

Bài 7:**CÀI ĐẶT VÀ CẤU HÌNH DỊCH VỤ DNS**

Các nội dung chính sẽ được đề cập:

- ✓ Cài đặt và cấu hình DNS Server.
- ✓ Cấu hình dịch vụ Backup DNS.

7.1 Cài đặt và cấu hình DNS Server.**1. Yêu cầu bài lab:**

+ Cài đặt dịch vụ **DNS** trên máy **BKAP-SRV12-01**.

+ Cấu hình dịch vụ **DNS**:

- Cấu hình **Primary Zone** trong **Forward Lookup Zone** với tên: **bkaptech.vn**.
- Cấu hình **Reverse Zone** trong **Reverse Lookup Zone** với dải **:192.168.1.0**.
- Cấu hình các bản ghi : A, PTR, CNAME, MX....

+ Khai báo **DNS client** và kiểm tra:

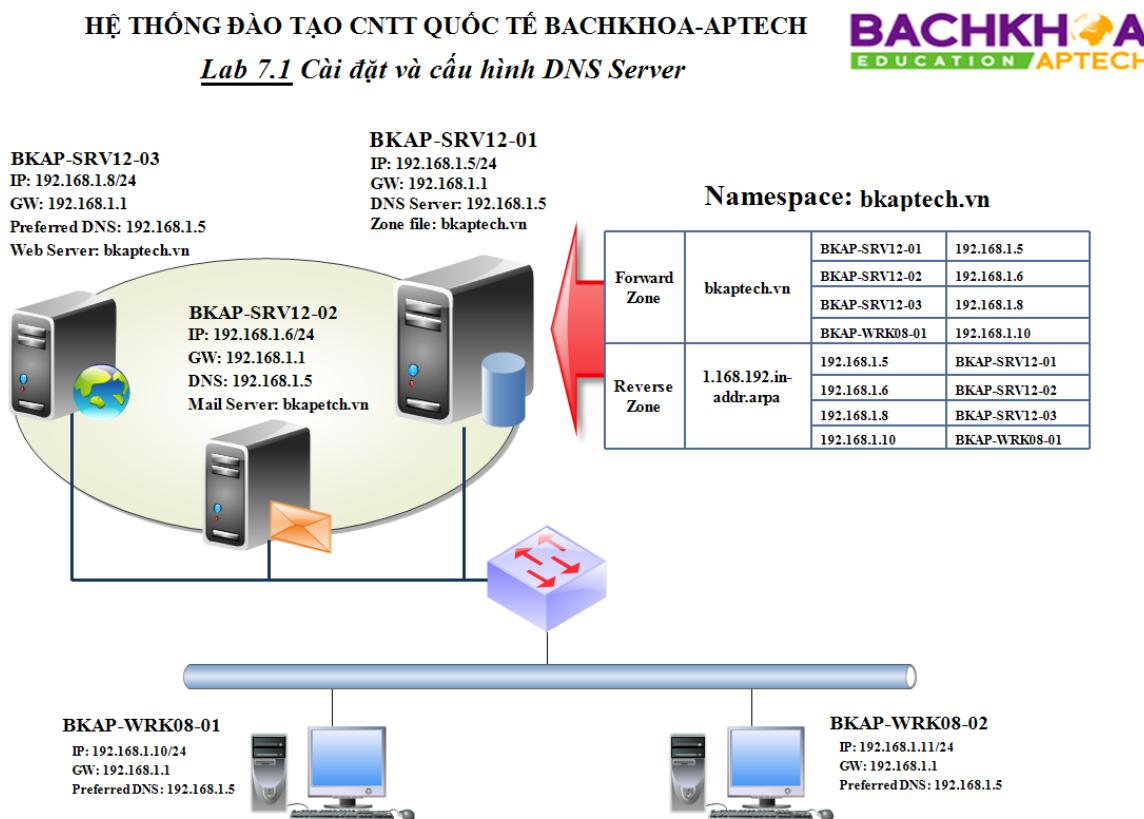
- Khai báo tên máy :**BKAP-SRV12-01**.
- Dùng **nslookup** để kiểm tra phân giải.

2. Yêu cầu chuẩn bị:

+ Chuẩn bị 1 máy Server **BKAP-SRV12-01** để cài đặt dịch vụ **DNS**.

+ Chuẩn bị 1 máy Client **BKAP-WRK08-01** để kiểm tra phân giải.

3. Mô hình lab:



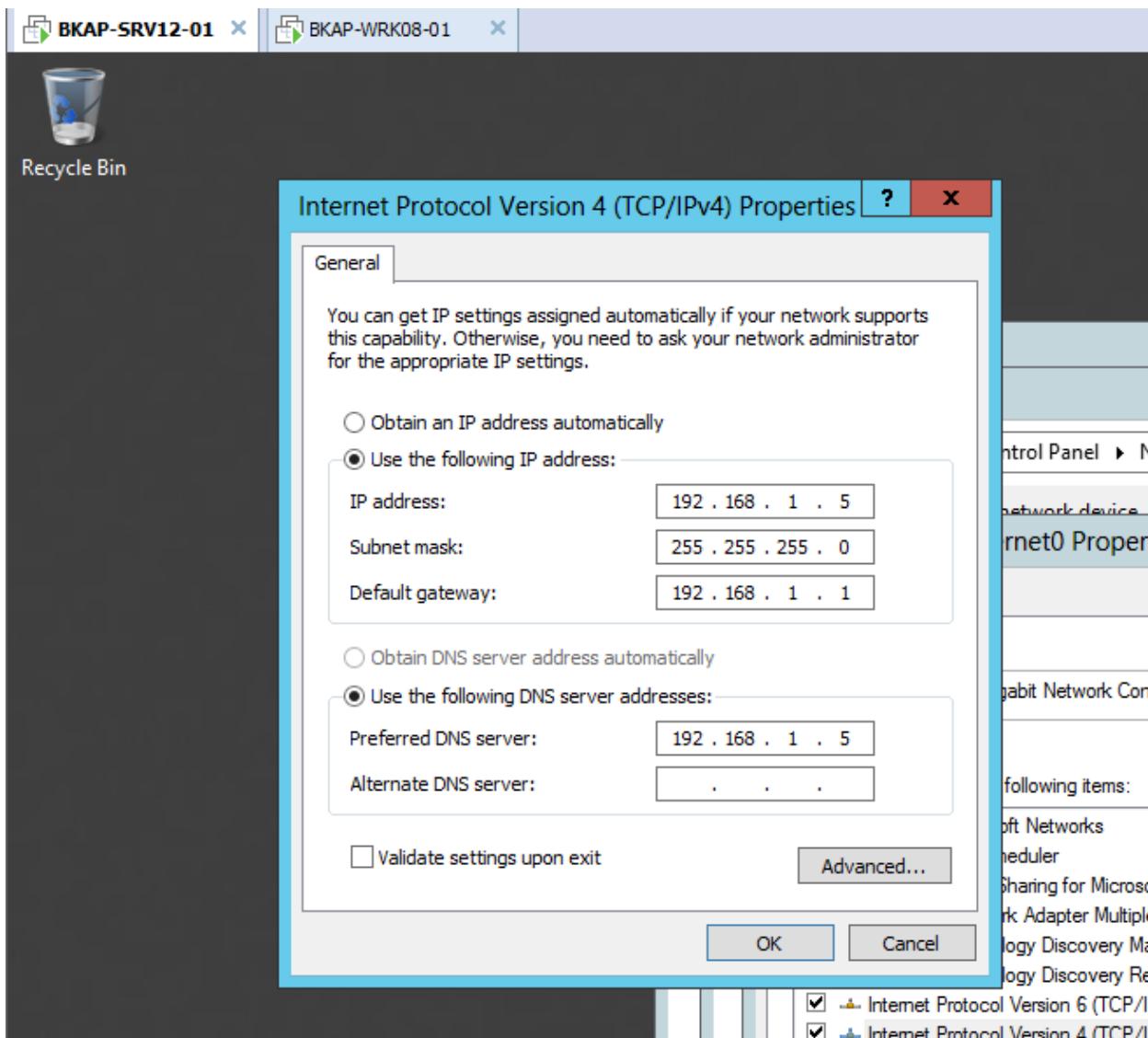
Hình 7.1

Sơ đồ địa chỉ như sau:

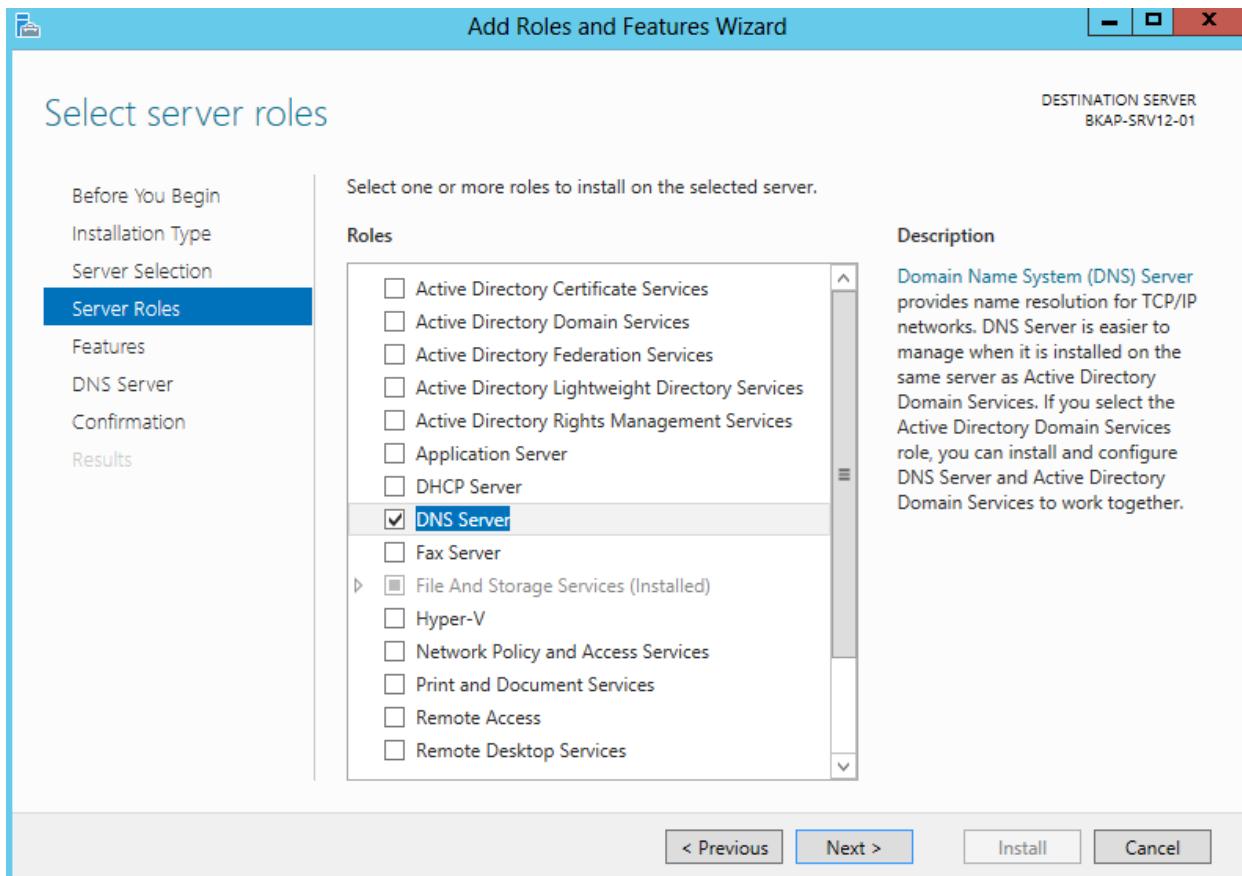
Thông số	BKAP-SRV12-01	BKAP-WRK08-01
IP address	192.168.1.5	192.168.1.10
Subnet Mask	255.255.255.0	255.255.255.0
Default gateway	192.168.1.1	192.168.1.1
Preferred DNS Server	192.168.1.5	192.168.1.5

Hướng dẫn chi tiết:

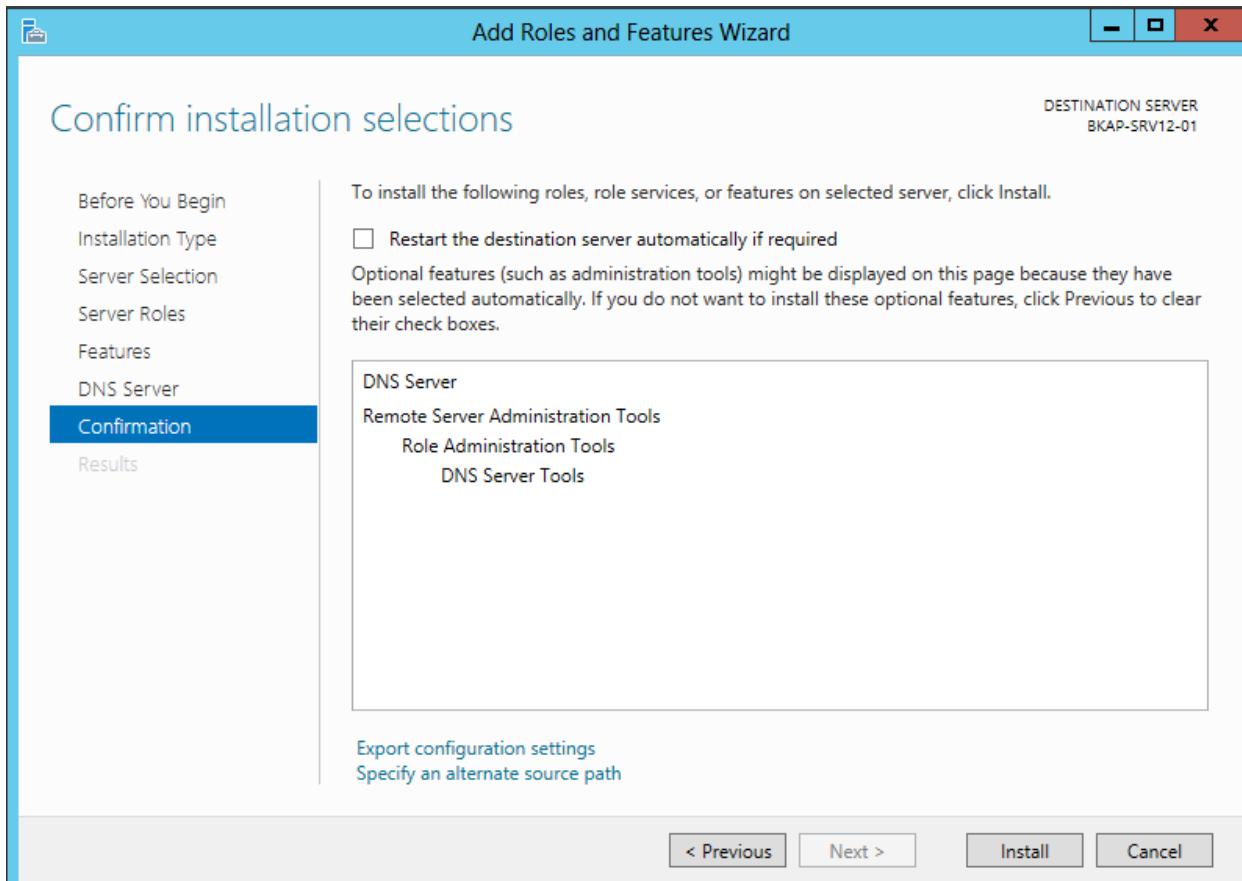
- Thực hiện trên máy **BKAP-SRV12-01**:
 - Cài đặt dịch vụ **DNS** và tạo các bản ghi:
 - Địa chỉ của máy **BKAP-SRV12-01**:



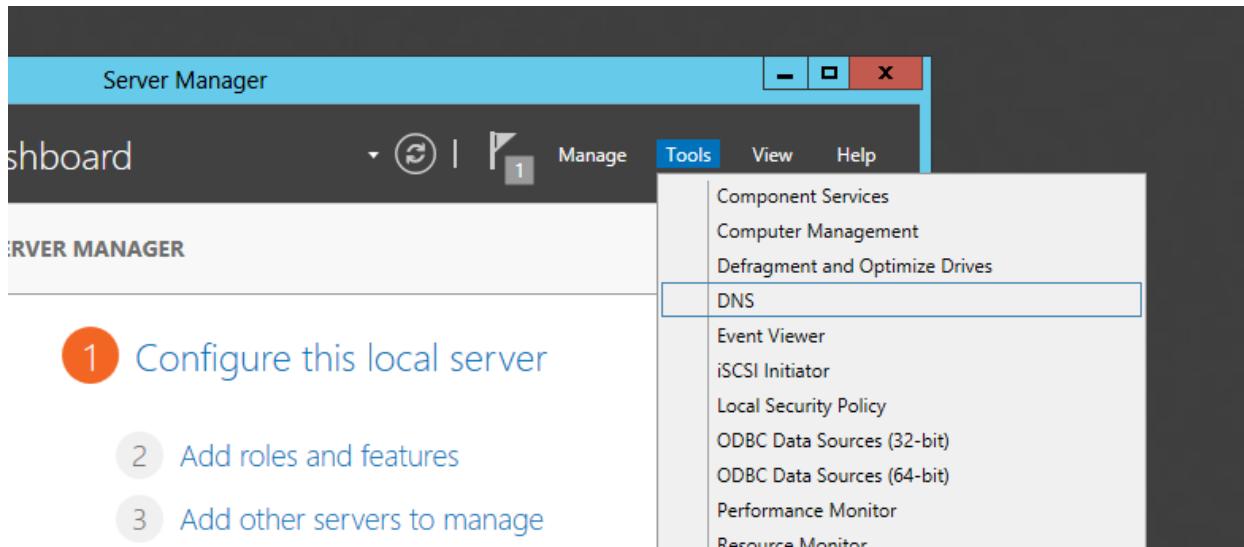
- Cài đặt dịch vụ **DNS**:
 - Vào **Server Manager /Add roles and features**
 - Tại cửa sổ **Select server roles**, click chọn vào dịch vụ **DNS**



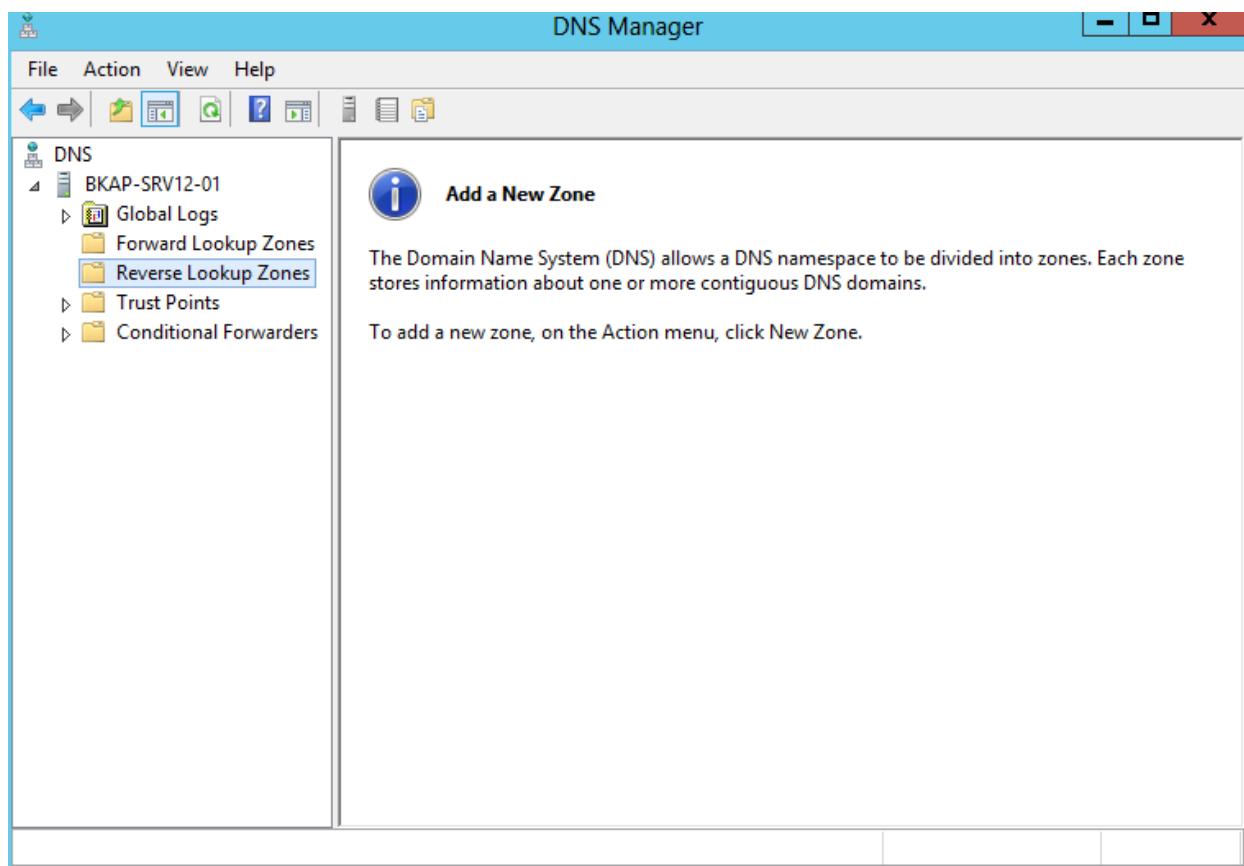
- Tiếp tục click vào **Next**, tại cửa sổ **Confirm installation selections**, click vào **Install** để Server cài đặt dịch vụ DNS.



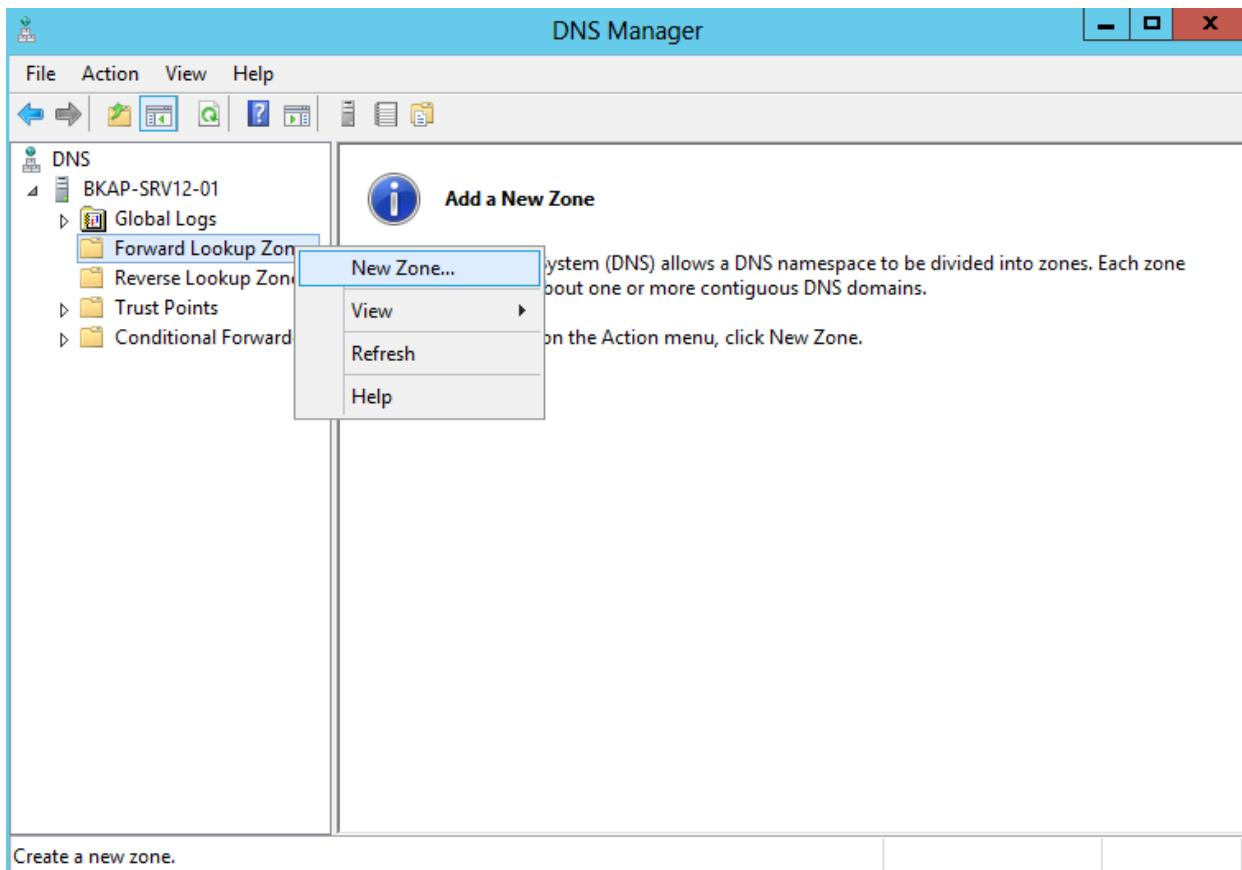
- Tại cửa sổ **Installation progress**, click vào **Close** để kết thúc quá trình cài đặt.
- Cấu hình dịch vụ **DNS**:
 - Vào **Server Manager / Tools** / chọn vào dịch vụ **DNS**.



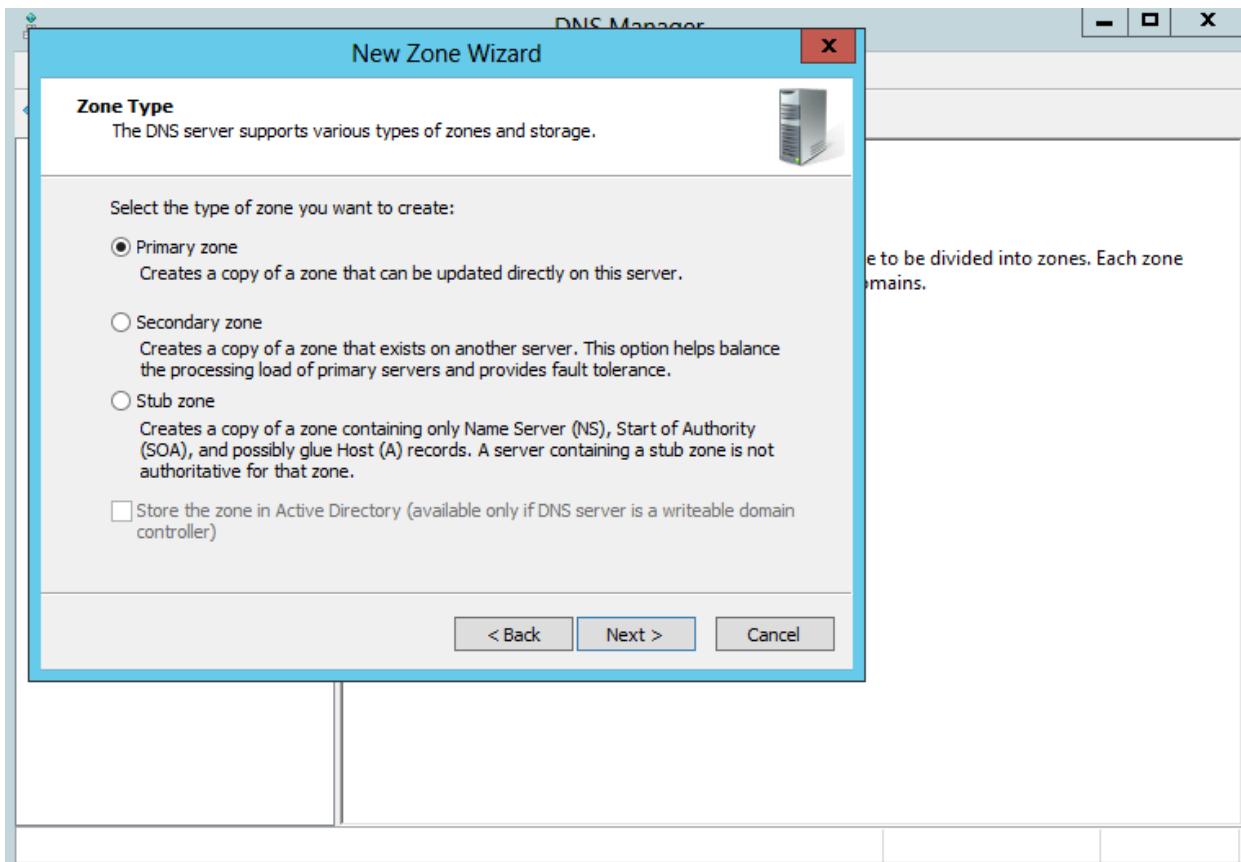
▪ Cửa sổ **DNS**:



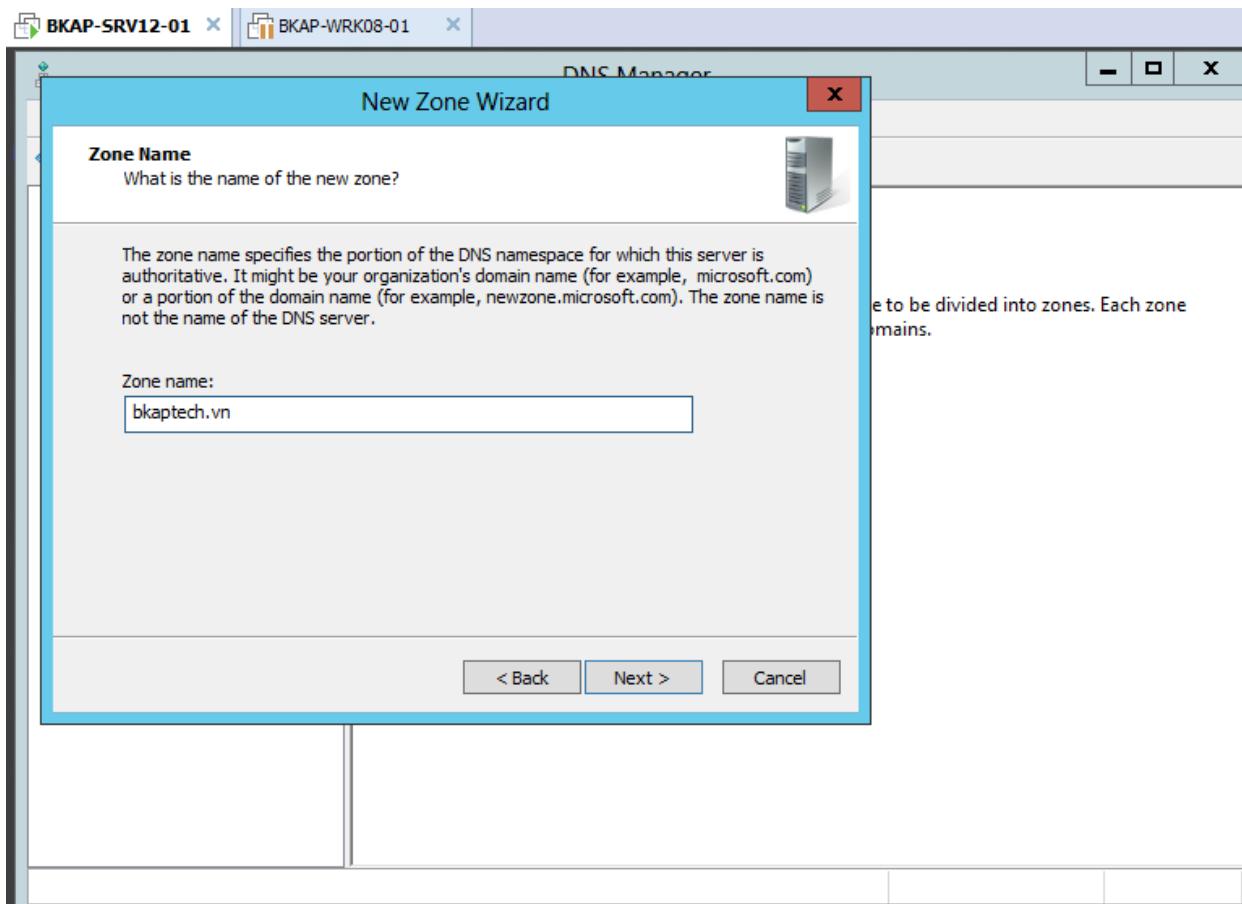
- Click chuột phải tại **Forward Lookup Zones** chọn **New Zone...**



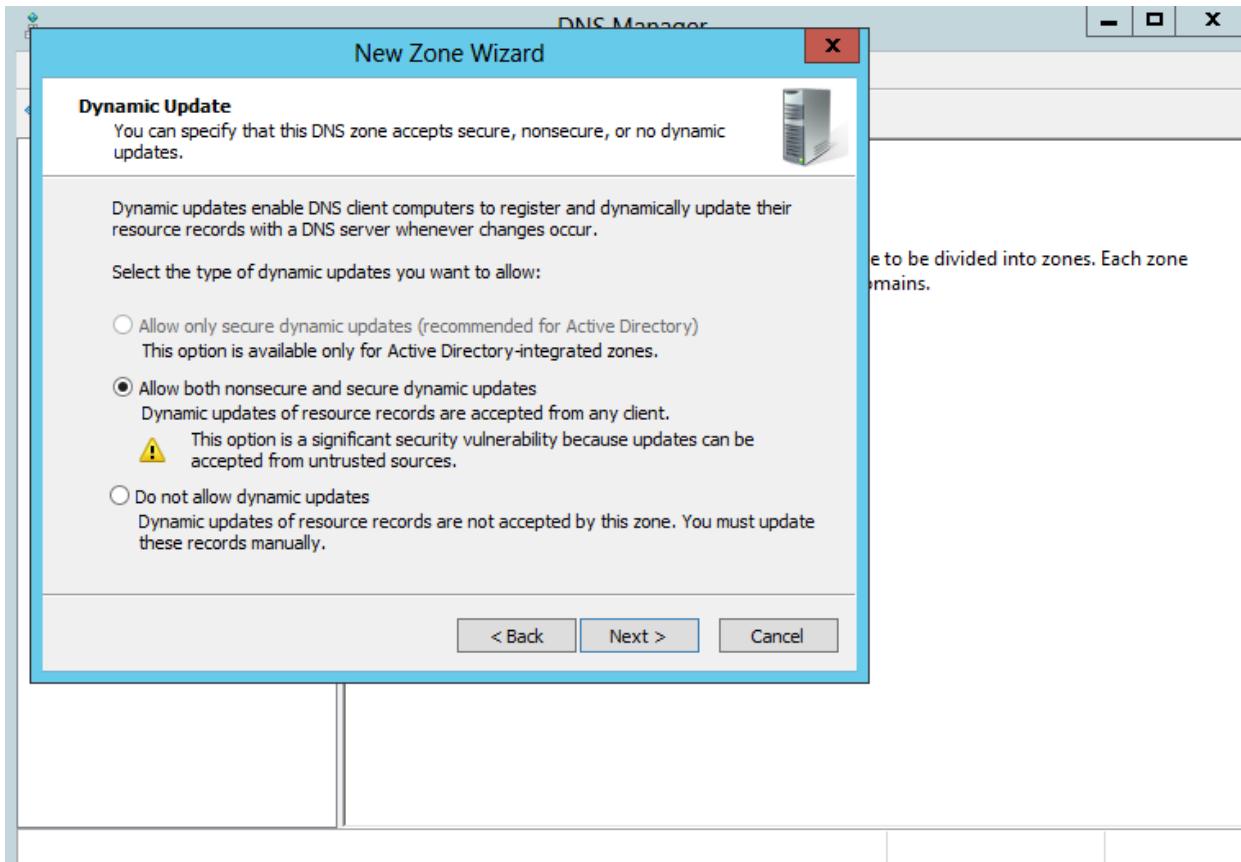
- Tại cửa sổ **Zone Type**, chọn vào **Primary zone**.



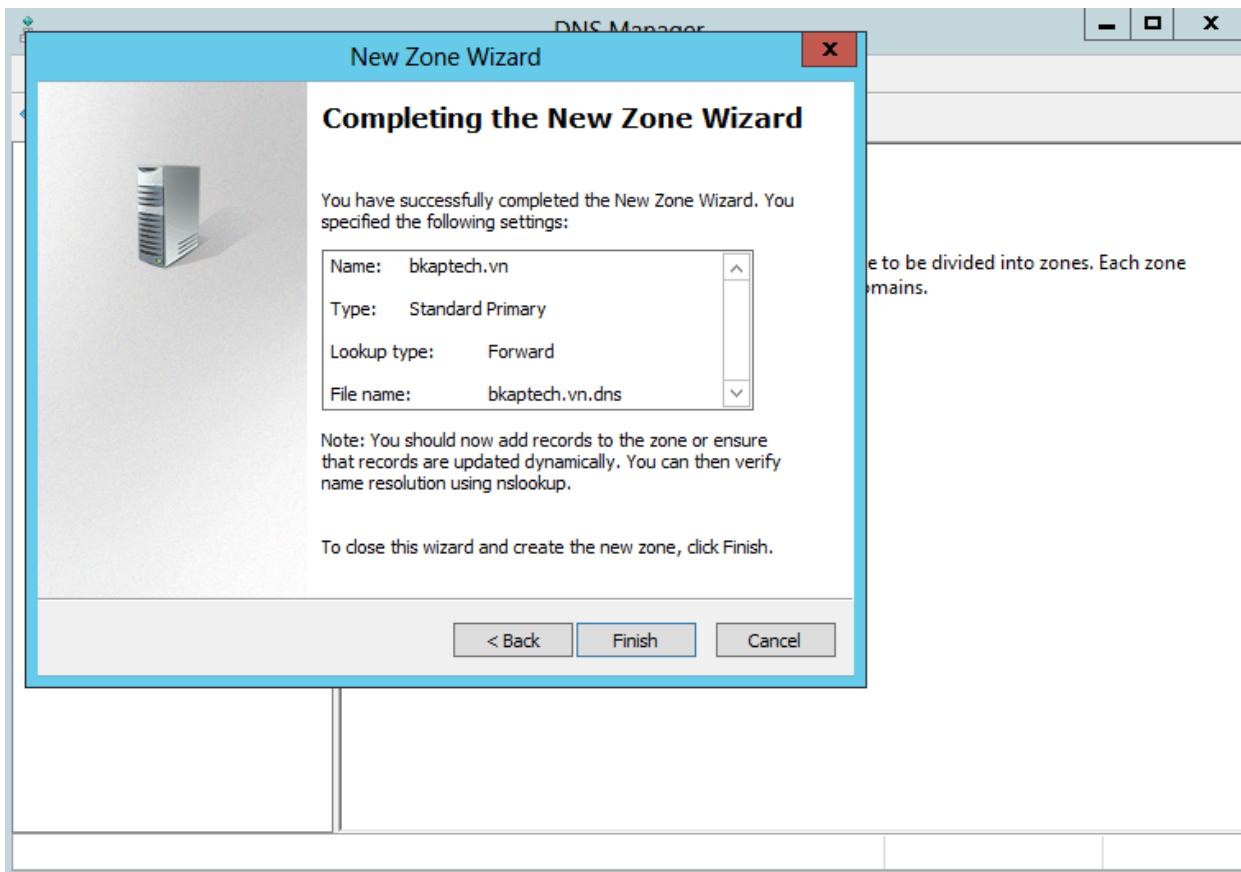
- Tại cửa sổ **Zone Name**, nhập vào tên miền : **bkaptech.vn**



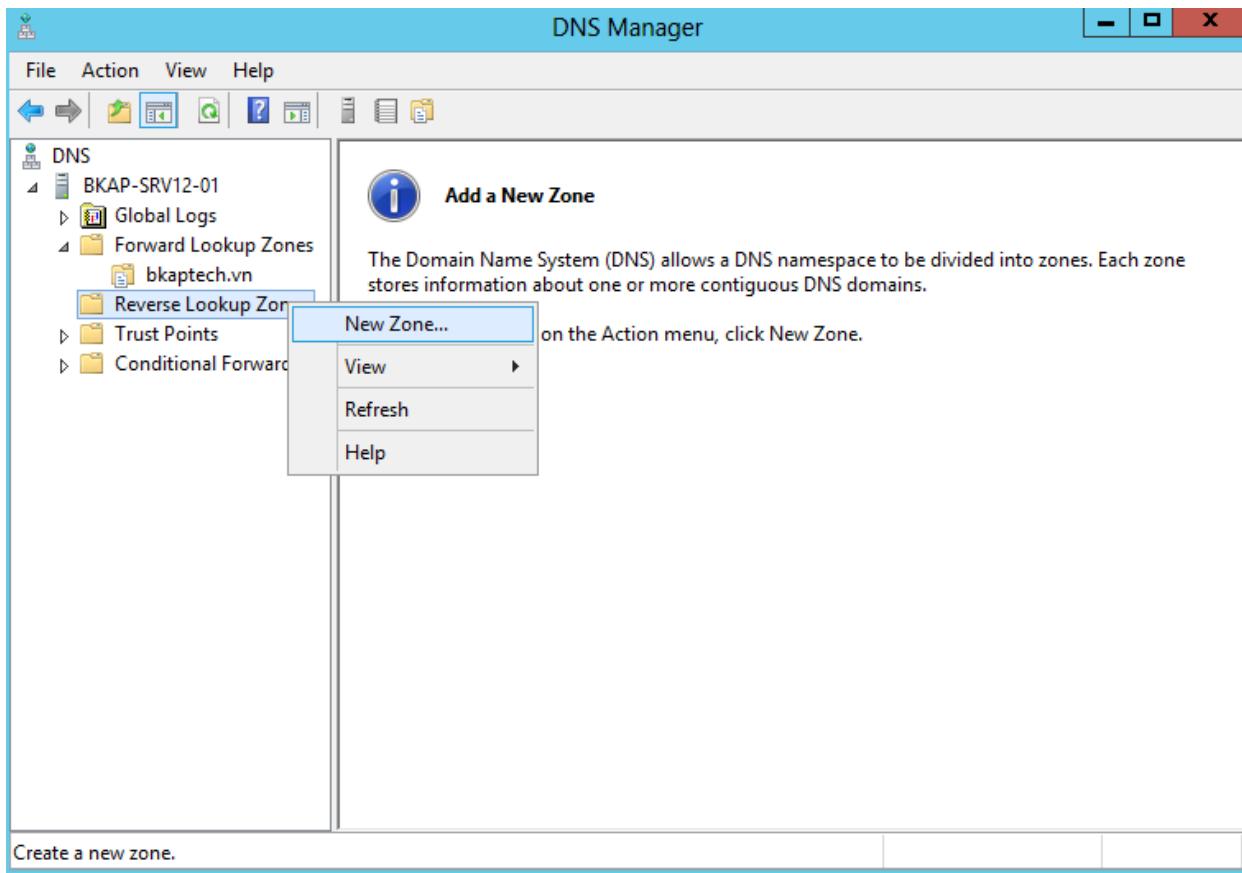
- Tiếp tục click vào **Next**, tại cửa sổ **Dynamic Update**, chọn vào **Allow both nonsecure and secure dynamic updates**.



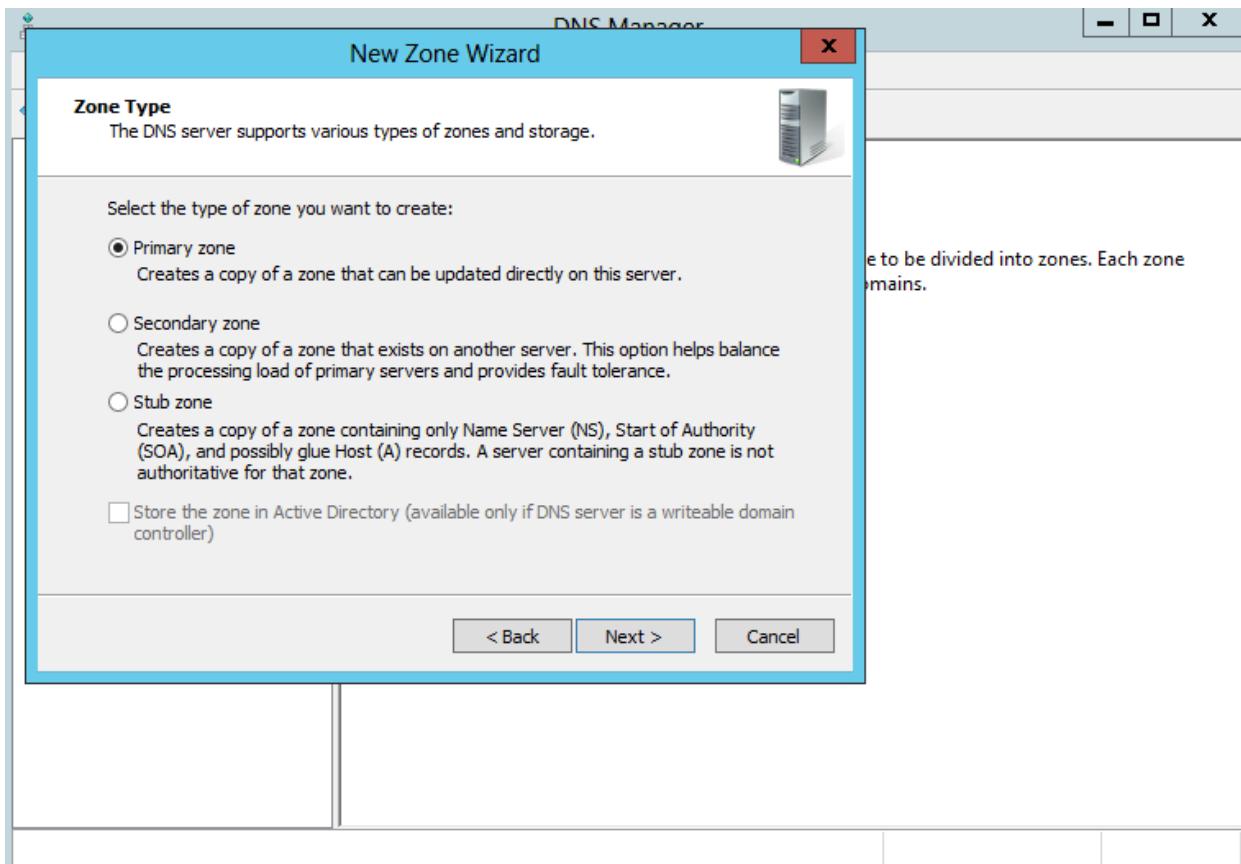
- Click vào **Finish** để kết thúc quá trình cài đặt.



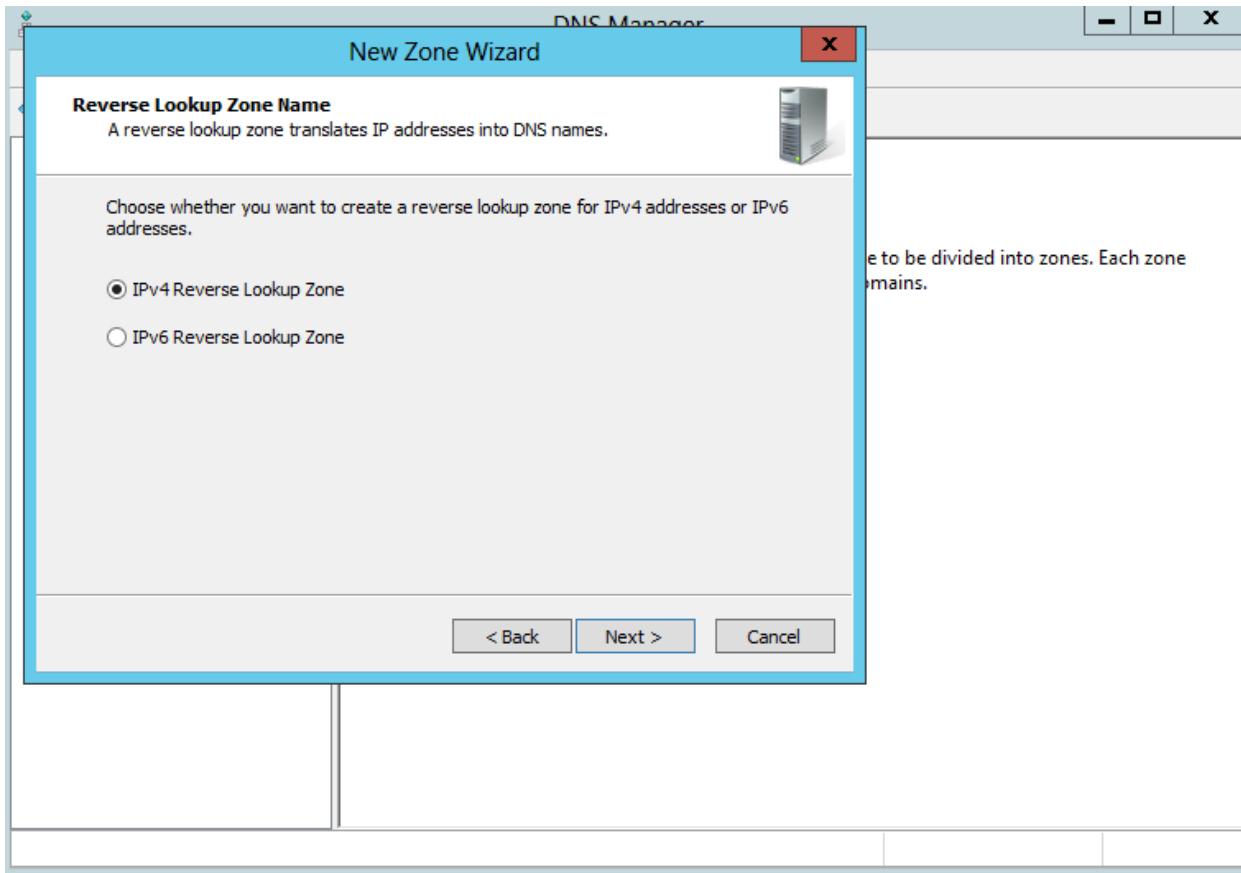
- Click chuột phải tại **Reverse Lookup Zones**, chọn vào **New Zone**.



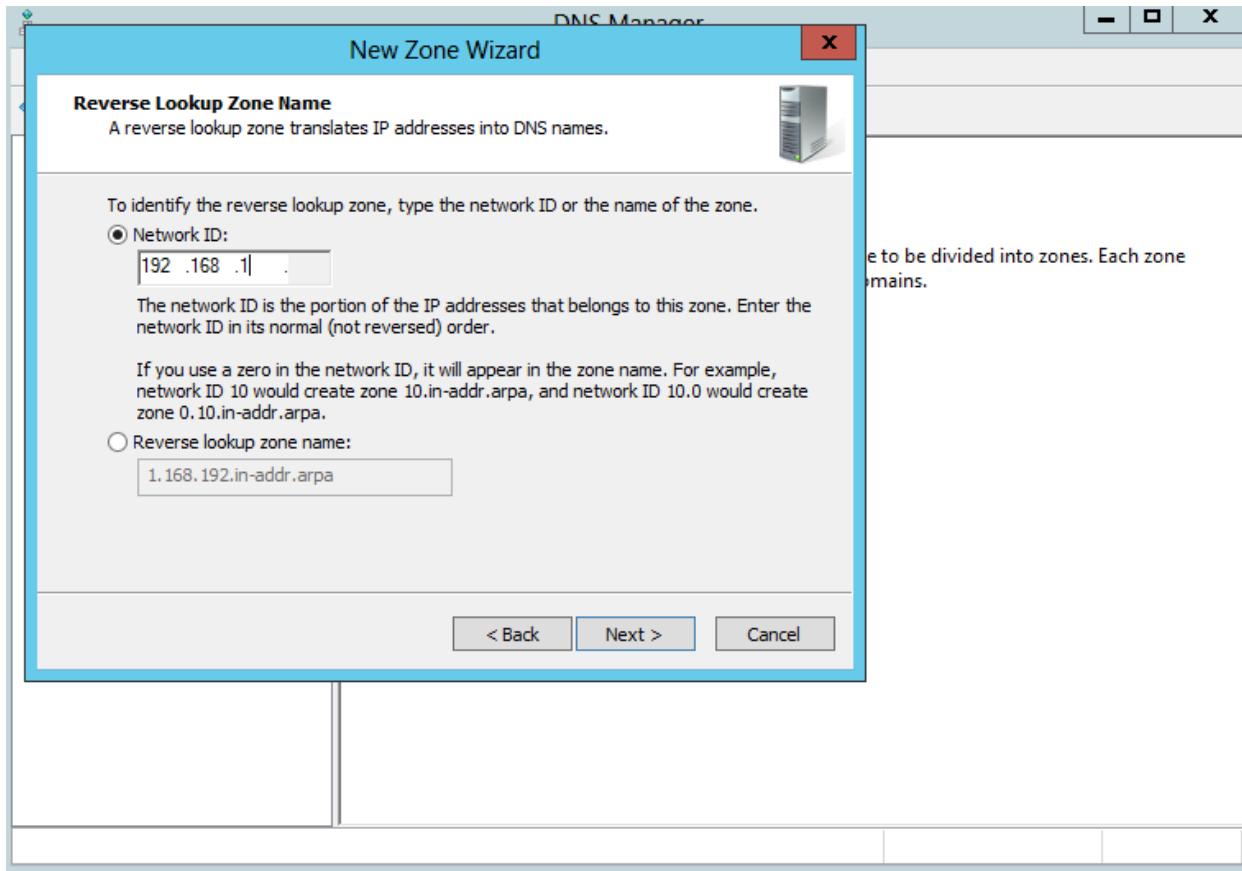
- Tại cửa sổ **Zone Type**, click chọn vào **Primary zone**



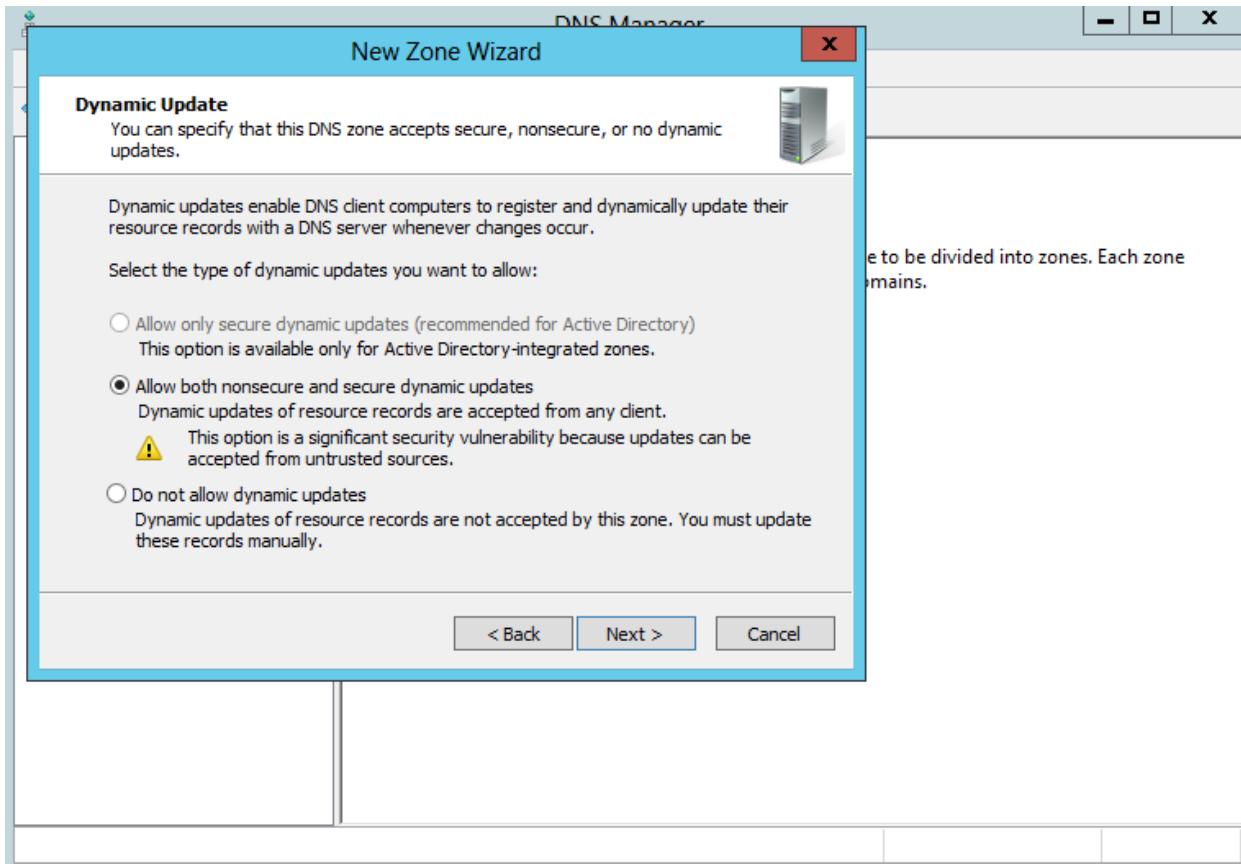
- Tại cửa sổ **Reverse Lookup Zone Name**, click chọn vào IPv4 Reverse Lookup Zone.



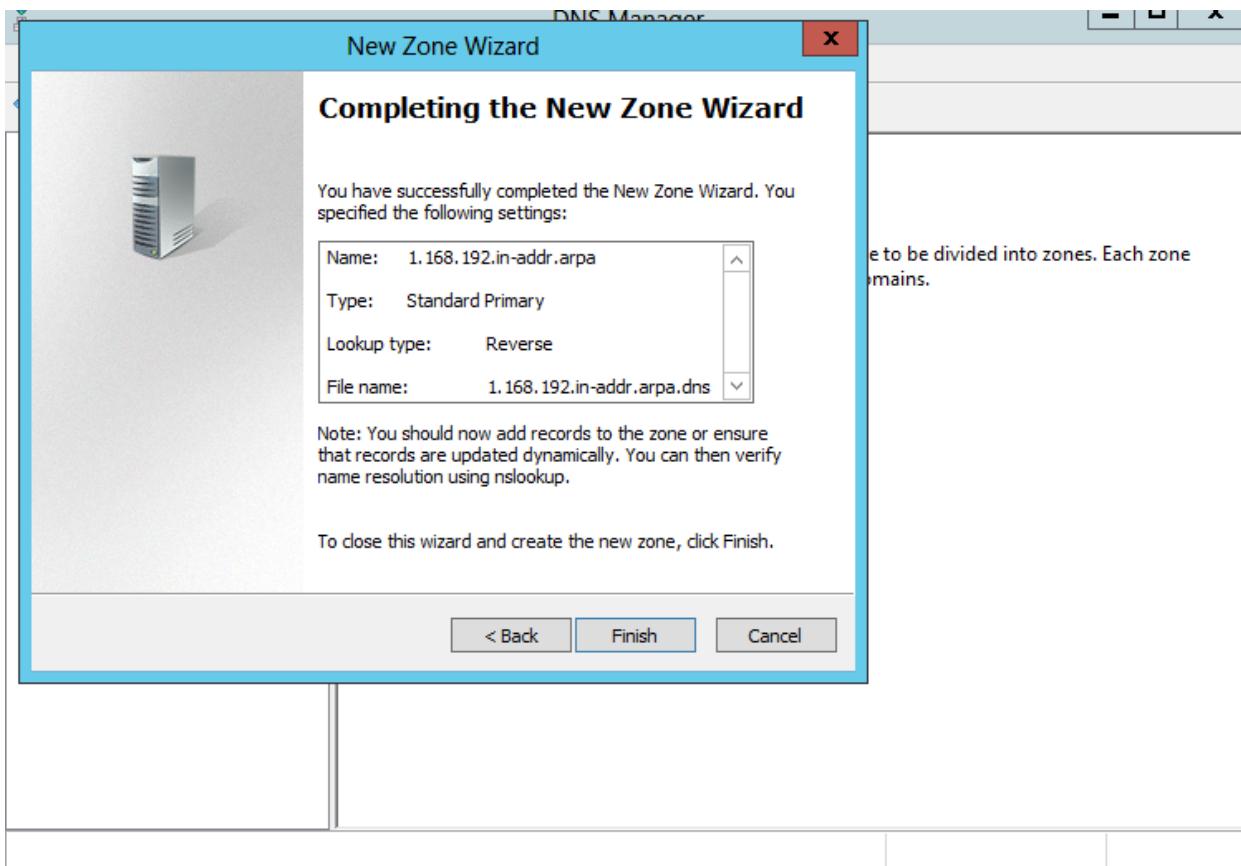
- Tại cửa sổ **Reverse Lookup Zone Name**, nhập **vào Network ID :192.168.1.**



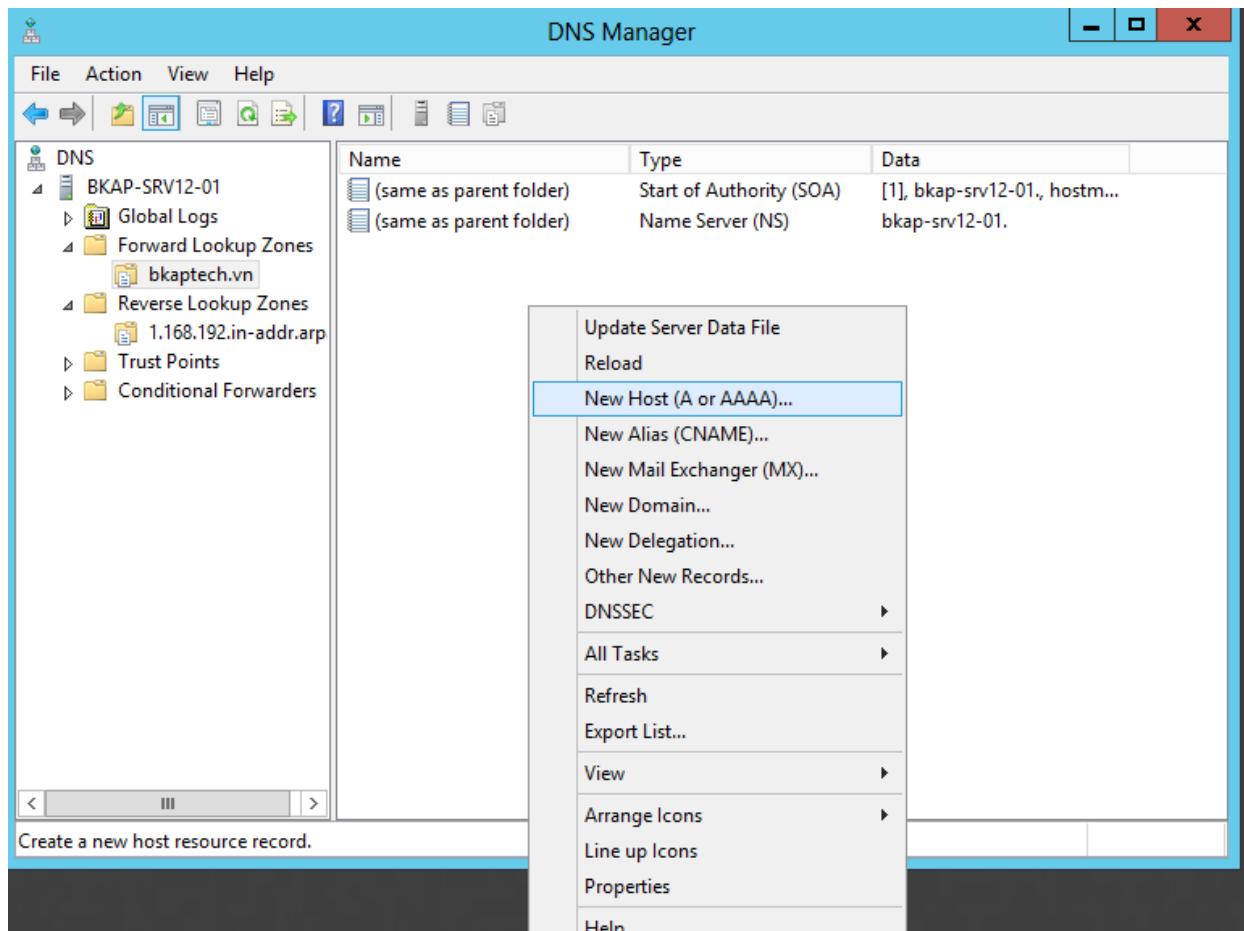
- Tại cửa sổ **Dynamic Update**, chọn vào **Allow both nonsecure and secure dynamic updates**.



- Tại cửa sổ tiếp theo, click chọn vào **Finish** để kết thúc quá trình cấu hình dịch vụ DNS.

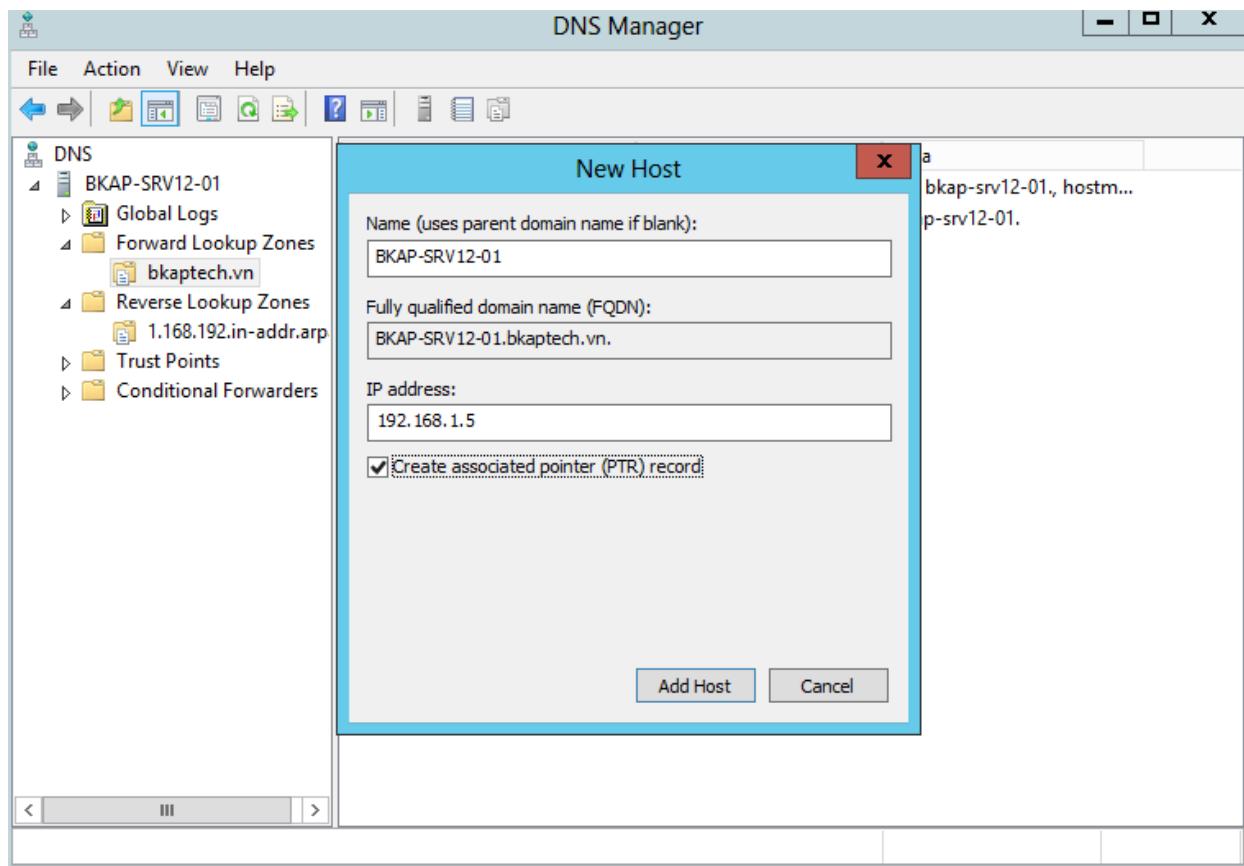


- Cấu hình tạo bản ghi cho máy *BKAP-SRV12-01*:
 - Click vào tên miền **bkaptech.vn**
 - Click chuột phải chọn **New Host (A or AAAA)**

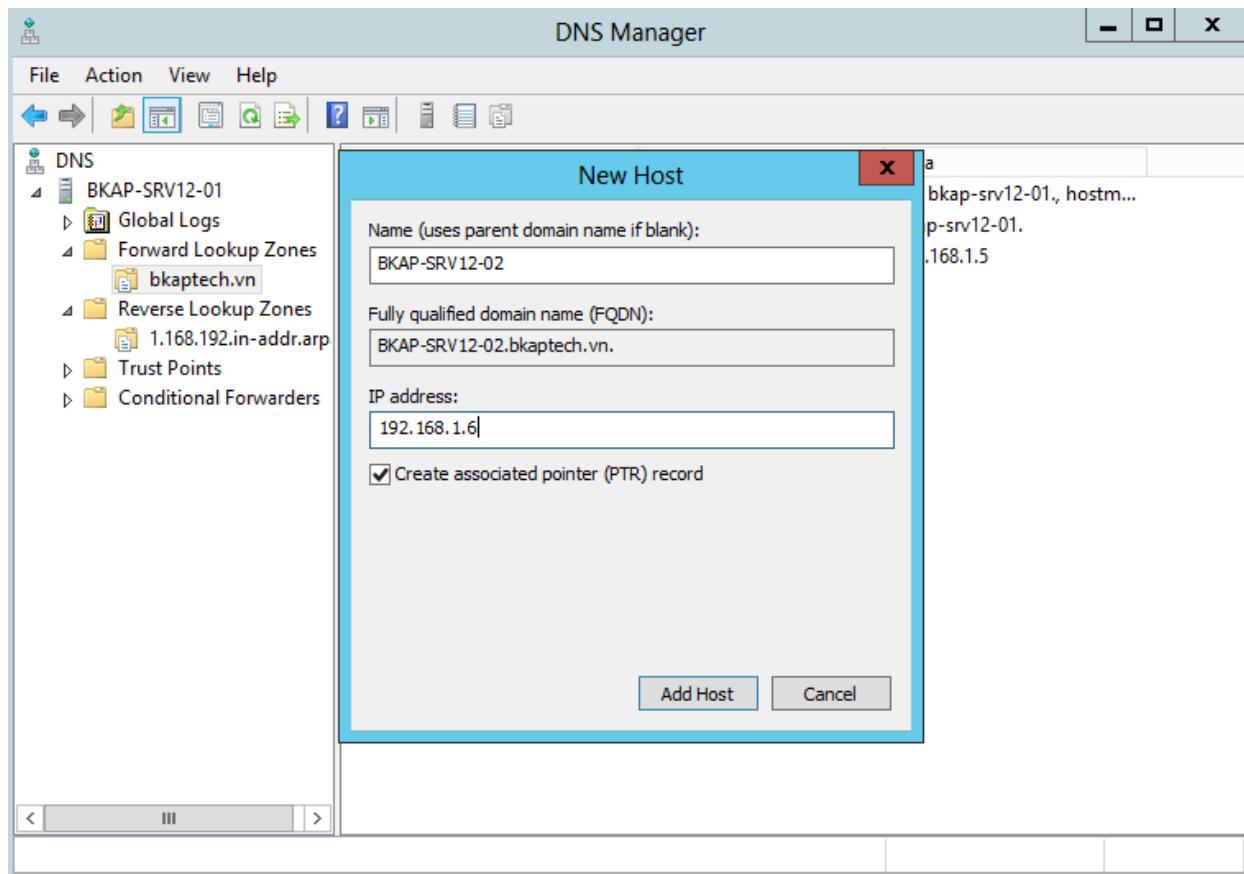


▪ Tại cửa sổ **New Host**:

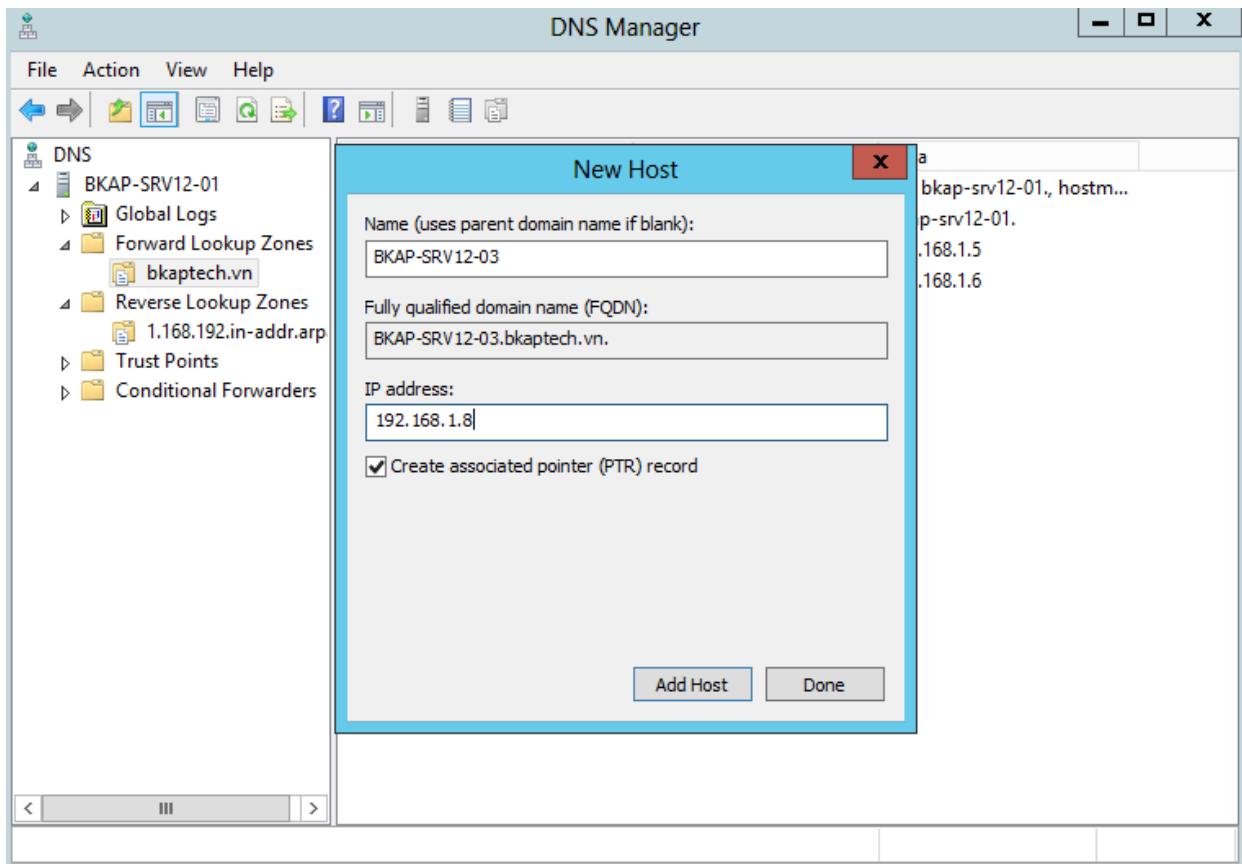
- **Name (users parent domain name if blank):** BKAP-SRV12-01
- **IP address :** 192.168.1.5
- Click tại **Create associated pointer (PTR) record.** (để máy tự động tạo bản ghi PTR)



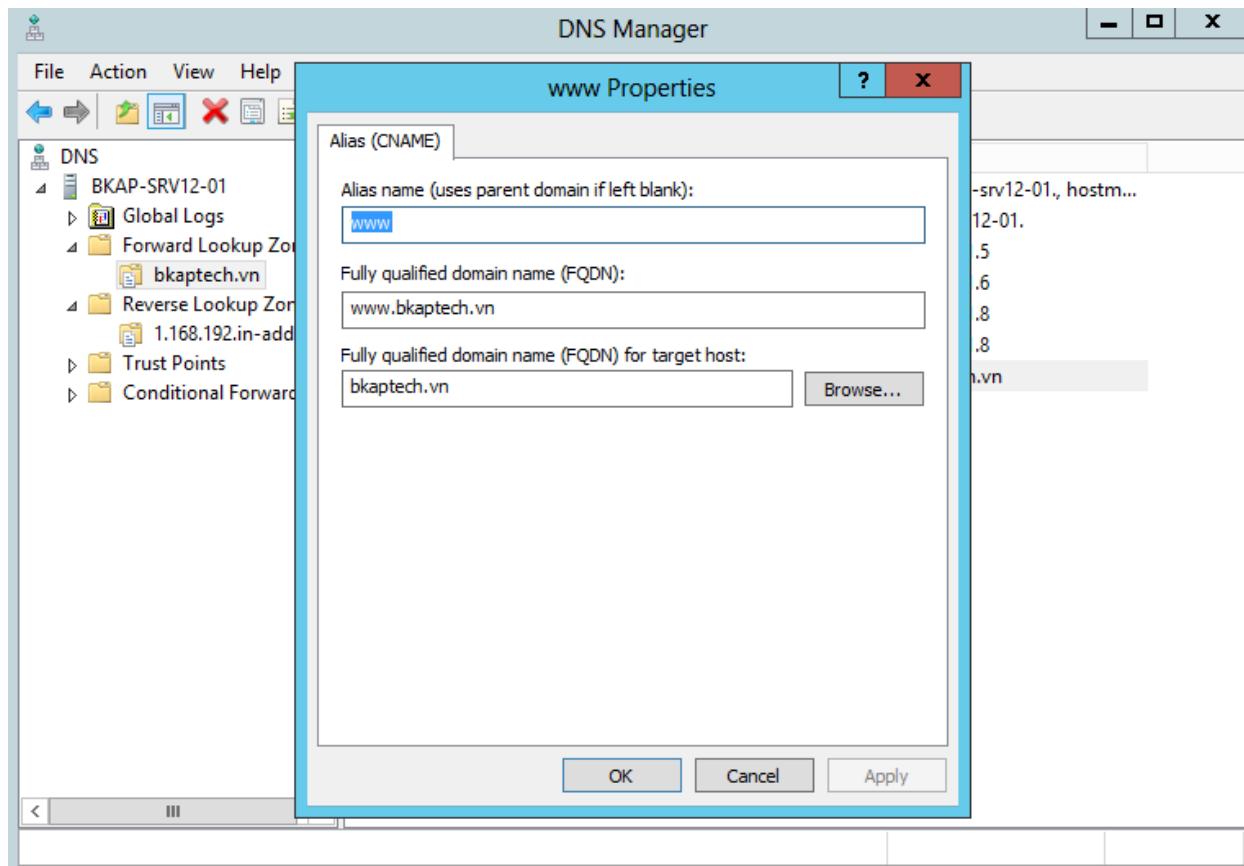
- Tạo bản ghi host A cho máy BKAP-SRV12-02:



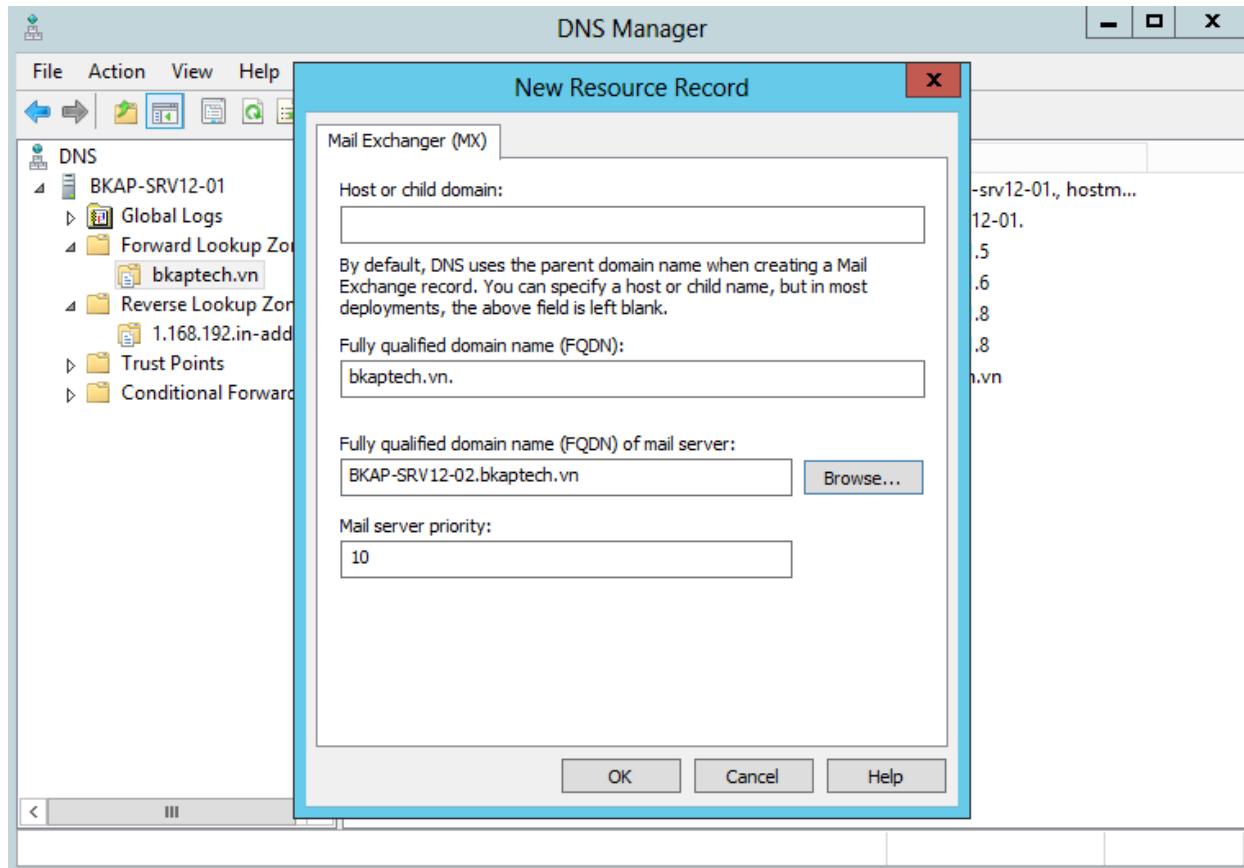
- Tạo bản ghi host A cho máy *BKAP-SRV12-03*:



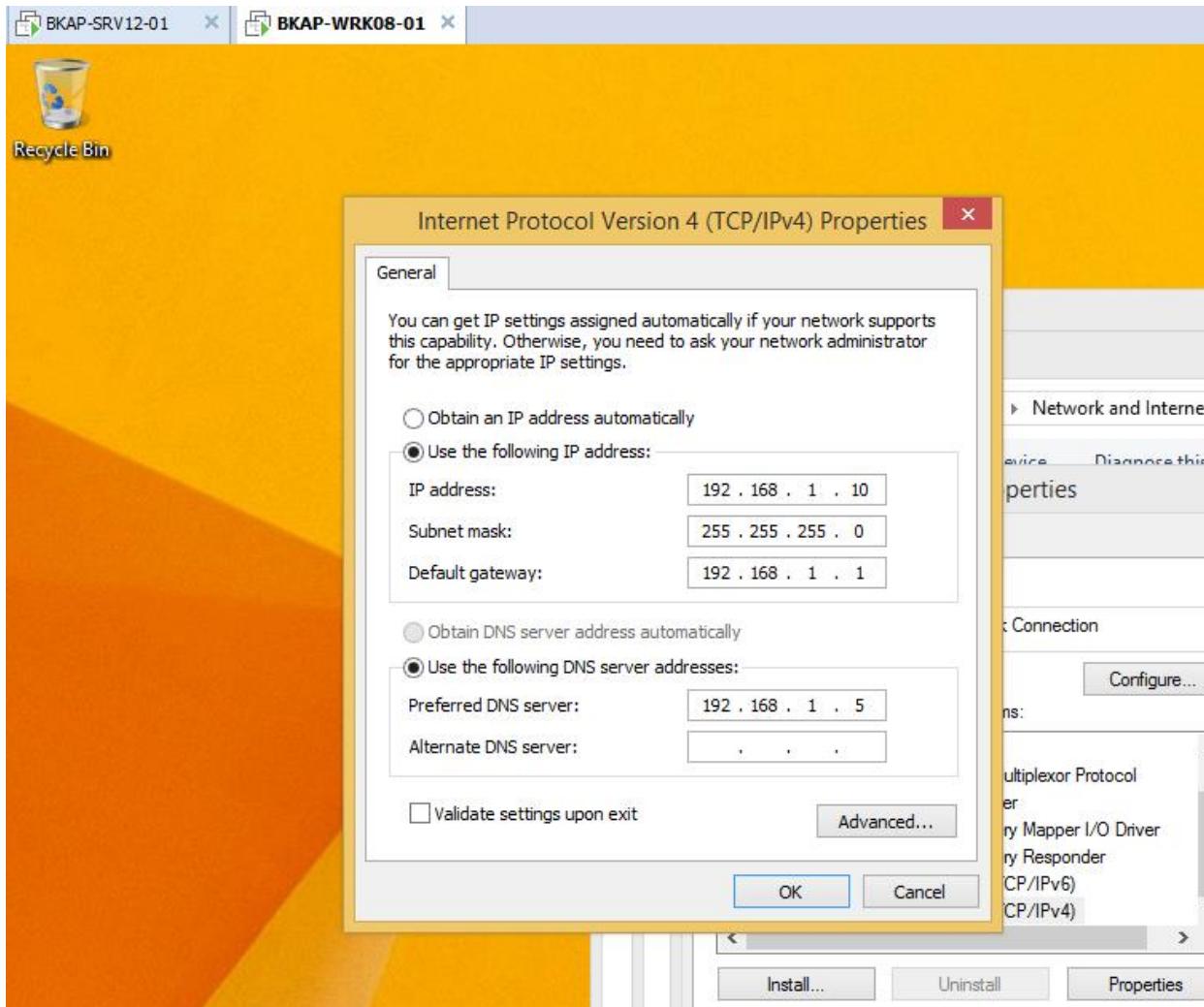
o Tạo bản ghi CNAME:



o Tạo bản ghi Mail Exchanger (MX):



- Chuyển sang máy *BKAP-WRK08-01*, kiểm tra phân giải IP sang tên miền.
 - Địa chỉ của máy *BKAP-WRK08-01*.



- Vào cmd, gõ lệnh nslookup :

```
C:\Windows\system32\cmd.exe - nslookup
C:\>nslookup
Default Server: bkap-srv12-01.bkaptech.vn
Address: 192.168.1.5

> 192.168.1.6
Server: bkap-srv12-01.bkaptech.vn
Address: 192.168.1.5

Name: bkap-srv12-02.bkaptech.vn
Address: 192.168.1.6

> 192.168.1.8
Server: bkap-srv12-01.bkaptech.vn
Address: 192.168.1.5

Name: bkap-srv12-03.bkaptech.vn
Address: 192.168.1.8

> www.bkaptech.vn
Server: bkap-srv12-01.bkaptech.vn
Address: 192.168.1.5

Name: bkaptech.vn
Address: 192.168.1.8
Aliases: www.bkaptech.vn

> -
```

7.2 Cấu hình dịch vụ Backup DNS.

1. Yêu cầu bài lab:

+ Xây dựng một hệ thống mạng có tên miền **bkaptech.vn**.

- Máy *BKAP-SRV12-01* làm Primary Zone quản lý miền **bkaptech.vn**.

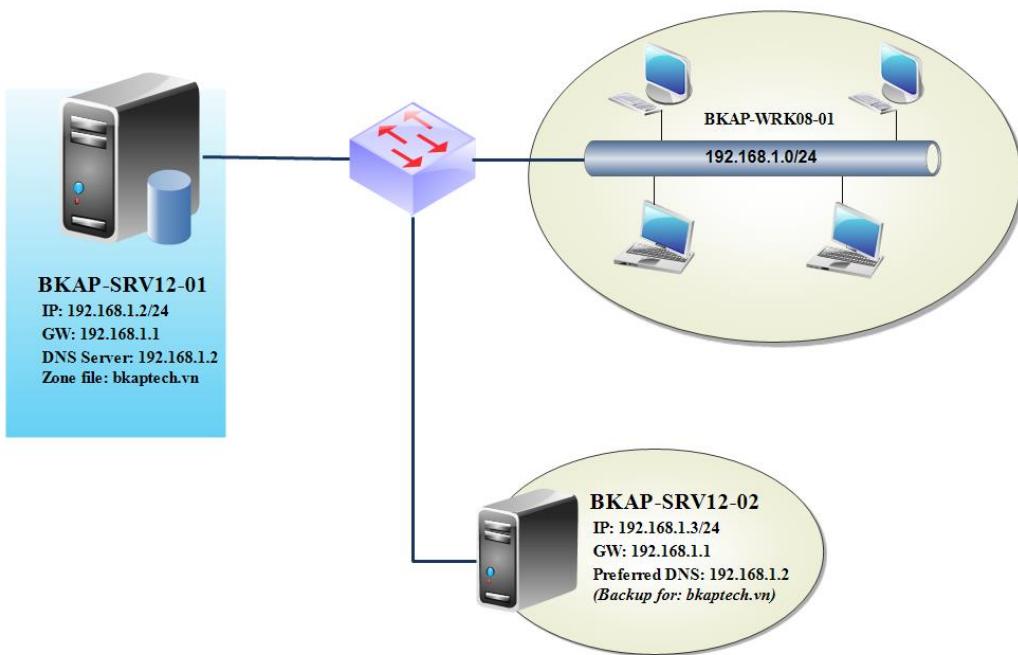
+ Xây dựng chế độ **Backup** cho miền :**bkaptech.vn** trên máy *BKAP-SRV12-02*.

2. Yêu cầu chuẩn bị:

+ Chuẩn bị 2 máy *Windows Server 2012 Datacenter* thực hiện cài đặt theo mô hình **sơ đồ lab 7.2**.

3. Mô hình Lab:

HỆ THỐNG ĐÀO TẠO CNTT QUỐC TẾ BACHKHOA-APTECH
Lab 7.2 Cấu hình backup DNS



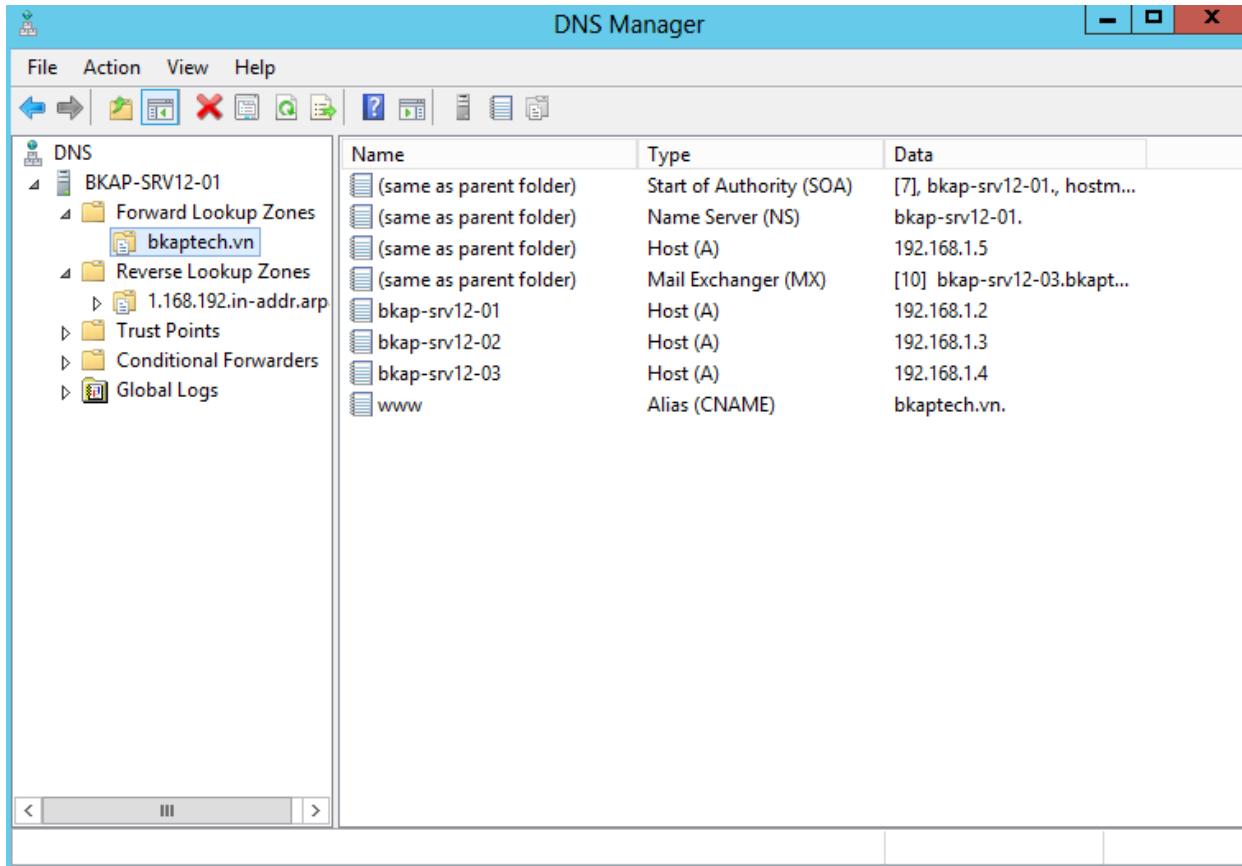
Hình 7.2

Sơ đồ địa chỉ như sau:

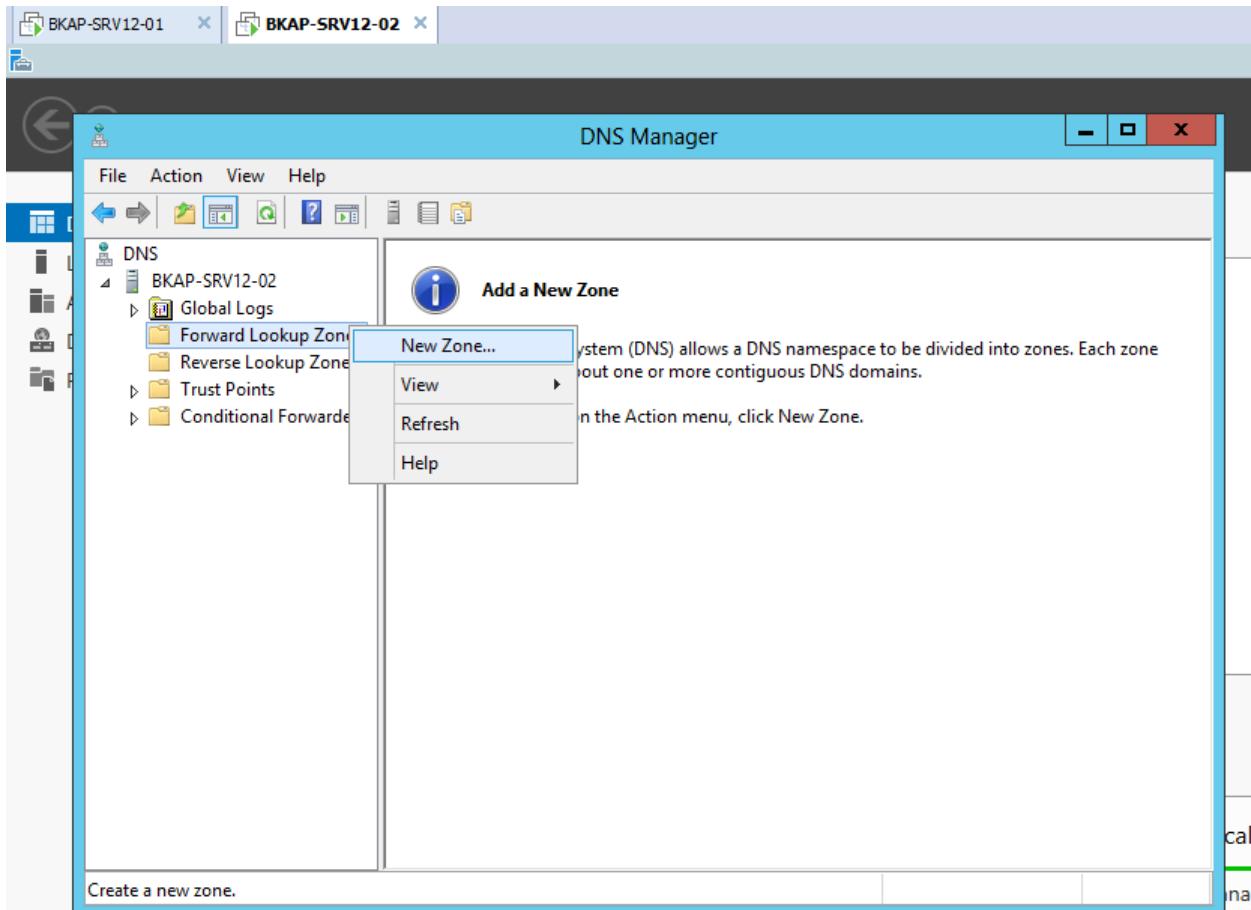
Thông số	BKAP-SRV12-01	BKAP-SRV12-02
IP address	192.168.1.2	192.168.1.3
Subnet Mask	255.255.255.0	255.255.255.0
Default gateway	192.168.1.1	192.168.1.1
Preferred DNS Server	192.168.1.2	192.168.1.2

Hướng dẫn chi tiết:

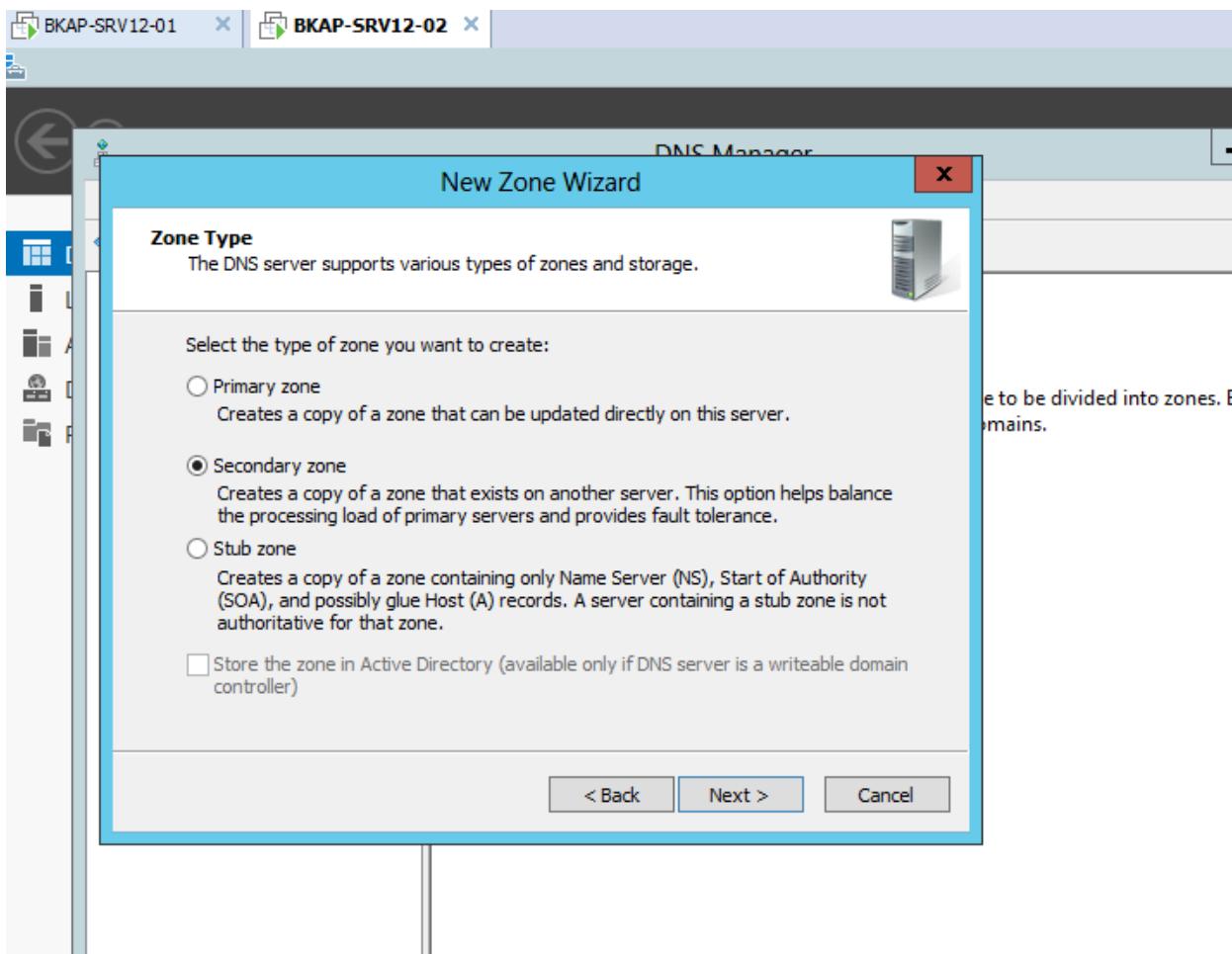
- Thực hiện trên máy *BKAP-SRV12-01*, cấu hình **DNS Server** và tạo các bản ghi (*bài lab 7.1*).



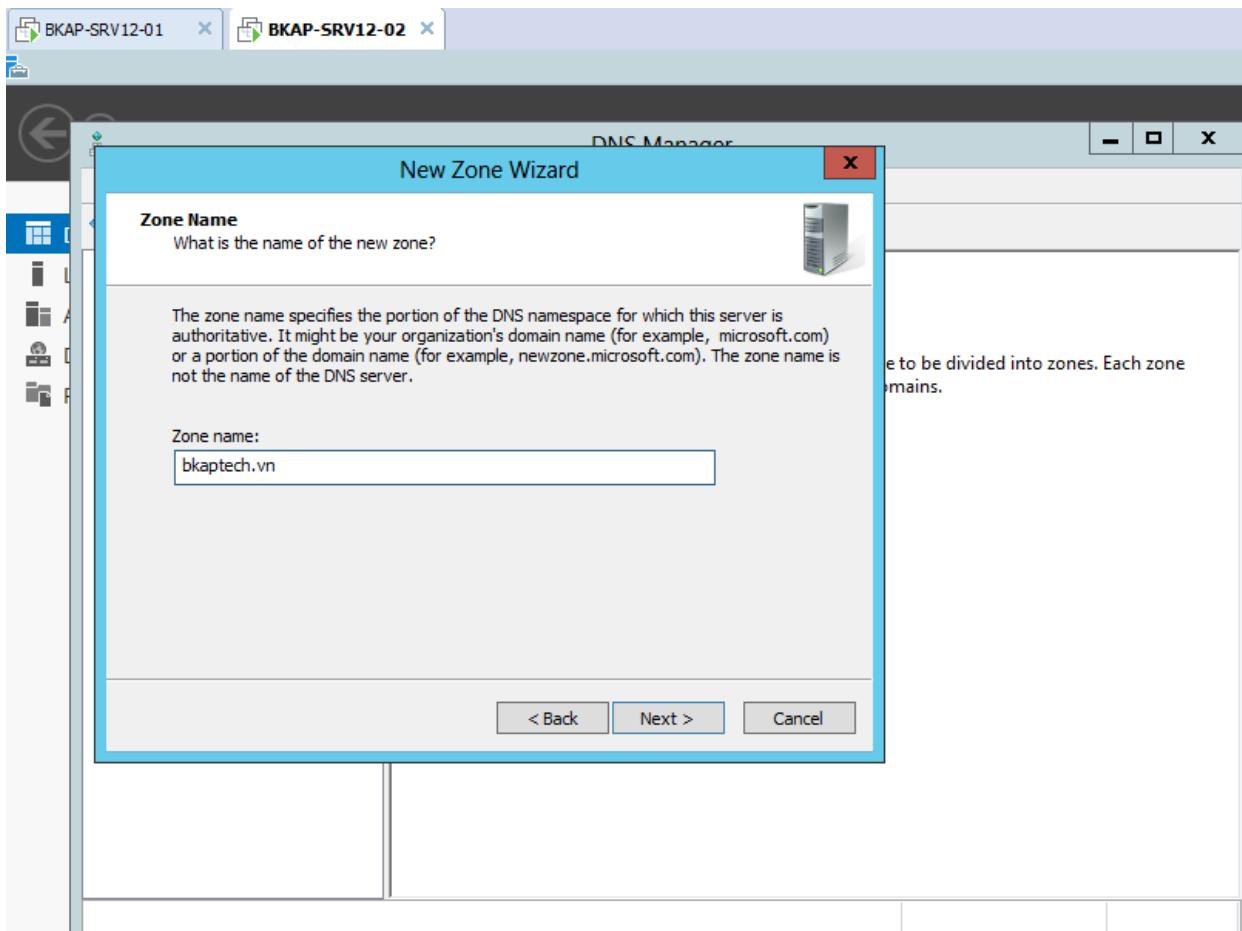
- Chuyển qua máy Server *BKAP-SRV12-02*, thực hiện cấu hình Backup DNS Server.
 - Cài đặt dịch vụ DNS trên máy *BKAP-SRV12-02*.
 - Cấu hình dịch vụ **Backup DNS** :
 - Tại **Forward Lookup Zones**, click chuột phải chọn **New Zone**.



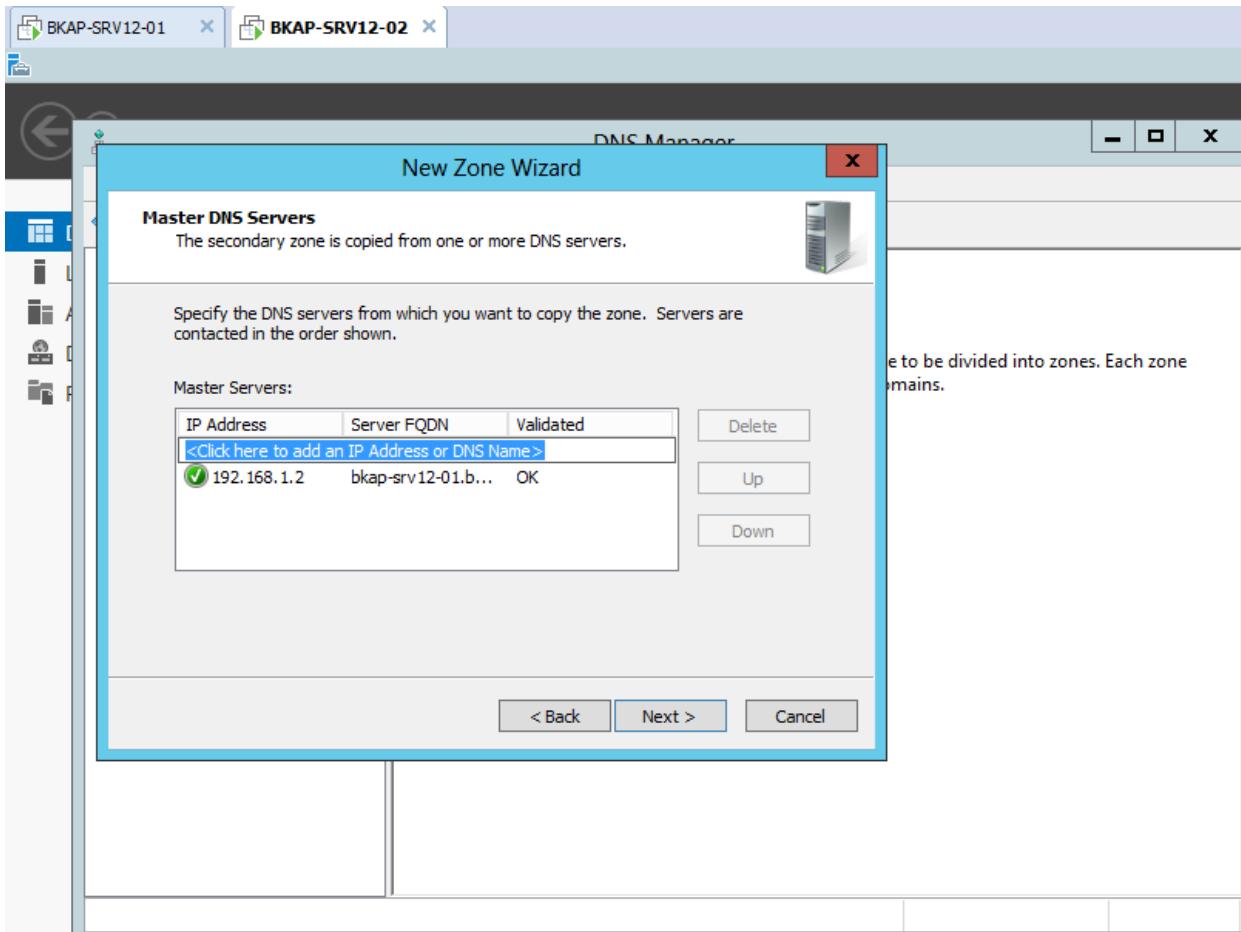
- Tại cửa sổ **Zone Type**, click chọn vào **Secondary zone**.



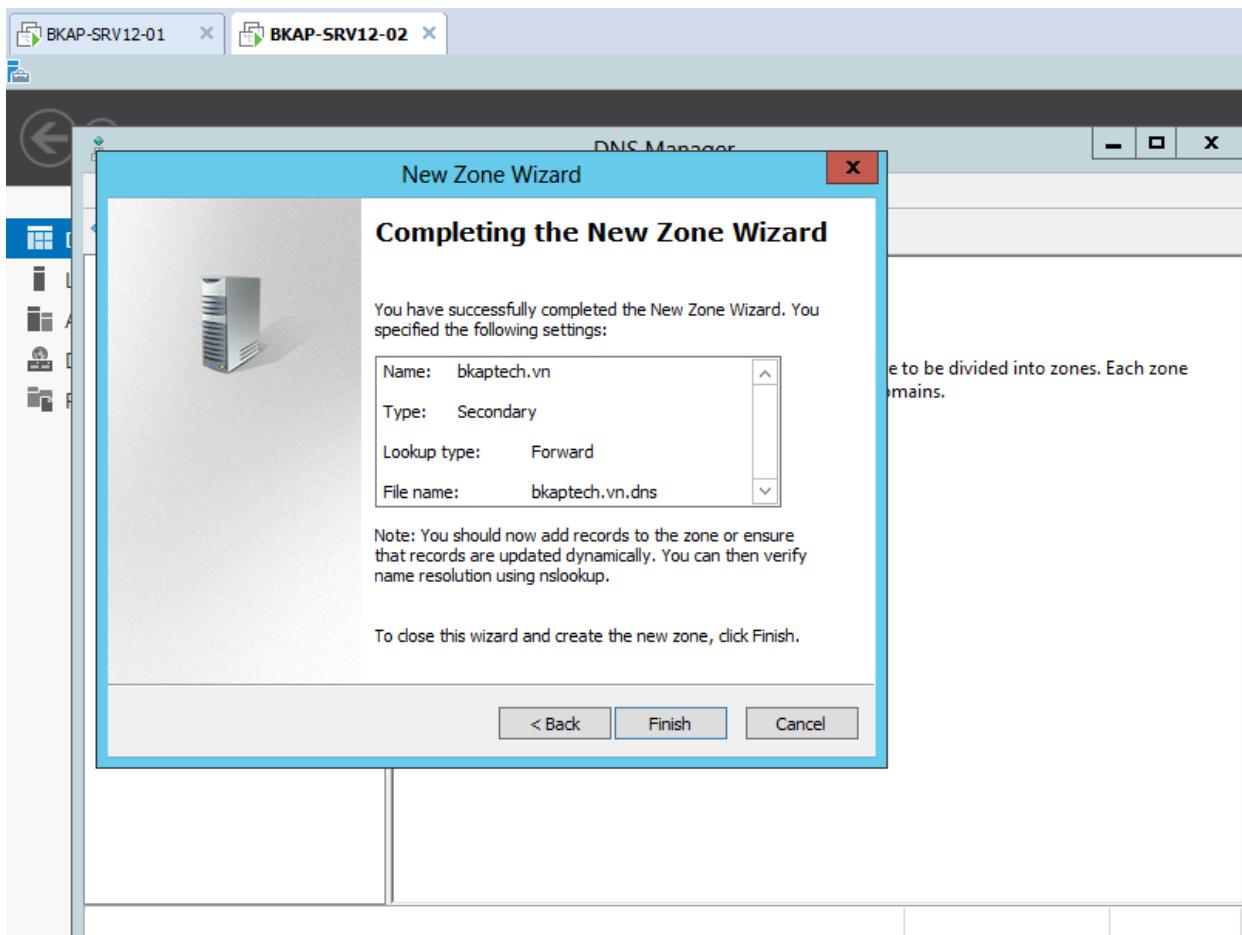
- Tại cửa sổ **Zone Name**, nhập vào tên miền **bkaptech.vn**



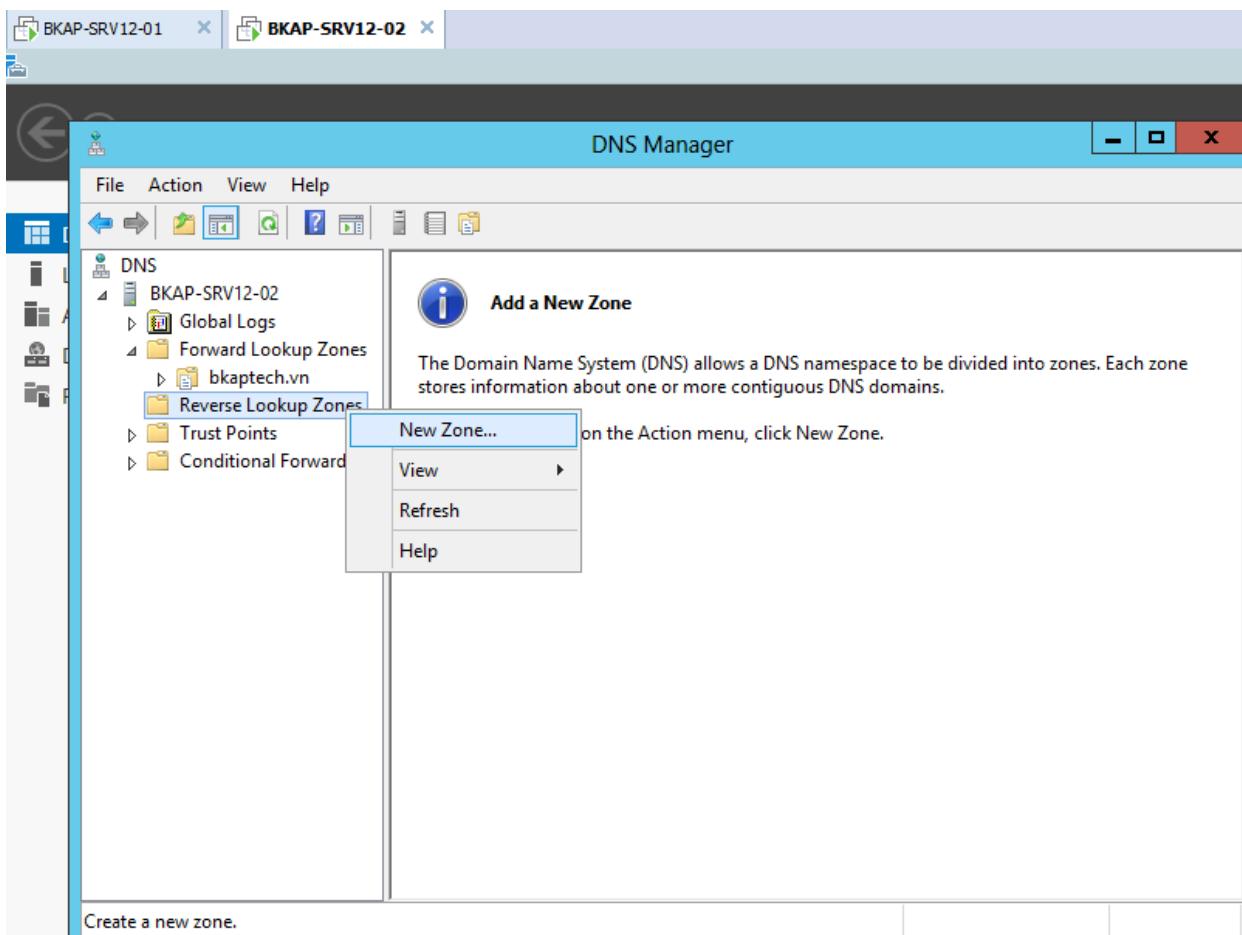
- Tại cửa sổ **Master DNS Servers**, nhập địa chỉ máy *BKAP-SRV12-01*.



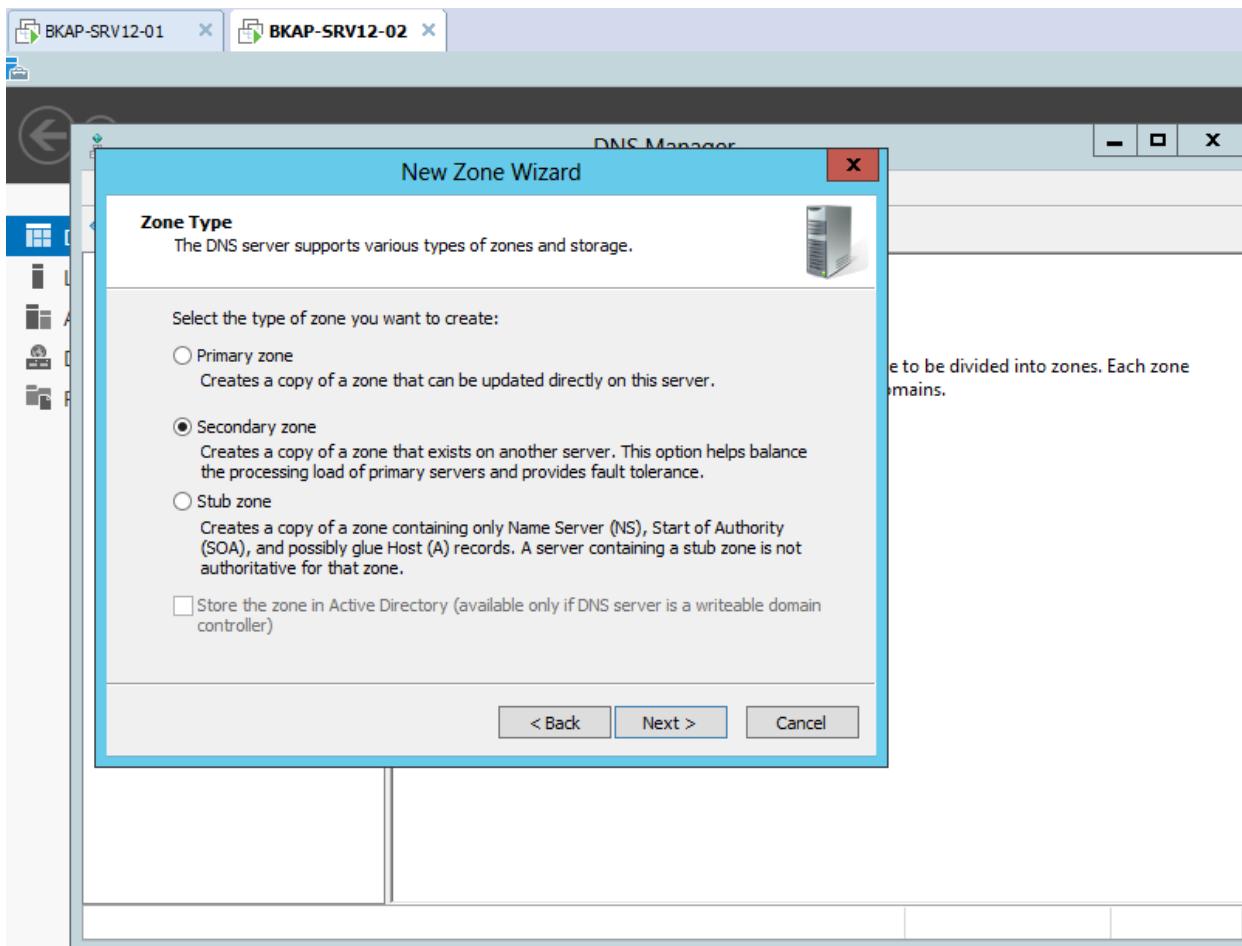
- Click vào Next và Finish ở các cửa sổ tiếp theo.



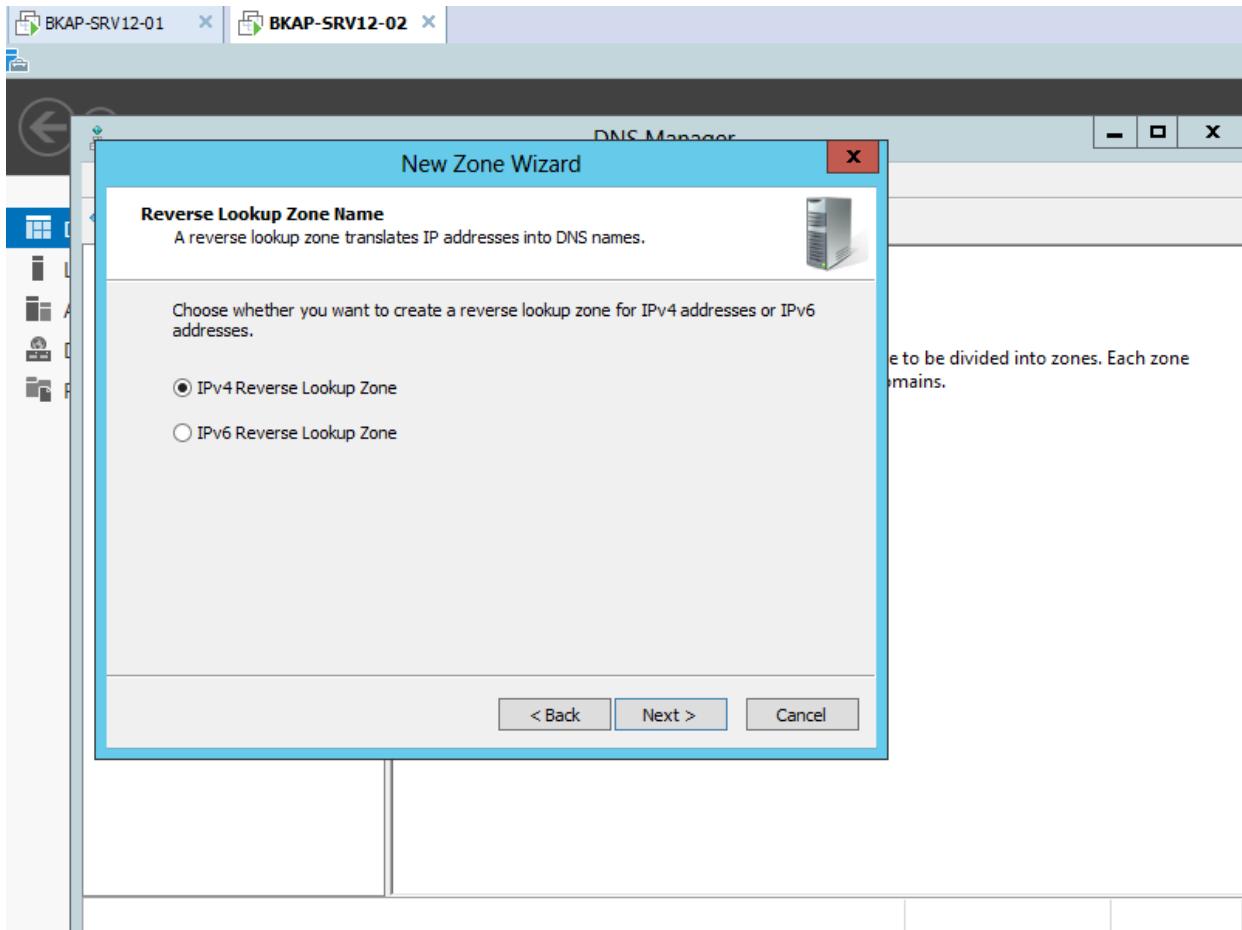
- Click chuột phải tại Reverse Lookup Zone, chọn New Zone...



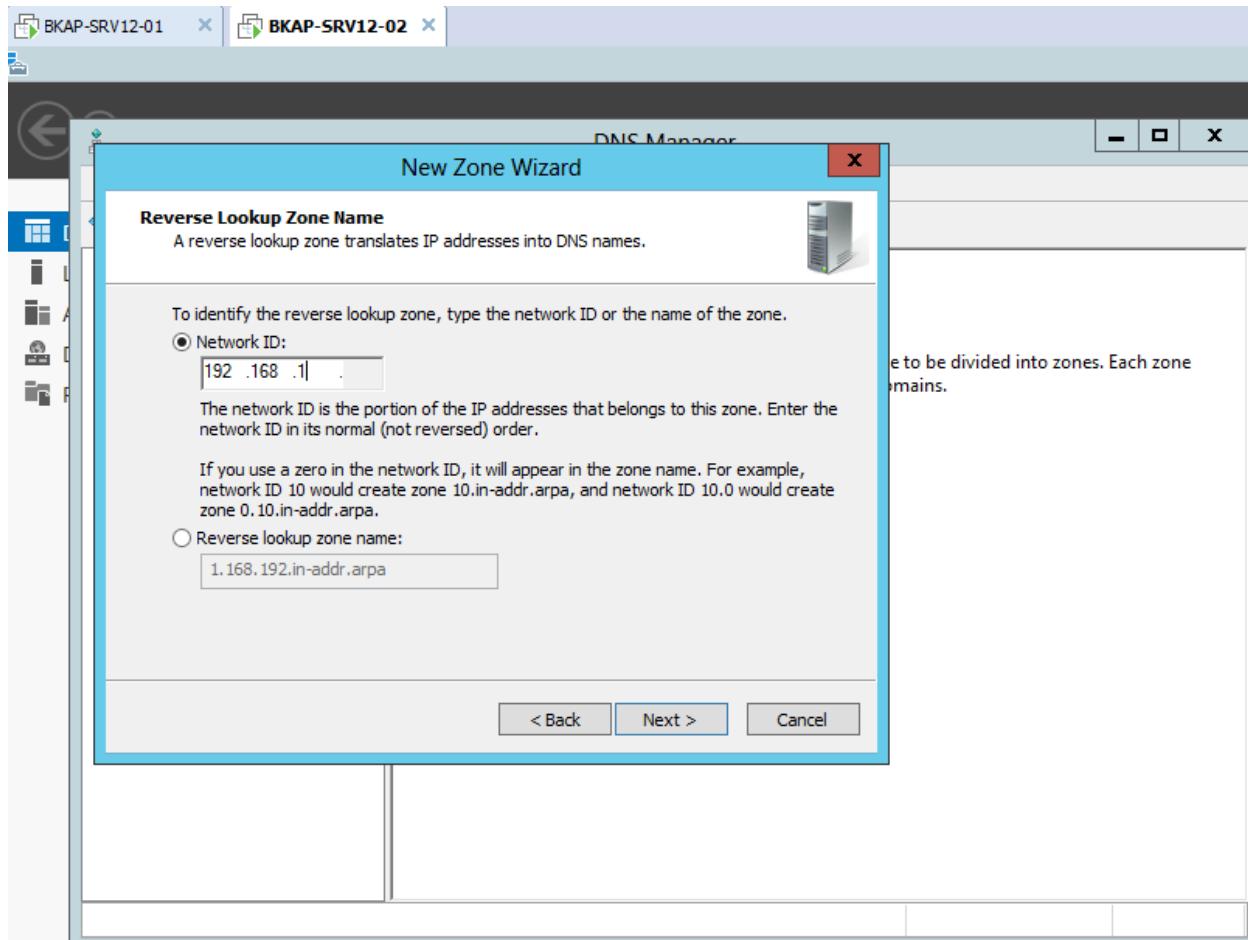
- Tại cửa sổ Zone Type, chọn vào Secondary zone.



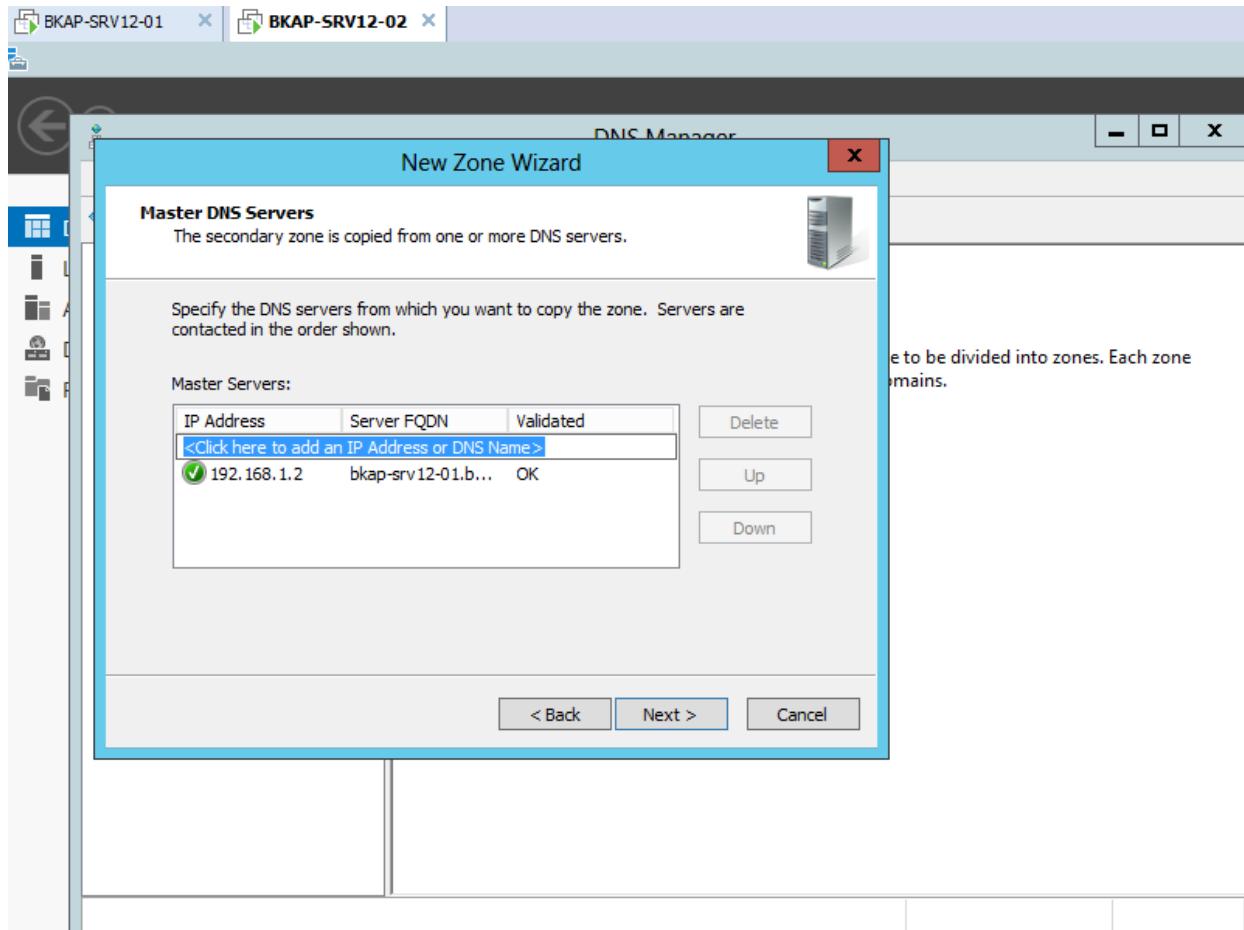
- Tại cửa sổ **Reverse Lookup Zone Name**, click chọn vào **IPv4 Reverse Lookup Zone**.



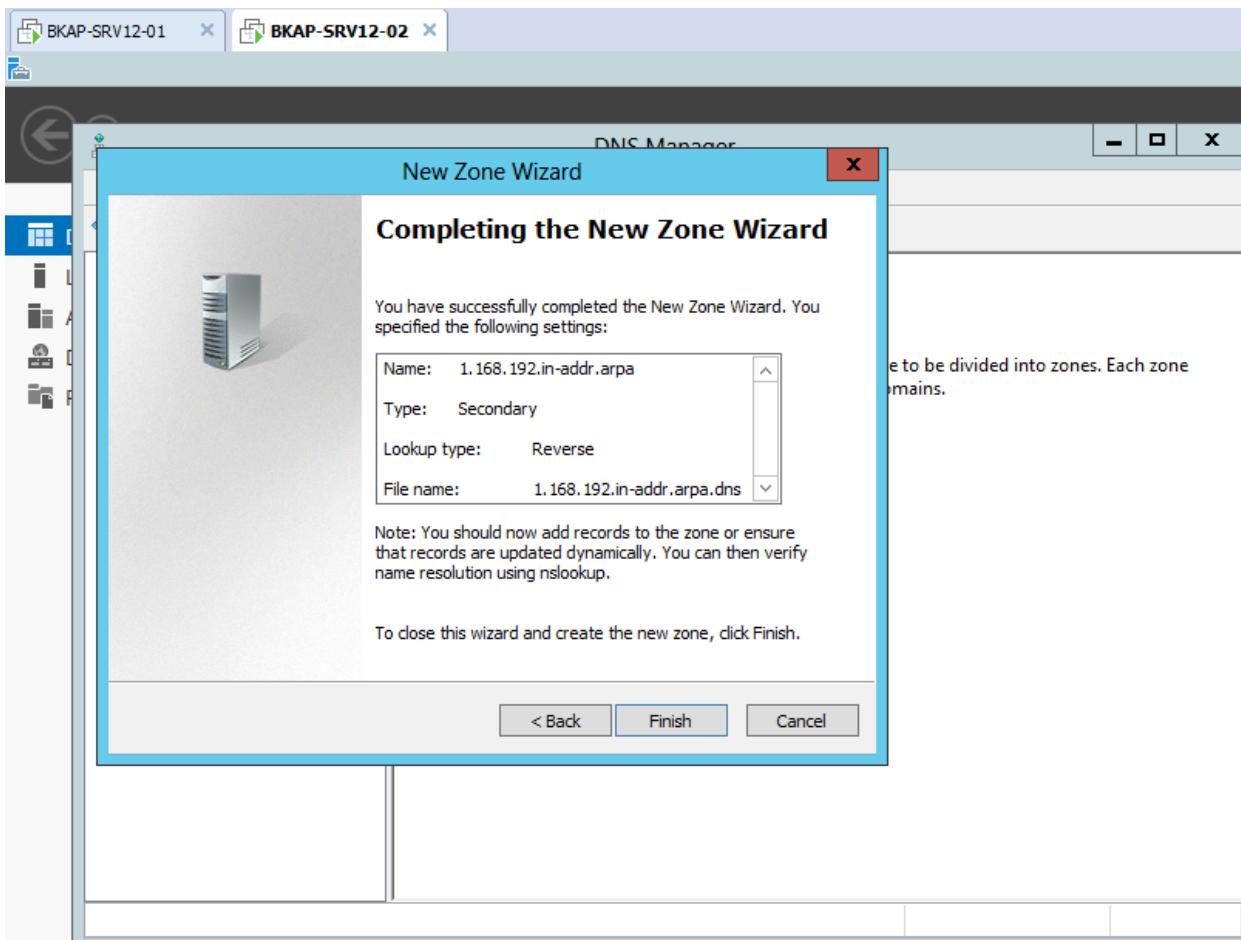
- Tại cửa sổ **Reverse Lookup Zone Name**, nhập vào **Network ID : 192.168.1**



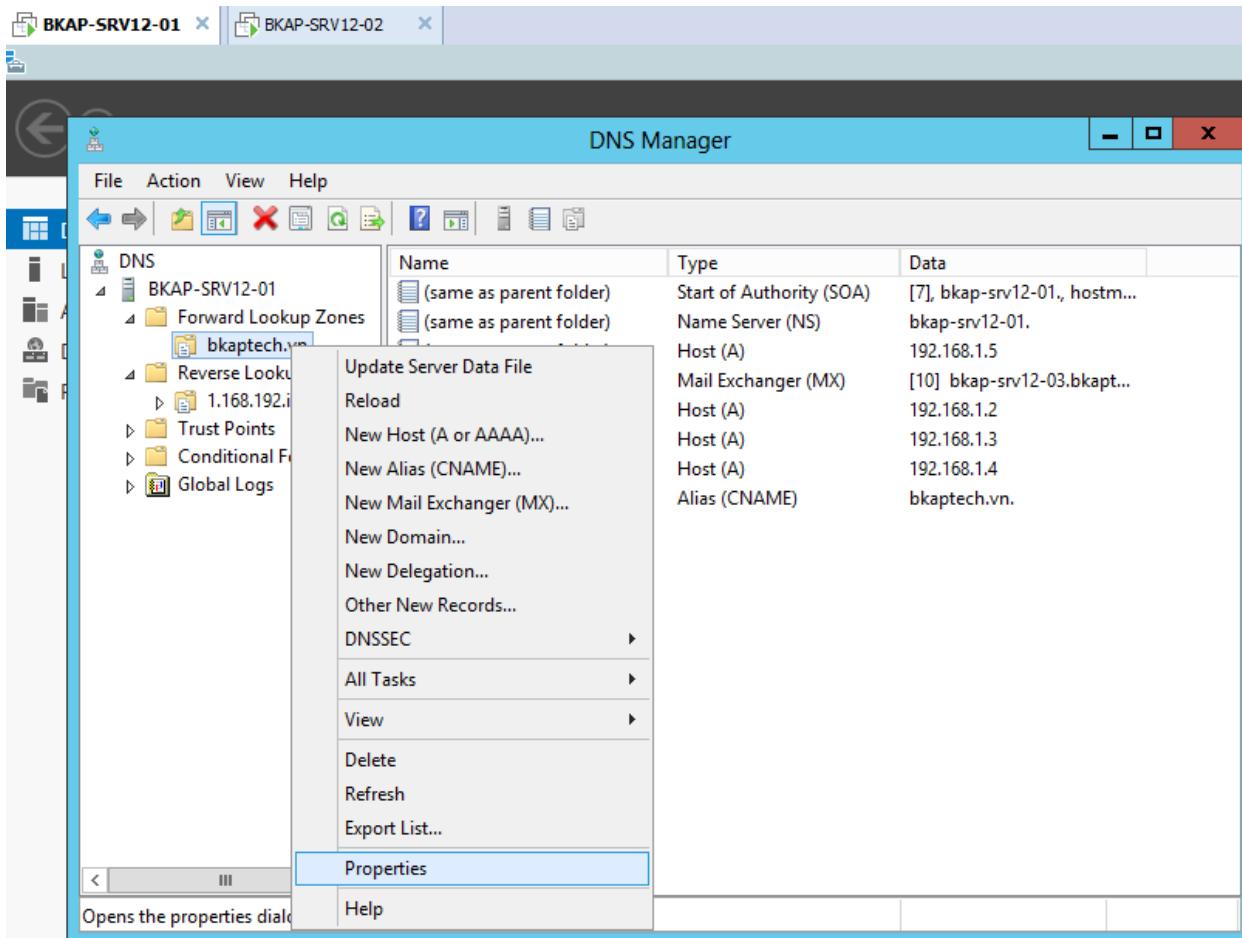
- Tại cửa sổ **Master DNS Servers**, nhập vào địa chỉ của máy **BKAP-SRV12-01 (192.168.1.2)**



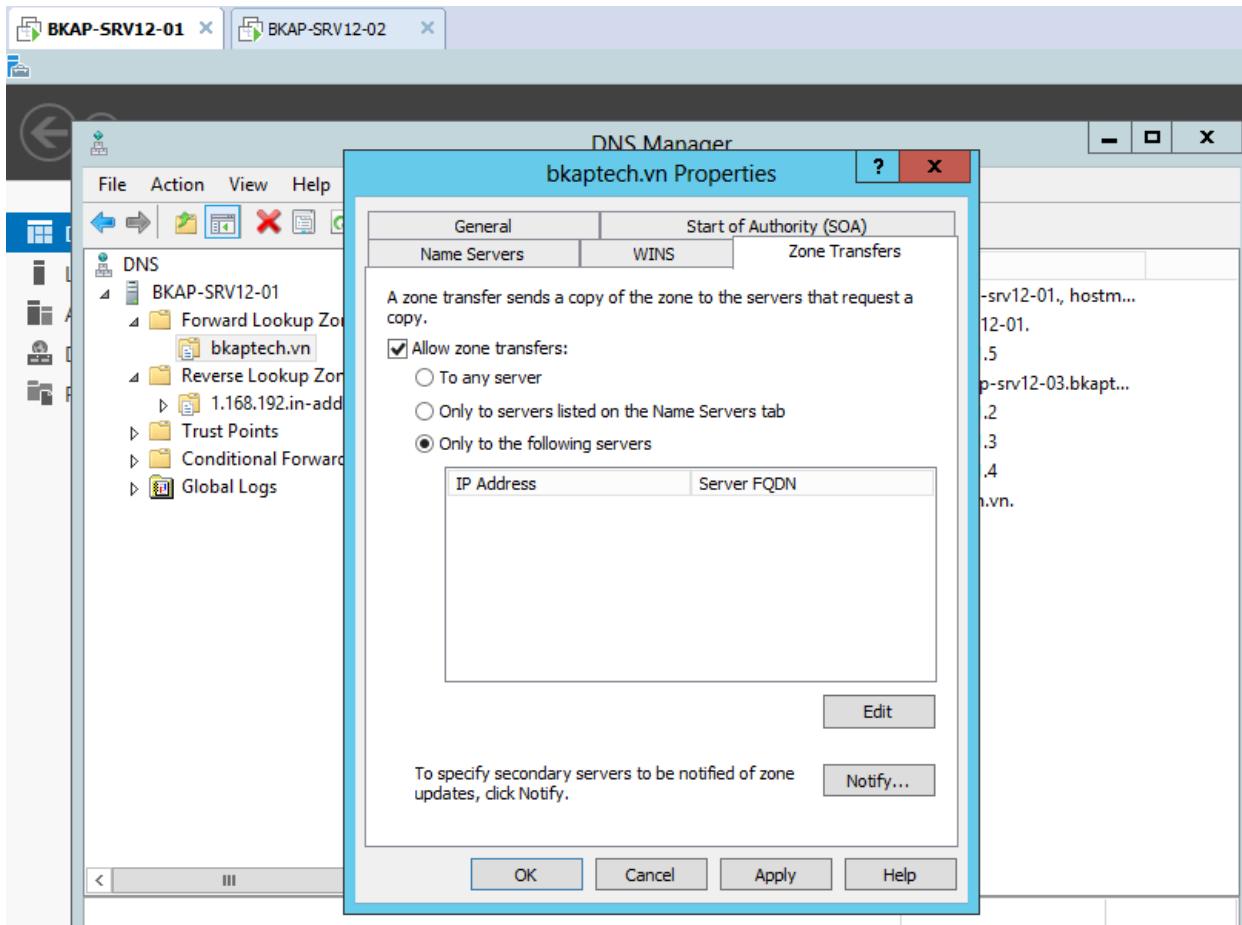
- Tại cửa sổ tiếp theo, click vào **Finish** để kết thúc quá trình cấu hình.



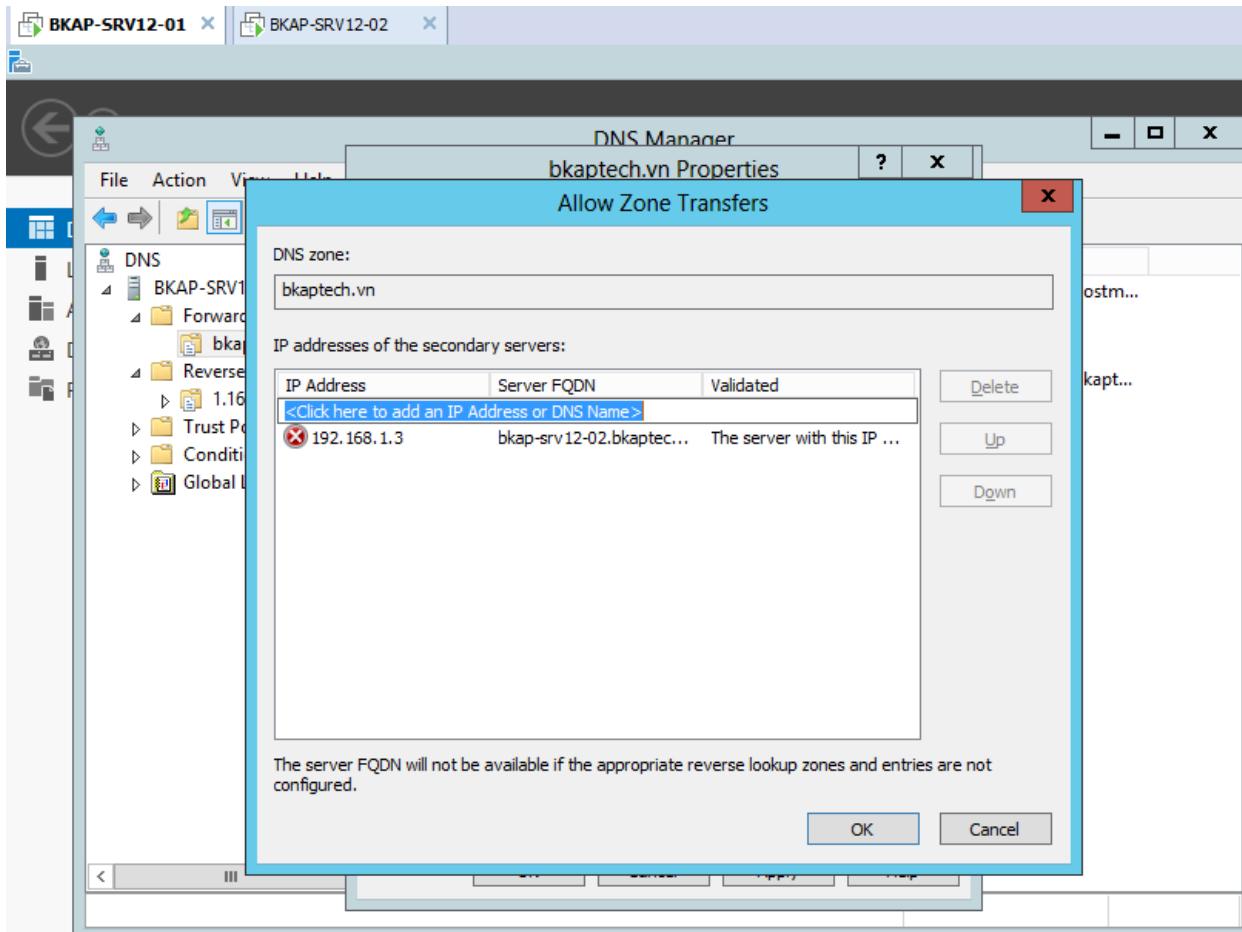
- Chuyển về Server BKAP-SRV12-01 cấu hình **backup DNS**.
 - Vào dịch vụ **DNS**, click chuột phải tại tên miền **bkaptech.vn / Properties**.



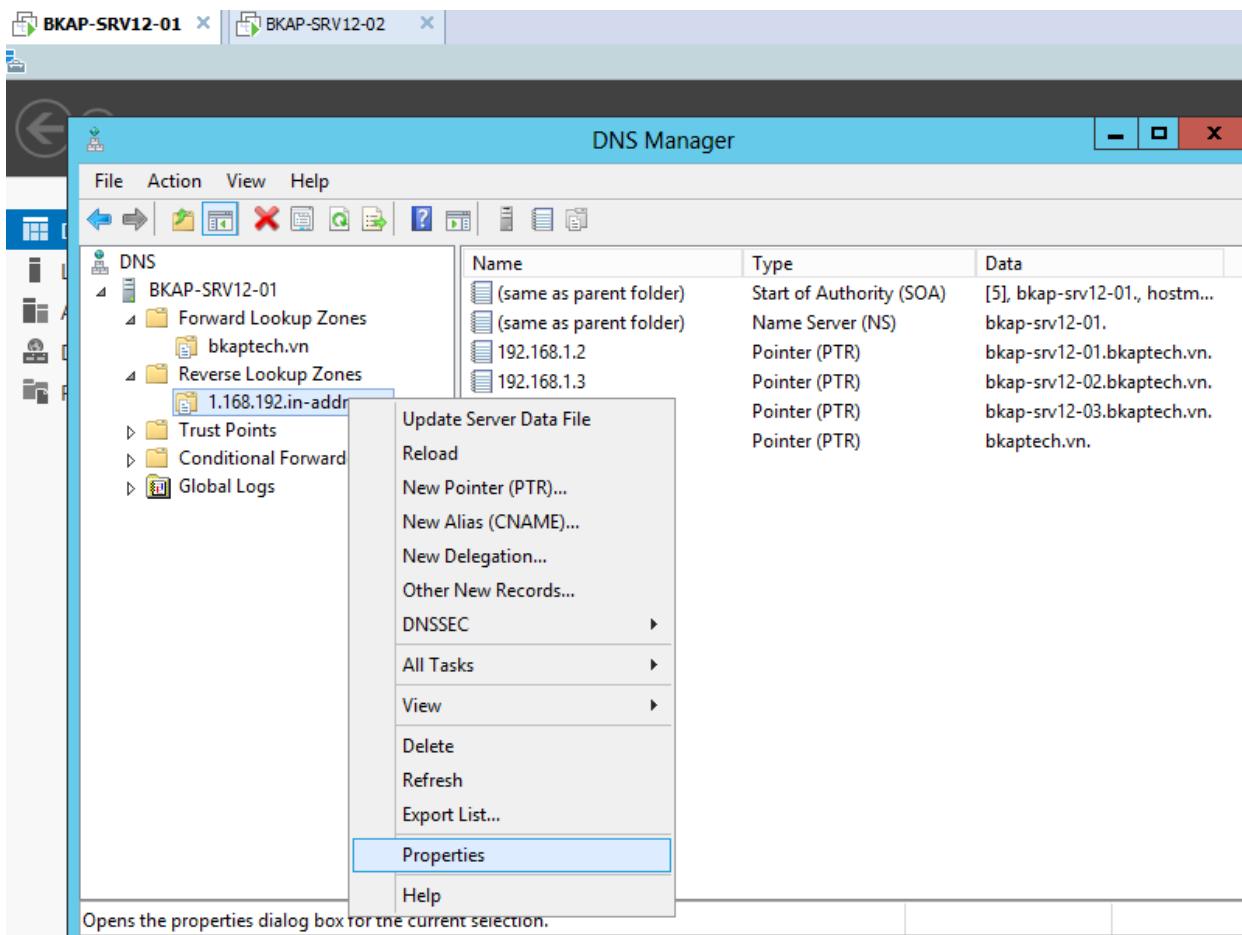
- Tại cửa sổ **bkaptech.vn Properties**, chuyển sang Tab **Zone Transfers**, click chọn vào **Allow zone transfers / Only to the following servers.**



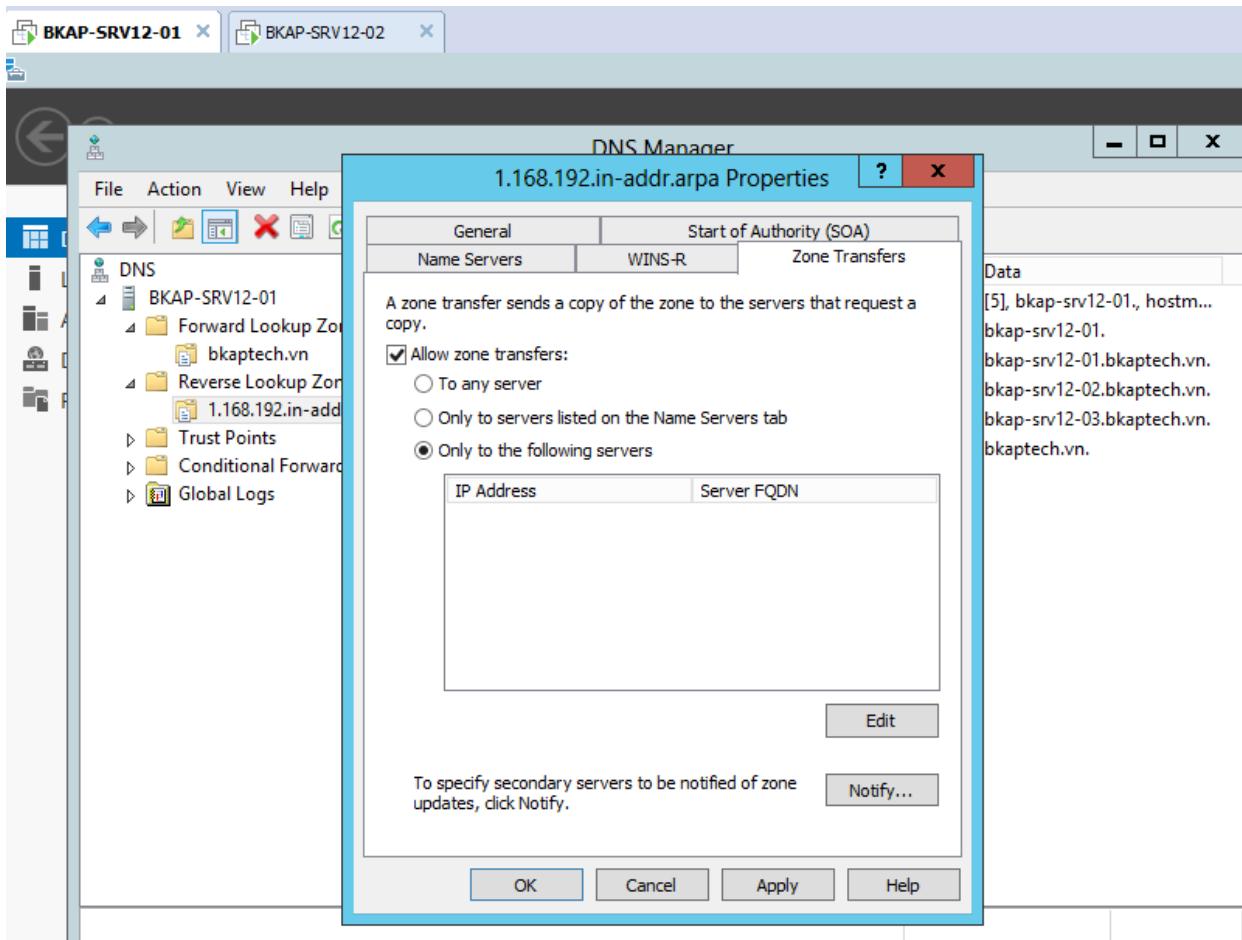
- Tại đây, tiếp tục chọn vào **Edit**. Tại cửa sổ **Allow Zone Transfers**, điền địa chỉ máy **BKAP-SRV12-02 (192.168.1.3)** tại **IP addresses of the secondary servers**
- **Apply / OK.**



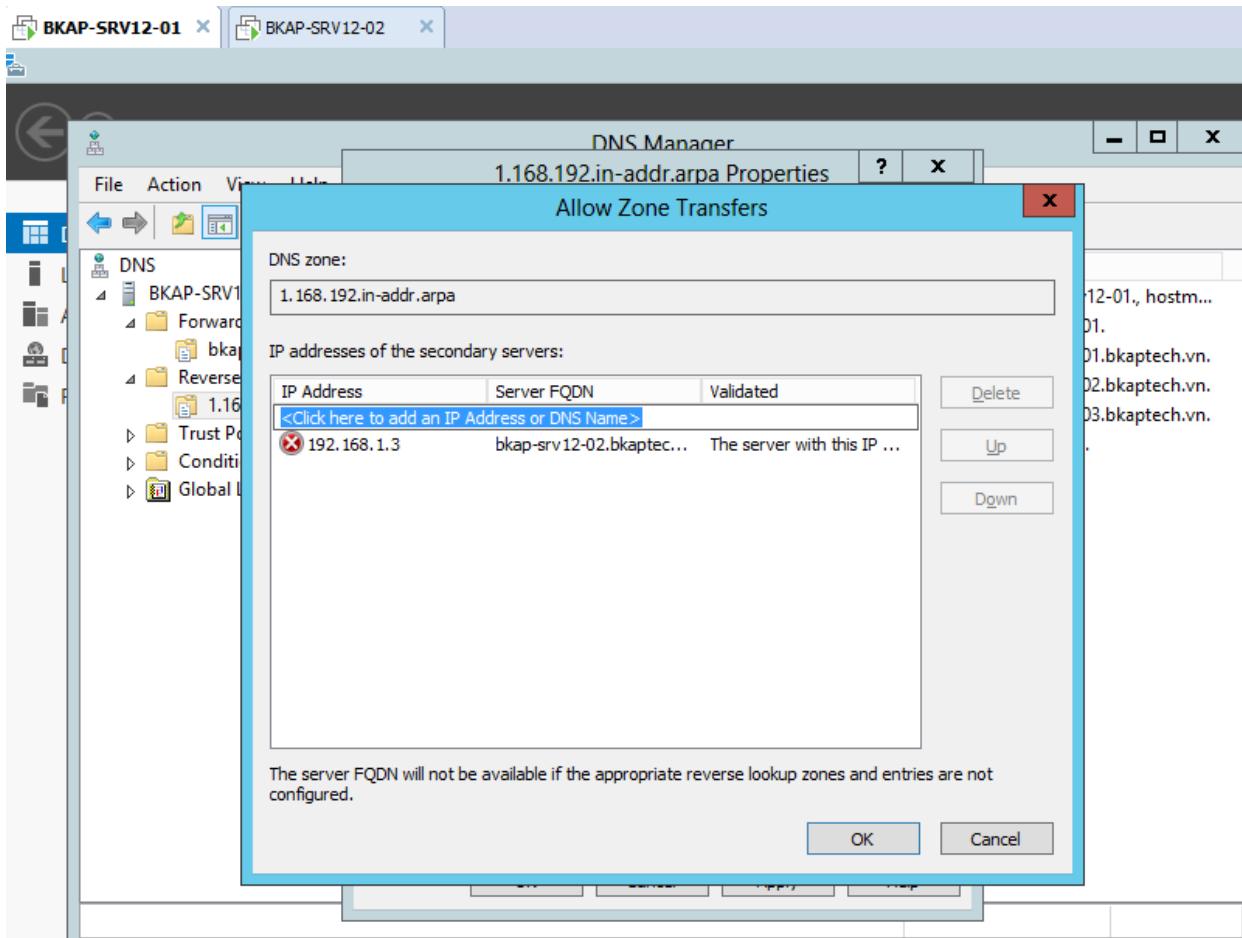
- Click chuột phải tại 1.168.192.in-addr.arpa / Properties.



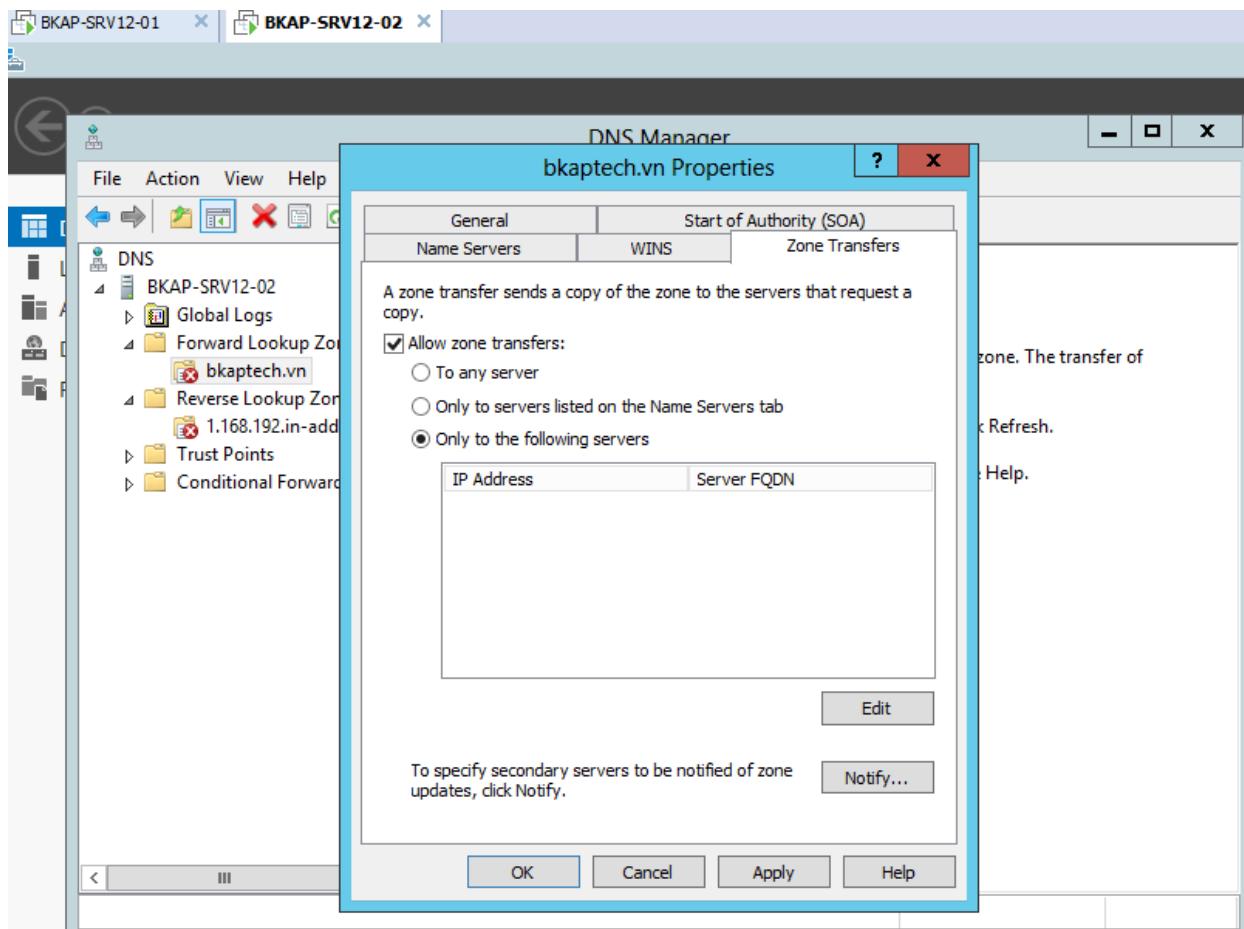
- Tại cửa sổ **1.168.192.in-addr-arpa Properties**, chuyển sang Tab **Zone Transfers**, click chọn vào **Allow zone transfers / Only to the following servers.**



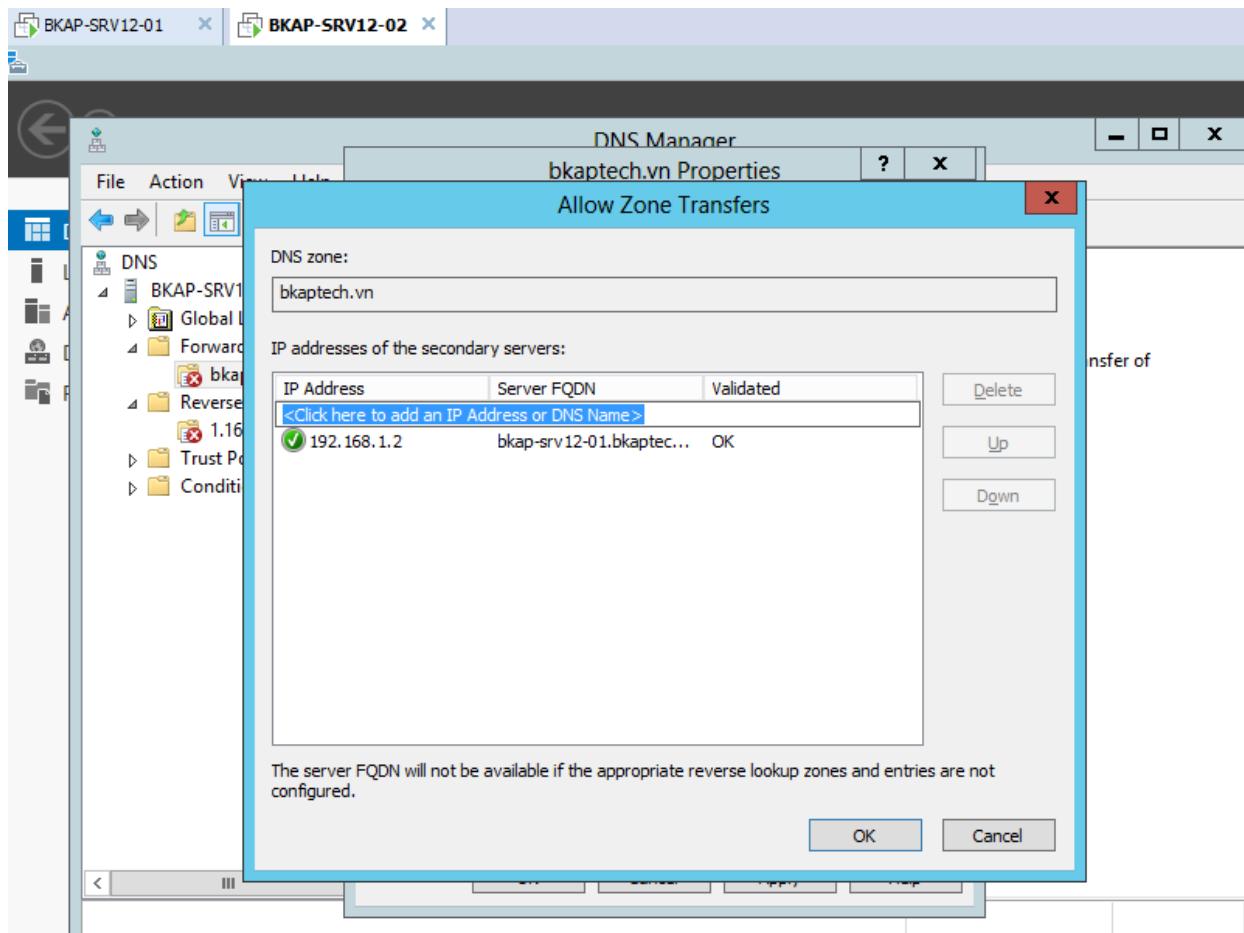
- Tại đây , tiếp tục chọn vào **Edit** , Tại cửa sổ **Allow Zone Transfers** , điền vào địa chỉ của máy *BKAP-SRV12-02 (192.168.1.3)*
- **Apply / OK.**



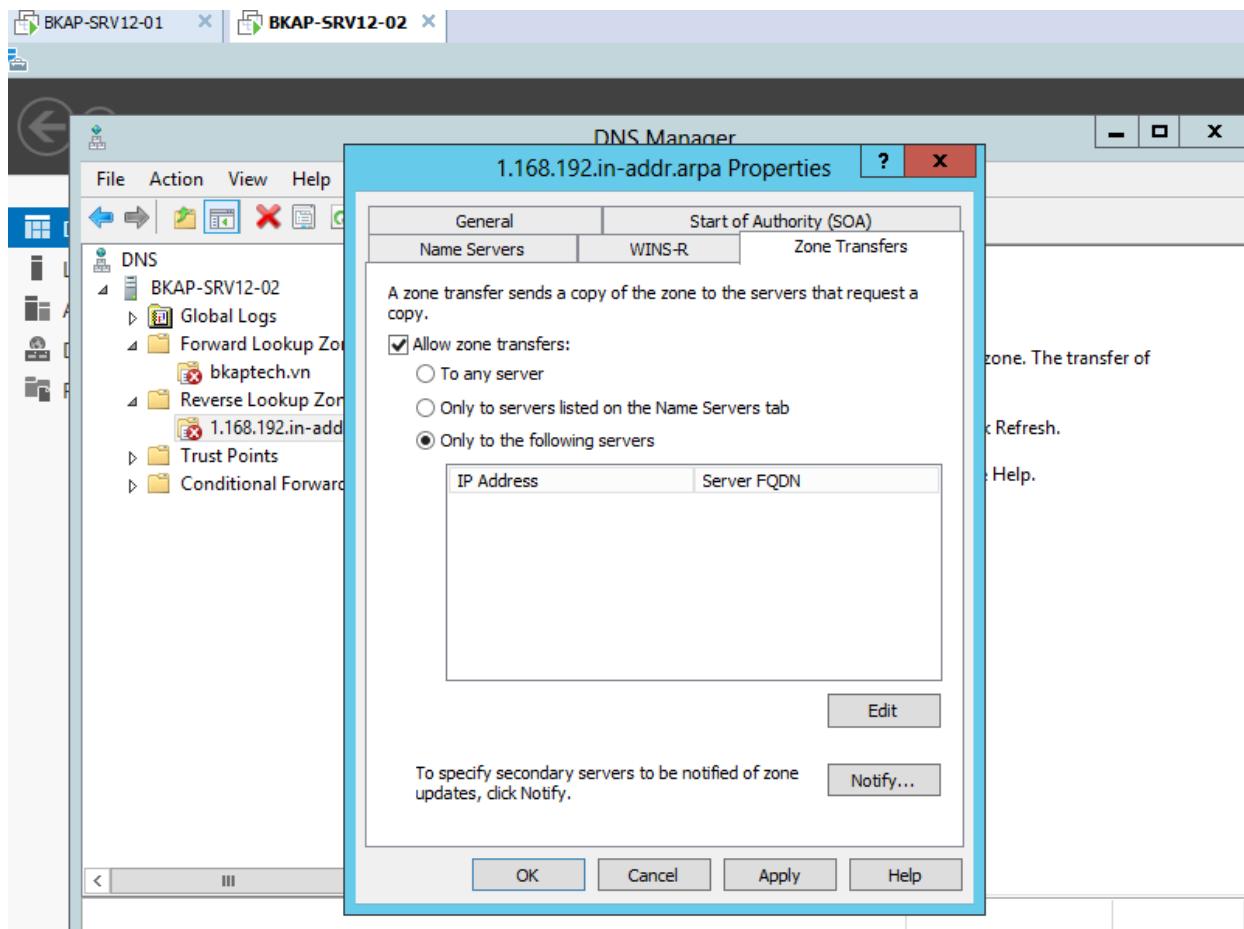
- Chuyển sang máy BKAP-SRV12-02, vào dịch vụ **DNS**.
 - Click chuột phải tại tên miền **bkaptech.vn** . / Properties.
 - Tại cửa sổ **bkaptech.vn Properties** , chuyển sang tab **Zone Transfers**, chọn vào **Allow zone transfers / Only to the following servers**.

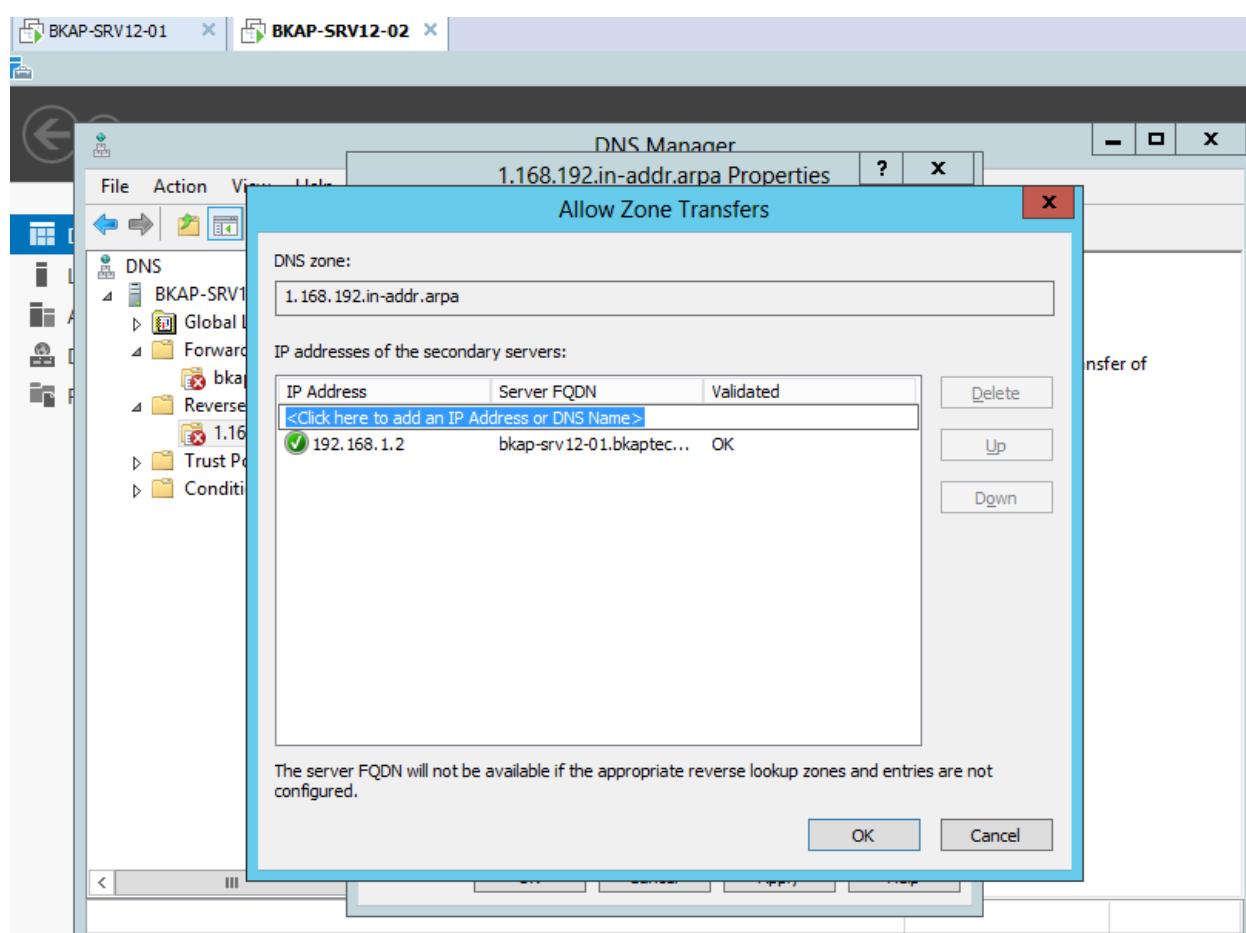


- Tại đây, tiếp tục click chọn vào **Edit**, tại cửa sổ **Allow Zone Transfers**, nhập vào địa chỉ của máy **BKAP-SRV12-01.(192.168.1.2)**

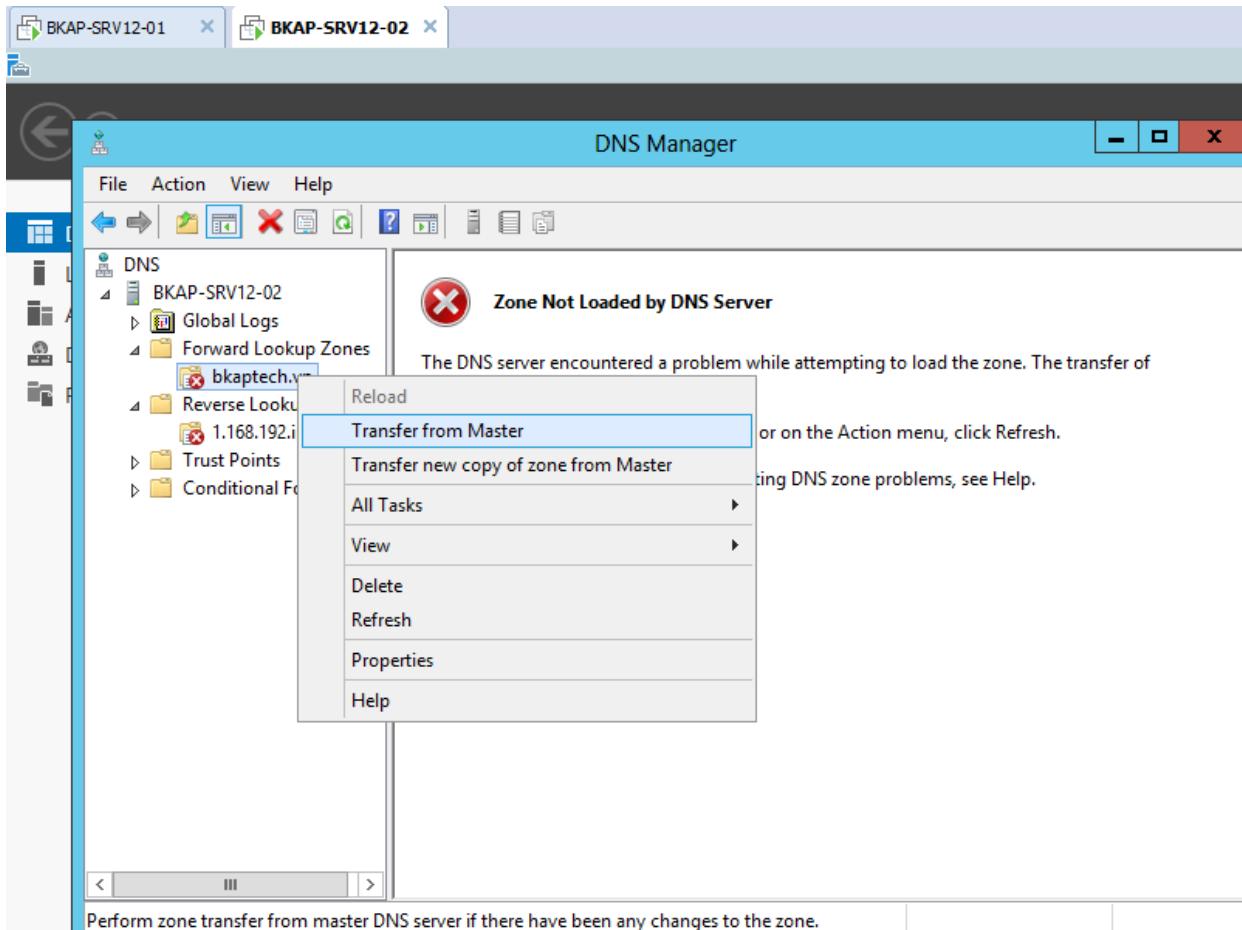


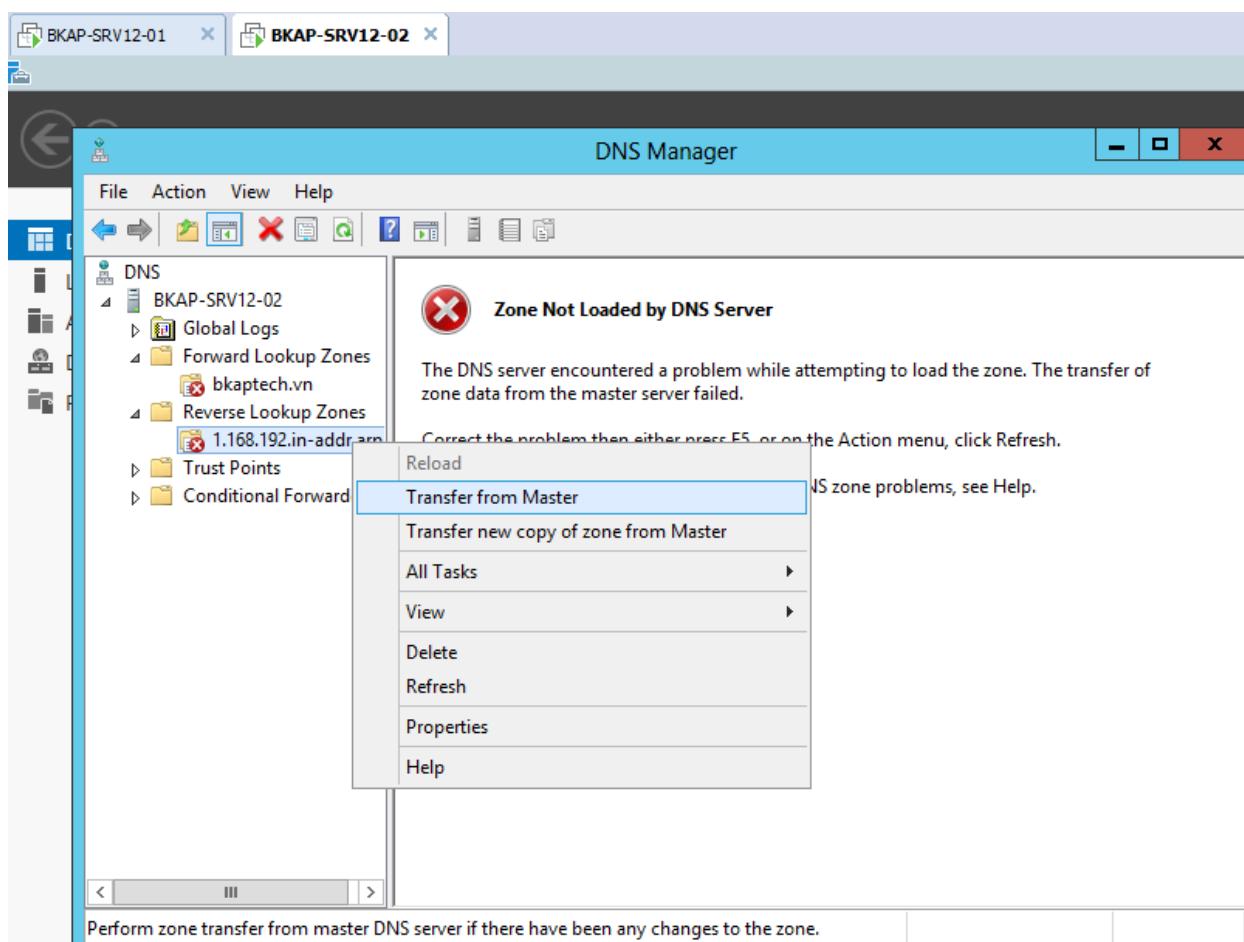
- Thực hiện tương tự đối với “1.168.192.in-addr.arpa”.



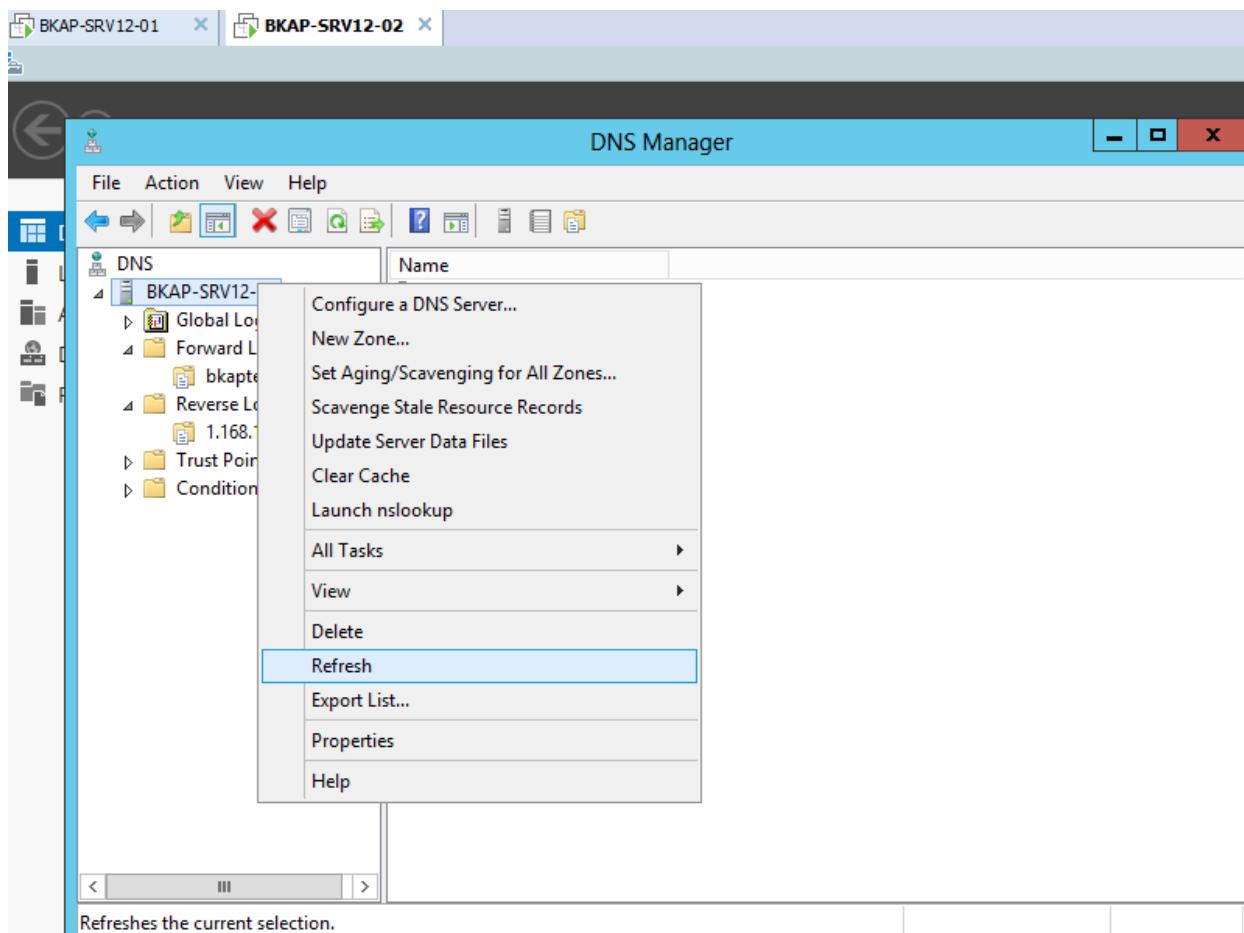


- Click chuột phải tại **bkaptech.vn** và **1.168.192.in-addr.arpa**, chọn vào **Transfer from Master**.

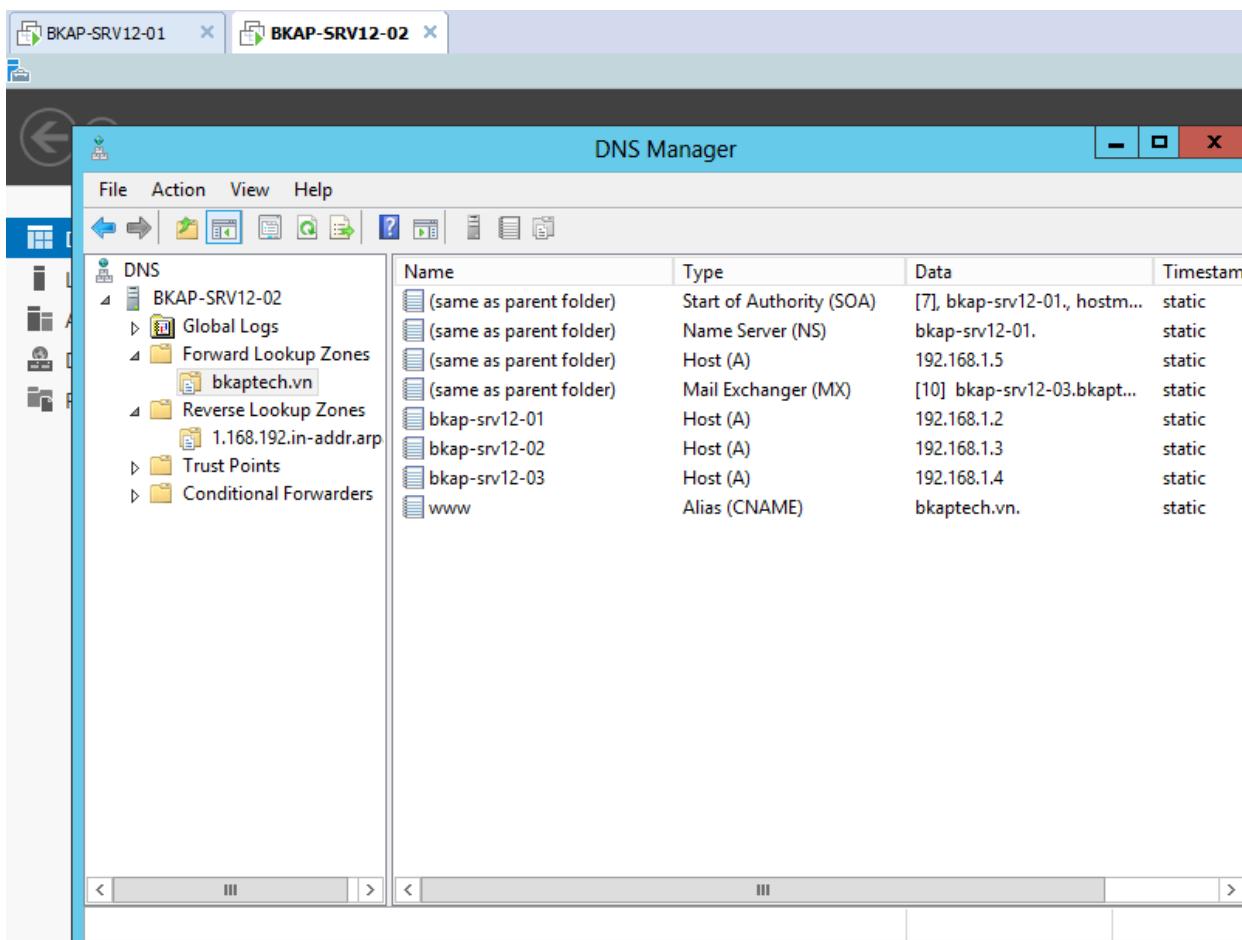


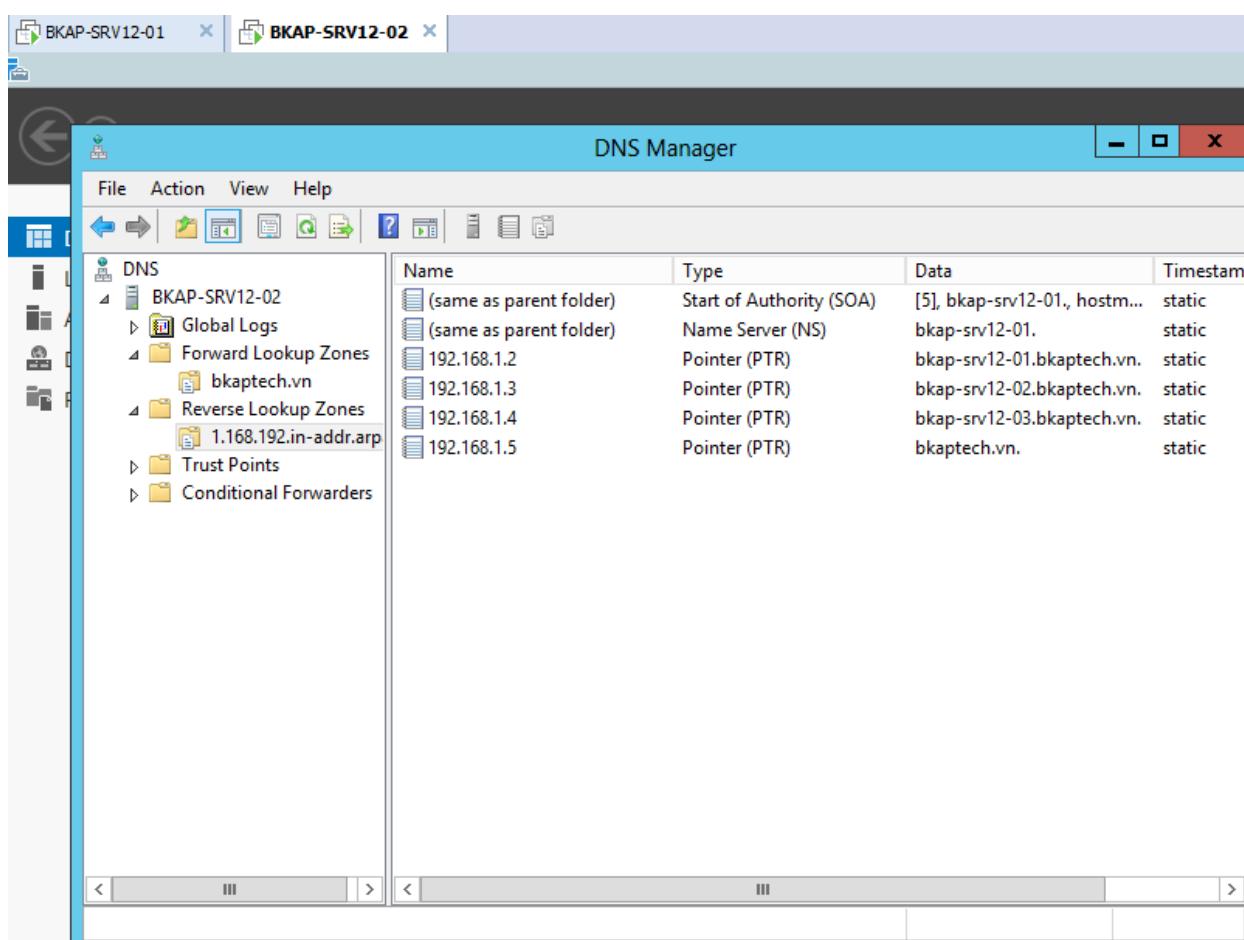


- Click vào BKAP-SRV12-02, chọn Refresh.



- DNS Server đã được Backup thành công.





Bài 10:

PHÂN QUYỀN VÀ CHIA SẺ DỮ LIỆU.

Các nội dung chính sẽ được đề cập:

- ✓ Cấu hình và phân quyền chia sẻ dữ liệu.
- ✓ Cấu hình **Shadow Copies** và **Windows Server Backup**.
- ✓ Cấu hình **Offline Files**.

10.1 Cấu hình và phân quyền chia sẻ dữ liệu.

1. Yêu cầu bài lab:

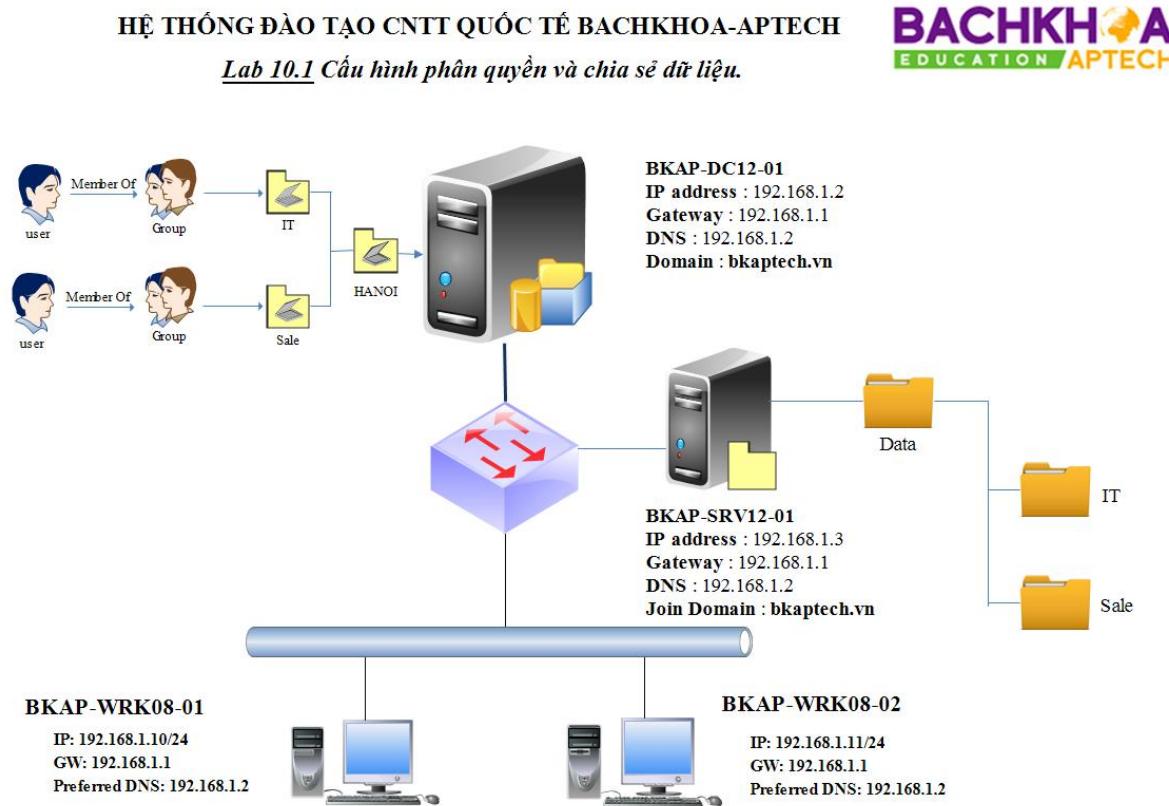
- + Tạo OU, tài khoản người dùng và tài khoản nhóm theo miền **bkaptech.vn**.
- + Tạo lần lượt các thư mục tương ứng trên máy **BKAP-SRV12-01** theo bảng:

Thư mục	Group	NTFS Permission
<i>IT</i>	<i>GG_S_IT</i>	<i>Modify</i>
<i>Sale</i>	<i>GG_S_Sale</i>	<i>Modify</i>

2. Yêu cầu chuẩn bị:

- + Máy **BKAP-DC12-01** dùng để tạo OU, Group, User.
- + Máy **BKAP-SRV12-01** Join vào miền dùng để tạo thư mục và phân quyền truy cập thư mục.
- + Máy **BKAP-WRK08-01** Join vào miền dùng để kiểm tra thư mục sau khi phân quyền.

3. Mô hình Lab:



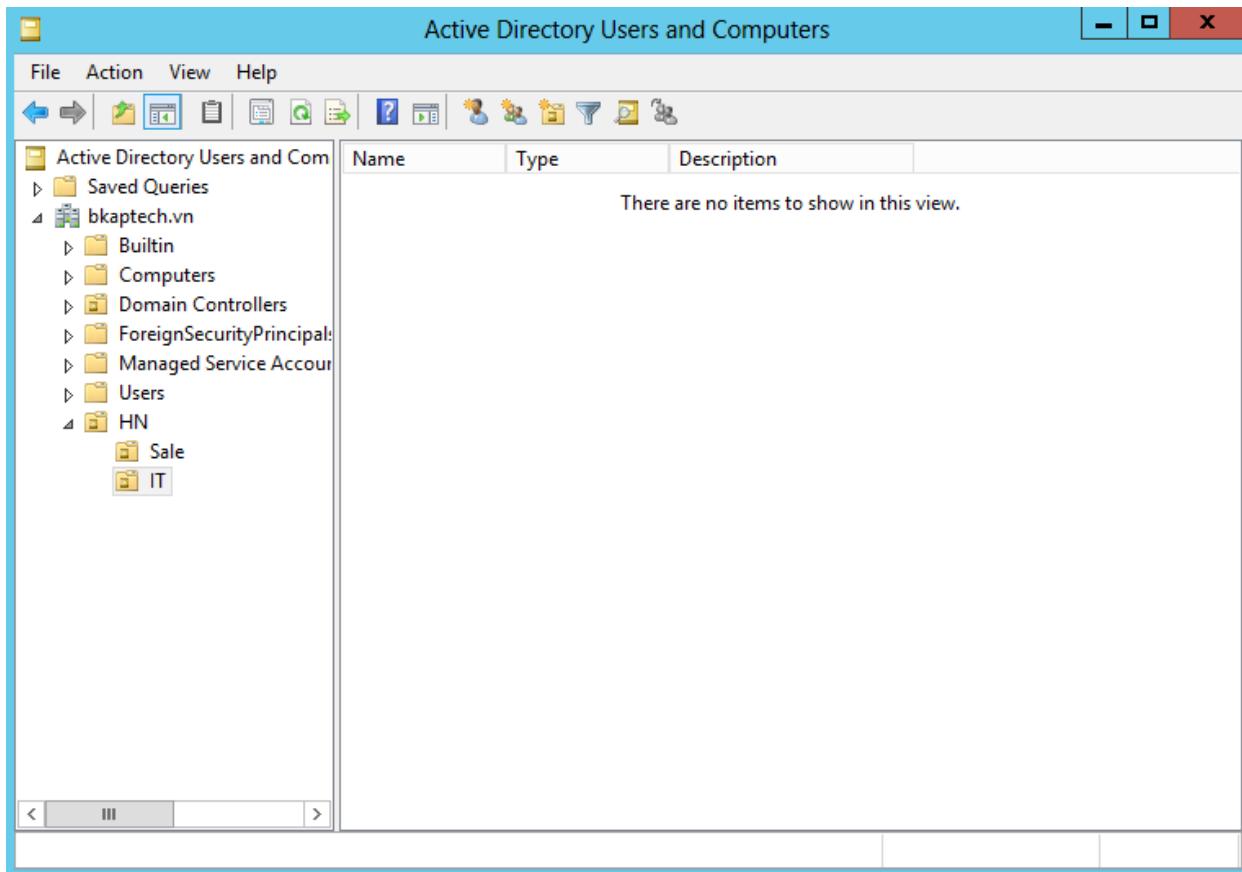
Hình 10.1

Sơ đồ địa chỉ như sau:

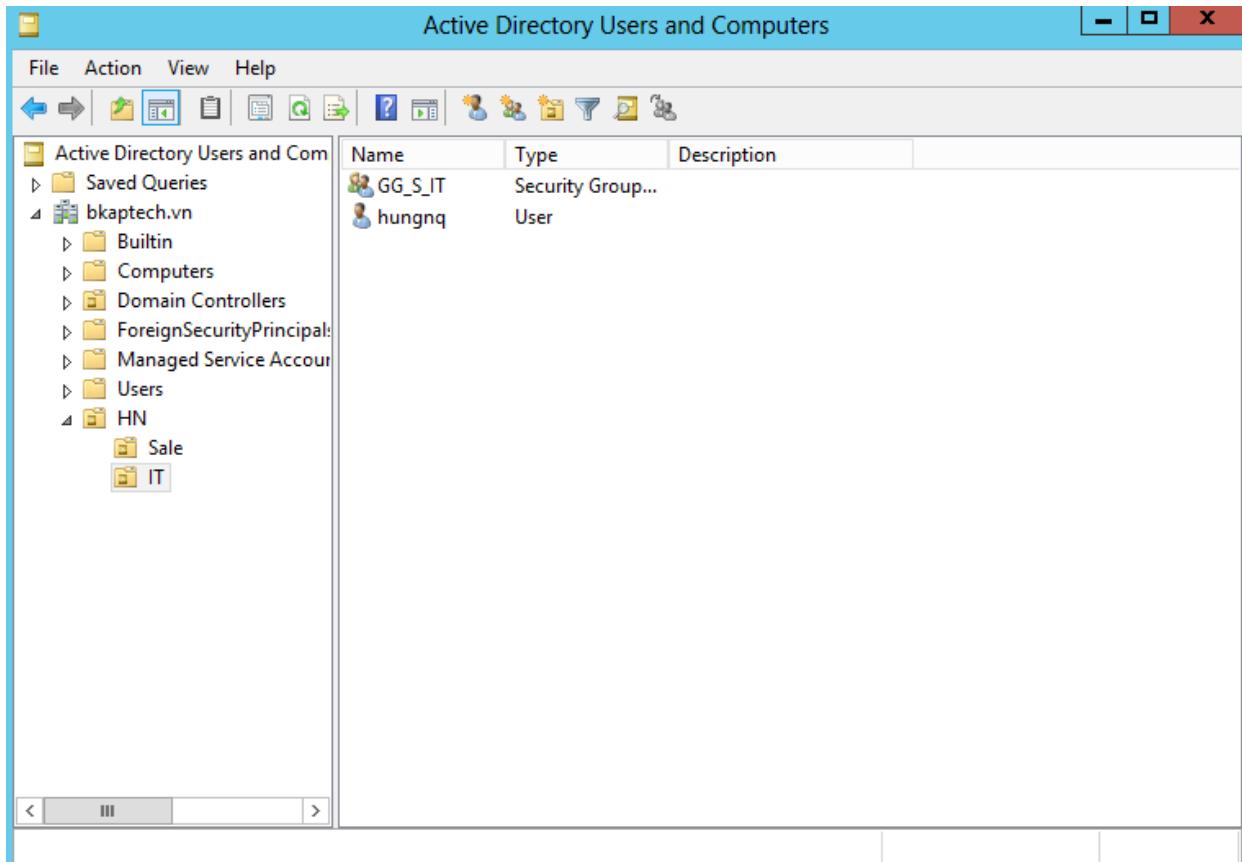
Thông số	BKAP-DC12-01	BKAP-SRV12-01	BKAP-WRK08-01
IP address	192.168.1.2	192.168.1.3	192.168.1.10
Default gateway	192.168.1.1	192.168.1.1	192.168.1.1
Subnet Mask	255.255.255.0	255.255.255.0	255.255.255.0
Preferred DNS Server	192.168.1.2	192.168.1.2	192.168.1.2

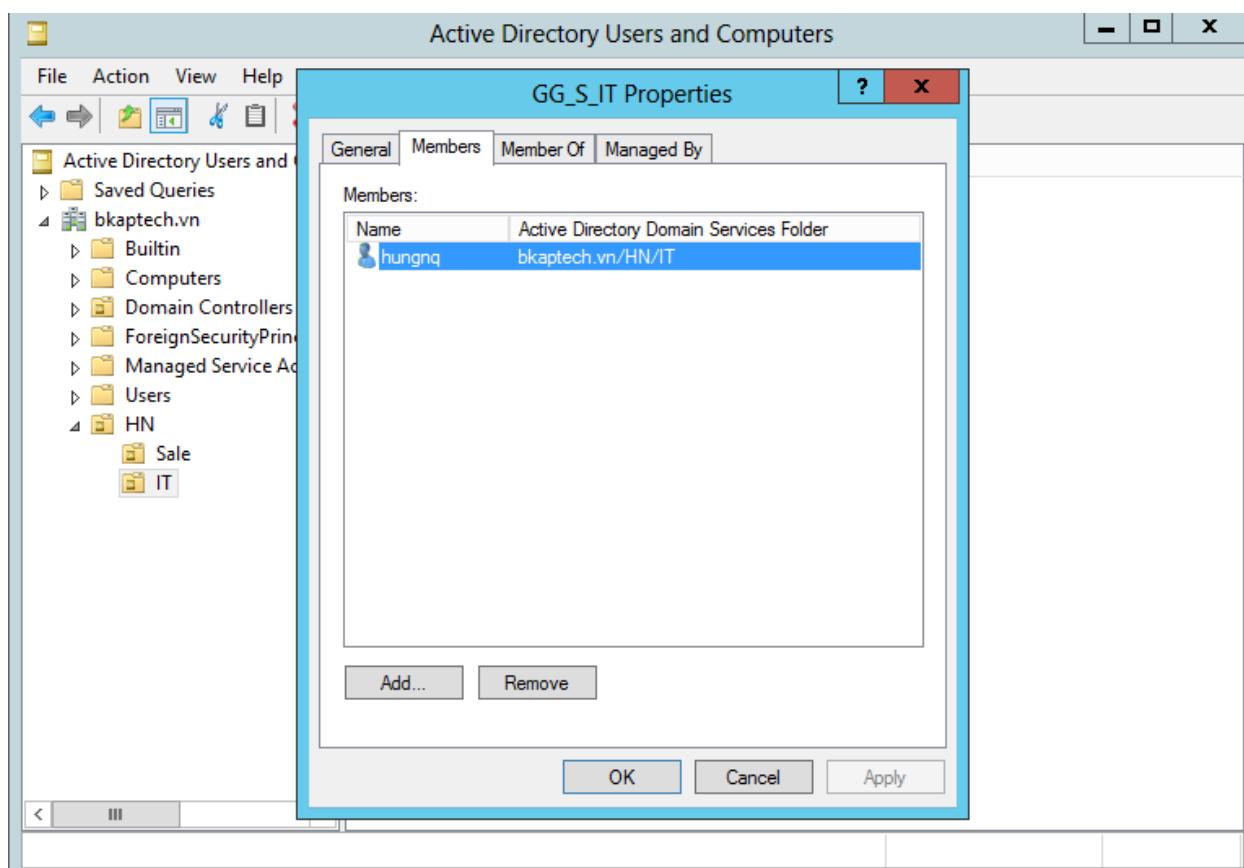
Hướng dẫn chi tiết :

- Thực hiện trên máy *BKAP-DC12-01*, tạo OU, Group, User.
 - Tạo OU **HN**.
 - Trong OU **HN**, tạo OU **Sale** và OU **IT**.

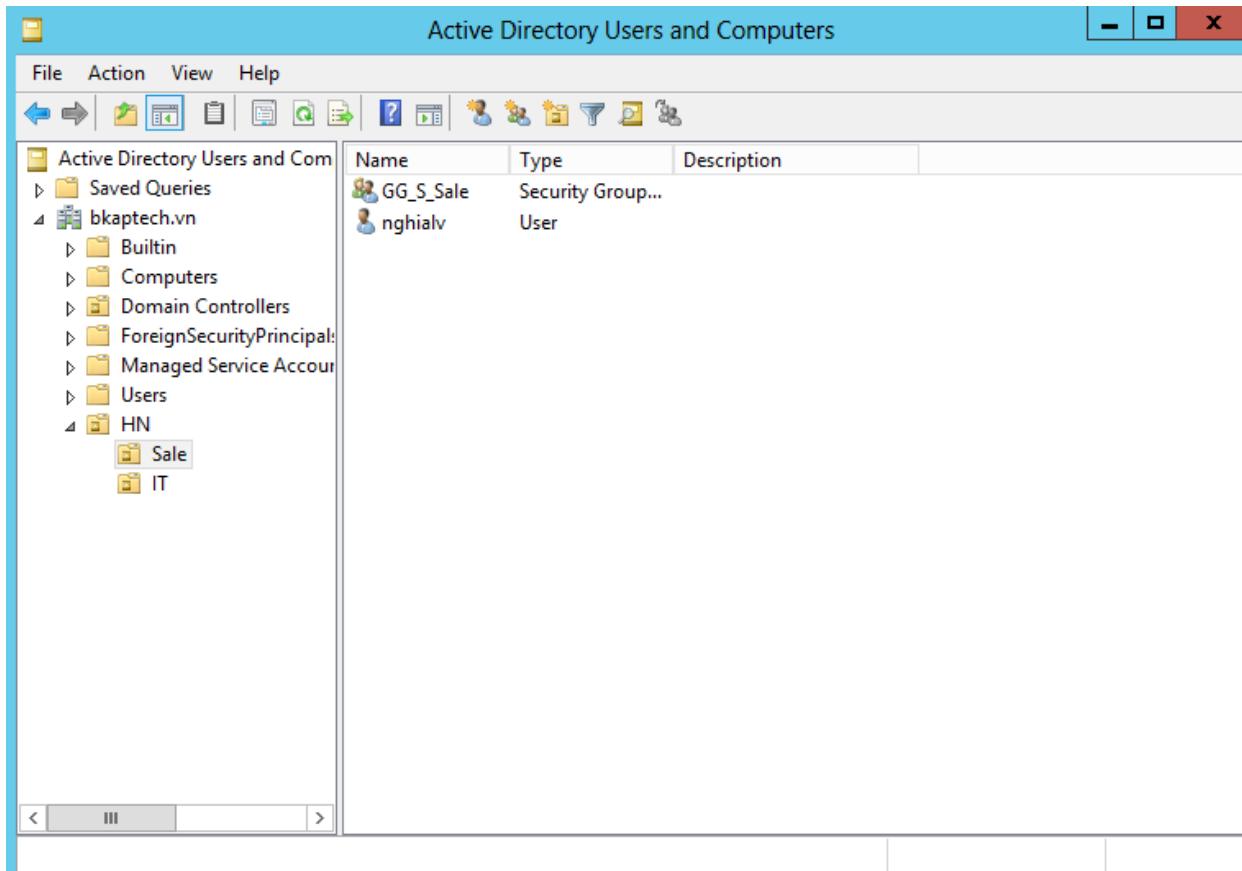


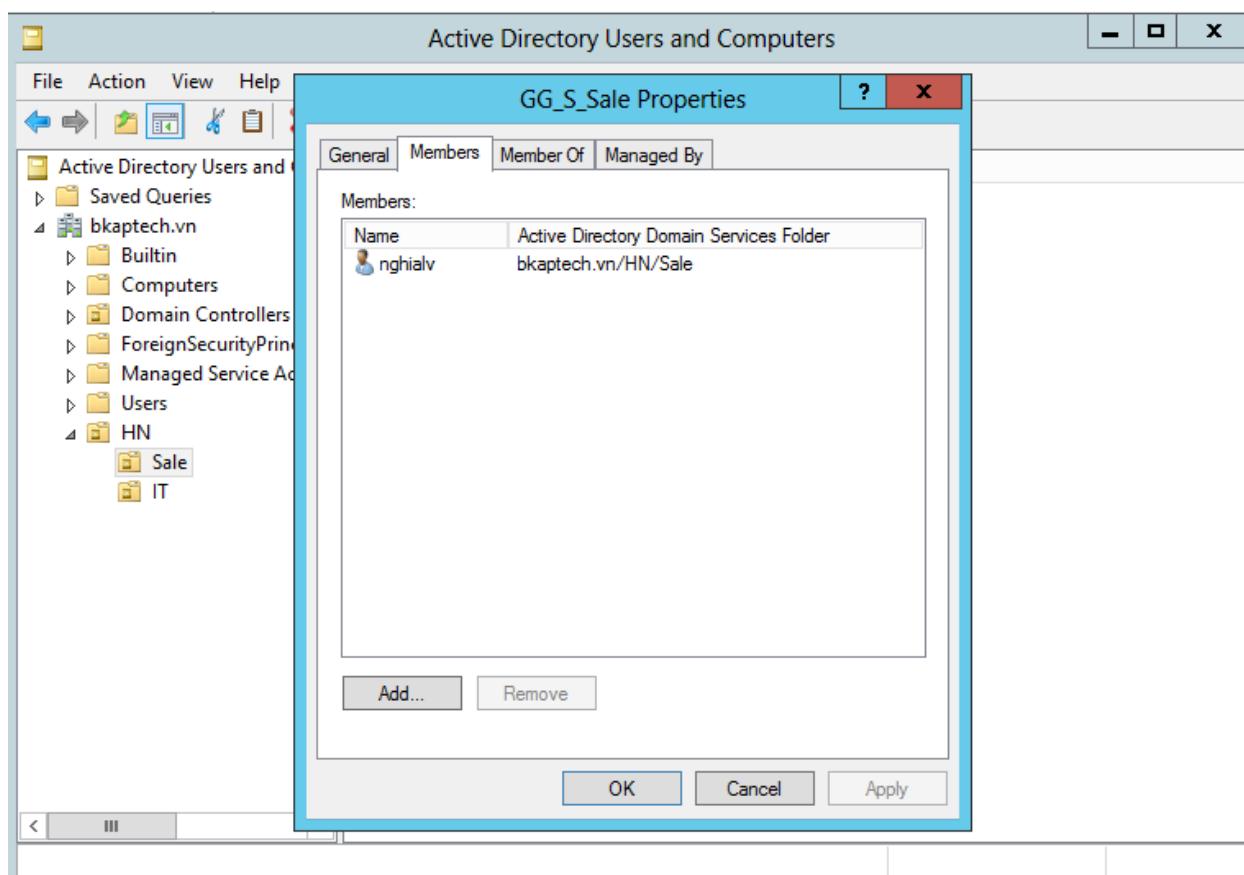
- Trong OU IT, tạo Group *GG_S_IT*, và User *hungnq*, add User *hungnq* vào group *GG_S_IT*.



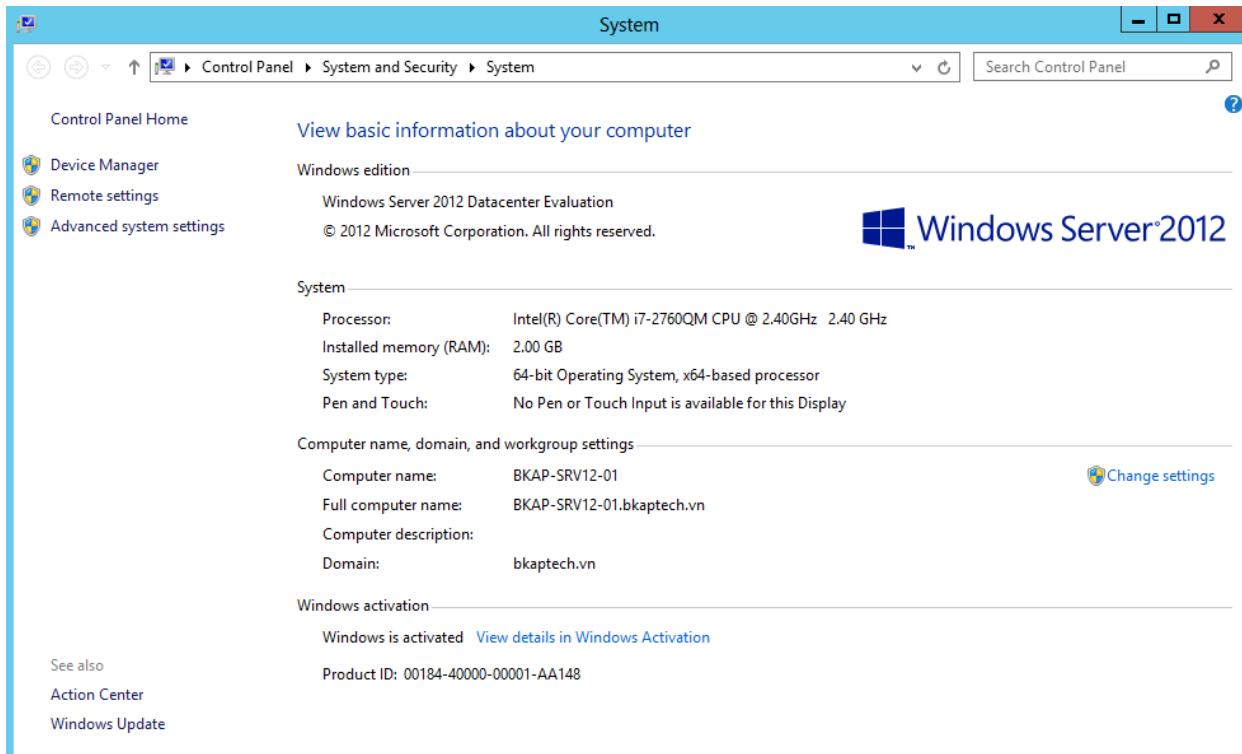


- Trong OU **Sale**, tạo Group *GG_S_Sale* và User *nghialv*, Add user *nghialv* vào Group *GG_S_Sale*.

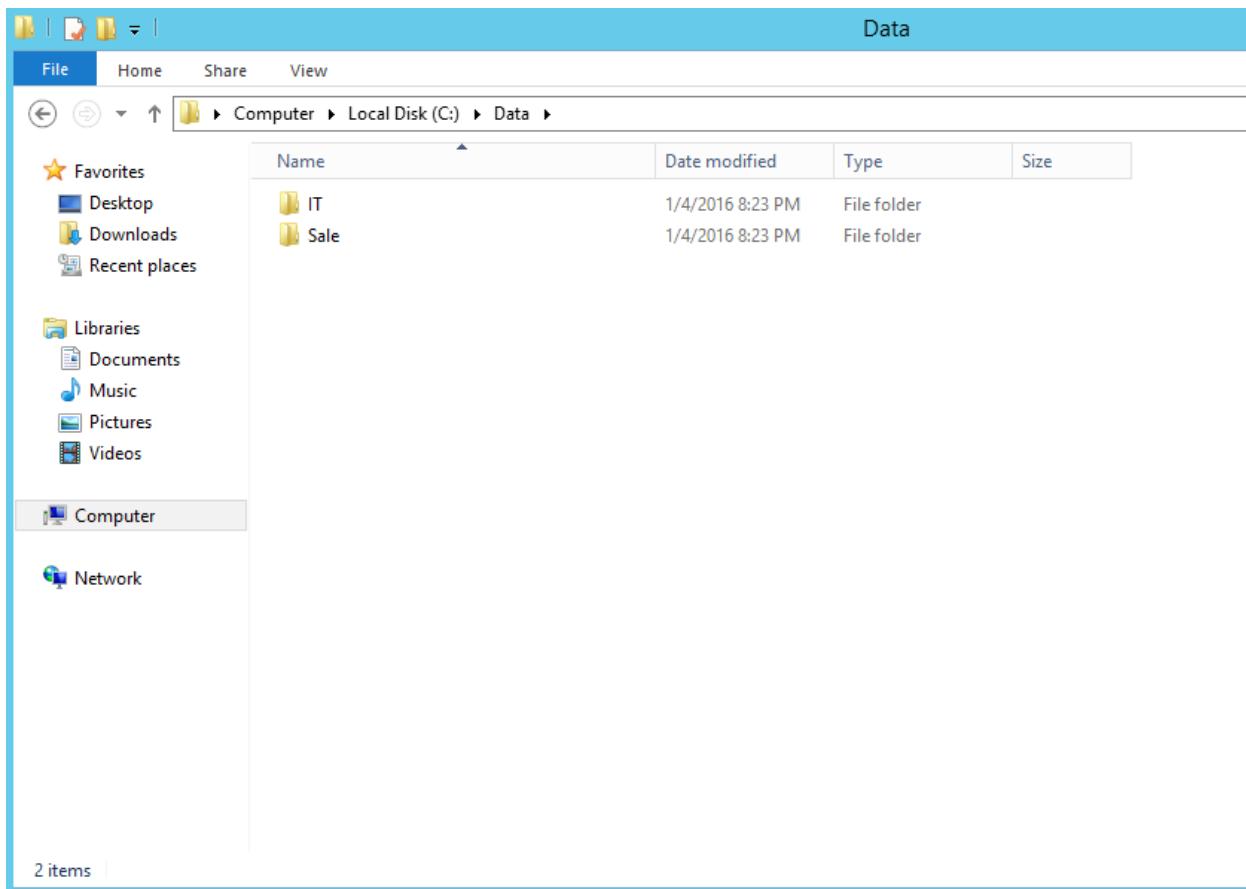




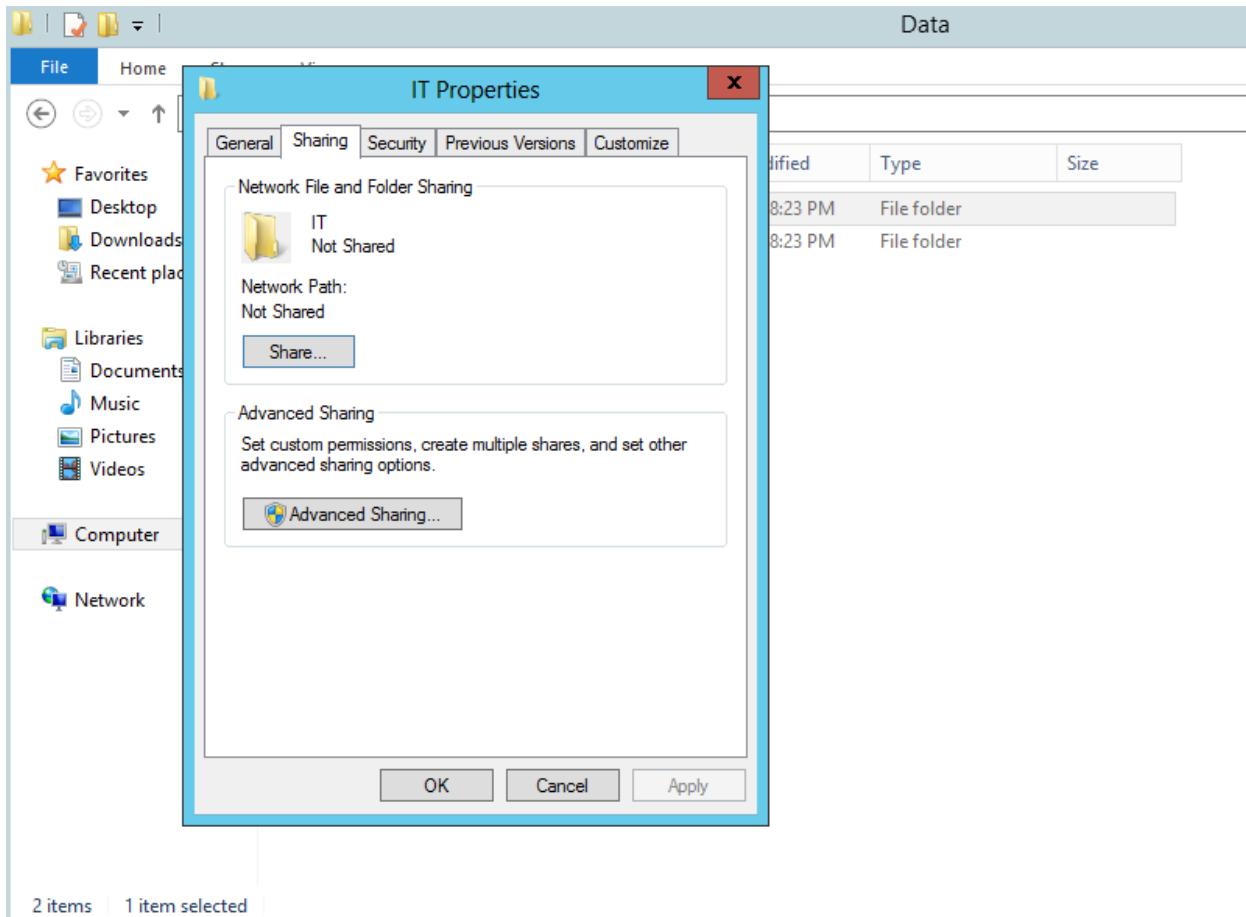
- Chuyển sang máy *BKAP-SRV12-01* để cấu hình chia sẻ tài nguyên cho các phòng ban.
 - Join máy *BKAP-SRV12-01* vào Domain.



- Vào ổ C, tiến hành tạo Folder “Data” , trong folder Data, tạo 2 Folder **IT** và **Sale**.

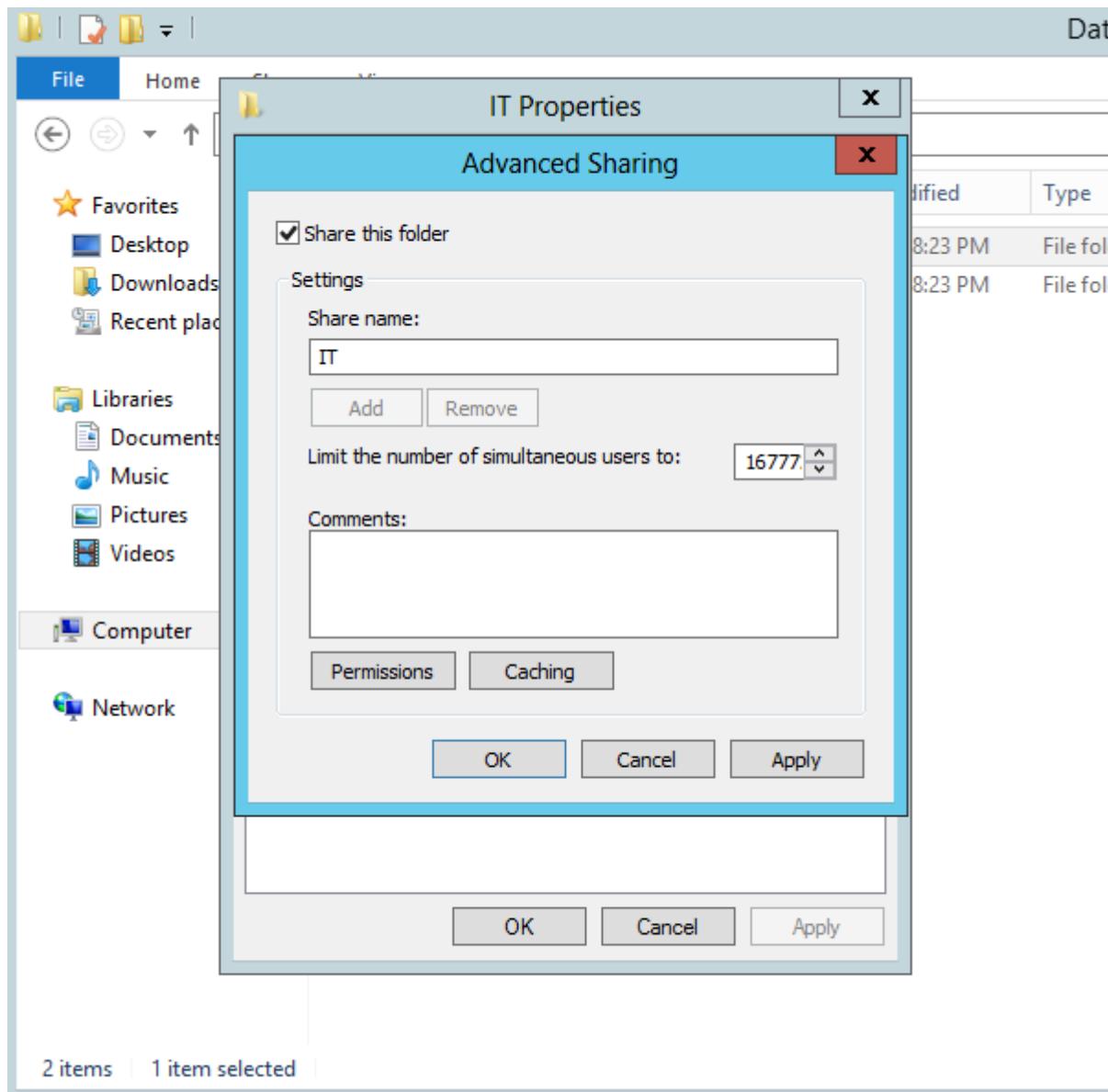


- Tiến hành Share *thư mục IT*(các tài khoản trong nhóm *GG_S_IT* được phép *đọc và sửa* tài liệu trong thư mục **IT**).
- Click chuột phải vào thư mục **IT**, chọn **Properties**.
- Tại cửa sổ **IT Properties**, chuyển sang tab **Sharing**.



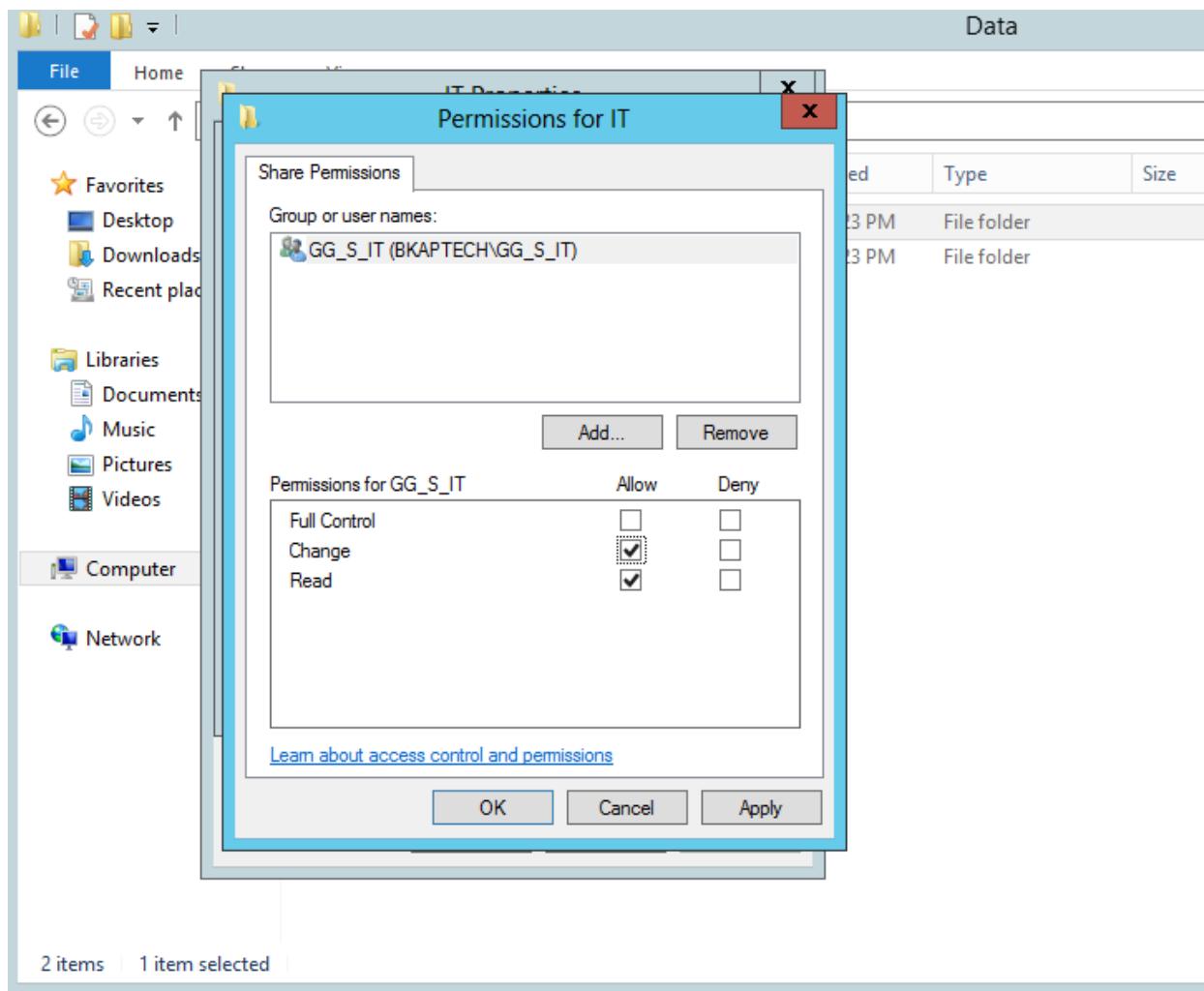
- Tại tab **Sharing**, click vào **Advanced Sharing...**

- Tại cửa sổ Advanced Sharing , click tích vào Share this folder.



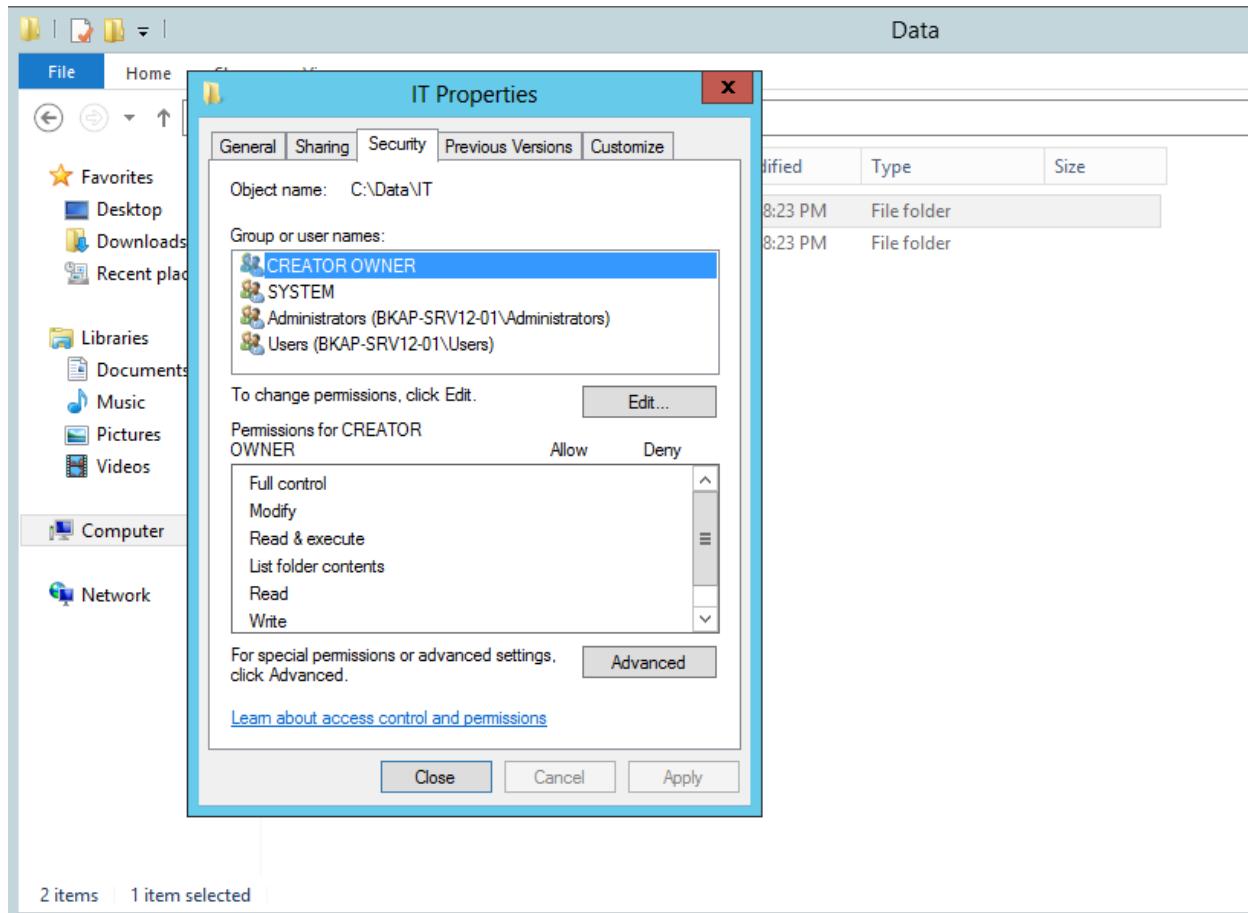
2 items | 1 item selected

- Click vào **Permissions**, tại cửa sổ **Permissions for IT**, thực hiện **Remove Group Everyone**, **Add group GG_S_IT** tại khung **Group or user name**.
- Tại khung **Permissions** bên dưới, click chọn 2 quyền **Change** và **Read**.



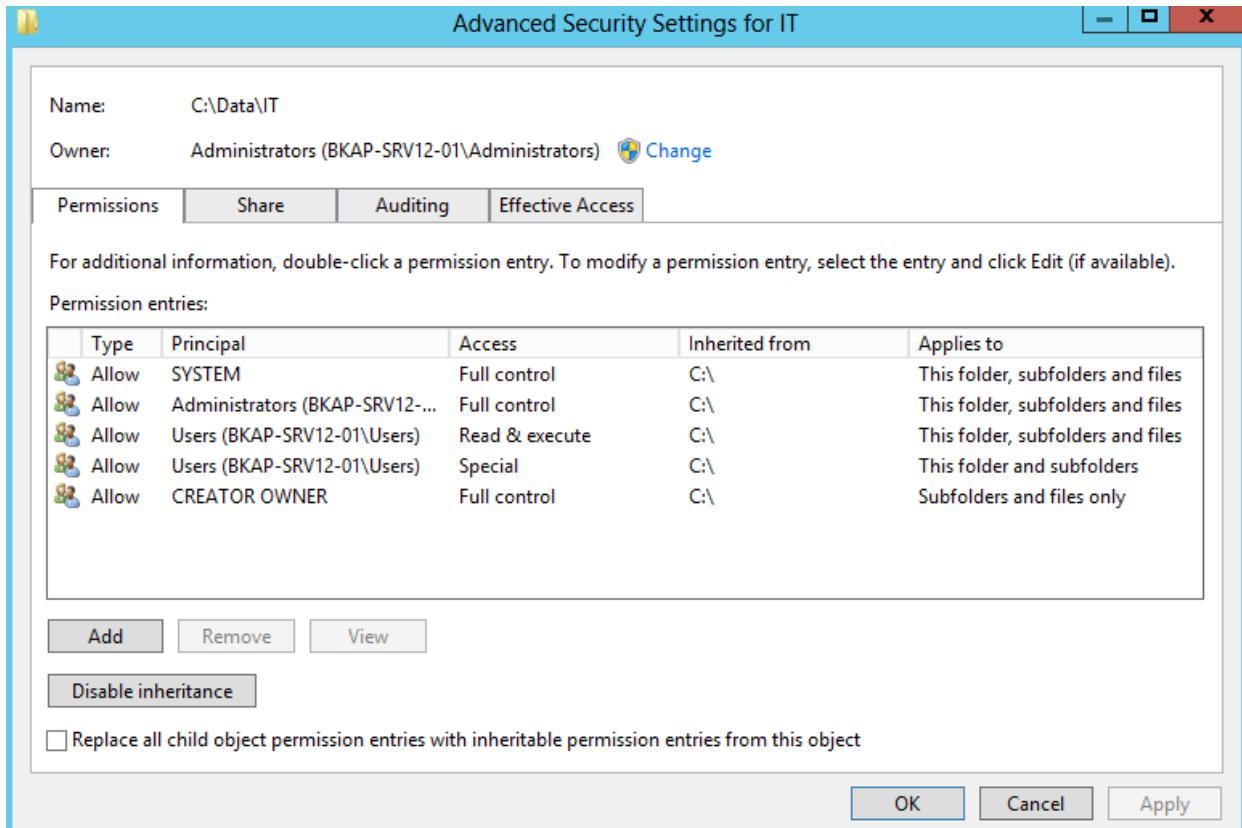
- **Apply / OK.**

- Tại cửa sổ **IT Properties**, chuyển sang Tab **Security**, click chọn vào **Advanced**

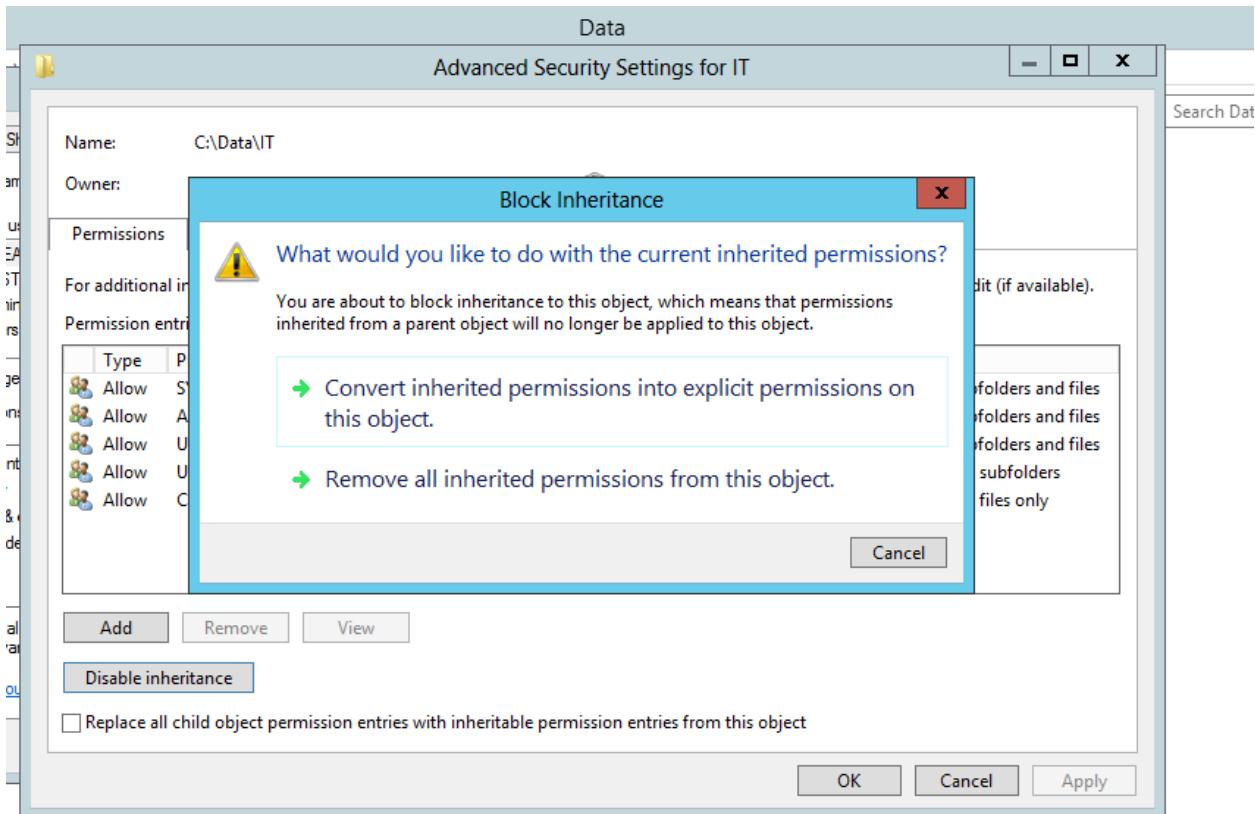


2 items | 1 item selected

- Tại cửa sổ **Advanced Security Settings for IT**, click vào **Disable inheritance(bỏ quyền kế thừa)**.

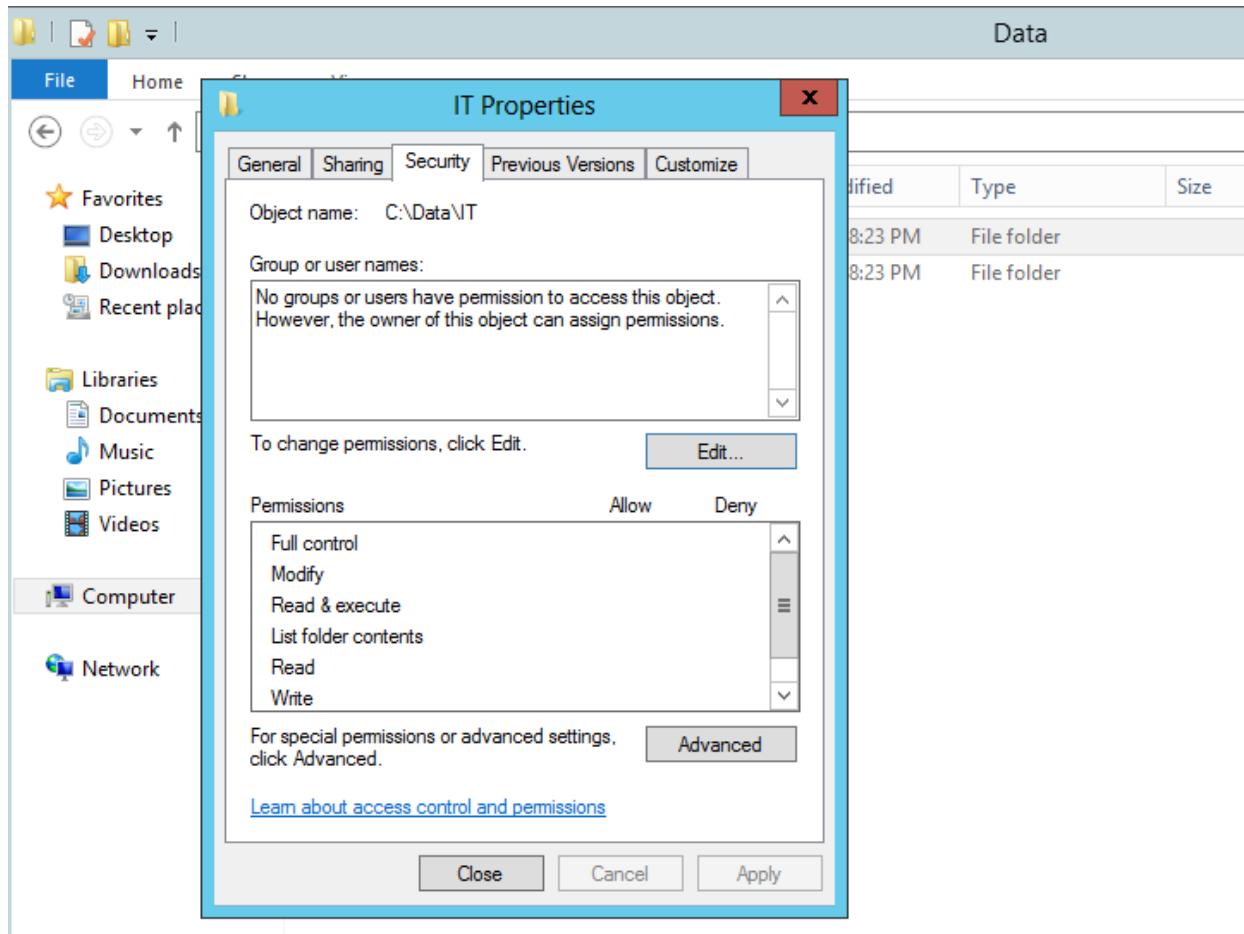


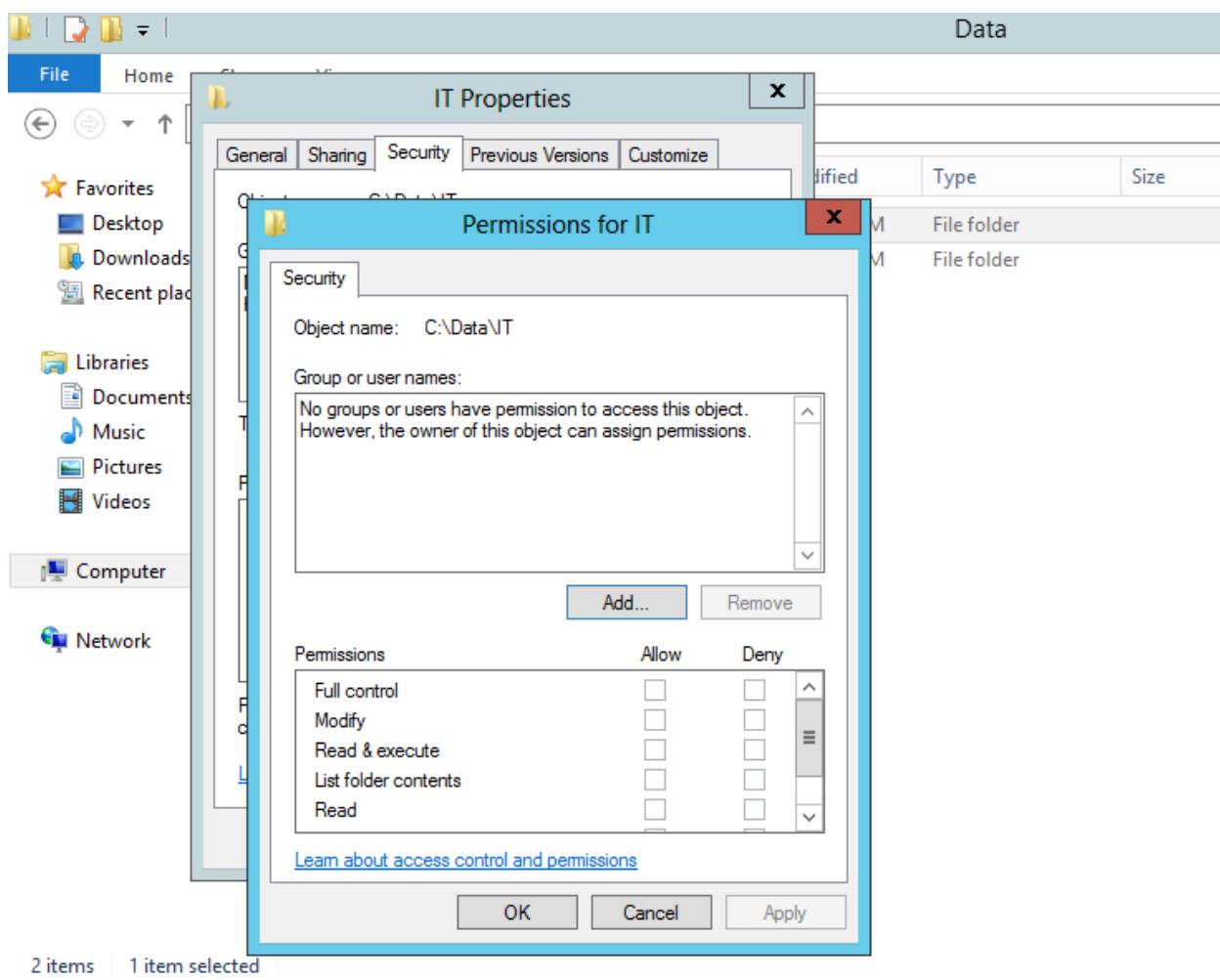
- Tại cửa sổ **Block Inheritance**, chọn vào **Remove all inherited permissions from this object**.



- **OK.**

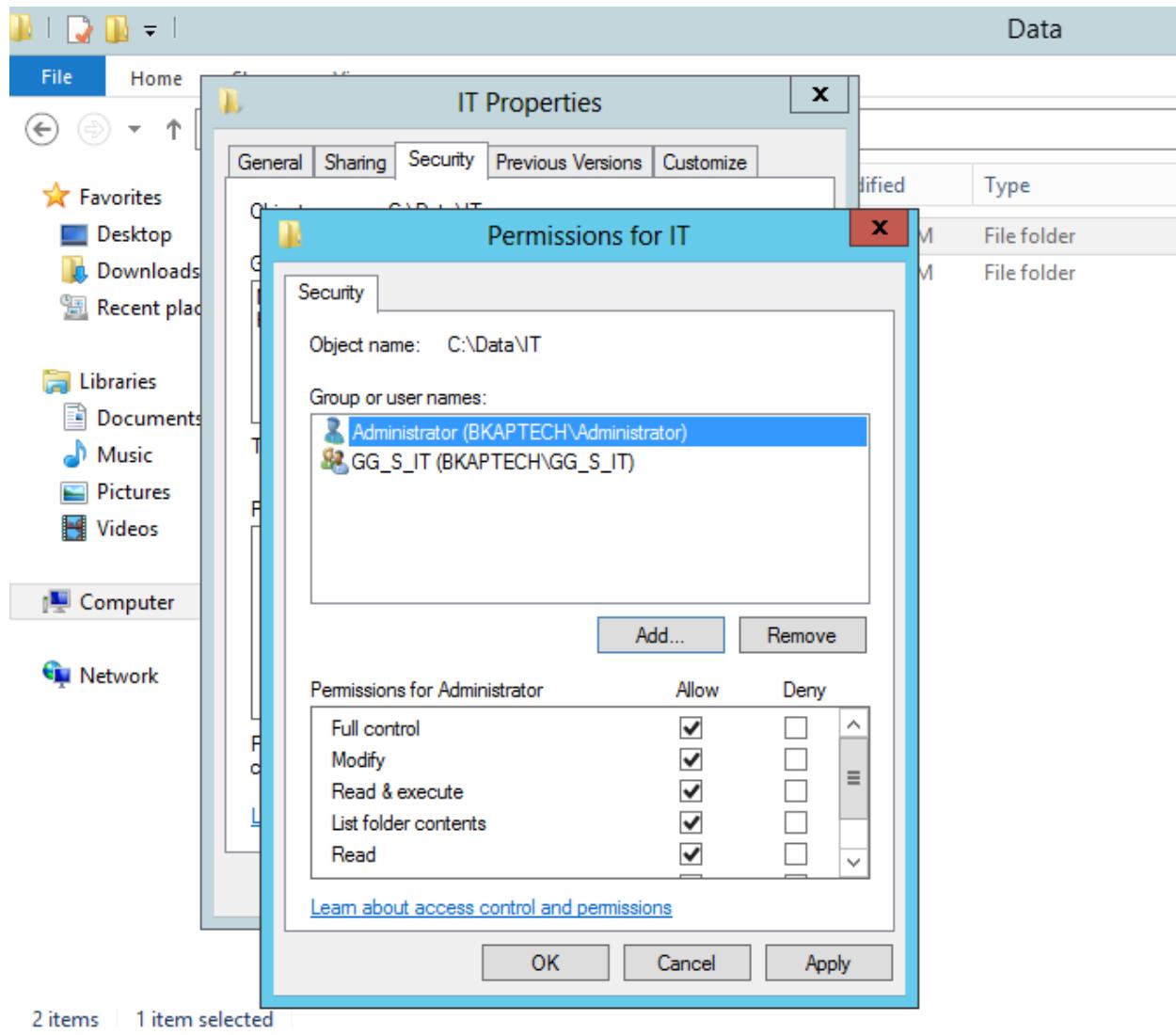
- Tại cửa sổ **IT Properties**, tab **Security**, click vào **Edit**, tại cửa sổ **Permissions for IT**, click vào **Add..**



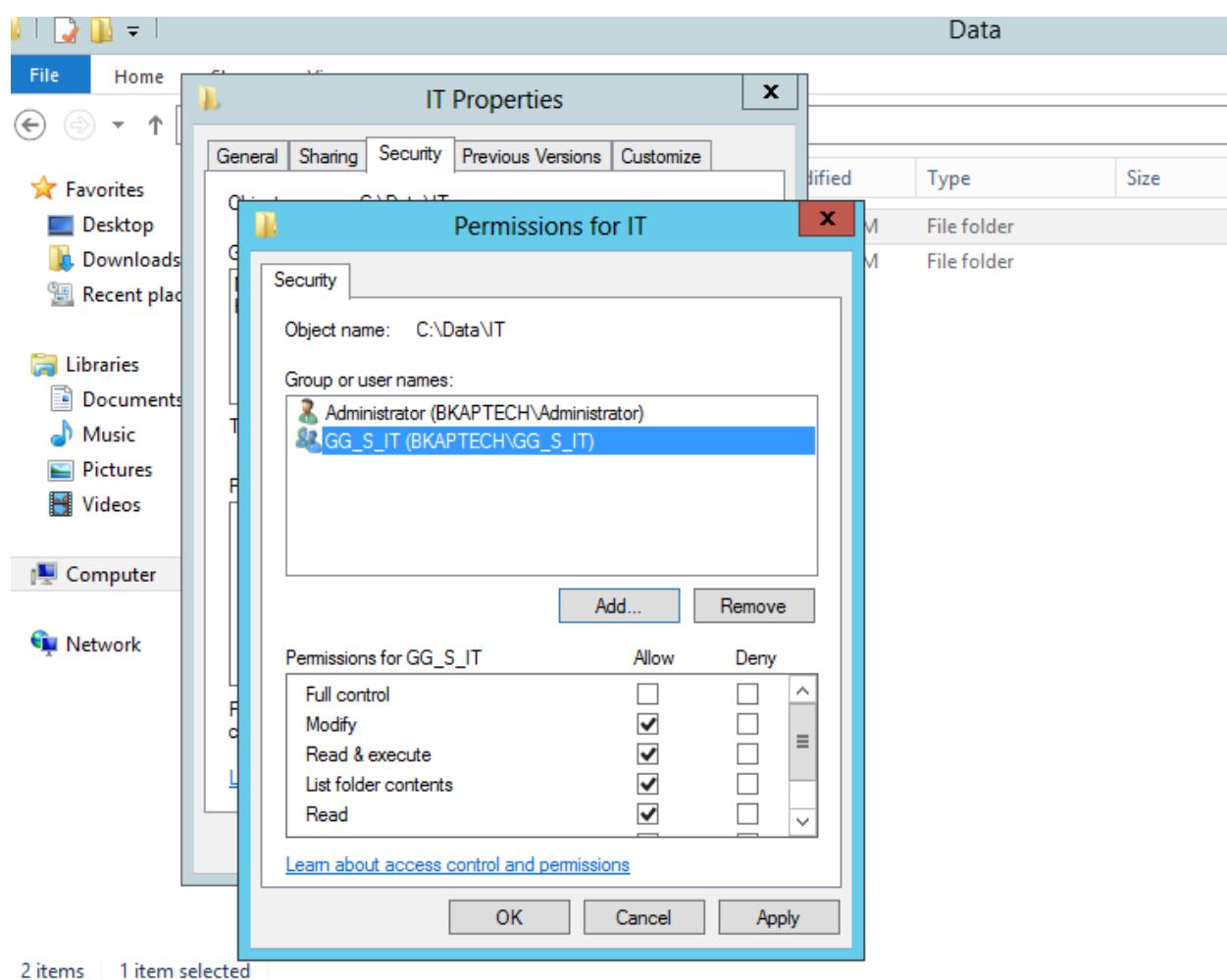


- Tại cửa sổ **Select Users, Computers, Service Accounts, or Groups**, nhập vào tên *User Administrator* và *Group GG_S_IT*.

- Phân quyền tương ứng như sau:
 - **Administrator : Full control**
 - **GG_S_IT : Modify**

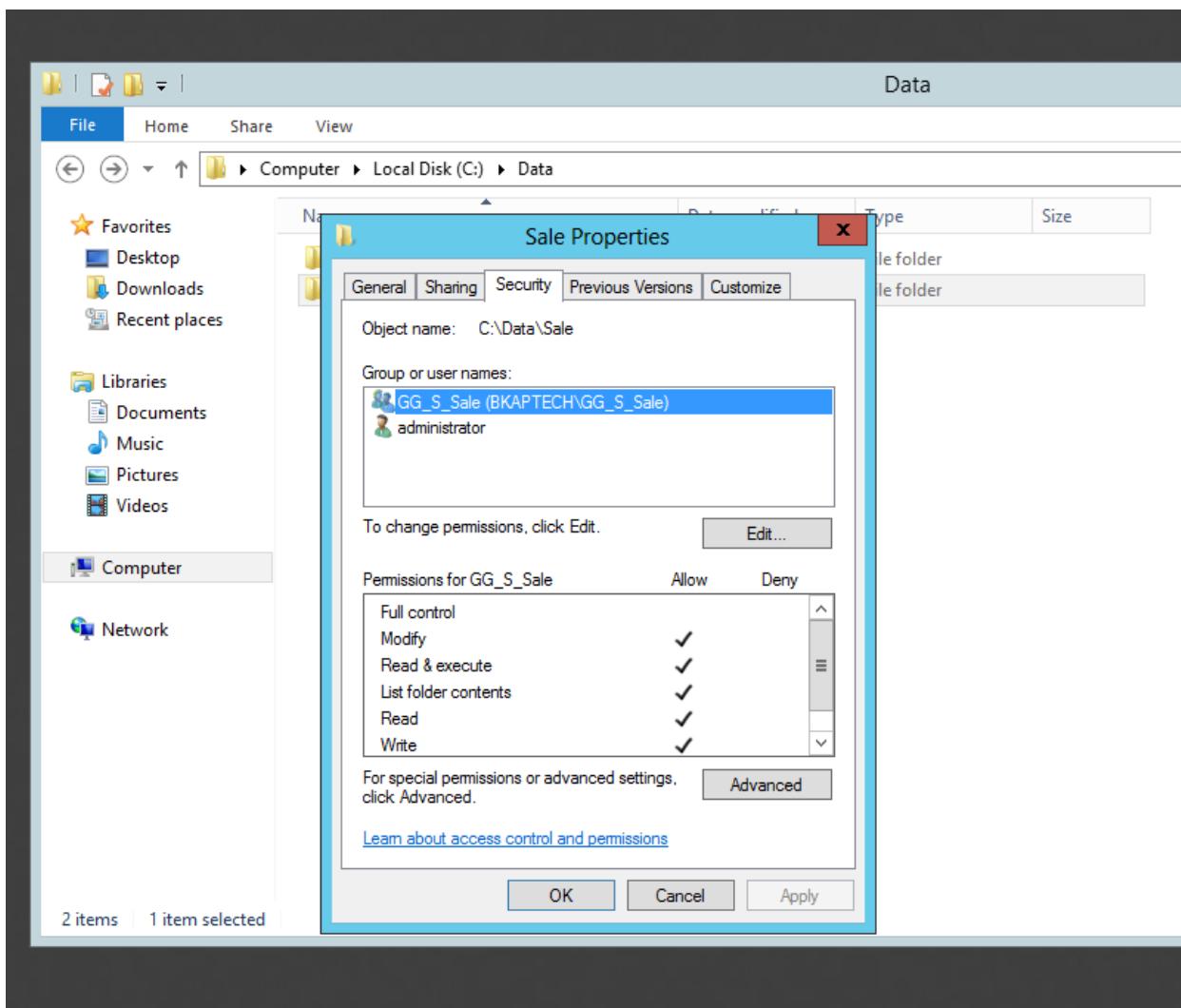


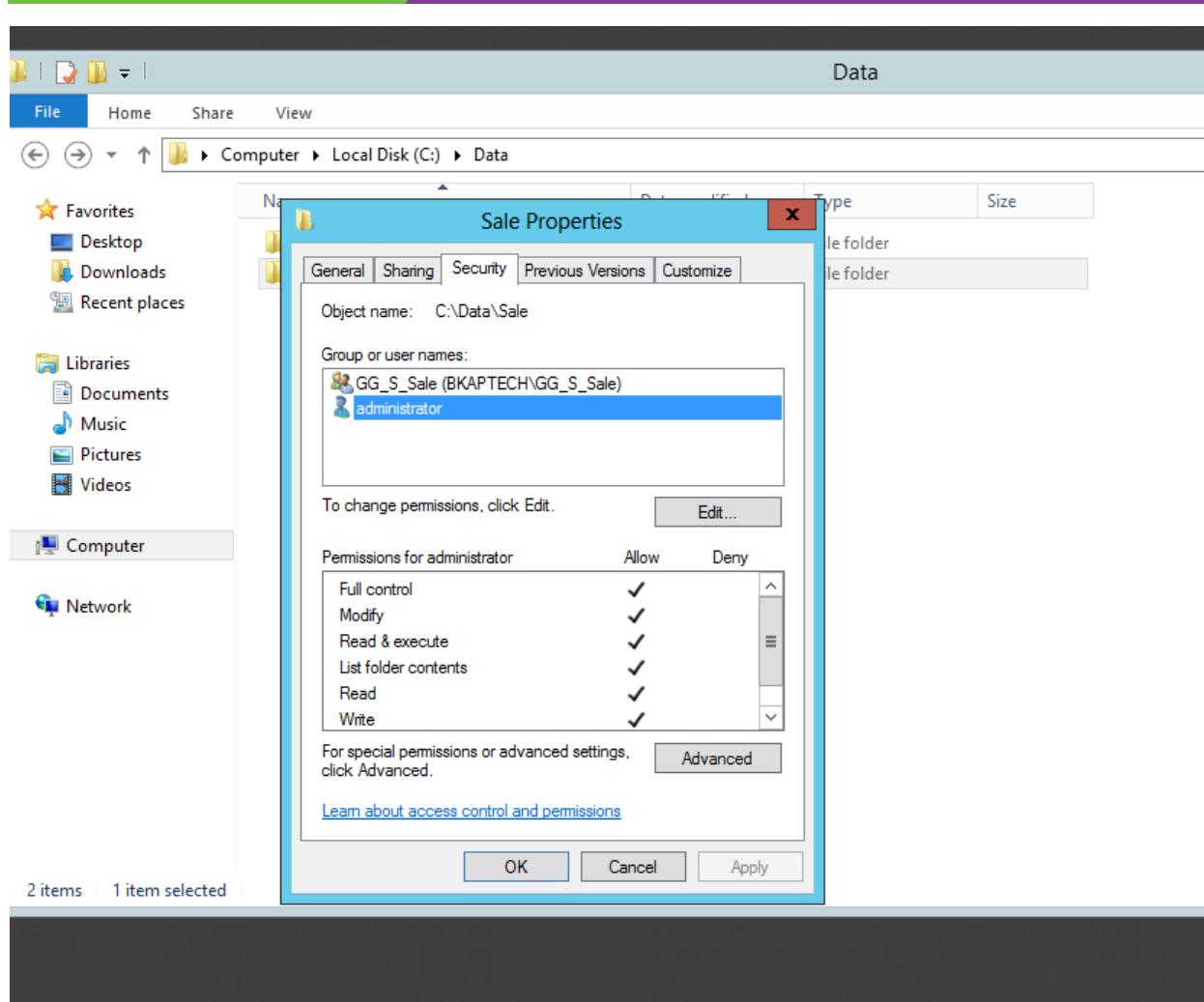
2 items | 1 item selected



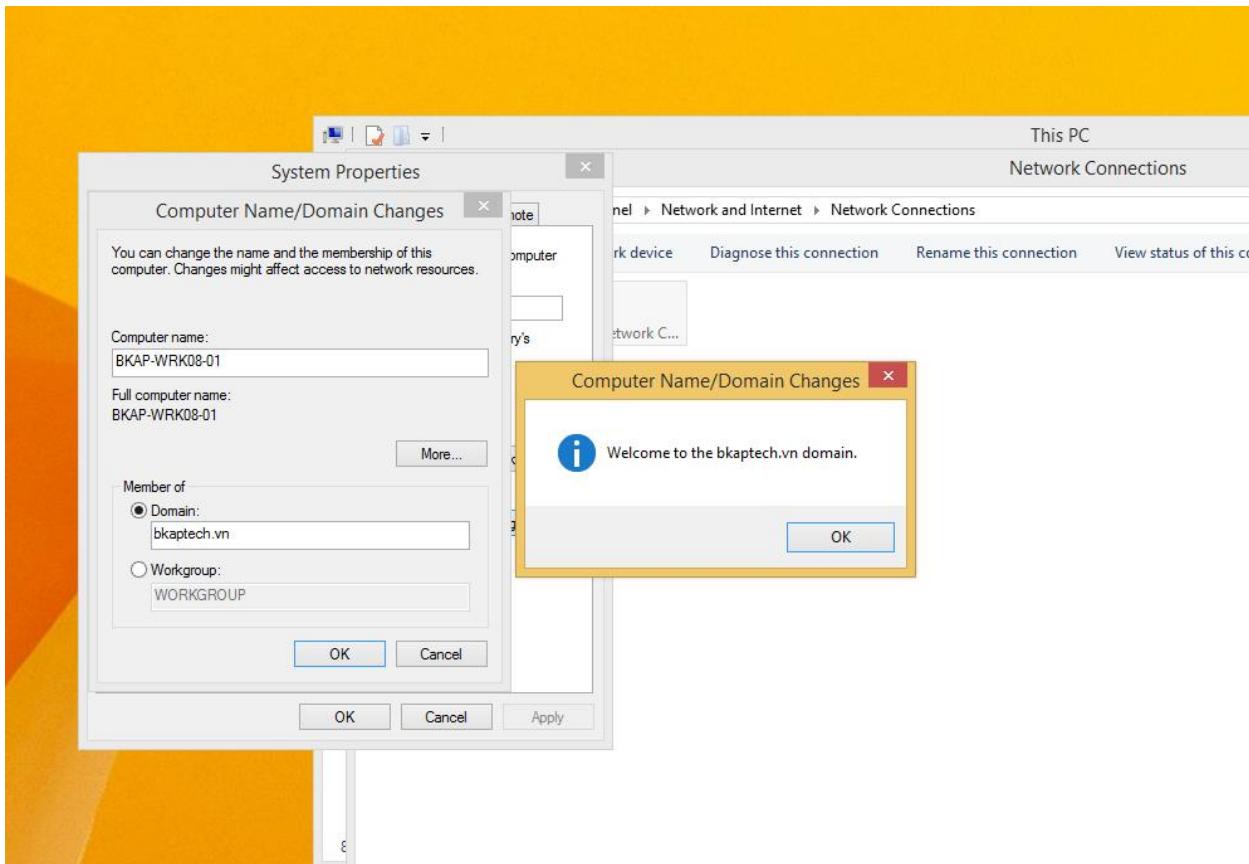
2 items | 1 item selected

- Thực hiện tương tự đối với thư mục Sale. Kết quả như sau:

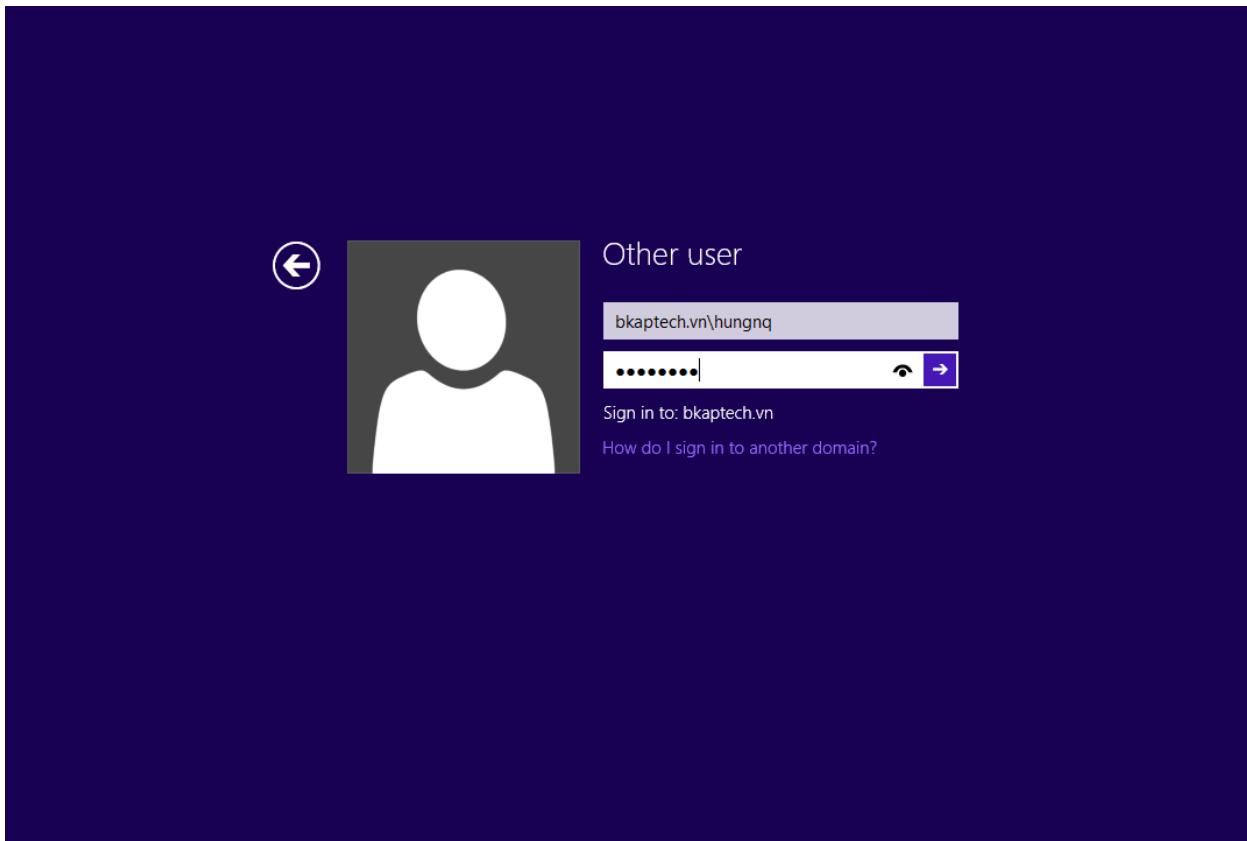




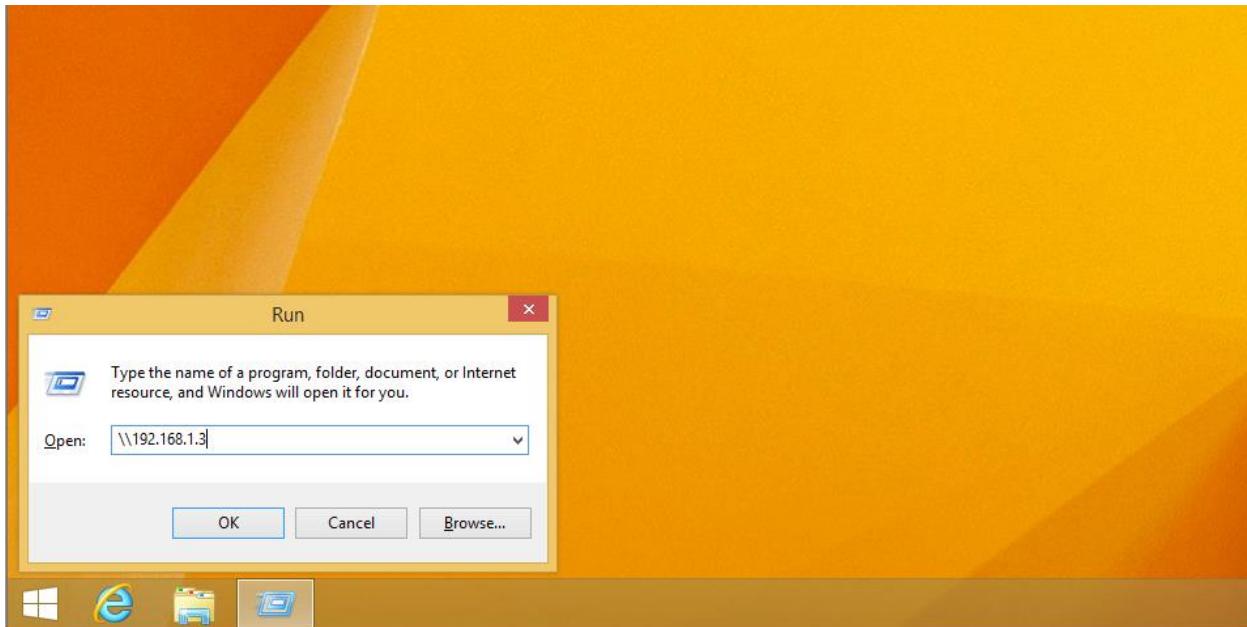
- Chuyển sang máy Client Win 8 đăng nhập bằng tài khoản người dùng để kiểm tra.
 - Join máy Client *BKAP-WRK08-01* vào Domain.



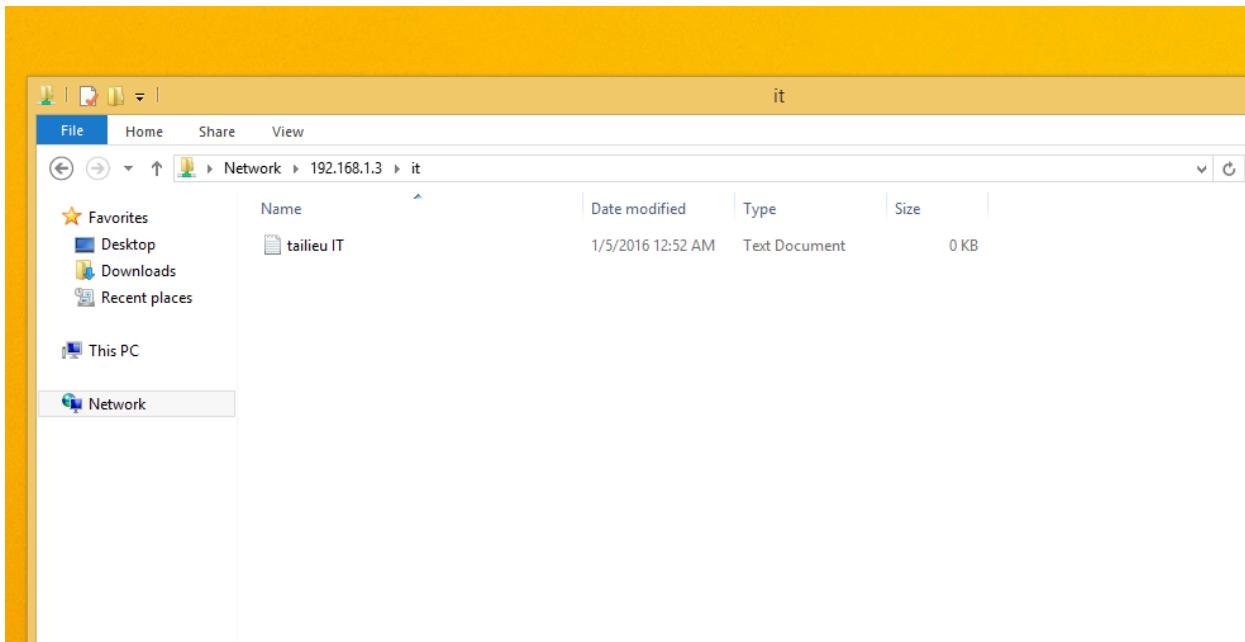
- Đăng nhập bằng tài khoản *hungnq* của phòng ban IT.



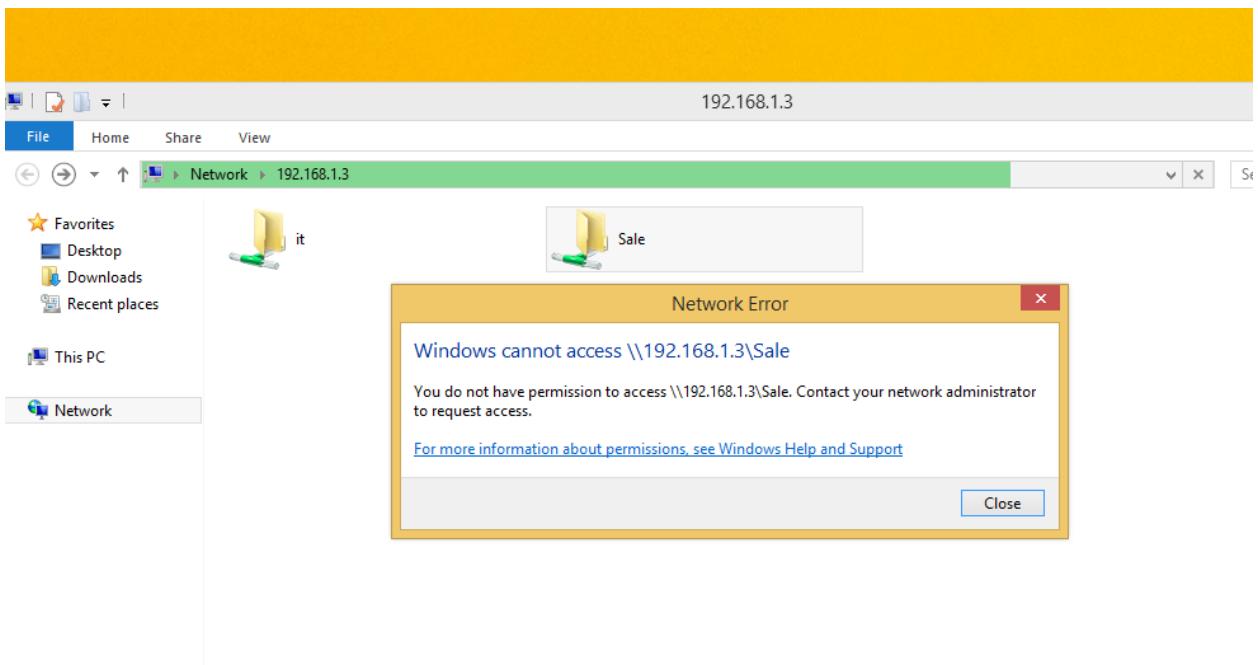
- Truy cập vào địa chỉ của máy *BKAP-SRV12-01* để lấy dữ liệu.



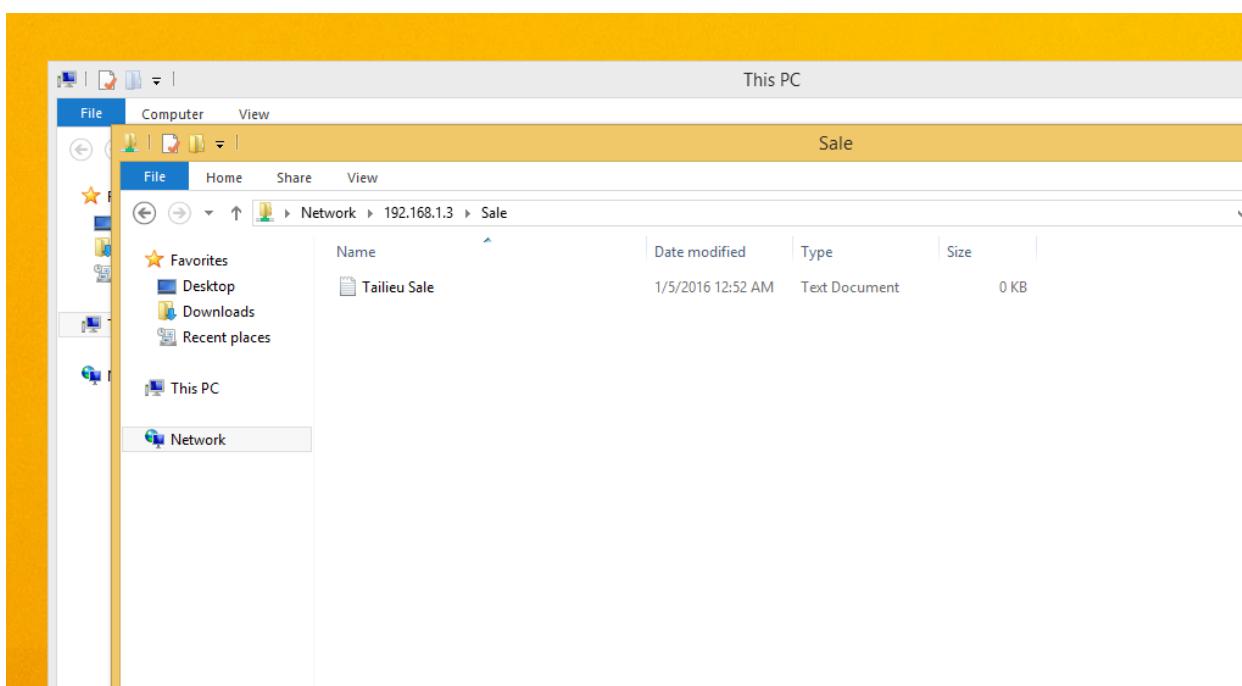
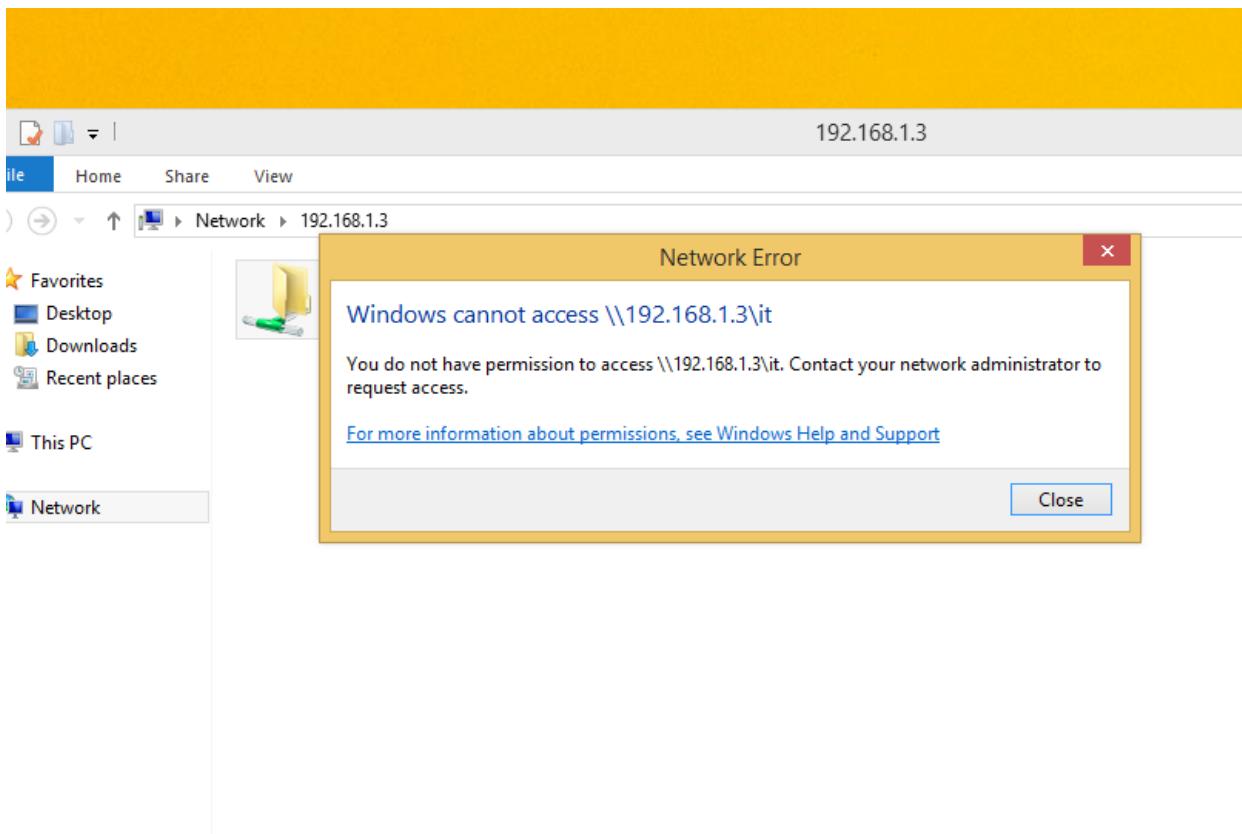
- Tài khoản *hungnq* ở trong phòng ban IT nên truy cập được vào thư mục IT.



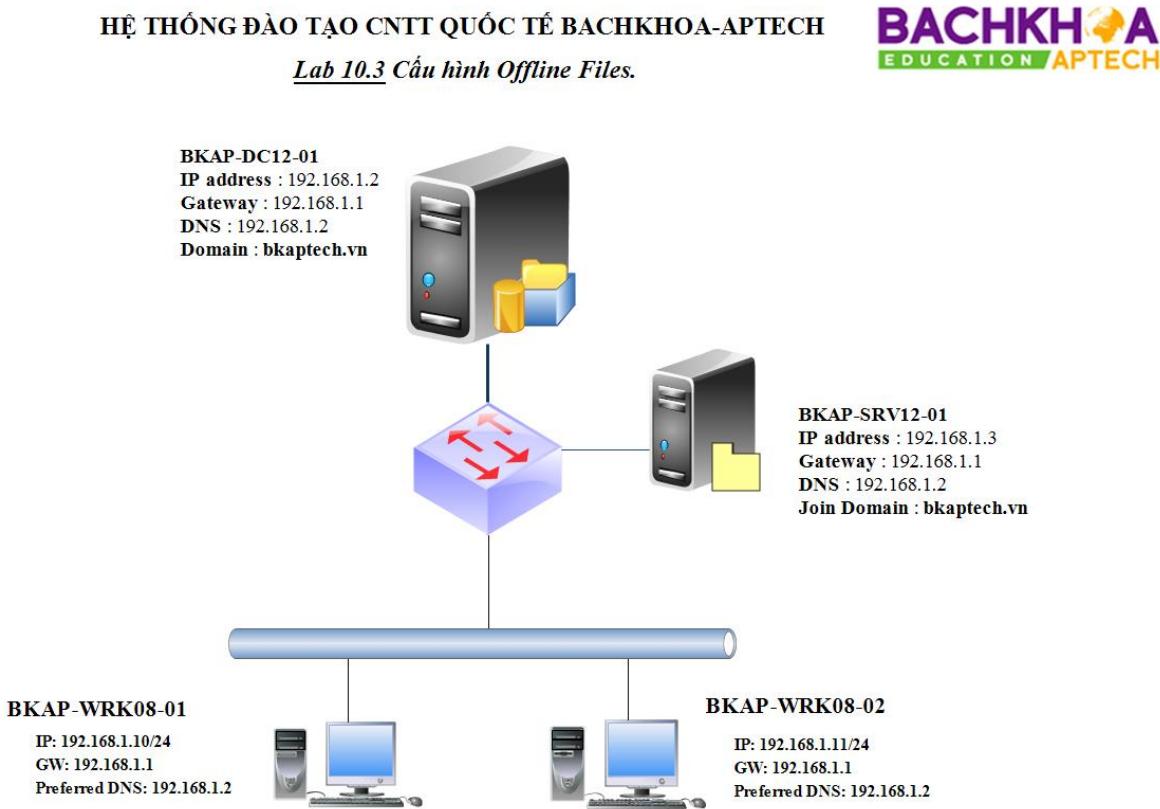
- Tài khoản *hungnq* ko thuộc phòng ban Sale nên ko truy cập được vào thư mục Sale.



- Tương tự, kiểm tra tài khoản *nghialv*.



3. Mô hình Lab:



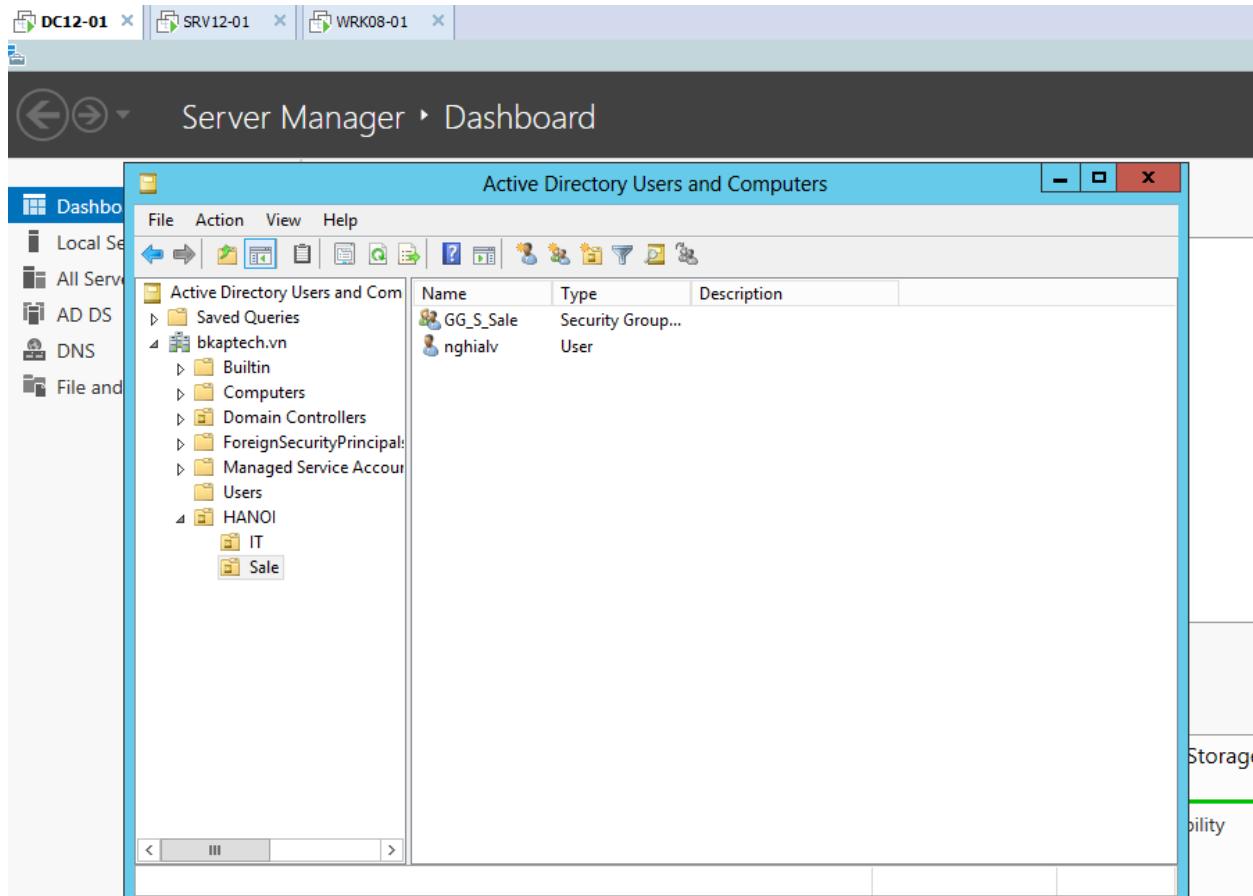
Hình 10.3

Sơ đồ địa chỉ như sau:

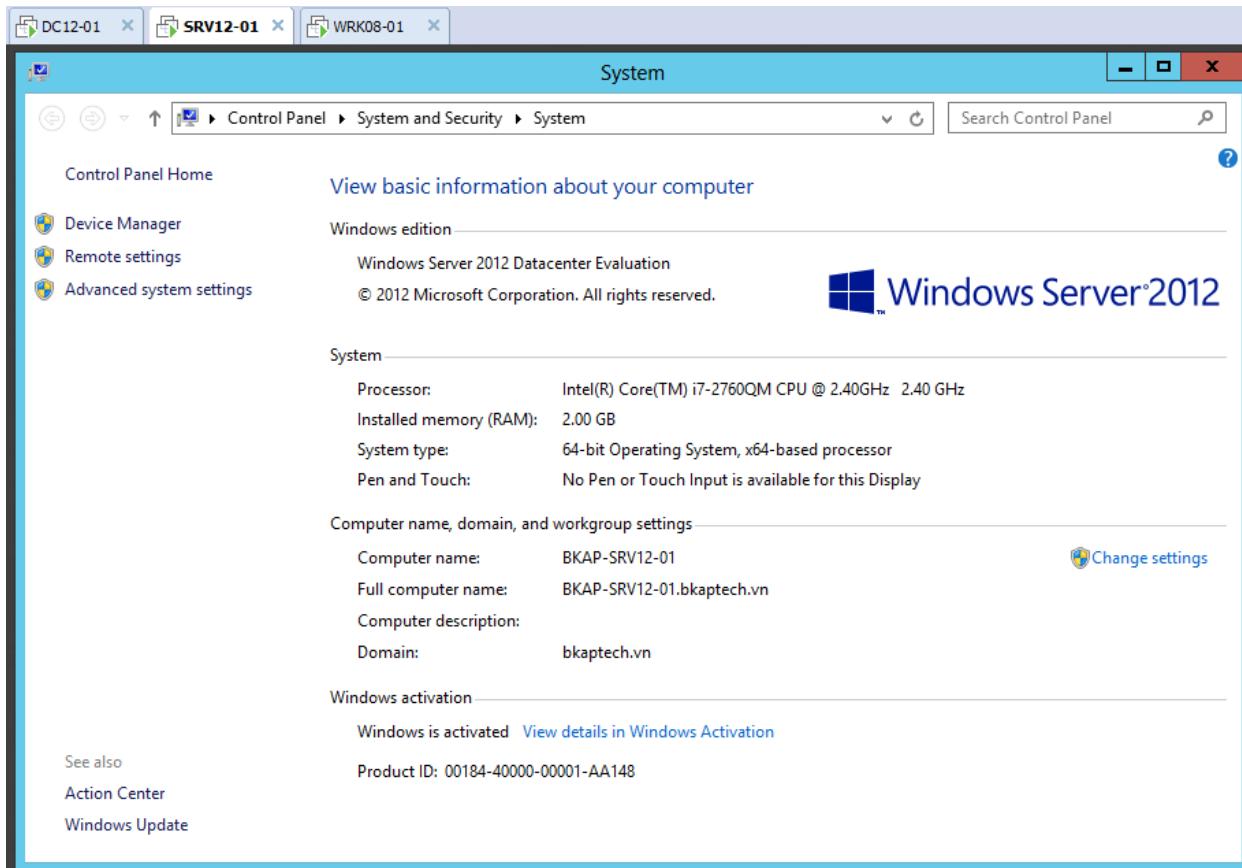
Thông số	BKAP-DC12-01	BKAP-SRV12-01	BKAP-WRK08-01
IP address	192.168.1.2	192.168.1.3	192.168.1.10
Subnet Mask	255.255.255.0	255.255.255.0	255.255.255.0
Gateway	192.168.1.1	192.168.1.1	192.168.1.1
Preferred DNS Server	192.168.1.2	192.168.1.2	192.168.1.2

Hướng dẫn chi tiết:

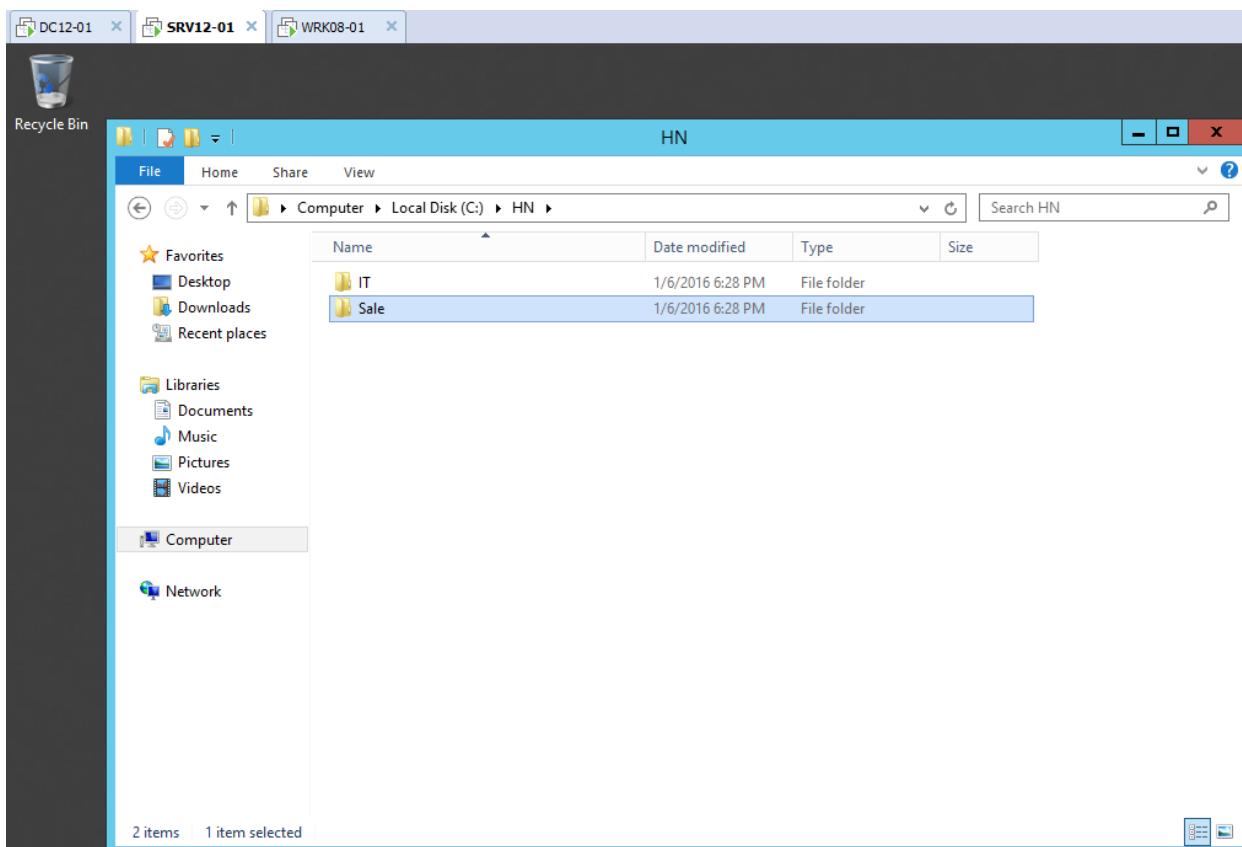
- Trên máy *BKAP-DC12-01*, thực hiện tạo OU, Group, User. Add User vào Group.



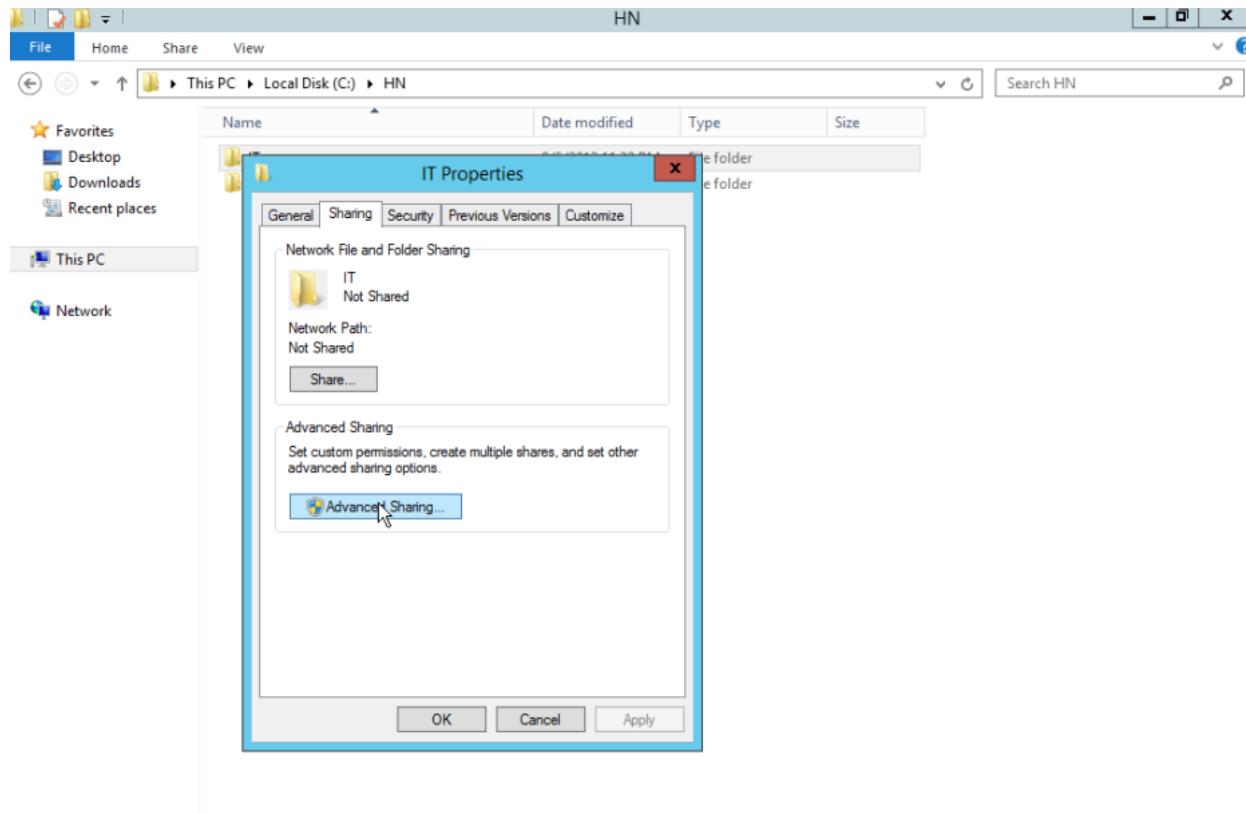
- Chuyển sang máy *BKAP-SRV12-01*, Join vào Domain, đăng nhập bằng tài khoản Administrator của miền.



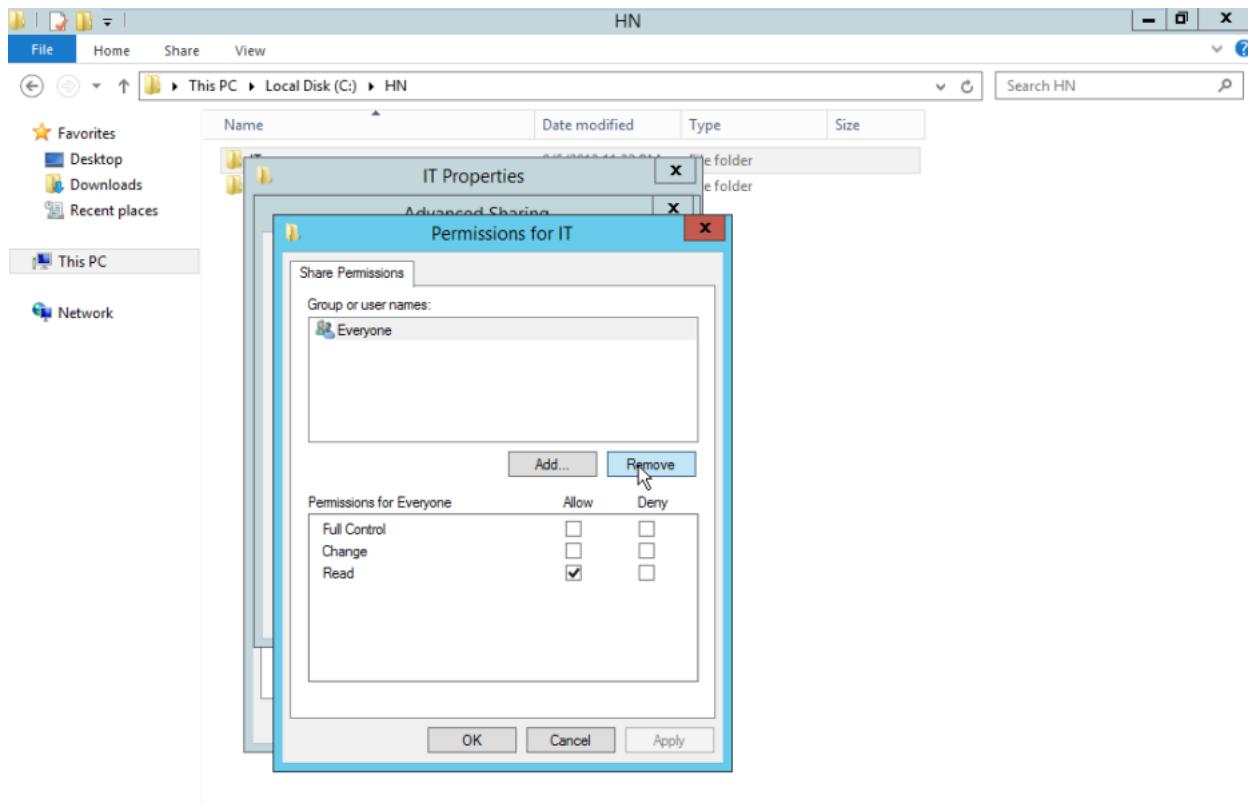
- Tạo thư mục chia sẻ và cấu hình Offline cho phòng ban IT.
 - Vào ổ C, tạo thư mục **HN** , trong thư mục **HN**, tạo 2 thư mục con là **IT** và **Sale**.

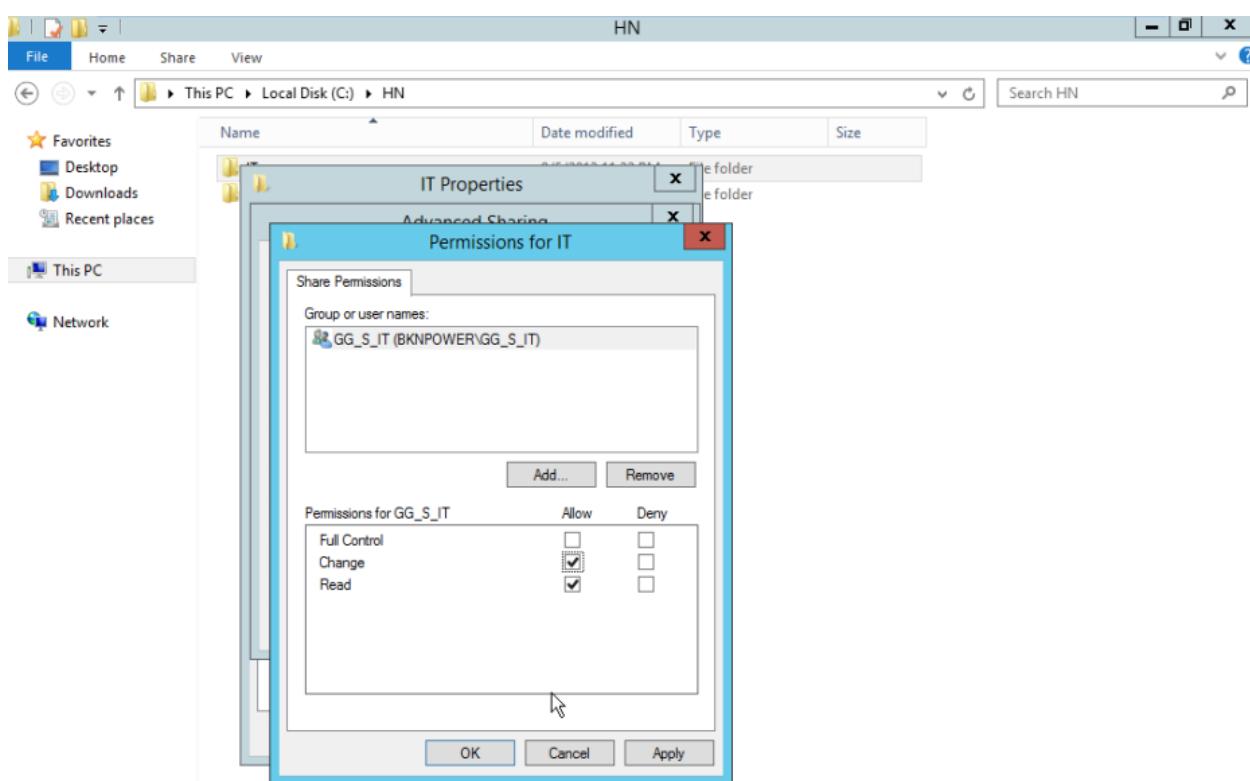


- Click chuột phải vào thư mục IT. Chọn Properties, tại cửa sổ IT Properties, click chọn vào Advanced Sharing...
 - Tại cửa sổ Advanced Sharing, click chuột vào Permissions.

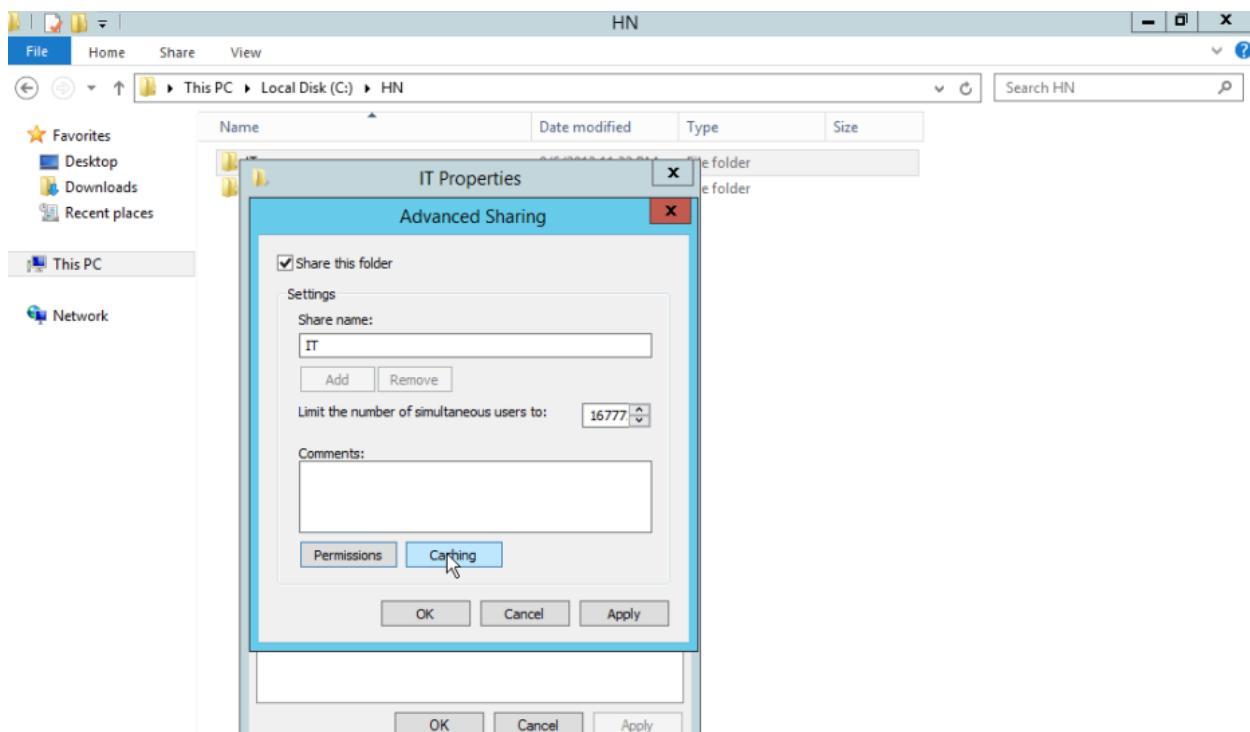


- Tại cửa sổ **Permissions for IT**, thực hiện xóa group **Everyone**, sau đó tiến hành Add vào Group **GG_S_IT**(*GG_S_IT có quyền Change và Read*).

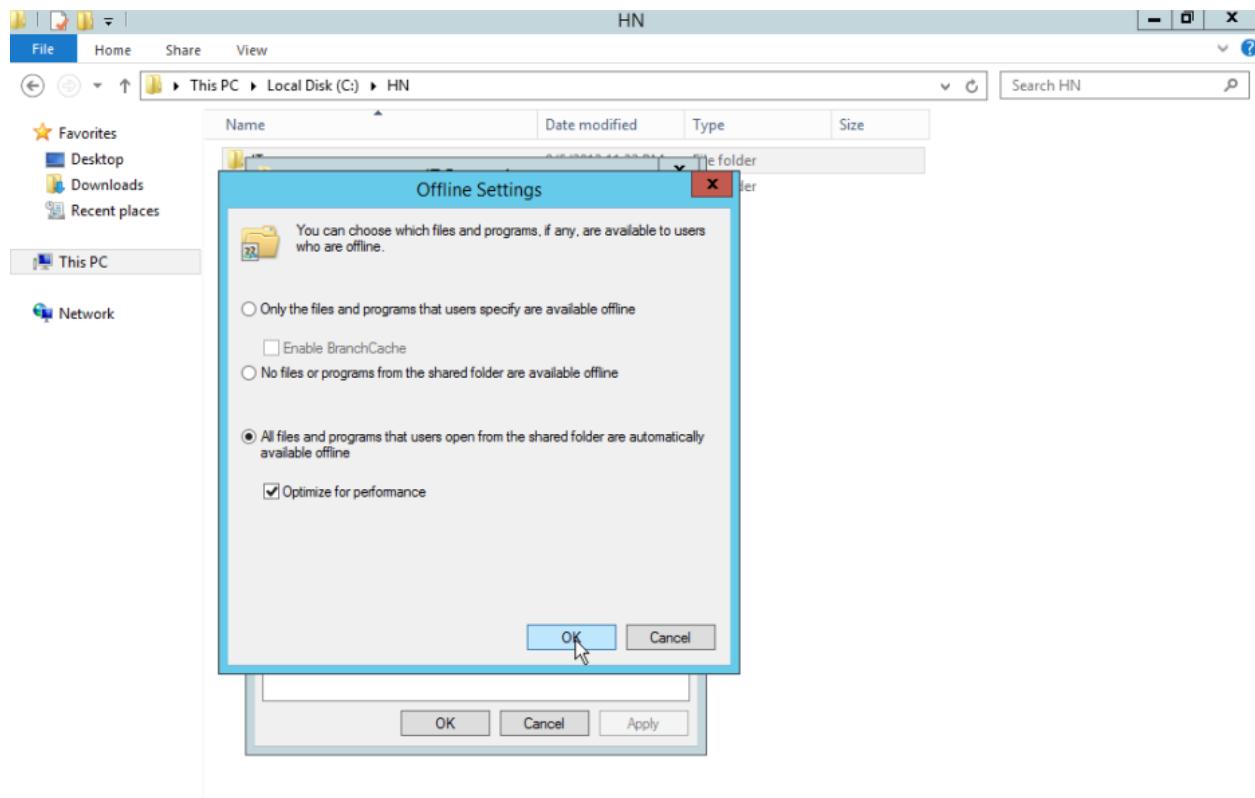




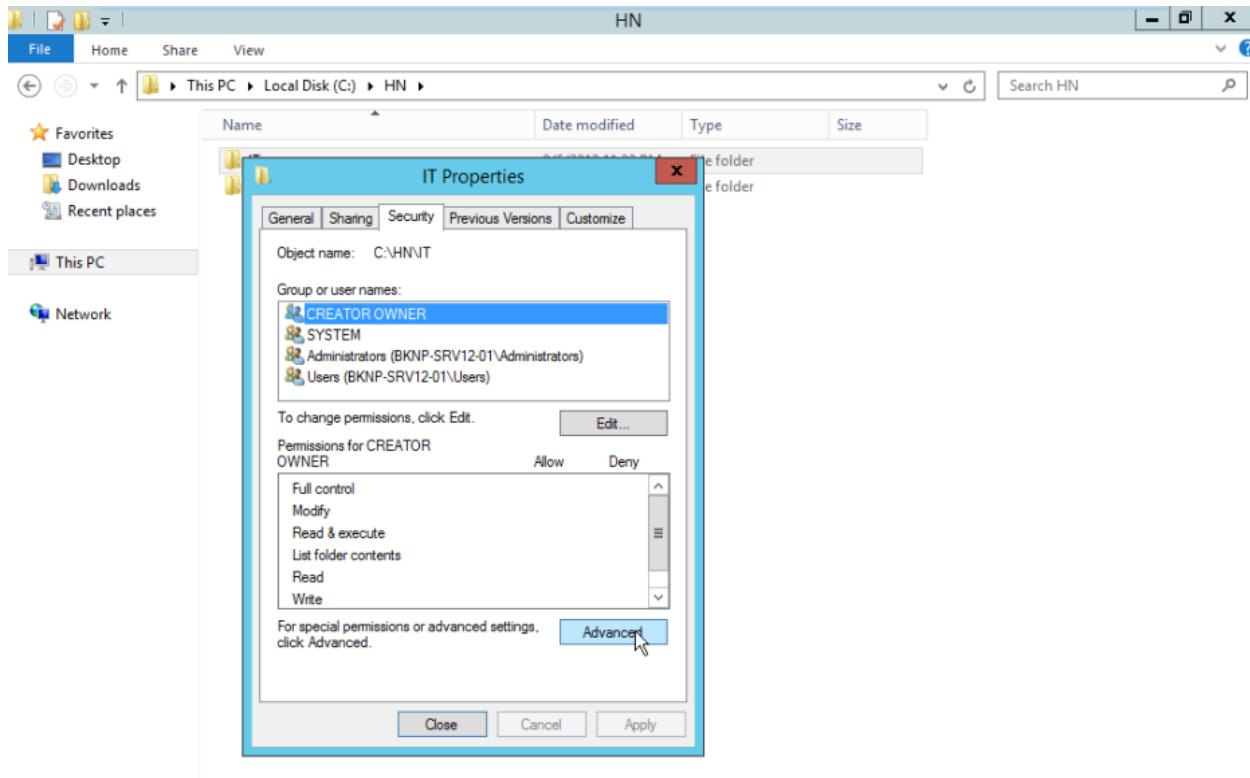
- Cấu hình Offline trên thư mục IT:
 - Tại cửa sổ Advanced Sharing, click chuột vào Caching.



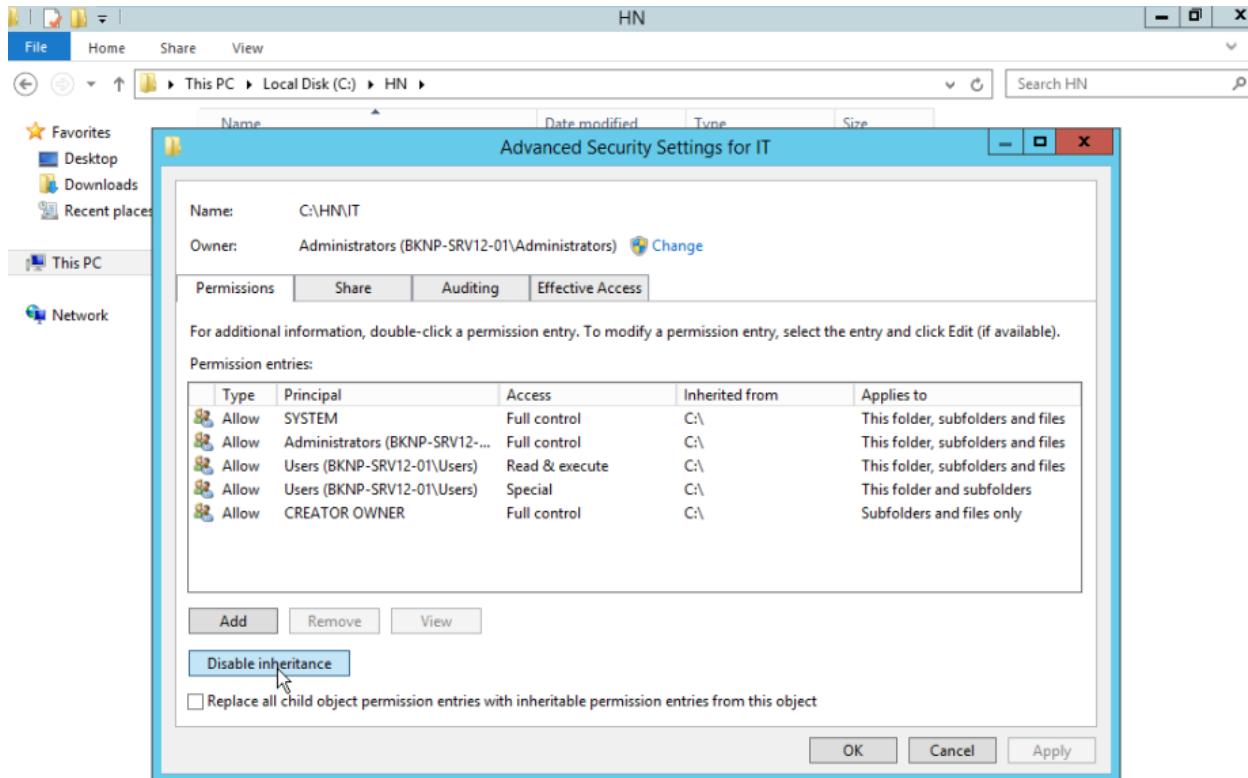
- Tại cửa sổ **Offline Settings**, click chuột vào dòng *Add files and programs that users open from the shared folder are automatically available offline. OK.*



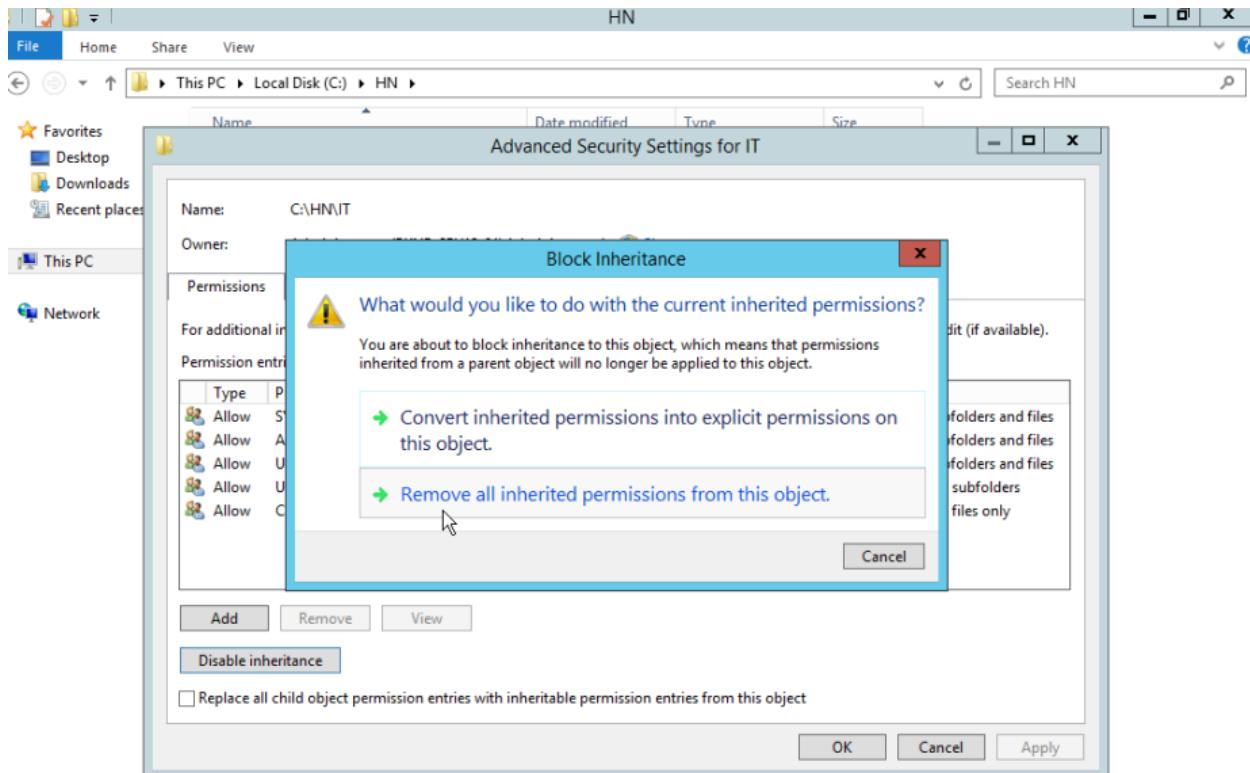
- Tại cửa sổ **IT Properties**, chuyển sang tab **Security** , sau đó click vào **Advanced**.



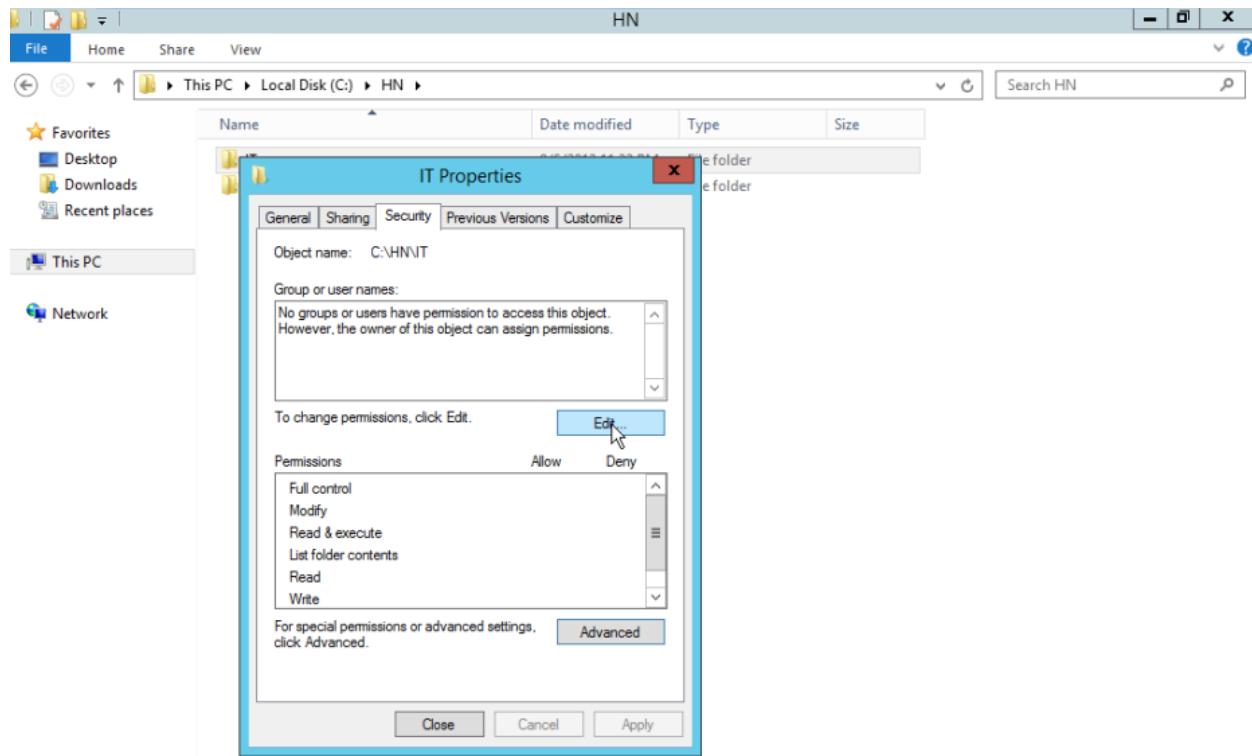
- Tại cửa sổ **Advanced Security Setting for IT**, click vào **Disable inheritance**.



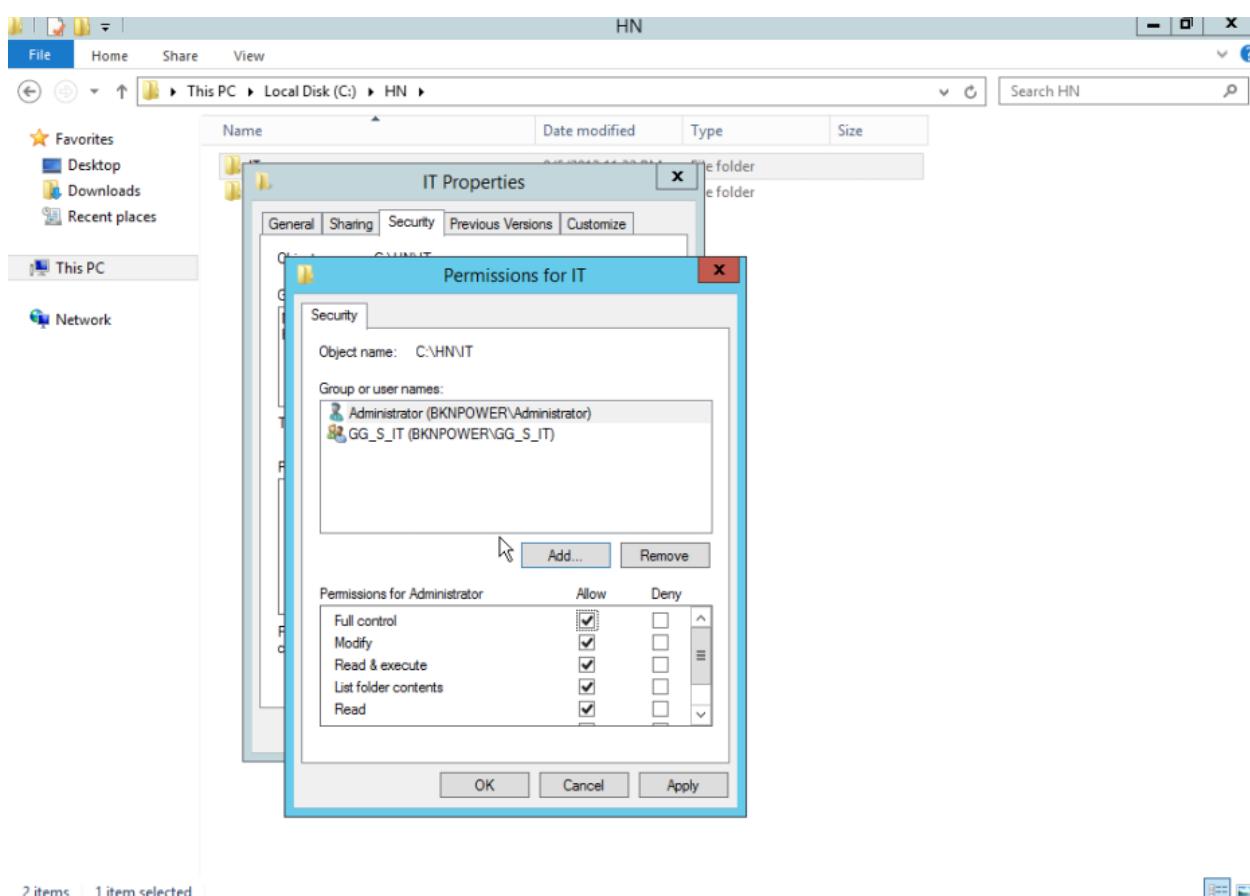
- Tại cửa sổ **Block Inheritance**, click chọn vào dòng **Remove all inherited permissions from this object. OK.**



- Tại cửa sổ **IT Properties / Tab Security**. Click vào **Edit**.

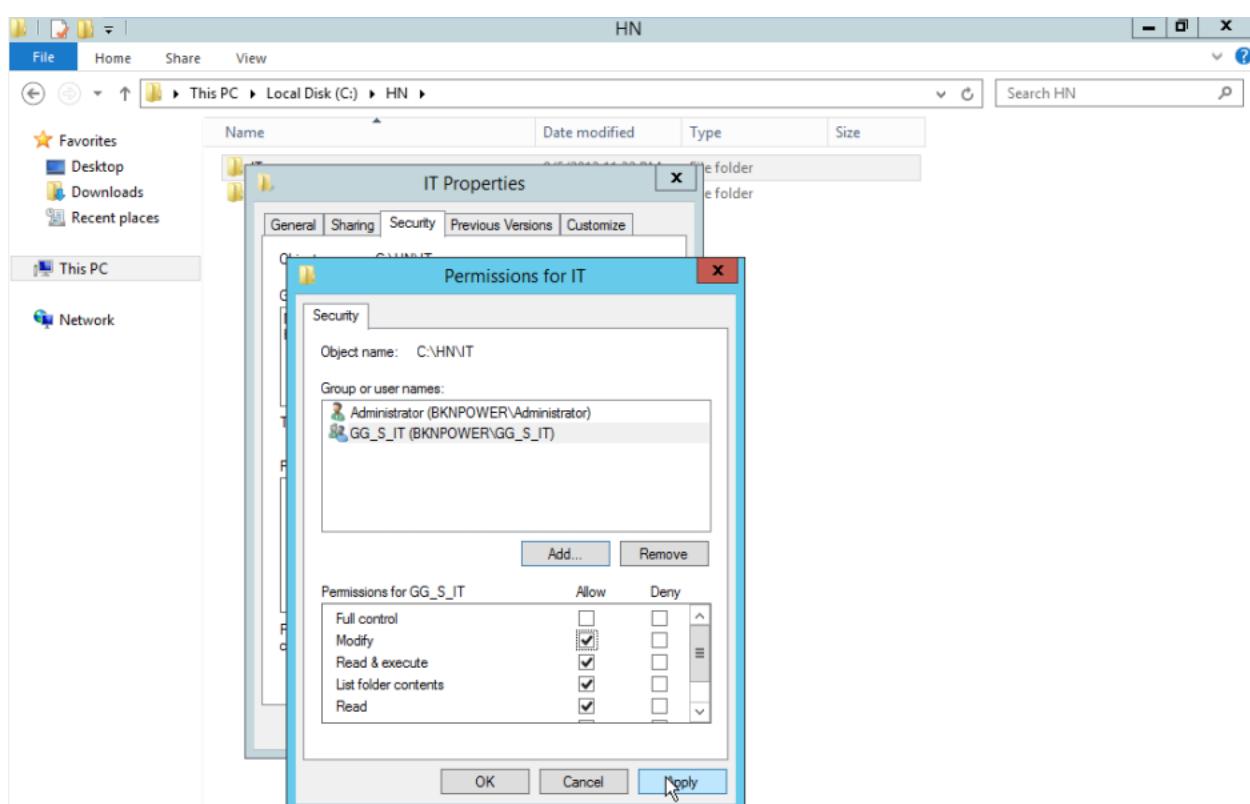


- Tại cửa sổ **Permissions for IT**, click vào **Add**, tiến hành add User **Administrator** và Group **GG_S_IT** vào khung **Group or user names**. Phân quyền như sau:
 - **Administrator** : *Full control*
 - **GG_S_IT** : *Modify*

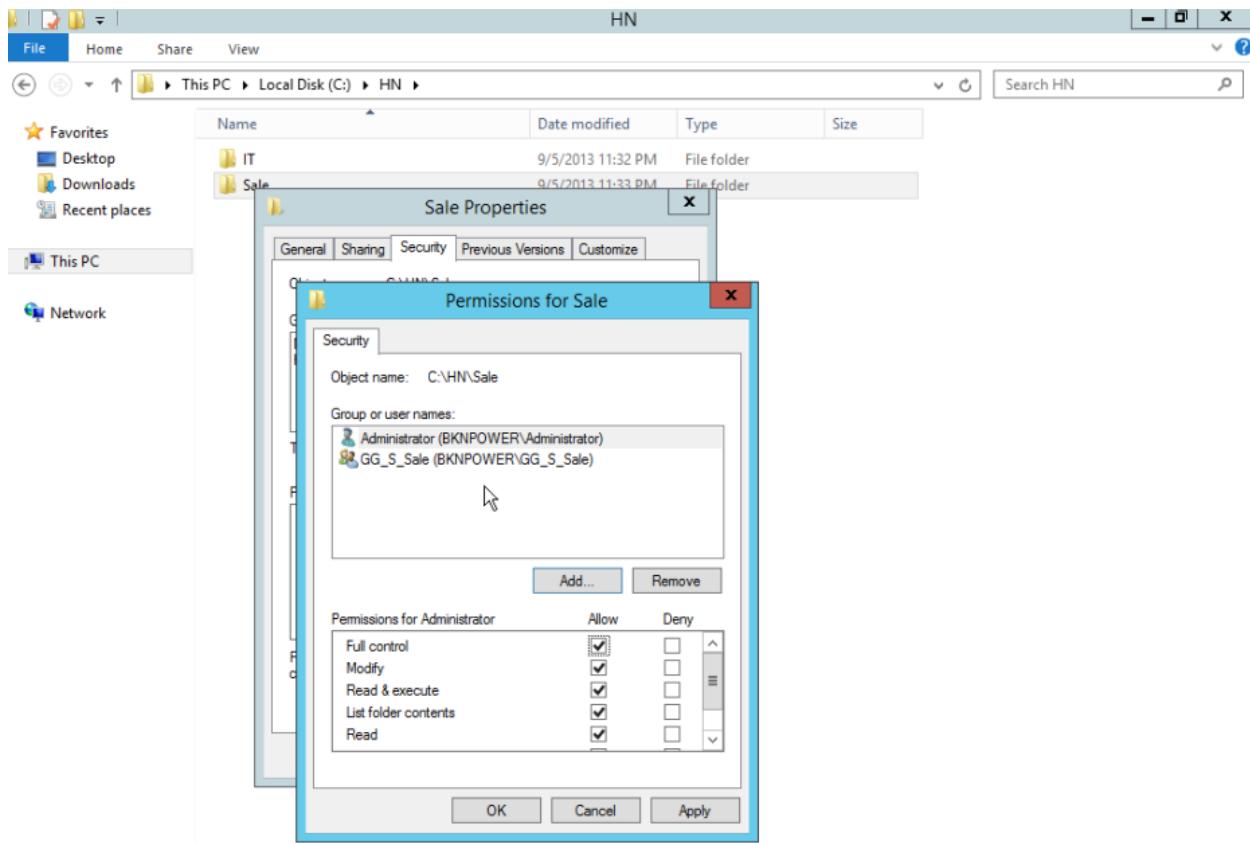


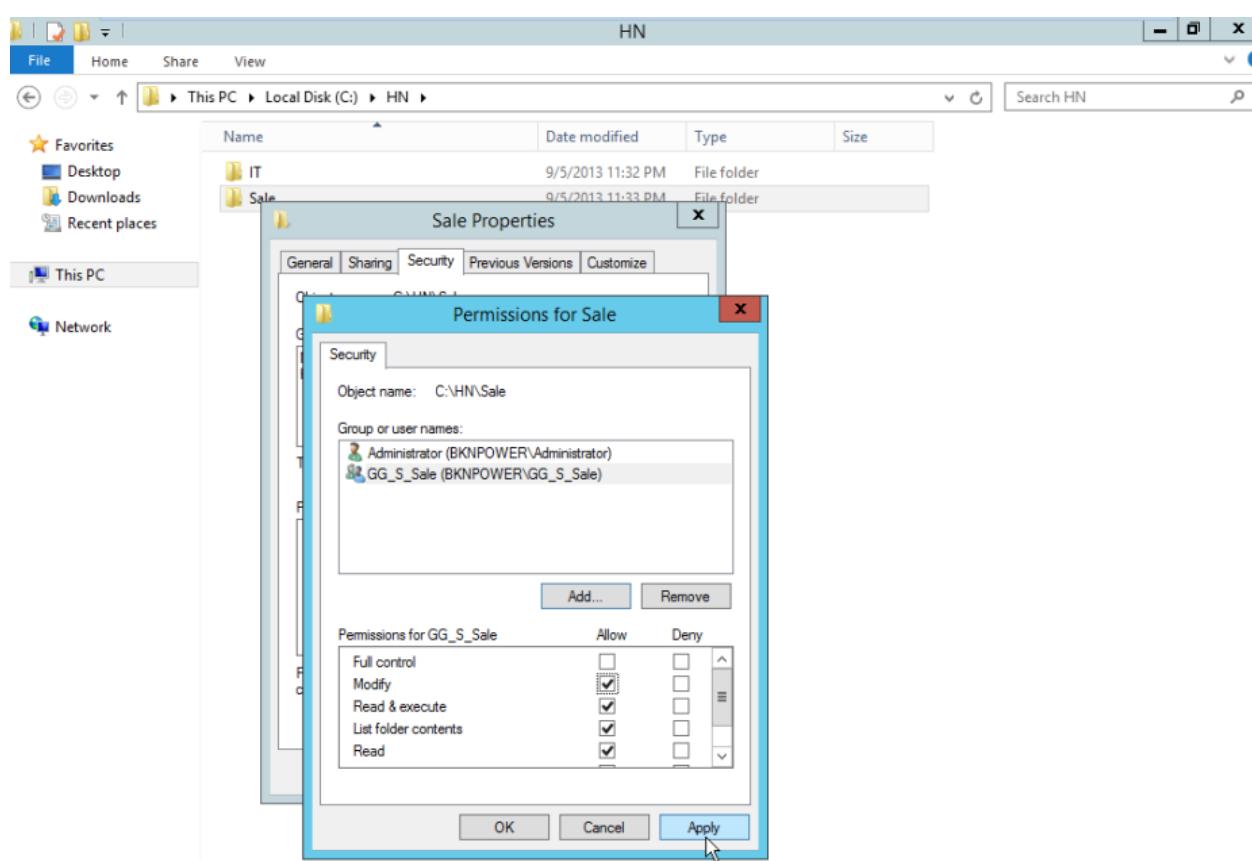
2 items 1 item selected



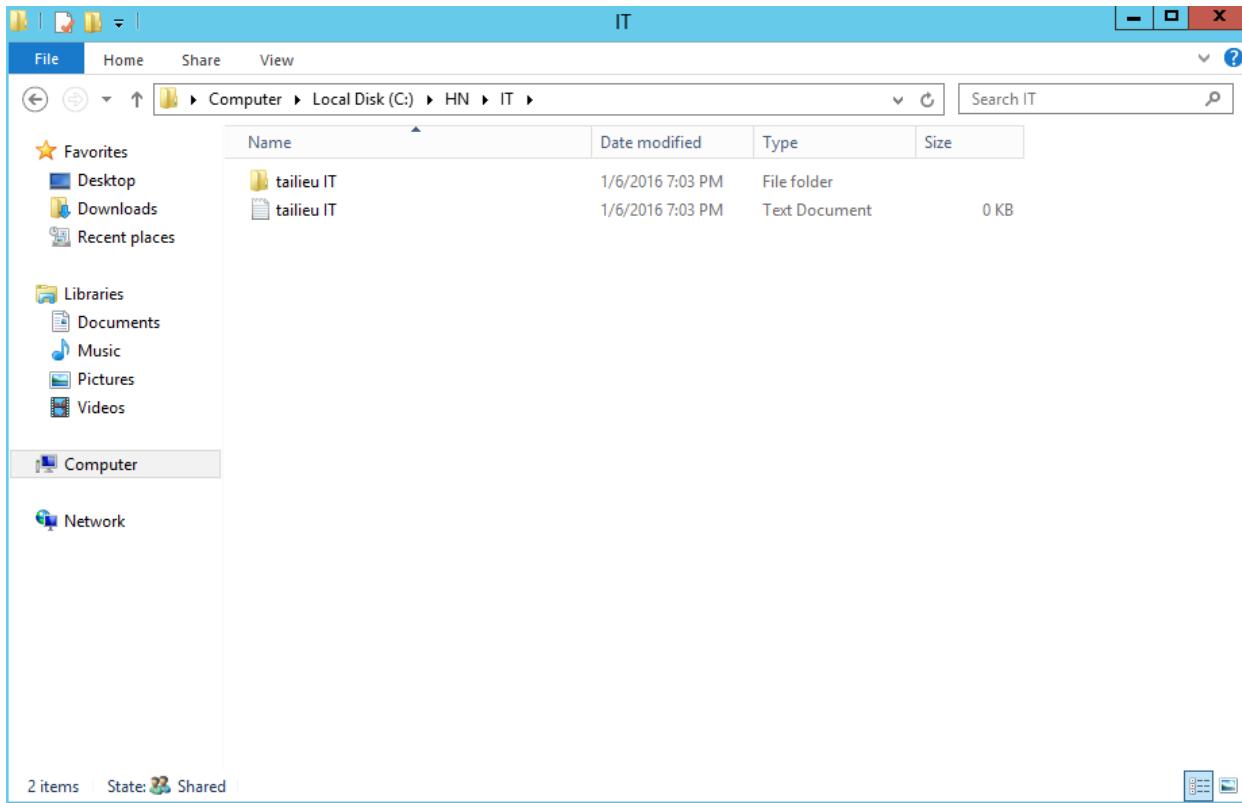


- Thư mục Sale tiến hành Share bình thường, ko cấu hình Offline file.

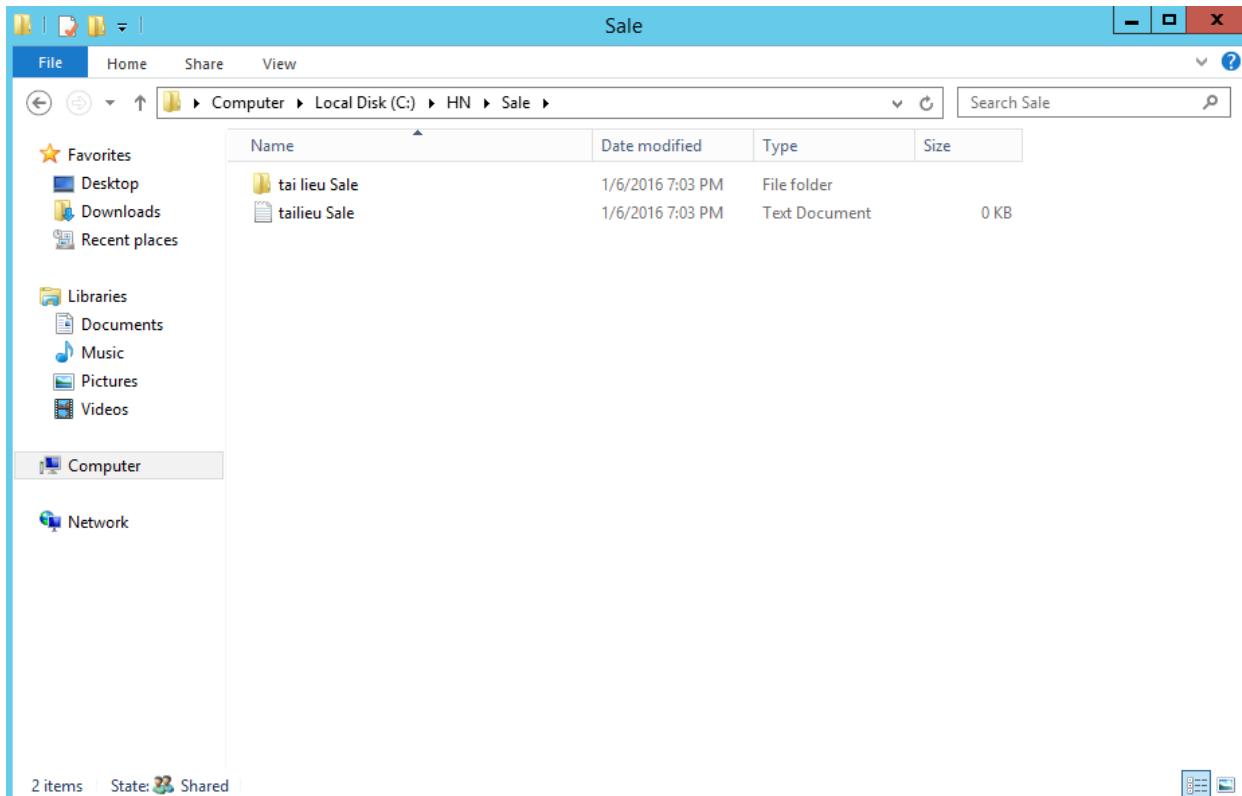




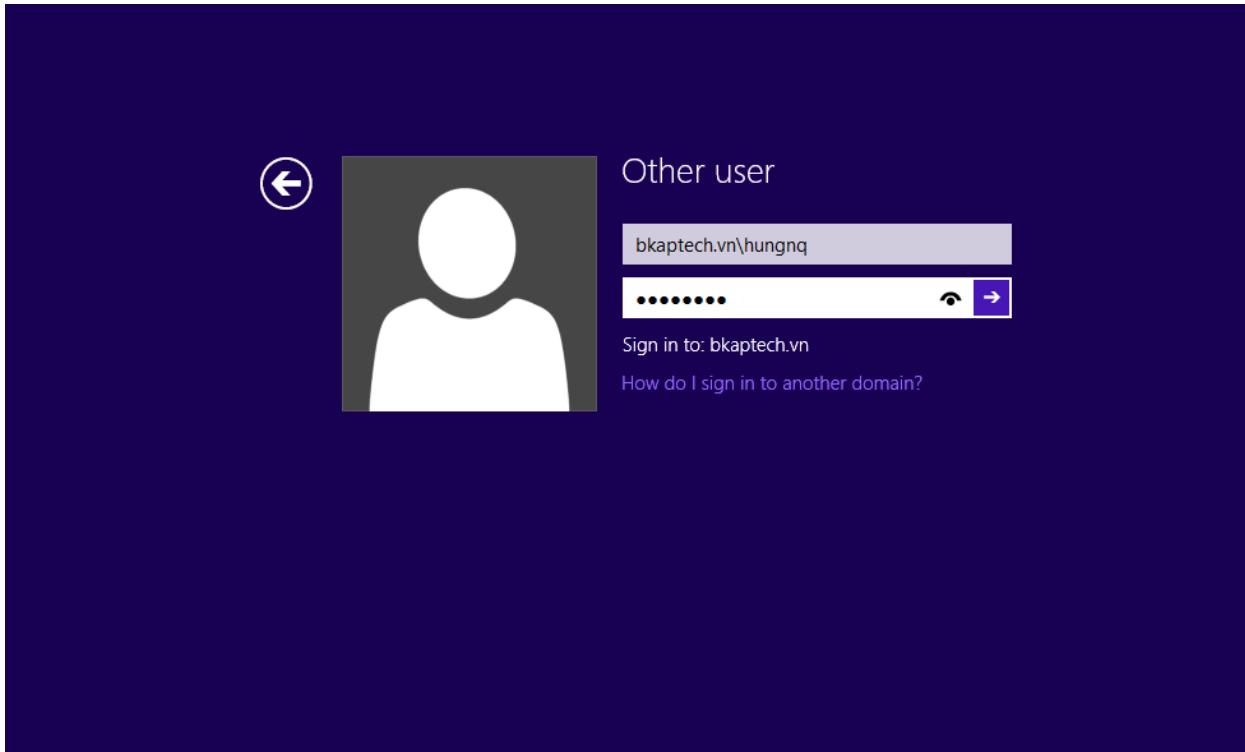
- Trong folder IT tạo các tài liệu IT



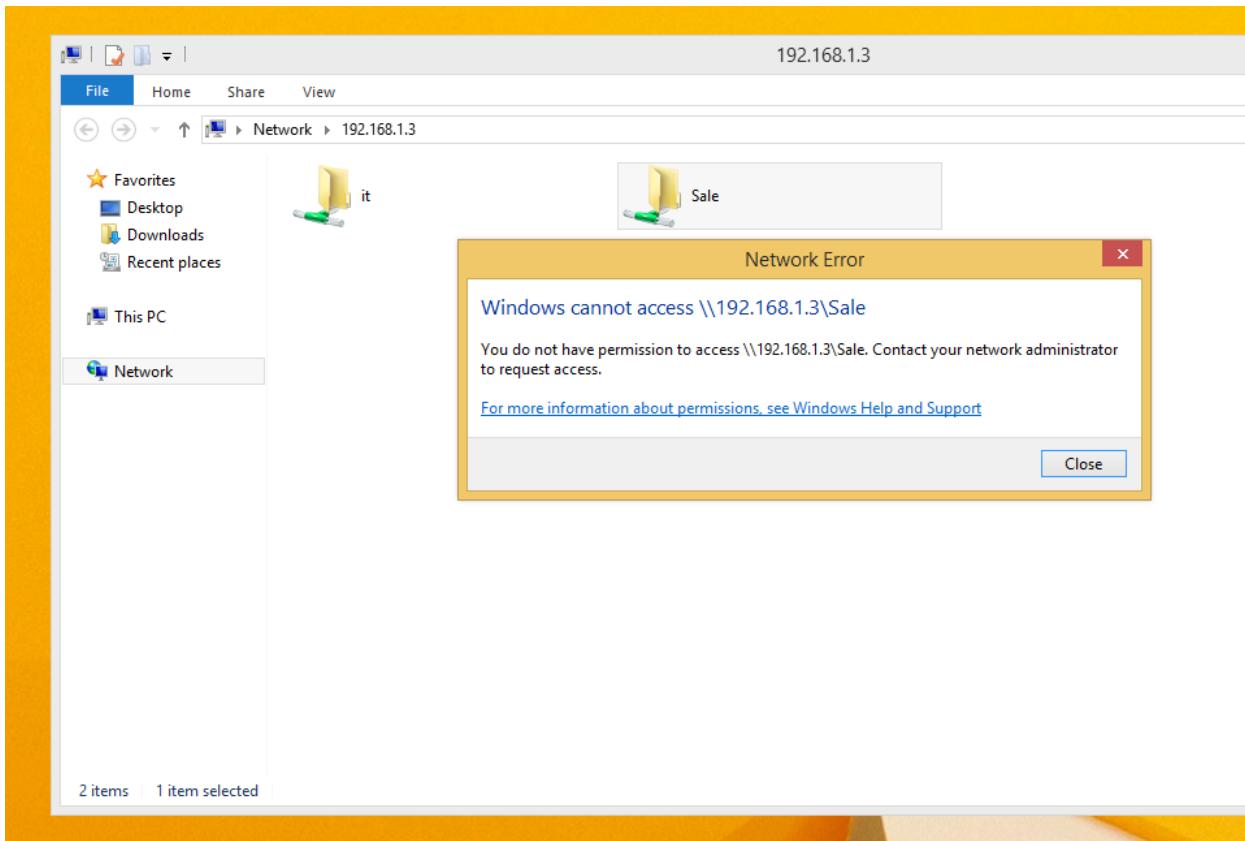
- Trong folder Sale tạo các tài liệu Sale :



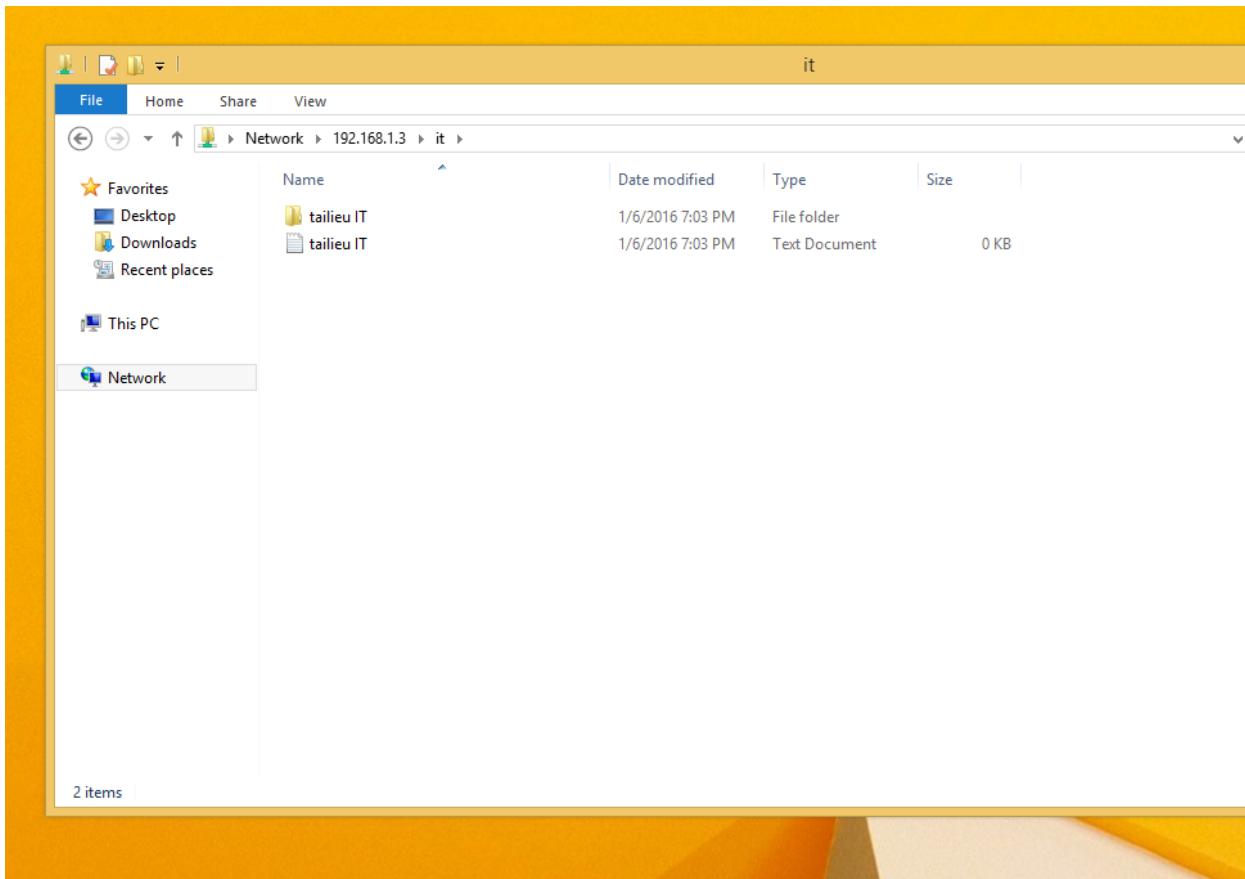
- Chuyển sang máy Client Win 8 thực hiện *Join vào domain* để kiểm tra.
 - Đăng nhập bằng User **hungnq** trong phòng ban IT.



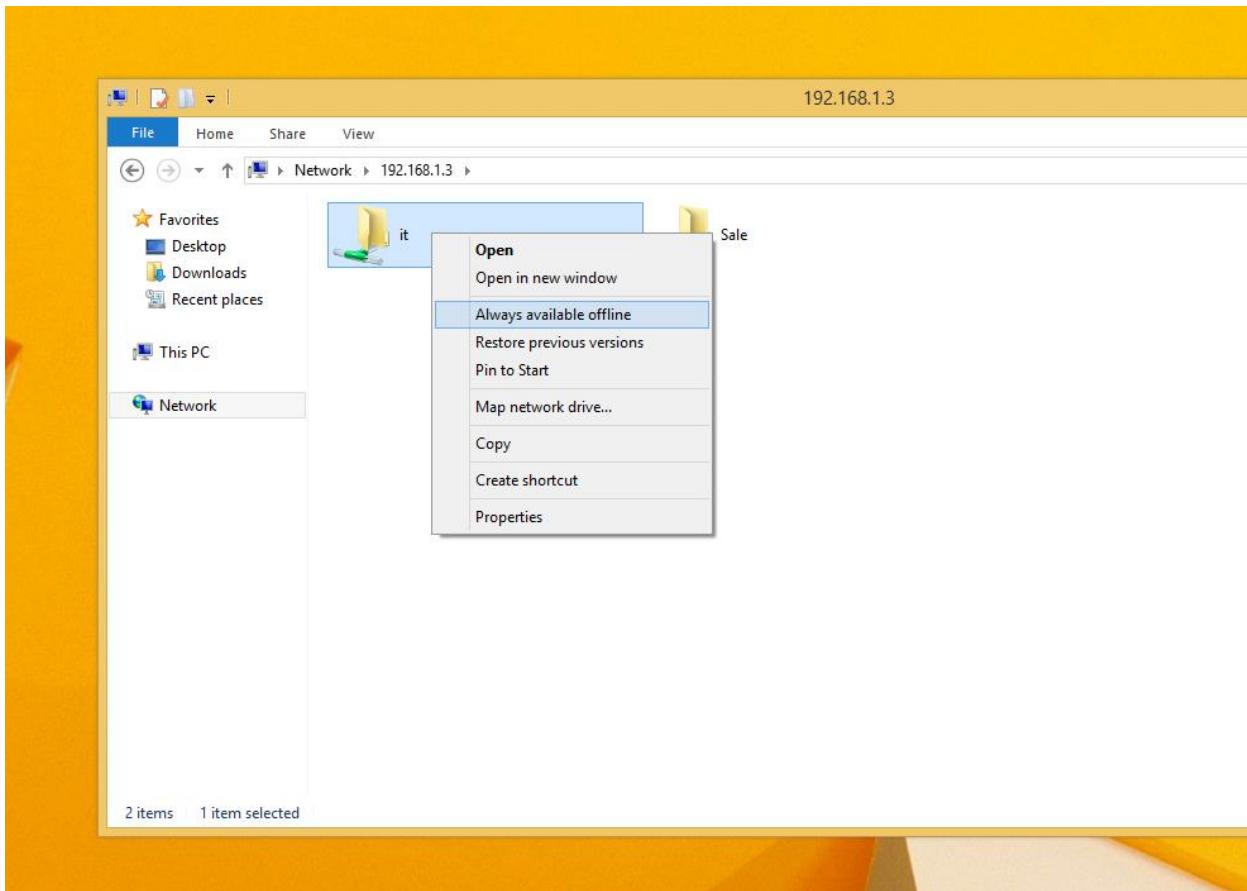
- User **hungnq** không thuộc phòng ban **Sale** nên ko truy cập được vào thư mục **Sale**.



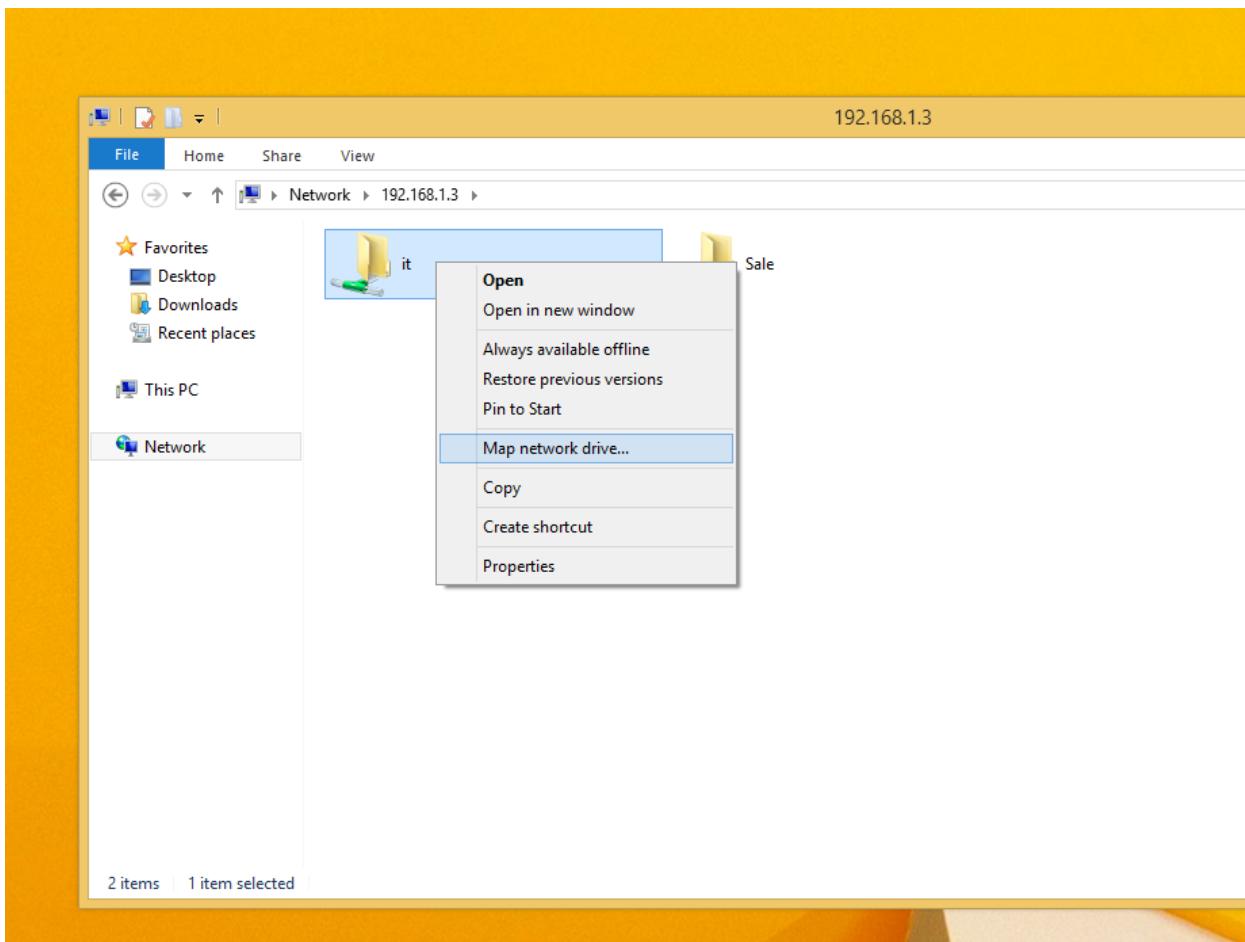
- User **hungnq** thuộc phòng ban **IT** nên được phép truy cập vào thư mục **IT**.

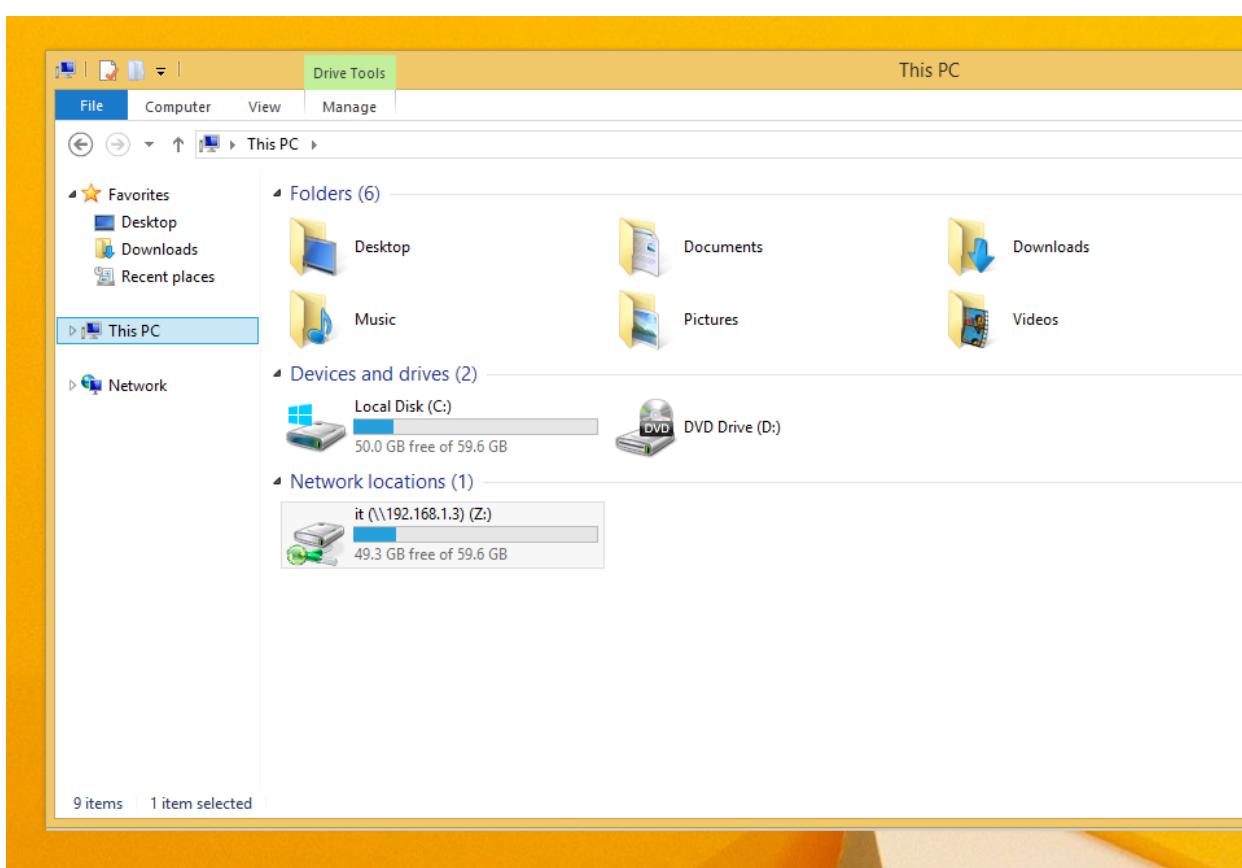


- Cấu hình Offline trên máy Client:
 - Tại cửa sổ Network , click vào thư mục IT đã được share, chọn Always available offline.

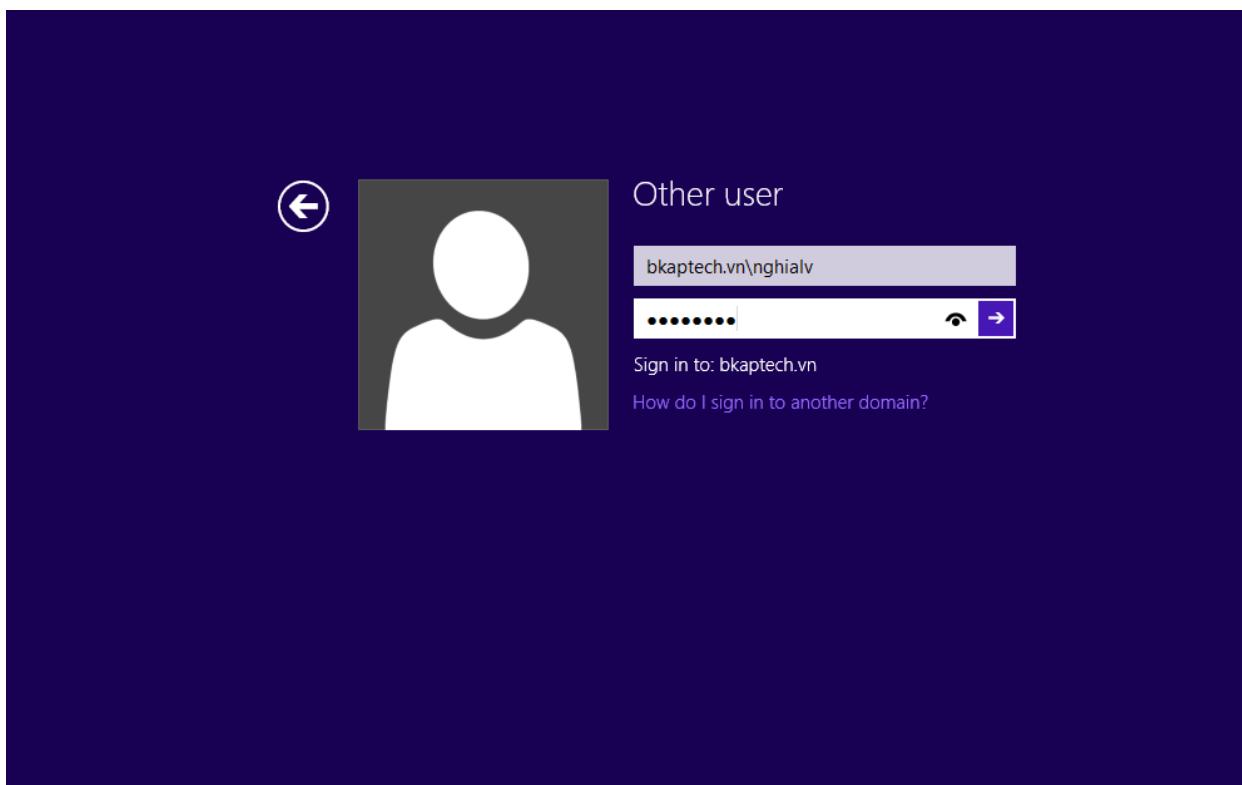


- Tiếp theo click vào Map Network Drive...

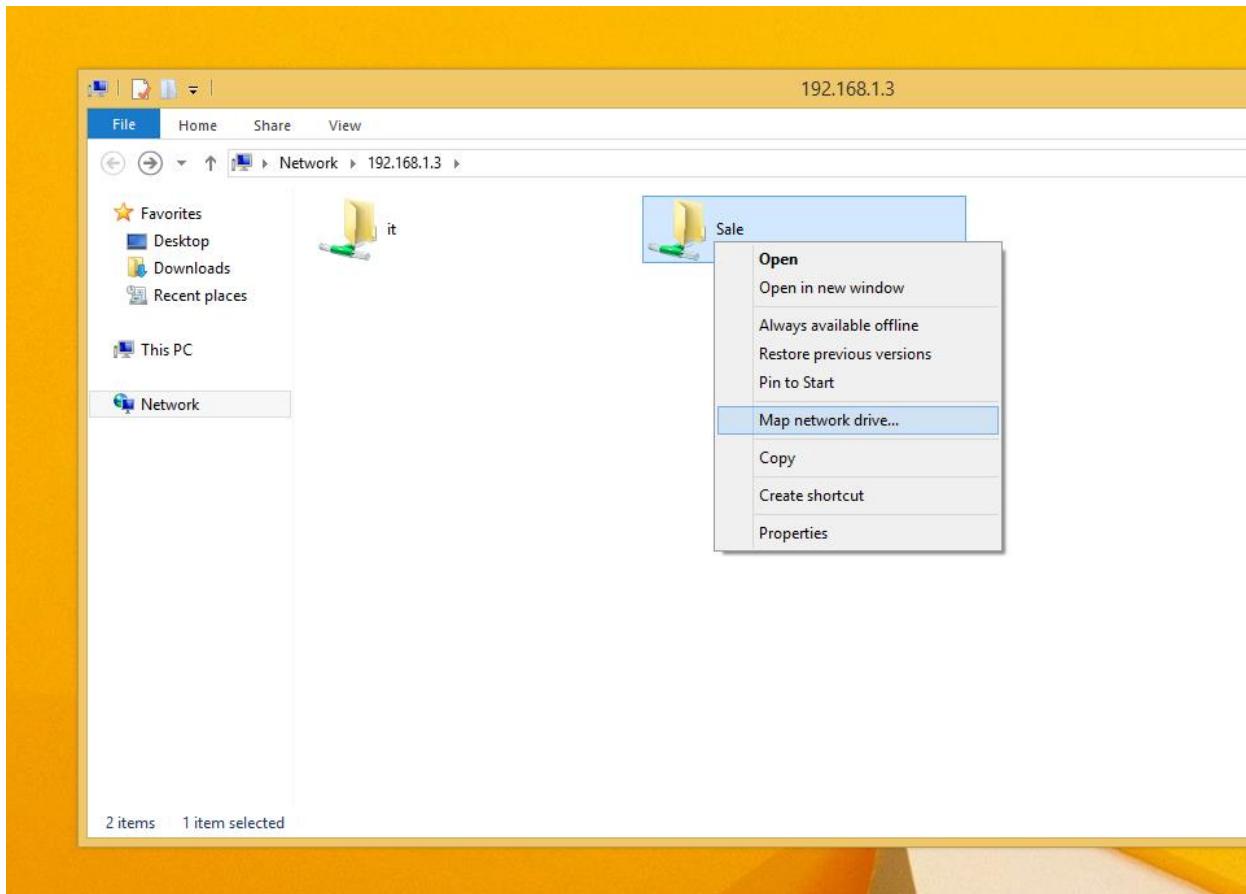


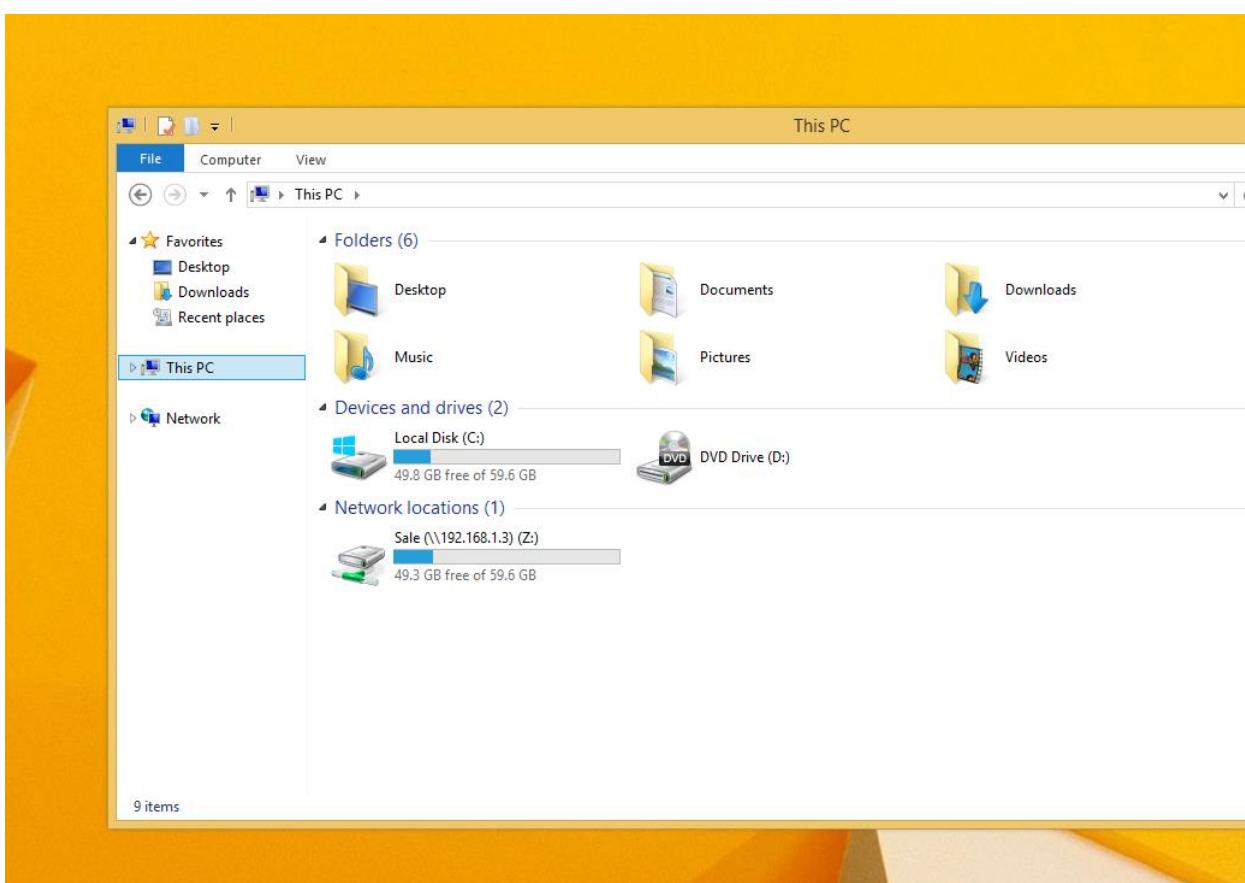


- Logout tài khoản **hungnq**, đăng nhập bằng tài khoản **nghialv**.

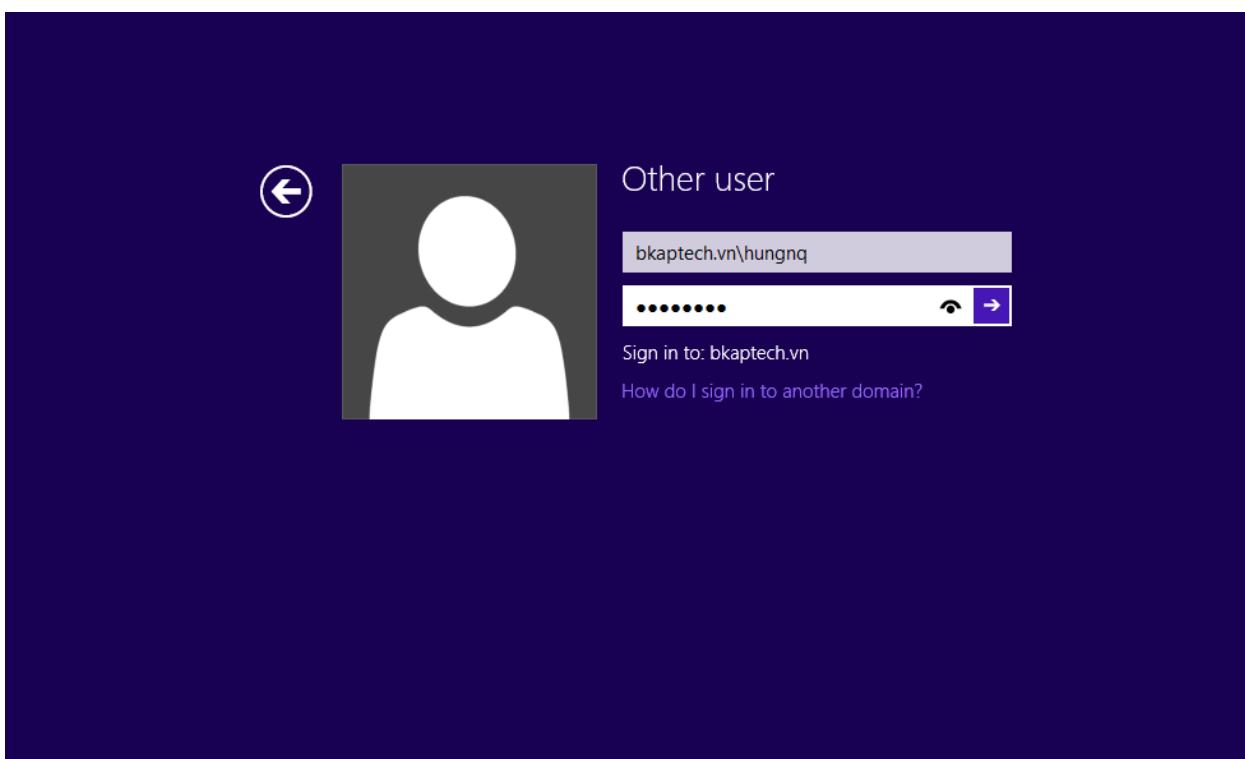


- Click vào thư mục Sale đã được share, chọn **Map network Drive...**

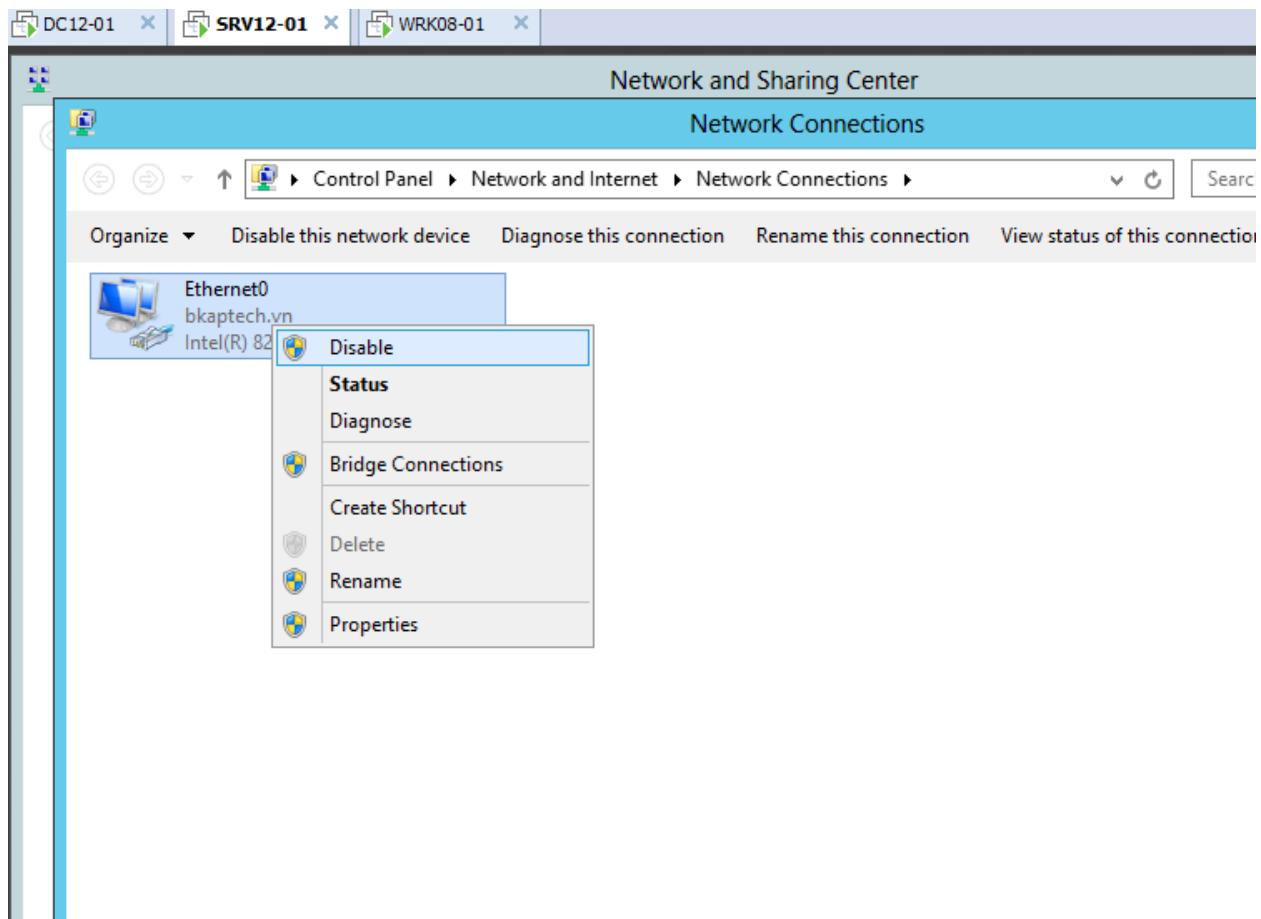




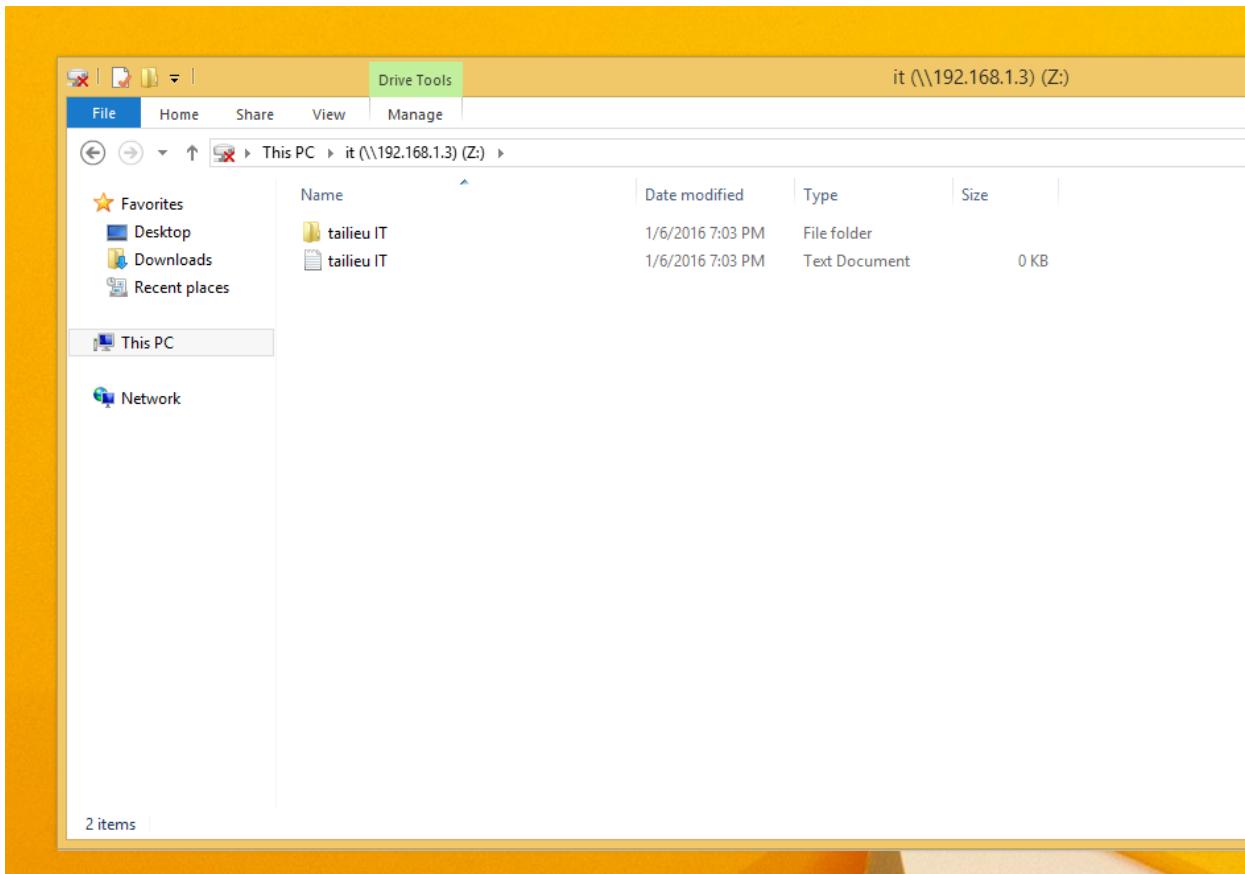
- Đăng nhập lại tài khoản **hungnq**.



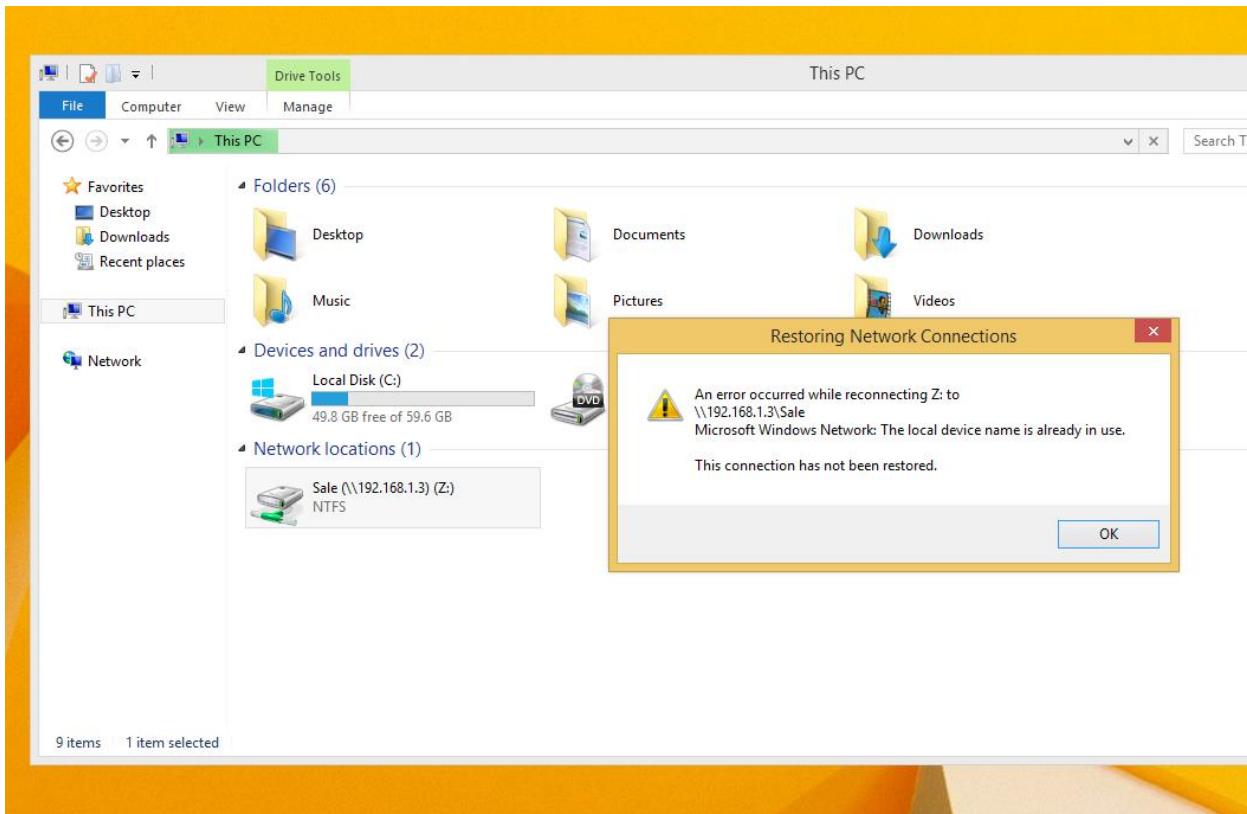
- Chuyển sang máy *BKAP-SRV12-01*, tiến hành tắt card mạng để kiểm tra Offline.



- Chuyển sang máy *Client Win 8*, tiến hành kiểm tra.
 - Đăng nhập bằng tài khoản **hungnq** đã cấu hình **offline file** , truy cập vào ổ đĩa **Z** thành công.



- Kiểm tra truy cập thư mục **Sale** bằng tài khoản **nghialv**, ko truy cập được thư mục, do tài khoản này ko được cấu hình **offline file**.



Bài 11.**TRIỂN KHAI CHÍNH SÁCH GROUP POLICY.**

Các nội dung chính sẽ được đề cập:

- ✓ Triển khai chính sách GPO cơ bản.
- ✓ Giám sát tệp tin và bắt xóa file.
- ✓ Triển khai chính sách giới hạn phần mềm.

11.1 Triển khai chính sách GPO cơ bản.

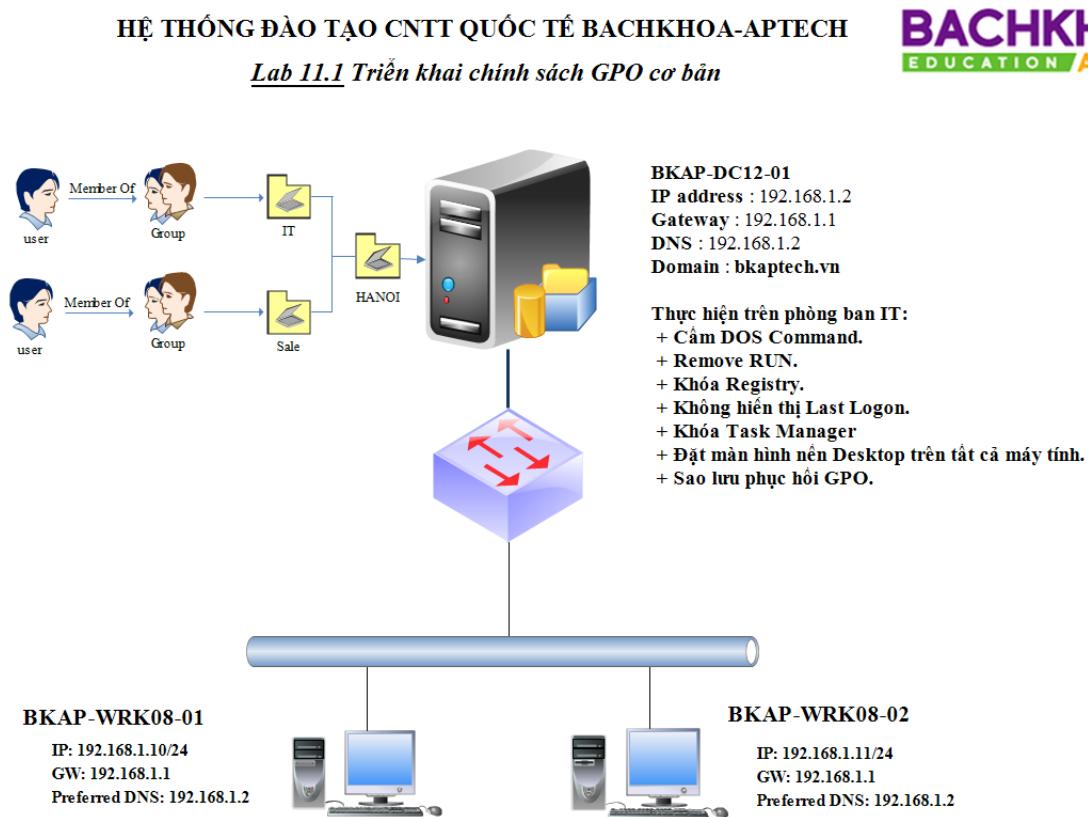
1. Yêu cầu bài lab: triển khai chính sách trên Domain:

- + Đặt màn hình nền Desktop tất cả các máy tính.
- + Khóa Registry.
- + Không hiển thị Last Logon.
- + Khóa Task Manager.
- + Cấm DOS Command.
- + Remove RUN.
- + Sao lưu phục hồi Group Policy.

2. Yêu cầu chuẩn bị:

- + Một máy *Server Windows Server 2012 Datacenter* đã nâng cấp lên Domain Controller :**bkaptech.vn**.
- + Tạo các OU tương ứng.
- + Triển khai các chính sách trên phòng ban IT.
- + Kiểm tra các chính sách khi áp dụng cho phòng ban IT bằng cách đăng nhập tài khoản thuộc phòng ban IT trên máy *BKAP-WRK08-01*.

3. Mô hình Lab:



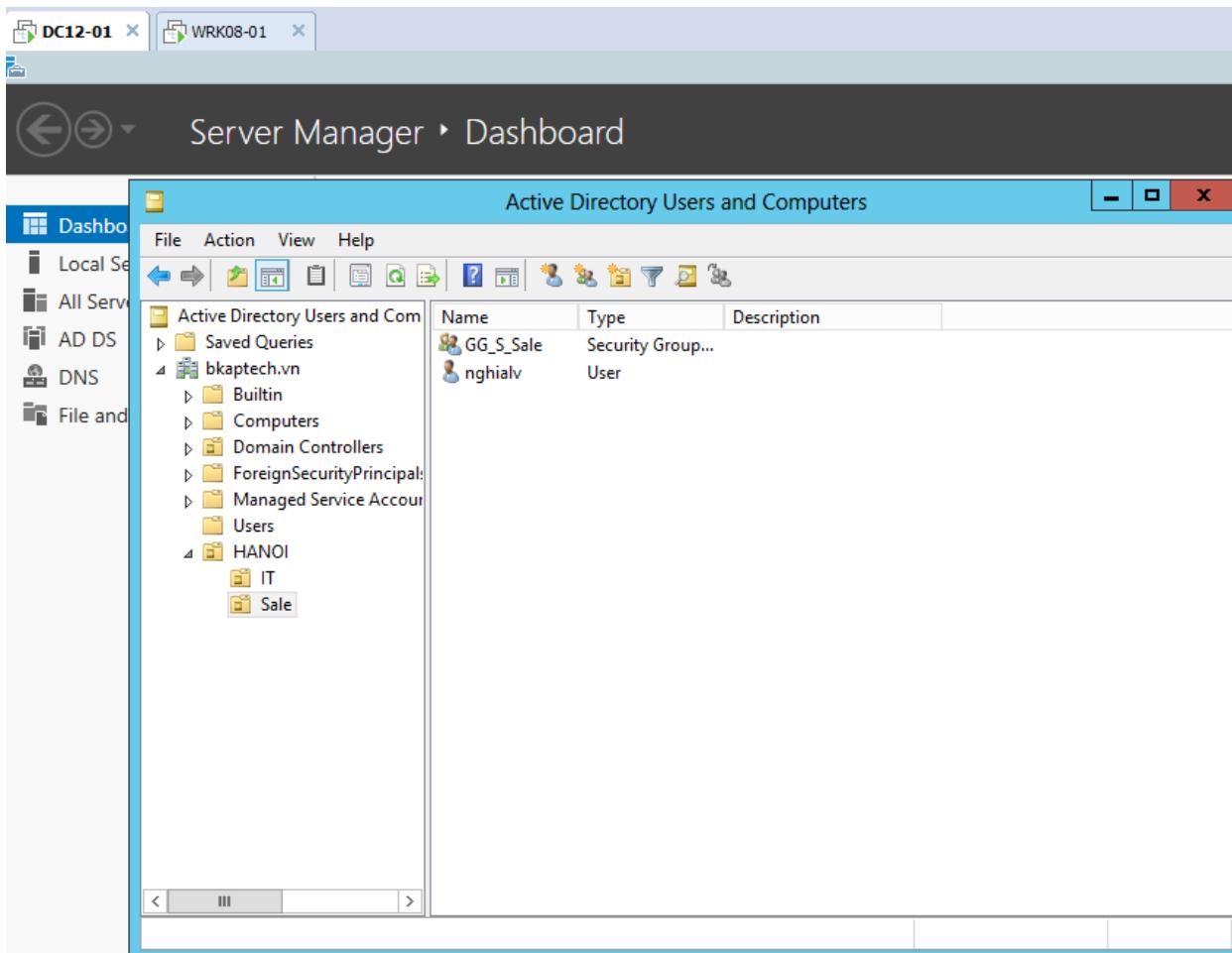
Hình 11.1

Sơ đồ địa chỉ như sau:

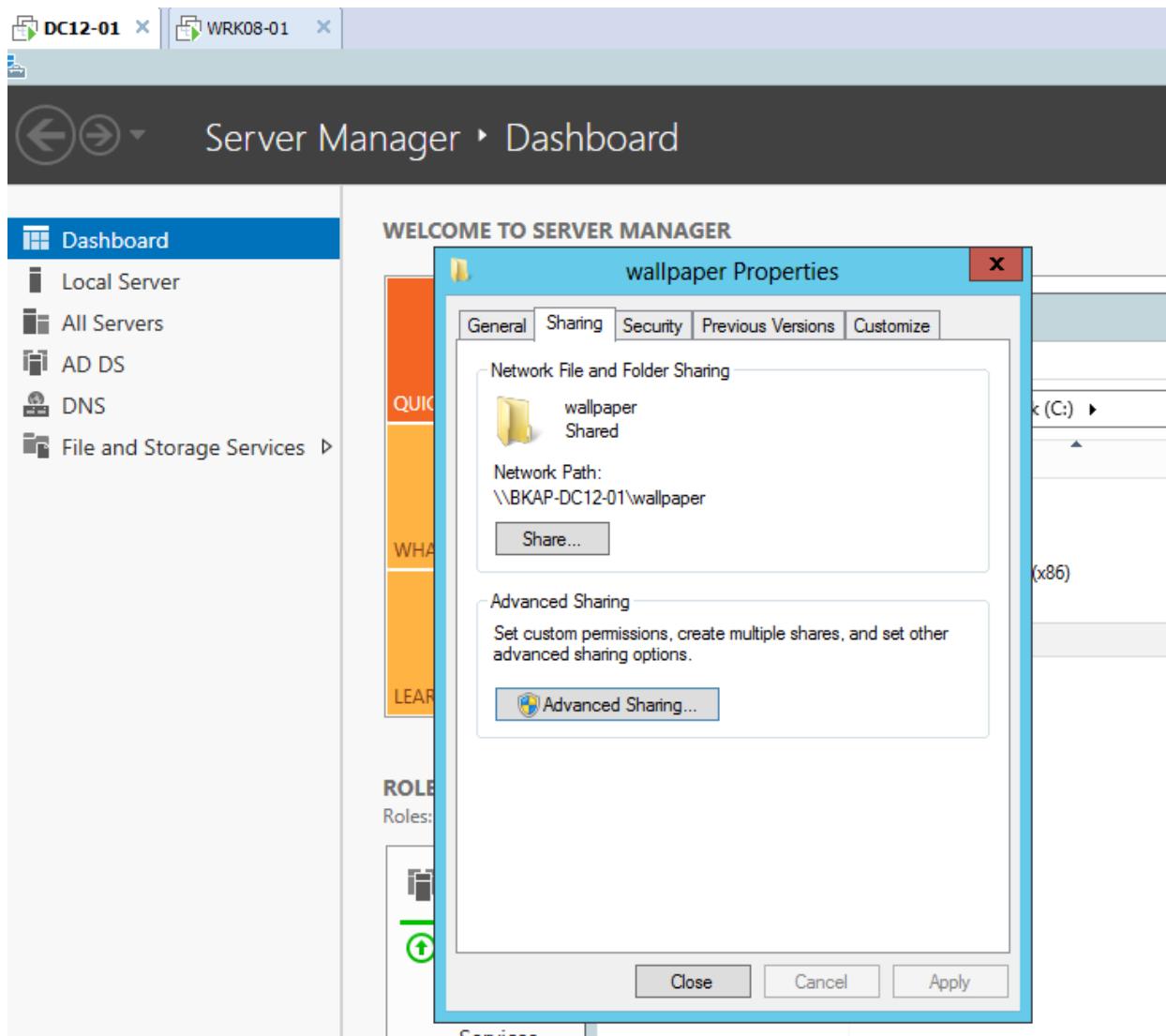
Thông số	BKAP-DC12-01	BKAP-WRK08-01
IP address	192.168.1.2	192.168.1.10
Subnet Mask	255.255.255.0	255.255.255.0
Gateway	192.168.1.1	192.168.1.1
DNS server	192.168.1.2	192.168.1.2

Hướng dẫn chi tiết:

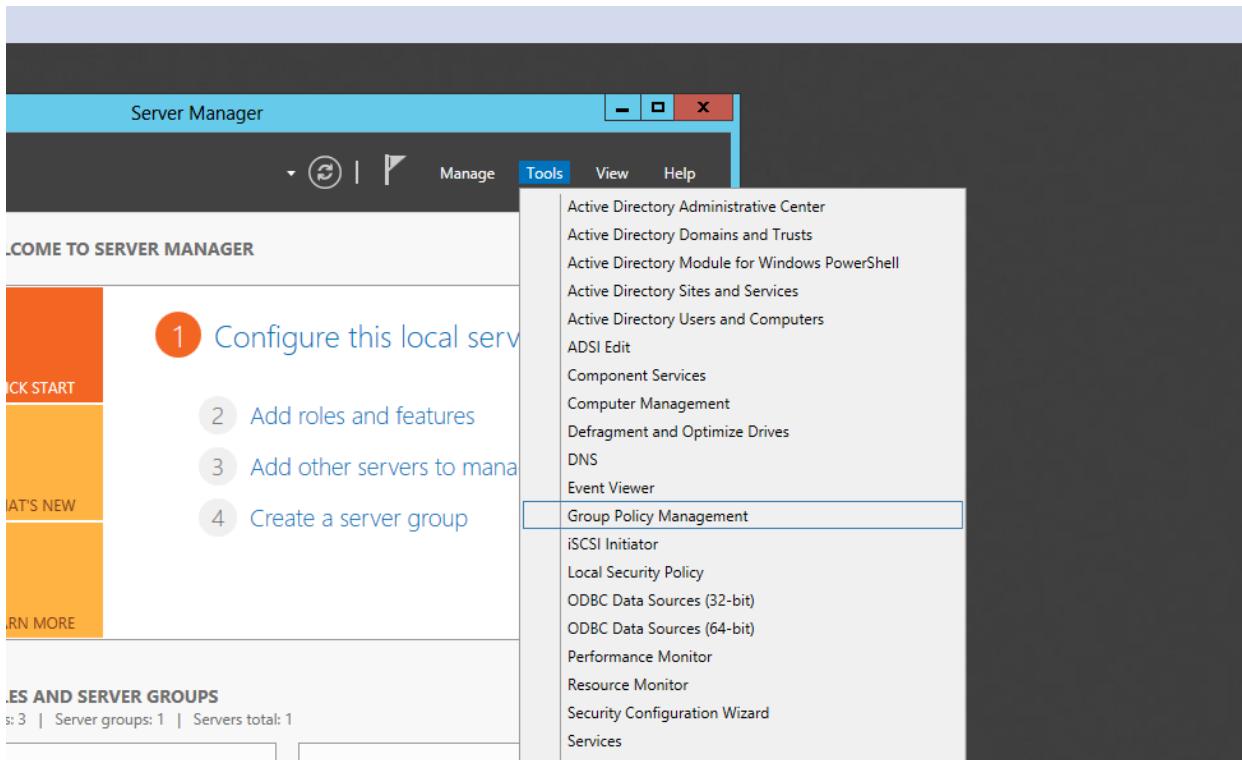
- Thực hiện trên máy *BKAP-DC12-01*, tạo OU, group, User như mô hình, add user vào Group.



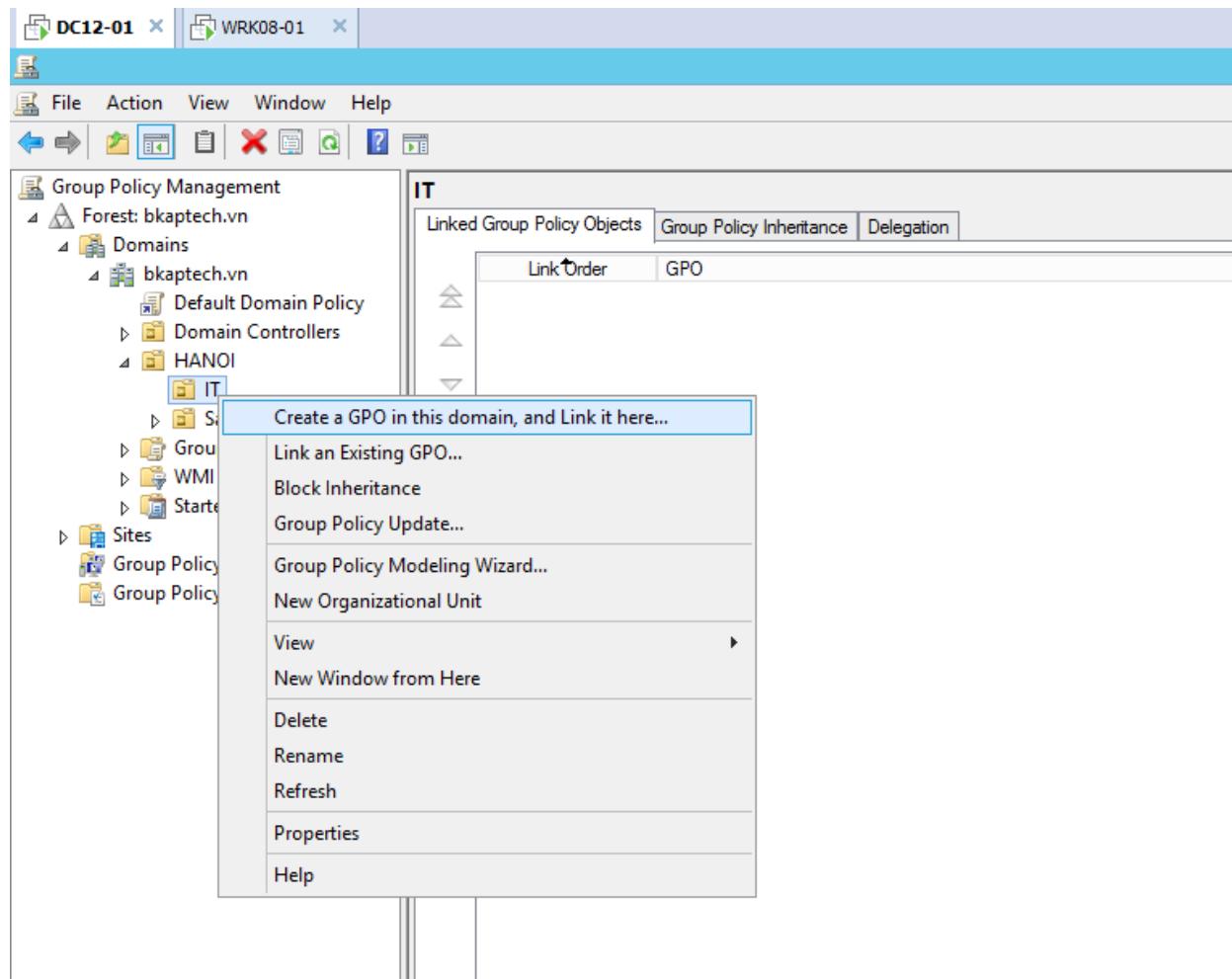
- Tạo thư mục **wallpaper** trong ổ C (thư mục chứa *background* màn hình nền) , tiến hành chia sẻ thư mục.



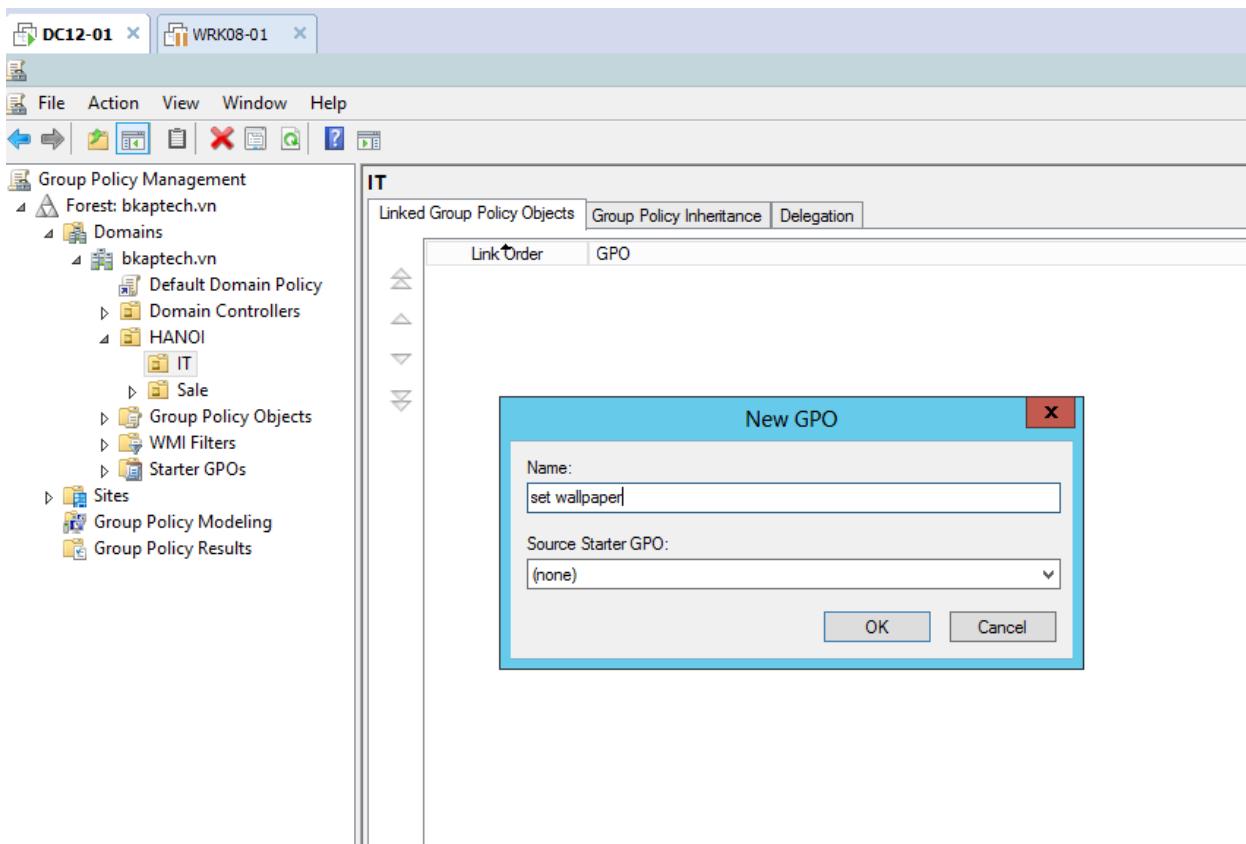
- Cấu hình GPO trên máy *BKAP-DC12-01* :Tạo các chính sách trên phòng ban IT.
 - Vào Server Manager / Tools / Group Policy Management.



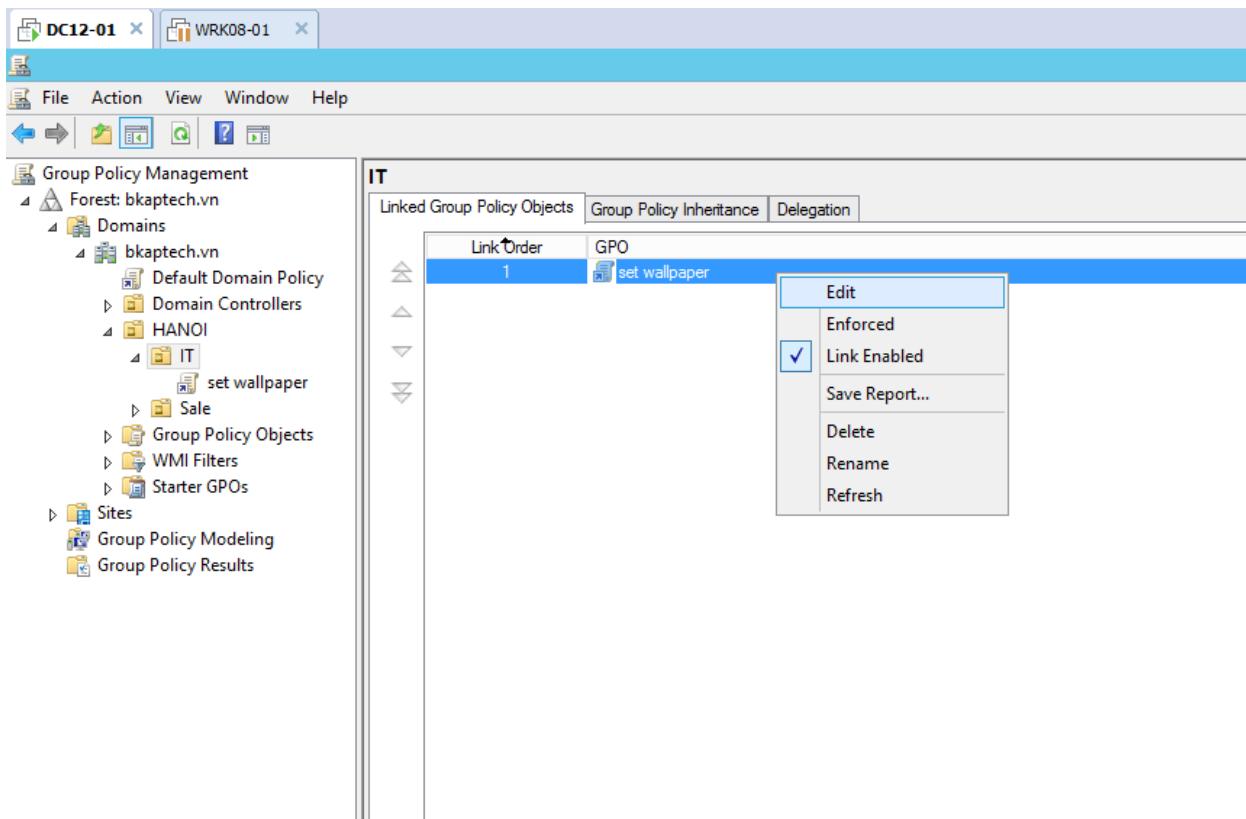
- Tại cửa sổ **Group Policy Management**, click chuột phải vào OU IT, chọn **Create a GPO in this domain, and Link it here...**



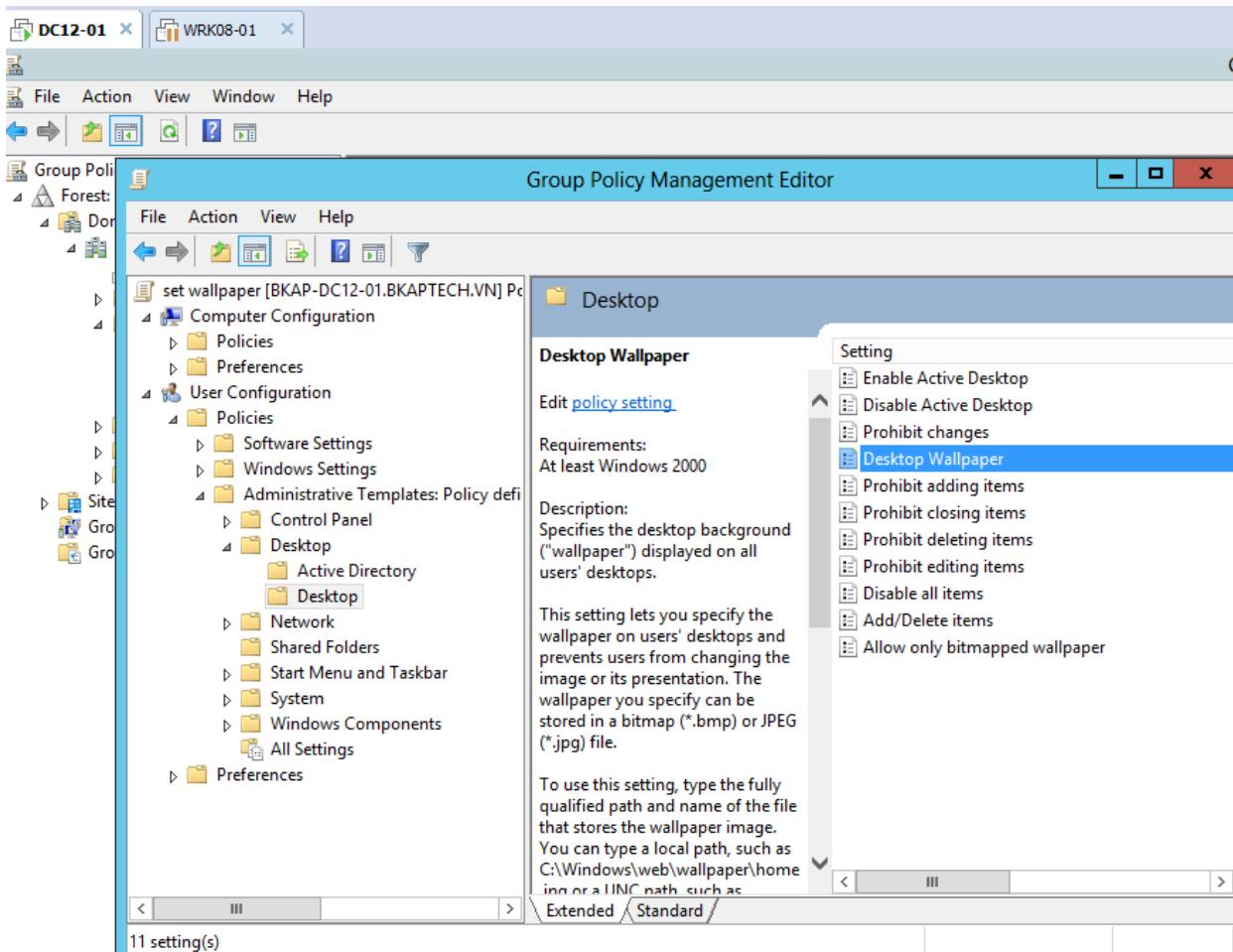
- Tại cửa sổ **New GPO**, nhập vào :
 - **Name** : set wallpaper
- OK.



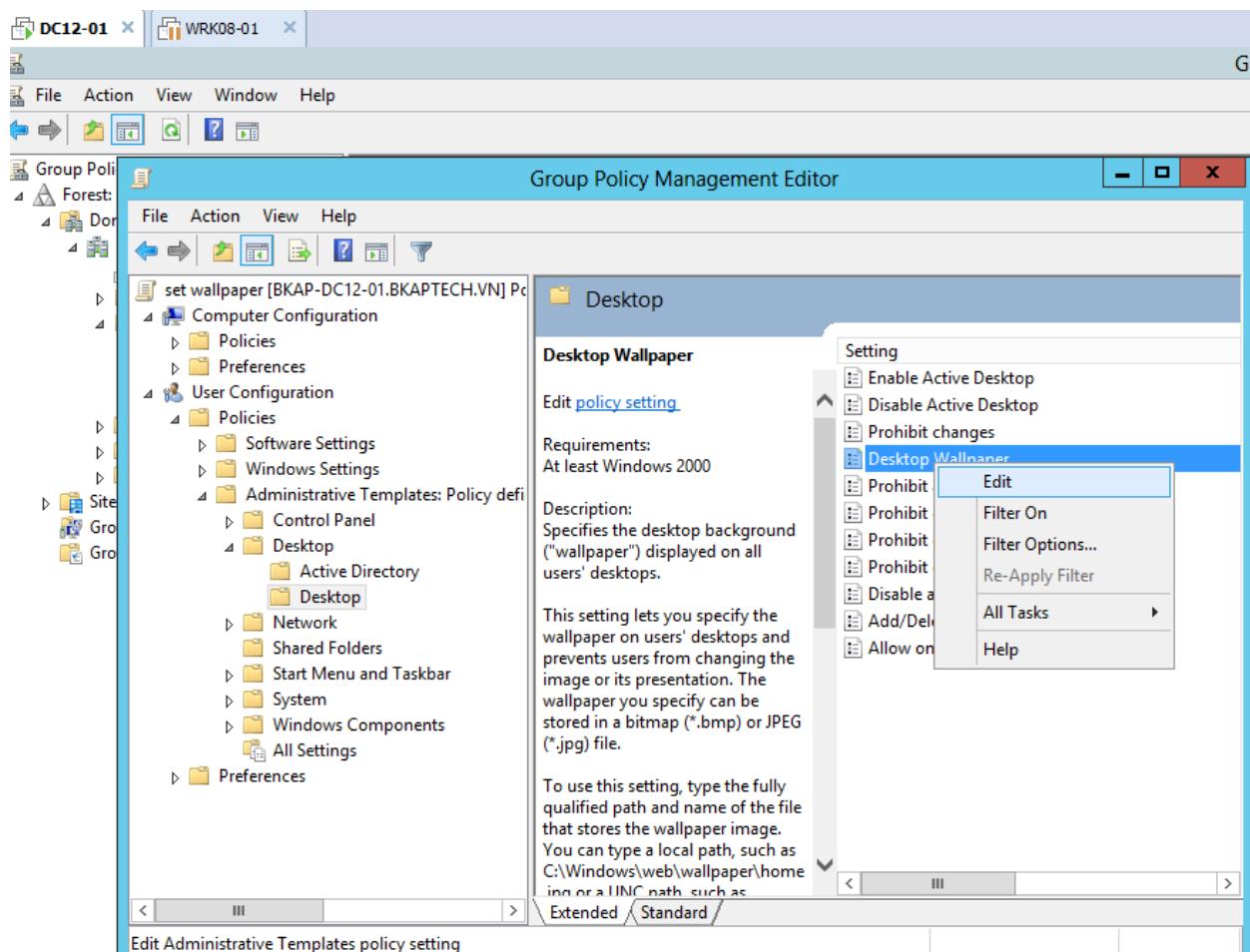
- Click chuột phải tại chính sách set **wallpaper** vừa tạo, chọn **Edit..**



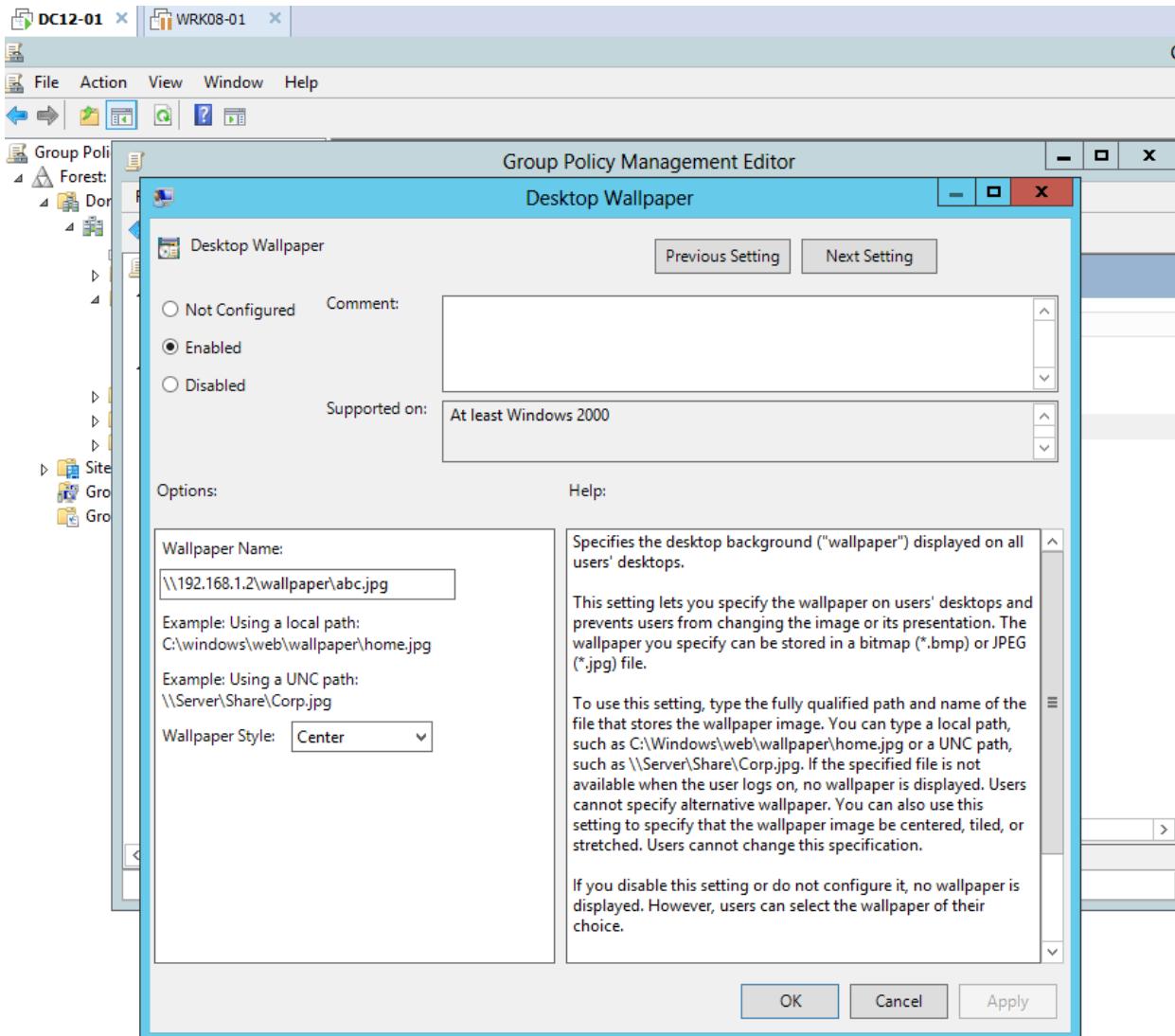
- Tại cửa sổ **Group Policy Management Editor**, click chọn vào **User Configuration / Policies / Administrative Template.. / Desktop / Desktop**.
 - Chọn vào *Desktop Wallpaper*.



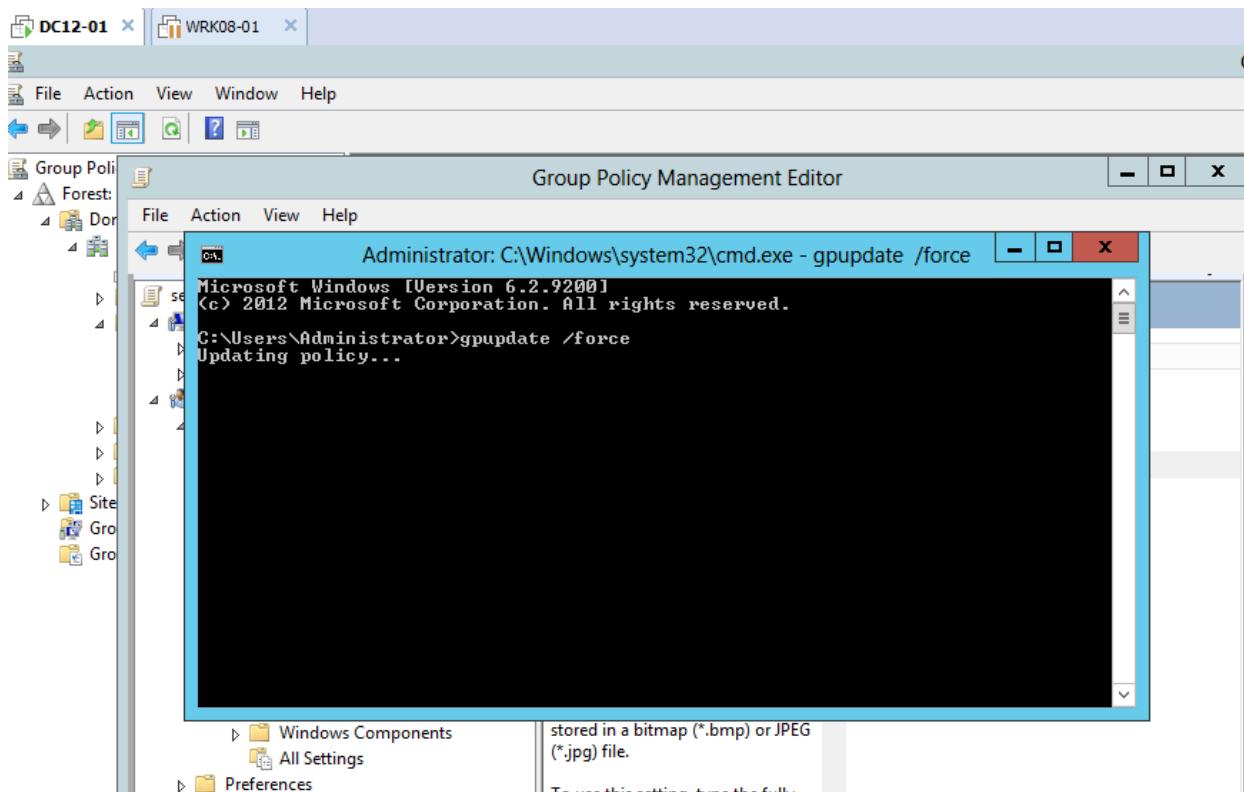
- Click vào Desktop Wallpaper, chọn Edit.



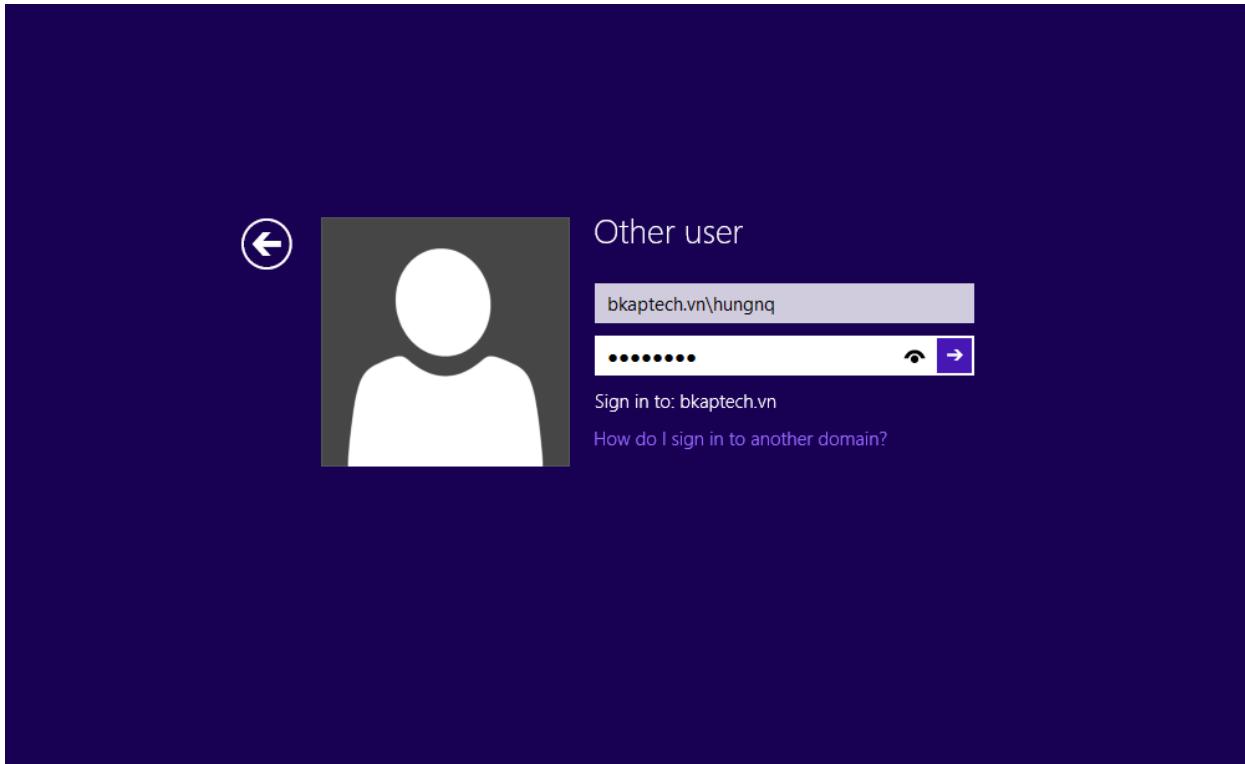
- Tại cửa sổ **Desktop Wallpaper**, click vào **Enable**.
 - Tại **Wallpaper Name** : đưa vào đường dẫn folder **wallpaper** vừa share ở trên.
 - **Wallpaper Name** : <\\192.168.1.2\\wallpaper\\abc.jpg>



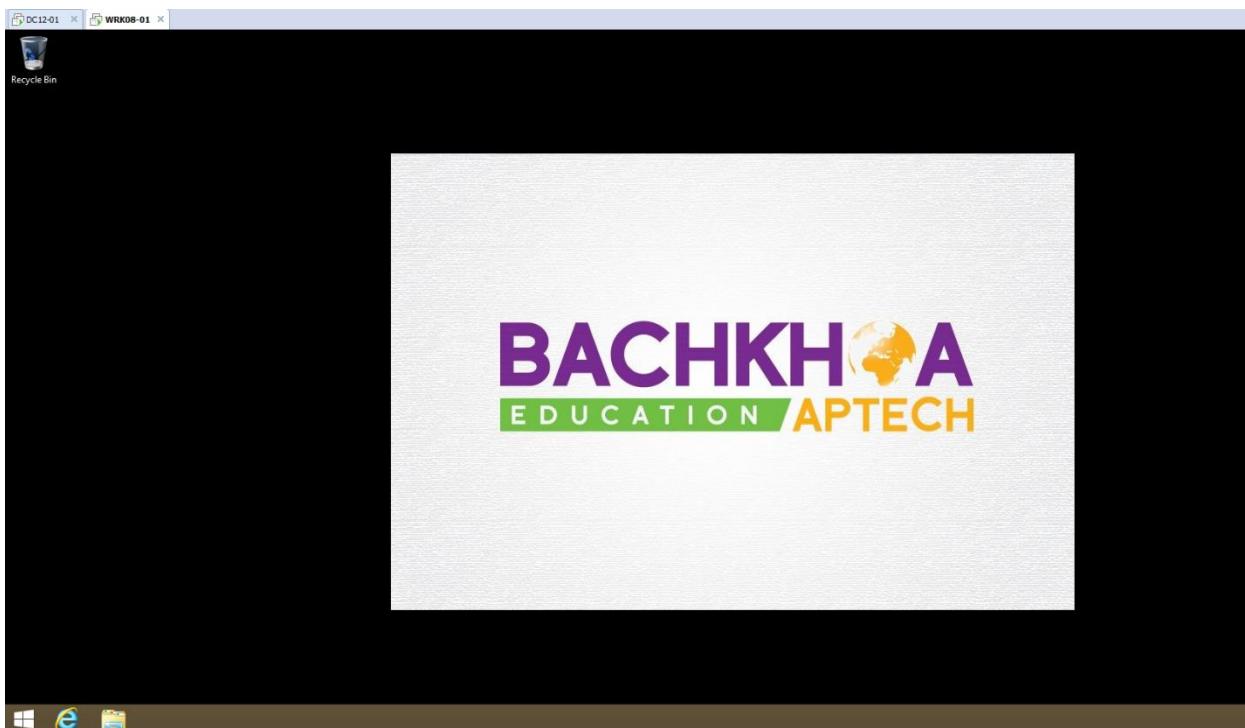
- Cập nhật GPO:
 - Cmd / gõ lệnh **gpupdate /force**



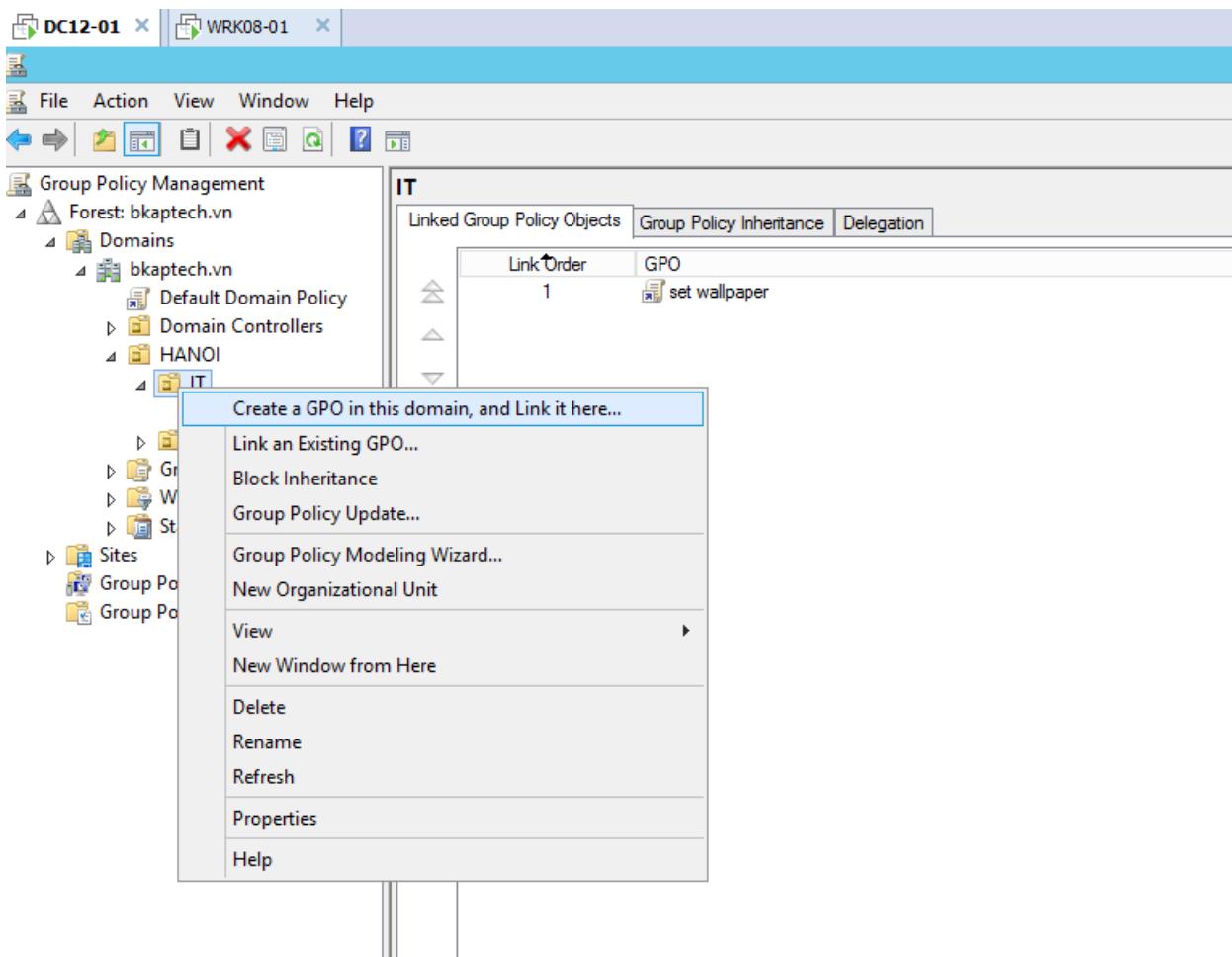
- Chuyển sang máy Client Win 8, đăng nhập bằng tài khoản **hungnq** trong phòng ban IT để kiểm tra.



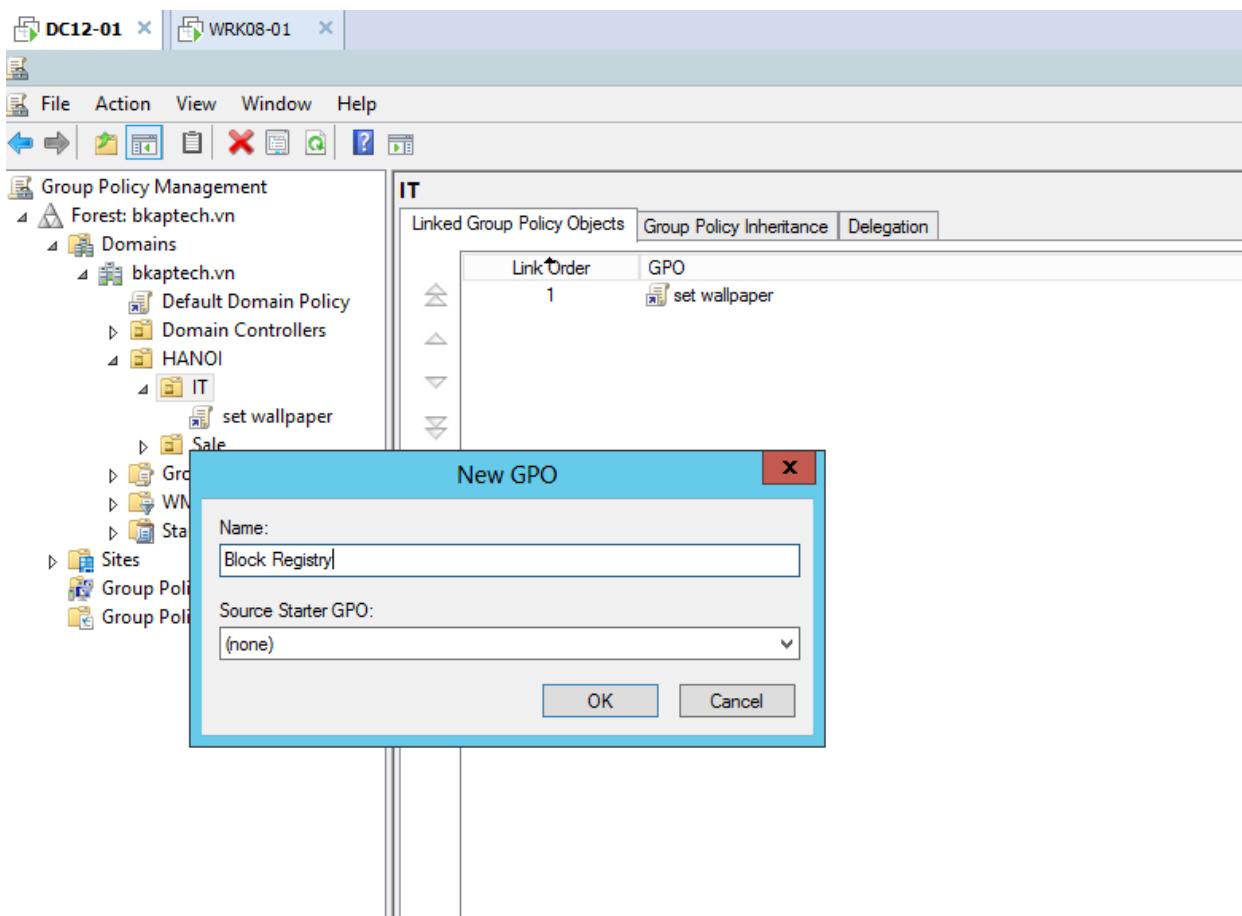
- Client đã cập nhật màn hình nền thành công.



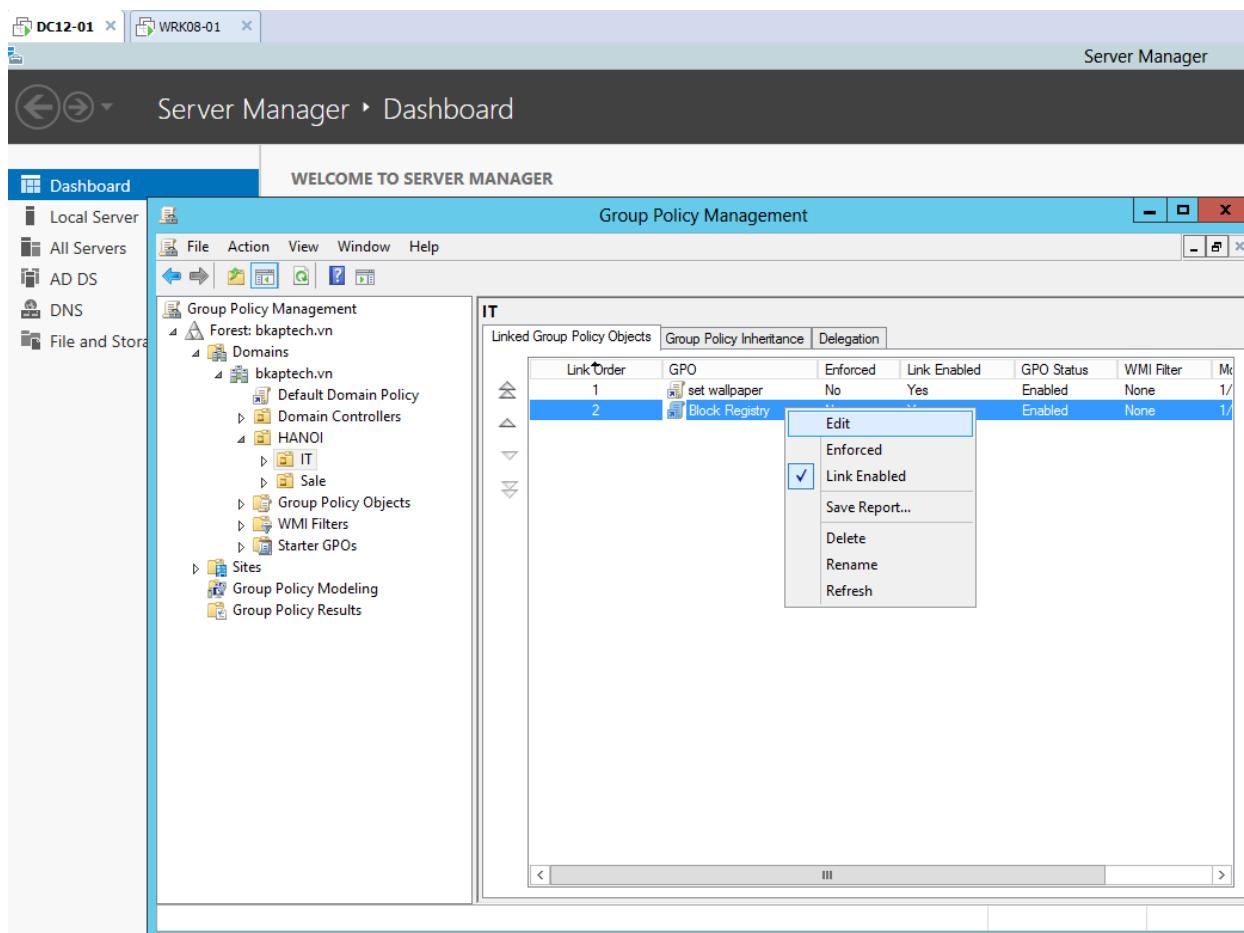
- Chuyển về máy *BKAP-DC12-01*, tạo chính sách **Block Registry**.
 - Click chuột phải tại OU **IT**, chọn **Create a GPO in this domain...**



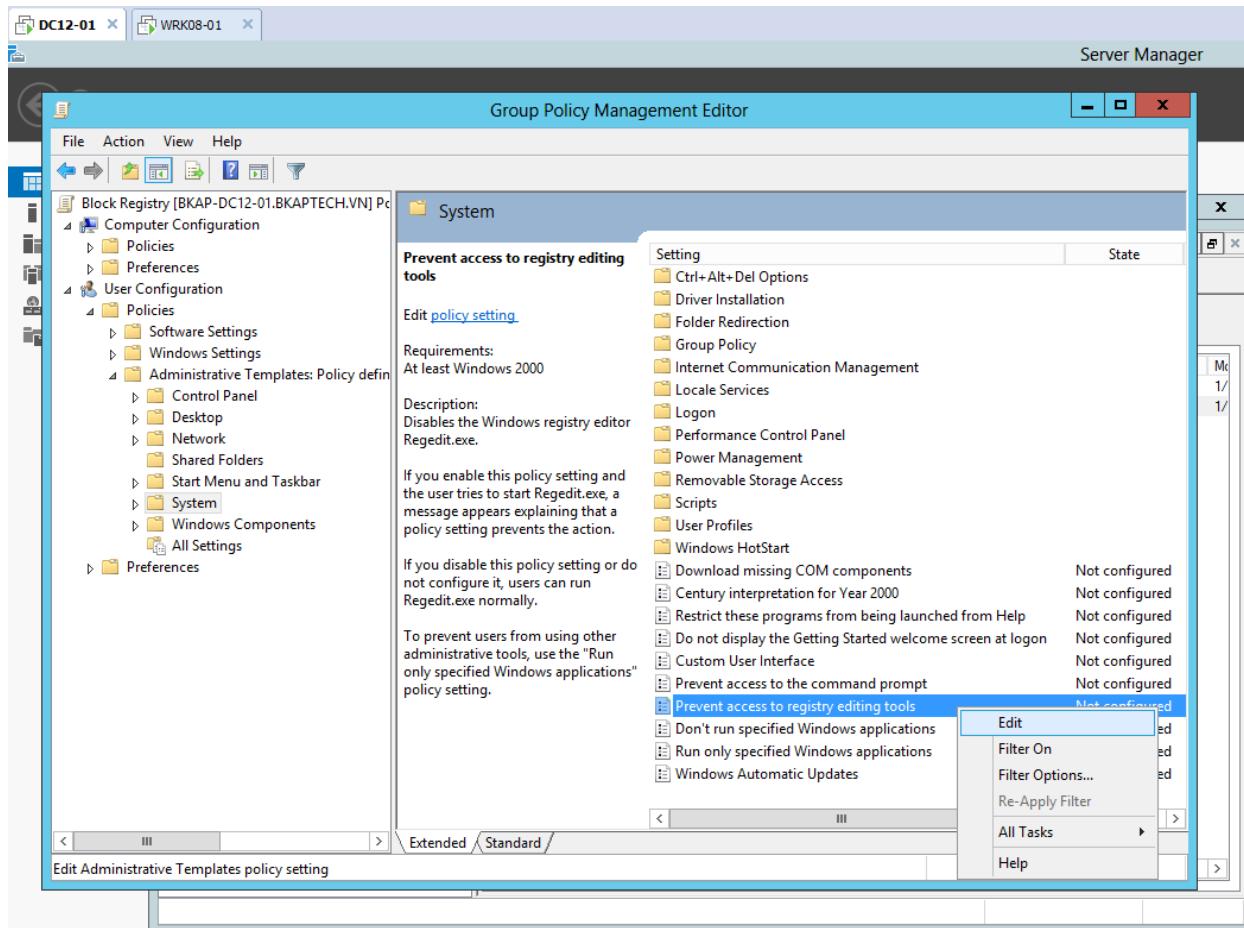
- Tại cửa sổ New GPO, nhập vào tên Name : Block registry.



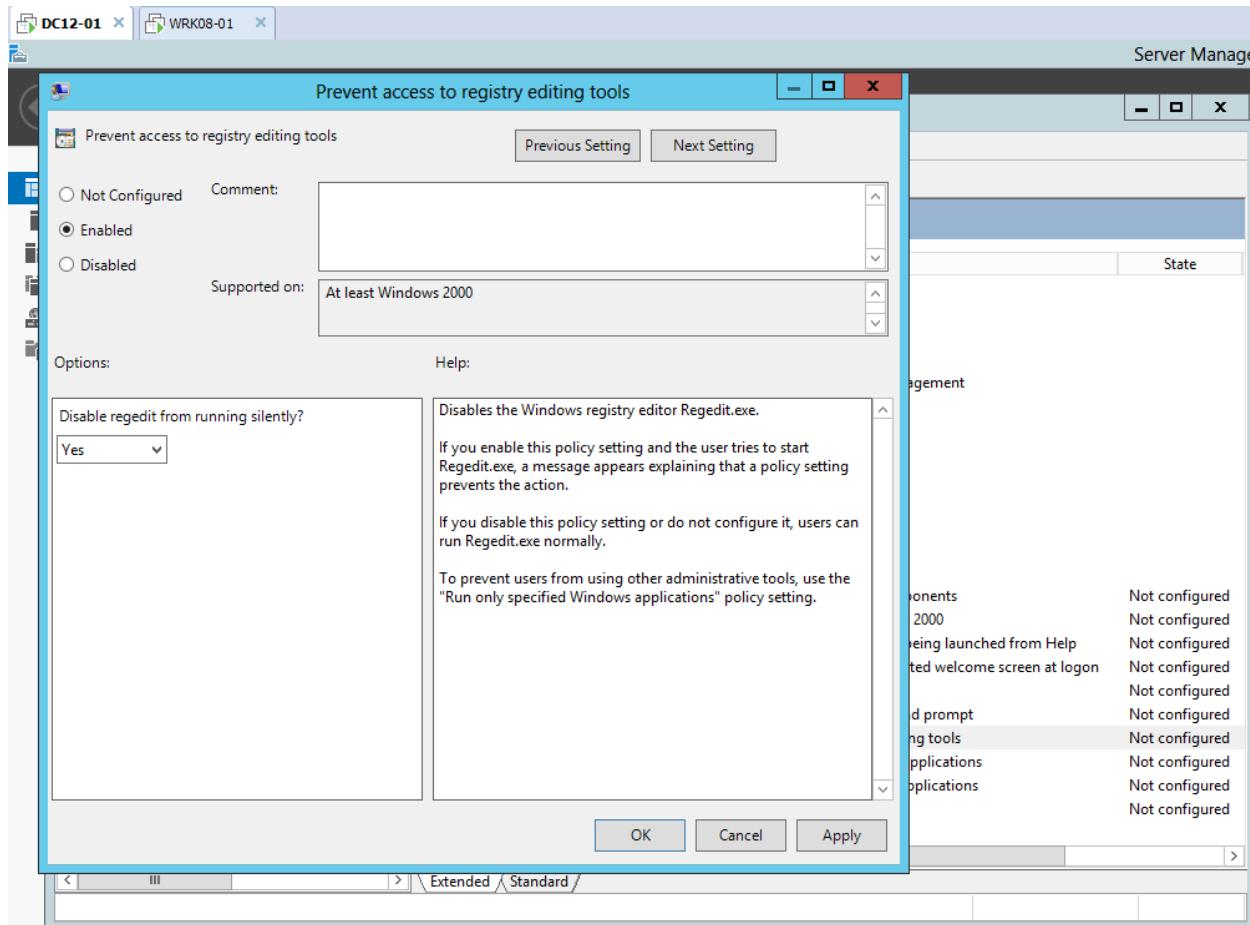
- Click chuột phải vào chính sách **Block Registry** vừa tạo, chọn **Edit**.



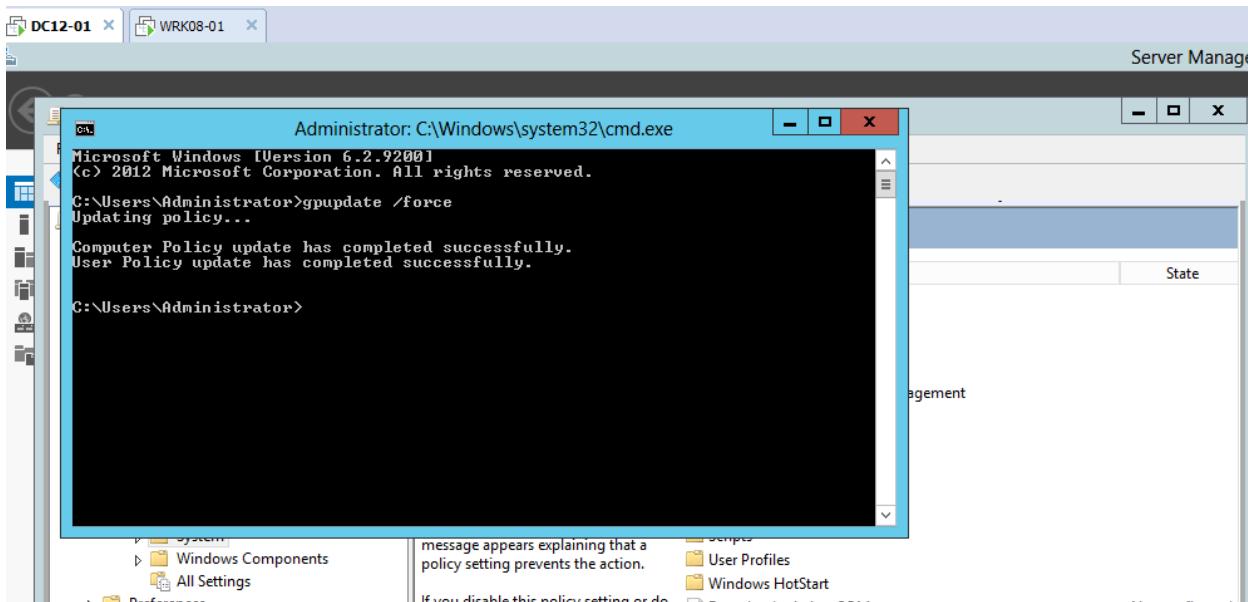
- Tại cửa sổ **Group Policy Management Editor**, chọn vào mục **User Configuration / Policies / Administrative Templates .. / System**, chọn vào chính sách **Prevent access to registry editing tools.**, tại đây click chuột phải chọn **Edit**.



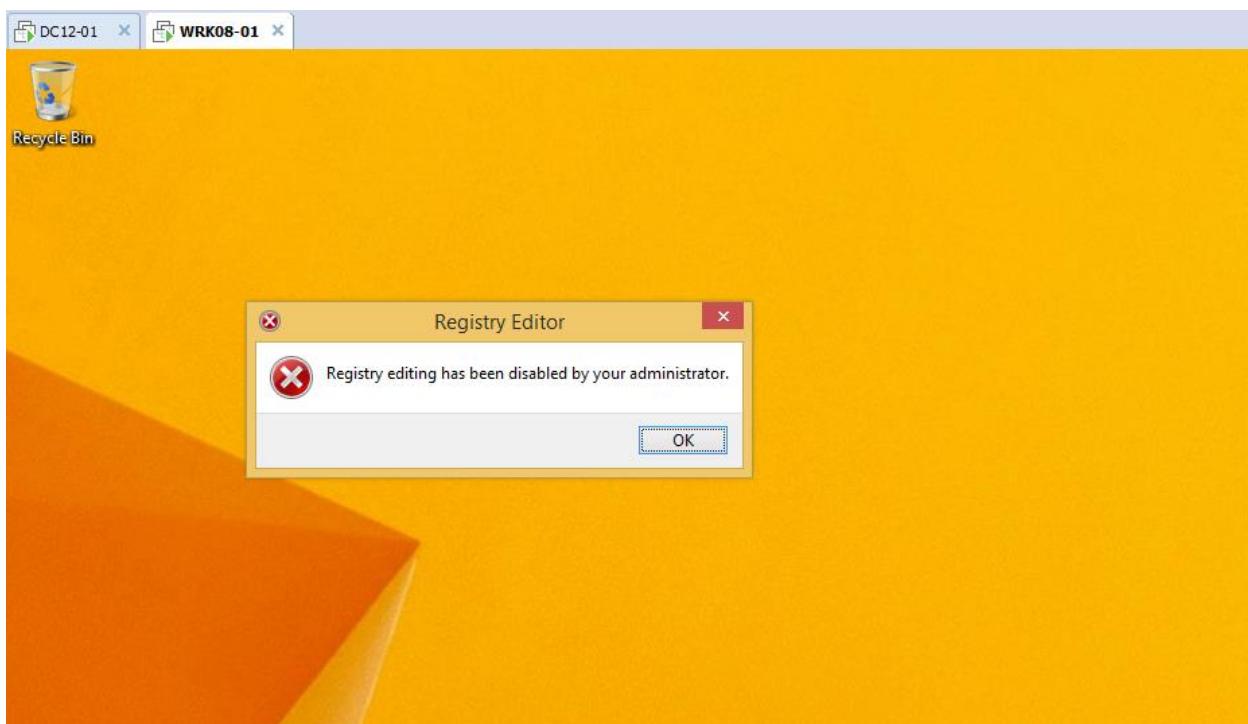
- Tại cửa sổ **Prevent access to registry editing tools** , click chọn vào **Enable** , **Apply** , **OK**.



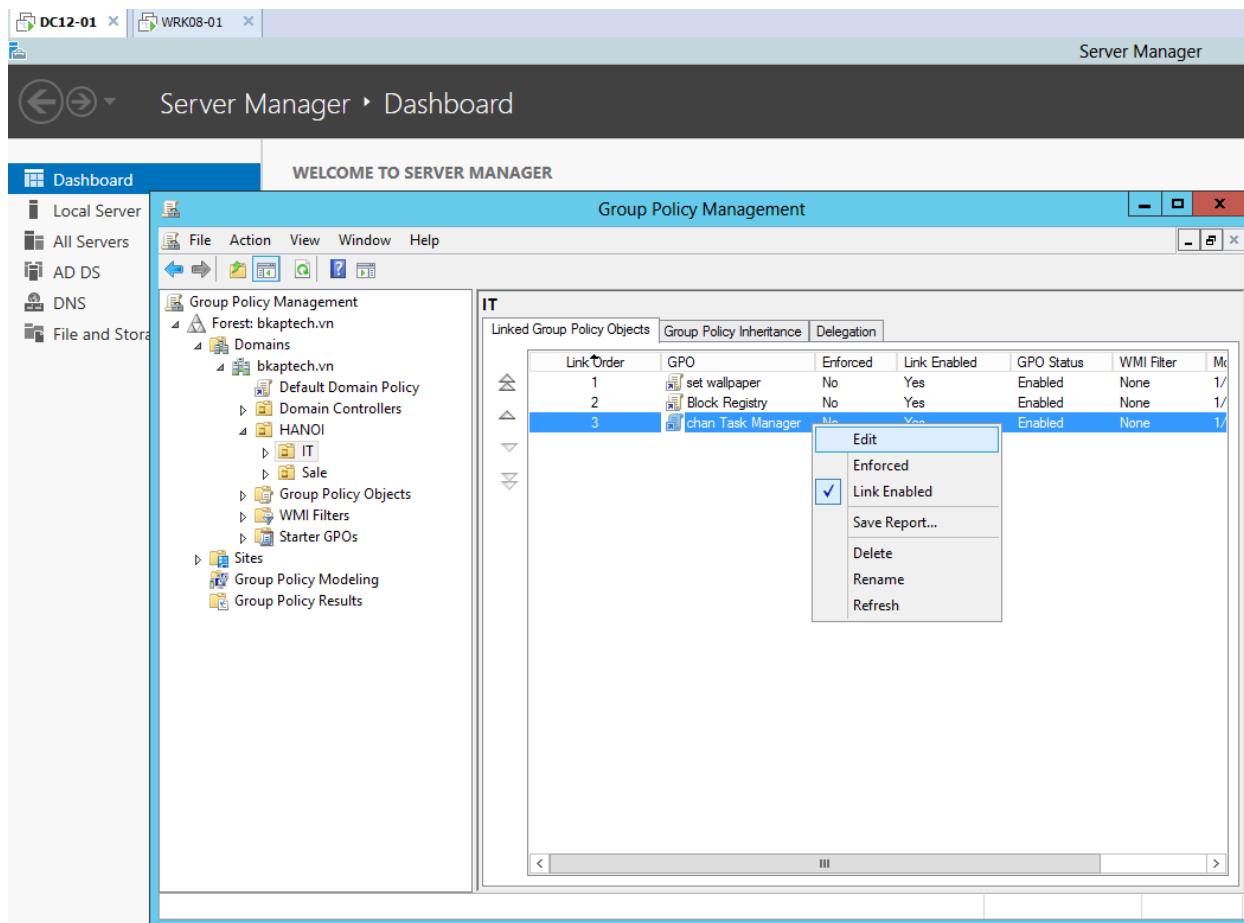
- Cập nhật chính sách bằng lệnh **gpupdate /force** trong cmd.



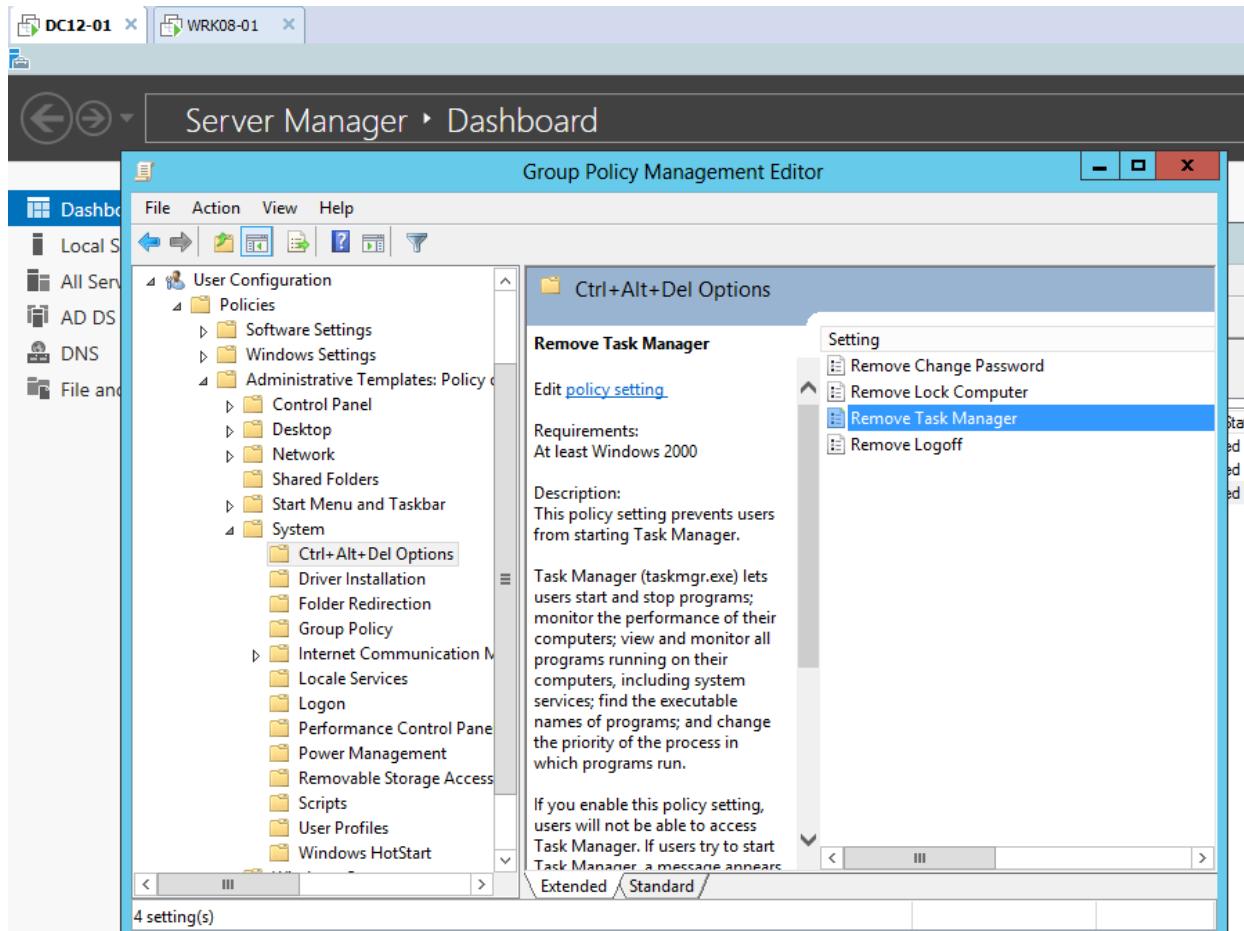
- Chuyển sang máy *Client Win 8* đăng nhập bằng tài khoản **hungnq** trong phòng ban IT để kiểm tra.



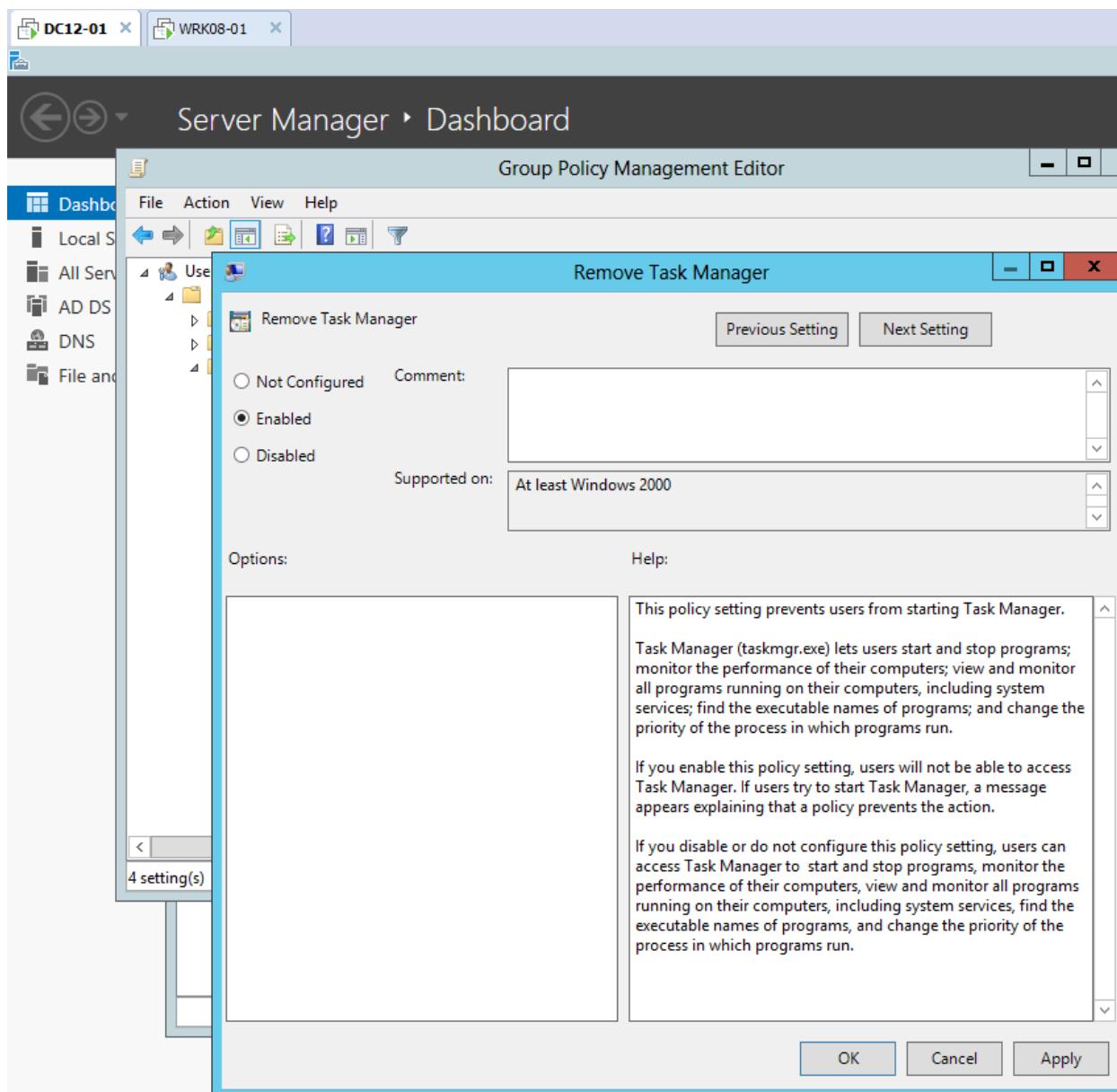
- Chuyển sang máy *BKAP-DC12-01*, tạo thêm chính sách **chặn Task Manager**.
 - Click chuột phải tại **OU IT**, chọn **Create a GPO in this domain...**
 - Tại cửa sổ **New GPO**, nhập vào tên chính sách **Name : Chặn Task Manager**.
 - Click chuột phải vào chính sách vừa tạo, chọn **Edit**.



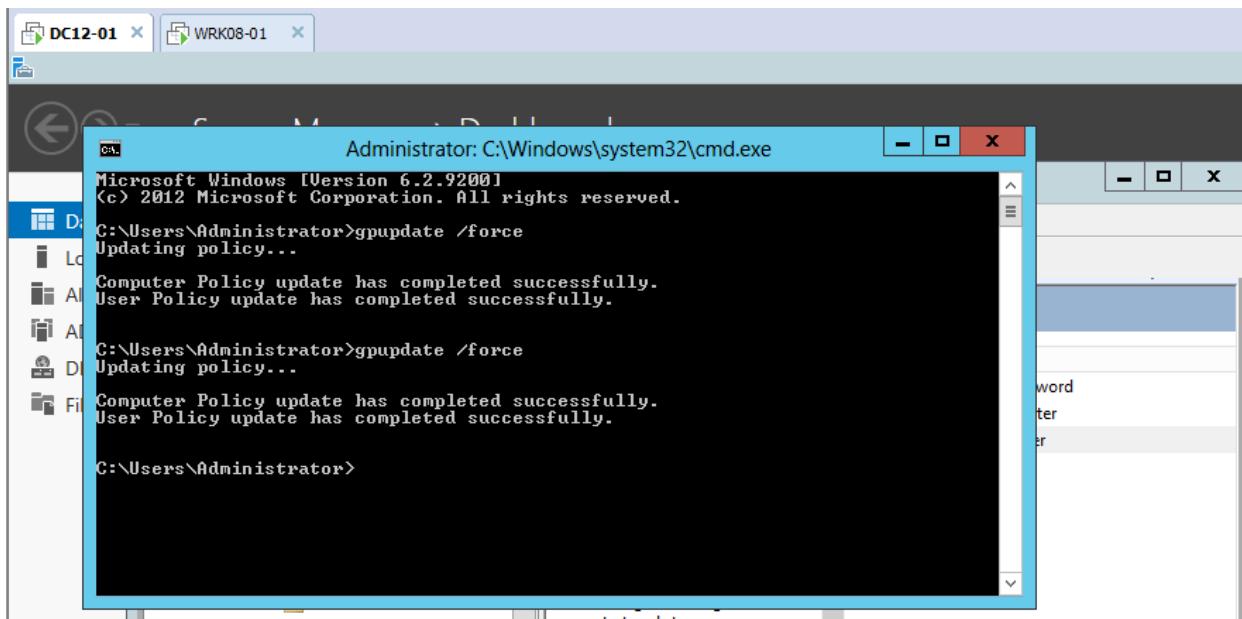
- Tại cửa sổ **Group Policy Management Editor**, chọn vào **User Configuration / Policies / Administrative Template... / System / Ctrl+Alt+Del Options**. Chọn vào chính sách **Remove Task Manager**.



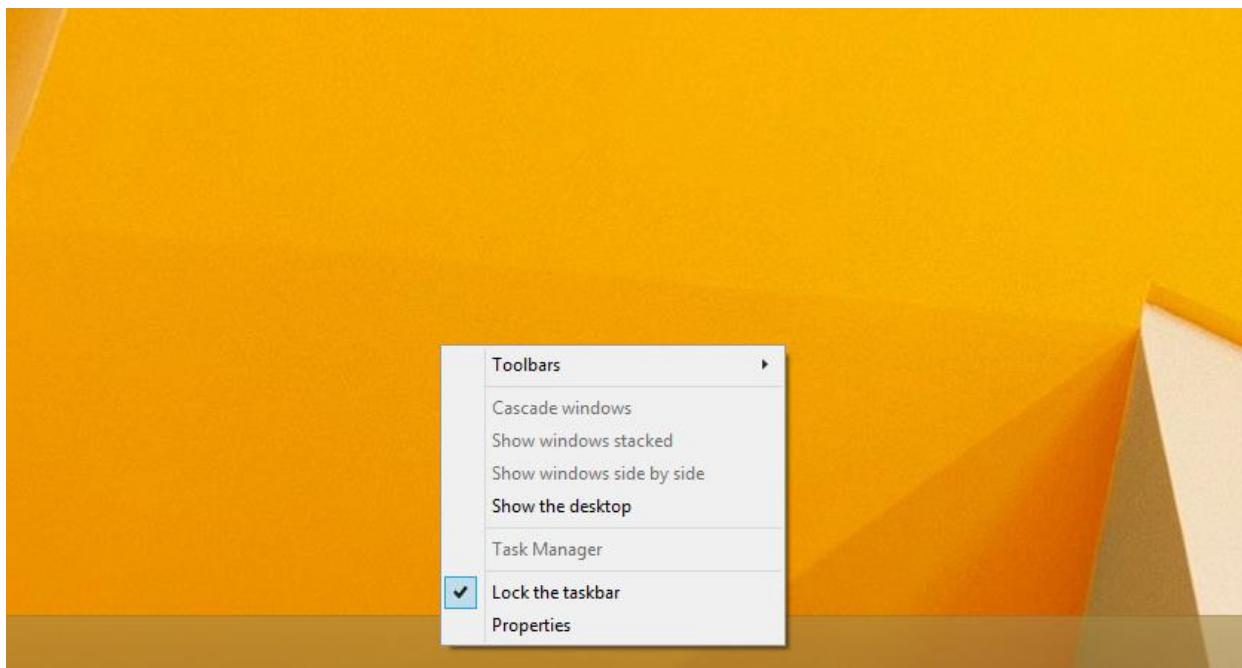
- Tại cửa sổ **Remove Task Manager** , click vào **Enable** , **Apply** , **OK**.



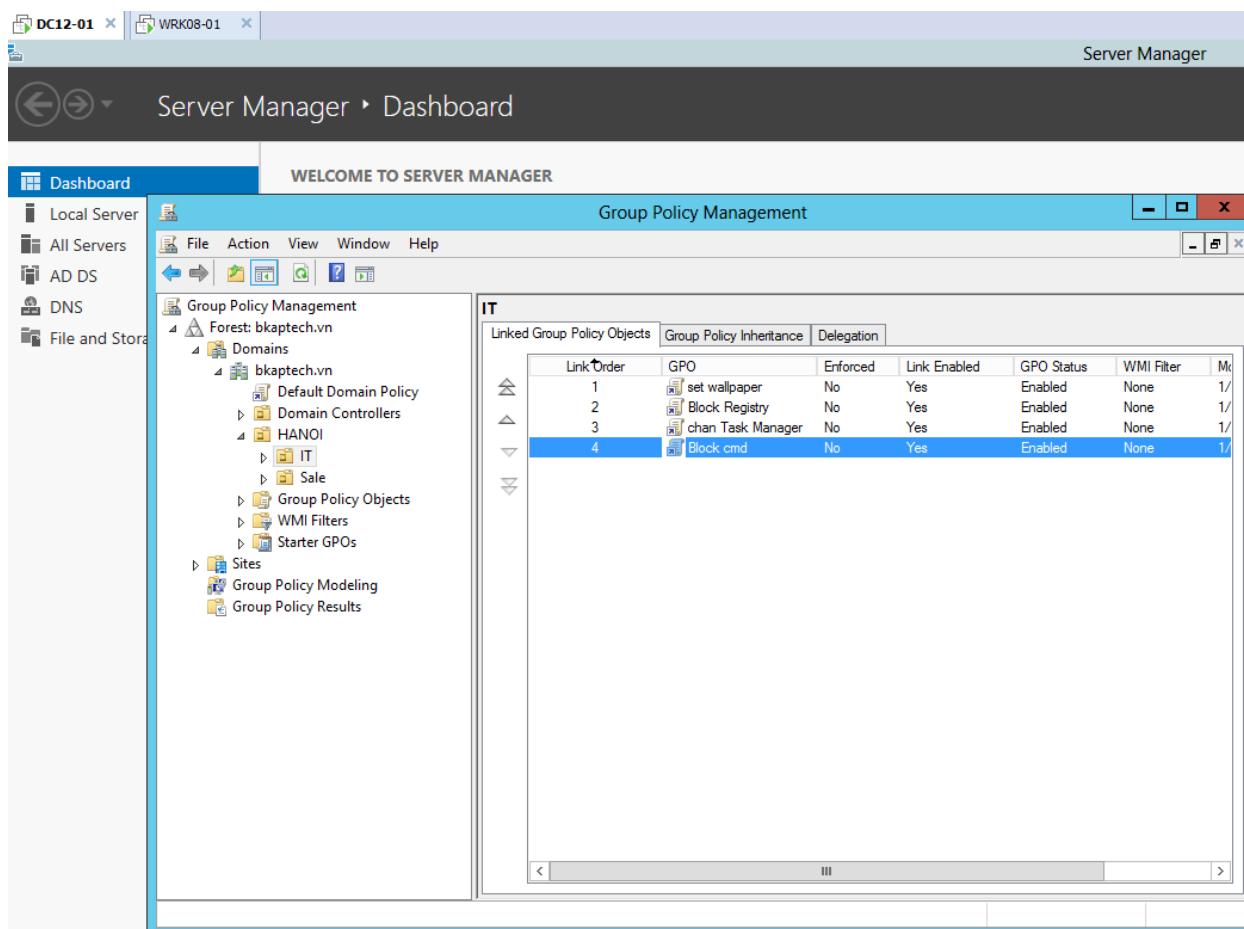
- Cập nhật chính sách bằng lệnh **gpupdate /force** trong cmd.



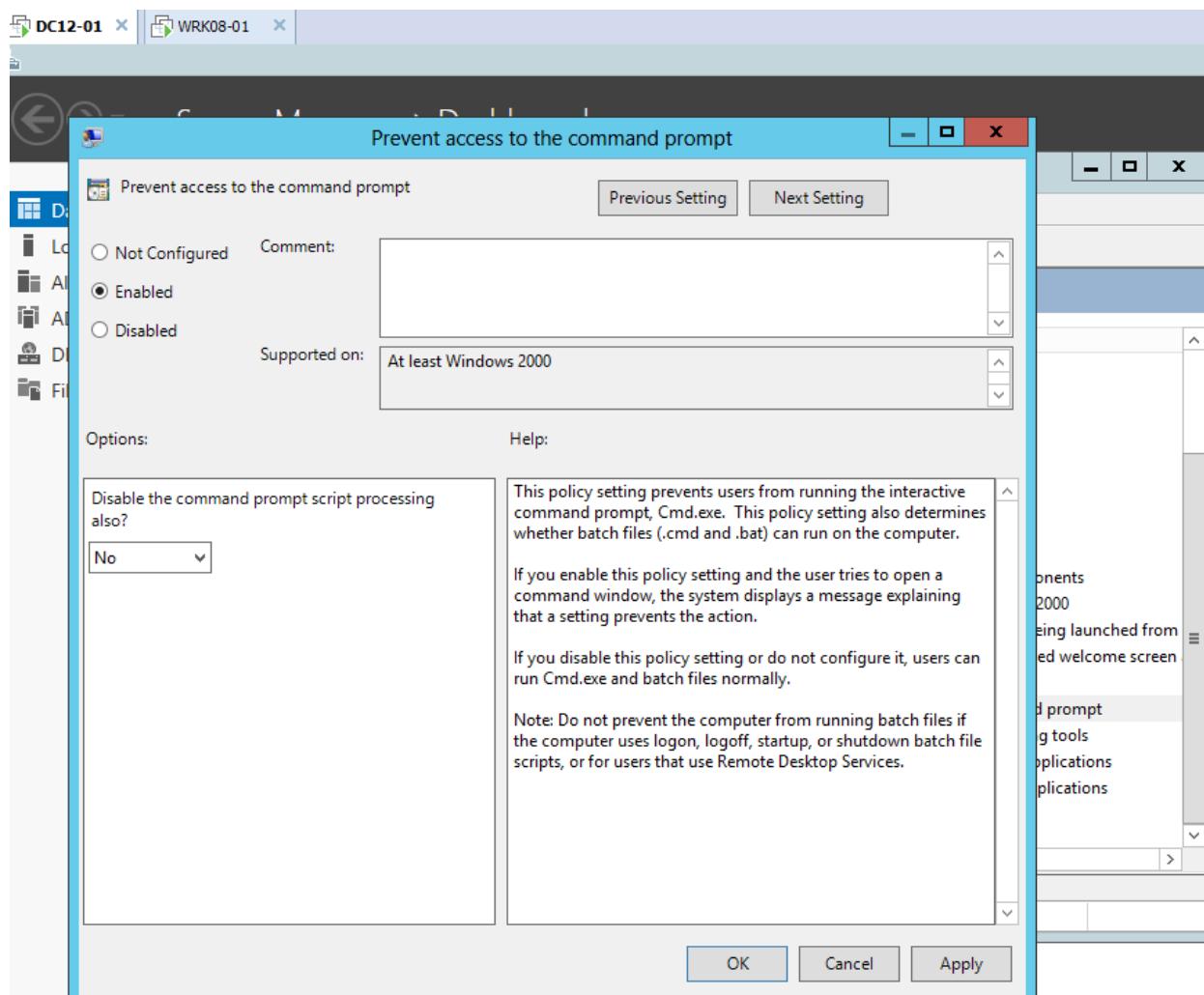
- Chuyển sang máy Client Win 8 kiểm tra, Task Manager đã bị khóa.



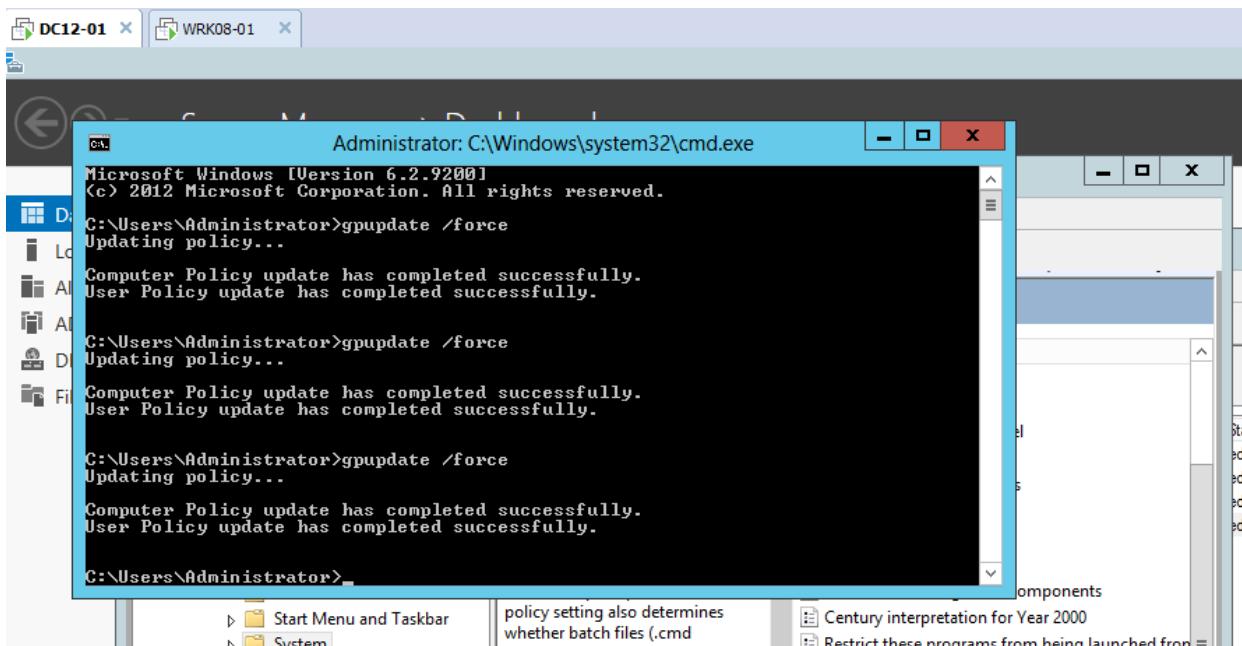
- Chuyển về máy *BKAP-DC12-01*, tại OU **IT**, tạo chính sách **Block cmd**.



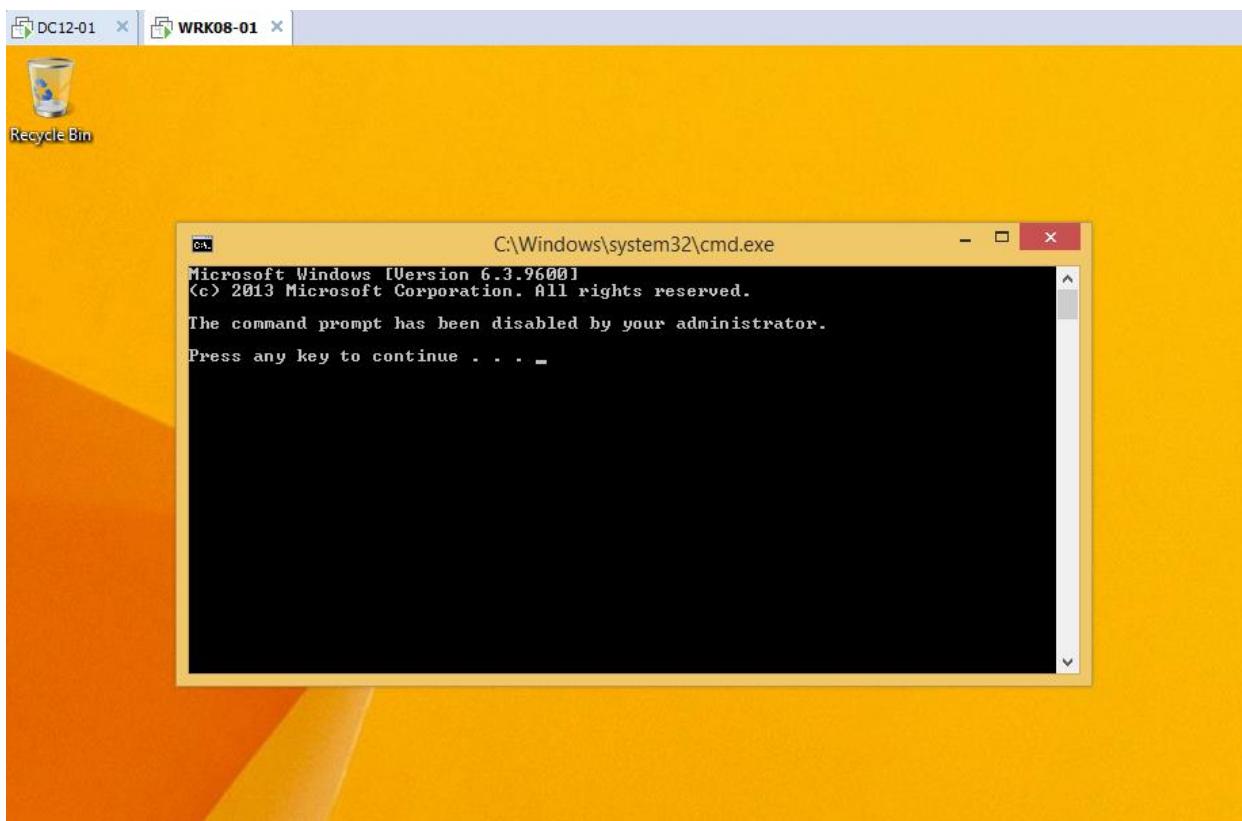
- Tại cửa sổ **Group Policy Management Editor**, click vào **User Configuration /... System** , chọn vào chính sách **Prevent access to the command prompt**.
 - Tại chính sách này, click chuột phải chọn **Edit, Enable , Apply , OK.**



- Cập nhật chính sách bằng lệnh **gpupdate /force** trong cmd.



- Chuyển sang máy *Client Win 8* kiểm tra chính sách **Block cmd**.



11.2 Giám sát tệp tin và bắt xóa file.

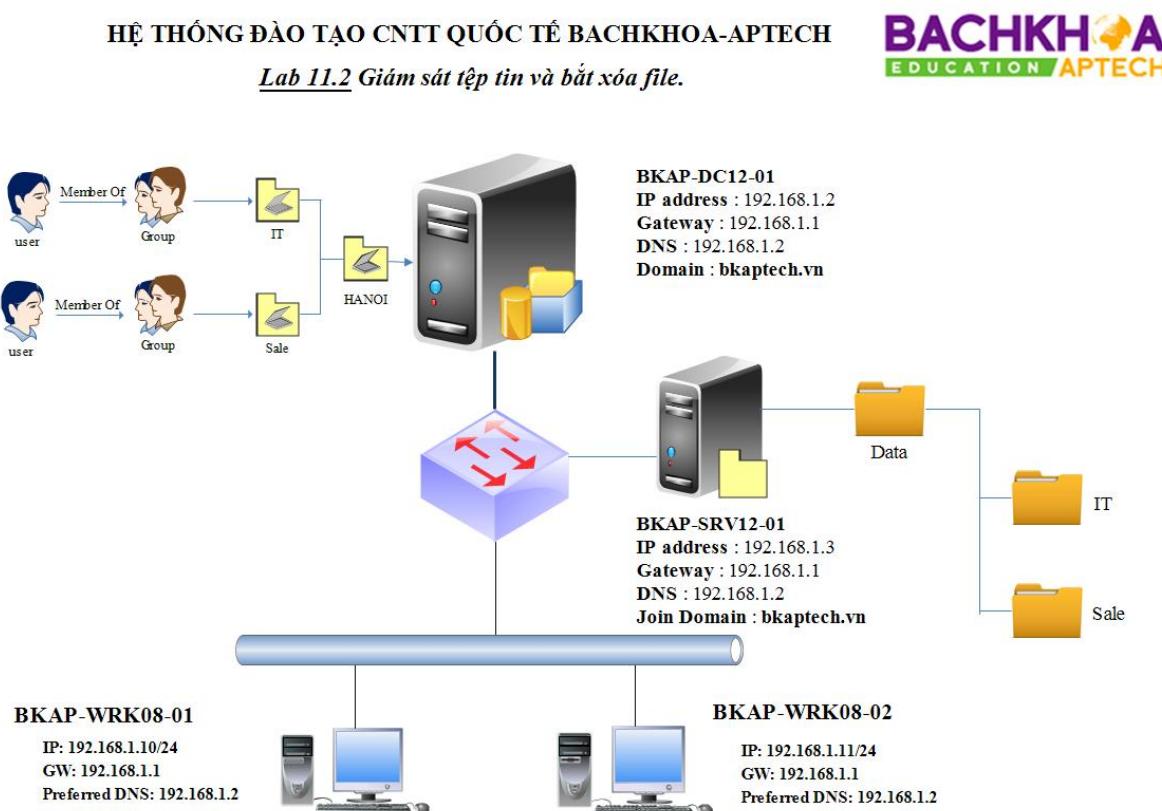
1. Yêu cầu bài lab:

- + Tạo OU, tài khoản người dùng và tài khoản nhóm theo miền bkaptech.vn
- + Tạo lần lượt các thư mục IT , Sale trên máy BKAP-SRV12-01.
- + Cấu hình giám sát tệp tin và bắt xóa File
- + Kiểm tra sau khi xóa file.

2. Yêu cầu chuẩn bị:

- + Máy BKAP-DC12-01 dùng để tạo OU, Group, User.
- + Máy BKAP-SRV12-01 Join vào miền, dùng để tạo thư mục và phân quyền truy cập thư mục.
- + Máy BKAP-WRK08-01 Join vào miền dùng để kiểm tra xóa file.

3. Mô hình Lab:



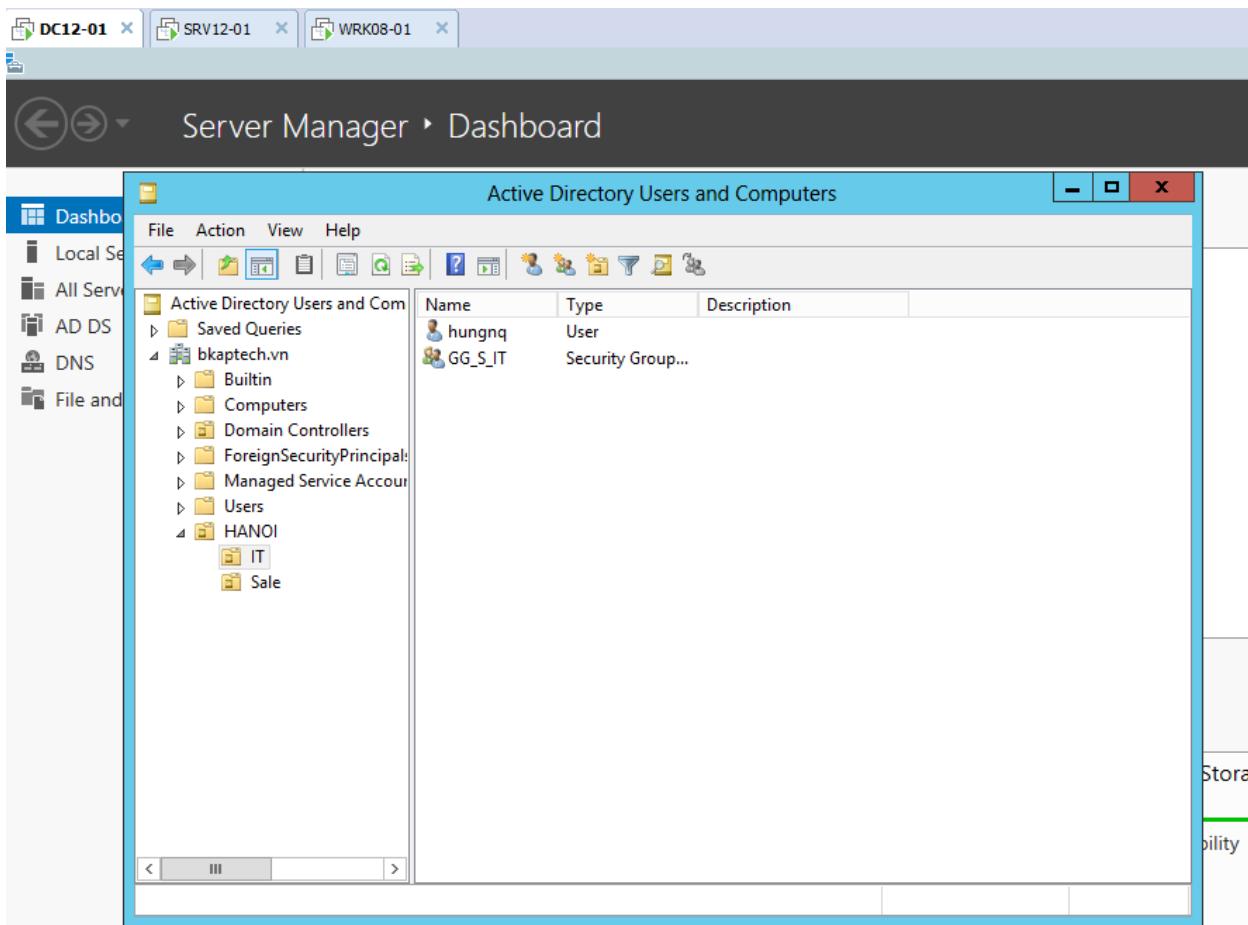
Hình 11.2

Sơ đồ địa chỉ như sau:

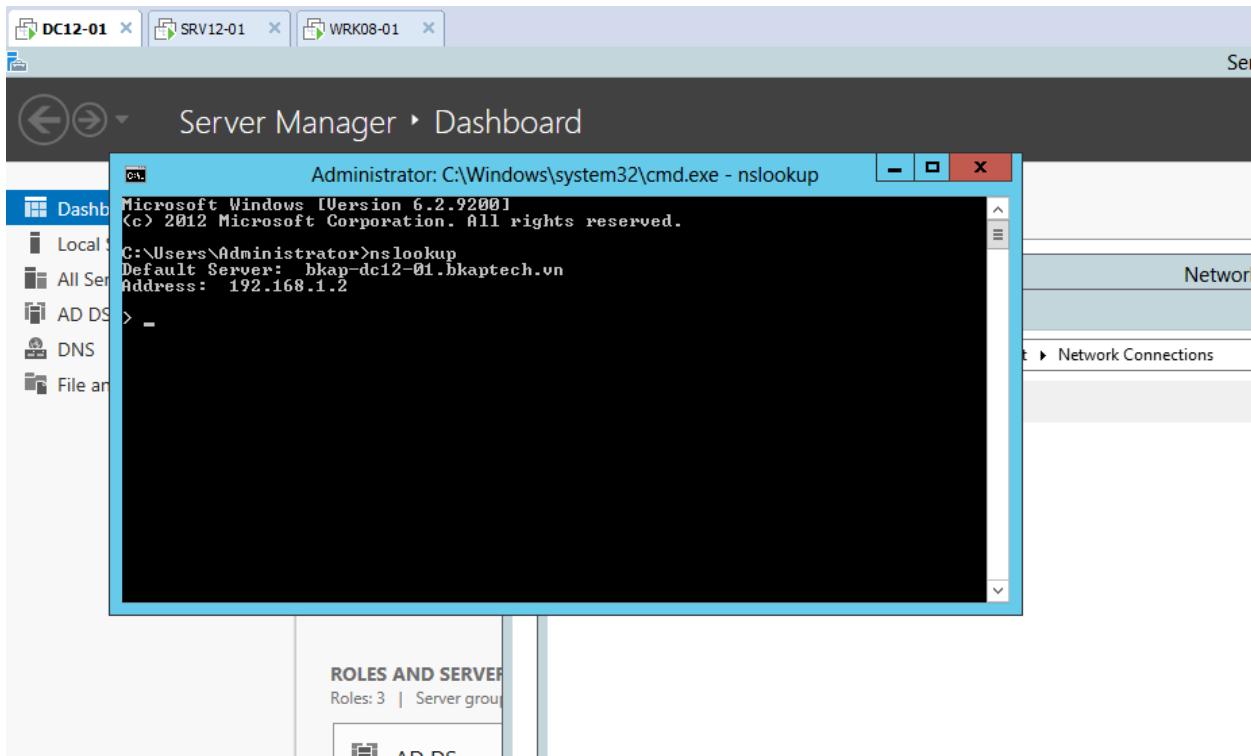
Thông số	BKAP-DC12-01	BKAP-SRV12-01	BKAP-WRK08-01
IP address	192.168.1.2	192.168.1.3	192.168.1.10
Subnet Mask	255.255.255.0	255.255.255.0	255.255.255.0
Gateway	192.168.1.1	192.168.1.1	192.168.1.1
DNS Server	192.168.1.2	192.168.1.2	192.168.1.2

Hướng dẫn chi tiết:

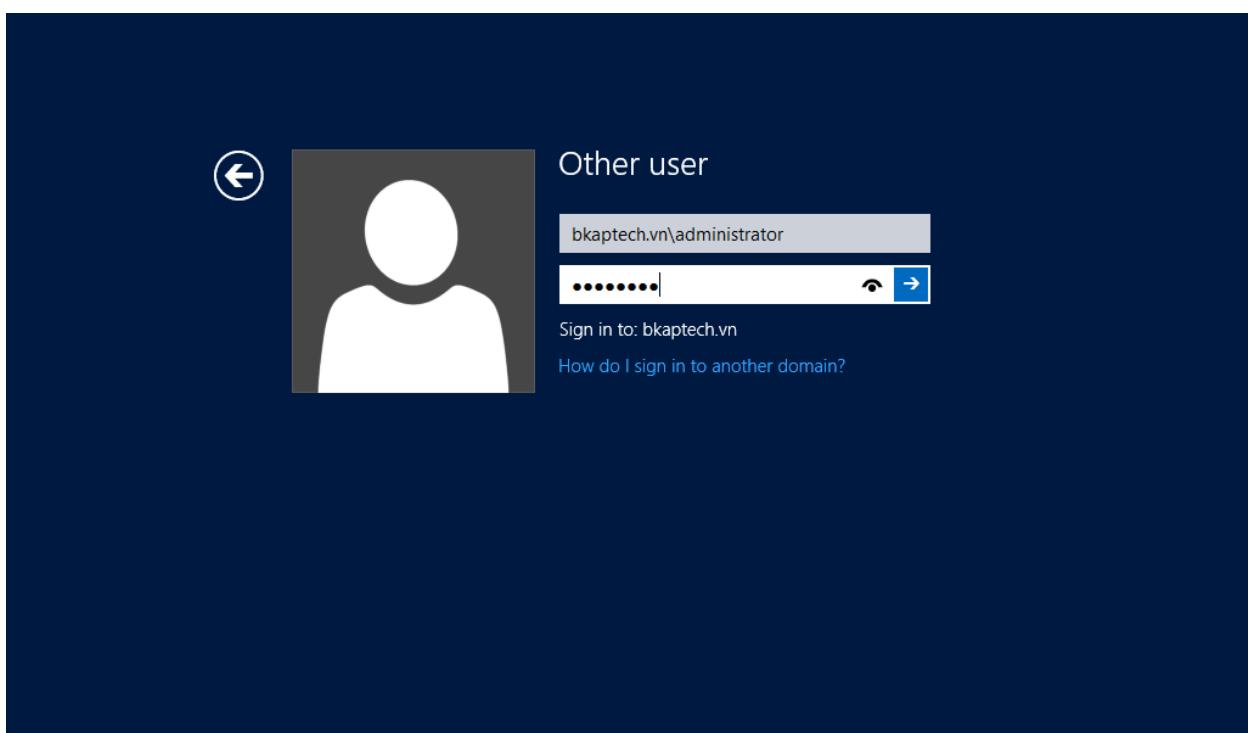
- Trên máy BKAP-DC12-01, thực hiện tạo OU, Group, User, add User vào Group.



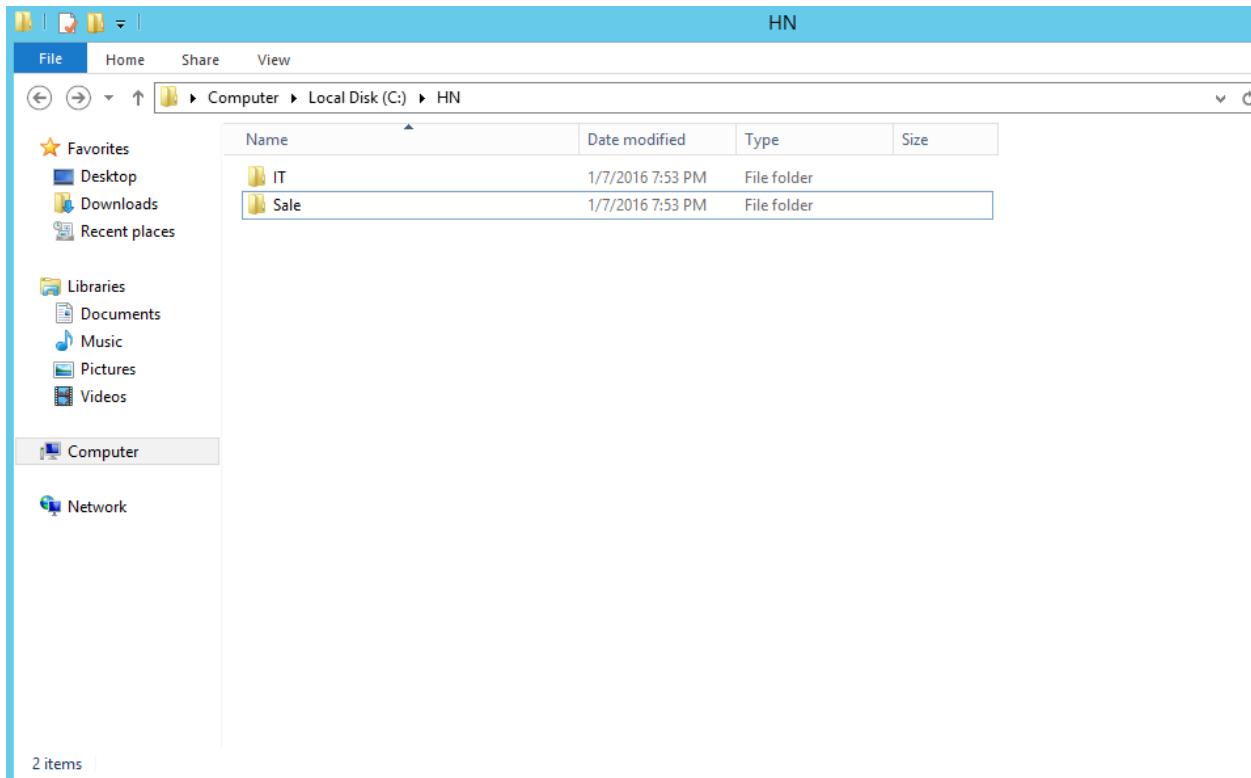
- Kiểm tra phân giải địa chỉ IP :



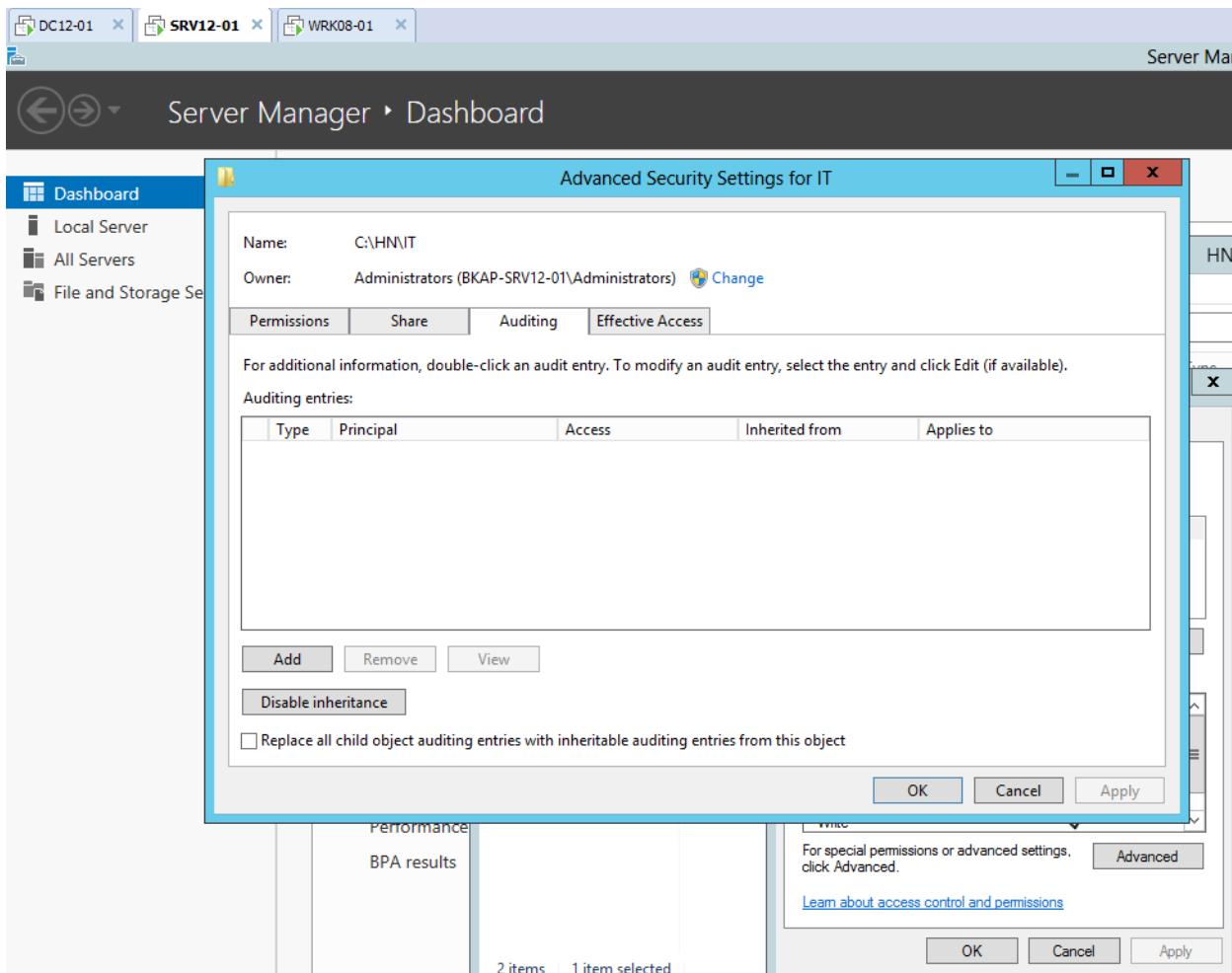
- Chuyển sang máy BKAP-SRV12-01, tiến hành Join vào domain, đăng nhập bằng tài khoản Administrator.



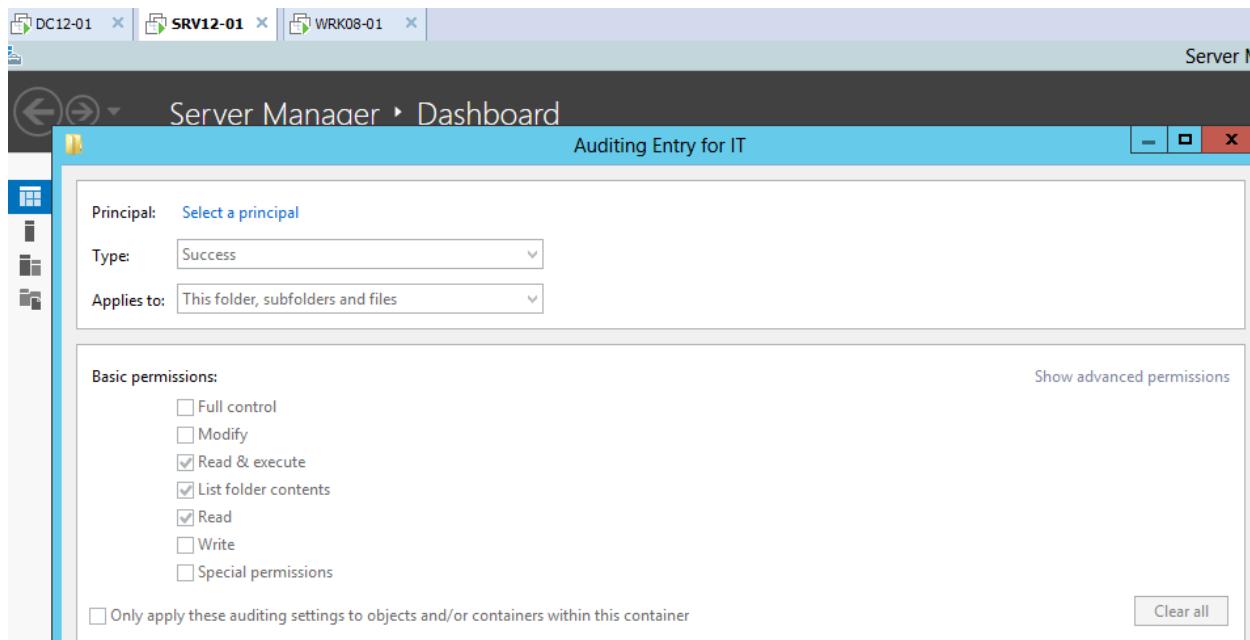
- Vào ô C của máy **SRV12-01**. Tạo thư mục **HN**, trong thư mục **HN**, tạo 2 thư mục **IT** và **Sale**.
- Tiến hành chia sẻ, phân quyền 2 thư mục **IT** và **Sale**(xem lại bài Lab 10.1)



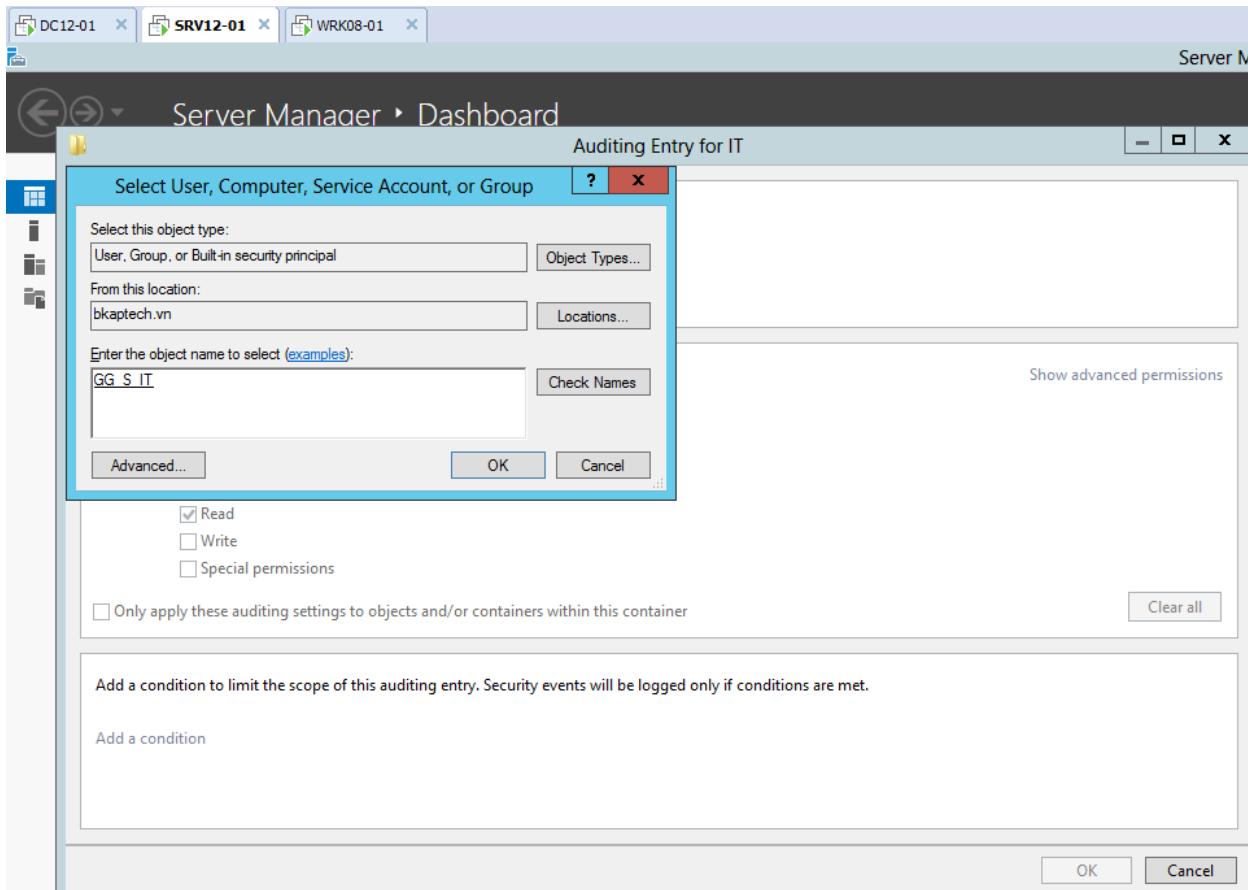
- Cấu hình ghi lại hoạt động của thư mục:
 - Trong cửa sổ **Advanced Security Settings for IT**, chuyển sang tab **Auditing**, tại đây click vào **Add**.



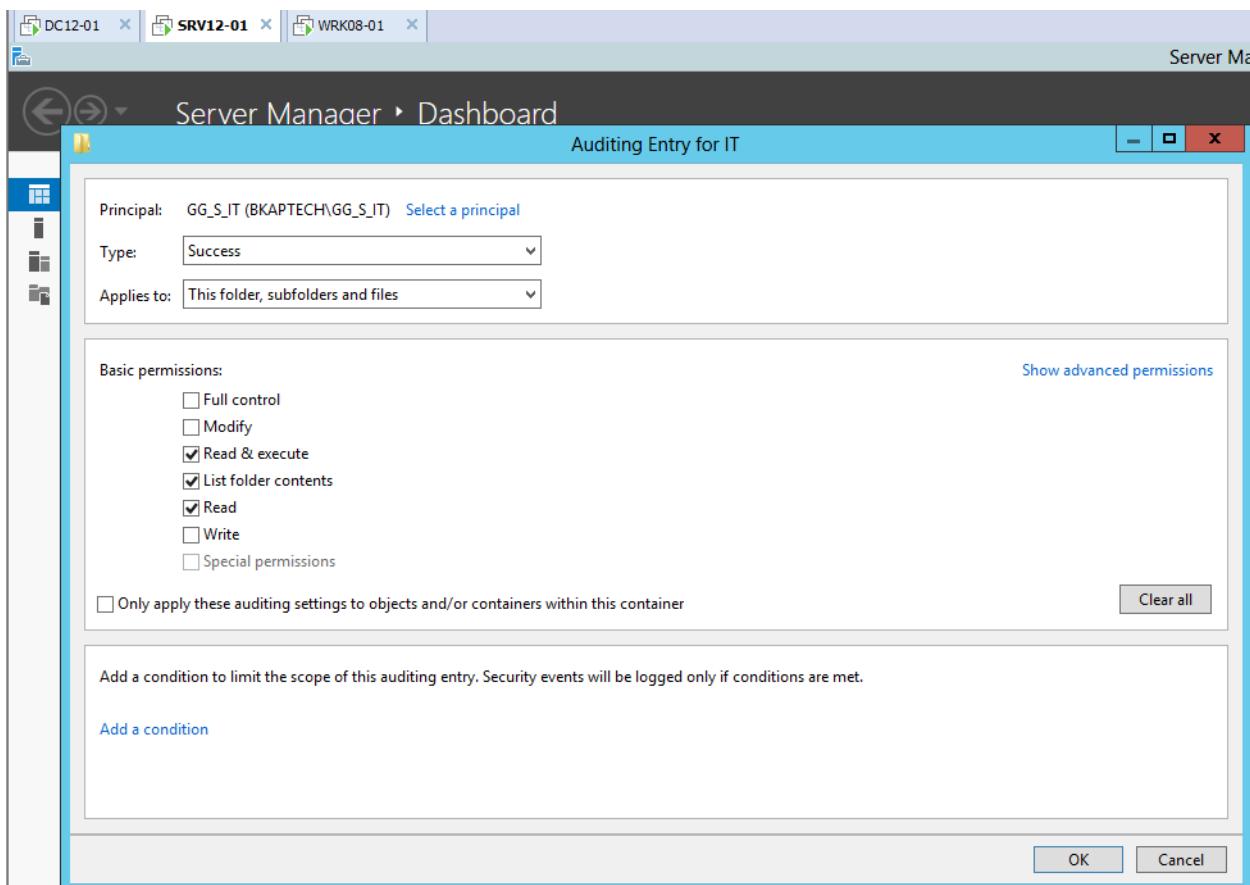
- Tại cửa sổ **Auditing Entry for IT**, click vào dòng chữ xanh **Select a principal**.



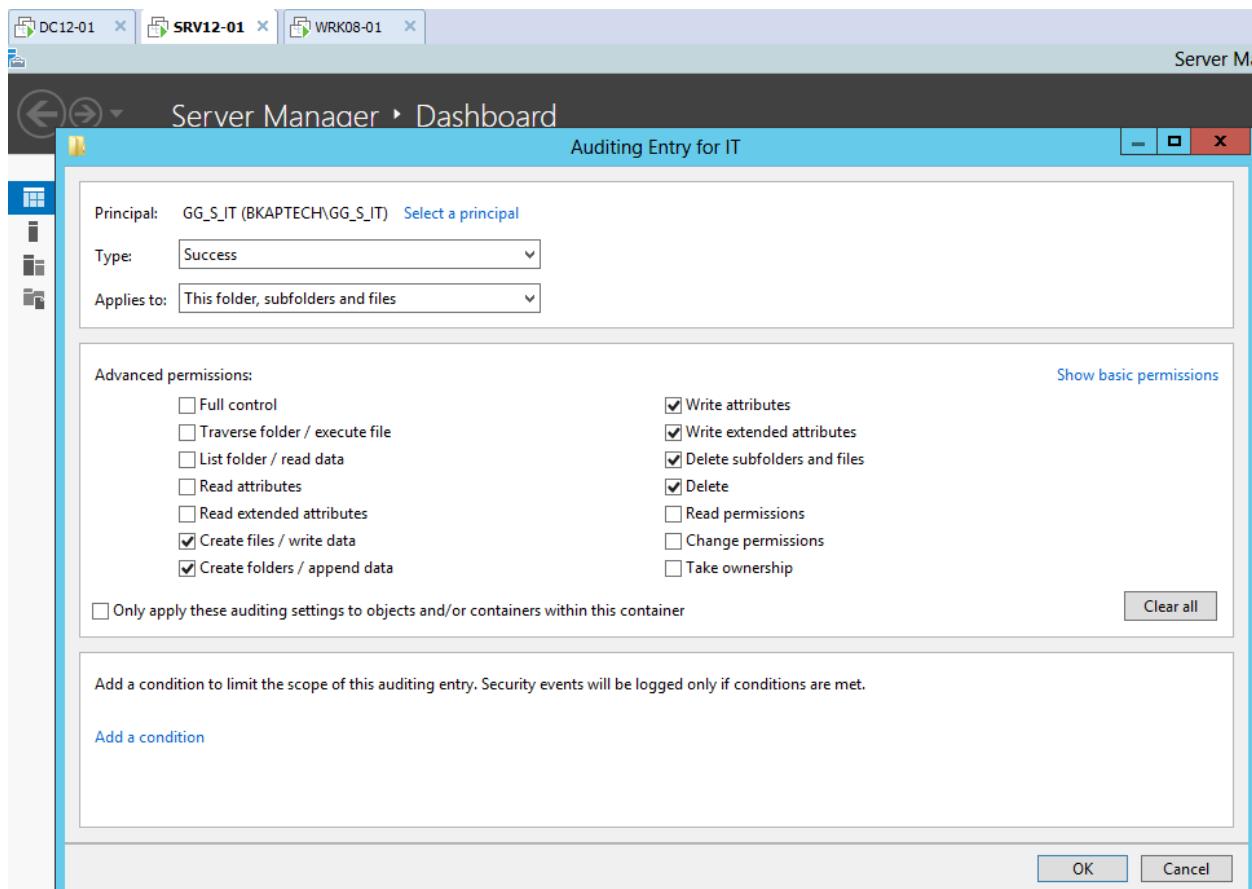
- Tại cửa sổ **Select User, Computer ...** thêm vào group **GG_S_IT**.



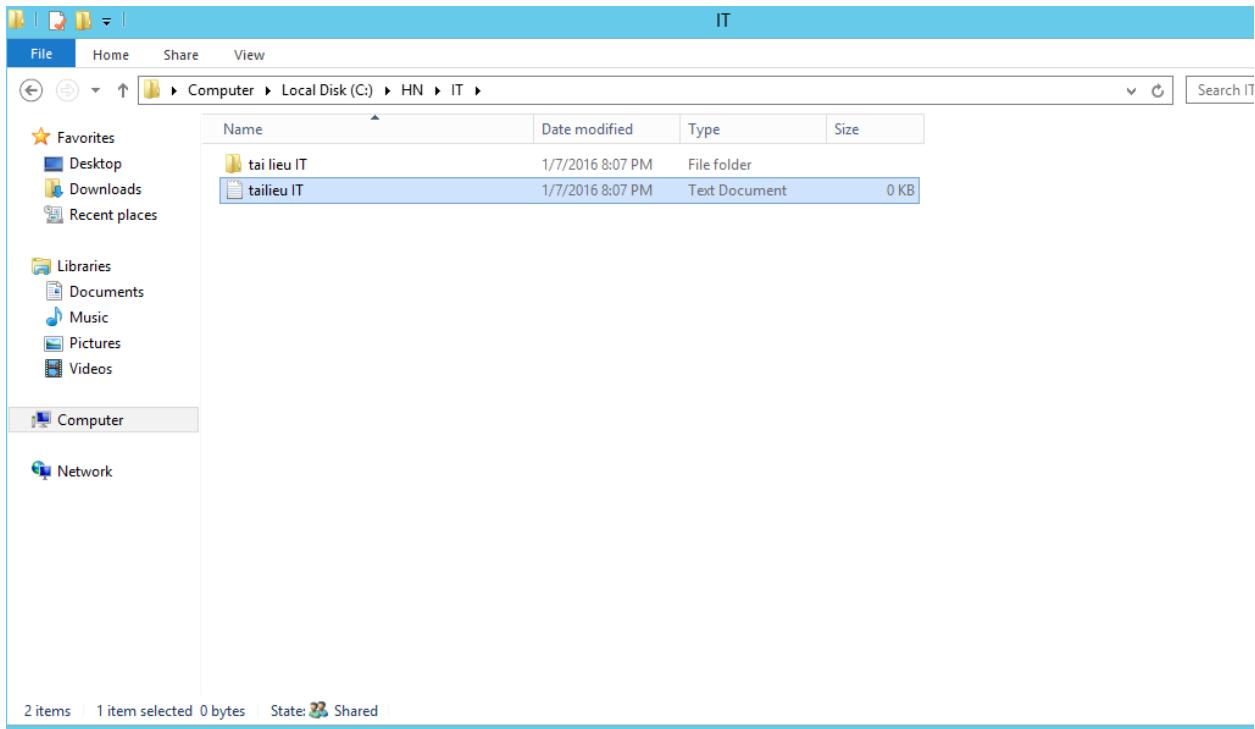
- Chọn vào dòng chữ xanh **Show advanced permissions.**



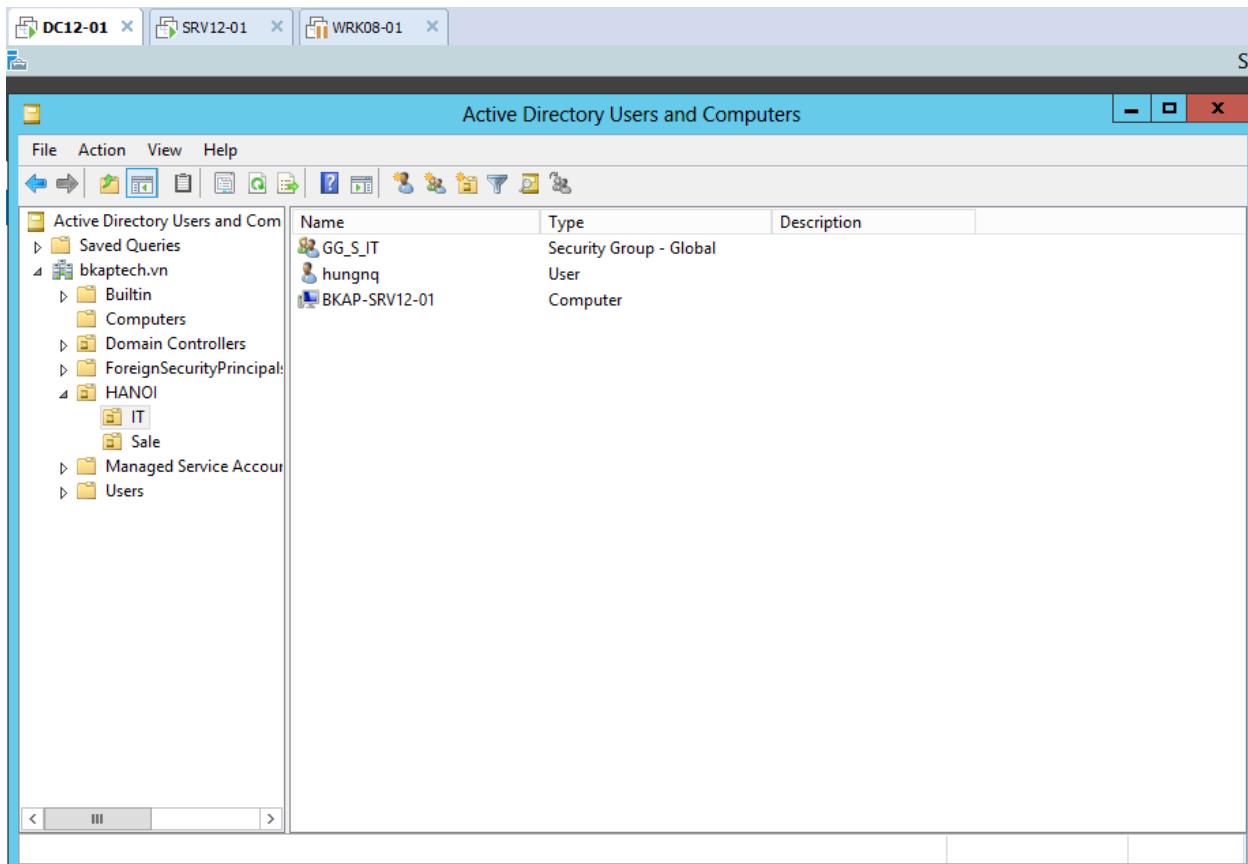
- Tại cửa sổ *Advanced permissions*, bỏ chọn các quyền đã được tích dấu, chọn vào các quyền sau:
 - *Create file / write data*
 - *Create folders / append data*
 - *Write attributes*
 - *Write extended*
 - *Delete subfolder*
 - *Delete*.
- OK.



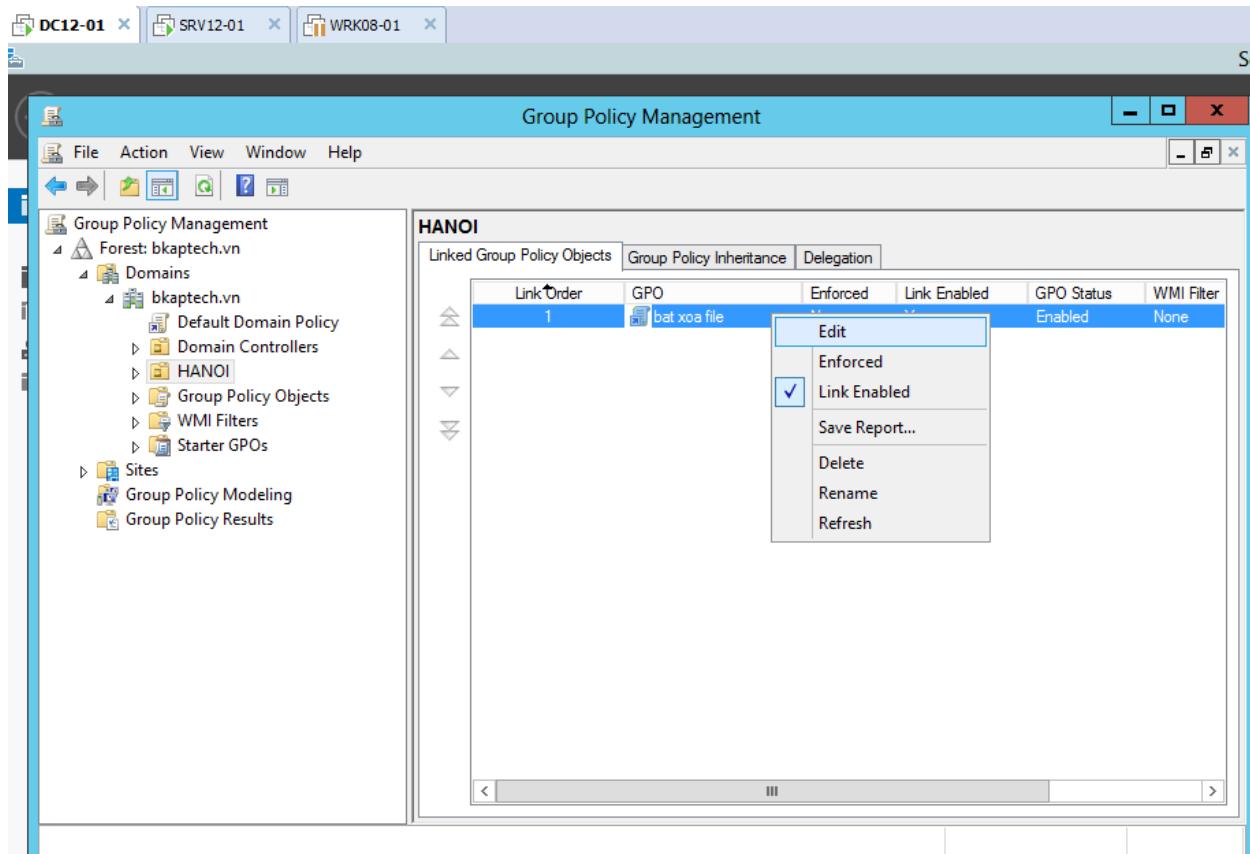
- Trong thư mục **IT**, tạo các thư mục và các file con để kiểm tra.



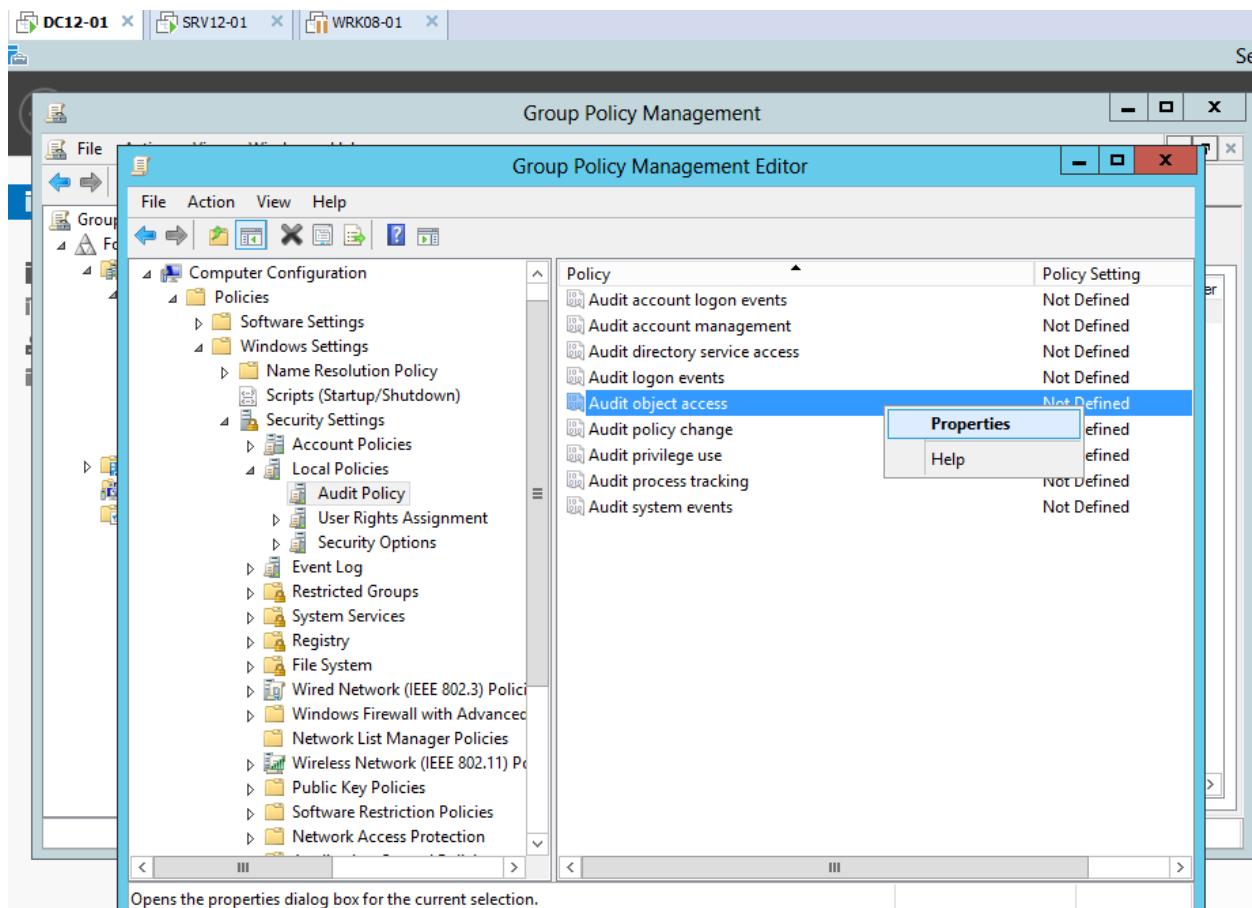
- Chuyển sang máy **Domain Controller** triển khai chính sách ghi lại hoạt động của thư mục.
 - Vào dịch vụ *Active Directory User and Computer*, di chuyển máy **BKAP-SRV12-01** vào OU **IT**.



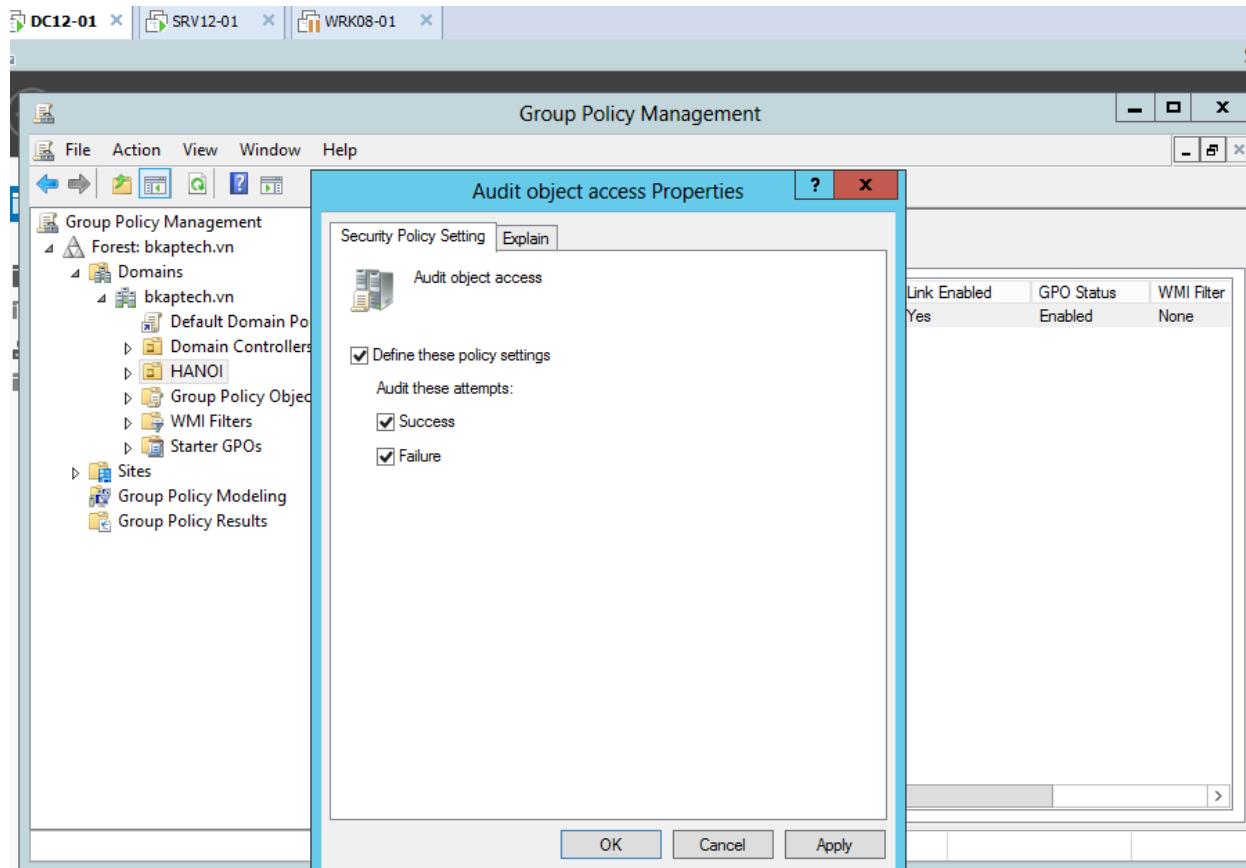
- Triển khai chính sách xóa File trong các phòng ban:
 - Vào **Group Policy Management**.
 - Tại OU **HANOI**, tạo 1 chính sách tên “*bắt xóa file*”.
 - Click chuột phải tại chính sách vừa tạo, chọn Edit.



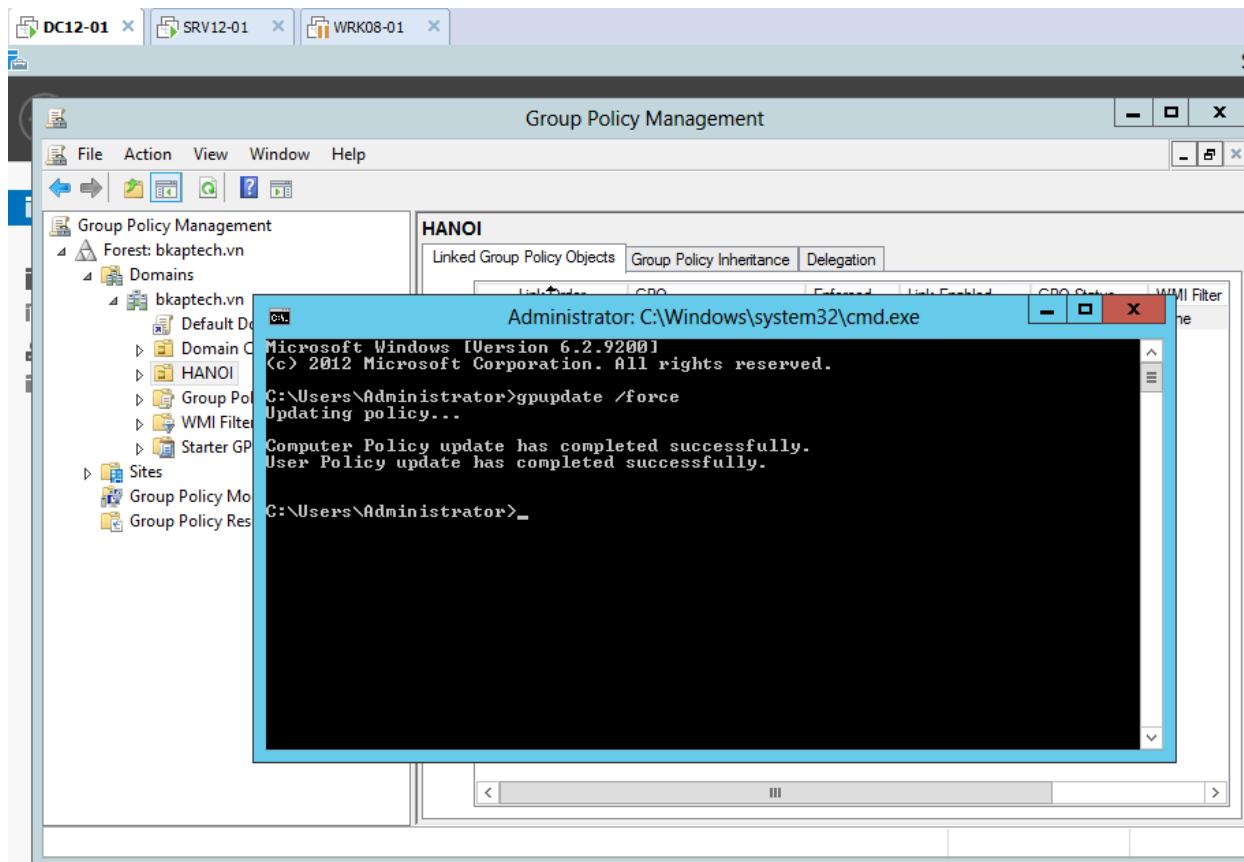
- Trong cửa sổ **Group policy Management Editor**, click vào **Computer Configuration / Policies / Windows Settings / Security Settings / Local Policies / Audit Policy**.
 - Chọn chính sách **Audit object access**.
 - Click chuột phải tại chính sách này, chọn **Properties**.



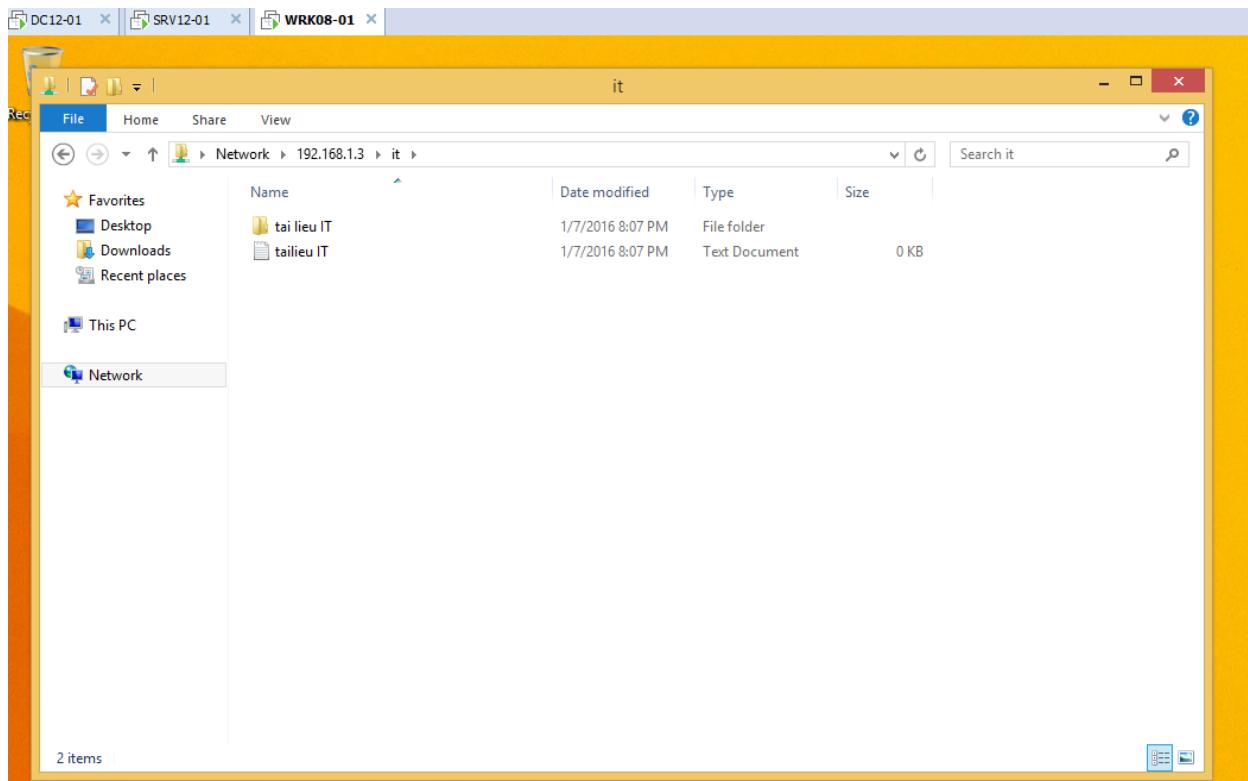
- Tại cửa sổ **Audit object access Properties**, click chọn vào **Define these policy settings** và 2 tùy chọn **Success , Failure**.
- Apply / OK.



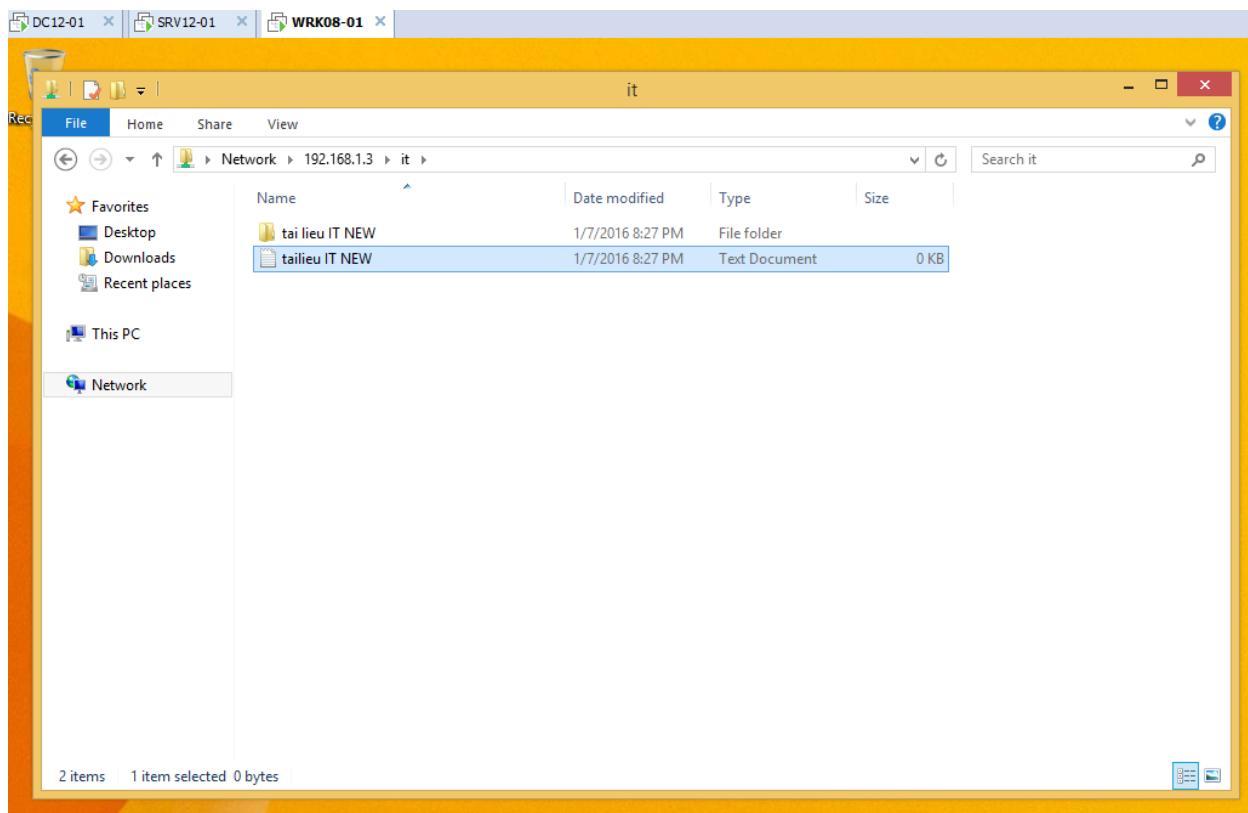
- Sử dụng lệnh **gpupdate /force** trong **cmd** để áp dụng chính sách.



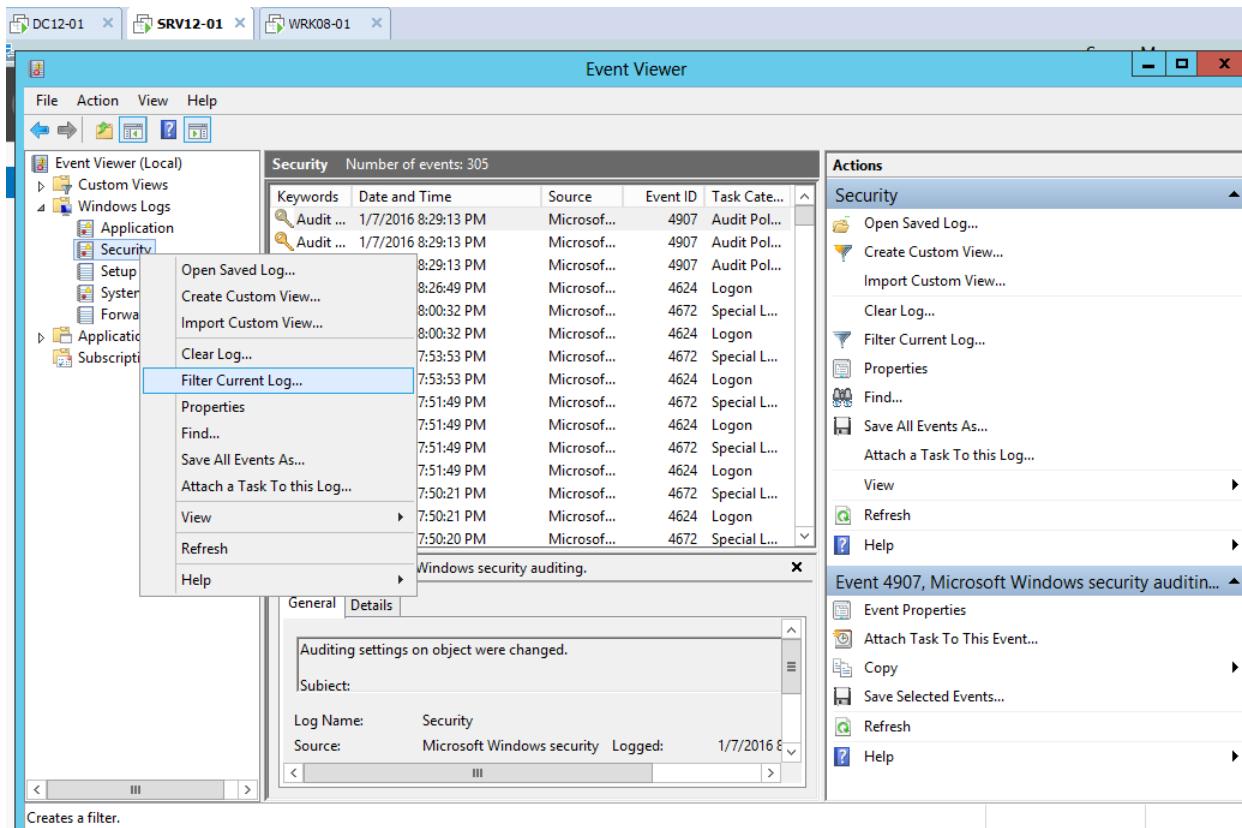
- Chuyển sang máy *Client Win 8*, Join vào Domain, đăng nhập bằng tài khoản **hungnq** trong phòng ban **IT**, truy cập vào thư mục **IT**, xóa File cũ, tạo File mới.



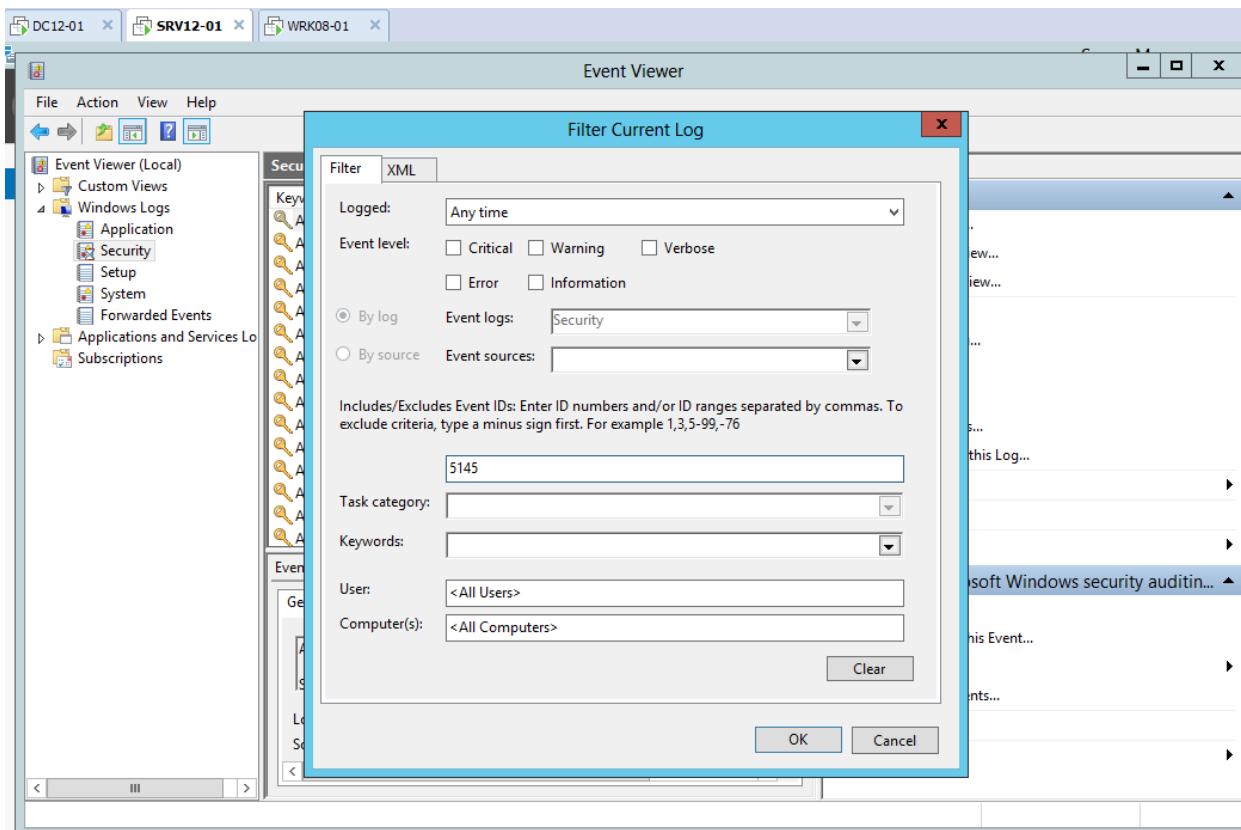
- Xóa file cũ, tạo File mới.



- Chuyển sang máy BKAP-SRV12-01 kiểm tra xóa file:
 - Vào **Event Viewer**.
 - Trong cửa sổ **Event Viewer**, click chọn **Windows Log / Security**
 - Click chuột phải tại **Security** / chọn **Filter Current Log**.



- Tại cửa sổ **Filter Current Log**, nhập vào ID 5145, tiến hành kiểm tra.



11.3 Triển khai chính sách (GPO) giới hạn sử dụng phần mềm.

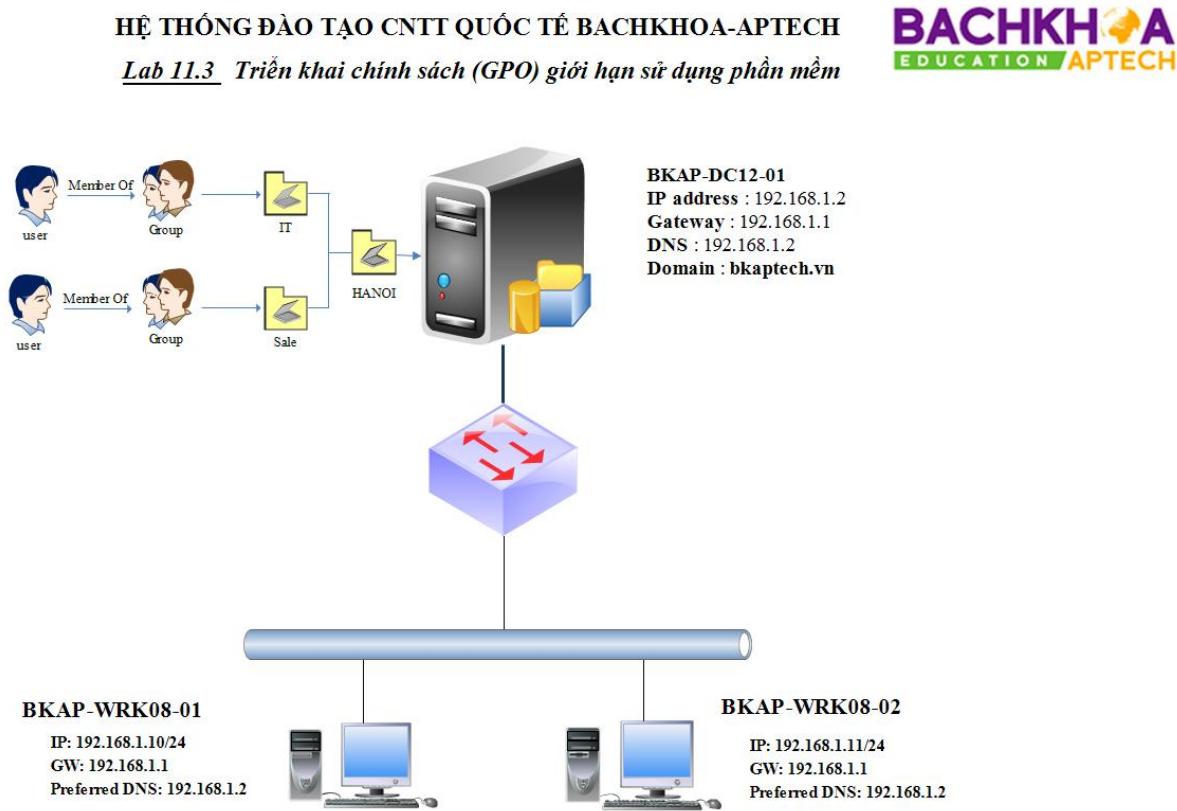
1. Yêu cầu bài Lab:

- + Tạo OU, tài khoản người dùng và Group theo miền.
- + Triển khai chính sách chặn phần mềm Firefox.
- + Sử dụng tài khoản trong miền kiểm tra truy cập sau khi chặn dịch vụ.

2. Yêu cầu chuẩn bị:

- + Máy BKAP-DC12-01 dùng để tạo OU, Group, User, quản lý miền **bkaptech.vn**
- + Máy BKAP-WRK08-01 Join vào miền dùng để kiểm tra.

3. Mô hình Lab:



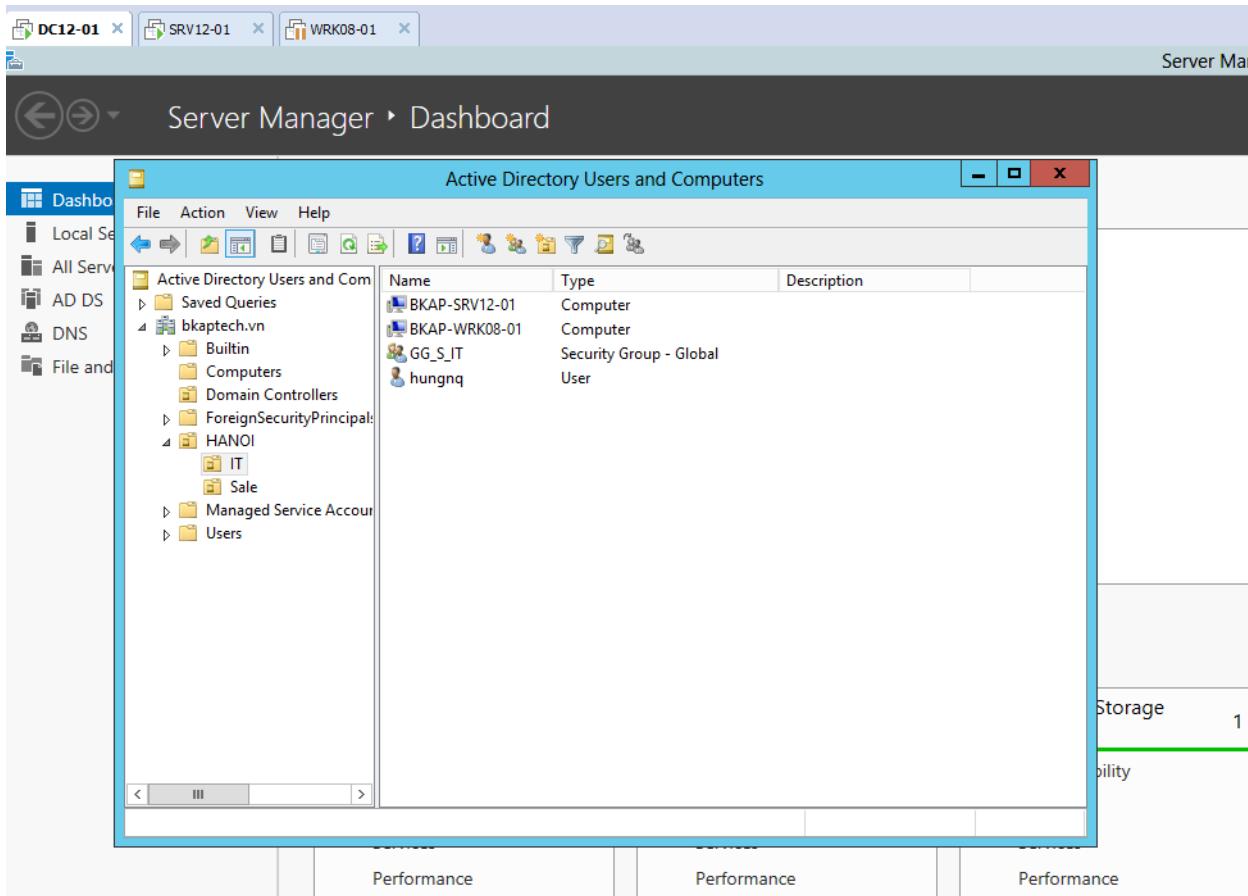
Hình 11.3

Sơ đồ địa chỉ như sau:

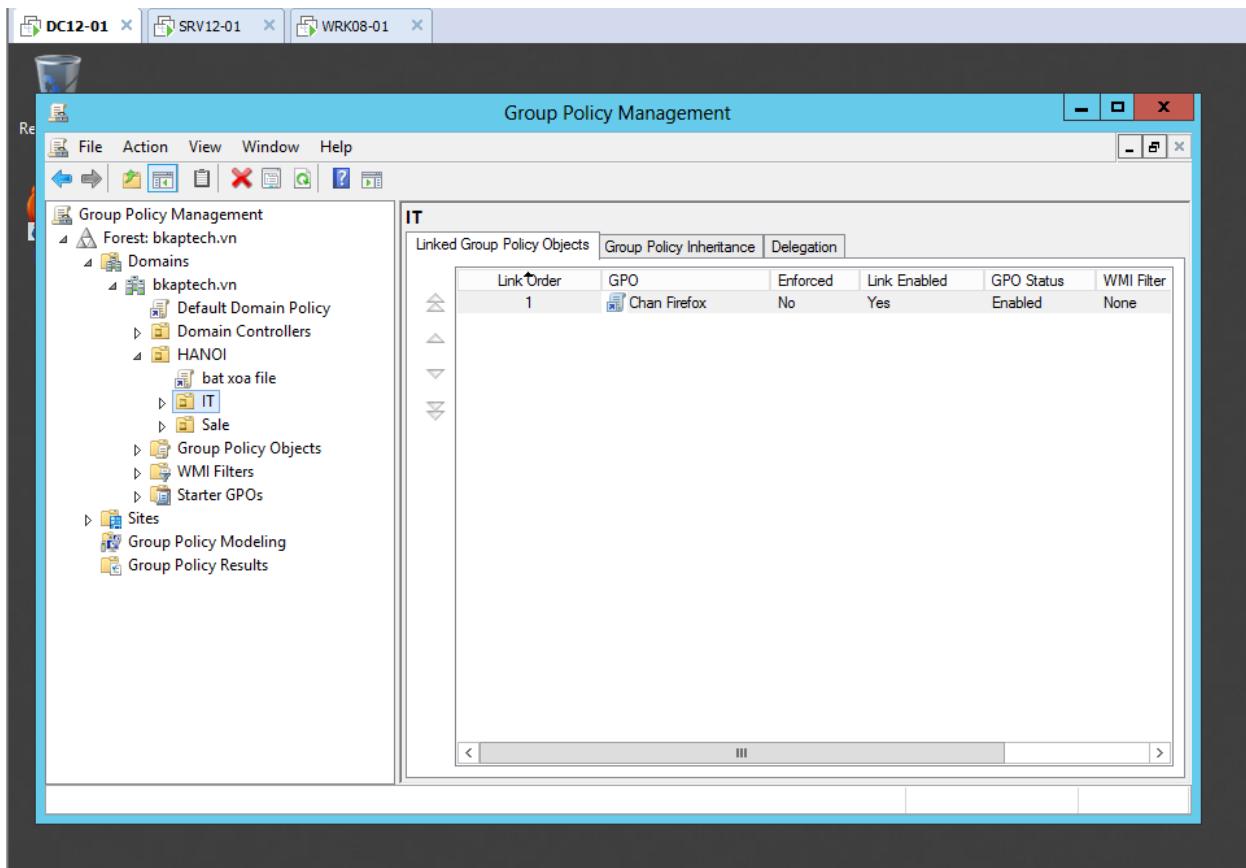
Thông số	BKAP-DC12-01	BKAP-SRV12-01
<i>IP address</i>	192.168.1.2	192.168.1.10
<i>Subnet Mask</i>	255.255.255.0	255.255.255.0
<i>Gateway</i>	192.168.1.1	192.168.1.1
<i>DNS Server</i>	192.168.1.2	192.168.1.2

Hướng dẫn chi tiết:

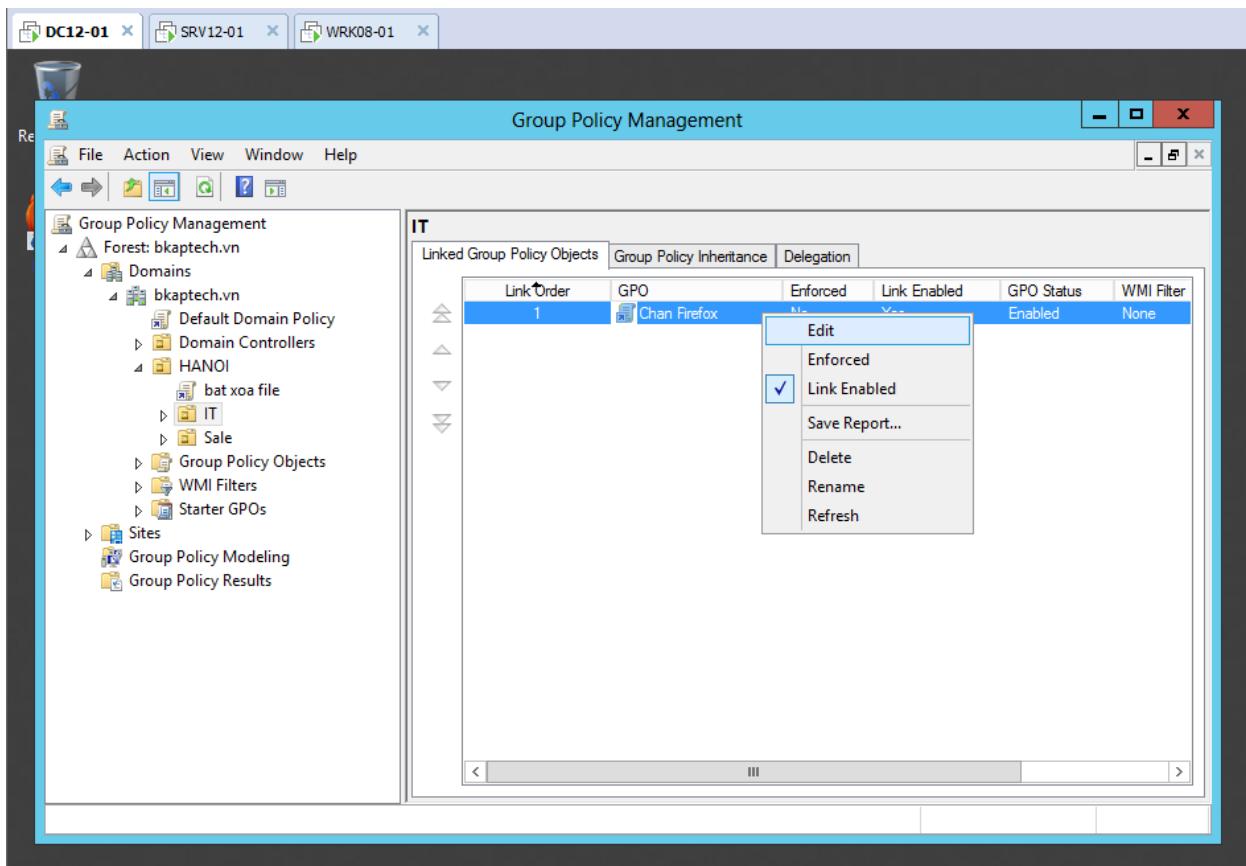
- Trên máy *BKAP-DC12-01*, tạo OU, Group, User , Add User vào Group
 - Di chuyển máy Client vào OU IT



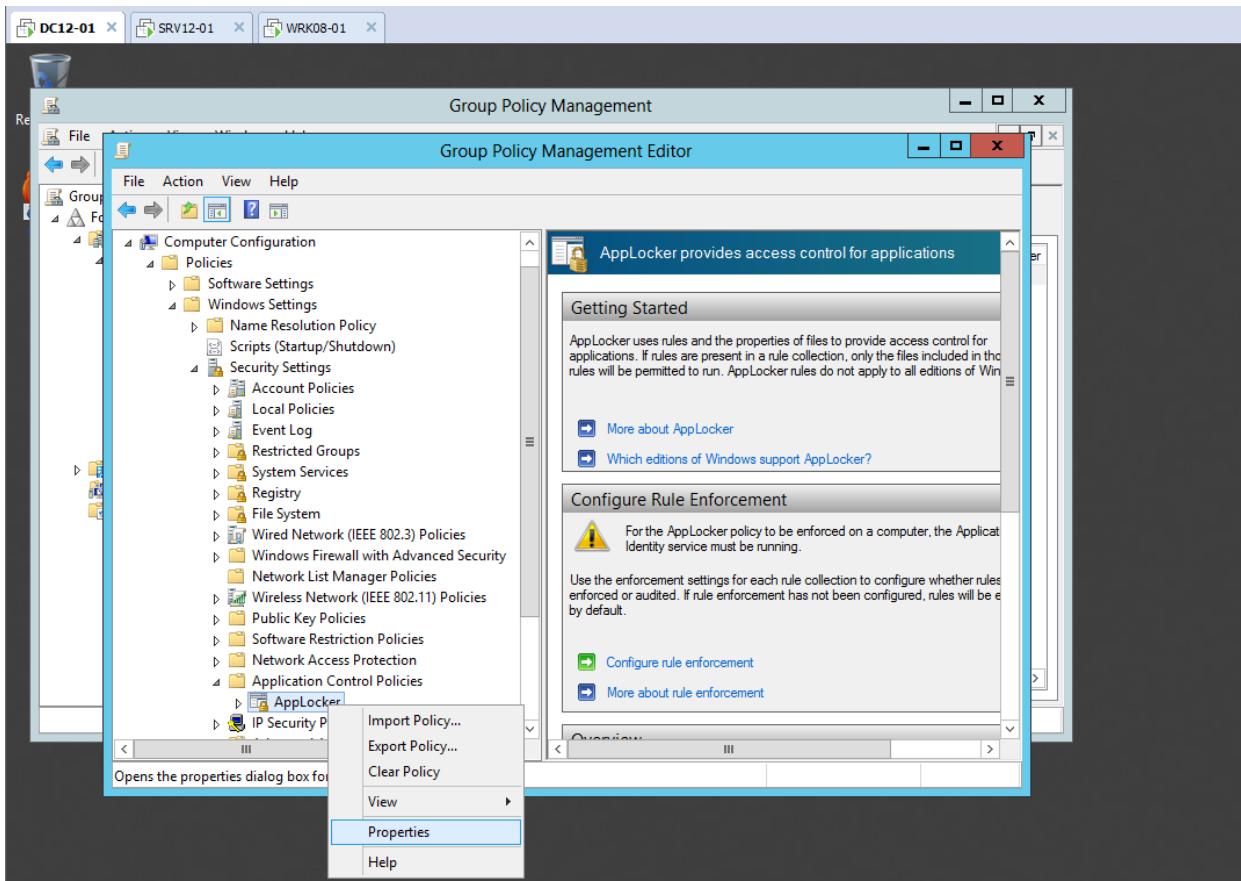
- Tạo chính sách chặn phần mềm Firefox.
 - Tại cửa sổ **Group Policy Management**, tạo chính sách “**Chặn Firefox**” cho phòng ban IT.



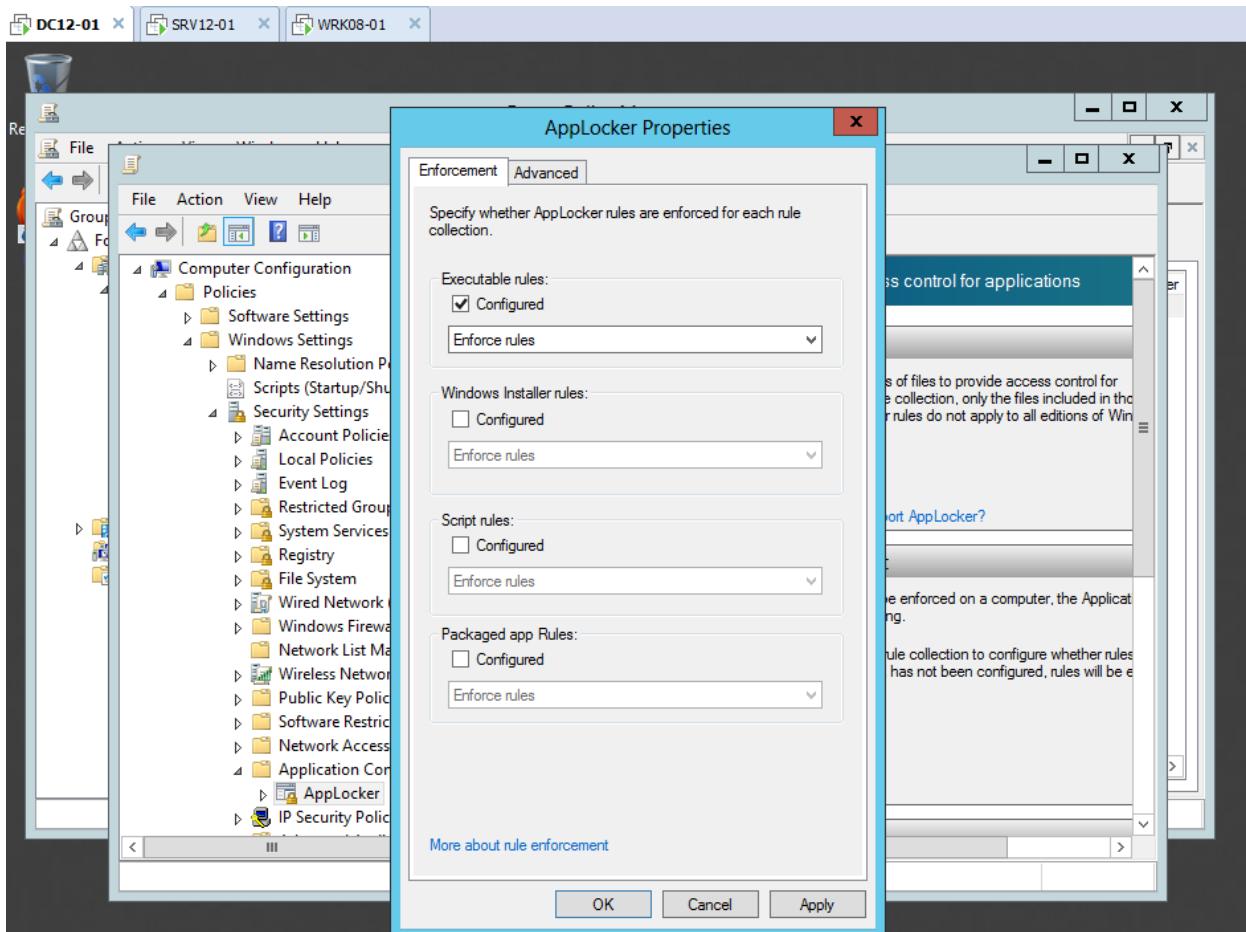
- Click chuột phải tại chính sách vừa tạo, chọn **Edit**.



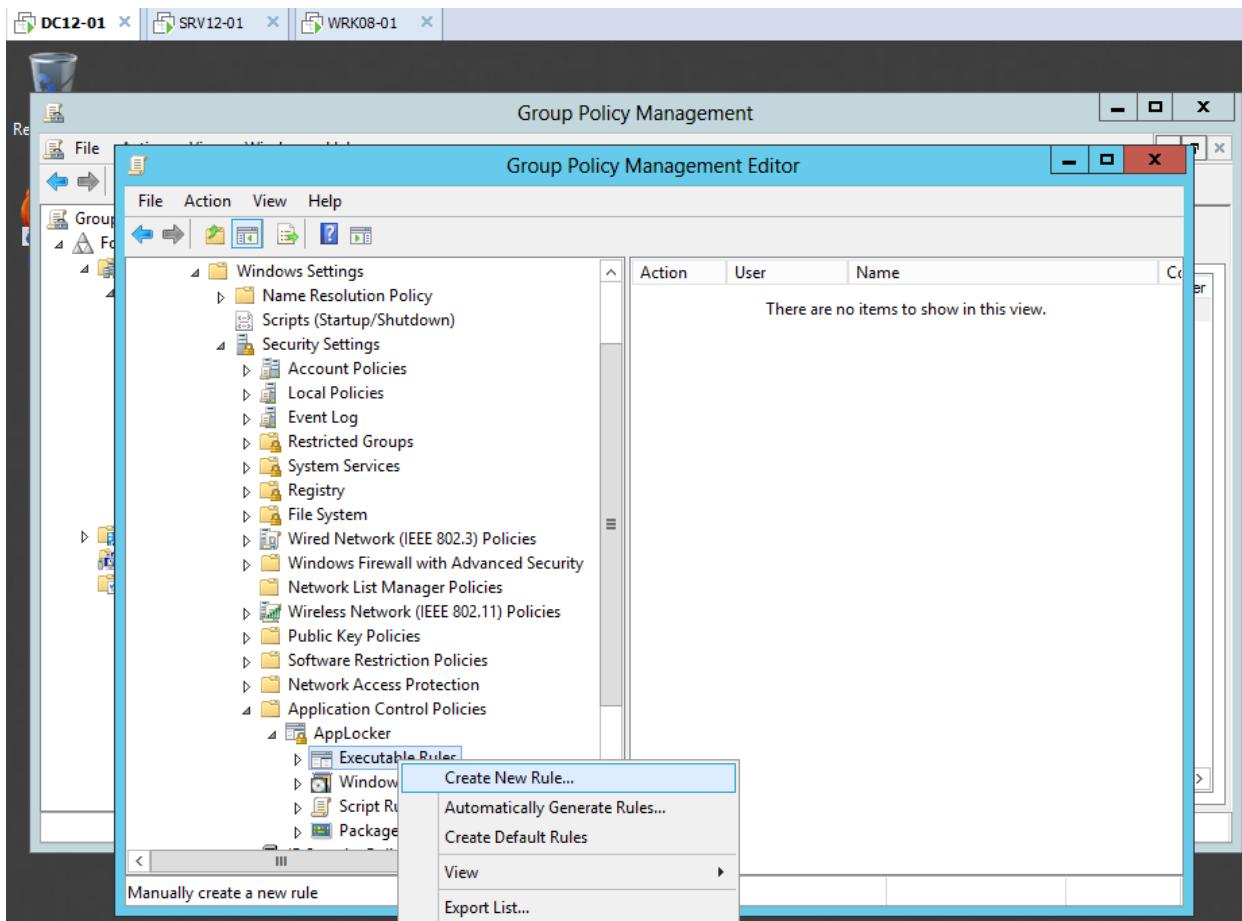
- Tại cửa sổ **Group Policy Management Editor**, chọn vào **Computer Configuration / Policies / Windows Settings / Security Settings / Application Control Policies / Applocker**
 - Click chuột phải tại **Applocker** chọn **Properties**.



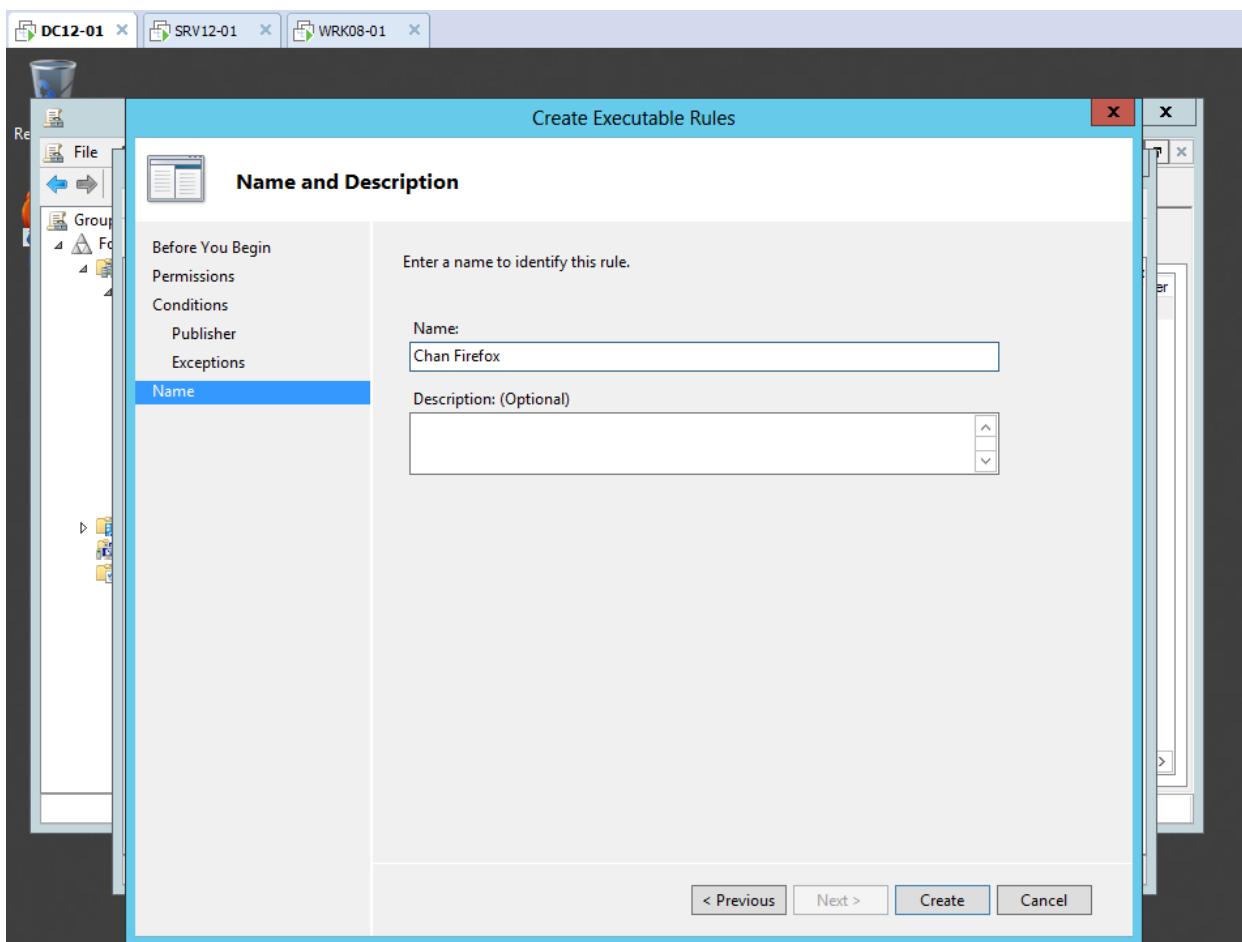
- Tại cửa sổ **Applocker Properties / Tab Enforcement** , Tích vào **Configured** tại **Executable rules / OK**.



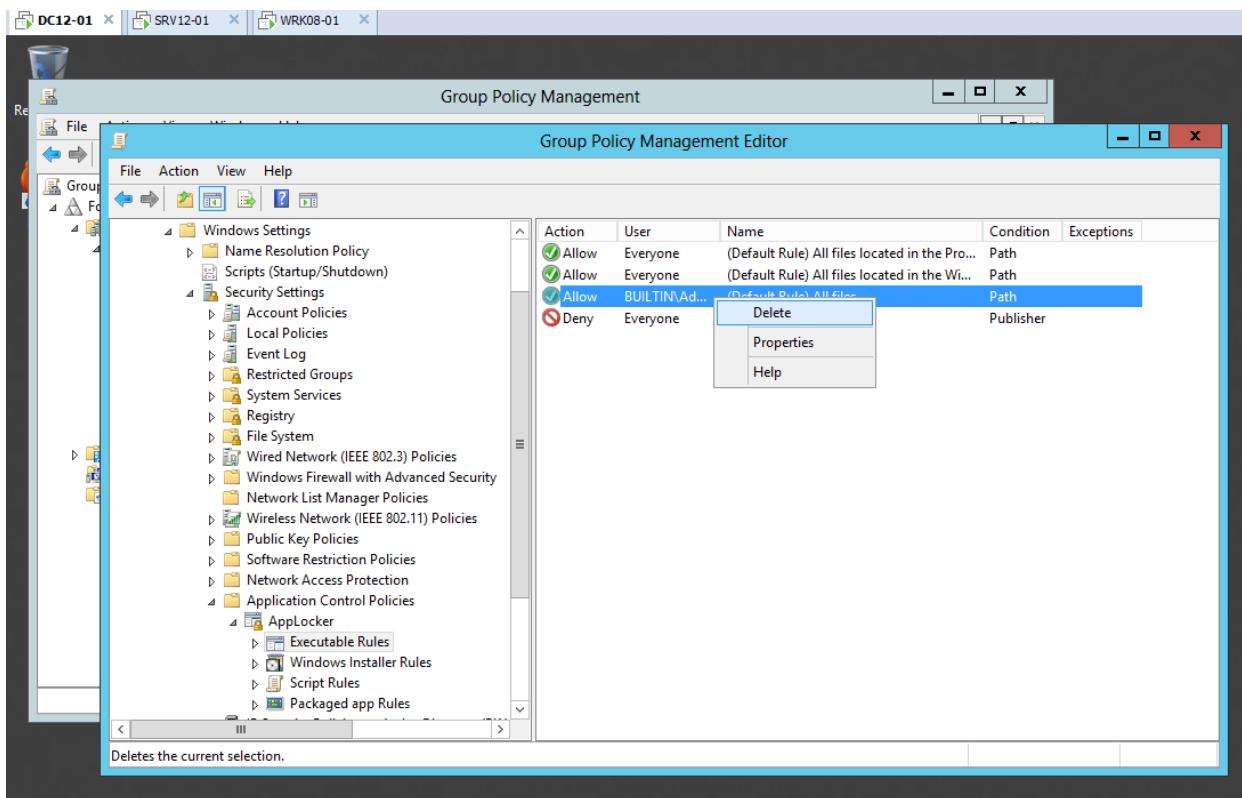
- Click vào Applocker / Executable Rules , click chuột phải chọn Create New Rule...



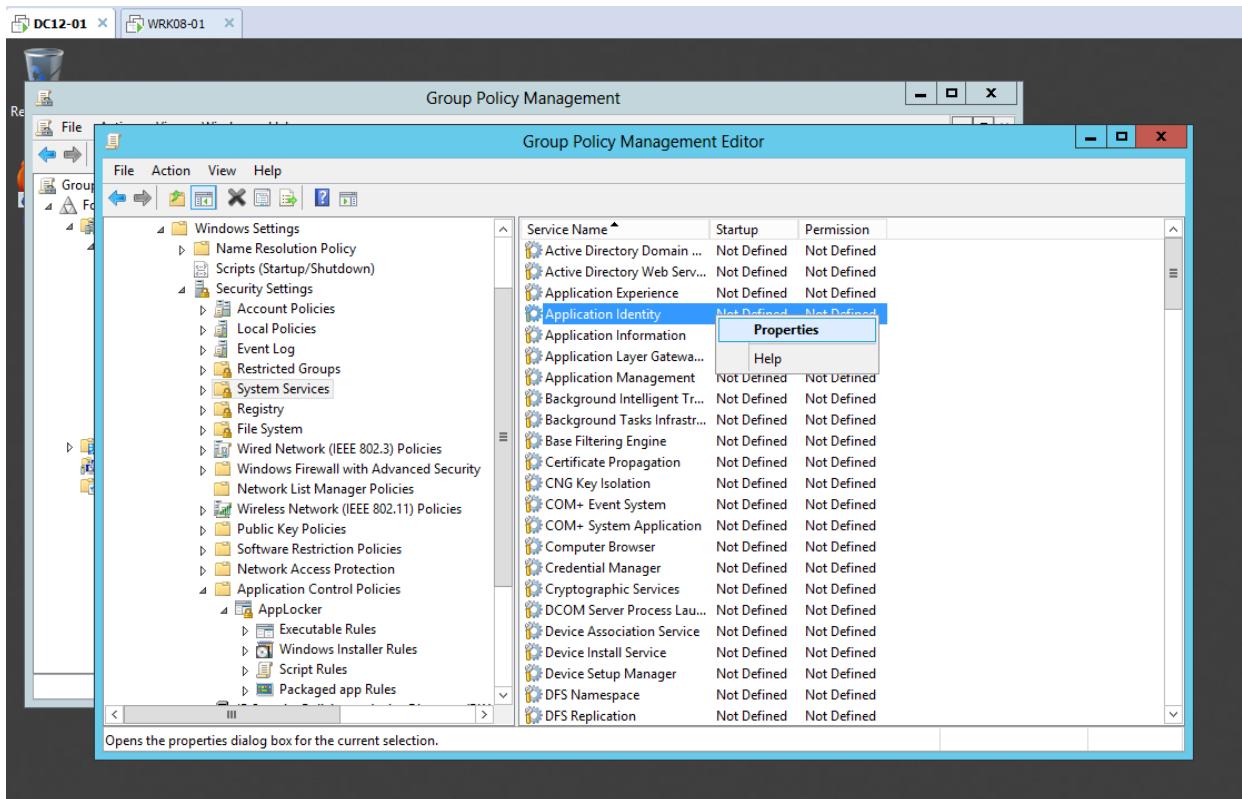
- Tại cửa sổ **Create Executable Rules / Permissions** :
 - Action : Deny
- Tại cửa sổ **Publisher**, Browse đến “firefox” trong ô C
 - Kéo con trỏ ở dưới lên phần **Any publisher**.
 - **Next.**
- Tại cửa sổ **Name and Description** nhập vào:
 - Name : Chan Firefox.
 - **Create.**



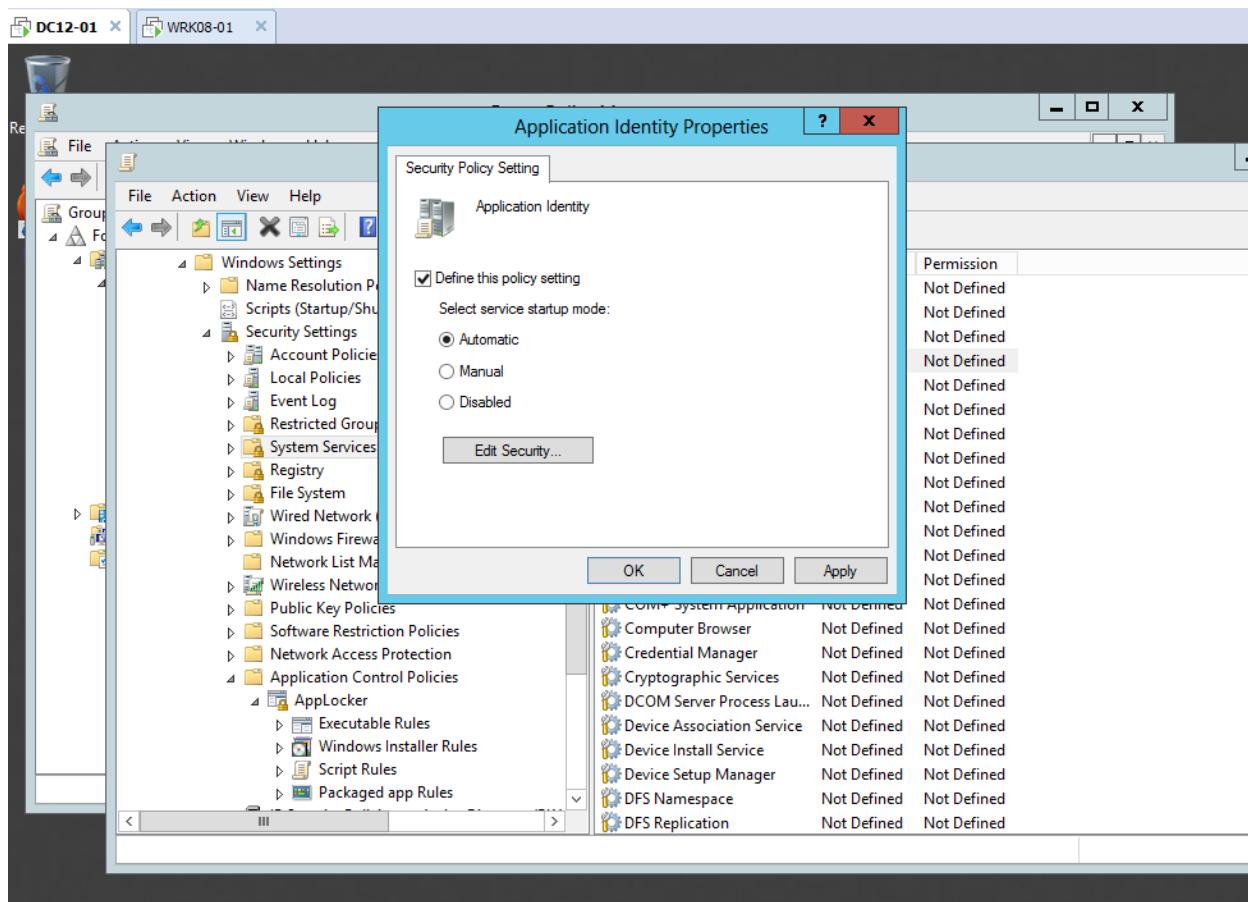
o Xóa Rule BUILTIN\Administrator ...



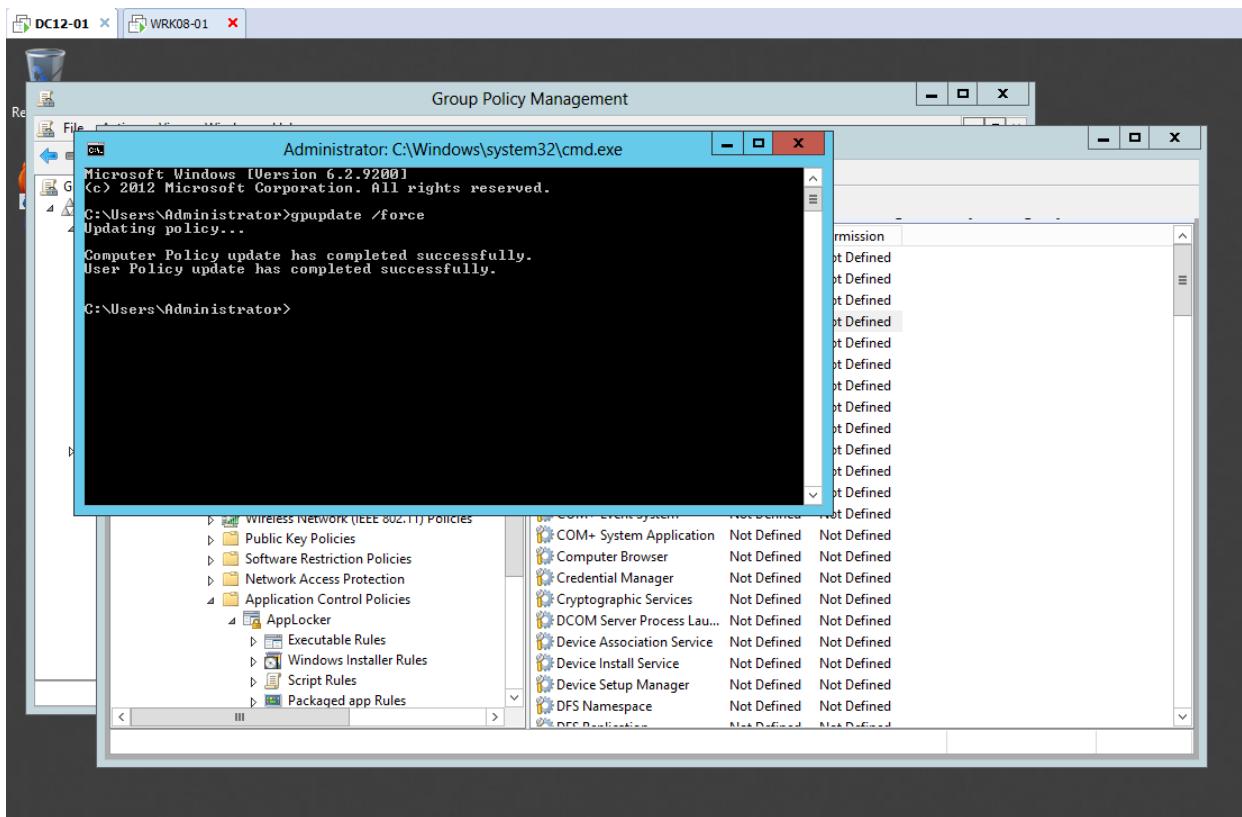
- Tại **Group Policy Management / Computer Configuration / ... Security Settings / System Services** , chọn vào **Application Identity**.
 - Click chuột phải tại **Application Identity**, chọn **Properties**.



- Tại cửa sổ **Application Identity Properties**, chọn vào Automatic.



- Sử dụng câu lệnh **gpupdate /force** trong **cmd** để áp dụng chính sách.



- Chuyển sang máy Client Win 8, đăng nhập bằng tài khoản **hungnq** trong phòng ban IT để kiểm tra

