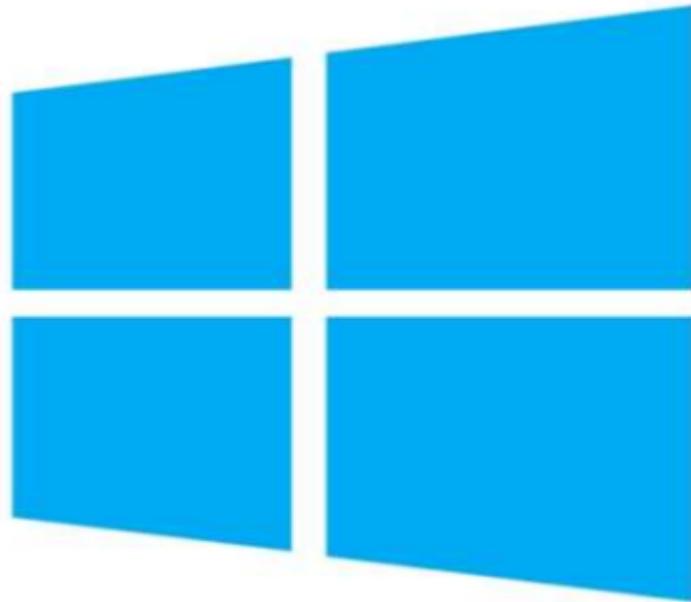


QUẢN TRỊ HỆ THỐNG MẠNG WINDOWS SERVER 2012 PHẦN 2



WINDOWS SERVER 2012

MỤC LỤC

Bài 1: TRIỂN KHAI WINDOWS DEPLOYMENT SERVICES (WDS).....	4
1.1 Cài đặt và cấu hình Windows Deployment Services (WDS).....	4
1.2 Triển khai cài đặt Windows 8 tự động qua mạng LAN.....	29
Bài 2: TRIỂN KHAI DỊCH VỤ INTERNET INFORMATION SERVICES (IIS)	31
2.1 Cấu hình IIS với Single Website.....	31
2.2 Cấu hình IIS Multi Website kết hợp với DNS Server.....	39
2.3 Sử dụng Active Directory Certificate Services để bảo mật Web Server.	50
Bài 3: TRIỂN KHAI DỊCH VỤ ACTIVE DIRECTORY (TIẾP).....	77
3.1 Triển khai cài đặt và cấu hình RODC.	77
3.2 Cấu hình AD DS snapshots.....	106
3.3 Khôi phục tài khoản người dùng bằng Active Directory Recycle Bin	124
BÀI 4: CHÍNH SÁCH TÀI KHOẢN NGƯỜI DÙNG.	131
4.1 Cấu hình chính sách khóa tài khoản người dùng.	131
4.2 Cấu hình chính sách “Fine-grained Password” cho từng phòng ban.	152
Bài 5: CẤU HÌNH MAP NETWORK DRIVE , MAP PRINTER BẰNG VBSCRIPT.	168
Bài 6: CẤU HÌNH FOLDER REDIRECTION.....	187
Bài 7: TRIỂN KHAI CÀI ĐẶT VÀ CẤU HÌNH DỊCH VỤ VPN SERVER	207
7.1 Triển khai cấu hình dịch vụ VPN Server (Client to Site)	207
7.2 Triển khai cài đặt và cấu hình dịch vụ VPN (Site to Site).	234
7.3 Triển khai cài đặt và cấu hình dịch vụ VPN Server (Client to Site) –SSTP	276
Bài 8: TRIỂN KHAI DỊCH VỤ NETWORK POLICY SERVER	339
8.1 Triển khai cài đặt và cấu hình dịch vụ VPN Server kết hợp với RADIUS.....	339
8.2 Triển khai cài đặt và cấu hình dịch vụ VPN Server kết hợp với NPS.	359
8.3 Triển khai cài đặt và cấu hình dịch vụ VPN Server kết hợp với RADIUS và NPS....	378
Bài 9: TRIỂN KHAI DỊCH VỤ NETWORK ACCESS PROTECTION.....	409
9.1 Triển khai cài đặt và cấu hình dịch vụ NAP DHCP.....	409

9.2 Triển khai cài đặt và cấu hình dịch vụ NAP VPN.	443
Bài 10: TRIỂN KHAI DỊCH VỤ FILE SERVICES	540
10.1 Cấu hình Quota, File Screening và Tạo thống kê lưu trữ.	540
10.2 Triển khai cài đặt và cấu hình dịch vụ DFS (Distributed File System)	565
10.3 Đồng bộ dữ liệu trên 2 Server sử dụng DFS Replication.....	581
Bài 11: CẤU HÌNH MÃ HÓA FILE , AUDITING NÂNG CAO.....	597
11.1 Cấu hình mã hóa File.	597
11.2 Cấu hình Auditing nâng cao.....	626

Bài 1:**TRIỂN KHAI WINDOWS DEPLOYMENT SERVICES (WDS).**

Các nội dung chính sẽ được đề cập:

- ✓ Cài đặt và cấu hình Windows Deployment Services (WDS).
- ✓ Triển khai cài đặt Windows tự động qua mạng LAN.

1.1 Cài đặt và cấu hình Windows Deployment Services (WDS).**1. Yêu cầu bài Lab:**

- + Trên máy *BKAP-DC12-01*, thực hiện cài đặt **DHCP Server**.
- + Trên máy *BKAP-SRV12-01*, triển khai cài đặt **Windows Deployment Services (WDS)**.
- + Chuẩn bị đĩa cài *Windows 8 Pro 32 bits* hoặc *64 bits*.

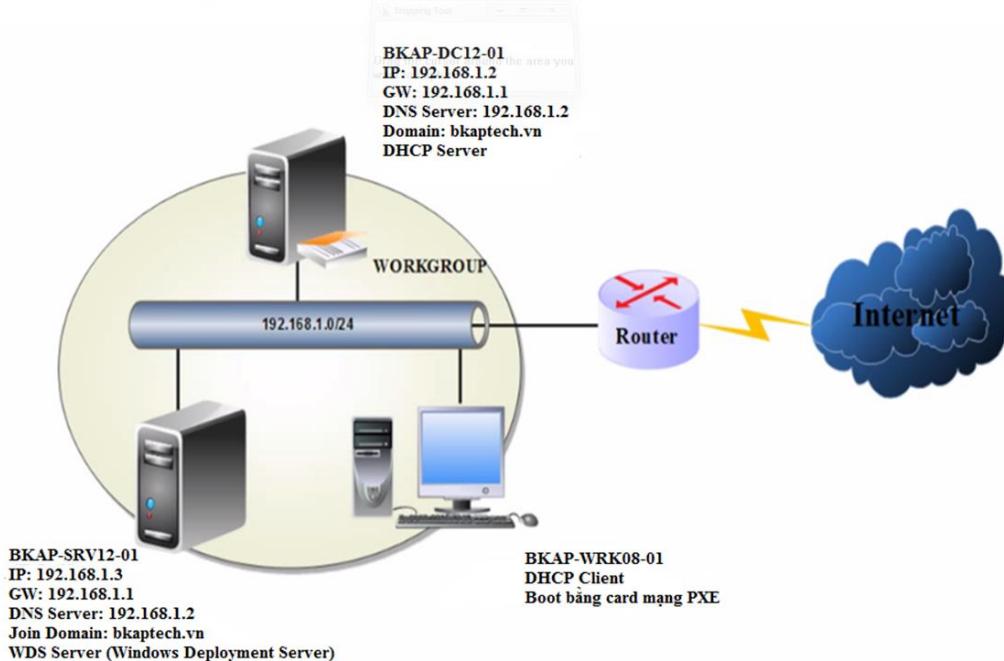
2. Yêu cầu chuẩn bị:

- + Máy *BKAP-DC12-01* : Domain Controller chạy *HDH Windows Server 2012* quản lý miền **bkaptech.vn** và đóng vai trò **DHCP Server**.
- + Máy *BKAP-SRV12-01* : Join vào Domain , đóng vai trò **WDS Server**.
- + Máy Client : chưa cài Hệ điều hành nào.

3. Mô hình Lab:

HỆ THỐNG ĐÀO TẠO CNTT QUỐC TẾ BACHKHOA-APTECH

Lab 1.1 Triển khai cài đặt và cấu hình Windows Deployment Services (WDS)



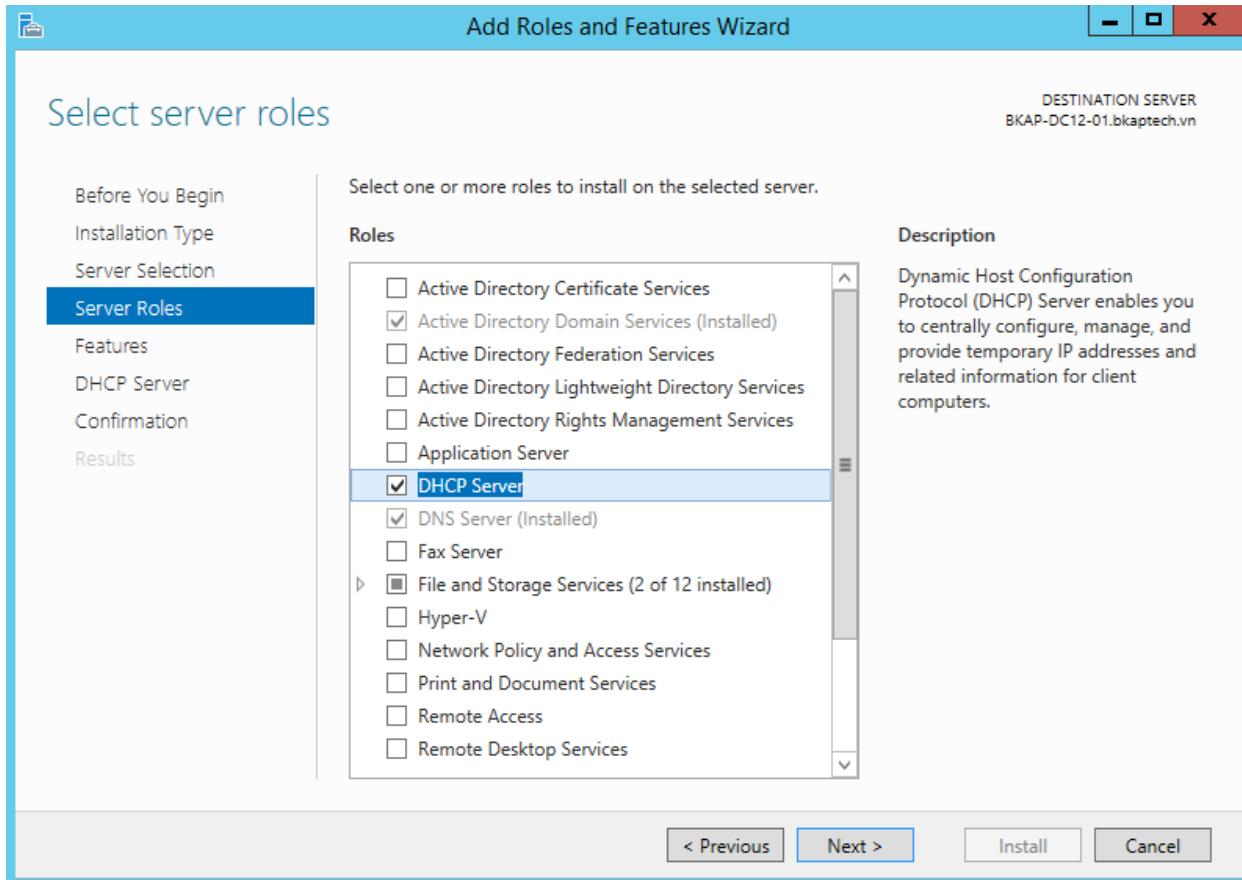
Hình 1.1

Sơ đồ địa chỉ như sau:

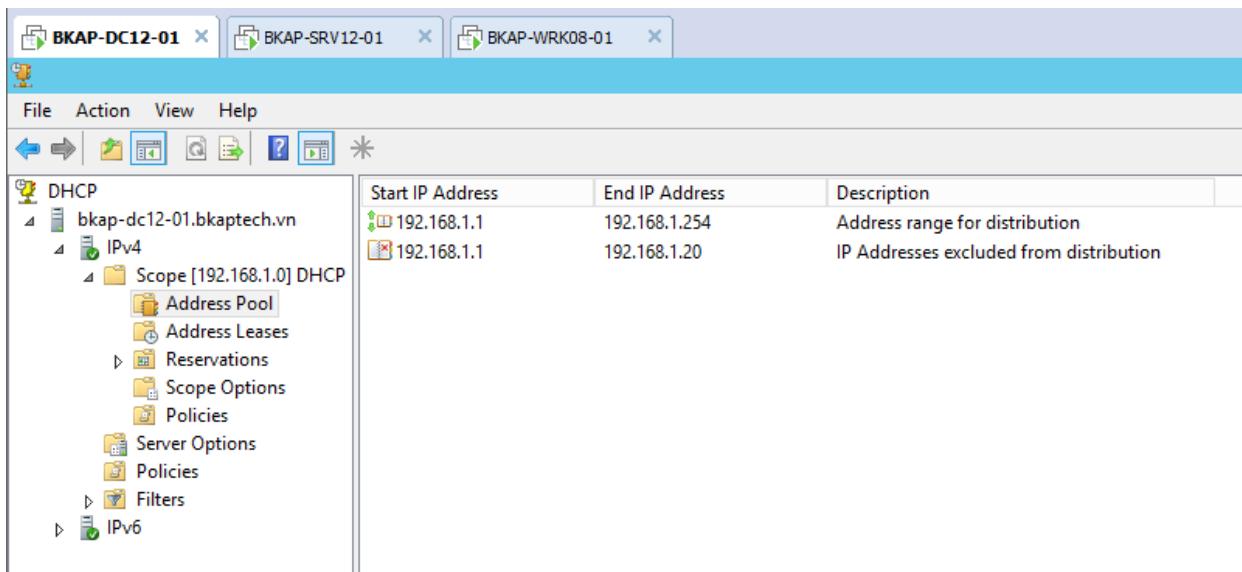
Thông số	BKAP-DC12-01	BKAP-SRV12-01	BKAP-WRK08-01
IP address	192.168.1.2	192.168.1.3	DHCP Client
Gateway	192.168.1.1	192.168.1.1	192.168.1.1
Subnet Mask	255.255.255.0	255.255.255.0	255.255.255.0
DNS Server	192.168.1.2	192.168.1.2	192.168.1.2

Hướng dẫn chi tiết:

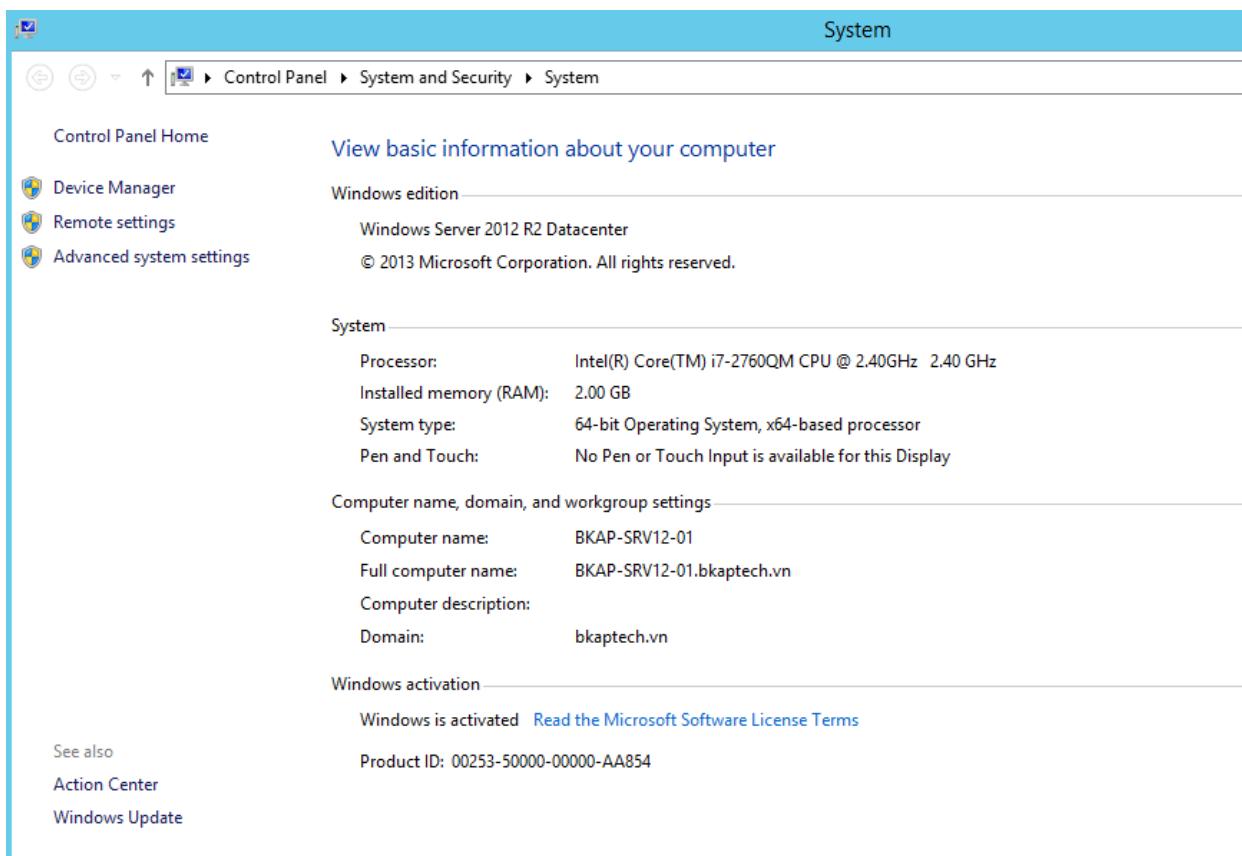
- Mở các máy ảo , kết nối như hình trên , thực hiện ping thông giữa các máy.
- Trên máy *BKAP-DC12-01* , thực hiện cài đặt và cấu hình **DHCP Server**.
 - Cài đặt **DHCP Server**.



- Cấu hình DHCP Server.

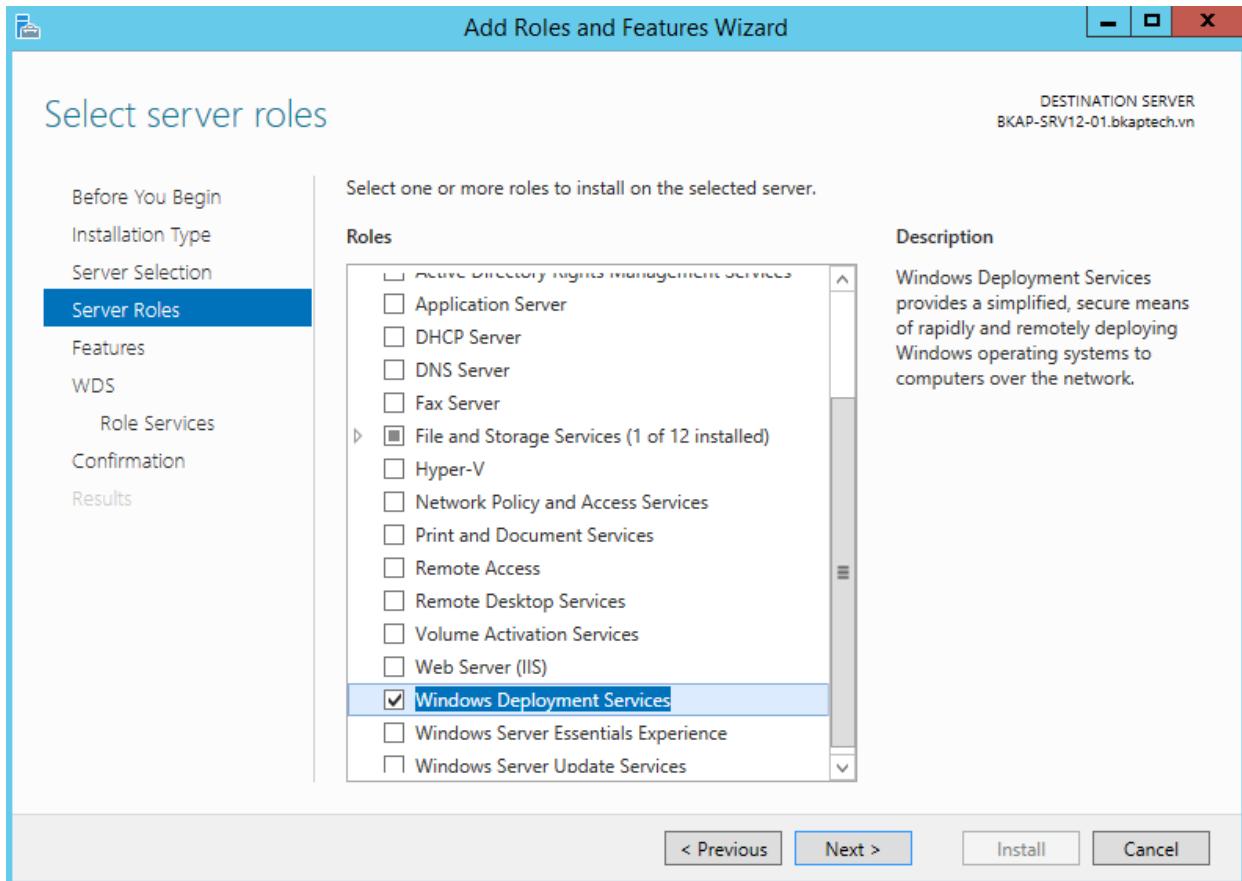


- Chuyển sang máy *BKAP-SRV12-01*, thực hiện:
 - Join vào Domain, đăng nhập bằng tài khoản **bkaptech\administrator**.

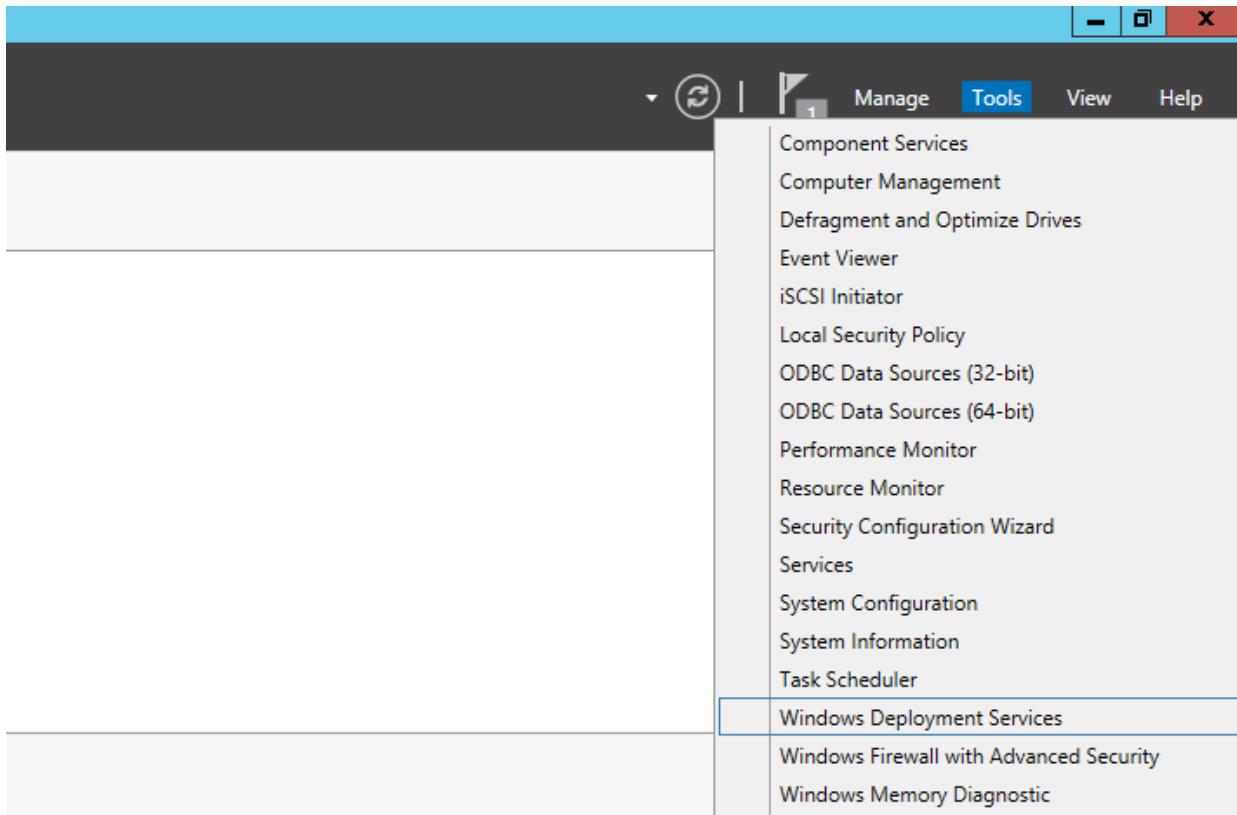


o Cài đặt và cấu hình dịch vụ WDS:

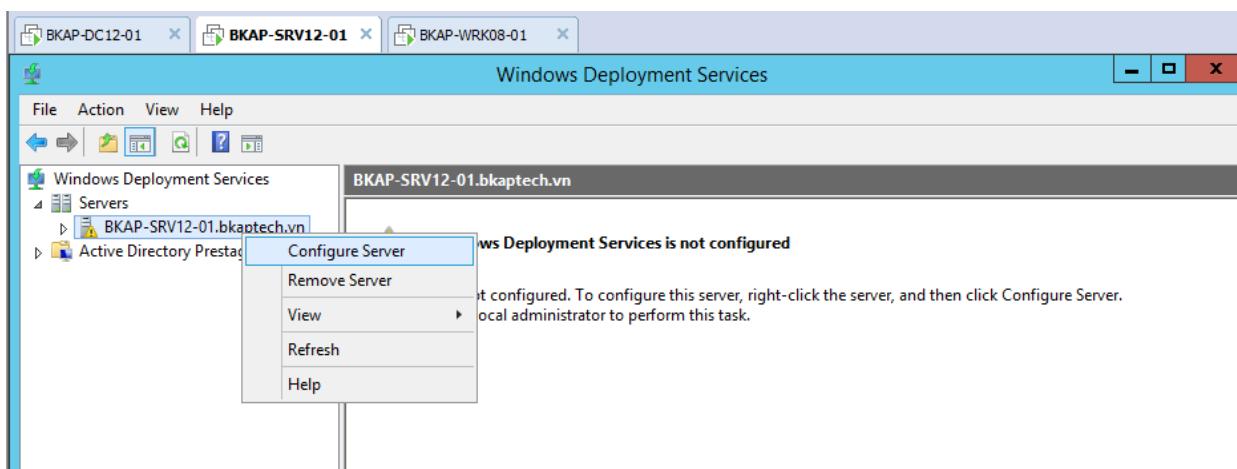
- Cài đặt dịch vụ WDS:



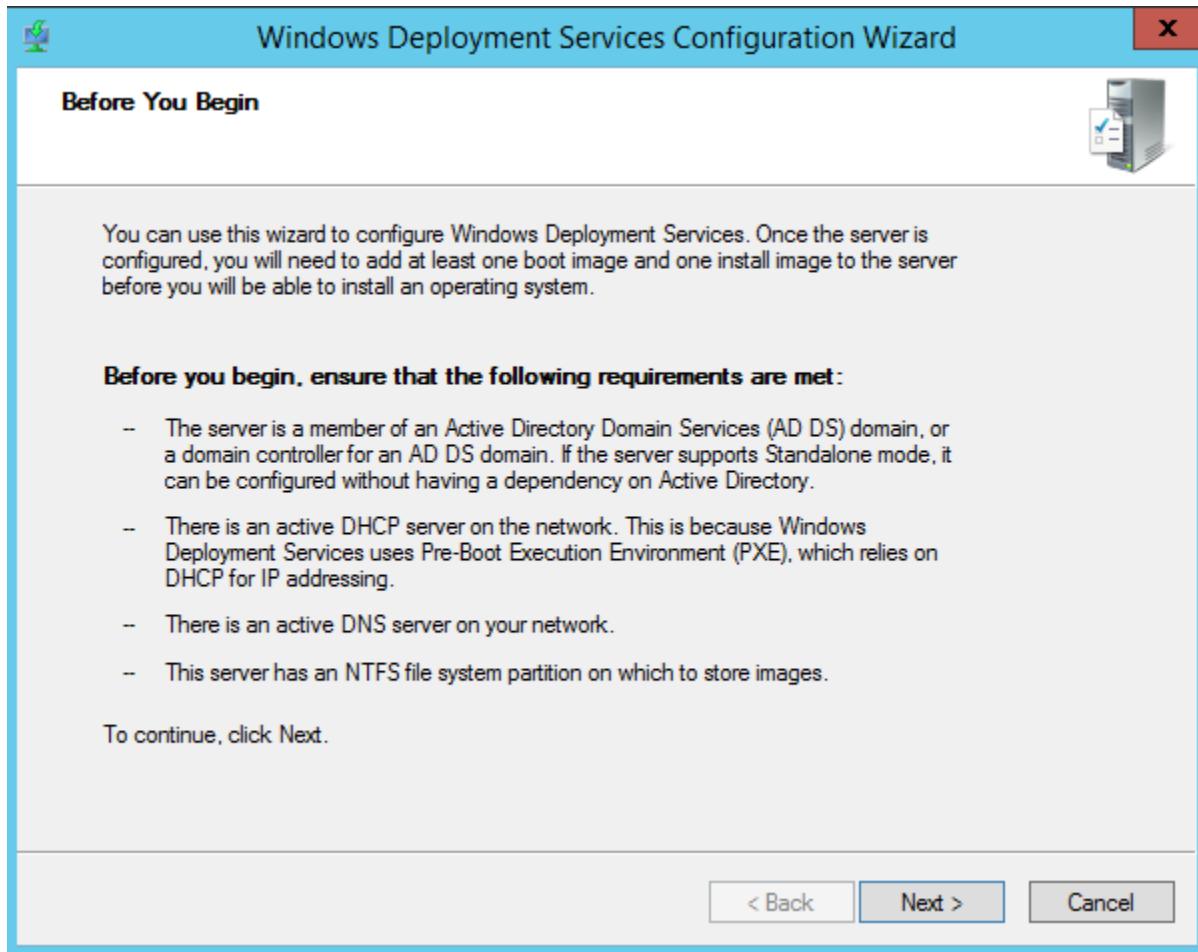
- Cấu hình dịch vụ WDS:
 - Trong cửa sổ **Server Manager**, click vào **Tools / Windows Deployment Services**.



- Trong cửa sổ **Windows Deployment Services**, click chuột phải vào Server chọn **Configure Server**.



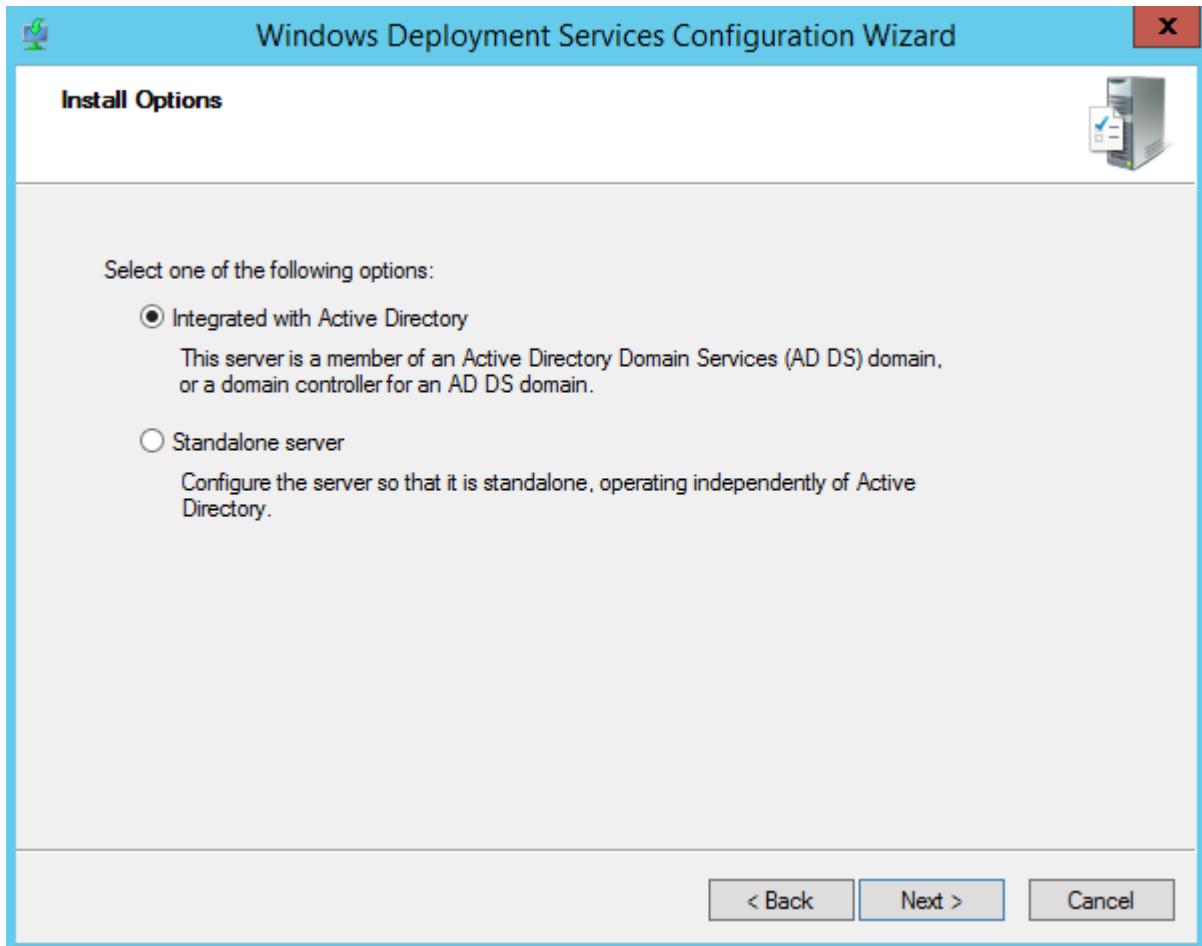
- Tại cửa sổ **Windows Deployment Services Configuration Wizard**, click vào Next.

**Before you begin, ensure that the following requirements are met:**

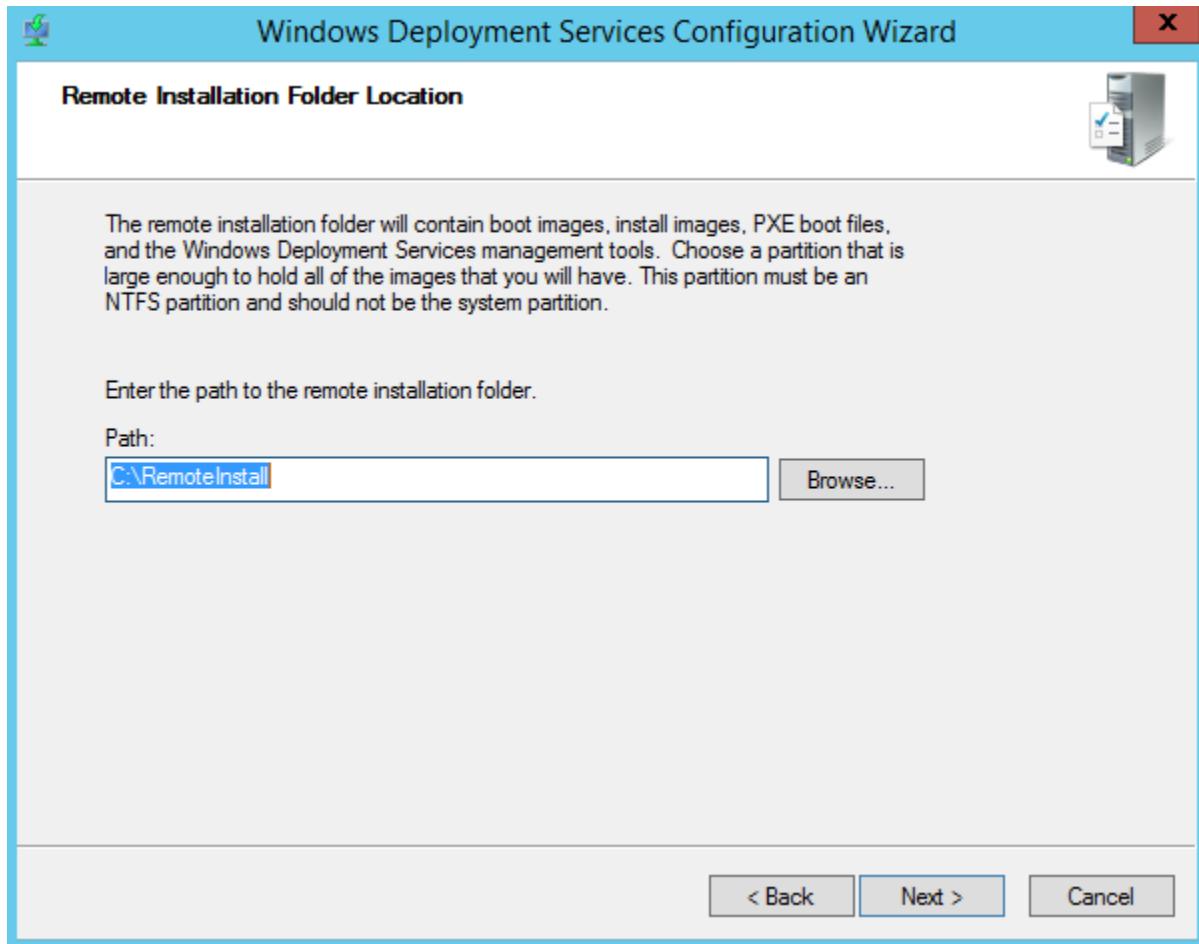
- The server is a member of an Active Directory Domain Services (AD DS) domain, or a domain controller for an AD DS domain. If the server supports Standalone mode, it can be configured without having a dependency on Active Directory.
- There is an active DHCP server on the network. This is because Windows Deployment Services uses Pre-Boot Execution Environment (PXE), which relies on DHCP for IP addressing.
- There is an active DNS server on your network.
- This server has an NTFS file system partition on which to store images.

To continue, click Next.

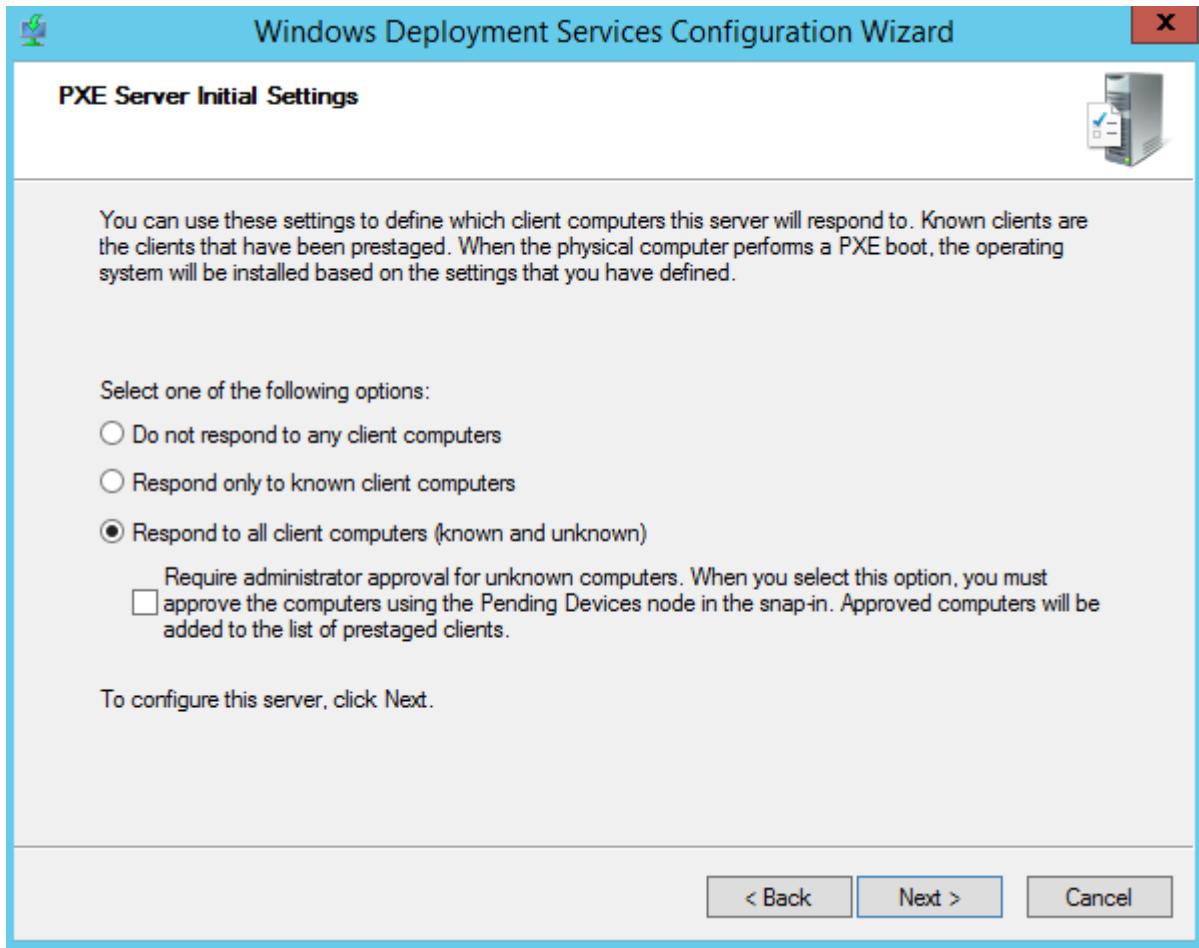
- Tại cửa sổ **Install Options**, chọn vào **Integrated with Active Directory**, click vào **Next**.



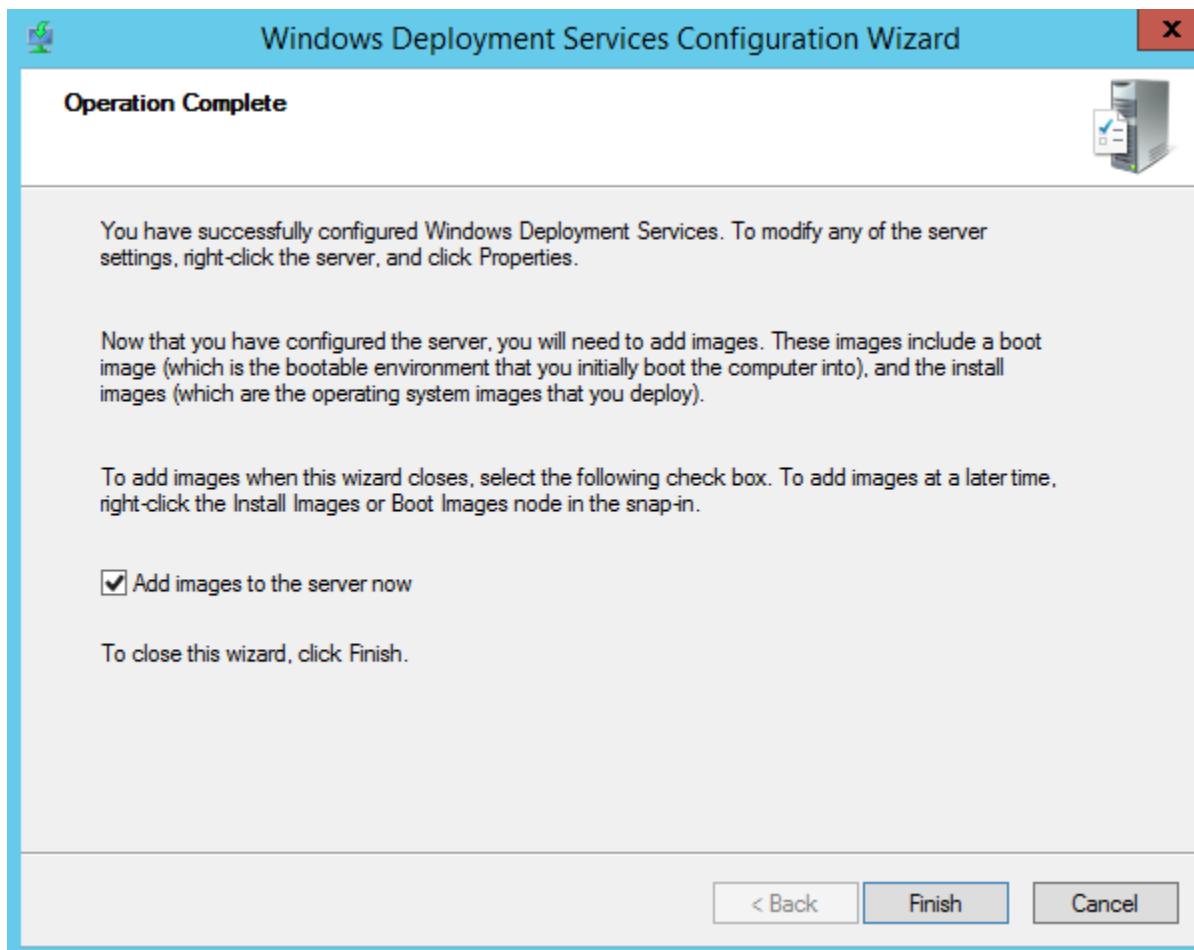
- Tại cửa sổ **Remote Installation Folder Location**, click vào **Next**.



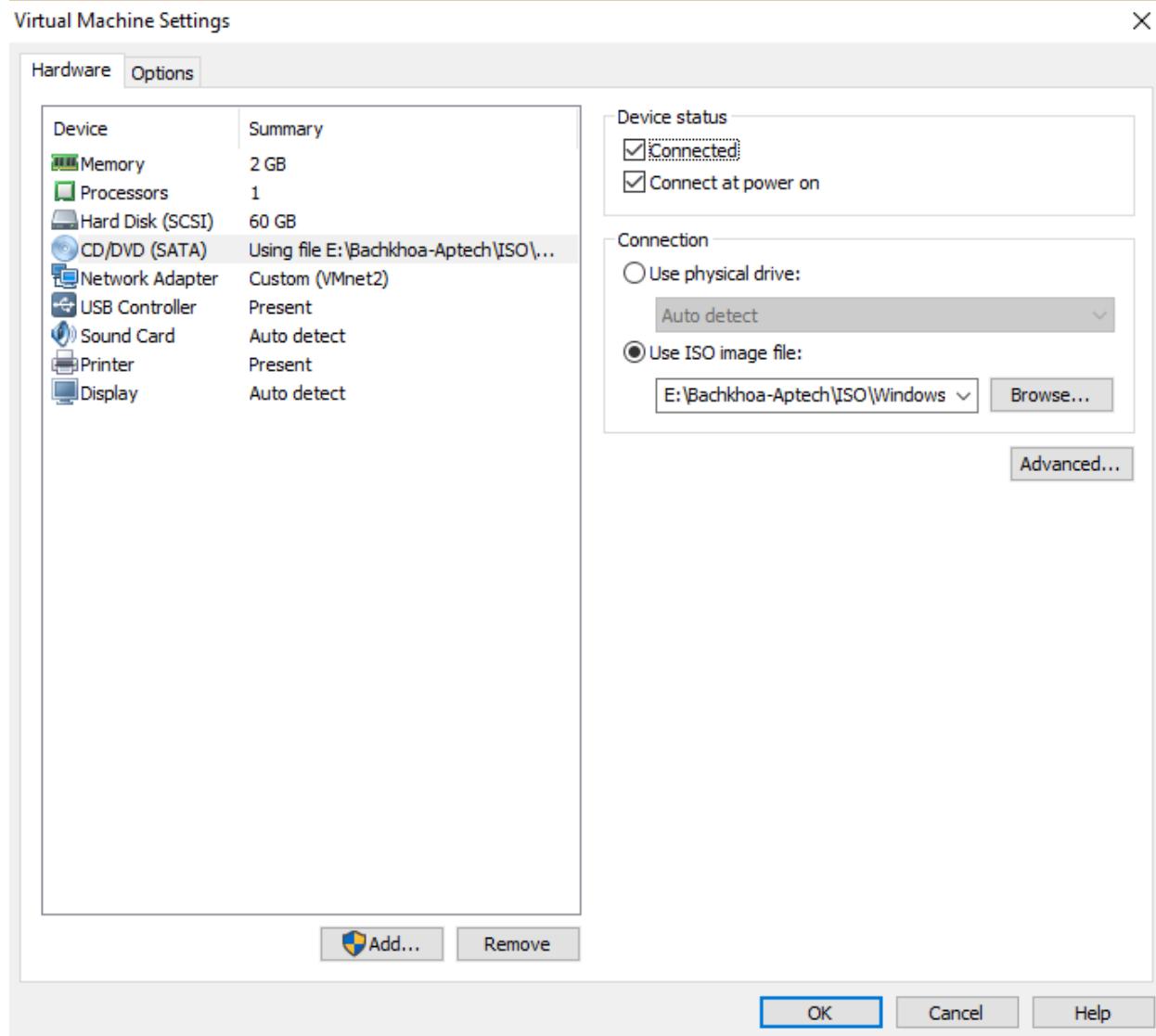
- Tại cửa sổ **PXE Server Initial Settings**, click chọn vào **Respond to all client computers (known and unknown)**, click vào Next.



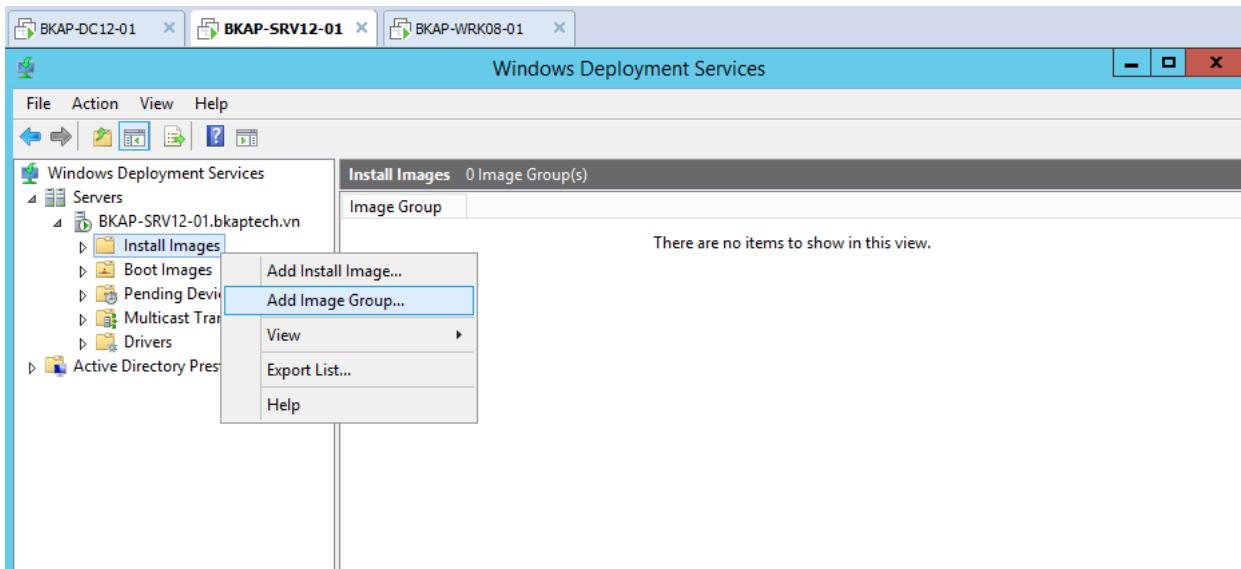
- Tại cửa sổ **Operation Complete**, click vào **Finish**.



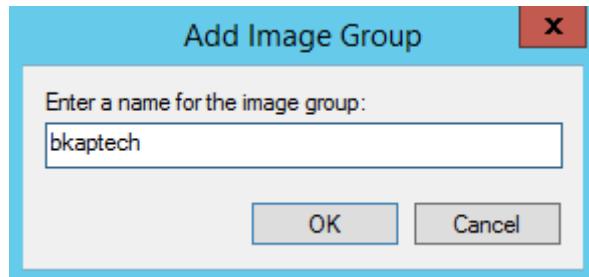
- Thực hiện *Add* file ISO cài đặt Windows 8.1 vào ổ đĩa DVD của máy BKAP-SRV12-01.



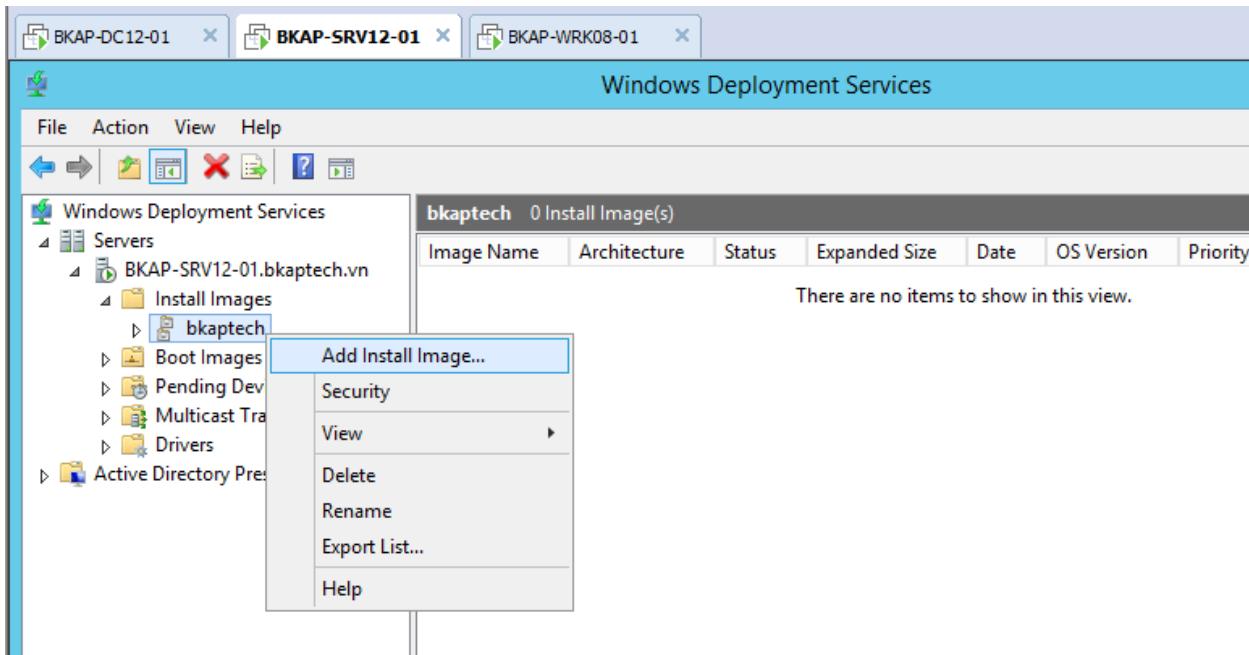
- Trong cửa sổ **Windows Deployment Services** , click chuột phải tại **Install Images** , chọn **Add Image Group...**



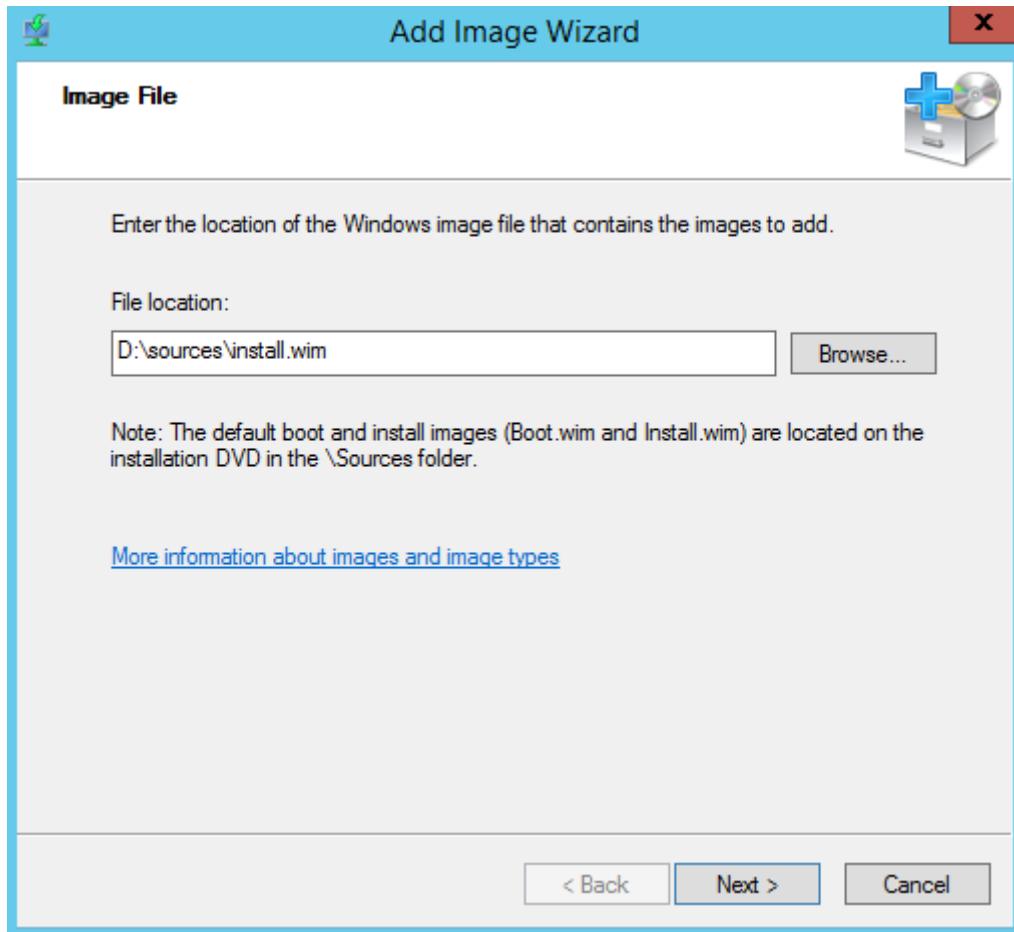
- Tại cửa sổ **Add Image Group** , nhập vào tên *bkaptech*.



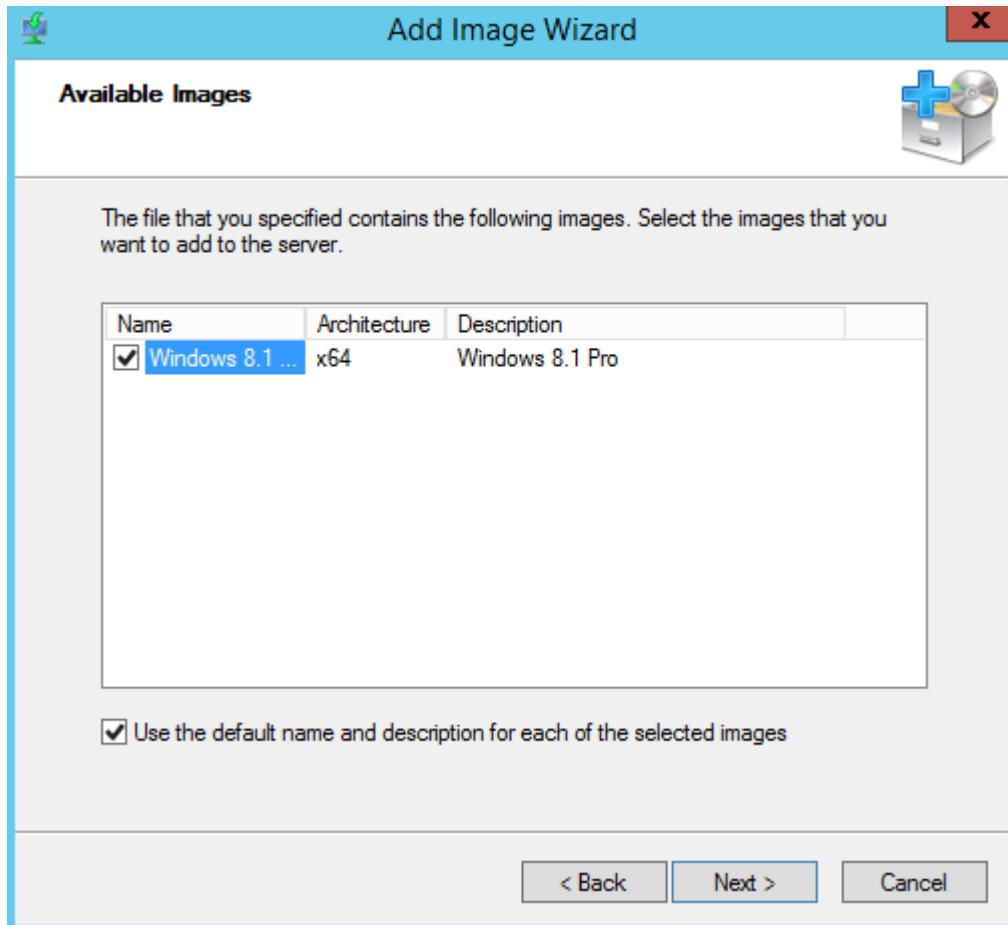
- Click chuột phải tại *bkaptech* vừa tạo , chọn **Add Install Image...**



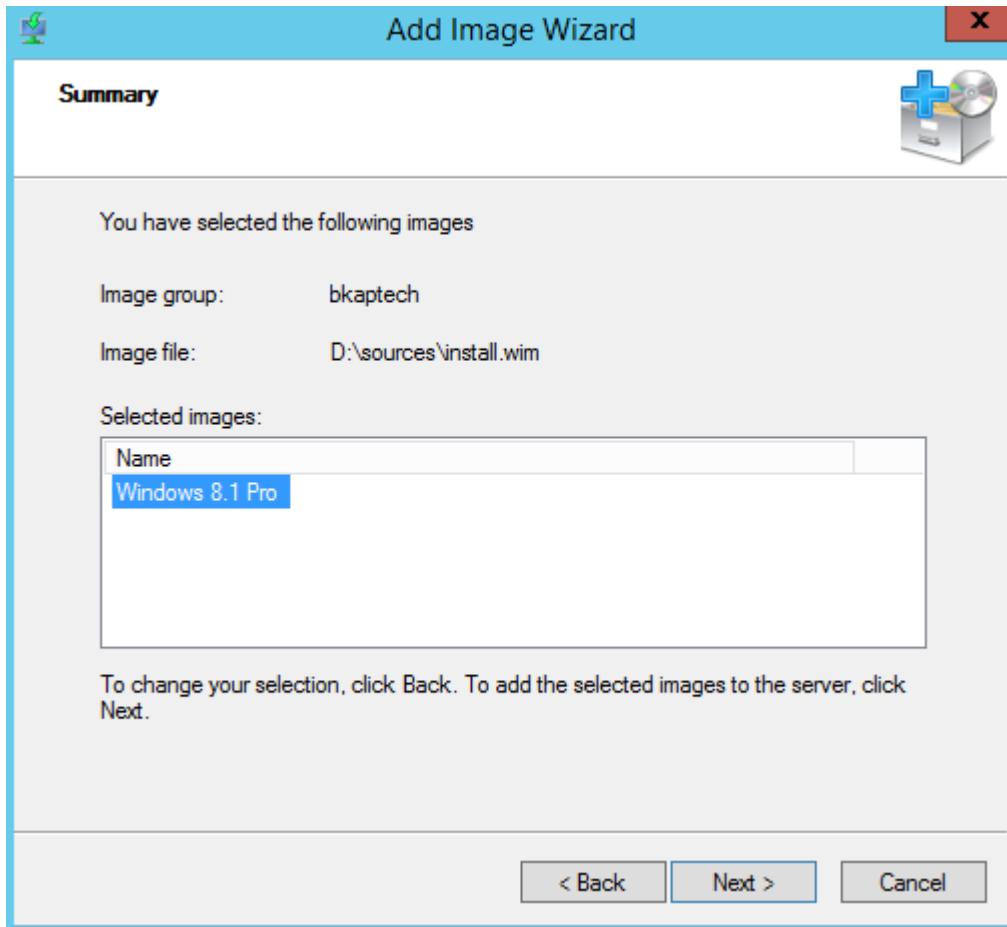
- Tại cửa sổ **Image File**, tại mục **File location** , **Browse** đến file **install.wim** trong ổ đĩa dvd windows.



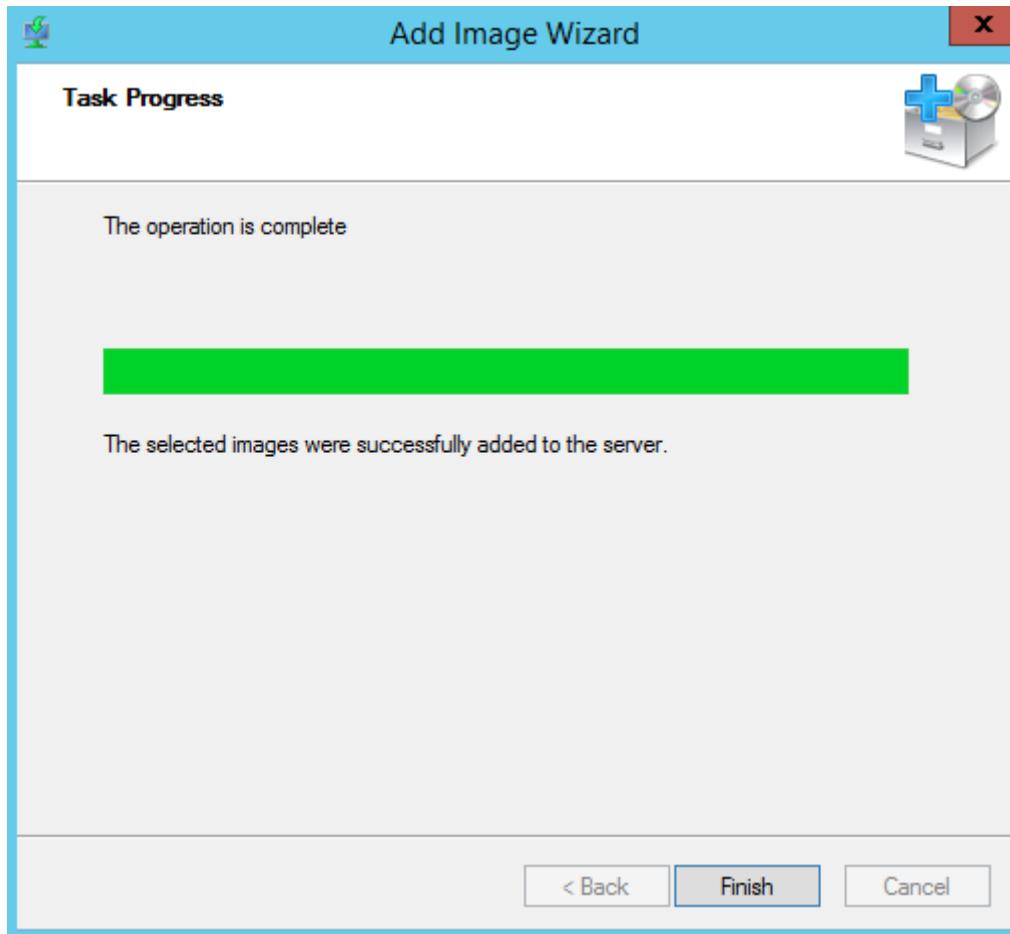
- Tại cửa sổ **Available Images**, chọn *HDH cần cài đặt*, click vào **Next**.



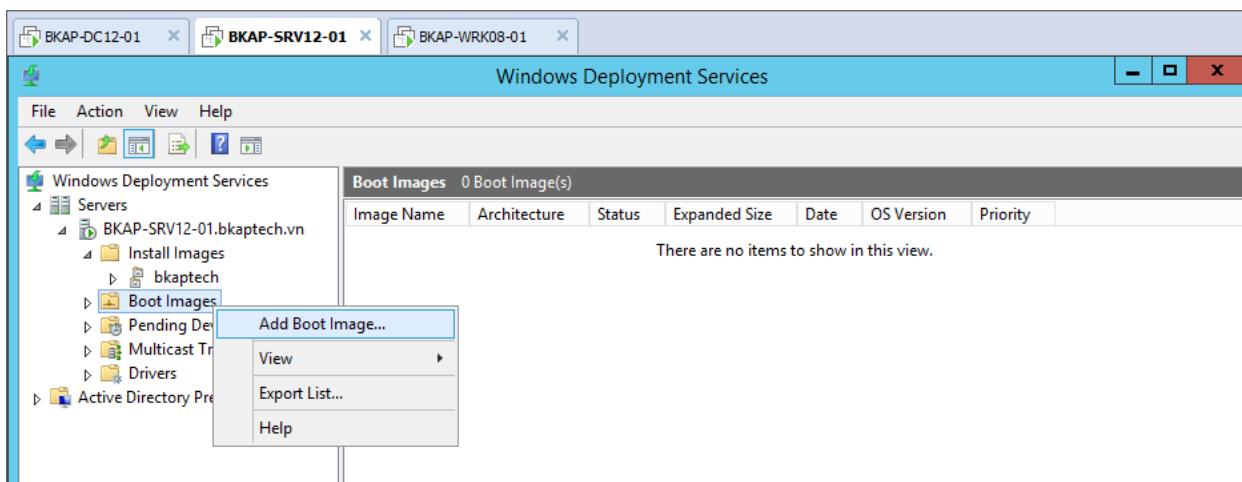
- Tại cửa sổ **Summary**, click vào **Next**.



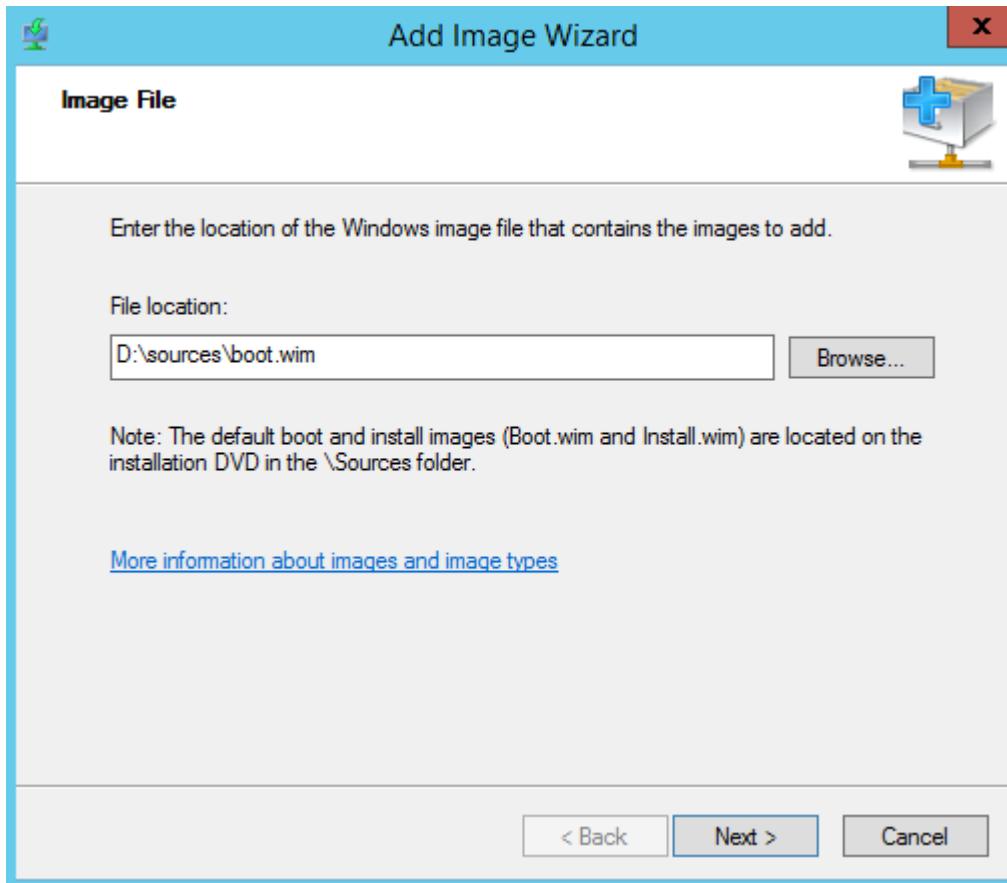
- Máy chủ tiến hành add file *install.wim*, tại cửa sổ Task Progress, click vào Finish.



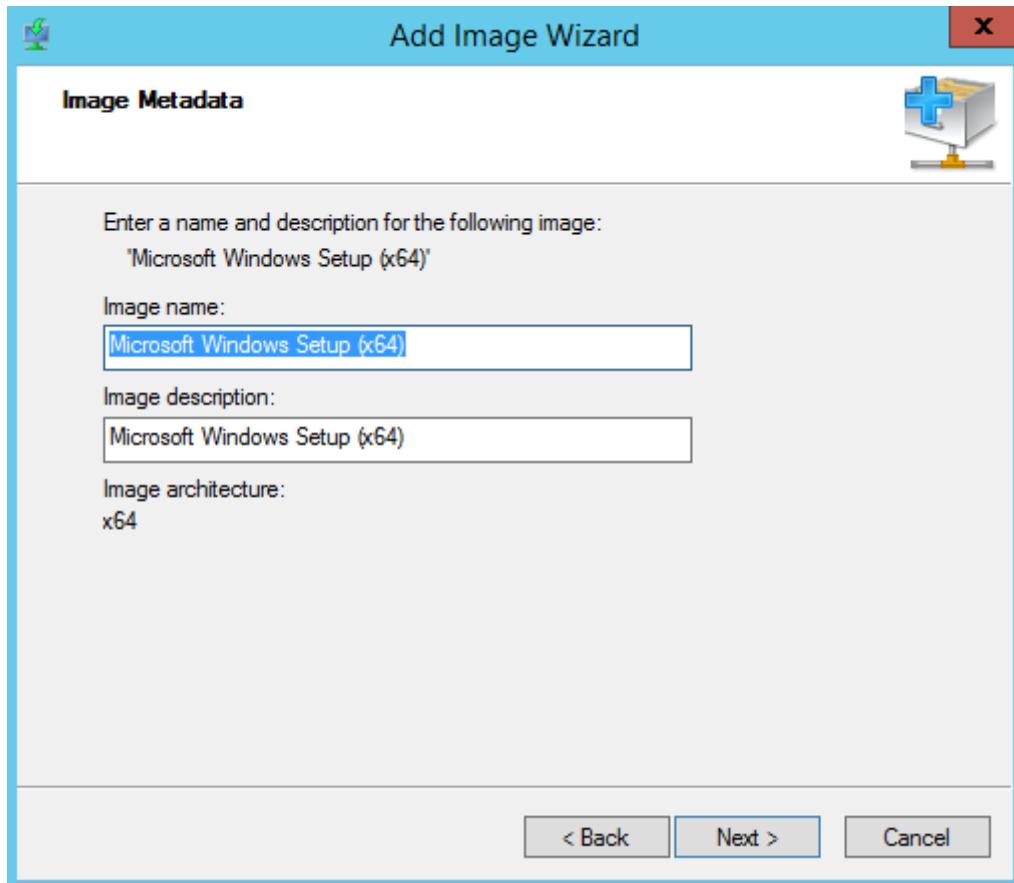
- Tại cửa sổ Windows Deployment Services, click chuột phải tại Boot Images , chọn Add Boot Images.

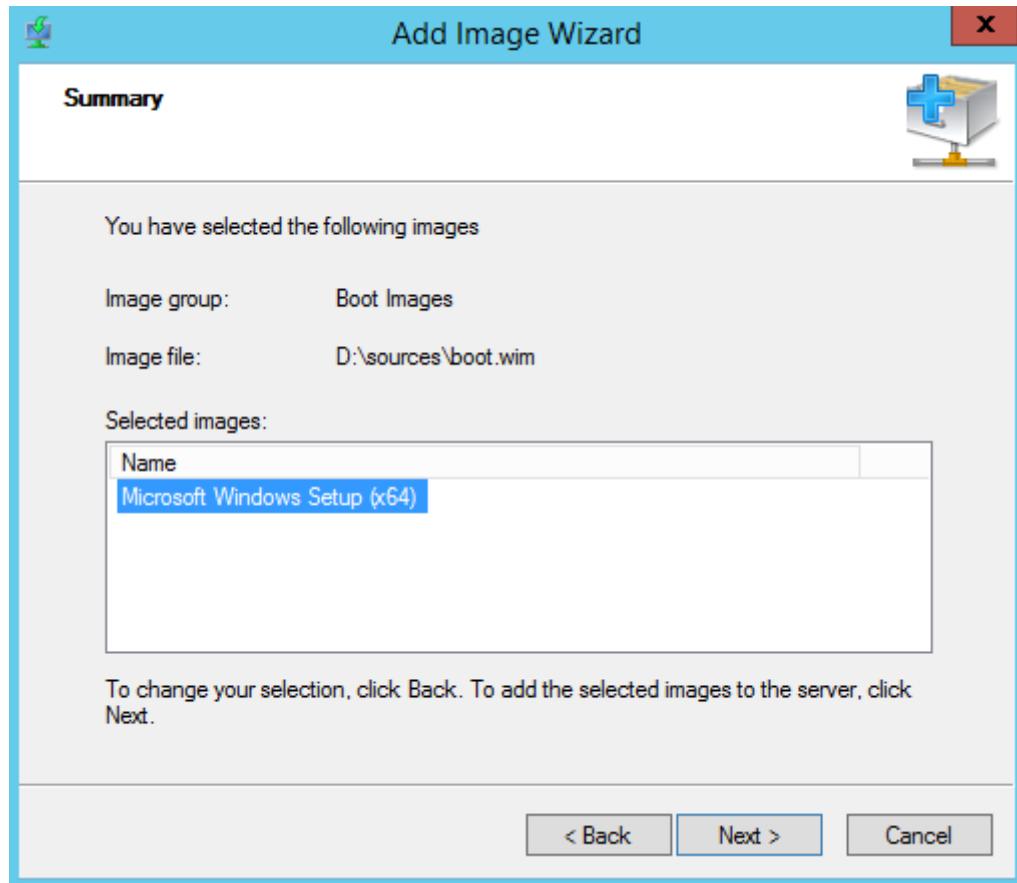


- Tại cửa sổ **Image File**, *Browse* đến file *Boot.wim*

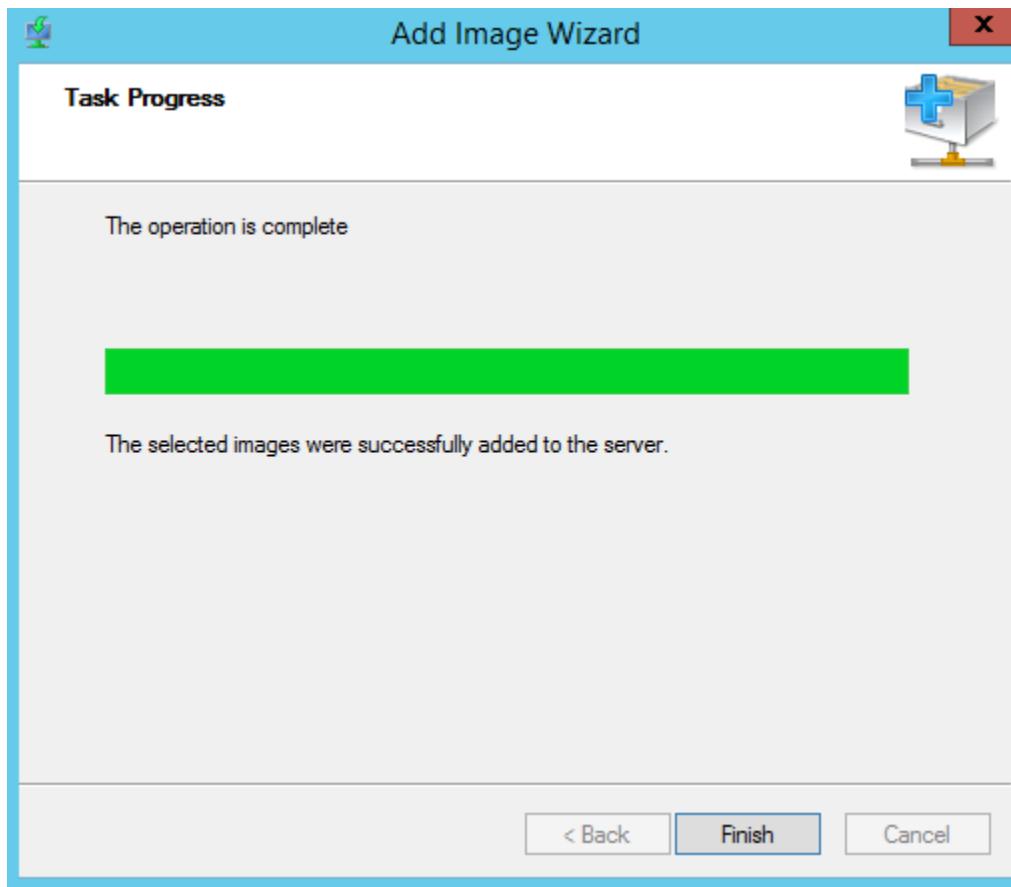


- Tại cửa sổ **Image Metadata** và cửa sổ **Summary**, click vào **Next**.





- Tại cửa sổ **Task Progress**, click vào **Finish**.



- Add thành công:

The screenshot shows the Windows Deployment Services management console. The title bar says "Windows Deployment Services". The left navigation pane shows "Windows Deployment Services" with "Servers" expanded, showing "BKAP-SRV12-01.bkaptech.vn" with its sub-folders: "Install Images", "Boot Images", "Pending Devices", "Multicast Transmissions", and "Drivers". The right pane shows a table titled "Boot Images" with 1 Boot Image(s). The table has columns: Image Name, Architecture, Status, Expanded Size, Date, OS Version, and Priority. One row is listed: "Microsoft ..." (Architecture: x64, Status: Online, Expanded Size: 1351 MB, Date: 3/13/..., OS Version: 6.3.9600, Priority: 500000...).

- Chuyển sang máy *Client*, Boot vào card mạng.

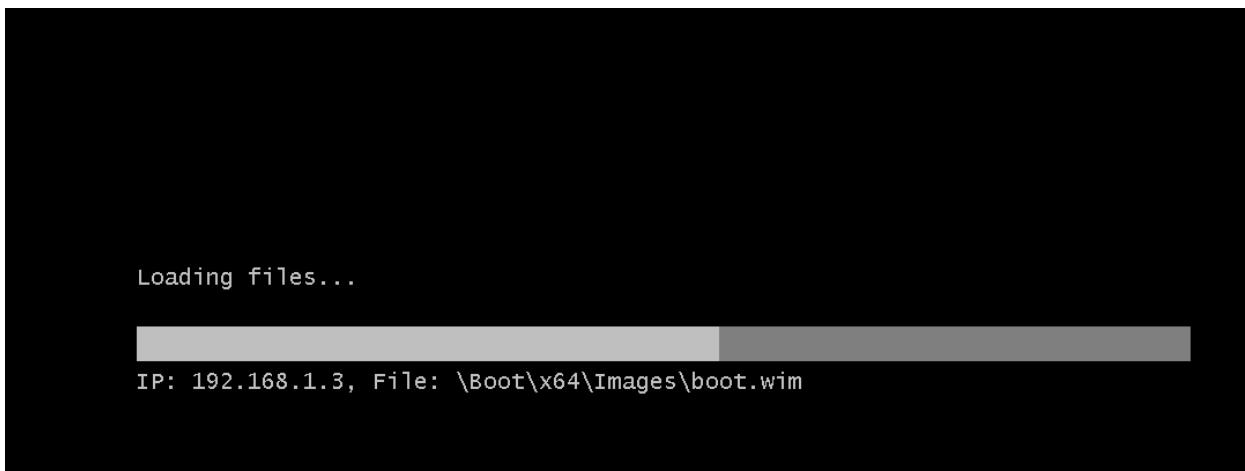
```
Network boot from Intel E1000e
Copyright (C) 2003-2014 VMware, Inc.
Copyright (C) 1997-2000 Intel Corporation

CLIENT MAC ADDR: 00 0C 29 81 B4 13  GUID: 564D64BF-3047-8930-26B4-EDF42881B413
CLIENT IP: 192.168.1.22  MASK: 255.255.255.0  DHCP IP: 192.168.1.2
GATEWAY IP: 192.168.1.1

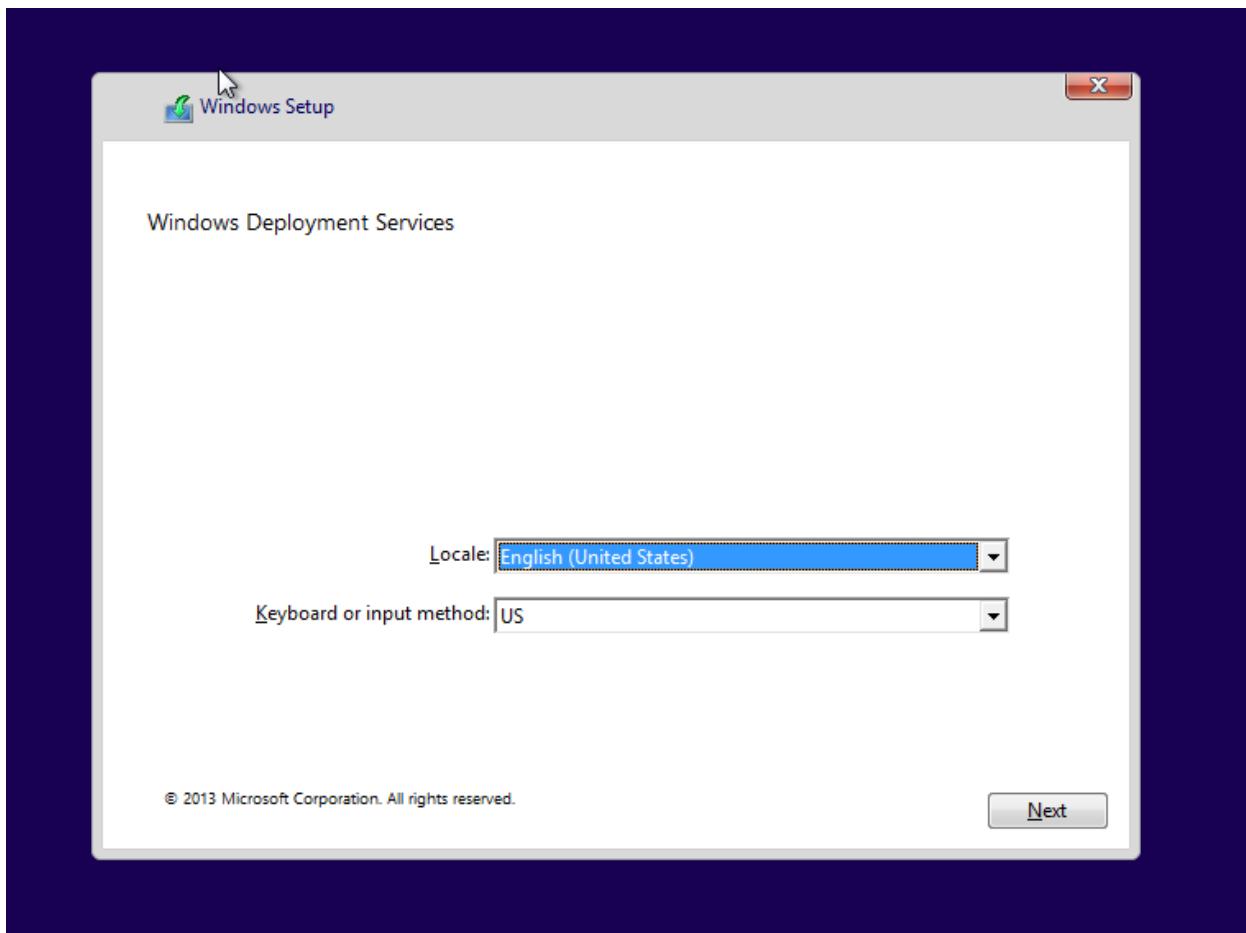
Downloaded WDSNBP from 192.168.1.3 BKAP-SRV12-01.bkaptech.vn

Press F12 for network service boot
```

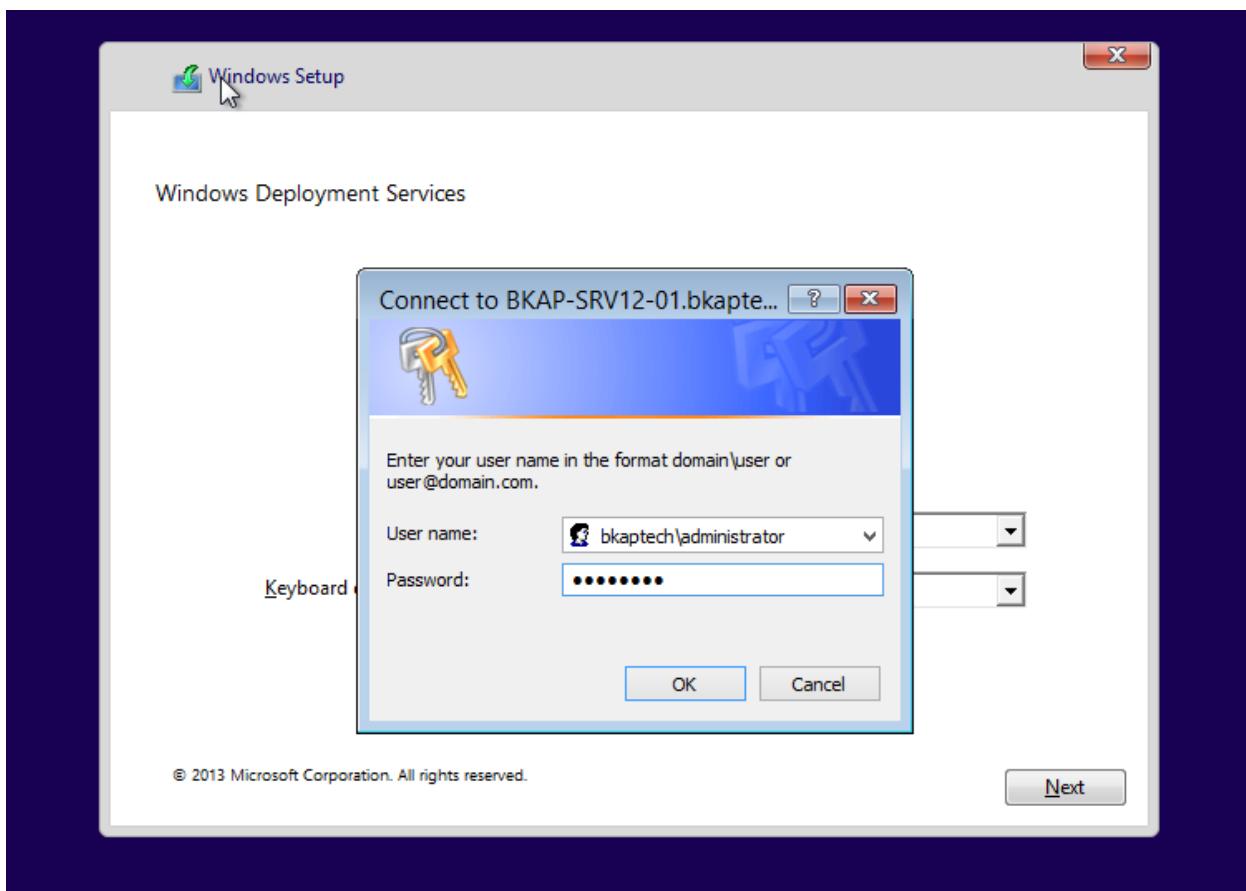
- Ấn phím **F12** để máy tính boot vào card mạng, cài đặt **HĐH**.



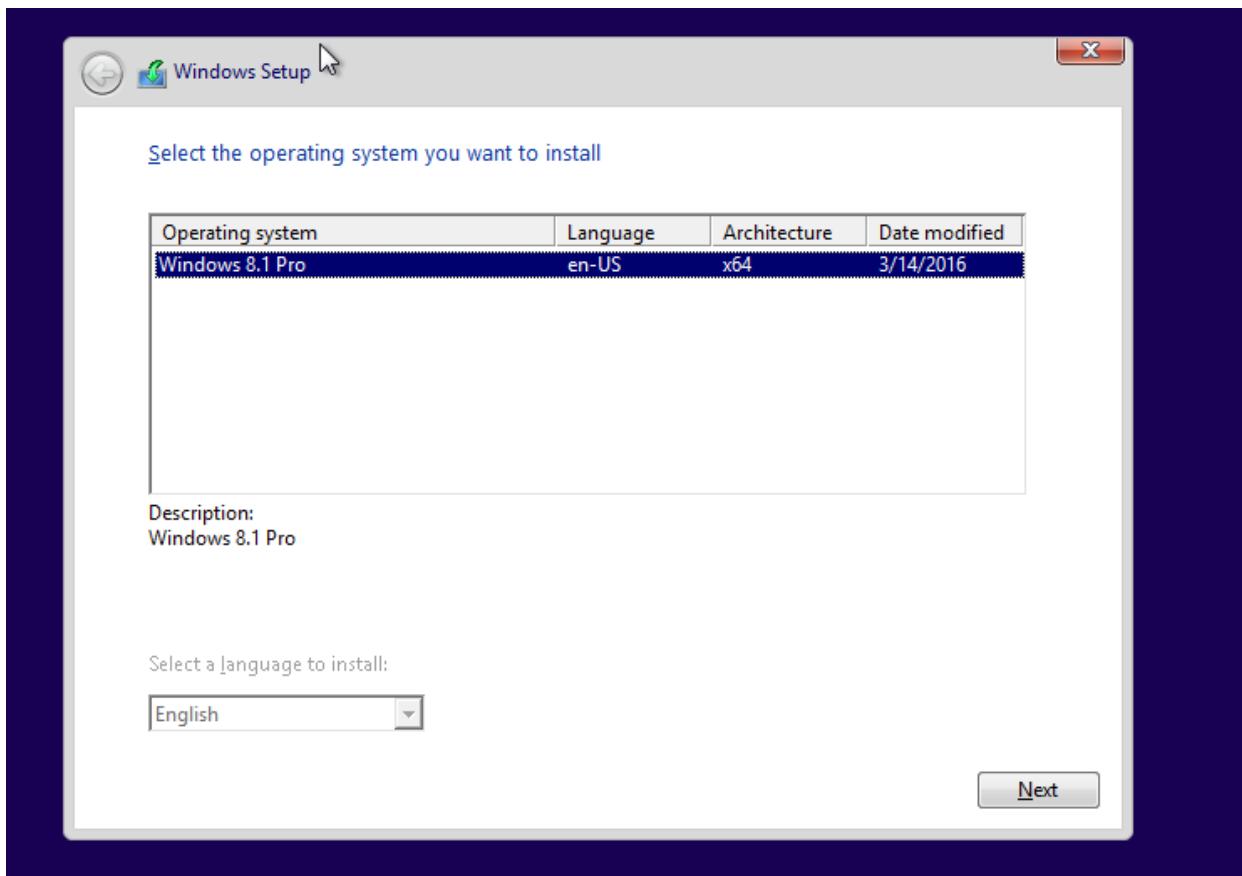
- Tại cửa sổ **Windows Deployment Services**, click vào **Next**.



- Tại cửa sổ **Connect to ...** nhập User **bkaptech\administrator**, *OK*.



- Thực hiện cài đặt HĐH Windows 8.1 Pro.



1.2 Triển khai cài đặt Windows 8 tự động qua mạng LAN.

1. Yêu cầu bài Lab:

+ Tạo *File trả lời tự động*:

- Cài đặt **Windows Assessment and Deployment Kit (ADK)**.
- Dùng **Windows AIK** tạo **Unattended Setup Answer File**.

+ Cài đặt và cấu hình **DHCP Server**.

+ Cài đặt và cấu hình dịch vụ **Windows Deployment Services (WDS)**.

2. Yêu cầu chuẩn bị:

+ Chuẩn bị 3 máy:

- Máy Server *BKAP-DC12-01* đã nâng cấp lên **Domain Controller**.
- Máy Server *BKAP-SRV12-01* Join vào Domain , cài đặt dịch vụ **WDS** và **ADK**.

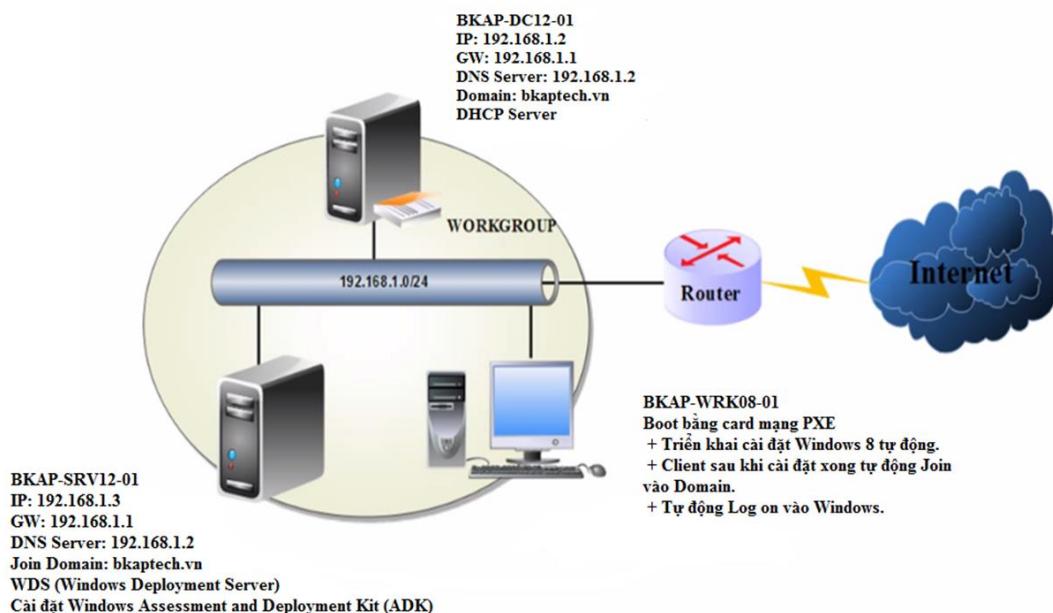
- Máy Client chưa cài đặt HĐH.

3. Mô hình Lab:

HỆ THỐNG ĐÀO TẠO CNTT QUỐC TẾ BACHKHOA-APTECH



Lab 1.2 Triển khai cài đặt Windows 8 tự động qua mạng LAN.



Hình 1.2

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	DHCP Client
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
DNS Server	192.168.1.2	192.168.1.2	192.168.1.2

Bài 2:**TRIỂN KHAI DỊCH VỤ INTERNET INFORMATION SERVICES (IIS)**

Các nội dung chính sẽ được đề cập:

- ✓ Cấu hình IIS với Single Website.
- ✓ Cấu hình Multi Website kết hợp với DNS Server.
- ✓ Sử dụng Active Directory Certificate Services để bảo mật Web Server.

2.1 Cấu hình IIS với Single Website.**1. Yêu cầu bài Lab:**

- + Trên máy **BKAP-DC12-01**, cấu hình **DNS Server**.
- + Trên máy **BKAP-SRV12-01**, thực hiện các công việc sau:
 - Tạo dữ liệu và nội dung **Website** trong ô C.
 - Cài đặt và cấu hình dịch vụ **Web Server (IIS)**.
 - Khảo sát các tính năng trên **IIS** như : *Default Document, Directory Browsing*.
- + Trên máy **BKAP-WRK08-01**, kiểm tra:
 - Truy cập Website bằng tên miền www.bkaptech.vn
 - Truy cập địa chỉ www.bkaptech.vn/BKAP để kiểm tra.

2. Yêu cầu chuẩn bị:

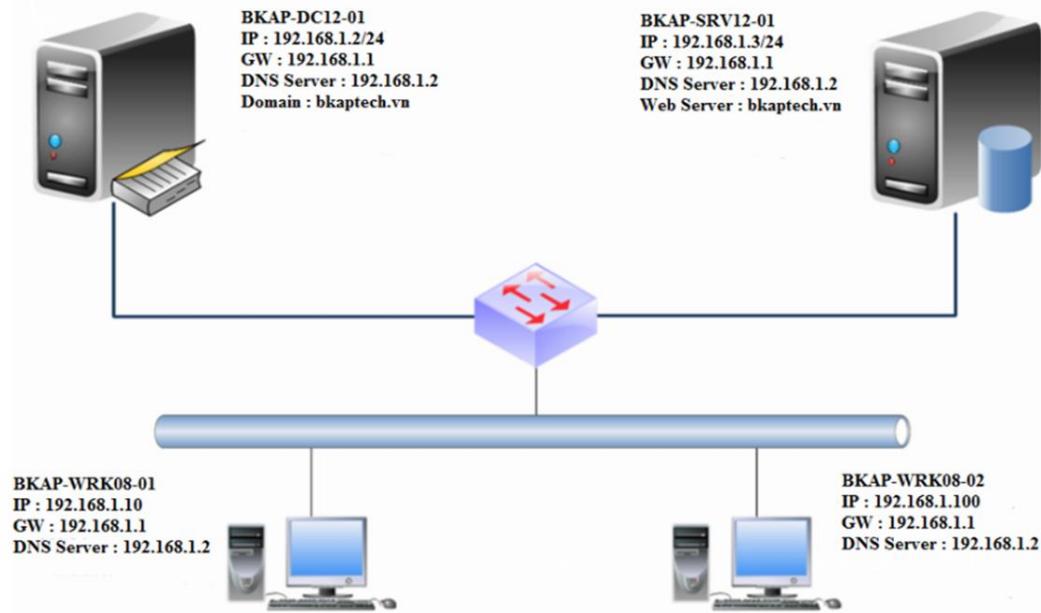
- + Chuẩn bị 2 máy Server và 1 máy Client theo mô hình Lab 2.1.
 - Máy **BKAP-DC12-01** làm **Domain Controller** cài đặt DNS Server với tên **bkaptech.vn**.
 - Máy **BKAP-SRV12-01** cài đặt và cấu hình **Web Server (IIS)**.
 - Máy **BKAP-WRK08-01** dùng để truy cập vào **Website**.

3. Mô hình Lab:

HỆ THỐNG ĐÀO TẠO CNTT QUỐC TẾ BACHKHOA-APTECH



Lab 2.1 Triển khai cài đặt và cấu hình Web Server (IIS)



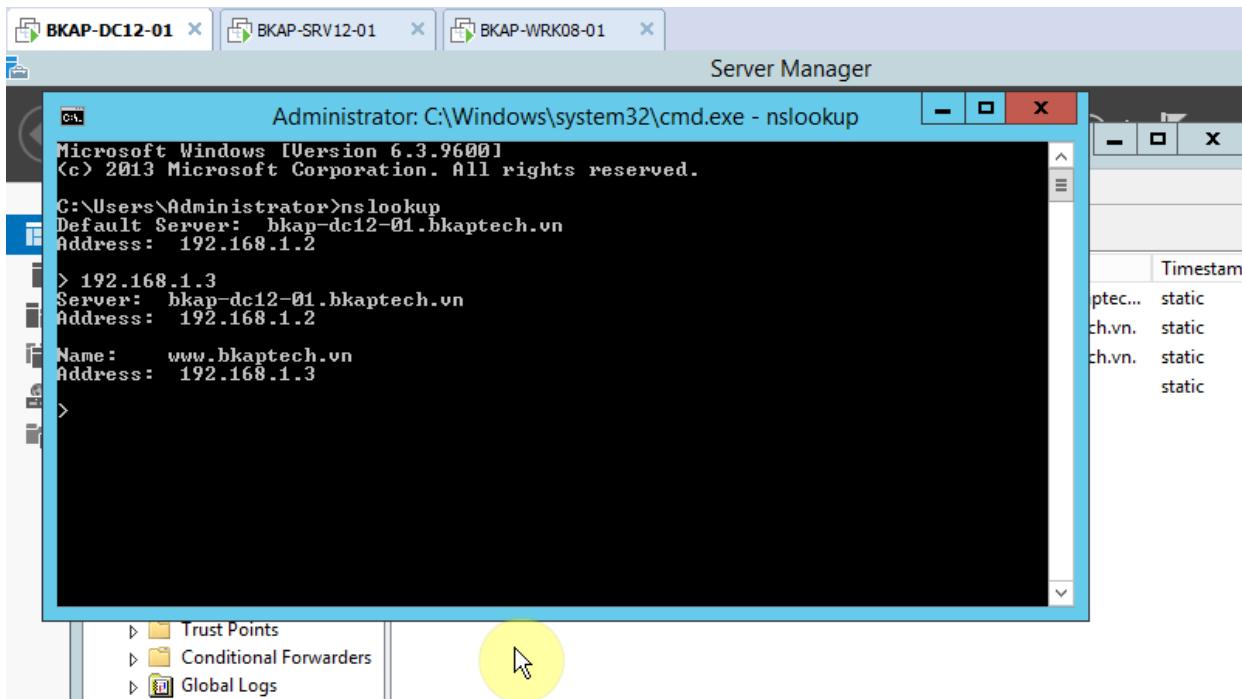
Hình 2.1

Sơ đồ địa chỉ như sau:

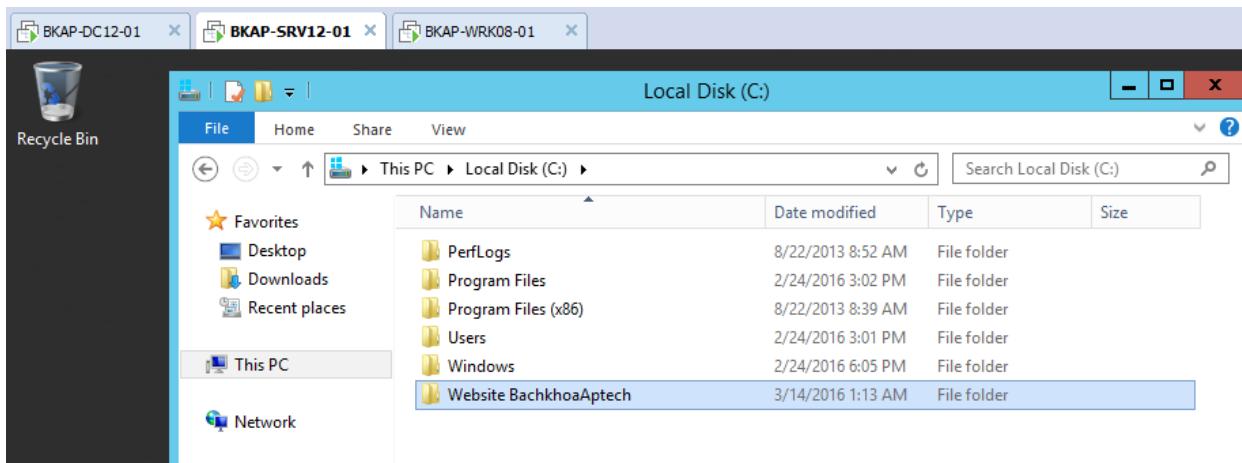
Thông số	BKAP-DC12-01	BKAP-SRV12-01	BKAP-WRK08-01
IP address	192.168.1.2	192.168.1.3	192.168.1.10
Gateway	192.168.1.1	192.168.1.1	192.168.1.1
Subnet Mask	255.255.255.0	255.255.255.0	255.255.255.0
DNS Server	192.168.1.2	192.168.1.2	192.168.1.2

Hướng dẫn chi tiết:

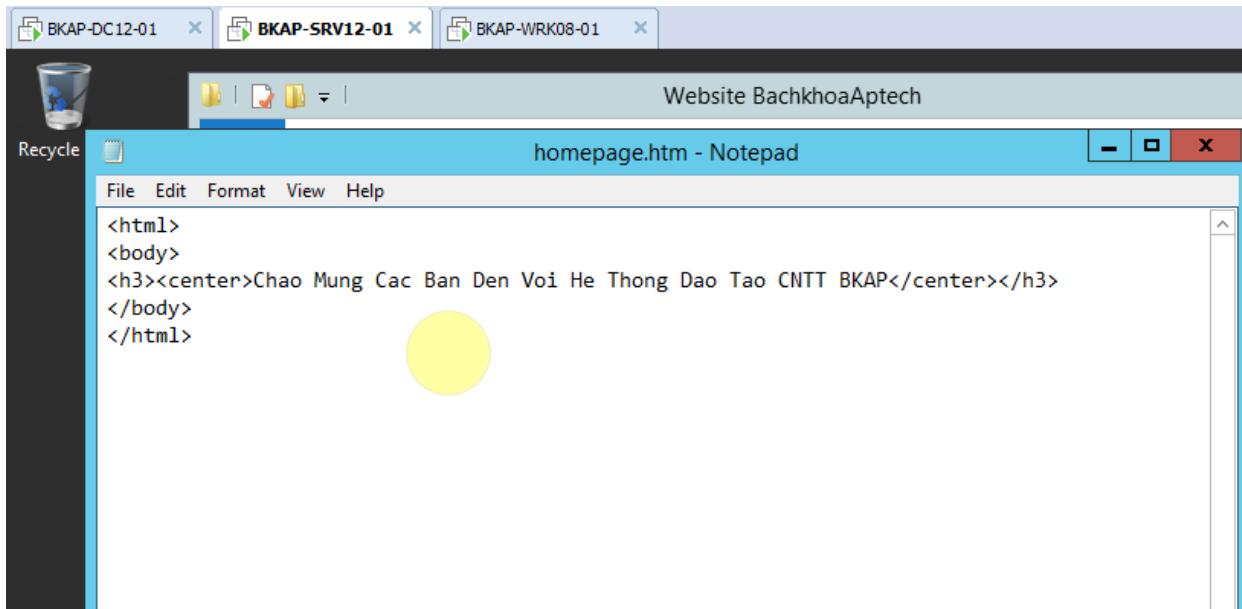
- Kết nối các máy ảo như hình trên, thực hiện ping thông giữa các máy trong mạng.
- Trên máy **BKAP-DC12-01**, thực hiện cấu hình **DNS Server**.



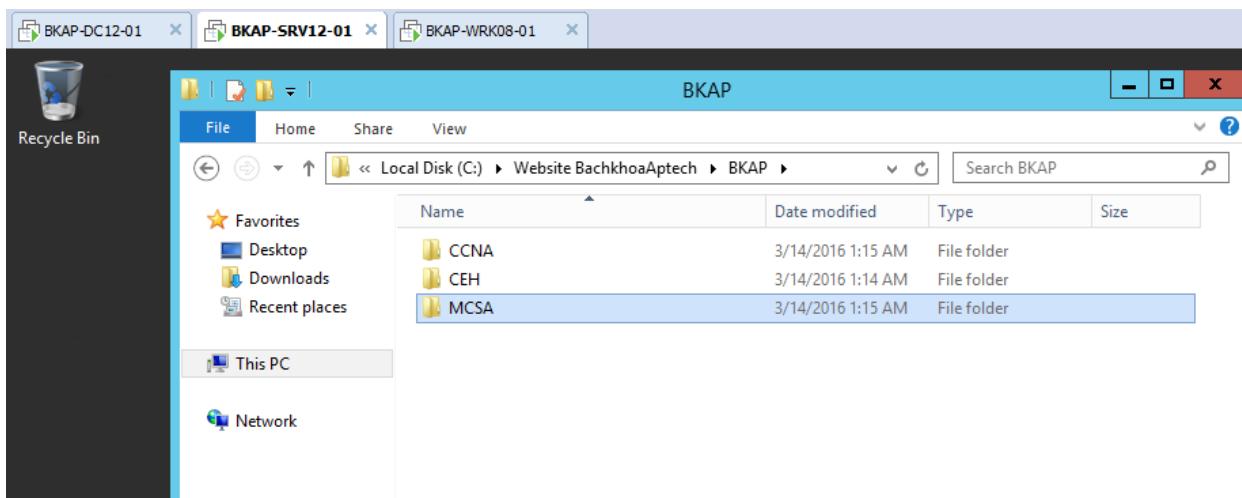
- Chuyển sang máy **BKAP-SRV12-01**, thực hiện cài đặt và cấu hình **Web Server (IIS)**.
 - Tạo dữ liệu và nội dung **Website** trong ô C.
 - Tạo thư mục **Website BachkhoaAptech**.



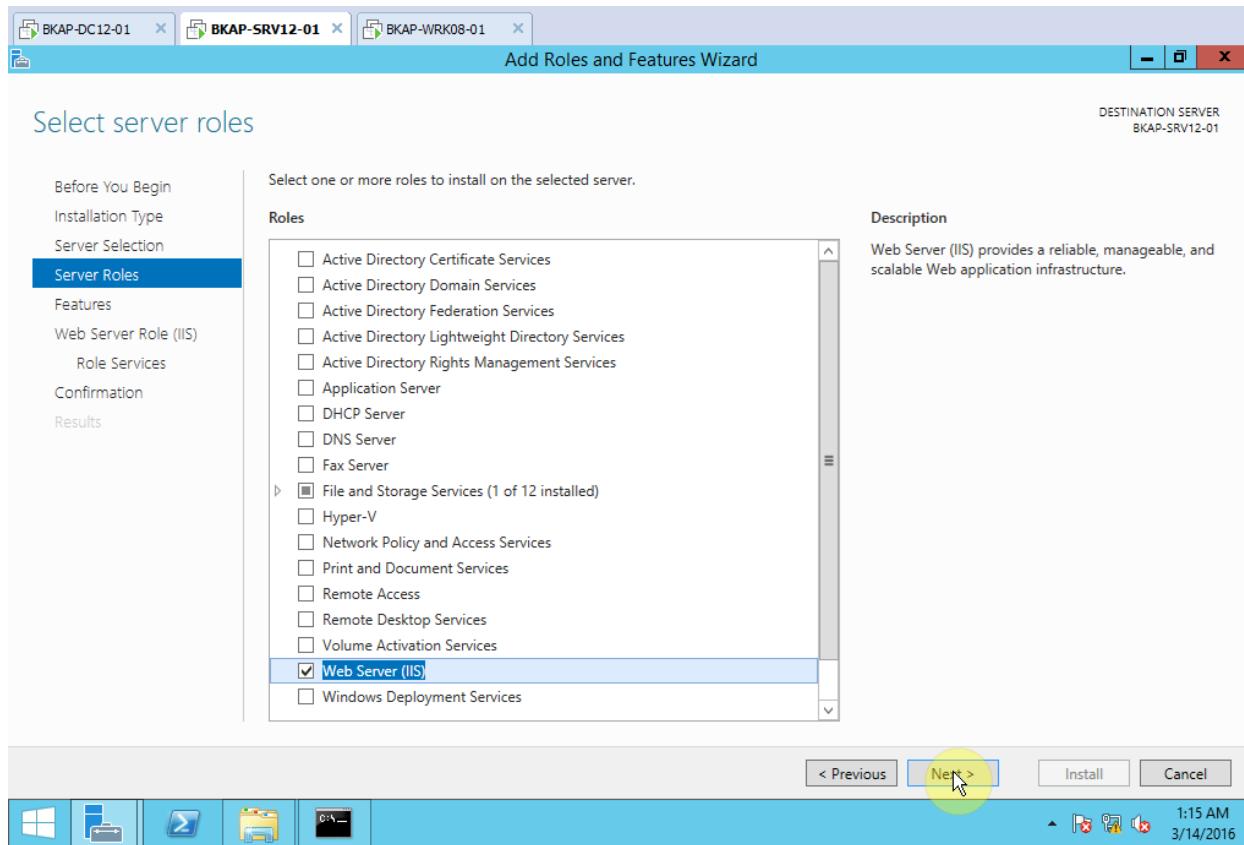
- Trong thư mục **Website BachkhoaAptech**, tạo 1 file **homepage.htm** và tạo nội dung Website theo hình sau:



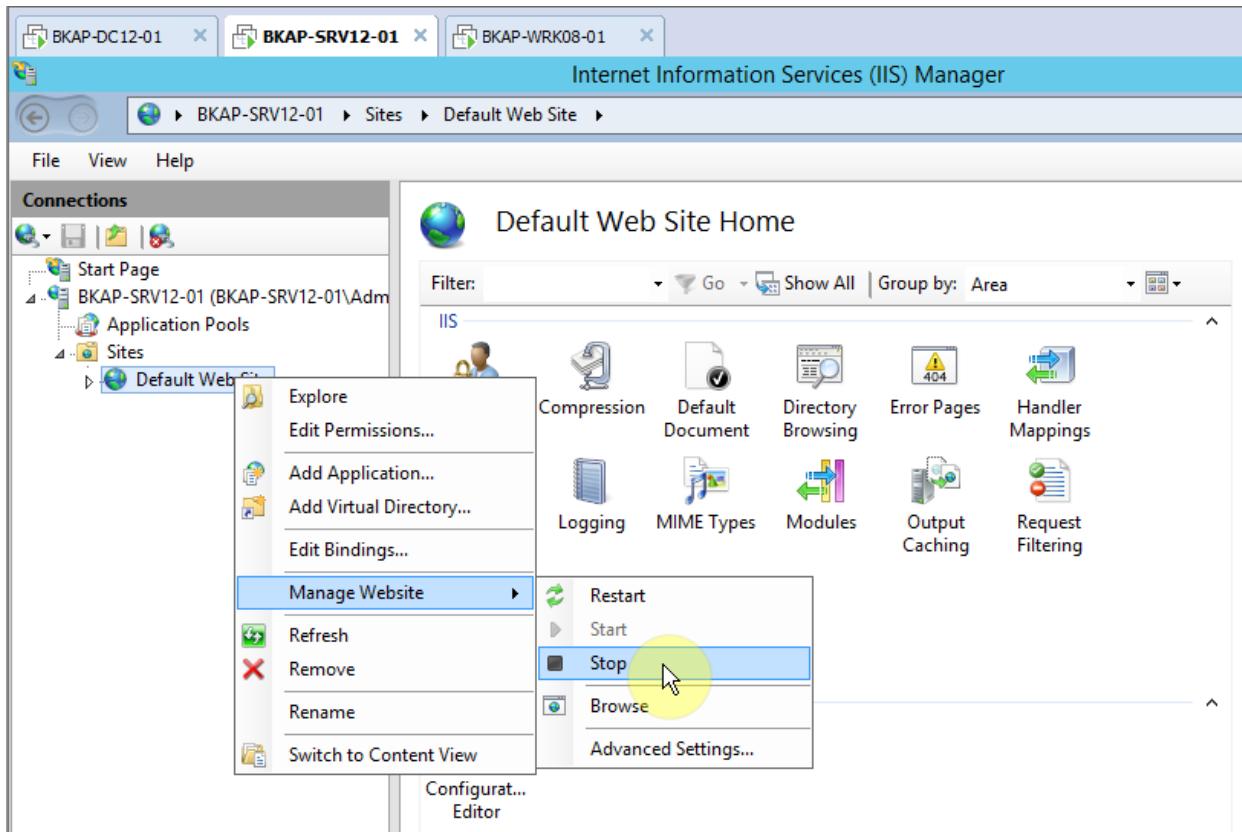
- Tạo thêm các thư mục con bên trong thư mục **Website BachkhoaAptech**.



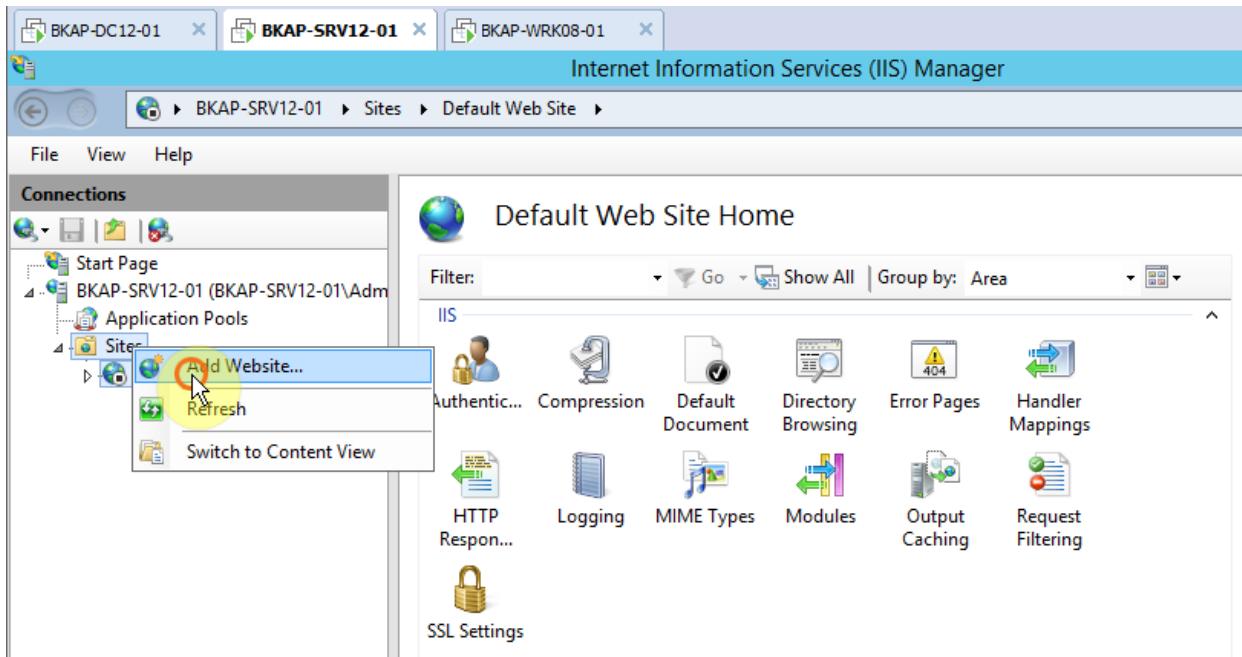
- Cài đặt dịch vụ IIS.



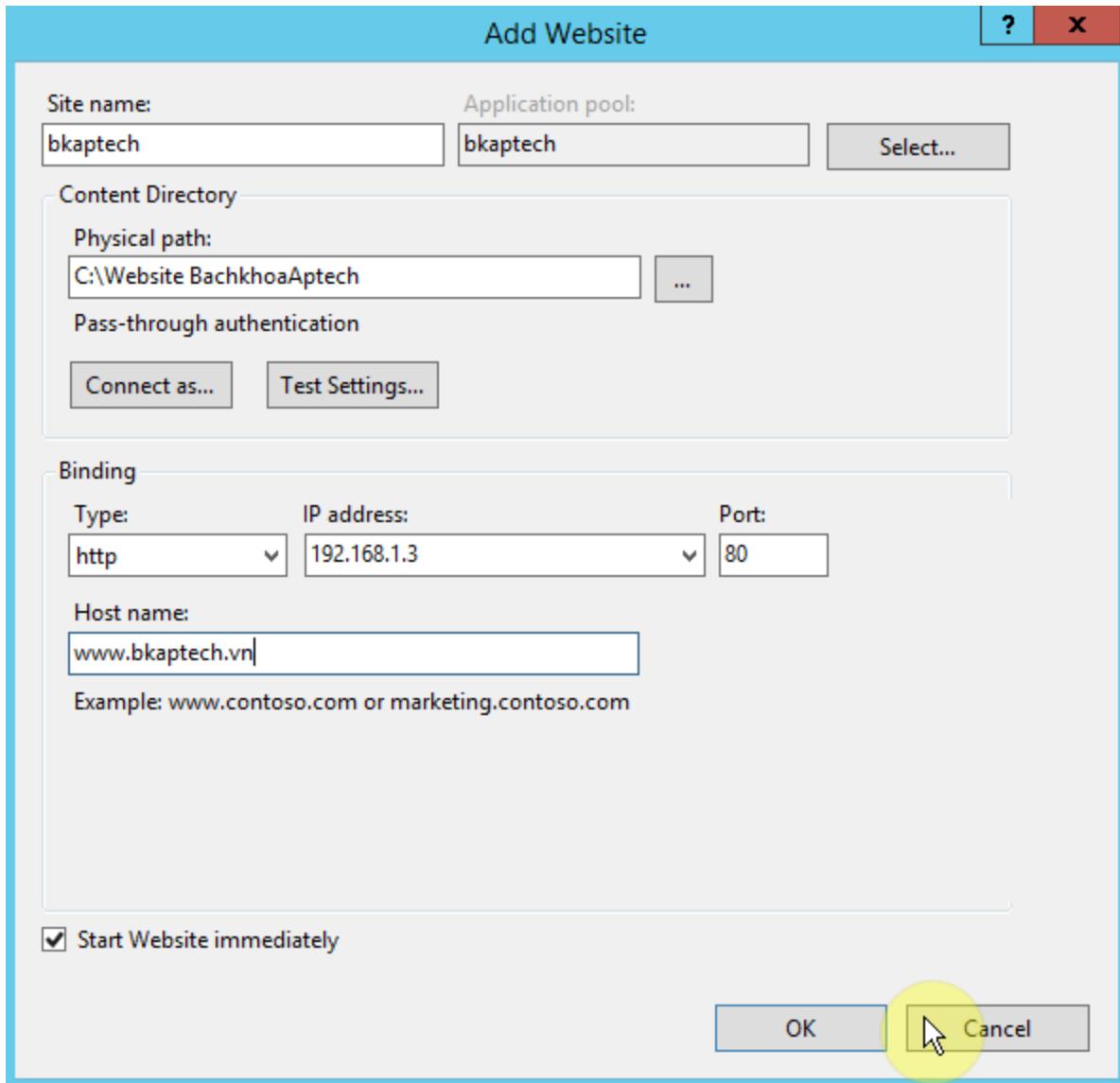
- Cấu hình dịch vụ IIS.
 - Tools / Internet Information Services (IIS) Manager.
 - Trong cửa sổ Internet Information Services (IIS) Manager , click vào Sites / Default WebSite => Stop.



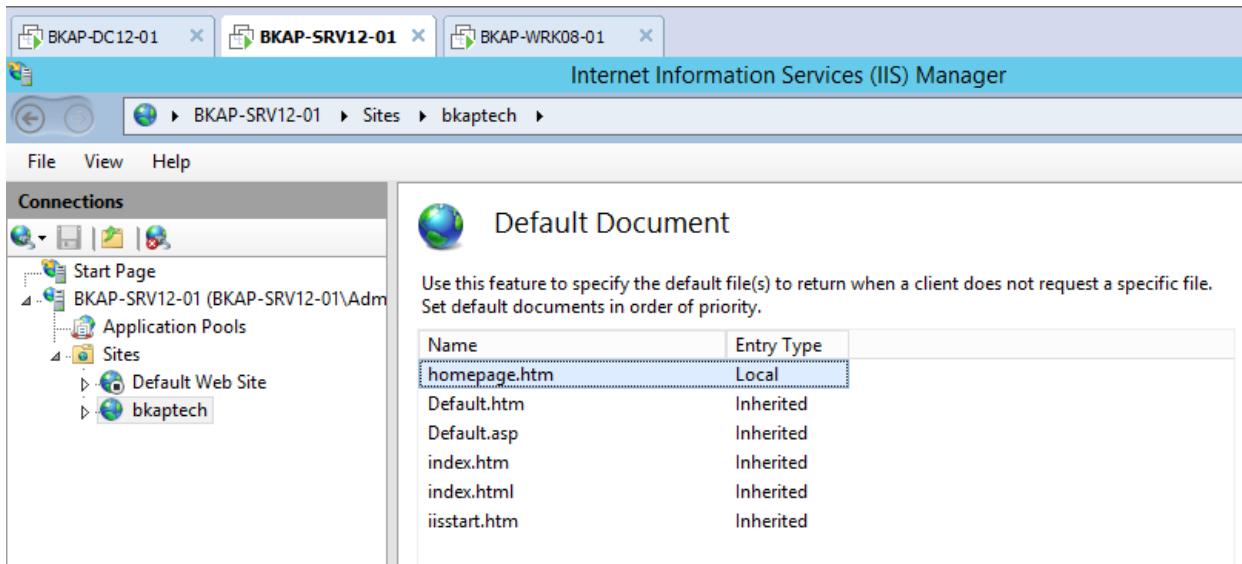
- Click chuột phải vào **Sites** chọn **Add Website...**



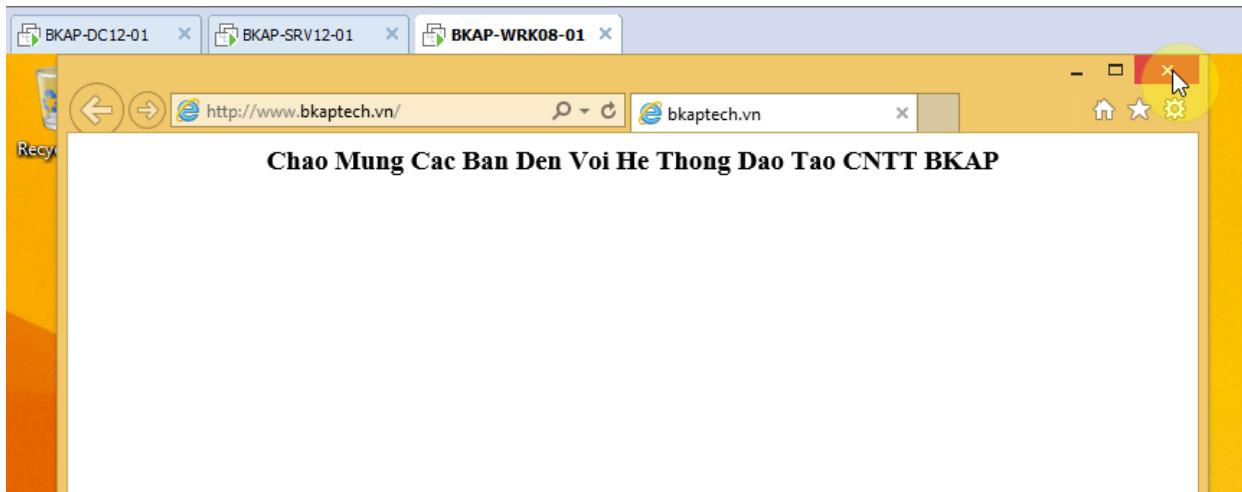
- Tại cửa sổ **Add Website**, nhập vào các thông số:
 - **Site name:** *bkaptech*
 - **Physical path :** browse đến thư mục **Website BachkhoaAptech.**
 - **IP address :** *192.168.1.3*
 - **Host name :** *bkaptech.vn*



- Tại Site **bkaptech** vừa tạo, click vào **Default Document**, thực hiện add vào file **homepage.htm**.



- Chuyển sang máy Client **BKAP-WRK08-01**, kiểm tra truy cập Website.



2.2 Cấu hình IIS Multi Website kết hợp với DNS Server.

1. Yêu cầu bài Lab:

+ Trên máy **BKAP-DC12-01**, cấu hình DNS Server.

- Tạo bản ghi trên **DNS Server** để phân giải cho **Website** với tên miền www.bkaptech.vn , www.bachkhoa-aptech.vn , www.bkap.vn .
- Trên máy **BKAP-SRV12-01** , thực hiện các công việc sau:

- Tạo dữ liệu và nội dung với 3 **website** đặt trong ô C.
- Cài đặt **Web Server (IIS)**.
- Tạo **hosting website** trên IIS với *multi website* có tên *bkaptech*, *bachkhoa-aptech*, *bkap*.
- Trên máy *Client*, kiểm tra truy cập bằng tên miền của website.

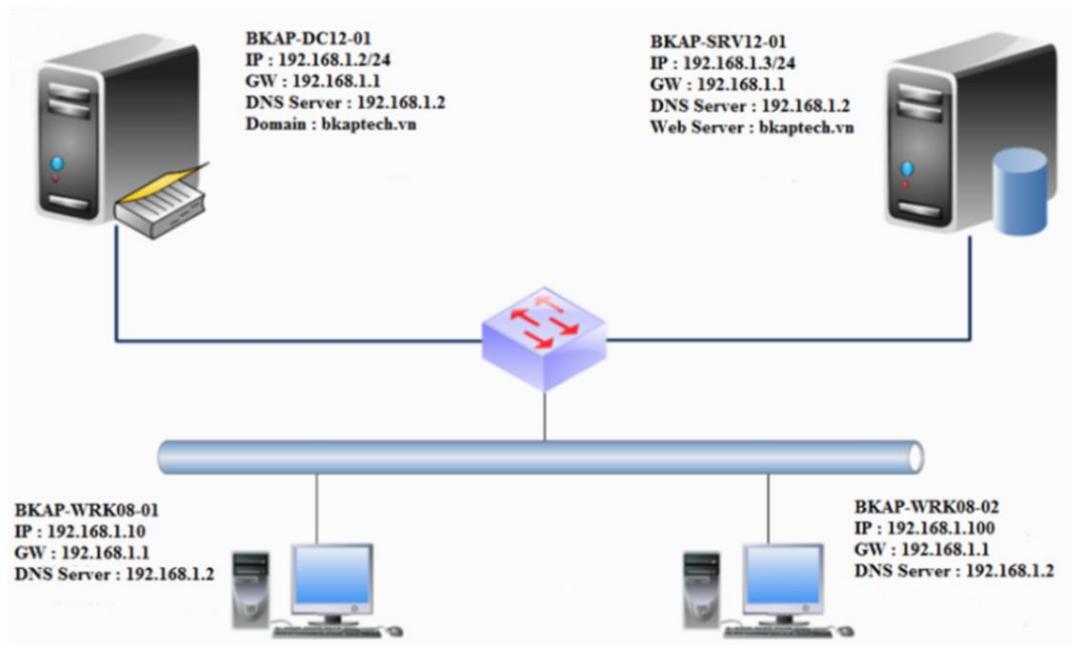
2. Yêu cầu chuẩn bị:

+ Chuẩn bị 2 máy Server và 1 máy Client theo mô hình.

- Máy *BKAP-DC12-01* làm **Domain Controller** cài đặt **DNS Server**.
- Máy *BKAP-SRV12-01* cài đặt và cấu hình **Web Server (IIS)**.
- Máy *BKAP-WRK08-01* dùng để truy cập vào **website**.

3. Mô hình Lab:

Lab 2.2 Cấu hình IIS Multi Website kết hợp DNS Server



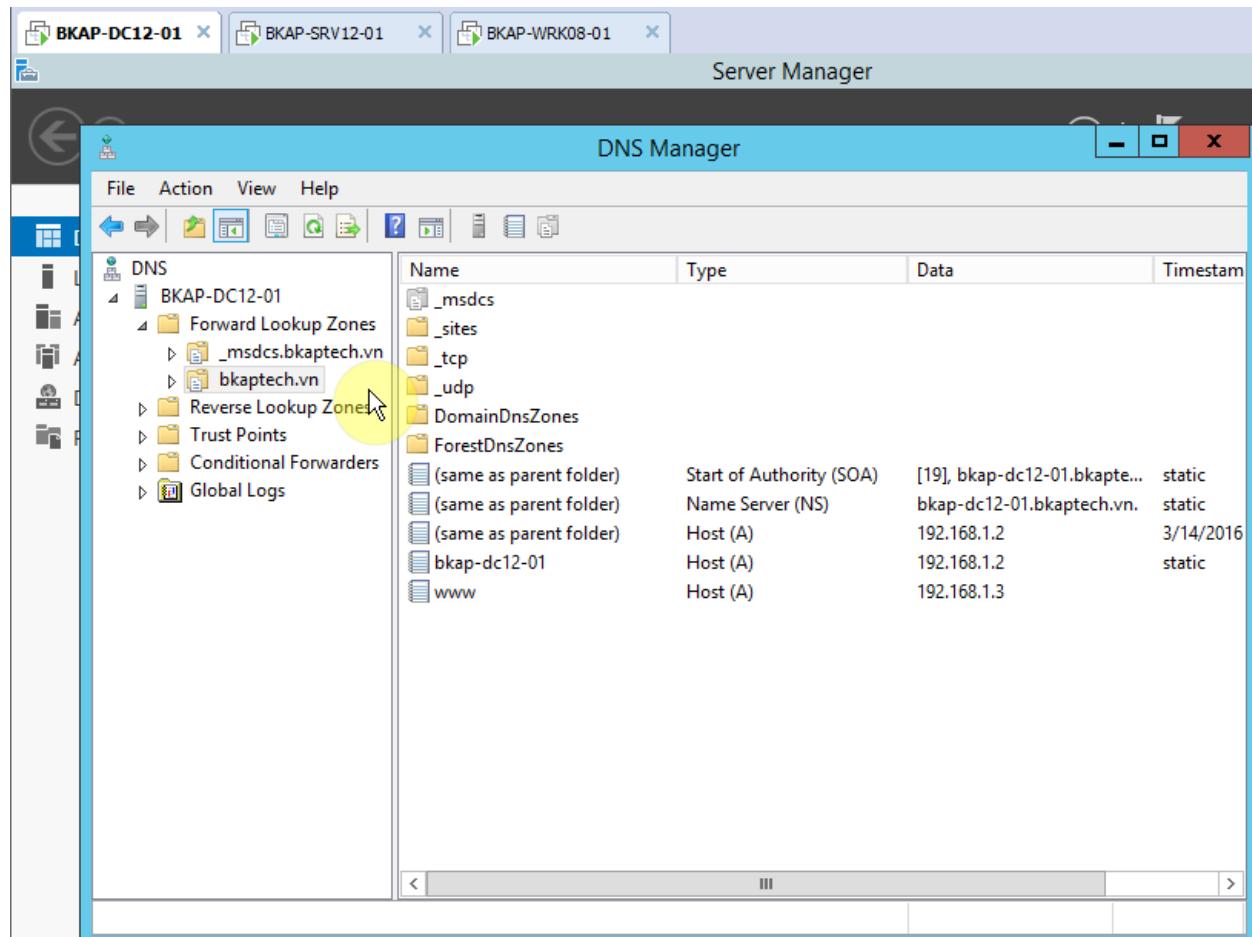
Hình 2.2

Sơ đồ địa chỉ như sau:

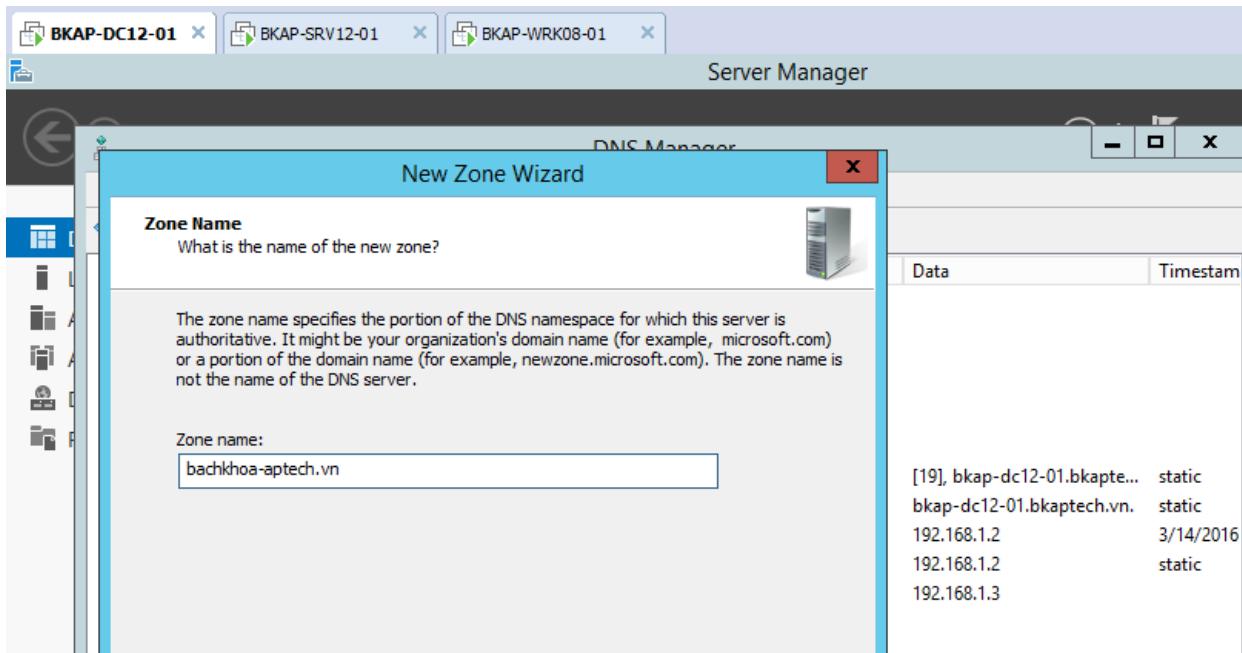
Thông số	BKAP-DC12-01	BKAP-SRV12-01	BKAP-WRK08-01
<i>IP address</i>	192.168.1.2	192.168.1.3	192.168.1.10
<i>Gateway</i>	192.168.1.1	192.168.1.1	192.168.1.1
<i>Subnet Mask</i>	255.255.255.0	255.255.255.0	255.255.255.0
<i>DNS Server</i>	192.168.1.2	192.168.1.2	192.168.1.2

Hướng dẫn chi tiết:

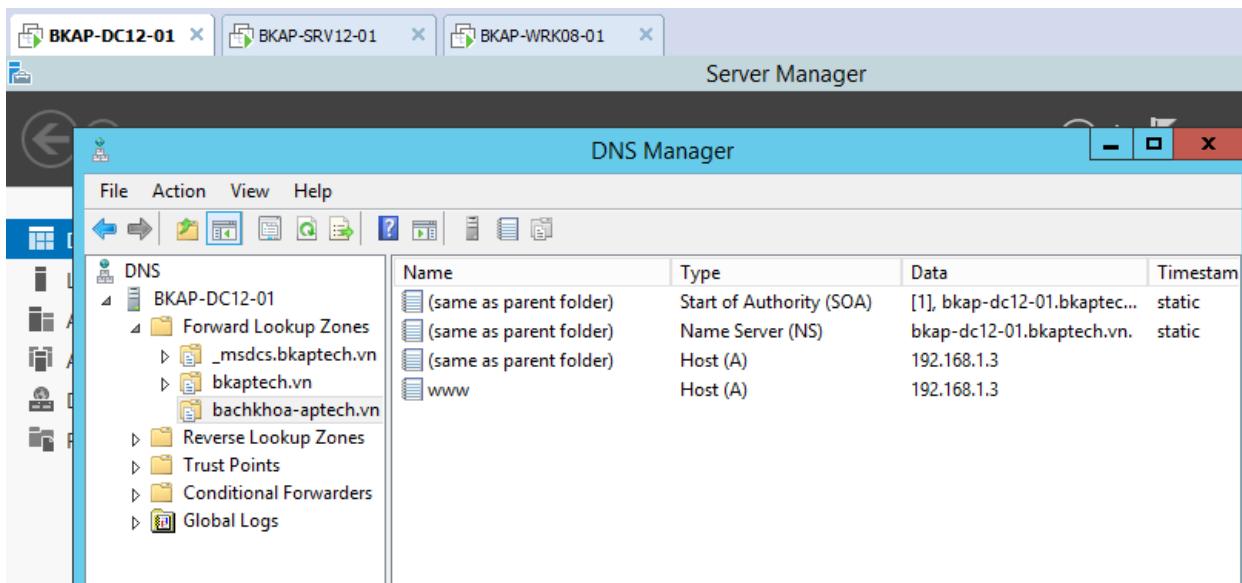
- Kết nối các máy ảo như hình trên , thực hiện ping thông giữa các máy trong mạng.
- Trên máy **BKAP-DC12-01**:
 - Cấu hình **DNS Server**.
 - Tạo bản ghi phân giải tên miền www.bkaptech.vn.



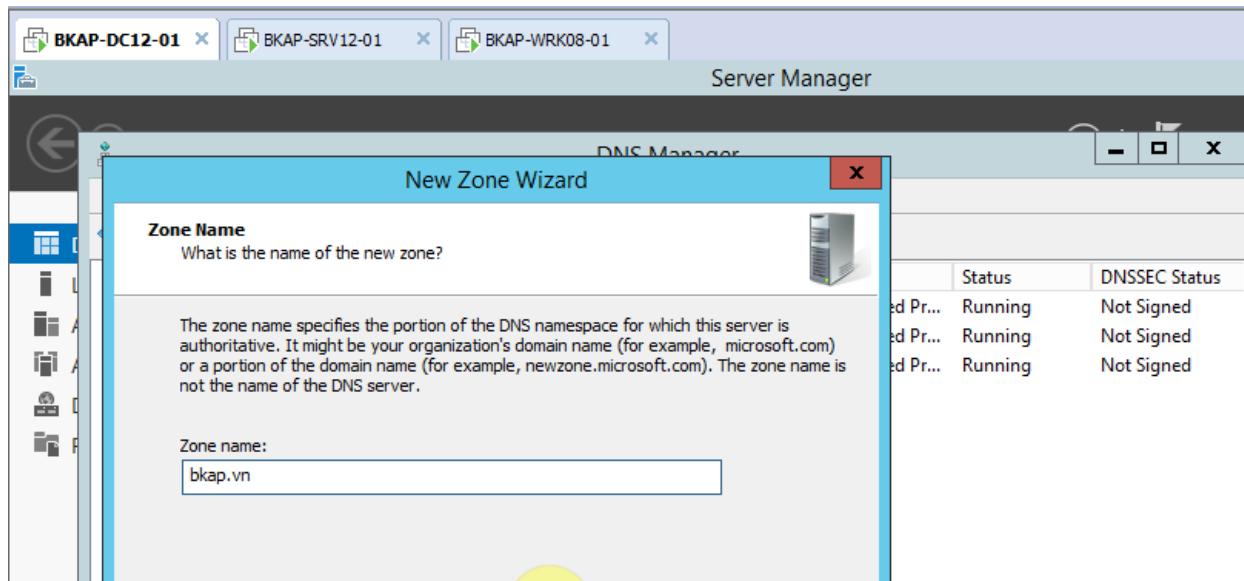
- Tạo Primary Zone cho site bachkhoa-aptech.vn.



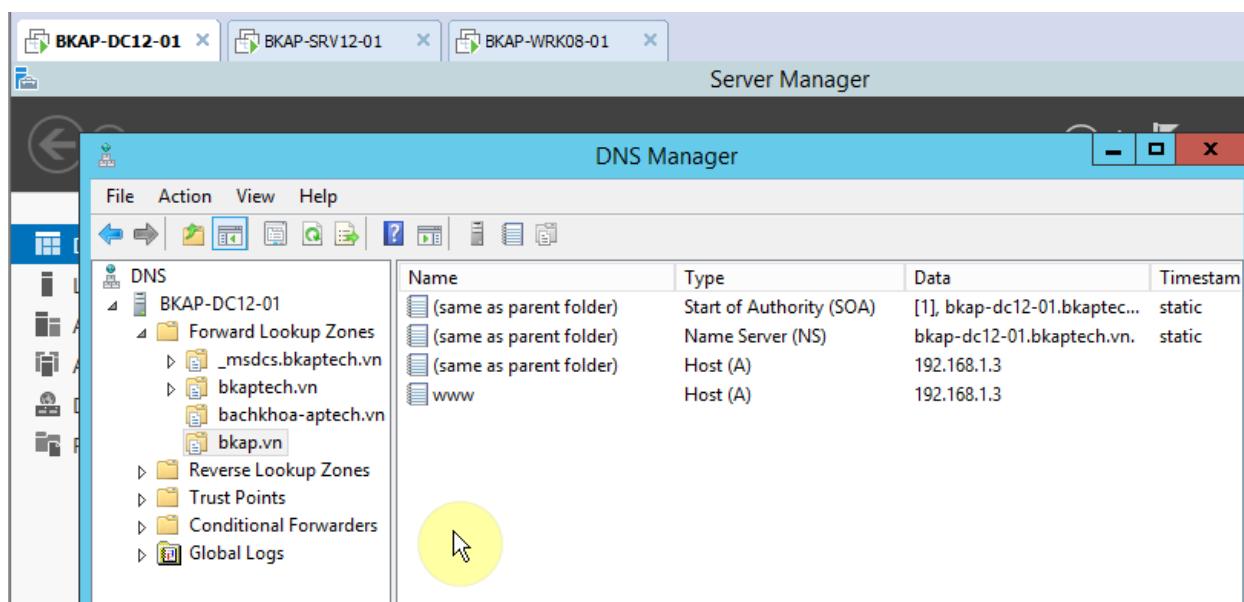
- Tạo bản ghi phân giải tên miền www.bachkhoa-aptech.vn



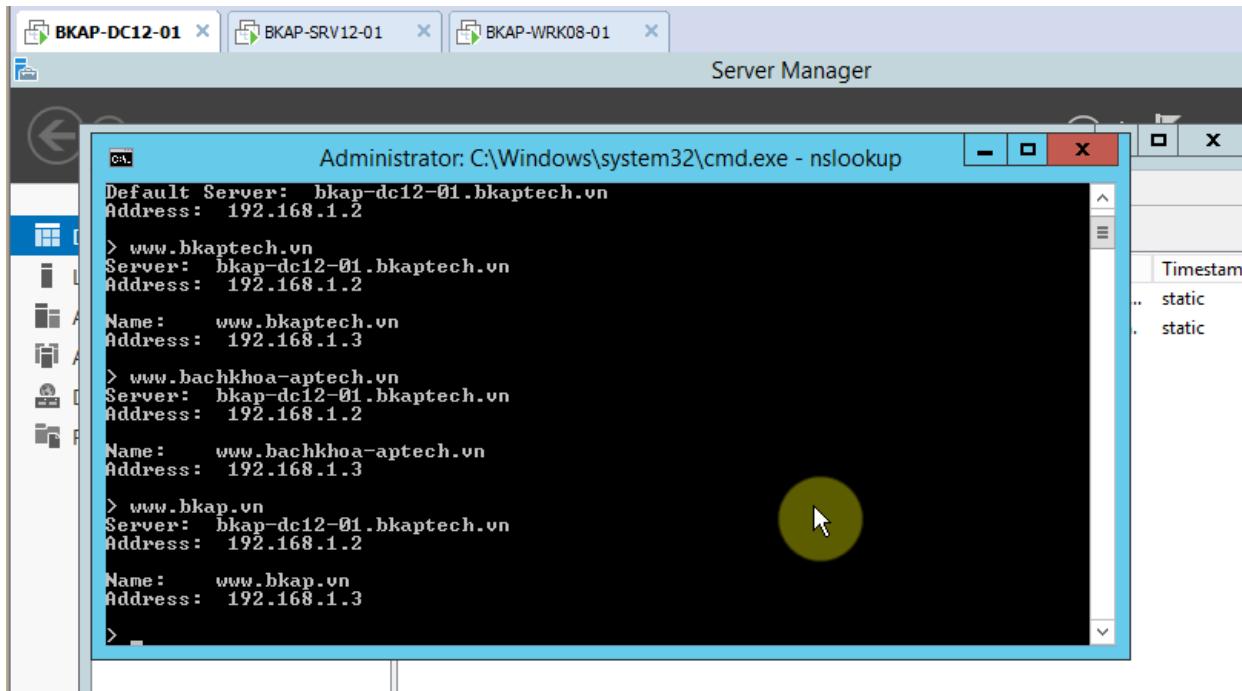
- Tạo Primary Zone cho site bkap.vn



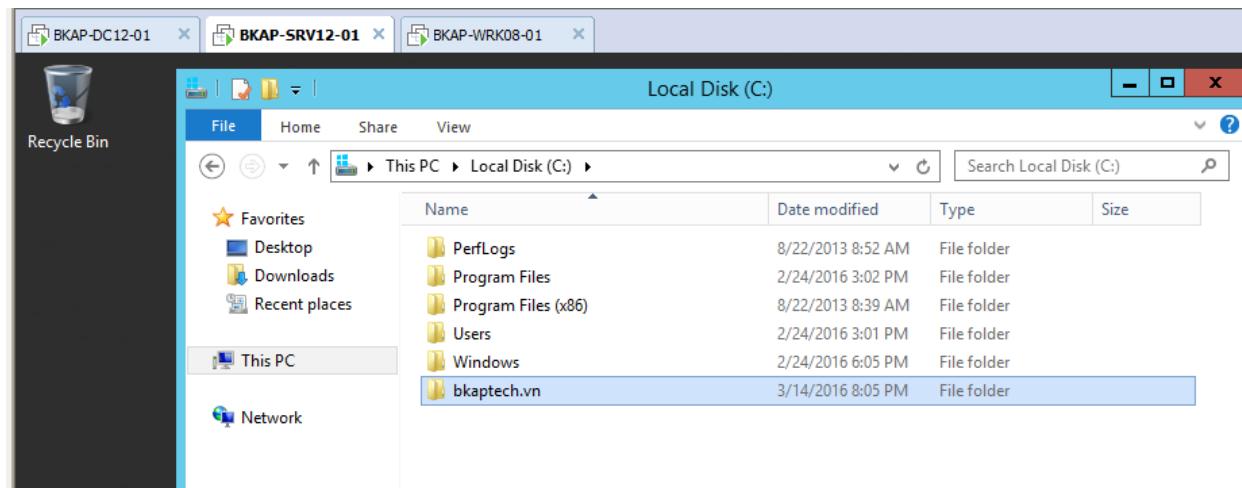
- Tạo bản ghi phân giải tên miền www.bkap.vn

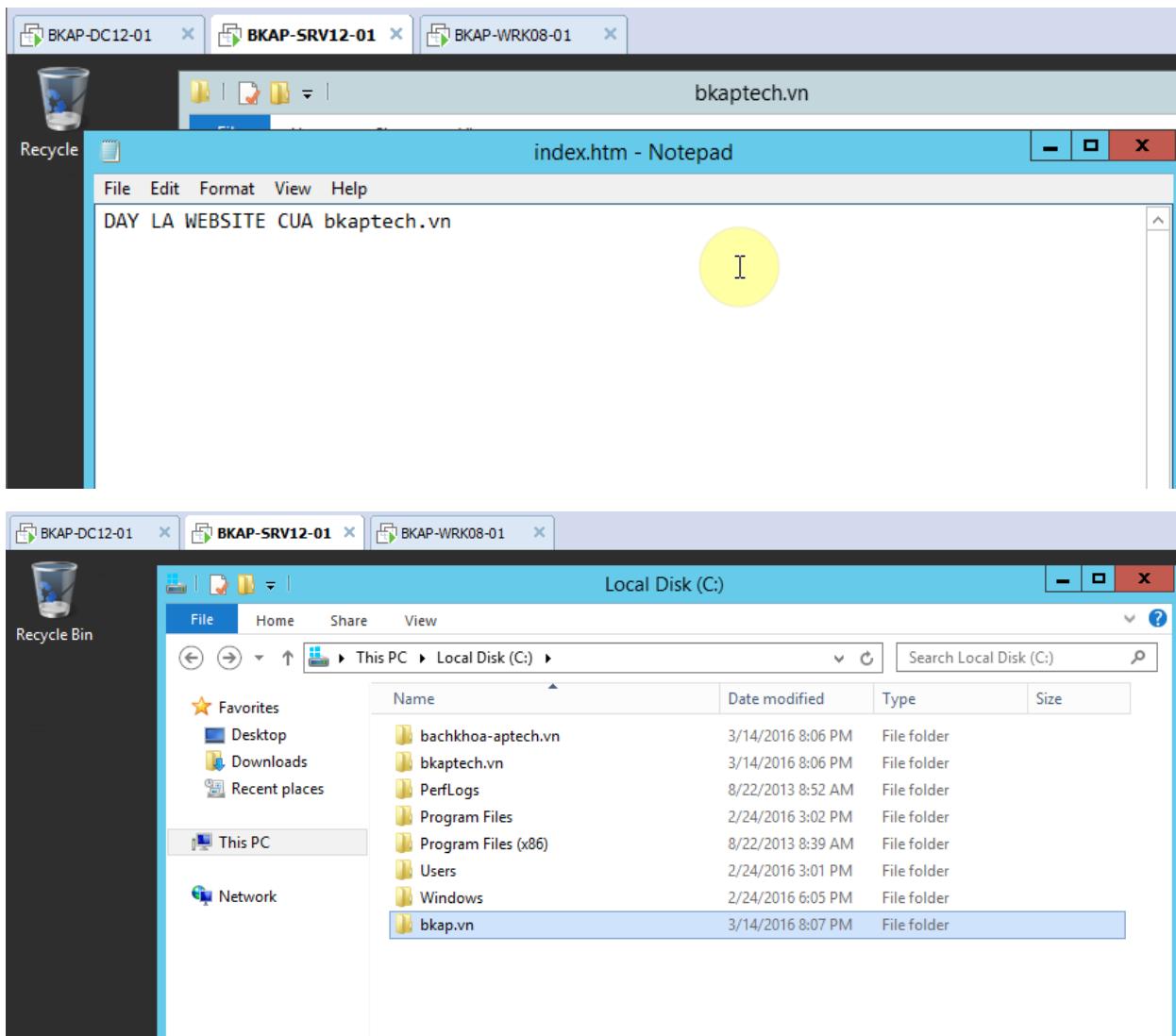


- Kiểm tra phân giải địa chỉ IP sang tên miền.

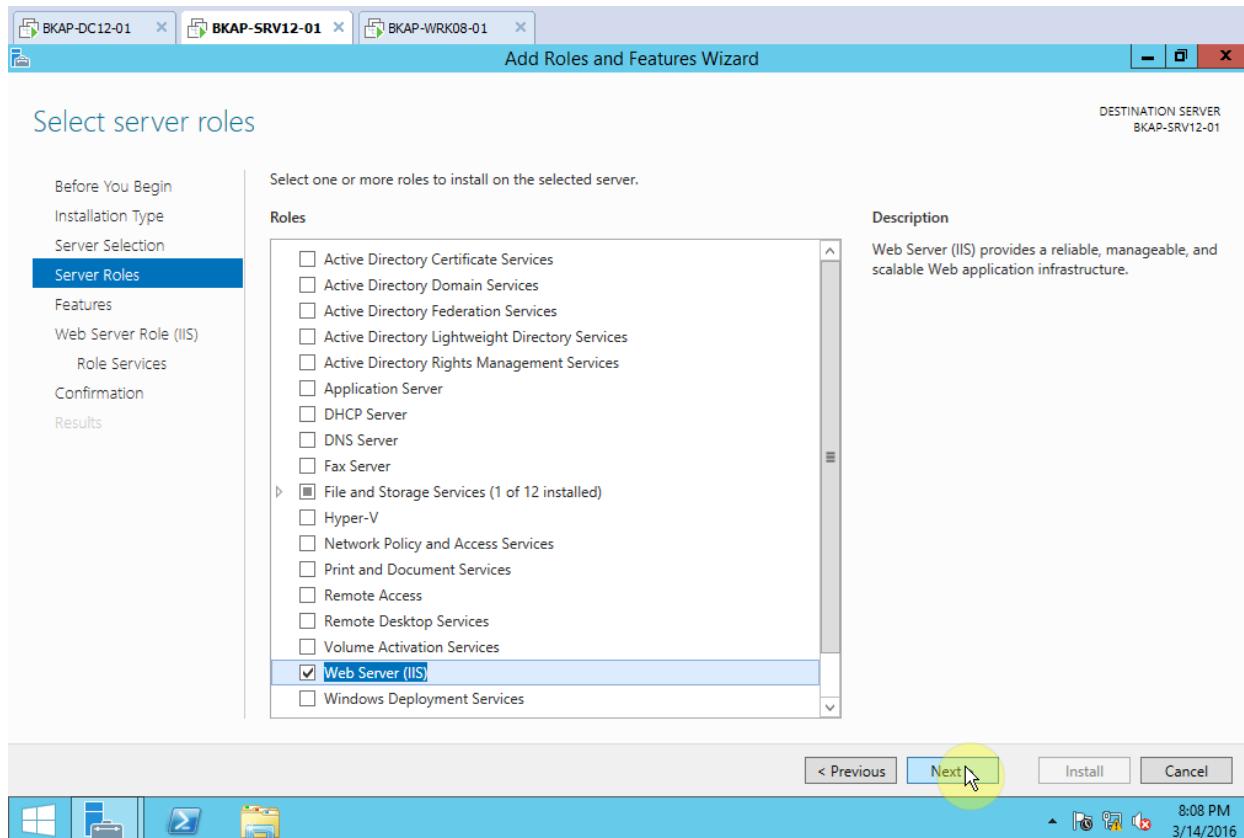


- Chuyển sang máy *BKAP-SRV12-01*, tạo dữ liệu và nội dung cho 3 website lưu trên ổ C.

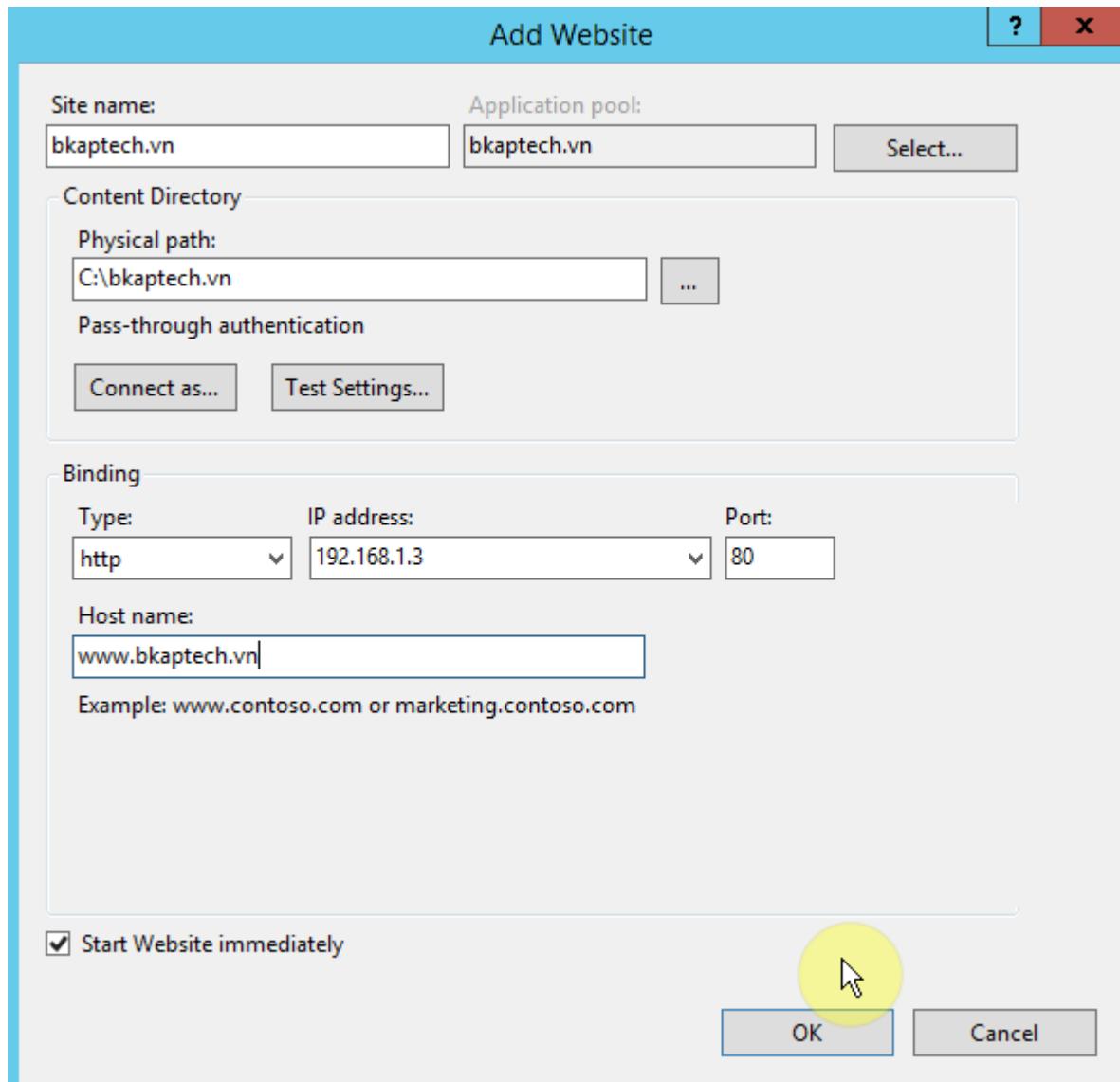




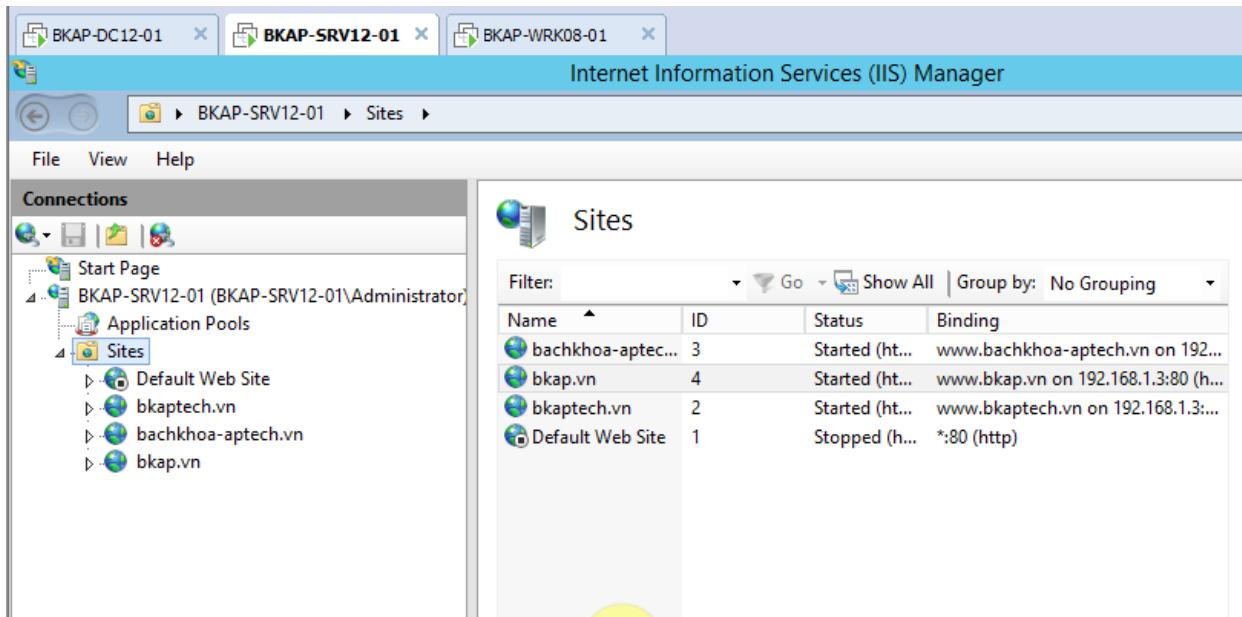
- Cài đặt dịch vụ Web Server (IIS).



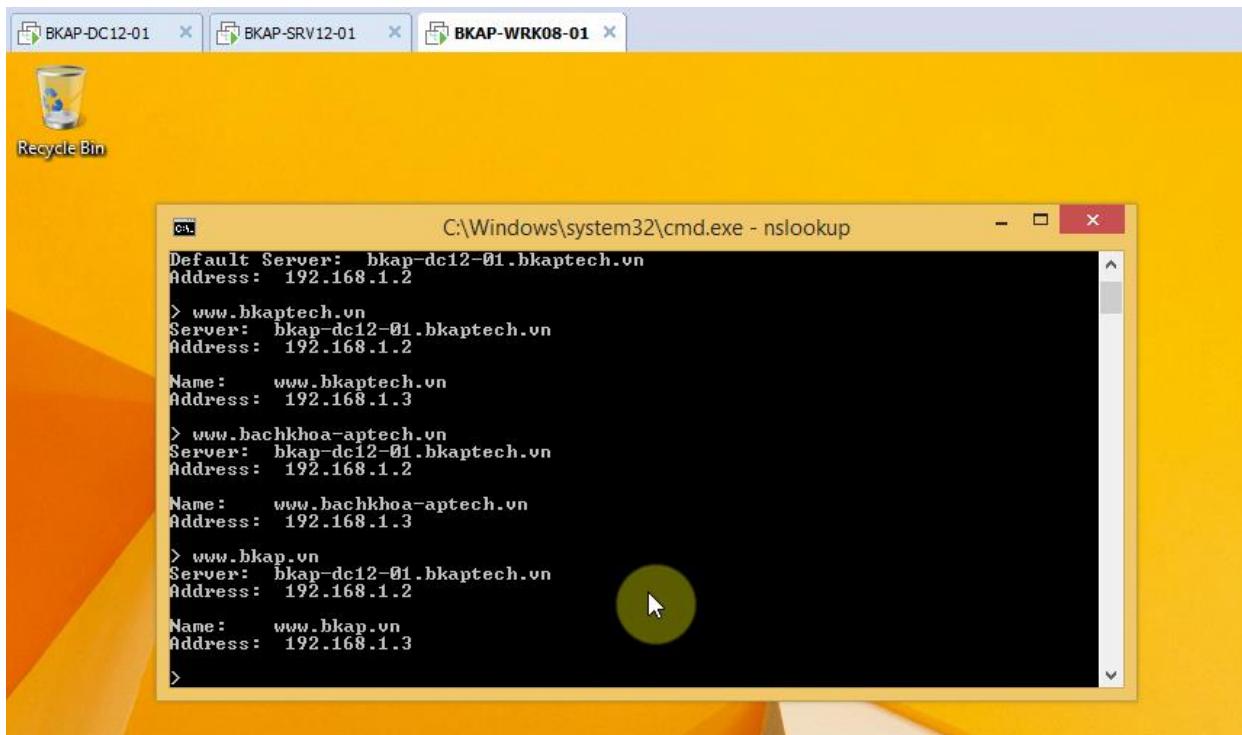
- Cấu hình dịch vụ IIS.
 - Tạo **Hosting Website** trên IIS với **multi Website** có tên là *bkaptech* , *bachkhoa-aptech* , *bkap*.
 - Tại cửa sổ **Add Website** nhập vào các thông số sau:



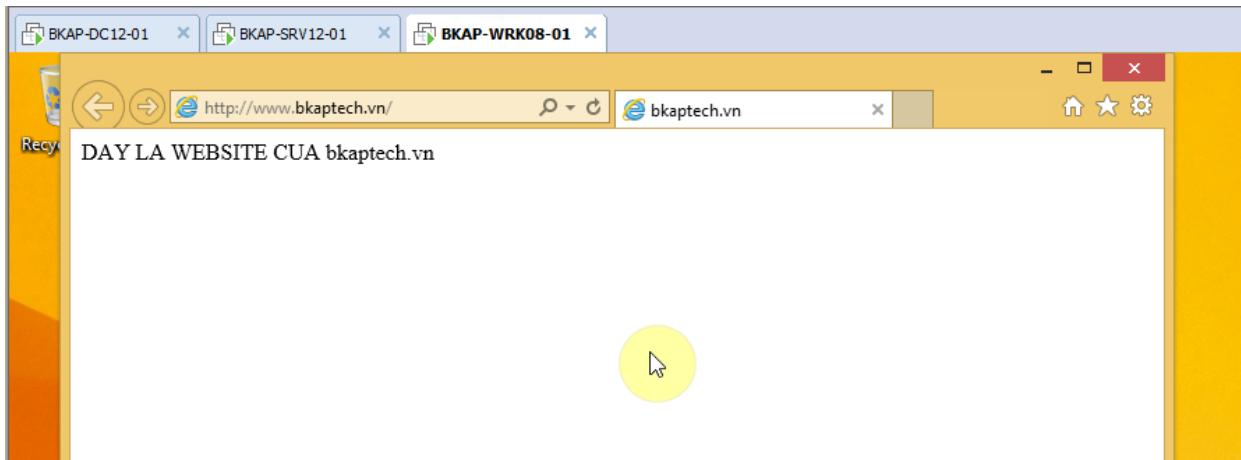
- Làm tương tự đối với các site còn lại, ta được kết quả sau:



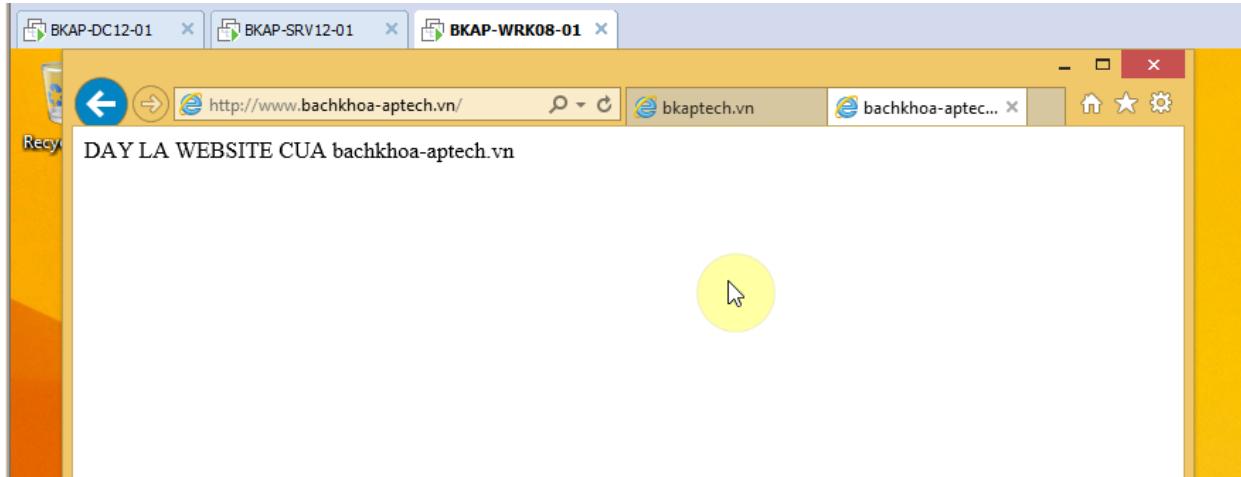
- Chuyển sang máy Client, kiểm tra phân giải từ IP sang tên miền.



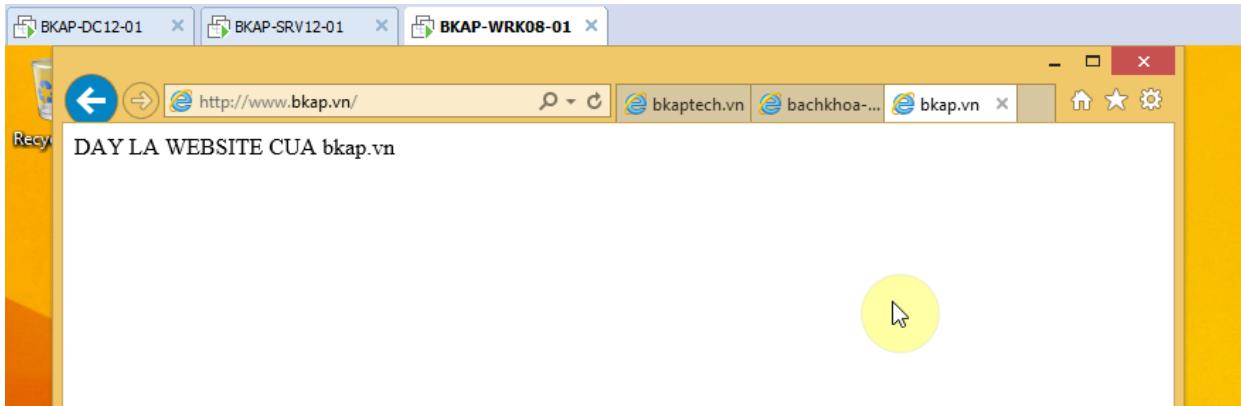
- Kiểm tra truy cập trang web www.bkaptech.vn.



- Kiểm tra truy cập trang web www.bachkhoa-aptech.vn



- Kiểm tra truy cập trang web www.bkap.vn



2.3 Sử dụng Active Directory Certificate Services để bảo mật Web Server.

1. Yêu cầu bài Lab:

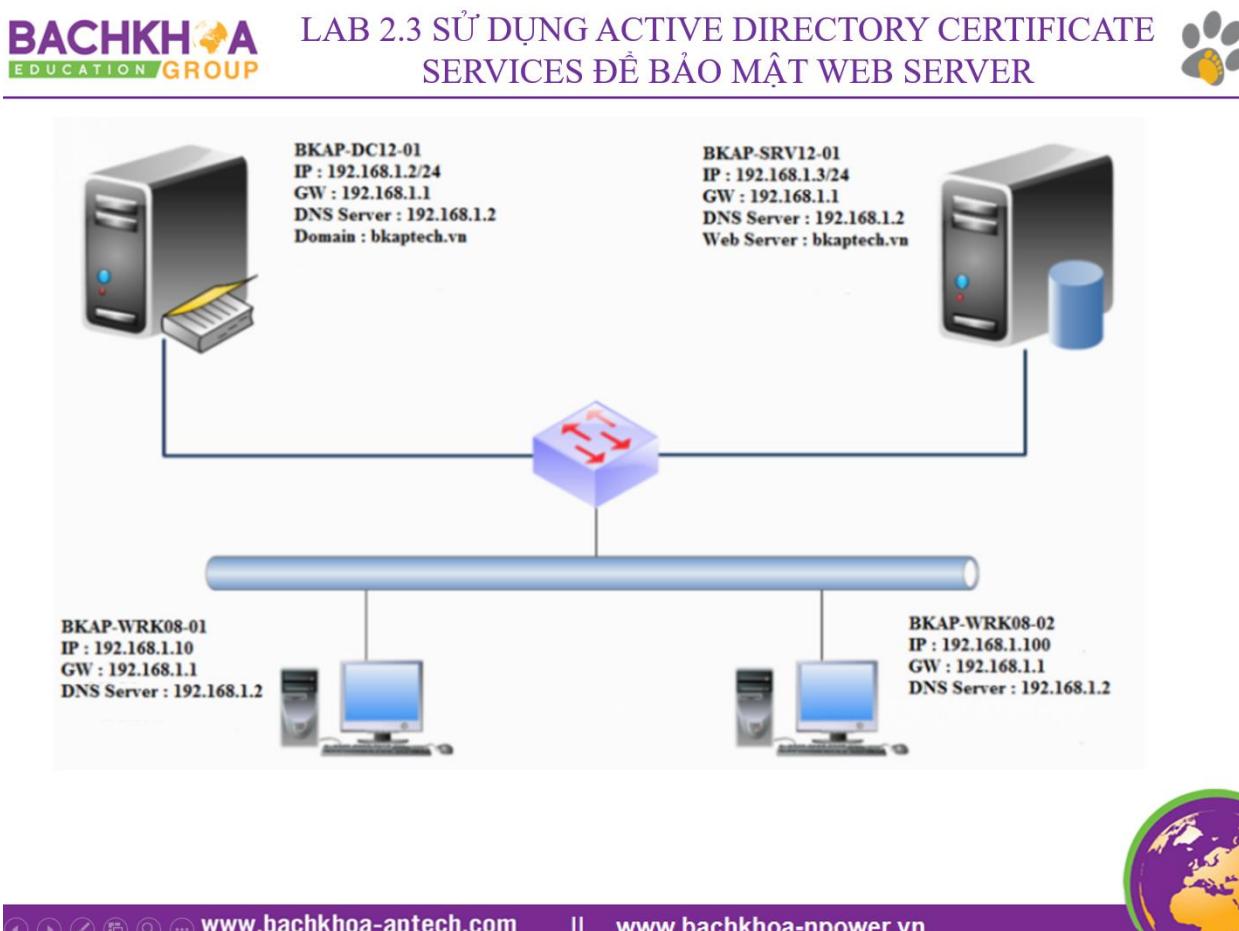
- + Trên máy **BKAP-DC12-01**, cài đặt và cấu hình **CA Server**.
- + Trên máy **BKAP-SRV12-01**, cài đặt và cấu hình **Web Server**, cấu hình giao thức **https**.
- + Trên máy **BKAP-WRK08-01**, kiểm tra truy cập **website** bằng giao thức **https** để kiểm tra.

2. Yêu cầu chuẩn bị:

- + Chuẩn bị 2 máy **Server** và 1 máy **Client**:

- Máy **BKAP-DC12-01** làm **Domain Controller** quản lý miền **bkaptech.vn**.
- Máy **BKAP-SRV12-01** cài đặt và cấu hình **Web Server (IIS)**.
- Máy **BKAP-WRK08-01** kiểm tra truy cập **website**.

3. Mô hình Lab:



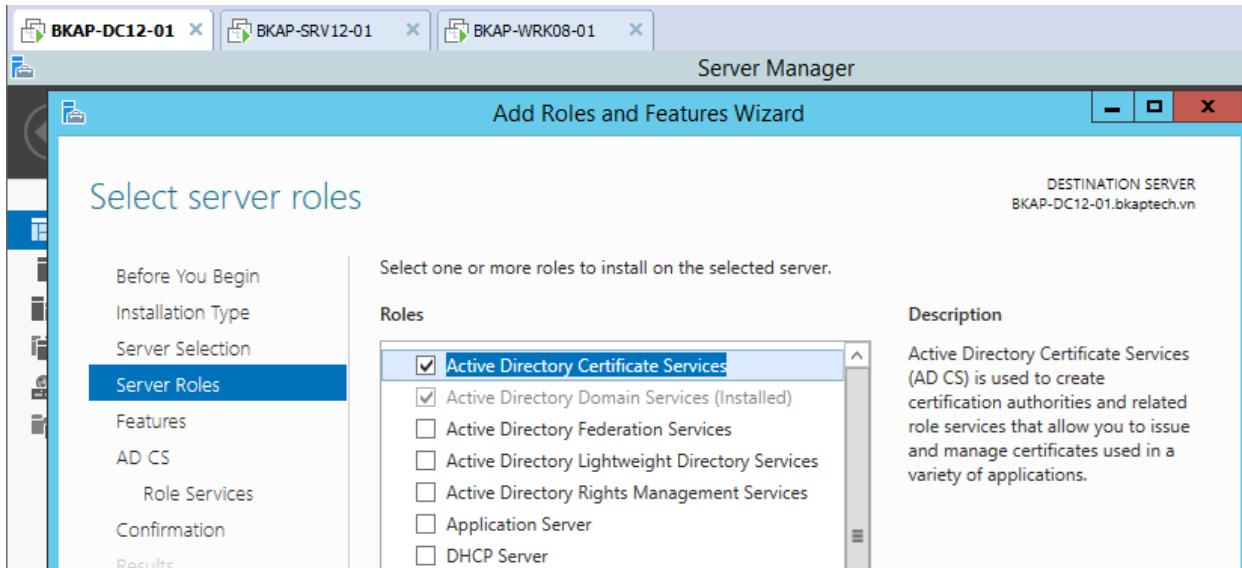
Hình 2.3

Sơ đồ địa chỉ như sau:

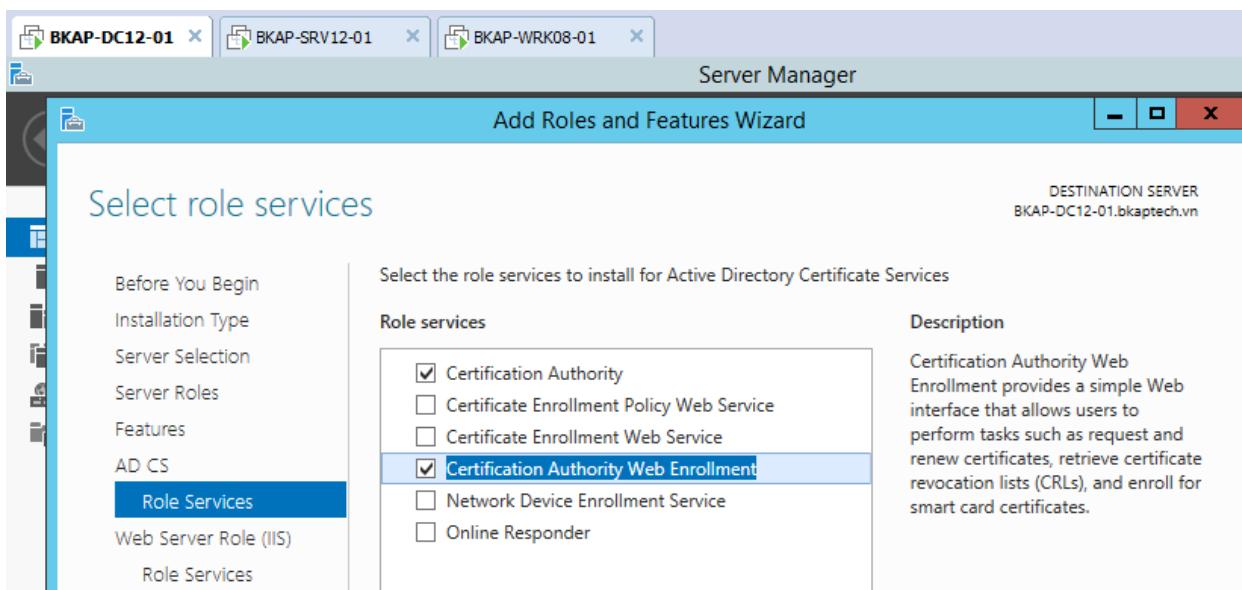
Thông số	BKAP-DC12-01	BKAP-SRV12-01	BKAP-WRK08-01
<i>IP address</i>	192.168.1.2	192.168.1.3	192.168.1.10
<i>Gateway</i>	192.168.1.1	192.168.1.1	192.168.1.1
<i>Subnet Mask</i>	255.255.255.0	255.255.255.0	255.255.255.0
<i>DNS Server</i>	192.168.1.2	192.168.1.2	192.168.1.2

Hướng dẫn chi tiết:

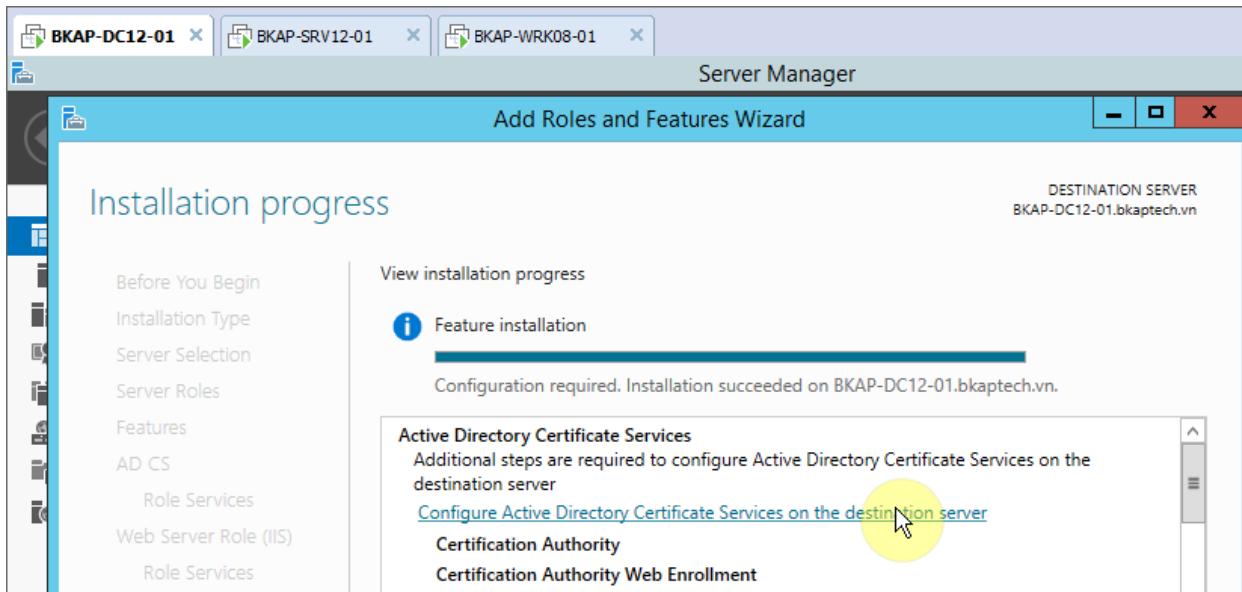
- Mở các máy ảo , kết nối như hình trên, thực hiện ping thông giữa các máy trong mạng.
- Trên máy **BKAP-DC12-01** , cài đặt và cấu hình **CA Server**.
 - Cài đặt **CA Server**.
 - Server Manager / Add roles and features / click chọn vào Active Directory Certificate Services**



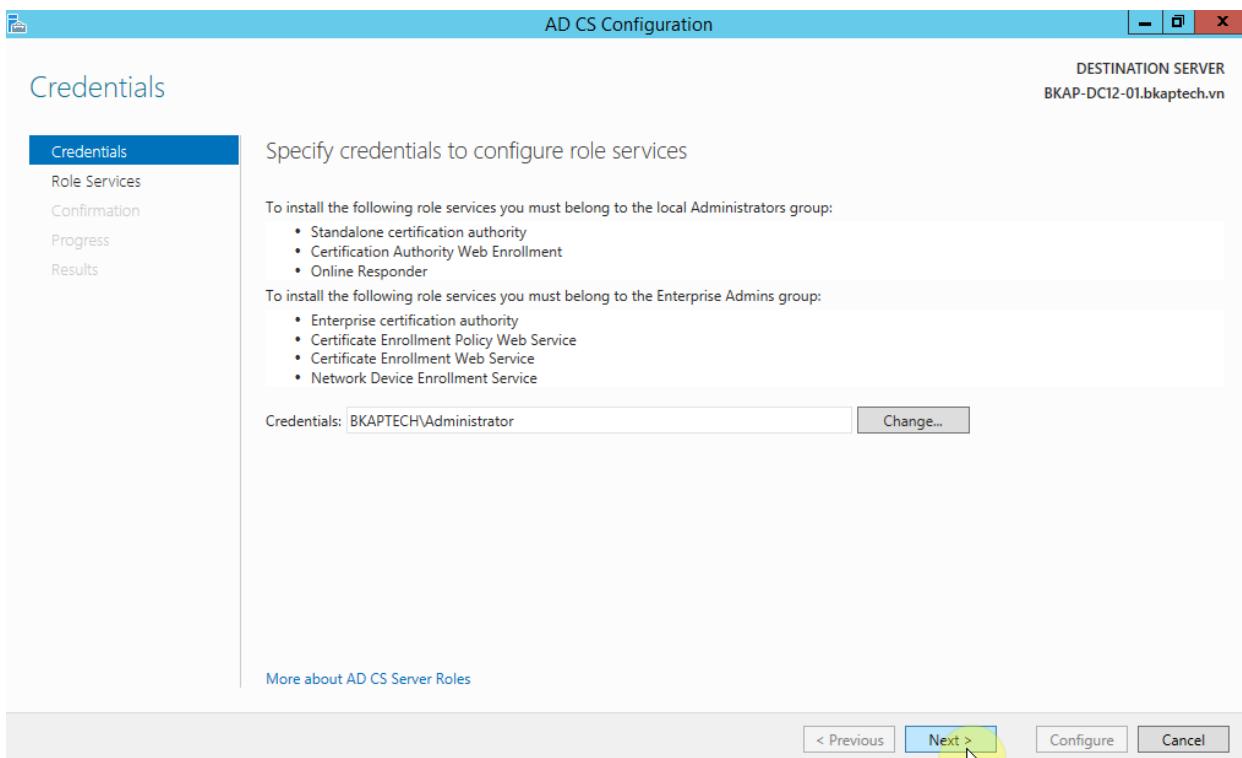
- Tại cửa sổ **Select role services**, , chọn vào **Certification Authority** và **Certification Authority Web Enrollment**.



- Click vào **Next**.
- Tại cửa sổ **Installation progress**, click tại dòng **Configure Active Directory Certificate Services on the destination server**.



- Tại cửa sổ **AD CS Configuration / Credentials**, click vào **Next**.



- Tại cửa sổ **Role Services**, click chọn vào **Certification Authority** và **Certification Authority Web Enrollment**.

AD CS Configuration

Role Services

Credentials

Role Services

- Setup Type
- CA Type
- Private Key
- Cryptography
- CA Name
- Validity Period
- Certificate Database
- Confirmation
- Progress

Select Role Services to configure

- Certification Authority
- Certification Authority Web Enrollment
- Online Responder
- Network Device Enrollment Service
- Certificate Enrollment Web Service
- Certificate Enrollment Policy Web Service

- Tại cửa sổ **Setup Type**, click chọn vào **Standalone CA**.

AD CS Configuration

Setup Type

Credentials

Role Services

Setup Type

- CA Type
- Private Key
- Cryptography
- CA Name
- Validity Period
- Certificate Database
- Confirmation
- Progress

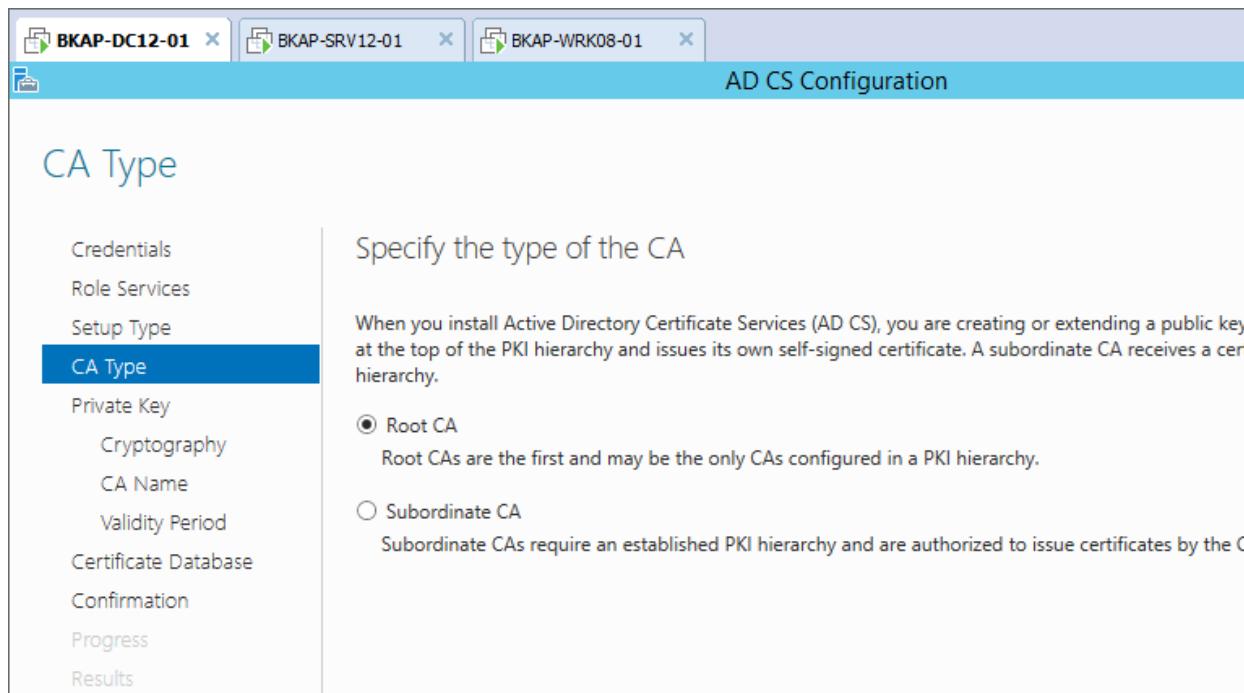
Specify the setup type of the CA

Enterprise certification authorities (CAs) can use Active Directory Domain Services (AD DS) to simplify the CAs do not use AD DS to issue or manage certificates.

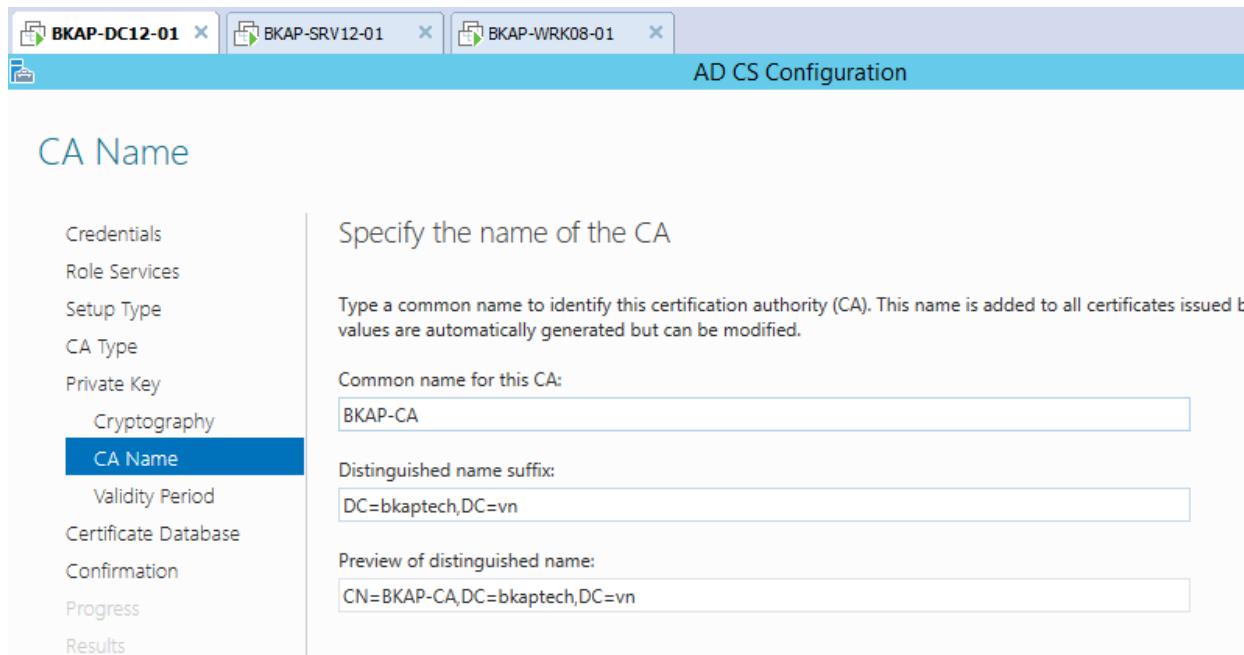
Enterprise CA
 Enterprise CAs must be domain members and are typically online to issue certificates or certificate pol

Standalone CA
 Standalone CAs can be members or a workgroup or domain. Standalone CAs do not require AD DS an connection (offline).

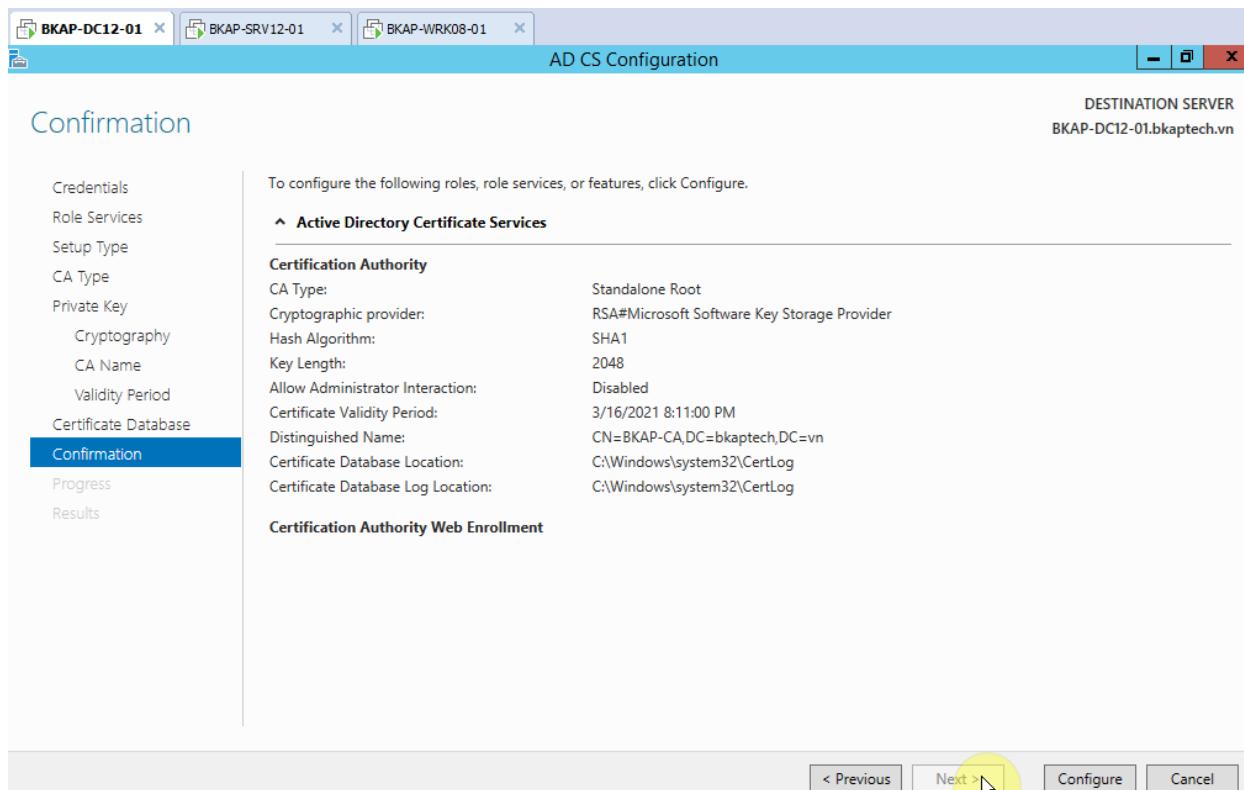
- Tại cửa sổ **CA Type**, click chọn vào **Root CA**.



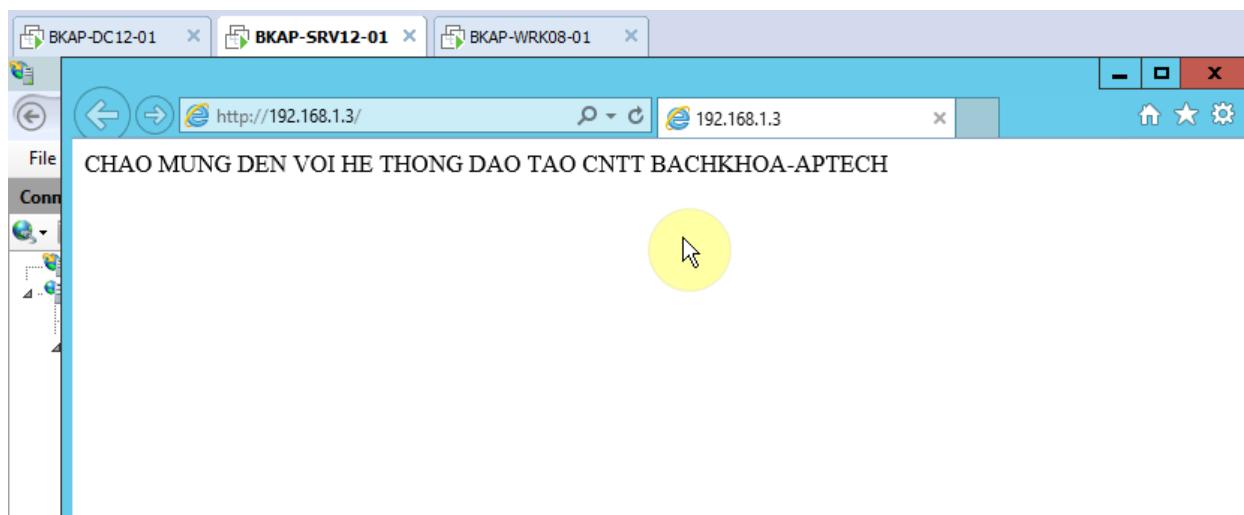
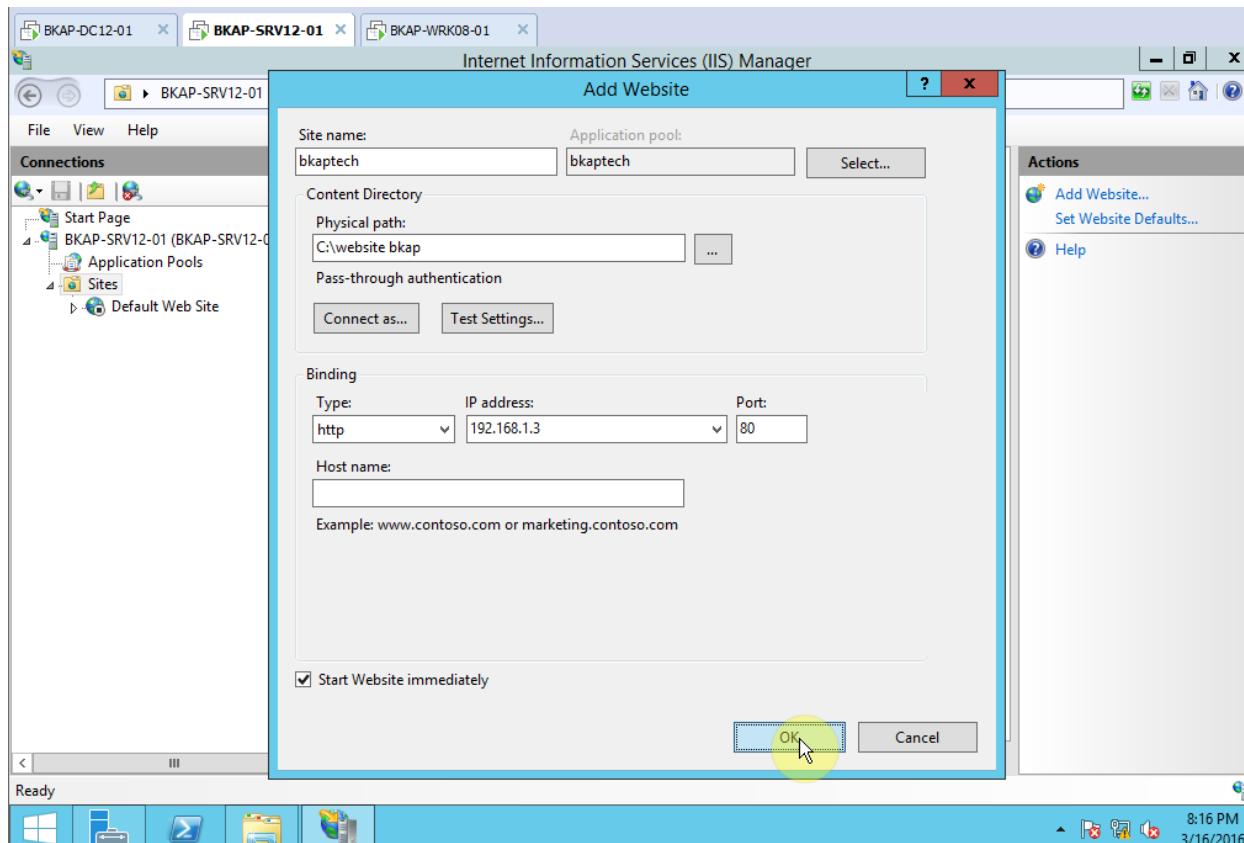
- Tại cửa sổ **CA Name**, tại mục **Common name for this CA**, nhập vào tên **BKAP-CA**.



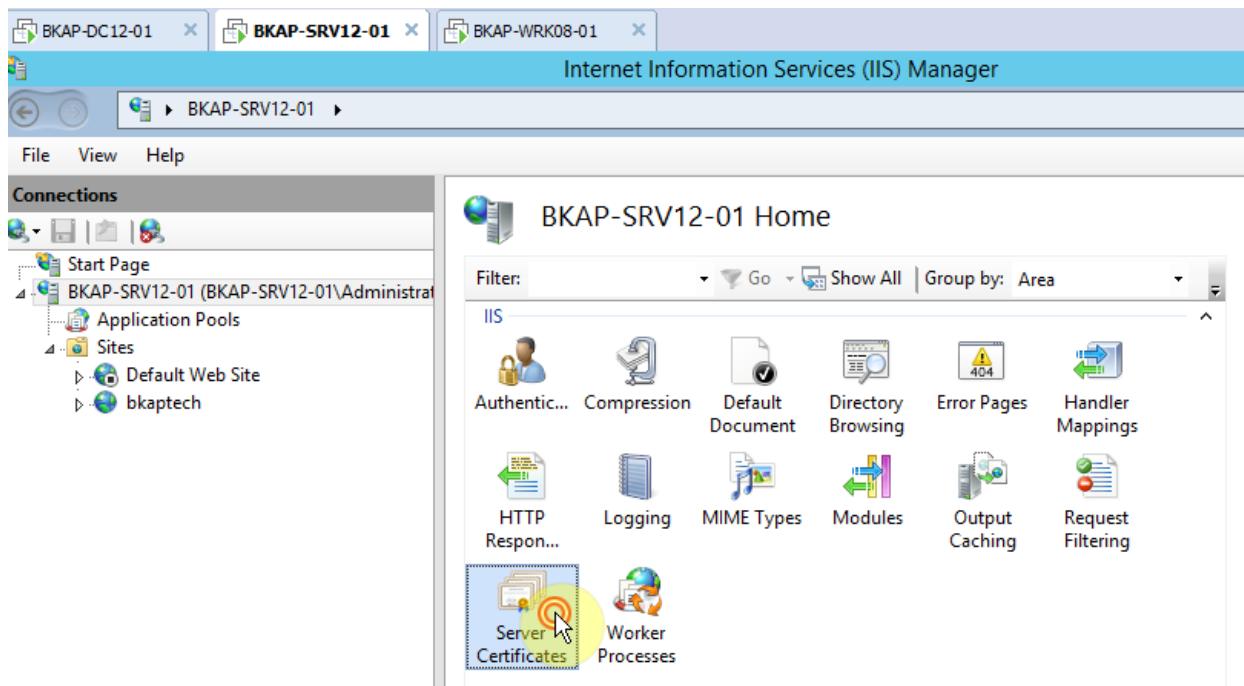
- Tại cửa sổ **Confirmation**, click vào **Configure**.



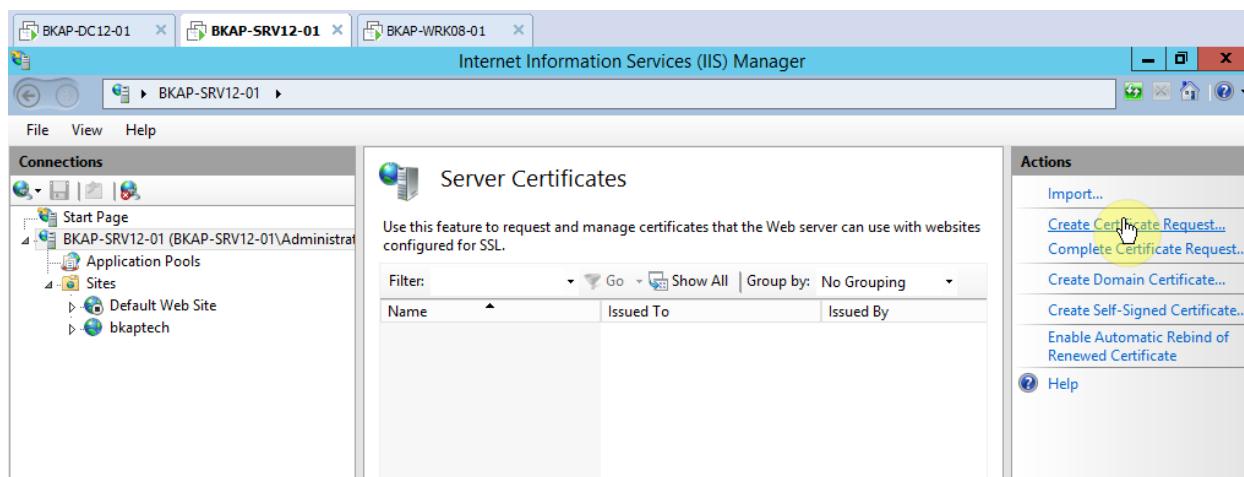
- Chuyển sang máy **BKAP-SRV12-01**, cài đặt và cấu hình Web Server (IIS).



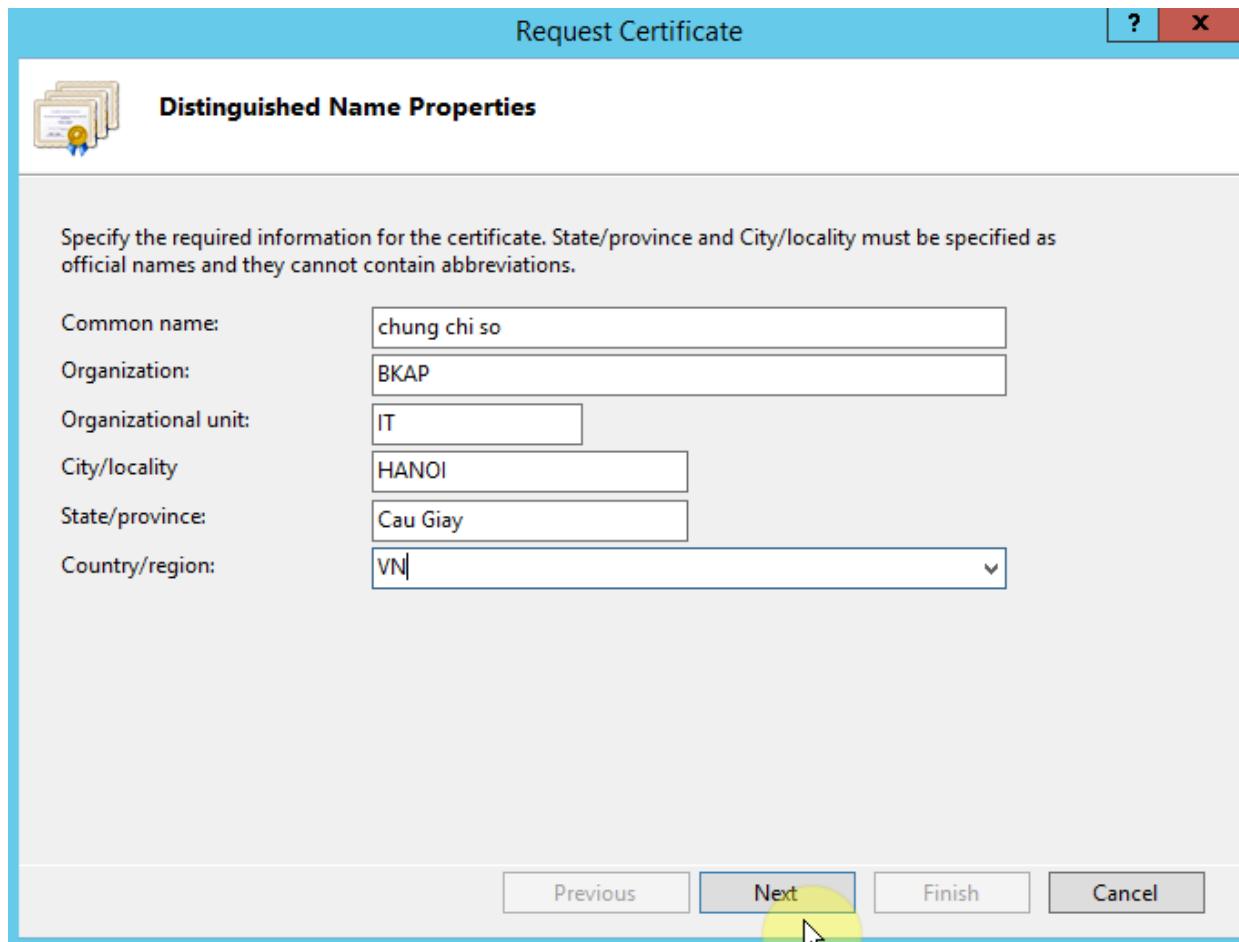
- Thực hiện xin chứng chỉ từ CA Server.
 - Tại cửa sổ **BKAP-SRV12-01 Home** (*trong IIS*) , click chọn **Server Certificates**.



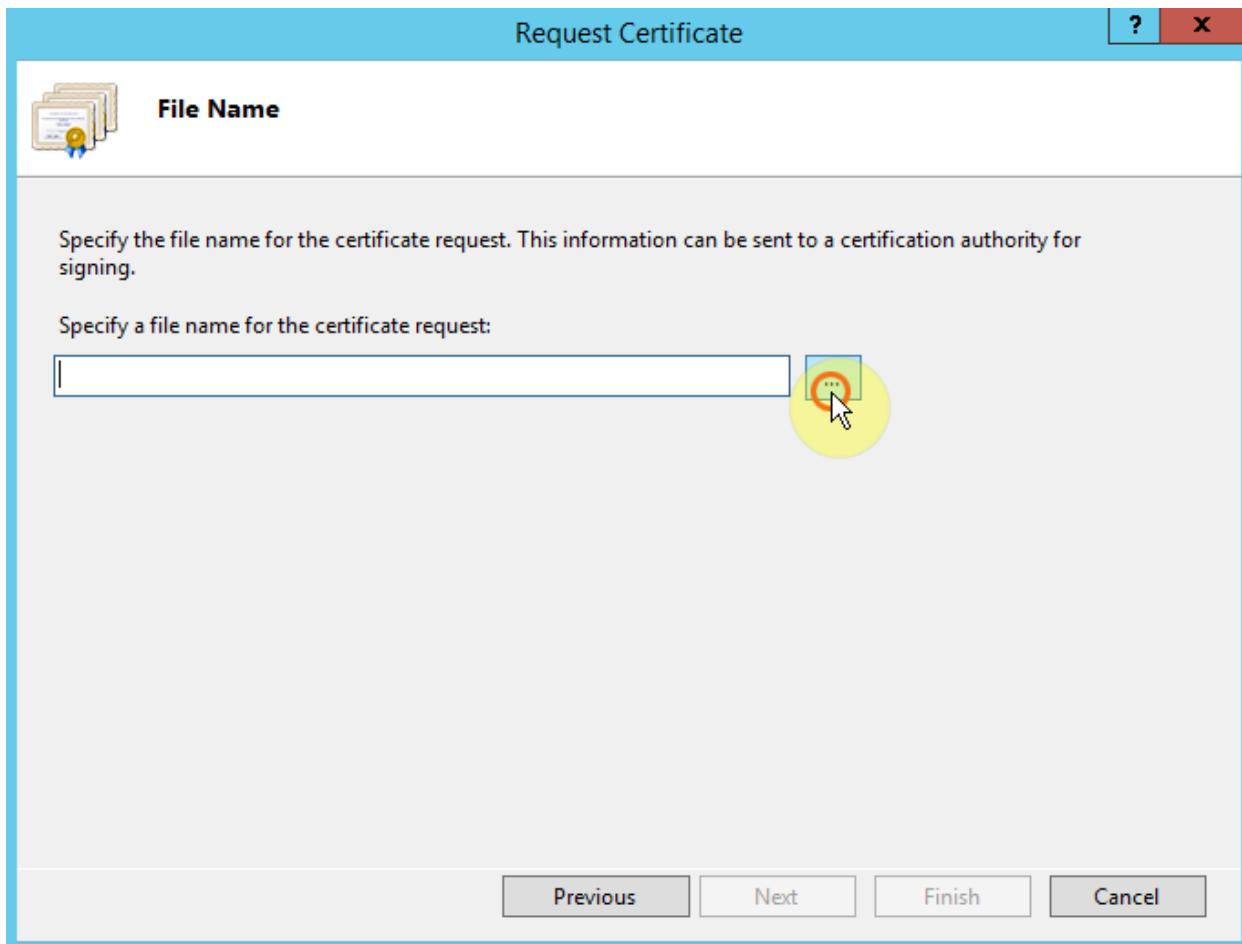
- Click chọn vào **Create Certificate Request...**



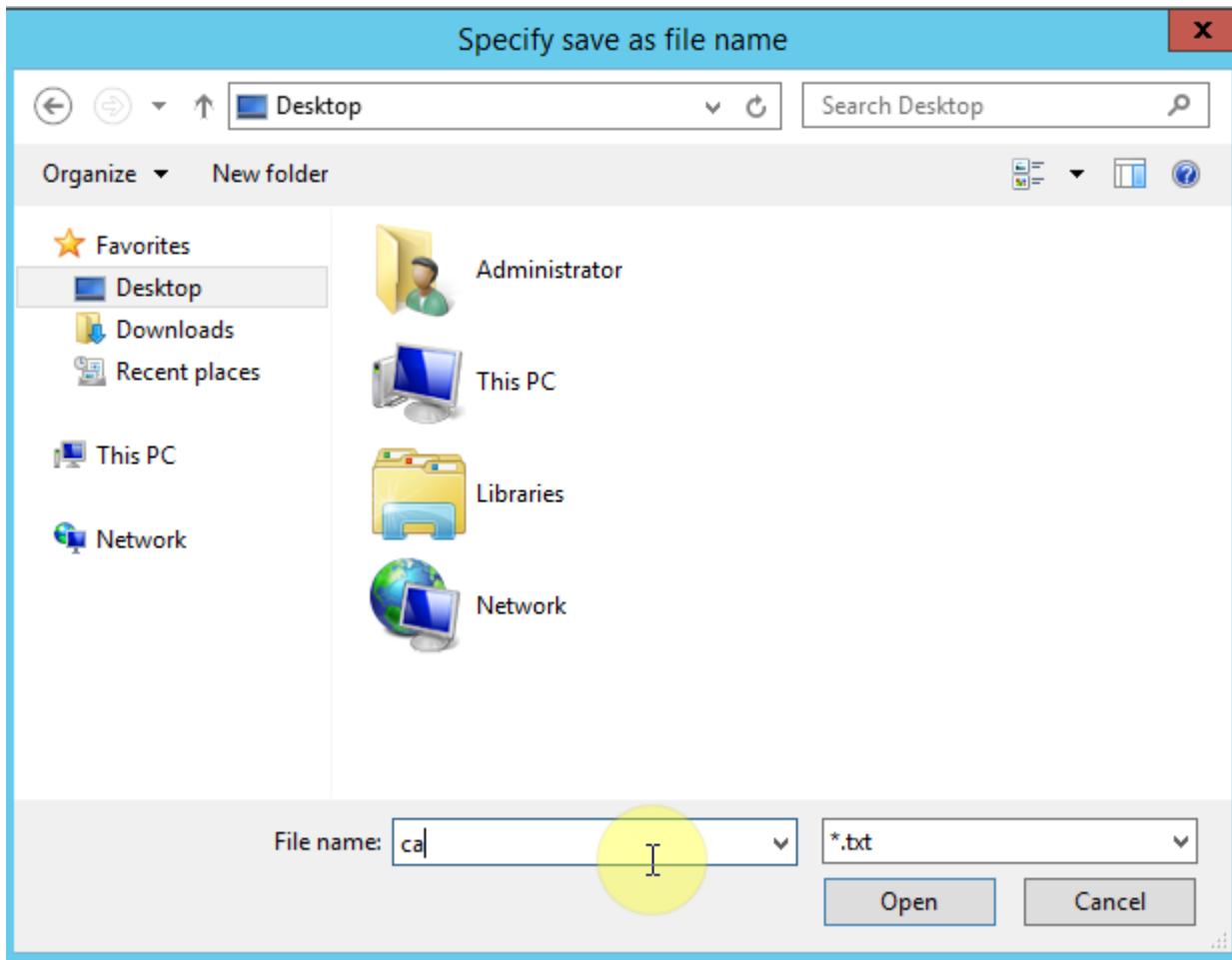
- Trong cửa sổ **Request Certificate**, nhập vào các thông số sau:



- Tại cửa sổ **File Name**, click chọn vào biểu tượng “...”.



- Lưu file với tên **ca.txt**.



? X

File Name

Specify the file name for the certificate request. This information can be sent to a certification authority for signing.

Specify a file name for the certificate request:

C:\Users\Administrator\Desktop\ca.txt

...

Previous Next  Finish Cancel

- Vào IE, truy cập địa chỉ **192.168.1.2/certsrv**, click chọn vào Request a Certificate.

Microsoft Active Directory Certificate Services -- BKAP-CA

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).

Select a task:

- [Request a certificate](#)
- [View the status of a pending certificate request](#)
- [Download a CA certificate, certificate chain, or CRL](#)

- Tại cửa sổ **Request a Certificate**, click chọn vào **advanced certificate request**.

Microsoft Active Directory Certificate Services -- BKAP-CA

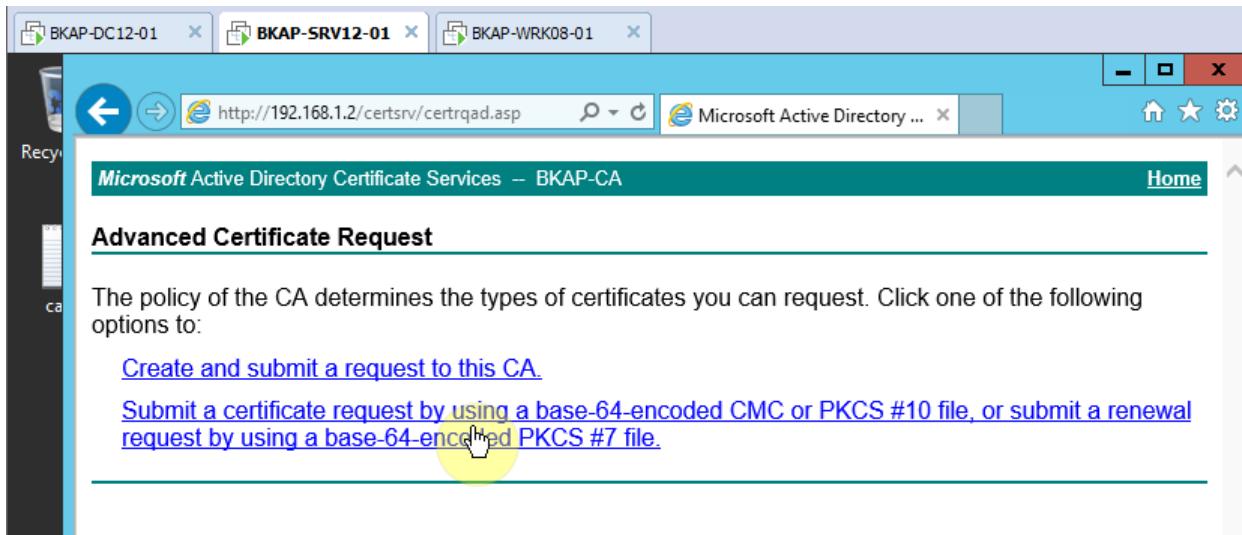
Request a Certificate

Select the certificate type:

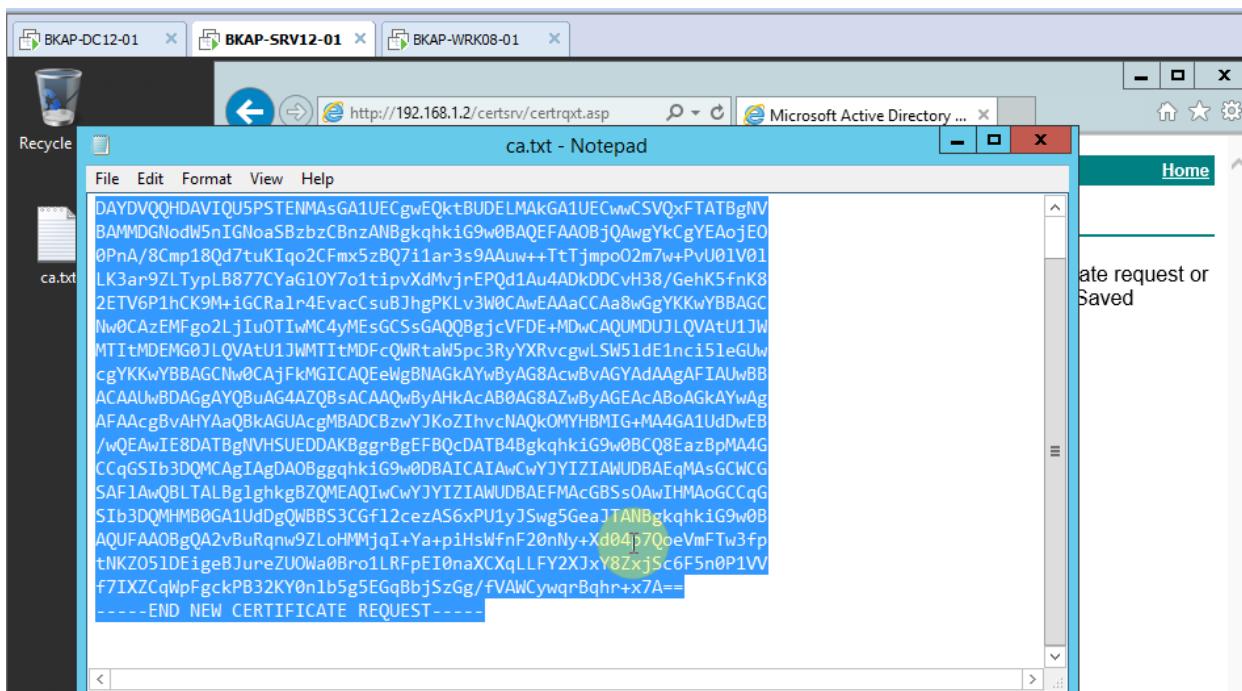
- [Web Browser Certificate](#)
- [E-Mail Protection Certificate](#)

Or, submit an [advanced certificate request](#).

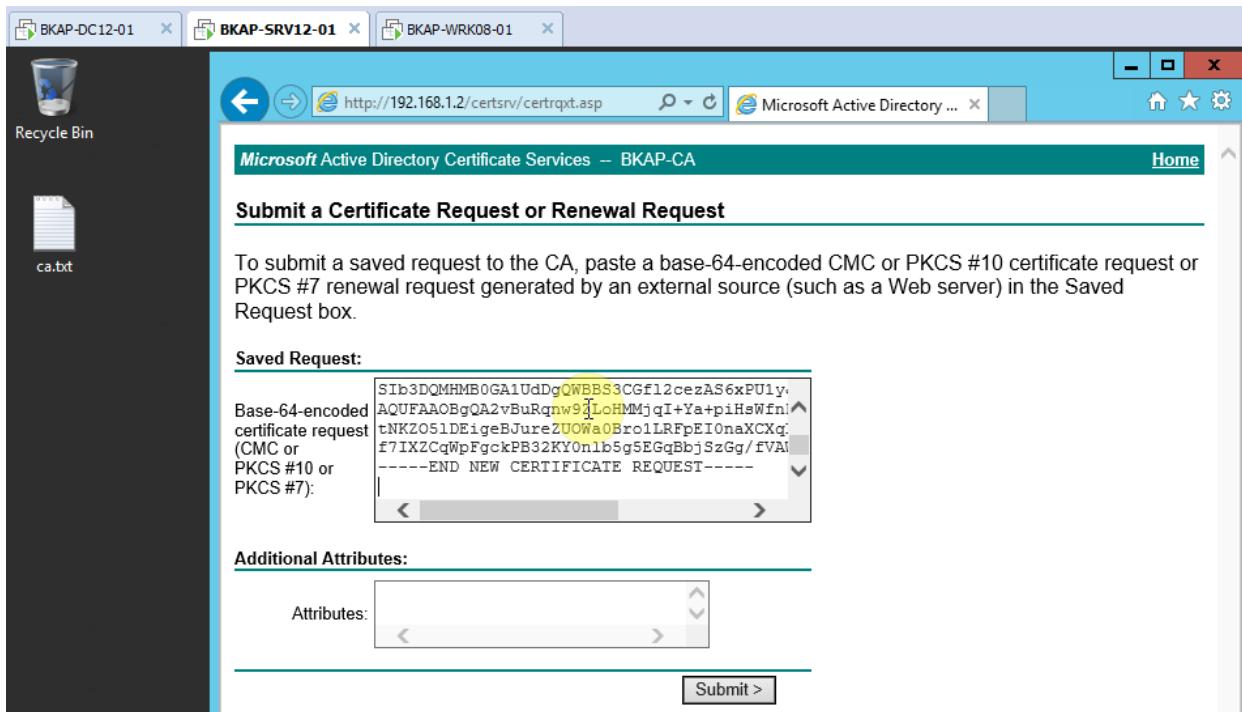
- Tại cửa sổ **Advanced Certificate Request**, click chọn vào **Submit a certificate request by using**



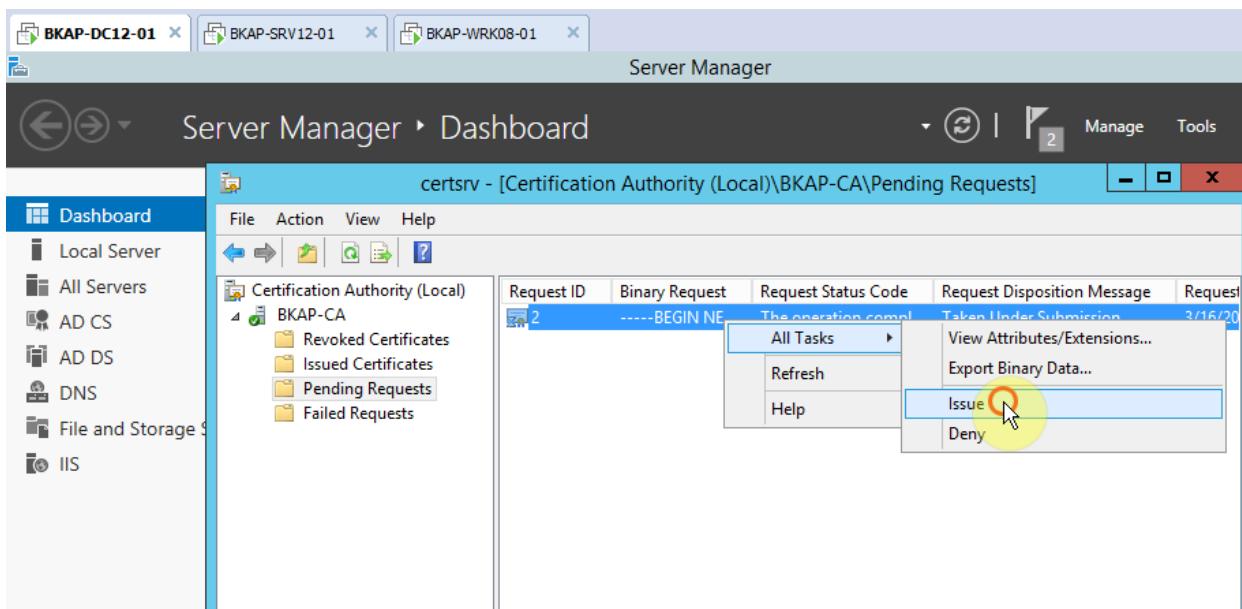
- Mở file **ca.txt**, copy toàn bộ nội dung file vào mục **Base-64-encoded...** trong cửa sổ **Submit a Certificate Request or Renewal Request.**



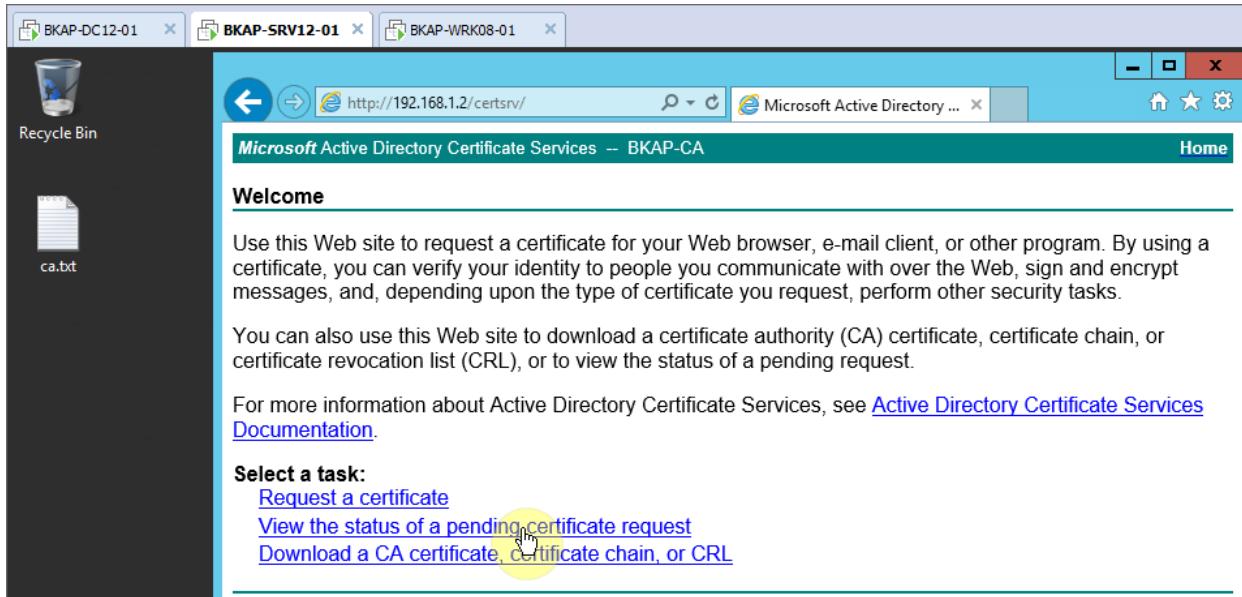
⇒ Click vào **Submit >**



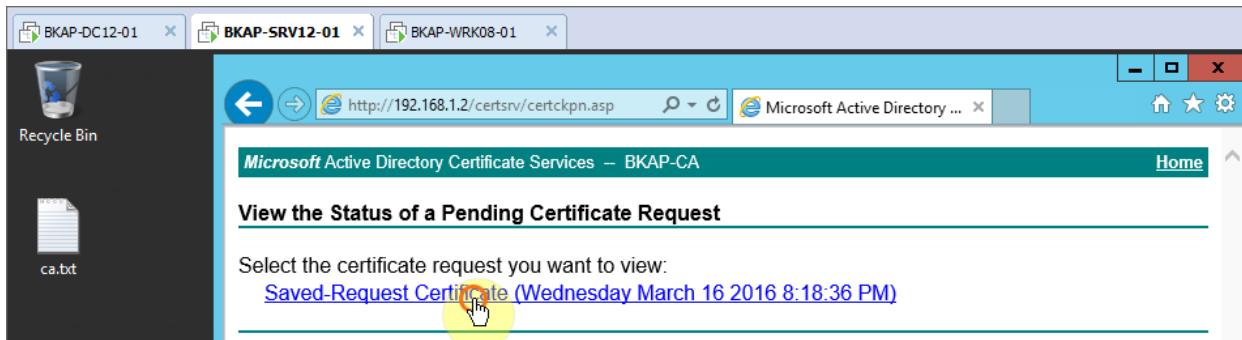
- Chuyển sang máy *BKAP-DC12-01* cấp phát chứng chỉ vừa được **Web Server** yêu cầu.
 - Vào dịch vụ **Certification Authority**, tại cửa sổ **certsrv ..** click chọn vào **Pending Requests**, click chuột phải vào chứng chỉ chọn **All Tasks / Issue**.



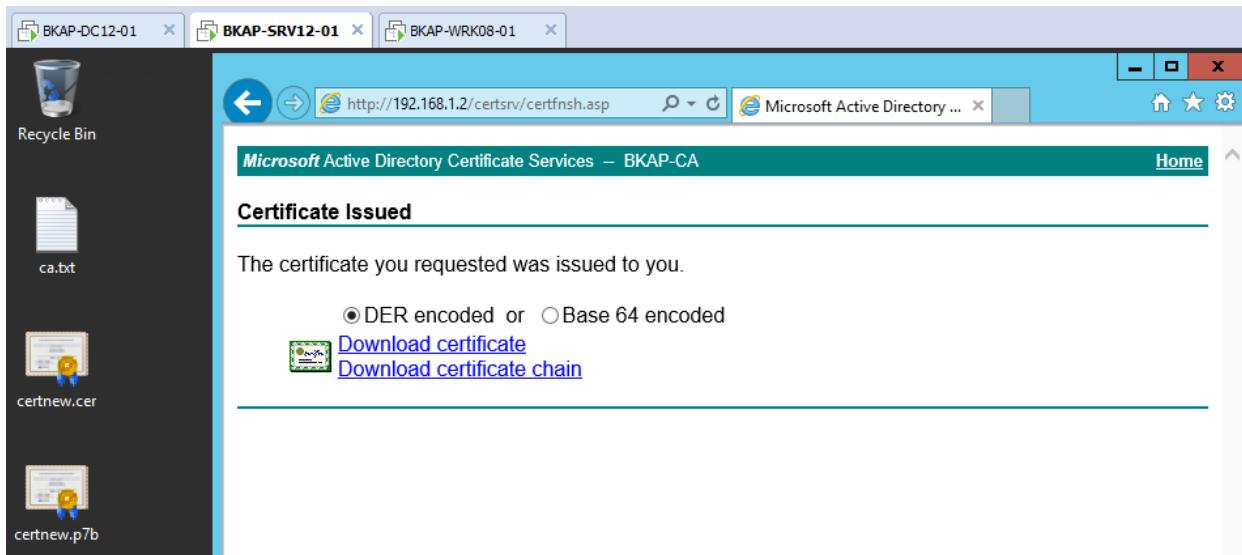
- Chuyển sang máy BKAP-SRV12-01, thực hiện *download* chứng chỉ về máy Web Server.
 - Vào IE, truy cập lại địa chỉ **192.168.1.2/certsrv**, click vào **View the status of a pending certificate request.**



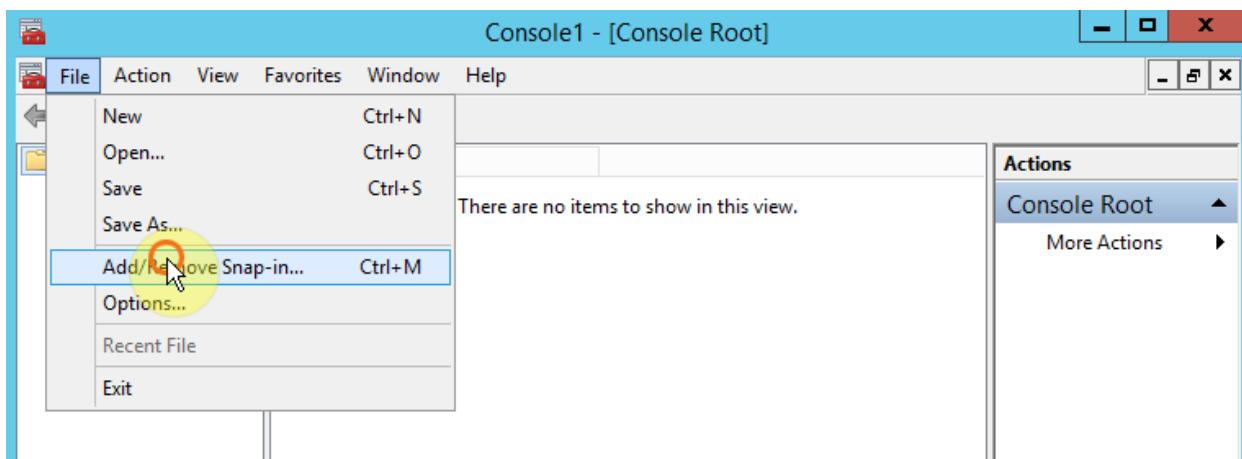
- Tại cửa sổ tiếp theo , click vào **Saved-Request Certificate...**



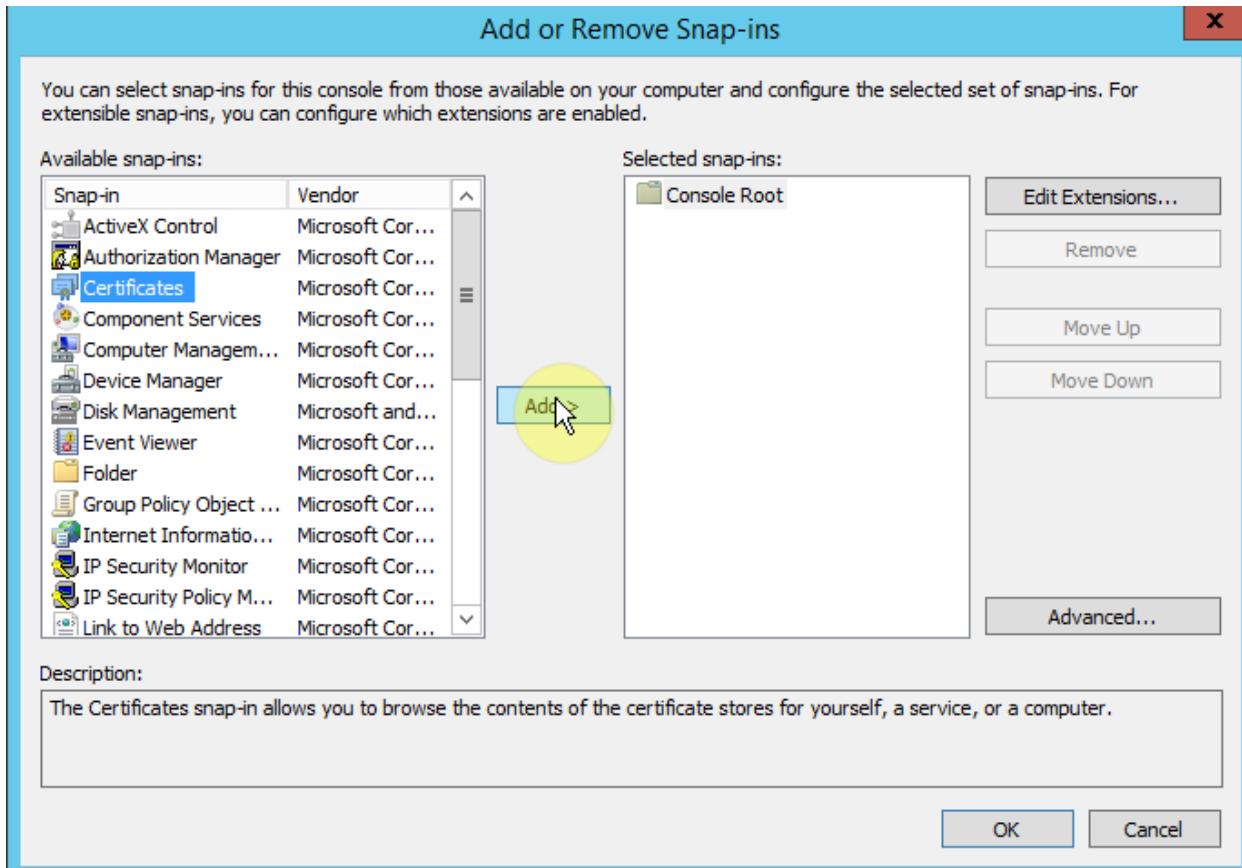
- Thực hiện *download* chứng chỉ về máy.



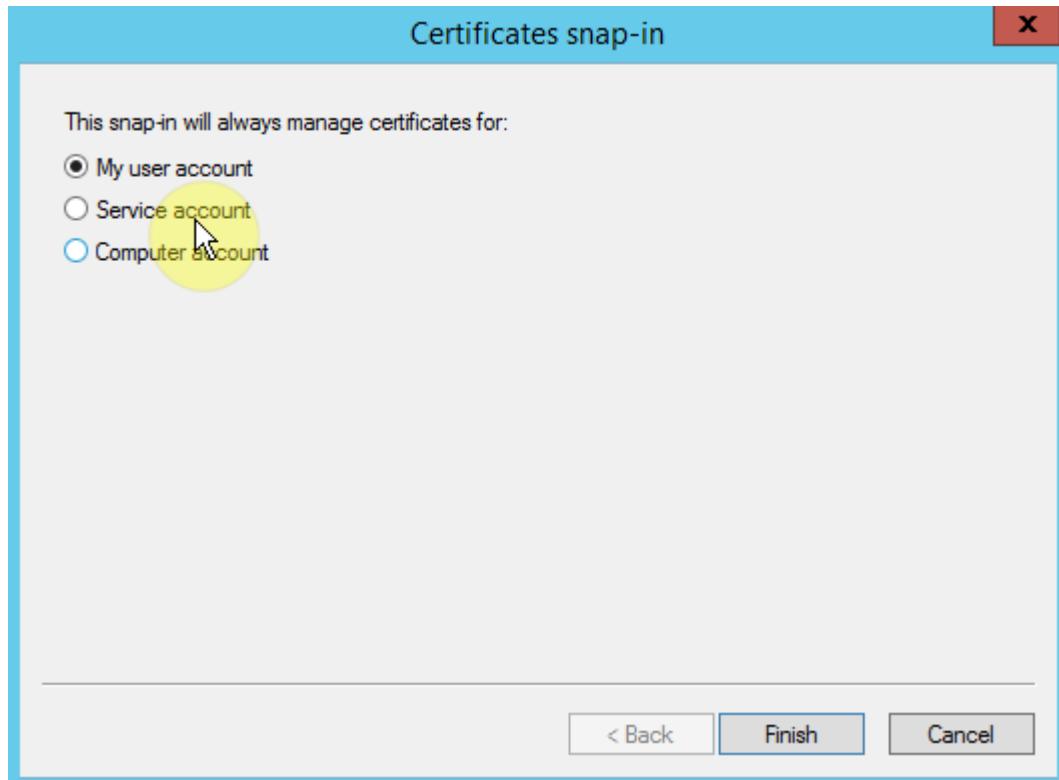
- Thực hiện **Trust CA** trên máy **Web Server**.
 - Run / mmc
 - Tại cửa sổ **Console 1...**, click vào **File / Add, Remove Snap-in...**



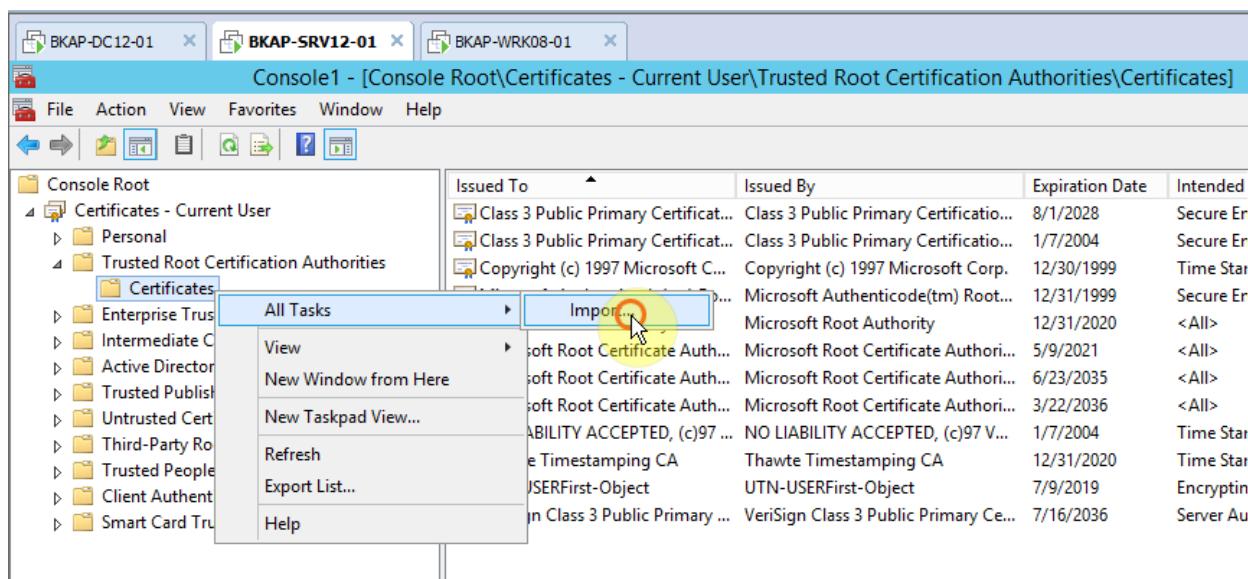
- Tại cửa sổ **Add or Remove Snap-ins**, click chọn vào **Certificates , Add >**



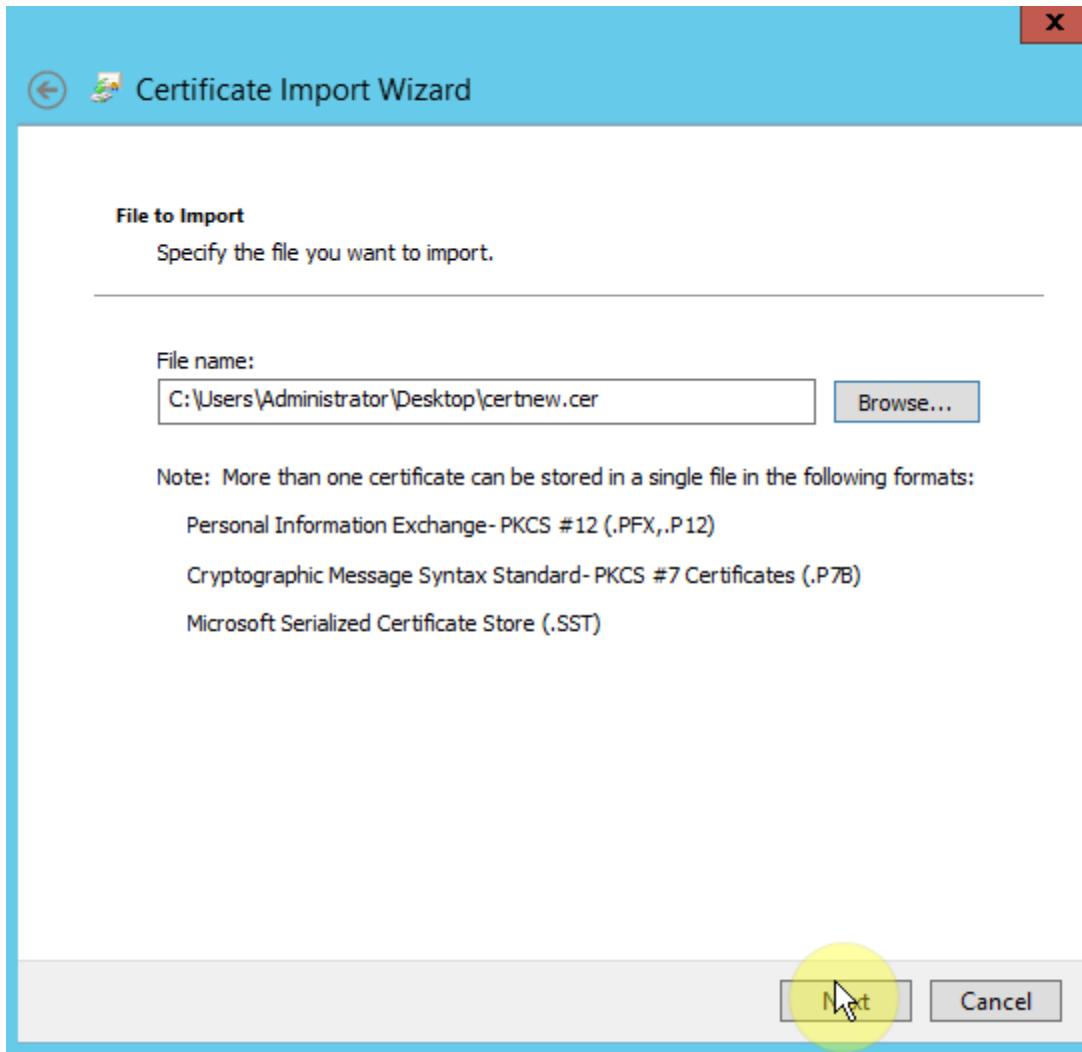
- Tại cửa sổ Certificates snap-in , chọn vào My user account => Finish.



- Tại cửa sổ Console 1...., click vào Trust Root Certification Authorities / Certificates , chọn All Tasks / Import...



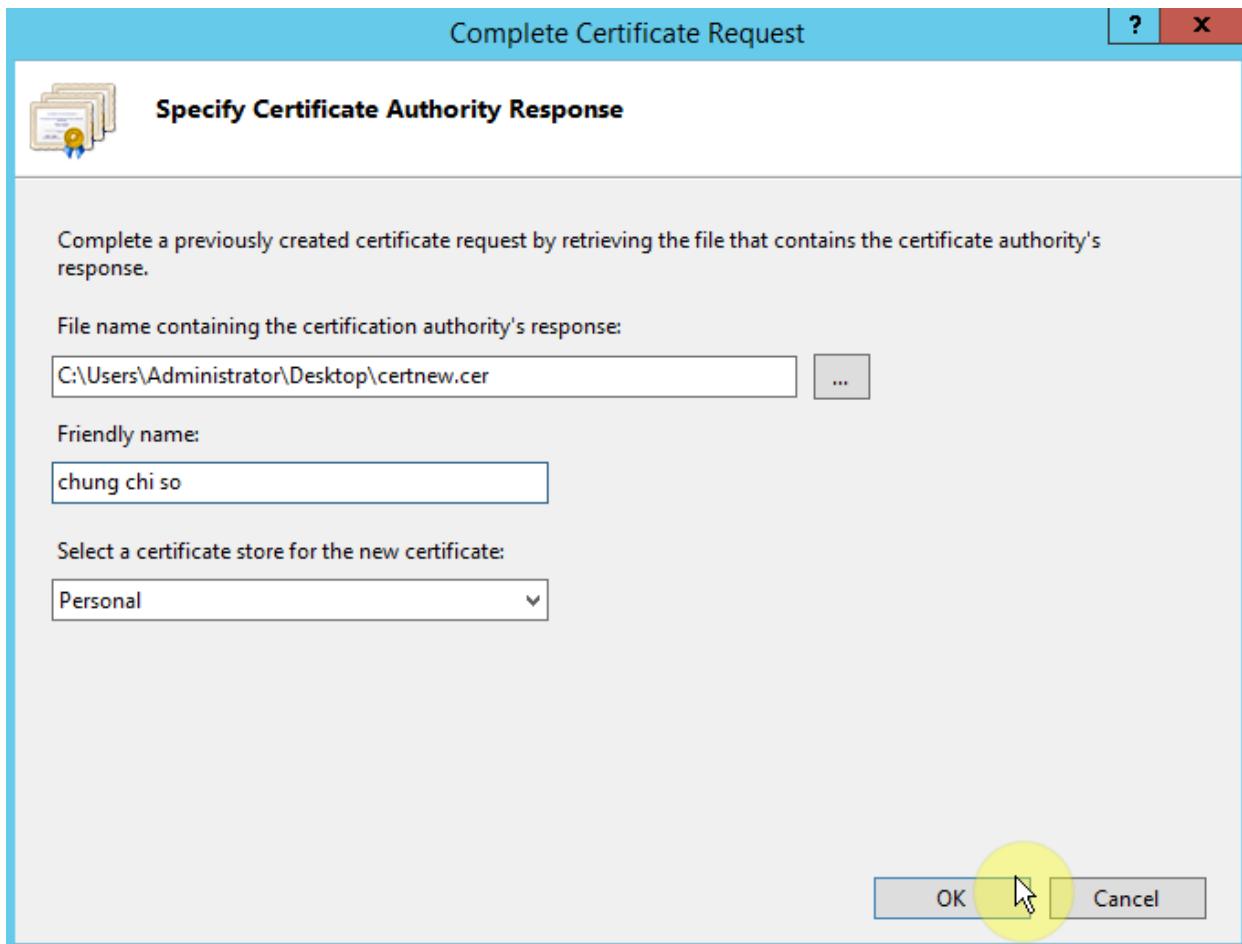
- Tại cửa sổ **File to Import**, browse đến file chứng chỉ vừa được download về máy.



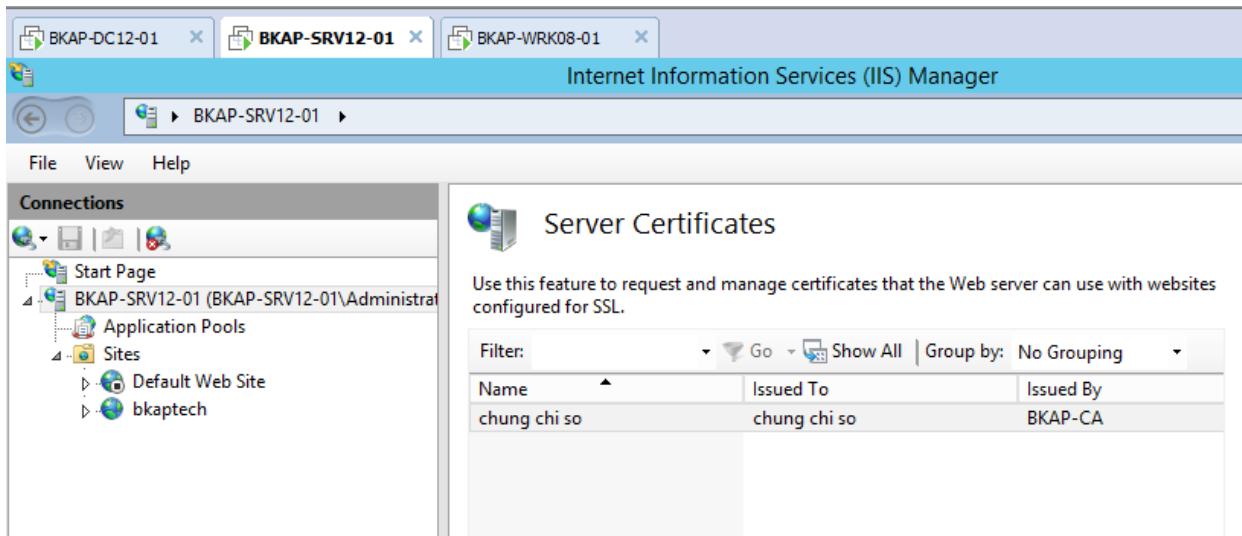
- Làm tương tự đối với file còn lại.

Issued To	Issued By	Expiration Date	Intended
BKAP-CA	BKAP-CA	3/16/2021	<All>
chung chi so	BKAP-CA	3/16/2017	Server Au
Class 3 Public Primary Certificat...	Class 3 Public Primary Certificatio...	8/1/2028	Secure Er
Class 3 Public Primary Certificat...	Class 3 Public Primary Certificatio...	1/7/2004	Secure Er
Copyright (c) 1997 Microsoft C...	Copyright (c) 1997 Microsoft Corp.	12/30/1999	Time Star
Microsoft Authenticode(tm) Root...	Microsoft Authenticode(tm) Root...	12/31/1999	Secure Er
Microsoft Root Authority	Microsoft Root Authority	12/31/2020	<All>
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	5/9/2021	<All>
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	6/23/2035	<All>
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	3/22/2036	<All>
NO LIABILITY ACCEPTED, (c)97 ...	NO LIABILITY ACCEPTED, (c)97 V...	1/7/2004	Time Star
Thawte Timestamping CA	Thawte Timestamping CA	12/31/2020	Time Star
UTN-USERFirst-Object	UTN-USERFirst-Object	7/9/2019	Encryptin
VeriSign Class 3 Public Primary ...	VeriSign Class 3 Public Primary Ce...	7/16/2036	Server Au

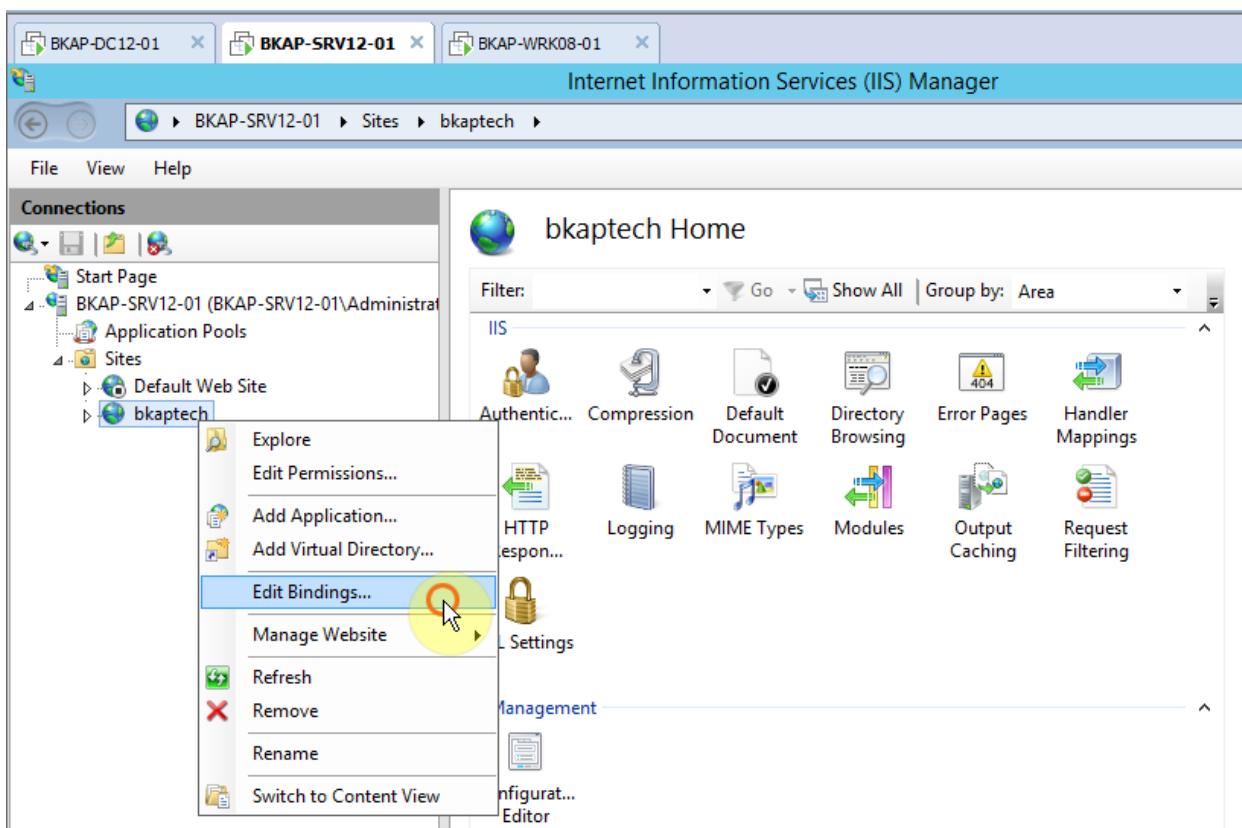
- Hoàn thành việc yêu cầu chứng chỉ:
 - Click vào **Complete Certificate Request** , tại cửa sổ này , thực hiện **Browse** đến file chứng chỉ. Tại mục **Friendly name** , nhập vào tên **chung chi so**.



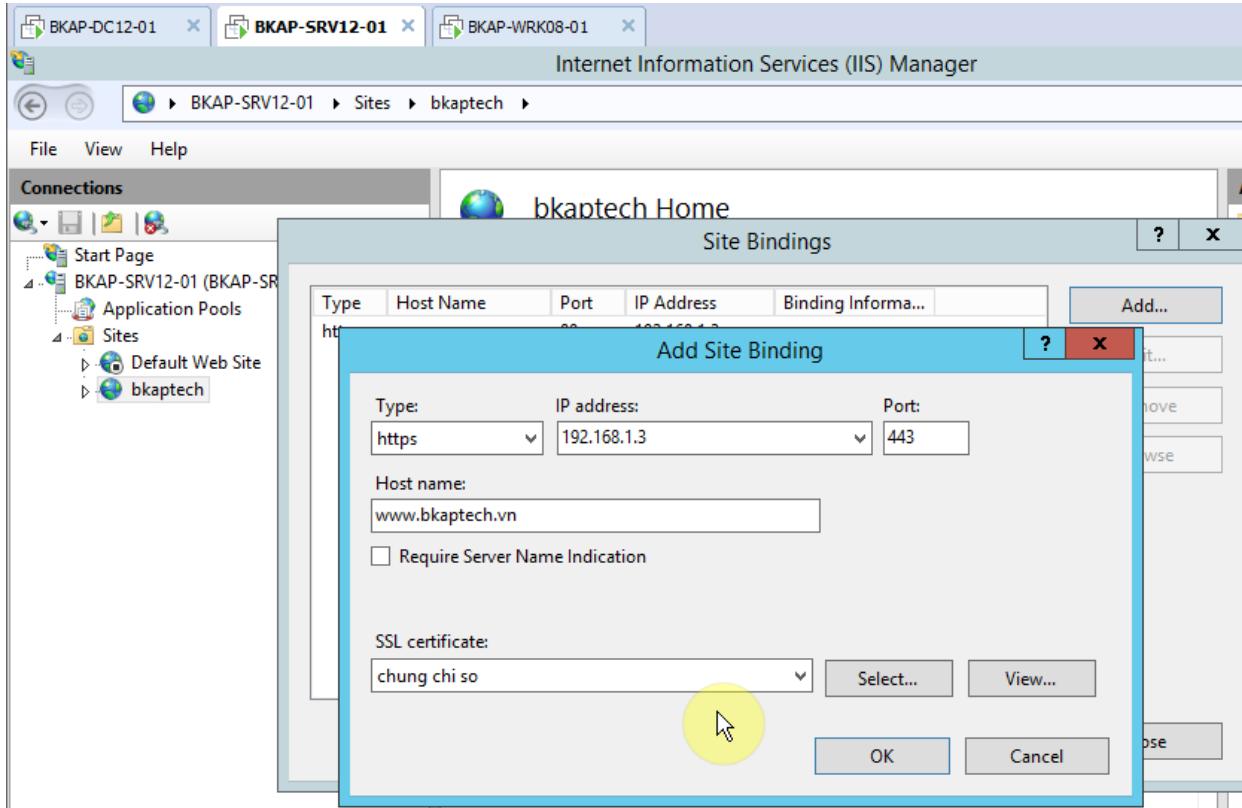
- Chứng chỉ đã được cấp cho Web Server.

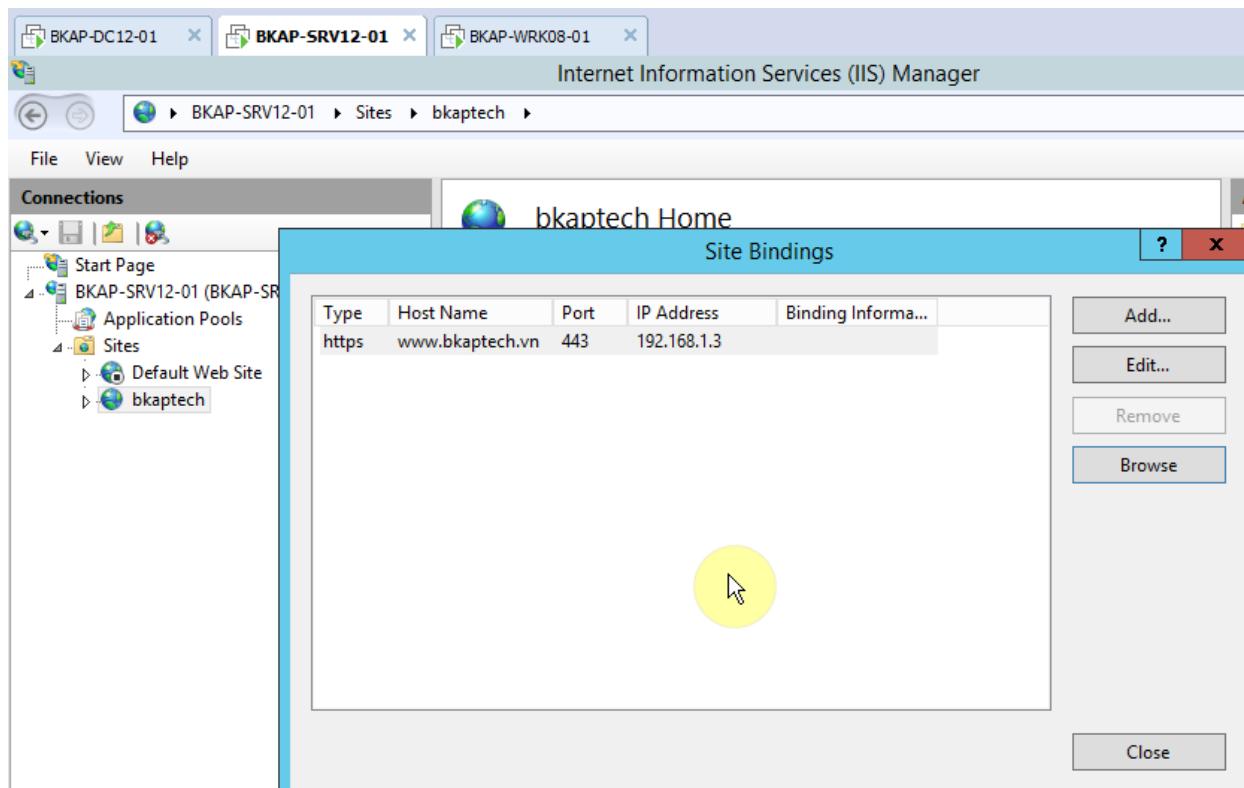


- Cấu hình Website sử dụng SSL , click chuột phải vào Hosting **bkaptech** , chọn **Edit Bindings...**

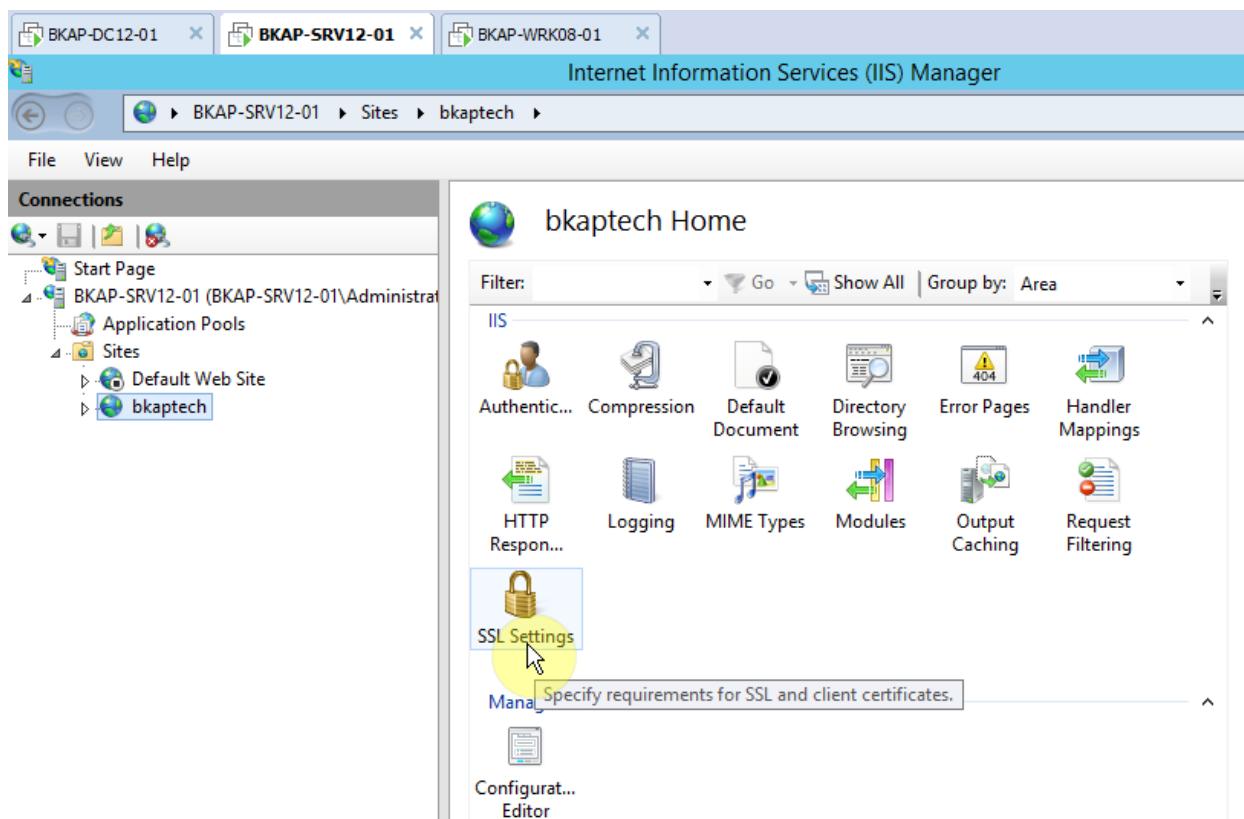


- Tại cửa sổ **Site Bindings**, thực hiện add thêm giao thức **https**, xóa giao thức **http**.

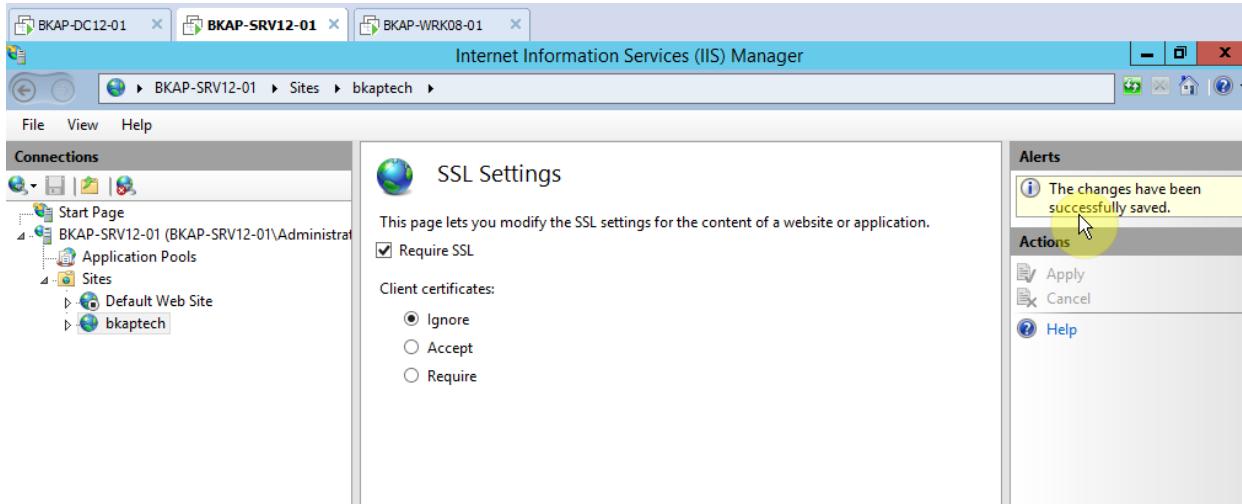




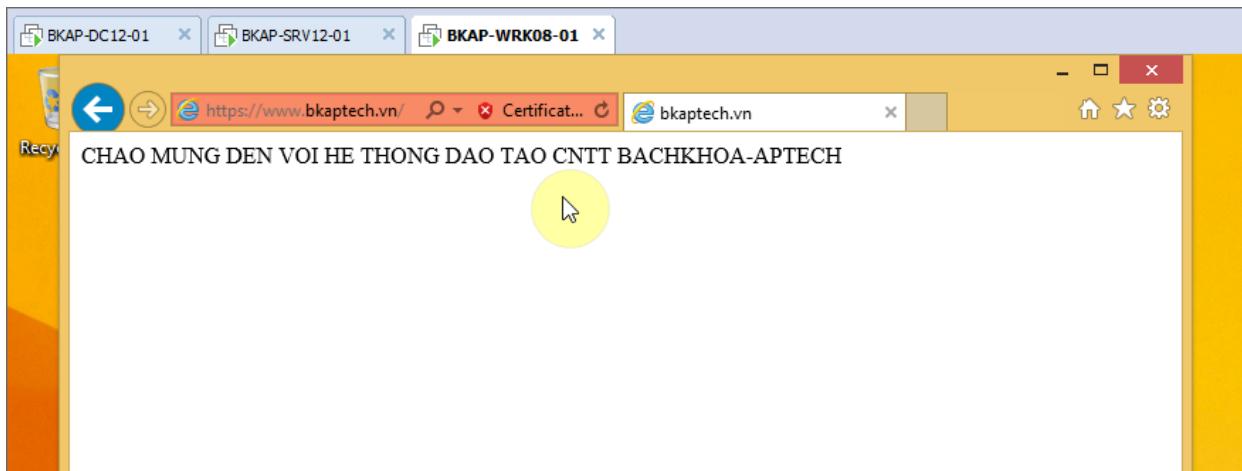
- Tại cửa sổ **bkaptech Home**, chọn vào **SSL Settings**.



- Tại cửa sổ **SSL Settings**, click chọn vào **Require SSL => Apply**.



- Chuyển sang máy **BKAP-WRK08-01**, kiểm tra truy cập Website bằng giao thức *https*.



Bài 3:**TRIỂN KHAI DỊCH VỤ ACTIVE DIRECTORY (TIẾP)**

Các nội dung chính sẽ được đề cập:

- ✓ Triển khai cài đặt và cấu hình RODC.
- ✓ Cấu hình AD DS snapshots.
- ✓ Khôi phục tài khoản người dùng bằng Active Directory Recycle Bin.

3.1 Triển khai cài đặt và cấu hình RODC.**1. Yêu cầu bài Lab:**

+ Cấu hình hệ thống sao cho Server *BKAP-SRV12-01* được triển khai thành **Read-Only Domain Controller**.

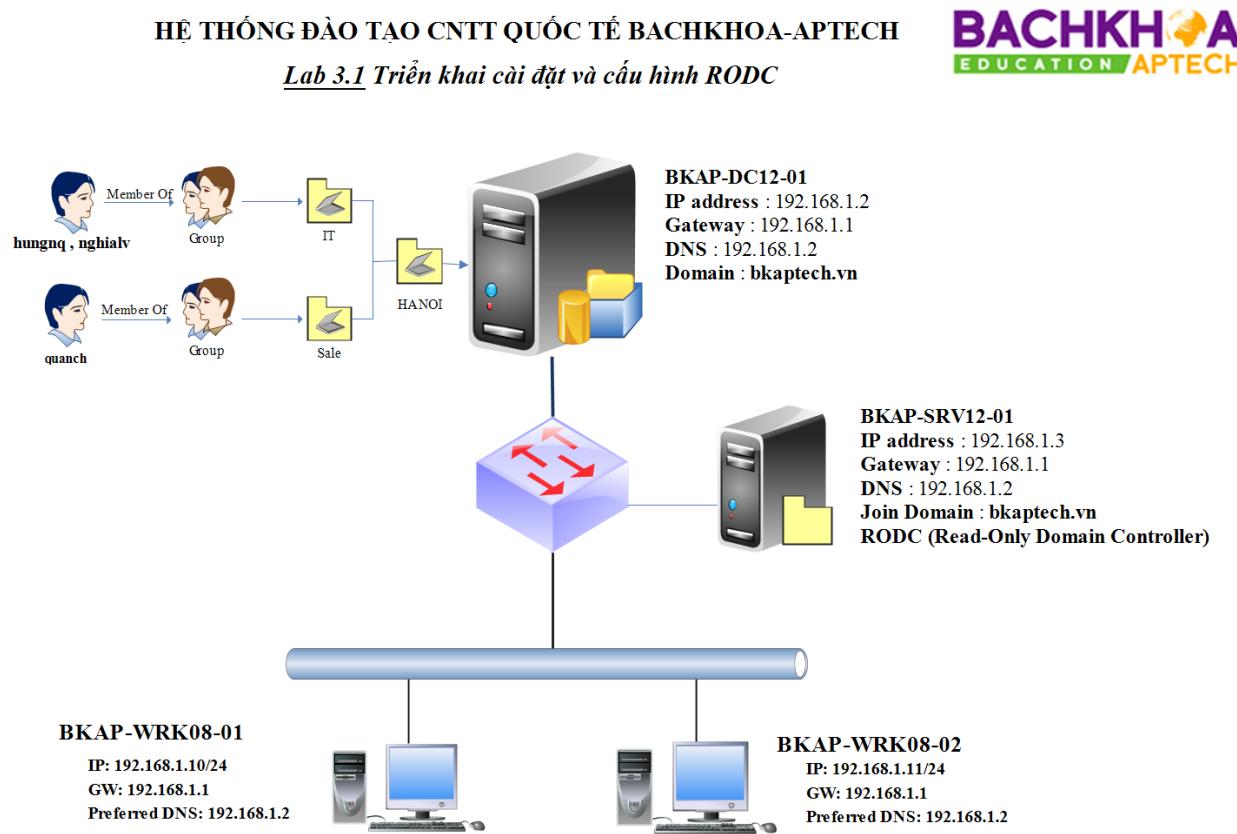
- Nâng cấp máy *BKAP-DC12-01* thành **Domain Controller** quản lý miền **bkaptech.vn**.
- Tạo các *User, Group, OU*.
- Nâng cấp Server *BKAP-SRV12-01* thành **RODC** thuộc miền **bkaptech.vn**.
- Trao quyền cài đặt và quản trị trên **RODC** cho tài khoản **hungnq**.
- Cấu hình **Password Replication Policy** cho phòng ban IT.
- Sau khi cấu hình **RODC**, tắt card mạng của DC chính và kiểm tra từ máy người dùng *BKAP-WR08-01*.

2. Yêu cầu chuẩn bị:

+ Chuẩn bị 2 máy *Server* và 1 máy *Client*:

- Máy *BKAP-DC12-01* làm **Domain Controller** quản lý miền **bkaptech.vn**.
- Máy *BKAP-SRV12-01* Join vào Domain , cấu hình **RODC**.
- Máy Client *BKAP-WRK08-01* dùng để kiểm tra.

3. Mô hình Lab:



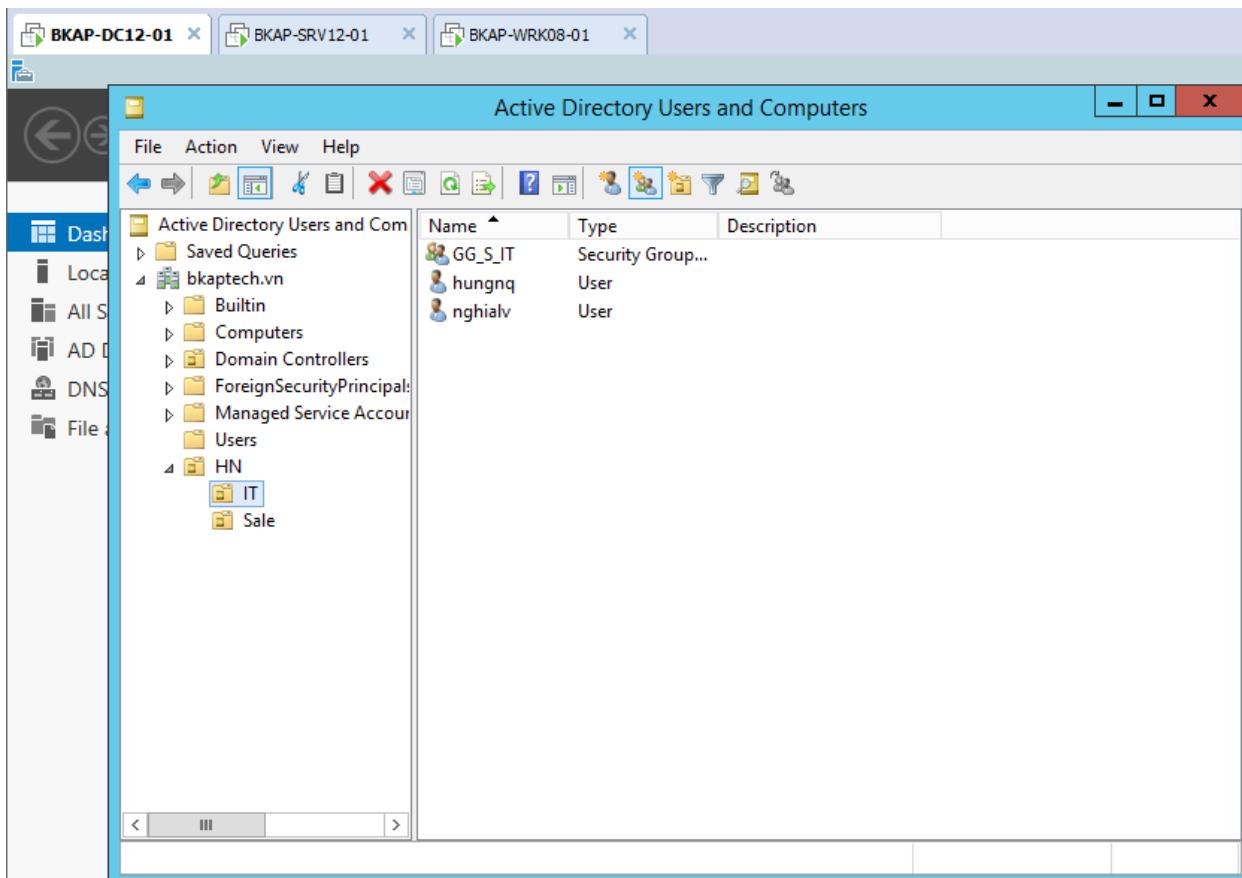
Hình 3.1

Sơ đồ địa chỉ như sau:

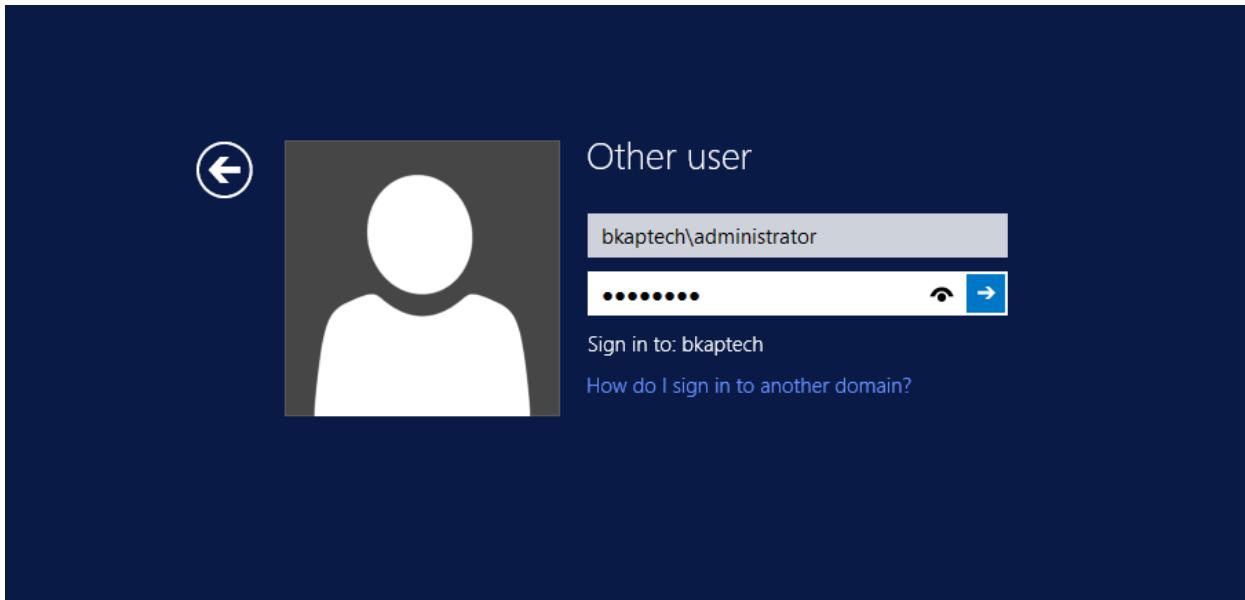
Thông số	BKAP-DC12-01	BKAP-SRV12-01	BKAP-WRK08-01
<i>IP address</i>	192.168.1.2	192.168.1.3	192.168.1.10
<i>Gateway</i>	192.168.1.1	192.168.1.1	192.168.1.1
<i>Subnet Mask</i>	255.255.255.0	255.255.255.0	255.255.255.0
<i>DNS Server</i>	192.168.1.2	192.168.1.2	192.168.1.2

Hướng dẫn chi tiết:

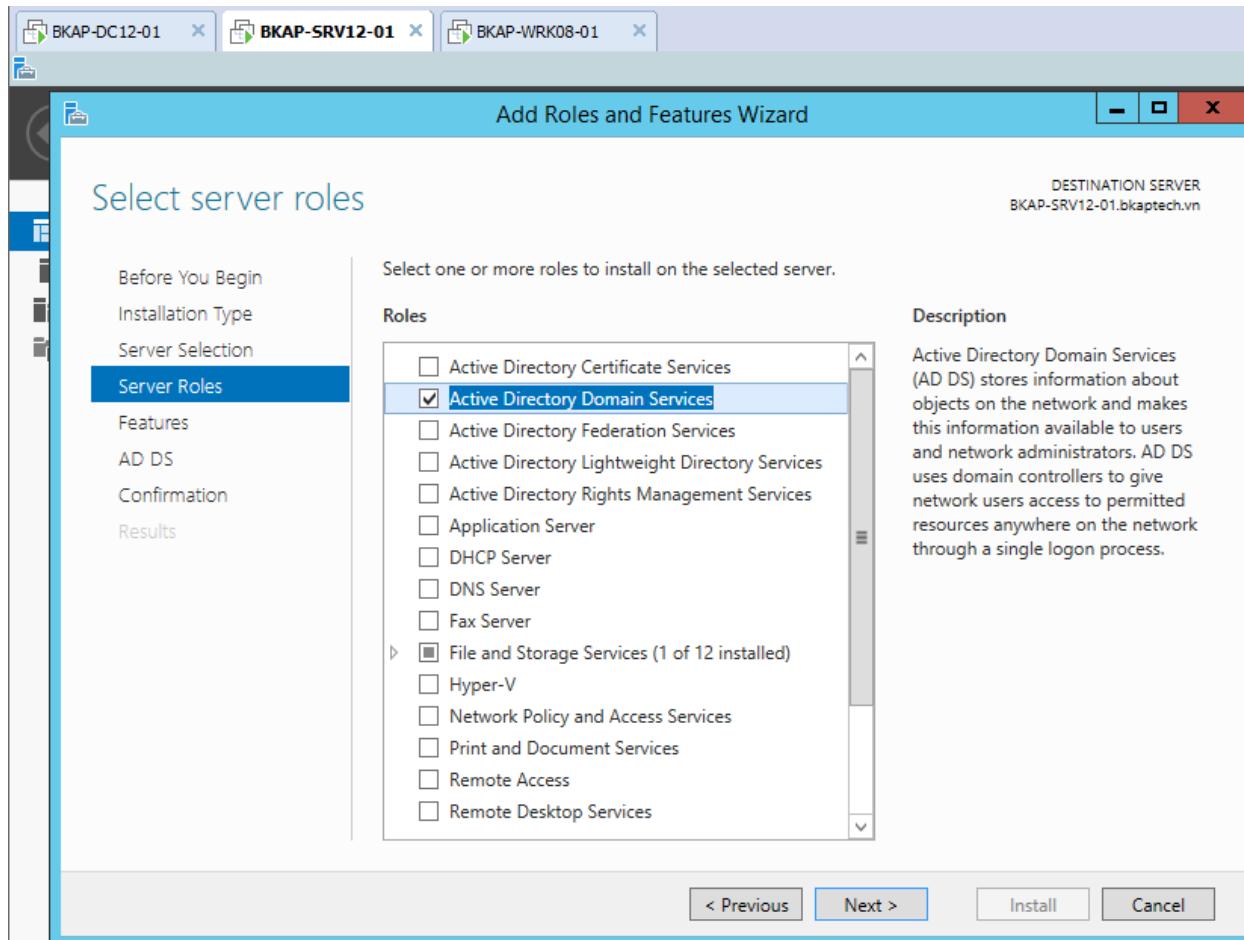
- Trên máy *BKAP-DC12-01*, tạo *OU, Group , User* như hình trên.



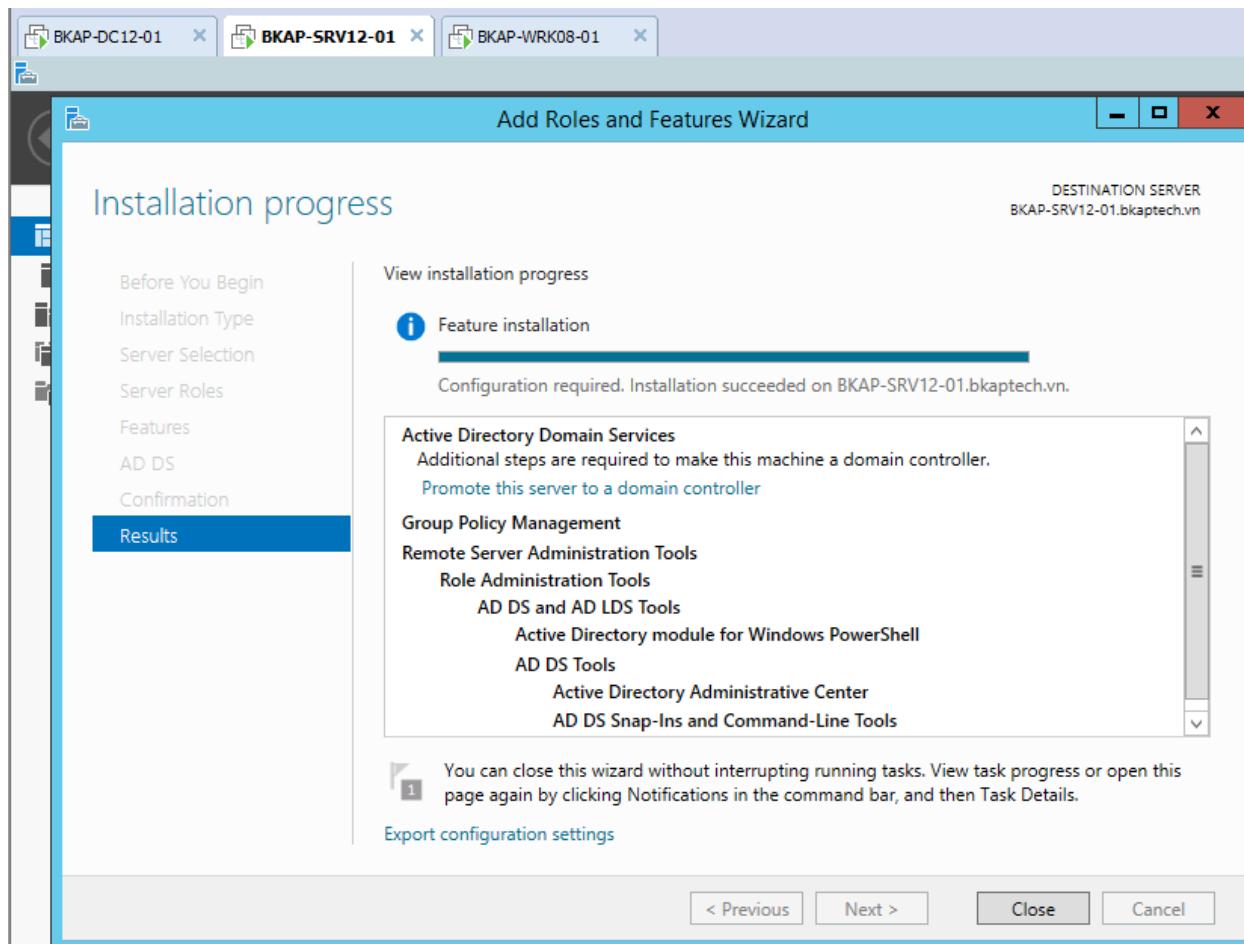
- Join máy *Client* vào Domain.
- Trên máy *BKAP-SRV12-01* , thực hiện Join vào Domain , đăng nhập bằng tài khoản **bkaptech\administrator**.



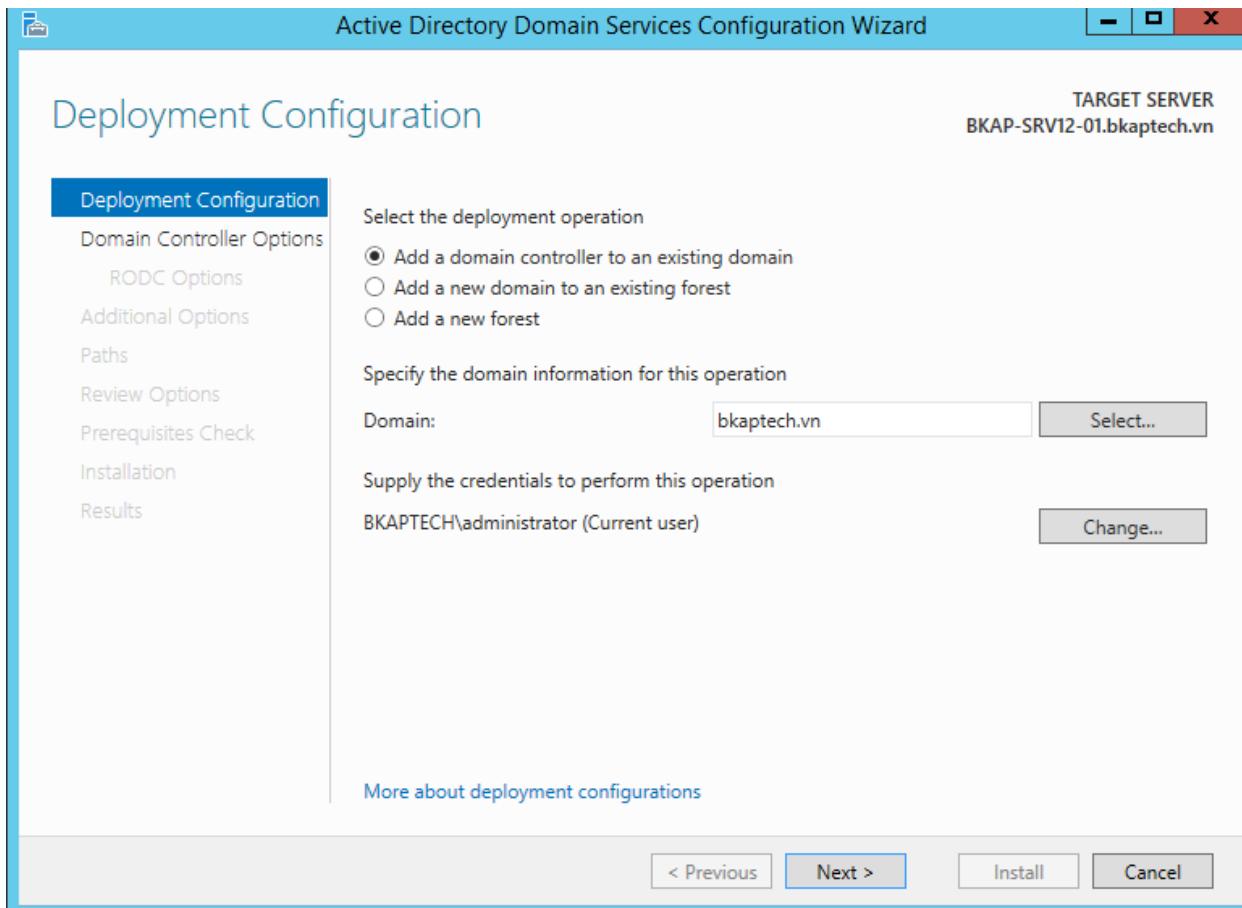
- Cài đặt dịch vụ *Active Directory Domain Services*.



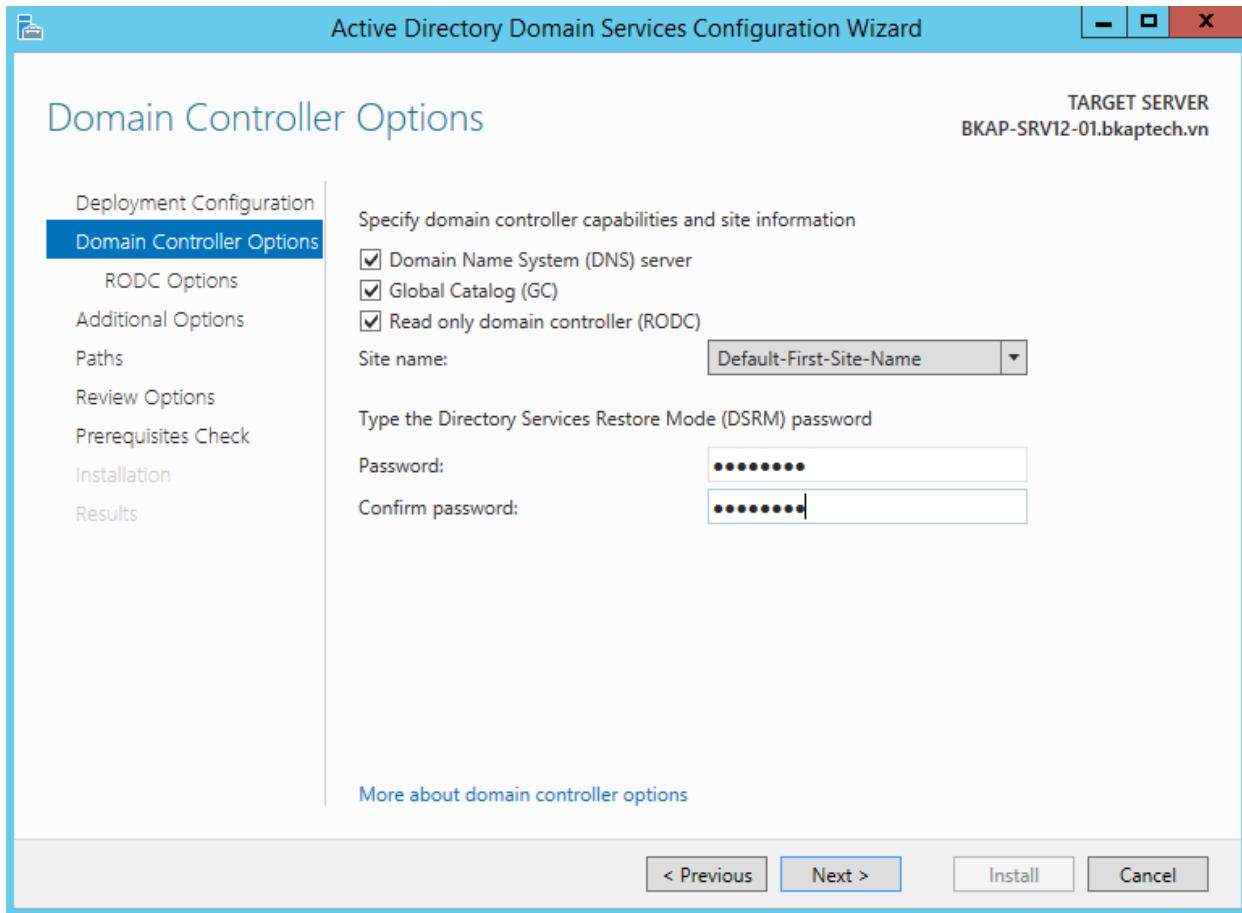
- Click vào Promote this server to a domain controller.



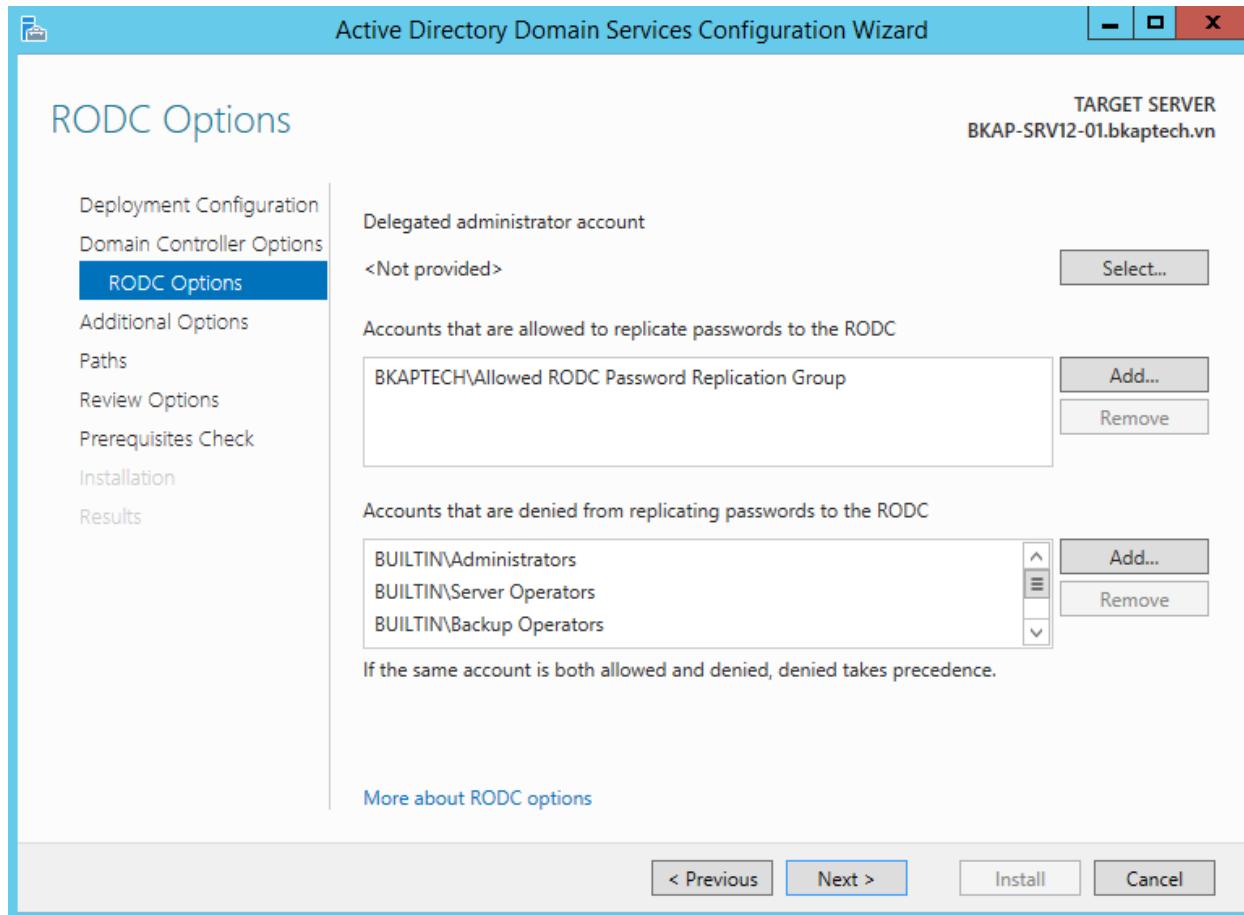
- Tại cửa sổ **Deployment Configuration**, click chọn vào **Add a domain controller to an existing domain**.



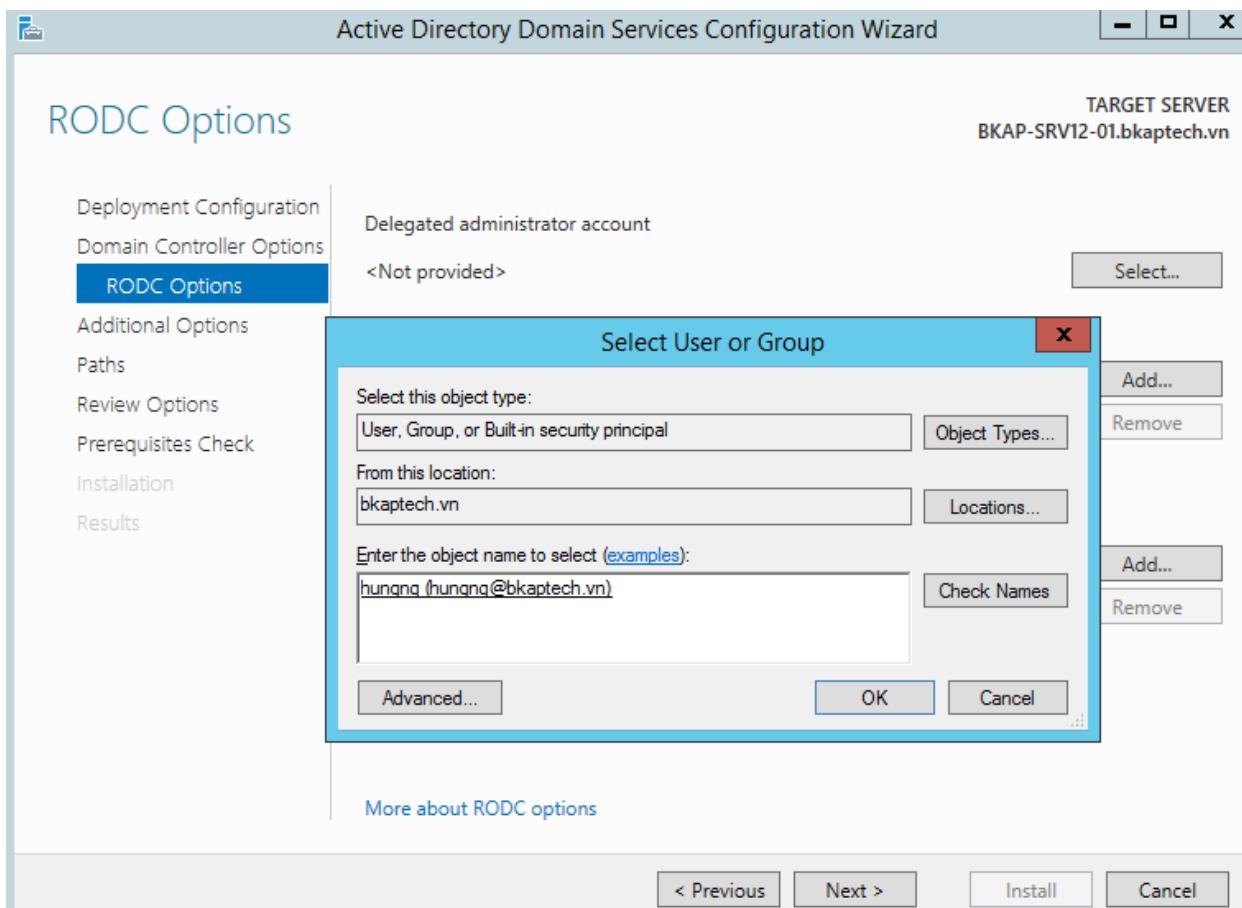
- Tại cửa sổ **Domain Controller Options**, click chọn vào **Read only domain controller (RODC)** và đặt mật khẩu **DSRM**.



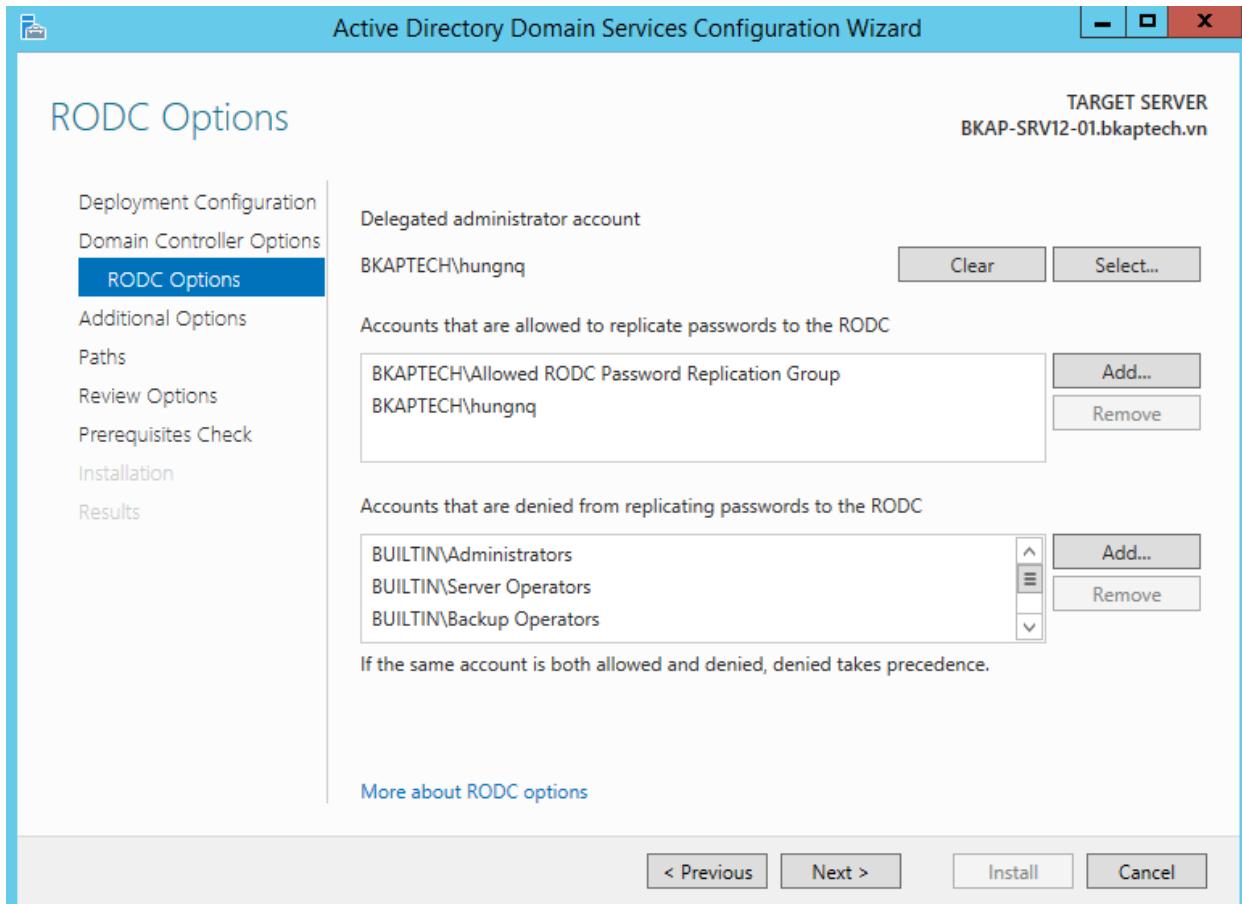
- Tại cửa sổ **RODC Options** , tại mục **Delegated administrator account** , click chọn vào **Select...**



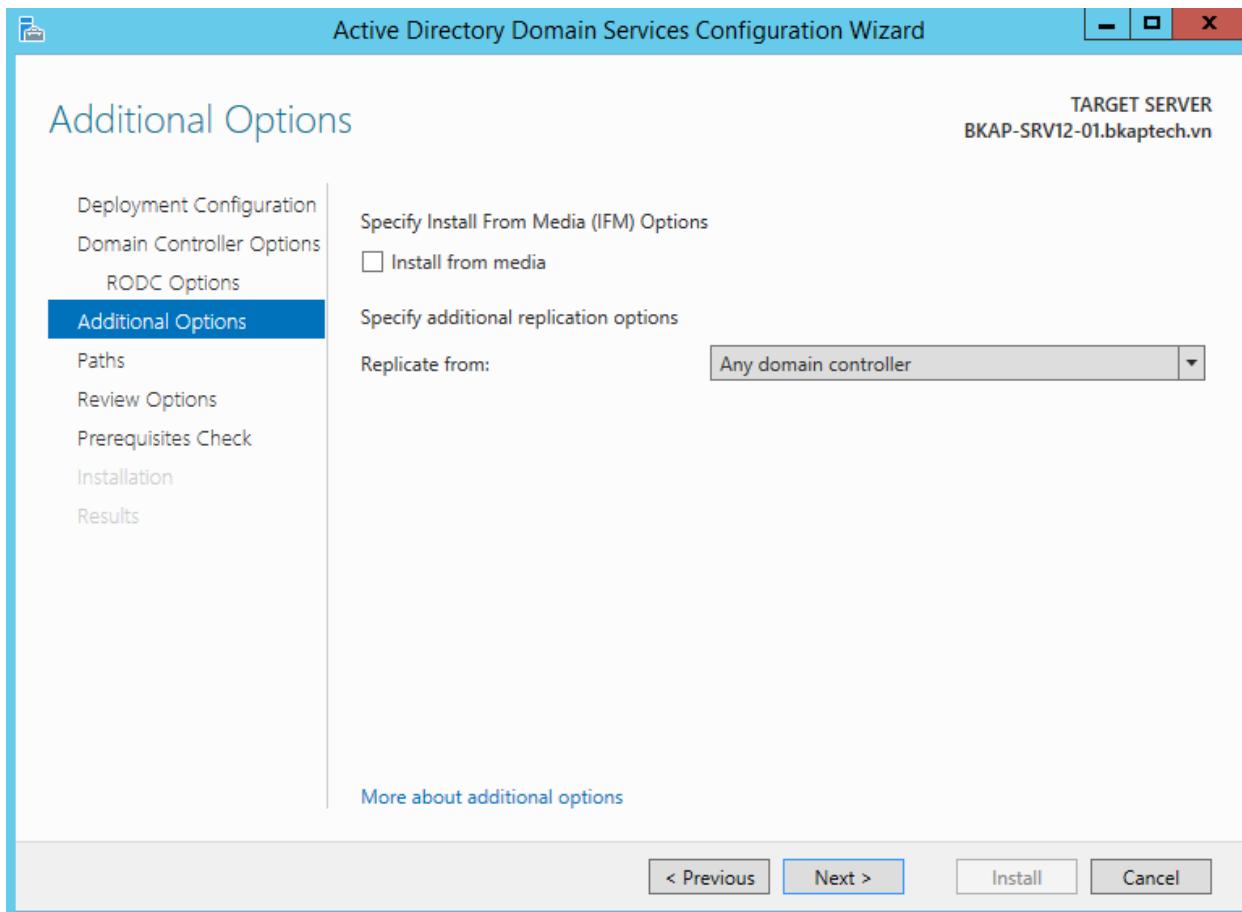
- Add vào tài khoản **hungnq**.



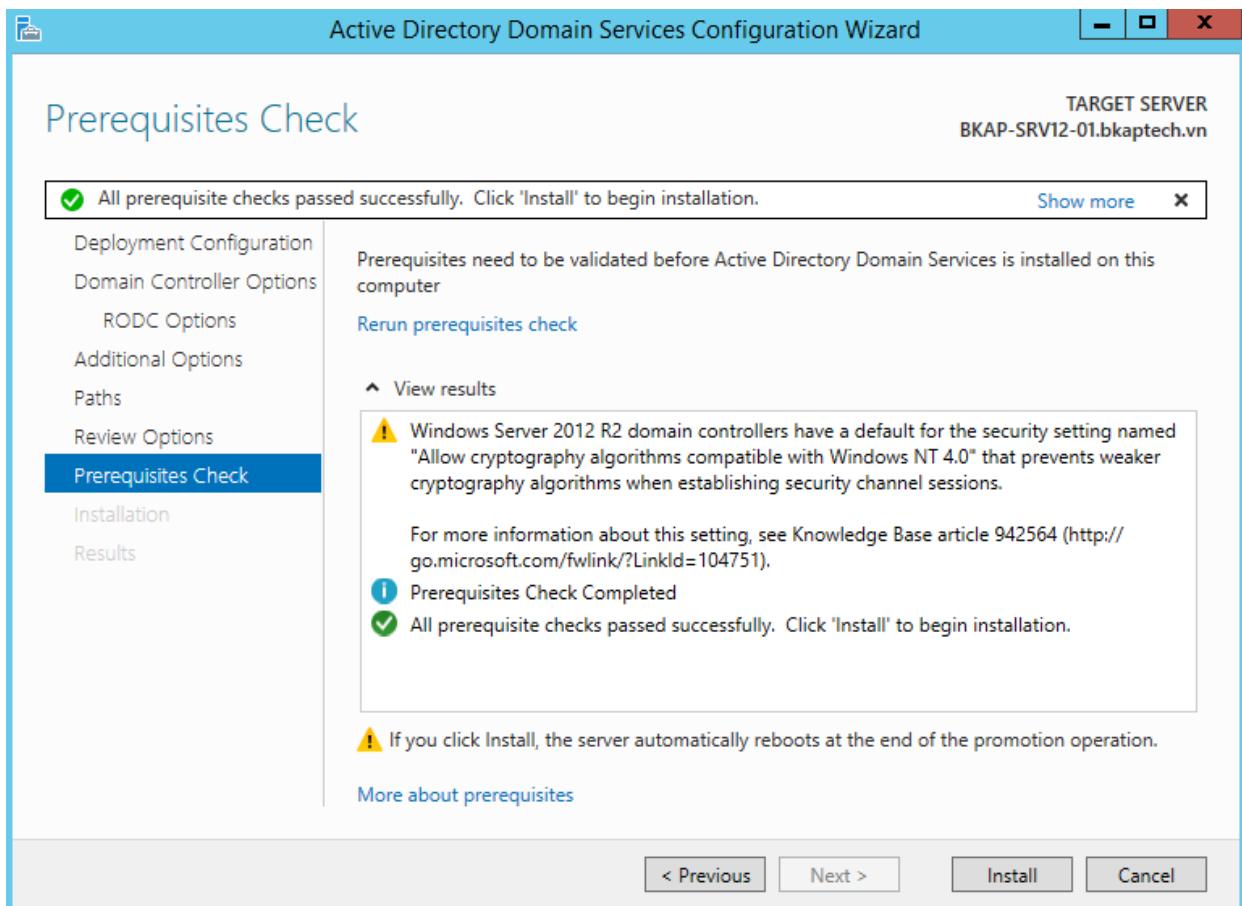
- Click vào **Add** tại mục **Accounts that are allowed to replicate passwords to the RODC**, add tài khoản **hungnq**.



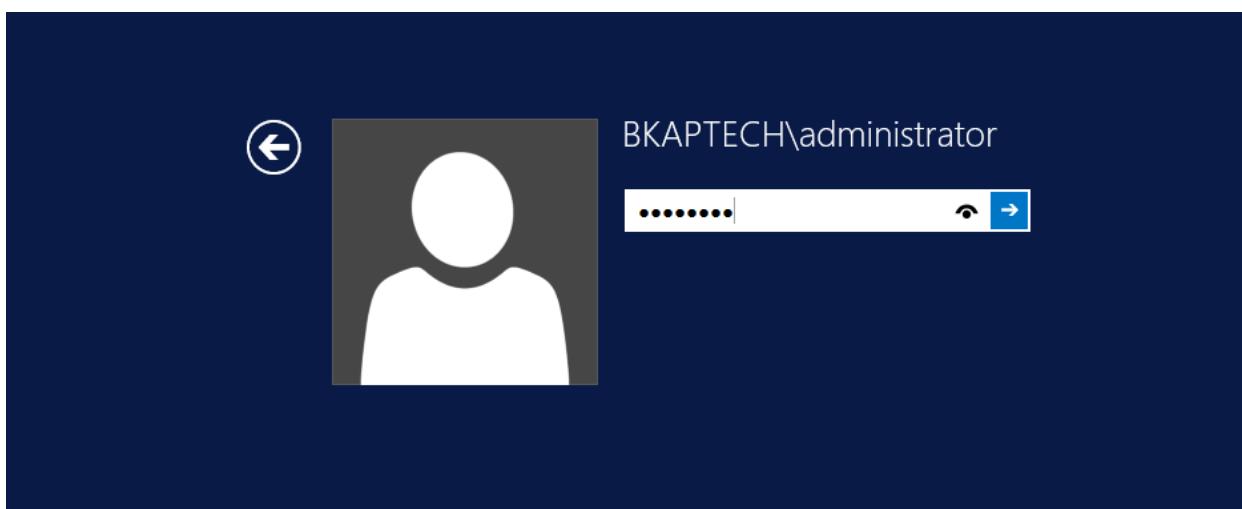
- Tại cửa sổ **Additional Options** , click vào **Next**.



- Click vào **Install**.



- Máy chủ tự động reset, đăng nhập lại bằng tài khoản **bkaptech\administrator**.

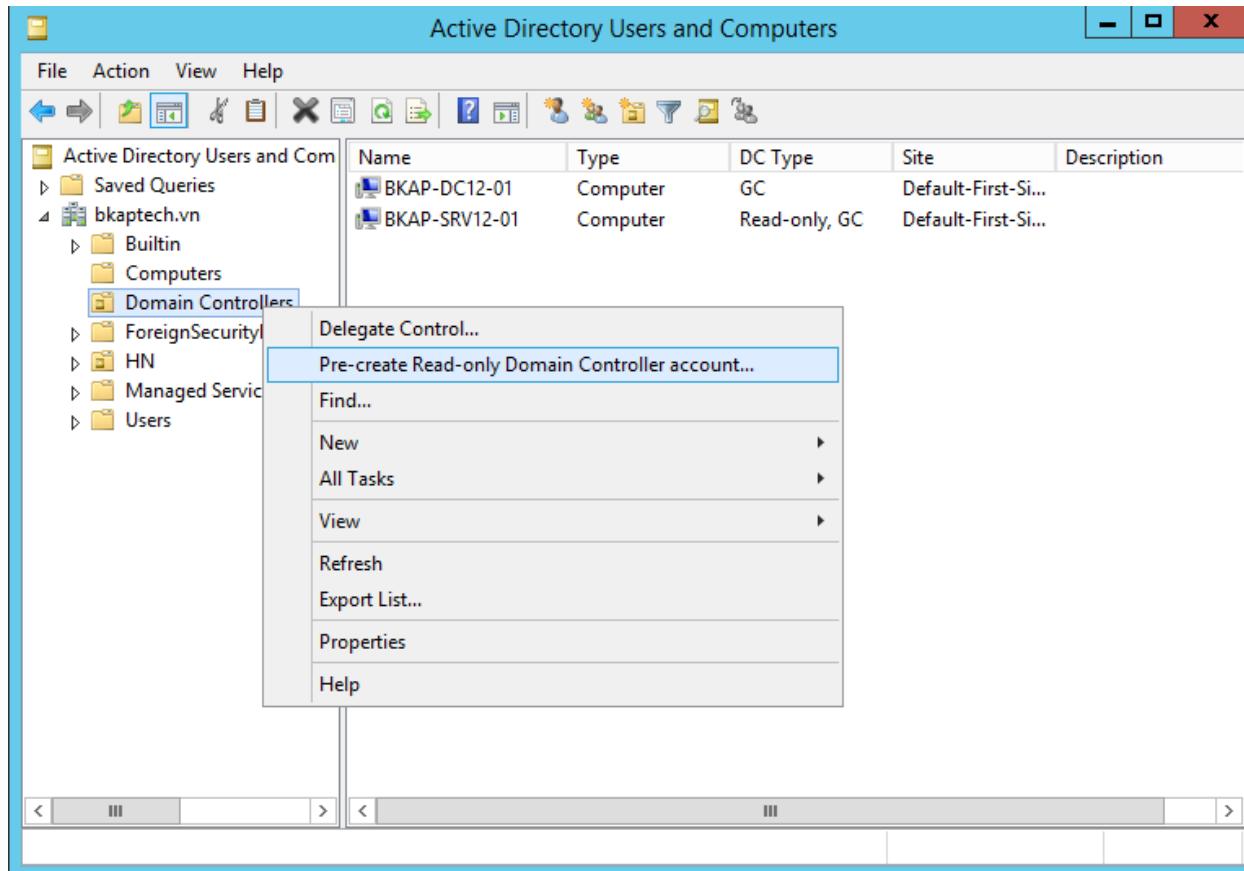


- Vào lại dịch vụ Active Directory User and Computer.

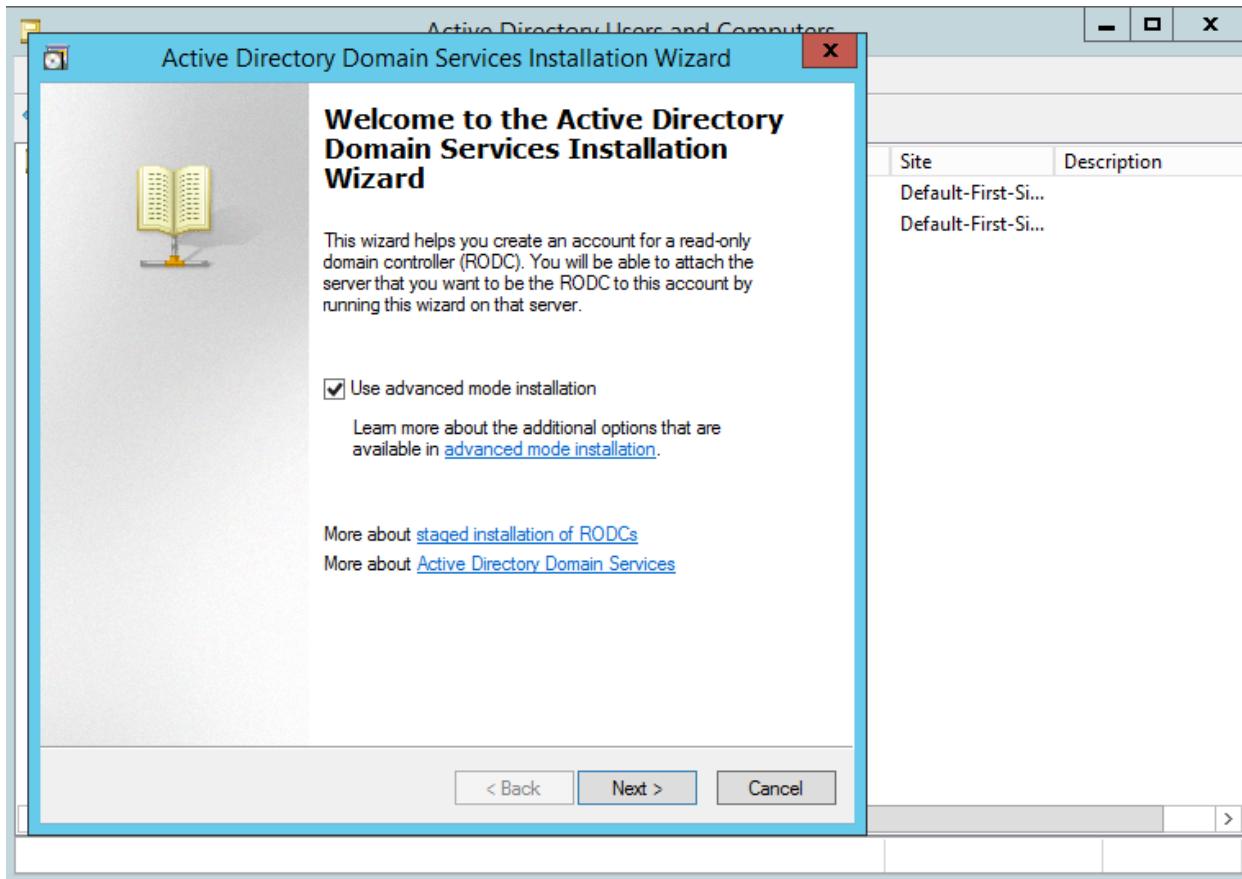
The screenshot shows the Windows Active Directory Users and Computers management console. On the left is a navigation pane displaying the domain structure under 'bkaptech.vn'. On the right is a table listing various objects in the domain, categorized by type (Container or Organizational...).

Name	Type	Description
Builtin	builtinDomain	
Computers	Container	Default container for up...
Domain Con...	Organizational...	Default container for do...
ForeignSecu...	Container	Default container for sec...
HN	Organizational...	
Managed Se...	Container	Default container for ma...
Users	Container	Default container for up...

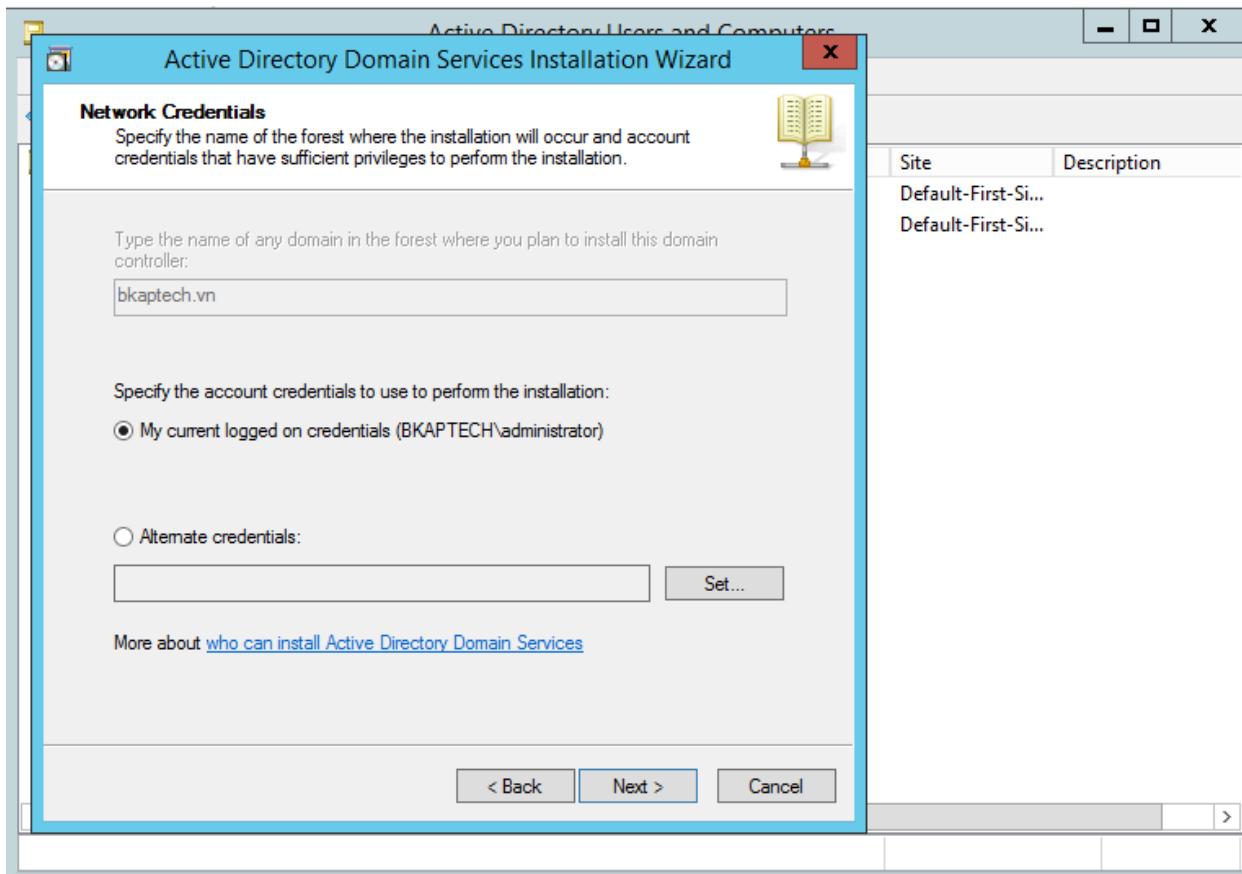
- Tại mục **Domain Controllers**, click chuột phải tại đây chọn **Pre-create RODC account...**



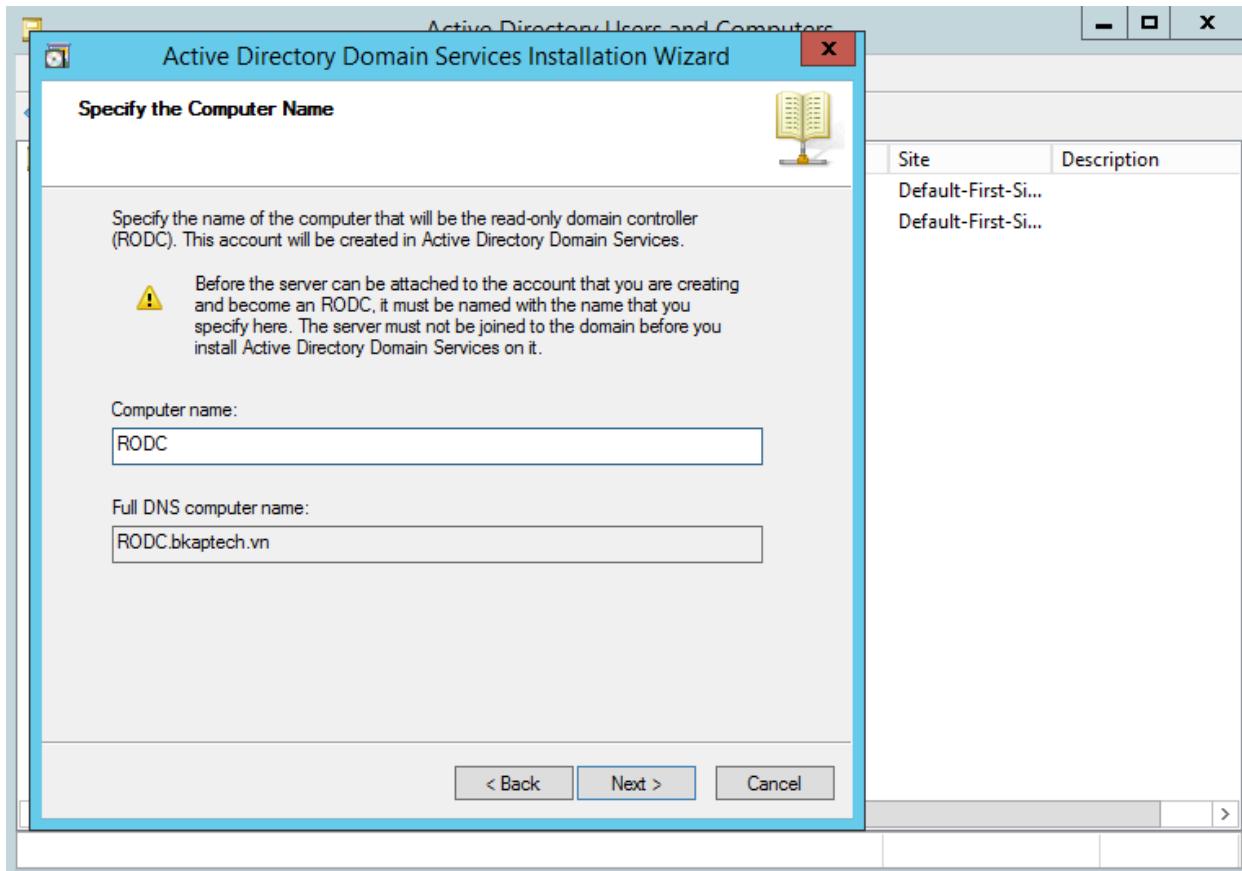
- Tại cửa sổ **Welcome to the Active Directory....**, click chọn vào **Use advanced mode installation**.



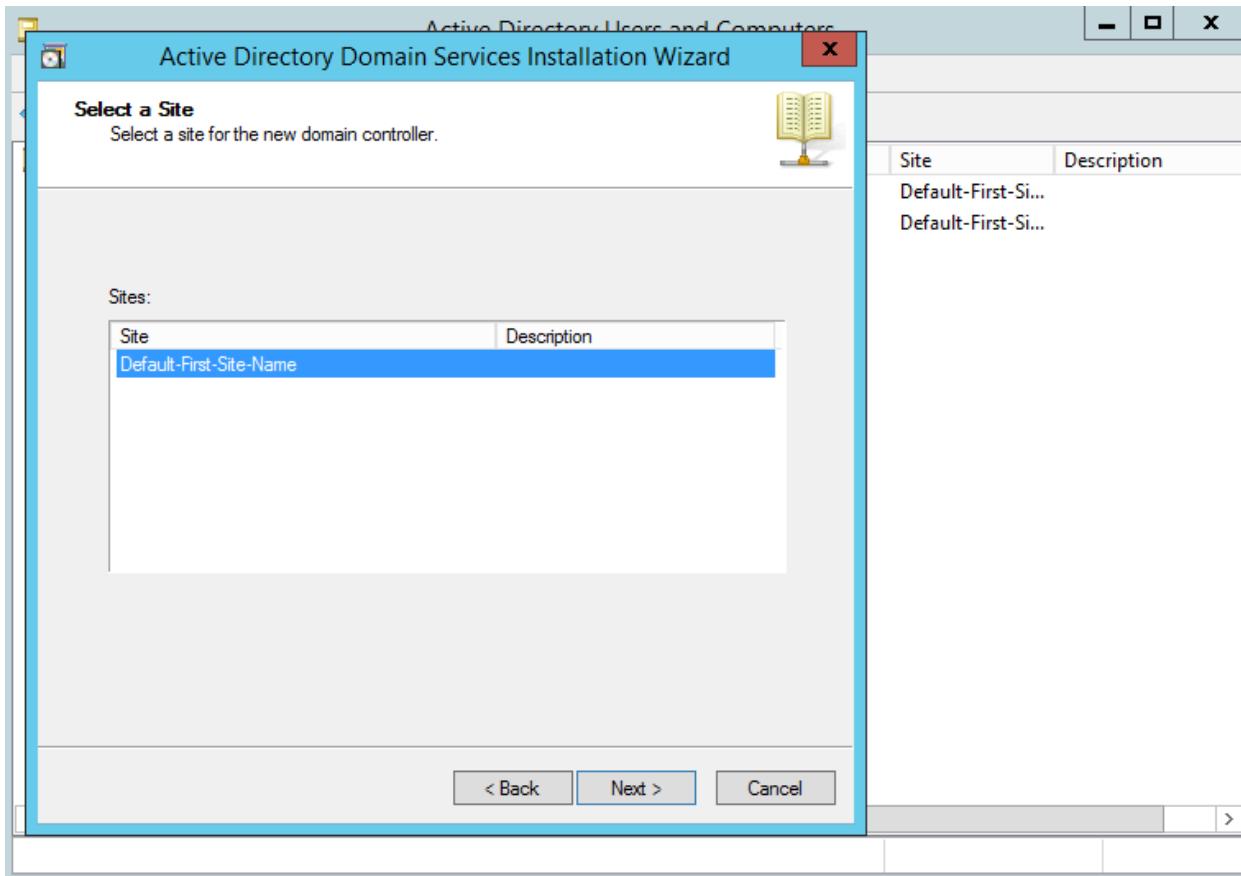
- Tại cửa sổ **Network Credentials**, click vào **Next**.



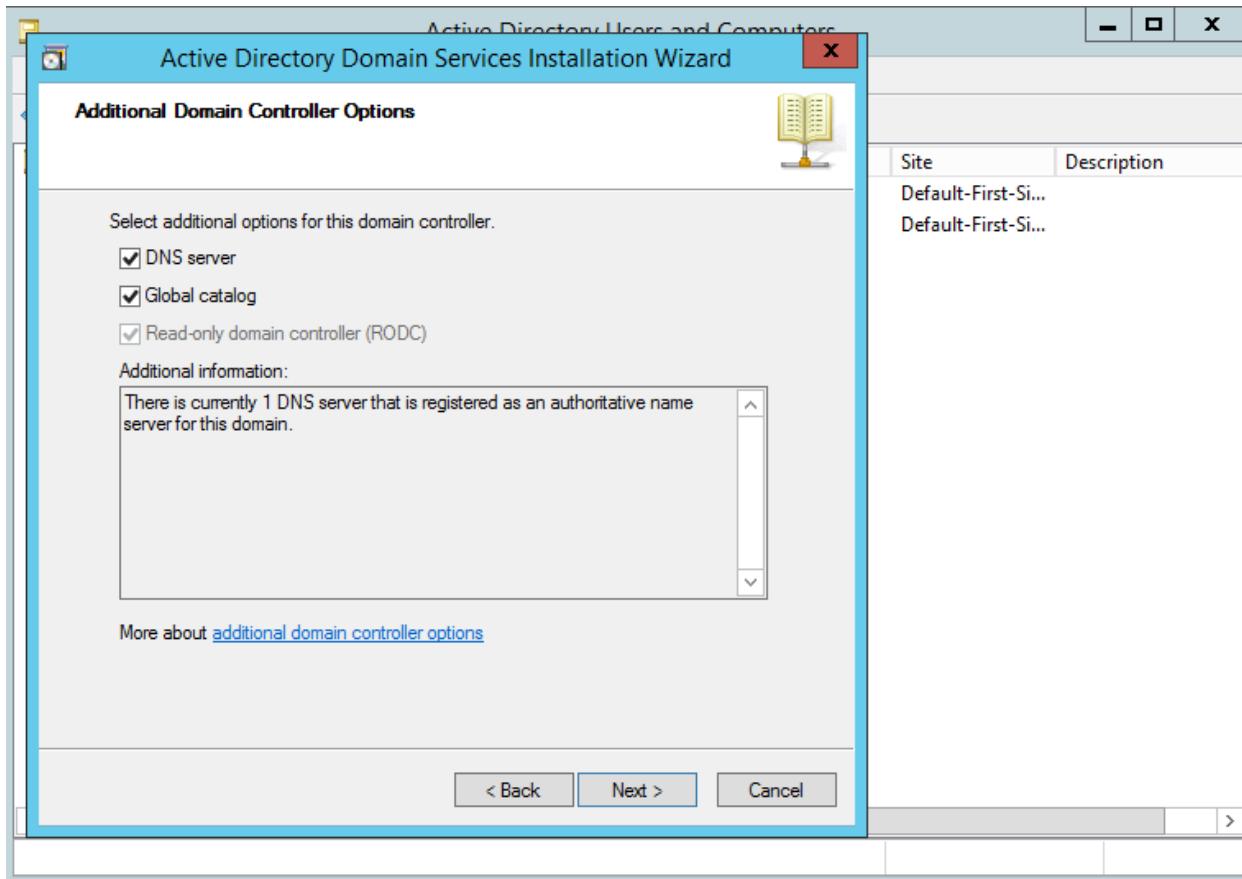
- Tại cửa sổ **Specify the Computer Name**, nhập vào tại mục **Computer name :RODC**.



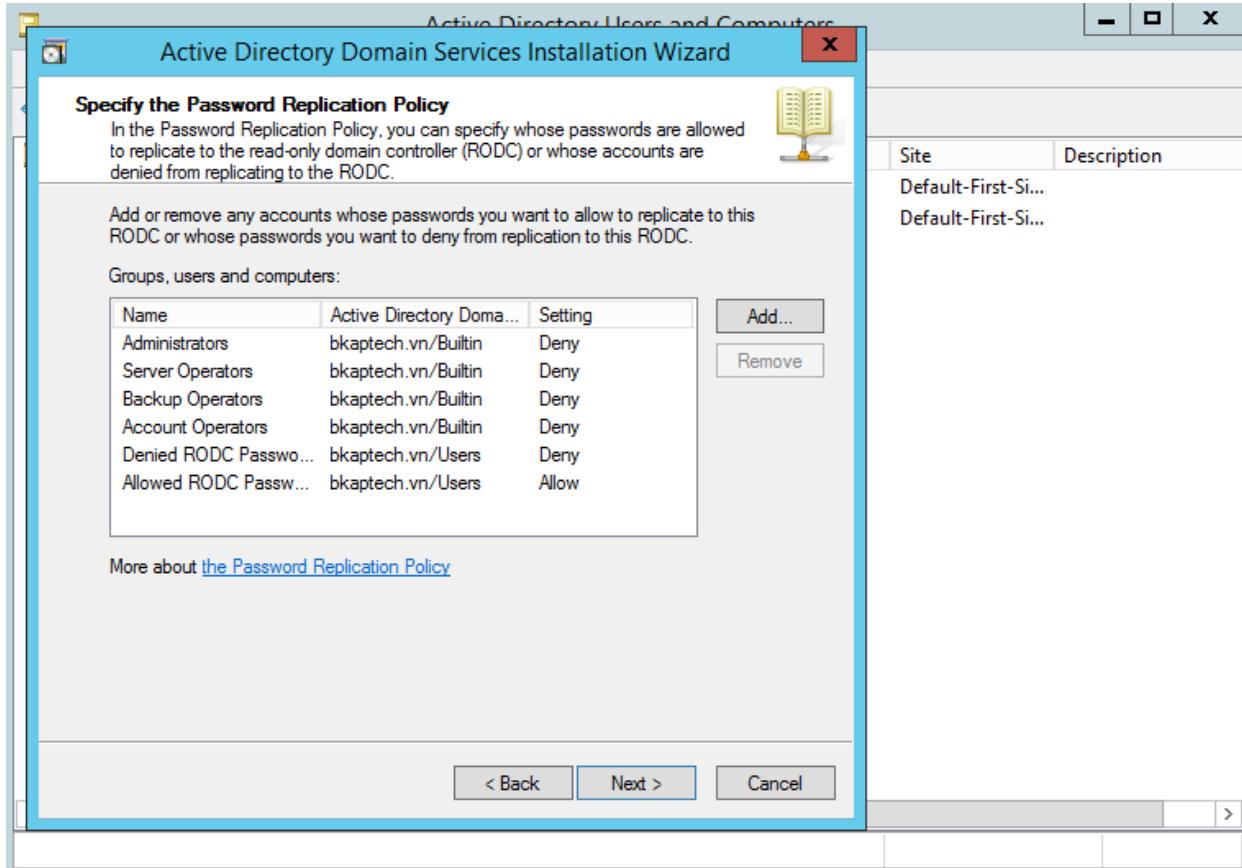
- Hiện ra cửa sổ **Select a Site**, click vào **Next**.



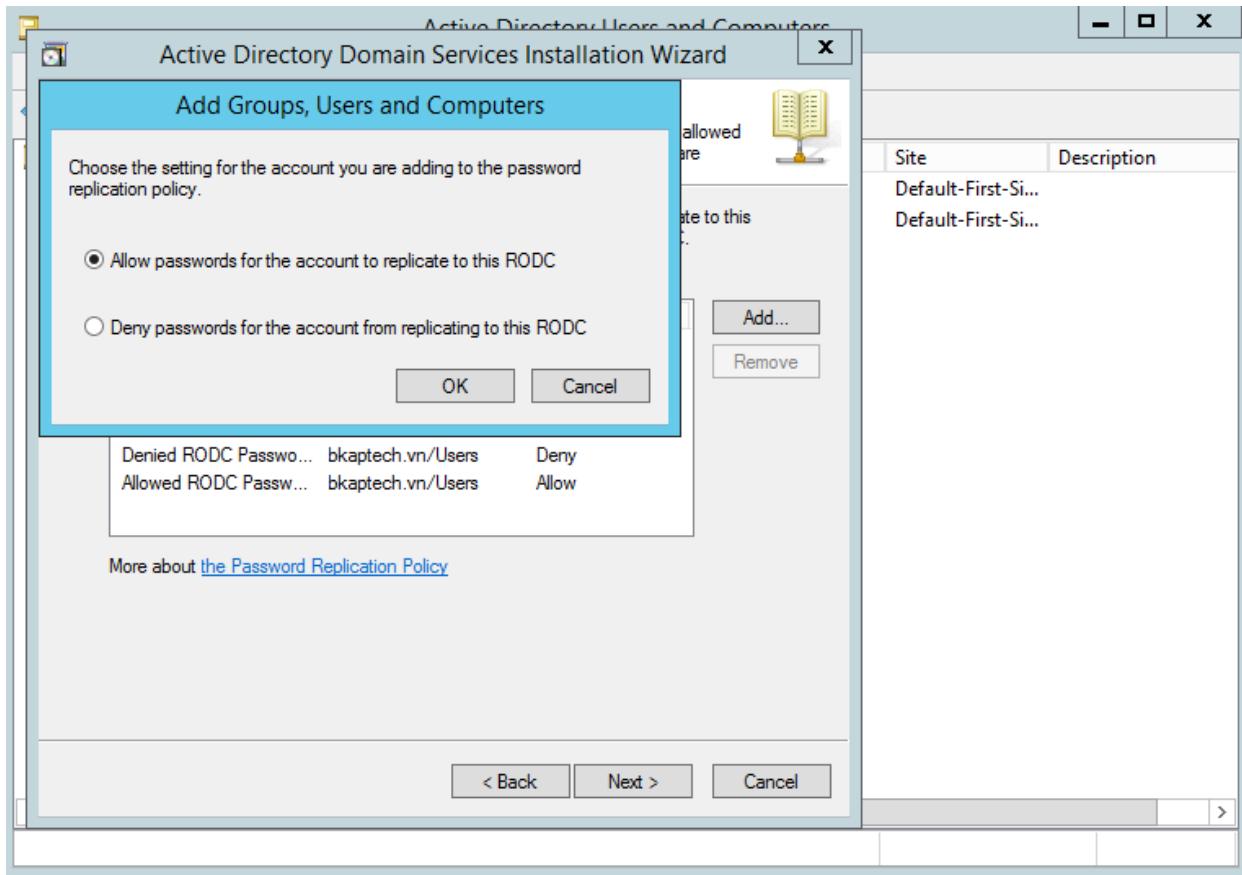
- Tại cửa sổ **Additional Domain Controller Options** , click vào **Next**.



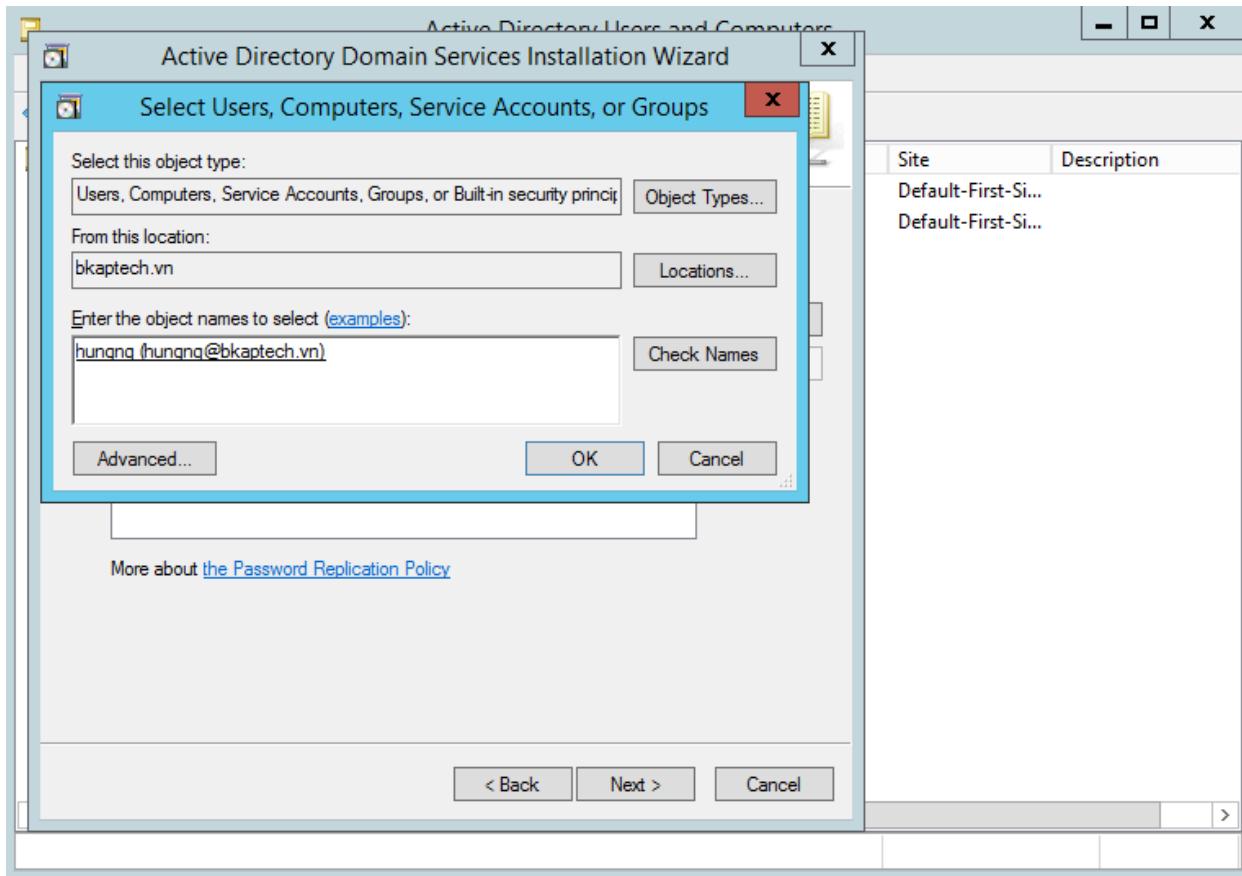
- Tại cửa sổ **Specify the Password Replication Policy**, click vào **Add...**



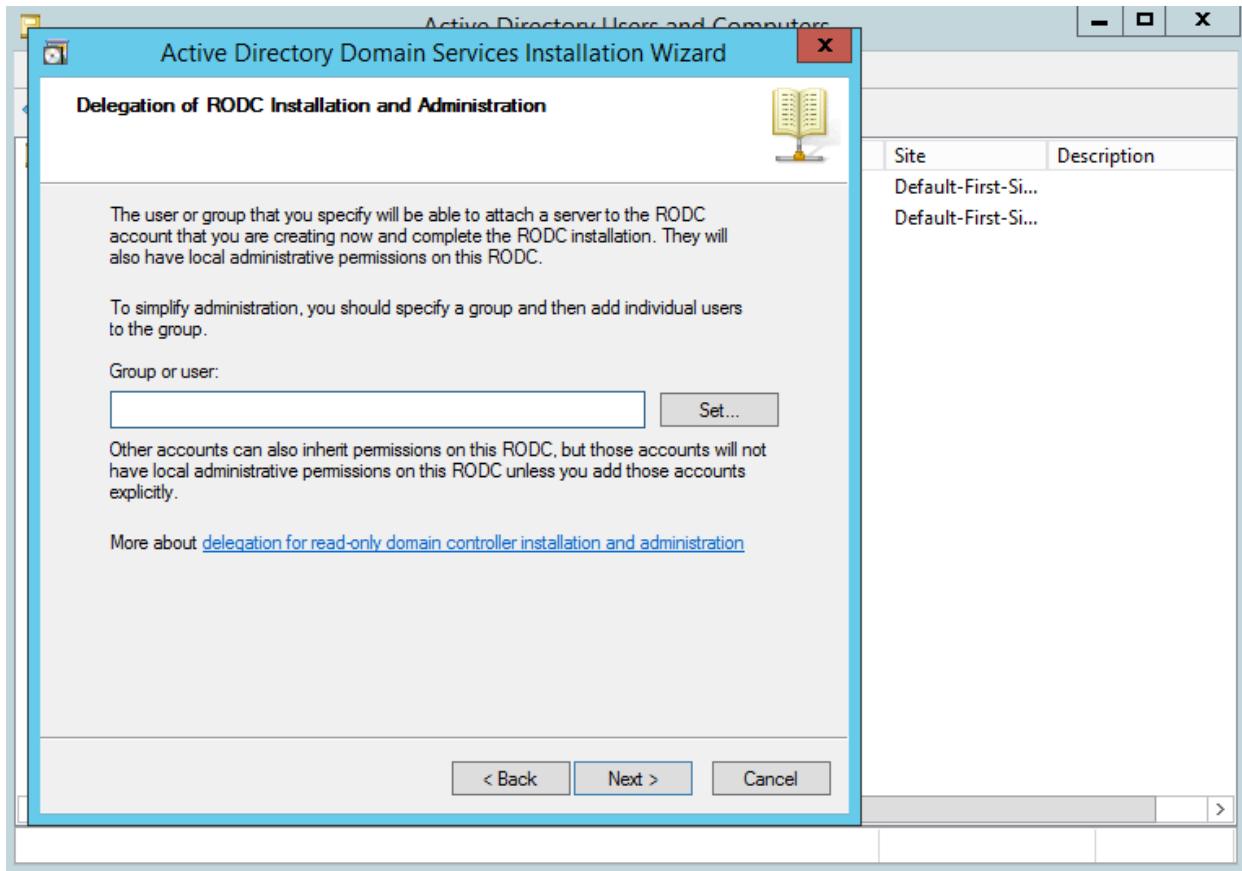
- Chọn vào **Allow passwords for the account to replicate to this RODC.**



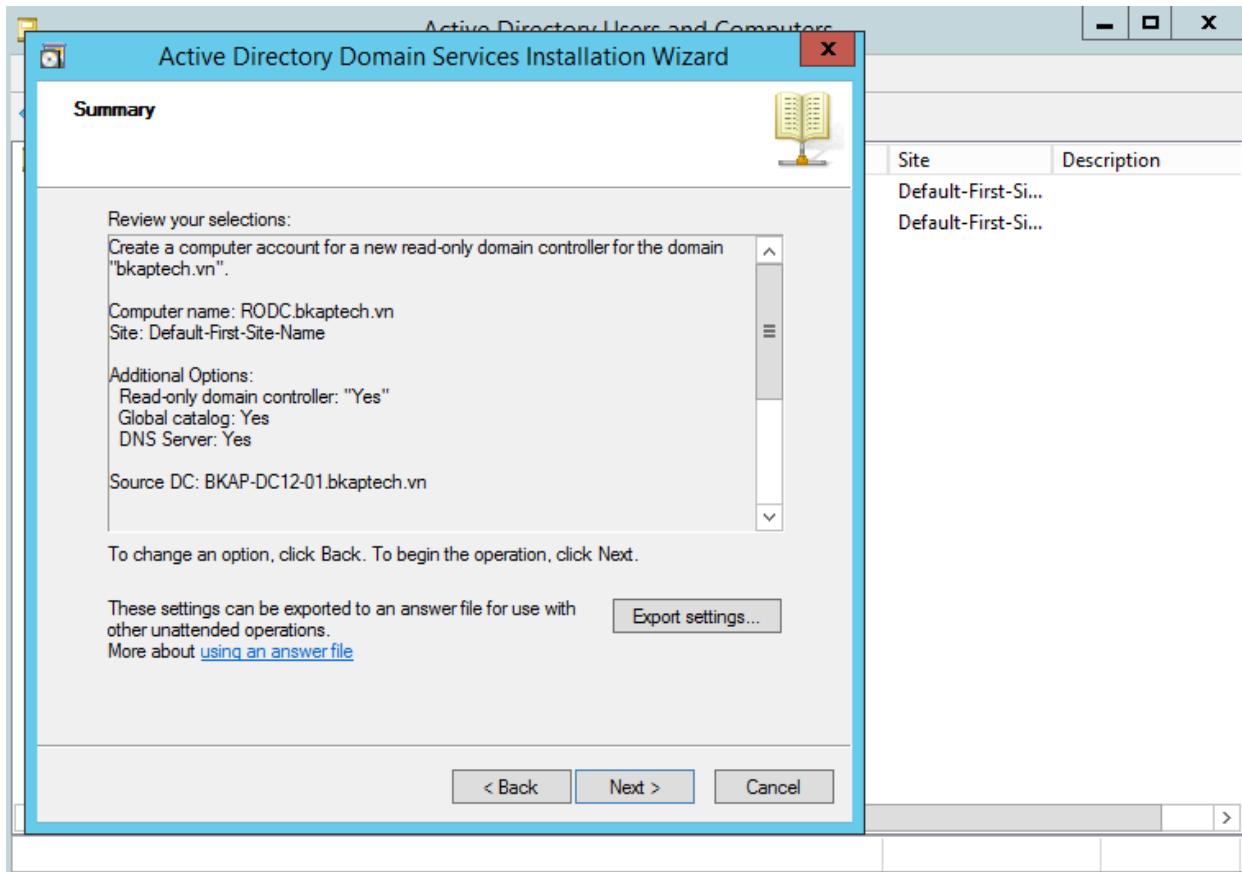
- Add vào tài khoản **hungnq**.



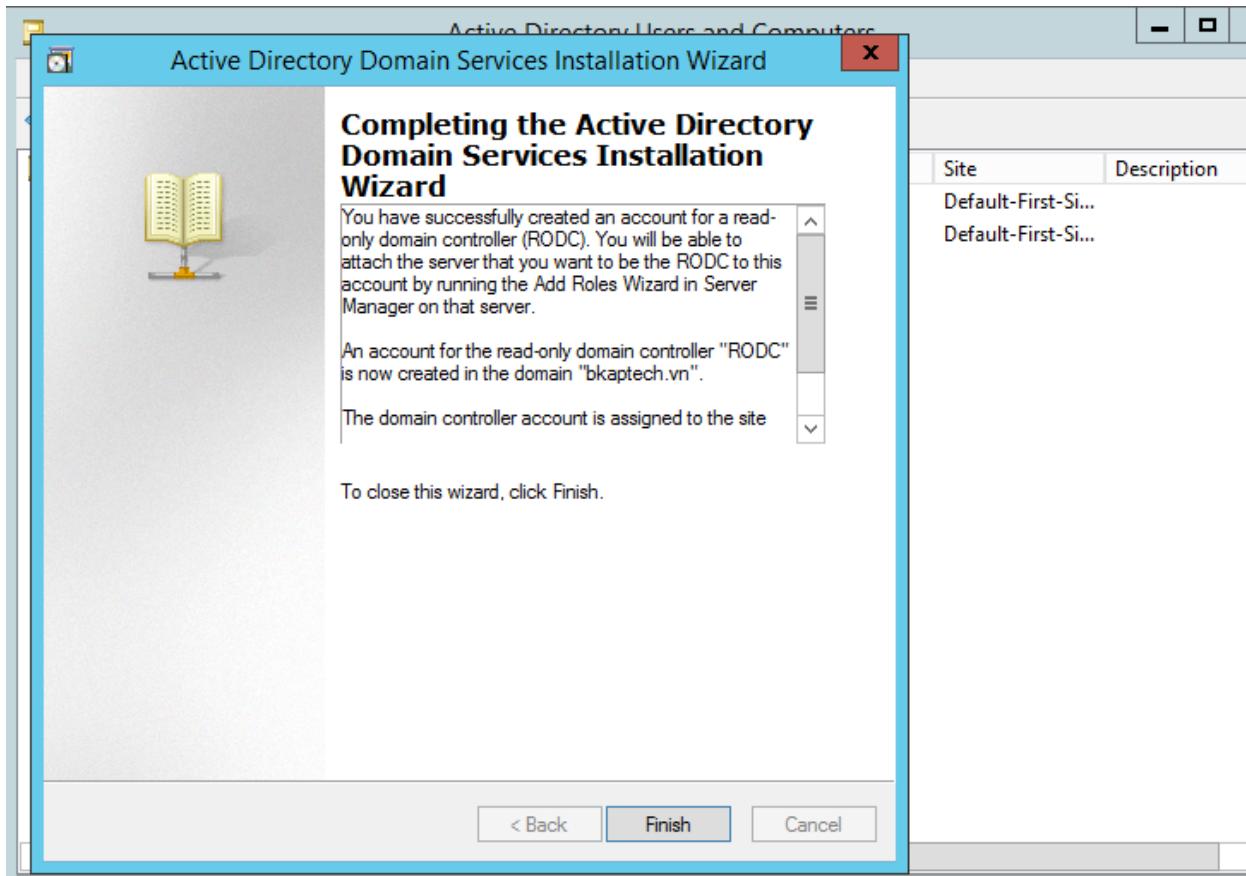
- Tại cửa sổ **Delegation of RODC Installation and Administration**, click vào Next.



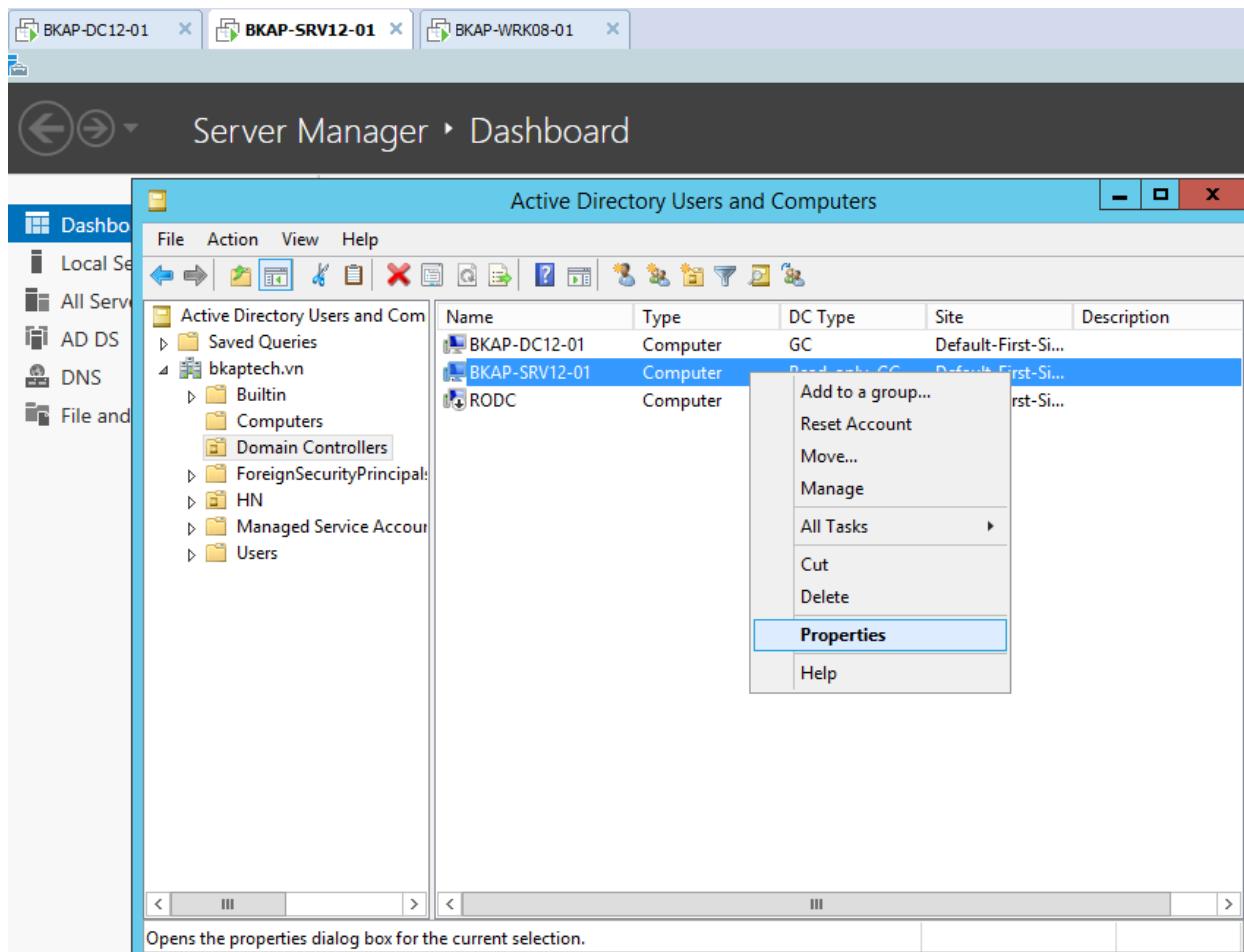
- Tại cửa sổ **Summary**, click vào **Next**.



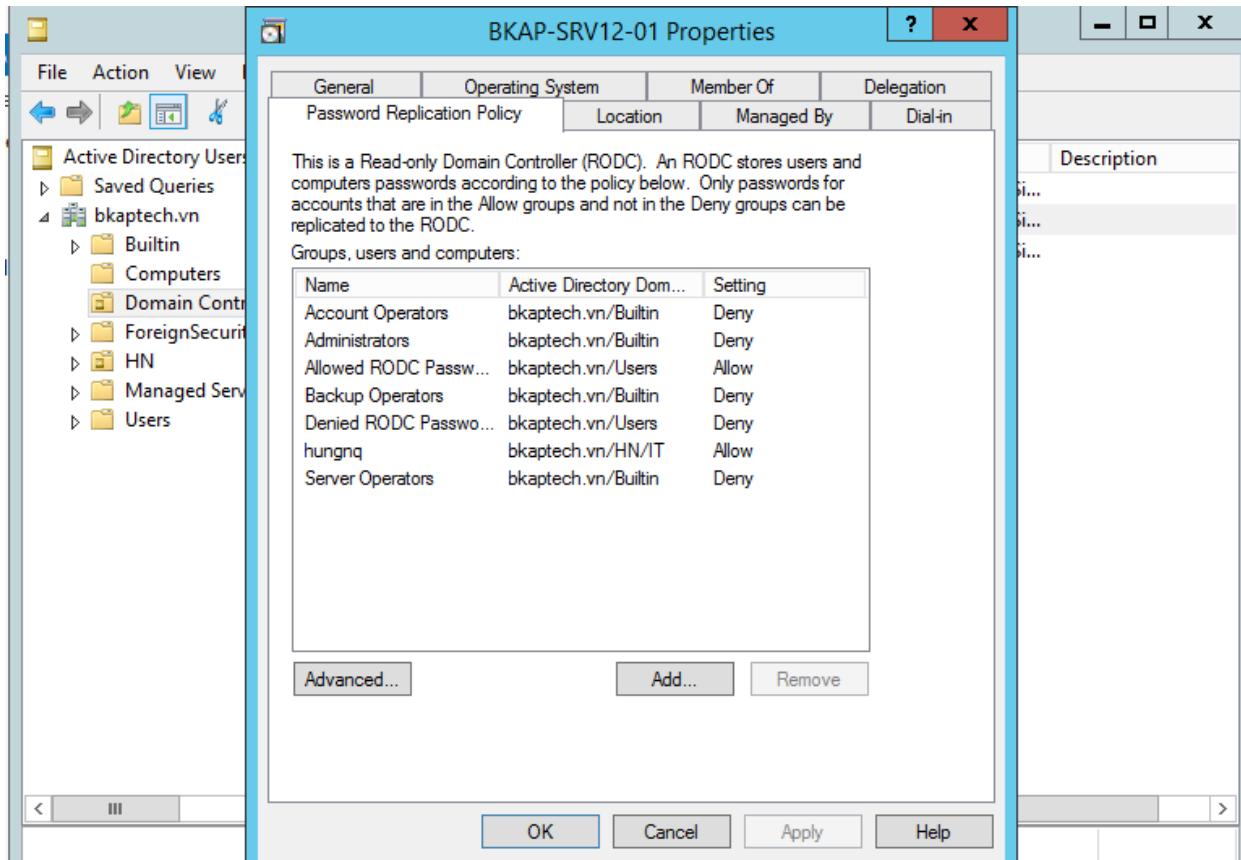
- Click vào **Finish**.



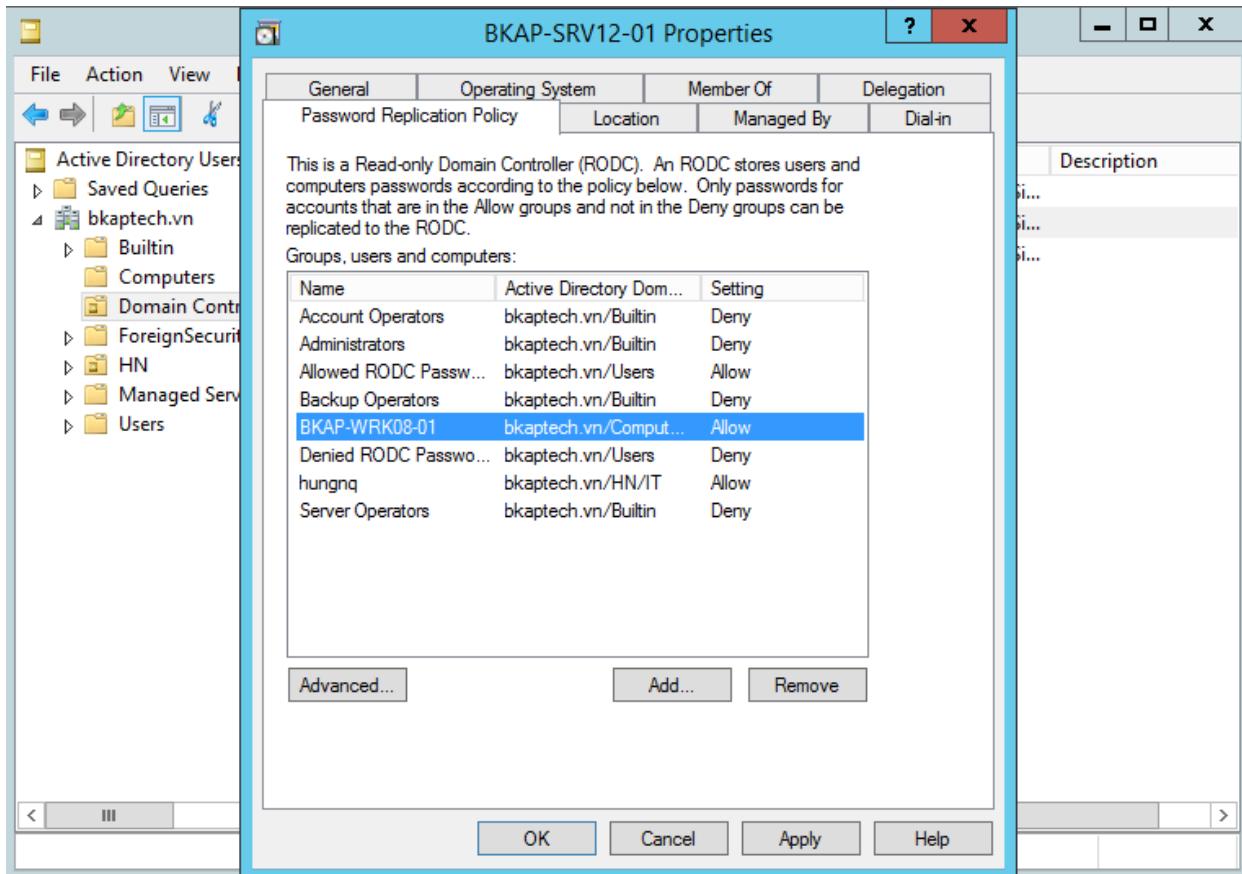
- Tại cửa sổ **Active Directory Users and Computers**, trong mục **Domain Controllers**, click chuột phải tại **BKAP-SRV12-01**, chọn **Properties**.



- Trong cửa sổ **BKAP-SRV12-01 Properties**, chuyển sang tab **Password Replication Policy**, click vào Add...



- Thực hiện *Add* thêm máy *BKAP-WRK08-01*.

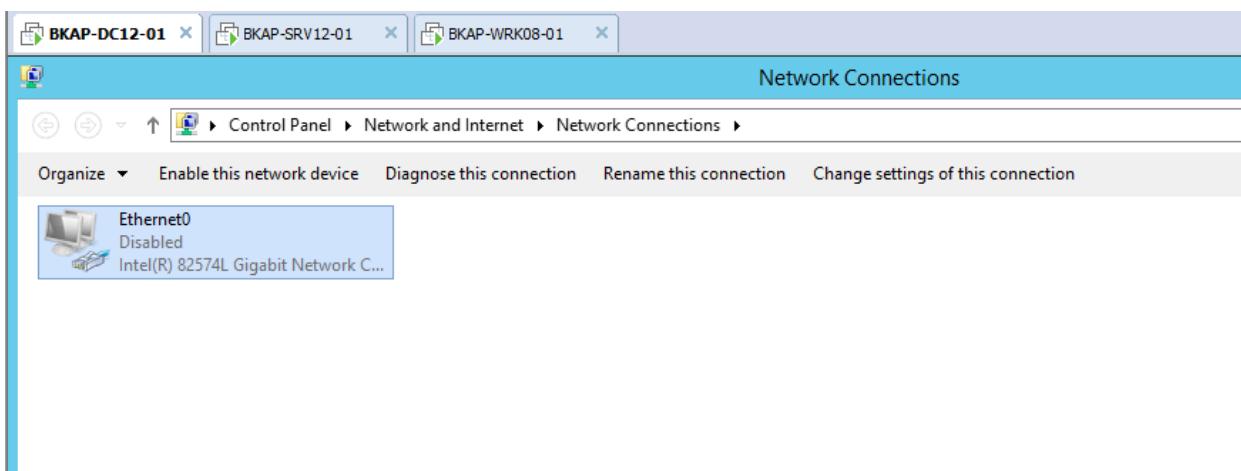


- Chuyển sang máy Client, đăng nhập tài khoản **hungnq** và **nghialv**





- Chuyển sang máy *BKAP-DC12-01*, tắt kết nối mạng, kiểm tra đăng nhập 2 tài khoản trên vẫn hoạt động bình thường.



3.2 Cấu hình AD DS snapshots.

1. Yêu cầu bài Lab:

- + Trên máy *BKAP-DC12-01*, tạo user trong ou **IT**.
 - Điền các thông tin cho tài khoản vừa tạo trong ou **IT**.
 - Description* : **Nhân viên phòng ban IT**.
 - Office* : **Bachkhoa-Aptech**
 - Telephone Number* : **09789 234 99**
 - Tạo **Snapshot** cho các thông tin của **Active Directory Domain Services**.
 - Xóa tài khoản vừa tạo.

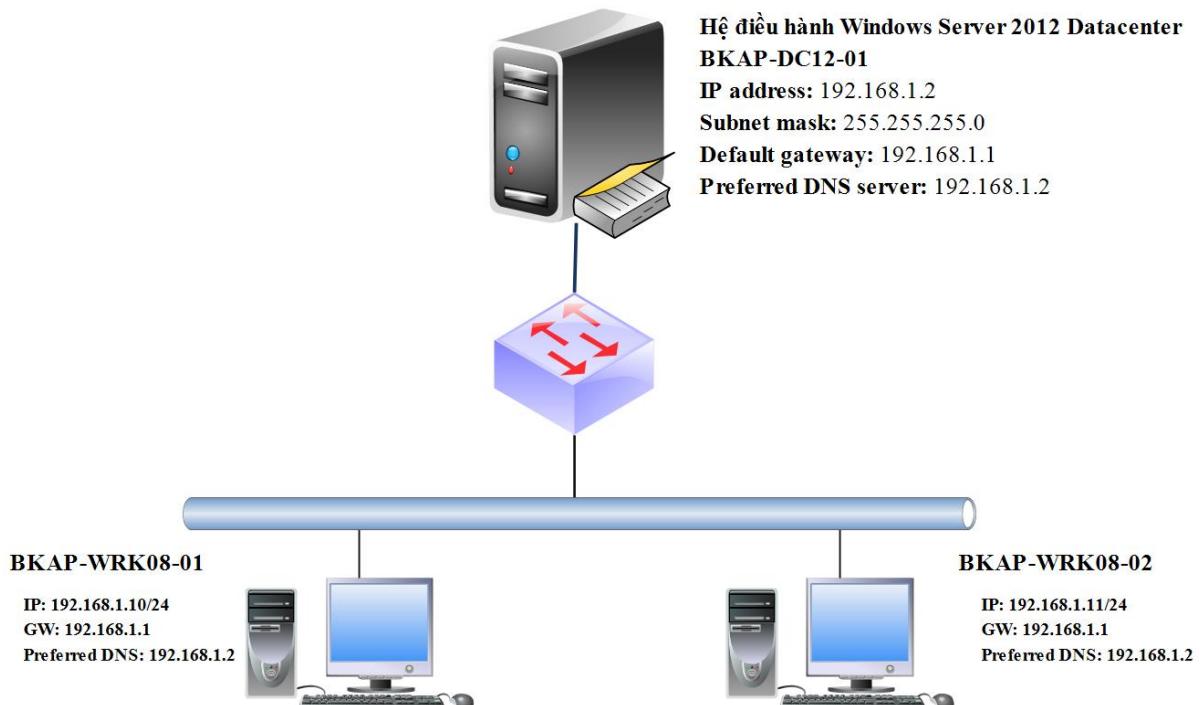
- Sử dụng **Ldp.exe** để khôi phục tài khoản.
- Hiển thị lại các *thông tin về user* đã bị xóa.

2. Yêu cầu chuẩn bị:

+ Chuẩn bị máy Server **BKAP-DC12-01** thành **Domain Controller** quản lý miền **bkaptech.vn**.

3. Mô hình Lab:

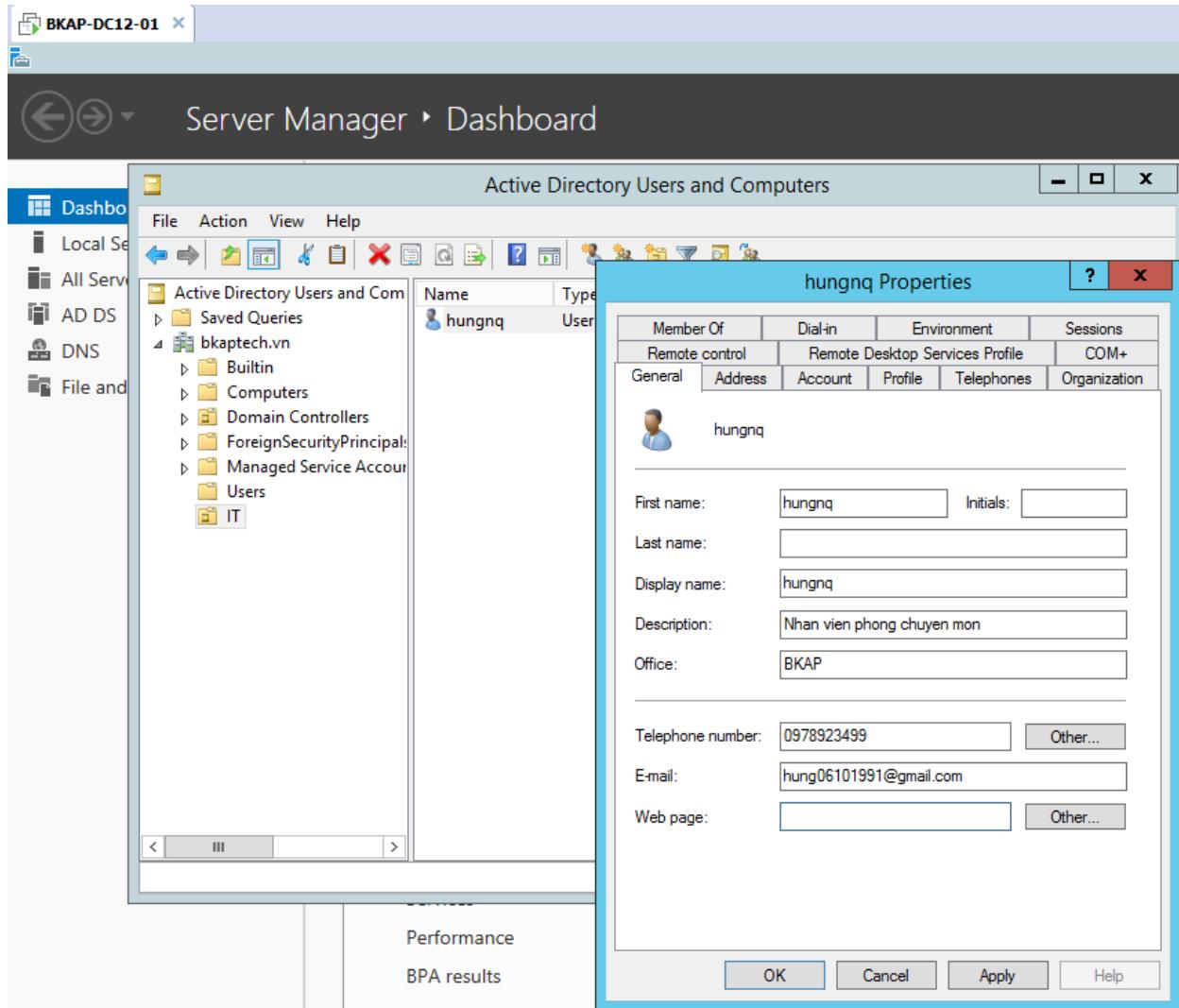
Lab 3.2 Cấu hình AD DS Snapshots.



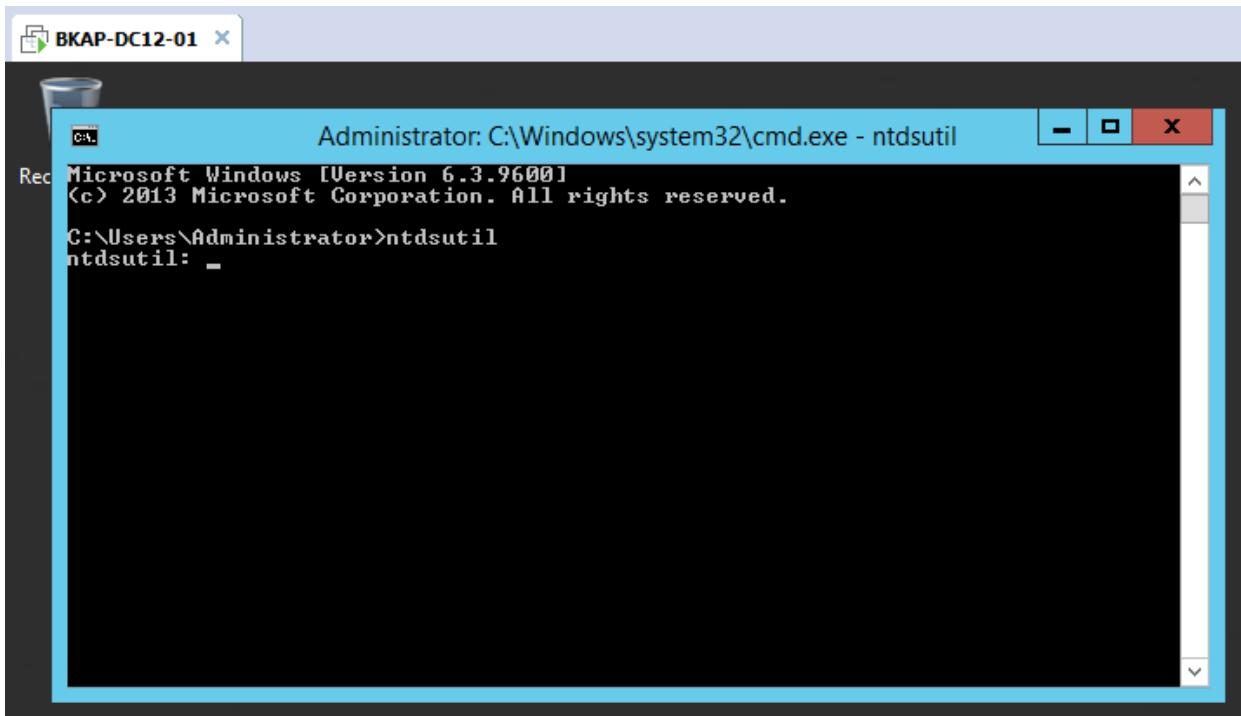
Hình 3.2

Hướng dẫn chi tiết:

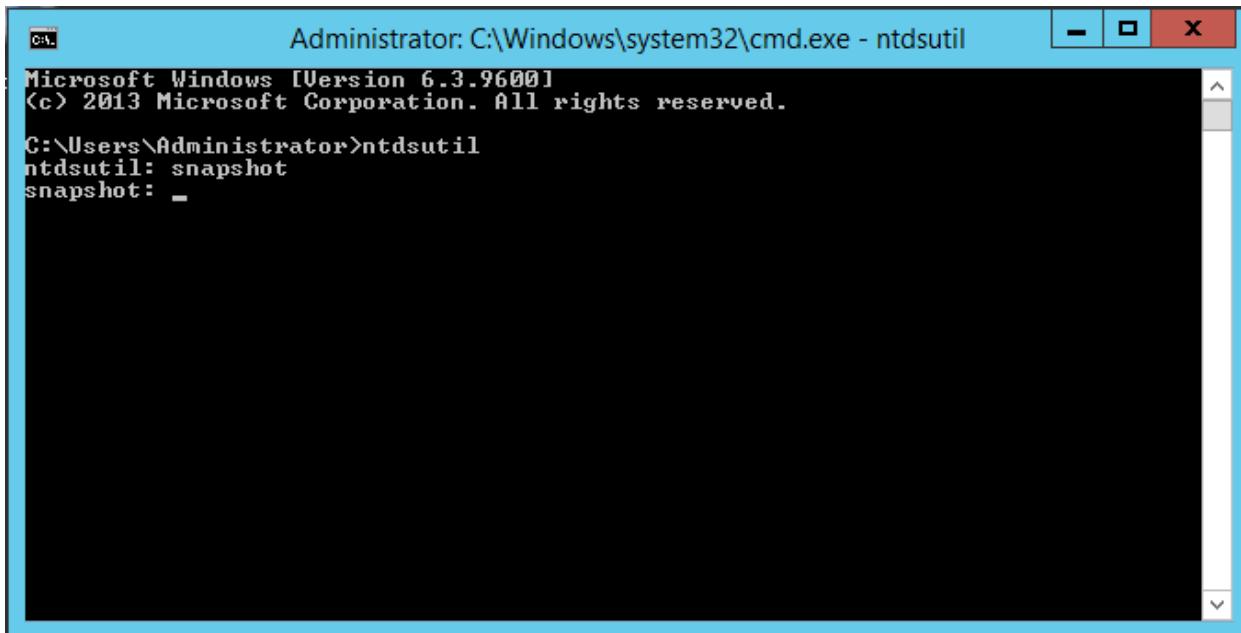
- Thực hiện trên máy **BKAP-DC12-01**, tạo user **hungnq** và các thông tin (tại tab **General**).



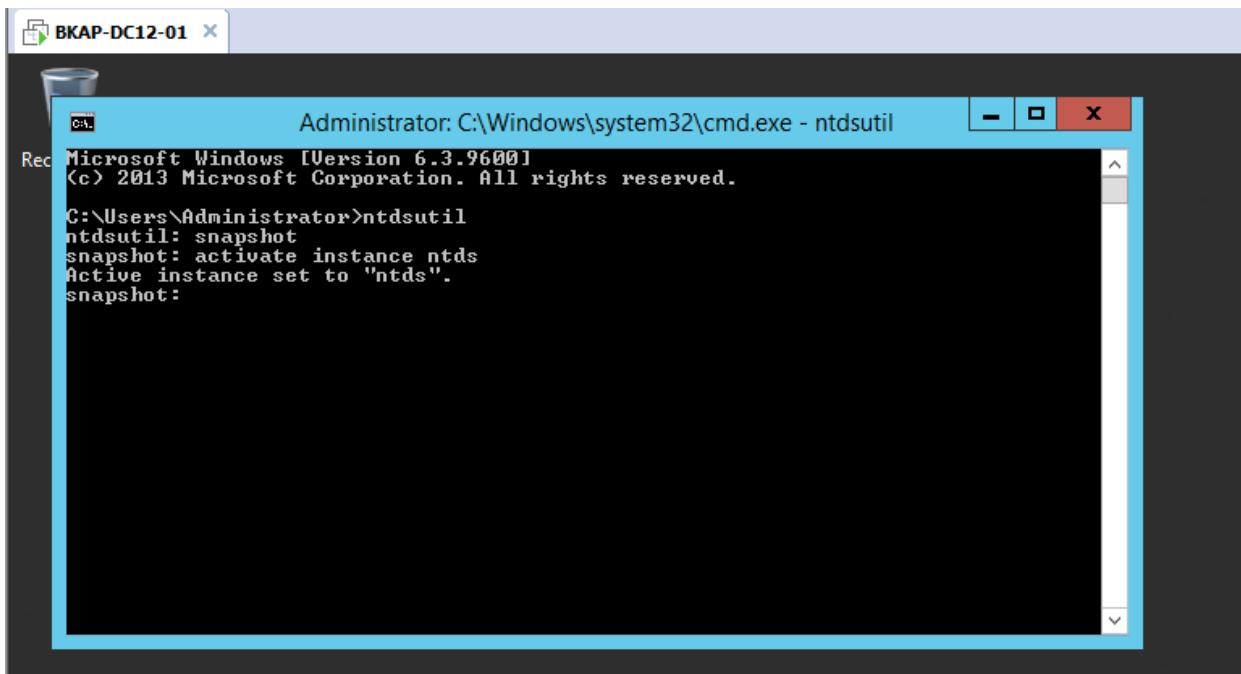
- Vào cmd , gõ lệnh ntdsutil



- Tại ntdsutil , gõ lệnh snapshot.



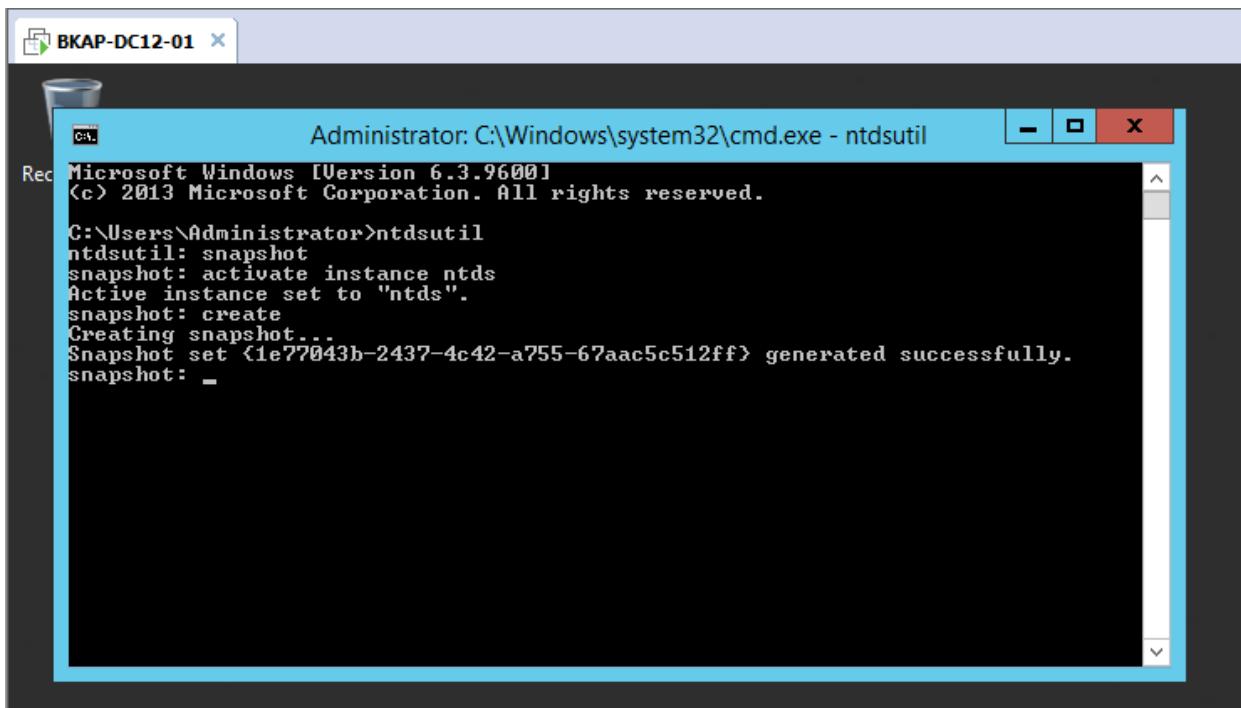
- Tại **snapshot**, gõ lệnh **activate instance ntds**



```
Administrator: C:\Windows\system32\cmd.exe - ntdsutil
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ntdsutil
ntdsutil: snapshot
snapshot: activate instance ntds
Active instance set to "ntds".
snapshot:
```

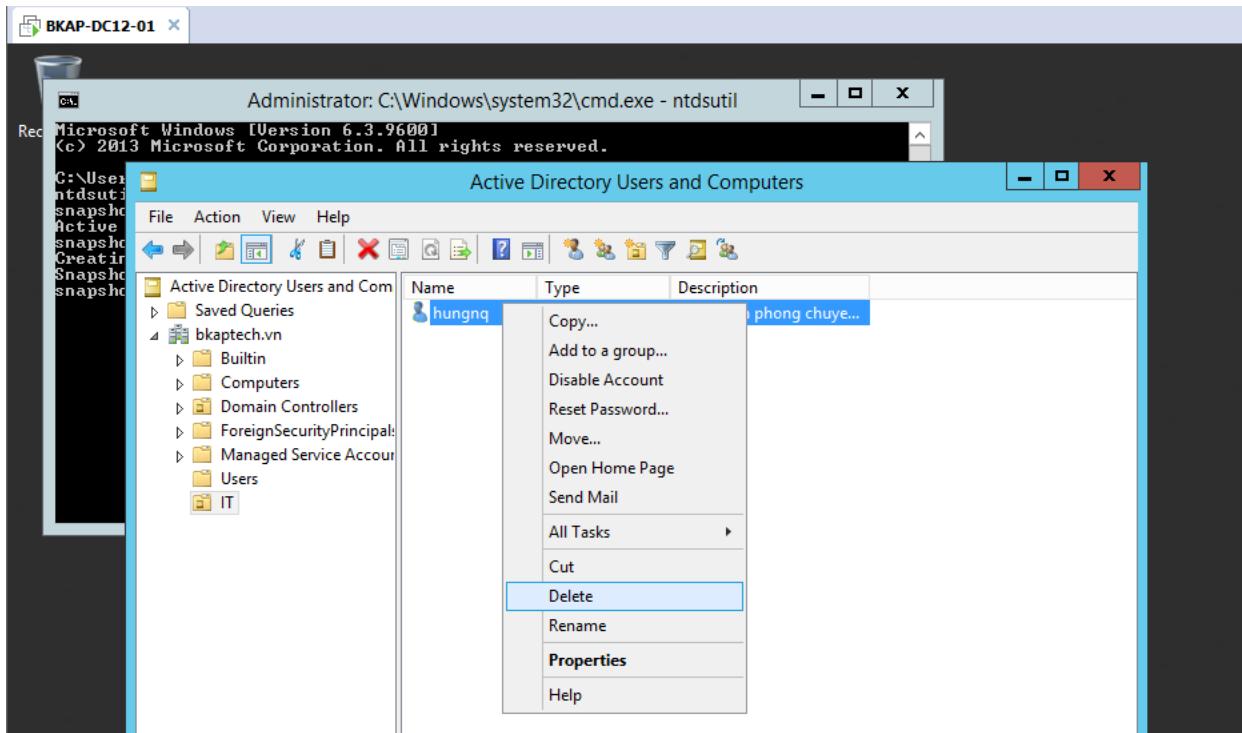
- Tiếp theo gõ lệnh **create**.



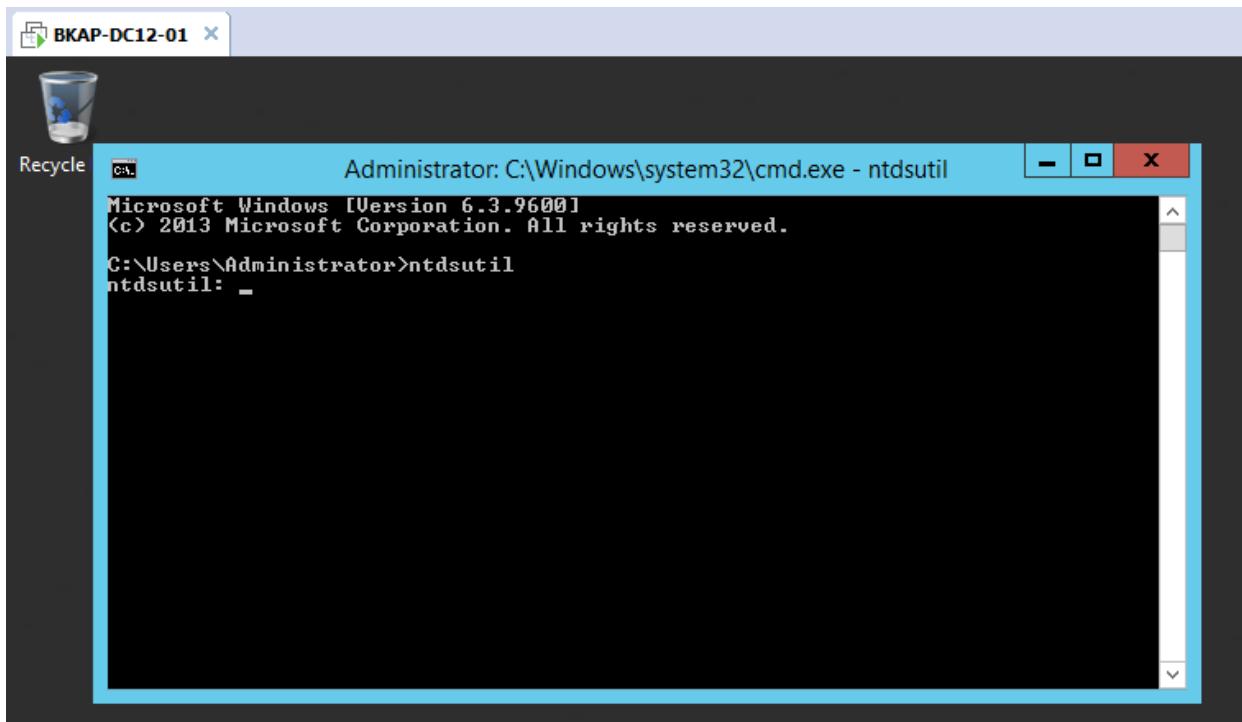
```
Administrator: C:\Windows\system32\cmd.exe - ntdsutil
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ntdsutil
ntdsutil: snapshot
snapshot: activate instance ntds
Active instance set to "ntds".
snapshot: create
Creating snapshot...
Snapshot set {1e77043b-2437-4c42-a755-67aac5c512ff} generated successfully.
snapshot: _
```

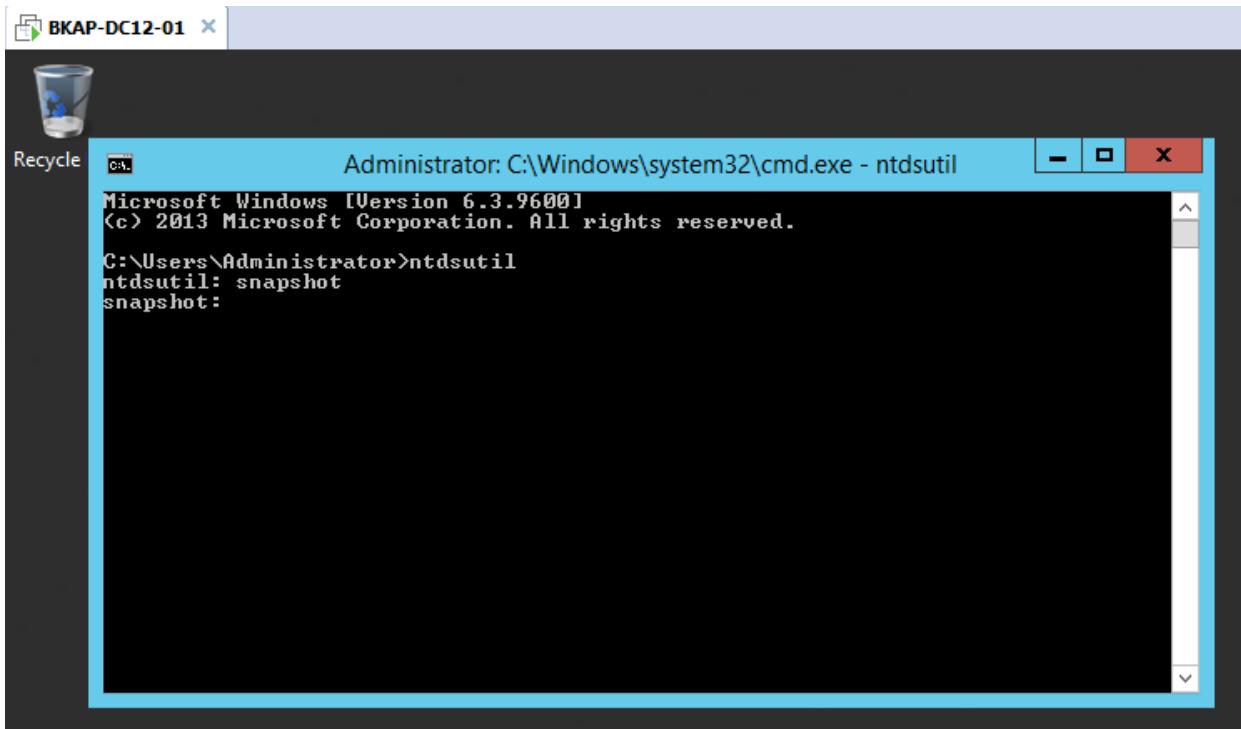
- Tiến hành xóa user **hungnq**.



- Vào cmd , gõ lại lệnh **ntdsutil**.



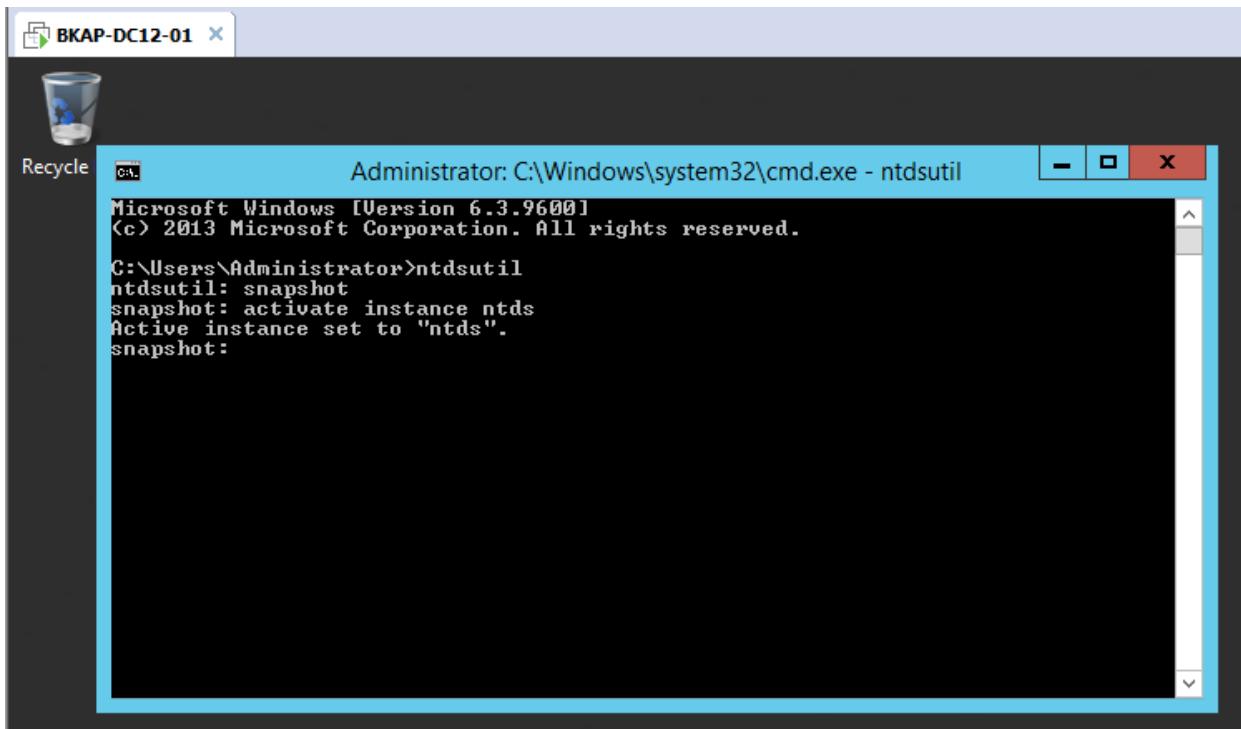
- Gõ lệnh **snapshot**.



```
Administrator: C:\Windows\system32\cmd.exe - ntdsutil
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ntdsutil
ntdsutil: snapshot
snapshot:
```

- Tiếp theo gõ lệnh **activate instance ntds**



```
Administrator: C:\Windows\system32\cmd.exe - ntdsutil
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ntdsutil
ntdsutil: snapshot
snapshot: activate instance ntds
Active instance set to "ntds".
snapshot:
```

- Tiếp theo gõ lệnh **list all** (*liệt kê danh sách snapshot*).

```
Administrator: C:\Windows\system32\cmd.exe - ntdsutil
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ntdsutil
ntdsutil: snapshot
snapshot: activate instance ntds
Active instance set to "ntds".
snapshot: list all
 1: 2016/03/18:00:48 {1e77043b-2437-4c42-a755-67aac5c512ff}
 2: C: {32cccd0b7-c521-40d2-bfcb-d322a82f58bc}

snapshot:
```

- Tiếp theo gõ lệnh **mount 1**.

```
Administrator: C:\Windows\system32\cmd.exe - ntdsutil
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ntdsutil
ntdsutil: snapshot
snapshot: activate instance ntds
Active instance set to "ntds".
snapshot: list all
 1: 2016/03/18:00:48 {1e77043b-2437-4c42-a755-67aac5c512ff}
 2: C: {32cccd0b7-c521-40d2-bfcb-d322a82f58bc}

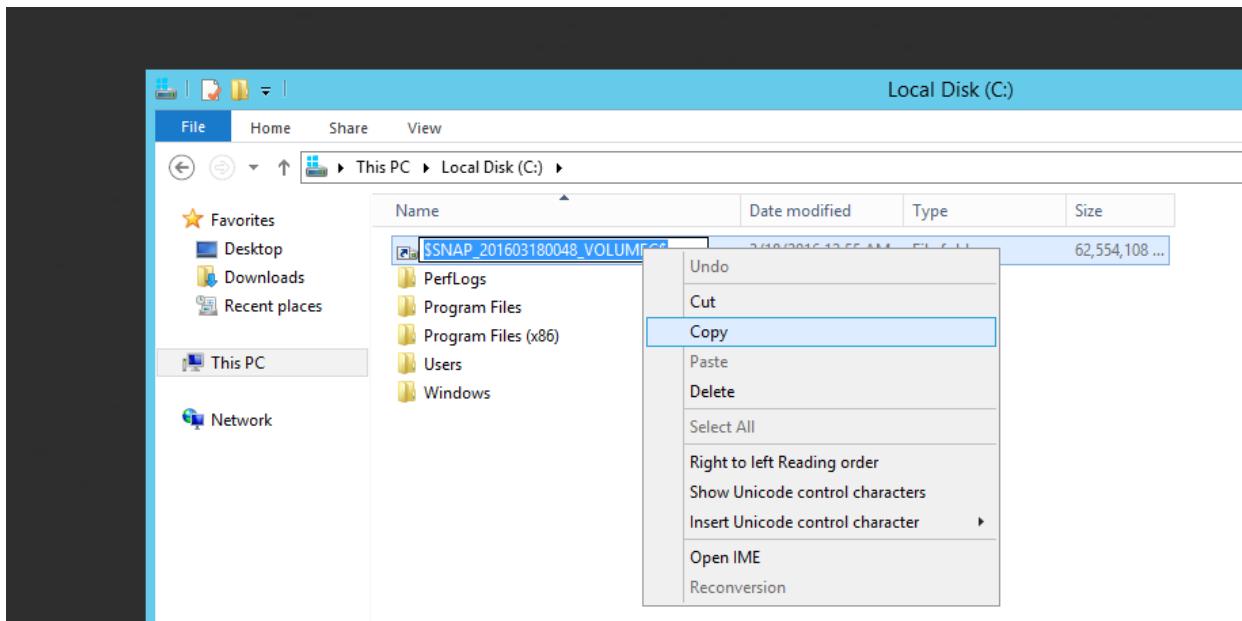
snapshot: mount 1
```

```
Administrator: C:\Windows\system32\cmd.exe - ntdsutil
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

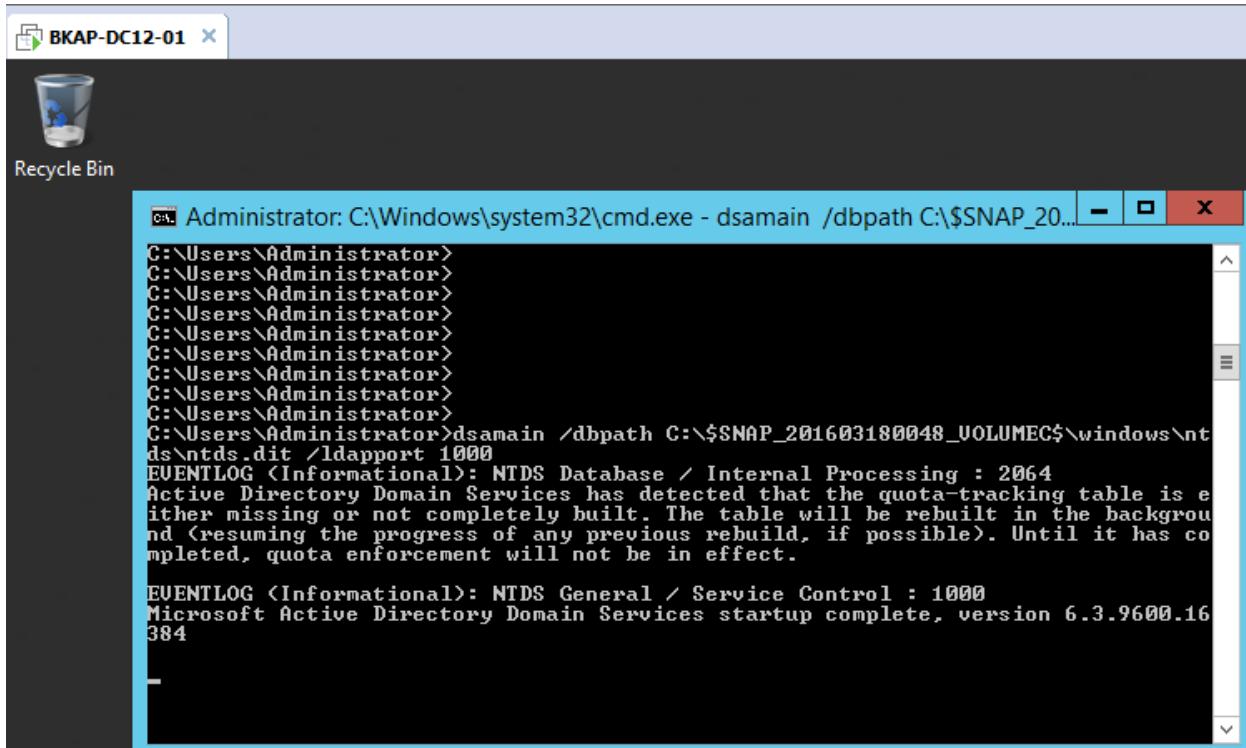
C:\Users\Administrator>ntdsutil
ntdsutil: snapshot
snapshot: activate instance ntds
Active instance set to "ntds".
snapshot: list all
  1: 2016/03/18:00:48 <1e77043b-2437-4c42-a755-67aac5c512ff>
  2:  C: <32cccd0b7-c521-40d2-bfcb-d322a82f58bc>

snapshot: mount 1
Snapshot <32cccd0b7-c521-40d2-bfcb-d322a82f58bc> mounted as C:\$SNAP_201603180048
_VOLUMEC$\
snapshot: -
```

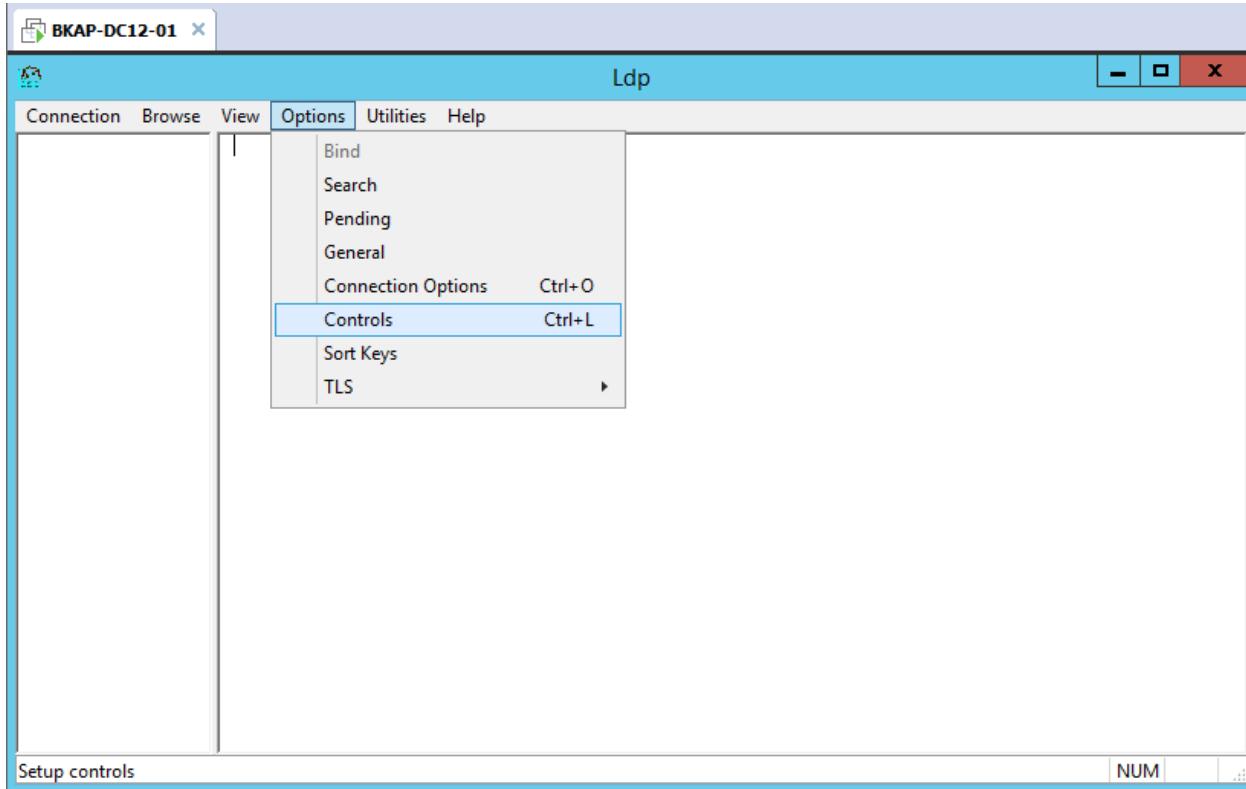
- Copy tên file snapshot trong ổ C.



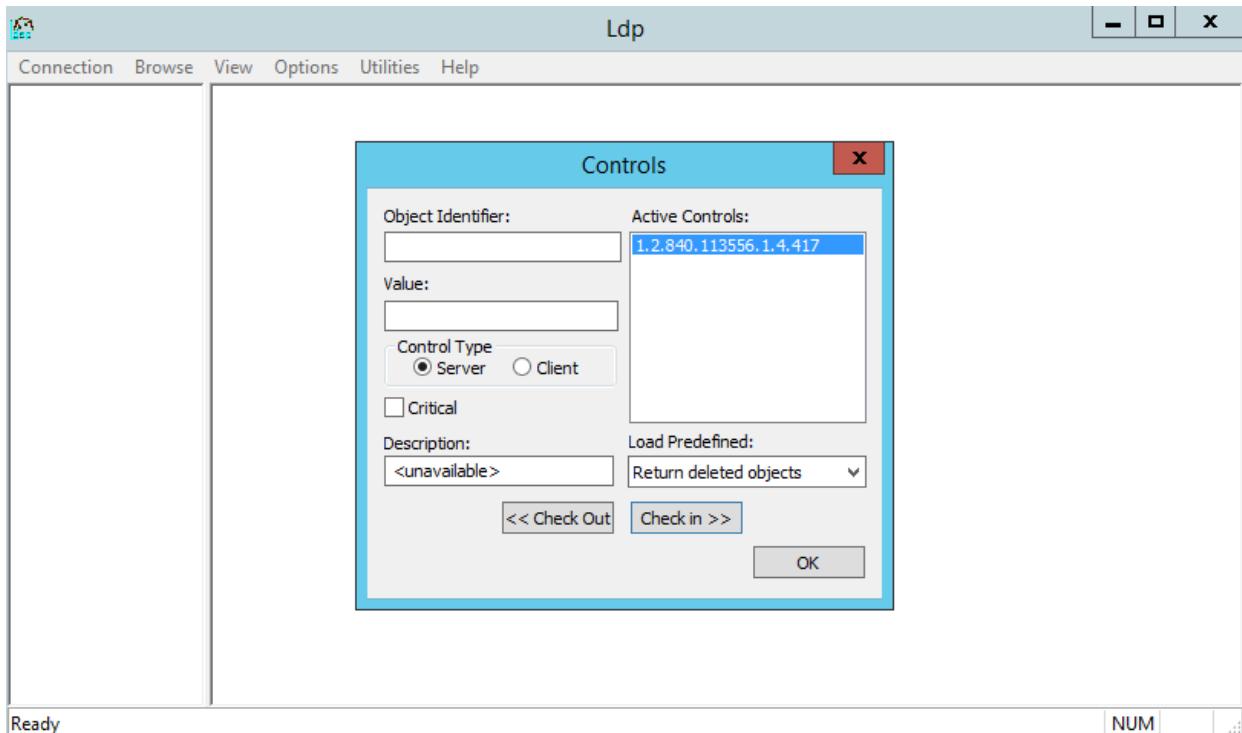
- Vào cmd , gõ lệnh
 - **dsamain /dbpath**
C:\\$SNAP_201603180048_VOLUMEC\$\windows\ntds\ntds.dit /ldapport 1000



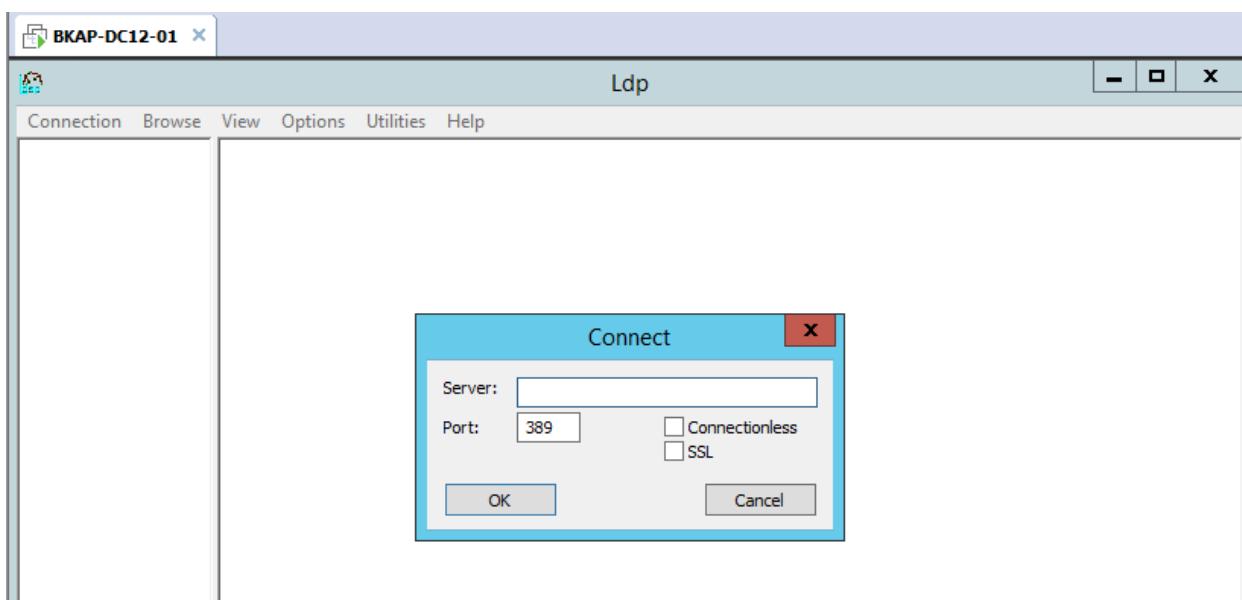
- Sử dụng **ldp.exe**
 - Tại cửa sổ **ldp** , click vào **Options / Controls**



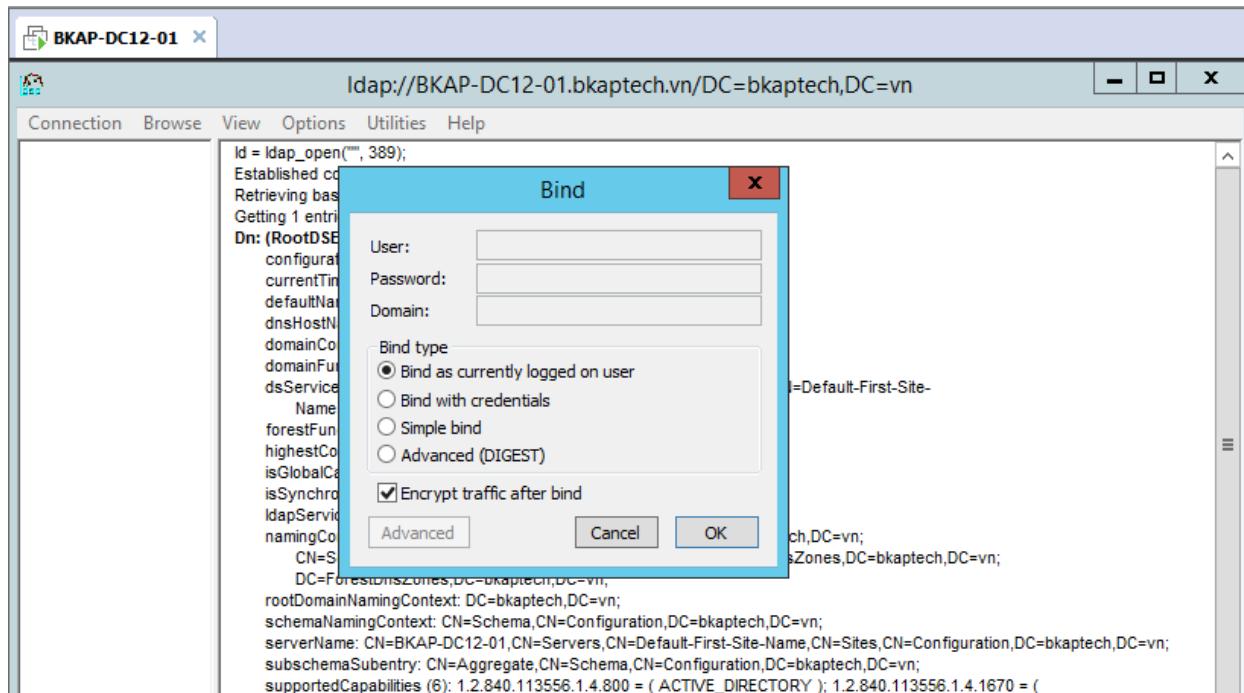
- Tại cửa sổ **Controls**, trong mục **Load Predefined**, chọn vào **Return deleted objects.** => **OK.**



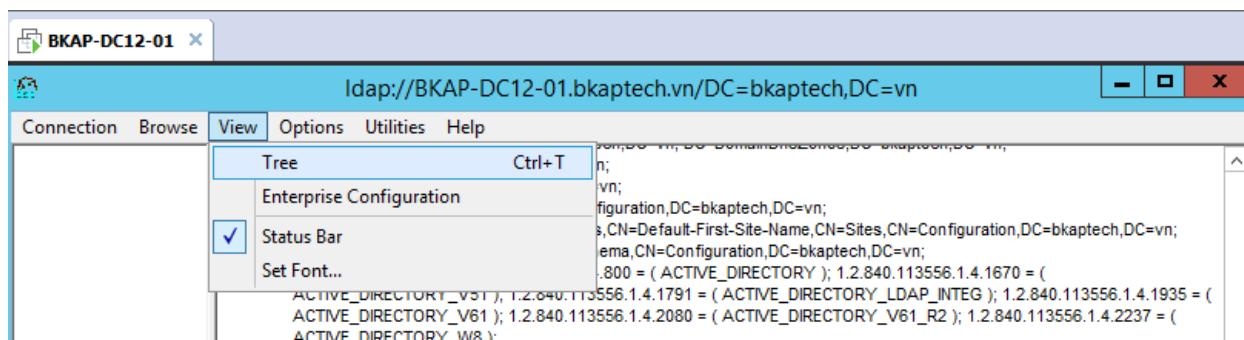
- Tại **Ldp**, chọn vào **Connection / Connect.../ OK**



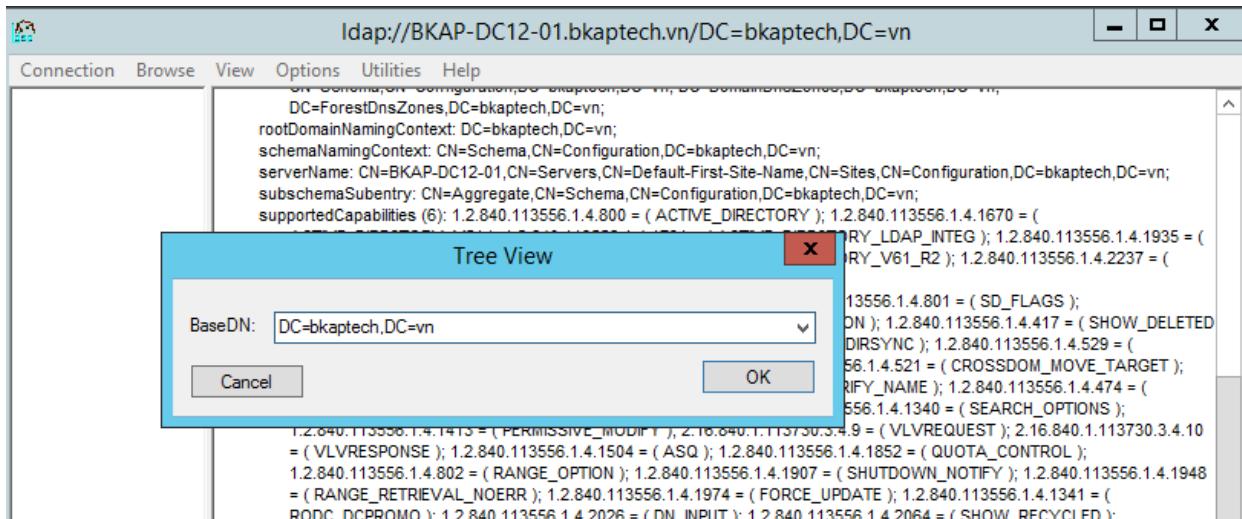
- Click vào Connection / Bind...OK



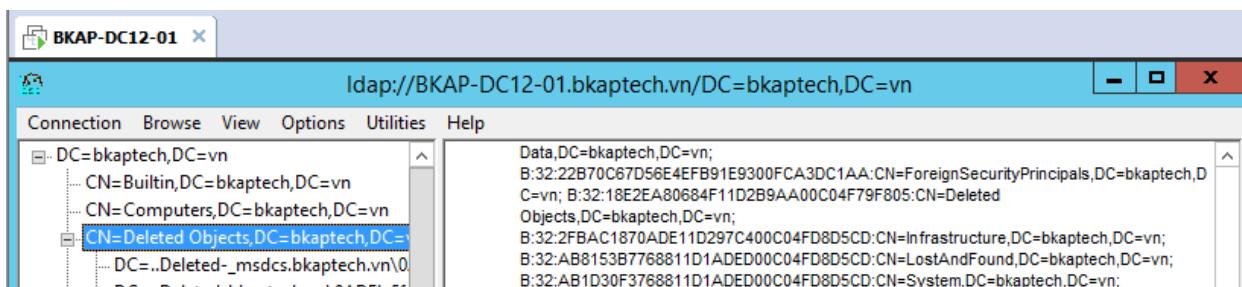
- Chọn sang tab View / Tree.



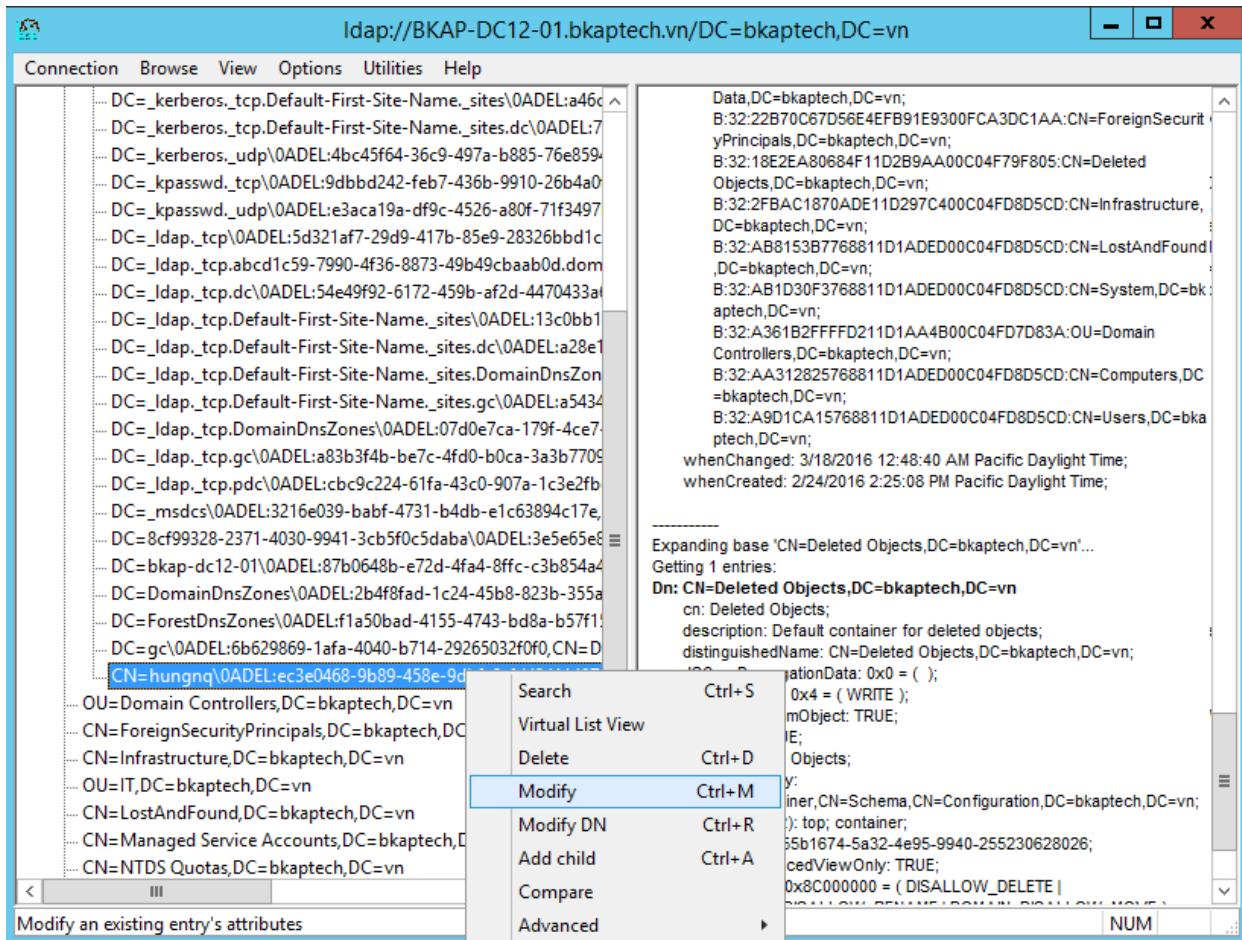
- Tại cửa sổ Tree View , nhập vào **DC=bkaptech,DC=vn**



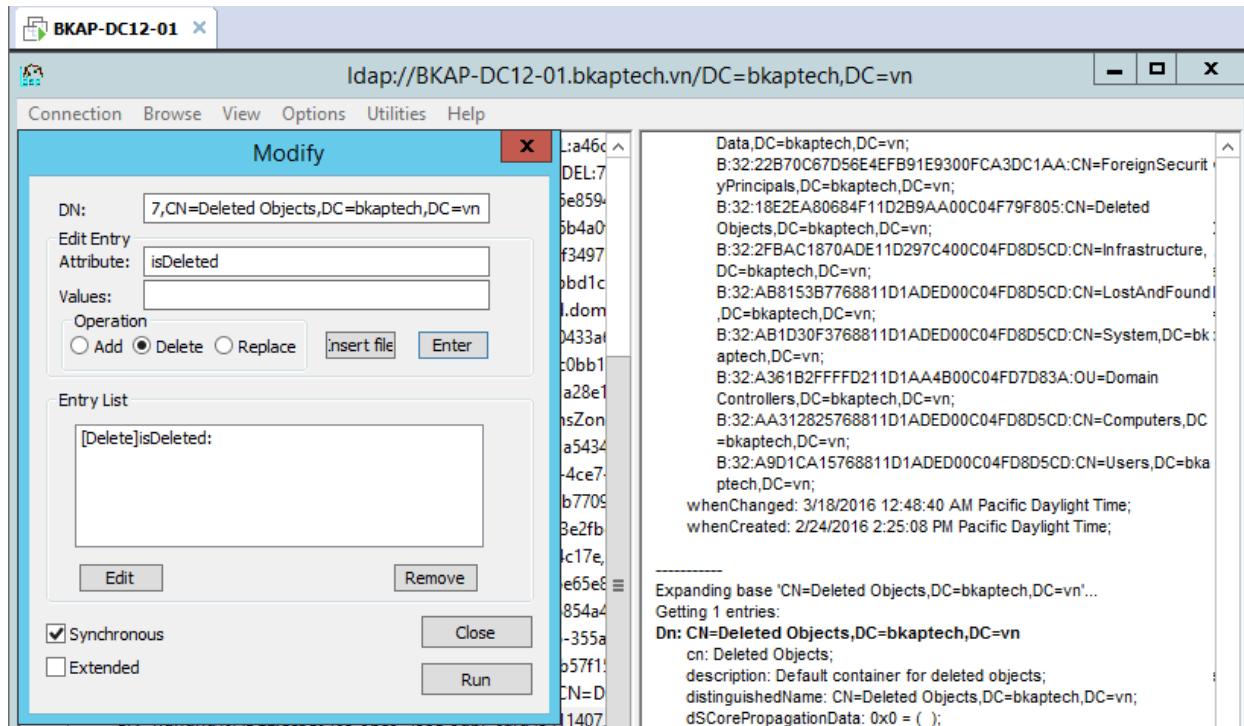
- Chọn vào dòng **CN=Deleted Objects,DC=bkaptech,DC=vn**



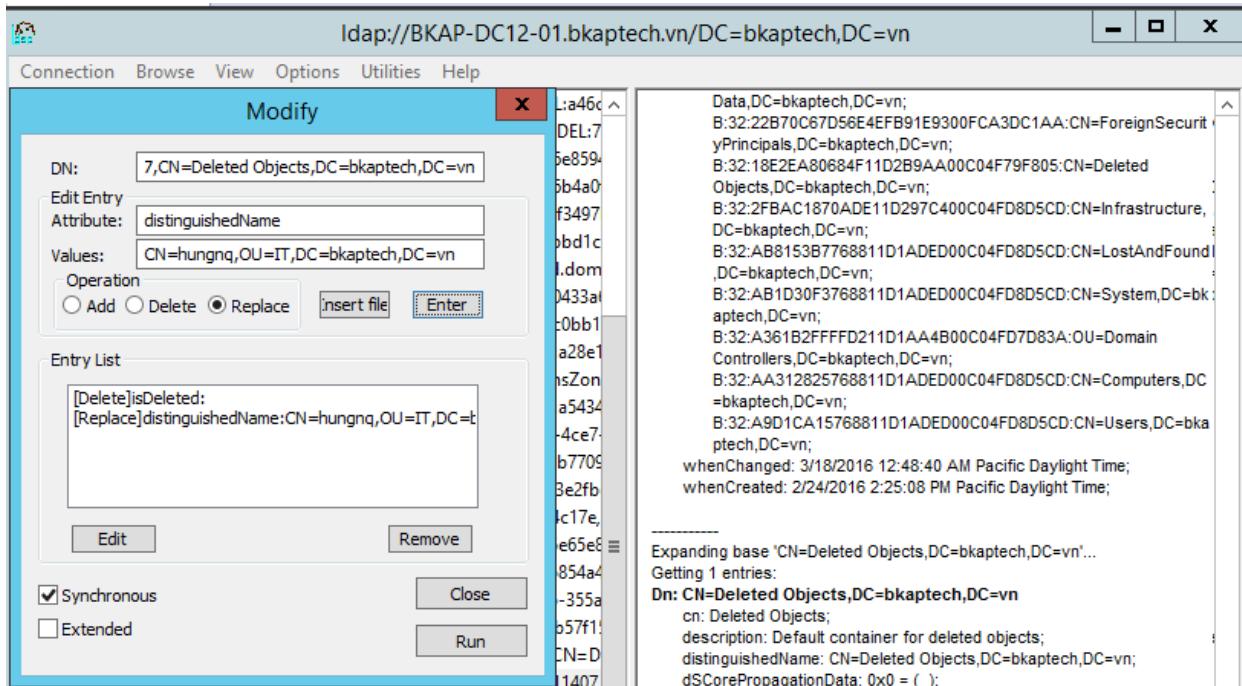
- Click chuột phải tại tên user **hungnq** , chọn **Modify**.



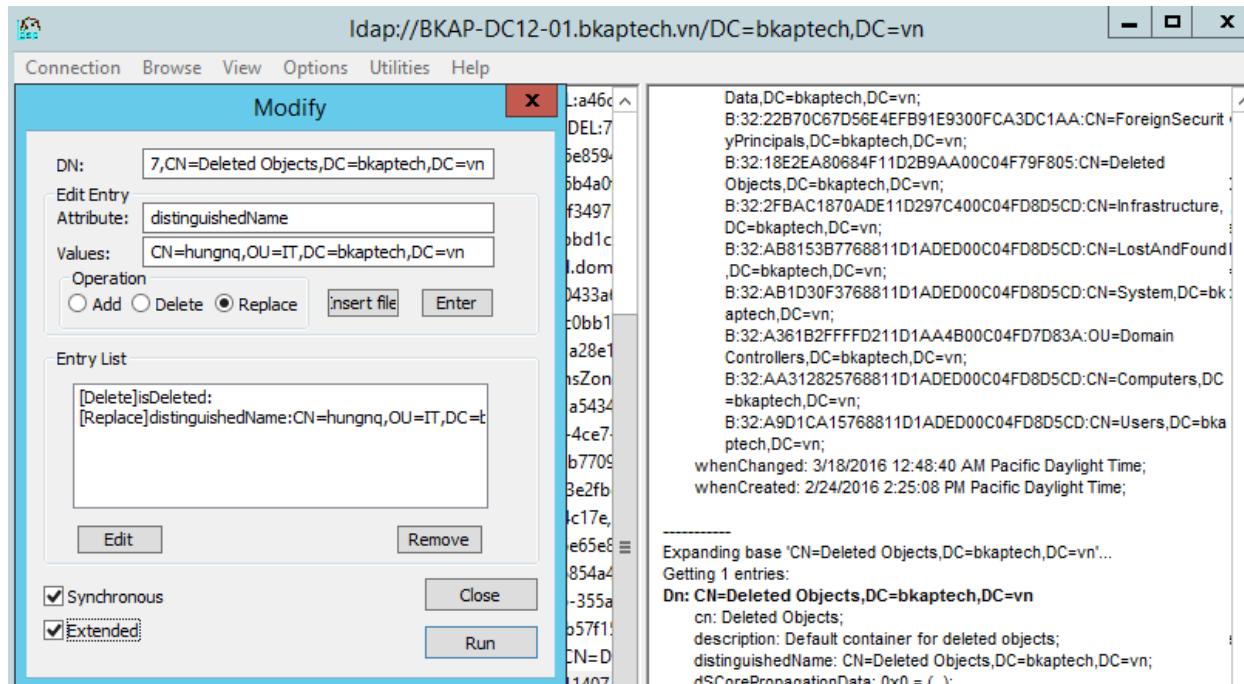
- Tại cửa sổ **Modify** , tại mục **Operation** , chọn vào **Delete** , sau đó nhập vào **isDeleted** tại mục **Edit Entry Attribute** , tiếp theo click vào **Enter**.



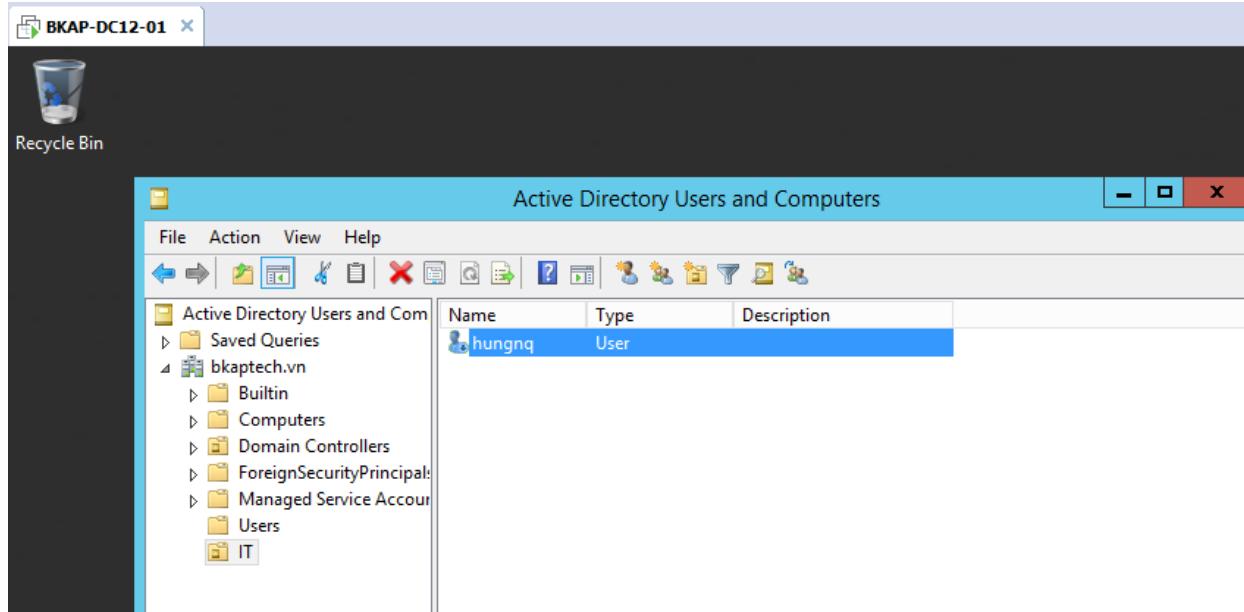
- Xóa chữ **isDeleted** vừa ghi ở mục **Edit Entry Attribute**, nhập vào **distinguishedName**
 - Tại mục **Values**, nhập vào : **CN=hungnq,OU=IT,DC=bkaptech,DC=vn.**
 - Tại **Operation**, chọn vào **Replace**.
 - => click vào **Enter**.



- Click chọn vào **Extend**, sau đó click vào **Run**, => **Close**.



- Kiểm tra trong **Active Directory User and Computers**, tài khoản **hungnq** đã được khôi phục.



Thực hiện **Reset Password** và **Enable User**.

3.3 Khôi phục tài khoản người dùng bằng Active Directory Recycle Bin

1. Yêu cầu bài Lab:

- + Khôi phục các đối tượng đã xóa do vô tình bằng cách nhanh chóng và giảm thời gian chết trong việc mất dữ liệu.

2. Yêu cầu chuẩn bị:

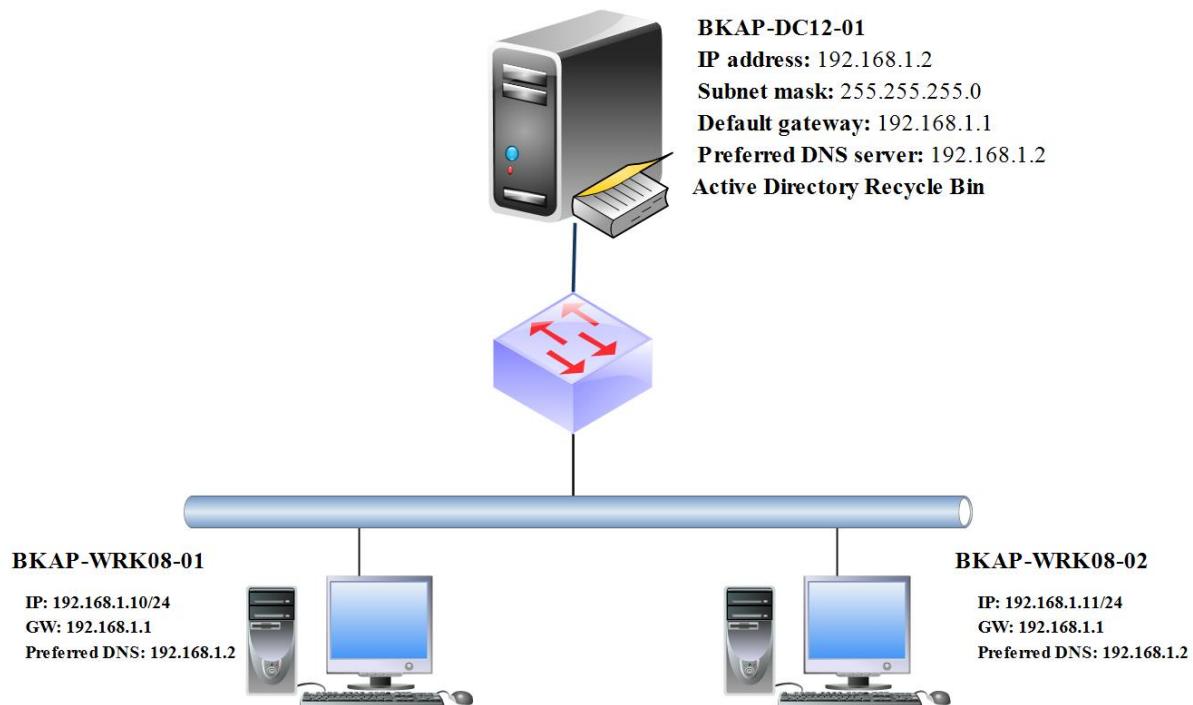
- + Máy BKAP-DC12-01 làm *Domain Controller* quản lý miền **bkaptech.vn**.
- + Tạo các tài khoản để kiểm tra.
- + Xóa và khôi phục tài khoản.
- + Enable tính năng **Active Directory Recycle Bin**.

3. Mô hình Lab:

HỆ THỐNG ĐÀO TẠO CNTT QUỐC TẾ BACHKHOA-APTECH



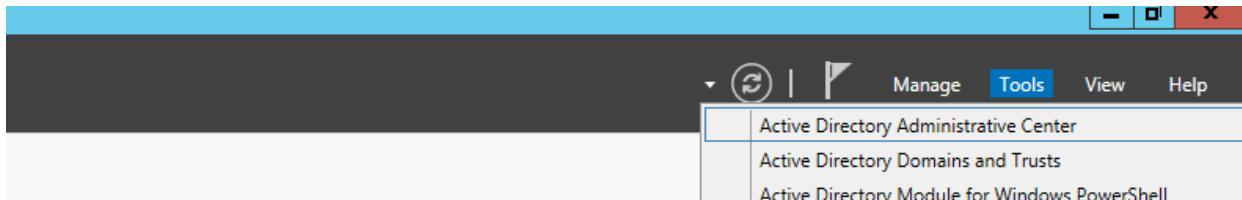
Lab 3.3 Khôi phục tài khoản người dùng bằng Active Directory Recycle Bin



Hình 3.3

Hướng dẫn chi tiết:

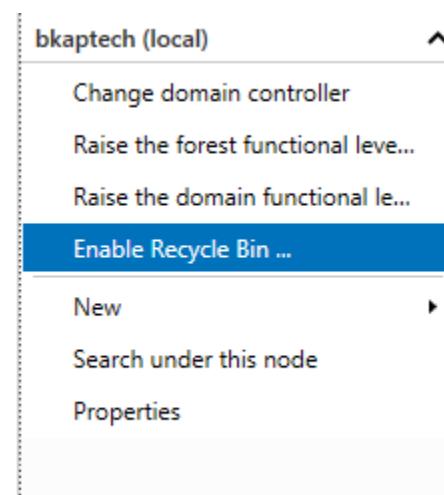
- Mở máy ảo *BKAP-DC12-01*, snapshot **Domain Controller**.
 - Vào **Server Manager**, **Tools**, vào dịch vụ **Active Directory Administrative Center**.



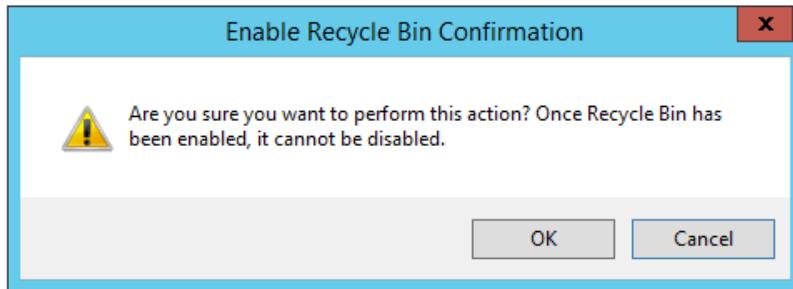
- Click vào *bkaptech (local)*.

Name	Type	Description
Builtin	builtinDom...	
Computers	Container	Default container for upgr...
Domain Controllers	Organizati...	Default container for dom...
ForeignSecurityPrincipals	Container	Default container for secur...

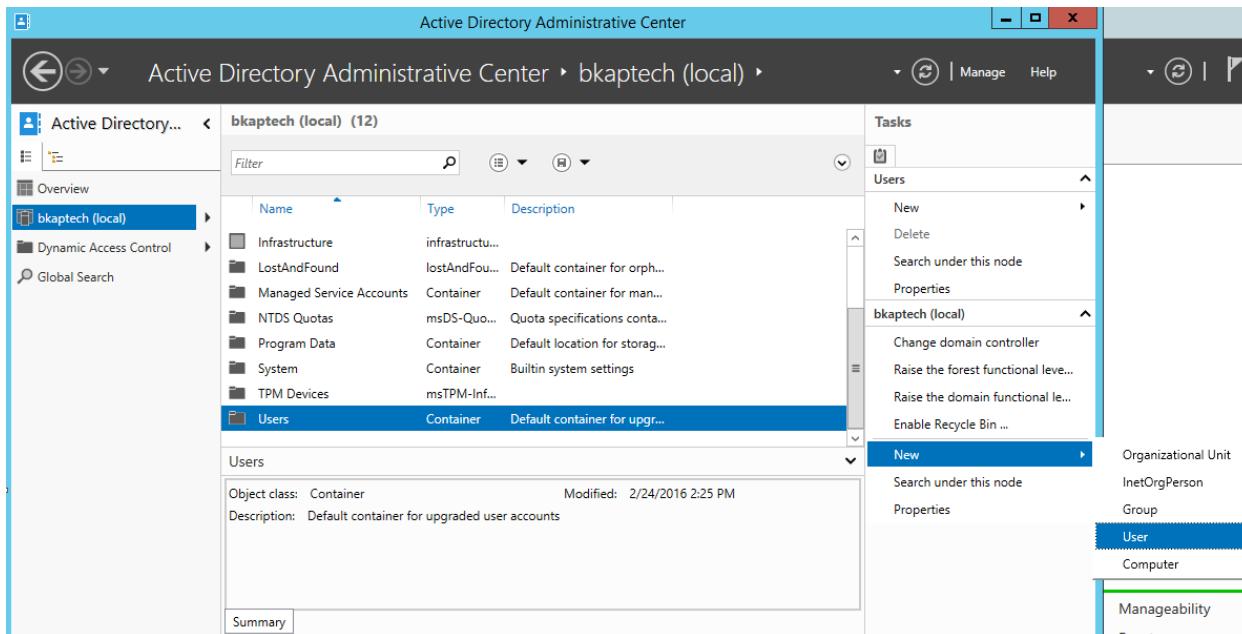
- Click vào **Enable Recycle Bin...**



- Tại cửa sổ **Enable Recycle Bin Confirmation**, click chọn vào **OK**.



- Tại cửa sổ **Active Directory Administrative Center**, click chọn vào **Users**, click vào **New** / chọn vào **User**. (*tạo User*).



▪ Tạo User hungnq.

Create User: Nguyen Quoc Hung

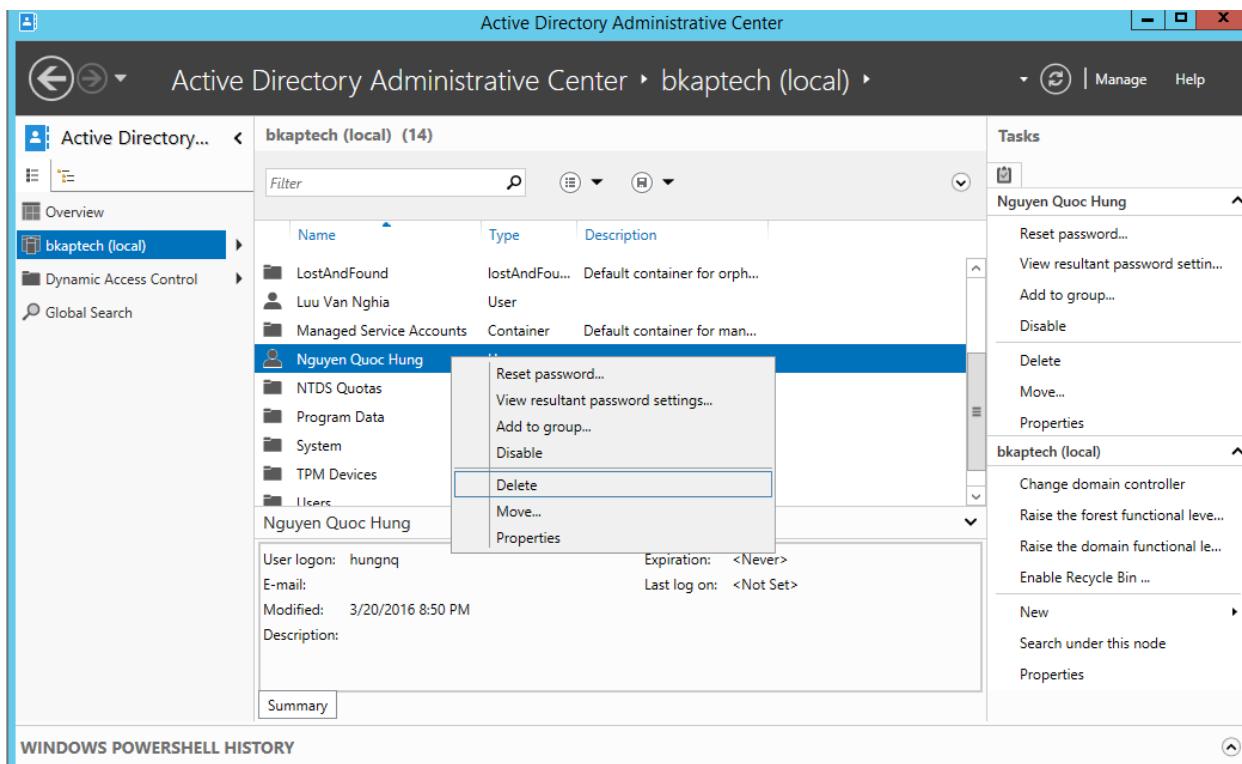
Account	Account <div style="float: right;"> ? X ^ </div> <div style="margin-top: 10px;"> Organization <div style="float: right;"> ? X ^ </div> </div> <div style="margin-top: 10px;"> Member Of </div> <div style="margin-top: 10px;"> Password Settings </div> <div style="margin-top: 10px;"> Profile </div>	
	<div style="border-bottom: 1px solid #ccc; padding-bottom: 5px;"> First name: Nguyen Quoc Middle initials: Last name: Hung Full name: * Nguyen Quoc Hung User UPN logon: hungnq @ bkaptech.vn User SamAccoun... bkaptech * hungnq </div> <div> Account expires: <input checked="" type="radio"/> Never <input type="radio"/> End of <input type="text"/> </div> <div> Password options: <input checked="" type="radio"/> User must change password at next log on <input type="radio"/> Other password options <div style="margin-left: 20px;"> <input type="checkbox"/> Smart card is required for interactive log... <input type="checkbox"/> Password never expires <input type="checkbox"/> User cannot change password </div> </div> <div> Encryption options: </div> <div> Other options: </div>	
	<div style="border-bottom: 1px solid #ccc; padding-bottom: 5px;"> Password: ***** Confirm password: ***** </div> <div style="margin-top: 5px;"> Create in: DC=kaptech,DC=vn Change... </div> <div style="margin-top: 5px;"> <input type="checkbox"/> Protect from accidental deletion </div> <div style="display: flex; justify-content: space-around; margin-top: 5px;"> Log on hours... Log on to... </div>	
	<div style="border-bottom: 1px solid #ccc; padding-bottom: 5px;"> Organization <div style="float: right;"> ? X ^ </div> </div> <div> Display name: Nguyen Quoc Hung Job title: Office: E-mail: Web page: </div> <div style="margin-top: 5px;"> Department: Company: Manager: Edit... Clear </div> <div style="text-align: center; margin-top: 5px;"> Other web pages... Direct reports: </div>	
More Information		
OK Cancel		

▪ Tạo User **nghialv**

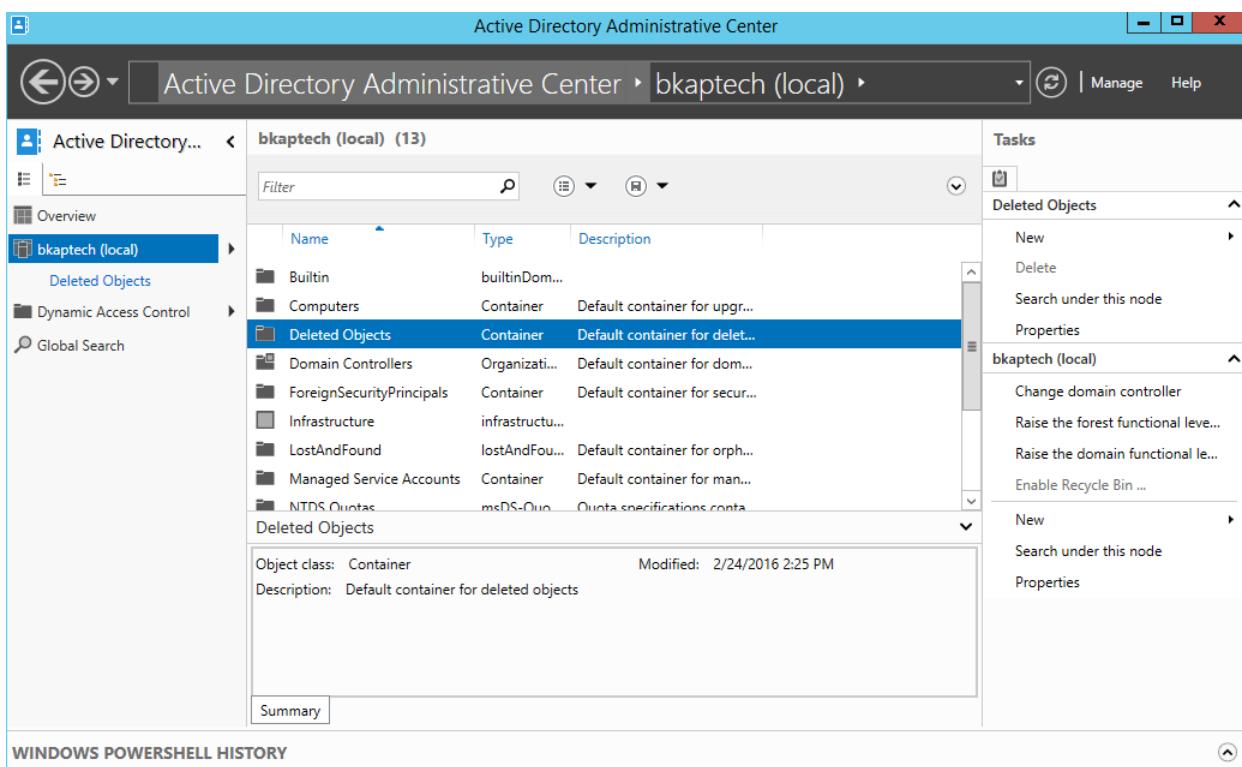
Create User: Luu Van Nghia

Account Organization Member Of Password Settings Profile	<div style="border-bottom: 1px solid #ccc; padding-bottom: 5px;"> Account </div> <div style="display: flex; justify-content: space-between;"> <div style="flex: 1;"> First name: <input type="text" value="Luu Van"/> Middle initials: <input type="text"/> Last name: <input type="text" value="Nghia"/> Full name: <input type="text" value="Luu Van Nghia"/> User UPN logon: <input type="text" value="nghialv"/> @ <input type="button" value="bkaptech.vn"/> User SamAccoun... <input type="text" value="bkaptech"/> * <input type="text" value="nghialv"/> Password: <input type="password" value="*****"/> Confirm password: <input type="password" value="*****"/> </div> <div style="flex: 1;"> Account expires: <input checked="" type="radio"/> Never <input type="radio"/> End of <input type="text"/> Password options: <input checked="" type="radio"/> User must change password at next log on <input type="radio"/> Other password options <input type="checkbox"/> Smart card is required for interactive log... <input type="checkbox"/> Password never expires <input type="checkbox"/> User cannot change password Encryption options: Other options: </div> </div> <div style="margin-top: 10px;"> Create in: DC=bkaptech,DC=vn Change... </div> <div style="display: flex; justify-content: space-around; margin-top: 5px;"> <input type="checkbox"/> Protect from accidental deletion </div> <div style="display: flex; justify-content: space-around; margin-top: 5px;"> Log on hours... Log on to... </div> <div style="border-bottom: 1px solid #ccc; padding-bottom: 5px;"> Organization </div> <div style="display: flex; justify-content: space-between;"> <div style="flex: 1;"> Display name: <input type="text" value="Luu Van Nghia"/> Office: <input type="text"/> E-mail: <input type="text"/> Web page: <input type="text"/> </div> <div style="flex: 1;"> Job title: <input type="text"/> Department: <input type="text"/> Company: <input type="text"/> Manager: <input type="button" value="Edit..."/> <input type="button" value="Clear"/> </div> </div> <div style="text-align: center; margin-top: 5px;"> Other web pages... Direct reports: Edit... Clear </div> <div style="margin-top: 10px;"> More Information </div> <div style="text-align: right; margin-top: 10px;"> <input type="button" value="OK"/> <input type="button" value="Cancel"/> </div>
--	--

- Thực hiện xóa tài khoản vừa tạo.



- Vào mục **Deleted Objects** để khôi phục tài khoản vừa xóa.



Active Directory Administrative Center

Deleted Objects (2)

Name	When Deleted	Last known pa...	Type	Description
Luu Van Nghia	3/20/2016 8:53...	DC=bkaptech,...	User	
Nguyen Quoc Hung			User	

Tasks

- 2 items selected
- Restore
- Restore To...

Deleted Objects

- New
- Delete
- Search under this node
- Properties

Summary

2 items selected

Organizational Units:
Users: 2
Groups:
Computers:

Contacts:
Password Settings:
Other Objects:

o Tài khoản đã được khôi phục.

Active Directory Administrative Center

bkaptech (local) (15)

Name	Type	Description
LostAndFound	lostAndFou...	Default container for orph...
Luu Van Nghia	User	
Managed Service Accounts	Container	Default container for man...
Nguyen Quoc Hung	User	
NTDS Quotas	msDS-Quo...	Quota specifications conta...
Program Data	Container	Default location for storag...
System	Container	Builtin system settings
TPM Devices	msTPM-Inf...	
Users	Container	Default container for user...

Nguyen Quoc Hung

User logon: hungnq Expiration: <Never>
E-mail: Last log on: <Not Set>
Modified: 3/20/2016 8:56 PM

Tasks

- Nguyen Quoc Hung
- Reset password...
- View resultant password settin...
- Add to group...
- Disable
- Delete
- Move...
- Properties

bkaptech (local)

- Change domain controller
- Raise the forest functional leve...
- Raise the domain functional le...
- Enable Recycle Bin ...
- New

BÀI 4:

CHÍNH SÁCH TÀI KHOẢN NGƯỜI DÙNG.

Các nội dung chính sẽ được đề cập:

- ✓ Cấu hình chính sách khóa tài khoản người dùng.
- ✓ Cấu hình chính sách Fine-grained Password cho từng phòng ban.

4.1 Cấu hình chính sách khóa tài khoản người dùng.

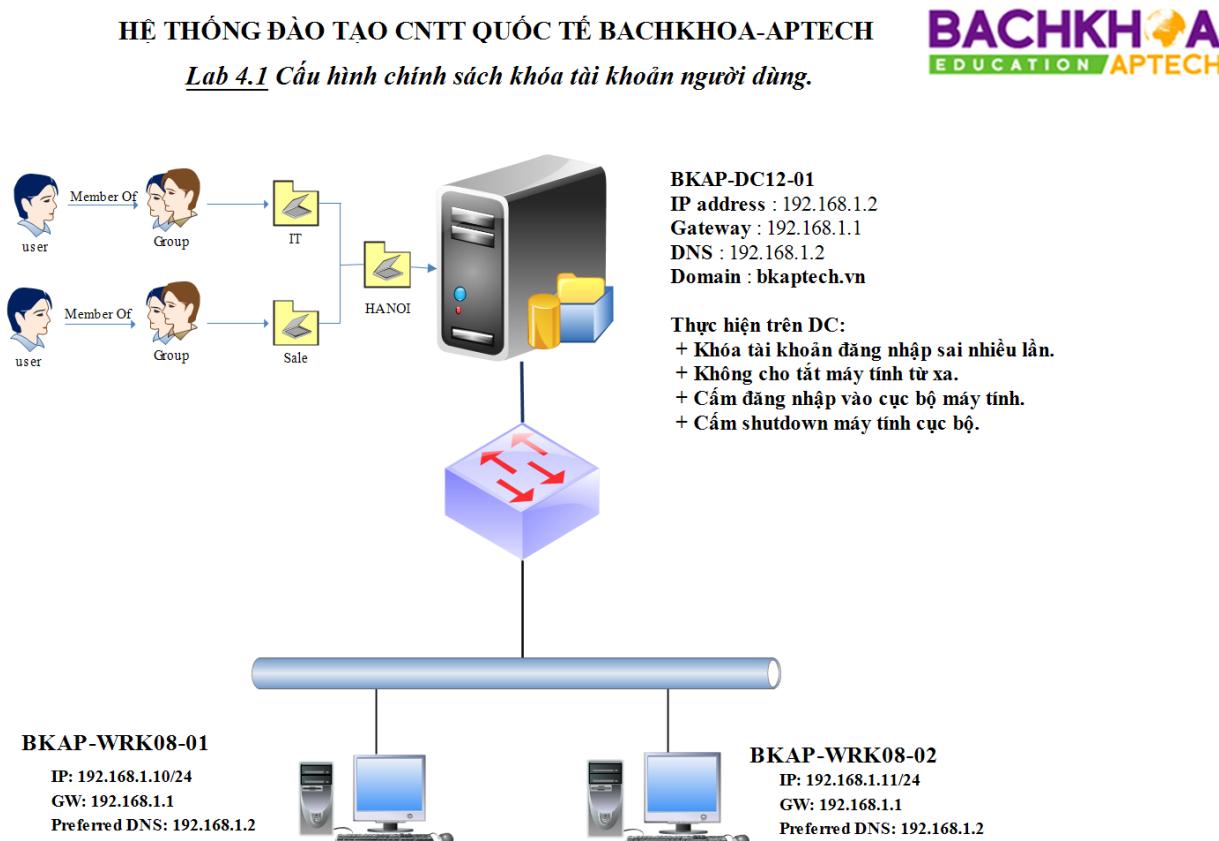
1. Yêu cầu bài Lab:

- + Khóa tài khoản đăng nhập sai nhiều lần.
- + Không cho tắt máy tính từ xa.
- + Cấm shutdown máy tính cục bộ.
- + Cấm đăng nhập cục bộ vào máy tính.

2. Yêu cầu chuẩn bị:

- + Chuẩn bị máy BKAP-DC12-01 làm Domain Controller quản lý miền **bkaptech.vn**.
- + Tạo OU tương ứng với phòng ban IT , Giám Đốc.
- + Triển khai các chính sách trên DC với tài khoản **hungnq** thuộc nhóm Server Operators.
- + Kiểm tra các chính sách khi áp dụng cho tài khoản **hungnq**.

3. Mô hình lab:



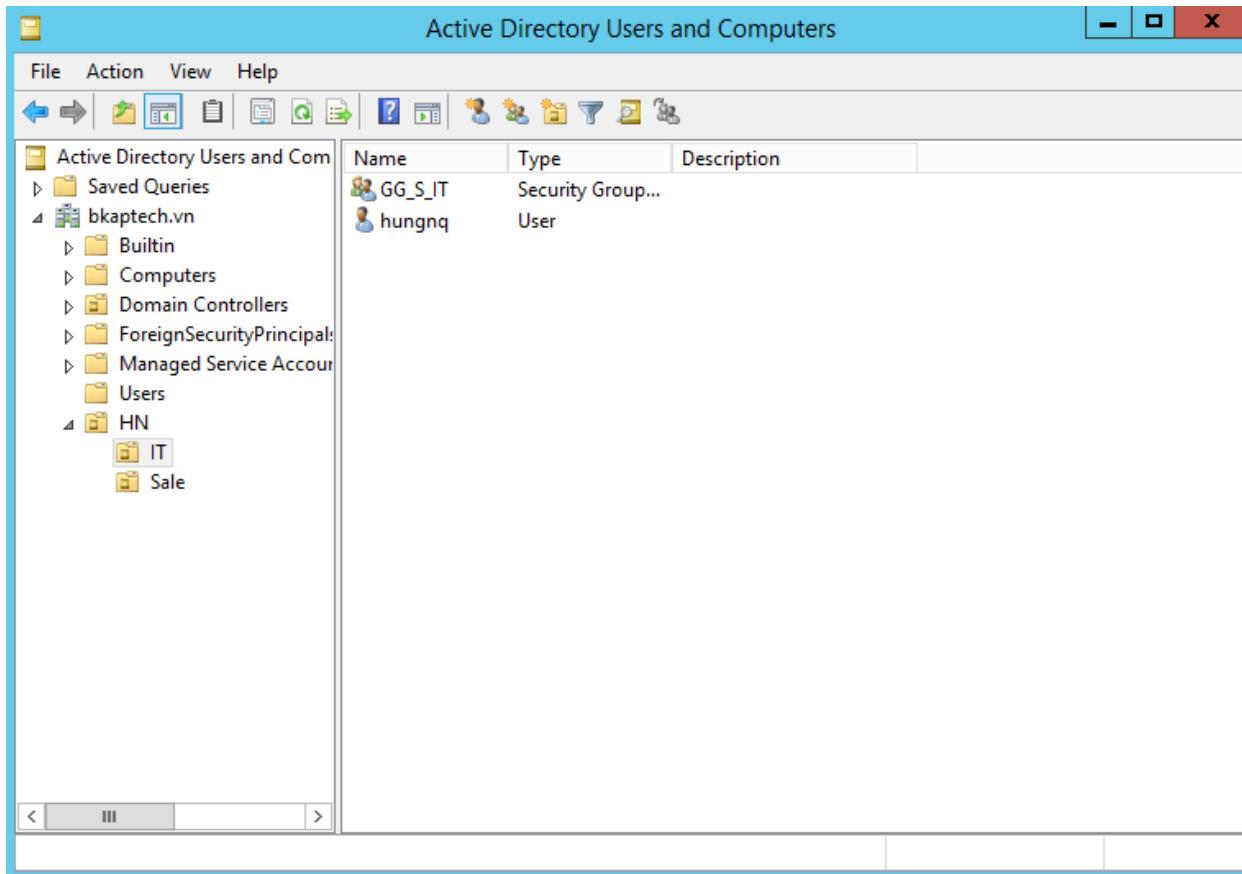
Hình 4.1

Sơ đồ địa chỉ như sau:

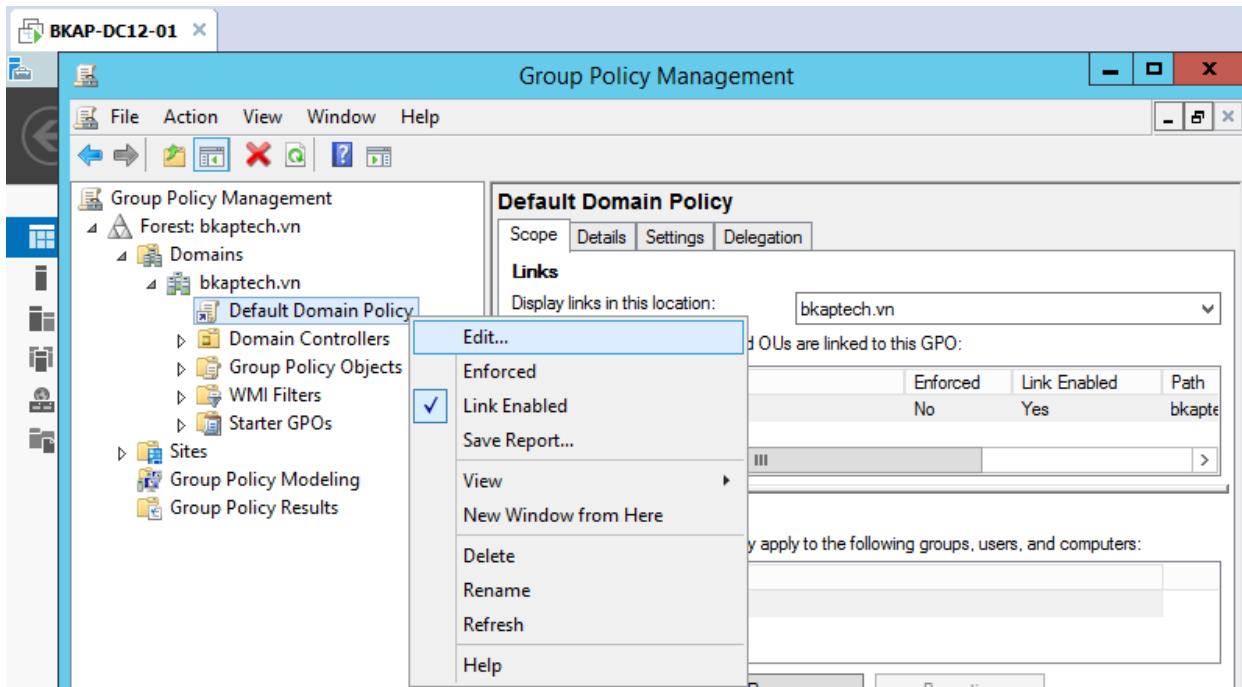
Thông số	BKAP-DC12-01	BKAP-WRK08-01
IP address	192.168.1.2	192.168.1.10
Gateway	192.168.1.1	192.168.1.1
Subnet Mask	255.255.255.0	255.255.255.0
DNS Server	192.168.1.2	192.168.1.2

Hướng dẫn chi tiết:

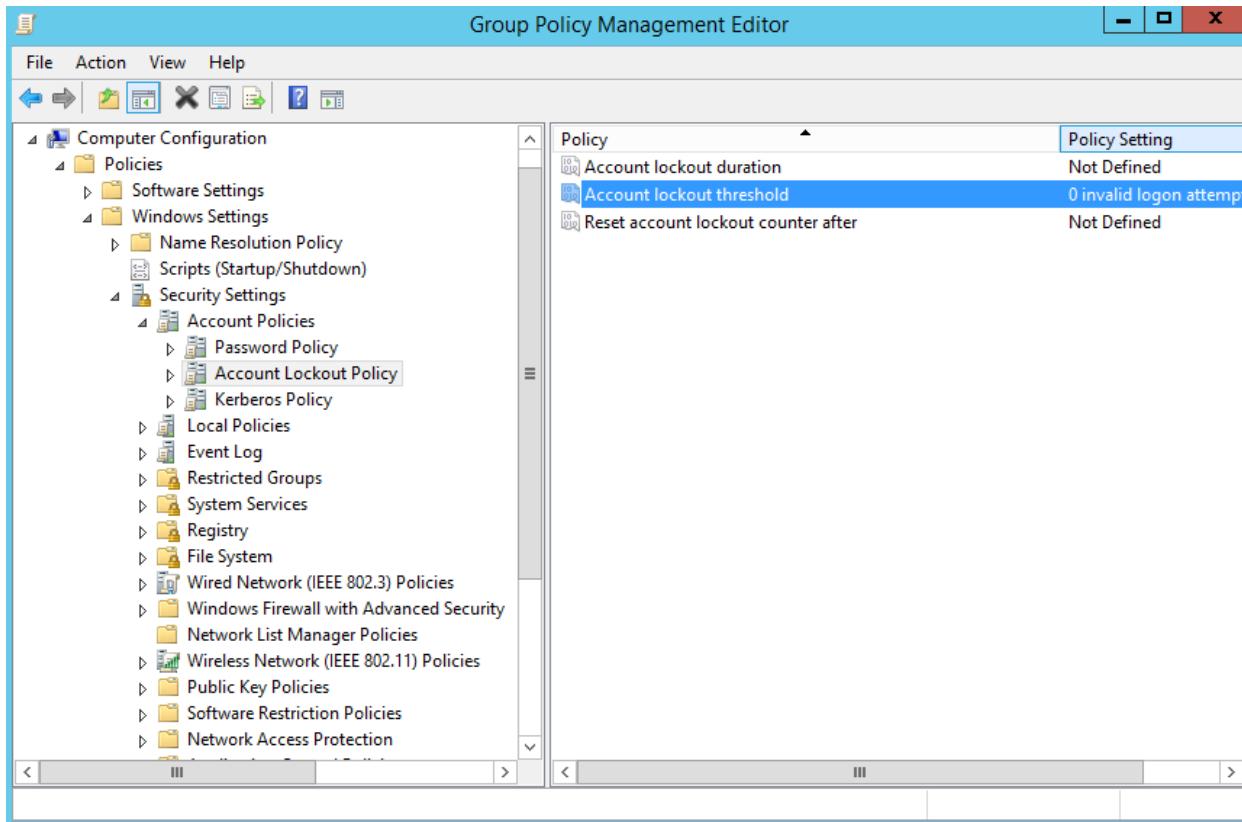
- Thực hiện trên máy BKAP-DC12-01 , tạo *OU, Group, User* như hình trên.



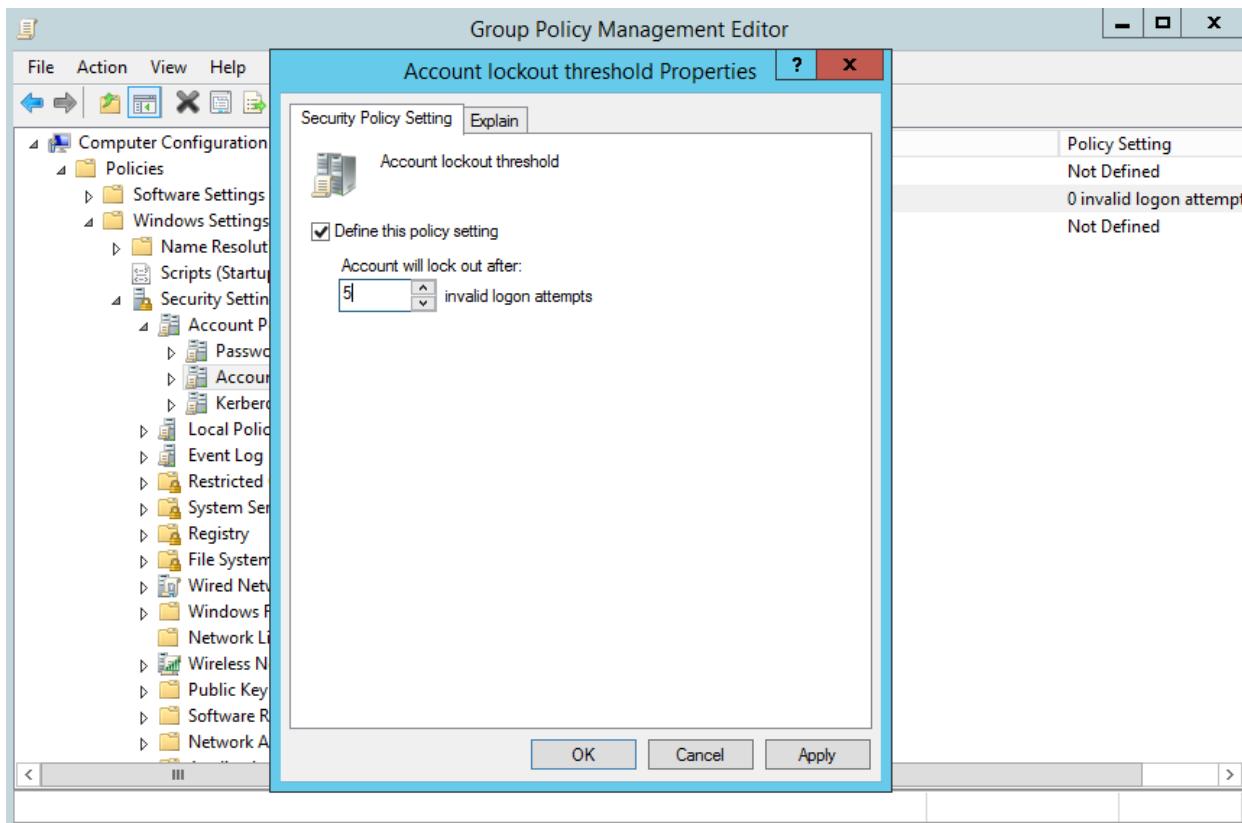
- Triển khai chính sách khóa tài khoản người dùng đăng nhập sai nhiều lần.
 - Vào **Group Policy Management**, click chuột phải vào Default Domain Policy, chọn Edit.



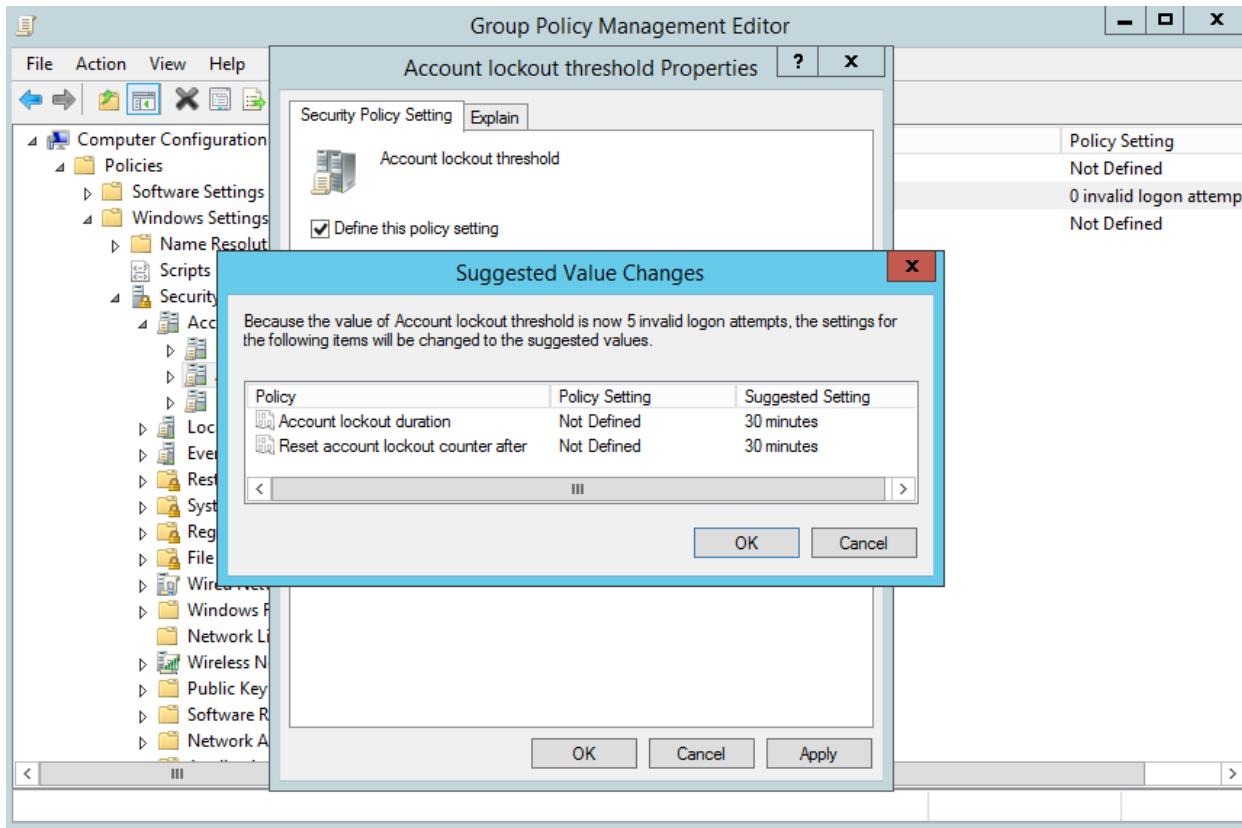
- Trong cửa sổ **Group Policy Management Editor**, chọn vào **Computer Configuration / Policies / Windows Settings / Security Settings / Account Policies / Account Lockout Policy** / chọn tiếp vào **Account lockout threshold**.



- Tại cửa sổ **Account lockout threshold Properties** , click chọn vào **Define this policy setting** , tại mục bên dưới , nhập vào **5 invalid logon attempts** (*đăng nhập sai 5 lần sẽ bị khóa*).



- Tại mục **Suggested Value Changes**, click vào **OK**.



- **Gpupdate /force.**

```

Administrator: C:\Windows\system32\cmd.exe

Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

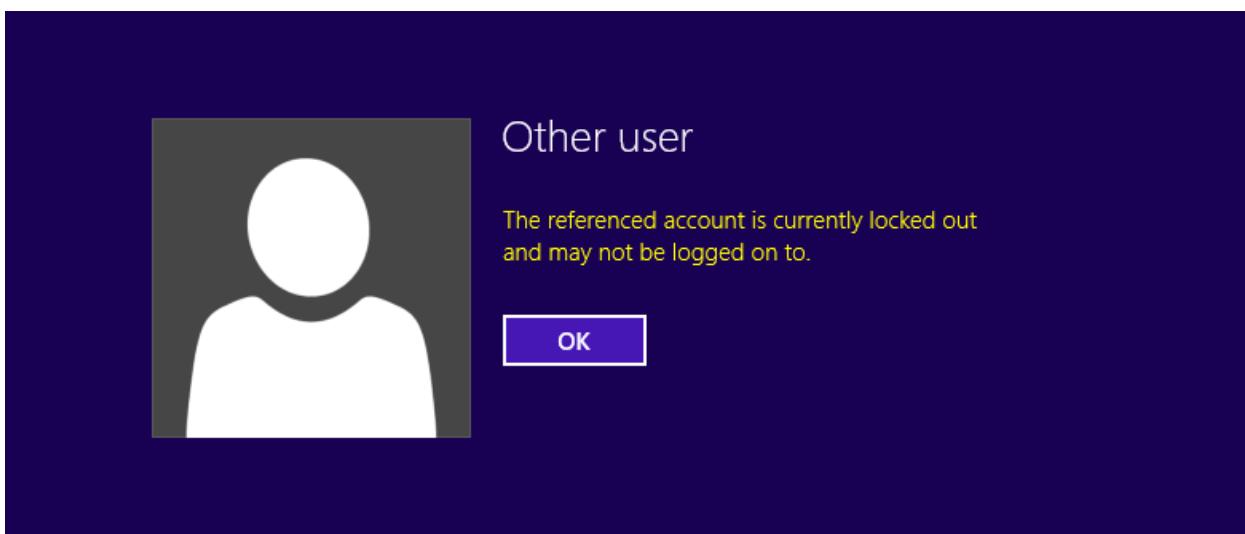
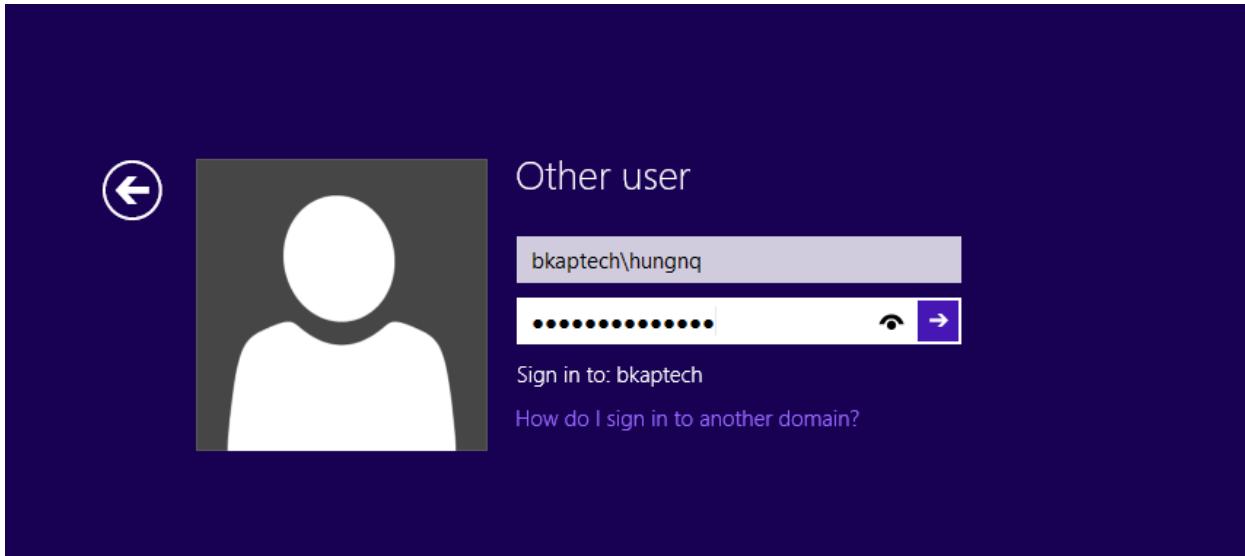
C:\Users\Administrator>gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.

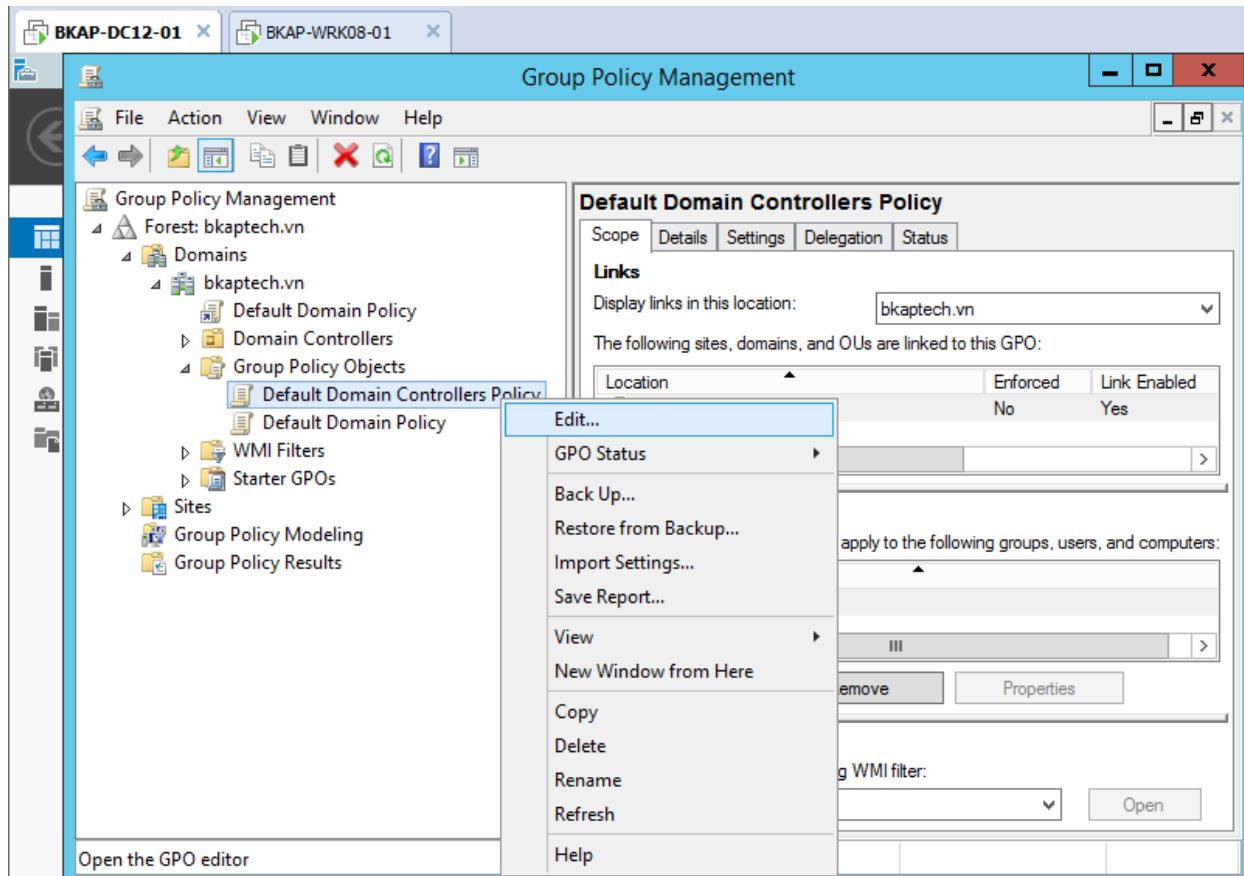
C:\Users\Administrator>_

```

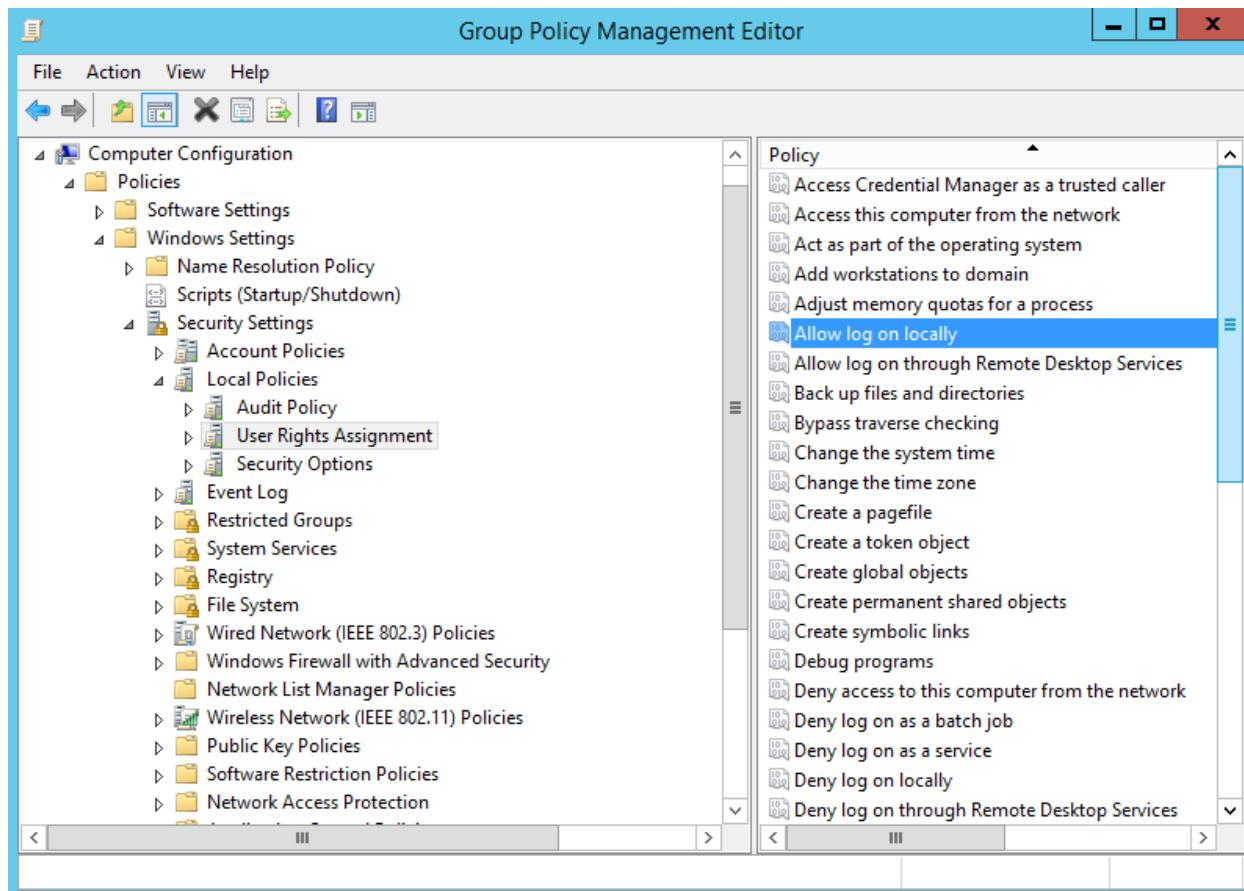
- Chuyển sang máy BKAP-WRK08-01 , Join vào Domain , đăng nhập bằng tài khoản **hungnq** để kiểm tra.
 - Thực hiện nhập vào password sai 5 lần để kiểm tra.



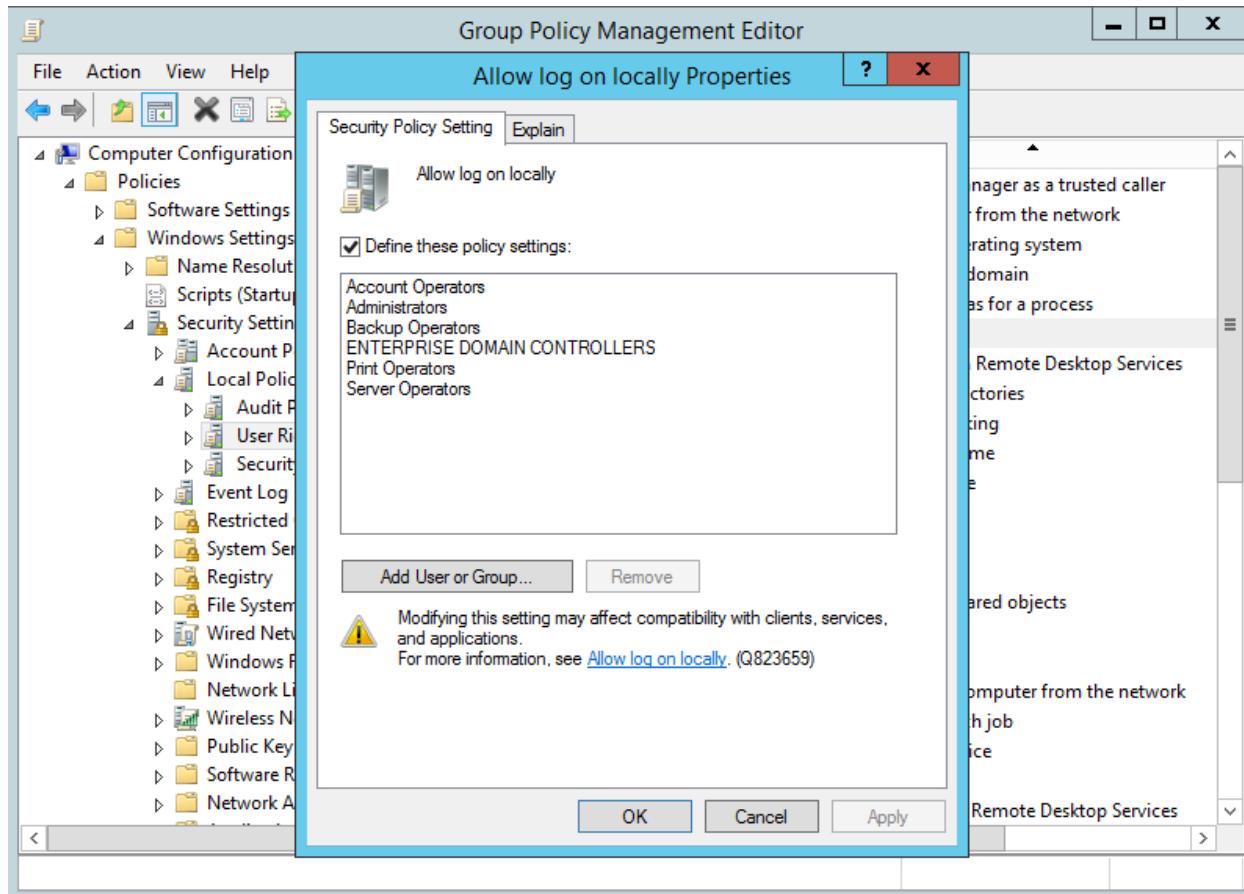
- Chuyển về máy BKAP-DC12-01:
 - Tại cửa sổ **Group Policy Management**, click chọn vào **Group Policy Objects / Default Domain Controllers Policy / Edit.**



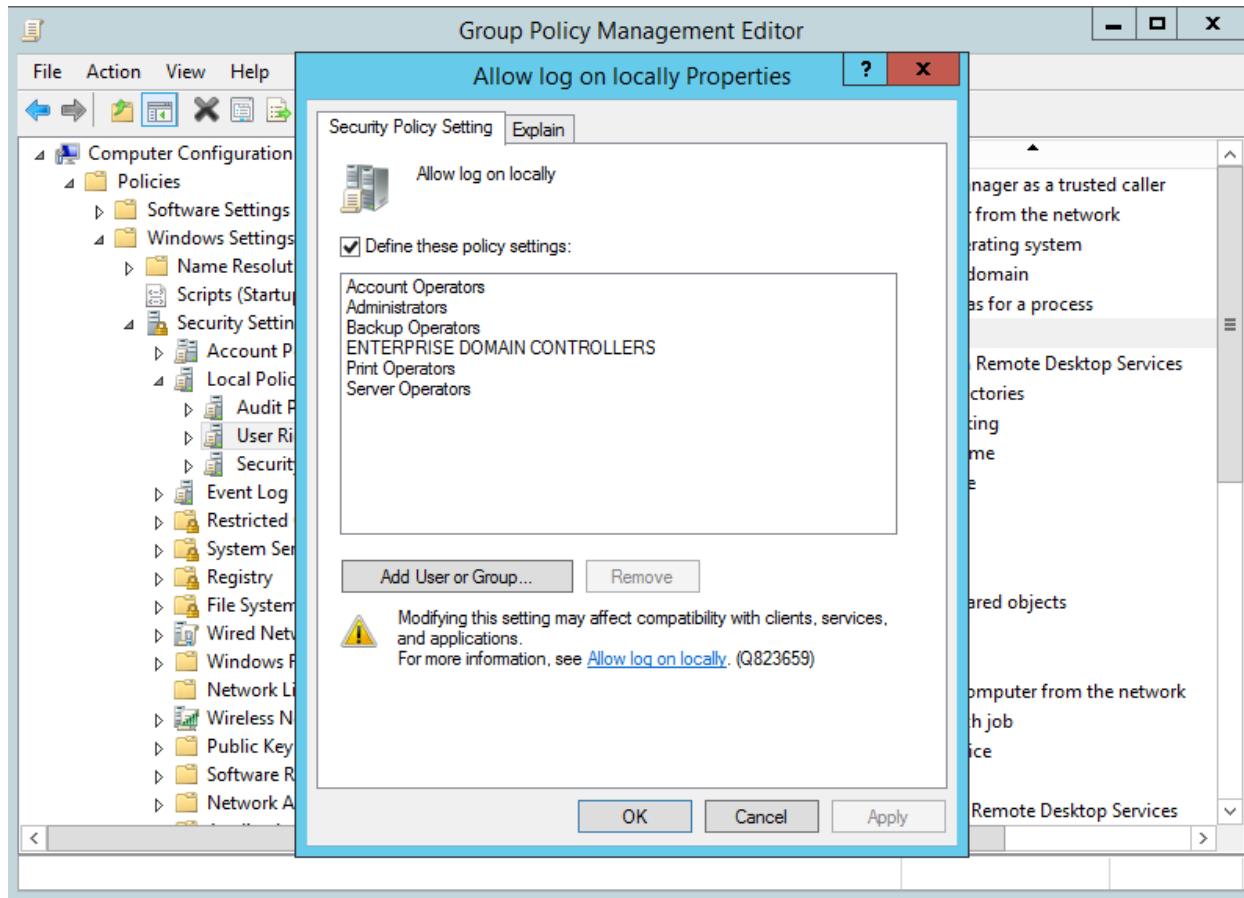
- Tại cửa sổ **Group Policy Management Editor**, click chọn vào **Computer Configuration / Policies / Windows Settings / Security Settings / Local Policies / User Rights Assignment** / chọn vào **Allow log on locally**. (*cho phép user được quyền đăng nhập trên máy BKAP-DC12-01*).

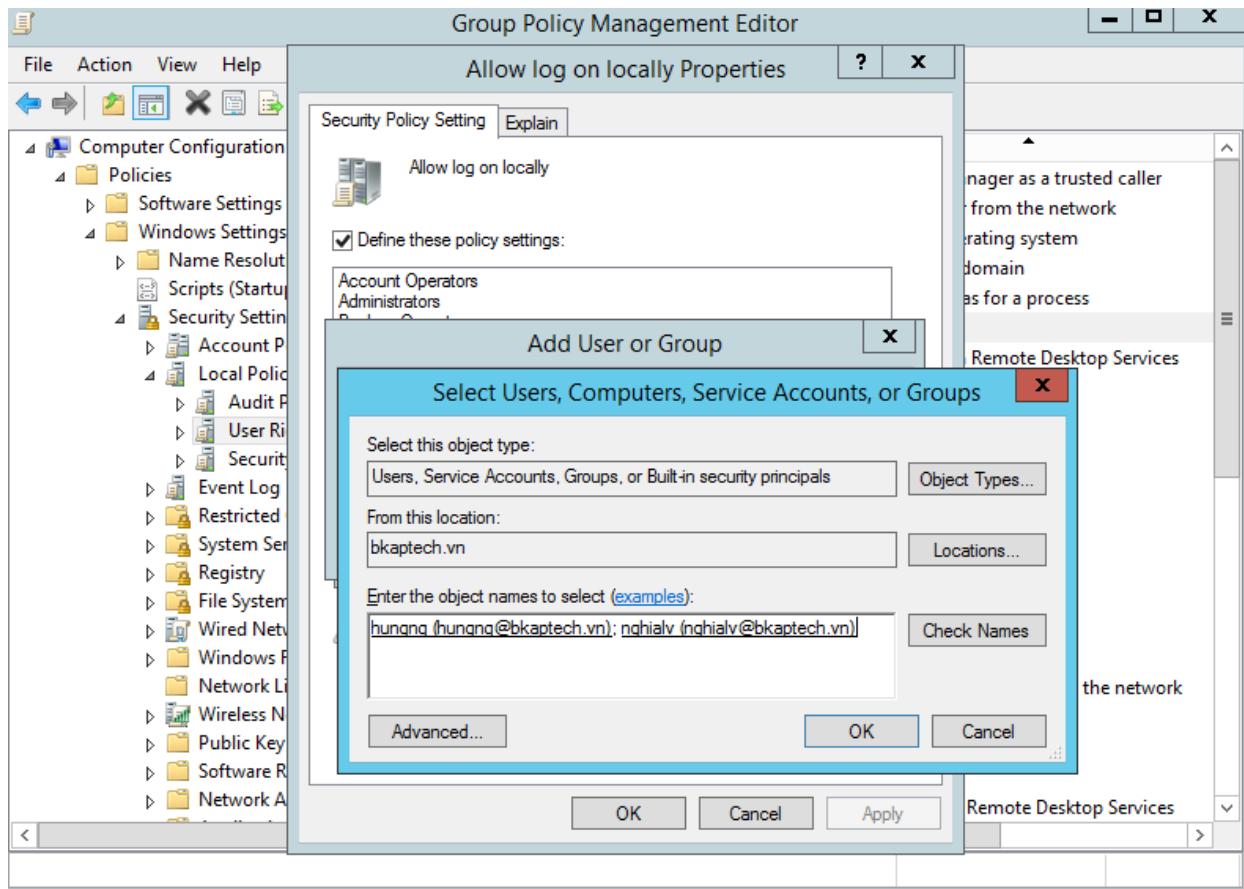


- Tại cửa sổ Allow log on locally properties , click vào Add User or Group...



- Thực hiện add vào 2 tài khoản **hungnq** và **nghialv**.





■ Gpupdate /force.

```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>gpupdate /force
Updating policy...

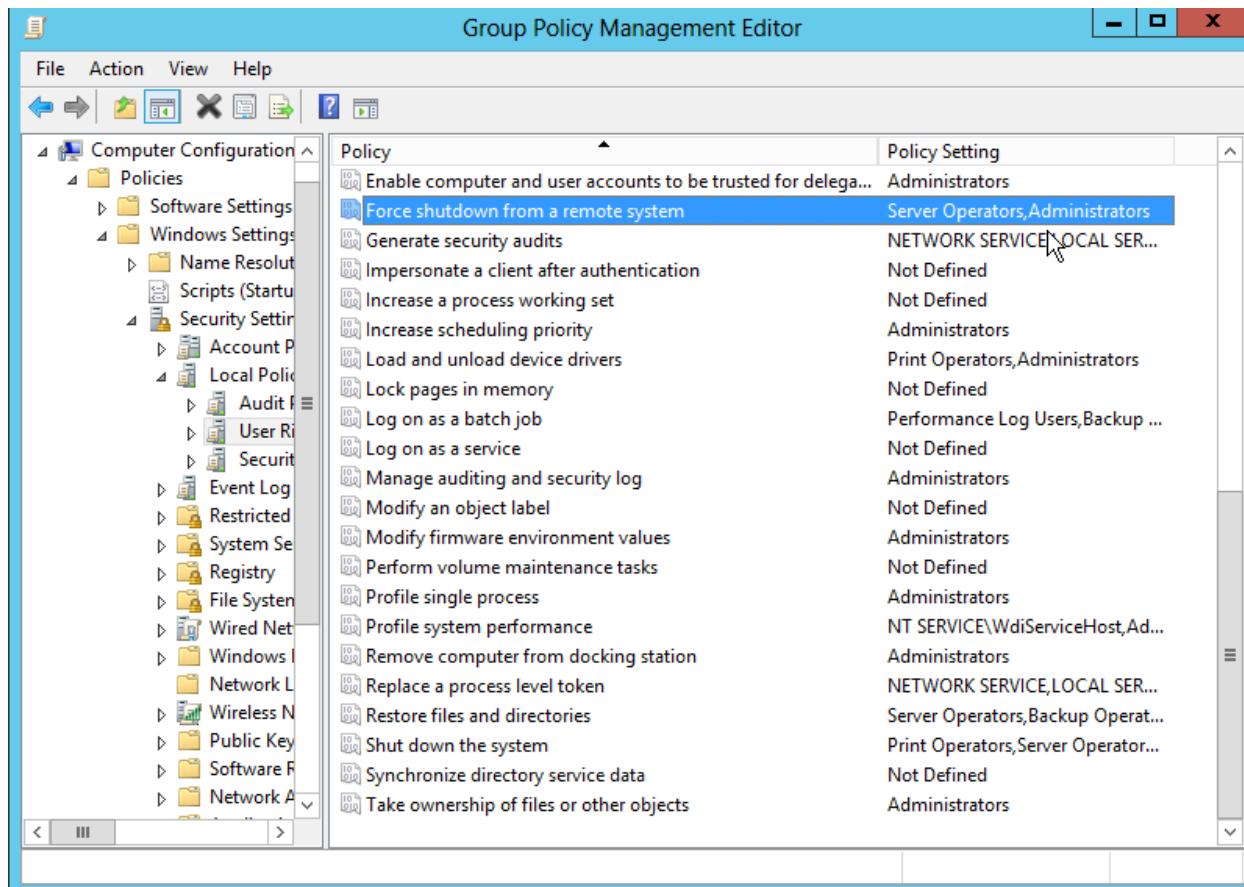
Computer Policy update has completed successfully.
User Policy update has completed successfully.

C:\Users\Administrator>gpupdate /force
Updating policy...

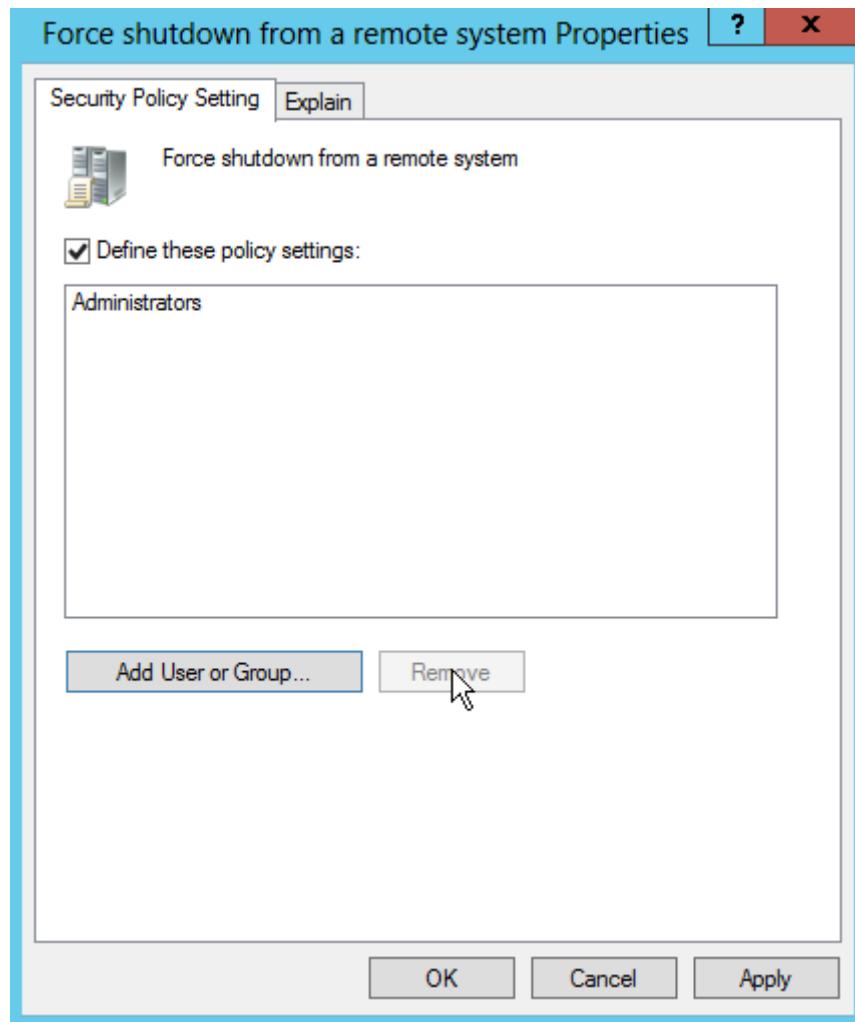
Computer Policy update has completed successfully.
User Policy update has completed successfully.

C:\Users\Administrator>
```

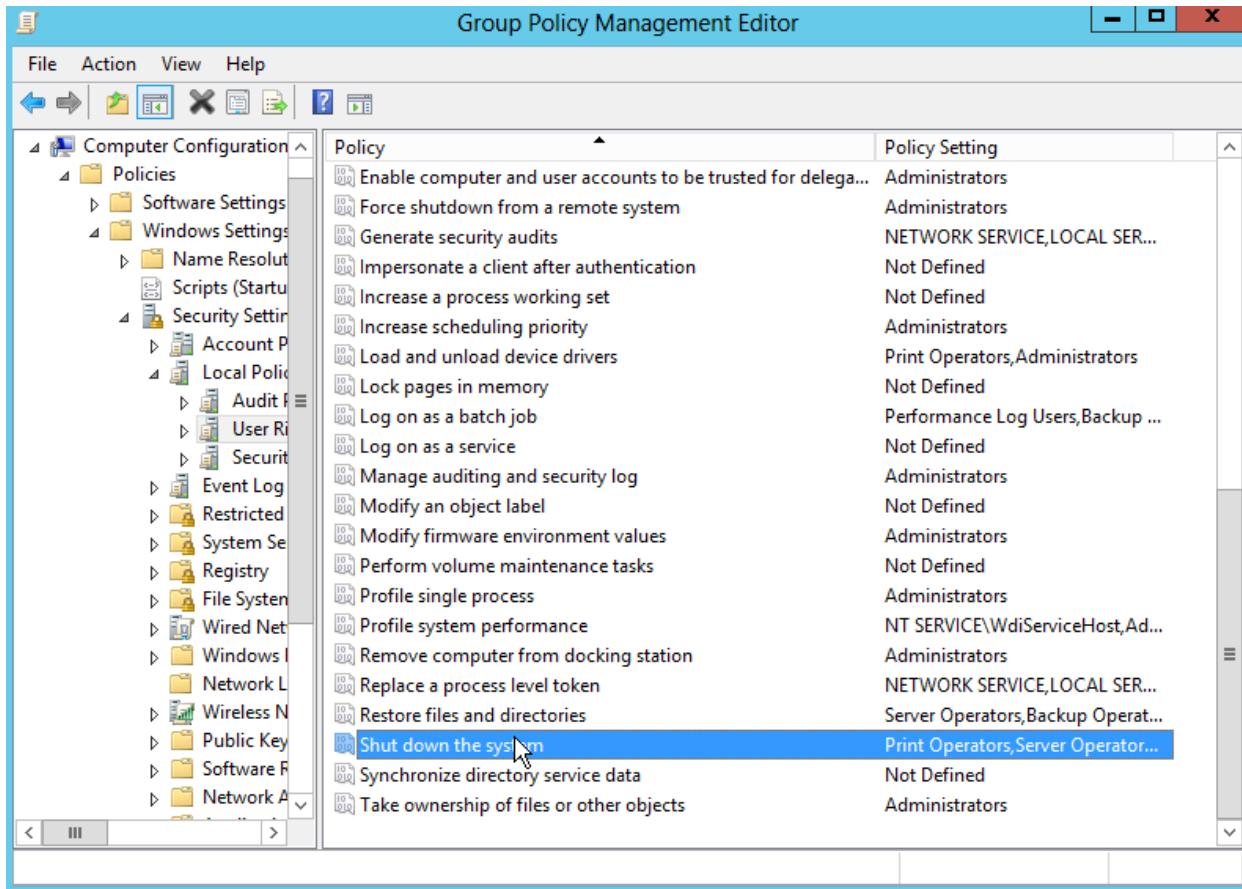
- Tại Computer Configuration / Policies / Windows Settings / Security Settings / Local Policies / User Rights Assignment / chọn vào Force shutdown from a remote system.



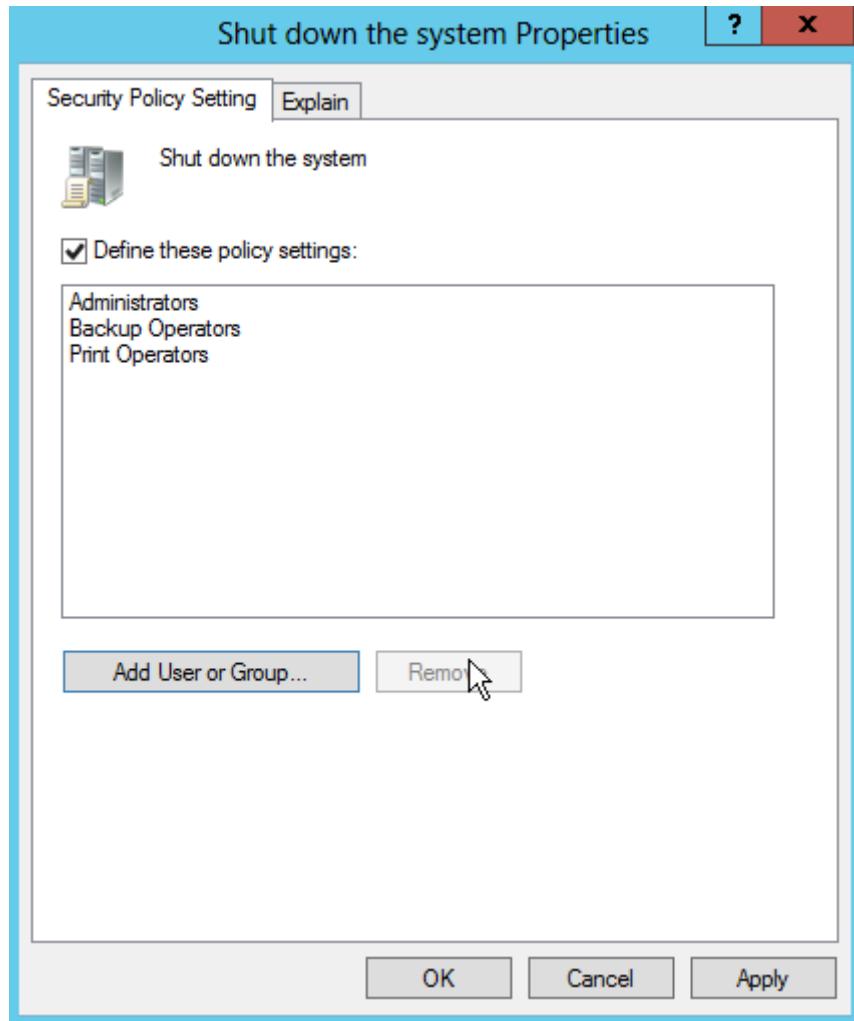
- Thực hiện Remove Server Operators. => Apply / OK.



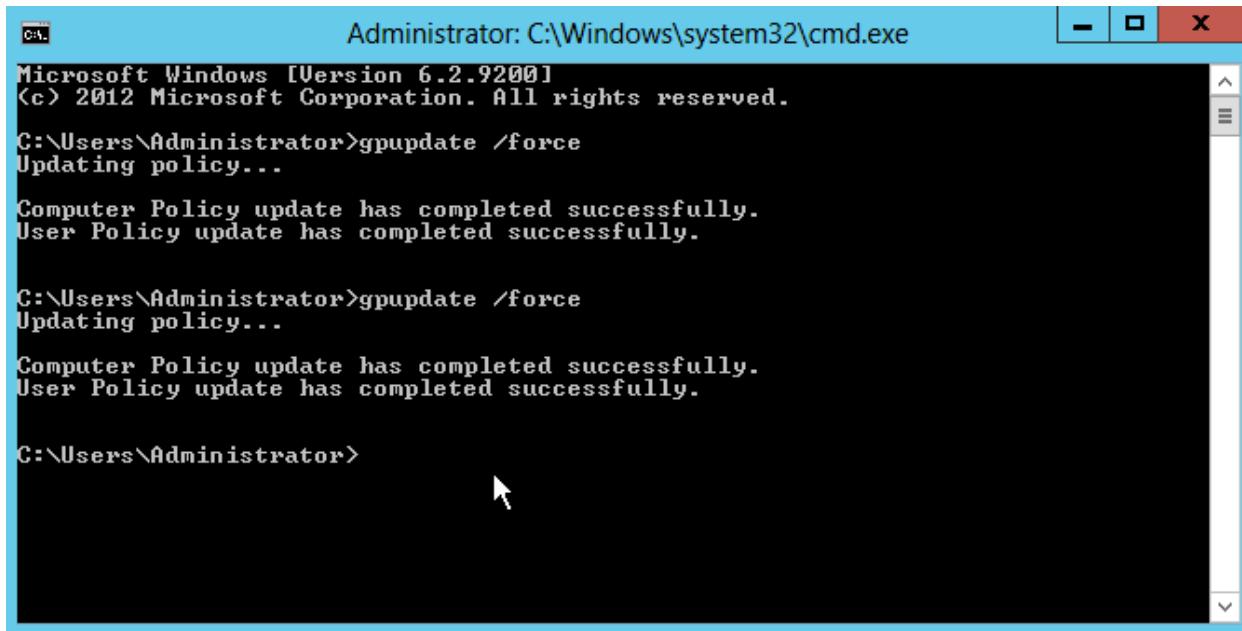
- Thực hiện chính sách cấm shutdown máy tính cục bộ:
 - Chọn vào **Shutdown the system**.



- Trong cửa sổ **Shut down the system Properties**, thực hiện **remove Server Operators** khỏi chính sách.



▪ Gpupdate /force



```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>gpupdate /force
Updating policy...

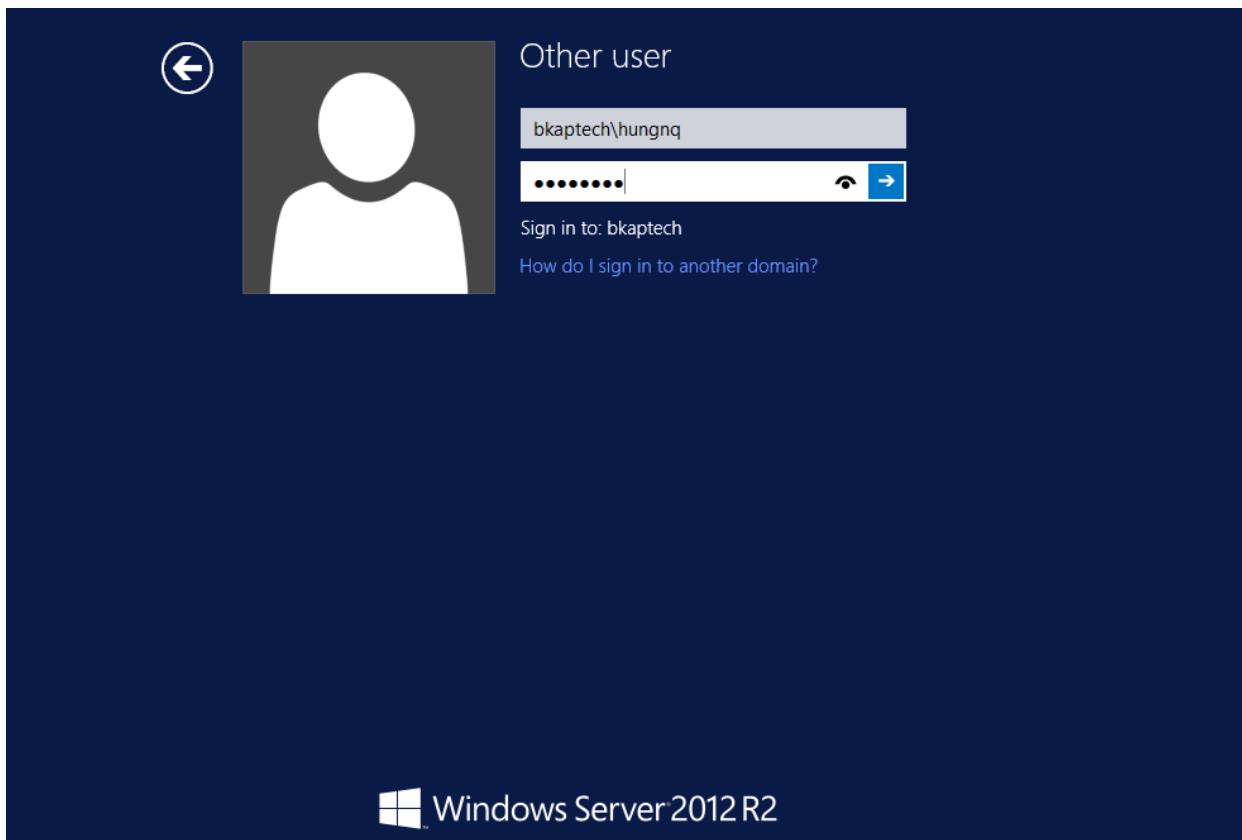
Computer Policy update has completed successfully.
User Policy update has completed successfully.

C:\Users\Administrator>gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.

C:\Users\Administrator>
```

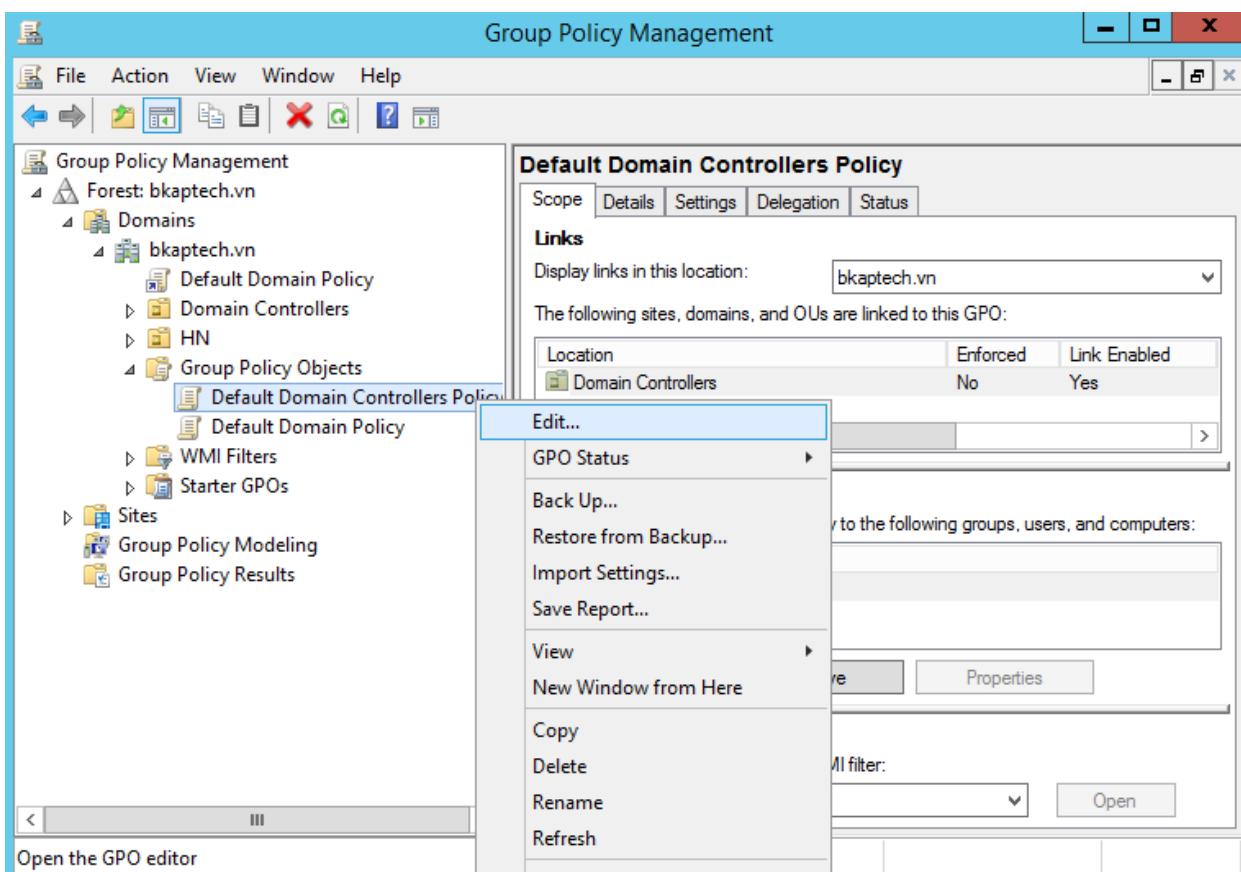
- Kiểm tra đăng nhập bằng tài khoản **hungnq** trên máy **BKAP-DC12-01**.



- Tài khoản **hungnq** đăng nhập thành công trên máy **BKAP-DC12-01**.



- Thực hiện chính sách *cấm đăng nhập cục bộ vào máy tính*.
 - Đăng nhập lại bằng tài khoản **bkaptech\administrator**.
 - Vào **Group Policy Management / Group policy Objects / Default Domain Controllers / Edit**.

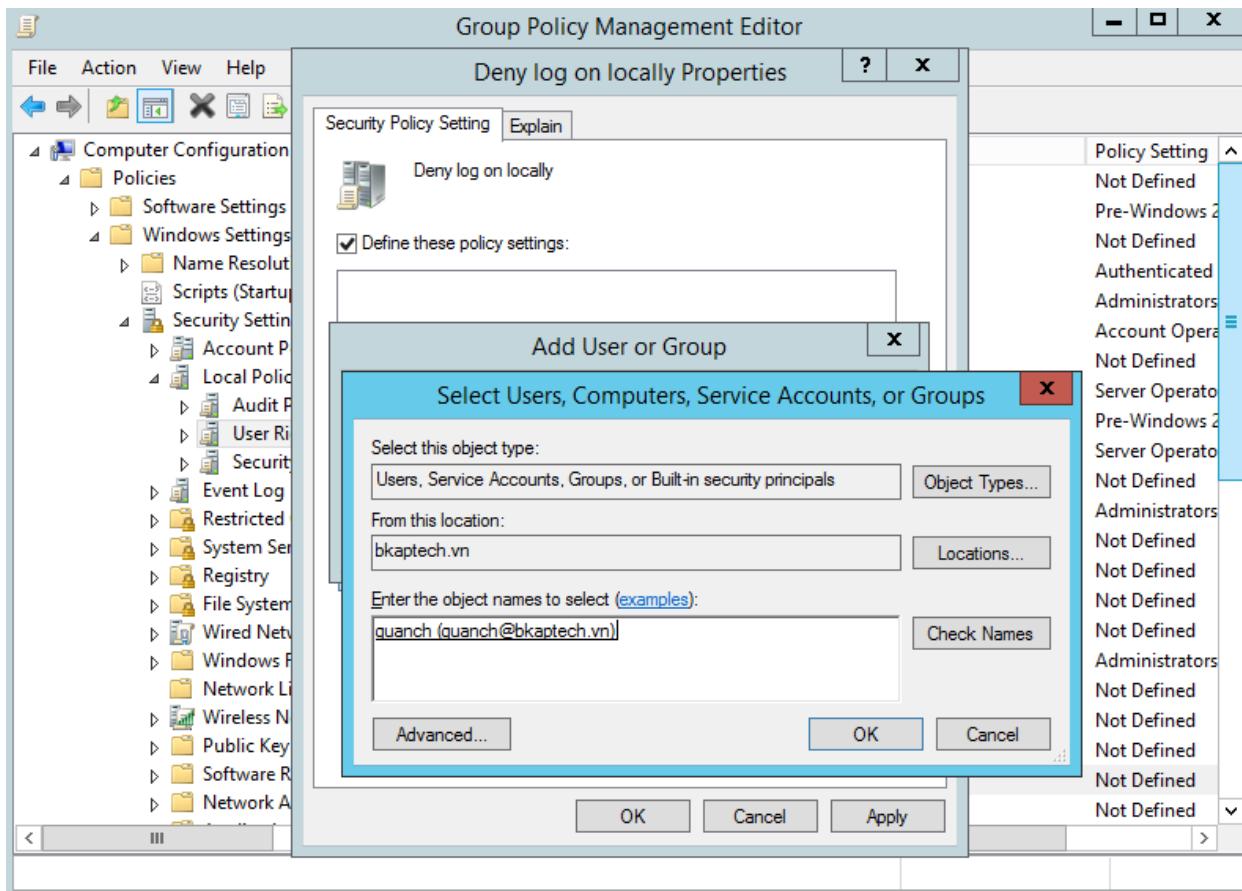


- Chọn vào **Deny log on locally**.

Group Policy Management Editor

Policy	Policy Setting
Access Credential Manager as a trusted caller	Not Defined
Access this computer from the network	Pre-Windows 2
Act as part of the operating system	Not Defined
Add workstations to domain	Authenticated
Adjust memory quotas for a process	Administrators
Allow log on locally	Account Opera
Allow log on through Remote Desktop Services	Not Defined
Back up files and directories	Server Operato
Bypass traverse checking	Pre-Windows 2
Change the system time	Server Operato
Change the time zone	Not Defined
Create a pagefile	Administrators
Create a token object	Not Defined
Create global objects	Not Defined
Create permanent shared objects	Not Defined
Create symbolic links	Not Defined
Debug programs	Administrators
Deny access to this computer from the network	Not Defined
Deny log on as a batch job	Not Defined
Deny log on as a service	Not Defined
Deny log on locally	Not Defined
Deny log on through Remote Desktop Services	Not Defined

- Add vào tài khoản **quanch** (*cấm user này đăng nhập cục bộ*).



- **Gpupdate /force**

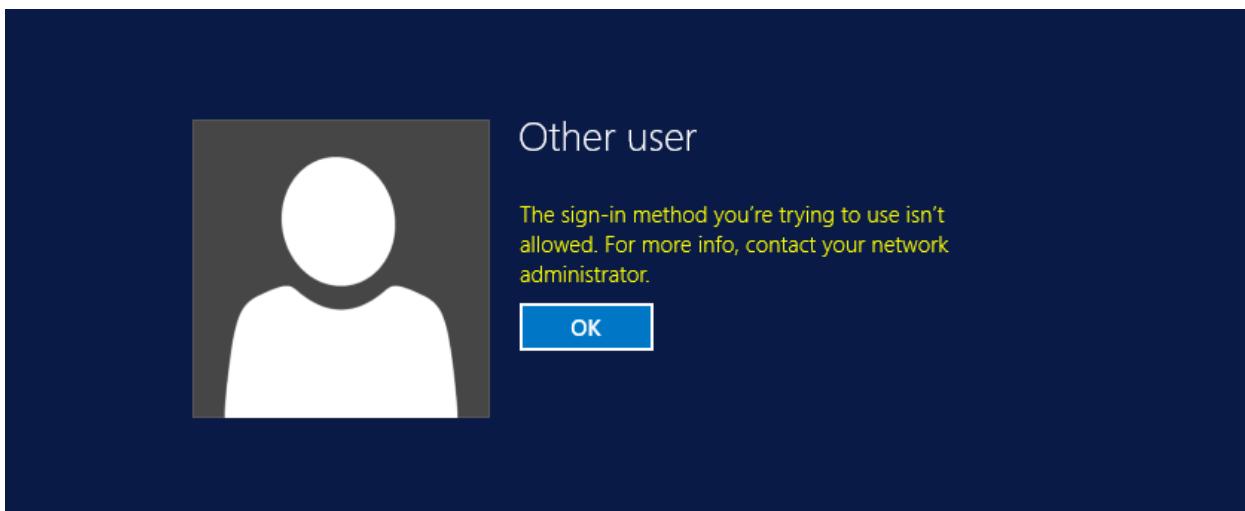
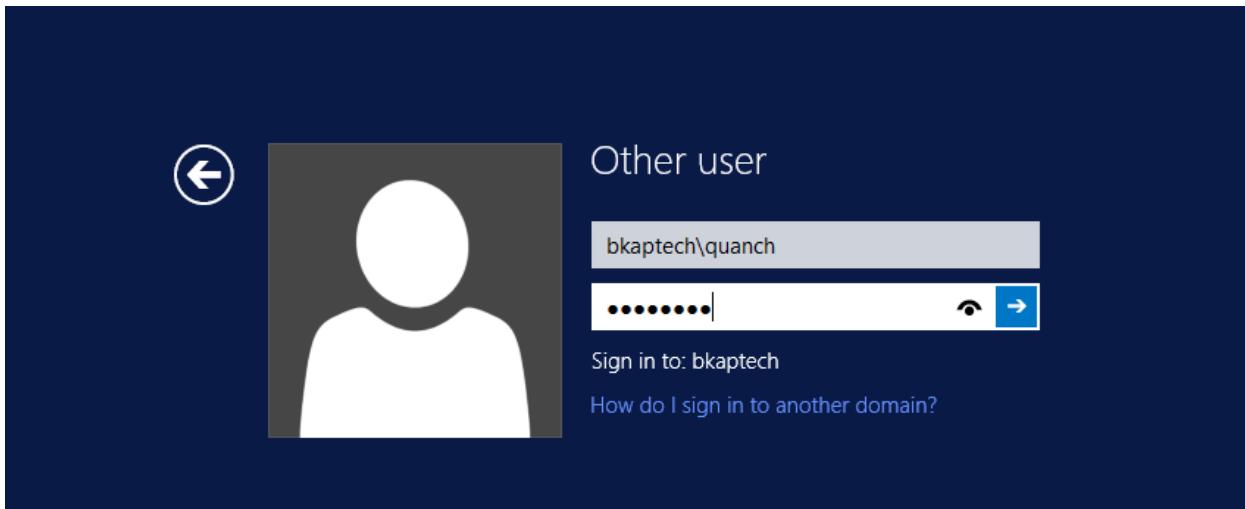
```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.

C:\Users\Administrator>
```

- Kiểm tra đăng nhập tài khoản **quanch** trên máy **BKAP-DC12-01**.



4.2 Cấu hình chính sách “Fine-grained Password” cho từng phòng ban.

1. Yêu cầu bài Lab:

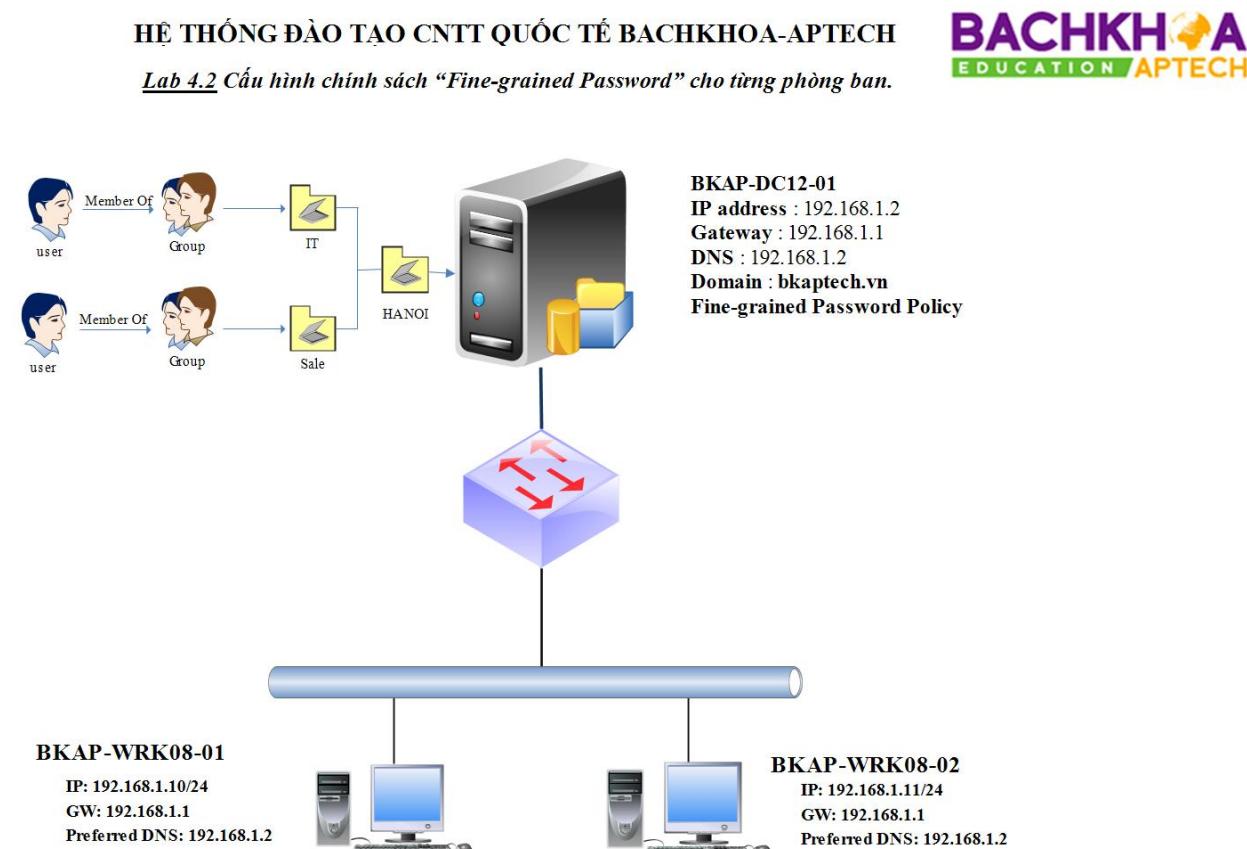
+ Trên máy **BKAP-DC12-01 (Domain Controller)** cần thực hiện:

- Tạo các user thuộc phòng ban *IT*, *Sale*, *Giam Doc*.
- Tạo 1 PSO (Password Settings Object).
- Áp dụng PSO lên user hoặc group (không áp dụng trực tiếp lên OU).

2. Yêu cầu chuẩn bị:

+ Chuẩn bị máy **BKAP-DC12-01** làm **Domain Controller** quản lý miền **bkaptech.vn**.

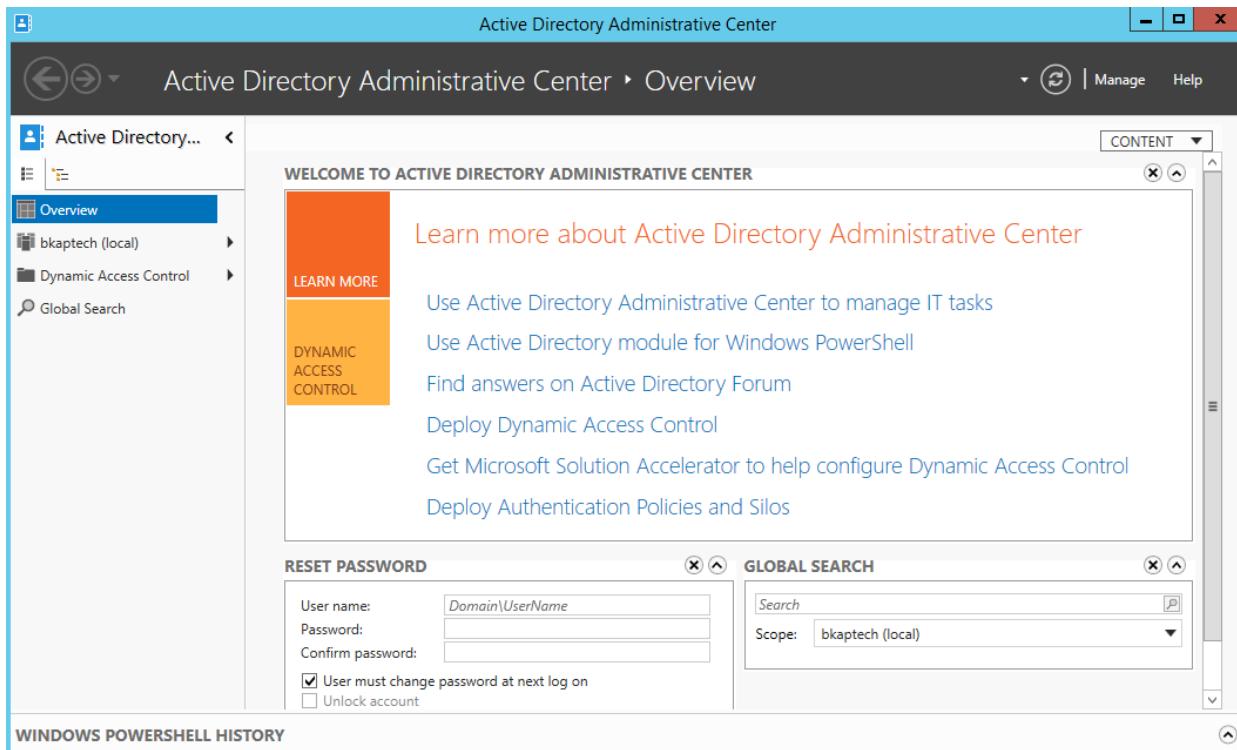
3. Mô hình Lab:



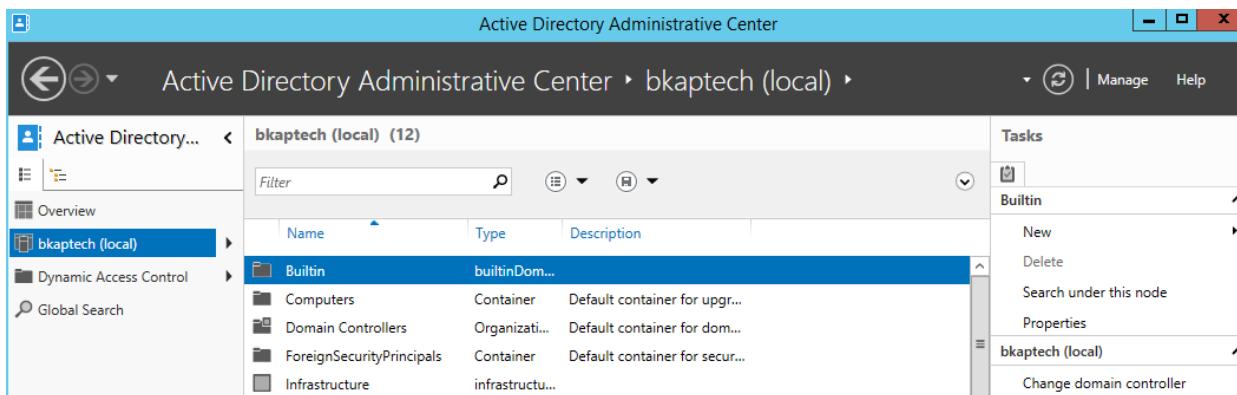
Hình 4.2

Hướng dẫn chi tiết:

- Trên máy BKAP-DC12-01 vào Tools mở **Active Directory Administrative Center**.



- Tạo các Group User :
 - Click chọn vào **bkaptech (local)**.



- `Click chọn vào **Users**.

Active Directory Administrative Center

bkaptech (local) (12)

	Name	Type	Description
Domain Controllers	Organizational Unit	Default container for domain controllers	
ForeignSecurityPrincipals	Container	Default container for security principals	
Infrastructure	Container	Default container for infrastructure objects	
LostAndFound	Container	Default container for orphaned objects	
Managed Service Accounts	Container	Default container for managed service accounts	
NTDS Quotas	msDS-Quota	Quota specifications container	
Program Data	Container	Default location for storage of application data	
System	Container	Builtin system settings	
TPM Devices	msTPM-Inf	Container for TPM devices	
Users	Container	Default container for upgraded user accounts	

Object class: Container Modified: 2/24/2016 2:25 PM
Description: Default container for upgraded user accounts

Summary

- Click vào **New / Group**.

Active Directory Administrative Center

bkaptech (local) > Users

	Name	Type	Description
Administrator	User	Built-in account for administrators	
Allowed RODC Password...	Group	Members of this group can...	
Cert Publishers	Group	Members of this group are...	
Cloneable Domain Control...	Group	Members of this group th...	
Denied RODC Password R...	Group	Members in this group ca...	
DnsAdmins	Group	DNS Administrators Group	
DnsUpdateProxy	Group	DNS clients who are perm...	
Domain Admins	Group	Designated administrators...	
Domain Computers	Group	All workstations and serve...	
Domain Controllers	Group	All domain controllers in t...	

Administrator

User logon: Administrator Expiration: <Never>
E-mail: Last log on: 2/24/2016 2:28 PM

Tasks

- Administrator
- Reset password...
- View resultant password settings...
- Add to group...
- Disable
- Delete
- Move...
- Properties

Users

- New
 - InetOrgPerson
 - Group**
 - User
 - Computer
- Delete
- Search under this node
- Properties

▪ Nhập vào tên để tạo Group : IT

Create Group: IT

Group

Managed By

Member Of

Members

Password Settings

Group name: * IT
Group (SamAccountName): * IT

Group type: Security Distribution

Group scope: Domain local Global Universal

Protect from accidental deletion

E-mail: Create in: CN=Users,DC=bkaptech,DC=vn Change... Description: Notes: Notes:

Managed by: Manager can update membership list: Edit... Clear Office: Address: Street: Main: City: State/Province: Zip/Postal code: Mobile: Fax: Country/Region:

More Information OK Cancel

▪ Tạo Group Sale:

Create Group: Sale

Group

Managed By

Member Of

Members

Password Settings

Group name: * Sale
Group (SamAccountName): * Sale

Group type: Security Distribution

Group scope: Domain local Global Universal

Protect from accidental deletion

E-mail: Create in: CN=Users,DC=bkaptech,DC=vn Change... Description: Notes: Notes:

Managed by: Manager can update membership list: Edit... Clear Office: Address: Street: Main: City: State/Province: Zip/Postal code: Mobile: Fax: Country/Region:

More Information OK Cancel

▪ Tạo Group Giam Doc:

Create Group: Giam Doc

Group	Group Group name: <input type="text" value="Giam Doc"/> E-mail: Group (SamAccountName): <input type="text" value="Giam Doc"/> Create in: CN=Users,DC=bkaptech,DC=vn Change... Description: Notes: <input type="checkbox"/> Protect from accidental deletion
Managed By	Managed By Managed by: <input type="checkbox"/> Manager can update membership list Phone numbers: Main: <input type="text"/> Mobile: <input type="text"/> Fax: <input type="text"/> Address: <input type="text"/> City: <input type="text"/> State/Province: <input type="text"/> Zip/Postal code: <input type="text"/> Country/Region: <input type="text"/>
Members	Member Of <input type="text"/>
Password Settings	

OK Cancel

▪ Tạo User hungnq:

Create User: Nguyen Quoc Hung

Account	Account First name: <input type="text" value="Nguyen Quoc"/> Middle initials: <input type="text"/> Last name: <input type="text" value="Hung"/> Full name: <input type="text" value="Nguyen Quoc Hung"/> User UPN logon: <input type="text" value="hungnq"/> @ <input type="text" value="bkaptech.vn"/> User SamAccountName: <input type="text" value="bkaptech"/> \ <input type="text" value="hungnq"/> Password: <input type="text" value="*****"/> Confirm password: <input type="text" value="*****"/> Create in: CN=Users,DC=bkaptech,DC=vn Change... <input type="checkbox"/> Protect from accidental deletion Log on hours... Log on to...	Account expires: <input checked="" type="radio"/> Never <input type="radio"/> End of <input type="text"/> Password options: <input checked="" type="radio"/> User must change password at next log on <input type="radio"/> Other password options <input type="checkbox"/> Smart card is required for interactive log on <input type="checkbox"/> Password never expires <input type="checkbox"/> User cannot change password Encryption options: Other options:
Organization	Organization Display name: <input type="text" value="Nguyen Quoc Hung"/> Office: <input type="text"/> E-mail: <input type="text"/> Web page: <input type="text"/> Other web pages...	Job title: <input type="text"/> Department: <input type="text"/> Company: <input type="text"/> Manager: <input type="text"/> Edit... Clear Direct reports: <input type="text"/>
Profile		
Password Settings		

OK Cancel

▪ Tạo User **nghialv**:

Create User: Luu Van Nghia

Account Organization Member Of Password Settings Profile	Account First name: Luu Van Middle initials: Last name: Nghia Full name: Luu Van Nghia User UPN logon: nghialv @ bkaptech.vn User SamAccountName I... bkaptech ** nghialv Password: ***** Confirm password: ***** Create in: CN=Users,DC=bkaptech,DC=vn Change... <input type="checkbox"/> Protect from accidental deletion Log on hours... Log on to...	Account expires: <input checked="" type="radio"/> Never <input type="radio"/> End of <input type="text"/> Password options: <input checked="" type="radio"/> User must change password at next log on <input type="radio"/> Other password options <input type="checkbox"/> Smart card is required for interactive log on <input type="checkbox"/> Password never expires <input type="checkbox"/> User cannot change password Encryption options: Other options:
Organization Display name: Luu Van Nghia Office: E-mail: Web page: Other web pages...		
Job title: Department: Company: Manager: Edit... Clear Direct reports: Edit... Clear		
More Information OK Cancel		

▪ Tạo User **quanch**:

Create User: Chu Hong Quan

Account Organization Member Of Password Settings Profile	Account First name: Chu Hong Middle initials: Last name: Quan Full name: Chu Hong Quan User UPN logon: quanch @ bkaptech.vn User SamAccountName I... bkaptech ** quanch Password: ***** Confirm password: ***** Create in: CN=Users,DC=bkaptech,DC=vn Change... <input type="checkbox"/> Protect from accidental deletion Log on hours... Log on to...	Account expires: <input checked="" type="radio"/> Never <input type="radio"/> End of <input type="text"/> Password options: <input checked="" type="radio"/> User must change password at next log on <input type="radio"/> Other password options <input type="checkbox"/> Smart card is required for interactive log on <input type="checkbox"/> Password never expires <input type="checkbox"/> User cannot change password Encryption options: Other options:
Organization Display name: Chu Hong Quan Office: E-mail: Web page: Other web pages...		
Job title: Department: Company: Manager: Edit... Clear Direct reports: Edit... Clear		
More Information OK Cancel		

▪ Tạo User cuongnt:

Create User: Nguyen Tien Cuong

Account	Account First name: Nguyen Tien Middle initials: Cuong Last name: Nguyen Tien Cuong Full name: * Nguyen Tien Cuong User UPN logon: cuongnt @ bkaptech.vn User SamAccountName: bkaptech * cuongnt Password: ***** Confirm password: ***** Create in: CN=Users,DC=bkaptech,DC=vn Change... <input type="checkbox"/> Protect from accidental deletion Log on hours... Log on to...	Account expires: <input checked="" type="radio"/> Never <input type="radio"/> End of [] Password options: <input checked="" type="radio"/> User must change password at next log on <input type="radio"/> Other password options <input type="checkbox"/> Smart card is required for interactive log on <input type="checkbox"/> Password never expires <input type="checkbox"/> User cannot change password Encryption options: Other options:
Organization	Organization Display name: Nguyen Tien Cuong Office: [] E-mail: [] Web page: [] Other web pages...	Job title: [] Department: [] Company: [] Manager: [] Edit... Clear Direct reports:

[More Information](#) [OK](#) [Cancel](#)

▪ Tạo user duynh:

Create User: Nguyen Hoai Duy

Account	Account First name: Nguyen Hoai Middle initials: Duy Last name: Nguyen Hoai Duy Full name: * Nguyen Hoai Duy User UPN logon: duynh @ bkaptech.vn User SamAccountName: bkaptech * duynh Password: ***** Confirm password: ***** Create in: CN=Users,DC=bkaptech,DC=vn Change... <input type="checkbox"/> Protect from accidental deletion Log on hours... Log on to...	Account expires: <input checked="" type="radio"/> Never <input type="radio"/> End of [] Password options: <input checked="" type="radio"/> User must change password at next log on <input type="radio"/> Other password options <input type="checkbox"/> Smart card is required for interactive log on <input type="checkbox"/> Password never expires <input type="checkbox"/> User cannot change password Encryption options: Other options:
Organization	Organization Display name: Nguyen Hoai Duy Office: [] E-mail: [] Web page: [] Other web pages...	Job title: [] Department: [] Company: [] Manager: [] Edit... Clear Direct reports:

[More Information](#) [OK](#) [Cancel](#)

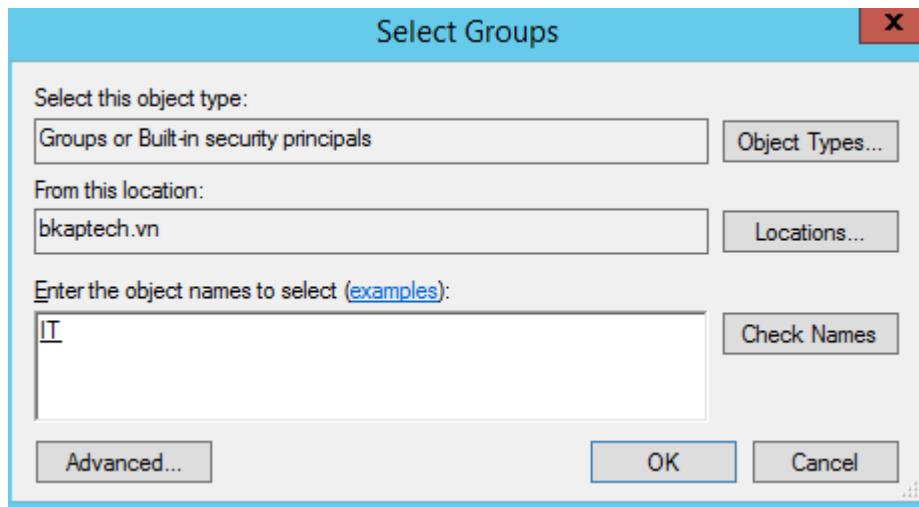
- Add user **hungnq** vào group **IT**.

The screenshot shows the 'Active Directory Administrative Center' interface. On the left, there's a navigation pane with 'Active Directory...', 'Overview', and 'bkaptech (local)' expanded to show 'Users', 'Dynamic Access Control', and 'Global Search'. The main area is titled 'Users (30)' and lists several users and one group:

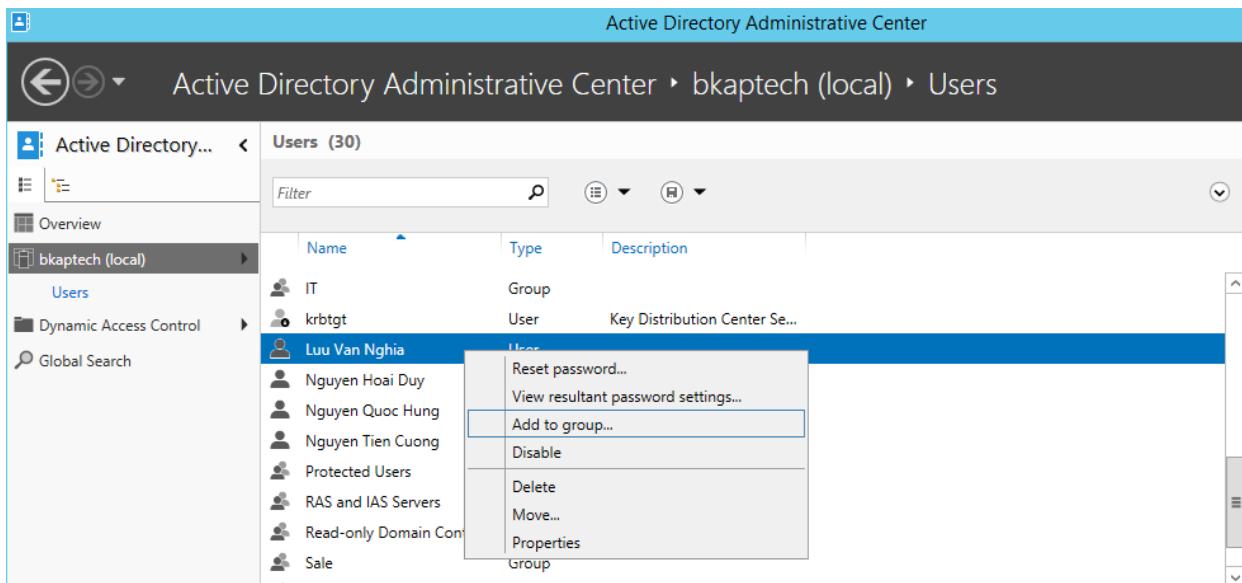
Name	Type	Description
IT	Group	
krbtgt	User	Key Distribution Center Se...
Luu Van Nghia	User	
Nguyen Hoai Duy	User	
Nguyen Quoc Hung	User	
Nguyen Tien Cuong		Reset password...
Protected Users		View resultant password settings...
RAS and IAS Servers		Add to group...
Read-only Domain Contr		Disable
Sale		Delete
Nguyen Quoc Hung		Move...
		Properties

Below the table, user details are shown: User logon: hungnq, E-mail: , Modified: 3/23/2016 7:15 PM, Description: . At the bottom, there are 'Summary' and 'Expiration: <Never>' fields.

- Chọn đến group **IT**.



- Add user **nghialv** vào group **Sale**.



The screenshot shows the 'Active Directory Administrative Center' interface. On the left, there's a navigation pane with 'Active Directory...', 'Overview', 'bkaptech (local)' (which is expanded to show 'Users', 'Dynamic Access Control', and 'Global Search'), and a 'Filter' search bar. The main area is titled 'Users (30)' and lists users and groups. A context menu is open over the user 'Luu Van Nghia', with 'Add to group...' highlighted.

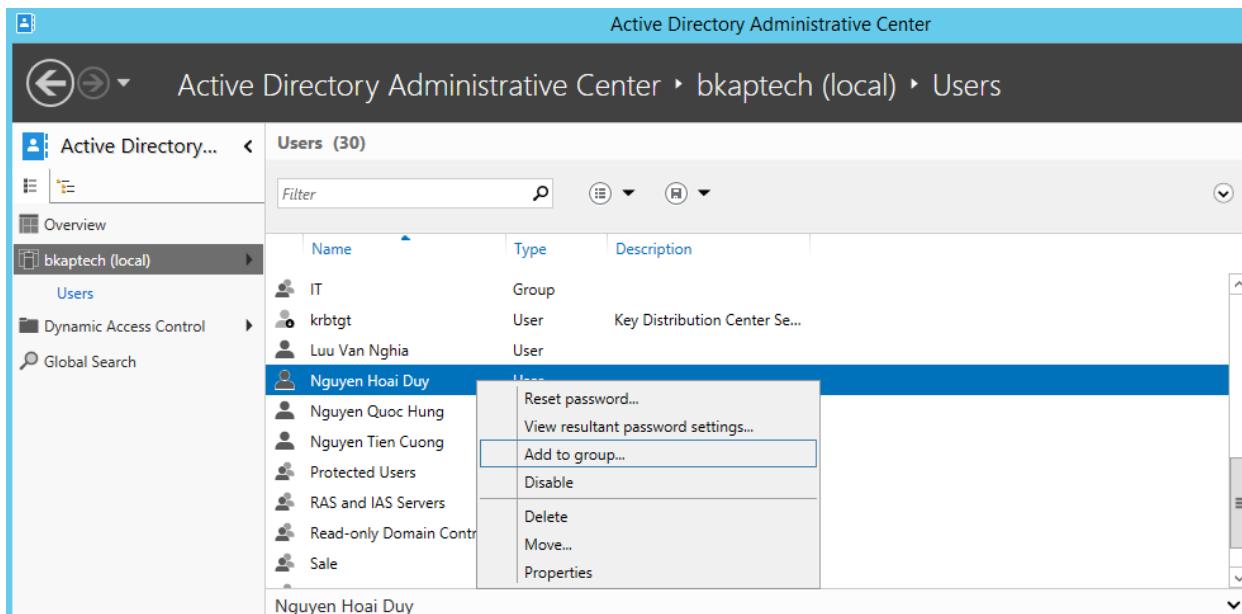
Select Groups

Select this object type:

From this location:

Enter the object names to select ([examples](#)):

- Add user **huynh** vào group **Giam Doc**.



The screenshot shows the 'Active Directory Administrative Center' interface. On the left, there's a navigation pane with 'Active Directory...', 'Overview', 'bkaptech (local)' (which is expanded to show 'Users', 'Dynamic Access Control', and 'Global Search'), and 'Filter' and search icons. The main area is titled 'Users (30)' and lists users and groups. One user, 'Nguyen Hoai Duy', is selected, and a context menu is open over it. The menu options include 'Reset password...', 'View resultant password settings...', 'Add to group...', 'Disable', 'Delete', 'Move...', and 'Properties'. The 'Add to group...' option is highlighted with a blue selection bar.

Select Groups

Select this object type:

From this location:

Enter the object names to select (examples):

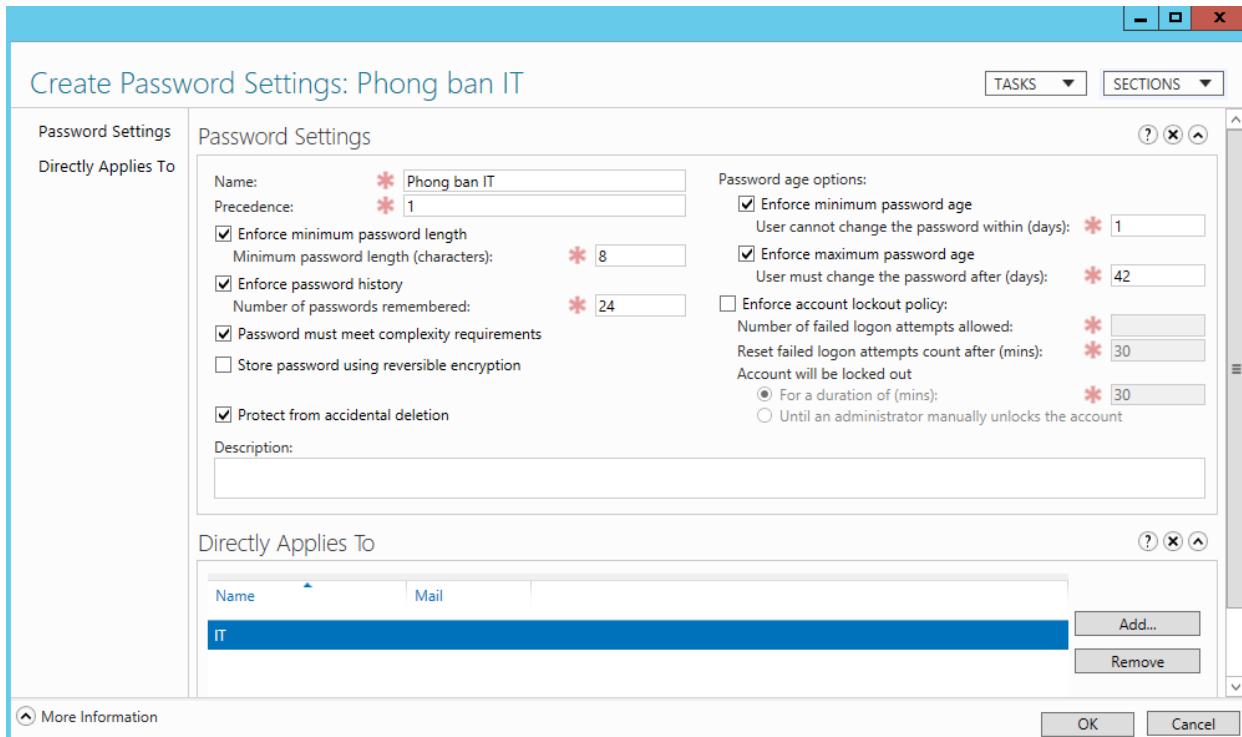
- Triển khai *chính sách Password* xuống cho từng phòng ban:
 - Click vào *mũi tên* tại **bkaptech (local)** , chọn vào **System**.

The screenshot shows the Active Directory Administrative Center interface. The left navigation pane is collapsed, showing the main menu. The central pane displays the 'System (25)' configuration for the 'bkaptech (local)' domain controller. The 'System' node is selected in the tree view. The right pane contains a detailed list of system components, with 'System' also highlighted in blue. At the bottom, there are fields for 'Object class: Container' and 'Description:', and a 'Summary' button.

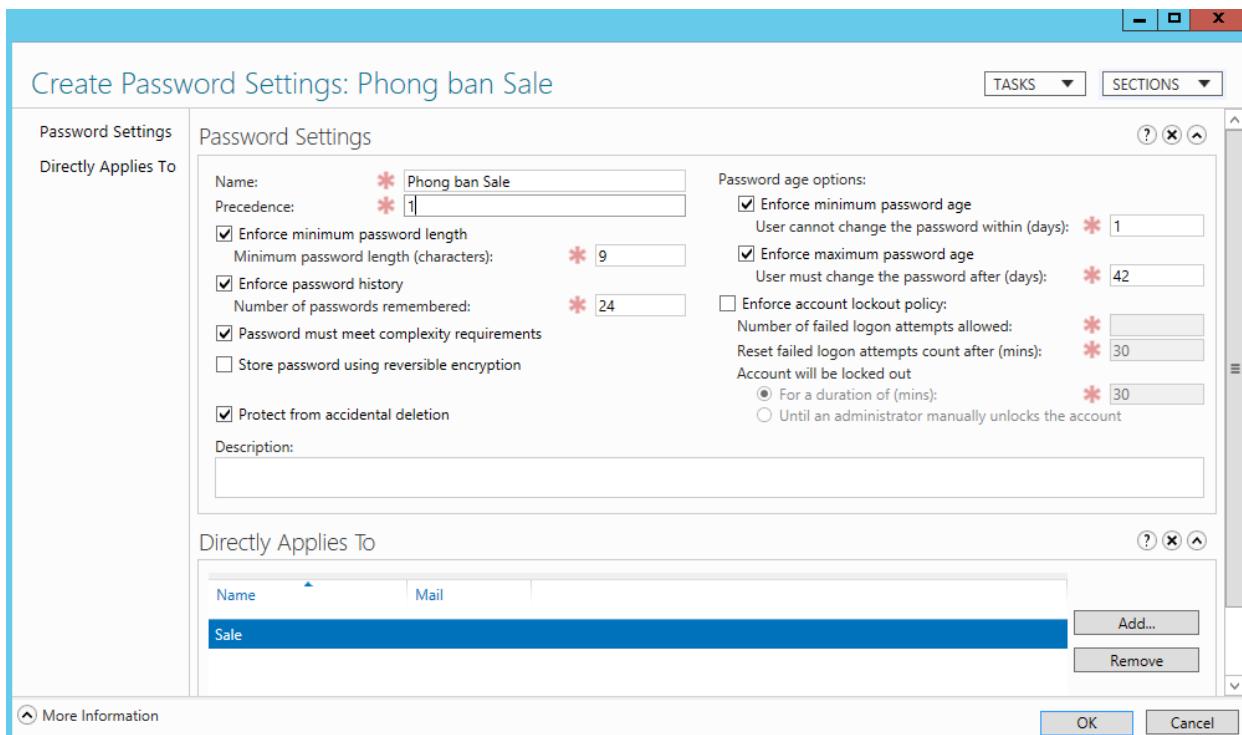
- Chọn vào **Password Settings Container / New / Password Settings.**

The screenshot shows the 'Active Directory Administrative Center' interface. The left navigation pane shows 'Active Directory...', 'Overview', and 'bkaptech (local)' which is expanded to show 'System', 'Users', 'Dynamic Access Control', and 'Global Search'. The main pane displays the 'System (25)' section with a table of objects. One object, 'Password Settings Container', has a context menu open. The menu items are: 'New' (highlighted), 'Delete', 'Search under this node', and 'Properties'. Below the table, there is a summary box for the 'Password Settings Container' object, showing its 'Object class: msDS-PasswordSettingsContainer' and 'Modified: 2/24/2016 2:25 PM'.

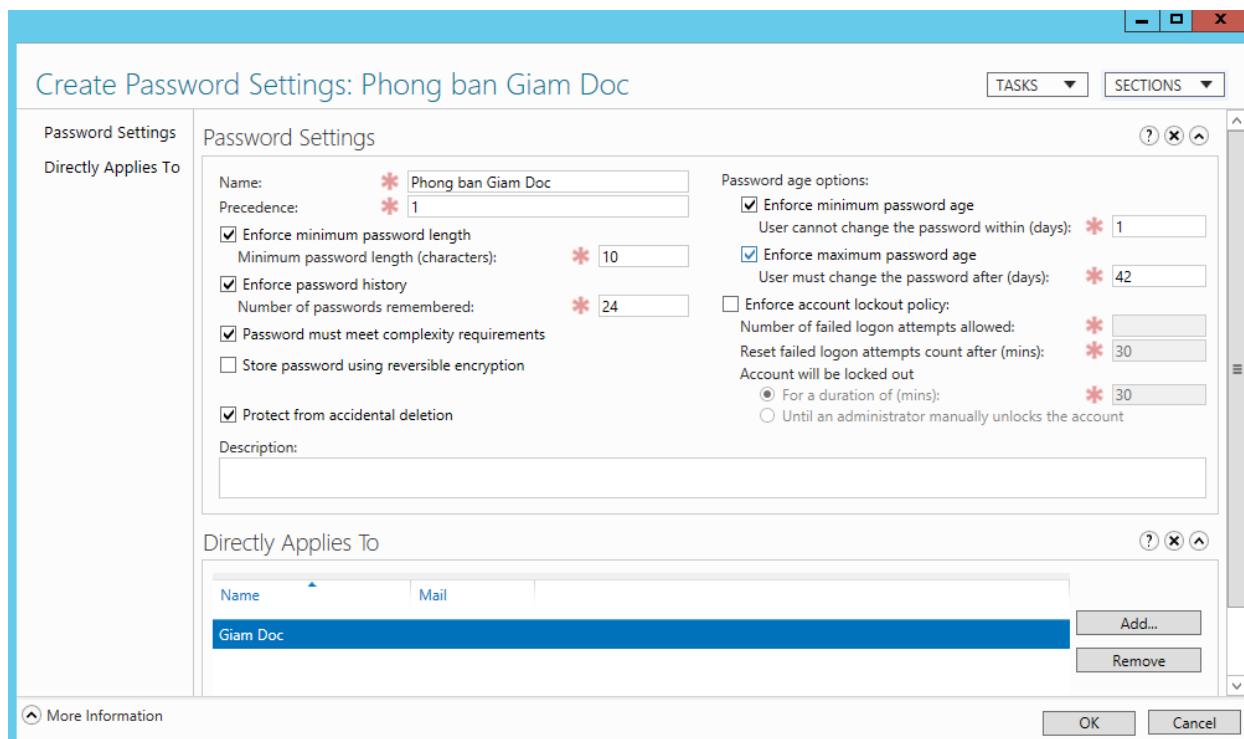
- Thiết lập *chính sách password* cho phòng ban IT.(thiết lập password là 8 ký tự).



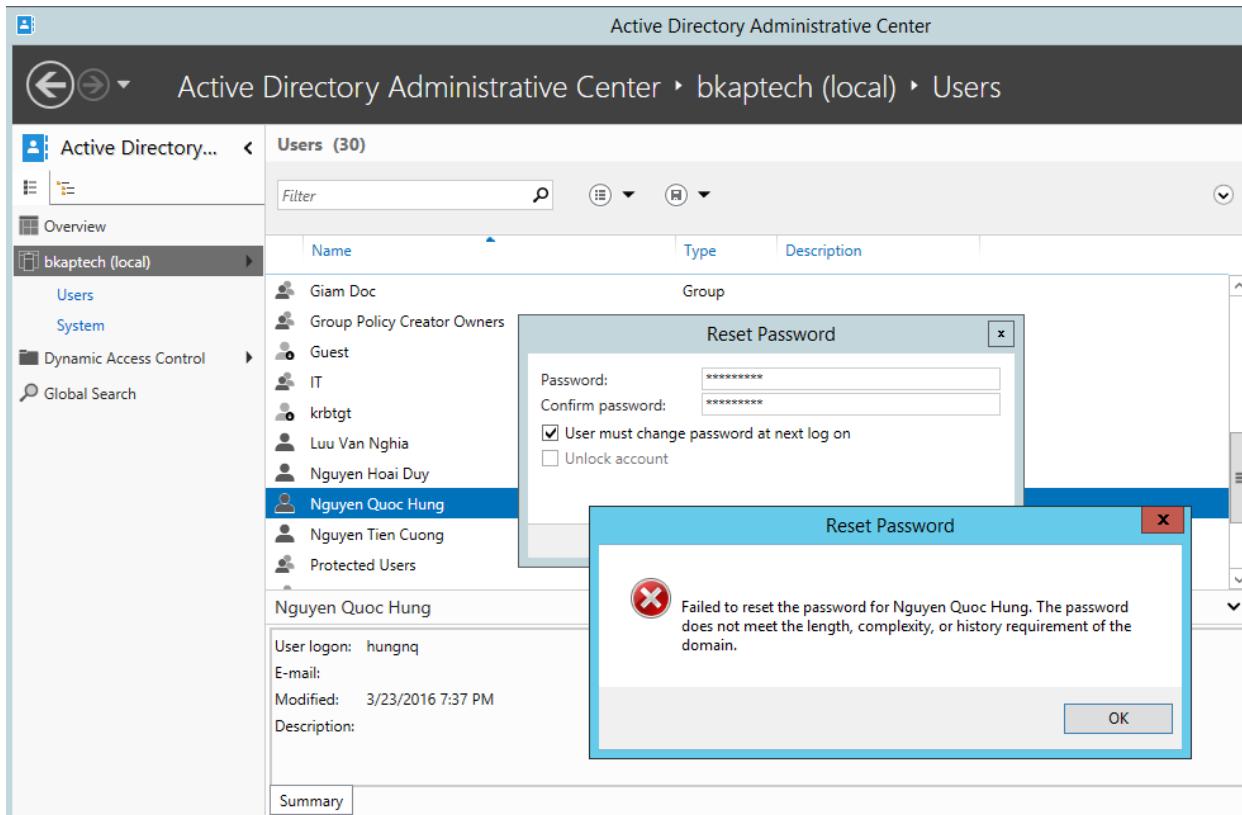
- Thiết lập chính sách cho phòng ban Sale (password là 9 ký tự).



- Thiết lập chính sách cho phòng ban **Giam Doc** (*Password là 10 kí tự*).



- Thủ **Restart Password** để kiểm tra chính sách:
 - User **hungnq** thuộc phòng ban **IT** có chính sách *password* ko được dài hơn 8 kí tự :



- Kiểm tra tương tự đối với những tài khoản khác.

Bài 5:

CẤU HÌNH MAP NETWORK DRIVE , MAP PRINTER BẰNG VBSCRIPT.

1. Yêu cầu bài Lab:

- + Map ổ đĩa , máy tin tự động về các tài khoản khi đăng nhập các user thuộc ou BKAP.

2. Yêu cầu chuẩn bị:

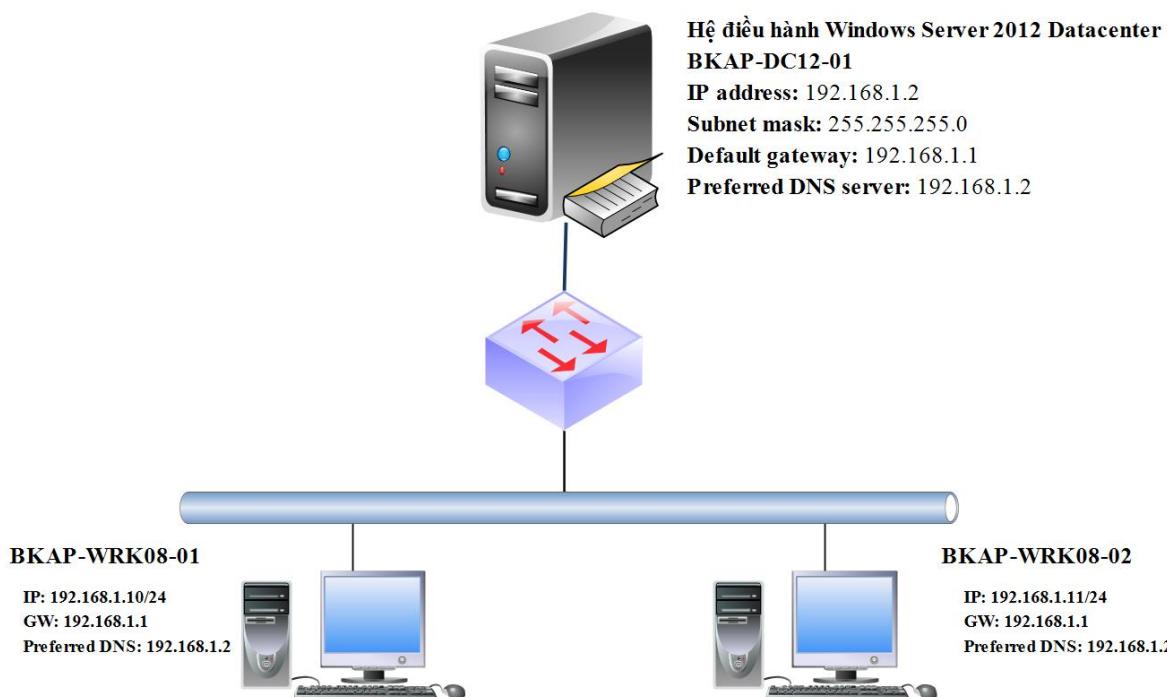
- + Máy Server *BKAP-DC12-01* đã nâng cấp lên **Domain Controller** quản lý miền **bkaptech.vn**.
- + Chuẩn bị sẵn các file *VBScript* để cấu hình.
- + Máy Client *BKAP-WRK07-01* Join vào miền.

3. Mô hình Lab:

HỆ THỐNG ĐÀO TẠO CNTT QUỐC TẾ BACHKHOA-APTECH

Lab 5 Cấu hình Map Network Drive , Map Printer bằng VBScript

BACHKHOA
EDUCATION / APTECH



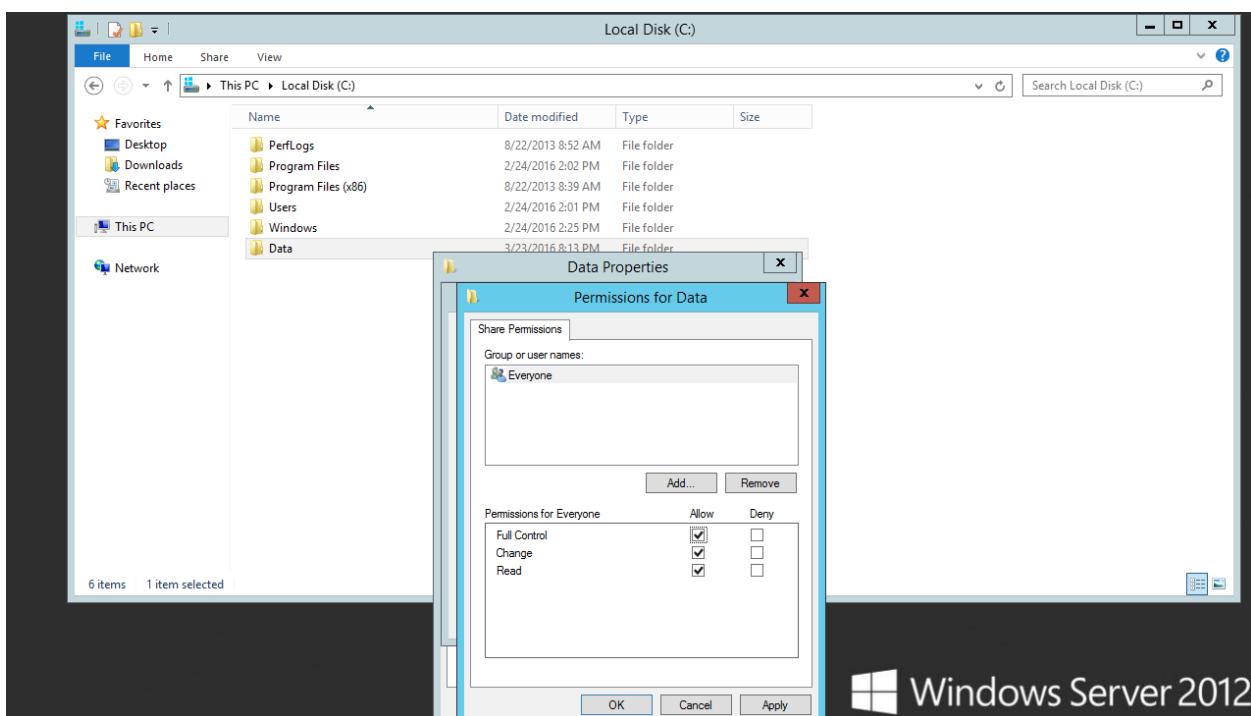
Hình 5

Sơ đồ địa chỉ như sau:

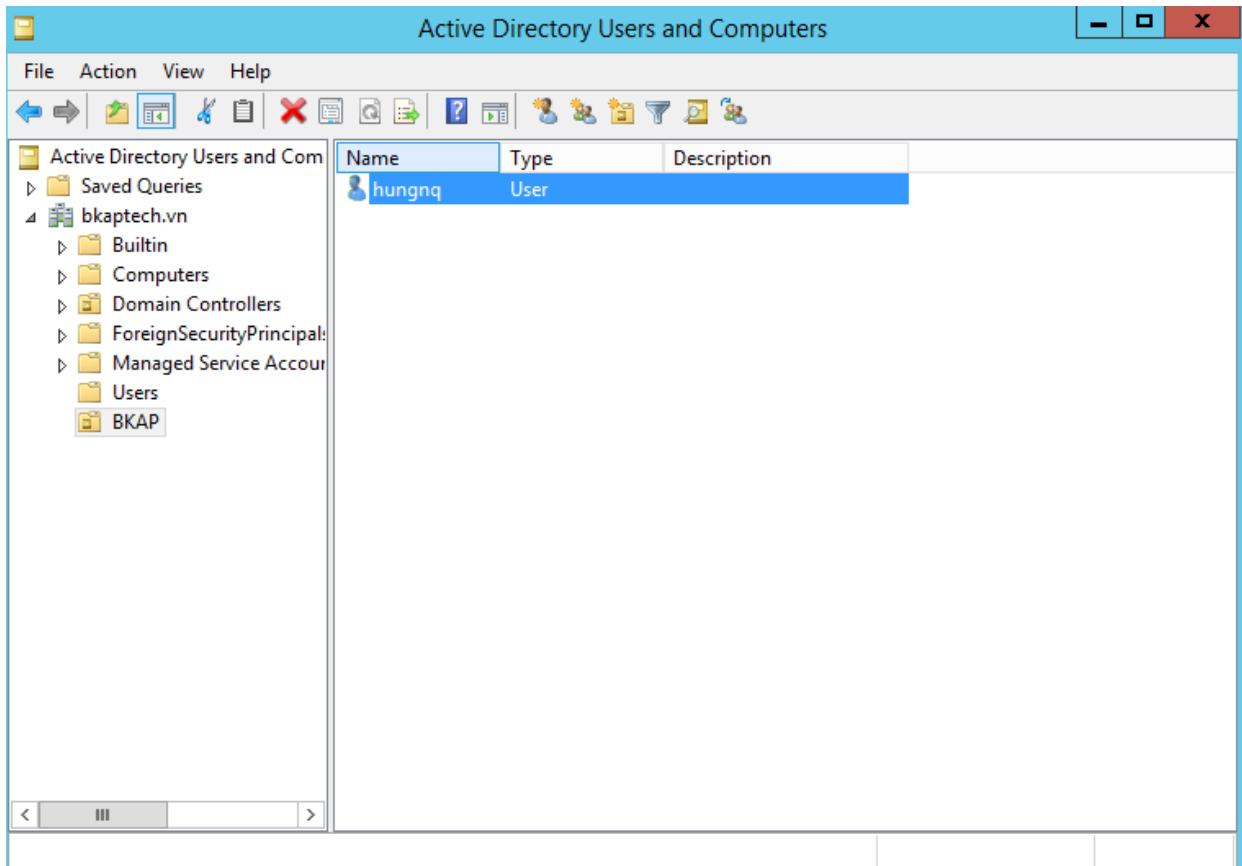
Thông số	BKAP-DC12-01	BKAP-WRK08-01
IP address	192.168.1.2	192.168.1.10
Gateway	192.168.1.1	192.168.1.1
Subnet Mask	255.255.255.0	255.255.255.0
DNS Server	192.168.1.2	192.168.1.2

Hướng dẫn chi tiết:

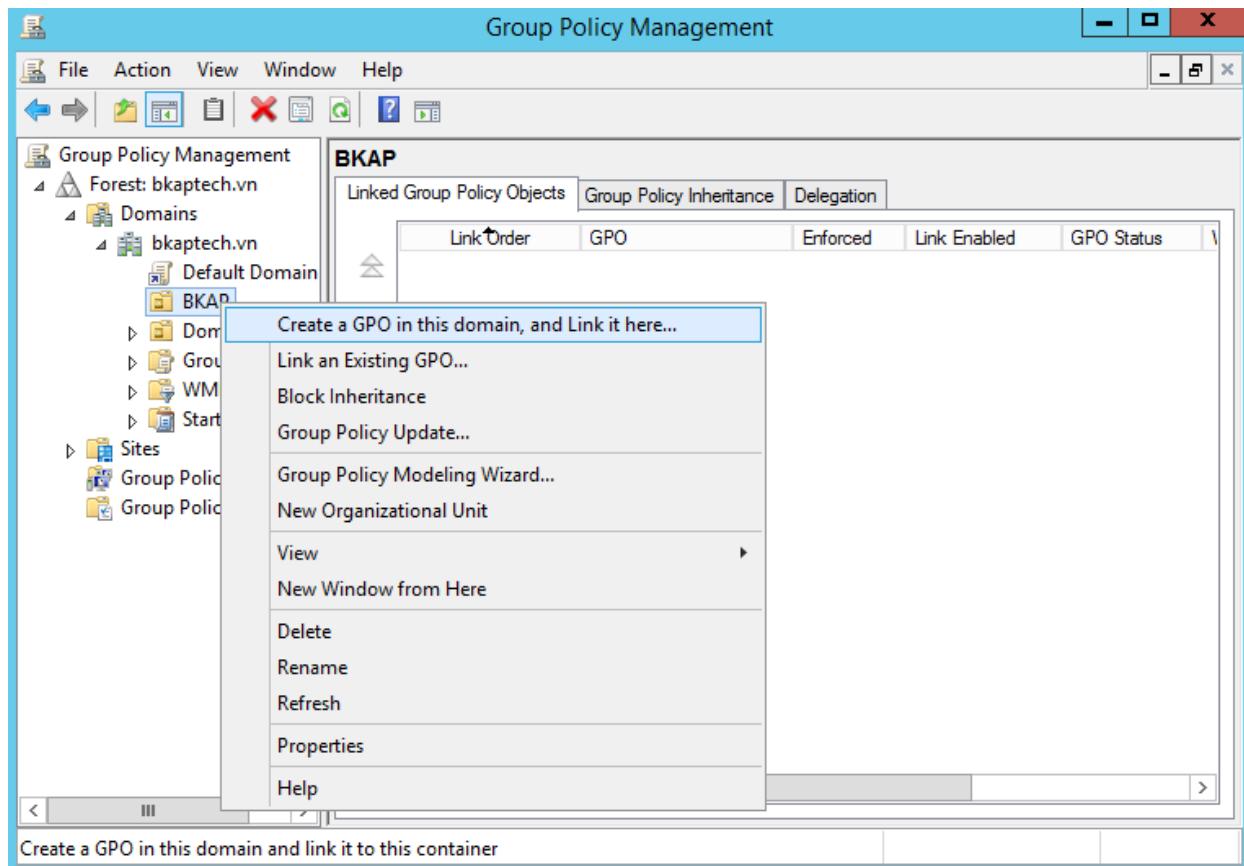
- Trên máy **BKAP-DC12-01**, thực hiện tạo thư mục **Data** và chia sẻ dữ liệu.



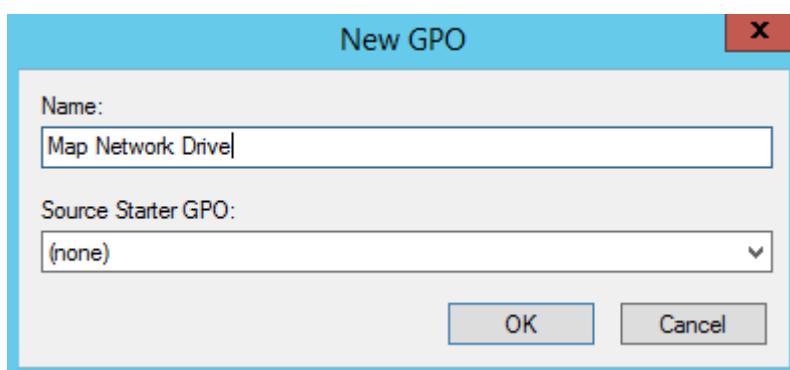
- Tạo ou BKAP , và tài khoản hungnq thuộc ou BKAP.



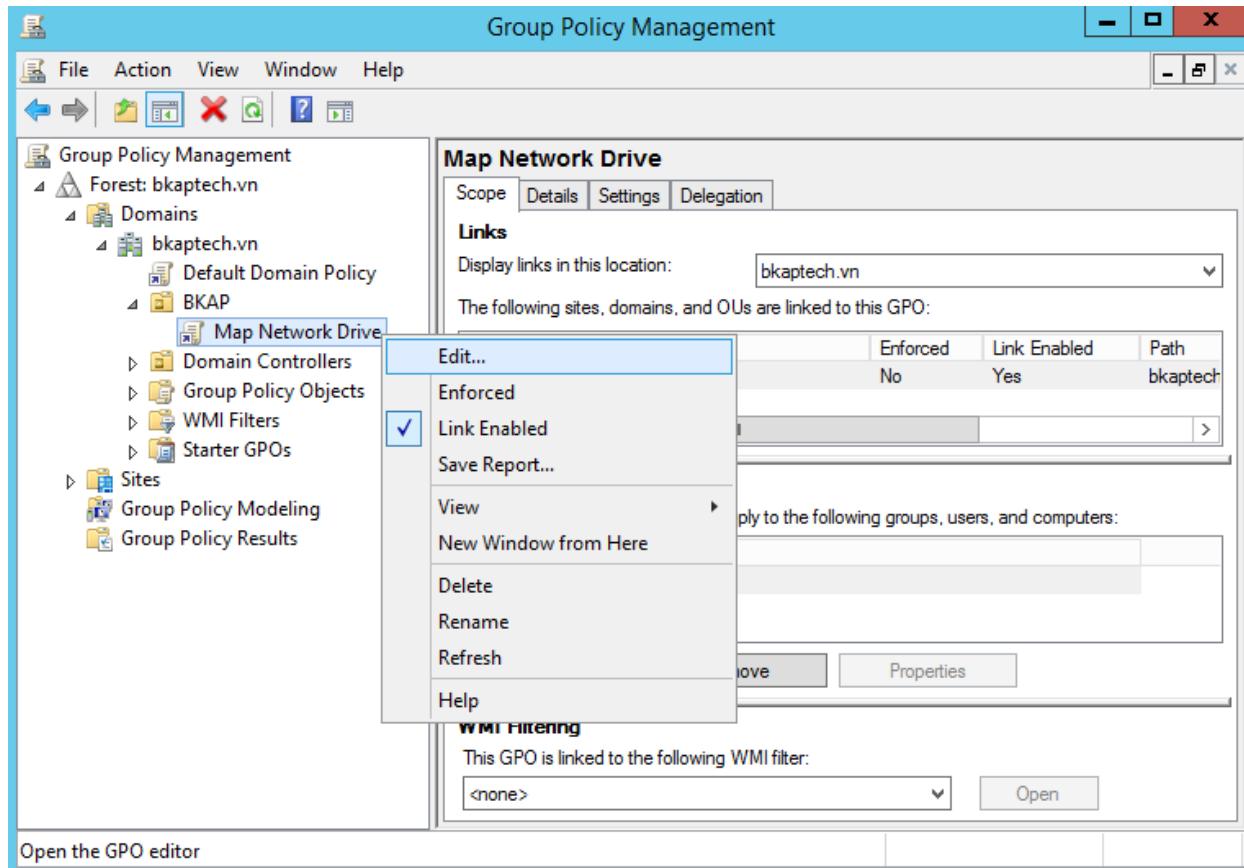
- Cấu hình Map Network Drive.
 - Vào **Group Policy Management** , click vào ou **BKAP** / **Create a GPO in this domain...**



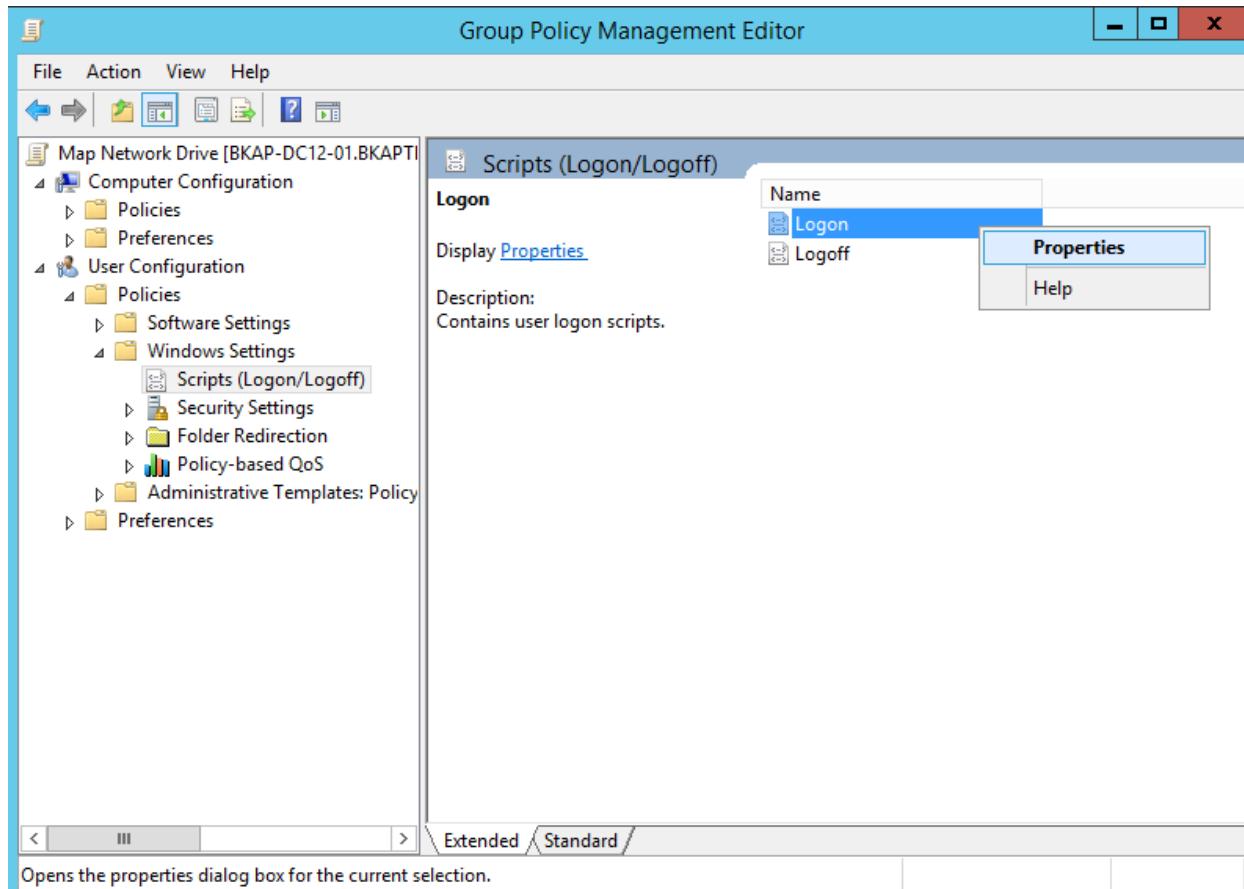
- Nhập vào tên của chính sách : **Map Network Drive.**



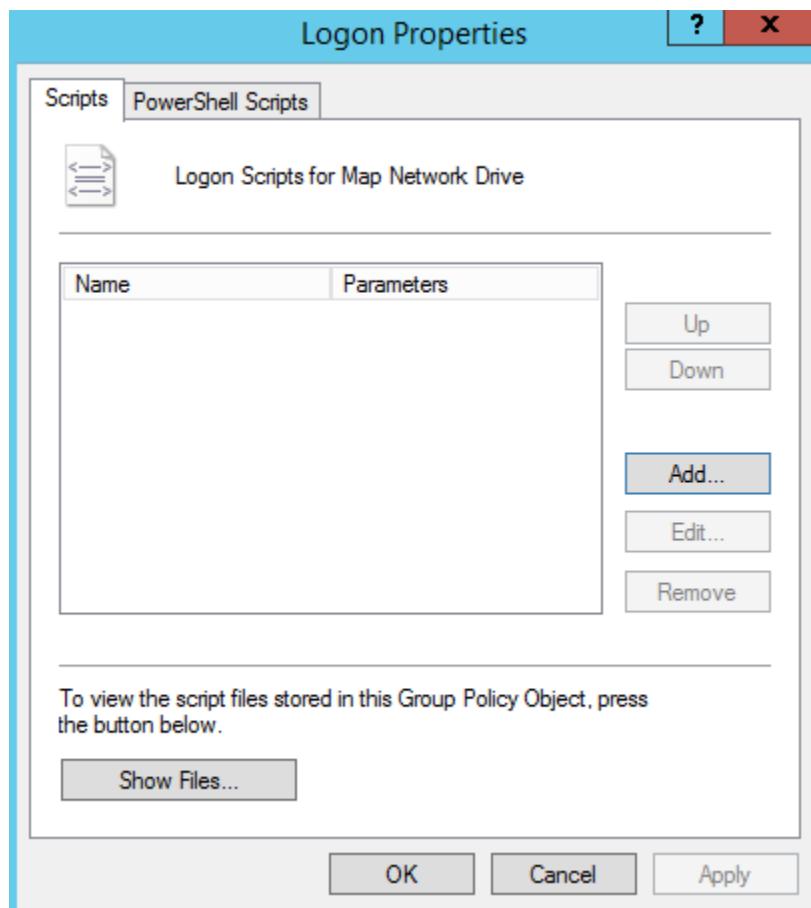
- Click chuột phải vào chính sách vừa tạo , chọn **Edit...**



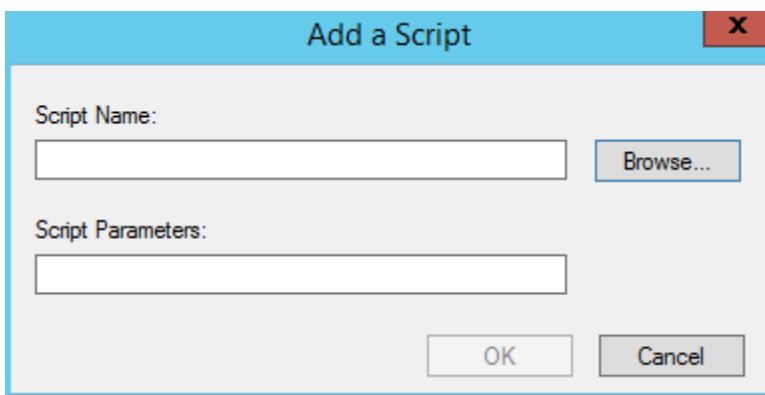
- Trong cửa sổ **Group Policy Management Editor**, chọn vào **User Configuration / Windows Settings / Scripts (Logon/Logoff)**, click vào **Logon / Properties**.



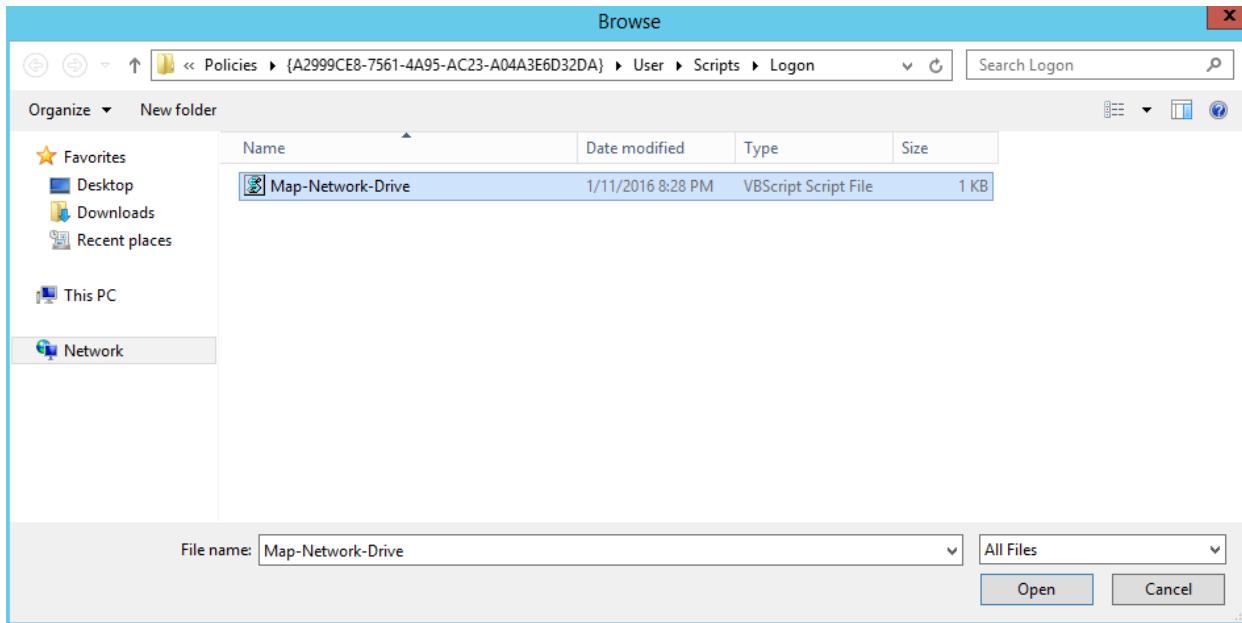
- Tại cửa sổ **Logon Properties**, click vào **Add...**



- Tại cửa sổ **Add a Script**, click vào **Browse...**



- **Copy / Paste file Script** vào trong cửa sổ **Browse**.



- **Gpupdate /force.**

```

Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

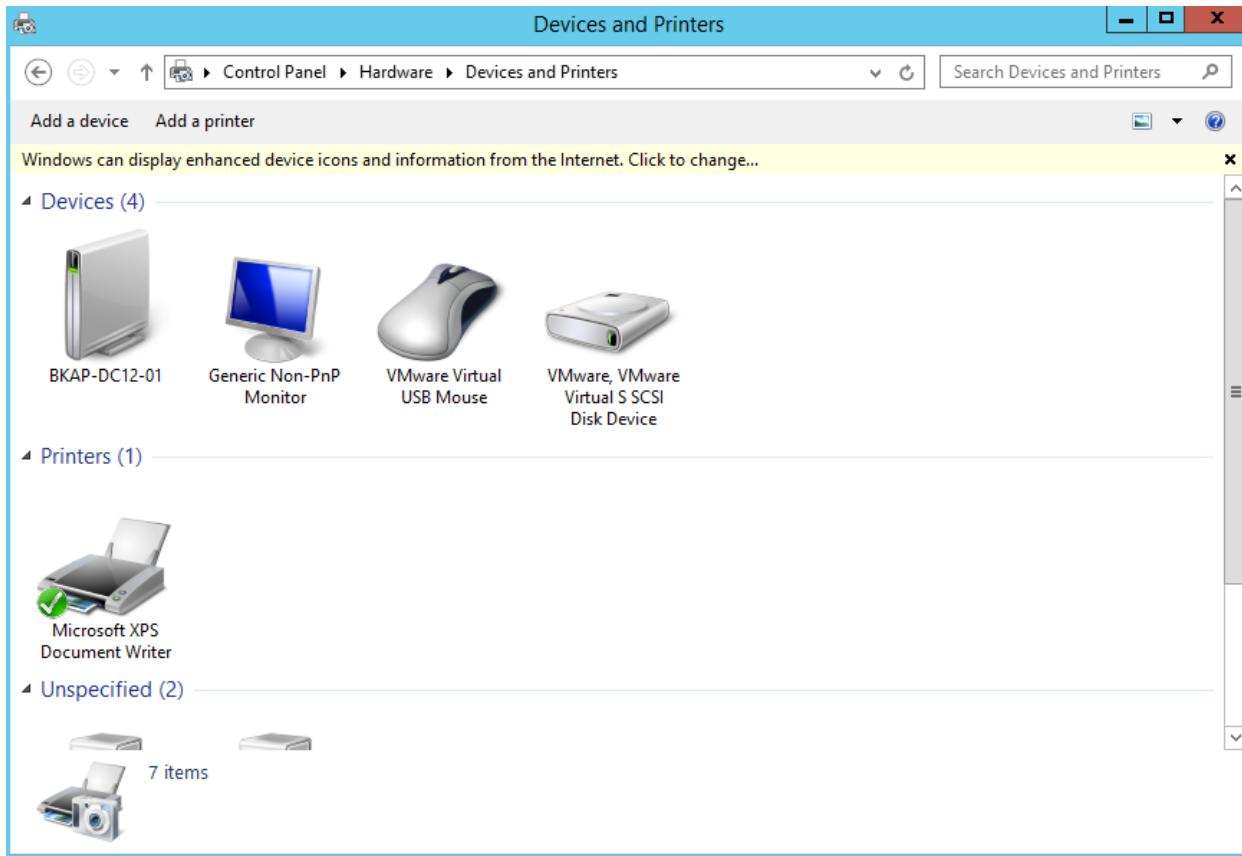
C:\Users\Administrator>gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.

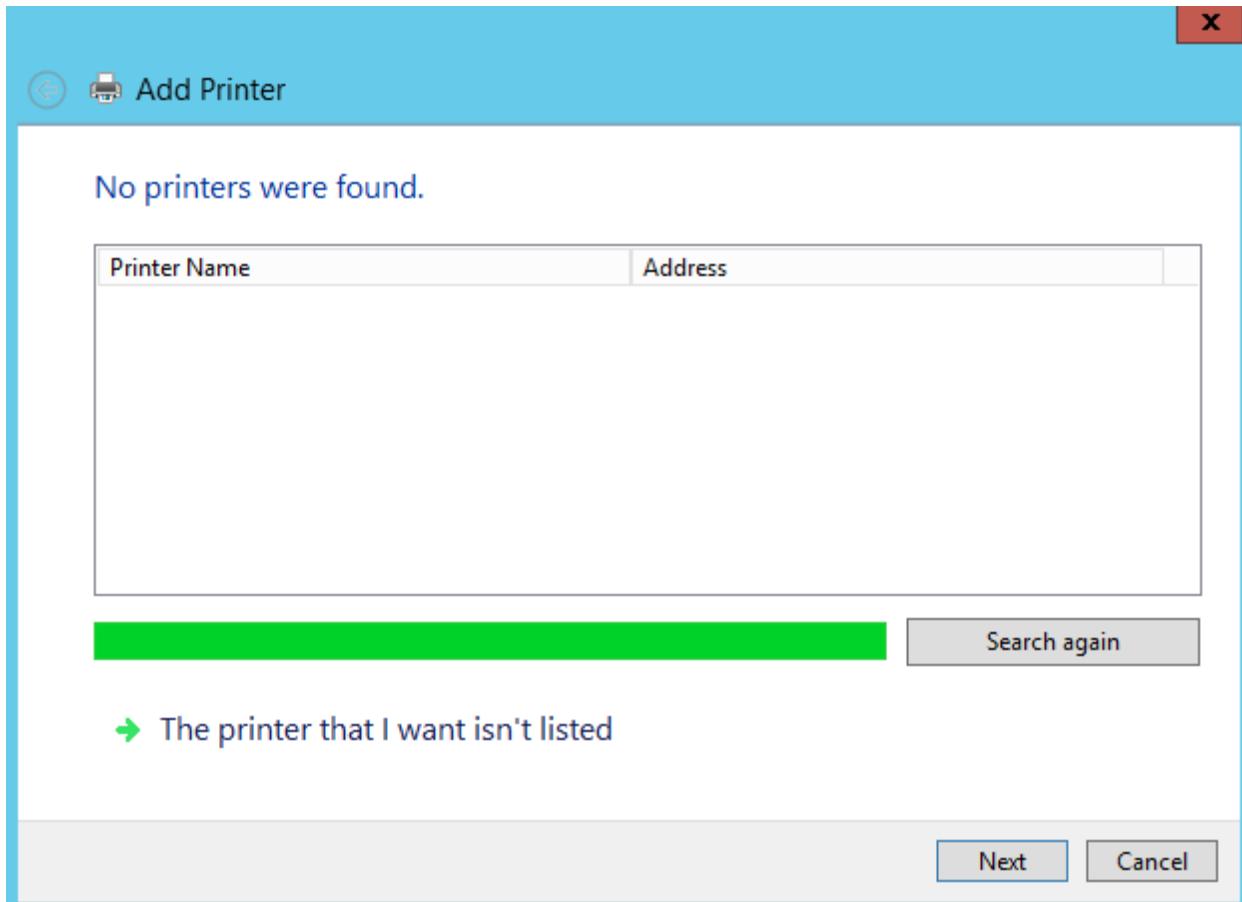
C:\Users\Administrator>

```

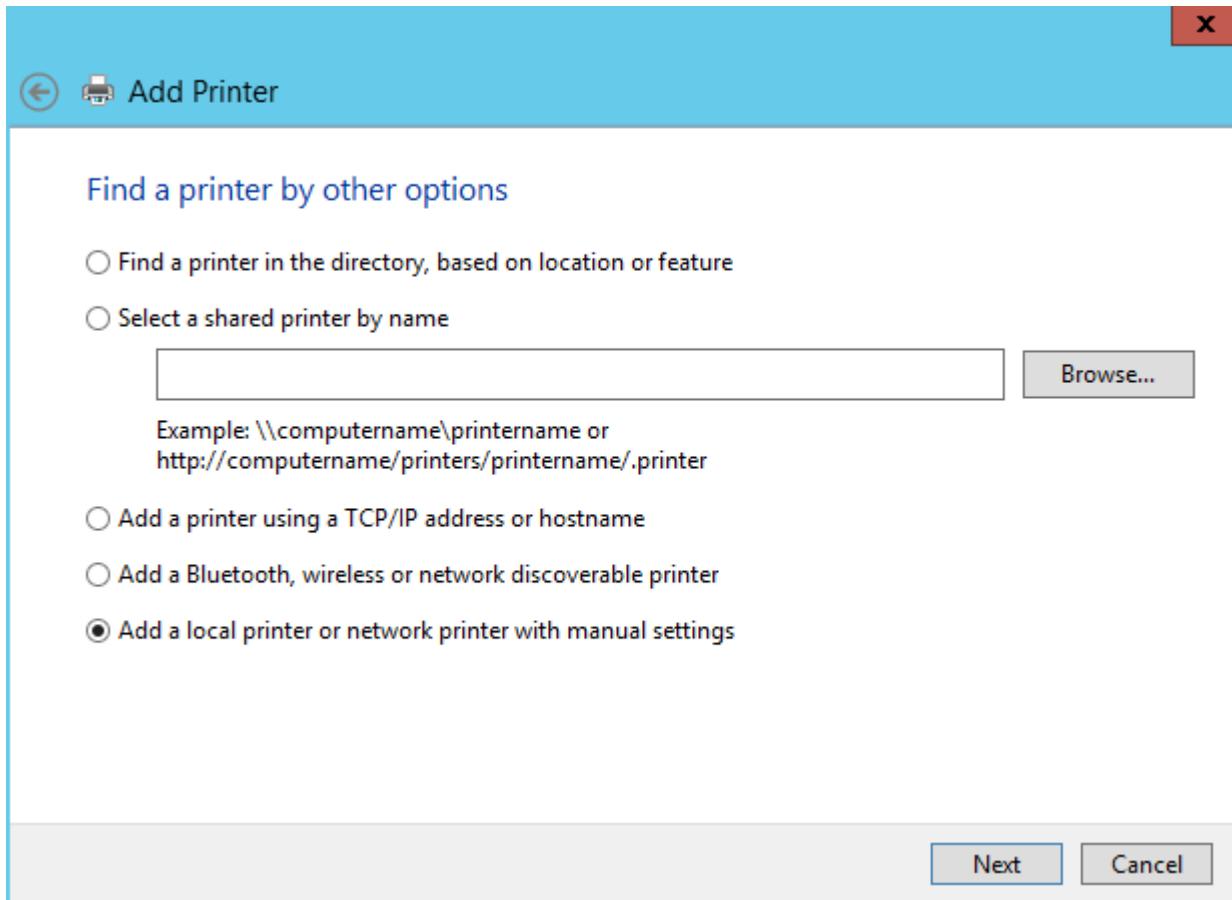
- Cấu hình Map Printer.
 - Vào Control Panel / Devices and Printers.



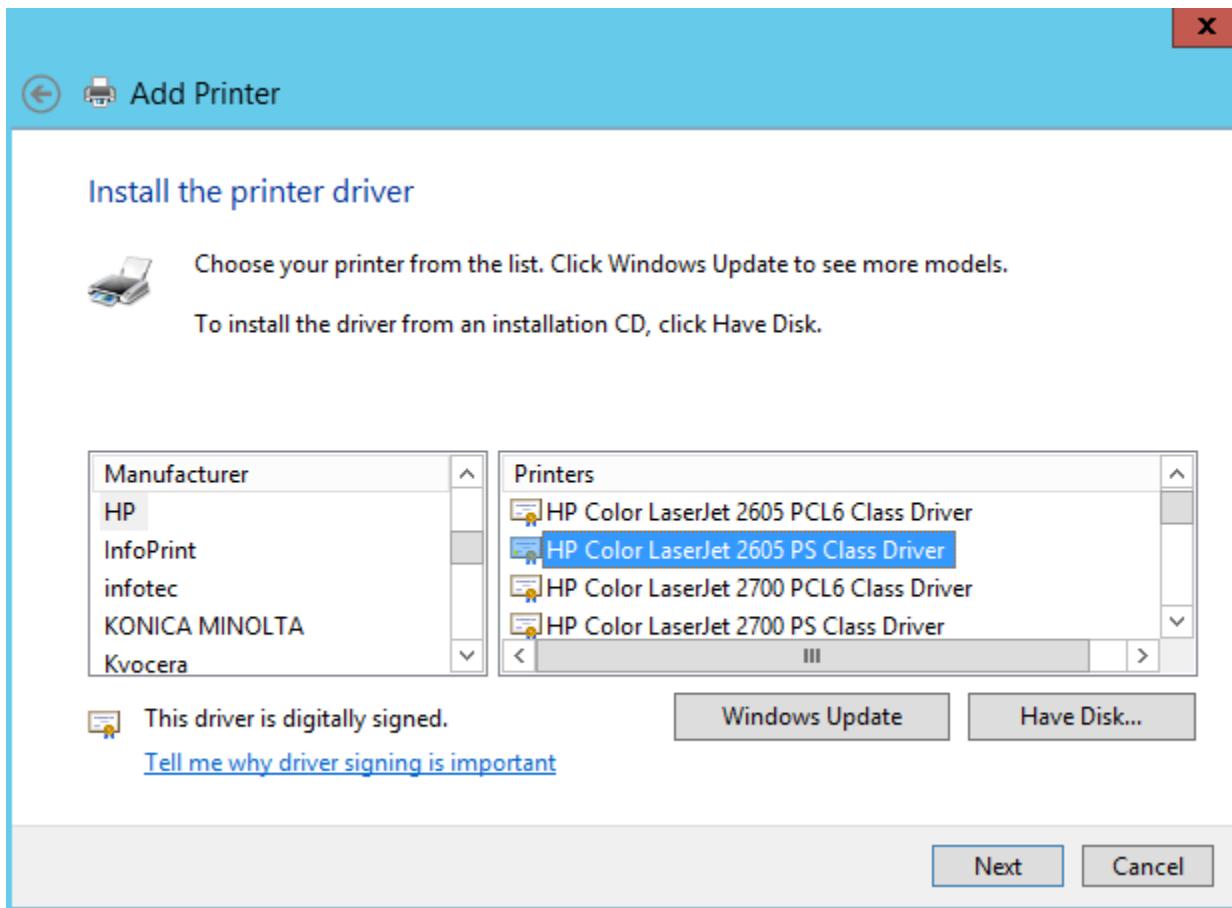
- Click vào **Add a printer** , tại cửa sổ **Add Printer** , click vào **Next**.



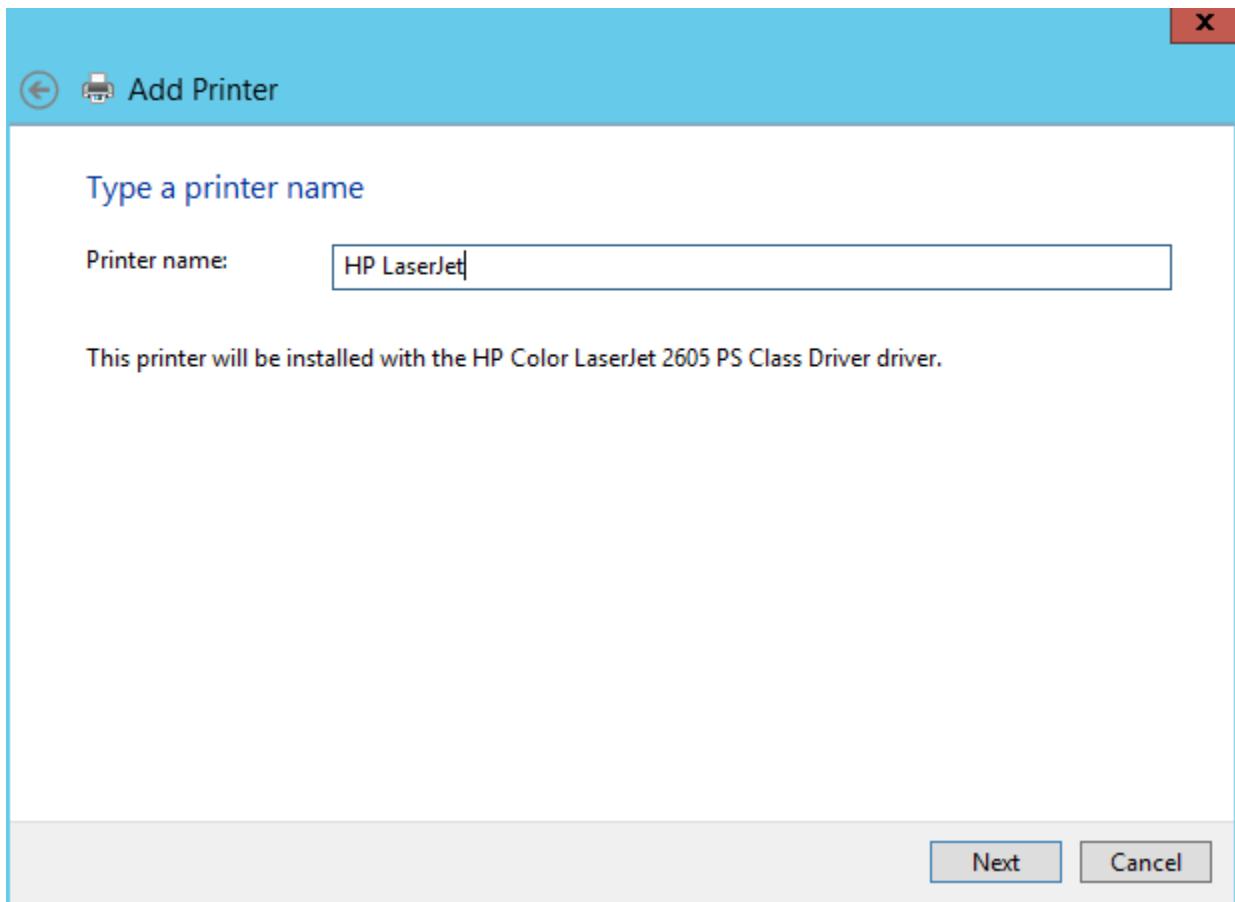
- Trong cửa sổ **Find a printer by other options**, click vào **Add a local printer or network printer with manual settings**.



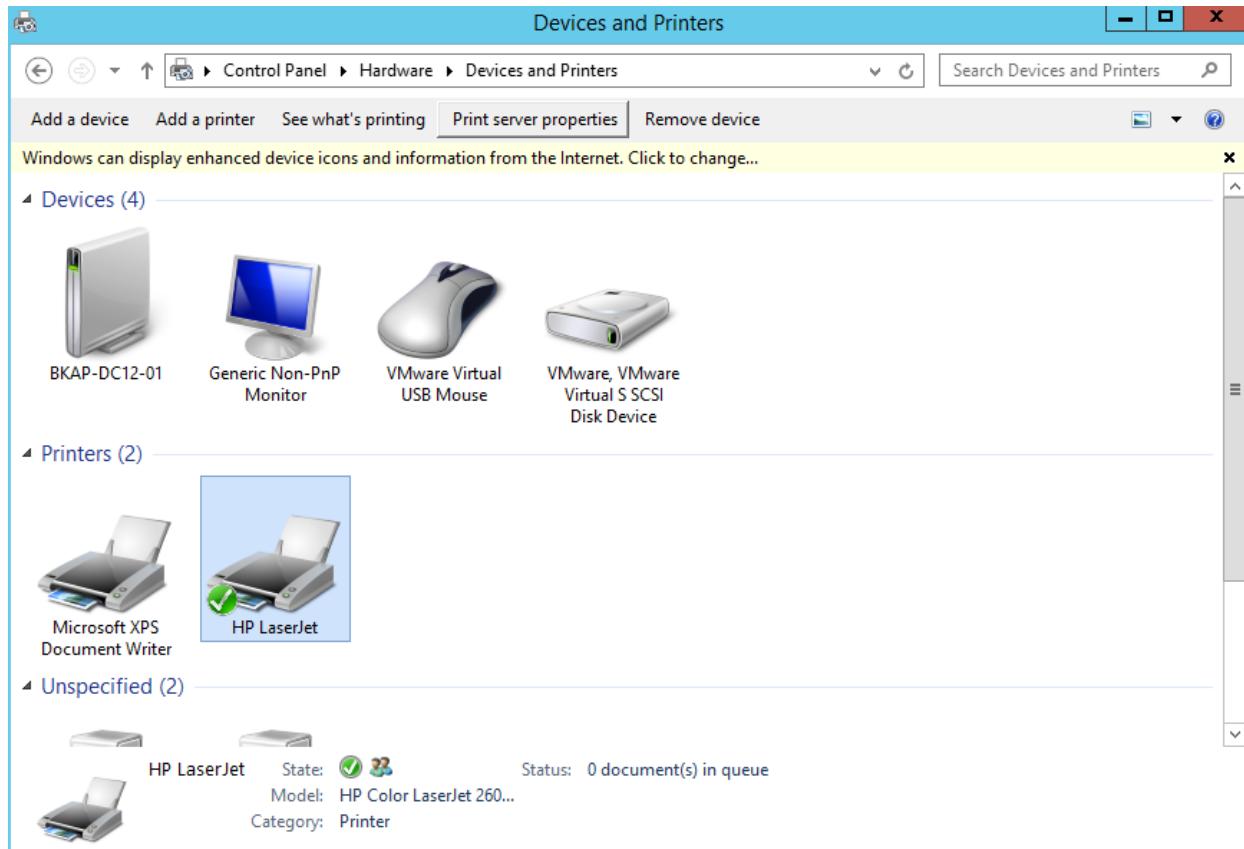
- Tại cửa sổ **Choose a printer port**, click vào **Next**.
- Tại cửa sổ **Install the printer driver**, chọn vào hãng máy in.



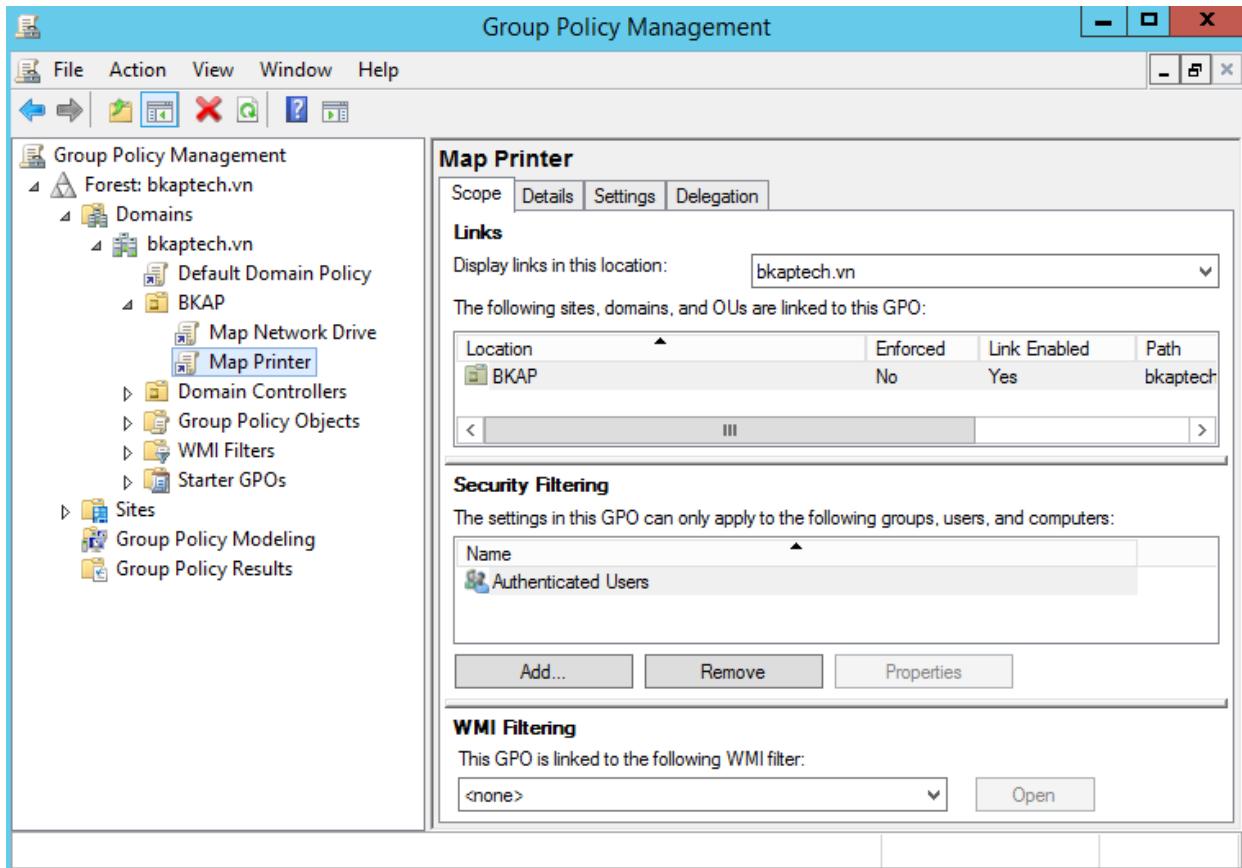
- Tại cửa sổ **Type a printer name**, nhập vào tên của máy in (*giống tên trong file script*).

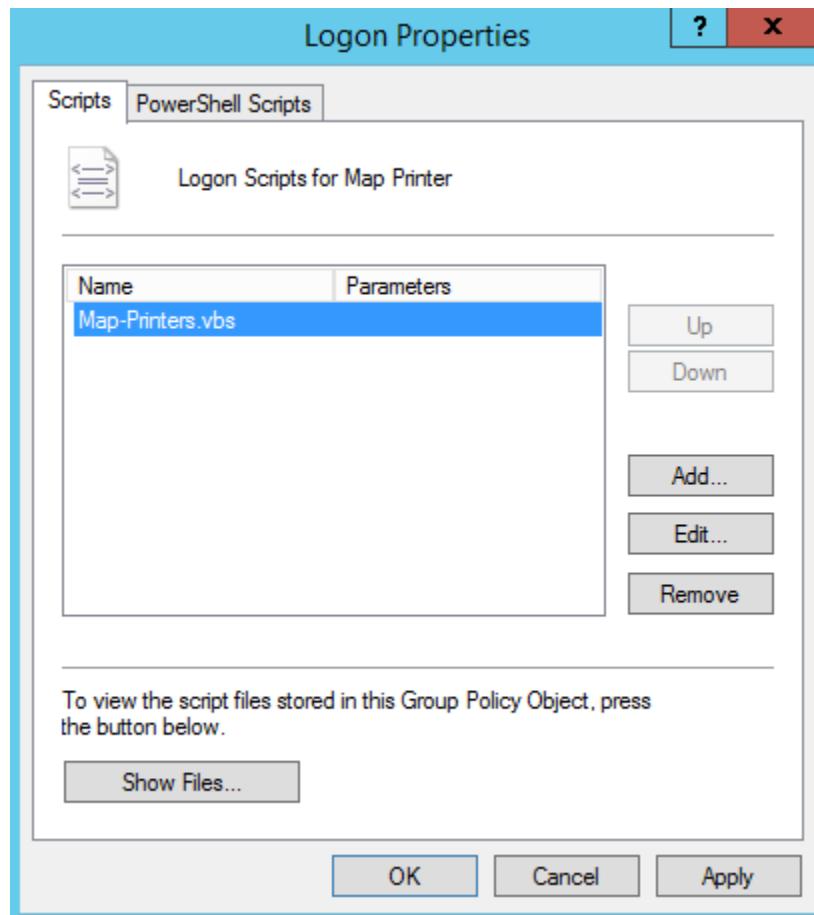


- Cấu hình máy in thành công.



- Tạo chính sách **Map Printer**, add file script tương tự như chính sách trên.





▪ Gpupdate /force

```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>gpupdate /force
Updating policy...

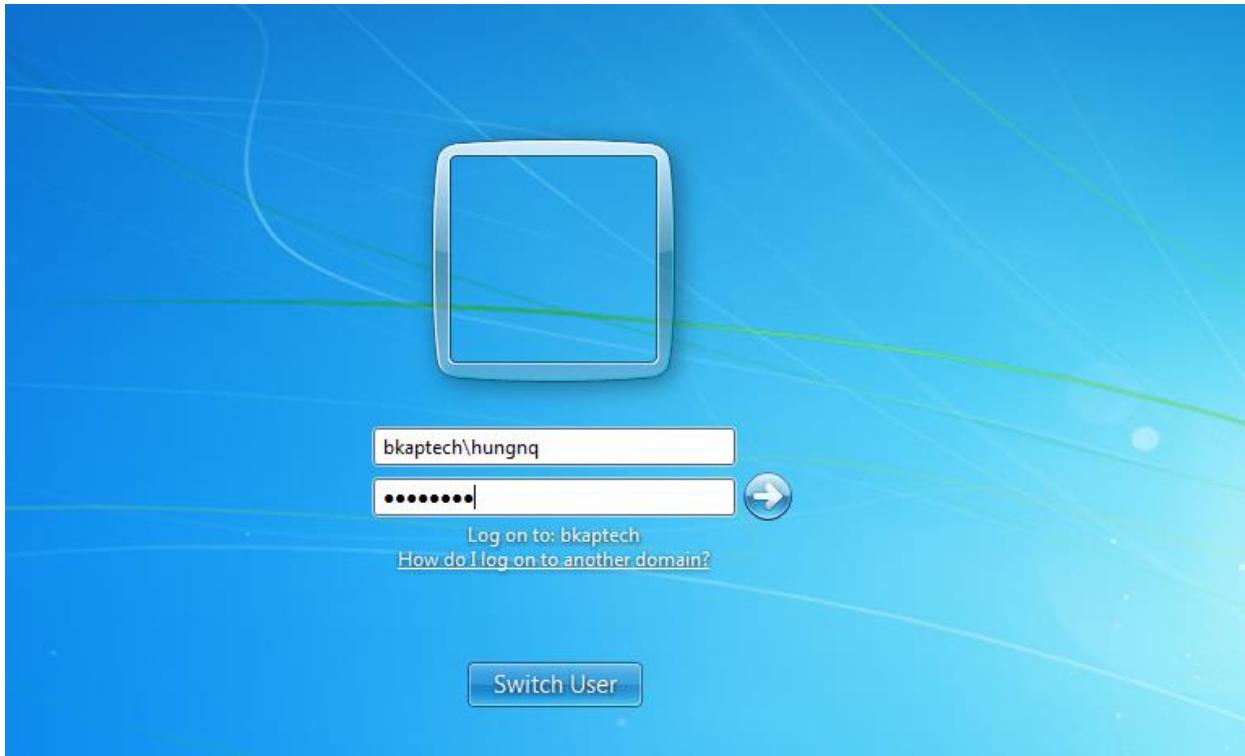
Computer Policy update has completed successfully.
User Policy update has completed successfully.

C:\Users\Administrator>gpupdate /force
Updating policy...

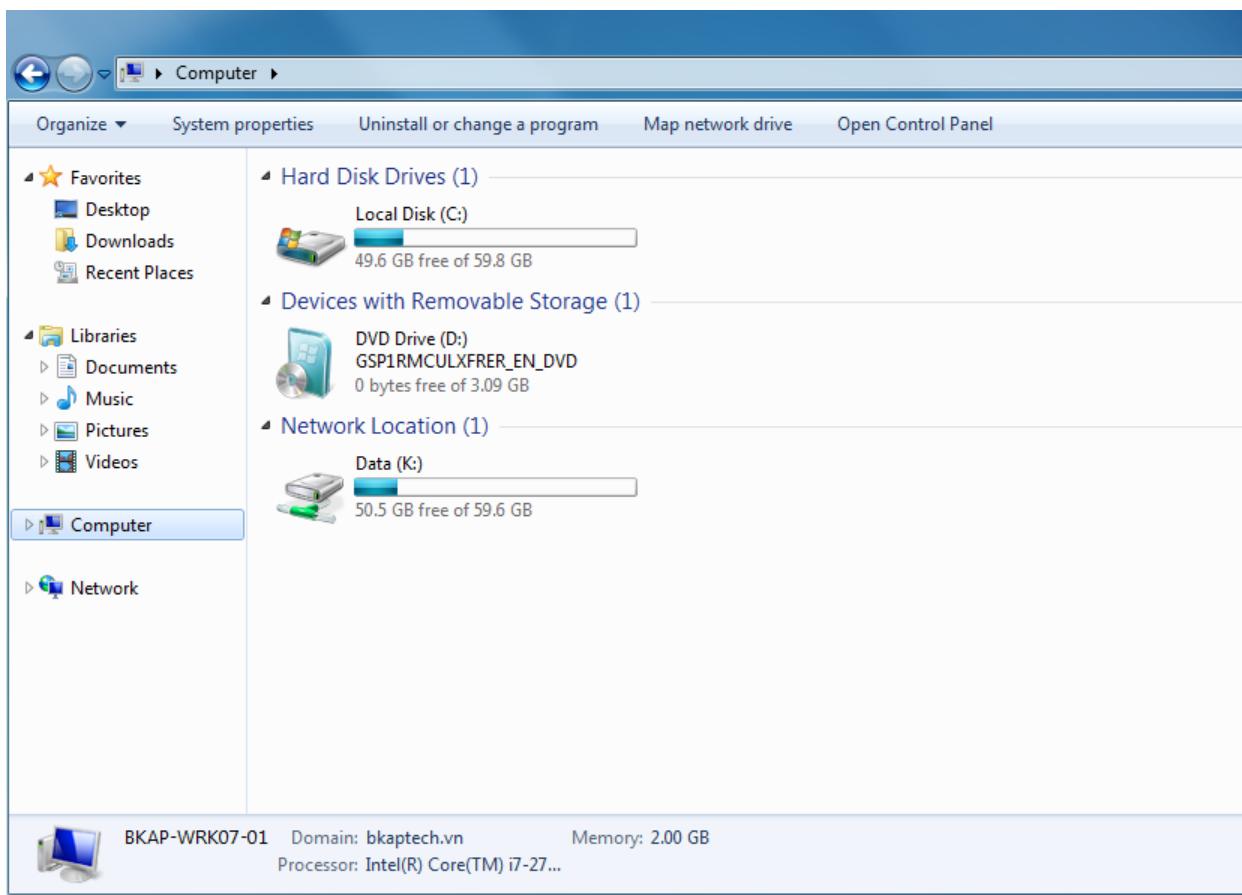
Computer Policy update has completed successfully.
User Policy update has completed successfully.

C:\Users\Administrator>
```

- Chuyển sang máy Client *BKAP-WRK07-01* , Join vào miền , đăng nhập bằng user **hungnq** để kiểm tra.



- Các chính sách đã được áp dụng sang máy Client.



Control Panel > Hardware and Sound > Devices and Printers

Add a device Add a printer See what's printing Print server properties Remove device

Windows can display enhanced device icons and information from the Internet. Click to change...

Devices (4)

- BKAP-WRK07-01
- Generic Non-PnP Monitor
- VMware Virtual USB Mouse
- VMware, VMware Virtual S SCSI Disk Device

Printers and Faxes (3)

- Fax
- HP LaserJet on BKAP-DC12-01
- Microsoft XPS Document Writer

HP LaserJet on BKAP-DC12-01 State: Status: 0 document(s) in queue
Model: HP Color LaserJet 2605 ...
Category: Printer

Bài 6:**CẤU HÌNH FOLDER REDIRECTION****1. Yêu cầu bài lab:**

+ Chuyển hướng thư mục “**Desktop, Documents, My Documents**” từ các User **Ketoan1** và **Ketoan2** về thư mục chia sẻ của Server **BKAP-DC12-01**.

- Trên máy Server **BKAP-DC12-01**, thực hiện các bước :
 - Tạo 1 thư mục có tên “**Folder Redirection**” và chia sẻ ẩn.
 - Tạo **OU Ketoan**, tạo 2 tài khoản **ketoan1** và **ketoan2**.
 - Triển khai chính sách **GPO** cho toàn bộ phòng ban **Ketoan**.
- Trên máy Client **BKAP-WRK08-01** và **BKAP-WRK08-02**, thực hiện các bước:
 - Đăng nhập tài khoản **ketoan1** để kiểm tra.
 - Đăng nhập tài khoản **ketoan2** để kiểm tra.

2. Yêu cầu chuẩn bị:

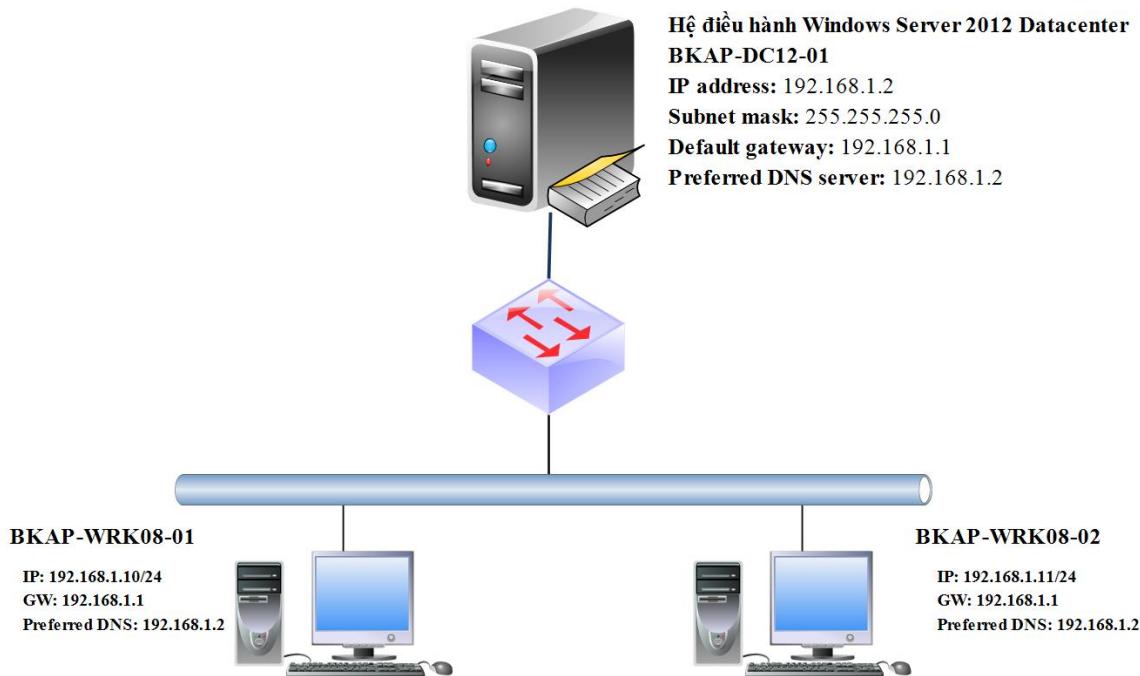
+ Máy Server **BKAP-DC12-01** đã nâng cấp lên Domain Controller quản lý miền **bkaptech.vn**.

+ Máy Client **BKAP-WRK08-01** và **BKAP-WRK08-02** đã Join vào miền **bkaptech.vn**.

3. Mô hình lab:

HỆ THỐNG ĐÀO TẠO CNTT QUỐC TẾ BACHKHOA-APTECH

Lab 6.2 Cấu hình Folder Redirection trên Windows Server 2012



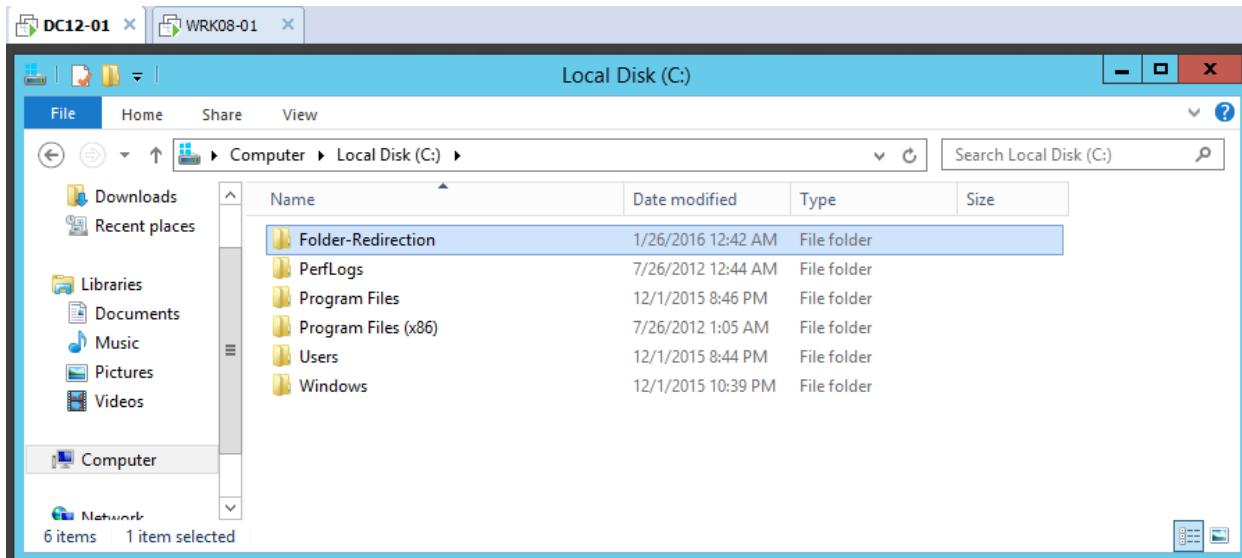
Hình 6.2

Sơ đồ địa chỉ như sau:

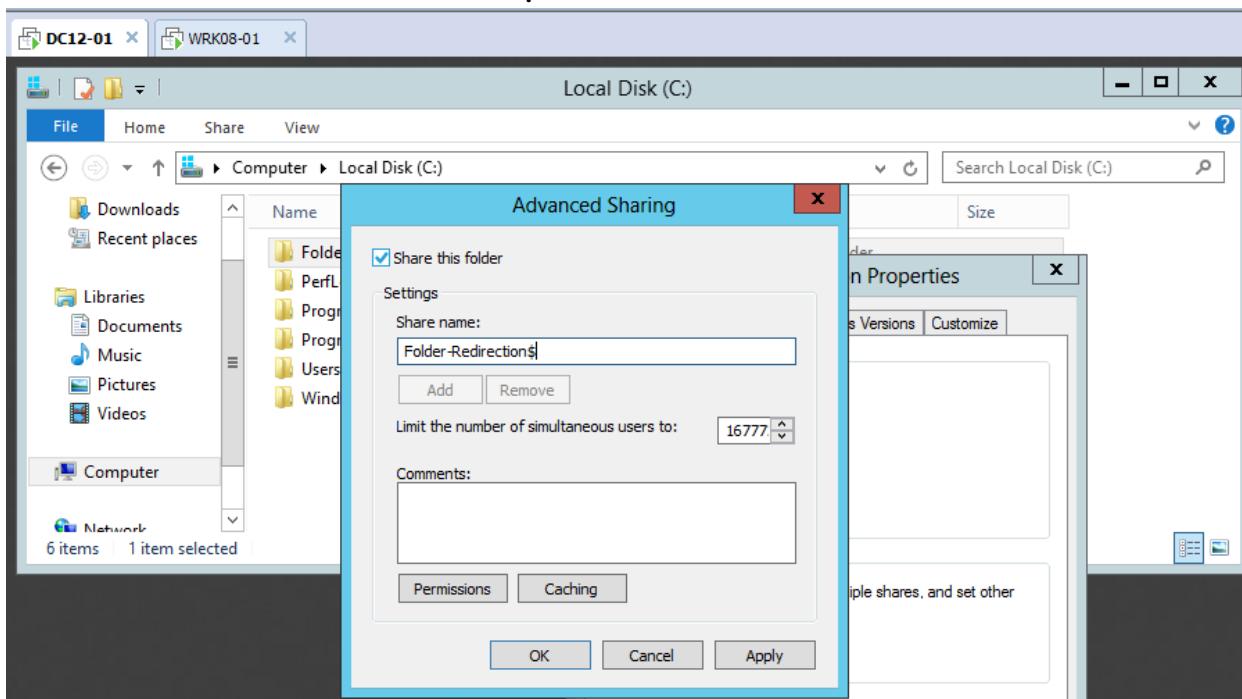
Thông số	BKAP-DC12-01	BKAP-WRK08-01
<i>IP address</i>	192.168.1.2	192.168.1.10
<i>Subnet Mask</i>	255.255.255.0	255.255.255.0
<i>Gateway</i>	192.168.1.1	192.168.1.1
<i>DNS Server</i>	192.168.1.2	192.168.1.2

Hướng dẫn chi tiết:

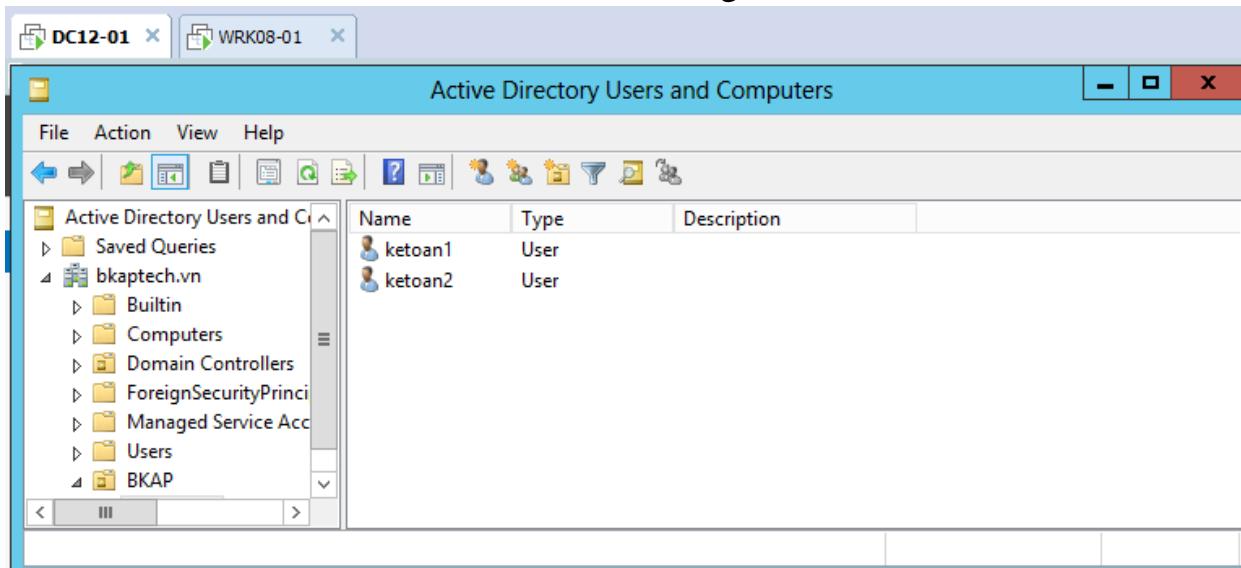
- Trên máy **BKAP-DC12-01**, thực hiện:
 - Tạo thư mục tên **Folder-Redirection** và chia sẻ ẩn thư mục.



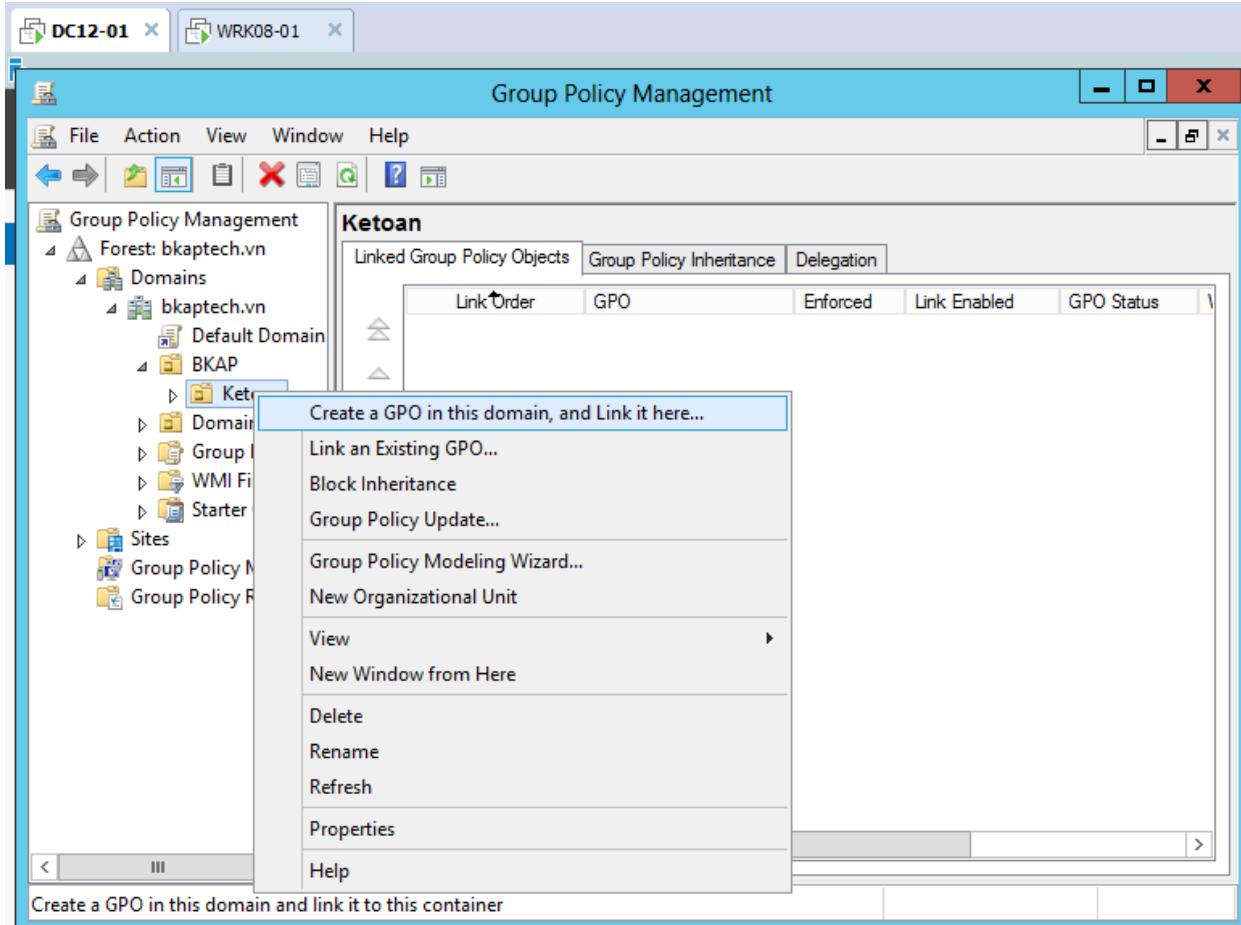
▪ Share ẩn thư mục :



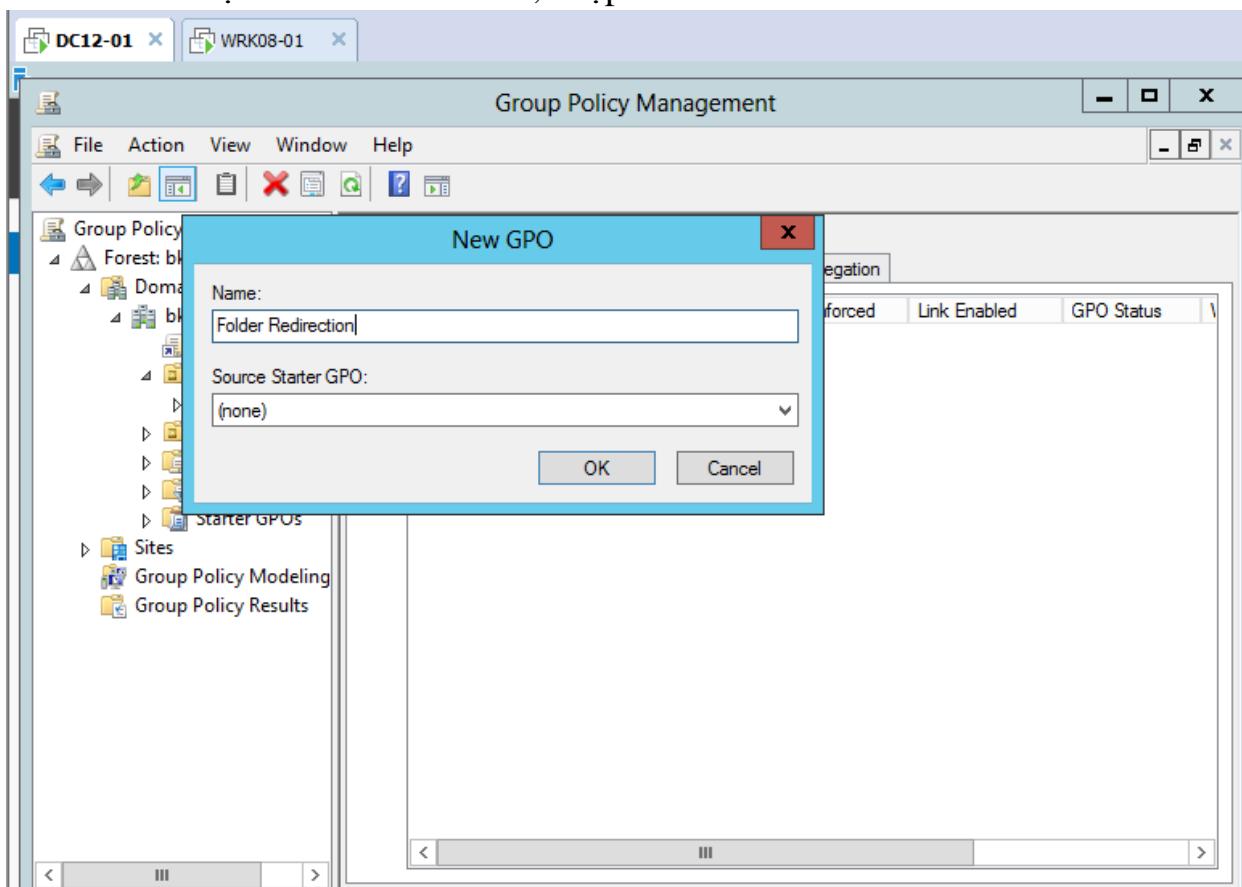
- Tạo OU **BKAP**, trong OU **BKAP** tiến hành tạo OU **Ketoan**, tạo các tài khoản **ketoan1** và **ketoan2** trong OU **Ketoan**.



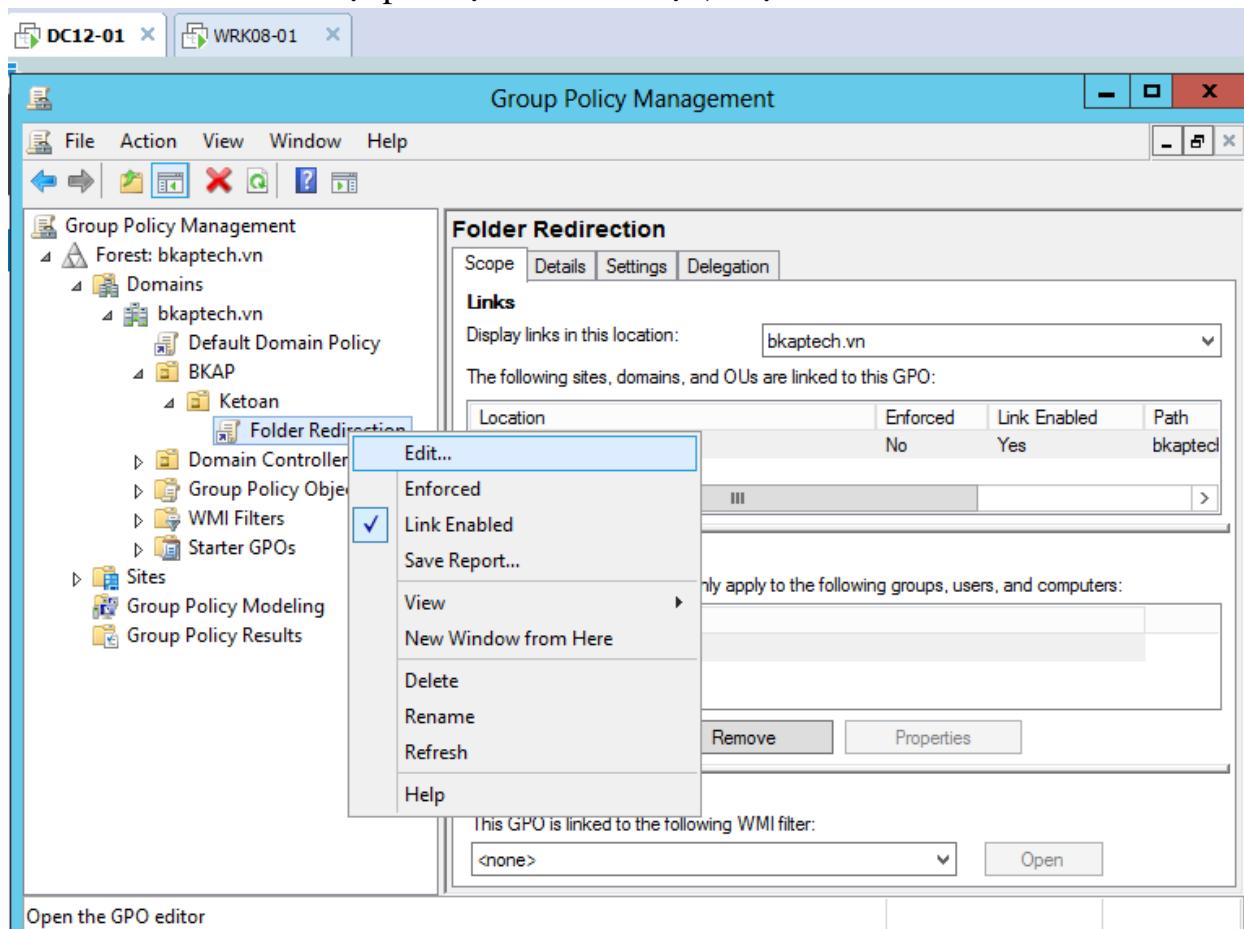
- Thực hiện triển khai chính sách **GPO** cho phòng ban **Ketoan**.
 - Vào **Group Policy Management**, click chuột phải tại OU **Ketoan**, chọn **Create a GPO in this domain, and Link it here...**



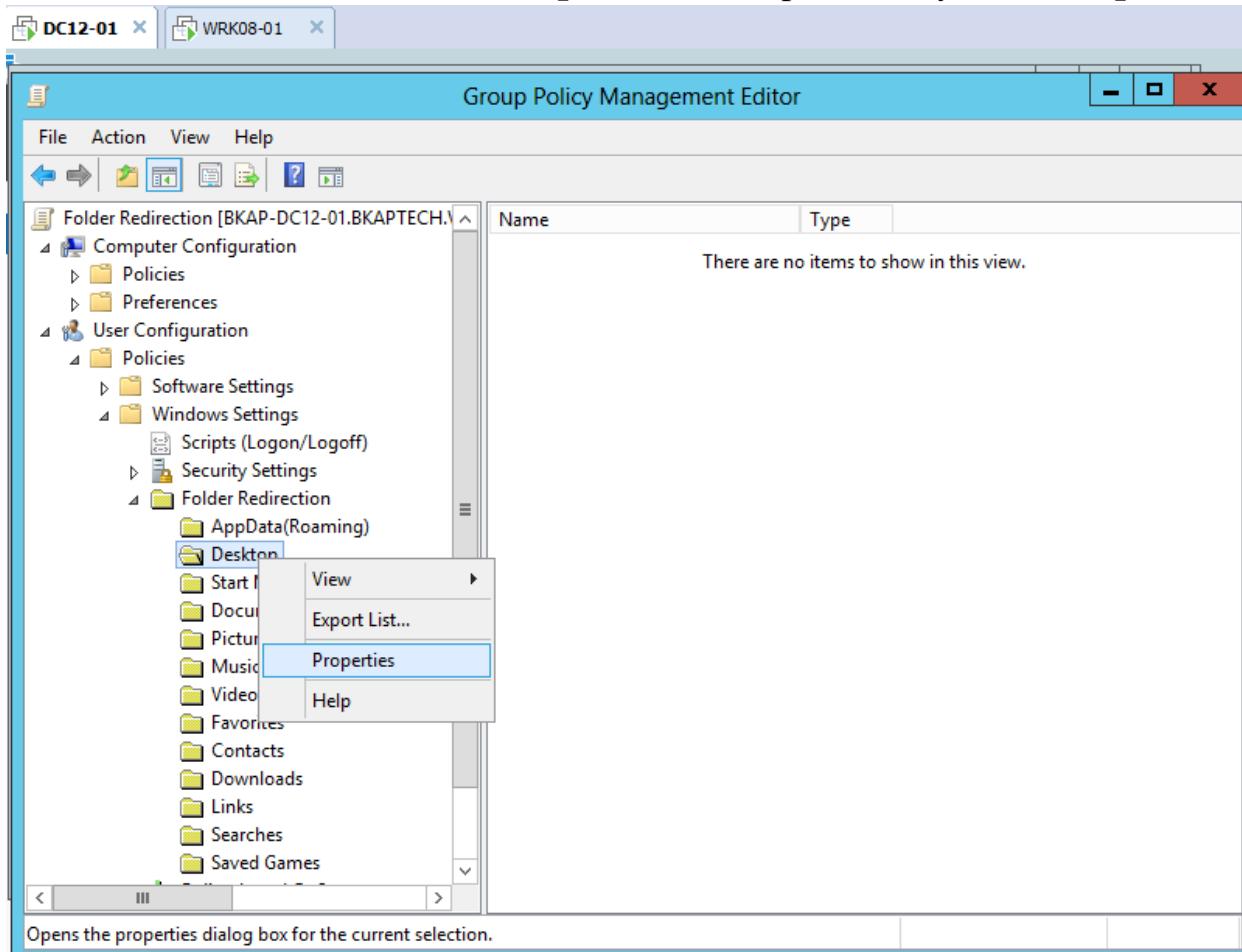
- Tại cửa sổ **New GPO**, nhập vào tên **GPO Folder Redirection**.



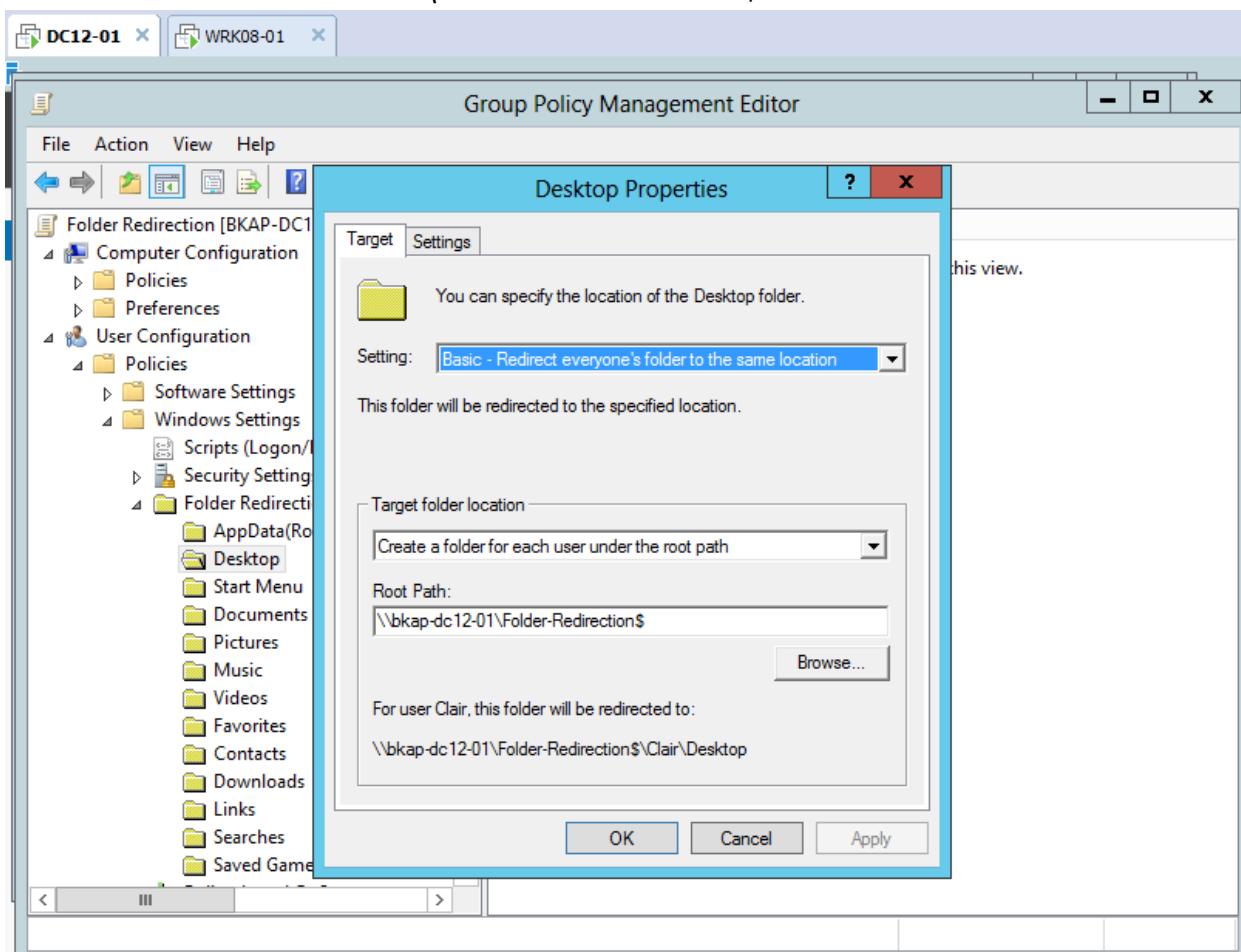
- Click chuột phải tại GPO vừa tạo, chọn Edit.



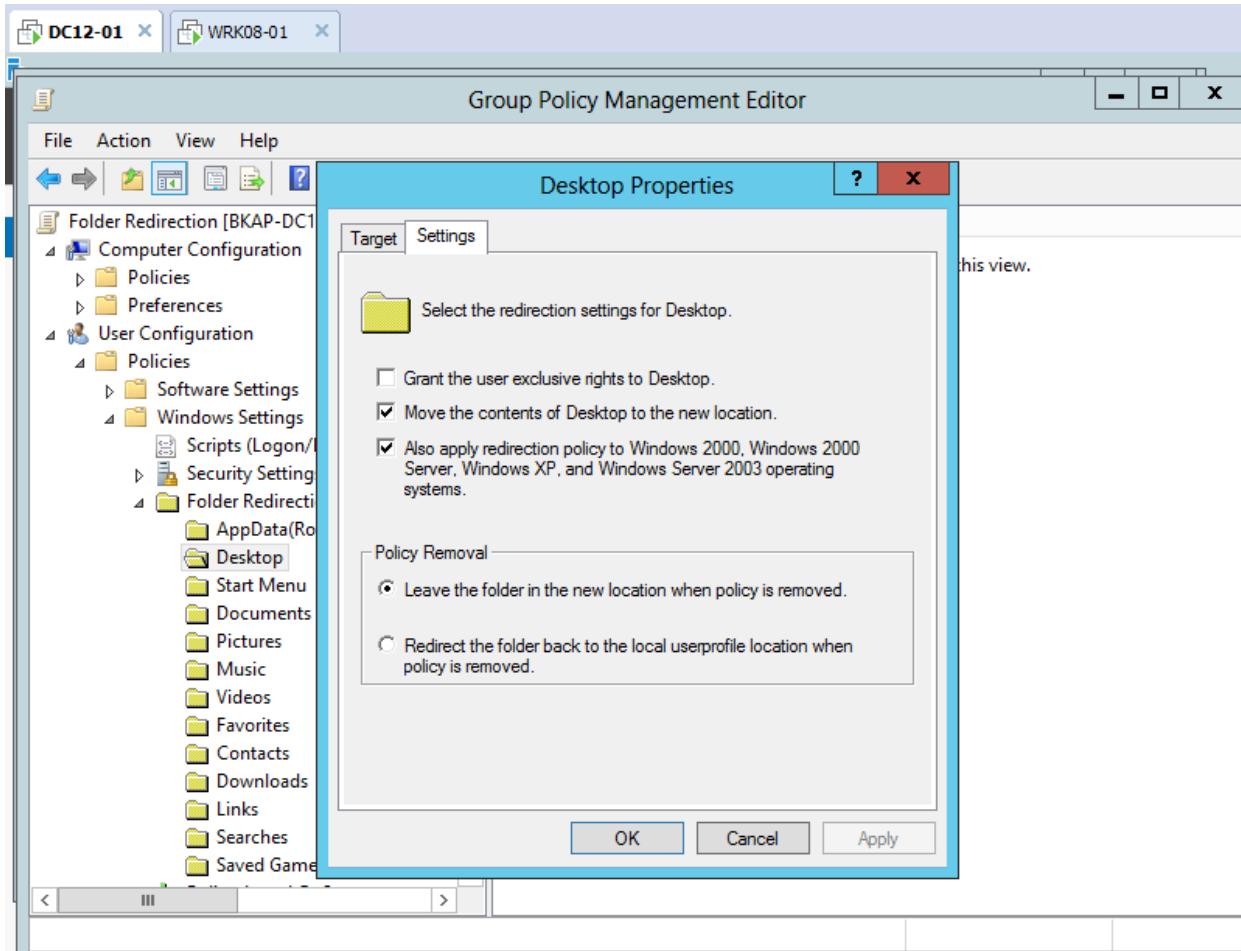
- Tại cửa sổ **Group Policy Management Editor**, chọn vào **User Configuration / Policies / Security Settings / Folder Redirection**.
 - Chọn vào **Desktop** / click chuột phải tại đây, chọn **Properties**



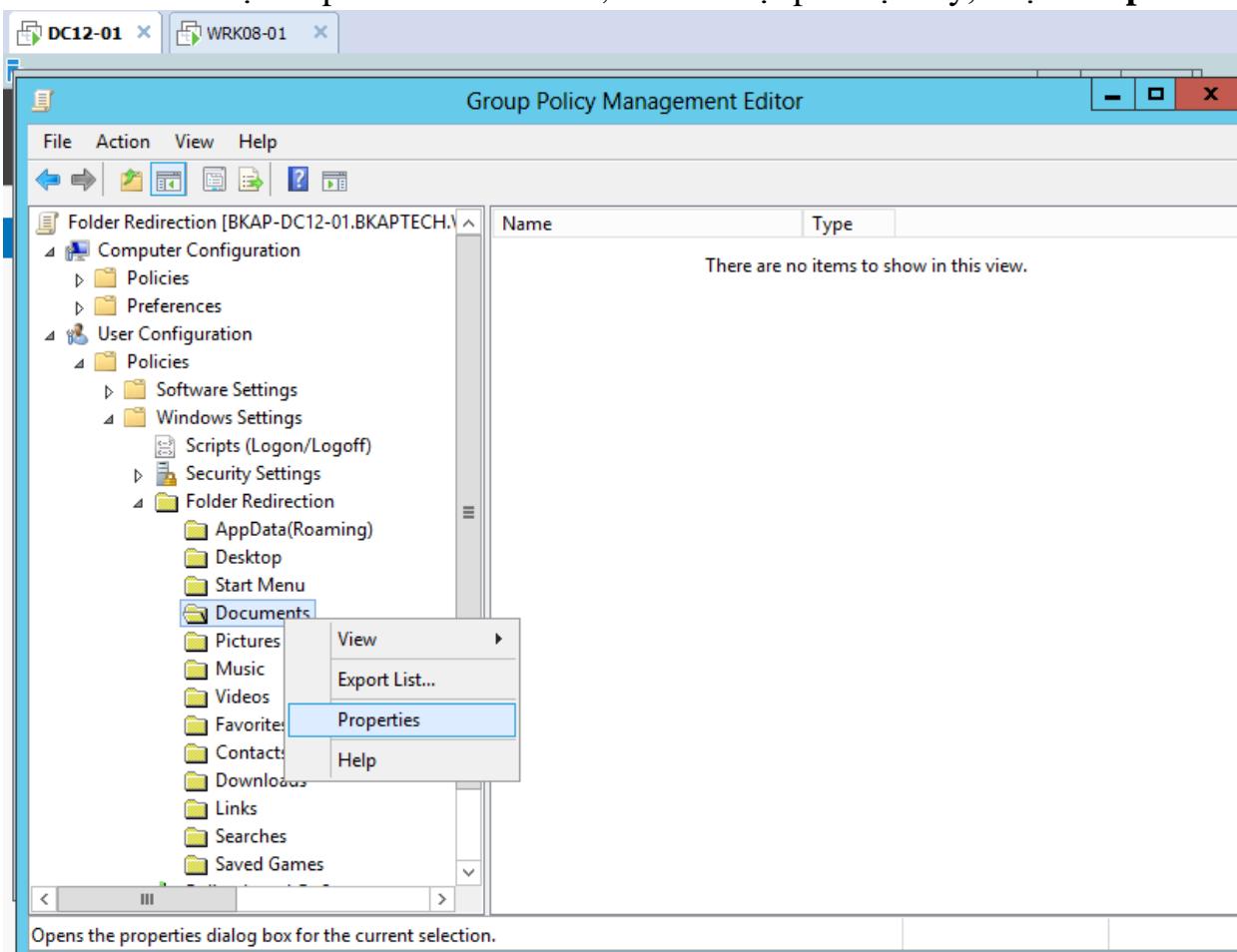
- Tại cửa sổ **Desktop Properties** :
 - Tab Target, tại mục Setting, chọn vào **Basic – Redirect everyone's folder to the same location.**
 - Tại mục **Root Path**, nhập vào đường dẫn **\bkap-dc12-01\Folder-Redirection\$**.



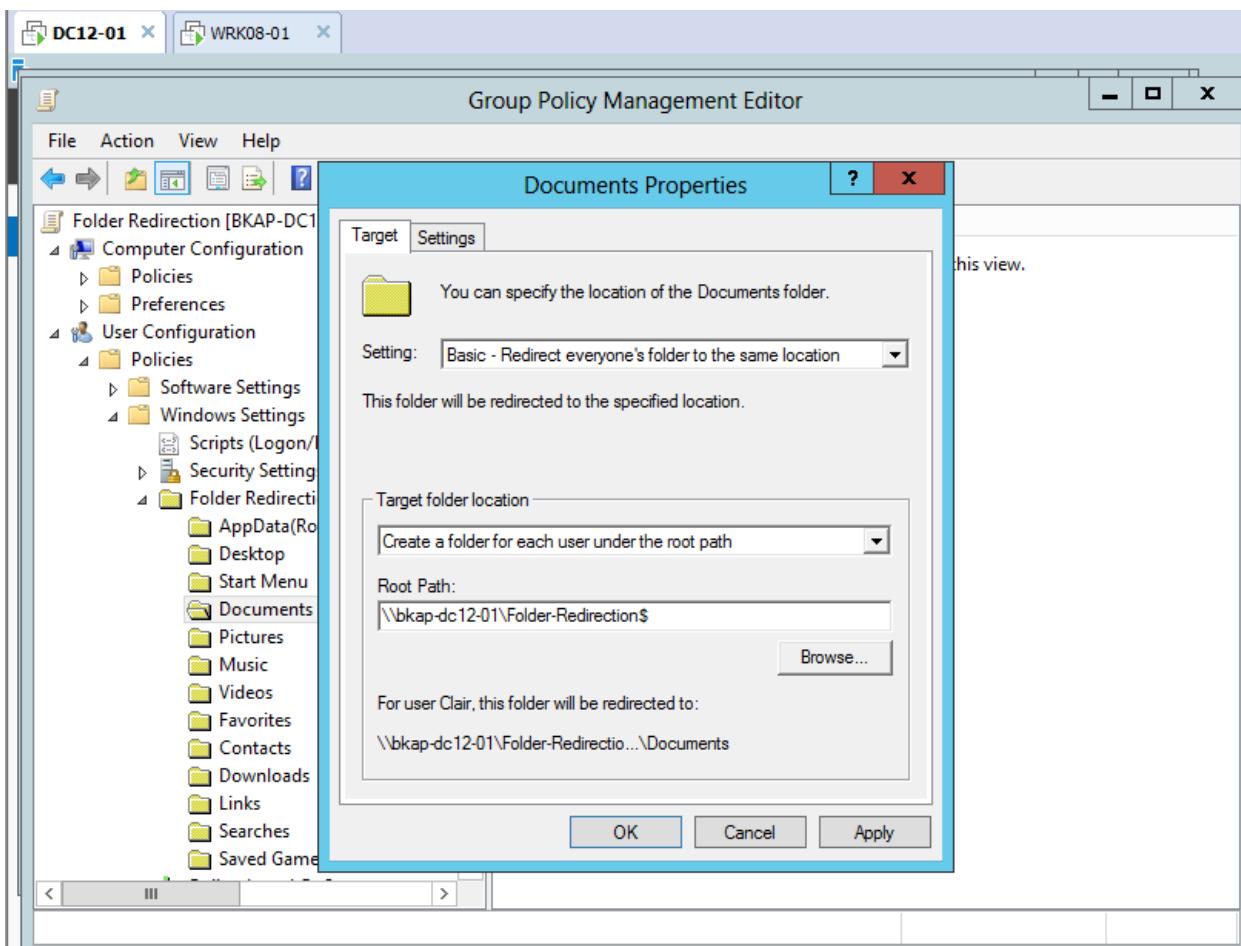
- Chuyển sang Tab **Settings**, bỏ chọn tại dòng **Grant the user exclusive rights to Desktop**, click chọn vào dòng **Also apply redirection policy to**
- **Apply, OK.**

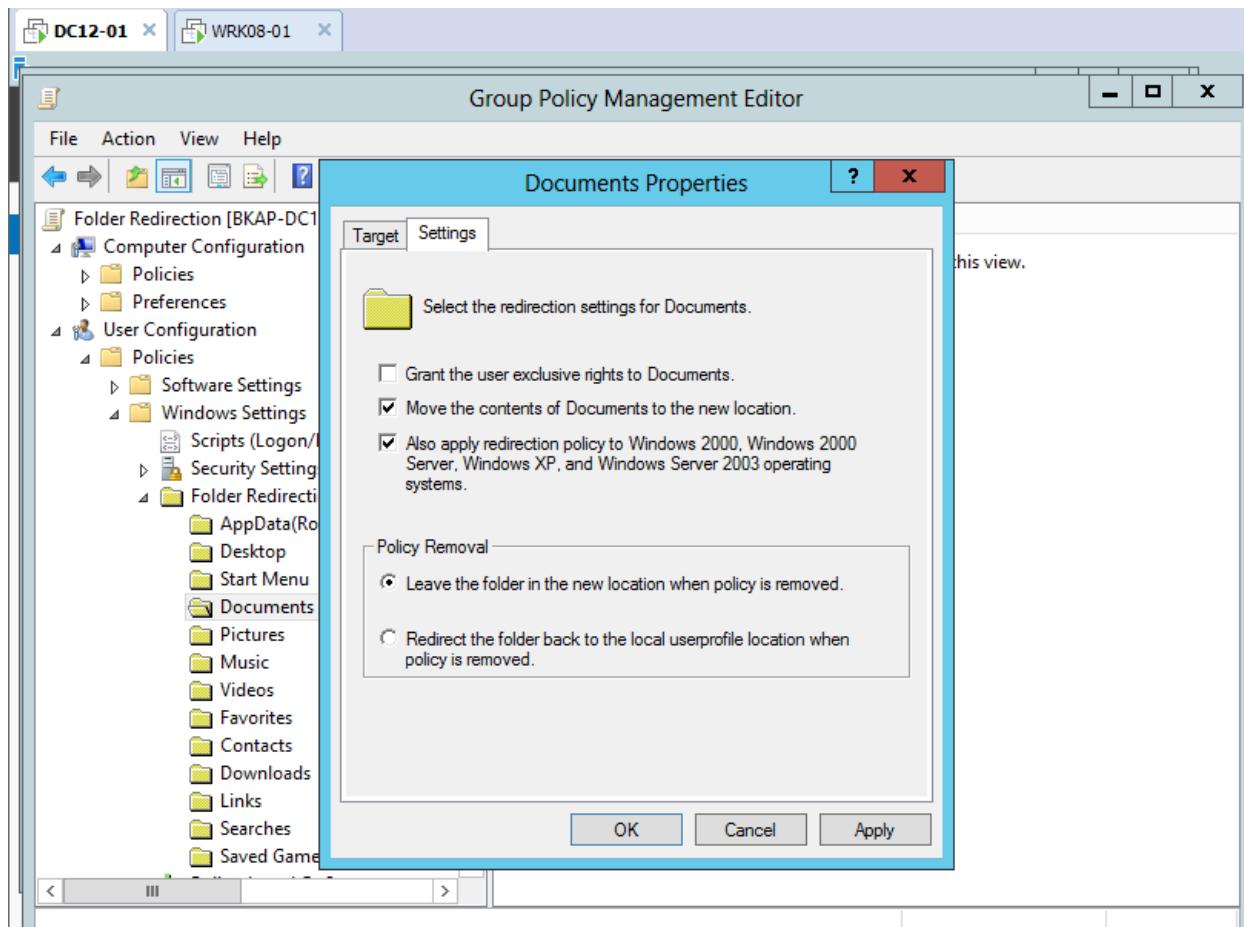


- Chọn tiếp vào **Documents** , click chuột phải tại đây, chọn **Properties**.

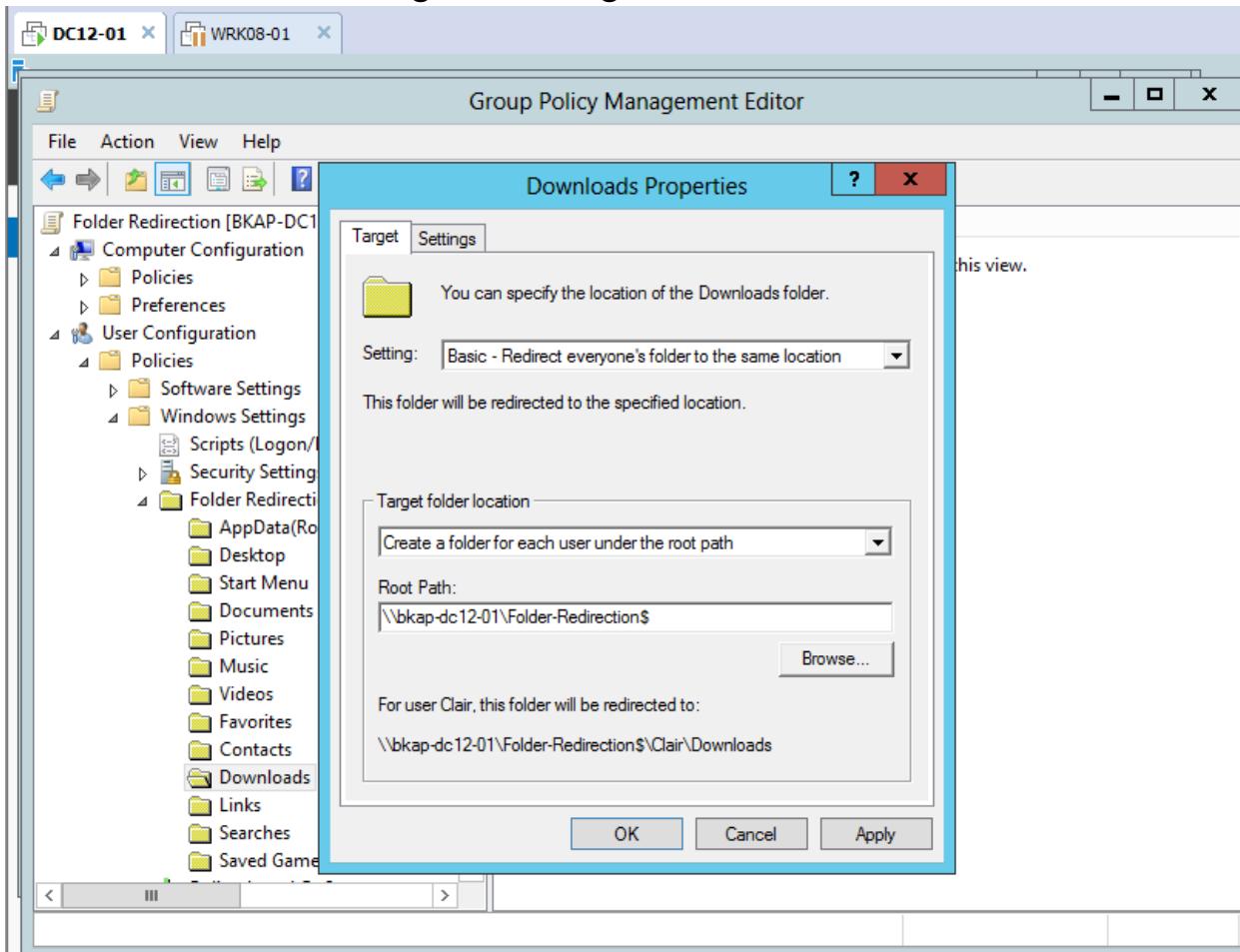


- Tại cửa sổ **Document Properties**, làm tương tự như trên. Kết quả như sau:

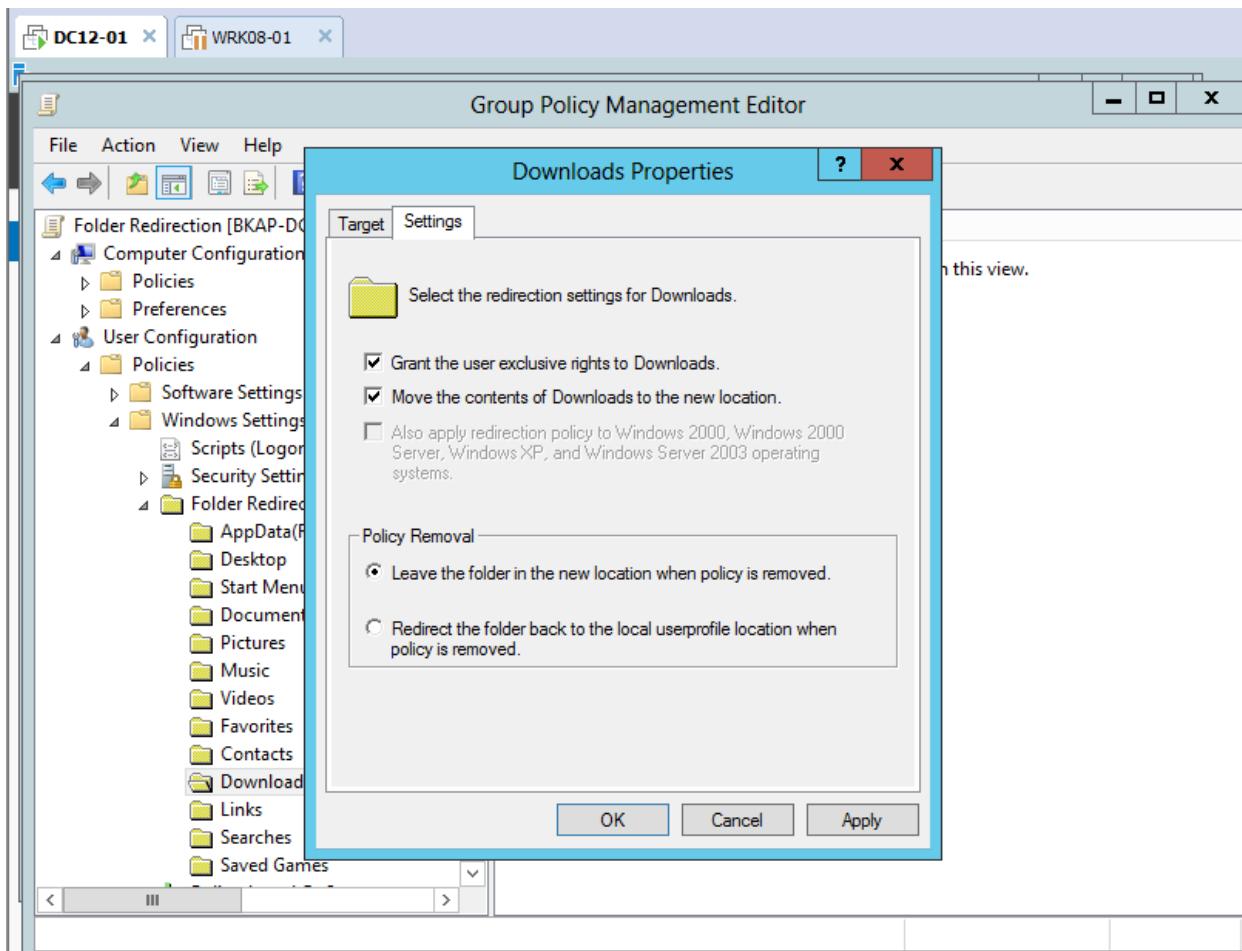




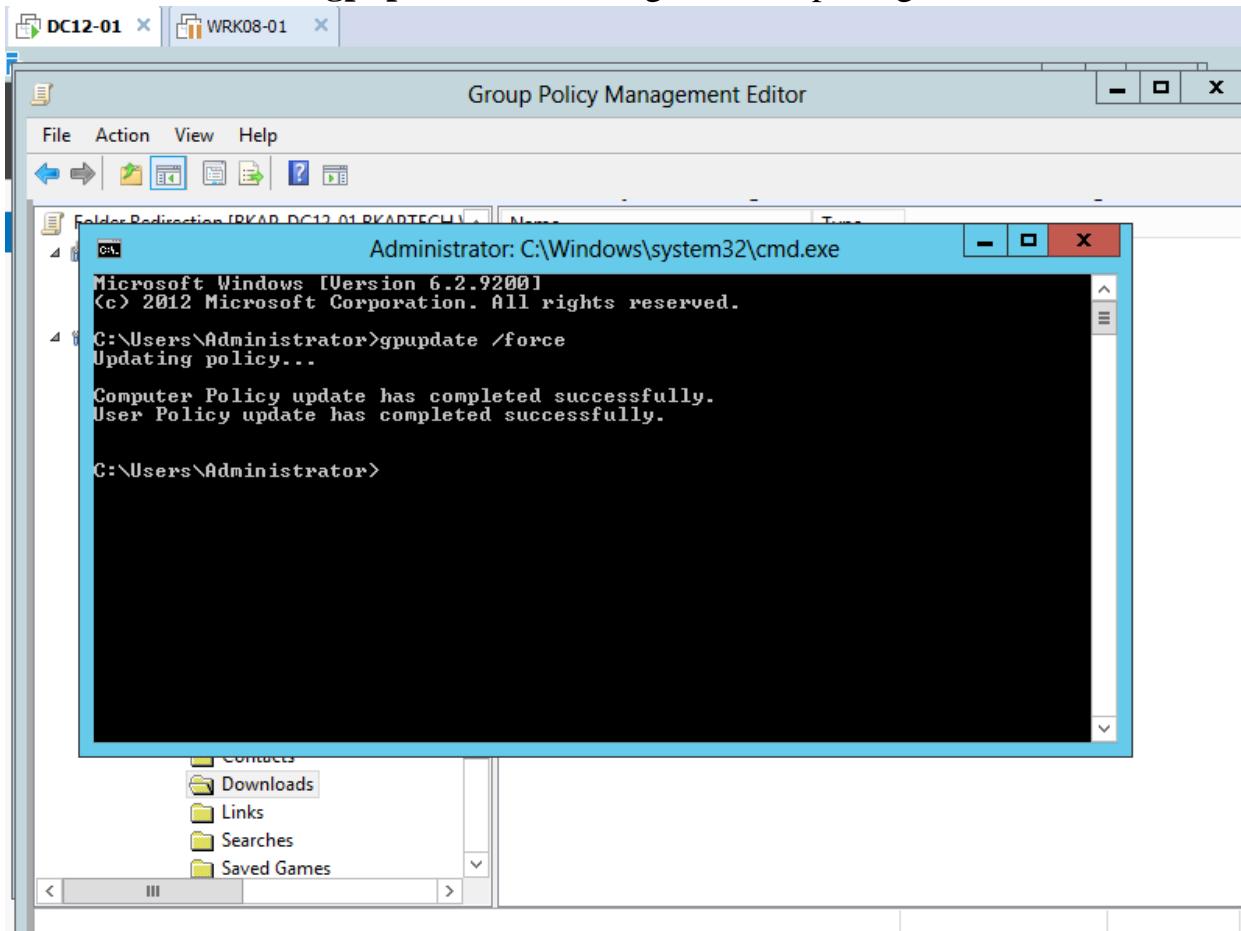
- Click chuột phải tại **Downloads**, tại cửa sổ **Downloads Properties**:
 - Tab Target làm tương tự như trên.



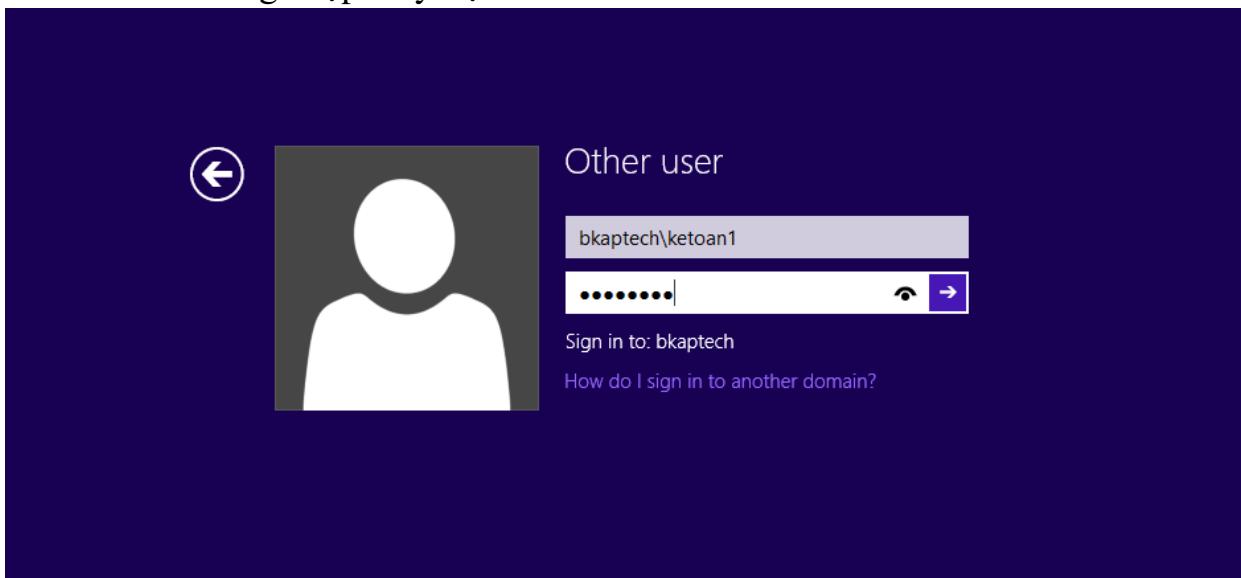
- Tab **Settings**, click chọn vào **Grant the user...** và **Move the contents...**



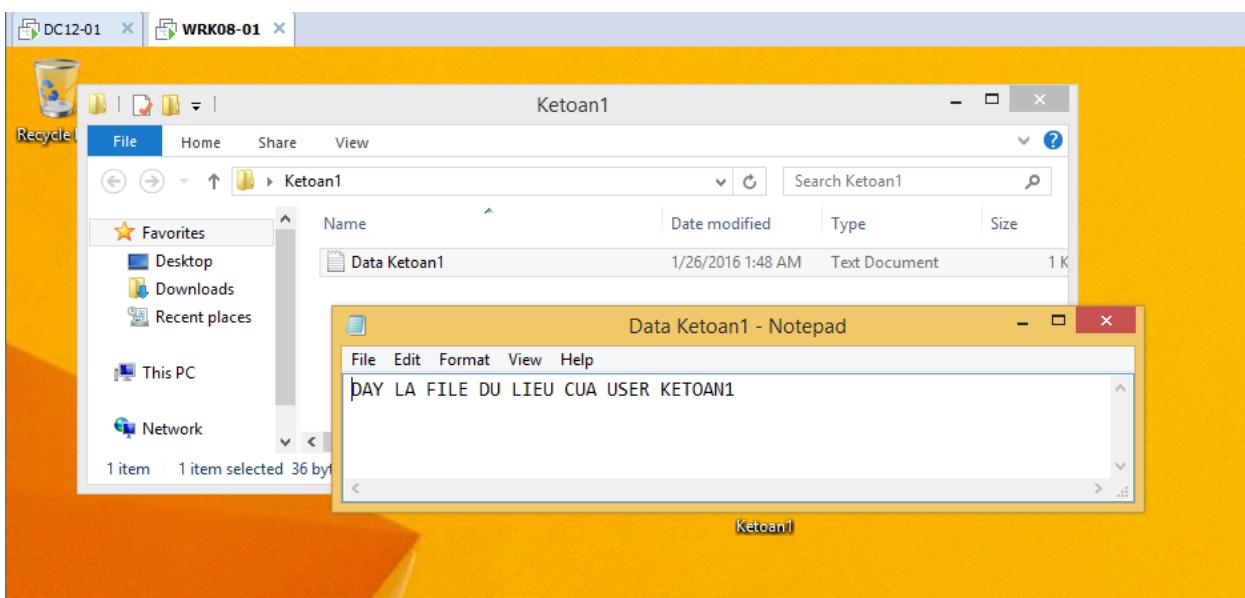
- Gõ lệnh **gpupdate /force** trong **cmd** để áp dụng chính sách vừa tạo.



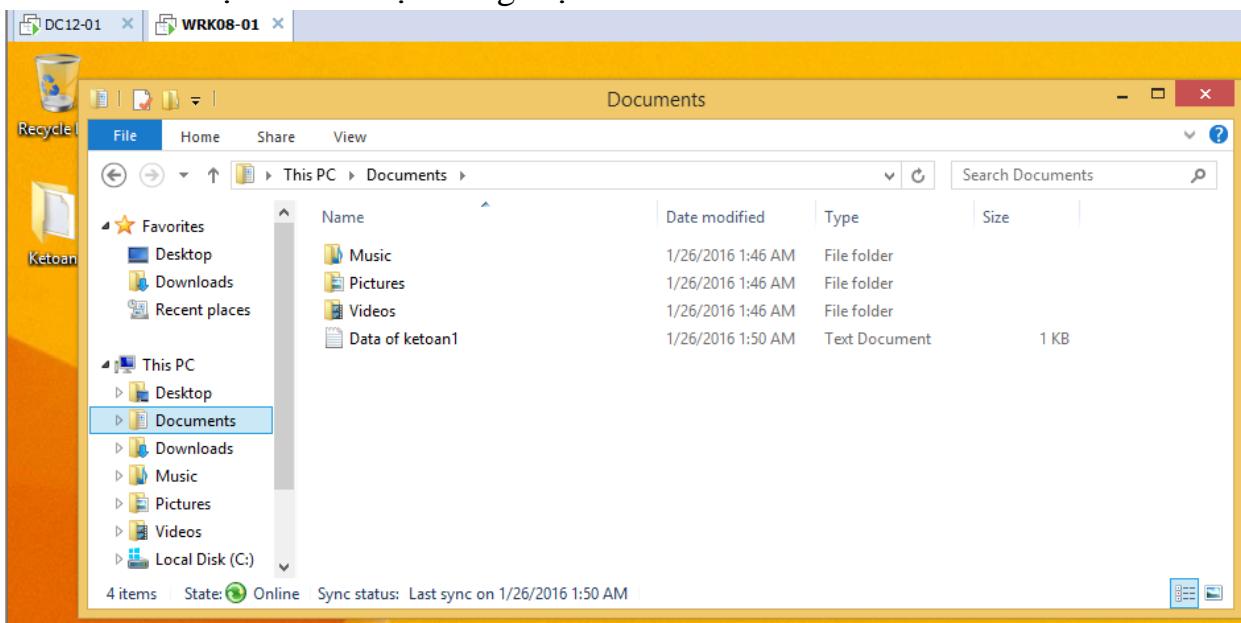
- Chuyển sang máy trạm *BKAP-WRK08-01* đăng nhập với 2 tài khoản **ketoan1** và **ketoan2**.
 - Đăng nhập máy trạm với tài khoản **ketoan1**.



- Tạo thư mục và file dữ liệu ở ngoài Desktop để kiểm tra.

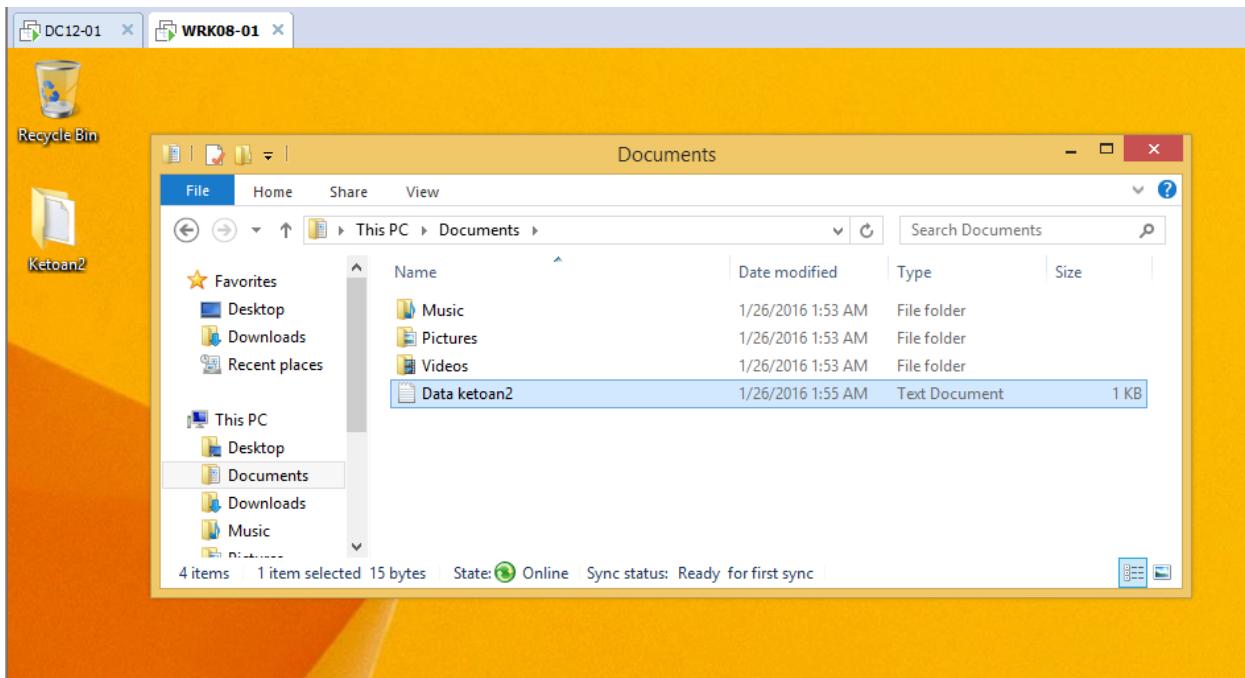


- Tạo file dữ liệu trong mục **Documents**.

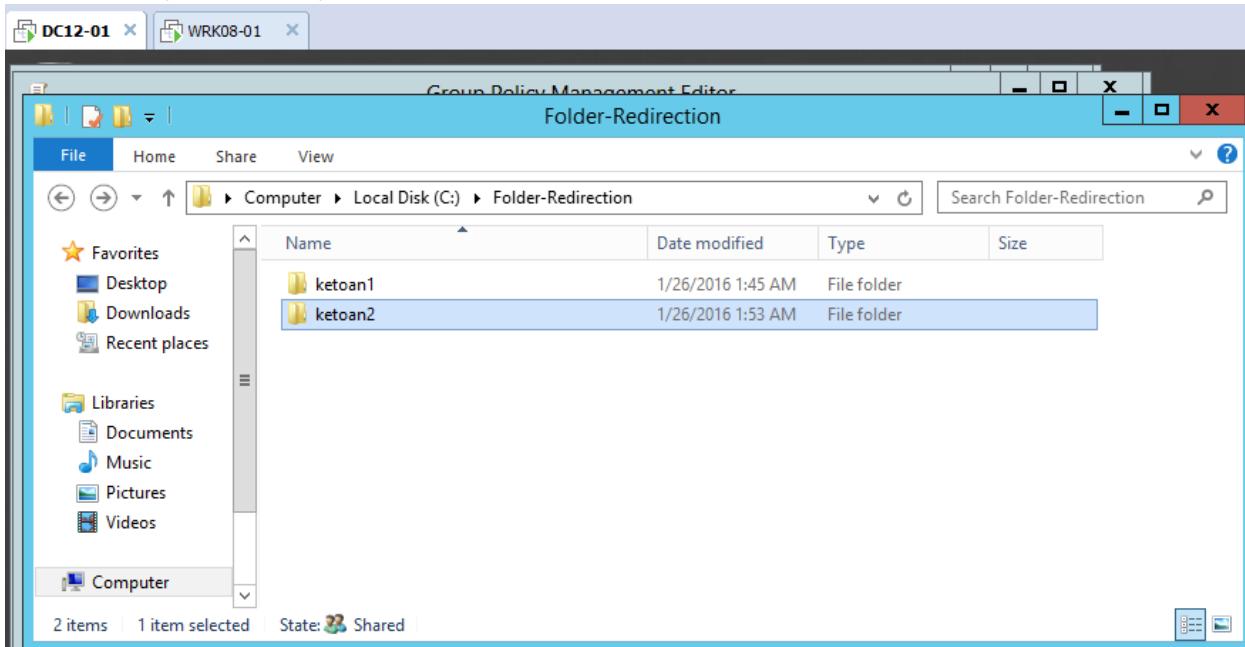


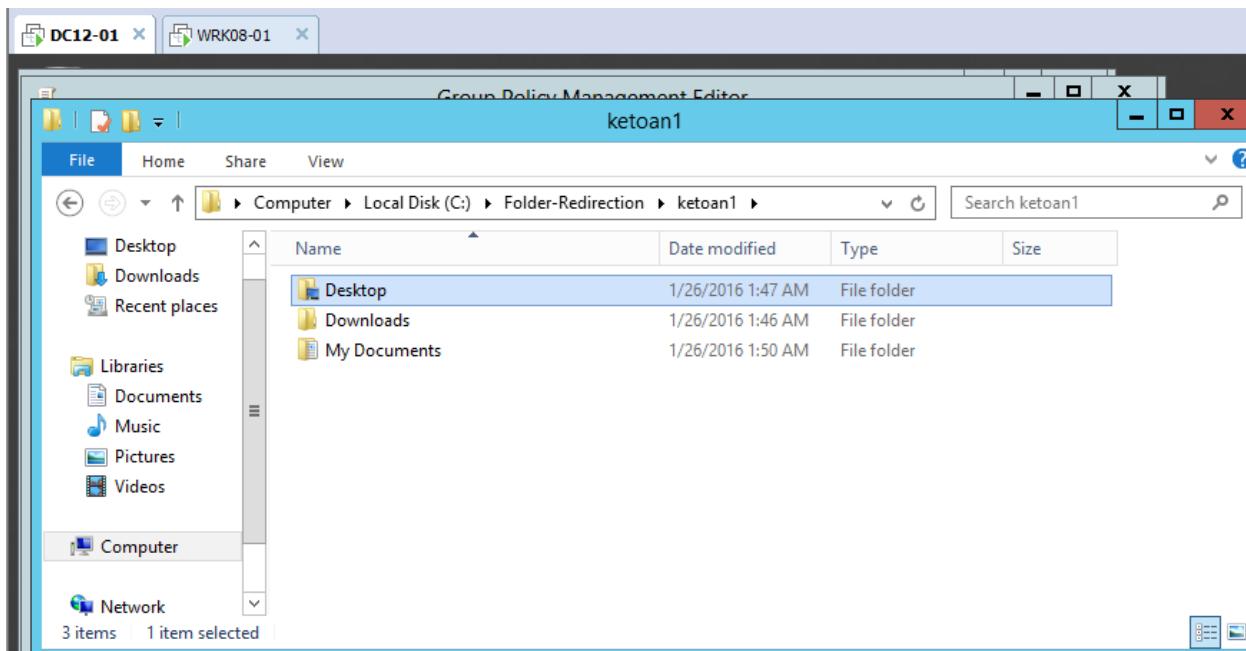
- Logout tài khoản **ketoan1**, đăng nhập tài khoản **ketoan2**, tạo các folder và file dữ liệu tương tự.





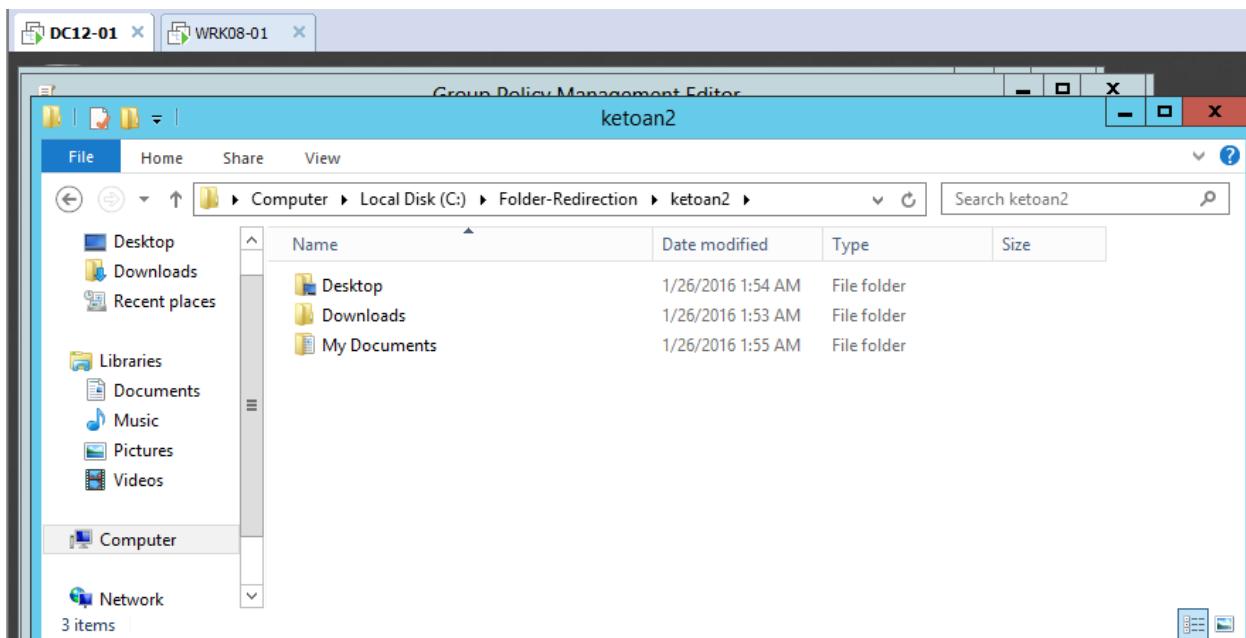
- Chuyển về máy BKAP-DC12-01 để kiểm tra.





The screenshot shows the Group Policy Management Editor window for a user named ketoan1. The navigation pane on the left lists 'Computer' and 'Network'. The main pane displays a file list under 'Computer > Local Disk (C:) > Folder-Redirection > ketoan1'. The list contains three items: Desktop, Downloads, and My Documents, all of which are file folders. The desktop icons on the left include Desktop, Downloads, Recent places, Libraries, and a Computer icon.

Name	Date modified	Type
Desktop	1/26/2016 1:47 AM	File folder
Downloads	1/26/2016 1:46 AM	File folder
My Documents	1/26/2016 1:50 AM	File folder



The screenshot shows the Group Policy Management Editor window for a user named ketoan2. The navigation pane on the left lists 'Computer' and 'Network'. The main pane displays a file list under 'Computer > Local Disk (C:) > Folder-Redirection > ketoan2'. The list contains three items: Desktop, Downloads, and My Documents, all of which are file folders. The desktop icons on the left include Desktop, Downloads, Recent places, Libraries, and a Computer icon.

Name	Date modified	Type
Desktop	1/26/2016 1:54 AM	File folder
Downloads	1/26/2016 1:53 AM	File folder
My Documents	1/26/2016 1:55 AM	File folder

Bài 7:**TRIỂN KHAI CÀI ĐẶT VÀ CẤU HÌNH DỊCH VỤ VPN SERVER****Các nội dung chính sẽ được đề cập:**

- ✓ Triển khai cài đặt và cấu hình dịch vụ VPN Server (Client to Site).
- ✓ Triển khai cài đặt và cấu hình dịch vụ VPN Server (Site to Site).
- ✓ Triển khai cài đặt và cấu hình dịch vụ VPN Server (Client to Site) – SSTP.

7.1 Triển khai cấu hình dịch vụ VPN Server (Client to Site)**1. Yêu cầu bài lab:**

+ Trên máy *BKAP-SRV12-01*, xây dựng làm máy chia sẻ tài nguyên với thư mục Data.

+ Trên máy *BKAP-SRV12-02*, thực hiện các công việc sau:

- Tạo tài khoản dùng để thiết lập dịch vụ **VPN**.
- Cài đặt dịch vụ **Remote Access**.
- Cấu hình **VPN Server** cho *remote client* với giao thức **PPTP**. **VPN Server** cấp dải địa chỉ cho *Client* truy cập vào là *10.0.0.10 – 10.0.0.60*.
- Trên máy *BKAP-WRK08-01* thực hiện cài đặt **VPN client** và *kết nối*.

2. Yêu cầu chuẩn bị:

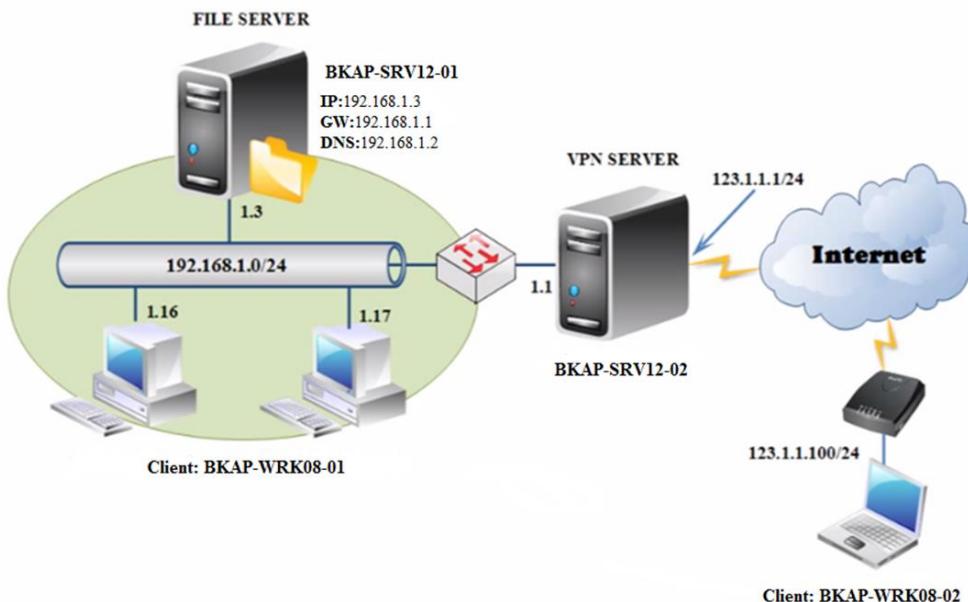
+ Chuẩn bị 2 máy *Server* và 1 máy *Client*.

Sử dụng máy *BKAP-SRV12-01* làm **VPN Server** có 2 card mạng: Card mạng 1 ứng với *LAN*, Card mạng 2 ứng với *WAN*.

+ Từ máy *BKAP-WRK08-01* ping thông tới máy *BKAP-SRV12-02* với địa chỉ của Card mạng 2.

3. Mô hình Lab:

HỆ THỐNG ĐÀO TẠO CNTT QUỐC TẾ BACHKHOA-APTECH
Lab 7.1 Triển khai cài đặt và cấu hình dịch vụ VPN Server (Client to Site)



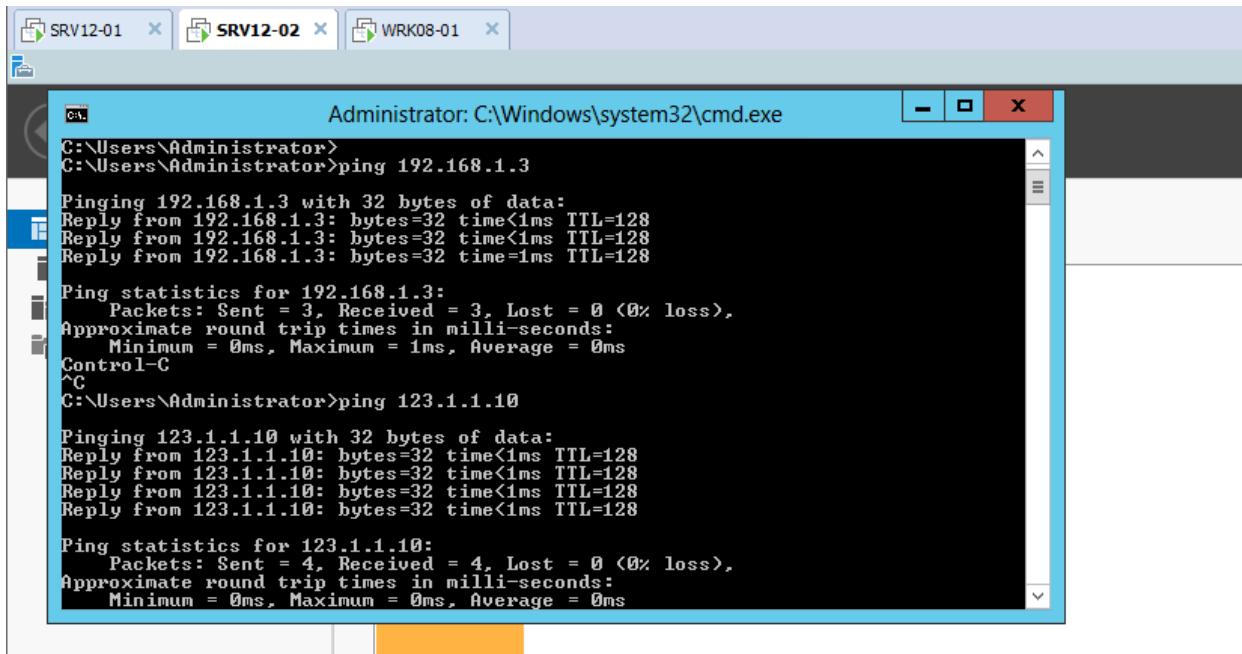
Hình 7.1

Sơ đồ địa chỉ như sau:

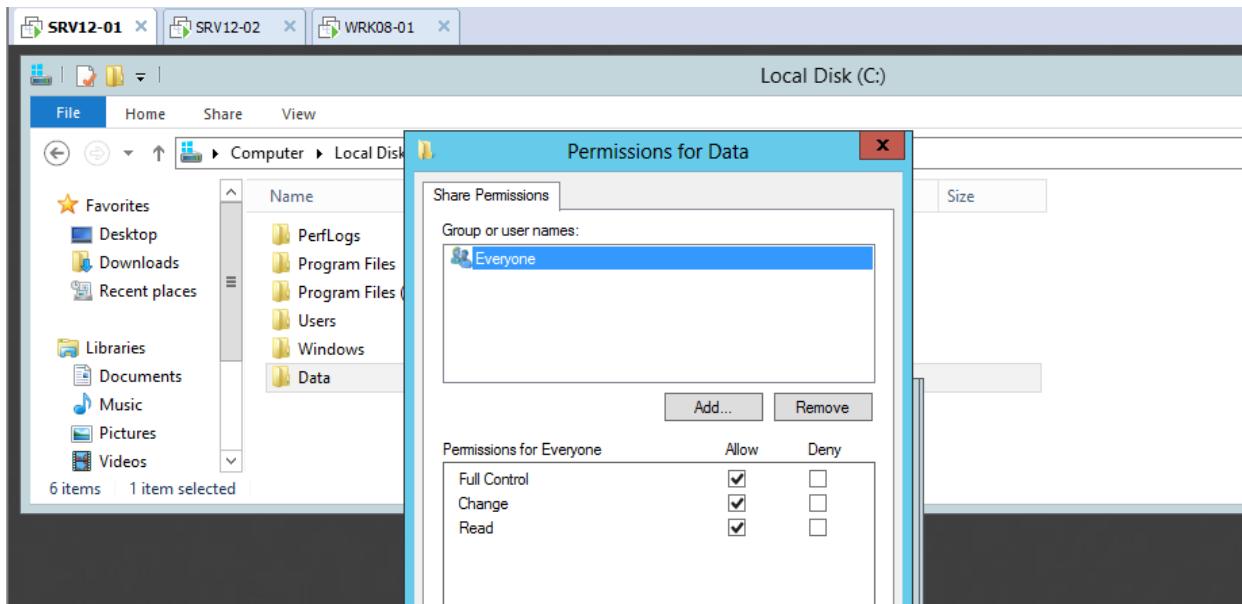
Thông số	BKAP-SRV12-01	BKAP-SRV12-02	BKAP-WRK08-01
<i>IP address</i>	192.168.1.3	LAN: 192.168.1.1 WAN: 123.1.1.1	123.1.1.10
<i>Gateway</i>	192.168.1.1	--	123.1.1.1
<i>SubnetMask</i>	255.255.255.0	255.255.255.0	255.255.255.0
<i>DNS server</i>	192.168.1.2	--	--

Hướng dẫn chi tiết:

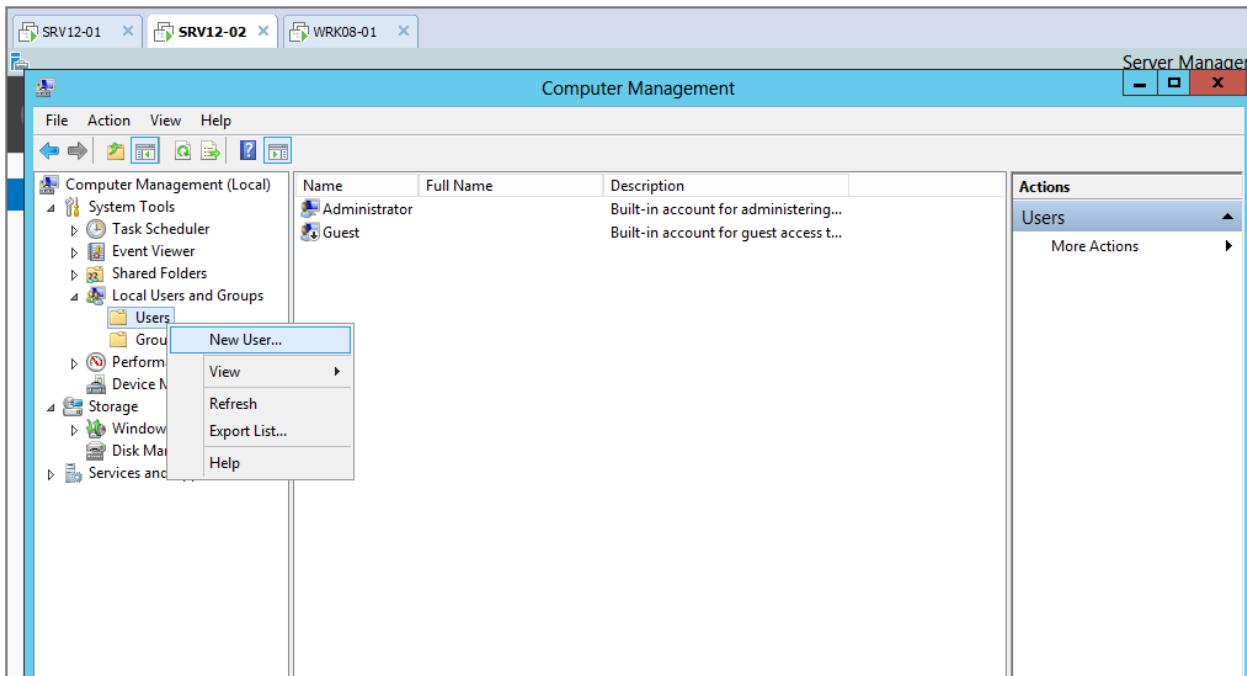
- Mở các máy ảo, đặt snapshot “Begin”, kết nối theo mô hình trên.
 - Máy **BKAP-SRV12-02** có 2 Card mạng **LAN** và **WAN**.
 - Ping thông giữa các máy kết nối trực tiếp.



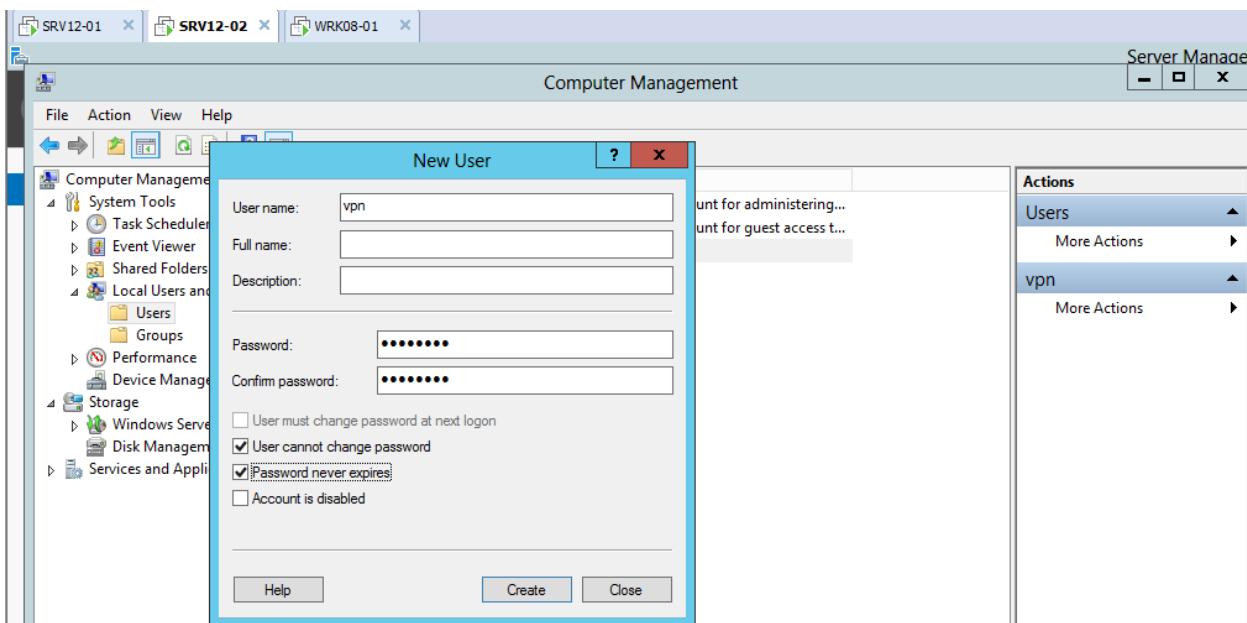
- Trên máy **BKAP-SRV12-01**, thực hiện tạo thư mục **Data** và chia sẻ dữ liệu.



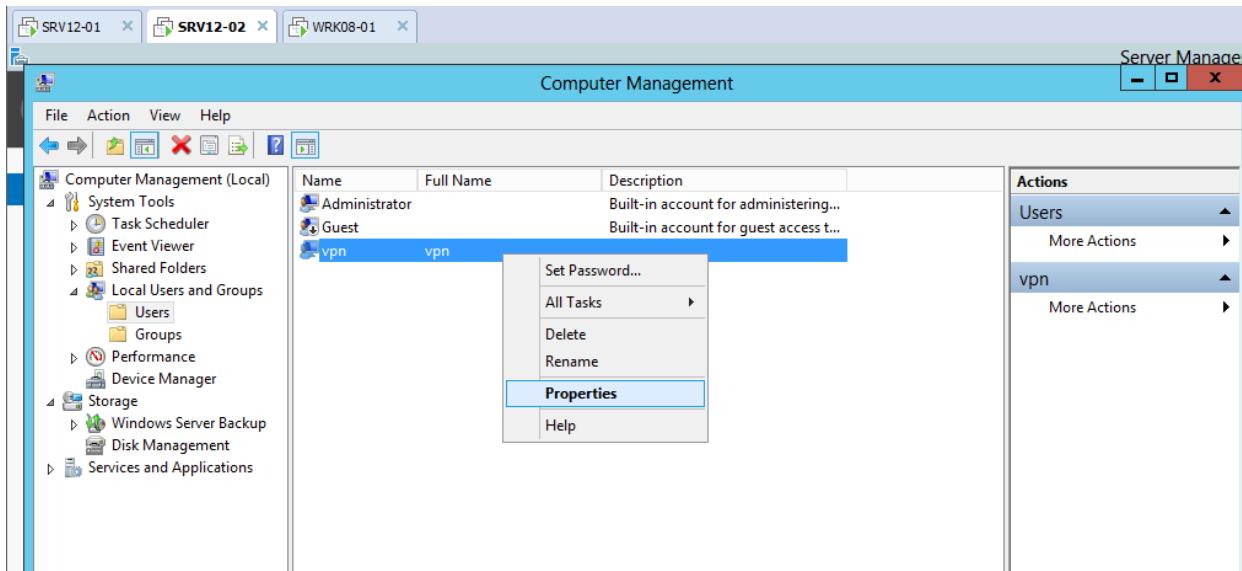
- Chuyển sang máy server *BKAP-SRV12-02*, thực hiện:
 - Tạo 1 tài khoản dùng để thiết lập dịch vụ VPN.
 - Vào **Server Manager / Tools / Computer Management** , chọn vào **Local Users and Groups /Users**, click chuột phải chọn **New User...**



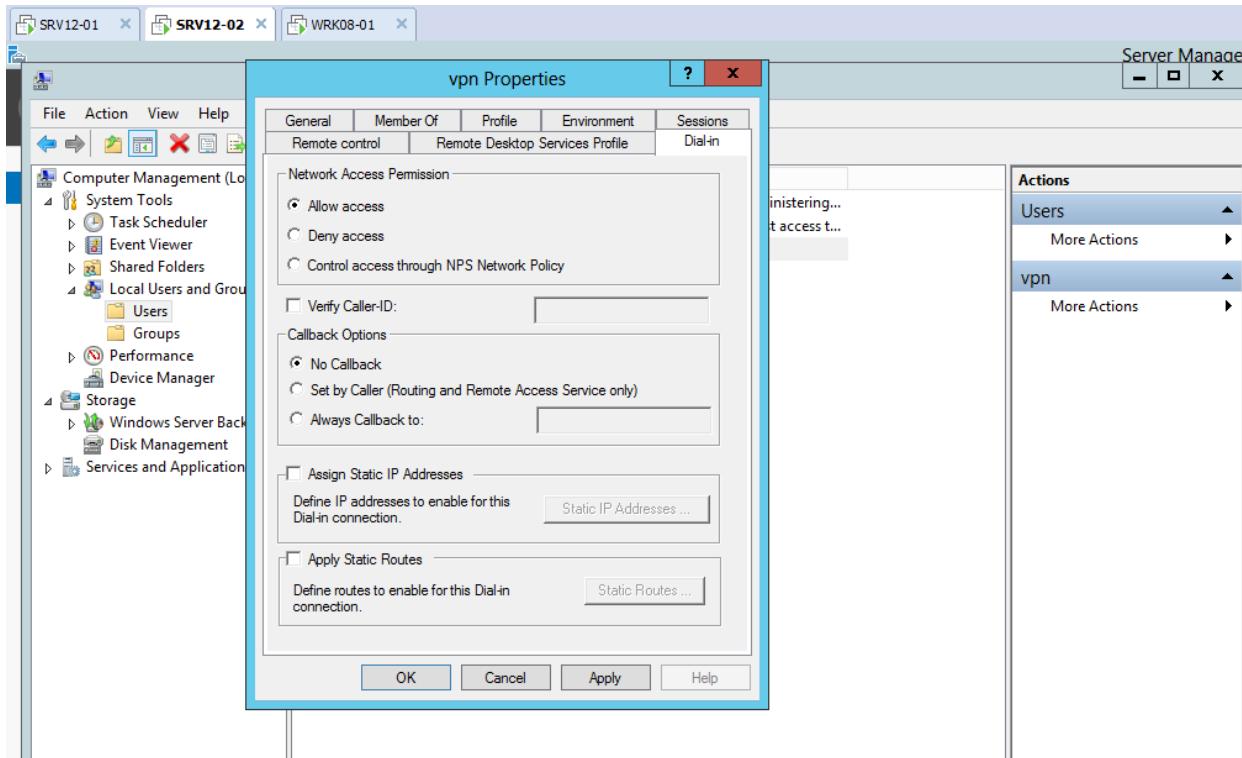
- Tại cửa sổ **New User** , nhập vào tên user cần tạo.



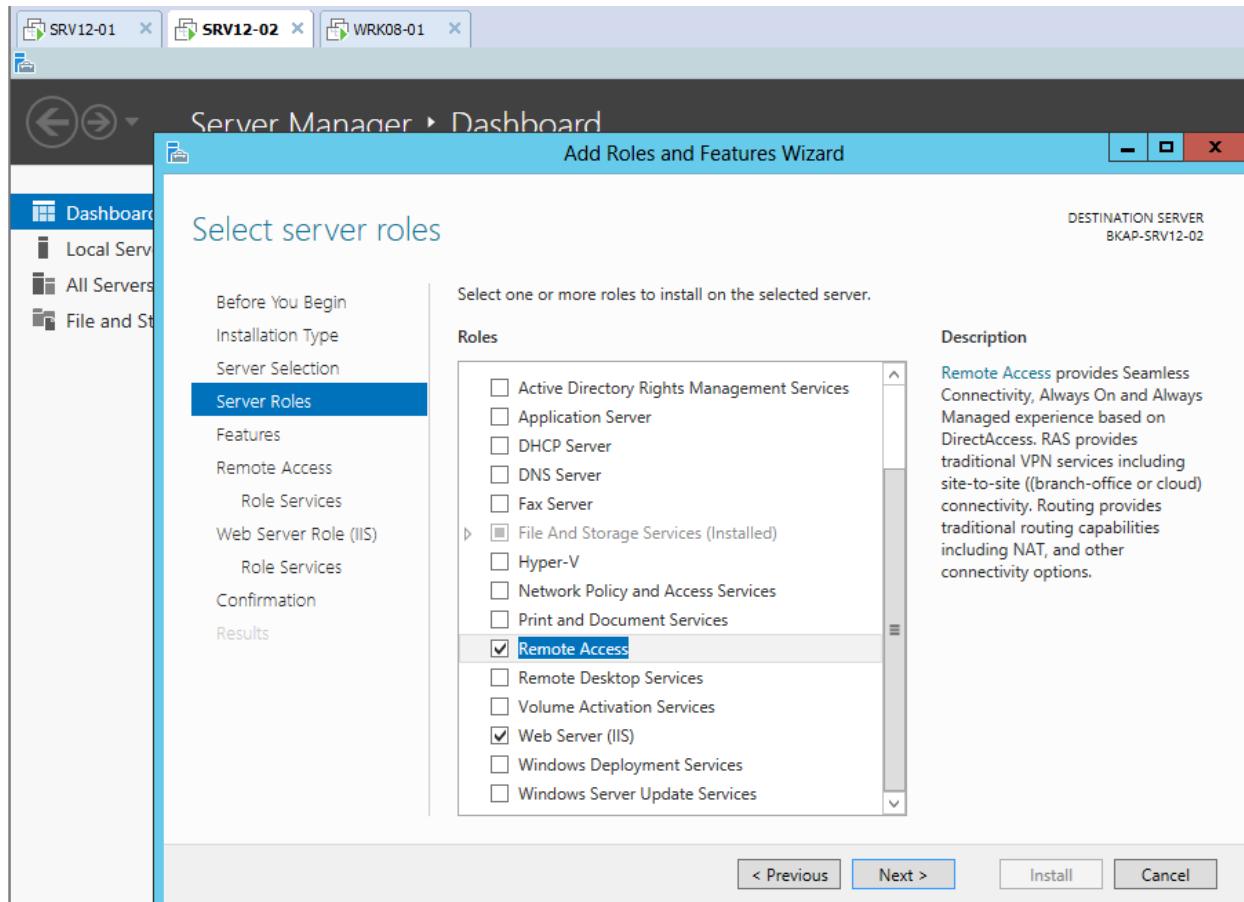
- Cho phép User được quyền truy cập từ xa:
 - Click chuột phải tại user vừa tạo, chọn Properties.



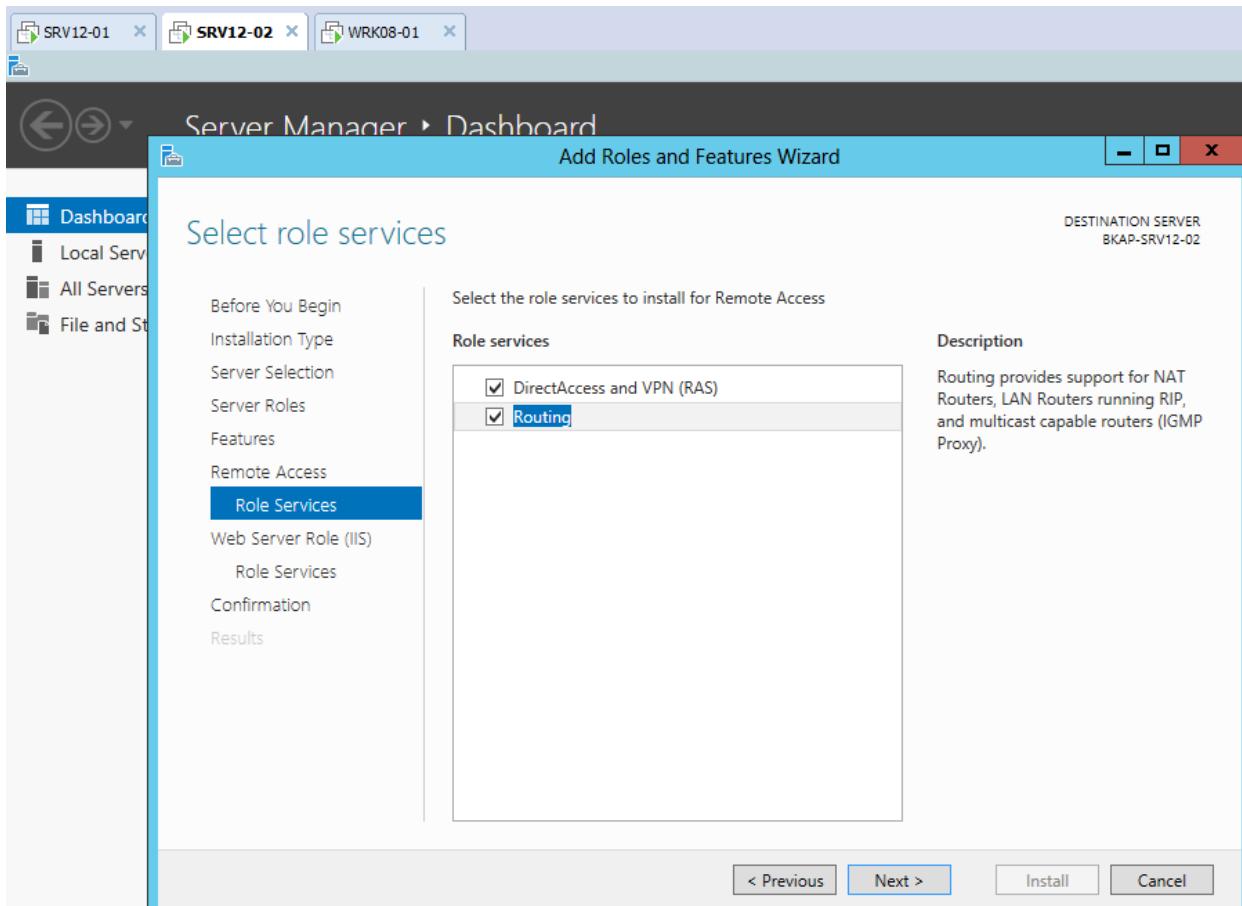
- Chuyển sang tab Dial-in, tại Network Access Permission , chọn vào Allow access., Apply OK.



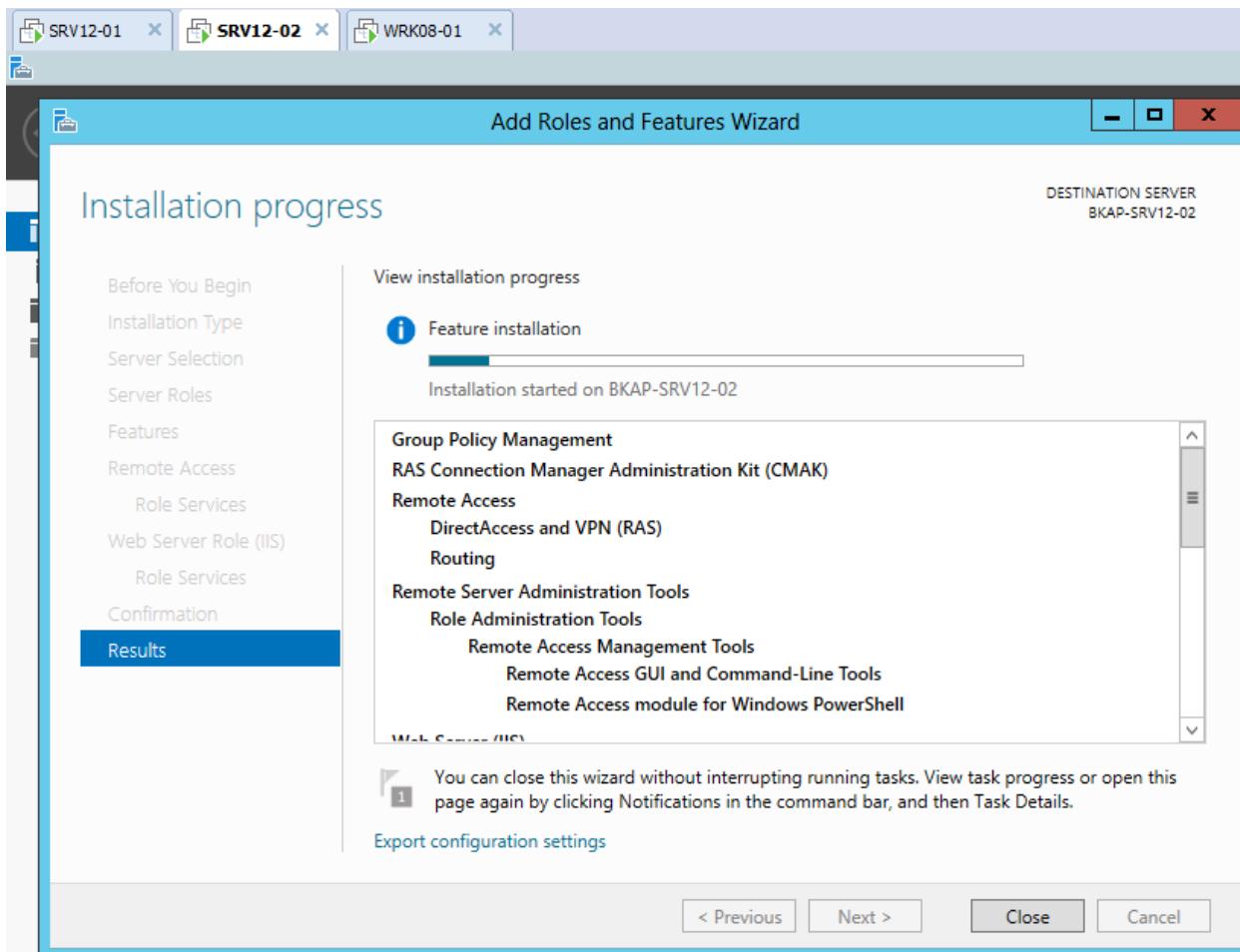
- Thực hiện cài đặt dịch vụ **Remote Access**.
 - **Server Manager / Add Roles and Features** / tại cửa sổ **Select server roles** , click chọn vào dịch vụ **Remote access**.



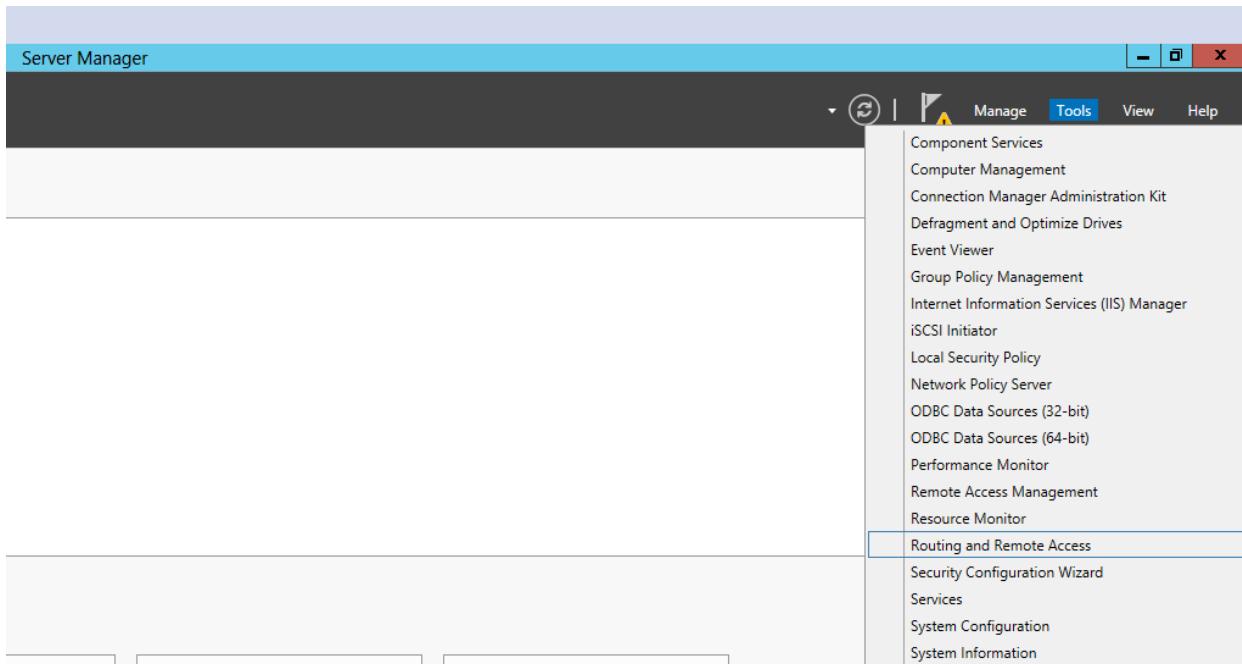
- Tại cửa sổ **Select role services** , click chọn vào **Routing**.



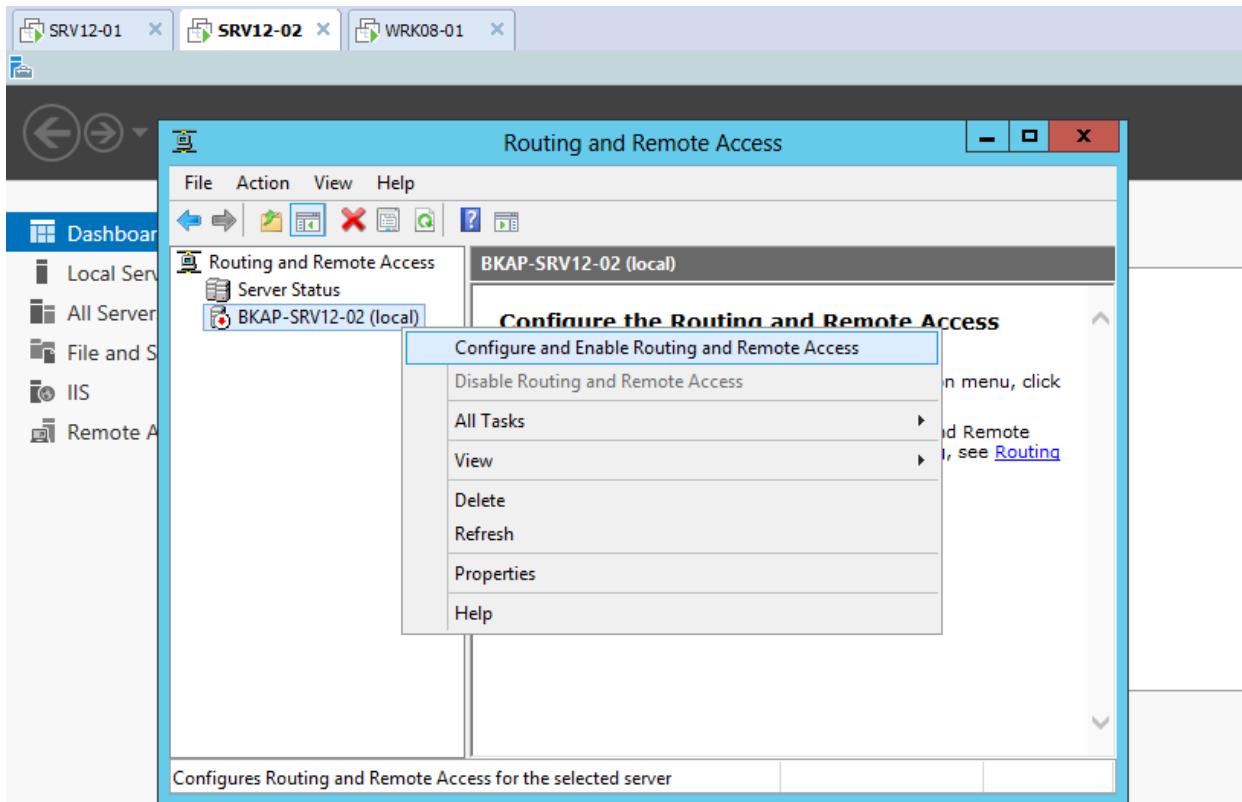
- Click vào Next ..Install để máy chủ tiến hành cài đặt dịch vụ.



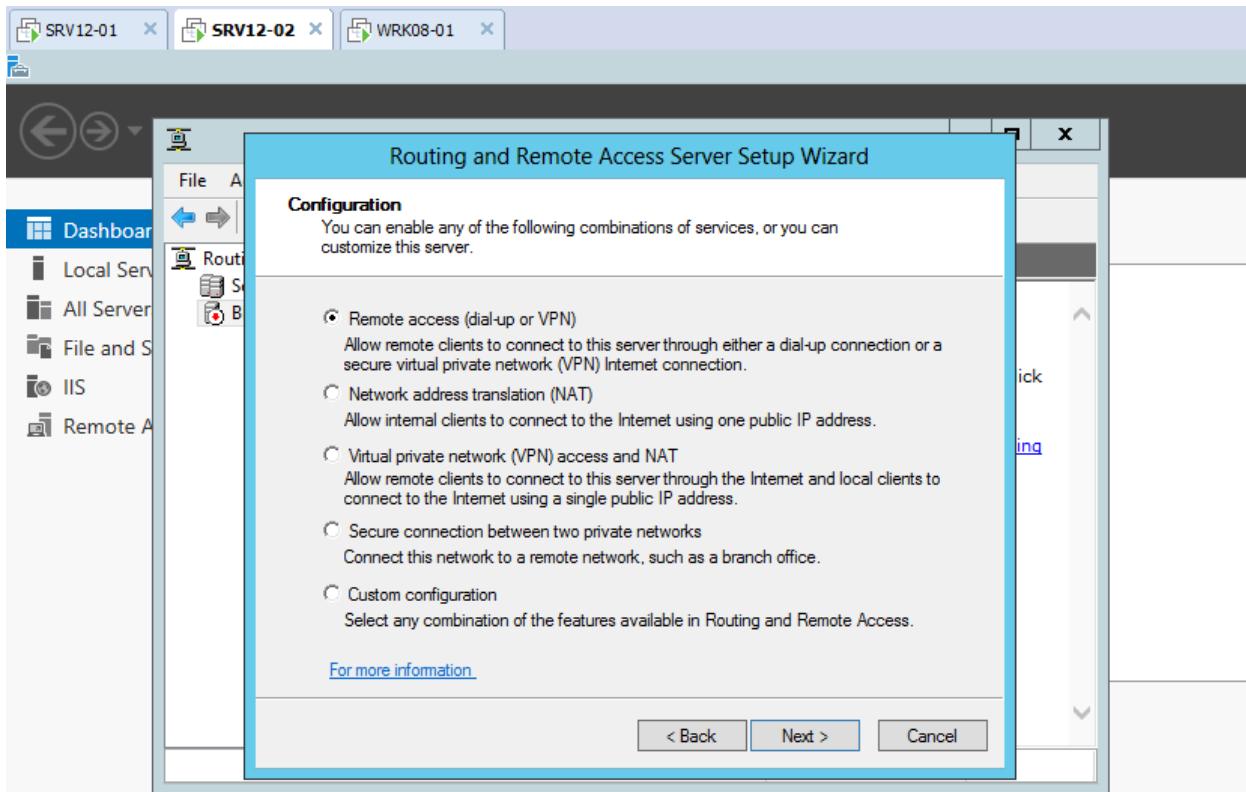
- Thực hiện cấu hình dịch vụ **VPN Server**.
 - **Tools / Routing and Remote Access**



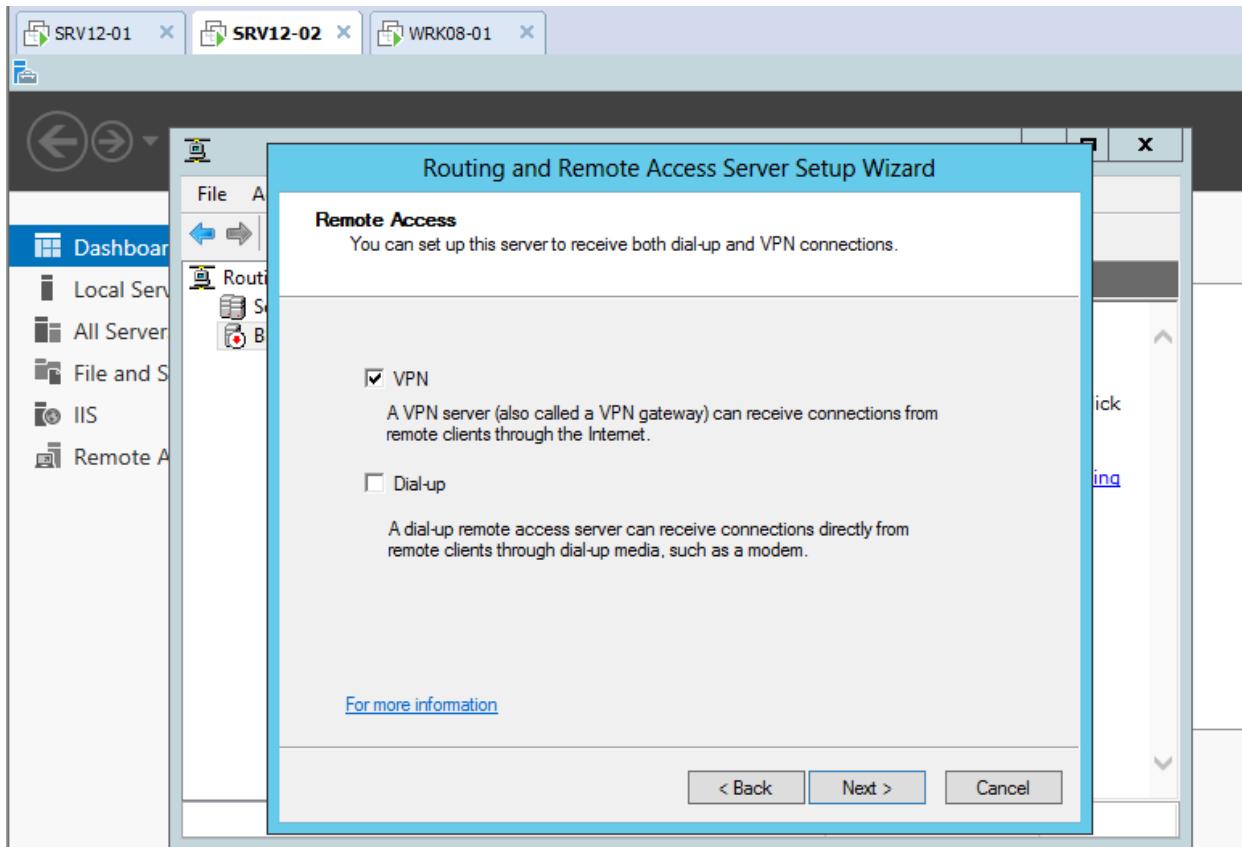
- Tại cửa sổ **Routing and Remote Access**, click chuột phải tại **BKAP-SRV12-02(local)**, chọn vào **Configure and Enable Routing and Remote Access**.



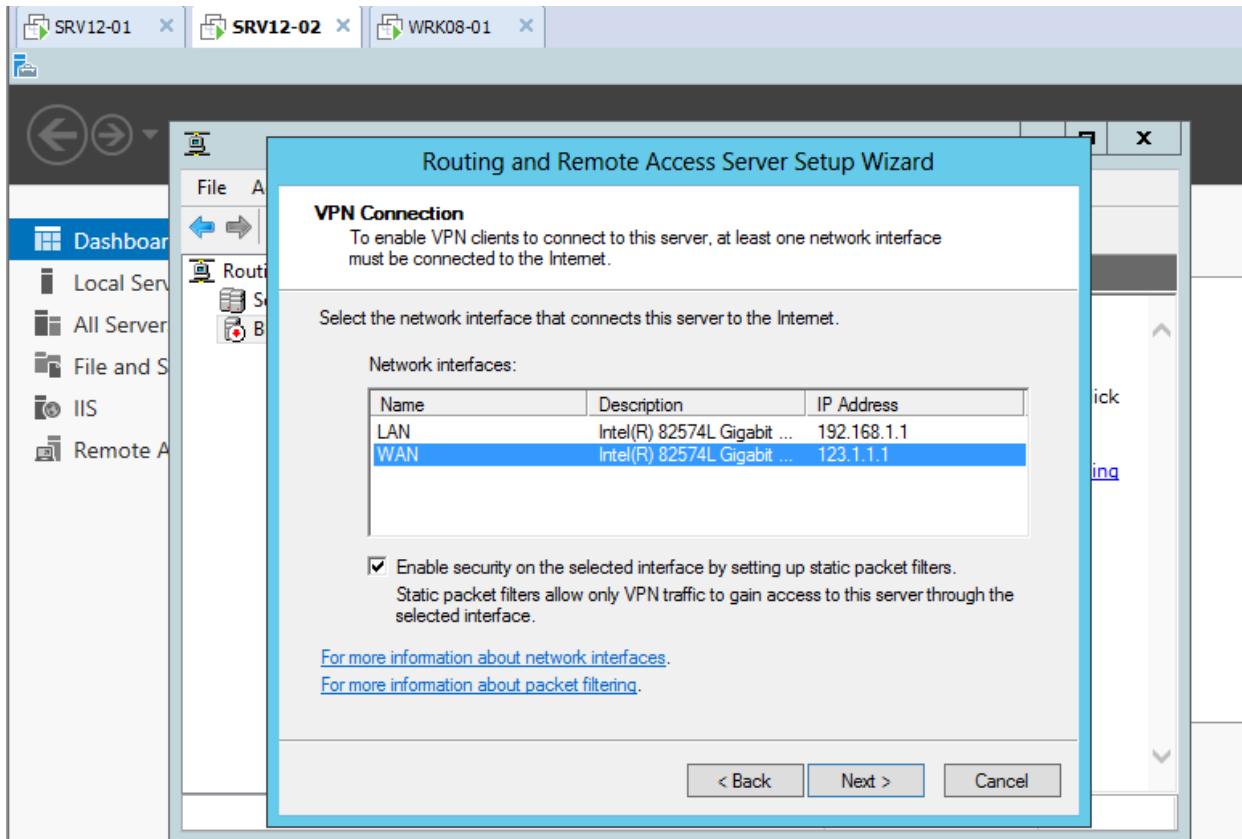
- Tại cửa sổ Configuration , chọn vào Remote access (dial-up or VPN).



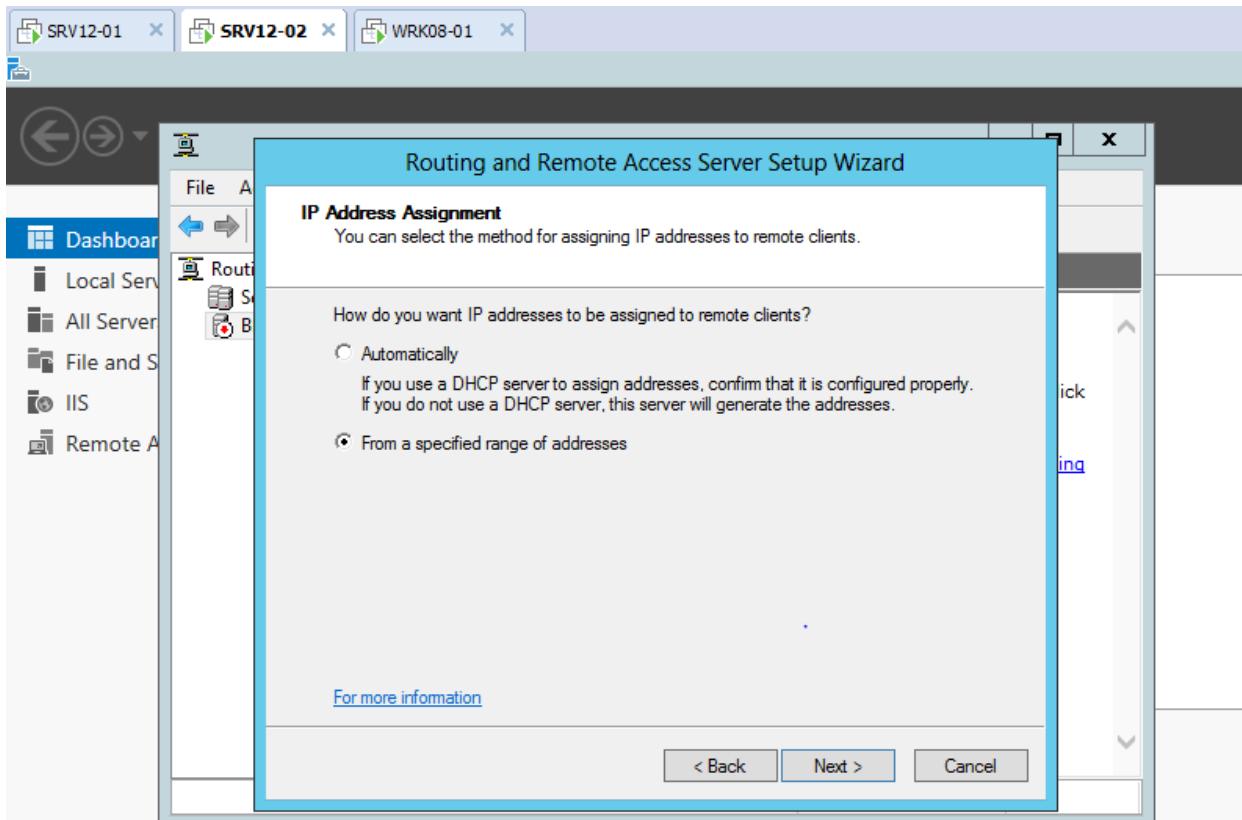
- Tại cửa sổ **Remote Access**, chọn vào **VPN...Next**



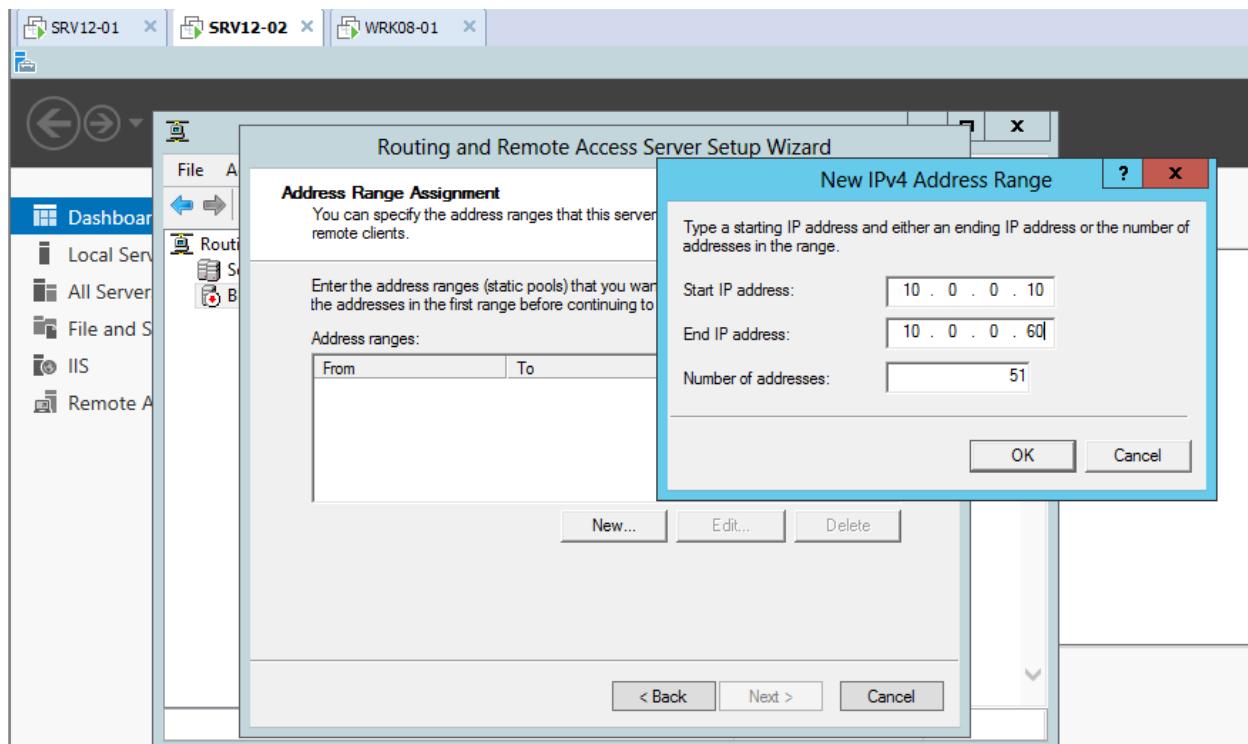
- Tại cửa sổ **VPN Connection**, click chọn vào Card mạng WAN.(mạng bên ngoài) ..Next.



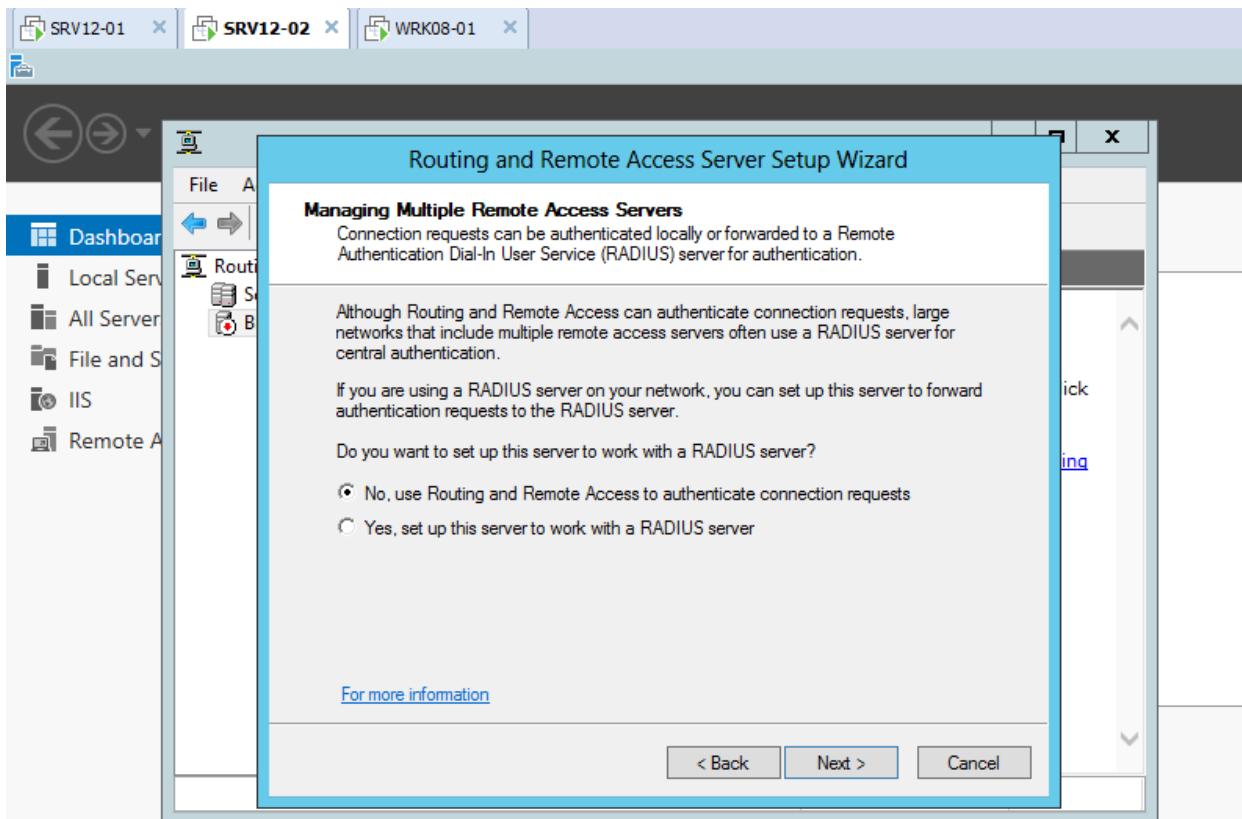
- Tại cửa sổ IP Address Assignment , chọn vào From a specified range of address... Next.



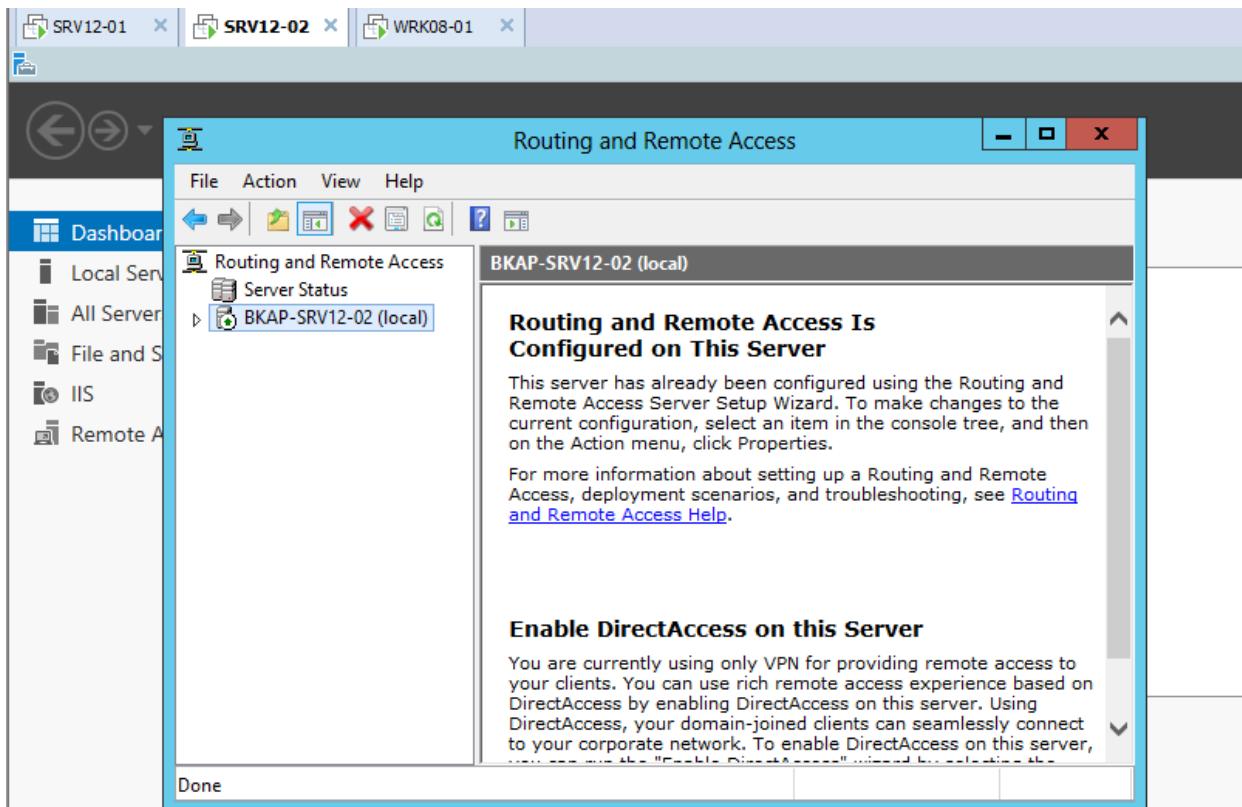
- Tại cửa sổ **Address Range Assignment**, click vào **New...**
- Tại cửa sổ **New IPv4 Address Range**, nhập vào dải địa chỉ IP
 - *10.0.0.10 – 10.0.0.60*
- Next.



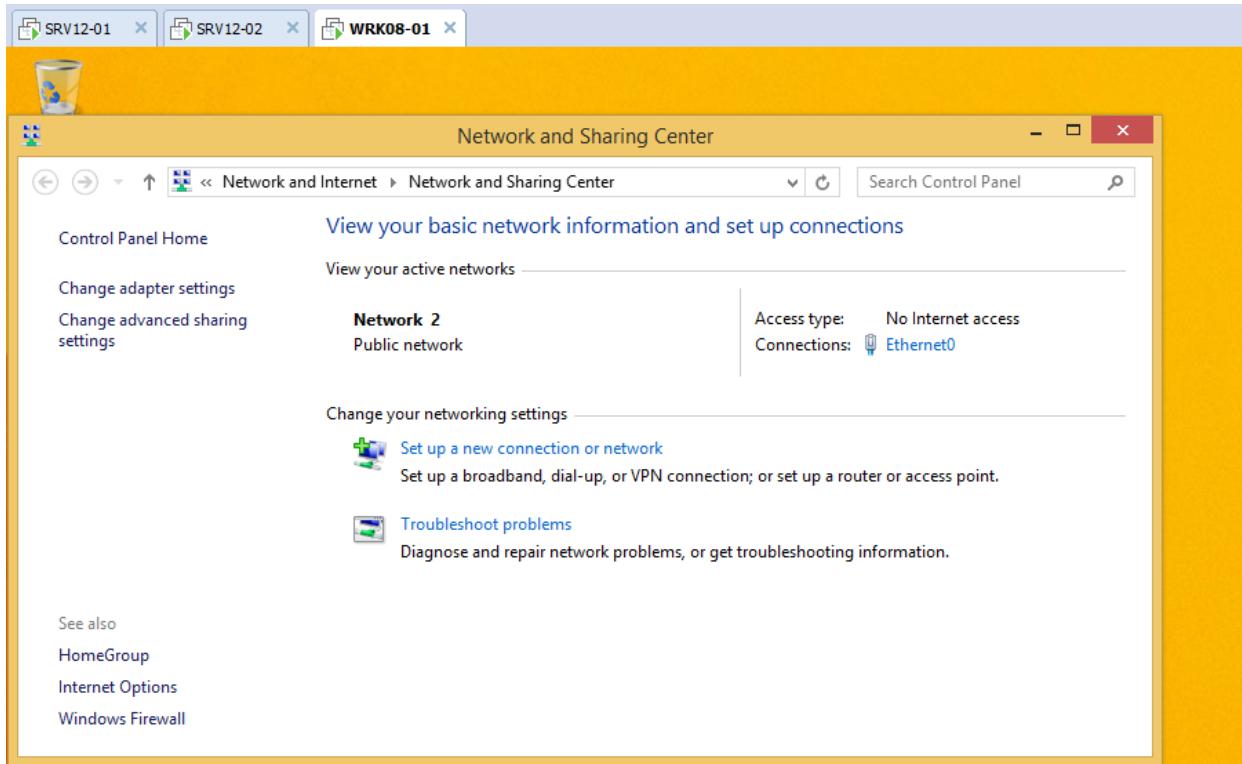
- Tại cửa sổ **Managing Multiple Remote Access Servers**, click chọn vào **No, use Routing and Remote Access to authenticate connection requests.**



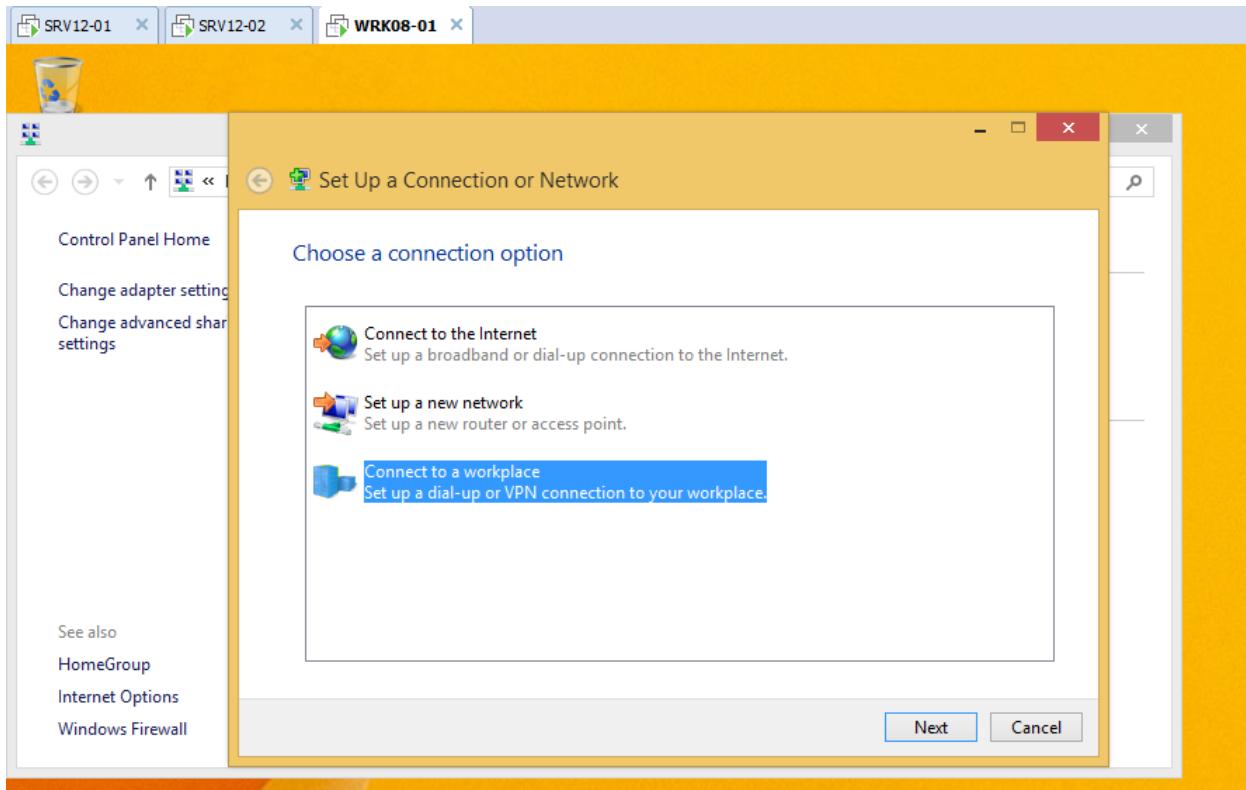
- Click **Finish / OK** để kết thúc quá trình cấu hình dịch vụ **VPN Server**.



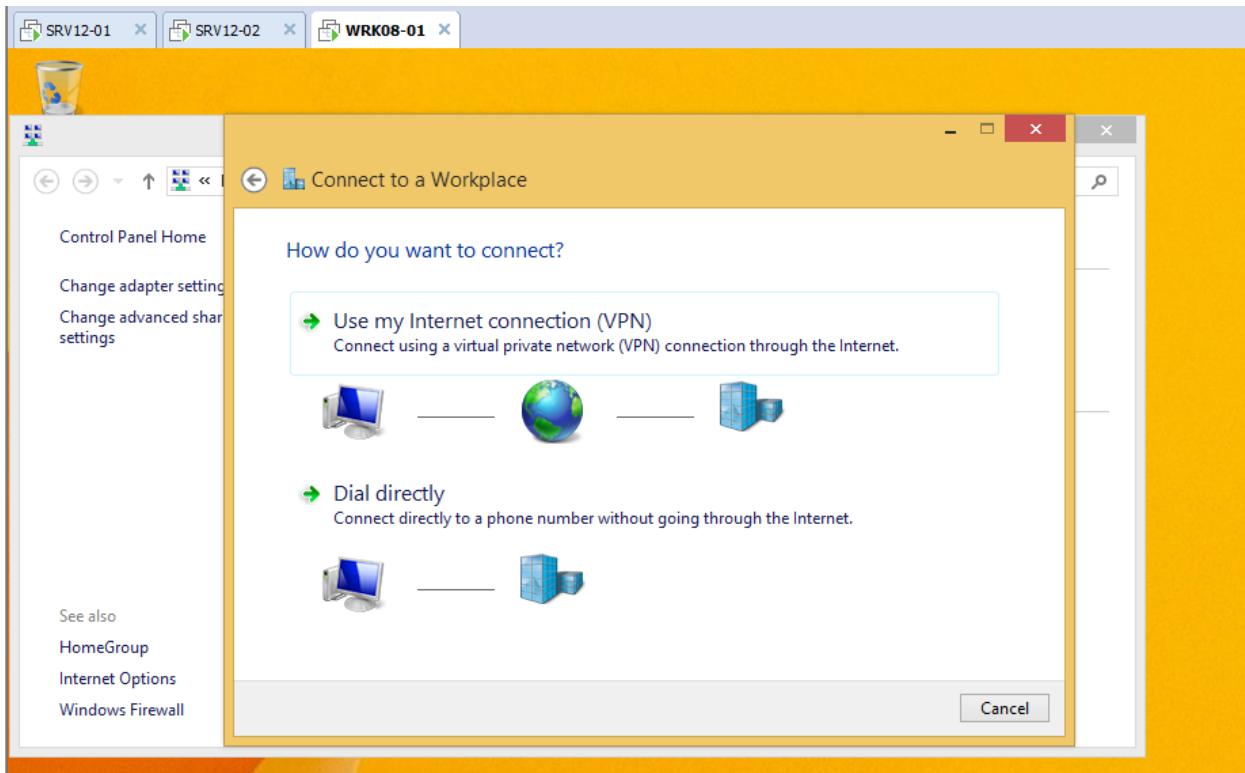
- Chuyển qua máy client **BKAP-WRK08-01** thực hiện tạo kết nối **VPN Client**.
 - Tại cửa sổ **Network and Sharing Center**, click chọn vào **Set up a new connection or network**.



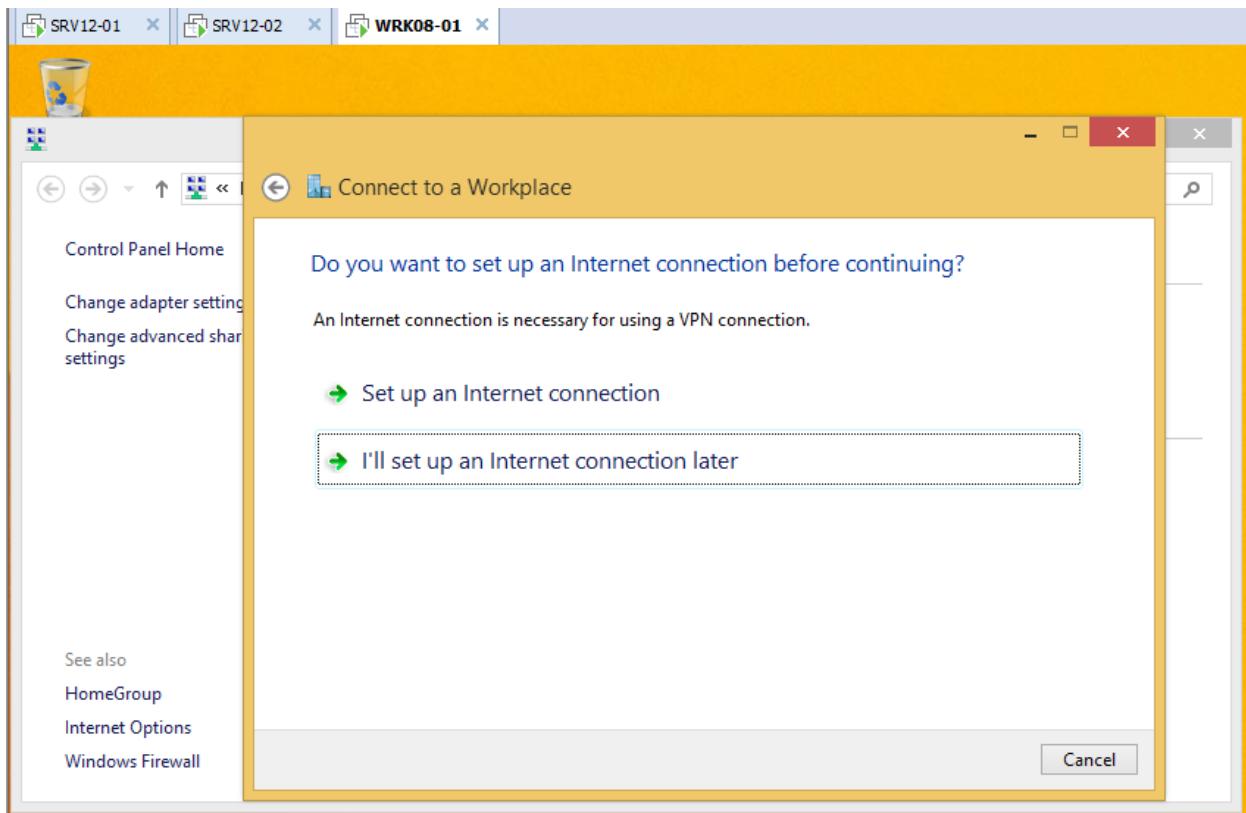
- Tại cửa sổ **Set Up a Connection or Network** , click chọn vào **Connect to a workplace... Next.**



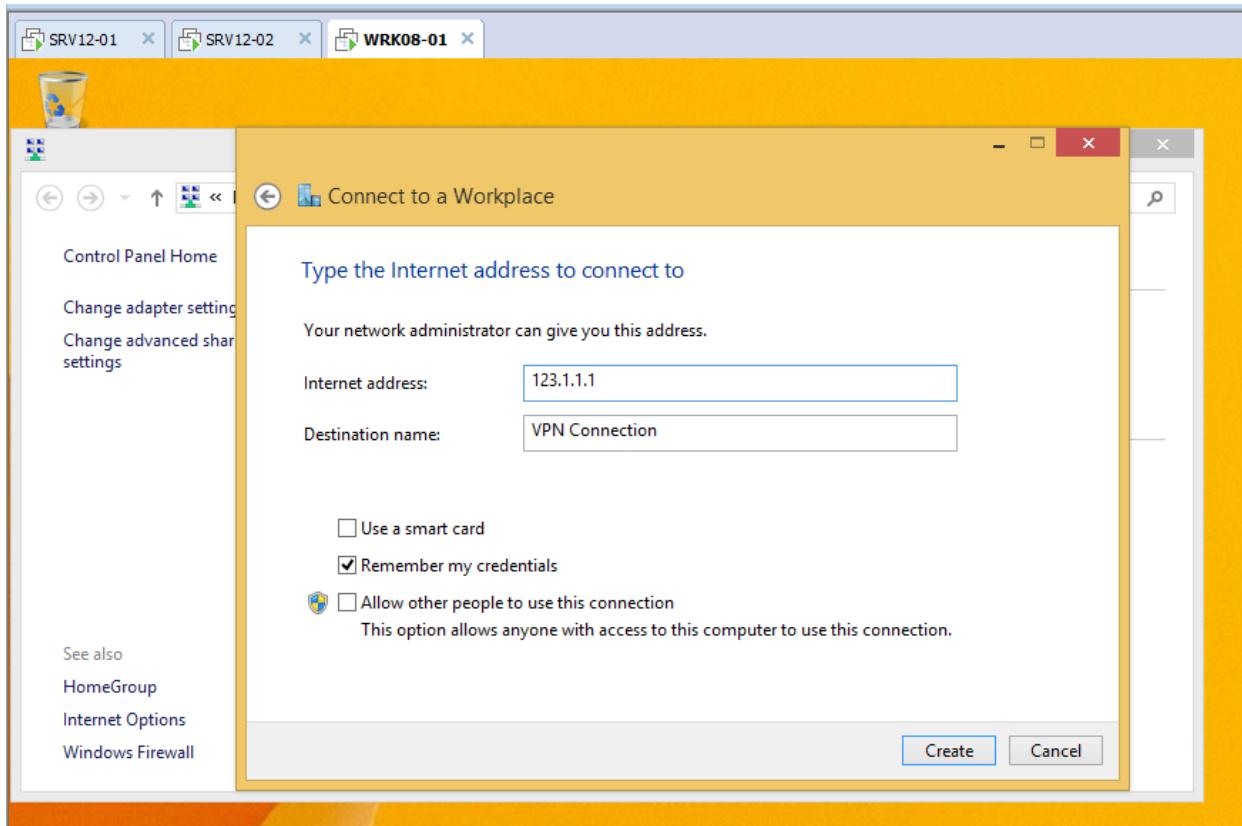
- Tại cửa sổ **Connect to a Workplace**, click chọn vào **Use my Internet connection (VPN)**.



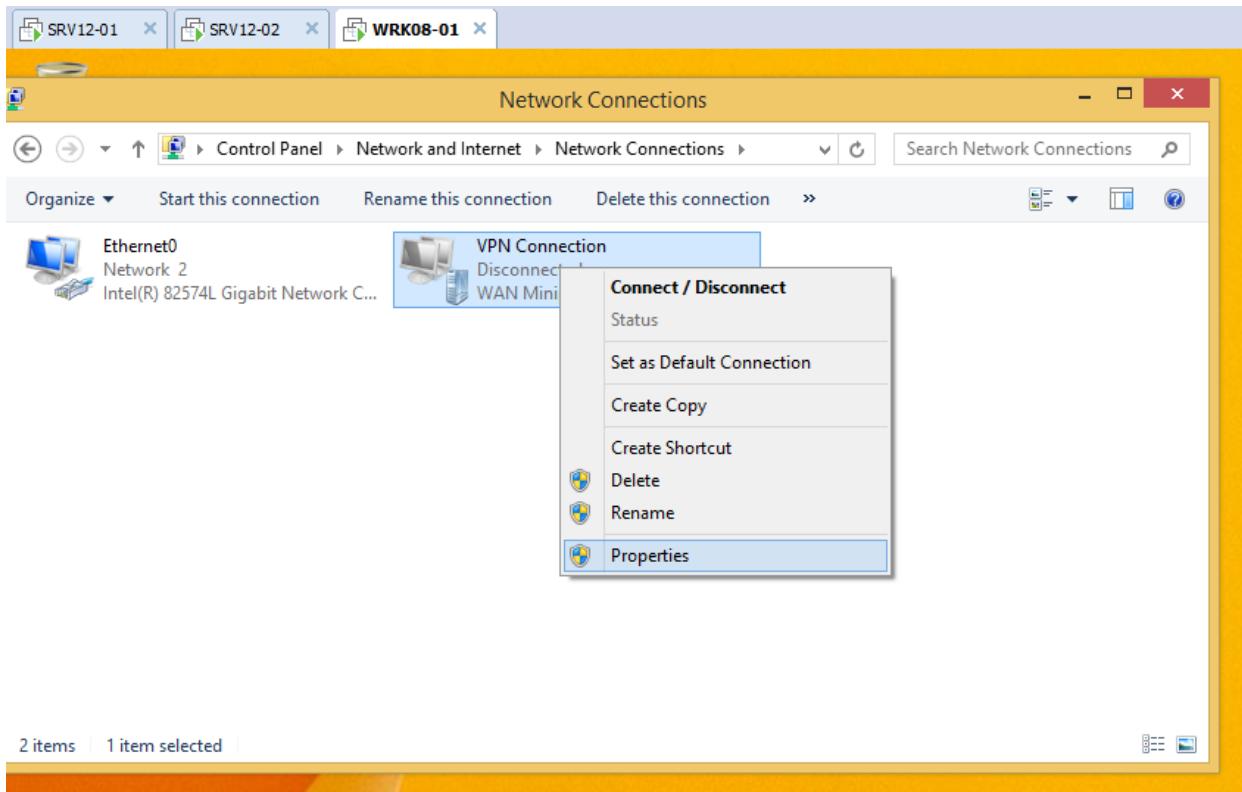
- Tại cửa sổ tiếp theo , chọn vào **I'll set up an Internet connection later.**



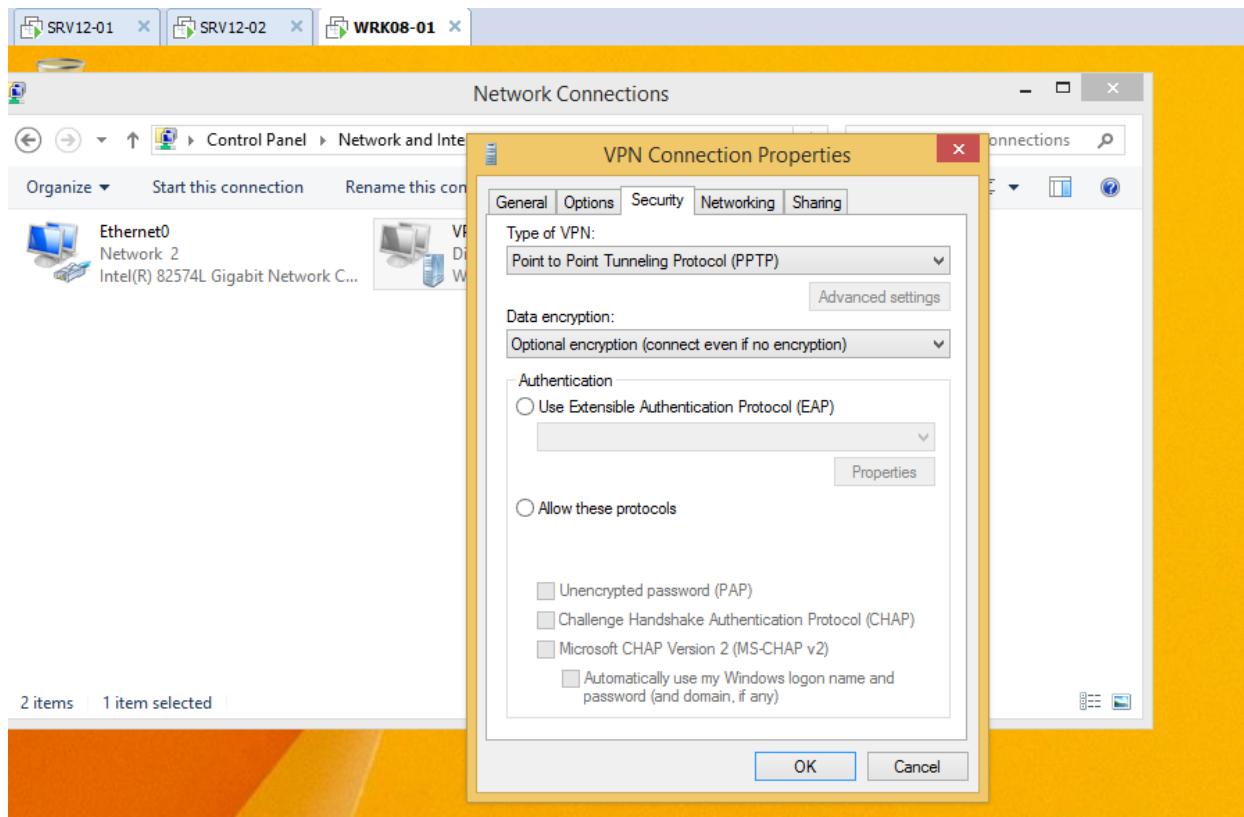
- Tại cửa sổ tiếp theo, nhập vào địa chỉ *Gateway* của mạng bên ngoài
 - *Internet address : 123.1.1.1*
 - Click vào **Create**.



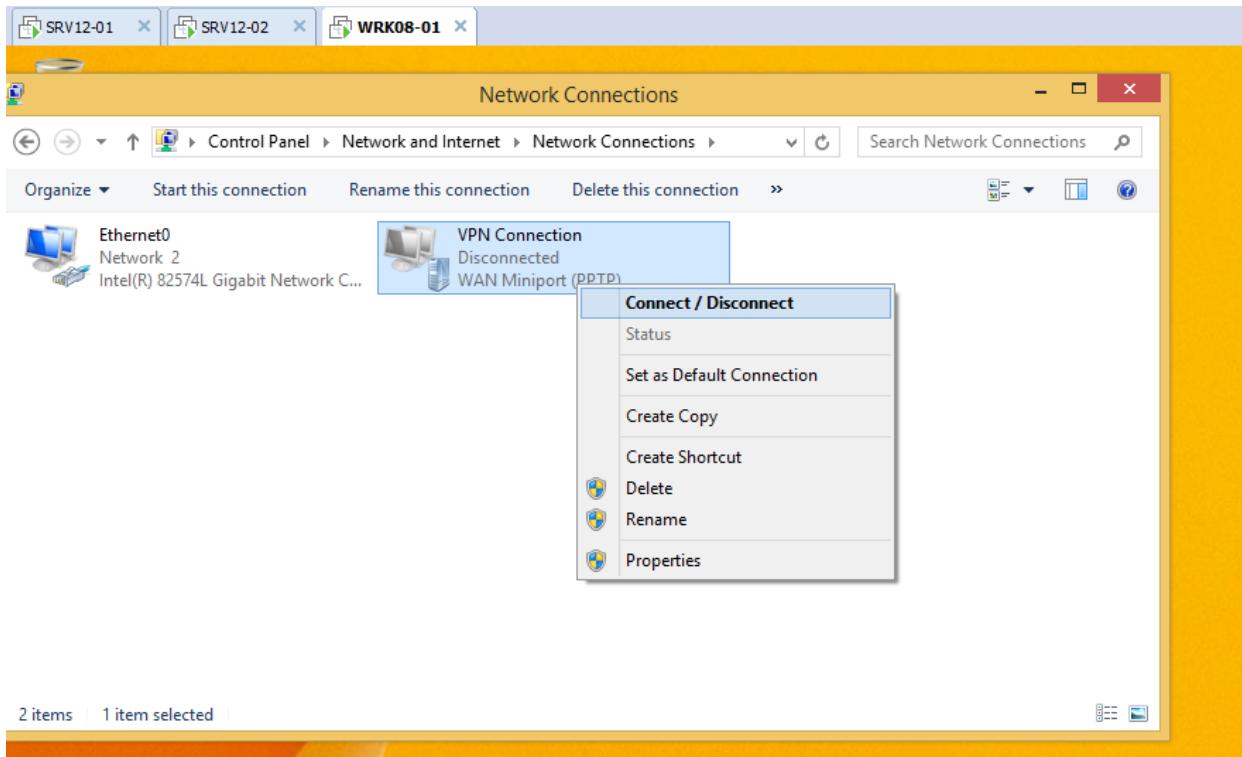
- Click chuột phải tại Card mạng **VPN Connection** vừa tạo, chọn **Properties**.



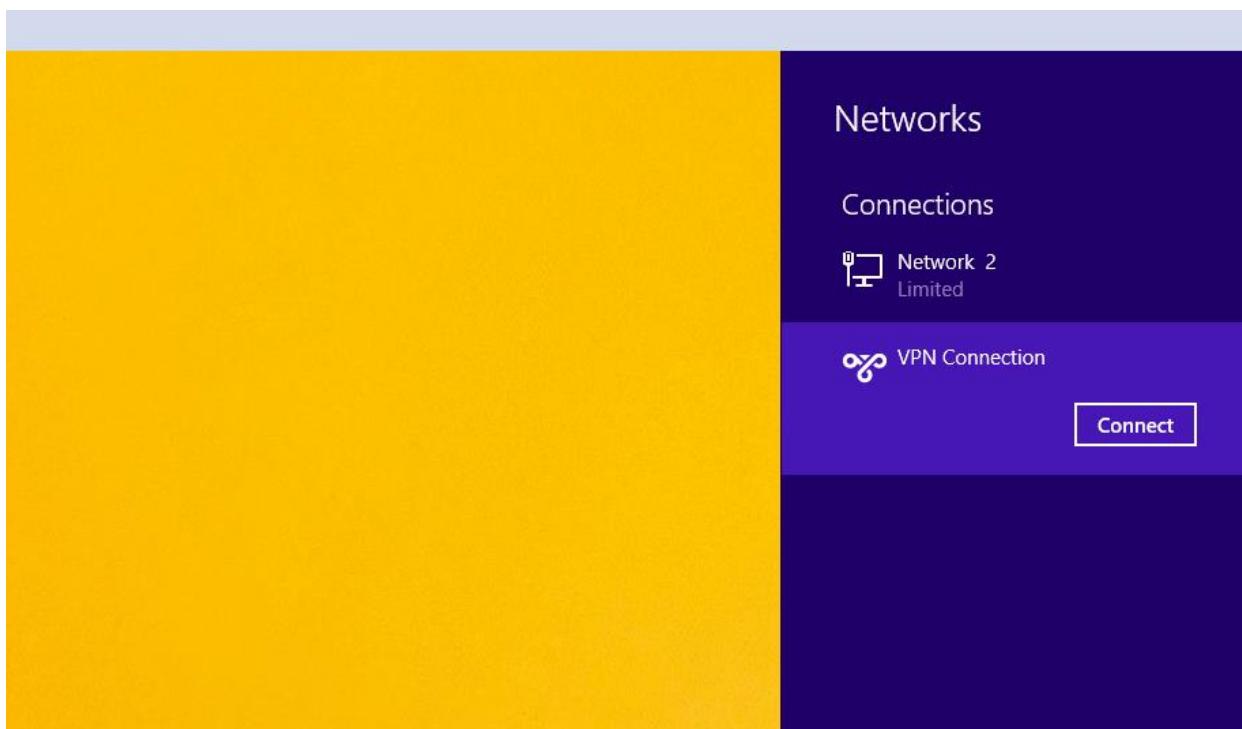
- Tại cửa sổ **VPN Connection Properties**, chuyển sang tab **Security**, tại mục **Type of VPN**, chọn kiểu giao thức kết nối VPN là **Point to Point Tunneling Protocol (PPTP)**...OK.



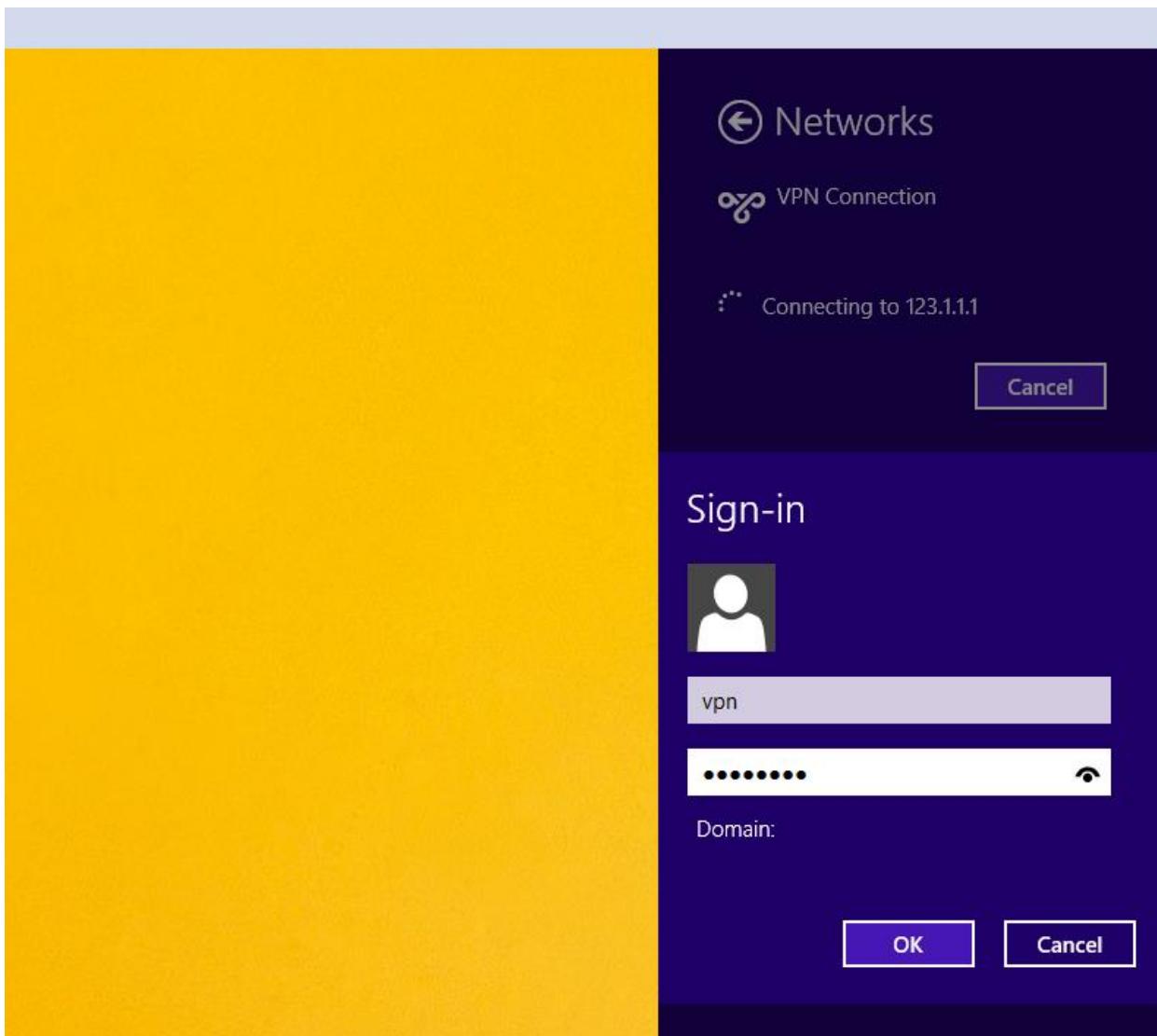
- Click chuột phải tại **Card mạng VPN Connection**, chọn **Connect / Disconnect**.



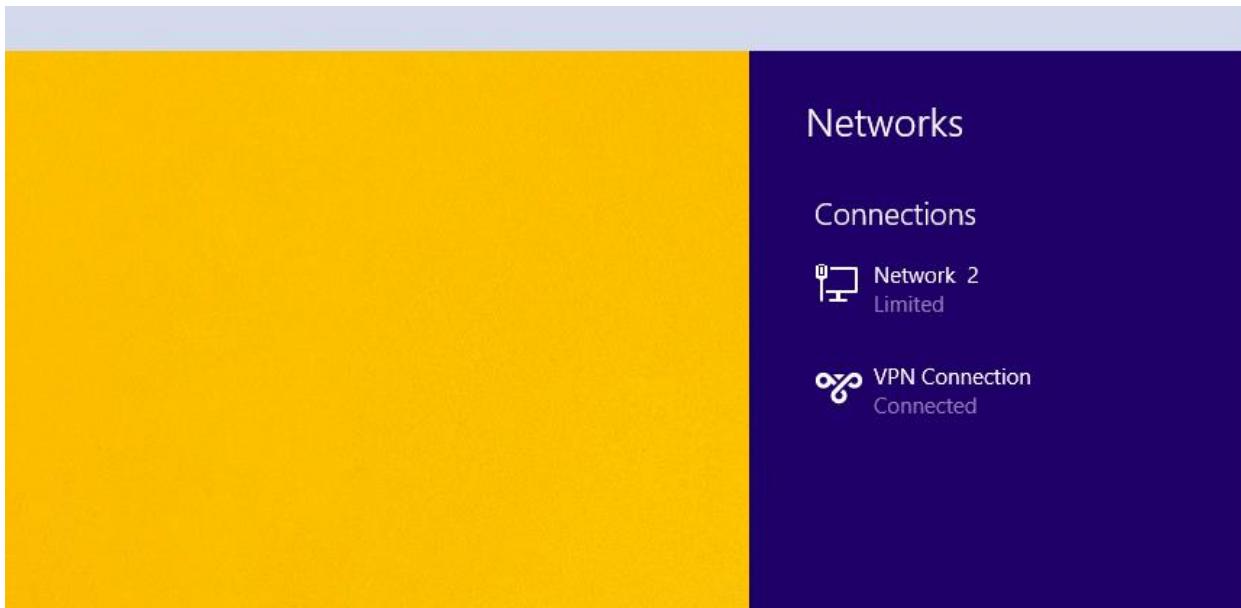
- Click vào **Connect** tại card mạng **VPN Connection**.



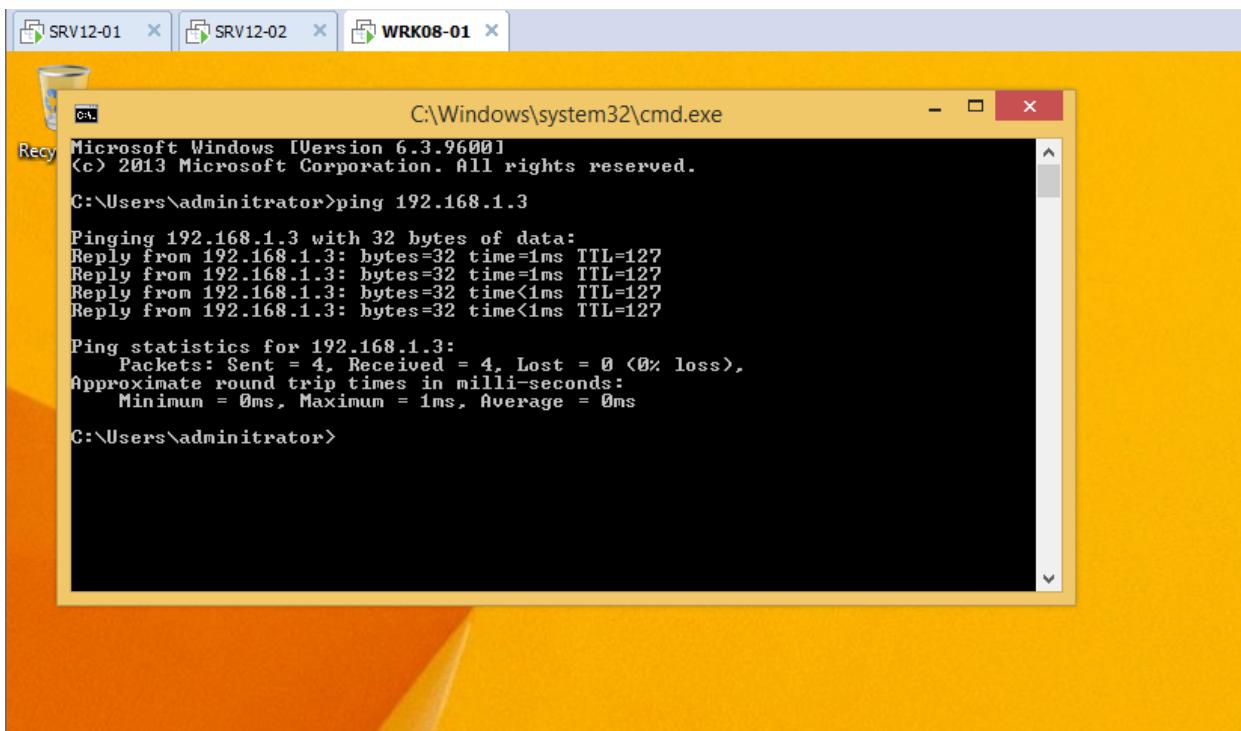
- Nhập vào tài khoản **vpn** vừa tạo ở trên...OK



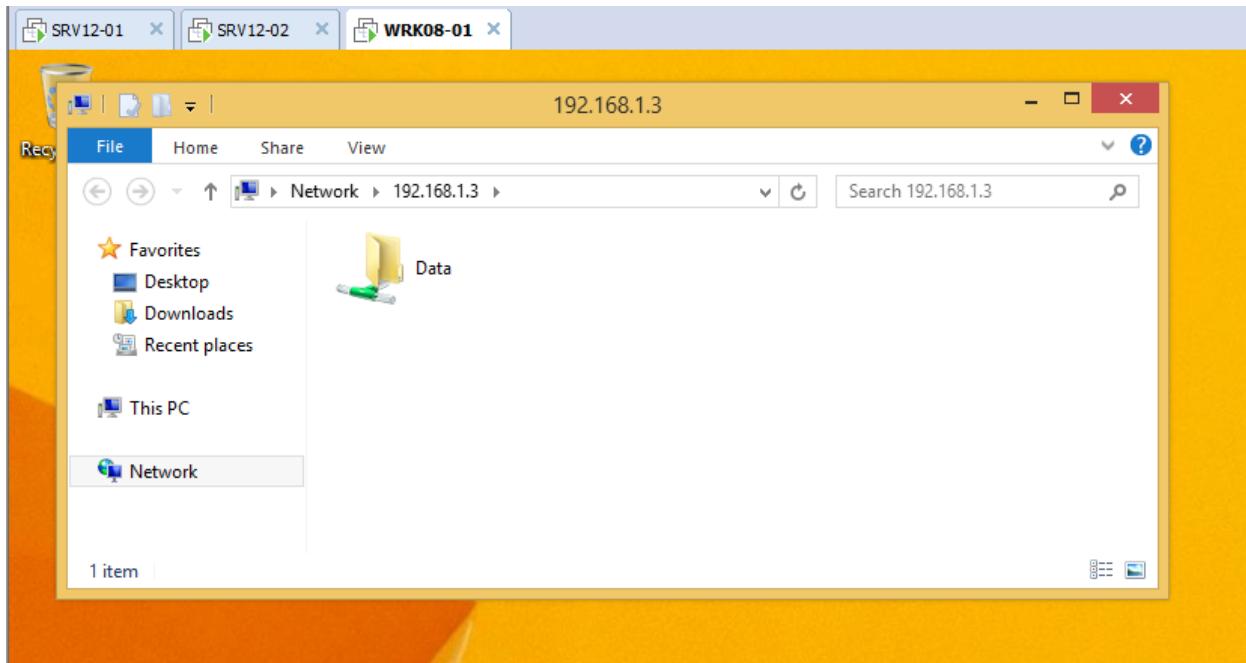
- Kết nối VPN thành công.



- Kiểm tra ping đến máy *BKAP-SRV12-01*:



- Truy cập vào máy **BKAP-SRV12-01** để lấy dữ liệu:



7.2 Triển khai cài đặt và cấu hình dịch vụ VPN (Site to Site).

1. Yêu cầu bài lab:

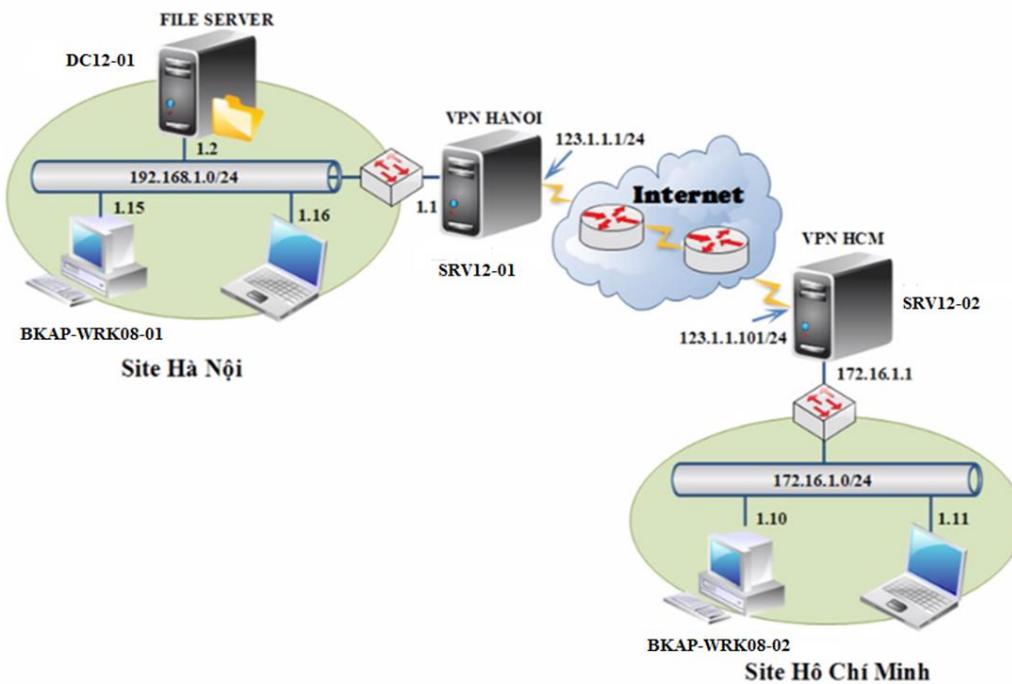
- + Trên máy **BKAP-DC12-01**, tạo thư mục **Data** và chia sẻ dữ liệu.
- + Trên máy **BKAP-SRV12-01** và **BKAP-SRV12-02** thực hiện các công việc sau:
 - Tạo tài khoản dịch vụ dùng để kết nối **VPN**.
 - Cài đặt dịch vụ **Remote Access**.
 - Cấu hình **VPN Server** và tạo Site với giao thức **PPTP**. Site **HN** cho phép Client ở **HCM** truy cập vào là 192.168.1.0/24. Site **HCM** cho phép dải địa chỉ Client **HN** truy cập vào là 172.16.1.0/24
- + Thực hiện ping thông và truy cập dữ liệu từ máy **BKAP-WRK08-01** tới máy **BKAP-DC12-01** thông qua hệ thống **VPN** vừa thiết lập.

2. Yêu cầu chuẩn bị:

- + Chuẩn bị 1 máy *BKAP-DC12-01* làm *Domain Controller* quản lý miền **bkaptech.vn**, đóng vai trò là *File Server*.
- + Chuẩn bị 2 máy Server *BKAP-SRV12-01* và *BKAP-SRV12-02*, mỗi máy có 2 card mạng.
- + Máy Client bên ngoài ping thông tin card bên ngoài của máy *BKAP-SRV12-02*.

3. Mô hình Lab:

HỆ THỐNG ĐÀO TẠO CNTT QUỐC TẾ BACHKHOA-APTECH
Lab 7.2 Triển khai cài đặt và cấu hình dịch vụ VPN Server (Site to Site)



Hình 7.2

Sơ đồ địa chỉ như sau:

Thông số	DC12-01	SRV12-01	SRV12-02	WRK08-01
IP address	192.168.1.2	NIC1:192.168.1.1 NIC2:123.1.1.1	NIC1:123.1.1.101 NIC2:172.16.1.1	172.16.1.10
Subnet Mask	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
Gateway	192.168.1.1	123.1.1.100	123.1.1.1	172.16.1.1

DNS Server	192.168.1.2	--	--	--
------------	-------------	----	----	----

Hướng dẫn chi tiết:

- Mở các máy ảo, kết nối như mô hình, đặt địa chỉ IP như sơ đồ trên.
 - Máy *BKAP-SRV12-01* có 2 card mạng :
 - VMnet2 : 192.168.1.1
 - VMnet3 : 123.1.1.1
 - Máy *BKAP-SRV12-02* có 2 card mạng :
 - VMnet3 : 123.1.1.101
 - VMnet4 : 172.16.1.1
 - Thực hiện ping thông giữa các máy kết nối trực tiếp.

```

Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:
Reply from 192.168.1.2: bytes=32 time=1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
Control-C
^C

C:\Users\Administrator>ping 123.1.1.101

Pinging 123.1.1.101 with 32 bytes of data:
Reply from 123.1.1.101: bytes=32 time<1ms TTL=128

Ping statistics for 123.1.1.101:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss).

```

```

Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ping 123.1.1.1

Pinging 123.1.1.1 with 32 bytes of data:
Reply from 123.1.1.1: bytes=32 time<1ms TTL=128
Reply from 123.1.1.1: bytes=32 time<1ms TTL=128

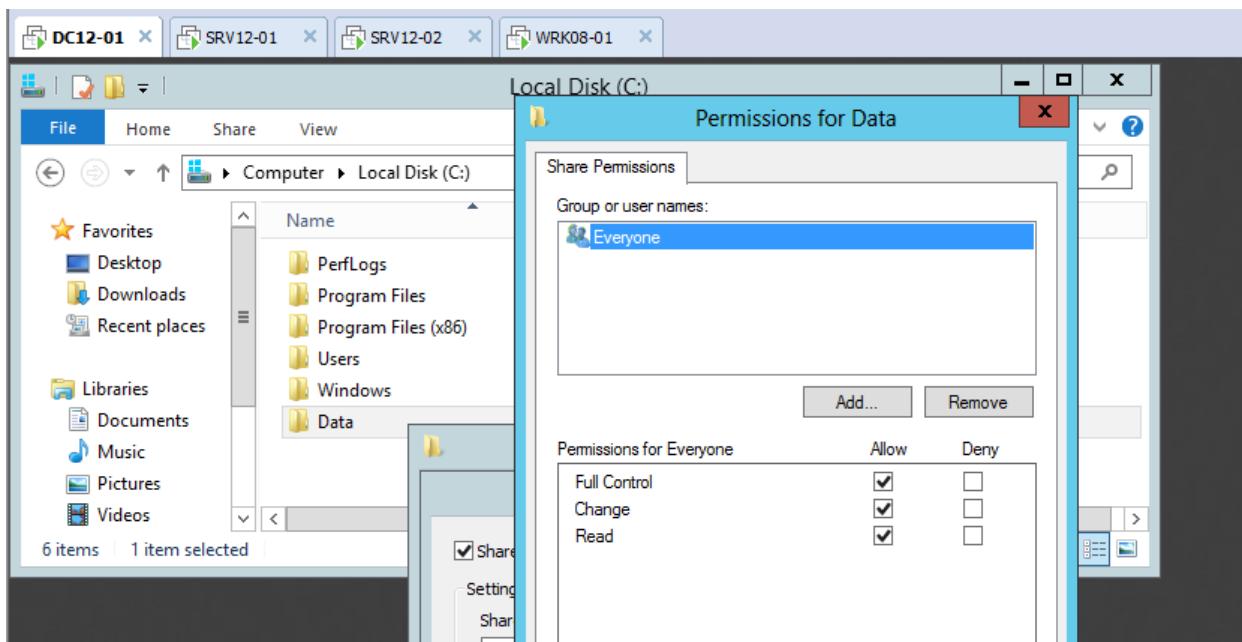
Ping statistics for 123.1.1.1:
    Packets: Sent = 2, Received = 2, Lost = 0 <0% loss>,
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
Control-C
^C
C:\Users\Administrator>ping 172.16.1.10

Pinging 172.16.1.10 with 32 bytes of data:
Reply from 172.16.1.10: bytes=32 time<1ms TTL=128
Reply from 172.16.1.10: bytes=32 time<1ms TTL=128
Reply from 172.16.1.10: bytes=32 time<1ms TTL=128

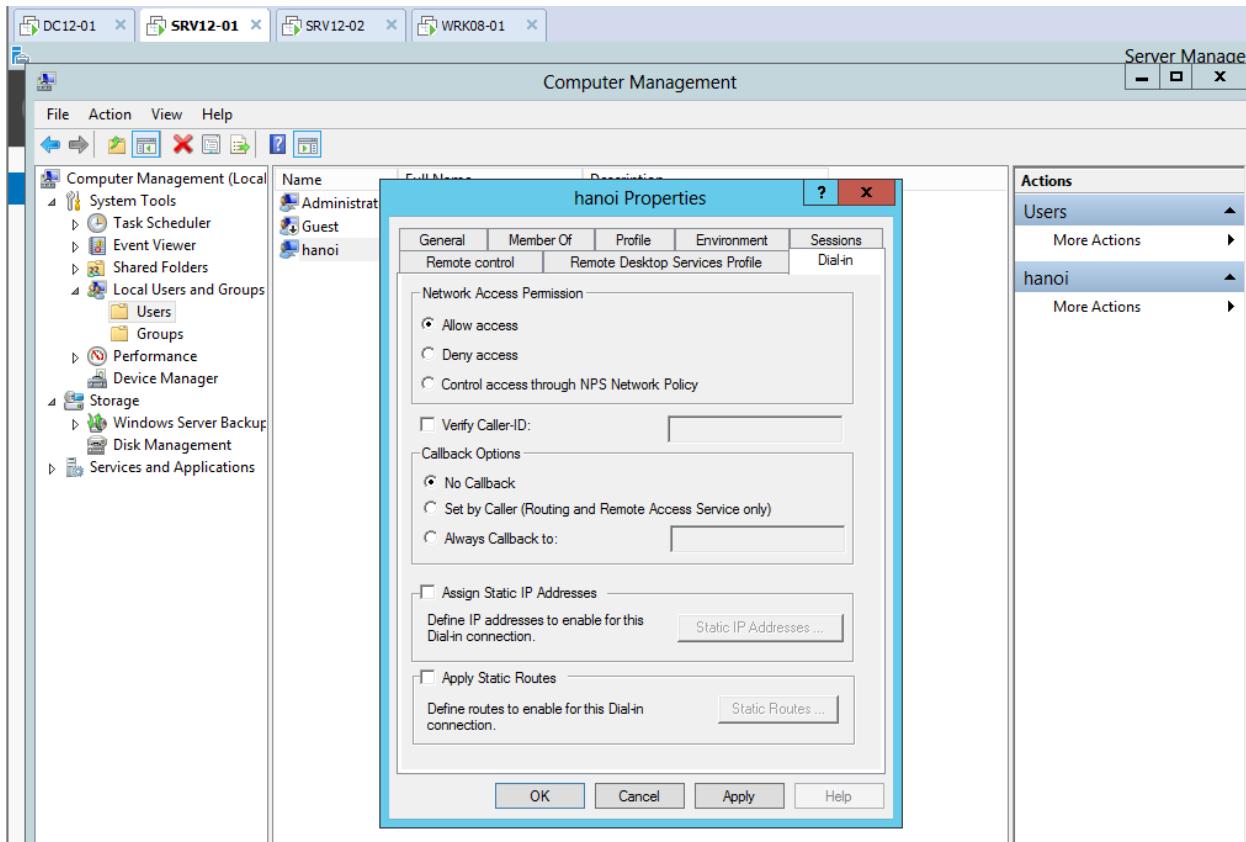
Ping statistics for 172.16.1.10:
    Packets: Sent = 3, Received = 3, Lost = 0 <0% loss>,
    Approximate round trip times in milli-seconds:

```

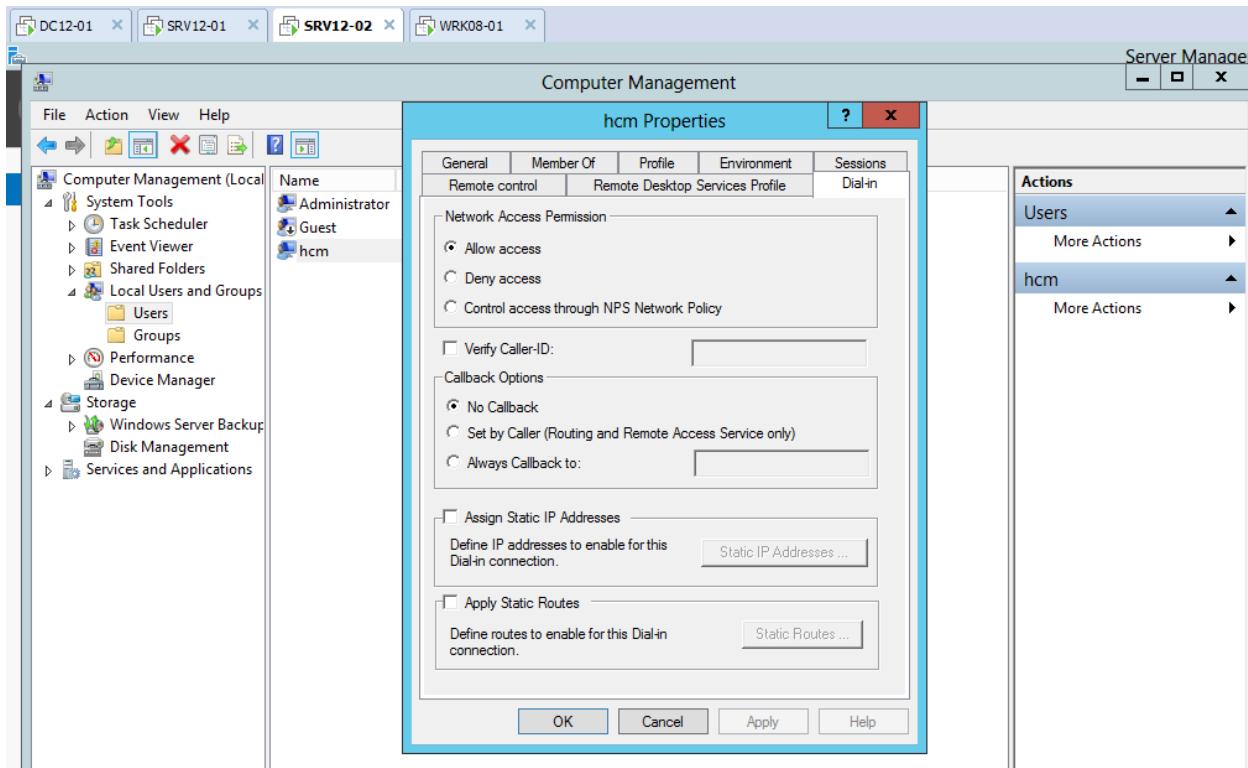
- Thực hiện trên máy BKAP-DC12-01, tạo 1 thư mục **Data** và chia sẻ dữ liệu.



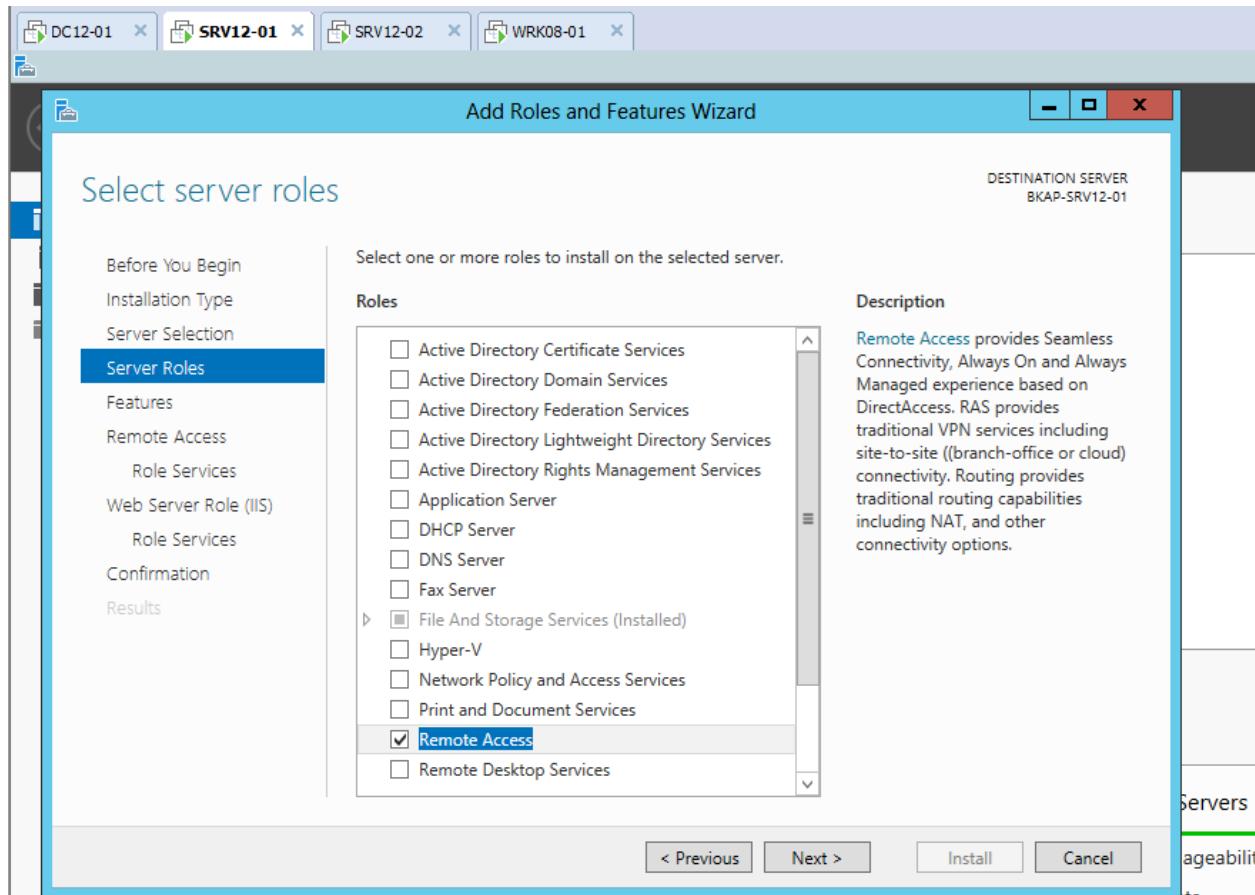
- Chuyển qua máy **BKAP-SRV12-01** thực hiện :
 - Tạo tài khoản **hanoi** và cấp quyền truy cập từ xa.

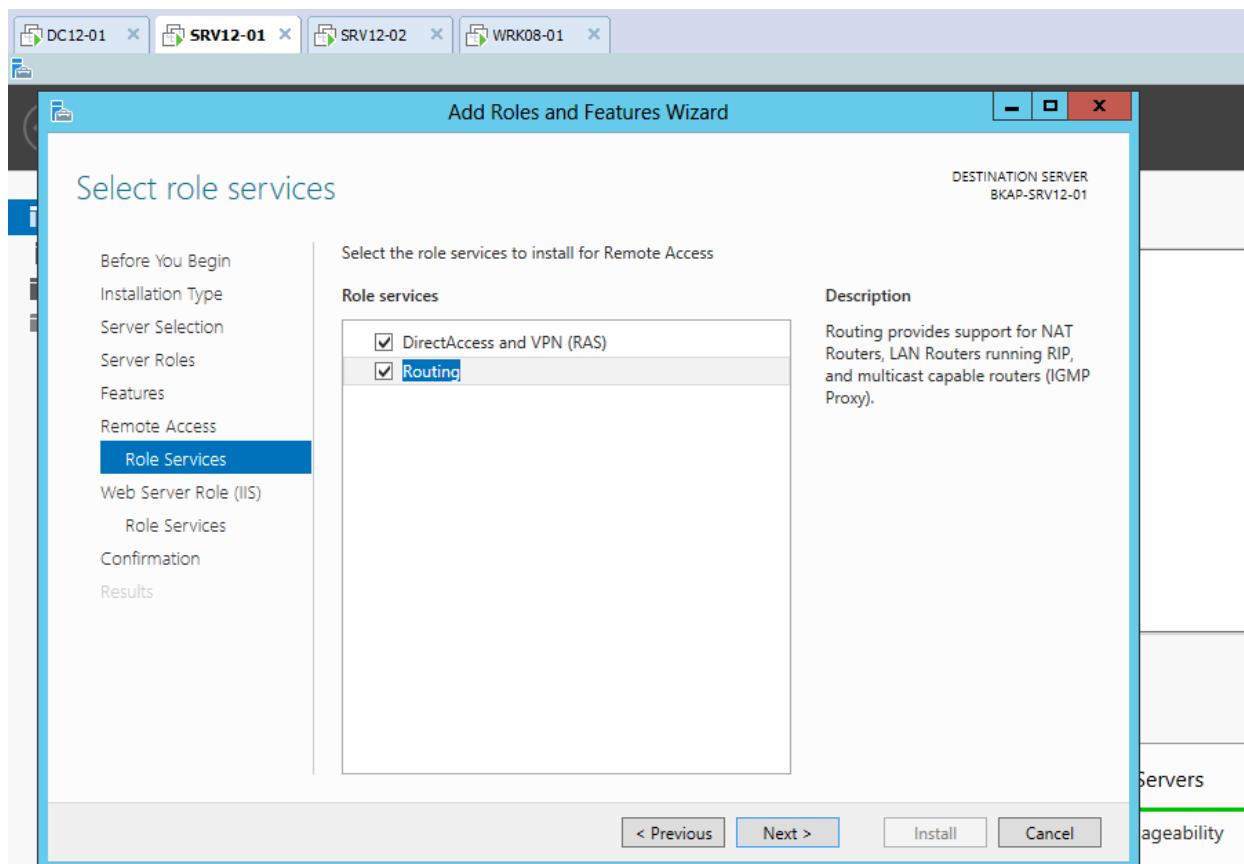


- Chuyển sang máy **BKAP-SRV12-02** thực hiện:
 - Tạo tài khoản **hcm** và cấp quyền truy cập từ xa.

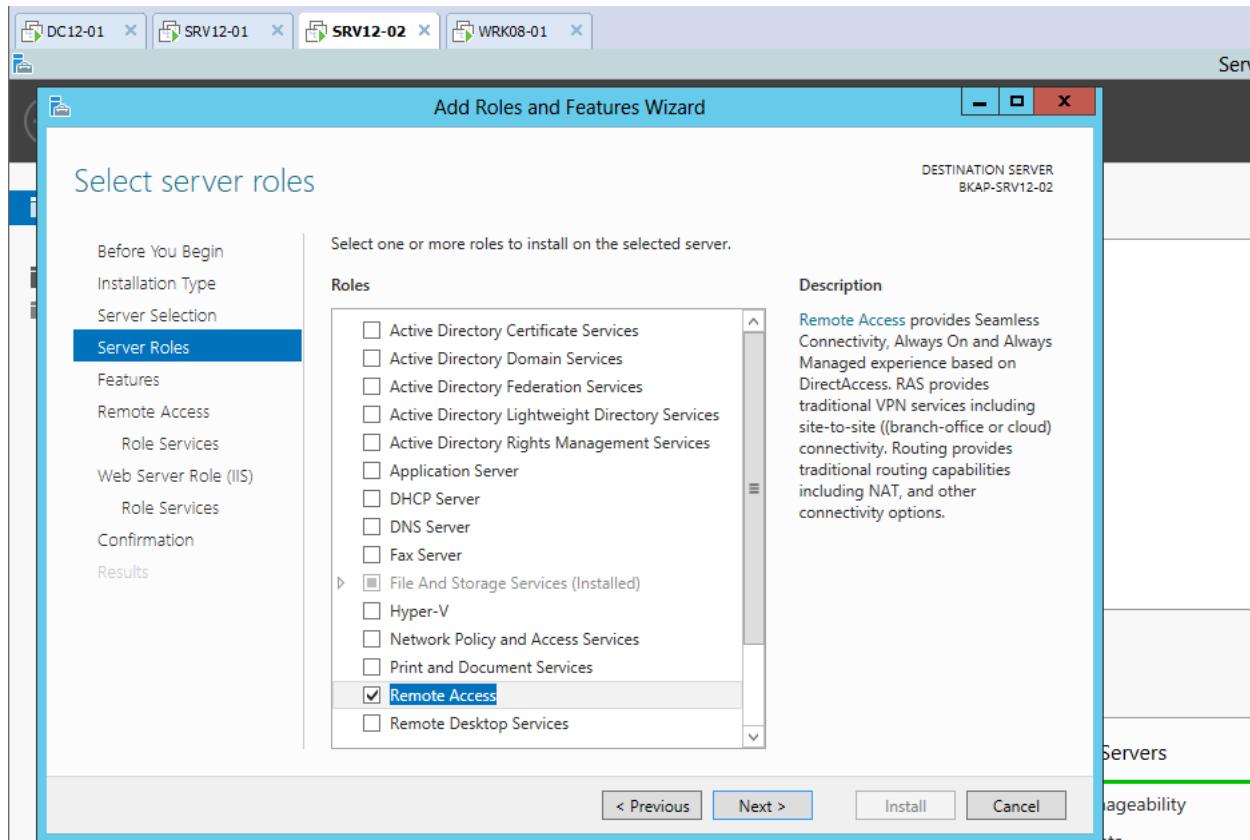


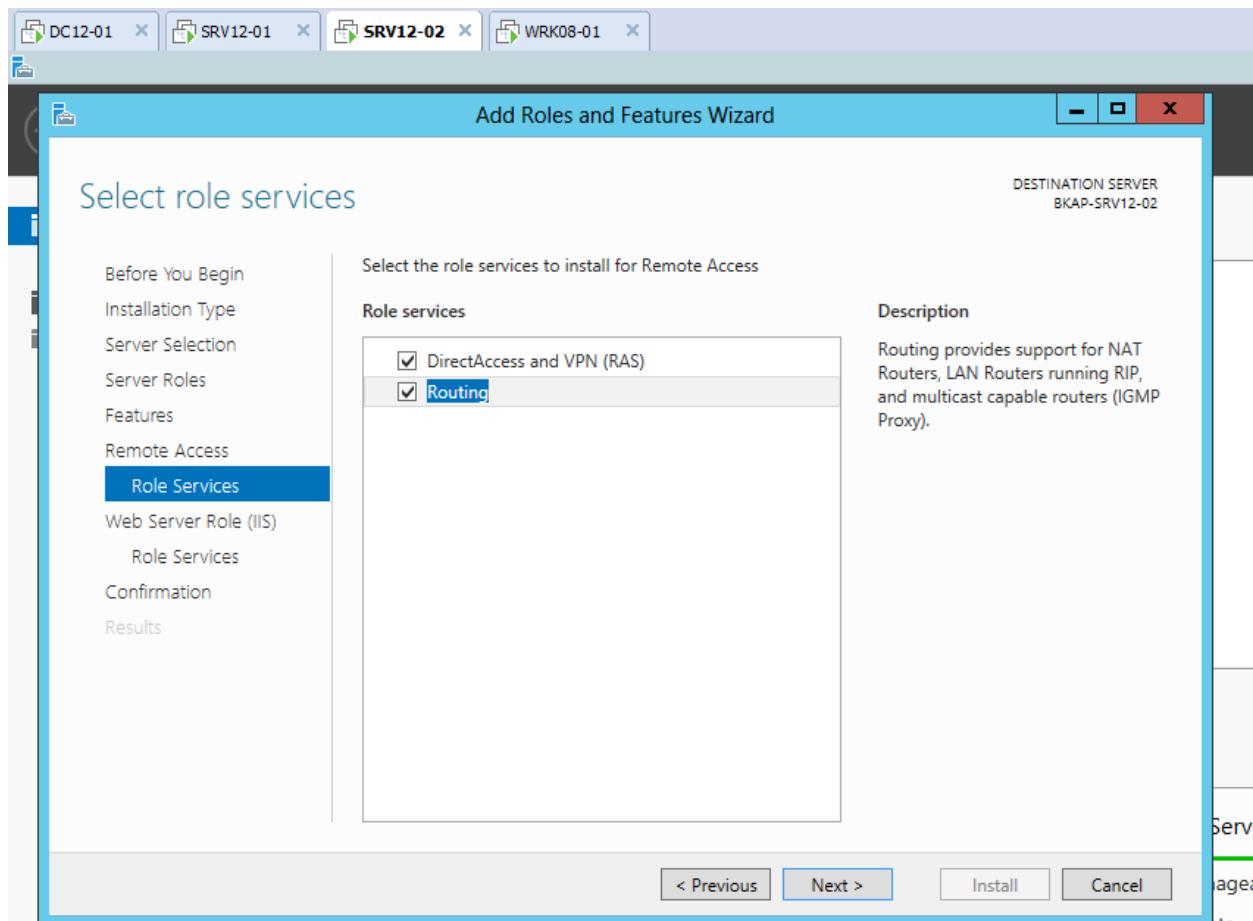
- Chuyển sang máy **BKAP-SRV12-01**, thực hiện cài đặt dịch vụ **Remote Access / Routing**:



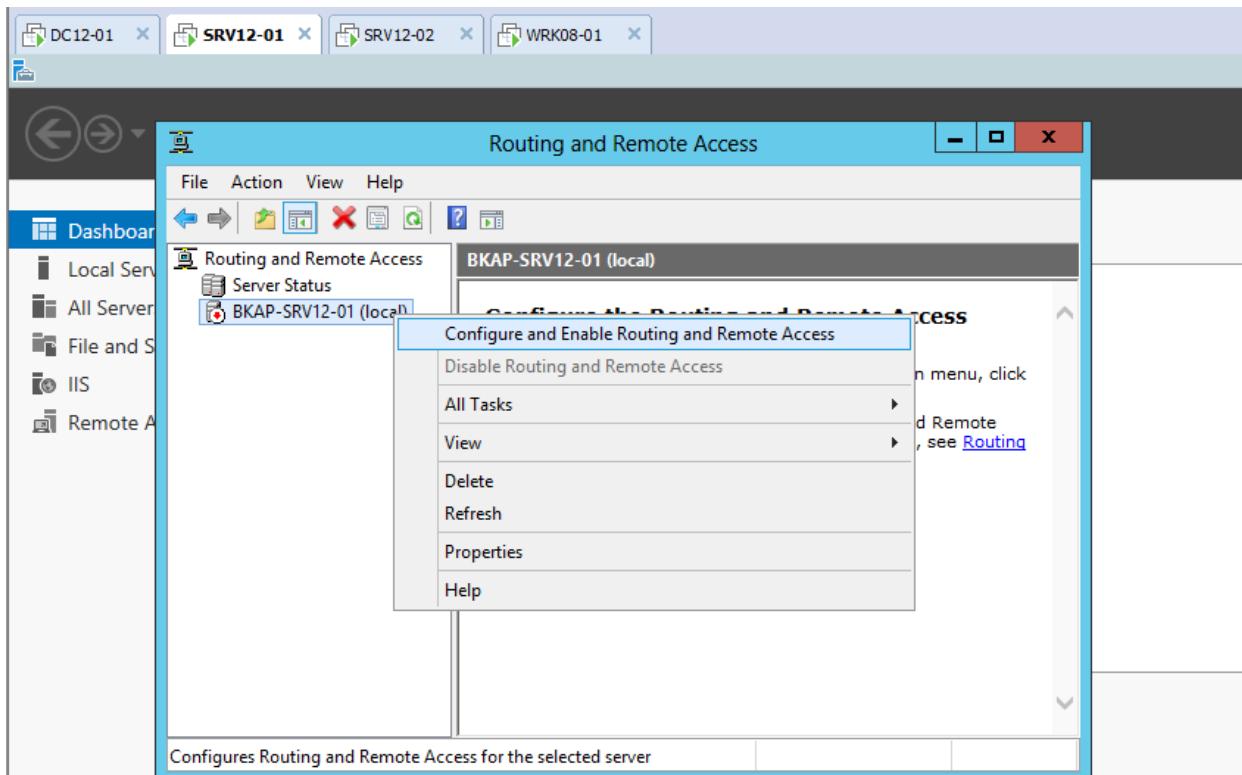


- Chuyển sang máy BKAP-SRV12-02, thực hiện cài đặt dịch vụ **Remote Access / Routing**:

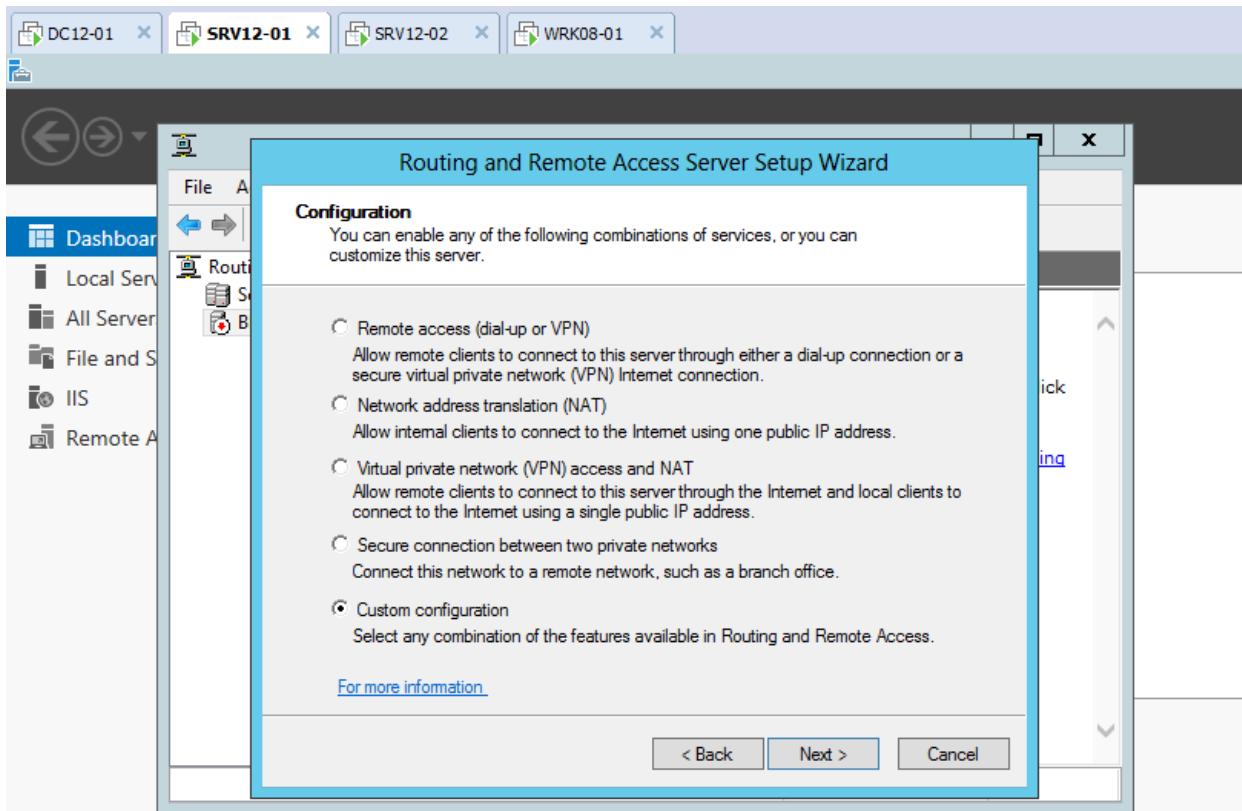




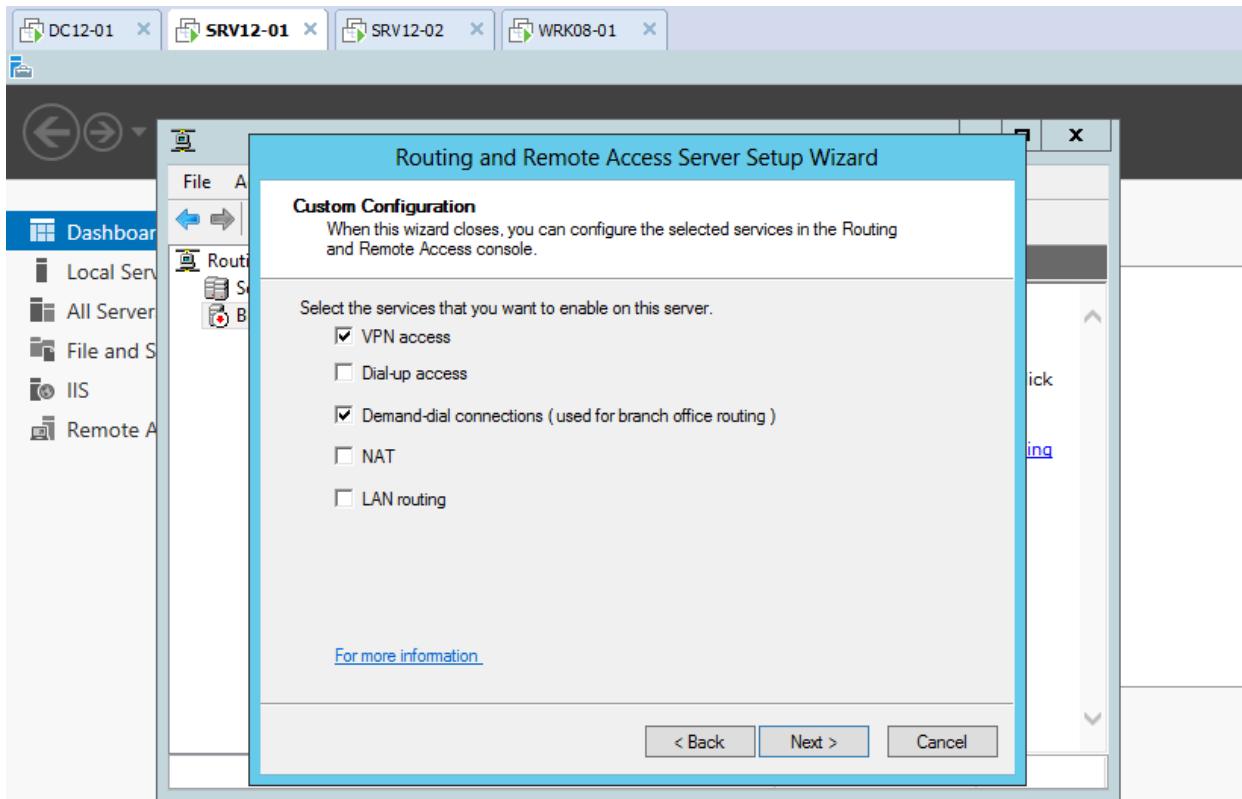
- Chuyển sang máy server **BKAP-SRV12-01** thực hiện : tạo kết nối **VPN** từ Site **HANOI** tới Site **HCM**.
 - Vào **Server Manager / Tools / Routing and Remote Access**.
 - Tại cửa sổ **Routing and Remote Access** , click chuột phải tại **BKAP-SRV12-01 (local)** , chọn **Configure and Enable Routing and Remote Access**.



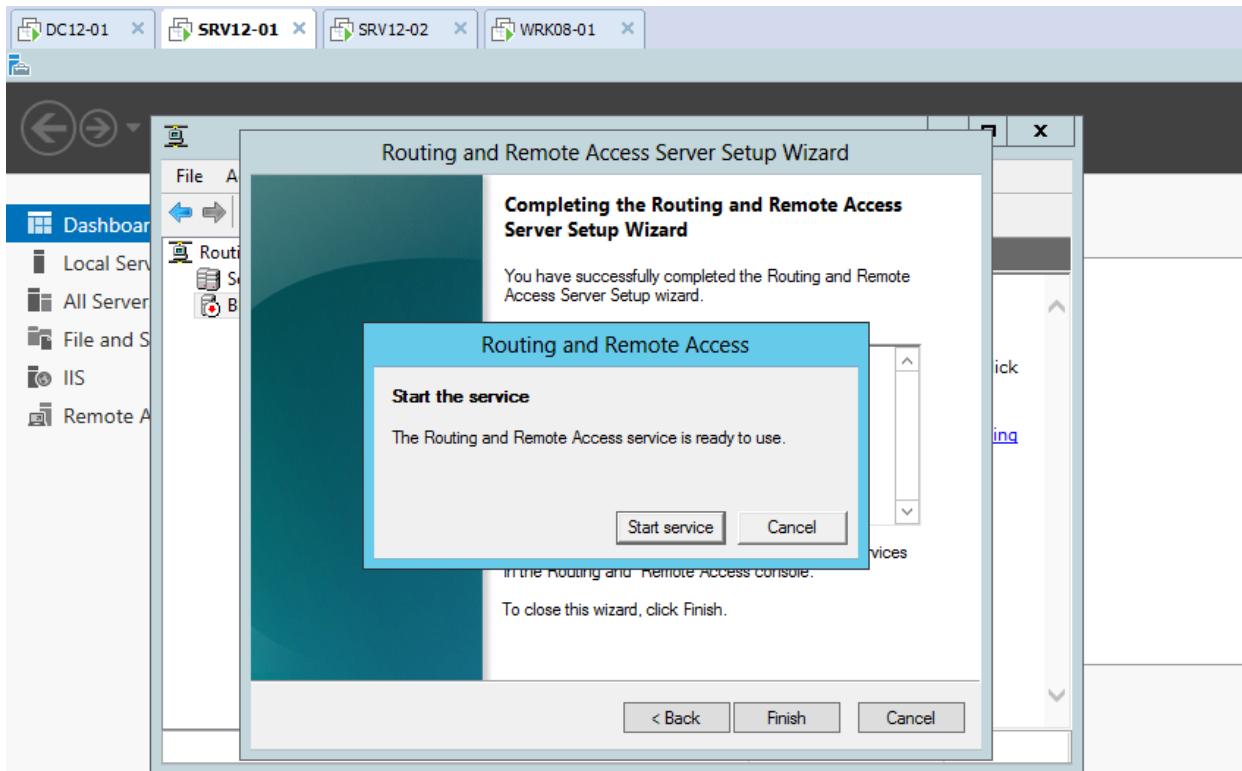
- Tại cửa sổ **Configuration**, chọn vào **Custom configuration**



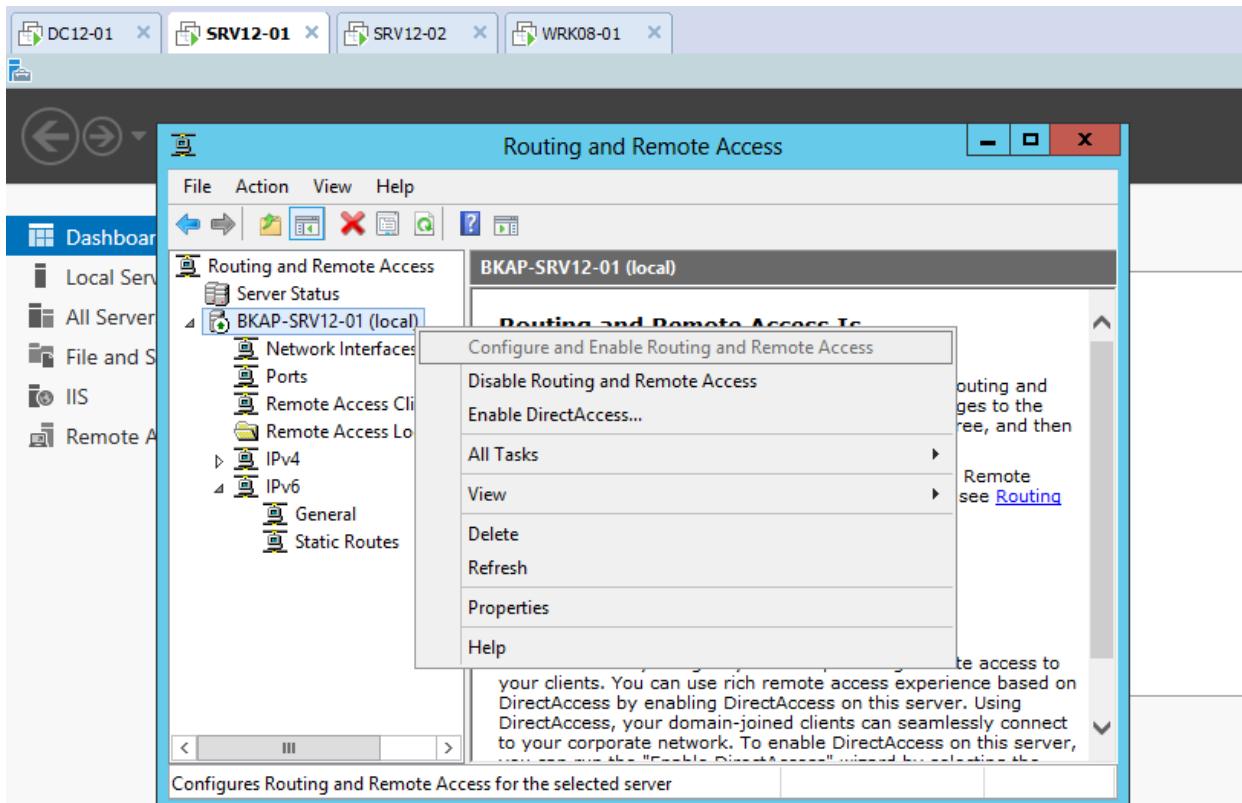
- Tại cửa sổ **Custom Configuration**, chọn vào **VPN access** và **Demand-dial connections (used for branch office routing)**



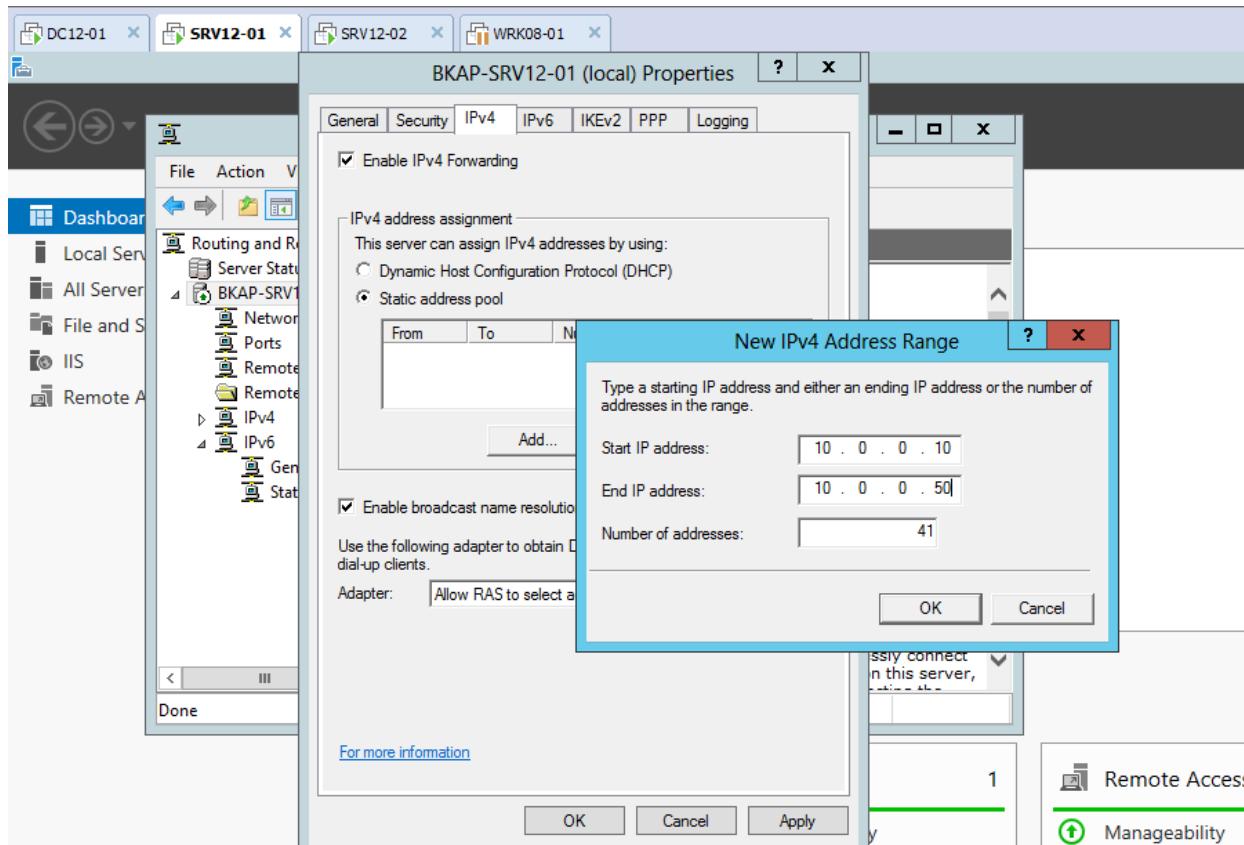
- Click vào **Finish / Start service** để hoàn tất quá trình.



- Click chuột phải tại **BKAP-SRV12-01 (local)** , chọn **Properties**.

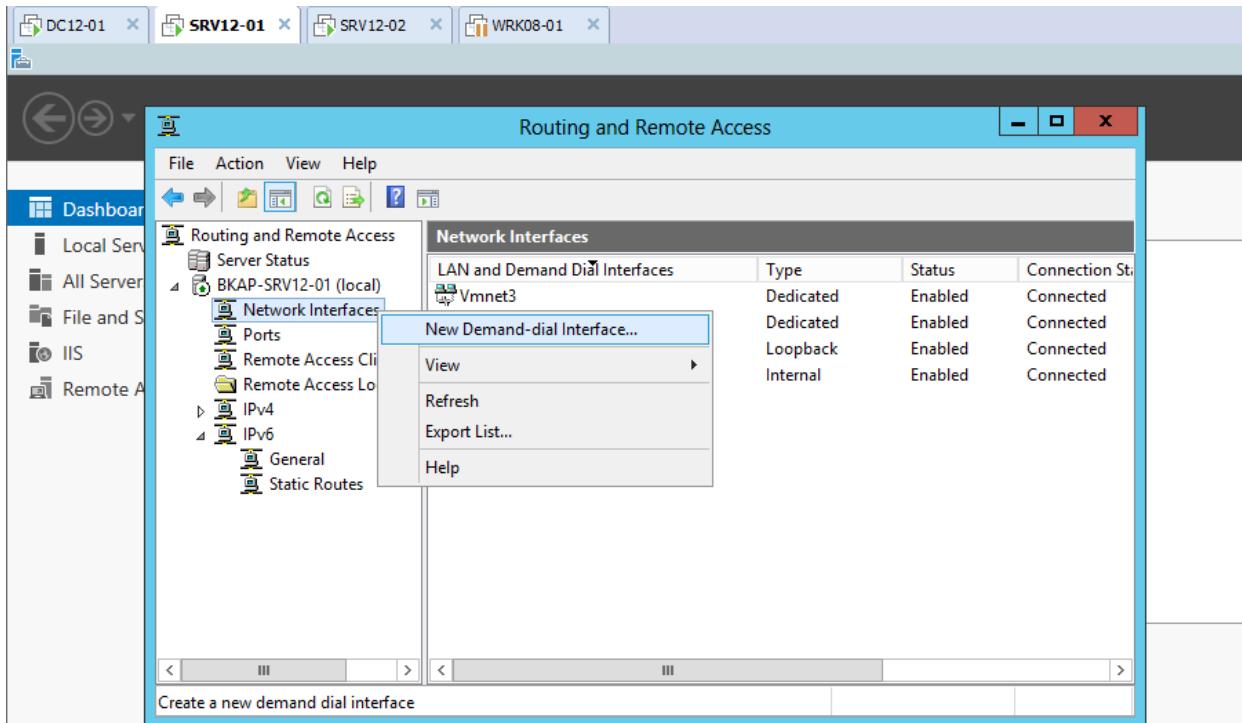


- Tại cửa sổ **BKAP-SRV12-01 (local) Properties**, chuyển sang tab **IPv4**, click chọn vào **Static address pool**, click vào **Add...**, nhập vào dải địa chỉ IP **10.0.0.10 – 10.0.0.50**.

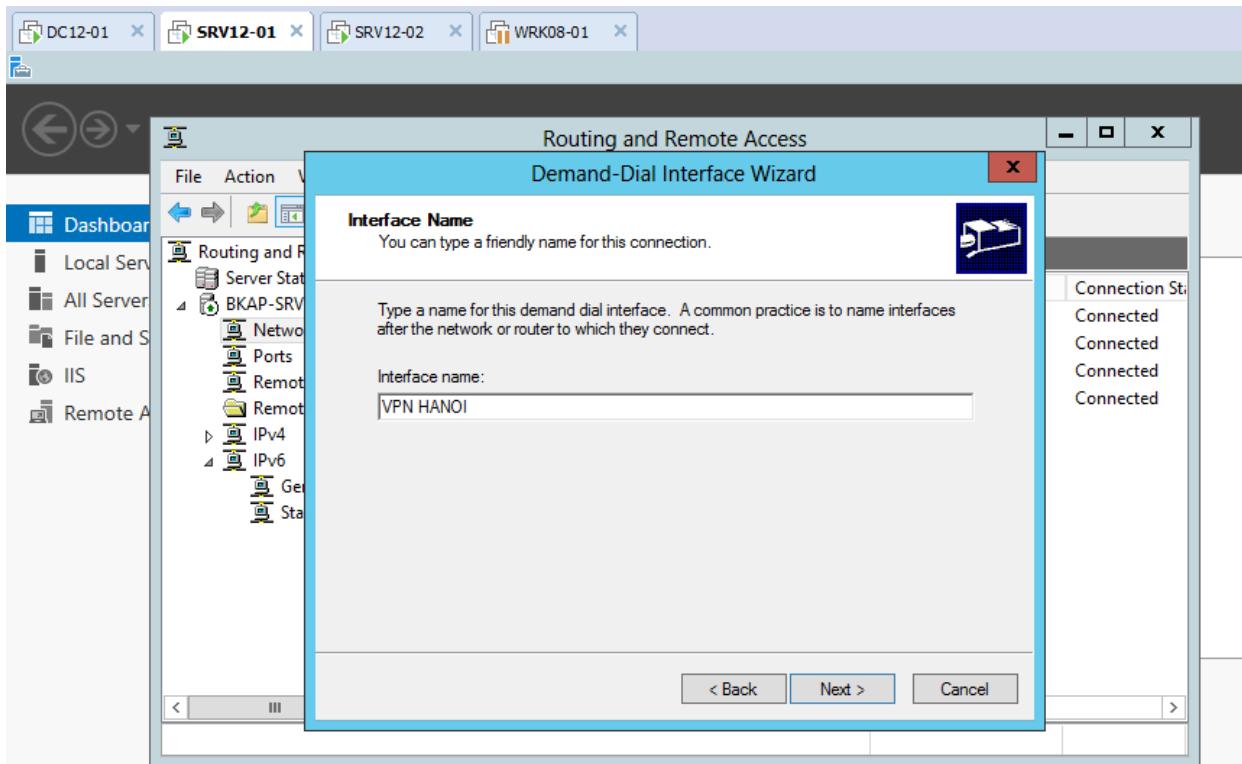


▪ **Apply / OK .**

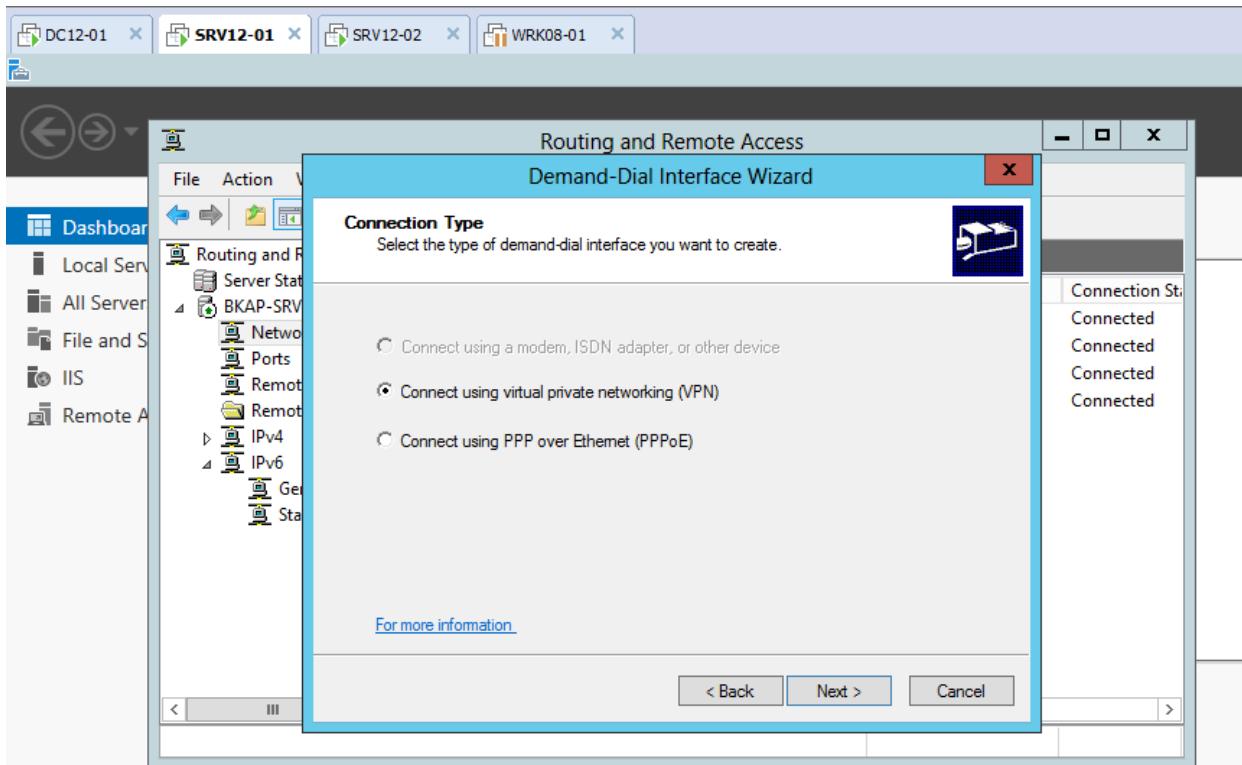
- Click chuột phải tại **Network Interface**, chọn **New Demand-dial Interface...**



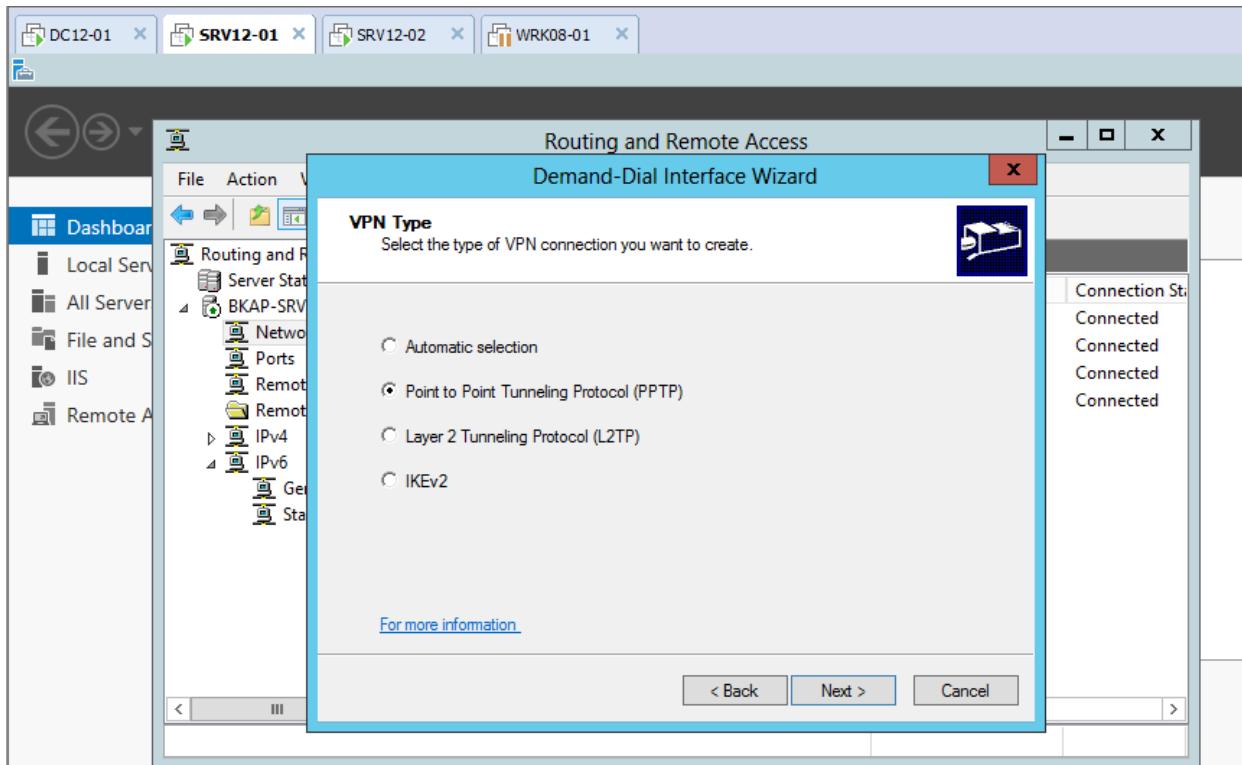
- Tại cửa sổ **Interface Name**, nhập vào tên **VPN HANOI**.



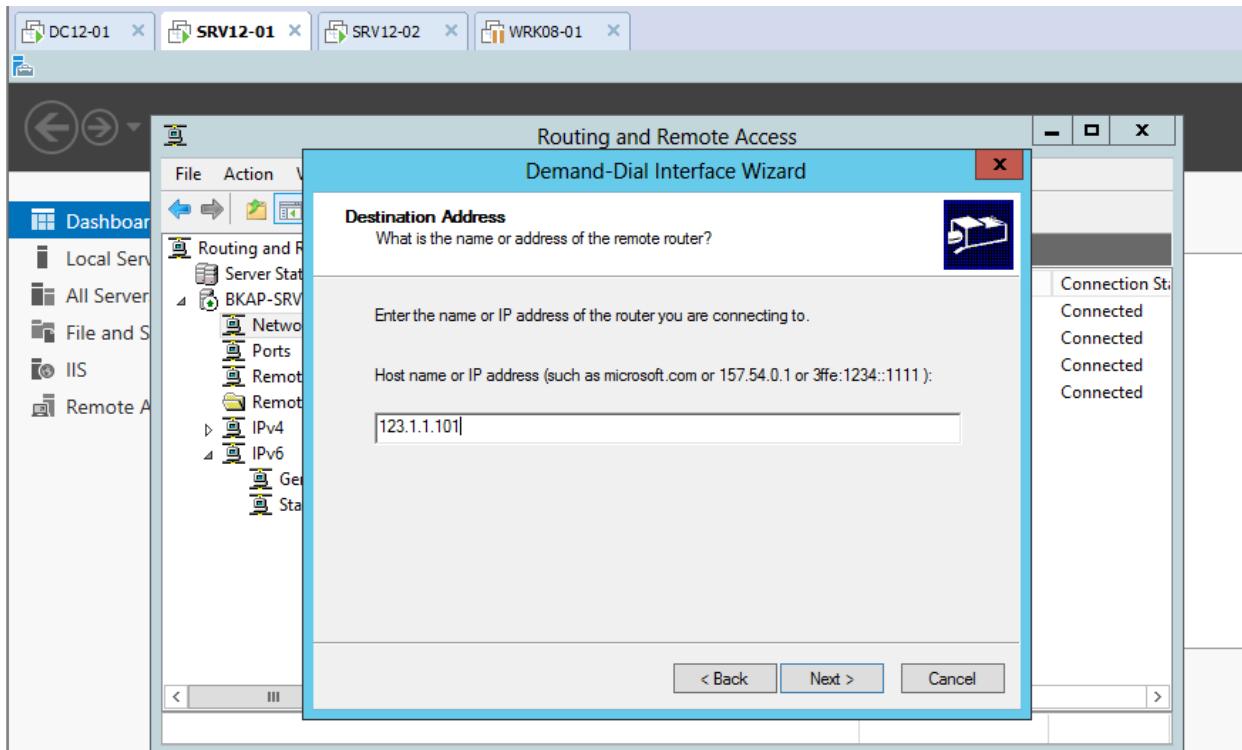
- Tại cửa sổ **Connecton Type**, chọn vào **Connect using virtual private networking (VPN)**.



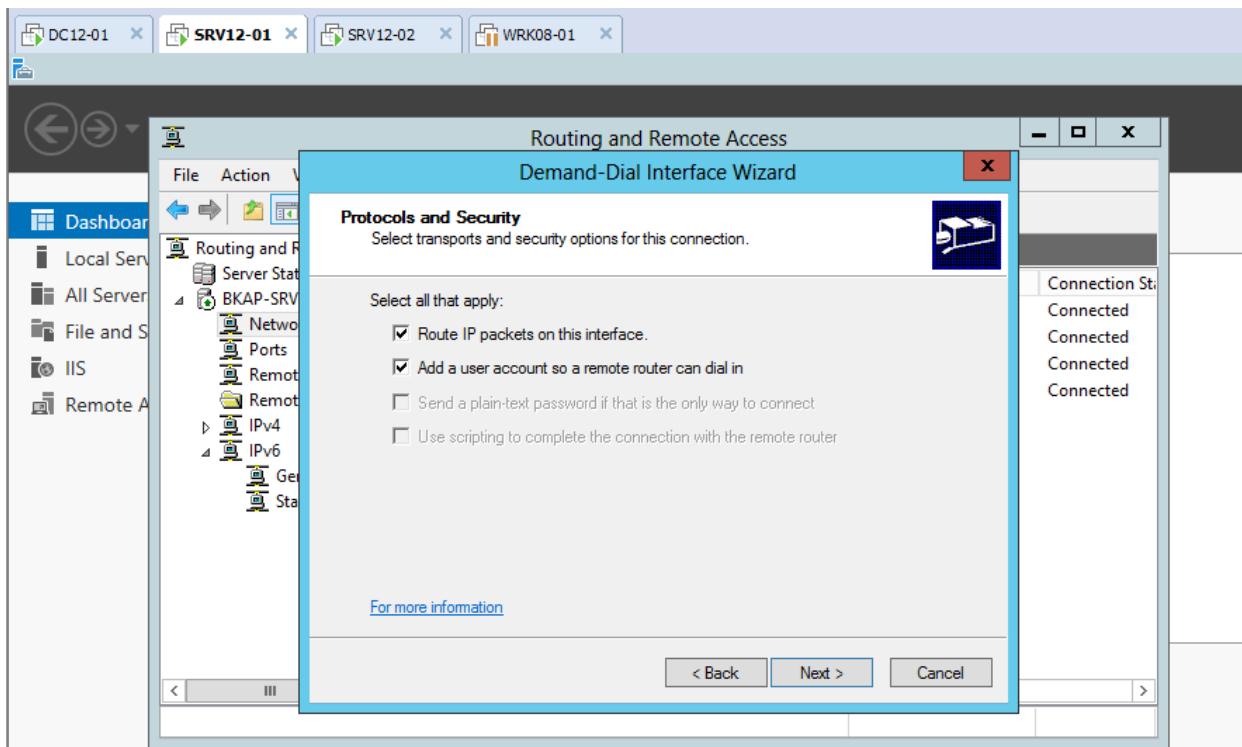
- Tại cửa sổ **VPN Type**, click chọn vào **Point to Point Tunneling Protocol (PPTP)**.



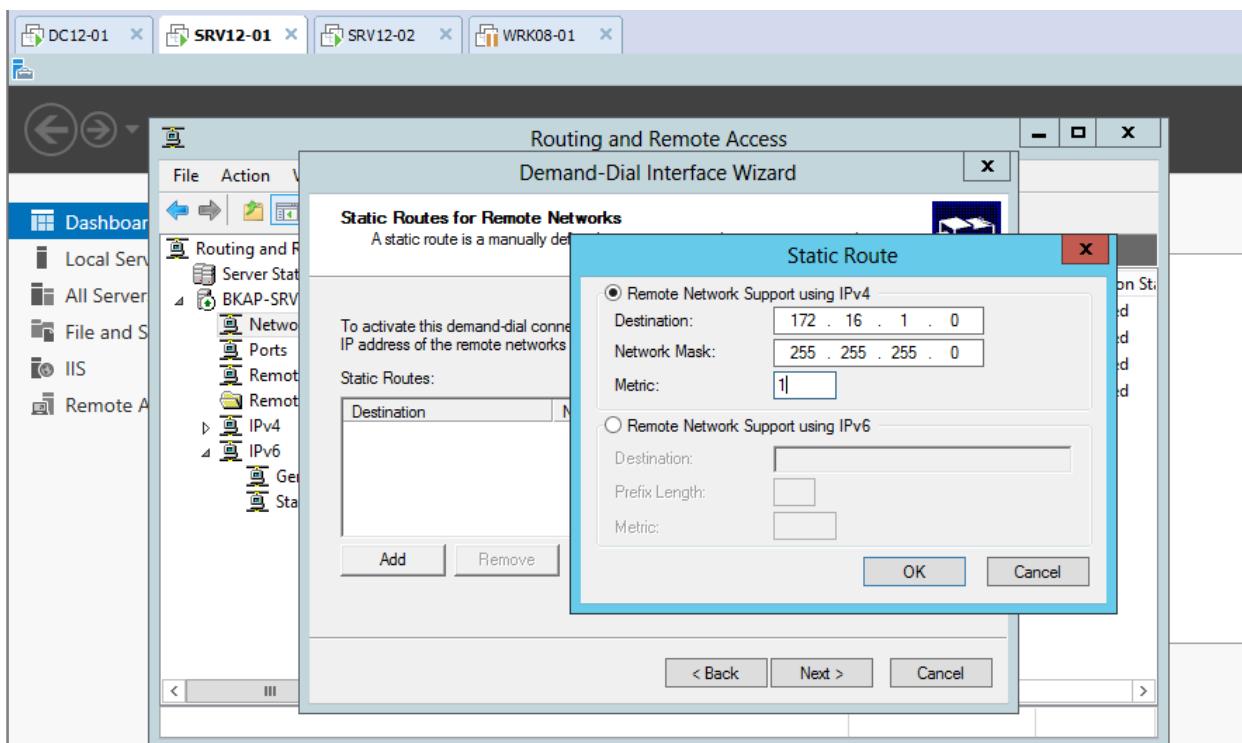
- Tại cửa sổ **Destination Address**, nhập vào địa chỉ **IP gateway** của máy **SRV12-01 : 123.1.1.101**.



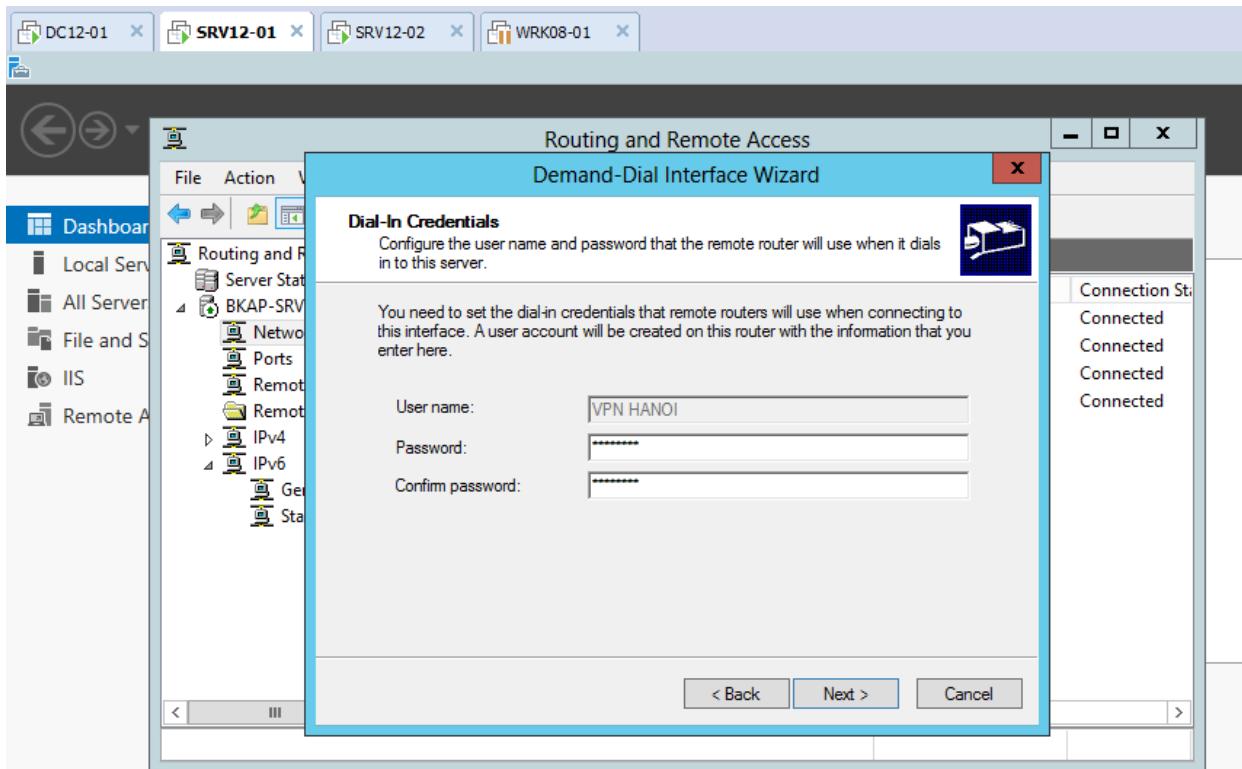
- Tại cửa sổ **Protocols and Security**, click chọn vào **Router IP packets on this interface** và **Add a user account so a remote router can dial in**.



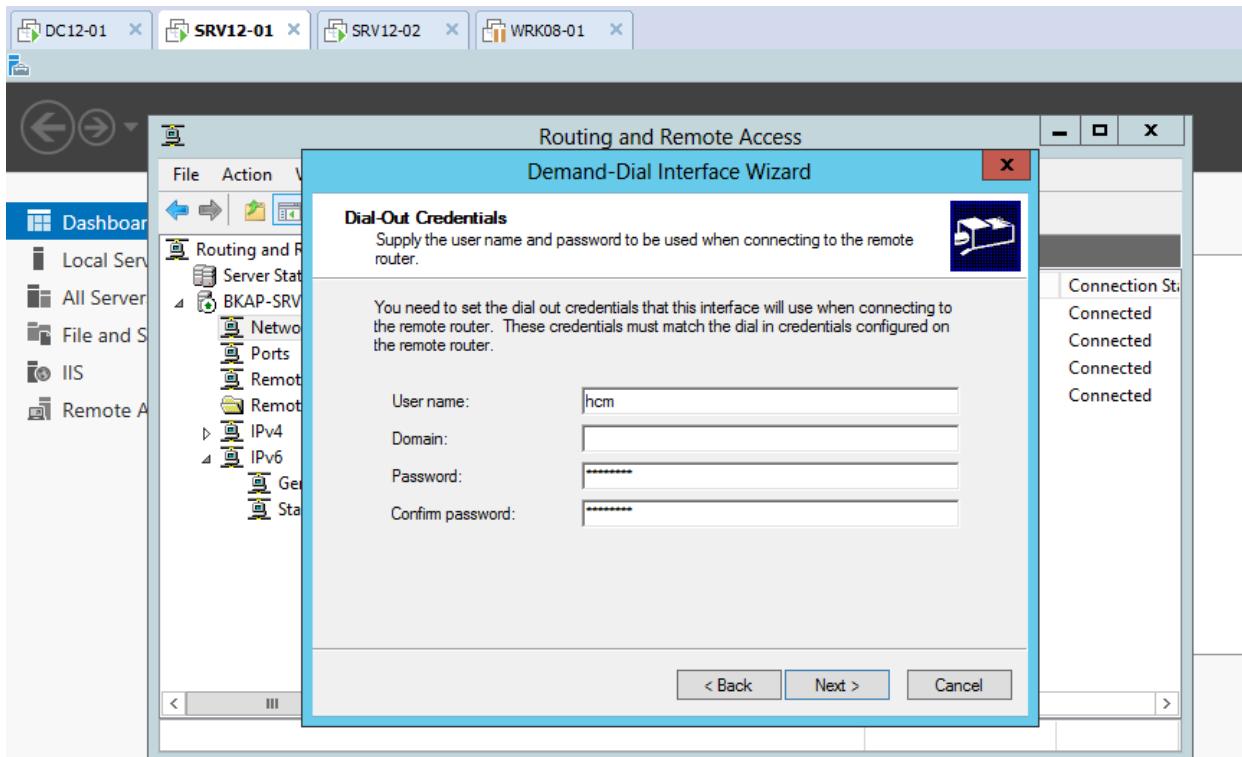
- Tại cửa sổ **Static Routers for Remote Networks**, click vào **Add** , tại cửa sổ **Static Route** nhập vào các thông số :
 - *Destination : 172.16.1.0*
 - *Network Mask : 255.255.255.0*
 - *Metric : 1*



- Tại cửa sổ **Dial-In Credentials**, nhập vào **Password** của user **VPN HANOI**:



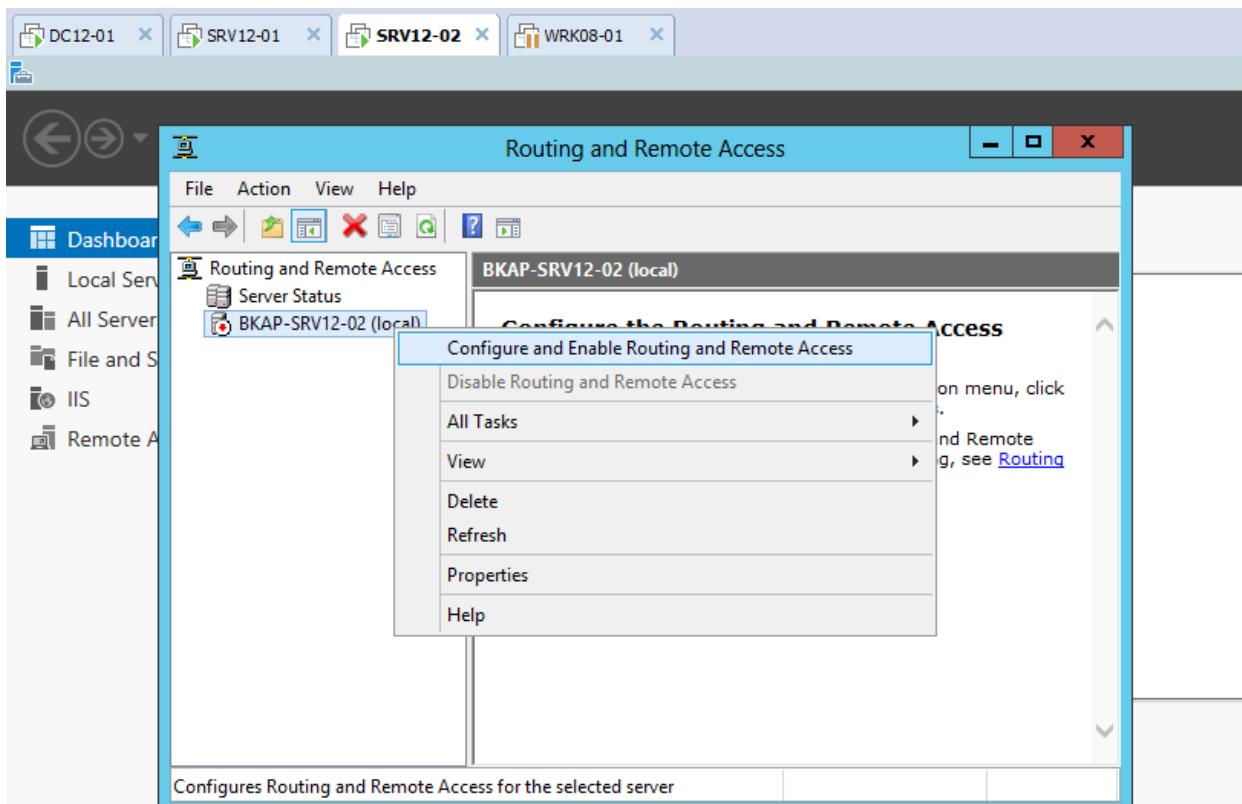
- Tại cửa sổ **Dial-out Credentials**, nhập vào *User* tạo trên máy *BKAP-SRV12-02*.



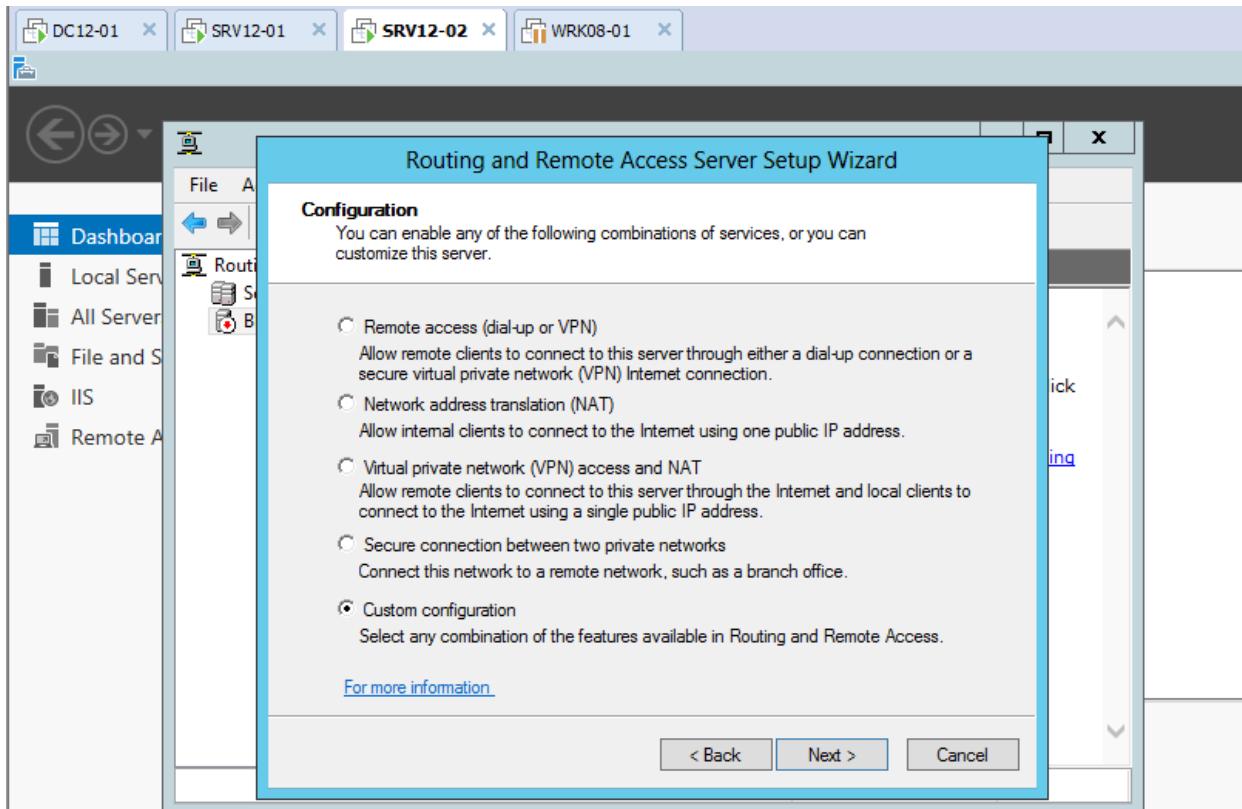
- Click vào **Finish** để kết thúc quá trình cấu hình.

- Chuyển sang máy Server **BKAP-SRV12-02**, thực hiện tạo kết nối site **HCM** tới site **HANOI**.

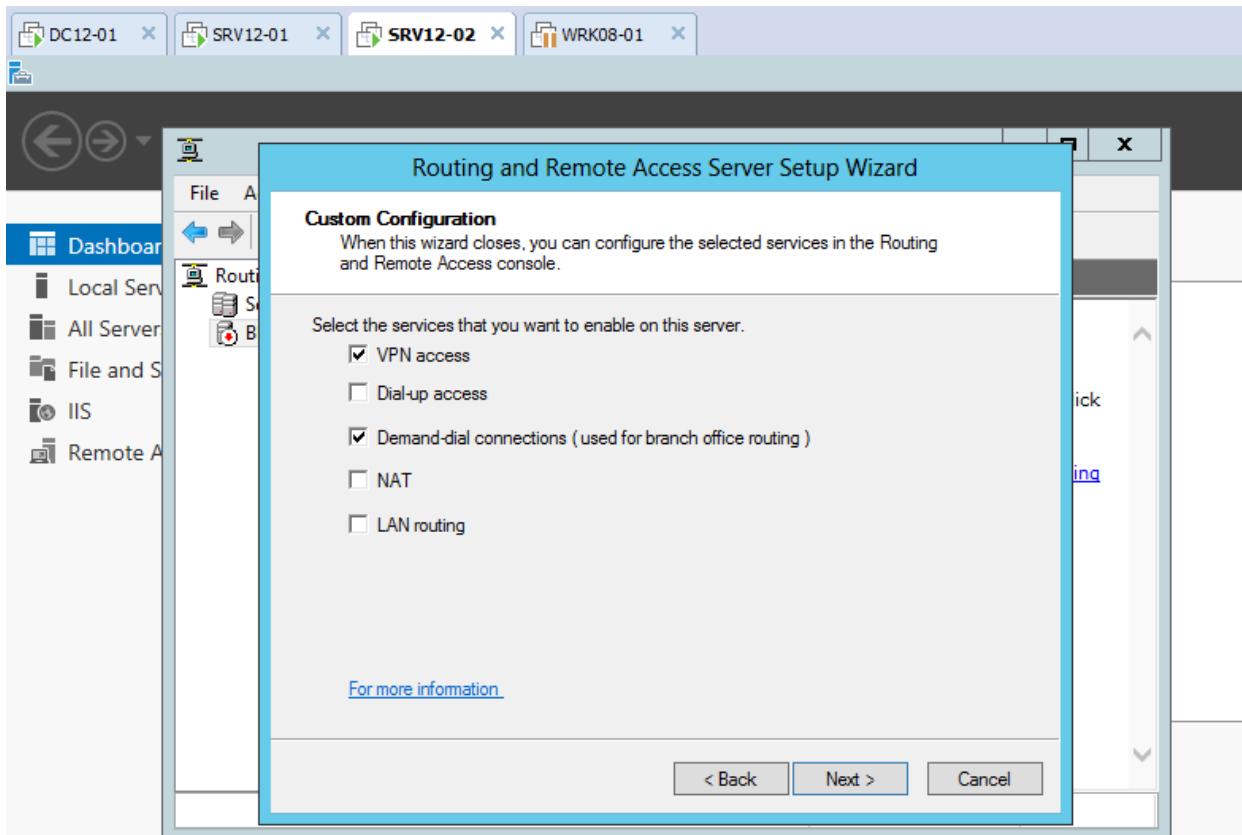
- Tại cửa sổ **Routing and Remote Access**, click chuột phải vào **BKAP-SRV12-02 (local)** , chọn vào **Configure and Enable Routing and Remote Access**.



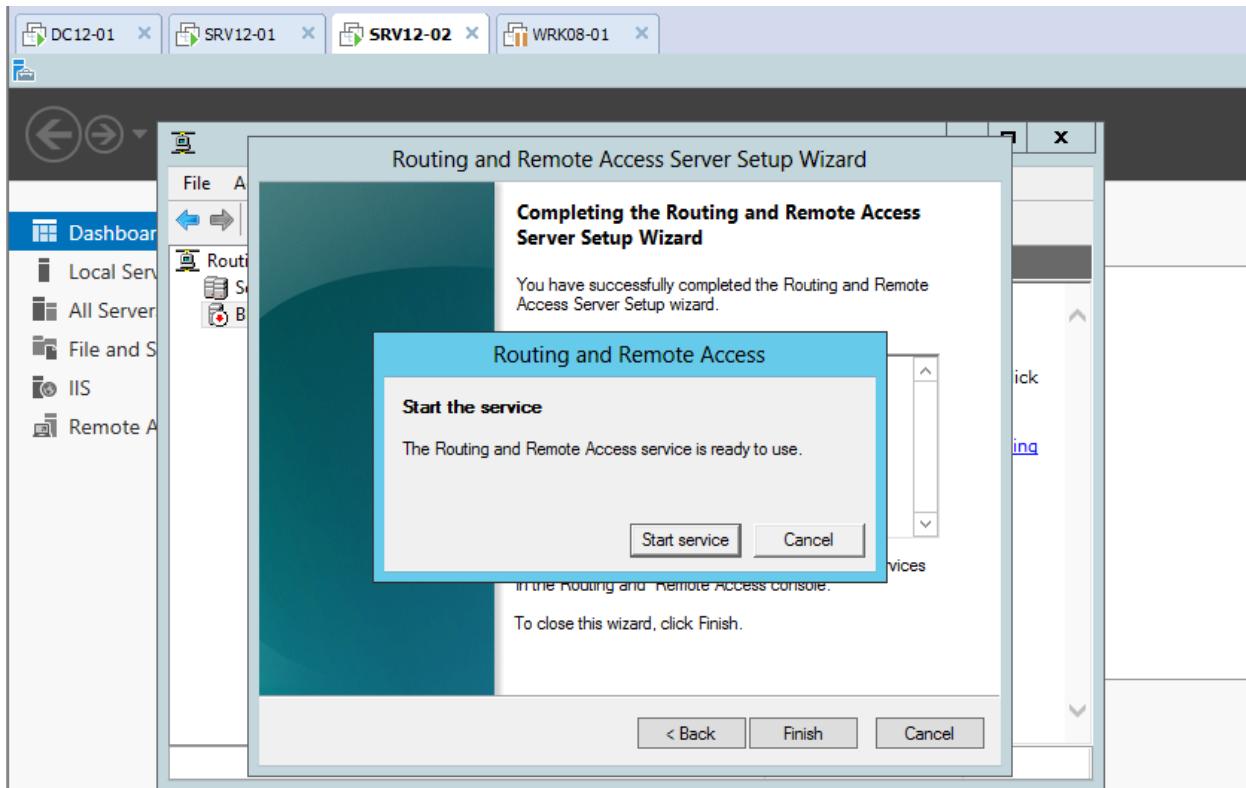
- Tại cửa sổ **Configuration**, chọn vào **Custom configuration**



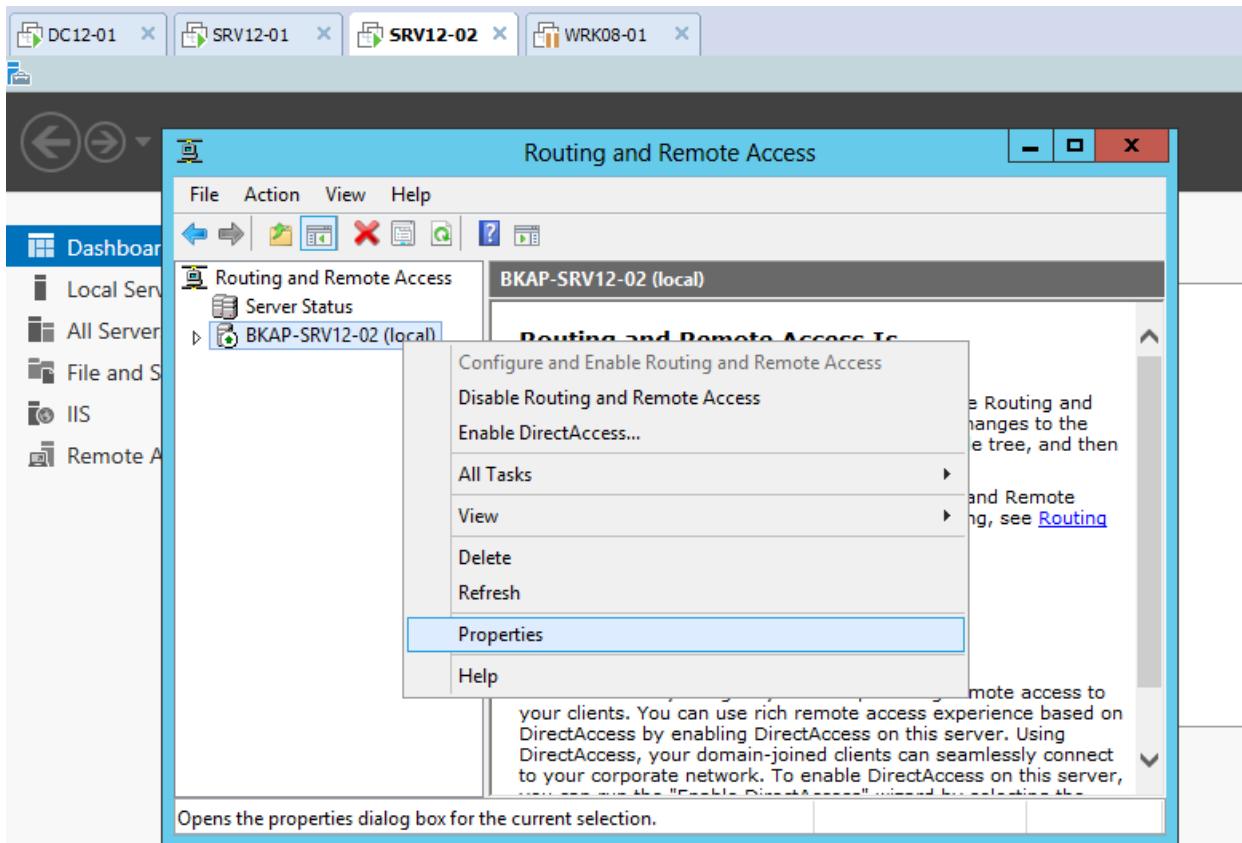
- Tại cửa sổ **Custom Configuration**, chọn vào **VPN access** và **Demand-dial connections (used for branch office routing)**



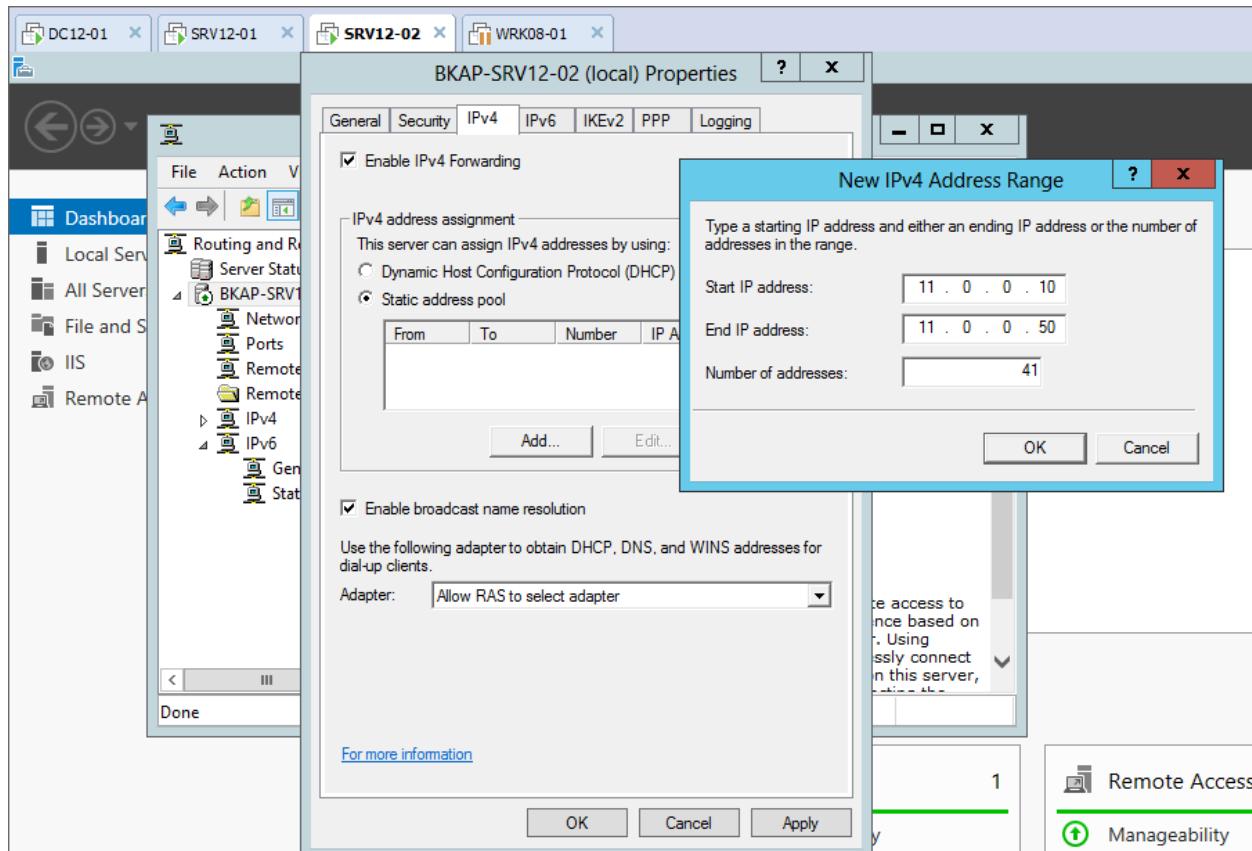
- Click vào **Finish / Start service** để kết thúc tiến trình .



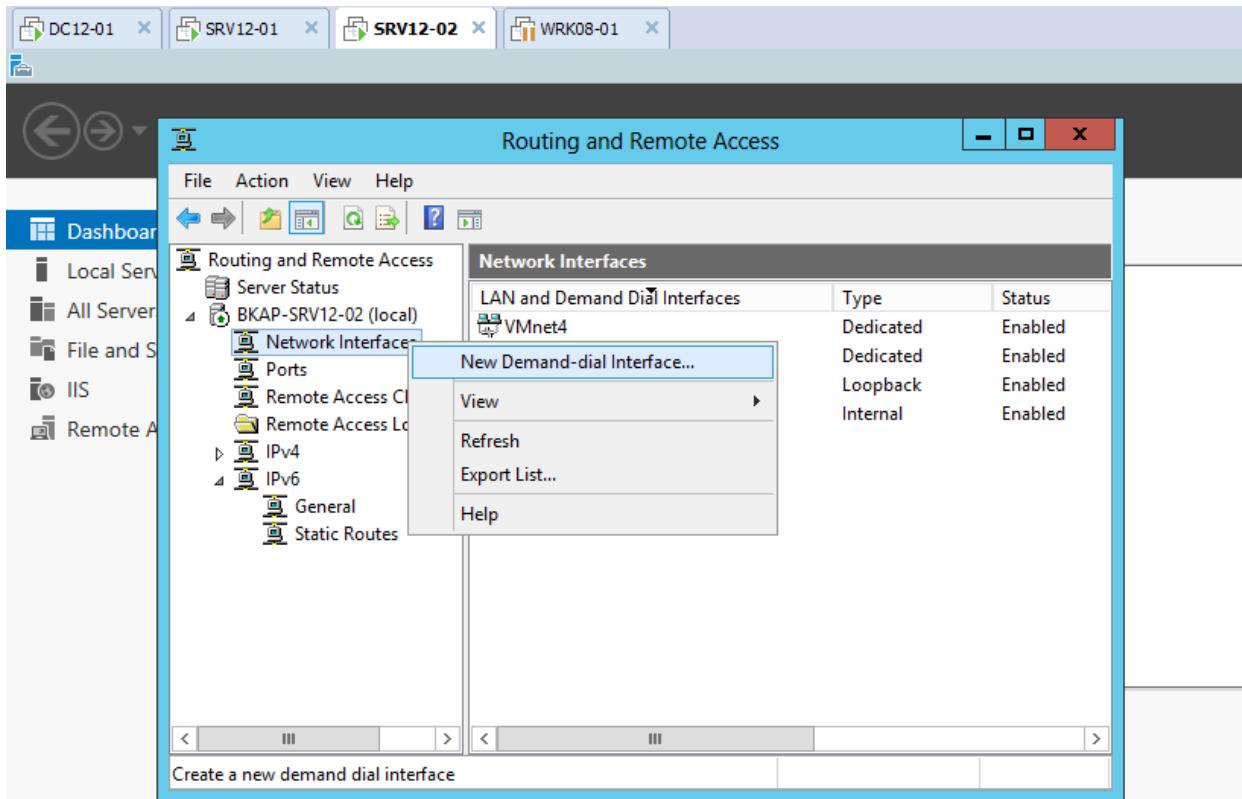
- Click chuột phải tại **BKAP-SRV12-02 (local)**, chọn **Properties**.



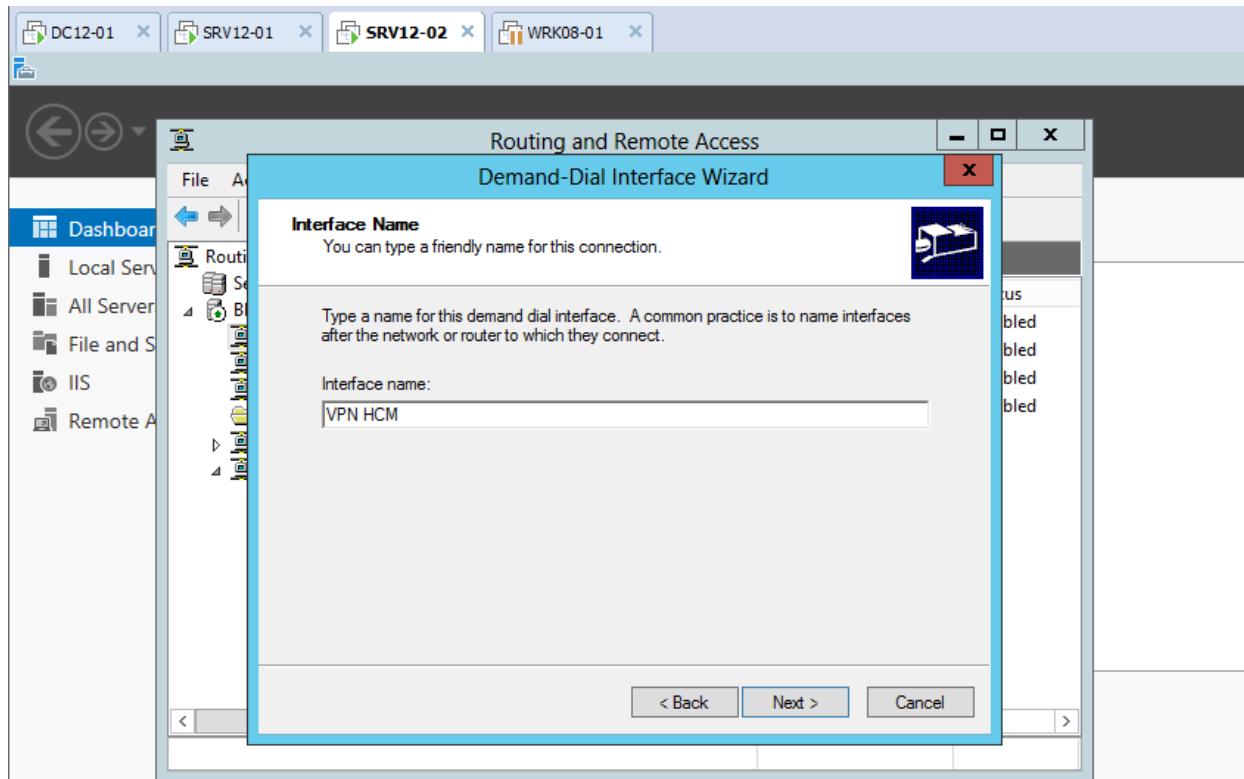
- Tại cửa sổ **BKAP-SRV12-02 (local) Properties**, chuyển sang tab **IPv4**, chọn vào **Static address pool**, click vào **Add...** tại cửa sổ **New IPv4 Address Range**, nhập vào dải địa chỉ **11.0.0.10 – 11.0.0.50**.



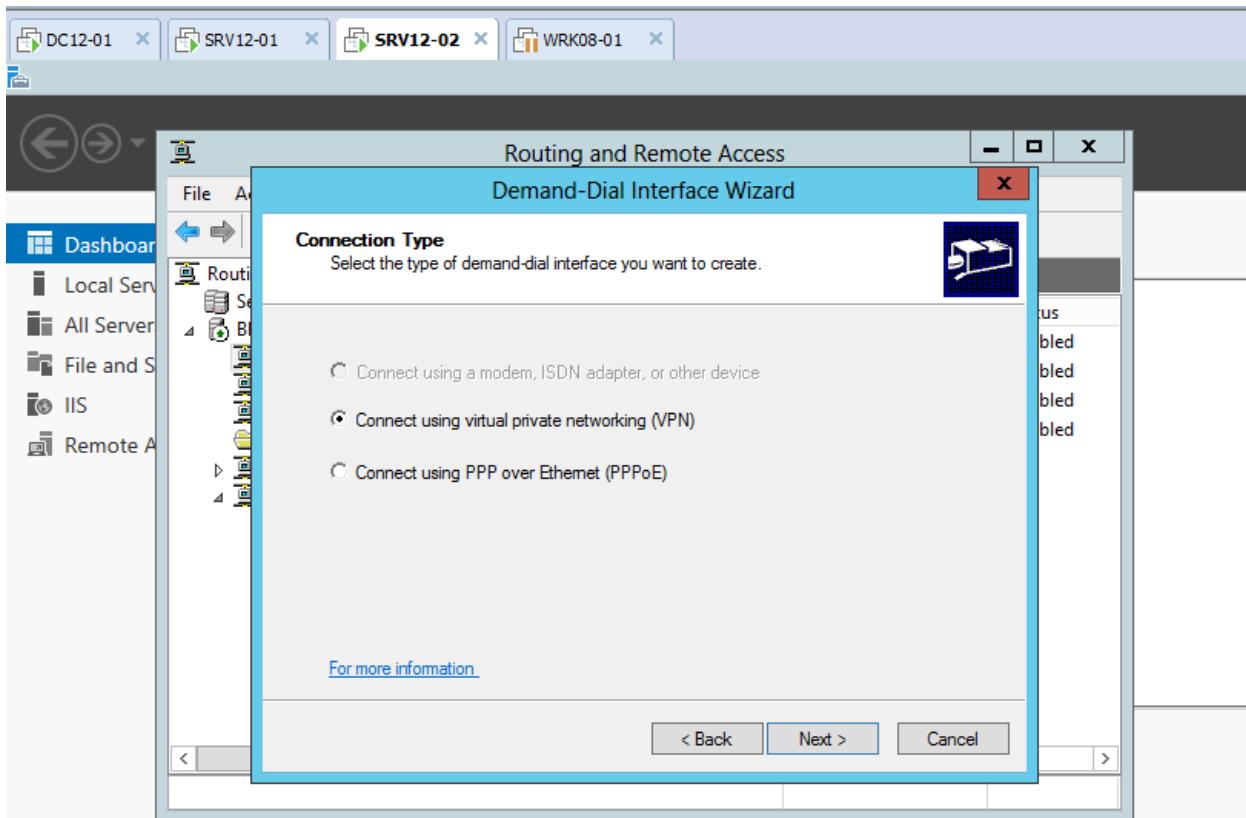
- Click chuột phải tại **Network Interface** , chọn **New Demand-dial Interface..**



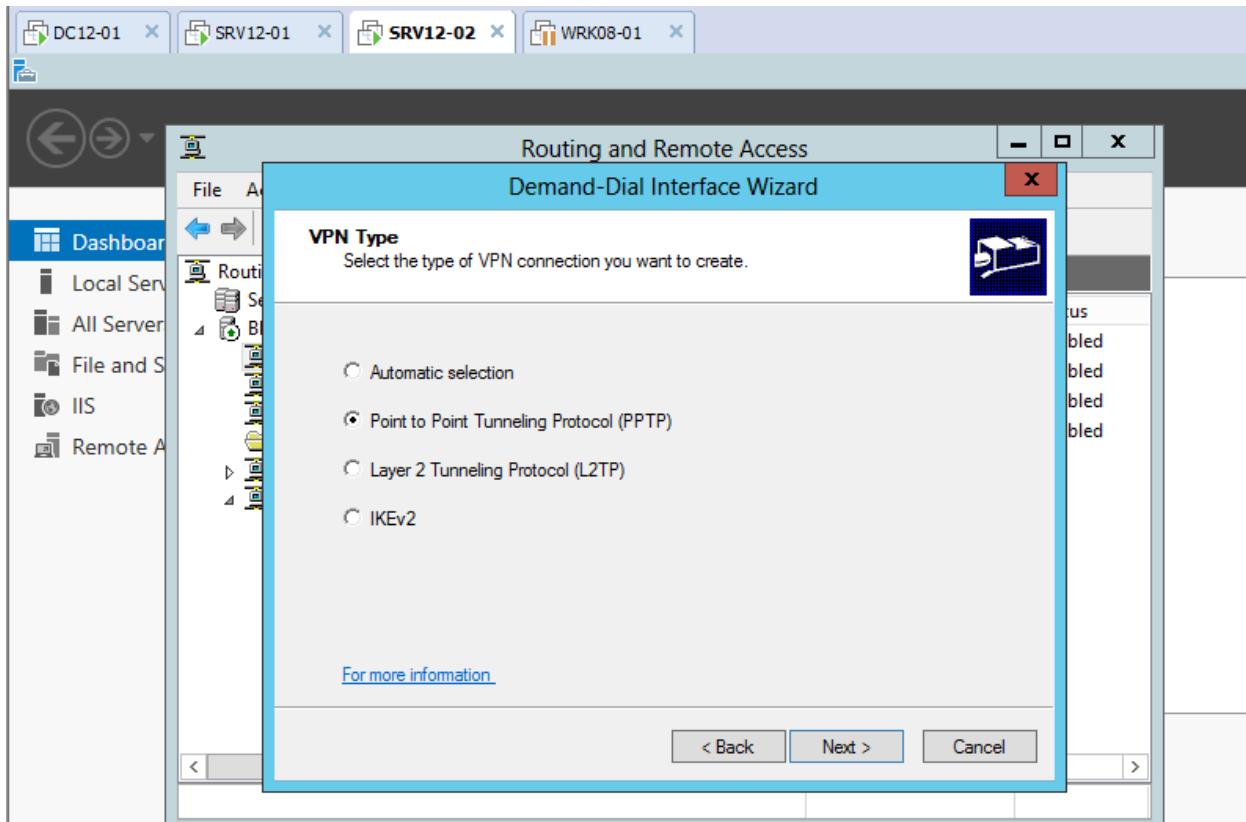
- Tại cửa sổ **Interface Name**, nhập vào tên **VPN HCM**.



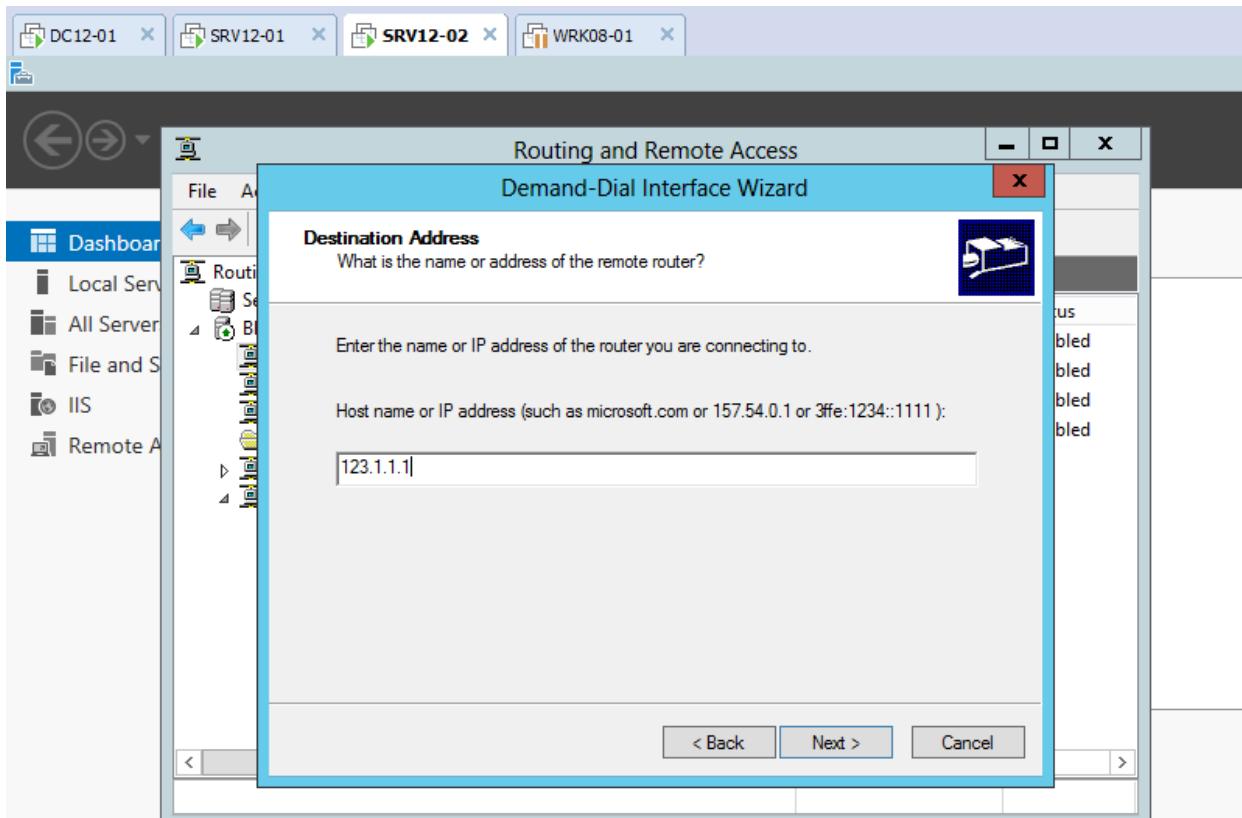
- Tại cửa sổ **Connection Type**, chọn vào **Connect using virtual private networking (VPN)**.



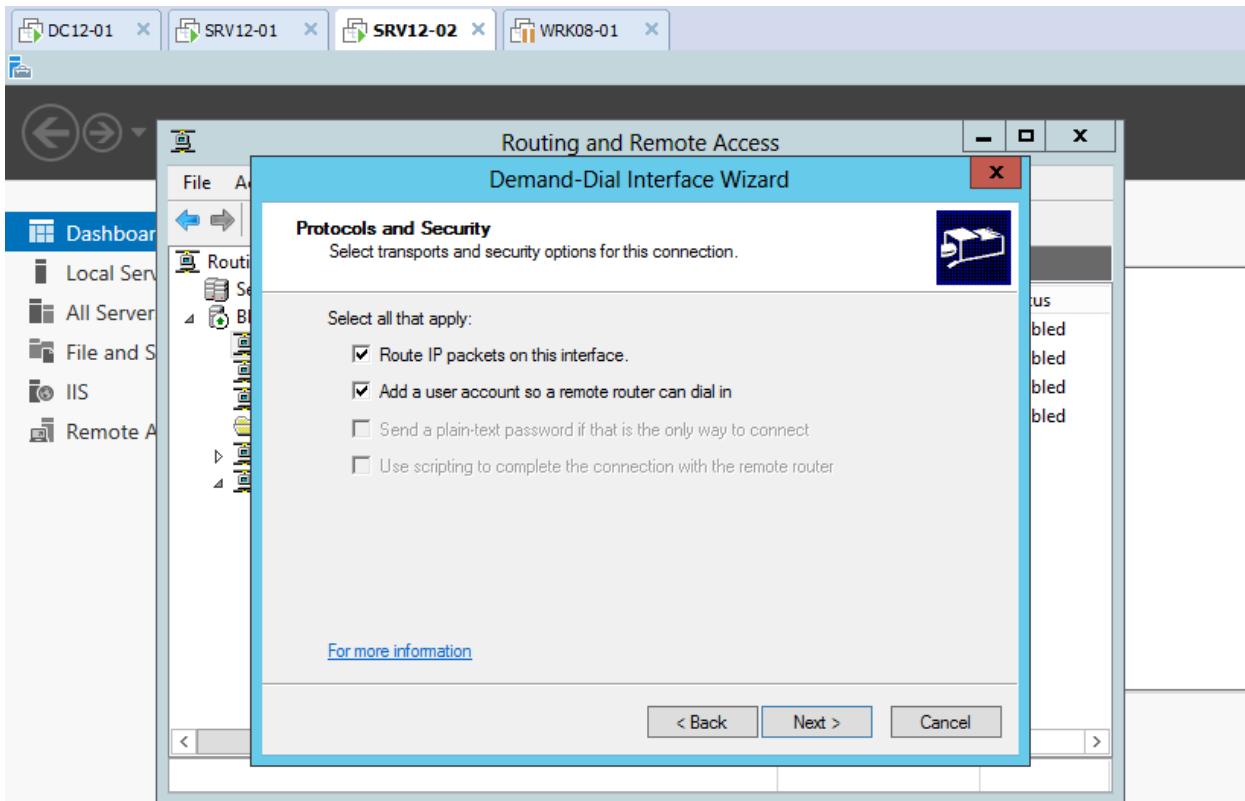
- Tại cửa sổ **VPN Type**, chọn vào Point to Point Tunneling Protocol (PPTP).



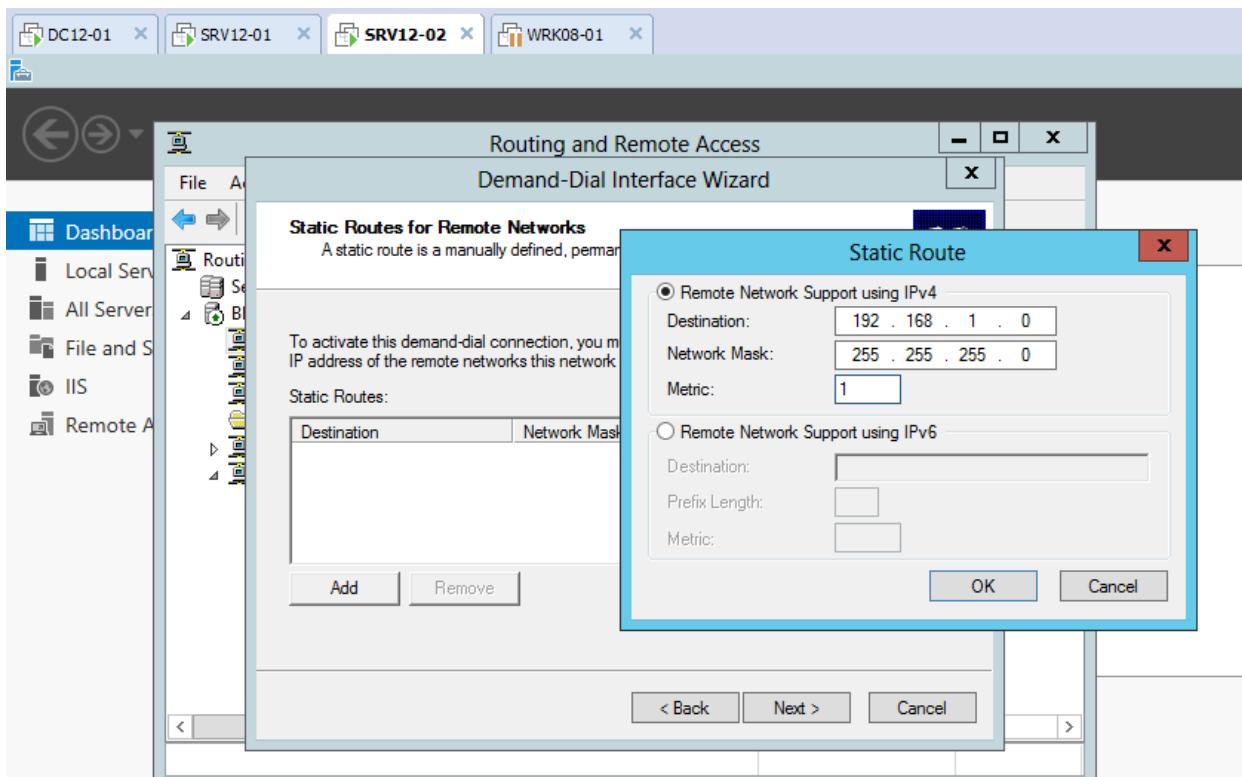
- Tại cửa sổ **Destination Address**, nhập vào địa chỉ **Gateway** của máy **BKAP-SRV12-02** : 123.1.1.1.



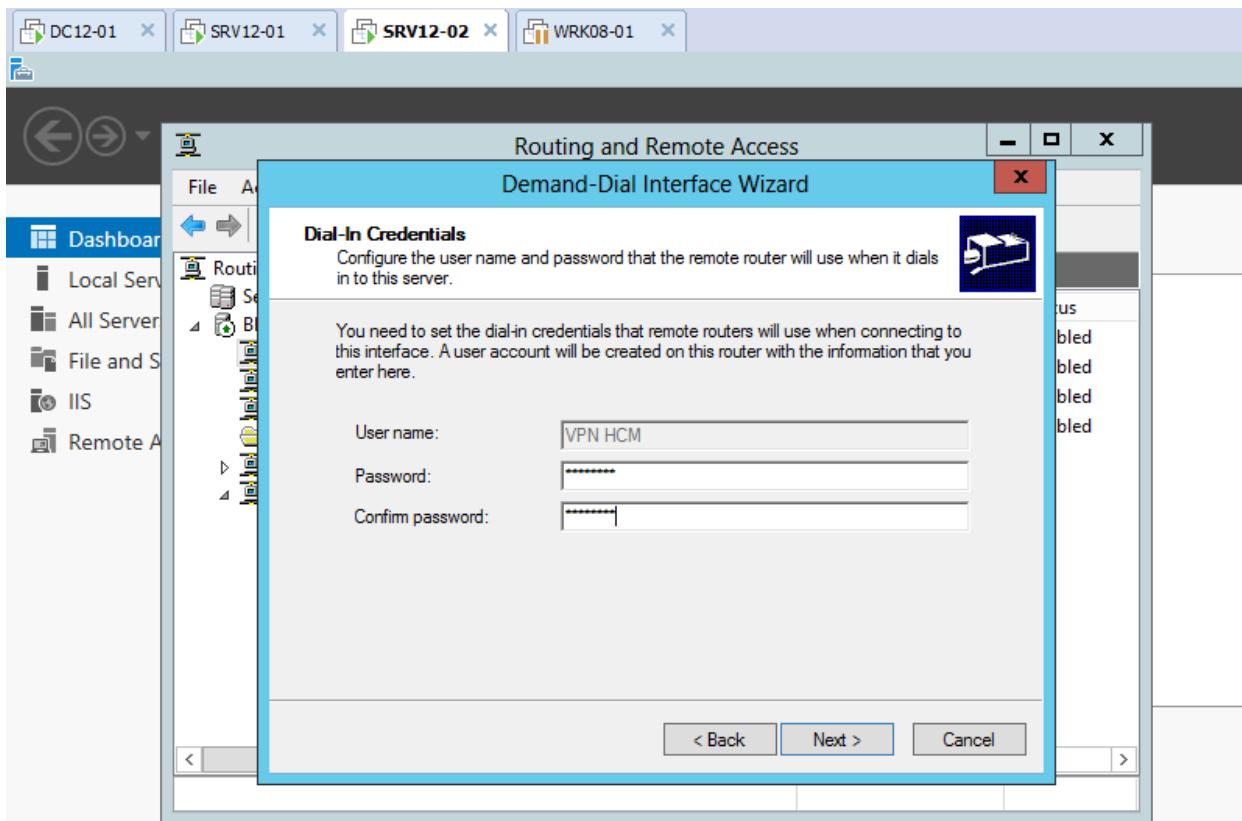
- Tại cửa sổ **Protocol and Security**, click chọn vào cả 2 dòng **Router IP ...** và **Add a user account...**



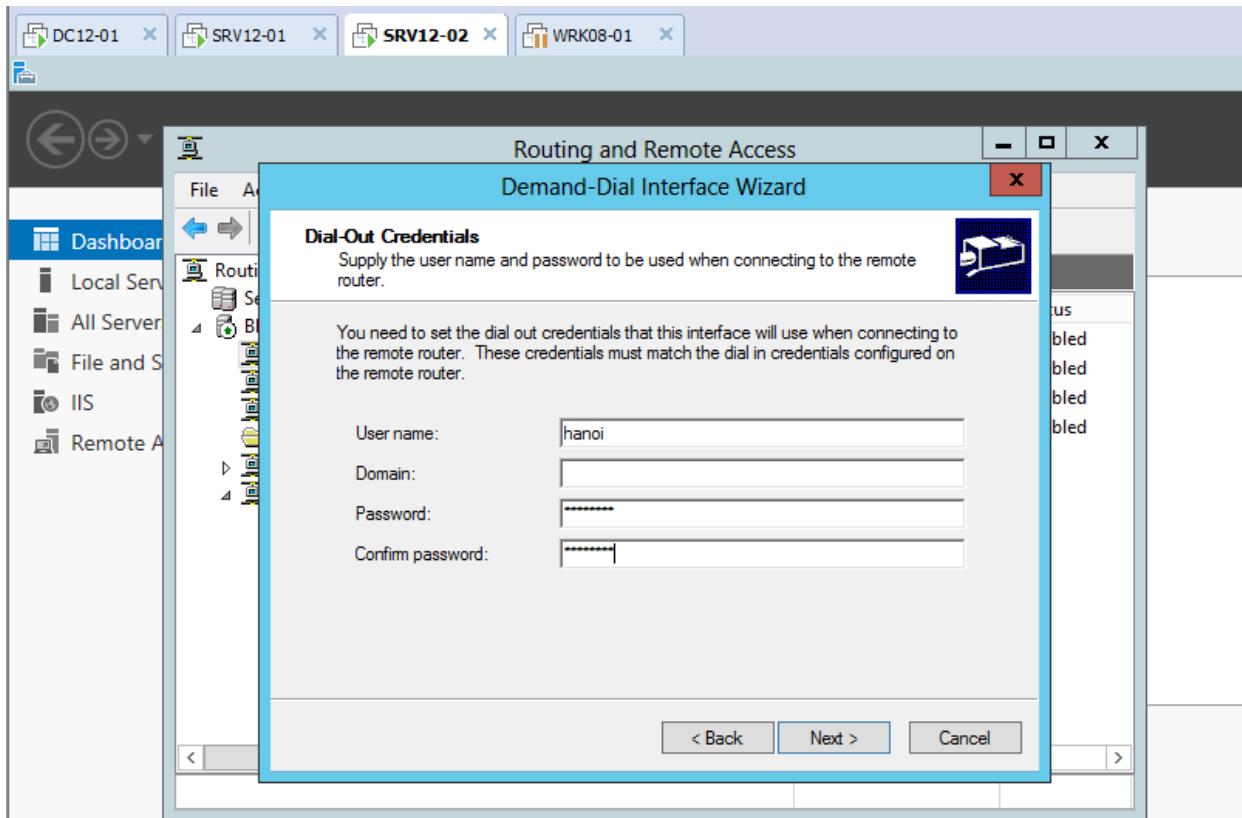
- Tại cửa sổ **Static for Remote Networks**, click vào **Add**, tại cửa sổ **Static Route**, nhập vào các thông số sau:
 - *Destination* : 192.168.1.0
 - *Network Mask* : 255.255.255.0
 - *Metric* : 1



- Tại cửa sổ **Dial-In Credentials**, nhập vào **Password**.

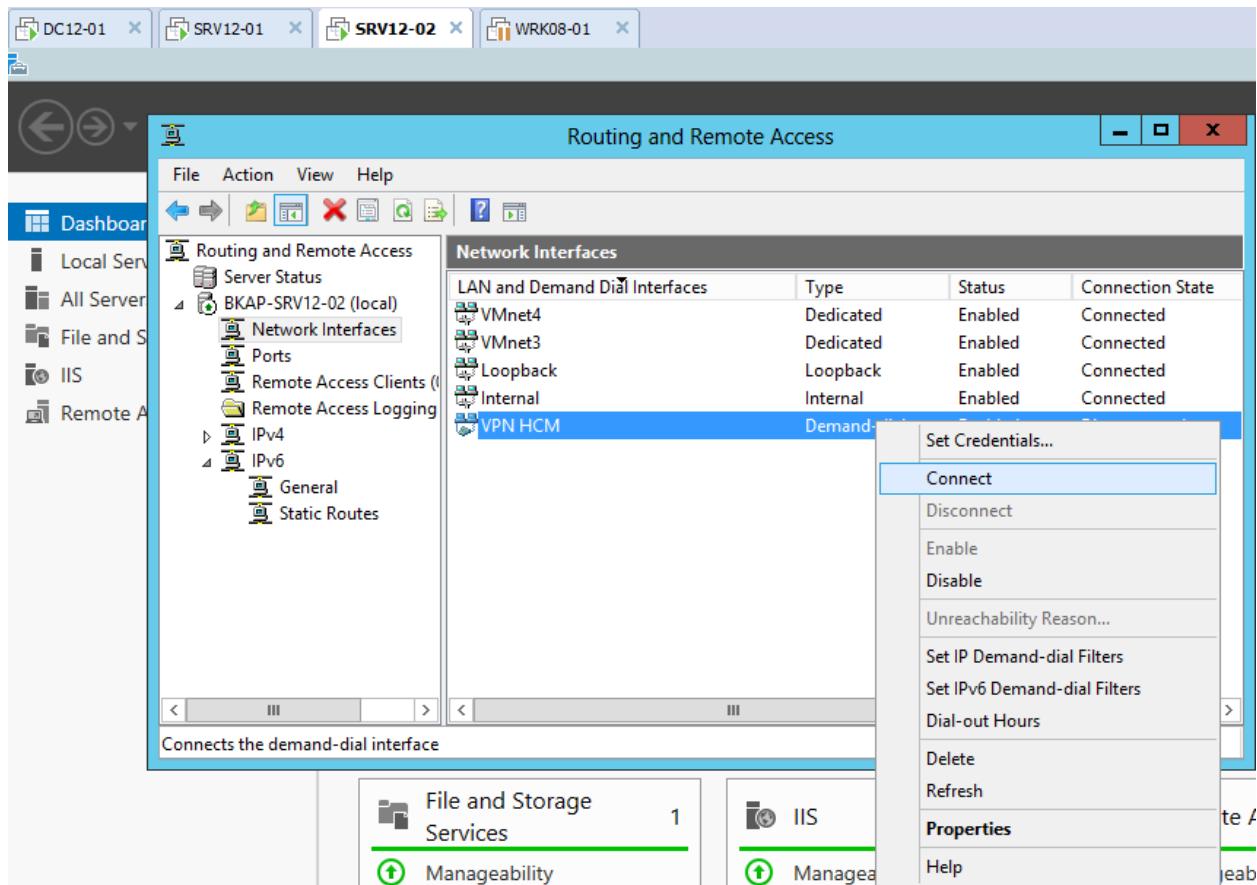


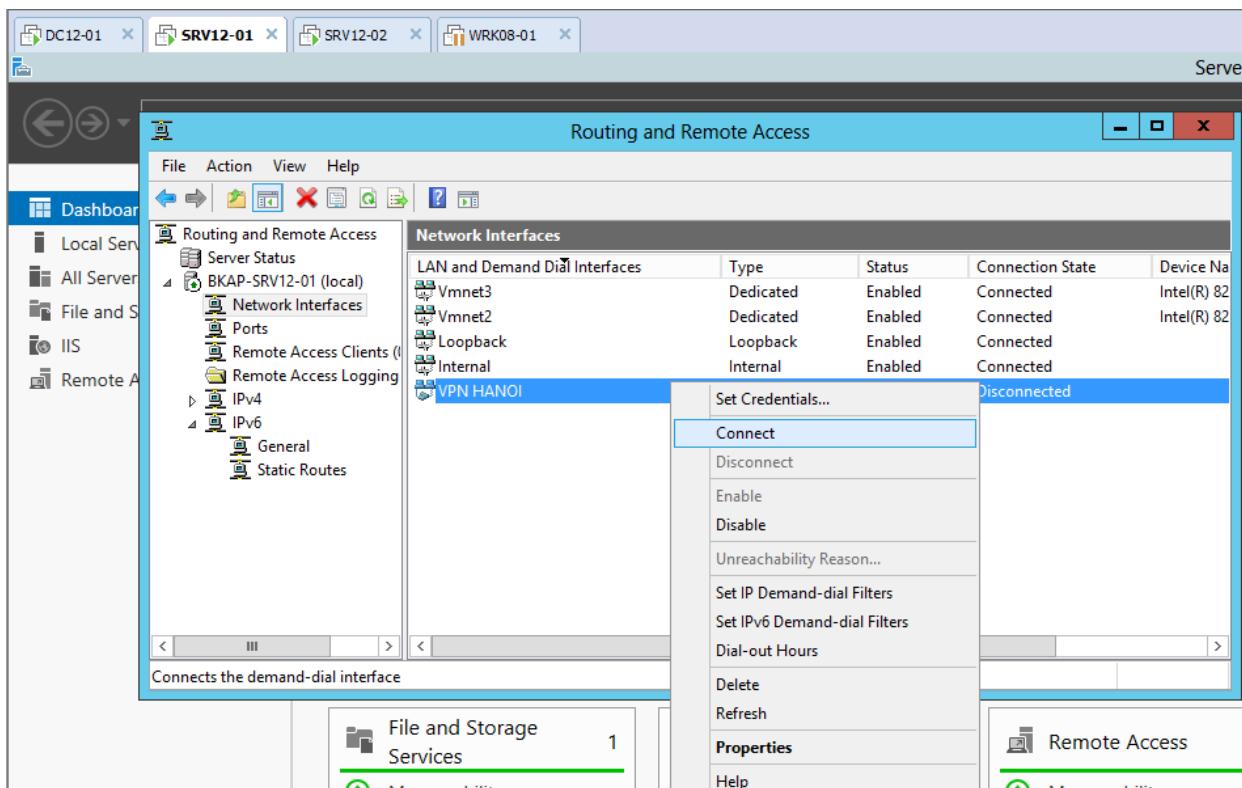
- Tại cửa sổ **Dial-Out Credentials**, nhập vào user **hanoi** bên máy **BKAP-SRV12-01**.



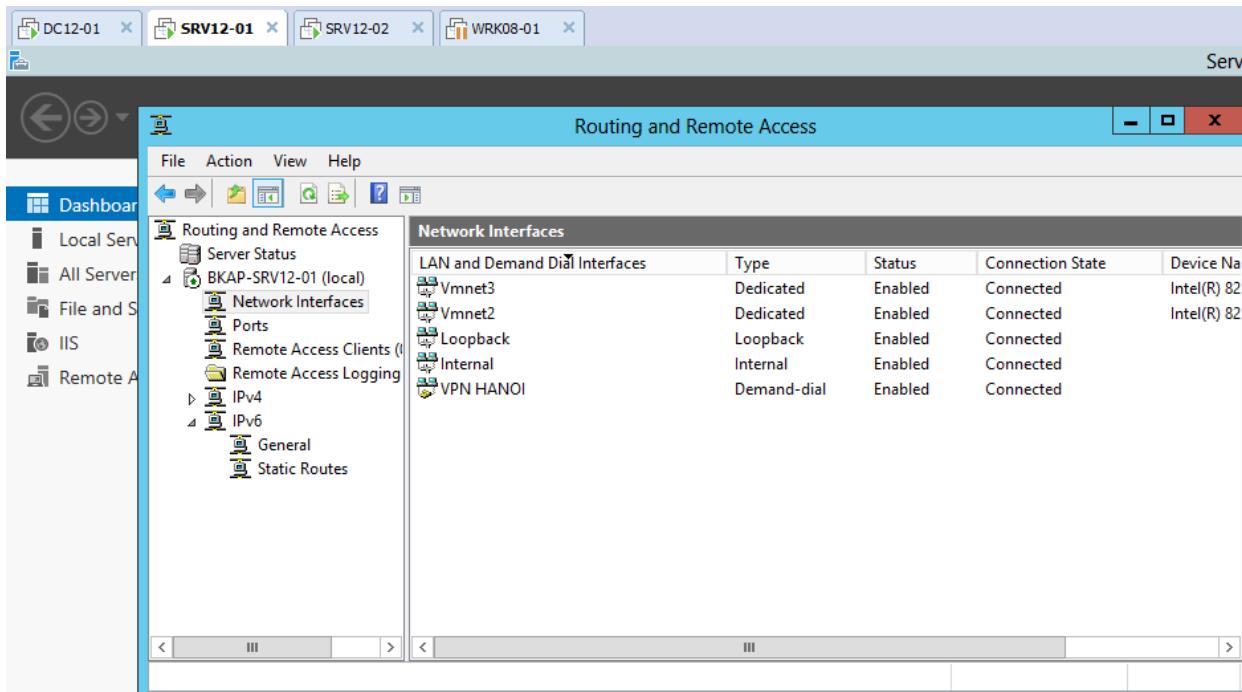
- Click vào **Finish** để kết thúc tiến trình cấu hình.

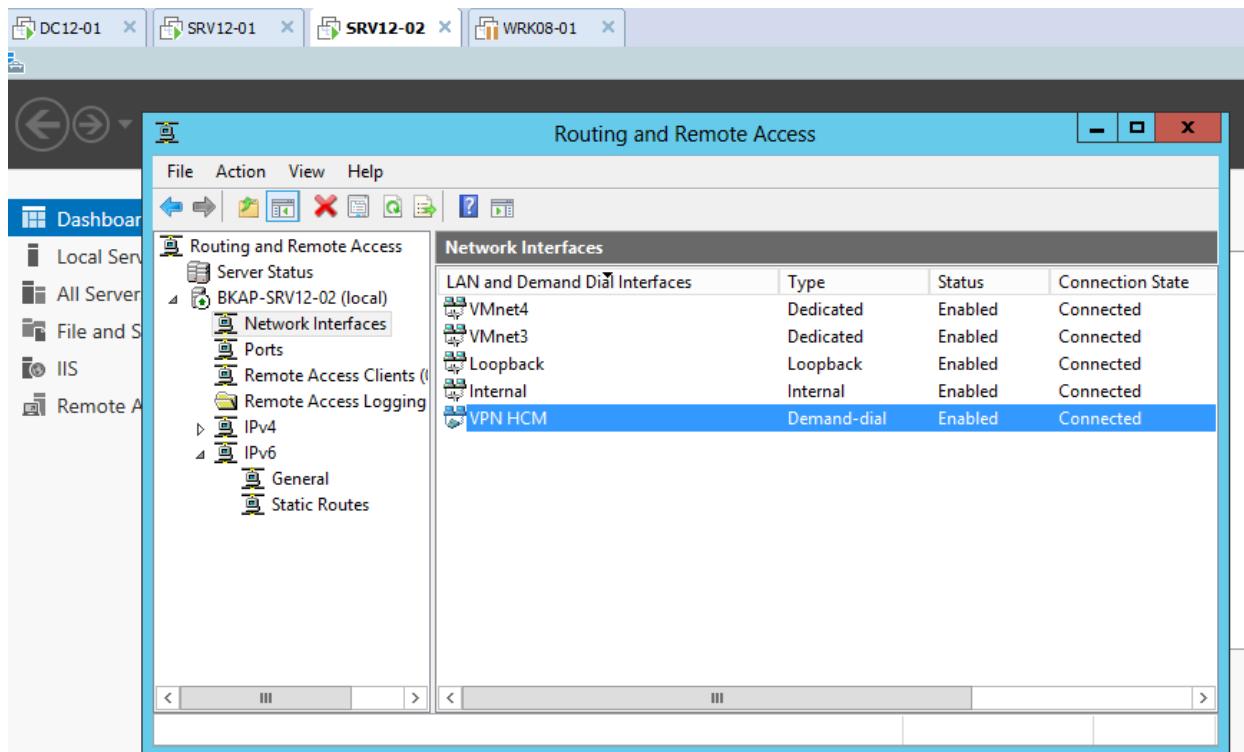
- Click vào **VPN HCM** và **VPN HANOI** vừa tạo, chọn **Connect**.



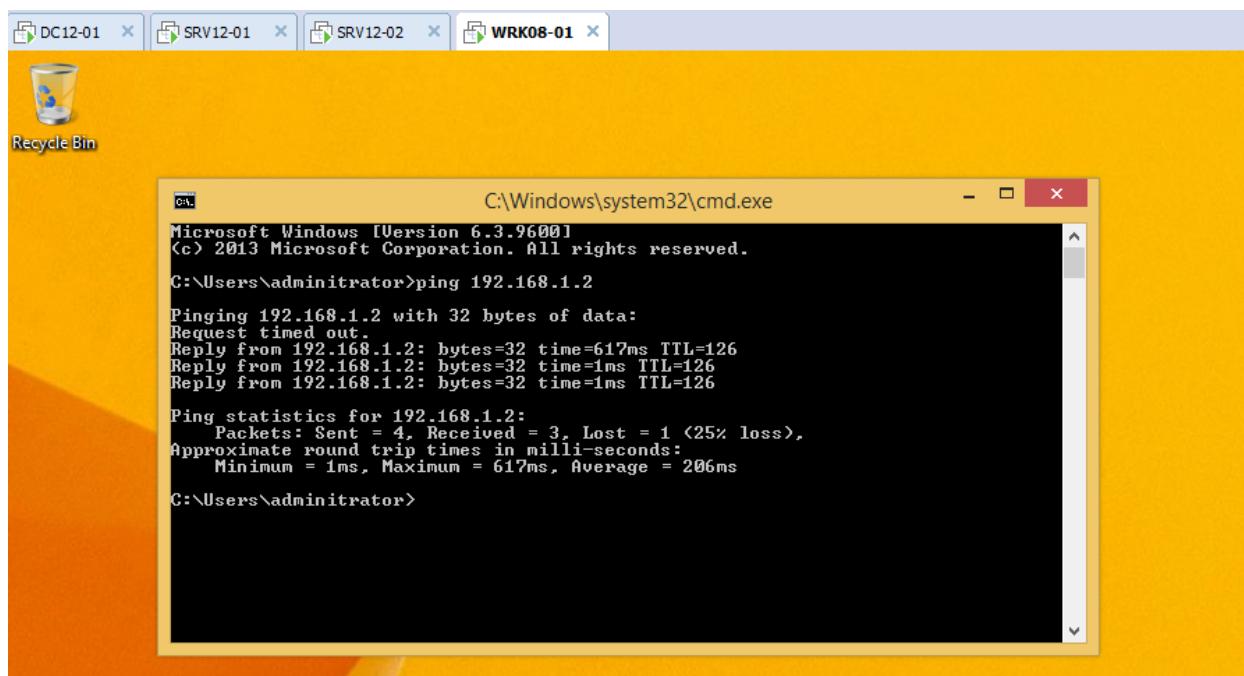


○ Kết nối VPN giữa HANOI và HCM thành công.

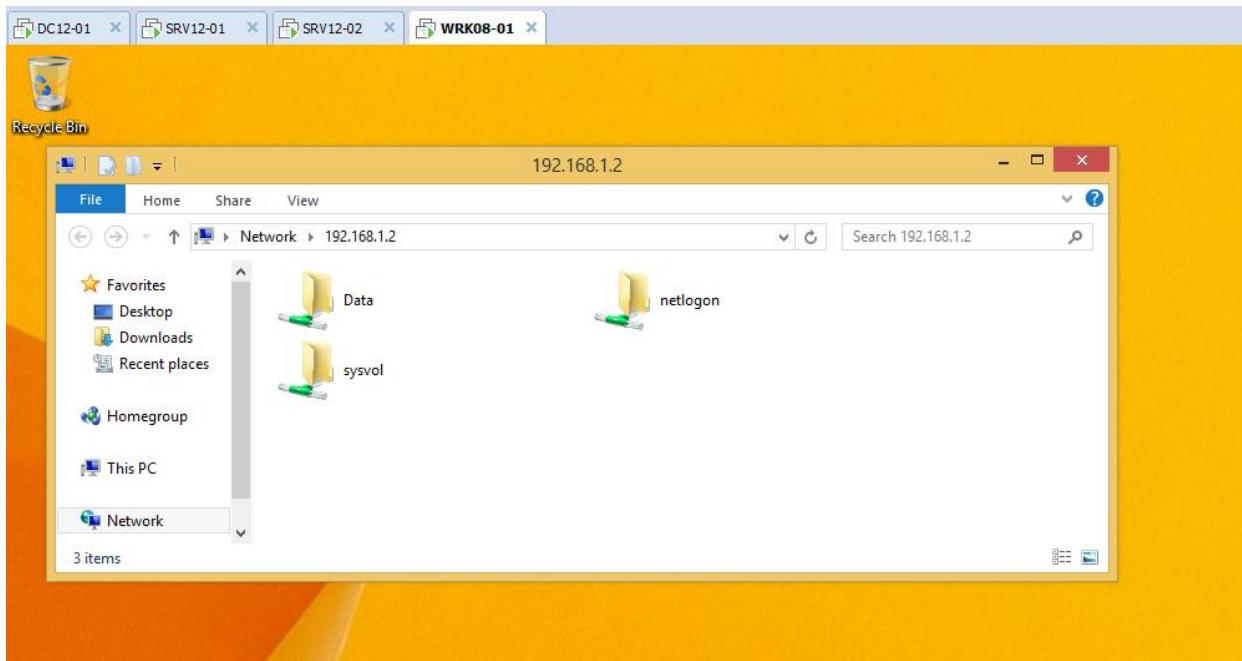




- Chuyển sang máy **Client Win 8**, tạo kết nối **VPN client** (xem lại bài 7.1), ping đến máy **DC12-01** để kiểm tra.



- Kiểm tra truy cập tài nguyên đến máy **DC12-01**.



7.3 Triển khai cài đặt và cấu hình dịch vụ VPN Server (Client to Site) –SSTP

1. Yêu cầu bài Lab:

+ Trên máy BKAP-**DC12-01**, thực hiện các công việc sau:

- Tạo **User** và cho phép truy cập từ xa, tạo thư mục chia sẻ có tên là **Data**.
- Cài đặt *Enterprise CA*.
- Tạo *Certificate Template* và phát hành *Certificate Template*.

+ Trên máy **BKAP-SRV12-01**, thực hiện các công việc sau:

- Xin *SSTP Certificate* cho **VPN Server**.
- Cài đặt **Remote Access**.
- Cấu hình **VPN Client-to-Gateway**.
 - Dải cấp phát VPN: 10.0.0.10 – 10.0.0.50
- Cấu hình **NAT Inbound**.

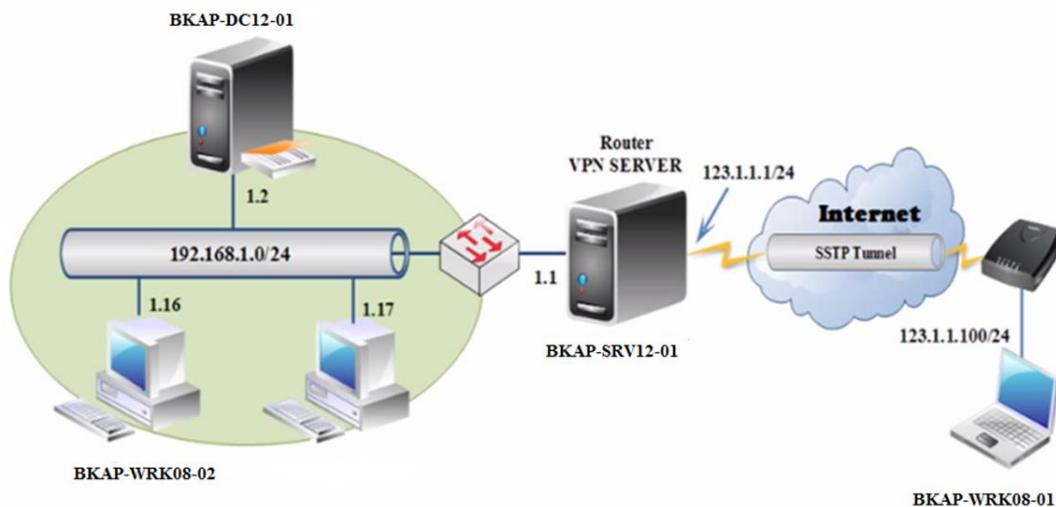
2. Yêu cầu chuẩn bị:

- + Chuẩn bị máy **BKAP-DC12-01** làm **Domain Controller** quản lý miền bkaptech.vn.
- + Chuẩn bị máy **BKAP-SRV12-01** đóng vai trò làm **VPN Server**.
- + Máy Client **BKAP-WRK08-01** làm **VPN Client**.

3. Mô hình lab:

HỆ THỐNG ĐÀO TẠO CNTT QUỐC TẾ BACHKHOA-APTECH

Lab 7.3 Cấu hình dịch vụ VPN Server Client to Site (SSTP)



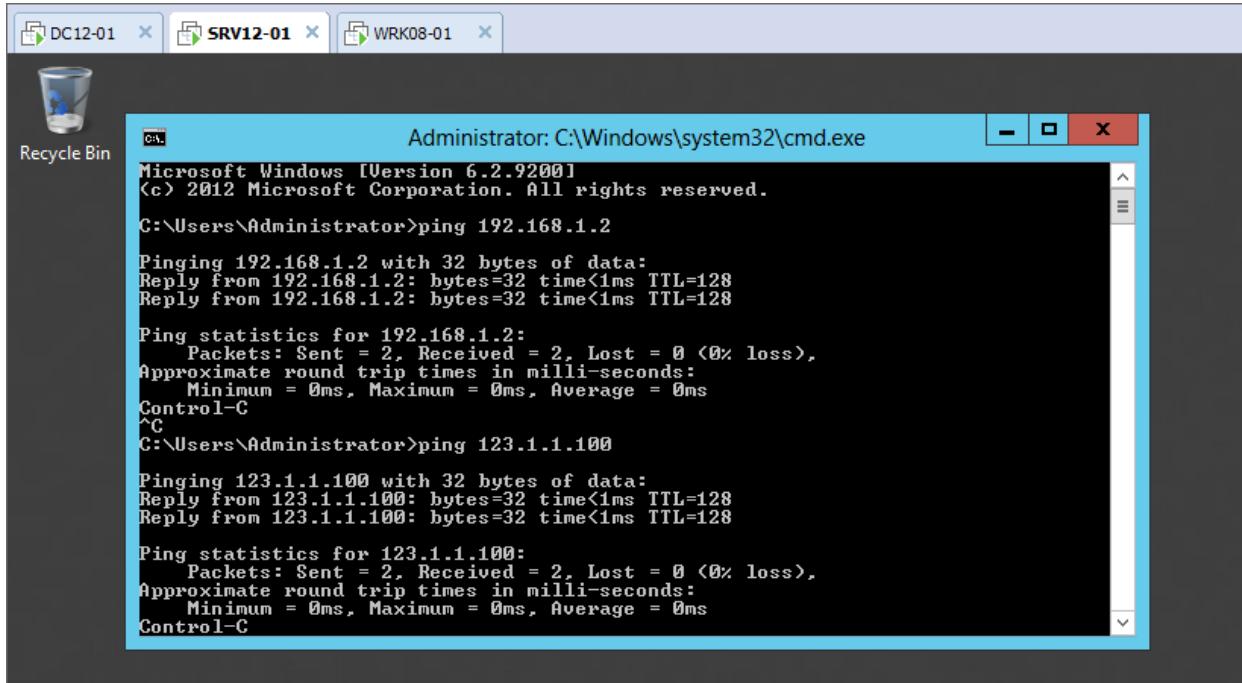
Hình 7.3

Sơ đồ địa chỉ như sau :

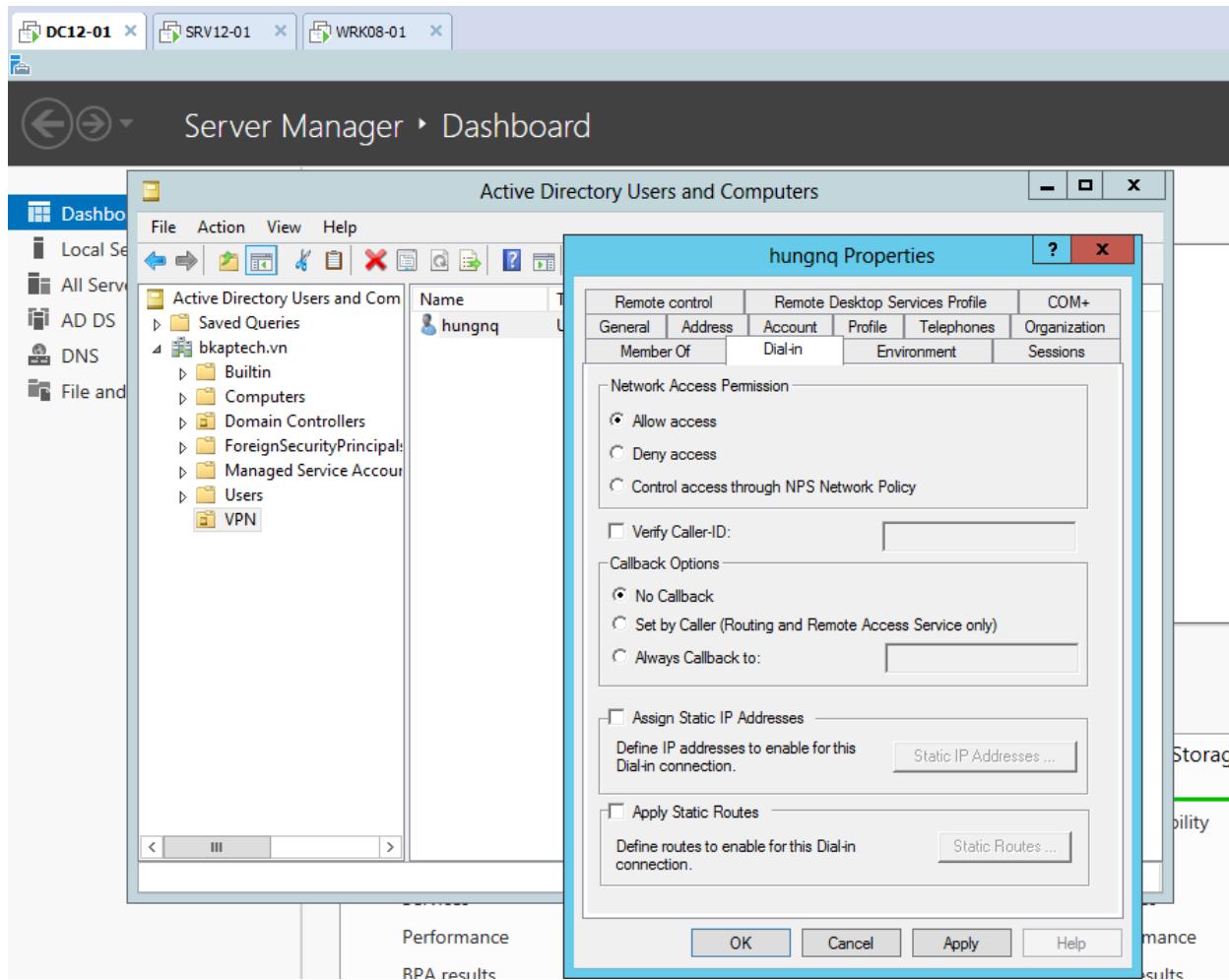
Thông số	BKAP-DC12-01	BKAP-SRV12-01	BKAP-WRK08-01
IP address	192.168.1.2	NIC1: 192.168.1.1 NIC2: 123.1.1.1	123.1.1.100
Subnet Mask	255.255.255.0	255.255.255.0	255.255.255.0
Gateway	192.168.1.1	--	192.168.1.1
DNS Server	192.168.1.2	--	--

Hướng dẫn chi tiết :

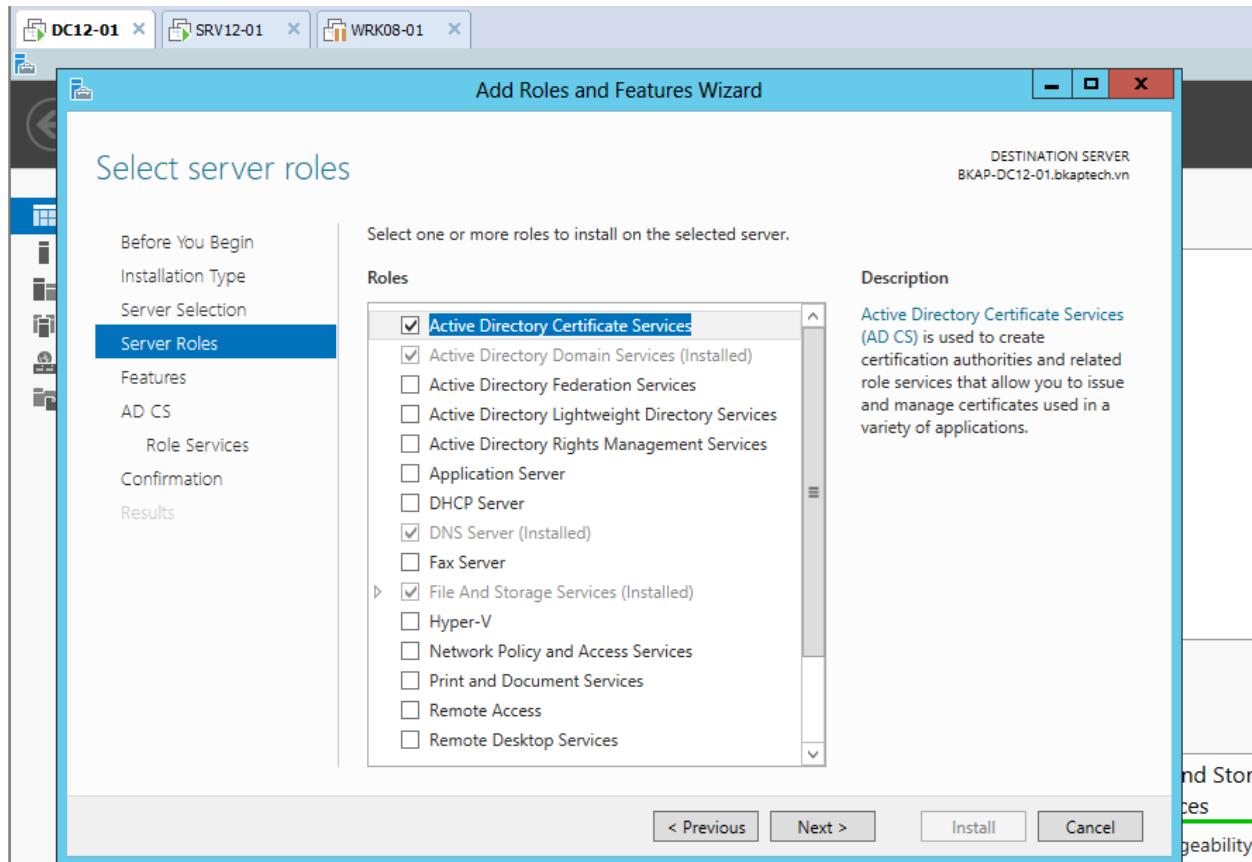
- Mở các máy ảo, kết nối theo mô hình, ping thông giữa các máy kết nối trực tiếp .



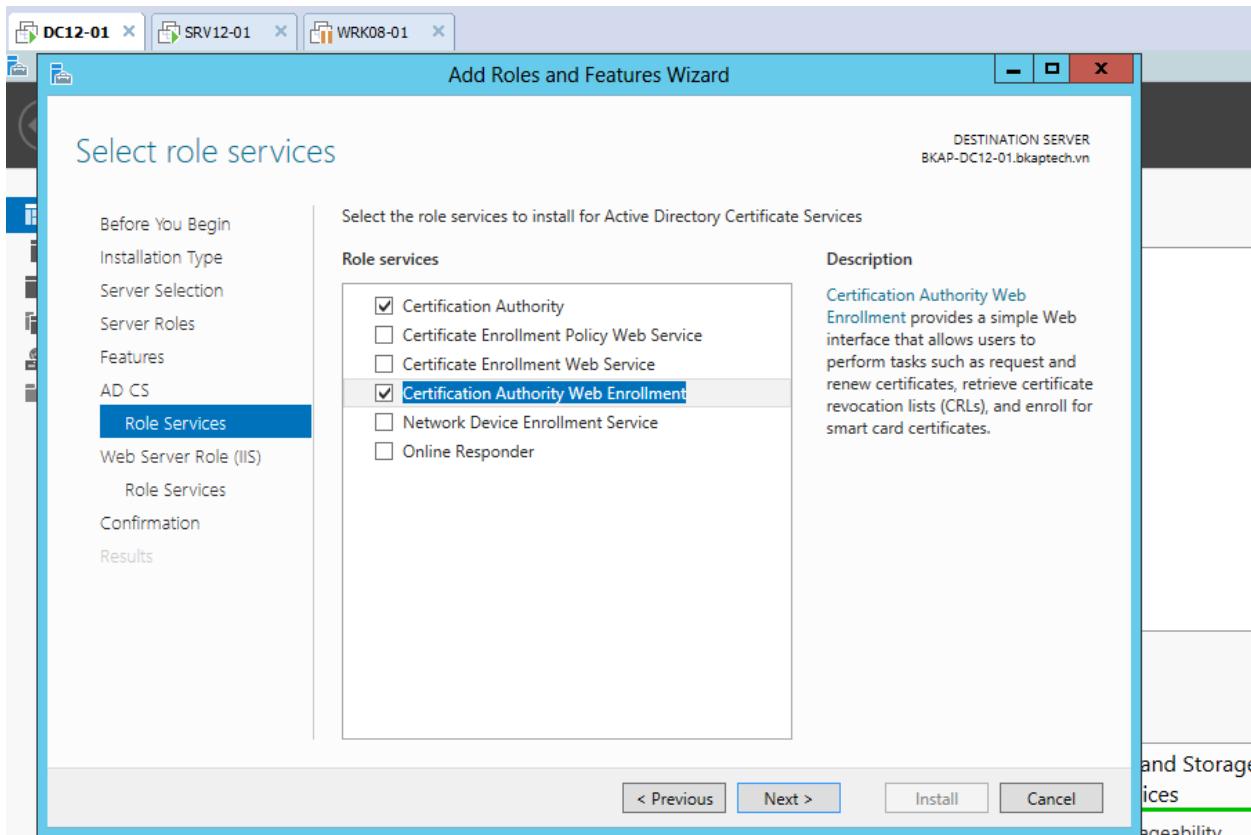
- Trên máy **BKAP-DC12-01**, thực hiện :
 - Tạo 1 OU tên **VPN**, trong ou **VPN**, tạo user **hungnq** và cấp quyền truy cập **VPN**.



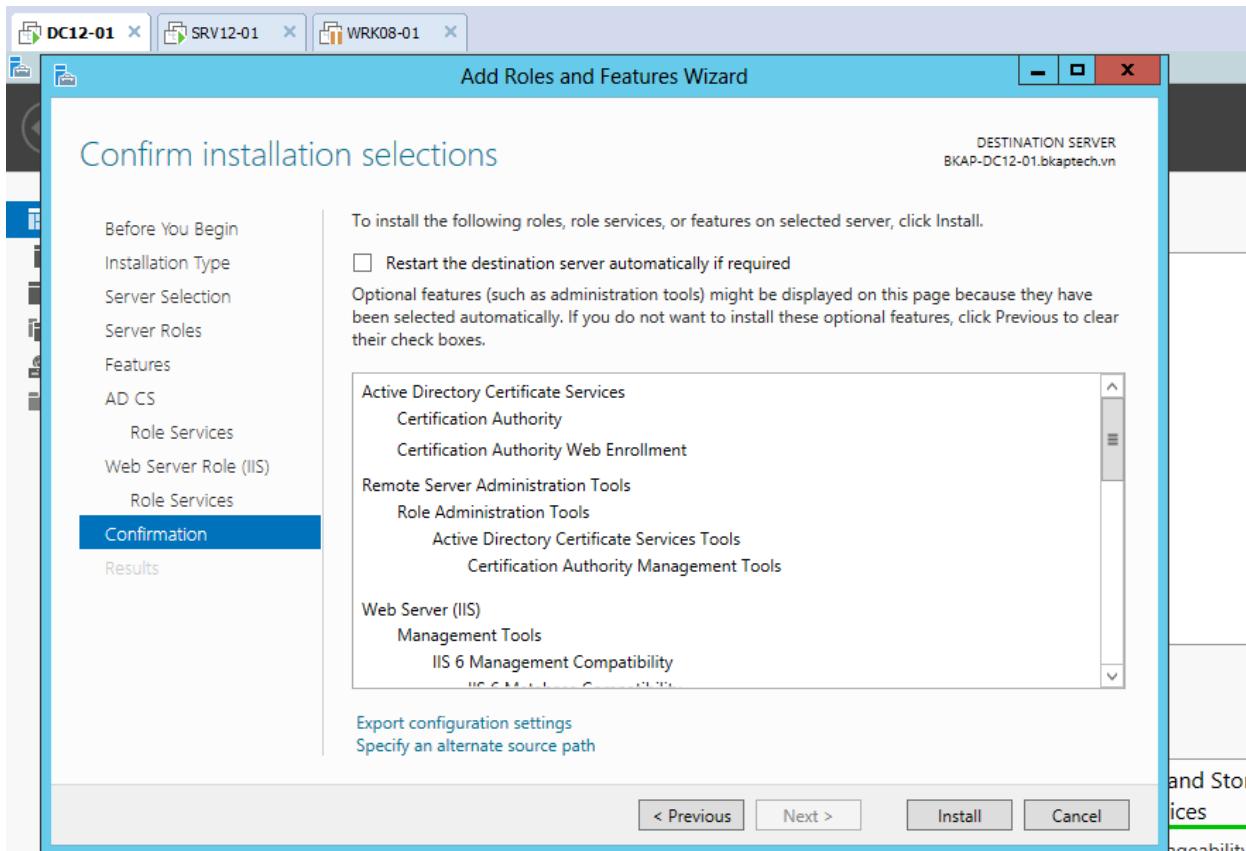
- Thực hiện cài đặt dịch vụ **Enterprise CA**.
 - **Server Manager / Add Roles and Features / chọn vào dịch vụ Active Directory Certificate Services**



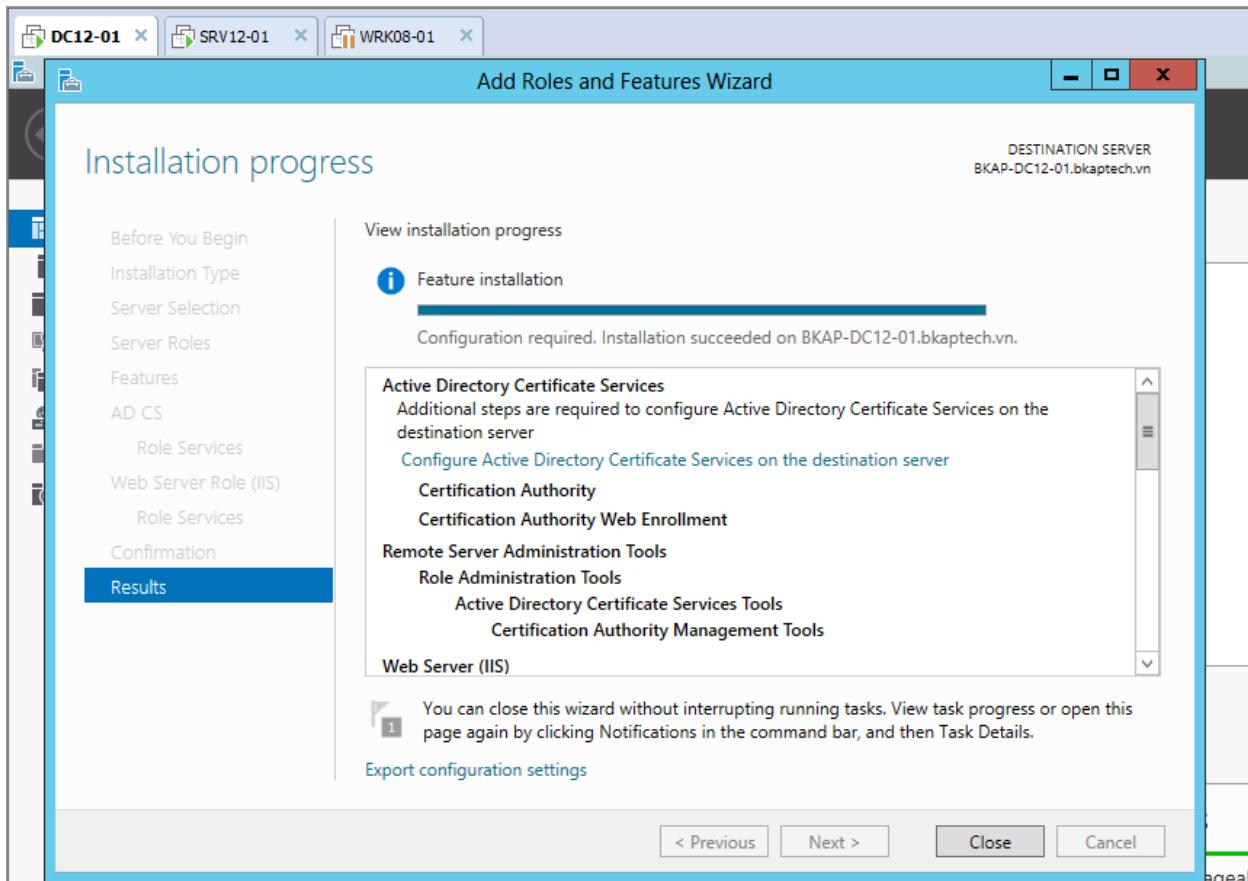
- Tại **Select role services** , chọn vào **Certification Authority** và **Certification Authority Web Enrollment**.



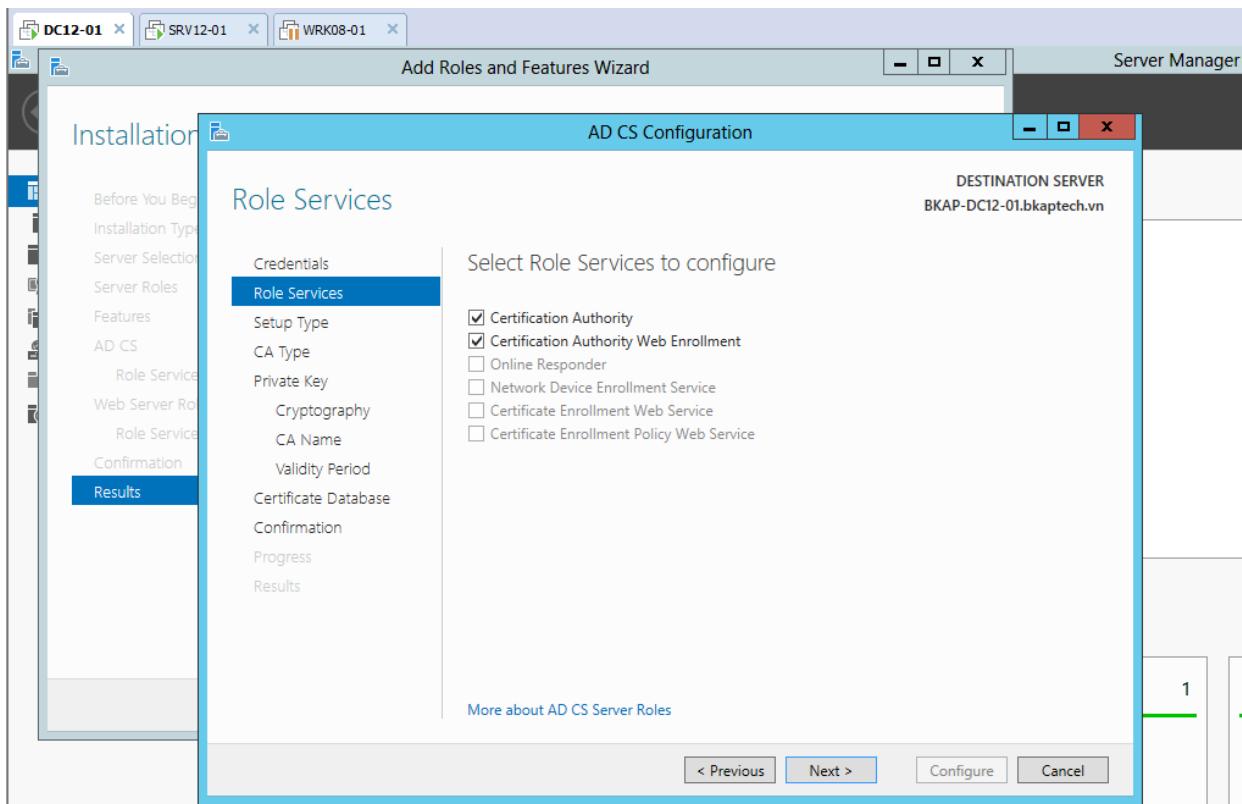
- Click **Install** để máy chủ tiến hành cài đặt dịch vụ **CA**.



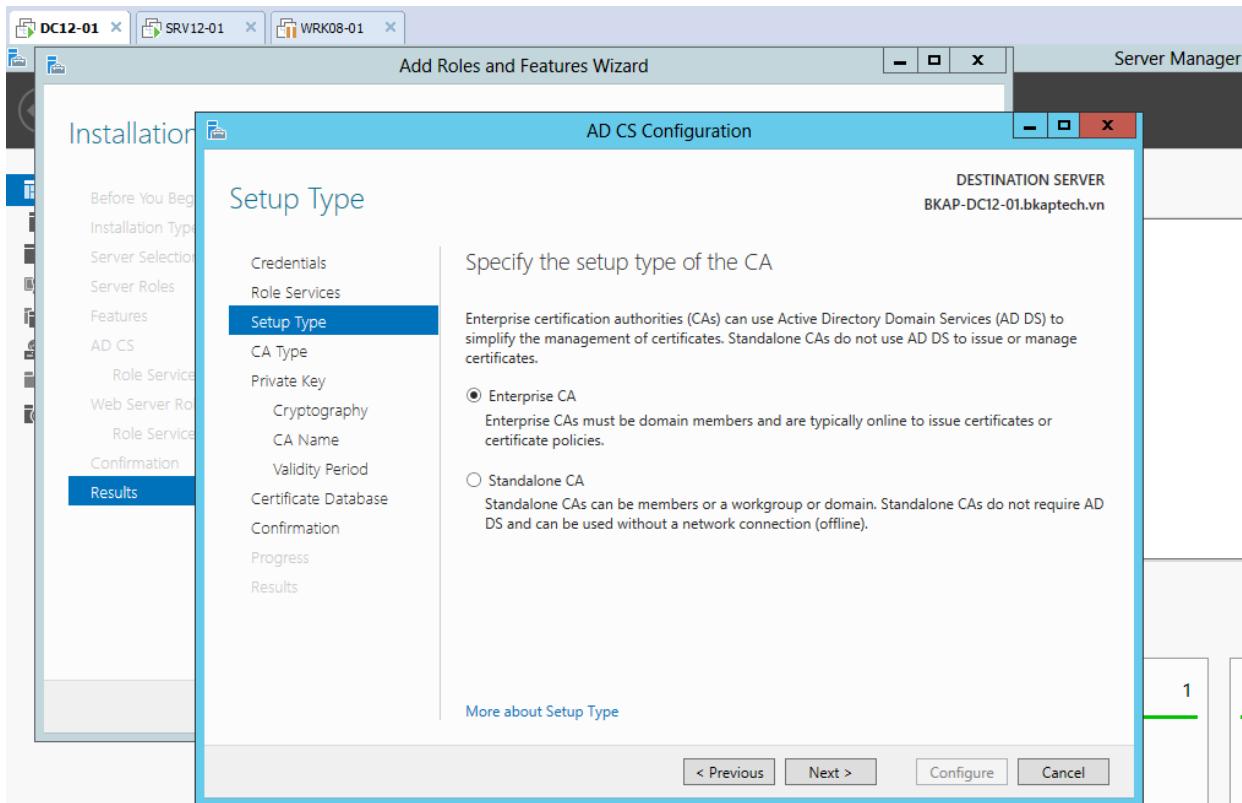
- Tại **Installation Process**, click vào **Configure Active Directory Services** on the destination server.



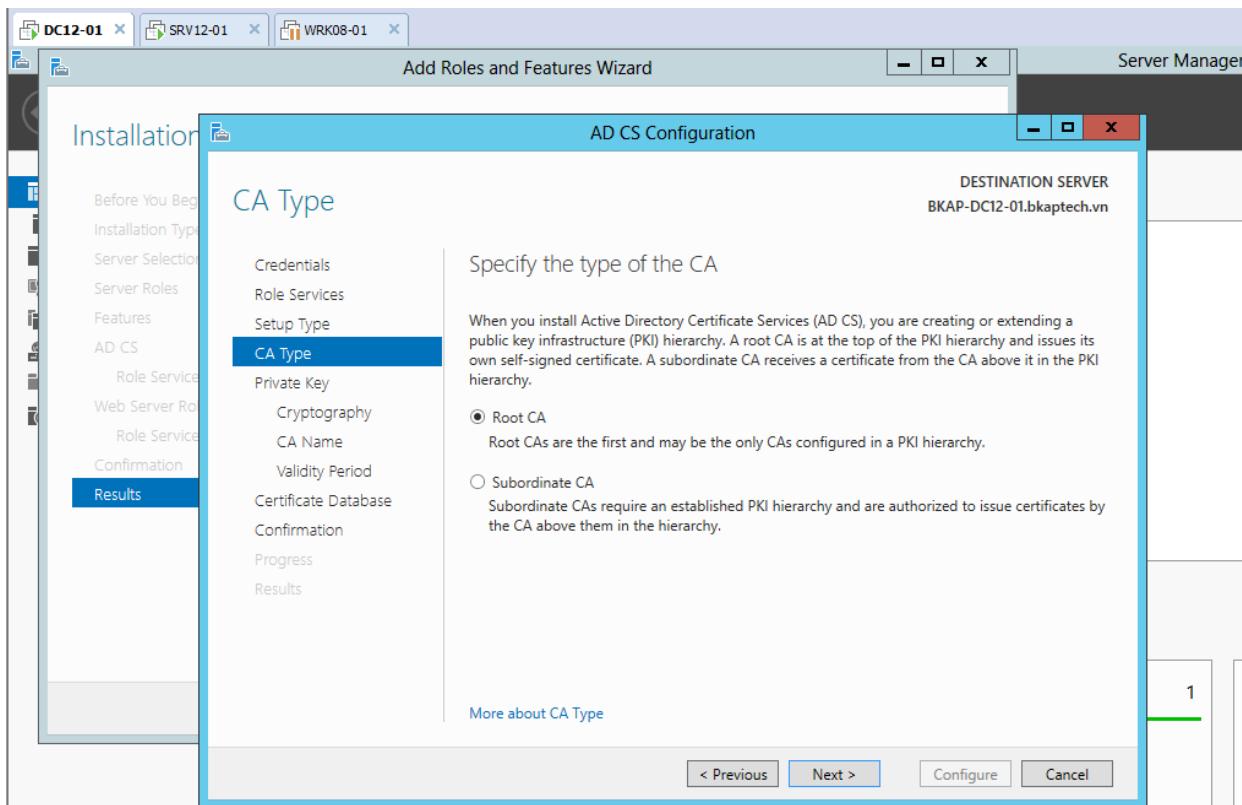
- Click vào **Next** tại cửa sổ tiếp theo, tại cửa sổ **Role Services**, chọn vào **Certification Authority** và **Certification Authority Web Enrollment**.



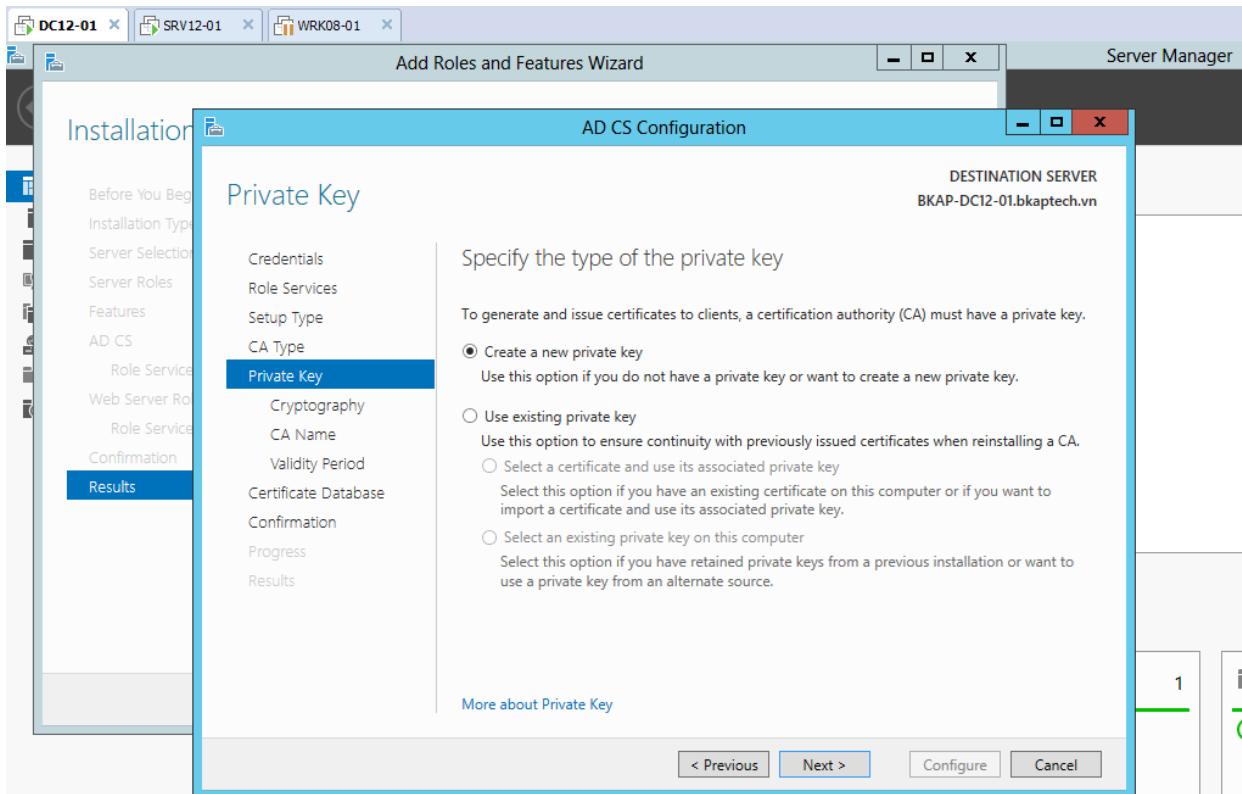
- Tại Setup Type, chọn Enterprise CA.



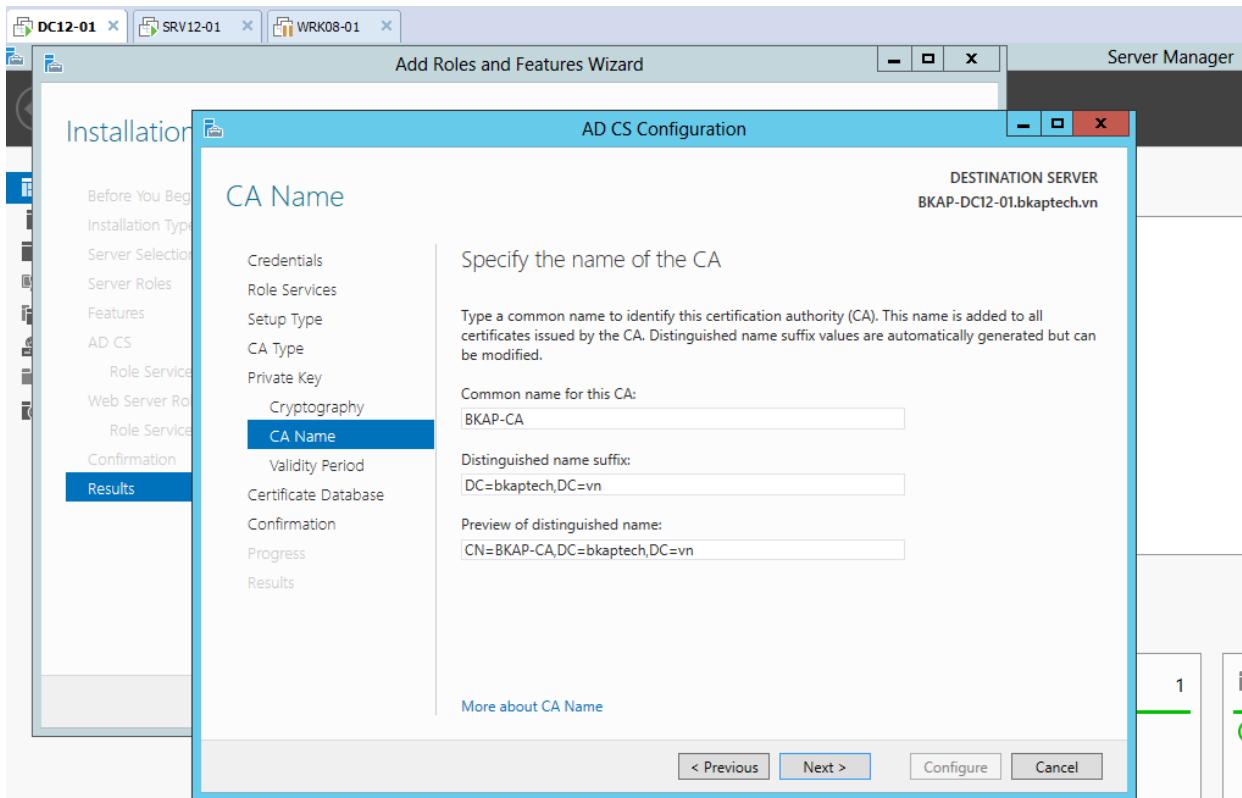
▪ Tại CA type, chọn Root CA.



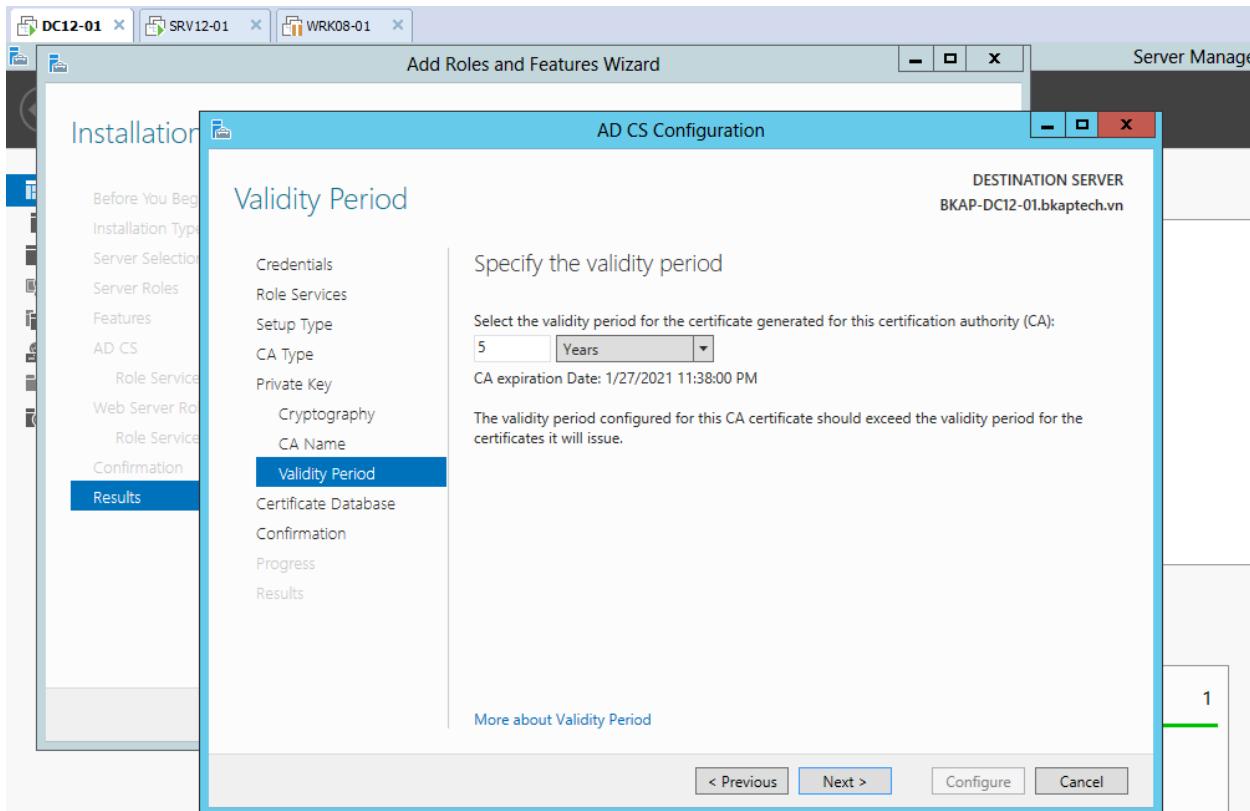
- Tại cửa sổ **Private Key**, chọn vào **Create a new private key**.

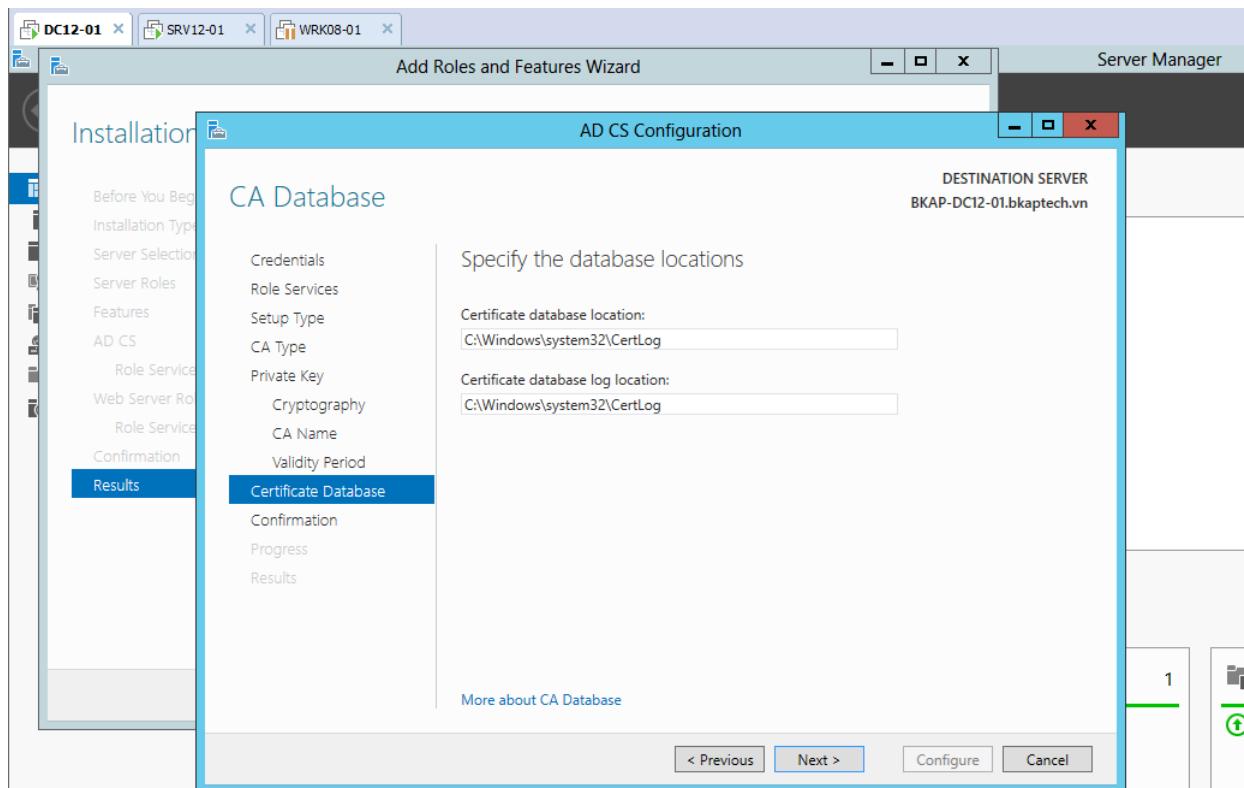


- Click vào **Next** tại cửa sổ **Cryptography for CA** , tại cửa sổ **CA Name** , nhập vào tên **CA** tại mục **Common name for this CA : BKAP-CA.**

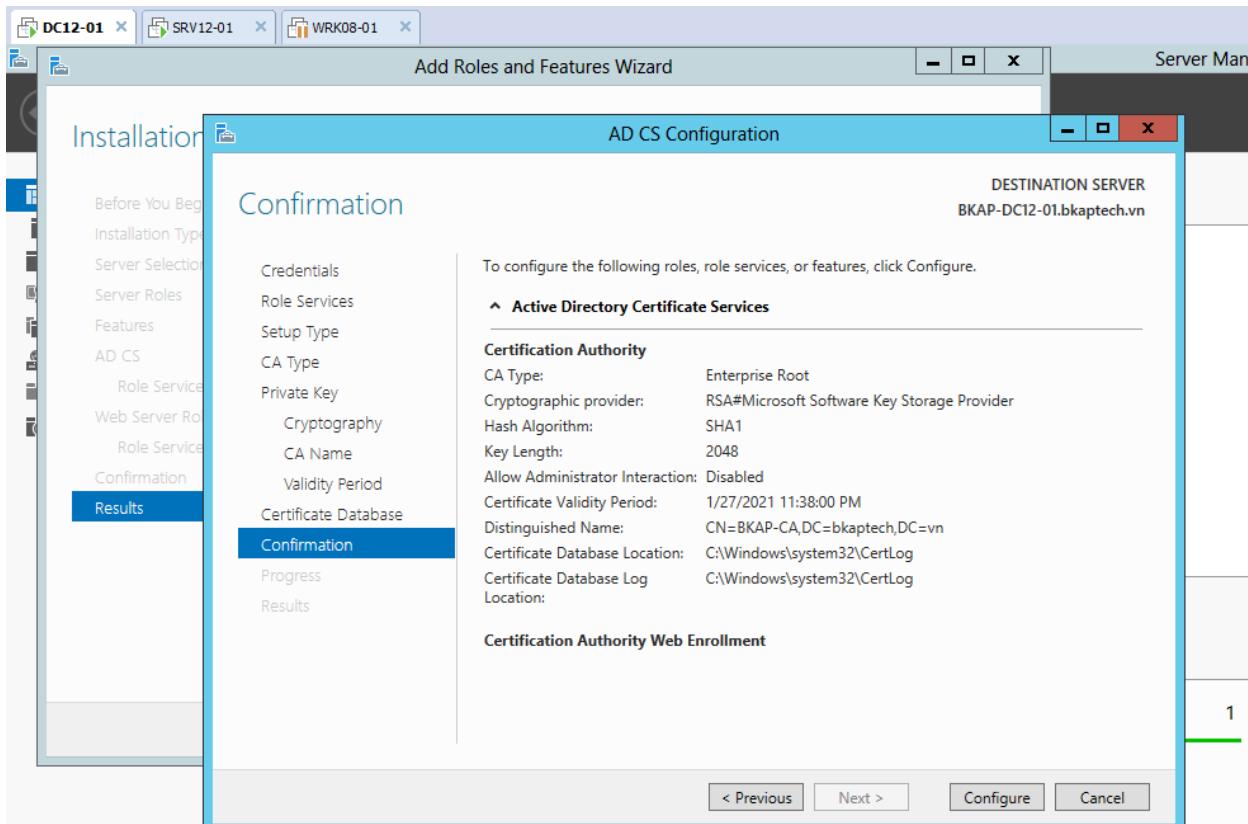


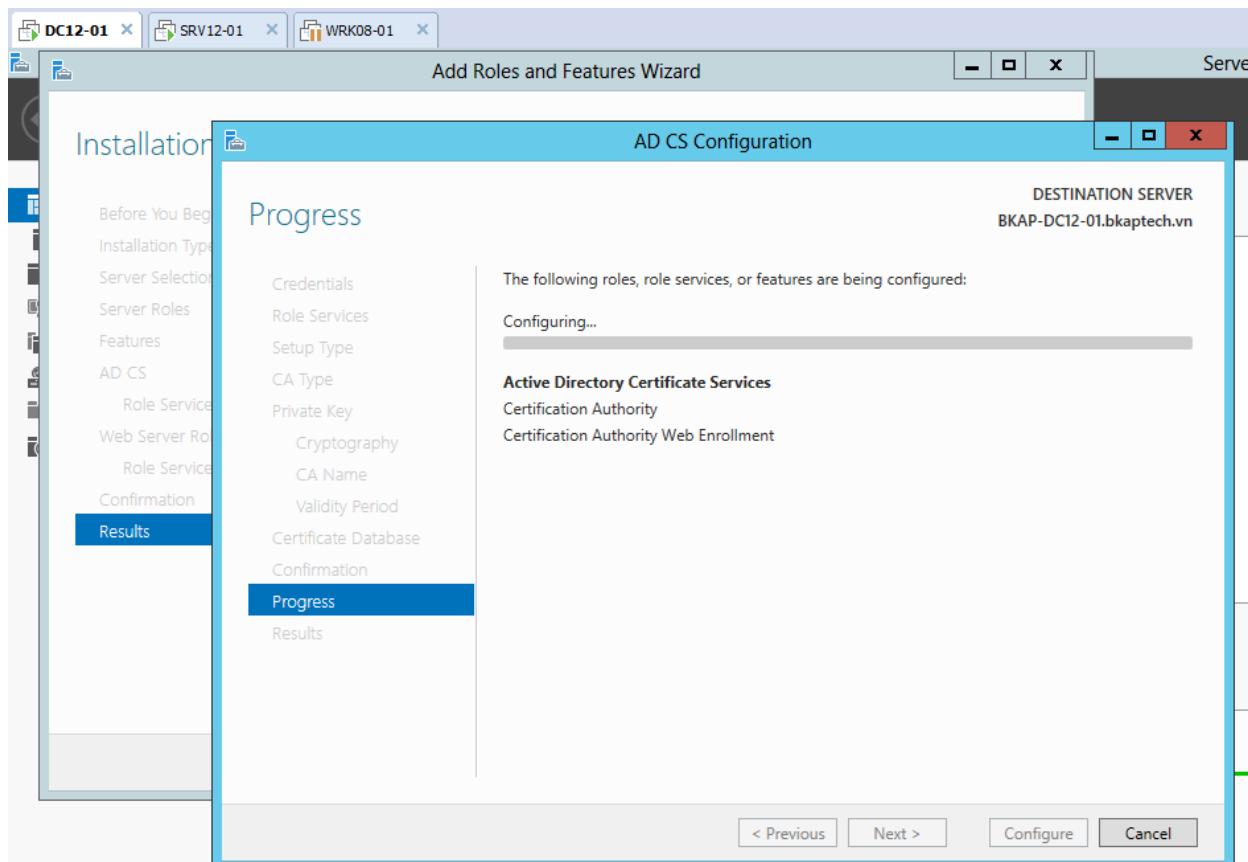
- Click vào **Next** tại cửa sổ **Validity Period**, cửa sổ **CA Database**.



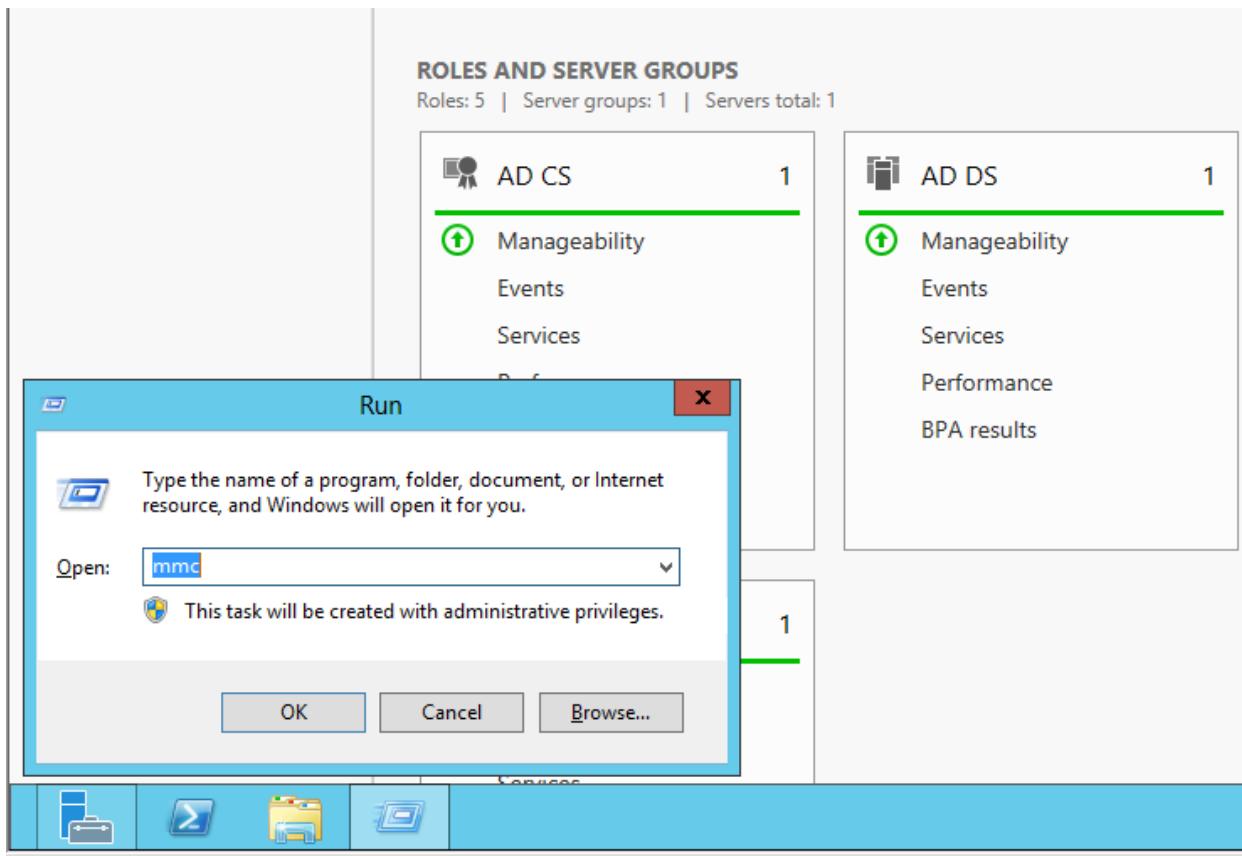


- Tại cửa sổ **Confirmation**, click vào **Configure** để máy chủ cấu hình CA.

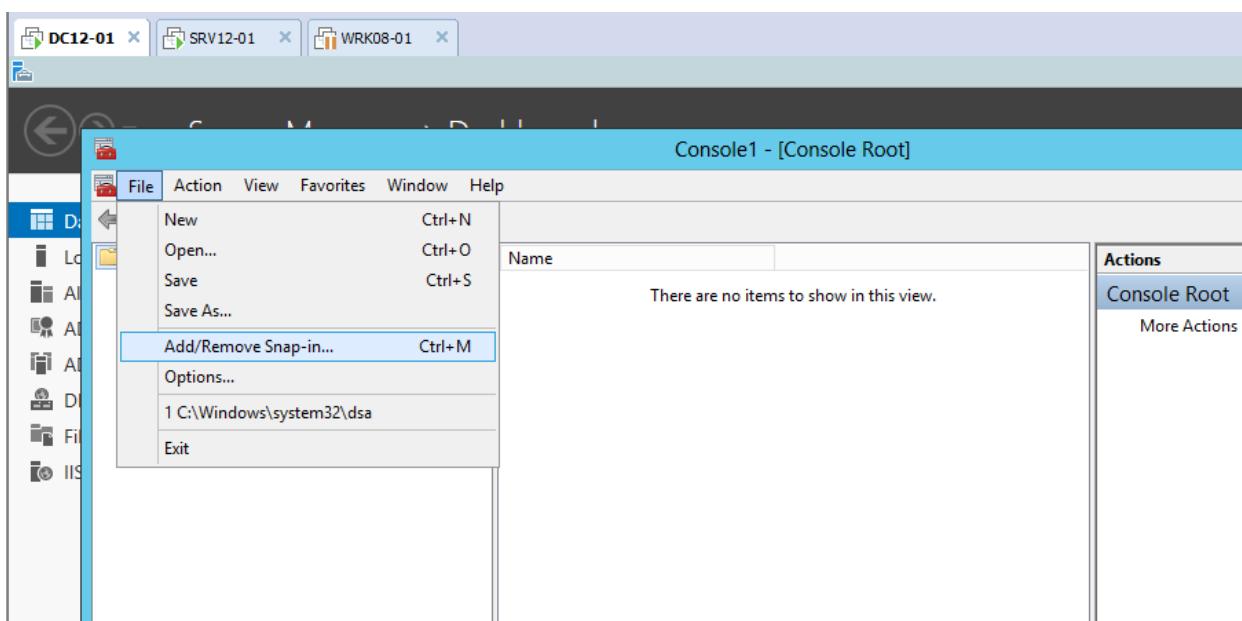




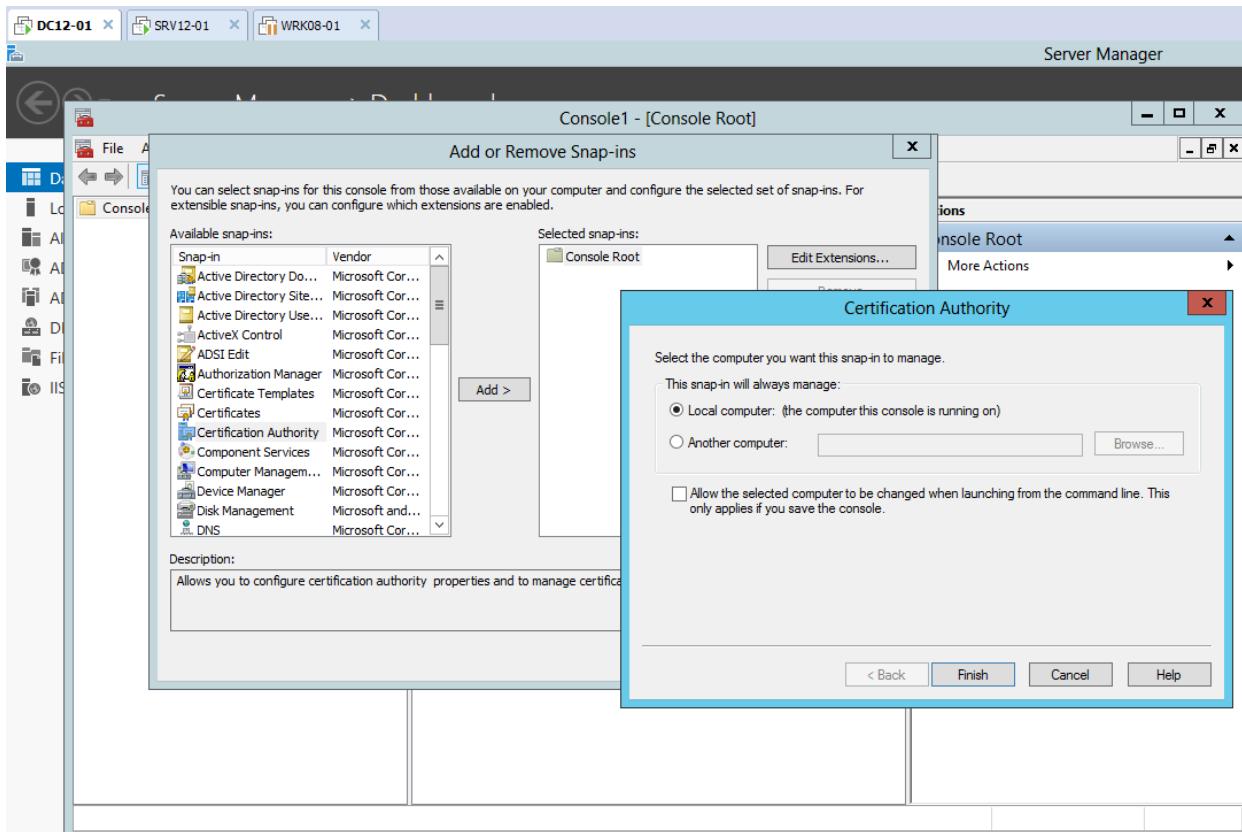
- Tạo Certificate Template và phát hành nó :
 - Run / mmc .



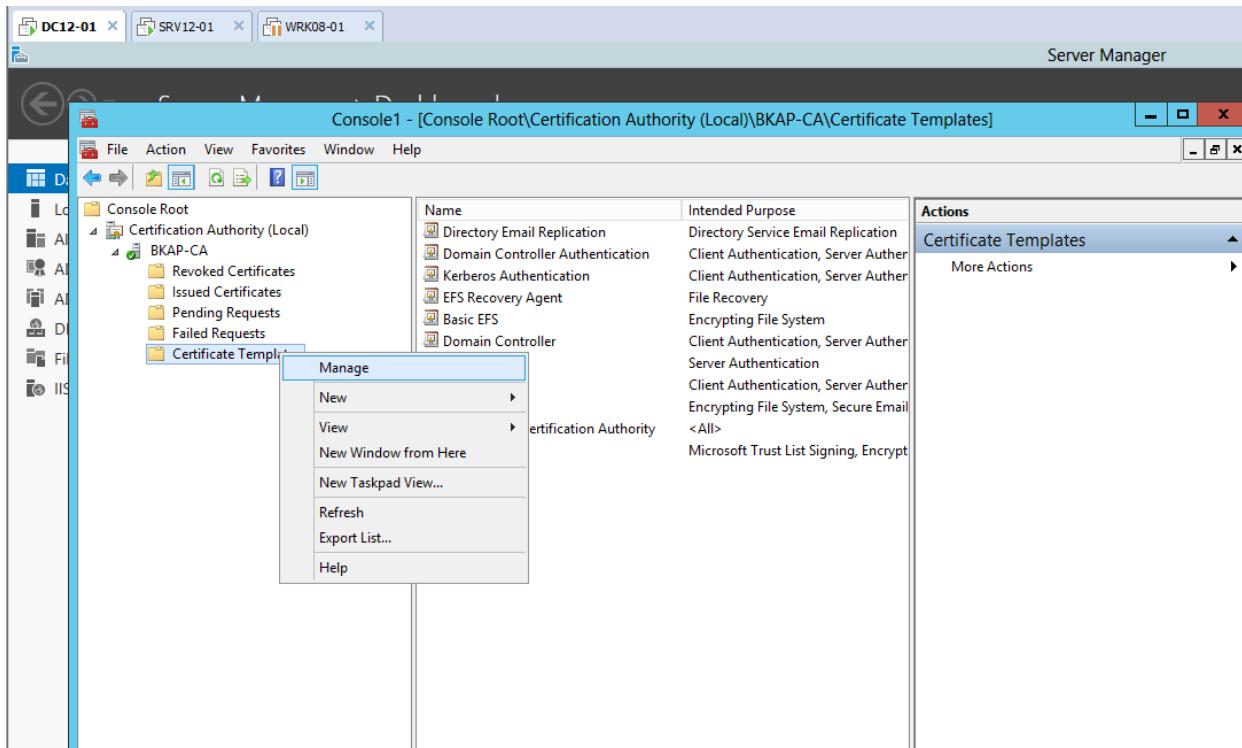
- Tại cửa sổ Console1 – [Console Root] , click vào File => Add/Remote Snap-in.



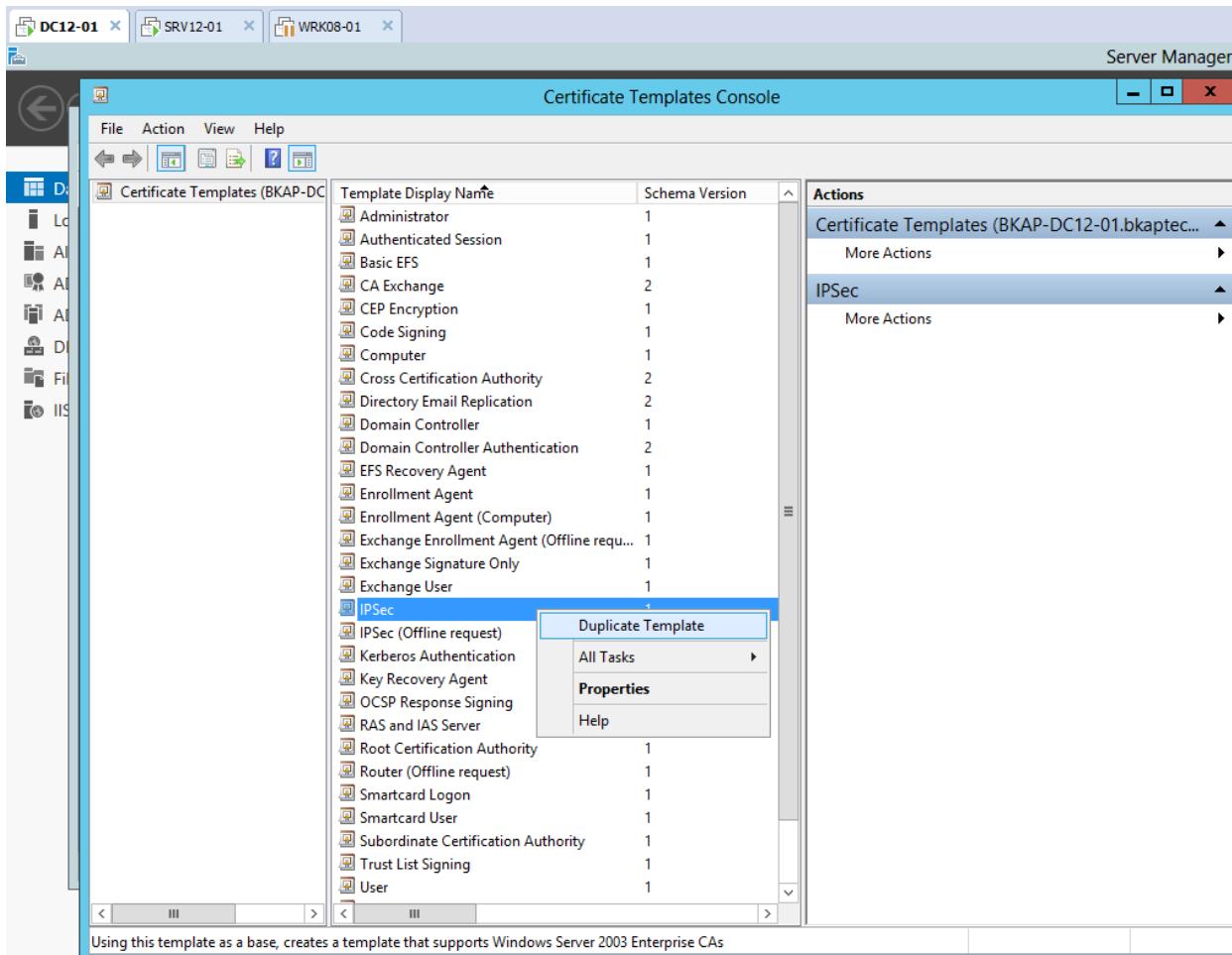
- Tại cửa sổ **Add or Remove Snap-in**, chọn vào **Certificate Authority**, click vào **Add**, chọn vào **Finish** tại cửa sổ **Certification Authority.** / **OK.**



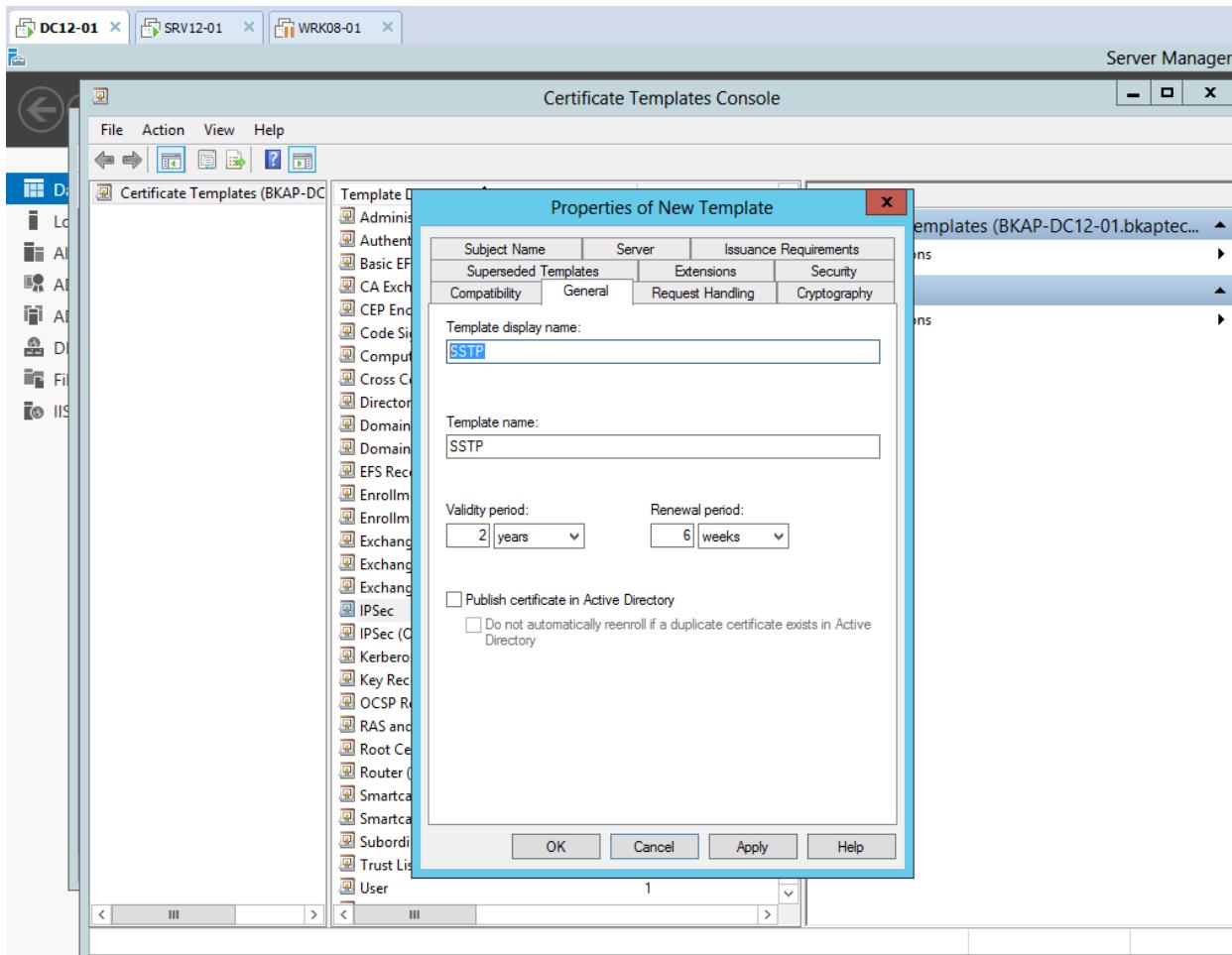
- Tại BKAP-CA , chọn vào Certificate Templates / click chuột phải tại đây chọn Manager.



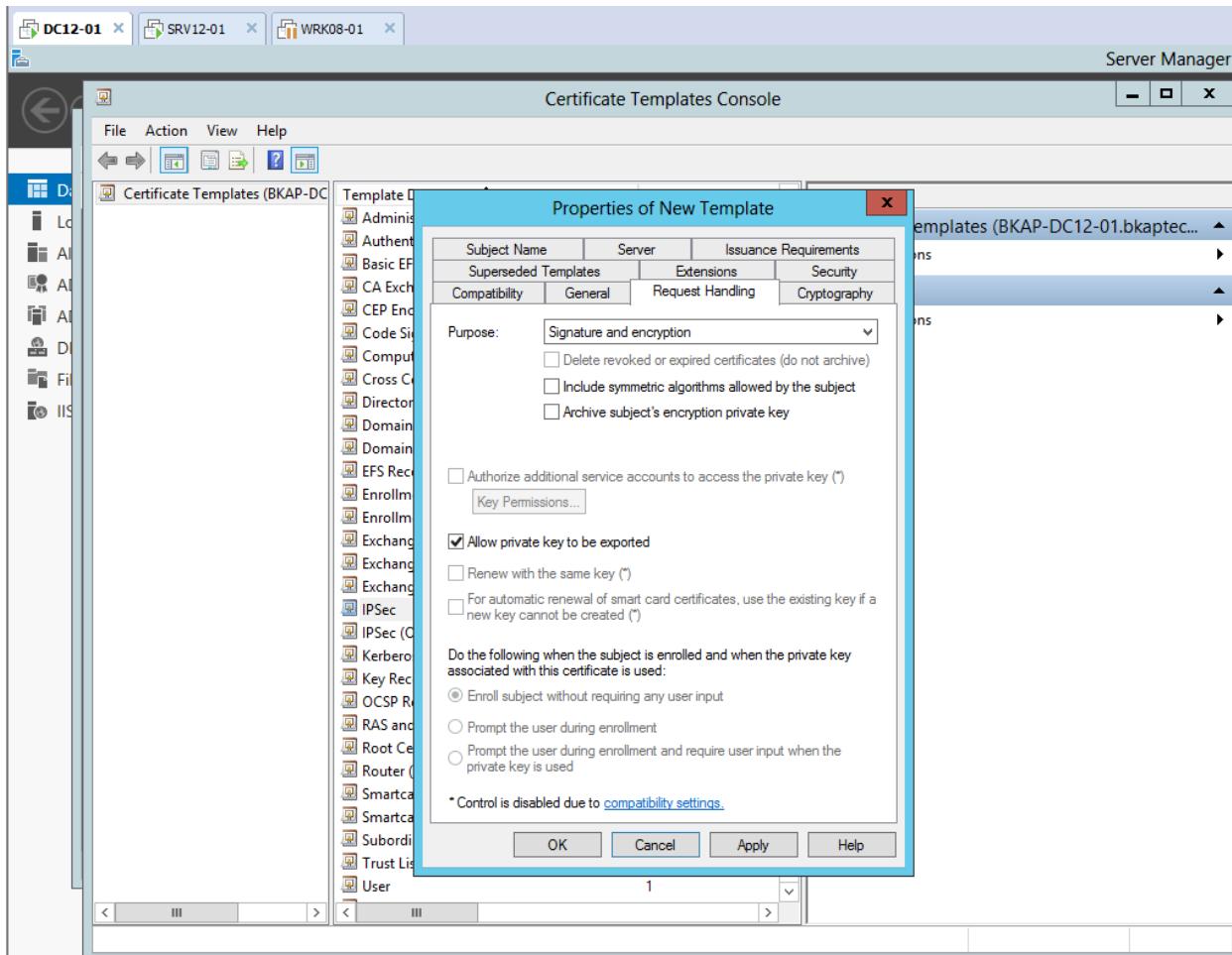
- Tại cửa sổ **Certificate Templates Console**, chọn **IPSec**, click chuột phải tại **IPSec** chọn vào **Duplicate Template**.



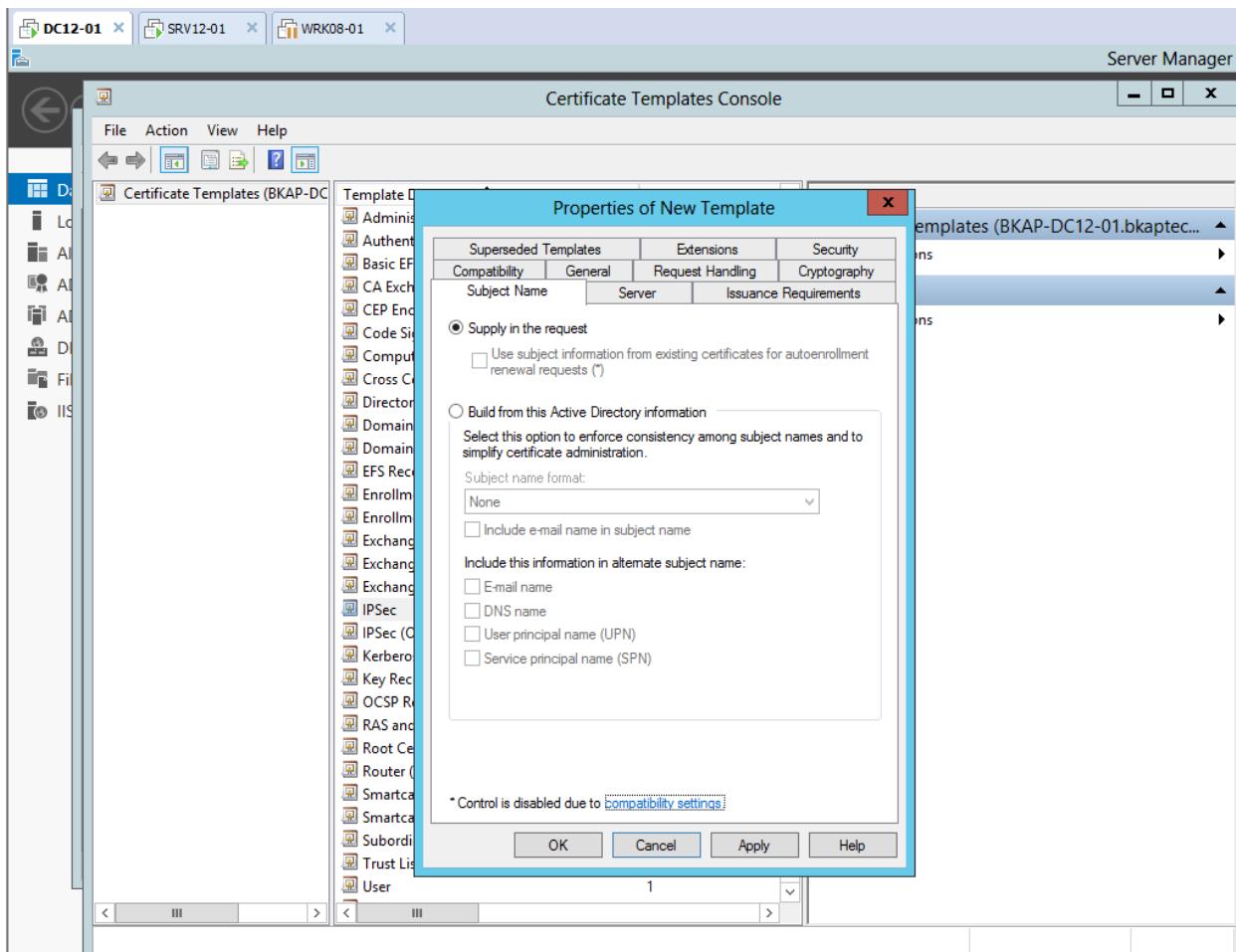
- Tại cửa sổ **Properties of New Template**, chuyển sang tab **General**, nhập vào tại mục **Template display name** : SSTP



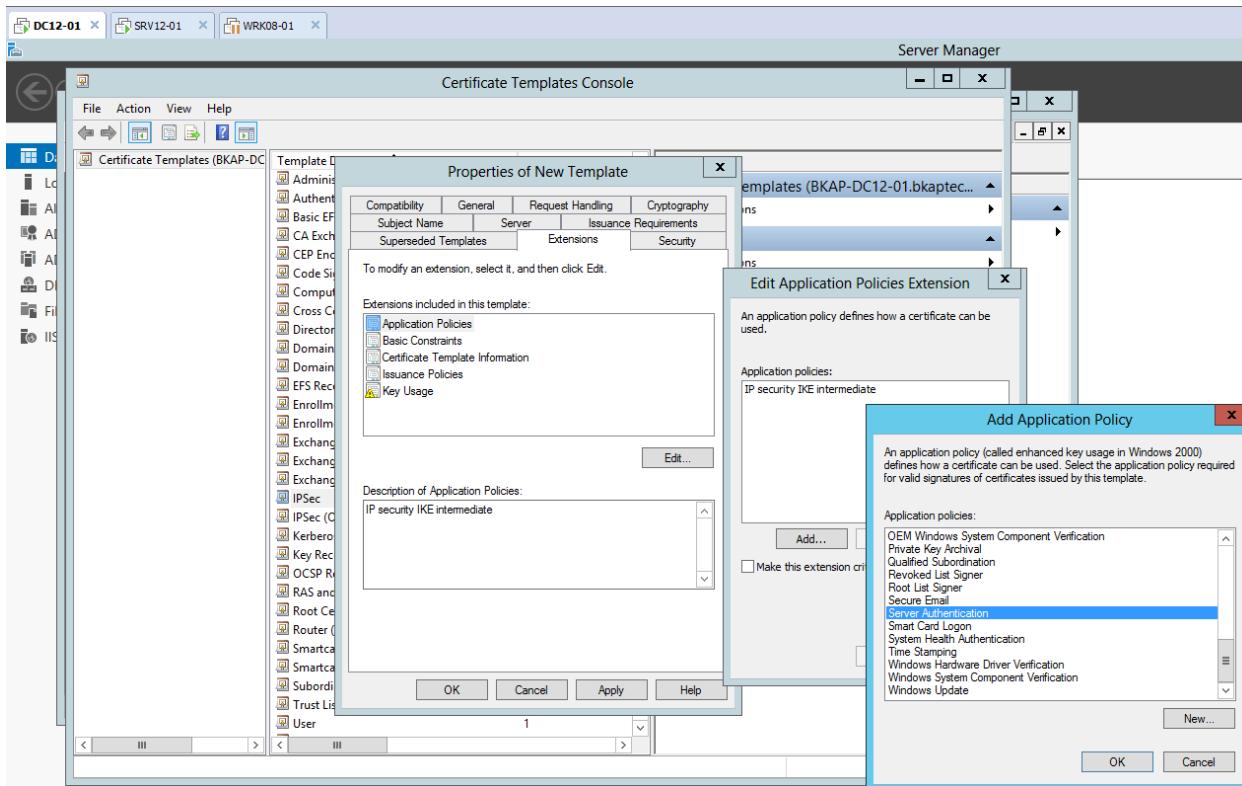
- Chuyển sang tab **Request Handling**, đánh dấu tại **Allow private key to be exported**.



- Chuyển sang tab **Subject Name**, chọn vào **Supply in the request**.

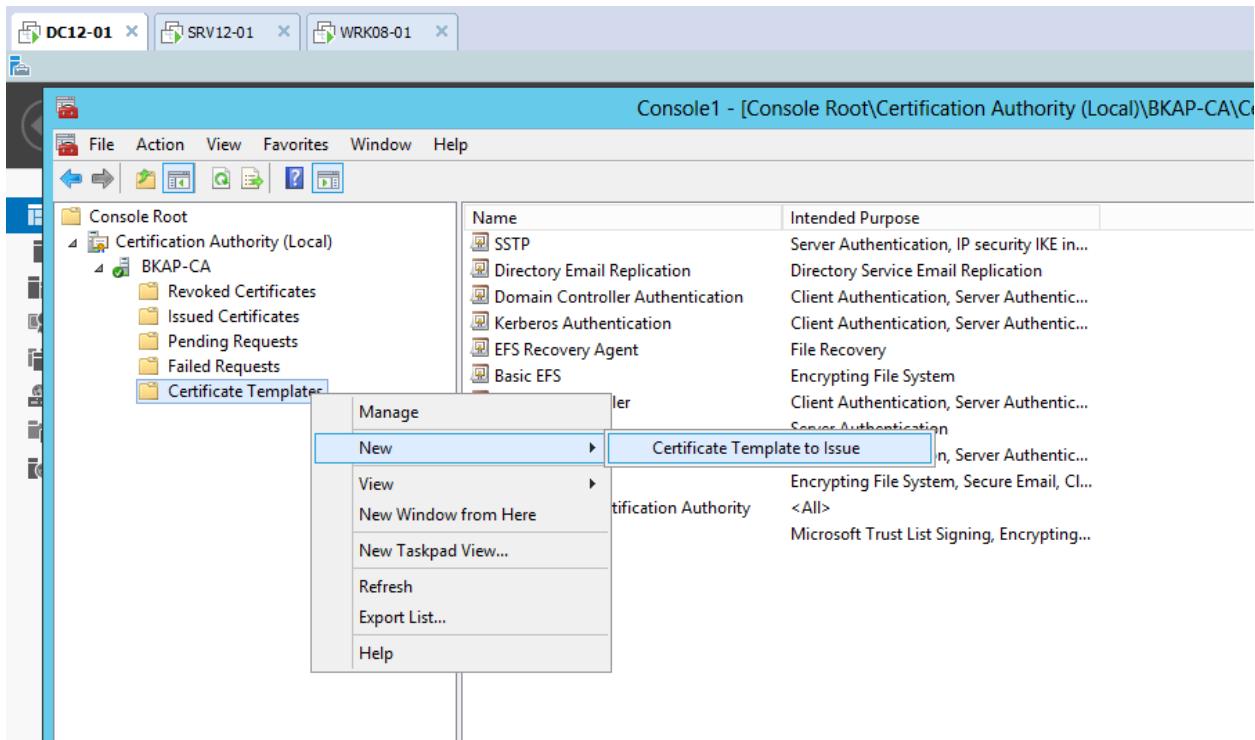


- Chuyển sang tab **Extensions** , click vào **Edit.. / Add...**
 - Tại cửa sổ **Add Application Policy** , chọn **Server Authentication**, / OK.

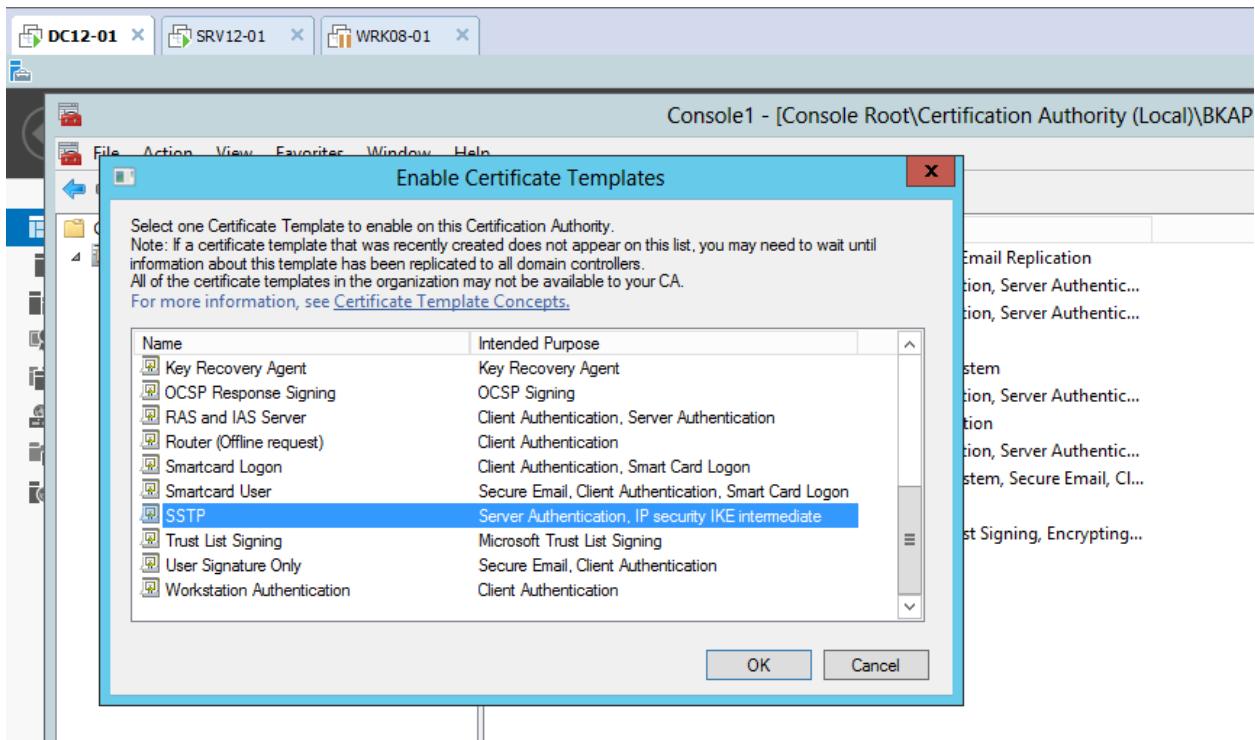


- **OK ...**

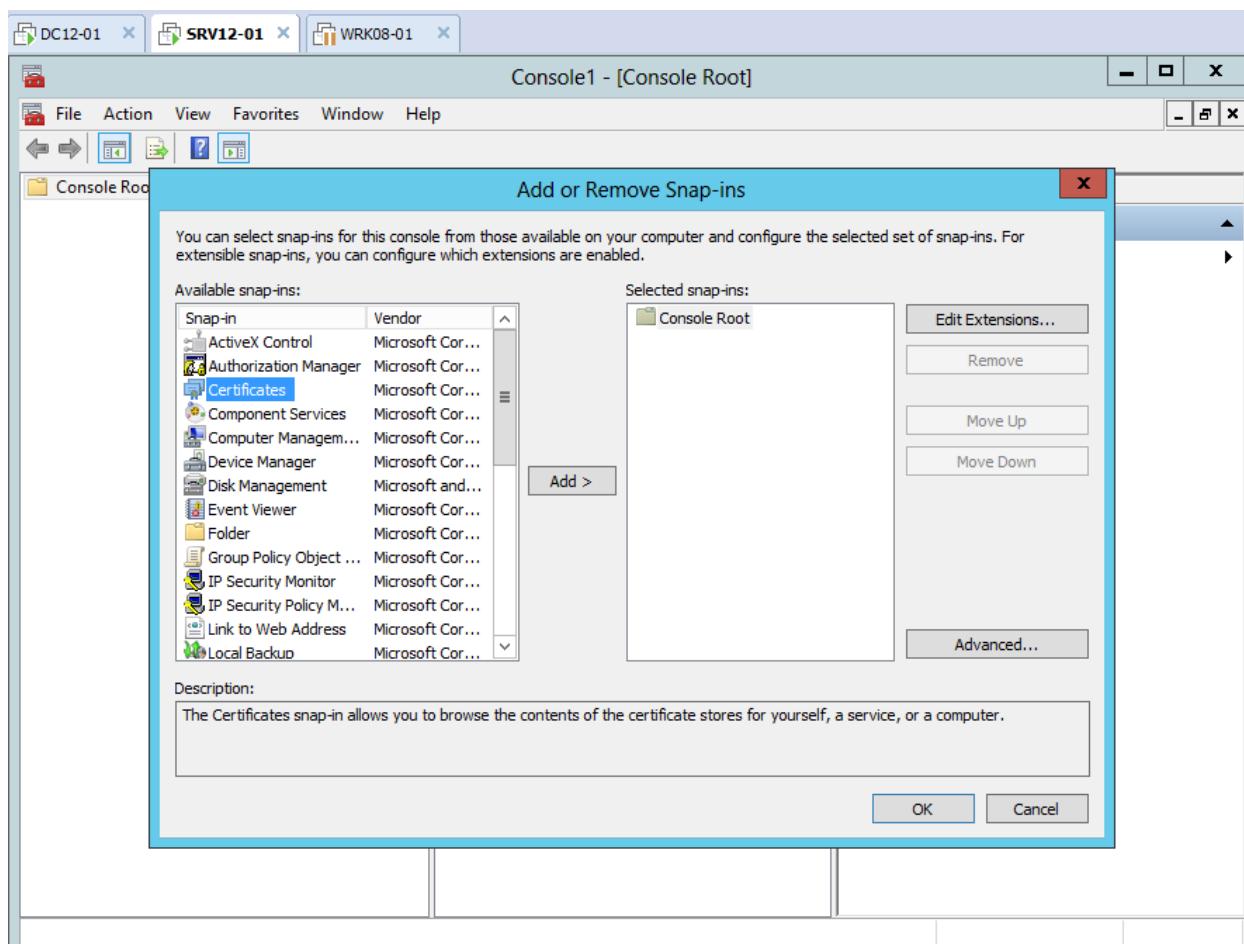
- Tại **Certificate Template** , click chuột phải chọn **New / Certificate to Issue** .



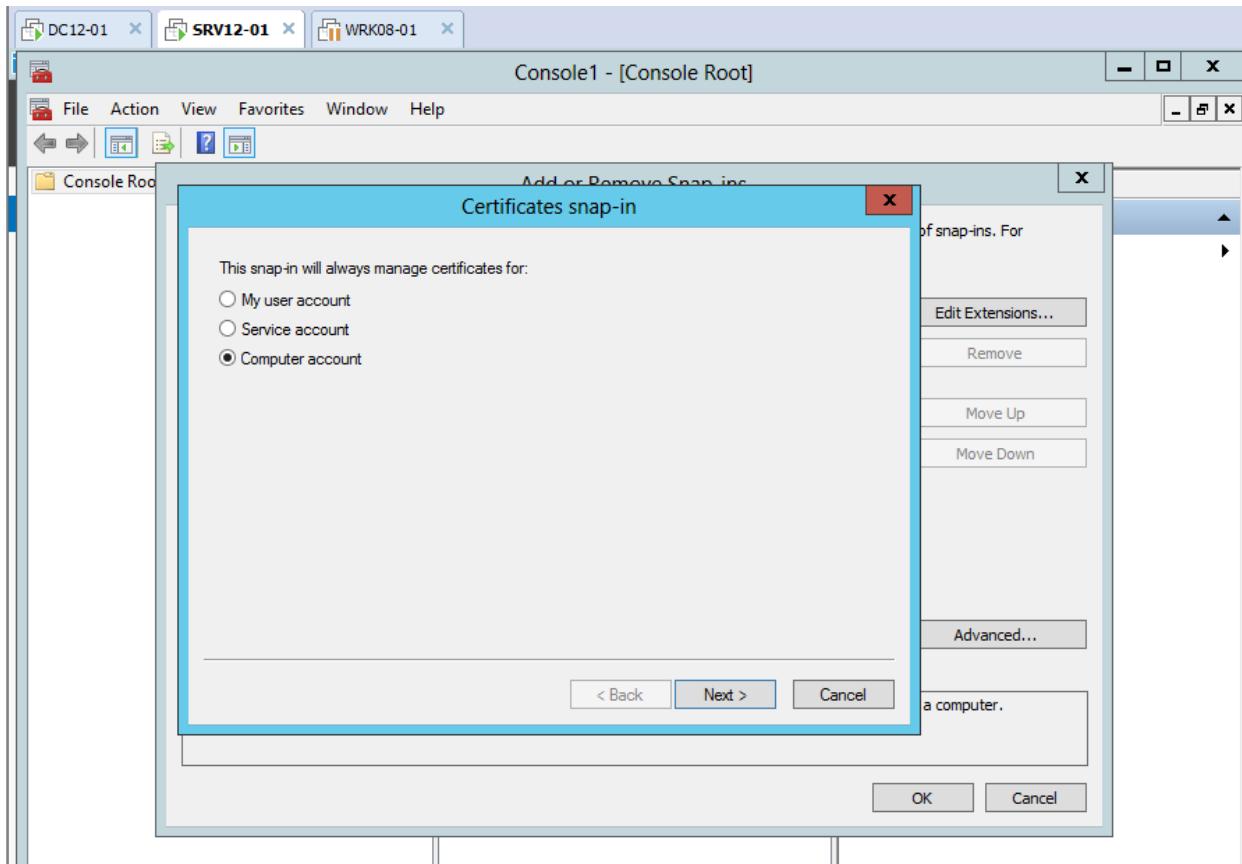
- Tại cửa sổ **Enable Certificate Templates** , chọn vào **SSTP**.

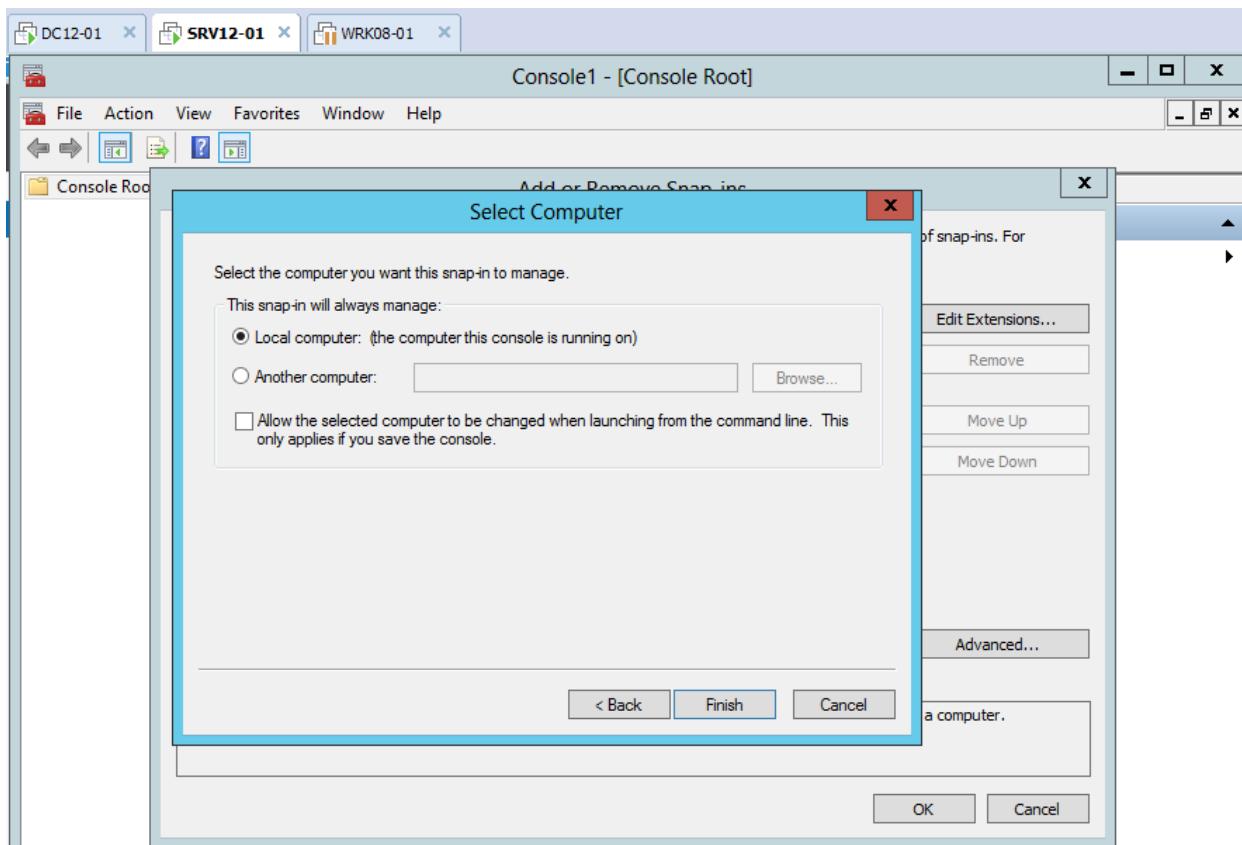


- Chuyển sang máy **BKAP-SRV12-01**, tiến hành **Join vào Domain**, đăng nhập bằng user **bkaptech\administrator**.
 - Xin **SSTP Certificate** cho **VPN Server**.
 - Run / mmc.
 - Tại cửa sổ **Console1 – [Console Root]**, click vào **File /Add or remove Snap-ins**
 - Tại cửa sổ **Add or remove Snap-ins**, chọn **Certificates => Add**

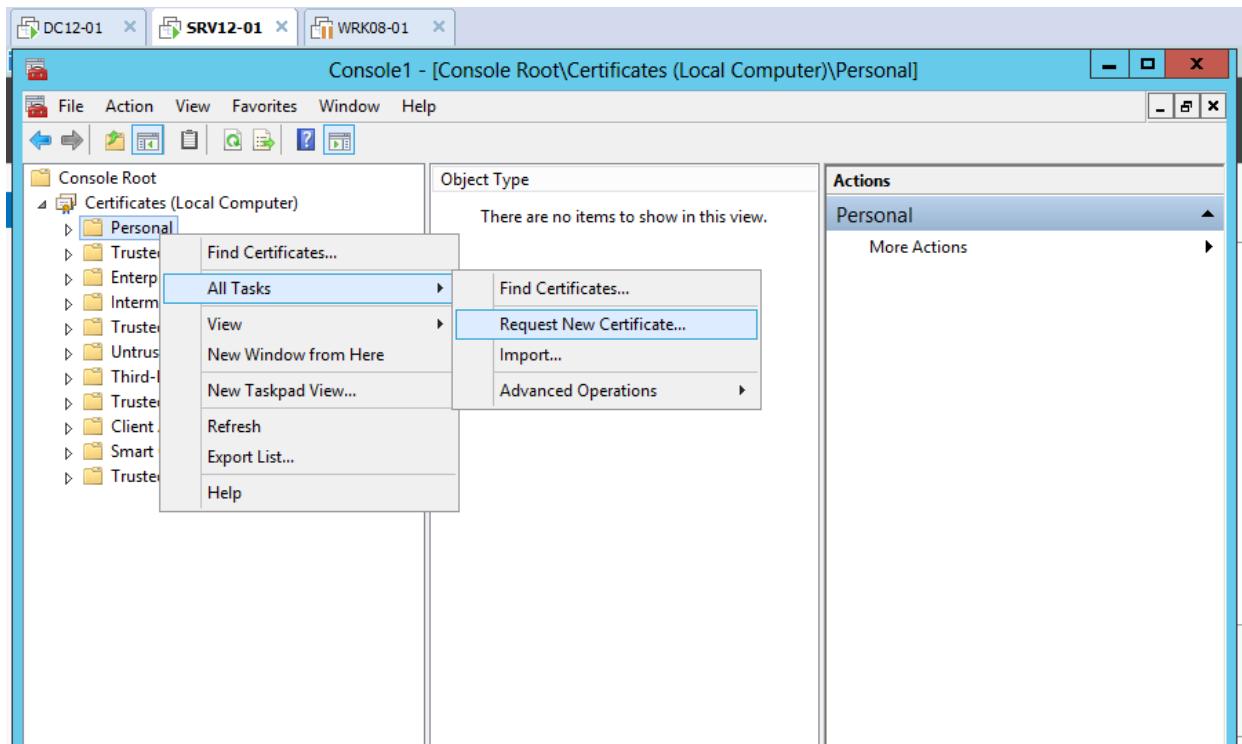


- Tại cửa sổ Certificate snap-in, chọn Computer account , Next...Finish.

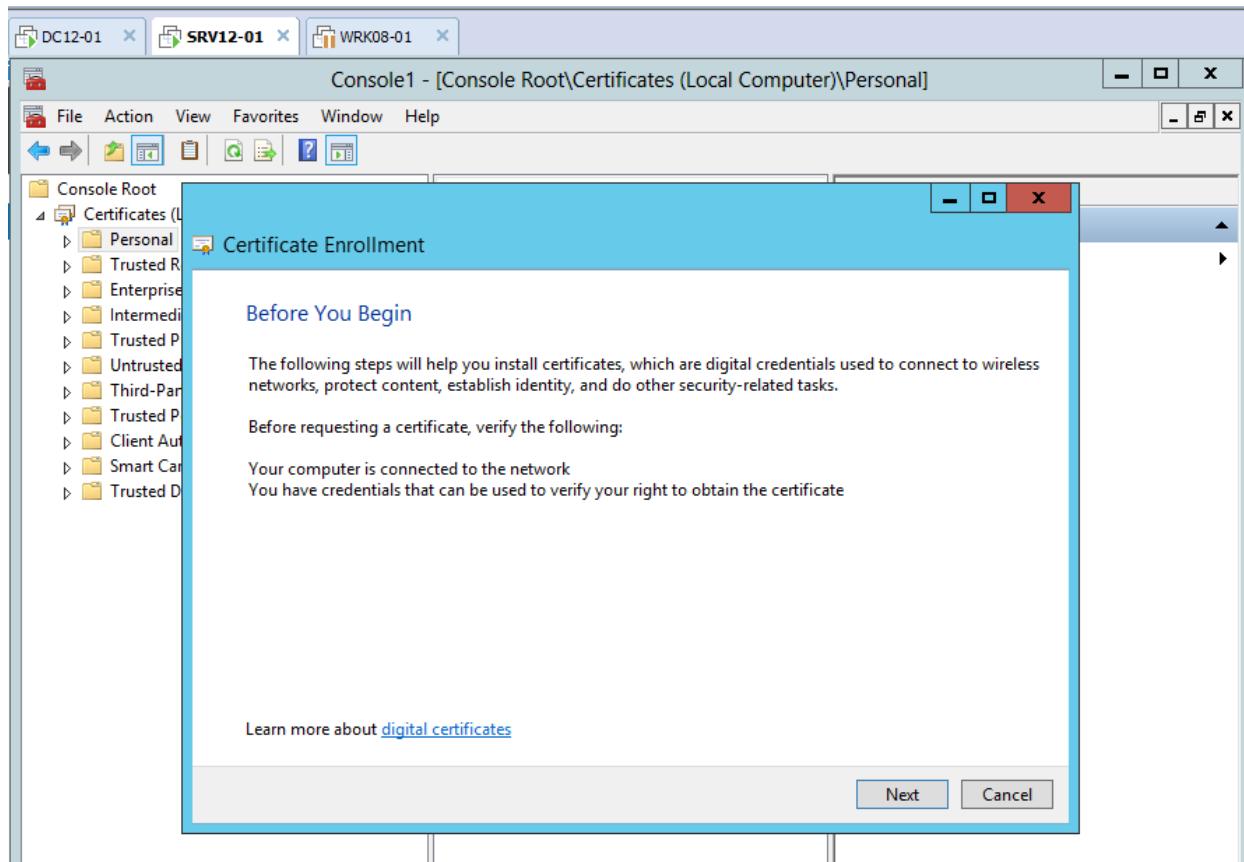


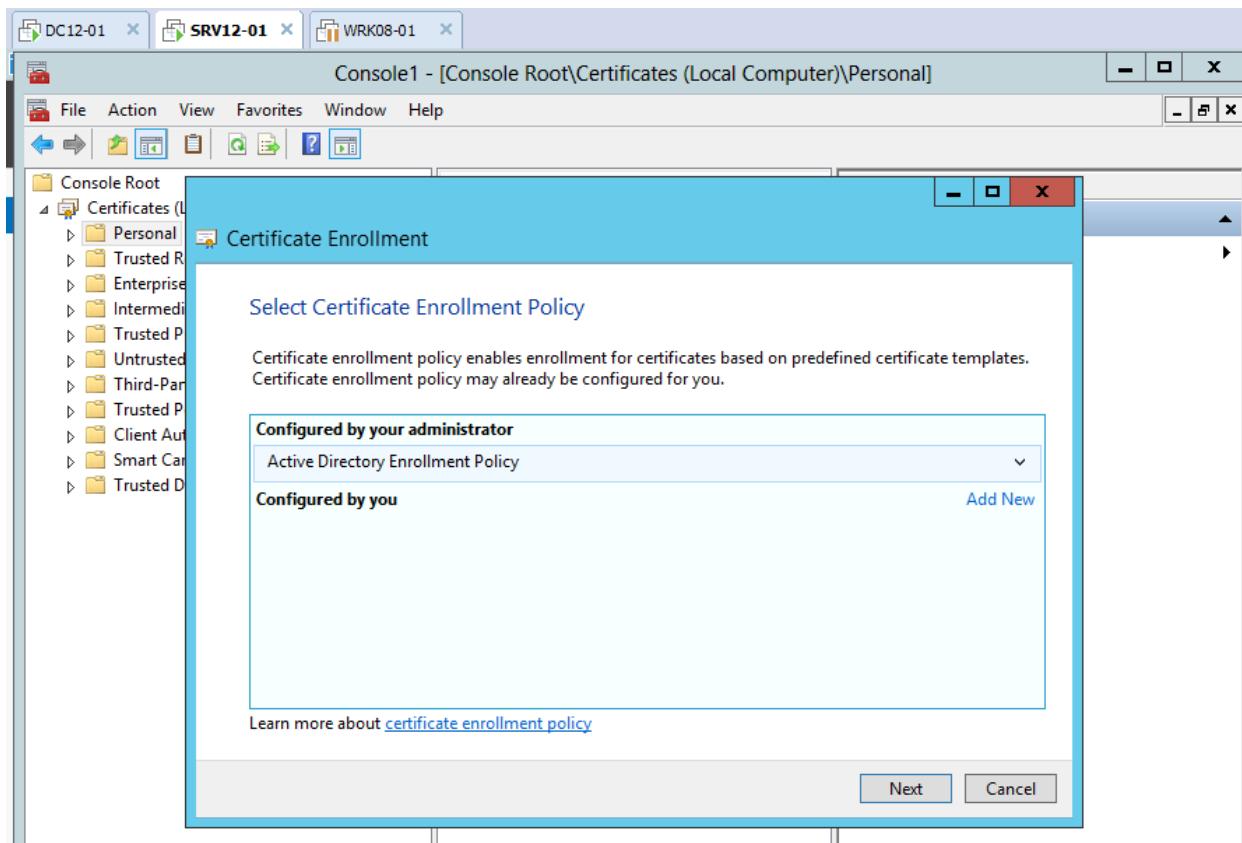


- Tại cửa sổ **Console1** .. chọn vào **Certificate (Local Computer)** / **Personal** / **All Tasks** / **Request New Certificate...**

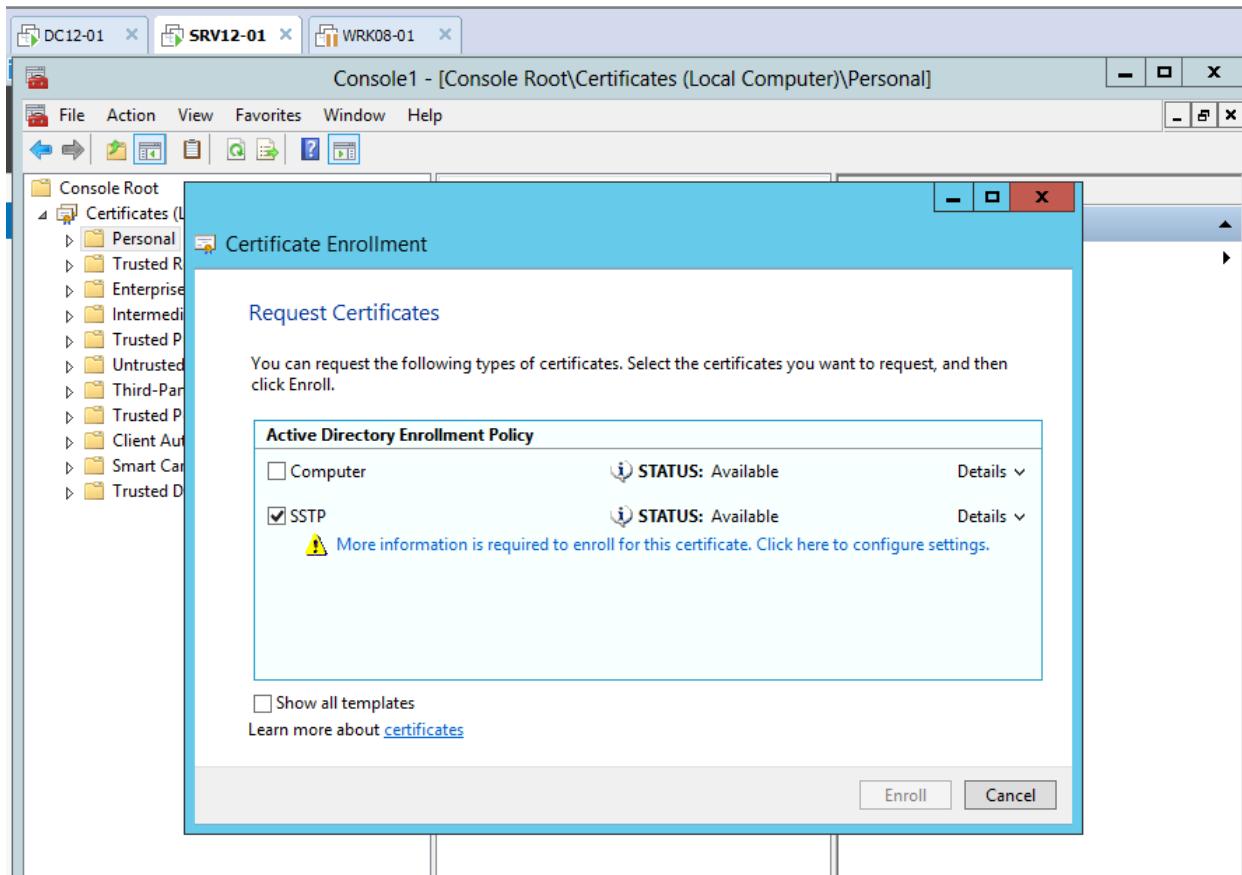


- Tại cửa sổ **Certificate Enrollment** , click **Next**



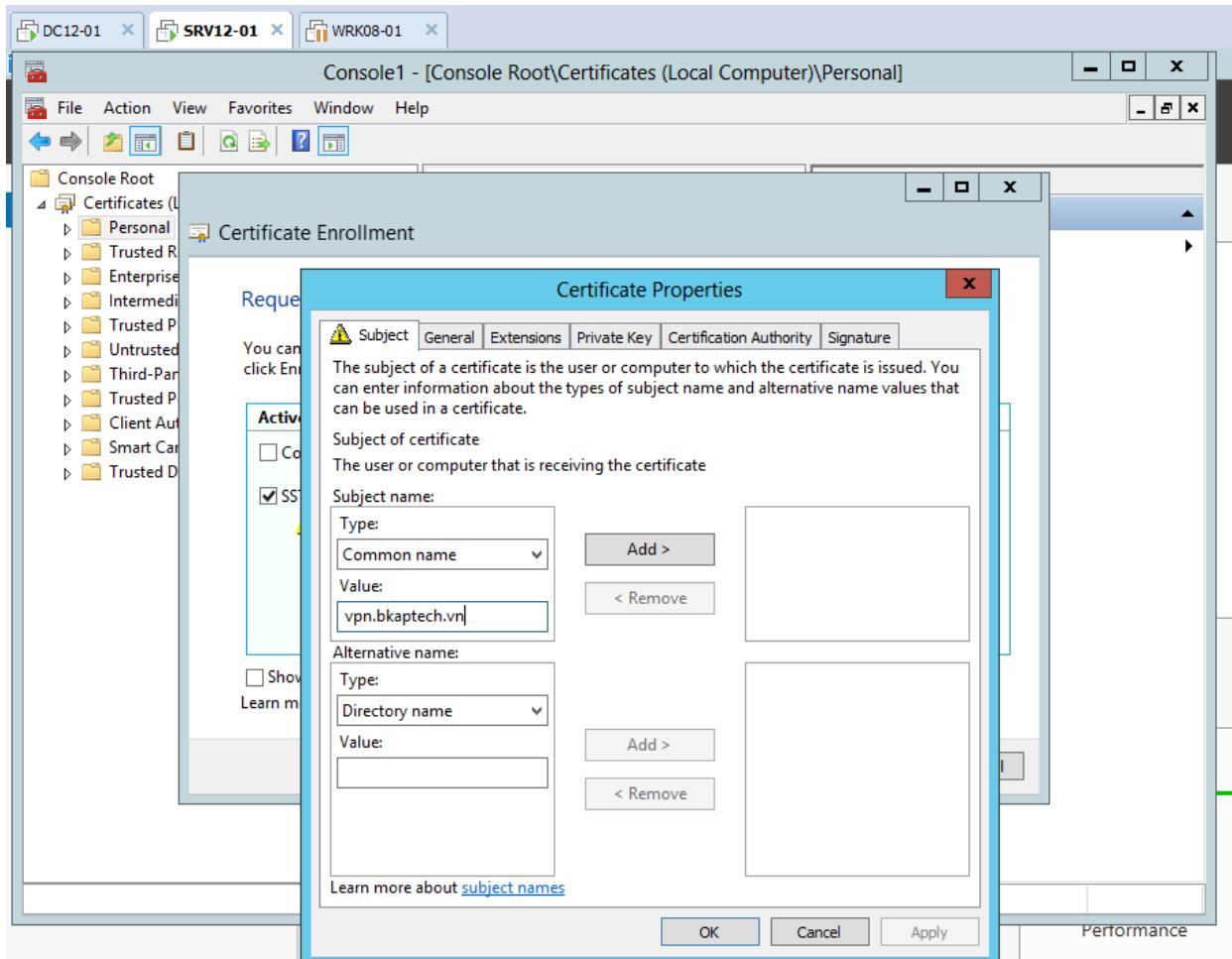


- Tại Request Certificates , chọn Sstp , click vào More information is required to enroll...

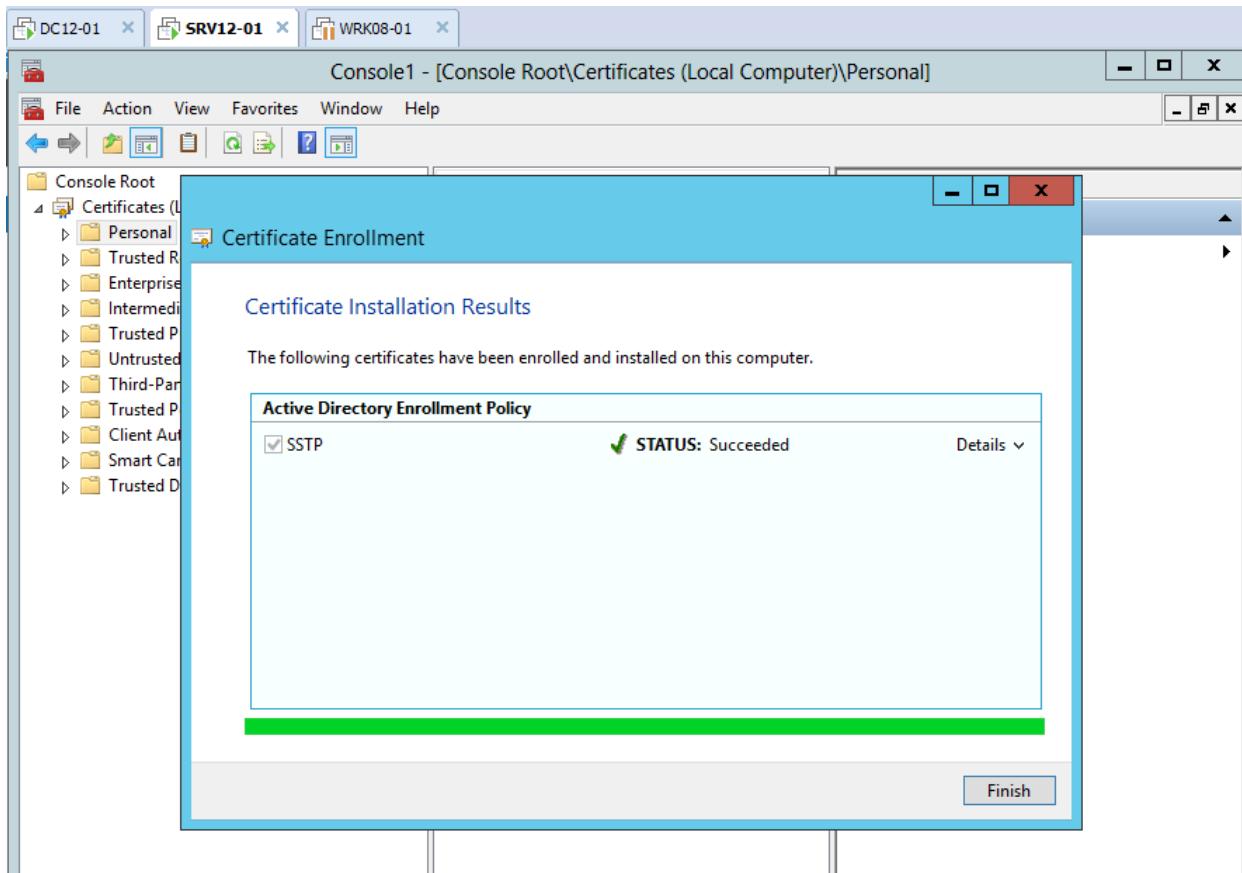


▪ Tại cửa sổ **Certificate Properties** , tab **Subject**:

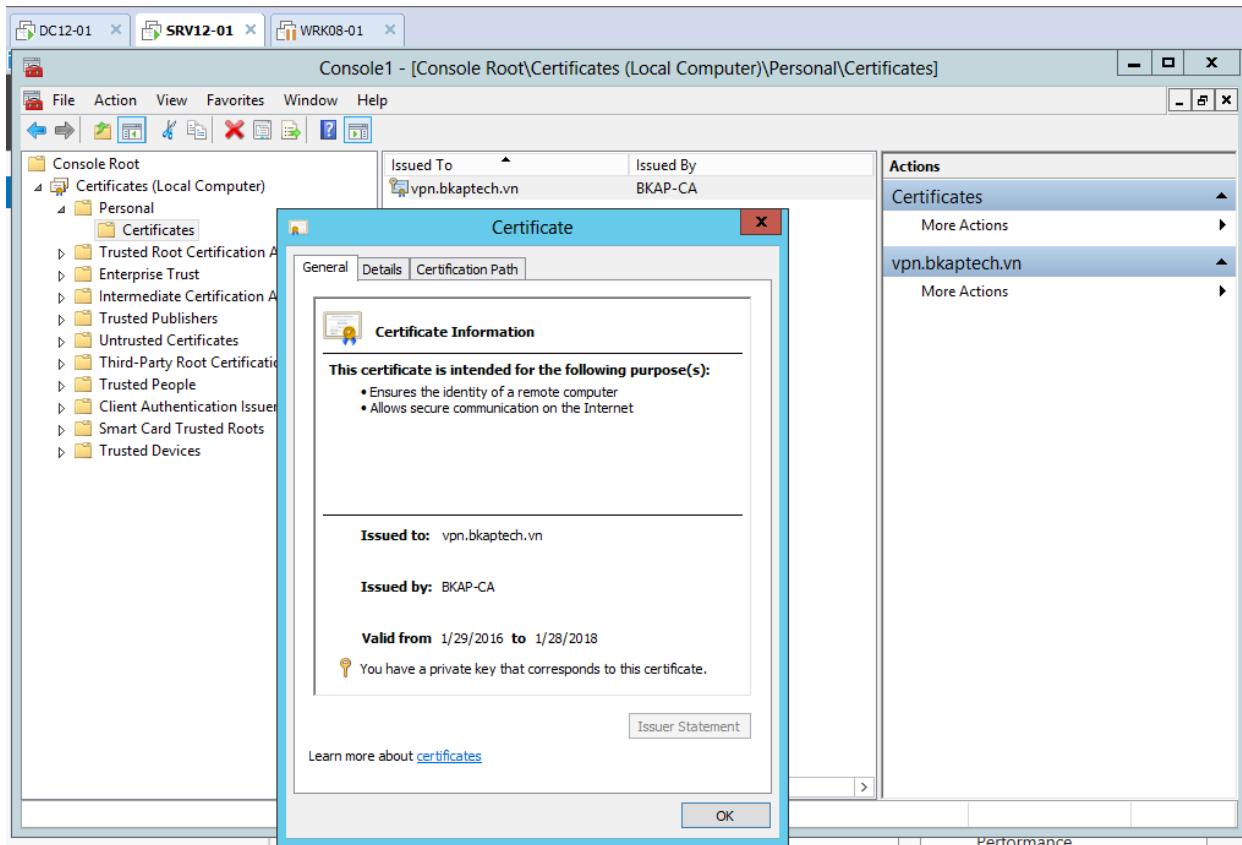
- *Subject name: Common name*
- *Value : vpn.bkaptech.vn*
- *Click vào Add > . OK.*

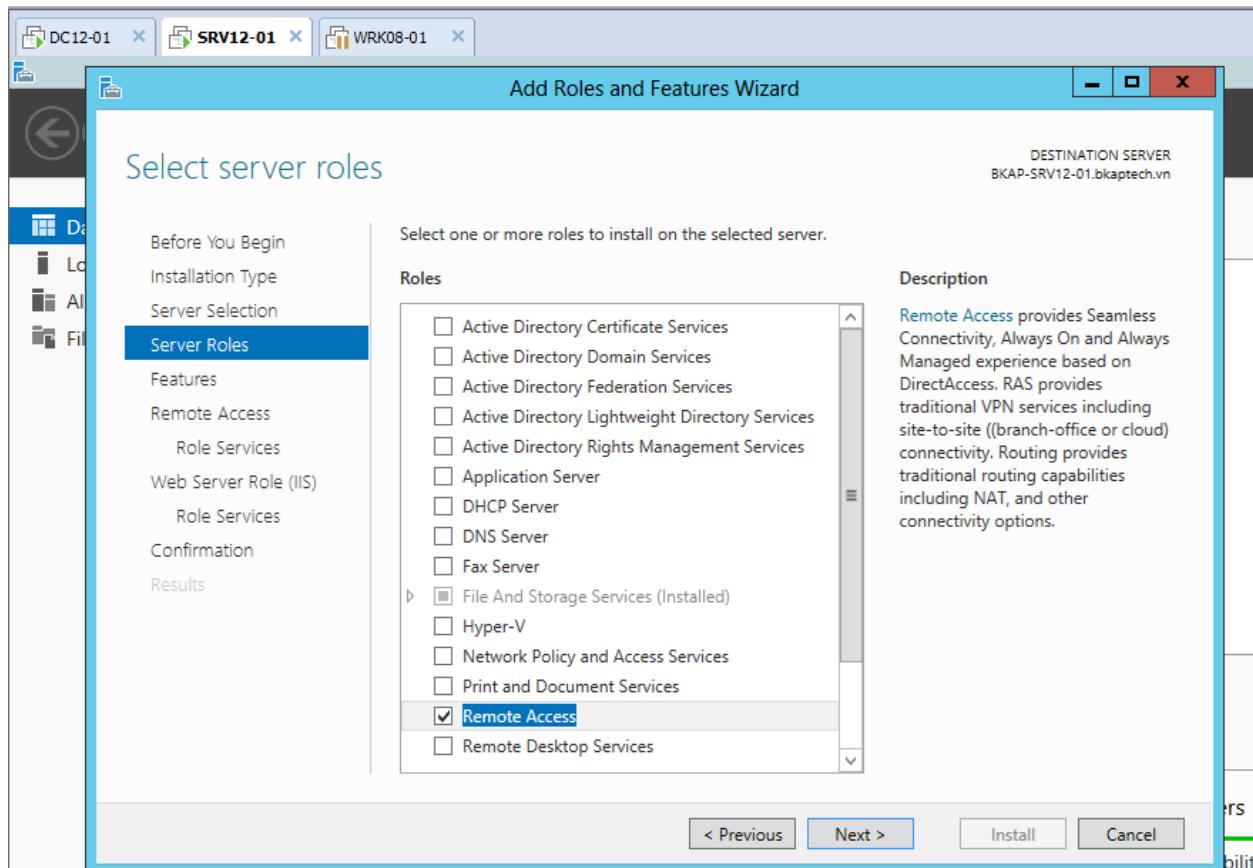


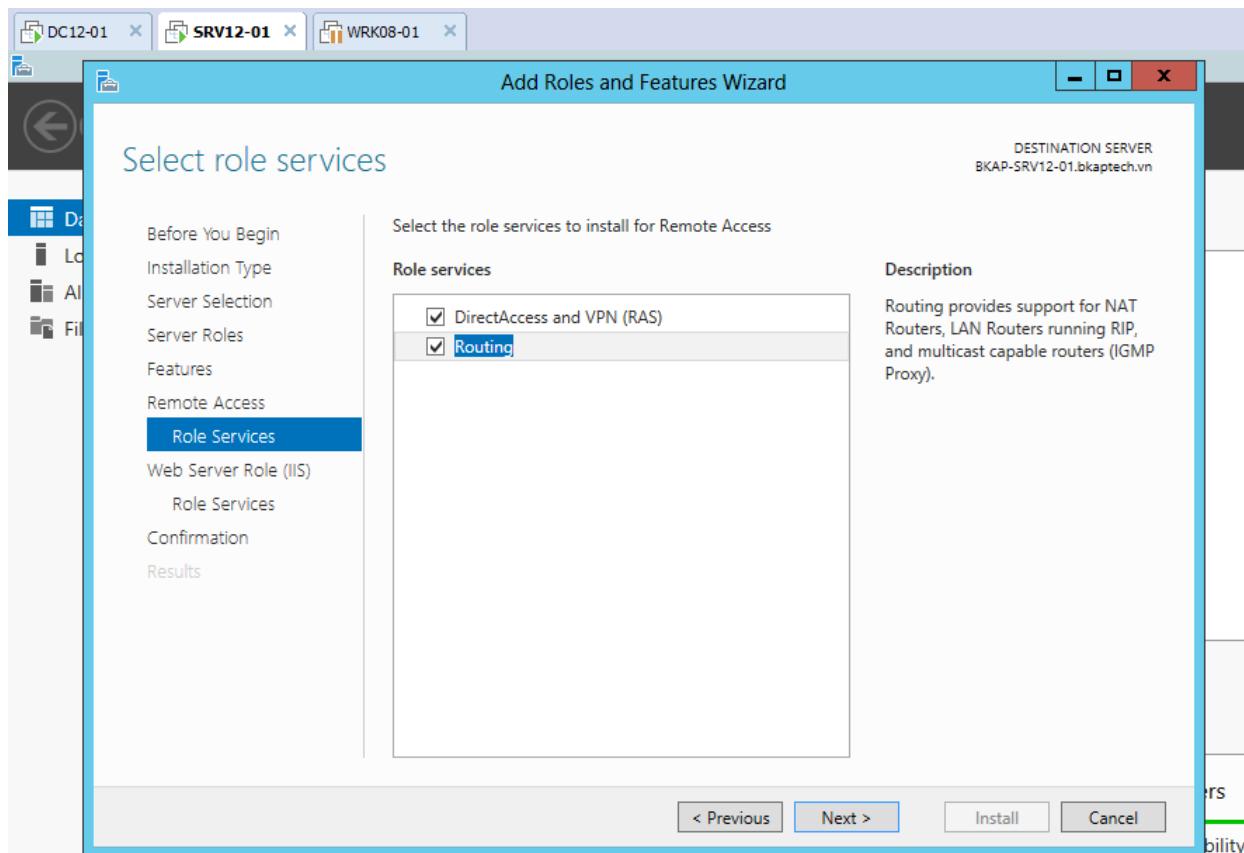
- Tại cửa sổ **Request Certificates**, click vào **Enroll**, sau khi hiện **STATUS: Succeeded**, click vào **Finish**.



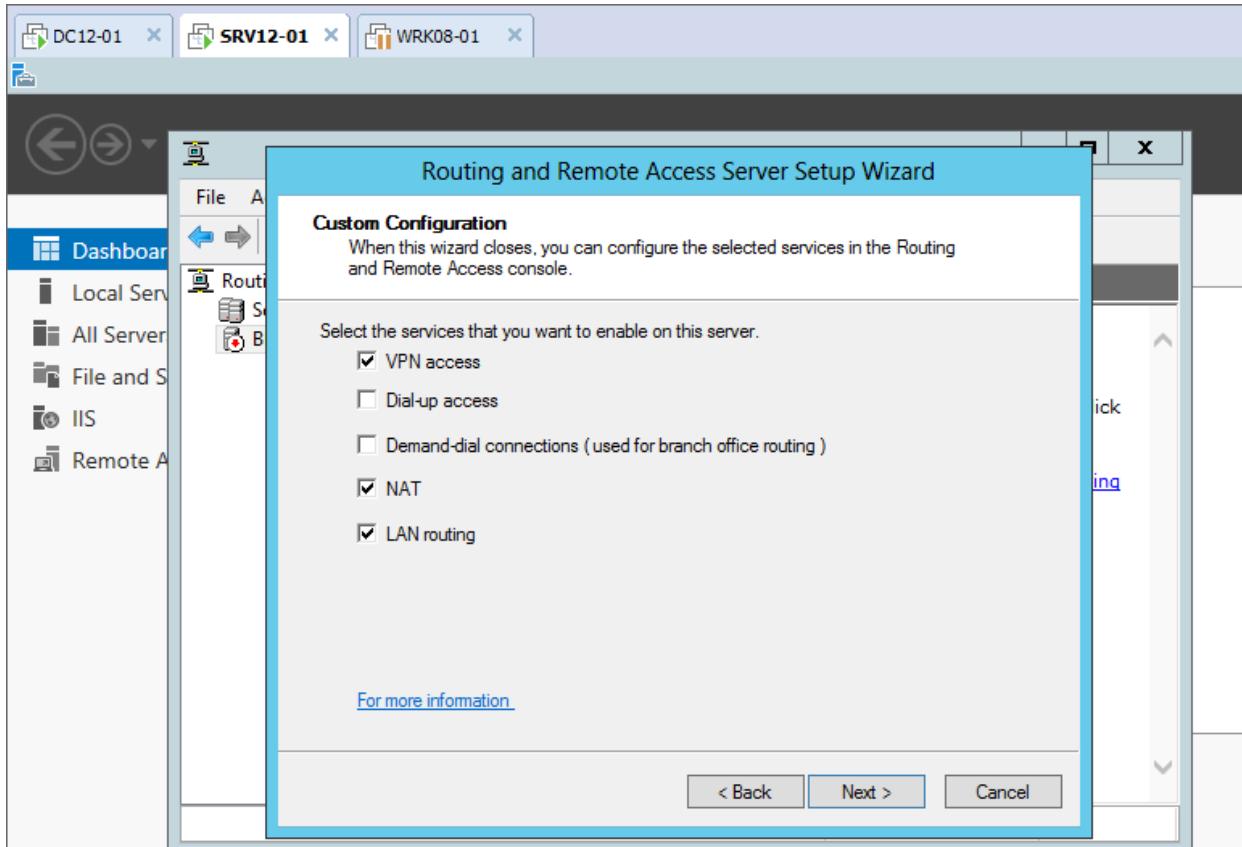
- Kiểm tra CA tại Personal / Certificates.



o Thực hiện cài đặt dịch vụ **Remote Access**.

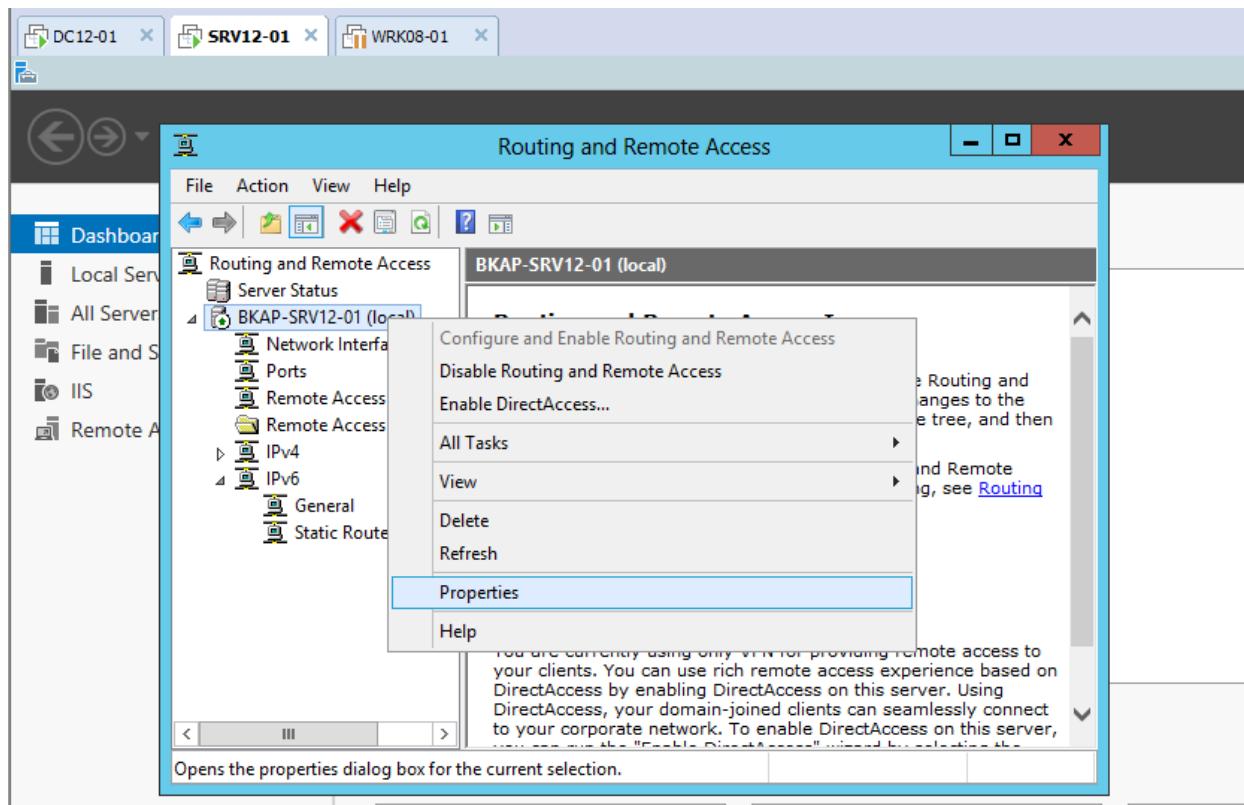


- Thực hiện cấu hình **VPN Client – to – Gateway**.
 - Vào **RRAS / Custom configuration** / chọn vào :
 - *VPN Access*
 - *NAT*
 - *Lan Routing*.

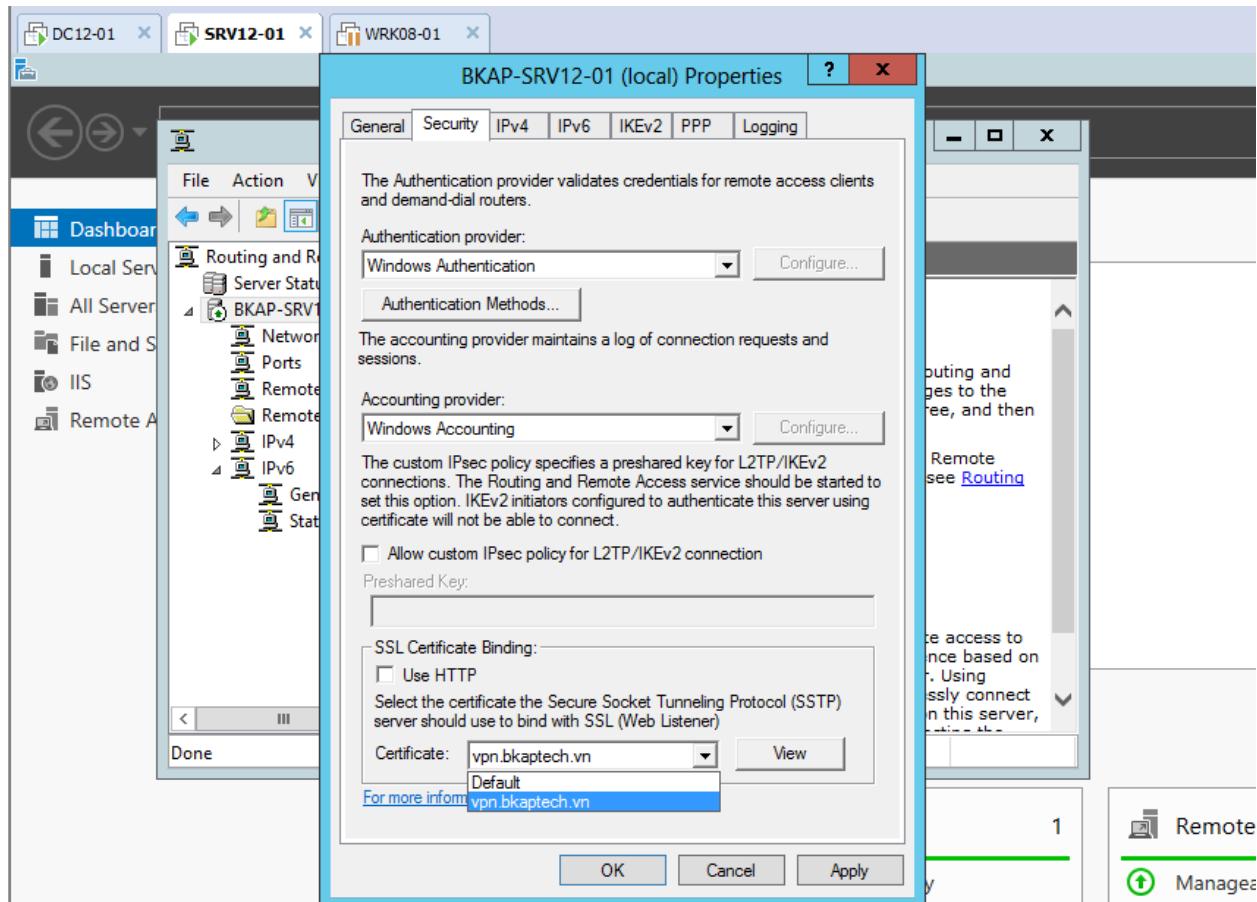


- **Start Services.**

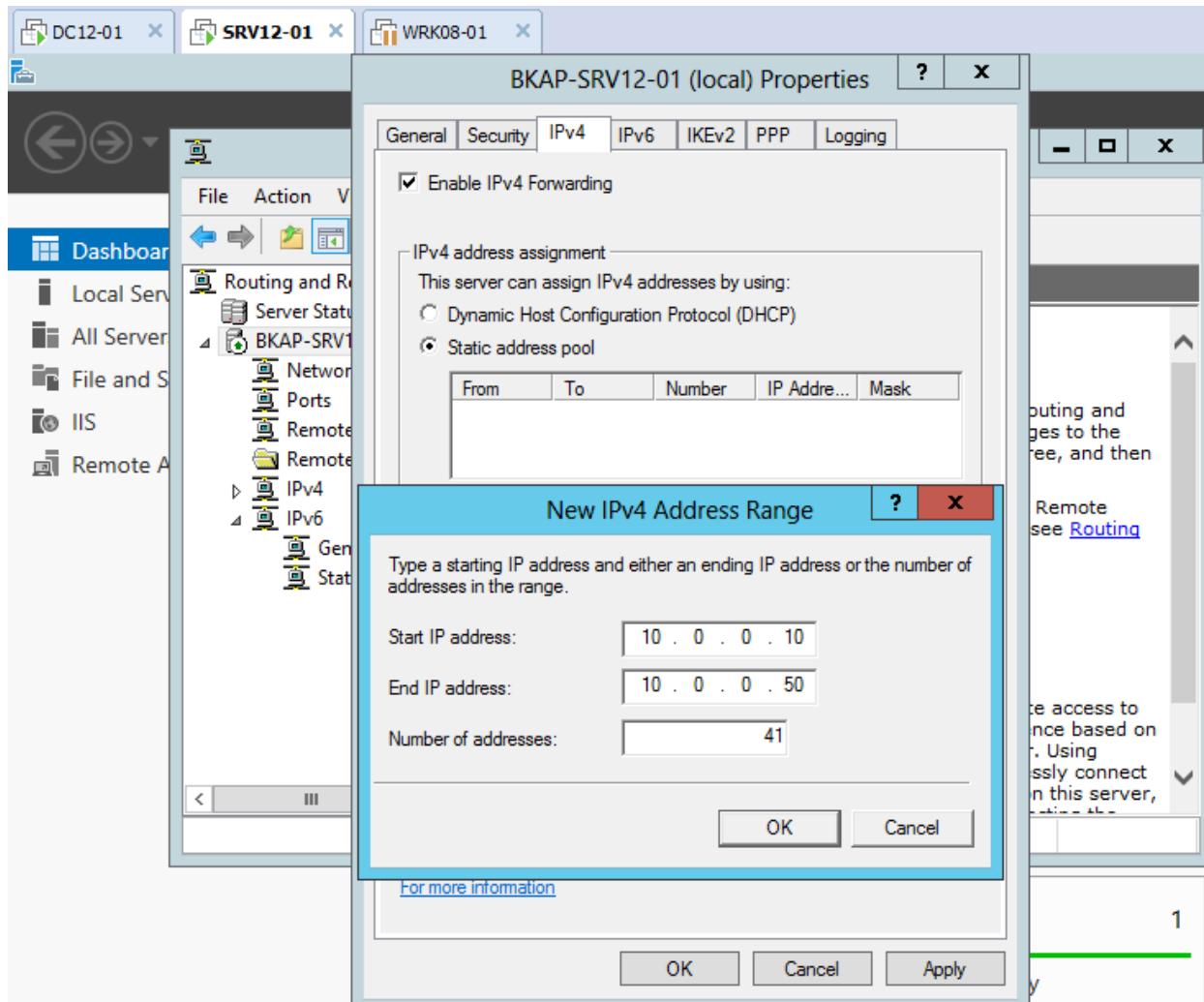
- Tại **BKAP-SRV12-01 (local)** , click chuột phải chọn **Properties**



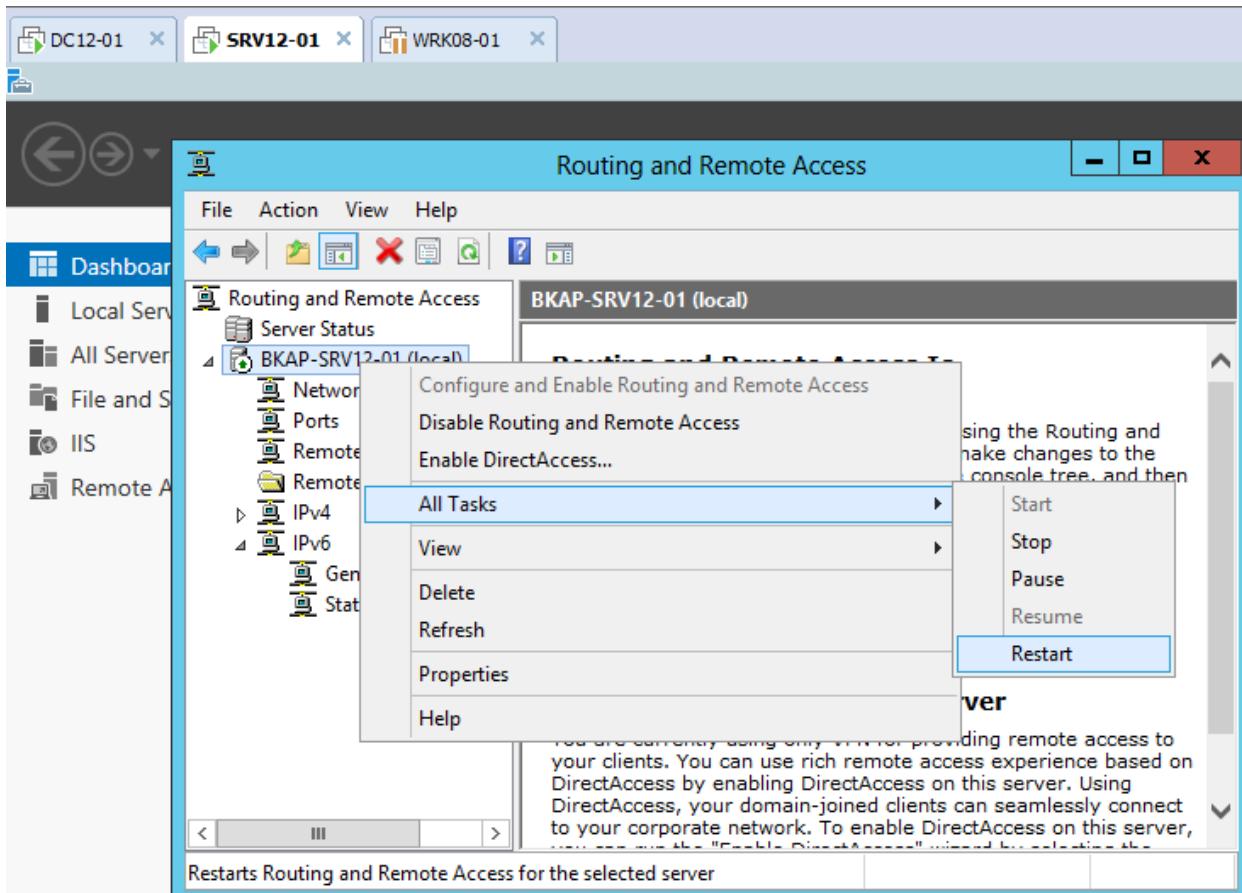
- Tại **BKAP-SRV12-01 (local) Properties**, chuyển sang tab **Security**, tại mục **Certificate** chọn **vpn.bkaptech.vn** / **Apply** (máy chủ stop dịch vụ RRAS)



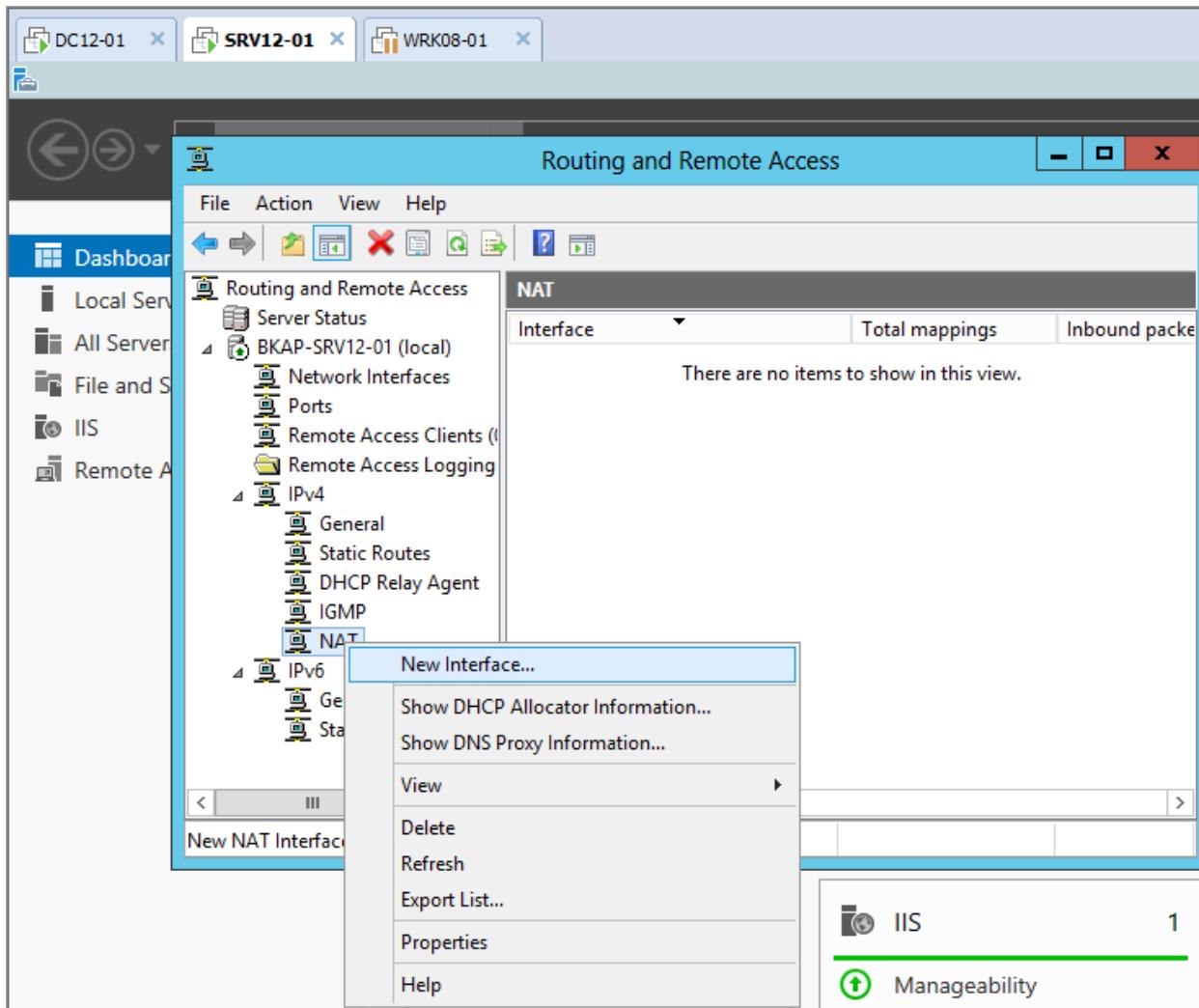
- Chuyển sang tab **IPv4** , chọn **Static address pool** , nhập vào dải địa chỉ cấp phát cho máy trạm (10.0.0.10 – 10.0.0.50).



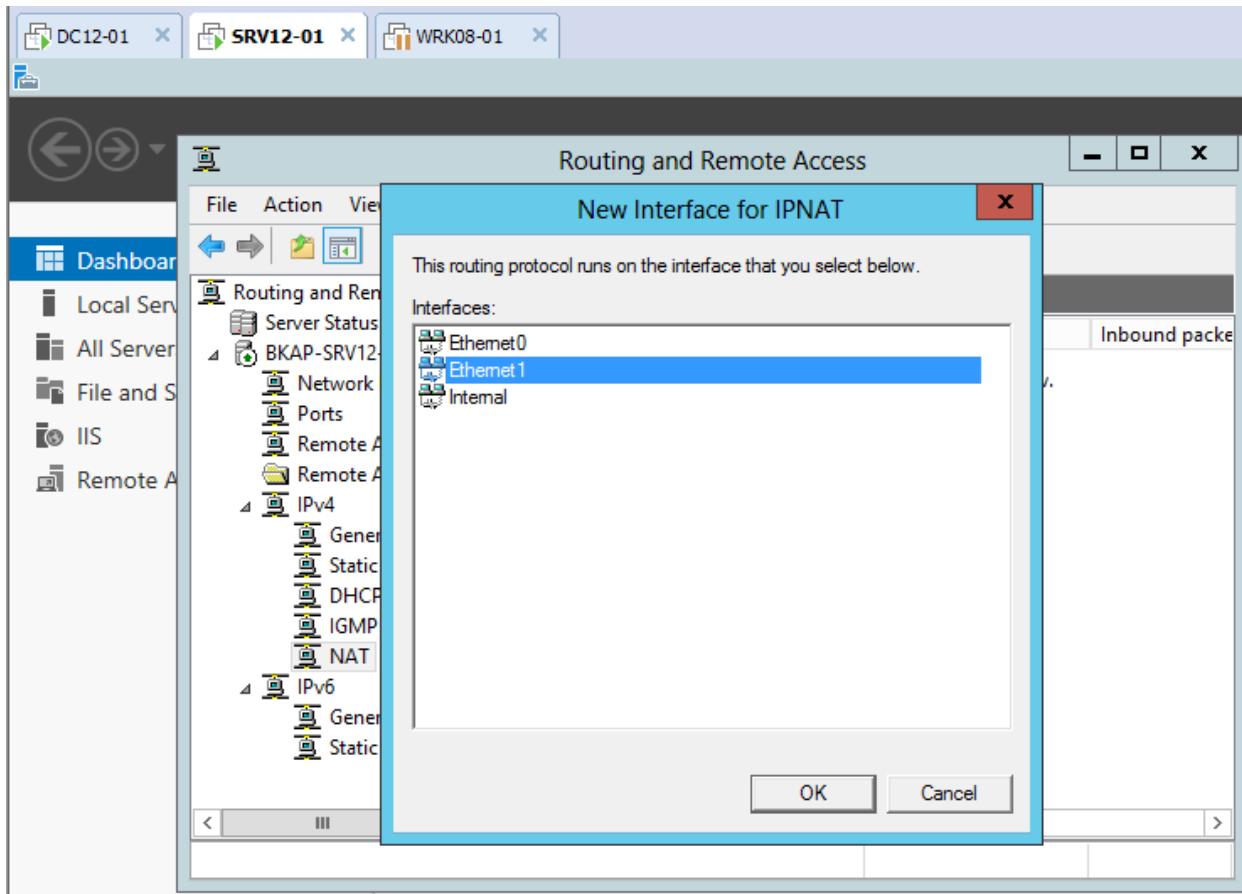
- Restart lại dịch vụ RRAS.



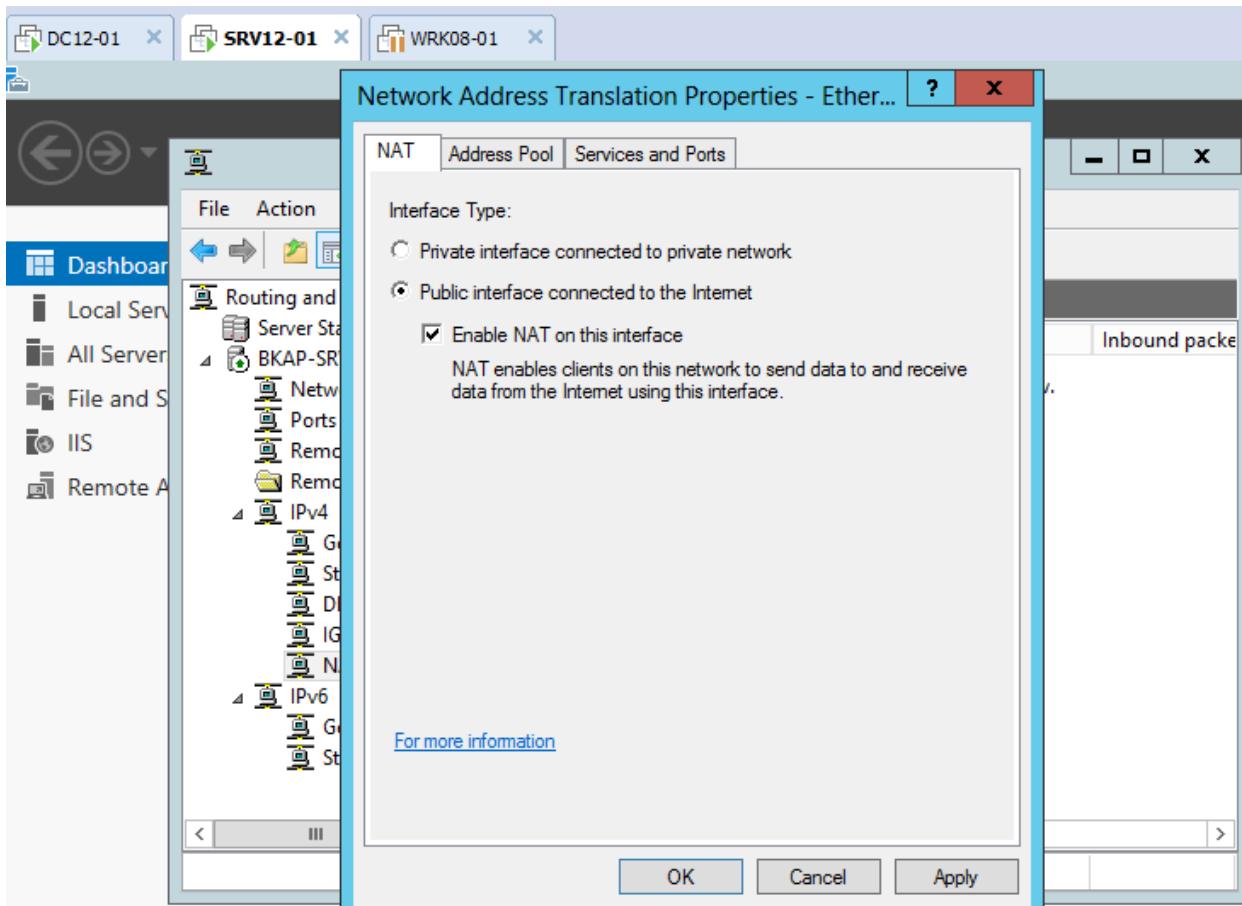
- Click vào **IPv4 / NAT** , click chuột phải tại đây , chọn **New Interface...**



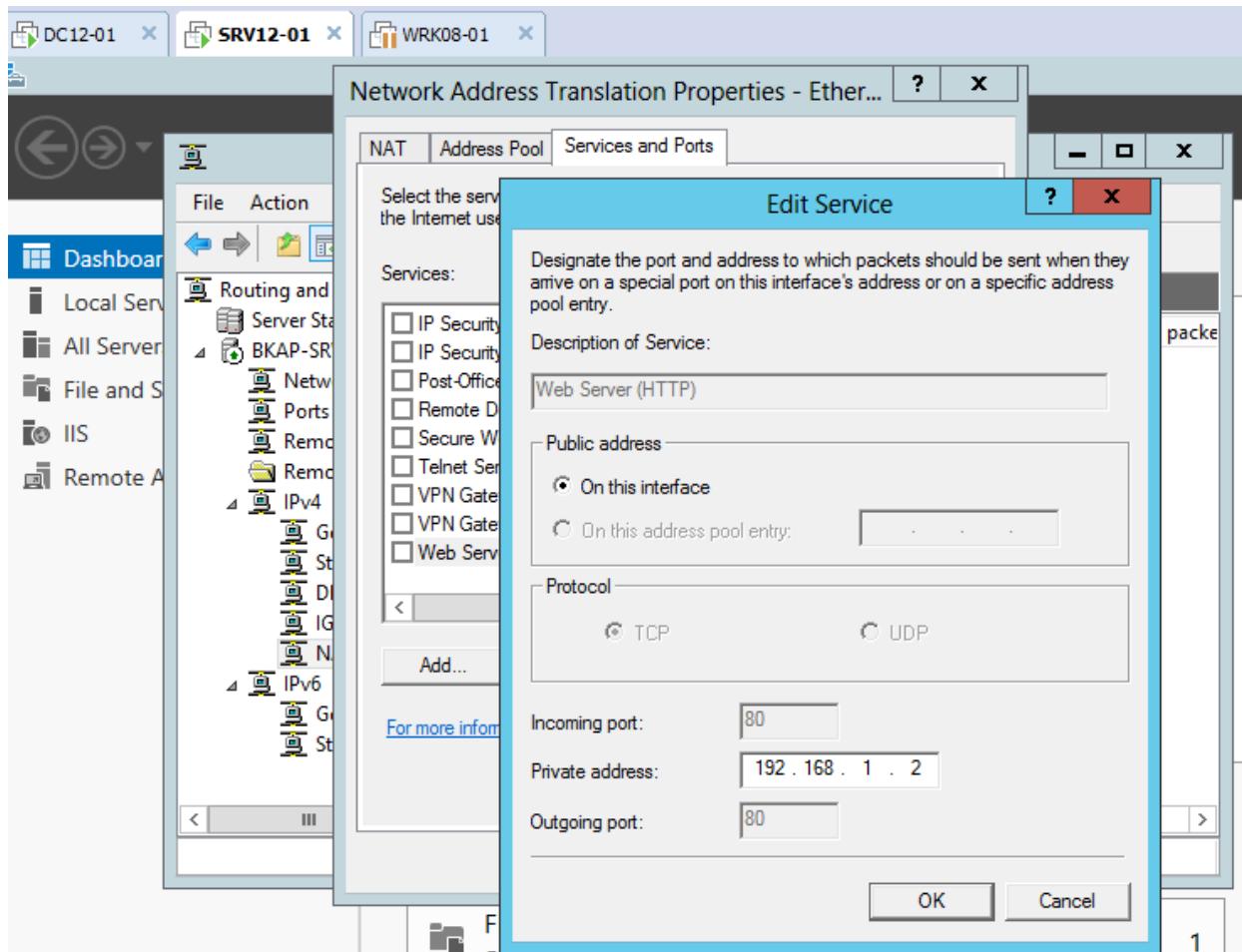
- Tại cửa sổ **New Interface for IPNAT**, chọn card bên ngoài (*Ethernet1*) / **OK**.

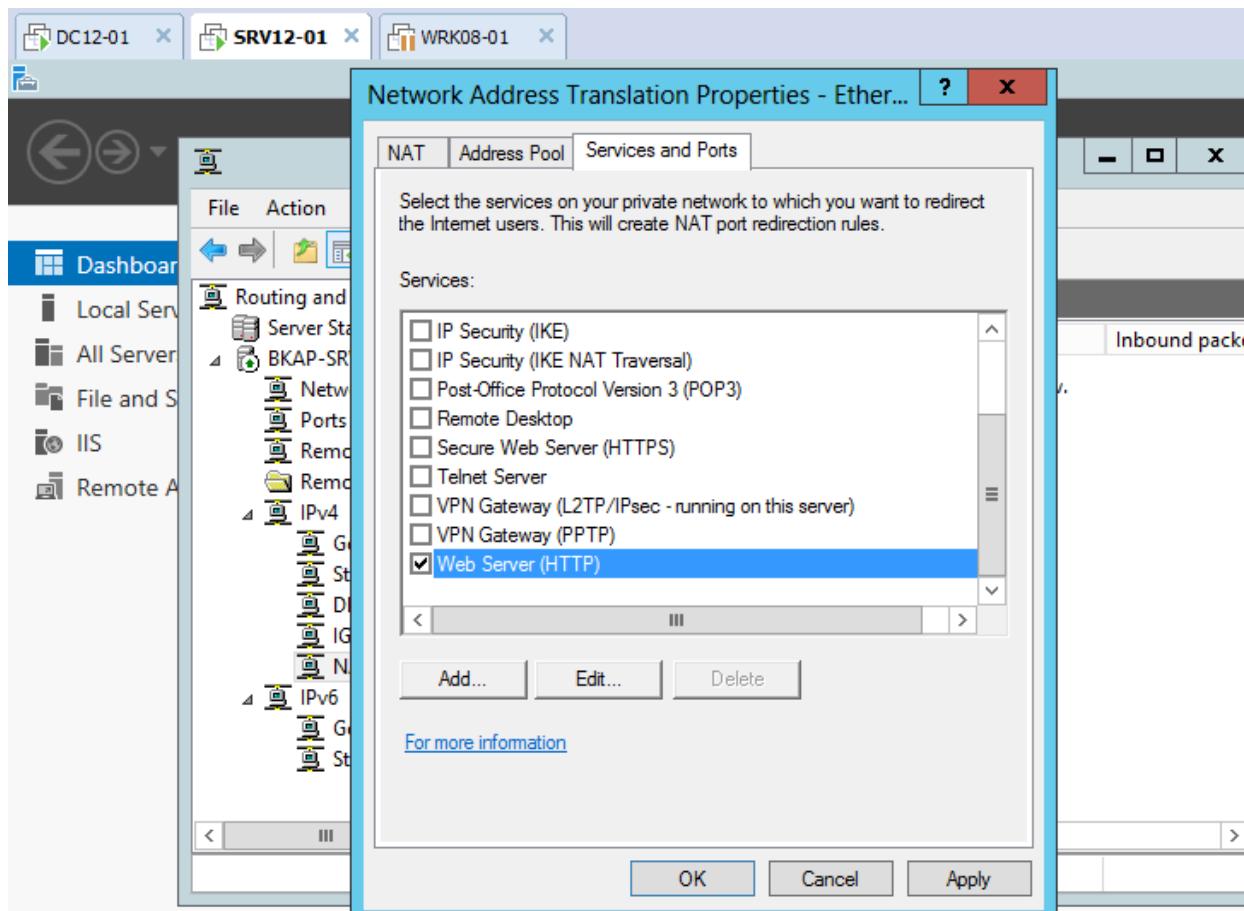


- Tại cửa sổ Network Address Translation Properties... , chọn vào loại Interface Type là Public (NAT enables...)

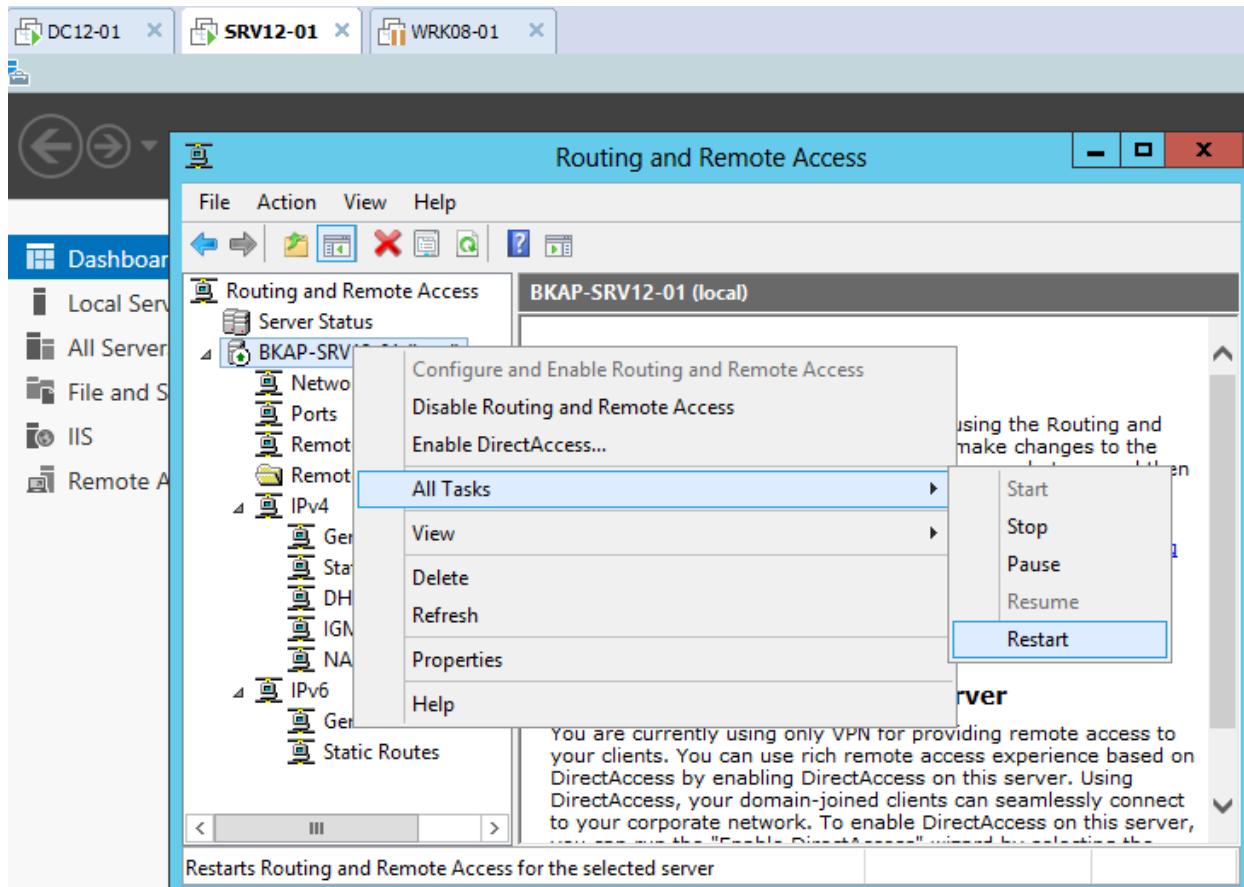


- Chuyển sang tab **Services and Ports**, chọn dịch vụ **Web Server**, nhập vào địa chỉ **Private address : 192.168.1.2 (Domain Controller)**

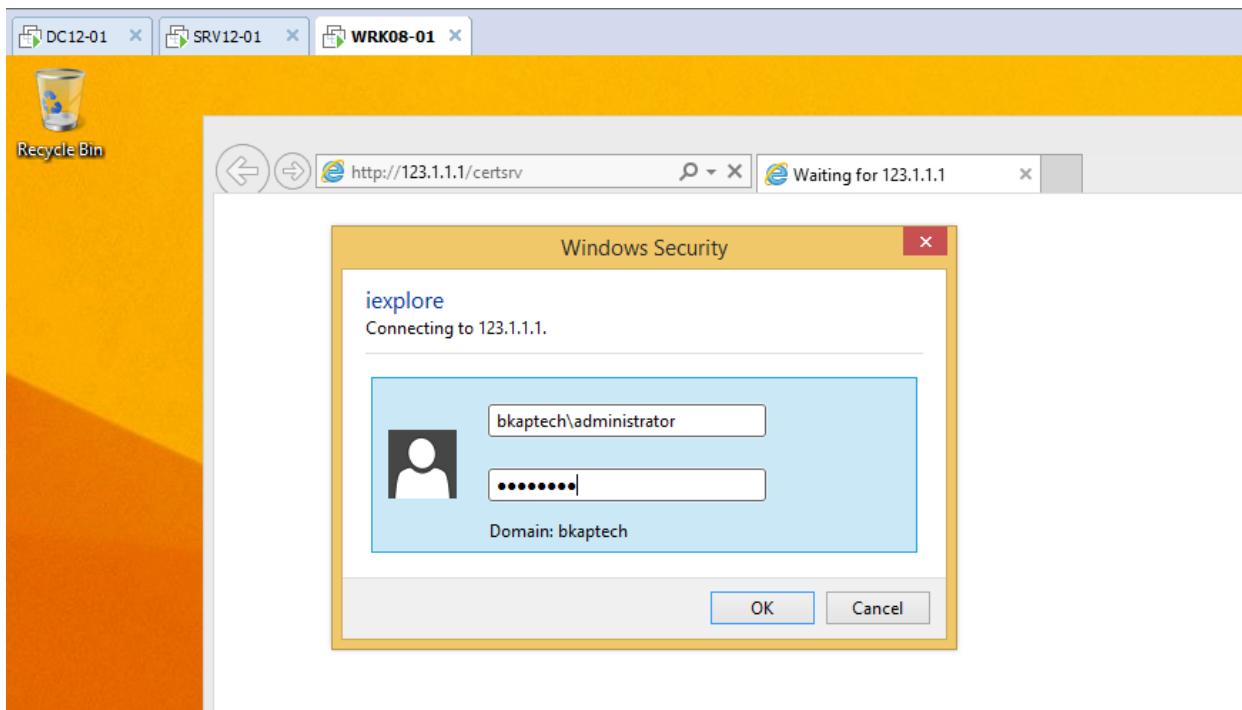




- Restart lại dịch vụ **RRAS**.



- Chuyển sang máy trạm **Client Win 8**, thực hiện download CA cho máy trạm:
 - Vào **Internet Explorer**, gõ địa chỉ <http://123.1.1.1/certsrv>
 - Nhập địa chỉ **administrator** trong miền *bkaptech.vn*



Microsoft Active Directory Certificate Services -- BKAP-CA

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other tasks.

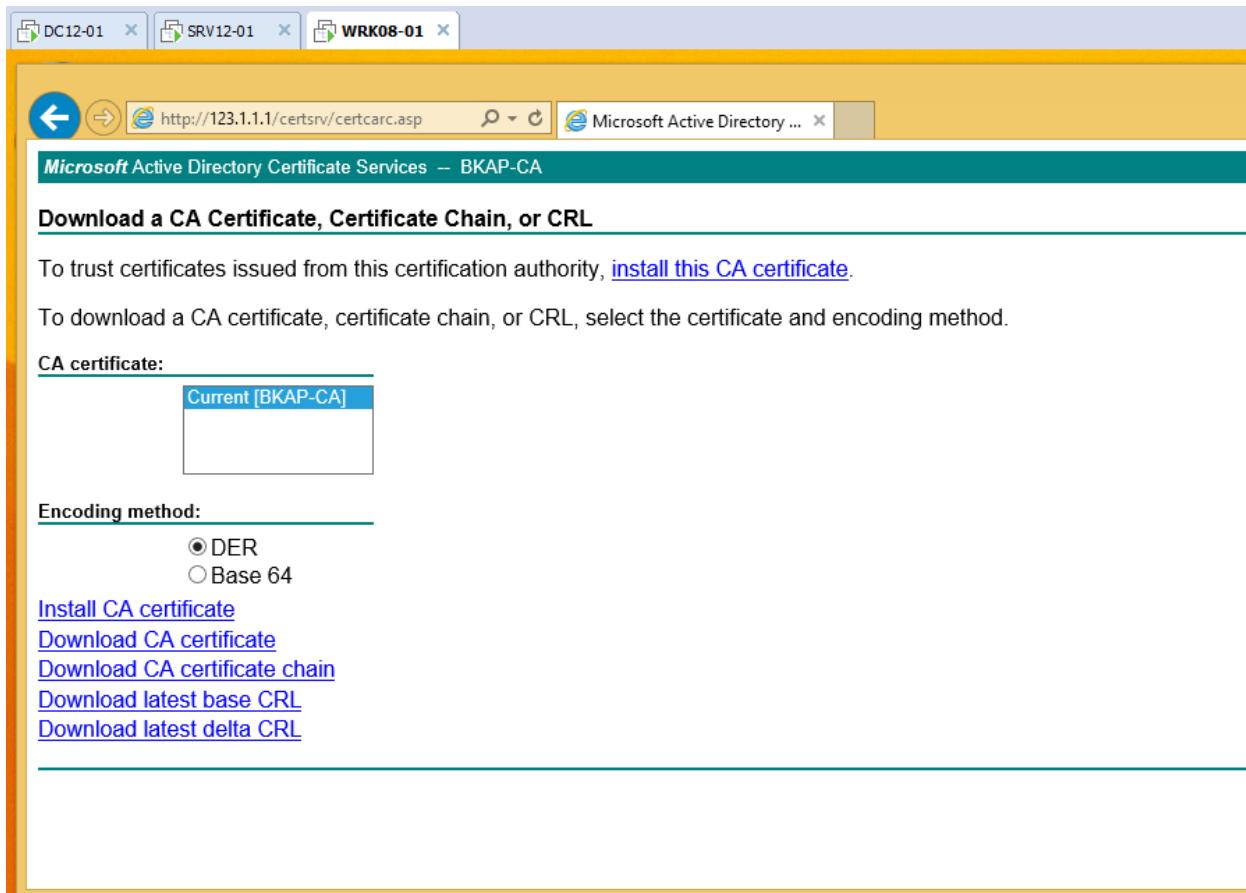
You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), pending request.

For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).

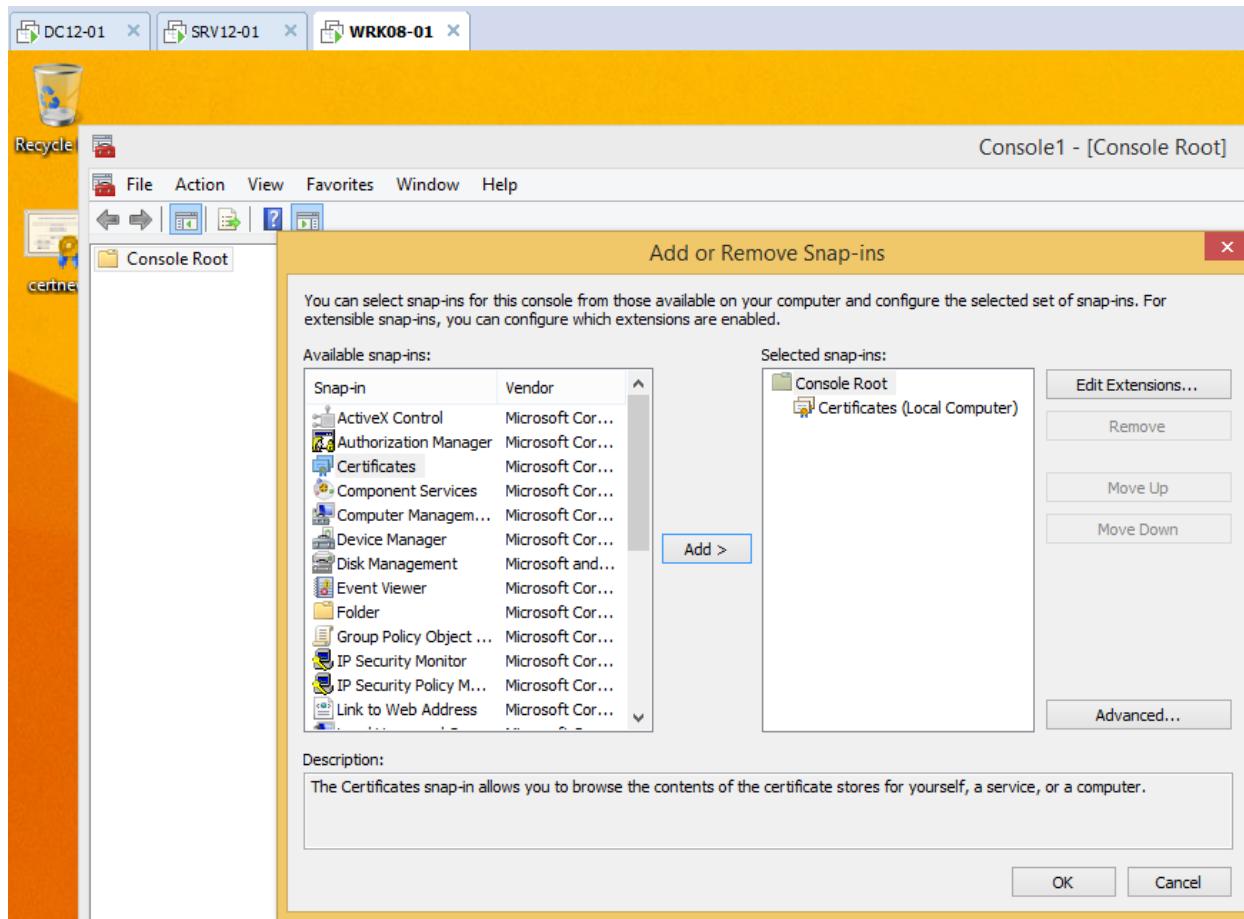
Select a task:

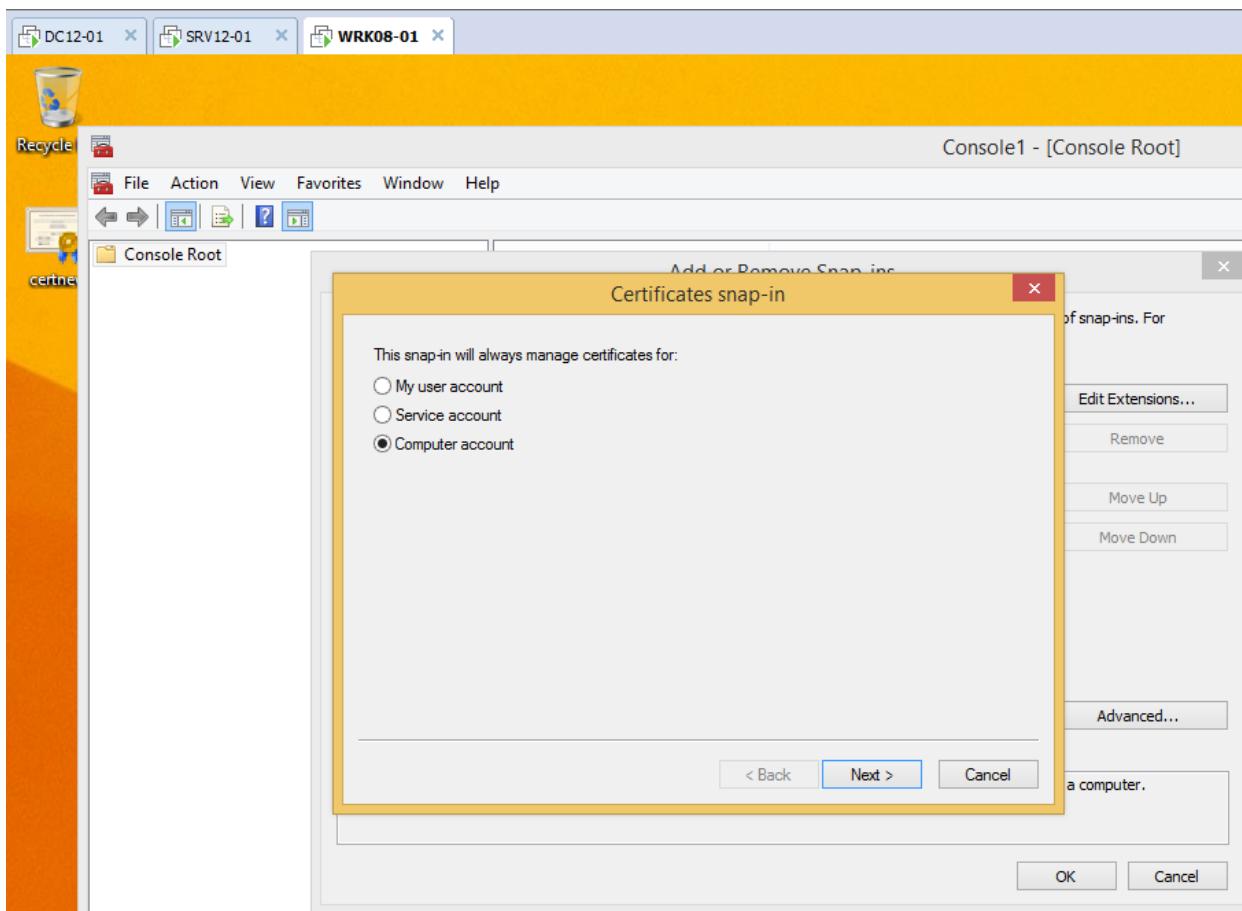
- [Request a certificate](#)
- [View the status of a pending certificate request](#)
- [Download a CA certificate, certificate chain, or CRL](#)

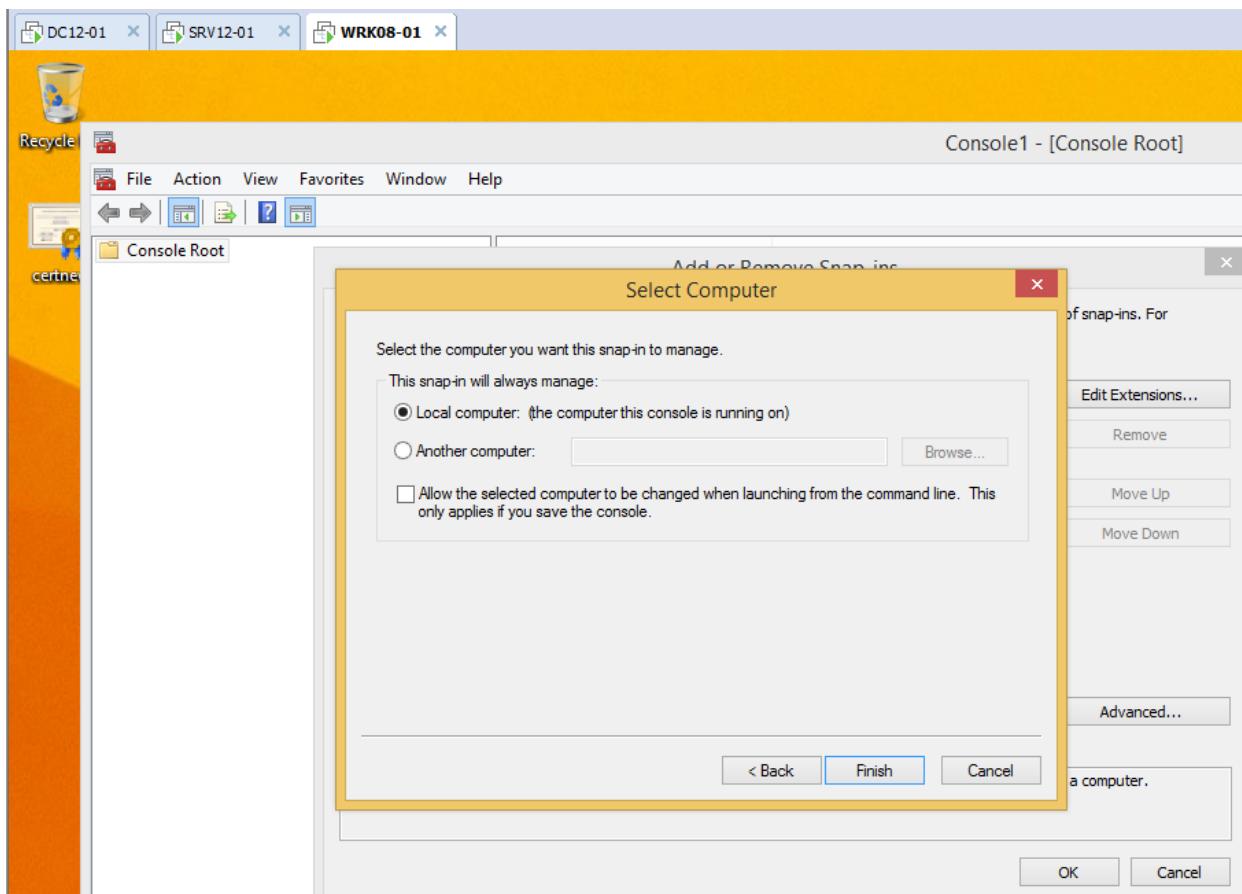
- Trong trang web *Certificate* , tiến hành download CA về máy.



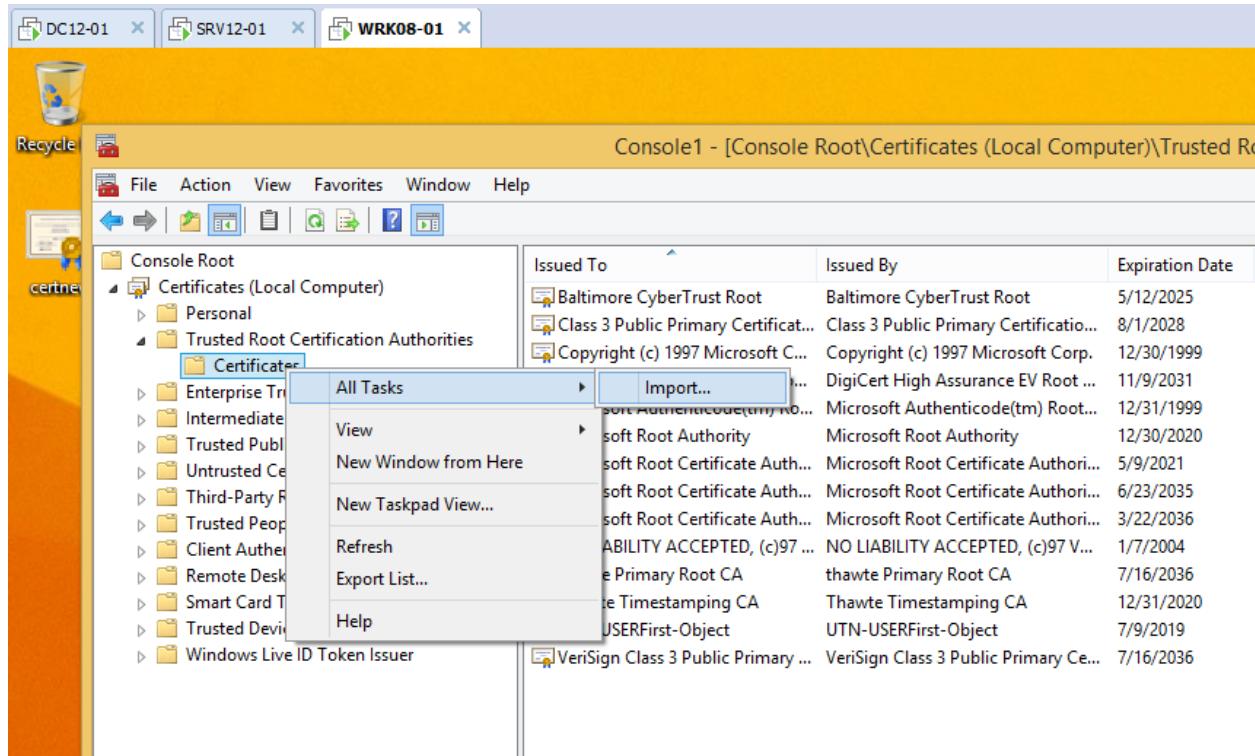
- Thực hiện cấu hình Trust Root CA trên VPN Client.
 - Run / mmc / Add / Remove Snap-ins
 - Trong cửa sổ Add or Remove Snap-ins , chọn Certificates / Add / Computer Account Finish.



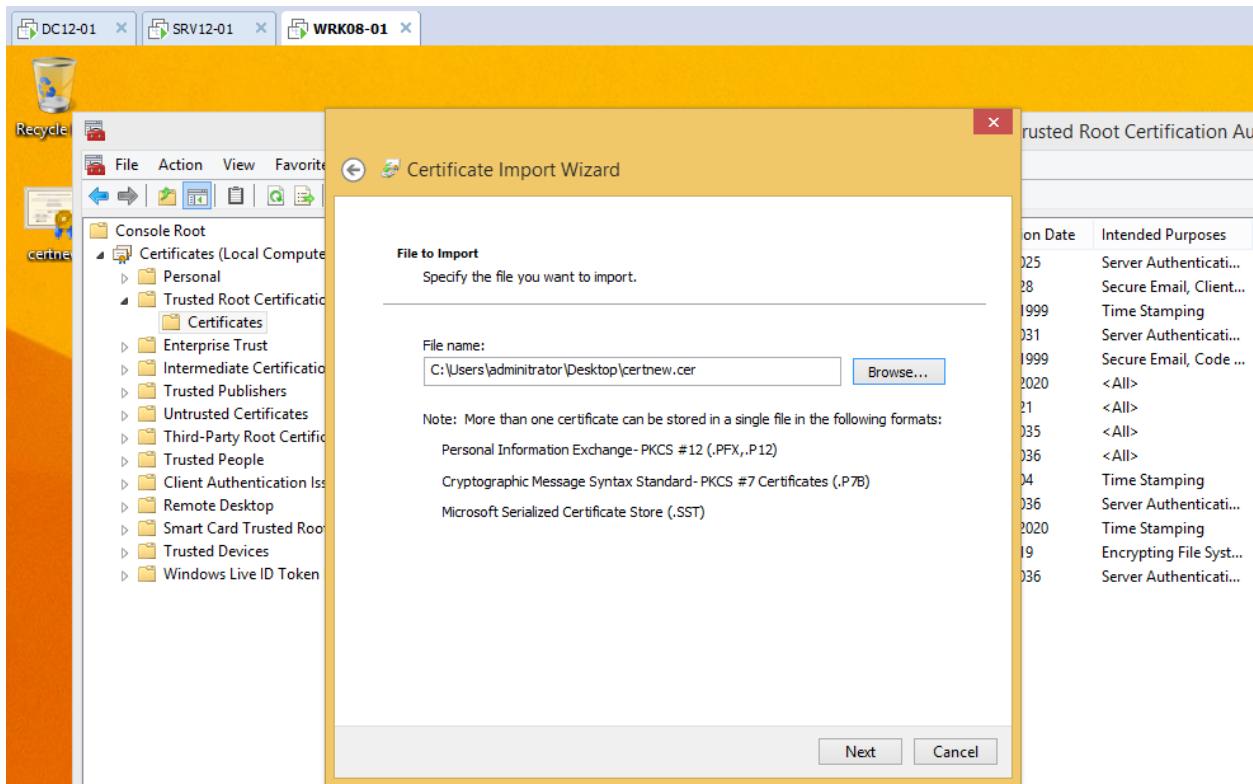




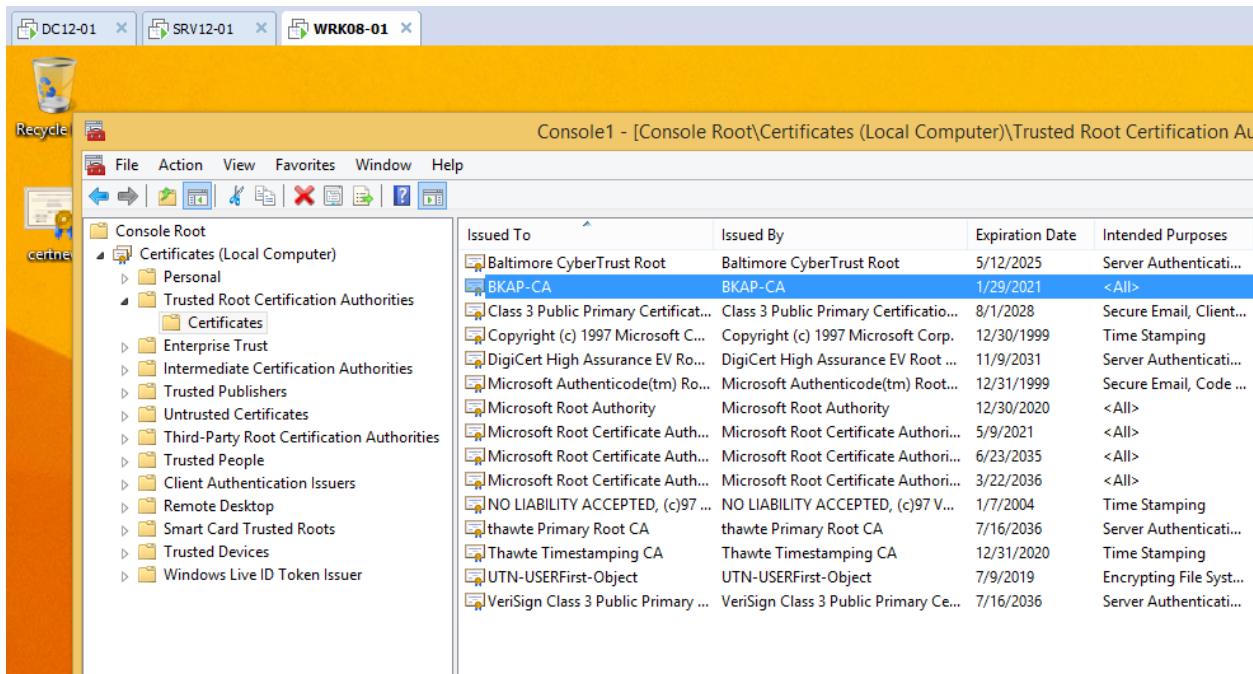
- Chọn vào **Cerficates (Local Computer) / Trust Root Certification Authorities / Certificates** , tại đây , click chuột phải chọn **All Tasks / Import...**



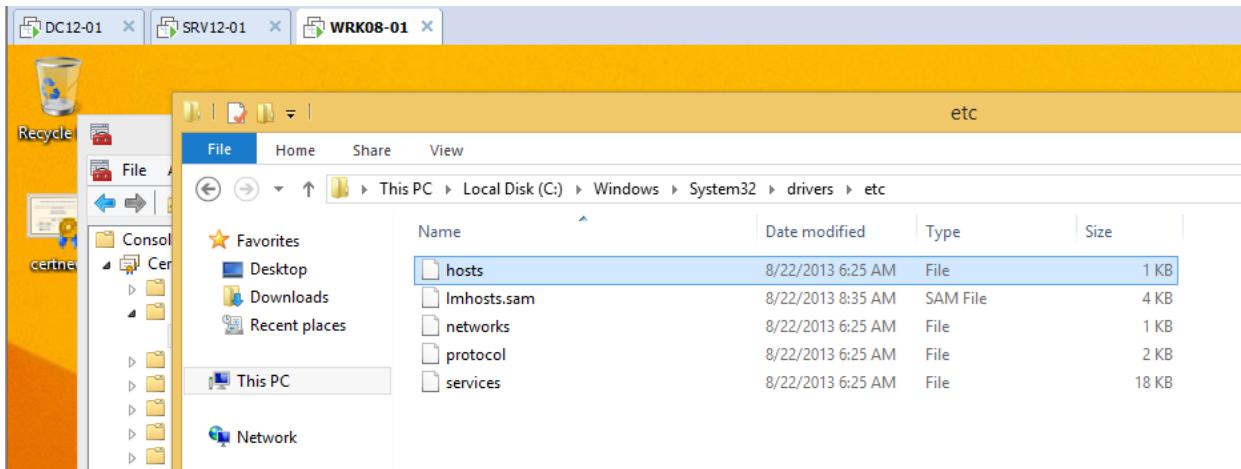
- Tại cửa sổ **File to Import , Browse...** đến file CA vừa download



- Click **Next .. Finish.**



- Vào ô C / Windows / System32 / drivers / etc / hosts.



- Mở file hosts bằng notepad chỉnh sửa như sau:

```

hosts - Notepad

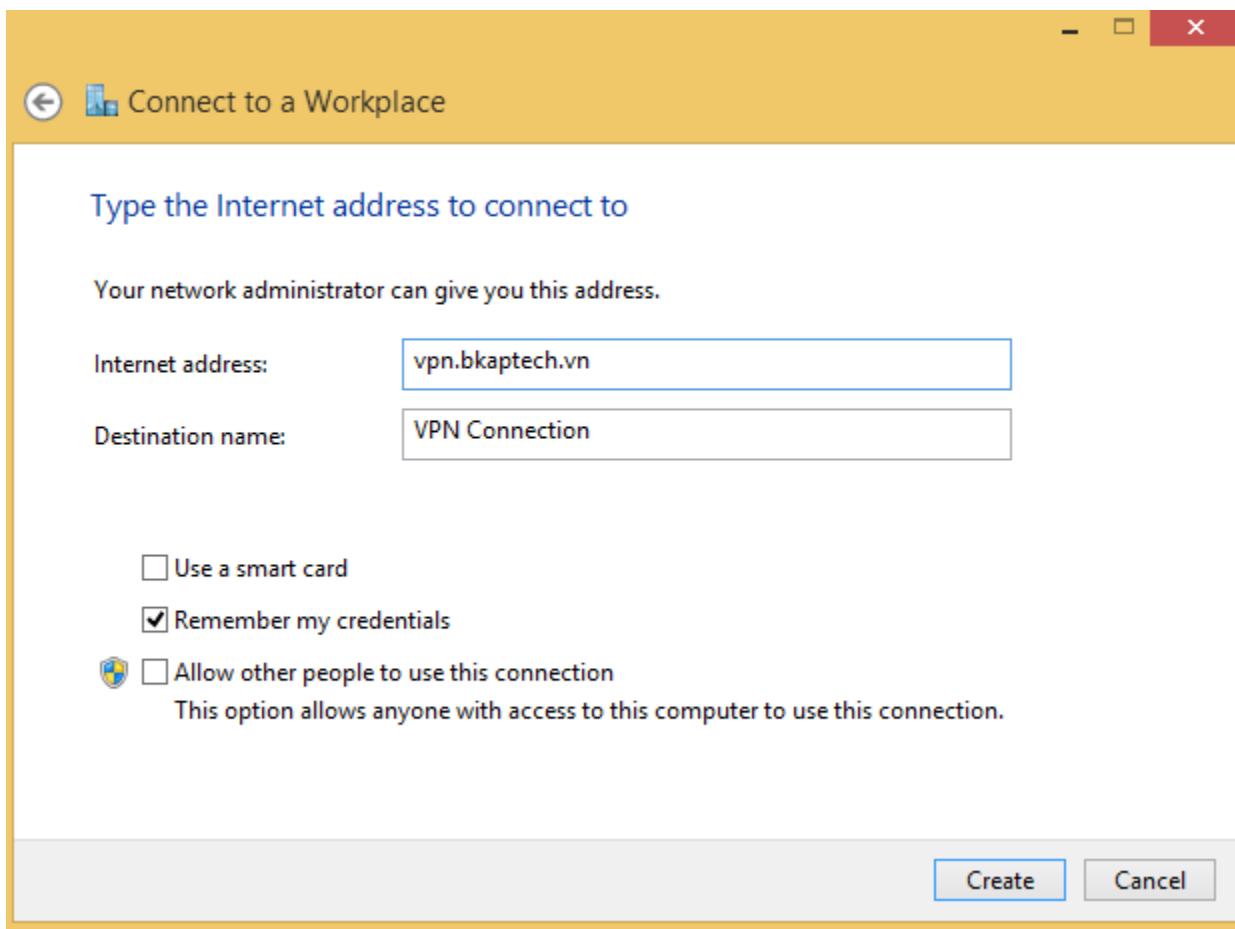
File Edit Format View Help

# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97    rhino.acme.com        # source server
#      38.25.63.10      x.acme.com            # x client host

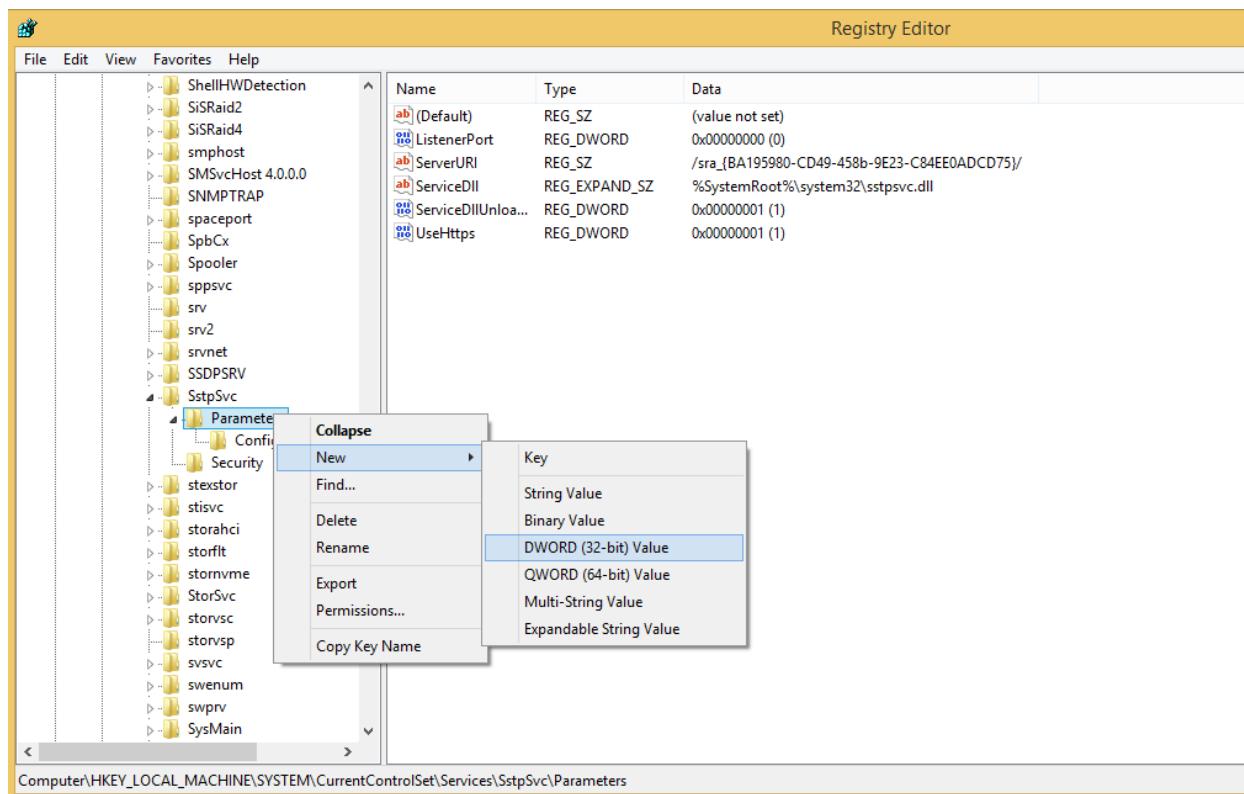
# localhost name resolution is handled within DNS itself.
#      127.0.0.1        localhost
#      ::1              localhost
123.1.1.1      vpn.bkaptech.vn

```

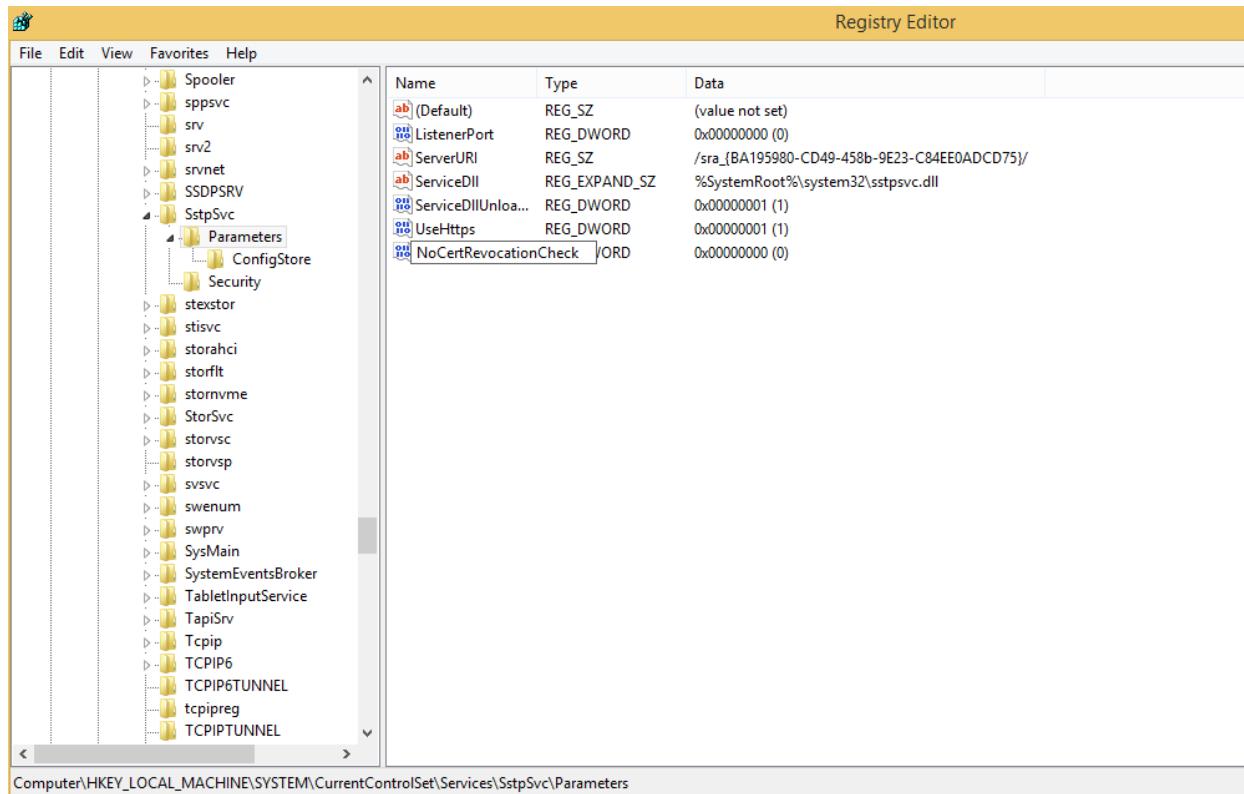
- Thực hiện tạo VPN Client.



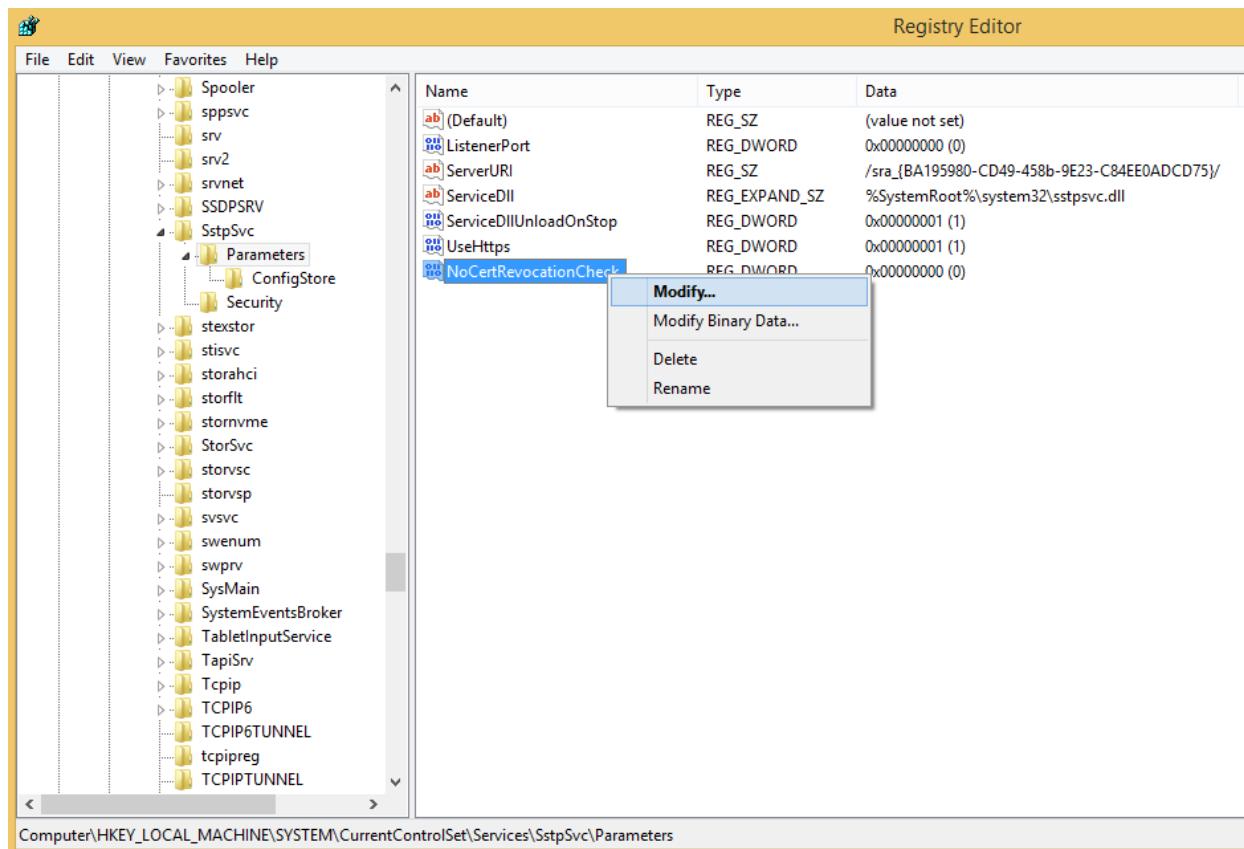
- Chính sửa Registry:
 - Run / regedit
 - Tìm theo đường dẫn:
 - **HKEY_LOCAL_MACHINE / SYSTEM / CurrentControlSet / Services / tìm đến SstpSvc / Parameters.**
 - Click chuột phải tại **Parameters** / New / **DWORD (32-bit) Value**.



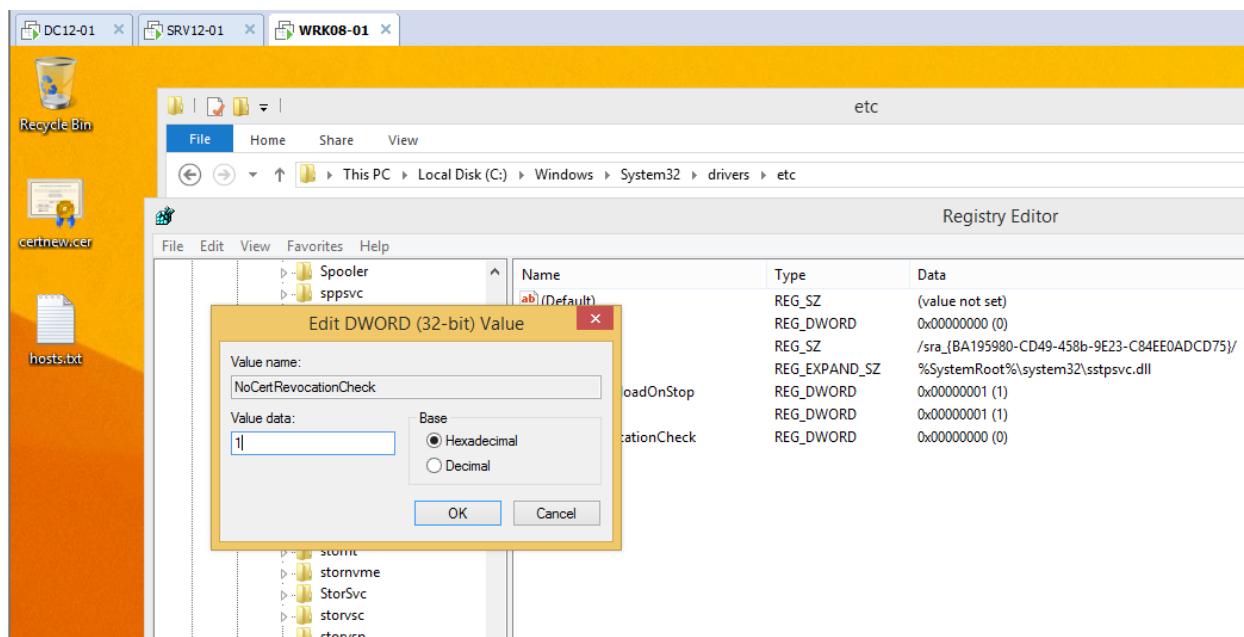
- Đổi tên file thành **NoCertRevocationCheck**.



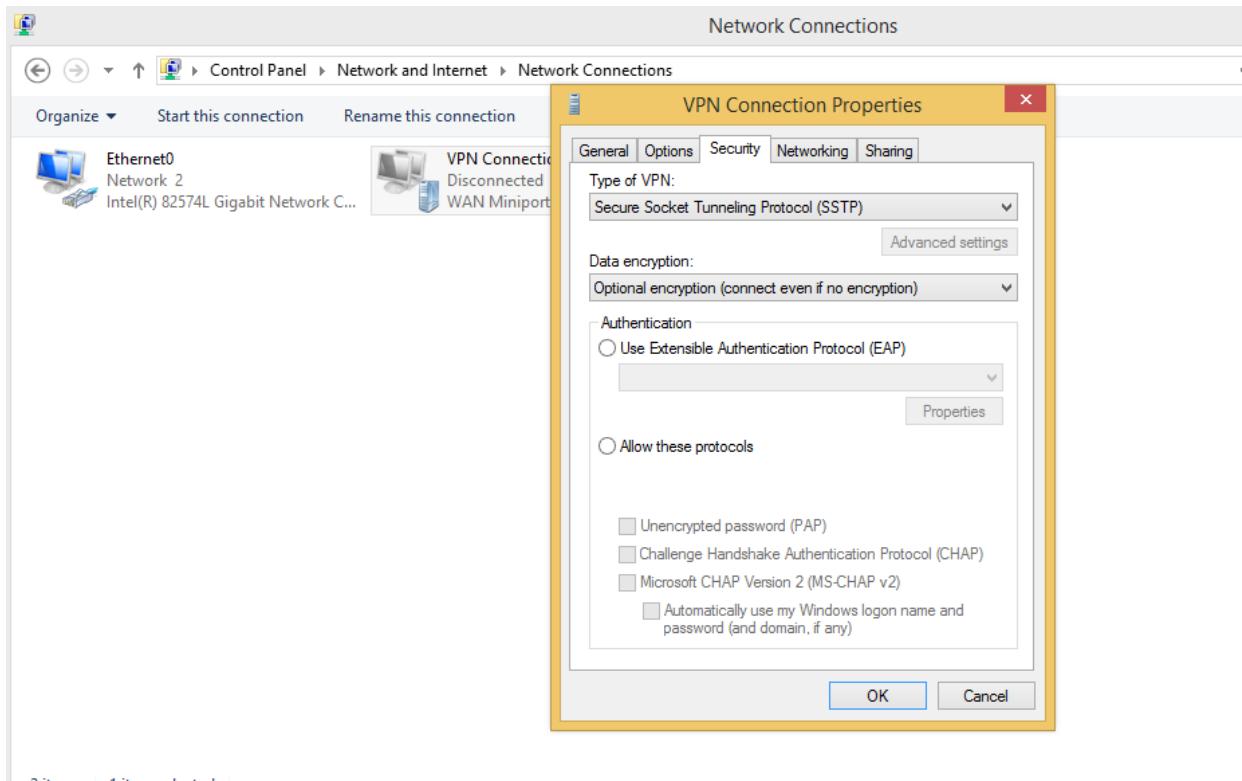
- Click vào File vừa tạo , chọn **Modify...**



- Sửa Value data: 1.

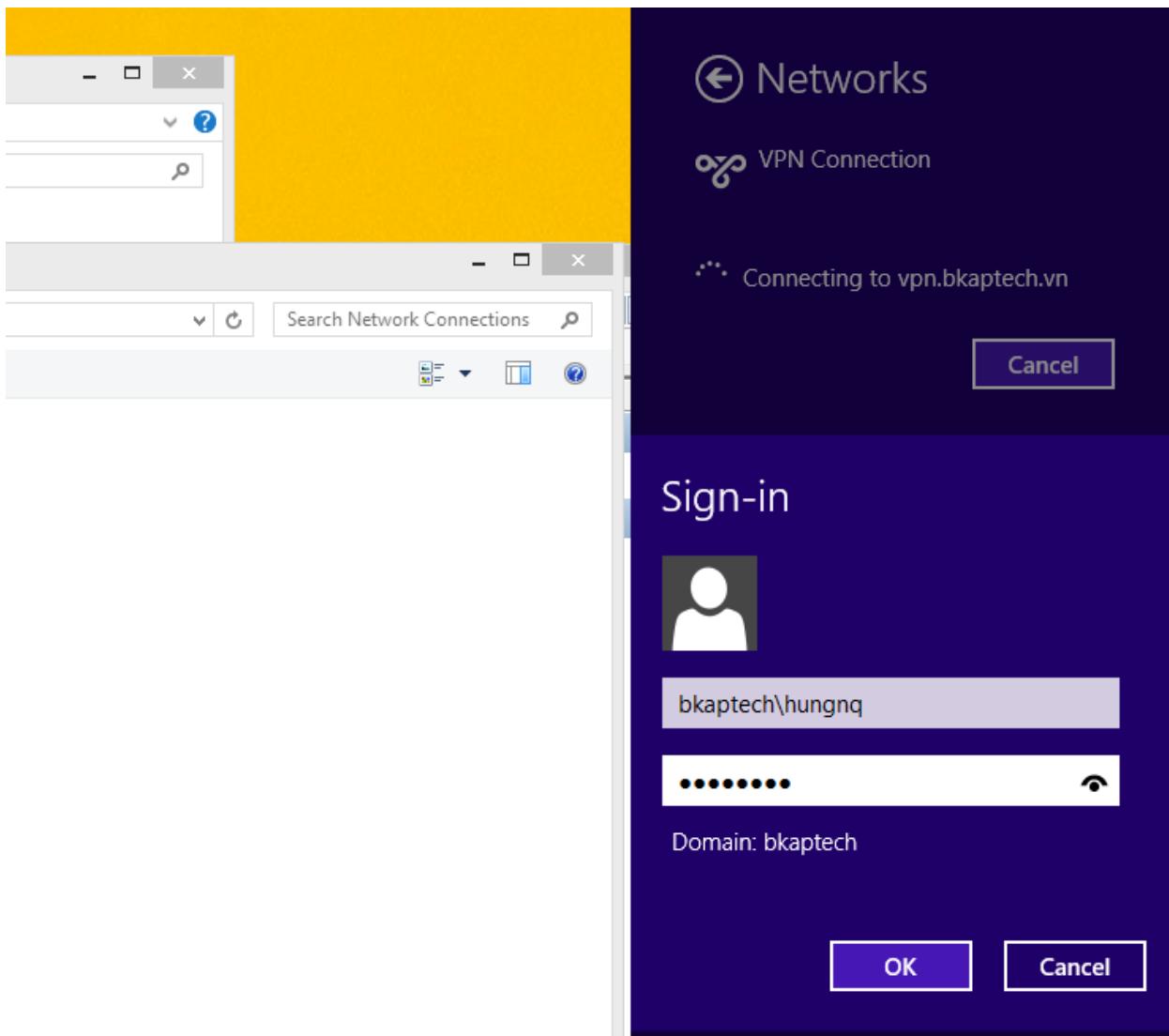


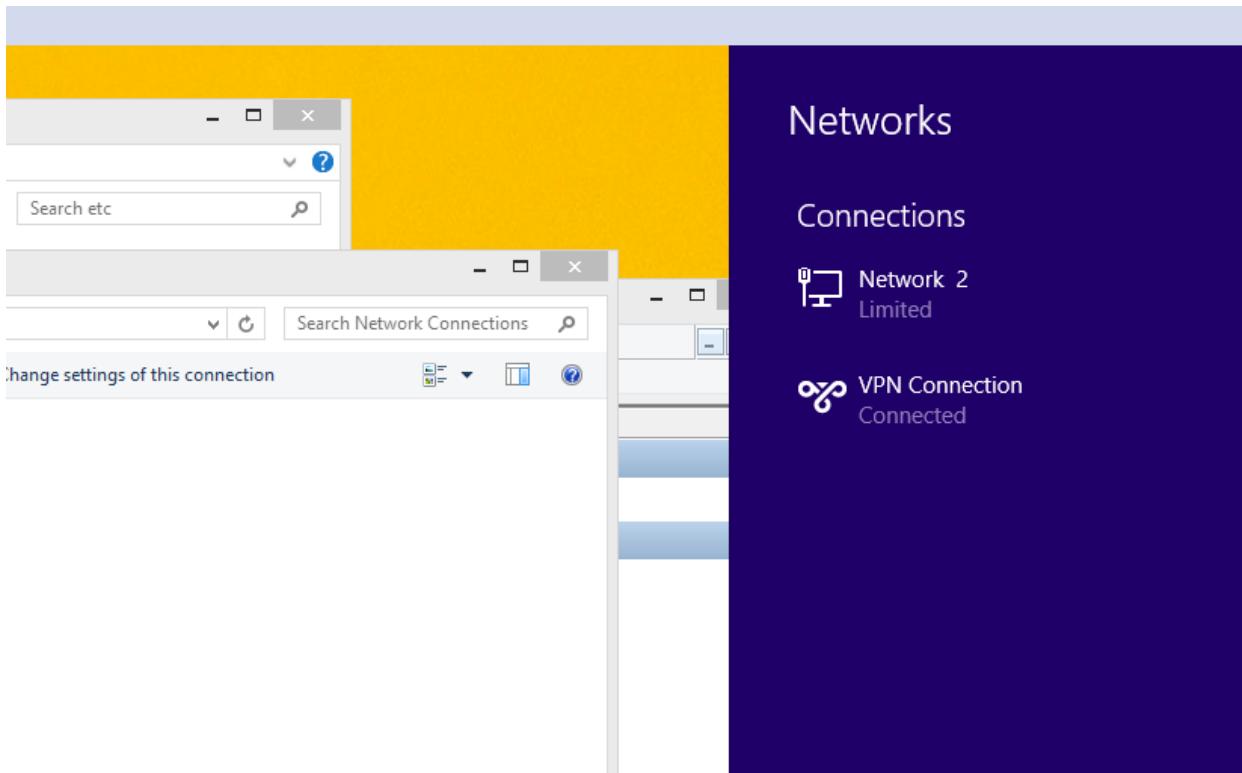
- Vào card mạng VPN, chỉnh sửa type of VPN thành SSTP.



2 items 1 item selected

o Tiến hành Connect.





Bài 8:**TRIỂN KHAI DỊCH VỤ NETWORK POLICY SERVER****Các nội dung chính sẽ được đề cập:**

- ✓ Triển khai cài đặt và cấu hình dịch vụ VPN Server kết hợp với RADIUS.
- ✓ Triển khai cài đặt và cấu hình dịch vụ VPN Server kết hợp với NPS.
- ✓ Triển khai cài đặt và cấu hình dịch vụ VPN Server kết hợp với RADIUS và NPS.

8.1 Triển khai cài đặt và cấu hình dịch vụ VPN Server kết hợp với RADIUS.**1. Yêu cầu bài lab:**+ Trên máy *BKAP-DC12-01*:

- Tạo OU, Group, tài khoản người dùng và cho phép truy cập từ xa.
- Tạo 1 Folder chia sẻ với tên **Data**.

+ Trên máy *BKAP-SRV12-01* :

- Cài đặt dịch vụ **RADIUS Server**, thiết lập **Radius Client**.

+ Trên máy *BKAP-SRV12-02* :

- Cài đặt dịch vụ **Remote Access**.
- Cấu hình **VPN Server** cho **Remote Client** với giao thức **PPTP, VPN** Server cấp dải địa chỉ cho Client truy cập vào là *10.0.0.10 – 10.0.0.50*.

+ Trên máy *BKAP-WRK08-01*:

- Tạo **VPN Client** và kết nối.
- Thực hiện ping thông và truy cập dữ liệu tới máy *BKAP-DC12-01* thông qua **VPN** vừa thiết lập.

2. Yêu cầu chuẩn bị:

Chuẩn bị 4 máy ảo :

- *BKAP-DC12-01* : đã nâng cấp lên Domain Controller quản lý miền *bkaptech.vn*.
- *BKAP-SRV12-01* : cài đặt Radius Server.

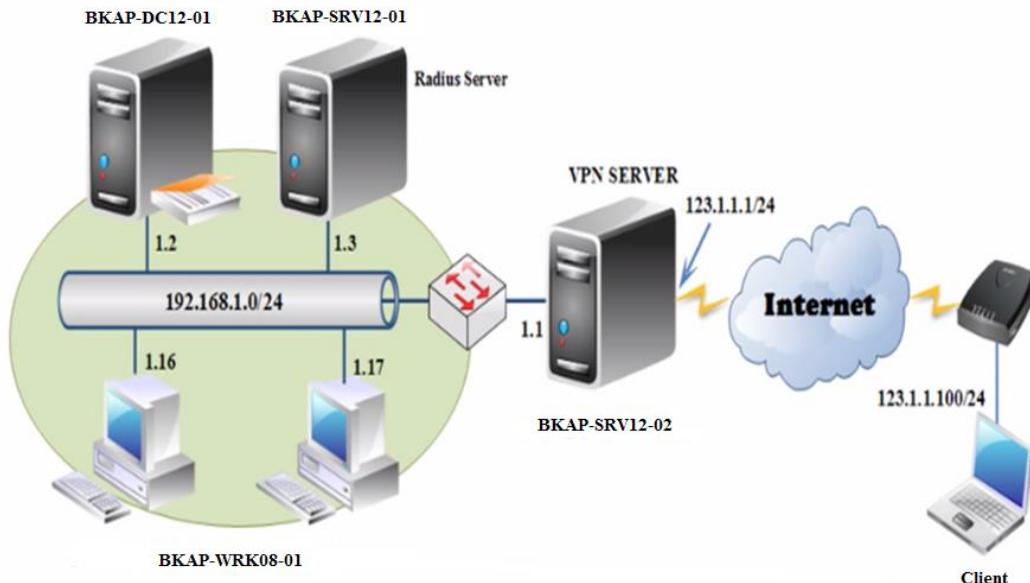
- *BKAP-SRV12-02* : làm **VPN Server** có 2 card mạng : card mạng 1 ứng với **VMnet2** , card mạng 2 ứng với **VMnet3**.
- *BKAP-WRK08-01* : ping thông tin tới máy *BKAP-SRV12-02* với địa chỉ IP của card mạng 2.

3. Mô hình lab:

HỆ THỐNG ĐÀO TẠO CNTT QUỐC TẾ BACHKHOA-APTECH

Lab 8.1 Cấu hình dịch vụ **VPN Server** kết hợp với **RADIUS**

BACHKHOA
EDUCATION / APTECH



Hình 8.1

Sơ đồ địa chỉ như sau:

Thông số	DC12-01	SRV12-01	SRV12-02	WRK08-01
IP address	192.168.1.2	192.168.1.3	NIC1:192.168.1.1 NIC2:123.1.1.1	123.1.1.100
Subnet Mask	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
Gateway	192.168.1.1	192.168.1.1	--	123.1.1.1
DNS Server	192.168.1.2	192.168.1.2	--	--

Hướng dẫn chi tiết :

- Kết nối các máy ảo theo mô hình trên. Thực hiện **ping** thông giữa các máy kết nối trực tiếp.

```

Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
Control-C
^C
C:\Users\Administrator>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.3:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
Control-C

```

```

Administrator: C:\Windows\system32\cmd.exe
C:\Users\Administrator>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128

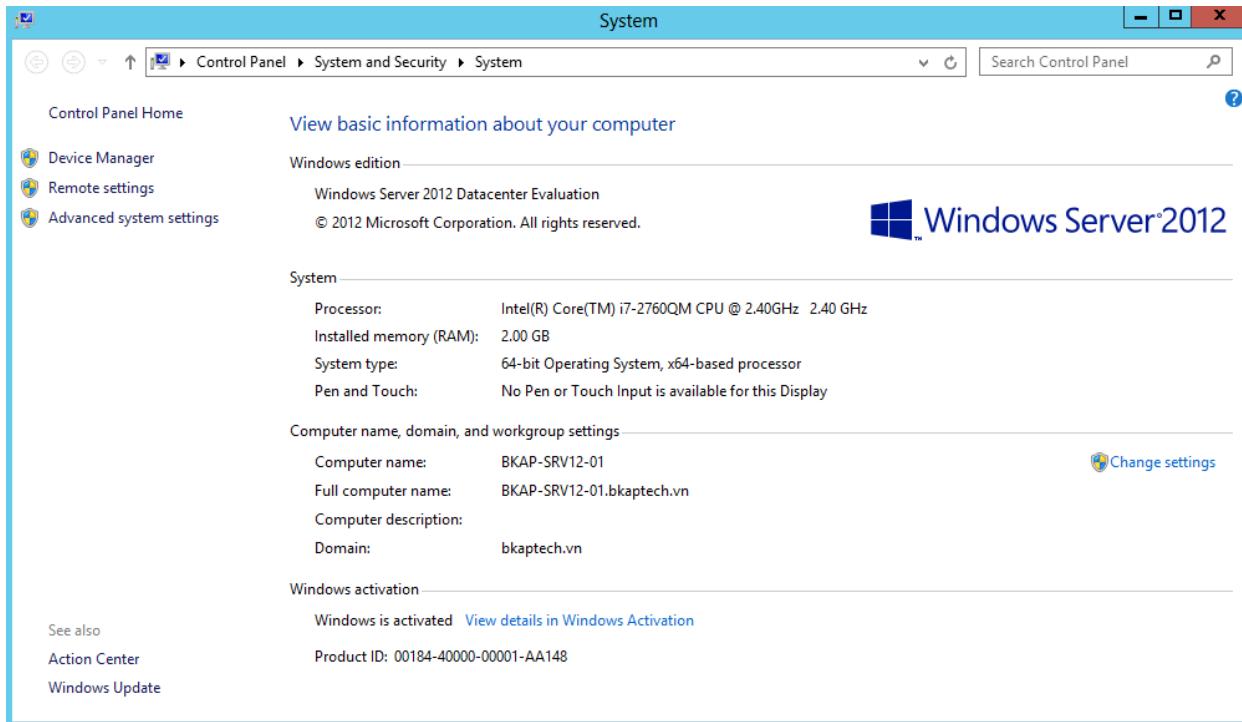
Ping statistics for 192.168.1.3:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
Control-C
^C
C:\Users\Administrator>ping 123.1.1.100

Pinging 123.1.1.100 with 32 bytes of data:
Reply from 123.1.1.100: bytes=32 time<1ms TTL=128

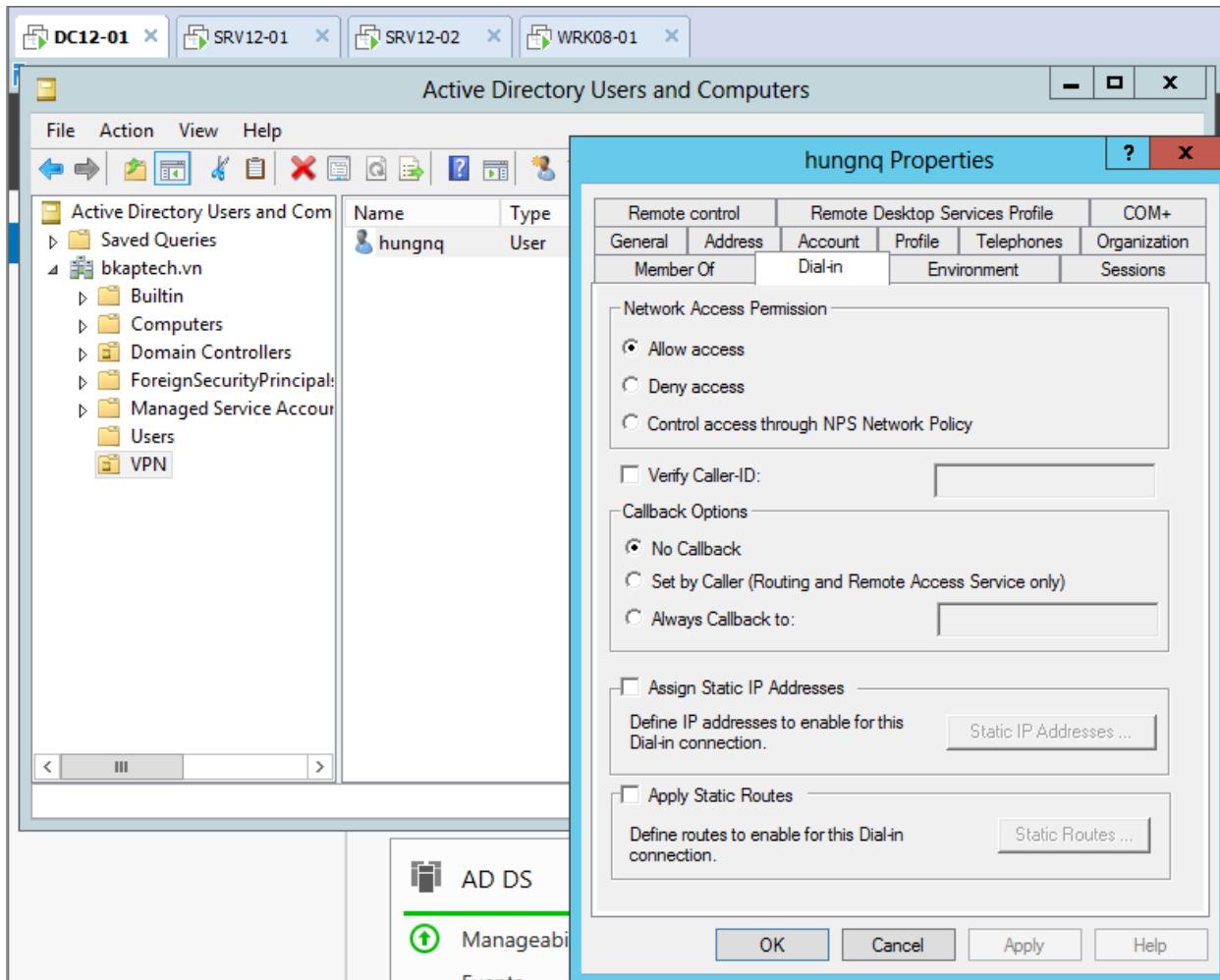
Ping statistics for 123.1.1.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
Control-C

```

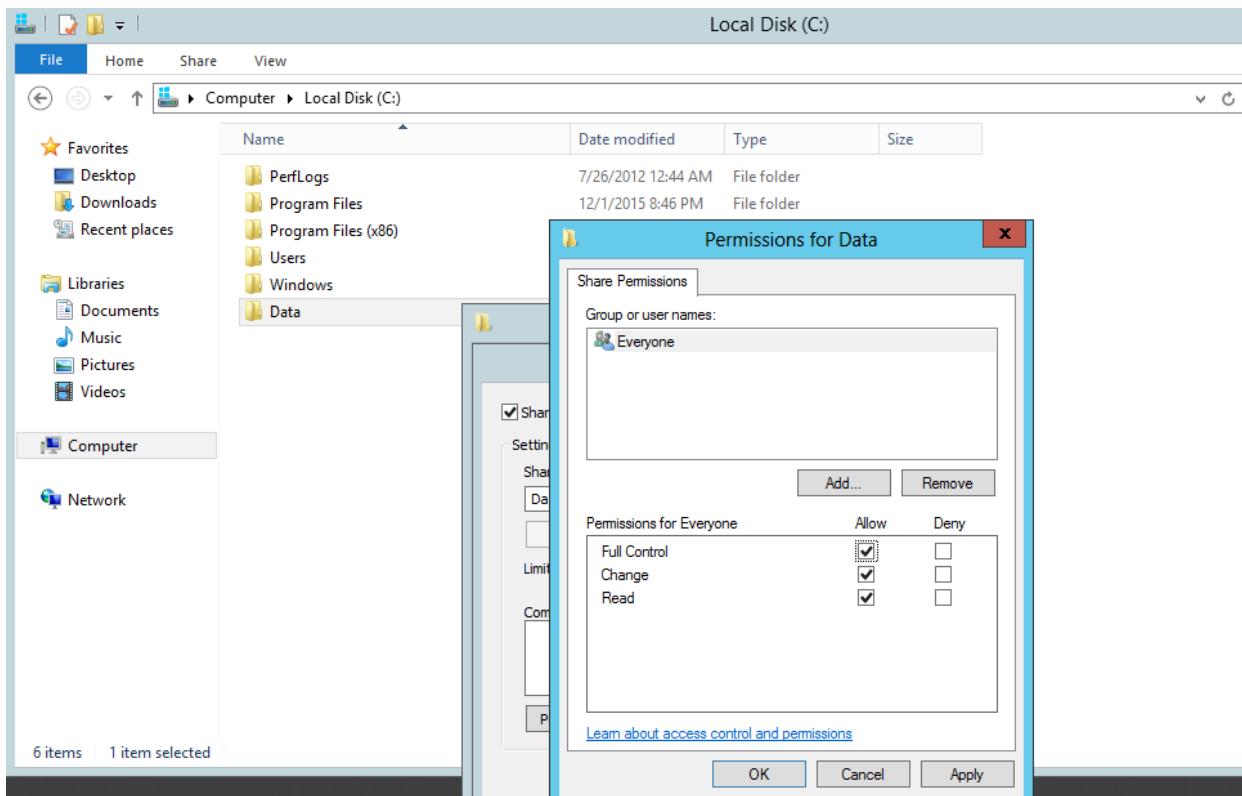
- Chuyển qua máy BKAP-SRV12-01, thực hiện *Join* vào miền **bkaptech.vn**.
 - Đăng nhập bằng tài khoản trong miền *bkaptech\administrator*.



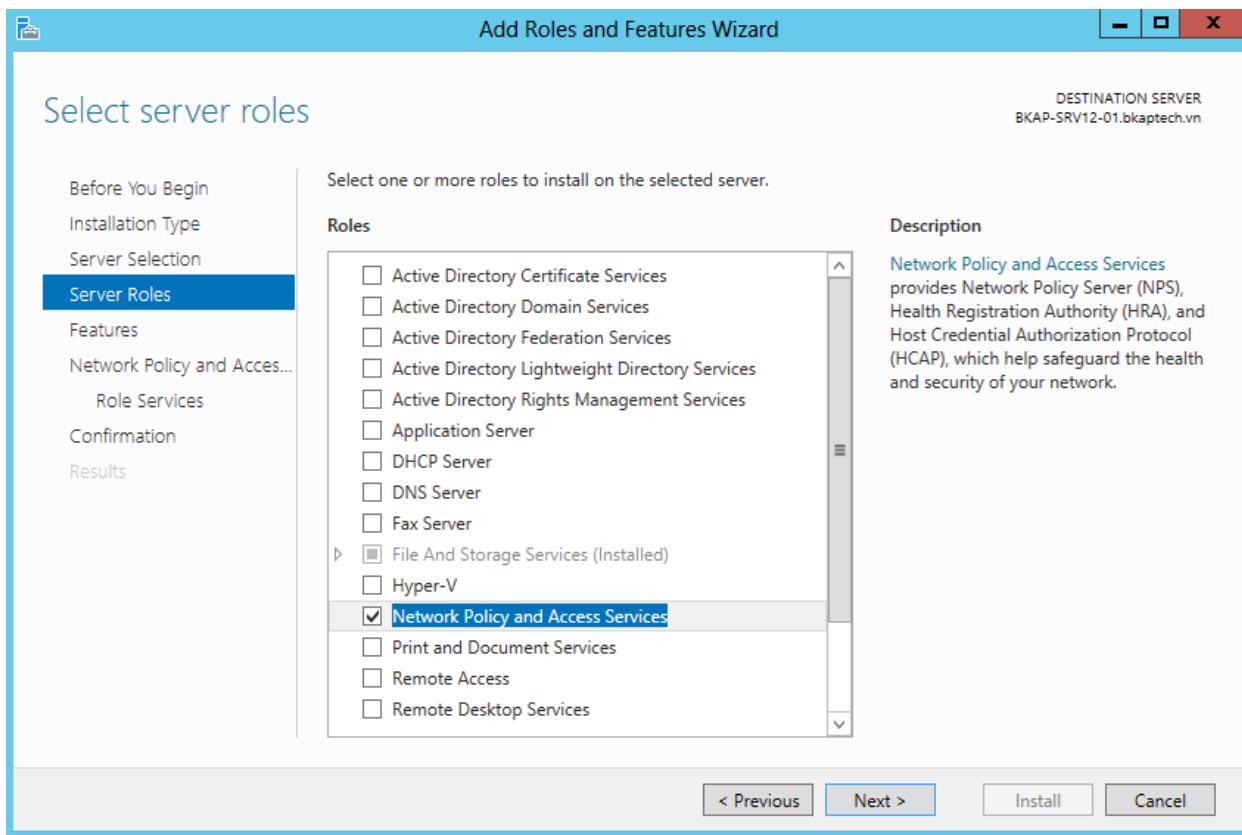
- Chuyển sang máy Server *BKAP-DC12-01* thực hiện tạo 1 *OU*, tài khoản người dùng và cho phép truy cập từ xa :



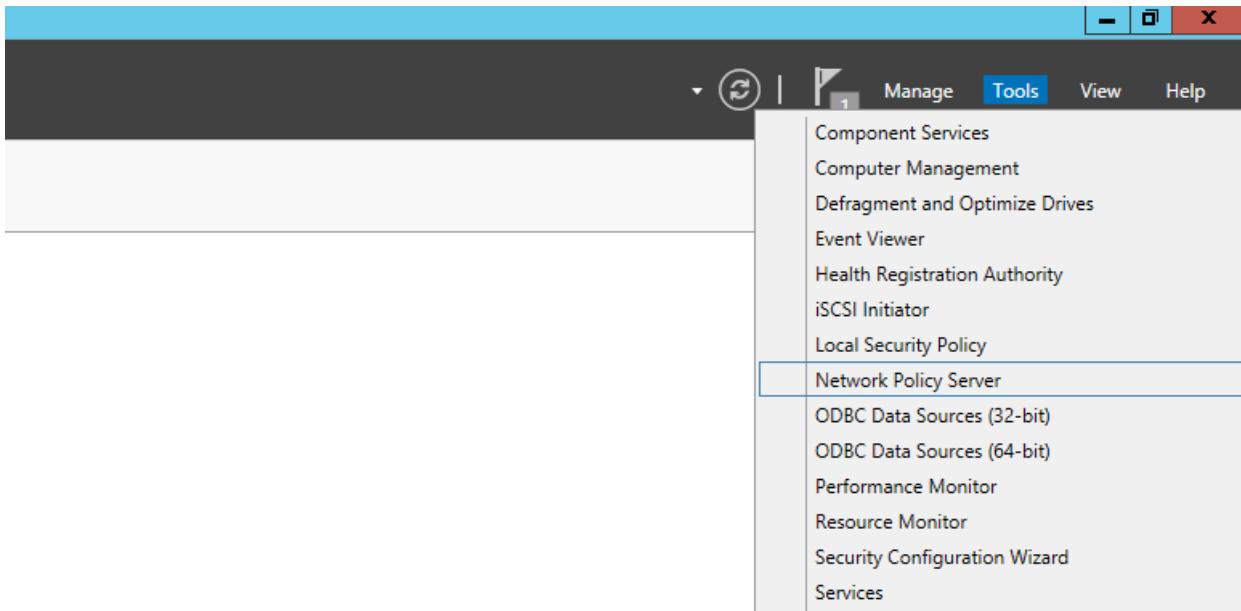
- Tạo 1 thư mục tên **Data**, chia sẻ thư mục này.



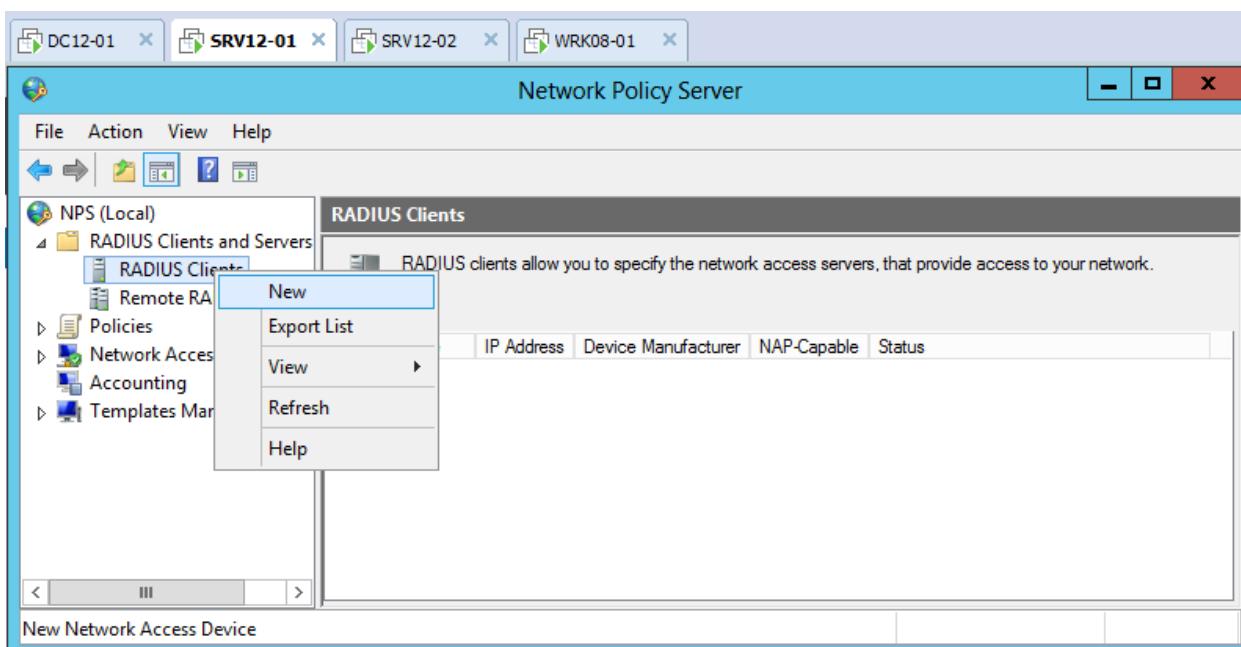
- Chuyển sang máy **BKAP-SRV12-01**, thực hiện cài đặt dịch vụ **RADIUS Server**.
 - Server Manager / Add roles and features /**
 - Tại **Select server roles**, chọn vào **Network Policy and Access Services**.
 - Next ... Install.**



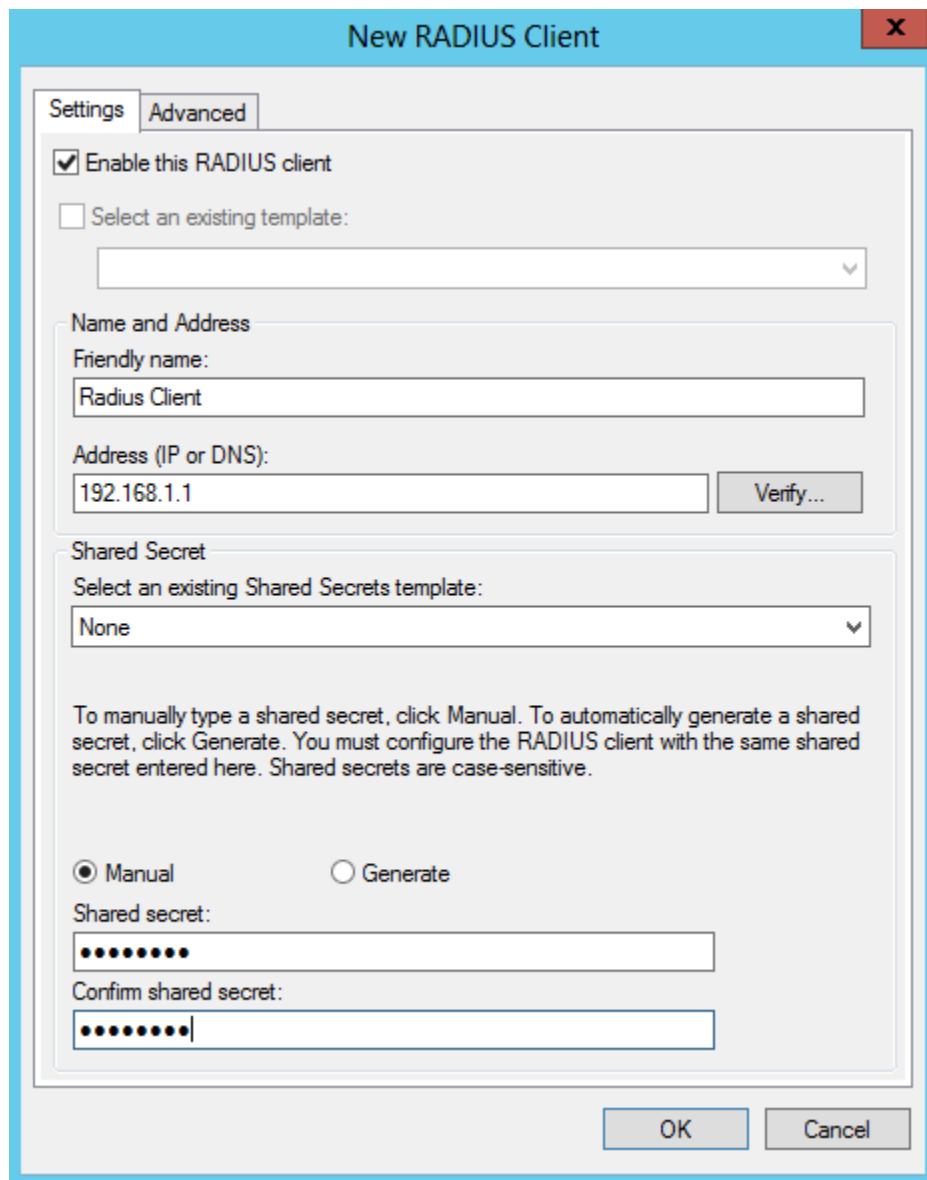
- Thiết lập Radius Client :
 - Tools / Network Policy Server



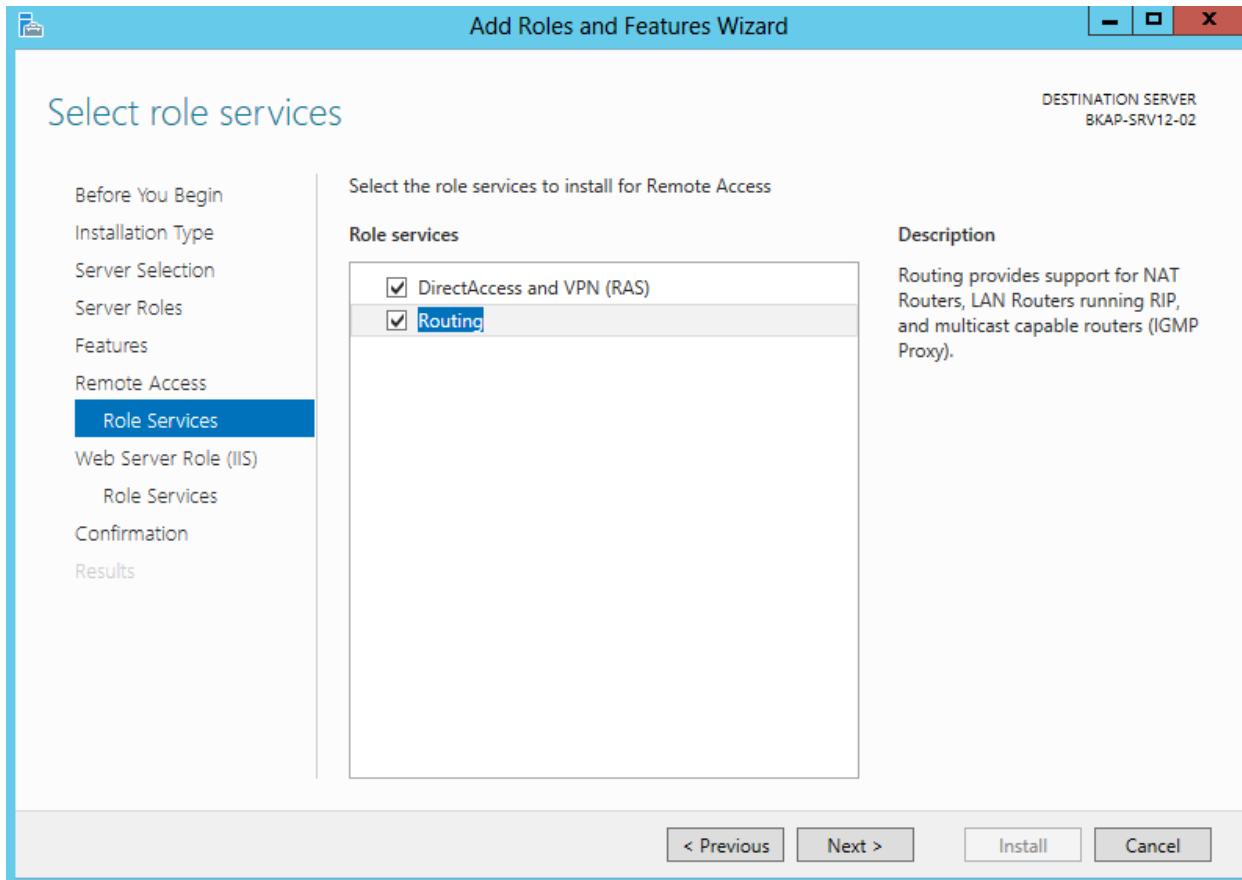
- Tại cửa sổ Network policy Server, chọn vào RADIUS Client and Servers / RADIUS Client.
- Click chuột phải tại RADIUS Client , chọn New.



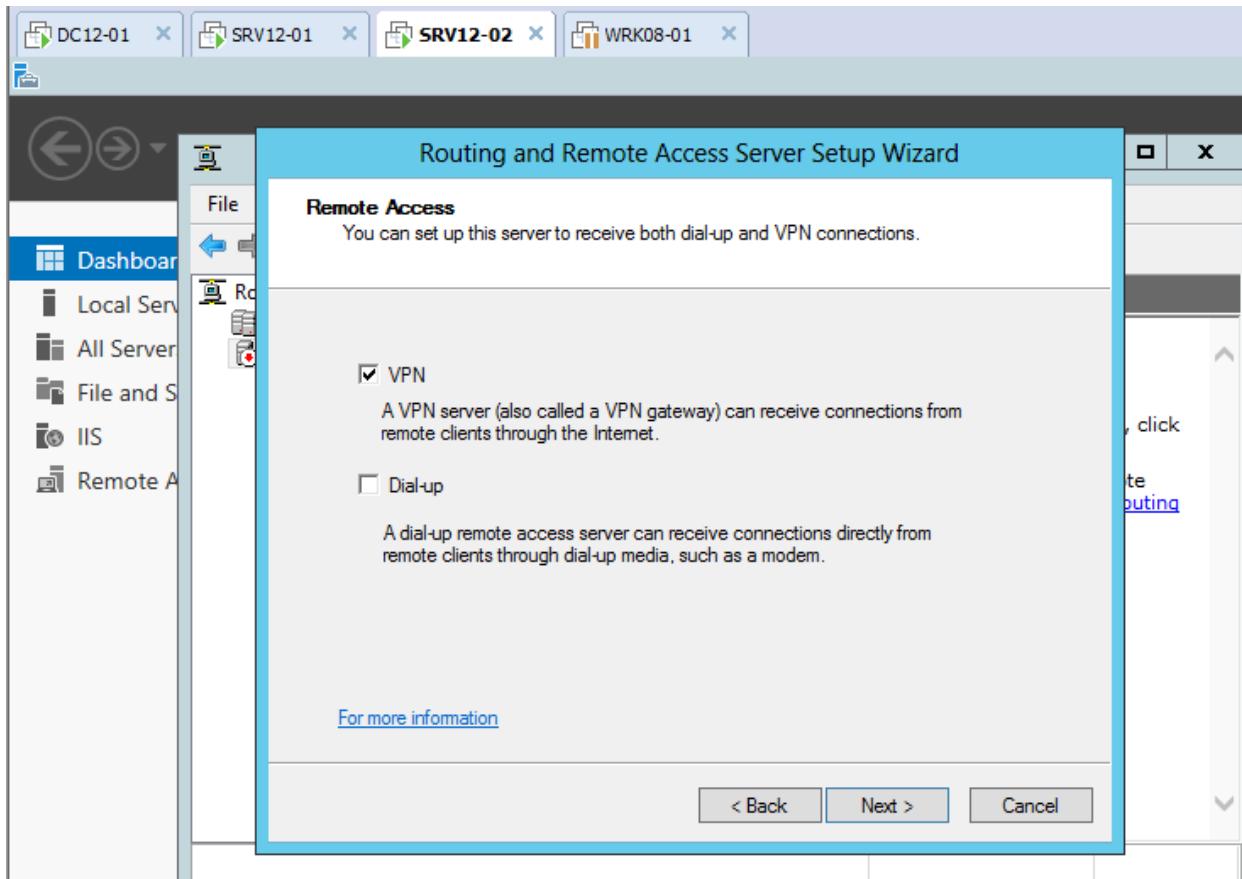
- Tại cửa sổ **New RADIUS Client**, nhập vào các thông số :
 - *Friendly name:* Radius Client
 - *Address (IP or DNS):* 192.168.1.1
 - Nhập mật khẩu **Shared secret:** (123456a@)

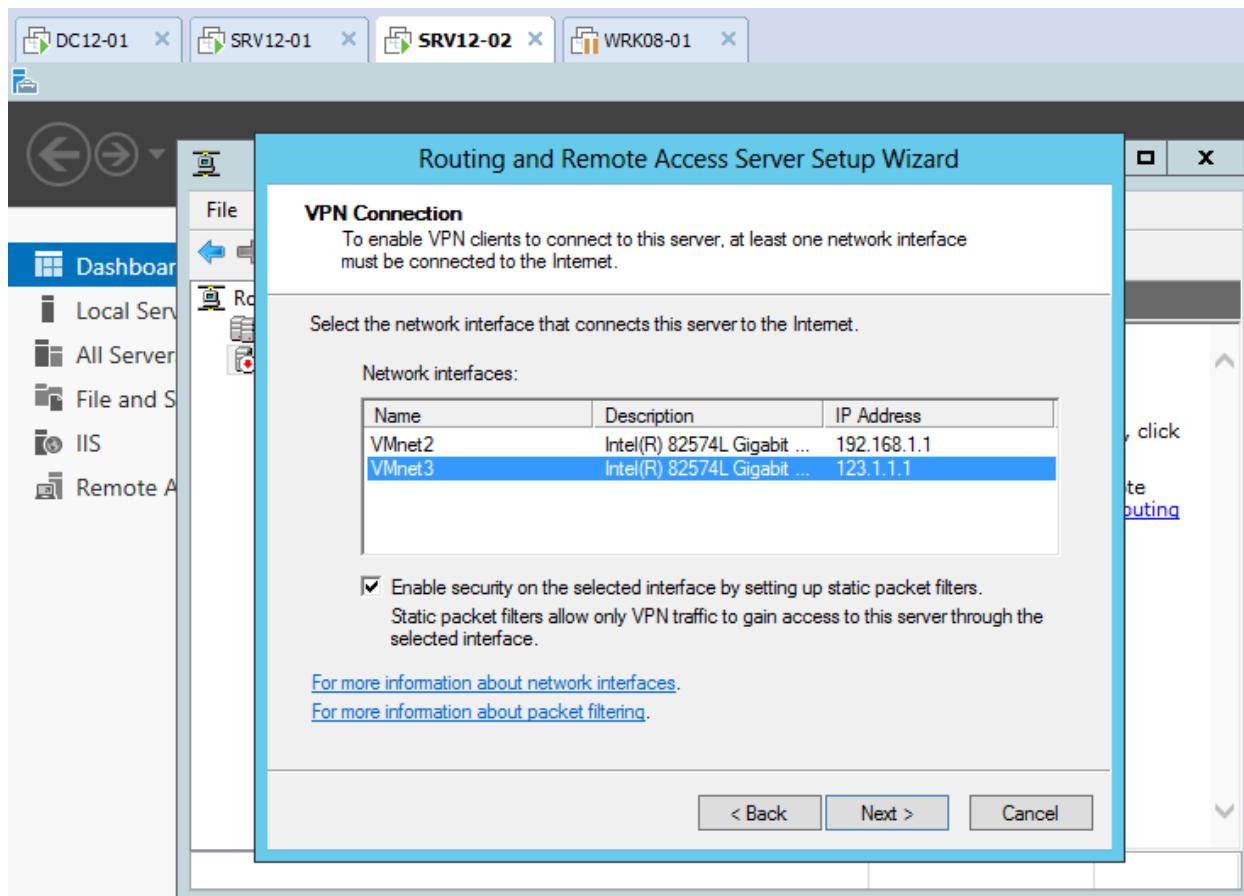


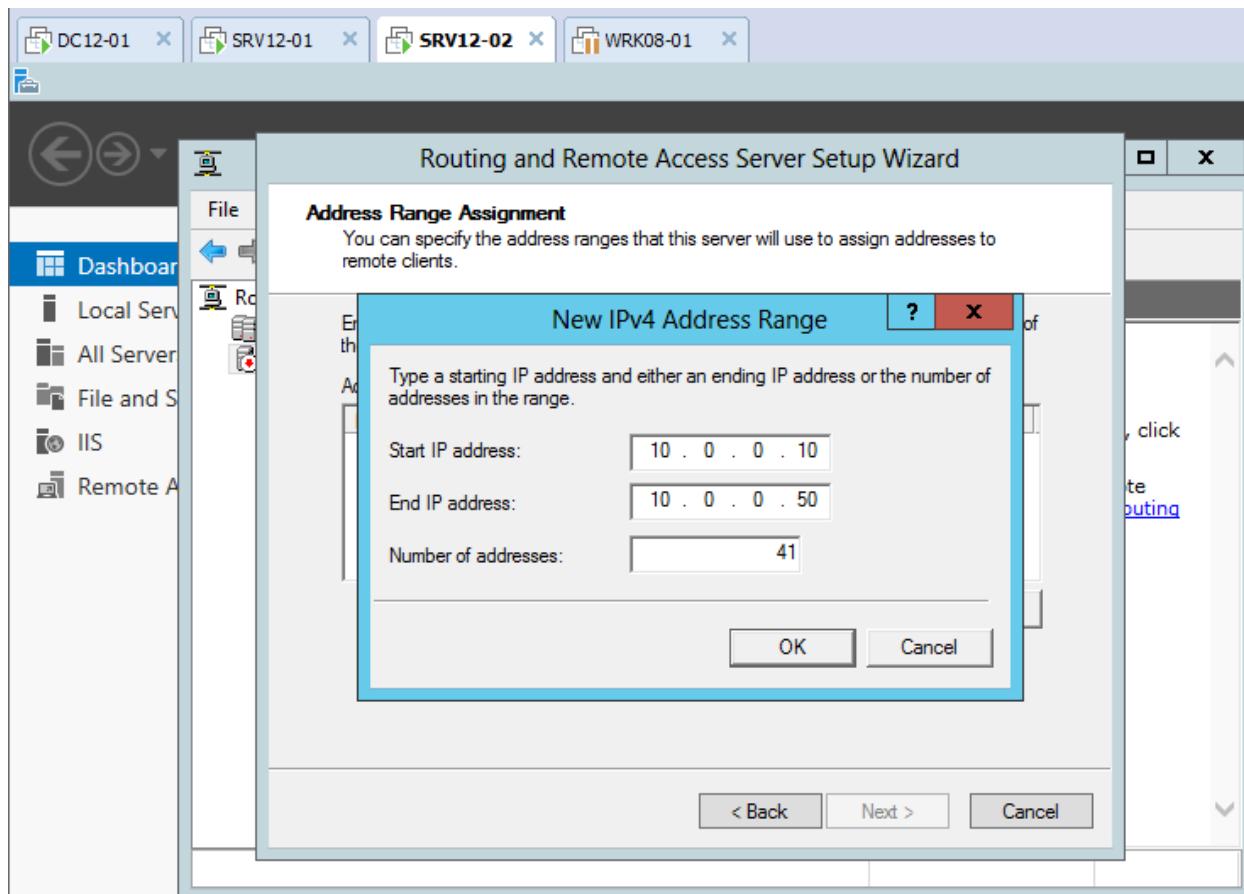
- Chuyển sang máy server *BKAP-SRV12-02*, thực hiện cài đặt dịch vụ **VPN Server (Remote Access /Routing)**.



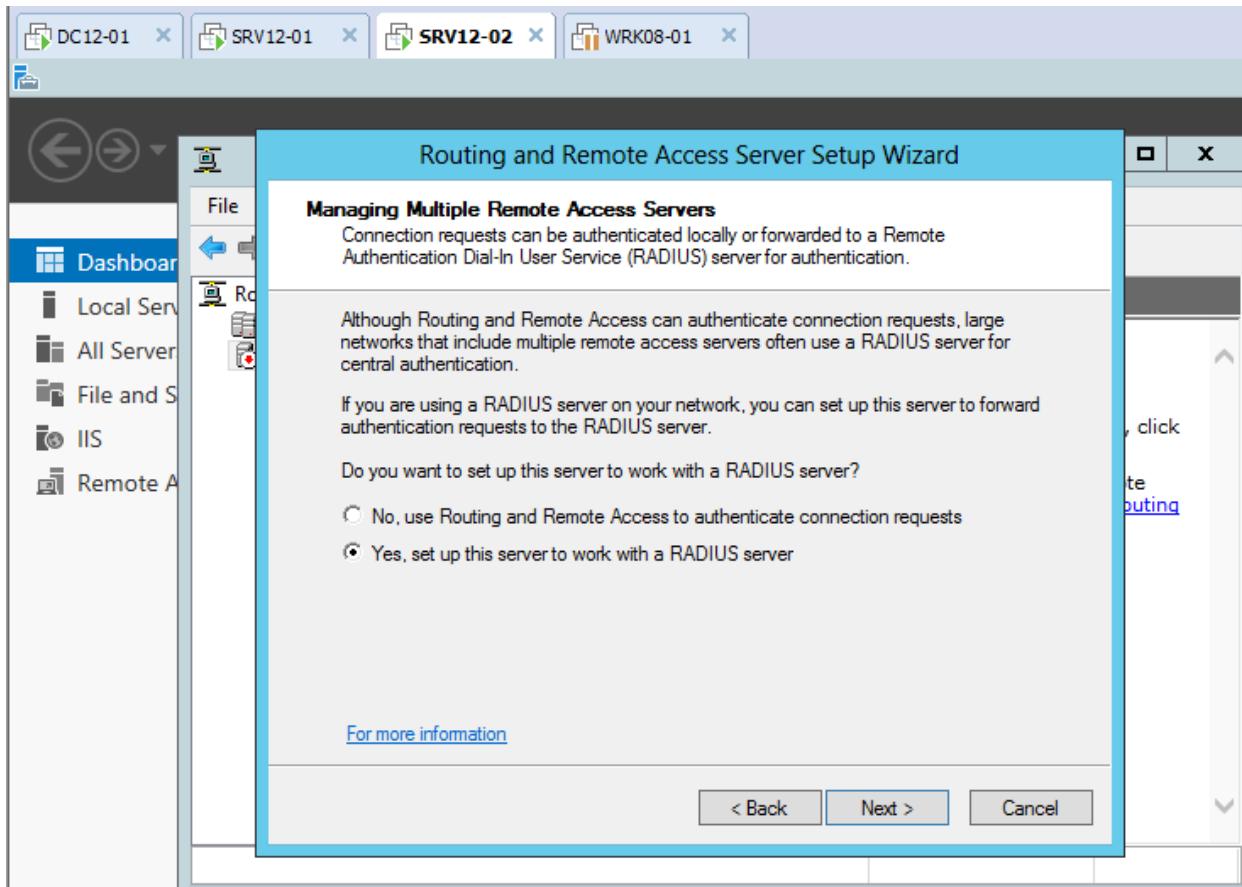
- Cấu hình VPN Server cho Remote Client với giao thức PPTP.



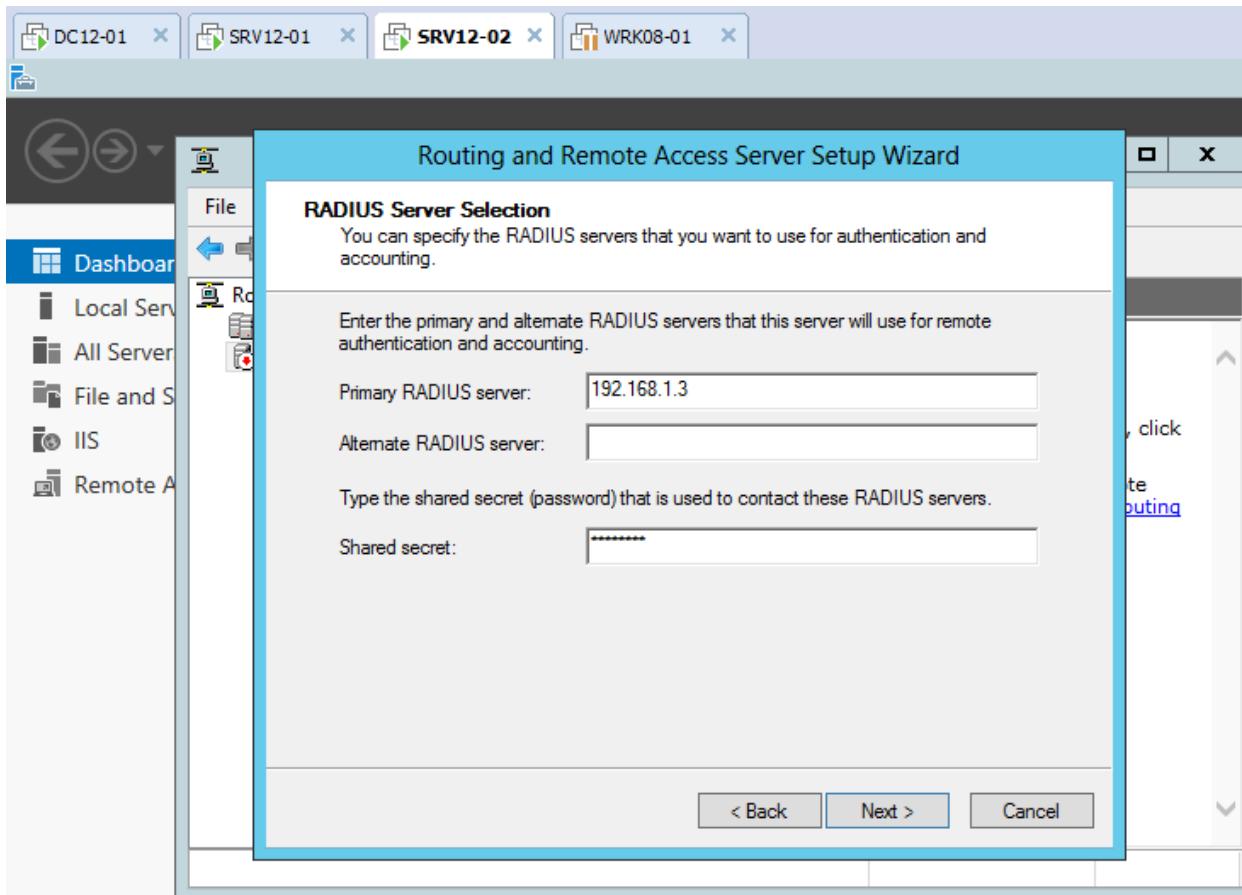


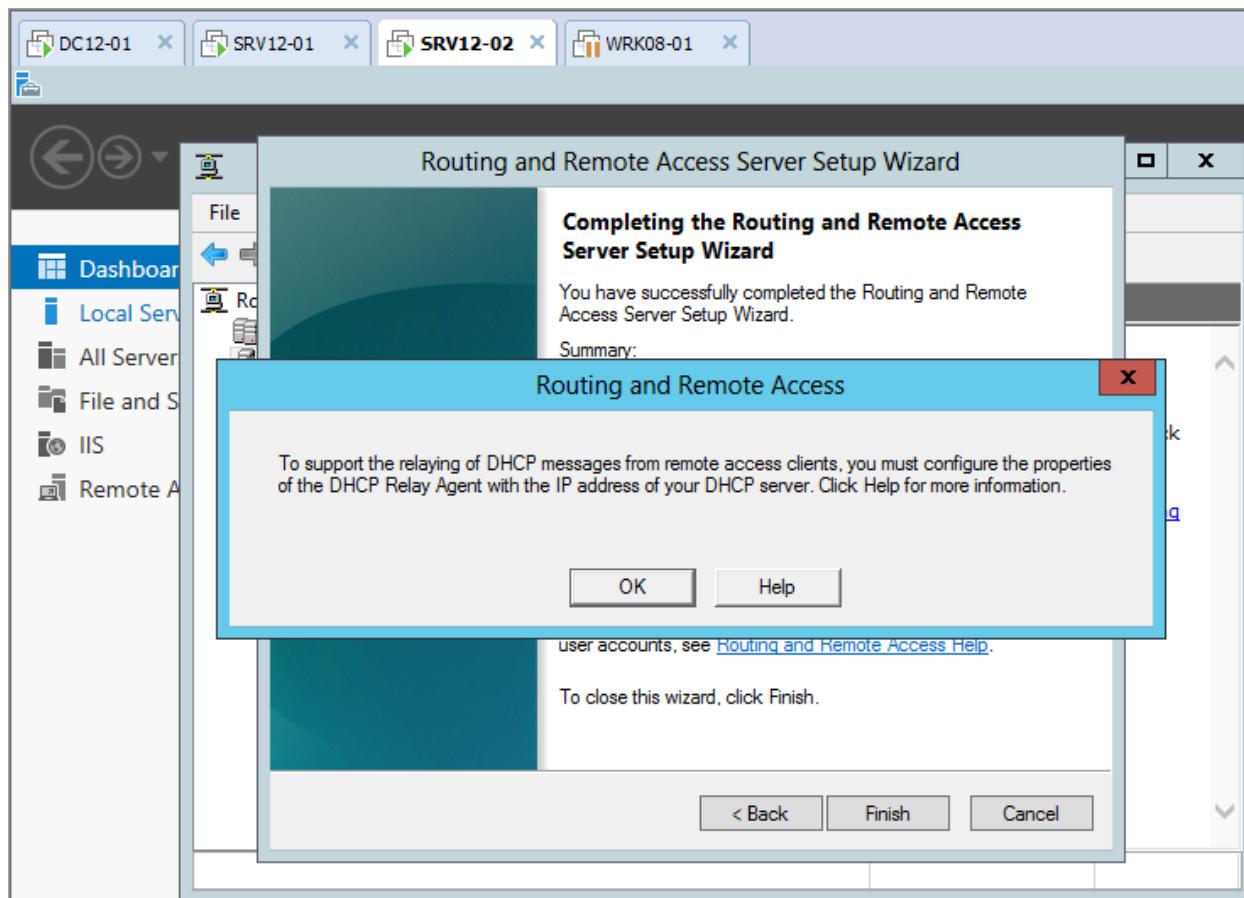


- Tại **Managing Multiple Remote Access Servers**, chọn **Yes , set up this server to work with a RADIUS server.**



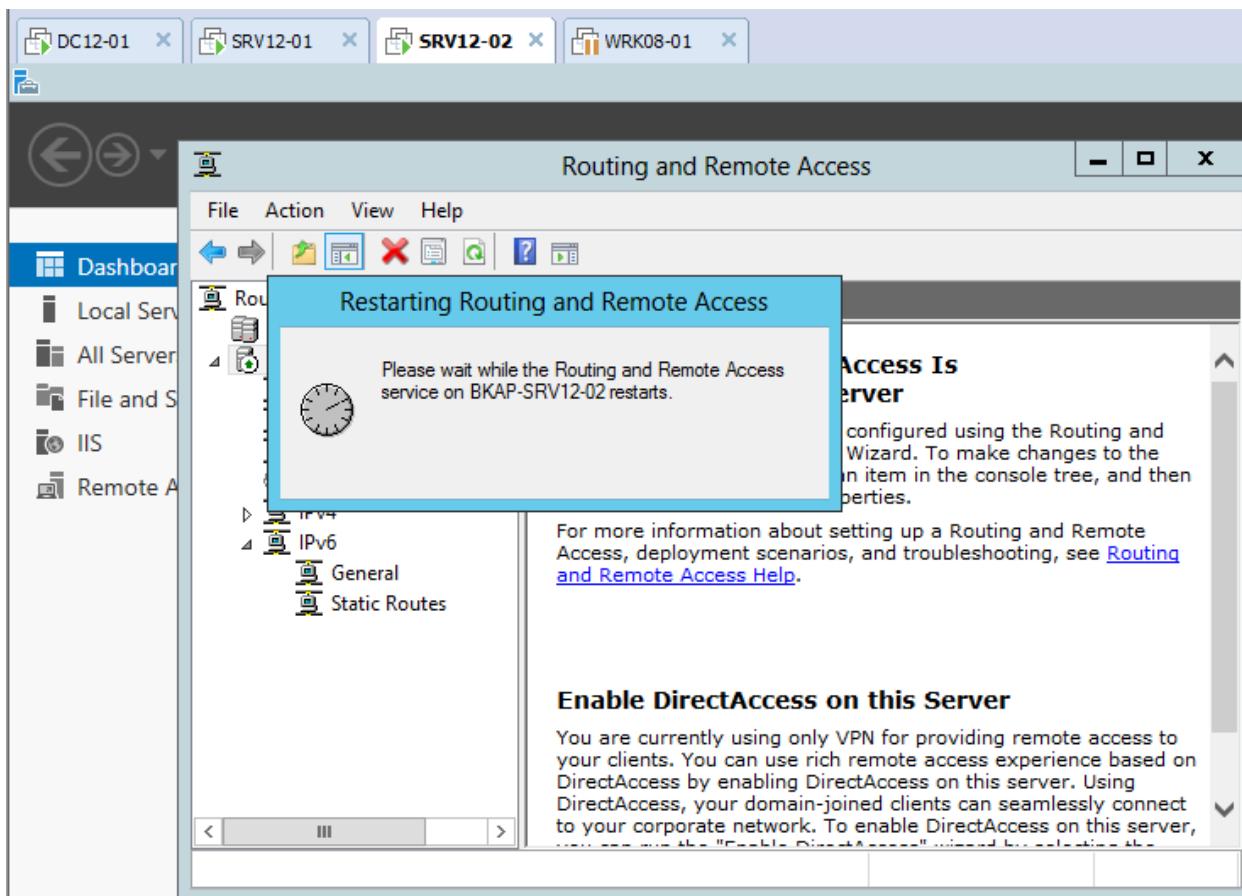
- Nhập vào các thông số như sau:



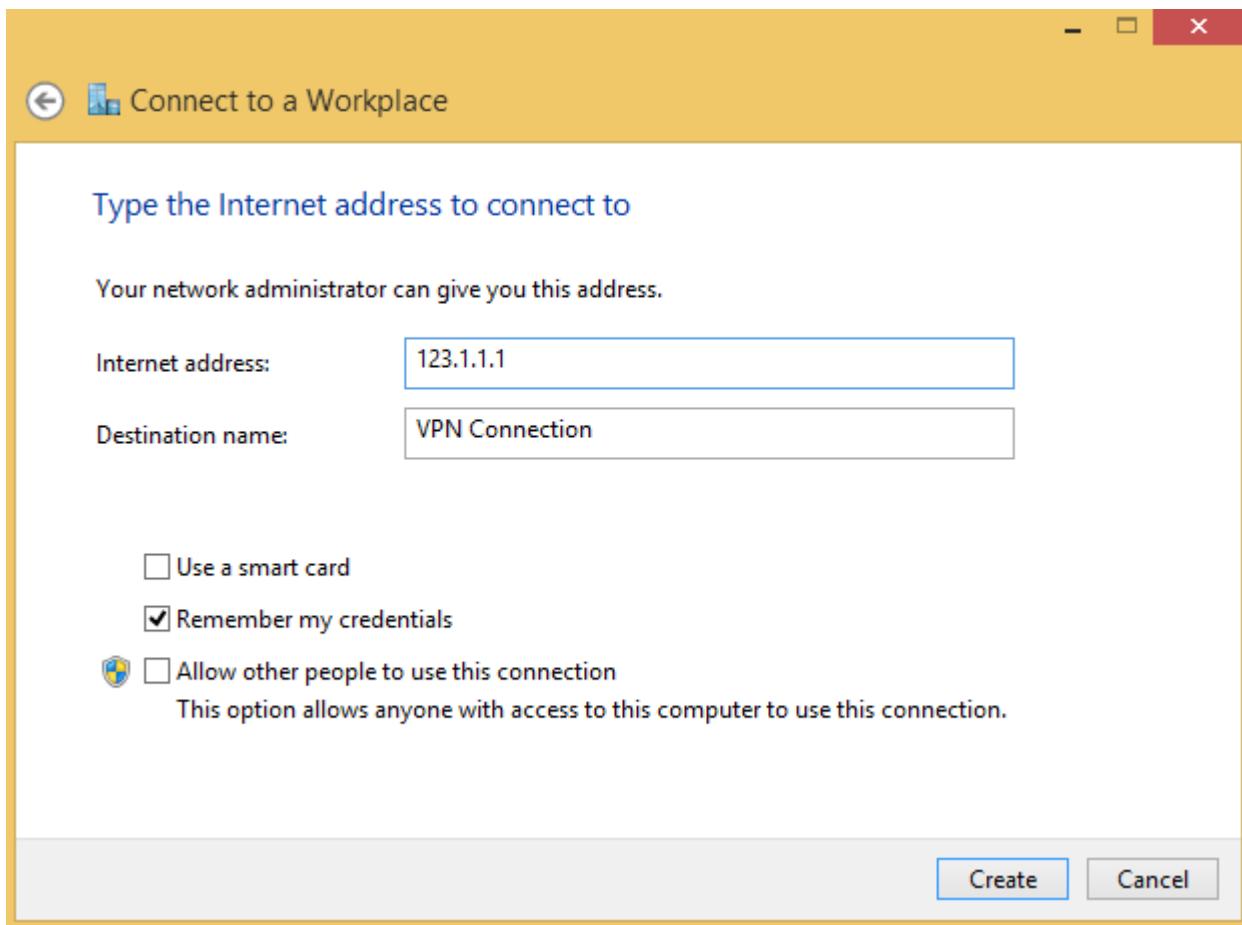


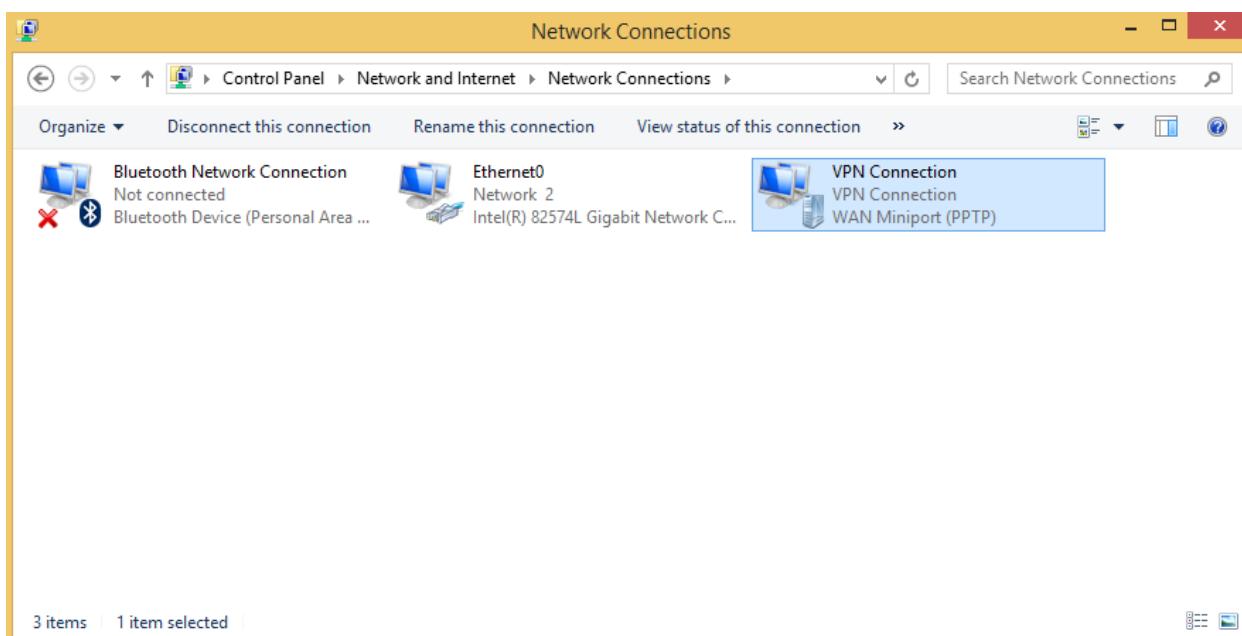
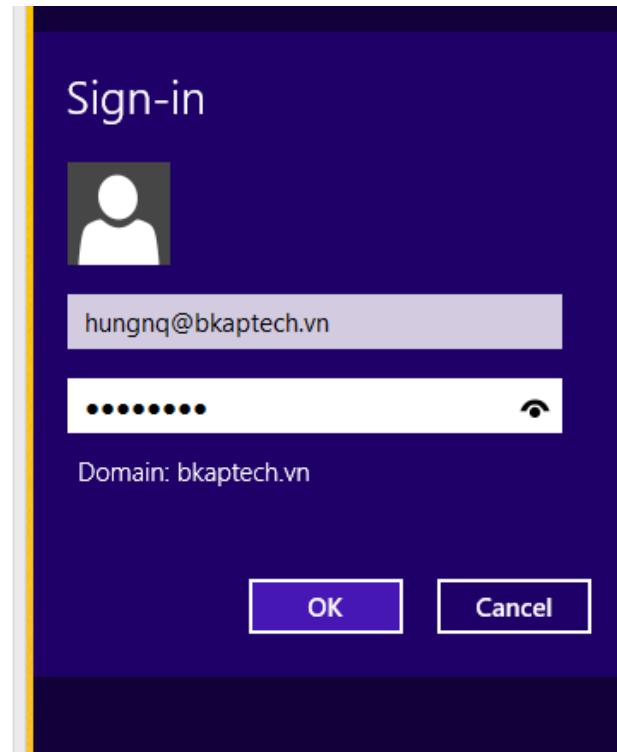
▪ OK.

- Restart lại dịch vụ RRAS.



- Chuyển qua máy trạm Client , thực hiện tạo **VPN Client**.





- Thực hiện ping đến máy *BKAP-DC12-01*.

The screenshot shows a Windows Command Prompt window titled 'cmd' running as administrator. The window displays the output of a 'ping' command to the IP address 192.168.1.2. The output shows four successful replies from the target host, each with 32 bytes of data and a TTL of 127. Below the replies, ping statistics are provided: 4 packets sent, 4 received, 0 lost (0% loss), and approximate round-trip times (Minimum = 0ms, Maximum = 1ms, Average = 0ms). The command prompt prompt is 'C:\Users\administrator>'.

```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

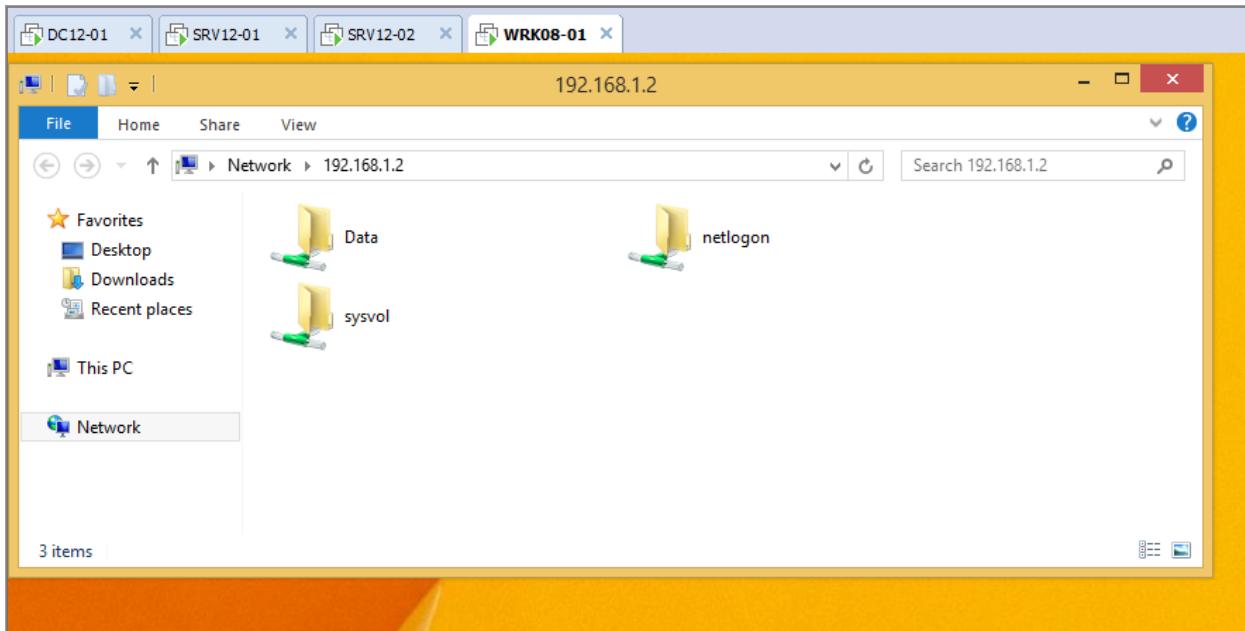
C:\Users\administrator>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:
Reply from 192.168.1.2: bytes=32 time=1ms TTL=127
Reply from 192.168.1.2: bytes=32 time<1ms TTL=127
Reply from 192.168.1.2: bytes=32 time<1ms TTL=127
Reply from 192.168.1.2: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\administrator>
```

- Thực hiện truy cập tài nguyên trên máy *BKAP-DC12-01*.



8.2 Triển khai cài đặt và cấu hình dịch vụ VPN Server kết hợp với NPS.

1. Yêu cầu bài lab:

+ Trên máy *BKAP-SRV12-01* : xây dựng làm máy chia sẻ tài nguyên với thư mục Data.

+ Trên máy *BKAP-SRV12-02* thực hiện các công việc sau :

- Tạo tài khoản có tên là **vpn** và nhóm người dùng tên là **vpns**.
- Cài đặt dịch vụ **Remote Access**, cấu hình **VPN Server** (dải ip cấp phát :*10.0.0.10 – 10.0.0.50*).
- Cài đặt và cấu hình dịch vụ **Network Policy Server**

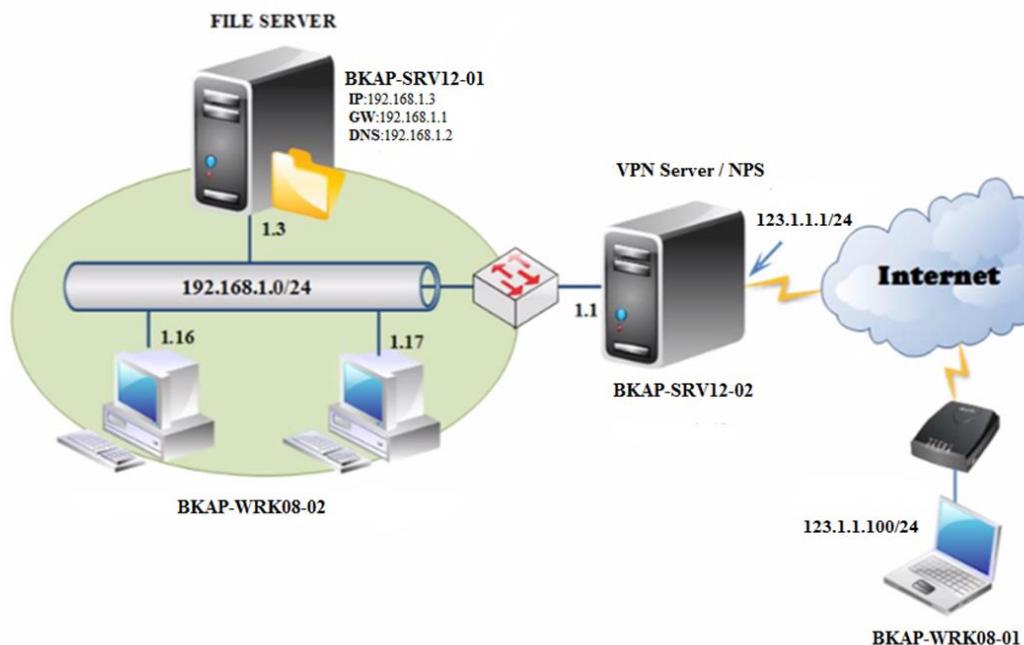
+ Trên máy *BKAP-WRK08-01* , thực hiện tạo **VPN Client** và kết nối.

2. Yêu cầu chuẩn bị:

- + Chuẩn bị 2 máy Server và 1 máy Client.
- + Sử dụng máy **BKAP-SRV12-02** làm **VPN Server** có 2 card mạng : card mạng 1 ứng với **VMnet2**, card mạng 2 ứng với **VMnet3**.
- + Từ máy **BKAP-WRK08-01** ping thông tin tới máy **BKAP-SRV12-02** với địa chỉ card **VMnet3**.

3. Mô hình lab:

HỆ THỐNG ĐÀO TẠO CNTT QUỐC TẾ BACHKHOA-APTECH
Lab 8.1 Cấu hình dịch vụ VPN Server kết hợp với NPS



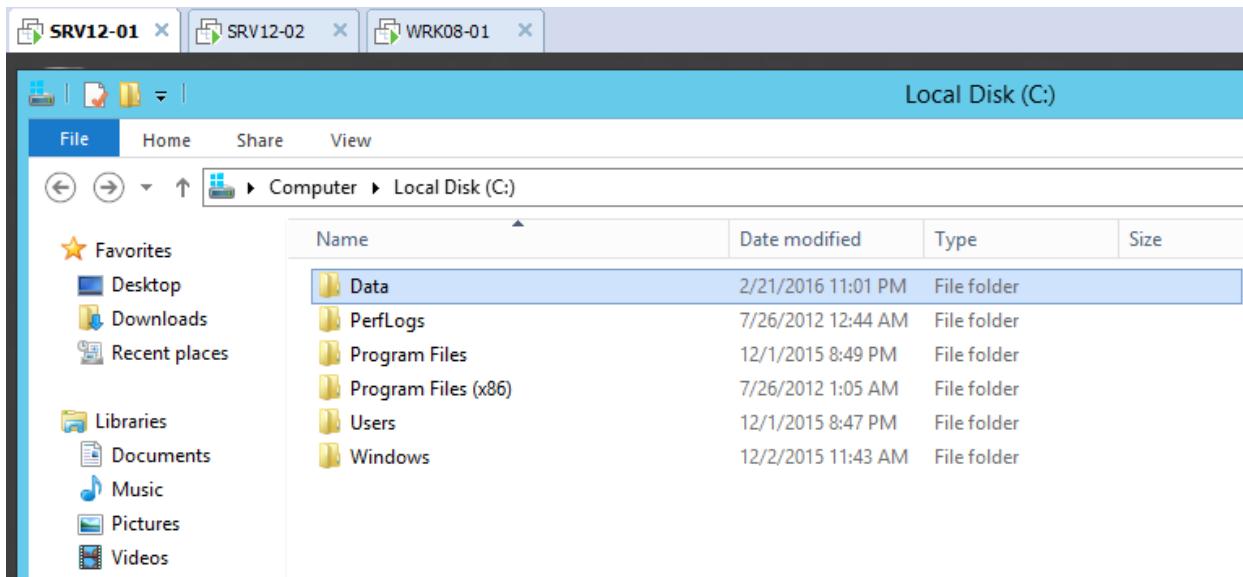
Hình 8.2

Sơ đồ địa chỉ như sau:

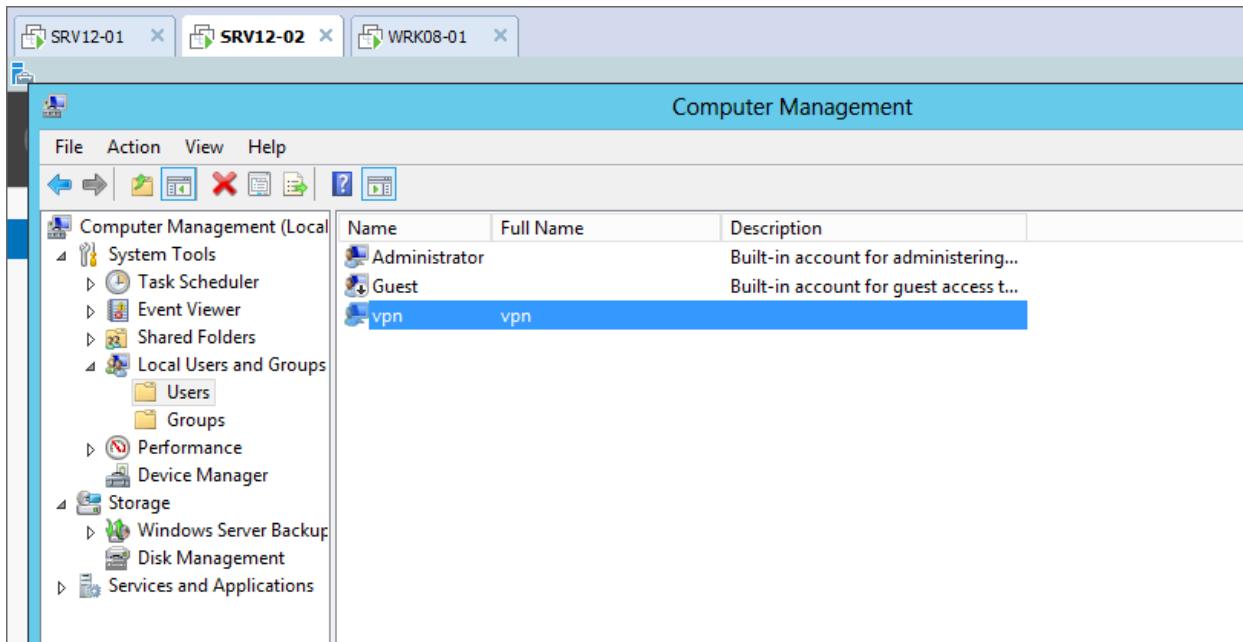
Thông số	BKAP-SRV12-01	BKAP-SRV12-02	BKAP-WRK08-01
IP address	192.168.1.3	VMnet2: 192.168.1.1 VMnet3: 123.1.1.1	123.1.1.100
Subnet Mask	255.255.255.0	255.255.255.0	255.255.255.0
Gateway	192.168.1.1	--	123.1.1.1

Hướng dẫn chi tiết :

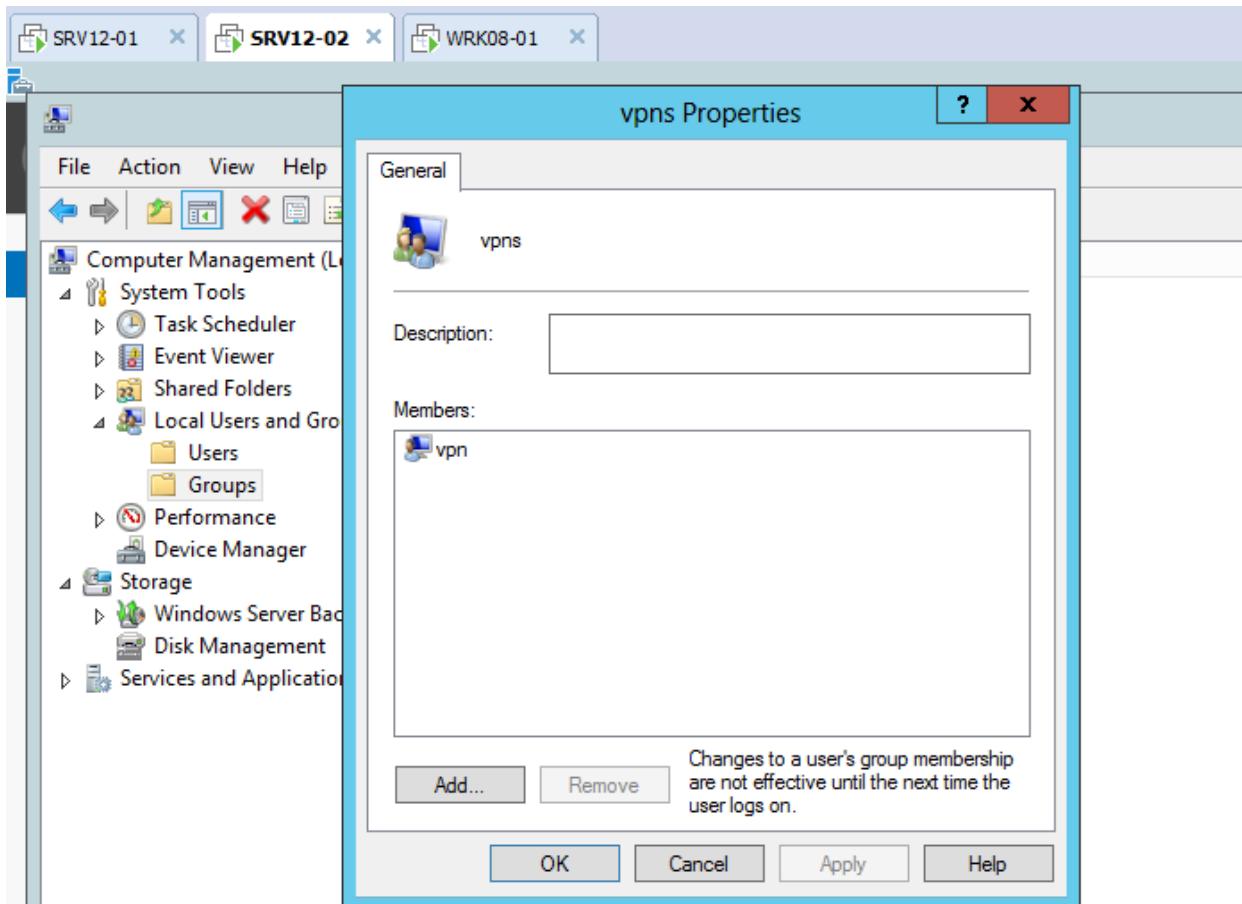
- Mở các máy ảo, kết nối như hình trên, ping thông giữa các mạng kết nối trực tiếp.
- Trên máy *BKAP-SRV12-01*, thực hiện tạo thư mục tên “**Data**” và chia sẻ dữ liệu.



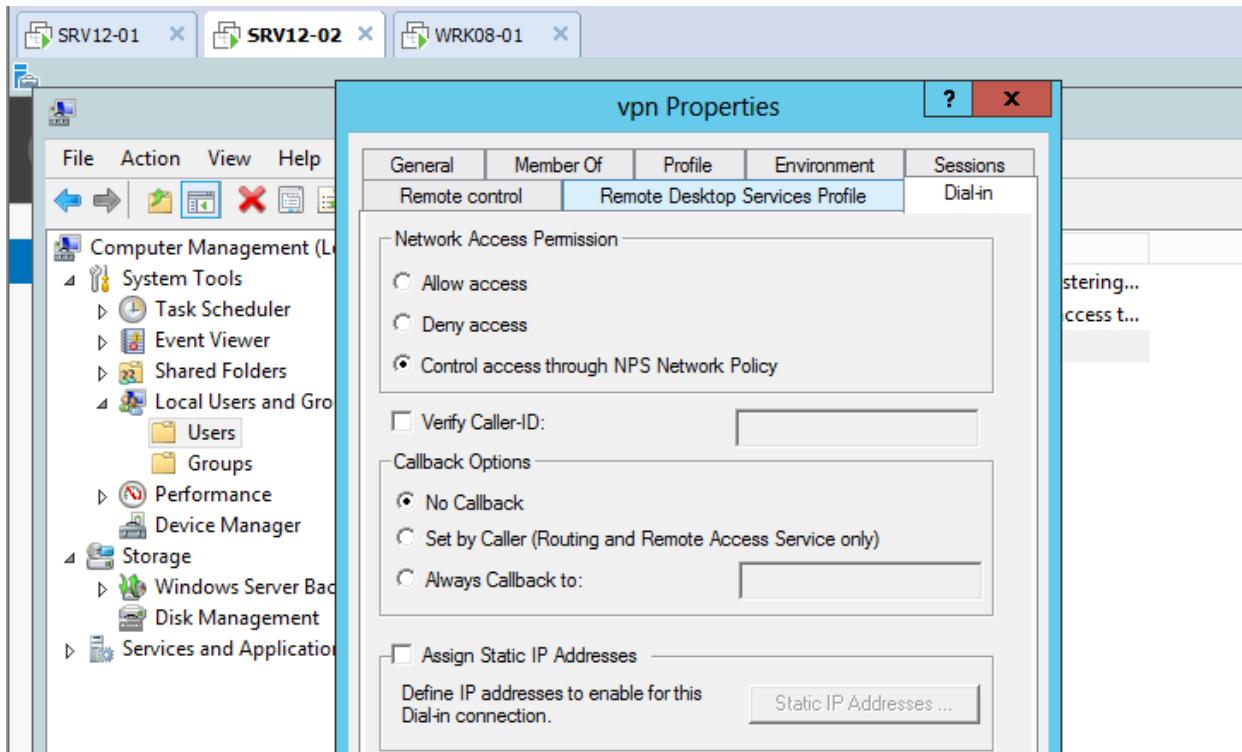
- Chuyển sang máy server *BKAP-SRV12-02*, thực hiện tạo tài khoản và nhóm để cấp phép **VPN** ở dạng **NPS** :
 - Tạo User *vpn* :



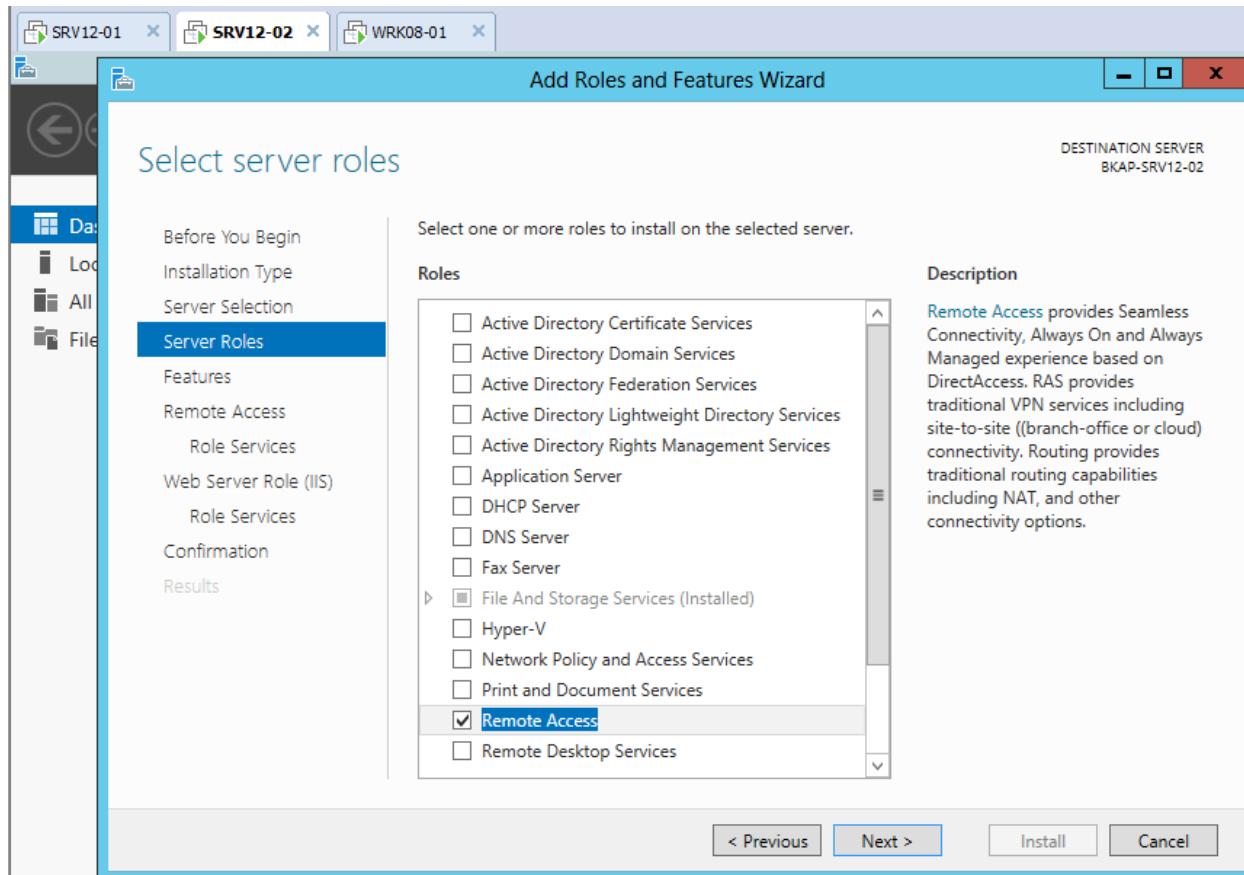
- Tạo Group **vpng** và add user **vpn** vào group.

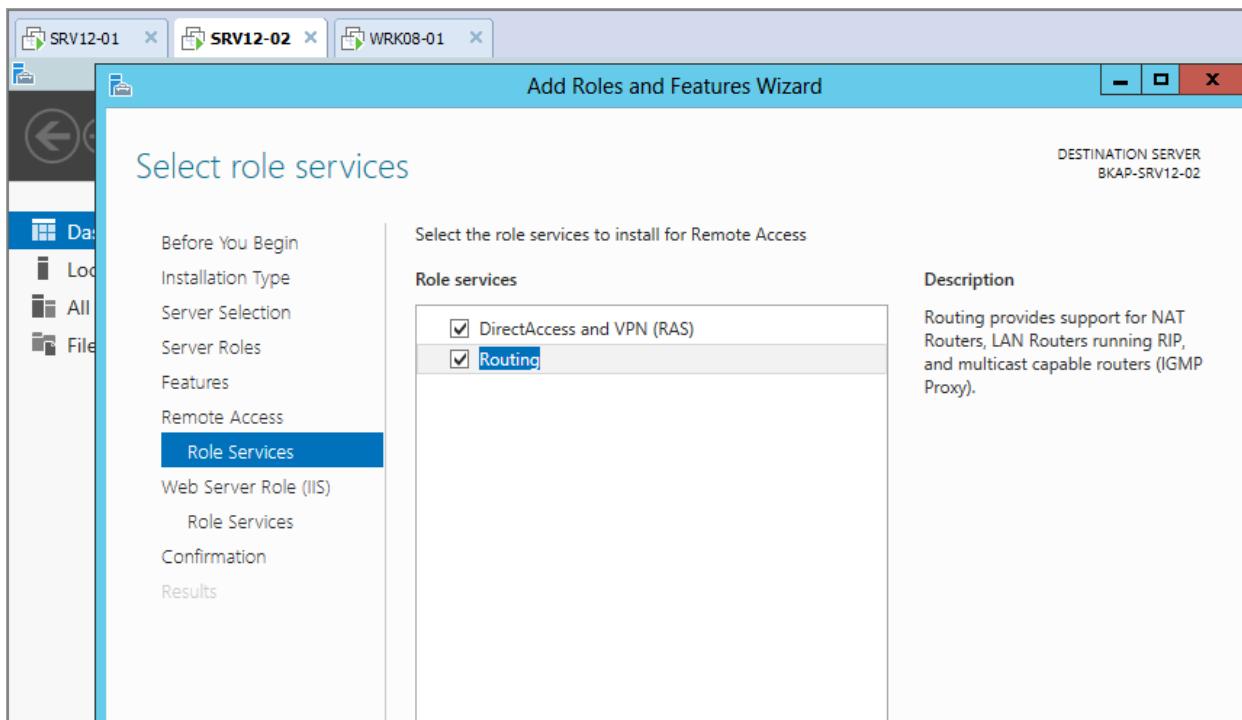


- Cấp quyền truy cập **VPN / NPS** cho user **vpn**.

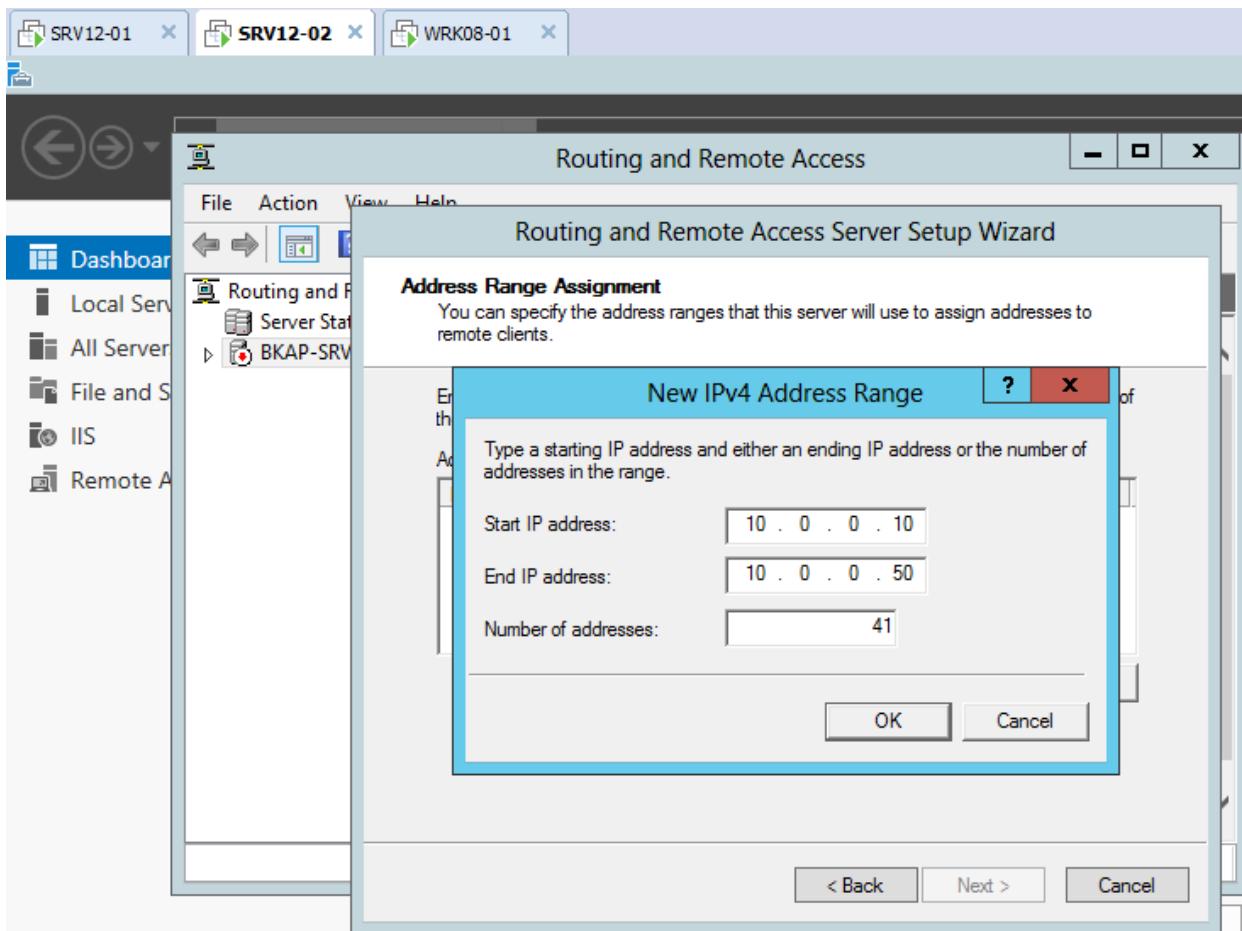


- Thực hiện cài đặt dịch vụ **Remote Access** và cấu hình **VPN Server**.
 - Cài đặt **Remote Access** :

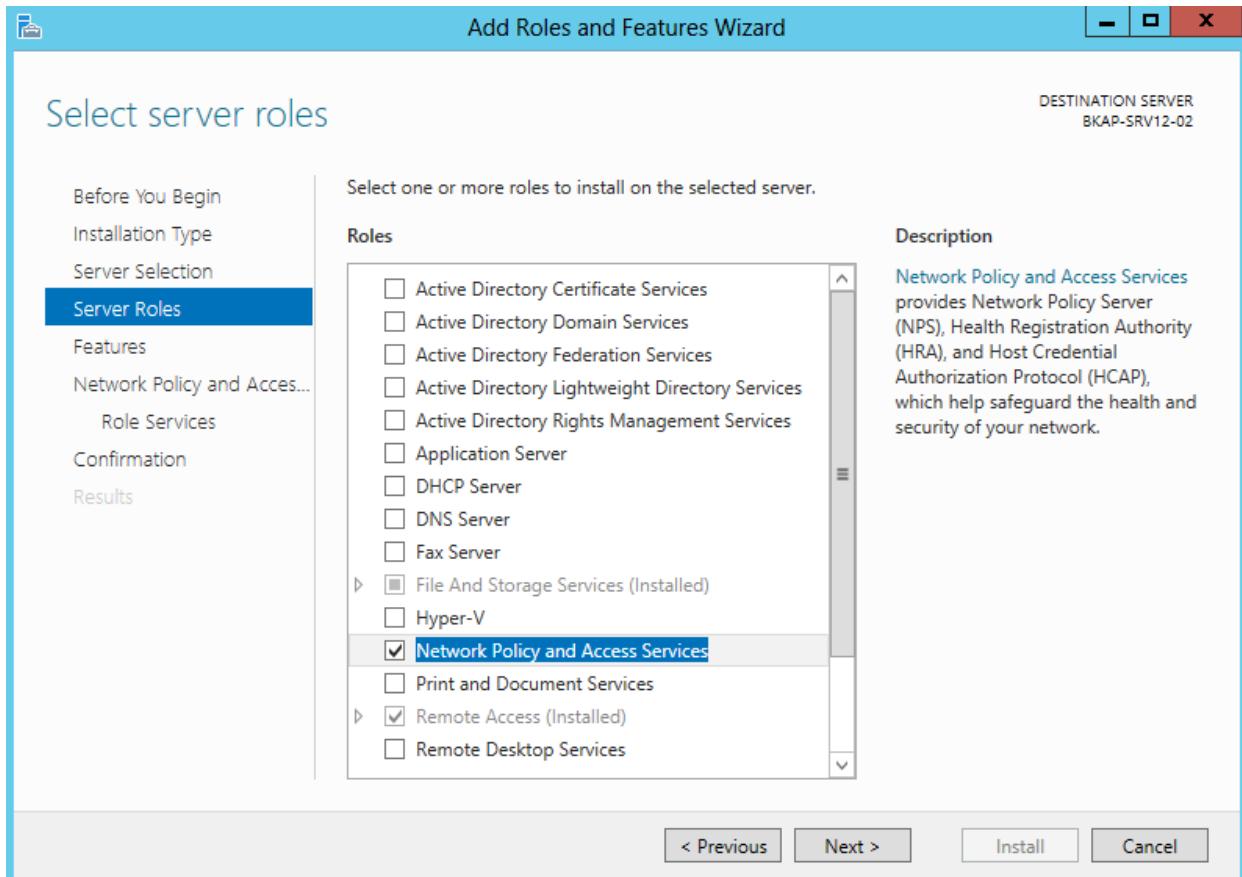




▪ Cấu hình VPN Server:

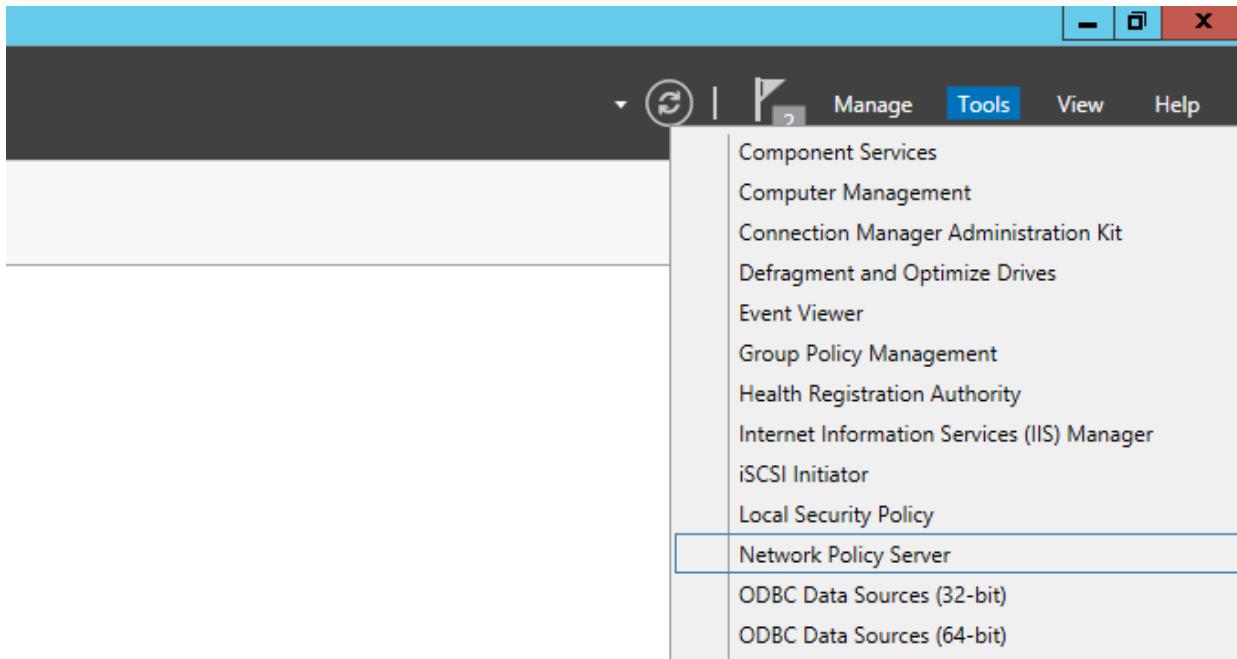


- Cài đặt dịch vụ **Network Policy Server** :
 - **Server Manager / Add roles and features**
 - Tại cửa sổ **Select server roles**, chọn vào dịch vụ **Network Policy and Access Services**.

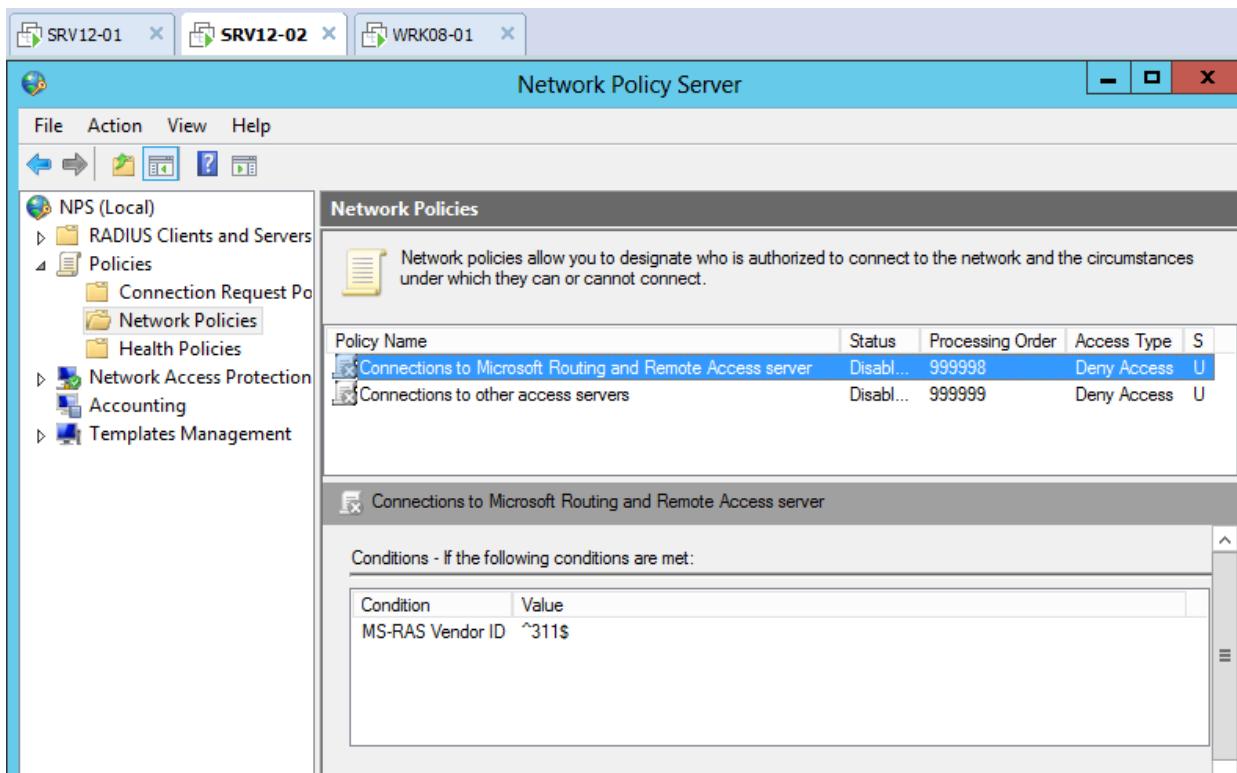


- Click vào **Next ... Install** .

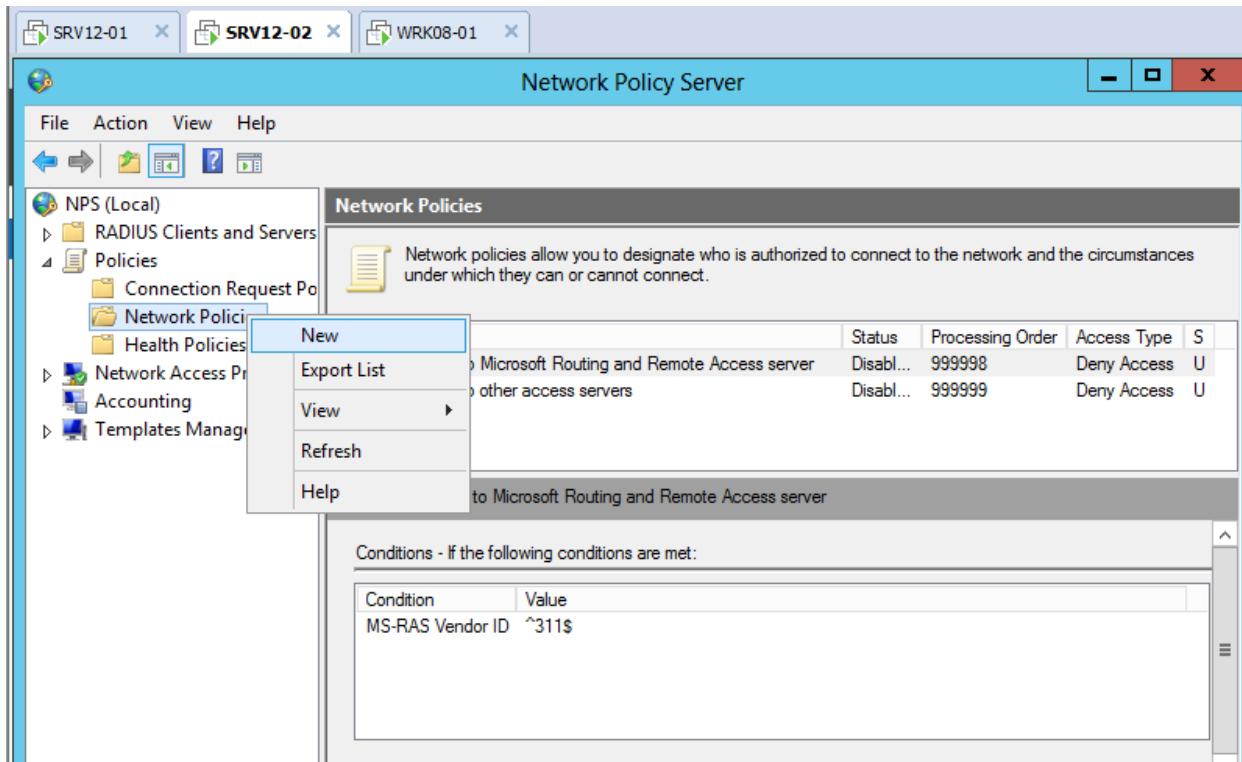
- Thực hiện cấu hình dịch vụ **Network Policy Server**.
 - Tools / Network Policy Server.



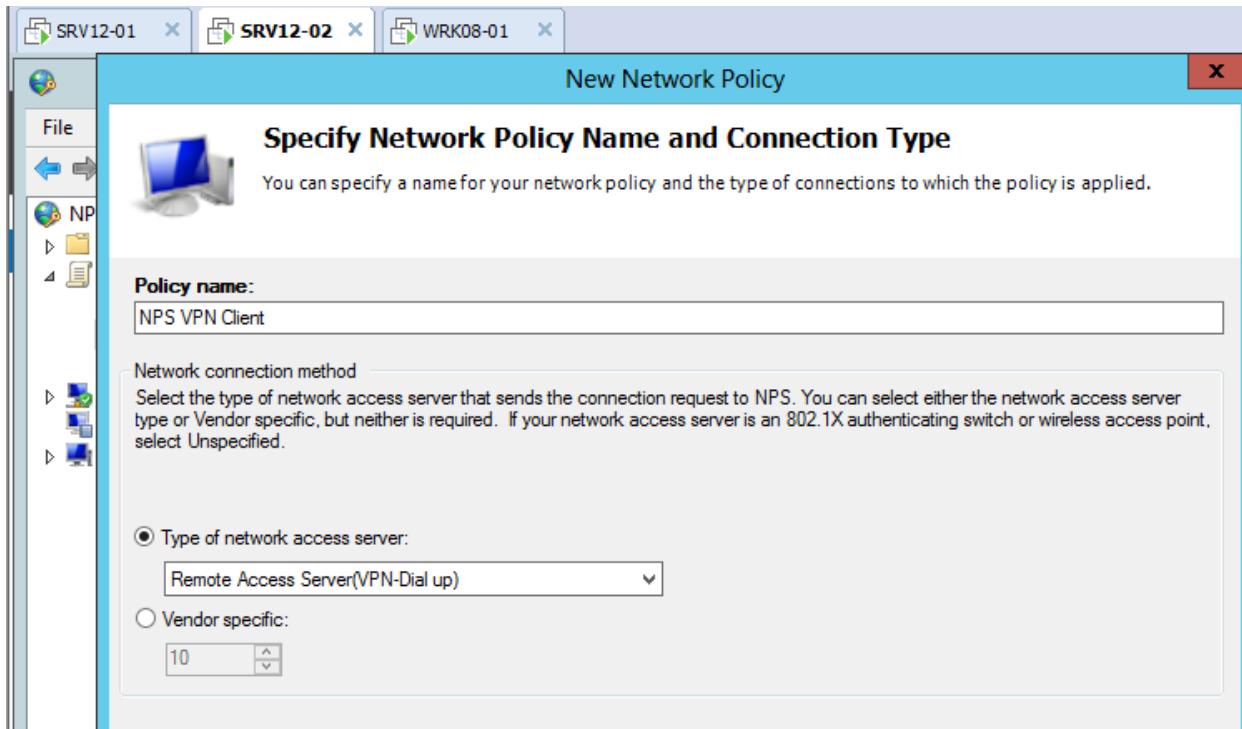
- Tại cửa sổ **Network Policy Server** , chọn vào **Policies / Network Policies** , thực hiện **Disable** 2 chính sách **Connections**



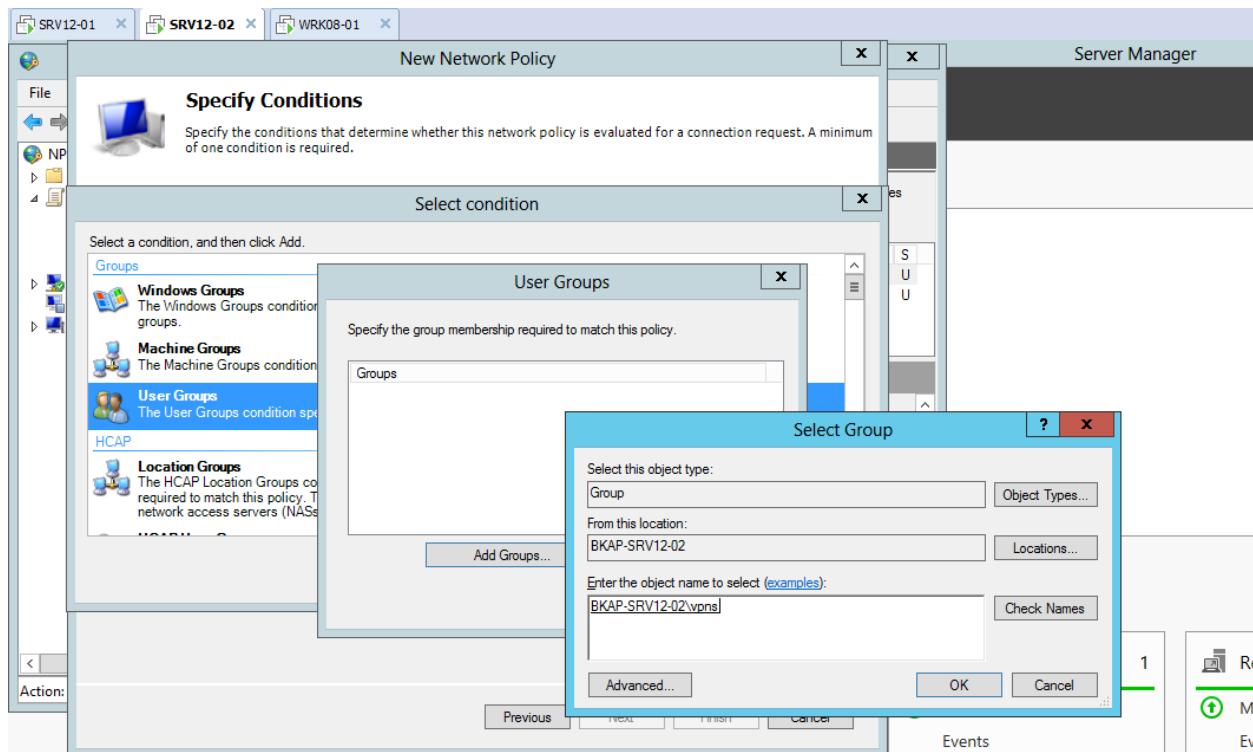
- Click chuột phải tại Network Policies / New.



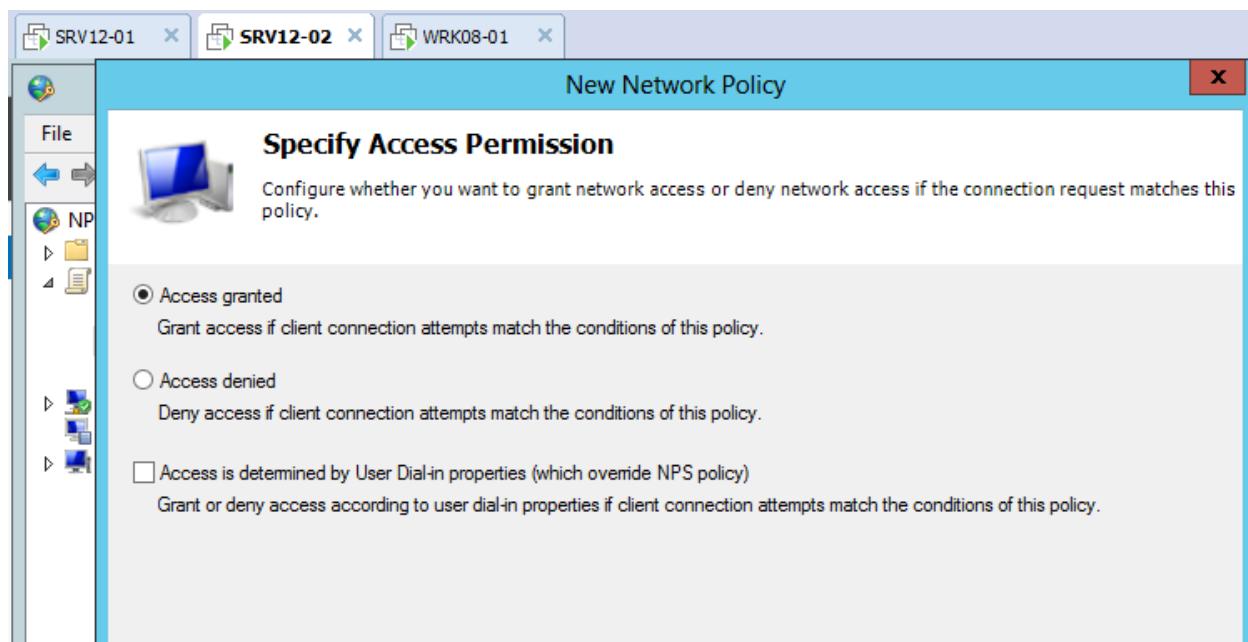
- Tại cửa sổ **Specify Network Policy Name and Connection Type**, nhập vào tại mục *Policy name* : **NPS VPN Client** , tại mục *Type of network access server* , chọn vào **Remote Access Server(VPN-Dial up)**.



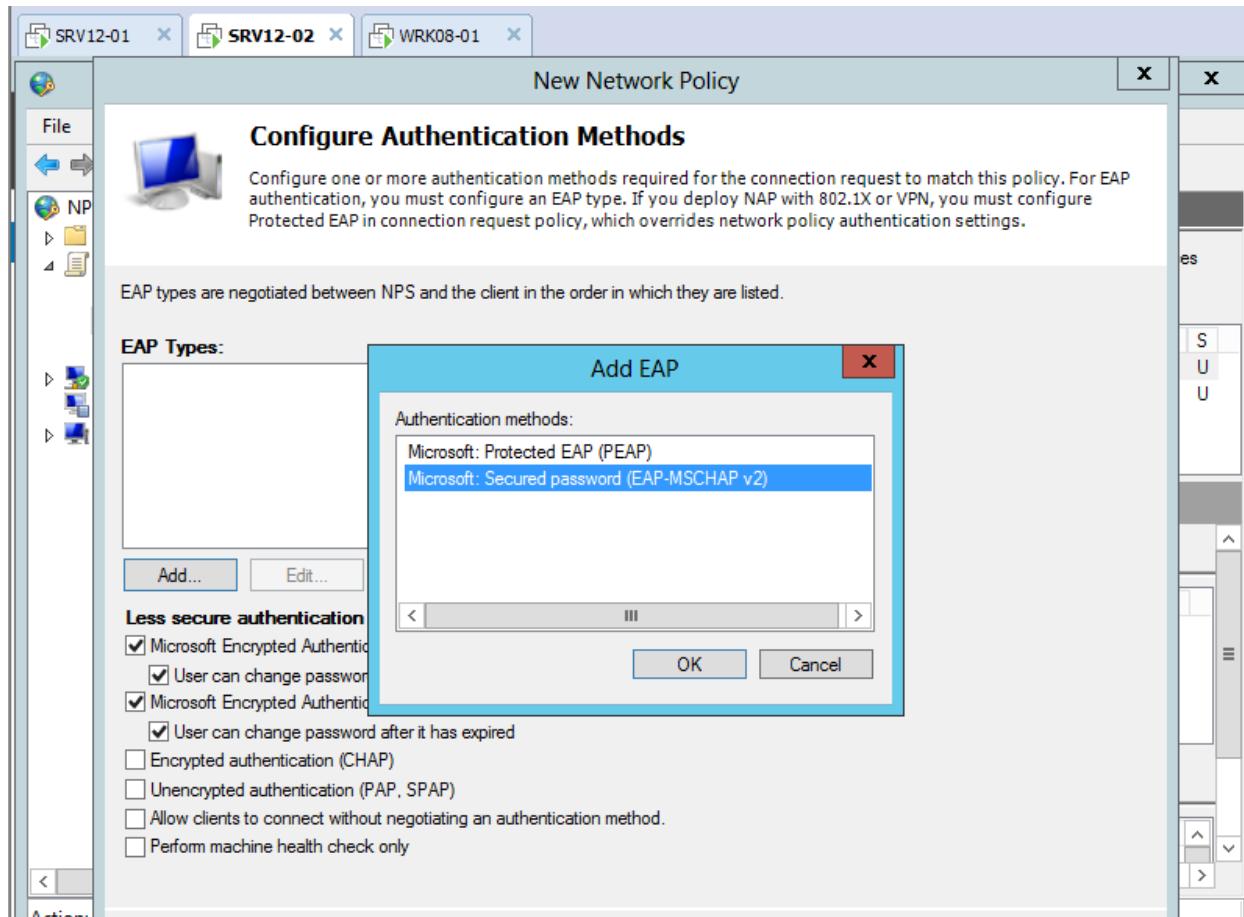
- Tại cửa sổ **Specify Conditions** , click vào **Add...**
- Tại cửa sổ **Select condition** , chọn vào **User Groups** , click vào **Add...**
- Tại cửa sổ **User Groups** , click vào **Add Groups...**
- Tại cửa sổ **Select Group** , chọn đến **Group vpns**.
- OK / Next.**



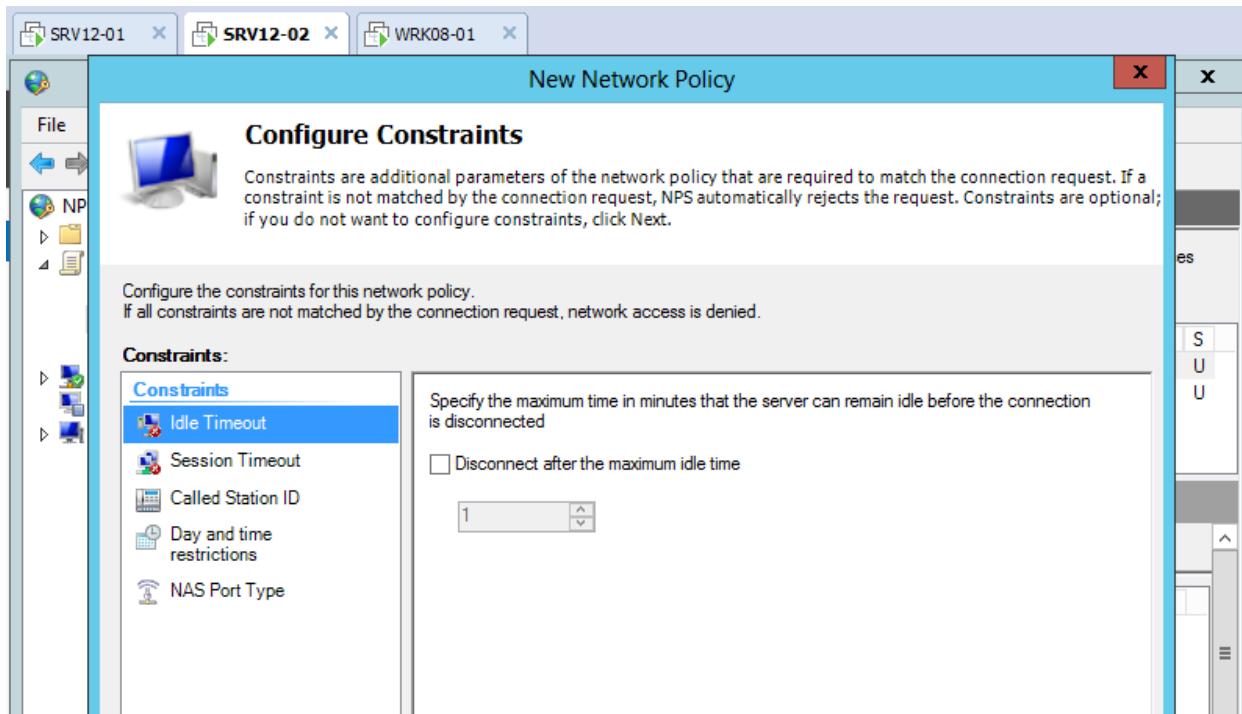
- Tại cửa sổ **Specify Access Permission**, chọn **Access granted / Next.**



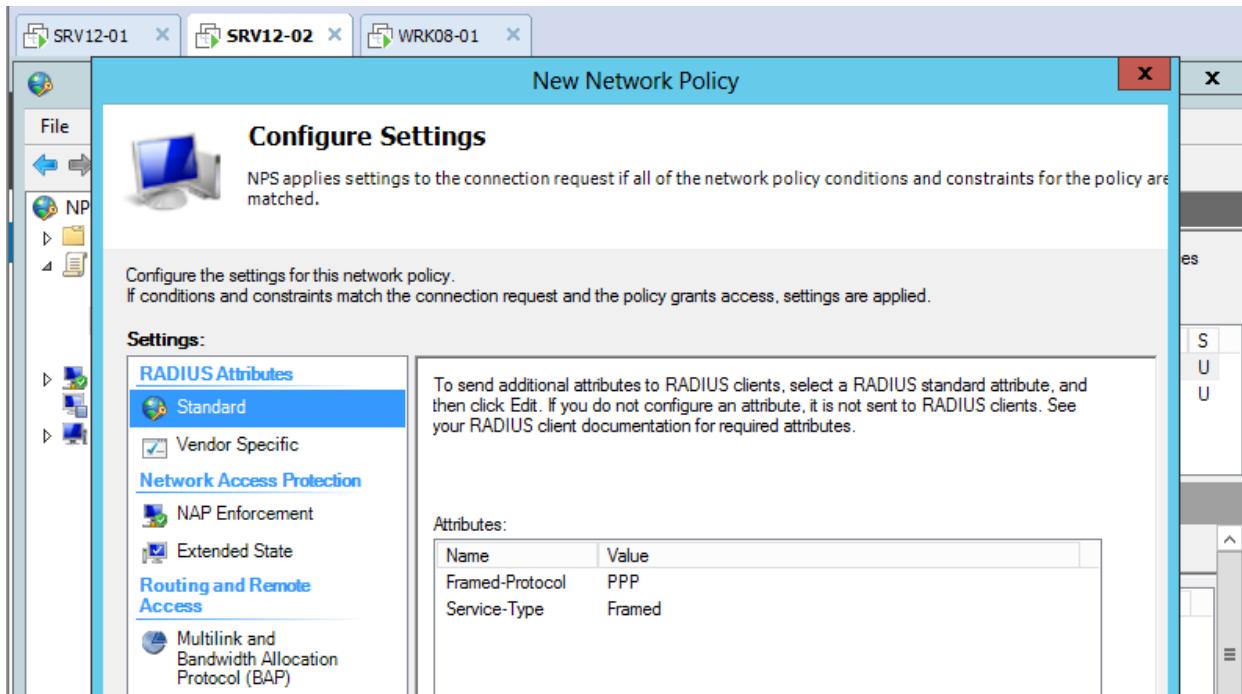
- Tại cửa sổ **Configure Authentication Methods**, click vào **Add...**
- Tại cửa sổ **Add EAP**, chọn **Microsoft: Secured password (EAP-MSCHAP v2)** / **OK** / **Next**.



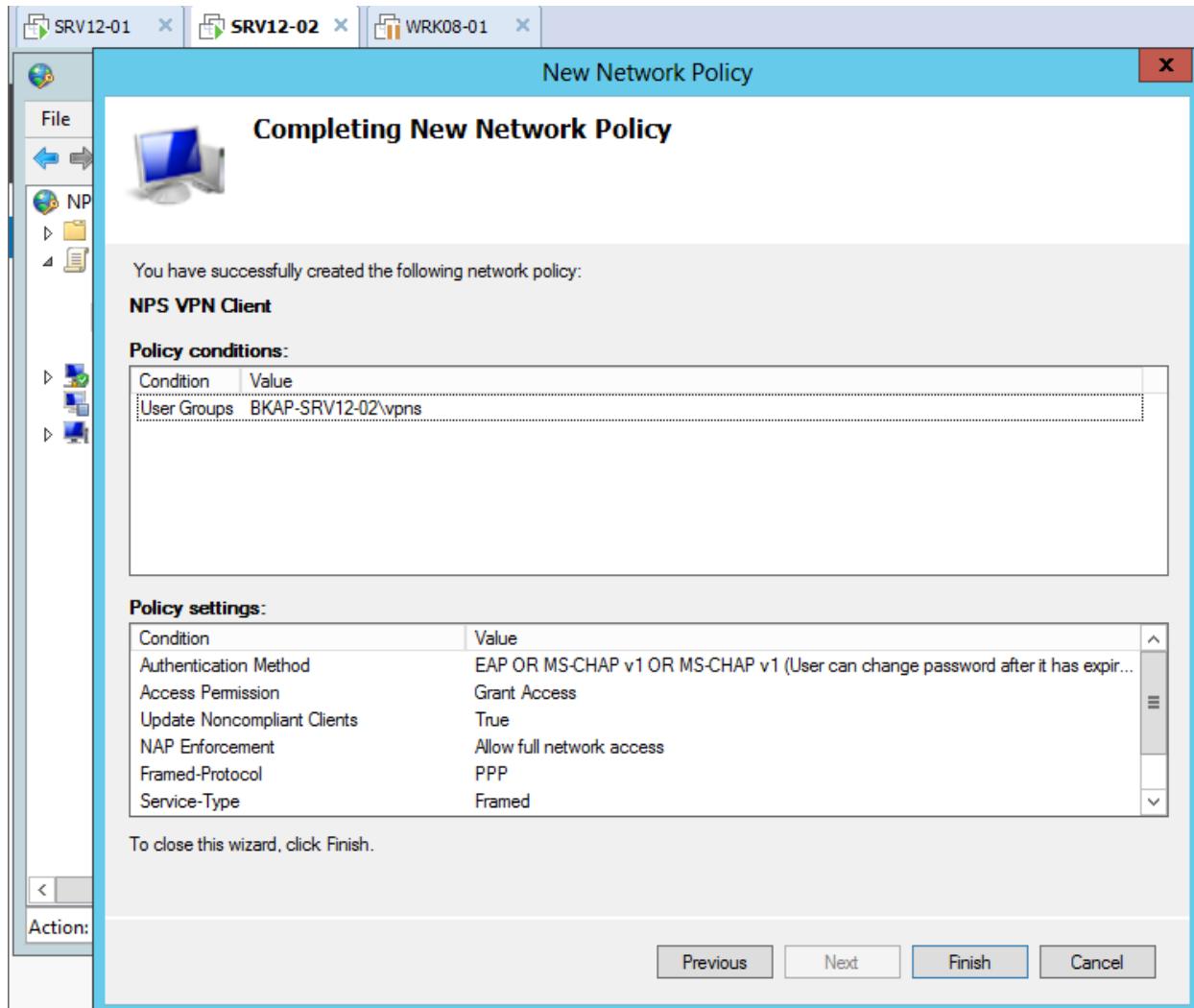
- Tại cửa sổ **Configure Constraints**, click vào Next



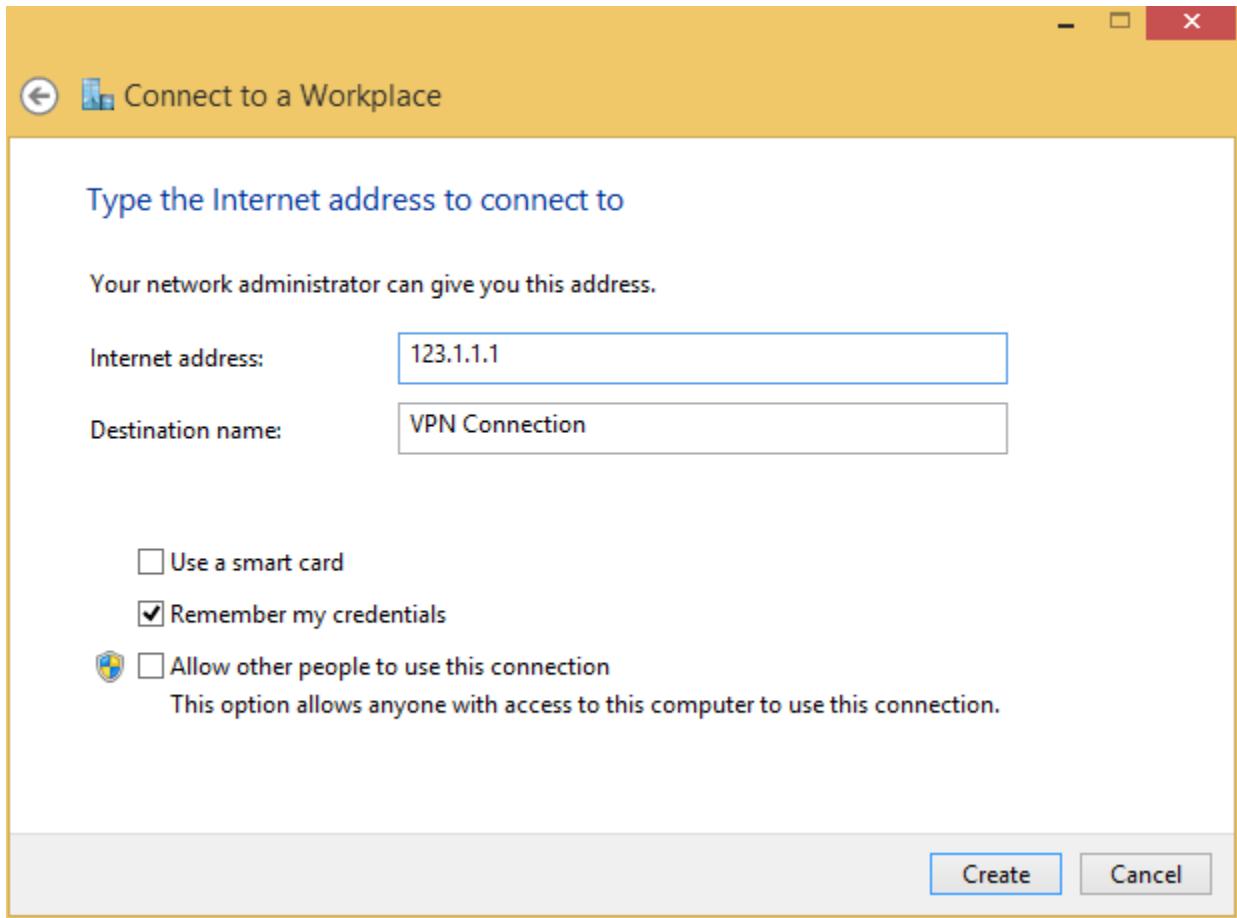
- Tại cửa sổ **Configure Settings**, click vào Next.



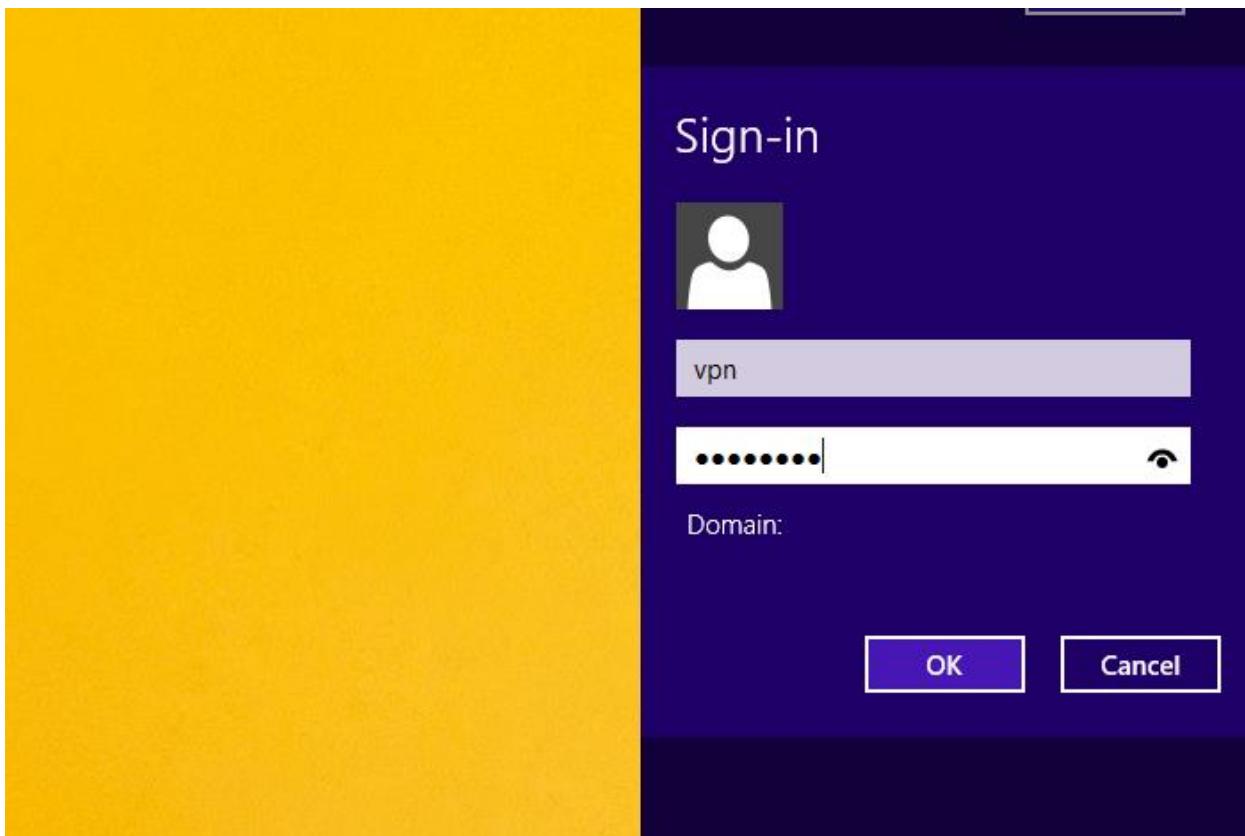
- Tại cửa sổ **Completing New Network Policy**, click vào **Finish**.



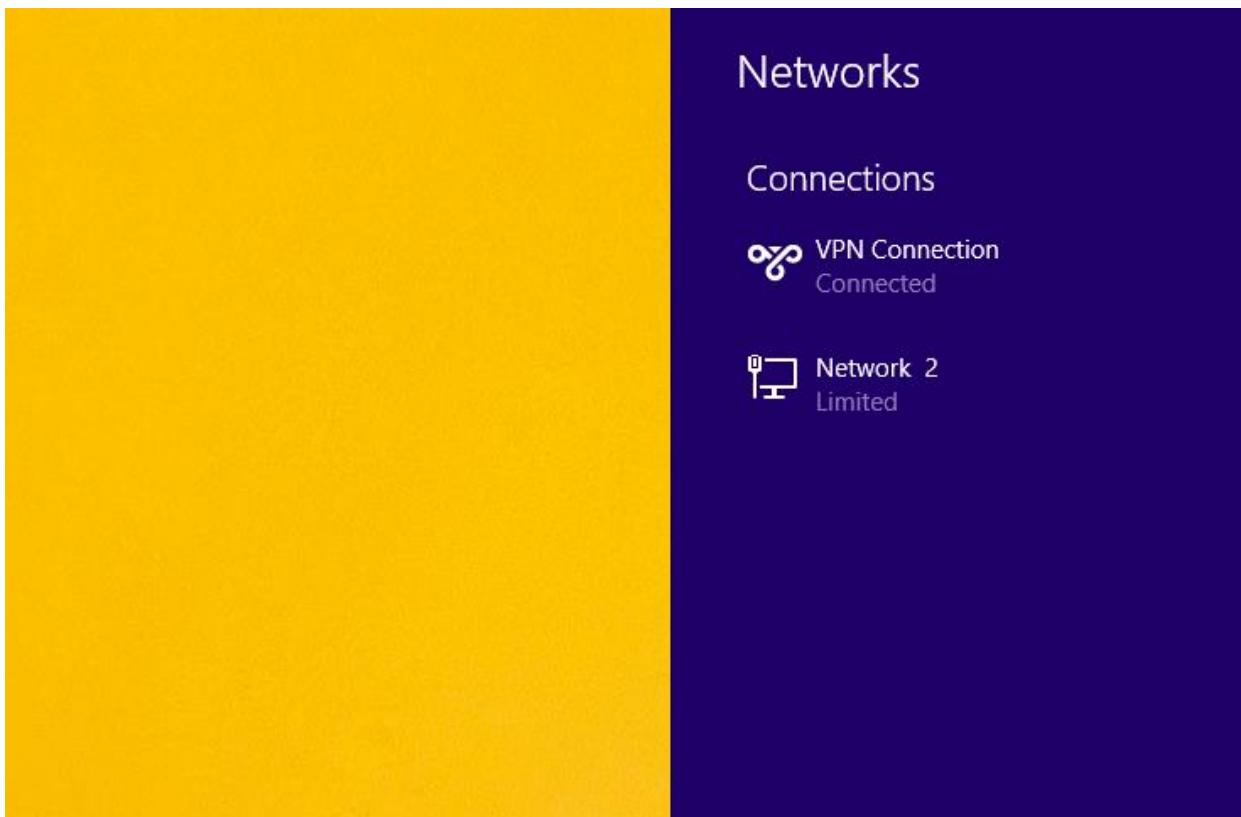
- Chuyển sang máy trạm *BKAP-WRK08-01*, thực hiện tạo kết nối **VPN Client**.



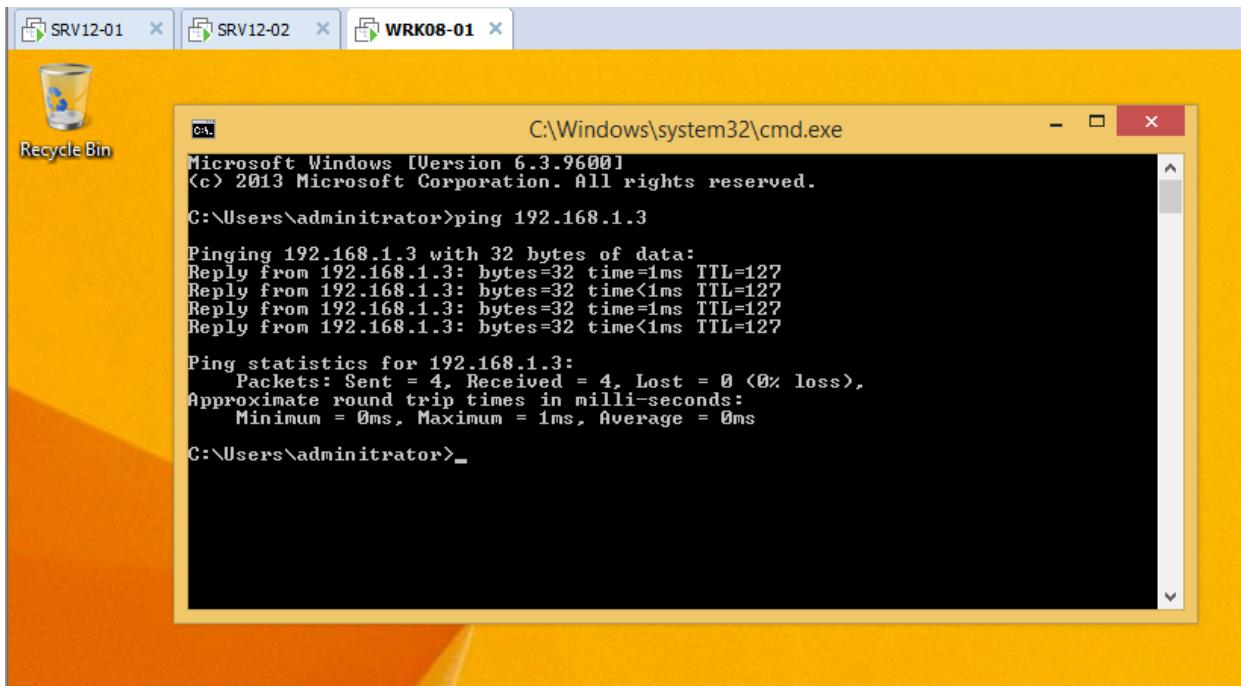
- Kết nối VPN;



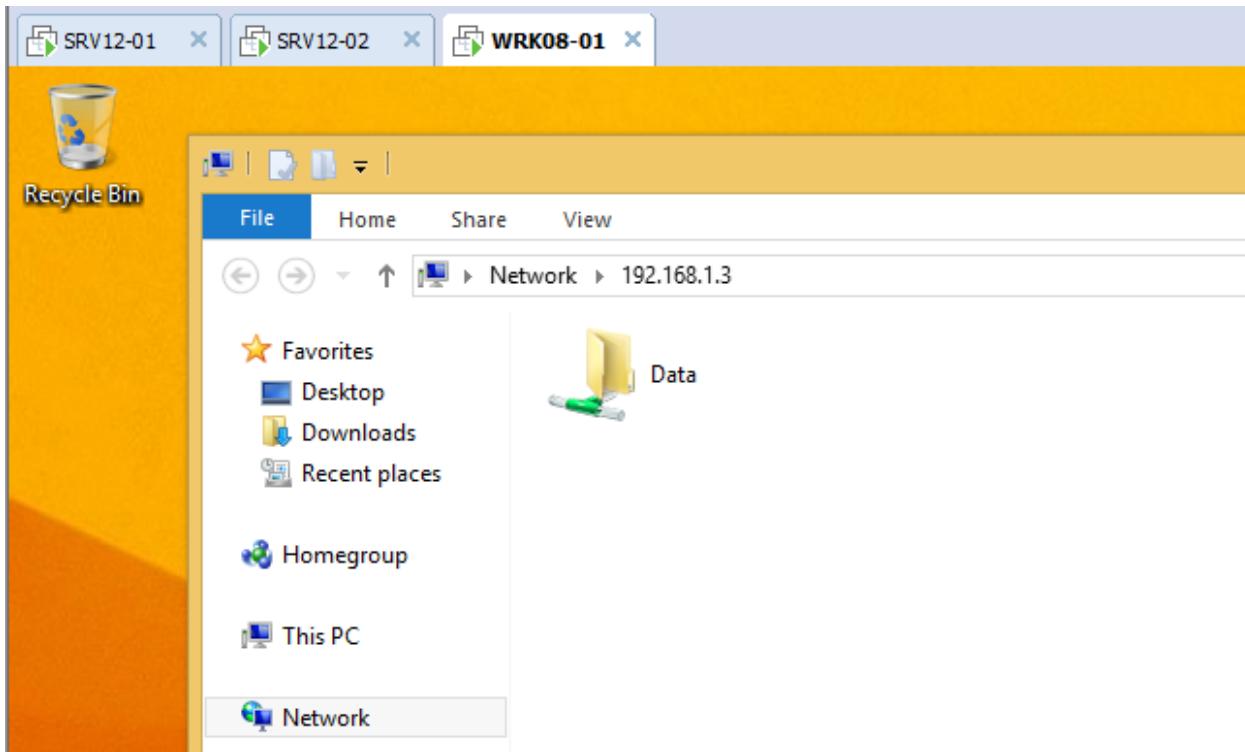
- Kết nối VPN thành công.



- Ping đến máy *BKAP-SRV12-01*:



- Truy cập dữ liệu trên máy *BKAP-SRV12-01*.



8.3 Triển khai cài đặt và cấu hình dịch vụ VPN Server kết hợp với RADIUS và NPS.

1. Yêu cầu bài Lab:

+ Trên máy server *BKAP-DC12-01*, thực hiện các công việc sau:

- Tạo *OU, Group, User* và cho phép tài khoản được truy cập **VPN**.
- Thực hiện tạo 1 thư mục “*Data*” và chia sẻ dữ liệu.

+ Trên máy server *BKAP-SRV12-01*, thực hiện công việc sau:

- Cài đặt và cấu hình dịch vụ **Network Policy and Access Services**.

+ Trên máy server *BKAP-SRV12-02*, thực hiện công việc sau:

- Thực hiện cài đặt **Remote Access** và cấu hình **VPN Server**.

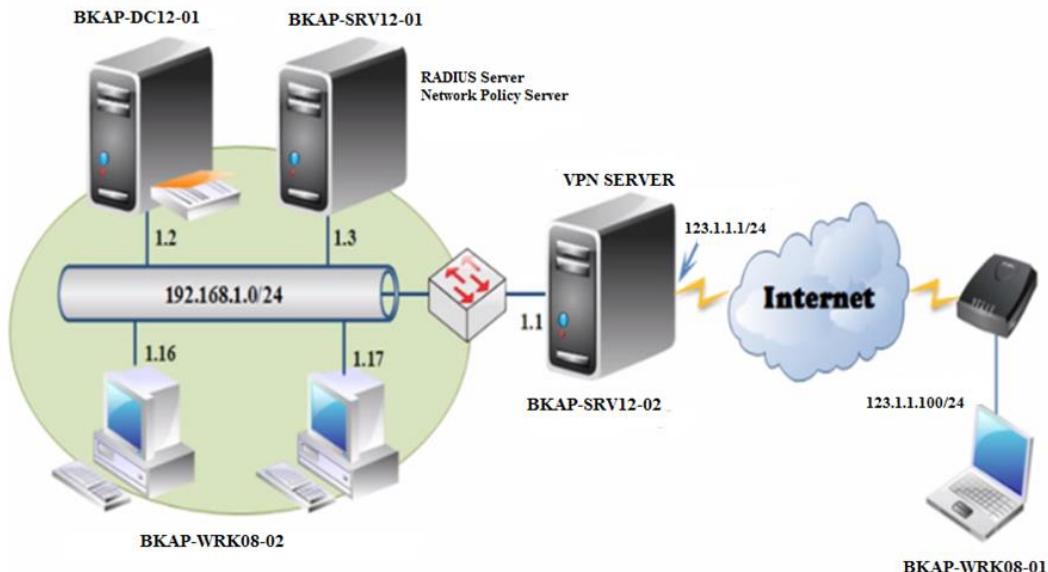
+ Trên máy trạm *BKAP-WRK08-01*, thực hiện tạo kết nối **VPN Client**.

2. Yêu cầu chuẩn bị:

- + Máy server **BKAP-DC12-01** : đã nâng cấp domain controller quản lý miền **bkaptech.vn**.
- + Máy server **BKAP-SRV12-01** : đã Join vào miền.
- + Máy server **BKAP-SRV12-02** : có 2 card mạng LAN và WAN.
- + Máy trạm **BKAP-WRK08-01**.

3. Mô hình Lab:

HỆ THỐNG ĐÀO TẠO CNTT QUỐC TẾ BACHKHOA-APTECH
Lab 8.3 Cấu hình dịch vụ VPN Server kết hợp với RADIUS và NPS



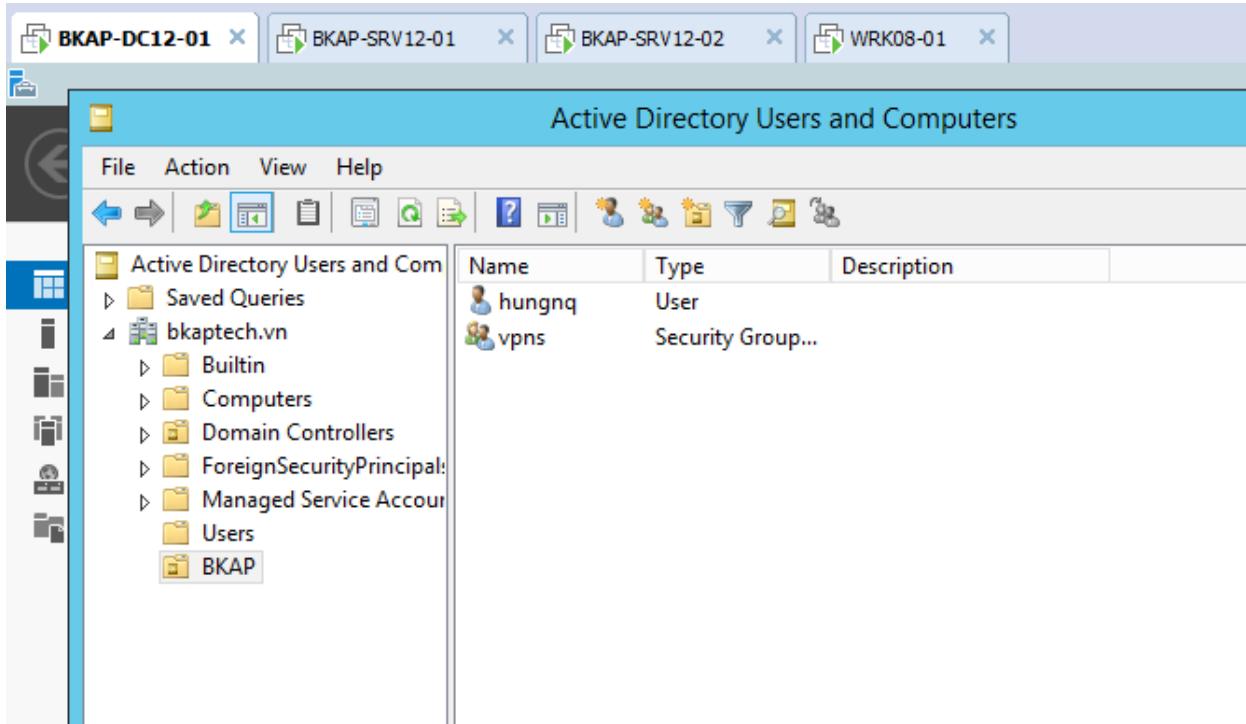
Hình 8.3

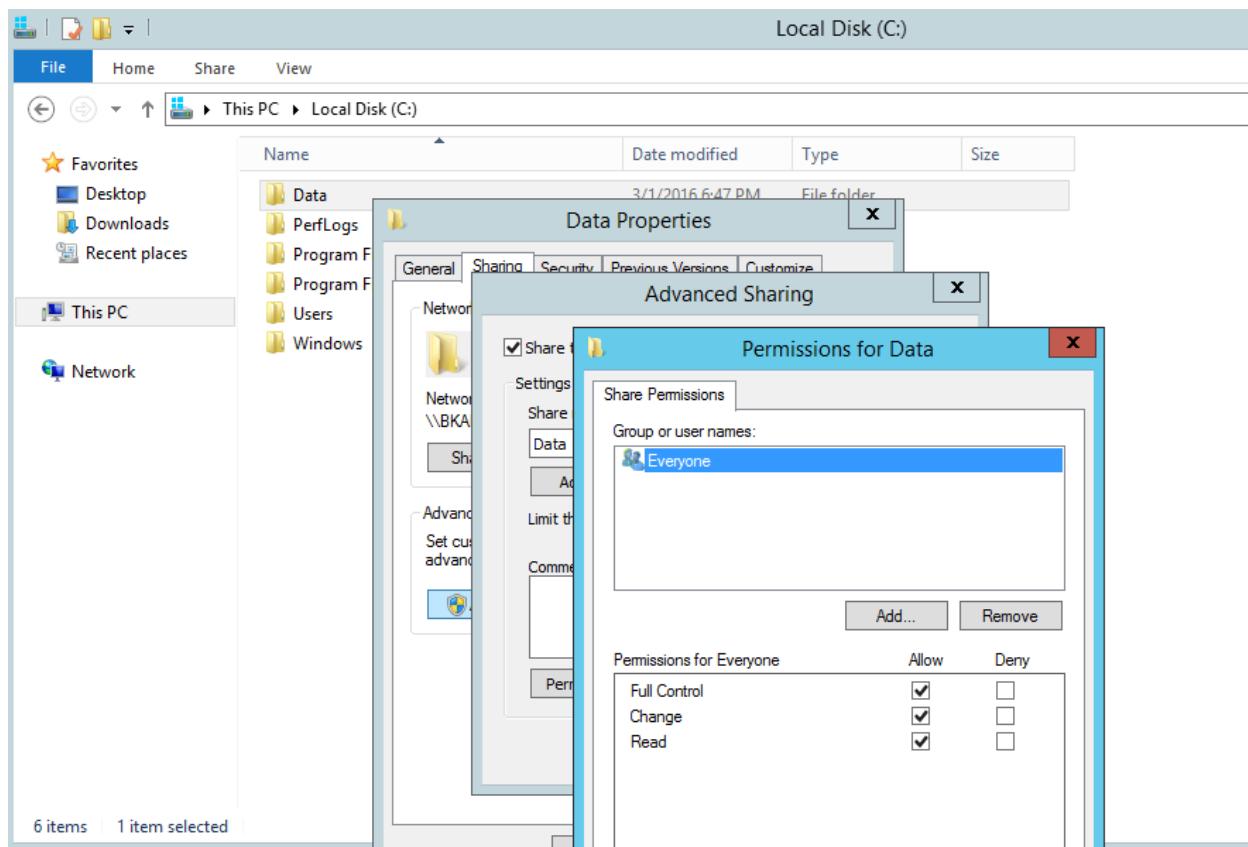
Sơ đồ địa chỉ như sau:

Thông số	DC12-01	SRV12-01	SRV12-02	WRK08-01
IP address	192.168.1.2	192.168.1.3	LAN:192.168.1.1 WAN:123.1.1.1	123.1.1.100
Gateway	192.168.1.1	192.168.1.1	--	123.1.1.1
Subnet Mask	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
DNS Server	192.168.1.2	192.168.1.2	--	--

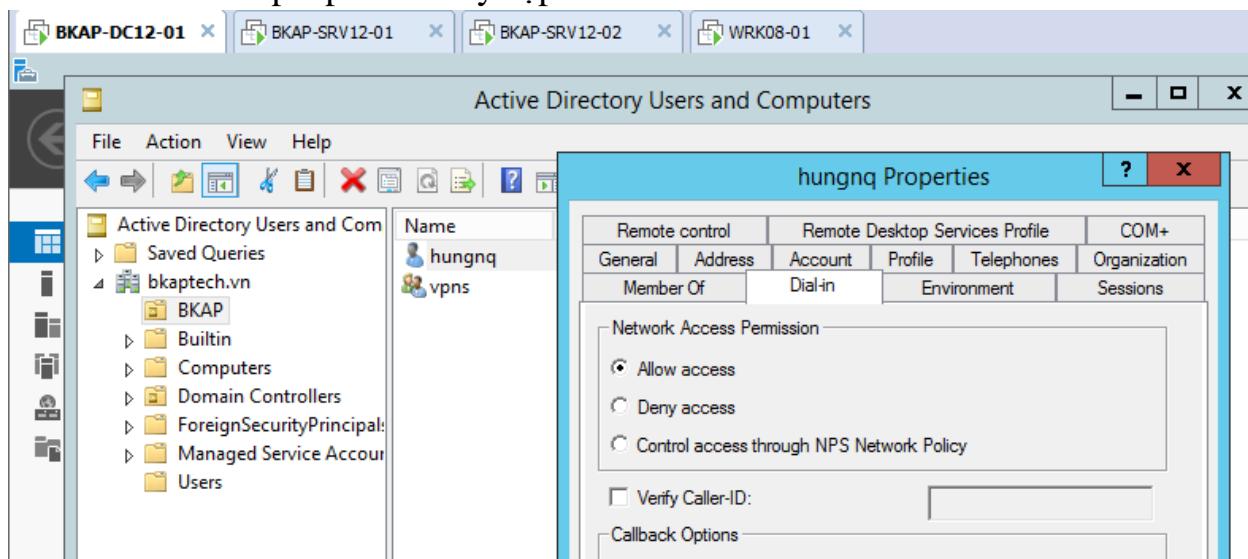
Hướng dẫn chi tiết:

- Kết nối các máy ảo như hình trên, ping thông giữa các mạng kết nối trực tiếp.
- Chuyển qua Server *BKAP-DC12-01*, thực hiện tạo *OU*, *Group*, *User* và tạo thư mục , chia sẻ dữ liệu.

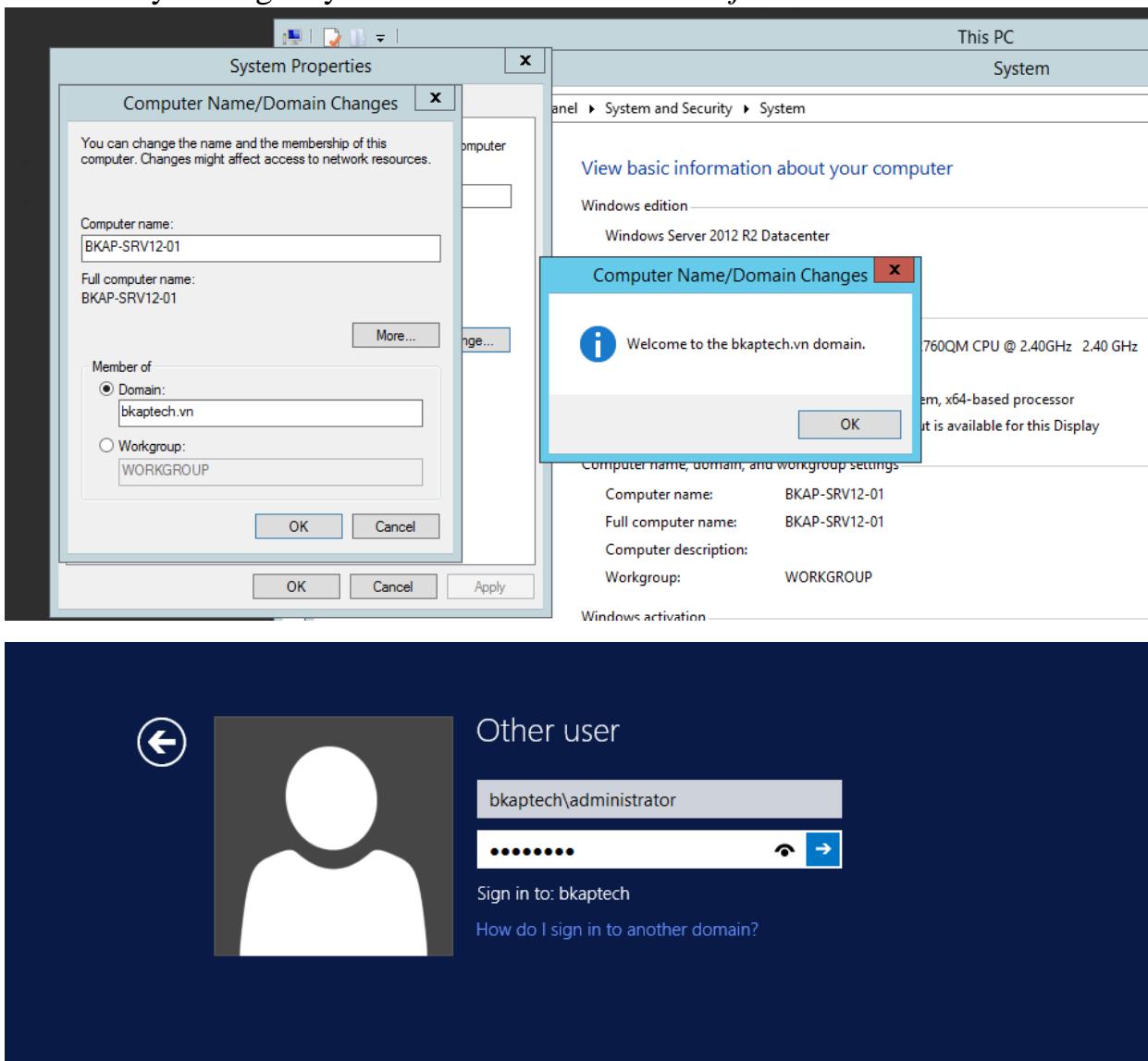




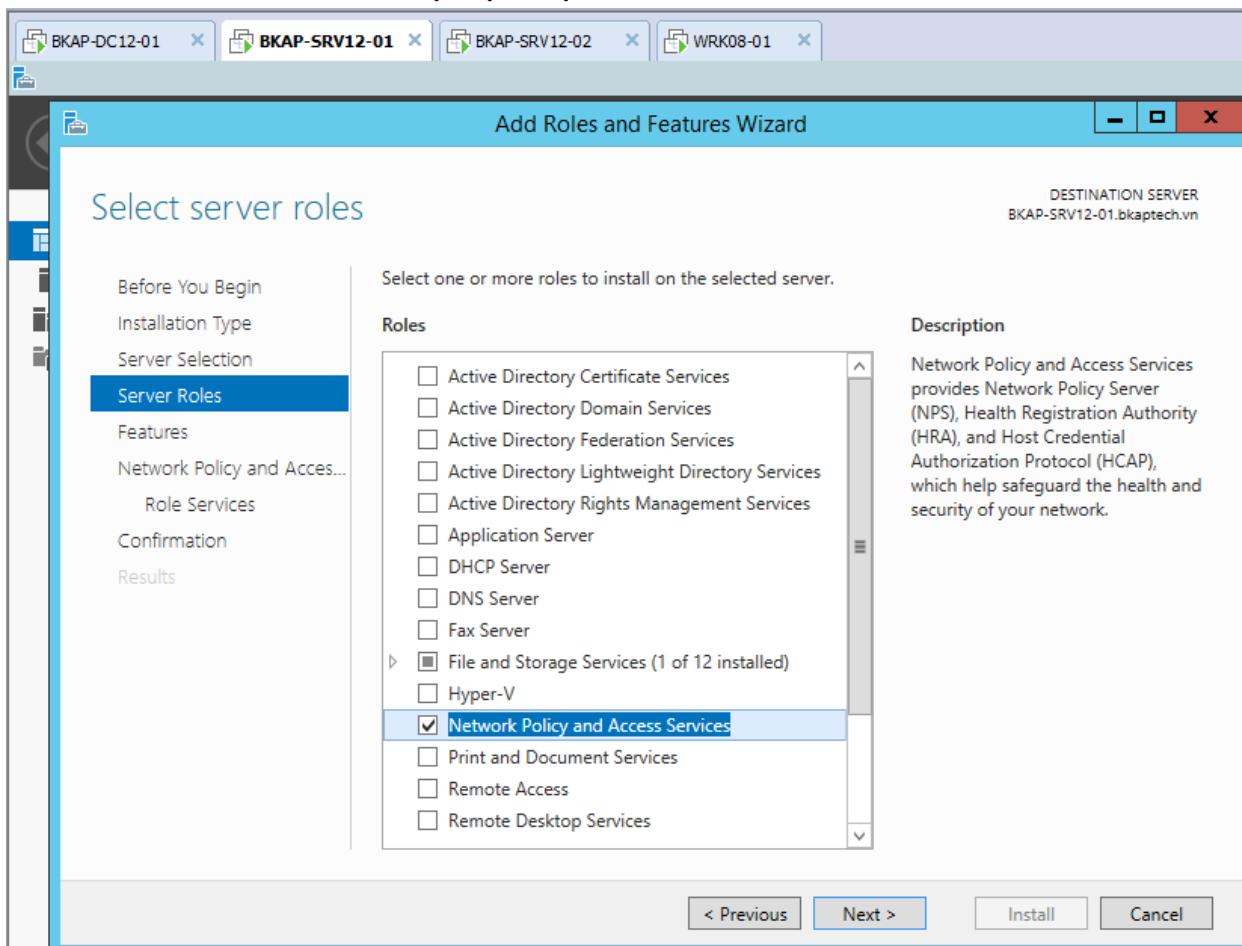
- Cho phép User truy cập VPN.



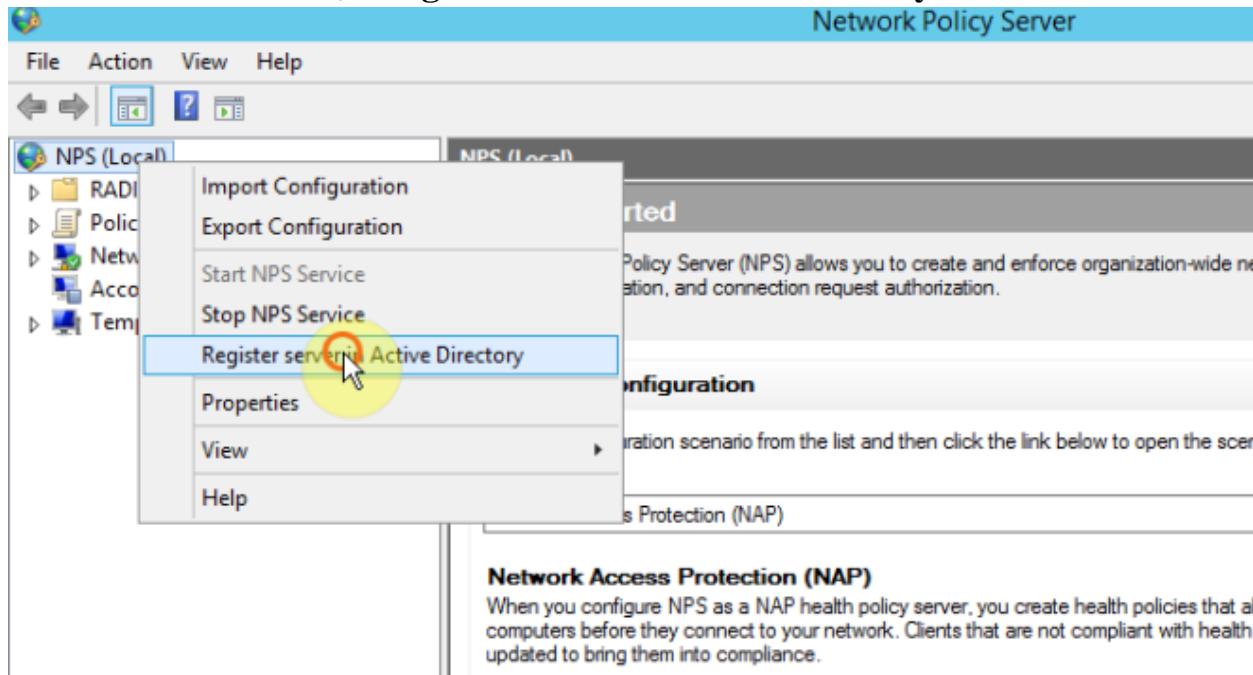
- Chuyển sang máy BKAP-SRV12-01 tiến hành *join* vào domain.



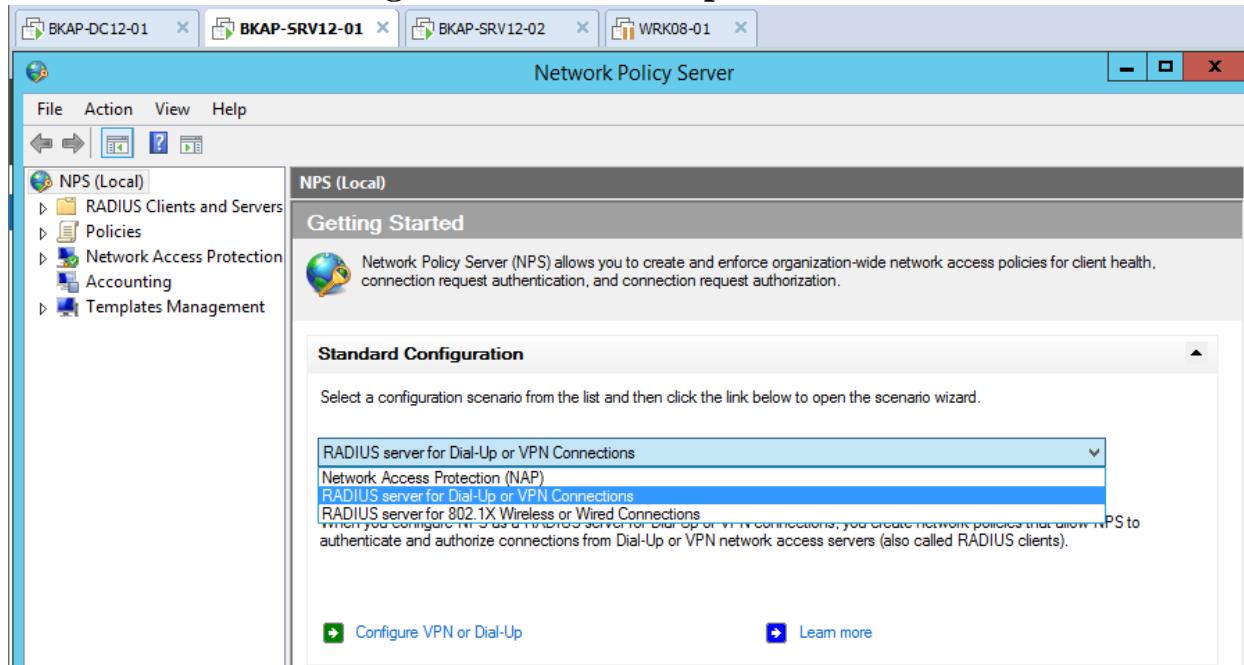
- Tiến hành cài đặt dịch vụ NPS.



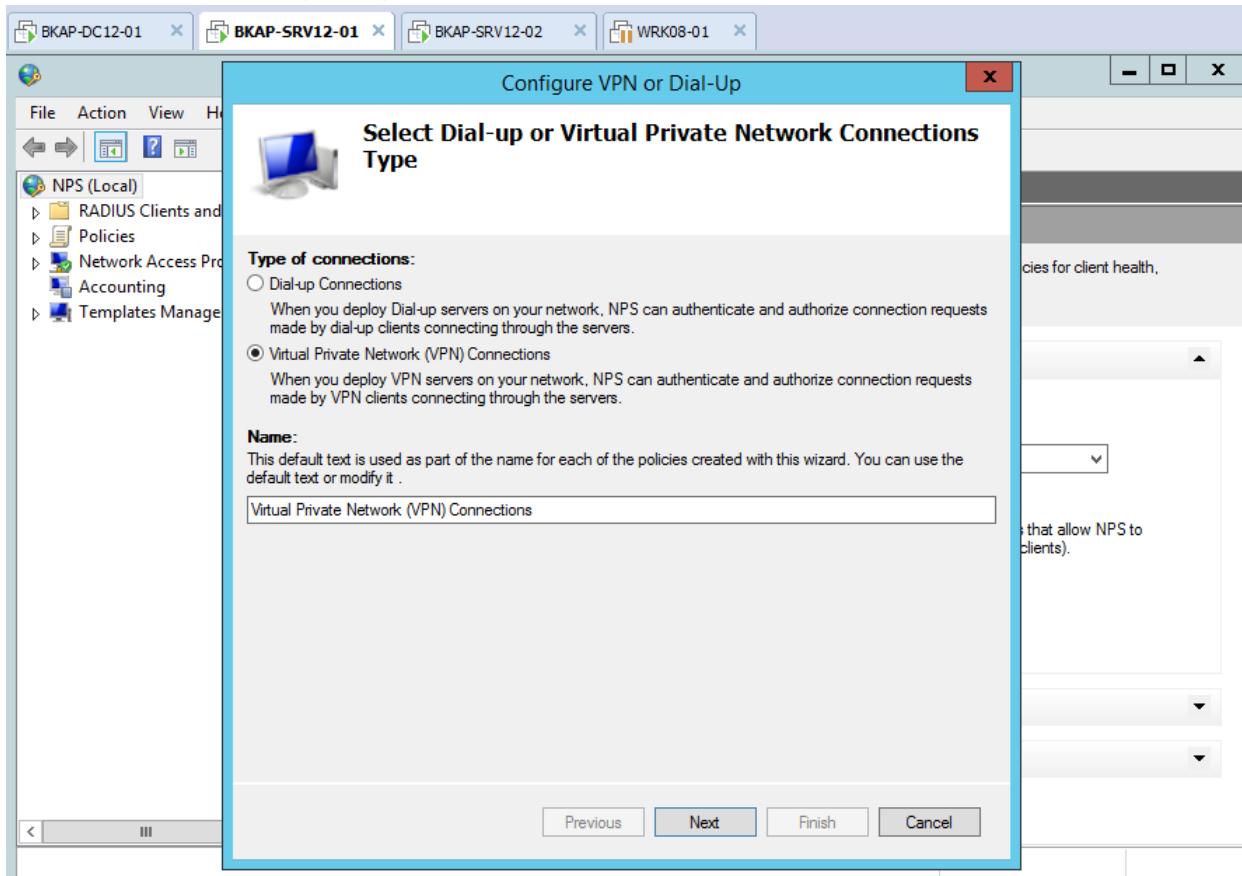
- Cấu hình dịch vụ Network Policy Server.
 - Trong cửa sổ Network Policy Server , click vào NPS (Local), chọn Register server in Active Directory.



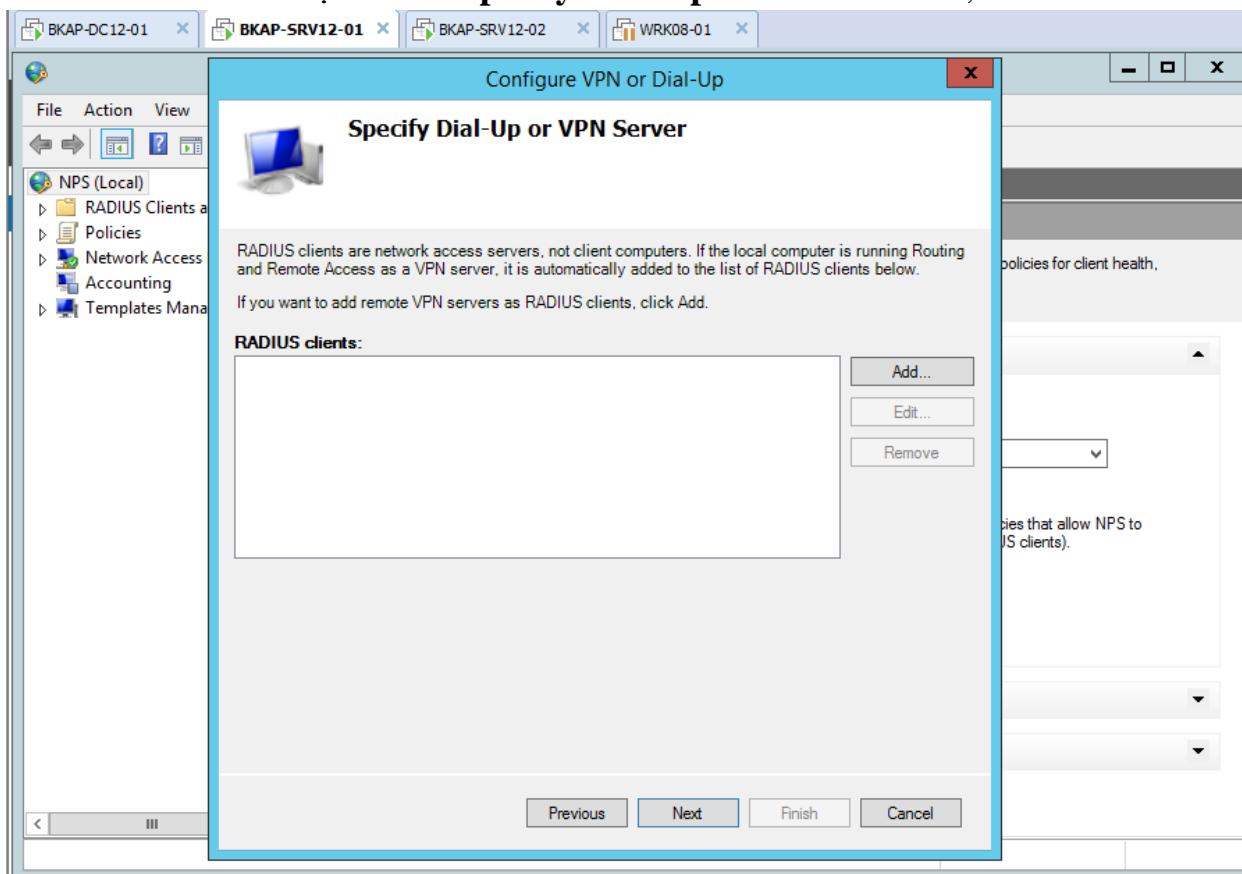
- Trong Standard Configuration , chọn vào RADIUS server for Dial-Up or VPN Connections. , => click chọn vào Configure VPN or Dial-Up.



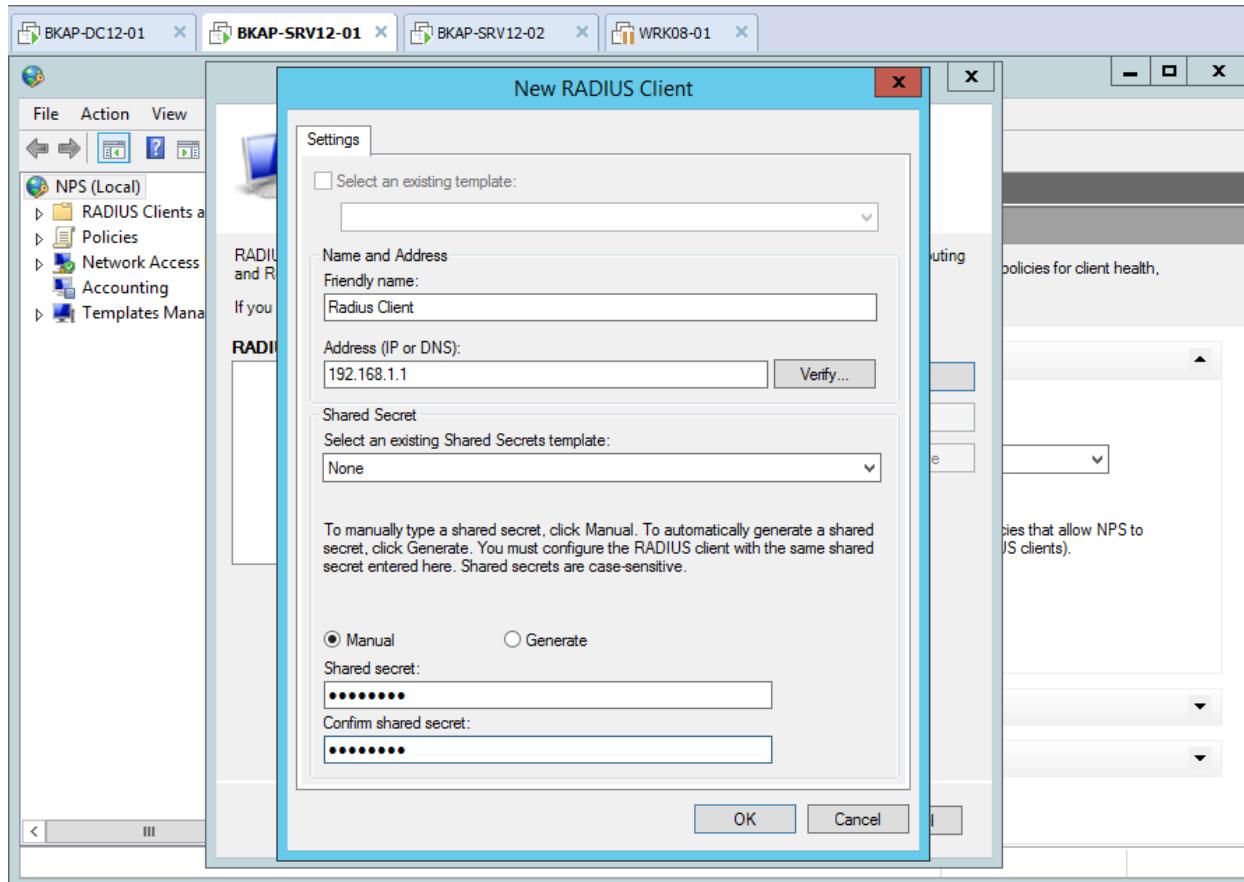
- Tại cửa sổ **Select Dial-up or Virtual Private Network Connections Type**, click chọn vào **Virtual Private Network (VPN) Connections**



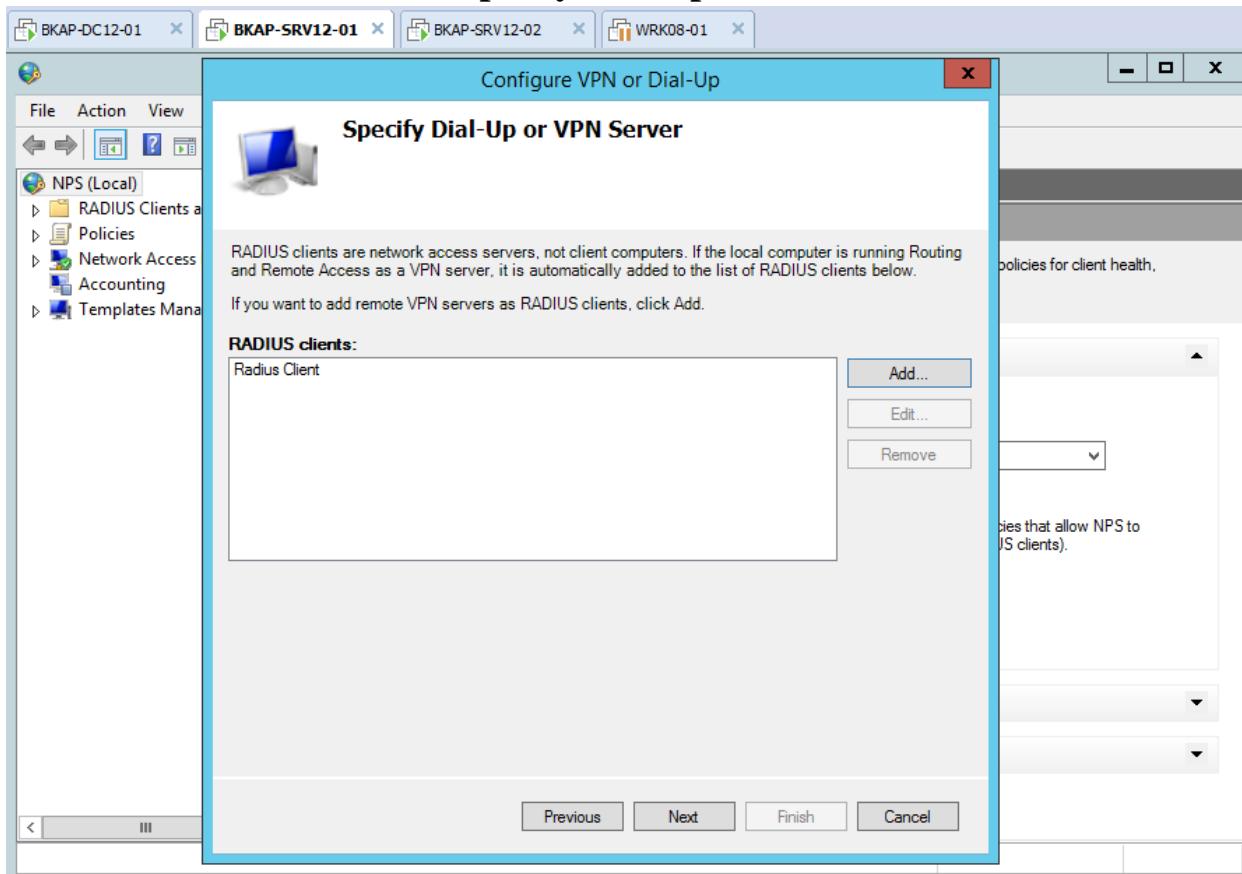
- Tại cửa sổ **Specify Dial-Up or VPN Server**, click vào **Add...**



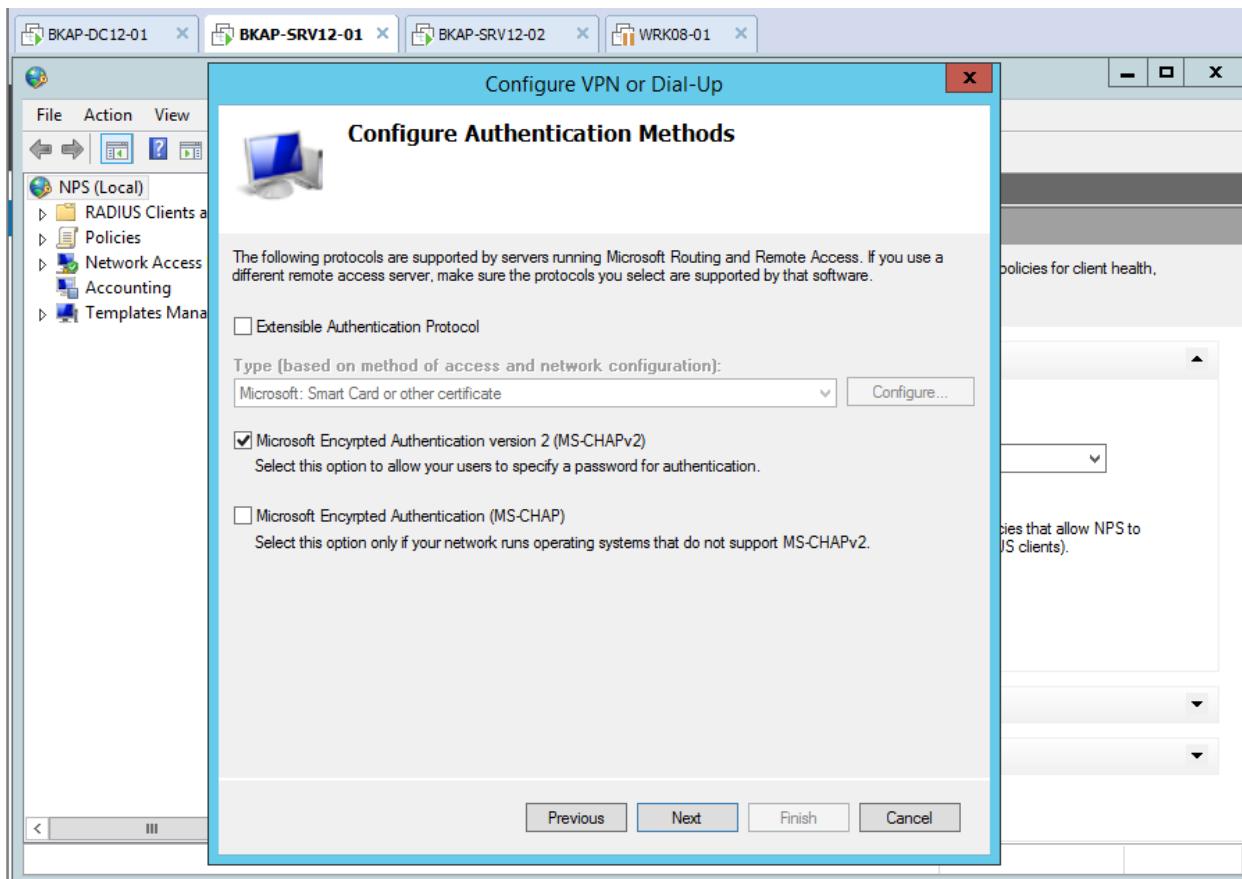
- Tại cửa sổ **New RADIUS Client** , nhập vào các thông số:
 - **Friendly name:** *Radius Client*
 - **Address (IP or DNS) :** *192.168.1.1*
 - **Shared secret:** *123456a@*



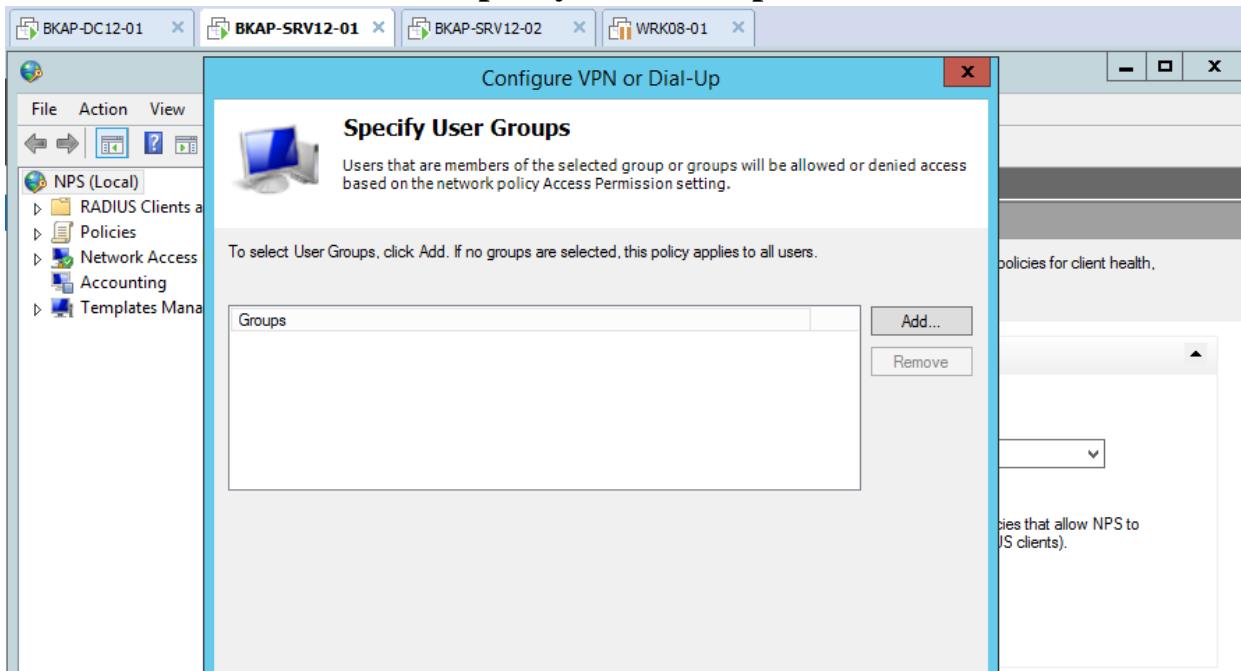
- Tại cửa sổ **Specify Dial-Up or VPN Server**, click vào **Next**.



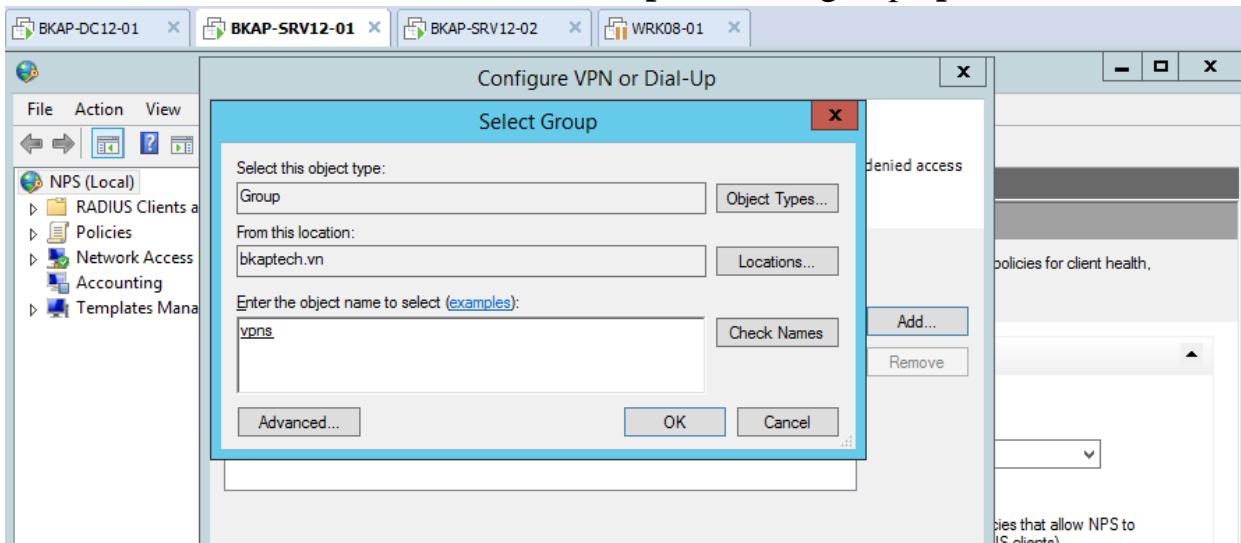
- Tại cửa sổ **Configure Authentication Methods**, click vào **Next**.



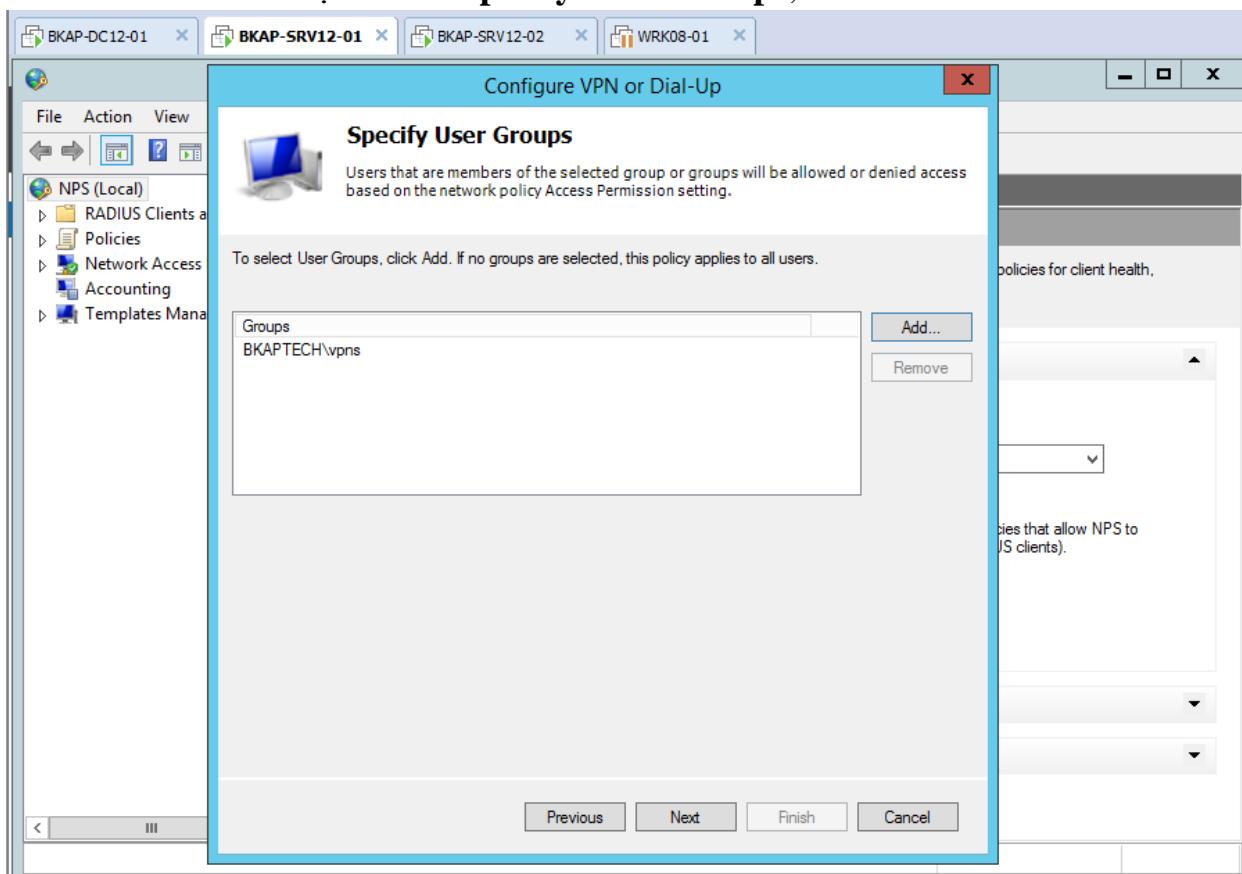
- Tại cửa sổ **Specify User Groups**, click vào Add...



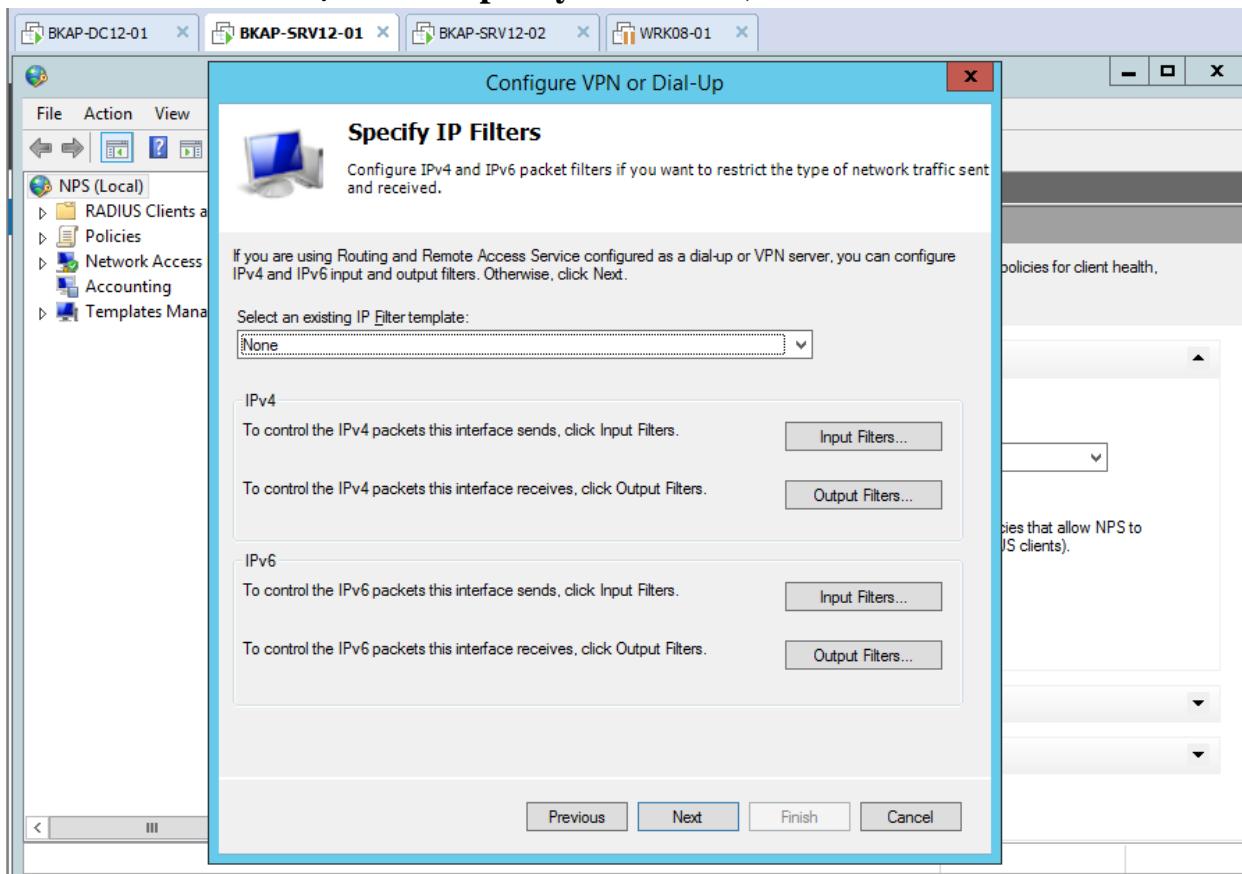
- Tại cửa sổ **Select Group**, add vào group vpns.



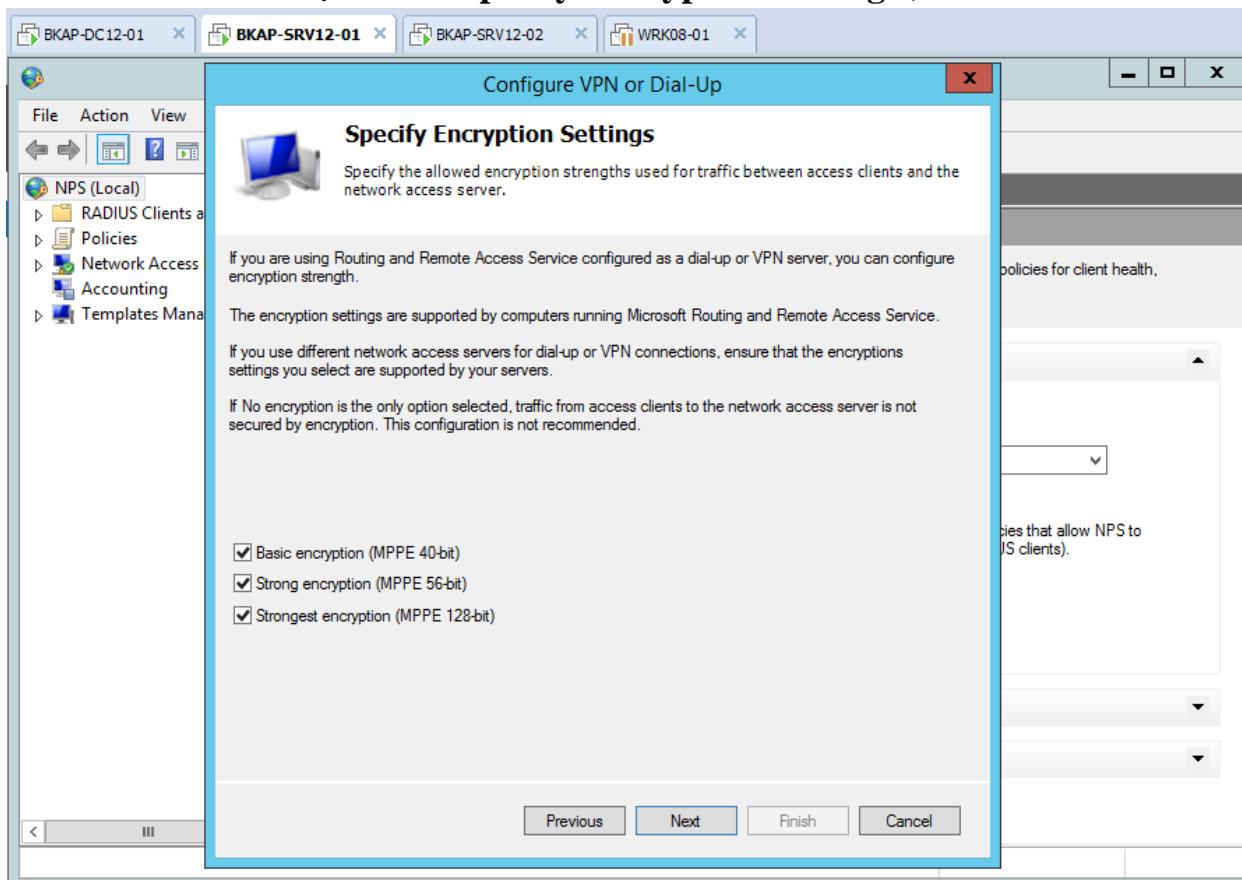
- Tại cửa sổ **Specify User Groups**, click vào **Next**.



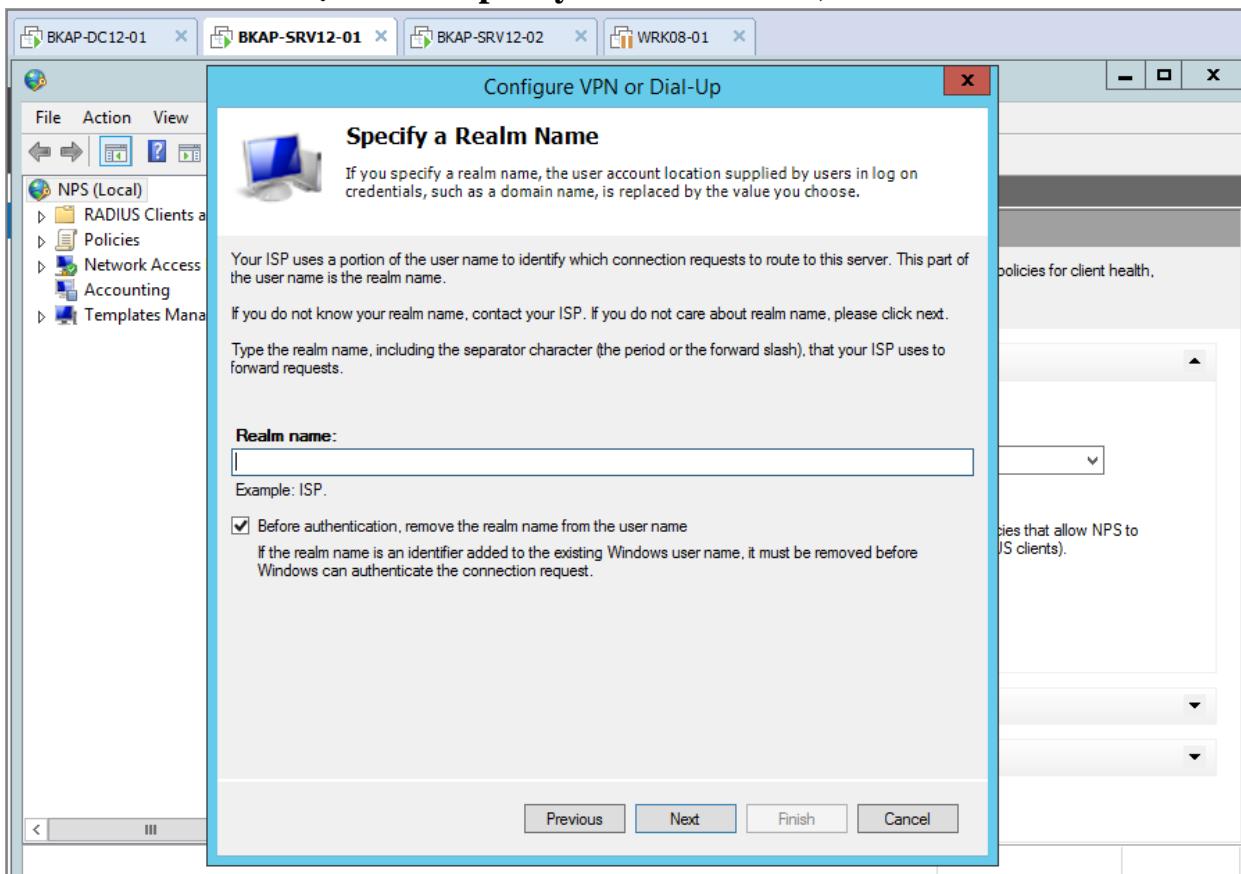
- Tại cửa sổ **Specify IP Filters**, click vào **Next**.



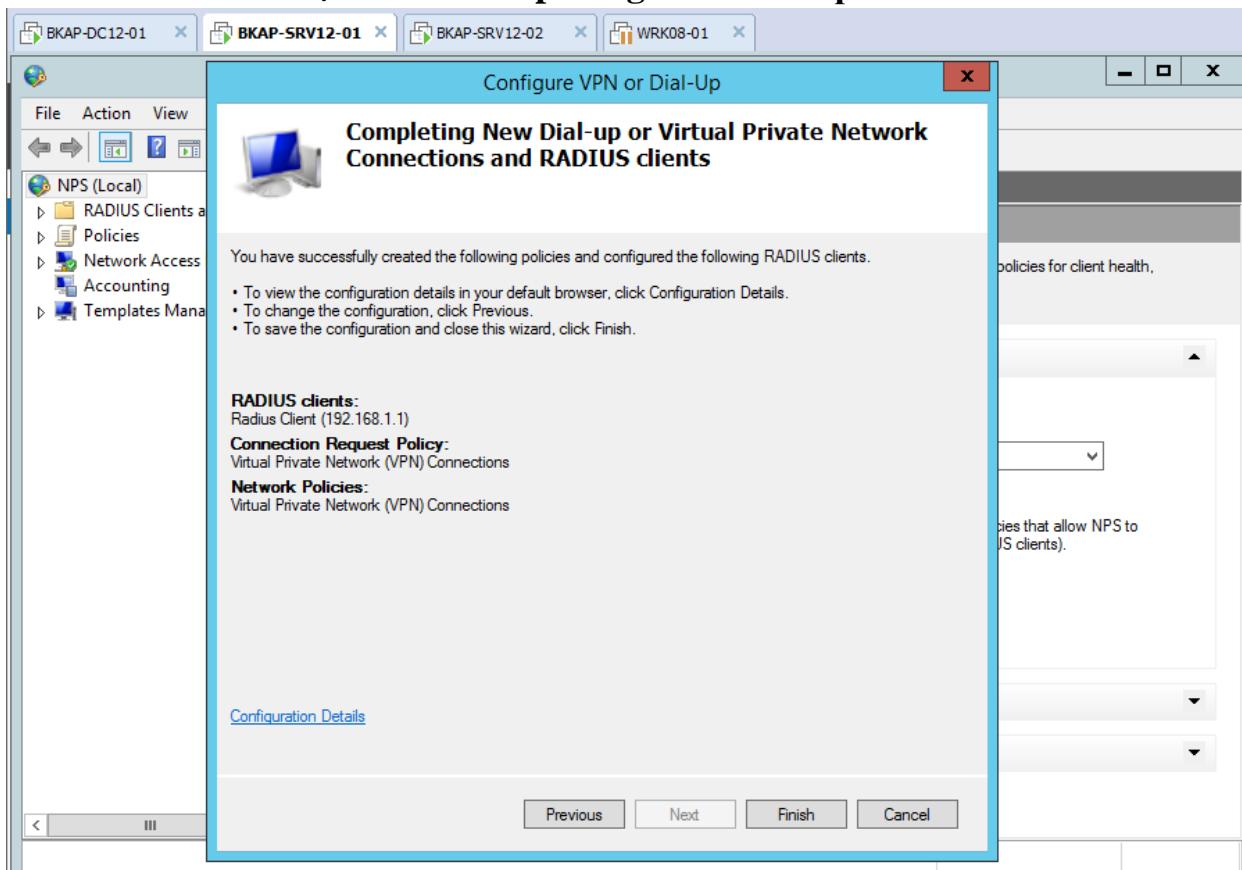
- Tại cửa sổ **Specify Encryption Settings**, click vào **Next**.



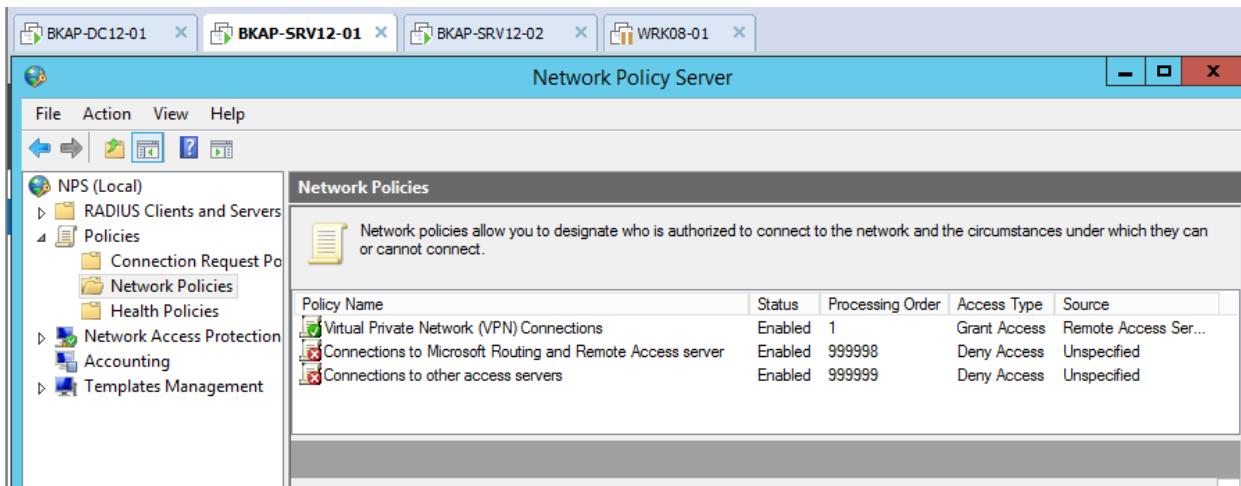
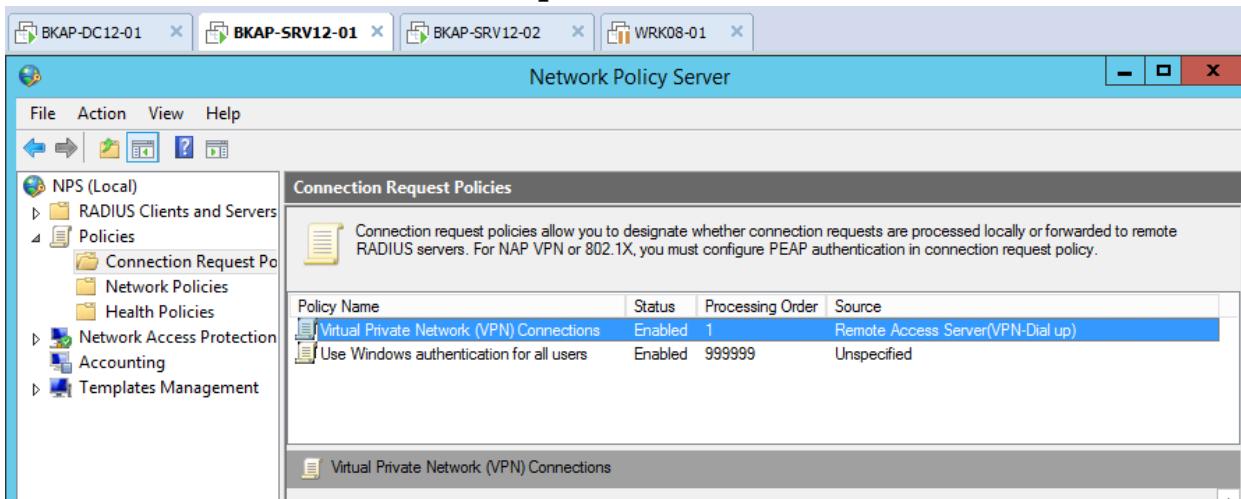
- Tại cửa sổ **Specify a Realm Name**, click vào **Next**.



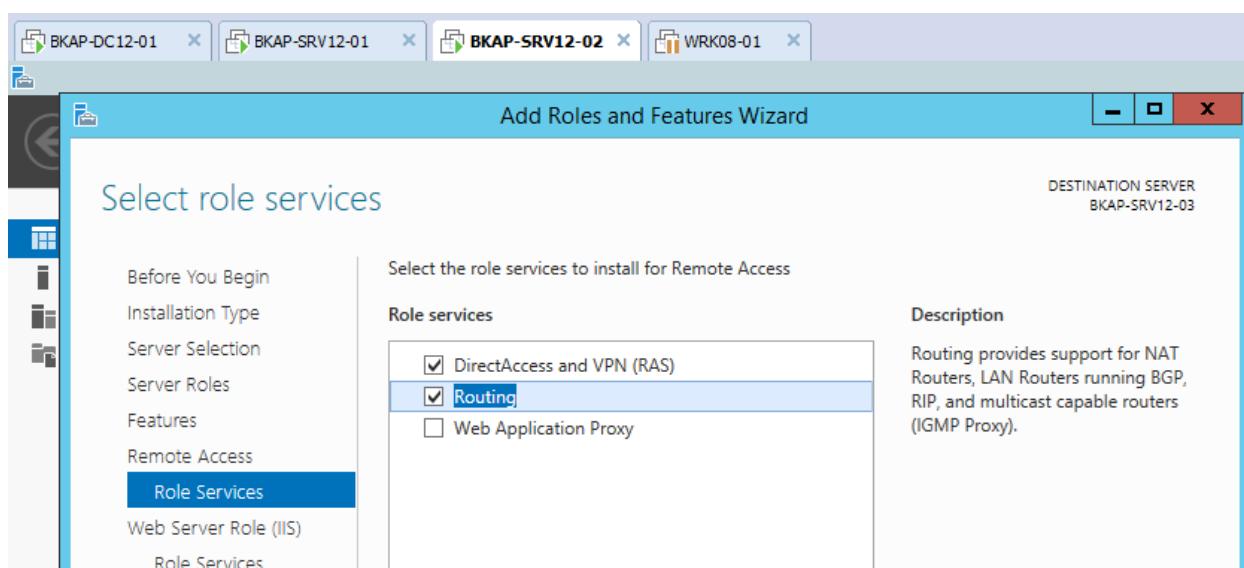
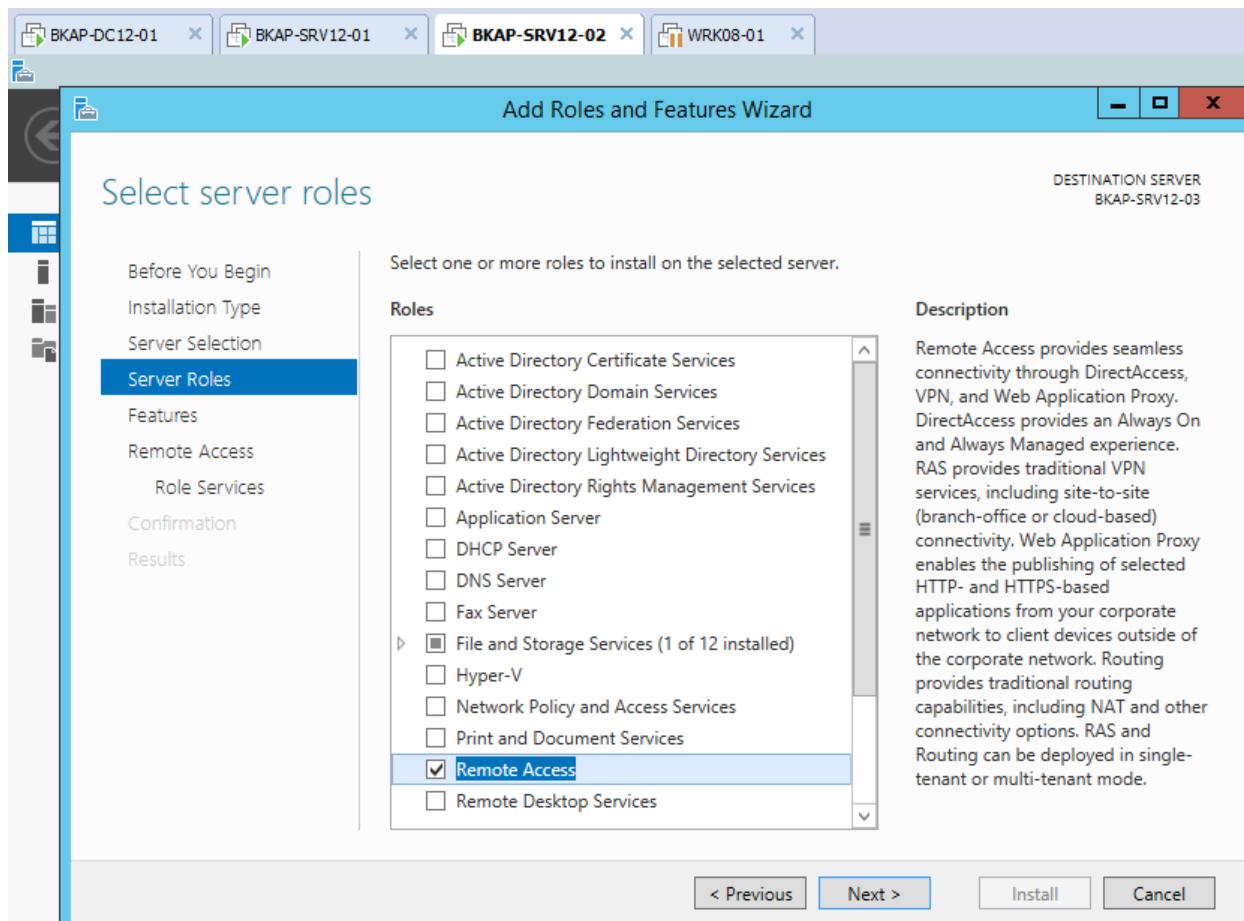
- Tại cửa sổ **Completing New Dial-up...** click vào **Finish**.



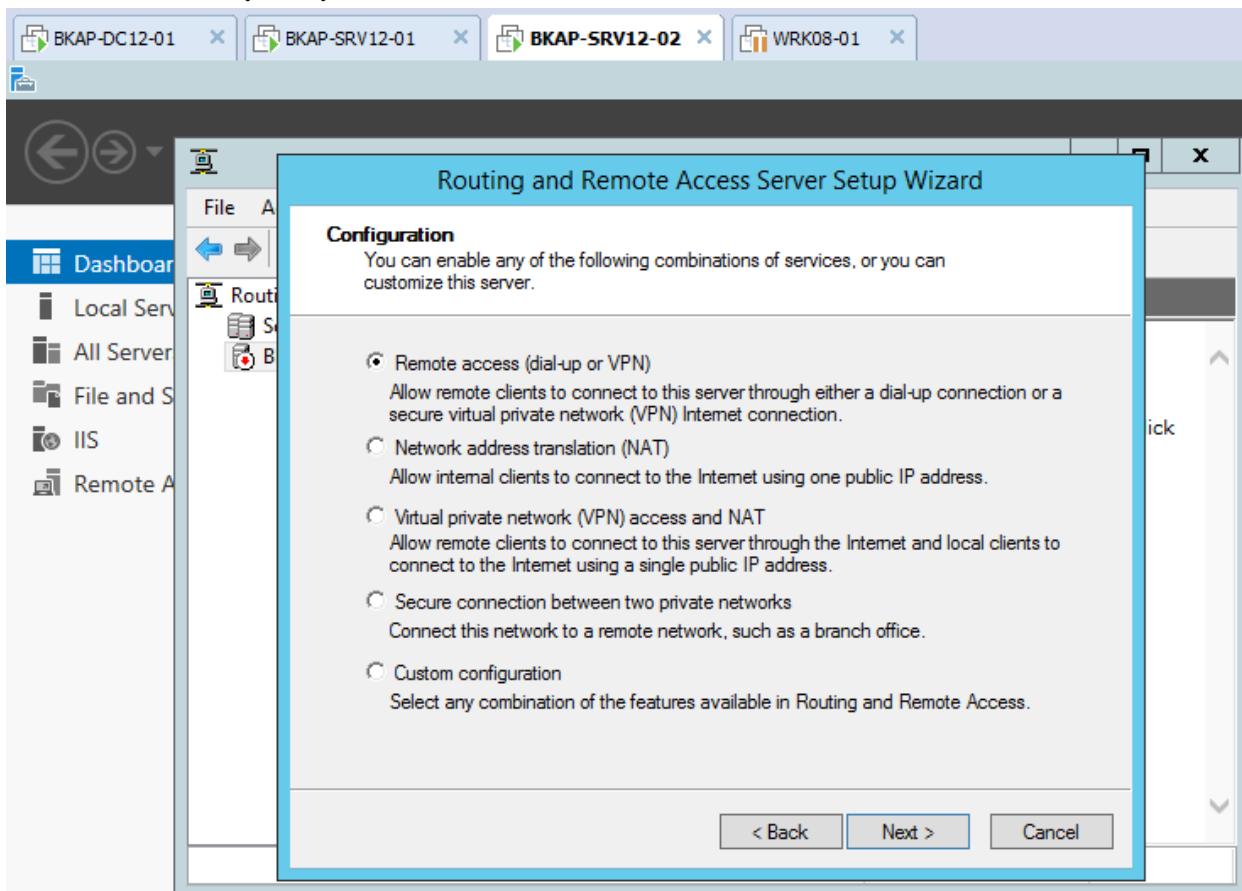
- Tại cửa sổ **Network Policy Server**, click vào **Policies / Connection Request Policies**, kiểm tra chính sách được tạo.

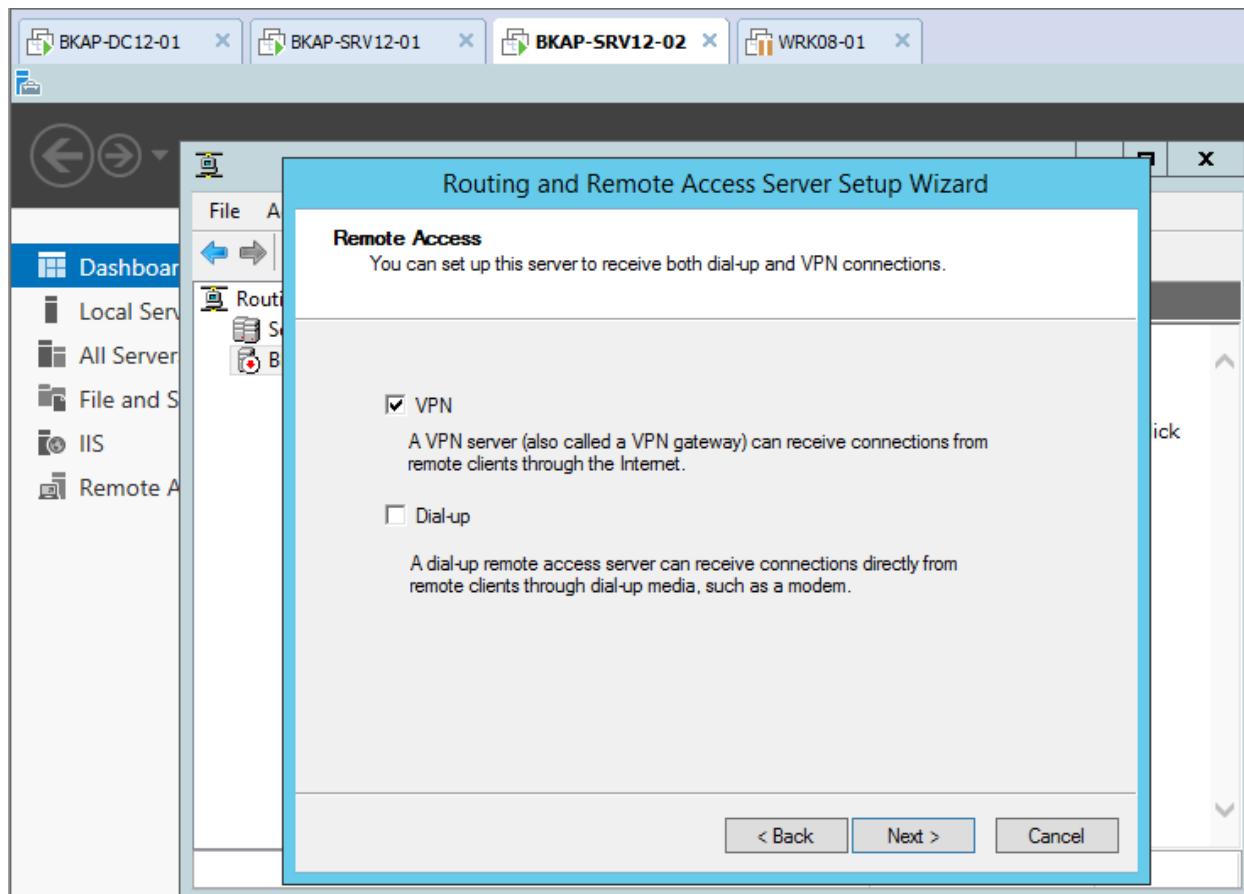


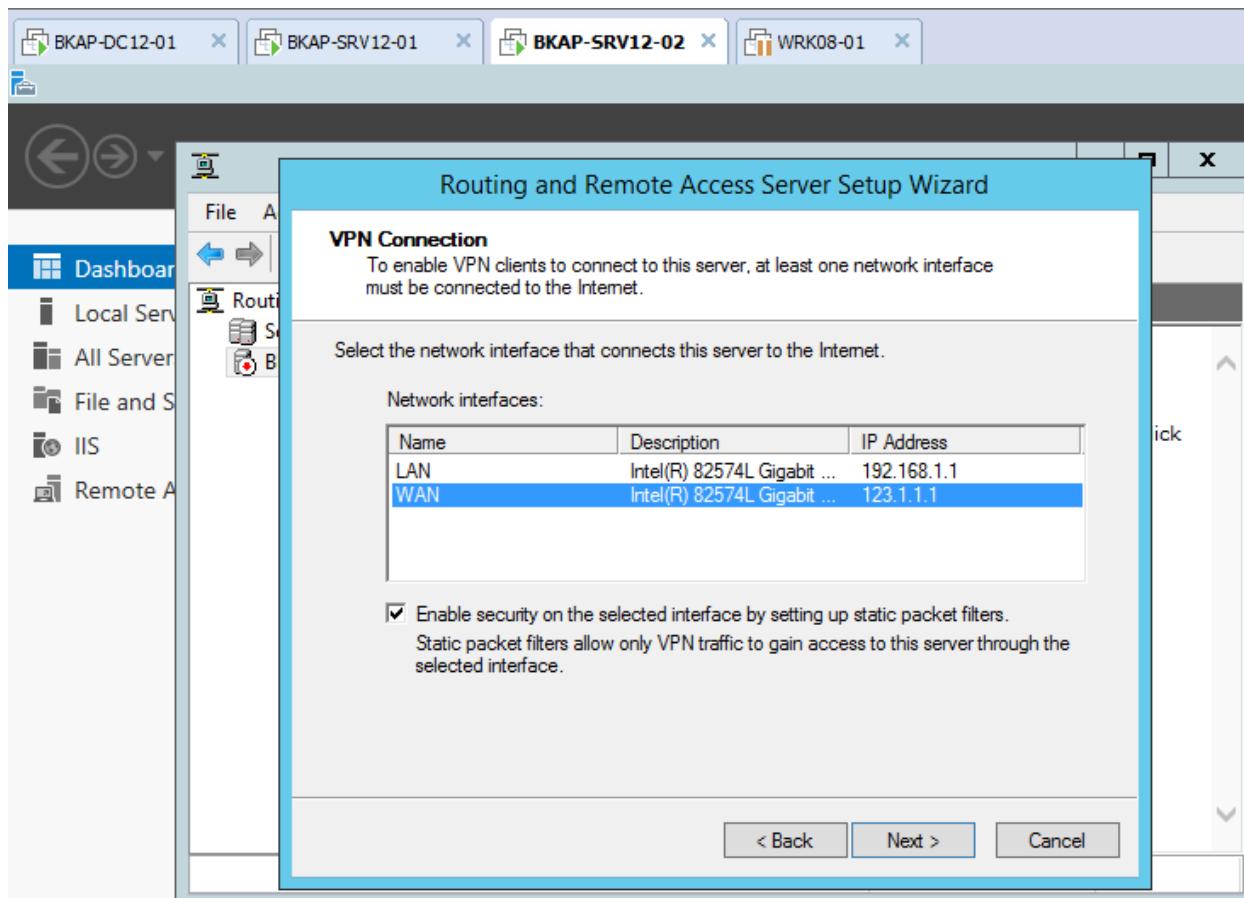
- Chuyển qua server **BKAP-SRV12-02**, thực hiện cài đặt dịch vụ **Remote Access / Routing**.

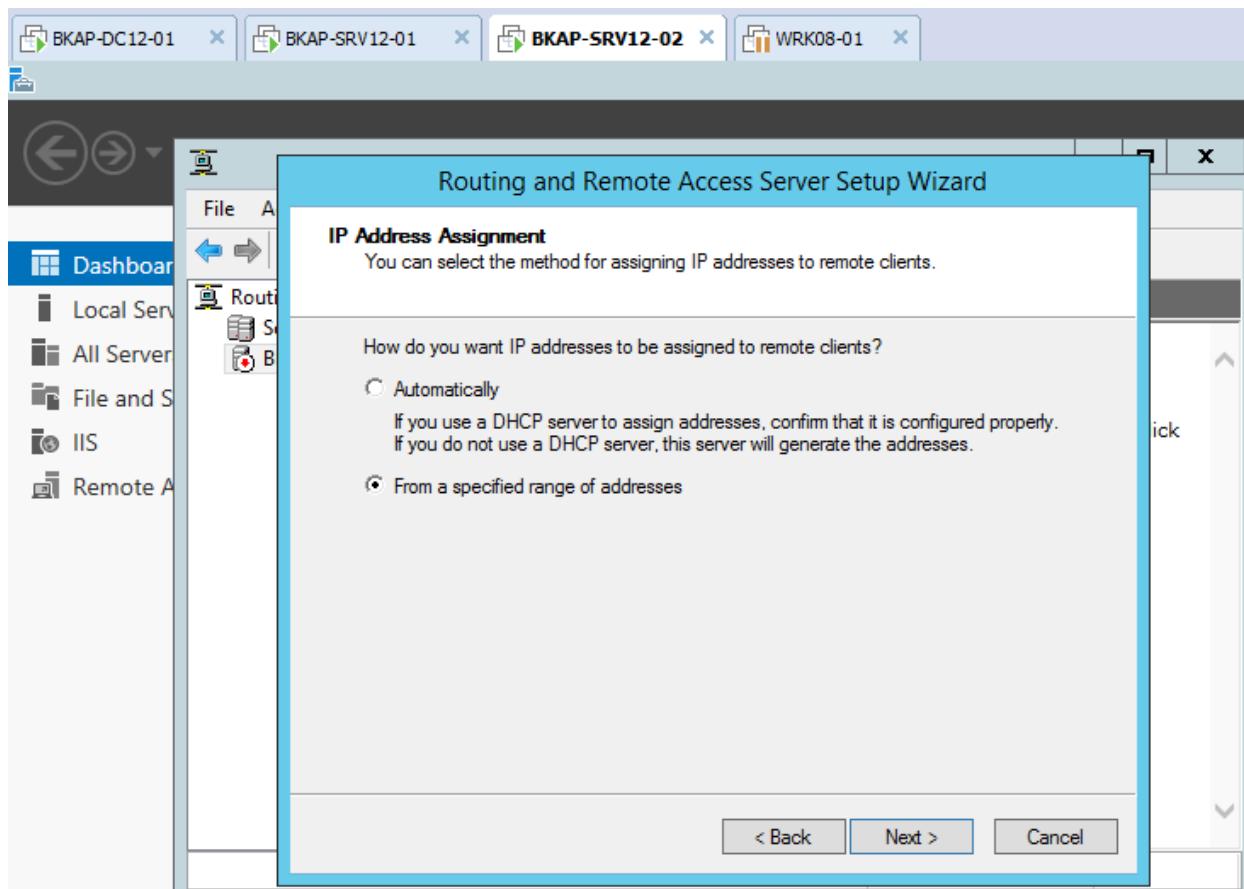


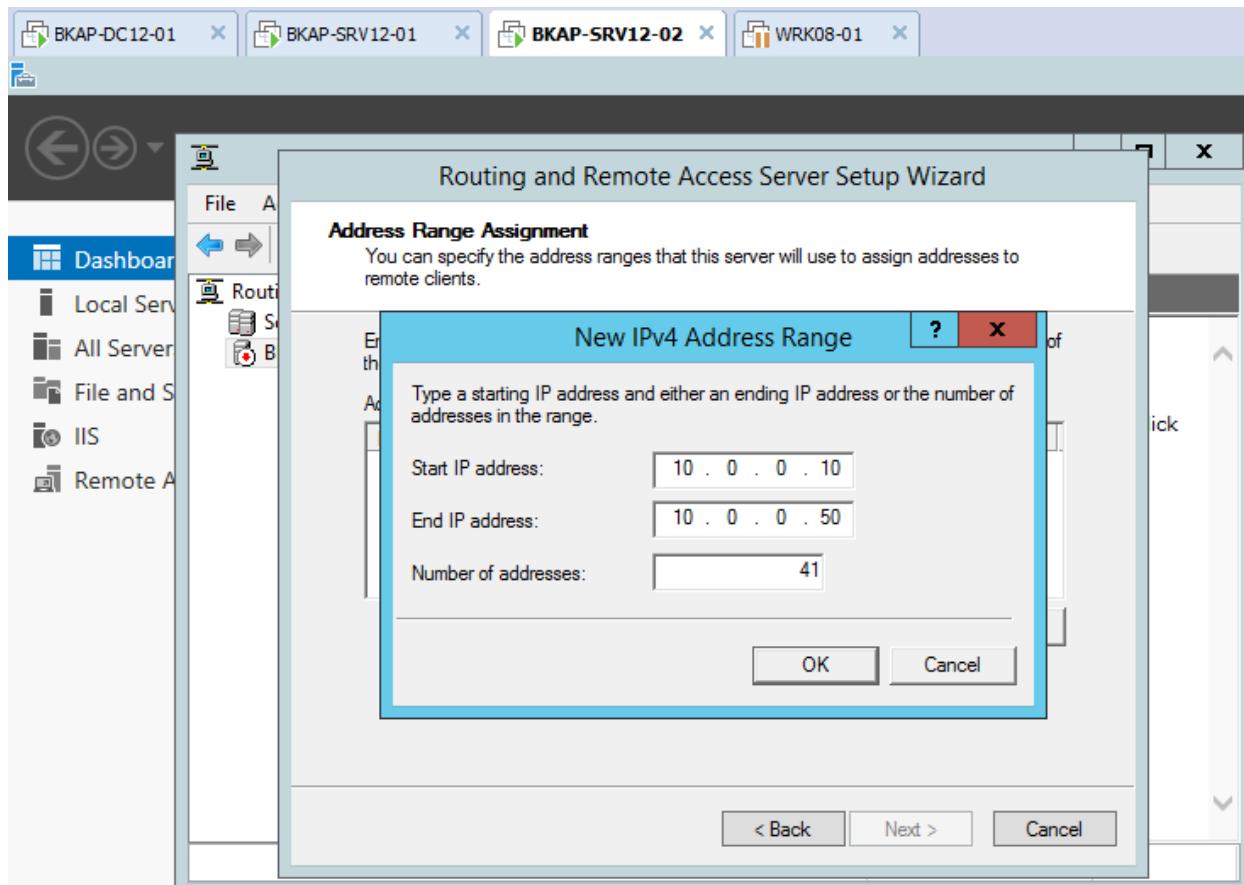
o Thực hiện cấu hình VPN Server :

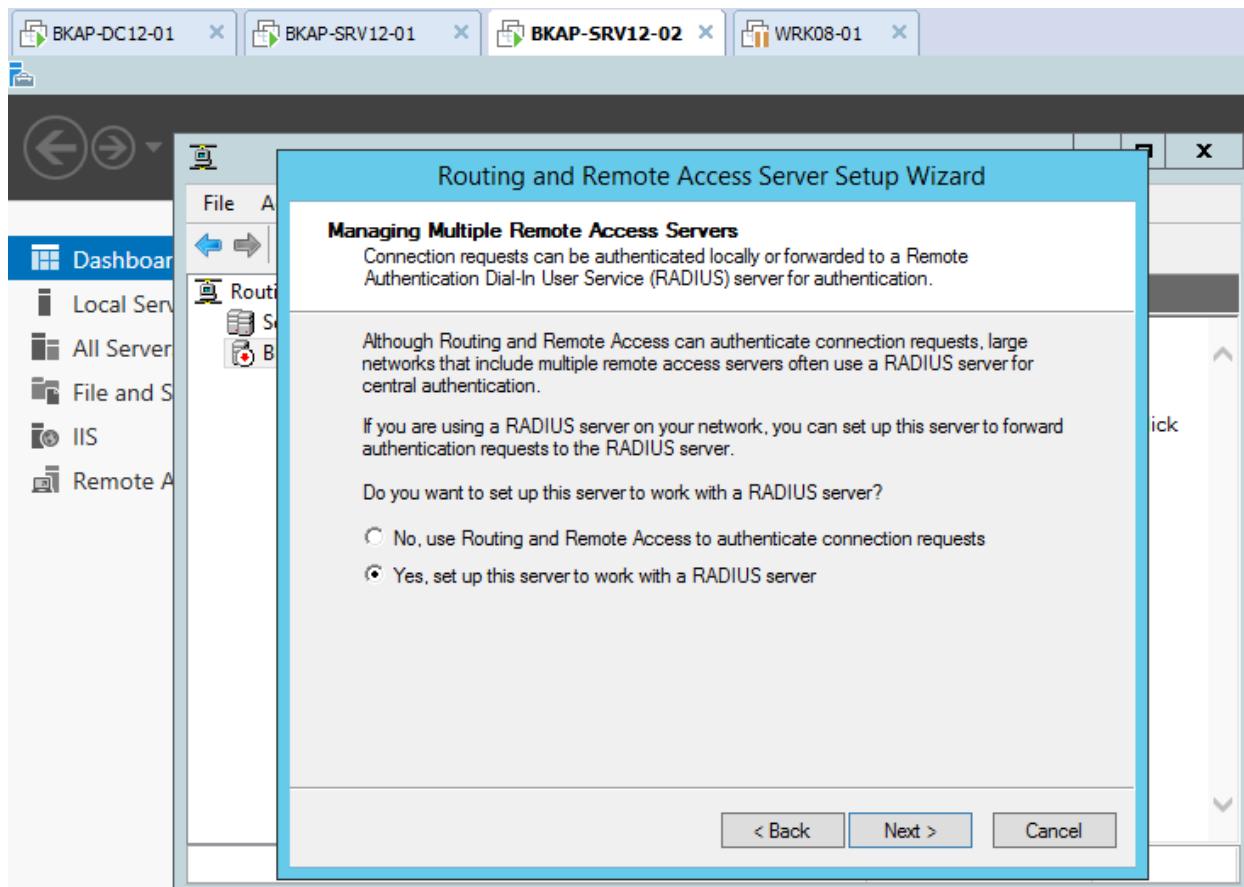


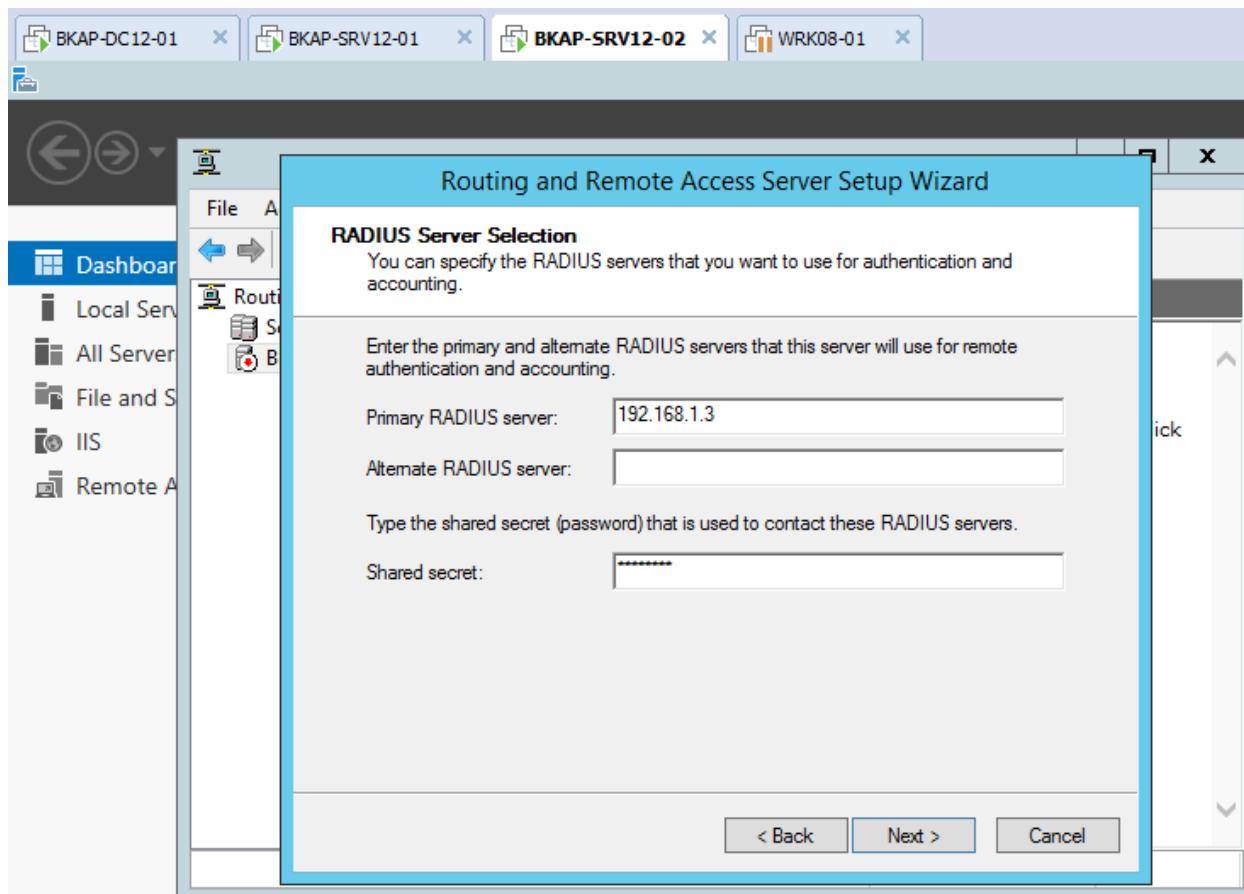


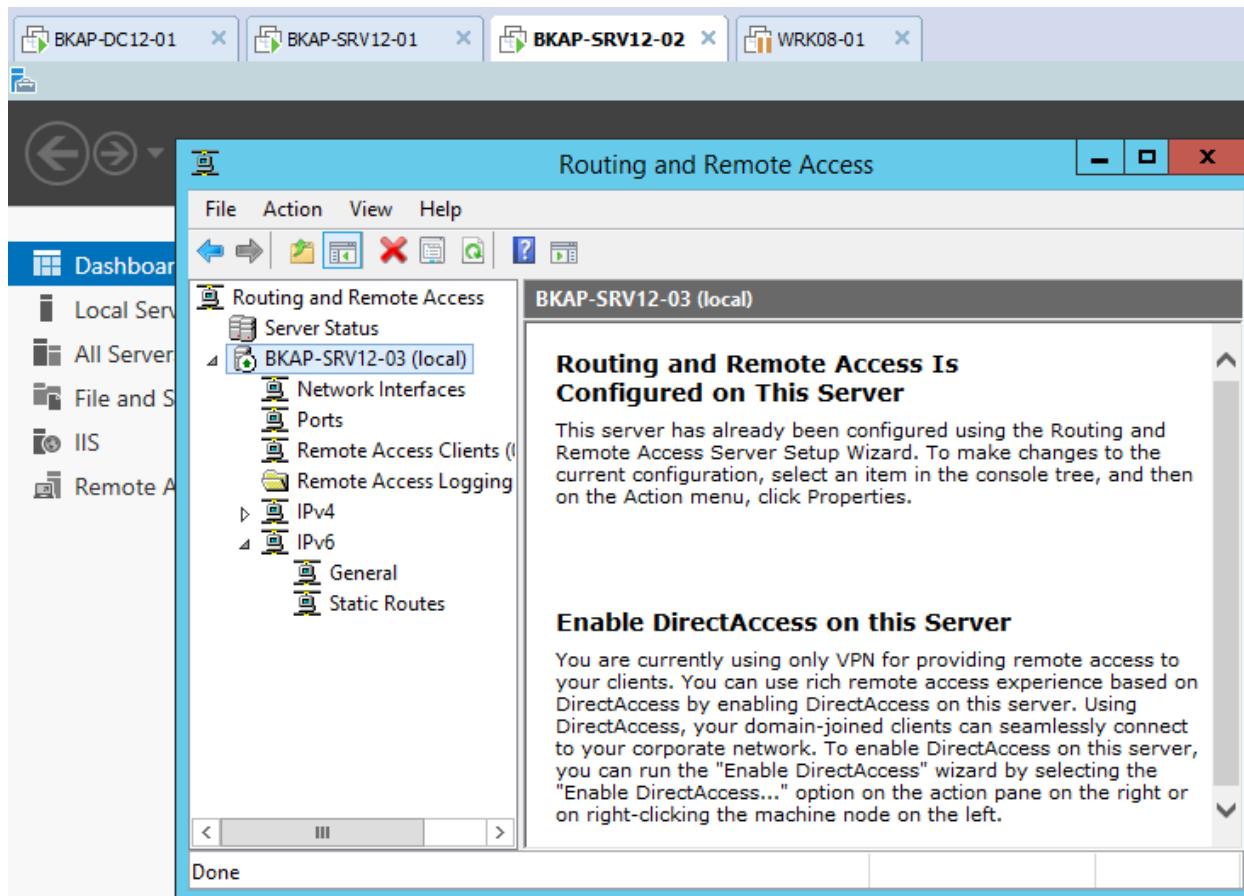




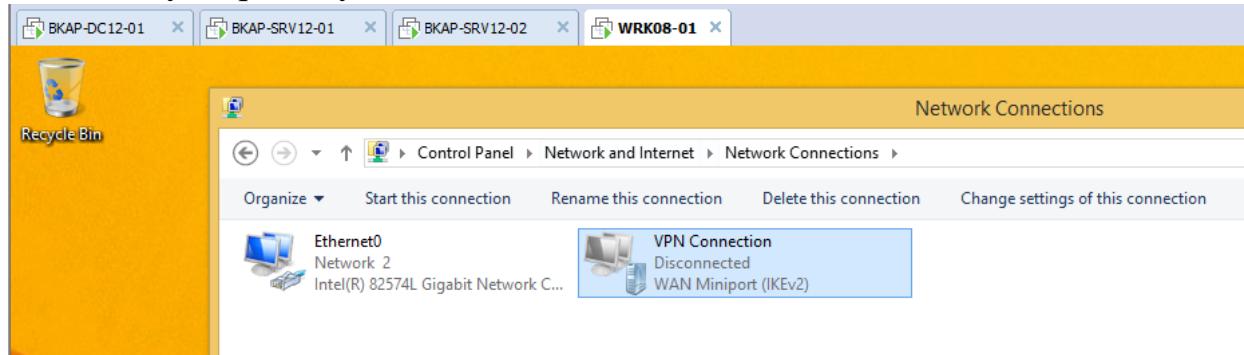




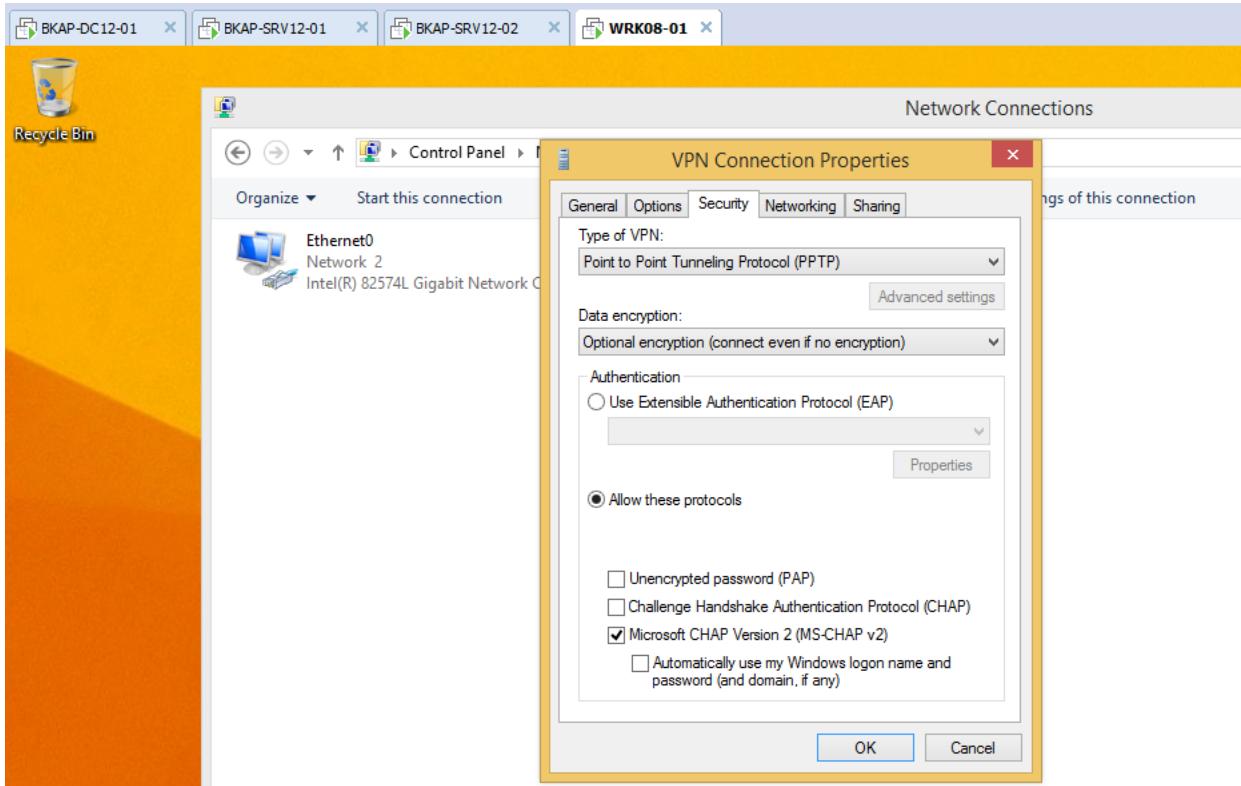




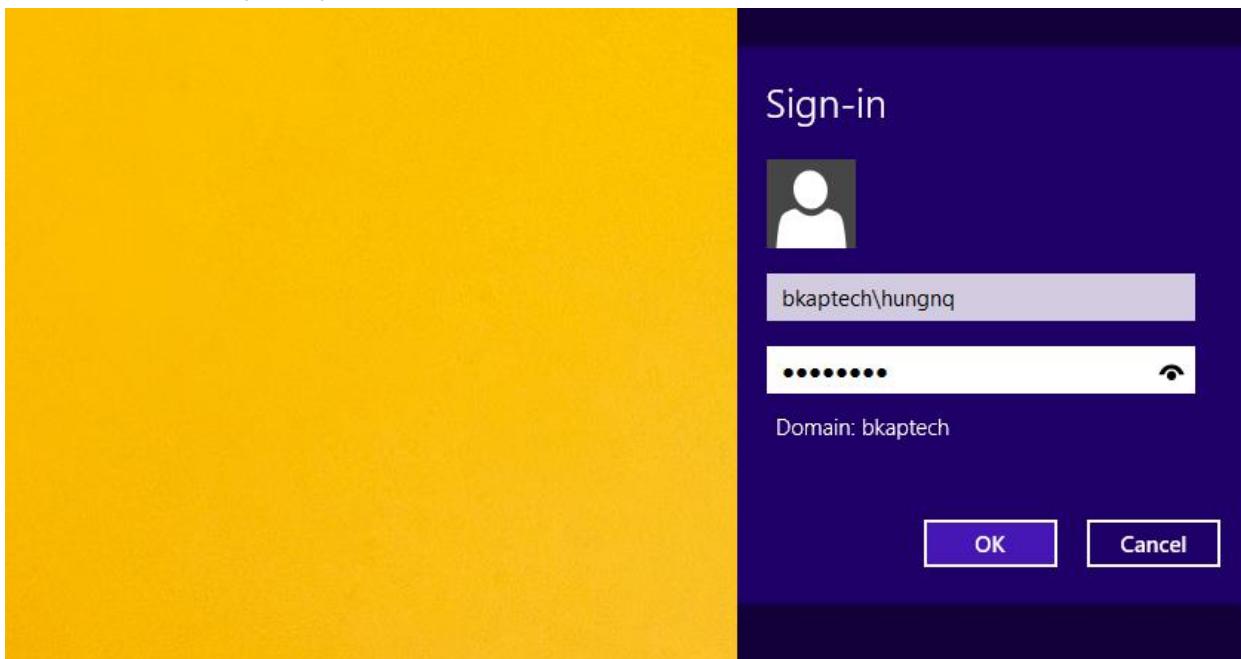
- Chuyển qua máy trạm **BKAP-WRK08-01**, thực hiện tạo kết nối **VPN Client**.



- Tại cửa sổ *VPN Connection Properties*, tại mục *Type of VPN*, chọn vào giao thức **PPTP**.
 - Click chọn vào **Allow these protocols => OK.**

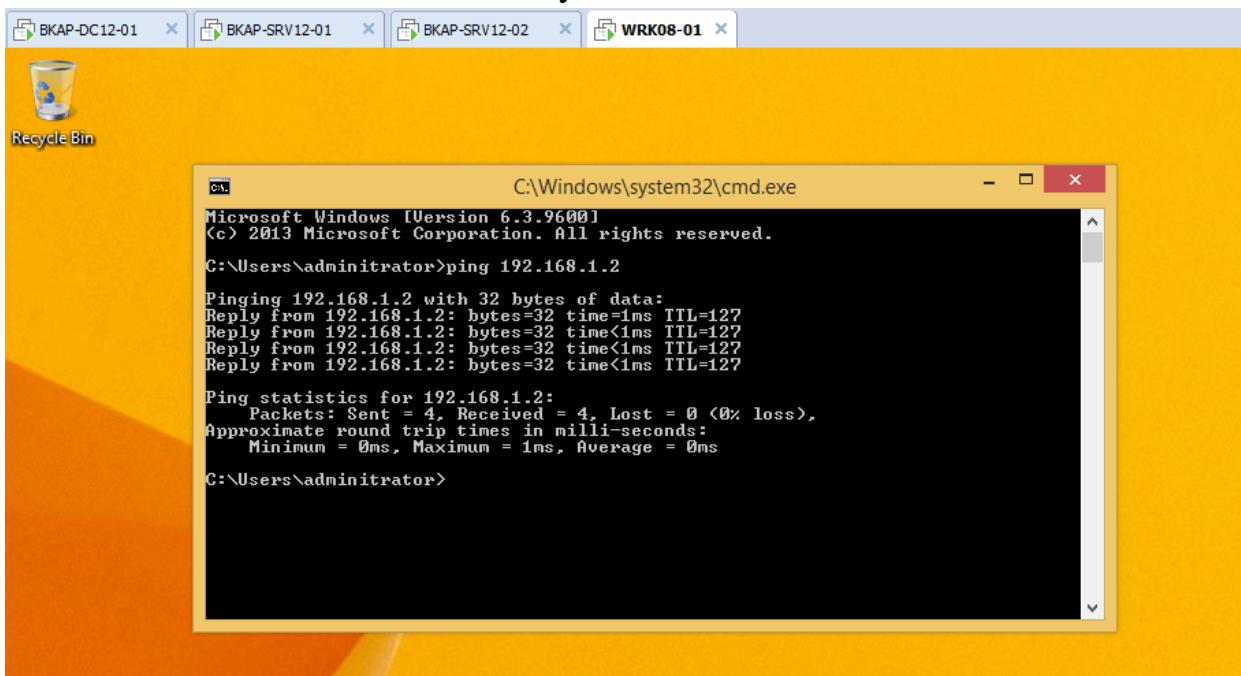


- Thực hiện kết nối **VPN**.

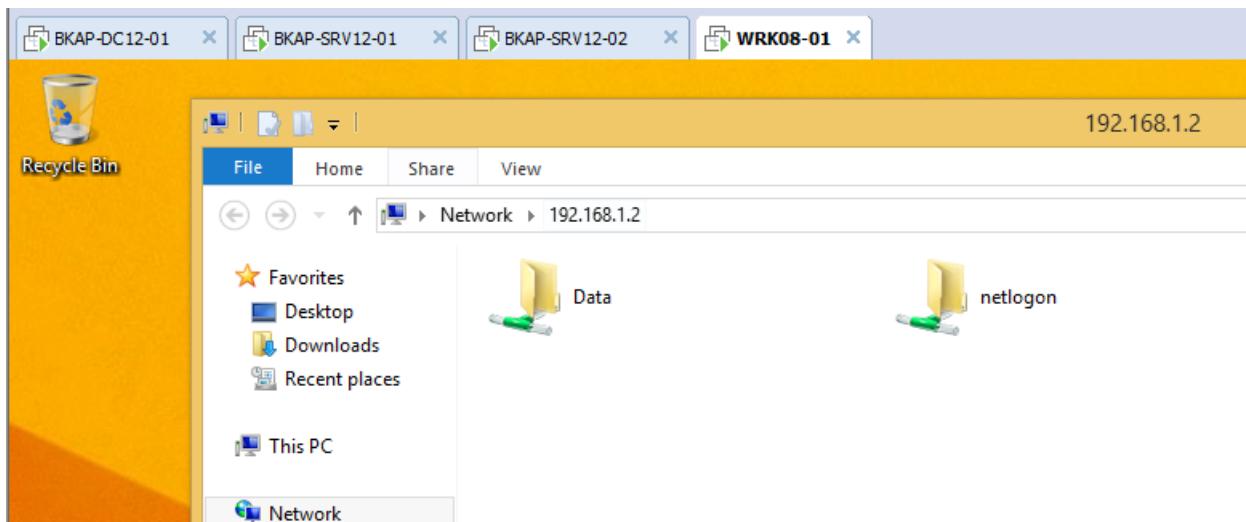




- Kiểm tra kết nối đến máy BKAP-DC12-01.



- Thực hiện truy cập tài nguyên :



Bài 9:**TRIỂN KHAI DỊCH VỤ NETWORK ACCESS PROTECTION****Các nội dung chính sẽ được đề cập:**

- ✓ Triển khai cài đặt và cấu hình dịch vụ NAP DHCP.
- ✓ Triển khai cài đặt và cấu hình dịch vụ NAP VPN.

9.1 Triển khai cài đặt và cấu hình dịch vụ NAP DHCP.**1. Yêu cầu bài lab:**

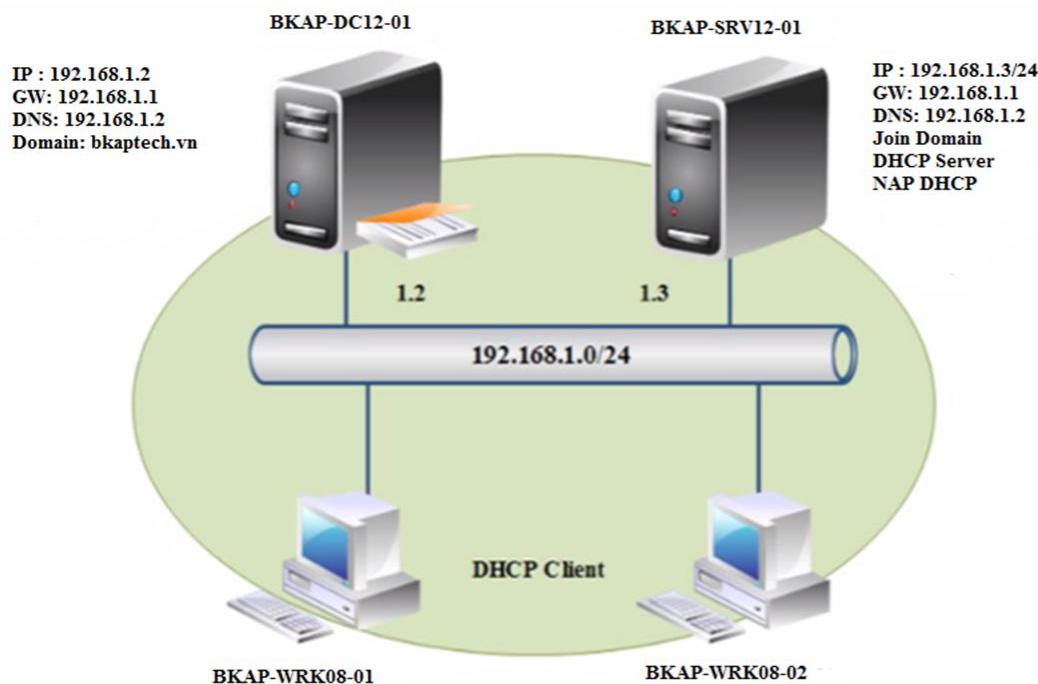
** Cấu hình **Network Access Protection (NAP)** để đưa ra các điều kiện bảo mật trong hệ thống **DHCP** :

- Các máy **Client** an toàn sẽ được **DHCP Server** cung cấp đầy đủ thông số **TCP/IP**.
 - Các máy *Client* không an toàn sẽ không được **DHCP Server** cung cấp **Default Gateway**.
- + Trên máy **BKAP-DC12-01** : xây dựng **Domain Controller** quản lý miền **bkaptech.vn** và **DNS Server**, triển khai **GPO** để cấu hình **NAP Client**.
- + Trên máy **BKAP-SRV12-01** :
- Join Domain :**bkaptech.vn**.
 - Cài đặt và cấu hình **DHCP Server**.
 - Cài đặt **Network Policy and Access Services**.
 - Cấu hình **NAP health policy server**.
 - Cấu hình **NAP enforcement** trên **DHCP Server**.
 - Cấu hình **System Health validator**.
- + Trên máy **BKAP-WRK08-01**:
- Cấu hình máy **Client** nhận IP từ **DHCP**.
 - Máy **Client** kiểm tra kết quả.
- 2. Yêu cầu chuẩn bị:**
- + Máy Server **BKAP-DC12-01**: Windows Server 2012 đã nâng cấp lên Domain Controller quản lý miền **bkaptech.vn**.
- + Máy Server **BKAP-SRV12-01** : Join Domain.
- + Máy Client **BKAP-WRK08-01** : Join Domain.

3. Mô hình lab:

HỆ THỐNG ĐÀO TẠO CNTT QUỐC TẾ BACHKHOA-APTECH

Lab 9.1 Triển khai cài đặt và cấu hình NAP DHCP



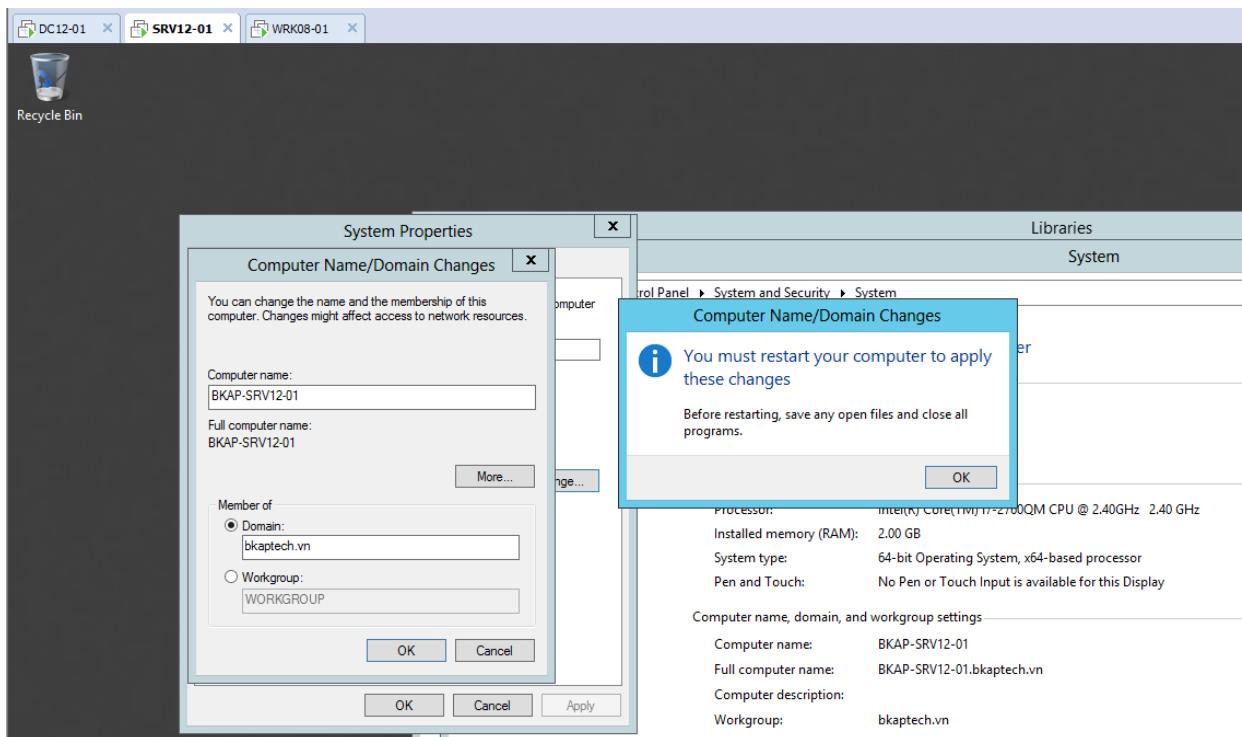
Hình 9.1

Sơ đồ địa chỉ như sau:

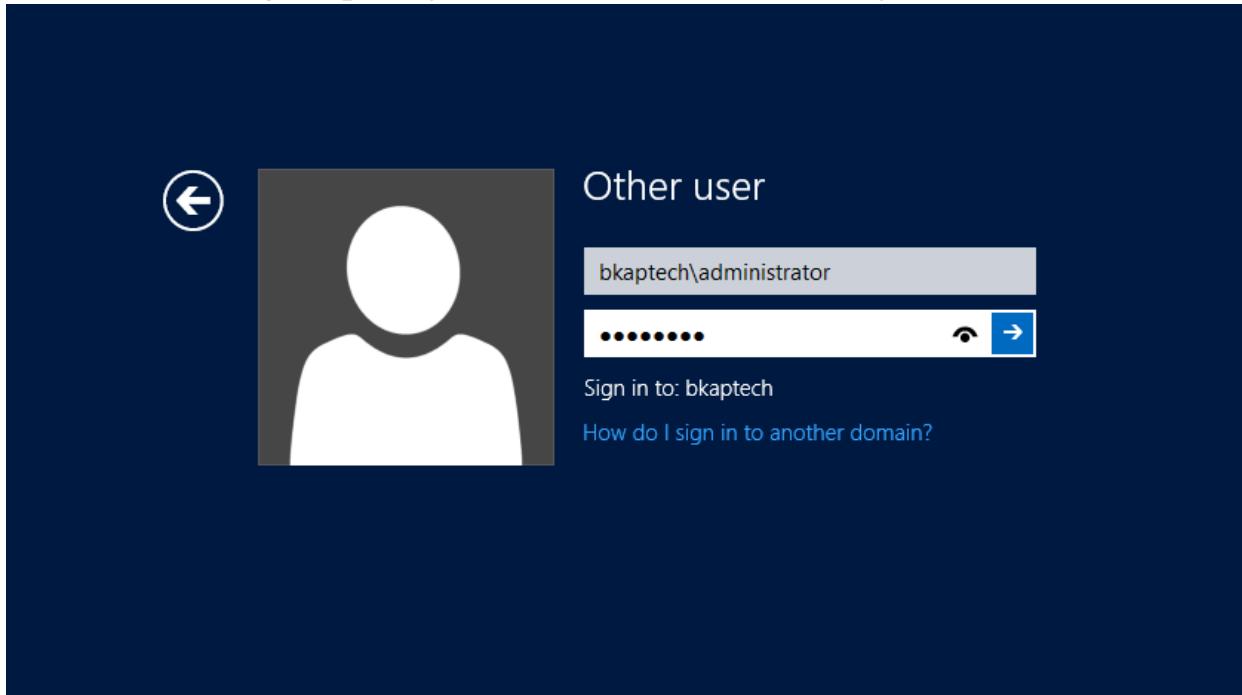
Thông số	BKAP-DC12-01	BKAP-SRV12-01	BKAP-WRK08-01
IP address	192.168.1.2	192.168.1.3	DHCP Client
Subnet Mask	255.255.255.0	255.255.255.0	255.255.255.0
Gateway	192.168.1.1	192.168.1.1	192.168.1.1
DNS Server	192.168.1.2	192.168.1.2	192.168.1.2

Hướng dẫn chi tiết:

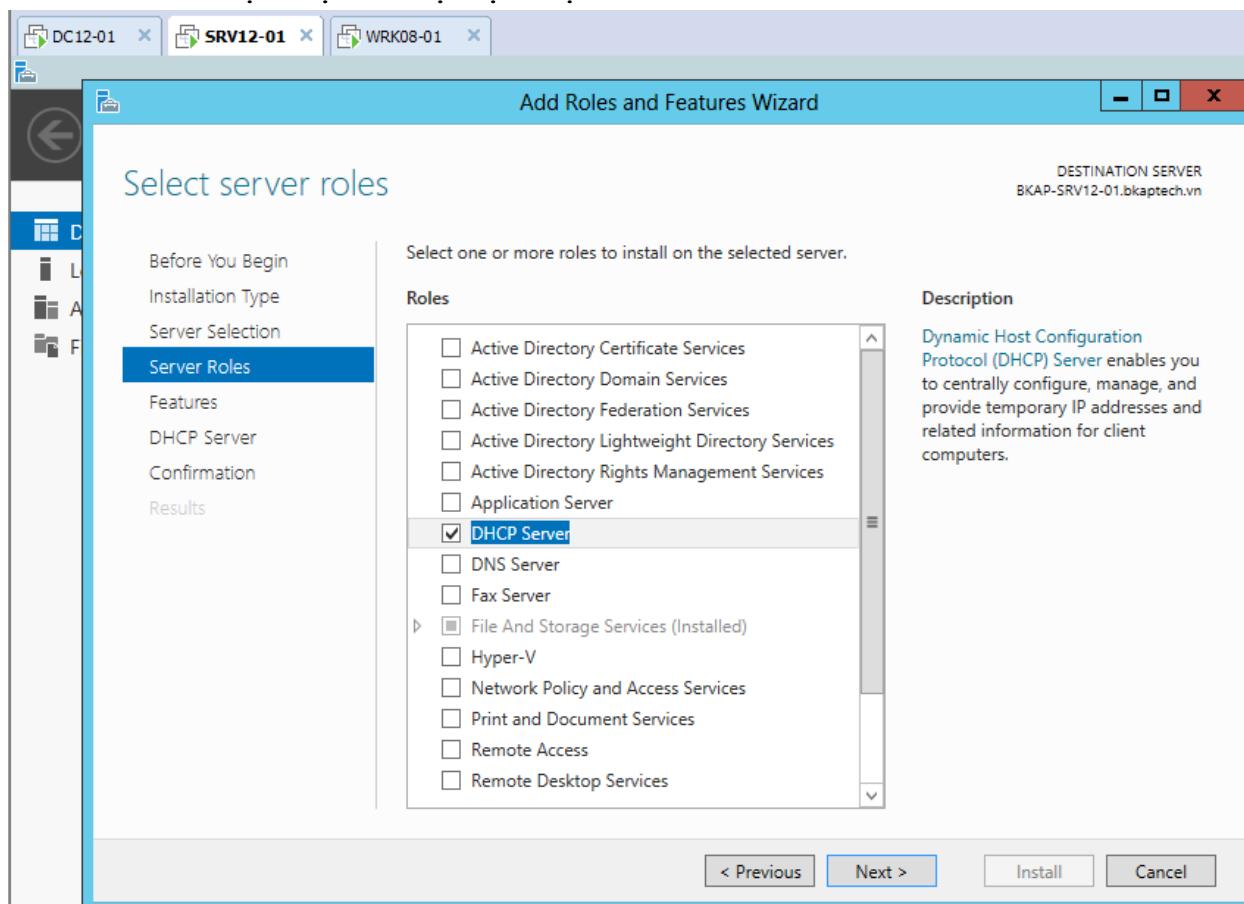
- Mở các máy ảo , kết nối đặt địa chỉ như hình vẽ, thực hiện *ping* thông giữa các máy trong mạng.
- Trên máy *BKAP-SRV12-01* , thực hiện:
 - Join vào Domain.



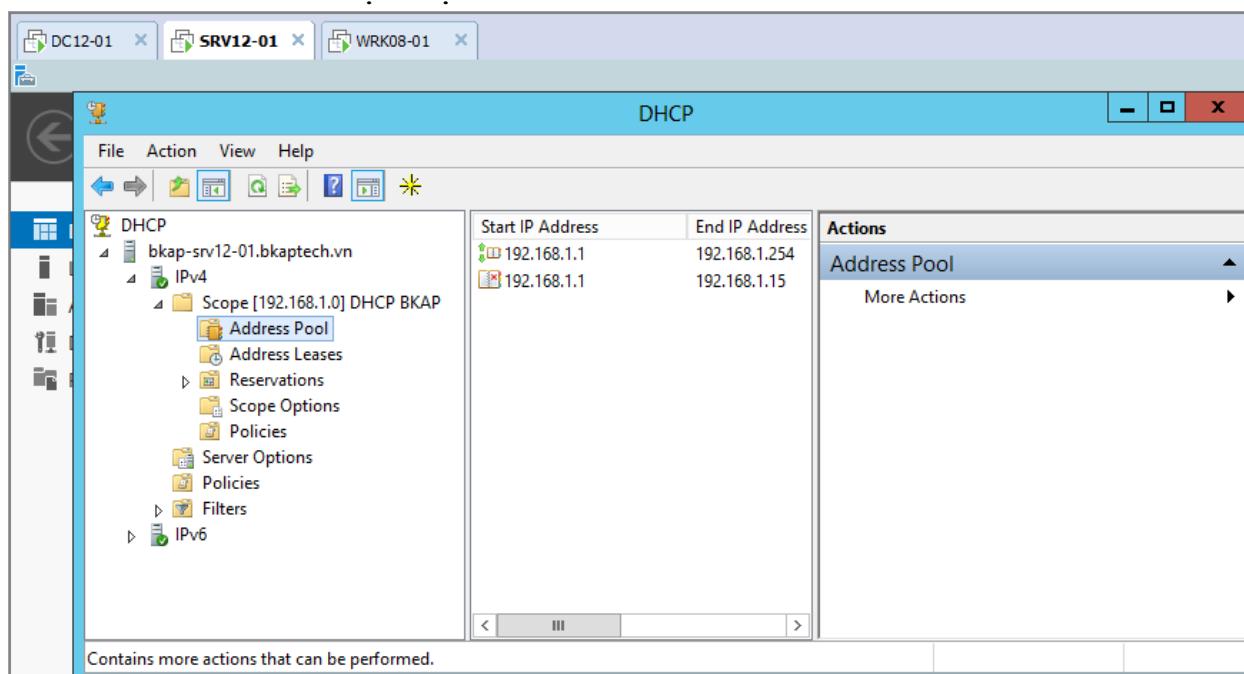
- Đăng nhập bằng tài khoản *administrator* trong miền.



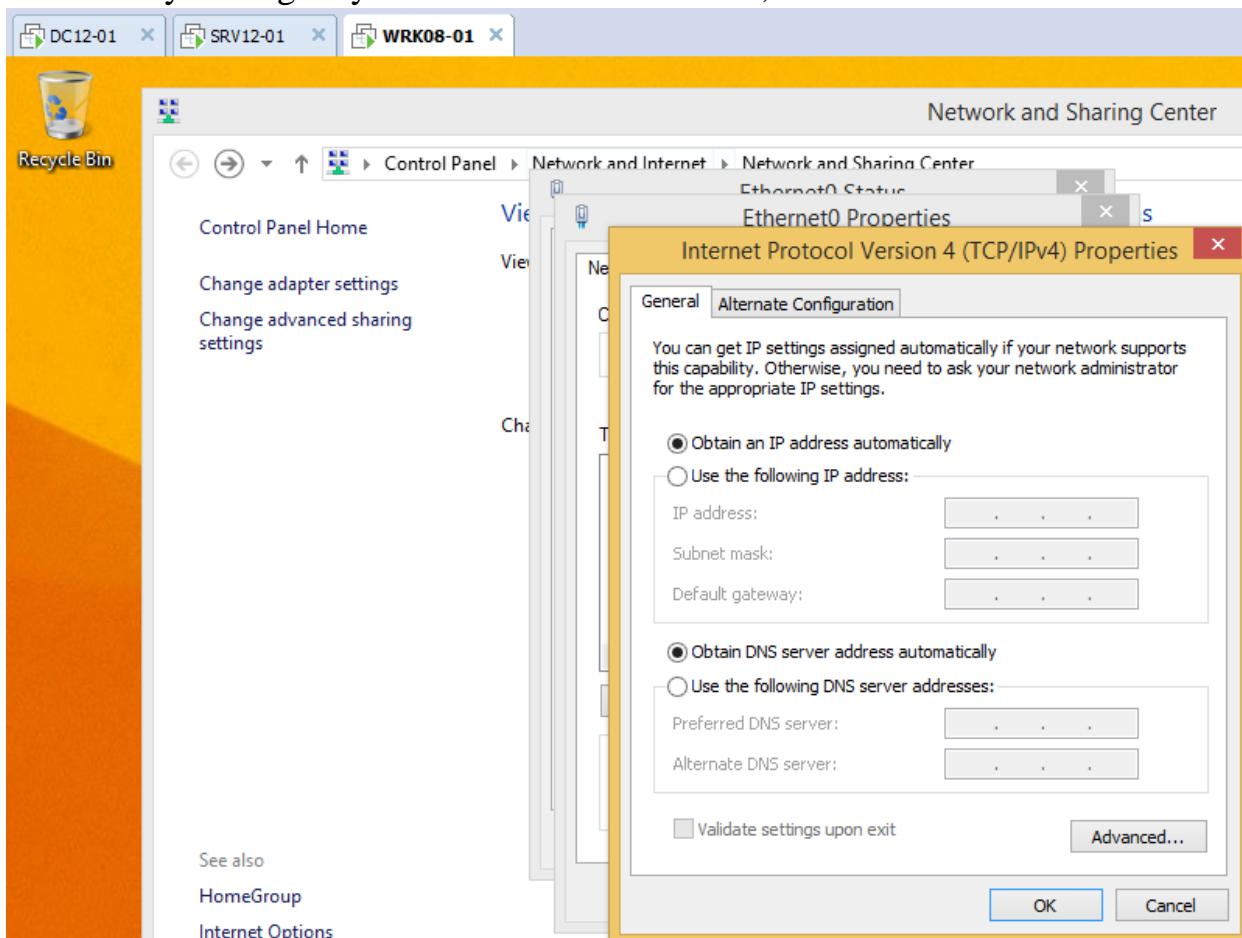
- Thực hiện cài đặt dịch vụ **DHCP Server**.



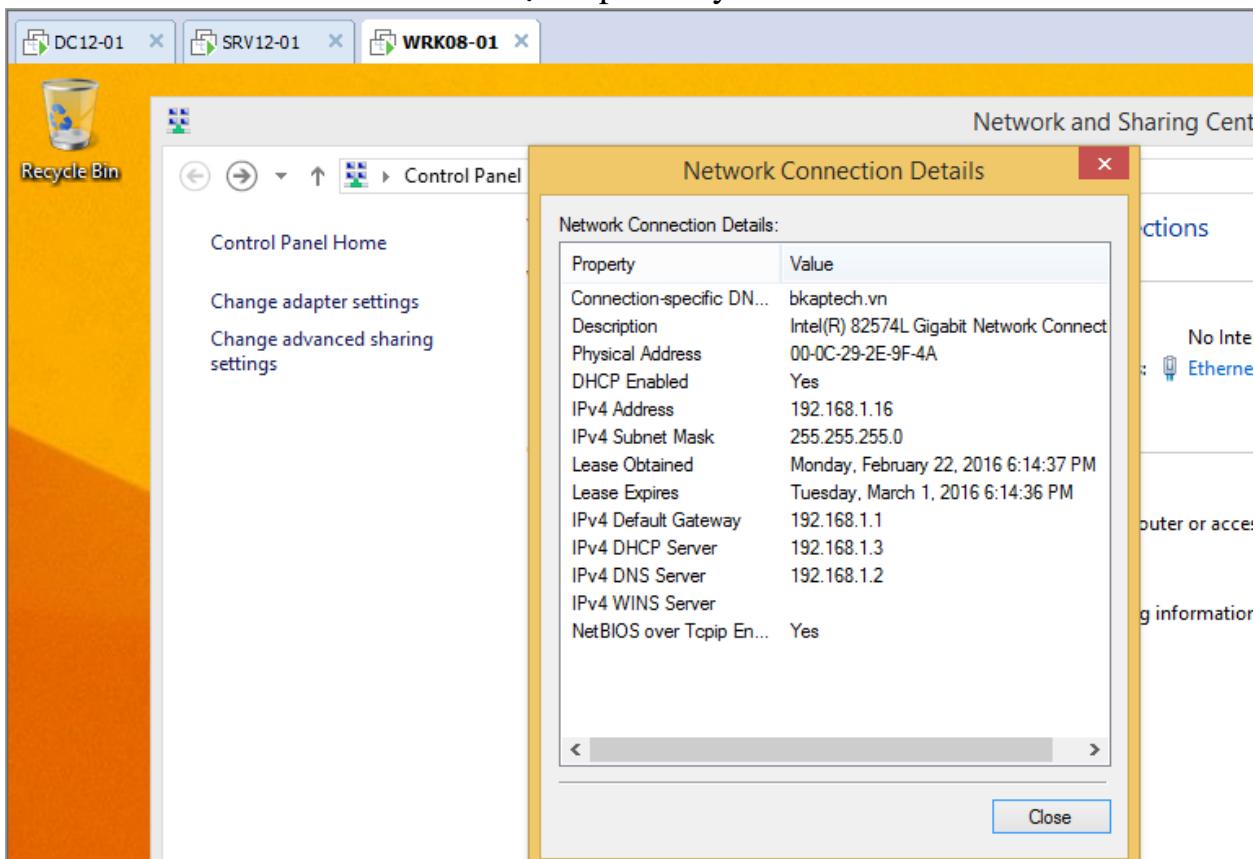
- Cấu hình dịch vụ **DHCP Server**.



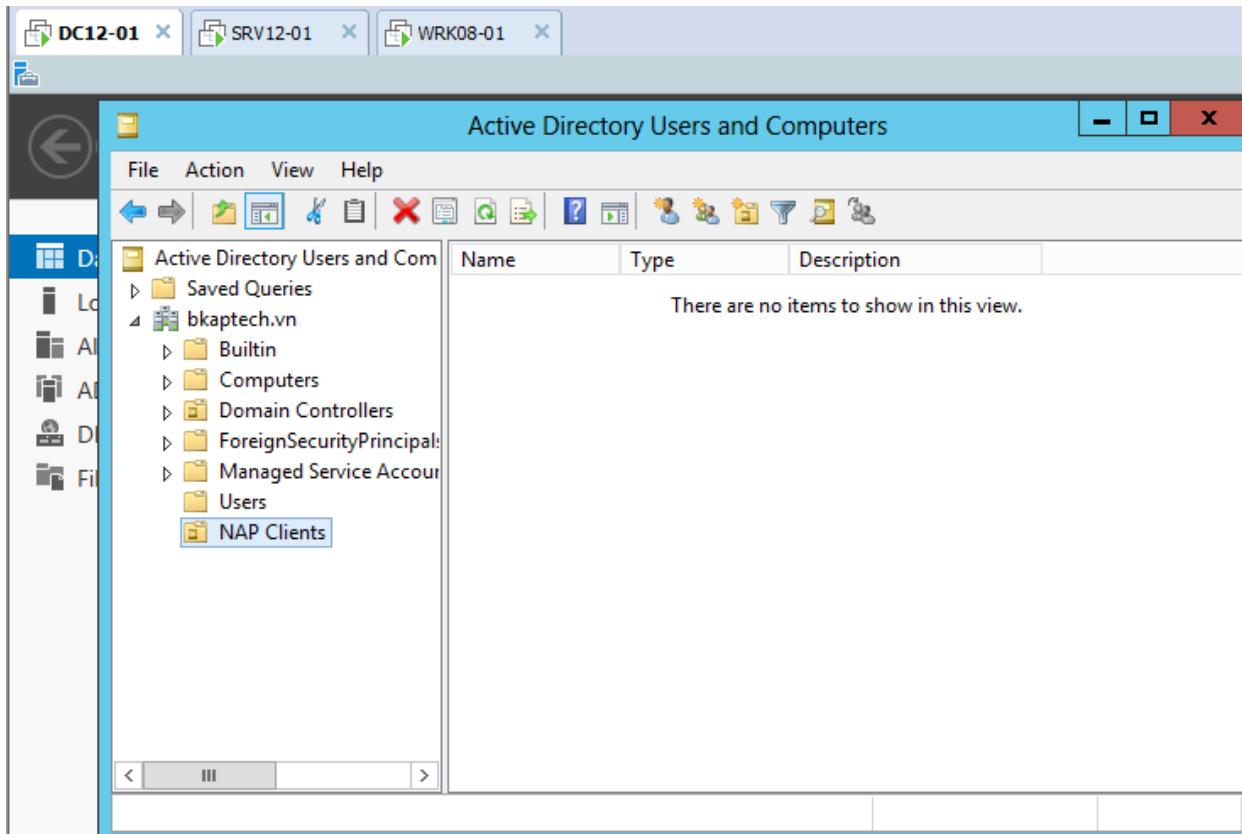
- Chuyển sang máy Client *BKAP-WRK08-01*, cấu hình DHCP Client.



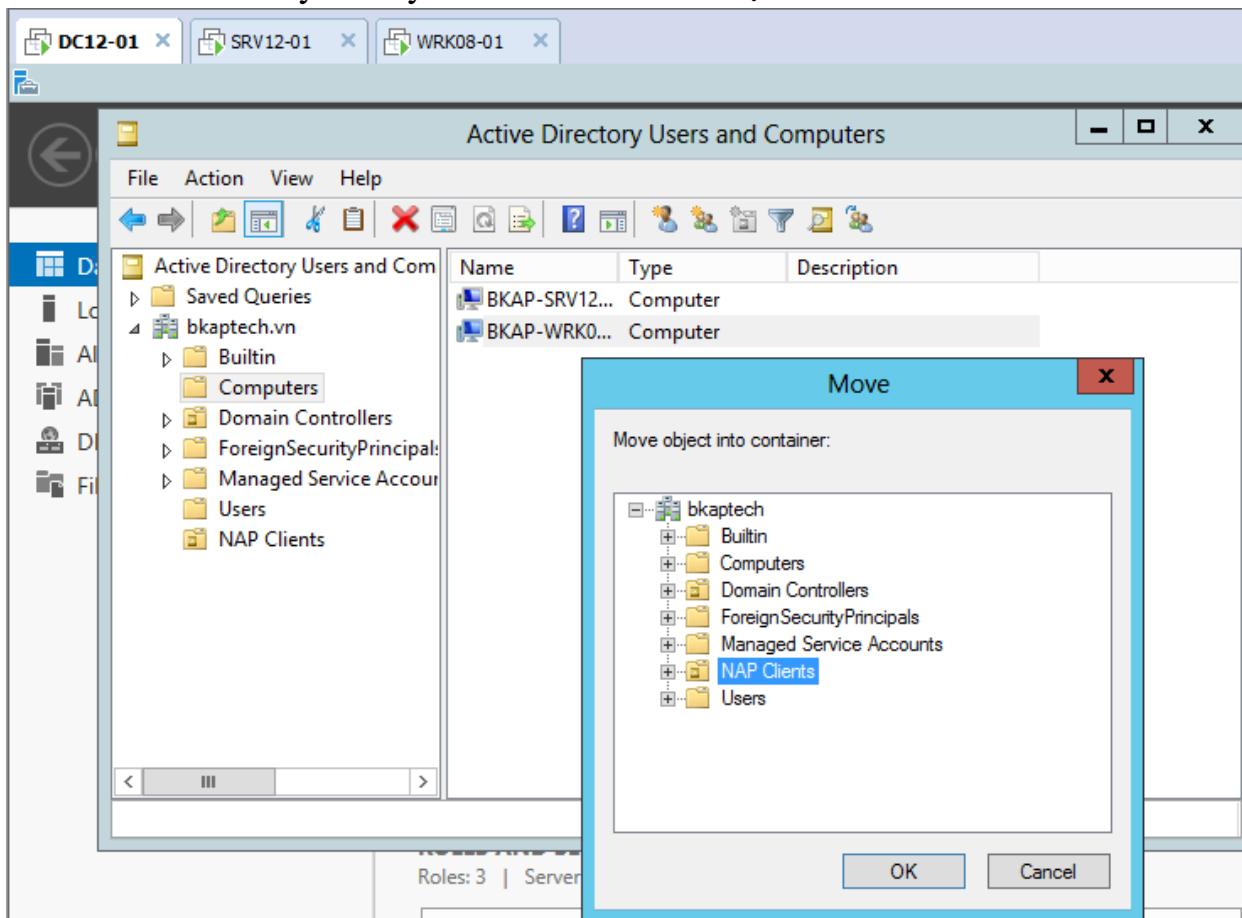
- Kiểm tra IP Client được cấp từ máy *DHCP Server*.

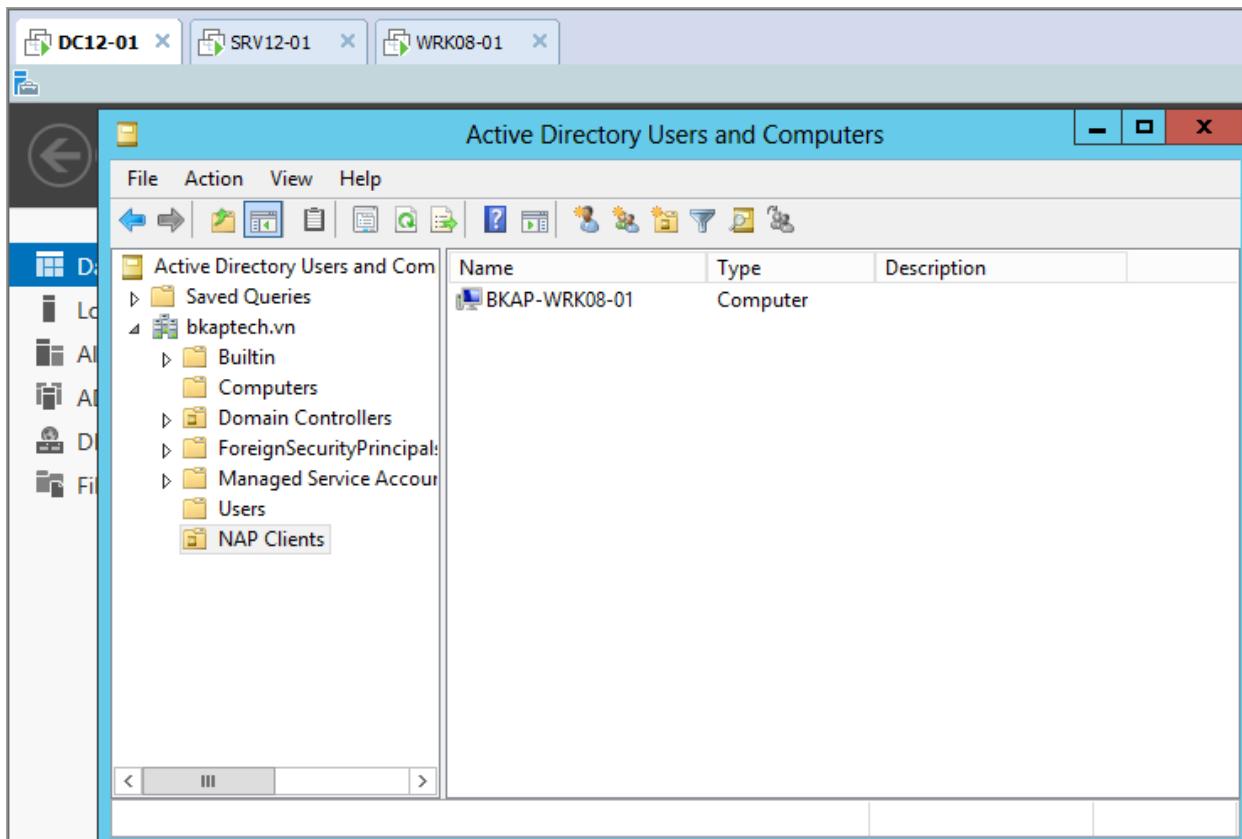


- Chuyển sang máy **BKAP-DC12-01**, thực hiện tạo **OU**, triển khai **GPO** để cấu hình **NAP Clients**.
 - Tạo **OU** tên “**NAP Client**”.

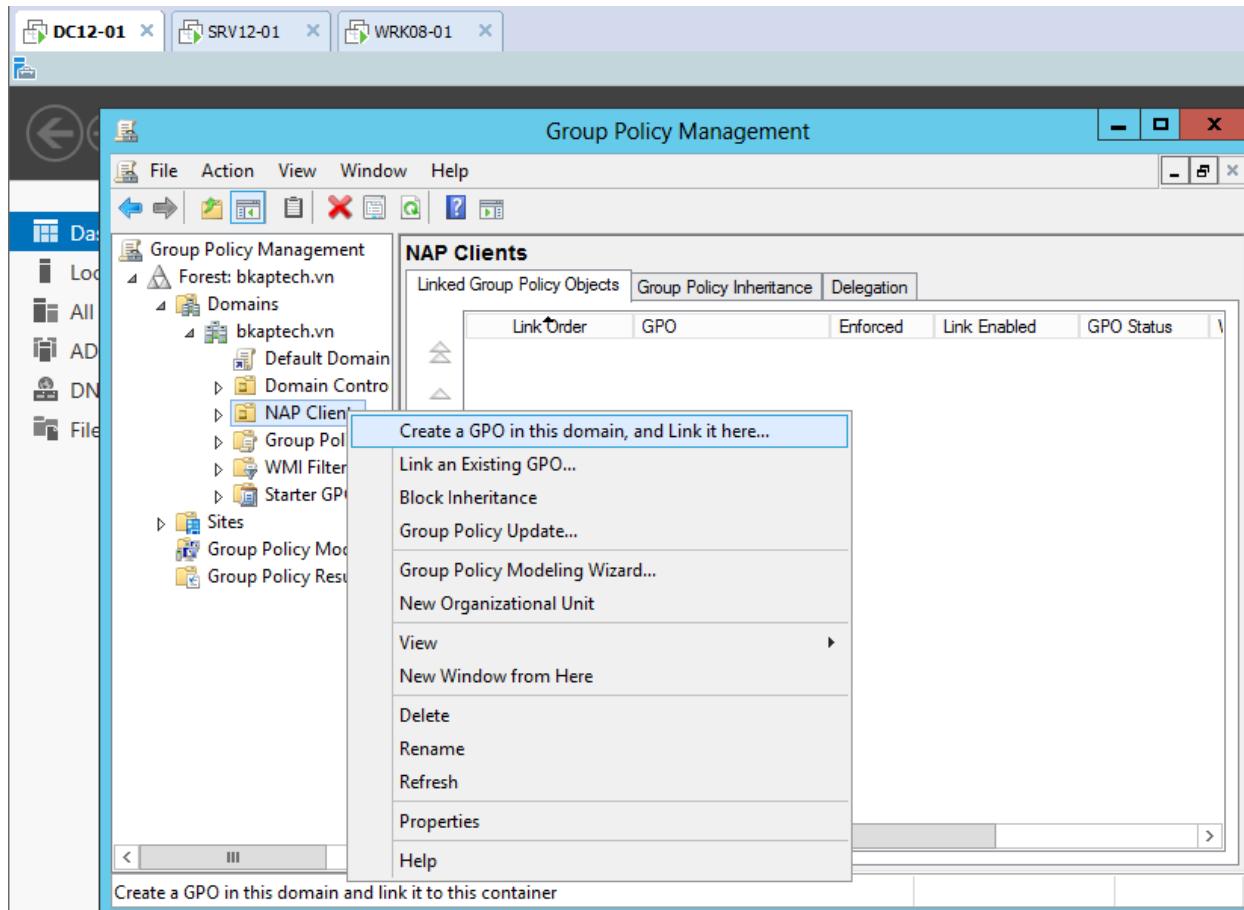


- Di chuyển máy Client vào OU vừa tạo.

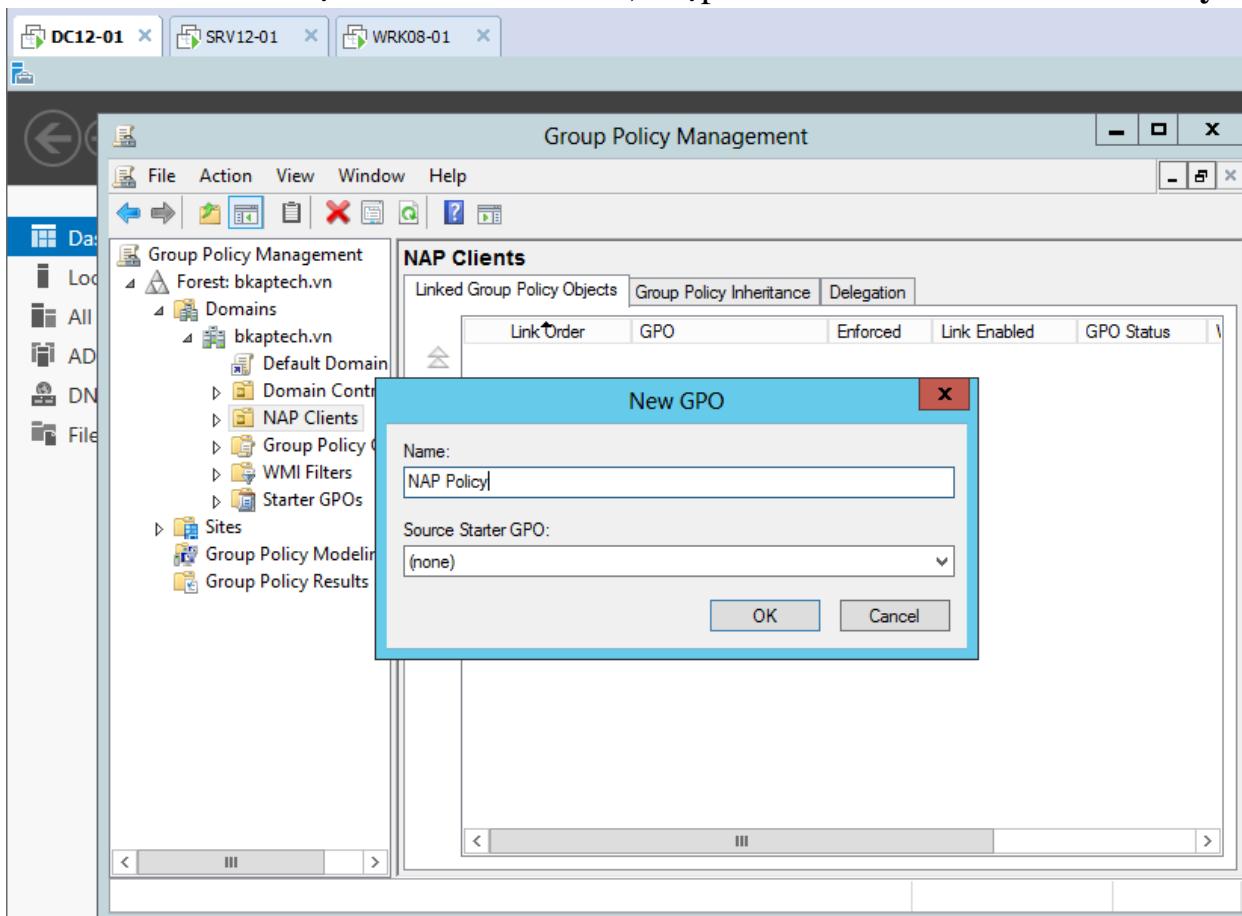




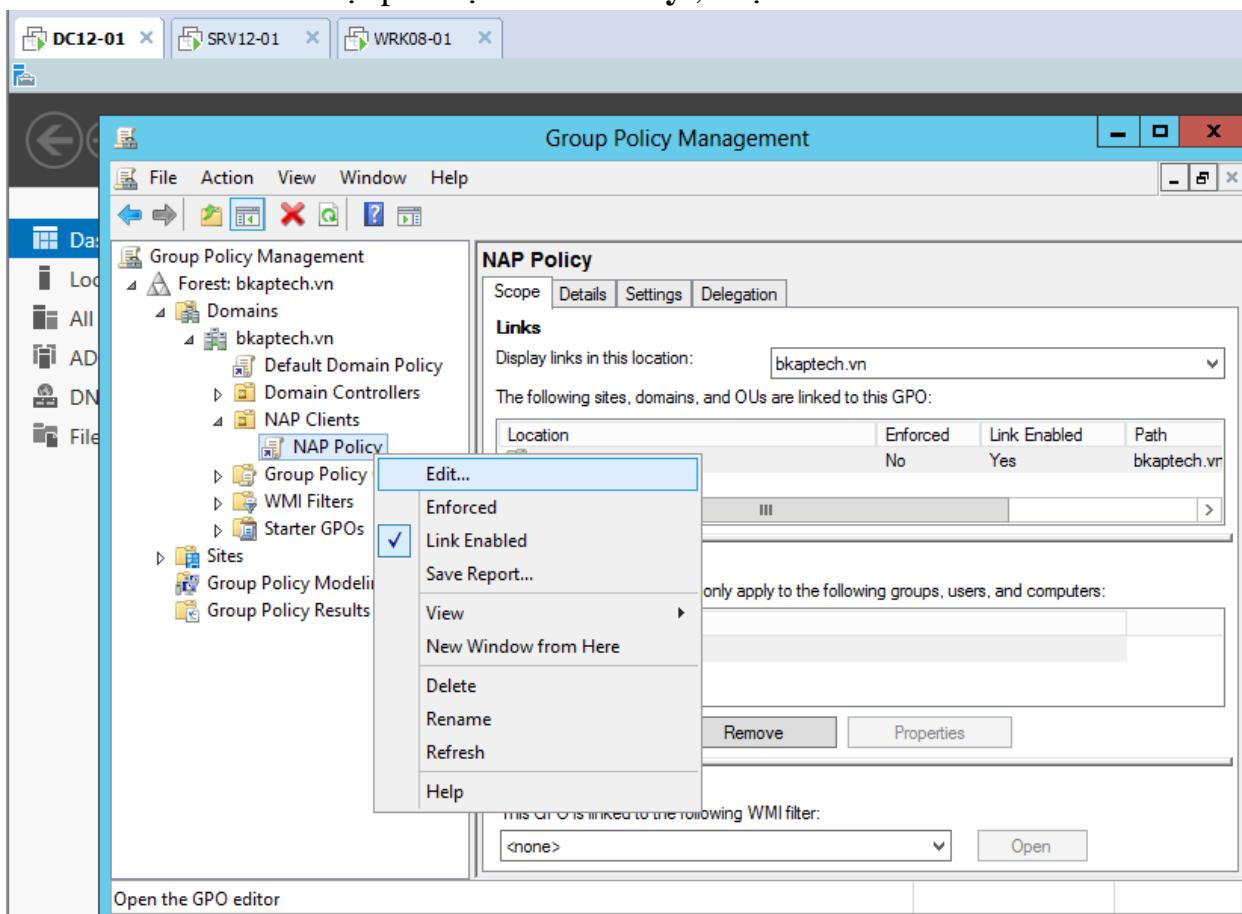
- Tạo chính sách *GPO NAP policy*.
 - **Tools / Group Policy Management.**
 - Tại OU **NAP Client** , click chuột phải chọn **Create OU in this domain...**



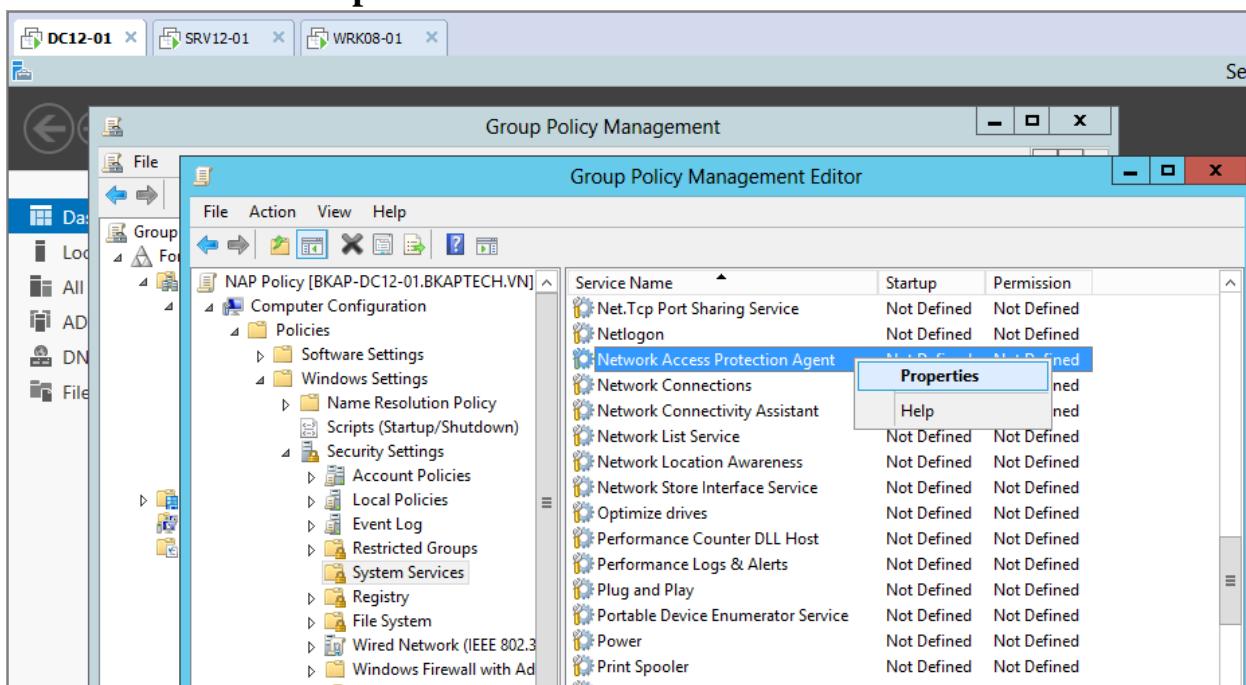
- Tại cửa sổ New GPO , nhập vào tên chính sách : NAP Policy.



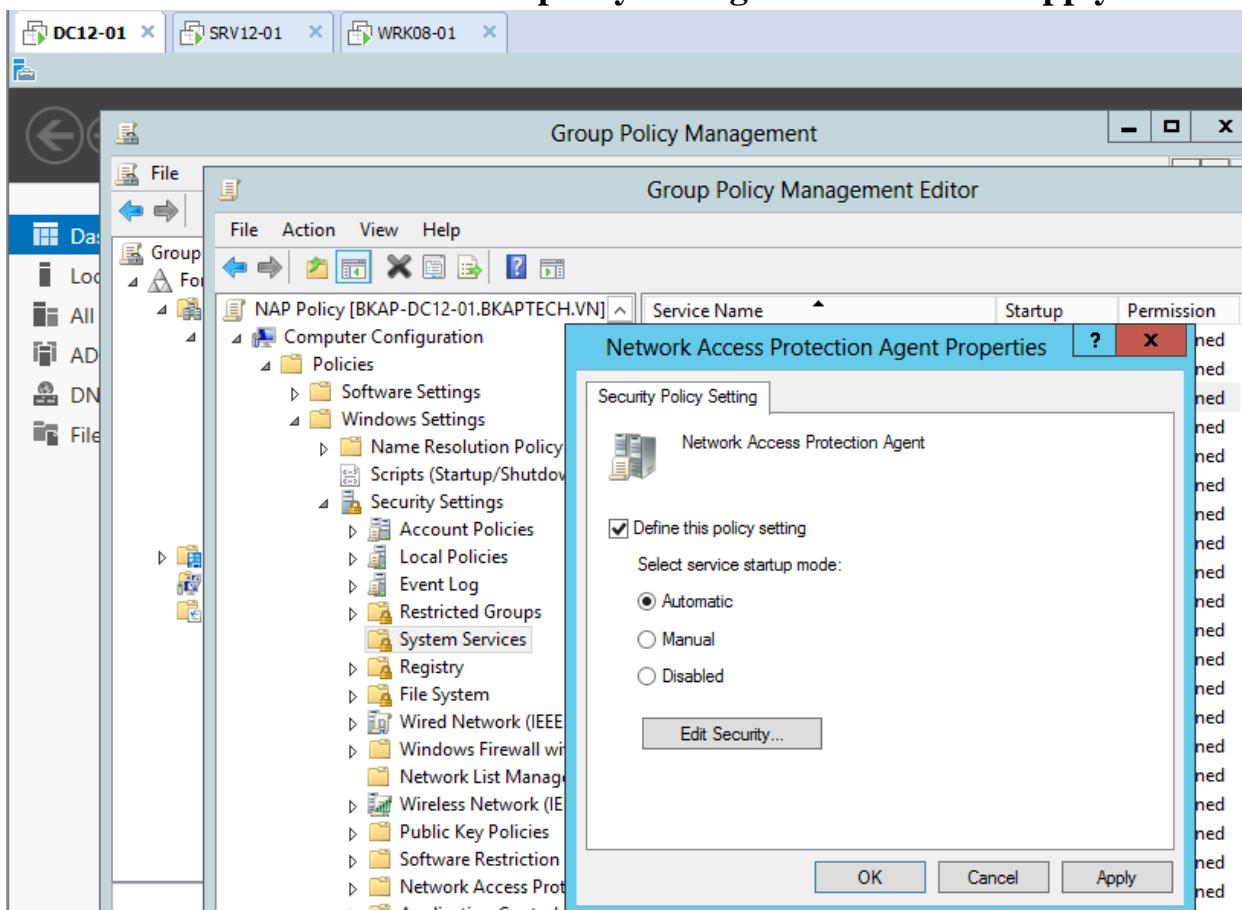
- Click chuột phải tại **NAP Policy** , chọn **Edit...**



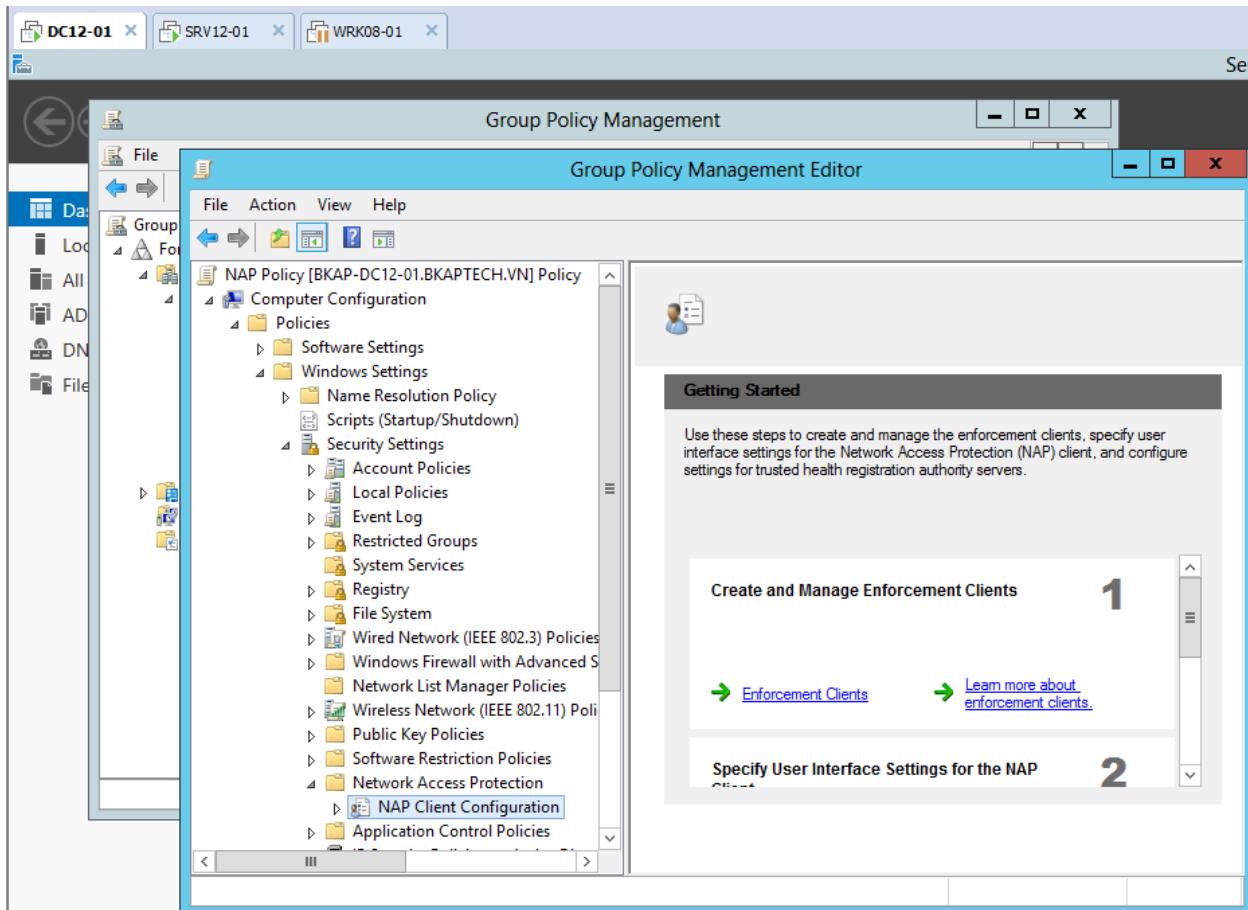
- Tại cửa sổ **Group Policy Management Editor**, chọn vào :
 - **Computer Configuration / Policies / Windows Settings / Security Settings / System Services /** chọn vào **Network Access Protection Agent**. Click chuột phải tại đây chọn **Properties**.



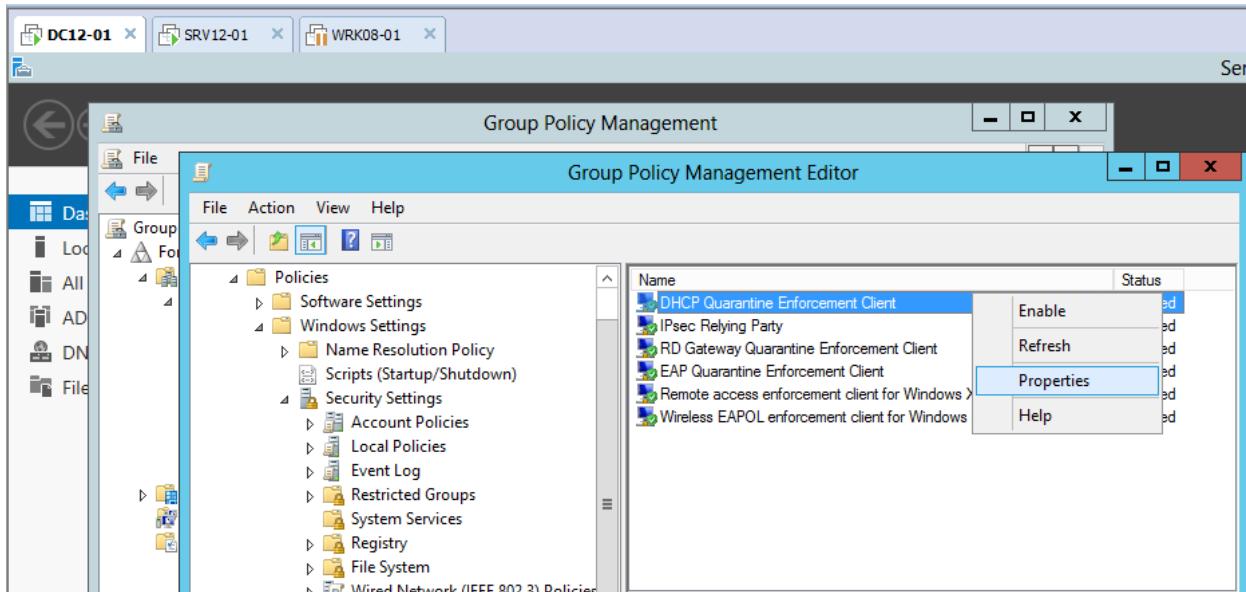
- Tại cửa sổ **Network Access Protection Agent Properties**, tích vào **Define this policy setting / Automatic.** => **Apply / OK.**



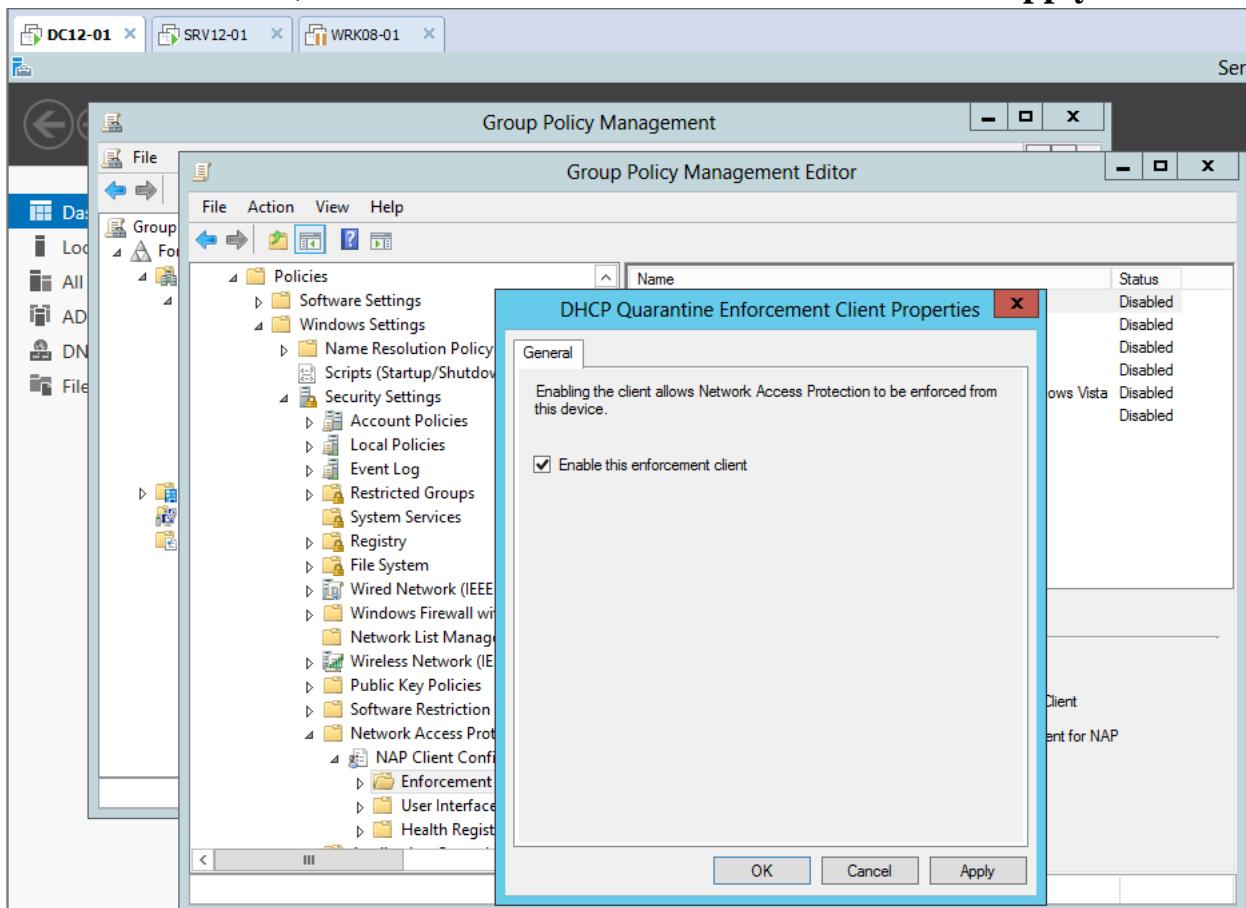
- Tại **Computer Configuration / Policies / Window Settings / Security Settings / System Services** , chọn vào **Network Access Protection / NAP Client Configuration** , click vào **Enforcement Clients**.



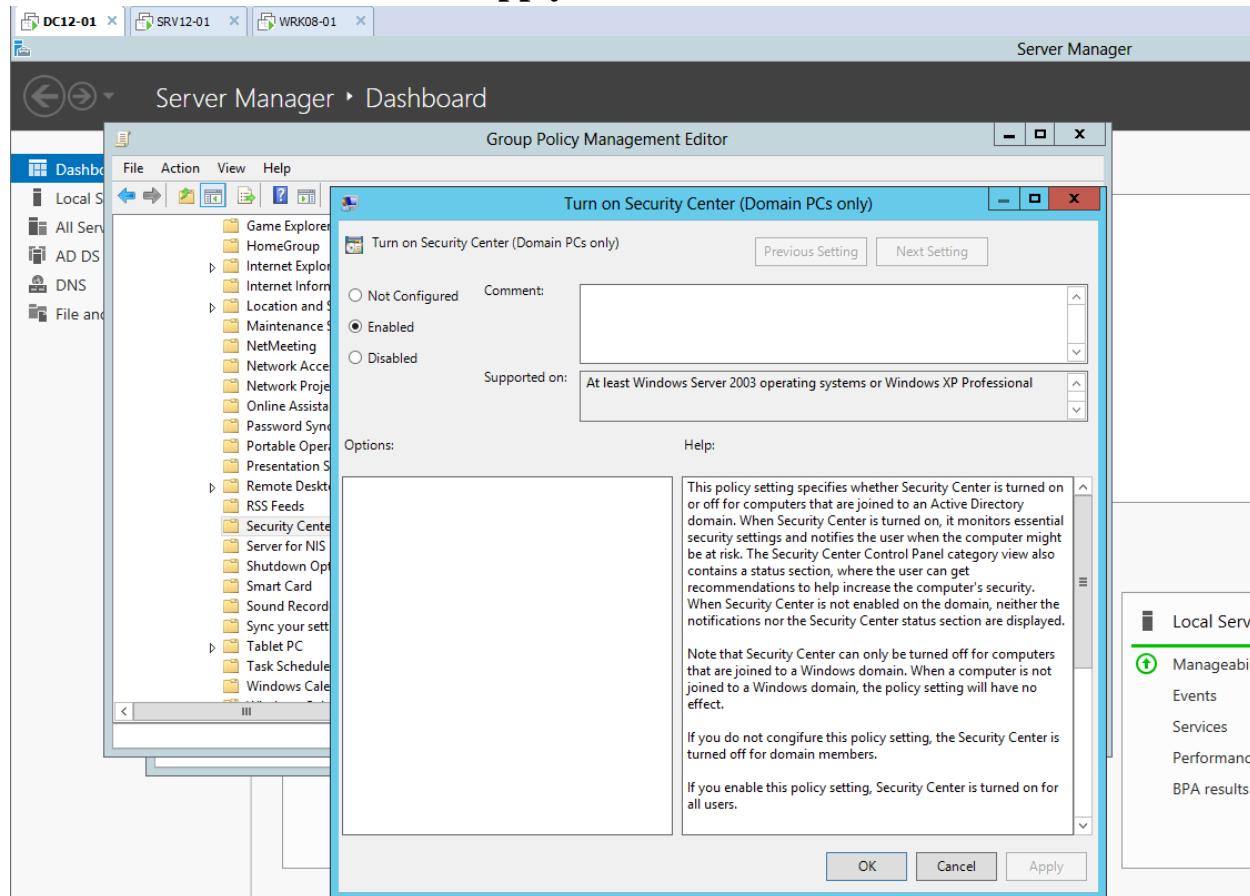
- Click chuột phải tại **DHCP Quarantine Enforcement Client** chọn **Properties**.



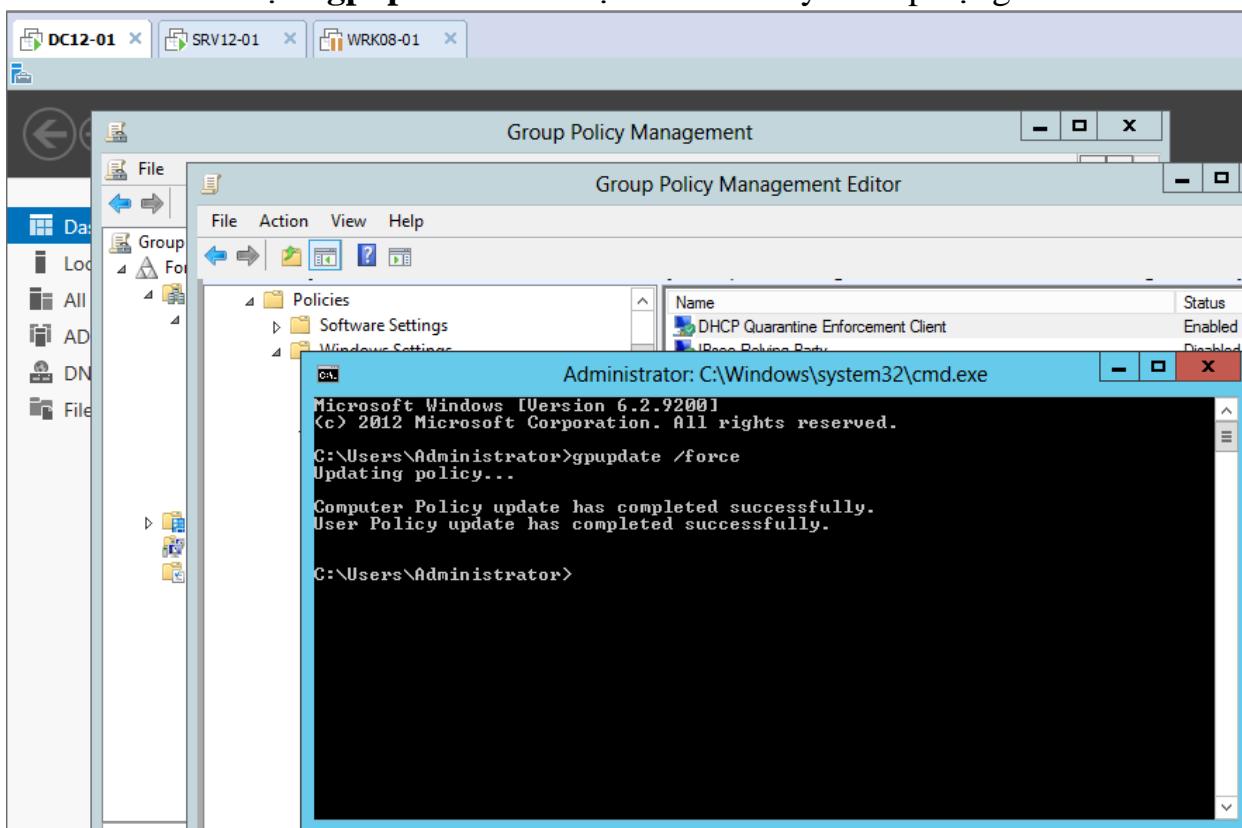
- Tại cửa sổ **DHCP Quarantine Enforcement Client Properties**, click vào **Enable this enforcement client**. => **Apply / OK**.



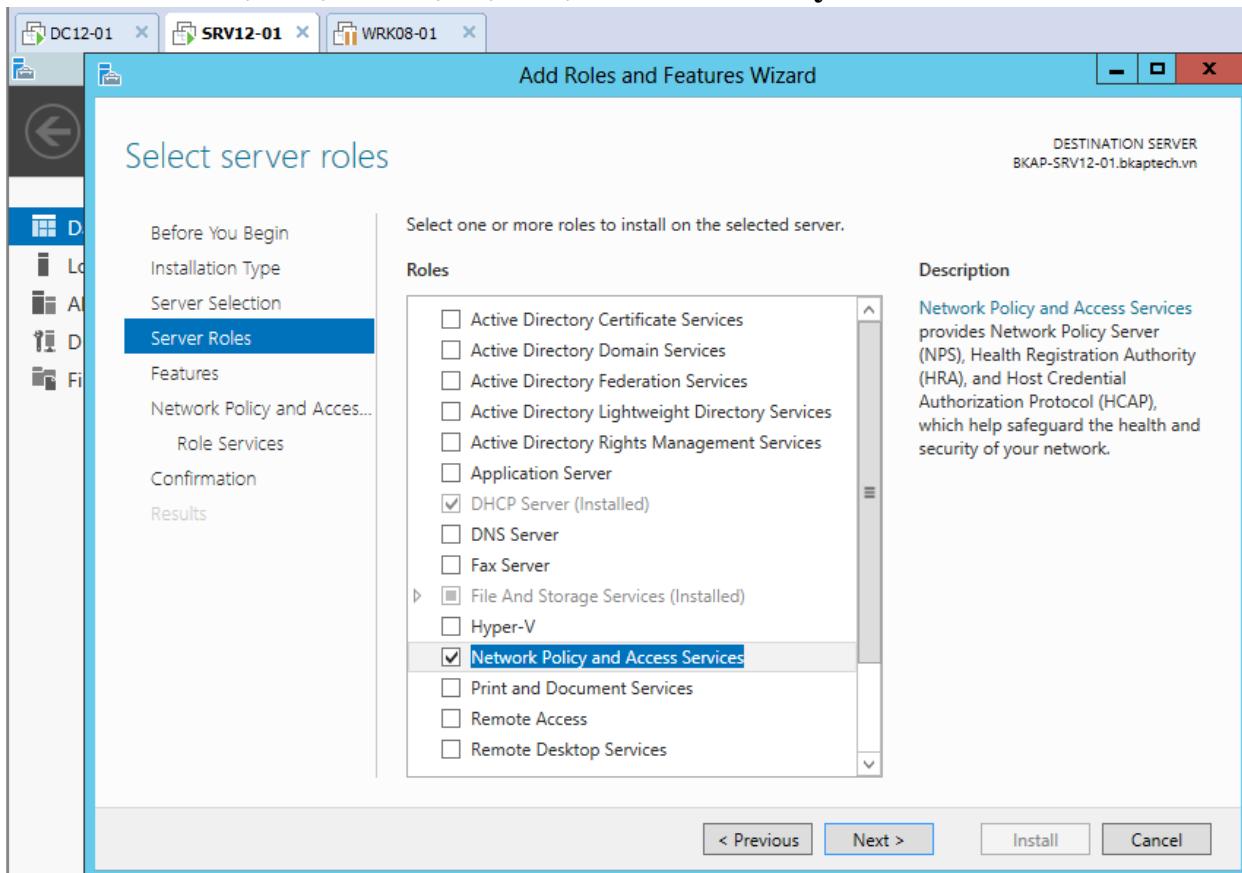
- Chọn vào **Administrative Templates: Policy definitions / Window Components / Security Center.**
 - Tại **Turn on Security Center ..** / click chuột phải chọn **Edit => Enable => Apply / OK.**



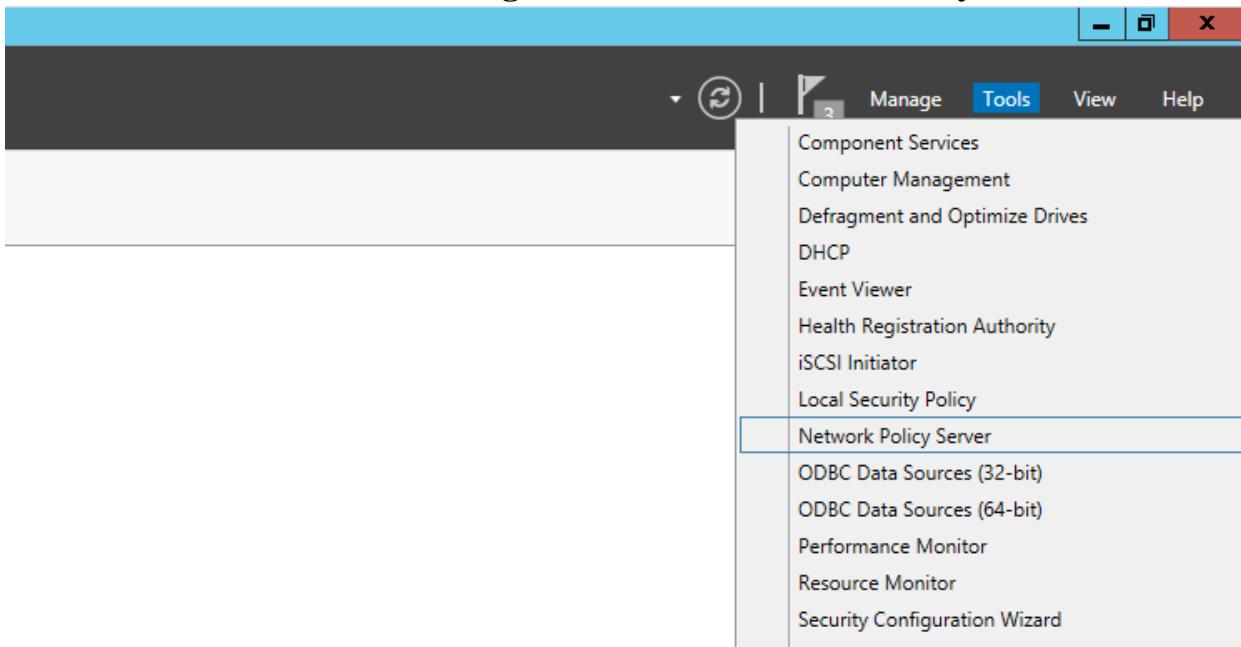
- Gõ lệnh **gpupdate /force** tại **cmd** để máy chủ áp dụng chính sách.



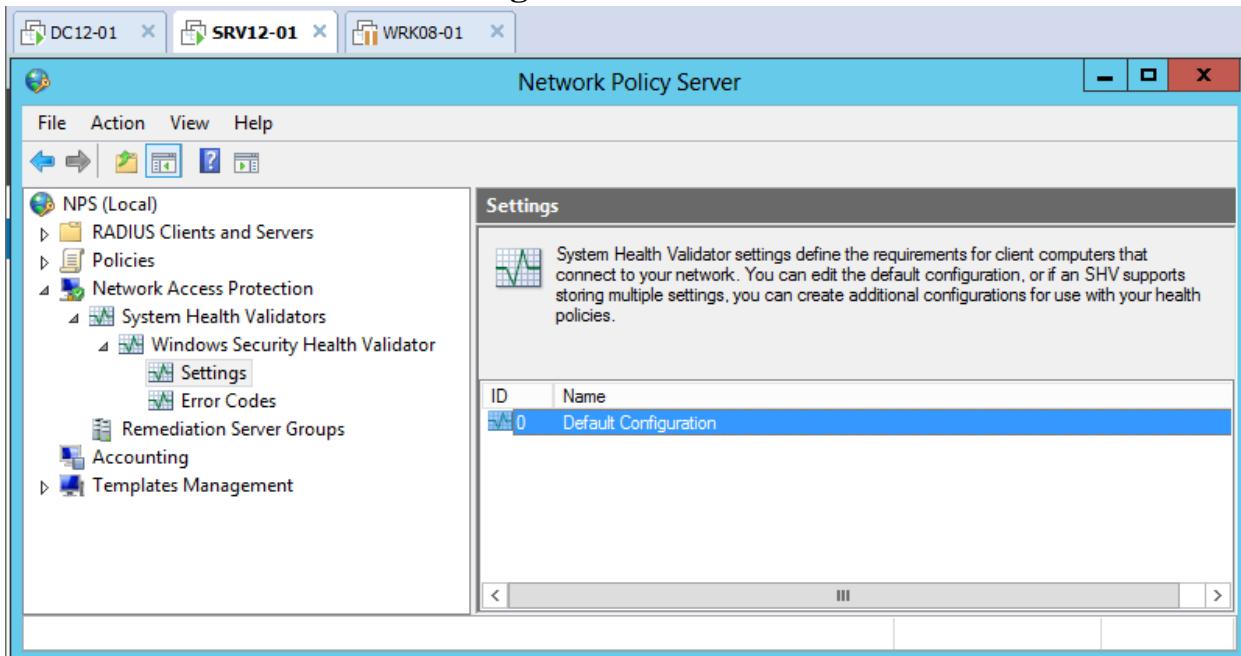
- Chuyển sang máy *BKAP-SRV12-01*.
 - Thực hiện cài đặt dịch vụ **Network Policy and Access Services**.



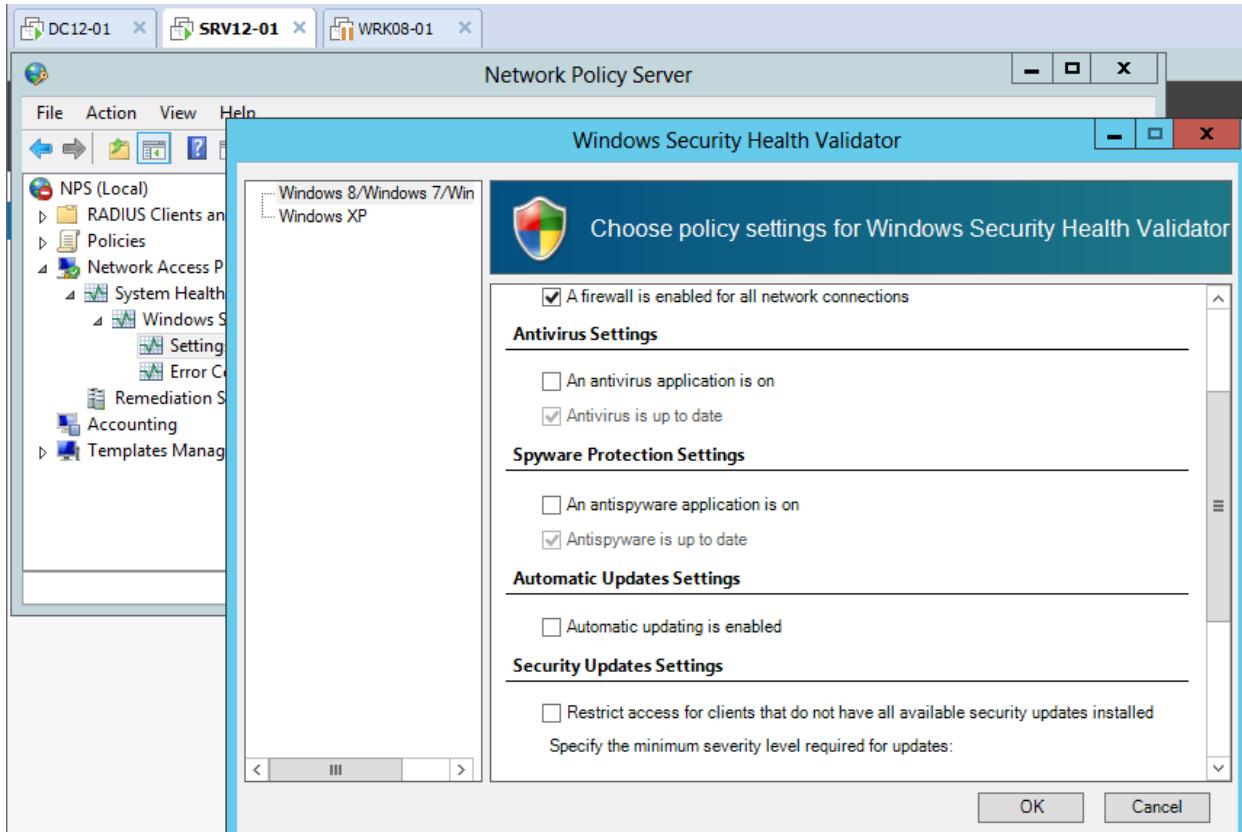
- Cấu hình dịch vụ **Network Policy Server**:
 - Server Manager / Tools => Network Policy Server.



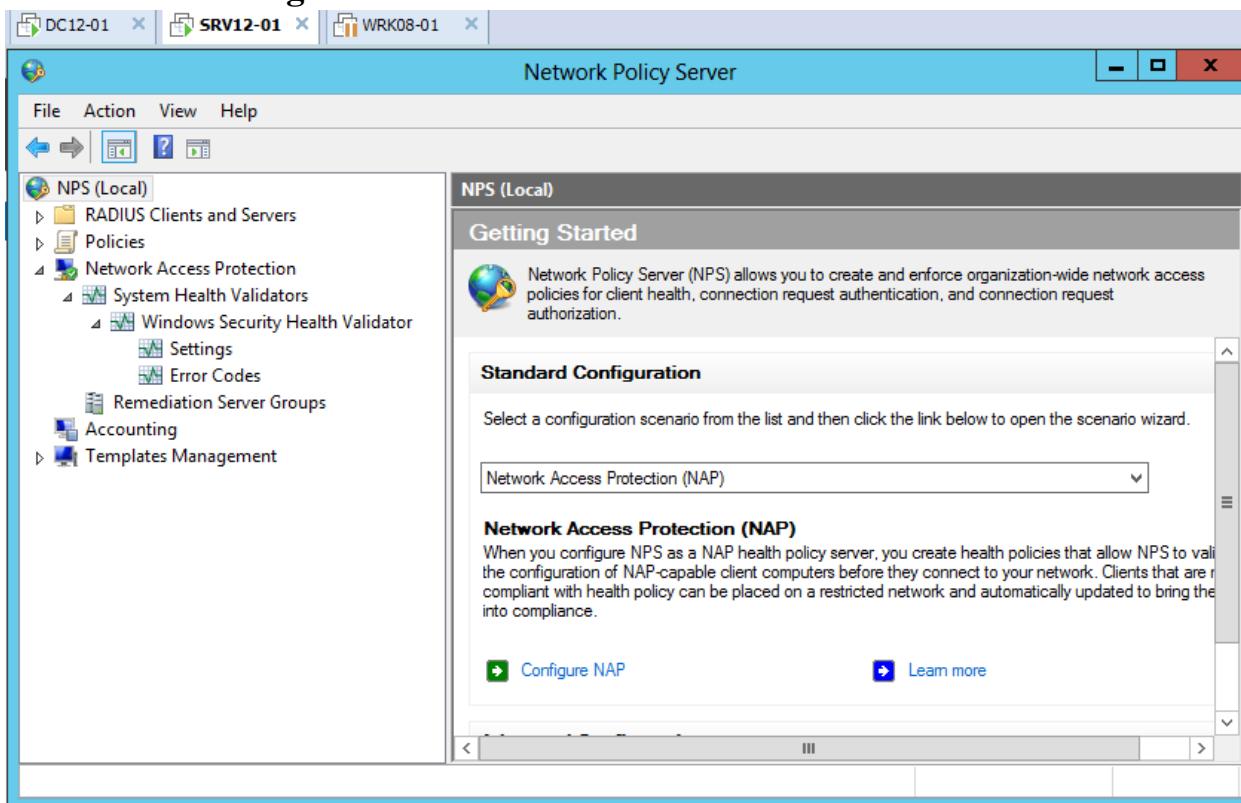
- Tại cửa sổ **Network Policy Server** , chọn vào **NPS (Local) / Network Access Protection / System Health Validators / Windows Security Health Validator / Settings**. => chọn vào **Default Configuration**.



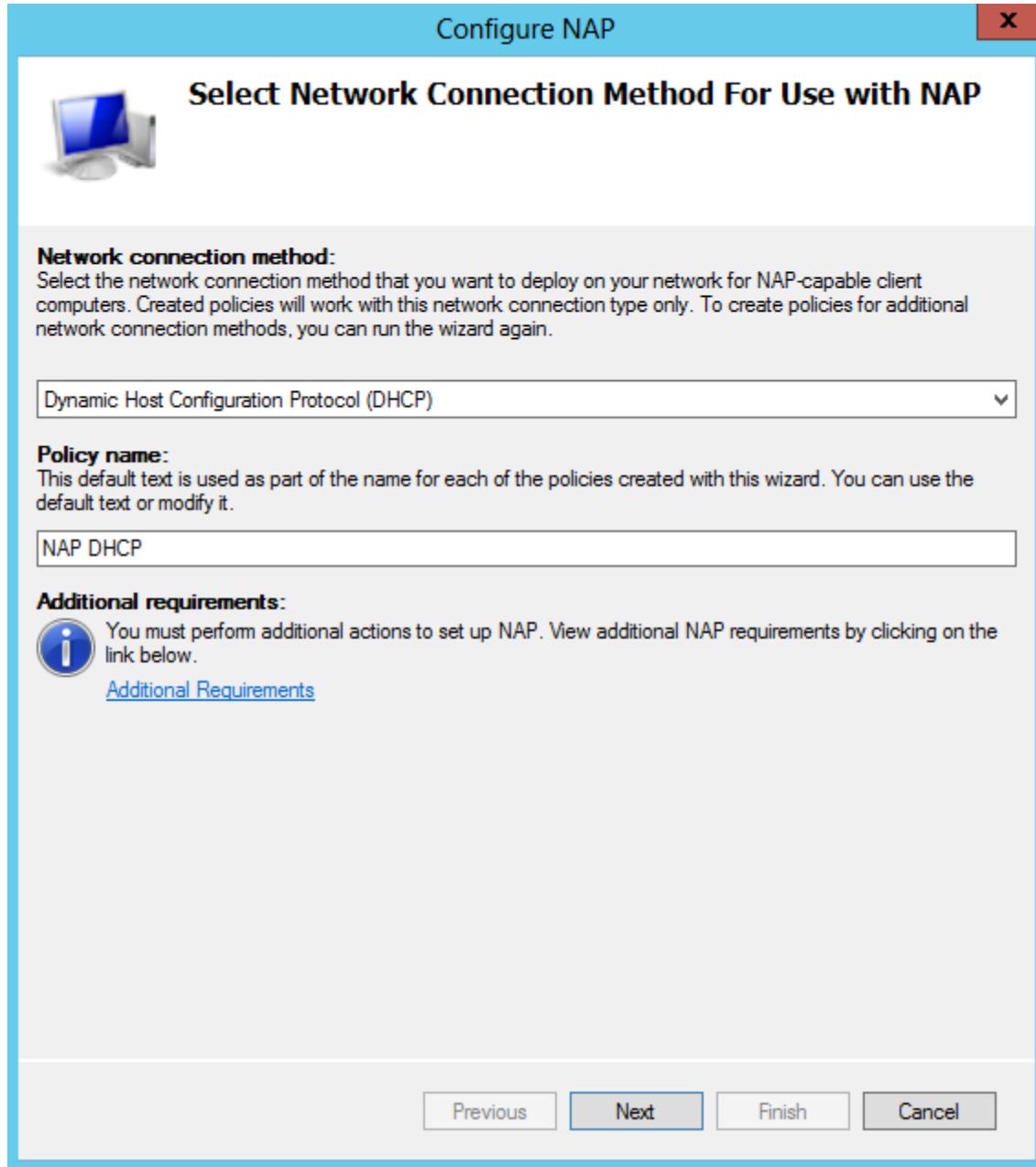
- Click chuột phải tại **Default Configuration**, chọn **Properties**, tại cửa sổ **Windows Security Health Validator**, thực hiện bỏ dấu tích tại **Antivirus Settings**, **Spyware Protection Settings**, và **Automatic Update Settings**. => OK.



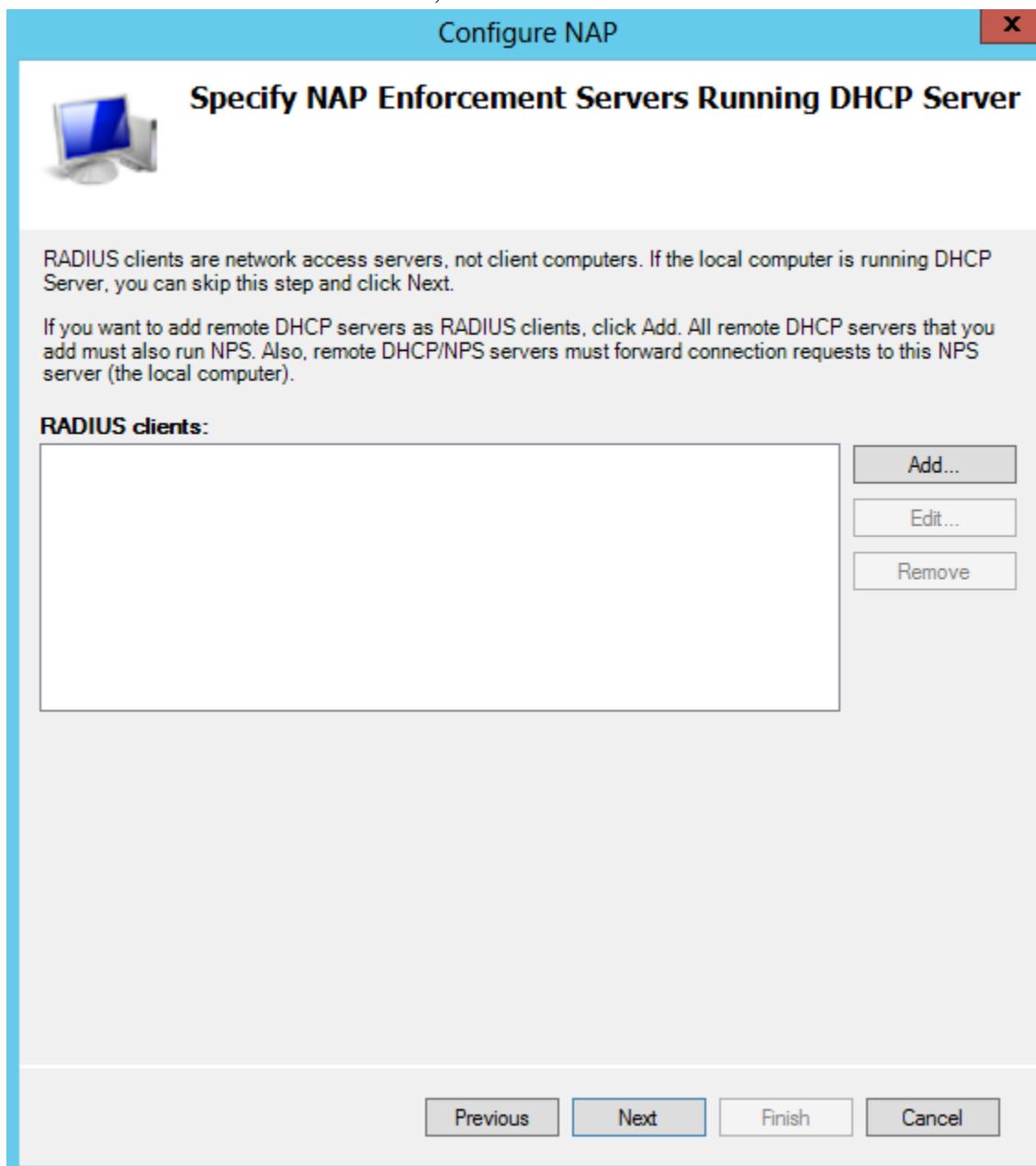
- Tại cửa sổ **Network Policy Server**, click vào **NPS (Local)** , chọn vào **Configure NAP**.



- Tại cửa sổ **Configure NAP** , tại mục **Network connection method** , chọn **Dynamic Host Configuration Protocol (DHCP)**.
 - Tại mục *Policy Name* : **NAP DHCP**. => Next.



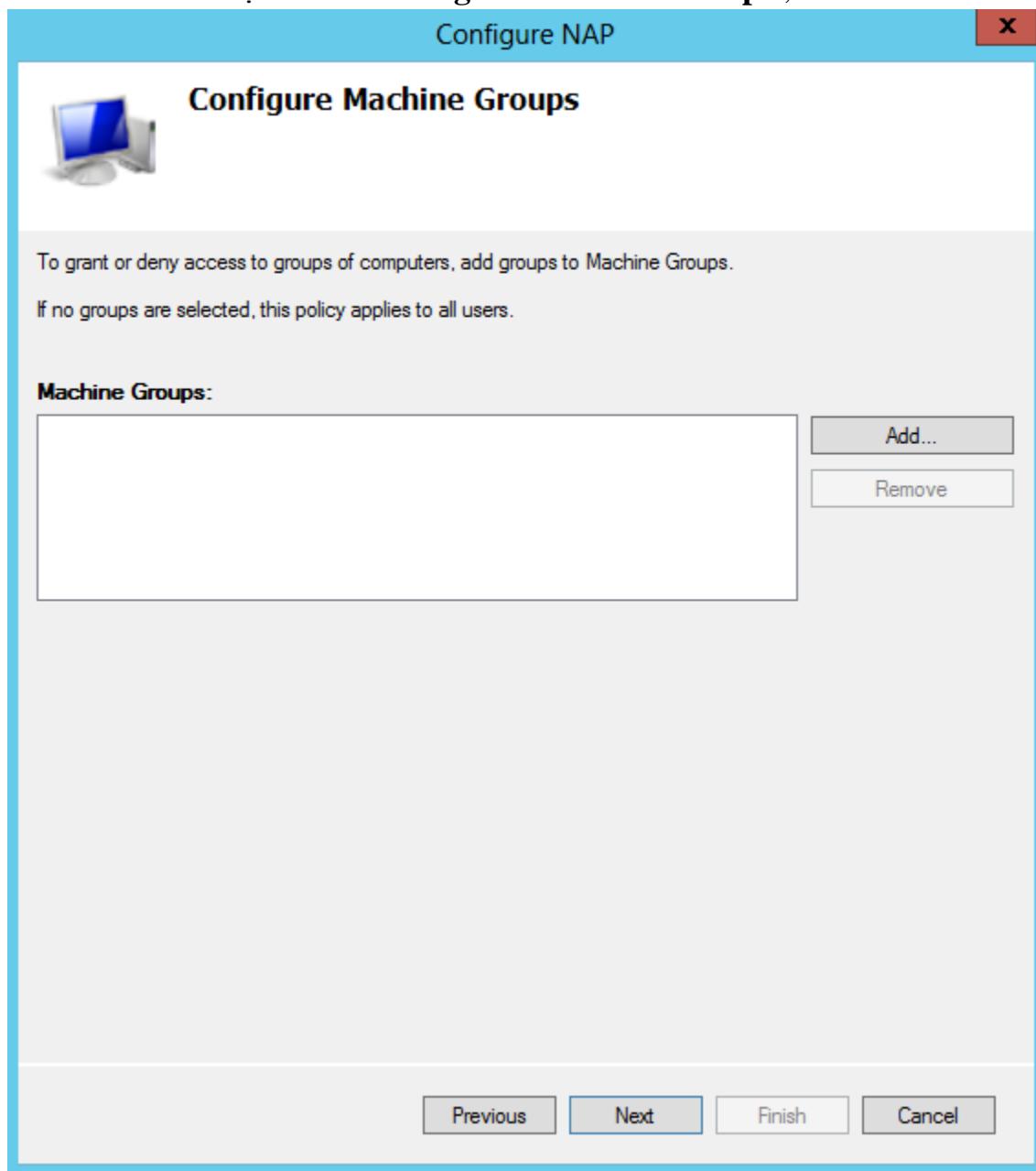
- Tại cửa sổ **Specify NAP Enforcement Servers Running DHCP Server**, click vào Next.



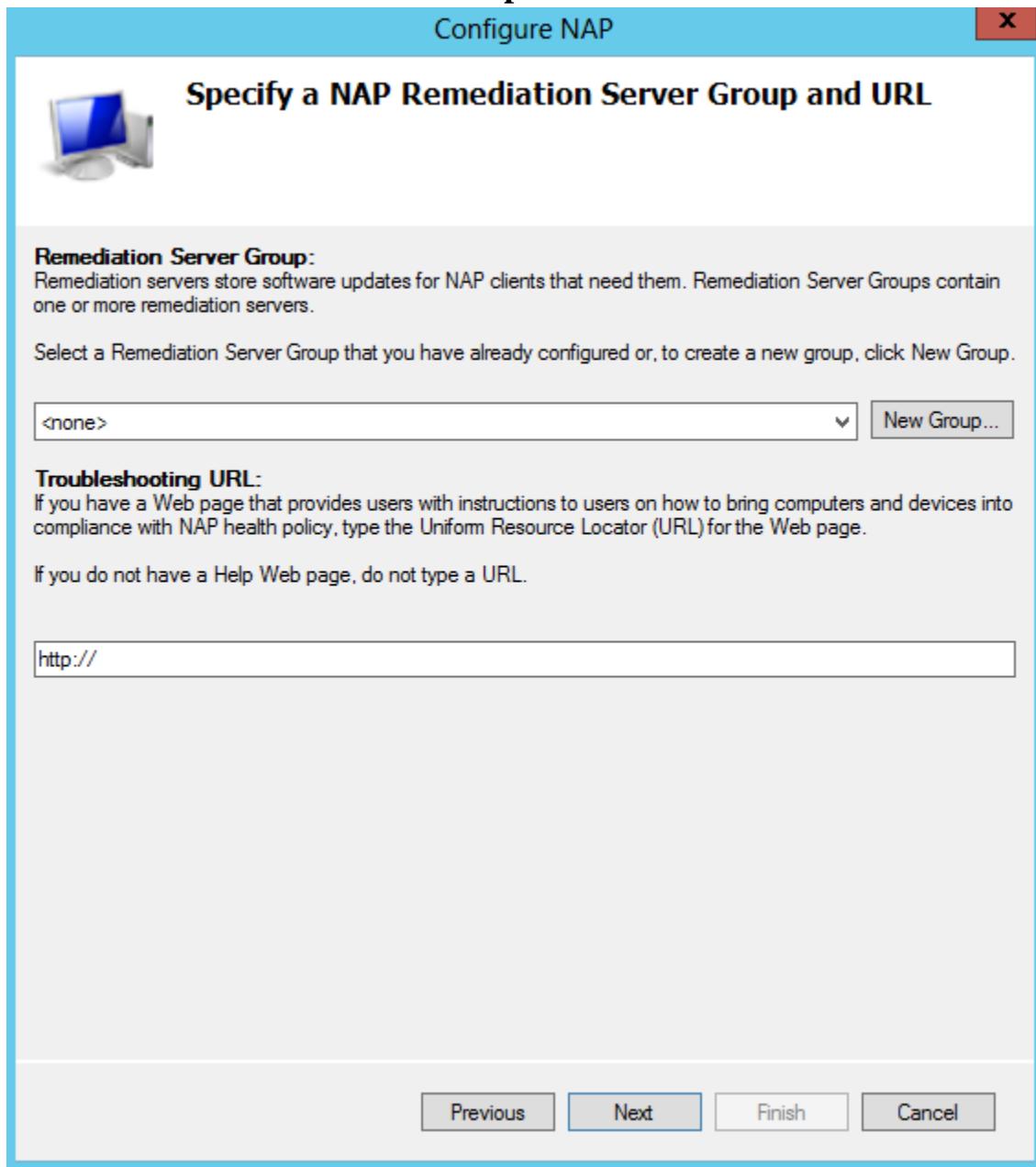
- Tại cửa sổ **Specify DHCP Scopes**, click vào *Next*.



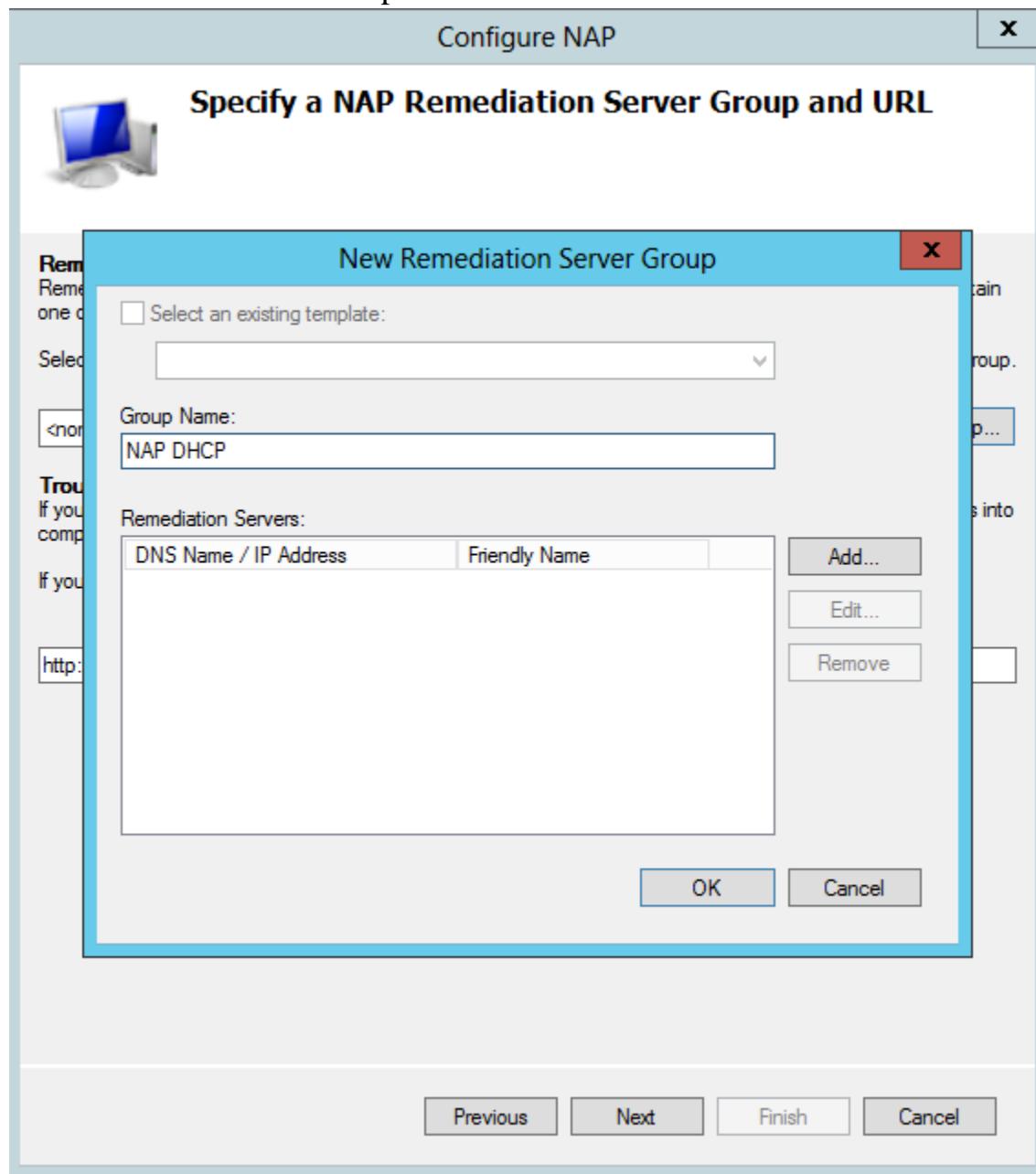
- Tại cửa sổ **Configure Machine Groups**, click vào *Next*.



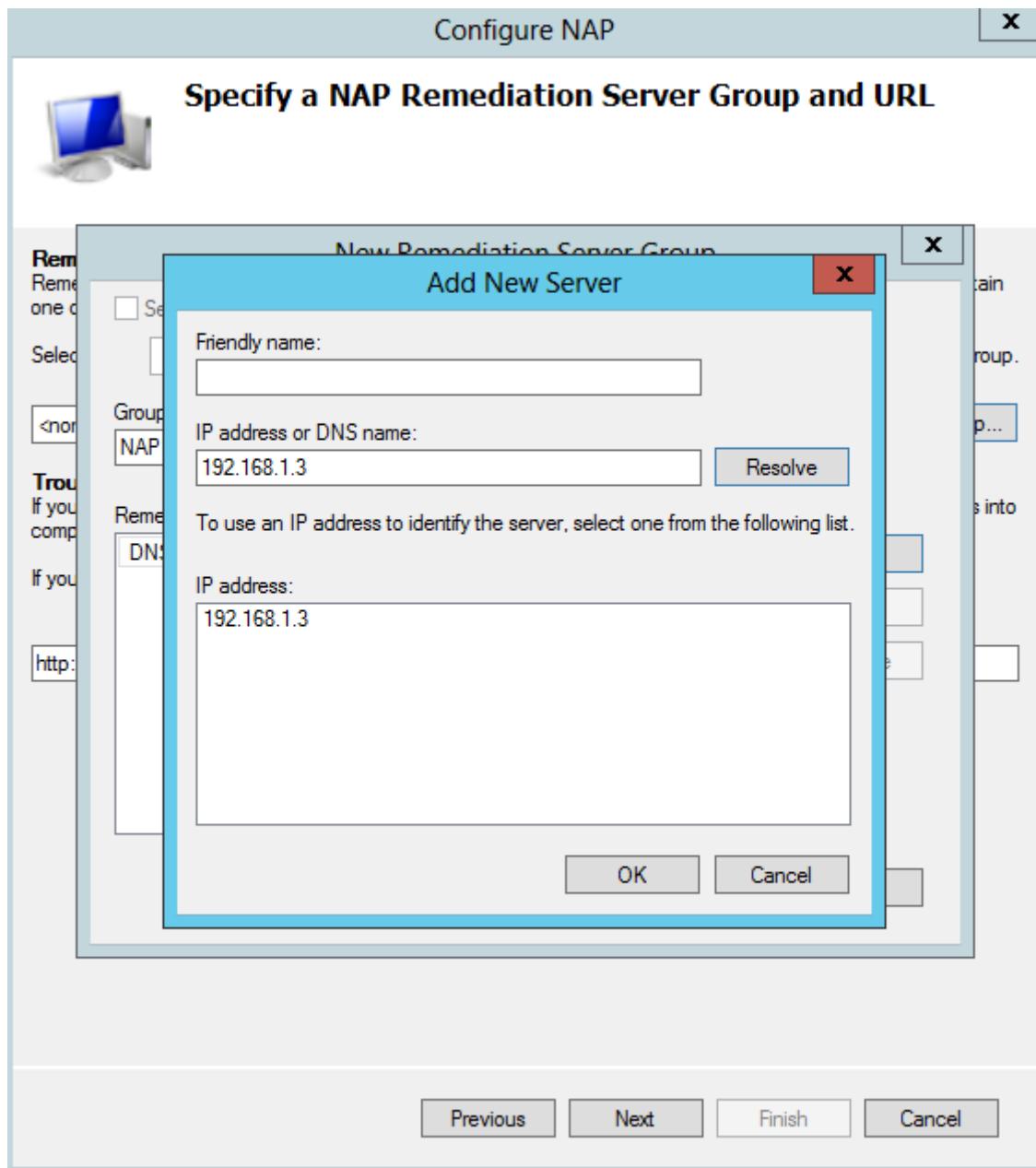
- Tại **Specify a NAP Remediation Server Group and URL** , click vào **New Group**.



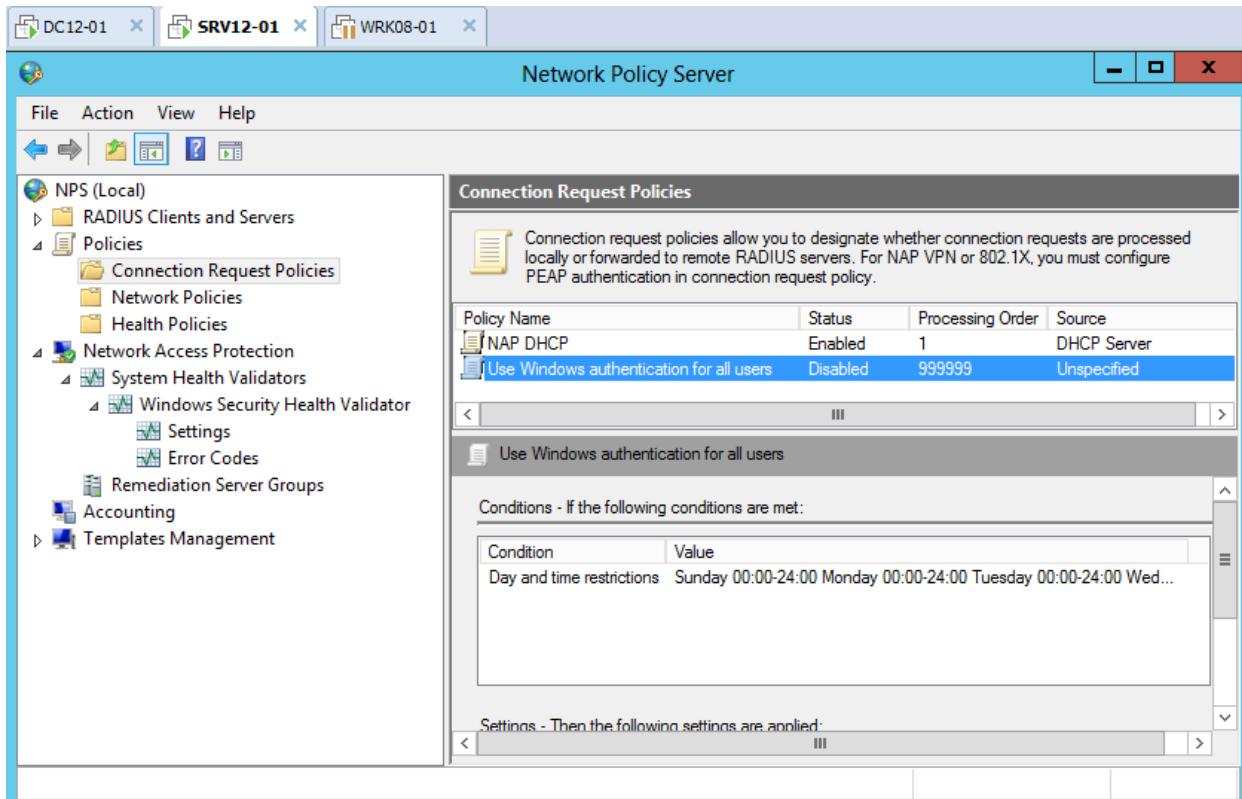
- Tại cửa sổ **New Remediation Server Group**, nhập vào :
 - Group Name: **NAP DHCP**. => click vào Add...



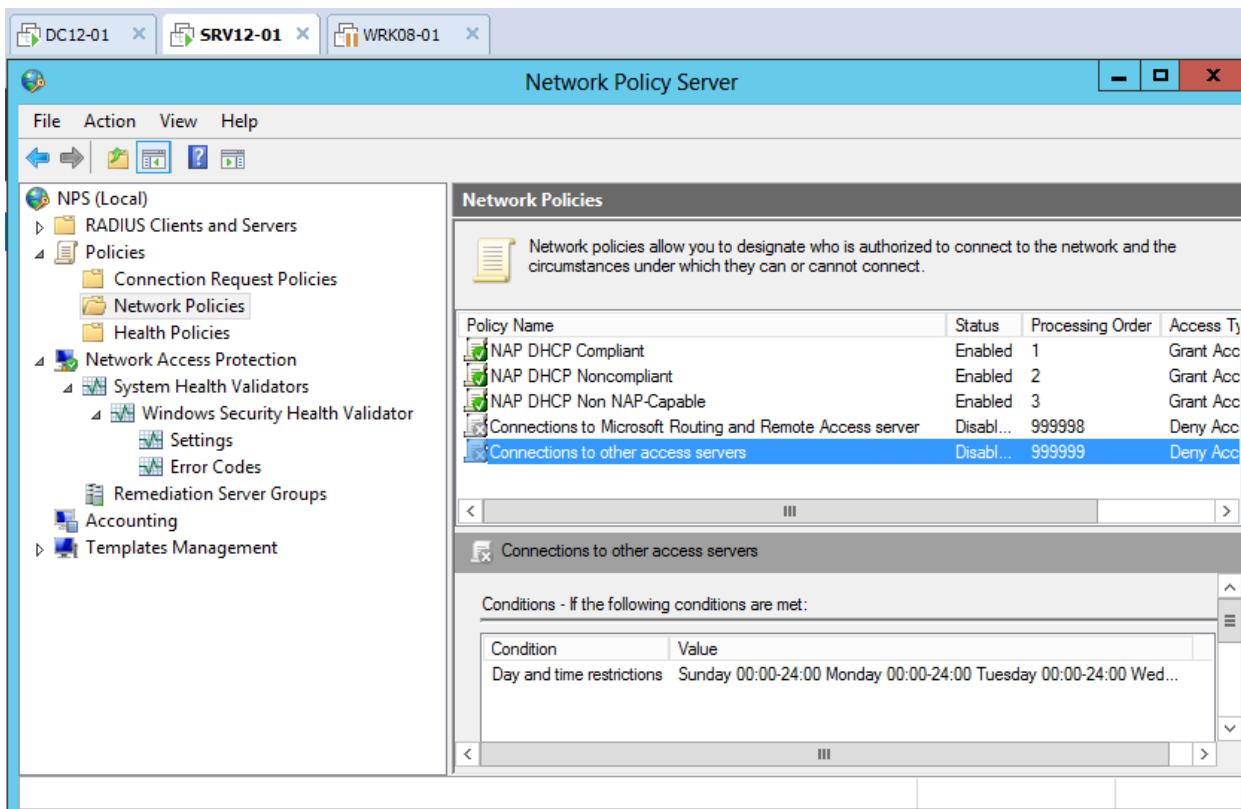
- Tại cửa sổ **Add New Server**, nhập vào :
 - *IP address or DNS name* : **192.168.1.3** (địa chỉ máy DHCP Server) => click vào **Resolve**.
 - **OK**
 - **Next => Finish.**



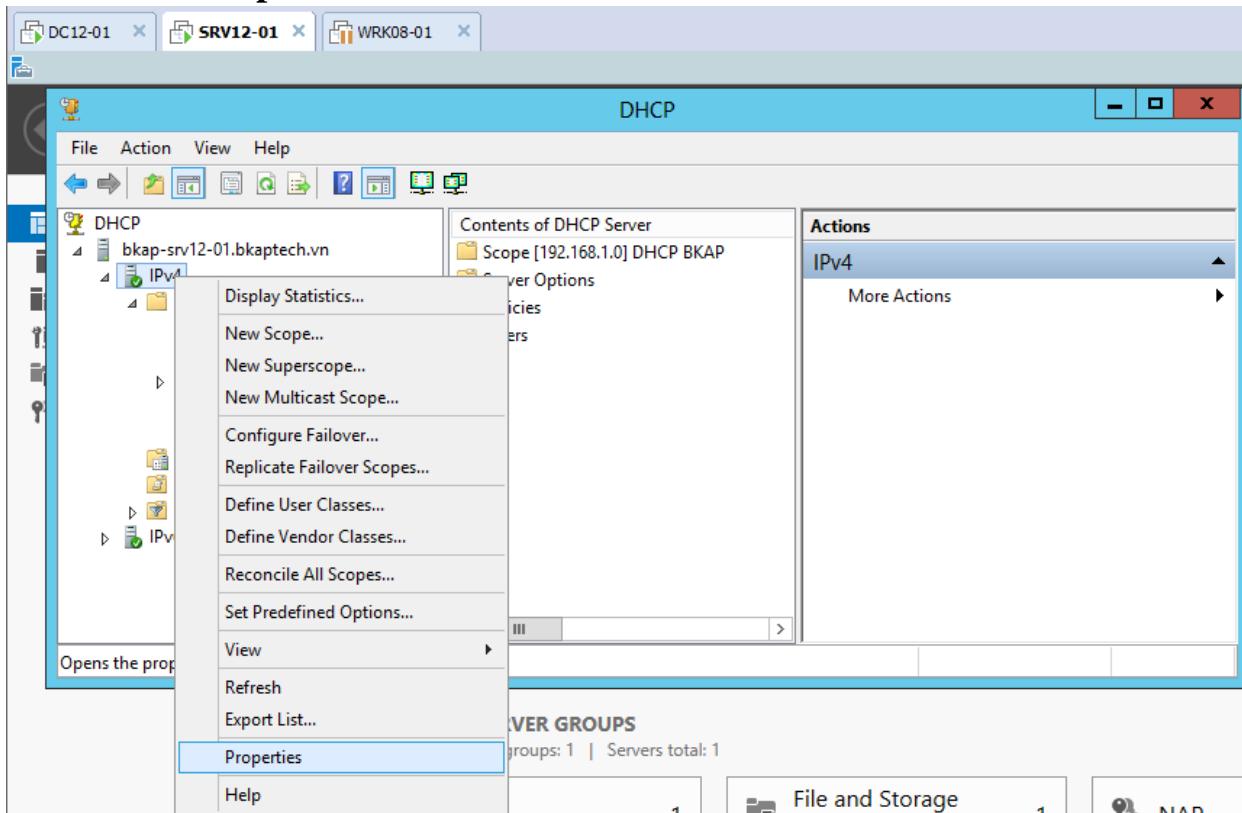
- Tại cửa sổ **Network Policy Server**, chọn vào **NPS (Local) / Policies / Connection Request Policies**.
 - Thực hiện *Disable* chính sách “**Use Windows authentication for all users**”.



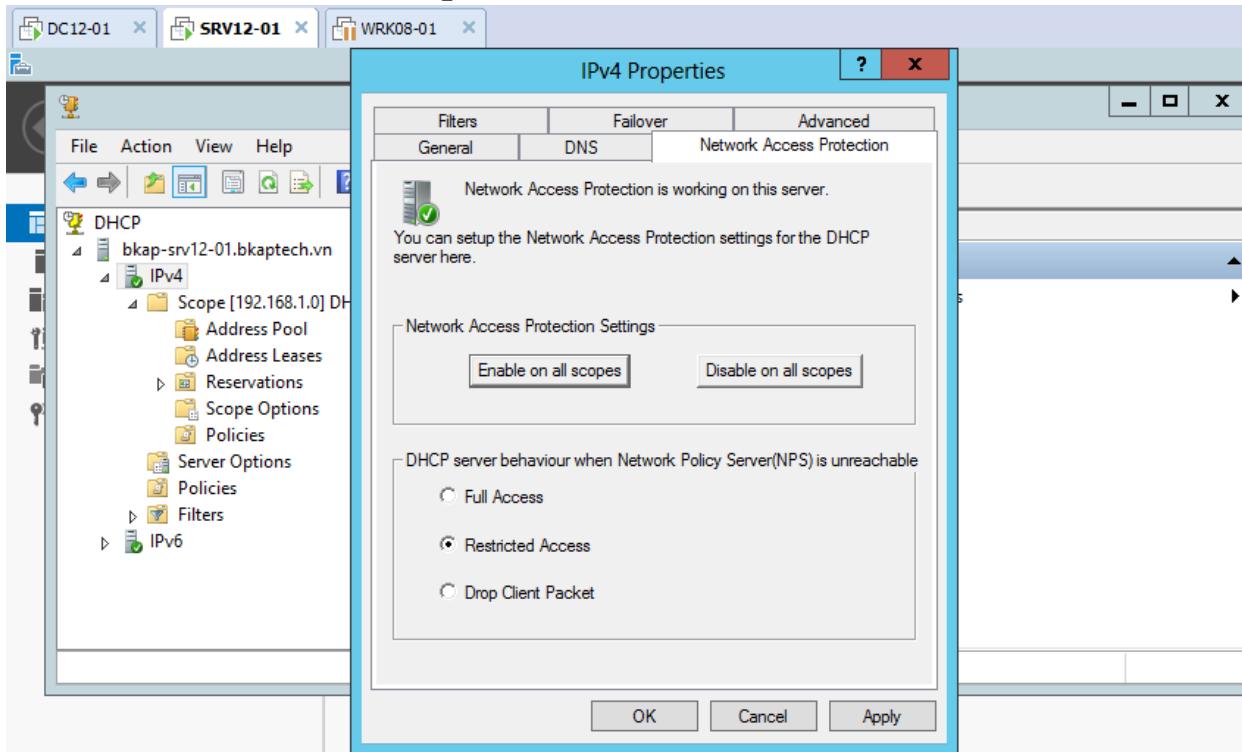
- Tại Network Policies , thực hiện **Disable 2** chính sách Connections



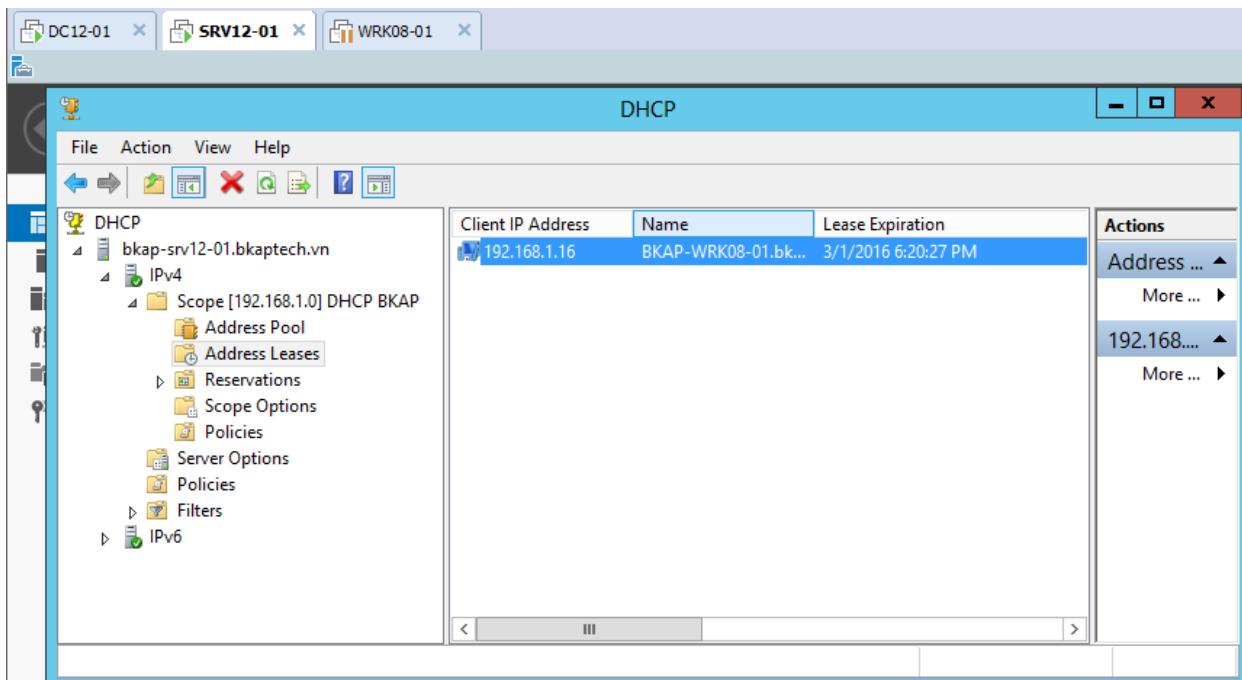
- Vào dịch vụ **DHCP Server**, click chuột phải tại **IPv4** chọn **Properties**.



- Tại cửa sổ **IPv4 Properties**, chuyển sang tab **Network Access Protection**, chọn vào **Restricted Access**, => click vào **Enable on all scopes** => OK.



- Vào **Address Leases** để kiểm tra.



- Chuyển sang máy **Client BKAP-WRK08-01**, gõ lệnh gpupdate /force tại cmd để máy Client áp dụng chính sách.

```

Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

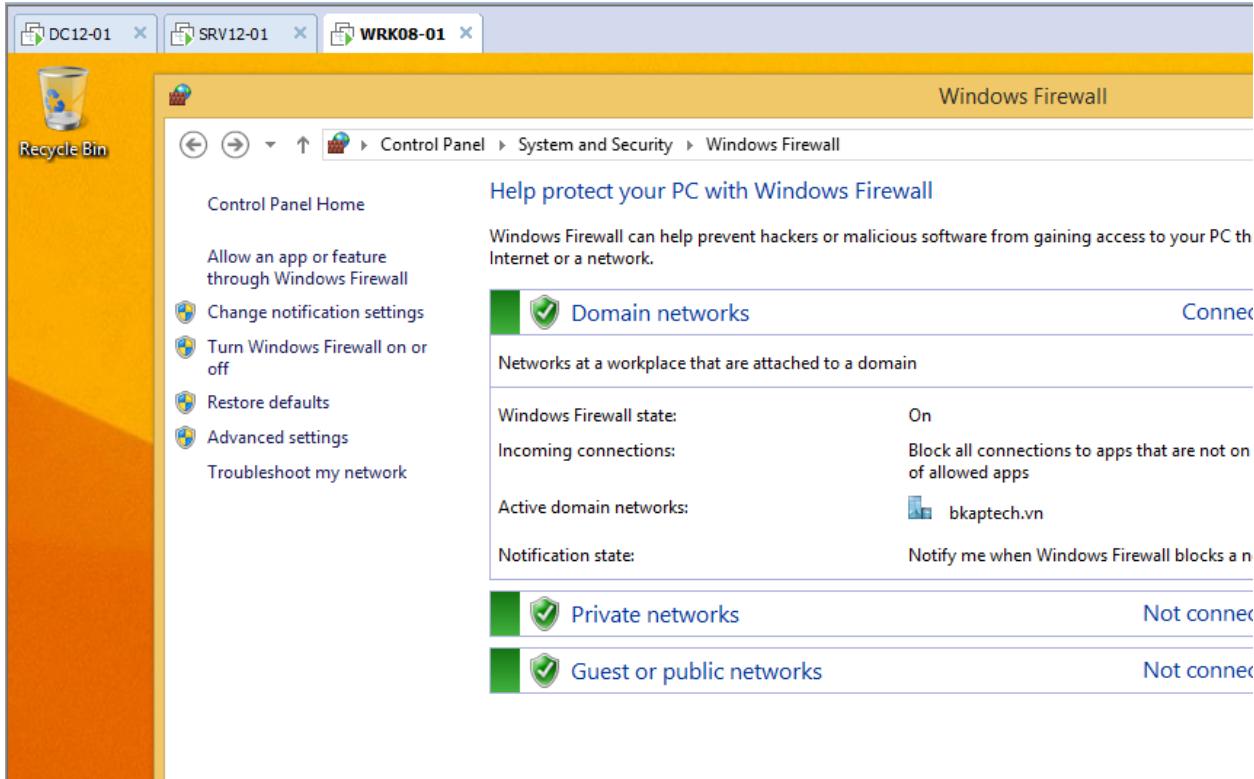
C:\Users\administrator>gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.

C:\Users\administrator>_

```

- Kiểm tra tắt Firewall (Firewall sẽ tự động bật trở lại).



9.2 Triển khai cài đặt và cấu hình dịch vụ NAP VPN.

1. Yêu cầu bài lab:

+ Triển khai NAP để bảo mật cho hệ thống VPN:

- Máy **VPN Client** nào không bật **Windows Firewall**, khi kết nối VPN thành công sẽ tự động bật **Windows Firewall**.

+ Trên máy *BKAP-DC12-01*:

- Tạo 1 tài khoản để thiết lập VPN.
- Cài **Enterprise root CA**.

+ Trên máy *BKAP-SRV12-01*:

- Join Domain: **bkaptech.vn**
- Xin **Computer Certificate** cho *Server*.
- Cấu hình **Trust Root CA**.
- Cài đặt **Network Policy and Access Services** và cấu hình **Network Policy Server (NPS)**.
- Cài đặt và cấu hình **VPN Server**.
- Cấu hình **Windows Firewall**.
- Cấu hình **System Health Validators**.

+ Trên máy *BKAP-WRK08-01*:

- Cấu hình **NAP Client** và bật một số dịch vụ hỗ trợ.
- Tạo **VPN Connection**.
- Client kiểm tra kết nối **VPN**.

2. Yêu cầu chuẩn bị:

+ Máy *BKAP-DC12-01*:

- **Windows Server 2012** đã nâng cấp **Domain Controller** quản lý miền **bkaptech.vn** và cài **DNS Server**.
- Trên AD tạo user : **hungnq** , Password : **123456a@** , cấp quyền **Remote Access Permission**.

+ Máy *BKAP-SRV12-01*:

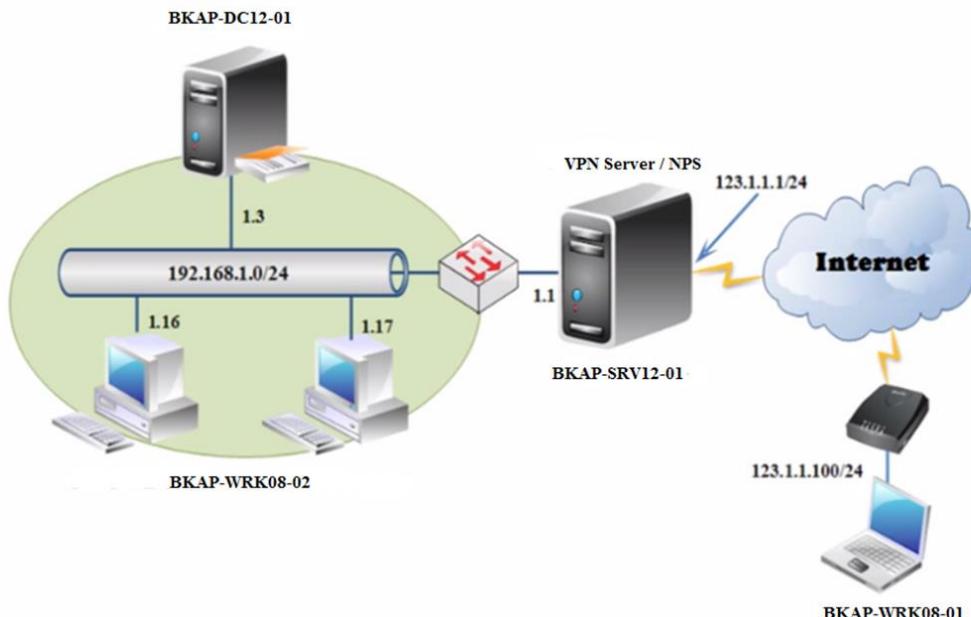
- Có 2 card mạng : Card mạng 1 ứng với **LAN** , card mạng 2 ứng với **WAN**.

+ Máy *BKAP-WRK08-01*:

- Làm **VPN Client** là **Windows 8**.

3. Mô hình lab:

HỆ THỐNG ĐÀO TẠO CNTT QUỐC TẾ BACHKHOA-APTECH
Lab 9.2 Triển khai cài đặt và cấu hình dịch vụ NAP VPN



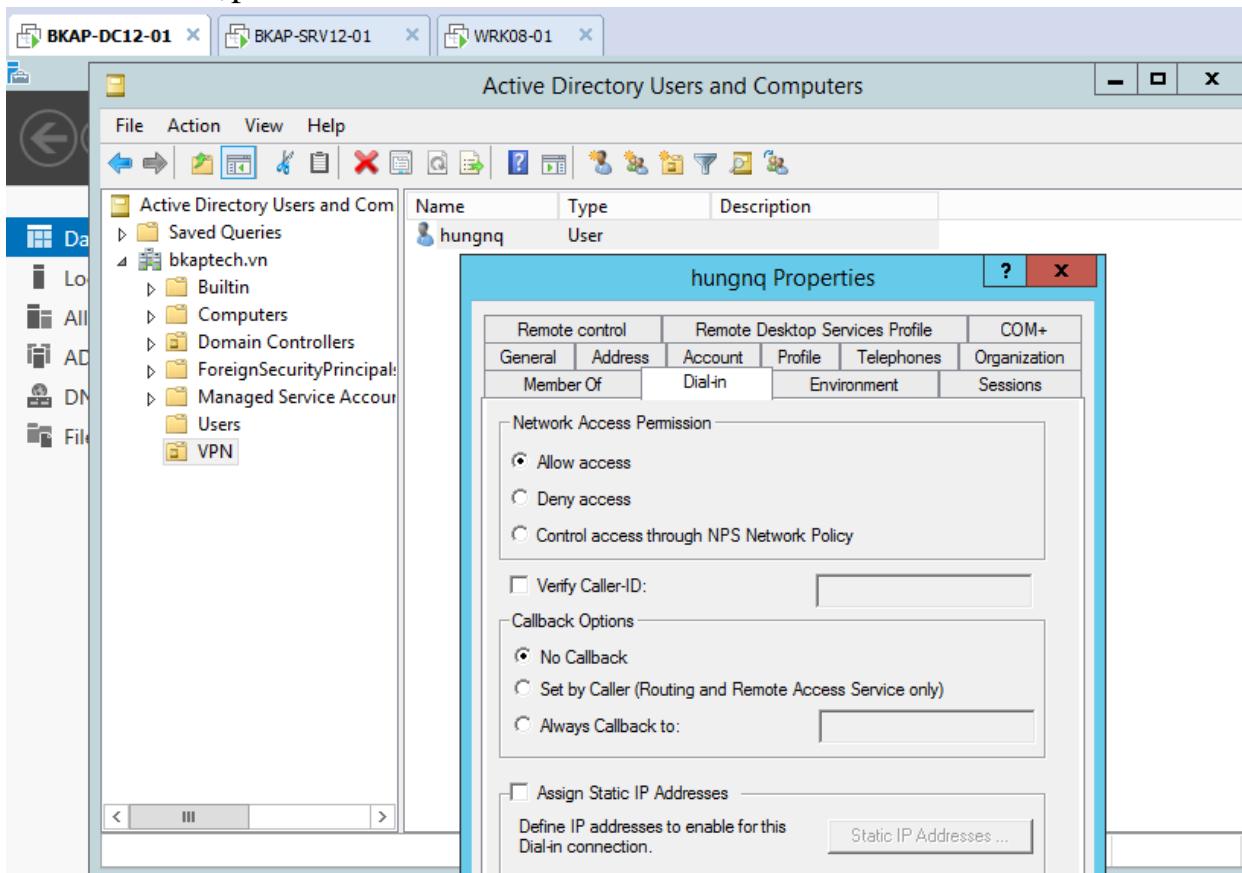
Hình 9.2

Sơ đồ địa chỉ như sau:

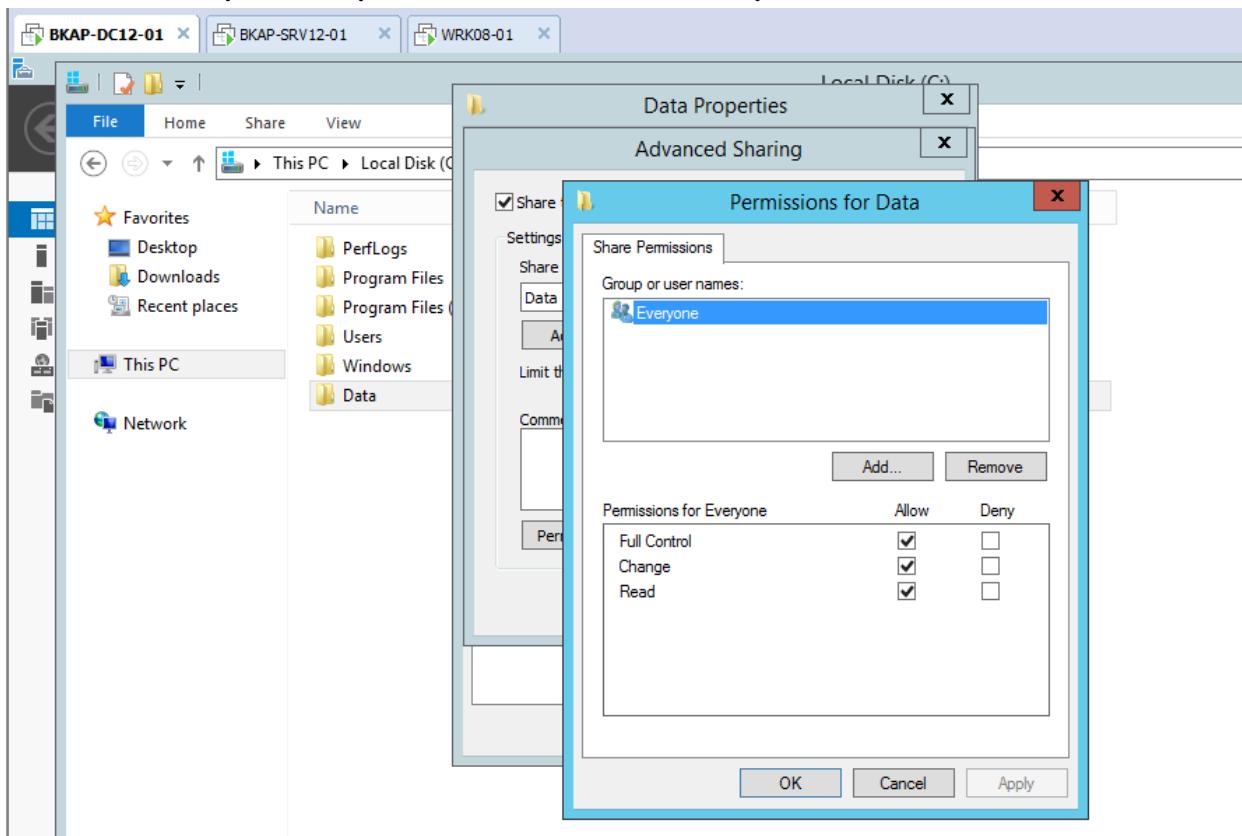
Thông số	BKAP-DC12-01	BKAP-SRV12-01	BKAP-WRK08-01
IP address	192.168.1.2	NIC 1: 192.168.1.1 NIC 2: 123.1.1.1	123.1.1.100
Gateway	192.168.1.1	--	123.1.1.1
Subnet Mask	255.255.255.0	255.255.255.0	255.255.255.0
DNS Server	192.168.1.2	--	--

Hướng dẫn chi tiết:

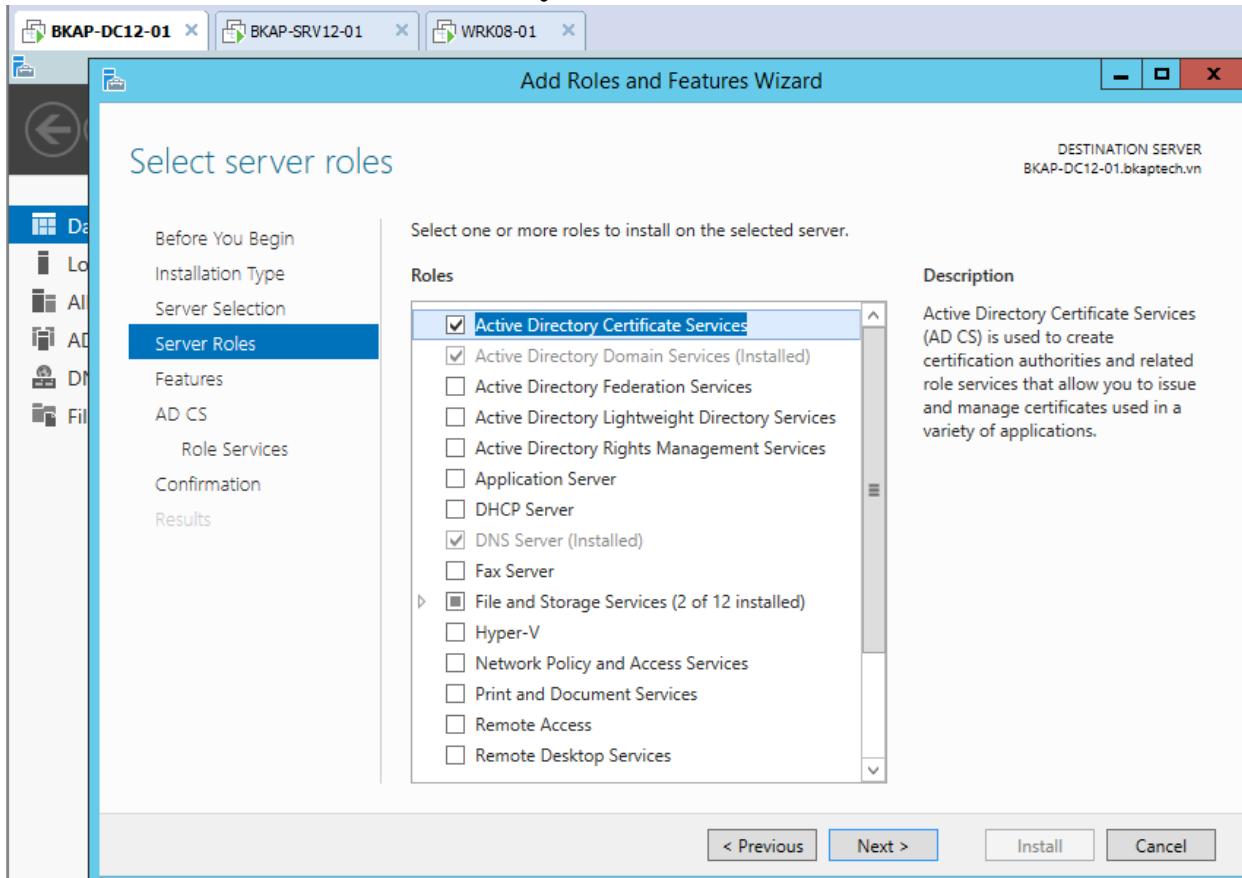
- Mở các máy ảo, kết nối như hình trên, **ping** thông giữa các máy kết nối trực tiếp.
- Trên máy *BKAP-DC12-01*, thực hiện các bước sau:
 - Tạo *OU VPN*, trong *OU VPN*, tạo tài khoản **hungnq**, cấp quyền truy cập *VPN* cho tài khoản.



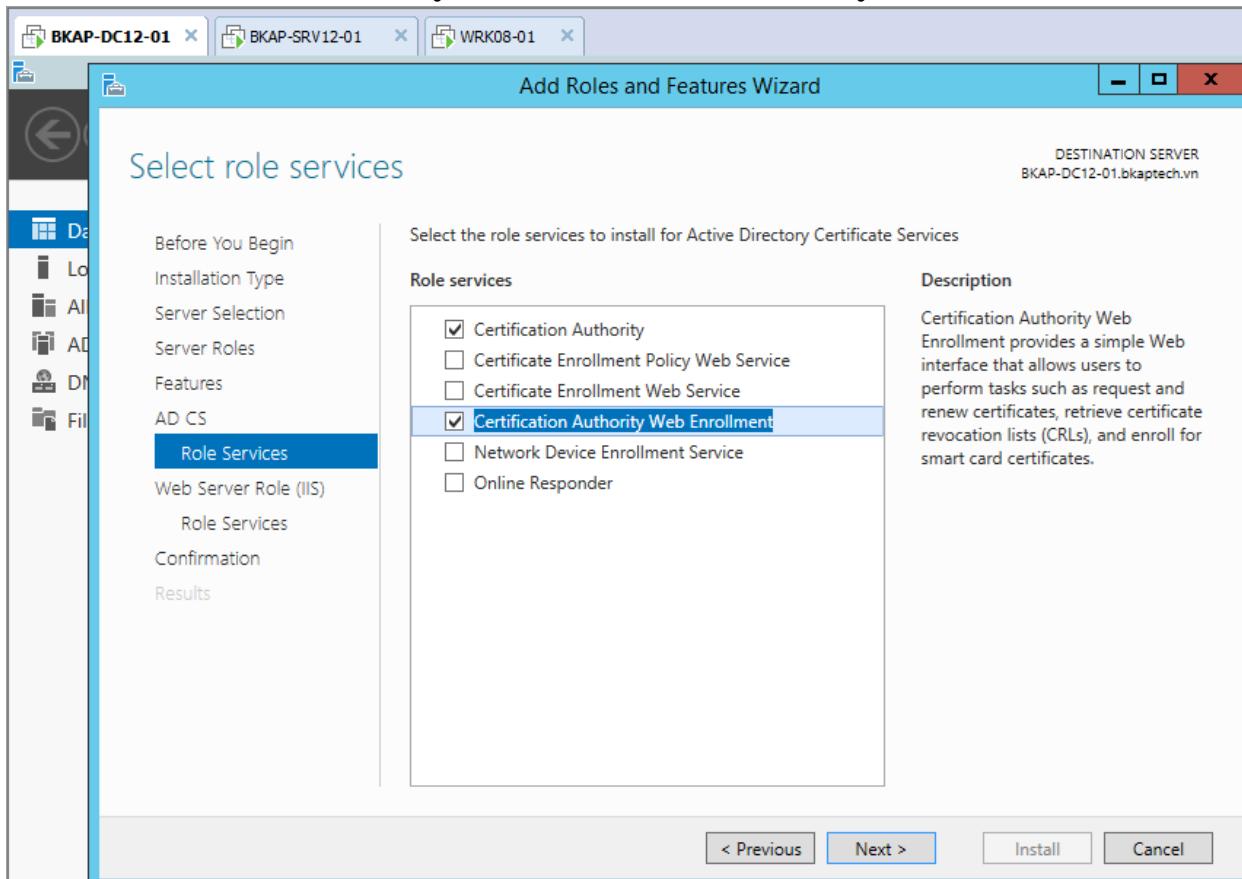
- Tạo thư mục “Data” và chia sẻ dữ liệu.



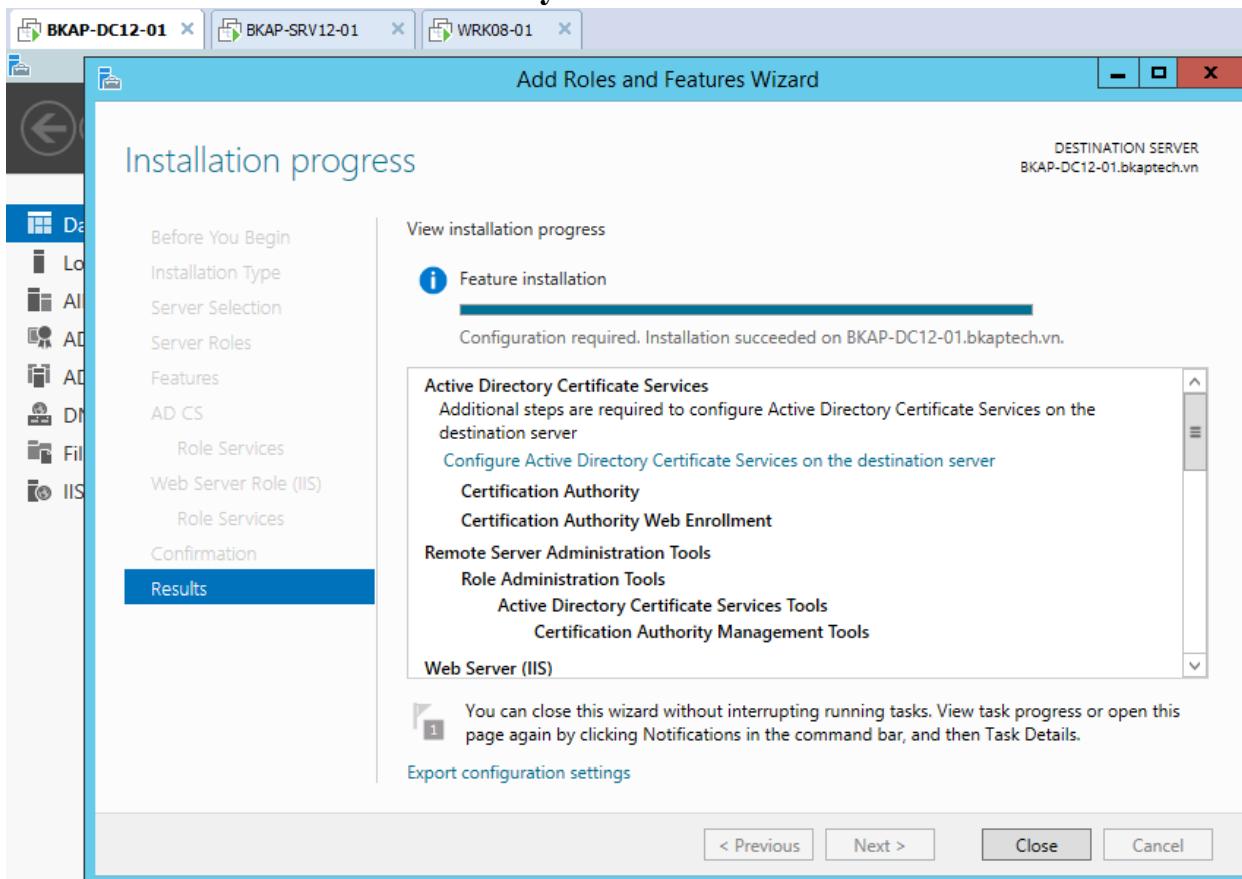
- Thực hiện cài đặt dịch vụ **Enterprise Root CA**.
 - **Server Manager / Add roles and features / chọn vào dịch vụ Active Directory Certificate Services.**



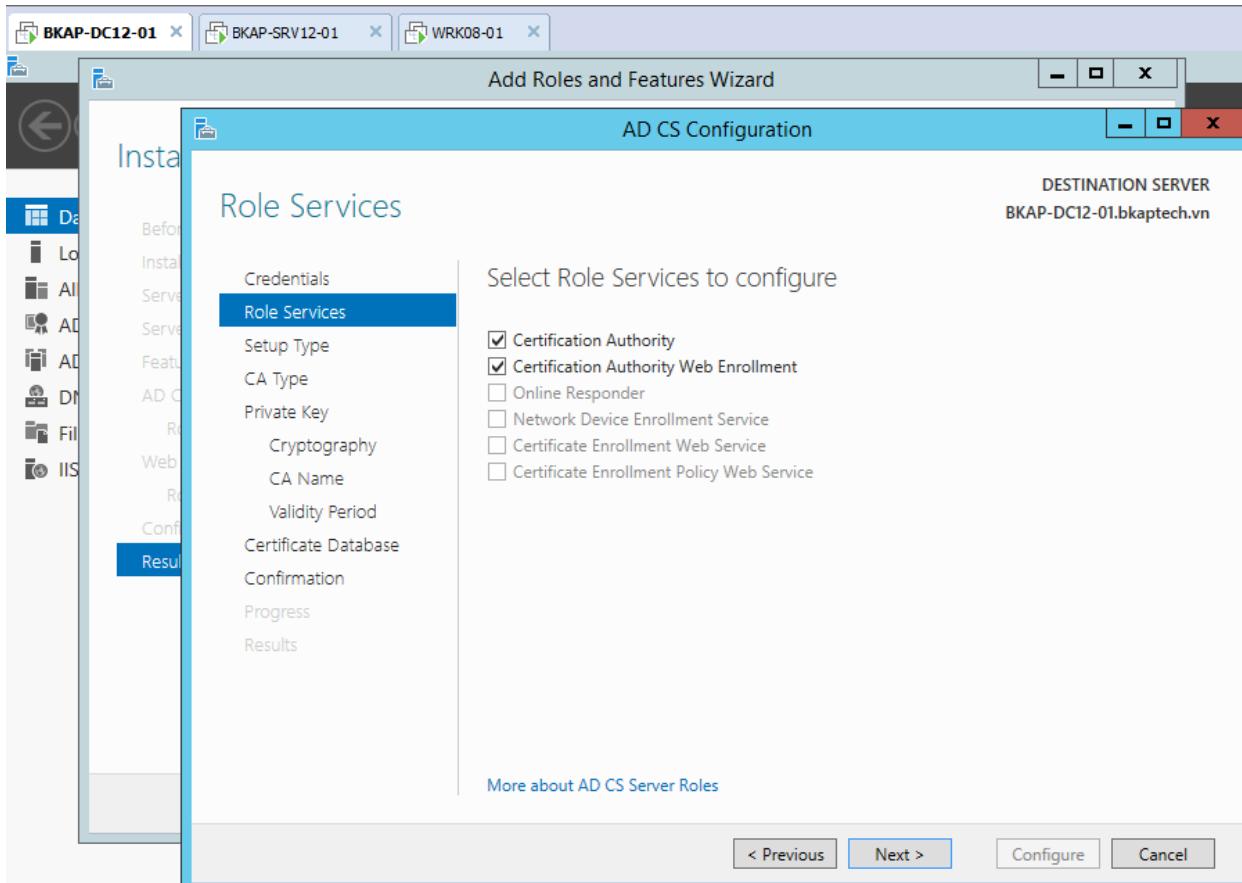
- Tại cửa sổ **Select role services**, chọn vào **Certification Authority** và **Certification Authority Web Enrollment**.



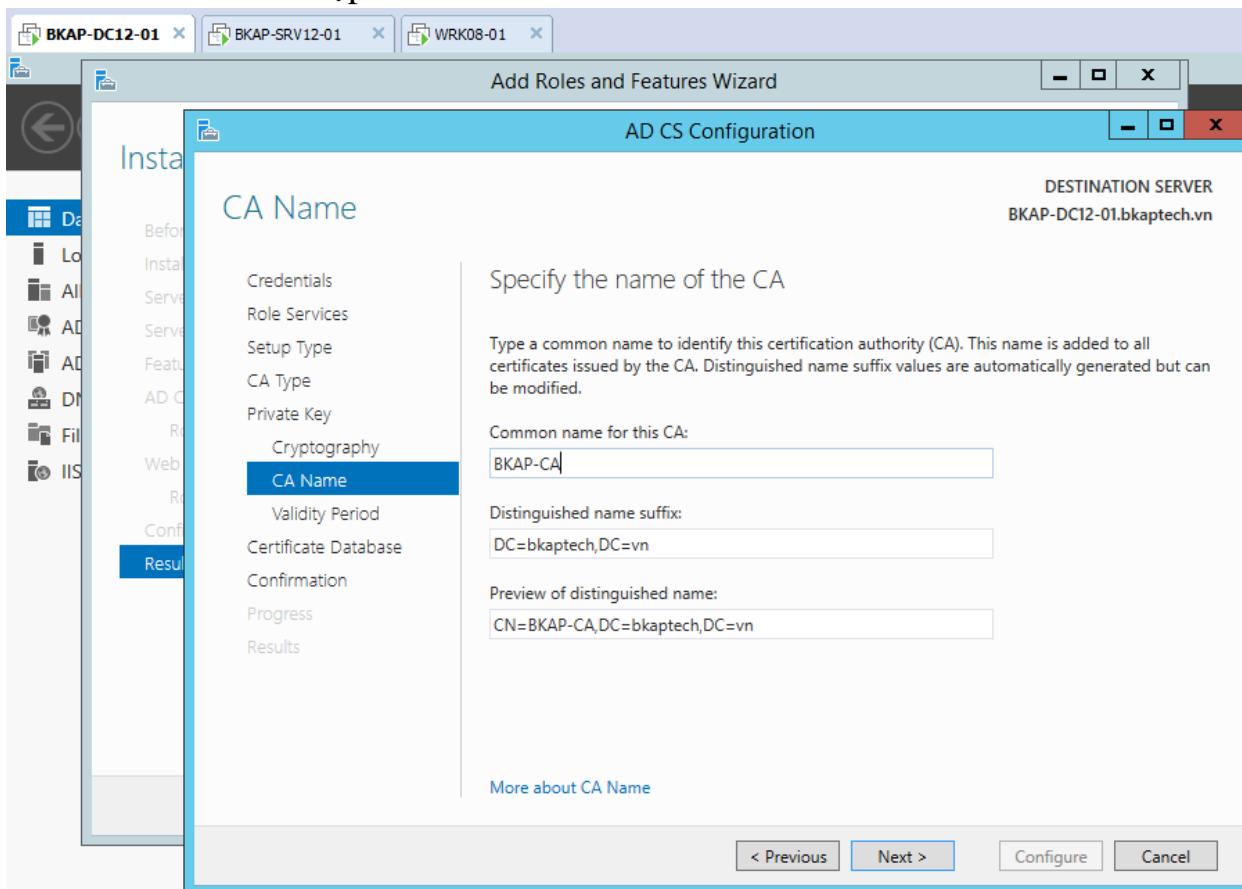
- Khi tiến trình cài đặt được hoàn tất , click vào **Configure Active Directory....on the destination server.**



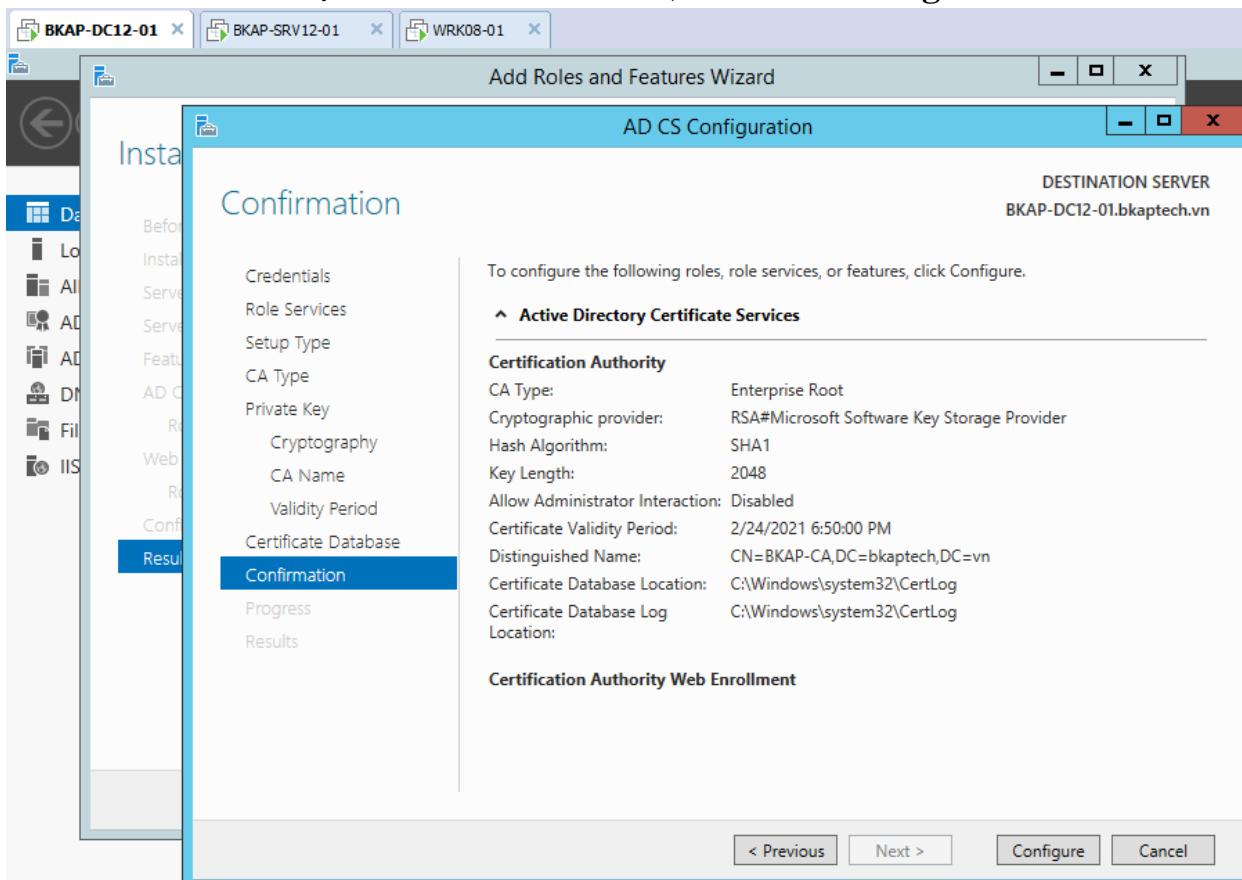
- Tại cửa sổ **Select Role Services to configure**, đánh dấu tại **Certification Authority** và **Certification Authority Web Enrollment**. => Next.

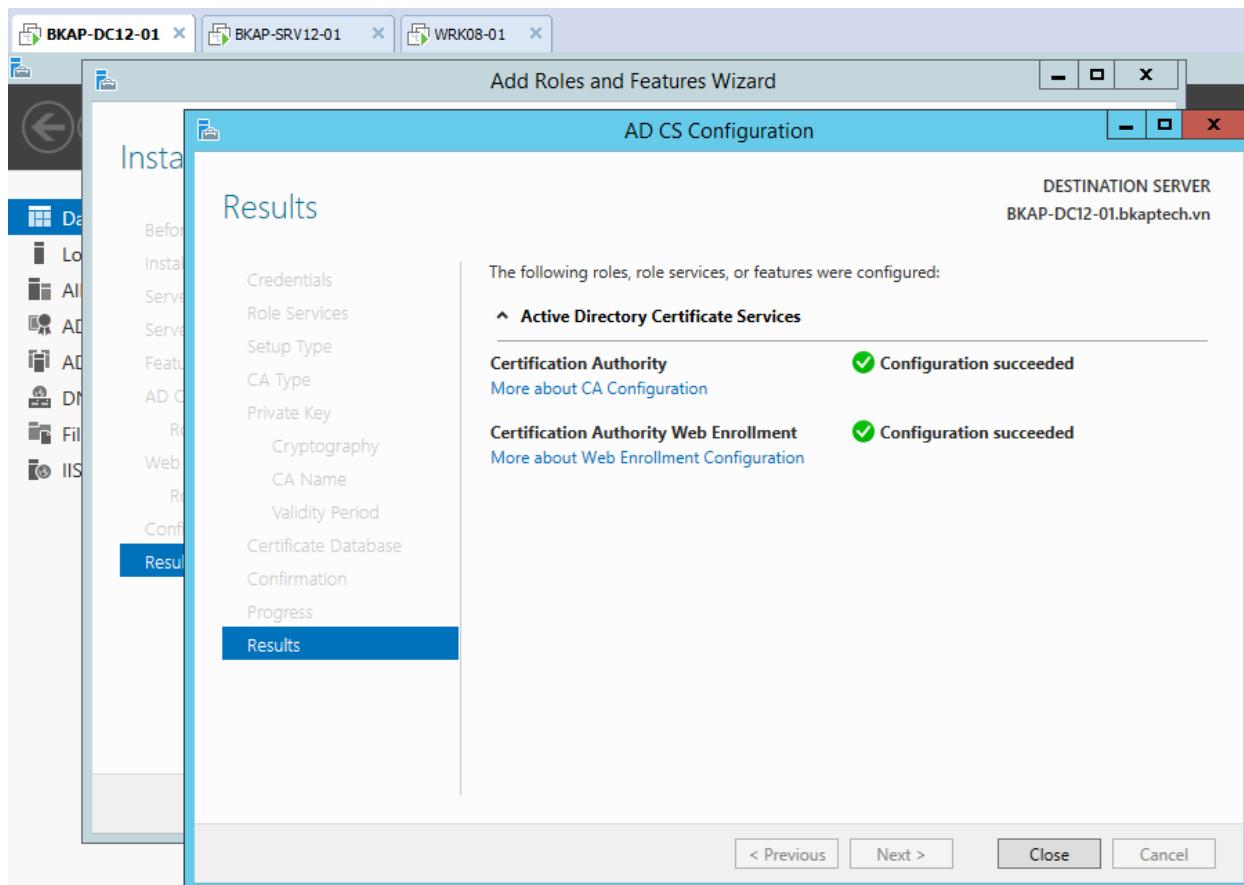


- Tại cửa sổ **CA Name**, tại mục **Common name for this CA** , nhập vào tên CA : **BKAP-CA**.=> Next.



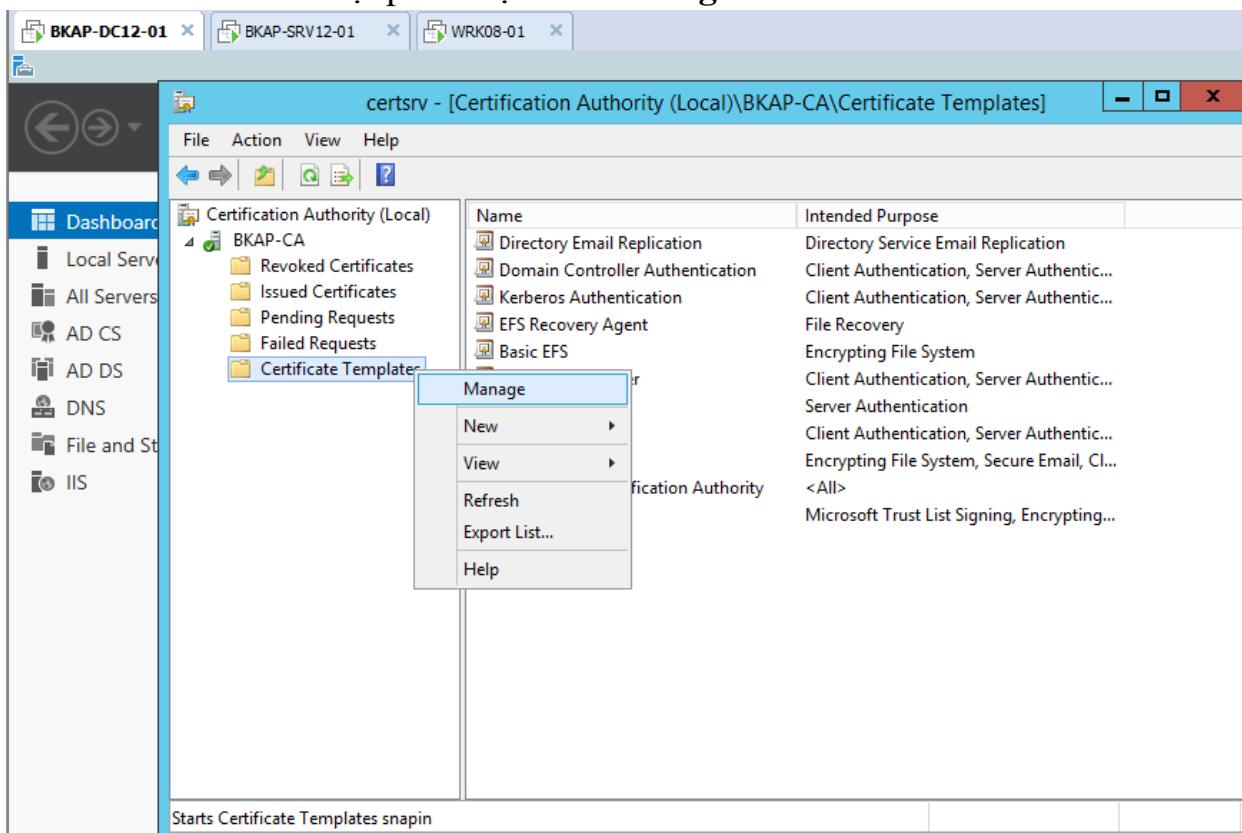
- Tại cửa sổ Confirmation , click vào Configure.



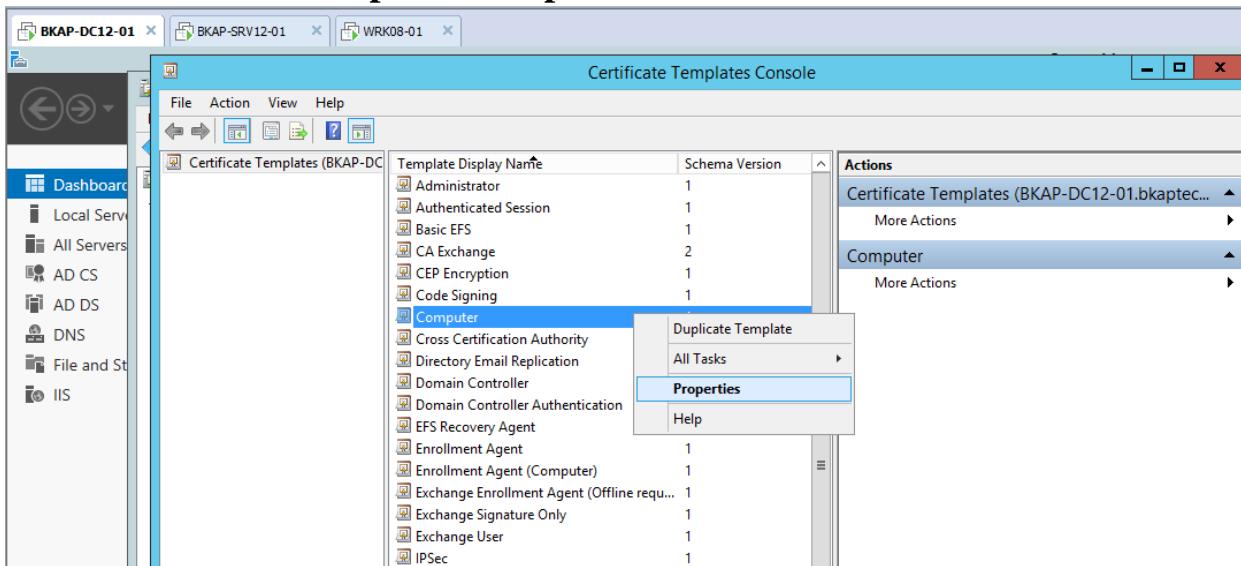


- Cấu hình CA:

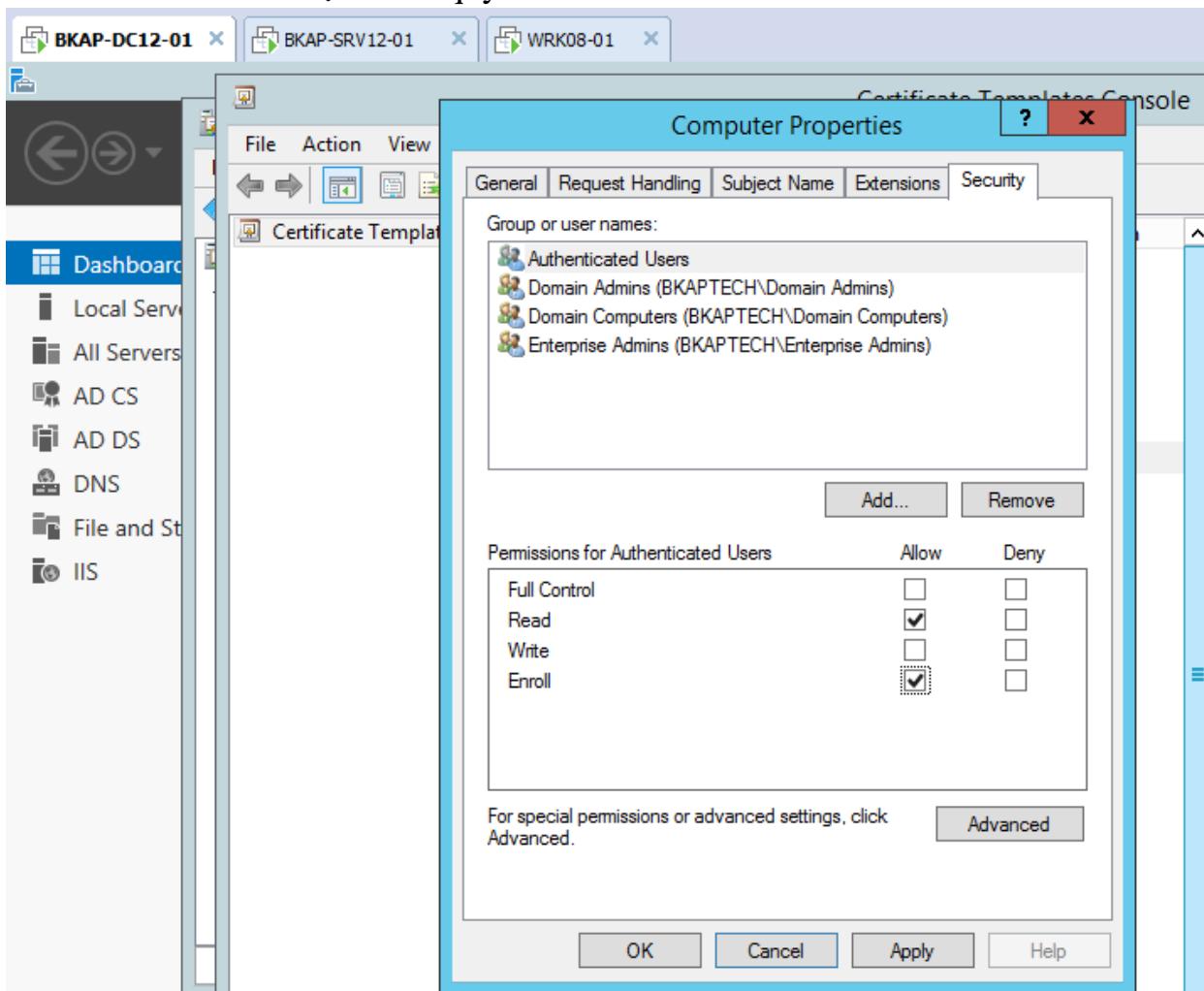
- Tại Server Manager , click vào Tools / Certification Authority
- Trong cửa sổ certsrv... chọn đến Certificate Template / click chuột phải chọn vào Manager.



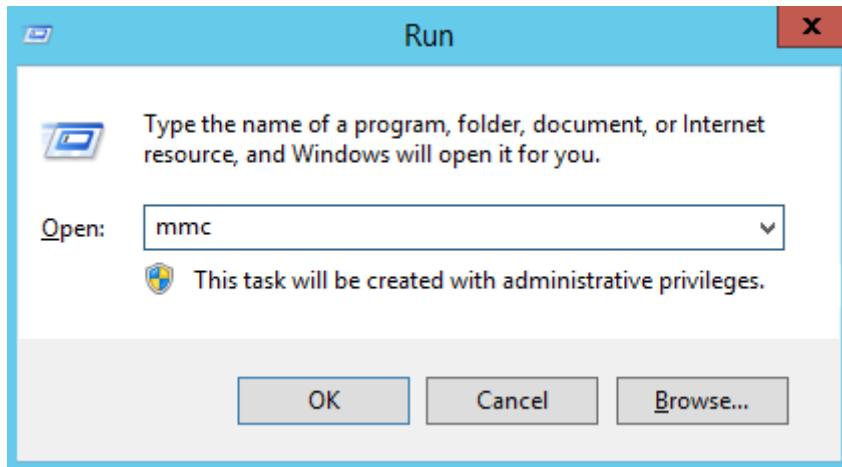
- Tại cửa sổ Certificate Templates Console , chọn đến Computer / Properties.



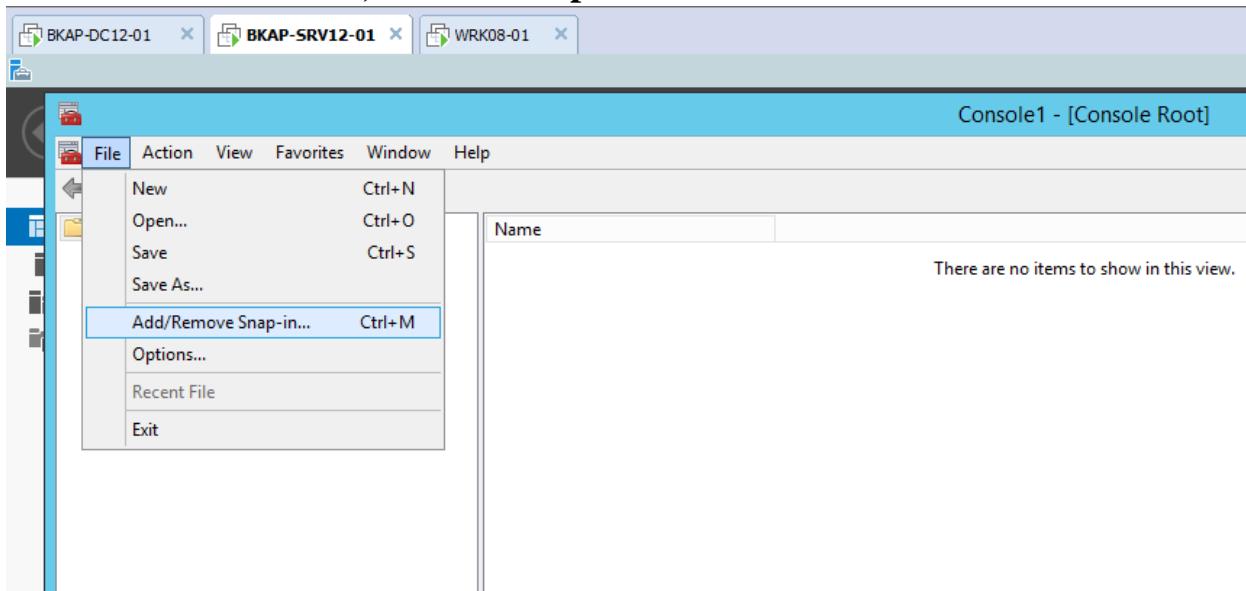
- Tại cửa sổ **Computer Properties**, chuyển sang tab **Security**, chọn thêm quyền “Enroll” cho **Authenticated Users**. => OK.



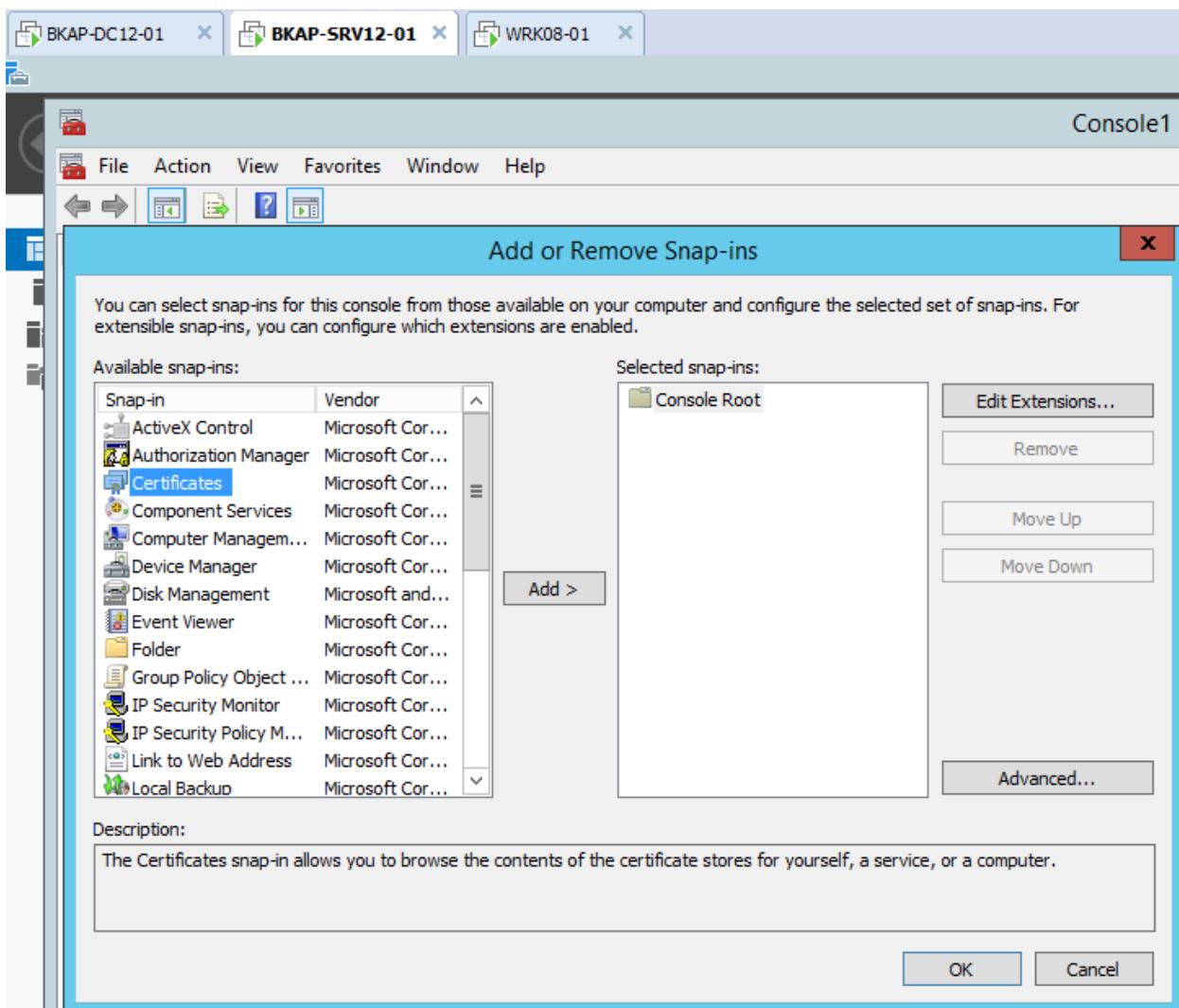
- Chuyển sang máy **BKAP-SRV12-01** :
 - Join máy vào *Domain*, đăng nhập bằng tài khoản *bkaptech\administrator*.
 - Thực hiện xin **Computer Certificate** cho server *BKAP-SRV12-01*.
 - Run / mmc.**



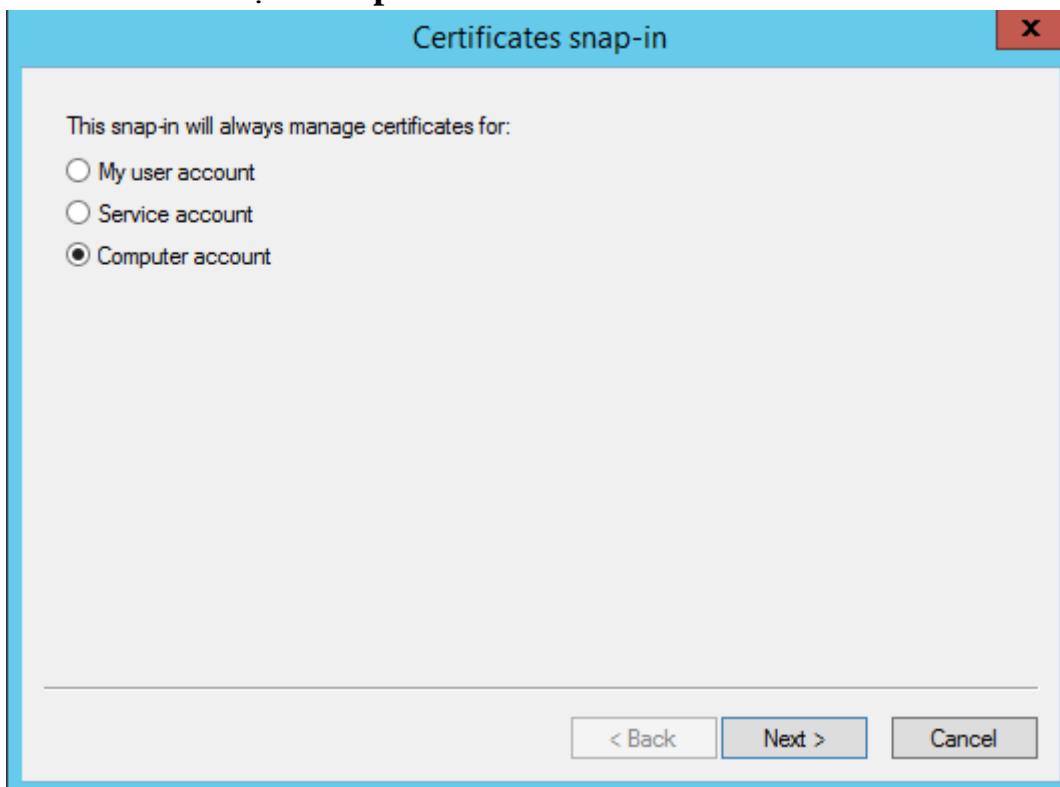
- Tại cửa sổ **Console1 – [Console Root]**, chọn vào **File / Add,Remove Snap-in**.



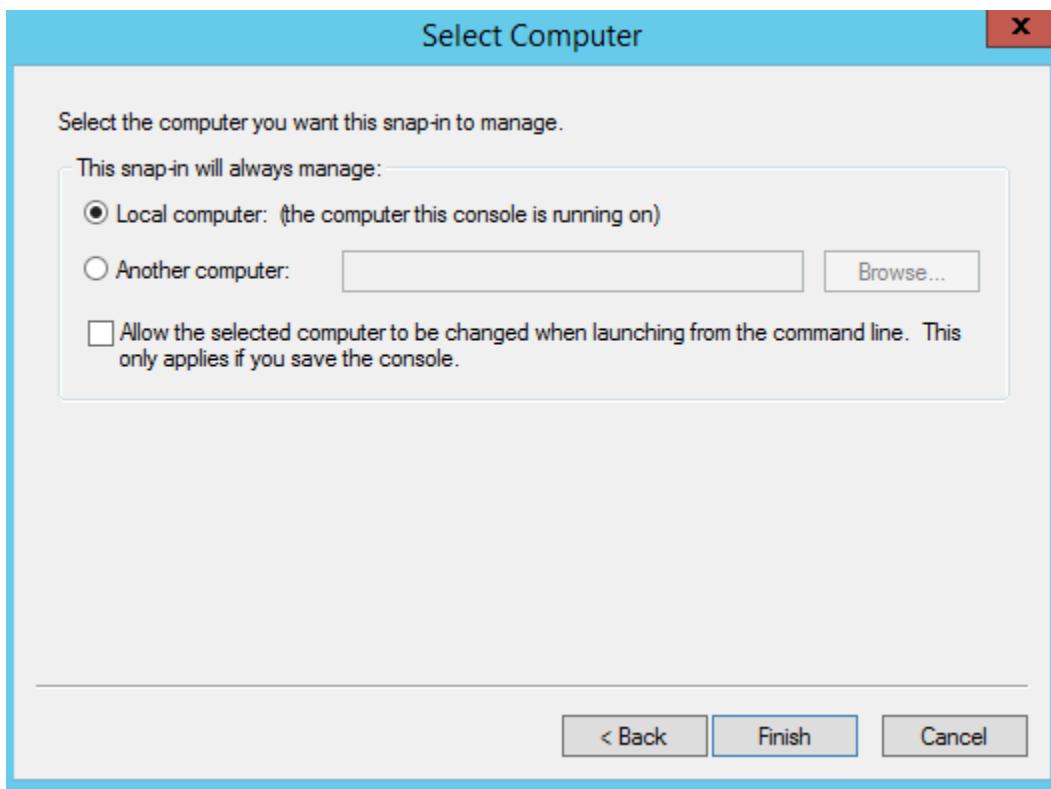
- Tại cửa sổ Add or Remove Snap-ins , chọn đến Certificates => Add.



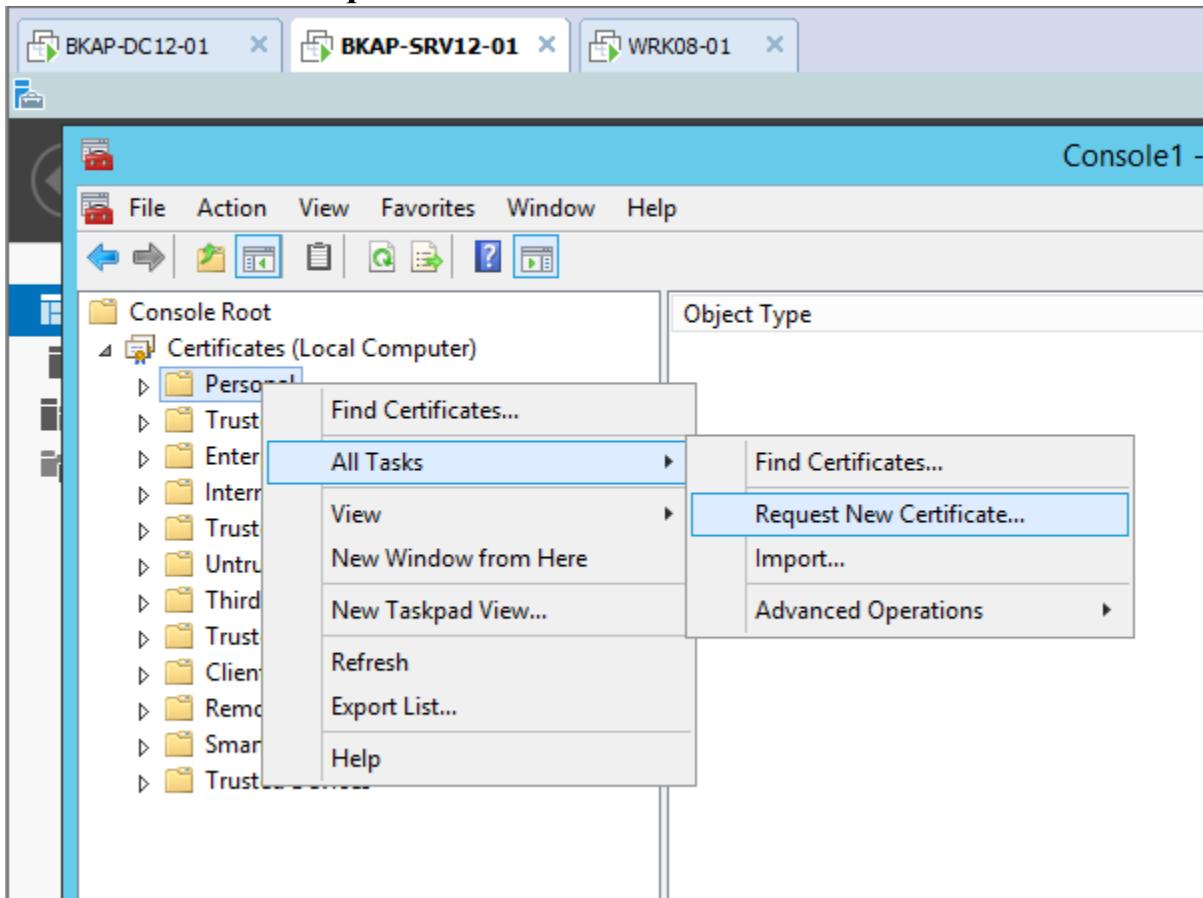
▪ Chọn Computer account => Next.



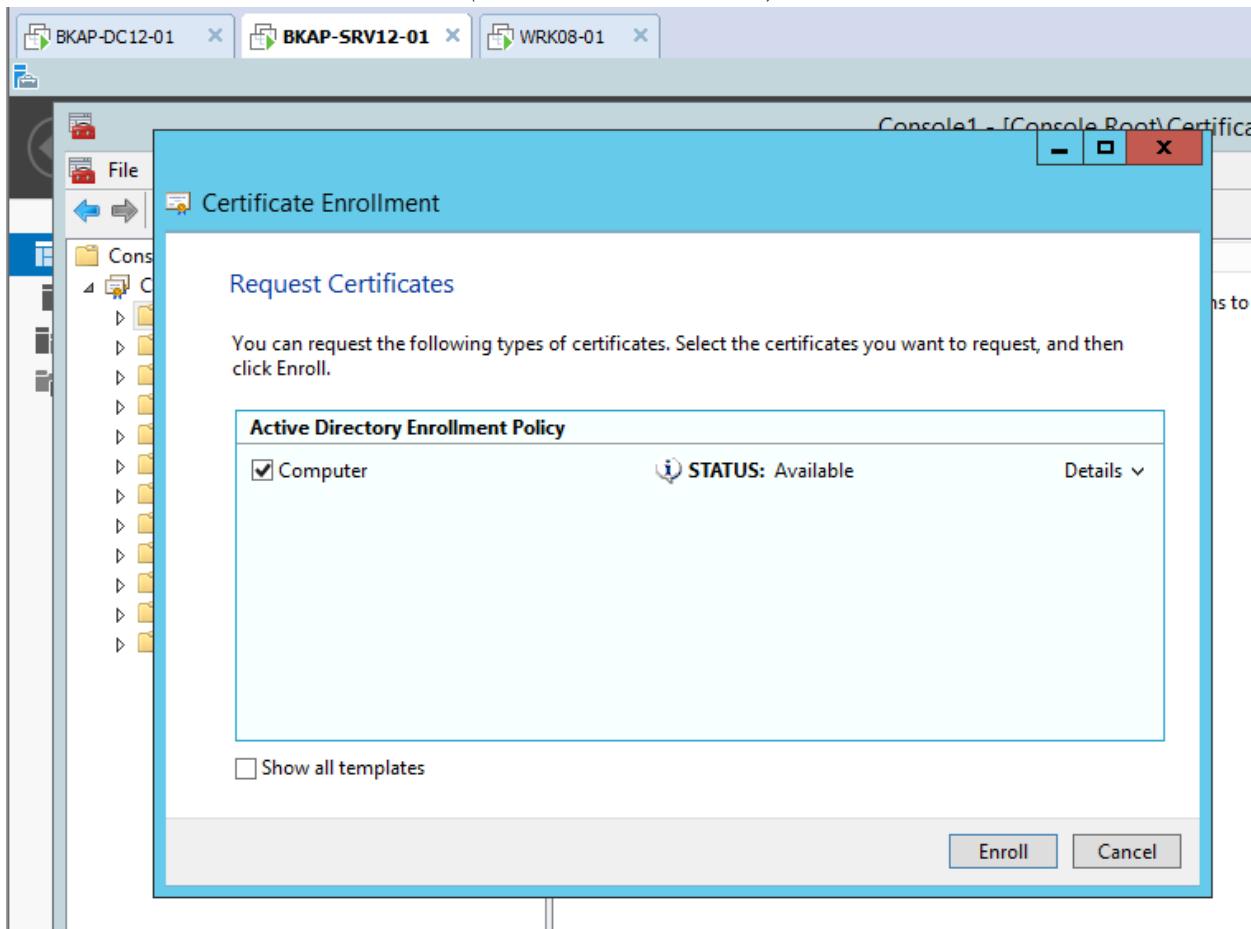
- Click vào **Finish**.

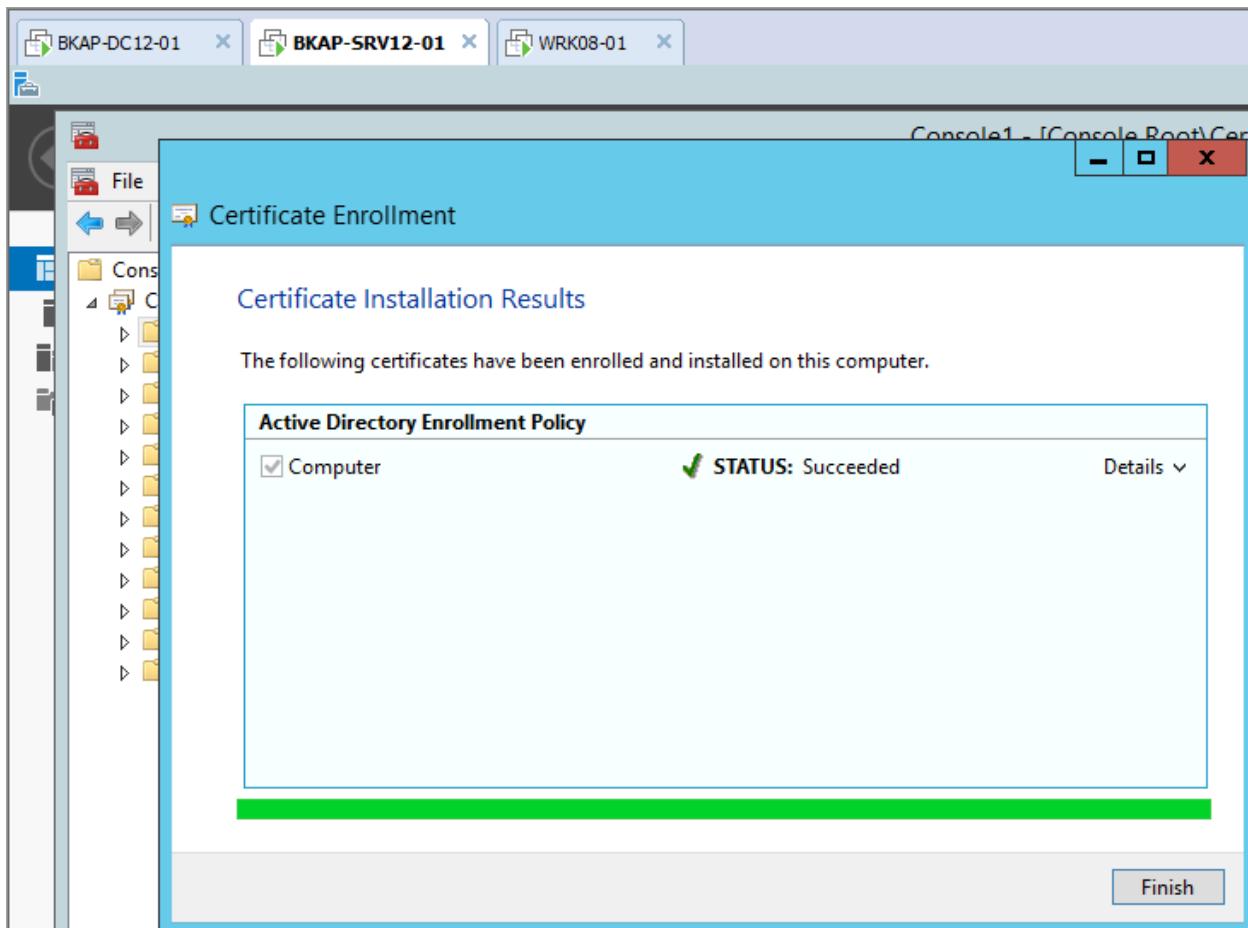


- Tại cửa sổ Console1... chọn vào Personal / All Task => Request New Certificate...

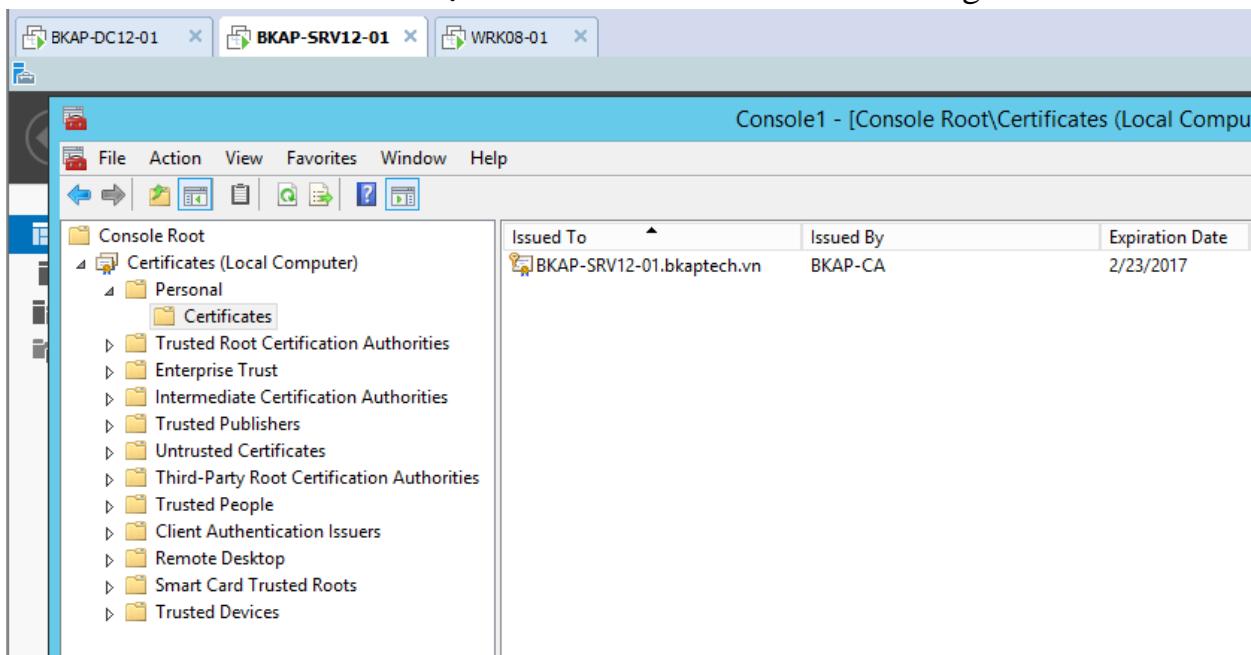


- Tại cửa sổ **Certificate Enrollment** , click vào **Next**.
- Tại **Request Certificates** , đánh dấu vào **Computer** => click vào **Enroll** (*Status: succeeded*)

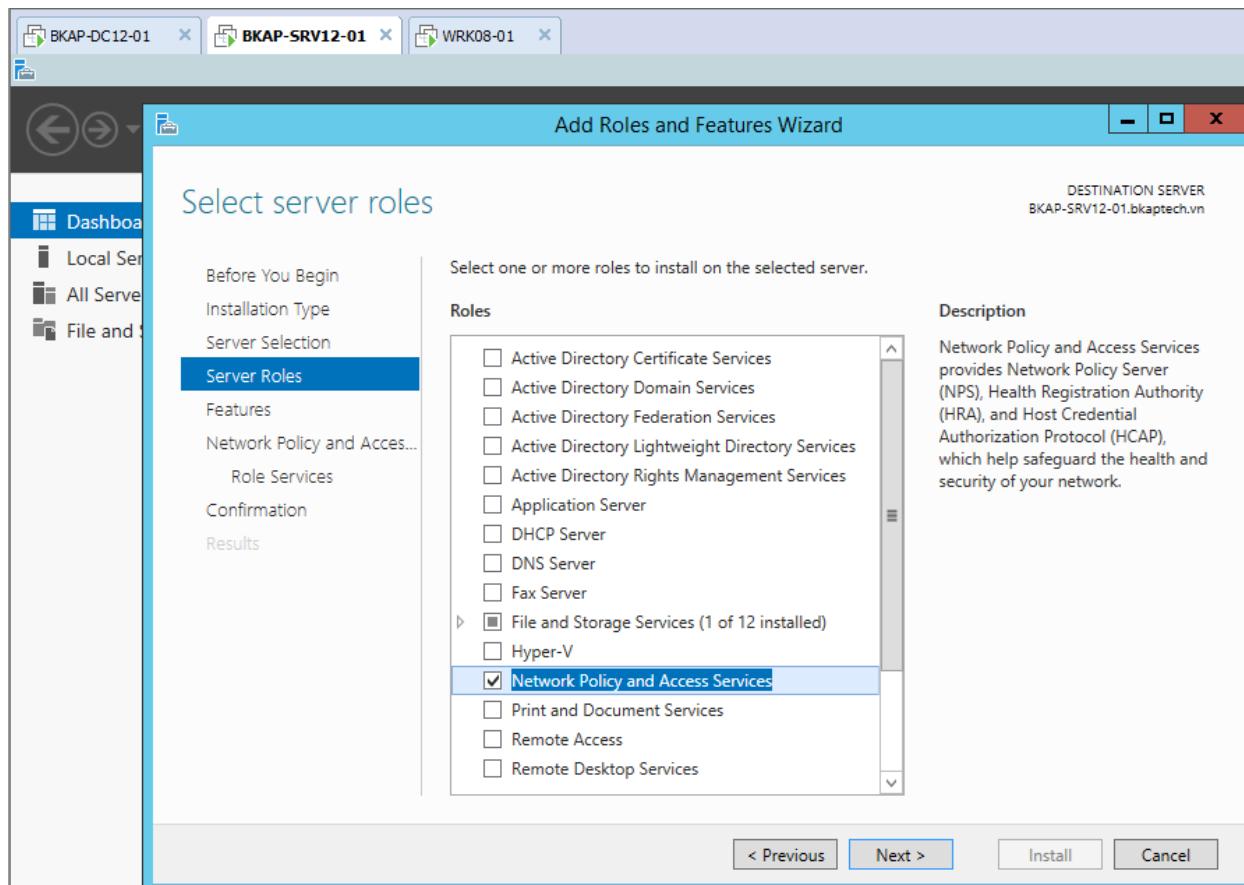




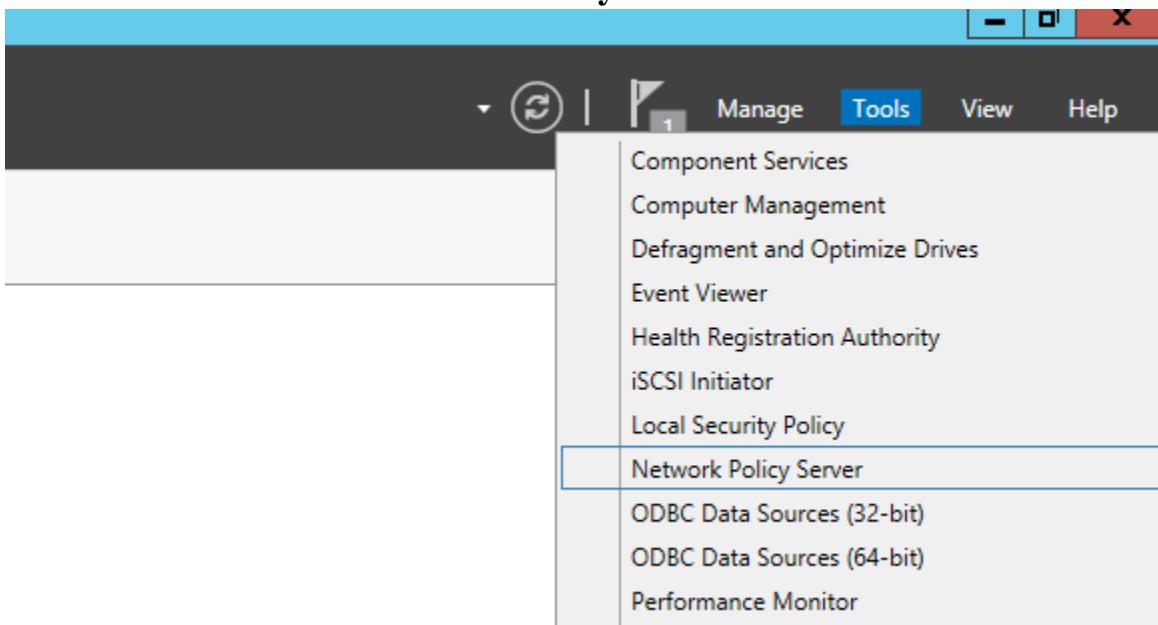
- Kiểm tra tại Personal / Certificates có chứng chỉ CA.



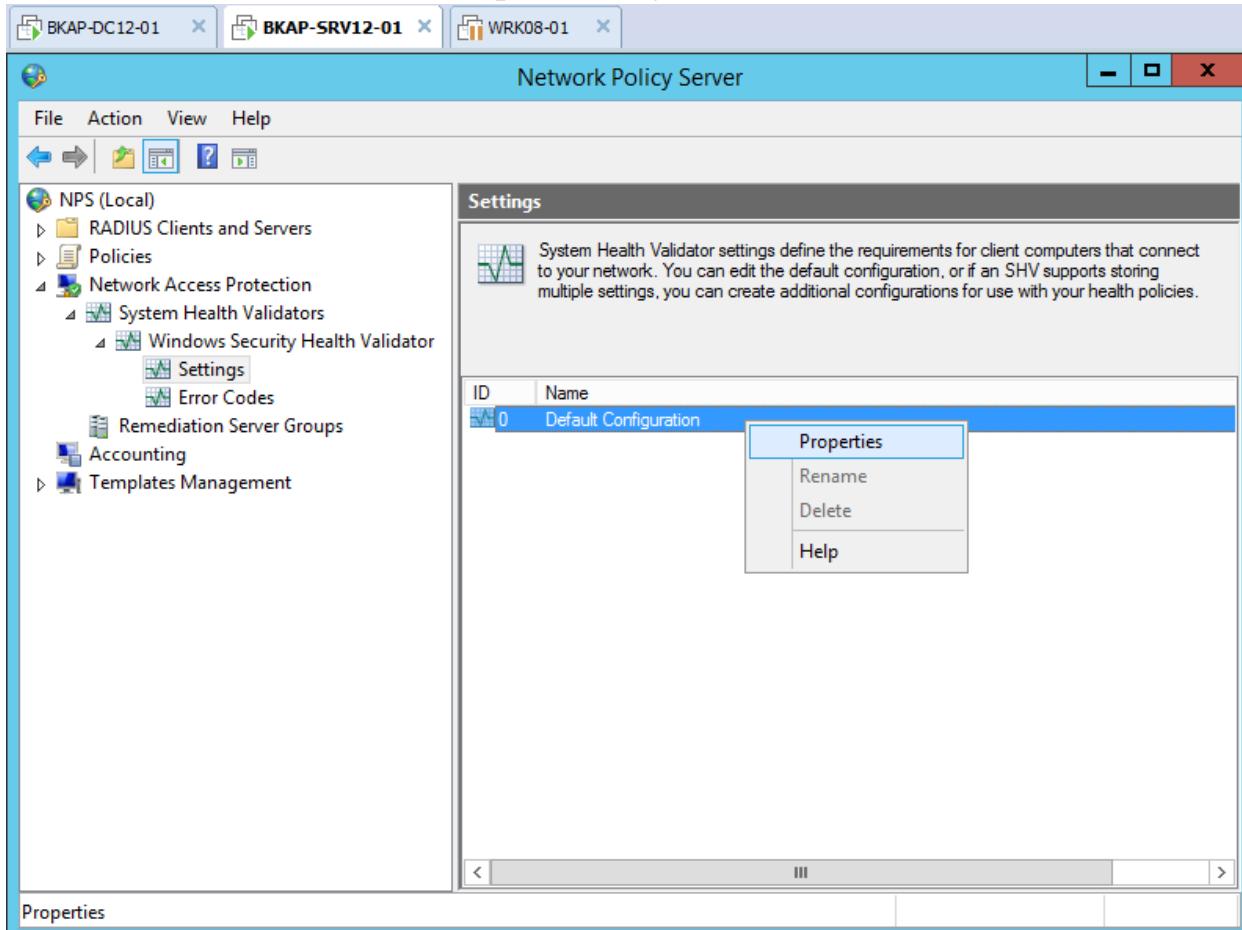
- Cài đặt dịch vụ Network Policy and Access Services.



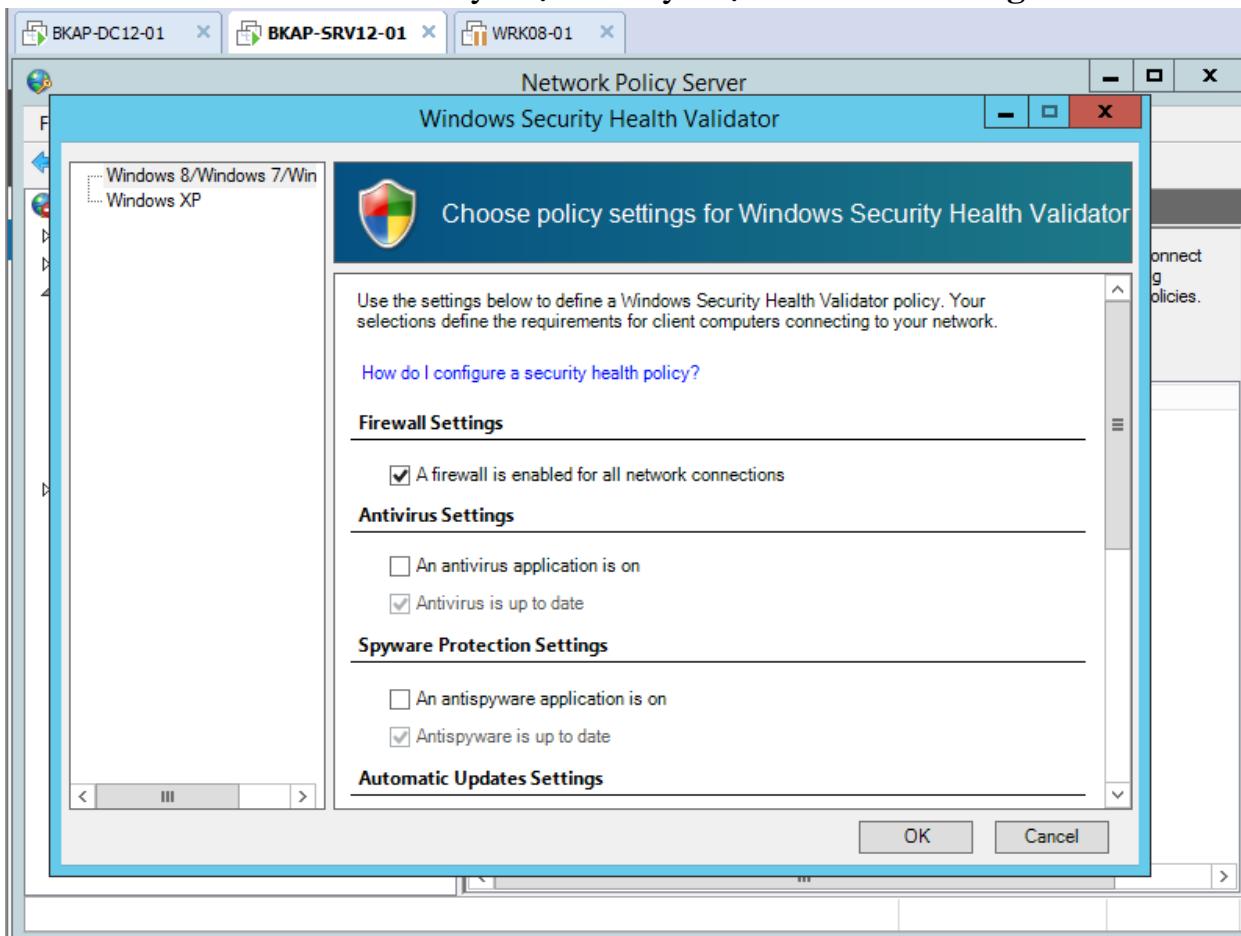
- Cấu hình dịch vụ NPS.
 - Tools / Network Policy Server.



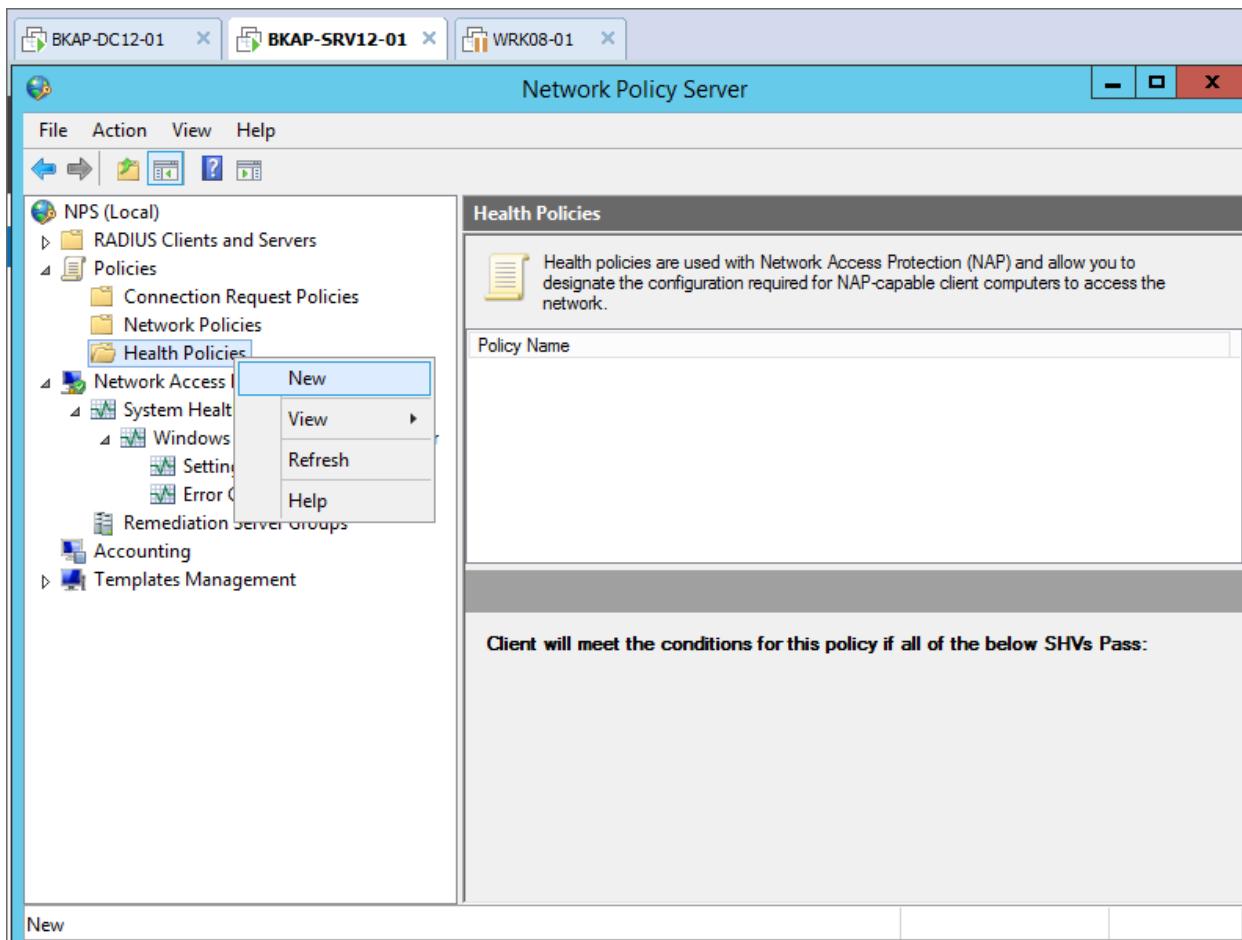
- Trong cửa sổ **Network Policy Server**, chọn vào **Network Access Protection / System Health Validators / Windows Security Health Validator / Settings /Default Configuration** / Click chuột phải tại đây , chọn **Properties**.



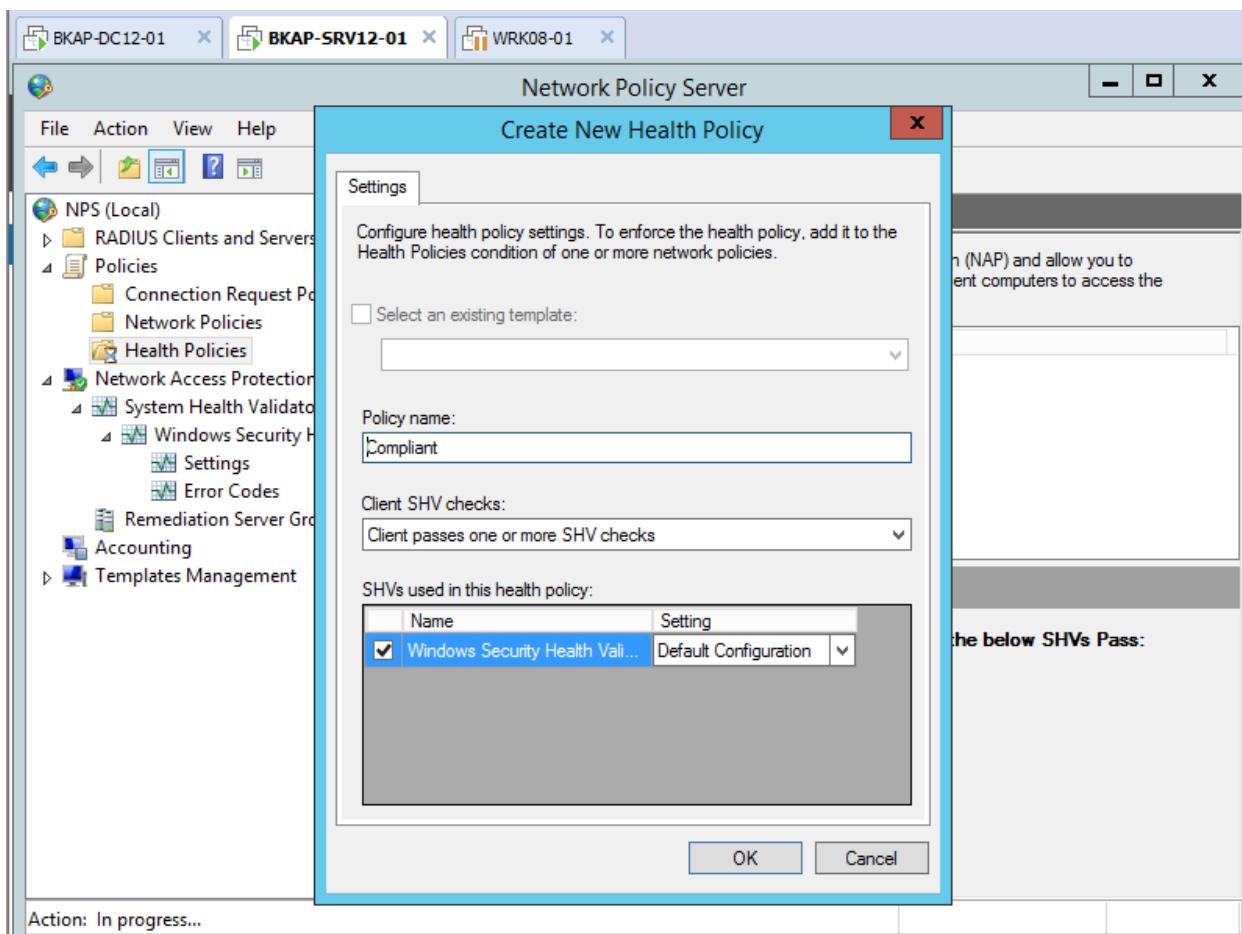
- Trong cửa sổ **Windows Security Health Validator**, bỏ chọn tất cả các tùy chọn trừ tùy chọn **Firewall Settings**.



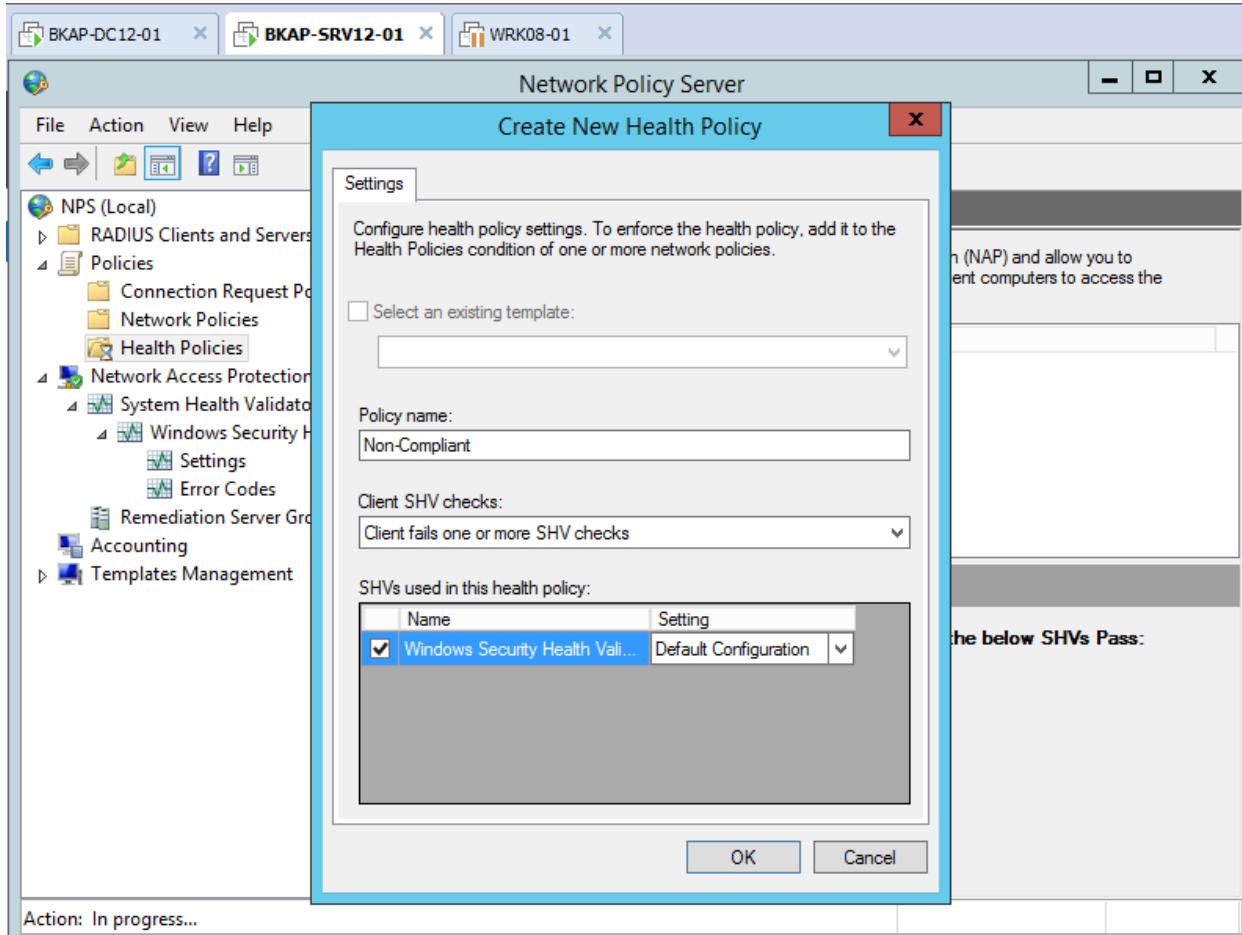
- Tại Policies / chọn vào Health Policies , click chuột phải chọn New.



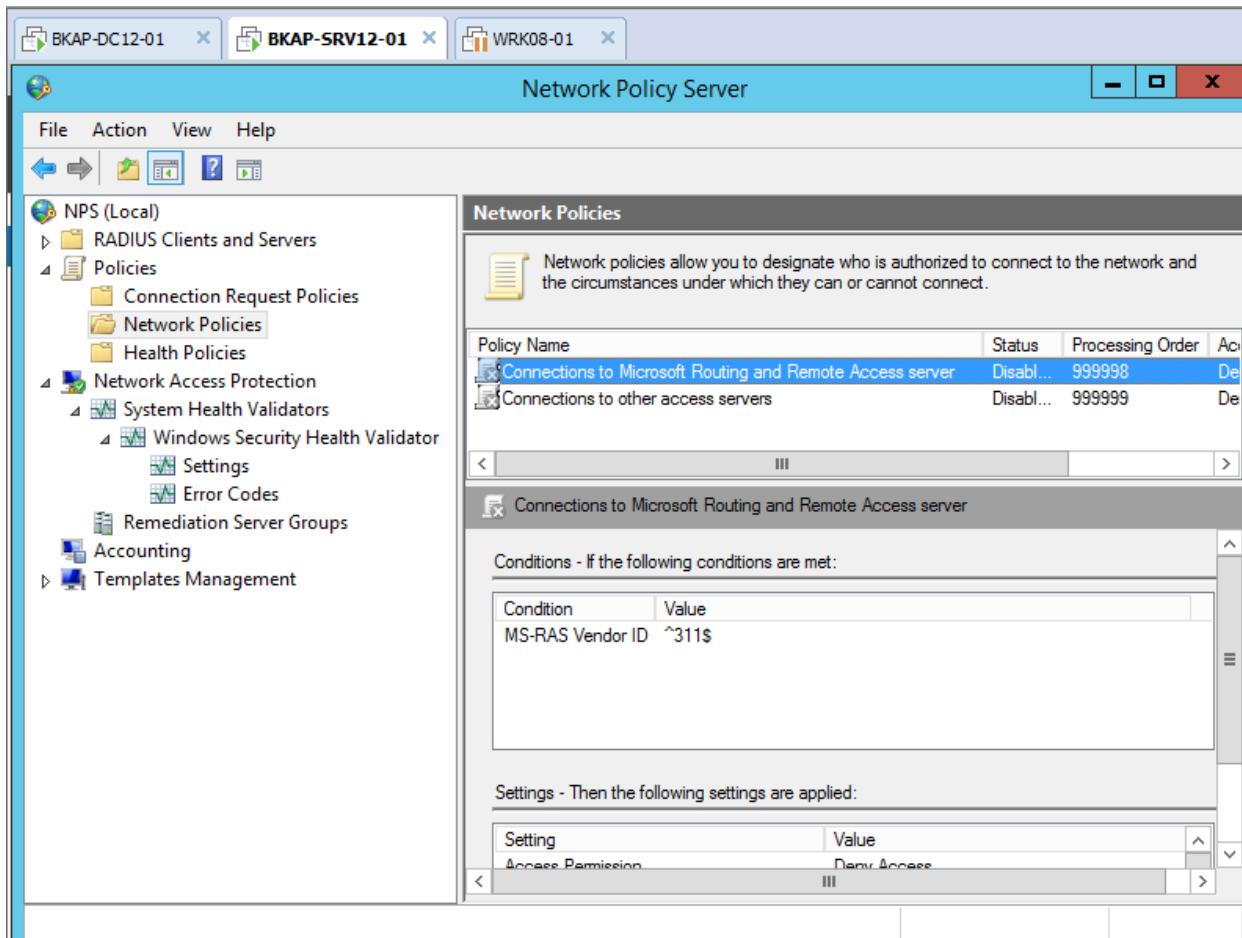
- Tại cửa sổ **Create New Health Policy**, nhập vào thông số :
 - *Policy name* :Compliant.
 - *Client SHV checks* : Client passes one or more SHV checks.
 - Đánh dấu vào mục **Windows Security Health...**



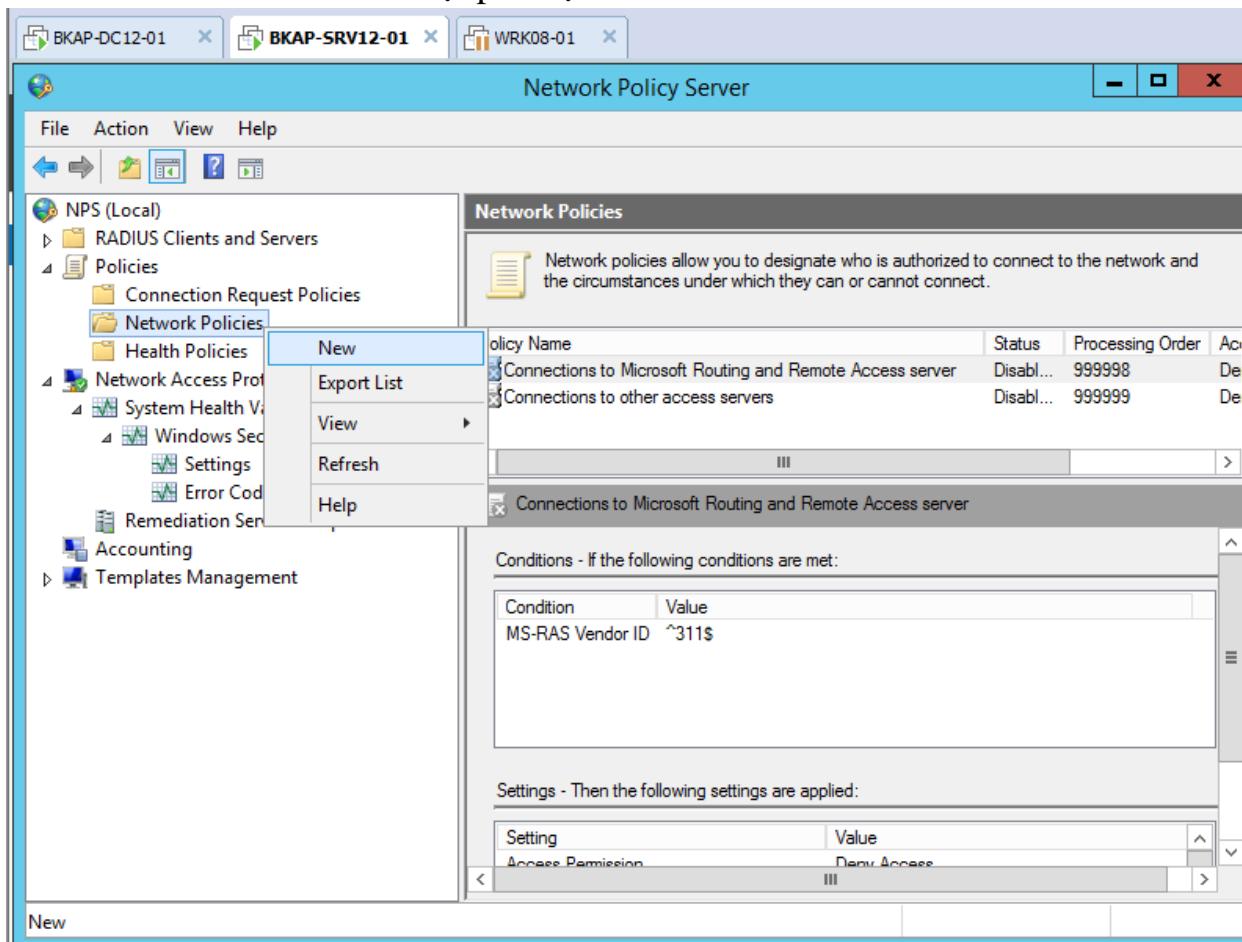
- Tại **Health Policies / New.(tạo mới)** , nhập vào thông số:
 - **Policy name: Non-Compliant**
 - **Client SHV Check: Client fails one or more SHV checks.**
 - Đánh dấu vào mục **Windows Security Health...**



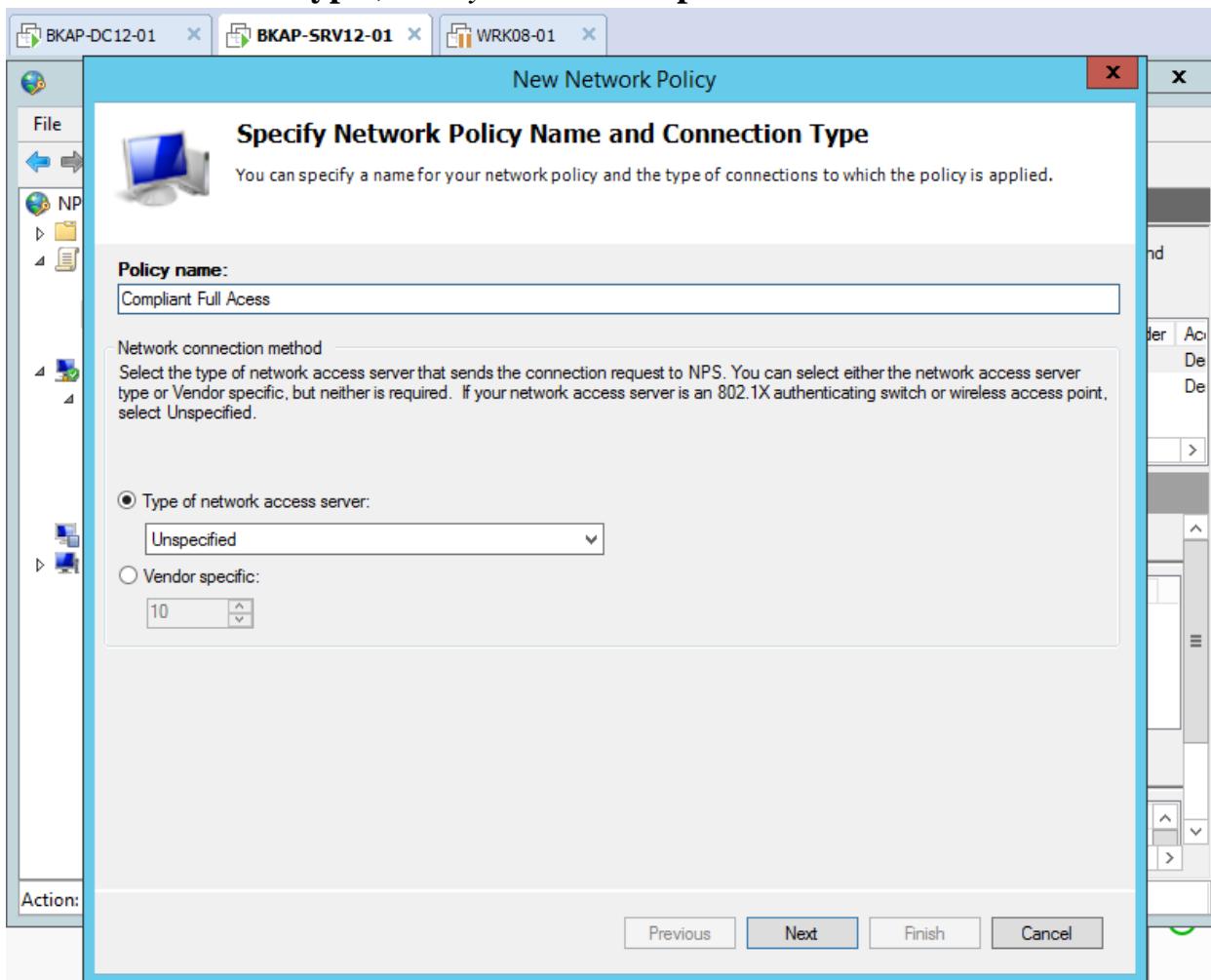
- Tại Network Policies , thực hiện **Disable** 2 chính sách Connections...



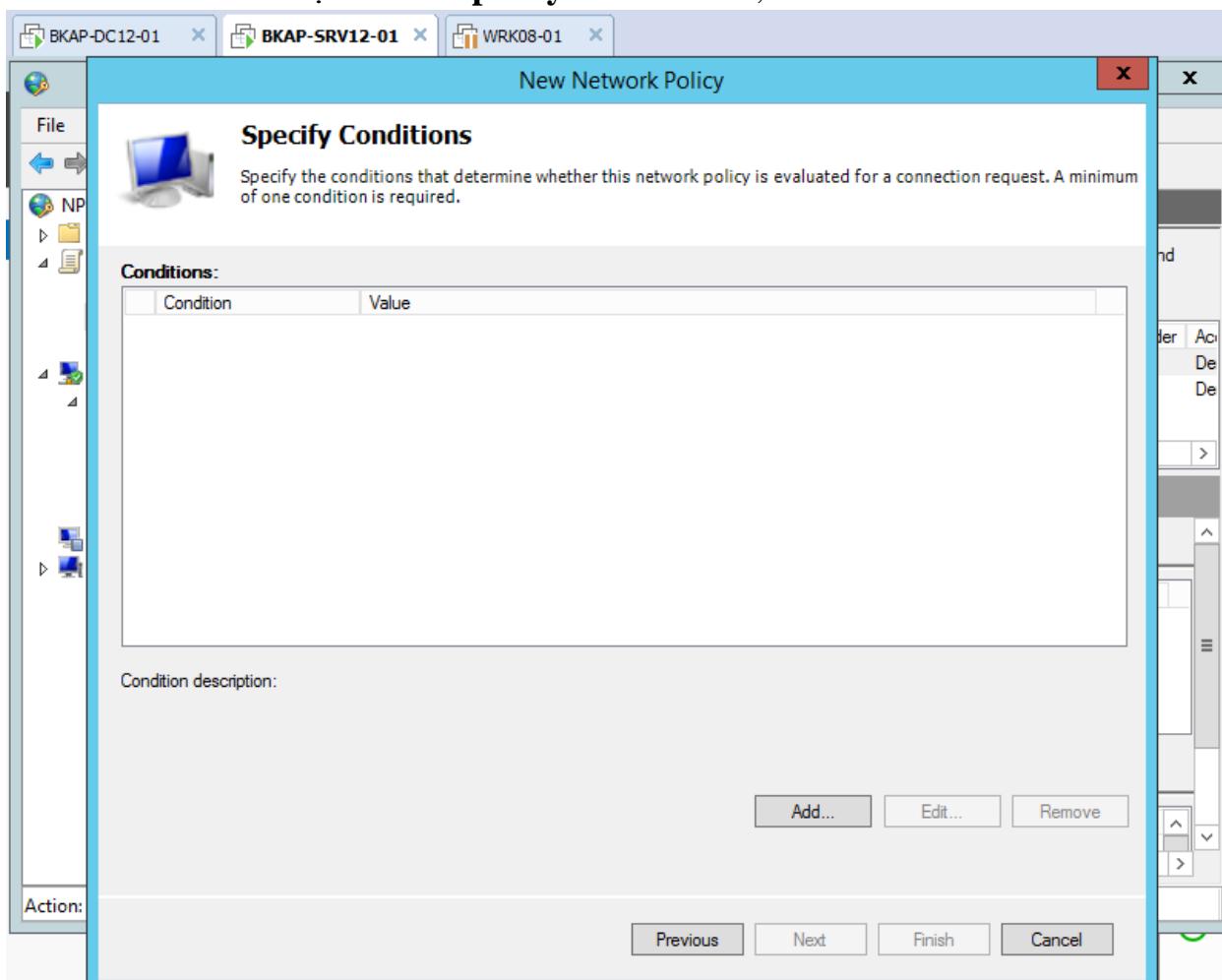
- Click chuột phải tại Network Policies / New.



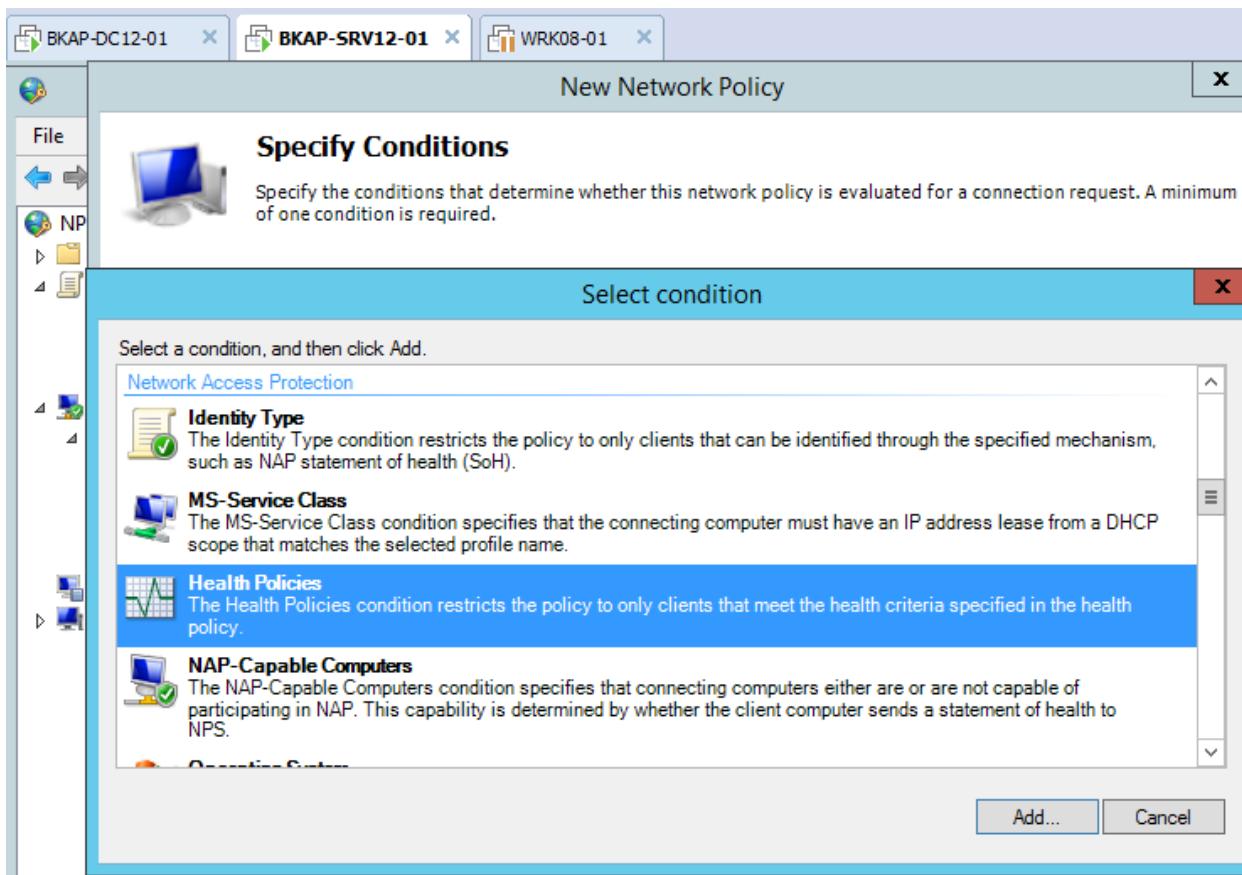
- Tại cửa sổ **Specify Network Policy Name and Connection Type**, *Policy name* : Compliant Full Access.



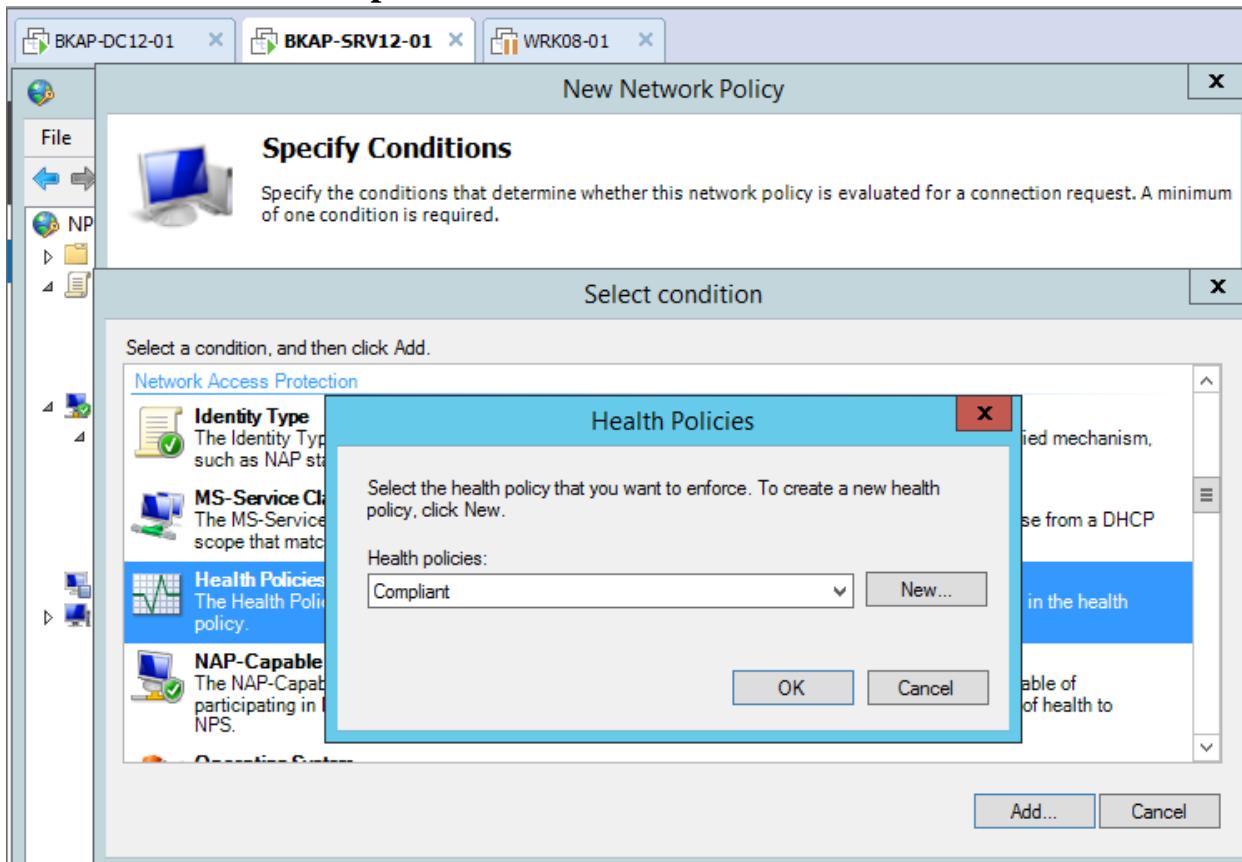
- Tại cửa sổ **Specify Conditions**, click vào **Add**.



- Tại cửa sổ **Select condition** , chọn đến **Health Policies => Add.**

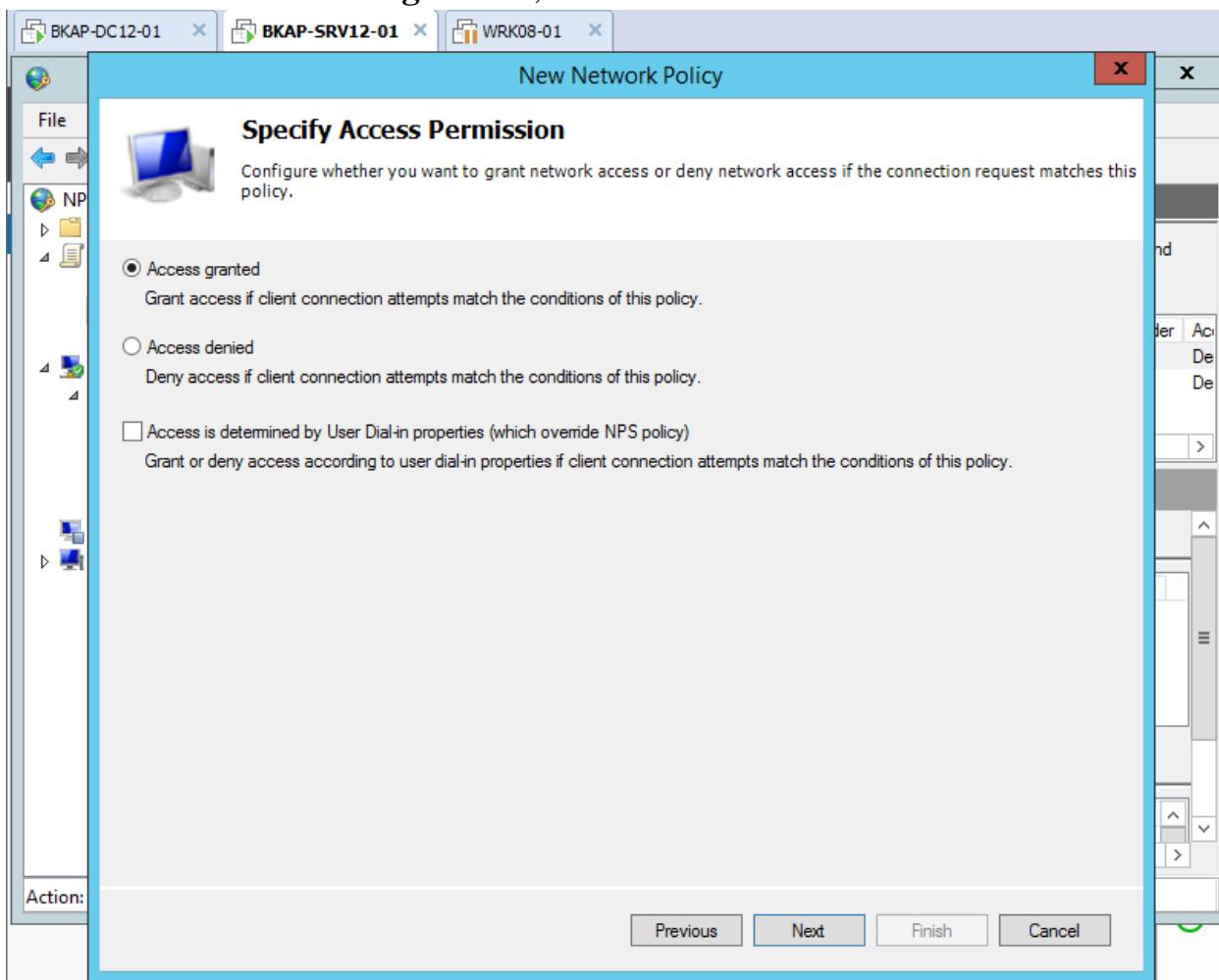


- Hiện ra cửa sổ **Health Policies** , tại **Health policies** , chọn **Compliant.** => **OK.**

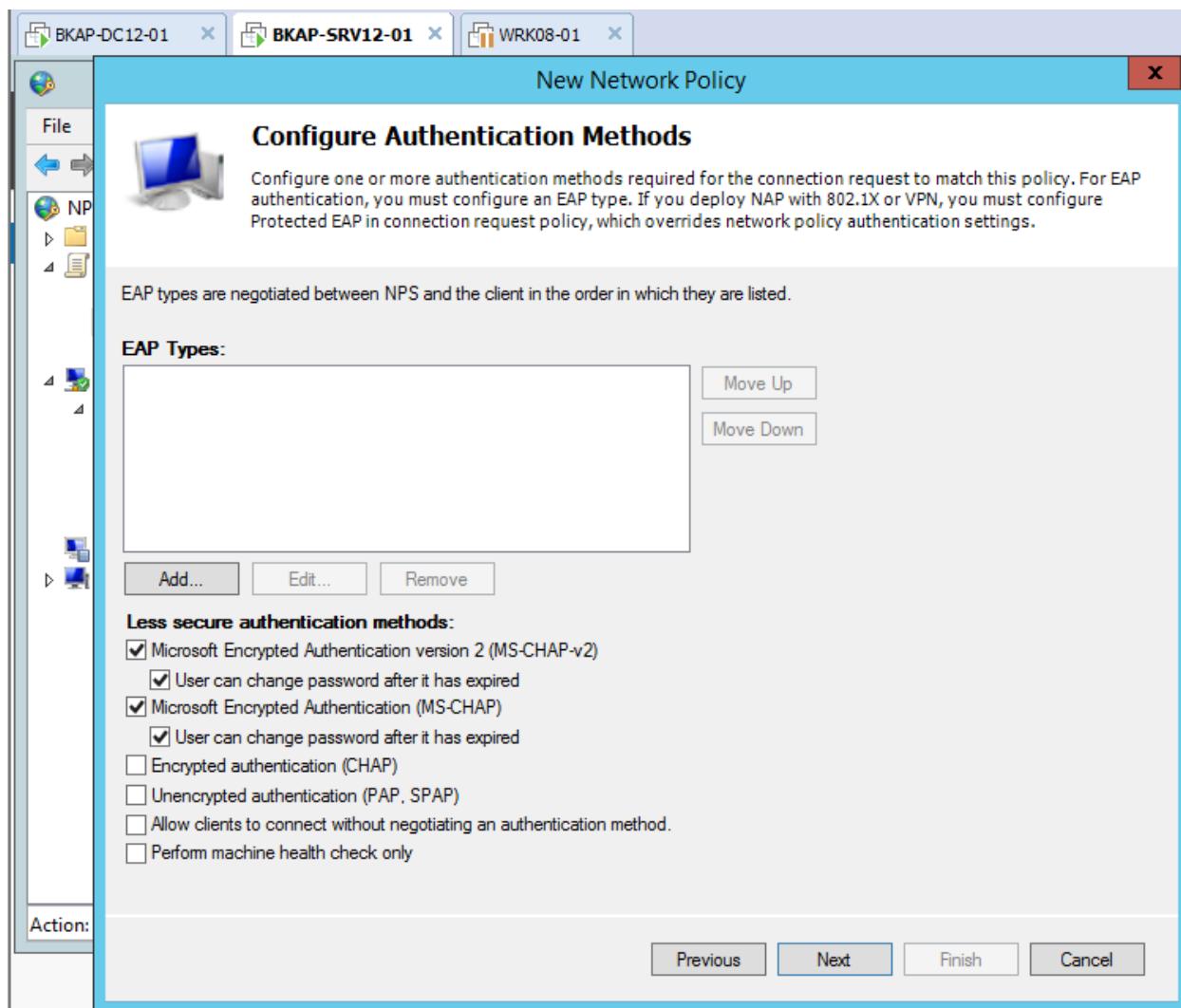


- **Next.**

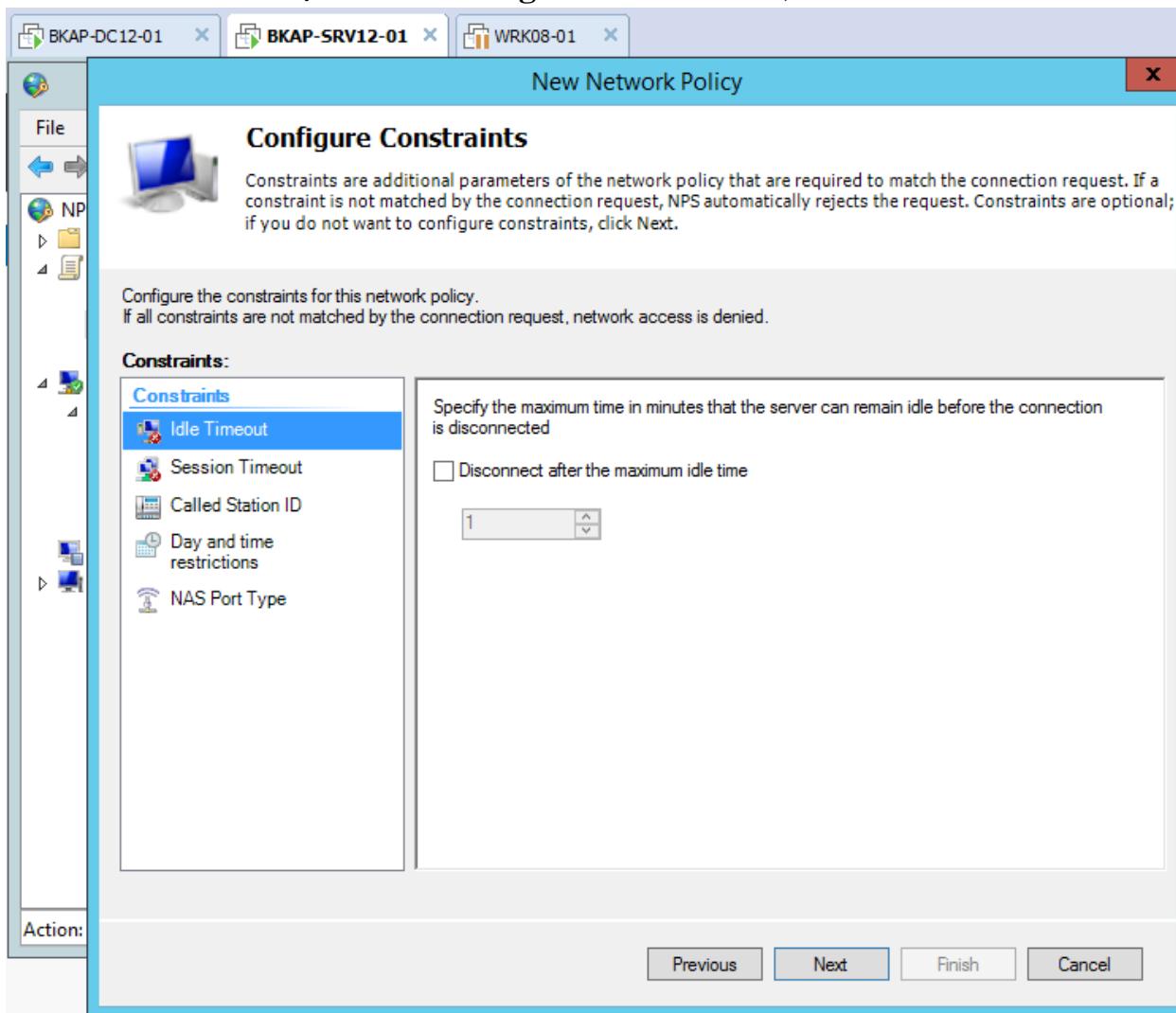
- Click vào **Next** tại cửa sổ **Specify Access Permission** , chọn **Access granted** , => Next.



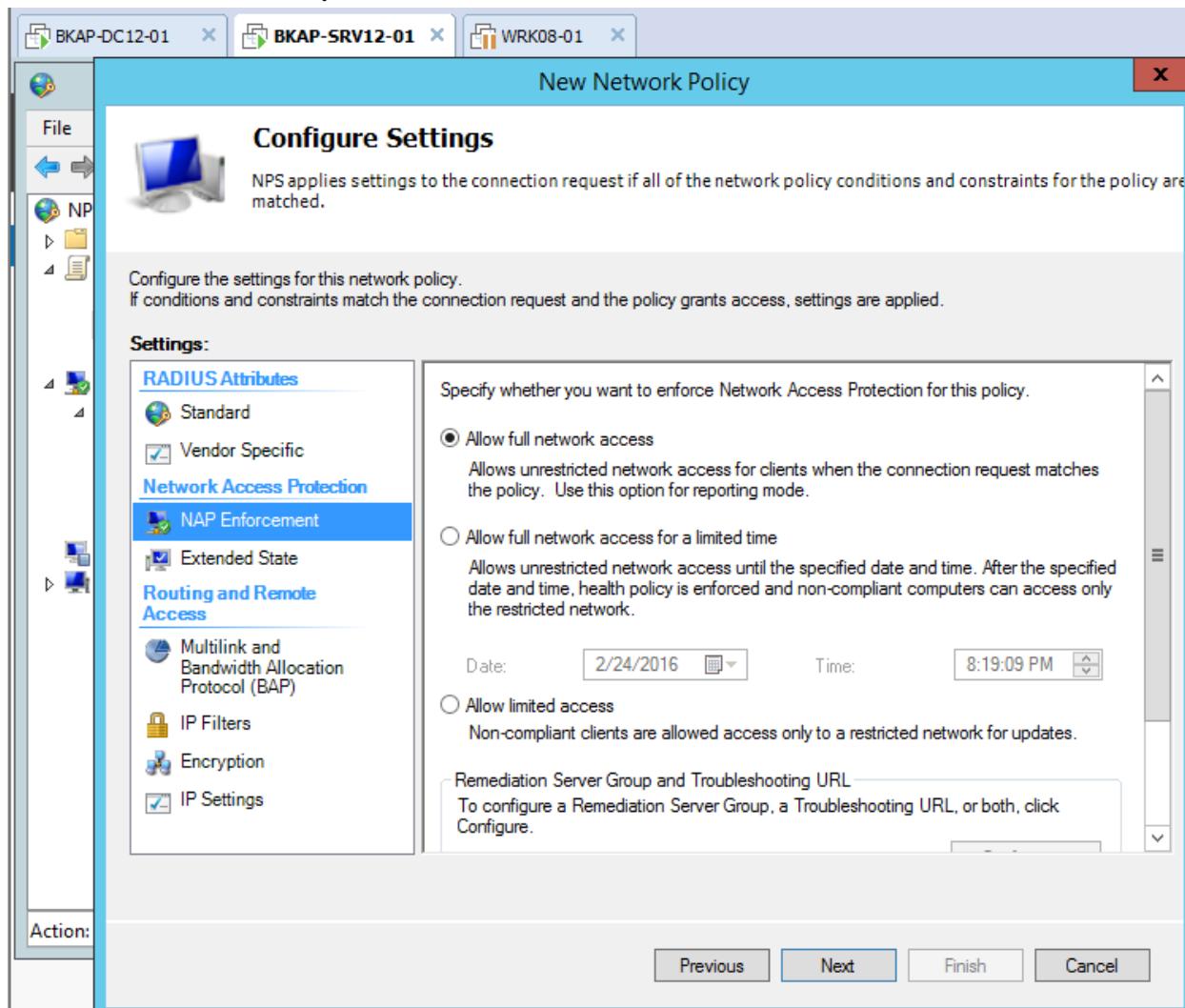
- Tại cửa sổ **Configure Authentication Methods**, click vào **Next**.



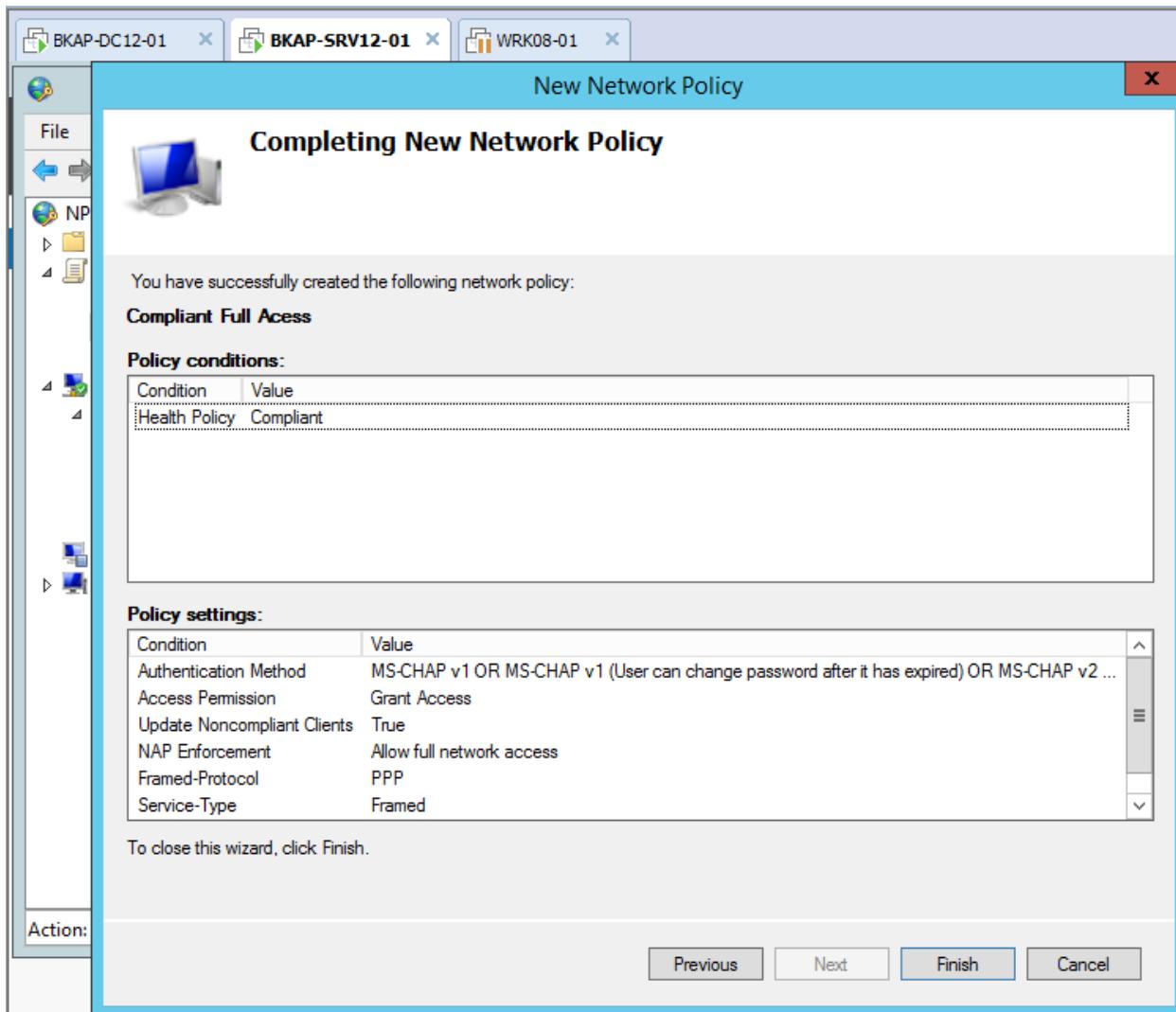
- Tại cửa sổ **Configure Constraints**, click vào **Next**.



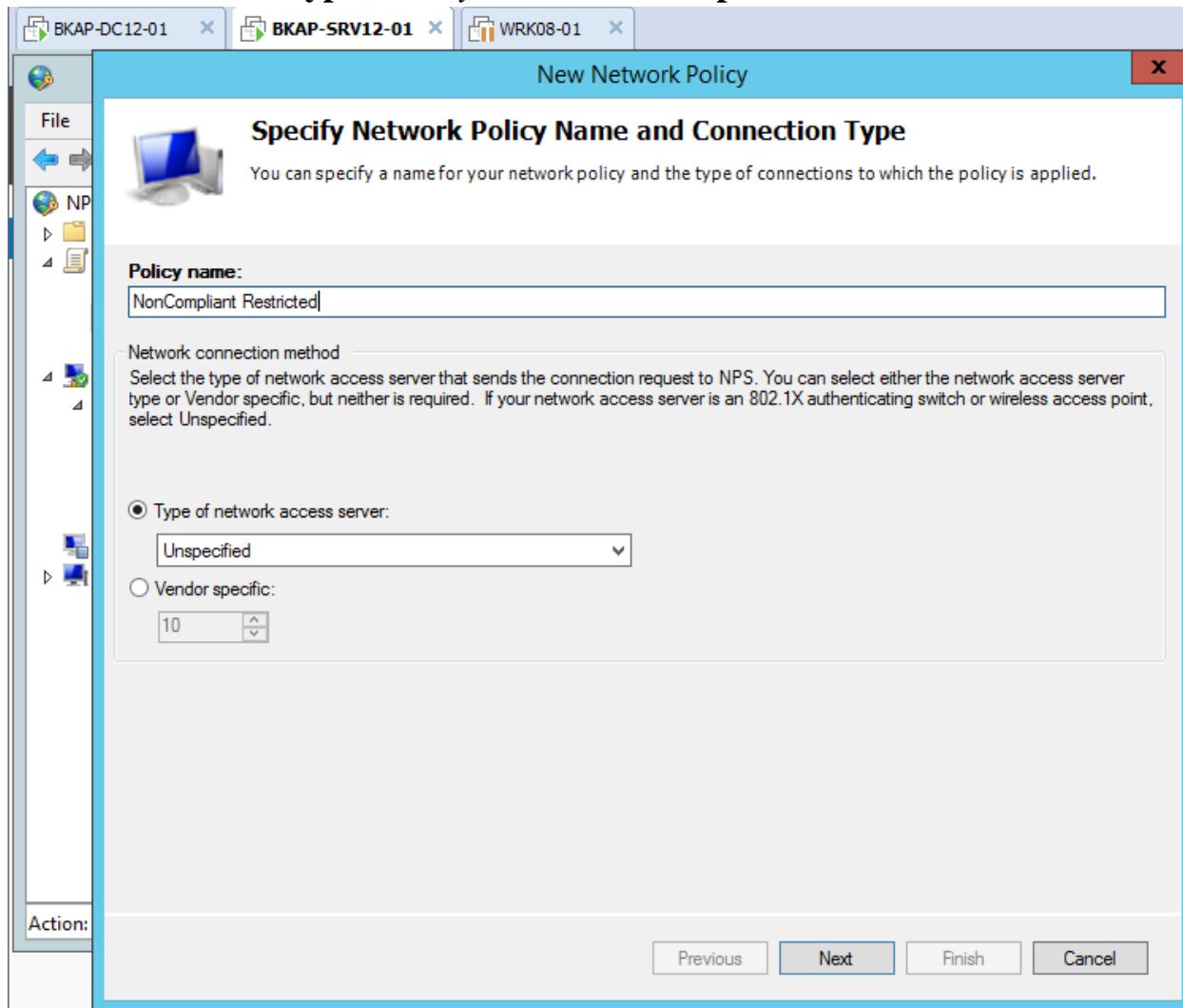
- Tại cửa sổ **Configure Settings**, chọn đến **NAP Enforcement**, chọn **Allow full network access**.



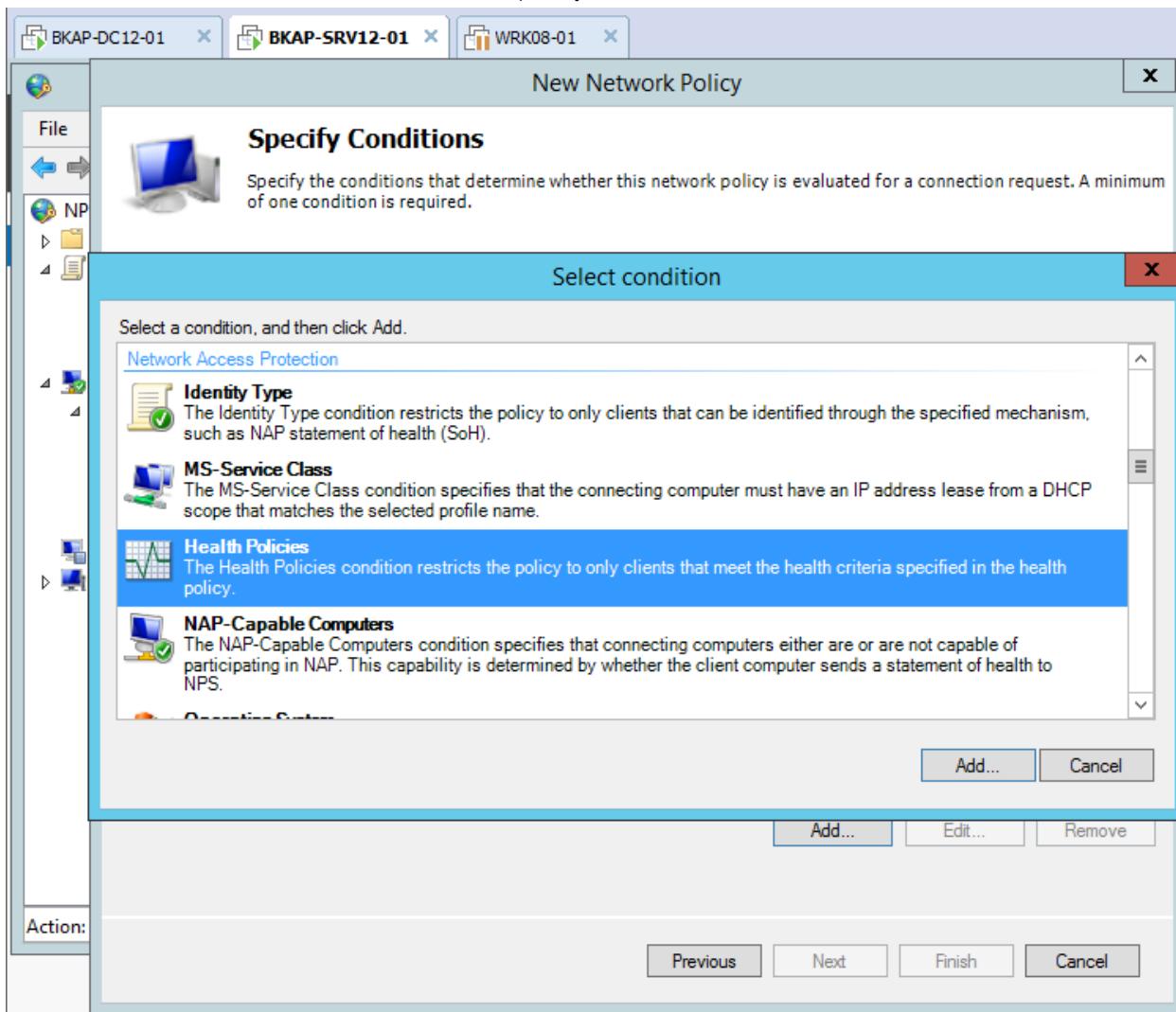
- Tại cửa sổ **Completing New Network Policy**, click vào **Finish**.



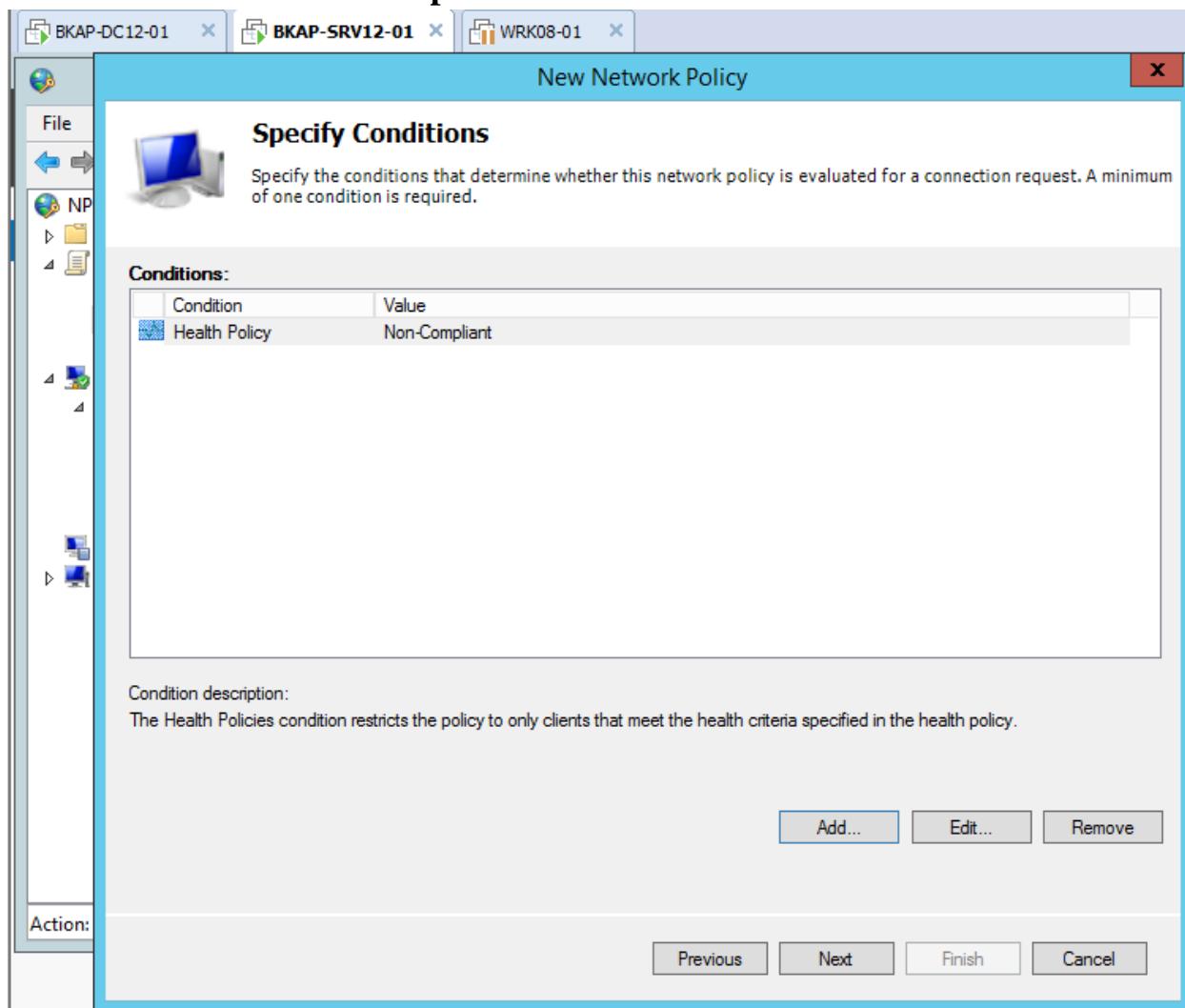
- Click vào Network Policies / New.(tạo mới).
- Tại cửa sổ Specify Network Policy Name and Connection Type , Policy name: NonCompliant Restricted. => Next.



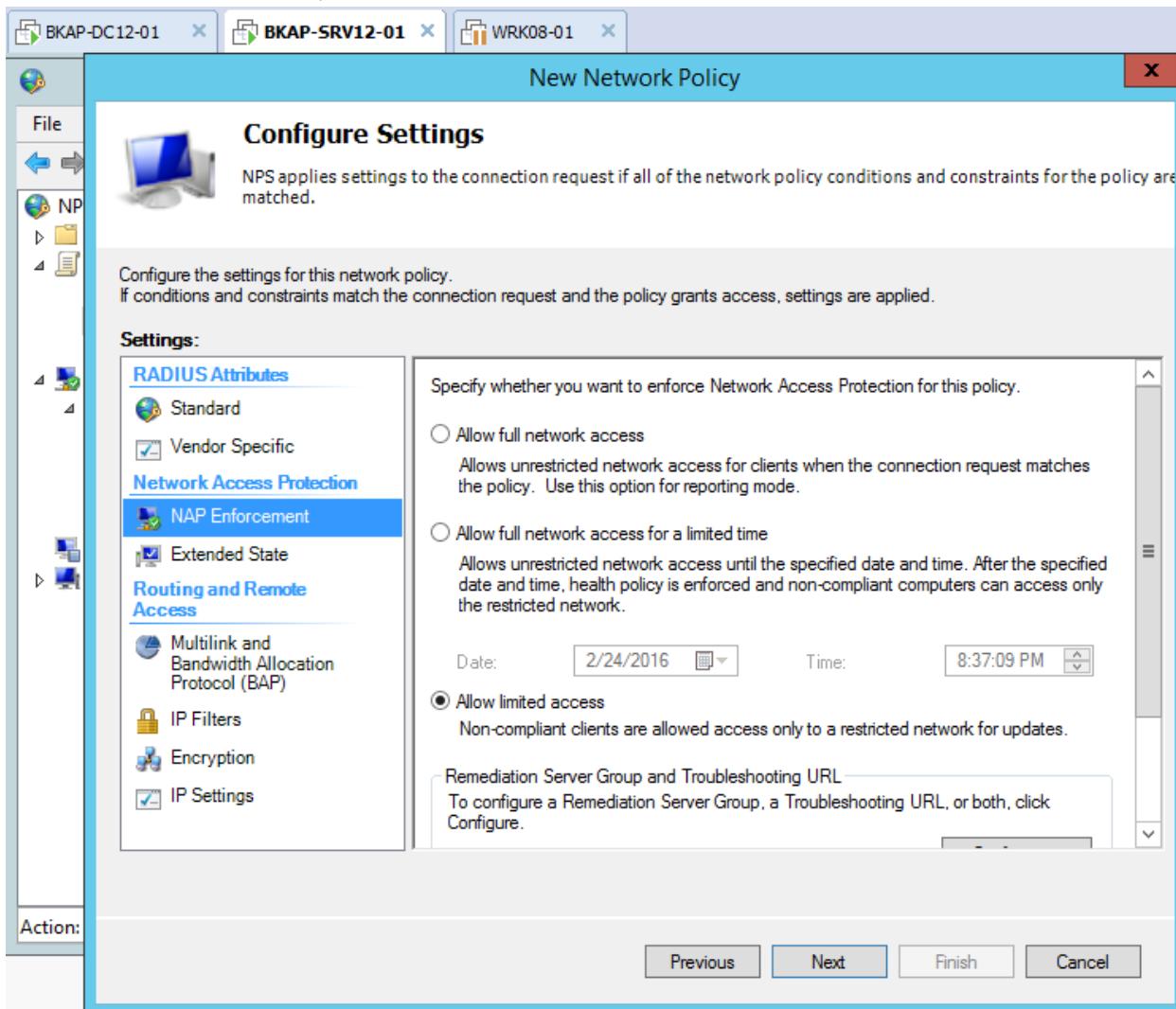
- Tại cửa sổ **Specify Conditions**, click vào **Add..**, tại cửa sổ **Select condition**, chọn đến **Health Policies**. => **Add...**



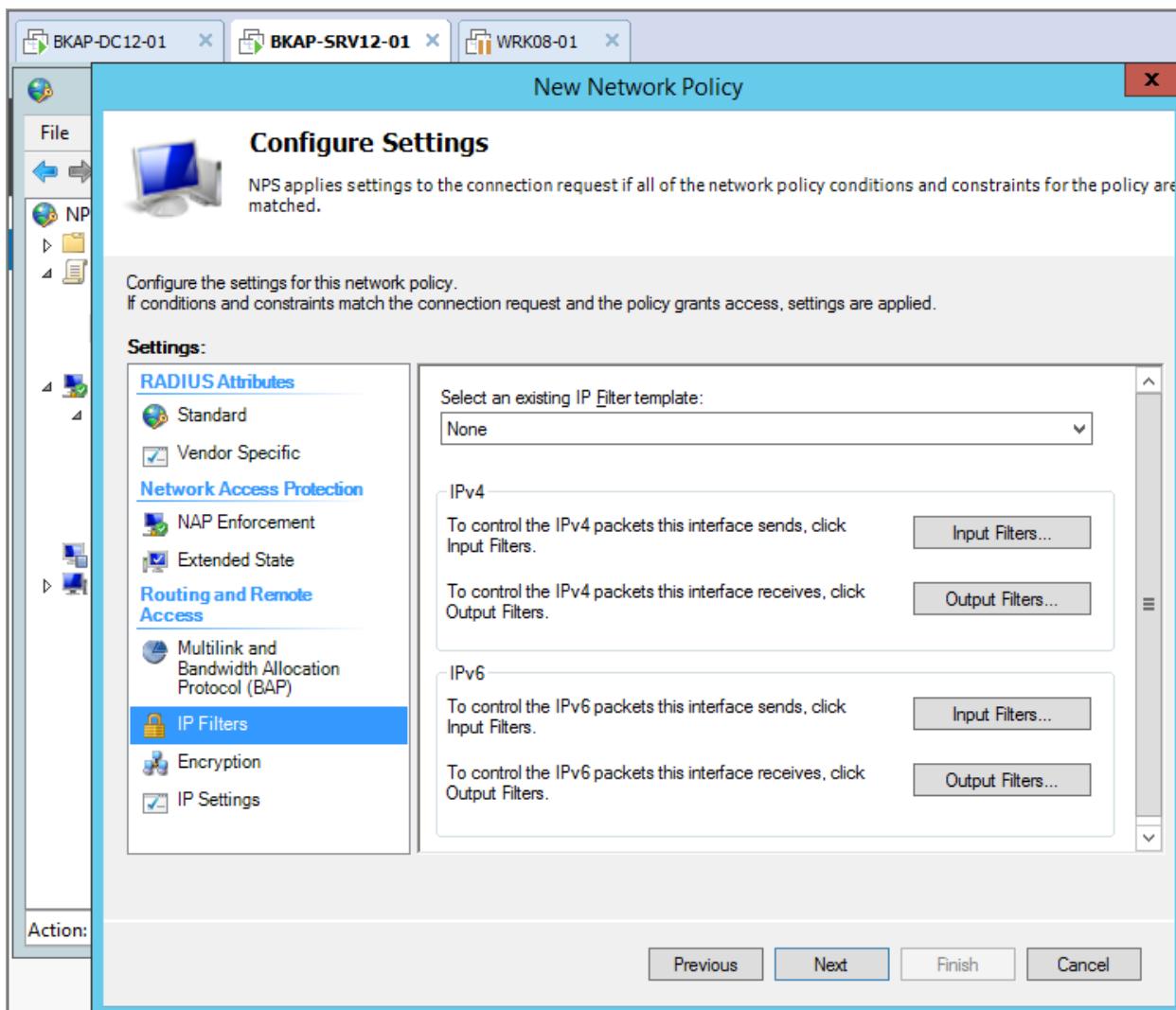
- Tại cửa sổ **Health Policies**, tại **Non-Compliant** , chọn vào **Non-Compliant**. => **OK**. => **Next**.



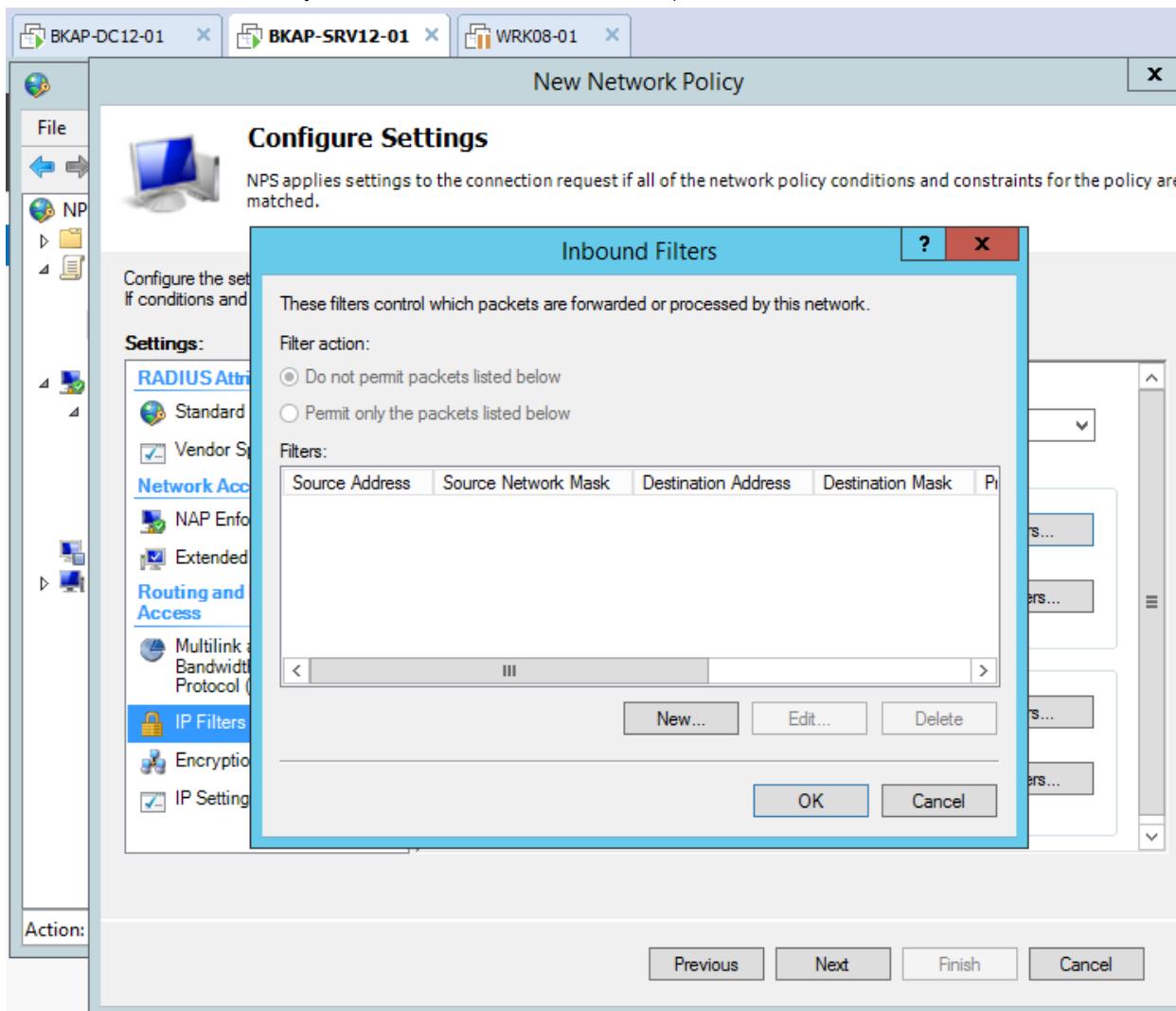
- Click vào **Next** tại các cửa sổ **Specify Access Permisson** , cửa sổ **Configure Authentication Methods** , cửa sổ **Configure Constraints** .
- Tại cửa sổ **Configure Settings** , chọn đến **NAP Enforcement** , chọn **Allow limited access**.



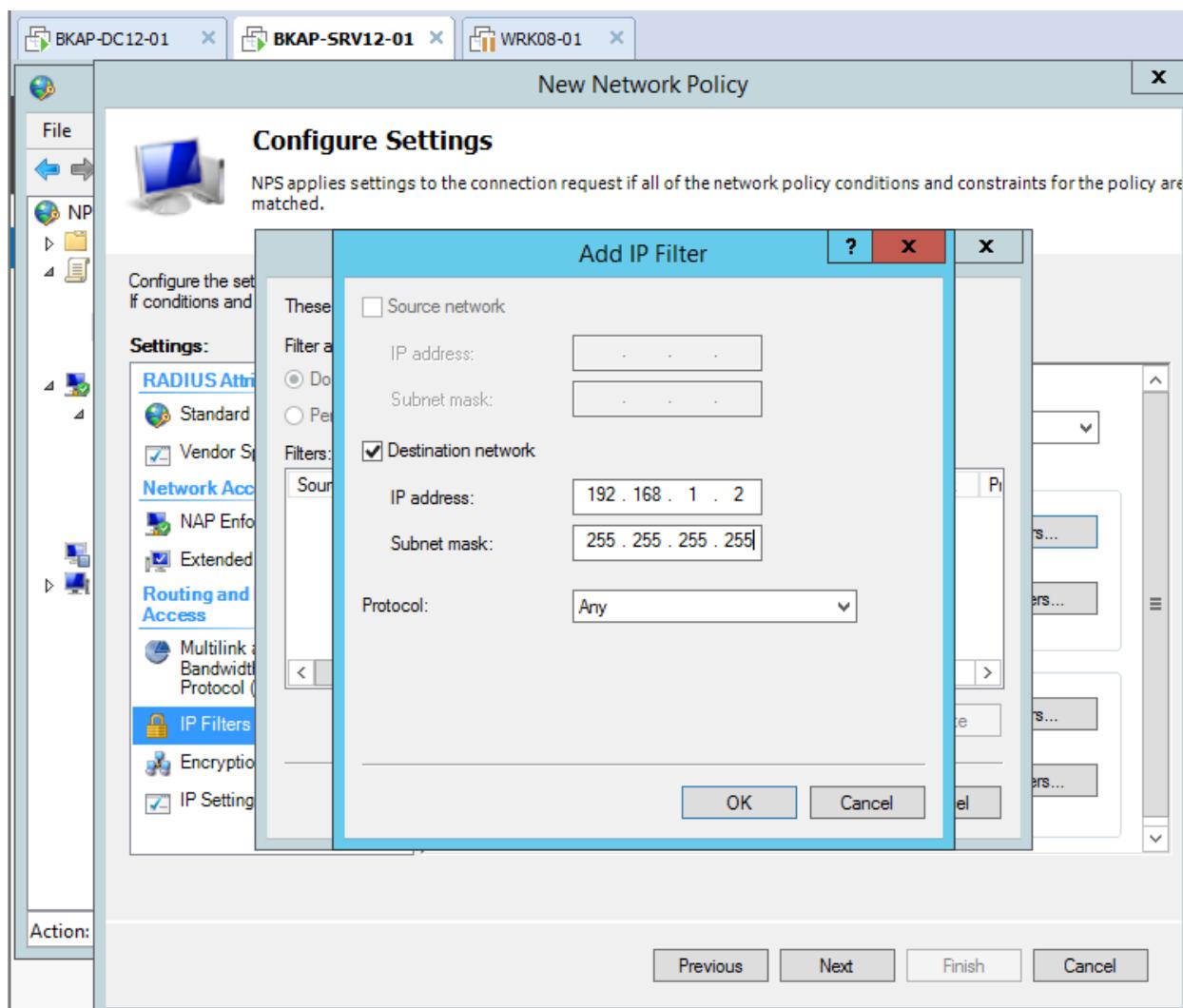
- Chọn tiếp xuống **IP Filters** , tại **IPv4** , click vào **Input Filters...**



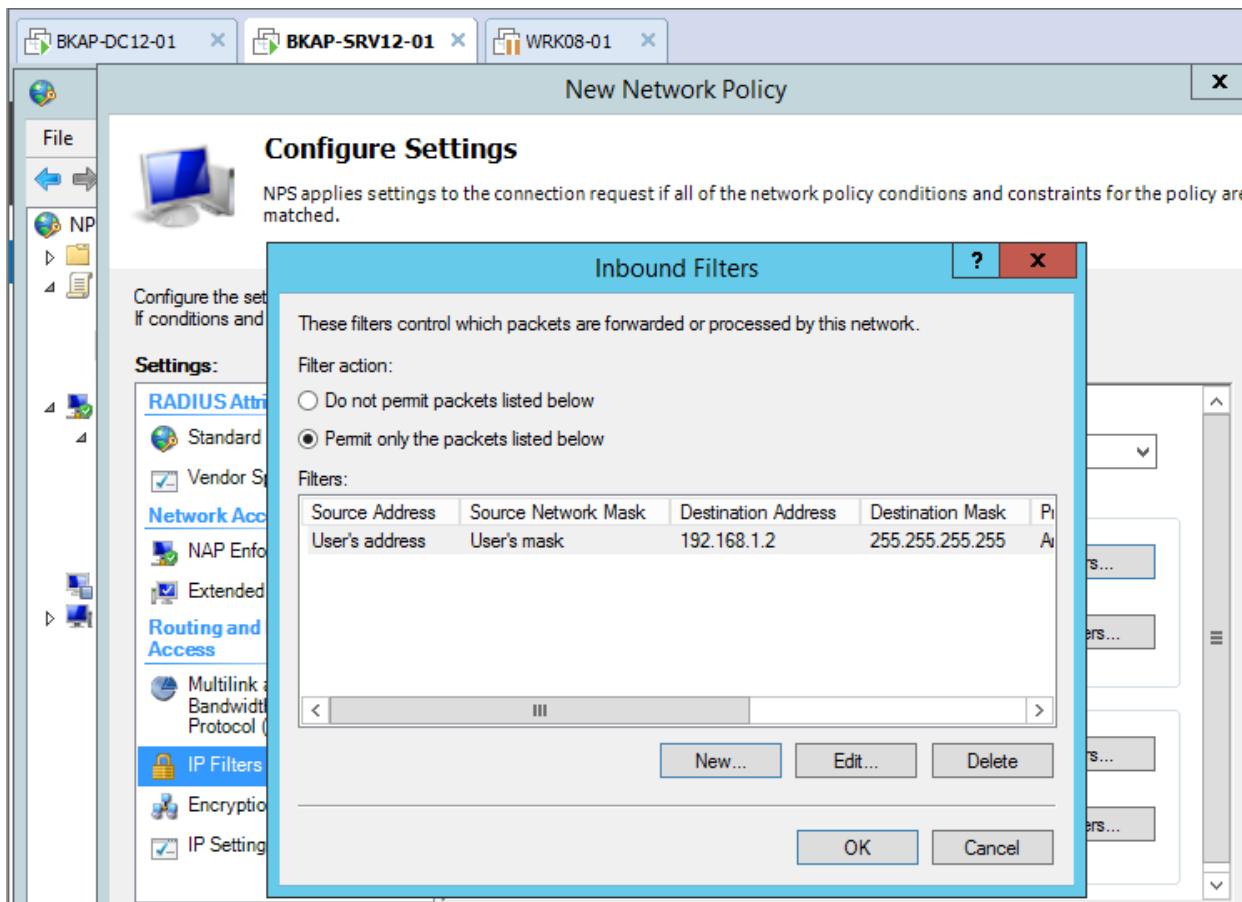
- Tại cửa sổ **Inbound Filters**, click vào New...



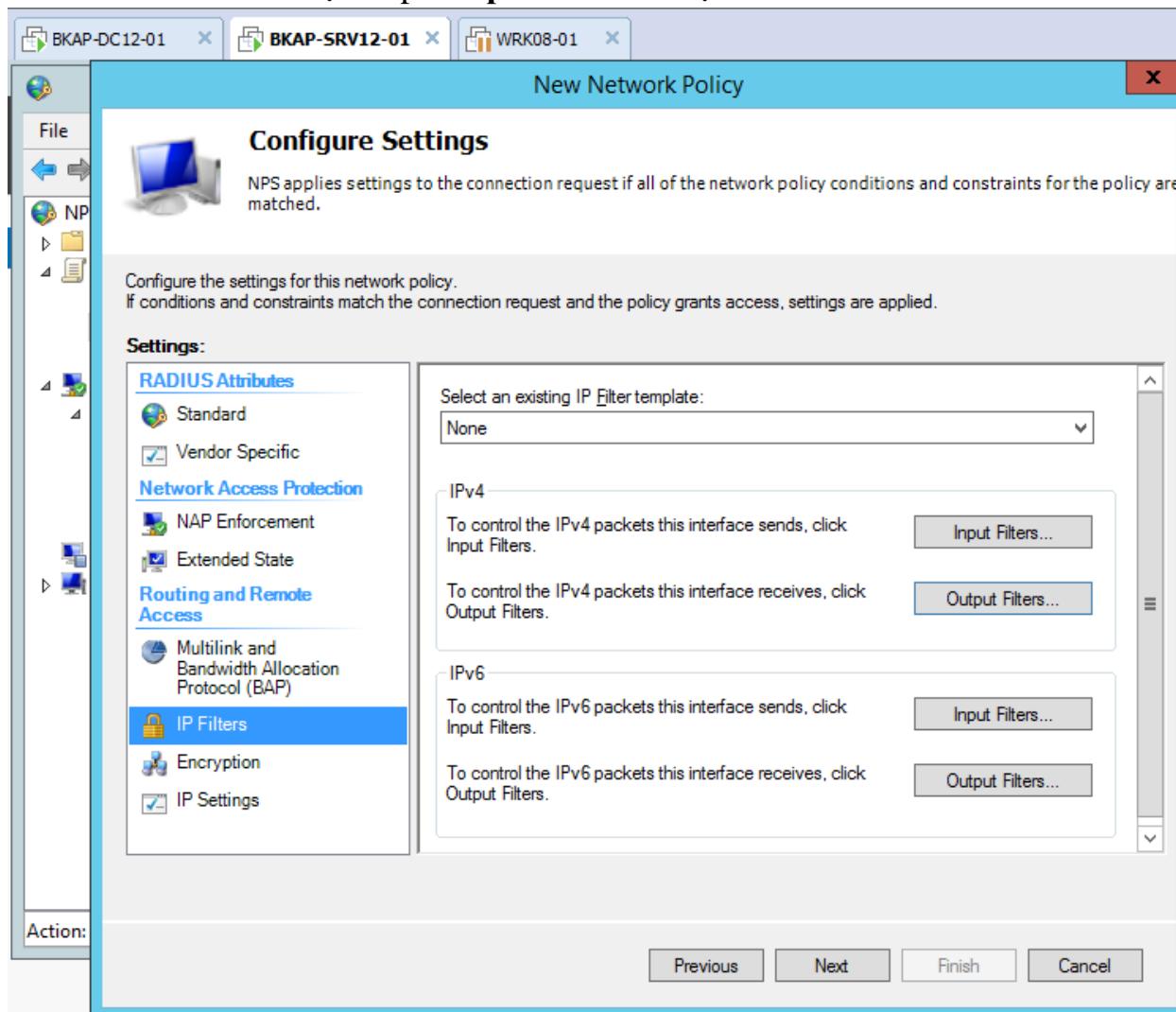
- Tại cửa sổ **Add IP Filter**, nhập vào thông số:
 - *Destination network:*
 - ⇒ *IP address:* **192.168.1.2**
 - ⇒ *Subnet mask:* **255.255.255.255**
 - **OK.**



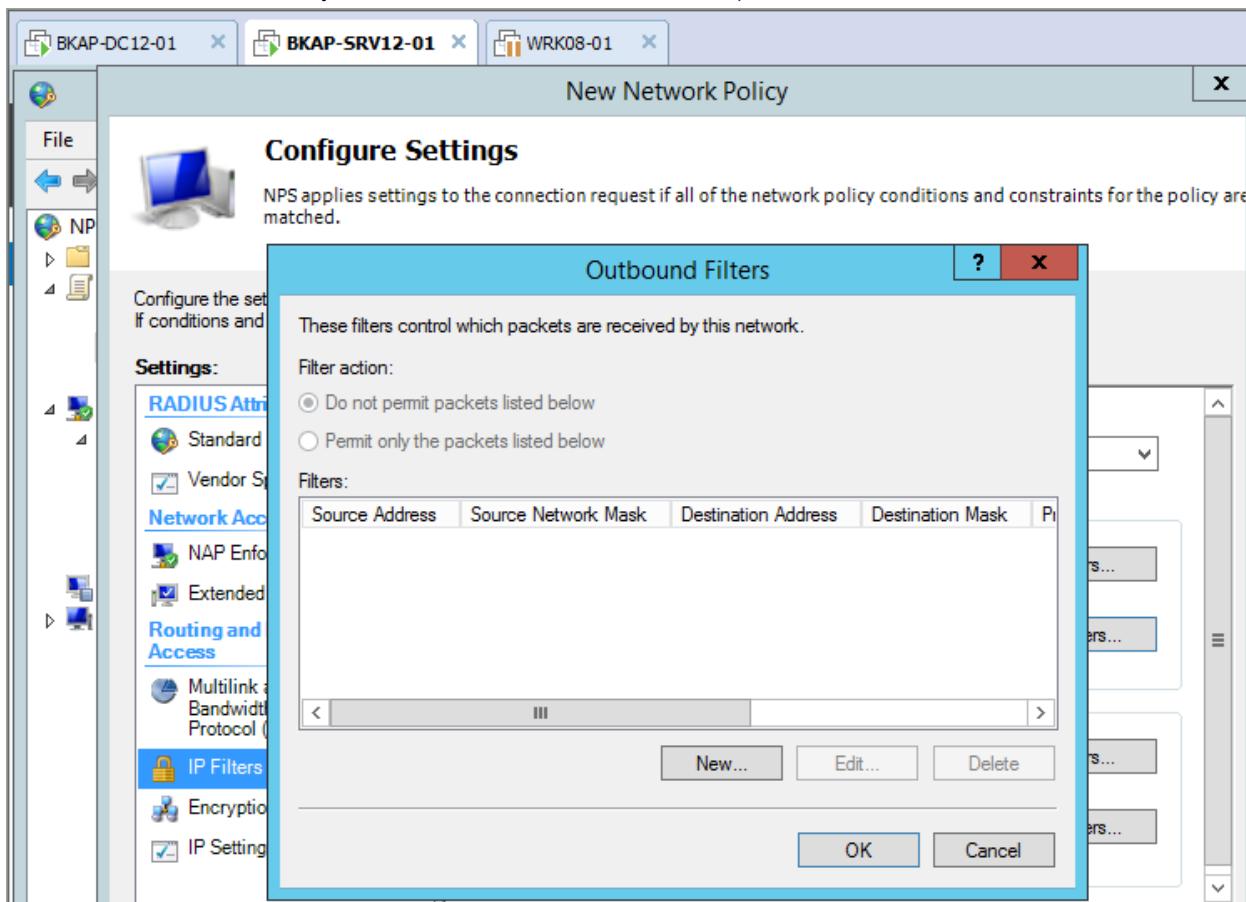
- Tại cửa sổ **Inbound Filters**, chọn **Pemit only the packets listed below => OK.**



▪ Chọn tiếp Output Filters... tại IPv4.

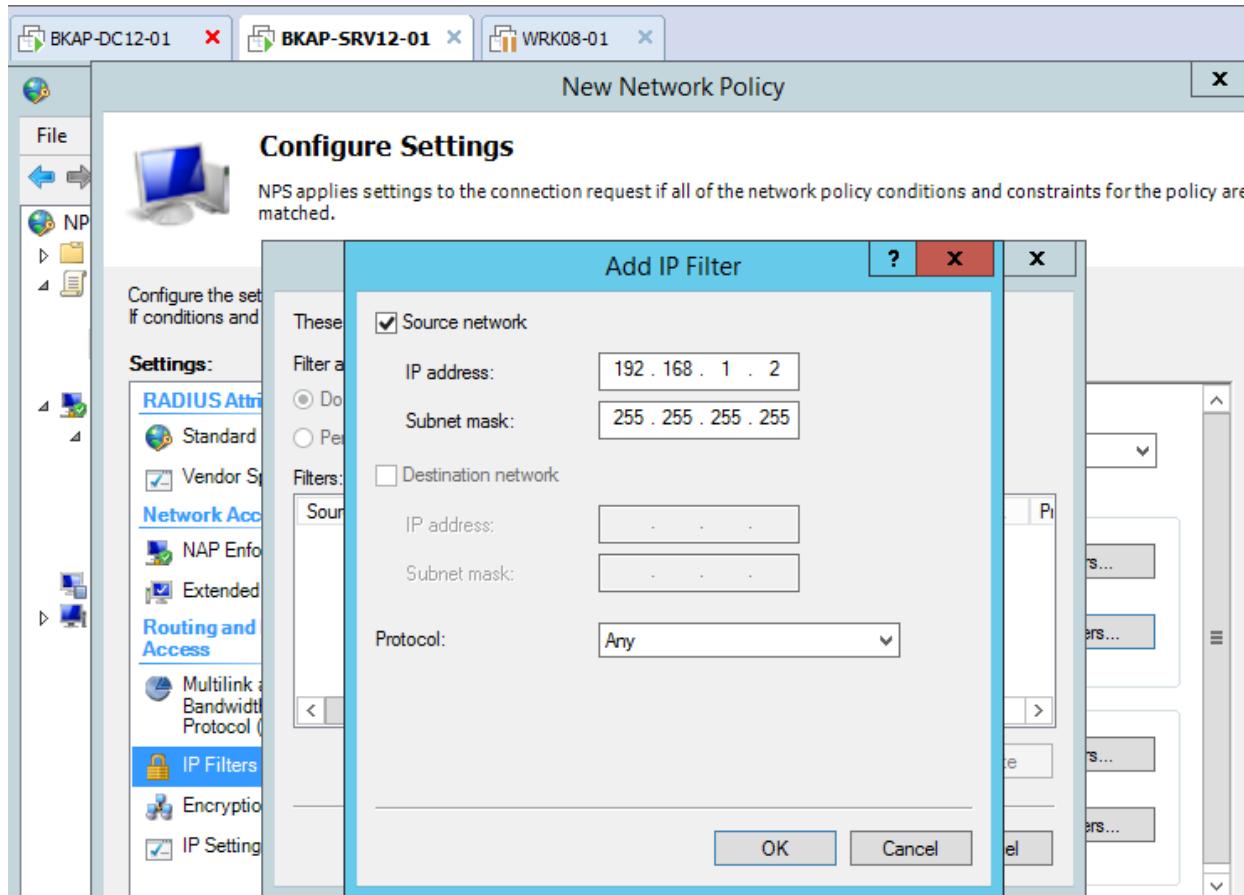


- Tại cửa sổ **Outbound Filters**, click vào **New...**

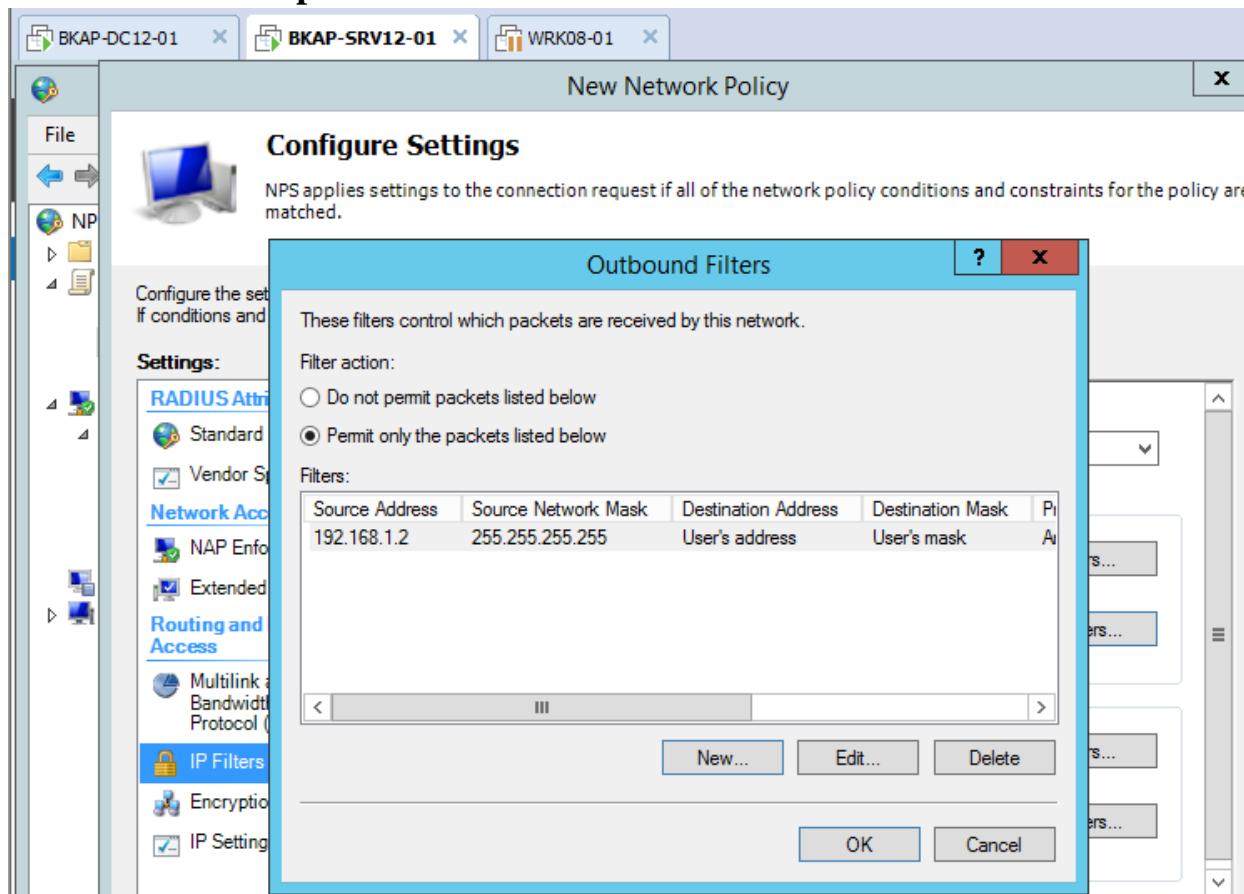


- Tại cửa sổ **Add IP Filter**, click vào **Source network**.

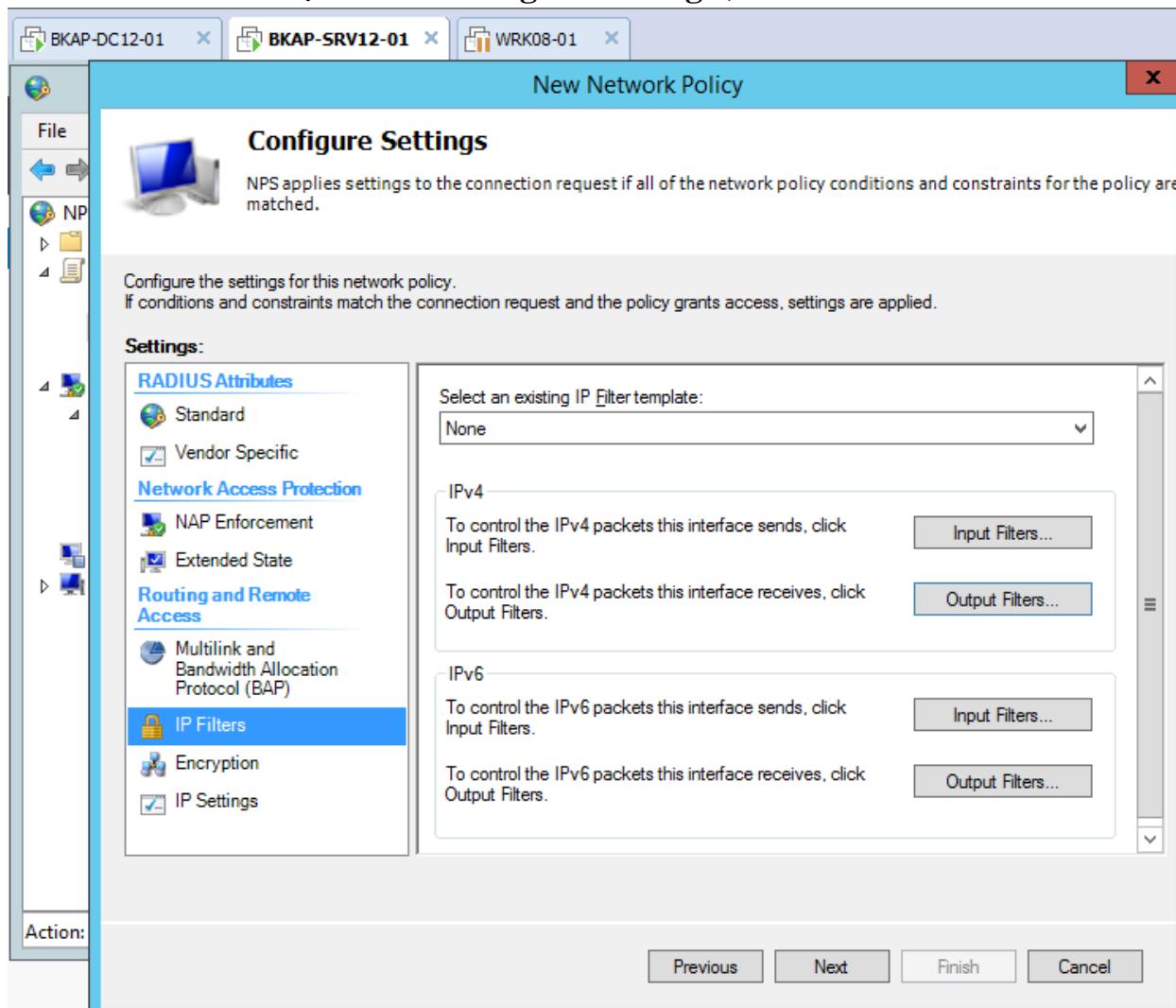
- *IP address: 192.168.1.2*
- *Subnet mask: 255.255.255.255*
- *OK*

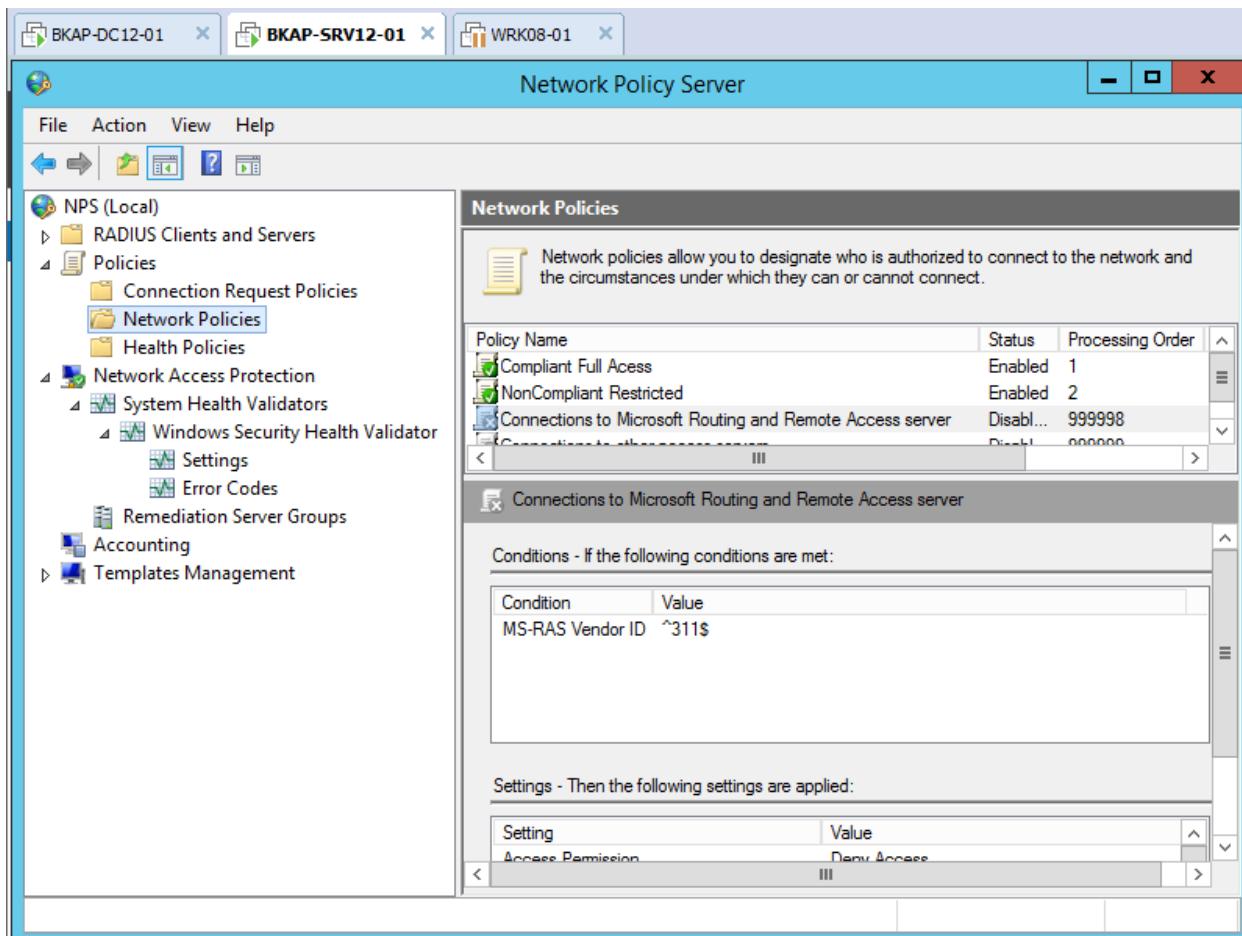


- Tại cửa sổ **Outbound Filters**, click chọn vào **Permit only the packets listed below.** => **OK**.

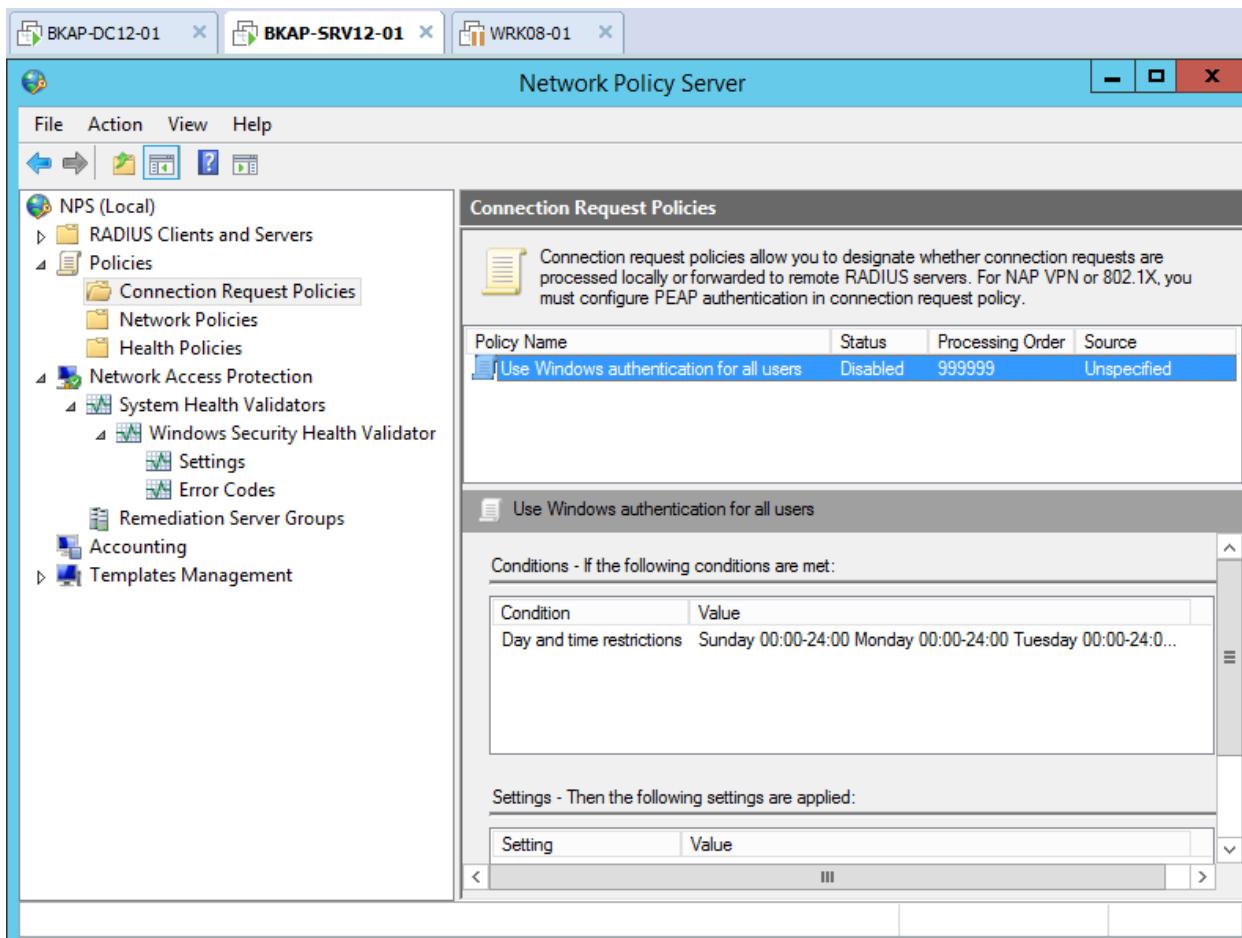


- Tại cửa sổ **Configure Settings**, click vào **Next => Finish**.

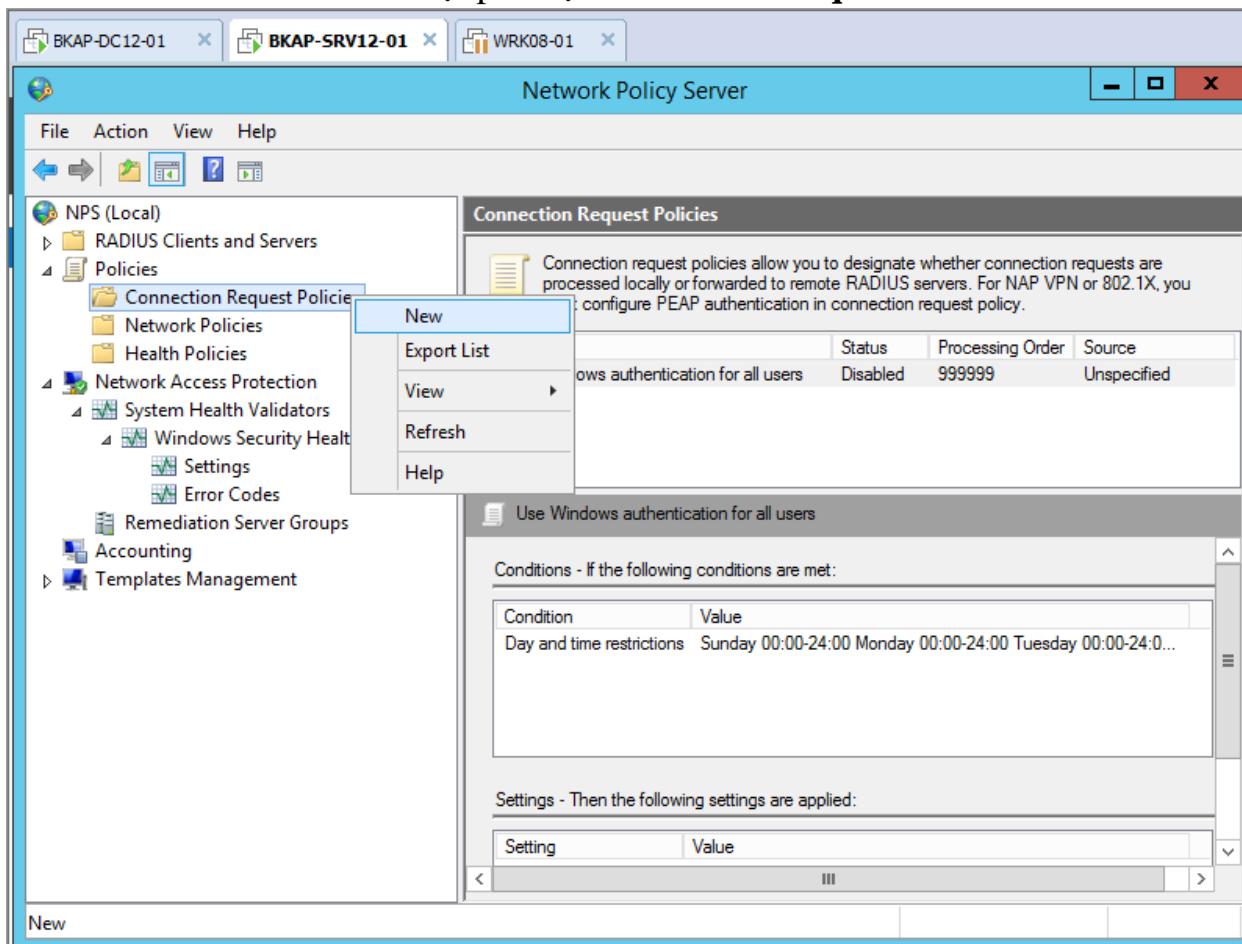




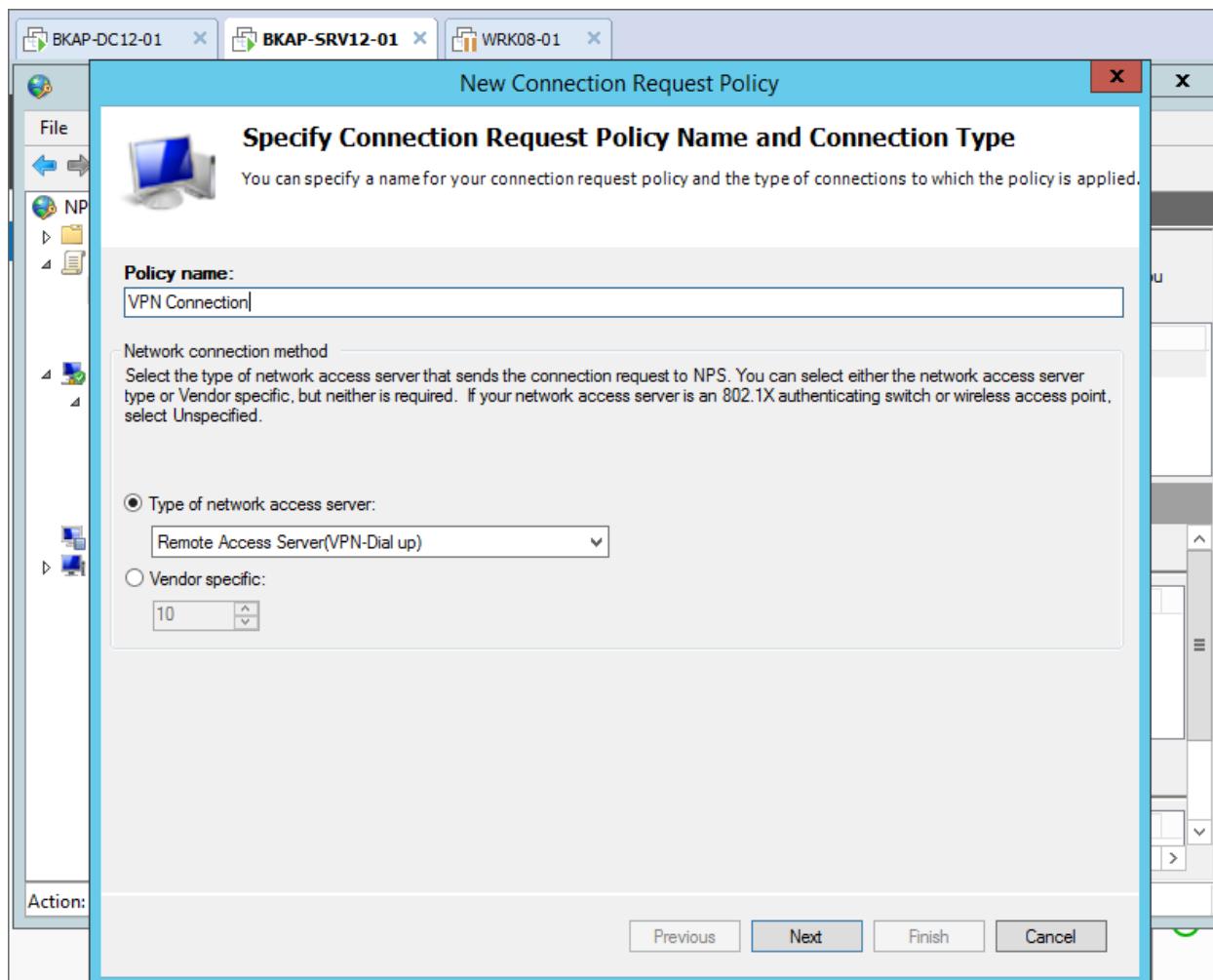
- Tại **Connection Request Policies**, tiến hành **Disable** chính sách **Use Windows authentication for all users**.



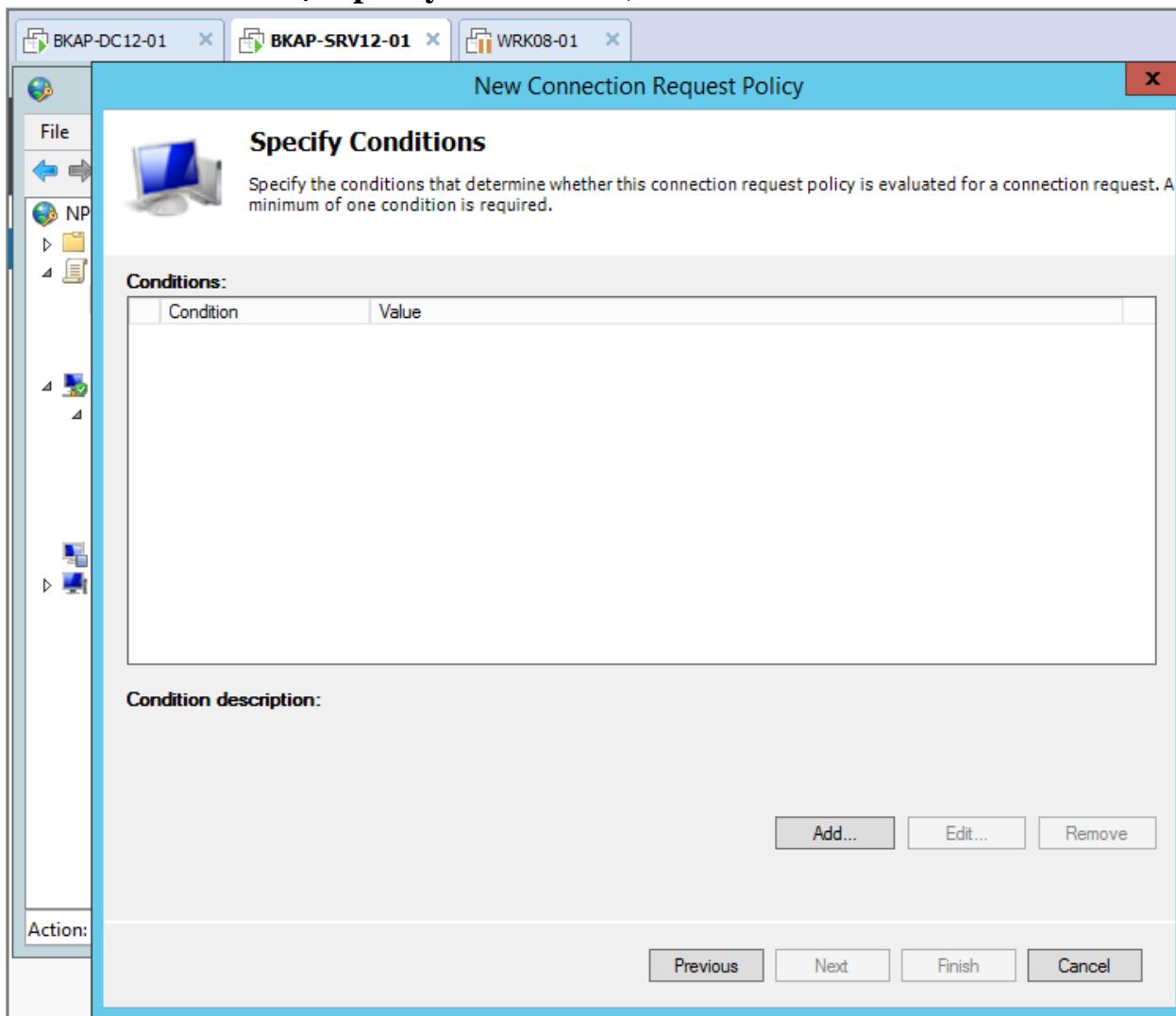
- Click chuột phải tại **Connection Request Policies / New**.



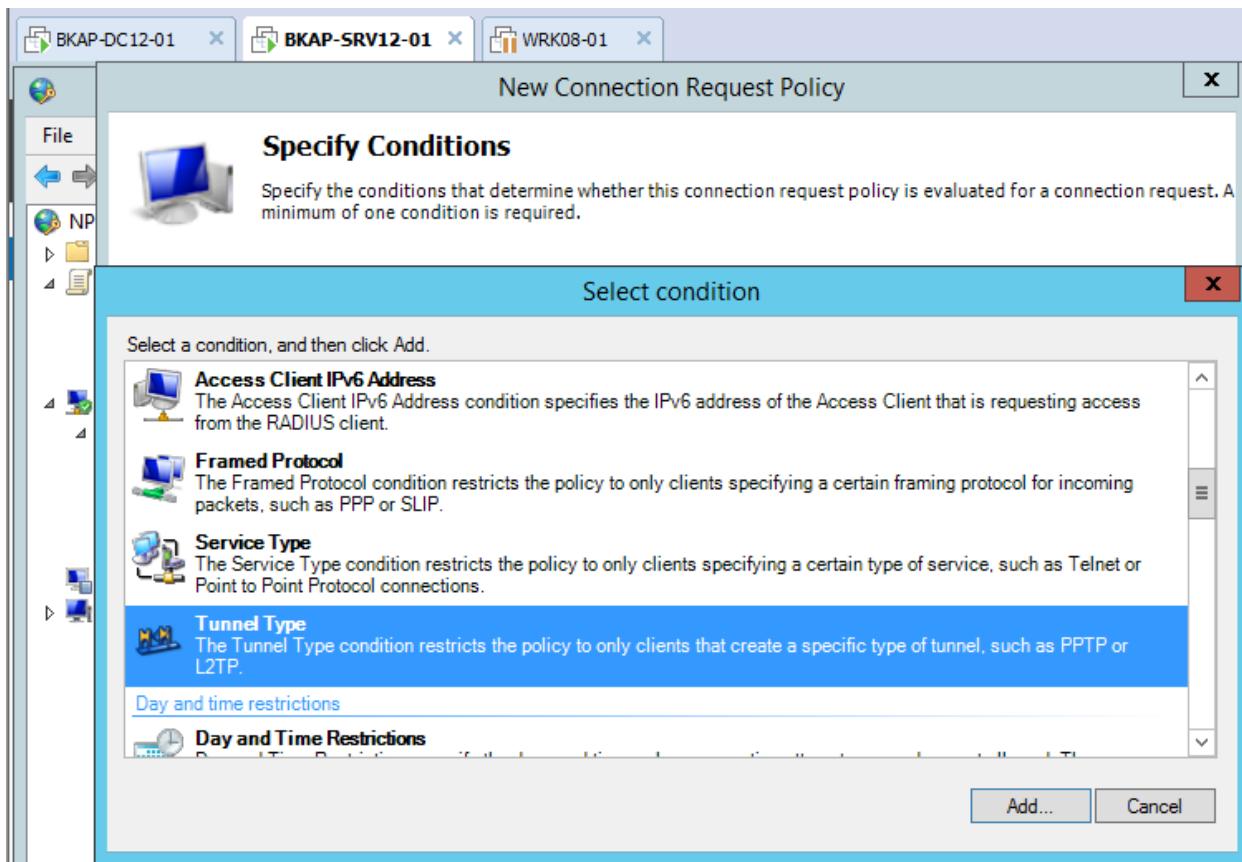
- Tại cửa sổ **Specify Connection Request...** nhập vào:
 - *Policy name:* **VPN Connection**.
 - Tại **Type of network access server** : chọn vào **Remote Access Server(VPN-Dial up)**
 - **Next.**



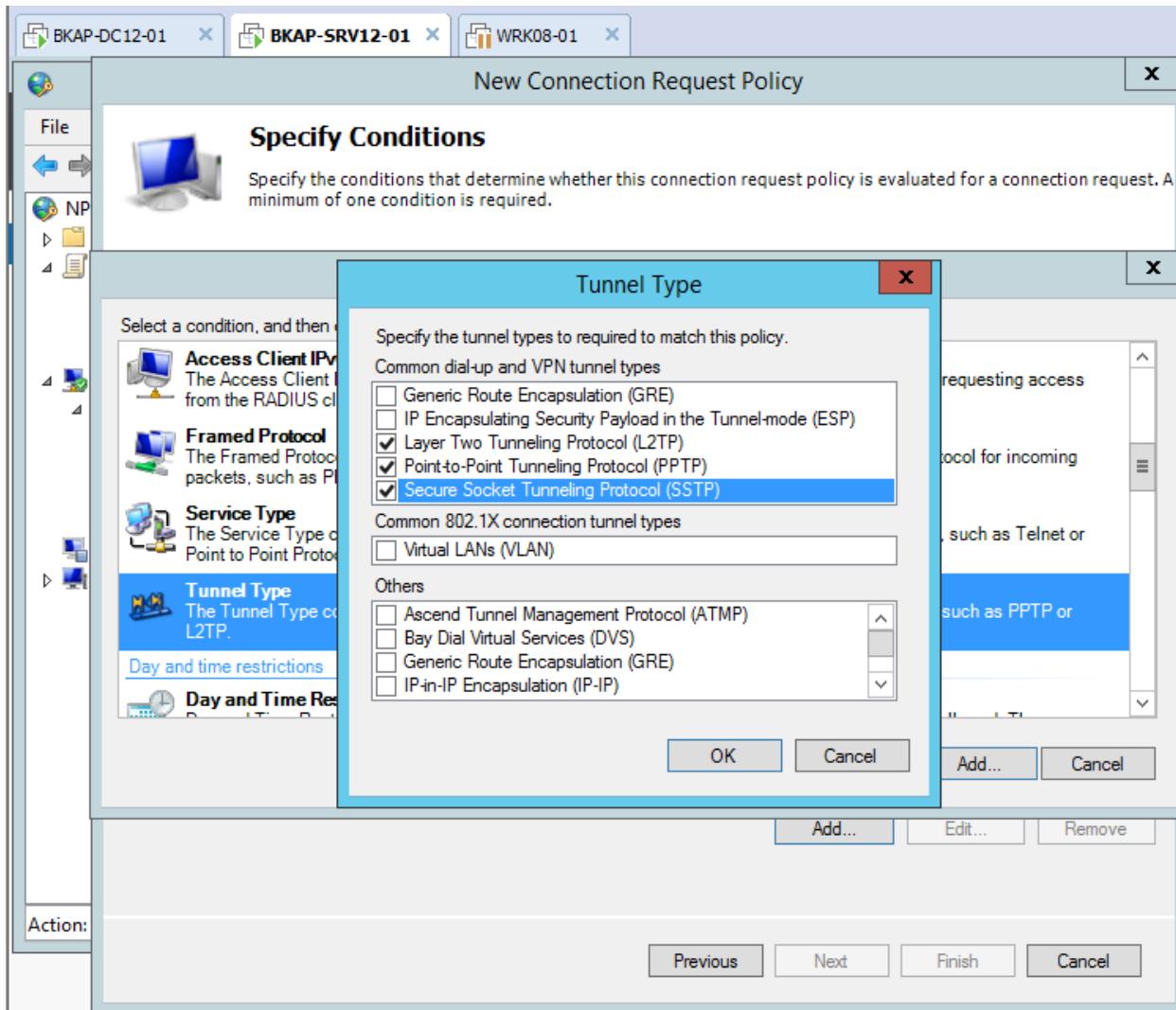
- Tại **Specify Conditions** , click vào **Add...**



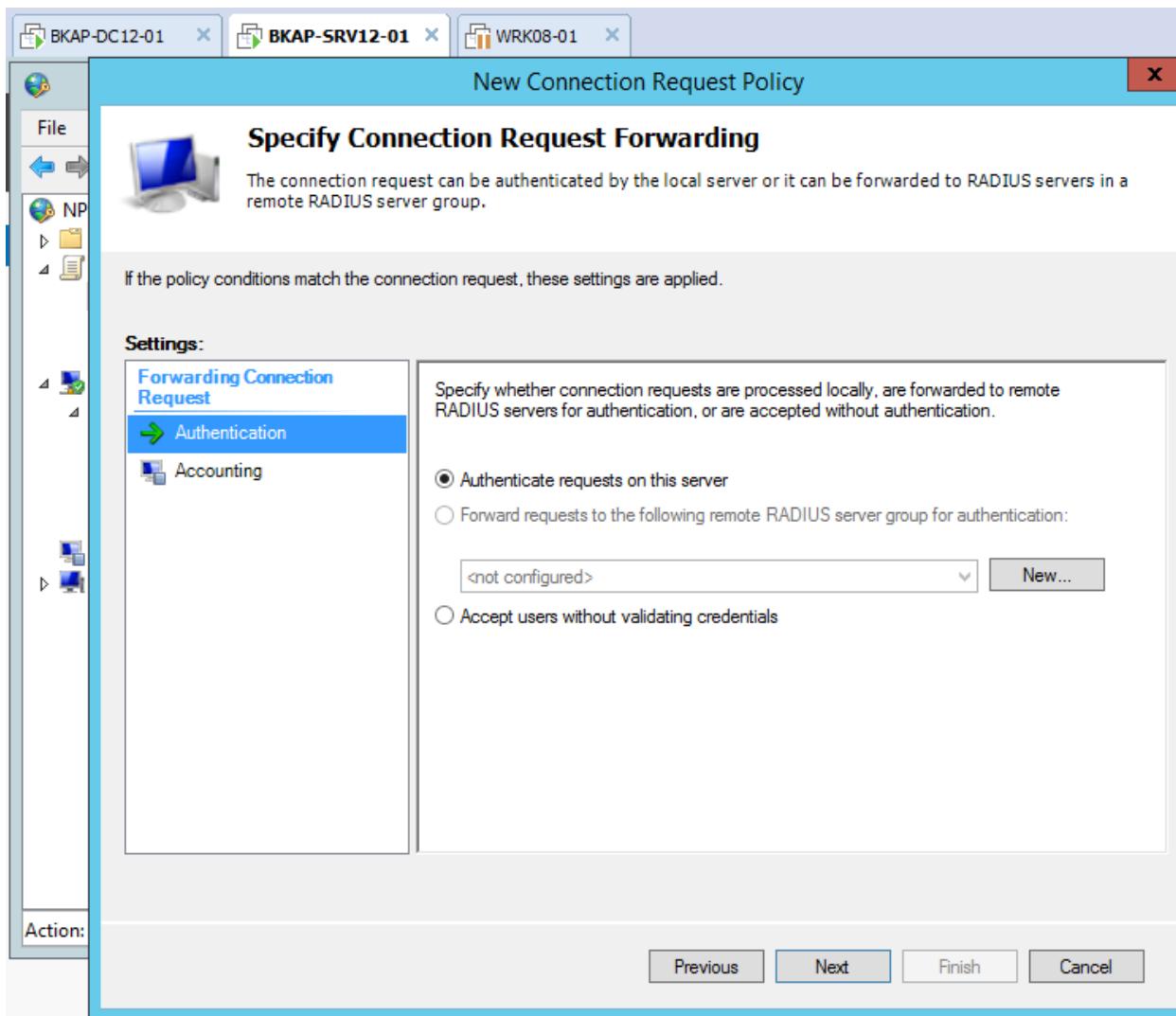
- Tại cửa sổ **Select condition**, chọn vào **Tunnel Type => Add...**



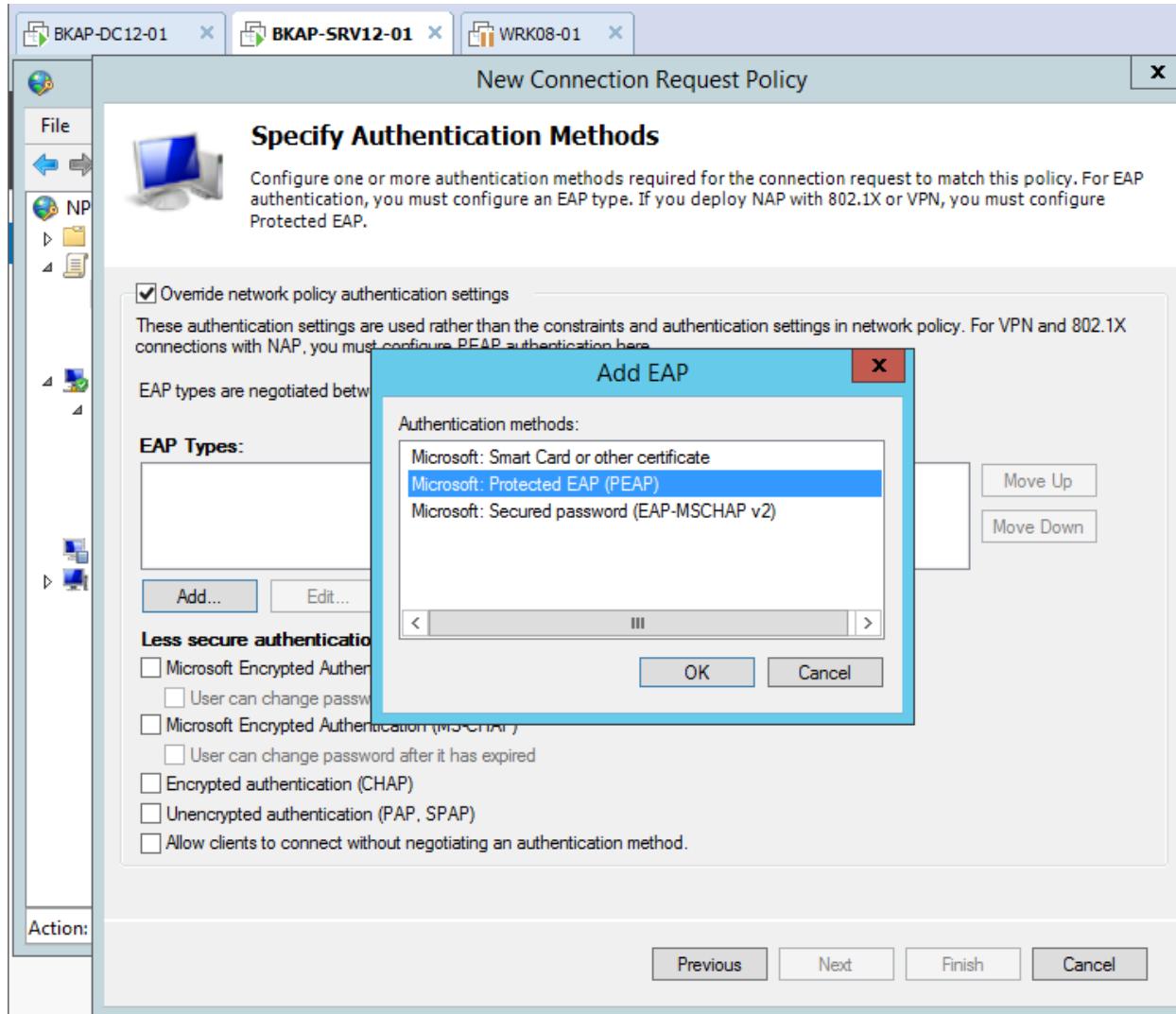
- Tại cửa sổ **Tunnel Type**, chọn vào 3 kiểu giao thức *L2TP, PPTP, SSTP*.



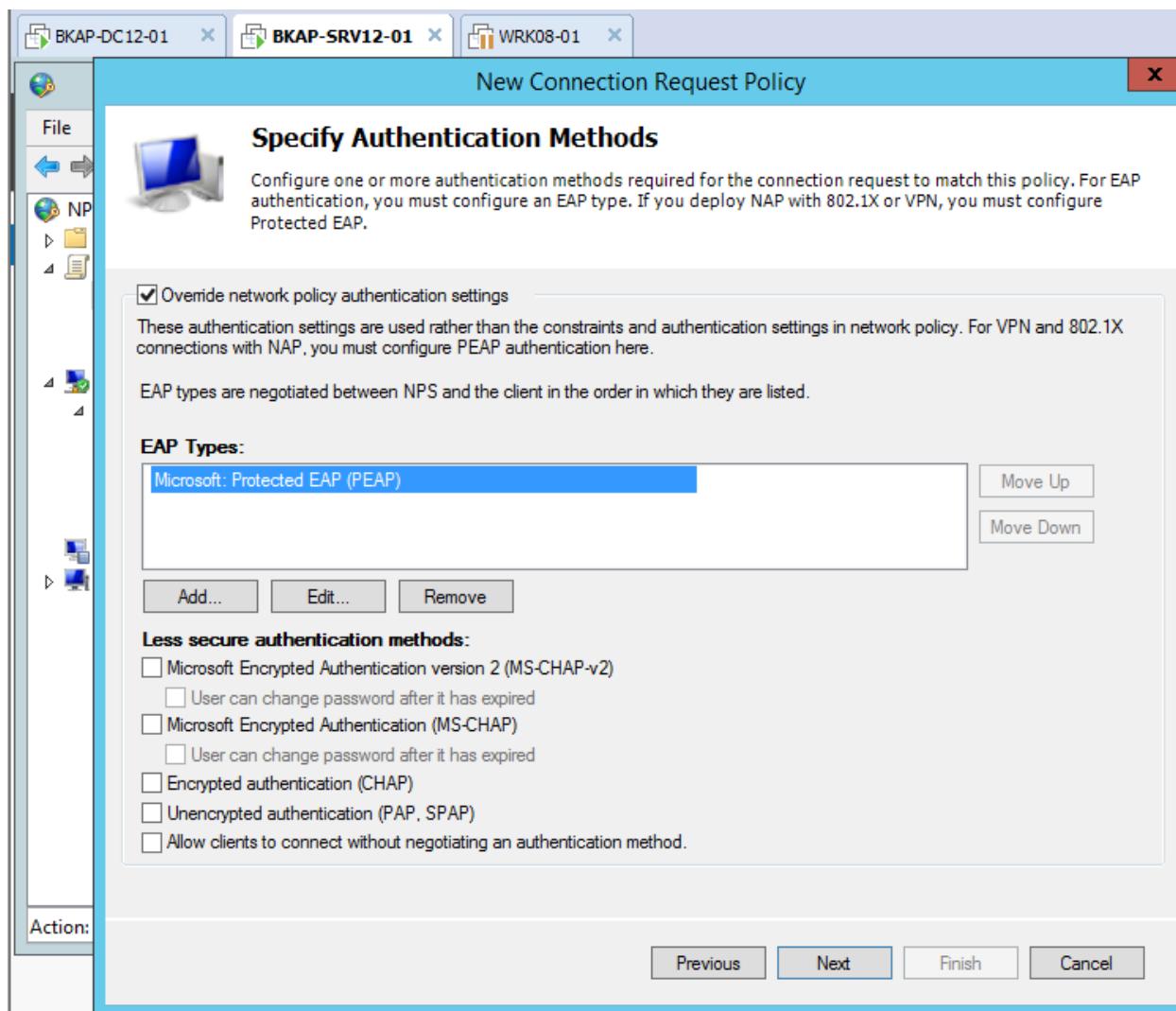
- Tại cửa sổ **Specify Connection Request Forwarding**, click vào Next.



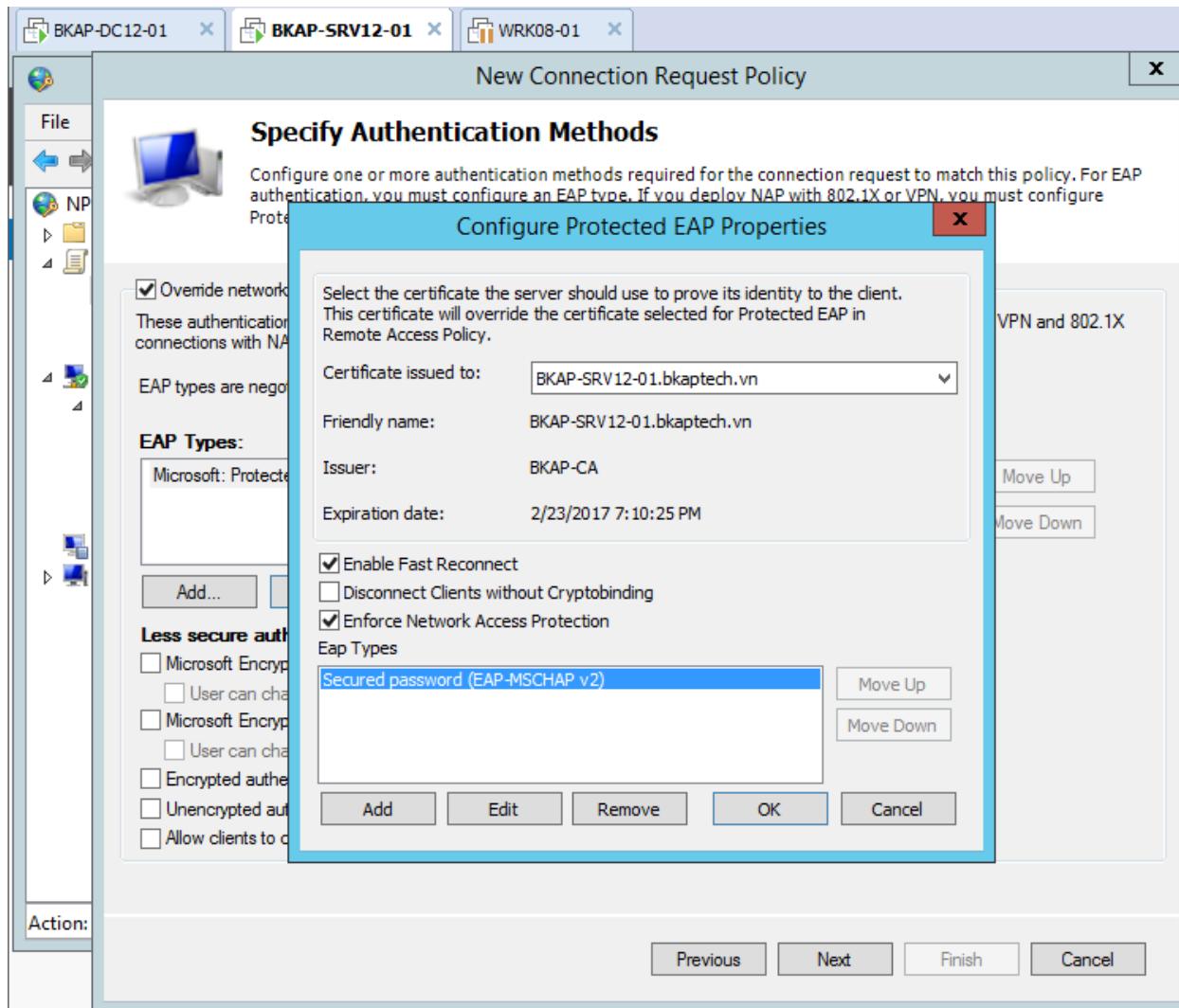
- Tại cửa sổ **Specify Authentication Methods** , tại mục **EAP Types:** , click vào **Add..**
 - Tại cửa sổ **Add EAP** , chọn vào **Microsoft: Protected EAP (PEAP)**.



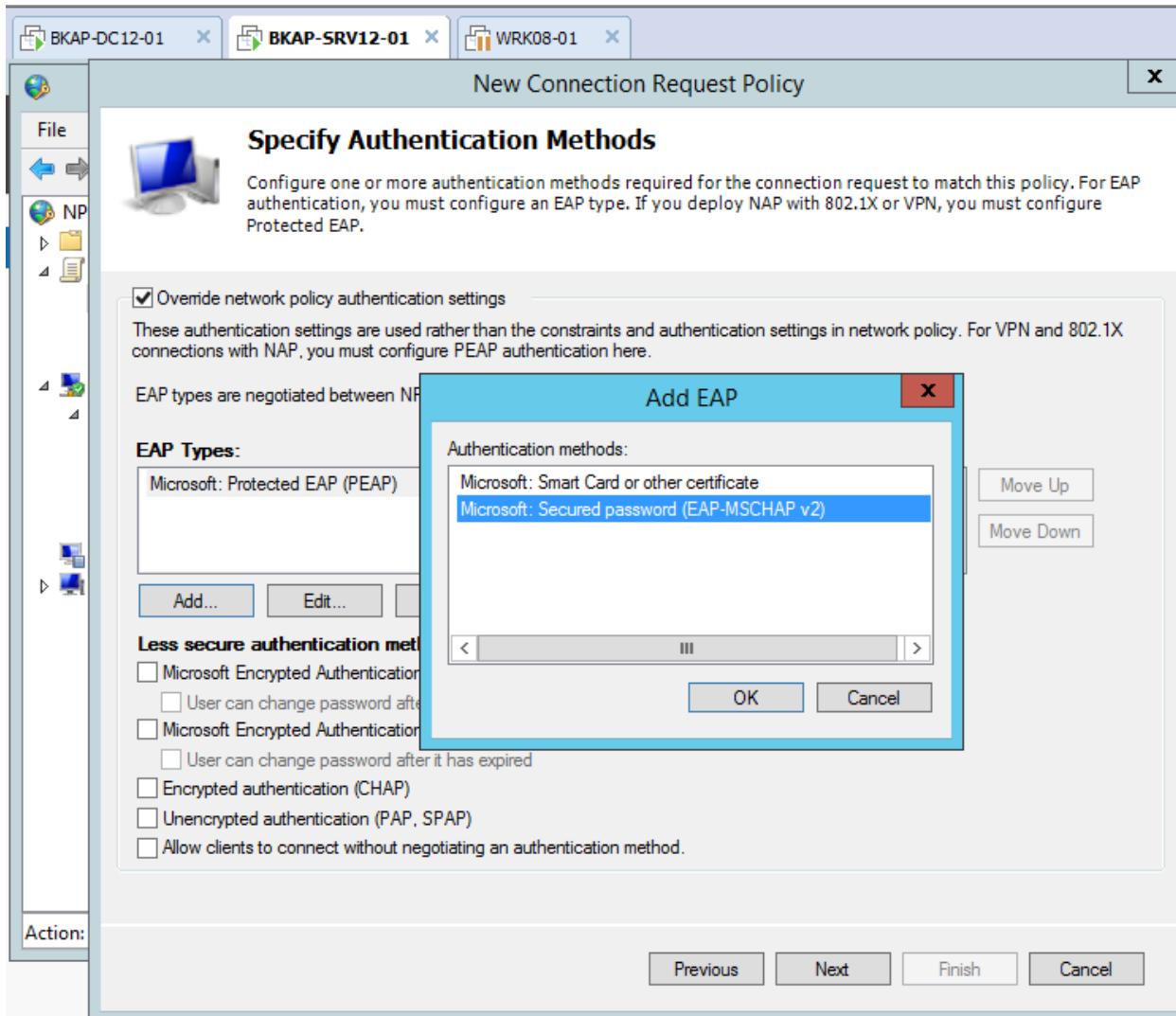
- Click vào dòng **Microsoft:Protected EAP (PEAP)** , click vào **Edit...**



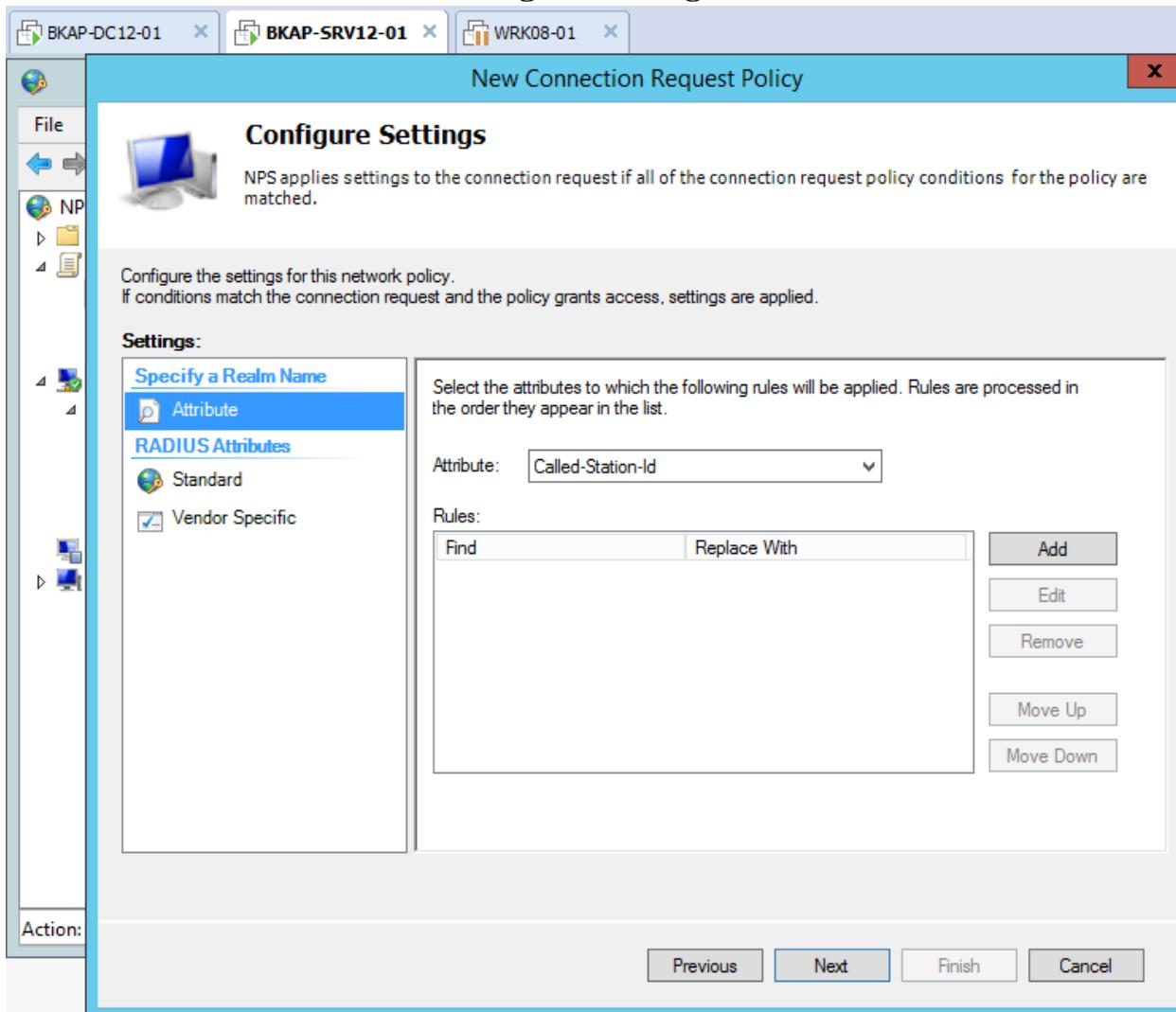
- Trong cửa sổ **Configure Protected EAP Properties**, đánh dấu tại **Enable Fast Reconnect** và **Enforce Network Access Protection**.=> OK.



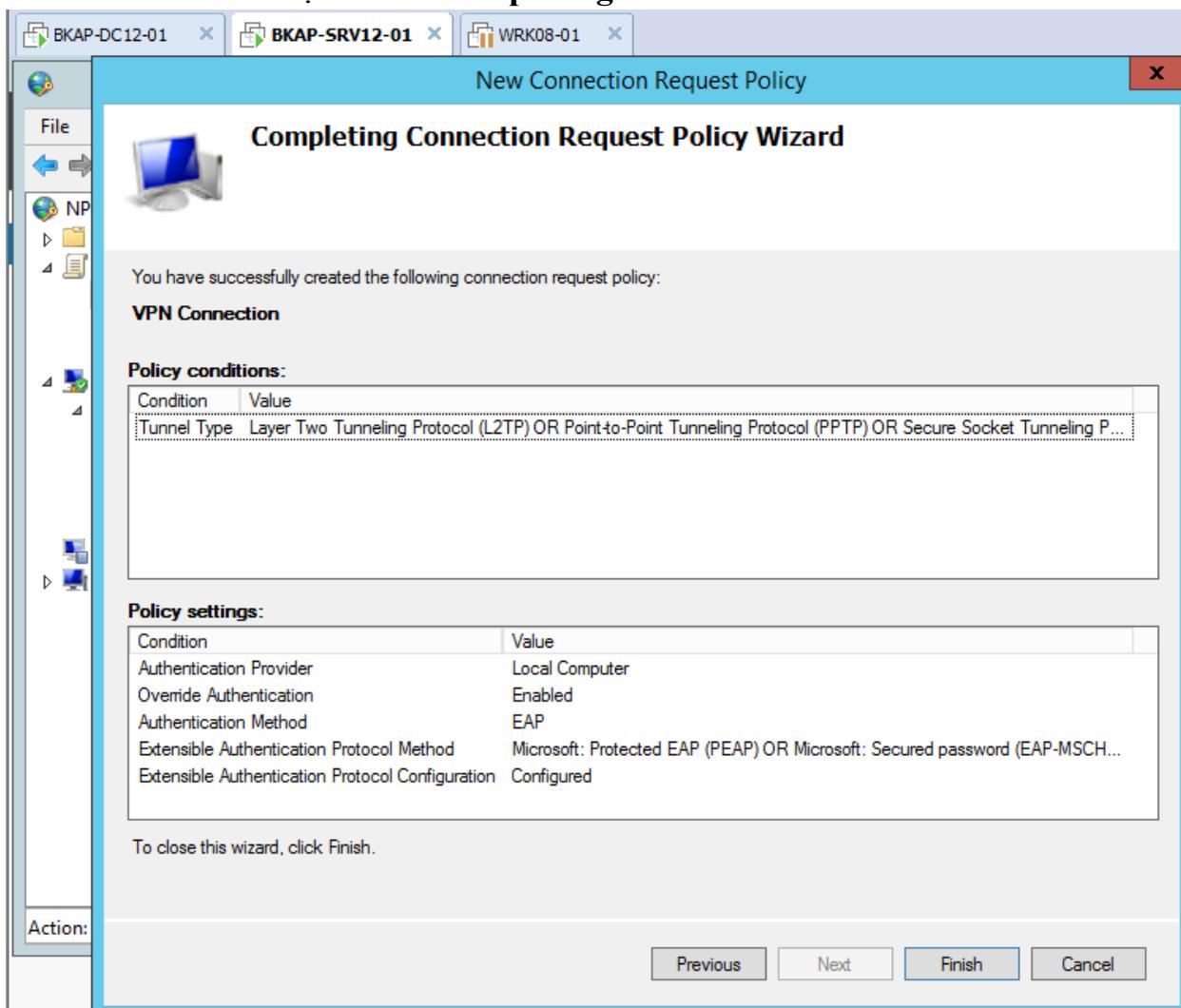
- Tại **EAP Types**, click vào **Add...**, trong cửa sổ **Add EAP**, chọn vào **Microsoft:Secured password (EAP-MSCHAP v2)** => **OK**.



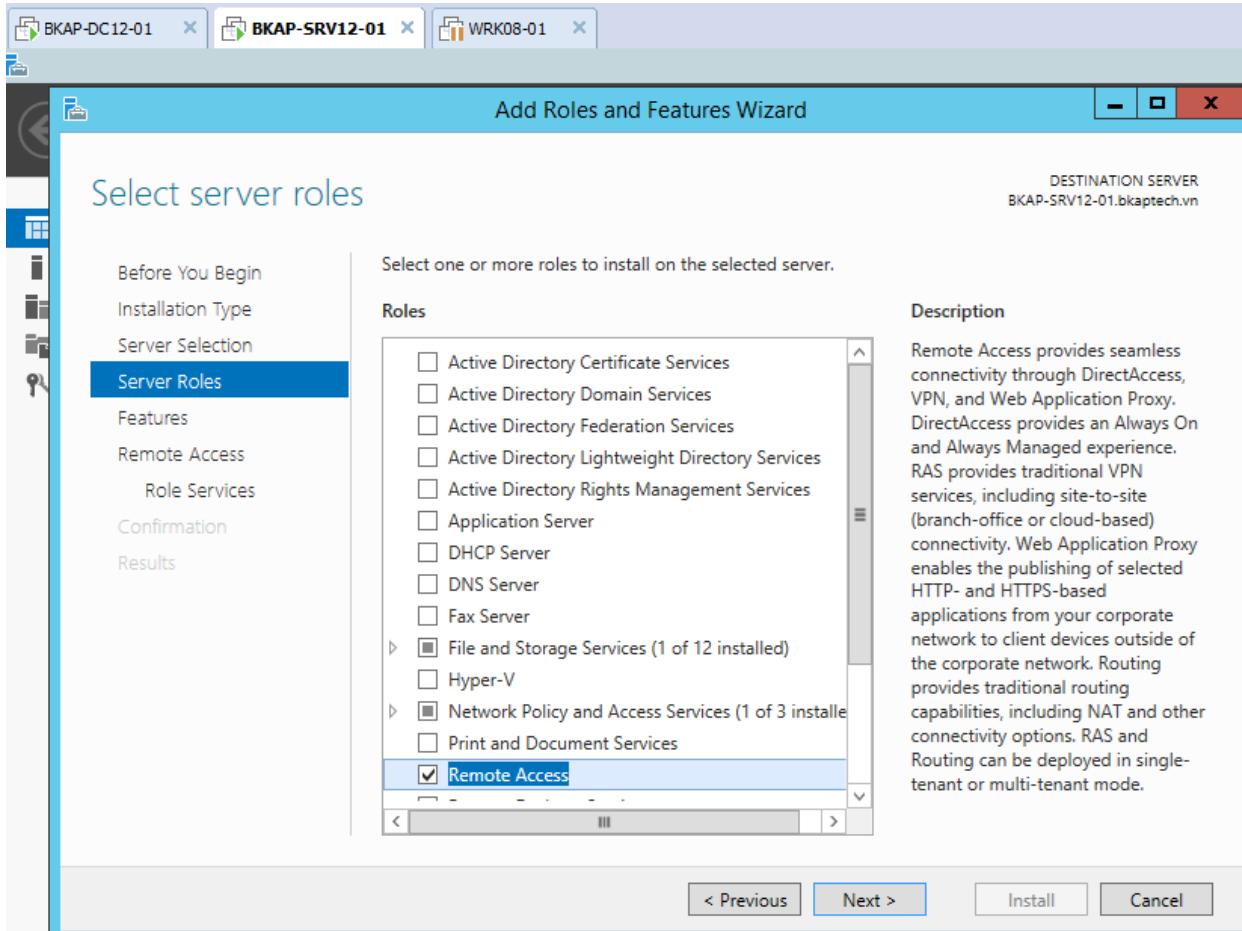
- Click vào **Next**.
- Tại cửa sổ **Configure Settings**, click vào **Next**.

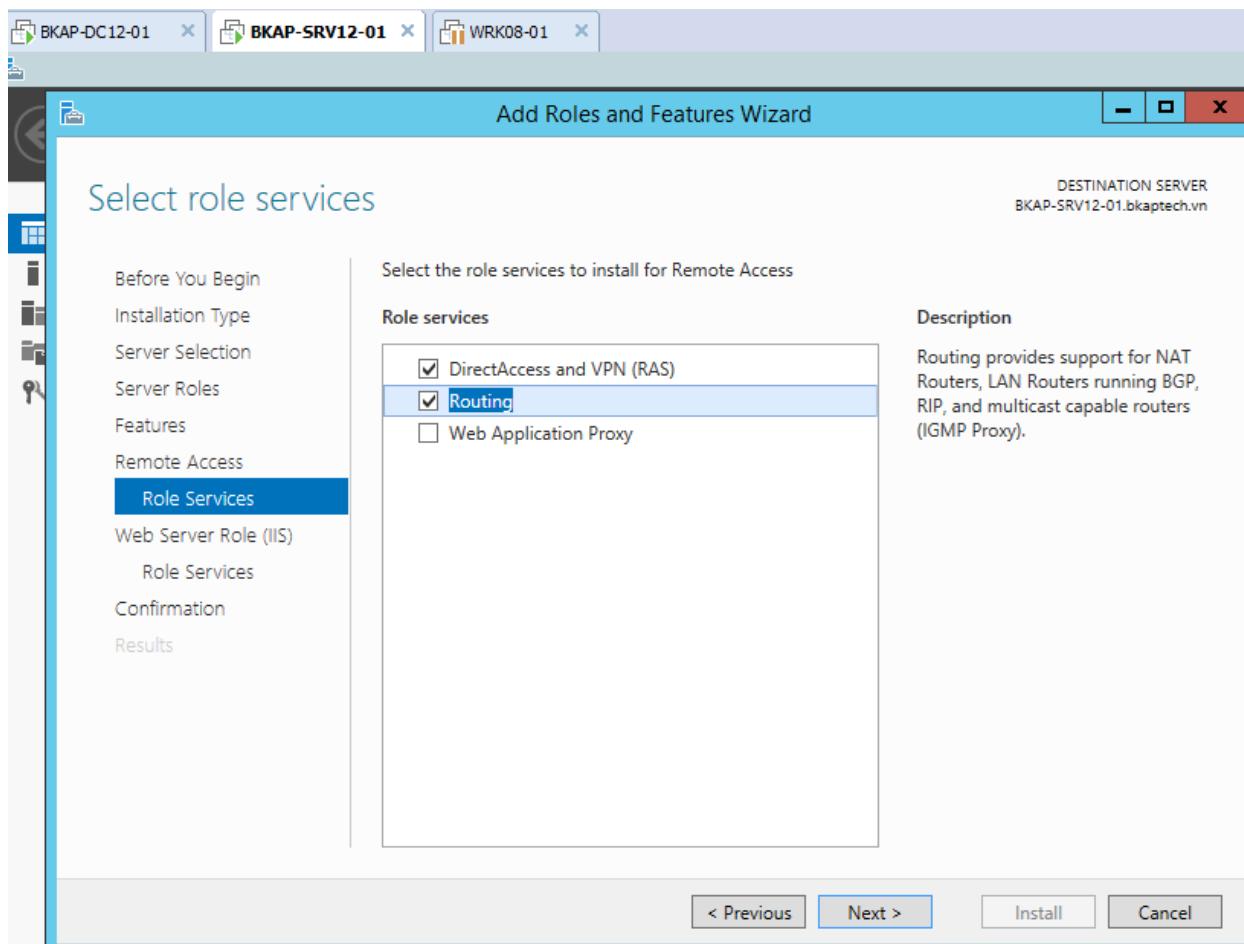


- Tại cửa sổ Completing Connection... click vào Finish.

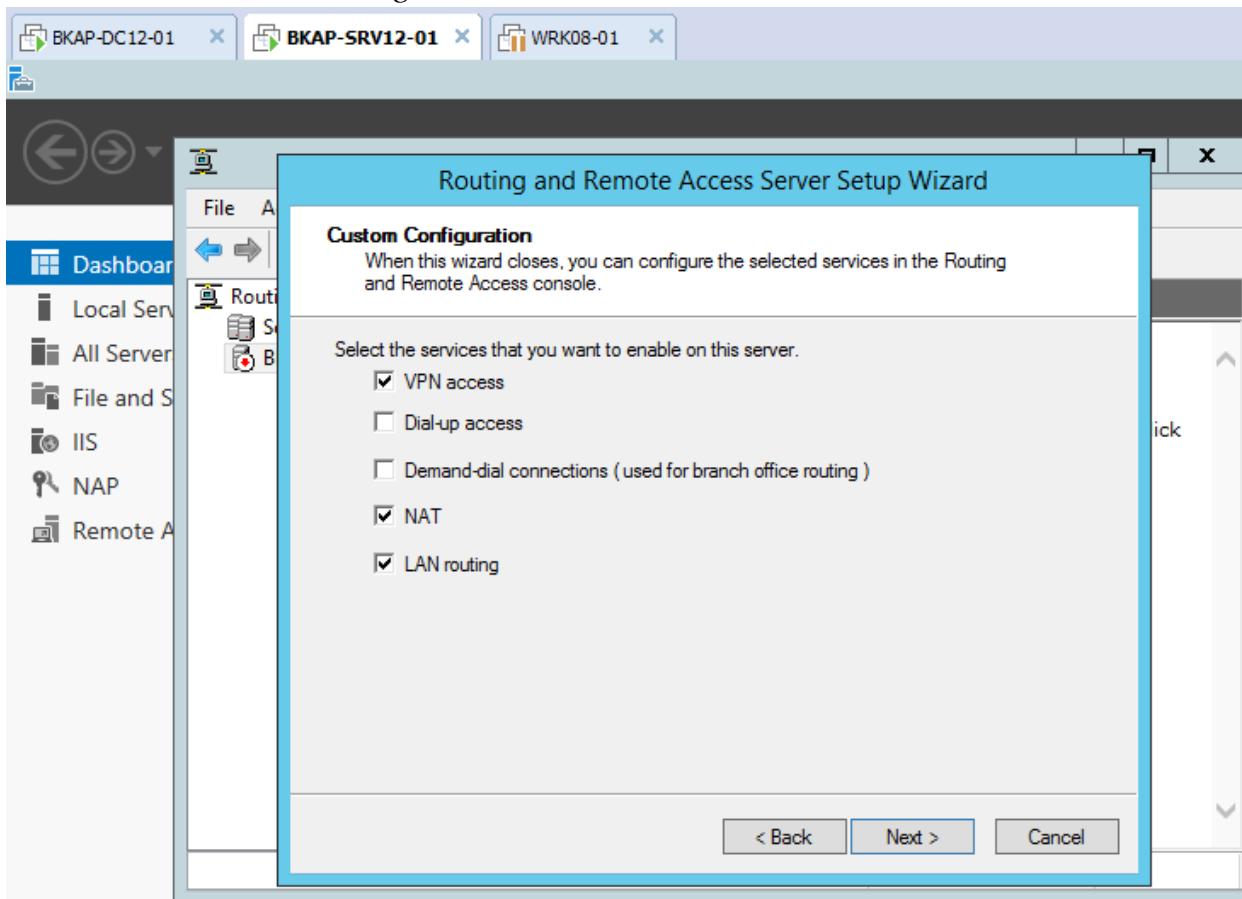


- Thực hiện cài đặt dịch vụ **Remote Access**.
 - *Direct Access and VPN (RAS)*
 - *Routing*.

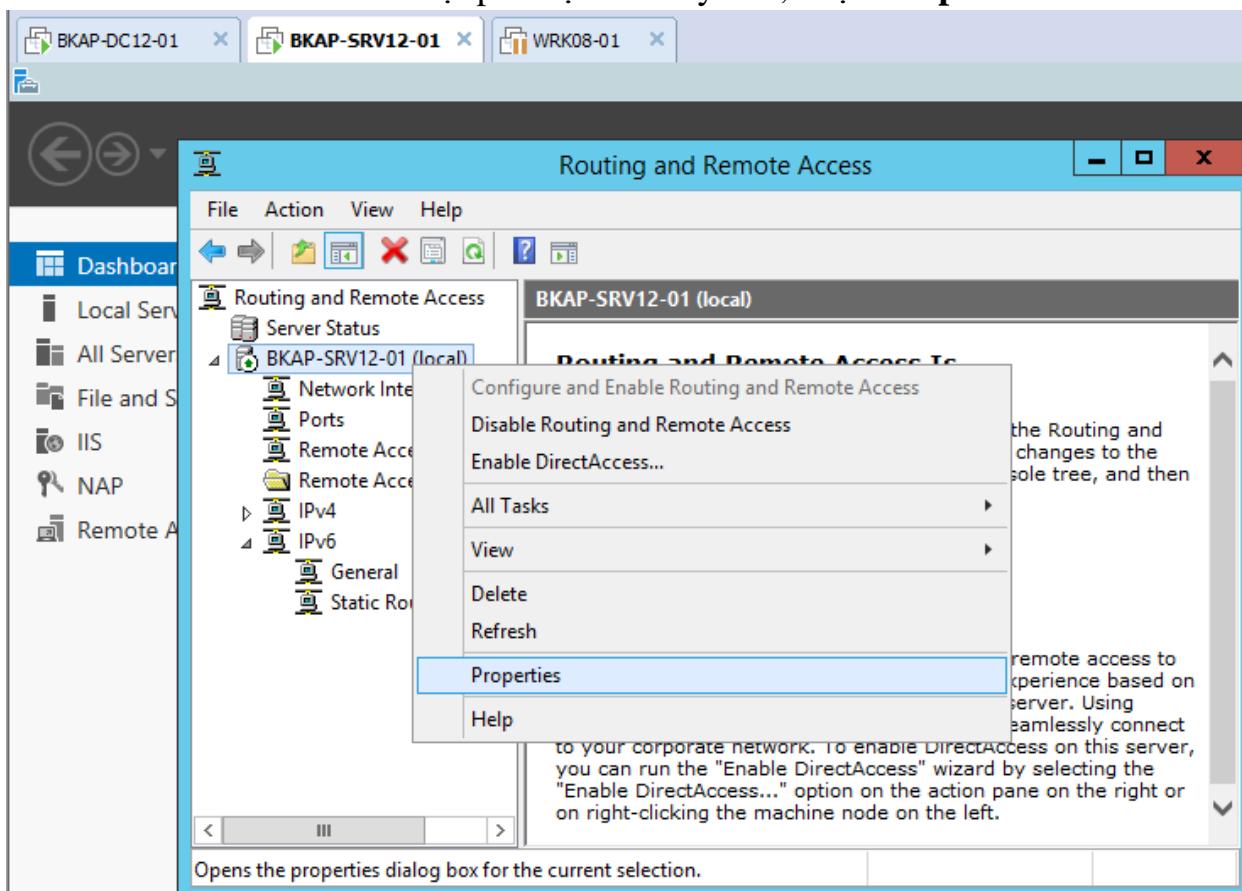




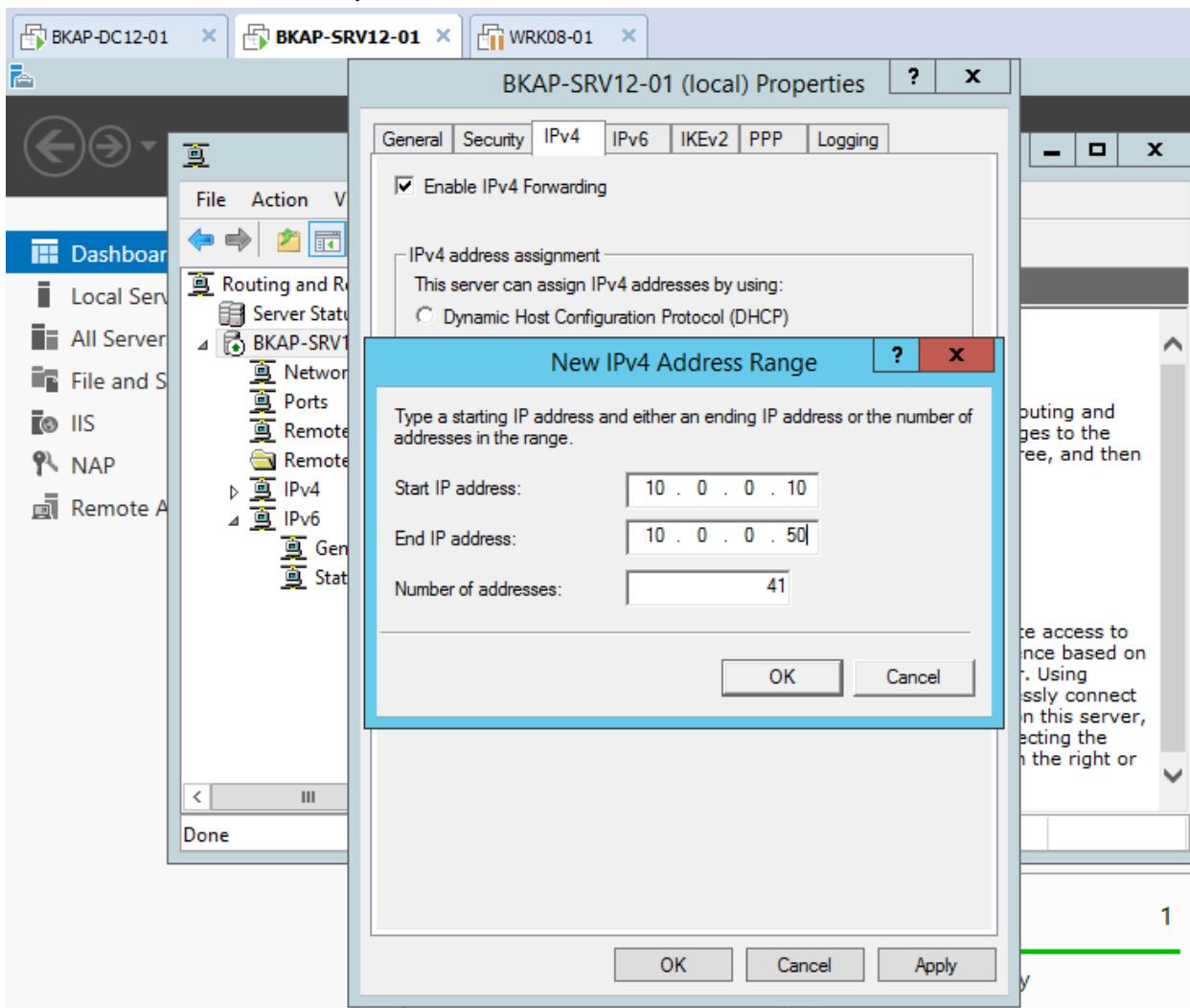
- Cấu hình dịch vụ VPN.
 - Tại **Custom Configuration** chọn *VPN Access , NAT , LAN Routing.*



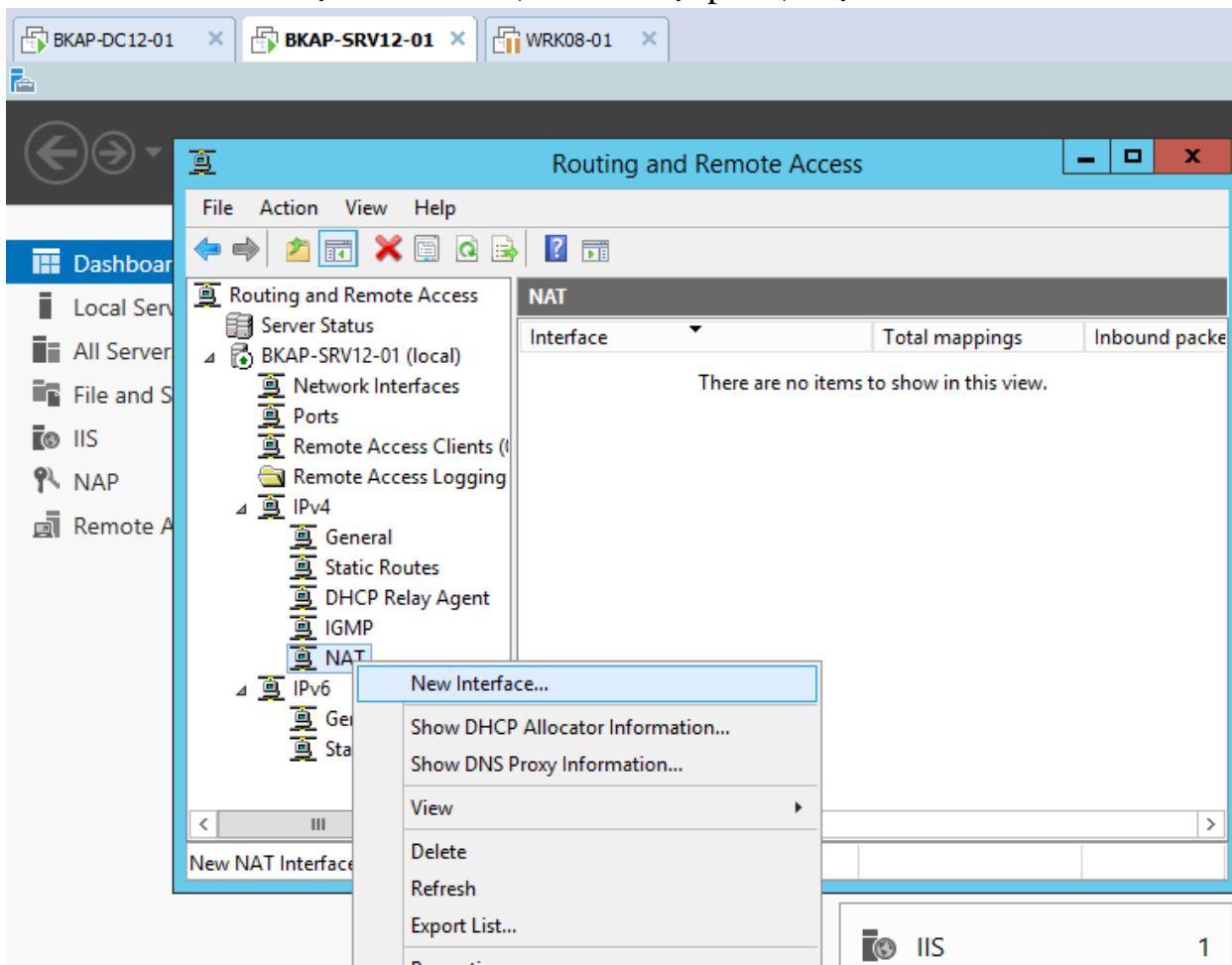
- Click chuột phải tại tên máy chủ, chọn **Properties**.



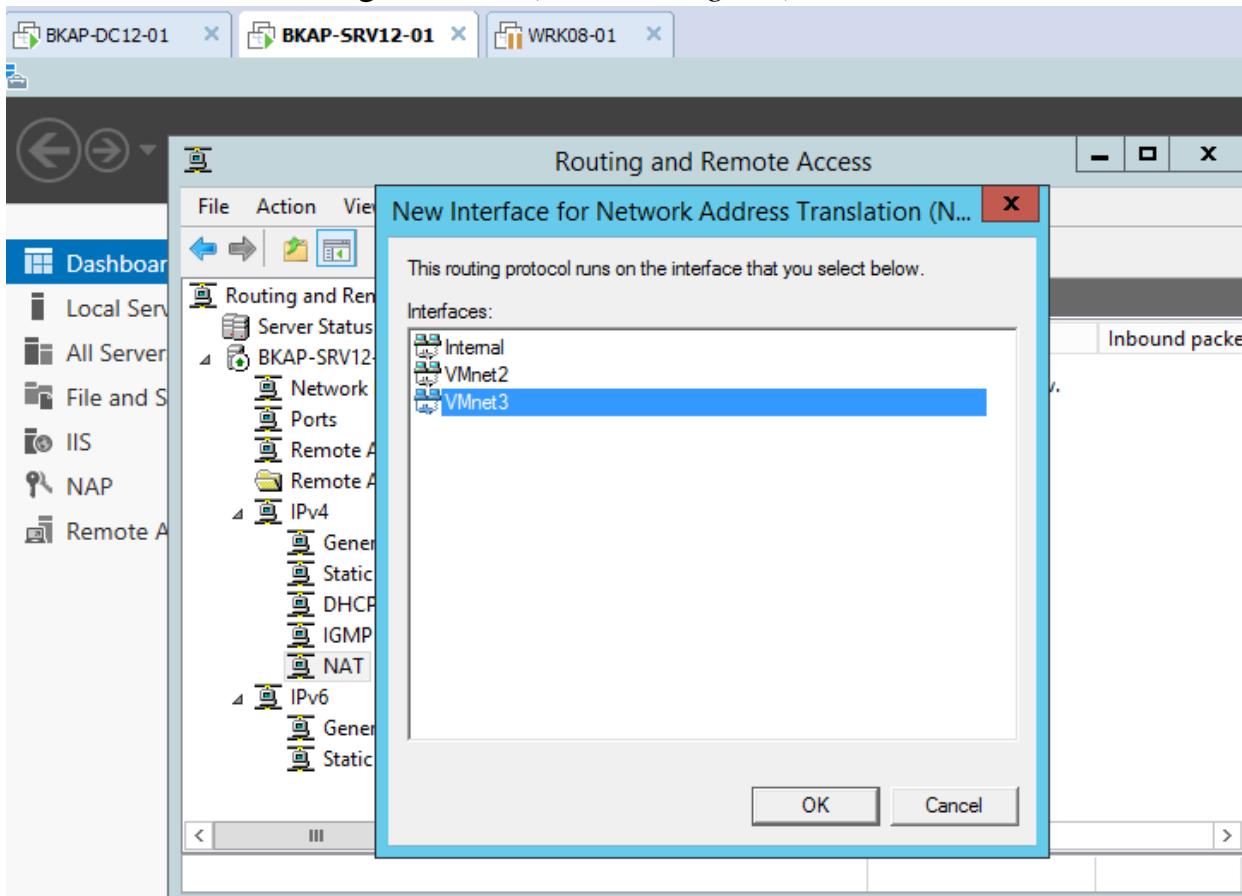
- Chuyển sang Tab **IPv4**, chọn vào **Static address pool**, Add dải địa chỉ $10.0.0.10 \Rightarrow 10.0.0.50$.



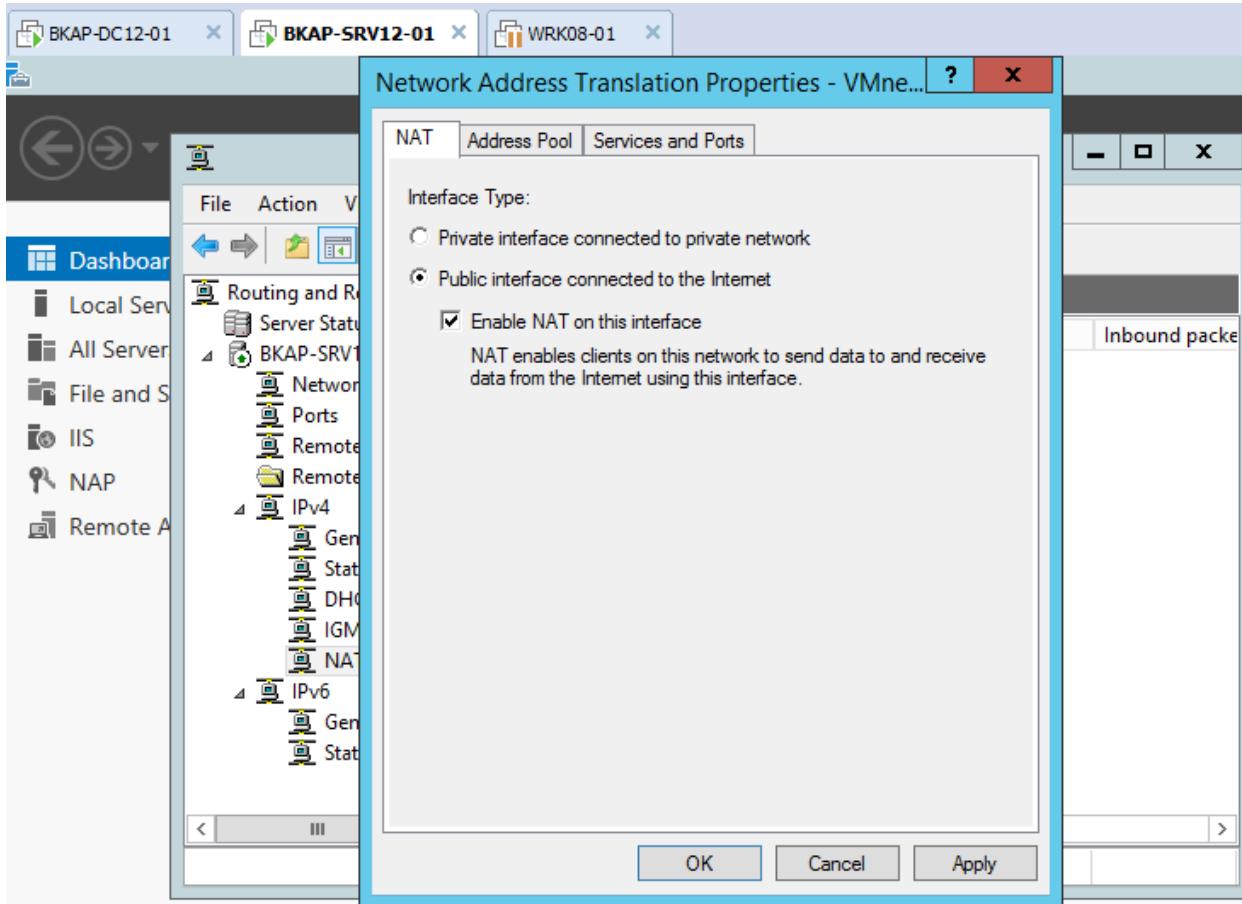
- Tại **IPv4/NAT** , click chuột phải , chọn **New Interface...**



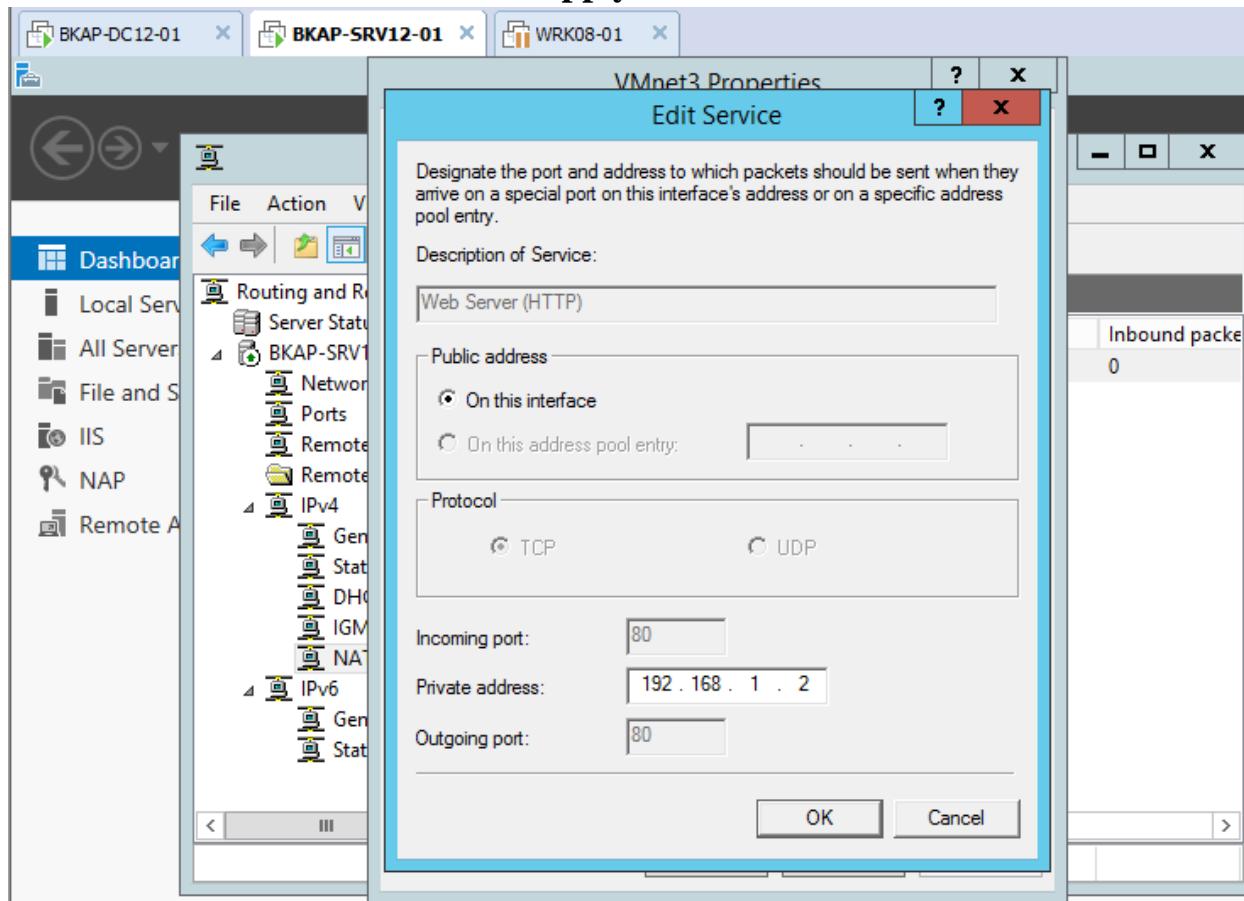
- Tại cửa sổ New Interface for Network Address...chọn card mạng **VMnet3** (*card bên ngoài*).

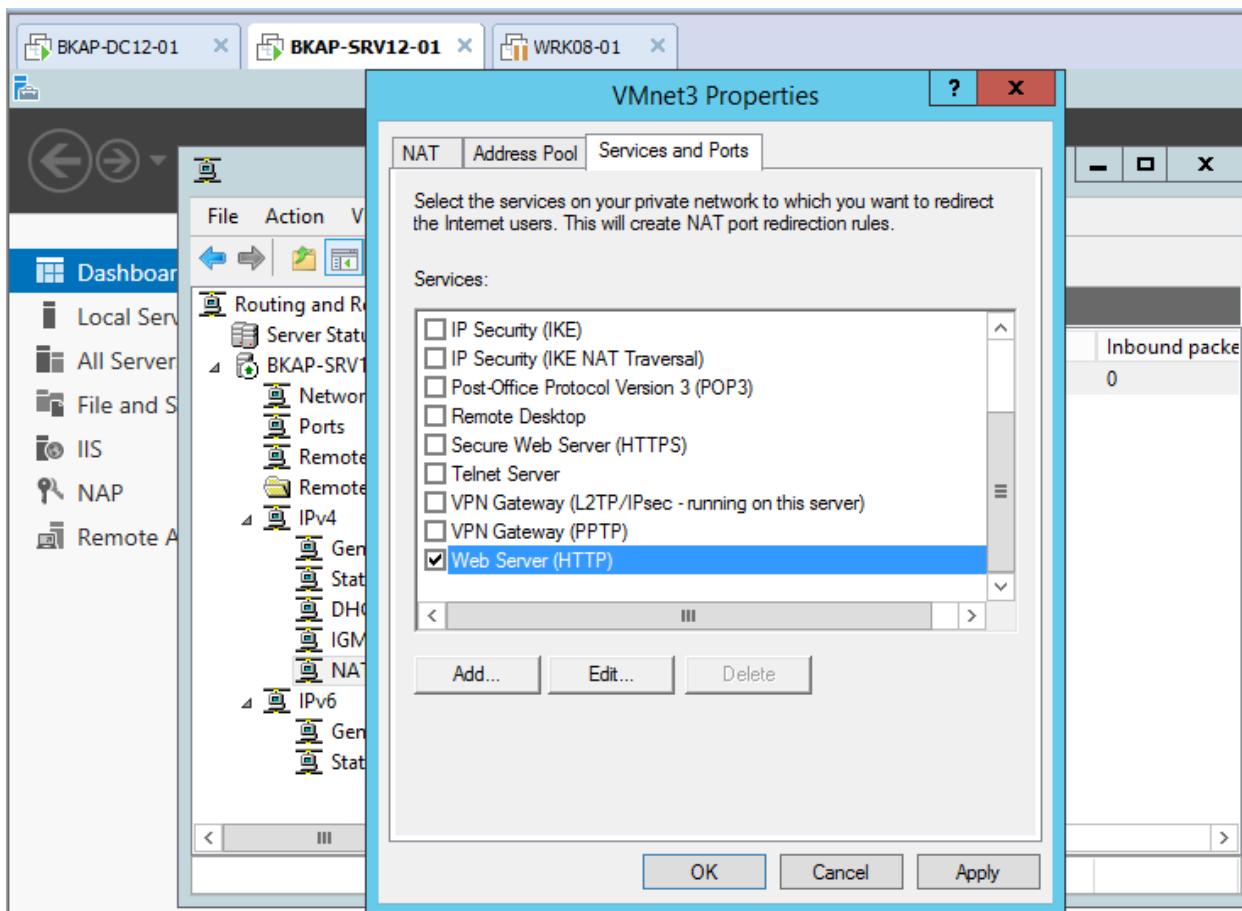


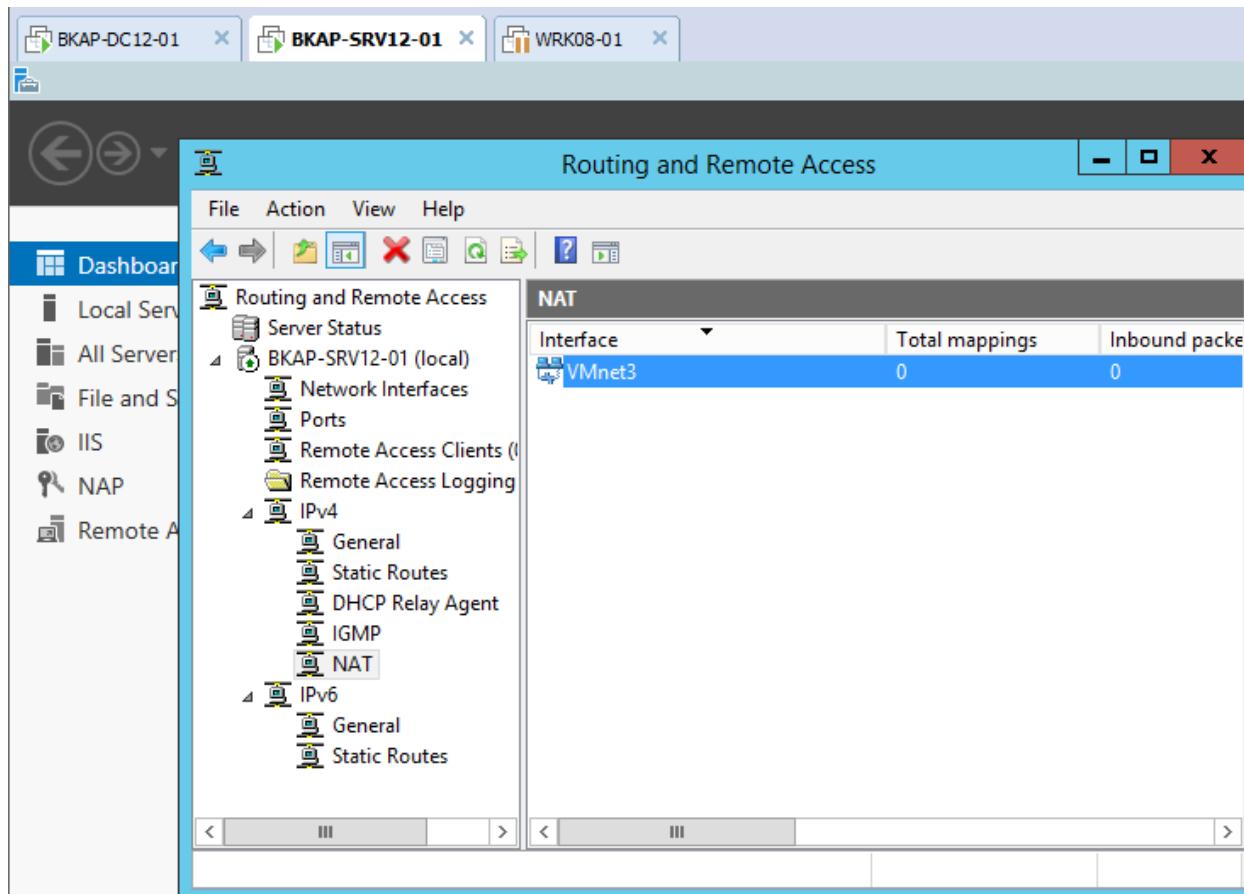
- Tại cửa sổ Network Address Translation Properties.. đánh dấu tại Public interface connected to the Internet và Enable NAT...



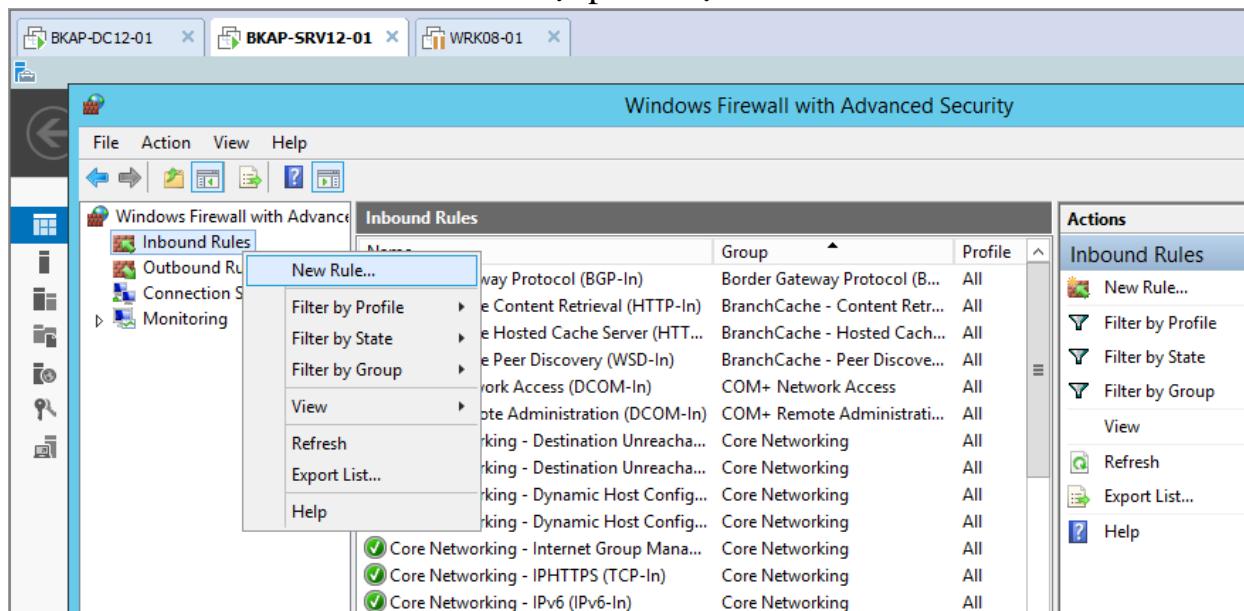
- Chuyển sang tab **Services and Ports**, đánh dấu vào **Web Server (HTTP)** , nhập vào địa chỉ **Private address** : **192.168.1.2 => Apply / OK.**



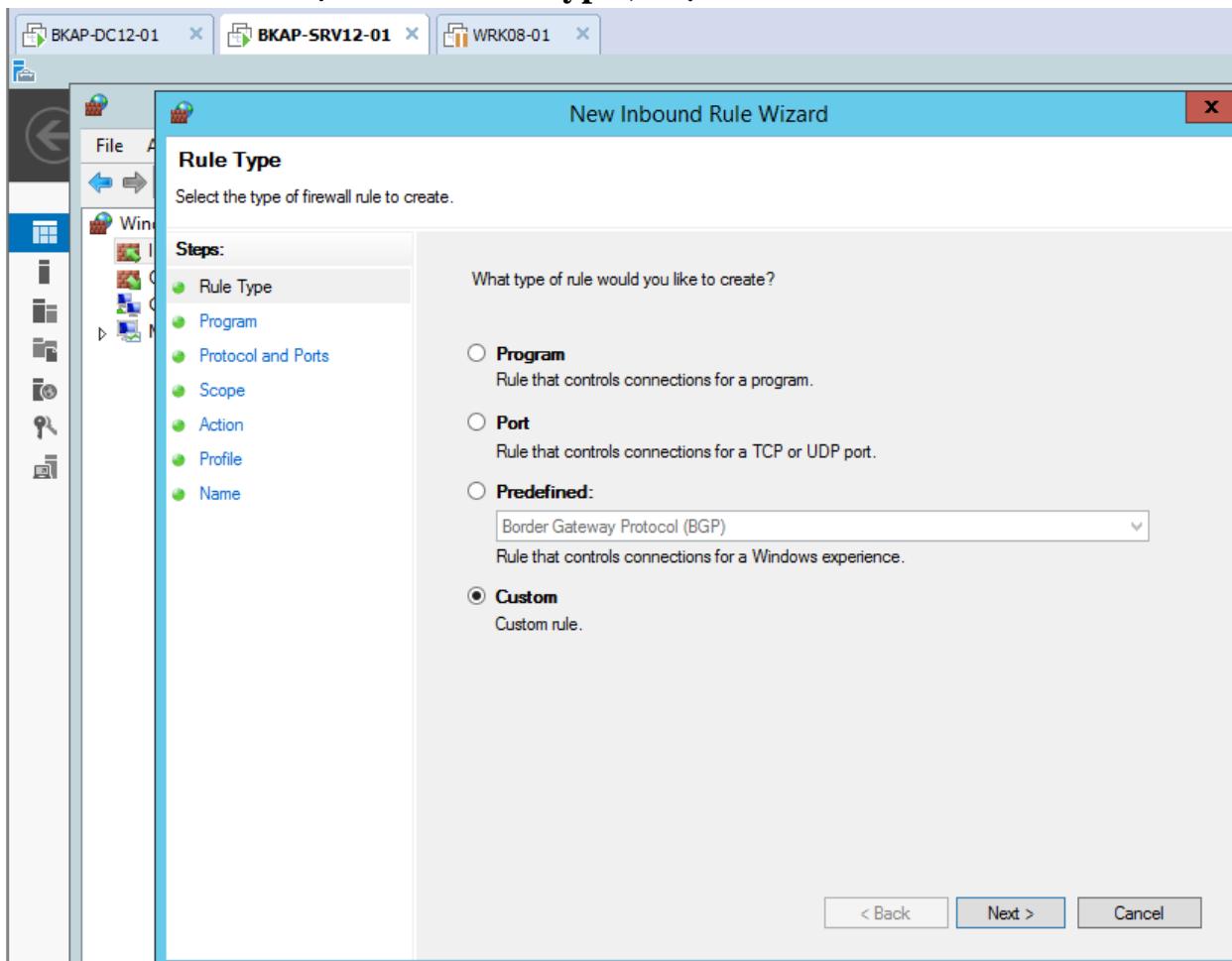




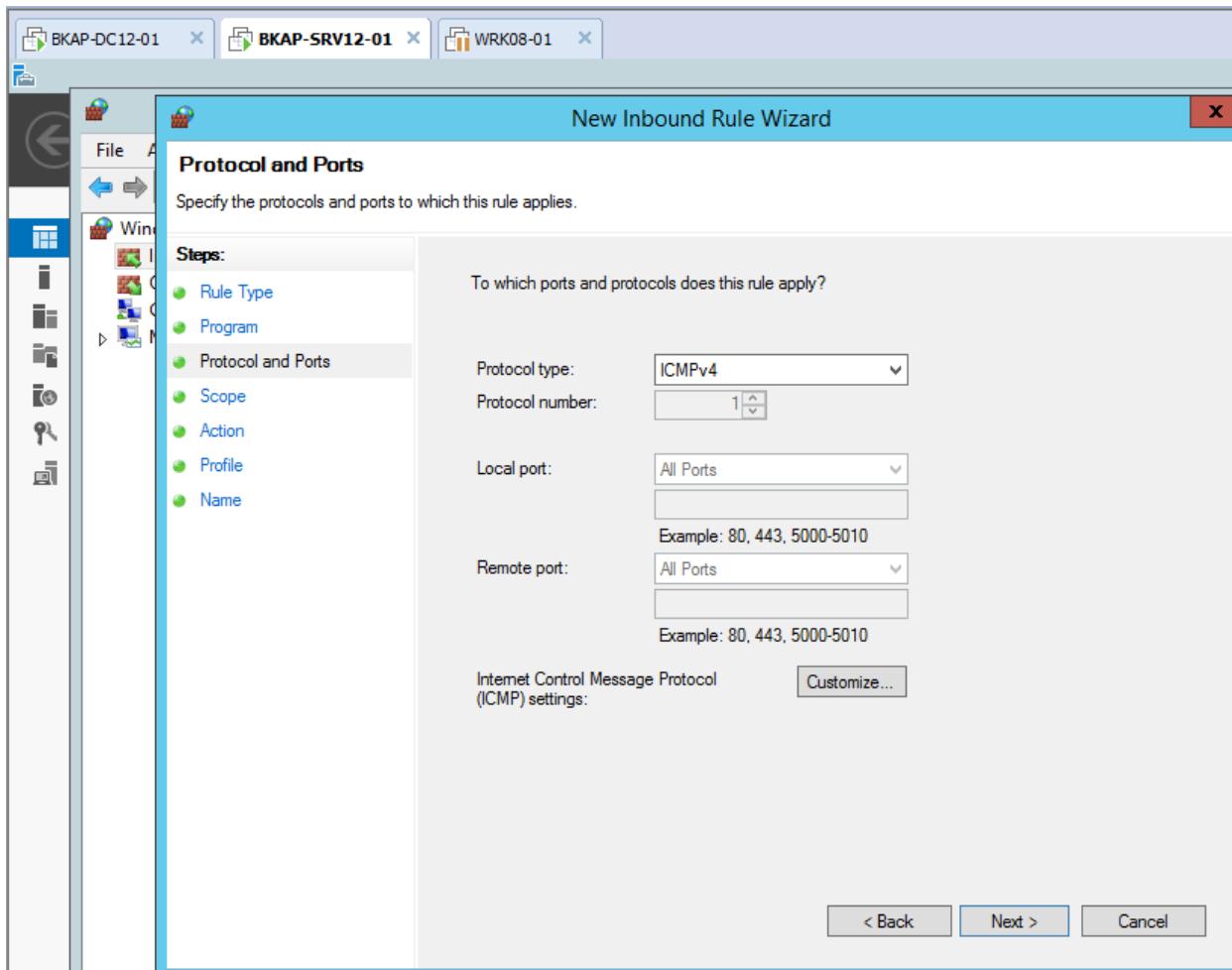
- Thực hiện cấu hình Windows Firewall.
 - Vào Windows Firewall with Advanced Security / Inbound Rules / click chuột phải chọn New Rule.



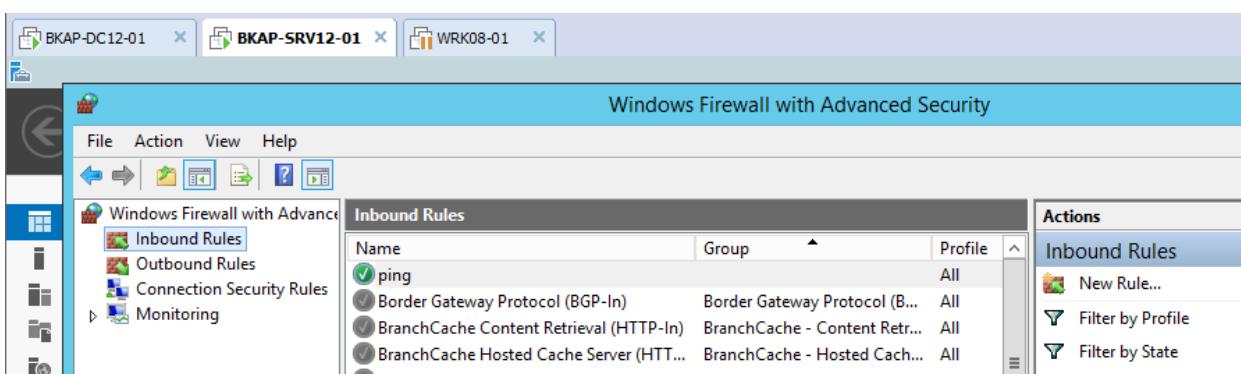
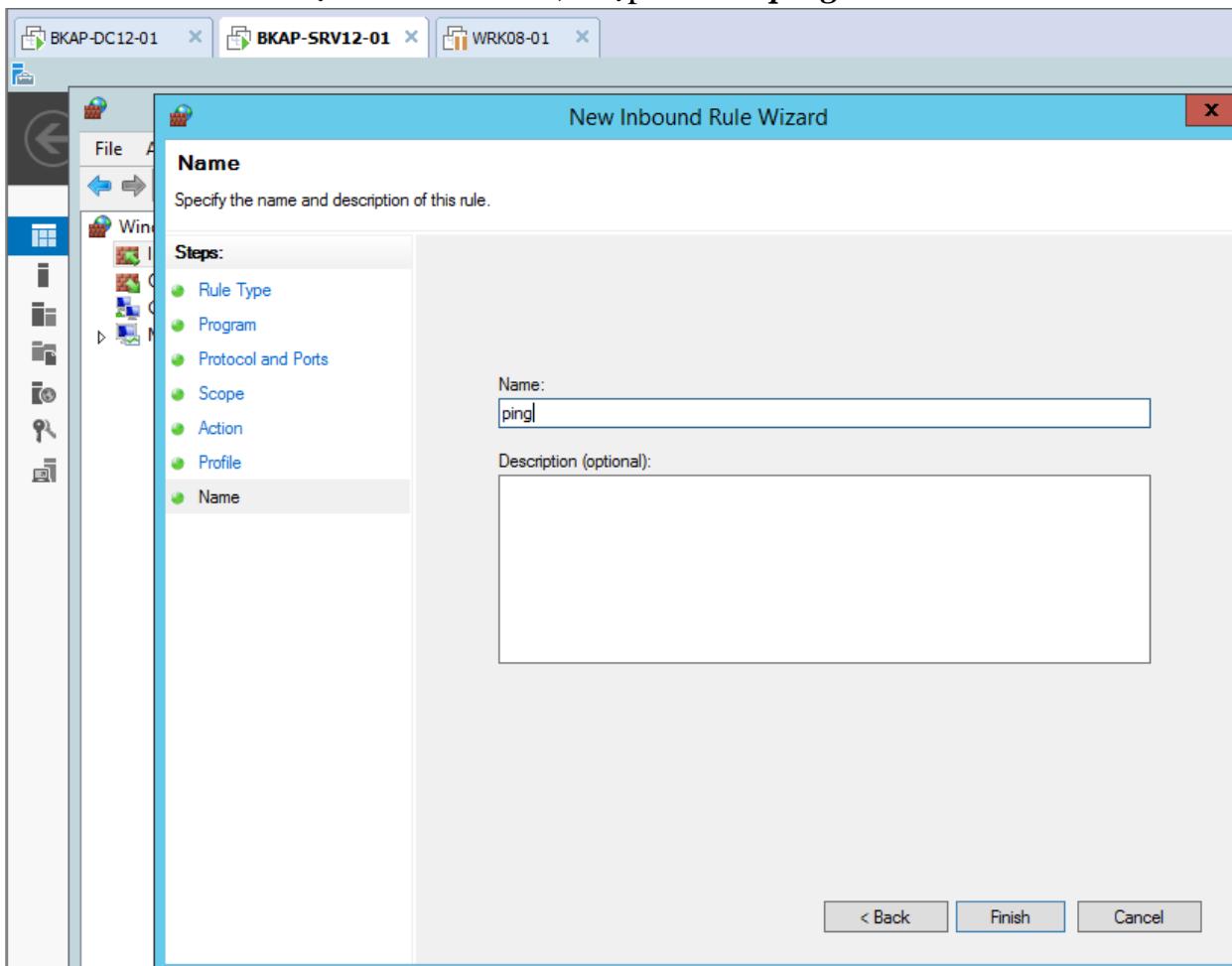
- Tại cửa sổ Rule Type , chọn Custom.



- Tại cửa sổ **Protocol and Ports**, tại mục **Protocol type**, chọn **ICMPv4**.

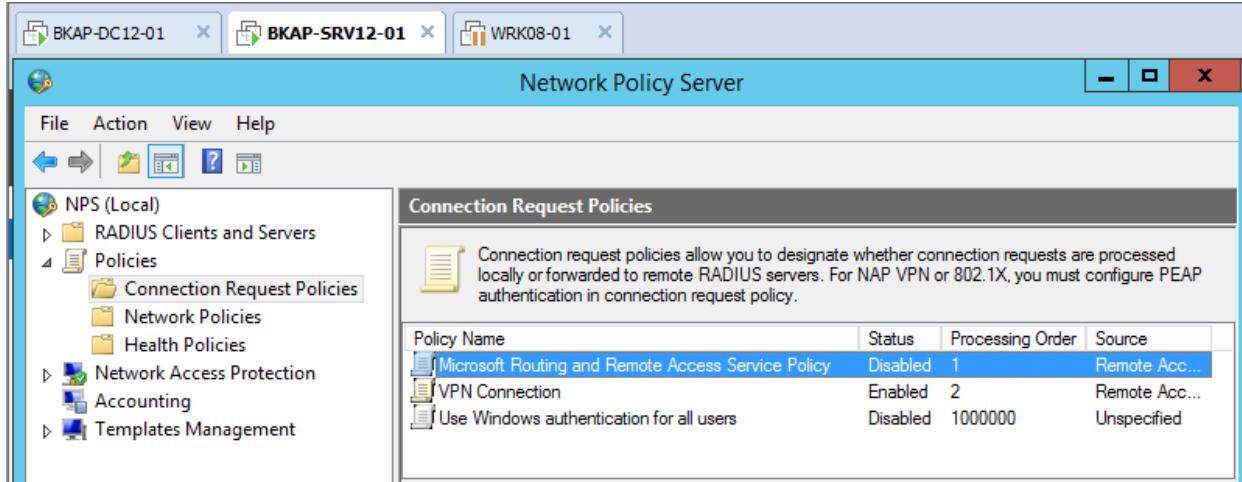


- Tại cửa sổ **Name**, nhập vào tên *ping*.



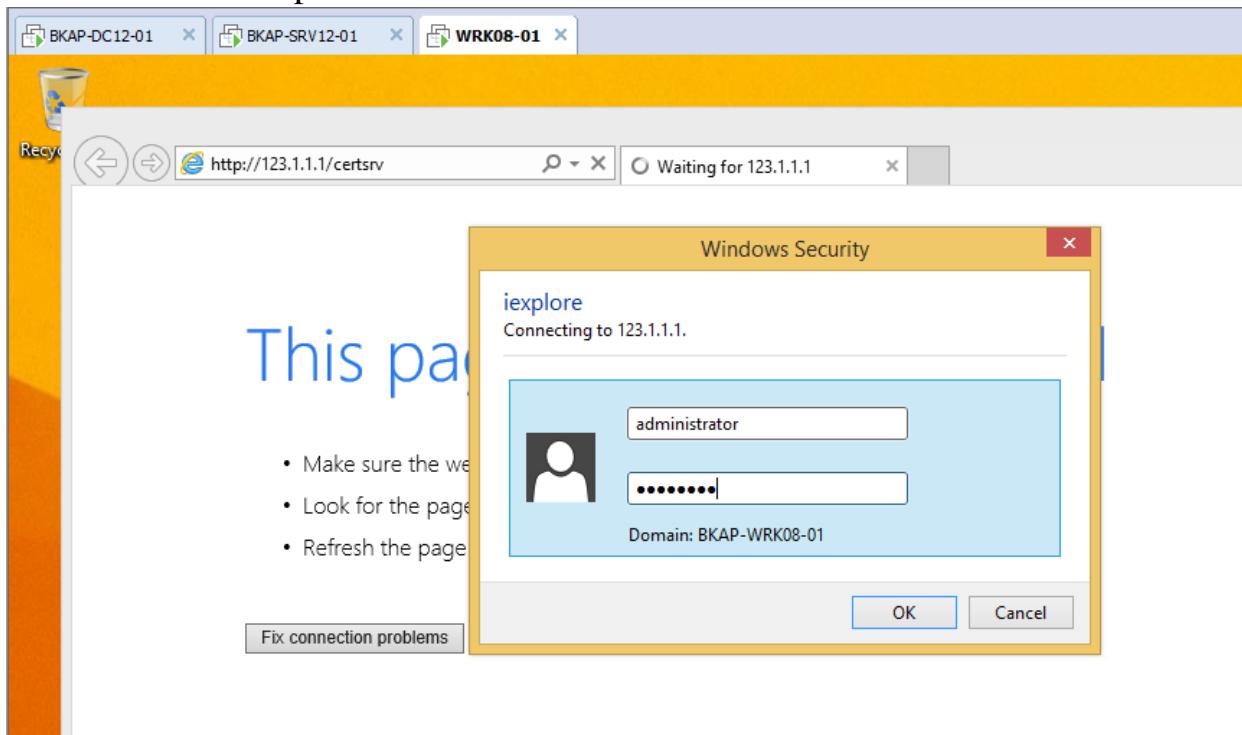
- Vào Network Policy Server:

- Tại Policies / Connection Request Policies , thực hiện *Disable* chính sách **Microsoft Routing and Remote Access Service Policy**.



- Chuyển sang máy trạm BKAP-WRK08-01, thực hiện download CA về máy.

- Vào IE , truy cập địa chỉ **123.1.1.1/certsrv**.
 - Tại cửa sổ **Windows Security** , nhập vào user **administrator**, password **123456a@**.



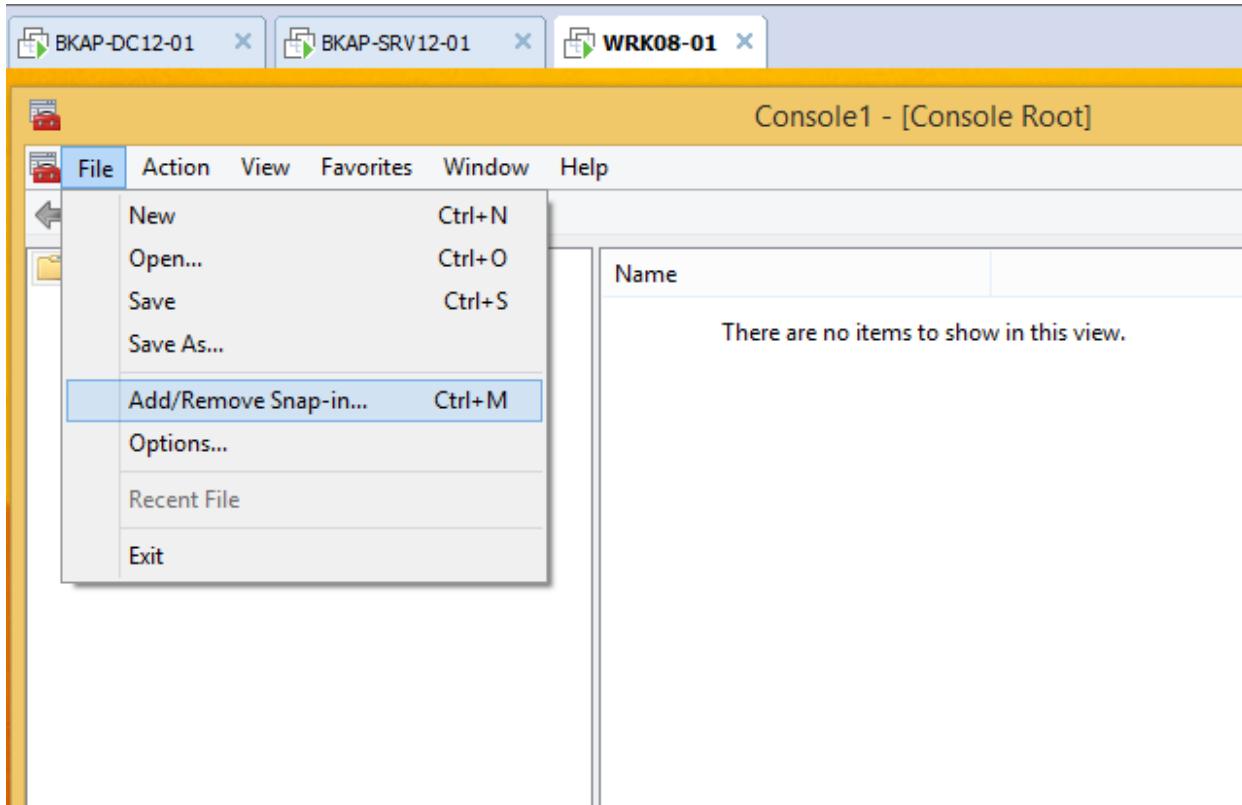
- Thực hiện **download CA** về máy Client.

The screenshot shows the Microsoft Active Directory Certificate Services interface. At the top, there are three tabs: BKAP-DC12-01, BKAP-SRV12-01, and WRK08-01. Below the tabs, the address bar shows the URL <http://123.1.1.1/certsrv/certcarr.asp>. The main content area has a teal header bar with the text "Microsoft Active Directory Certificate Services – BKAP-CA". Below this, a section titled "Download a CA Certificate, Certificate Chain, or CRL" contains instructions: "To trust certificates issued from this certification authority, install this CA certificate chain." and "To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method." A "CA certificate:" section shows a list with "Current [BKAP-CA]" selected. An "Encoding method:" section shows radio buttons for "DER" (selected) and "Base 64". Below these are four download links: "Download CA certificate", "Download CA certificate chain", "Download latest base CRL", and "Download latest delta CRL".

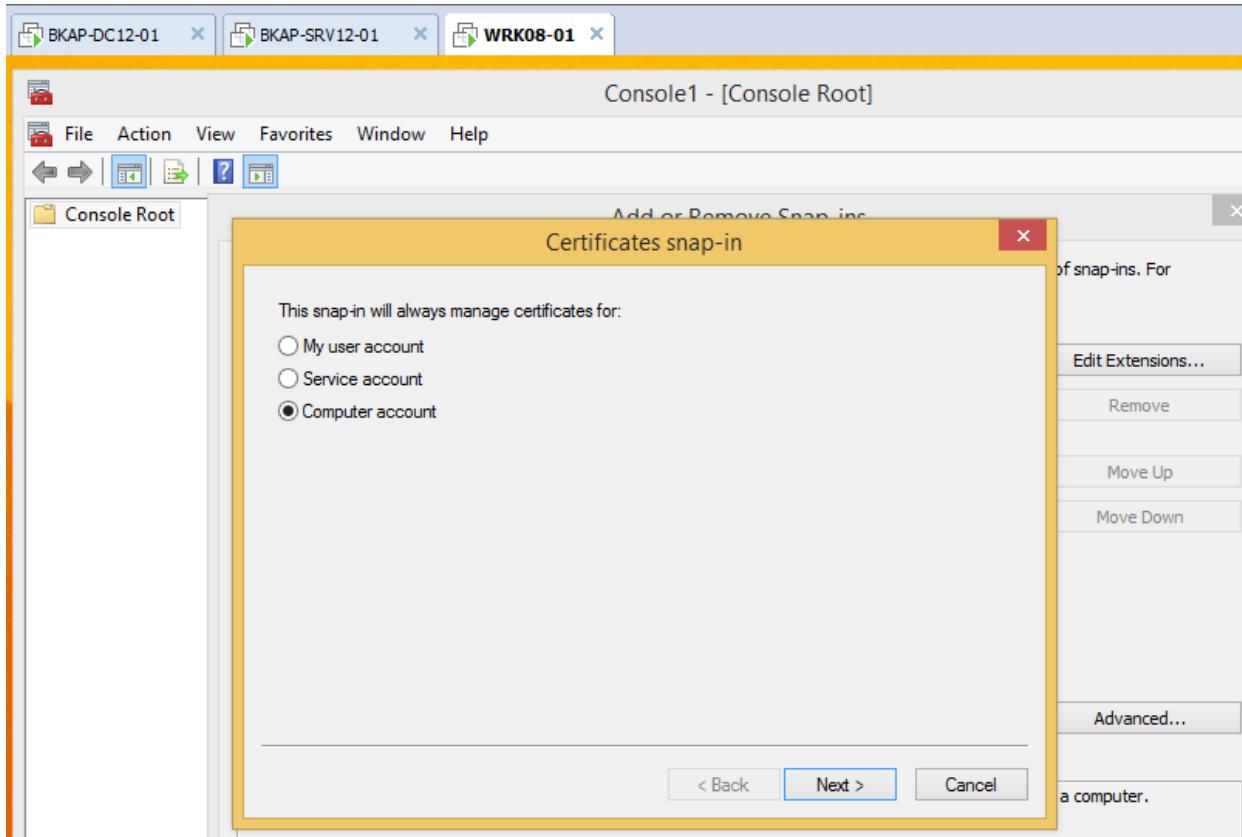
The screenshot shows a Windows File Explorer window titled "Downloads". The address bar shows "This PC > Downloads". The left sidebar shows "Favorites" with "Desktop" and "Downloads" selected. The main pane displays a list of files in the "Downloads" folder:

Name	Date modified	Type	Size
certnew	2/25/2016 12:19 AM	Security Certificate	1 KB
certnew	2/25/2016 12:19 AM	PKCS #7 Certificates	1 KB

- Thực hiện **Trust CA** cho máy trạm và tiến hành cấu hình **NAP VPN Client**.
 - Run / mmc
 - File / Add or Remove Snap-in

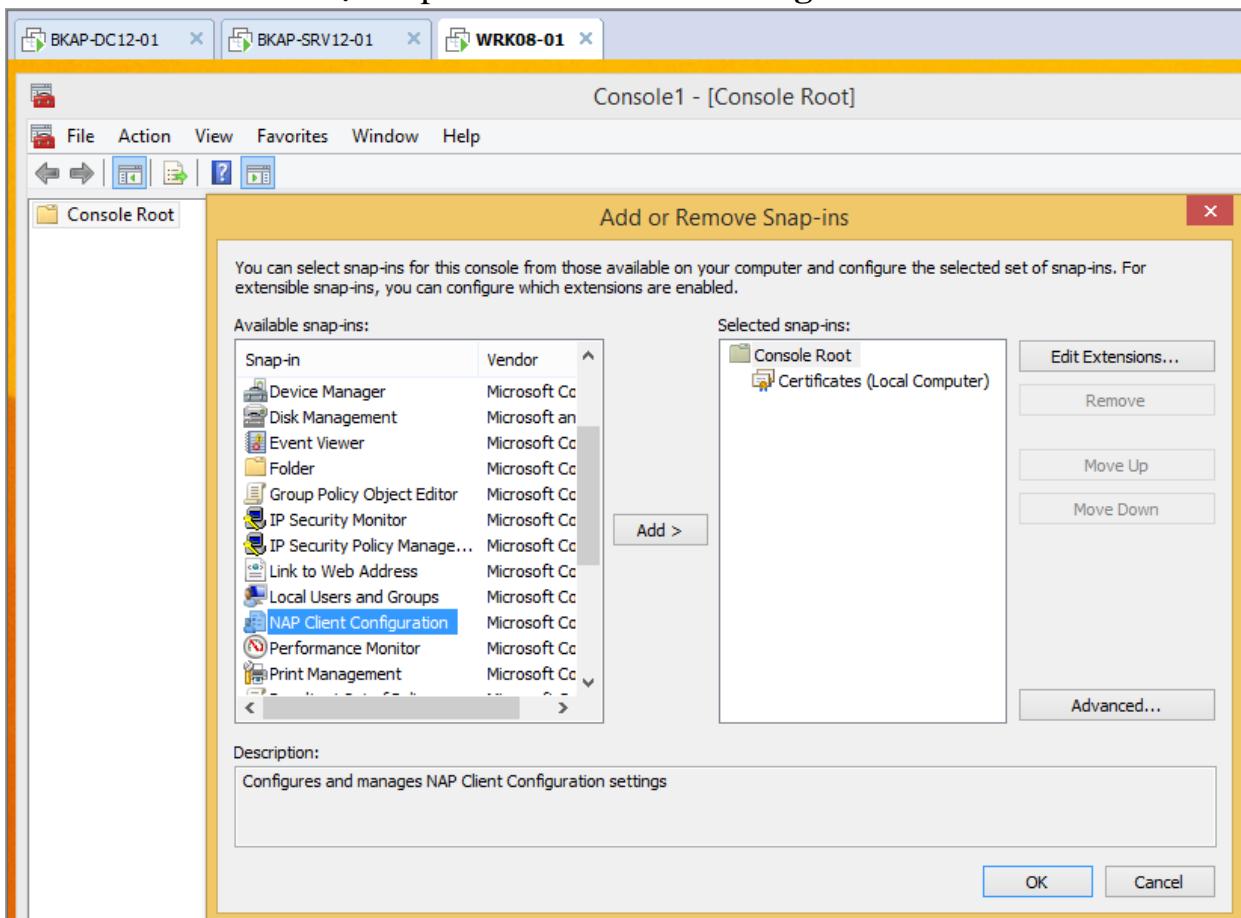


- Tại cửa sổ **Add or Remove Snap-ins** , chọn **Certificates => Add**
 - Tại cửa sổ **Certificates snap-in** , chọn vào **Computer account => Next.**

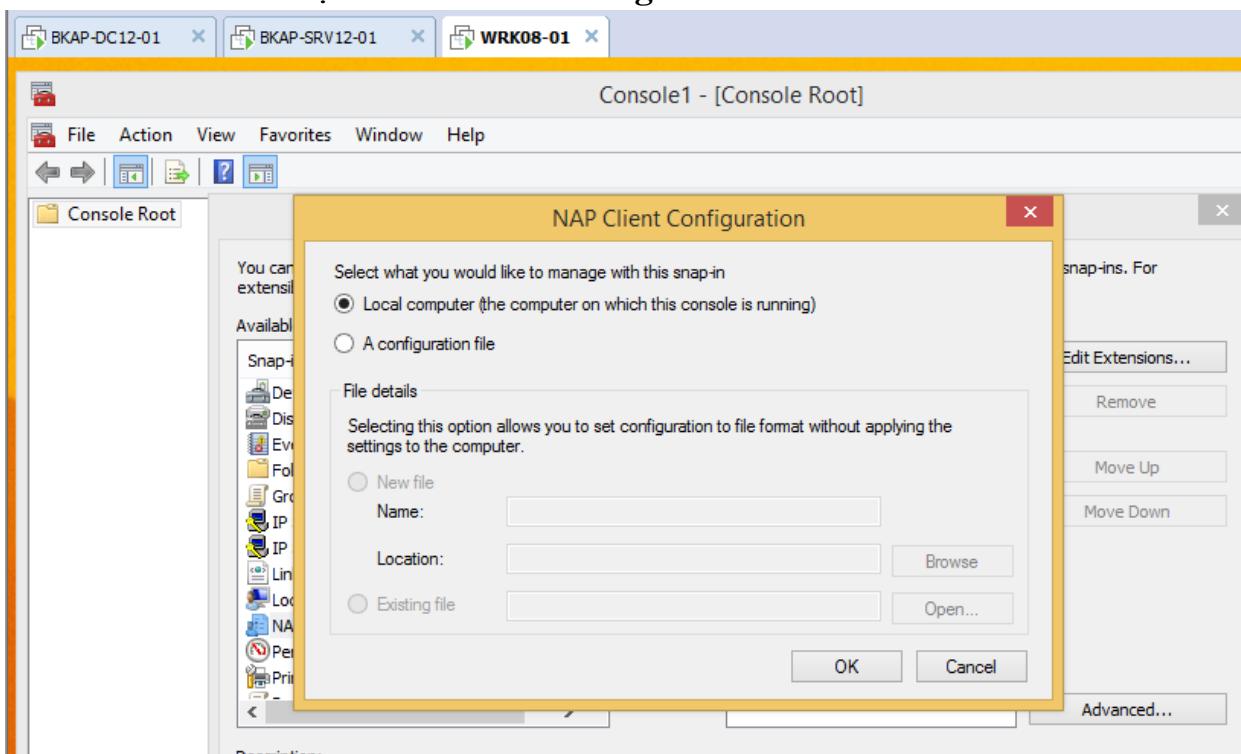


- => **Finish.**

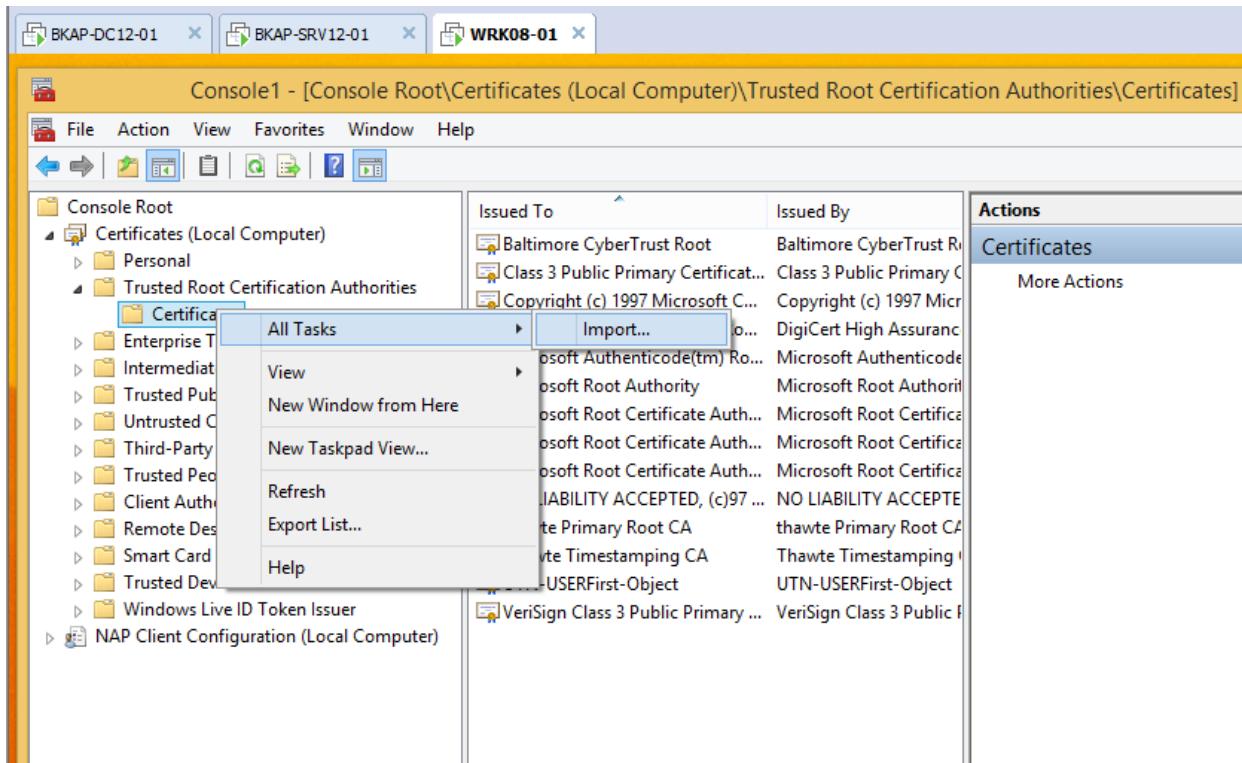
▪ Chọn tiếp vào NAP Client Configuration => Add.

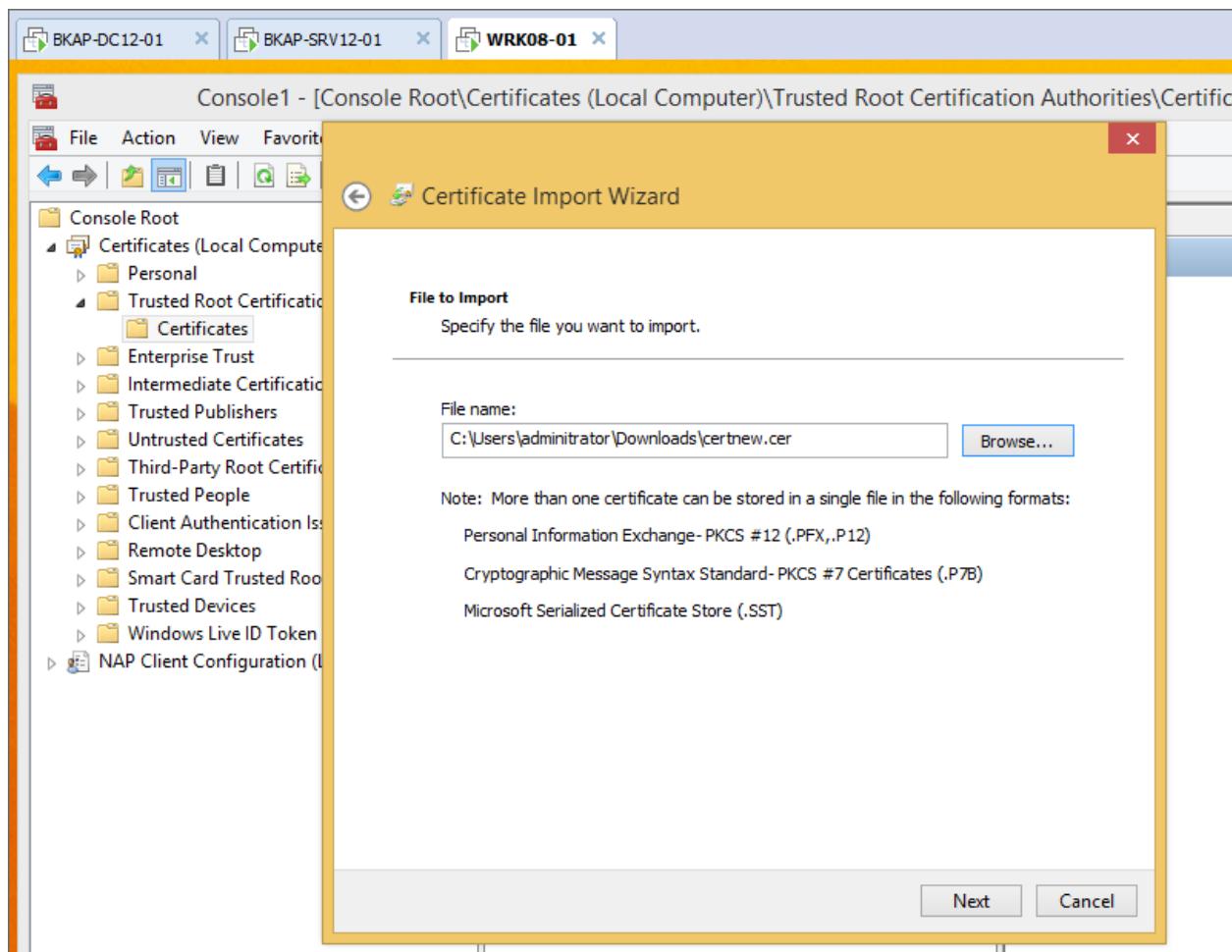


- Tại NAP Client Configuration => OK. => Finish.

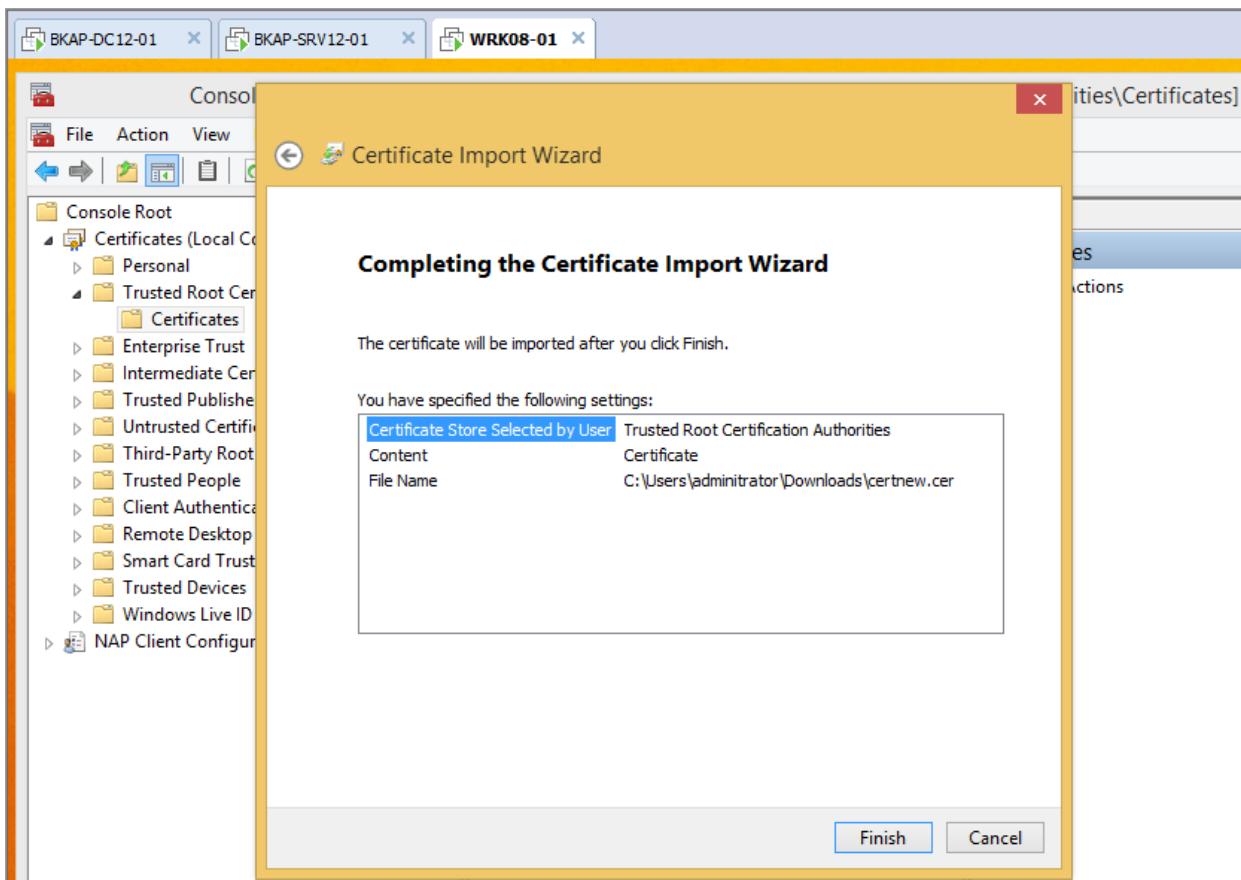


- Tại cửa sổ **Console1** ... chọn vào **Trust Root Certification Authorities / Certificates** / click chuột phải tại đây chọn **All Tasks => Import...**
 - **Browse** đến CA vừa download.

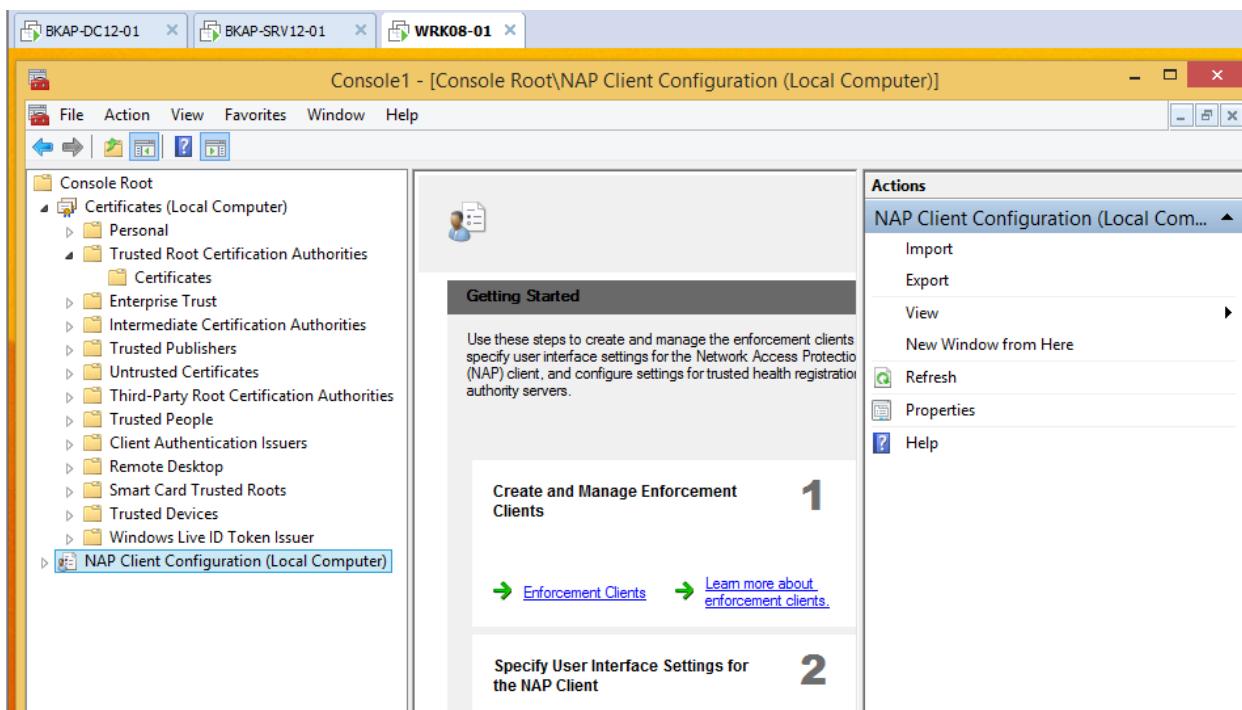




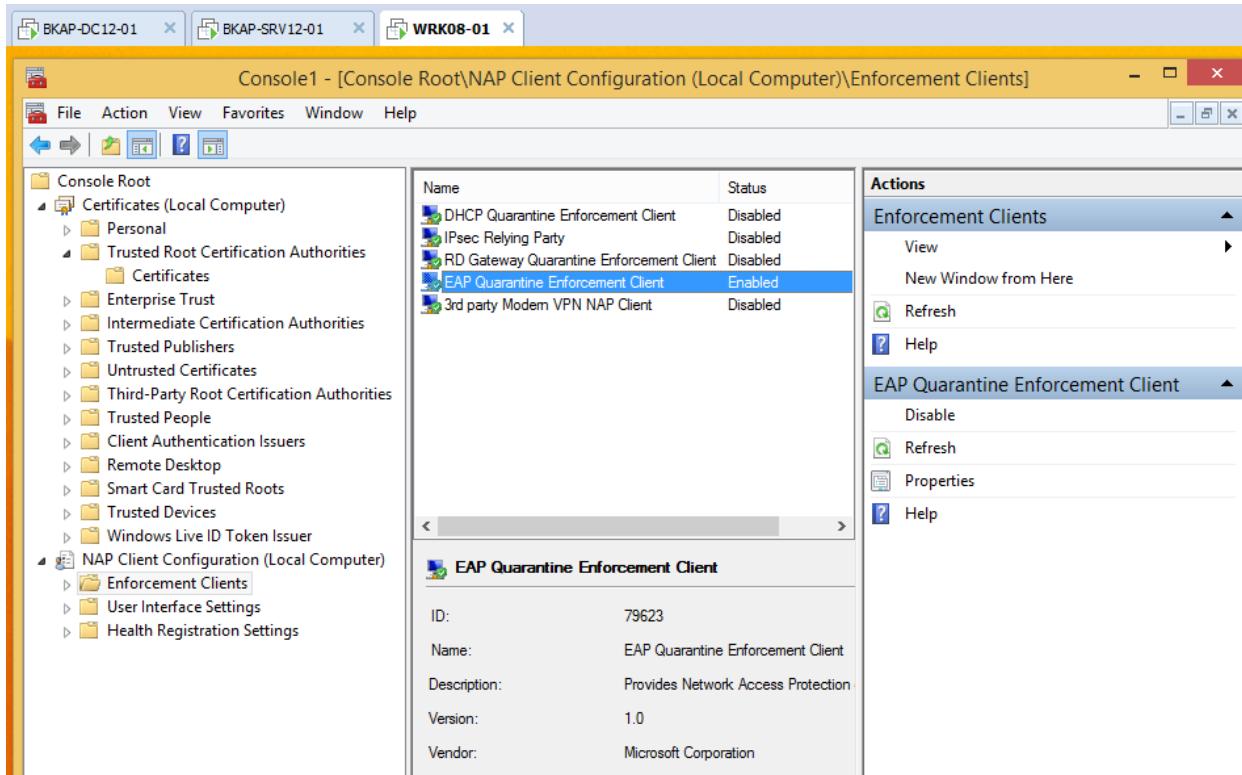
- Click vào Next => Finish.



- Click vào **NAP Client Configuration (Local Computer)**, click vào **Enforcement Clients**.

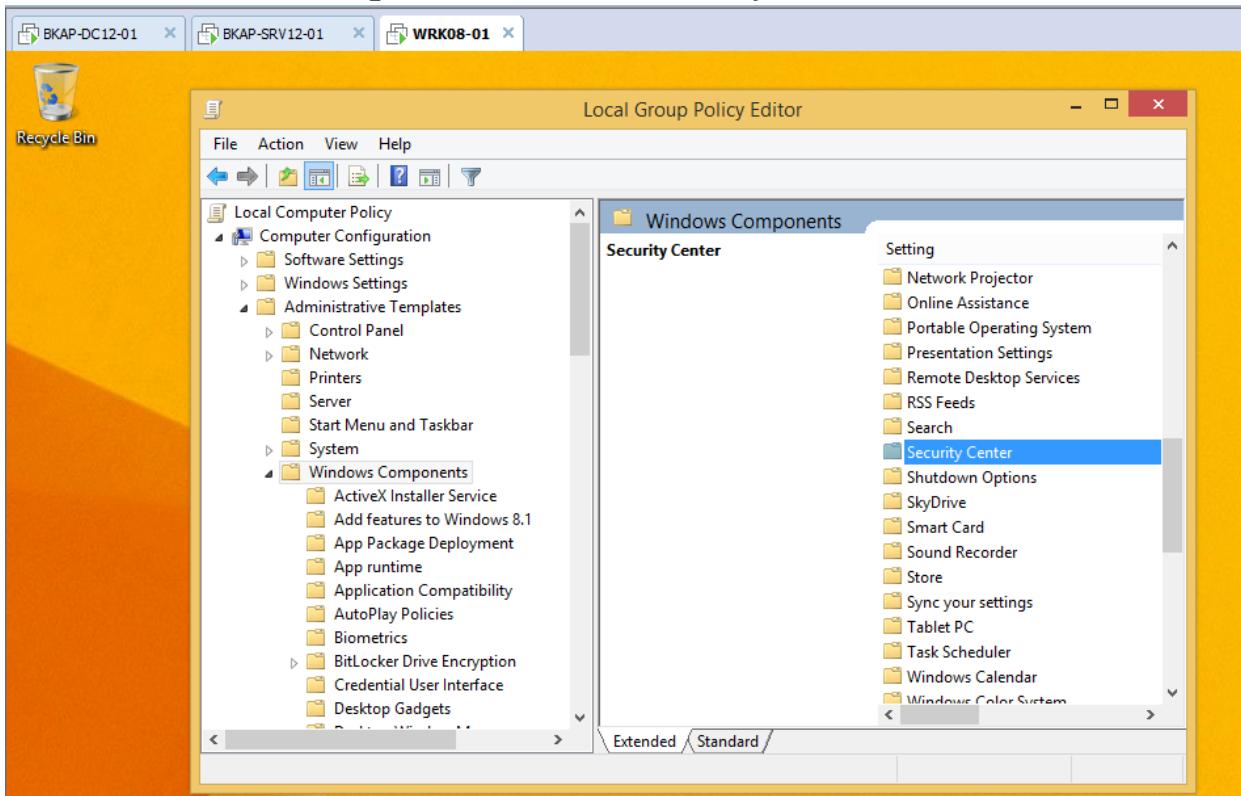


- Chọn vào **EAP Quarantine Enforcement Client => Enable.**

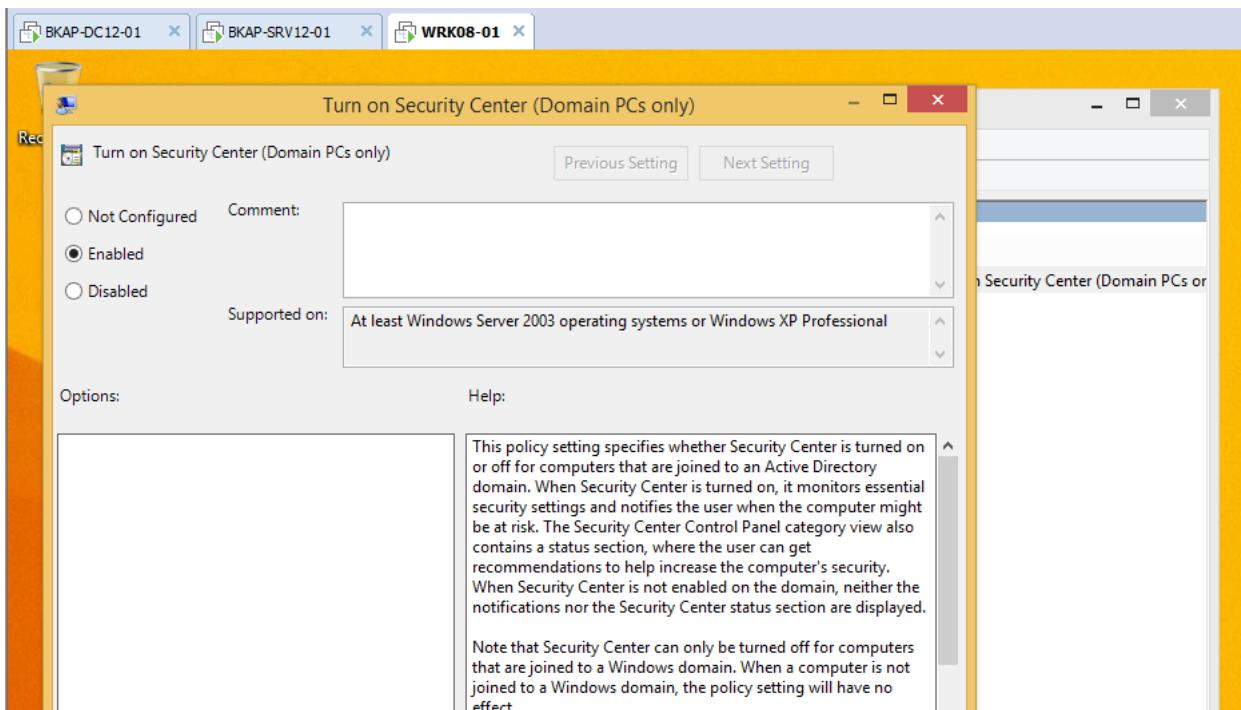


- Run / gpedit.msc

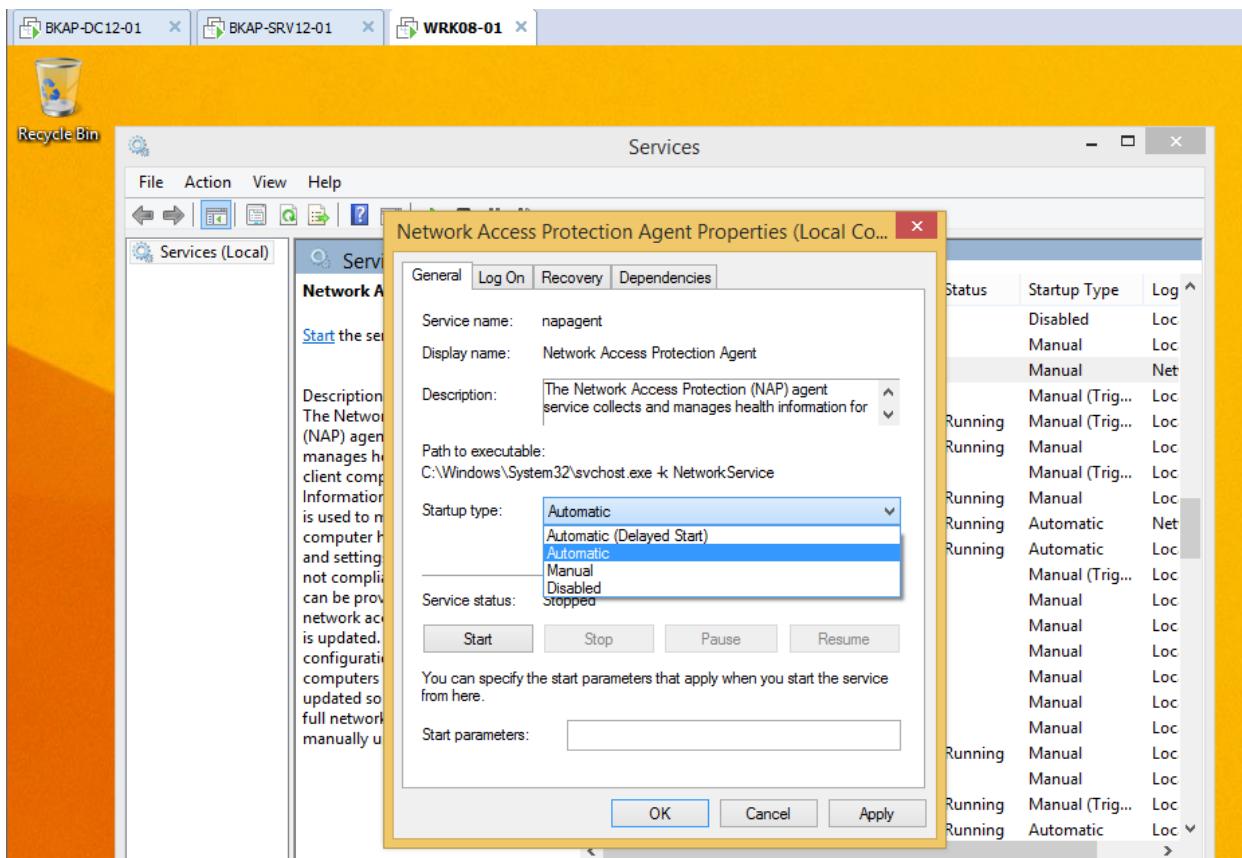
- Tại cửa sổ Local Group Policy Editor , chọn vào Computer Configuration / Administrative Templates / Windows Components => chọn Security Center.



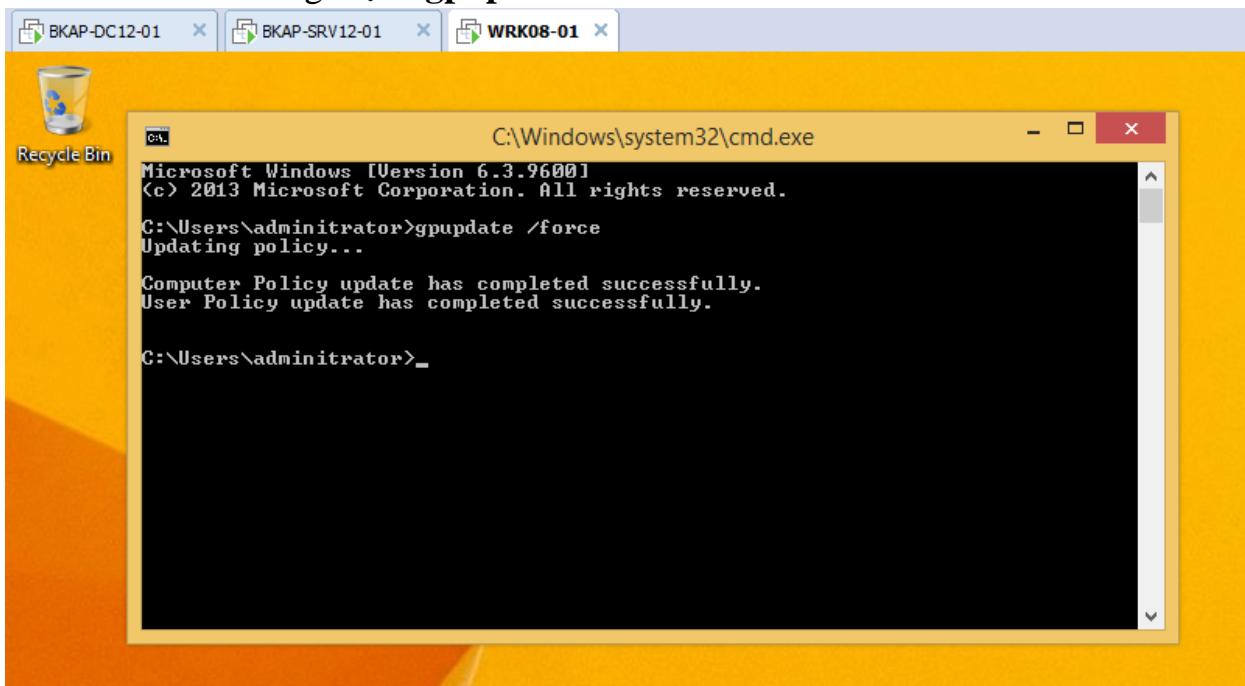
- Click vào Turn on Security Center (Domain PCs only) => Enable.



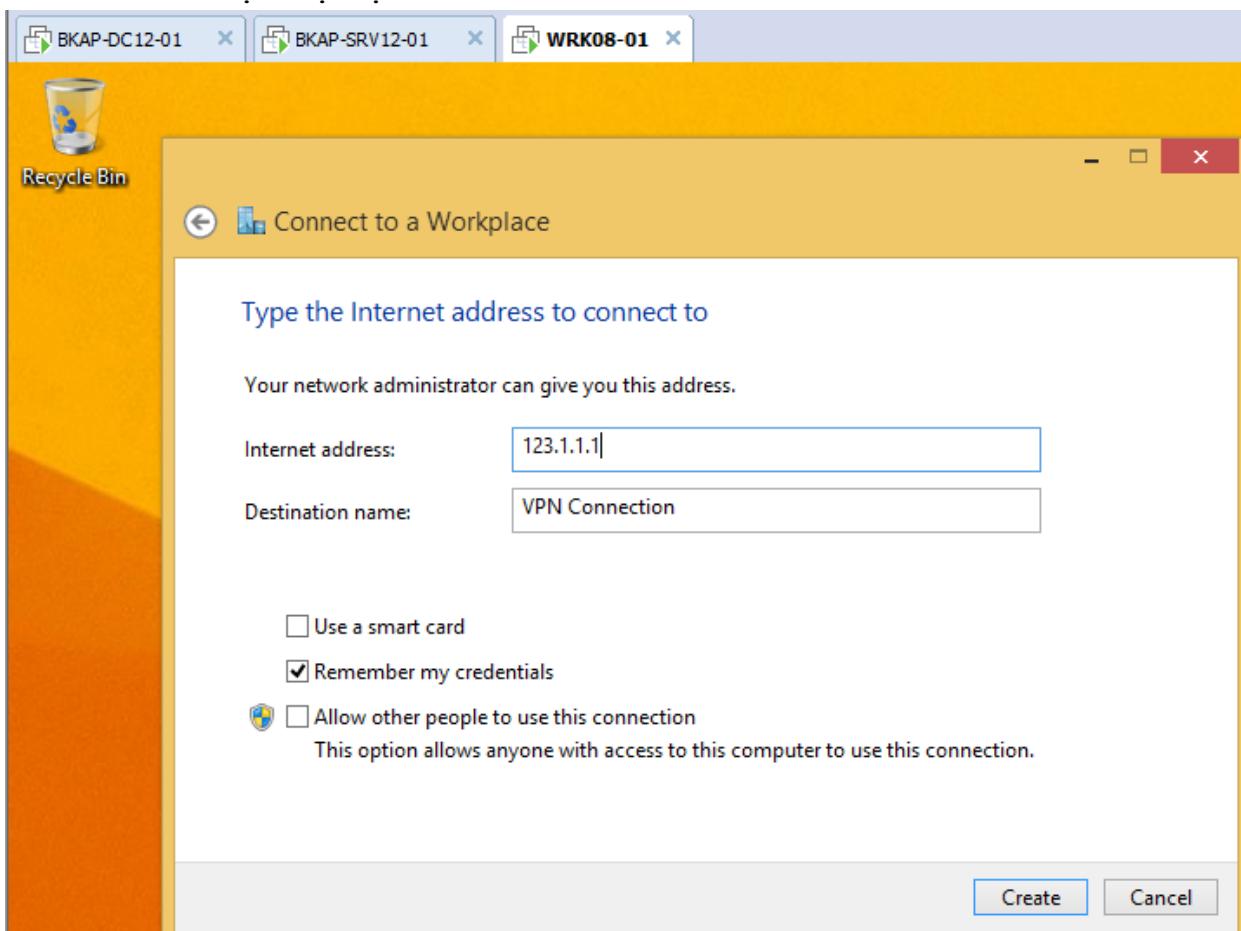
- Run / services.msc
 - Chọn vào Network Access Protection Agent / Properties
 - Tại startup type : Automatic
 - Click vào Start.



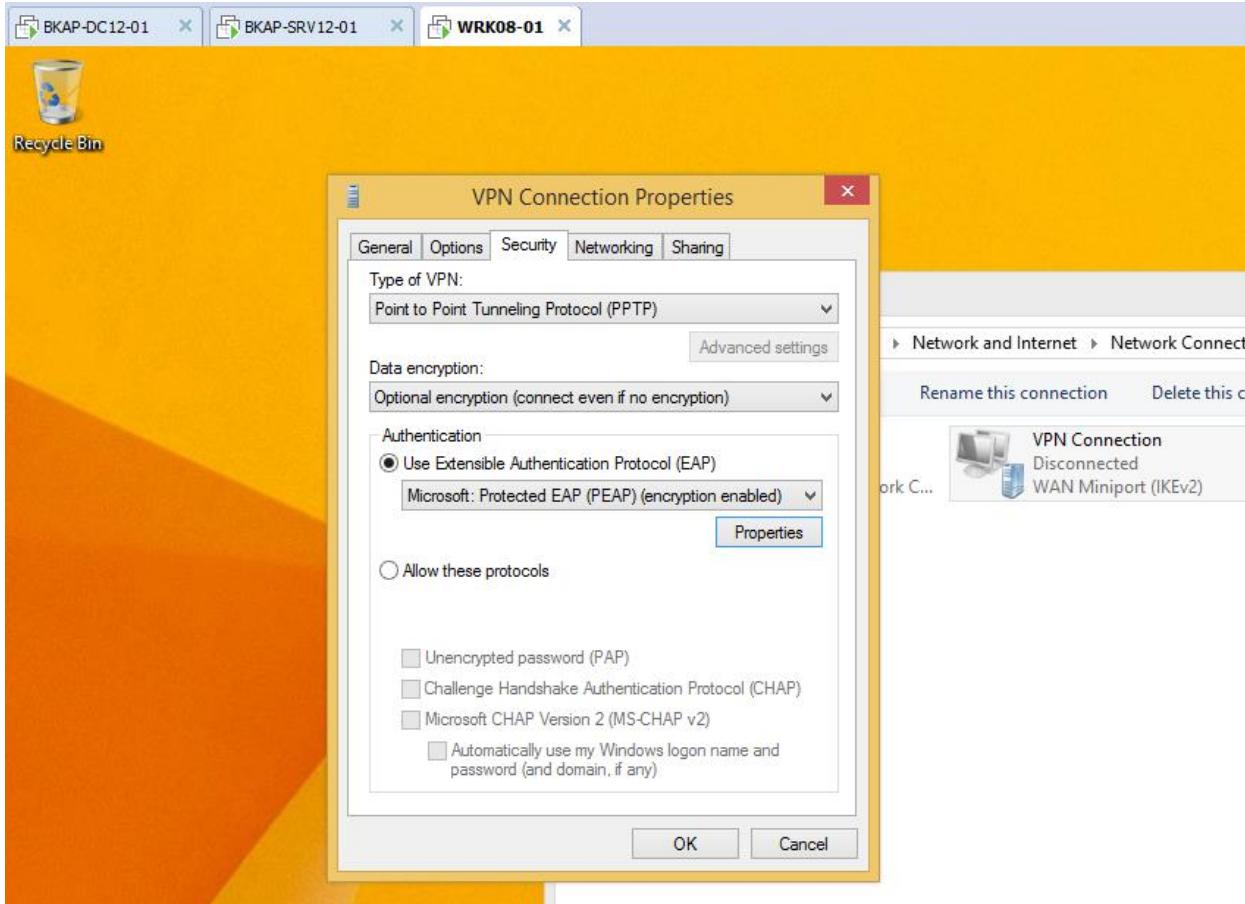
o Cmd / gõ lệnh gpupdate /force.



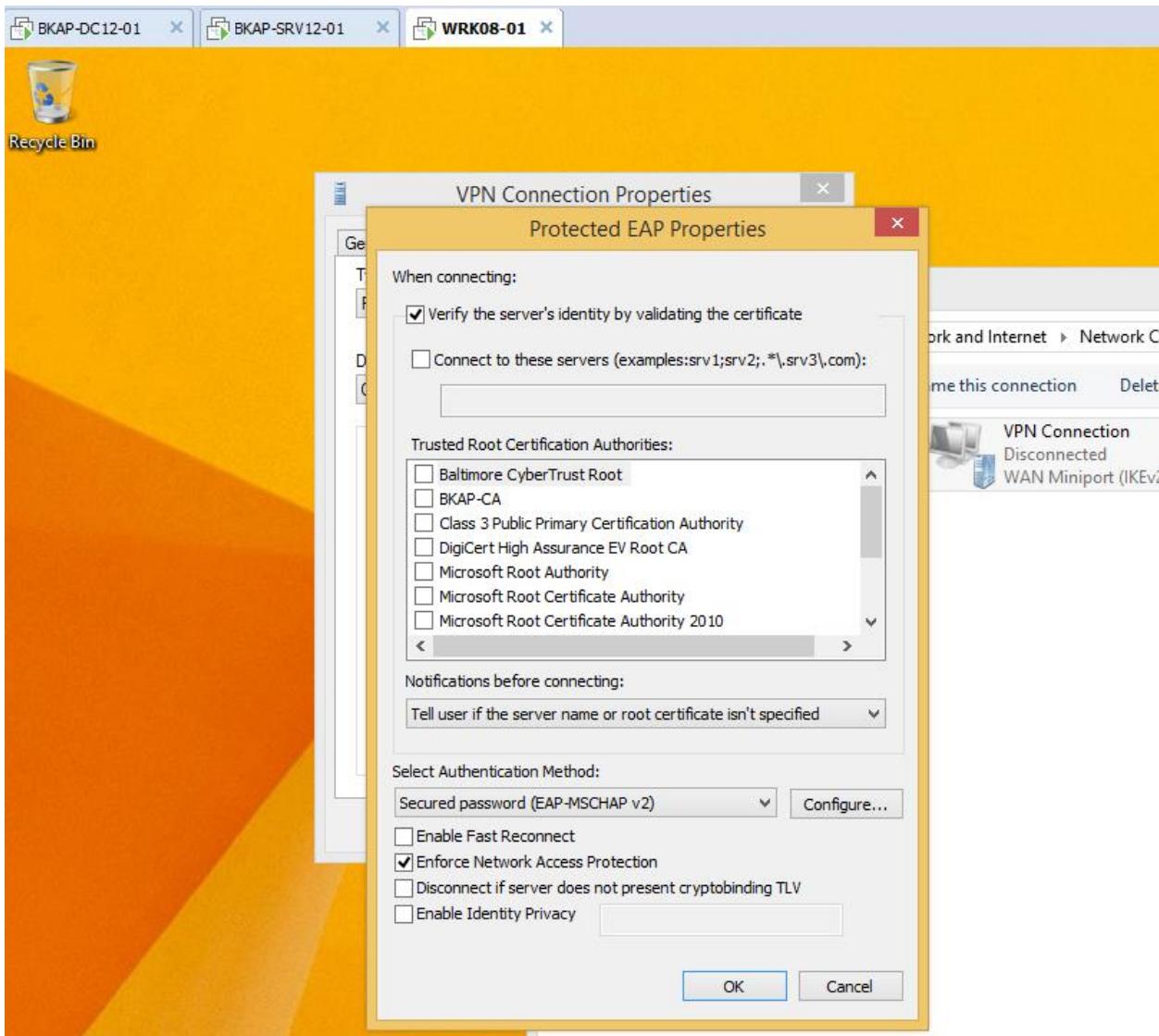
- Thực hiện tạo kết nối VPN.



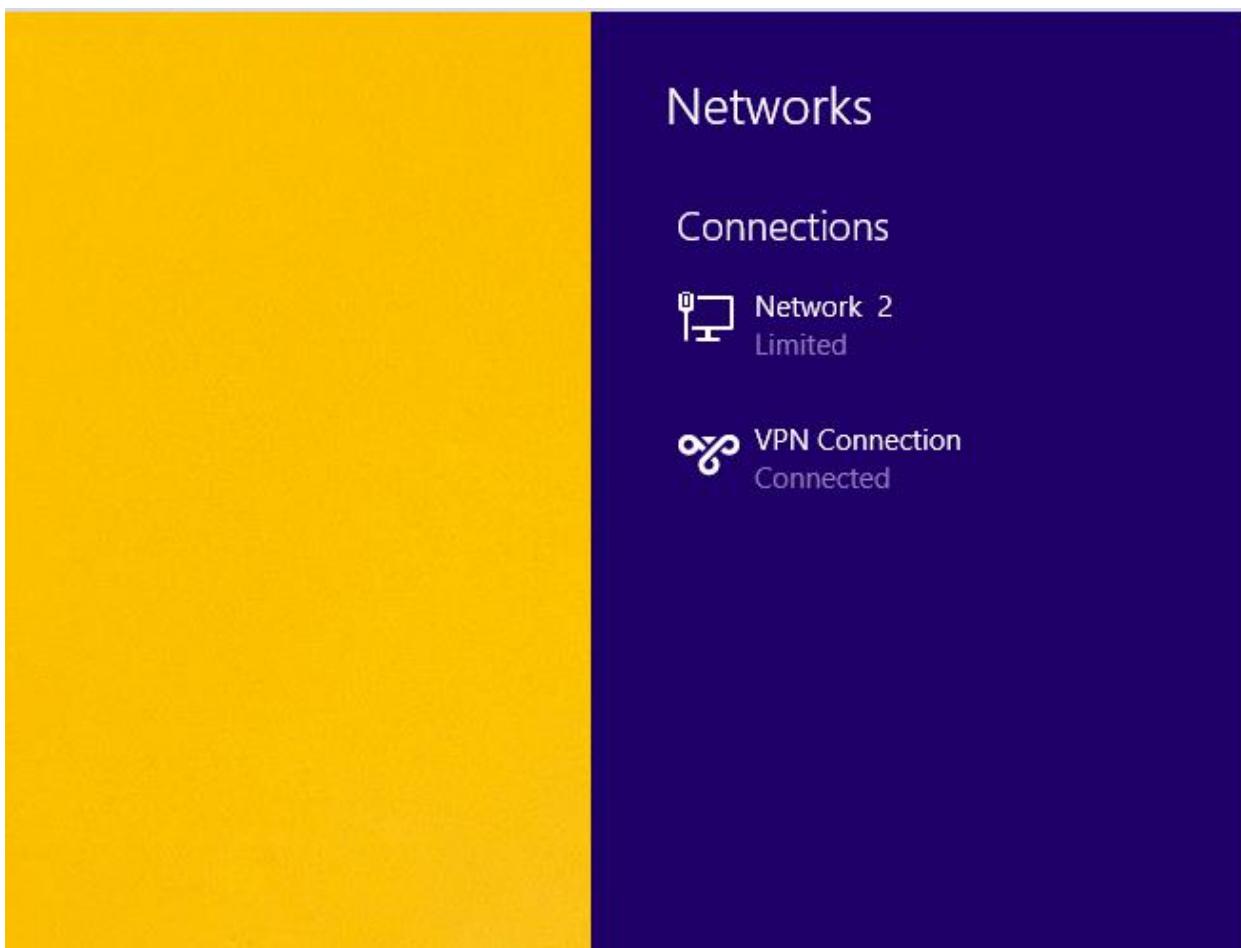
- Tại **VPN Connection Properties** , chuyển sang tab **Security**, chọn giao thức **PPTP**.
 - Tại **Authentication** , chọn vào **Use Extensible Authentication Protocol (EAP)**.
 - ⇒ Bên dưới chọn vào **Microsoft: Protected EAP (PEAP) (encryption enable)**



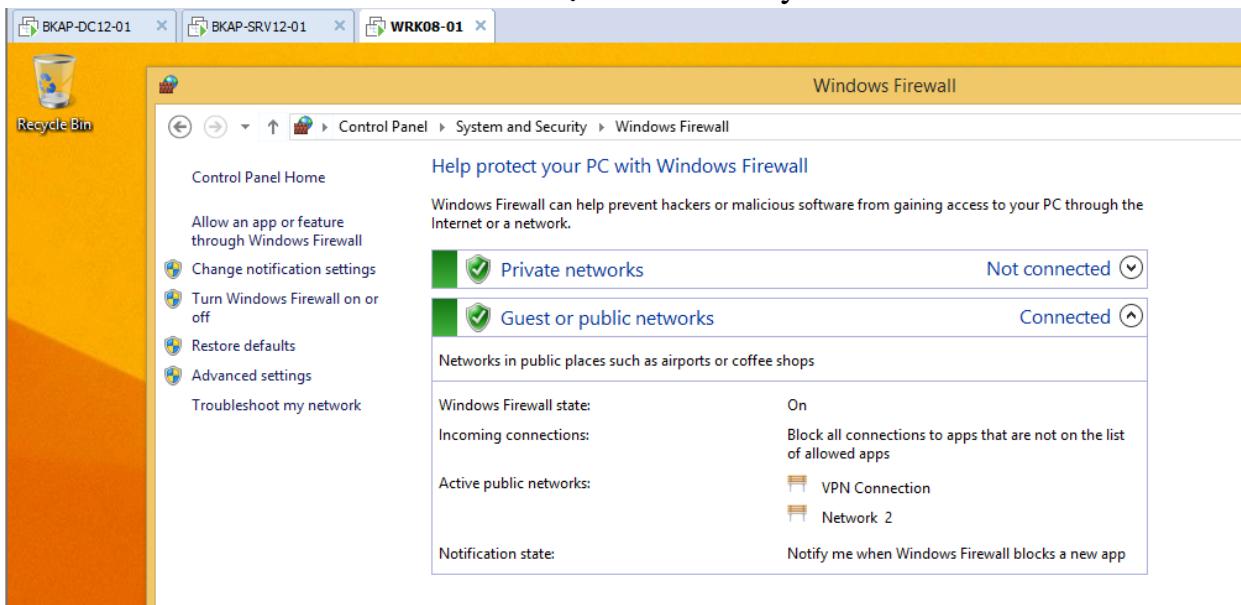
- Chọn tiếp vào **Properties**, bỏ chọn tại **Connect to these servers** và **Enable Fast Reconnect**, click chọn vào **Enforce Network Access Protection**



- Kết nối VPN.



- Kiểm tra Firewall đã được mở trên máy Client.



Bài 10:

TRIỂN KHAI DỊCH VỤ FILE SERVICES

Các nội dung chính sẽ được đề cập:

- ✓ Cấu hình Quota , File Screening và tạo thông kê lưu trữ.
- ✓ Triển khai cài đặt và cấu hình dịch vụ DFS.
- ✓ Đồng bộ dữ liệu trên 2 Server sử dụng DFS Replication.

10.1 Cấu hình Quota, File Screening và Tạo thông kê lưu trữ.

1. Yêu cầu bài Lab:

+ Trên Server *BKAP-SRV12-01*:

- Thực hiện cài đặt **FSRM** (*File Server Resource Manager*).
- Tạo **Quota Template** giới hạn **100 Mb** và thiết lập **Quota** cho người dùng.
- Vào **File Screening Management** cấu hình giới hạn người dùng lưu trữ các dạng file: *exe* , *audio* , *video*.
- Tạo 1 báo cáo mới và thiết lập báo cáo theo lịch biểu.

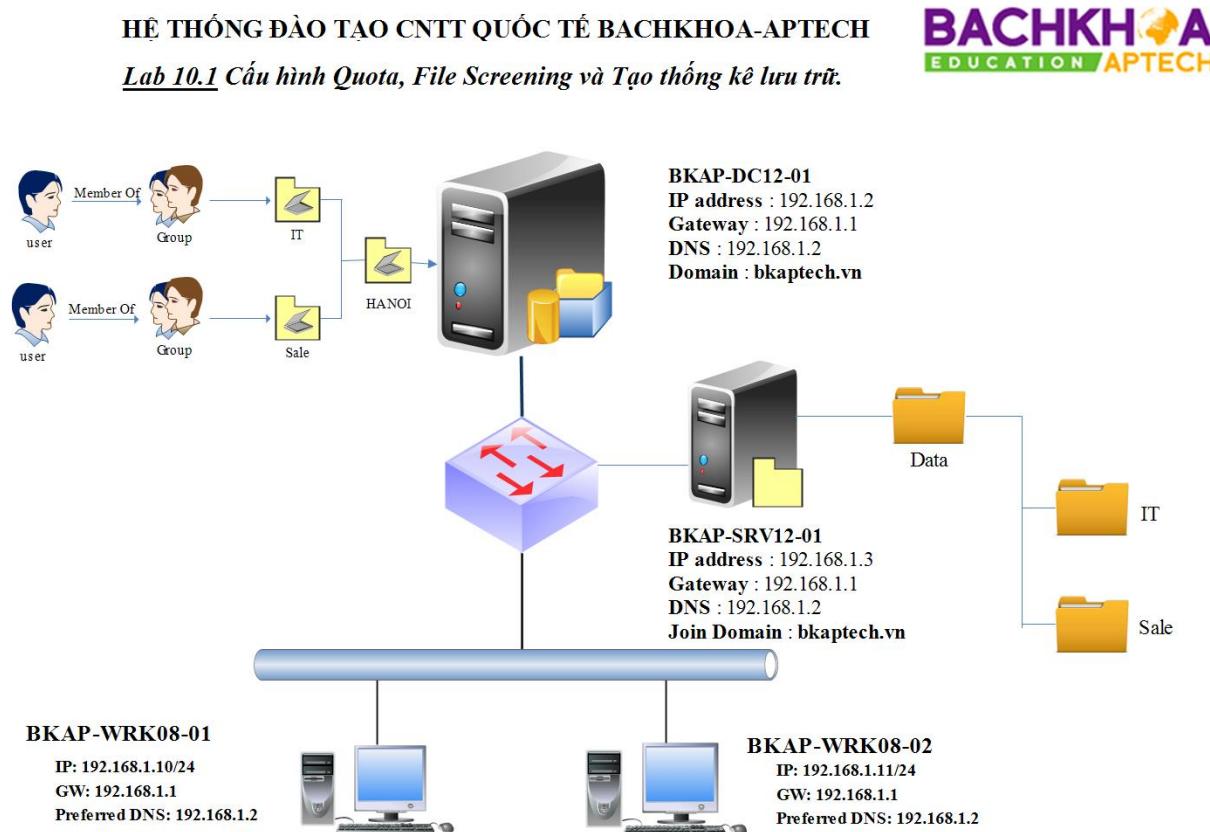
+ Kiểm tra sau khi cấu hình:

- Trên máy *BKAP-WRK08-01*:
 - Copy thử 1 file lớn hơn **100 Mb** vào thư mục lưu trữ.
 - Đăng nhập vào bằng 1 User trong miền và chép 1 file *audio* để kiểm tra.

2. Yêu cầu chuẩn bị:

- + Máy Server *BKAP-DC12-01* nâng cấp lên **Domain Controller** quản lý miền **bkaptech.vn** và cài đặt **DNS Server**.
- + Máy Server *BKAP-SRV12-01* cài đặt **FSRM** và **Join Domain**.
- + Máy Client *BKAP-WRK08-01* Join vào Domain.

3. Mô hình Lab:



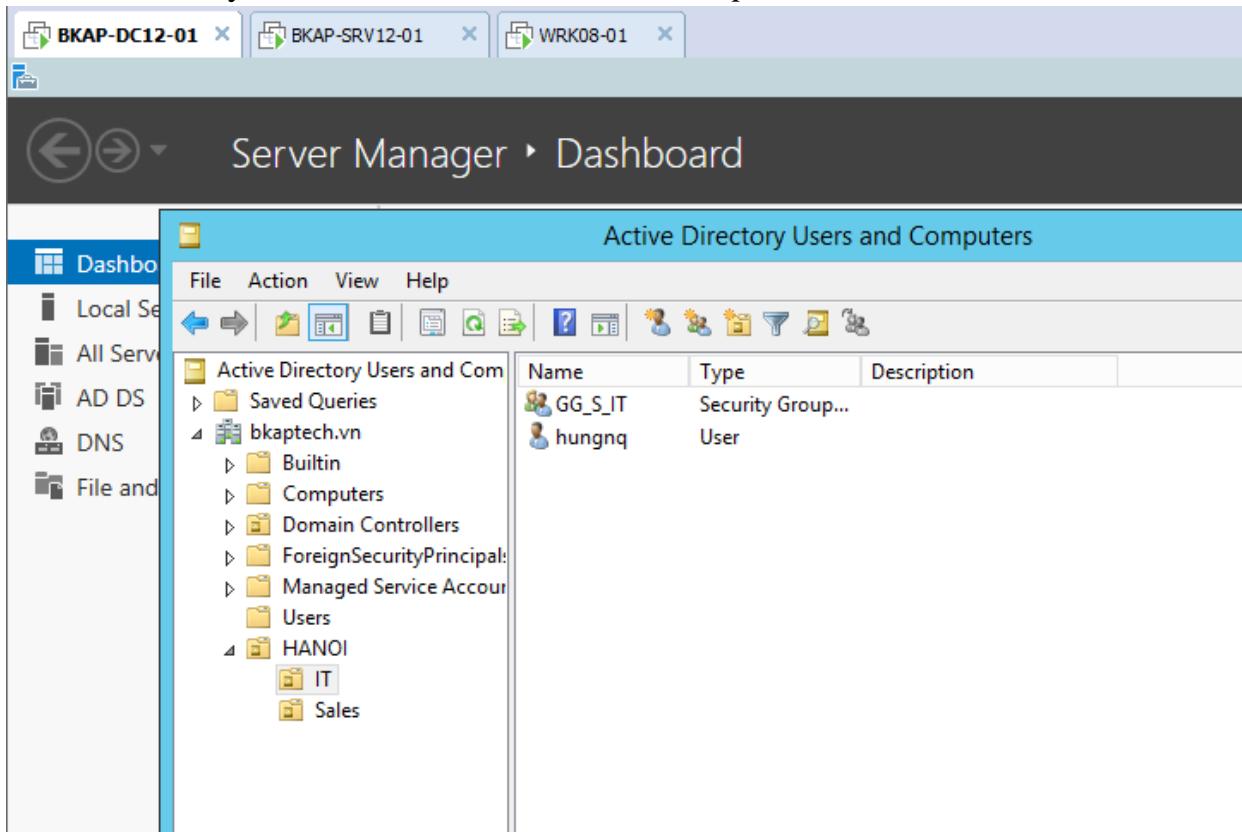
Hình 10.1

Sơ đồ địa chỉ như sau:

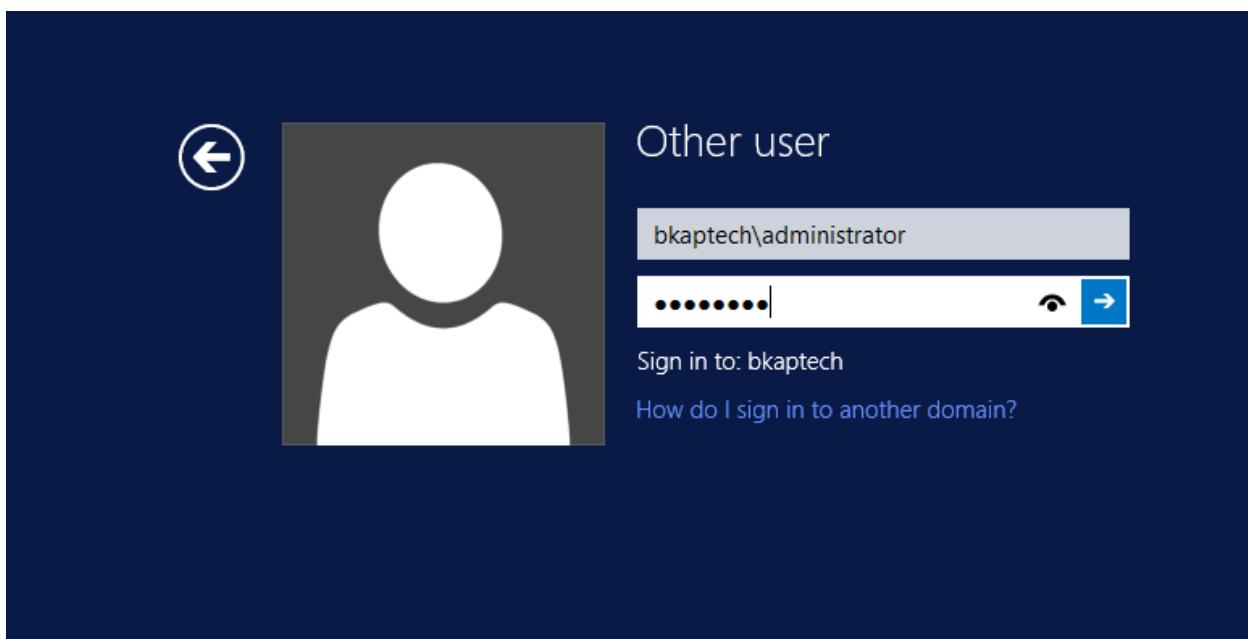
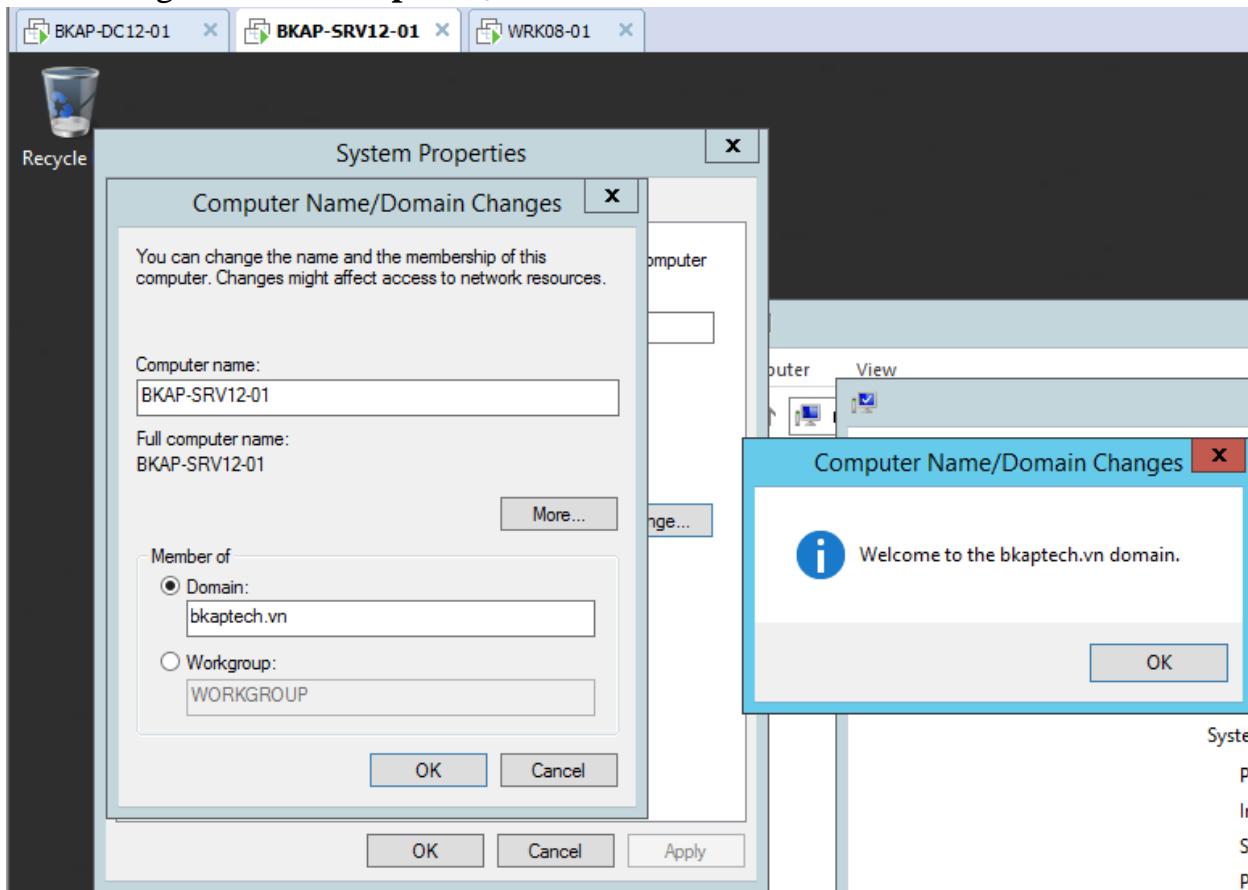
Thông số	BKAP-DC12-01	BKAP-SRV12-01	BKAP-WRK08-01
IP address	192.168.1.2	192.168.1.3	192.168.1.10
Gateway	192.168.1.1	192.168.1.1	192.168.1.1
Subnet Mask	255.255.255.0	255.255.255.0	255.255.255.0
DNS Server	192.168.1.2	192.168.1.2	192.168.1.2

Hướng dẫn chi tiết:

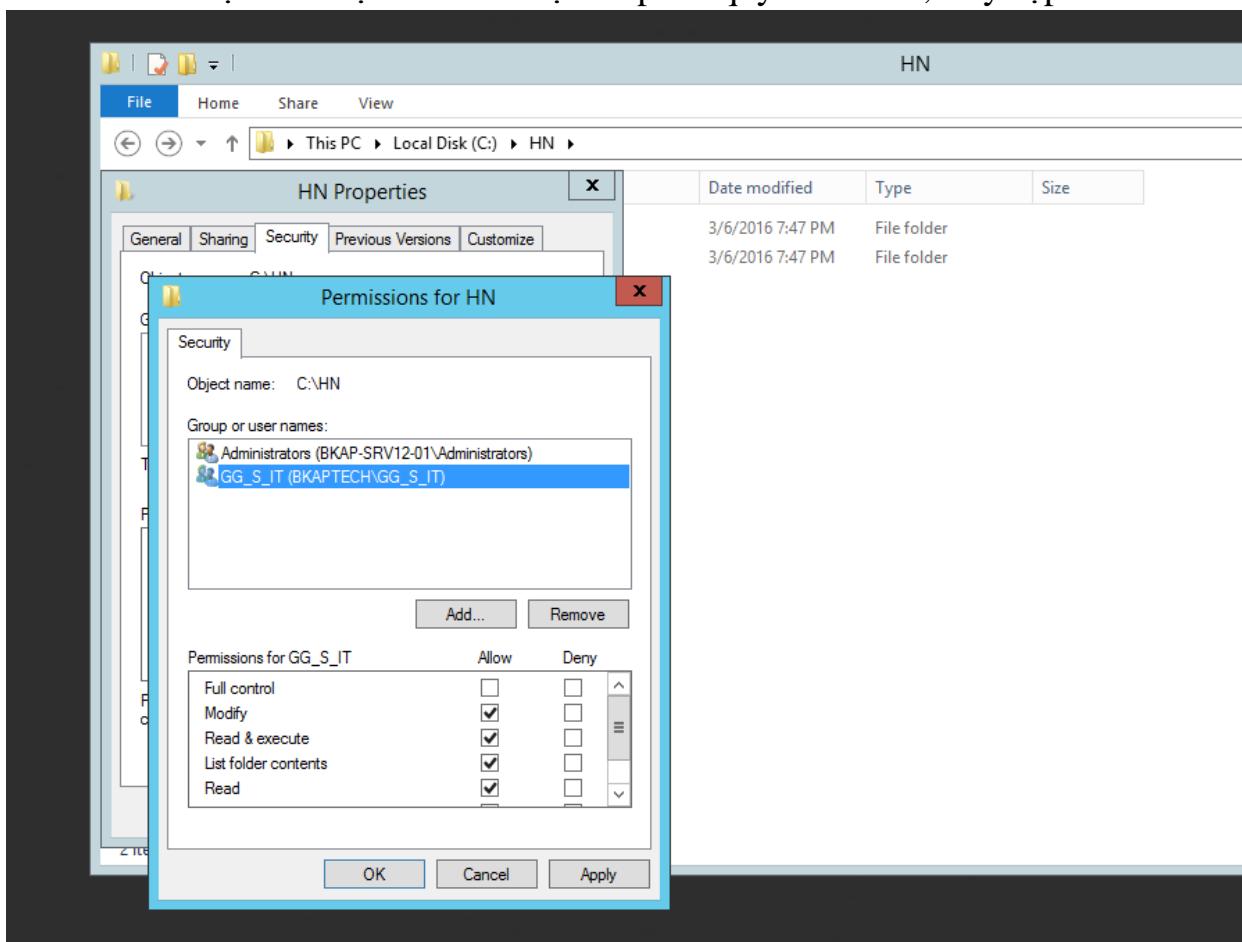
- Trên máy *BKAP-DC12-01*, tạo *OU, Group, User* theo hình trên.



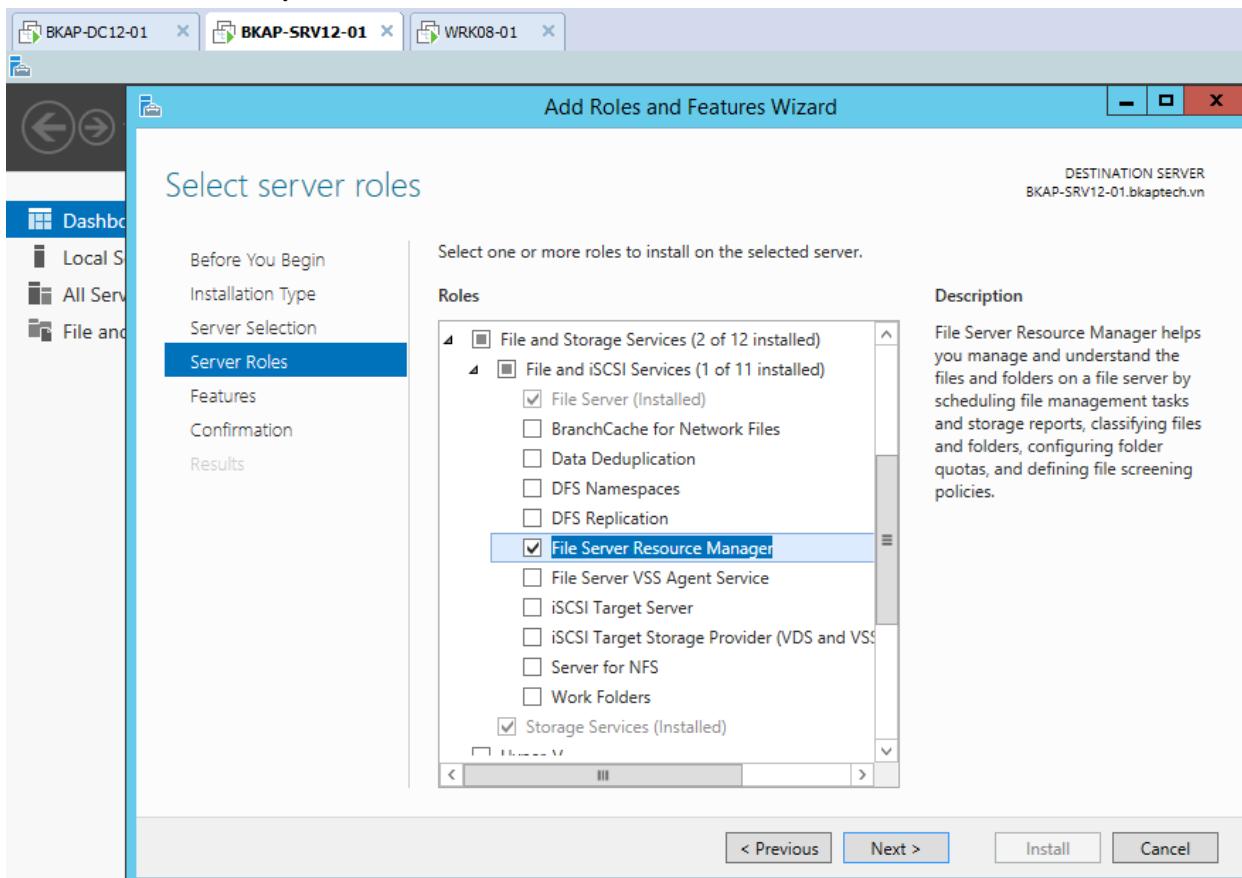
- Chuyển sang máy BKAP-SRV12-01, tiến hành Join vào Domain , đăng nhập bằng tài khoản **bkaptech\administrator**.



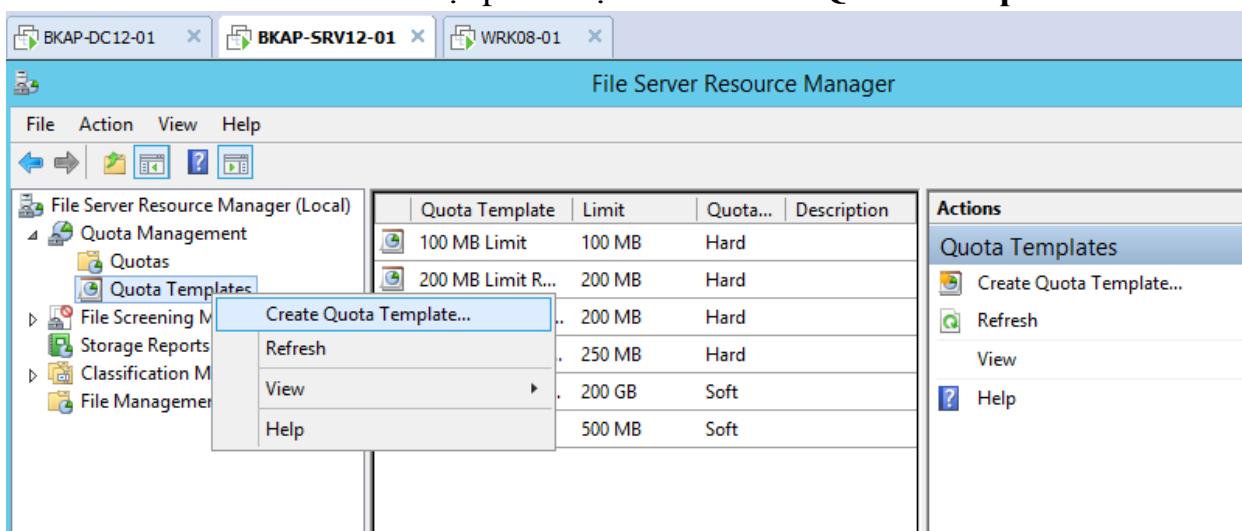
- Tạo thư mục chứa dữ liệu và phân quyền chia sẻ, truy cập.



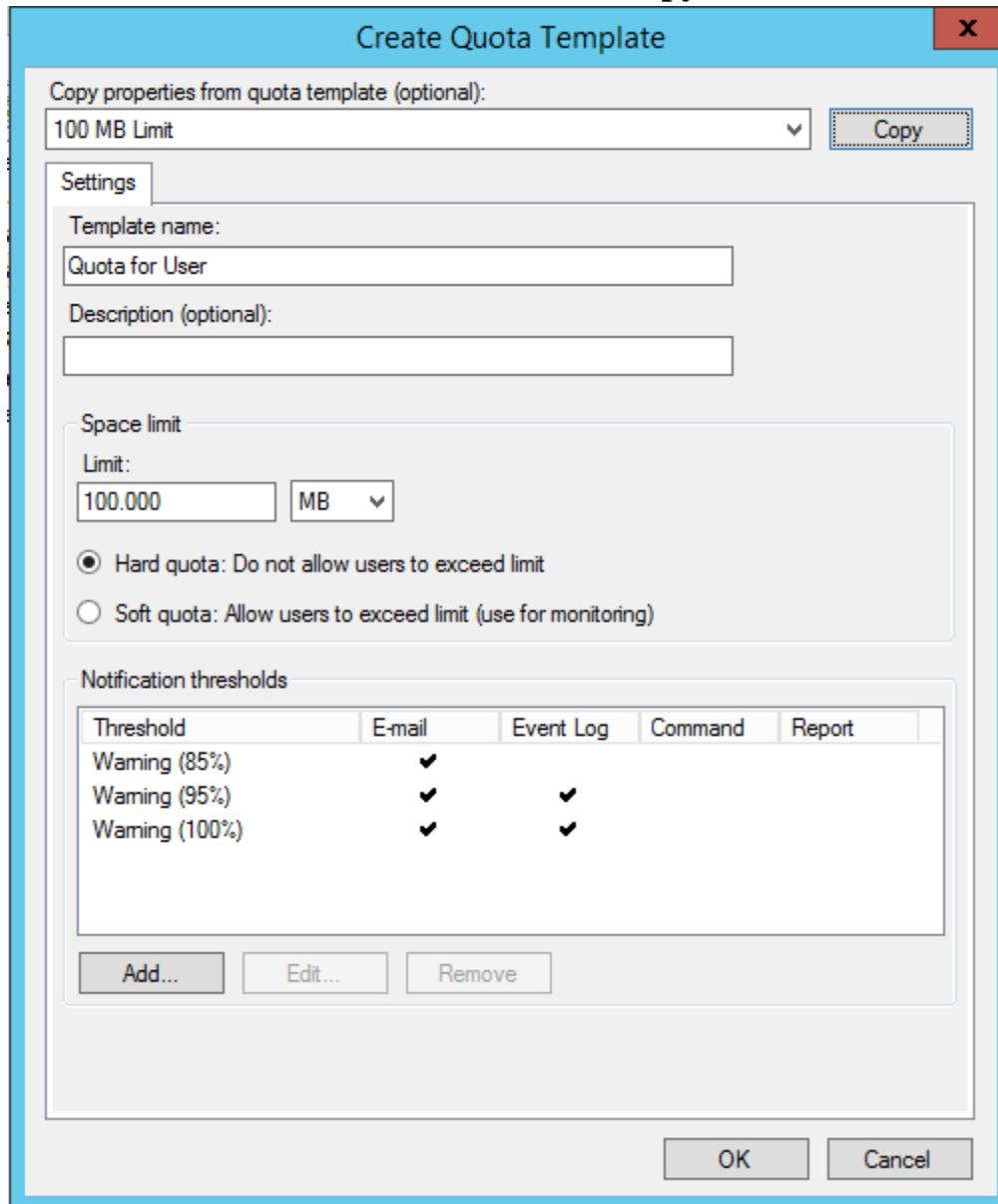
- Cài đặt FSRM.



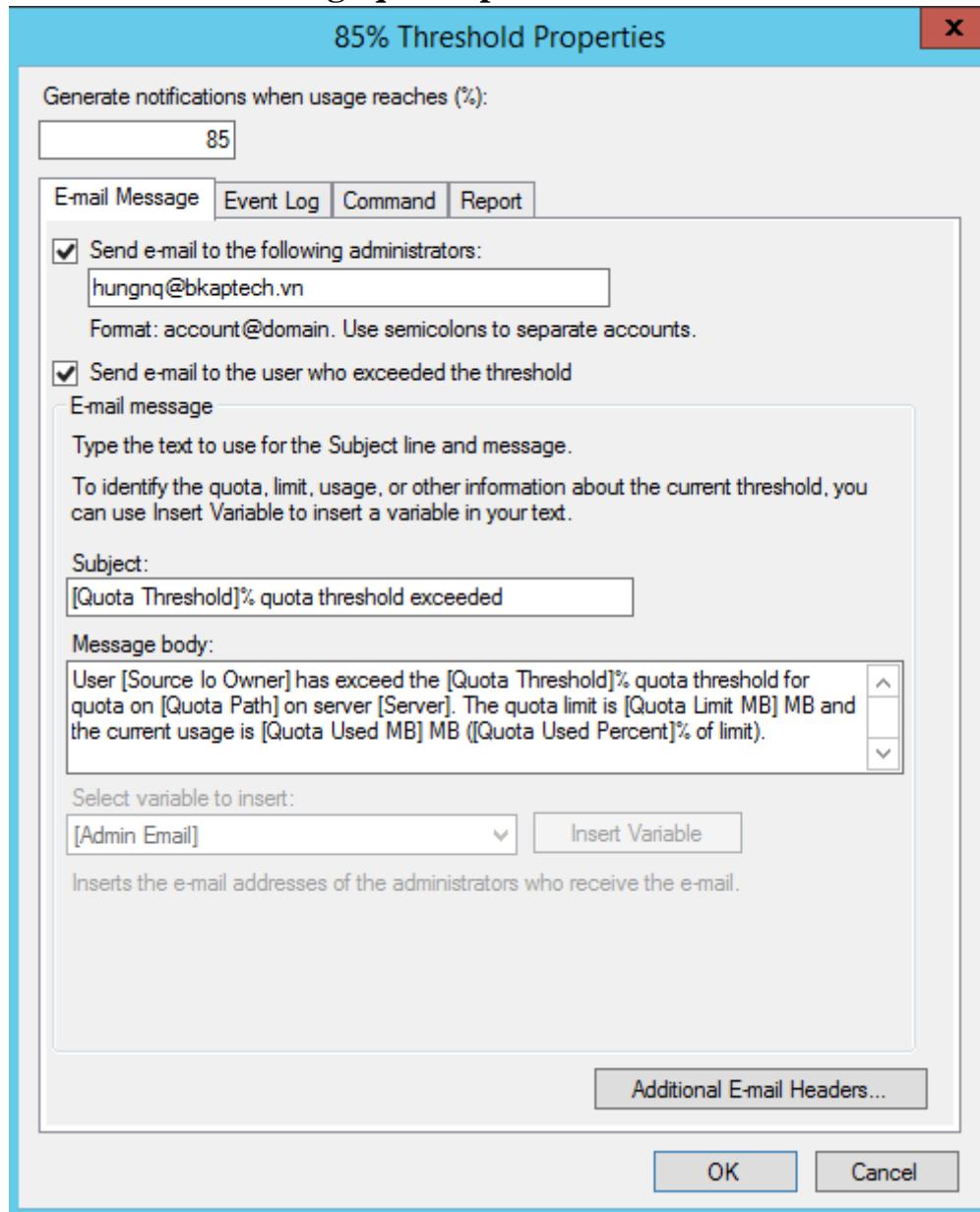
- Cấu hình FSRM : vào dịch vụ **File Server Resource Manager**.
 - Cấu hình Quota.
 - Tại **Quota Management / Quota Templates** , click chuột phải chọn vào **Create Quota Template...**



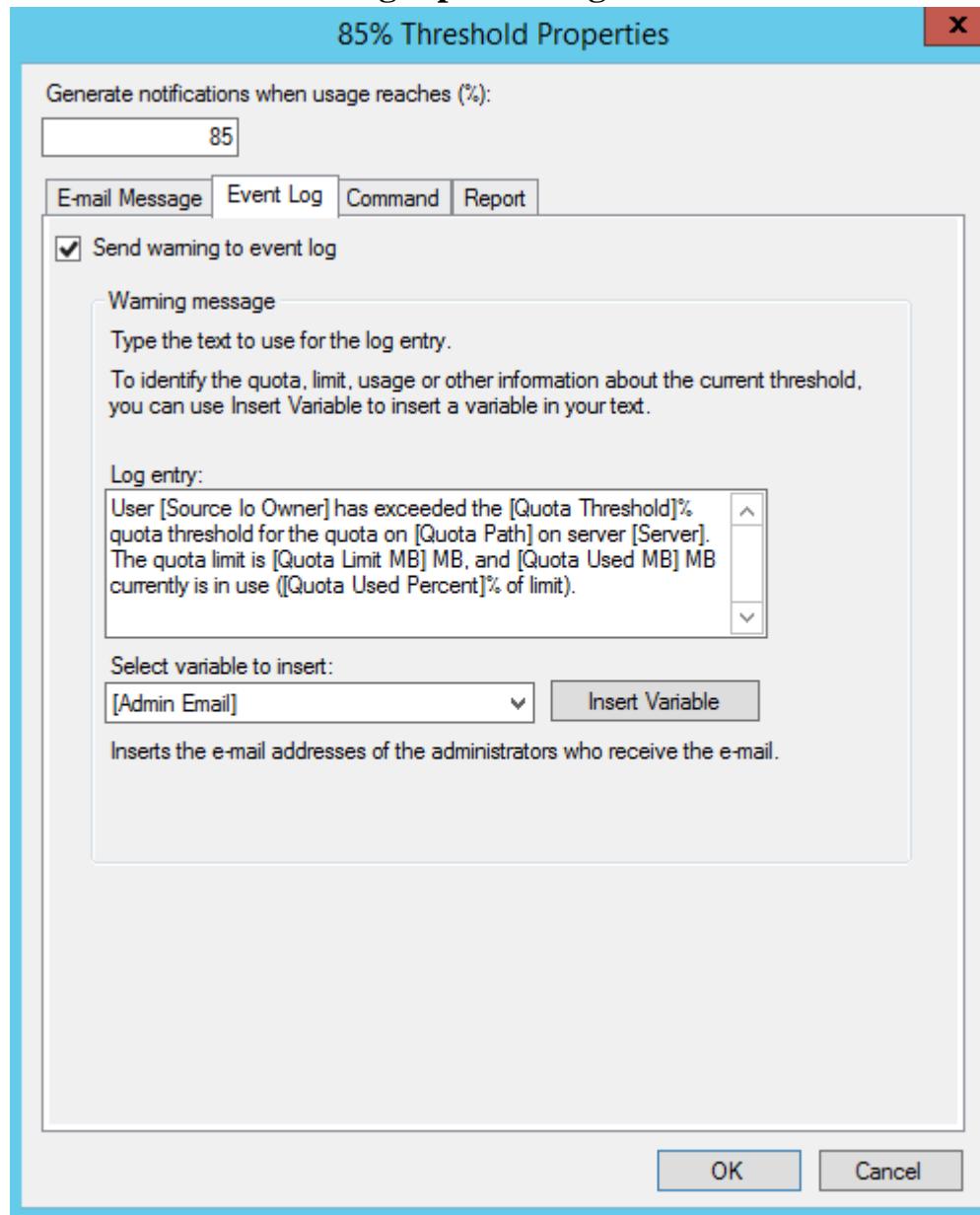
- Trong cửa sổ **Create Quota Template**, nhập vào :
 - Template name : Quota for User.*
 - Description (optional) : Quota.*
 - Click vào **Copy**.



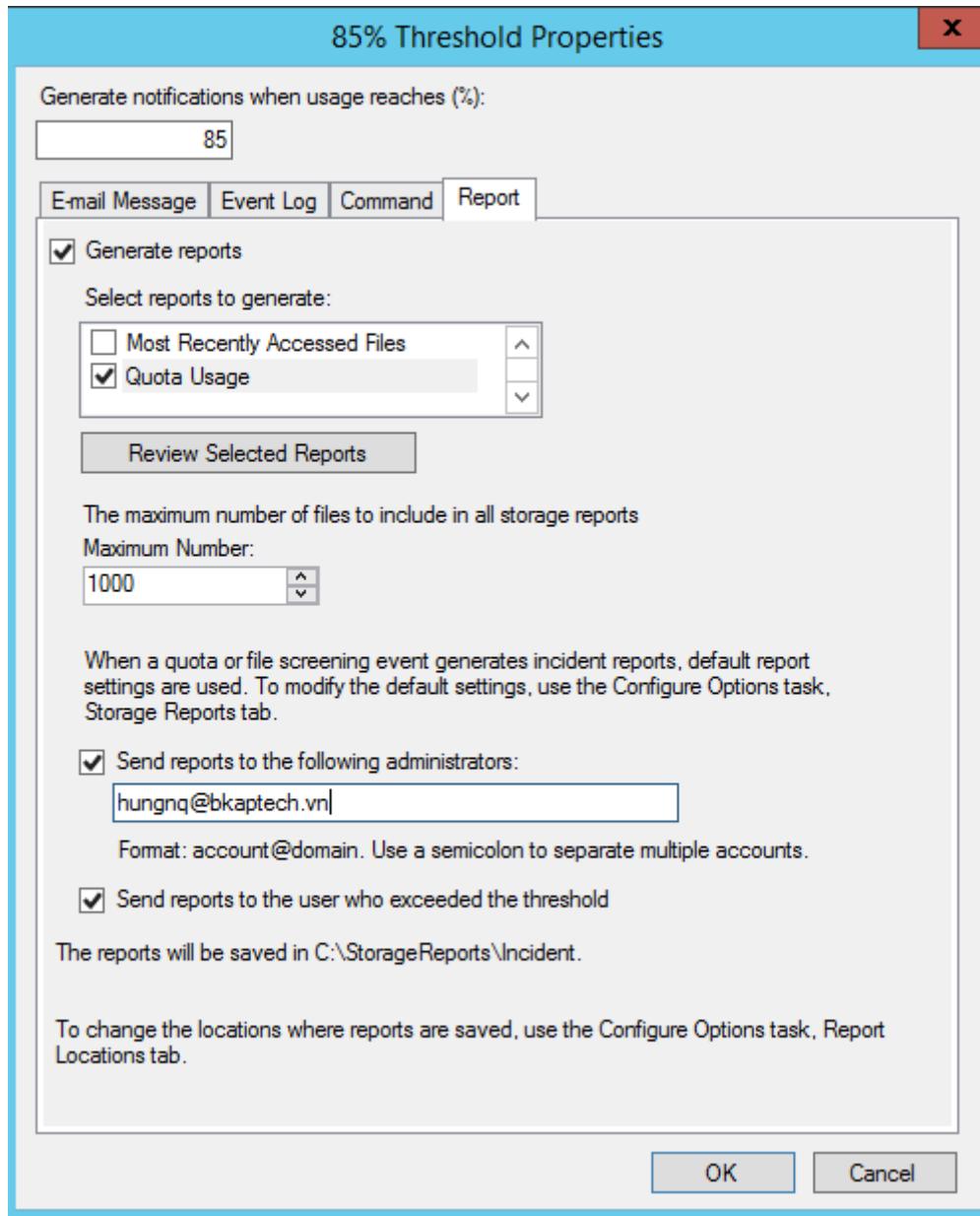
- Click vào **Warning (85%)**, chọn **Edit...**, tại cửa sổ **85% Threshold Properties**, click chọn vào **Send e-mail to the following administrators**, nhập vào tên user **hungnq@bkaptech.vn**



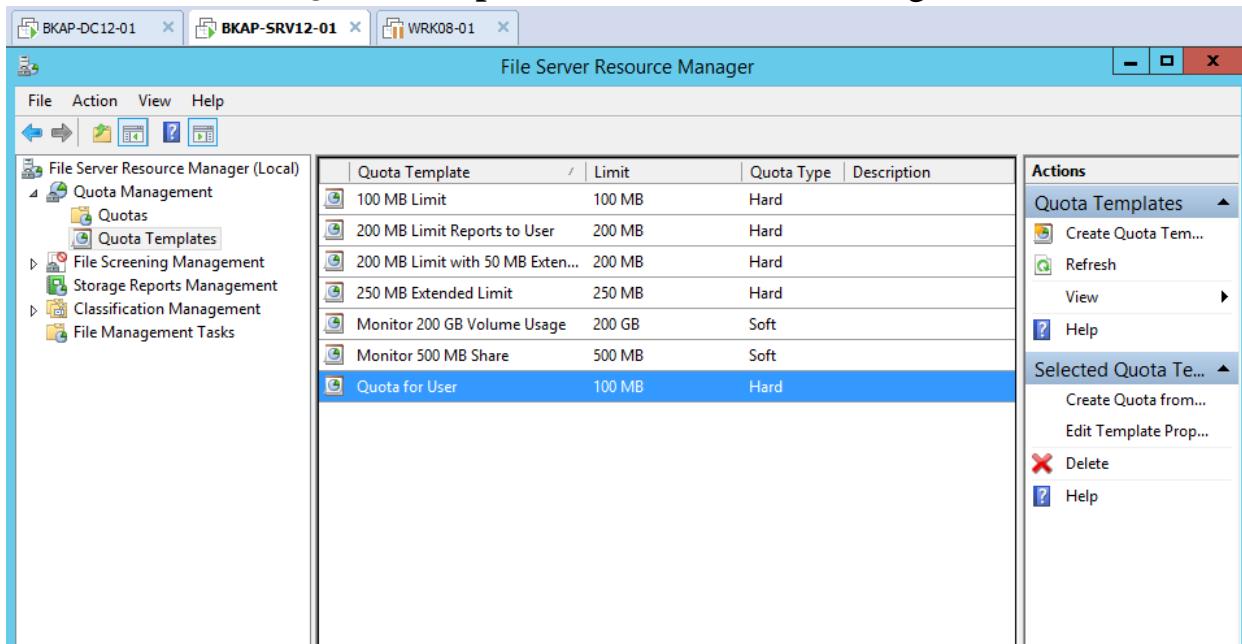
- Chuyển sang tab **Event Log**, click chọn vào **Send warning top event log**.



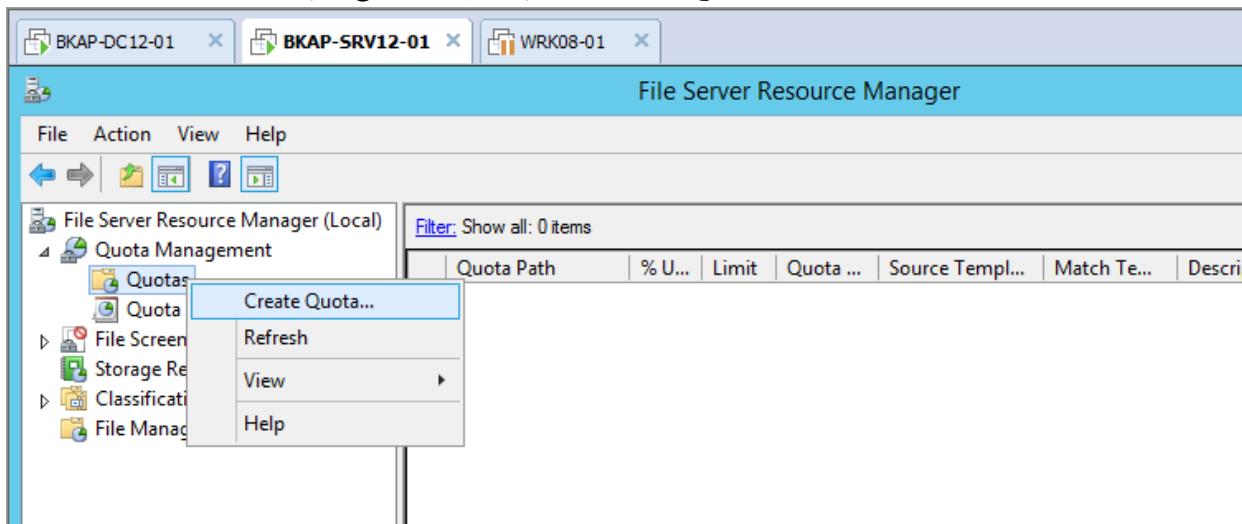
- Chuyển sang tab **Report**, click chọn vào **Generate reports**. Tại mục **Select reports to generate**, click chọn vào **Quota Usage**.
 - ⇒ Click chọn vào **Send reports to the following administrators**, nhập user **hungnq@bkaptech.vn** vào mục bên dưới.
 - ⇒ Click chọn vào **Send reports to the user who exceeded the threshold**.



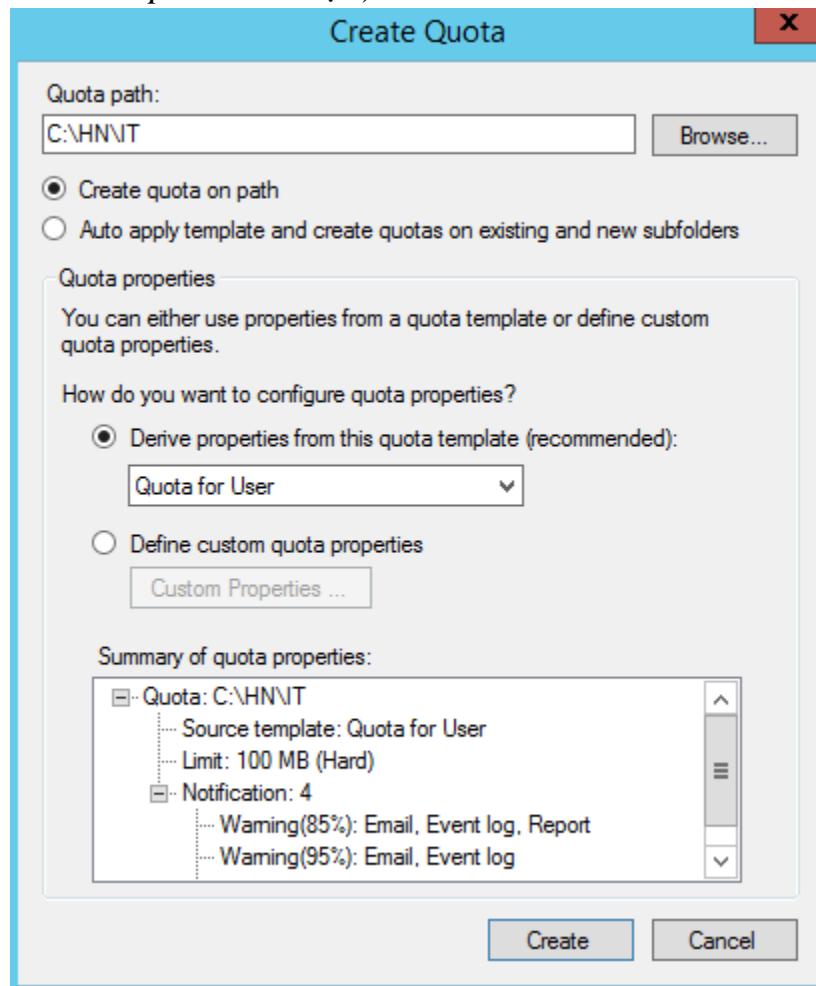
- Quota Templates đã được tạo thành công.



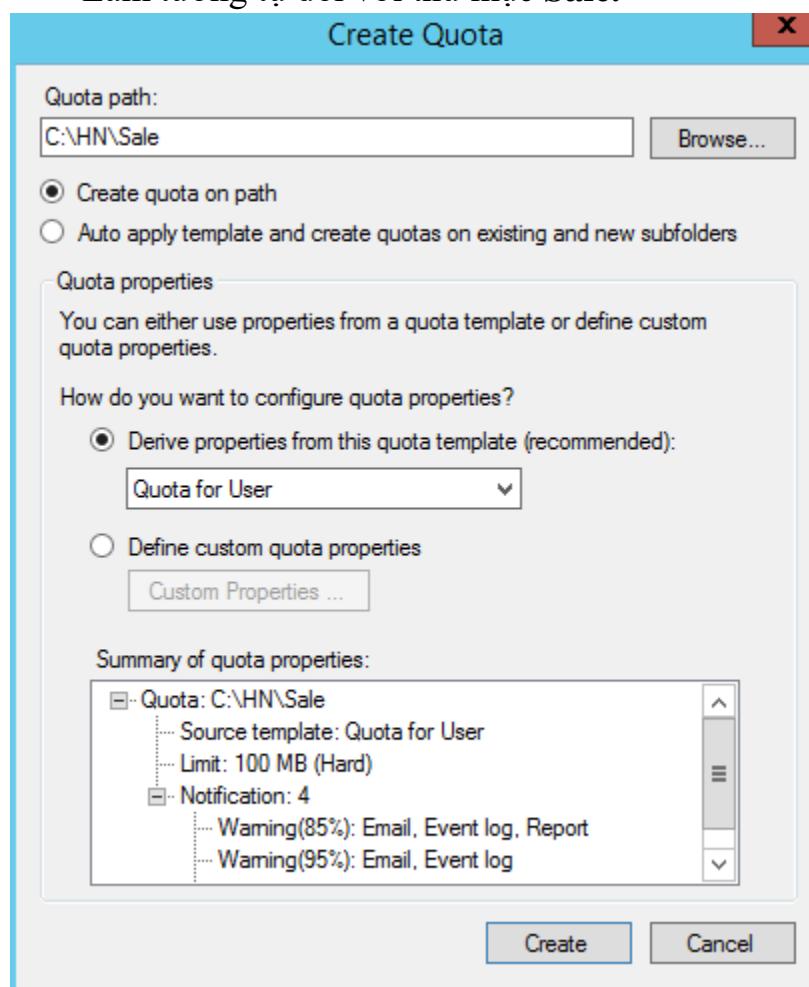
- Tại cửa sổ File Server Resource Manager , click chuột phải tại Quotas , chọn Create Quota...



- Tại cửa sổ **Create Quota**, tại mục **Quota path**, *Browse* đến thư mục **IT**. Tại mục **Derive properties from this quota template (recommended)**, chọn vào **Quota for User (Quota Templates vừa tạo)**. => Click vào **Create**.



- Làm tương tự đối với thư mục Sale.



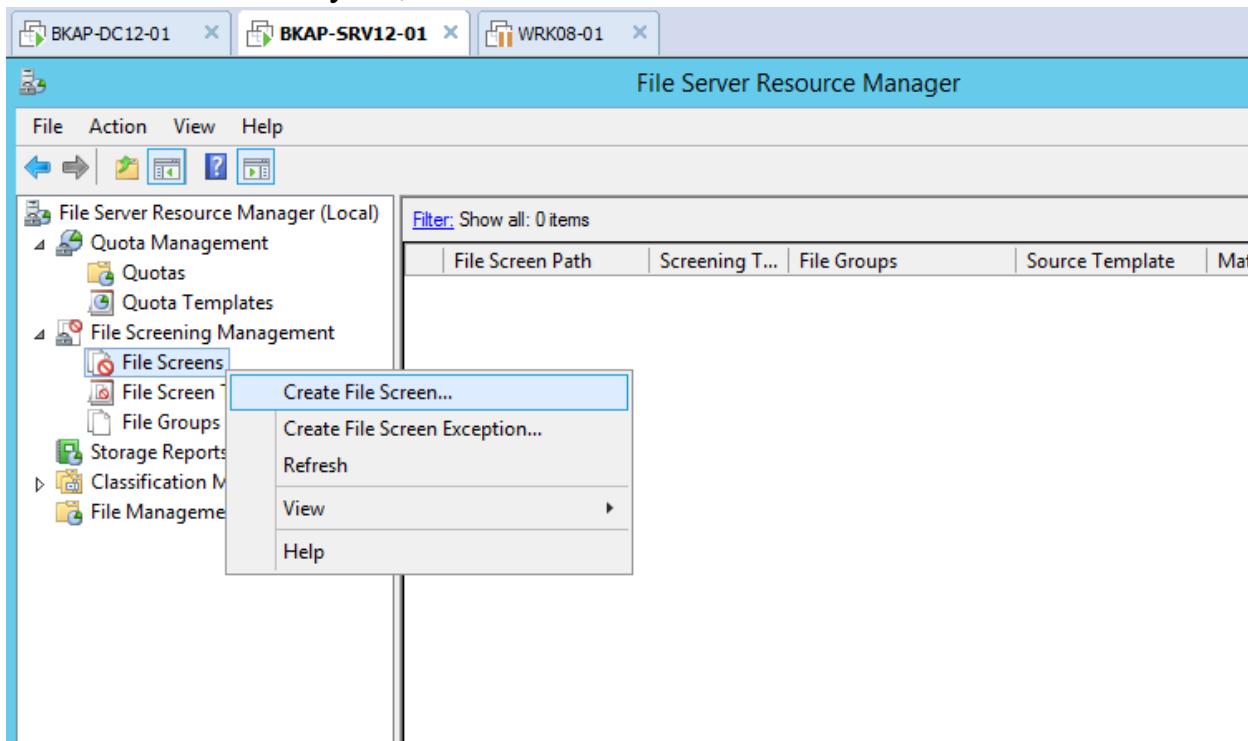
- Ta được kết quả sau:

Quota Path	% Used	Limit	Quota Type	Source Template	Description
C:\HN\IT	0%	100 ... Hard	Quota for User	Yes	
C:\HN\Sale	0%	100 ... Hard	Quota for User	Yes	

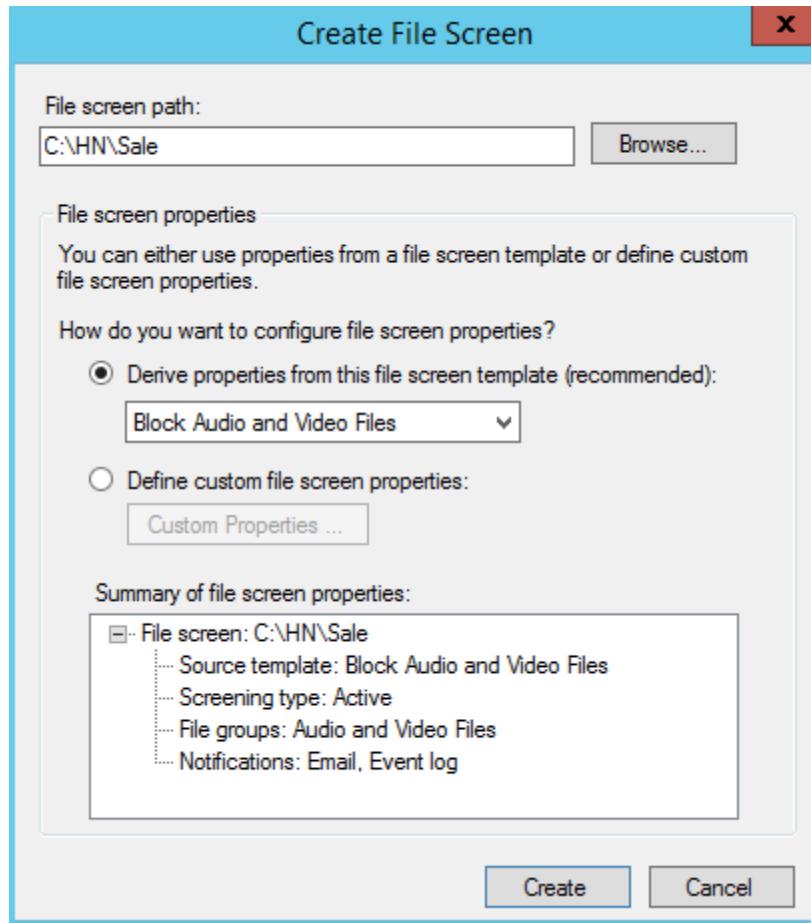
○

Cấu hình File Screening Management.

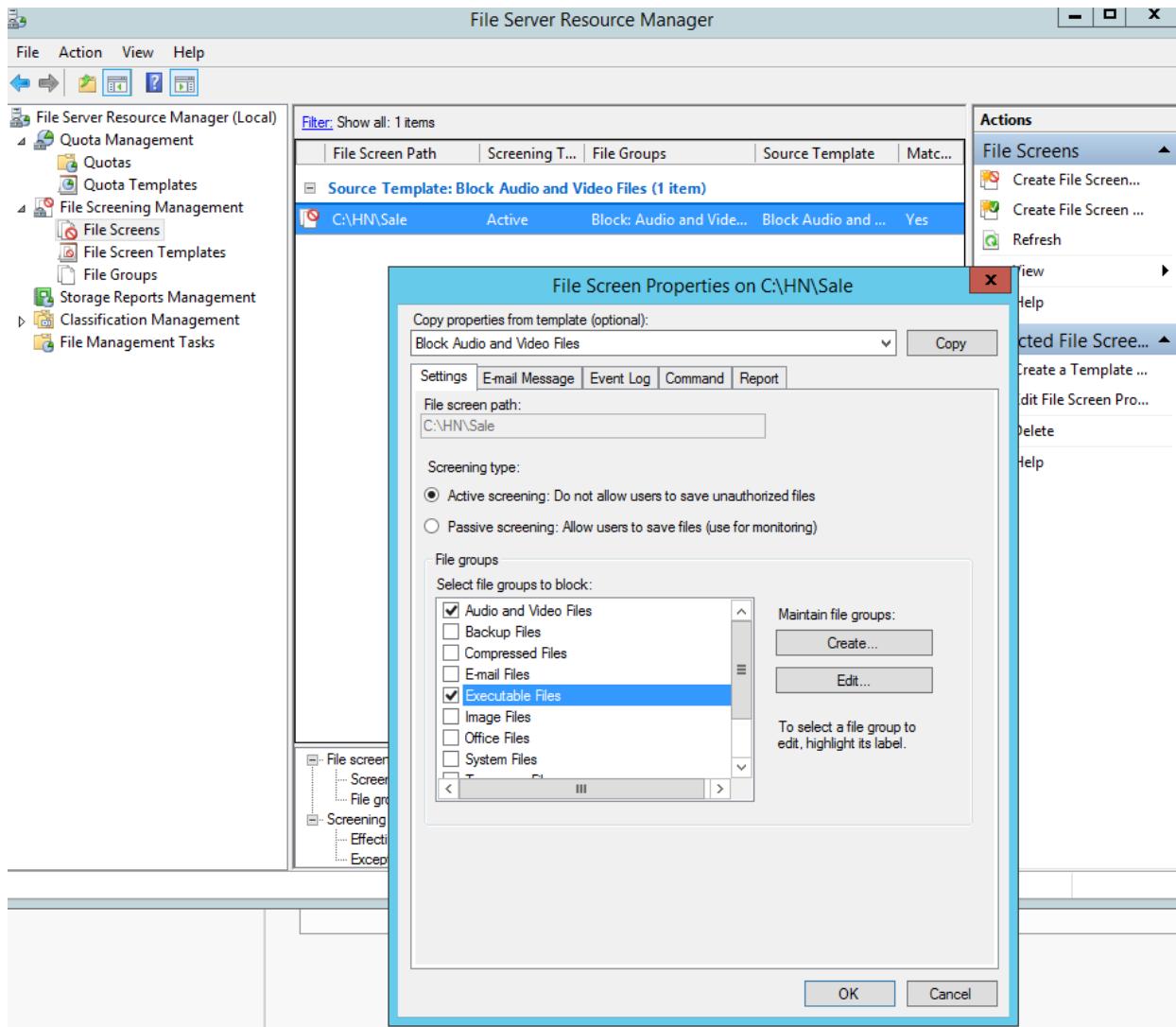
- Tại cửa sổ **File Server Resource Manager** , click vào **File Screening Management / File Screens** , click chuột phải tại đây chọn **Create File Screen...**



- Tại cửa sổ **Create File Screen**, tại mục **File screen path**, **browse** đến thư mục **Sale**. Tại mục **Derive properties from this file screen template (recommended)**, chọn vào **Block Audio and Video Files**, => **Create**.

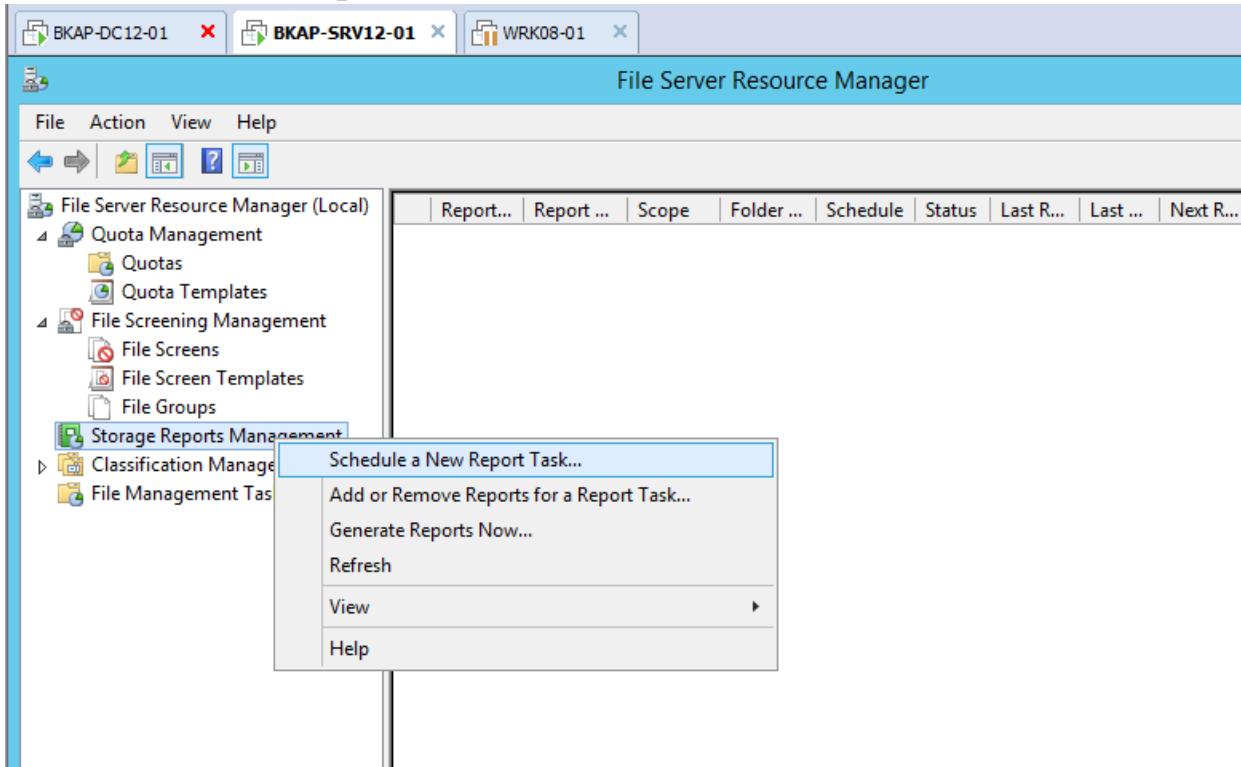


- Click vào chính sách vừa tạo ở trên trong cửa sổ **File Server Resource Manager** , tại cửa sổ **File Screen Properties on C:\HN\Sale** , tại mục **Select file groups to block** , chọn vào **Executable Files**. => OK.

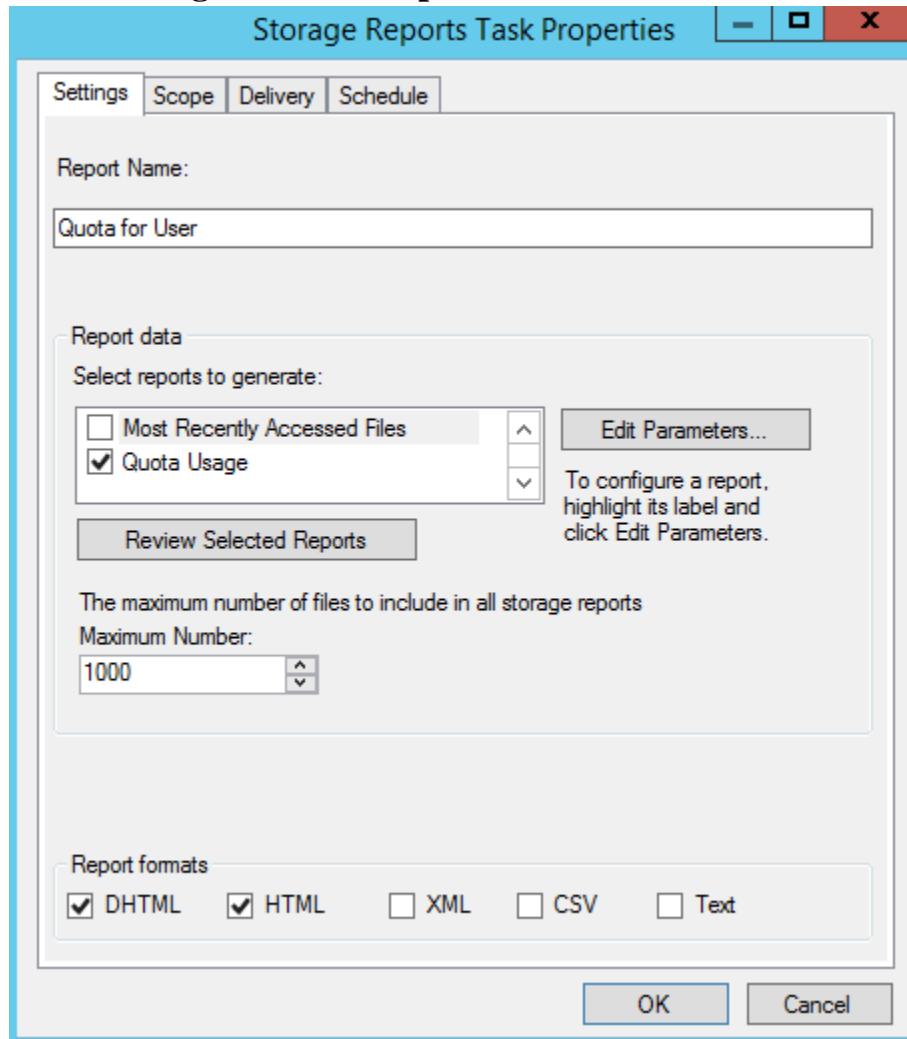


o Tạo báo cáo :

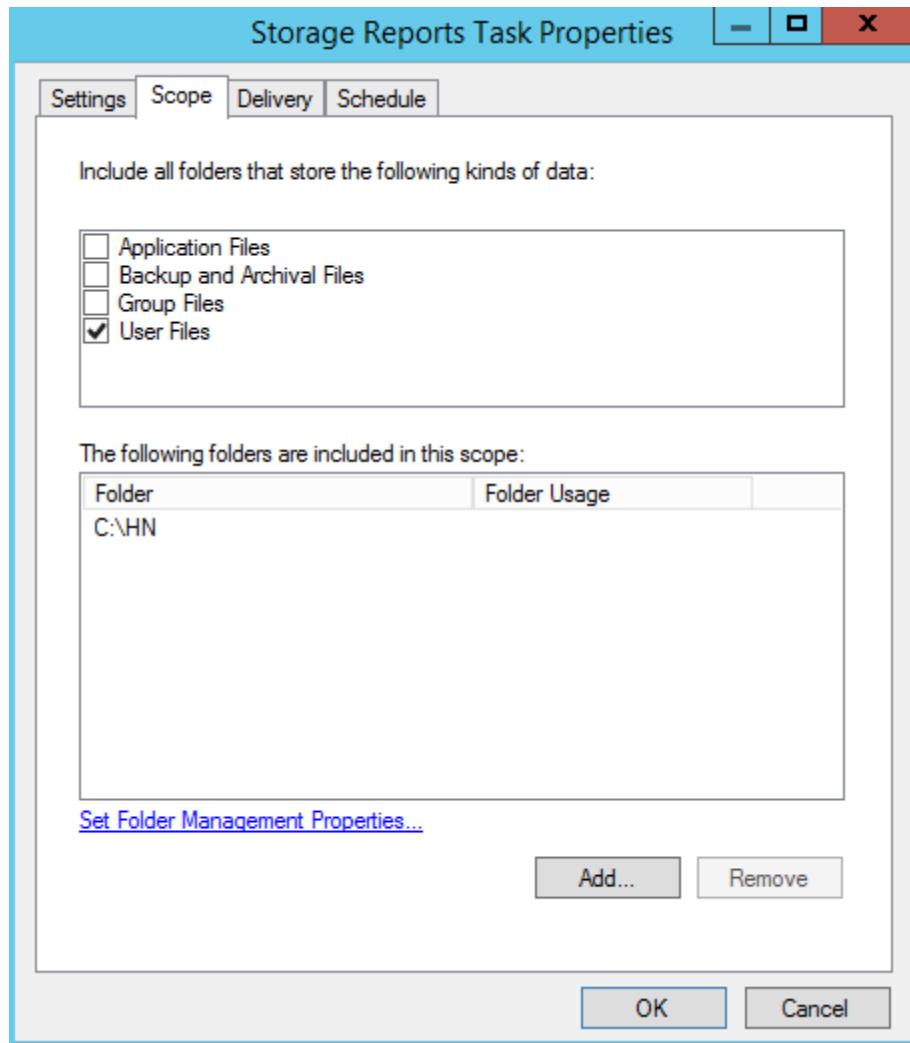
- Tại cửa sổ **File Server Resource Manager** , click chuột phải tại **Storage Reports Management** , chọn **Schedule a New Report Task...**



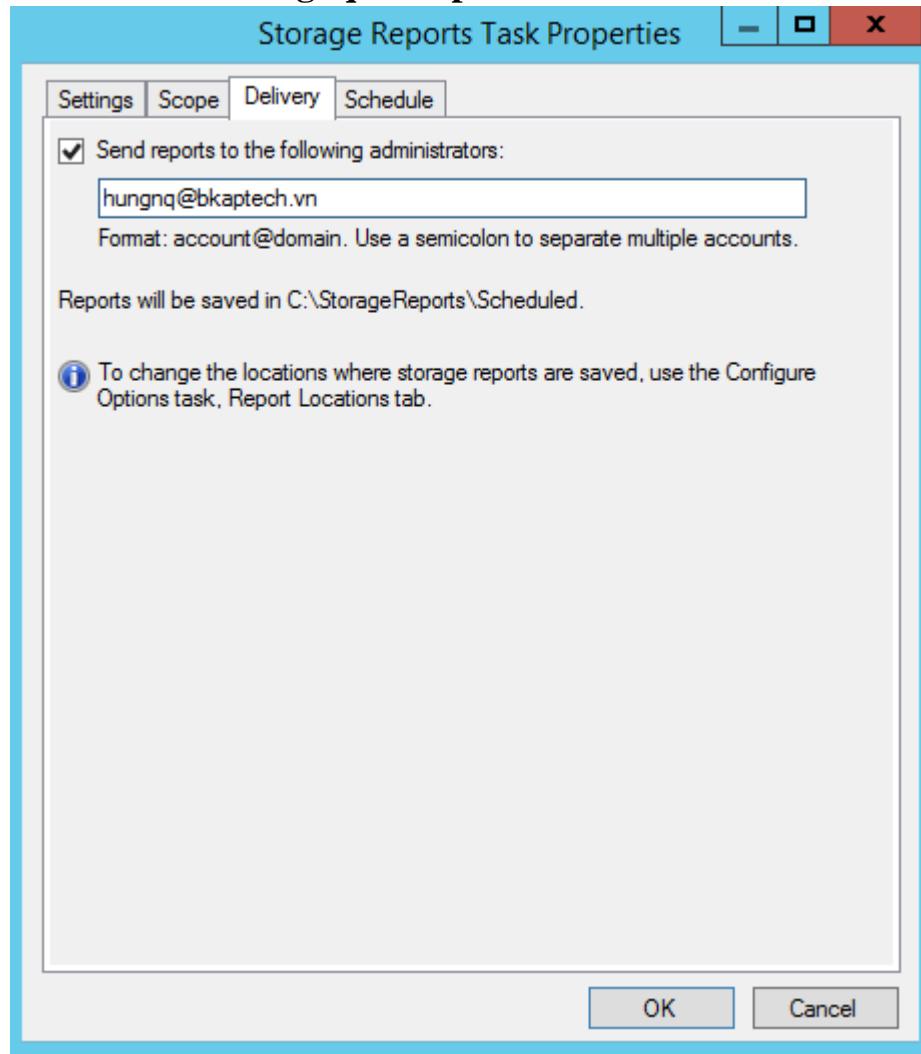
- Tại cửa sổ **Storage Reports Task Properties**, tại tab **Settings**, tại mục **Report Name**, nhập vào tên **Quota for User**, tại mục **Select reports to generate**, bỏ chọn tất cả trừ mục **Quota Usage**, tại mục **Report formats** chọn **DHTML** và **HTML**.



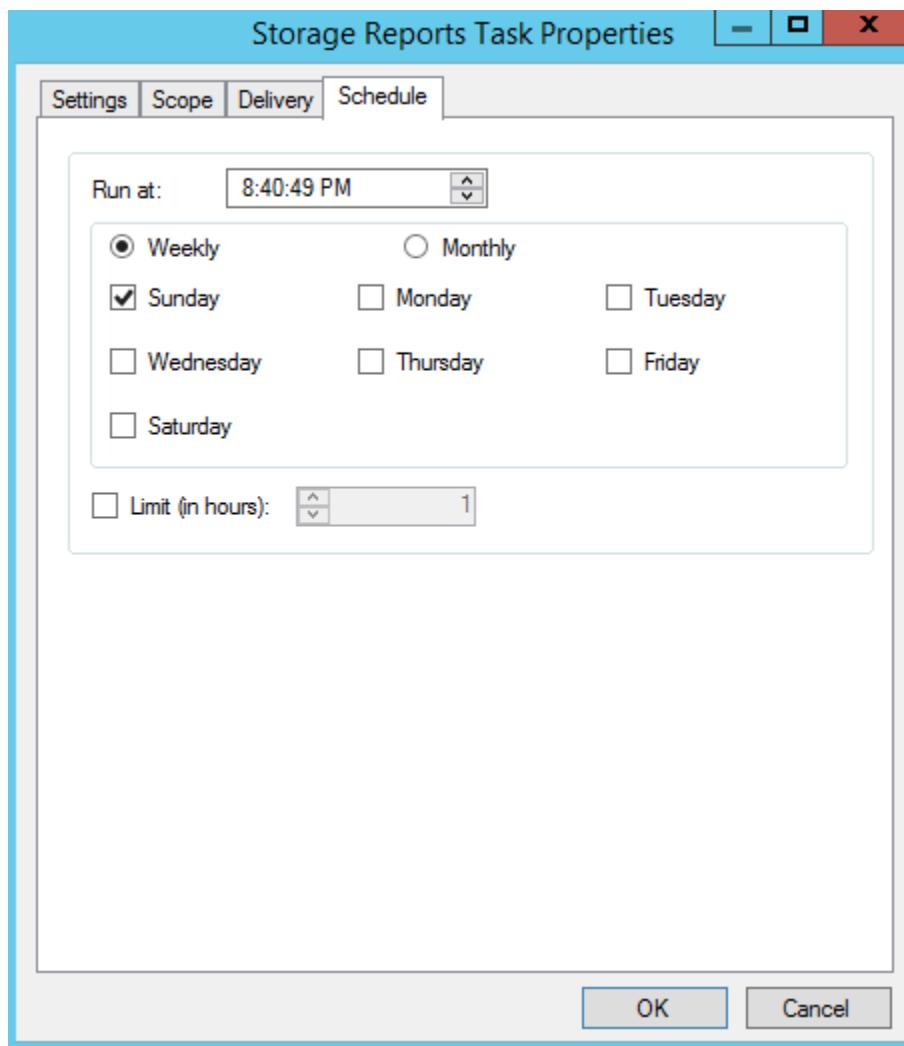
- Chuyển sang tab **Scope** , click vào **Add...** , browse đến thư mục *HN* , tại mục **Include all folders...** click chọn vào **User Files**.



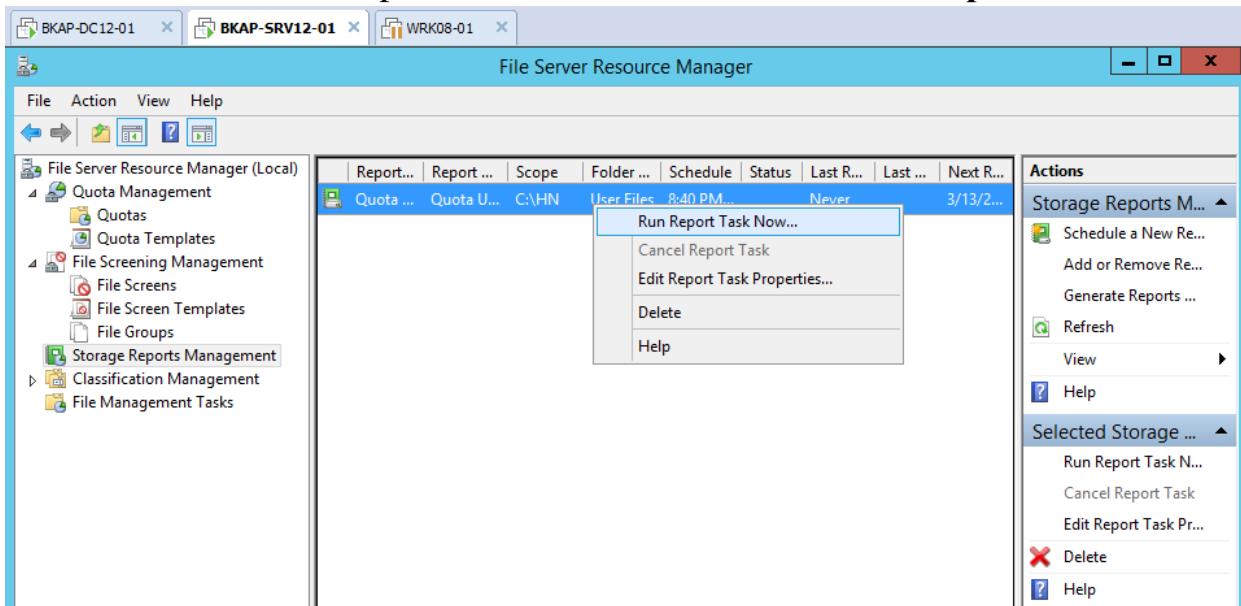
- Chuyển sang tab **Delivery**, click chọn vào **Send reports to the following administrators**, nhập vào user **hungnq@bkaptech.vn**



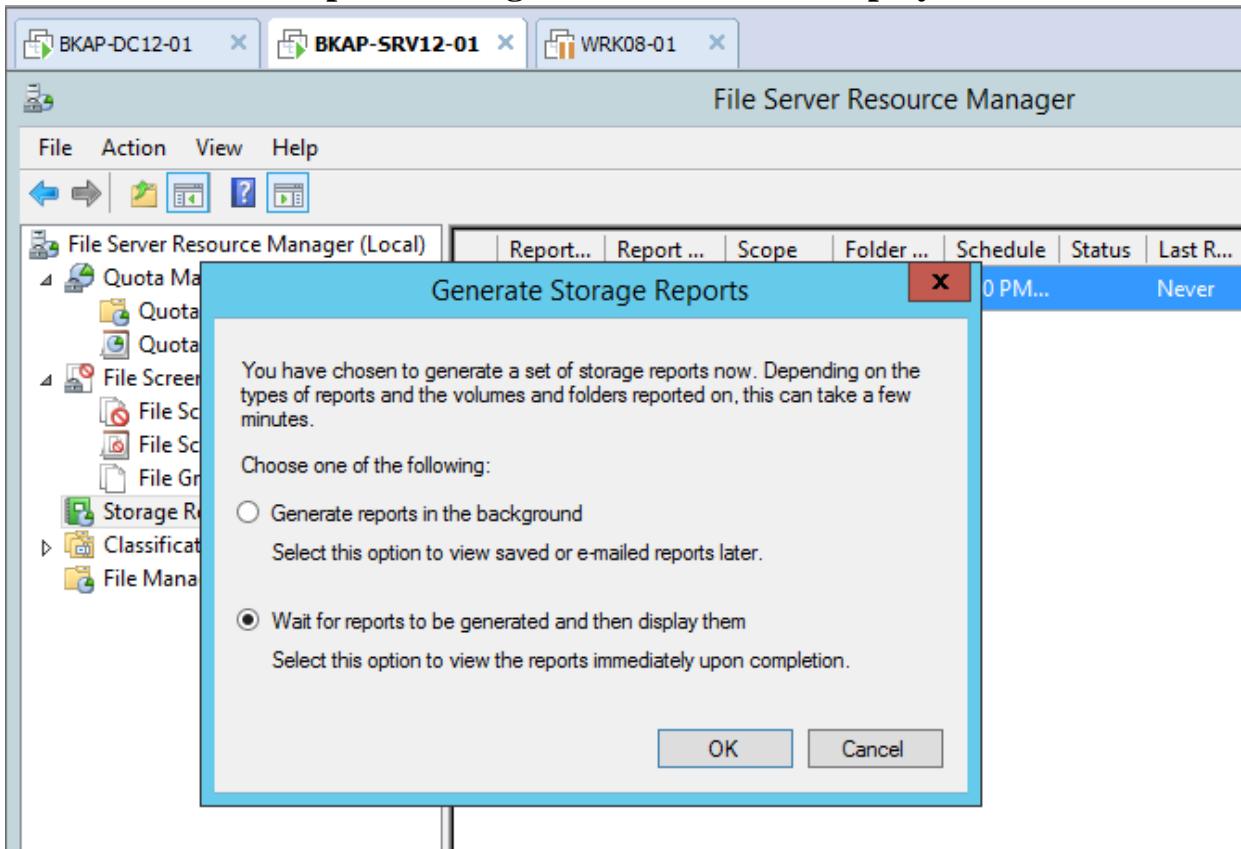
- Chuyển sang tab **Schedule** , chọn thời gian xuất báo cáo. => **OK.**



- Click chuột phải tại báo cáo vừa tạo , chọn **Run Report Task Now...**



- Tại cửa sổ **Generate Storage Reports** , chọn vào **Wait for reports to be generated and then display them.**



▪ Xem báo cáo.

The screenshot shows a Windows application window titled "File Server Resource Manager". The title bar has three tabs: "BKAP-DC12-01", "BKAP-SRV12-01" (which is active), and "WRK08-01". The main content area displays a report titled "Quota Usage Report Table of Contents". The report includes sections for "Report Description", "Machine", "Report Folders", and "Parameters". Below this is a table titled "Report Totals" showing the number of quotas and their total usage. Further down is a section titled "Report statistics" with a table showing usage details for specific folders like "c:\hn\IT" and "c:\hn\Sale".

Report Description: Lists the quotas that exceed a certain disk space usage level. Use this report to quickly identify quotas that may soon be exceeded.

Machine: BKAP-SRV12-01

Report Folders: 'User Files ()', 'C:\HN'

Parameters: Minimum Quota used percent: 0%

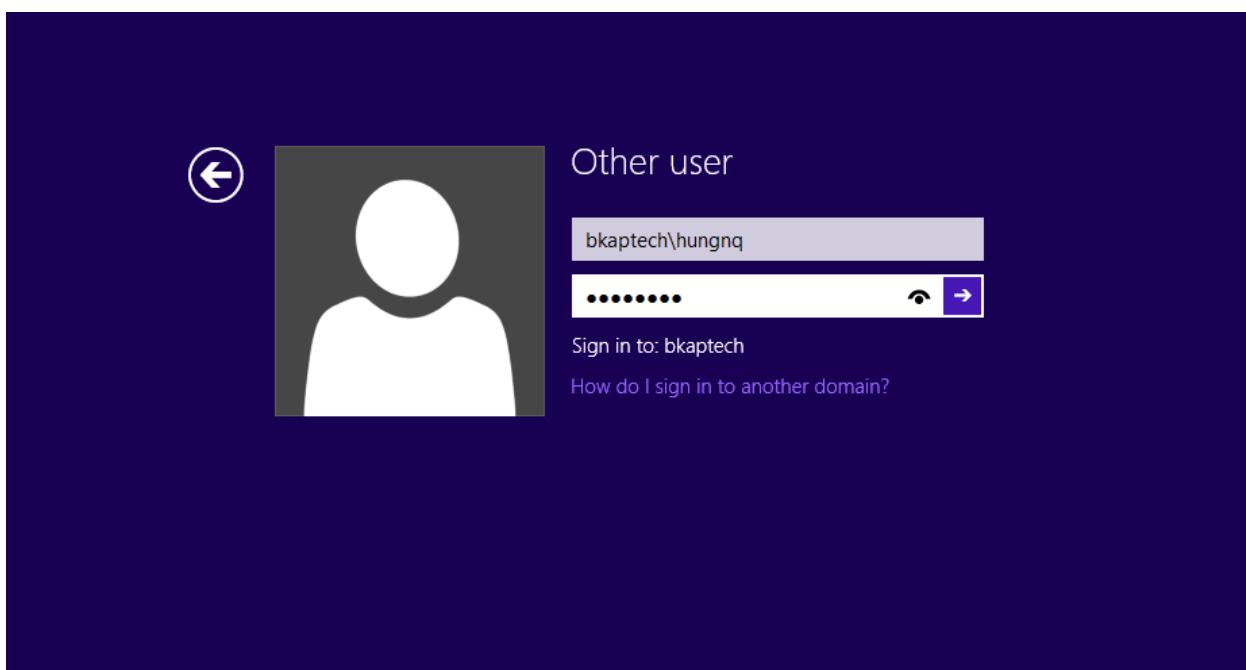
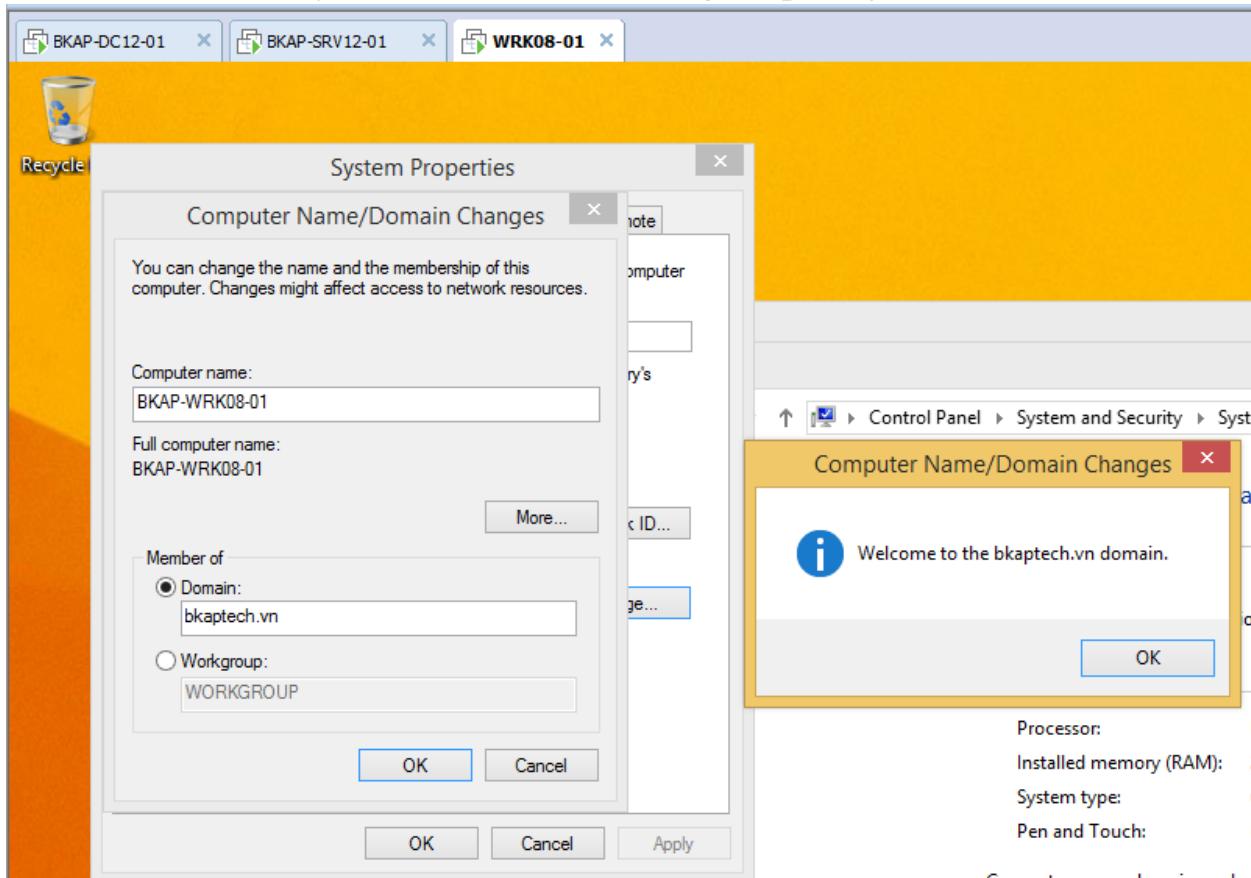
Report Totals					
Quotas shown in report		All quotas matching report criteria			
Quotas	Total Usage	Quotas	Total Usage		
2	0.00 MB	2	0.00 MB		

[To top of the current report](#)

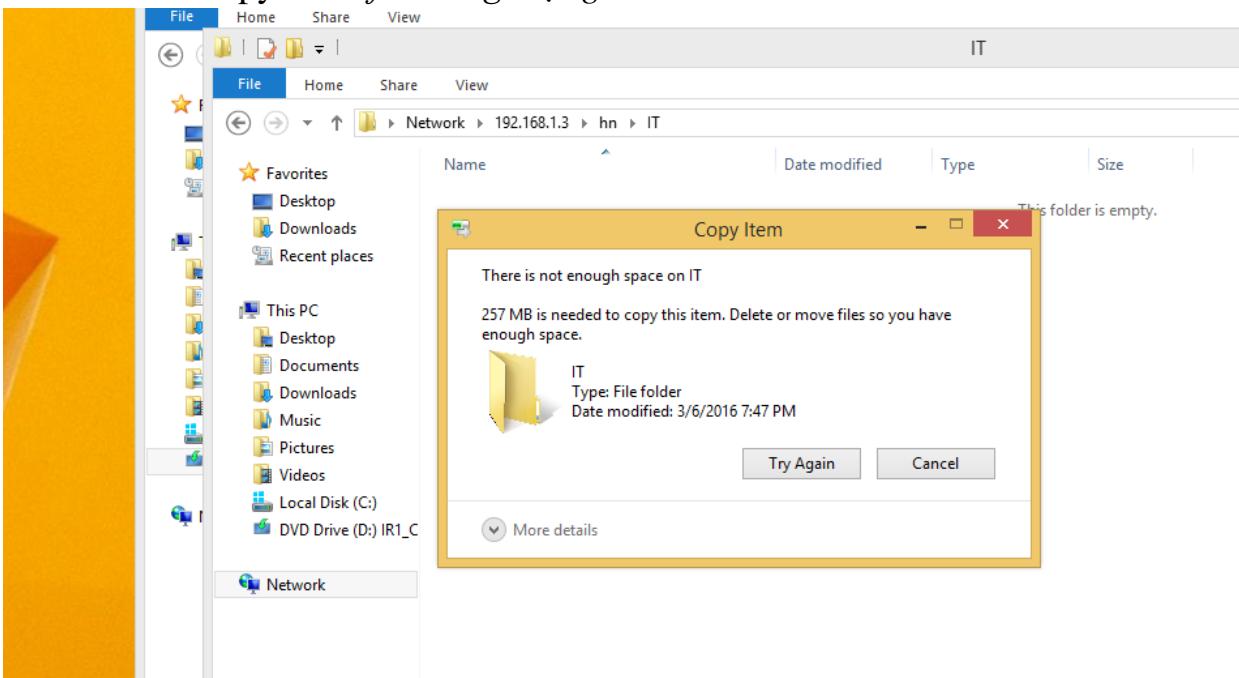
Report statistics					
Folder					
Owner	Quota	Usage	Used	Peak Usage	Peak Usage Time
c:\hn\IT					
BUILTIN\Administrators	100.0 MB	0.00 MB	0.00 %	0.00 MB	3/6/2016 8:27:07 PM
c:\hn\Sale					
BUILTIN\Administrators	100.0 MB	0.00 MB	0.00 %	0.00 MB	3/6/2016 8:28:13 PM

[To top of the current report](#)

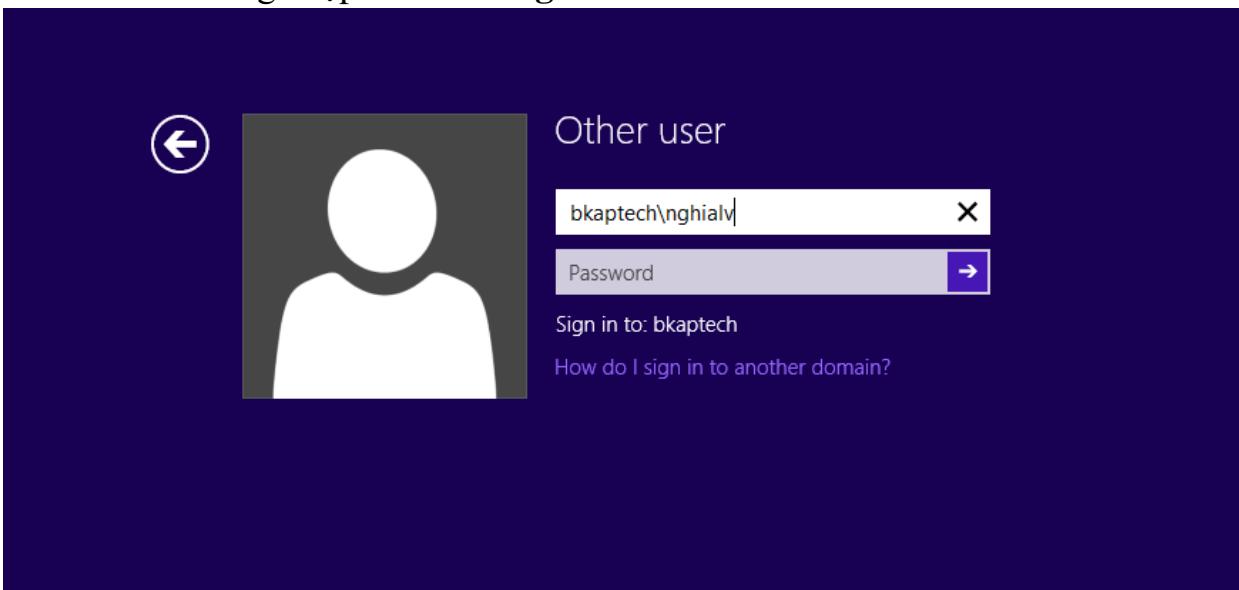
- Chuyển sang máy **BKAP-WRK08-01** kiểm tra.
 - Join máy Client vào Domain, đăng nhập bằng tài khoản **hungnq**.



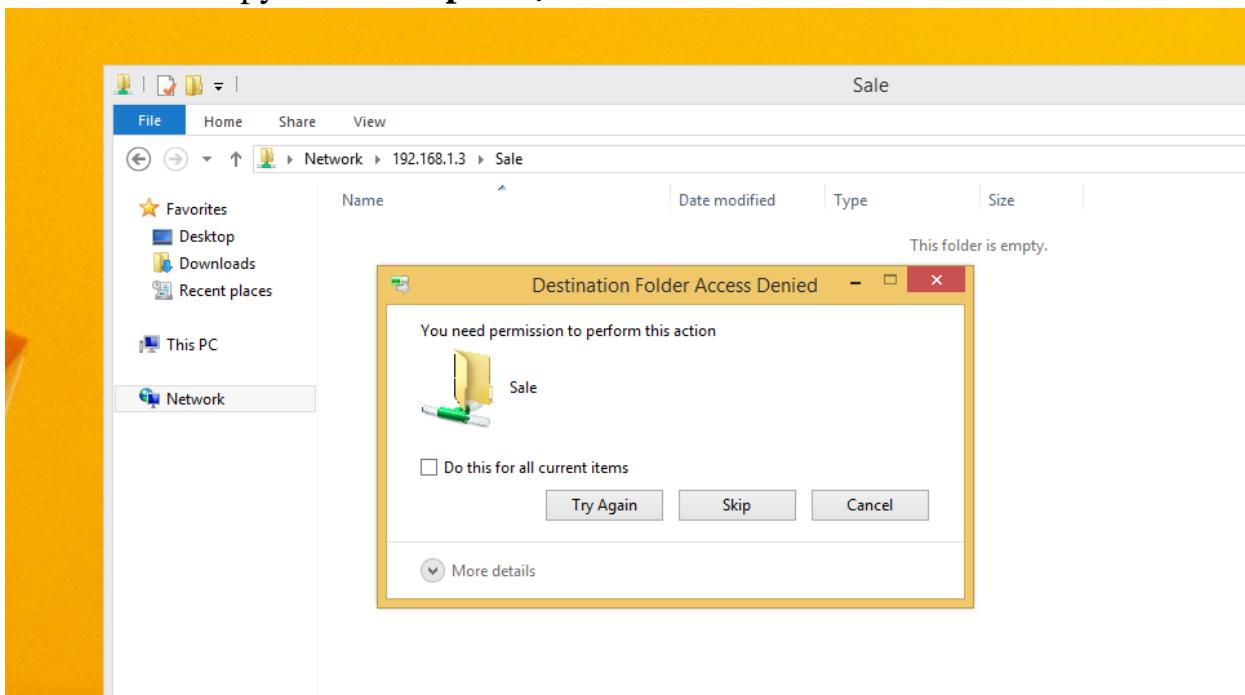
- Copy thử *1 file dung lượng lớn* vào folder **IT** để kiểm tra.



- Đăng nhập tài khoản **nghialv** để kiểm tra.



- Copy thử file .mp3 hoặc file .exe để kiểm tra.



10.2 Triển khai cài đặt và cấu hình dịch vụ DFS (Distributed File System)

1. Yêu cầu bài lab:

+ Trên máy *BKAP-DC12-01*:

- Snapshot “*Domain Controller*”.
- *DNS Server* : **bkaptech.vn**.
- Cài đặt và cấu hình *DFS*.
- Tạo *DFS Namespace* chứa các thư mục chia sẻ tài nguyên với tên `\bkaptech.vn\Data`.

+ Trên máy *BKAP-SRV12-01* : Đặt làm máy chủ *File Server*.

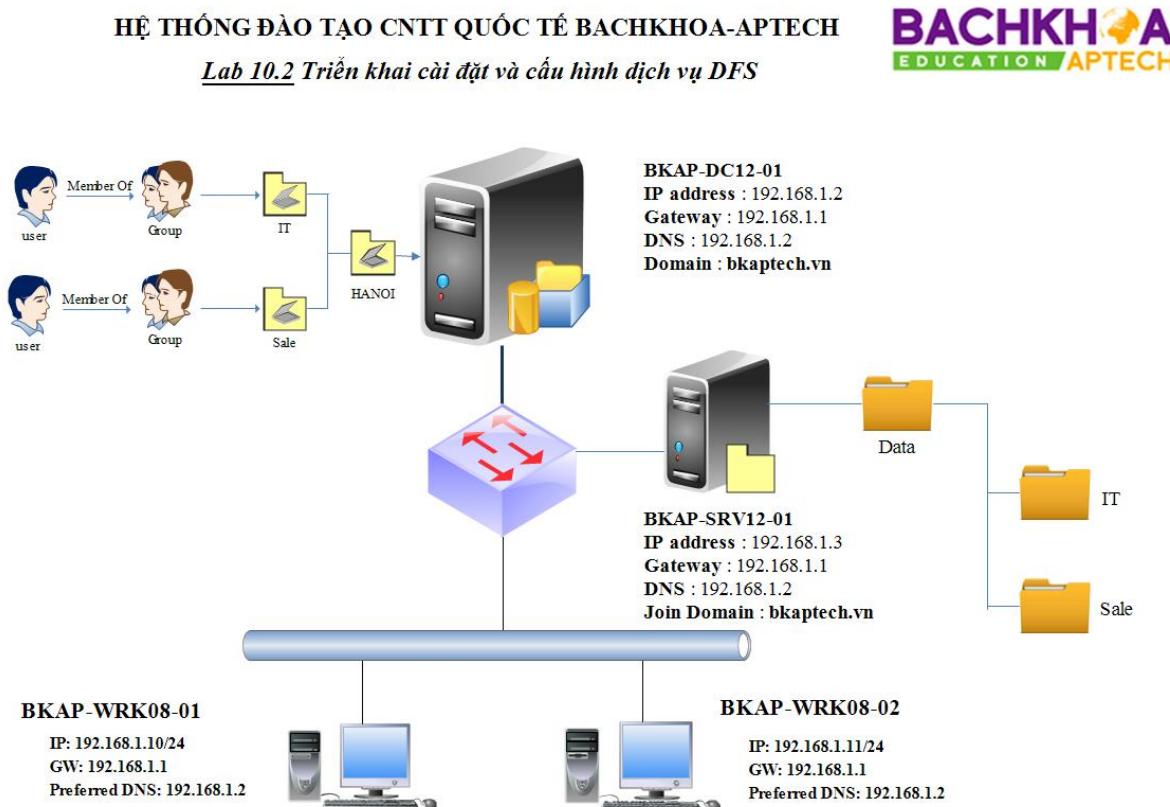
+ Trên máy *BKAP-WRK08-01* : Các máy người dùng trong hệ thống mạng truy cập dữ liệu thành công với tên `:\\bkaptech.vn\Data`.

2. Yêu cầu chuẩn bị :

+ Máy Server *BKAP-DC12-01* : đã nâng cấp lên *Domain Controller* quản lý miền **bkaptech.vn** và cài đặt cấu hình *DNS Server*.

- + Máy Server *BKAP-SRV12-01* Join Domain.
- + Máy Client *BKAP-WRK08-01* Join Domain.

3. Mô hình Lab:



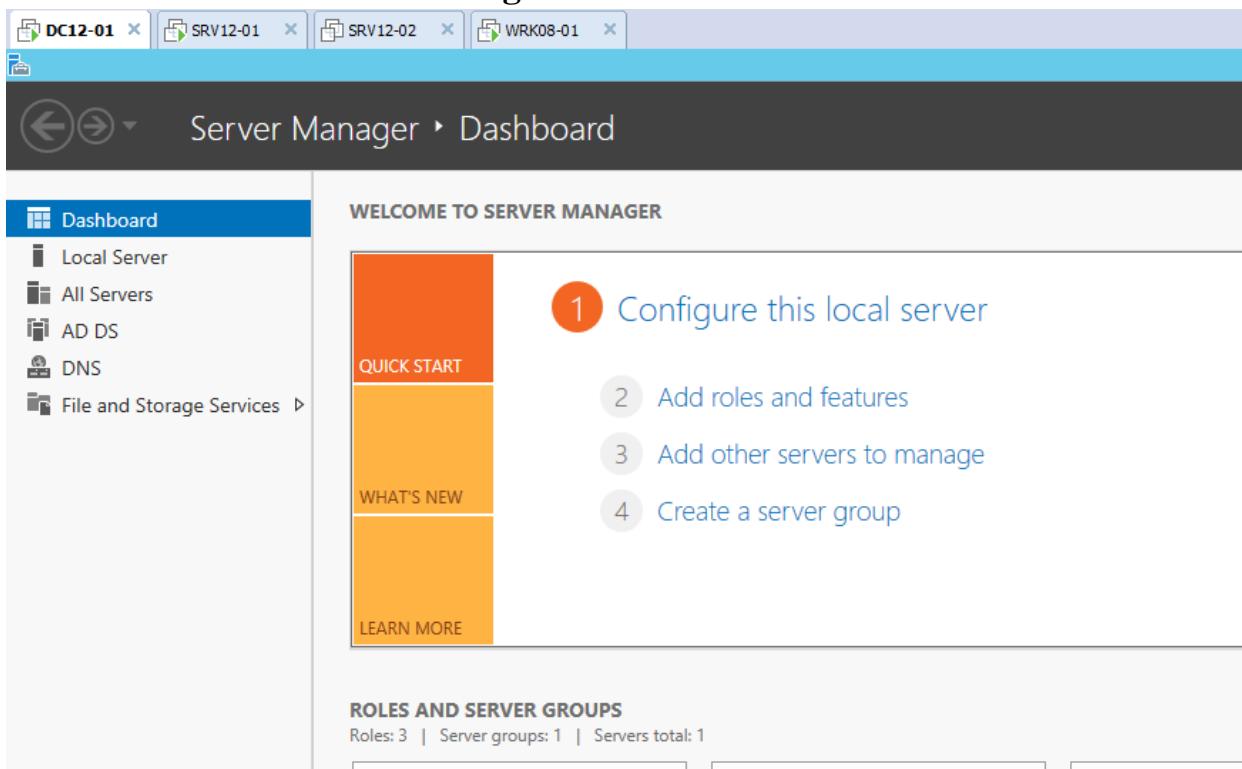
Hình 10.2

Sơ đồ địa chỉ như sau:

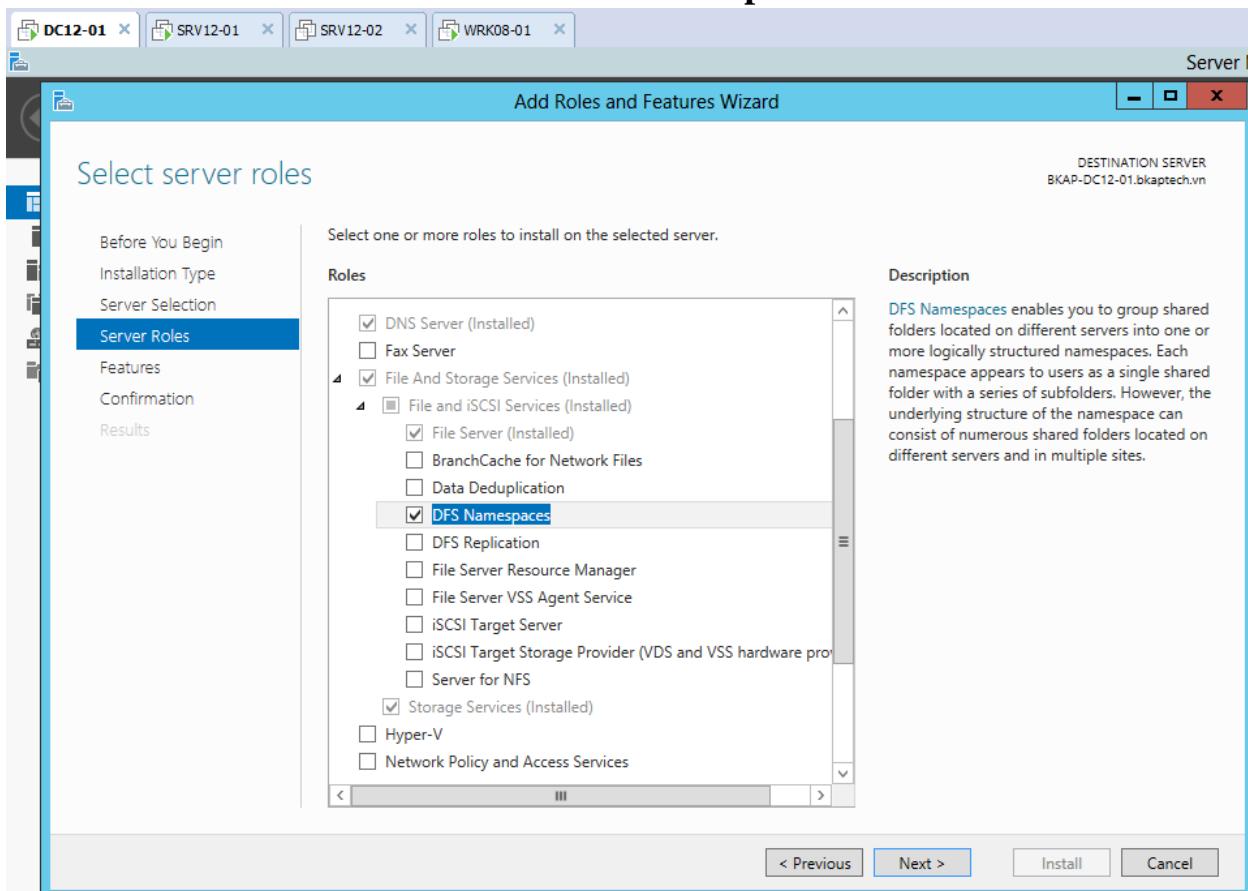
Thông số	BKAP-DC12-01	BKAP-SRV12-01	BKAP-WRK08-01
<i>IP address</i>	192.168.1.2	192.168.1.3	192.168.1.10
<i>Subnet Mask</i>	255.255.255.0	255.255.255.0	255.255.255.0
<i>Gateway</i>	192.168.1.1	192.168.1.1	192.168.1.1
<i>DNS Server</i>	192.168.1.2	192.168.1.2	192.168.1.2

Hướng dẫn chi tiết:

- Thực hiện trên máy *BKAP-DC12-01* :
 - Tạo OU, Group, User , add user vào Group như mô hình trên.
 - Cấu hình dịch vụ *DNS Server*, tạo bản ghi cho *DNS Server*:
 - Cài đặt **DFS Namespace**.
 - **Server Manager / Add roles and features**

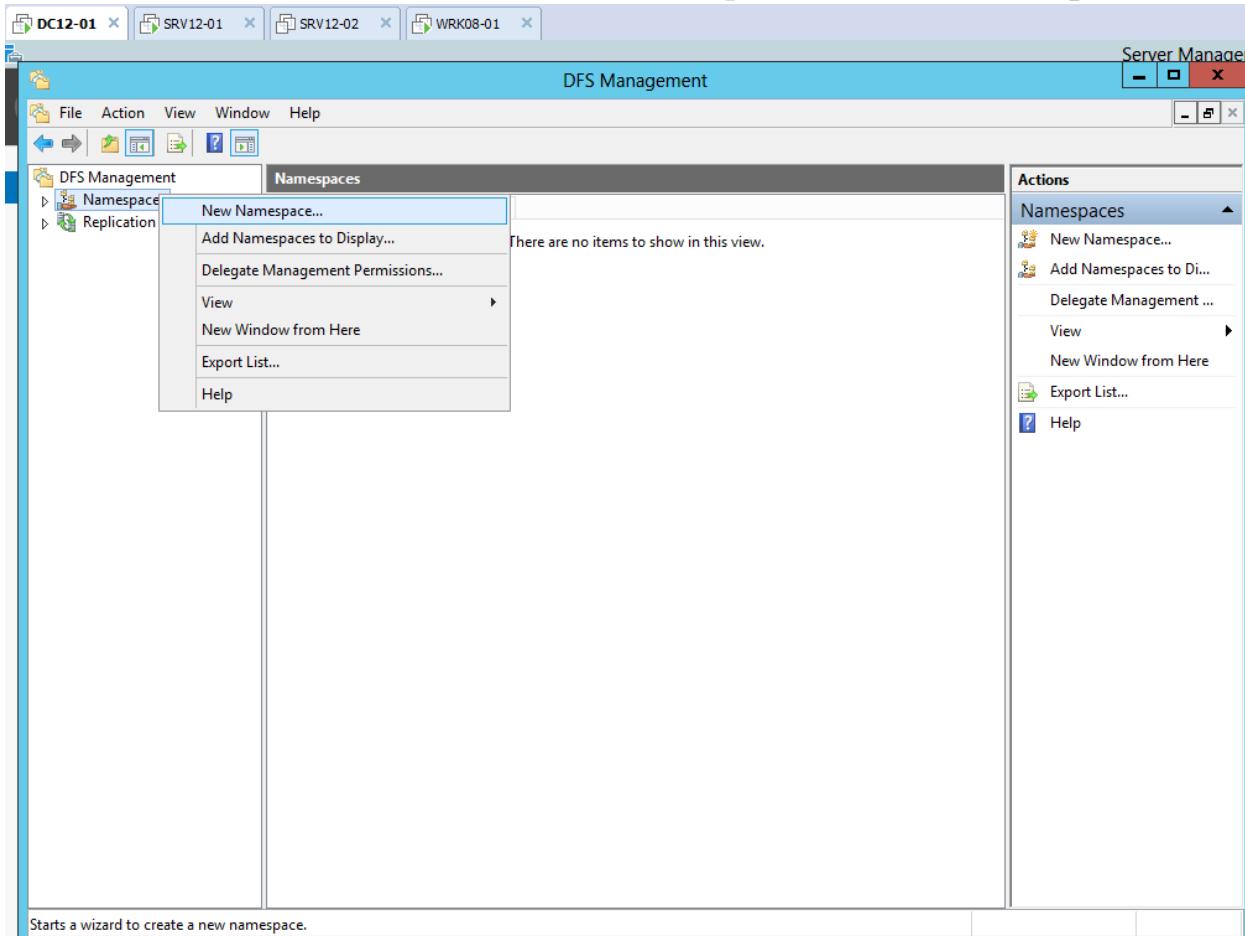


- Tại cửa sổ **Select server roles**, chọn vào dịch vụ **File and iSCSI Services / DFS Namespaces**

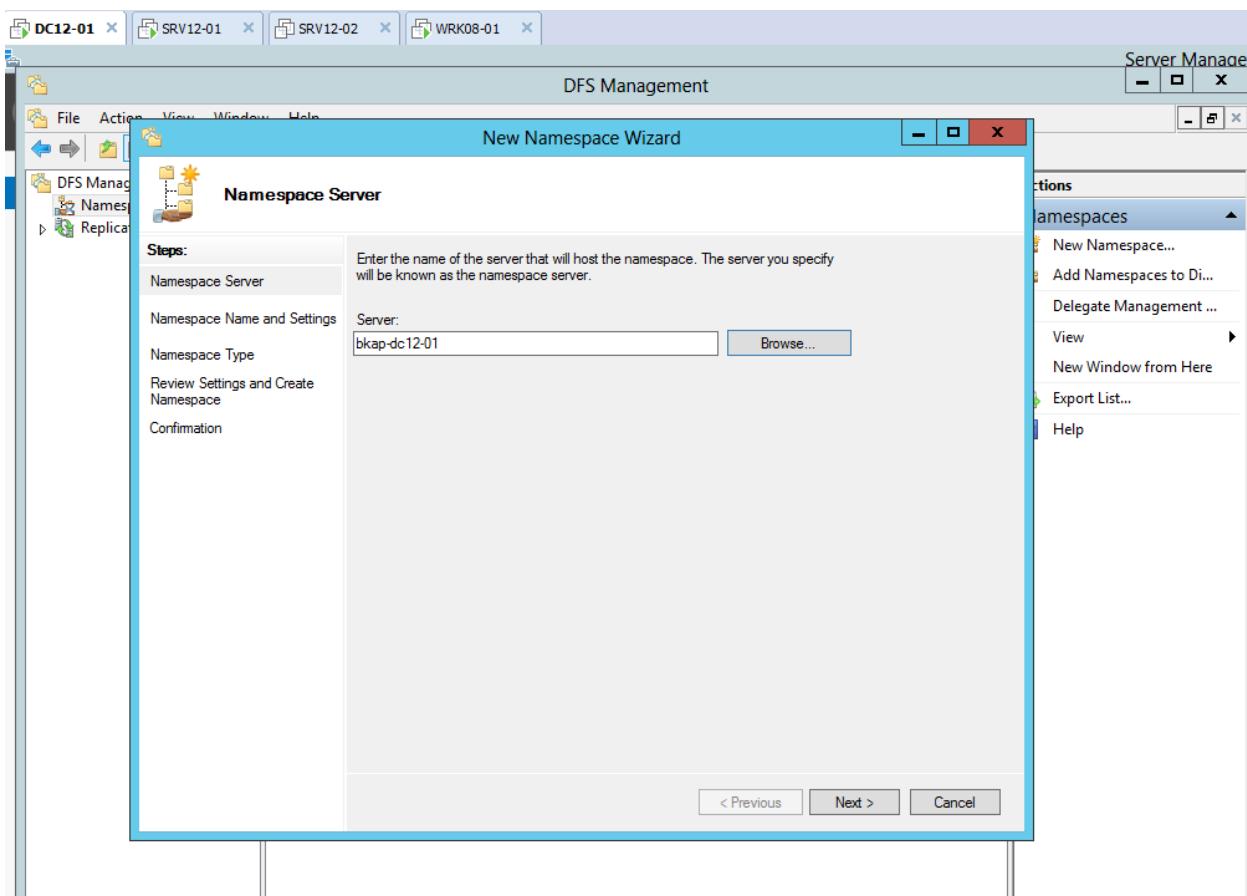


- Click vào **Next / Install** / để máy chủ tiến hành cài đặt,
- Trên máy *BKAP-SRV12-01*, tạo các thư mục như mô hình trên.
 - Join vào Domain, đăng nhập bằng tài khoản *administrator*.
 - Cài đặt dịch vụ **DFS Namespace**.

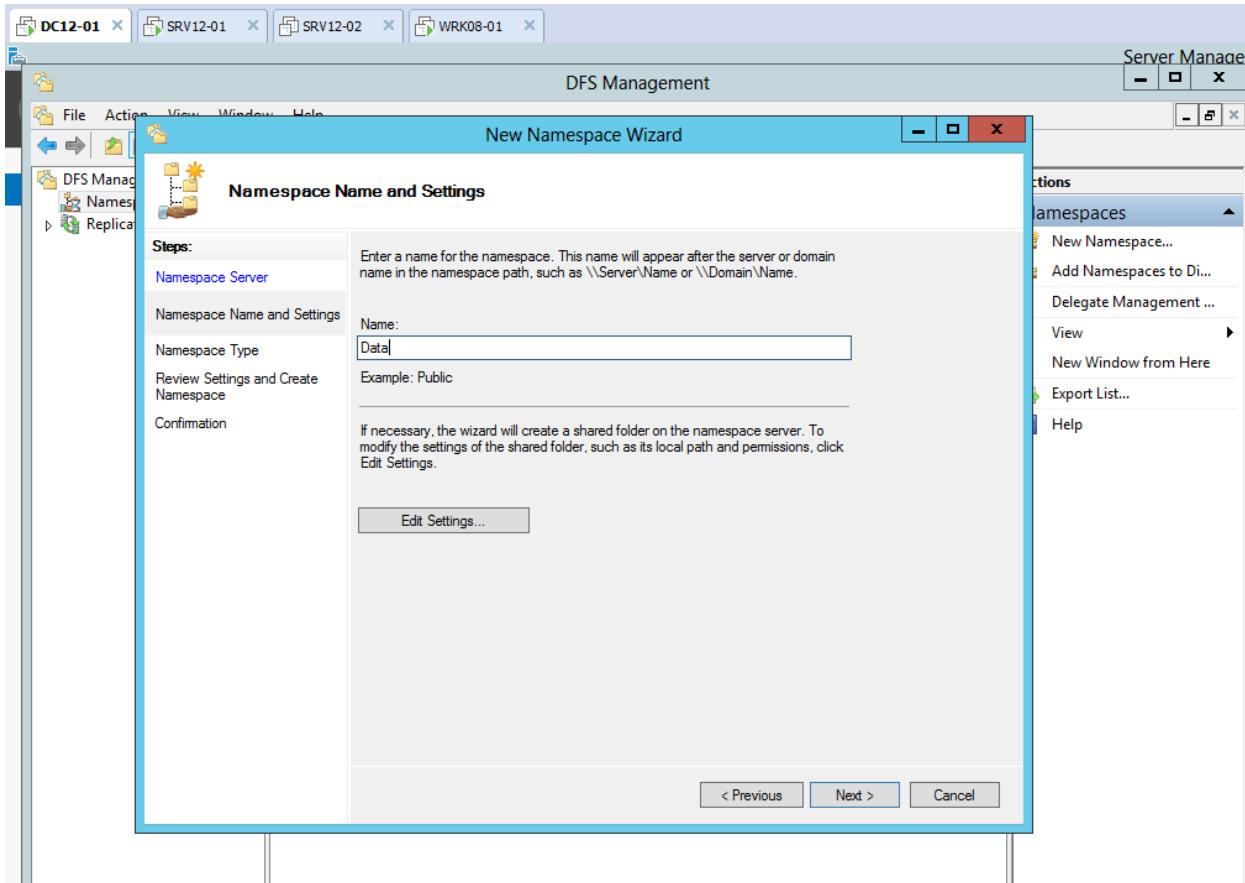
- Chuyển sang máy **BKAP-DC12-01**:
 - Cấu hình DFS :
 - Vào Tools / DFS Management
 - Tại Namespace, click chuột phải chọn New Namespace...

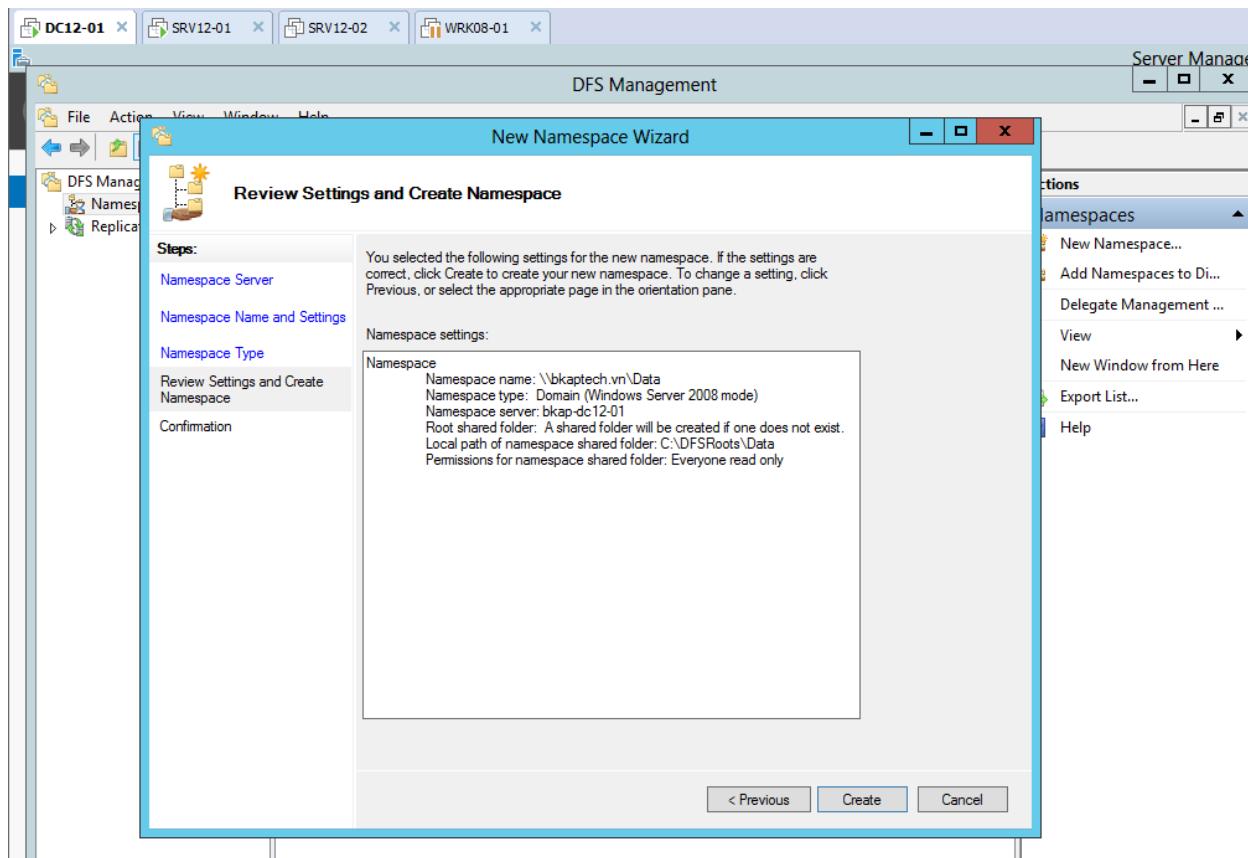


- Tại cửa sổ **Namespace Server**, click vào **Browse...** đến máy chủ *BKAP-DC12-01*.

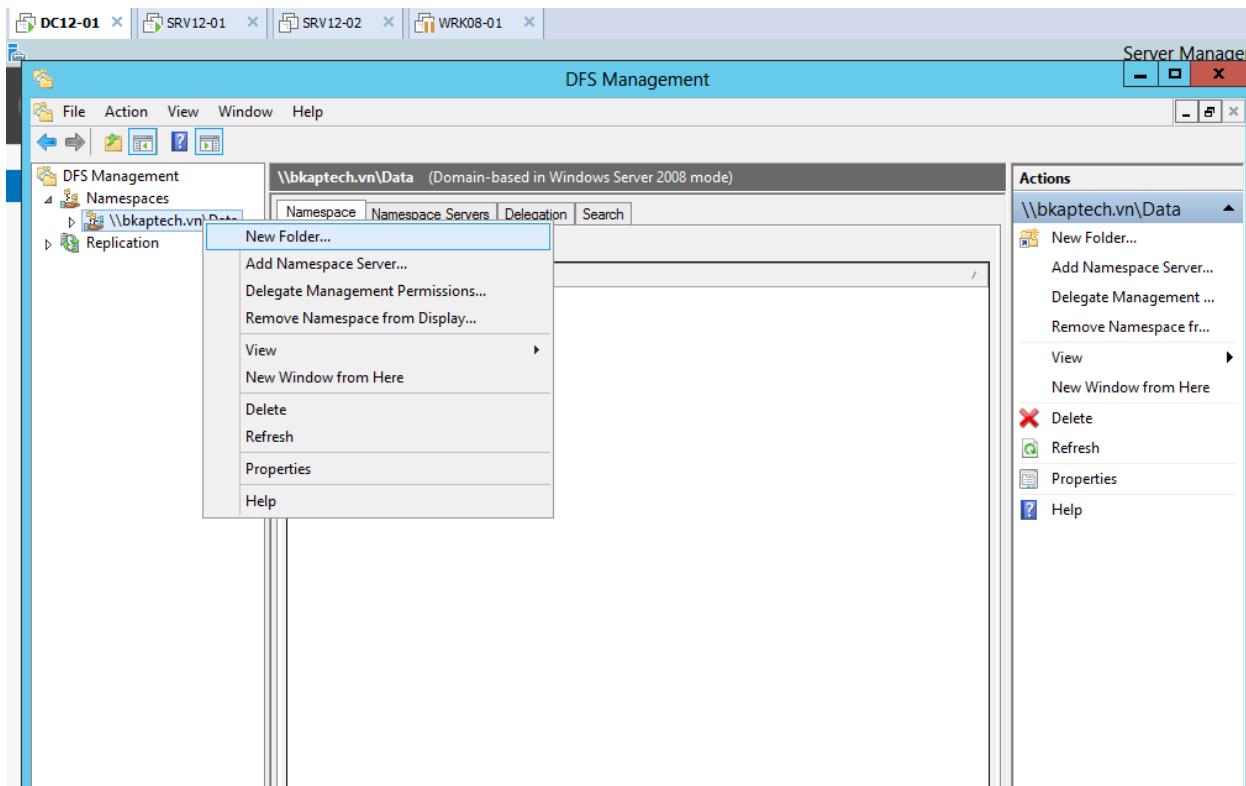


- Tại cửa sổ **Namespace Name and Settings**, nhập vào:
 - Name : *Data*
- **Next , Create.**

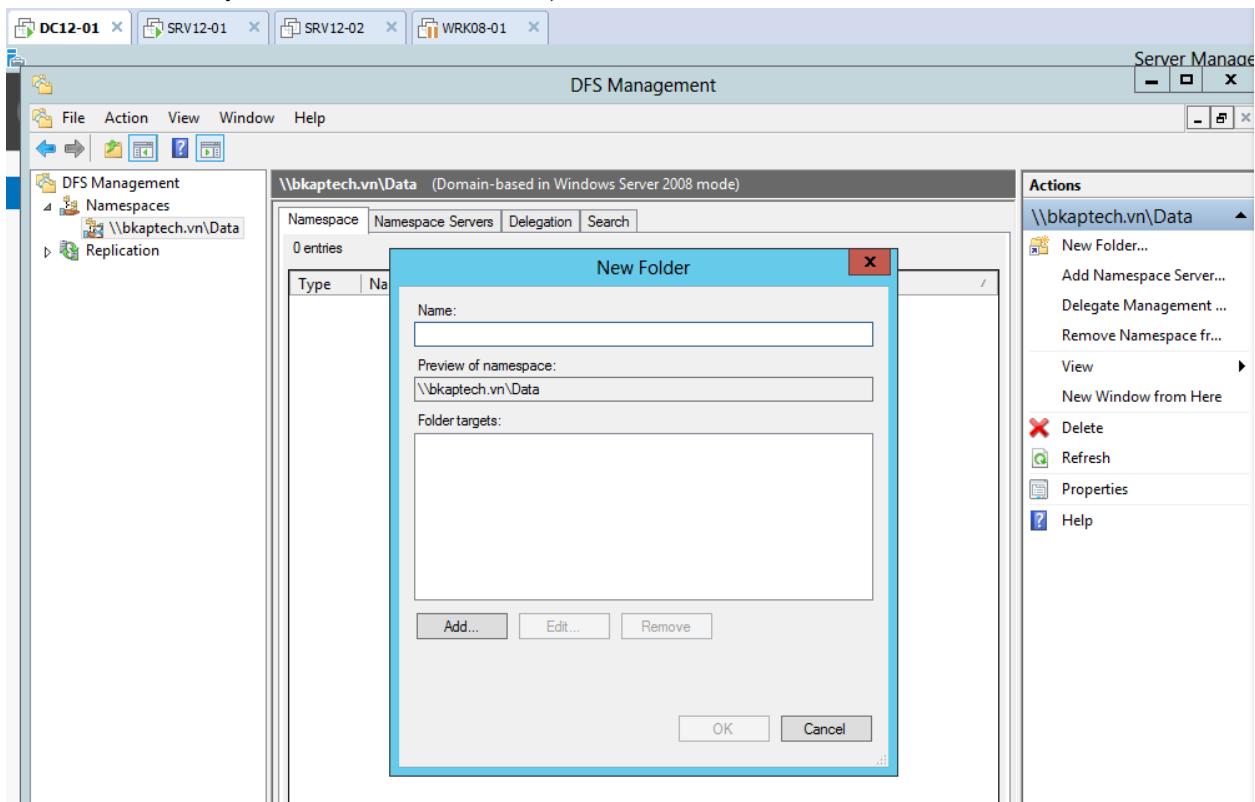




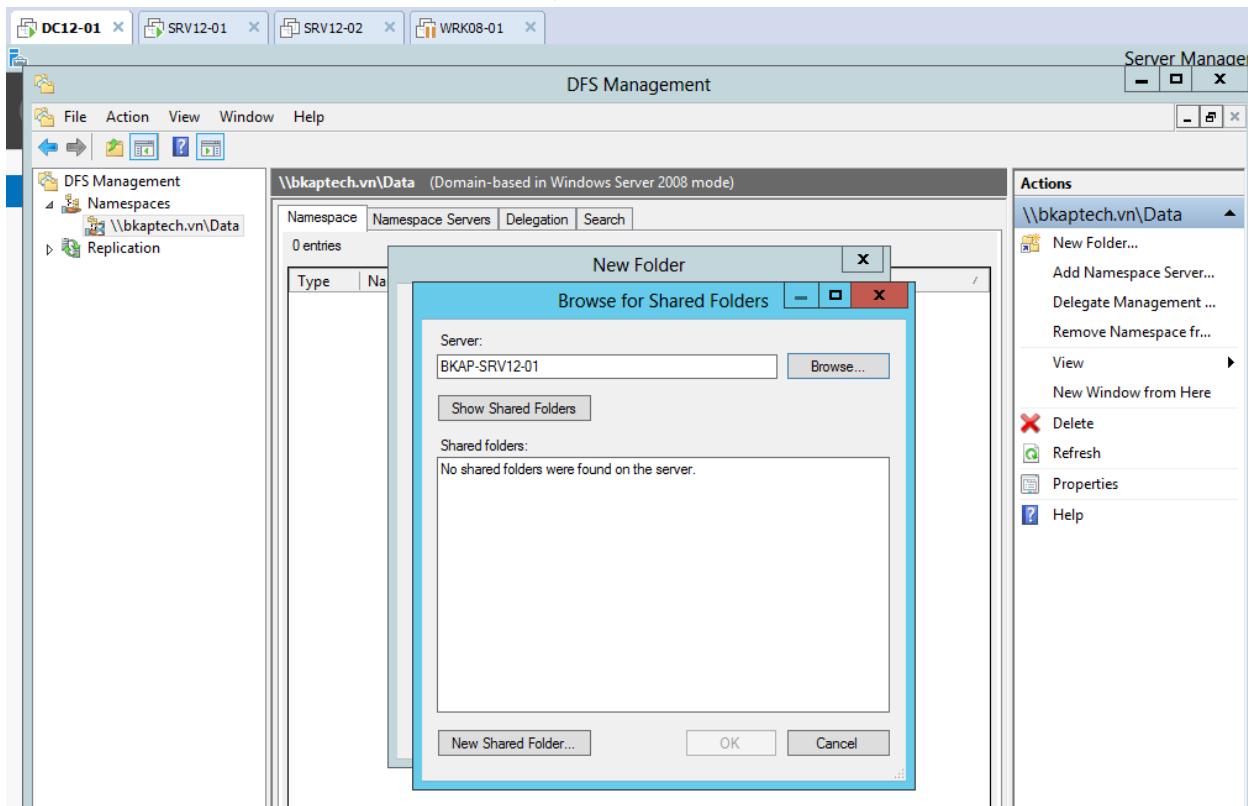
- Tại Namespaces / \\bkaptech.vn\Data , click chuột phải chọn New Folder...



- Tại cửa sổ **New Folder**, click vào **Add...**

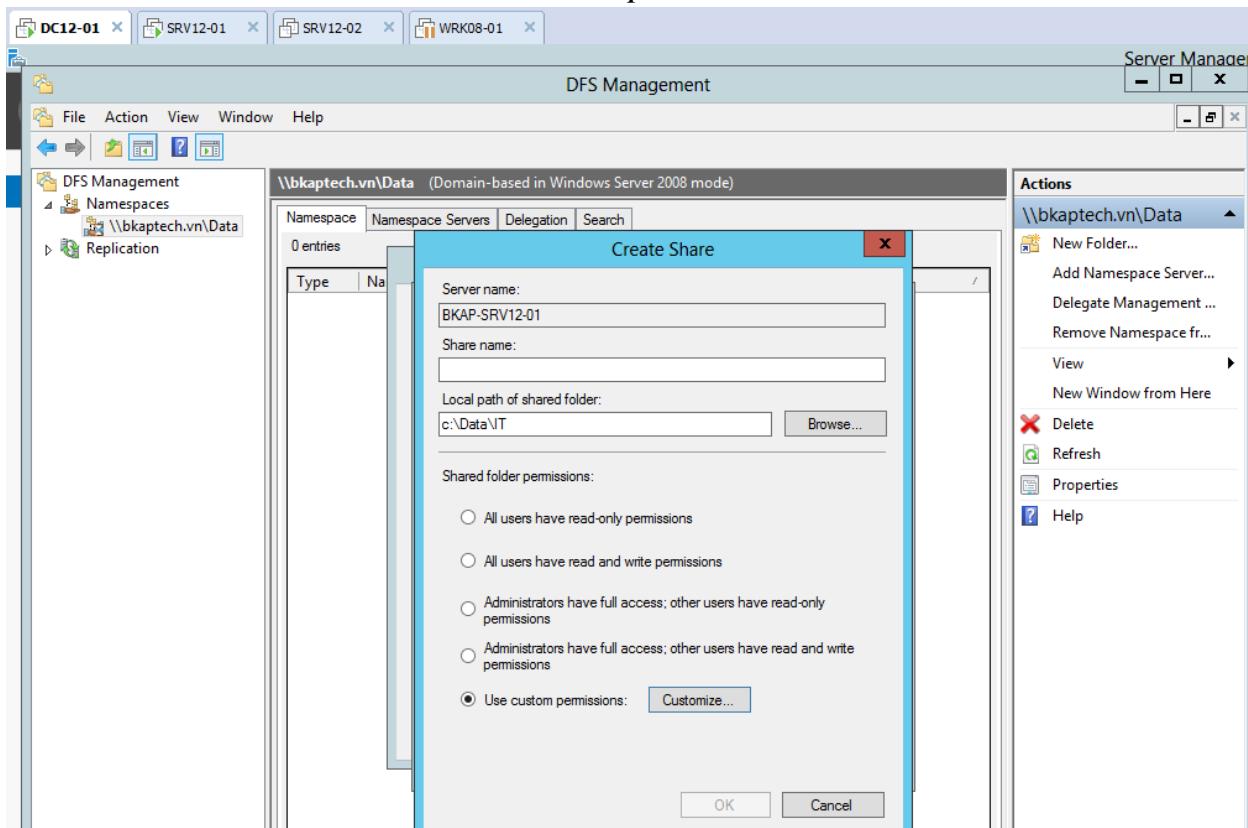


- Tại cửa sổ **Add Folder Target**, Click vào **Browse...**
 - Tại cửa sổ **Browse for Shared Folders**, **Browse...** đến máy **BKAP-SRV12-01**, click vào **New Shared Folder...**

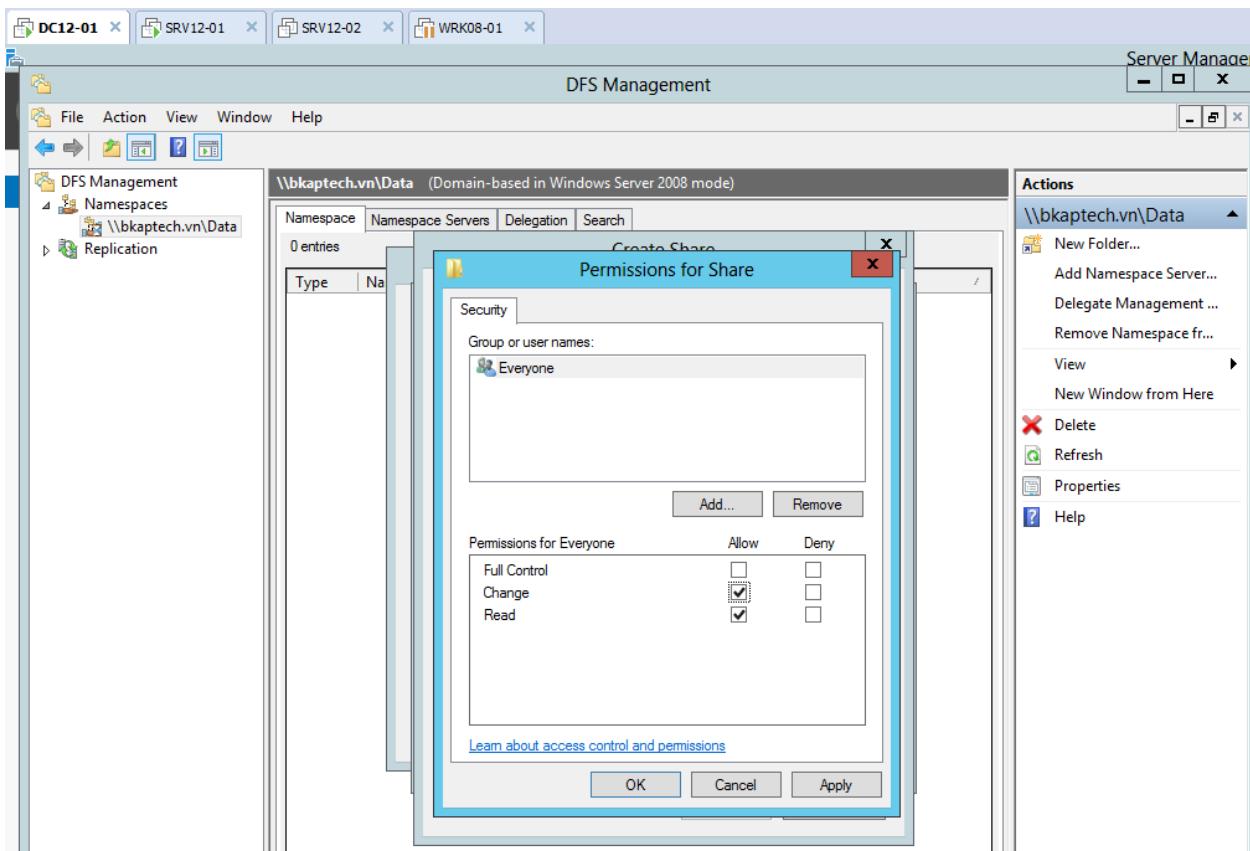


- Tại cửa sổ **Create Share**:

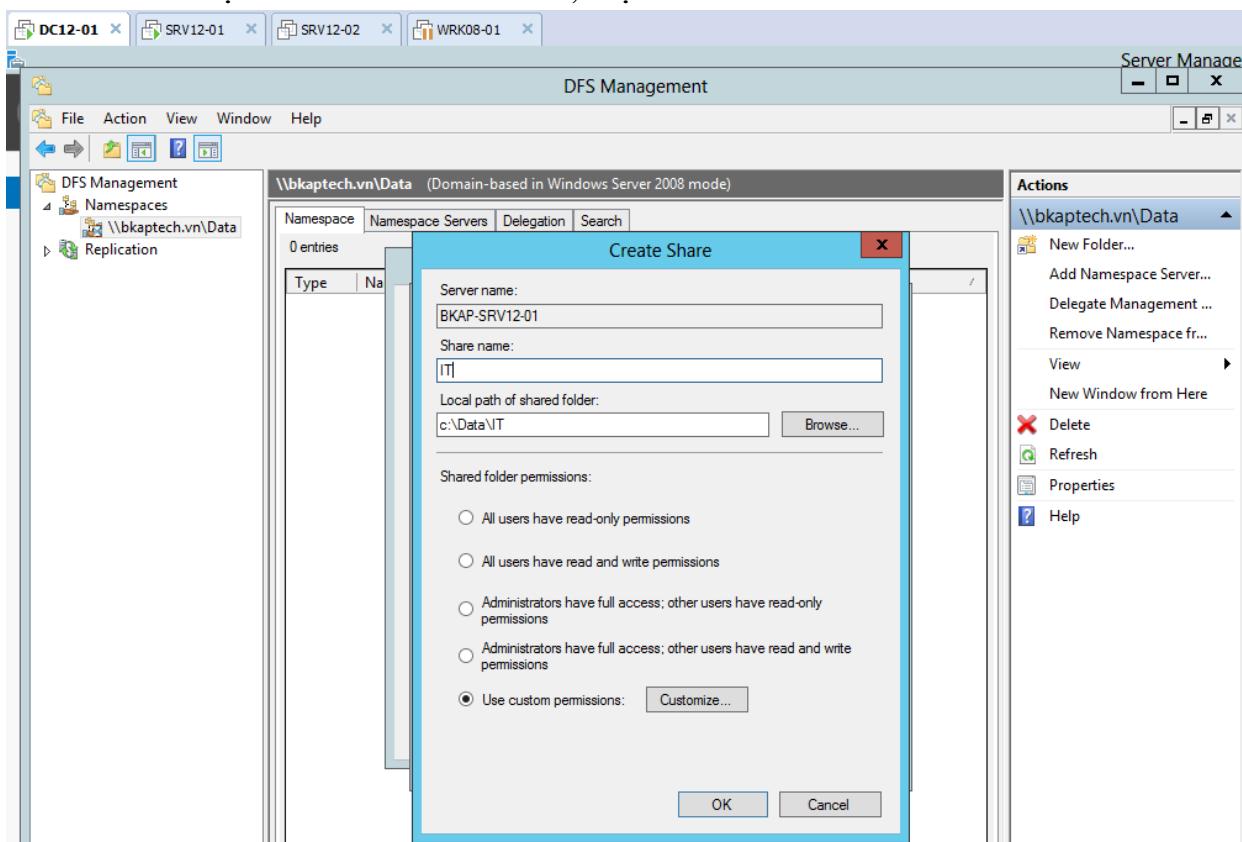
- *Local path of shared folder : Browse... đến thư mục IT*
- Click vào *Use custom permissions: Customize*



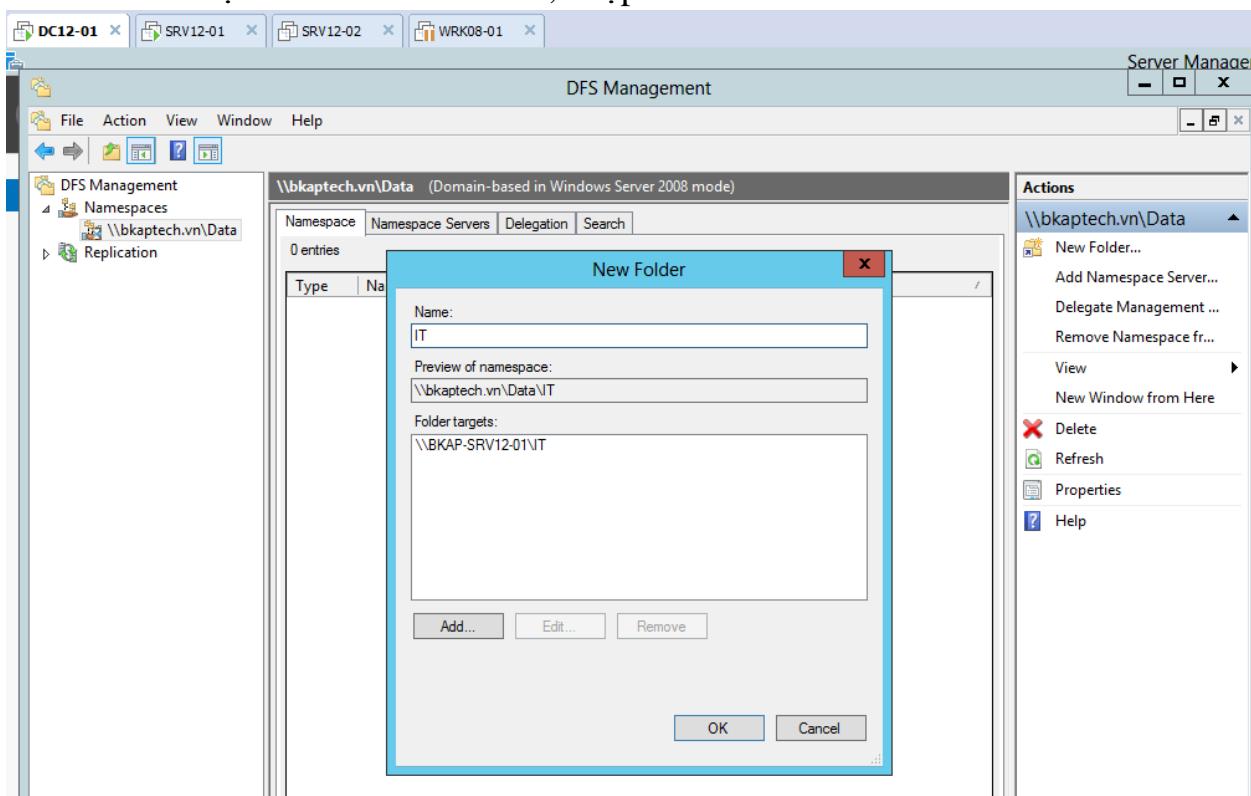
- Tại cửa sổ **Permissions for Share**, chọn vào 2 quyền *Change* và *Read*.



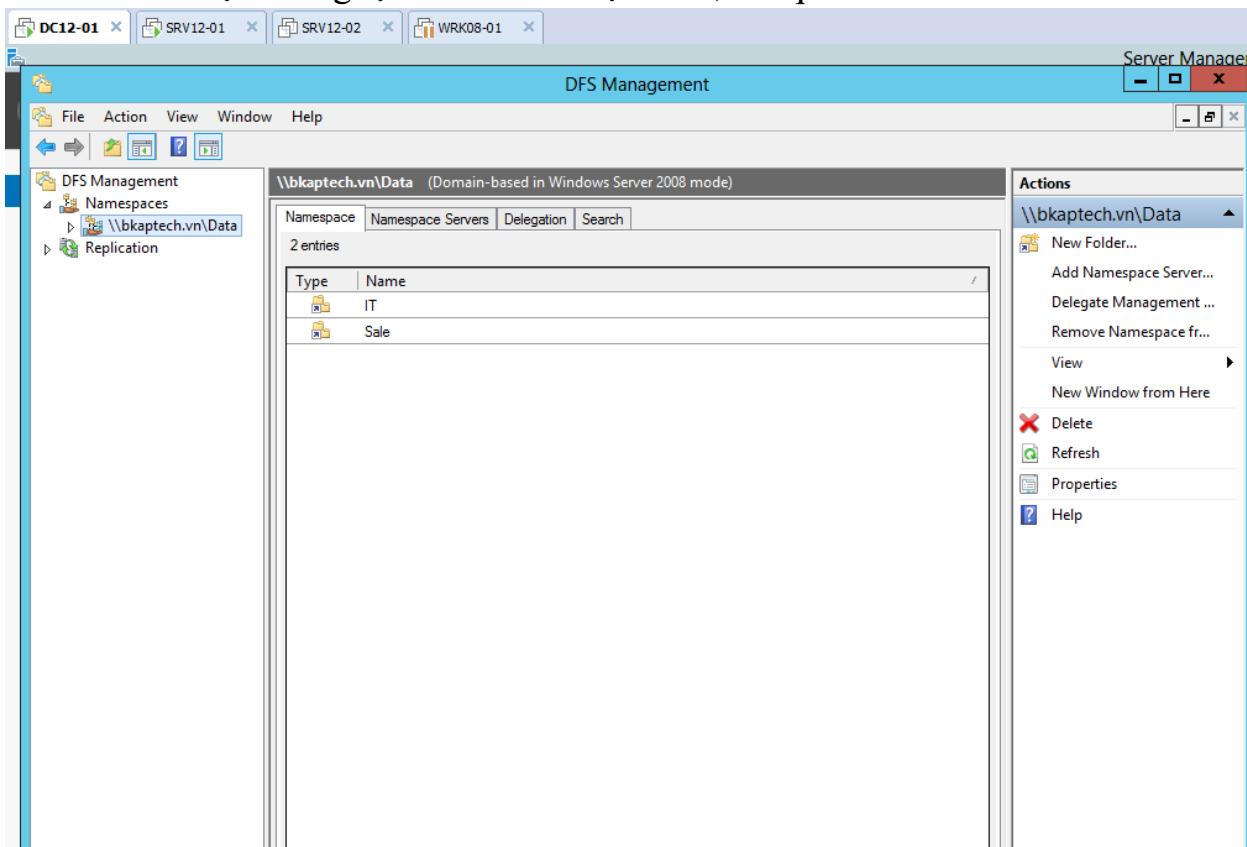
- Tại cửa sổ *Create Share*, mục *Share name : IT*



- Tại cửa sổ **New Folder**, nhập vào *Name : IT*

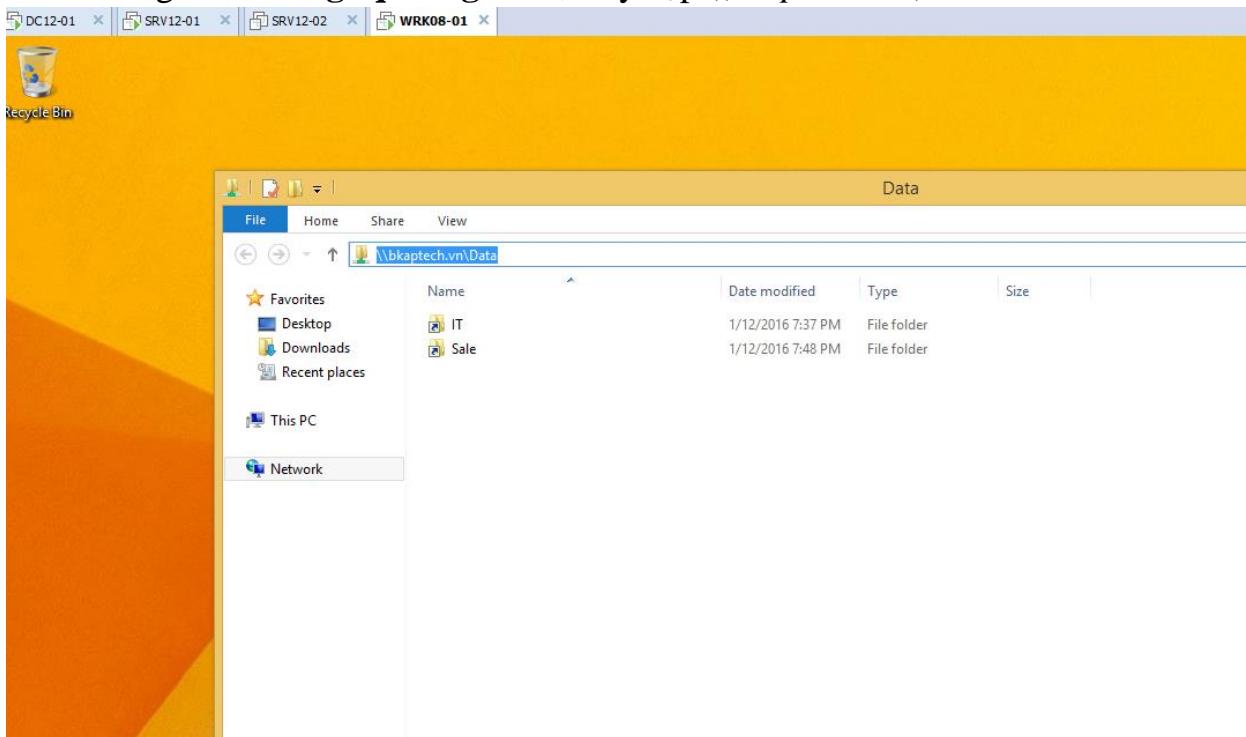


- Tạo tương tự đối với thư mục *Sale*, kết quả như sau:



- Chuyển sang máy *BKAP-SRV12-01*, cấu hình phân quyền và chia sẻ thư mục.

- Chuyển sang máy BKAP-WRK08-01, **Join vào Domain**, đăng nhập lần lượt bằng User **hungnq** và **nghialv**, truy cập **\bkaptech.vn\Data** để kiểm tra.



10.3 Đóng bộ dữ liệu trên 2 Server sử dụng DFS Replication.

1. Yêu cầu bài Lab:

+ Thiết lập **DFS Namespace** và đồng bộ thư mục theo mô hình Lab 10.2.

+ Trên máy **BKAP-DC12-01**:

- Domain Controller : **bkaptech.vn**.
- DNS Server : **bkaptech.vn**.
- Cài đặt **DFS Namespace** và **DFS Replication**.
- Tạo **DFS Namespace** chia sẻ tài nguyên với tên **\bkaptech.vn\Data**

+ Trên máy **BKAP-SRV12-01**:

- Cài đặt dịch vụ **DFS Namespace** và **Replication**.

+ Trên máy **BKAP-SRV12-02**:

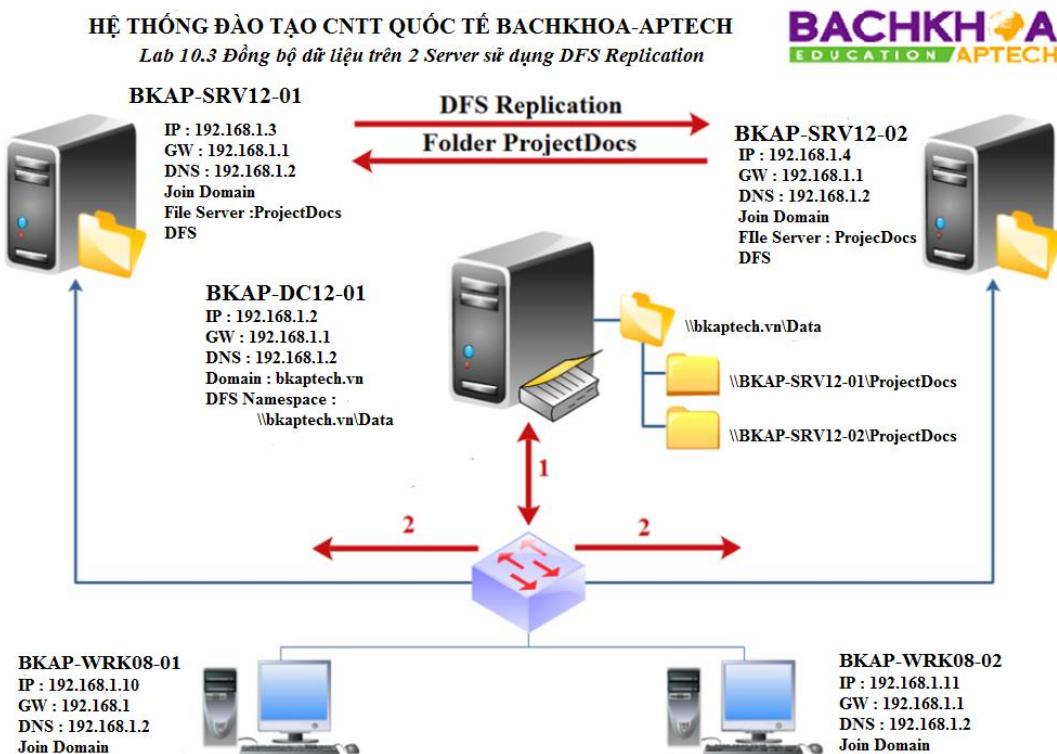
- Cài đặt dịch vụ **DFS Namespace** và **Replication**.

+ Trên máy **BKAP-WRK08-01**, truy cập dữ liệu thành công với tên **\bkaptech.vn\Data**, kiểm tra đồng bộ thư mục.

2. Yêu cầu chuẩn bị:

- + Máy server *BKAP-DC12-01* đã nâng cấp lên *Domain Controller* quản lý miền *bkaptech.vn* và cài đặt DNS Server.
- + Máy server *BKAP-SRV12-01* và *BKAP-SRV12-02* Join vào Domain.
- + Máy Client *BKAP-WRK08-01* Join vào Domain.

3. Mô hình Lab:



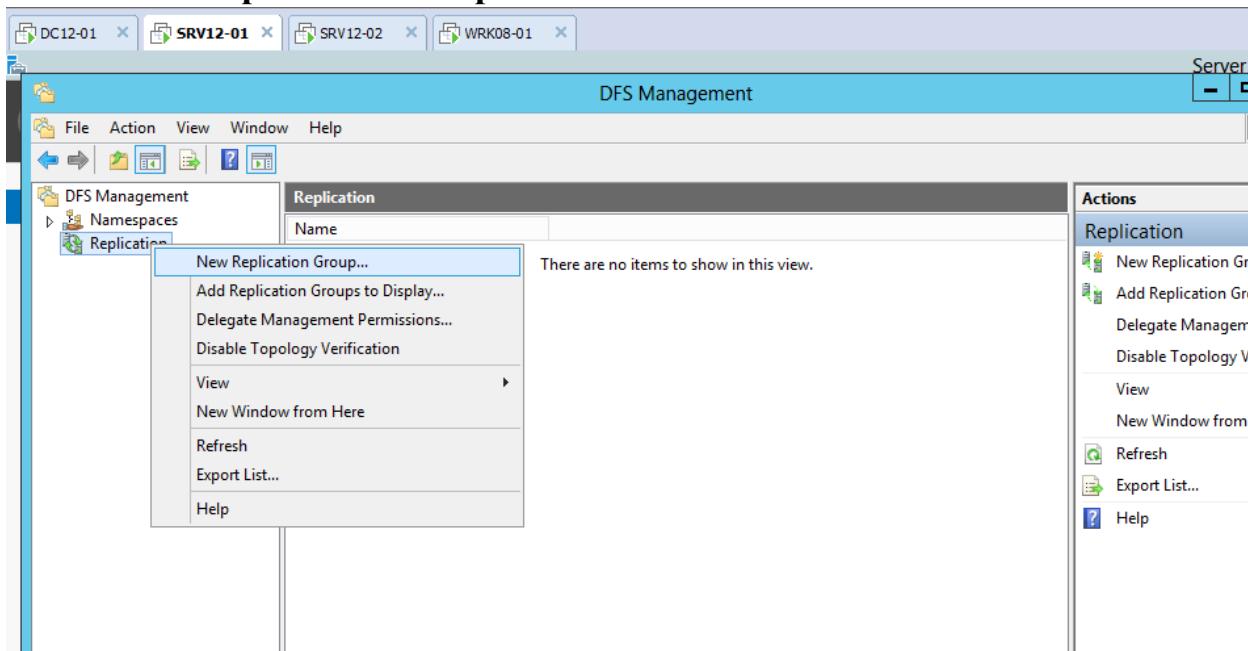
Hình 10.3

Sơ đồ địa chỉ như sau:

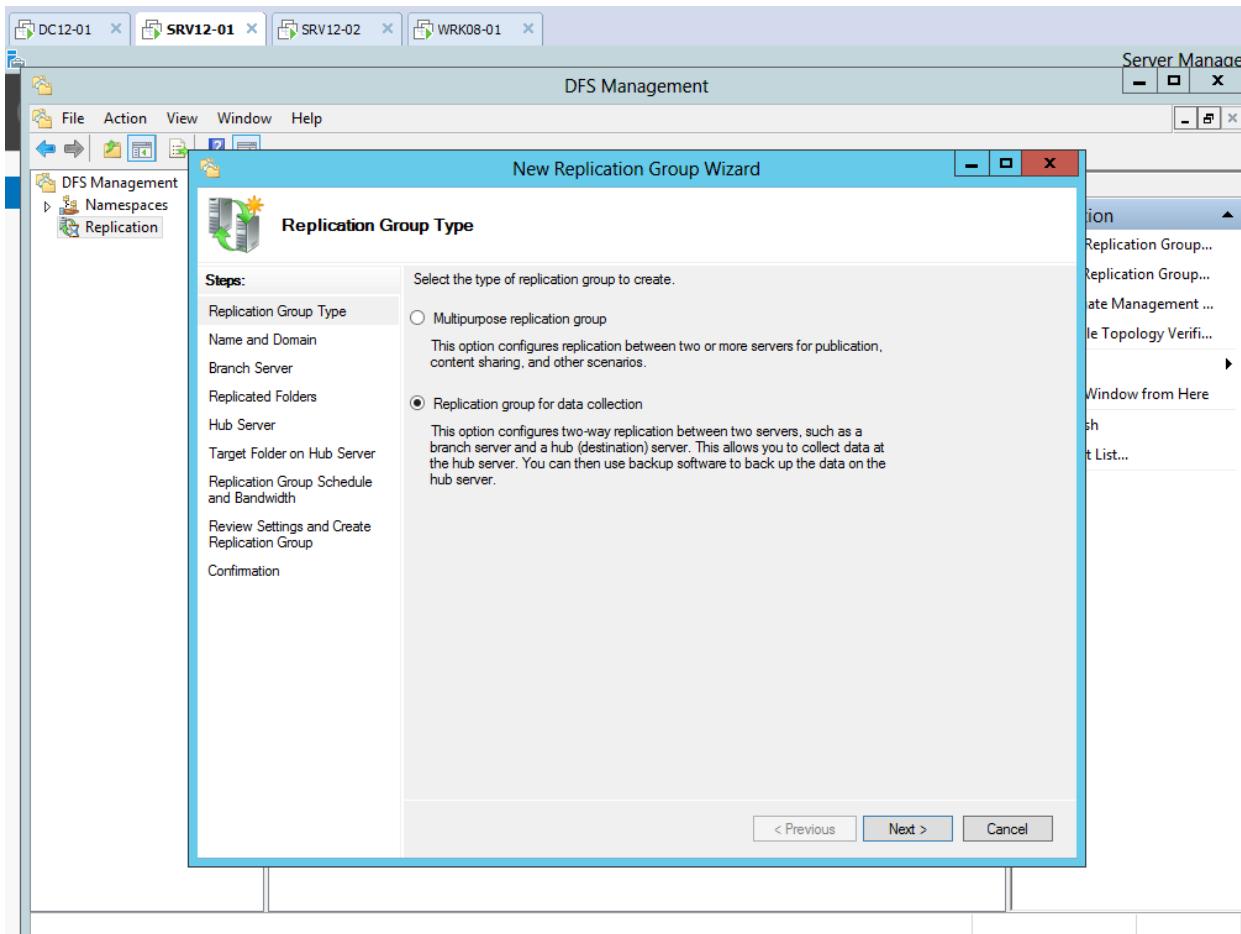
Thông số	DC12-01	SRV12-01	SRV12-02	WRK08-01
<i>IP address</i>	192.168.1.2	192.168.1.3	192.168.1.4	192.168.1.10
<i>Subnet Mask</i>	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
<i>Gateway</i>	192.168.1.1	192.168.1.1	192.168.1.1	192.168.1.1
<i>DNS Server</i>	192.168.1.2	192.168.1.2	192.168.1.2	192.168.1.2

Hướng dẫn chi tiết:

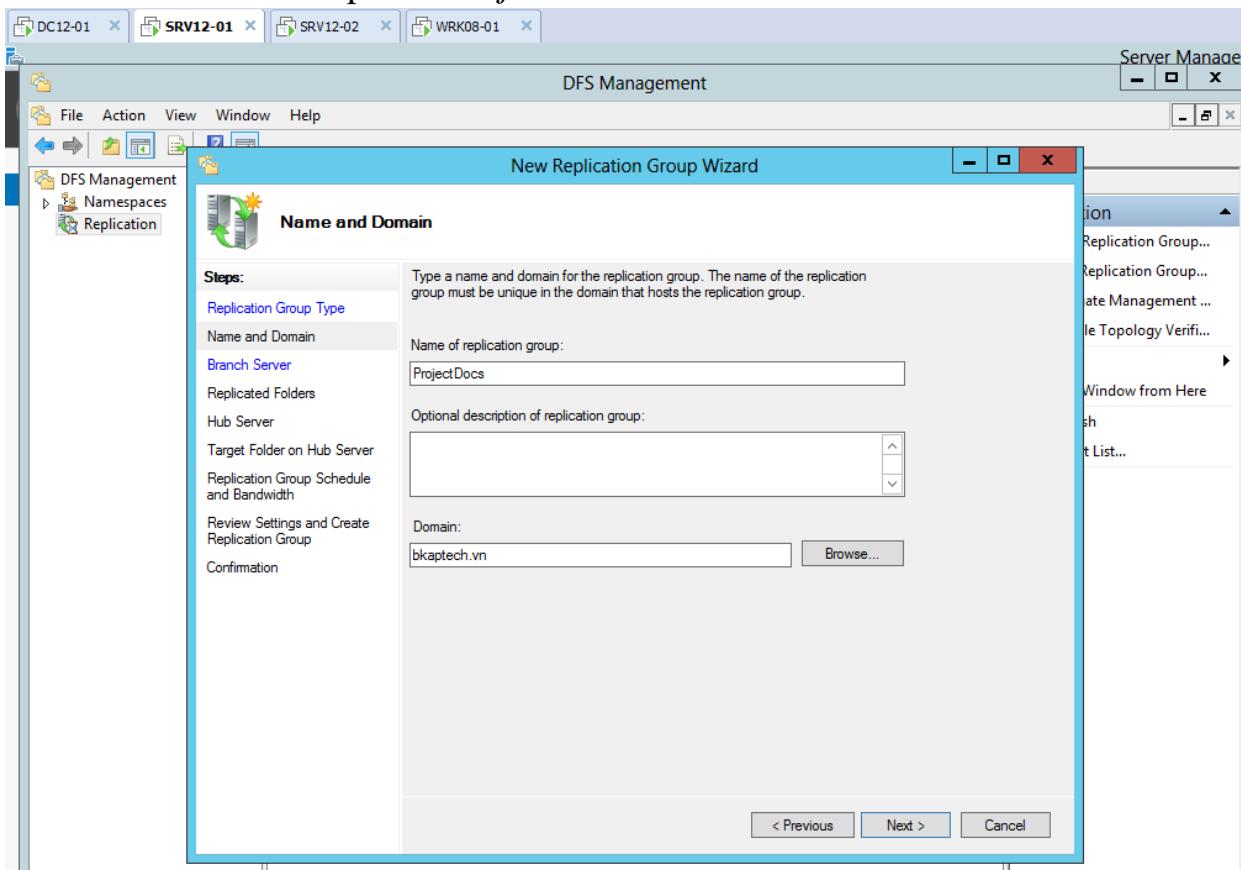
- Thực hiện cài đặt **DFS Namespace** và **DFS Replication** trên cả 3 máy *DC12-01, SRV12-01, SRV12-02*.
- Join 2 máy *SRV12-01, SRV12-02* vào Domain.
- Trên máy *BKAP-SRV12-01* :
 - Tiến hành Join vào Domain, đăng nhập bằng tài khoản **administrator**.
 - Tạo thư mục **ProjectDocs** trong ổ C.
 - Vào **DFS Management / Replication**, click chuột phải chọn **New Replication Group...**



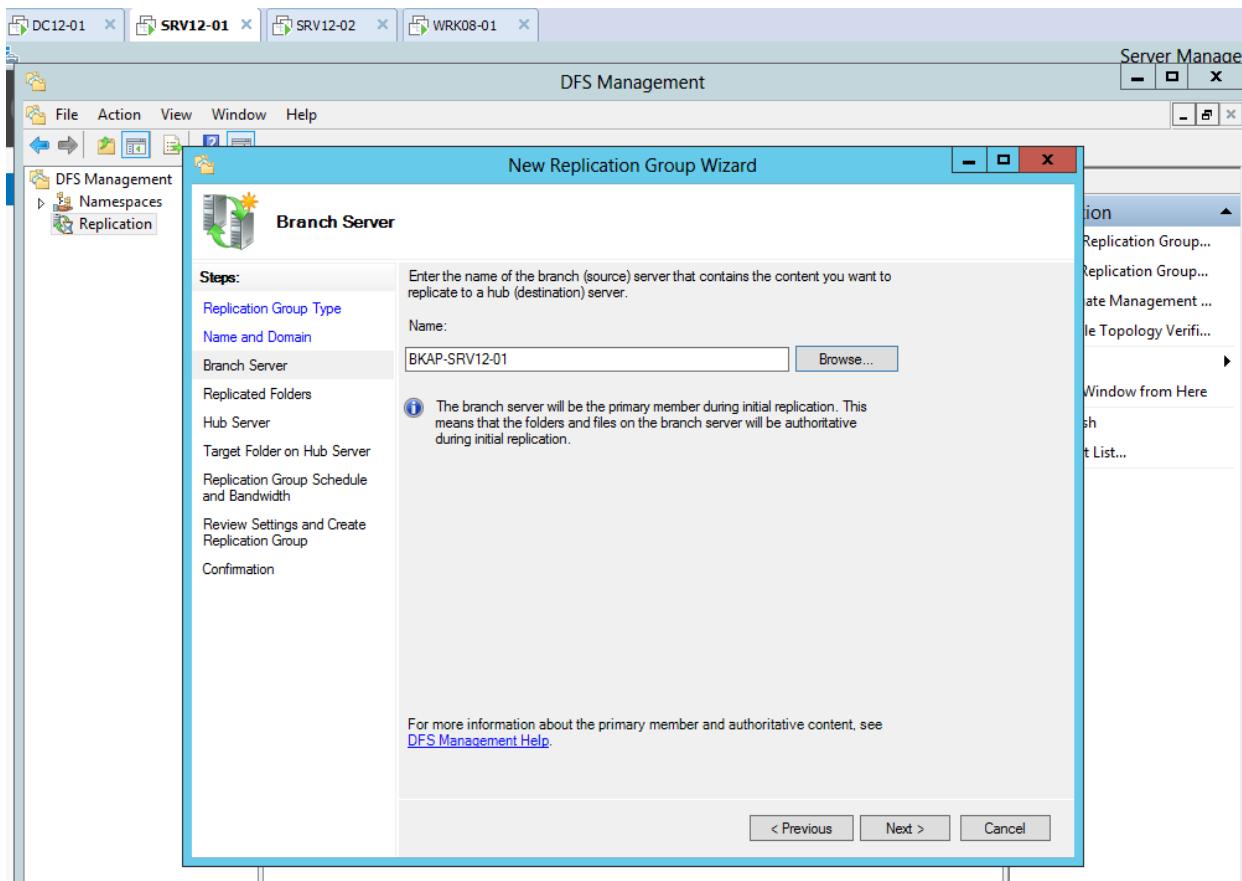
- Tại cửa sổ **Replication Group Type**, chọn **Replication group for data collection**.



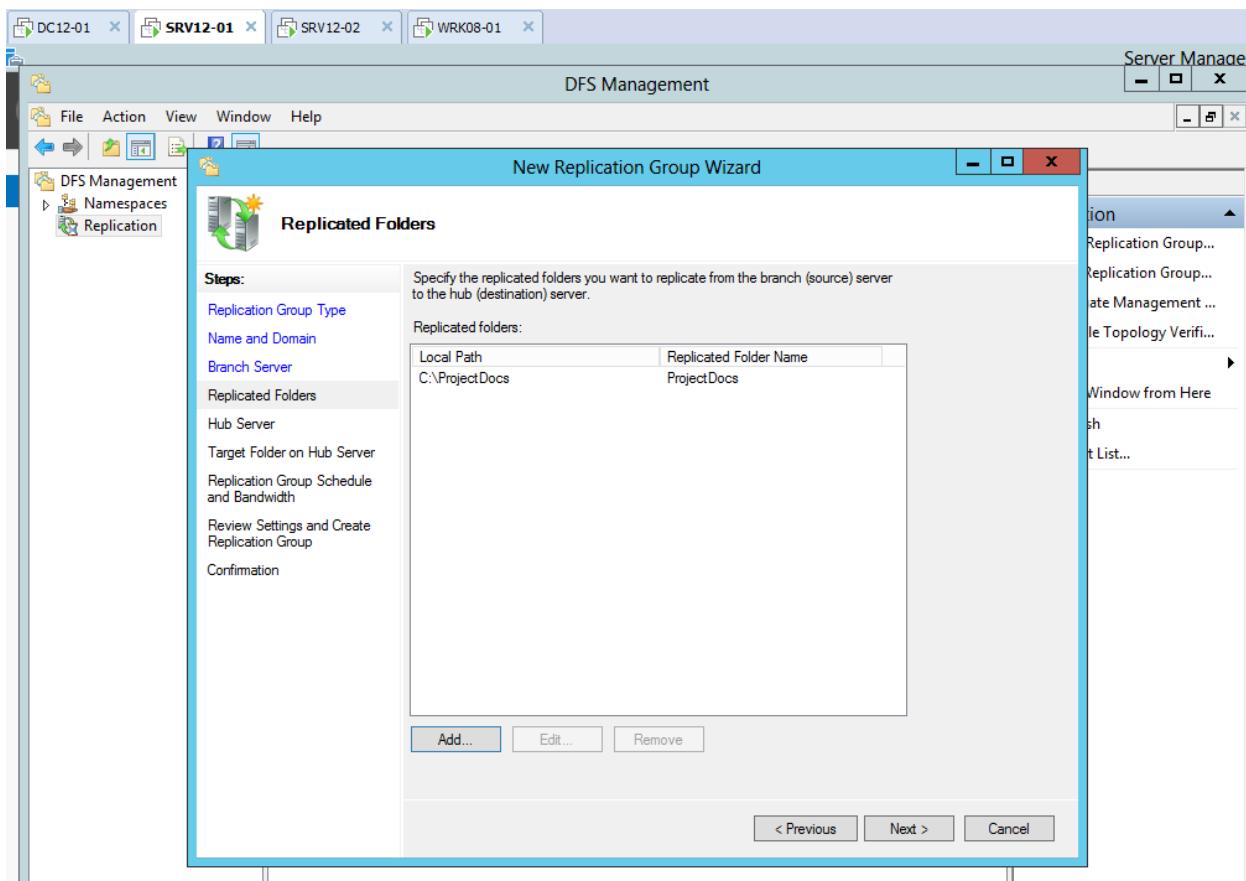
- Tại cửa sổ **Name and Domain / Name of replication group**, chỉ định tên namespace : *ProjectDocs*.



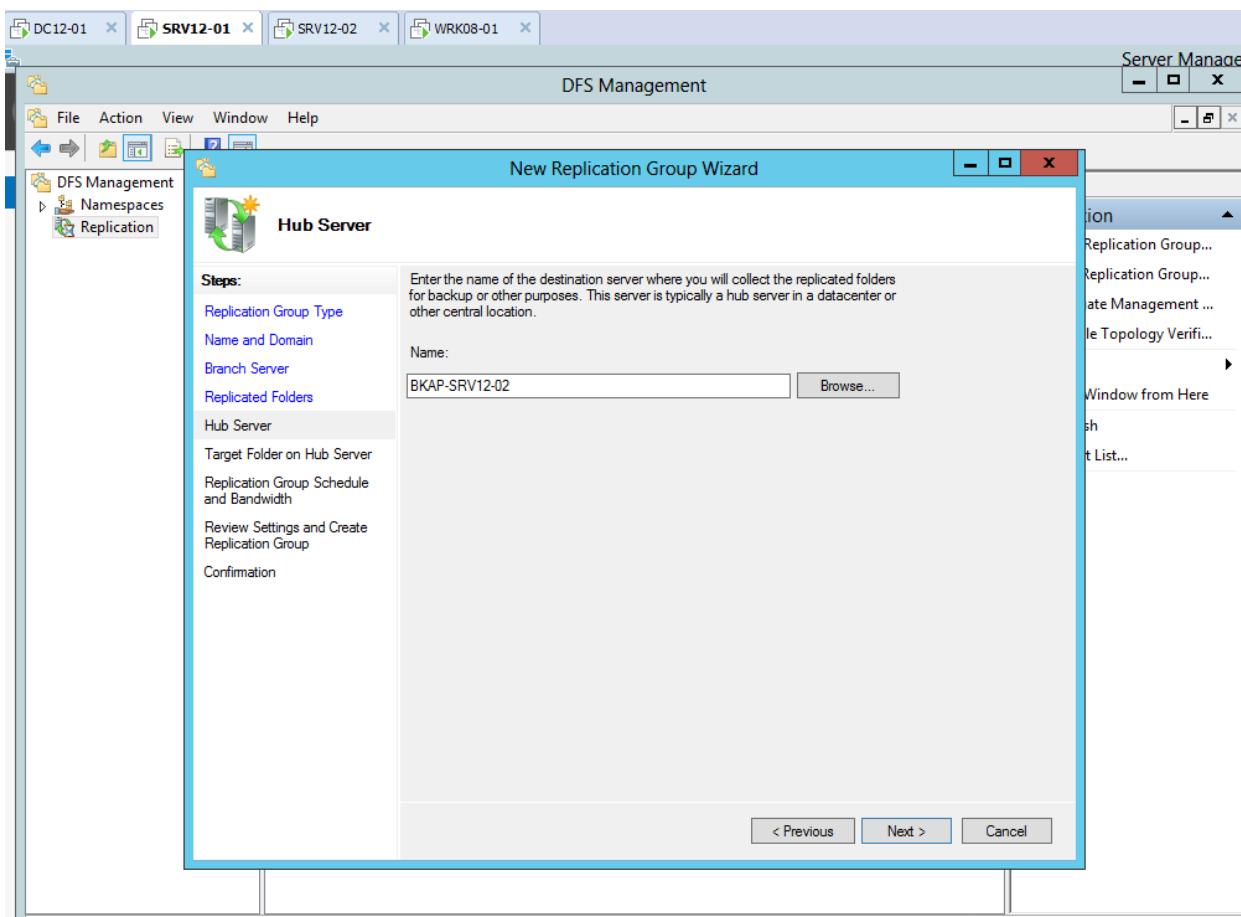
- Tại cửa sổ **Branch Server** , chọn Server cần đồng bộ :browse ... đến máy *BKAP-SRV12-01*.



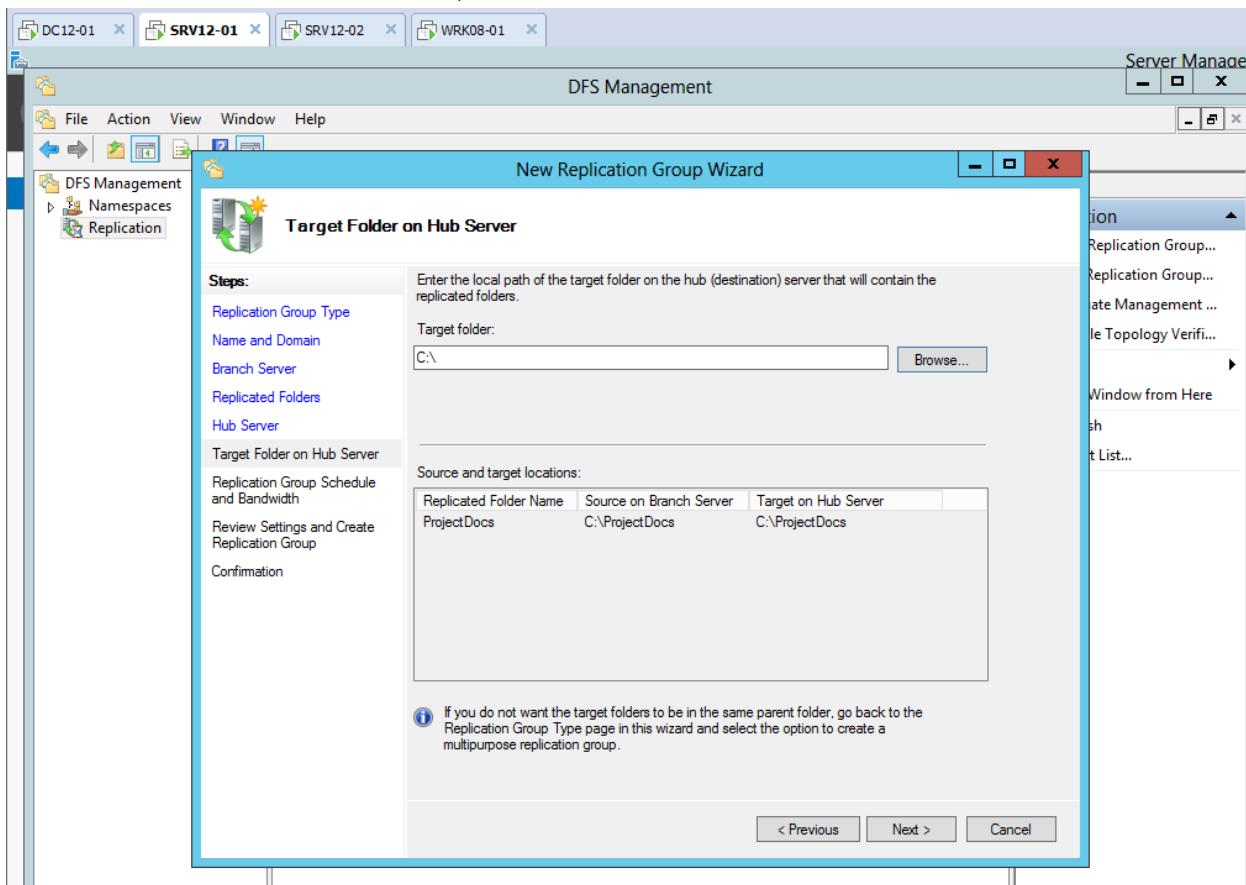
- Tại cửa sổ **Replicated Folders**, chỉ định thư mục cần đồng bộ : click vào **Add... ProjectDocs**.



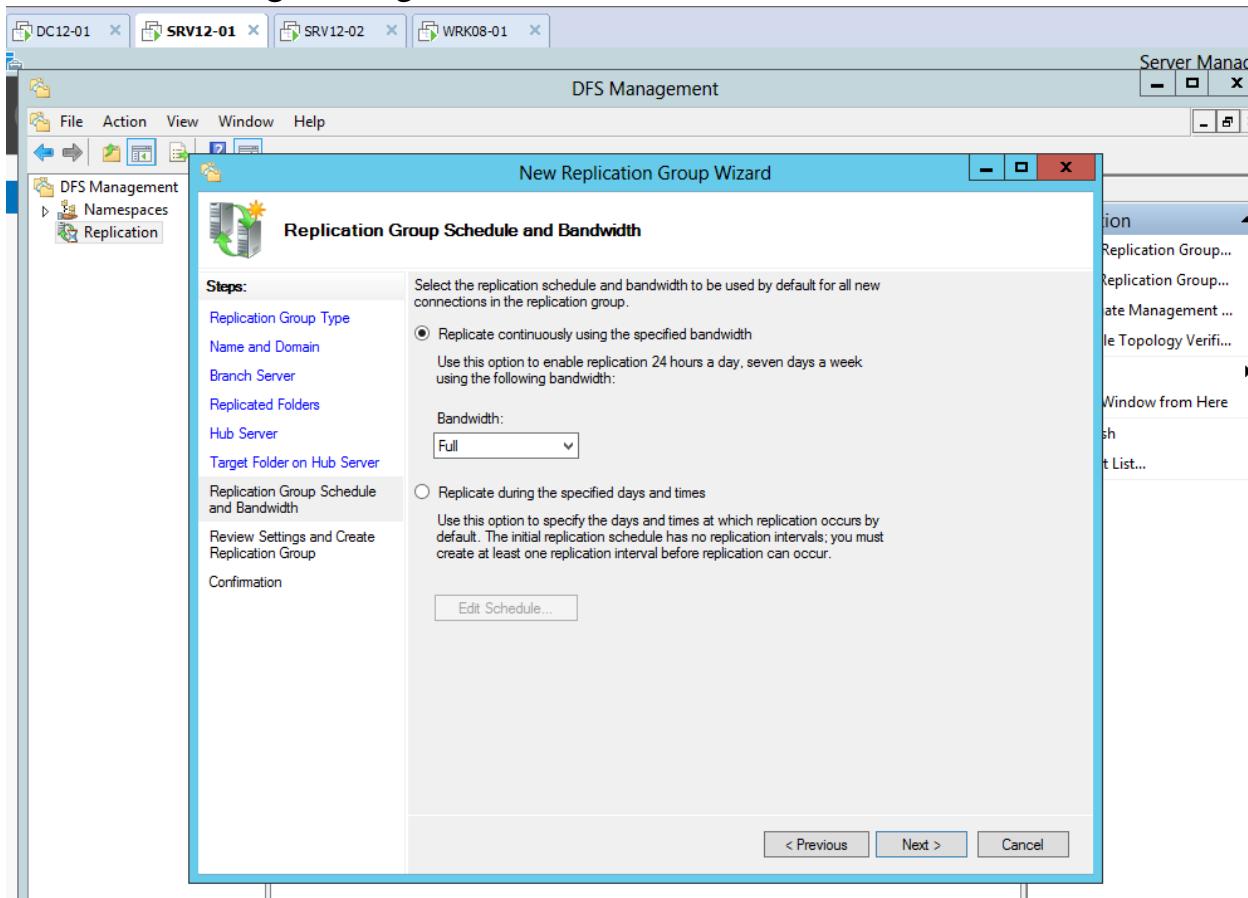
- Tại **Hub Server**, chỉ định server đích đến để đồng bộ, **Browse...** đến server *BKAP-SRV12-02*.



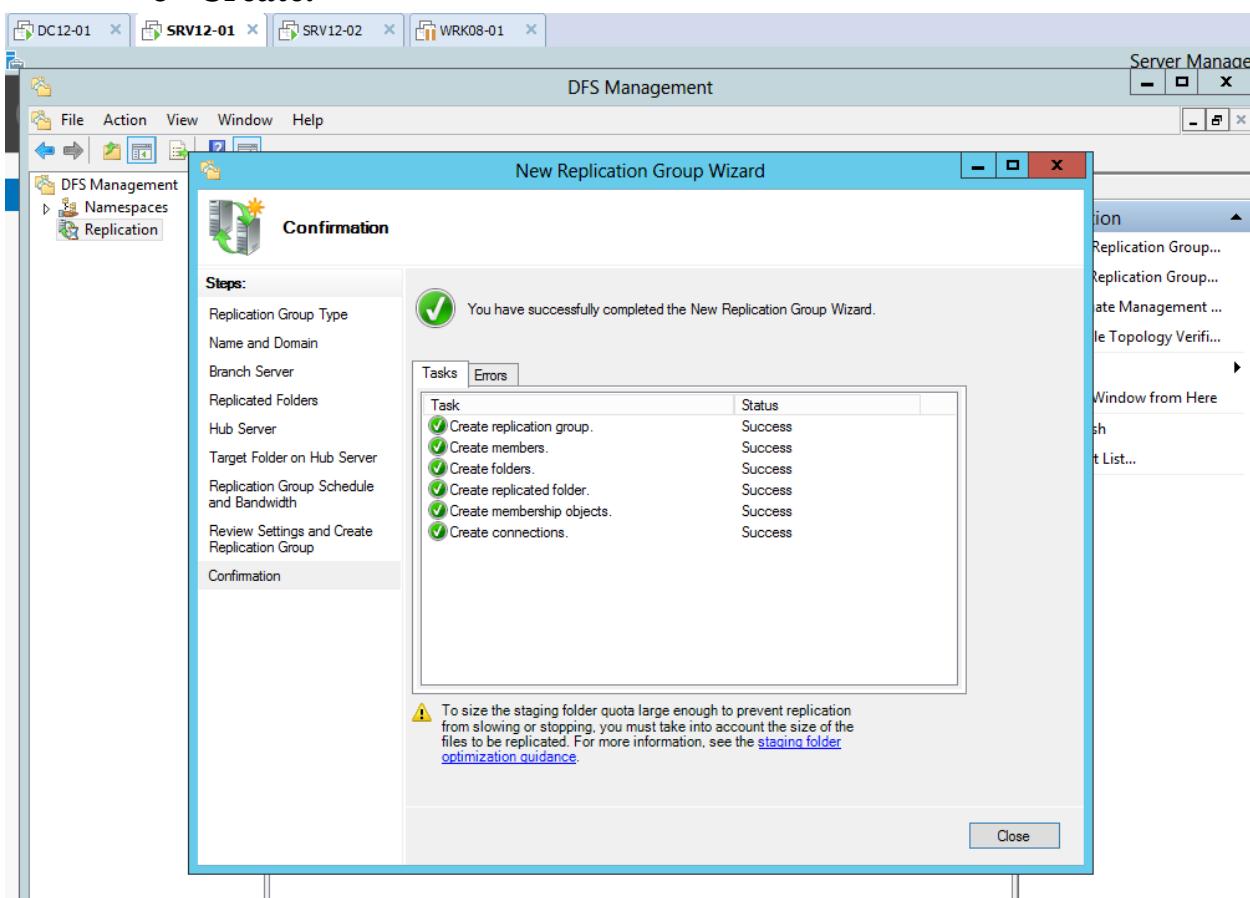
- Tại **Target Folder on Hub Server**, chỉ định thư mục đồng bộ trên **BKAP-SRV12-02**, **Browse...** đến ổ C.



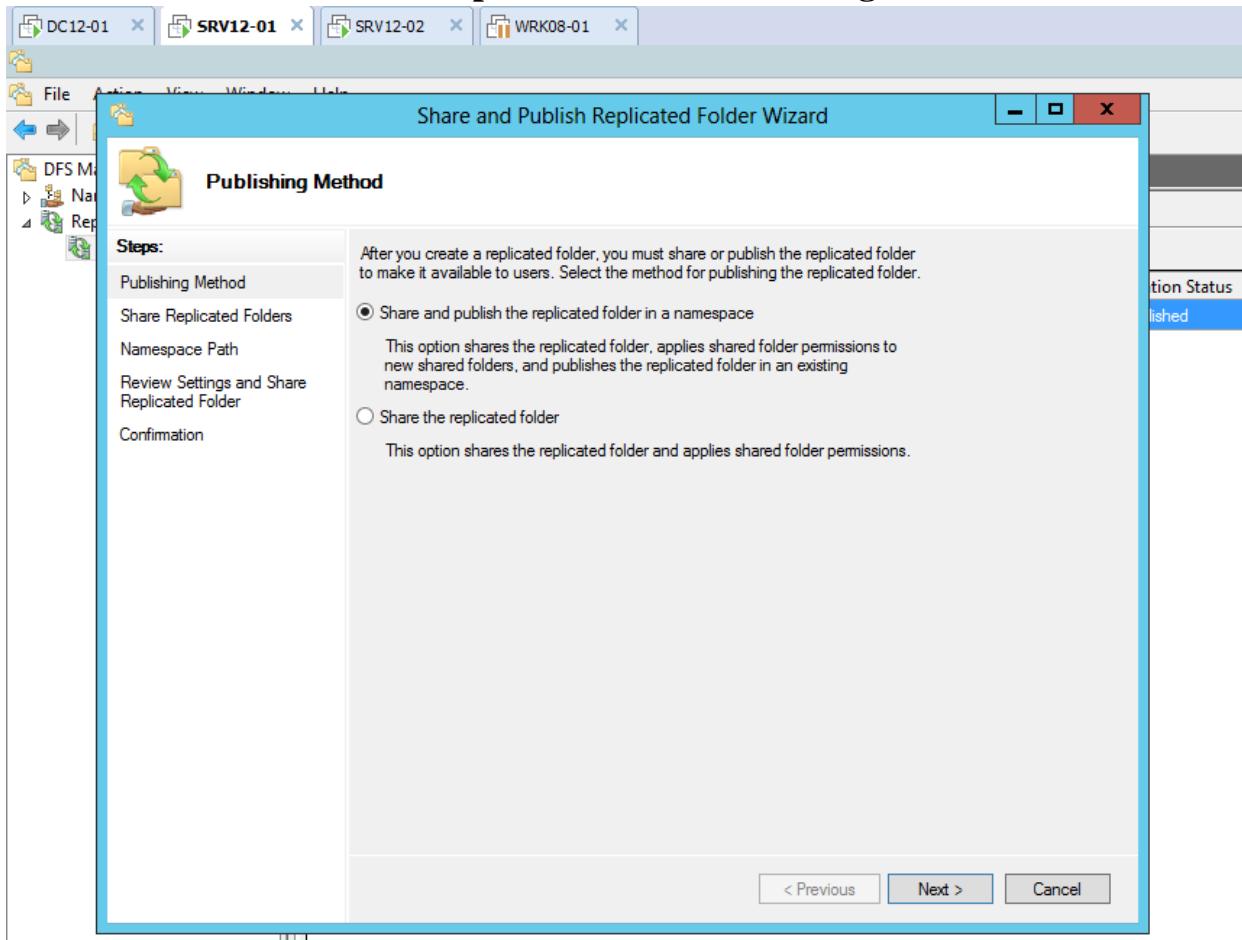
- Tại cửa sổ **Replication Group Schedule and Bandwidth**, chỉ định thời gian đồng bộ.



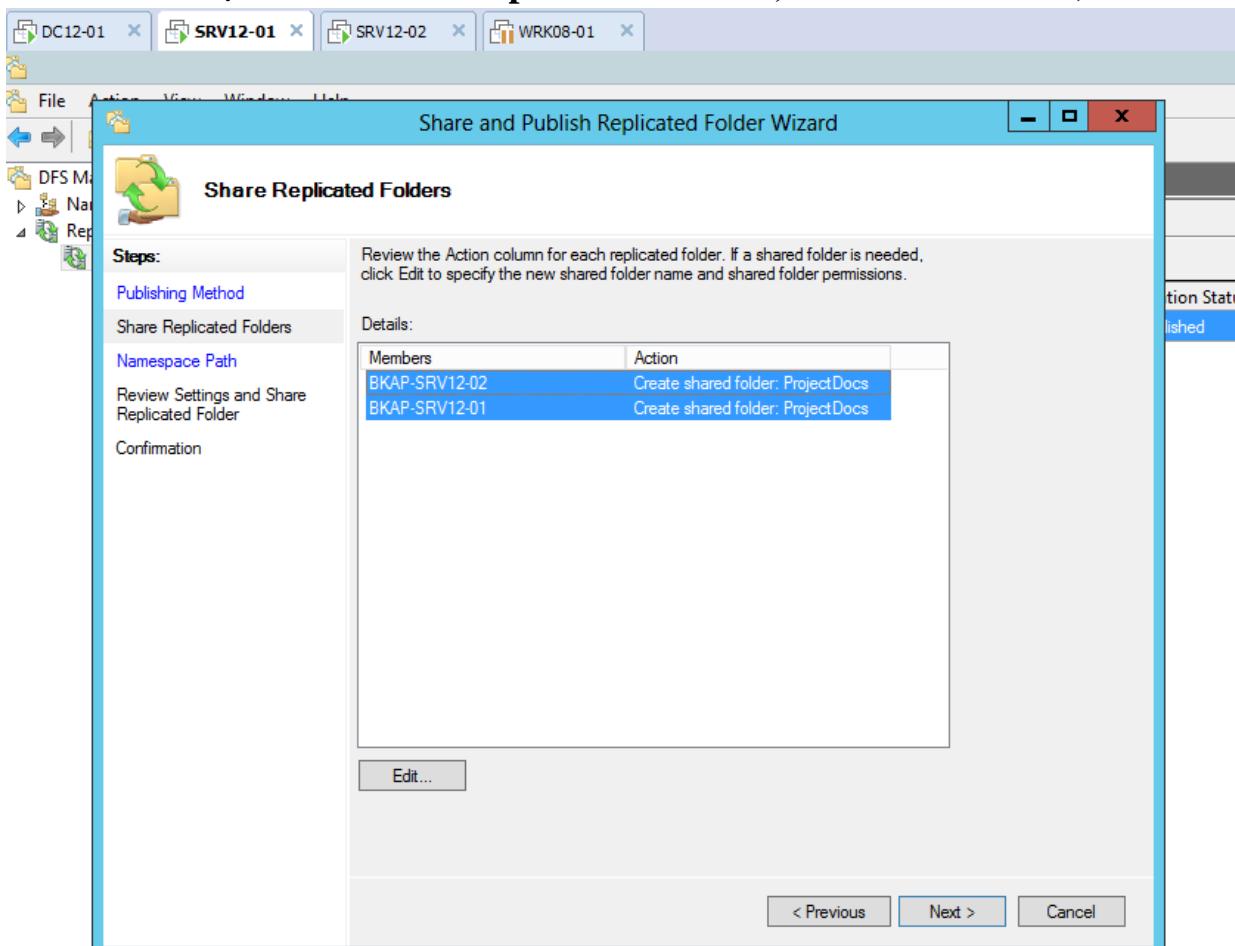
○ Create.



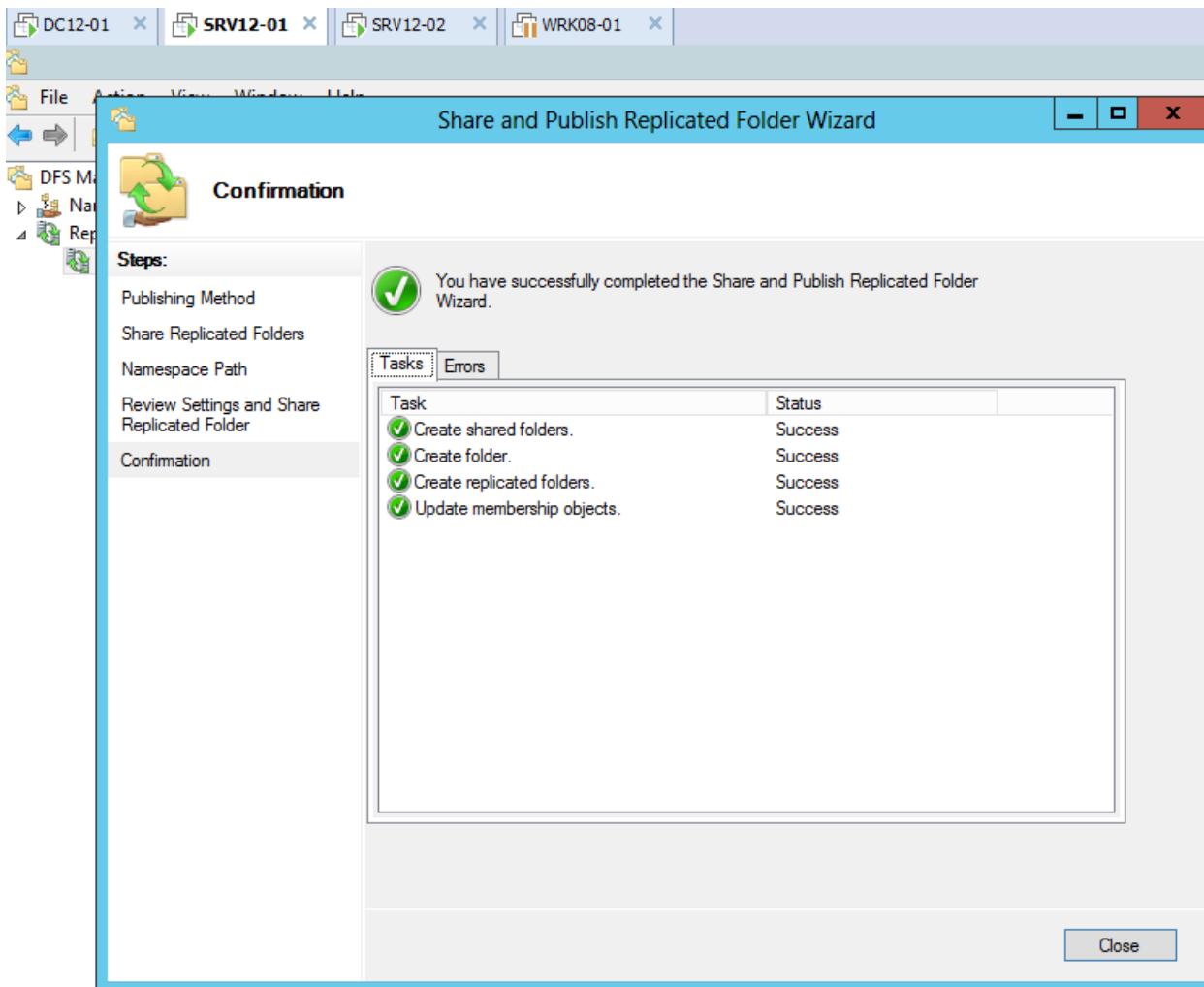
- Tại **Replication / ProjectDocs** , chuyển sang tab **Replicated Folders** , click vào **ProjectDocs** , click chuột phải chọn **Share and Publish in Namespace....** Chọn tiếp vào **Share and publish the replicated folder in a namespace** tại cửa sổ **Publishing Method**.



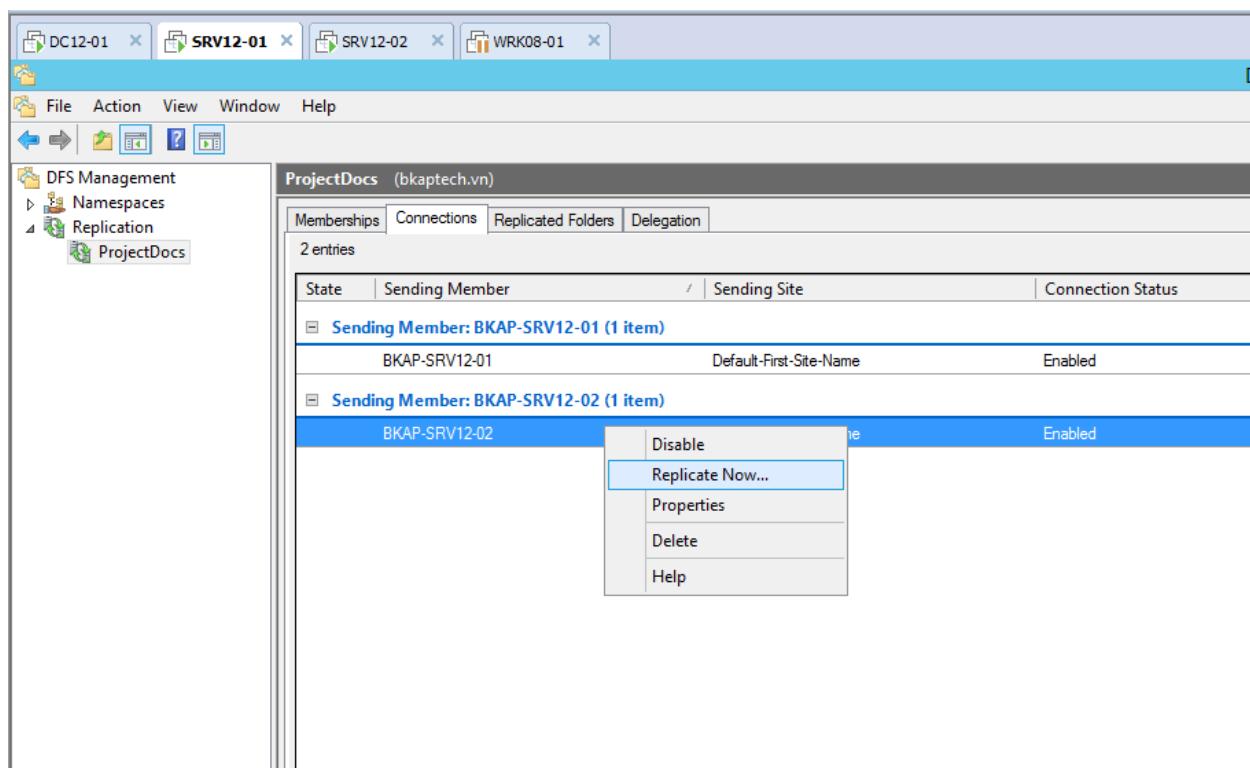
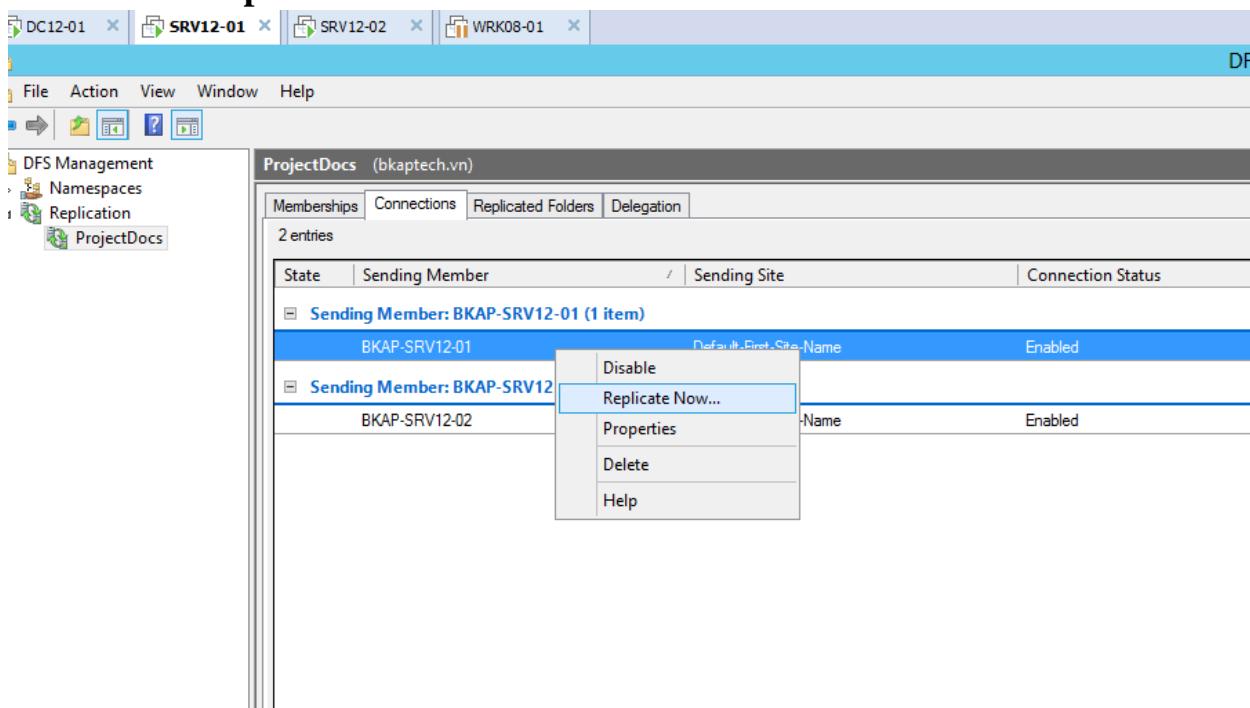
- Tại cửa sổ **Share Replicated Folders**, bôi đen cả 2 server, Next.



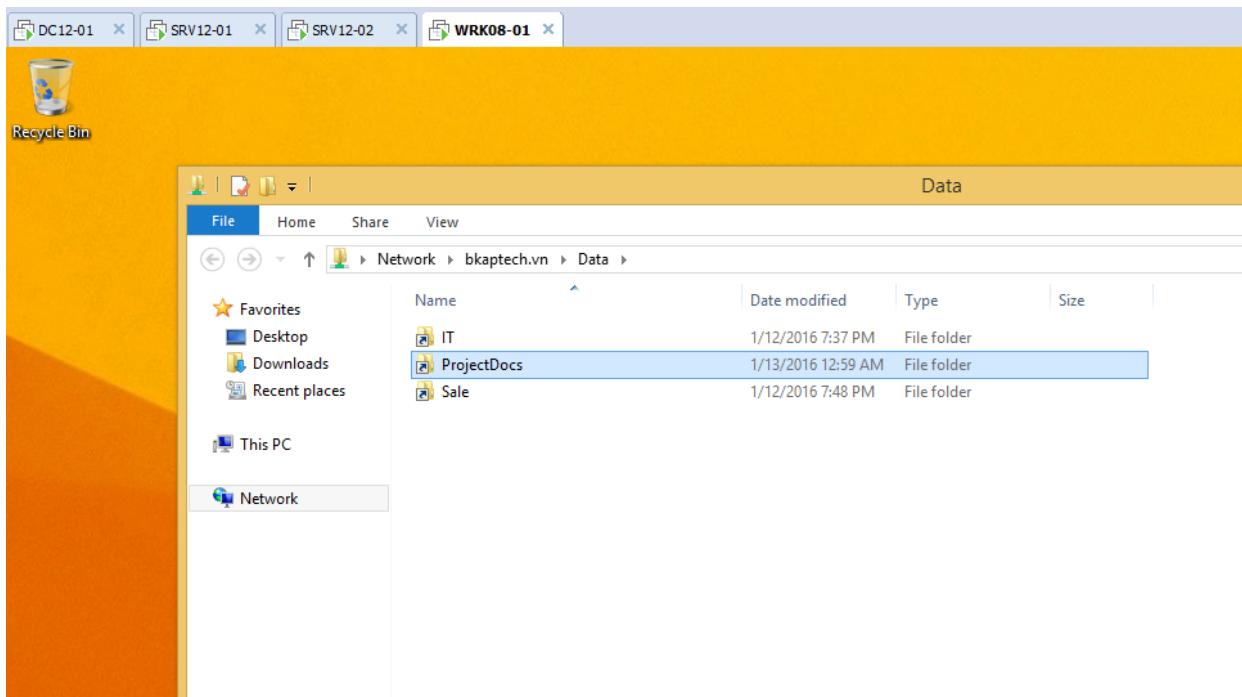
- Tại cửa sổ **Namespace Path**, chọn đường dẫn \\bkaptech\Data.
- Next / Share



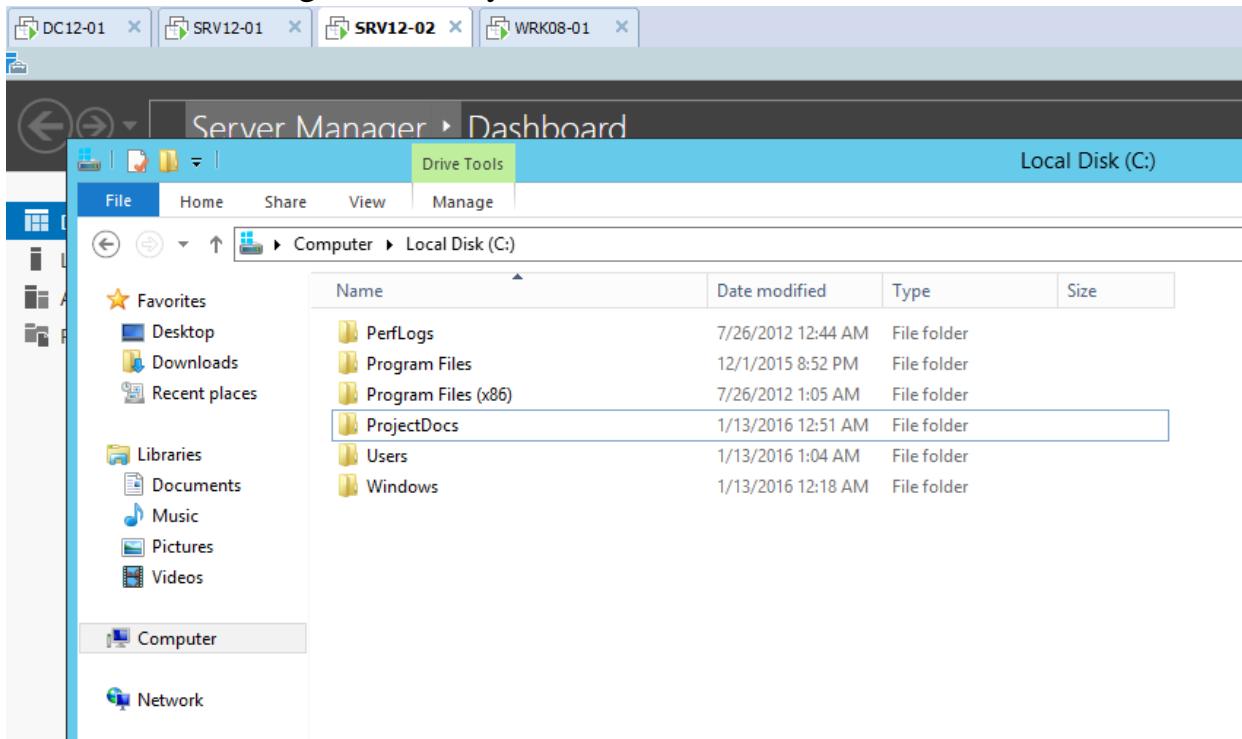
- Chuyển sang tab **Connections**, click chuột phải vào 2 Server, chọn **Replicated Now...**.



- Chuyển sang máy Client *BKAP-WKR08-01*, truy cập `\bkaptech.vn\Data` để kiểm tra.



- Kiểm tra đống bộ trên máy *BKAP-SRV12-02*.



Bài 11:**CẤU HÌNH MÃ HÓA FILE , AUDITING NÂNG CAO****Các nội dung chính sẽ được đề cập:**

- ✓ Cấu hình mã hóa file.
- ✓ Cấu hình Auditing nâng cao.

11.1 Cấu hình mã hóa File.**1. Yêu cầu bài Lab:**+ Trên Server **BKAP-DC12-01**:

- **Domain Controller** quản lý miền **bkaptech.vn** và cài đặt **DNS Server**.
- Cài đặt **CA Server**.
- Xóa **key Public** mặc định trong chính sách của **Domain**.
- Tạo thư mục chia sẻ.

+ Trên máy **Client**:

- Xin **key Public** cho người dùng
- Truy cập thư mục và mã hóa file.

Kiểm tra sau khi thiết lập:

- Sử dụng **tài khoản khác** để mở **File** đã mã hóa.

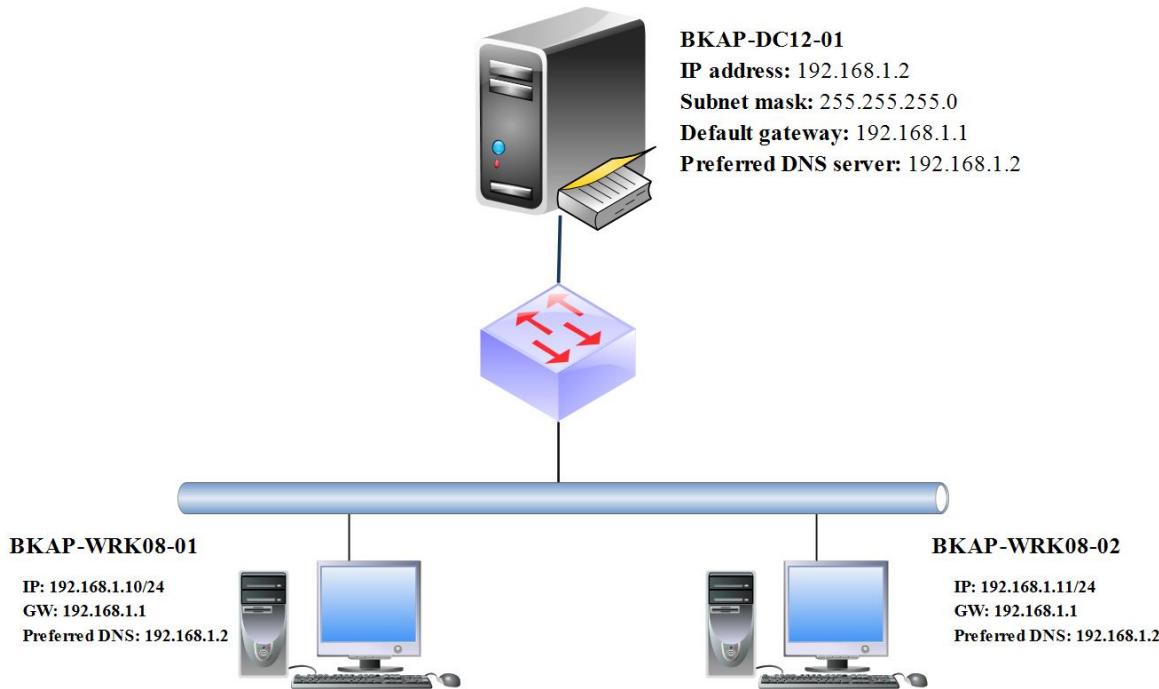
2. Yêu cầu chuẩn bị:+ Máy Server **BKAP-DC12-01** nâng cấp lên **Domain Controller** quản lý miền **bkaptech.vn** và cài **DNS Server**.+ Máy Client **BKAP-WRK08-01** Join vào Domain.

3. Mô hình Lab:

HỆ THỐNG ĐÀO TẠO CNTT QUỐC TẾ BACHKHOA-APTECH

Lab 11.1 Cấu hình mã hóa File

BACHKHOA
EDUCATION / APTECH



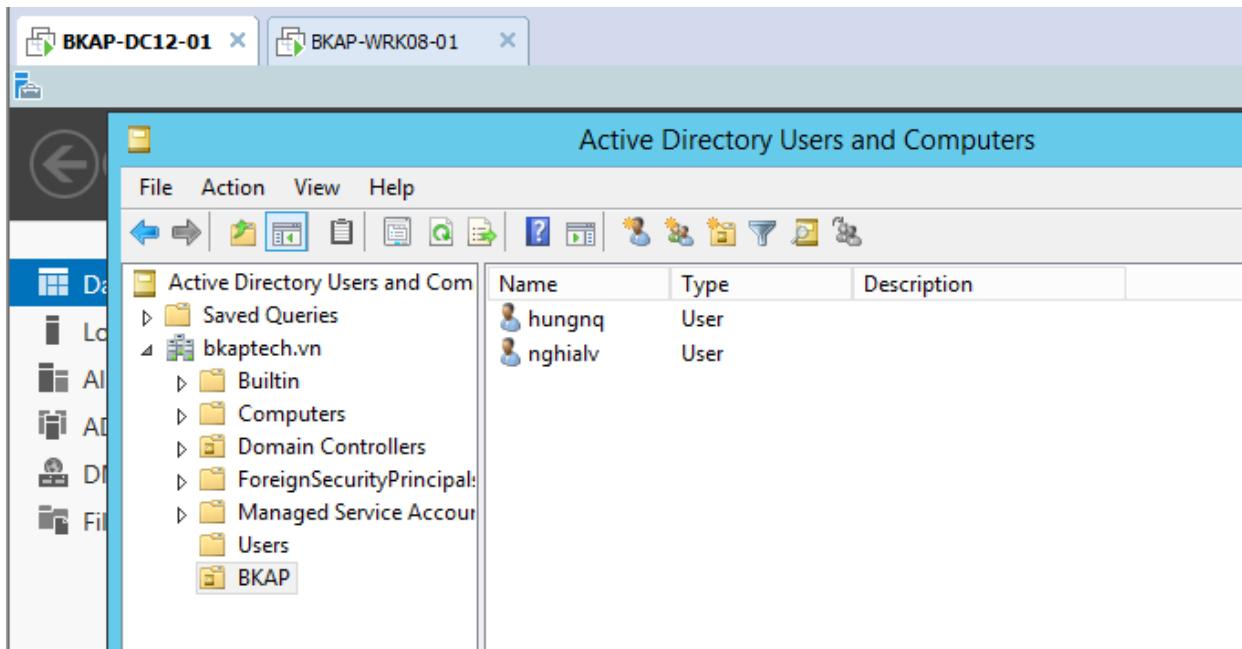
Hình 11.1

Sơ đồ địa chỉ như sau:

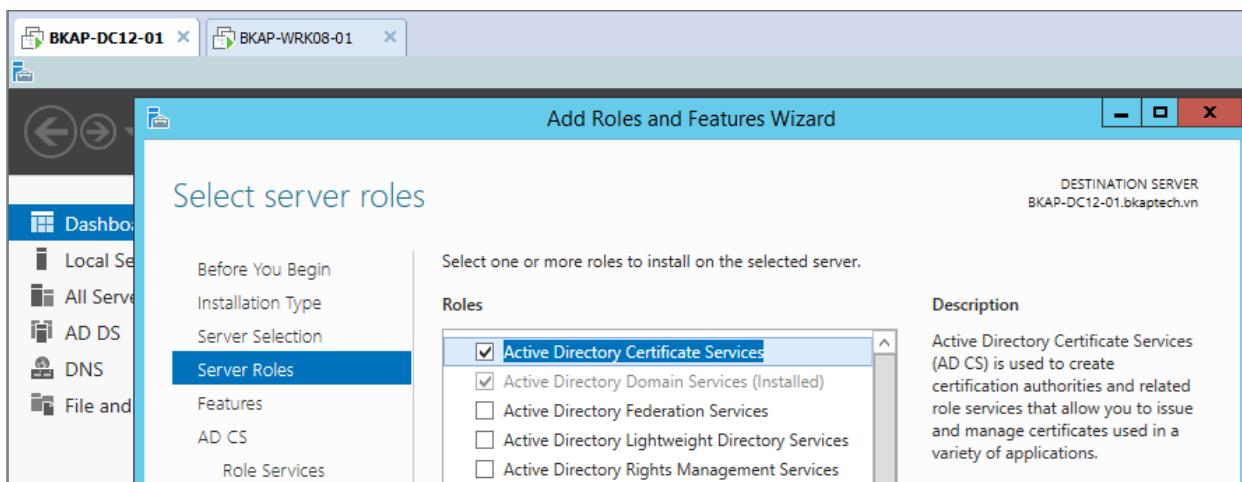
Thông số	BKAP-DC12-01	BKAP-SRV12-01
<i>IP address</i>	192.168.1.2	192.168.1.10
<i>Gateway</i>	192.168.1.1	192.168.1.1
<i>Subnet Mask</i>	255.255.255.0	255.255.255.0
<i>DNS Server</i>	192.168.1.2	192.168.1.2

Hướng dẫn chi tiết:

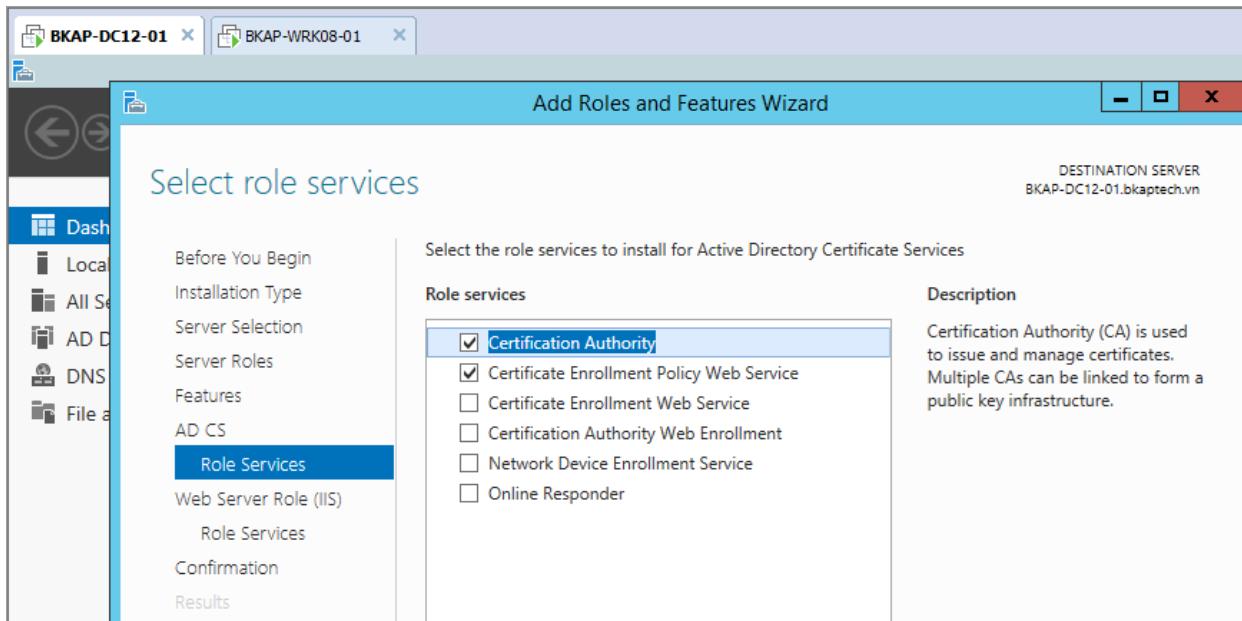
- Mở các máy ảo, kết nối như hình trên, thực hiện ping thông giữa các máy với nhau.
- Trên máy **BKAP-DC12-01** thực hiện :
 - Tạo OU **BKAP**, tạo 2 user **hungnq** và **nghialv** bên trong OU **BKAP**.



- Cài đặt CA Server.
 - Server Manager / Add roles and features.. tại Select server roles , click chọn vào Active Directory Cerfificate Services.

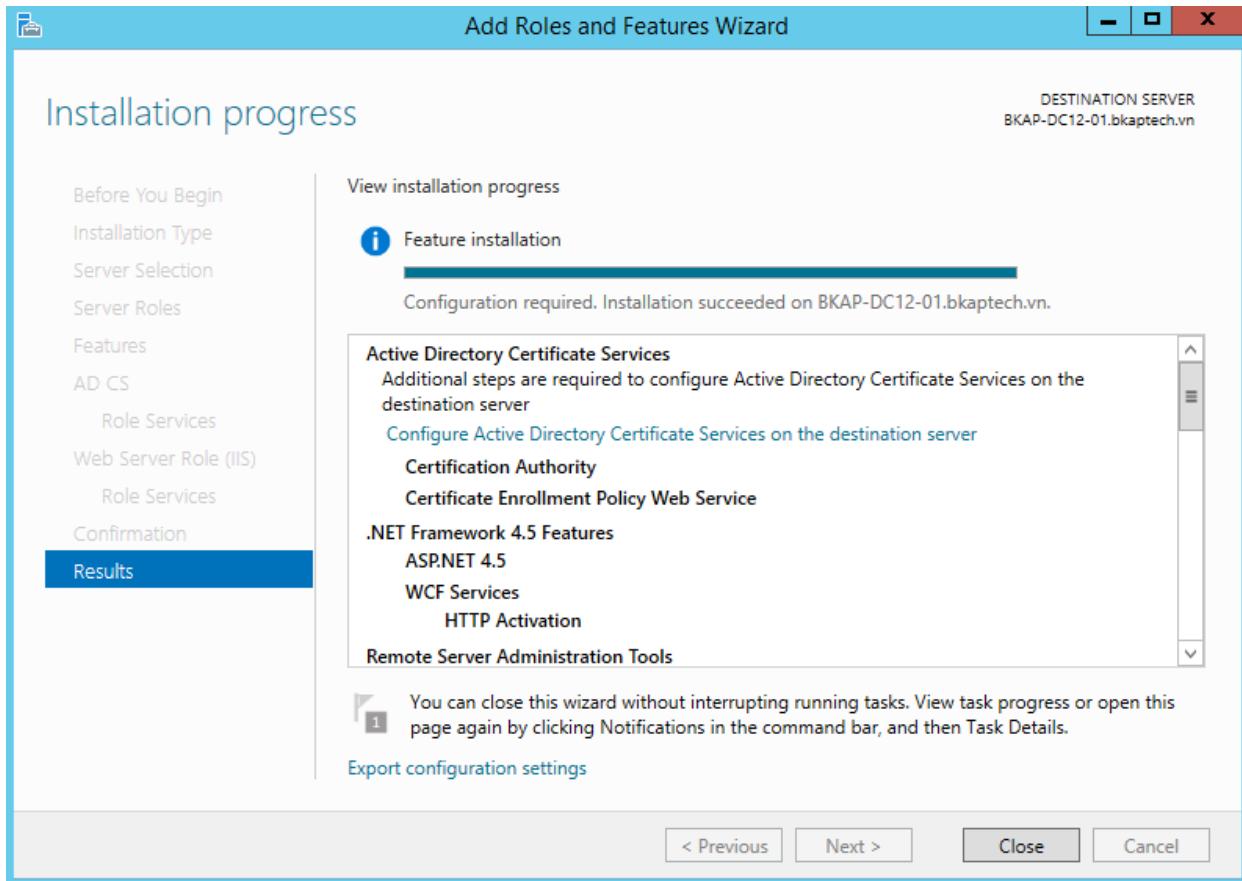


- Tại **Select role services** , click chọn vào **Certification Authority** và **Certificate Enrollment Policy Web Service**.

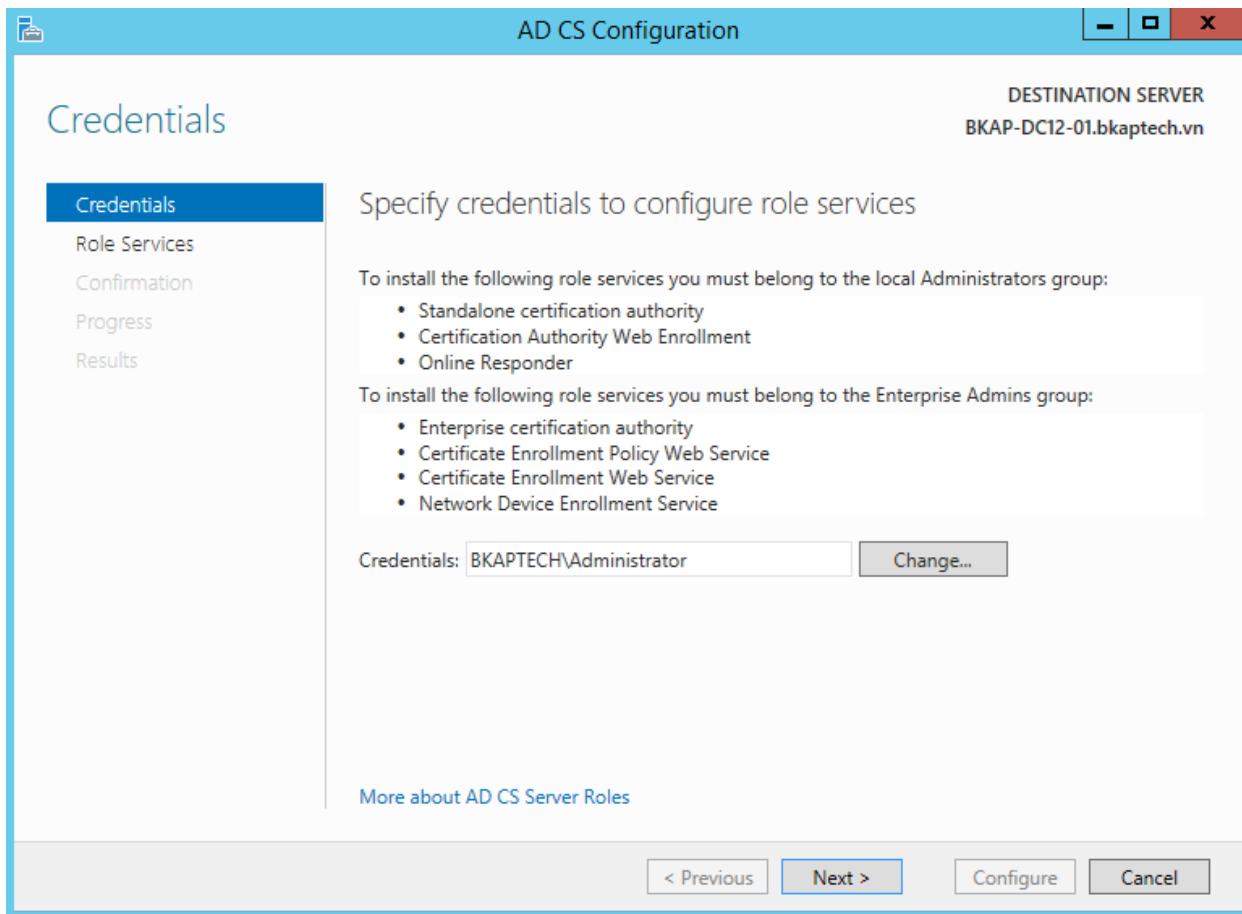


⇒ **Install.**

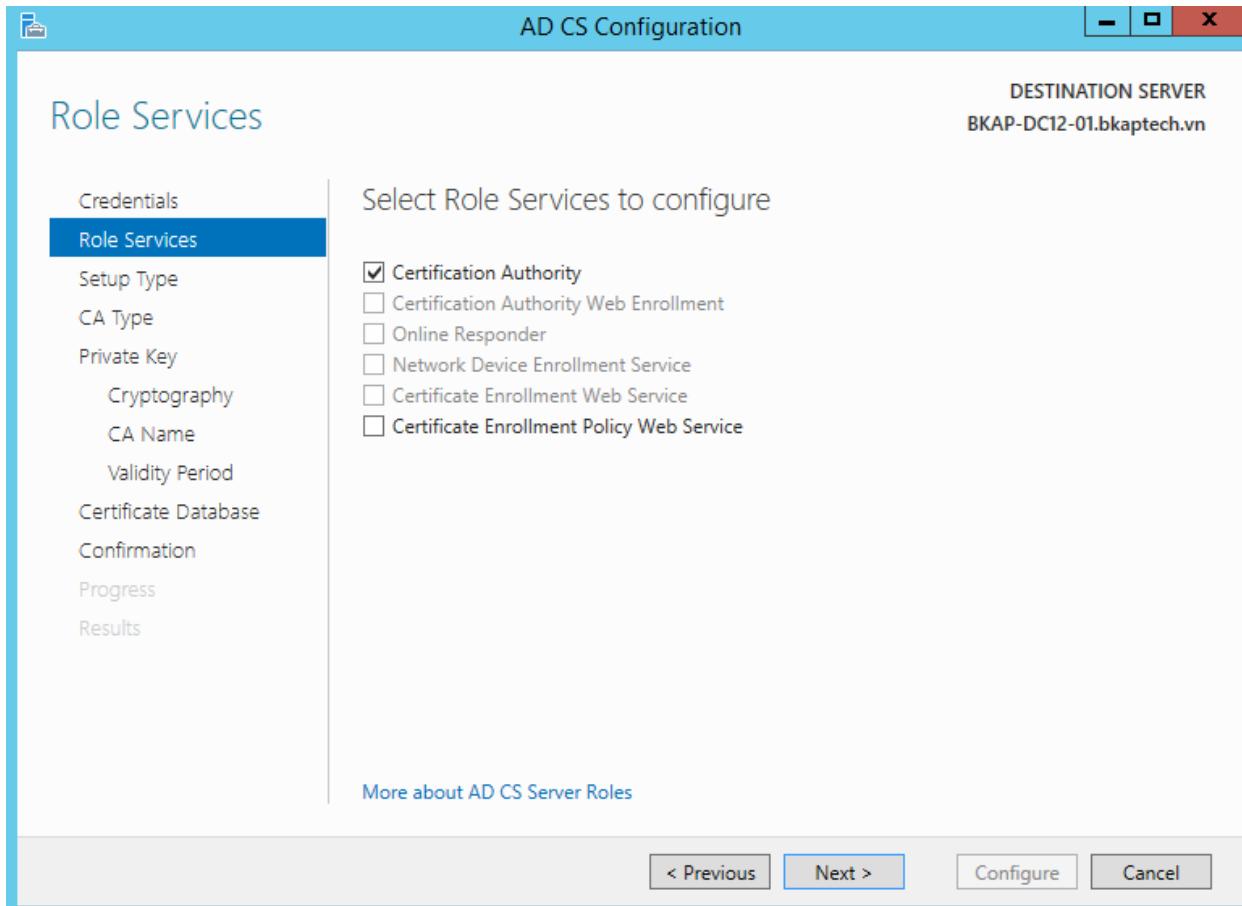
- Tại cửa sổ **Installation process**, click vào dòng chữ *Configure Active Directory Certificate Services on the destination server.*



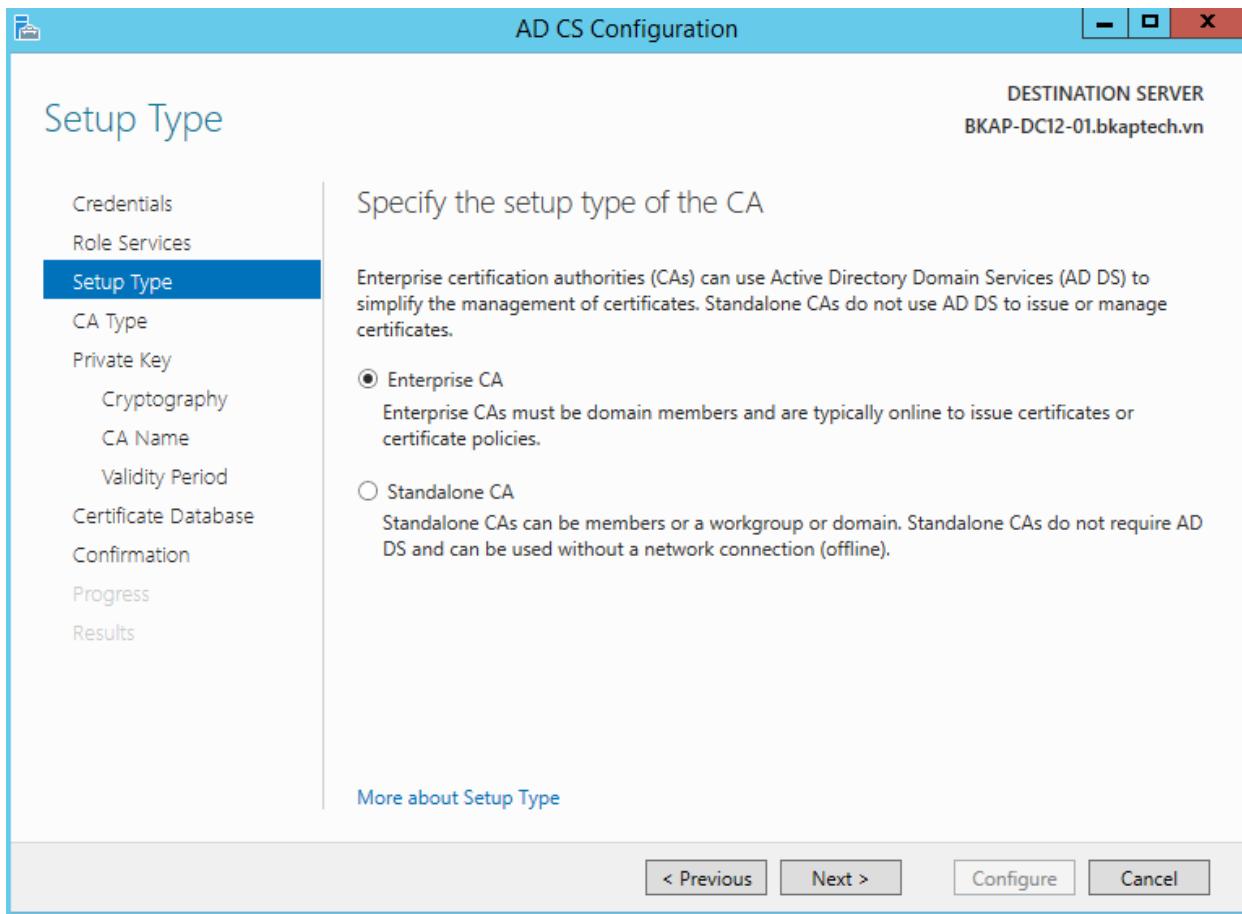
- Tại cửa sổ **Credential**, click vào **Next**.



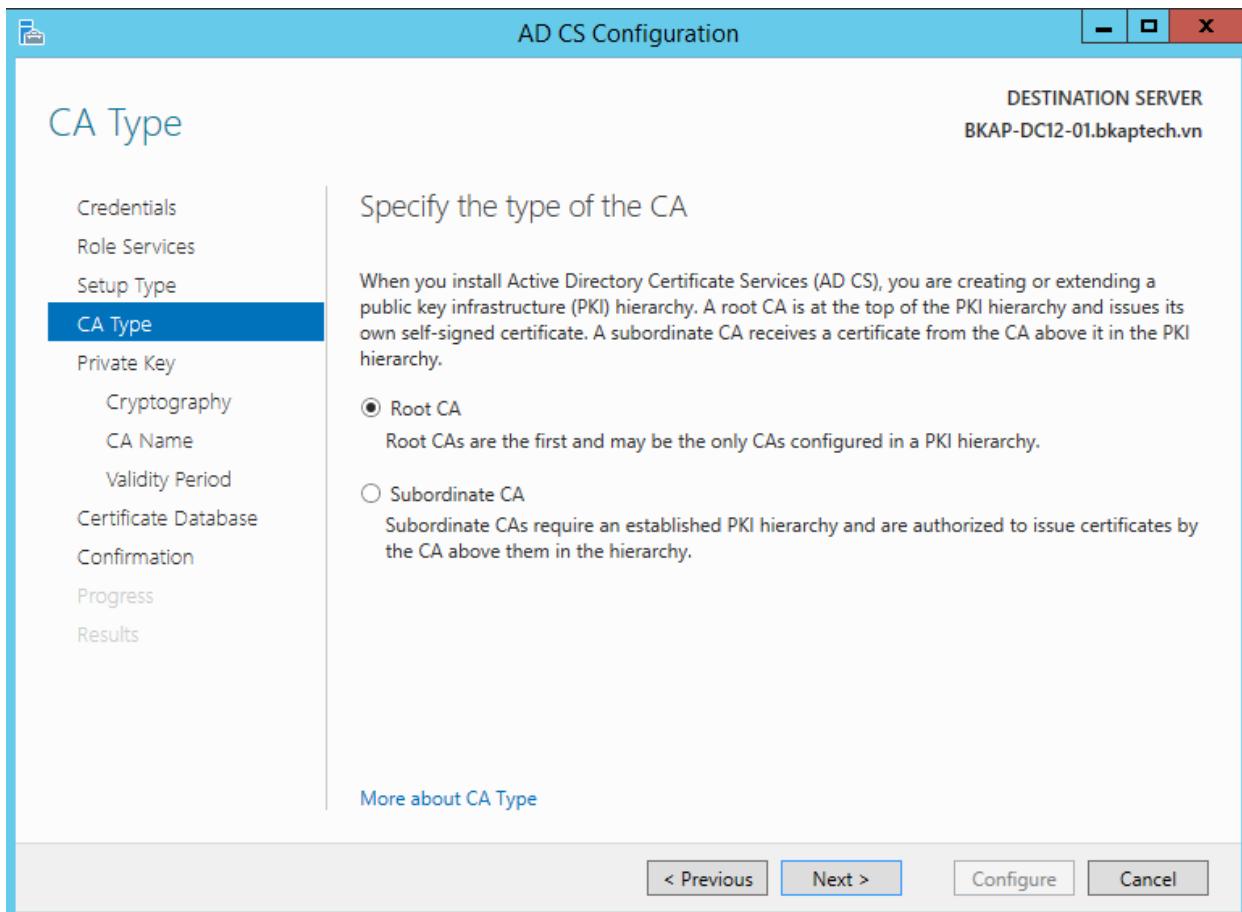
- Tại cửa sổ **Role Services** , click chọn vào **Certification Authority** , => Next.



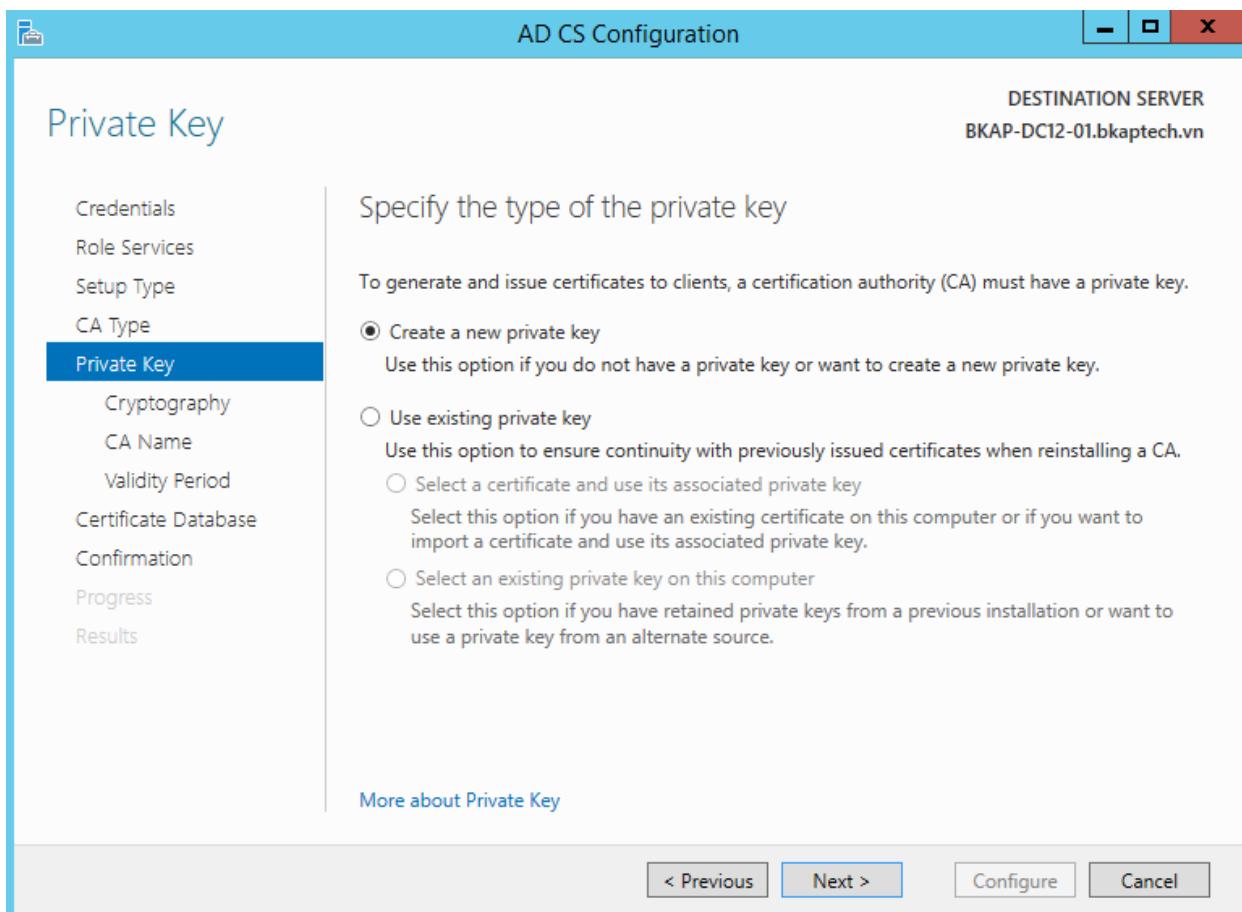
▪ Chọn vào Enterprise CA



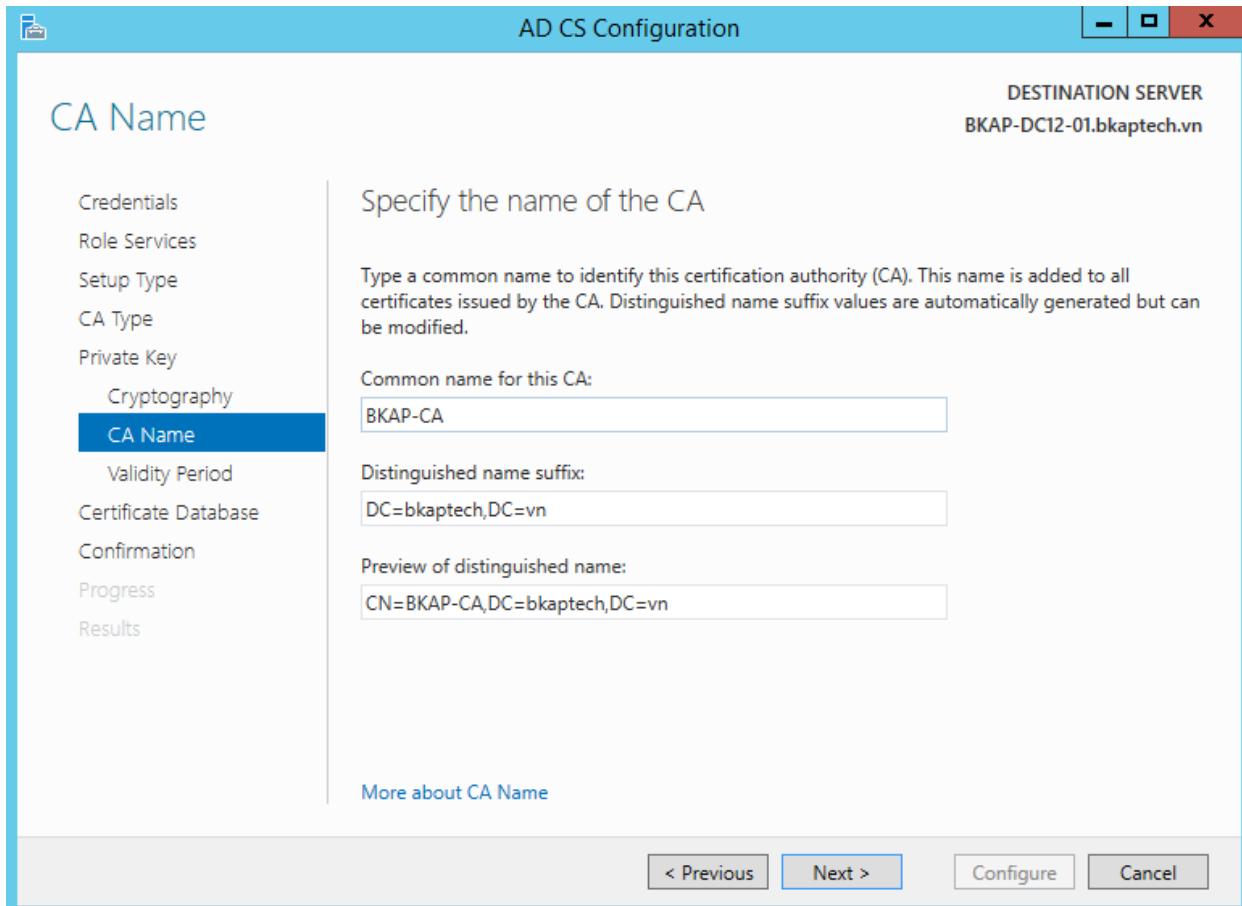
- Click vào Root CA.



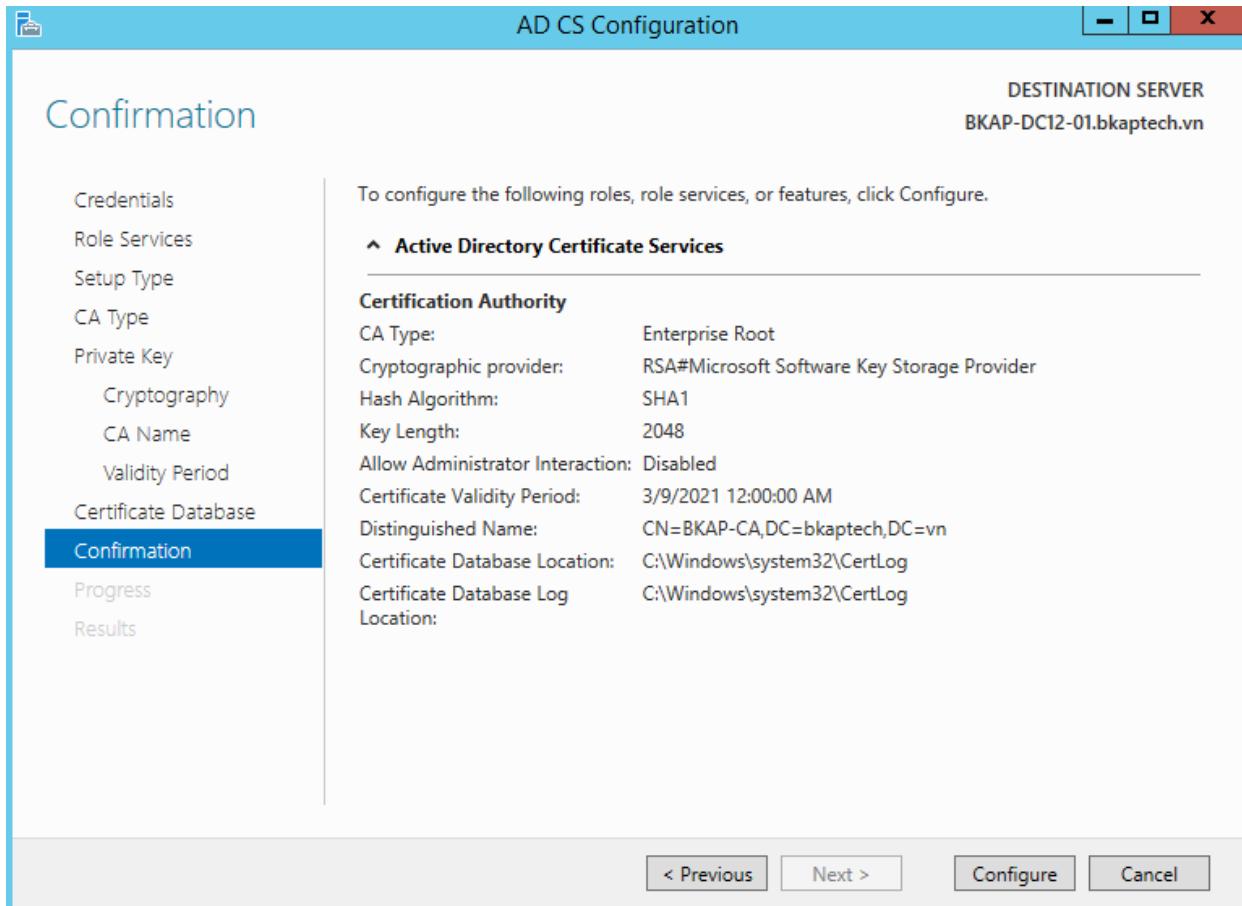
- Click vào **Create a new private key**.



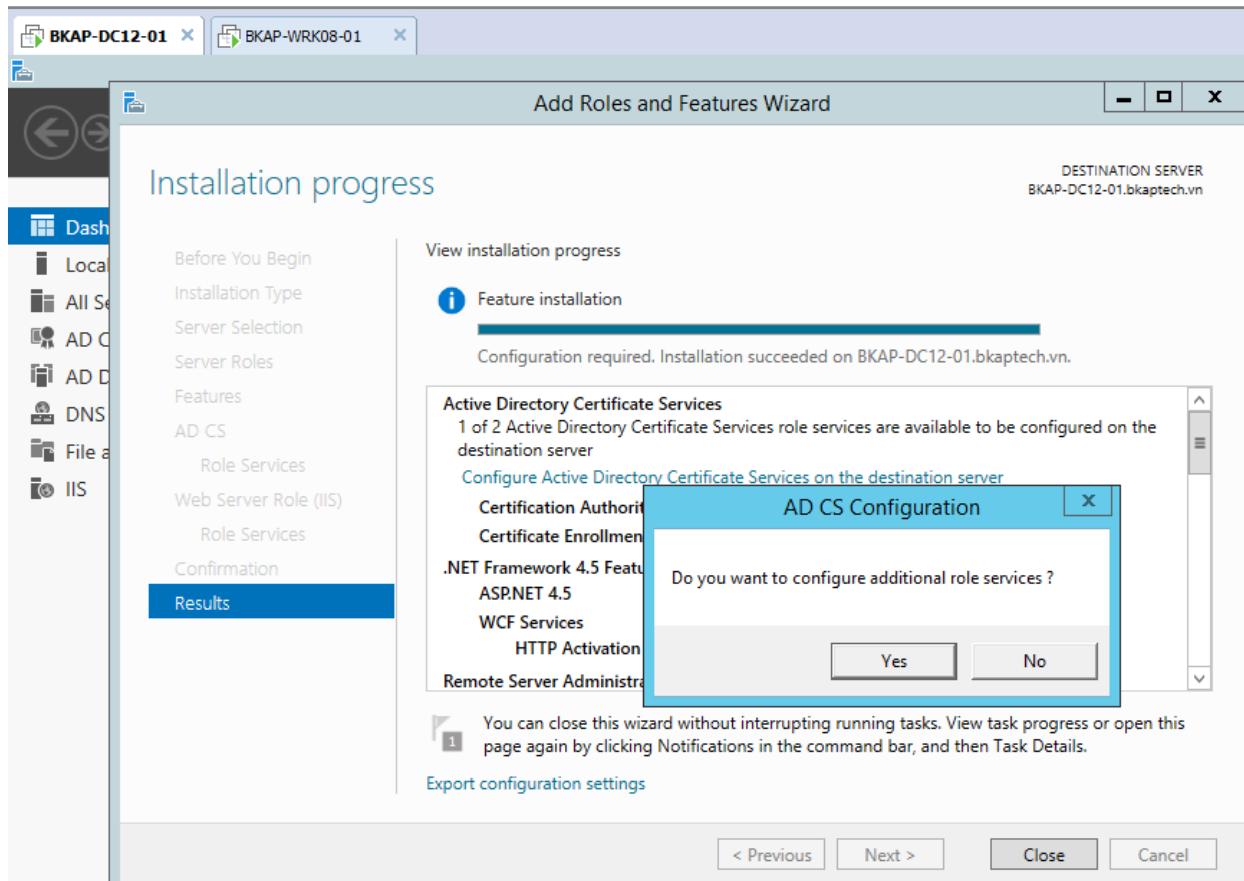
- Tại cửa sổ **CA Name** , tại mục **common name for this CA** , nhập vào tên **BKAP-CA**.



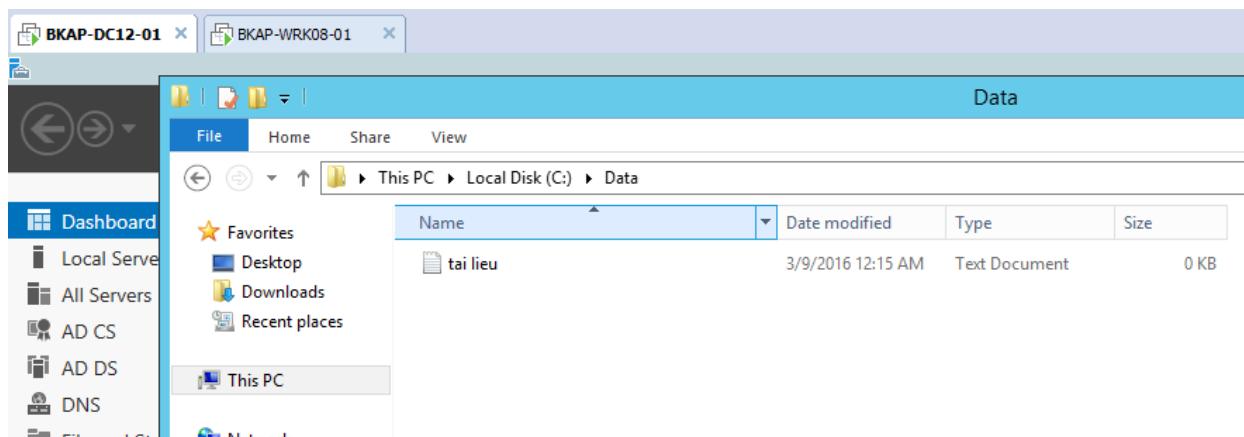
⇒ Click vào **Next**, tại cửa sổ **Confirmation** , click vào **Configure**.

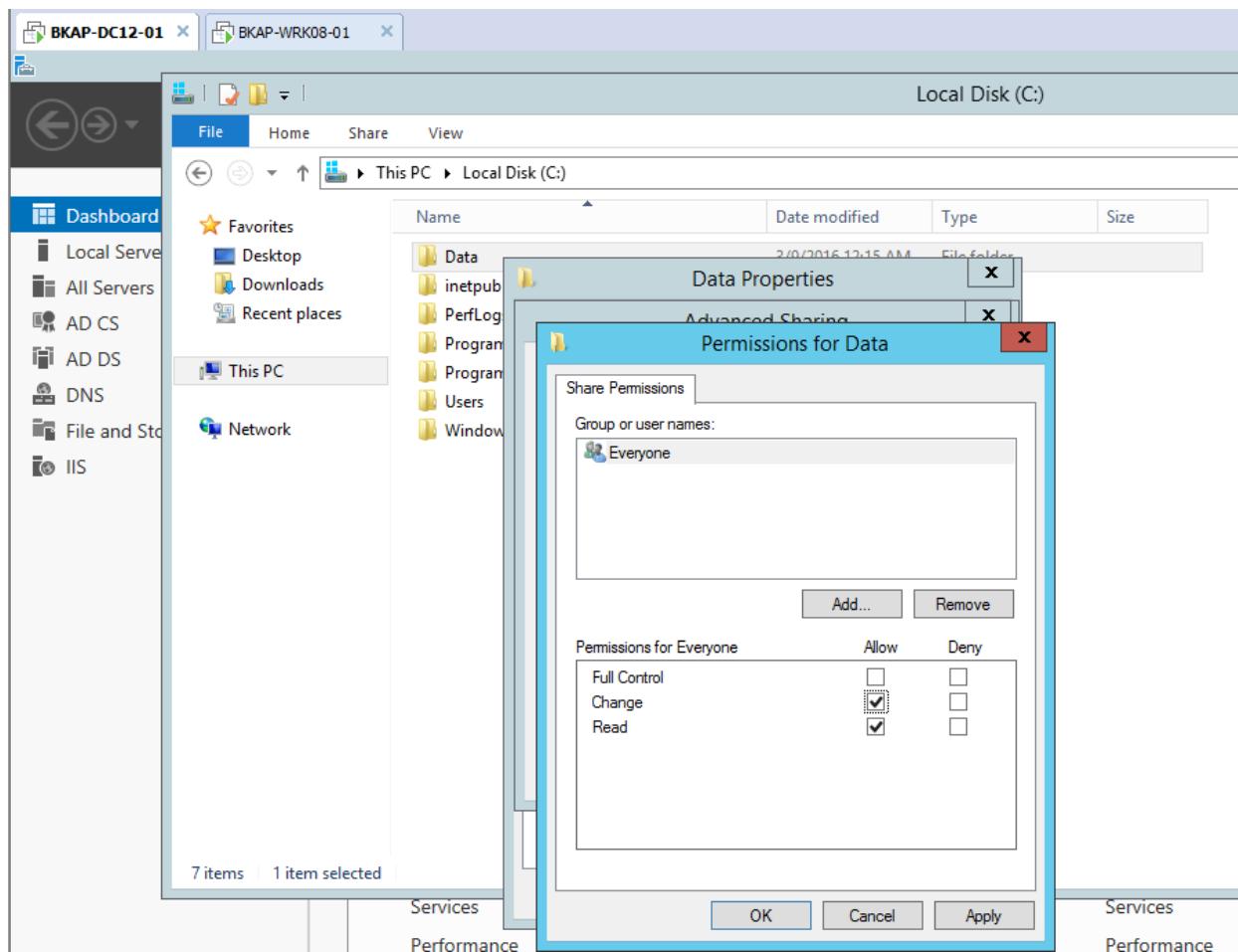


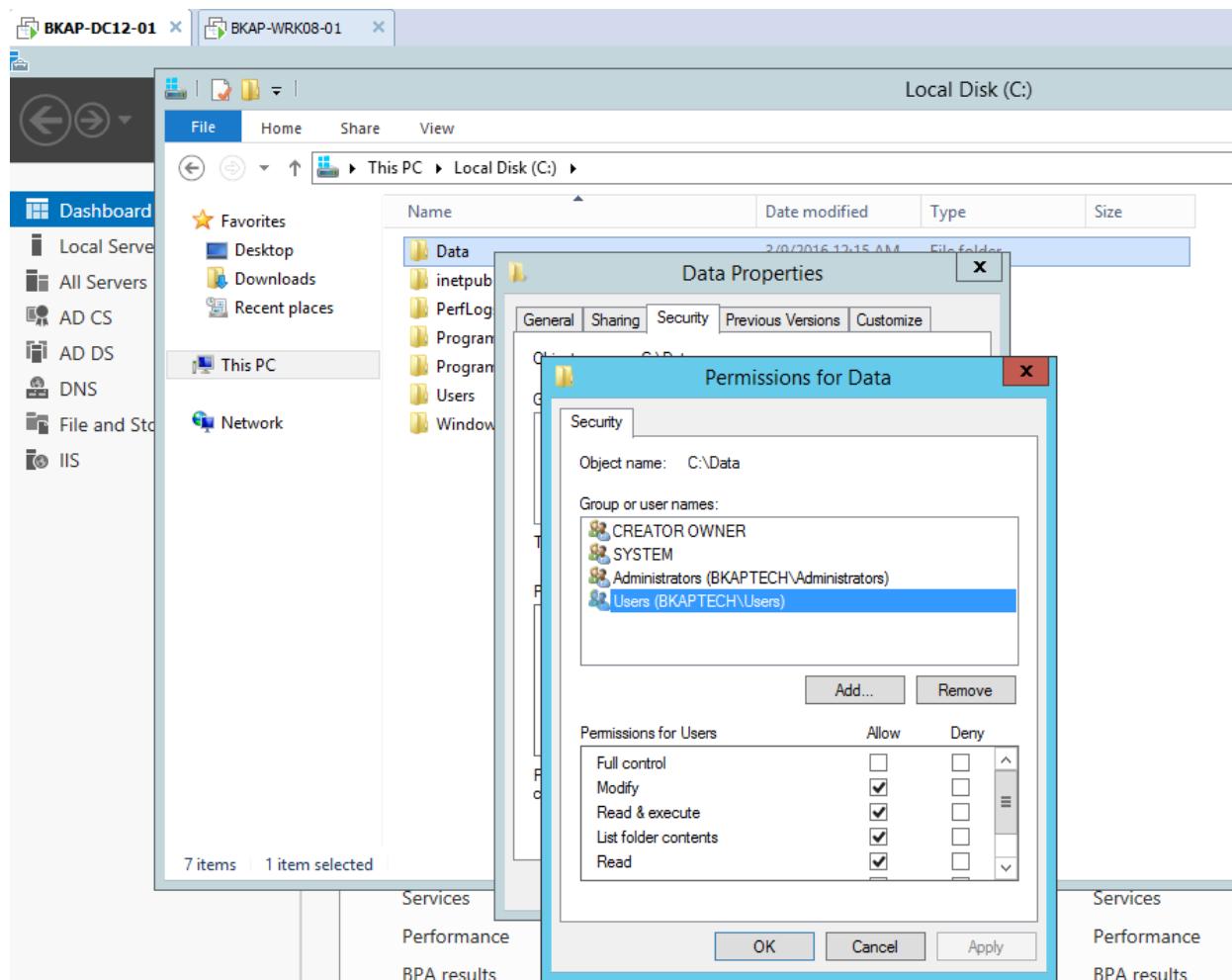
- Tại cửa sổ AD CS Configuration , click vào No



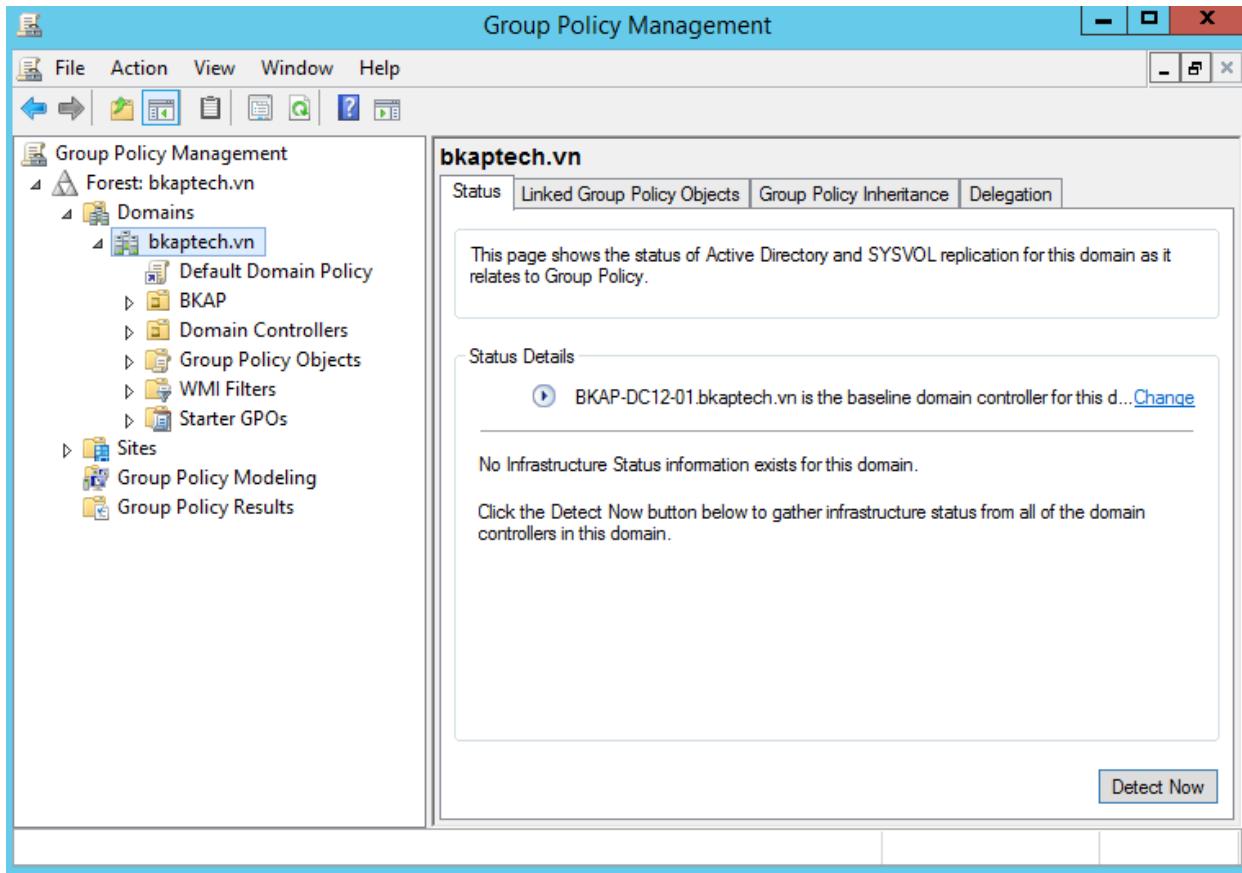
- Tạo 1 folder tên **Data** trong ổ C ,tạo 1 *file txt* trong folder **Data**, tiến hành phân quyền chia sẻ dữ liệu.



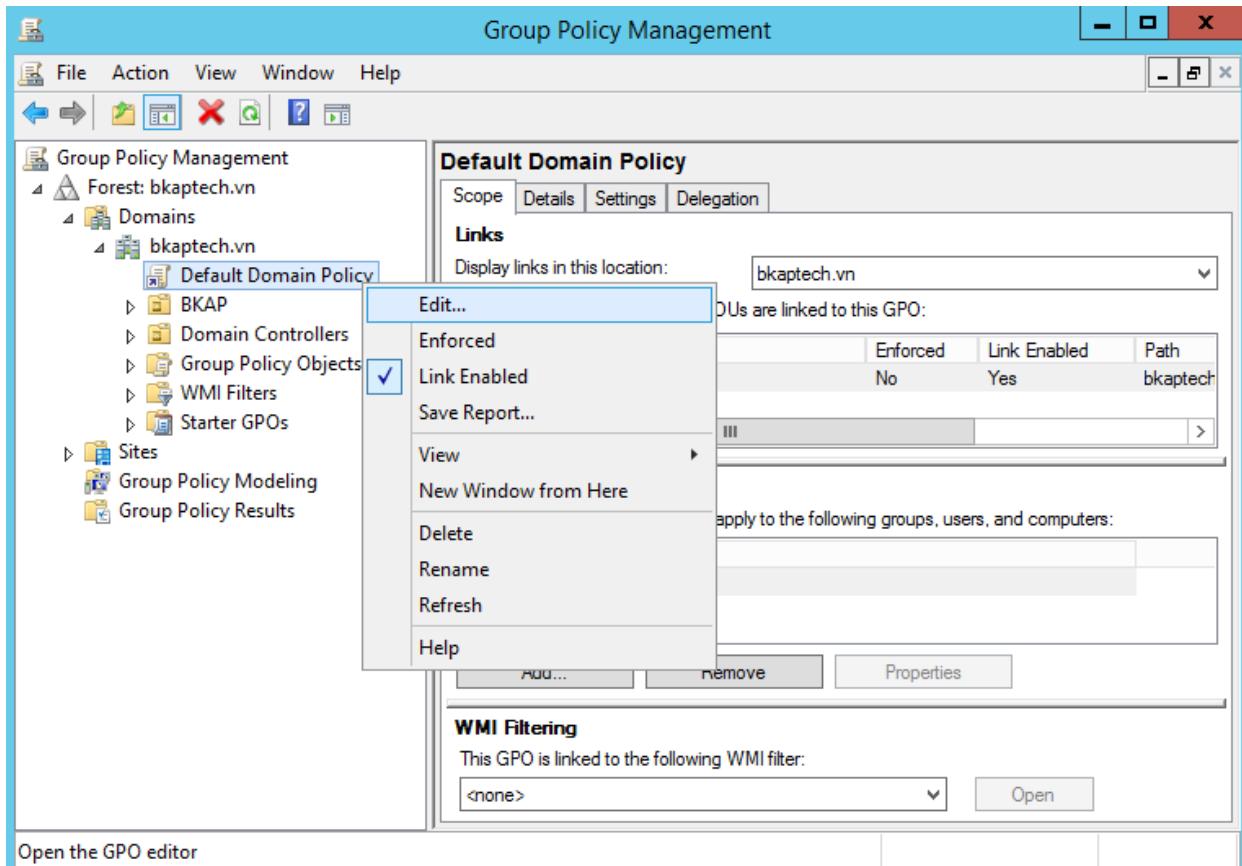




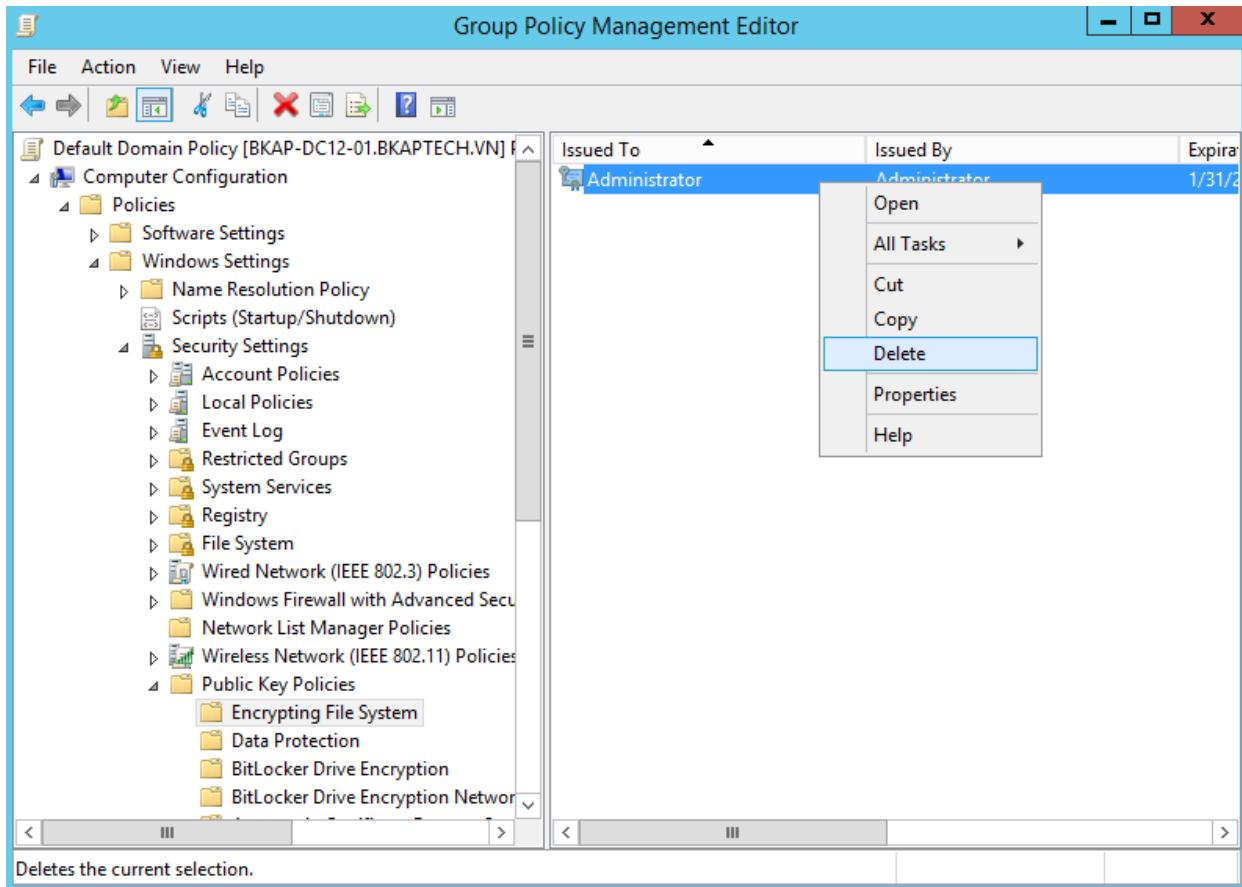
- Bỏ **Key Public** mặc định:
 - Vào **Group Policy Management**.



- Click chuột phải tại **Default Domain Policy**, chọn **Edit...**



- Click vào Computer Configuration / Policies / Windows Settings / Security Settings / Public key Policies / Encrypting File System. Tại đây xóa key Administrator.



- Gõ lệnh **gpupdate /force** trong cmd.

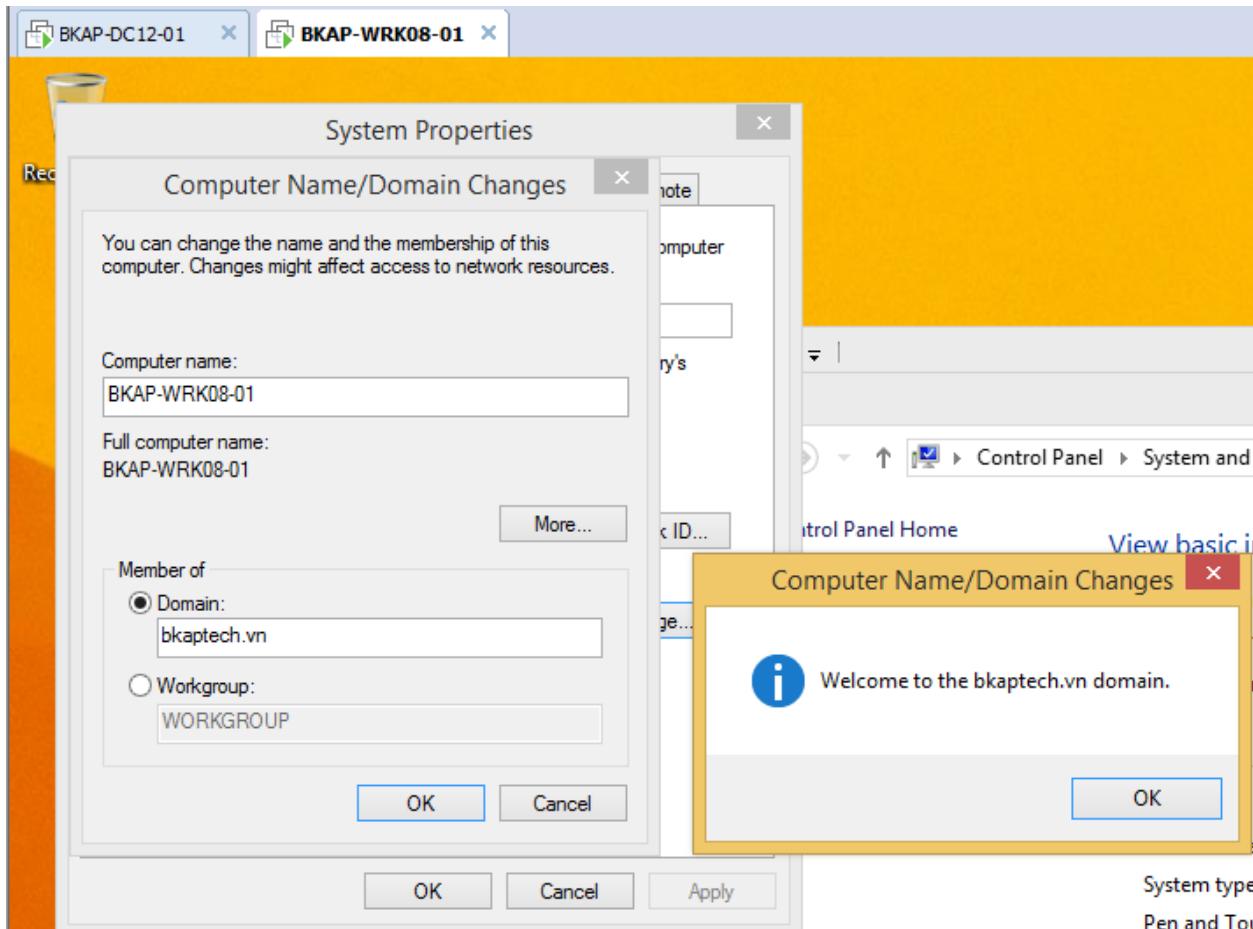
```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>gpupdate /force
Updating policy...

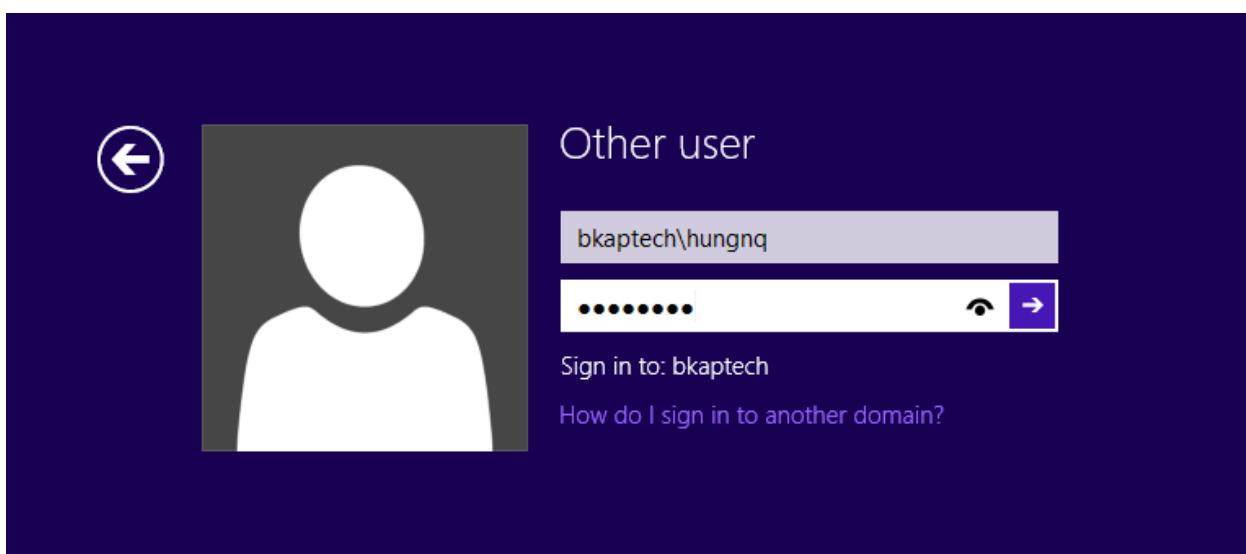
Computer Policy update has completed successfully.
User Policy update has completed successfully.

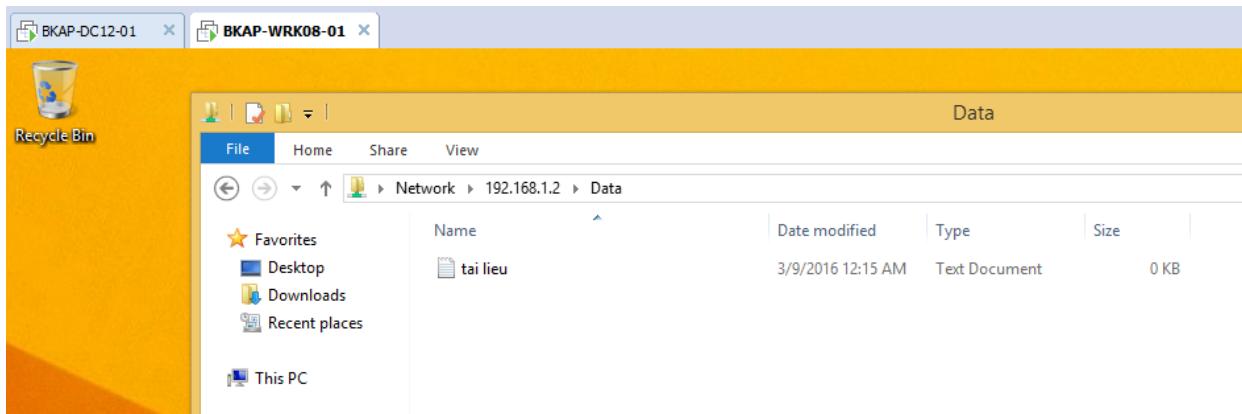
C:\Users\Administrator>
```

- Chuyển sang máy client **BKAP-WRK08-01**:
 - Join Client* vào **Domain**.



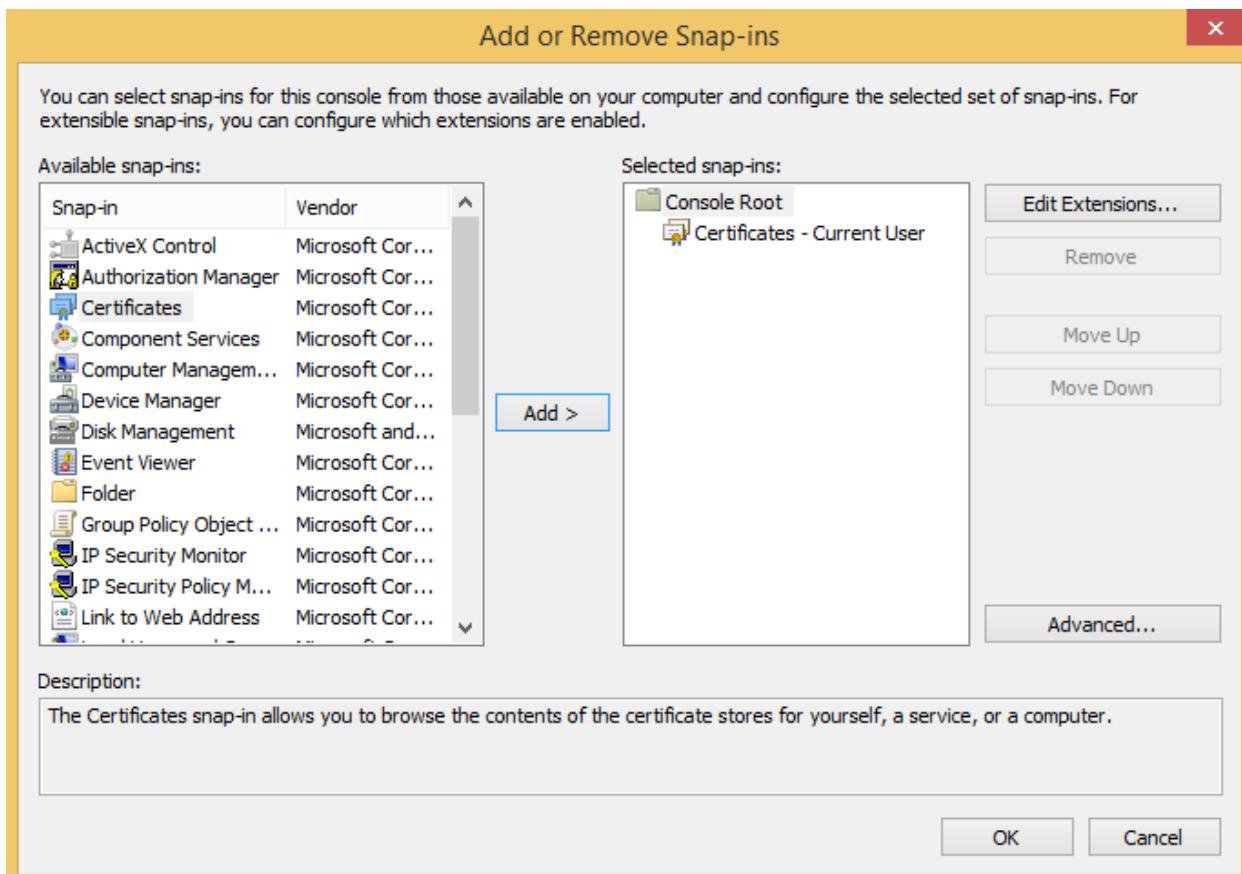
- Đăng nhập tài khoản **hungnq**, truy cập file để kiểm tra.



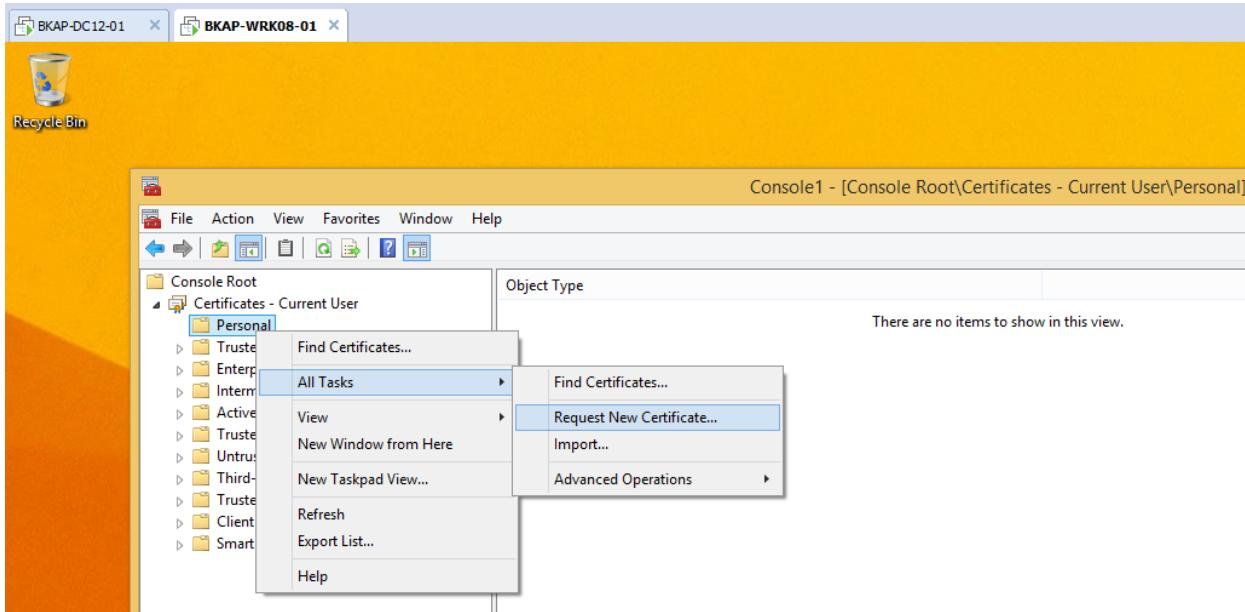


- Xin Public key cho User.

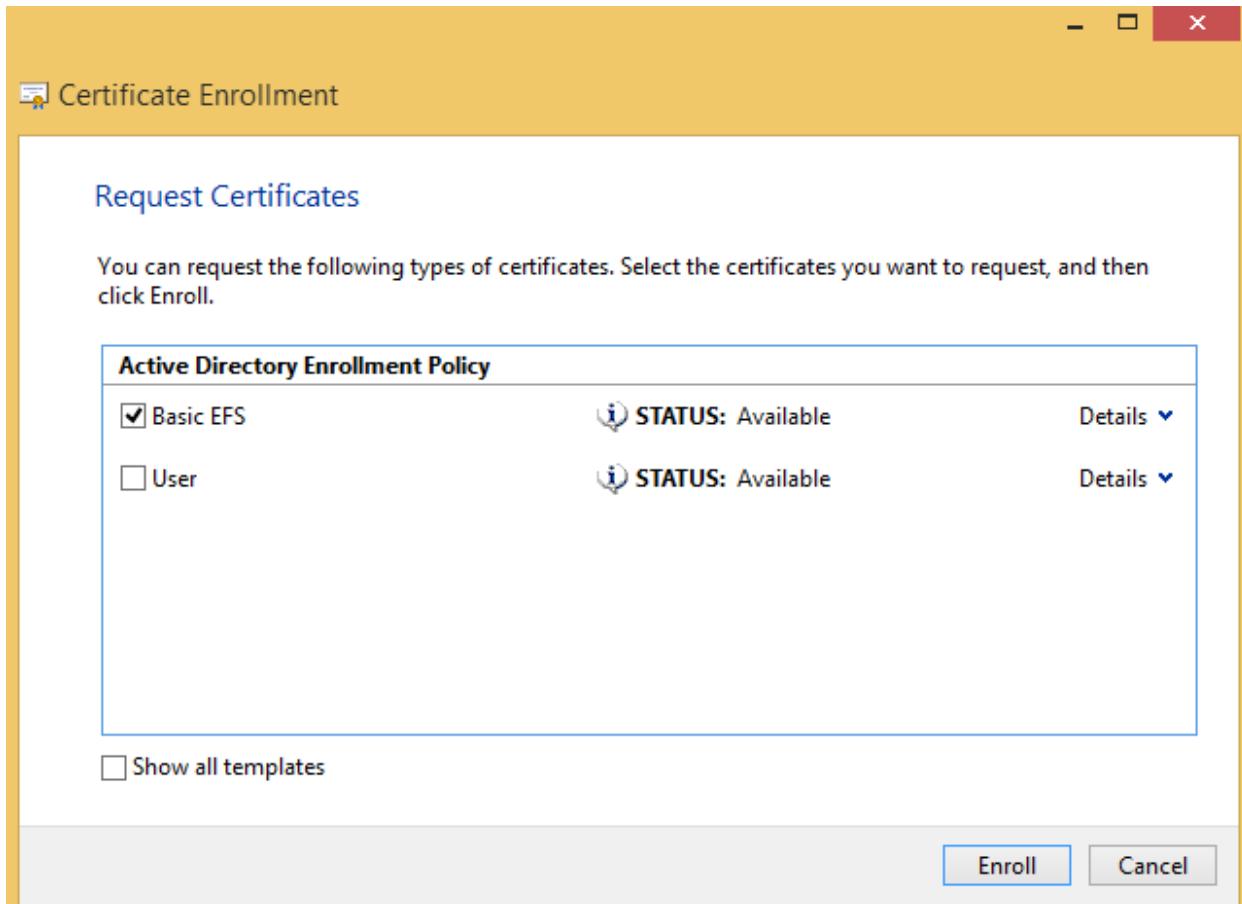
- *Cmd / mmc.*
- Tại cửa sổ **Console 1...** , click vào **File / Add,Remove Snap-in..**
- Tại cửa sổ **Add or Remove Snap-ins** , click vào **Certificates** , click vào **Add >**

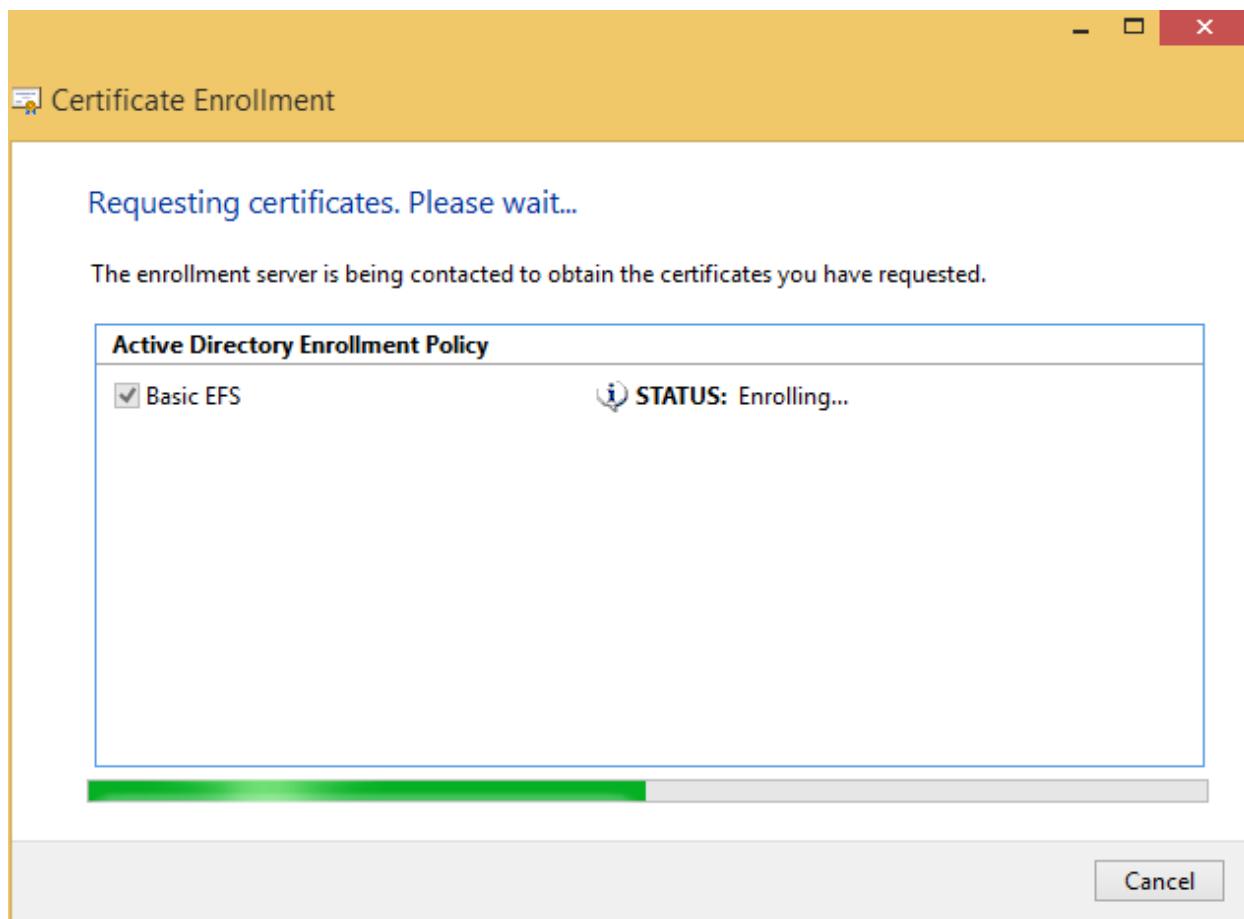


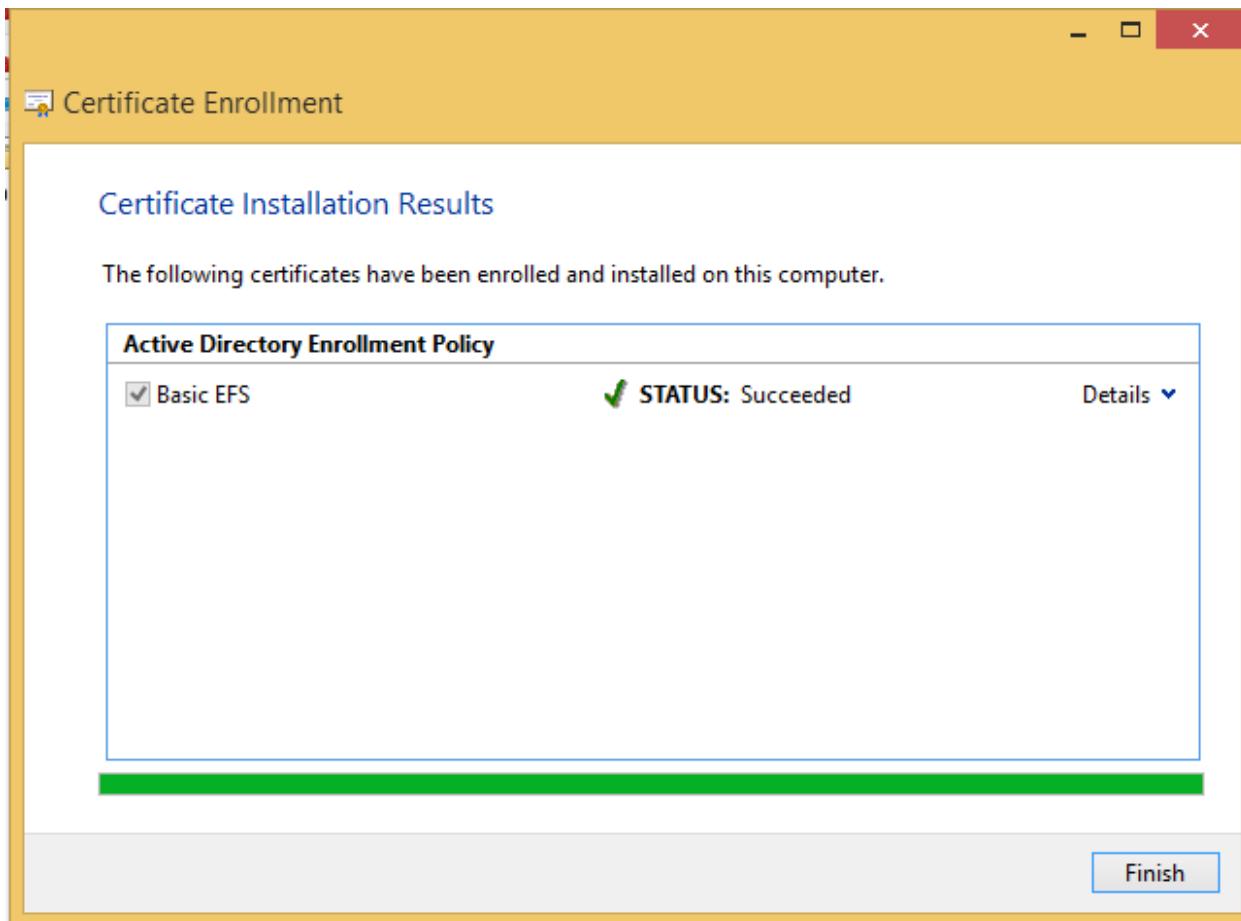
- Tại cửa sổ **Console 1** .. click chuột phải vào **Personal / All Tasks / Request New Certificate...**



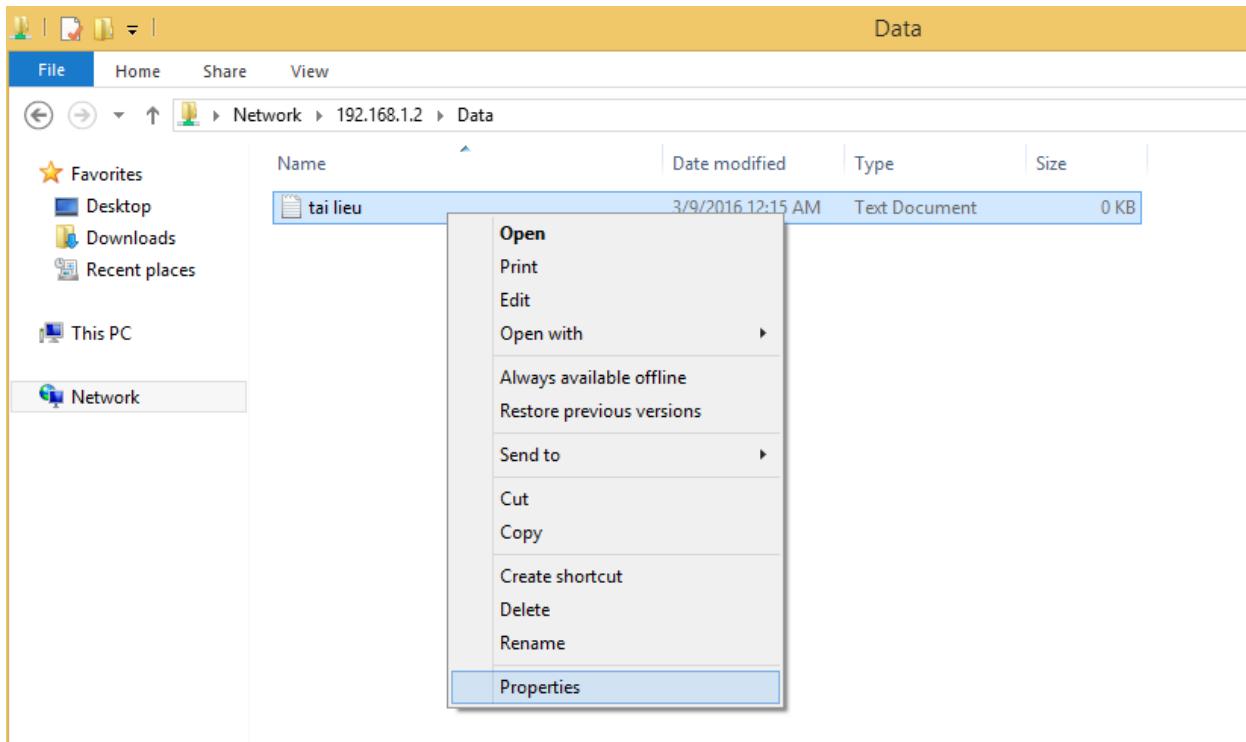
- Tại cửa sổ **Certificate Enrollment** , click chọn vào **Basic EFS** => **Enroll**.



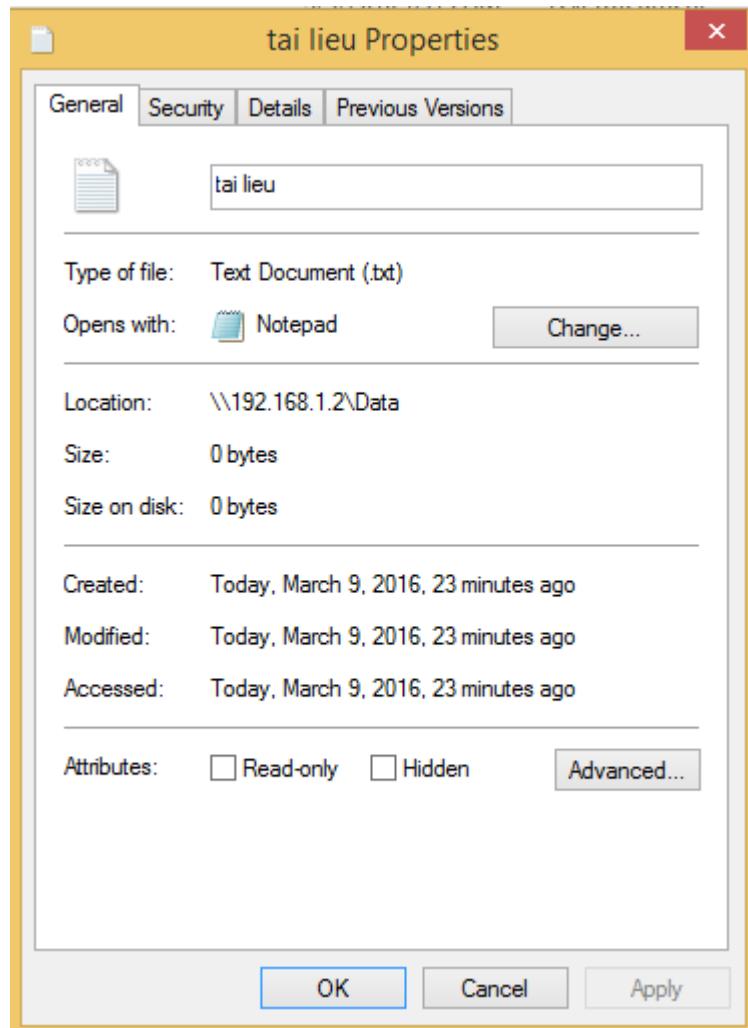




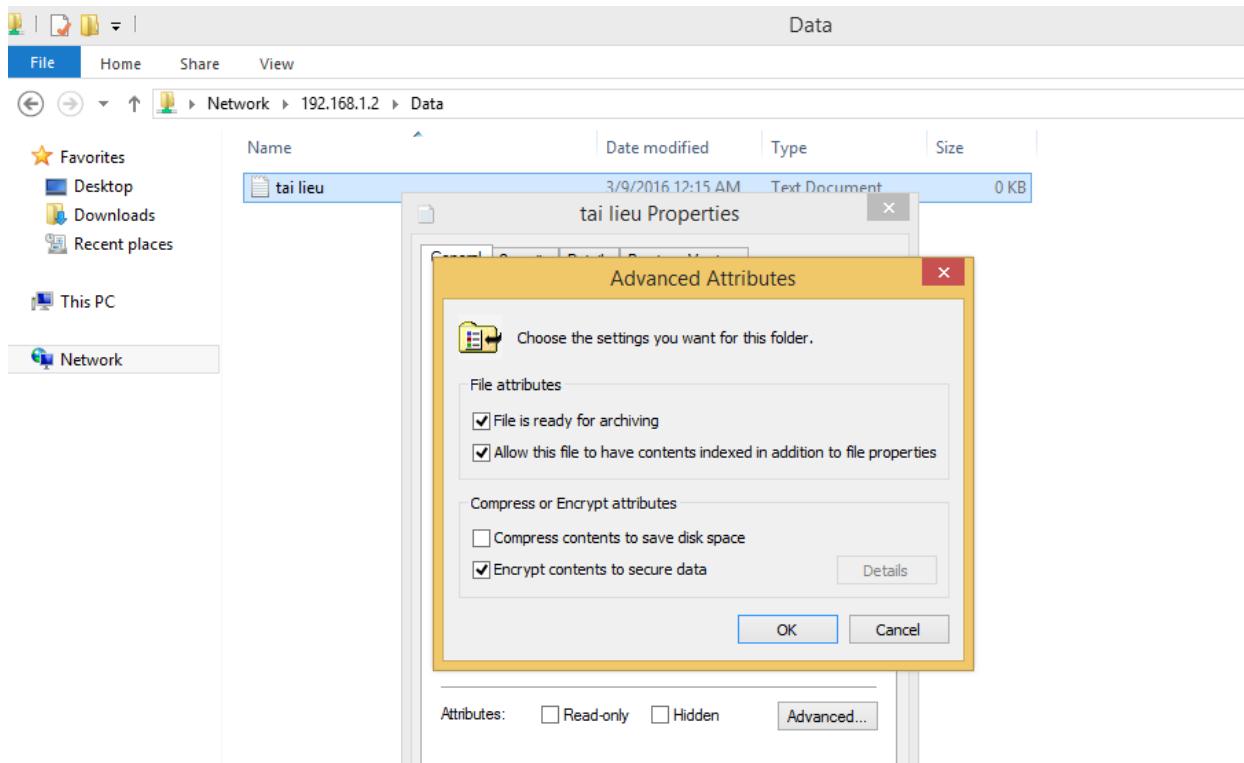
- Thực hiện mã hóa file:
 - Click vào file txt / Properties.



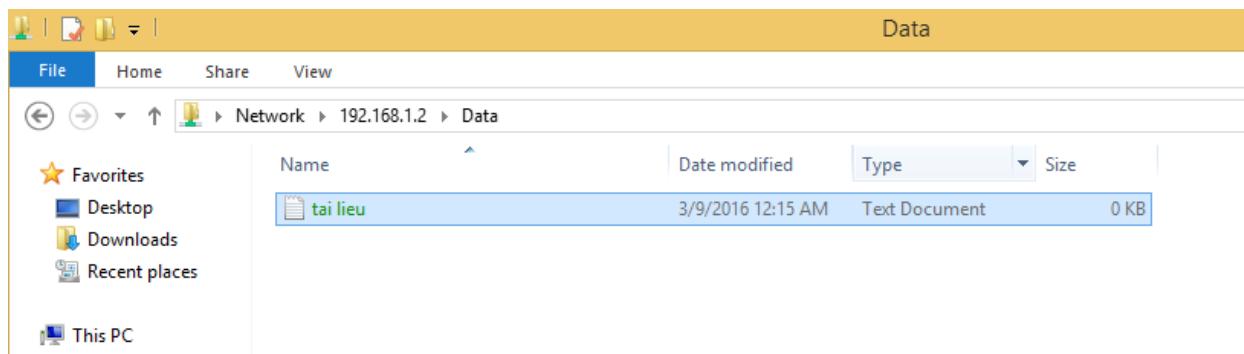
- Tại tab General , click vào Advanced...



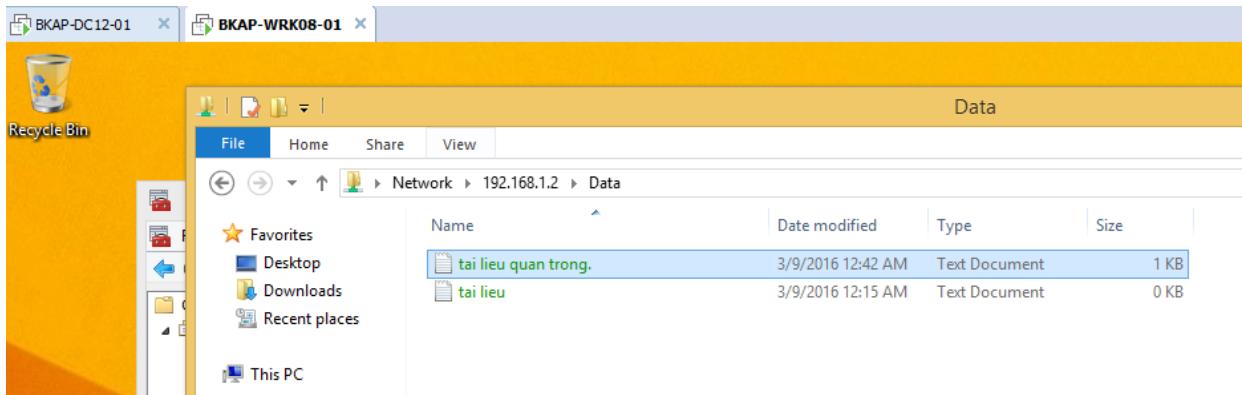
- Tại cửa sổ **Advanced Attributes**, click chọn vào **Encrypt contents to secure data**.



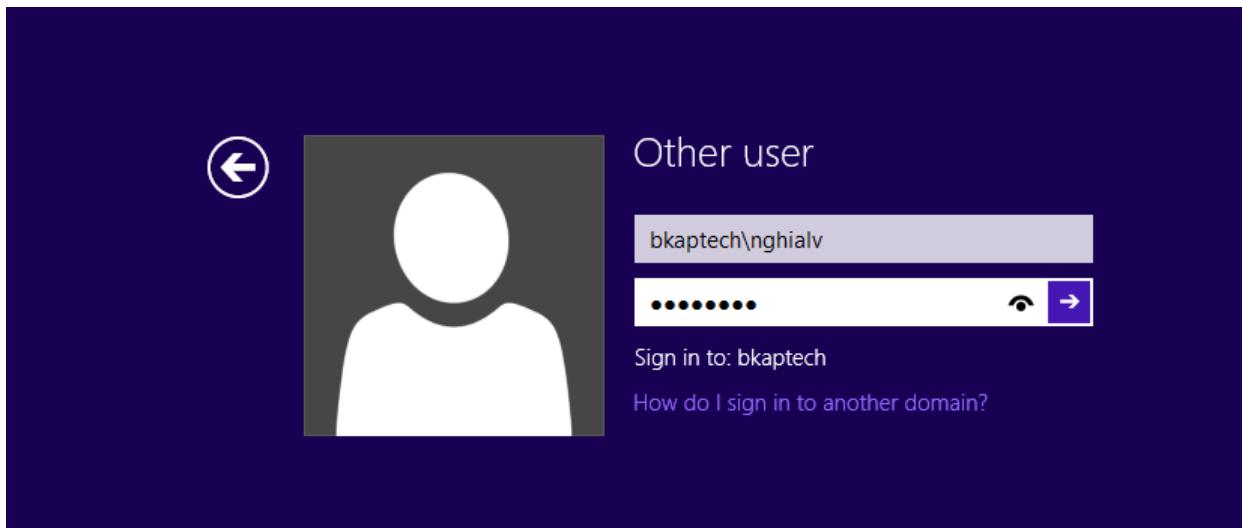
⇒ Apply / OK.



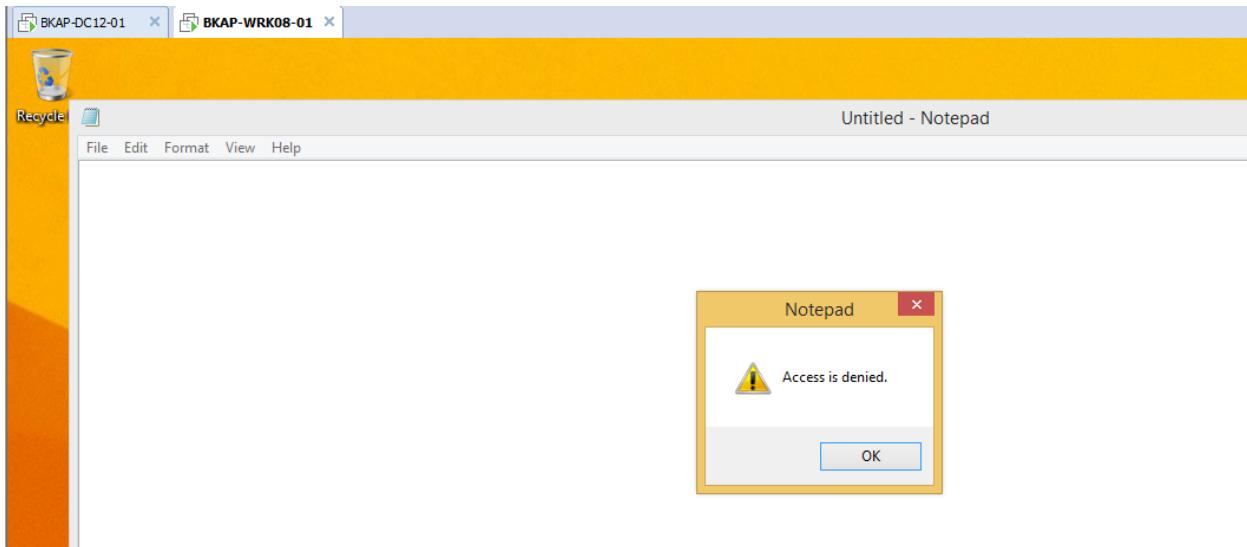
- Thay đổi nội dung file và save thành file khác.



- Đăng nhập bằng tài khoản **nghialv** để kiểm tra độ bảo mật của file.



⇒ Tài khoản **nghialv** ko truy cập được vào file do bị mã hóa.



11.2 Cấu hình Auditing nâng cao.

1. Yêu cầu bài lab:

+ Trên *BKAP-DC12-01*, thực hiện :

- Tạo *OU, Group, User* theo miền bkaptech.vn.
- Kiểm tra phân giải **DNS**.

+ Trên *BKAP-SRV12-01*, thực hiện :

- Join vào **Domain**.
- Tạo folder **Data**, tạo folder **IT ,Sale** trong folder **Data**.
- Cấu hình phân quyền và chia sẻ dữ liệu.
- Sử dụng **Auditing** để giám sát file.

+ Trên máy *BKAP-WRK08-01*, thực hiện:

- *Join vào Domain*.
- Tiến hành đăng nhập, truy cập thư mục, xóa file, tạo thư mục mới.

+ Trên máy *BKAP-SRV12-01* , kiểm tra sau khi xóa file.

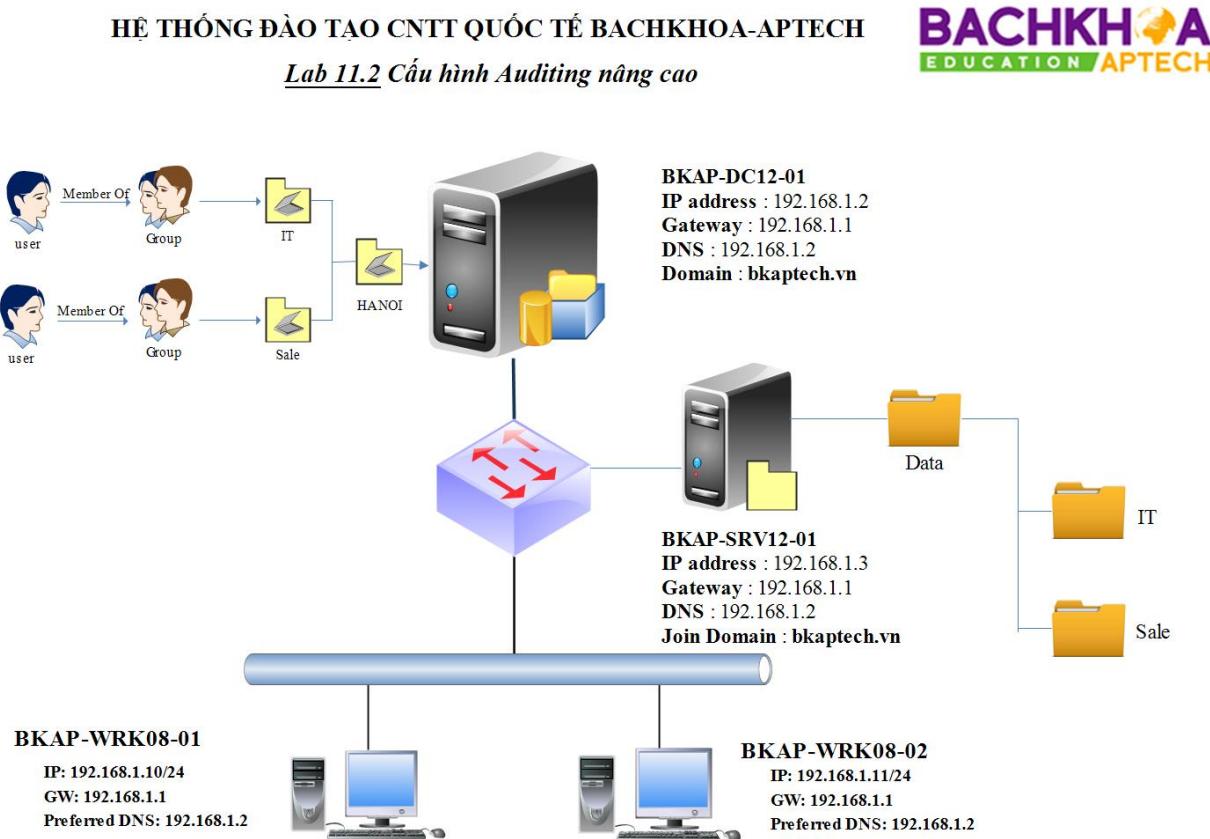
2. Yêu cầu chuẩn bị:

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

+ Máy BKAP-SRV12-01 , Join vào miền , tạo thư mục và phân quyền chia sẻ thư mục.

+ Máy BKAP-WRK08-01 , Join vào miền dùng để kiểm tra xóa file.

3. Mô hình Lab:



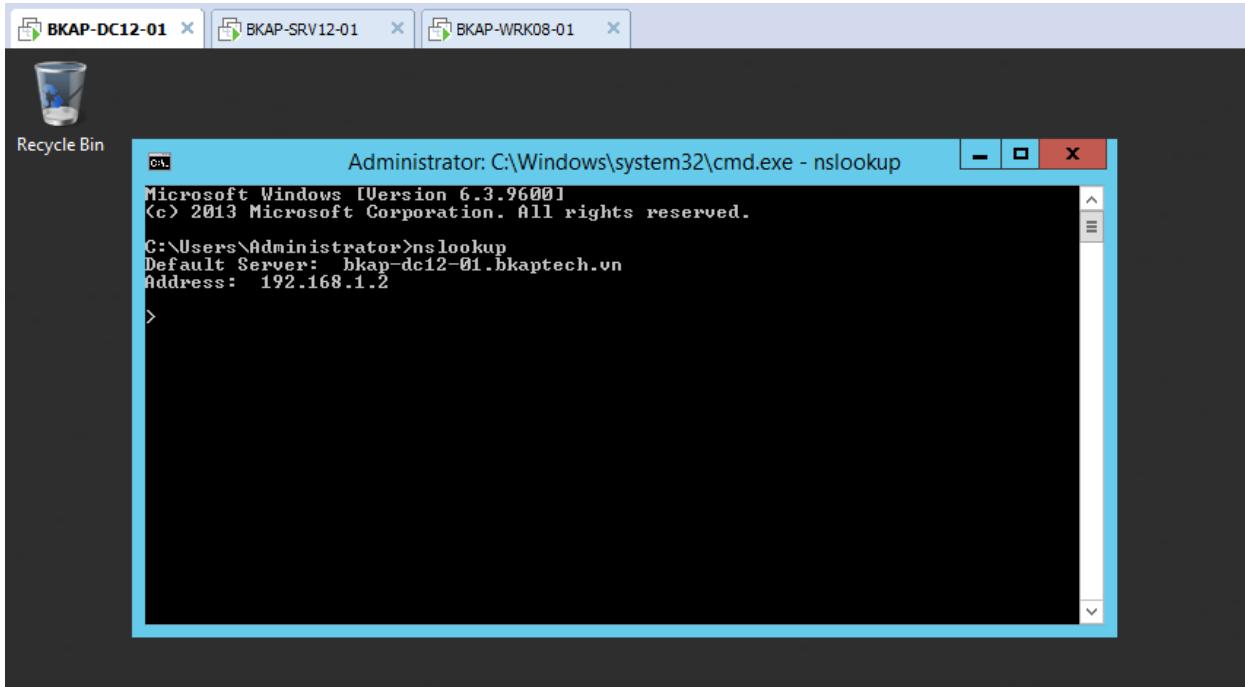
Hình 11.2

Sơ đồ địa chỉ như sau:

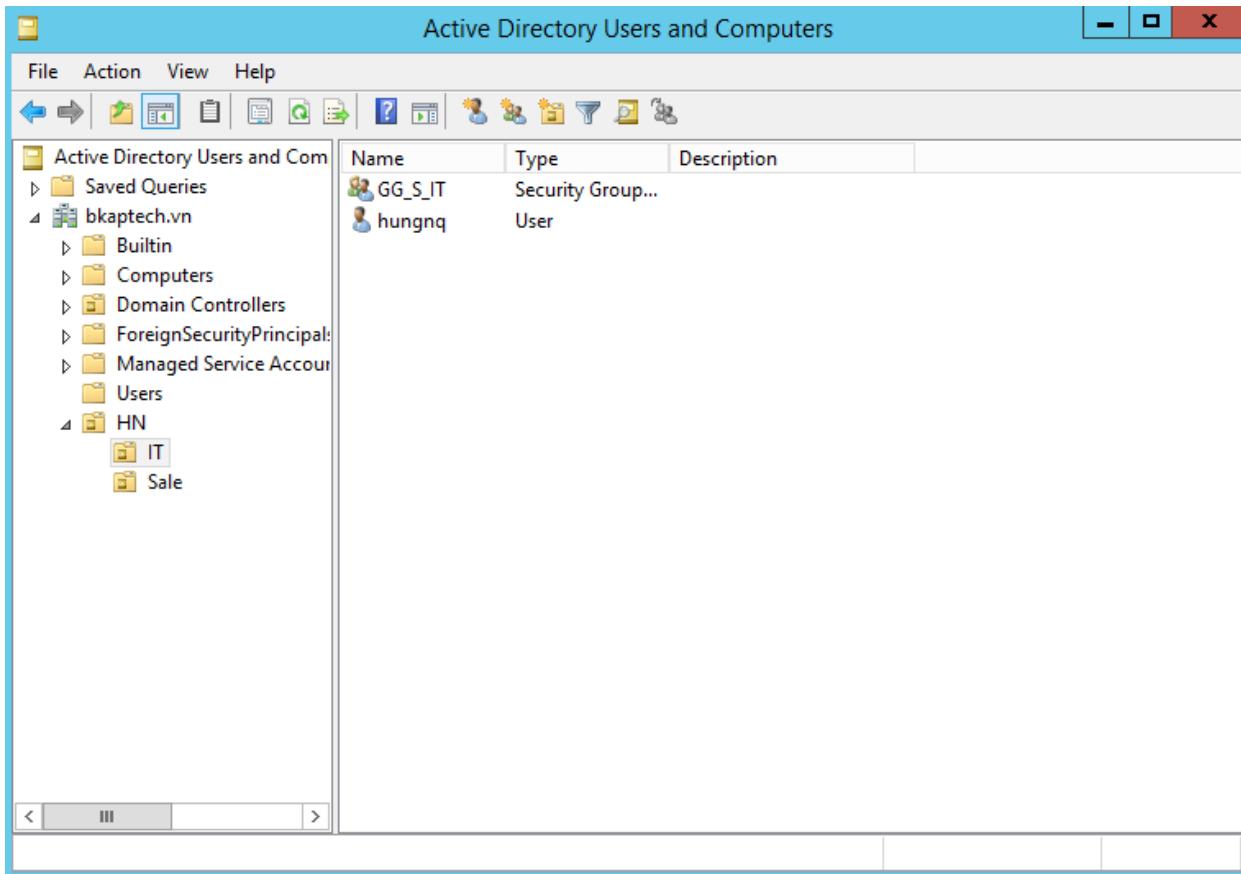
Thông số	BKAP-DC12-01	BKAP-SRV12-01	BKAP-WRK08-01
IP address	192.168.1.2	192.168.1.3	192.168.1.10
Gateway	192.168.1.1	192.168.1.1	192.168.1.1
Subnet Mask	255.255.255.0	255.255.255.0	255.255.255.0
DNS Server	192.168.1.2	192.168.1.2	192.168.1.2

Hướng dẫn chi tiết:

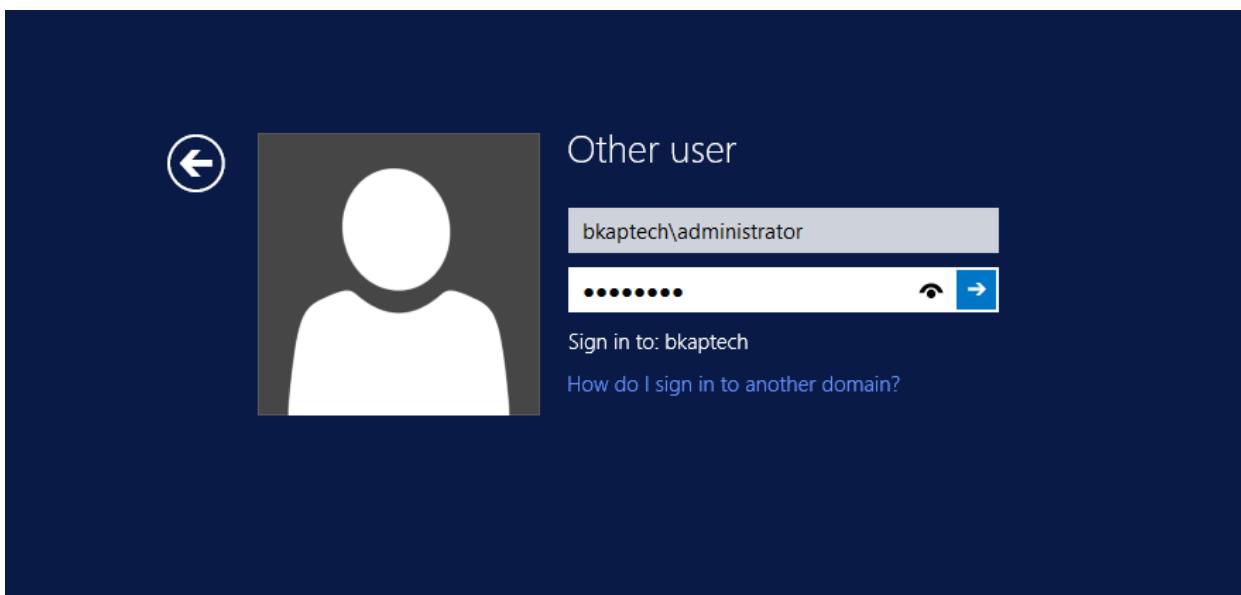
- Kết nối các máy ảo theo mô hình trên, thực hiện *ping* thông giữa các máy trong mạng.
- Trên máy *BKAP-DC12-01* thực hiện:
 - Cấu hình **DNS Server**, kiểm tra phân giải **DNS**.



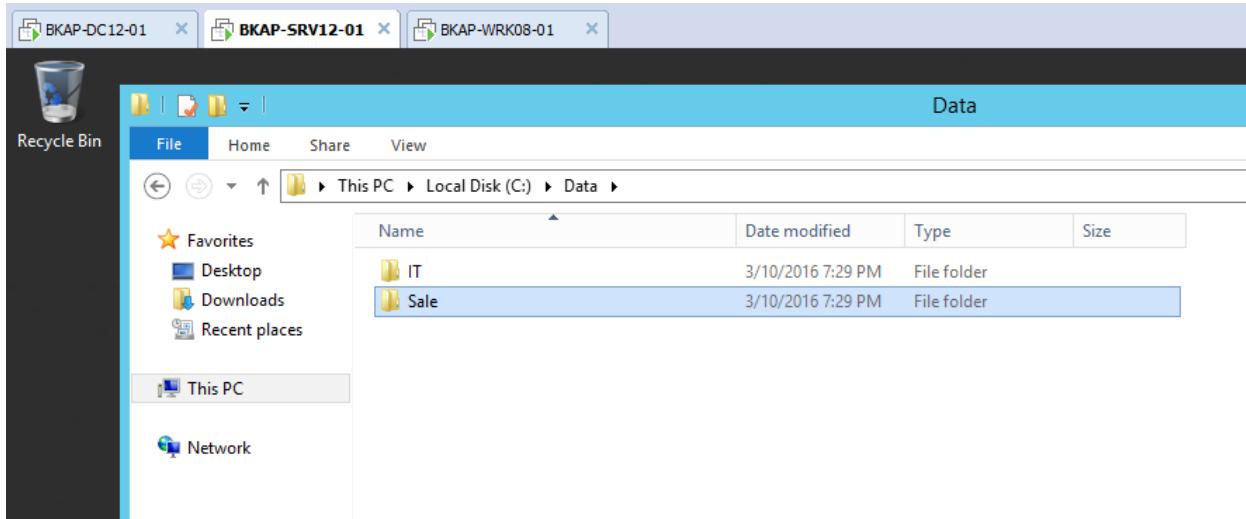
- Tạo *OU*, *Group*, *User* theo mô hình 11.2.



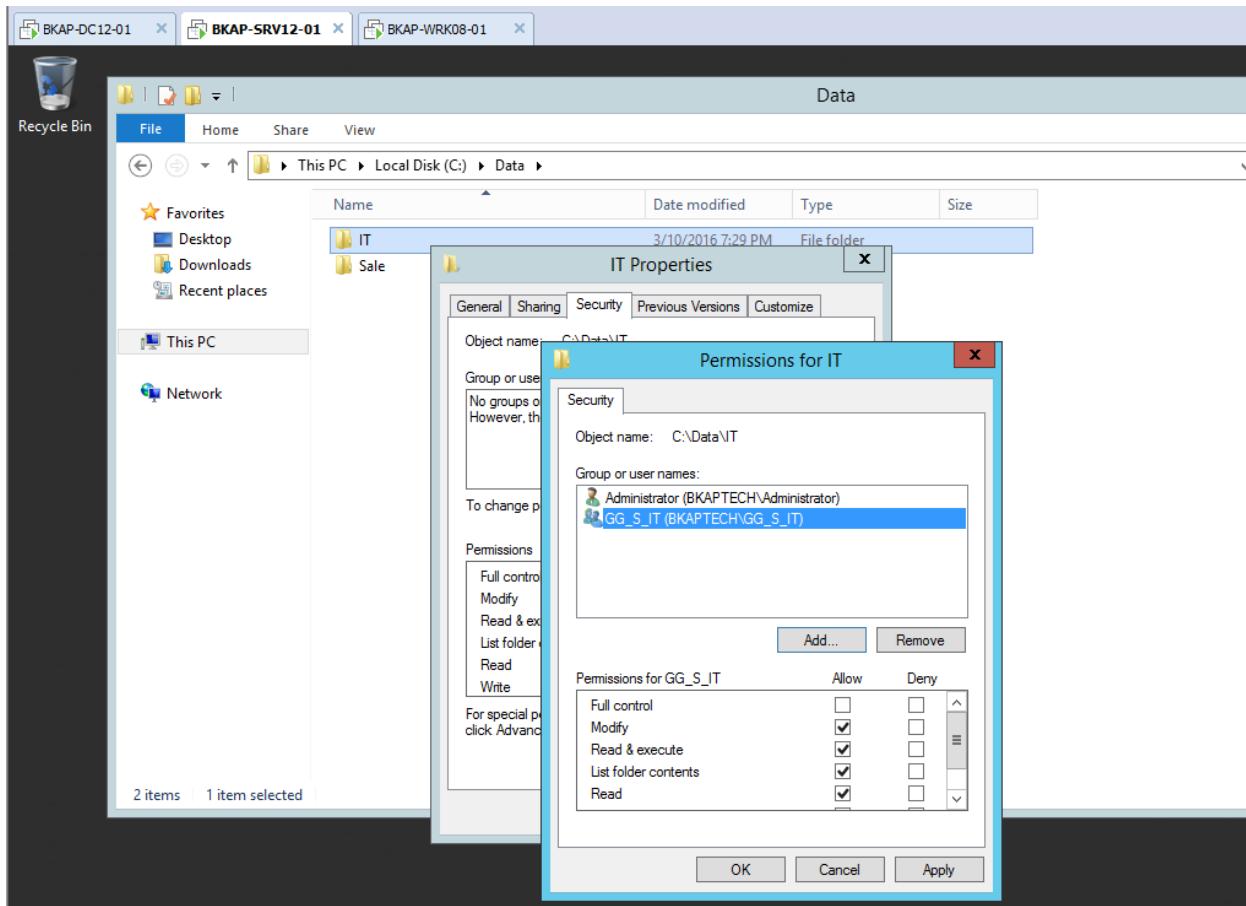
- Chuyển sang máy Server *BKAP-SRV12-01*, thực hiện :
 - Join vào *Domain*, đăng nhập bằng tài khoản *bkaptech\administrator*.

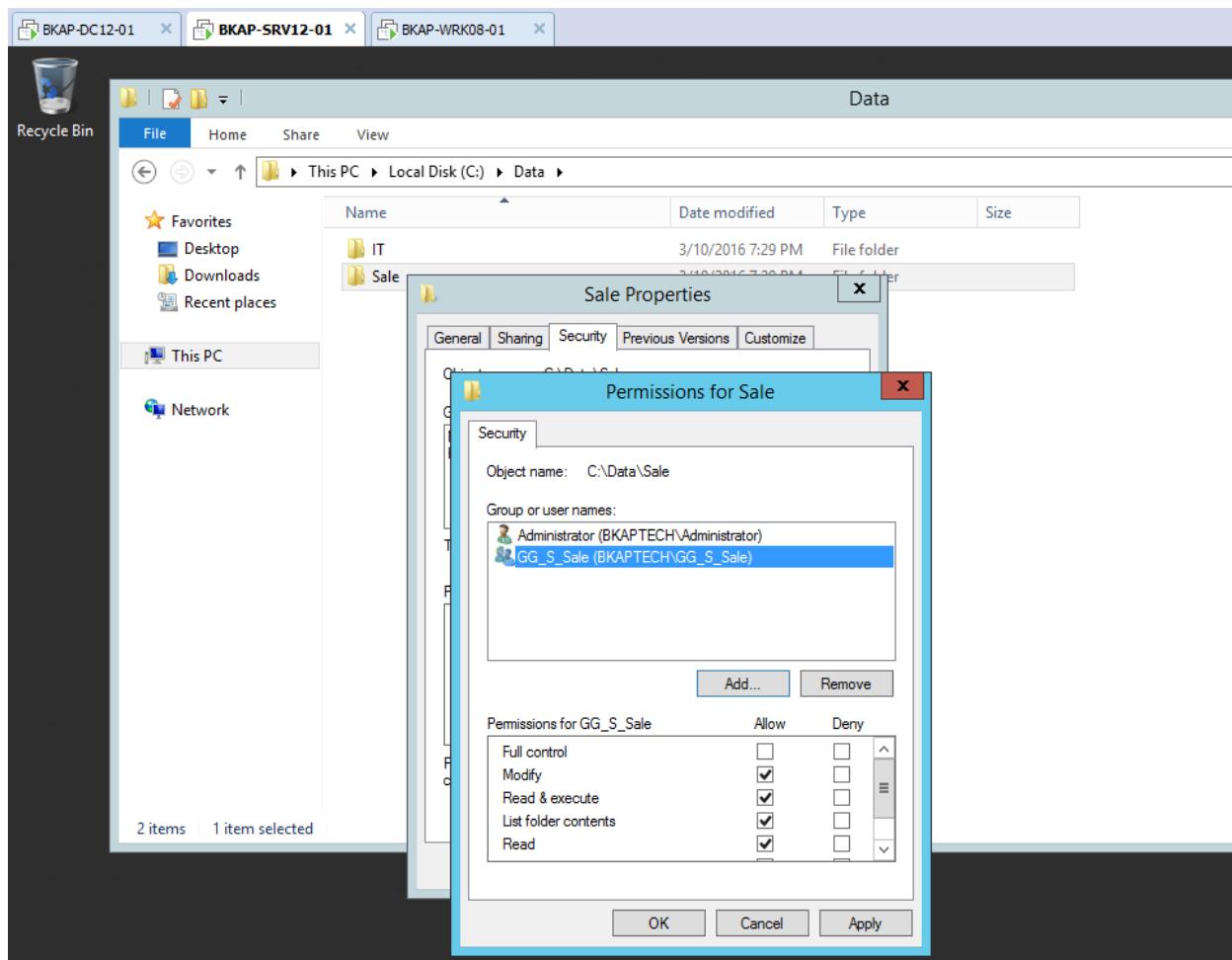


- Trong ô C , tạo thư mục **Data** , trong thư mục **Data** , tạo thư mục **IT** , **Sale**.

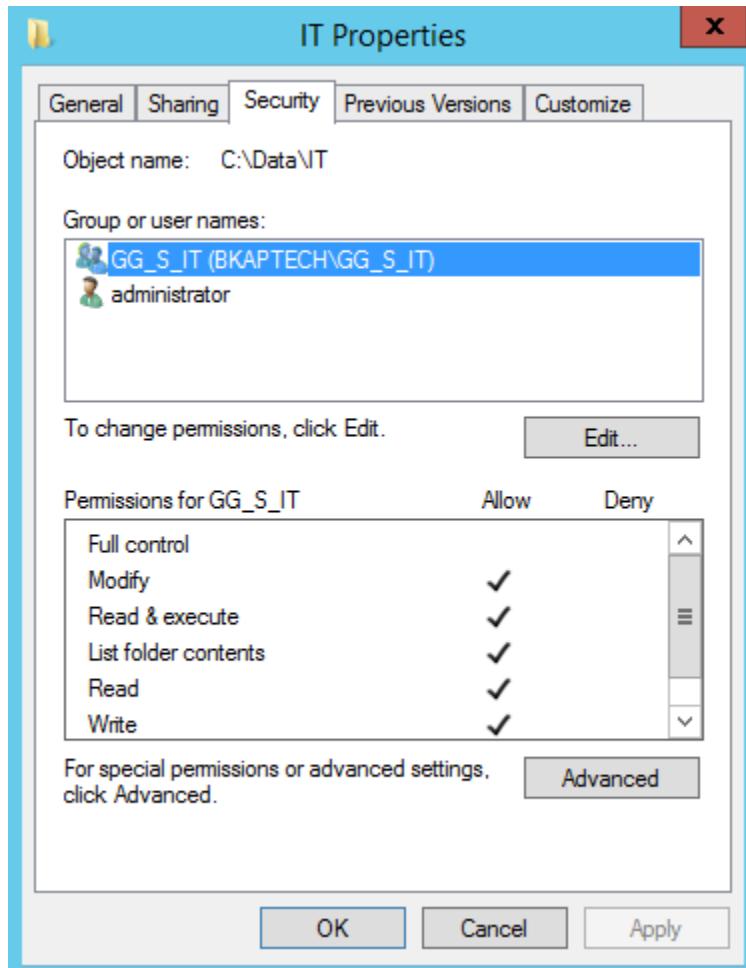


- Cấu hình phân quyền và chia sẻ dữ liệu:

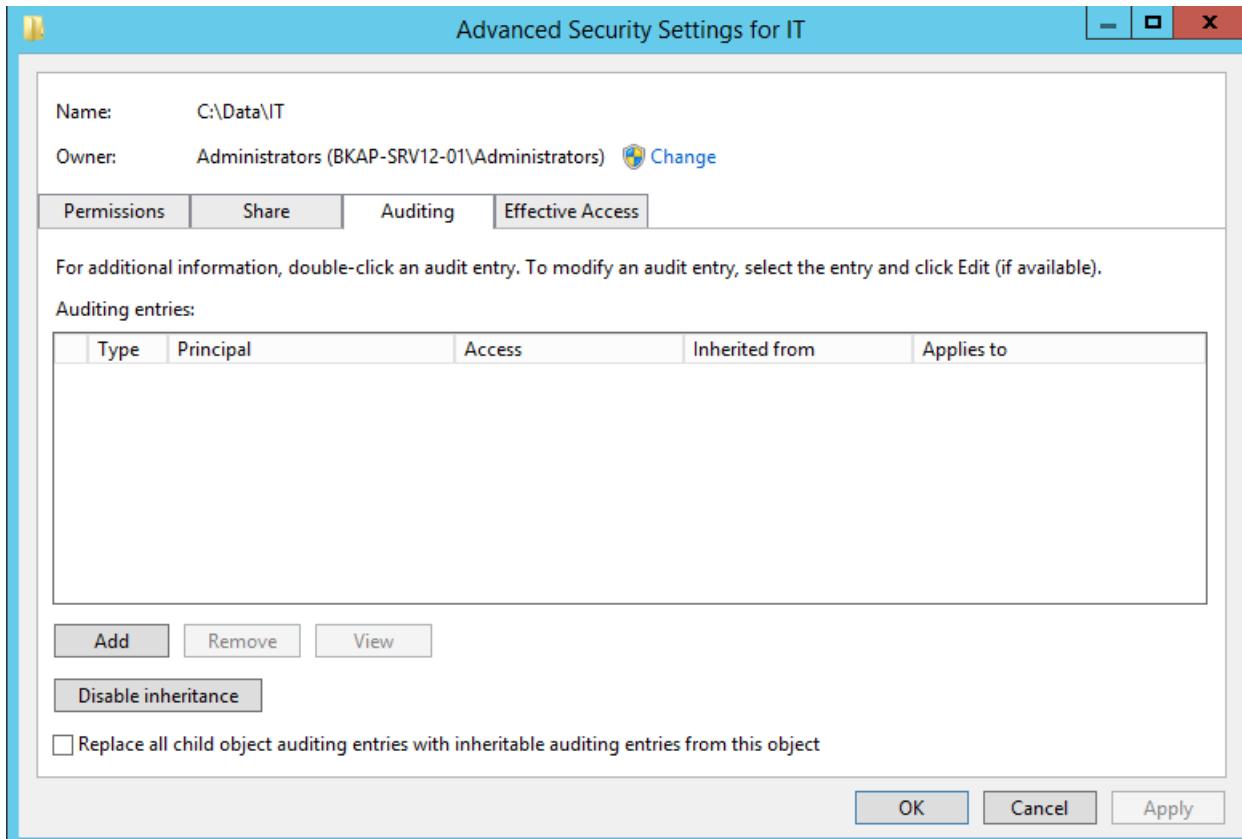




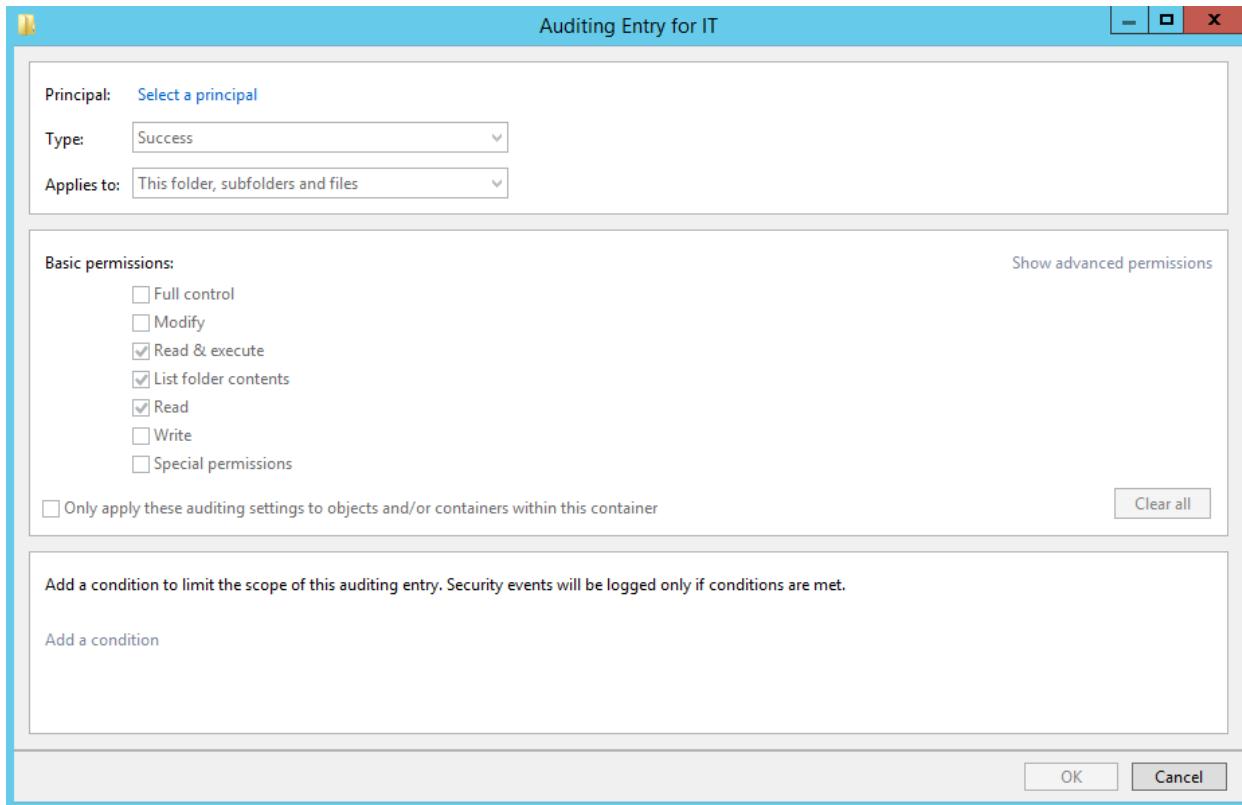
- Cấu hình ghi lại hoạt động của thư mục:
 - Trong cửa sổ **IT Properties**, click vào **Advanced**.



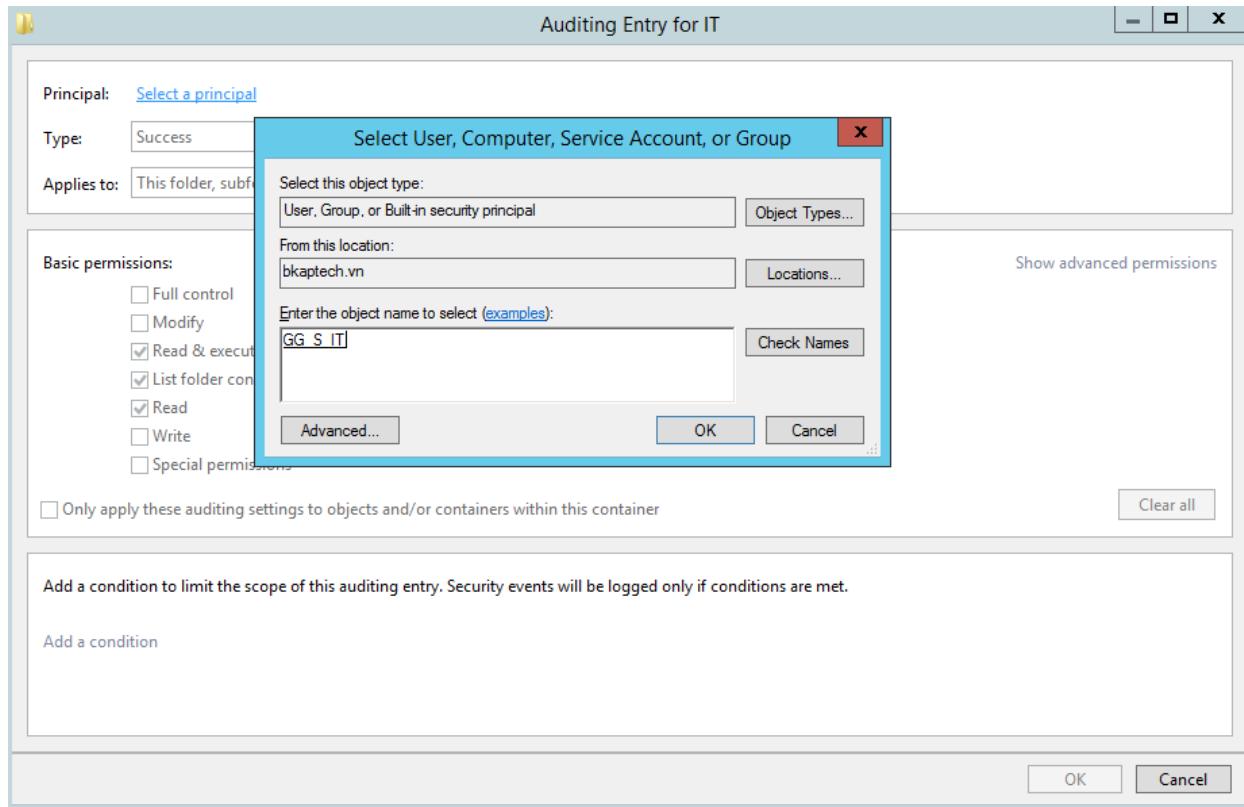
- Trong cửa sổ **Advanced Security Settings for IT**, click sang tab **Auditing**. Click vào **Add**.



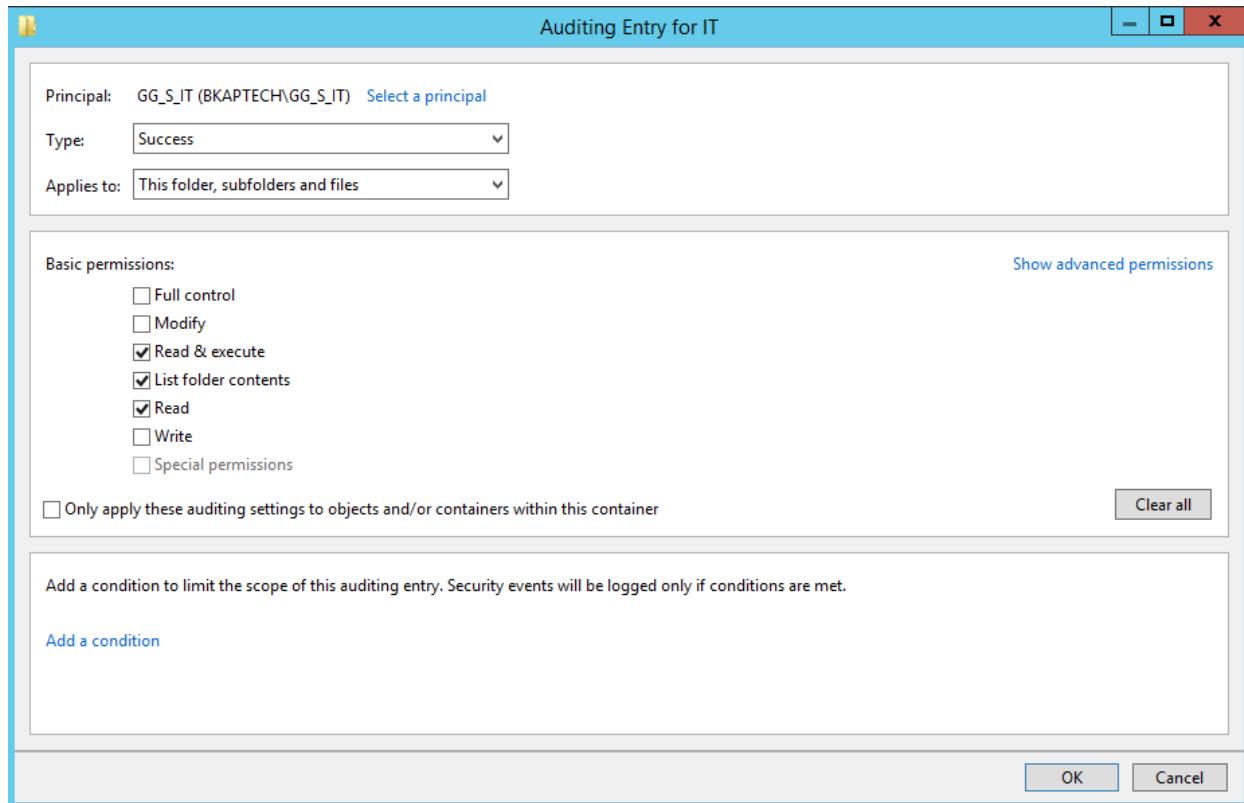
- Tại cửa sổ **Auditing Entry for IT**, click vào **Select a principal**.



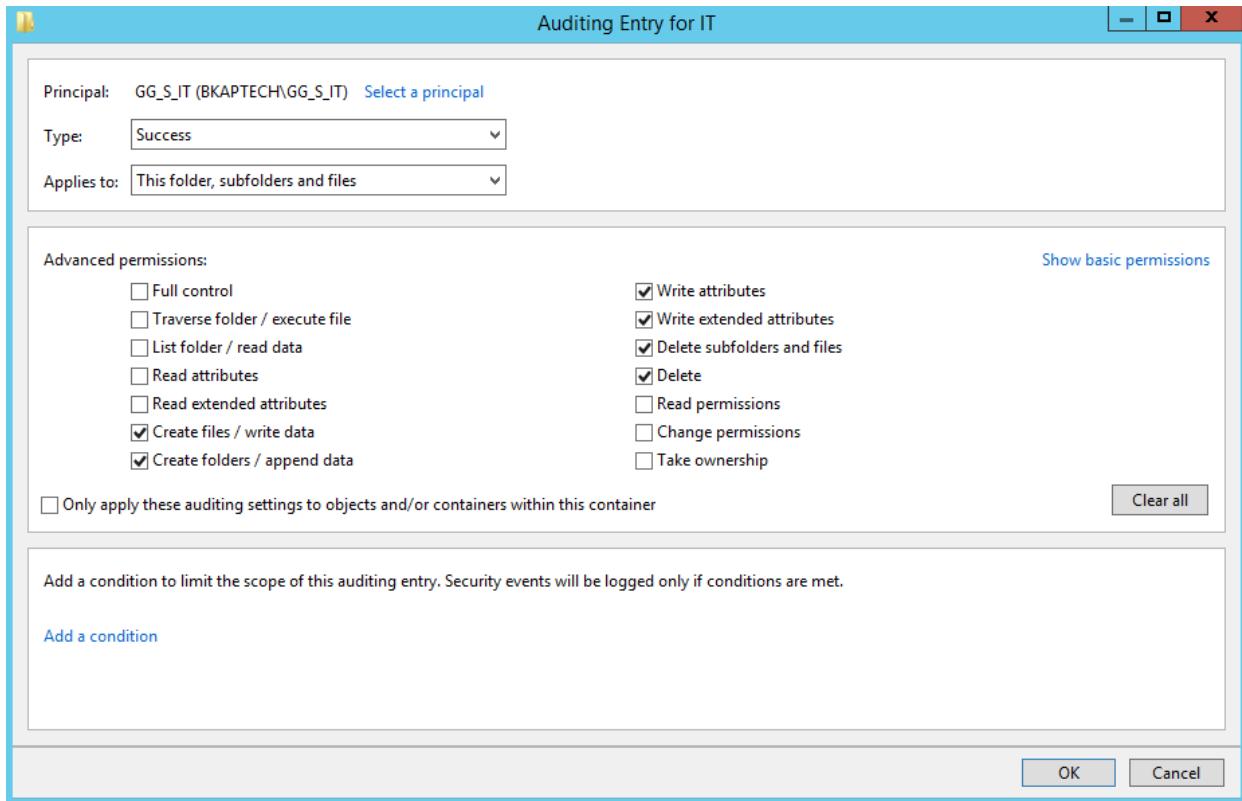
- Tại cửa sổ **Select User, Computer...** tiến hành add vào Group **GG_S_IT**.



- Tại cửa sổ **Auditing Entry for IT**, click vào **Show advanced permissions**.

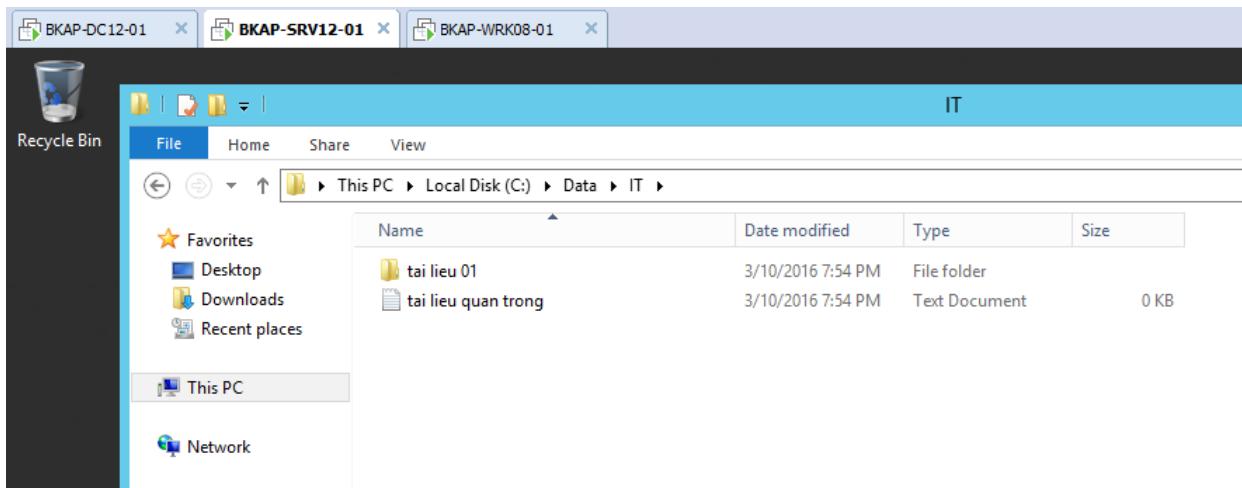


- Bỏ chọn các *permissions* được tích sẵn , tiến hành chọn vào các quyền theo hình sau:

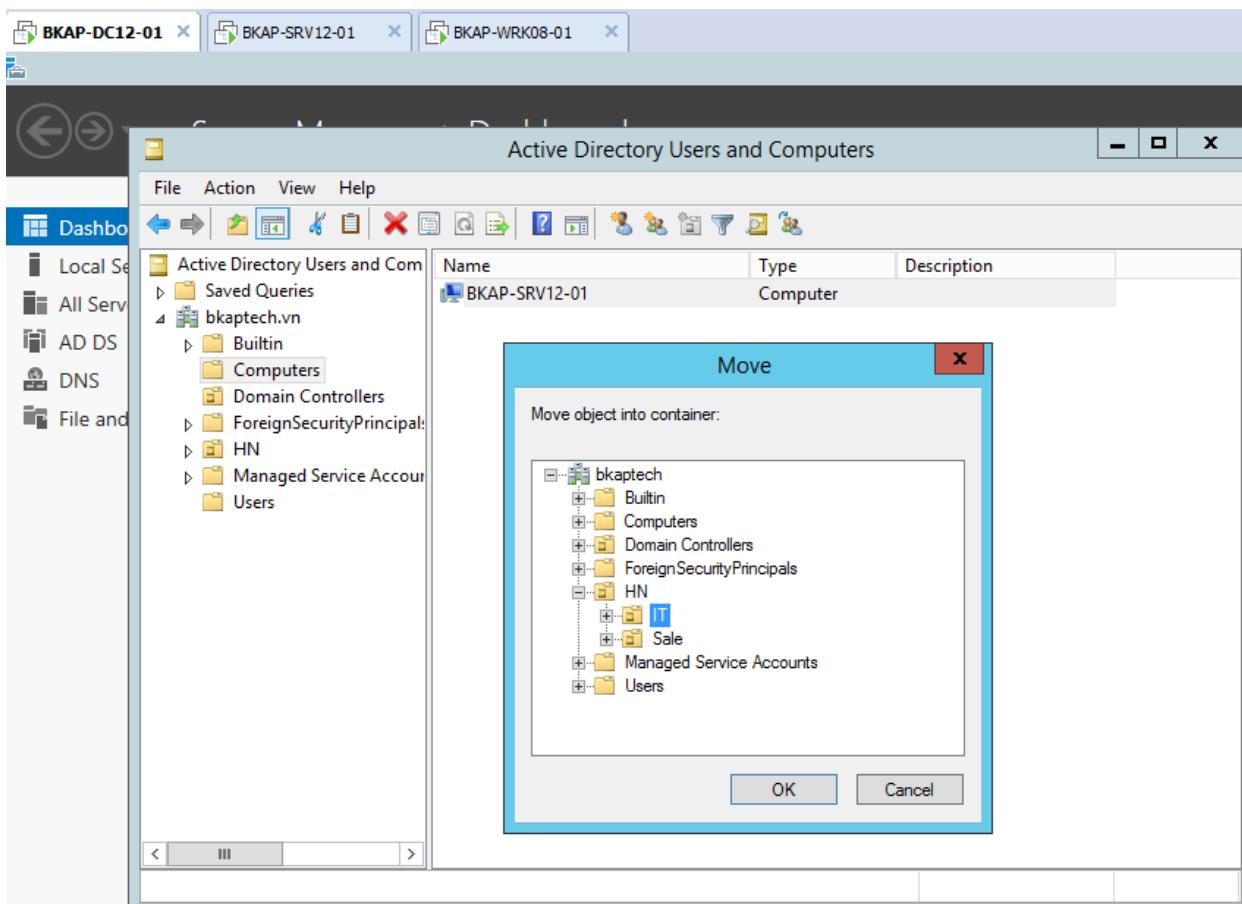


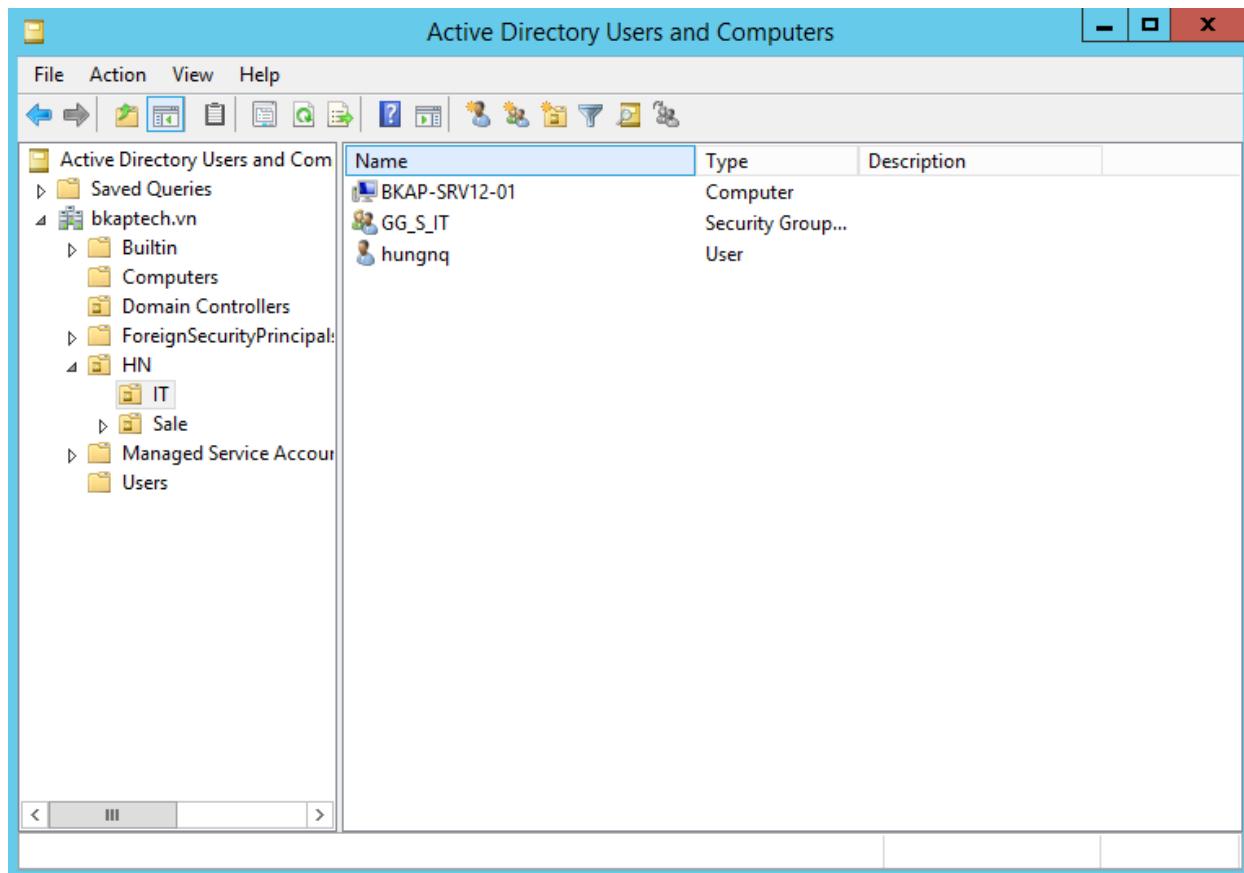
⇒ OK.

- Trong thư mục **IT**, tạo folder và file **txt**.

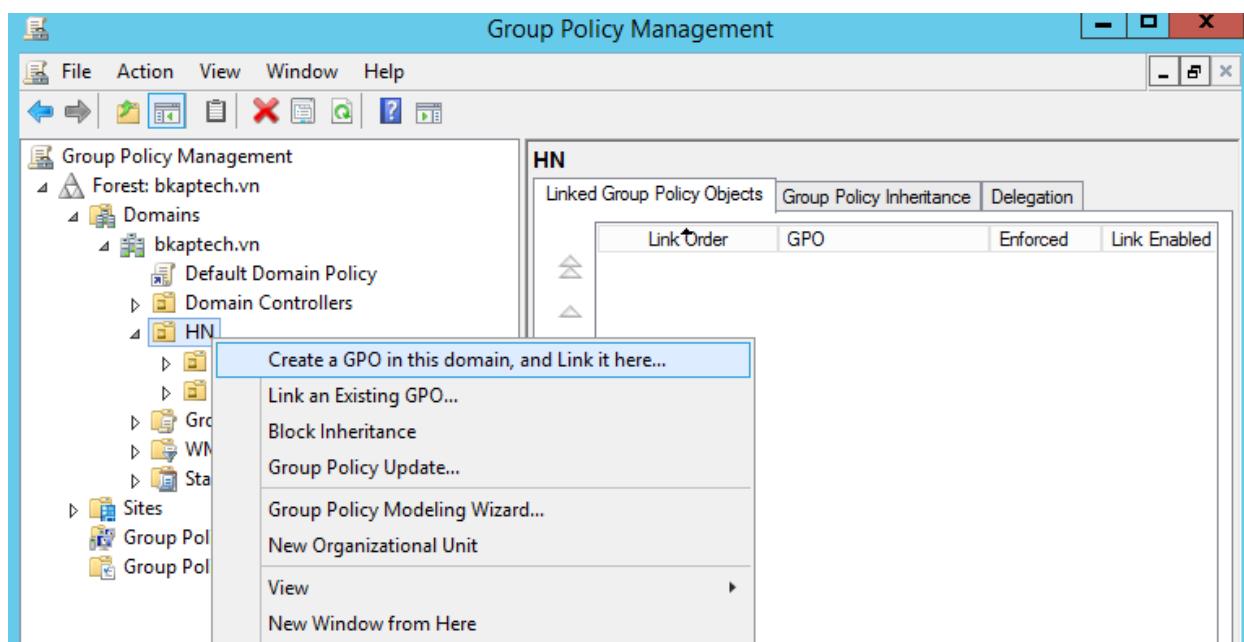


- Chuyển sang máy **BKAP-DC12-01**, triển khai chính sách ghi lại hoạt động thư mục:
 - Vào **Active Directory Users and Computers**, thực hiện **Move** máy server **BKAP-SRV12-01** vào OU **IT**.

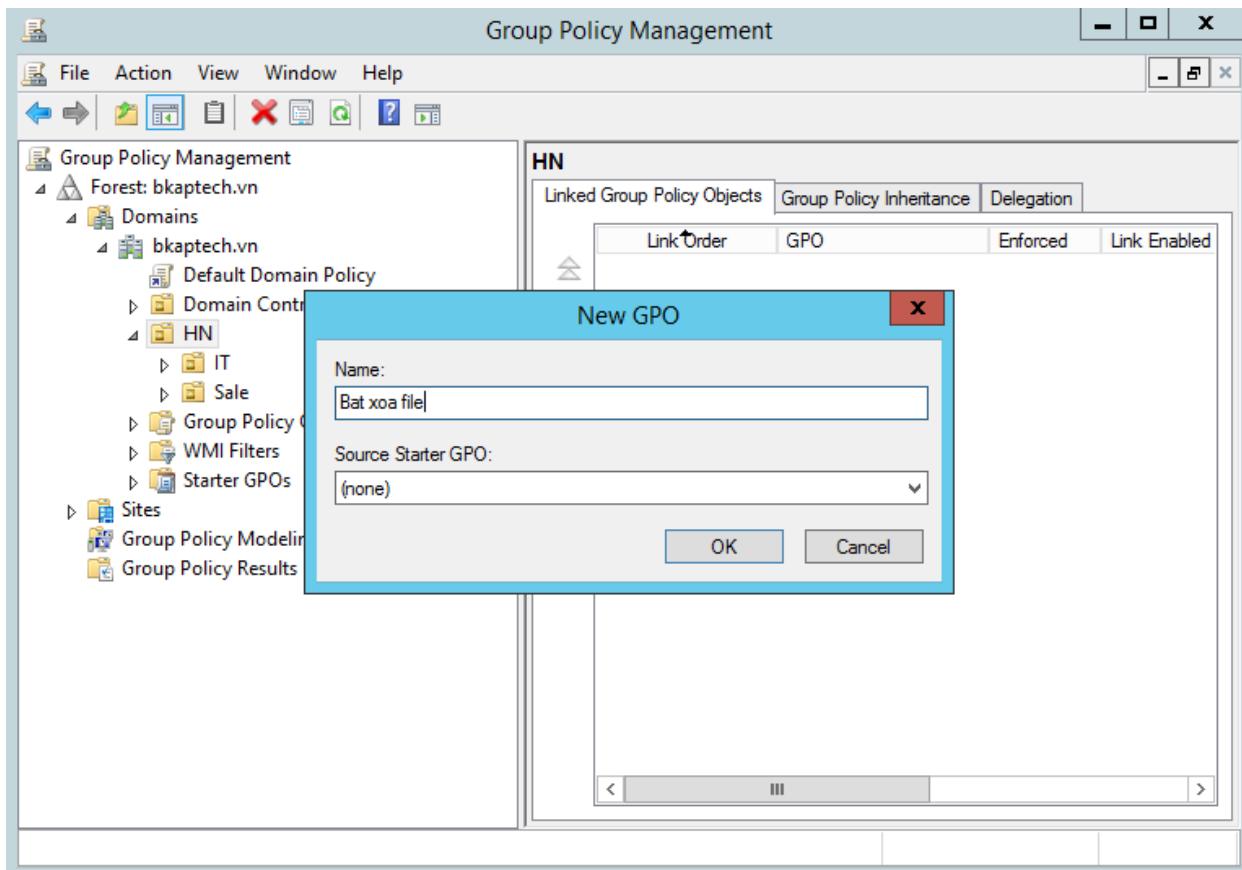




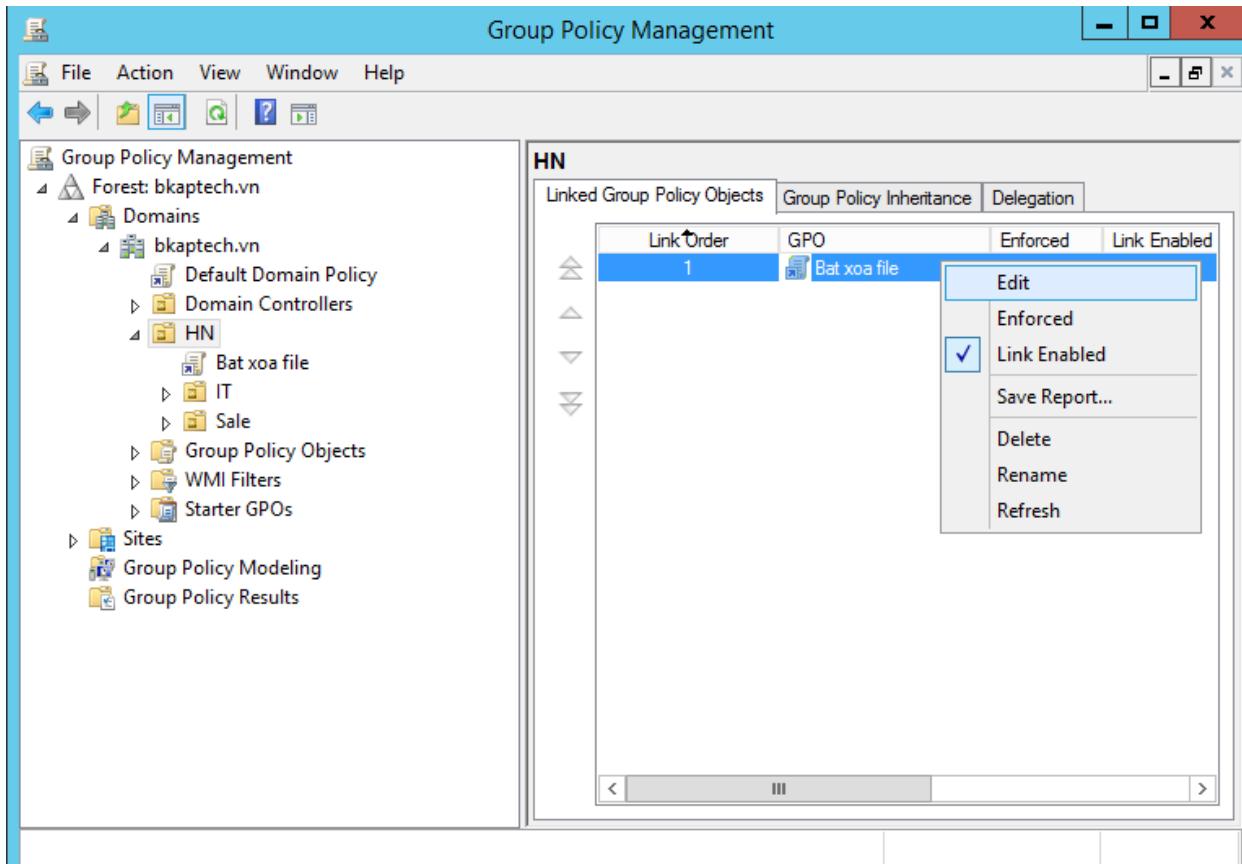
- Triển khai chính sách *xóa File* cho các phòng ban.
 - Vào **Group Policy Management**, click vào OU **HN**, chọn **Create a GPO in this domain..**



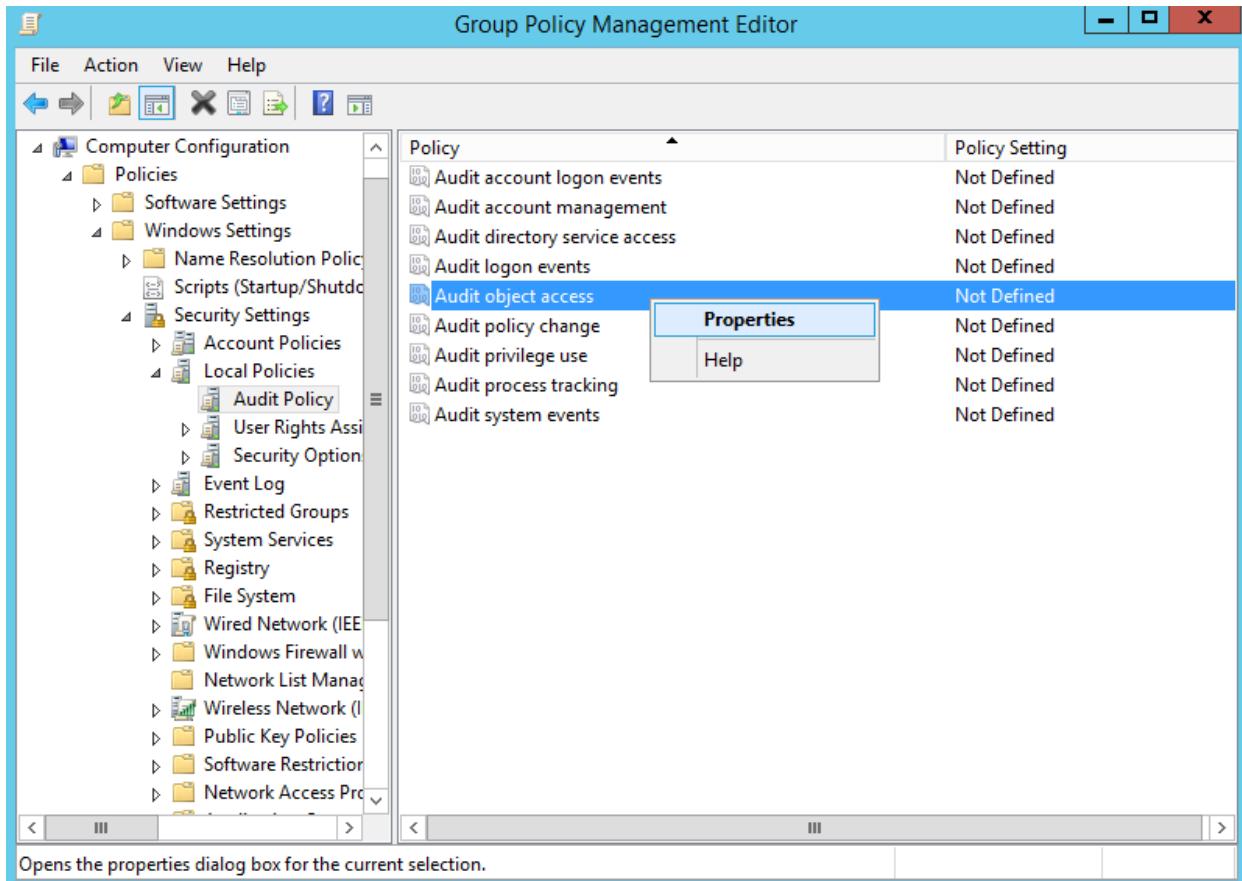
- Tại cửa sổ New GPO , nhập vào tên *Bat xoa File*.



- Click vào chính sách vừa tạo, chọn **Edit**.

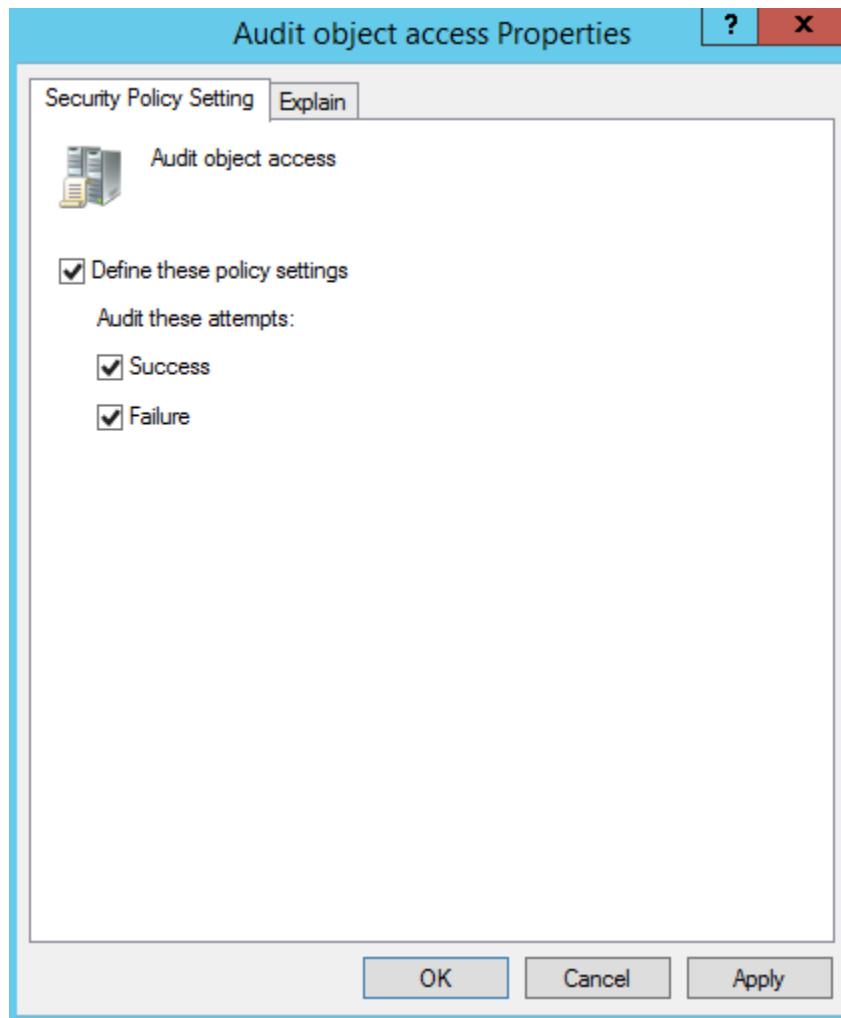


- Tại cửa sổ **Group Policy Management Editor**, chọn vào **Computer Configuration / Policies / Windows Settings / Security Settings / Local Policies / Audit Policy**. Chọn vào **Audit object access / Properties**.



Opens the properties dialog box for the current selection.

- Tại cửa sổ **Audit object access Properties** , click vào **Define these policy settings** , Success / Failure.



⇒ Gpupdate /force.

```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.

C:\Users\Administrator>
```

- Chuyển sang máy *BKAP-SRV12-01*, cập nhật chính sách.

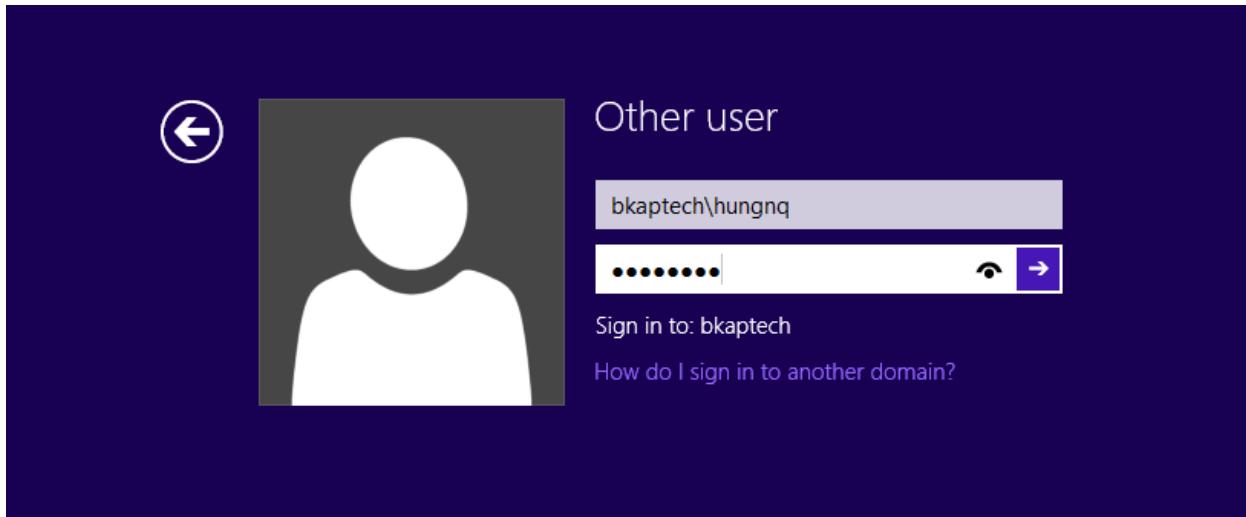
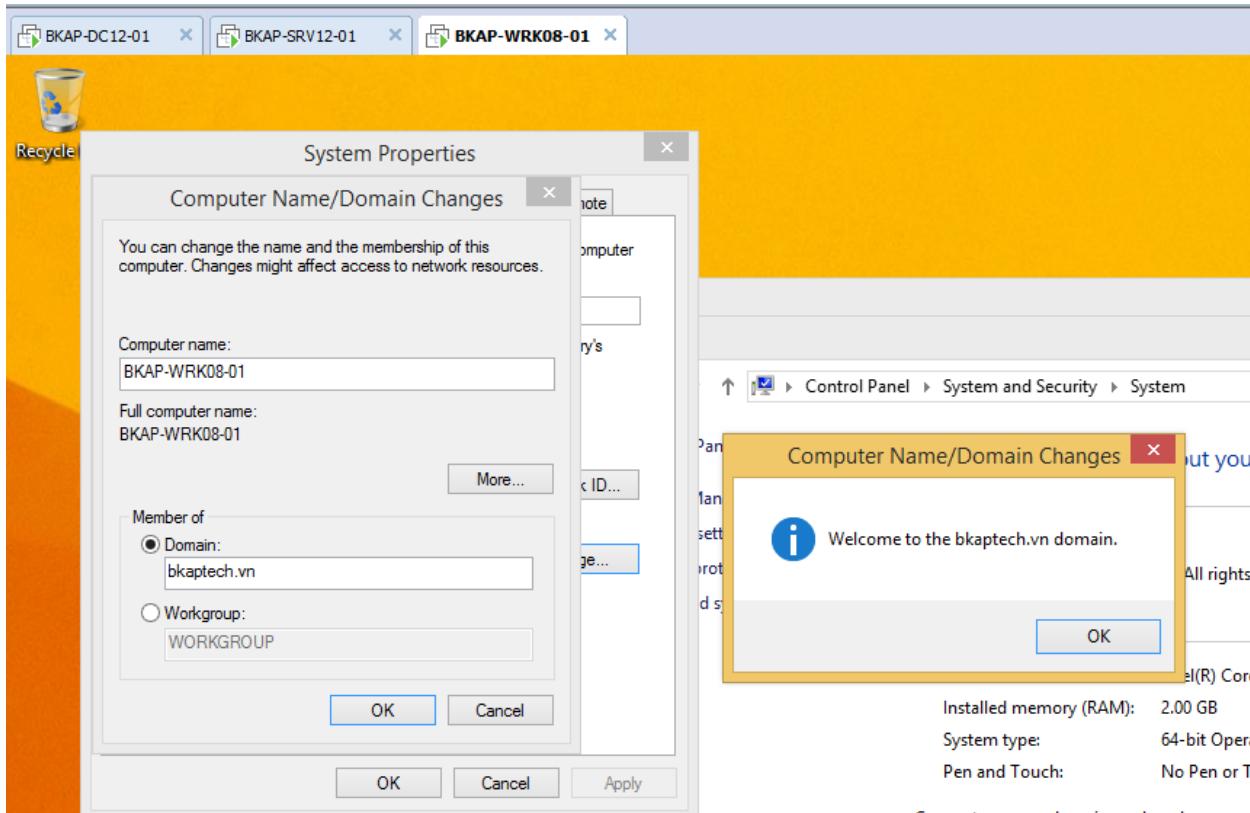
```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\administrator.BKAPTECH>gpupdate /force
Updating policy...

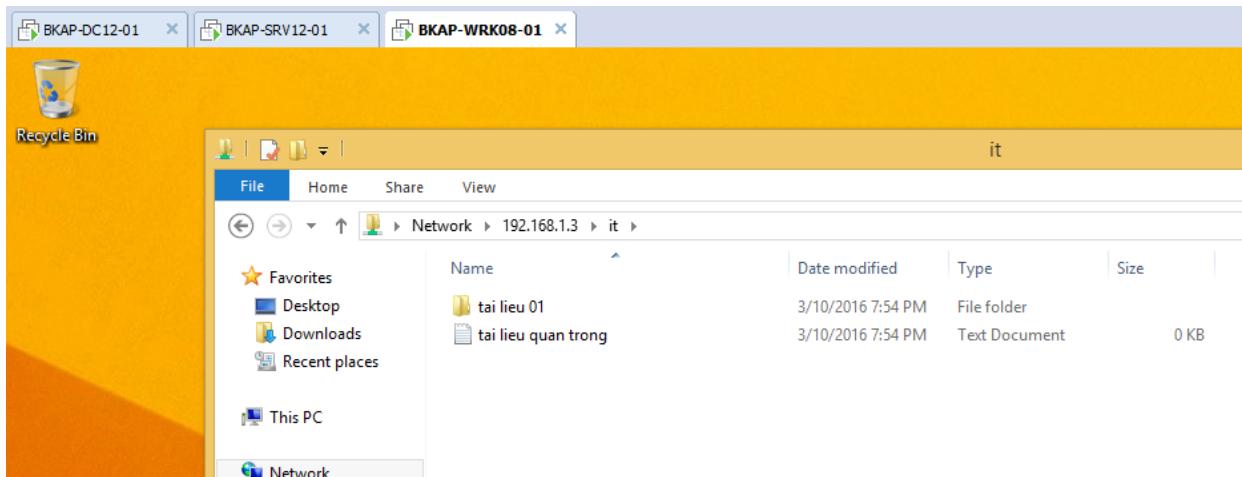
Computer Policy update has completed successfully.
User Policy update has completed successfully.

C:\Users\administrator.BKAPTECH>_
```

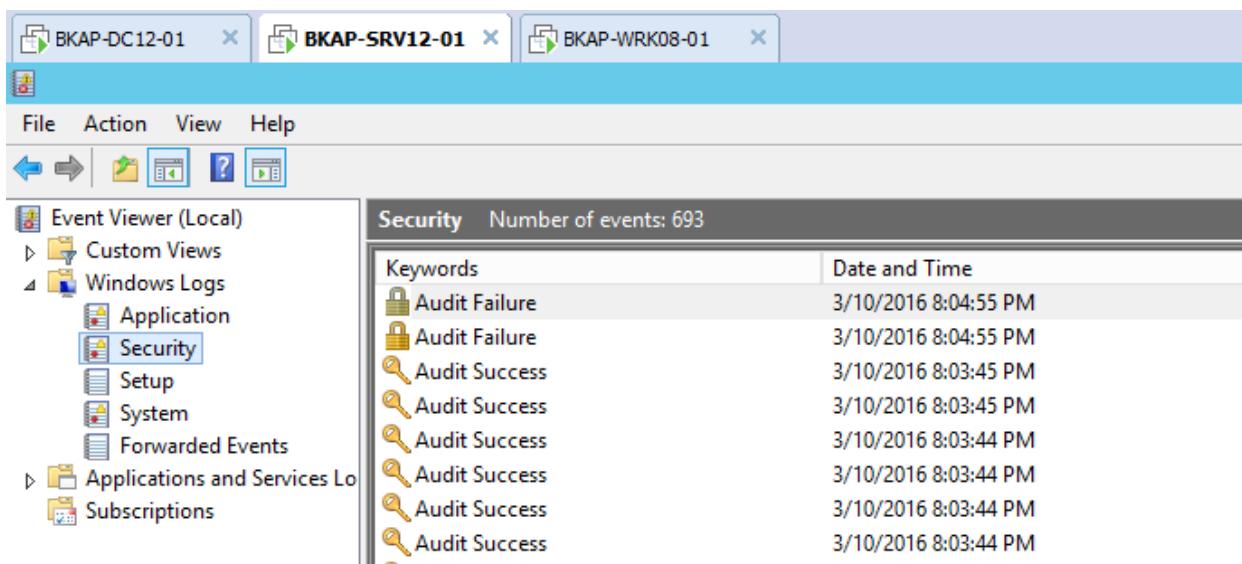
- Chuyển sang máy **Client**, thực hiện:
 - Join vào *Domain*, đăng nhập bằng tài khoản **hungnq** trong OU IT.



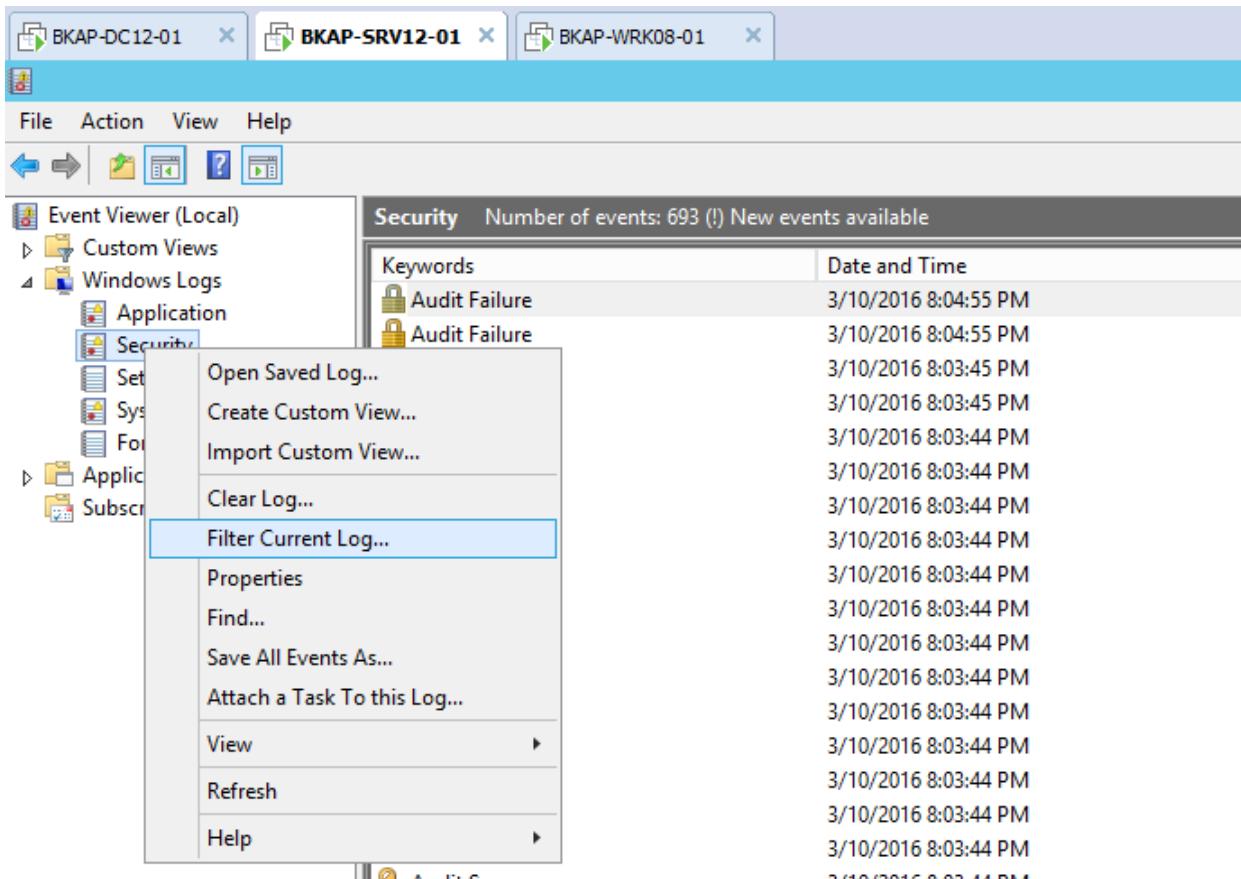
- Truy cập thư mục **IT** , xóa file , tạo thư mục mới.



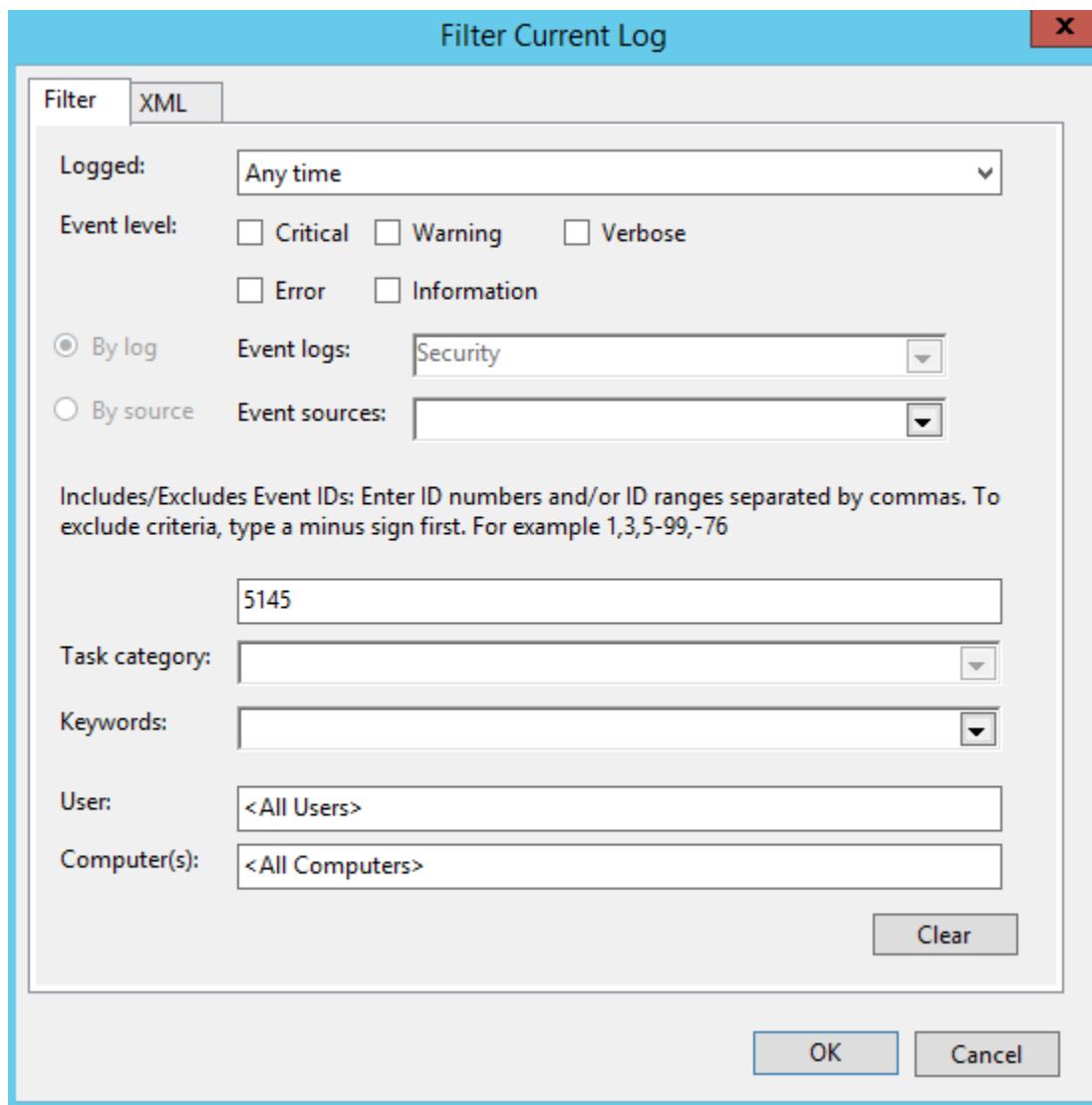
- Chuyển sang máy **BKAP-SRV12-01**, vào **Tools / Event Viewer**.
 - Tại **Windows Logs / Security**.



- Click chuột phải tại **Security** , chọn **Filter Current Log...**



- Trong cửa sổ **Filter Current Log**, nhập vào *Event IDs* **5145**.



- Kiểm tra Event đầu tiên.

The screenshot shows a Windows event viewer window. On the left, there's a tree view with nodes like 'Share Information', 'Access Request Information', and 'Access Check Results'. The main pane displays the following details for Event ID 5145:

Share Information:

- Share Name: \\?\IT
- Share Path: \\?\C:\Data\IT
- Relative Target Name: TAI LIEU 01

Access Request Information:

- Access Mask: 0x110080
- Accesses: DELETE, SYNCHRONIZE, ReadAttributes

Access Check Results:

Share Information:

Share Name: \\\?\IT
Share Path: \?\?(\C:\Data\IT
Relative Target Name: tai lieu quan trong.txt

Access Request Information:

Access Mask: 0x10080
Accesses: DELETE
ReadAttributes

Access Check Results:

DELETE: Granted by D:(A;;0x1301bf;;;S-1-5-21-626577198-345122506-3767312900-1602)
ReadAttributes: Granted by D:(A;;0x1301bf;;;S-1-5-21-626577198-345122506-3767312900-1602)



- Tài liệu mới được tạo .

Event Properties - Event 5145, Microsoft Windows security auditing.

General Details

A network share object was checked to see whether client can be granted desired access.

Subject:

Security ID:	BKAPTECH\hungnq
Account Name:	hungnq
Account Domain:	BKAPTECH
Logon ID:	0xB6121

Network Information:

Object Type:	File
Source Address:	192.168.1.10
Source Port:	58480

Share Information:

Share Name:	\\\IT
Share Path:	\??\C:\Data\IT
Relative Target Name:	TAI LIEU QUAN TRONG 002

Access Request Information:

Access Mask:	0x100081
Accesses:	SYNCHRONIZE ReadData (or ListDirectory) ReadAttributes

Access Check Results:

SYNCHRONIZE:	Granted by D:(A;;0x1301bf;;;S-1-5-21-626577198-345122506-3767312900-1602)
ReadData (or ListDirectory):	Granted by D:(A;;0x1301bf;;;S-1-5-21-626577198-345122506-3767312900-1602)
ReadAttributes:	Granted by D:(A;;0x1301bf;;;S-1-5-21-626577198-345122506-3767312900-1602)

Log Name: Security

Source: Microsoft Windows security Logged: 3/10/2016 8:03:45 PM

Event ID: 5145 Task Category: Detailed File Share

Level: Information Keywords: Audit Success

User: N/A Computer: BKAP-SRV12-01.bkaptech.vn

OpCode: Info

More Information: [Event Log Online Help](#)

Copy **Close**

