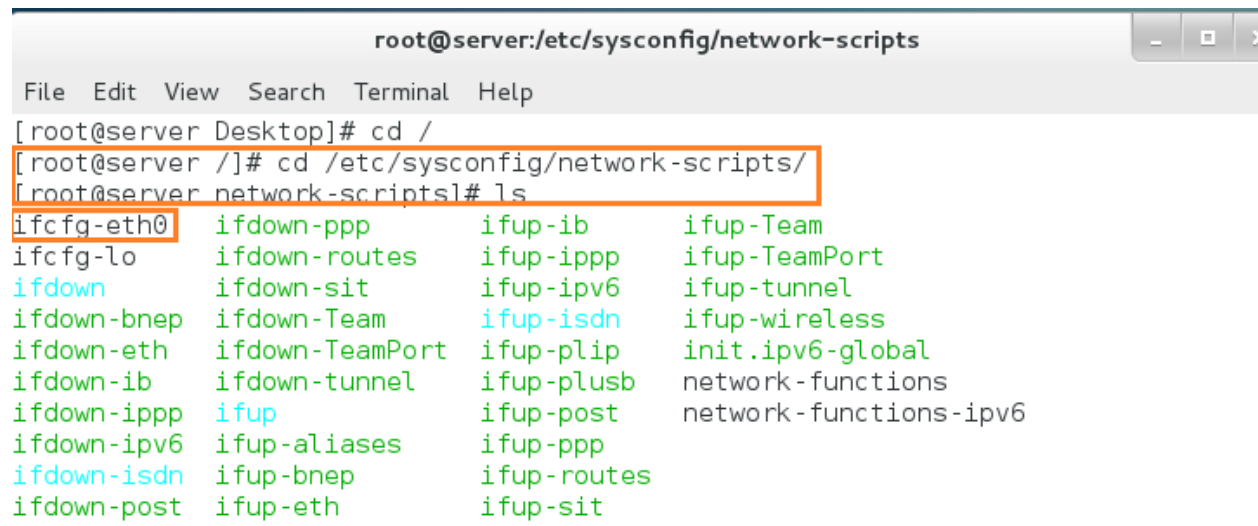
#### **Bước 1: Đặt IP tĩnh**

Cấu hình IP tĩnh cho CentOS. Ta có thể cấu hình bằng giao diện GNOME.

Hoặc cũng có thể cấu hình bằng dòng lệnh như sau:

Vào thư mục `/etc/sysconfig/network-scripts/`, chỉnh sửa file `ifcfg-eth0`

```
# cd /etc/sysconfig/network-scripts/
```



```
root@server:/etc/sysconfig/network-scripts
File Edit View Search Terminal Help
[root@server Desktop]# cd /
[root@server /]# cd /etc/sysconfig/network-scripts/
[root@server network-scripts]# ls
ifcfg-eth0  ifdown-ppp      ifup-ib         ifup-Team
ifcfg-lo    ifdown-routes  ifup-ipppp     ifup-TeamPort
ifdown      ifdown-sit      ifup-ipv6      ifup-tunnel
ifdown-bnep ifdown-Team     ifup-isdn      ifup-wireless
ifdown-eth  ifdown-TeamPort ifup-plip      init.ipv6-global
ifdown-ib   ifdown-tunnel  ifup-plusb     network-functions
ifdown-ippp ifup           ifup-post      network-functions-ipv6
ifdown-ipv6 ifup-aliases   ifup-ppp
ifdown-isdn ifup-bnep      ifup-routes
ifdown-post ifup-eth       ifup-sit
```

Chỉnh sửa file `ifcfg-eth0`

```
# nano ifcfg-eth0
```

```
HWADDR="00:0c:29:5d:b6:e8"          # Địa chỉ MAC của card
mạng
```

```

TYPE=Ethernet

BOOTPROTO=static                    # Đặt IP tĩnh
IPADDR=192.168.1.11                 # IP Address
NETMASK=255.255.255.0               # Netmask
GATEWAY=192.168.1.11                # Default Gateway
DNS=192.168.1.11                    # DNS server
DEFROUTE=yes
IPV4_FAILURE_FATAL=no
NAME=eth0
DEVICE=eth0
ONBOOT=yes                           # Bật card mạng khi
khởi động

```

Lưu file và khởi động lại dịch vụ mạng bằng lệnh

```
# systemctl restart network.service
```

Kiểm tra IP

```
# ip addr
```

## Bước 2: Cài đặt gói BIND

Để cài đặt BIND, ta phải có kết nối đến internet. Do đó, thông thường ta nên cài đặt gói BIND trước khi thực hiện bước 1.

```
[root@server ~]# yum install bind bind-utils -y
```

Quá trình cài đặt sẽ tự diễn ra, trong lúc cài đặt, hệ thống sẽ tự động cập nhật các gói tin từ internet.

## Bước 3: Cấu hình DNS

Ta cấu hình tập tin named.conf

```
[root@server ~]# nano /etc/named.conf
```

Ta chỉnh sửa một số thông số như sau:

Không sử dụng **IPv6** và cho phép lắng nghe trên địa chỉ **IP 192.168.1.11**:

```
listen-on port 53 { 127.0.0.1; 192.168.1.11; };
#listen-on-v6 port 53 { ::1; };

```

Cho phép nhận truy vấn **DNS** từ dải địa chỉ **192.168.1.0/24**:

```
allow-query { localhost; 192.168.1.0/24; };

```

Định nghĩa vùng phân giải xuôi (**Forward**) và phân giải ngược (**Reverse**) sau phần **zone "." IN**:

```
zone "." IN {

```

```

    type hint;
    file "named.ca";
};
zone "vnlab.com.vn" IN {
type master;
file "forward.vnlab.com.vn";
allow-update { none; };
};
zone "1.168.192.in-addr.arpa" IN {
type master;
file "reverse.vnlab.com.vn";
allow-update { none; };
;

```

Ta cấu hình forward zone và reverse zone

Tạo vùng phân giải xuôi (forward zone):

```
[root@server ~]# nano /var/named/forward.vnlab.com.vn
```

Tạo các bản ghi (Record) tương ứng:

```

$TTL 86400
@          IN      SOA      server1.vnlab.com.vn.
root.vnlab.com.vn. (
                2011071001  ;Serial
                3600        ;Refresh
                1800        ;Retry
                604800      ;Expire
                86400       ;Minimum TTL
)
@          IN      NS       server1.vnlab.com.vn.
@          IN      A        192.168.1.11
server1    IN      A        192.168.1.11

```

Tạo vùng phân giải ngược (reverse zone)

```
[root@server ~]# nano /var/named/reverse.vnlab.com.vn
```

Tạo các bản ghi (record) tương ứng:

```

$TTL 86400
@      IN      SOA      server1.vnlab.com.vn. root.vnlab.com.vn. (
                2011071001  ;Serial
                3600        ;Refresh
                1800        ;Retry
                604800      ;Expire
                86400       ;Minimum TTL
)

```

```
@      IN      NS      server1.vnlab.com.vn.
@      IN      PTR     vnlab.com.vn.
server1 IN      A      192.168.1.11
11     IN      PTR     server1.vnlab.com.vn.
```

#### Bước 4: Khởi động lại DNS

Ta phải tạo file named.root và chép file vào thư mục named

```
nano /var/named/named.root
```

Ta dùng 2 câu lệnh sau để khởi động DNS:

```
[root@server1 ~]# systemctl enable named
[root@server1 ~]# systemctl start named
```

Ngoài ra, đôi khi ta phải tắt firewall để DNS hoạt động.

```
firewall-cmd --permanent --zone=public --add-service=dns
firewall-cmd --reload
```

Sau đó ta có thể kiểm tra lại DNS bằng câu lệnh nslookup.

Sau khi thực hiện xong, ta mở 1 máy trạm, có thể dùng WinXP để mở, sau đó mở command line. Tại đây, ta sử dụng câu lệnh nslookup để kiểm tra DNS giống như đã làm trên CentOS server. Tuy nhiên, lưu ý rằng, trên máy winXP này cũng phải đặt IP để kết nối đến CentOS server, và địa chỉ DNS server phải trở về địa chỉ IP của CentOS server.

Để các máy client có thể phân giải được một số tên miền hoặc địa chỉ IP không có trong DNS server ta cần forward lời đề nghị đó đến một DNS server khác, ở đây chọn DNS Server của Google.

```
...
directory "/var/named";
forwarders {8.8.8.8; };
...
```

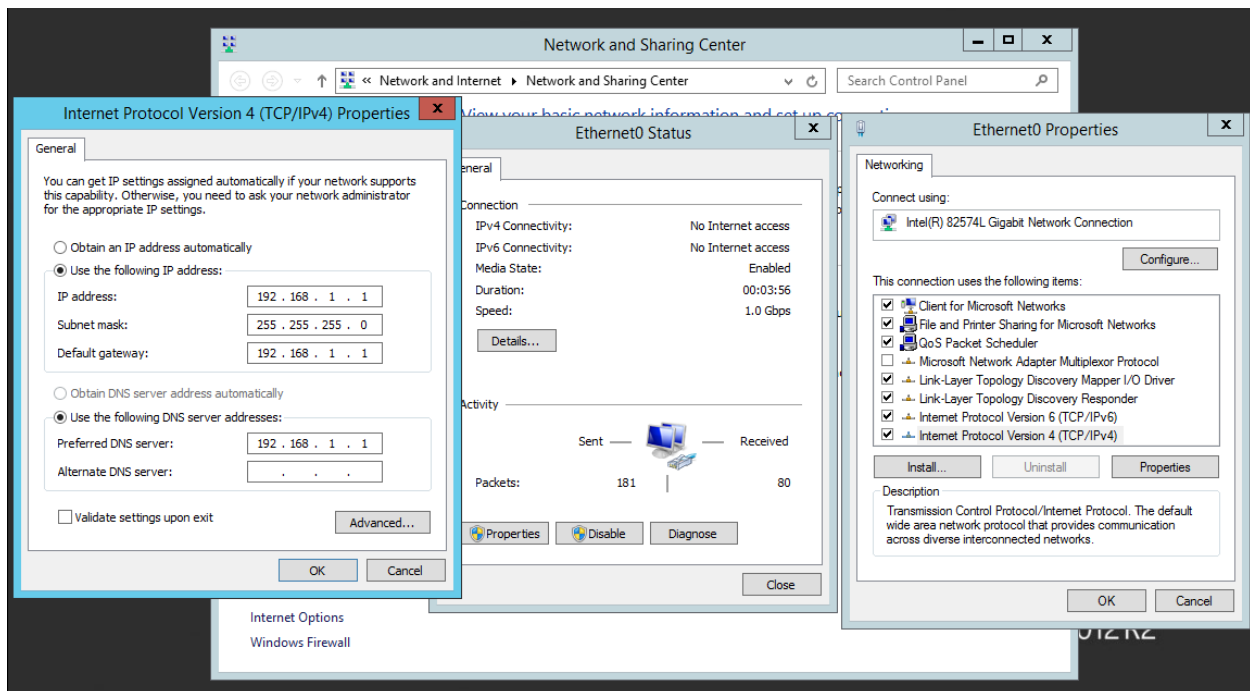
#### Cấu hình trên windows server 2012

Tương tự, ta cũng có thể cấu hình DNS server trên windows server 2012.

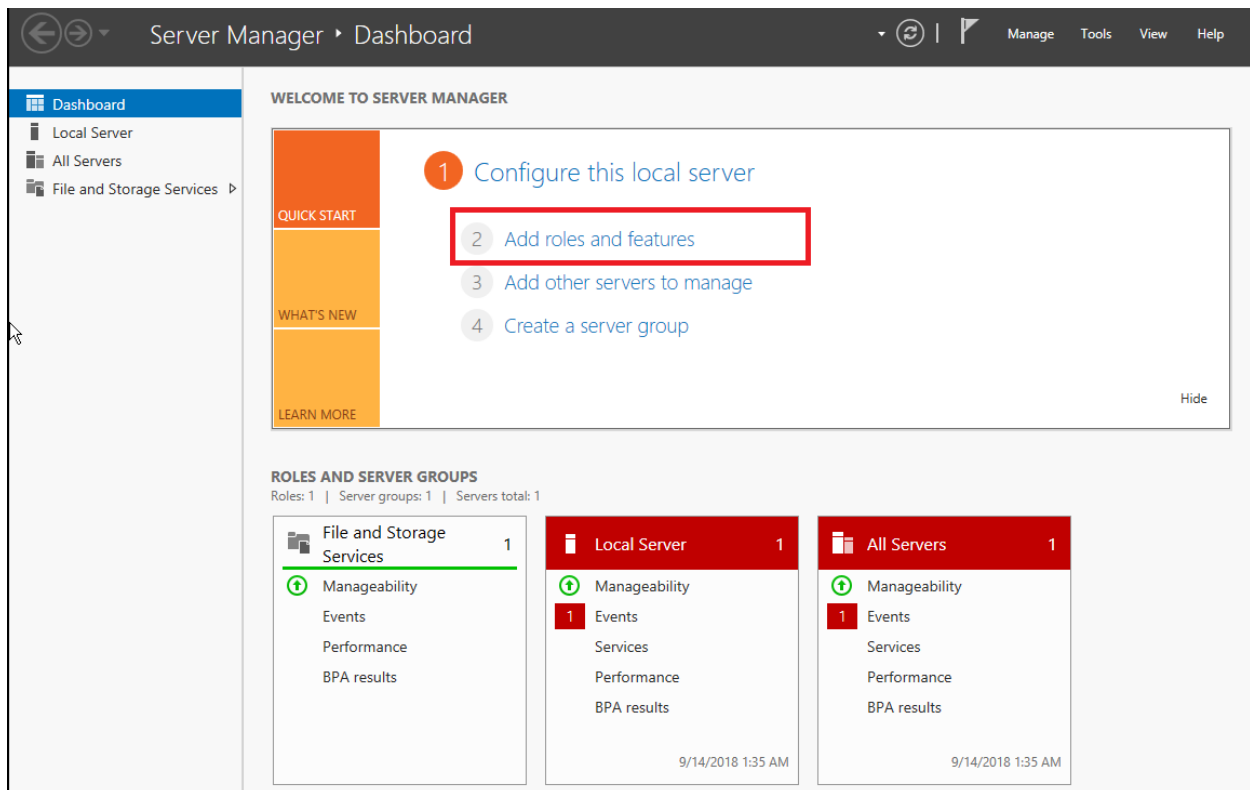
Để thực hiện được, ta cũng phải thiết lập IP tĩnh trên máy windows server 2012. Khác với cấu hình DNS trên CentOS7, khi làm trên windows server 2012, ta có thể không cần sử dụng kết nối internet.

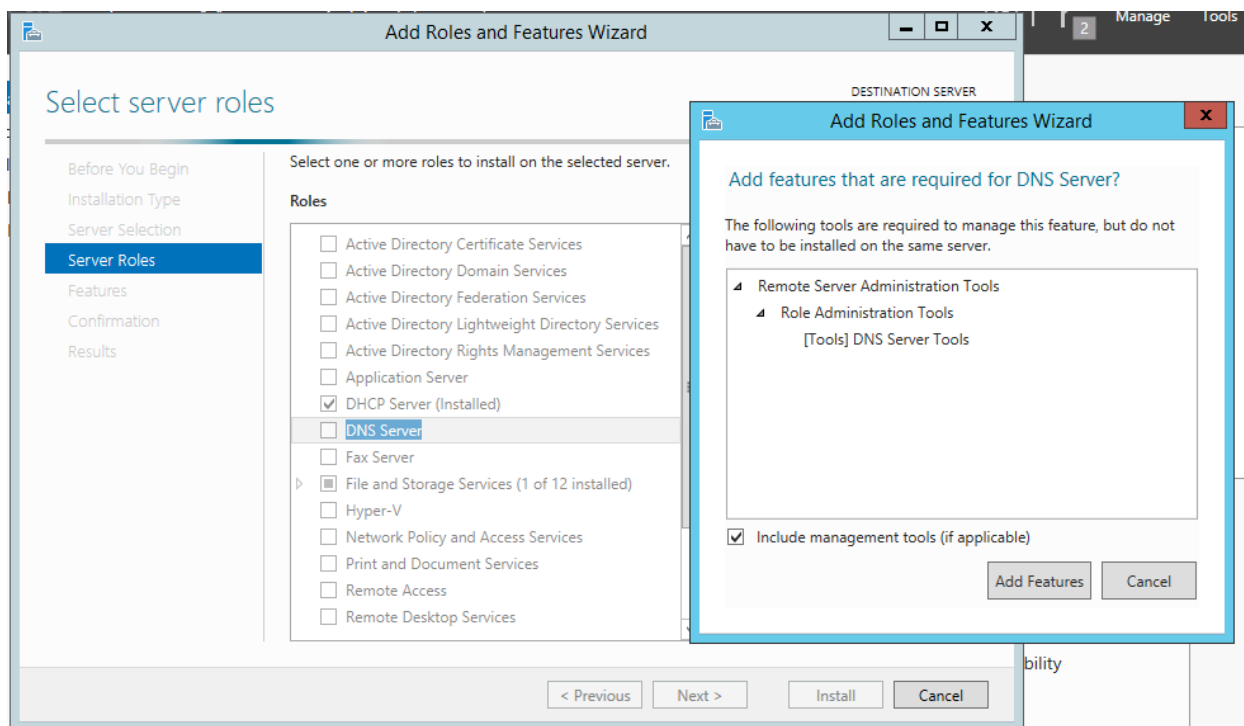
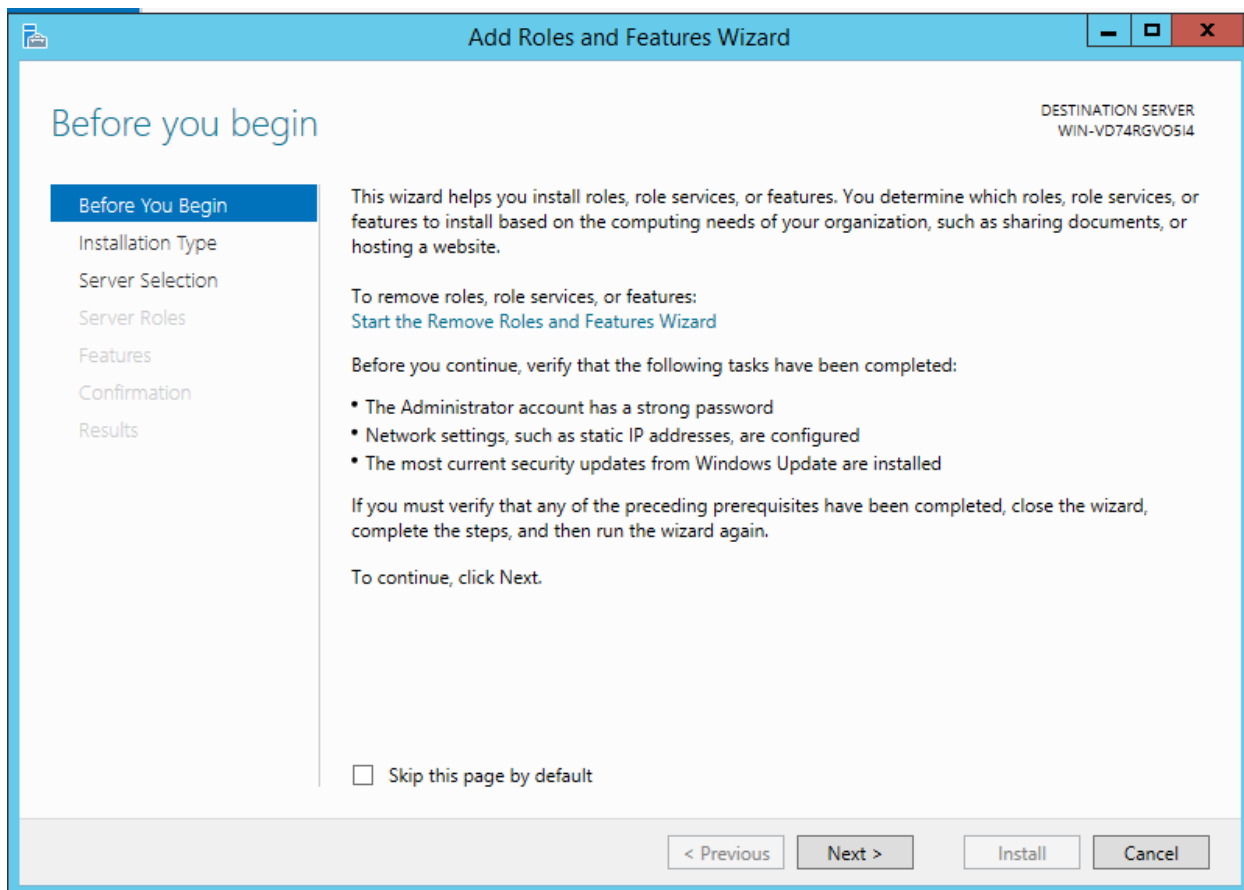
Các bước thực hiện như sau:

Thiết lập IP tĩnh cho server



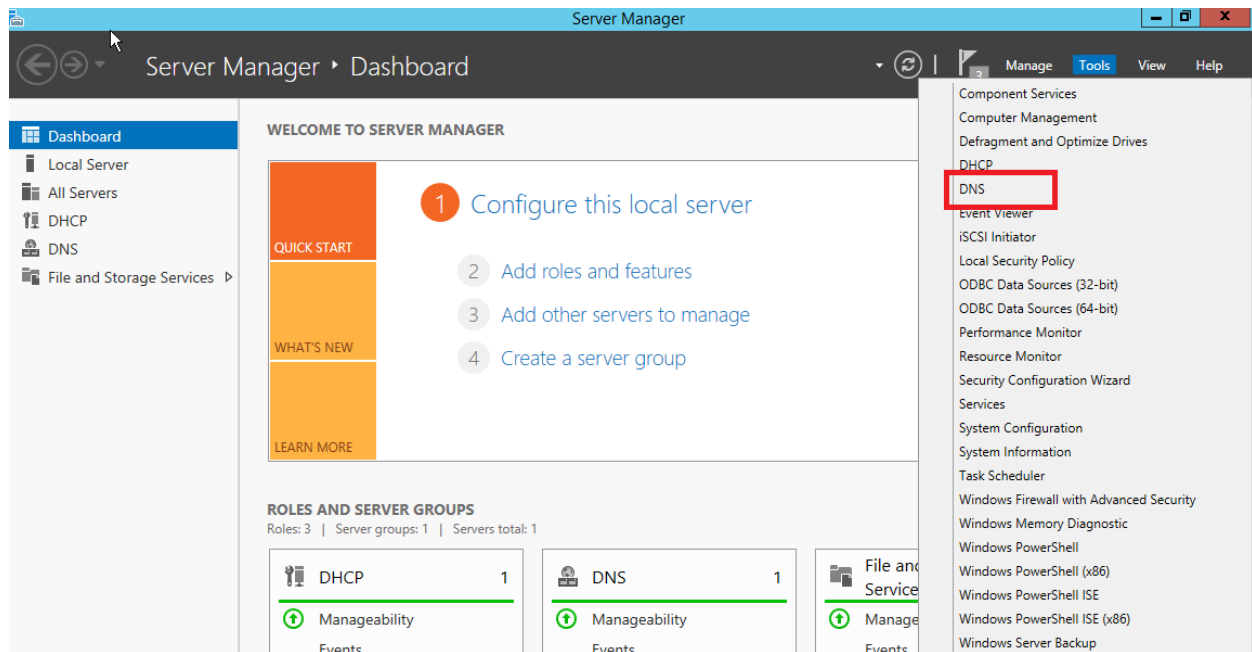
## Cài đặt DNS:





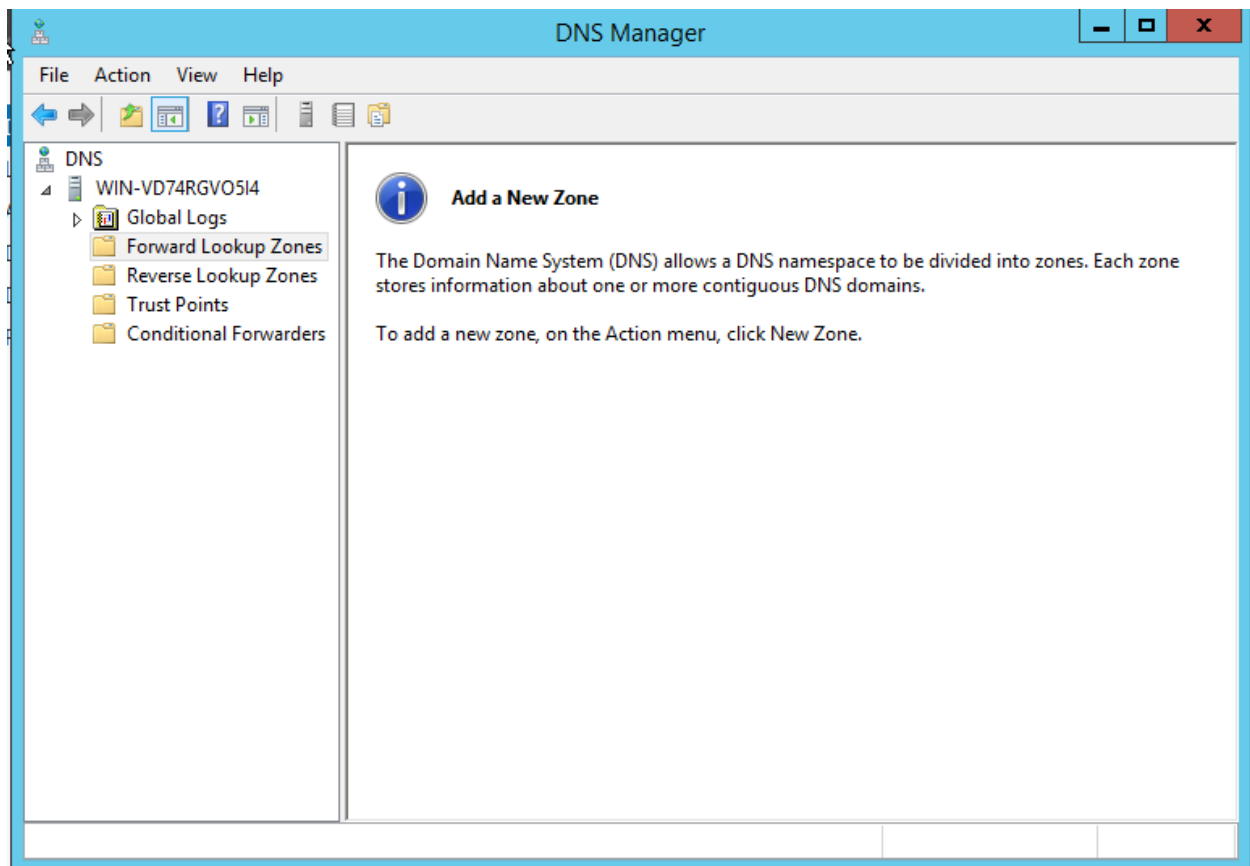
Sau đó, ta chọn Next tiếp cho các bước tiếp theo, cho đến khi cuối cùng là Install.

Sau khi hoàn thành, ta tiếp tục cấu hình:

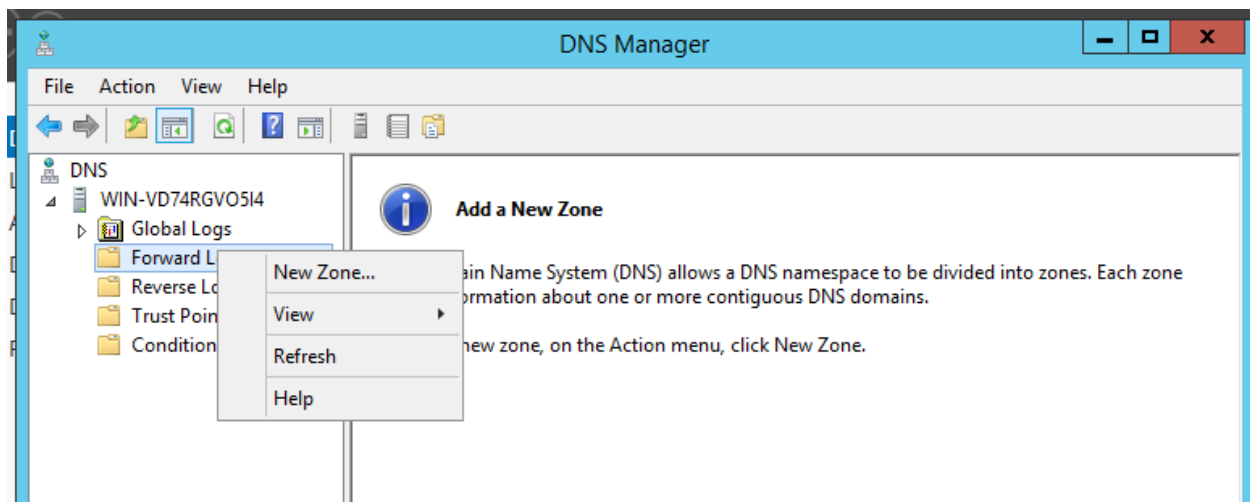


Ta cấu hình tại 2 phần là:

- Forward lookup zone: cấu hình zone thuận.
- Reverse lookup zone: cấu hình zone nghịch



Click phải vào cấu hình zone thuận:







- Primary Zone: vùng phân giải chính.
- Secondary Zone: vùng phân giải dự phòng.
- Stub Zone: chứa bản sao của các Name Server từ các DNS Server chính đã được xác thực.
- Tại đây, để tạo ra một DNS Server mới hoàn toàn, ta chọn Primary zone.

**New Zone Wizard**

**Zone Type**  
The DNS server supports various types of zones and storage.

Select the type of zone you want to create:

- ☒ **Primary zone**  
Creates a copy of a zone that can be updated directly on this server.
- ☐ **Secondary zone**  
Creates a copy of a zone that exists on another server. This option helps balance the processing load of primary servers and provides fault tolerance.
- ☐ **Stub zone**  
Creates a copy of a zone containing only Name Server (NS), Start of Authority (SOA), and possibly glue Host (A) records. A server containing a stub zone is not authoritative for that zone.
- ☐ **Store the zone in Active Directory** (available only if DNS server is a writeable domain controller)

< Back   Next >   Cancel

- Tại đây, ta nhập tên miền quản lý vào mục zone name

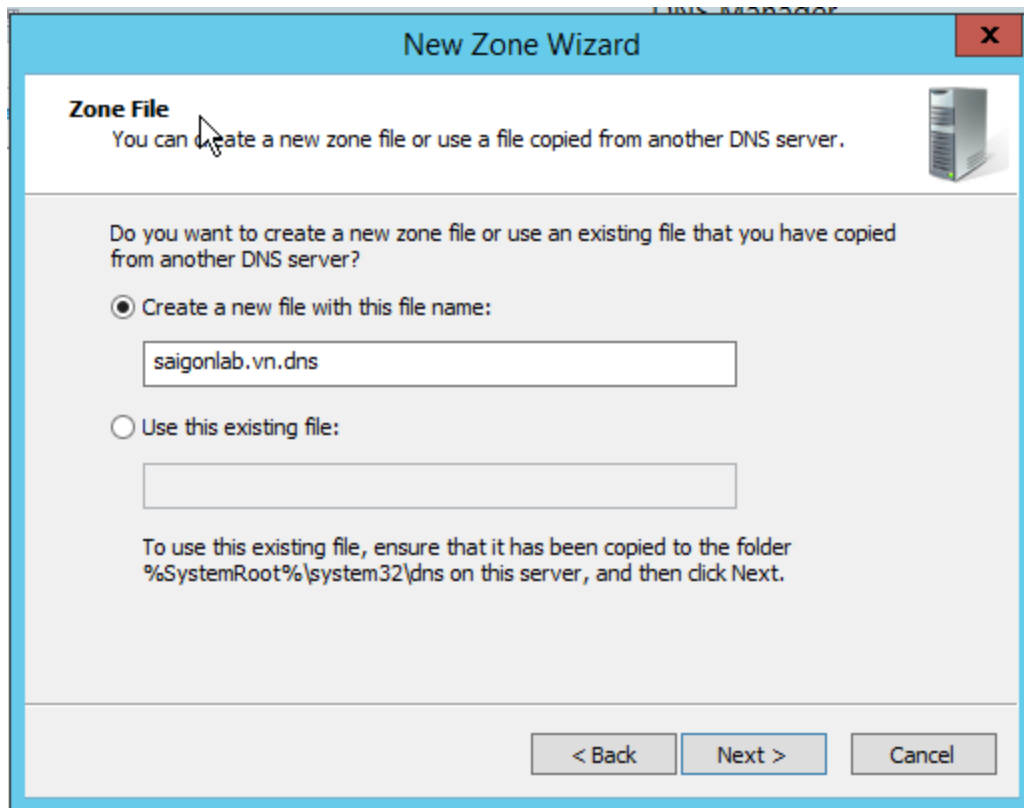
**New Zone Wizard**

**Zone Name**  
What is the name of the new zone?

The zone name specifies the portion of the DNS namespace for which this server is authoritative. It might be your organization's domain name (for example, microsoft.com) or a portion of the domain name (for example, newzone.microsoft.com). The zone name is not the name of the DNS server.

Zone name:  
saigonlab.vn

< Back   Next >   Cancel



- Chọn Allow both nonsecure and secure dynamic-updates: để cho phép cập nhật thông tin từ bất kỳ client một cách tự động.


### New Zone Wizard

**Dynamic Update**

You can specify that this DNS zone accepts secure, nonsecure, or no dynamic updates.

Dynamic updates enable DNS client computers to register and dynamically update their resource records with a DNS server whenever changes occur.

Select the type of dynamic updates you want to allow:

- ☐ Allow only secure dynamic updates (recommended for Active Directory)  
This option is available only for Active Directory-integrated zones.
- ☒ Allow both nonsecure and secure dynamic updates  
Dynamic updates of resource records are accepted from any client.  
 This option is a significant security vulnerability because updates can be accepted from untrusted sources.
- ☐ Do not allow dynamic updates  
Dynamic updates of resource records are not accepted by this zone. You must update these records manually.

< Back   Next >   Cancel

### New Zone Wizard

## Completing the New Zone Wizard

You have successfully completed the New Zone Wizard. You specified the following settings:

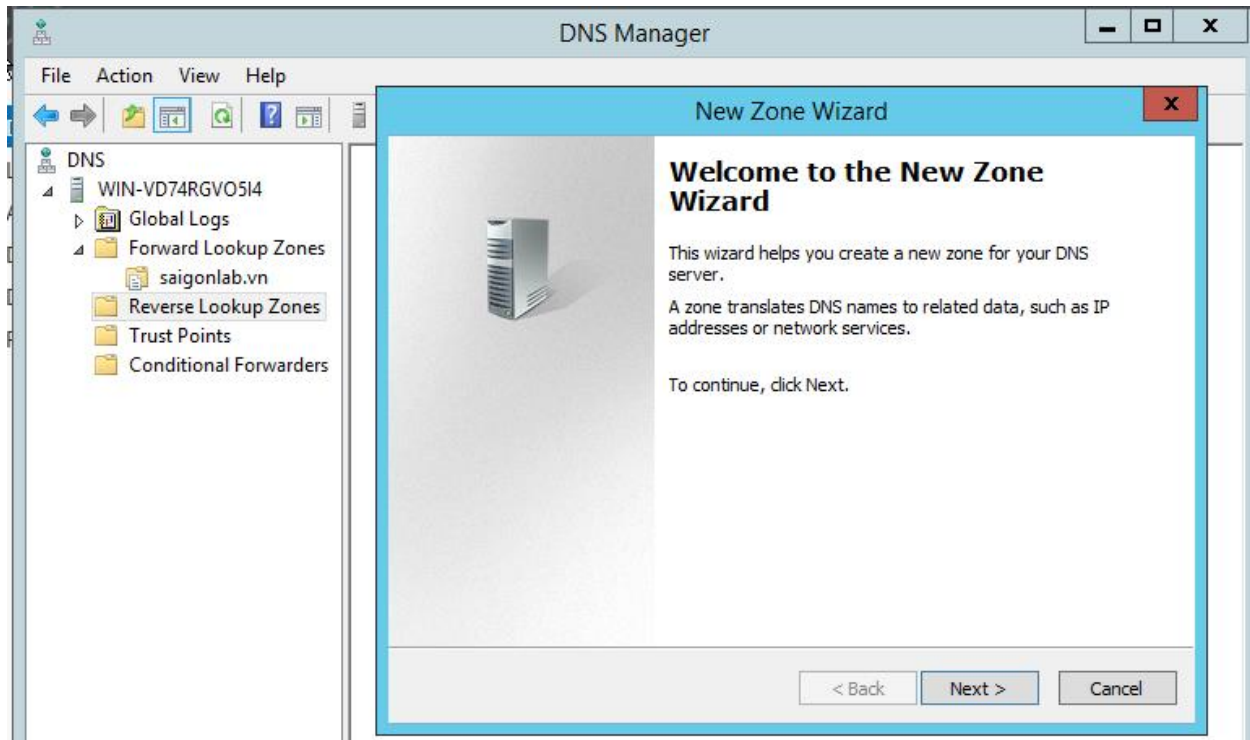
Name:	saigonlab.vn
Type:	Standard Primary
Lookup type:	Forward
File name:	saigonlab.vn.dns

Note: You should now add records to the zone or ensure that records are updated dynamically. You can then verify name resolution using nslookup.

To close this wizard and create the new zone, click Finish.

< Back   Finish   Cancel

- Click phải vào Reverse Lookup zones để cấu hình phân giải IP sang tên miền. Ta chọn New Zone



- Tương tự như khi tạo Forward Lookup Zone, ta cũng tạo ra Primary zone.

**New Zone Wizard**

**Zone Type**  
The DNS server supports various types of zones and storage.

Select the type of zone you want to create:

- ☒ **Primary zone**  
Creates a copy of a zone that can be updated directly on this server.
- ☐ **Secondary zone**  
Creates a copy of a zone that exists on another server. This option helps balance the processing load of primary servers and provides fault tolerance.
- ☐ **Stub zone**  
Creates a copy of a zone containing only Name Server (NS), Start of Authority (SOA), and possibly glue Host (A) records. A server containing a stub zone is not authoritative for that zone.
- ☐ **Store the zone in Active Directory** (available only if DNS server is a writeable domain controller)

< Back   Next >   Cancel

Tại đây, ta chọn IPv4 Reverse Lookup Zone.

**New Zone Wizard**

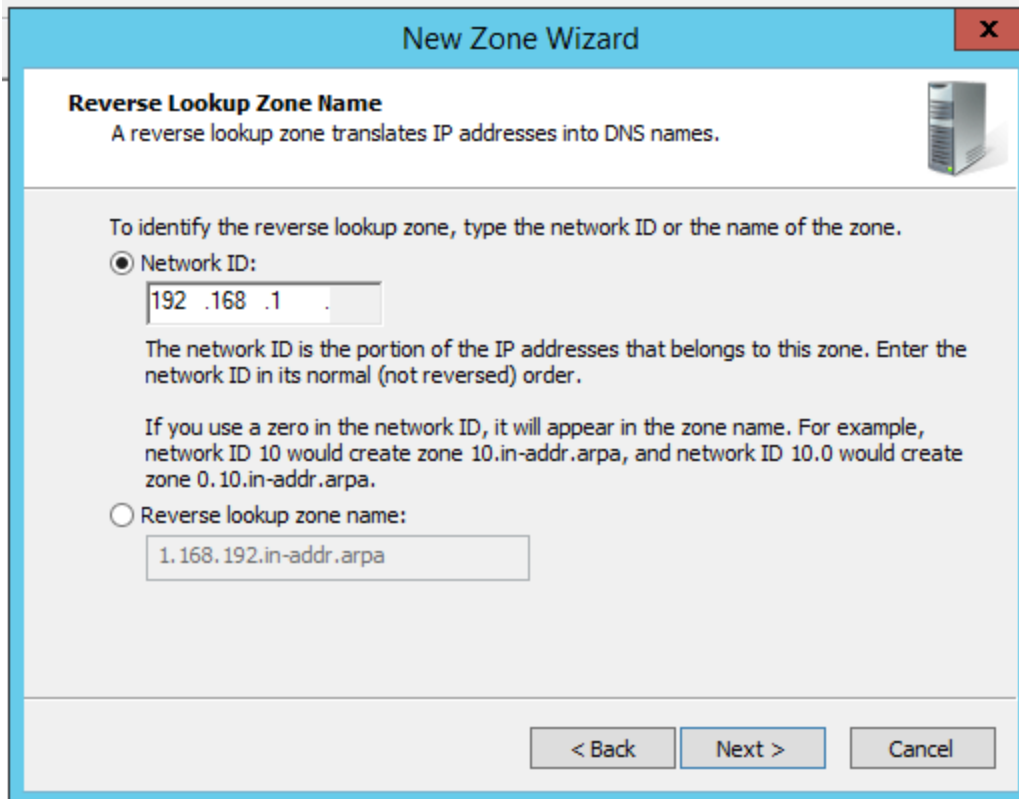
**Reverse Lookup Zone Name**  
A reverse lookup zone translates IP addresses into DNS names.

Choose whether you want to create a reverse lookup zone for IPv4 addresses or IPv6 addresses.

- ☒ **IPv4 Reverse Lookup Zone**
- ☐ **IPv6 Reverse Lookup Zone**

< Back   Next >   Cancel

- Ta nhập địa chỉ mạng của địa chỉ IP cần phân giải.



**New Zone Wizard**

**Reverse Lookup Zone Name**  
A reverse lookup zone translates IP addresses into DNS names.

To identify the reverse lookup zone, type the network ID or the name of the zone.

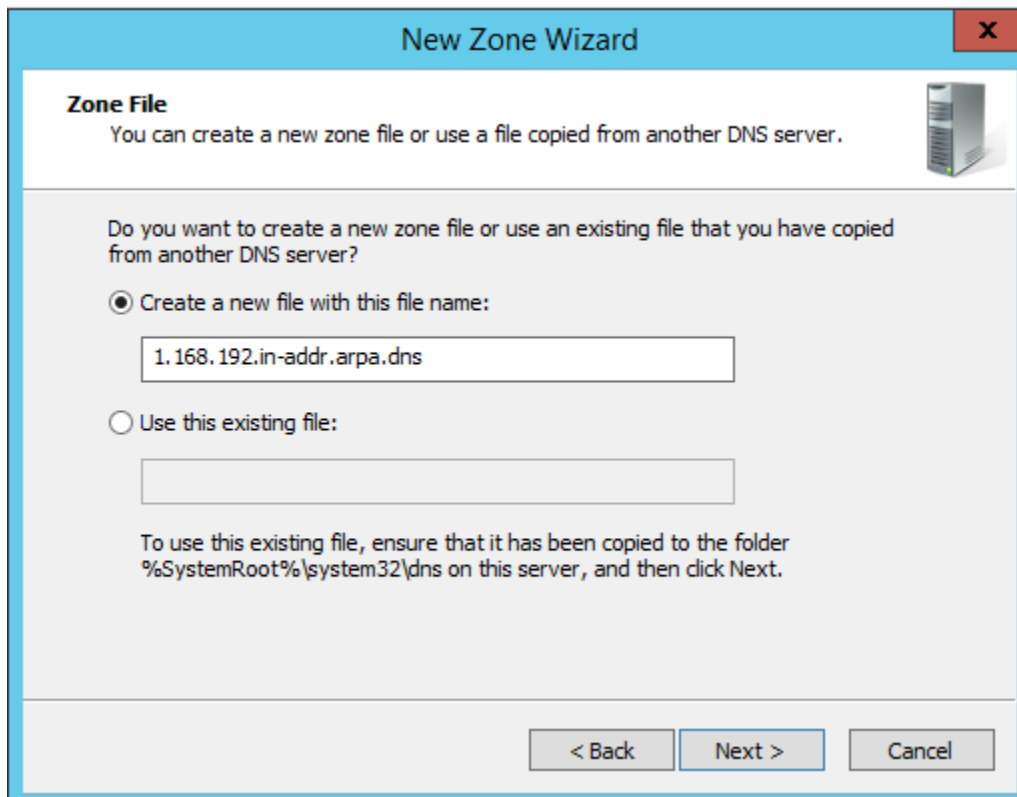
☒ Network ID:

The network ID is the portion of the IP addresses that belongs to this zone. Enter the network ID in its normal (not reversed) order.

If you use a zero in the network ID, it will appear in the zone name. For example, network ID 10 would create zone 10.in-addr.arpa, and network ID 10.0 would create zone 0.10.in-addr.arpa.

☐ Reverse lookup zone name:

< Back   Next >   Cancel



**New Zone Wizard**

**Zone File**  
You can create a new zone file or use a file copied from another DNS server.

Do you want to create a new zone file or use an existing file that you have copied from another DNS server?

☒ Create a new file with this file name:

☐ Use this existing file:

To use this existing file, ensure that it has been copied to the folder %SystemRoot%\system32\dns on this server, and then click Next.

< Back   Next >   Cancel

New Zone Wizard

**Dynamic Update**

You can specify that this DNS zone accepts secure, nonsecure, or no dynamic updates.

Dynamic updates enable DNS client computers to register and dynamically update their resource records with a DNS server whenever changes occur.

Select the type of dynamic updates you want to allow:

☐ Allow only secure dynamic updates (recommended for Active Directory)  
This option is available only for Active Directory-integrated zones.

☒ Allow both nonsecure and secure dynamic updates  
Dynamic updates of resource records are accepted from any client.  

!

This option is a significant security vulnerability because updates can be accepted from untrusted sources.

☐ Do not allow dynamic updates  
Dynamic updates of resource records are not accepted by this zone. You must update these records manually.

< Back

Next >

Cancel

New Zone Wizard

**Completing the New Zone Wizard**

You have successfully completed the New Zone Wizard. You specified the following settings:

Name: 1.168.192.in-addr.arpa

Type: Standard Primary

Lookup type: Reverse

File name: 1.168.192.in-addr.arpa.dns

Note: You should now add records to the zone or ensure that records are updated dynamically. You can then verify name resolution using nslookup.

To close this wizard and create the new zone, click Finish.

< Back

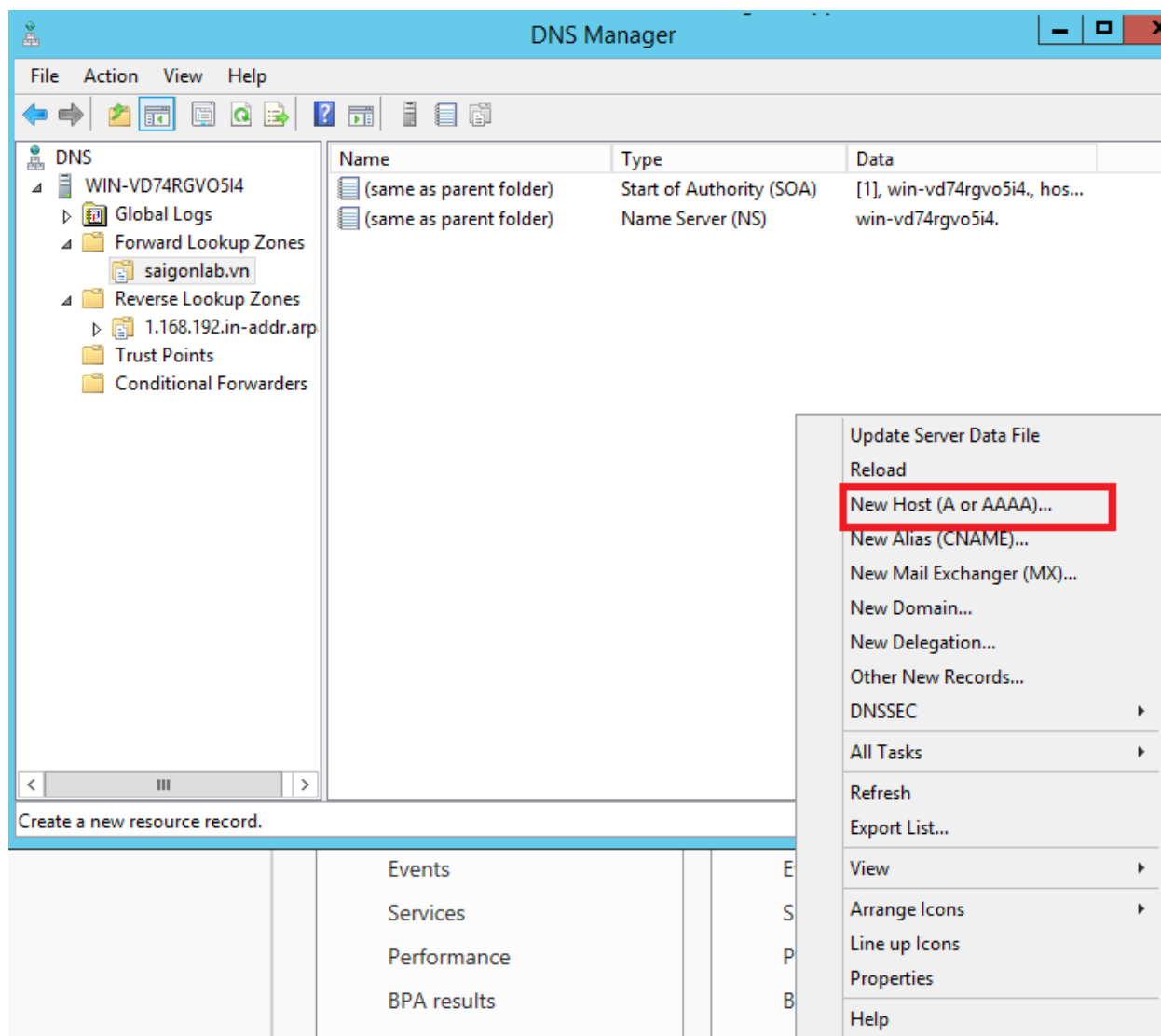
Finish

Cancel



Ta triển khai cấu hình sau khi cài đặt hoàn thành:

- Tại mục saigonlab.vn
- Ta click phải chọn New host (A or AAAA).. để cấu hình IP của tên miền này.



- Ta nhập địa chỉ IP vào phần IP address để xác định IP của tên miền saigonlab.vn.
- Lưu ý: chọn create associated pointer (PTR) record để tạo ra bản phân giải ngược.

New Host

Name (uses parent domain name if blank):

Fully qualified domain name (FQDN):

saigonlab.vn.

IP address:

192.168.1.1

☒ Create associated pointer (PTR) record

Add Host Cancel

- Nếu cần tạo ra một Alias (tên định danh), ta click phải chọn New Alias, sau đó nhập vào Alias Name. Tại đây nhập vào www
- Sau đó chọn vào tên miền hoàn chỉnh dùng để trở về. Ở đây là saigonlab.vn

**New Resource Record** [X]

Alias (CNAME)

Alias name (uses parent domain if left blank):

Fully qualified domain name (FQDN):

Fully qualified domain name (FQDN) for target host:

[OK] [Cancel]

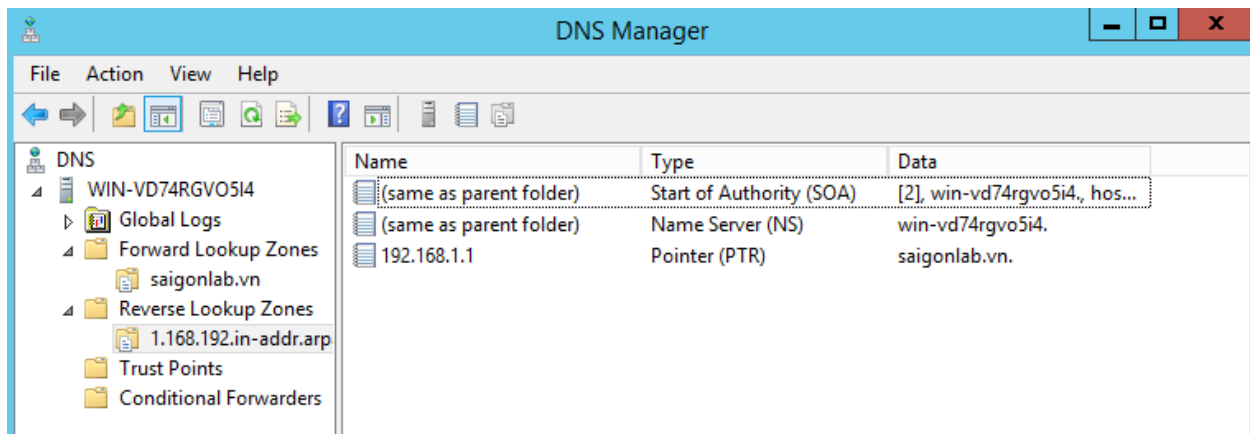
- Sau khi hoàn thành, ta có:

**DNS Manager** [-] [X]

File Action View Help

← → [Icons]

	Name	Type	Data
WIN-VD74RGVO5I4	(same as parent folder)	Start of Authority (SOA)	[1], win-vd74rgvo5i4, hos...
Global Logs	(same as parent folder)	Name Server (NS)	win-vd74rgvo5i4.
Forward Lookup Zones	(same as parent folder)	Host (A)	192.168.1.1
saigonlab.vn	www	Alias (CNAME)	saigonlab.vn
Reverse Lookup Zones			
1.168.192.in-addr.arp			
Trust Points			
Conditional Forwarders			



Tại client, sau khi trỏ DNS, ta nhập lệnh nslookup để kiểm tra DNS

```
C:\Documents and Settings\Administrator>nslookup
Default Server:  saigonlab.vn
Address:  192.168.1.1

> 192.168.1.1
Server:  saigonlab.vn
Address: 192.168.1.1

Name:    saigonlab.vn
Address: 192.168.1.1

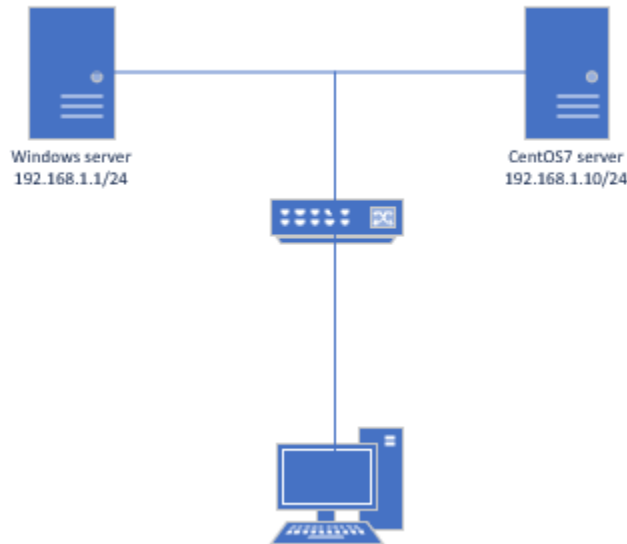
> saigonlab.vn
Server:  saigonlab.vn
Address: 192.168.1.1

DNS request timed out.
  timeout was 2 seconds.
Name:    saigonlab.vn
Address: 192.168.1.1

>
```

## Bài tập thực hành:

Cho sơ đồ như sau:



Hãy thực hiện các yêu cầu sau:

Đối với server sử dụng hệ điều hành CentOS 7, thực hiện cài đặt dịch vụ DNS:

- DNS: quản lý tên miền: sgu.edu.vn trở về địa chỉ: 192.168.1.210/24, qtm.vn trở về địa chỉ 192.168.1.200/24 và lab.net trở về địa chỉ: 172.16.0.1/16

Đối với server sử dụng hệ điều hành windows server 2012, thực hiện cài đặt dịch vụ DNS:

- DNS: quản lý tên miền: IT.net trở về địa chỉ: 192.168.1.150/24, data.org trở về địa chỉ: 172.16.20.5/16, và relax.com trở về địa chỉ: 210.5.3.100/16.

Hãy cấu hình để máy CentOS7 và máy Windows server có thể trao đổi quá trình phân giải tên với nhau.

**HẾT**

