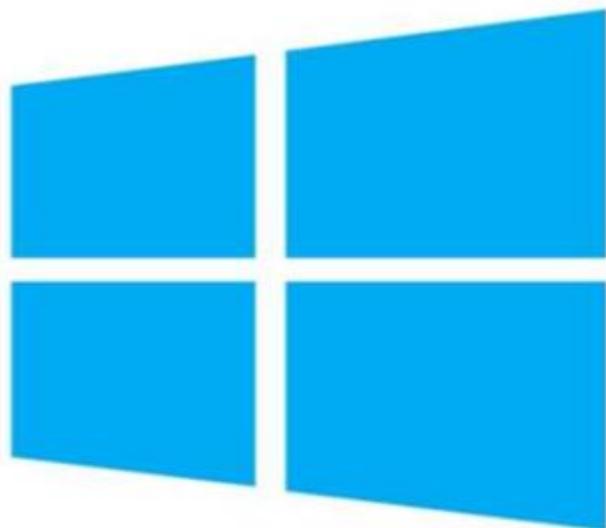


QUẢN TRỊ HỆ THỐNG MẠNG WINDOWS SERVER 2012 PHẦN 3



WINDOWS SERVER 2012

MỤC LỤC

Bài 1: TRIỂN KHAI CẤU HÌNH DỊCH VỤ MẠNG NÂNG CAO	3
1.1 Cài đặt và cấu hình DHCP Failover	3
1.2 Cấu hình thiết lập DNS nâng cao	22
Bài 2: TRIỂN KHAI CẤU HÌNH FILE SERVICES NÂNG CAO.	64
2.1 Cấu hình iSCSI Storage	64
2.2 Cấu hình cơ sở hạ tầng phân loại tập tin.	117
Bài 3: TRIỂN KHAI CẤU HÌNH DYNAMIC ACCESS CONTROL.....	152
3.Cấu hình Dynamic Access Control (DAC)	152
Bài 4: TRIỂN KHAI CẤU HÌNH AD DS NÂNG CAO	187
4.1 Triển khai Child Domains trong AD DS.....	187
4.2 Thực hiện Trust Forest	207
4.3 Cấu hình Active Directory Domain Services Sites and Replication.....	242
Bài 5: TRIỂN KHAI DỊCH VỤ ACTIVE DIRECTORY RIGHTS MANAGEMENT SERVICES	281
5.1 Cấu hình Active Directory Rights Management Services – P1	281
5.2 Cấu hình Active Directory Rights Management Services – P2	332
5.3 Cấu hình Active Directory Rights Management Services – P3	380
Bài 6: TRIỂN KHAI DỊCH VỤ DIRECT ACCESS SERVER	422
6. Cài đặt và cấu hình Direct Access Server	422
Bài 7: TRIỂN KHAI NETWORK LOAD BALANCING.....	548
7. Triển khai Network Load Balancing	548
Bài 8: TRIỂN KHAI FAILOVER CLUSTERING	581
8. Cấu hình Failover Clustering	581
Bài 9 : SAO LUƯ VÀ PHỤC HỒI DỮ LIỆU SỬ DỤNG WINDOWS SERVER BACKUP.....	646
9. Sao lưu và phục hồi dữ liệu sử dụng Windows Server Backup	646

Bài 1:**TRIỂN KHAI CẤU HÌNH DỊCH VỤ MẠNG NÂNG CAO**

Các nội dung chính sẽ được đề cập:

- ✓ Cài đặt và cấu hình nâng cao DHCP.
- ✓ Cấu hình thiết lập DNS nâng cao.

1.1 Cài đặt và cấu hình DHCP Failover.**1.Yêu cầu bài lab :**

+ Cấu hình nâng cao dịch vụ **DHCP**.

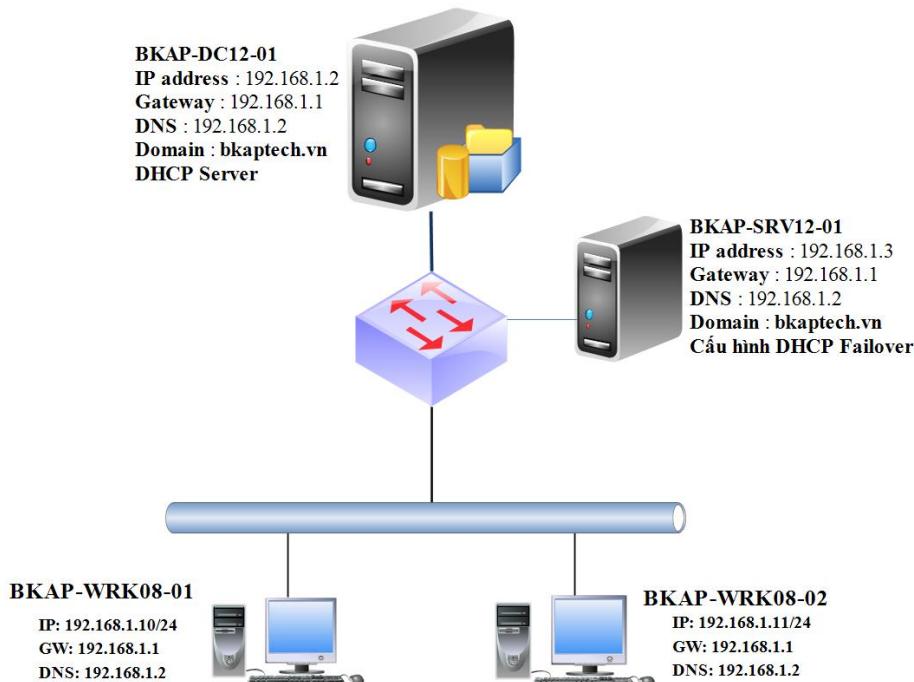
2.Yêu cầu chuẩn bị :

- + Chuẩn bị máy *BKAP-DC12-01* làm Domain Controller quản lý miền *bkaptech.vn*.
- + Chuẩn bị máy *BKAP-SRV12-01* ,cấu hình DHCP Failover.
- + Chuẩn bị máy Client *BKAP-WRK08-01* kiểm tra.

3.Mô hình Lab :

HỆ THỐNG ĐÀO TẠO CNTT QUỐC TẾ BACHKHOA-APTECH

Lab 1.1 Cài đặt và cấu hình dịch vụ nâng cao DHCP



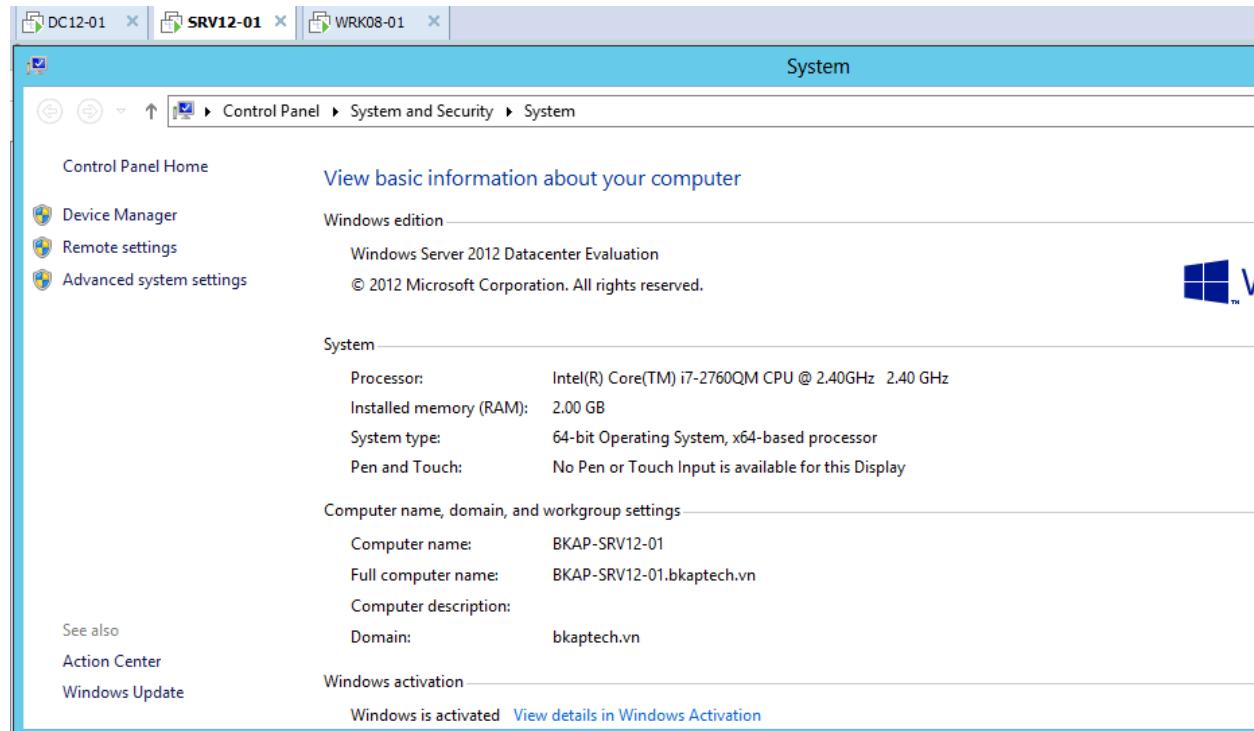
Hình 1.1

Sơ đồ địa chỉ như sau :

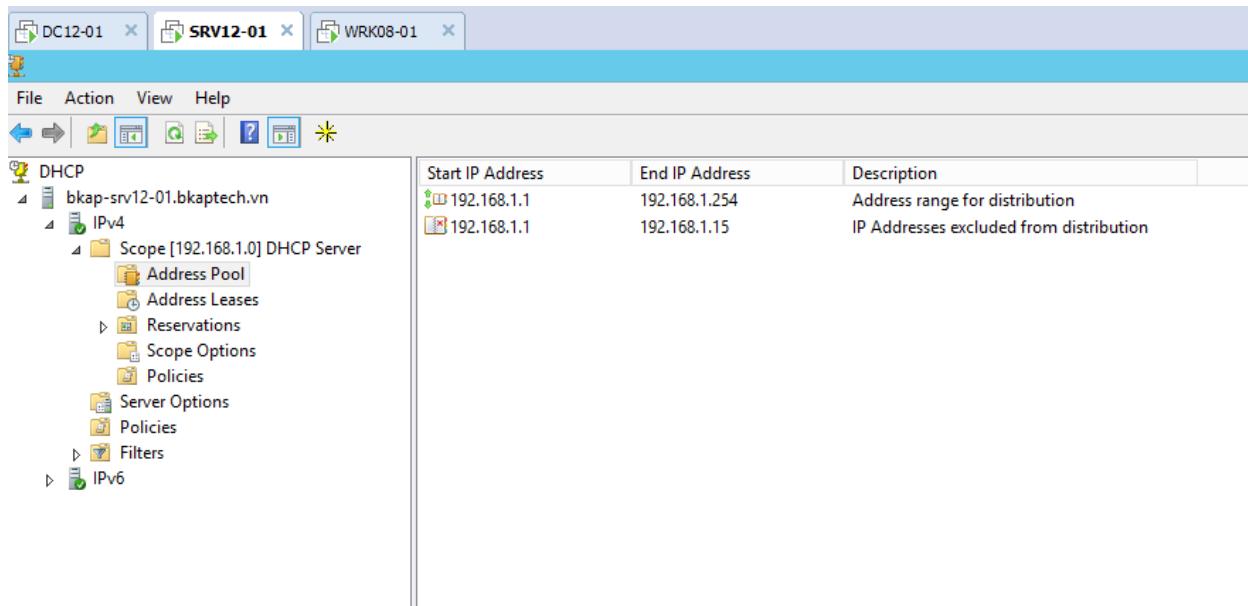
Thông số	BKAP-DC12-01	BKAP-SRV12-01	BKAP-WRK08-01
<i>IP address</i>	192.168.1.2	192.168.1.3	192.168.1.10
<i>Subnet Mask</i>	255.255.255.0	255.255.255.0	255.255.255.0
<i>Gateway</i>	192.168.1.1	192.168.1.1	192.168.1.1
<i>DNS Server</i>	192.168.1.2	192.168.1.2	192.168.1.2

Hướng dẫn chi tiết :

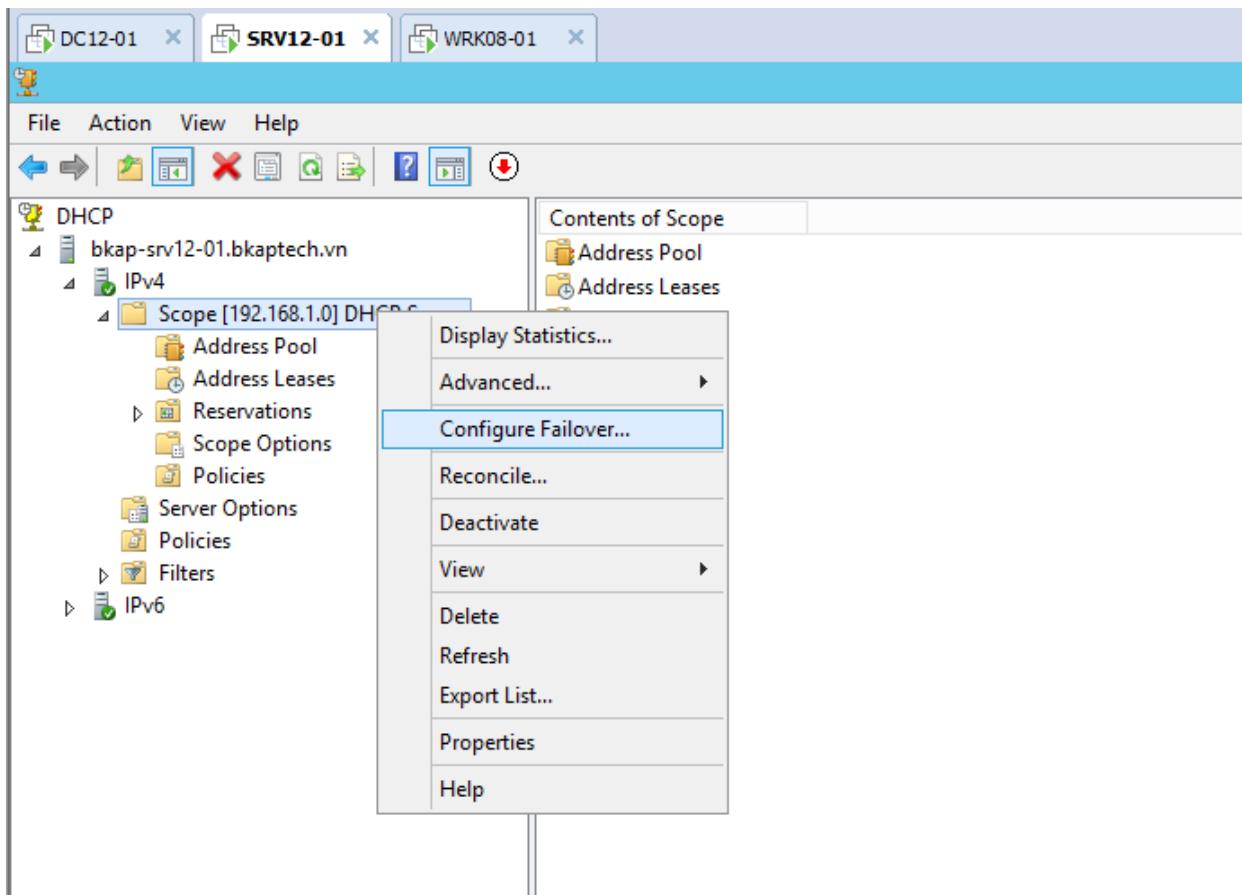
- Thực hiện trên máy **BKAP-DC12-01**, cài đặt dịch vụ **DHCP Server**. (xem lại *bài lab 6.1 Module 70-410*)
- Chuyển sang máy **BKAP-SRV12-01**:
 - Join vào miền **bkaptech.vn**. (đăng nhập bằng tài khoản *local*).



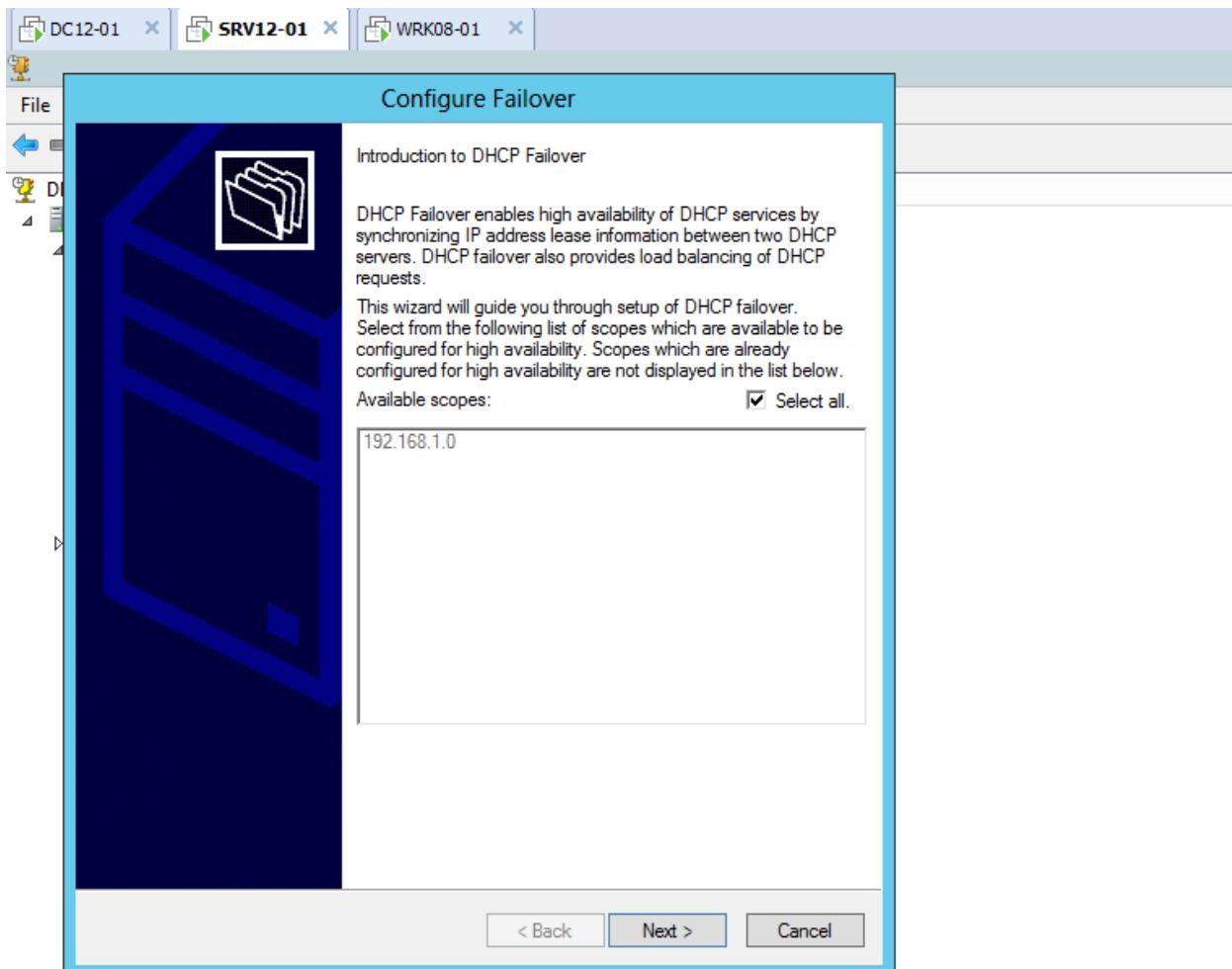
- Cài đặt và cấu hình dịch vụ **DHCP Server**.



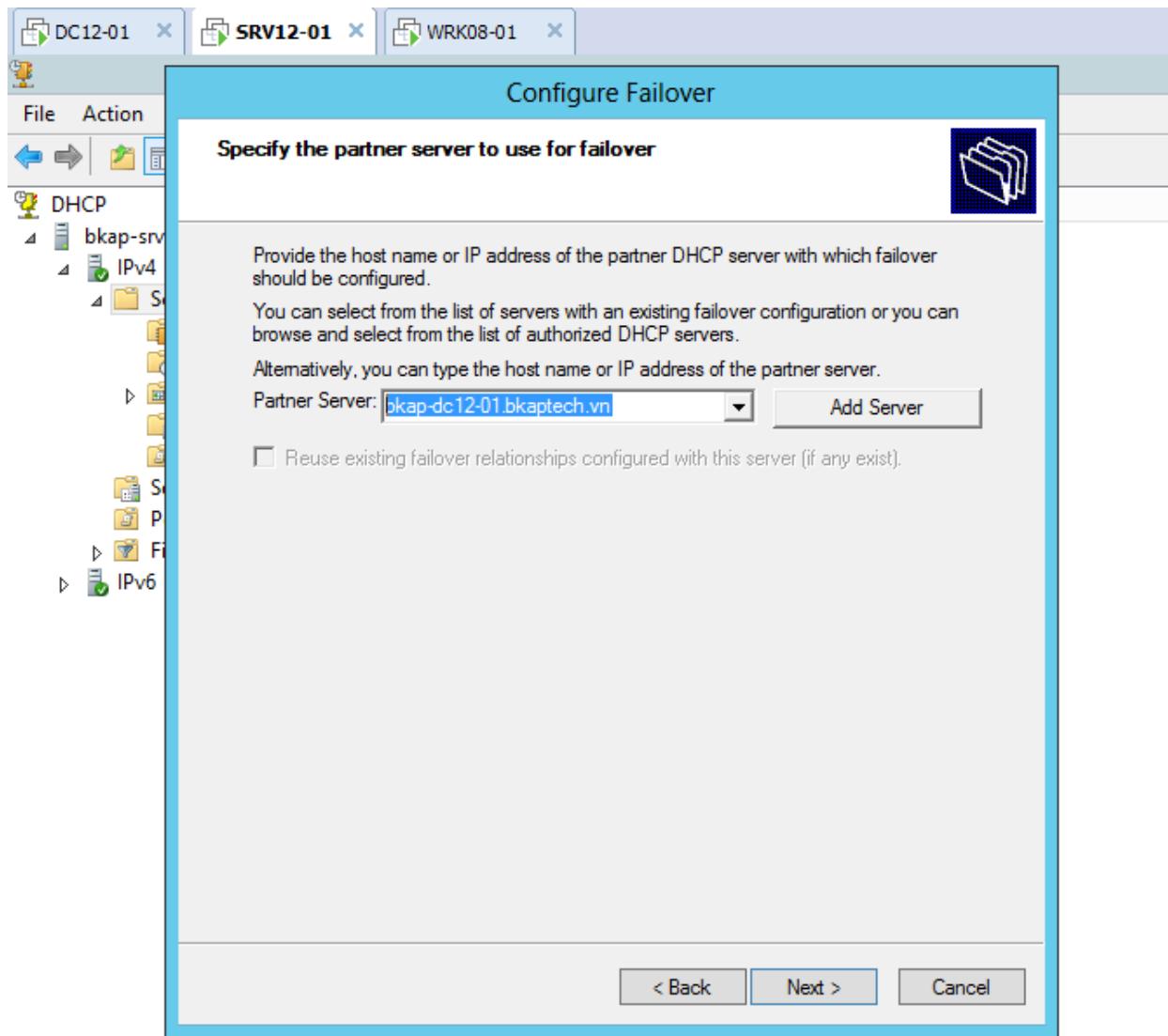
- Cấu hình tính năng **Failover DHCP** (Cấu hình cơ chế **Load-Balancing**).
 - Chọn **Scope** mà cả 2 *DHCP Server* sẽ dùng để chạy **Failover** (bước này tương đương tạo **1 Failover Relationships**).
 - Click chuột phải vào **Scope** vừa tạo, chọn **Configure Failover...**



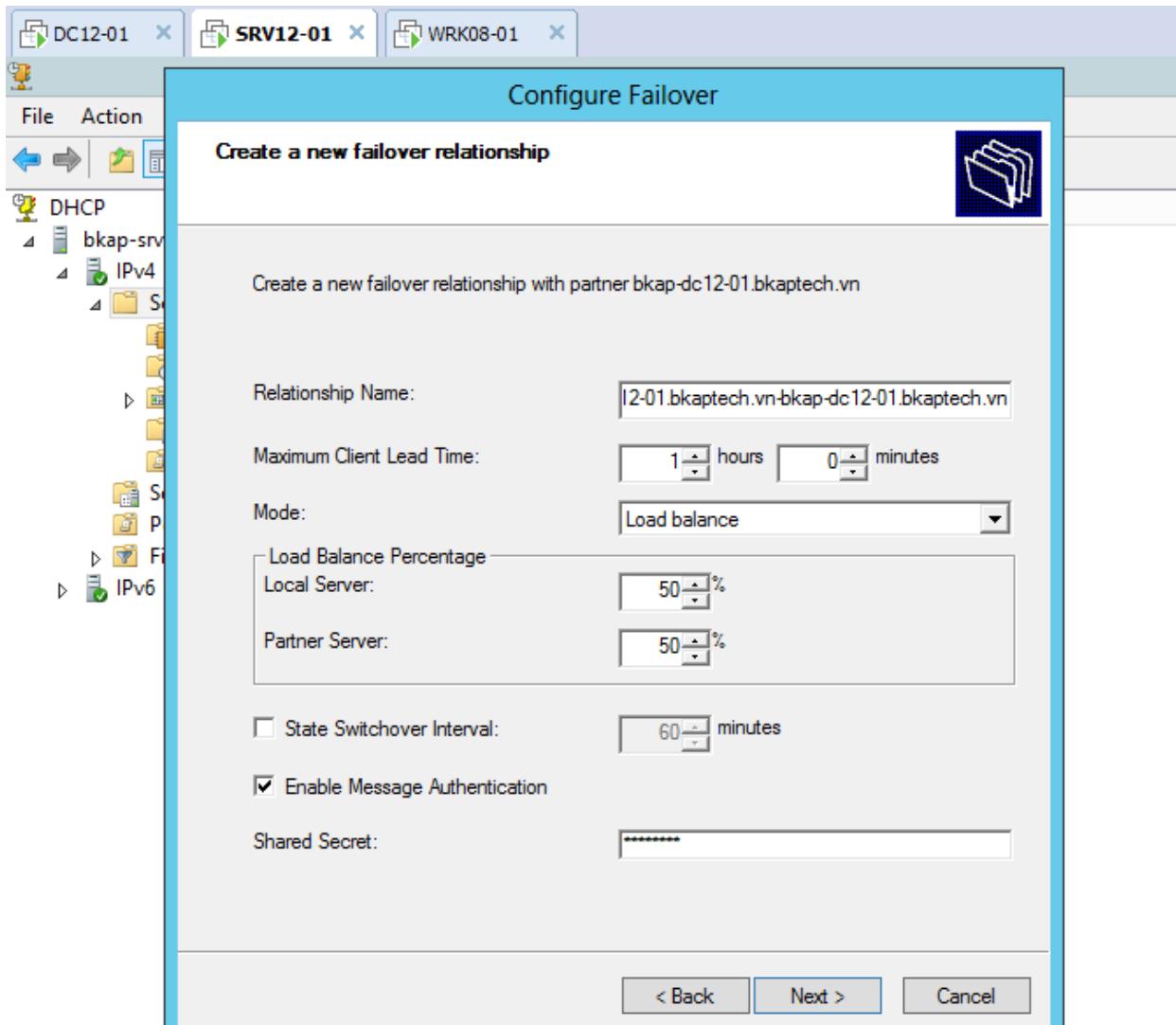
- Tại cửa sổ **Configure Failover**, click chọn vào **Select all, Next.**



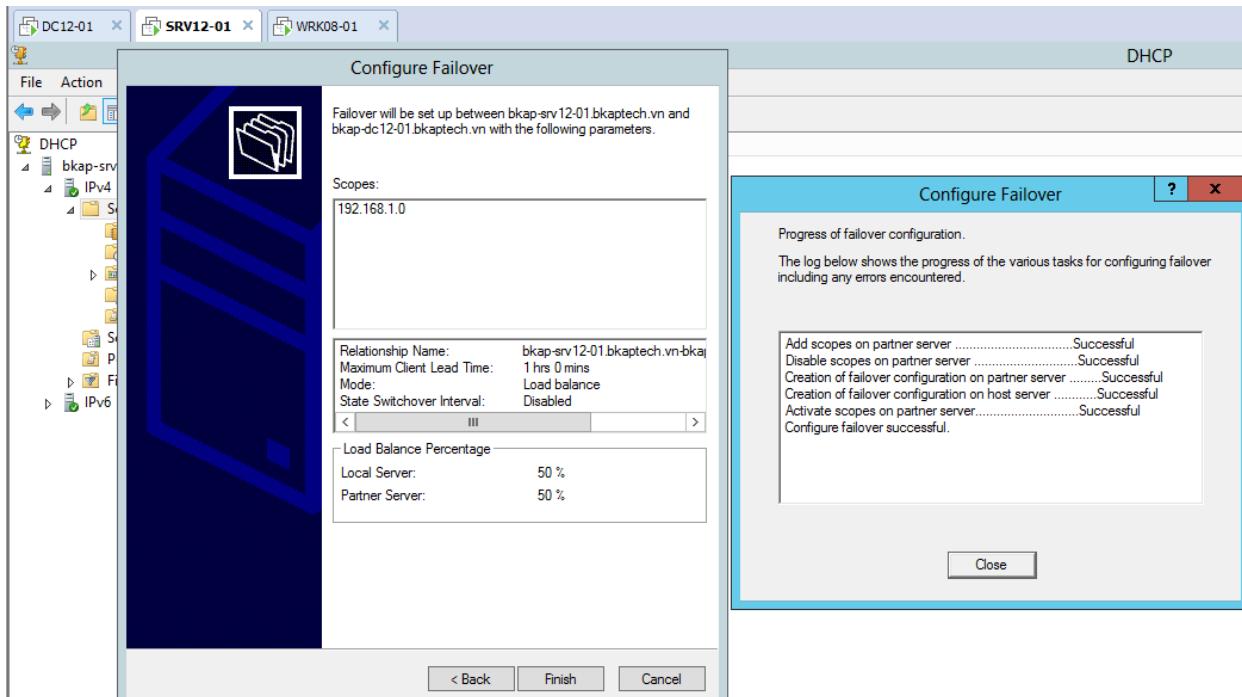
- Tại cửa sổ **Specify the partner server to use for failover** , tại **Partner Server** , nhập vào tên đầy đủ của máy *Domain Controller* (*khai báo DHCP Server thứ 2*).
 - **Next.**



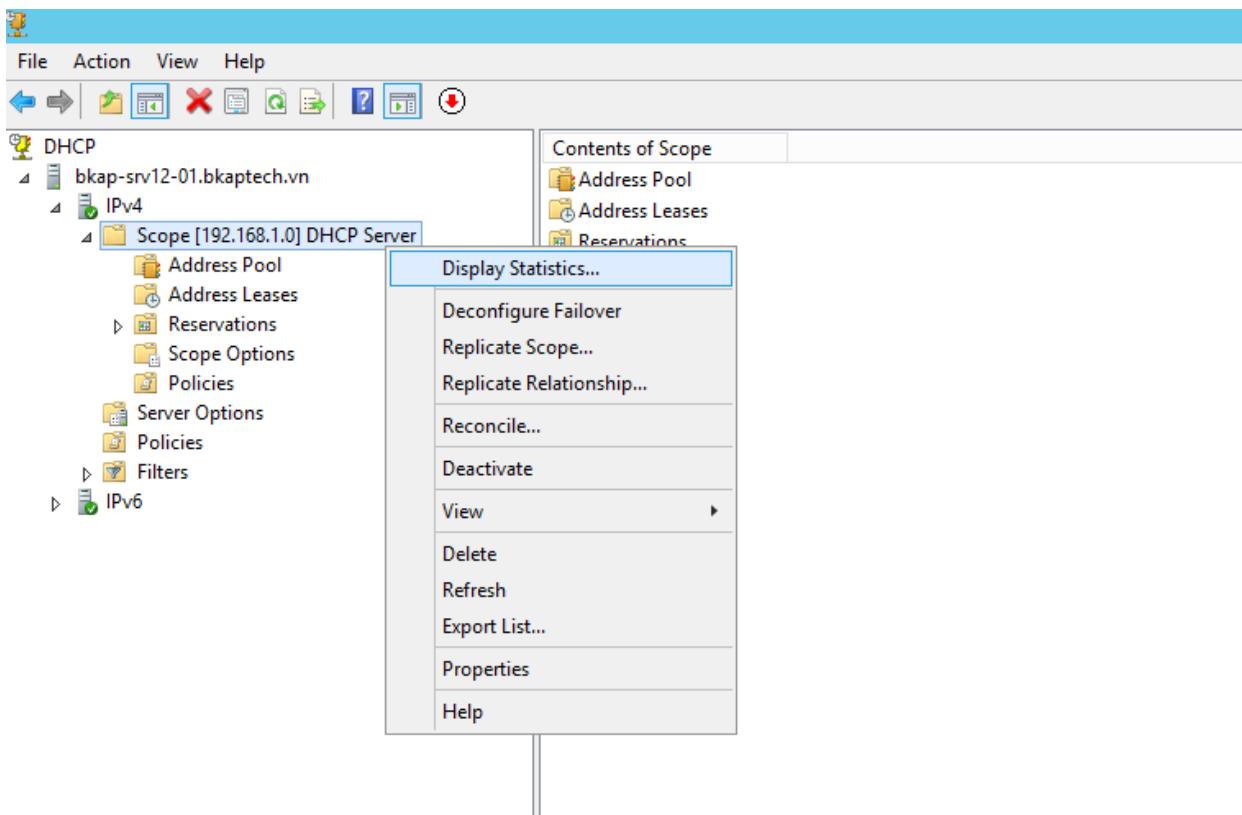
- Tại **Create a new failover relationship**, nhập mã *Shared Secret* (*123456a@*)

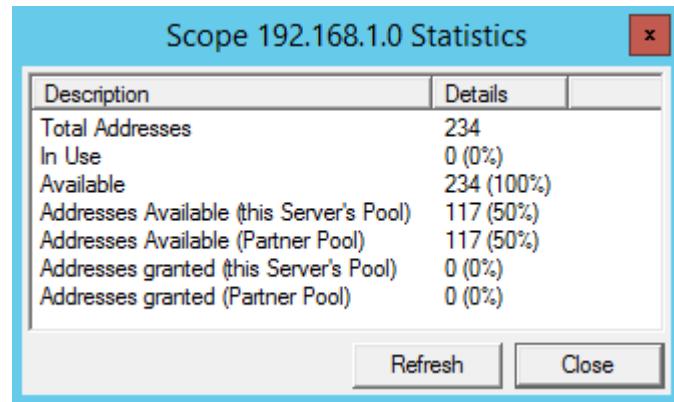


- Click **Finish** và **Close** tại cửa sổ tiếp theo.

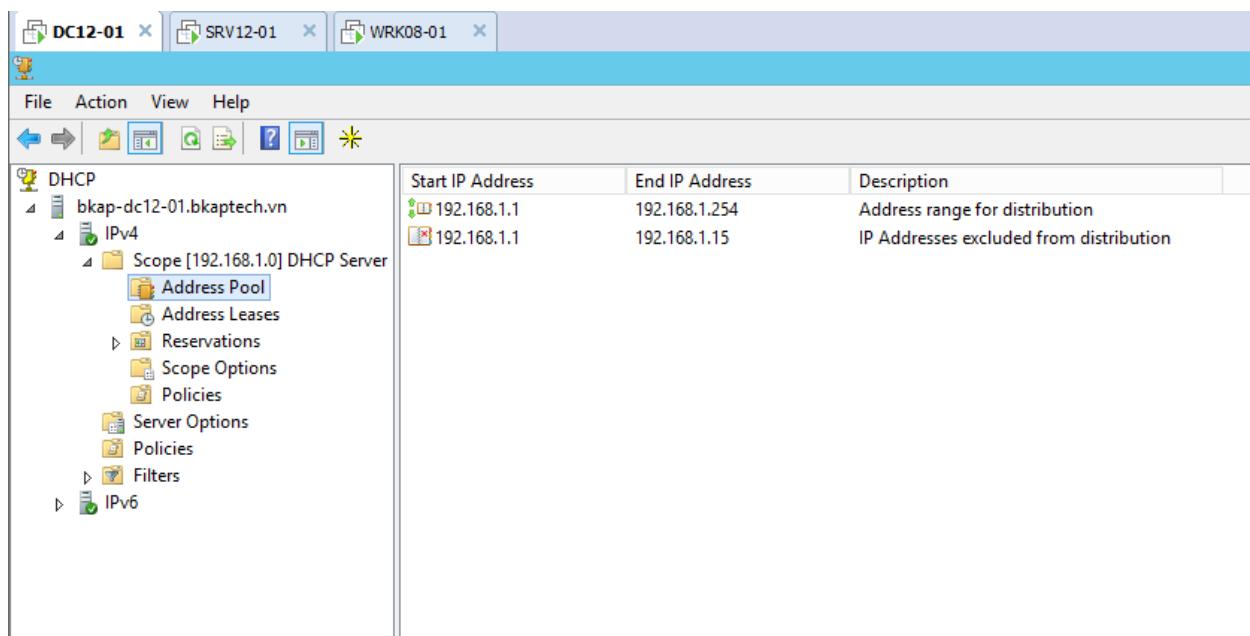


- Xem thống kê và thông tin chi tiết về **Scope**:
 - Click chuột phải tại **Scope** vừa tạo, chọn **Display Statistics...**

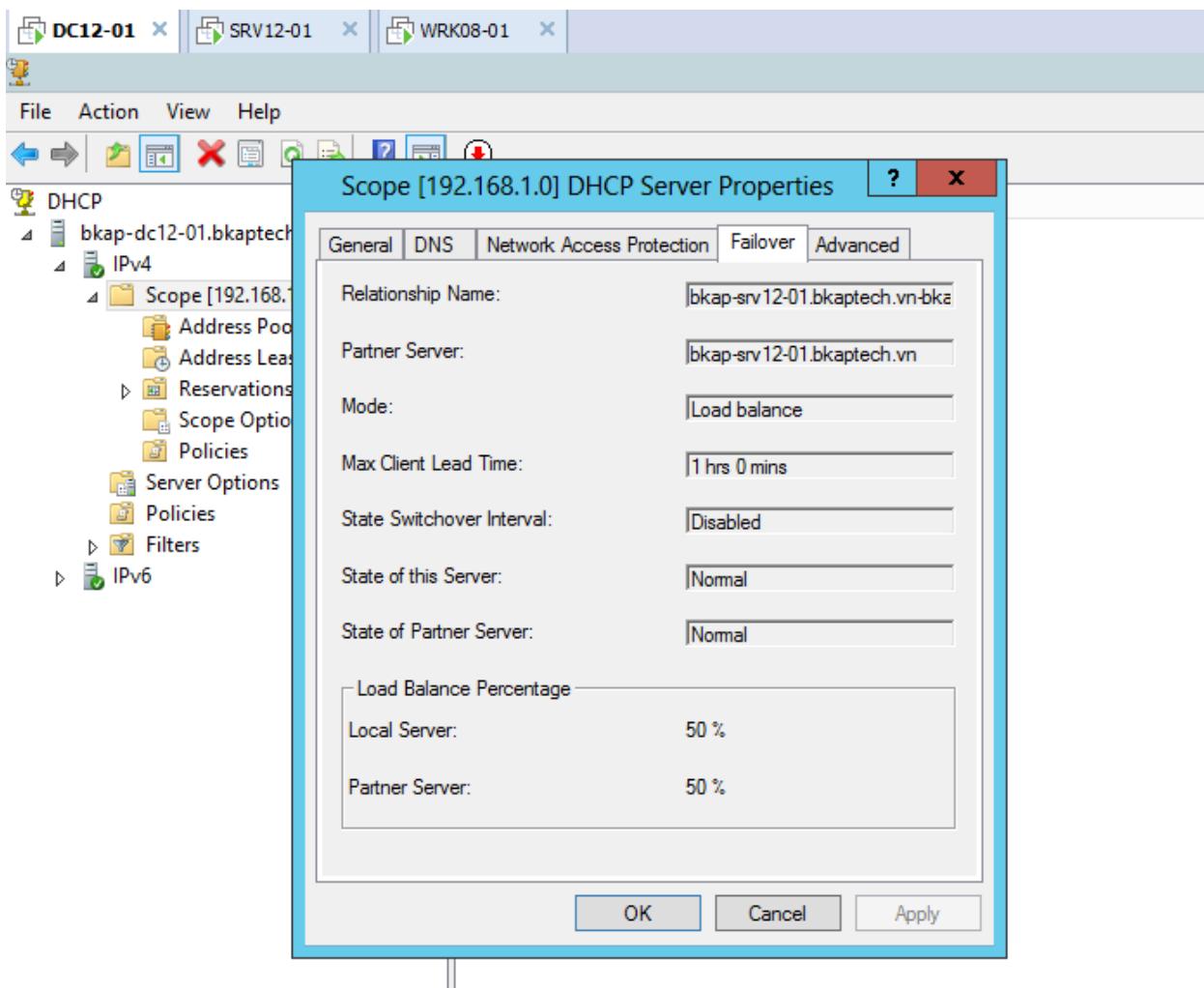




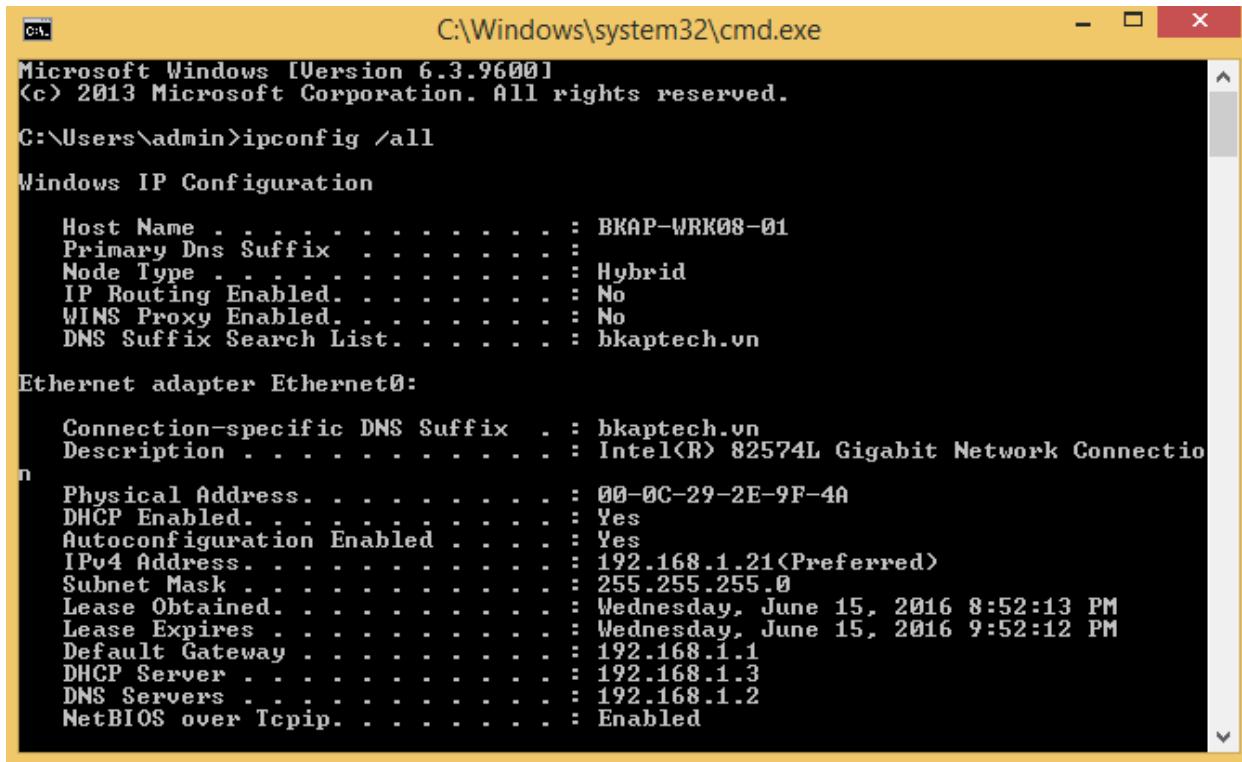
- Chuyển về máy **BKAP-DC12-01** xem máy *Domain Controller* đã đồng bộ **DHCP** chưa :



- Các thông số của Failover:



- Test tính năng **Load-Balancing** : trên máy Client *BKAP-WRK08-01*.
 - Sử dụng câu lệnh **ipconfig /all**.



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

C:\Users\admin>ipconfig /all

Windows IP Configuration

Host Name . . . . . : BKAP-WRK08-01
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : bkaptech.vn

Ethernet adapter Ethernet0:

Connection-specific DNS Suffix . . . . . : bkaptech.vn
Description . . . . . : Intel(R) 82574L Gigabit Network Connectio
n
Physical Address. . . . . : 00-0C-29-2E-9F-4A
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
IPv4 Address. . . . . : 192.168.1.21(PREFERRED)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Wednesday, June 15, 2016 8:52:13 PM
Lease Expires . . . . . : Wednesday, June 15, 2016 9:52:12 PM
Default Gateway . . . . . : 192.168.1.1
DHCP Server . . . . . : 192.168.1.3
DNS Servers . . . . . : 192.168.1.2
NetBIOS over Tcpip. . . . . : Enabled
```

- Gõ lệnh **Ipconfig /release** để xóa IP đang dùng.

- Dùng lệnh **ipconfig /renew** để xin địa chỉ IP mới.

- Dùng câu lệnh **ipconfig /all** để xem thông tin chi tiết về IP, ta thấy DHCP Server cấp IP là **DHCP Server (BKAP-SRV12-01)** có IP là **192.168.1.3**.

```
C:\Windows\system32\cmd.exe
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : bkaptech.vn

Ethernet adapter Ethernet0:

Connection-specific DNS Suffix . . . . . : bkaptech.vn
Description . . . . . : Intel(R) 82574L Gigabit Network Connection
Physical Address. . . . . : 00-0C-29-2E-9F-4A
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
IPv4 Address. . . . . : 192.168.1.21<Preferred>
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Wednesday, June 15, 2016 8:55:36 PM
Lease Expires . . . . . : Wednesday, June 15, 2016 9:55:36 PM
Default Gateway . . . . . : 192.168.1.1
DHCP Server . . . . . : 192.168.1.3
DNS Servers . . . . . : 192.168.1.2
NetBIOS over Tcpip. . . . . : Enabled

Tunnel adapter isatap.bkaptech.vn:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . . . . : bkaptech.vn
Description . . . . . : Microsoft ISATAP Adapter #2
Physical Address. . . . . : 00-00-00-00-00-00-E0
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . . : Yes

C:\Users\admin>
```

- Giả sử máy **DHCP Server (192.168.1.3)** gặp sự cố (có thể shutdown máy này). Thực hiện kiểm tra IP trên máy **BKAP-WRK08-01**.

```
C:\Windows\system32\cmd.exe
C:\Users\admin>ipconfig /release
Windows IP Configuration

Ethernet adapter Ethernet0:

  Connection-specific DNS Suffix . . . . . : bkaptech.vn
  Default Gateway . . . . . : 192.168.1.21
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 192.168.1.1

C:\Users\admin>ipconfig /renew
Windows IP Configuration

Ethernet adapter Ethernet0:

  Connection-specific DNS Suffix . . . . . : bkaptech.vn
  IPv4 Address. . . . . : 192.168.1.21
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 192.168.1.1

Tunnel adapter isatap.bkaptech.vn:

  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . . . . . : bkaptech.vn
```

- Lúc này **DHCP Server (192.168.1.2)** sẽ phục vụ cấp địa chỉ IP cho máy **Client**.

```
C:\Windows\system32\cmd.exe
C:\Users\admin>ipconfig /all
Windows IP Configuration

Host Name . . . . . : BKAP-WRK08-01
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : bkaptech.vn

Ethernet adapter Ethernet0:

  Connection-specific DNS Suffix . . . . . : bkaptech.vn
  Description . . . . . : Intel(R) 82574L Gigabit Network Connection
  Physical Address. . . . . : 00-0C-29-2E-9F-4A
  DHCP Enabled. . . . . : Yes
  Autoconfiguration Enabled . . . . . : Yes
  IPv4 Address. . . . . : 192.168.1.21<Preferred>
  Subnet Mask . . . . . : 255.255.255.0
  Lease Obtained. . . . . : Wednesday, June 15, 2016 9:00:18 PM
  Lease Expires . . . . . : Thursday, June 23, 2016 9:00:18 PM
  Default Gateway . . . . . : 192.168.1.1
  DHCP Server . . . . . : 192.168.1.2
  DNS Servers . . . . . : 192.168.1.2
  NetBIOS over Tcpip. . . . . : Enabled
```

- Cấu hình cơ chế **Hot-Standby**.
 - Thực hiện các bước giống cấu hình **Load-Balancing**, đến bước chọn cơ chế ta chọn **Hot Standby**.
 - *Partner Server* là máy **BKAP-DC12-01 (192.168.1.2)** và cho nó là **Standby (Passive) – dự phòng**.
 - Máy server **BKAP-SRV12-01** là **Hot Standby (Active)**.
 - **MCLT (Maximum Client Lead Time)**: là thời gian mà **Standby server** gia hạn IP cho **client**. Trường hợp này xảy ra khi **client** đã được cấp IP và đến lúc gia hạn lại mà không liên lạc được với **Active server**, thì lúc này **Standby server** đứng ra gia hạn cho **client** và áp dụng thời gian gia hạn tạm thời (**MCLT**).
 - **Address Reserved** : là phần trăm (%) lượng IP mà **DHCP Server (BKAP-DC12-01)** sẽ giữ để cấp cho **Client** trong trường hợp **Client** không liên lạc được với **DHCP Server (BKAP-SRV12-01) (Active)**.

Configure Failover

Create a new failover relationship

Create a new failover relationship with partner bkap-dc12-01.bkaptech.vn

Relationship Name: -01.bkaptech.vn-bkap-dc12-01.bkaptech.vn-1

Maximum Client Lead Time: 1 hours 0 minutes

Mode: Hot standby

Hot Standby Configuration

Role of Partner Server: Standby

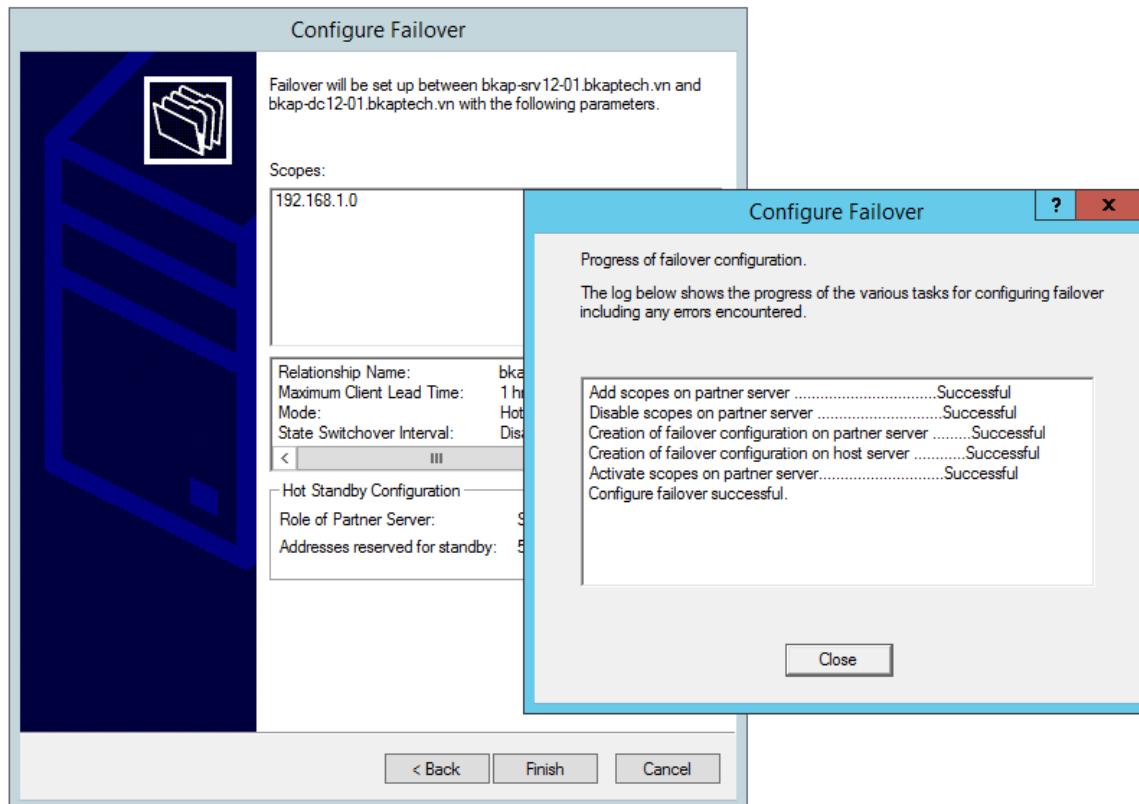
Addresses reserved for standby server: 5 %

State Switchover Interval: 60 minutes

Enable Message Authentication

Shared Secret: *****

< Back Next > Cancel



- Thực hiện kiểm tra trên máy **Client**.

1.2 Cấu hình thiết lập DNS nâng cao

1.Yêu cầu bài Lab:

+ Trên máy **BKAP-DC12-01**:

- Cấu hình **DNSSEC**.
- Cấu hình **DNS Socket pool**.
- Cấu hình **DNS cache locking**.
- Cấu hình **GlobalNames zone**.

2.Yêu cầu chuẩn bị:

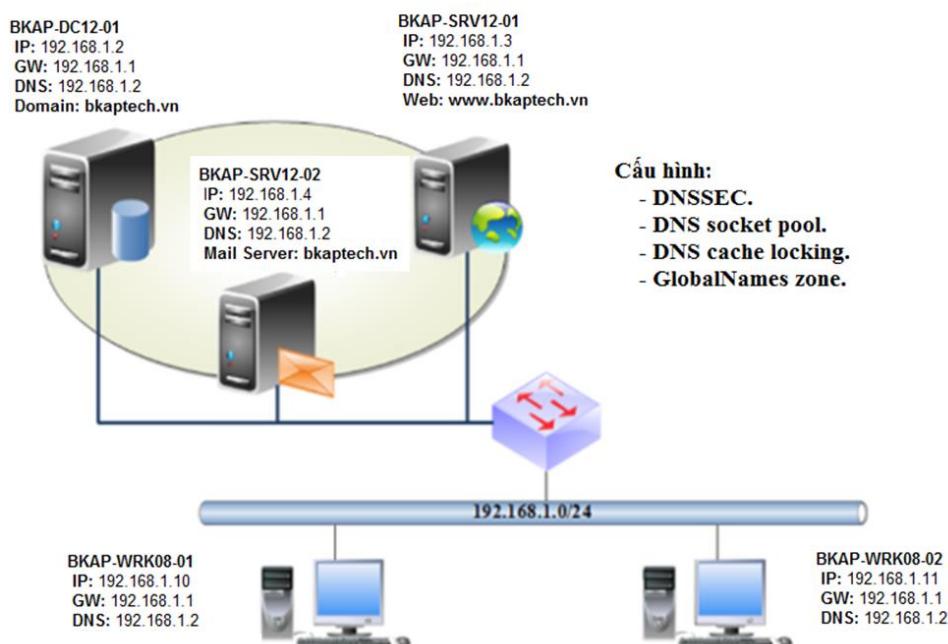
+ Máy **BKAP-DC12-01**: đã nâng cấp lên **Domain Controller** quản lý miền **bkaptech.vn**.

3.Mô hình Lab:

HỆ THỐNG ĐÀO TẠO CNTT QUỐC TẾ BACHKHOA-APTECH

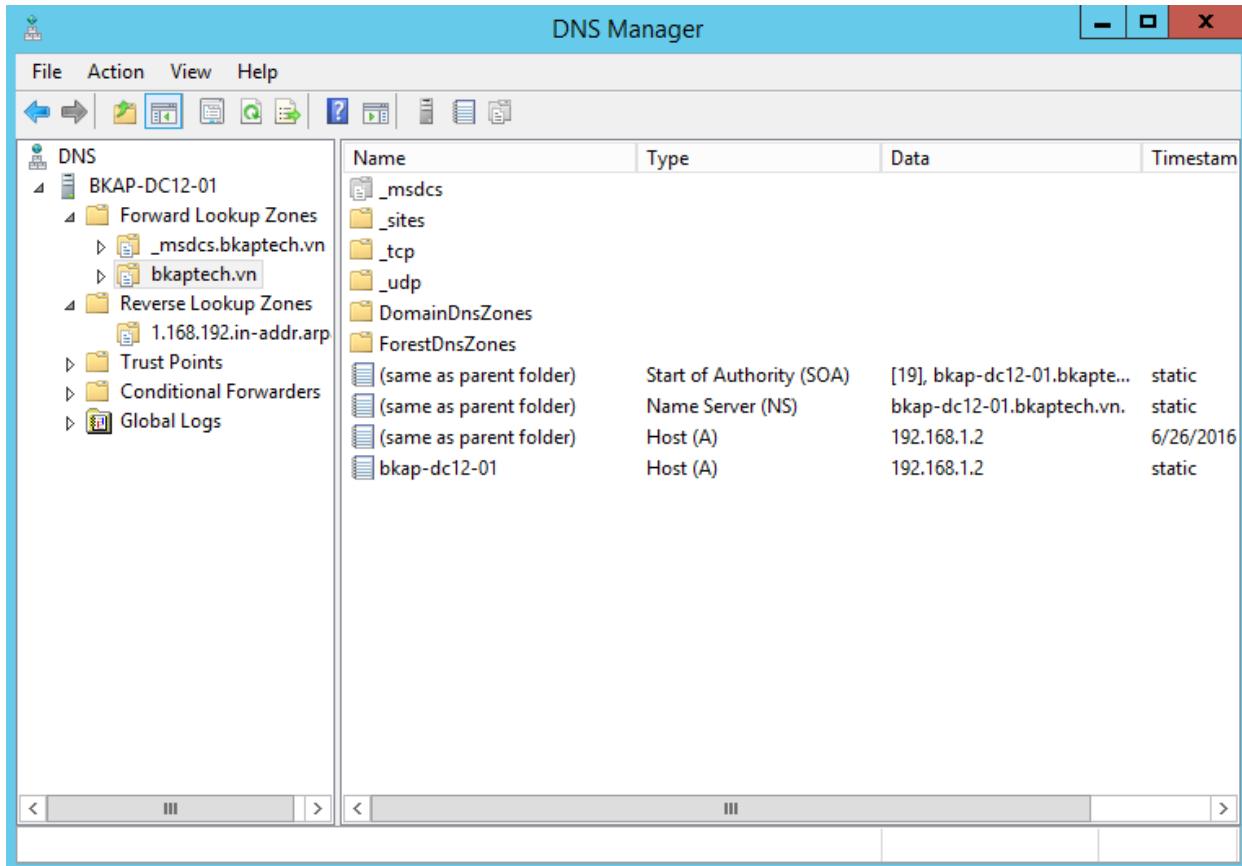
BACHKHOA
EDUCATION APTECH

Cấu hình thiết lập DNS nâng cao

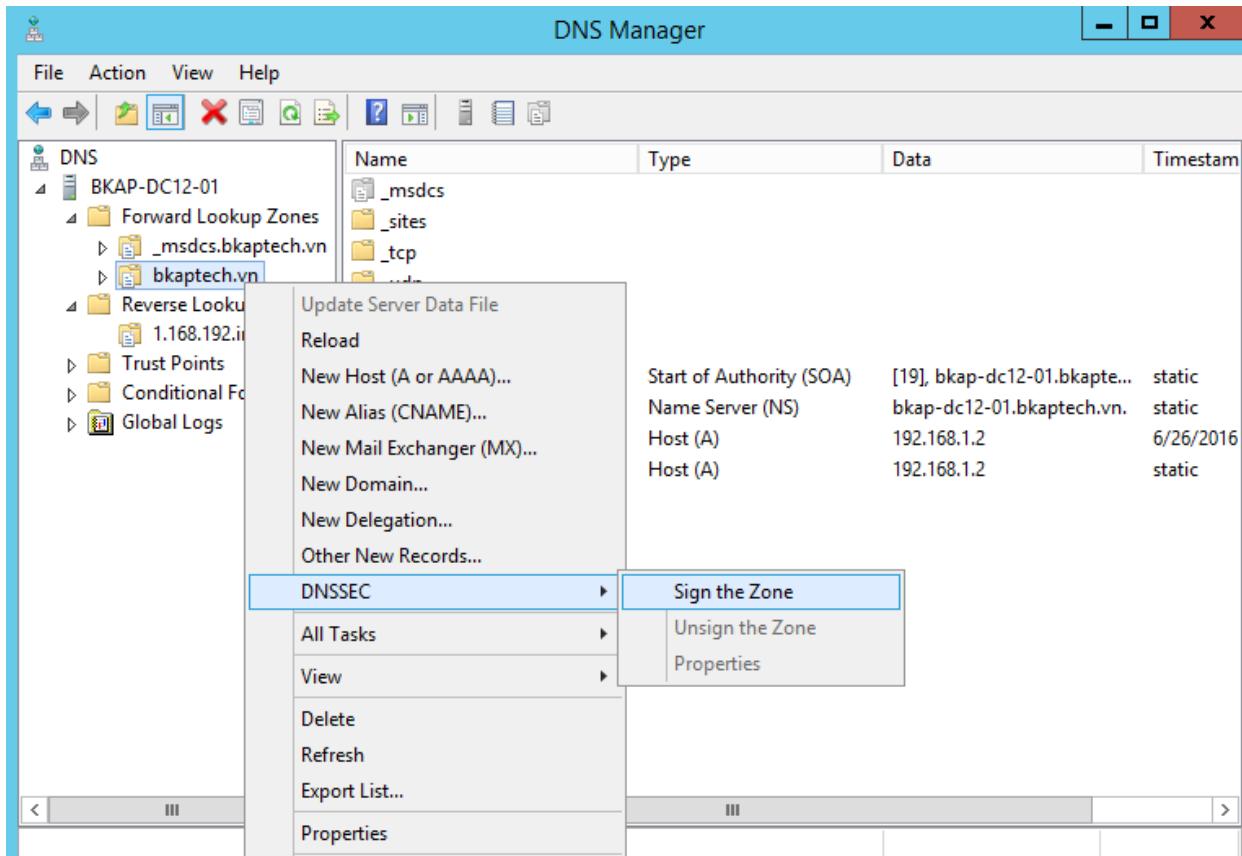


Hướng dẫn chi tiết:

- Trên máy *BKAP-DC12-01*, thực hiện cấu hình **DNSSEC**.
 - Vào **Server Manager / Tools / DNS**.



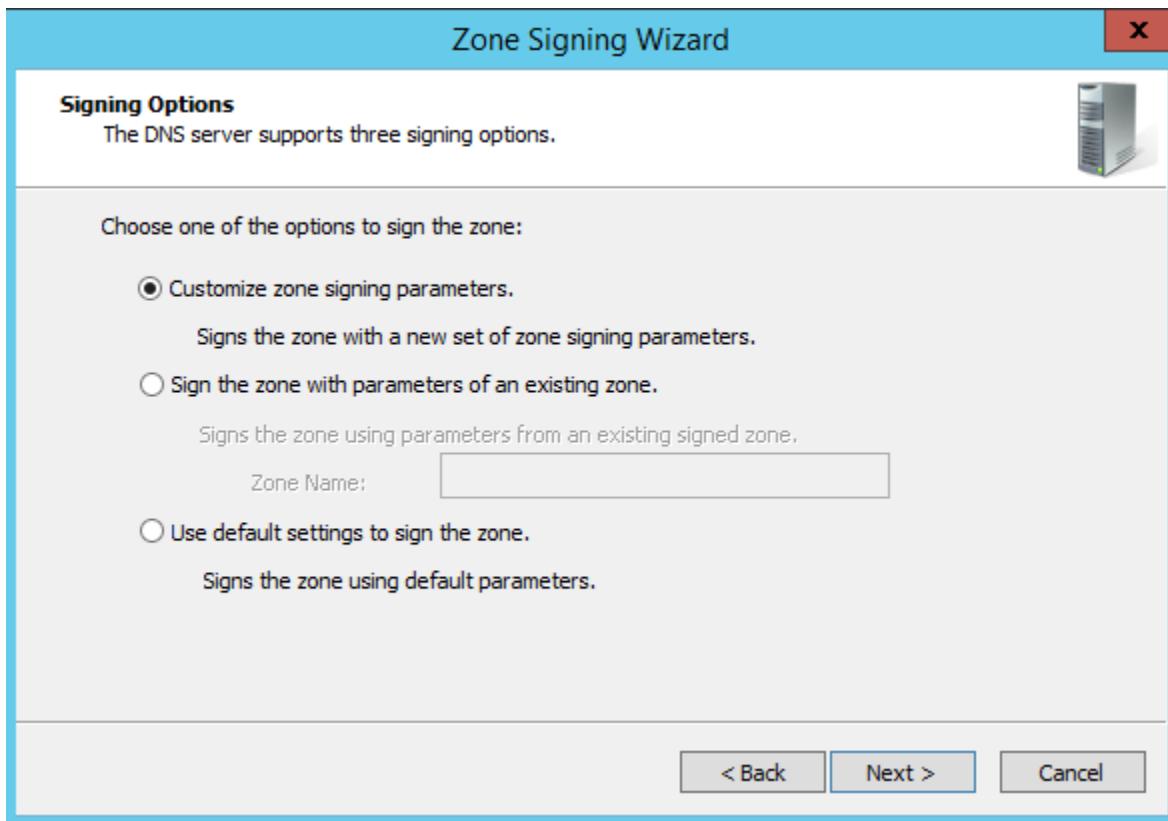
- Trong cửa sổ **DNS Manager**, click chuột phải vào tên miền **bkaptech.vn** , chọn **DNSSEC / Sign the Zone**.



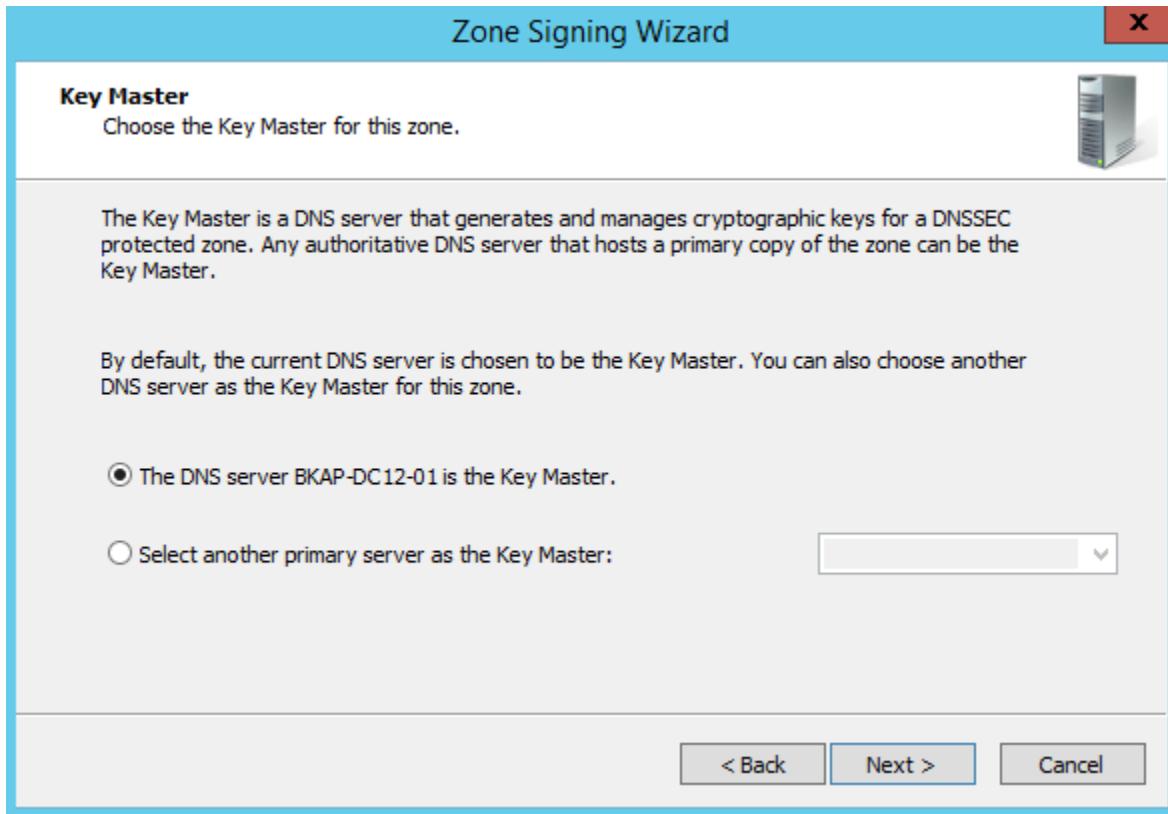
- Tại cửa sổ **DNS Security Extensions (DNSSEC)**, click vào **Next**.



- Tại cửa sổ **Zone Signing Wizard**, click vào **Next**.



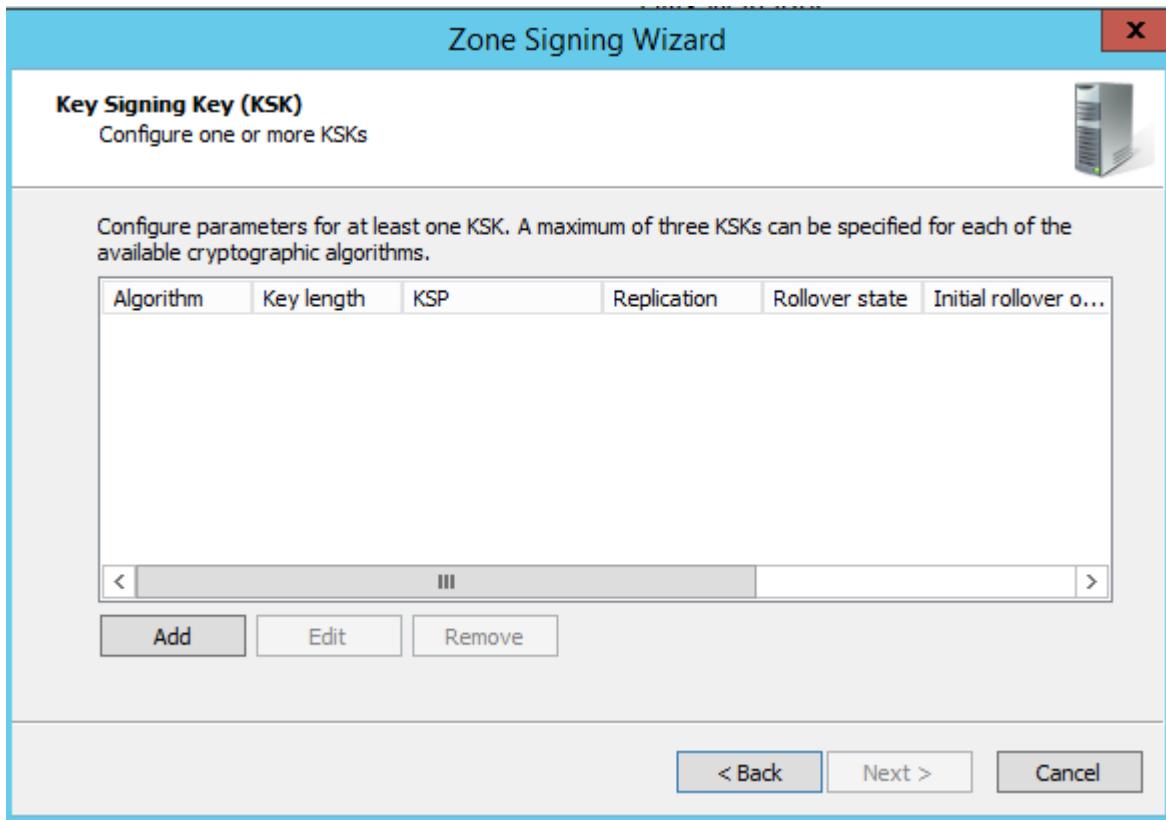
- Tại cửa sổ **Key Master**, kiểm tra tùy chọn là **The DNS Server BKAP-DC12-01 is the Key Master**, click vào **Next**.



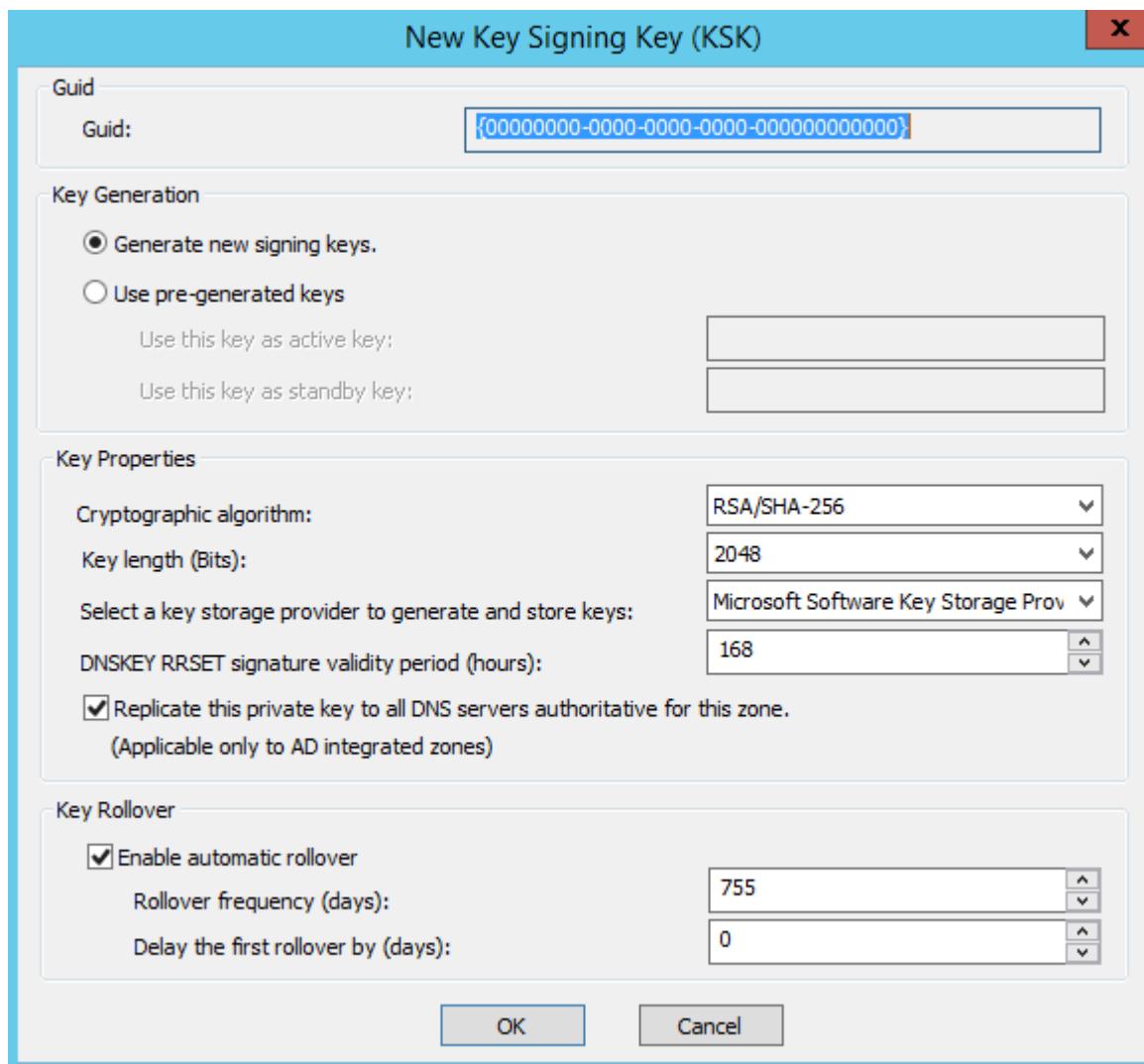
- Tại cửa sổ **Key Signing Key (KSK)** , click vào **Next**.



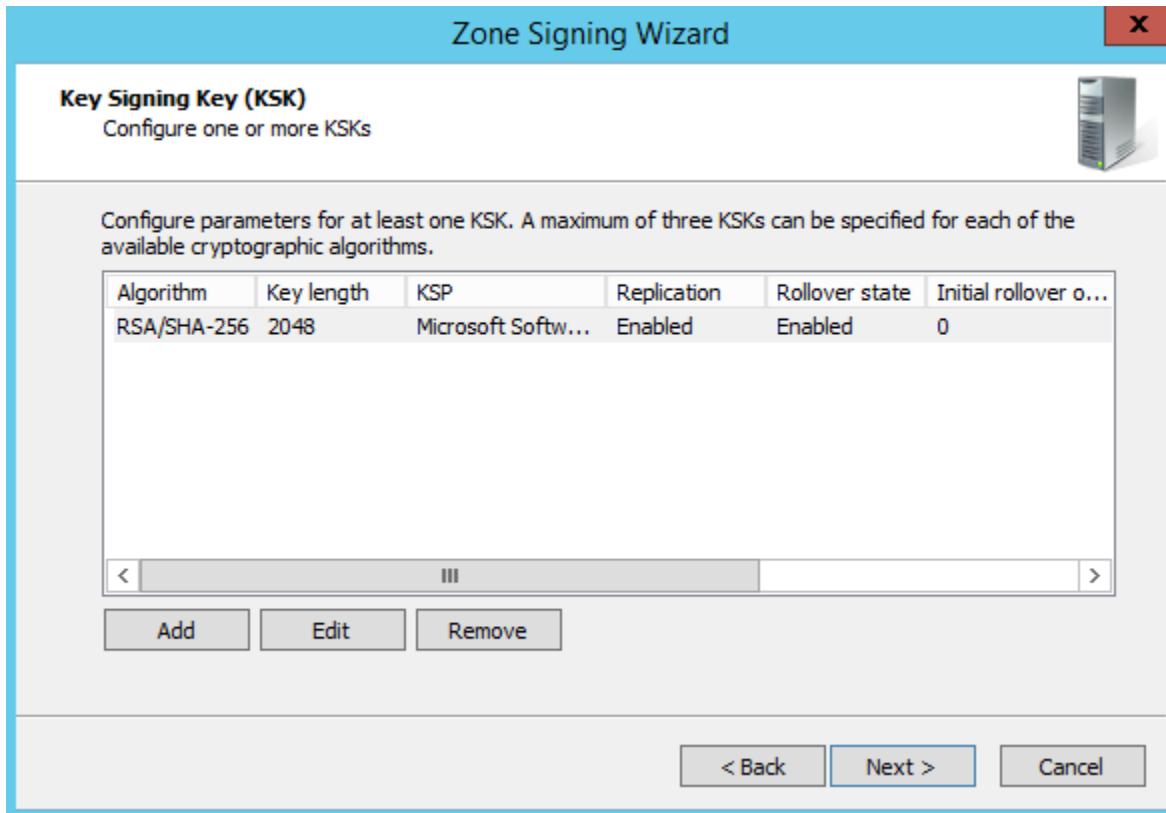
- Tại cửa sổ **Key Signing Key (KSK) / Configure one or more KSKs**, click vào **Add**.



- Tại cửa sổ **New Key Signing Key (KSK)**, click vào **OK**.



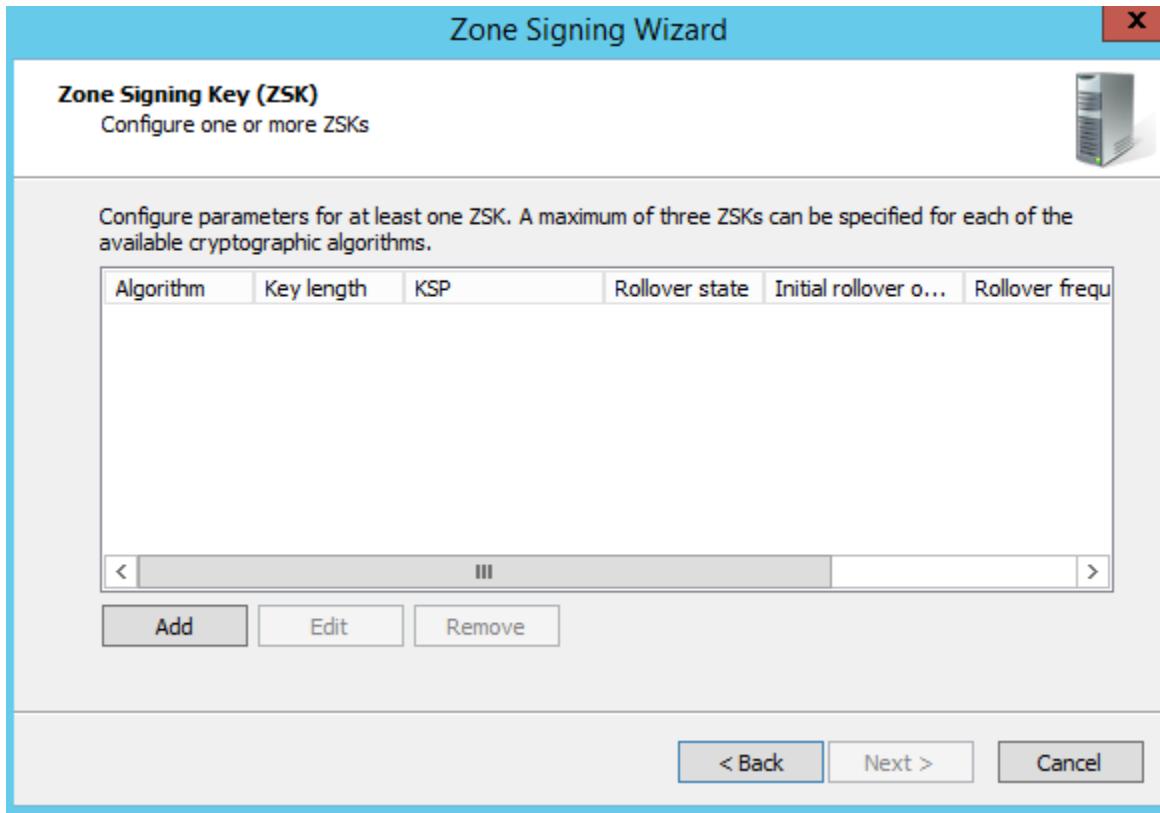
- Click vào Next tại cửa sổ Key Signing Key (KSK).



- Tại cửa sổ **Zone Signing Key (ZSK)**, click vào **Next**.



- Click vào Add.



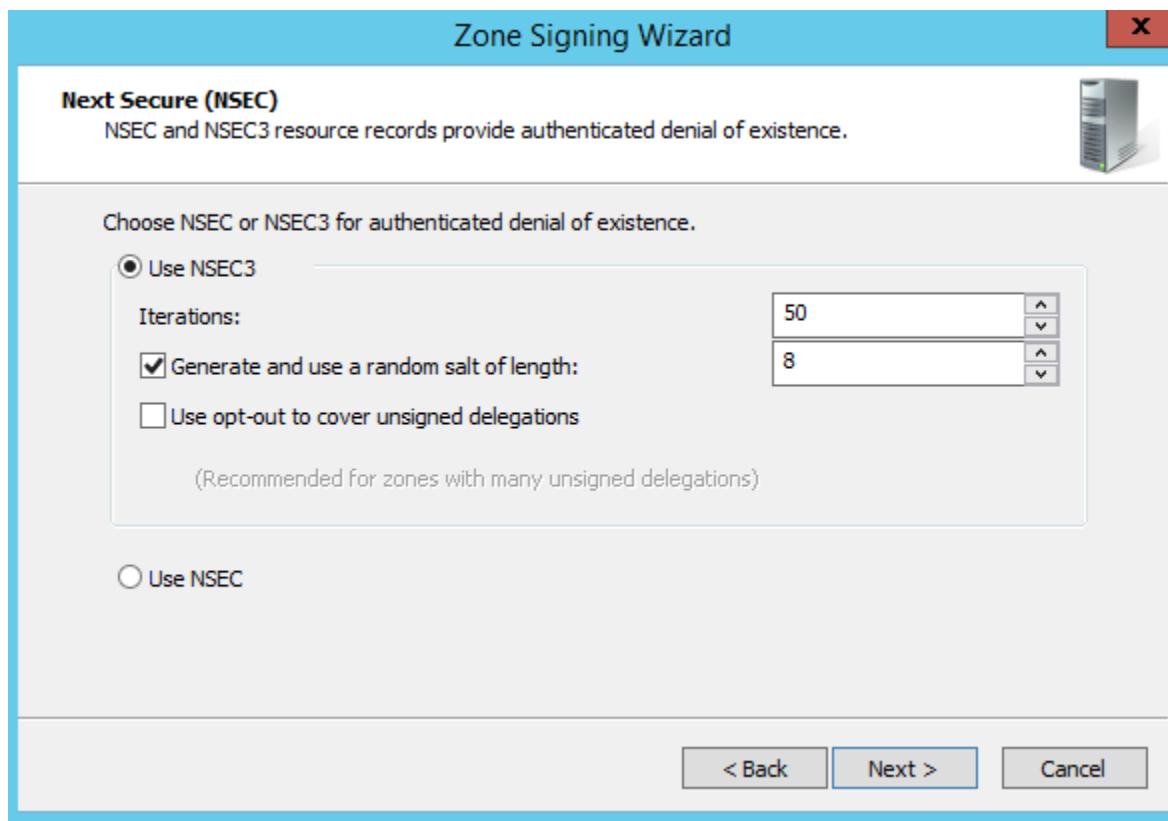
- Tại cửa sổ New Zone Signing Key (ZSK), click vào **OK**.



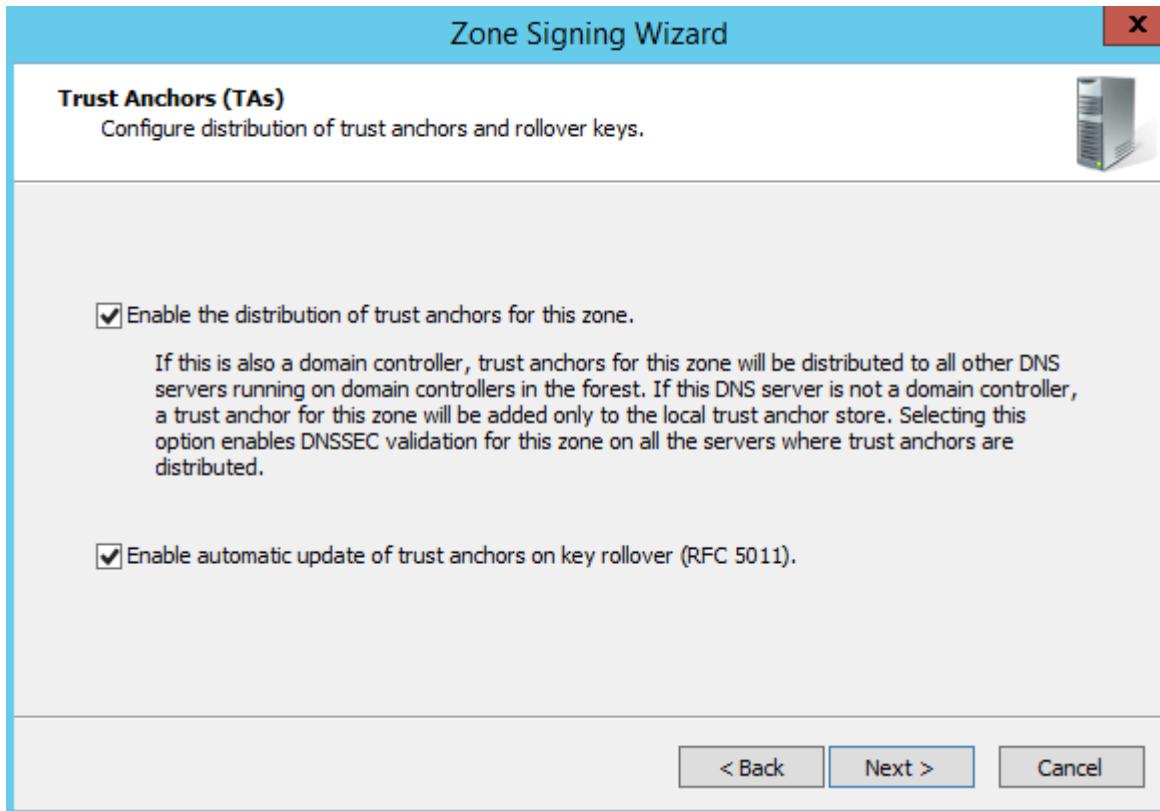
- Click vào Next.



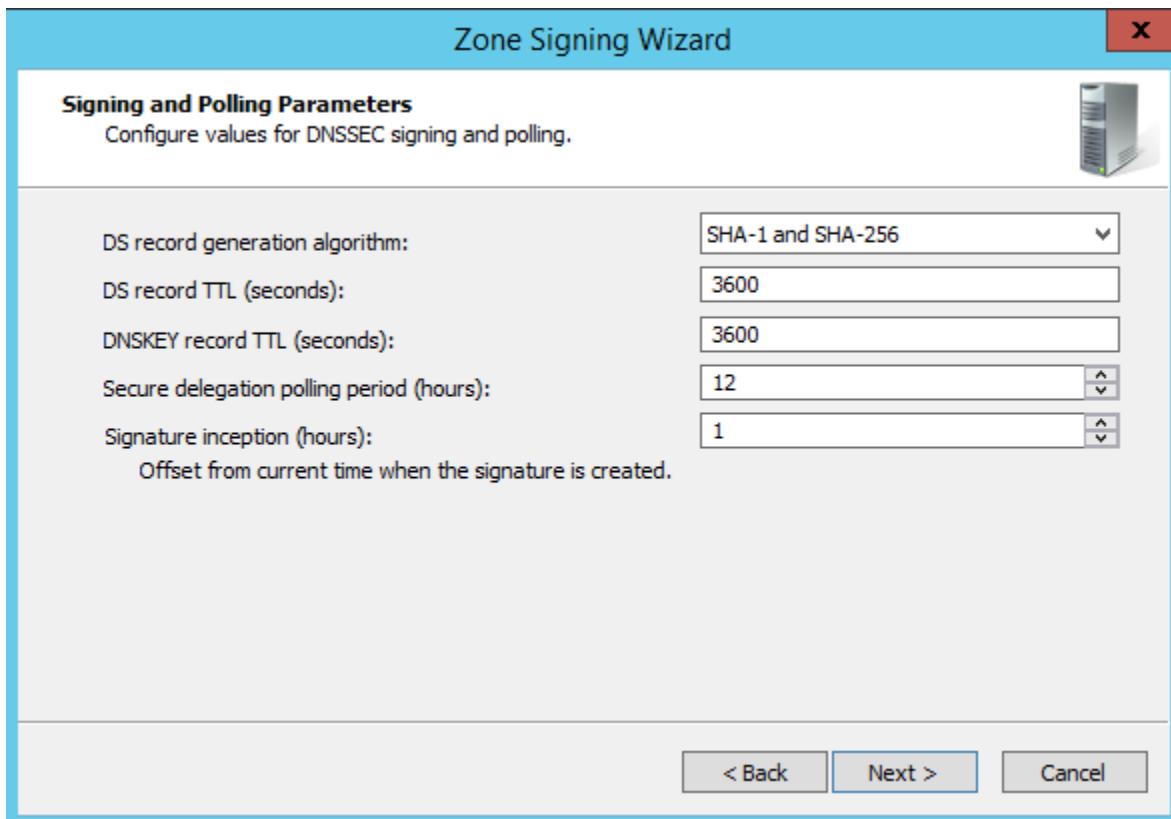
- Tại cửa sổ **Next Secure (NSEC)**, click vào **Next**.



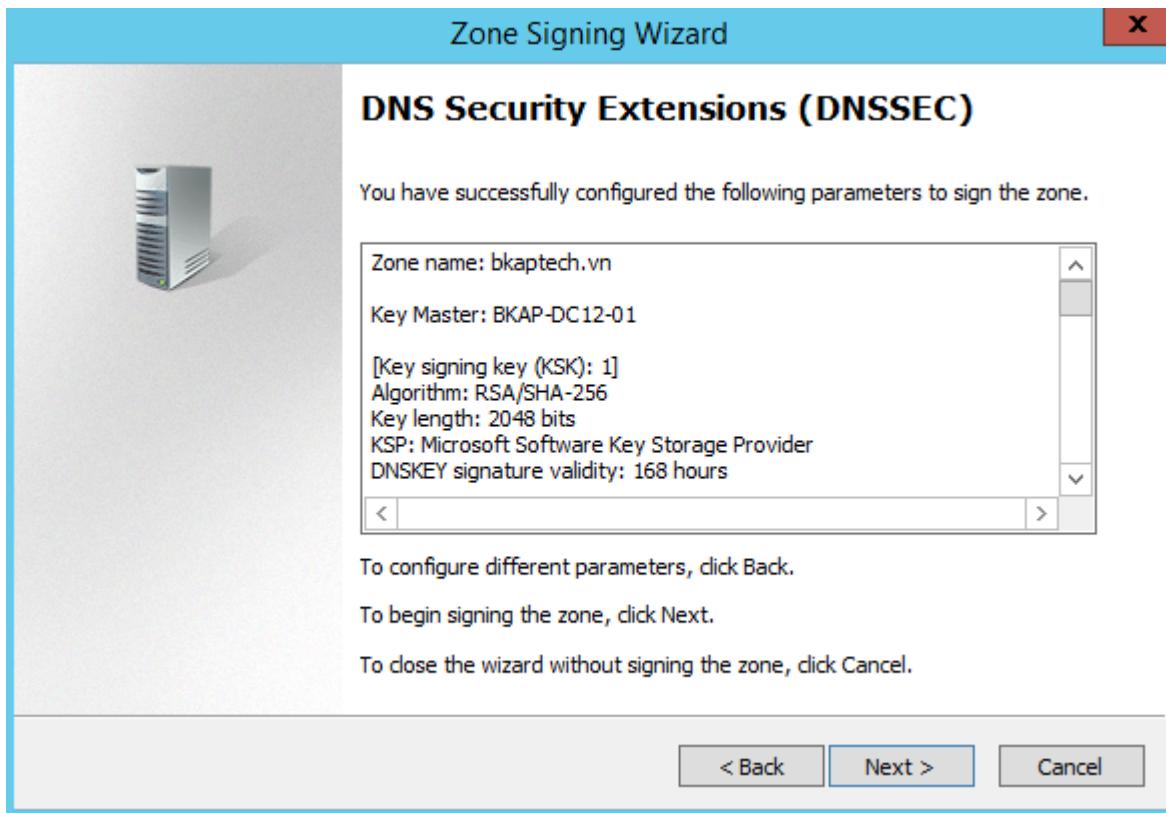
- Tại cửa sổ **Trust Anchors (TAs)**, click chọn vào **Enable the distribution of trust anchors for this zone**, click vào **Next**.



- Tại cửa sổ **Signing and Polling Parameters**, click vào Next.



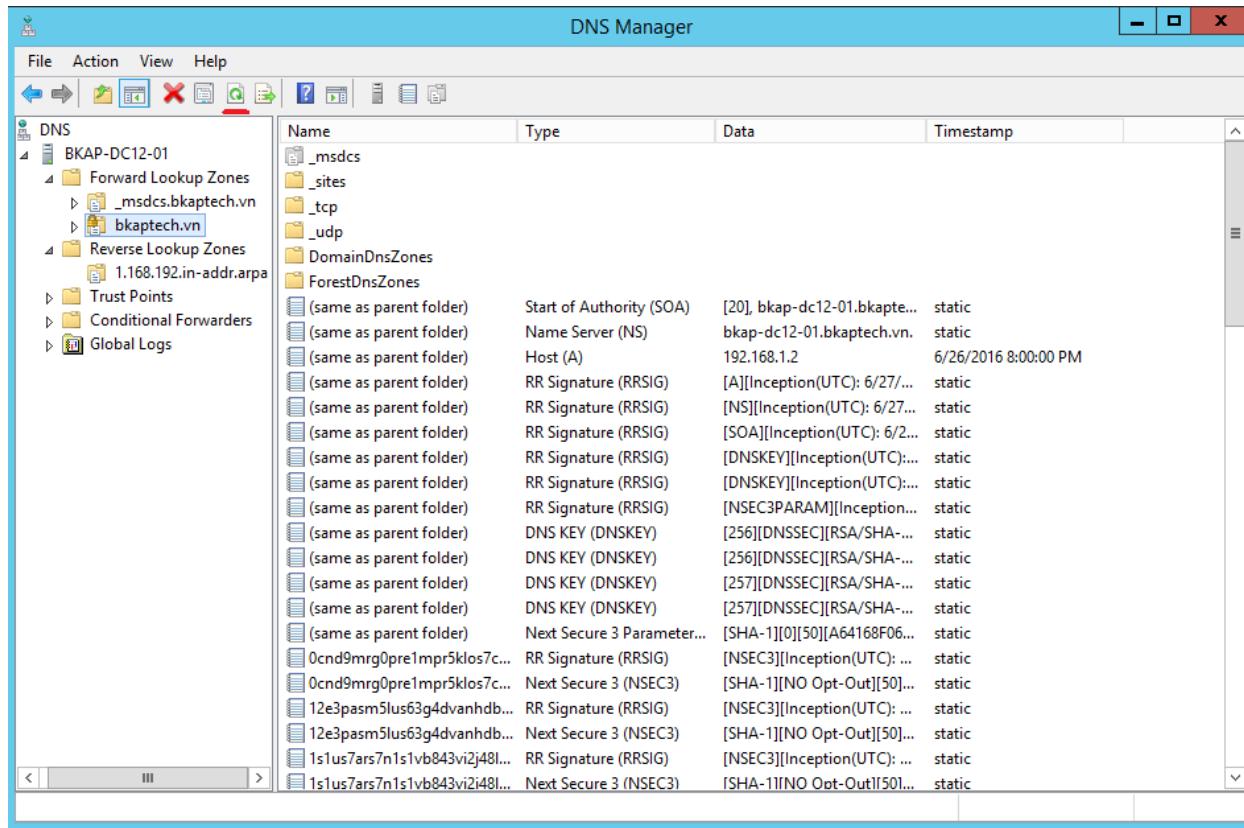
- Click vào **Next** tại cửa sổ **DNSSEC**.



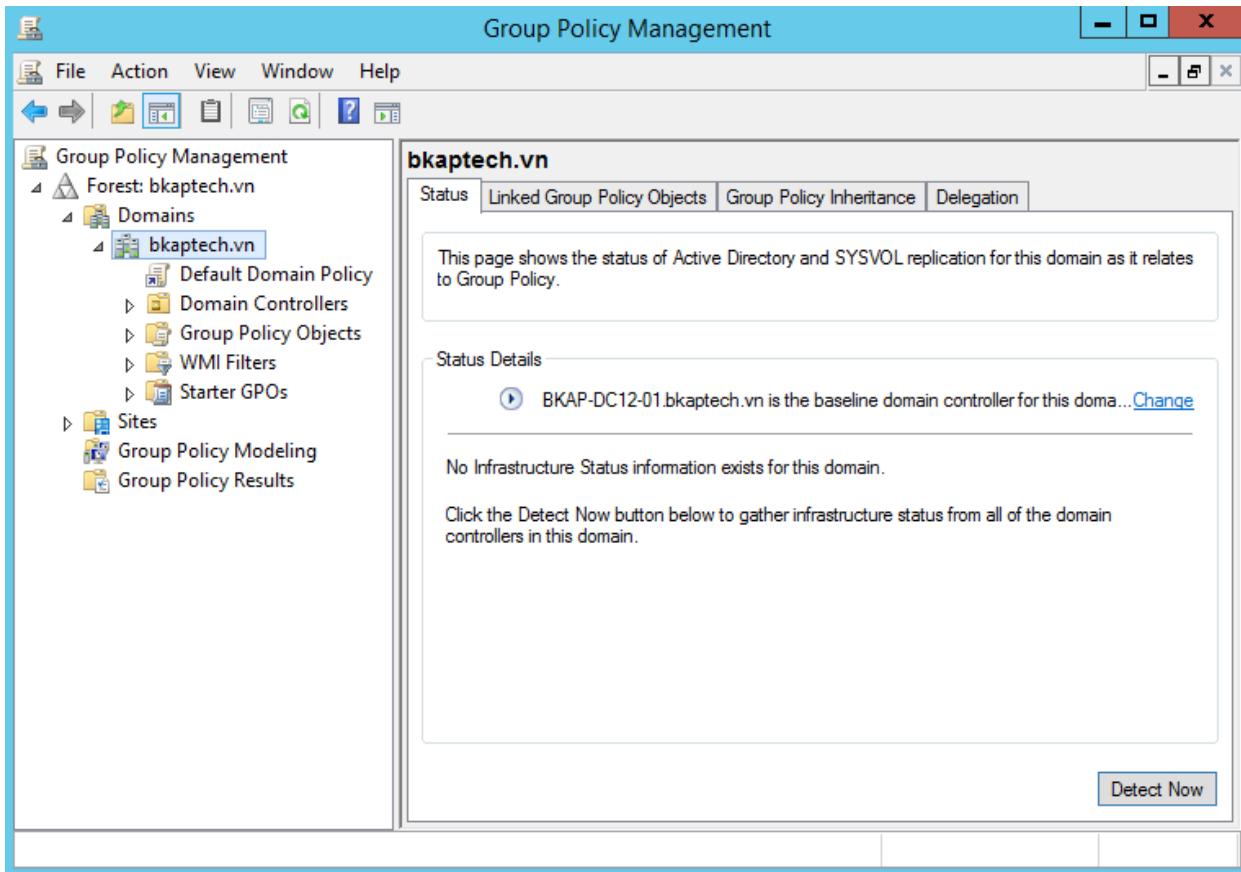
- Server tiến hành cấu hình, tại cửa sổ **Signing the Zone**, click vào **Finish**.



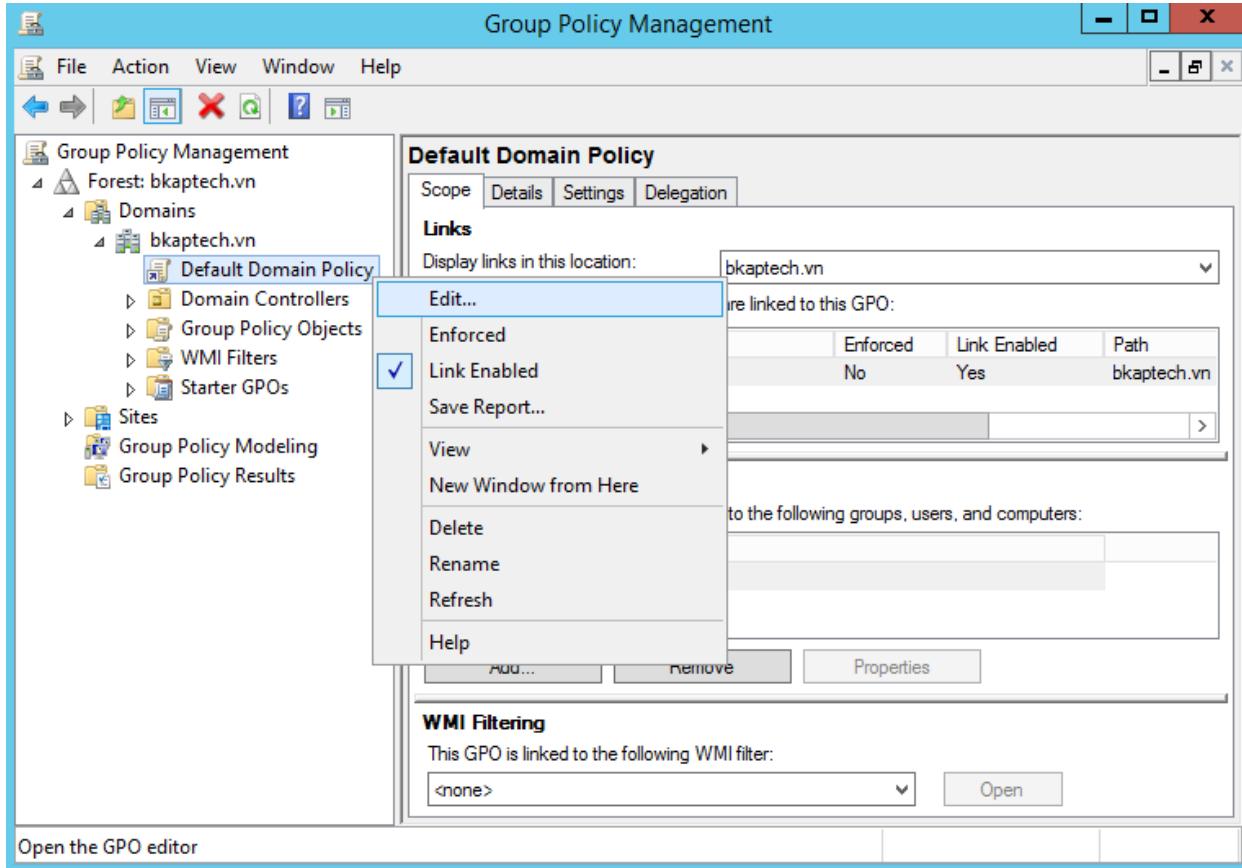
- Click vào Refresh để cập nhật bản ghi:



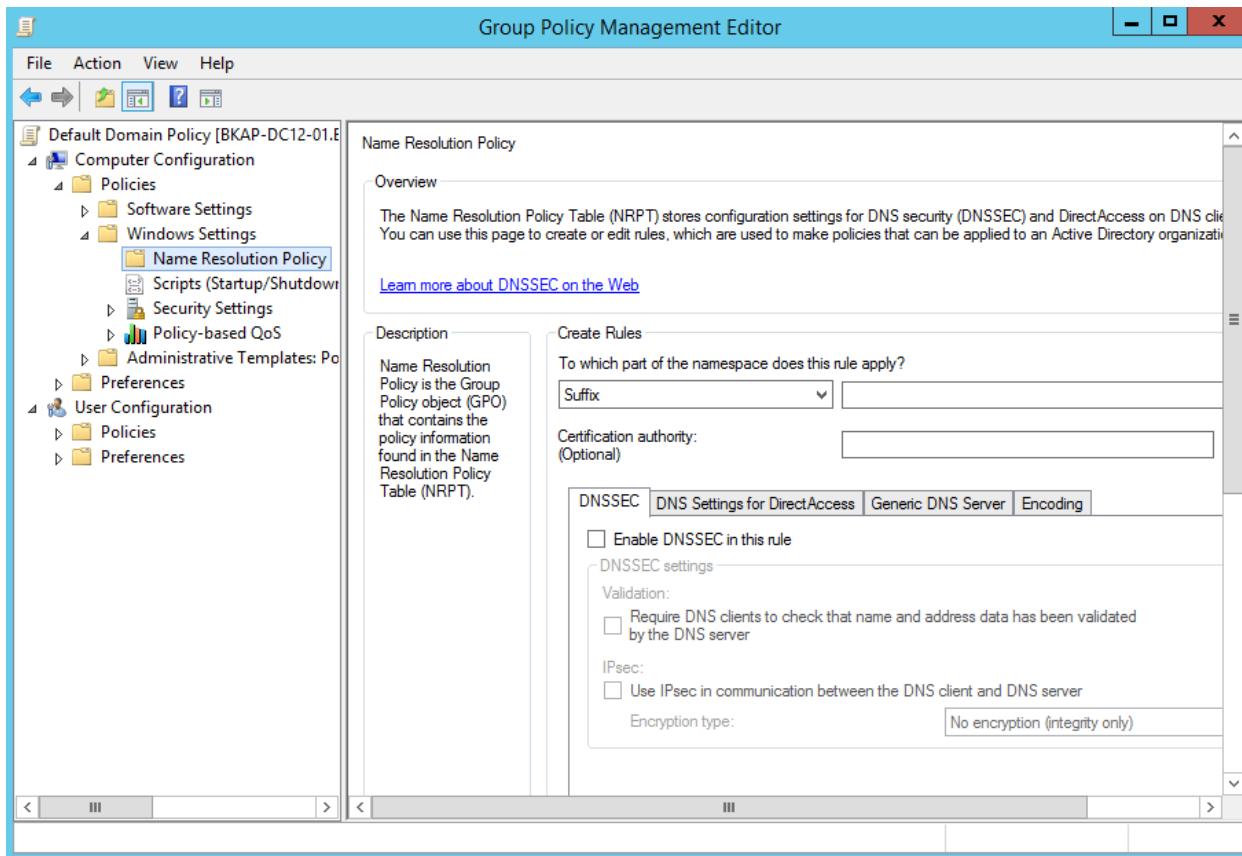
- Vào Group Policy Management.



- Trong cửa sổ **Group Policy Management**, click chuột phải tại **Default Domain Policy**, chọn **Edit...**



- Trong cửa sổ **Group Policy Management Editor**, click chọn vào **Computer Configuration / Policies / Windows Settings / Name Resolution Policy**.



- Trong cửa sổ **Name Resolution Policy**, tại mục **Create Rules** , nhập vào **bkaptech.vn** , tại mục **Certification authority**, trong Tab **DNSSEC**, tích vào **Enable DNSSEC in this rule** và **Require DNS Clients to check that name and address....**
- Click vào **Create**.

Name Resolution Policy

Overview

The Name Resolution Policy Table (NRPT) stores configuration settings for DNS security (DNSSEC) and DirectAccess on DNS client computers. You can use this page to create or edit rules, which are used to make policies that can be applied to an Active Directory organizational unit (OU).

[Learn more about DNSSEC on the Web](#)

<p>Description</p> <p>Name Resolution Policy is the Group Policy object (GPO) that contains the policy information found in the Name Resolution Policy Table (NRPT).</p>	<p>Create Rules</p> <p>To which part of the namespace does this rule apply?</p> <p>Suffix <input type="text" value="bkaptech.vn"/> <input type="button" value="Browse..."/></p> <p>Certification authority: <input type="text"/> <input type="button" value="Browse..."/> (Optional)</p> <p><input checked="" type="radio"/> DNSSEC <input type="radio"/> DNS Settings for DirectAccess <input type="radio"/> Generic DNS Server <input type="radio"/> Encoding</p> <p><input checked="" type="checkbox"/> Enable DNSSEC in this rule</p> <p>DNSSEC settings</p> <p>Validation:</p> <p><input checked="" type="checkbox"/> Require DNS clients to check that name and address data has been validated by the DNS server</p> <p>IPsec:</p> <p><input type="checkbox"/> Use IPsec in communication between the DNS client and DNS server</p> <p>Encryption type: <input type="text" value="No encryption (integrity only)"/></p> <p style="text-align: right;"><input type="button" value="Update"/> <input type="button" value="Create"/> <input type="button" value="Clear"/></p>
--	---

- Kiểm tra **Name Resolution Policy Table**, click vào **Apply**.

- Trong cửa sổ cmd, nhập vào **gpupdate /force** để 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>gpupdate /force
Updating policy...

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

C:\Users\Administrator>_
```

- Vào Windows PowerShell, nhập vào lệnh: **Resolve-DnsName bkaptech.vn -DnssecOk -Server BKAP-DC12-01.bkaptech.vn**

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> Resolve-DnsName bkaptech.vn -DnssecOk -Server BKAP-DC12-01.bkaptech.vn

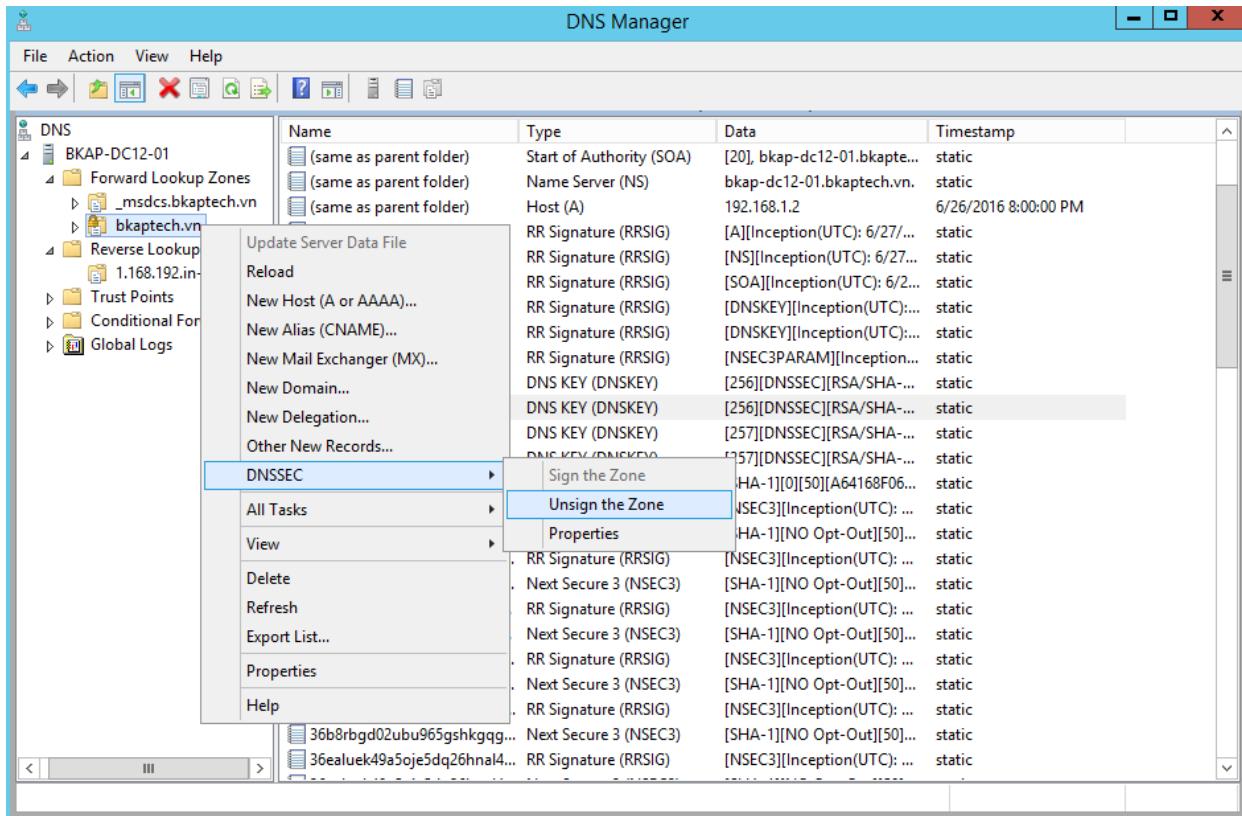
Name                           Type      TTL   Section    IPAddress
----                           ----      --   -----      -----
bkaptech.vn                   A          600  Answer     192.168.1.2

Name          : bkaptech.vn
QueryType    : RRSIG
TTL          : 600
Section      : Answer
TypeCovered  : A
Algorithm    : 8
LabelCount   : 2
OriginalTtl  : 600
Expiration   : 7/7/2016 4:06:08 AM
Signed        : 6/27/2016 3:06:08 AM
Signer       : bkaptech.vn
Signature    : {54, 5, 203, 92...}

Name          : .
QueryType    : OPT
TTL          : 32768
Section      : Additional
Data         : {}

PS C:\Users\Administrator>
```

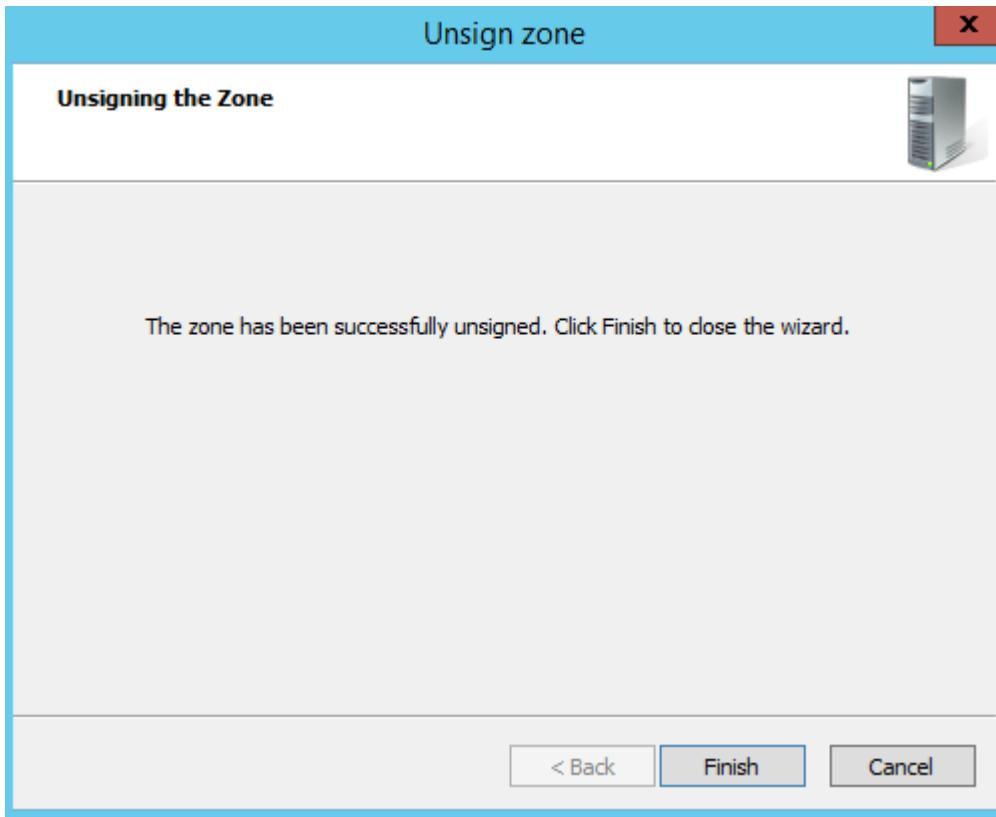
- Vào **DNS**, trong cửa sổ **DNS Manager**, click chuột phải tại tên miền **bkaptech.vn** , chọn vào **DNSSEC / Unsigned the Zone**.



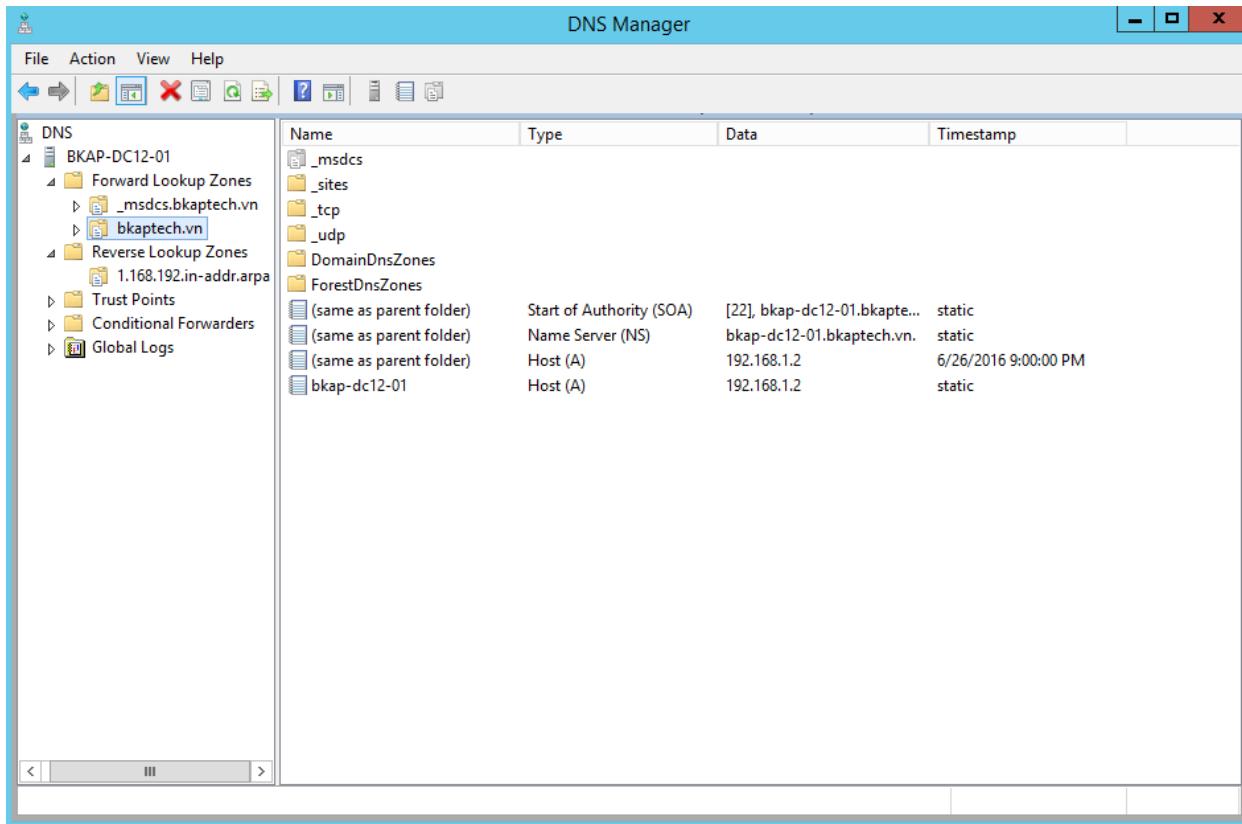
- Tại cửa sổ **DNS Security Extensions (DNSSEC)**, click vào **Next**.



- Tại cửa sổ **Unsigning the Zone**, click vào **Finish**.



- Click vào Refresh.



- Vào Windows PowerShell, thực hiện nhập vào câu lệnh: **Get-DnsServer**.

```

PS C:\Users\Administrator> Get-DnsServer
WARNING: EnableRegistryBoot not applicable on DNS Server BKAP-DC12-01 version.

ServerSetting:
=====
EnableOnlineSigning          True
TcpReceivePacketSize        65536
WriteAuthorityNs             False
SocketPoolSize               2500
AppendMsZoneTransferTag     False
NameCheckFlag                2
UpdateOptions                 783
MaximumTrustAnchorActiveRefreshInterval 15:00:00:00
EnableIPv6                    True
RpcProtocol                  5
ForestDirectoryPartitionBaseName ForestDnsZones
AutoCreateDelegation          2
EnableDirectoryPartitions    True
SelfTest                      4294967295
DsAvailable                   True
EnableSendErrorSuppression   True
SilentlyIgnoreCNameUpdateConflicts False
EnableDuplicateQuerySuppression True
DomainDirectoryPartitionBaseName DomainDnsZones
ReloadException               False
AdminConfigured                True
StrictFileParsing              False
AllowCNameAtNs                 True
MaximumSignatureScanPeriod    2:00:00:00
IsReadOnlyDC                   False
DisableAutoReverseZone        False
AllTCPAddress                 {192.168.1.2}
EnableUpdateForwarding        False
DeleteOutsideGlue              False
MinorVersion                  3
MajorVersion                  6
LocalNetPriority              True
RootTrustAnchorsURL          https://data.iana.org/root-anchors/ro...
MaxResourceRecordsInNonSecureUpdate 30
ComputerName                  BKAP-DC12-01.bkaptech.vn
RemoteIPv4RankBoost           5
ZoneWritebackInterval         00:01:00
EnableWinsR                   True
NoUpdateDelegations           False
LameDelegationTtl            00:00:00
SocketPoolExcludedPortRanges  {}
EnableRsoForRdc                True
AllowUpdate                    True
ListeningIPAddress             {192.168.1.2}
MaximumUdpPacketsize          4000
XfrConnectTimeout              30
OpenAc1OnProxyUpdates         True
EnableQueryResponseGeneration False
RoundRobin                     True
AutoConfigFileZones           1
SendPort                       0
MaximumRdcRsoQueueLength      300
RemoteIPv6RankBoost            0
AutoCacheUpdate                False
LooseWildcarding               False
BootMethod                      3
EnableVersionQuery              0
BuildNumber                     9600
AllowReadOnlyZoneTransfer      False
BindSecondaries                False
SyncDsZoneSerial                2
MaximumRdcRsoAttemptsPerCycle 100

```

```
Select Administrator: Windows PowerShell

ServerRootHint:
=====
NameServer          IPAddress
-----            -----
a.root-servers.net.    198.41.0.4
b.root-servers.net.    192.228.79.201
c.root-servers.net.    192.33.4.12
d.root-servers.net.    199.7.91.13
e.root-servers.net.    192.203.230.10
f.root-servers.net.    192.5.5.241
g.root-servers.net.    192.112.36.4
h.root-servers.net.    128.63.2.53
i.root-servers.net.    192.36.148.17
j.root-servers.net.    192.58.128.30
k.root-servers.net.    193.0.14.129
l.root-servers.net.    199.7.83.42
m.root-servers.net.    202.12.27.33

ServerZone:
=====
ZoneName      ZoneType   IsAutoCreated  IsDsIntegrated  IsReverseLookupZone  IsSigned
-----        -----      -----          -----          -----          -----
_msdcsv.bkaptech.vn Primary   False          True           False           False
0.in-addr.arpa Primary   True           False          True            False
1.168.192.in-addr.arpa Primary   False          True           True            False
127.in-addr.arpa Primary   True           False          True            False
255.in-addr.arpa Primary   True           False          True            False
bkaptech.vn     Primary   False          True           False           False
TrustAnchors    Primary   False          True           True            False

ServerZoneAging:
=====
ZoneName      AgingEnabled  AvailForScavengeTime RefreshInterval NoRefreshInterval ScavengeServers
-----        :           :           :           :           :
_msdcsv.bkaptech.vn : False       : 7.00:00:00   : 7.00:00:00   : 7.00:00:00   :
0.in-addr.arpa Primary   : False       : 7.00:00:00   : 7.00:00:00   : 7.00:00:00   :
1.168.192.in-addr.arpa Primary   : False       : 7.00:00:00   : 7.00:00:00   : 7.00:00:00   :
127.in-addr.arpa Primary   : False       : 7.00:00:00   : 7.00:00:00   : 7.00:00:00   :
255.in-addr.arpa Primary   : False       : 7.00:00:00   : 7.00:00:00   : 7.00:00:00   :
```

- Nhập tiếp câu lệnh: **dnscmd /config /socketpoolsize 3000.**

```
Administrator: Windows PowerShell
ZoneName      : TrustAnchors
AgingEnabled   : False
AvailForScavengeTime : 
RefreshInterval : 7.00:00:00
NoRefreshInterval : 7.00:00:00
ScavengeServers   : 

PS C:\Users\Administrator> dnscmd /config /socketpoolsize 3000
Registry property socketpoolsize successfully reset.
Command completed successfully.

PS C:\Users\Administrator>
```

- Nhập vào câu lệnh **net stop dns.**

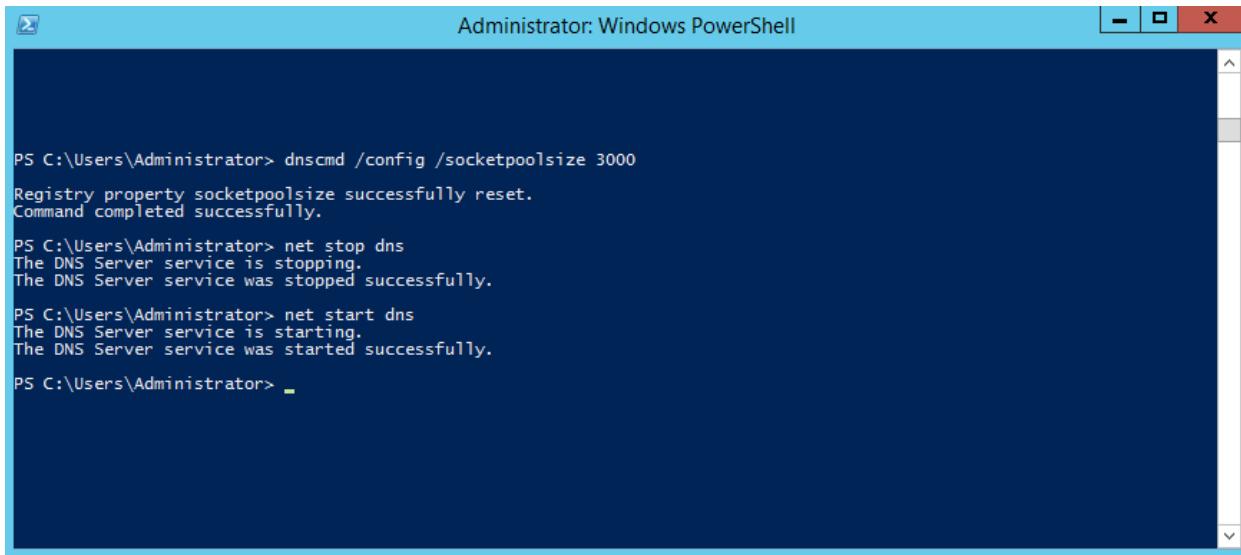
```
Administrator: Windows PowerShell
ZoneName      : TrustAnchors
AgingEnabled   : False
AvailForScavengeTime : 
RefreshInterval : 7.00:00:00
NoRefreshInterval : 7.00:00:00
ScavengeServers   : 

PS C:\Users\Administrator> dnscmd /config /socketpoolsize 3000
Registry property socketpoolsize successfully reset.
Command completed successfully.

PS C:\Users\Administrator> net stop dns
The DNS Server service is stopping.
The DNS Server service was stopped successfully.

PS C:\Users\Administrator>
```

- Nhập vào tiếp câu lệnh **net start dns**.



The screenshot shows an Administrator Windows PowerShell window titled "Administrator: Windows PowerShell". The command history is as follows:

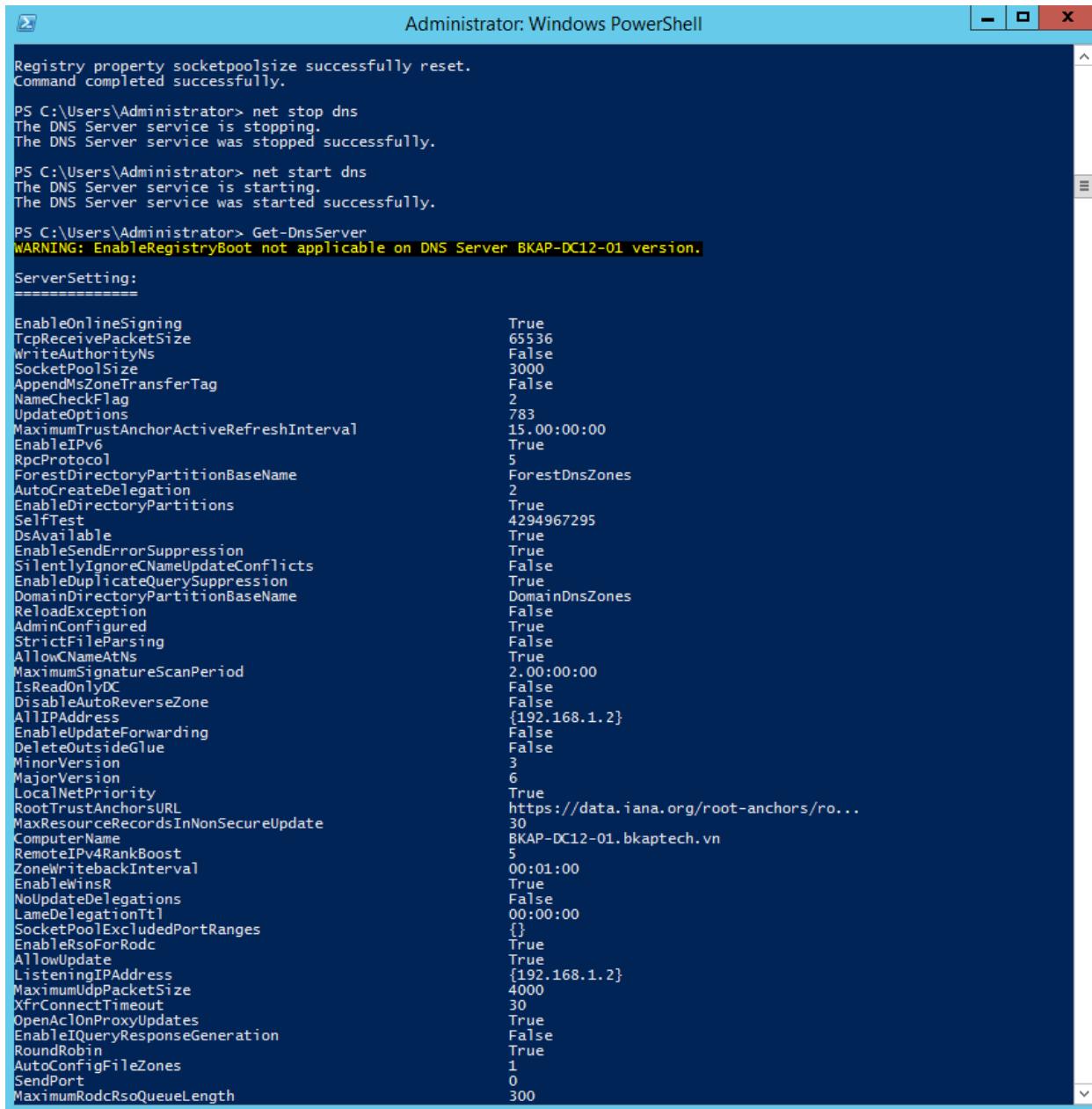
```
PS C:\Users\Administrator> dnscmd /config /socketpoolsize 3000
Registry property socketpoolsize successfully reset.
Command completed successfully.

PS C:\Users\Administrator> net stop dns
The DNS Server service is stopping.
The DNS Server service was stopped successfully.

PS C:\Users\Administrator> net start dns
The DNS Server service is starting.
The DNS Server service was started successfully.

PS C:\Users\Administrator>
```

▪ Nhập vào câu lệnh **Get-DnsServer**.



```

Administrator: Windows PowerShell

Registry property socketpoolsize successfully reset.
Command completed successfully.

PS C:\Users\Administrator> net stop dns
The DNS Server service is stopping.
The DNS Server service was stopped successfully.

PS C:\Users\Administrator> net start dns
The DNS Server service is starting.
The DNS Server service was started successfully.

PS C:\Users\Administrator> Get-DnsServer
WARNING: EnableRegistryBoot not applicable on DNS Server BKAP-DC12-01 version.

ServerSetting:
=====

EnableOnlineSigning True
TcpReceivePacketSize 65536
WriteAuthorityNs False
SocketPoolSize 3000
AppendMsZoneTransferTag False
NameCheckFlag 2
UpdateOptions 783
MaximumTrustAnchorActiveRefreshInterval 15.00:00:00
EnableIPv6 True
RpcProtocol 5
ForestDirectoryPartitionBaseName ForestDnsZones
AutoCreateDelegation 2
EnableDirectoryPartitions True
SelfTest 4294967295
DsAvailable True
EnableSendErrorSuppression True
SilentlyIgnoreCNameUpdateConflicts False
EnableDuplicateQuerySuppression True
DomainDirectoryPartitionBaseName DomainDnsZones
ReloadException False
AdminConfigured True
StrictFileParsing False
AllowCNameAtNs True
MaximumSignatureScanPeriod 2.00:00:00
IsReadOnlyDc False
DisableAutoReverseZone False
AllIpAddress {192.168.1.2}
EnableUpdateForwarding False
DeleteOutsideGlue False
MinorVersion 3
MajorVersion 6
LocalNetPriority True
RootTrustAnchorsURL https://data.iana.org/root-anchors/ro...
MaxResourceRecordsInNonSecureUpdate 30
ComputerName BKAP-DC12-01.bkaptech.vn
RemoteIPv4RankBoost 5
ZoneWritebackInterval 00:01:00
EnableWinsR True
NoUpdateDelegations False
LameDelegationTtl 00:00:00
SocketPoolExcludedPortRanges []
EnableRsoForRdc True
AllowUpdate True
ListeningIPAddress {192.168.1.2}
MaximumUdpPacketSize 4000
XfrConnectTimeout 30
OpenActionProxyUpdates True
EnableIQueryResponseGeneration False
RoundRobin True
AutoConfigFileZones 1
SendPort 0
MaximumRdcRsoQueueLength 300

```

```
Administrator: Windows PowerShell

NoRefreshInterval          7.00:00:00
ScavengingInterval          00:00:00
ScavengingState              False

ServerRecursion:
=====
AdditionalTimeout           4
SecureResponse                True
Enable                         True
Timeout                        8
RetryInterval                  3

ServerDiagnostics:
=====
SendPackets                  False
UdpPackets                   False
EnableLoggingForZoneLoadingEvent False
Update                          False
Answers                         False
EnableLogFileRollover          False
UnmatchedResponse              False
EnableLoggingForRemoteServerEvent False
EnableLoggingForServerStartStopEvent False
TcpPackets                     False
EventLogLevel                  4
EnableLoggingForPluginDllEvent False
EnableLoggingForTombstoneEvent False
FullPackets                    False
UseSystemEventLog              False
Notifications                  False
EnableLoggingToFile             True
EnableLoggingForLocalLookupEvent False
SaveLogsToPersistentStorage     False
ReceivePackets                 False
Queries                         False
EnableLoggingForZoneDataWriteEvent False
QuestionTransactions            False
FilterIpAddressList             {}
EnableLoggingForRecursiveLookupEvent False
WriteThrough                    False
MaxMBFileSize                  5000000000

ServerGlobalNameZone:
=====
Enable                         False
GlobalOverLocal                 False
SendTimeout                      3
AlwaysQueryServer                 False
ServerQueryInterval               06:00:00
EnableDnsProbes                  True
PreferAaaa                       False
BlockUpdates                     True

ServerCache:
=====
IsReverseLookupZone              False
IsDsIntegrated                  True
IsReadOnly                      False
MaxNegativeTtl                  00:15:00
ZoneName                         .
MaxTtl                           1.00:00:00
StoreEmptyAuthenticationResponse True
```

```
Administrator: Windows PowerShell

=====
EnableReordering          True
Timeout                   3
UseRootHint               True

ServerRootHint:

NameServer                IPAddress
-----  -----
m.root-servers.net.       202.12.27.33
l.root-servers.net.       199.7.83.42
k.root-servers.net.       193.0.14.129
j.root-servers.net.       192.58.128.30
i.root-servers.net.       192.36.148.17
h.root-servers.net.       128.63.2.53
g.root-servers.net.       192.112.36.4
f.root-servers.net.       192.5.5.241
e.root-servers.net.       192.203.230.10
d.root-servers.net.       199.7.91.13
c.root-servers.net.       192.33.4.12
b.root-servers.net.       192.228.79.201
a.root-servers.net.       198.41.0.4

ServerZone:

ZoneName                 ZoneType   IsAutoCreated  IsDsIntegrated  IsReverseLookupZone  IsSigned
-----  -----
_msdcsv.bkaptech.vn      Primary    False          True            False              False
0.in-addr.arpa           Primary    True           False          True              False
1.168.192.in-addr.arpa  Primary    False          True            True              False
127.in-addr.arpa         Primary    True           False          True              False
255.in-addr.arpa         Primary    True           False          True              False
bkaptech.vn               Primary    False          True            False              False
TrustAnchors              Primary    False          True            True              False

ServerZoneAging:

ZoneName      : _msdcsv.bkaptech.vn
AgingEnabled : False
AvailForScavengeTime :
RefreshInterval : 7.00:00:00
NoRefreshInterval : 7.00:00:00
ScavengeServers :

ZoneName      : 0.in-addr.arpa
AgingEnabled : False
AvailForScavengeTime :
RefreshInterval : 7.00:00:00
NoRefreshInterval : 7.00:00:00
ScavengeServers :

ZoneName      : 1.168.192.in-addr.arpa
AgingEnabled : False
AvailForScavengeTime :
RefreshInterval : 7.00:00:00
NoRefreshInterval : 7.00:00:00
ScavengeServers :

ZoneName      : 127.in-addr.arpa
AgingEnabled : False
AvailForScavengeTime :
RefreshInterval : 7.00:00:00
```

- Cấu hình DNS cache locking.
 - Trong cửa sổ Windows PowerShell, nhập vào câu lệnh **Set-DnsServerCache -LockingPercent 75**.

```
AgingEnabled      : False
AvailForScavengeTime :
RefreshInterval   : 7.00:00:00
NoRefreshInterval  : 7.00:00:00
ScavengeServers    :

PS C:\Users\Administrator> Set-DnsServerCache -LockingPercent 75
PS C:\Users\Administrator>
```

- Nhập vào câu lệnh **net stop dns , net start dns**.

```
AgingEnabled      : False
AvailForScavengeTime :
RefreshInterval   : 7.00:00:00
NoRefreshInterval  : 7.00:00:00
ScavengeServers    :

PS C:\Users\Administrator> Set-DnsServerCache -LockingPercent 75
PS C:\Users\Administrator> net stop dns
The DNS Server service is stopping.
The DNS Server service was stopped successfully.

PS C:\Users\Administrator> net start dns
The DNS Server service is starting.
The DNS Server service was started successfully.

PS C:\Users\Administrator>
```

- Nhập vào câu lệnh **Get-DnsServer** để kiểm tra.

```
=====
Enable          : False
GlobalOverLocal : False
SendTimeout     : 3
AlwaysQueryServer: False
ServerQueryInterval: 06:00:00
EnableEDnsProbes: True
PreferAaaa       : False
BlockUpdates    : True

ServerCache:
=====

IsReverseLookupZone   : False
IsDsIntegrated        : True
IsReadOnly             : False
MaxNegativeTtl         : 00:15:00
ZoneName               :
MaxTtl                : .
StoreEmptyAuthenticationResponse: True
ZoneType               : Cache
IsPaused               : False
IsShutdown              : False
DistinguishedName      : DC=RootDNSServers,cn=MicrosoftDNS,DC=...
EnablePollutionProtection: True
LockingPercent         : 75
MaxKBSIZE              : 0
IsAutoCreated           : False

ServerGlobalQueryBlockList:
=====
```

- Cấu hình GlobalNames zone:

- Trong cửa sổ **Windows PowerShell**, nhập vào câu lệnh **Add-DnsServerPrimaryZone -Name bkap.vn -ReplicationScope Forest**

```
ZoneName      : TrustAnchors
AgingEnabled  : False
AvailForScavengeTime: 00:00:00
RefreshInterval: 7.00:00:00
NoRefreshInterval: 7.00:00:00
ScavengeServers:
```

PS C:\Users\Administrator> Add-DnsServerPrimaryZone -Name bkap.vn -ReplicationScope Forest

PS C:\Users\Administrator>

- Nhập tiếp câu lệnh **Set-DnsServerGlobalNameZone – AlwaysQueryServer \$true.**

Administrator: Windows PowerShell

```
ZoneName      : TrustAnchors
AgingEnabled  : False
AvailForScavengeTime :
RefreshInterval : 7.00:00:00
NoRefreshInterval : 7.00:00:00
ScavengeServers :
```

PS C:\Users\Administrator> Add-DnsServerPrimaryZone -Name bkap.vn -ReplicationScope Forest
PS C:\Users\Administrator> Set-DnsServerGlobalNameZone -AlwaysQueryServer \$true
PS C:\Users\Administrator>

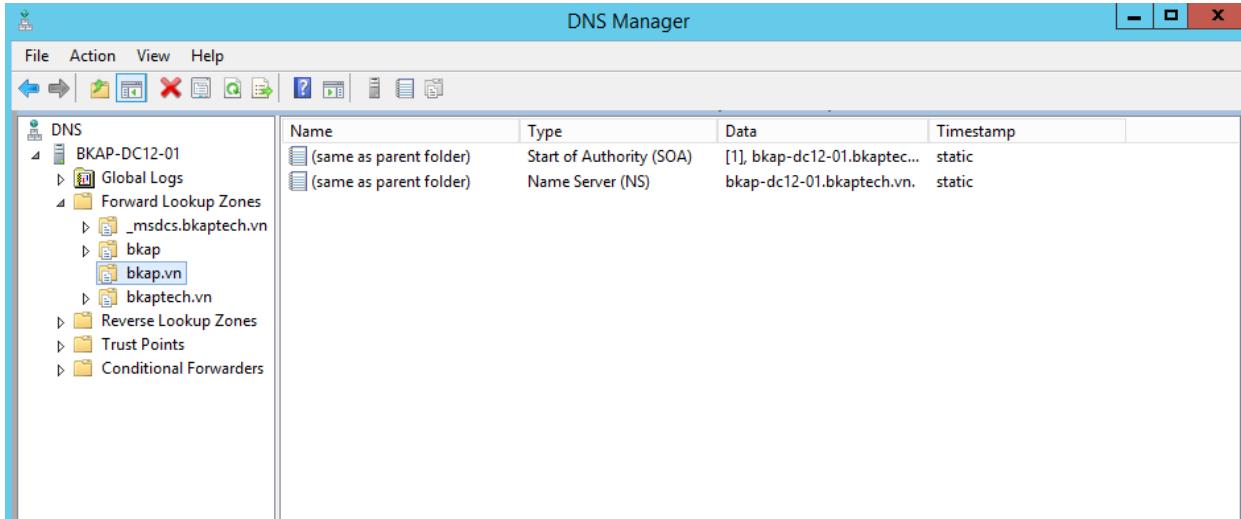
- Nhập vào câu lệnh **Add-DnsServerPrimaryZone –Name bkaptech –ReplicationScope Forest**

Administrator: Windows PowerShell

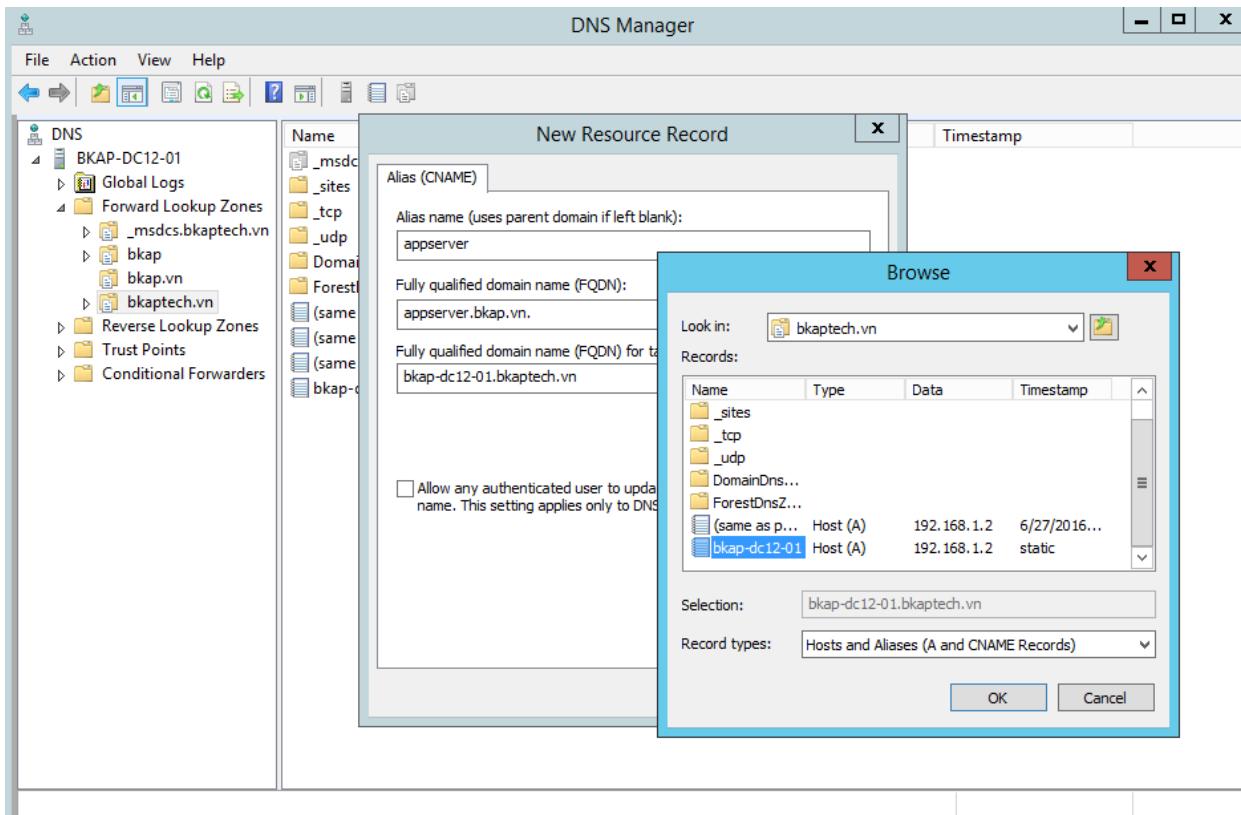
```
ZoneName      : TrustAnchors
AgingEnabled  : False
AvailForScavengeTime :
RefreshInterval : 7.00:00:00
NoRefreshInterval : 7.00:00:00
ScavengeServers :
```

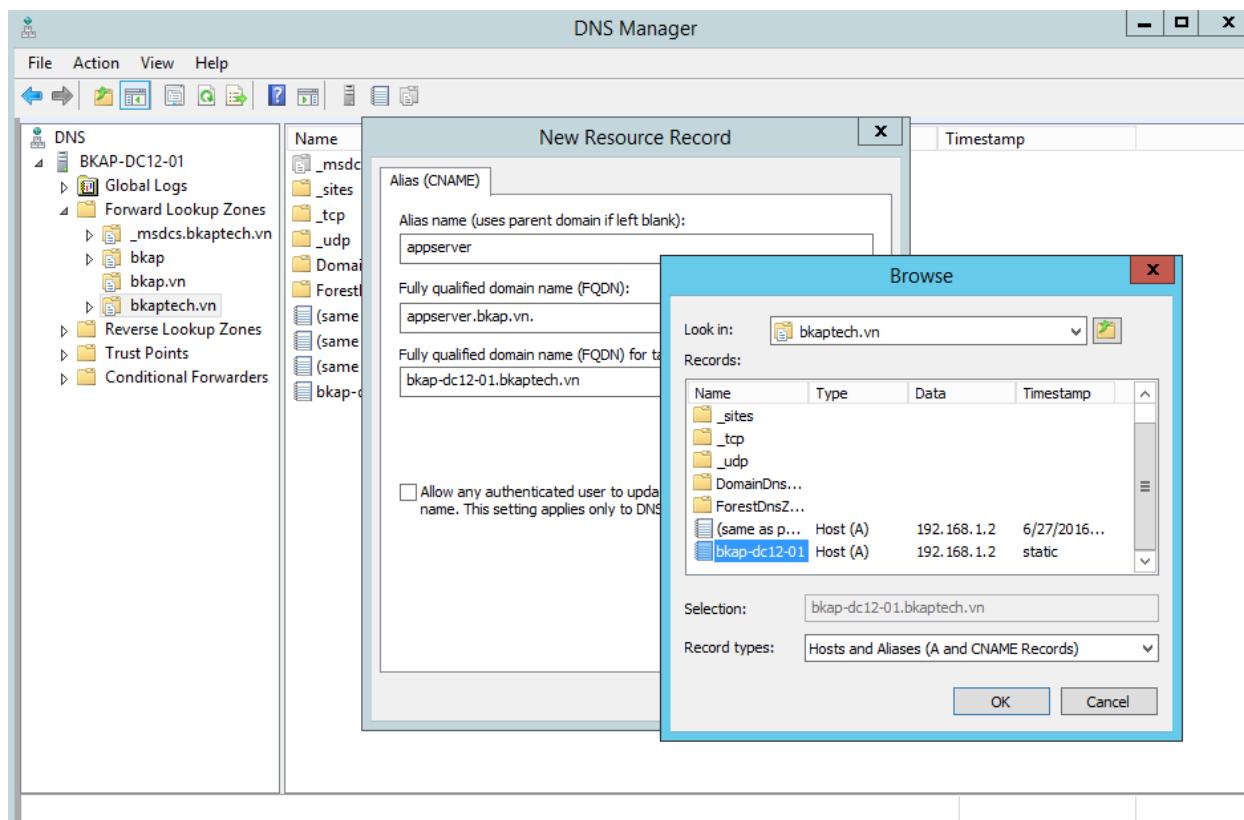
PS C:\Users\Administrator> Add-DnsServerPrimaryZone -Name bkap.vn -ReplicationScope Forest
PS C:\Users\Administrator> Set-DnsServerGlobalNameZone -AlwaysQueryServer \$true
PS C:\Users\Administrator> Add-DnsServerPrimaryZone -Name bkap -ReplicationScope Forest
PS C:\Users\Administrator>

- Trong **DNS Manager**, click vào **Refresh**, kiểm tra **Forward Lookup Zone**.



- Trong zone **bkap.vn**, tạo 1 bản ghi **CNAME** :
- Tại cửa sổ **New Resource Record**, nhập vào tại mục **Alias name : appserver**, tại mục **Fully qualified domain name (FQDN) for target host**, browse đến bản ghi *bkap-dc12-01*.





- Thực hiện ping appserver.bkap.vn.

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> ping appserver.bkap.vn

Pinging bkap-dc12-01.bkaptech.vn [192.168.1.2] with 32 bytes of data:
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128

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 = 0ms, Average = 0ms
PS C:\Users\Administrator>
```

Bài 2:**TRIỂN KHAI CẤU HÌNH FILE SERVICES NÂNG CAO.**

Các nội dung chính được đề cập:

- ✓ Cấu hình iSCSI Storage.
- ✓ Cấu hình cơ sở hạ tầng phân loại tập tin.

2.1 Cấu hình iSCSI Storage**1.Yêu cầu bài Lab:**

- + Cài đặt và cấu hình iSCSI SAN.
 - Cài đặt iSCSI Target Server.
 - Tạo iSCSI Virtual Disk.
 - Kết nối Server đến iSCSI Target.
 - Tạo Storage Pool.
 - Tạo Virtual Disk.
 - Tạo Volume.

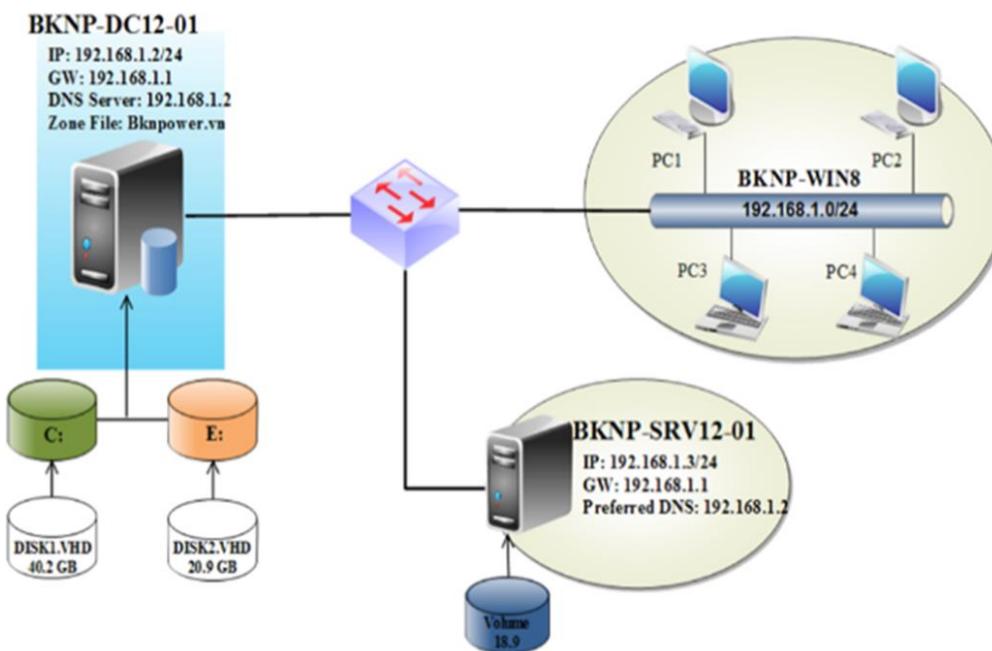
2.Yêu cầu chuẩn bị:

- + Máy BKAP-DC12-01: đã nâng cấp lên Domain Controller quản lý miền **bkaptech.vn** có gắn 2 ổ cứng đảm nhiệm vai trò lưu trữ dữ liệu.
- + Máy BKAP-SRV12-01: Domain Member đảm nhận vai trò File Server. Server này sẽ dùng hệ thống đĩa trên BKAP-DC12-01.
- + Máy BKAP-WRK08-01: Domain Member Client.

3.Mô hình Lab:

HỆ THỐNG ĐÀO TẠO CNTT QUỐC TẾ BACHKHOA-APTECH

Cấu hình iSCSI Storage

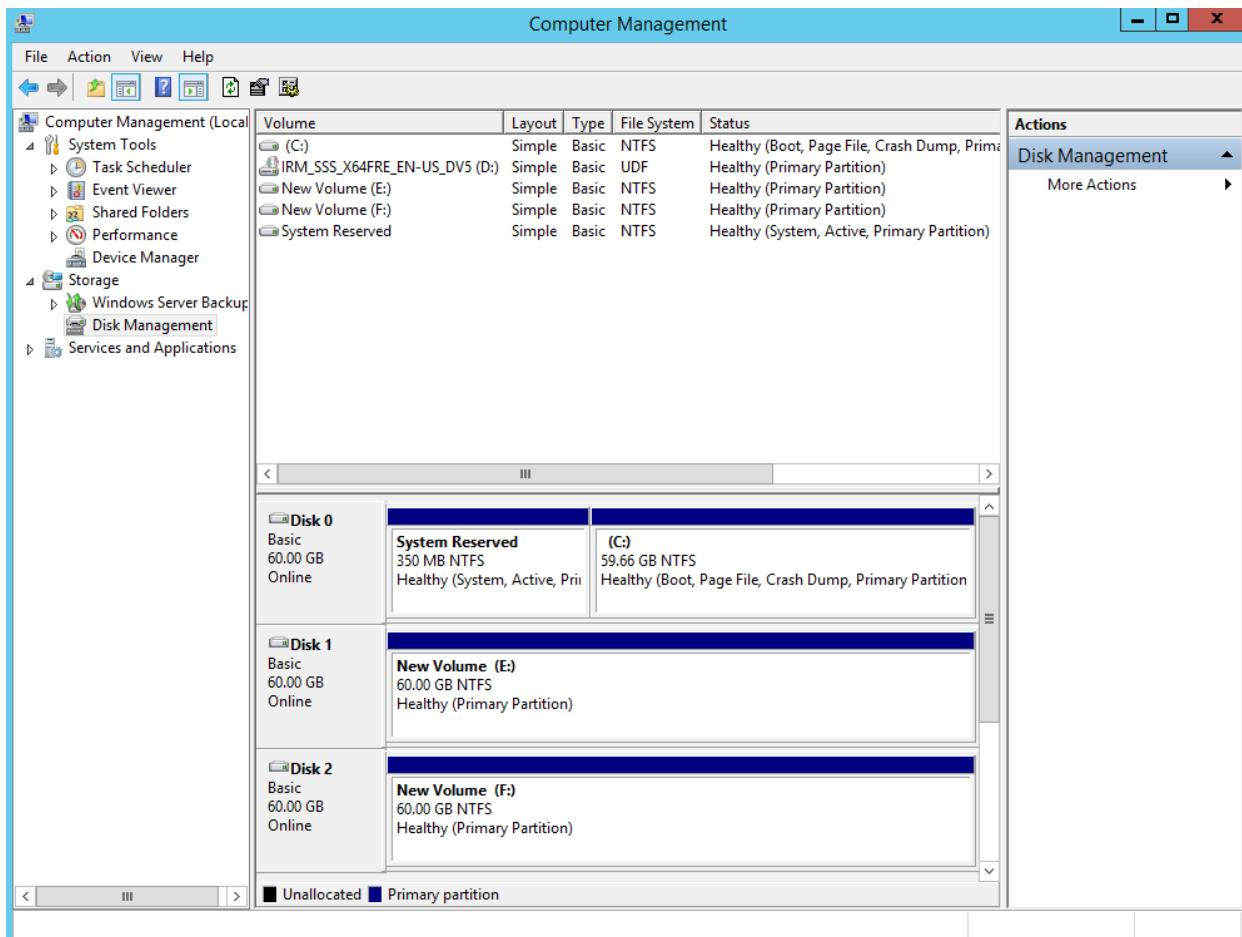


Sơ đồ địa chỉ như sau:

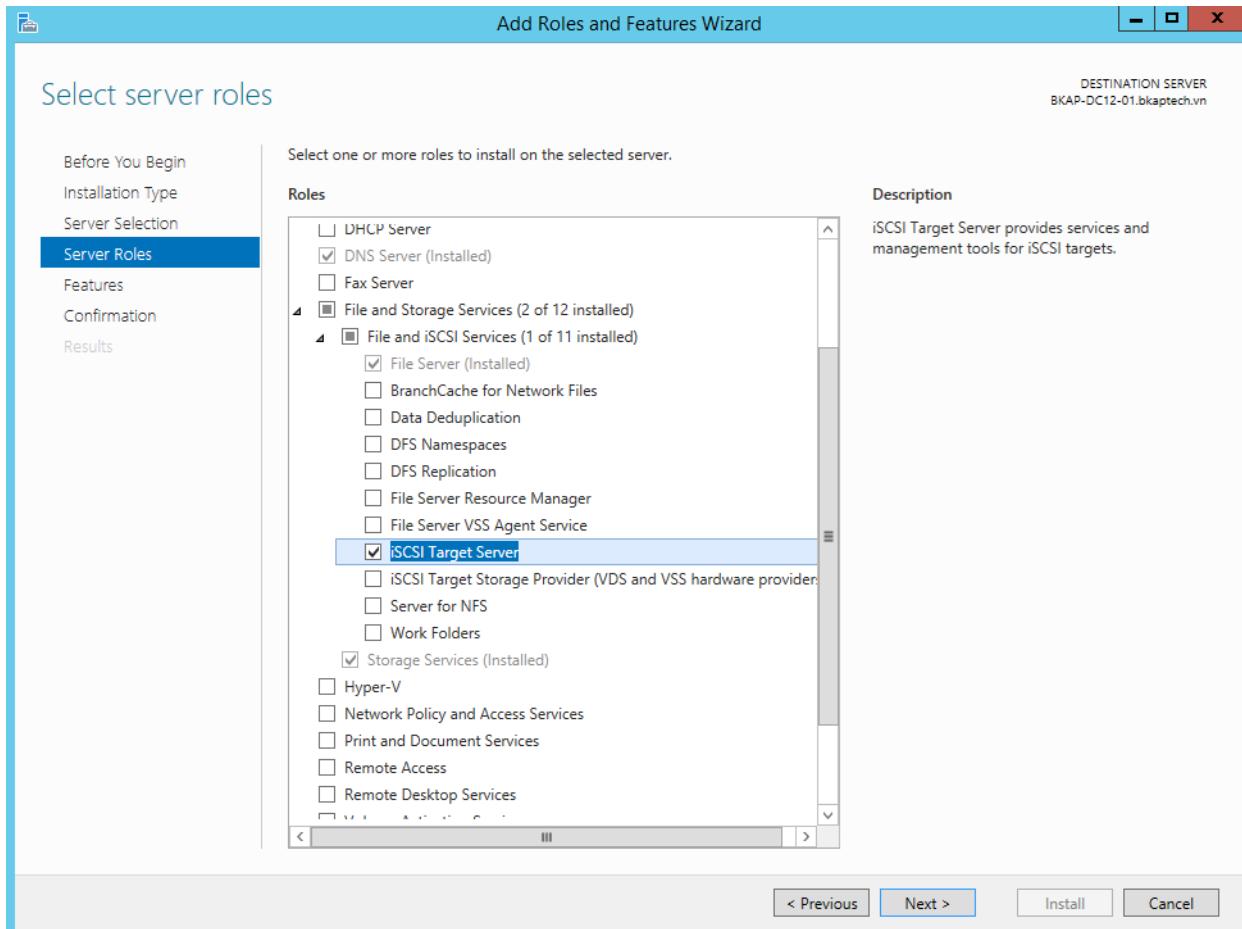
Thông số	BKAP-DC12-01	BKAP-SRV12-01	BKAP-WIN8
IP address	192.168.1.2	192.168.1.3	192.168.1.15
Subnet Mask	255.255.255.0	255.255.255.0	255.255.255.0
Default Gateway	192.168.1.1	192.168.1.1	192.168.1.1
DNS Server	192.168.1.2	192.168.1.2	192.168.1.2

Hướng dẫn chi tiết:

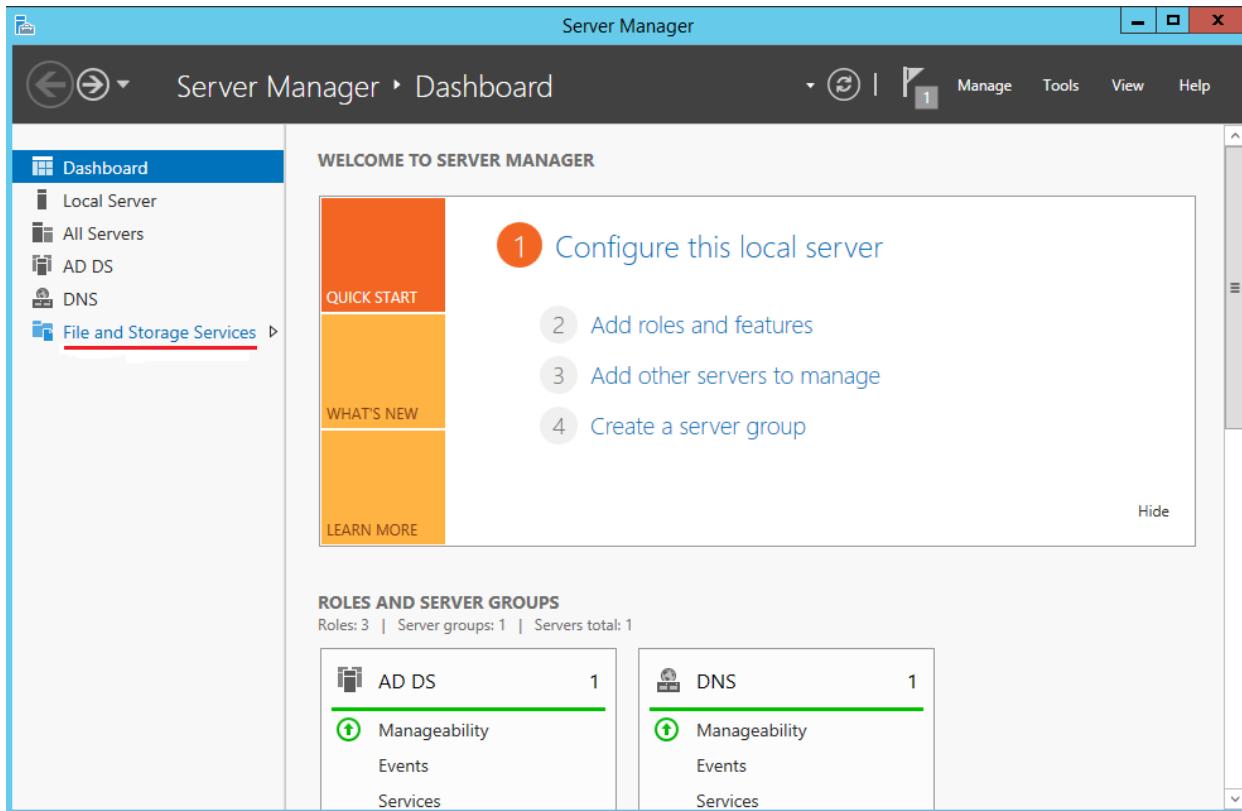
- Trên máy BKAP-DC12-01, gắn thêm 2 ổ cứng.



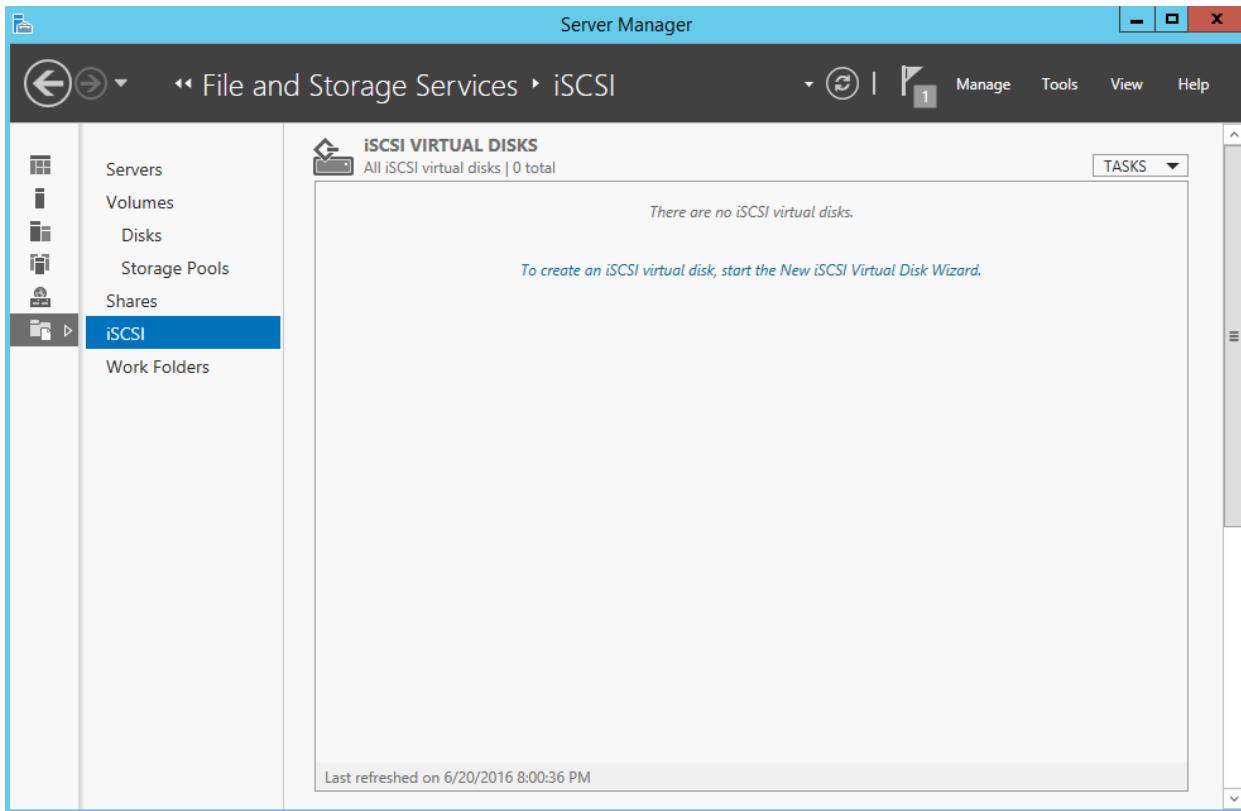
- Thực hiện cài đặt iSCSI Target Server.



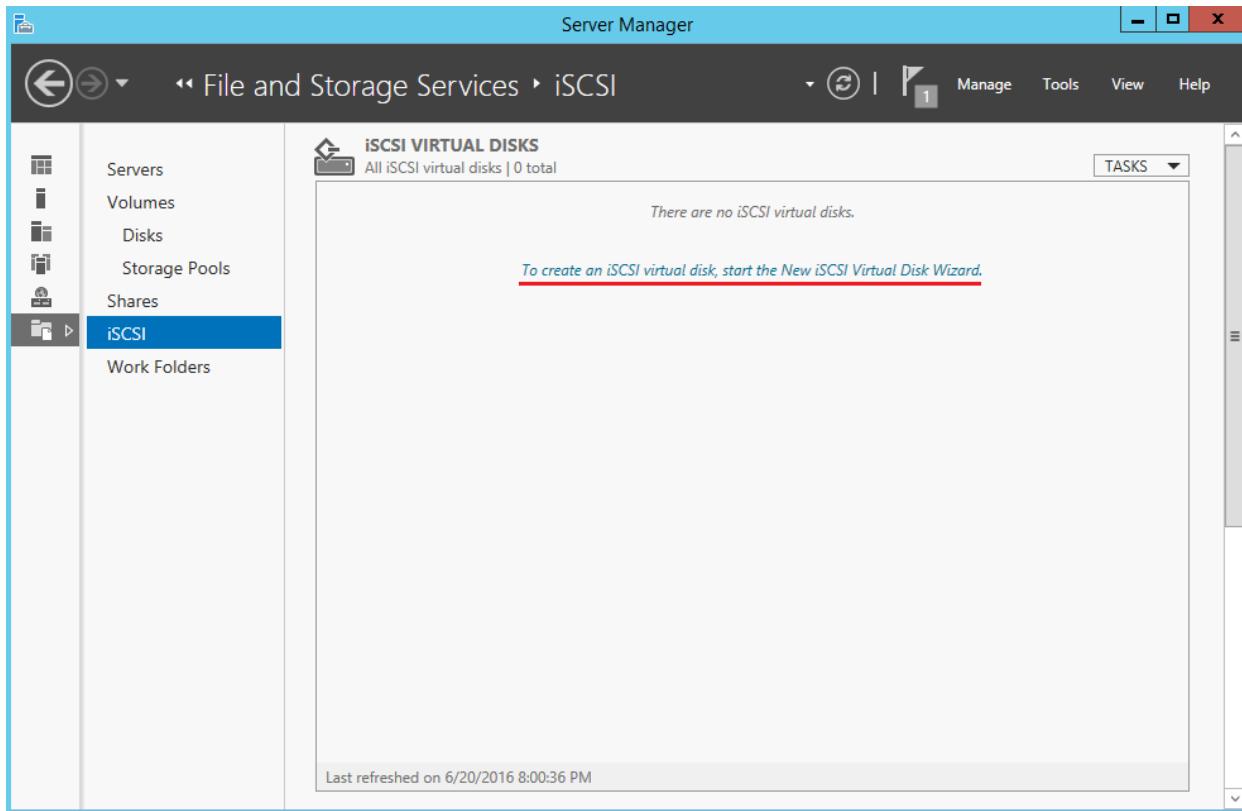
- Trong Server Manager, click chọn vào File and Storage Services.



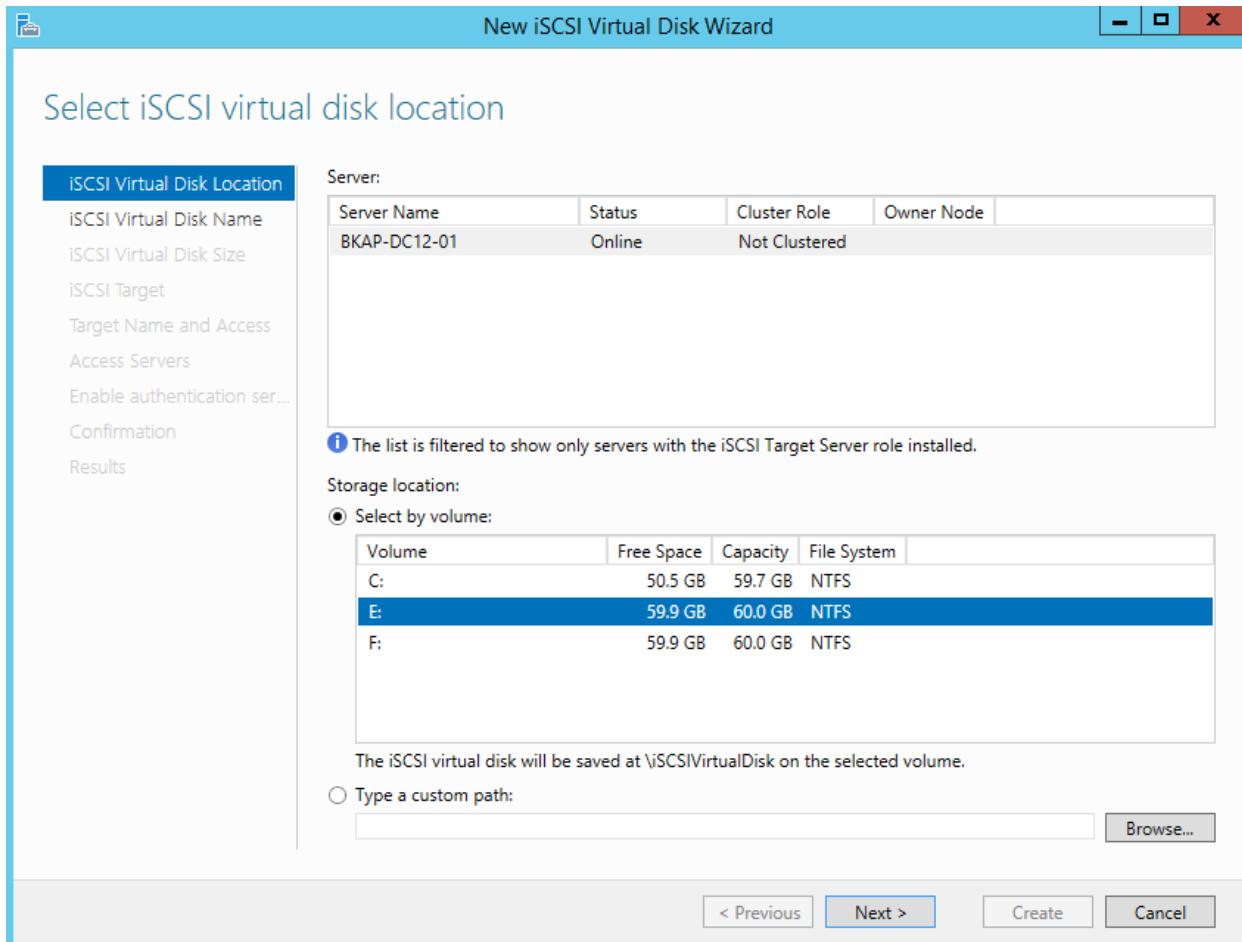
- Trong cửa sổ **File and Storage Services**, click chọn vào **iSCSI**.



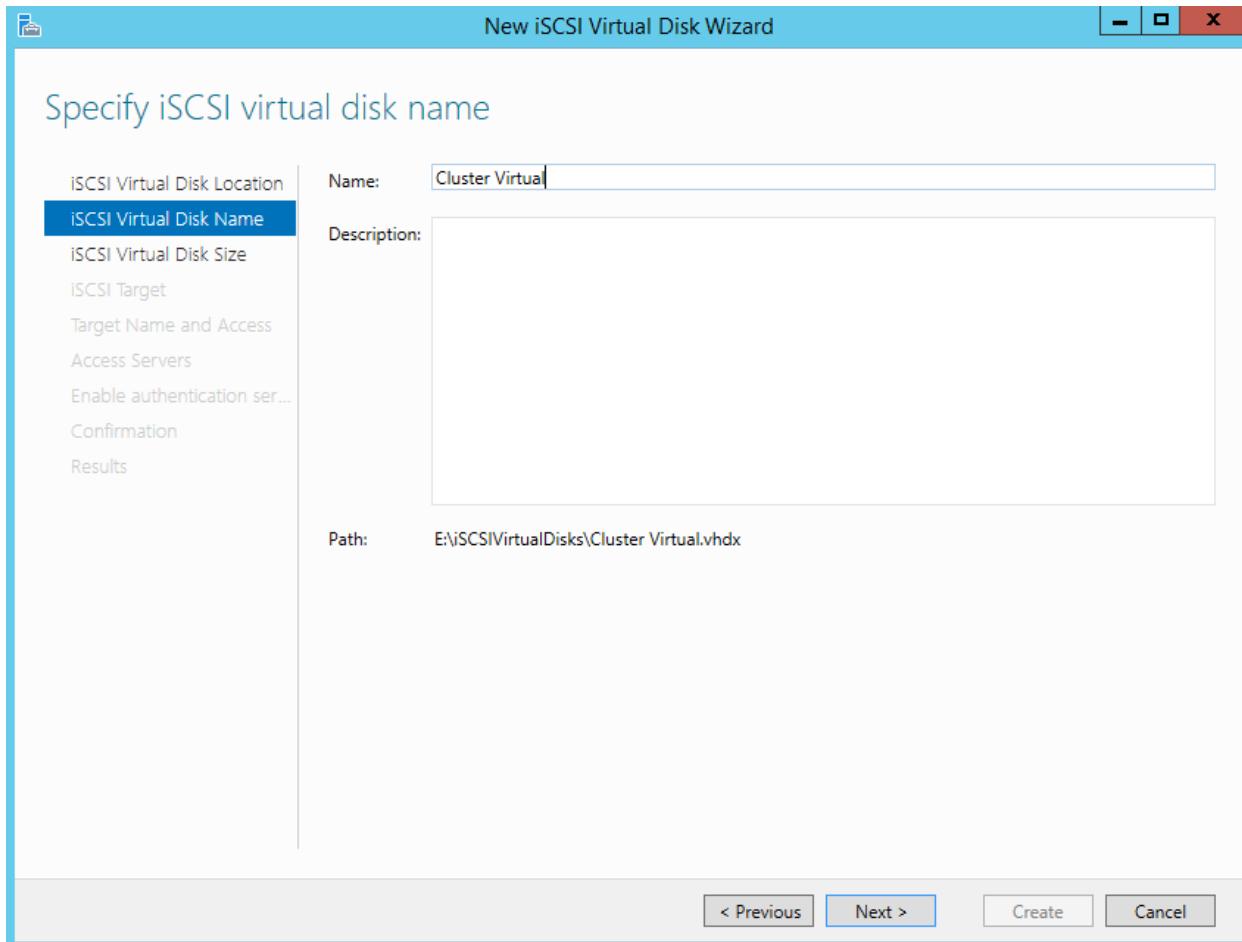
- Click chọn vào dòng *To create an iSCSI virtual disk, start the New iSCSI Virtual Disk Wizard.*



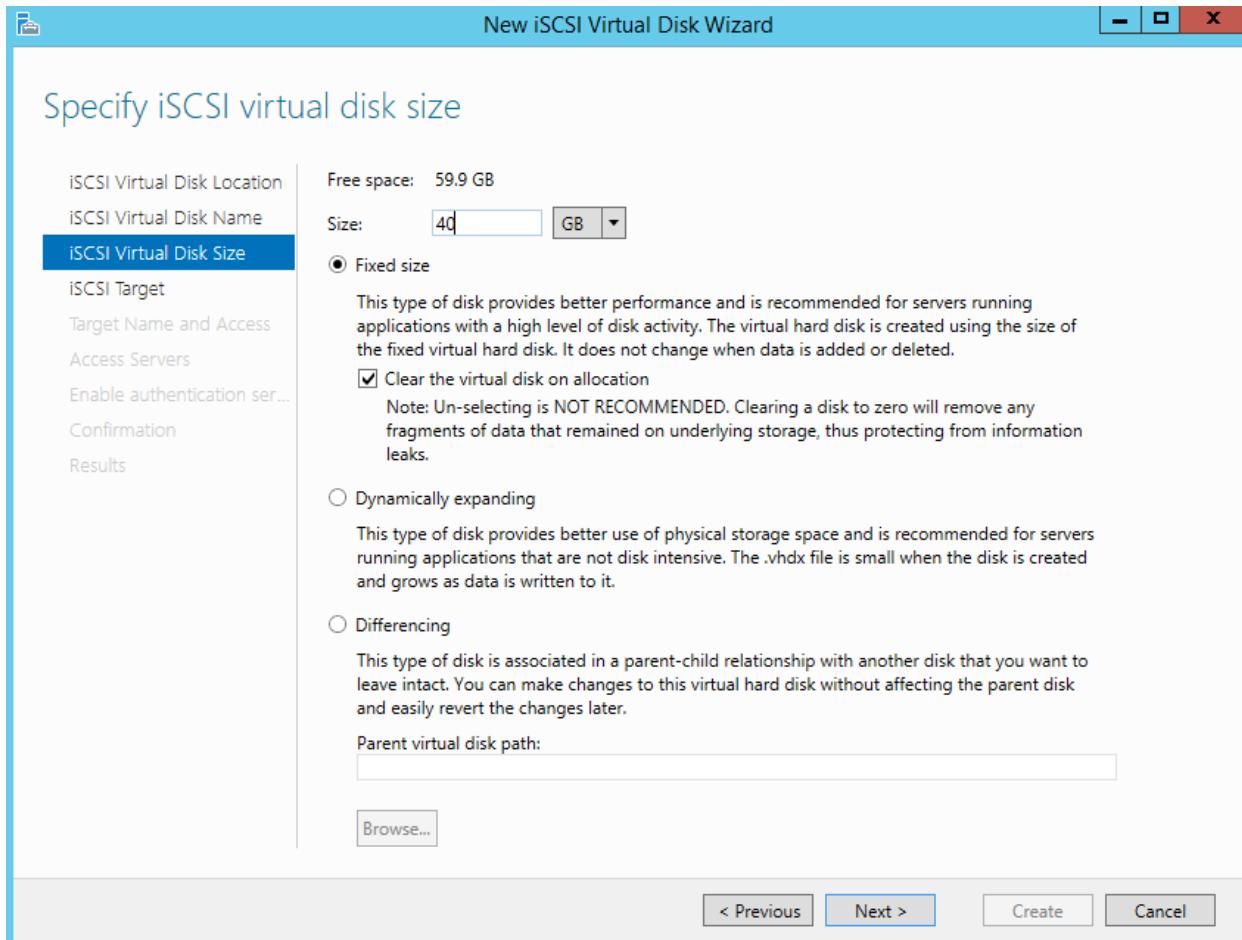
- Trong cửa sổ **Select iSCSI virtual disk location**, click chọn vào ô E , click vào **Next**.



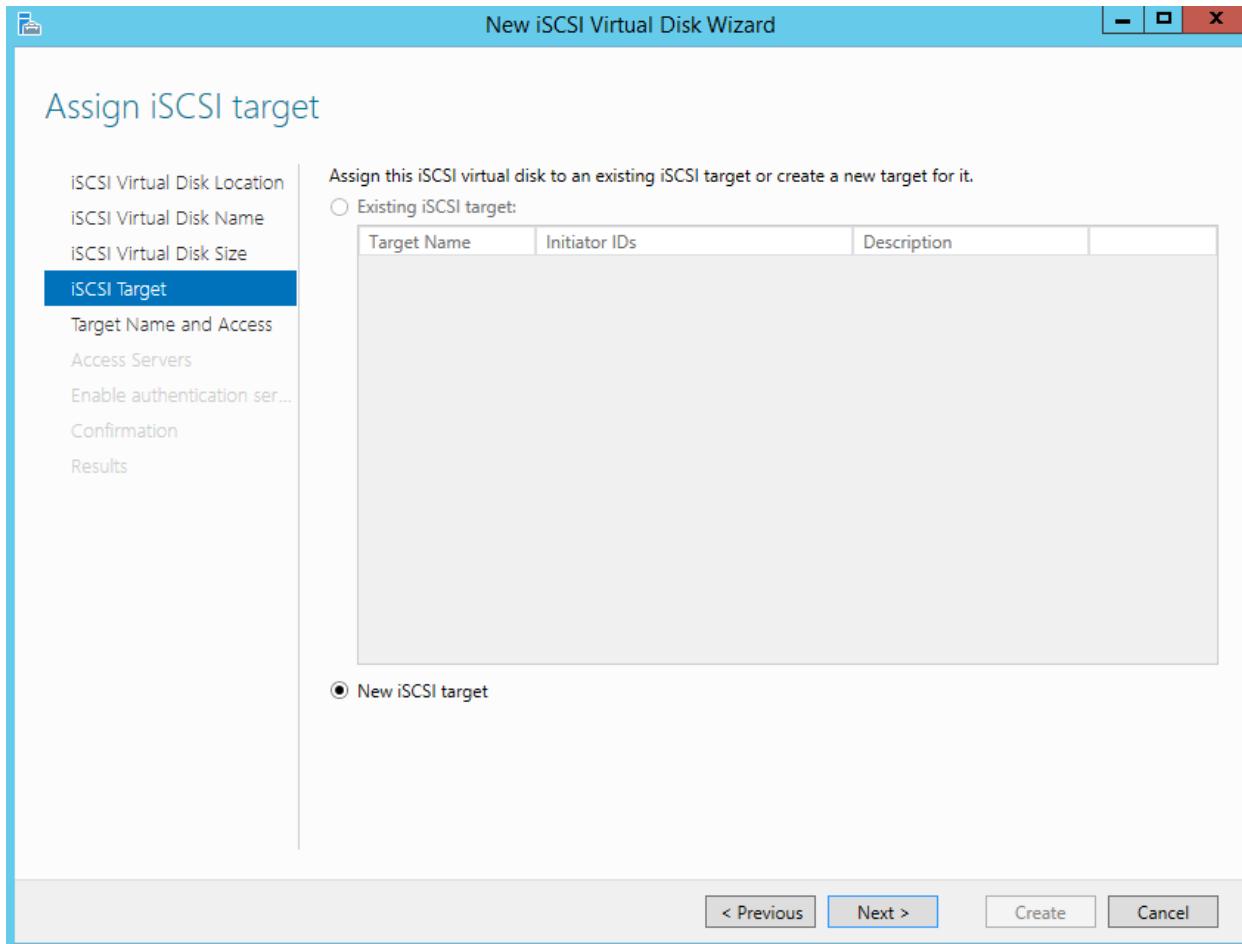
- Tại cửa sổ **Specify iSCSI virtual disk name**, nhập vào tại mục **Name: Cluster Virtual** , click vào **Next**.



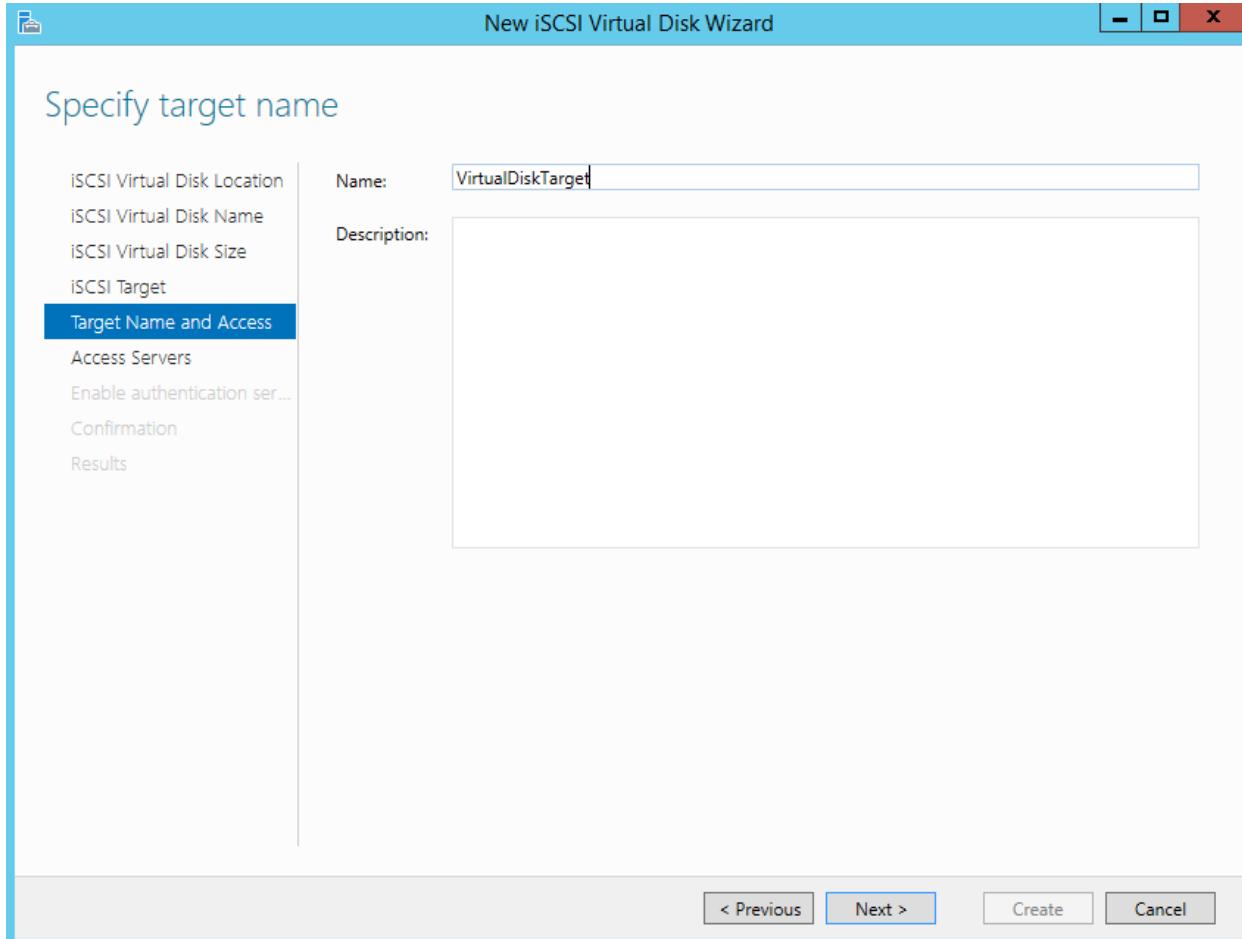
- Tại cửa sổ **Specify iSCSI virtual disk size**, nhập vào tại mục **Size:40 GB**, click vào **Next**.



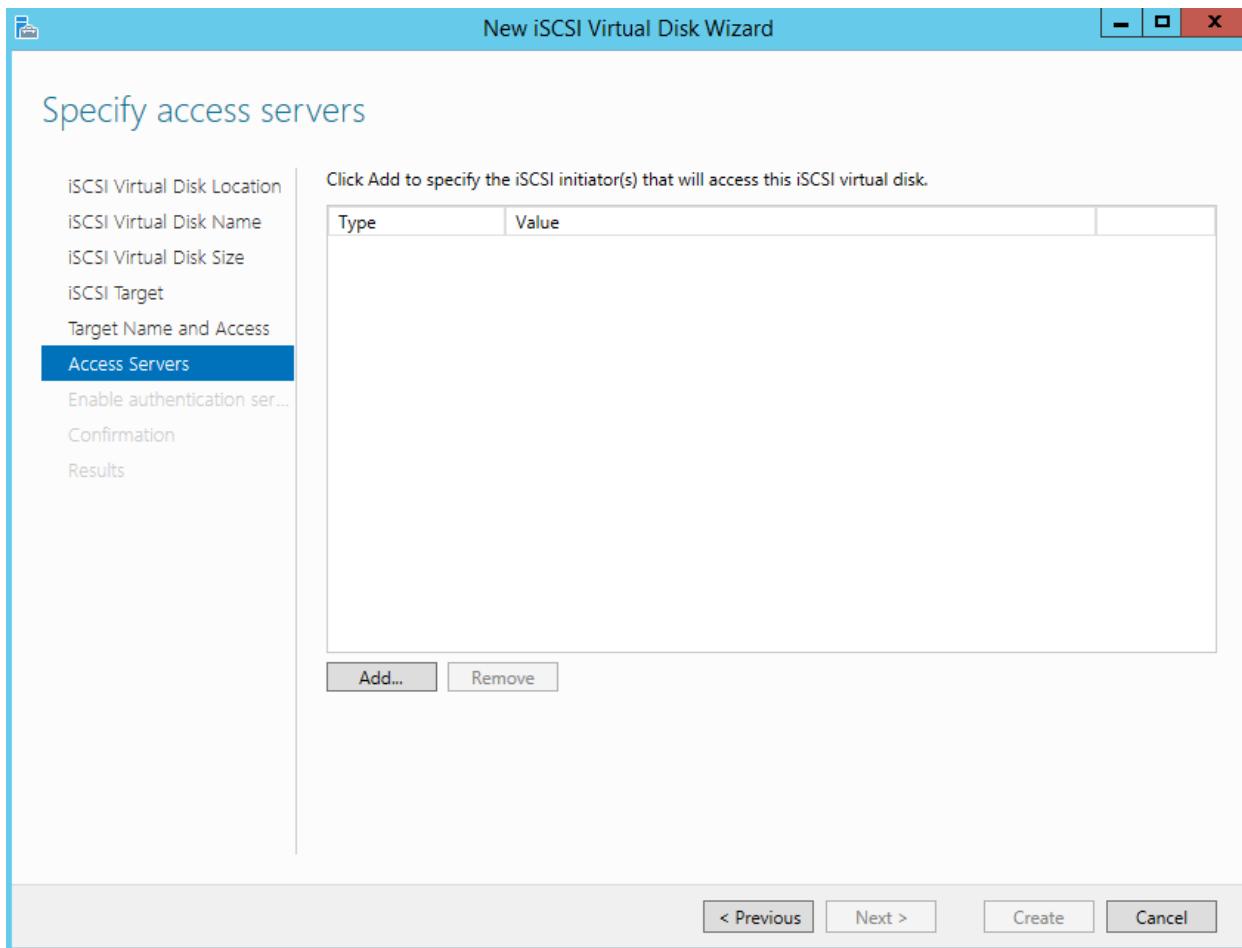
- Tại cửa sổ **Assign iSCSI target**, kiểm tra lựa chọn **New iSCSI target**, click vào **Next**.



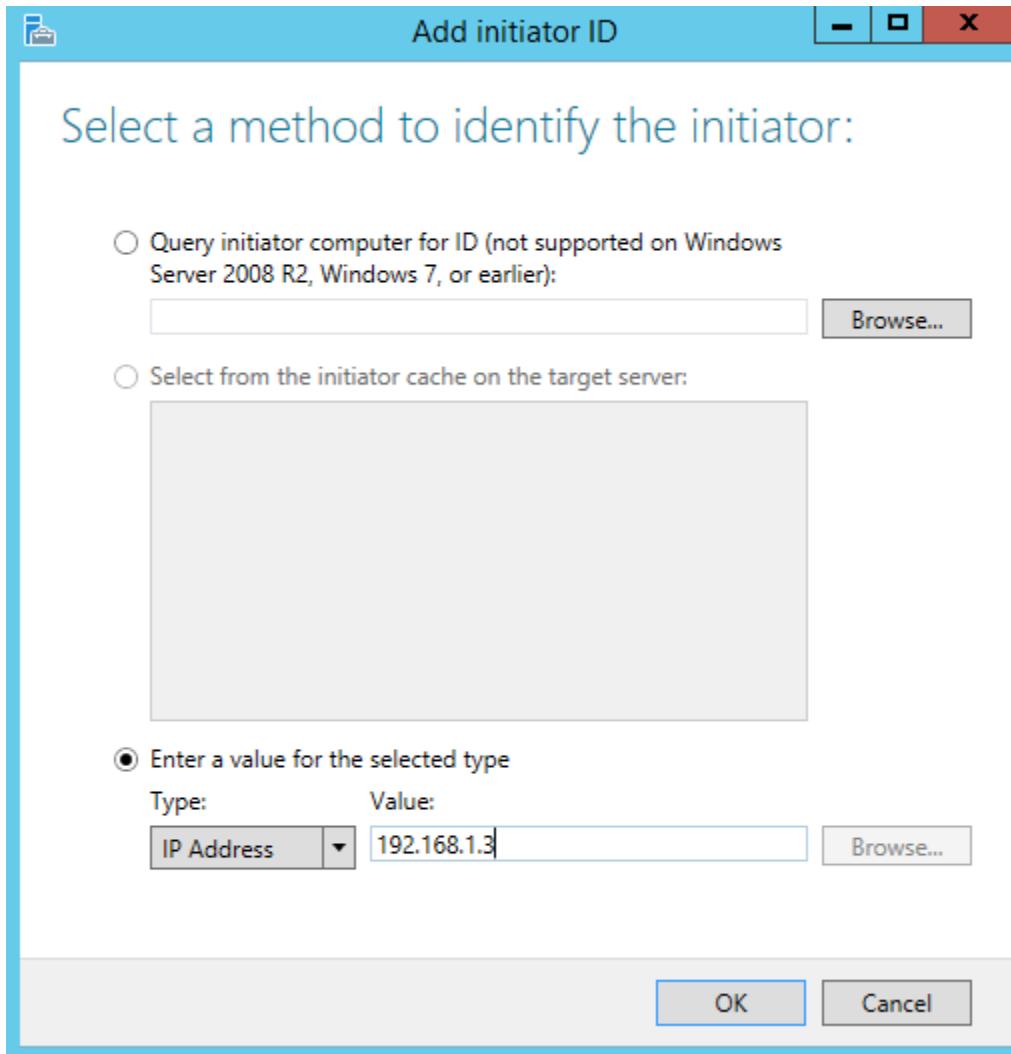
- Tại cửa sổ **Specify target name**, nhập vào tại mục *Name*: **VirtualDiskTarget**, click vào **Next**.



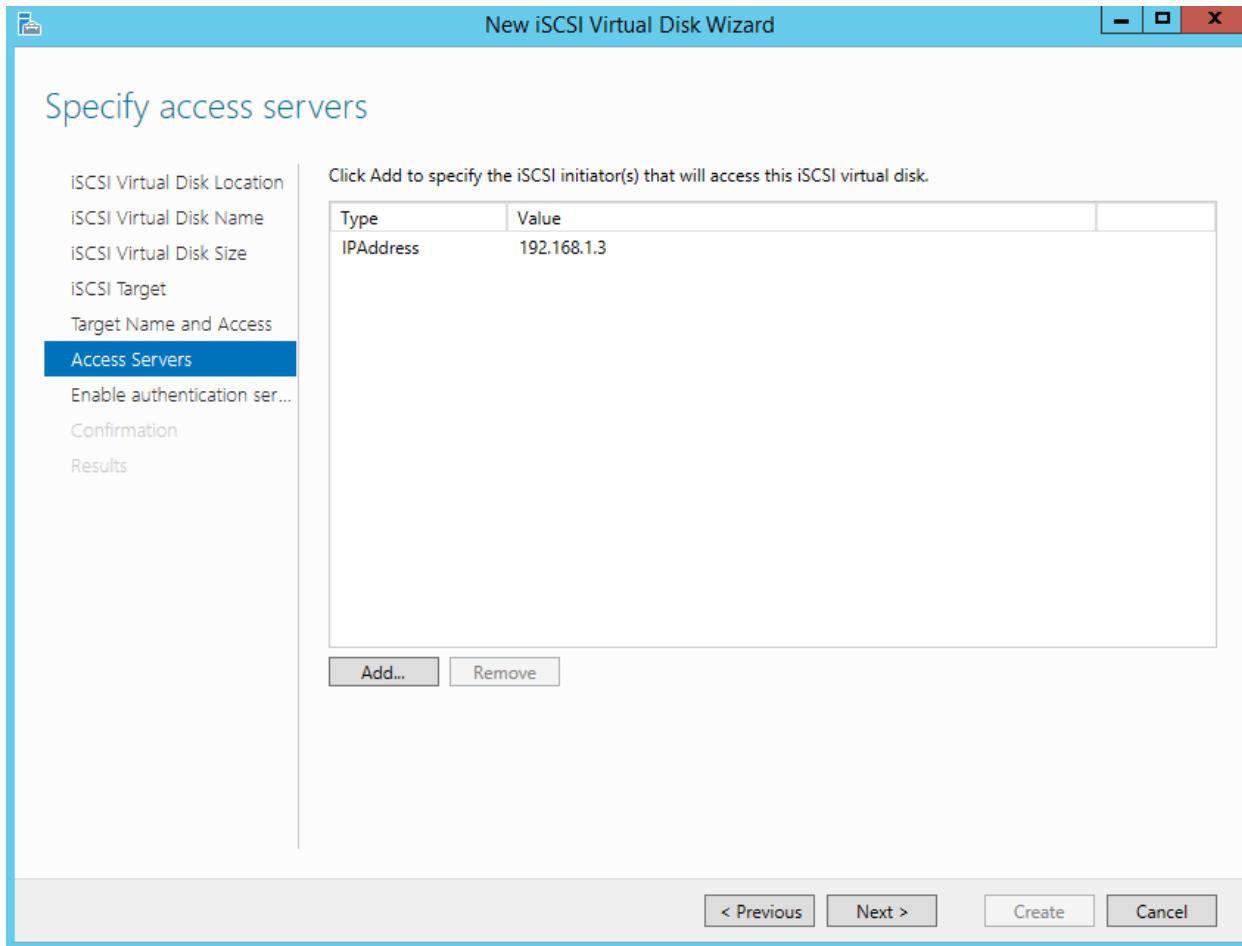
- Tại cửa sổ **Specify access servers**, click vào **Add...**



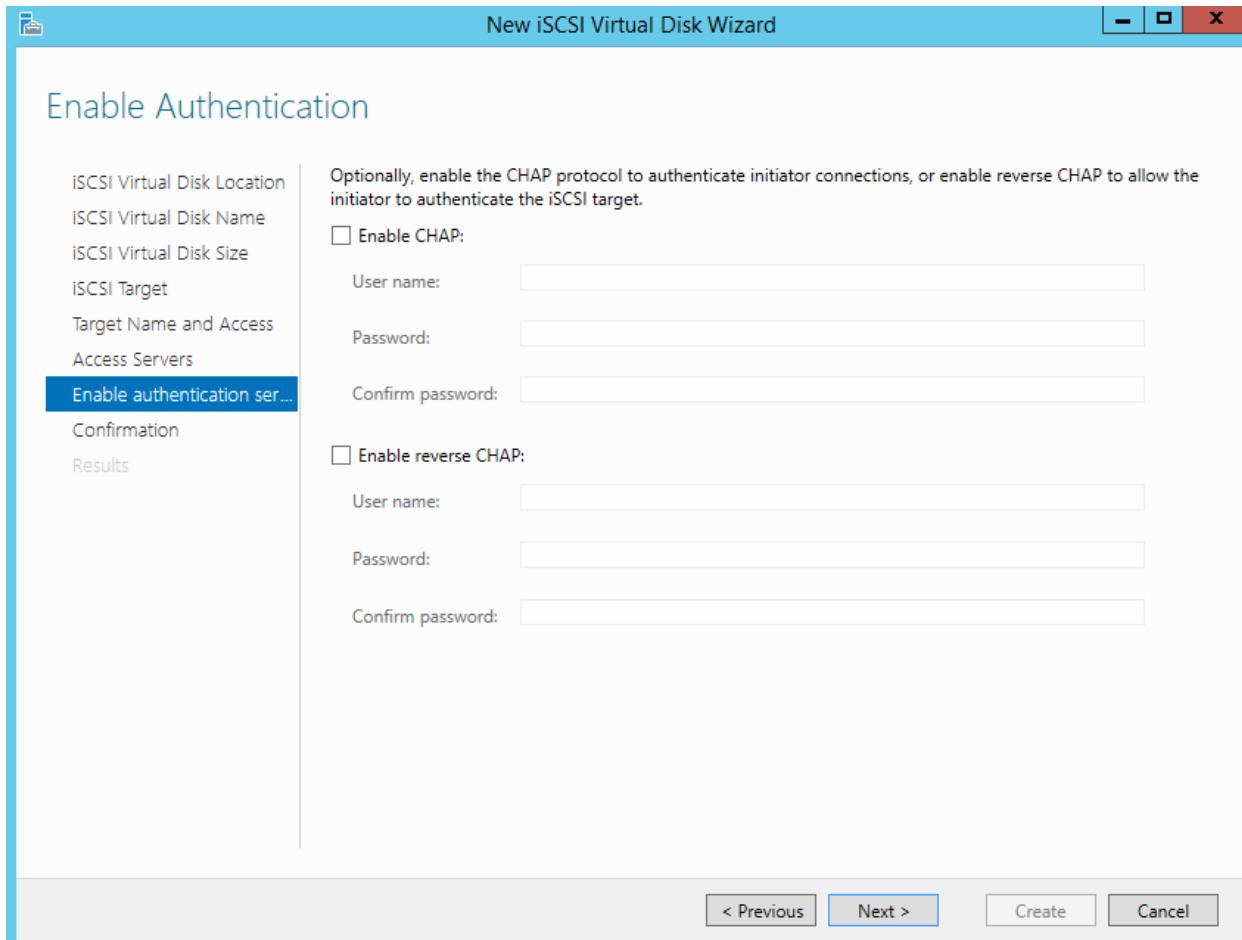
- Tại cửa sổ **Add initiator ID**, tại mục **Type**, chọn vào **IP Address**, tại mục **Value** nhập vào : **192.168.1.3**, click vào **OK**.



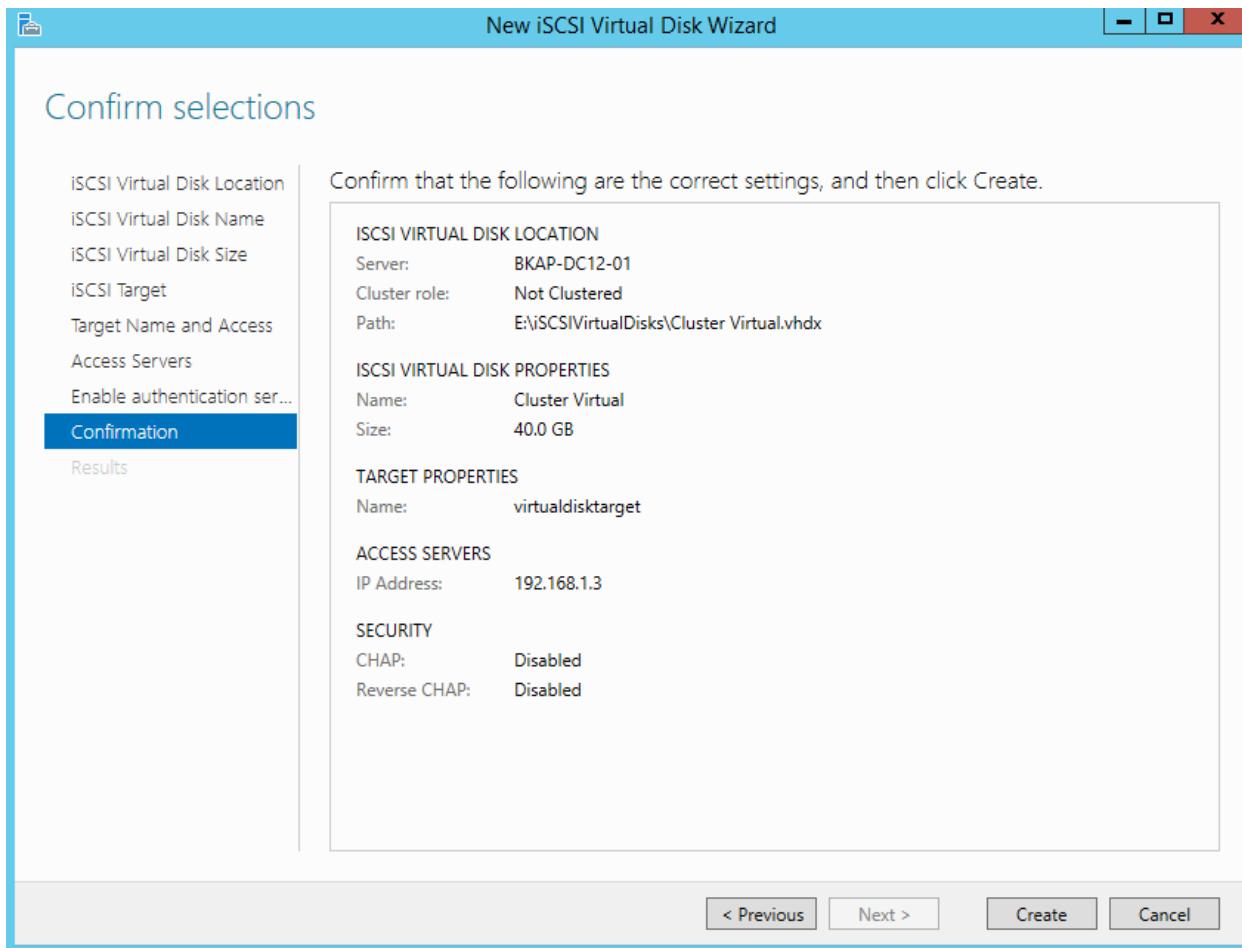
- Click vào **Next** tại cửa sổ **New iSCSI Virtual Disk Wizard**.



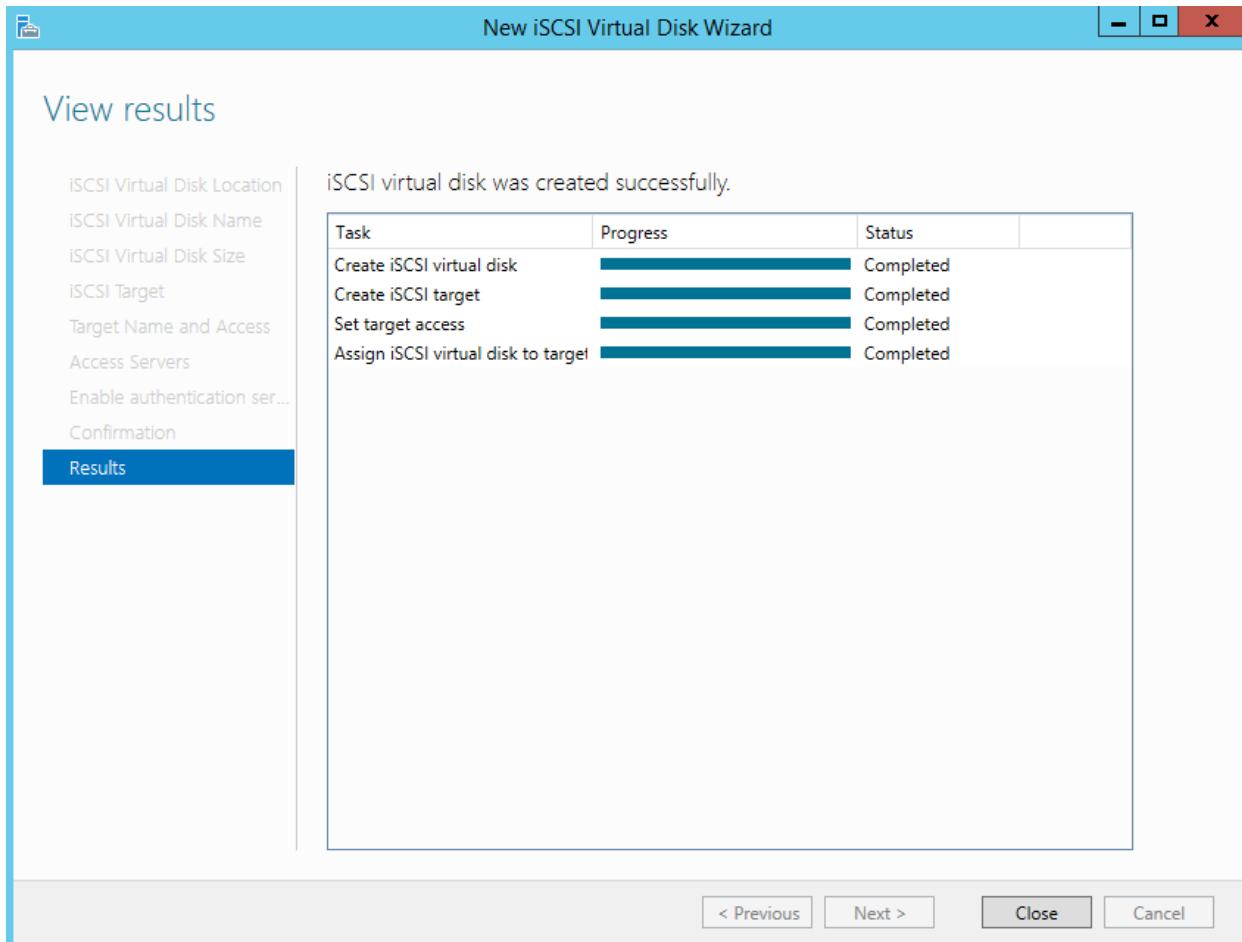
- Tại cửa sổ **Enable Authentication**, click vào **Next**.



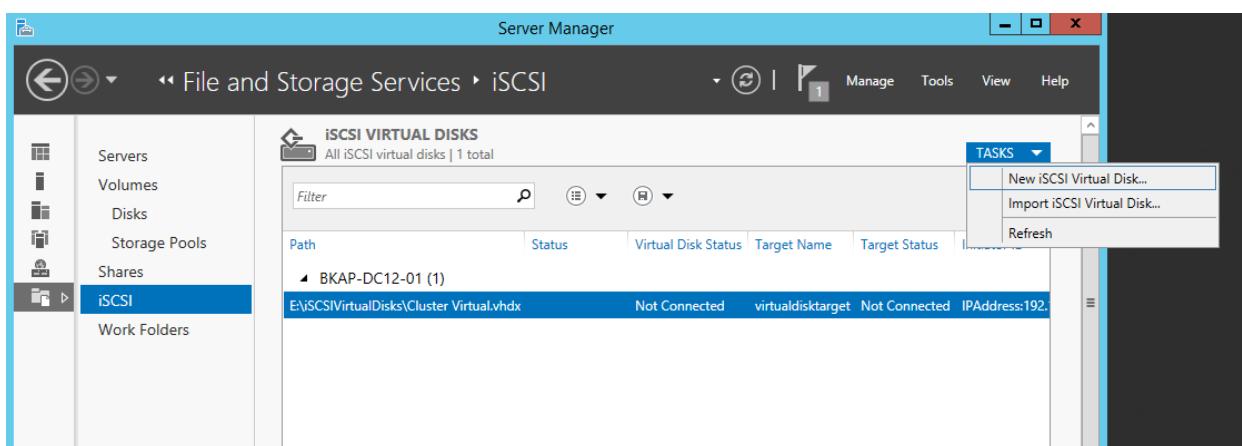
- Tại cửa sổ **Confirm selections**, click vào **Create**.



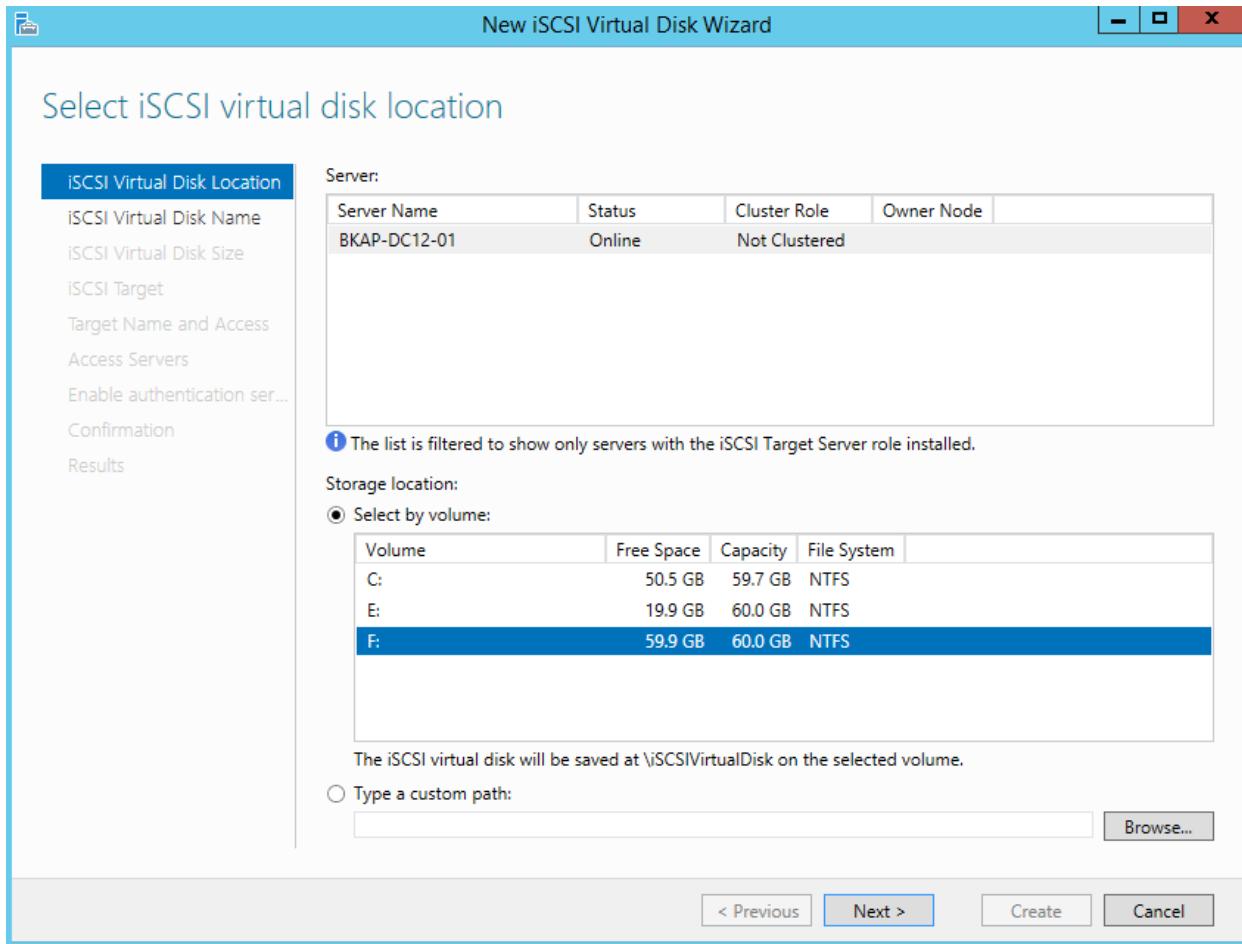
- Tại cửa sổ **View results**, kiểm tra kết quả, click vào **Close**.



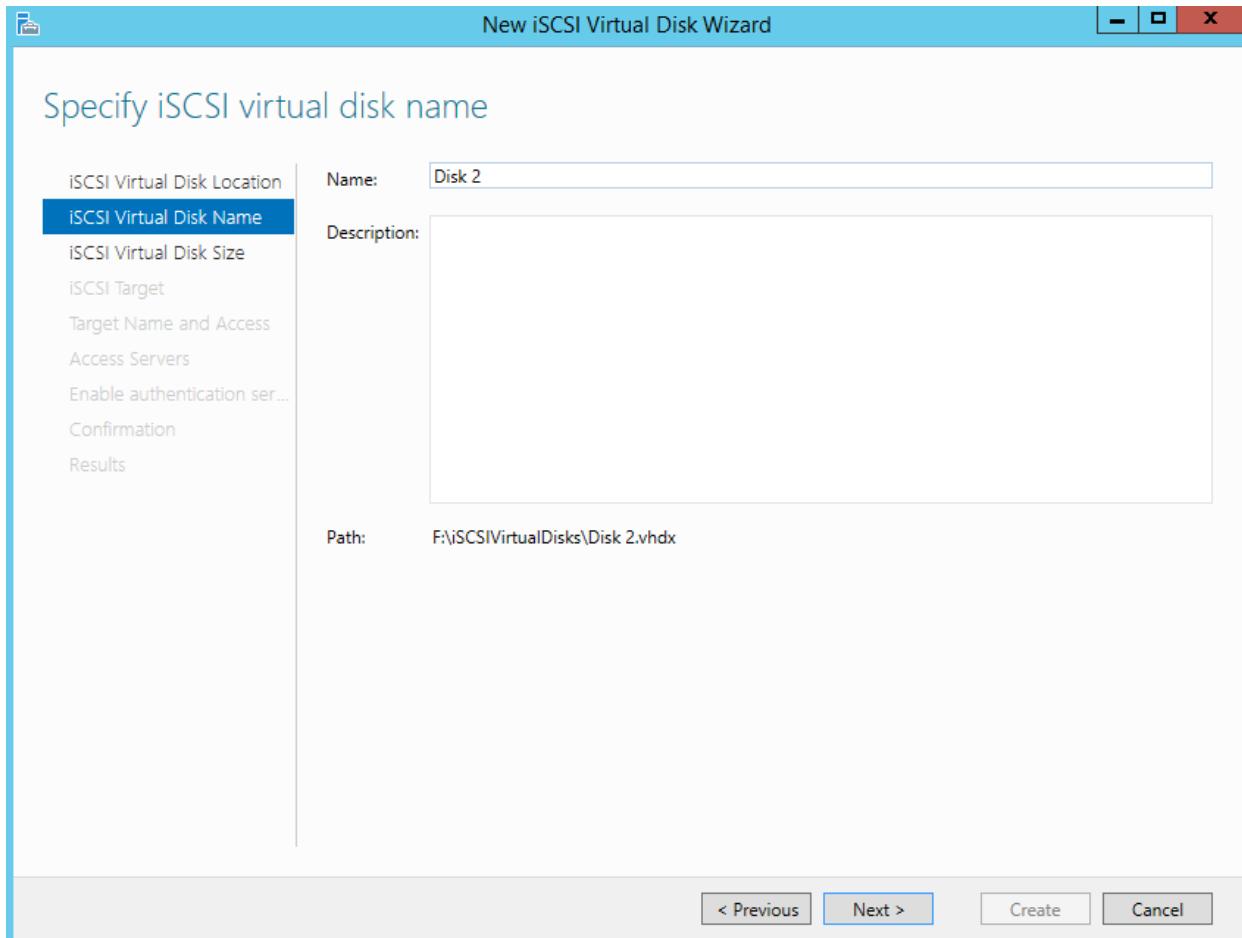
- Tại cửa sổ **iSCSI VIRTUAL DISKS**, click vào **TASKS / New iSCSI Virtual Disk...**



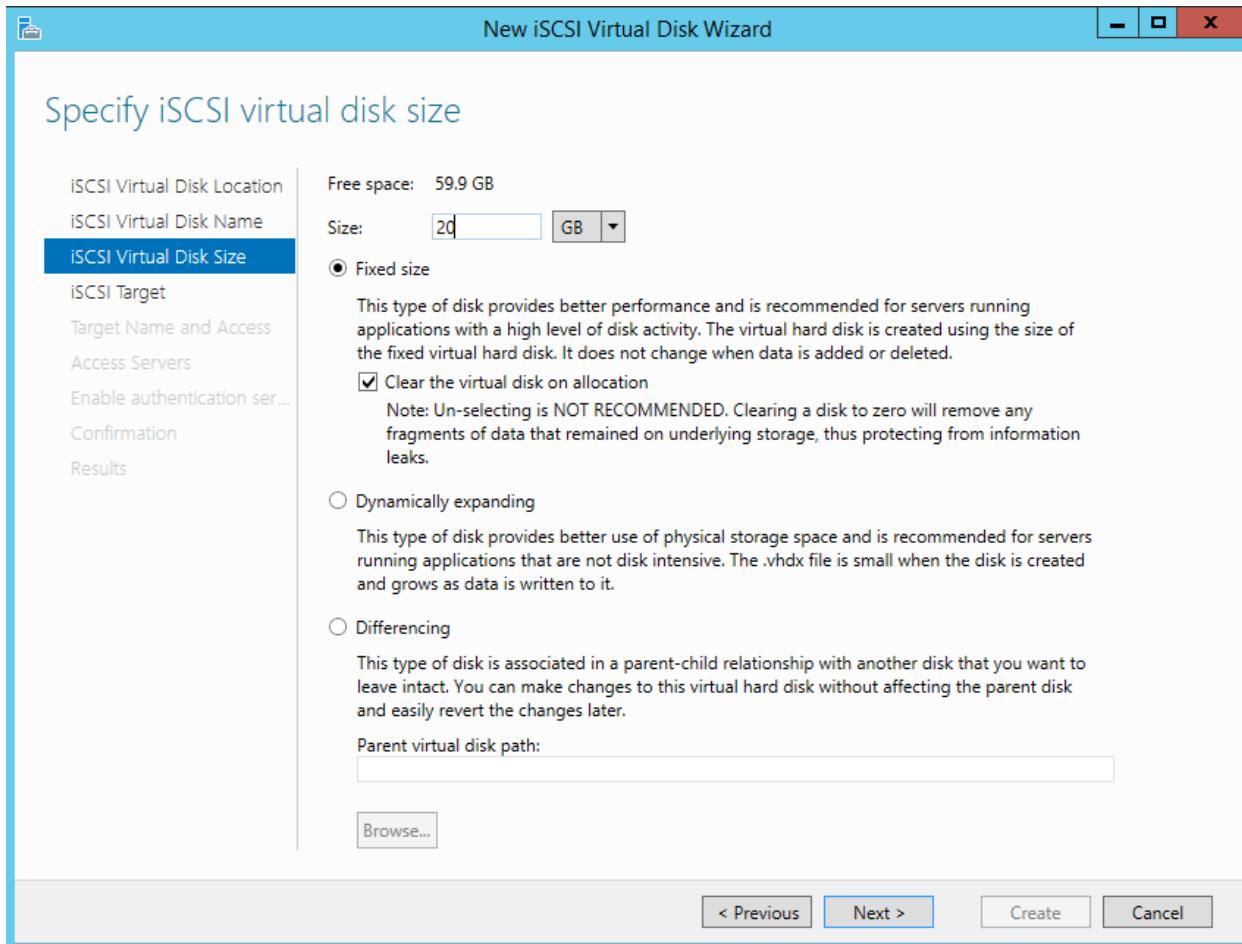
- Tại cửa sổ **Select iSCSI virtual disk location**, click chọn vào ô F, click vào **Next**.



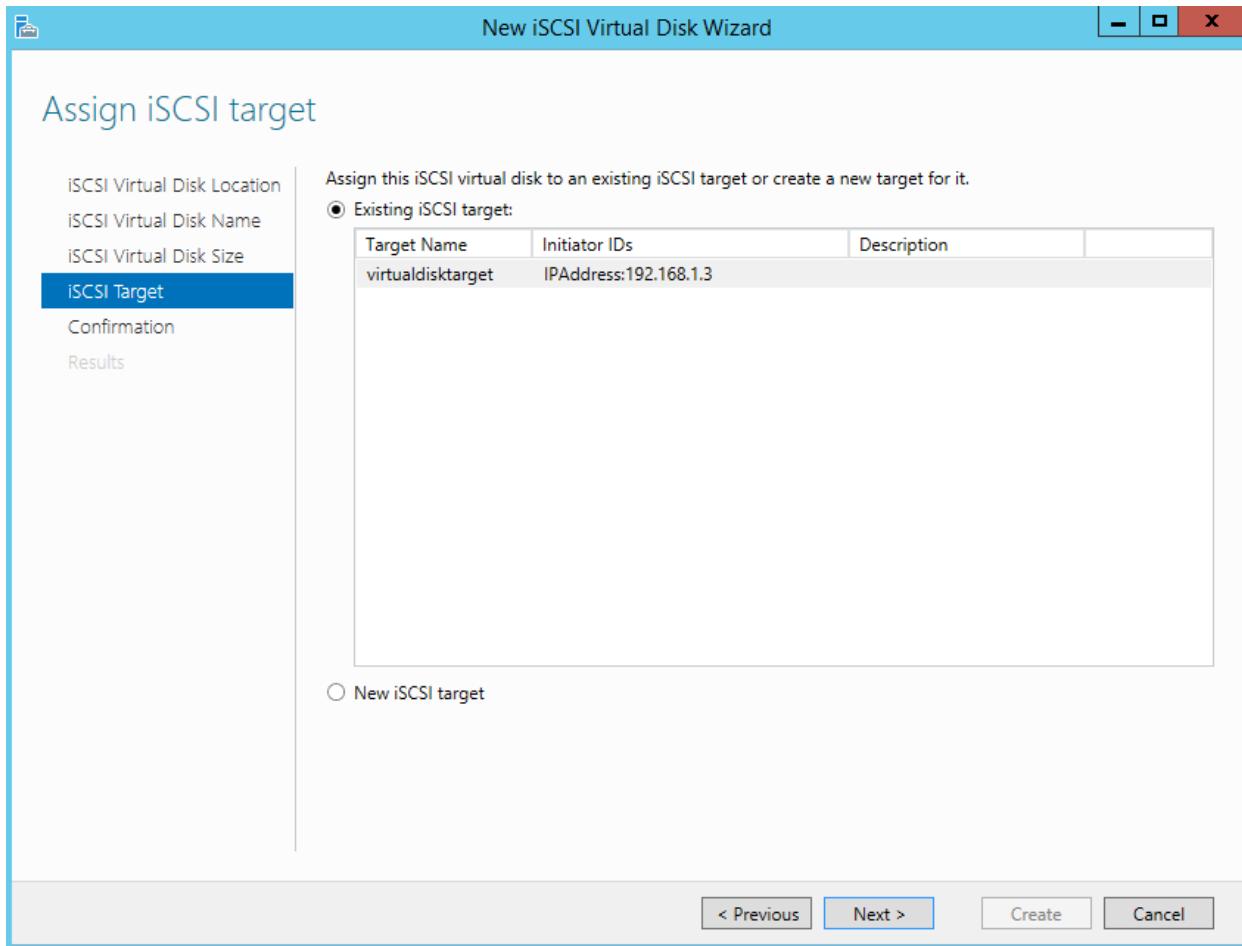
- Tại cửa sổ **Specify iSCSI virtual disk name**, nhập vào tại mục **Name: Disk 2**, click vào **Next**.



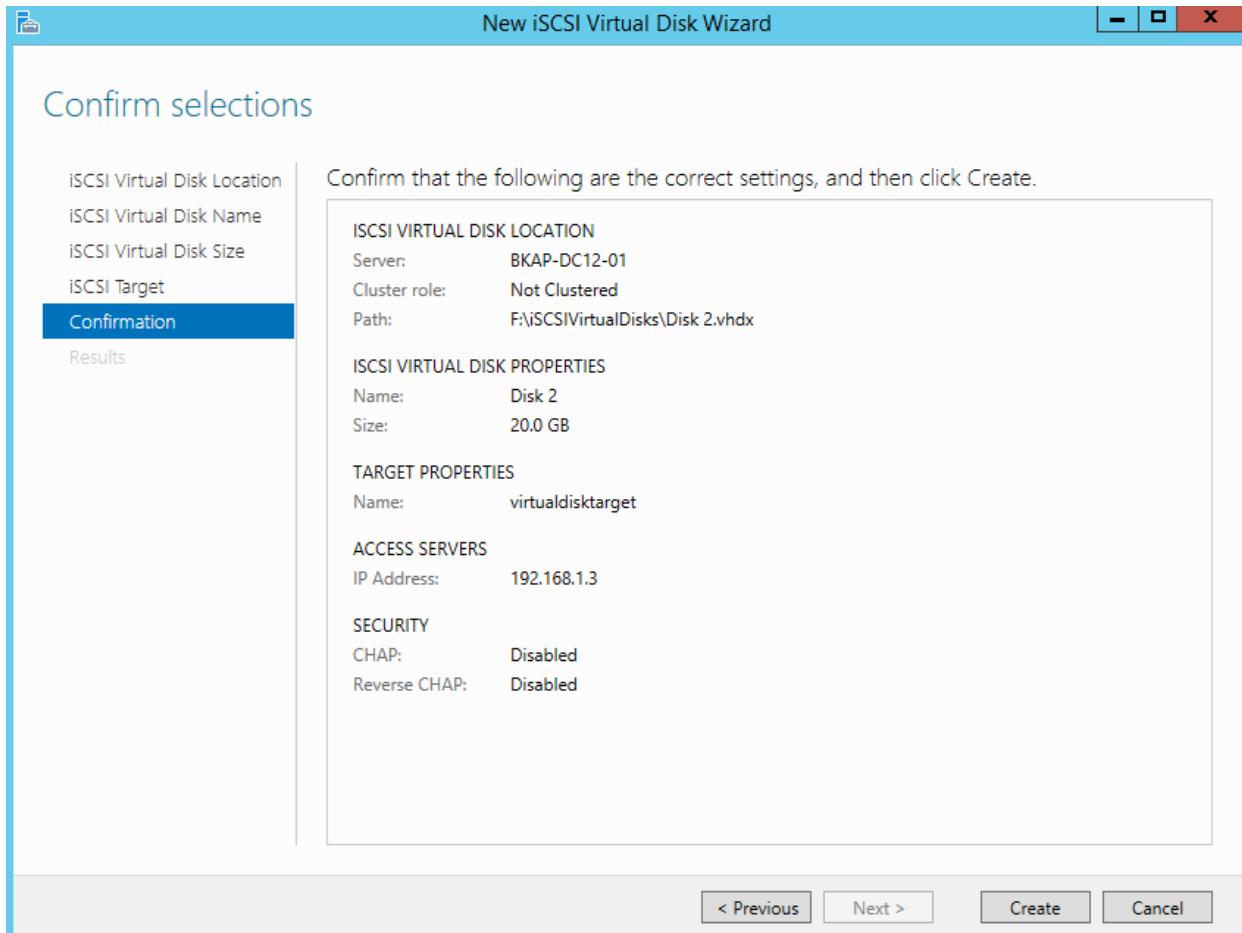
- Tại cửa sổ **Specify iSCSI virtual disk size**, nhập vào tại mục **Size: 20 GB** , click vào **Next**.



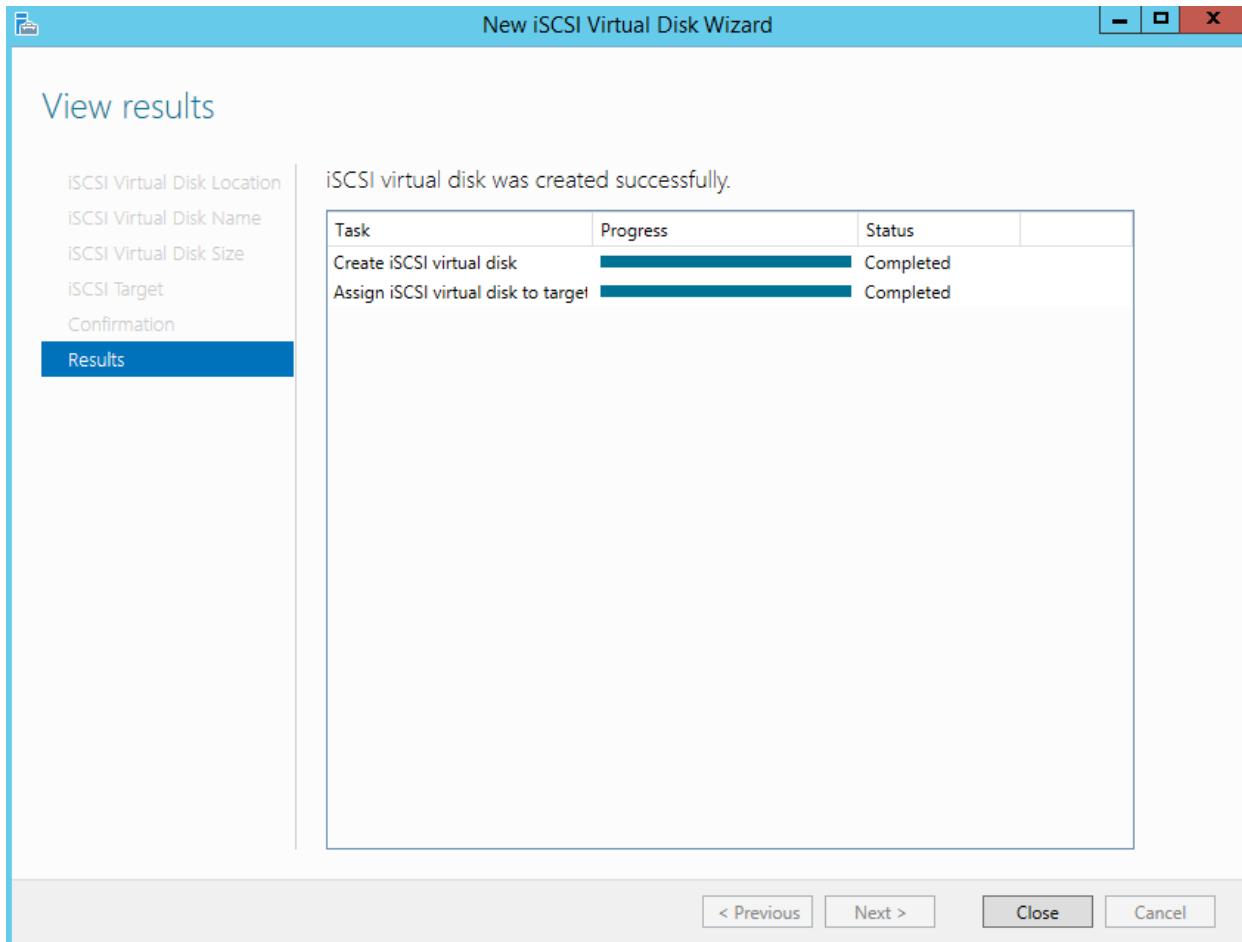
- Tại cửa sổ **Assign iSCSI target**, click vào **Next**.



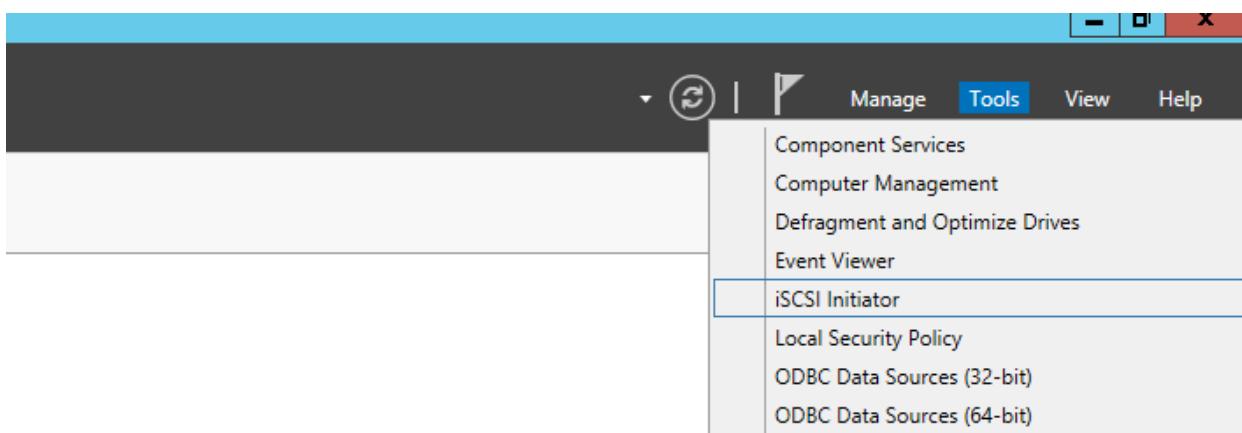
- Tại cửa sổ **Confirm selections**, click vào **Create**.



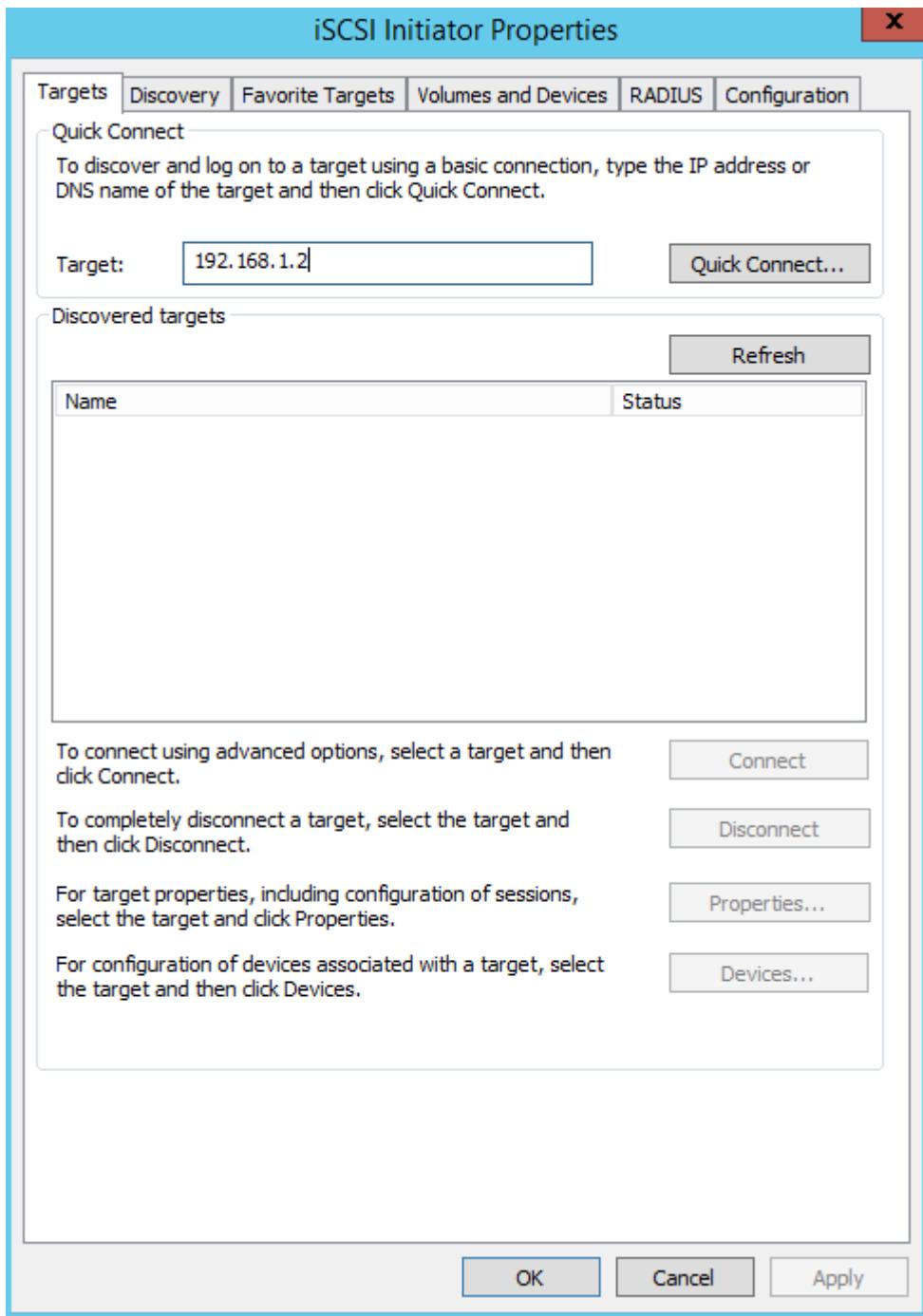
- Tại cửa sổ **View results**, kiểm tra kết quả, click vào **Close**.



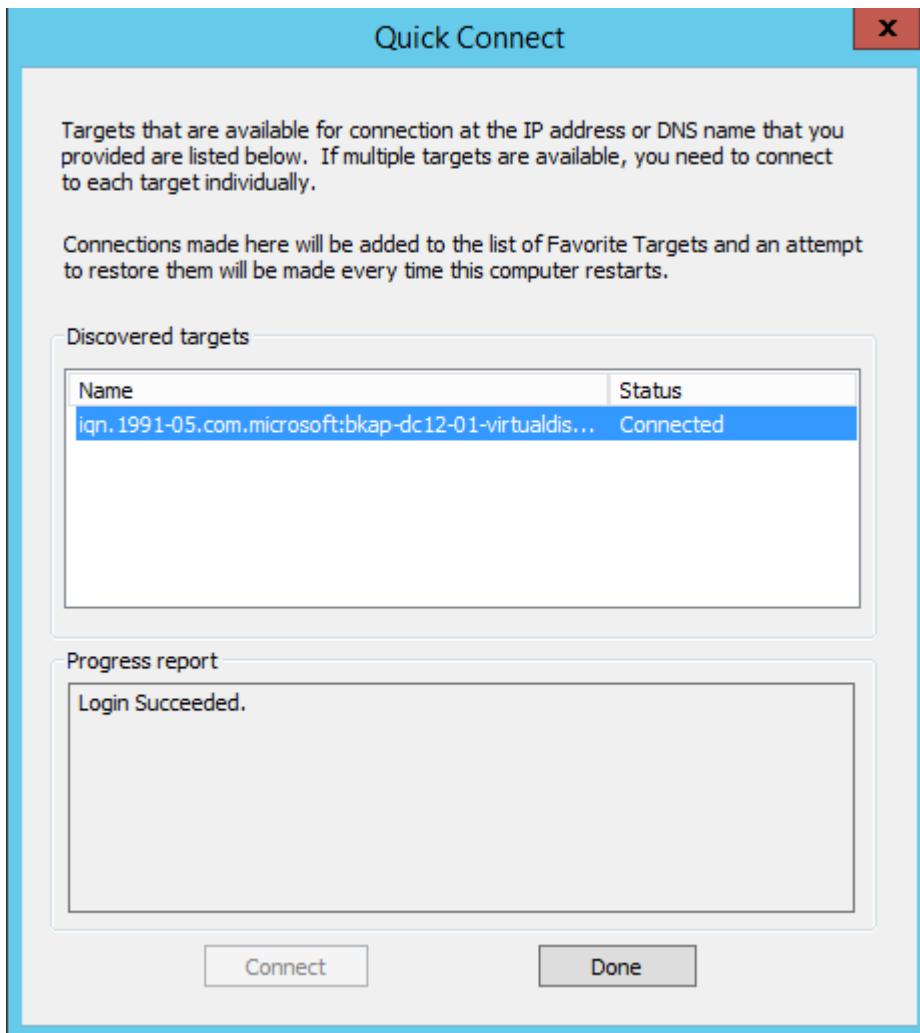
- Kết nối *BKAP-SRV12-01* đến **iSCSI Target**.
 - Vào **Server Manager / Tools / iSCSI Initiator**.



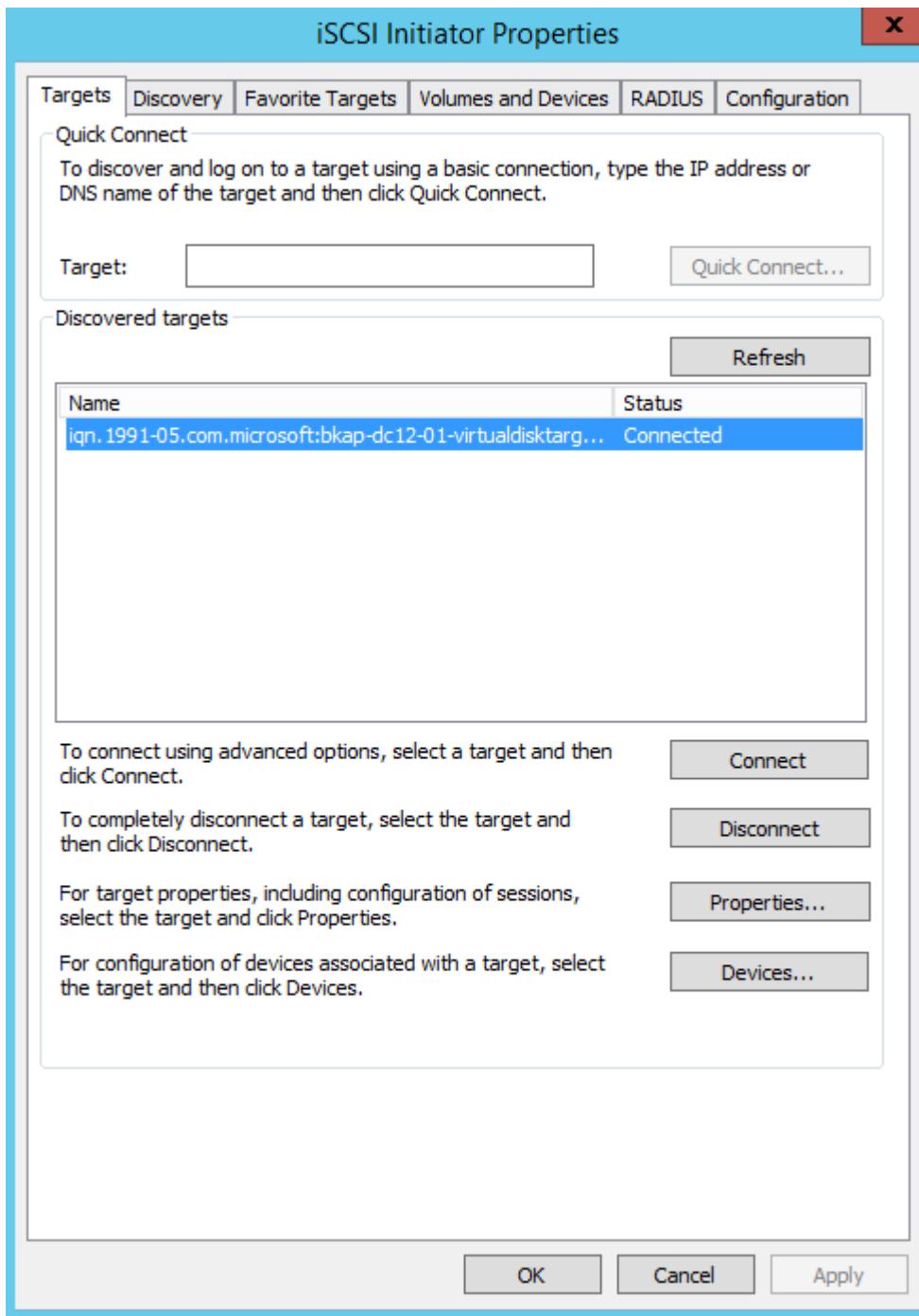
- Tại cửa sổ **iSCSI Initiator Properties**, trong Tab Targets, nhập vào tại mục **Target: 192.168.1.2**, click vào **Quick Connect...**



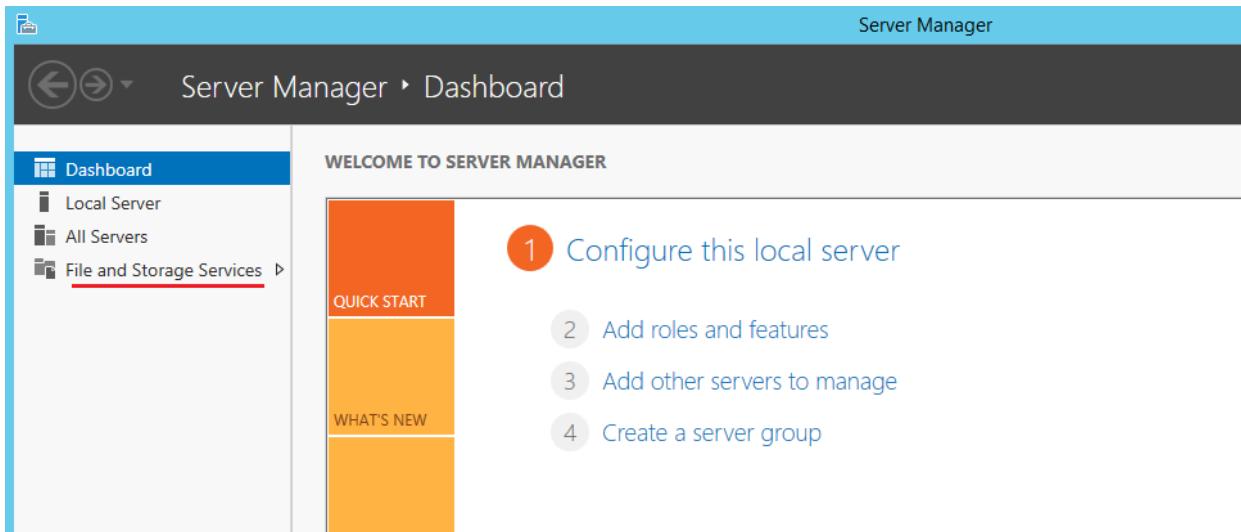
- Tại cửa sổ **Quick Connect**, click vào **Done**.



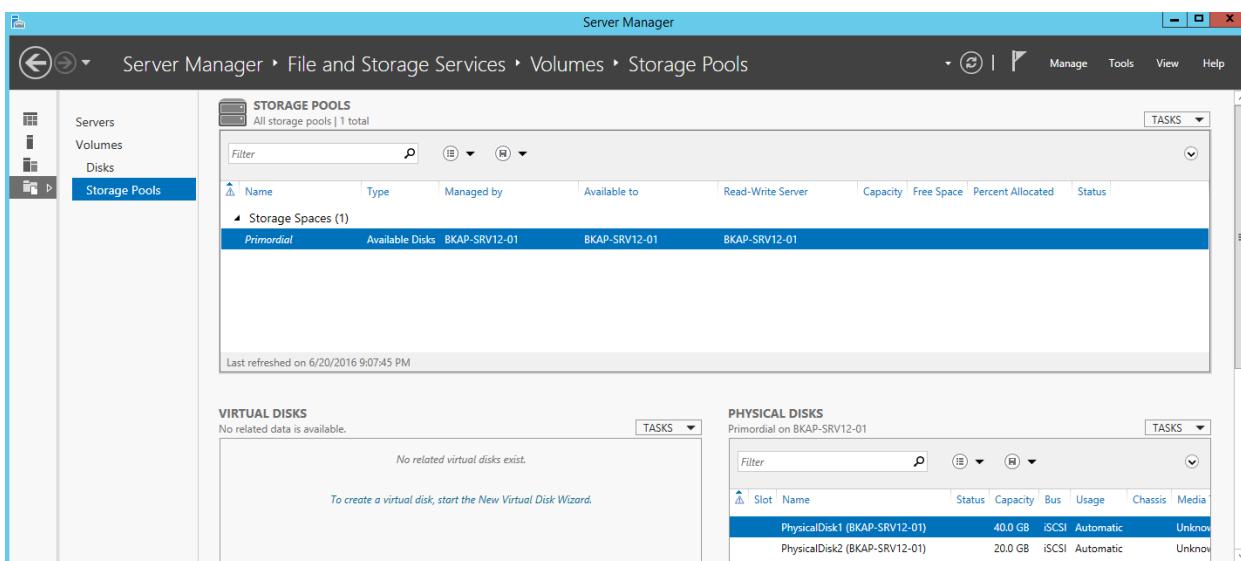
- Click vào **OK** tại cửa sổ iSCSI Initiator Properties.



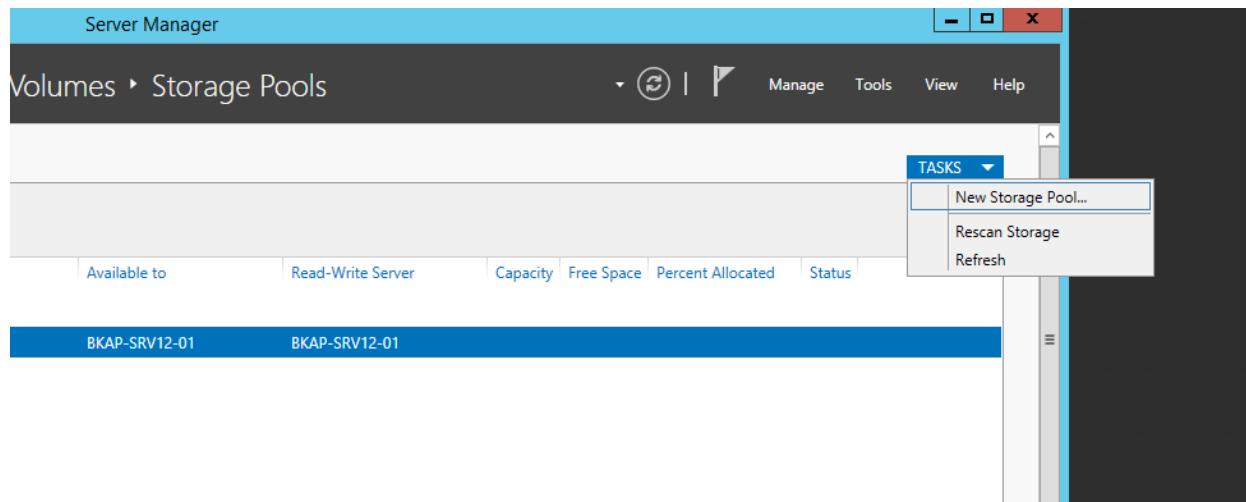
- Click vào **File and Storage Services** trong cửa sổ **Server Manager**.



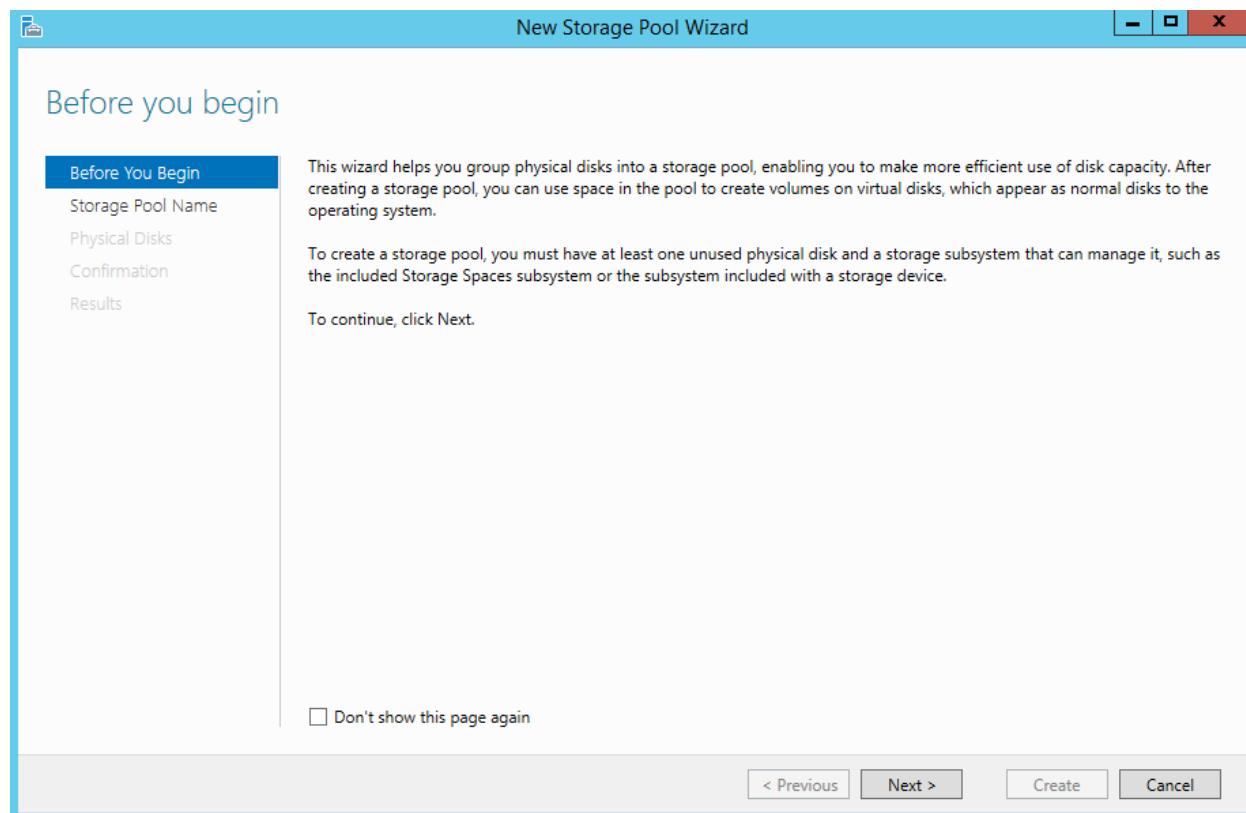
- Click chọn vào **Storage Pools**.



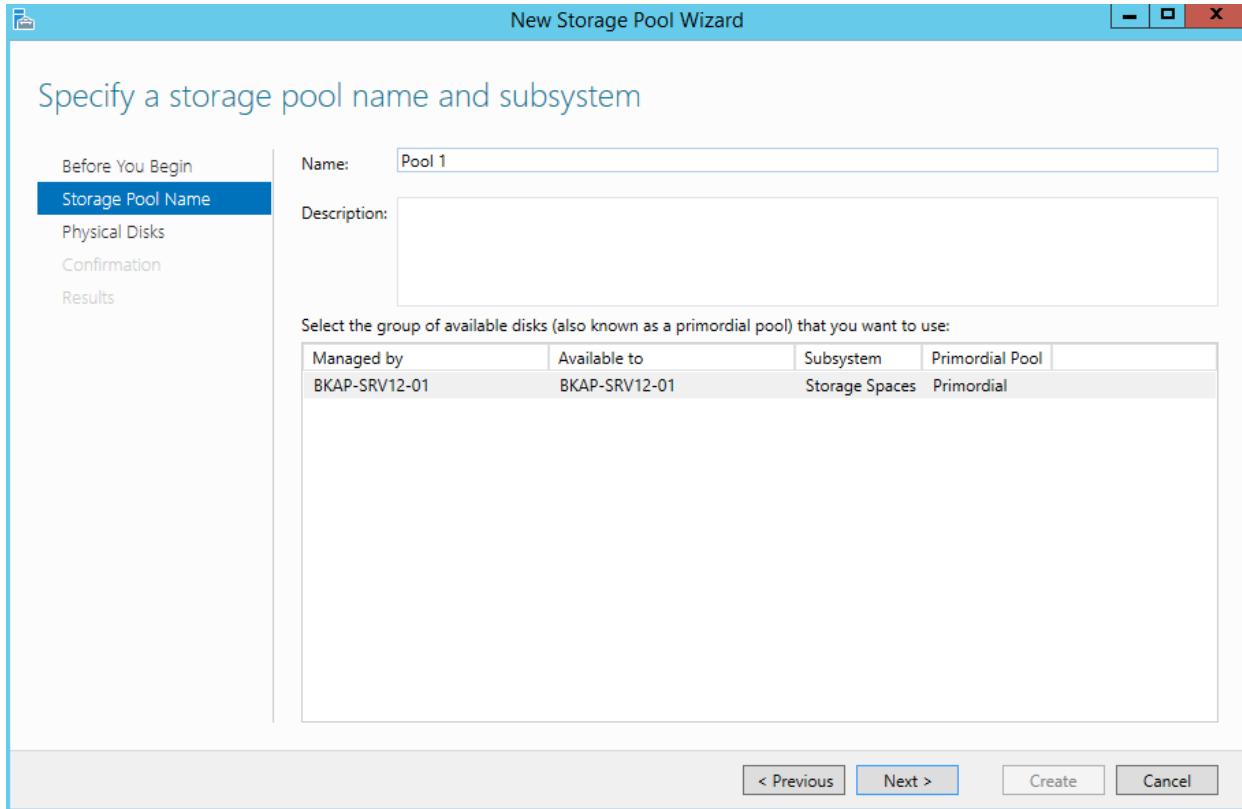
- Tạo Storage Pool: click vào **TASKS / New Storage Pool...**



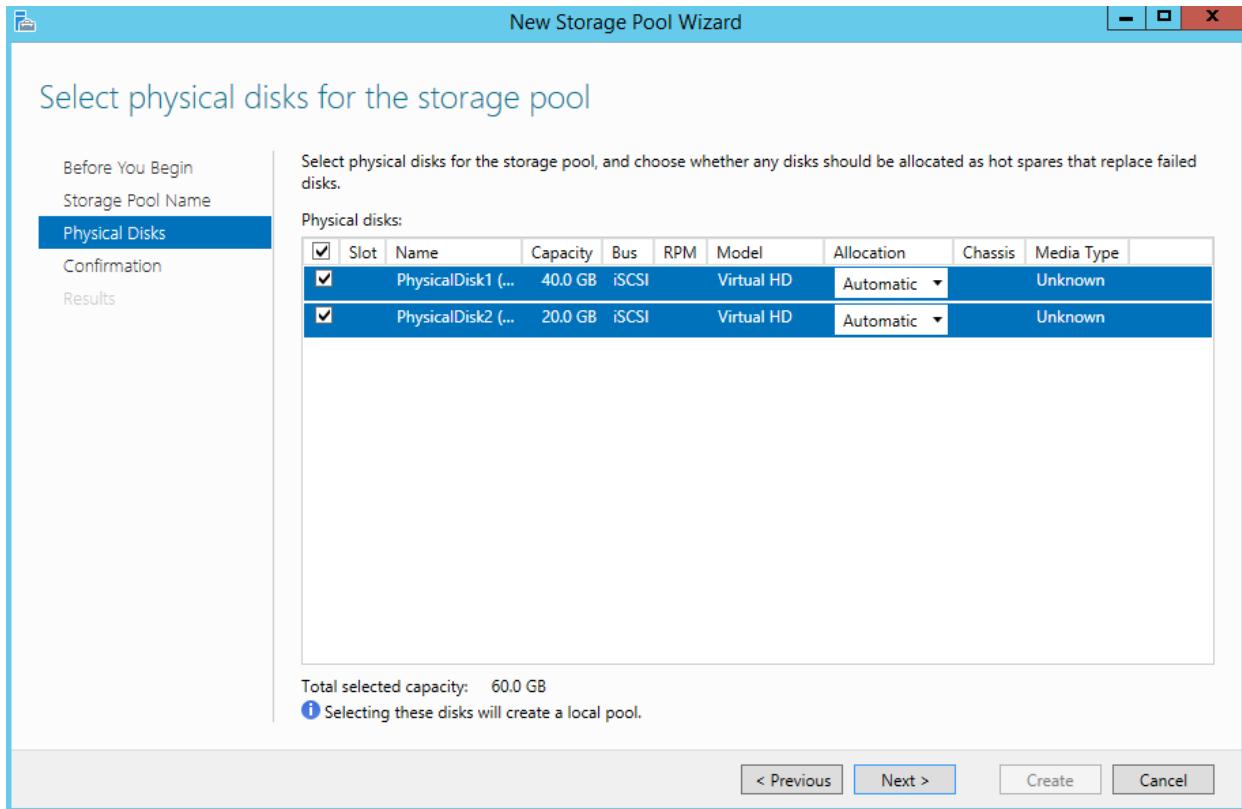
- Trong cửa sổ **Before you begin**, click vào **Next**.



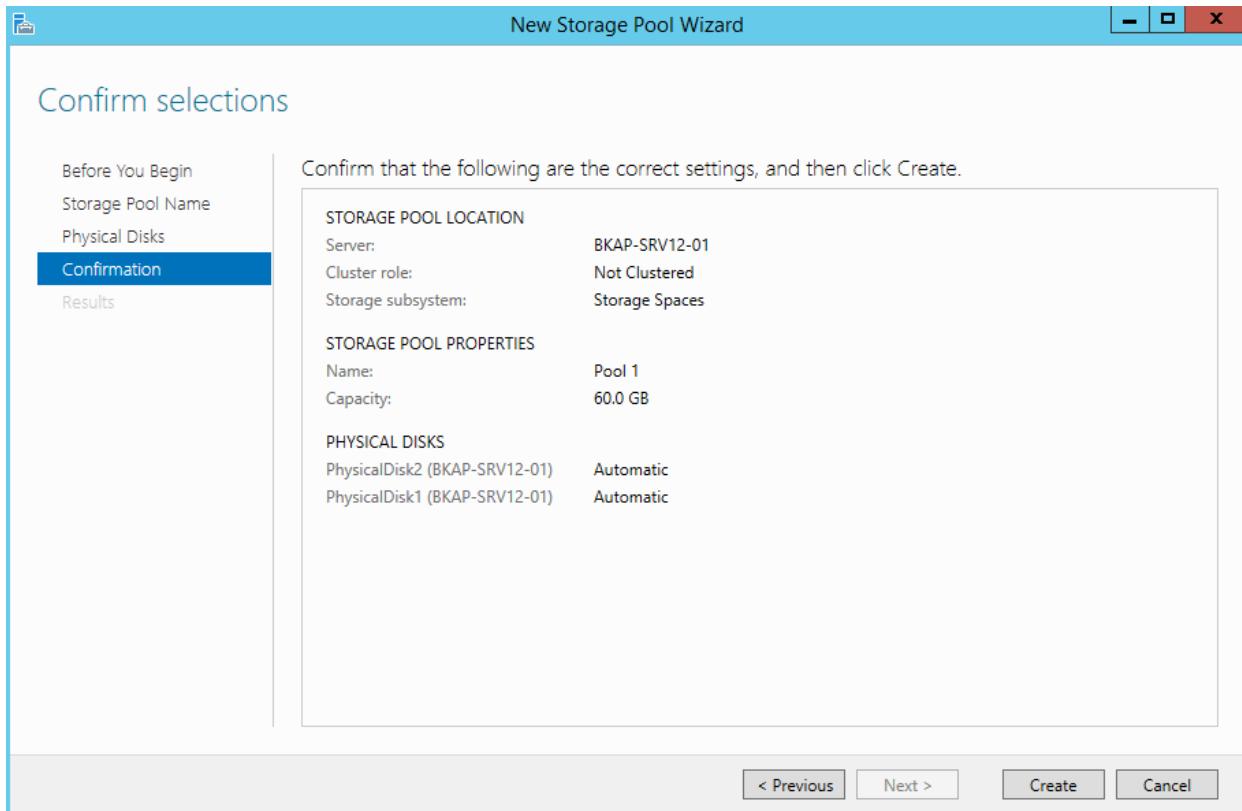
- Trong cửa sổ **Specify a storage pool name and subsystem**, nhập vào tại mục **Name: Pool 1**, Click vào **Next**.



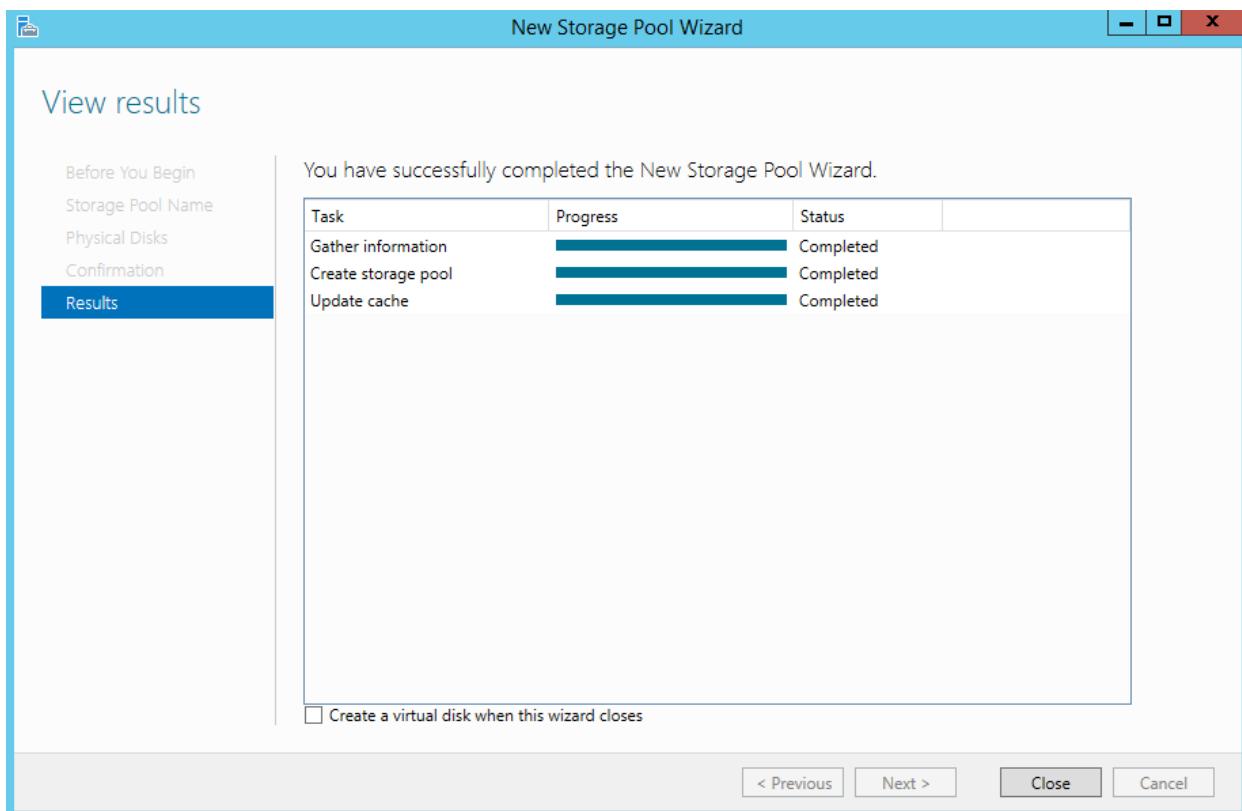
- Tại cửa sổ **Select physical disks for the storage pool**, chọn vào **2 Physical disks**, click vào **Next**.



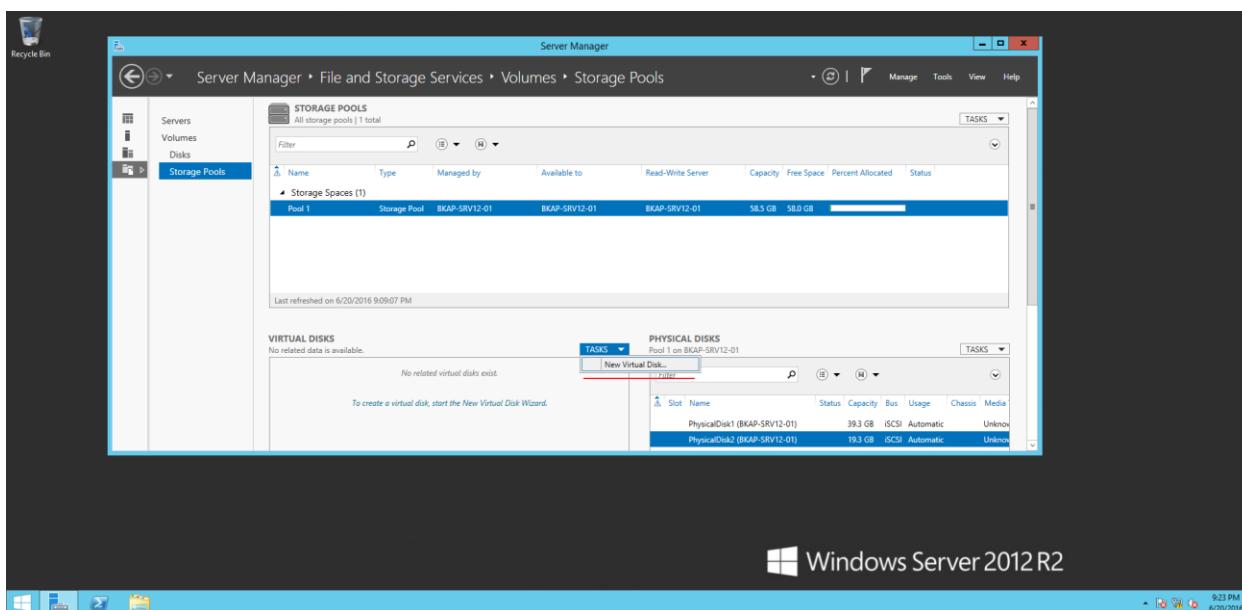
- Tại cửa sổ **Confirm selections**, click vào **Create**.



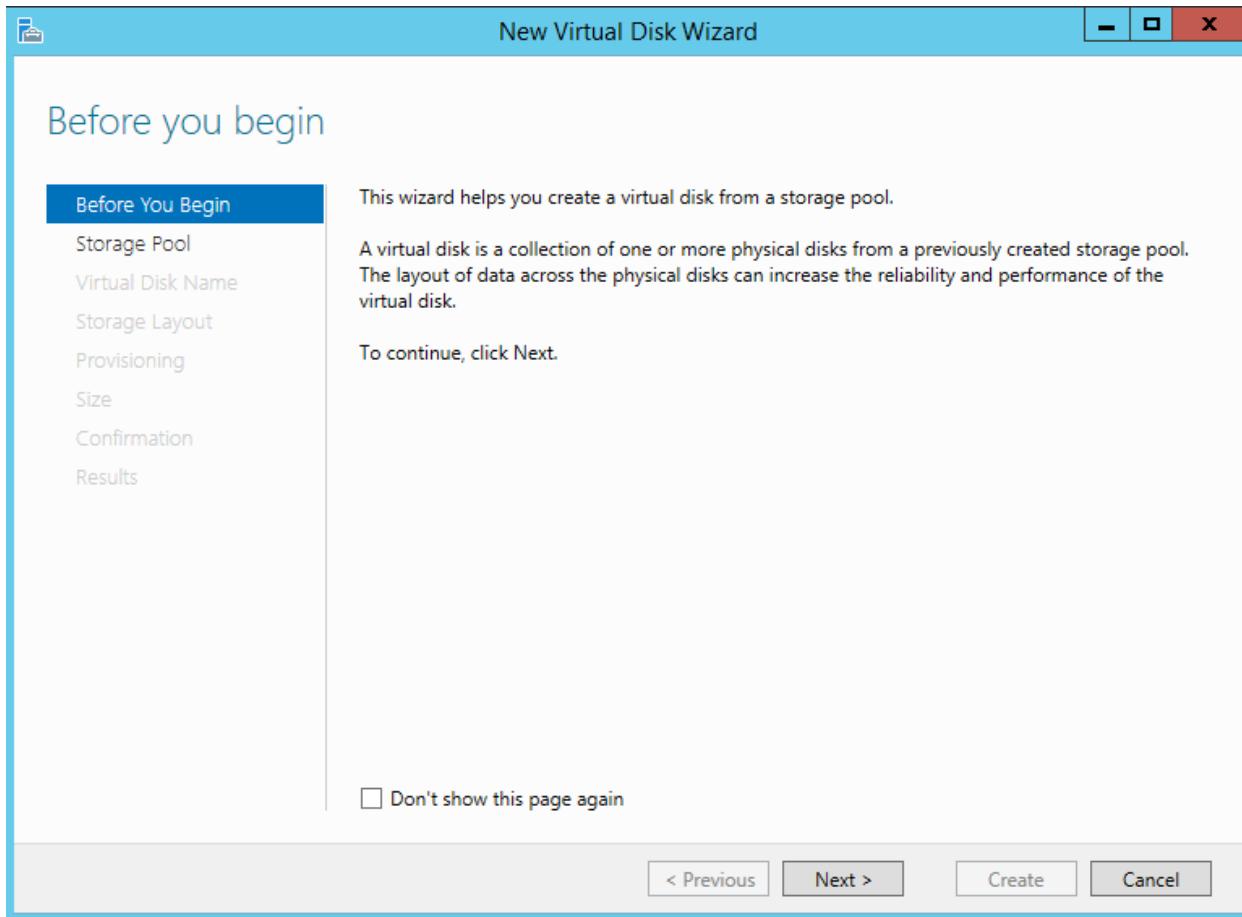
- Tại cửa sổ **View results**, kiểm tra kết quả, click vào **Close**.



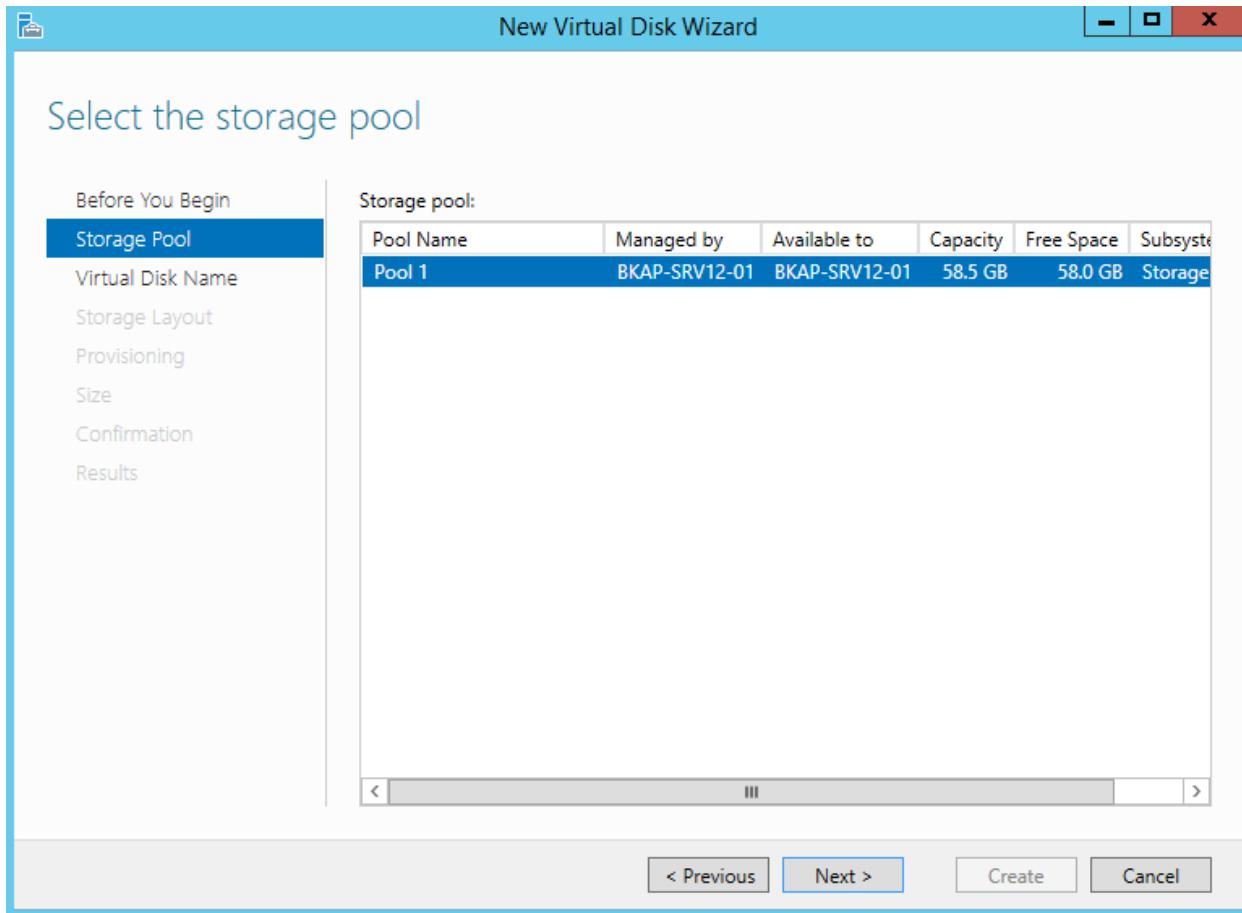
- Chọn vào **Storage Spaces Pool 1** vừa tạo, tại khung **VIRTUAL DISKS**, click chọn vào **TASKS / New Virtual Disk...**



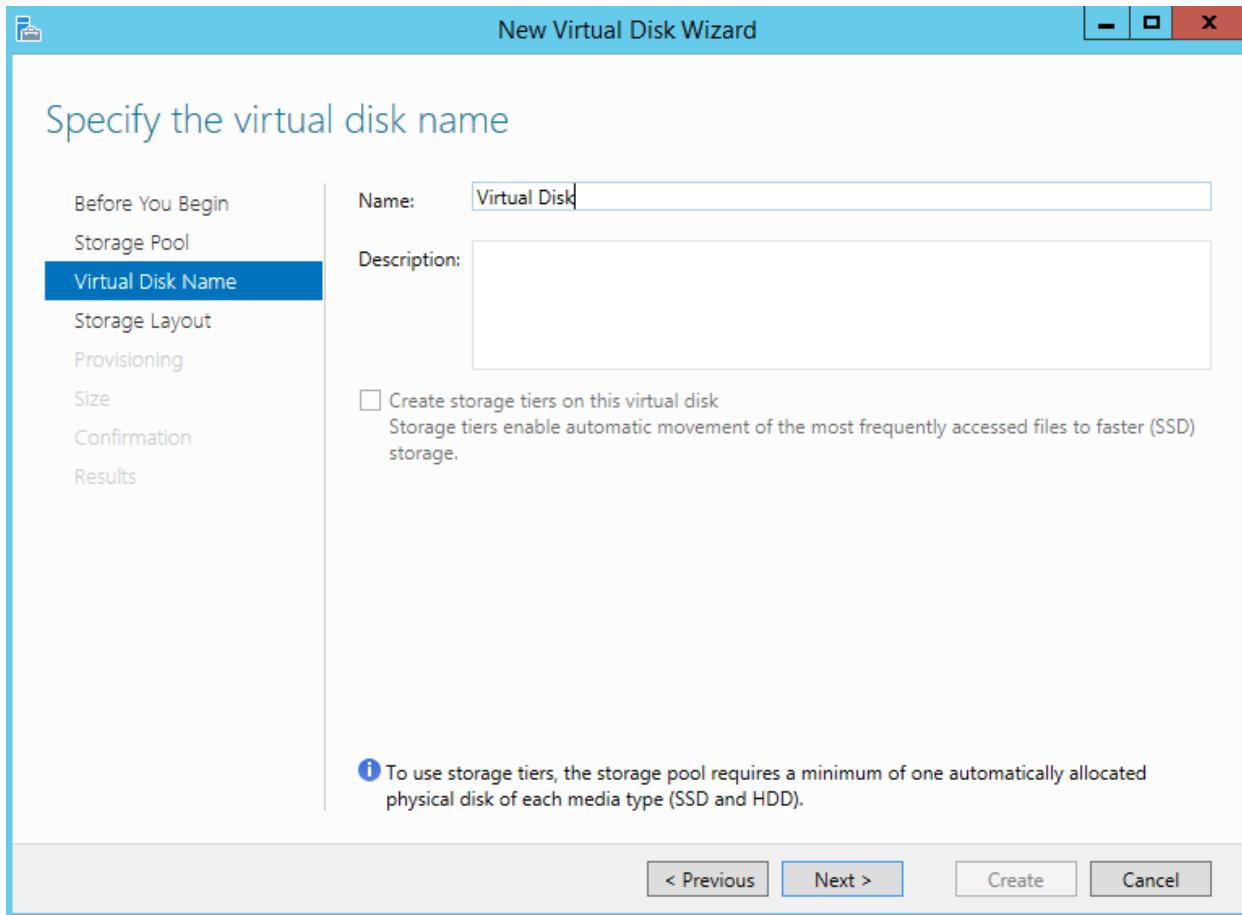
- Tại cửa sổ **Before you begin**, click vào **Next**.



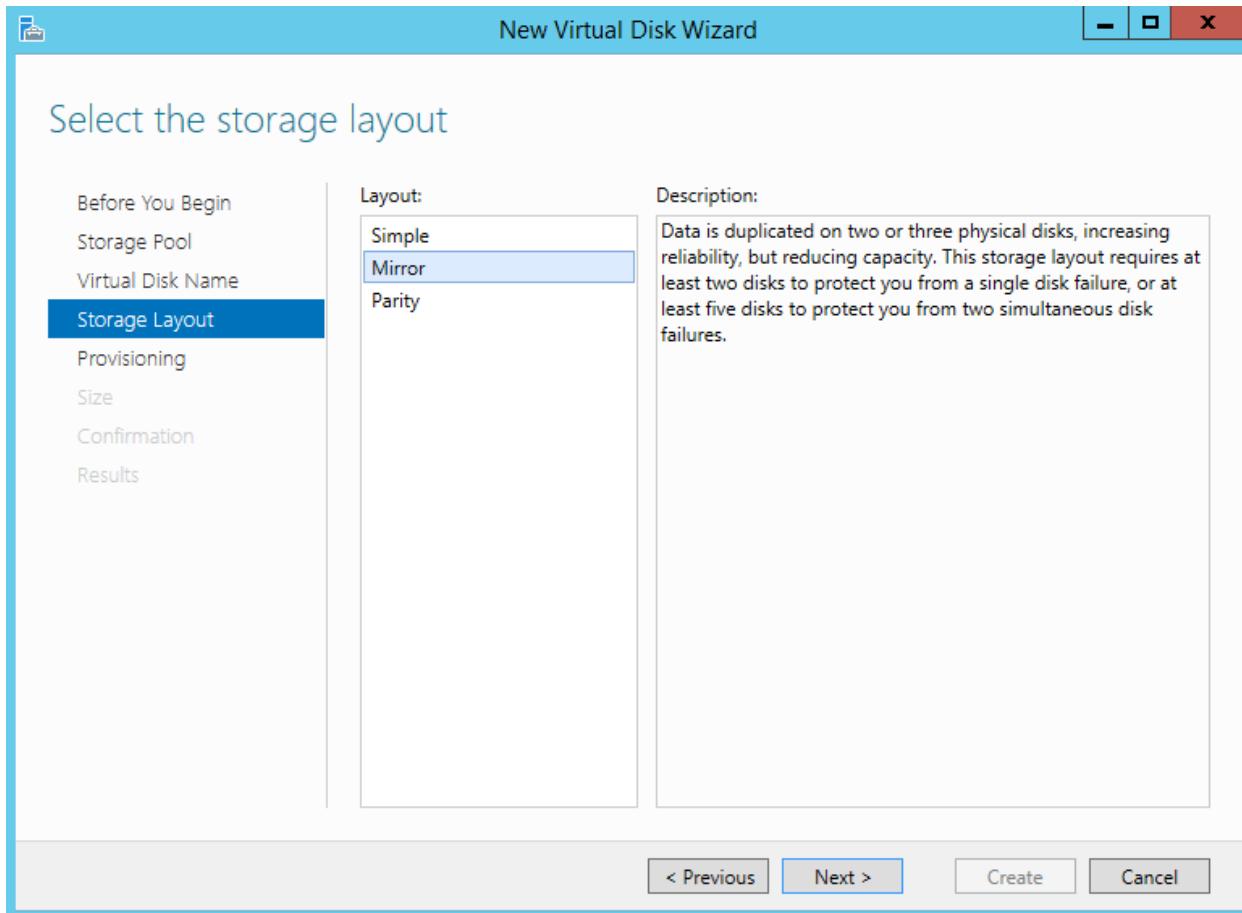
- Tại cửa sổ **Select the storage pool**, kiểm tra **Storage pool là Pool 1**, click vào **Next**.



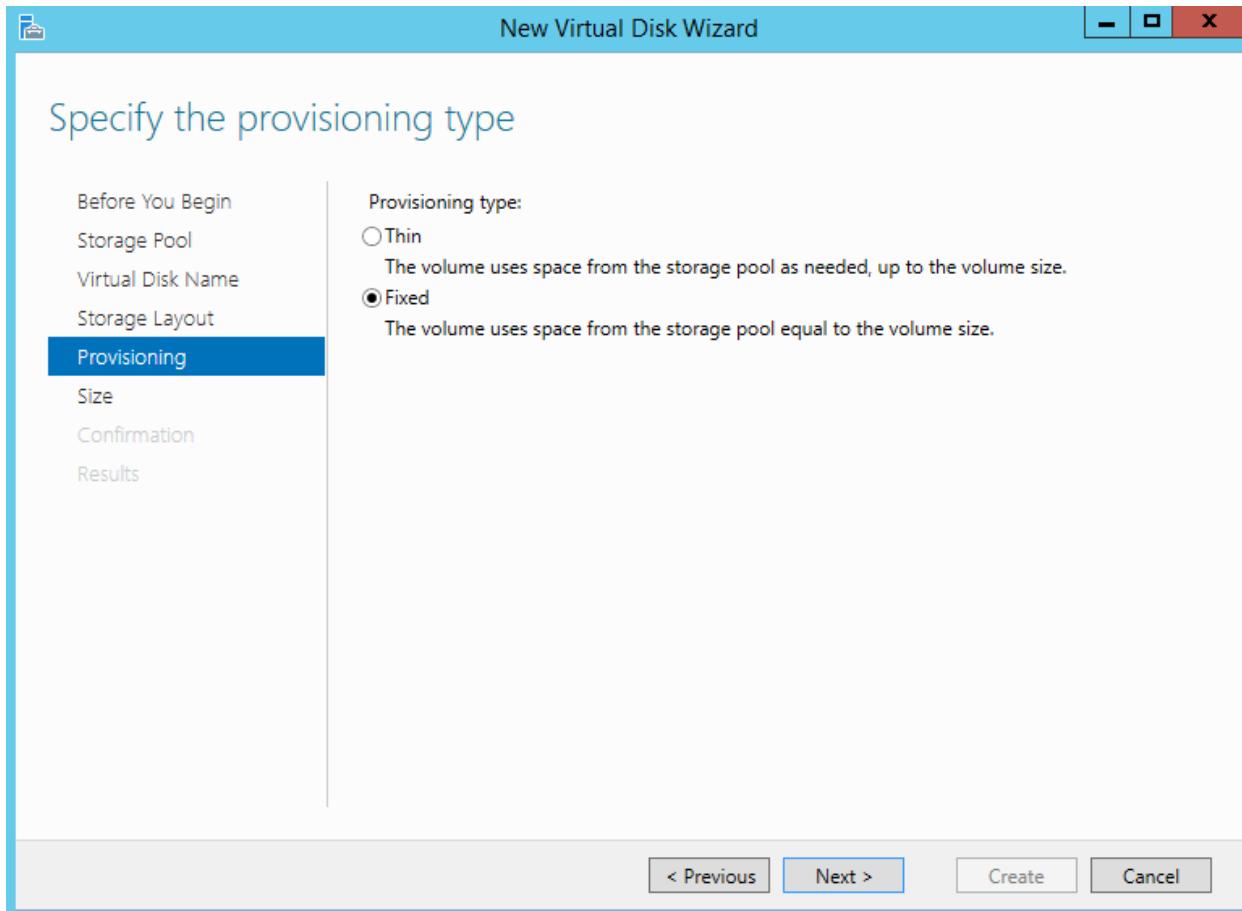
- Tại cửa sổ **Specify the virtual disk name**, nhập vào tại mục **Name: Virtual Disk** , click vào **Next**.



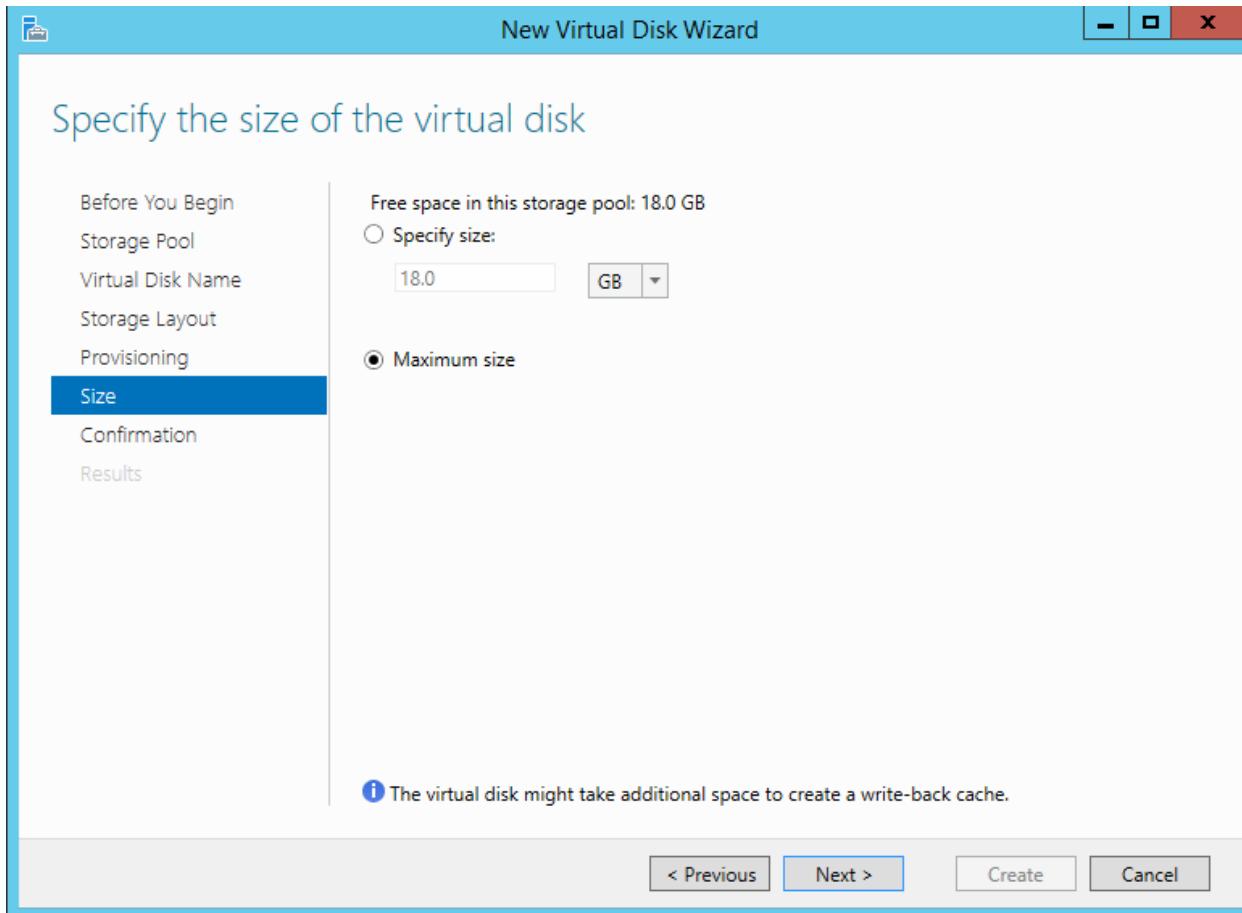
- Trong cửa sổ **Select the storage layout**, click chọn vào **Mirror**, click vào **Next**.



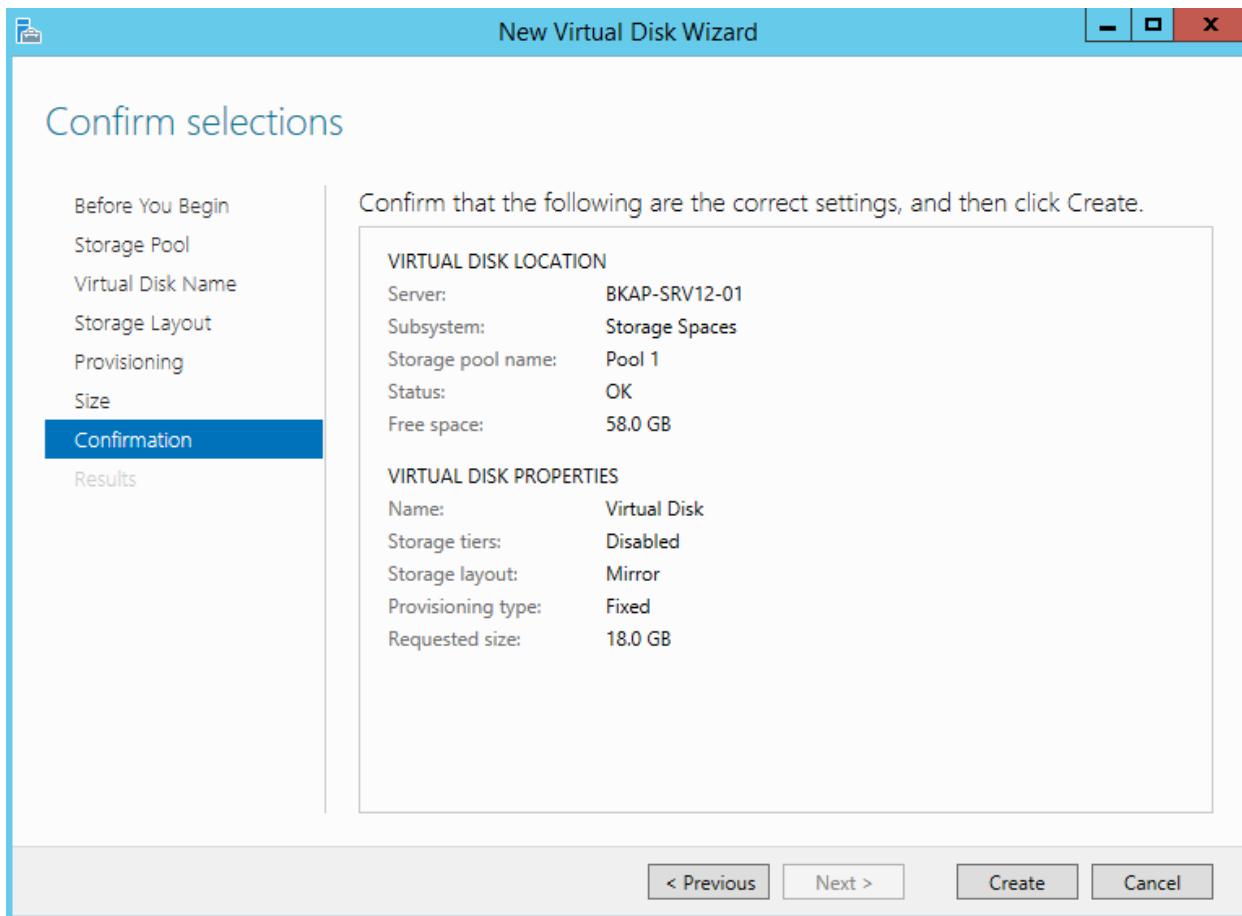
- Tại cửa sổ **Specify the provisioning type**, click chọn vào **Fixed**, click vào **Next**.



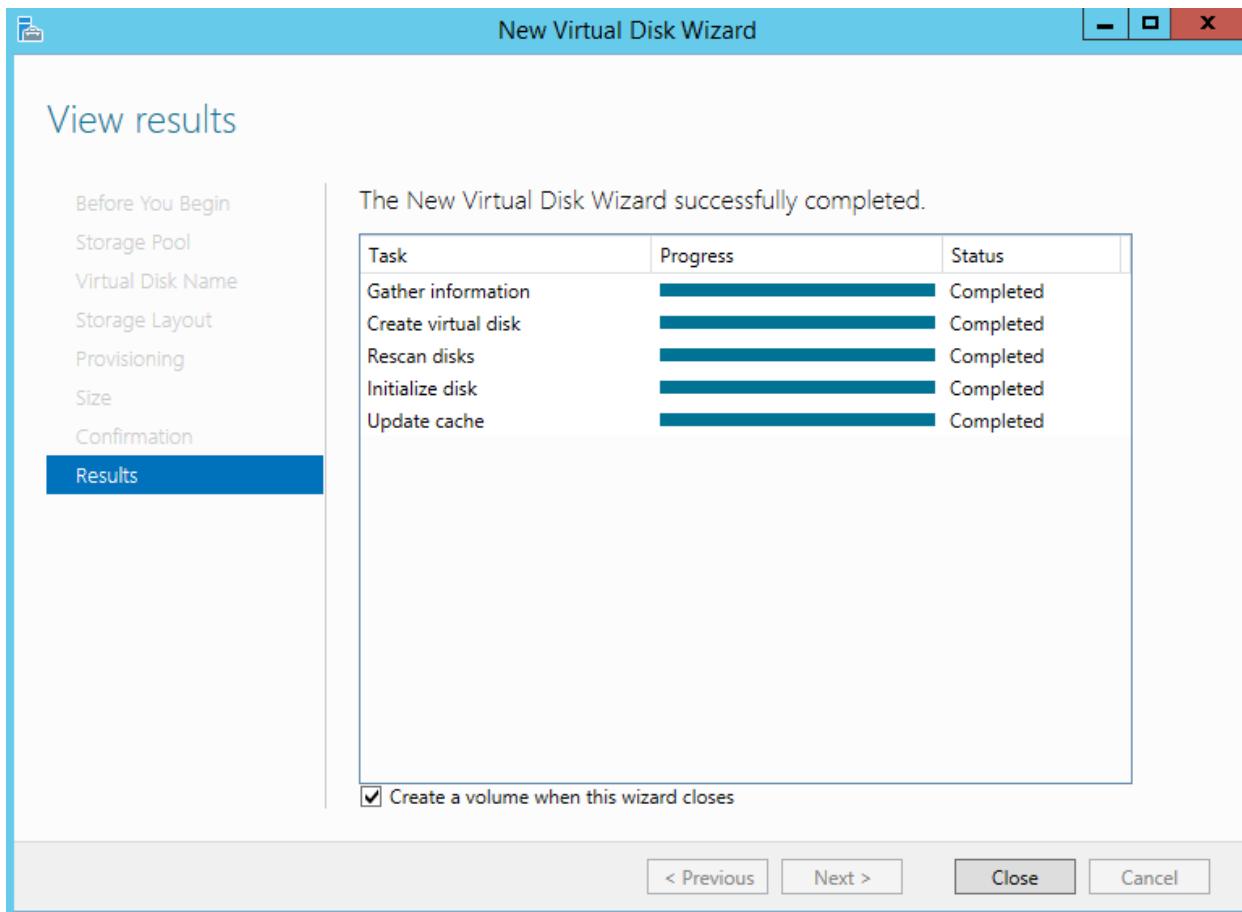
- Tại cửa sổ **Specify the size of the virtual disk**, click chọn vào **Maximum size**, click vào **Next**.



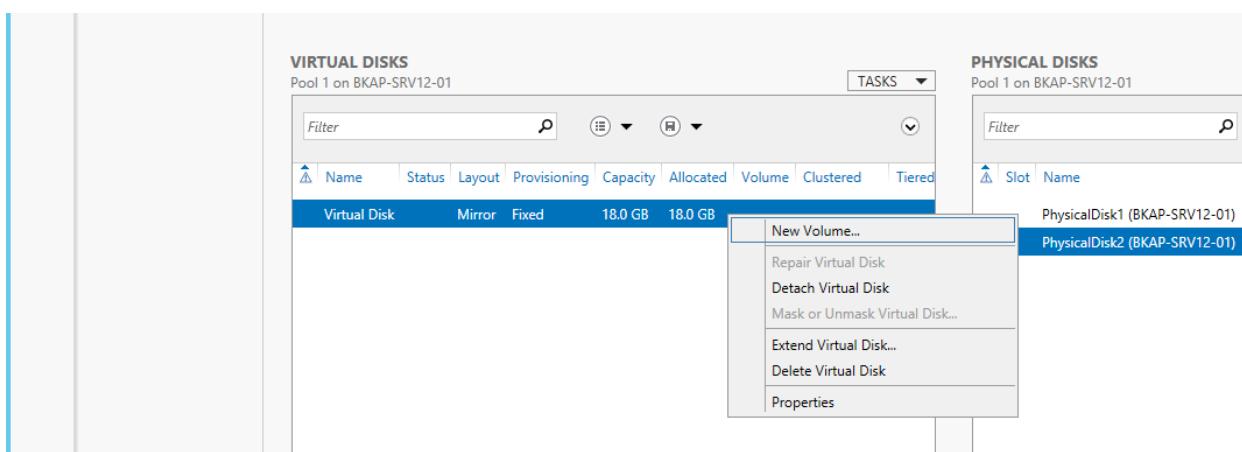
- Tại cửa sổ **Confirm selections**, click vào **Create**.



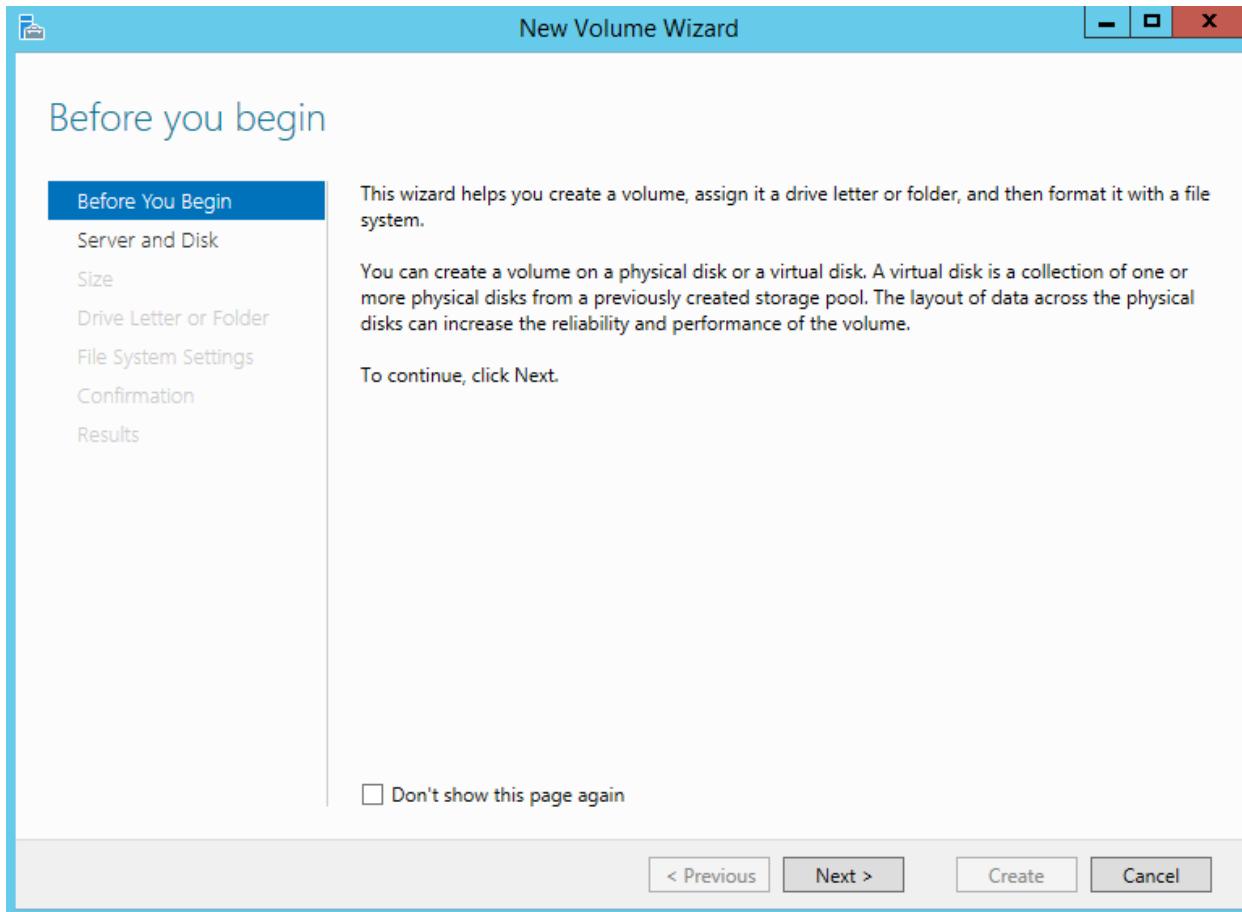
- Tại cửa sổ **View results**, kiểm tra kết quả, click vào **Close**.



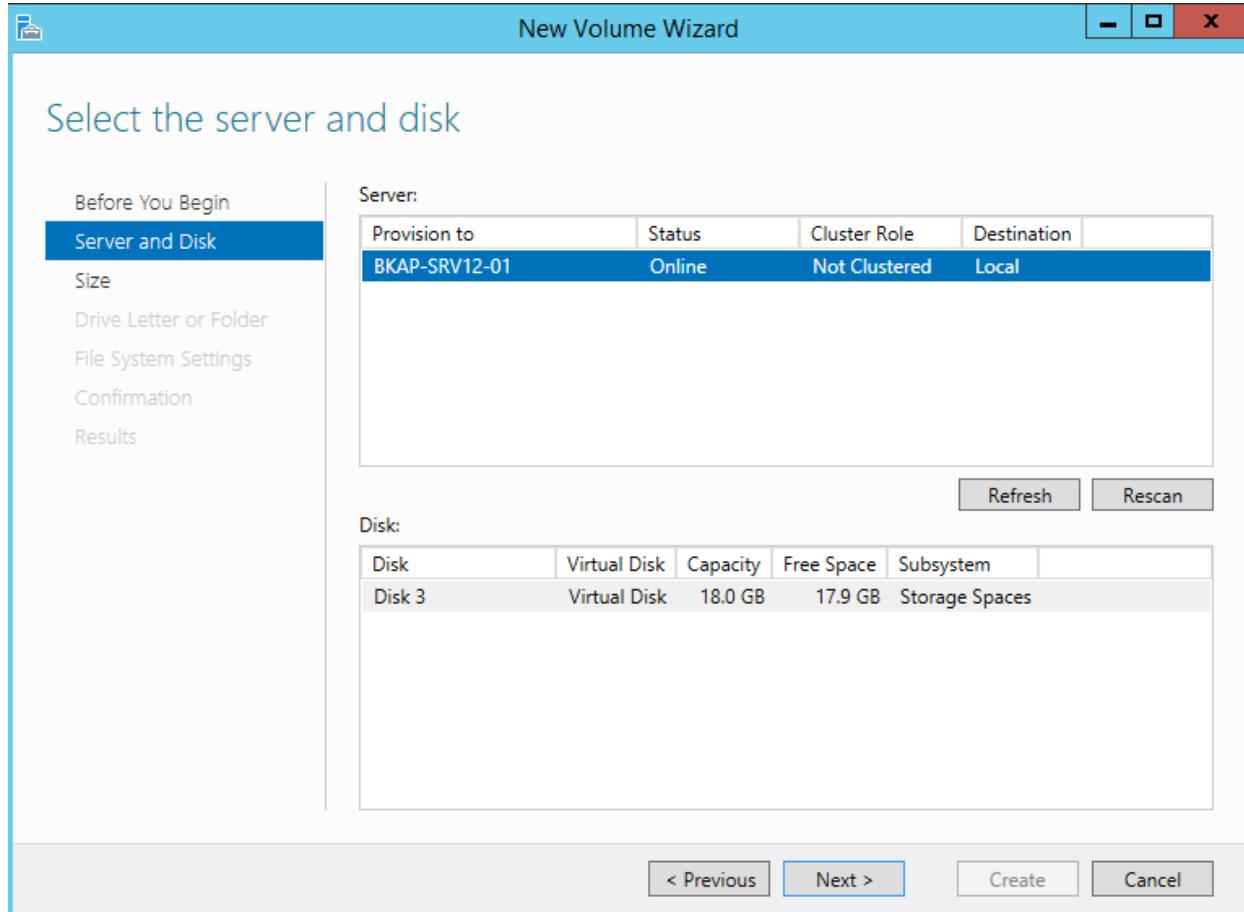
- Trong khung **VIRTUAL DISKS**, click chuột phải vào **Virtual Disk** vừa tạo, chọn **New Volume...**



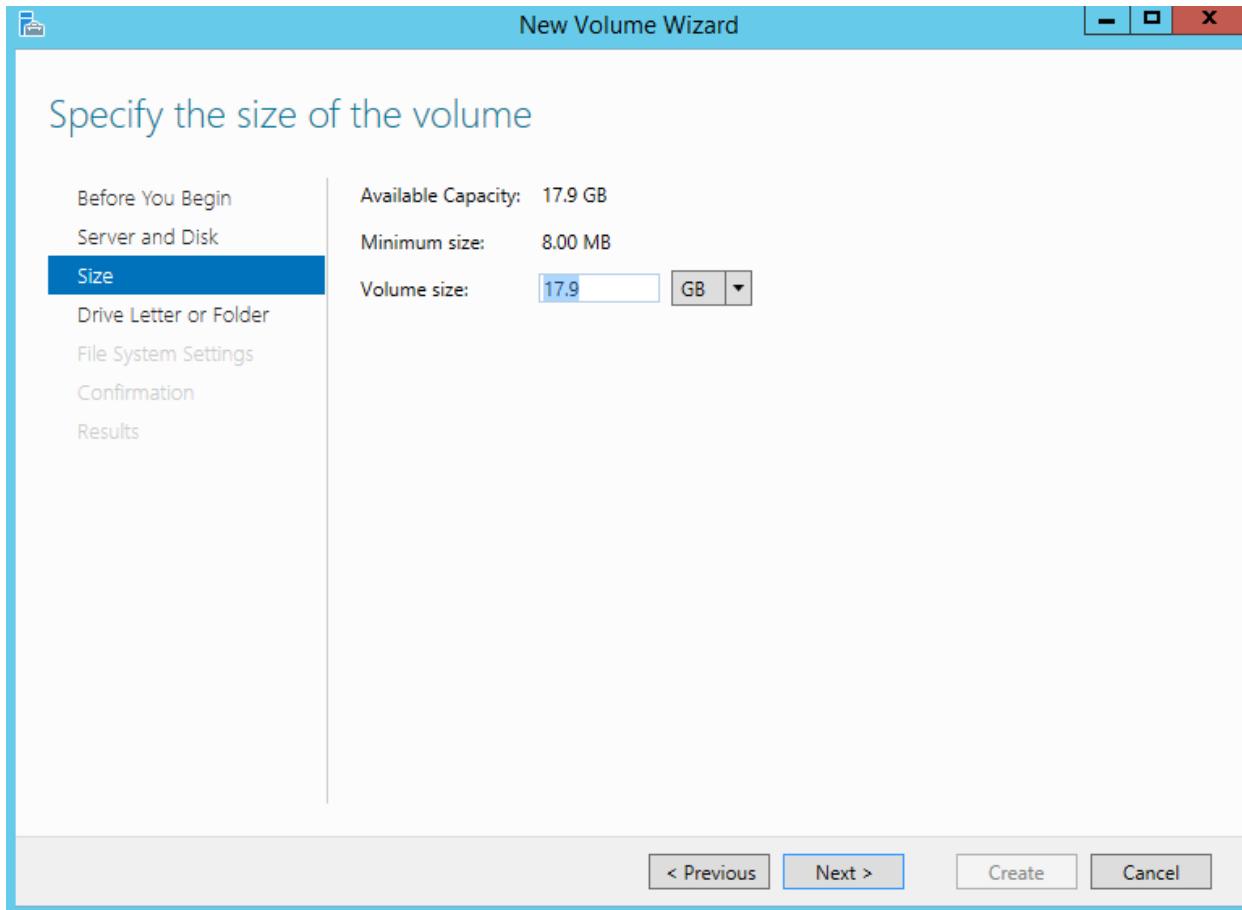
- Tại cửa sổ **Before you begin**, click vào **Next**.



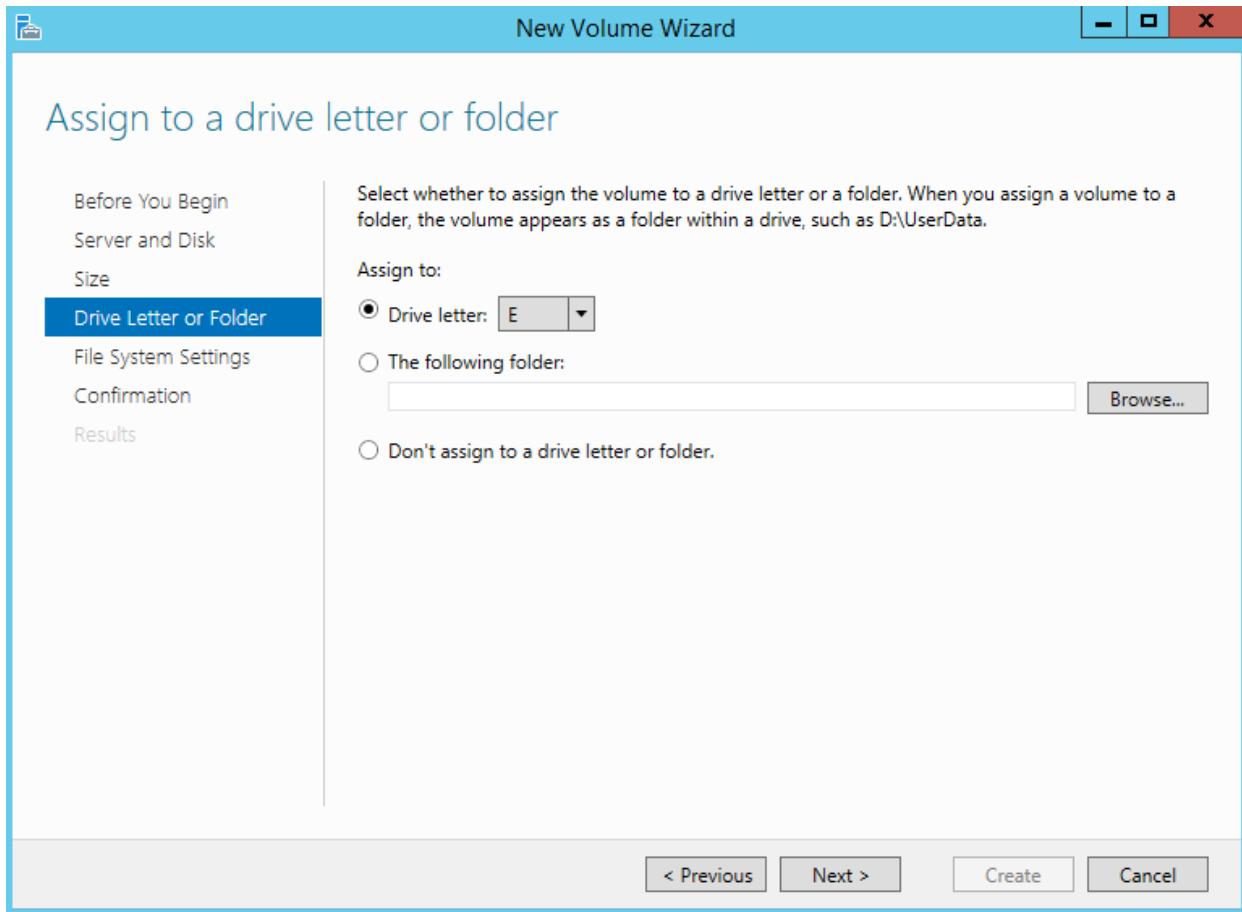
- Tại cửa sổ **Select the server and disk**, kiểm tra Server là **BKAP-SRV12-01**, click vào **Next**.



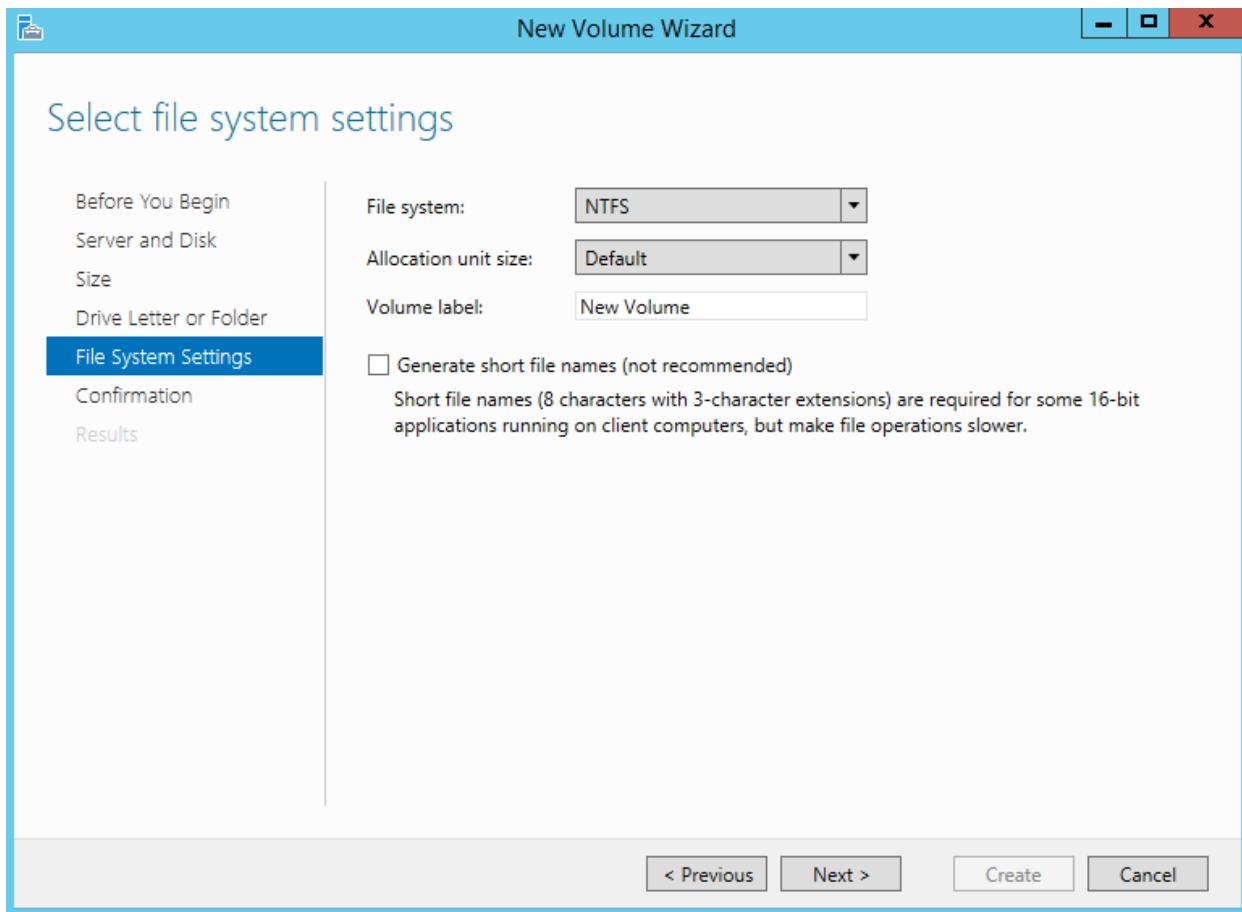
- Tại cửa sổ **Specify the size of the volume**, click vào **Next**.



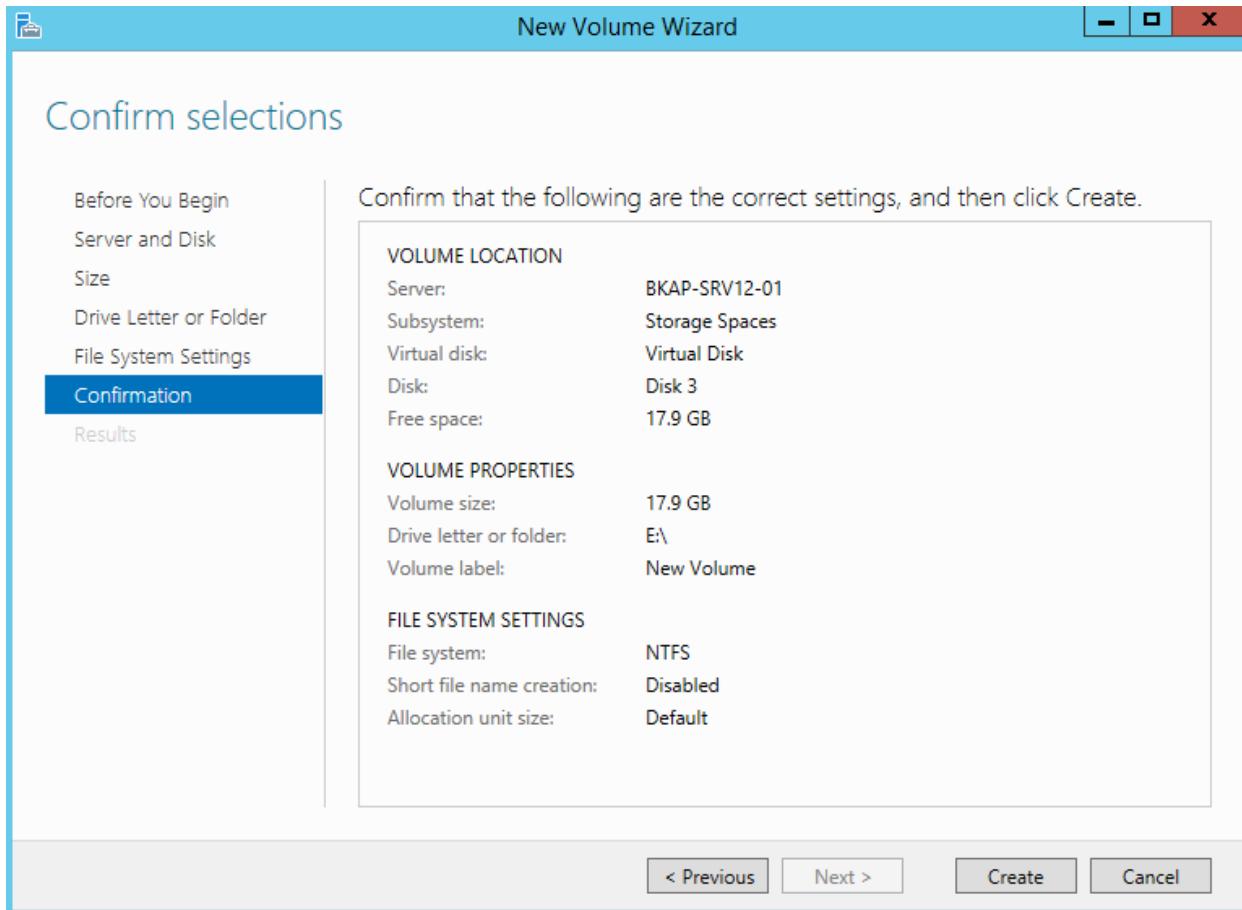
- Tại cửa sổ **Assign to a drive letter or folder**, click vào **Next**.



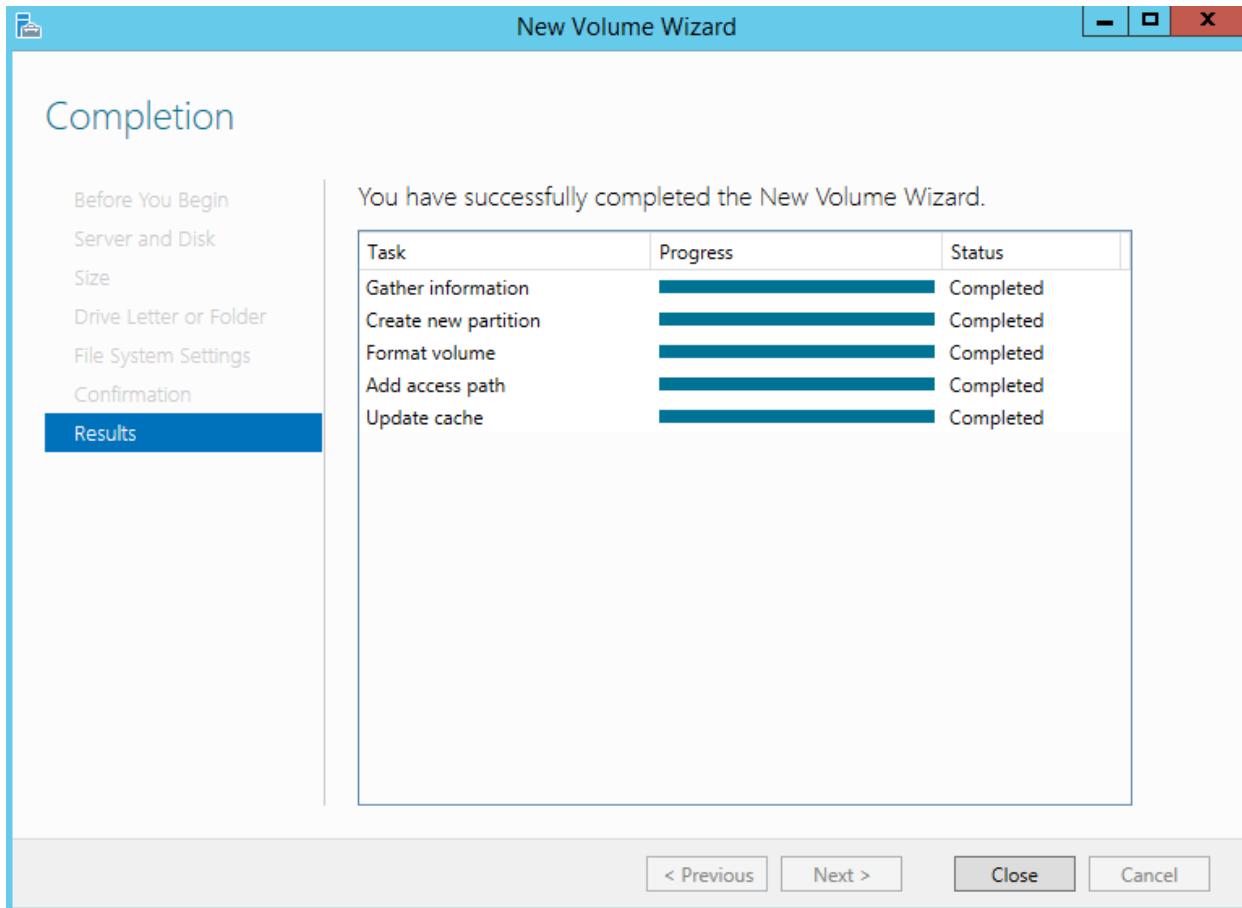
- Tại cửa sổ **Select file system settings**, click vào **Next**.



- Tại cửa sổ **Confirm selections**, click vào **Create**.



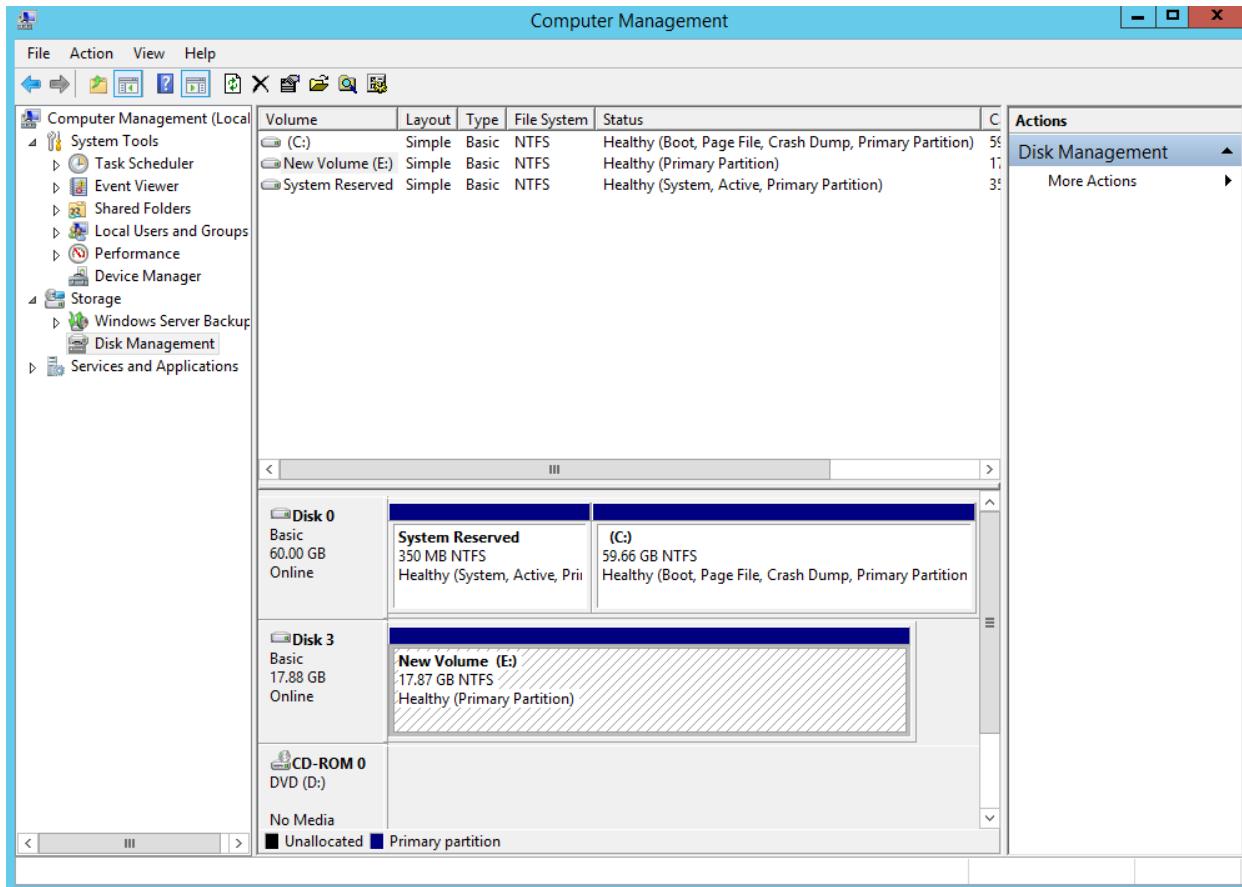
- Tại cửa sổ **Completion**, click vào **Close**.



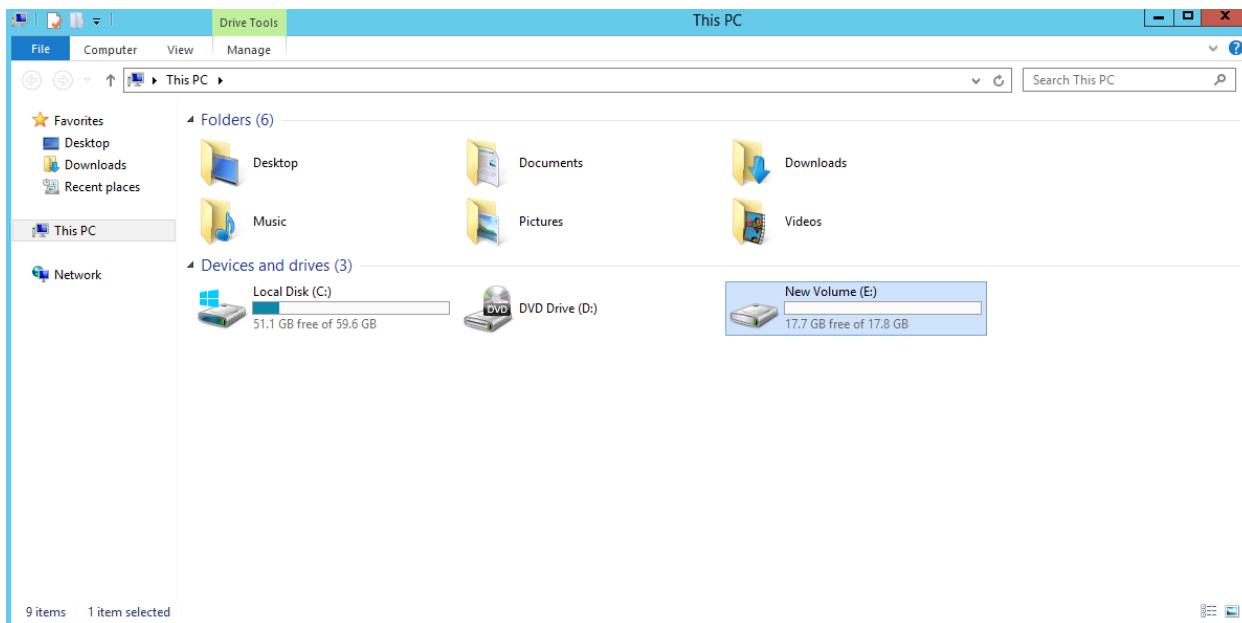
- Kiểm tra Virtual Disk đã được tạo.

The screenshot shows the Windows Server Manager interface under the 'File and Storage Services' section. In the left navigation pane, 'Disks' is selected. The main area displays two tables: 'DISKS' and 'VOLUMES'. The 'DISKS' table shows a single entry for 'BKAP-SRV12-01 (2)' with details: Number 0, Status Online, Capacity 60.0 GB, Unallocated 0.00 B, Partition MBR, Read Only No, Clustered No, Subsystem SAS, Bus Type VMware, Name VMWare, VMware Virt... The 'VOLUMES' table shows one volume 'E' from the pool, with details: Volume E, Status Fixed, Provisioning 17.9 GB, Capacity 17.8 GB, Free Space 0.00 B, Deduplication Rate 0.00%, and Deduplication Status Off. To the right of the 'VOLUMES' table is a 'STORAGE POOL' summary for 'Microsoft Storage Space Device on BKAP-SRV12-01'. It shows Pool 1 with Capacity 58.5 GB, 63.2% Used (37.0 GB Used Space), and 21.5 GB Free Space. The subsystem is Storage Spaces, and the server is BKAP-SRV12-01. The volume is labeled E.

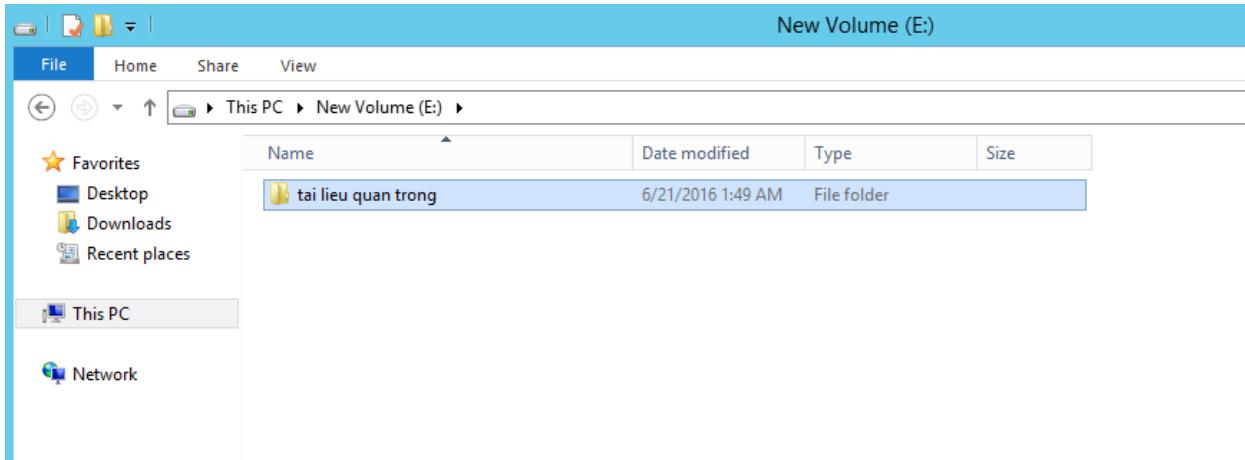
- Kiểm tra trong Disk Management.



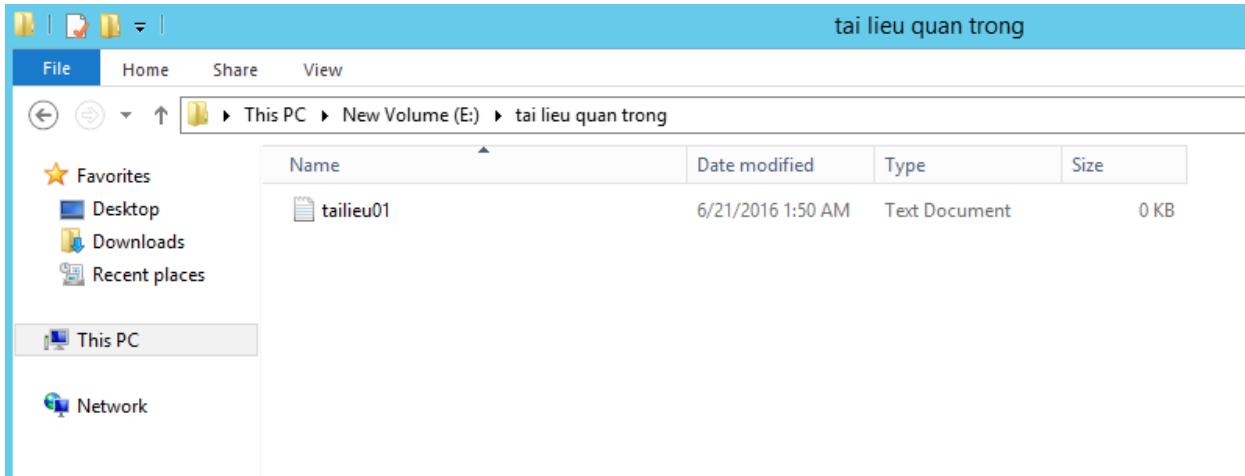
- Kiểm tra trong Computer.



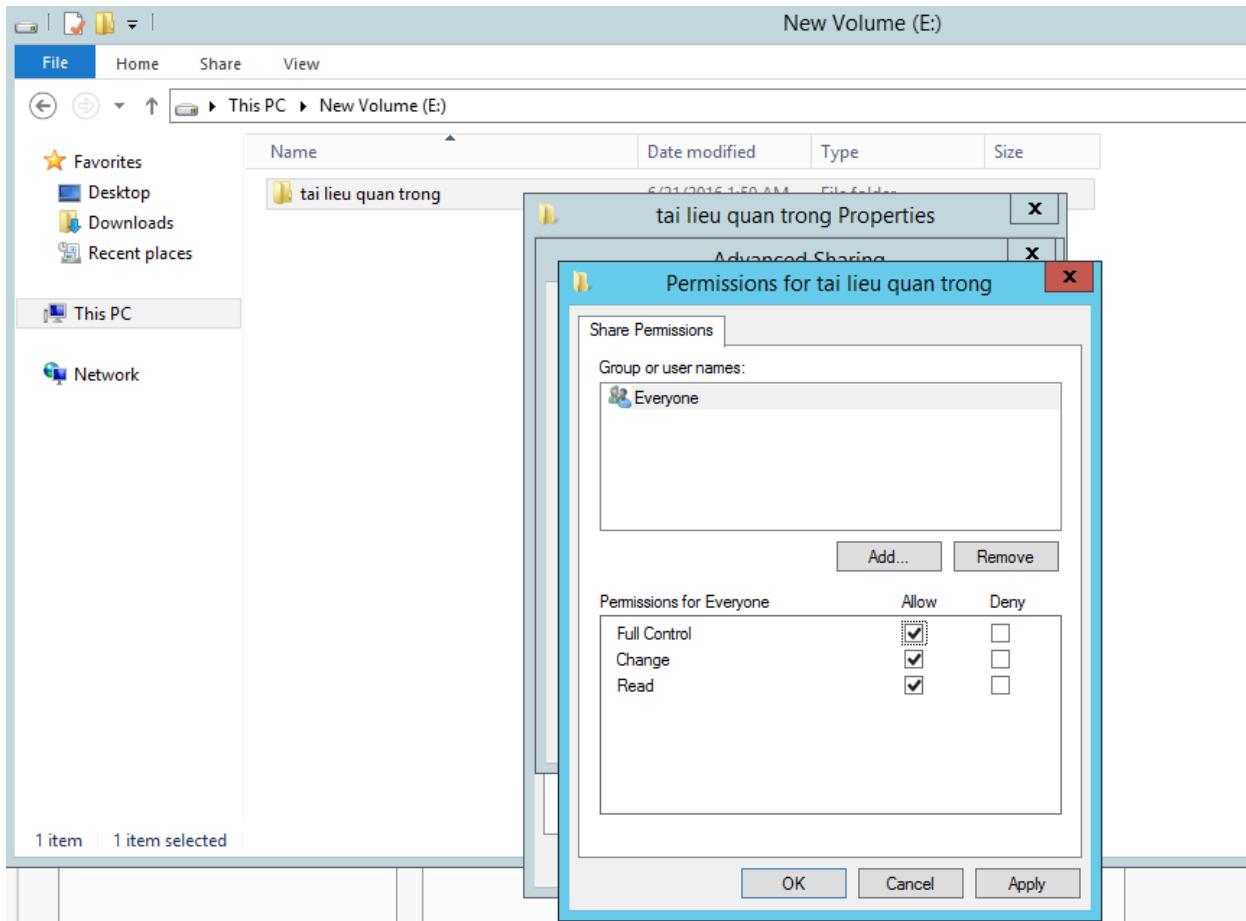
- Tạo thư mục trong ổ E vừa tạo.



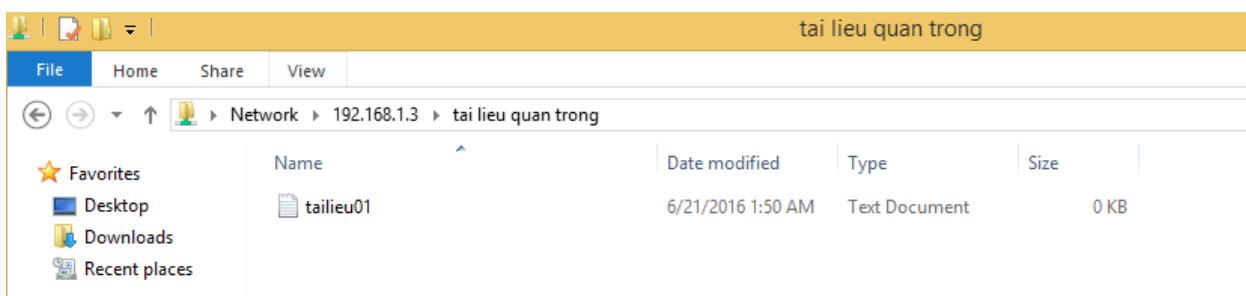
- Tạo file bất kì trong thư mục trên.



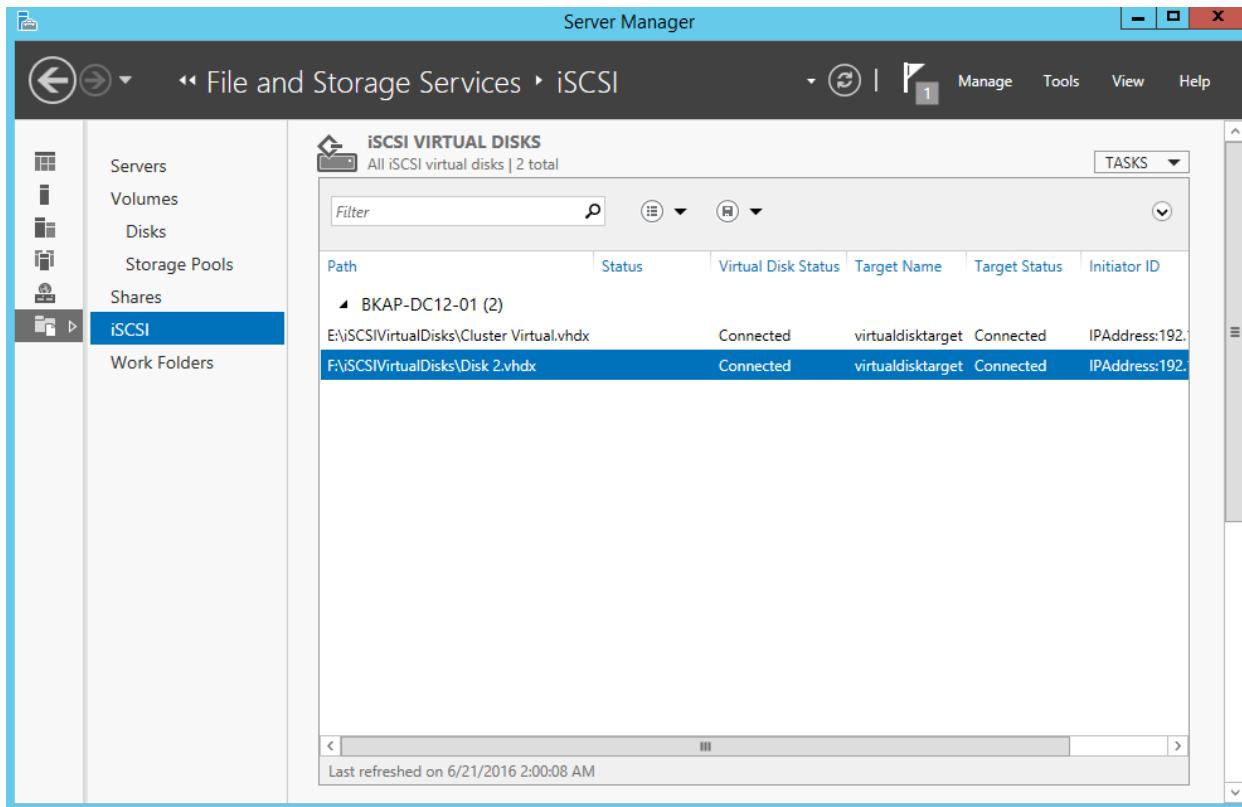
- Chia sẻ thư mục này với quyền **Full Control** cho **Everyone**.



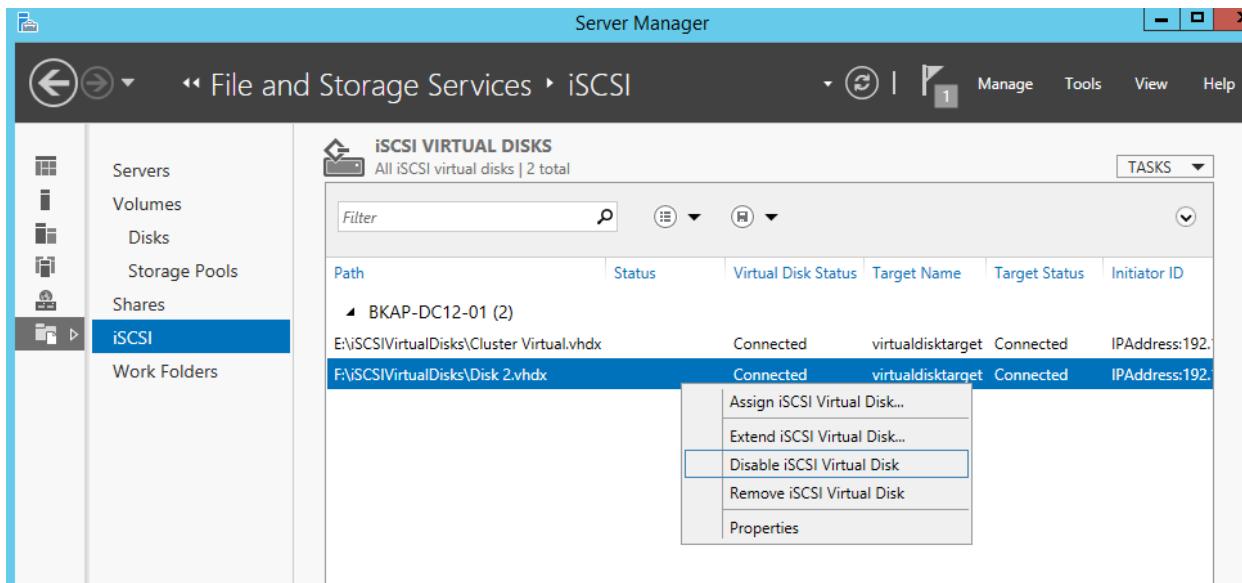
- Chuyển sang máy BKAP-WIN8, kiểm tra thư mục share folder.



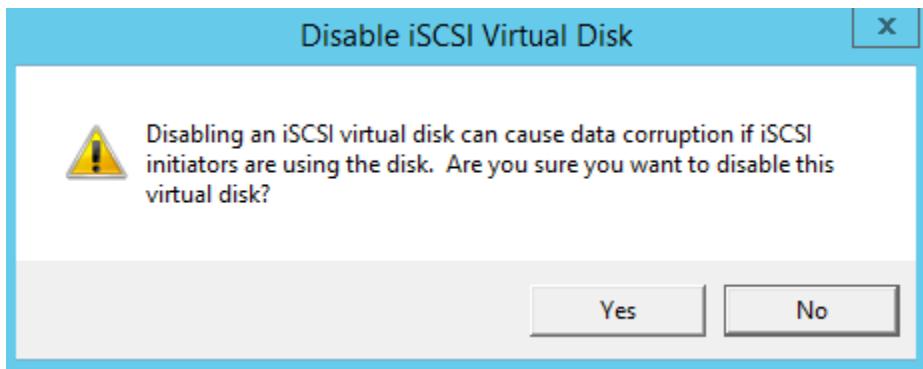
- Chuyển về máy *BKAP-DC12-01*, click vào *Refresh*.



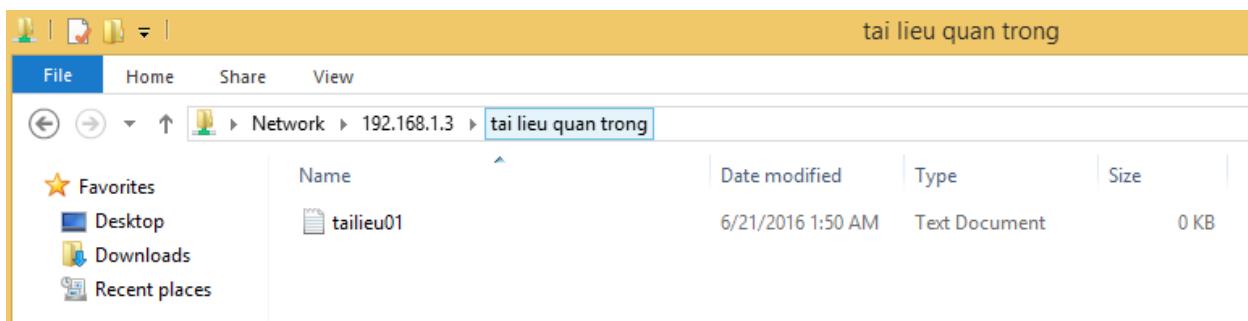
- Thực hiện **Disable iSCSI virtual disk**.
 - Click vào **F:\iSCSIVirtualDisks\Disk 2.vhdx**, chọn **Disable iSCSI Virtual Disk**.



- Tại cửa sổ **Disable iSCSI Virtual Disk**, click vào Yes.



- Chuyển sang máy *BKAP-WIN8*, kiểm tra truy cập vào folder share bình thường.



2.2 Cấu hình cơ sở hạ tầng phân loại tập tin.

1.Yêu cầu bài Lab:

Thực hiện cấu hình trên máy *BKAP-DC12-01*.

- Cài đặt **File Server Resource Manager**.
- Tạo 1 rule *corporate documentation*.
- Tạo 1 rule chia sẻ folder.
- Tạo *file management task to expire corporate documents*.

2.Yêu cầu chuẩn bị:

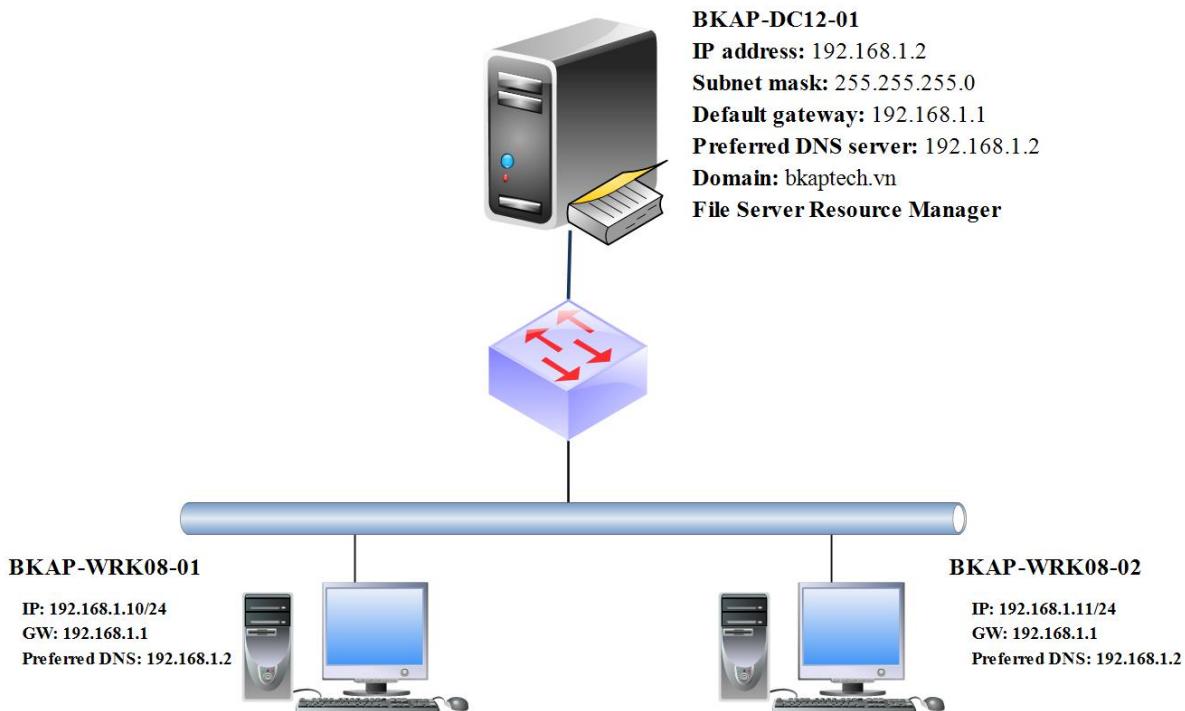
- + Máy *BKAP-DC12-01* đã nâng cấp lên Domain Controller quản lý miền **bkaptech.vn**.

3.Mô hình Lab:

HỆ THỐNG ĐÀO TẠO CNTT QUỐC TẾ BACHKHOA-APTECH

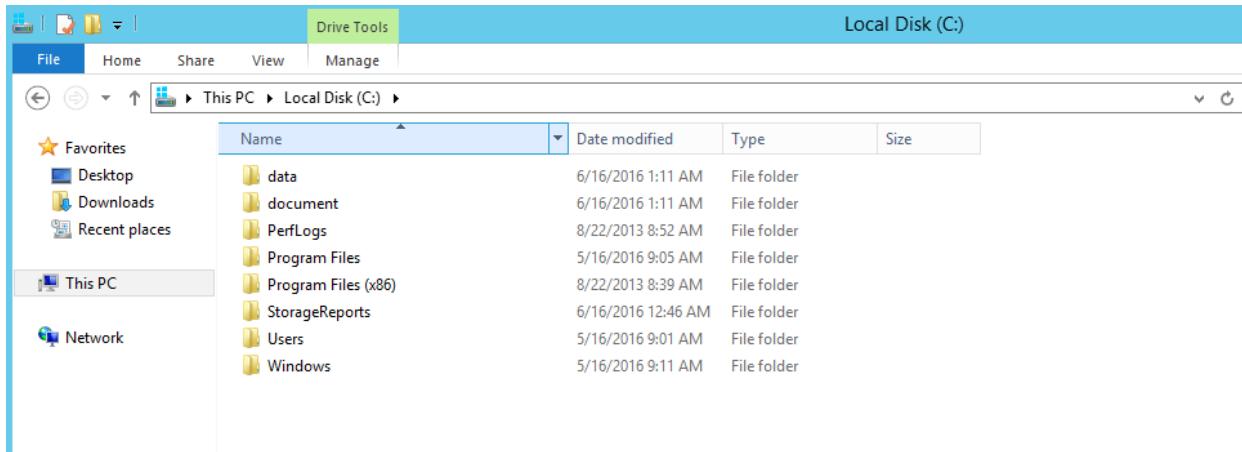
BACHKHOA
EDUCATION APTECH

Cấu hình cơ sở hạ tầng phân loại tập tin

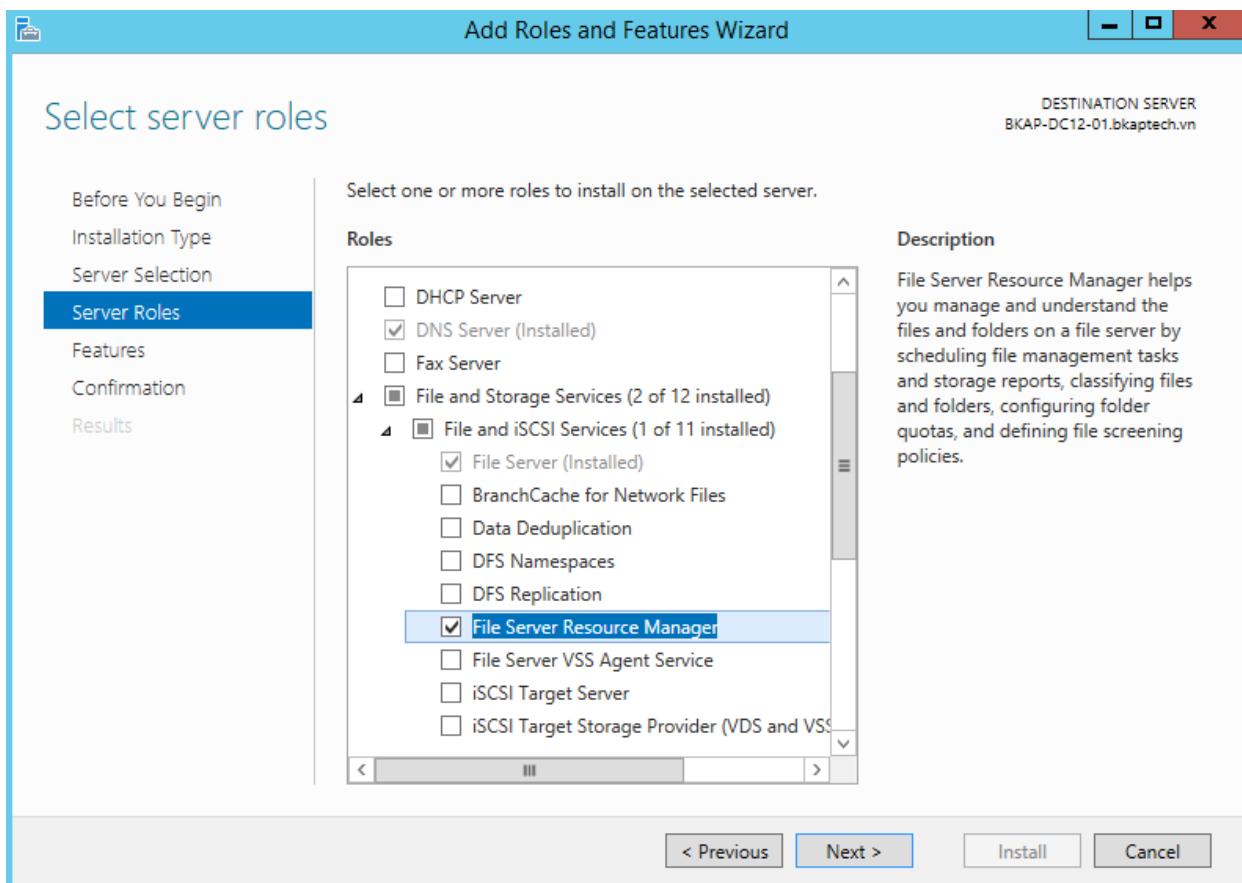


Hướng dẫn chi tiết:

- Trên máy **BKAP-DC12-01**:
 - Tạo 2 thư mục tên **data** và **document** trong ô C.

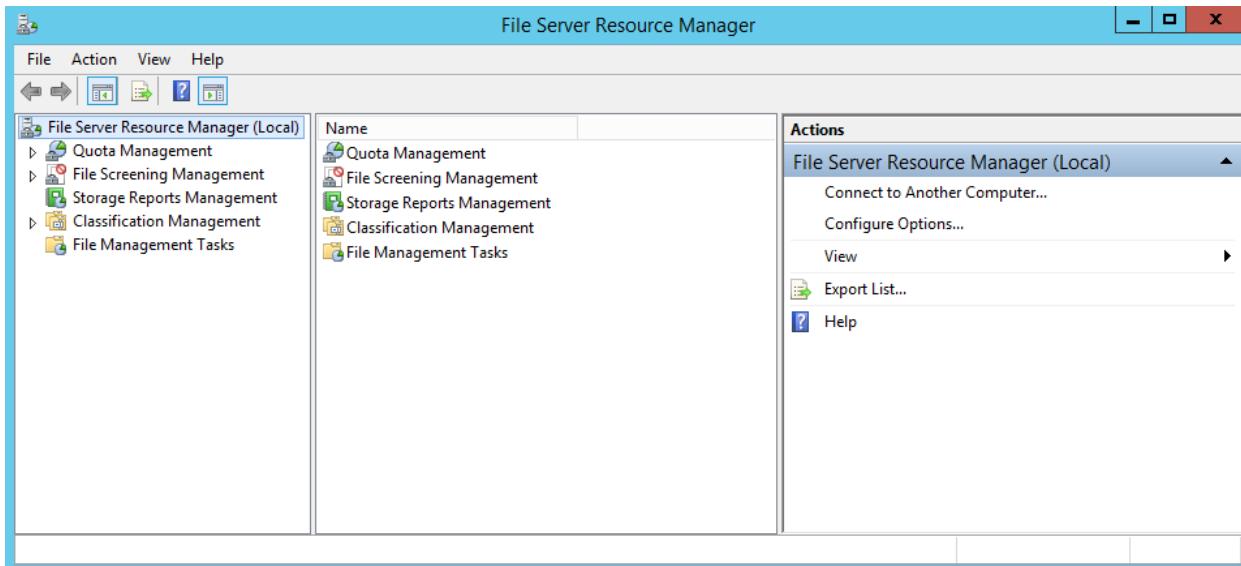


- Cài đặt **File Server Resource Manager**.

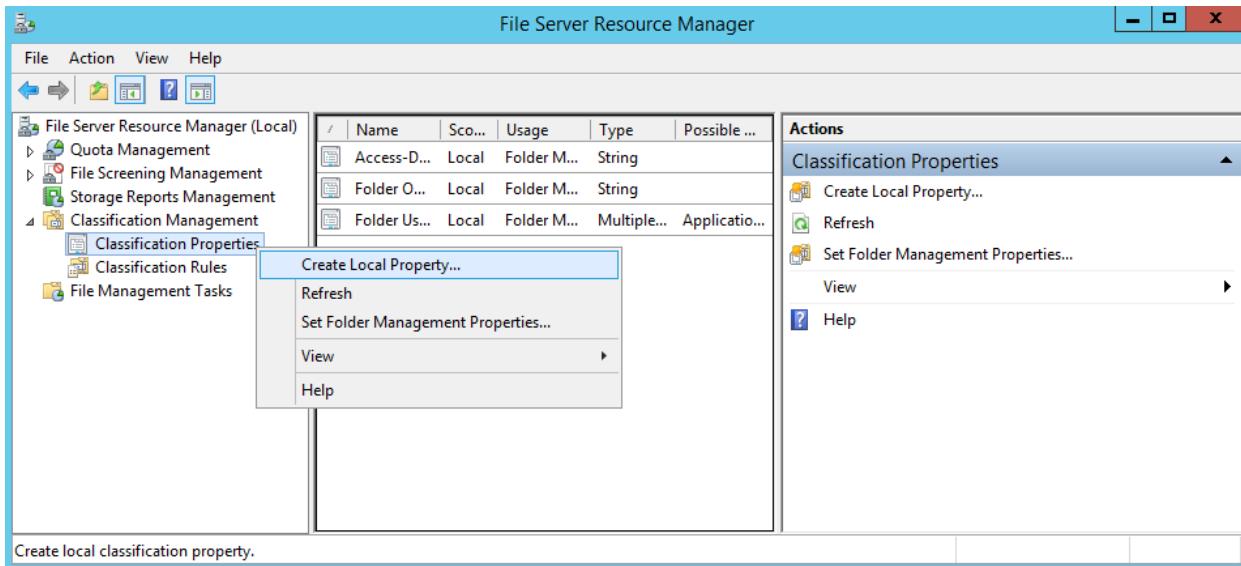


- Thực hiện cấu hình phân loại tập tin trong **FSRM**.

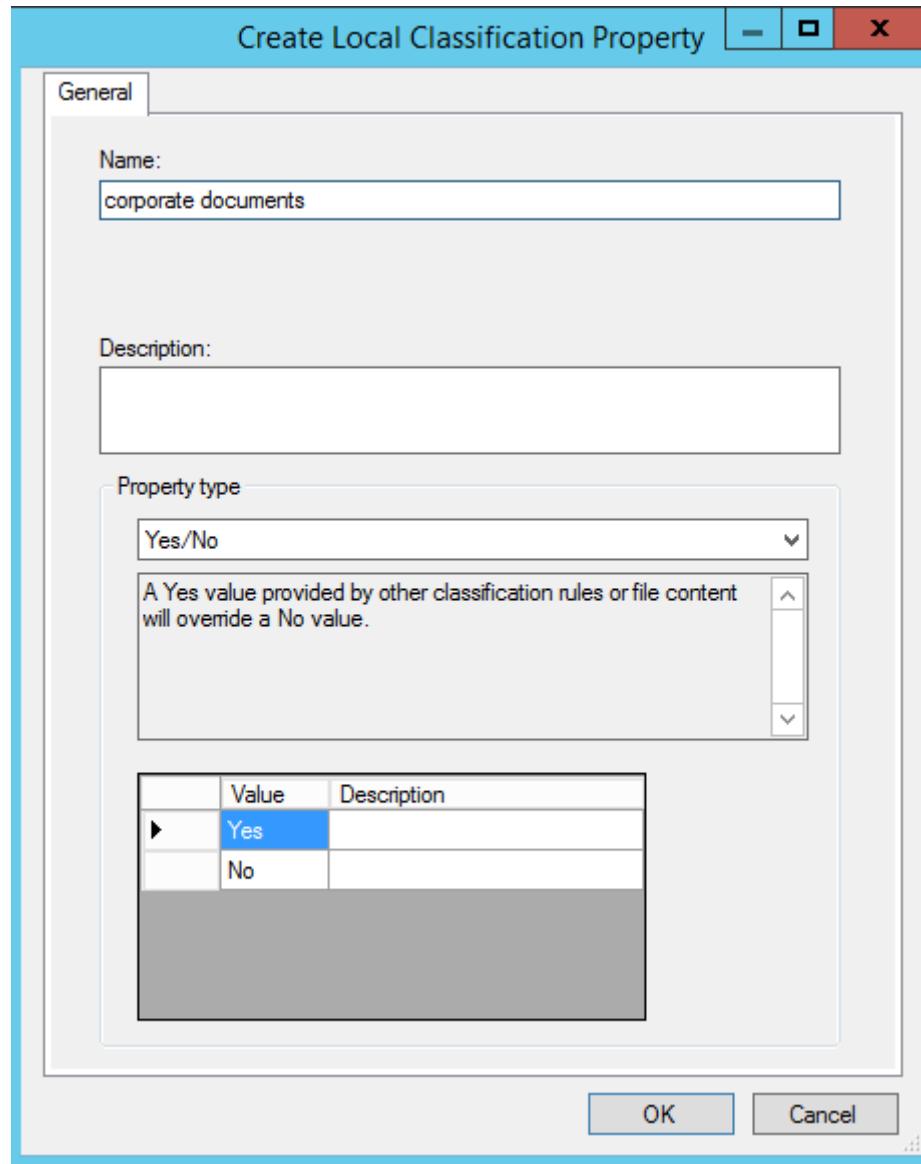
- **Mở File Server Resource Manager.**



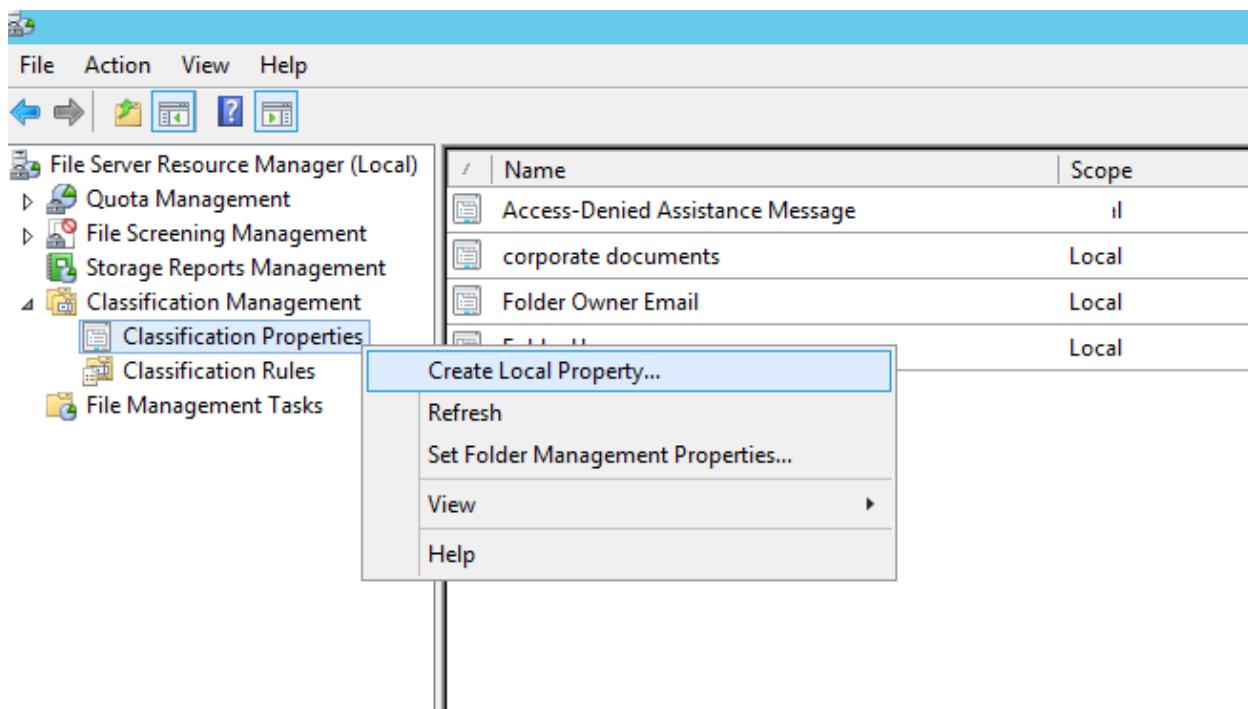
- Trong cửa sổ **File Server Resource Manager**, click chuột phải tại **Classification Management / Classification Properties**, chọn **Create Local Property...**



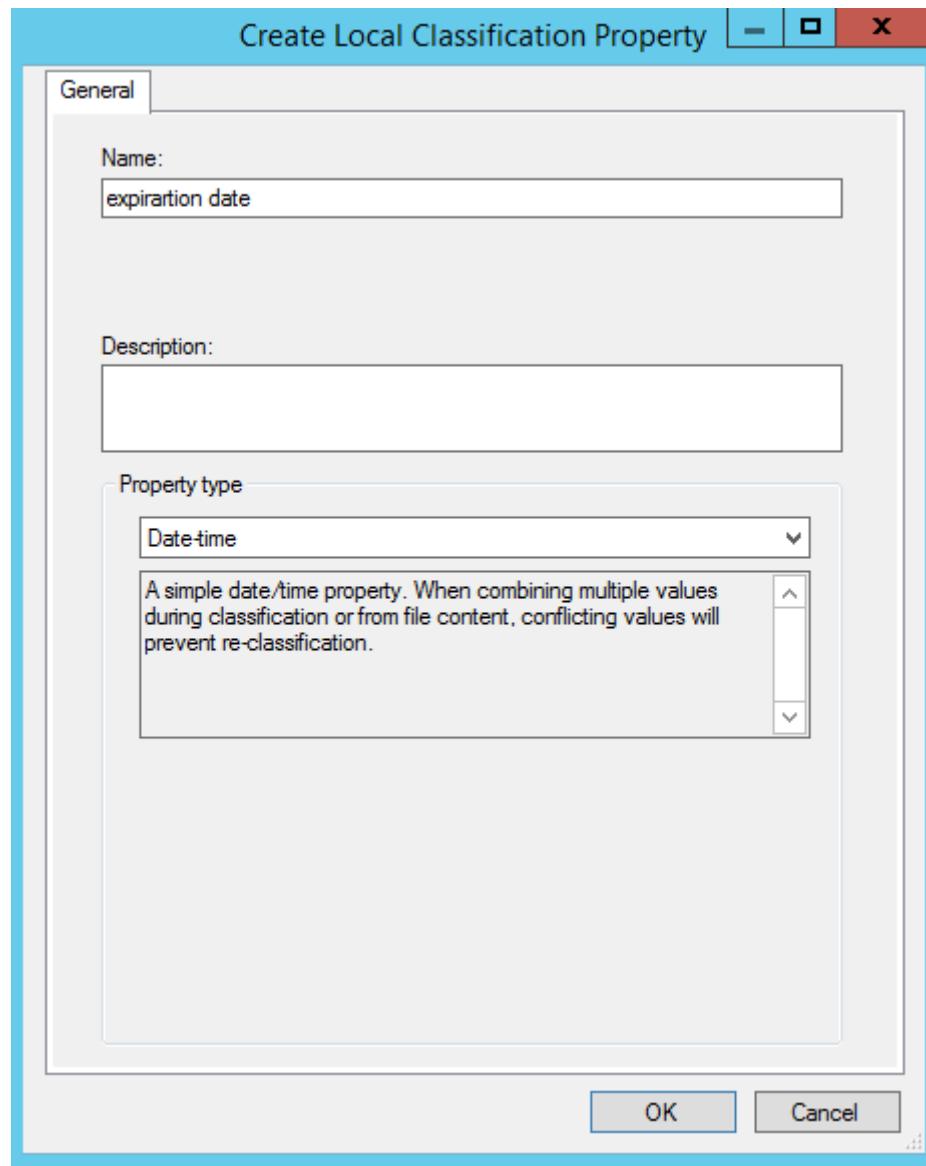
- Tại cửa sổ **Create Local Classification Property**, nhập vào tại mục *Name* : **corporate documents** , tại mục **Property type**, chọn **Yes/No => OK**.



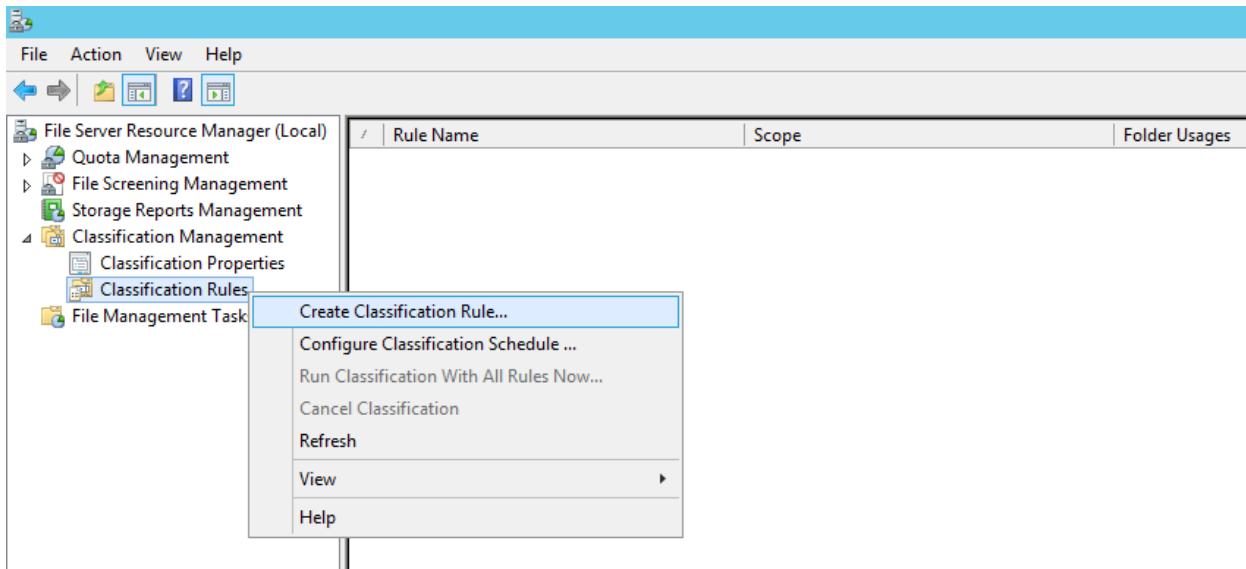
o Tiếp tục Create Local Property...



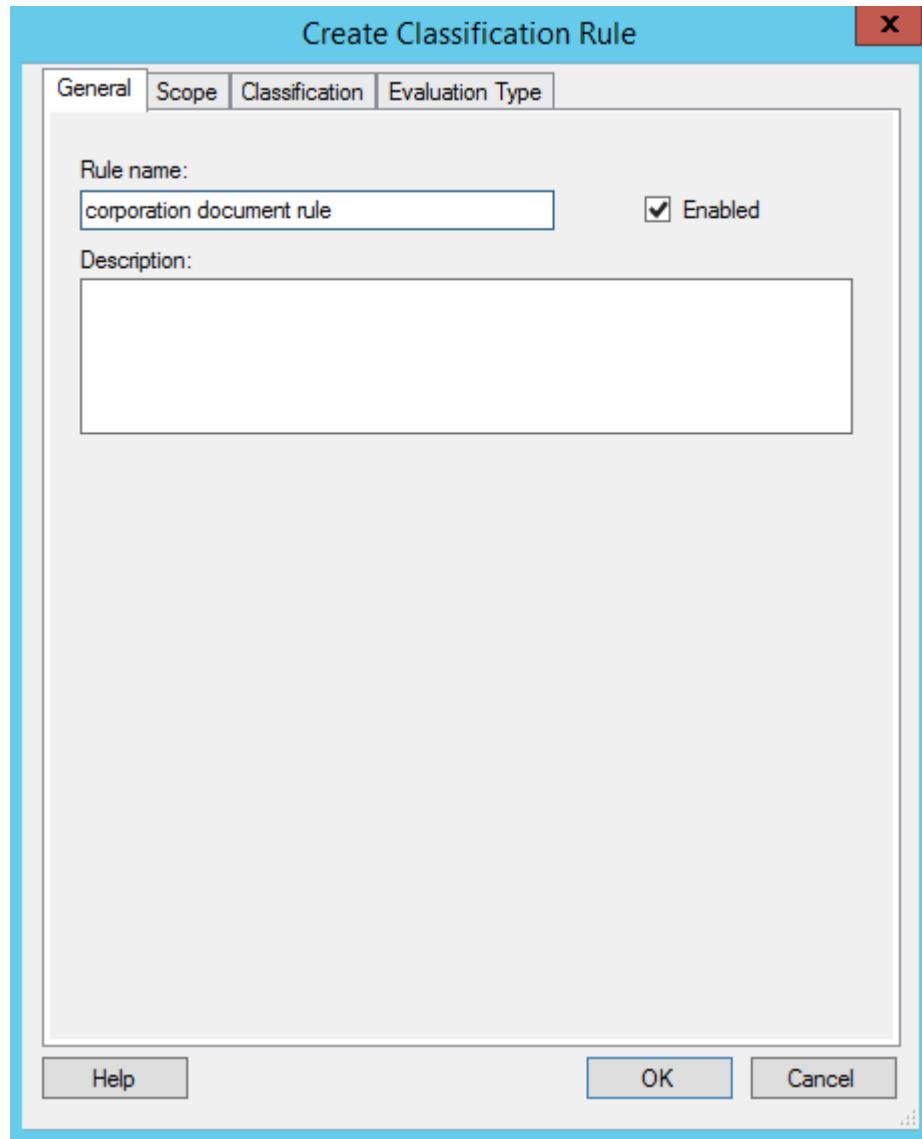
- Tại mục **Name**, nhập vào **expirartion date**, tại mục **Property type**, chọn **Date-time**, **OK**.



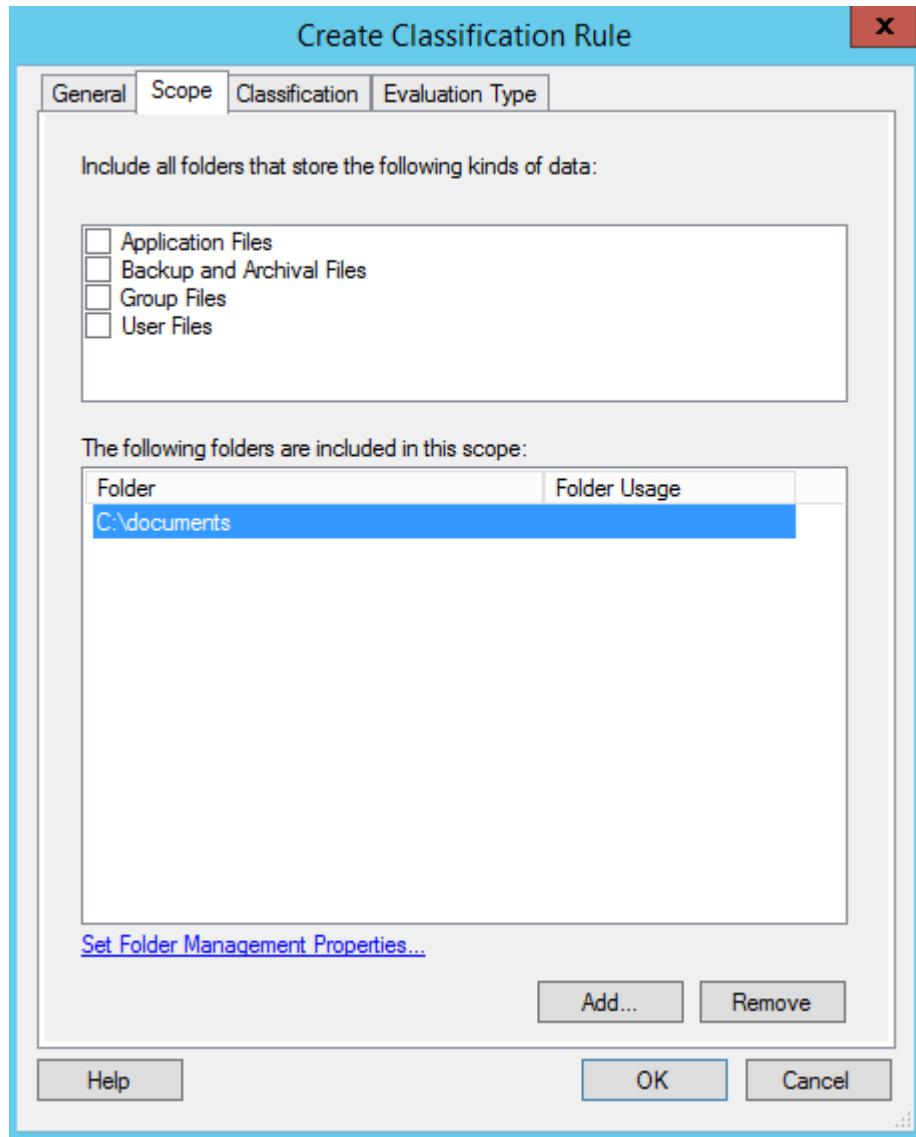
- Click chuột phải tại **Classification Rules**, chọn **Create Classification Rule...**



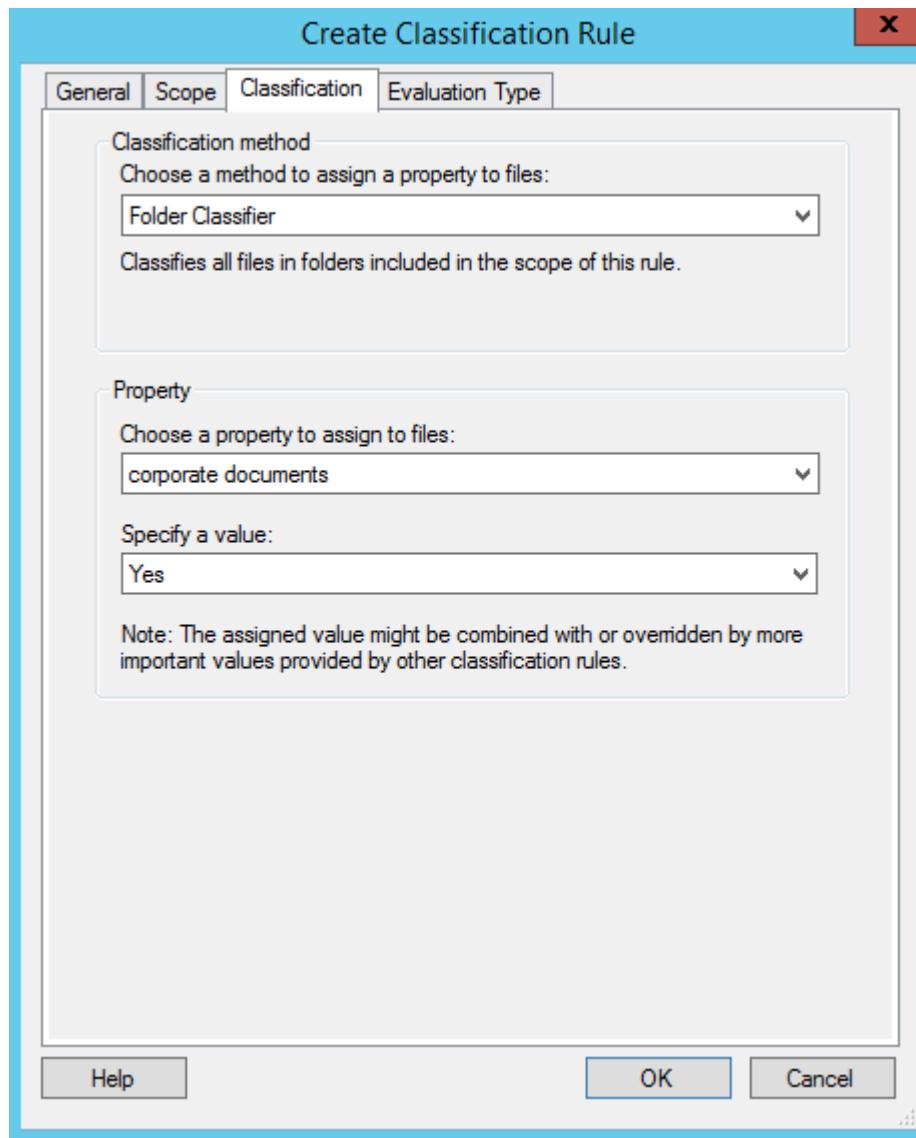
- Tại cửa sổ **Create Classification Rule**, trong Tab **General**, trong mục **Rule name**, nhập vào **corporation document rule**.



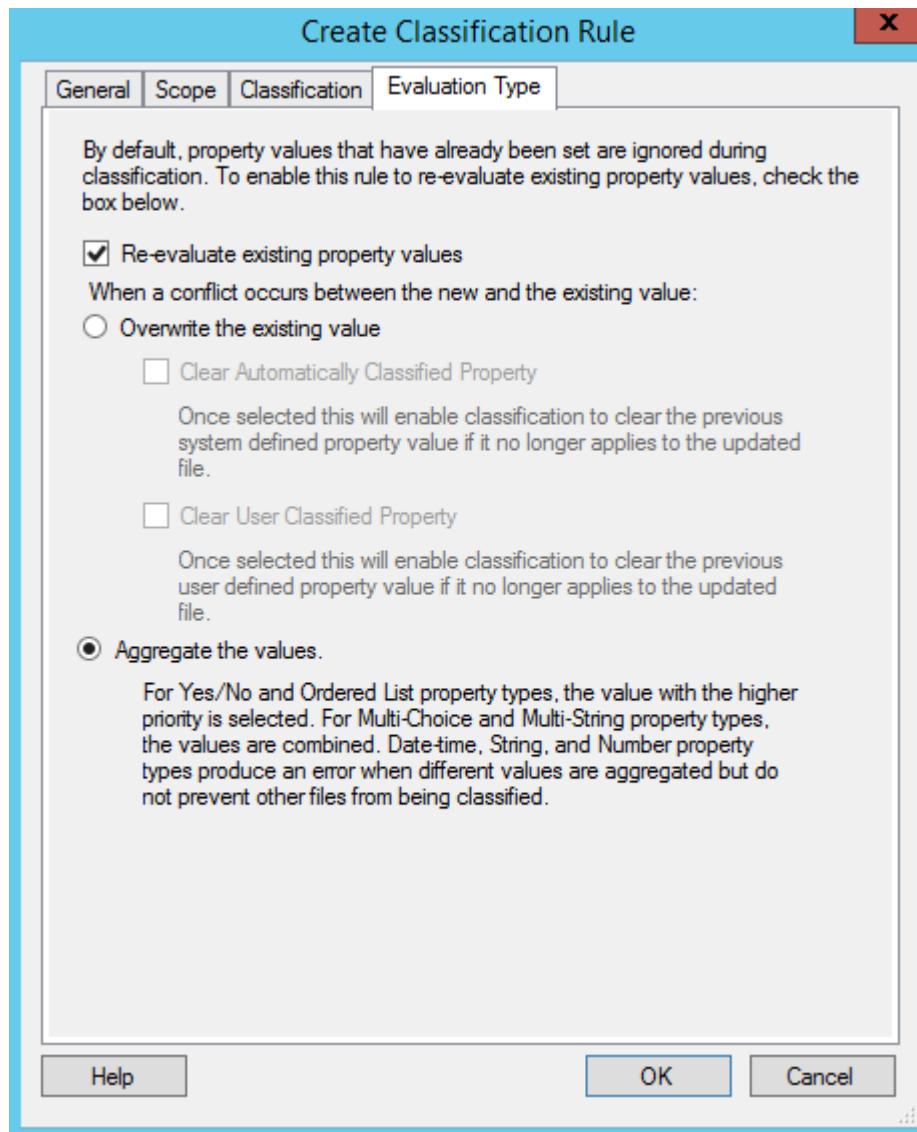
- Chuyển sang tab **Scope**, click vào **Add...**, thêm vào thư mục **documents** trong ổ C.



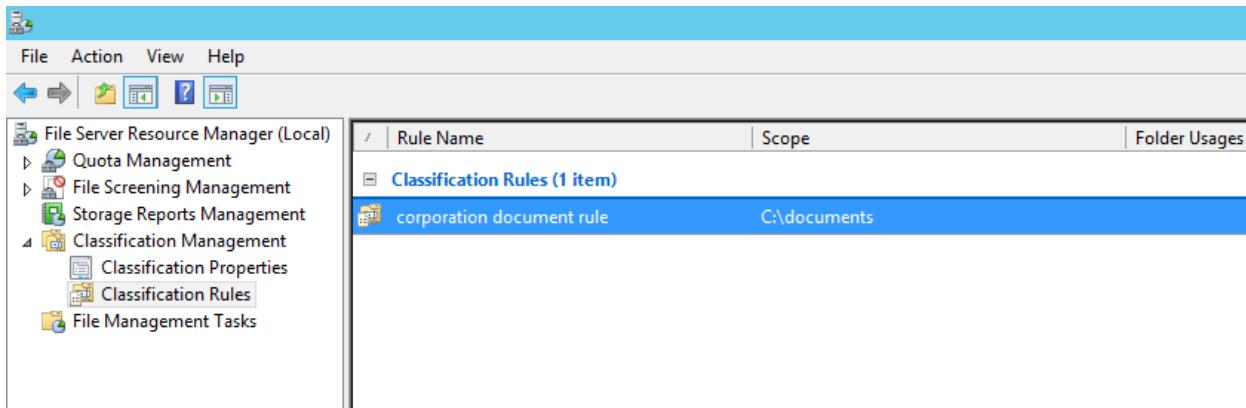
- Chuyển sang tab **Classification**, trong mục **Choose a method to assign a property to files**, chọn **Folder Classifier**, kiểm tra các tùy chọn như hình dưới.



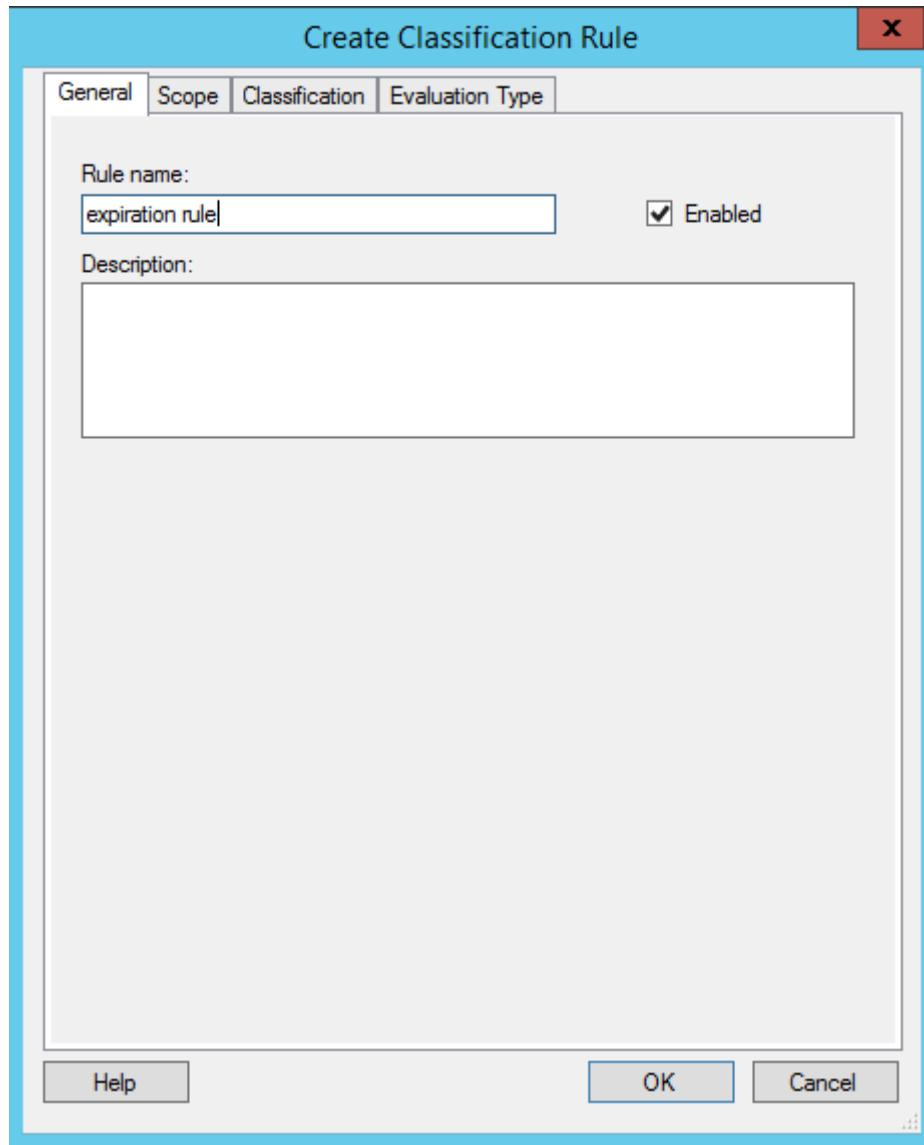
- Chuyển sang tab **Evaluation Type**, click chọn vào **Re-evaluate existing property values => OK.**



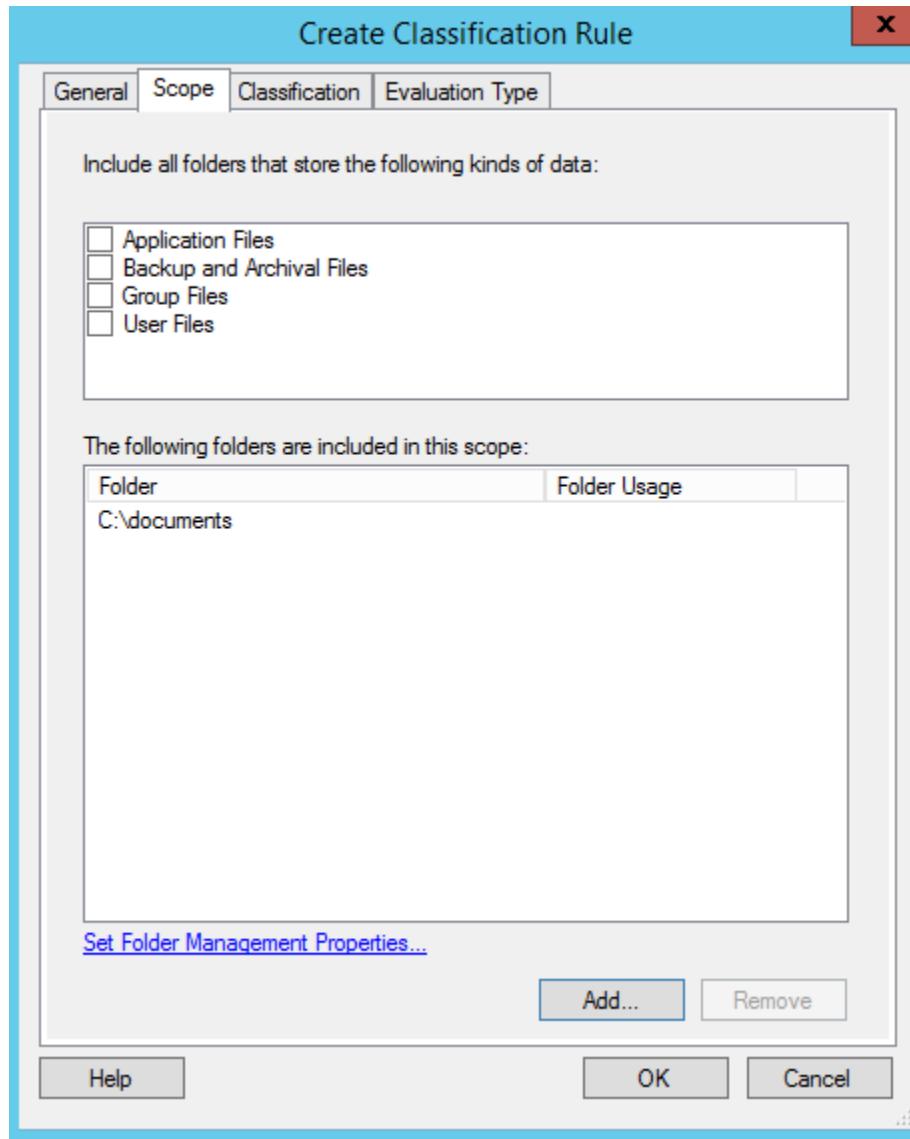
- Kiểm tra rule vừa tạo.



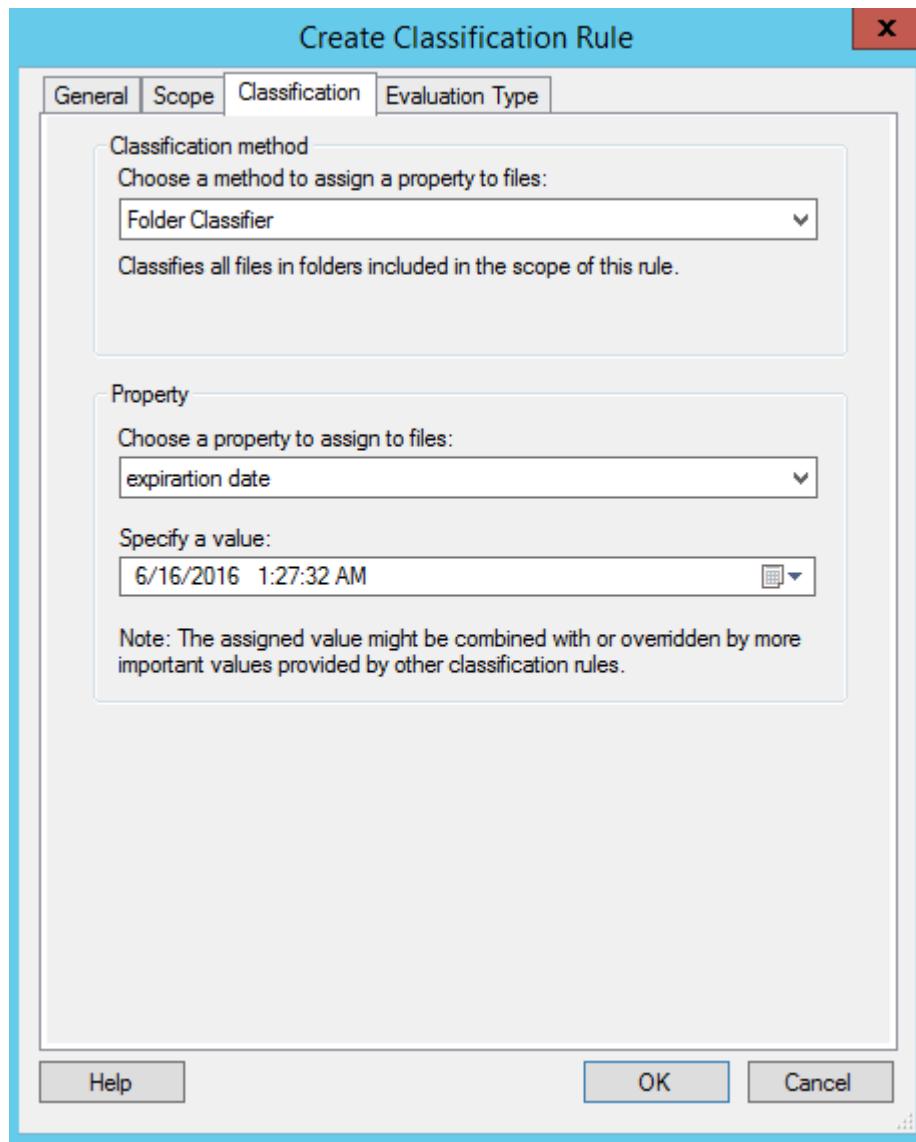
o Tạo expiration rule:



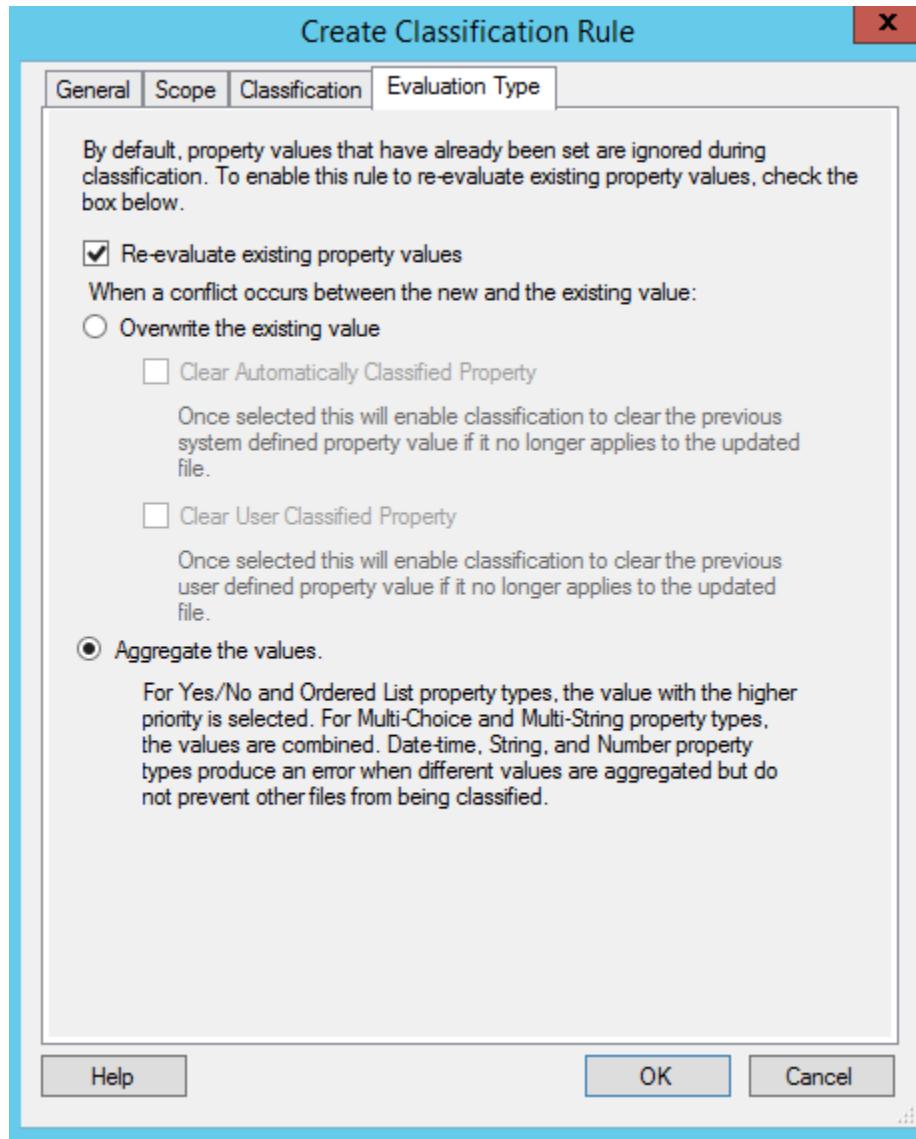
- Chuyển sang tab **Scope**, click vào **Add...** thêm vào thư mục **documents** trong ổ C.



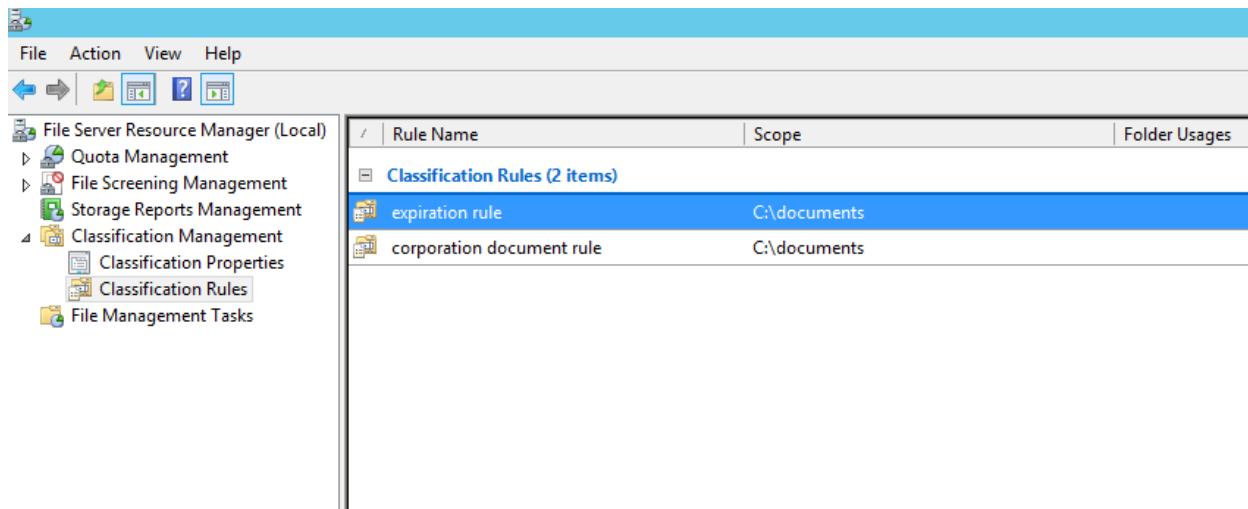
- Chuyển sang tab **Classification**, tại mục **Choose a method to assign a property to files**, chọn **Folder Classifier**, tại mục **Property** bên dưới, chọn **expiration date**.



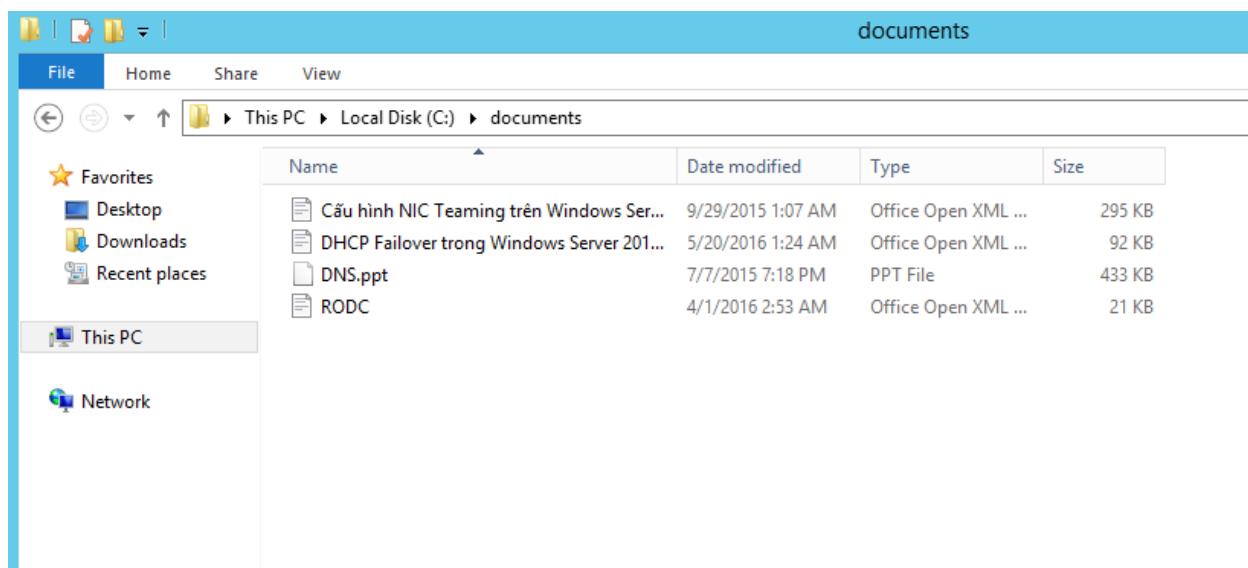
- Chuyển sang tab **Evaluation Type**, click chọn vào **Re-evaluate existing property values, OK.**



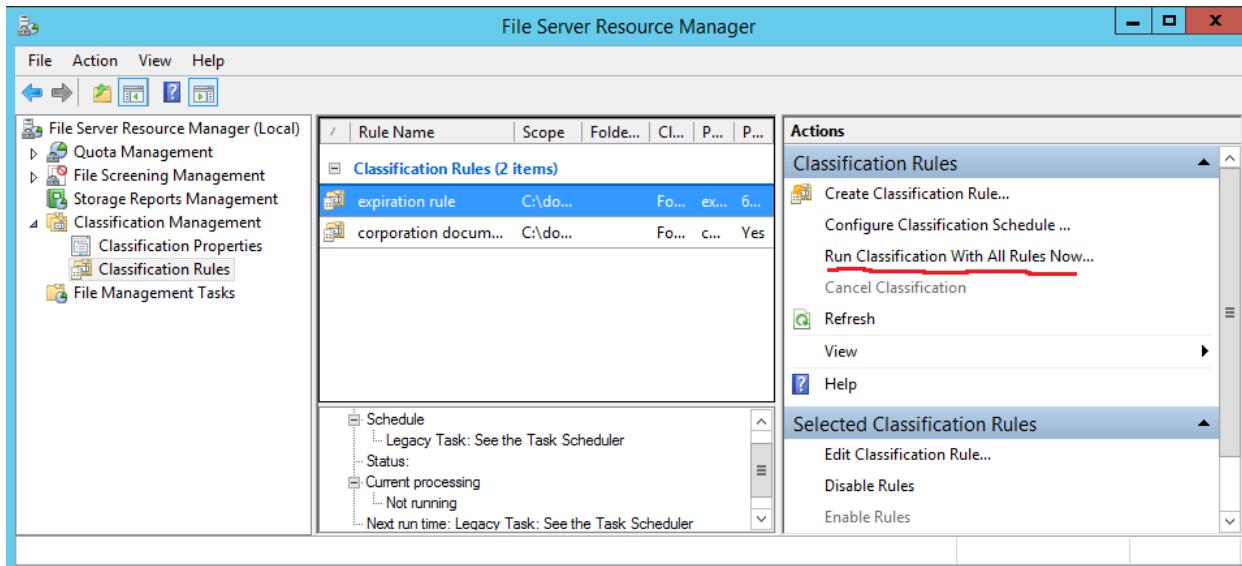
- Kiểm tra rule đã được tạo:



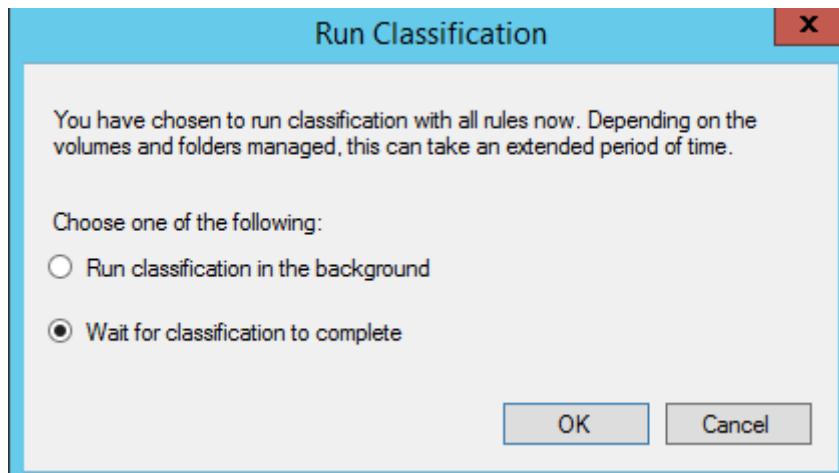
- Thực hiện copy một số file Word vào thư mục **documents** để kiểm tra.



- Tại **Classification Rule**, chọn vào **expiration rule**, click vào **Run Classification With All Rules Now...**



- Tại cửa sổ **Run Classification**, chọn vào **Wait for classification to complete**.



○ Kiểm tra báo cáo:



Automatic Classification Report	
Generated at: 6/16/2016 1:41:32 AM	
Report Description:	Lists files that were acted on by the classification policy. Use this report to understand how files were classified by the classification policy rules.
Machine:	BKAP-DC12-01
Report Folders:	'C:\documents'

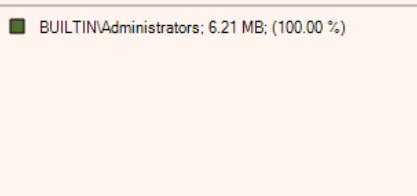
[Automatic Classification Report Table of Contents](#)

[Report Totals](#)
[Size by Owner](#)
[Size by File Group](#)
[Size by Property](#)
[Property: corporate documents Statistics](#)
[Property: expiration date Statistics](#)

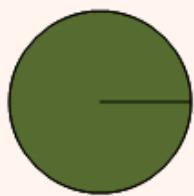
Report Totals					
Files shown in the report			All files matching report criteria		
Properties	Files	Total size on Disk	Properties	Files	Total size on Disk
2	6	6.21 MB	2	6	6.21 MB

[To top of the current report](#)

Size By Owner



Size by Owner		
Owner	Total size on Disk	Files
BUILTIN\Administrators	6.21 MB	6

Size By File Group**Size by File Group**

File Group	Total size on Disk	Files
Office Files	6.21 MB	6

[To top of the current report](#)**Size by Property**

Property	Total size on Disk	Files
corporate documents	6.21 MB	6
expirartion date	6.21 MB	6

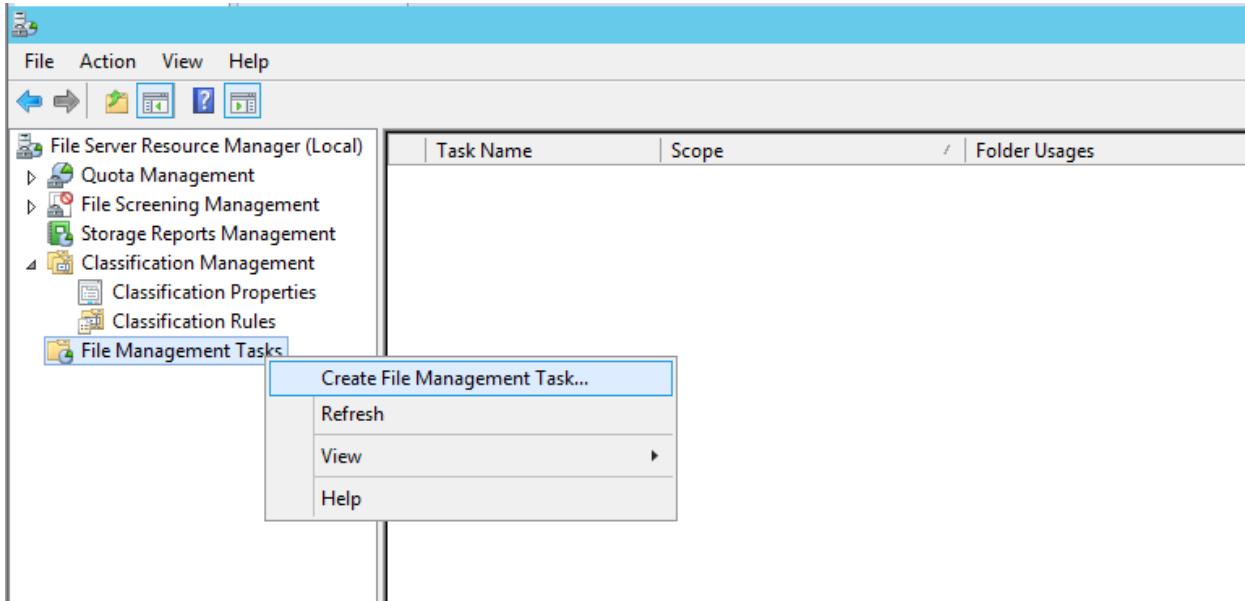
[To top of the current report](#)

Statistics for files by 'corporate documents'					
File name	Folder				
	Value	Rule	Last accessed	Last modified	Owner
Tạo và truy xuất thông tin Snapshot Active Directory trong Windows Server 2012.docx	C:\documents				
	Yes	corporation document rule	4/6/2016 12:26:21 AM	4/6/2016 12:26:21 AM	BUILTIN\Administrators
RODC.docx	C:\documents				
	Yes	corporation document rule	4/1/2016 2:53:53 AM	4/1/2016 2:53:54 AM	BUILTIN\Administrators
Active Directory tổng hợp.docx	C:\documents				
	Yes	corporation document rule	1/19/2016 7:51:52 PM	1/19/2016 7:47:07 PM	BUILTIN\Administrators
Làm việc với Read Only Domain Controller.docx	C:\documents				
	Yes	corporation document rule	12/2/2015 1:51:45 AM	8/2/2015 8:07:29 PM	BUILTIN\Administrators
DFS.docx	C:\documents				
	Yes	corporation document rule	12/2/2015 1:51:45 AM	8/2/2015 7:45:50 PM	BUILTIN\Administrators
Active Directory.doc	C:\documents				
	Yes	corporation document rule	12/2/2015 1:51:42 AM	7/30/2015 7:42:50 PM	BUILTIN\Administrators

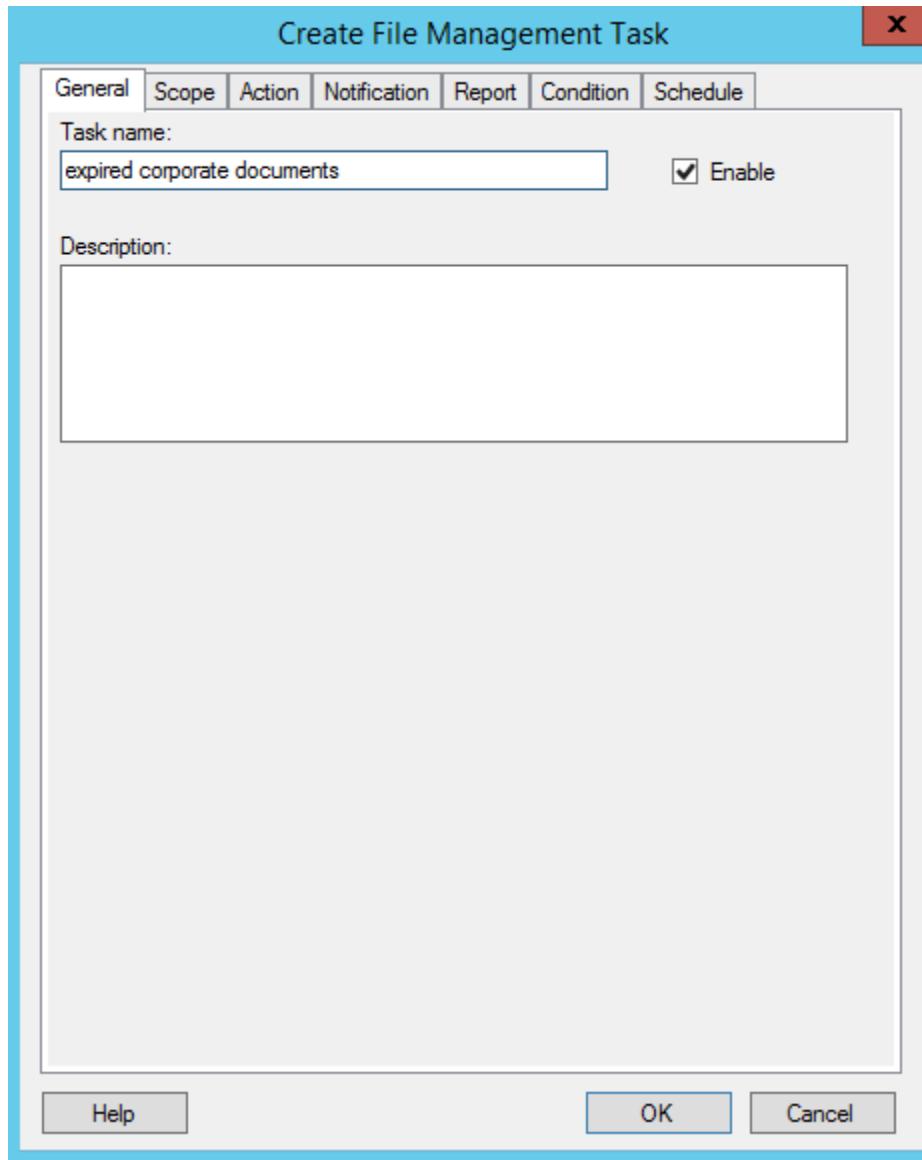
[To top of the current report](#)

Statistics for files by 'expirartion date'					
File name	Folder				
	Value	Rule	Last accessed	Last modified	Owner
Tạo và truy xuất thông tin Snapshot Active Directory trong Windows Server 2012.docx	C:\documents				
	6/16/2016 1:27:32 AM	expiration rule	4/6/2016 12:26:21 AM	4/6/2016 12:26:21 AM	BUILTIN\Administrators
RODC.docx	C:\documents				
	6/16/2016 1:27:32 AM	expiration rule	4/1/2016 2:53:53 AM	4/1/2016 2:53:54 AM	BUILTIN\Administrators
Active Directory tổng hợp.docx	C:\documents				
	6/16/2016 1:27:32 AM	expiration rule	1/19/2016 7:51:52 PM	1/19/2016 7:47:07 PM	BUILTIN\Administrators
Làm việc với Read Only Domain Controller.docx	C:\documents				
	6/16/2016 1:27:32 AM	expiration rule	12/2/2015 1:51:45 AM	8/2/2015 8:07:29 PM	BUILTIN\Administrators
DFS.docx	C:\documents				
	6/16/2016 1:27:32 AM	expiration rule	12/2/2015 1:51:45 AM	8/2/2015 7:45:50 PM	BUILTIN\Administrators
Active Directory.doc	C:\documents				
	6/16/2016 1:27:32 AM	expiration rule	12/2/2015 1:51:42 AM	7/30/2015 7:42:50 PM	BUILTIN\Administrators

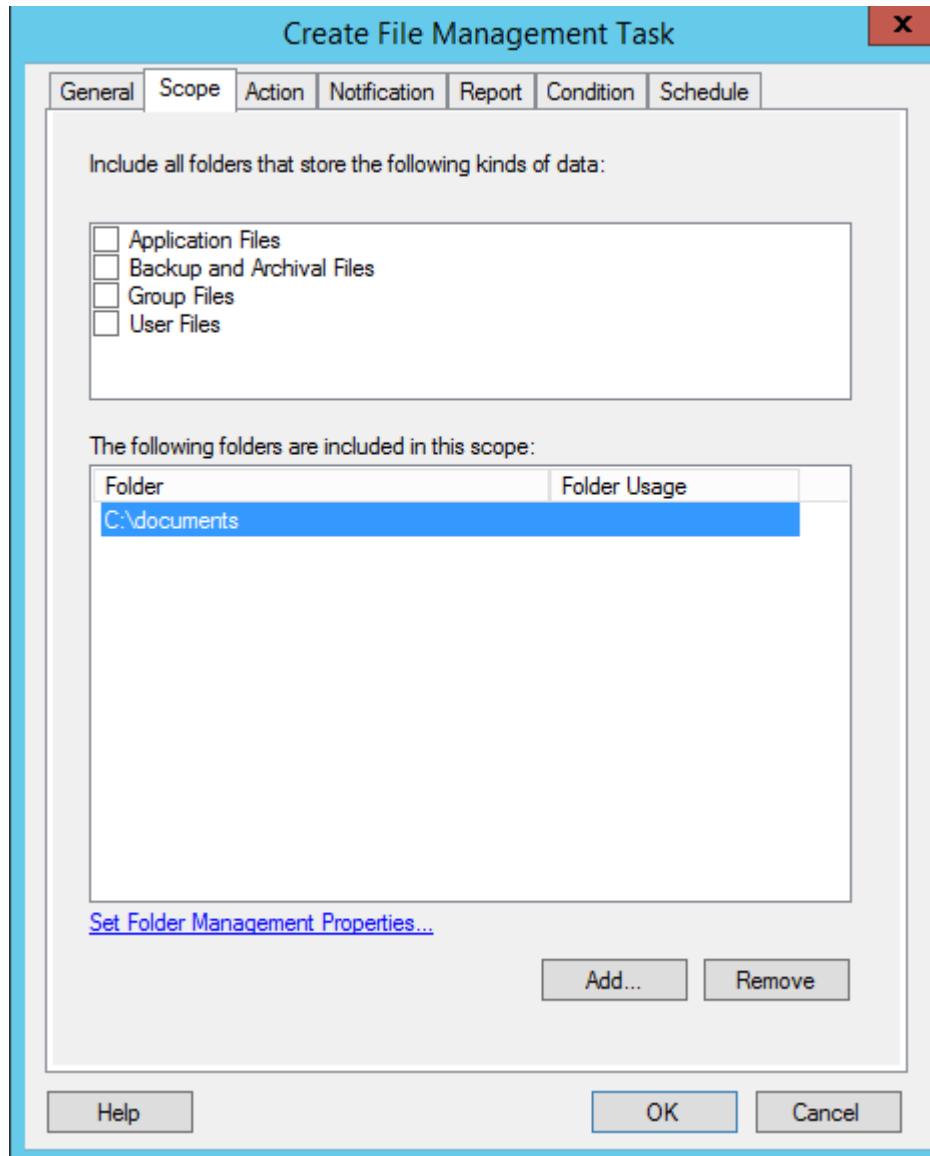
- Trong cửa sổ **File Server Resource Manager**, click chuột phải tại **File Management Tasks**, chọn **Create File Management Task...**



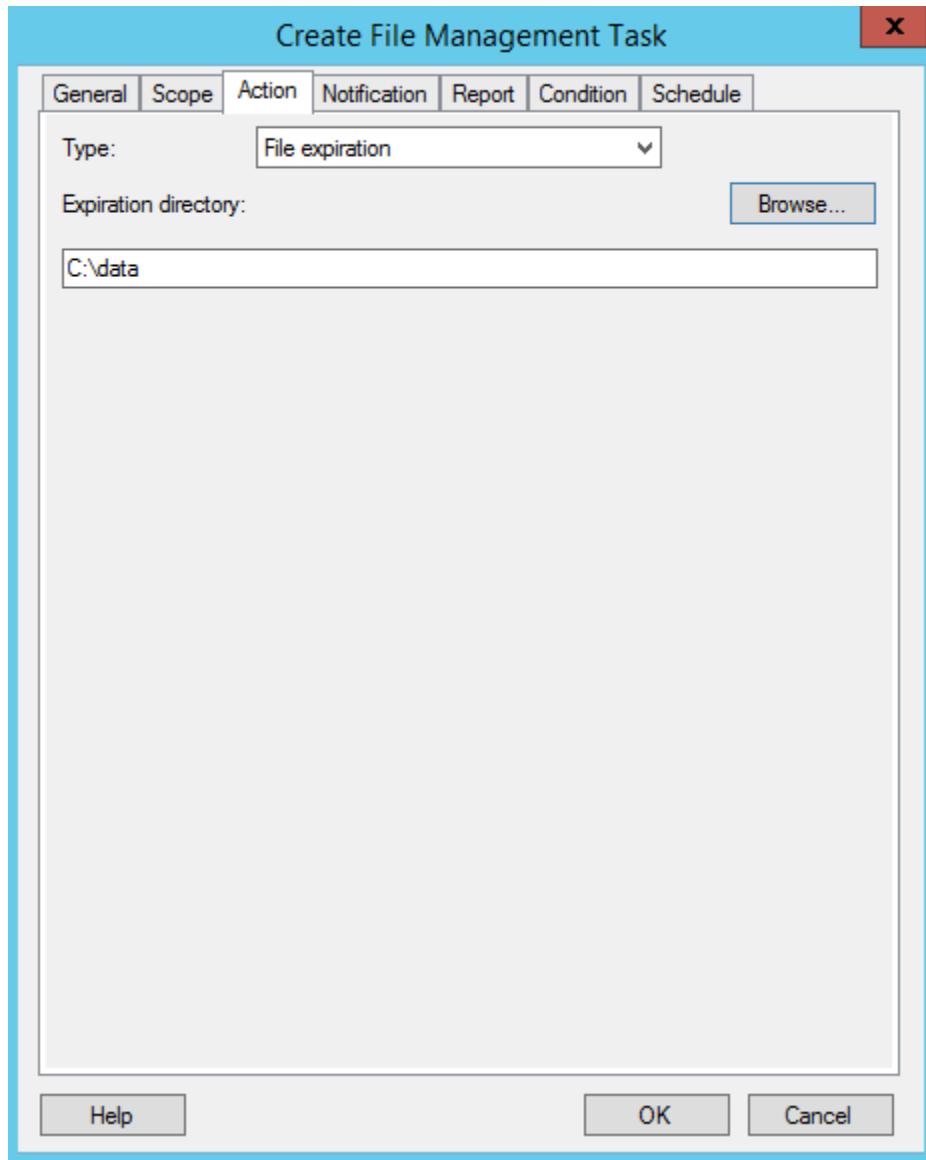
- Trong cửa sổ **Create File Management Task**, tại tab **General**, trong mục **Task name**, nhập vào tên **expired corporate documents**.



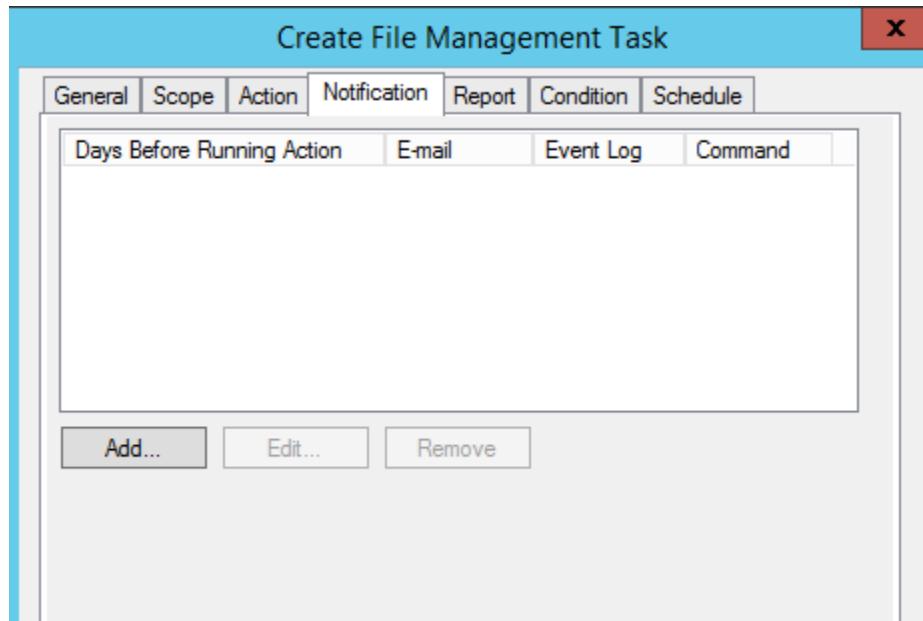
- Chuyển sang tab **Scope**, click vào **Add...** thêm vào thư mục **documents** trong ổ C.



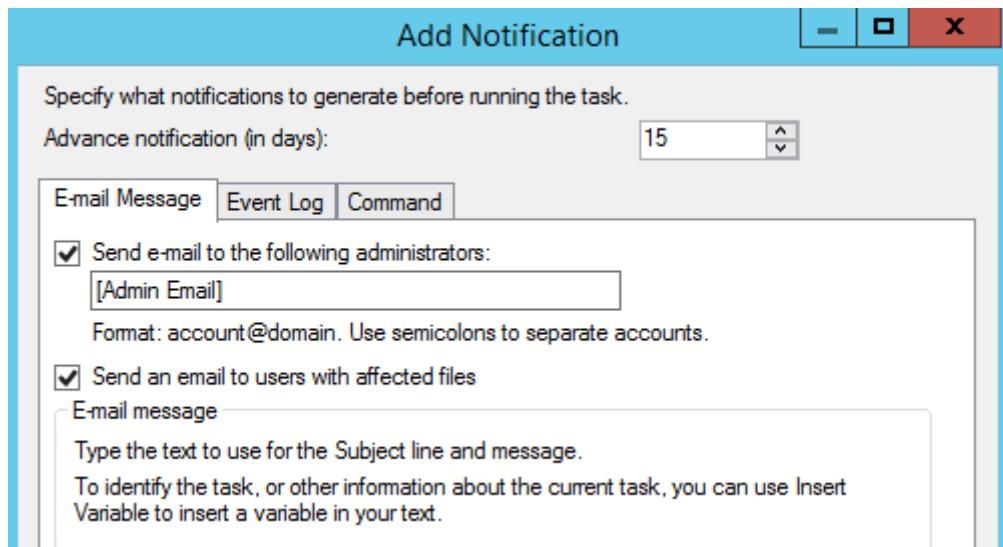
- Chuyển sang tab Action, click vào Browse..., tìm đến thư mục data trong ô C.



- Chuyển sang tab **Notification**, click vào **Add...**

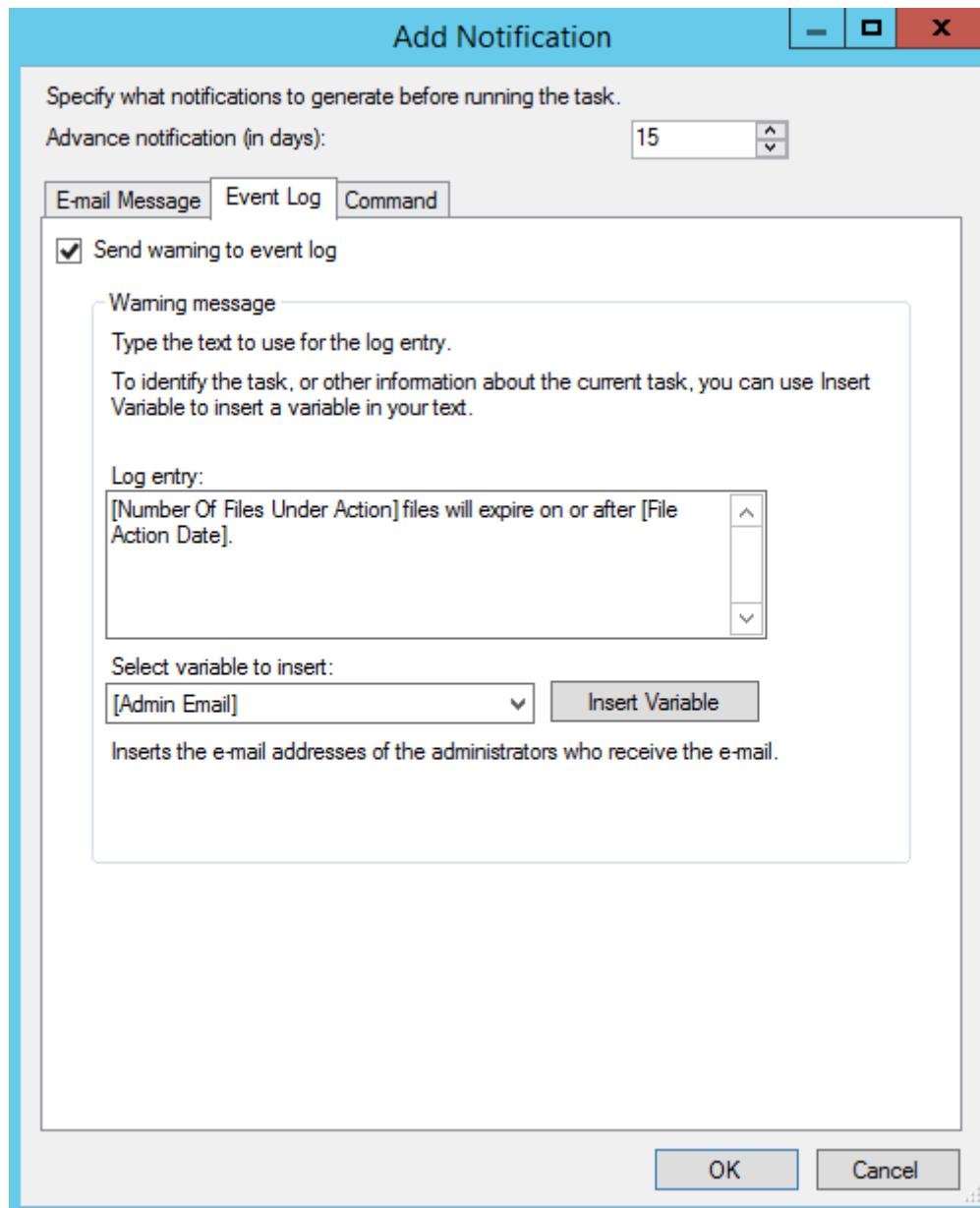


- Trong cửa sổ **Add Notification**, trong tab **E-mail Message**, click chọn vào **Send e-mail to the following administrators** và **Send e-mail to users with effected files**.

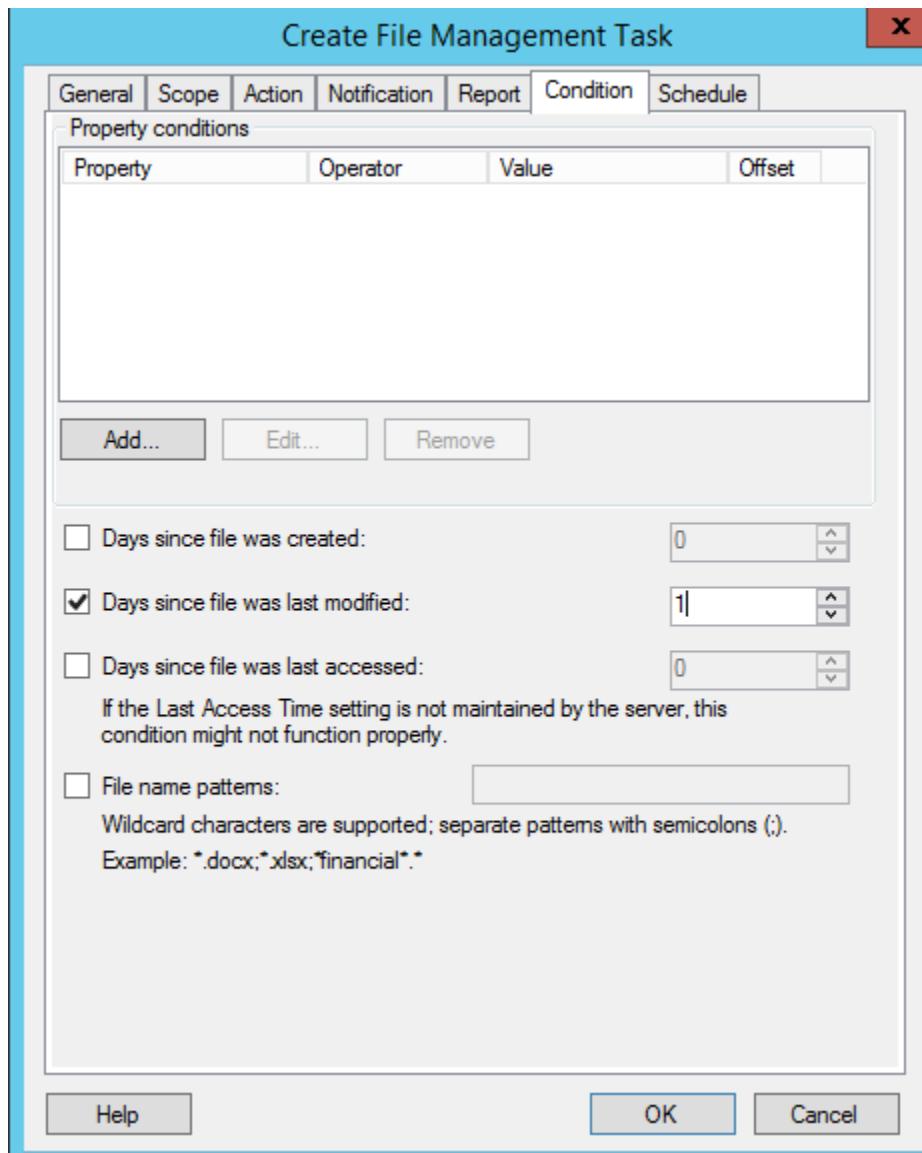


- Chuyển sang tab **Event Log**, click chọn vào **Send warning to event log**.

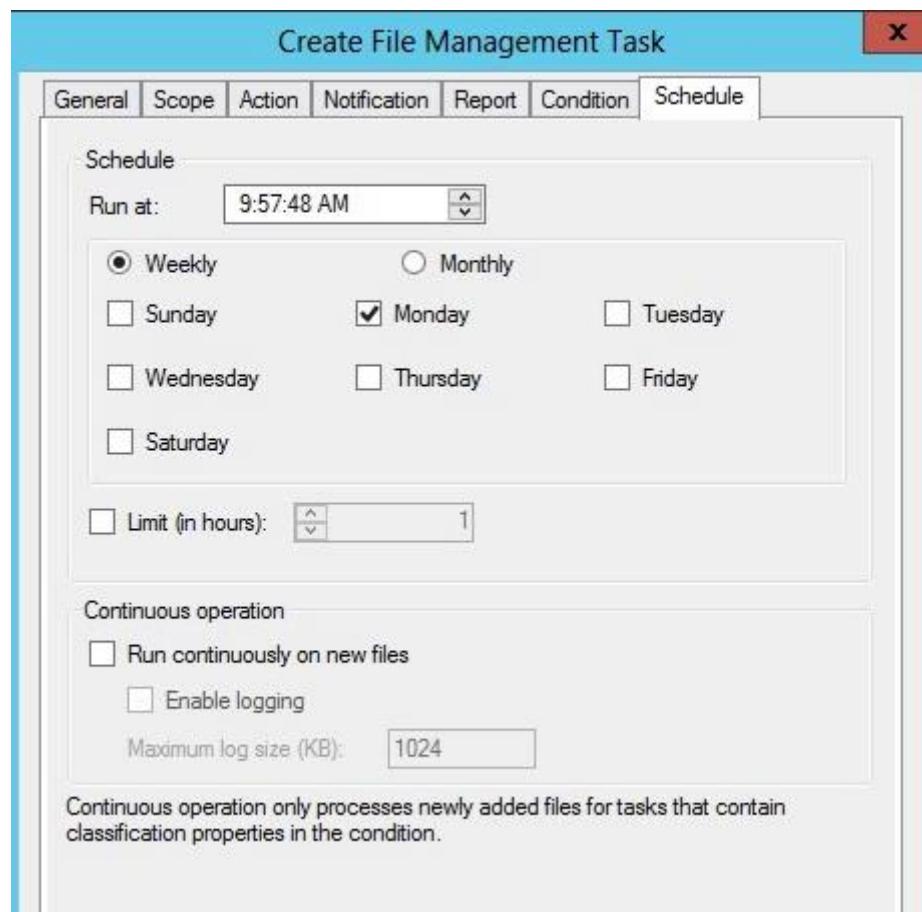
⇒ **OK.**



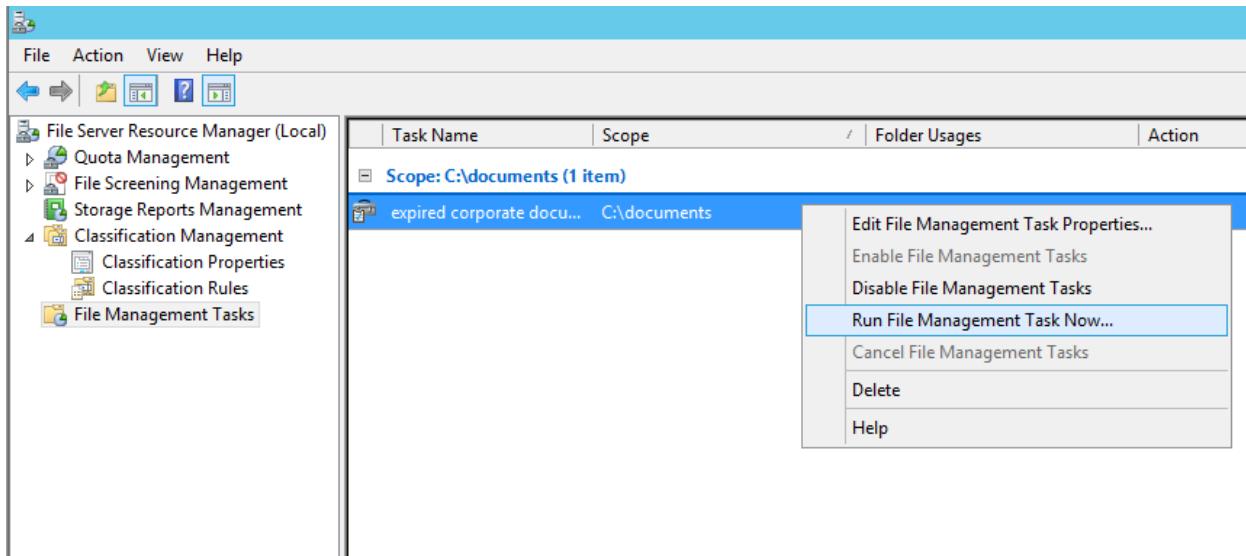
- Trong cửa sổ **Create File Management Task**, chuyển sang tab **Condition**, click chọn vào **Day since file was last modified**, nhập vào thông số 1.



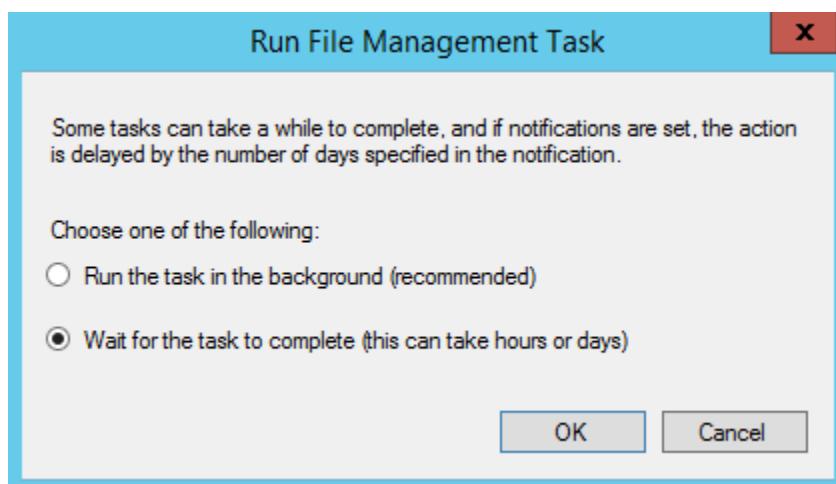
- Chuyển sang tab **Schedule**, điều chỉnh thời gian.=> **OK**.



- Click chuột phải vào **expired corporate documents** vừa tạo, chọn **Run File Management Task Now...**



- Tại cửa sổ **Run File Management Task**, click chọn vào **Wait for the task to complete (this can take hours or days)**.



- Kiểm tra báo cáo:

File Management Task Report	
Generated at: 6/16/2016 2:13:51 AM	
Report Description:	Report for files subject to action by File Management Task: expired corporate documents
Action Type:	expiration - Expiration directory C:\data\BKAP-DC12-01\2016-06-16_02-13-51
Machine:	BKAP-DC12-01
Report Folders:	'C:\documents'

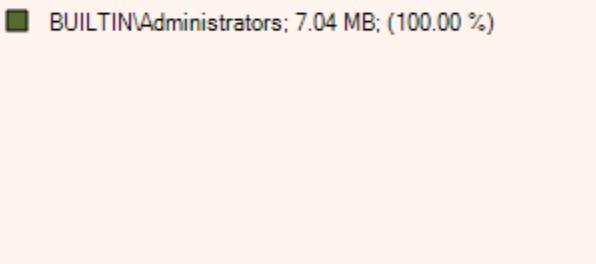
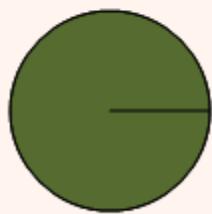
File Management Task Report Table of Contents

[Report Totals](#)
[Size by Owner](#)
[Size by File Group](#)
[Report statistics](#)
[Report Error for Files](#)

Report Totals			
Files shown in the report		All files matching report criteria	
Files	Total size on Disk	Files	Total size on Disk
9	7.04 MB	9	7.04 MB

[To top of the current report](#)

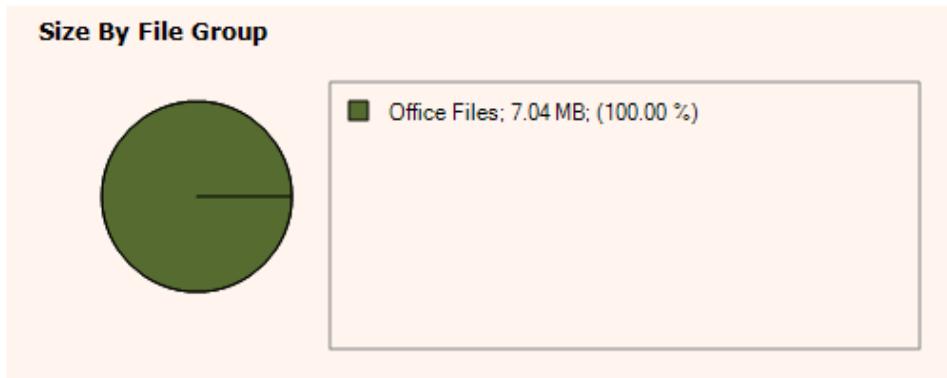
Size By Owner



Size by Owner		
Owner	Total size on Disk	Files
BUILTIN\Administrators	7.04 MB	9

Size by Owner		
Owner	Total size on Disk	Files
BUILTIN\Administrators	7.04 MB	9

[To top of the current report](#)



Size by File Group		
File Group	Total size on Disk	Files
Office Files	7.04 MB	9

[To top of the current report](#)

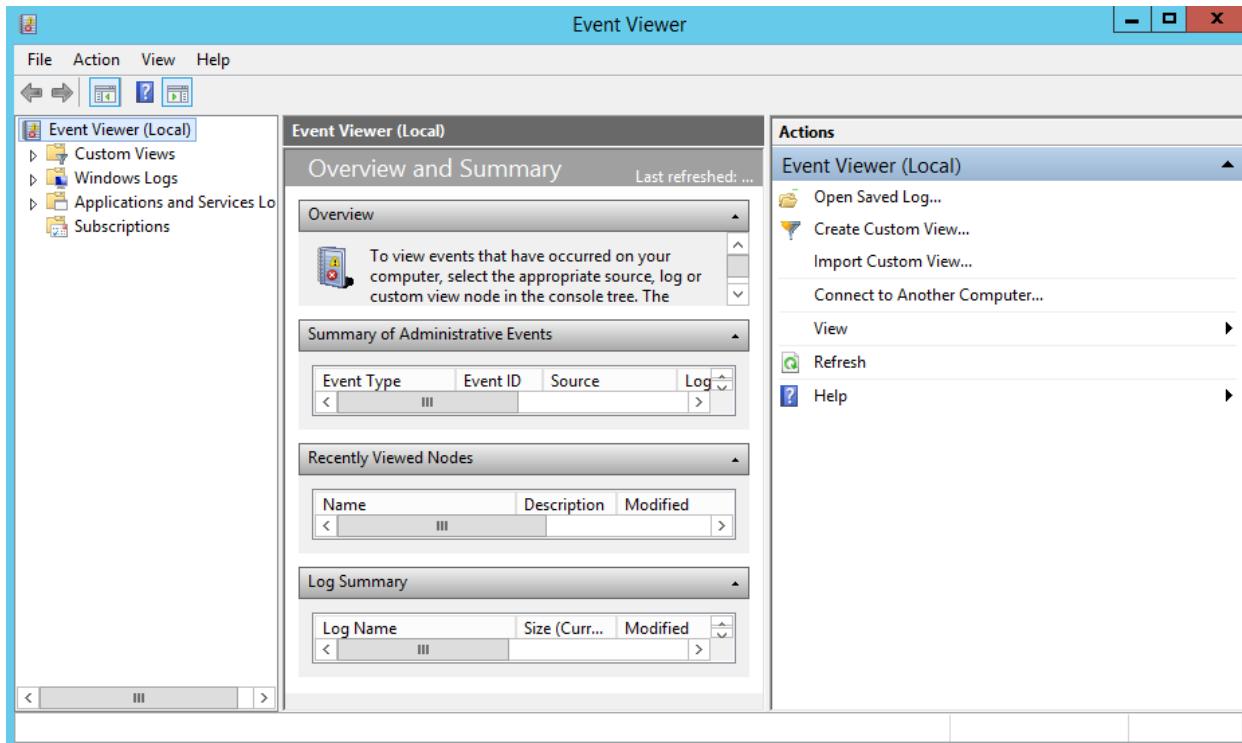
Report statistics						
File name	Folder					
	Owner	Size on Disk	Size	Created	Last accessed	Last modified
Active Directory.doc	C:\documents	BUILTIN\Administrators	3.21 MB	3.21 MB	12/2/2015 1:51:42 AM	12/2/2015 1:51:42 AM
Active Directory tổng hợp.docx	C:\documents	BUILTIN\Administrators	2.35 MB	2.34 MB	1/19/2016 7:46:55 PM	1/19/2016 7:51:52 PM
Làm việc với Read Only Domain Controller.docx	C:\documents	BUILTIN\Administrators	0.51 MB	0.51 MB	12/2/2015 1:51:45 AM	12/2/2015 1:51:45 AM
DNS.ppt	C:\documents	BUILTIN\Administrators	0.43 MB	0.42 MB	6/16/2016 1:41:08 AM	6/16/2016 1:41:08 AM
Cấu hình NIC Teaming trên Windows Server 2012.docx	C:\documents	BUILTIN\Administrators	0.29 MB	0.29 MB	6/16/2016 1:41:08 AM	6/16/2016 1:41:08 AM
DFS.docx	C:\documents	BUILTIN\Administrators	0.10 MB	0.10 MB	12/2/2015 1:51:45 AM	12/2/2015 1:51:45 AM
DHCP Failover trong Windows Server 2012 R2.docx	C:\documents	BUILTIN\Administrators	0.09 MB	0.09 MB	6/16/2016 1:41:08 AM	6/16/2016 1:41:08 AM
RODC.docx	C:\documents	BUILTIN\Administrators	0.03 MB	0.02 MB	12/2/2015 1:51:45 AM	4/1/2016 2:53:53 AM
Tạo và truy xuất thông tin Snapshot Active Directory trong Windows Server 2012.docx	C:\documents	BUILTIN\Administrators	0.02 MB	0.02 MB	4/6/2016 12:26:21 AM	4/6/2016 12:26:21 AM

[To top of the current report](#)

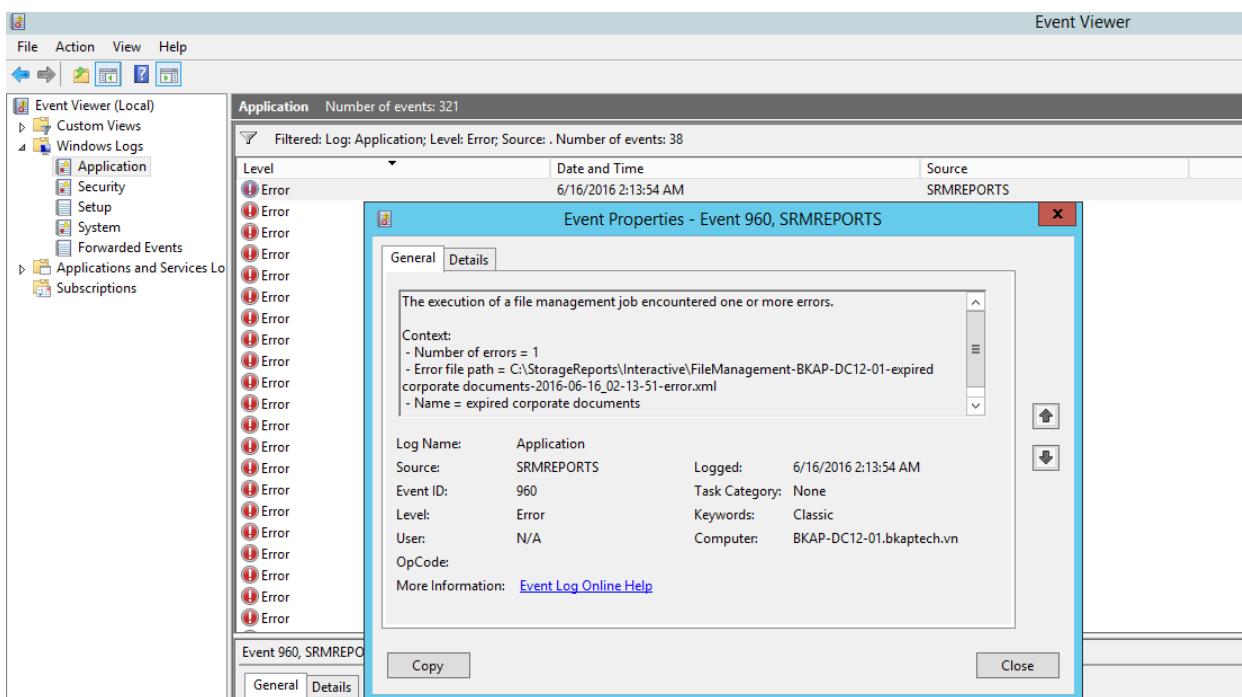
Error for files	
File	Folder
name	Error
	Owner

[To top of the current report](#)

- Vào Server Manager / Tools / Event Viewer.



- Trong cửa sổ Event Viewer, chọn vào Windows Logs / Application.
 - Thực hiện kiểm tra các event Error, có Source SRMREPORTS/SRMSVC



Bài 3:**TRIỂN KHAI CẤU HÌNH DYNAMIC ACCESS CONTROL**

Các nội dung chính được đề cập:

- ✓ Cấu hình Dynamic Access Control.

3.Cấu hình Dynamic Access Control (DAC)**1.Yêu cầu bài lab:**

Phân quyền truy cập trên các file/folder với những điều kiện dựa vào *User Claim*, *Device Claim*, hay *Resource Claim* cho phép điều khiển quyền hạn truy cập linh hoạt hơn so với phân quyền NTFS truyền thống như sau:

- Cấu hình **DAC** nhằm mục đích phân quyền cho phép truy cập vào thư mục BaoCao khi User thỏa mãn tất cả các kiều kiện:

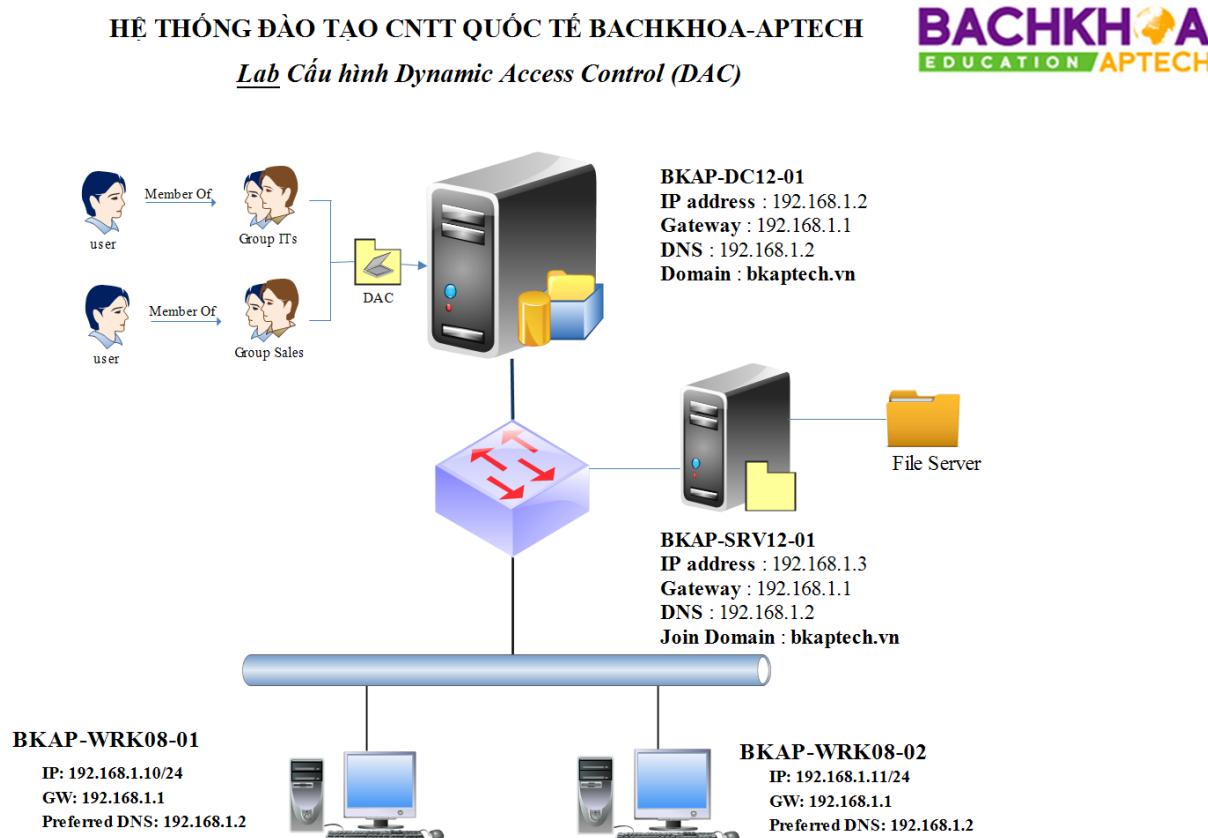
- + Là thành viên group **ITs**.
- + Có thuộc tính Department là *ChuyenMon*.
- + Phải logon trên máy tính chỉ định.

2.Yêu cầu chuẩn bị:

Chuẩn bị các máy theo yêu cầu sau:

- + *BKAP-DC12-01* : đã nâng cấp lên Domain Controller với tên miền **bkaptech.vn**.
- + *BKAP-SRV12-01* : File Server.
- + *BKAP-WRK08-01* : Client chạy Windows 8.

3.Mô hình lab:

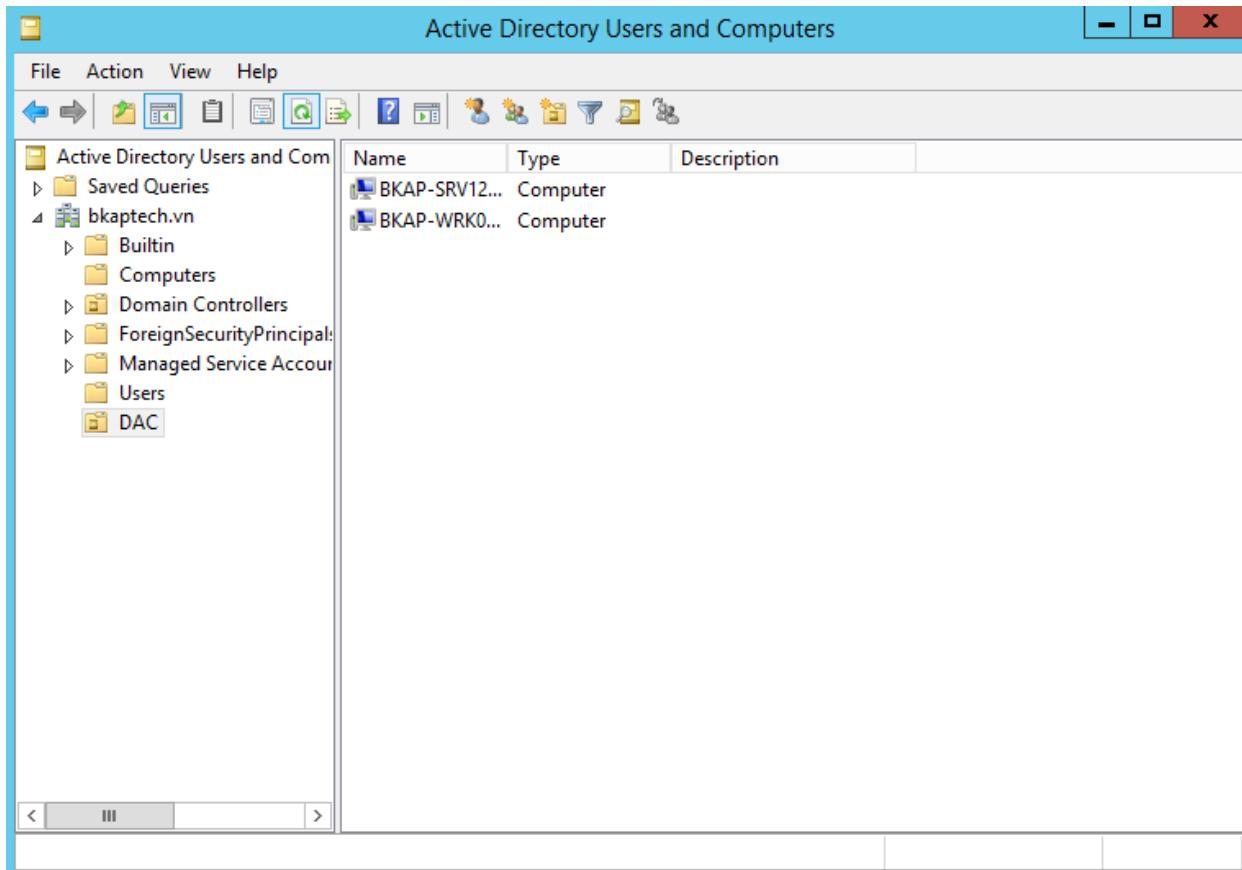


Sơ đồ địa chỉ như sau:

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:**Phần 1: Phân quyền truy cập dữ liệu:**

- Trên máy **BKAP-DC12-01**, thực hiện tạo ou **DAC** , move máy **File Server BKAP-SRV12-01** và Client **BKAP-WRK08-01** vào ou **DAC**.

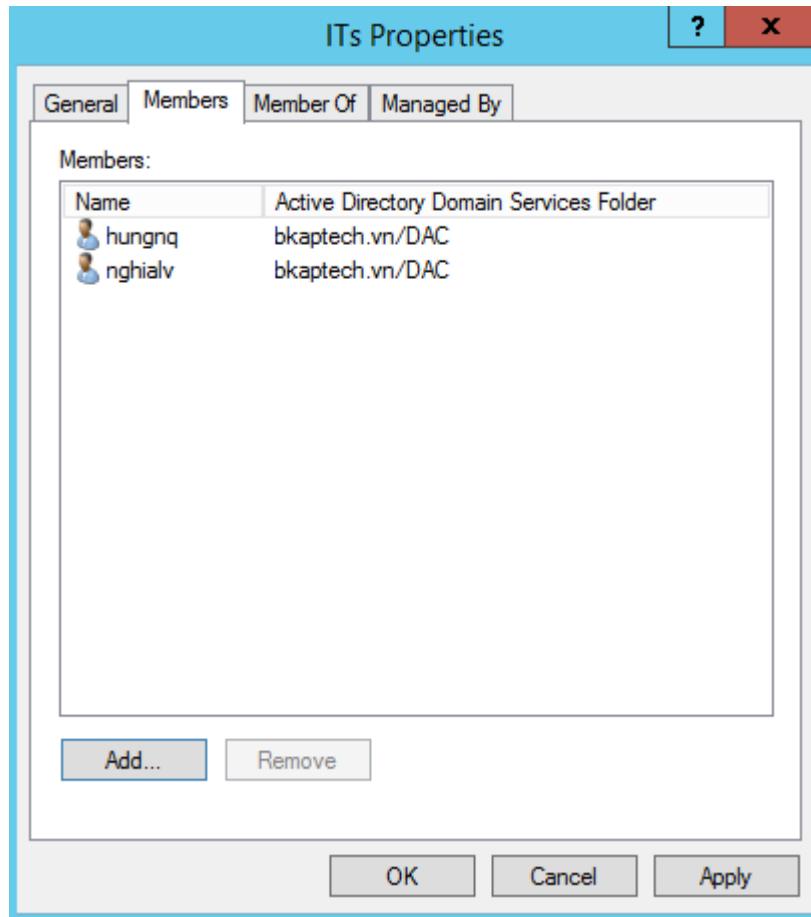


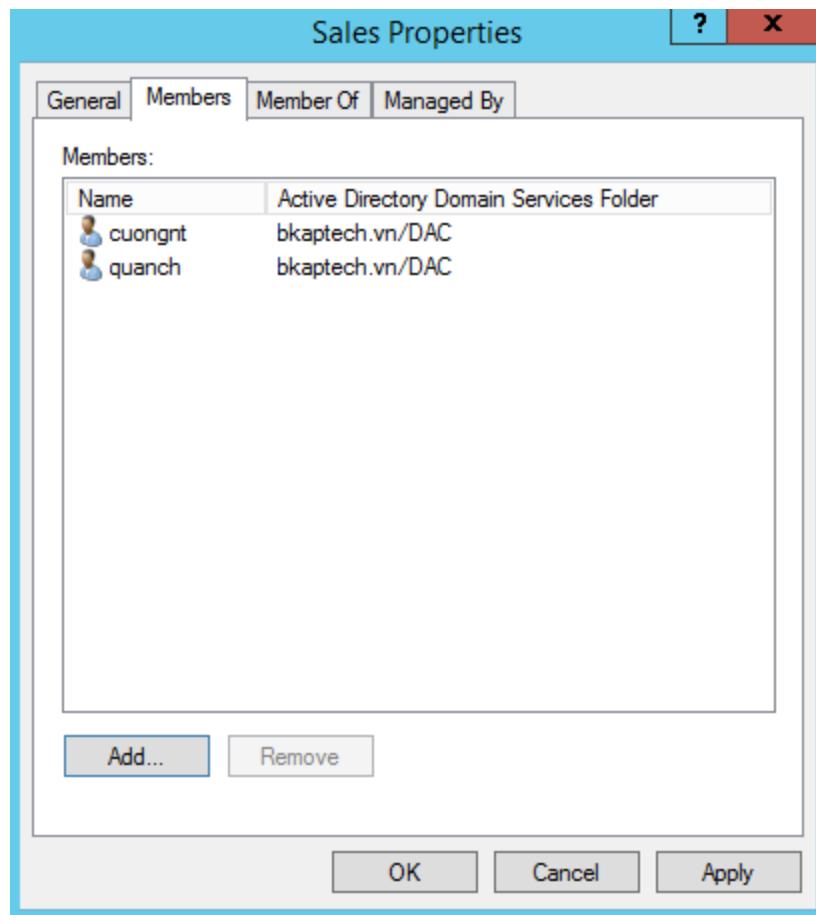
- Trong ou **DAC** , tạo group **ITs** và **Sales** , tạo 4 User : *hungnq , nghialv , cuongnt , quanch.*

The screenshot shows the Windows Active Directory Users and Computers (ADUC) management console. The left pane displays the navigation tree under 'Active Directory Users and Computers' for the domain 'bkaptech.vn'. The right pane is a table listing objects:

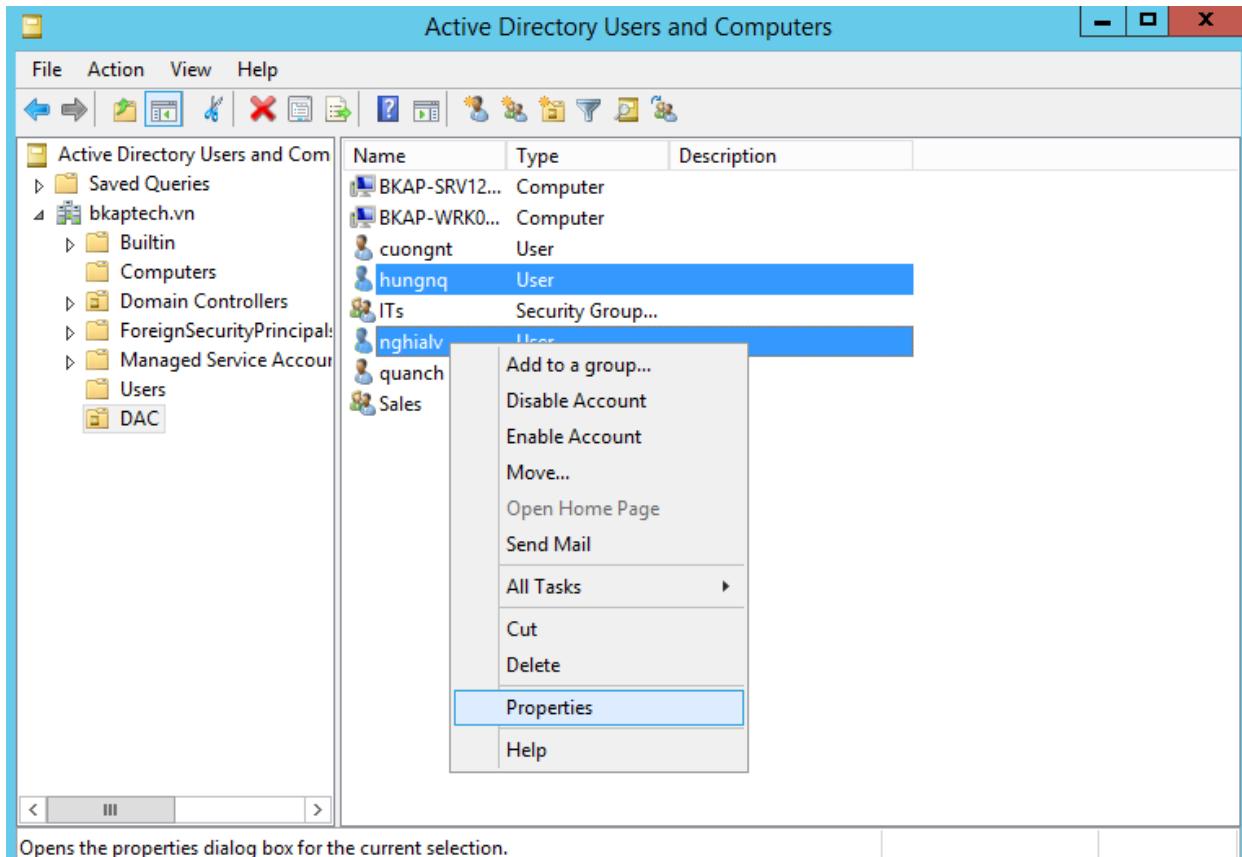
Name	Type	Description
BKAP-SRV12...	Computer	
BKAP-WRK0...	Computer	
cuongnt	User	
hungnq	User	
ITs	Security Group...	
nghialv	User	
quanch	User	
Sales	Security Group...	

- Thực hiện add user *hungnq* , *nghialv* vào group **ITs** , add user *cuongnt* , *quanch* vào group **Sales**.





- Điều chỉnh thuộc tính Department là “ChuyenMon” cho 2 user *hungnq* và *nghialv*.
 - Chọn cả 2 User / **Properties**.



- Chuyển sang Tab **Organization**, đánh dấu chọn vào ô **Department**, nhập vào “*ChuyenMon*”.

Properties for Multiple Items ? 

General Account Address Profile Organization

To change a property for multiple objects, first select the checkbox to enable the change, and then type the change.

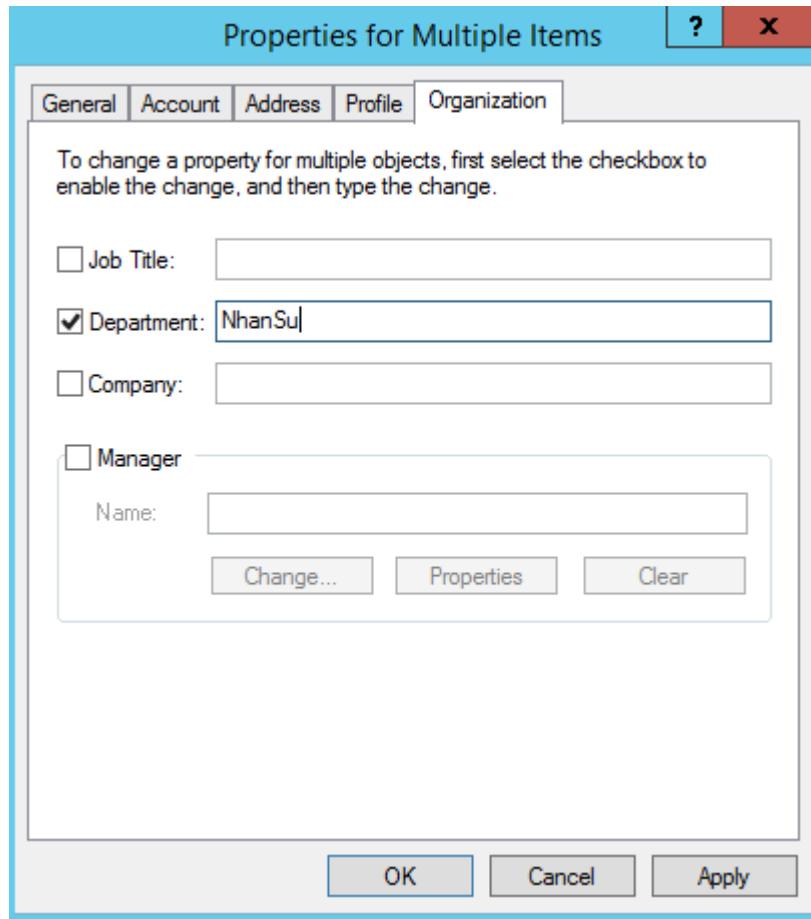
Job Title:

Department: ChuyenMon

Company:

Manager
Name:

- Tương tự , điều chỉnh thuộc tính Department là “NhanSu” cho 2 user cuongnt và quanch.



- Thực hiện **gpupdate /force** trên tất cả các máy để cập nhật Policy.

```

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

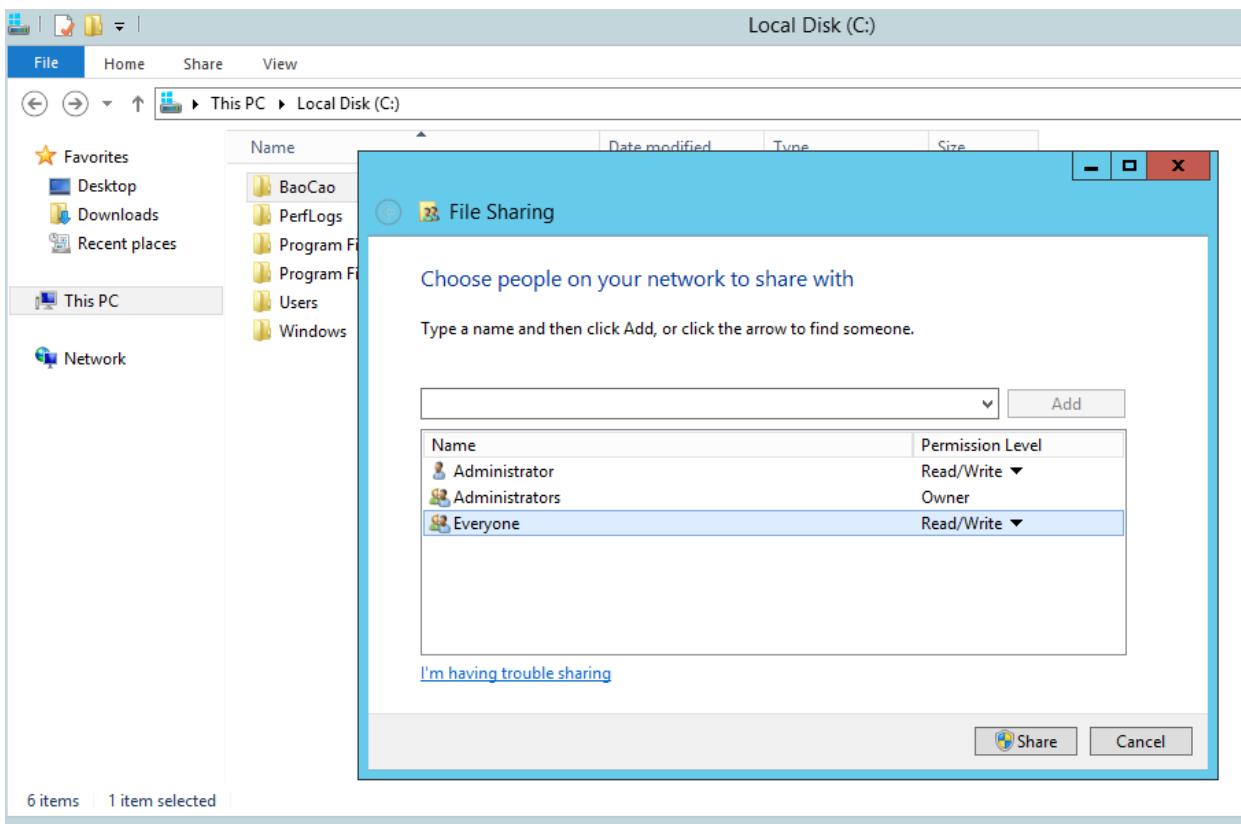
C:\Users\Administrator>gpupdate /force
Updating policy...

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

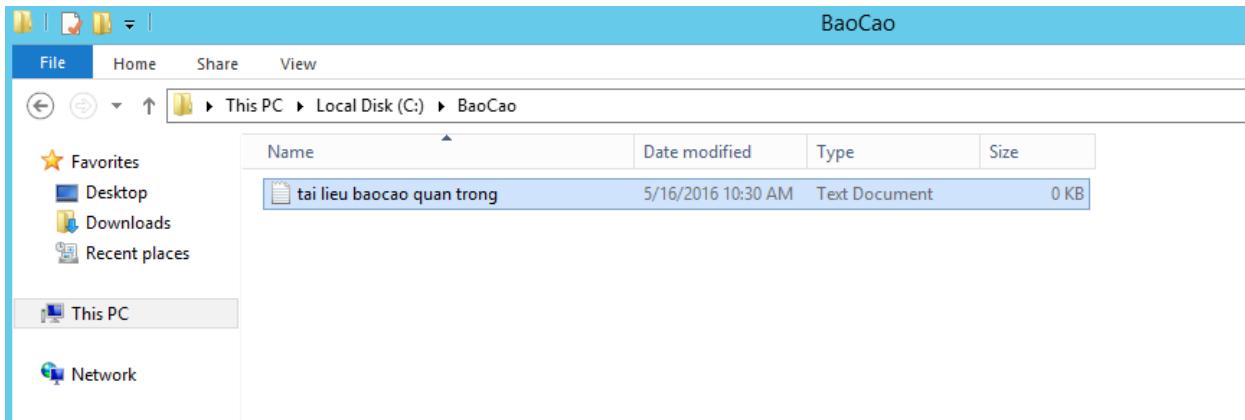
C:\Users\Administrator>

```

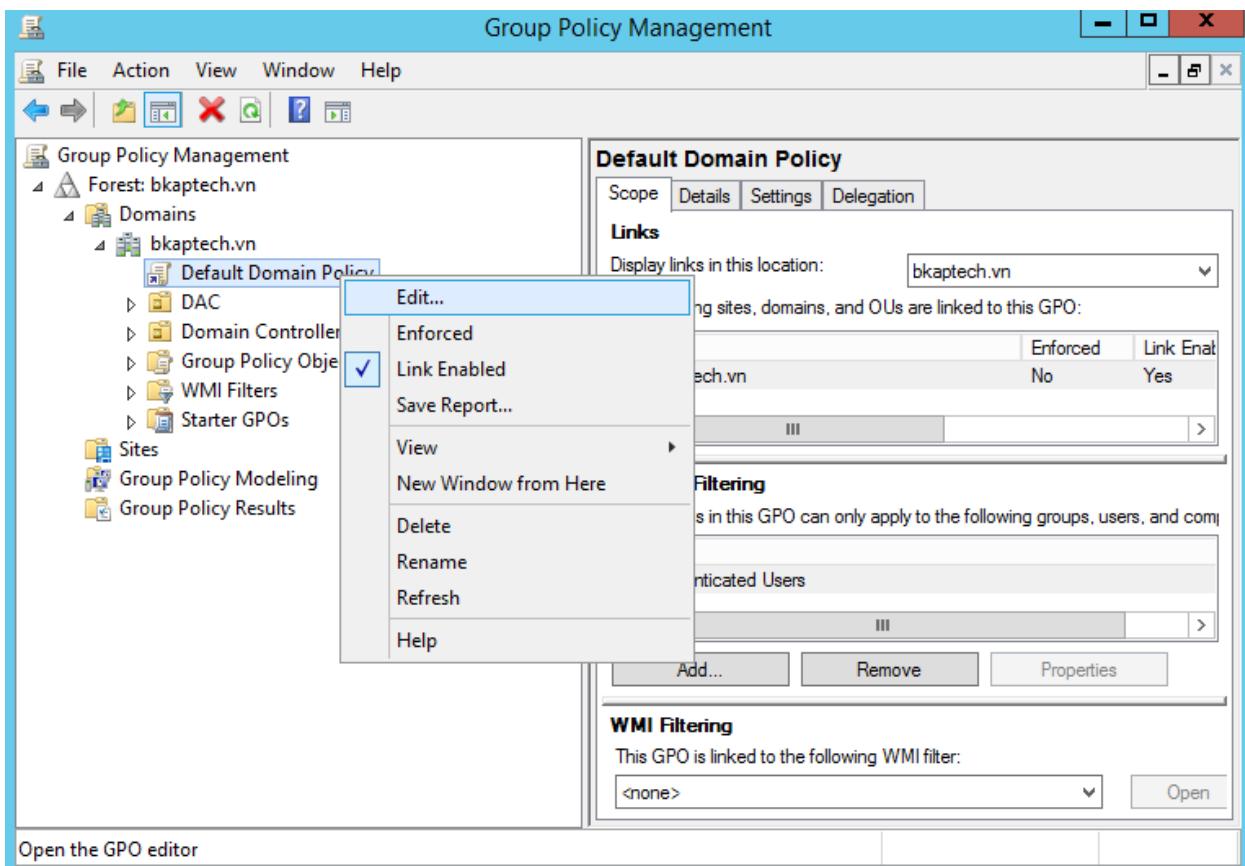
- Chuẩn bị dữ liệu cho *File Server*, trên máy *BKAP-SRV12-01* (*File Server*) , tạo Folder tên “**BaoCao**” , thực hiện share folder này cấp quyền *Read/Write* cho *EveryOne*.



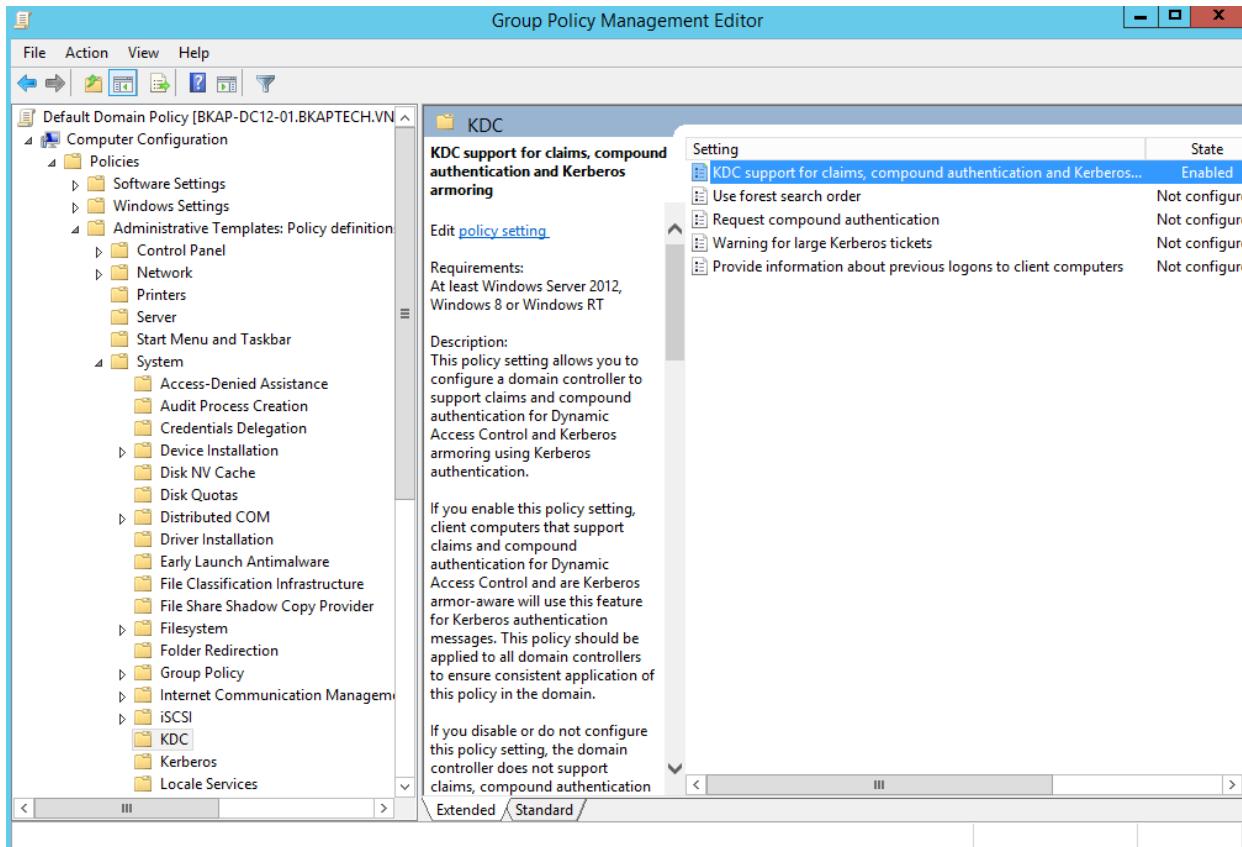
- Tạo file tùy ý trong thư mục **BaoCao**.



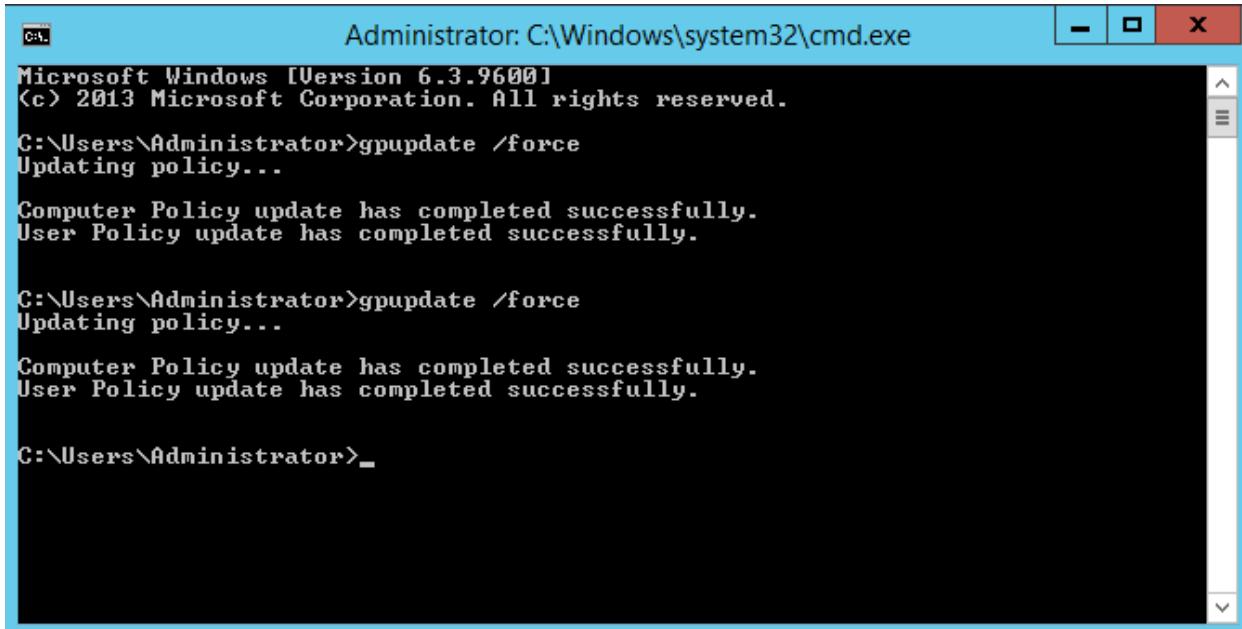
- Cấu hình policy cho phép chứng thực **Keberos** trên tất cả các thành viên của domain để hỗ trợ **DAC**.
 - Trên máy **BKAP-DC12-01** , vào **Group Policy Management** , click chuột phải tại **Default Domain Policy** chọn **Edit**.



- Chọn tiếp Computer Configuration / Policies / Administrative Templates / System / KDC => Chọn vào KDC support for claims , compound authentication... => click chuột phải tại đây chọn Edit => Enable => OK.



- Thực hiện **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...

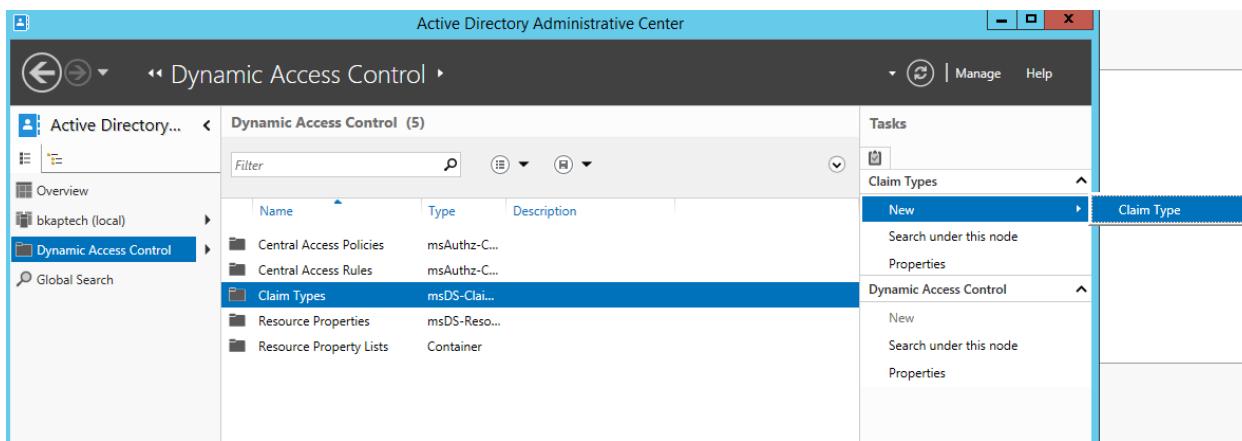
Computer Policy update has completed successfully.
User Policy update has completed successfully.

C:\Users\Administrator>_

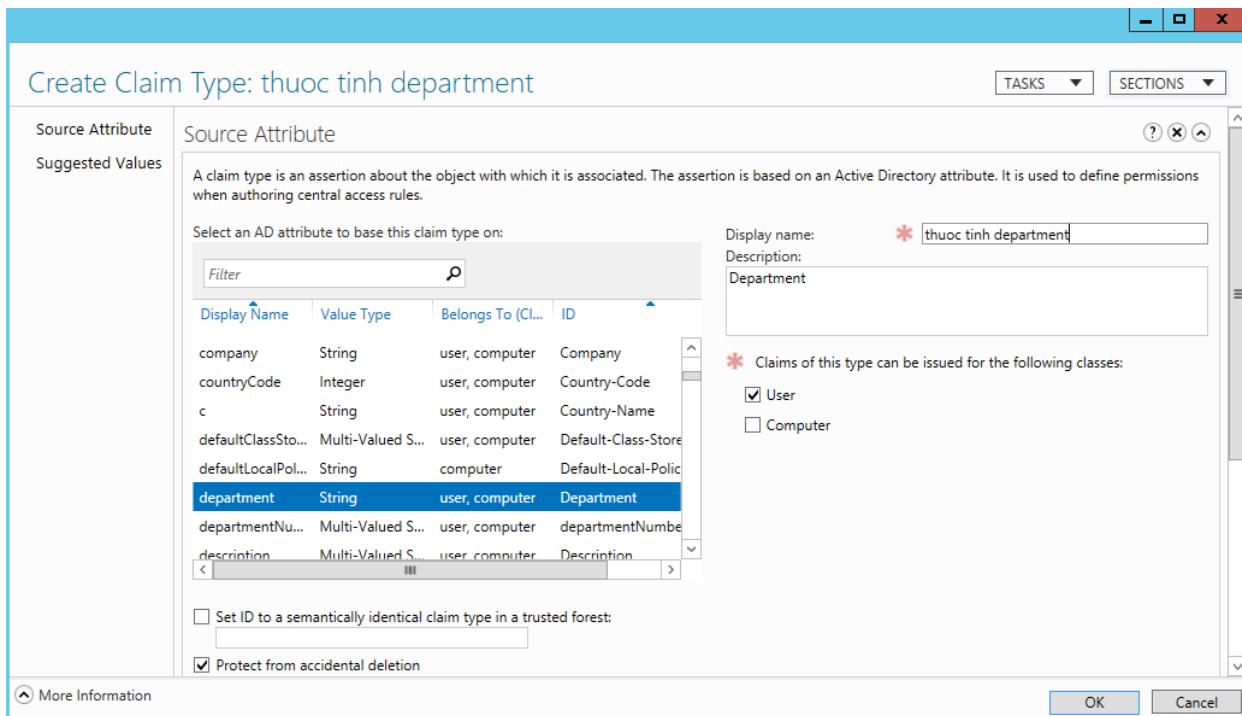
```

- Cấu hình **Dynamic Access Control (DAC)**.

- Trên *BKAP-DC12-01* , chọn **Active Directory Administrative Center** (các thao tác cấu hình DAC đều dùng công cụ này).
 - Trong cửa sổ **Active Directory Administrative Center** , chọn vào **Dynamic Access Control / Claim Types => click vào New / Claim Type**.



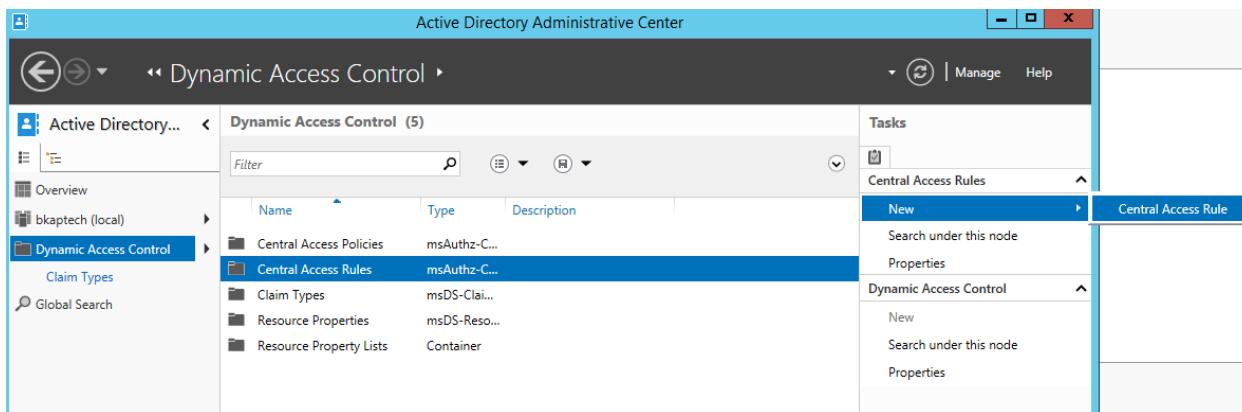
- Trong cửa sổ **Create Claim Type**, tìm kiếm thuộc tính “*department*”, đặt tên “*thuoc tinh department*” / OK.



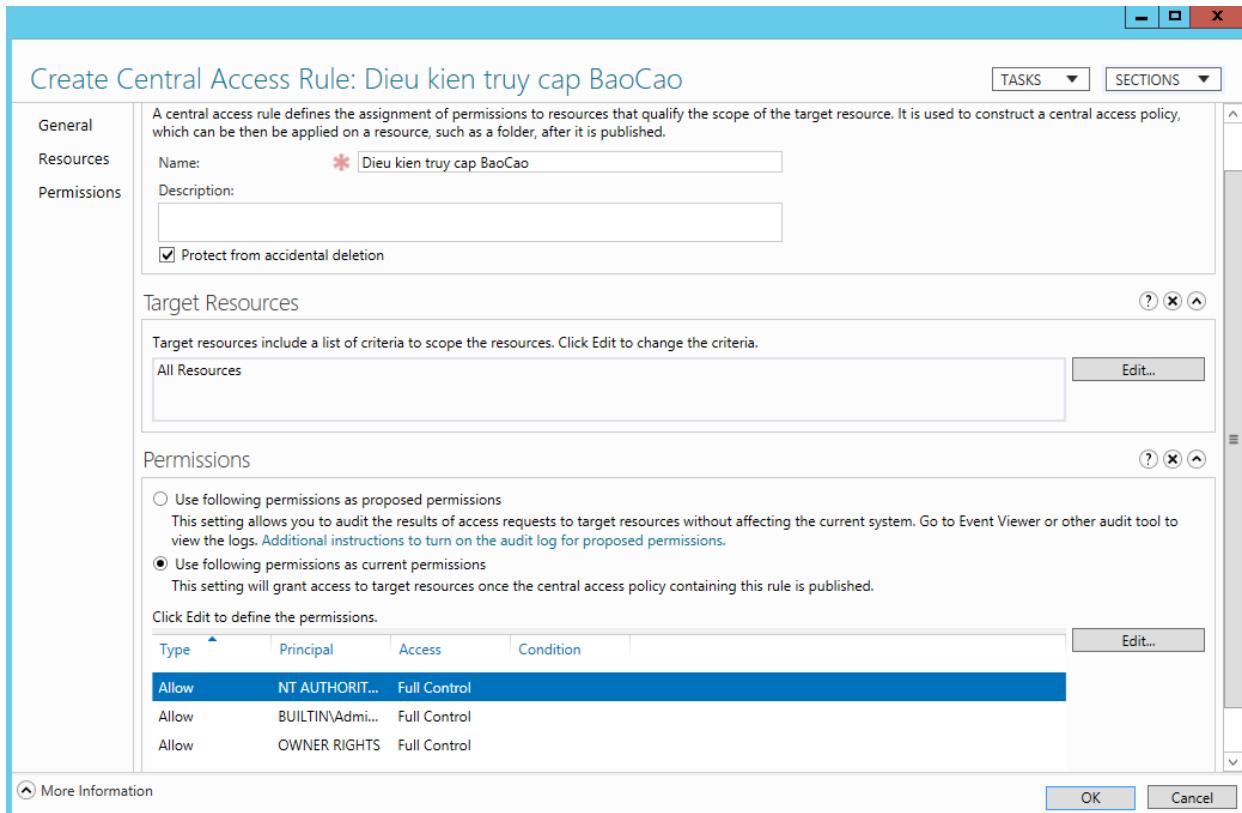
- Kiểm tra **Claim** vừa tạo bằng cách click vào **Claim Types**:

▪ **Tạo Central Access Rule:**

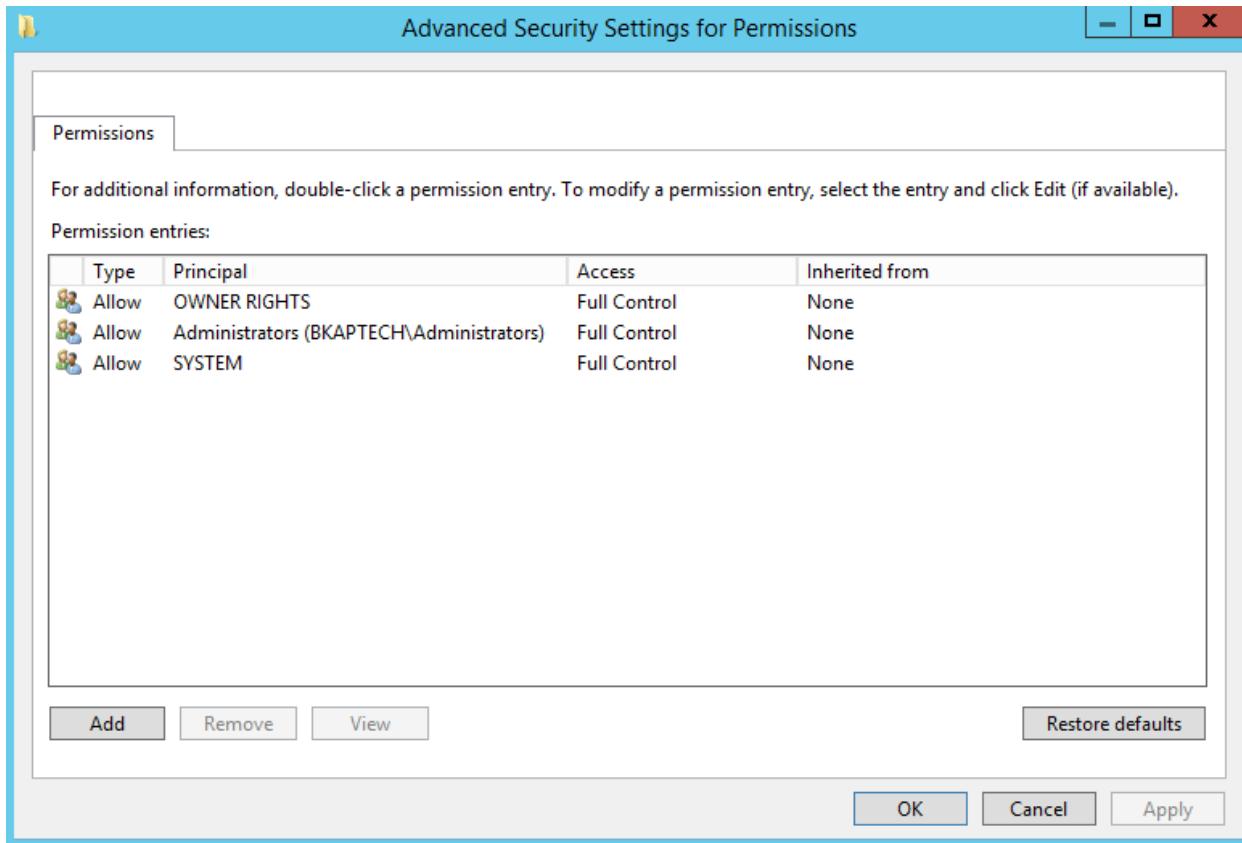
- Tại cửa sổ **Active Directory Administrative Center / Dynamic Access Control / Central Access Rule => New / Central Access Rule.**



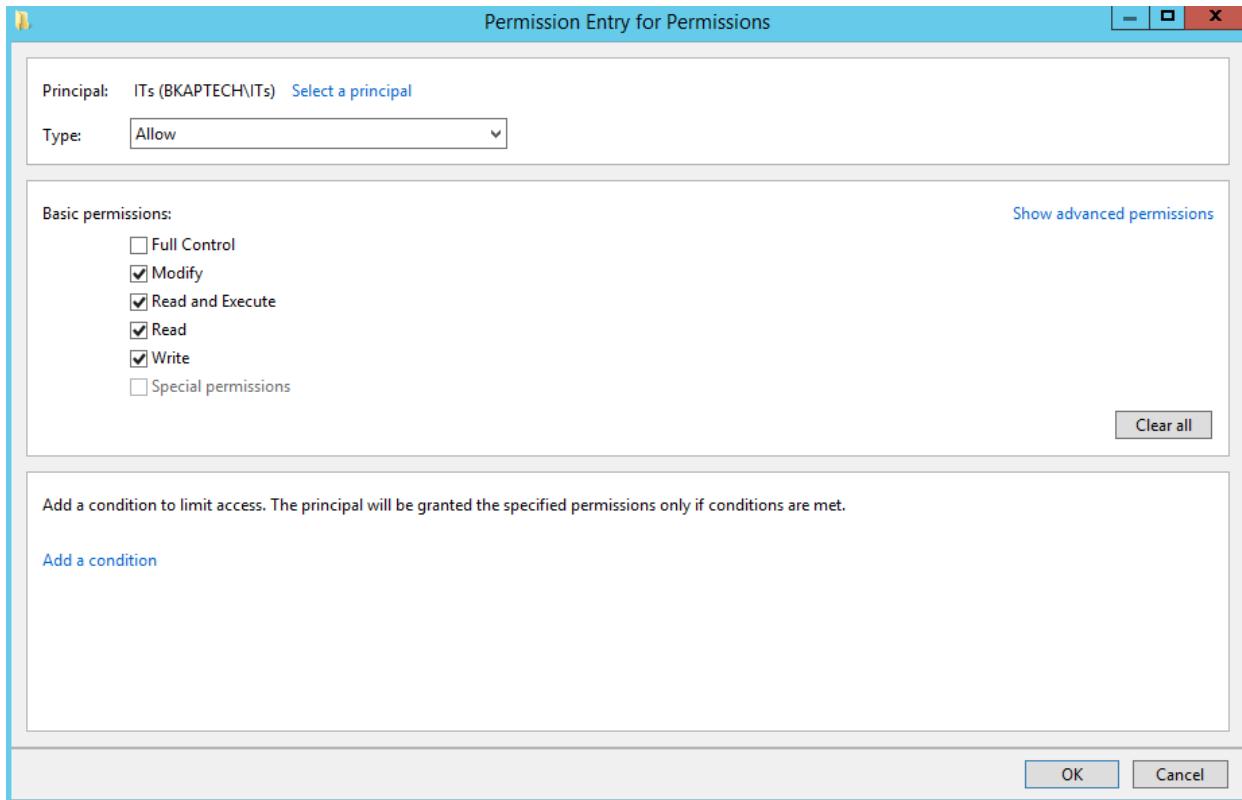
- Tại cửa sổ **Create Central Access Rule**, nhập tên “Rule-Dieu kien truy cap BaoCao”. Tại mục *permissions* bên dưới, chọn “*Use following permissions as current permissions*” => click vào **Edit**.



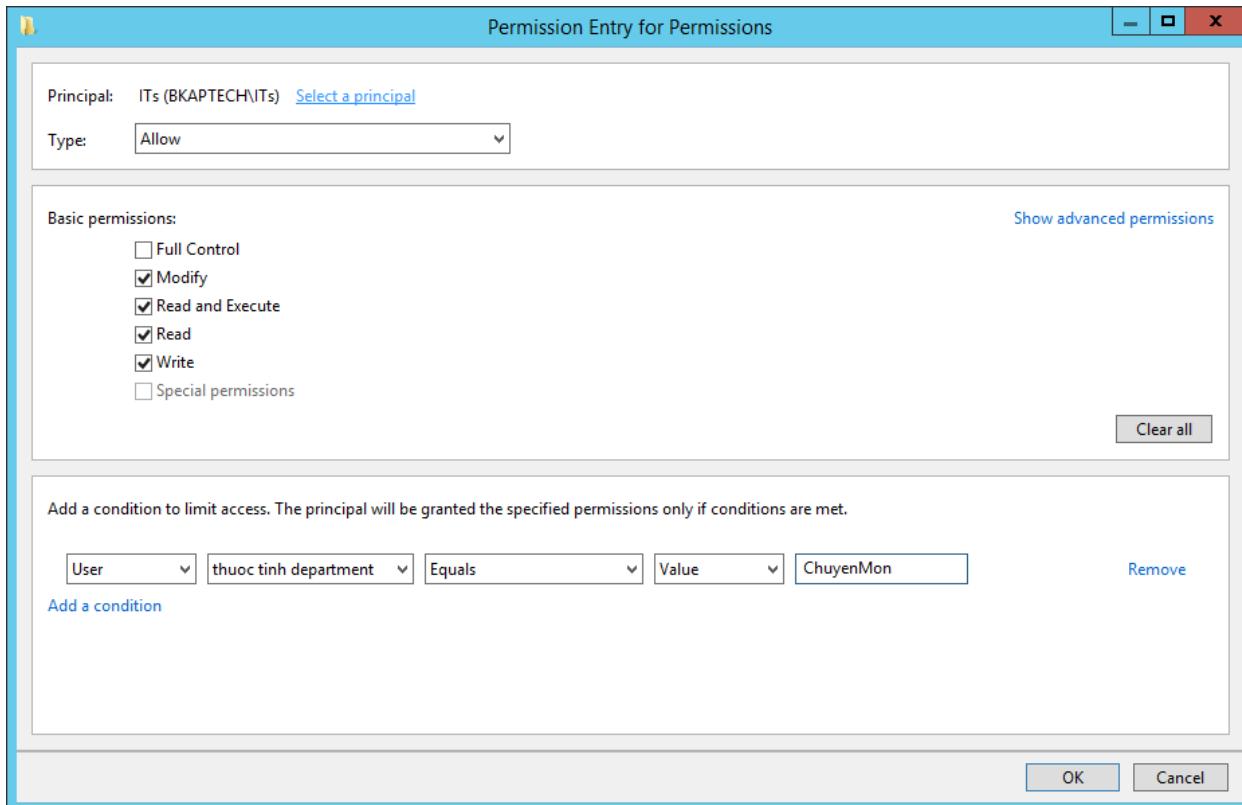
- Trong cửa sổ **Advanced Security Setting for Permissions**, click vào **Add** để thêm đối tượng phân quyền.



- Chọn tiếp vào **Add a Principal** , nhập vào Group ITs , phân quyền **Modify** cho group ITs , click chọn tiếp vào **Add a condition**.

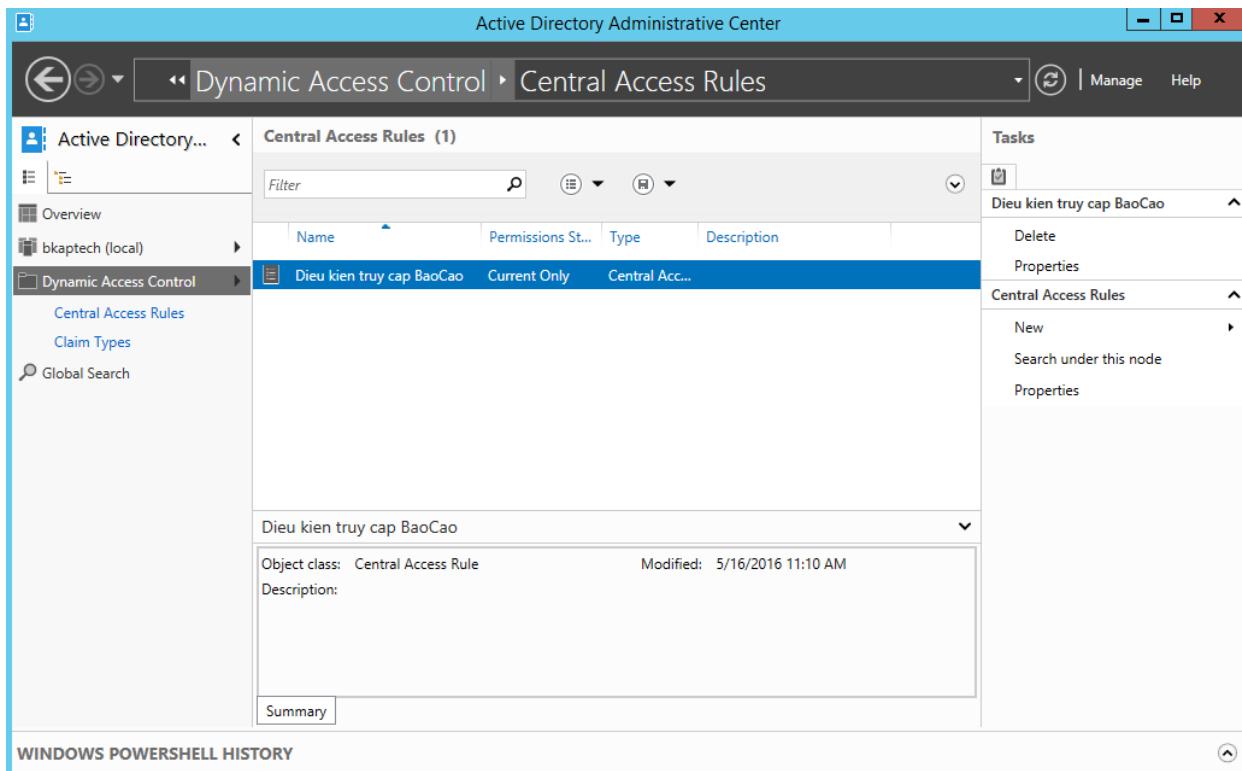


- Quy định User phải có thuộc tính *Department* đã quy định *Claim Type* là *ChuyenMon*.



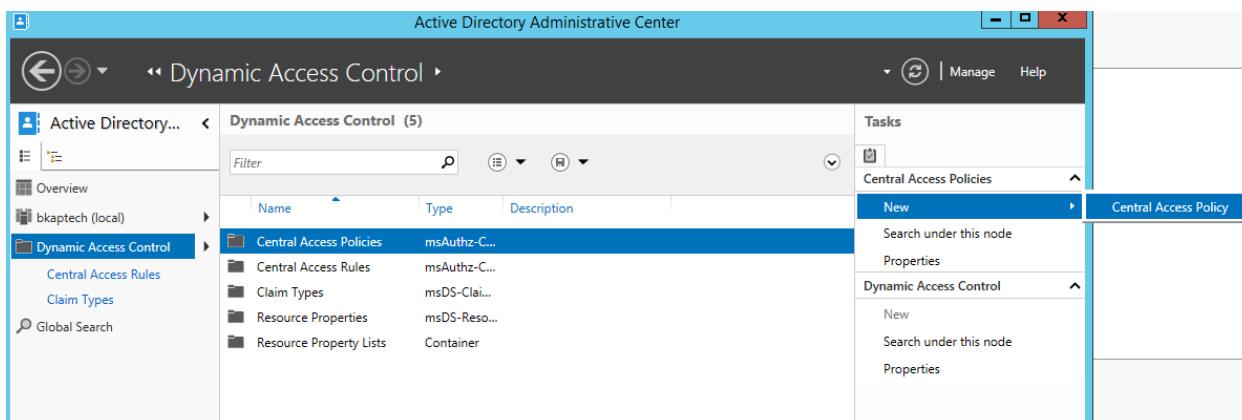
⇒ Click OK tất cả các cửa sổ đã mở.

- Kiểm tra Central Access Rule vừa tạo.

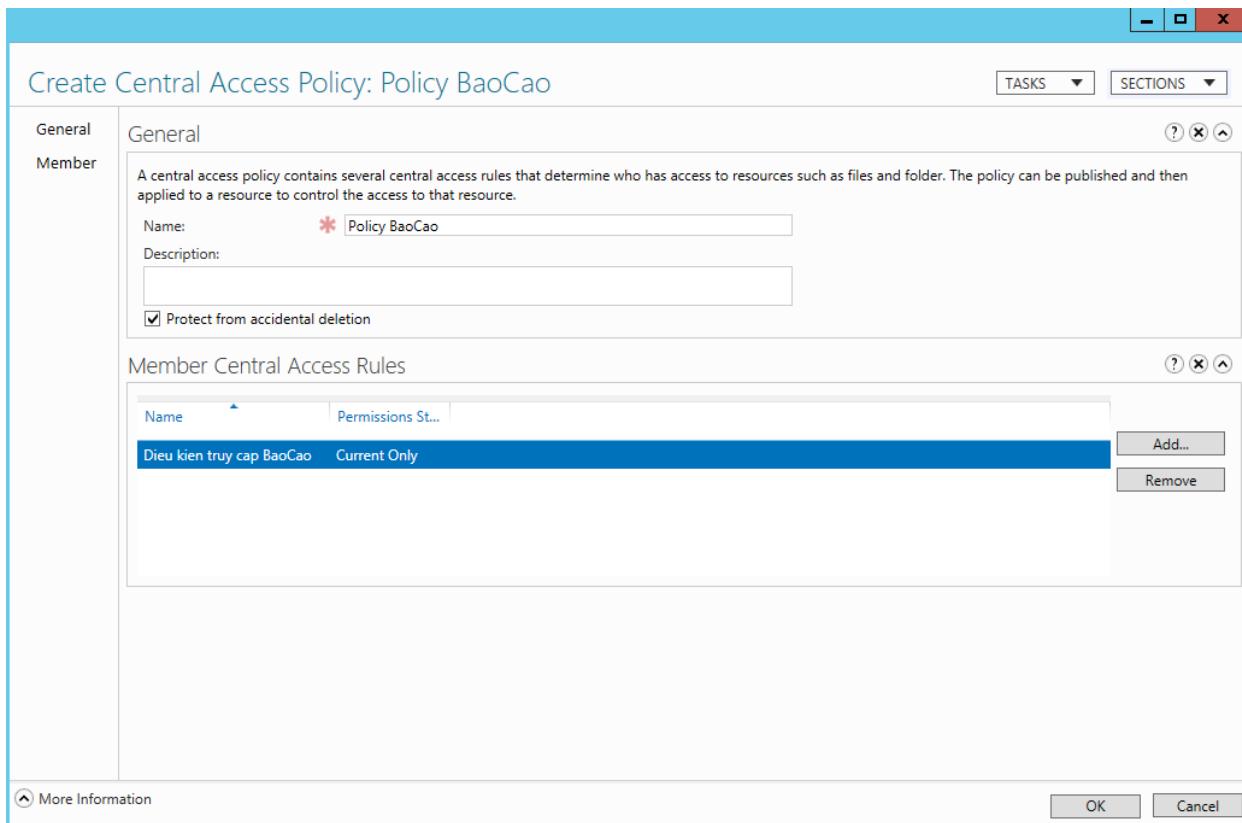


- Tạo Central Access Policy:

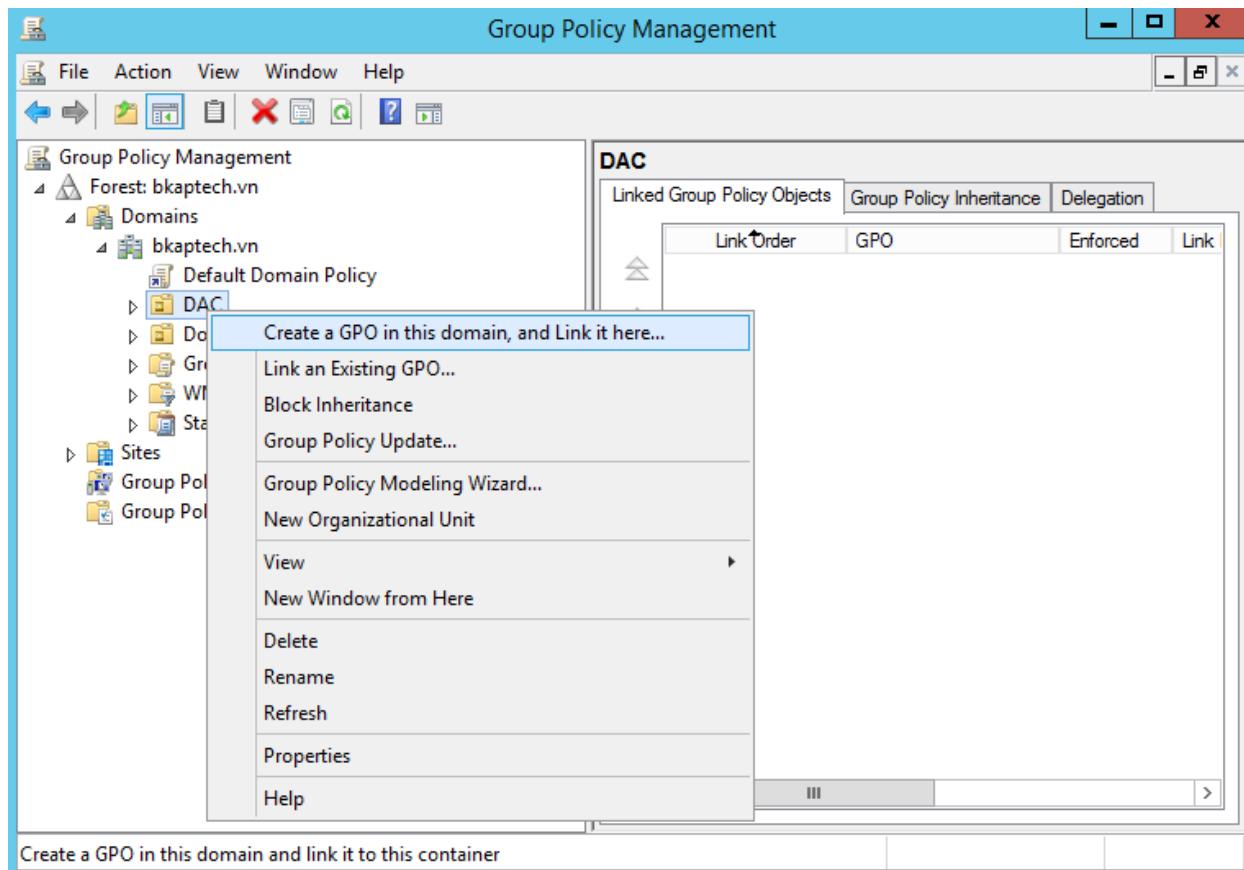
- Tại Active Directory Administrative Center / Dynamic Access Control / Central Access Policy / => chọn New / Central Access Policy.



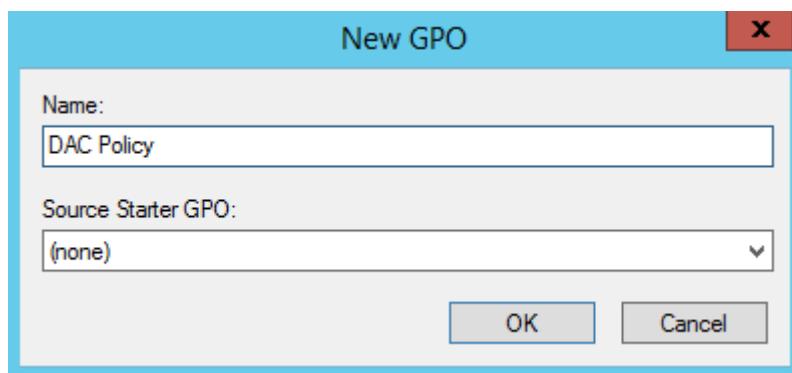
- Tại cửa sổ **Create Central Access Policy** , nhập tên “*Policy BaoCao*” , click vào Add để thêm **Central Access Rule** vào **Central Access Policy** => **OK**



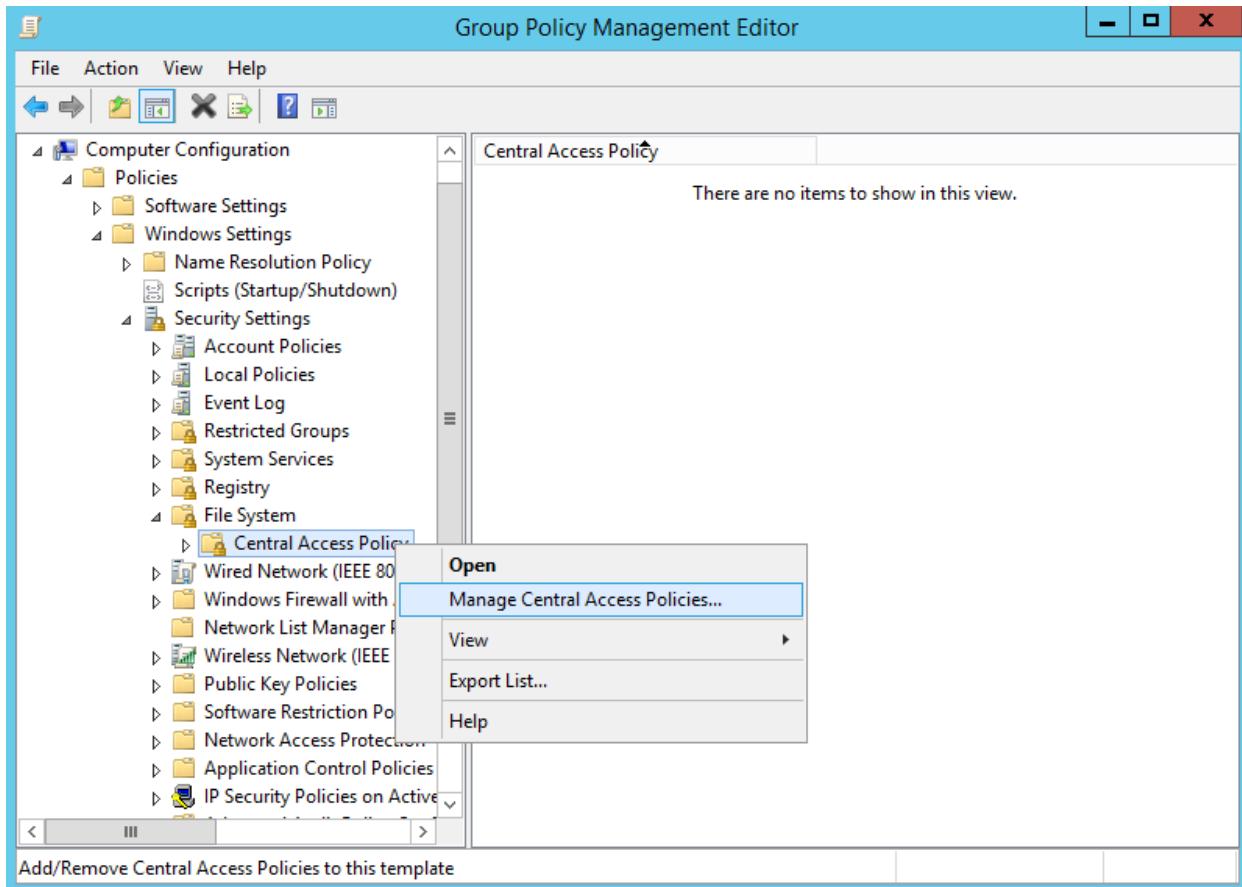
- Link Central Access Policy vào Group Policy để áp đặt lên OU chứa File Server (ou DAC).
 - Tại **Group Policy Management**, click chuột phải tại ou **DAC** / Create a GPO ...



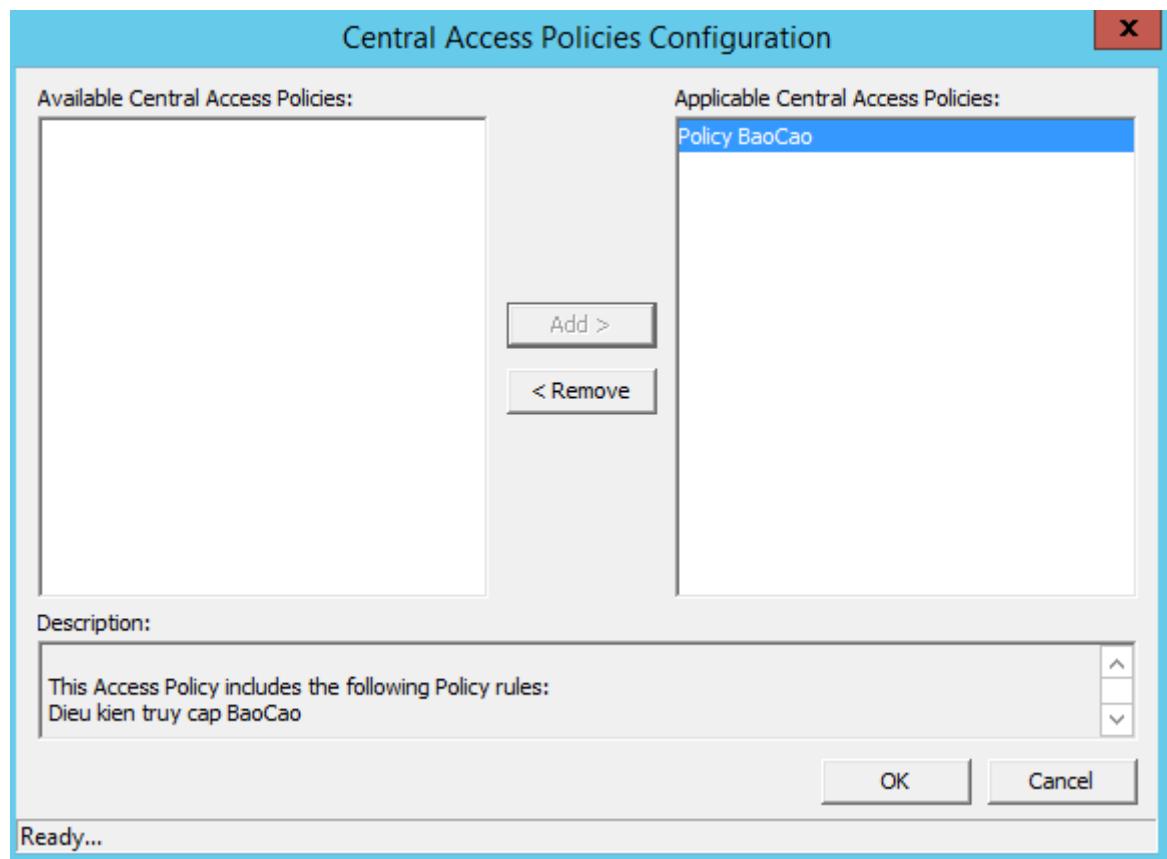
⇒ Name : **DAC Policy**.



- Edit **Group Policy** vừa tạo, tìm **Policy** theo đường dẫn sau: **Computer Configuration / Policies / Windows Settings / Security Setting / File System / Central Access Policy**, Click chuột phải tại đây chọn **Manager Central Access Policy**.



- Chọn Policy vừa tạo => Add / OK.



- Thực hiện gpupdate /force trên DC và File Server.

```

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

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

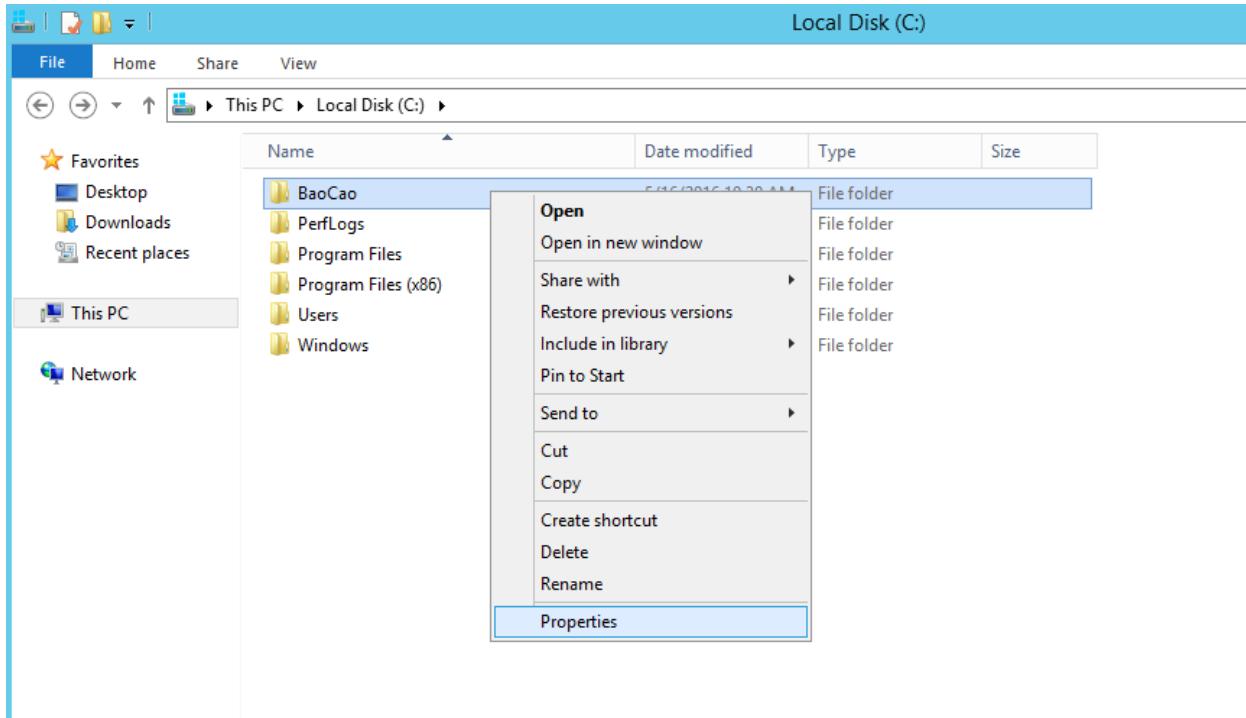
C:\Users\Administrator>gpupdate /force
Updating policy...
Computer Policy update has completed successfully.
User Policy update has completed successfully.

C:\Users\Administrator>

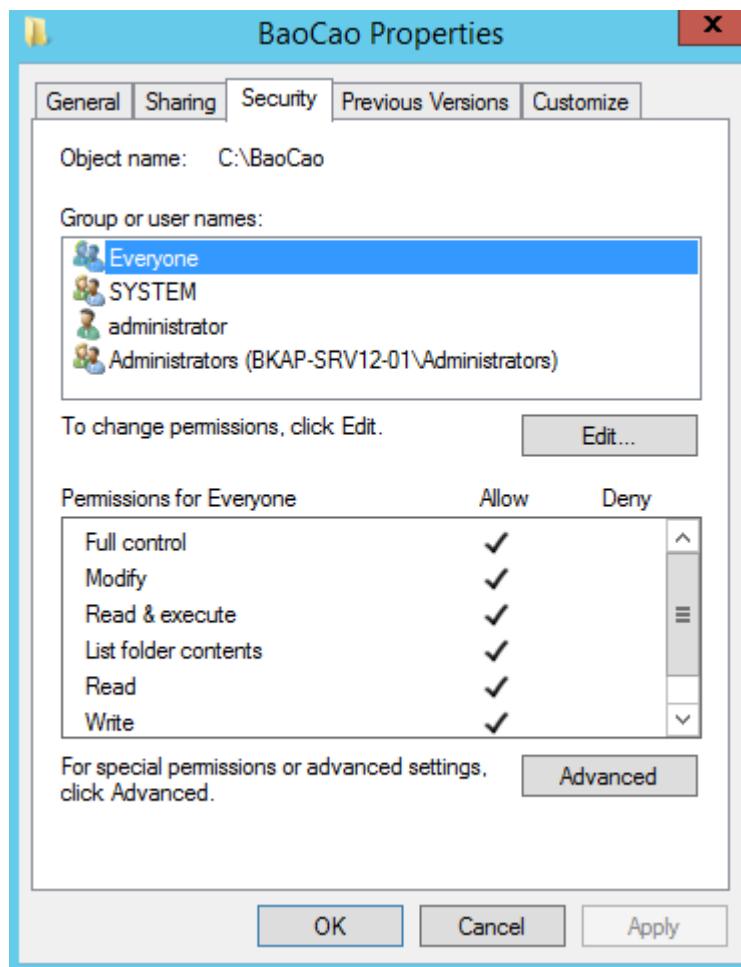
```

- Áp Central Access Policy vào Folder muốn phân quyền.

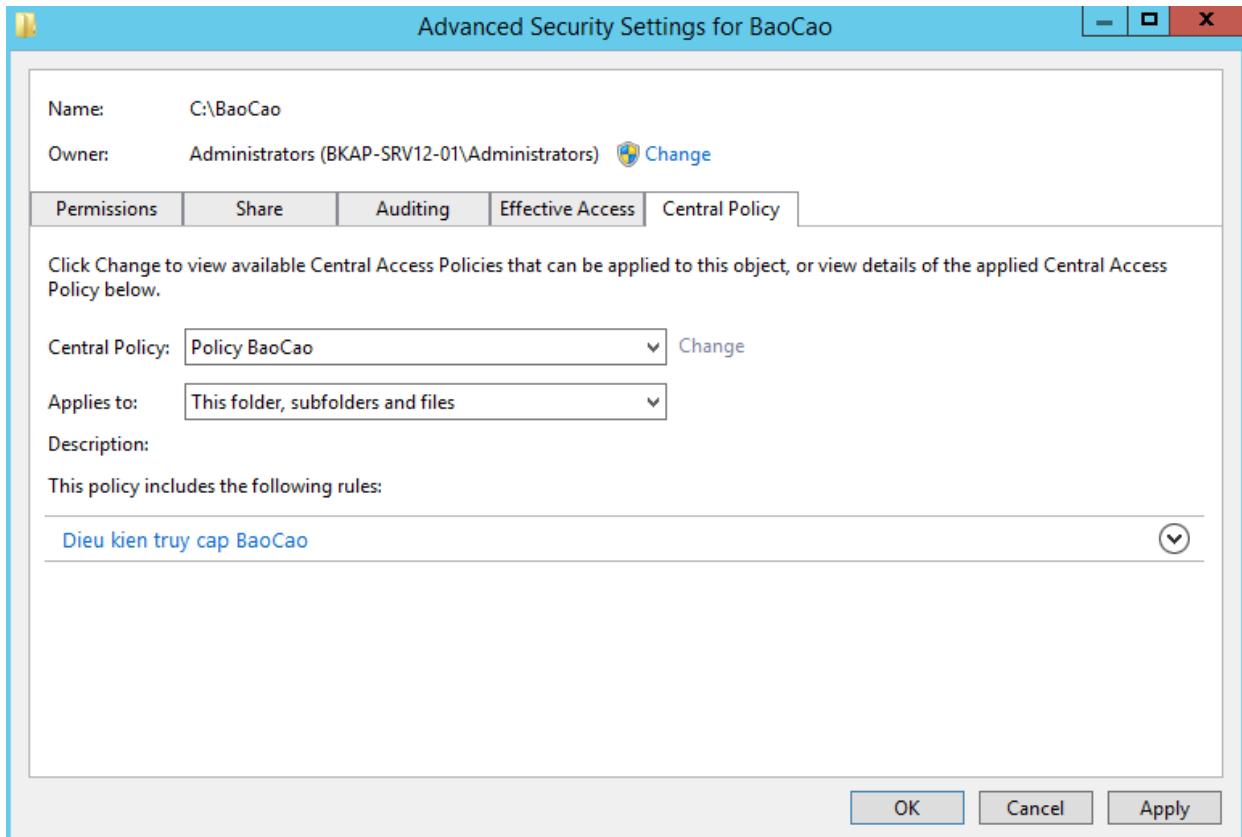
Trên File Server (*BKAP-SRV12-01*) , chuột phải tại Folder BaoCao / Properties.



▪ Chuyển sang Tab Security => Advanced

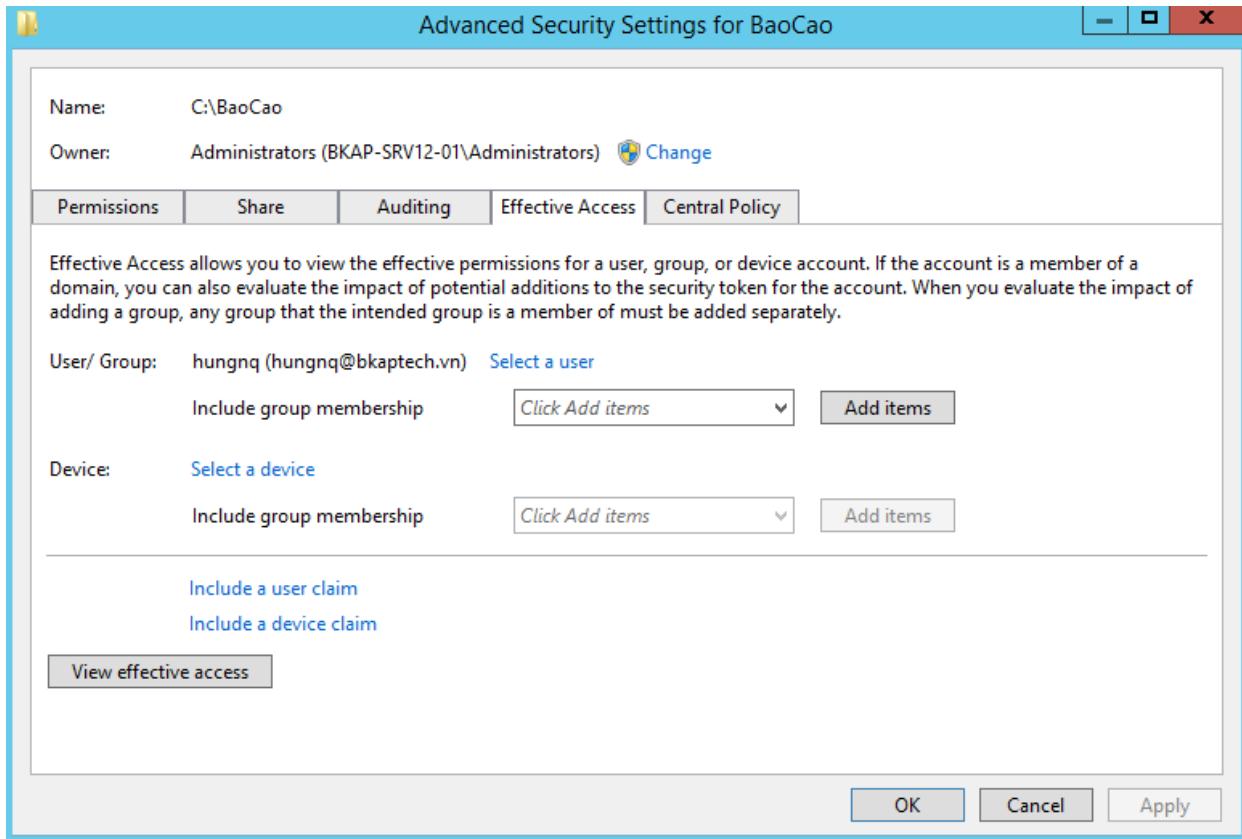


- Chuyển sang Tab **Central Policy**, click vào **Change** để chọn **Central Access Policy** đã tạo trước đó là *Policy BaoCao*.



⇒ Click **OK** tất cả cửa sổ.

- Kiểm tra truy cập từng User bằng chức năng **Effective Access**.
 - Trong folder *BaoCao* / **Properties** / tab **Security** / **Advanced** / tab **Effective Access**.
- ⇒ Chọn User *hungnq* (trong group ITs) để kiểm tra truy cập của user này trên thư mục *BaoCao*.



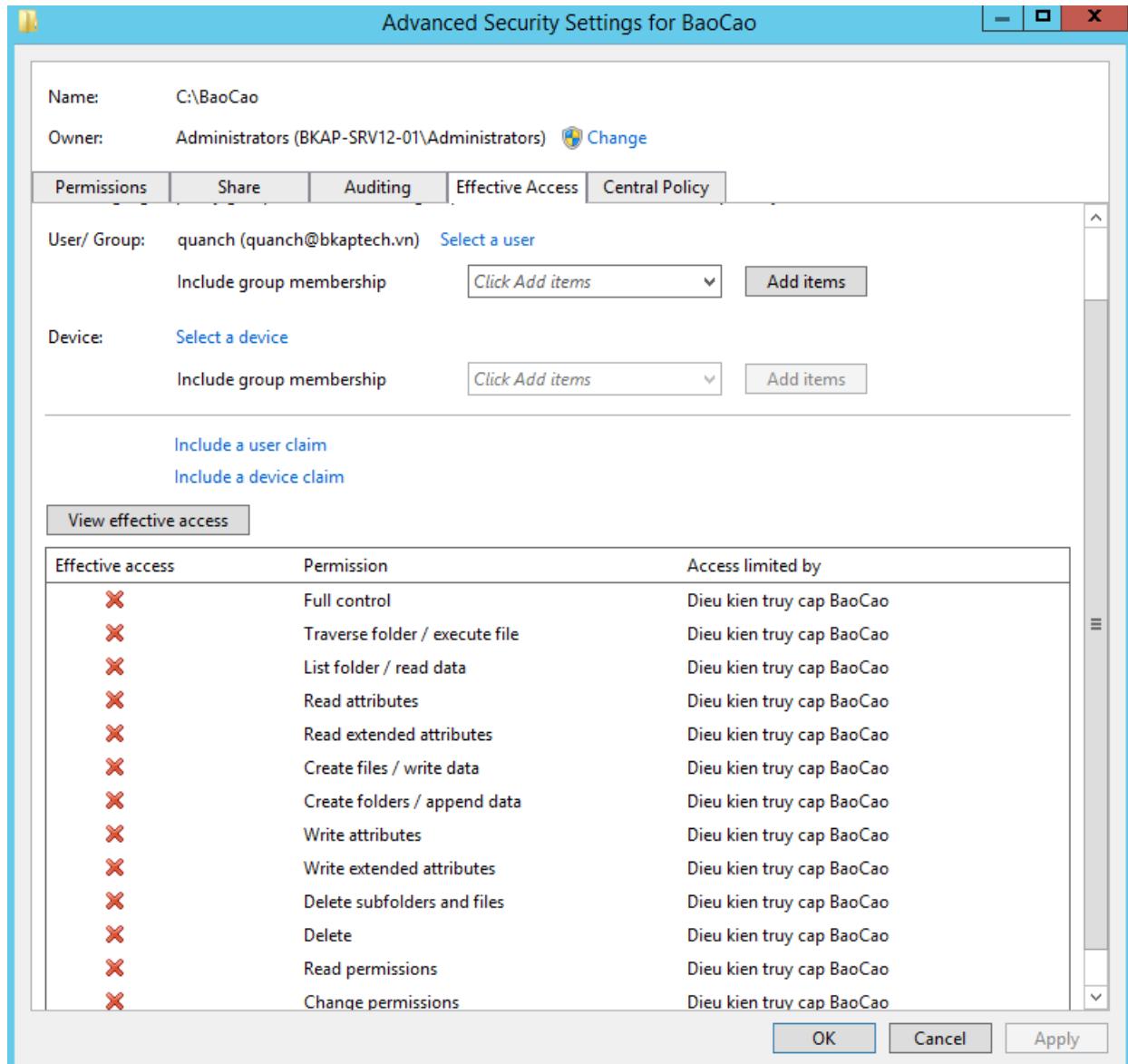
- Click vào View effective access để kiểm tra.

The screenshot shows the 'Advanced Security Settings for BaoCao' dialog box. At the top, it displays the path 'Name: C:\BaoCao' and 'Owner: Administrators (BKAP-SRV12-01\Administrators)'. Below this is a tab bar with 'Permissions', 'Share', 'Auditing', 'Effective Access' (which is selected), and 'Central Policy'. A descriptive text block explains what 'Effective Access' is. Under 'User/ Group', there is a dropdown menu 'Include group membership' with 'Click Add items' and an 'Add items' button. Under 'Device', there is a similar dropdown menu 'Include group membership' with 'Click Add items' and an 'Add items' button. Below these sections are two buttons: 'Include a user claim' and 'Include a device claim'. At the bottom left is a 'View effective access' button, which is highlighted. The main area contains a table titled 'Effective access' with columns for 'Effective access', 'Permission', and 'Access limited by'. The table lists various permissions with their corresponding icons and descriptions. At the bottom right of the dialog box are 'OK', 'Cancel', and 'Apply' buttons.

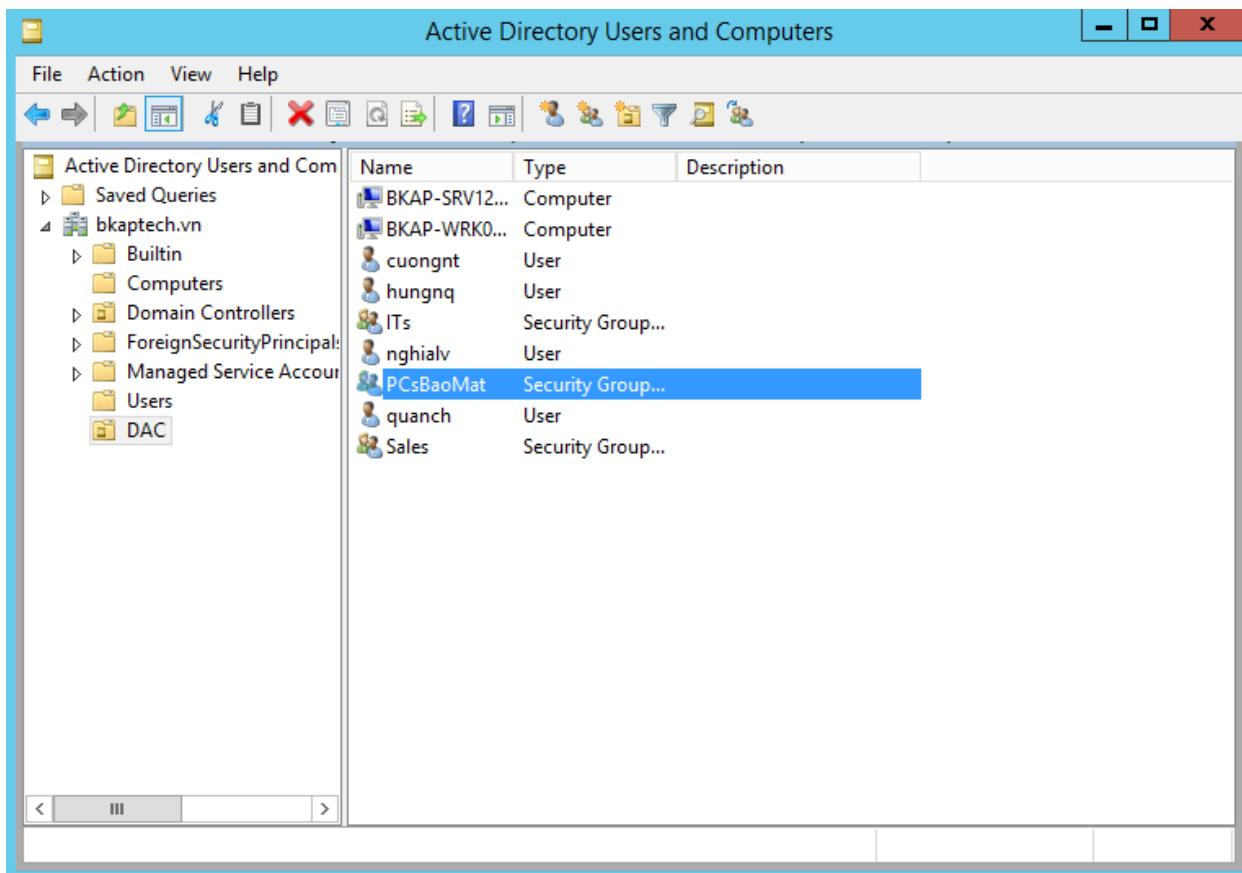
Effective access	Permission	Access limited by
✗	Full control	Dieu kien truy cap BaoCao
✓	Traverse folder / execute file	
✓	List folder / read data	
✓	Read attributes	
✓	Read extended attributes	
✓	Create files / write data	
✓	Create folders / append data	
✓	Write attributes	
✓	Write extended attributes	
✗	Delete subfolders and files	Dieu kien truy cap BaoCao
✓	Delete	
✓	Read permissions	
✗	Change permissions	Dieu kien truy cap BaoCao
✗	Take ownership	Dieu kien truy cap BaoCao

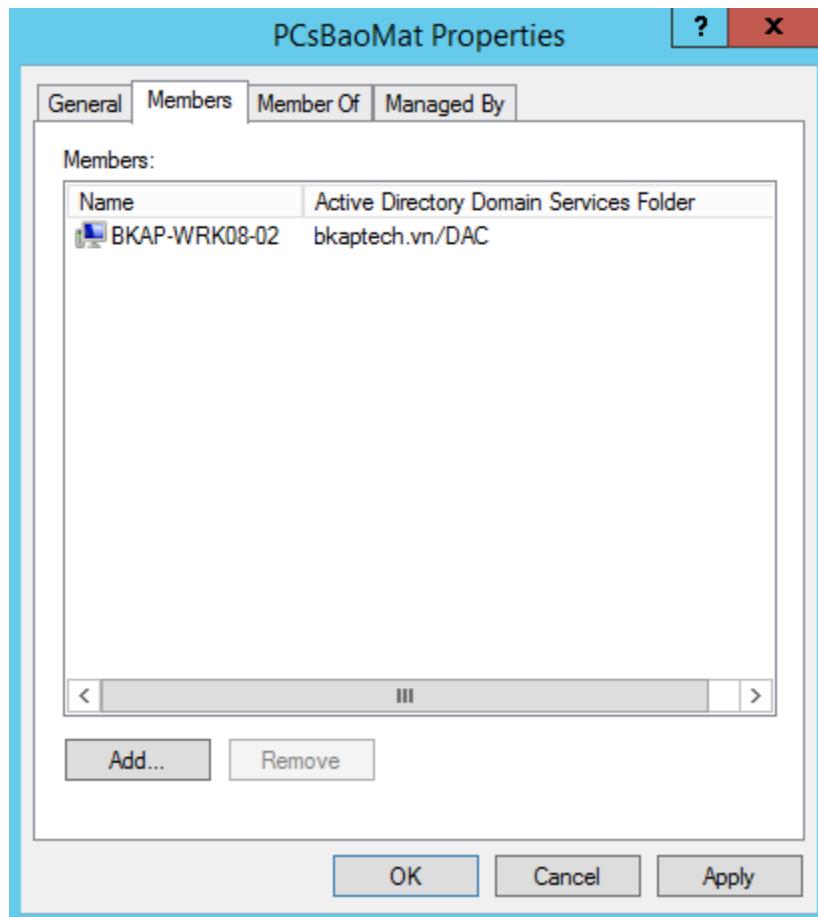
⇒ User *hungnq* thuộc nhóm **ITs** và có thuộc tính department là *ChuyenMon* nên được phép truy cập thư mục **BaoCao**.

- Kiểm tra truy cập bằng user *quanch* (thuộc group **Sales**) sẽ thấy user không được quyền truy cập.

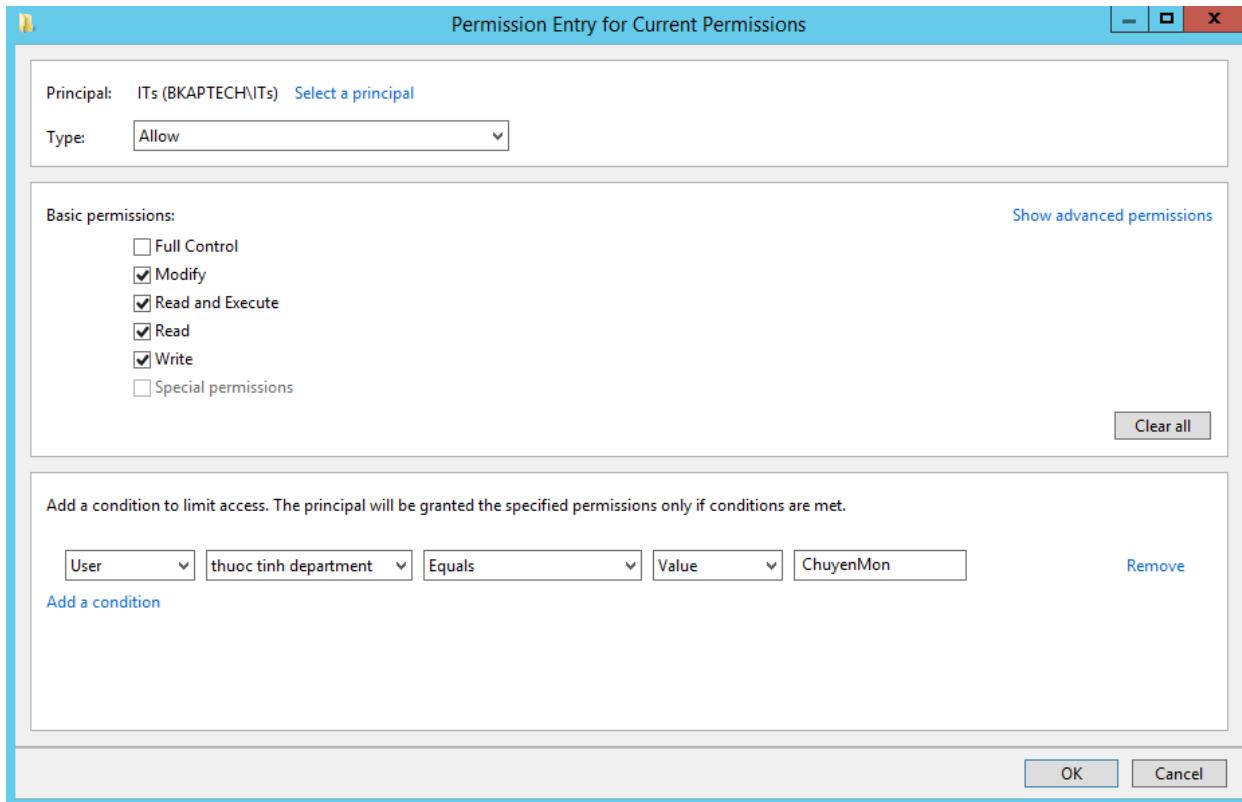


- Bổ sung điều kiện bắt buộc *User* thỏa mãn điều kiện **logon** trên Client chỉ định mới được phép truy cập.
 - Trên DC tạo Group tên **PCsBaoMat**, đưa Client Windows 8 vào group này.

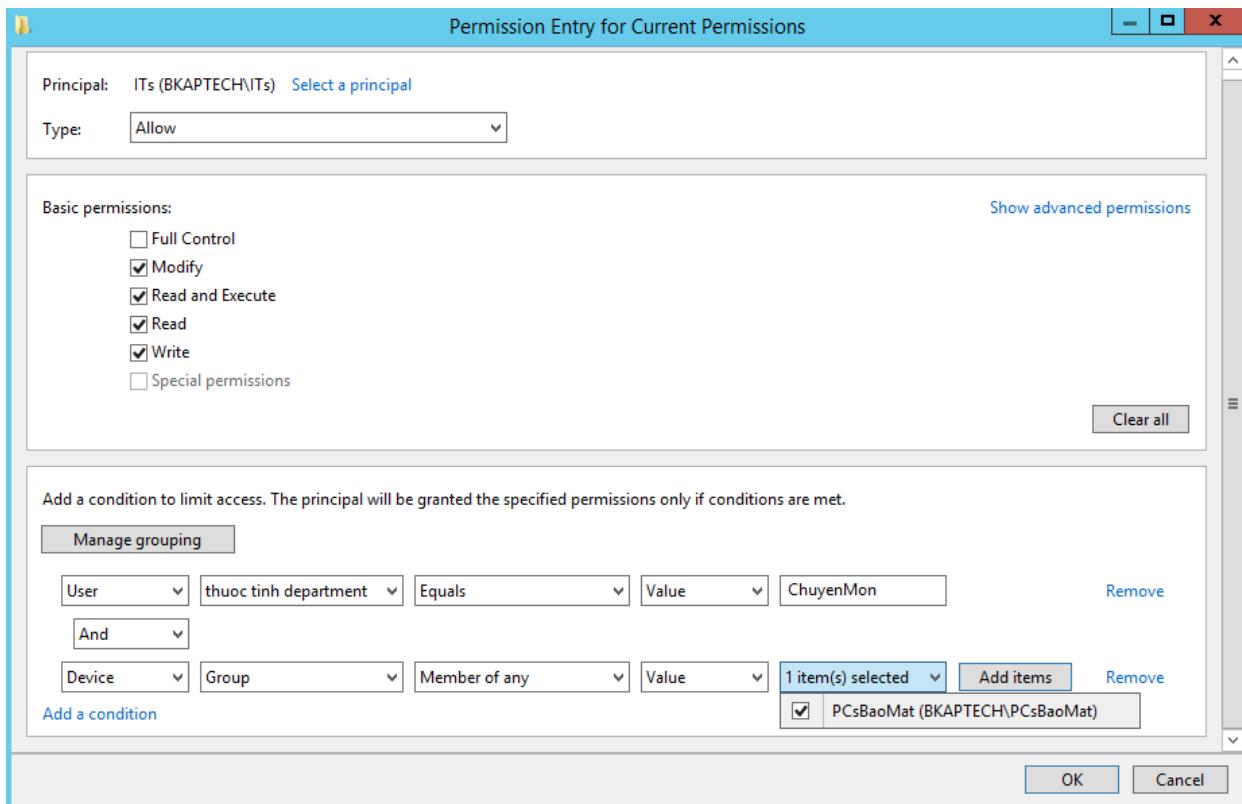




- Chỉnh sửa **Central Access Rule** để bổ sung điều kiện mới.
 - Click chuột phải tại **Access Rule** đã tạo / **Properties** / **Edit** (tại Current Permissions).
 - Trong cửa sổ **Advanced Security Setting for Current Permissions**, chọn Group ITs / Edit.
 - Chọn **Add a conditional** để thêm điều kiện mới.



- Quy định yêu cầu về Device thuộc group PCsBaoMat.
 - Click vào Add Item / Add vào group PCsBaoMat.



- Thực hiện gpupdate /force trên DC và File Server.

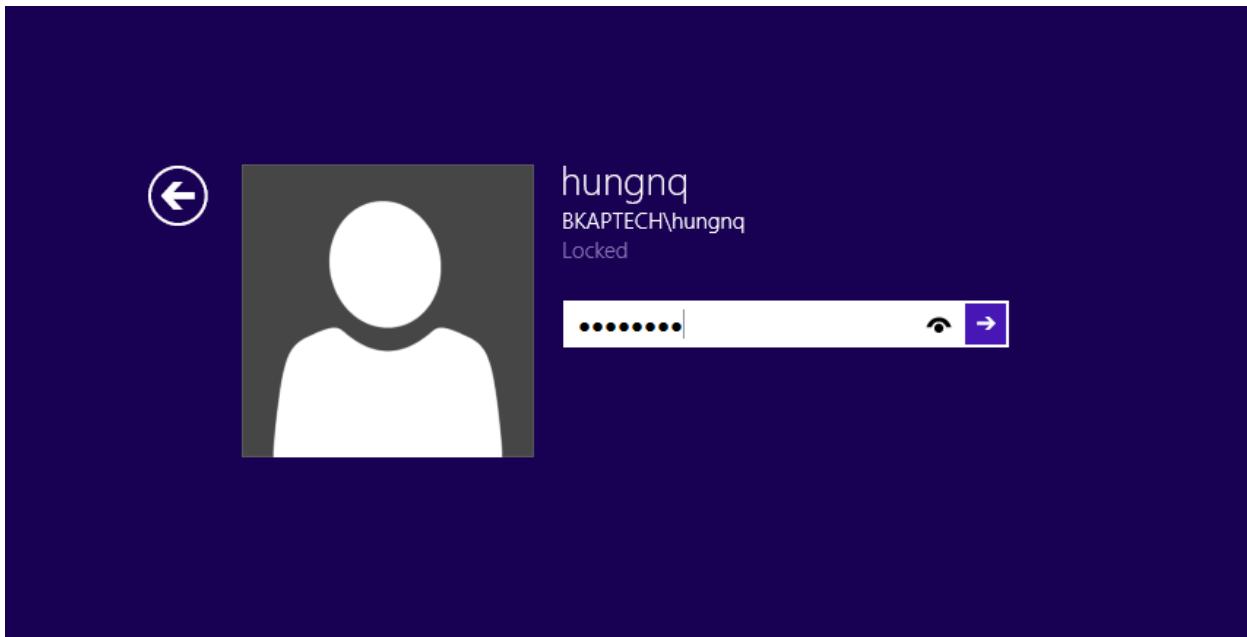
```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

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

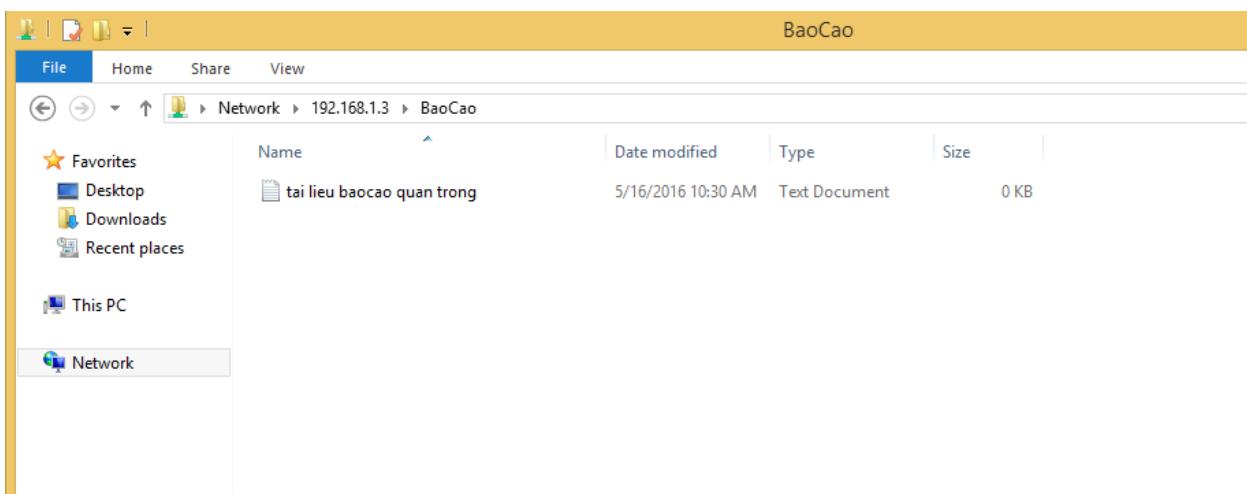
Computer Policy update has completed successfully.
User Policy update has completed successfully.

C:\Users\Administrator>
```

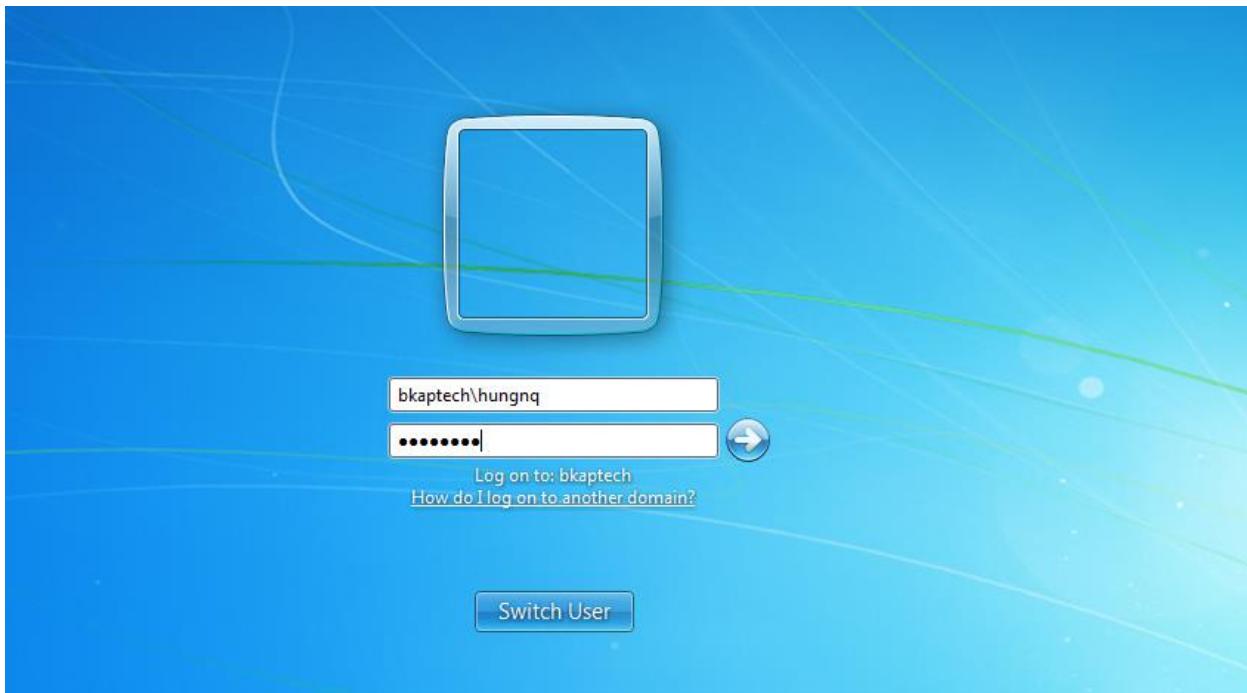
- Kiểm tra truy cập trên Client:
 - Đăng nhập tài khoản **hungnq** thuộc group ITs:



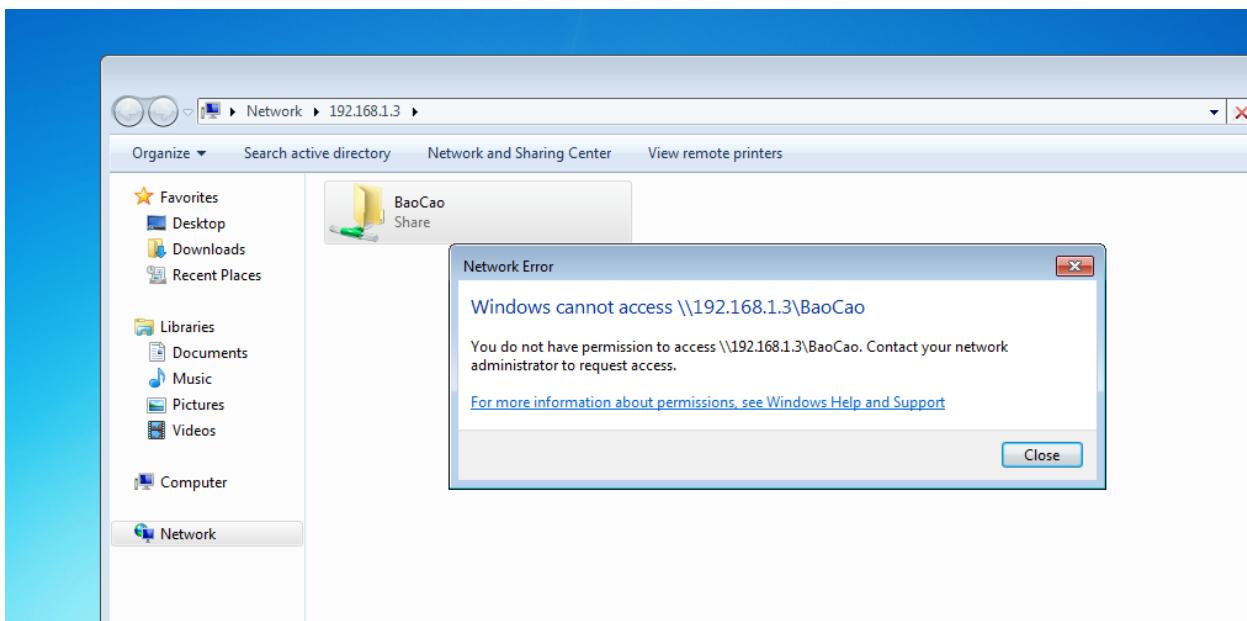
- Truy cập thành công thư mục **BaoCao** trên Client Windows 8.



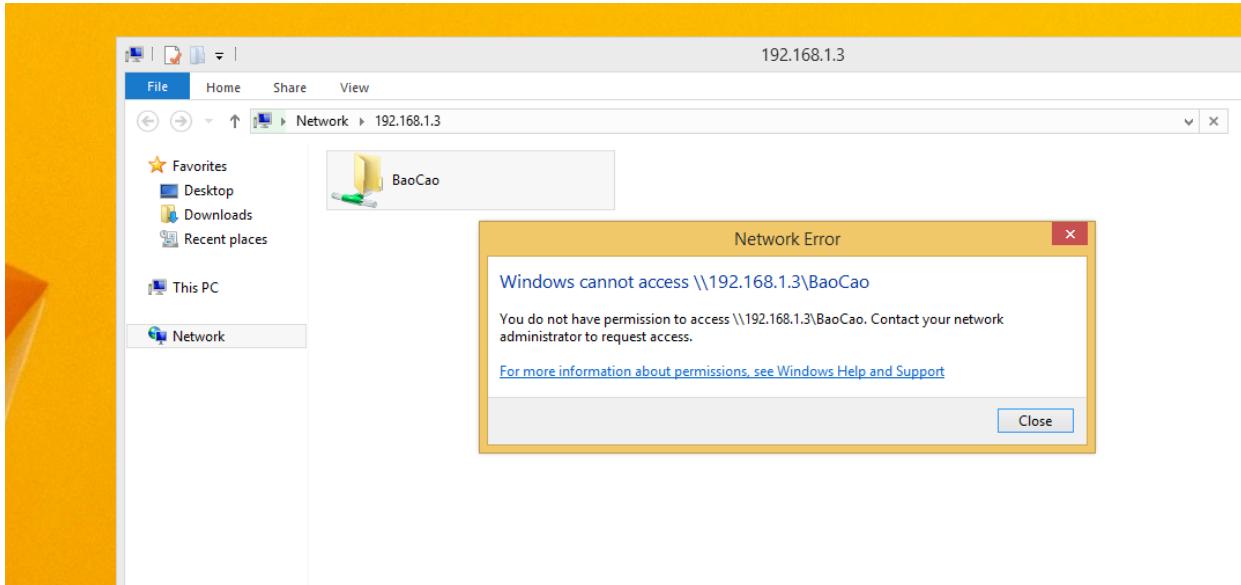
- Đăng nhập tài khoản **hungnq** thuộc group **ITs** trên máy **Client Windows 7** để kiểm tra.



- Tài khoản **hungnq** chỉ được quyền truy cập thư mục **BaoCao** tại **đuy nhất** máy **Client Windows 8**, ko được quyền truy cập trên các máy trạm khác.



- Tài khoản **quanch** ko thuộc group **ITs** , ko đủ các điều kiện truy cập thư mục **BaoCao**.



Bài 4:

TRIỀN KHAI CẤU HÌNH AD DS NÂNG CAO

Các nội dung chính được đề cập:

- ✓ Triển khai Child Domain trong AD DS.
- ✓ Thực hiện Trust Forest.
- ✓ Cấu hình AD DS Site and Replication.

4.1 Triển khai Child Domains trong AD DS.

1.Yêu cầu bài lab:

+ **BKAP-DC12-01:** Đã nâng cấp lên Domain Controller quản lý miền **bkaptech.vn**, cấu hình hệ thống tên miền DNS..

+ **BKAP-SRV12-01** và **BKAP-SRV12-02 :**

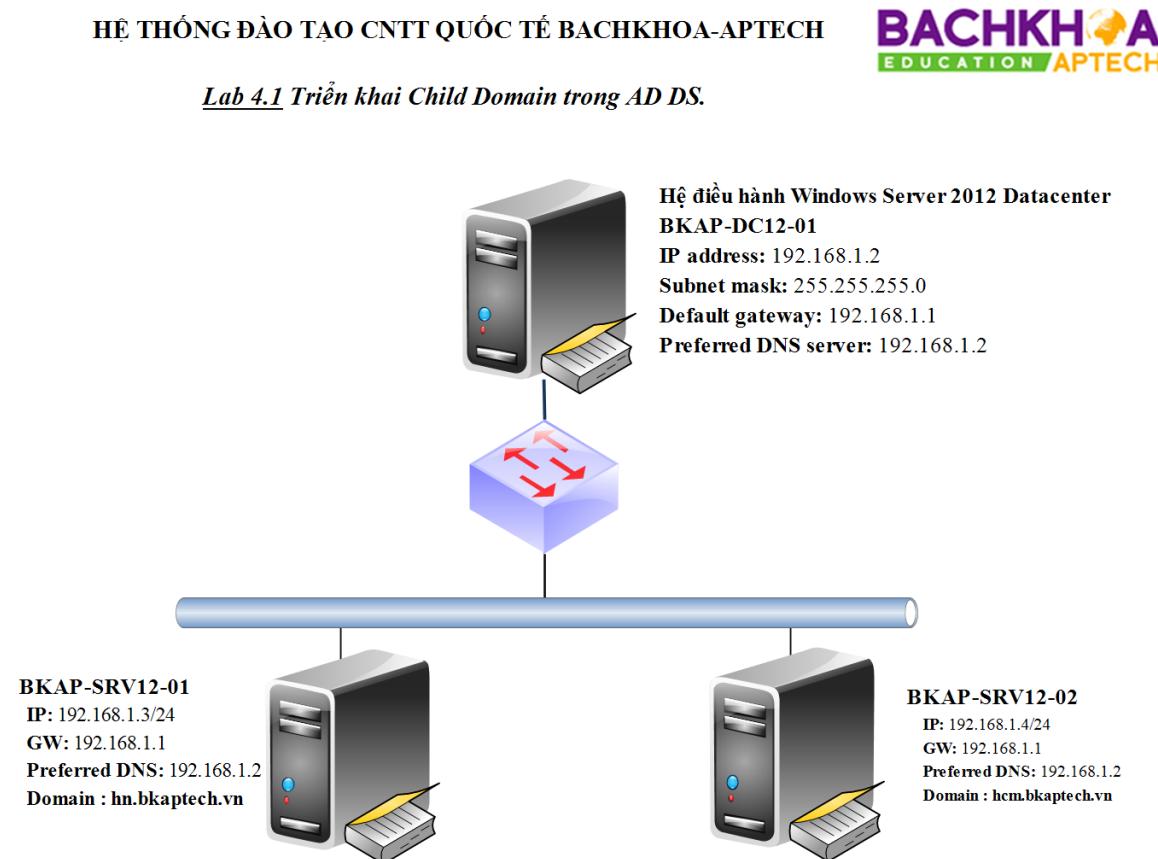
- Cài đặt và cấu hình Child Domains. (Domain con hn.bkaptech.vn)
- Kiểm tra Trust Domain giữa 2 máy.

- Kiểm tra ping 2 tên miền **hn.bkaptech.vn** và **hcm.bkaptech.vn**.

2.Yêu cầu chuẩn bị:

- + **BKAP-DC12-01**: máy Domain Controller với tên miền **bkaptech.vn**.
- + **BKAP-SRV12-01** : Child Domain (**hn.bkaptech.vn**)
- + **BKAP-SRV12-02** : Child Domain (**hcm.bkaptech.vn**).

3.Mô hình lab:

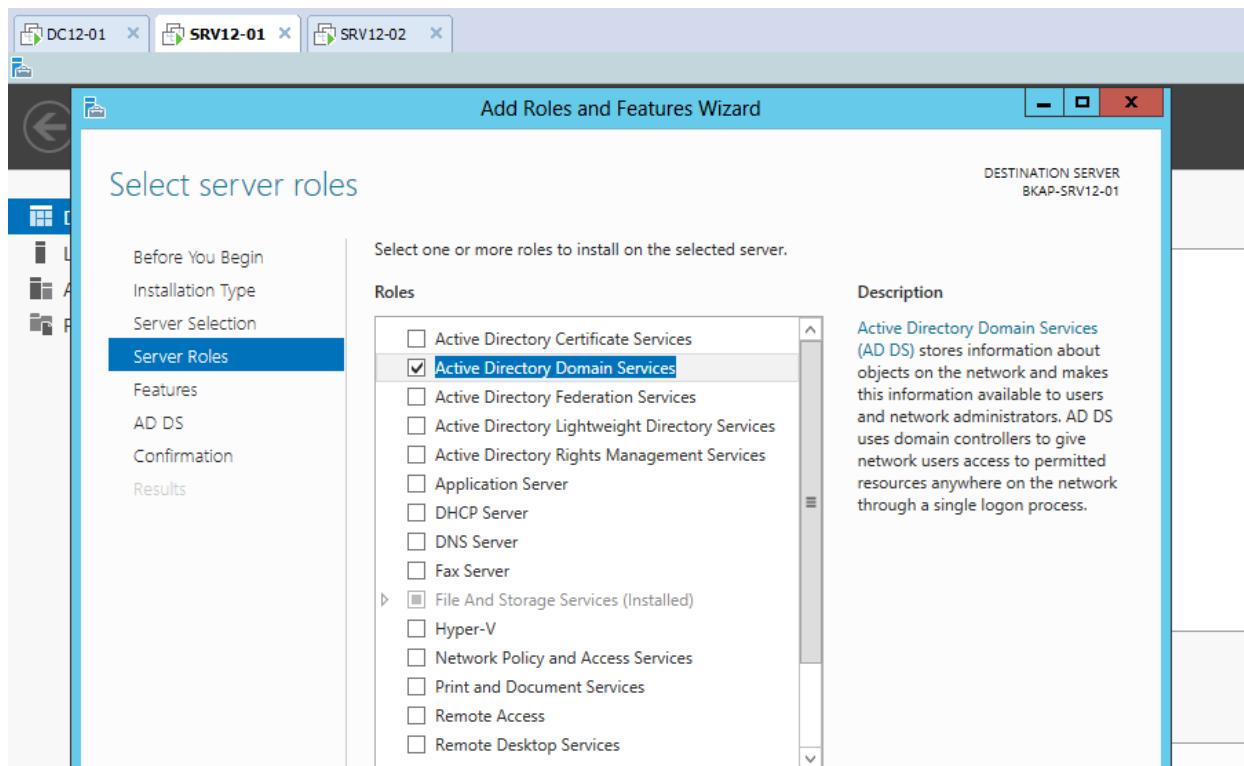


Sơ đồ địa chỉ sau :

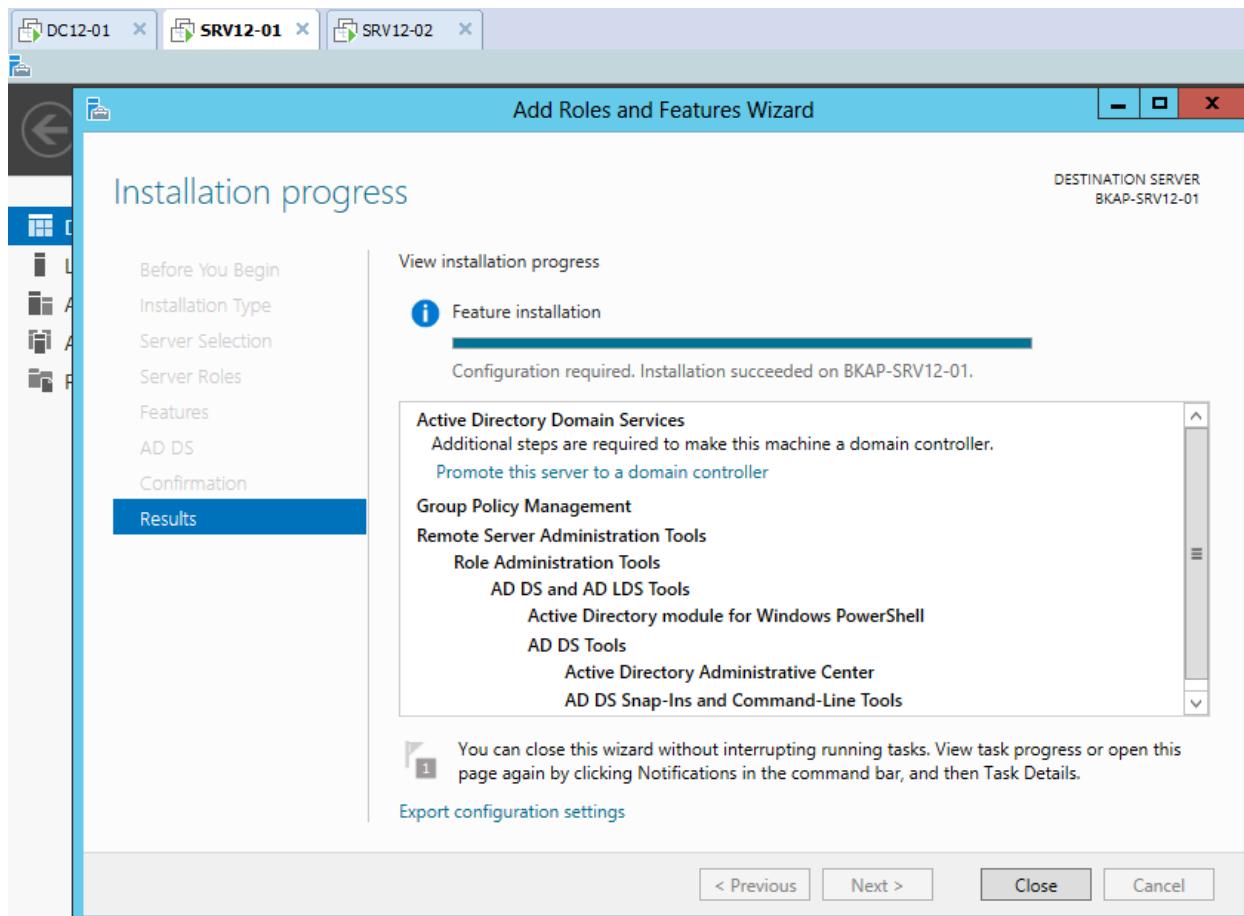
Thông số	BKAP-DC12-01	BKAP-SRV12-01	BKAP-SRV12-02
<i>IP address</i>	192.168.1.2	192.168.1.3	192.168.1.4
<i>Subnet Mask</i>	255.255.255.0	255.255.255.0	255.255.255.0
<i>Gateway</i>	192.168.1.1	192.168.1.1	192.168.1.1
<i>DNS server</i>	192.168.1.2	192.168.1.2	192.168.1.2

Hướng dẫn chi tiết :

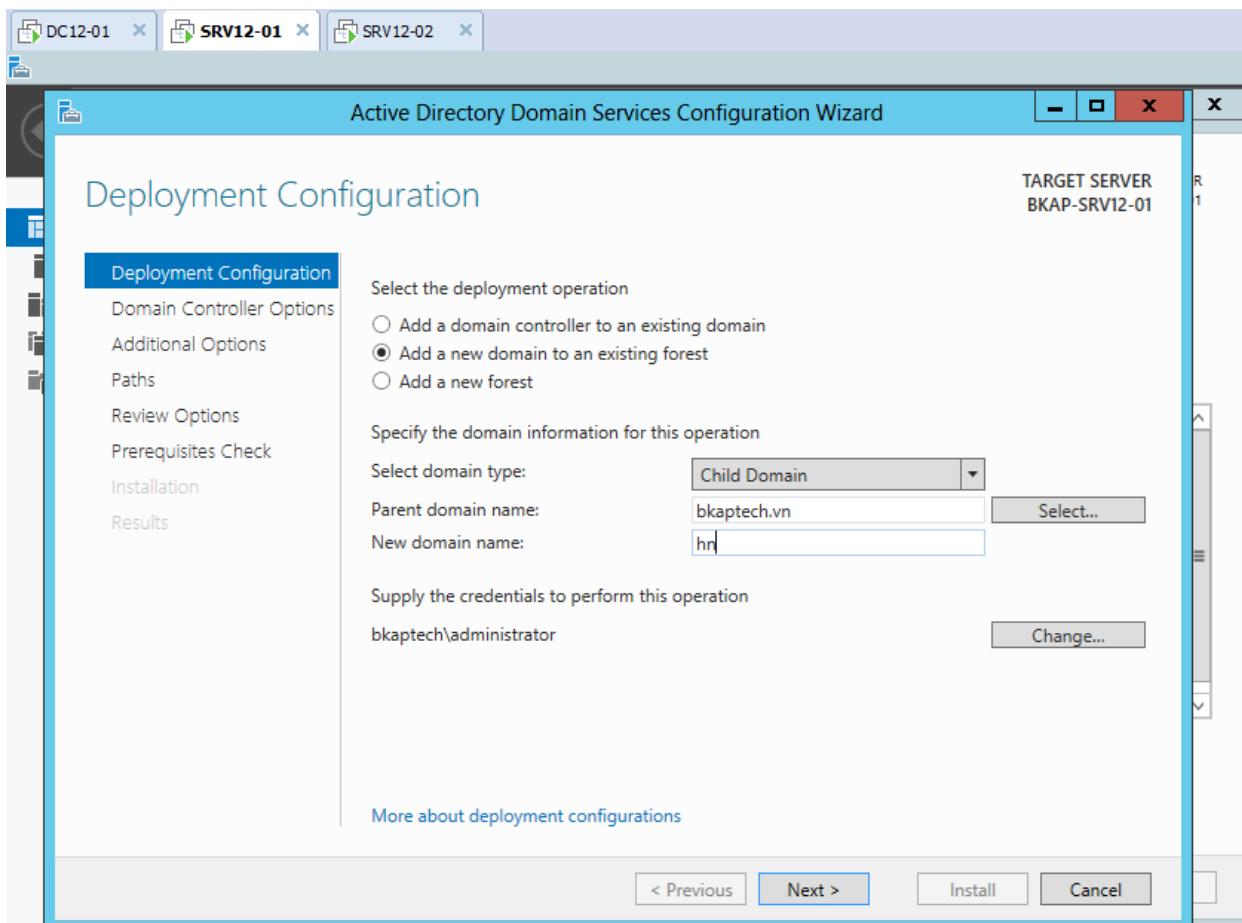
- Thực hiện trên máy BKAP-SRV12-01 cài đặt dịch vụ **Active Directory Domain Services**.



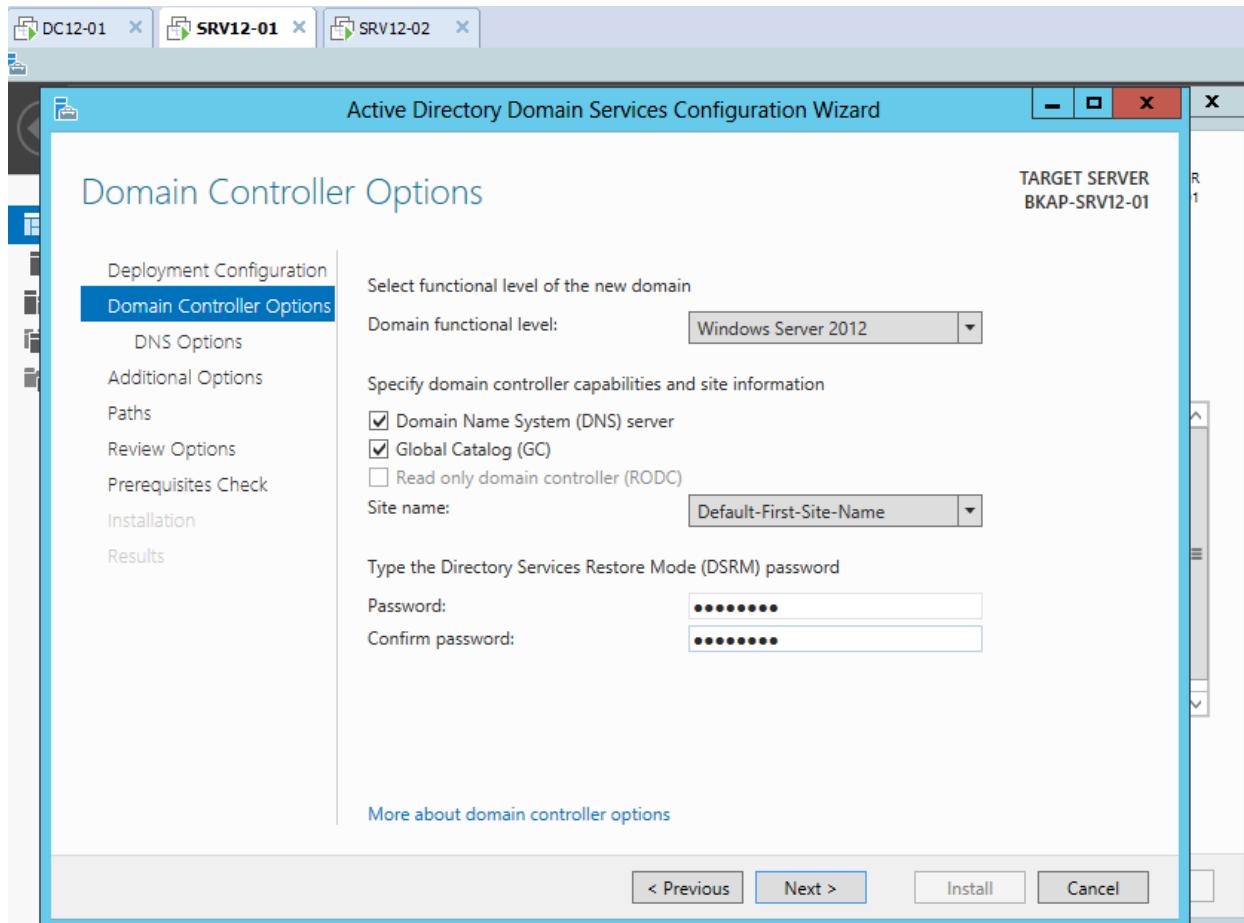
- Click vào **Promote this server to a domain controller**.



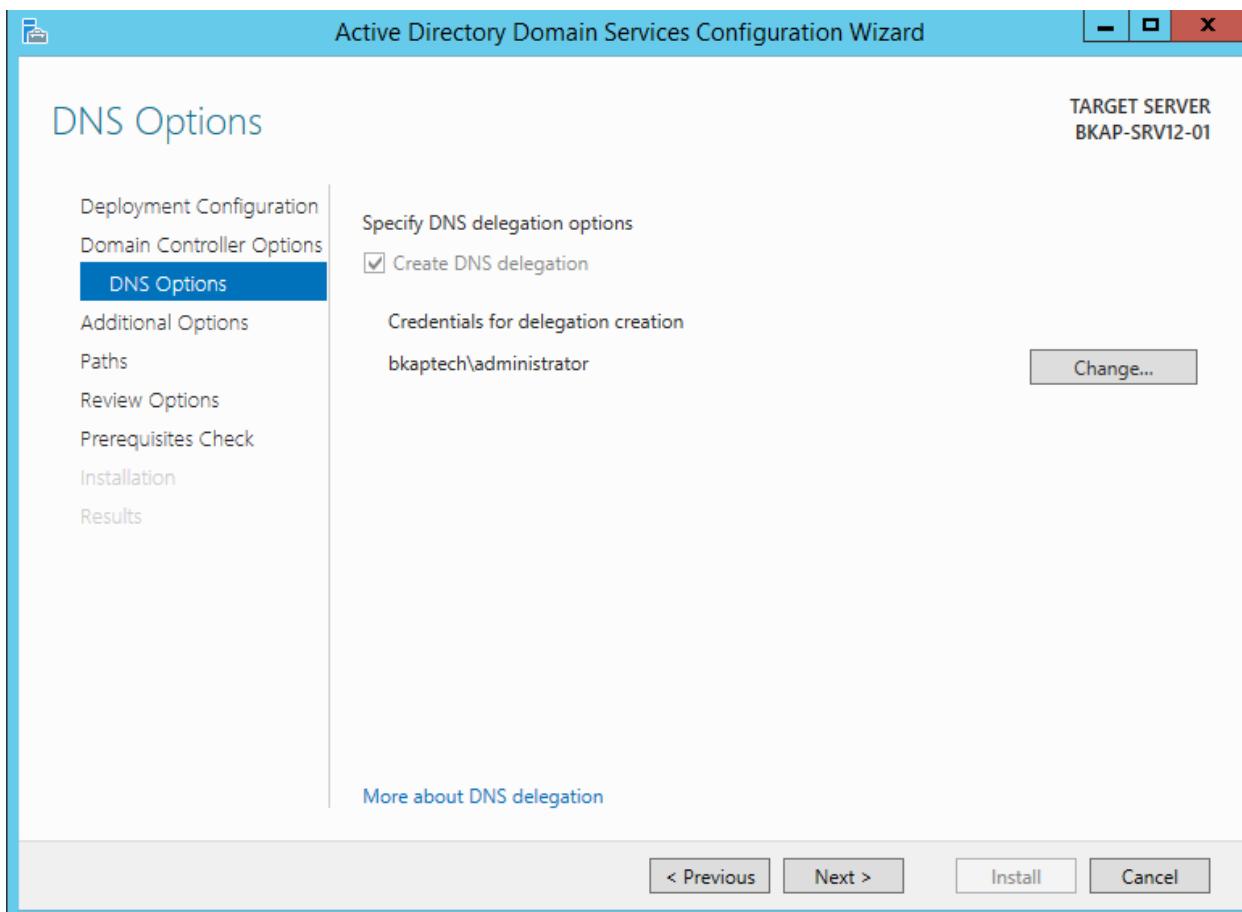
- Tại cửa sổ **Deployment Configuration**, click chọn vào *Add a new domain to an existing forest.*
 - Click vào Select , nhập User và Password **bkaptech.vn\administrator**
 - Parent domain name : **bkaptech.vn**
 - Tại New domain name : *hn*
 - Next.



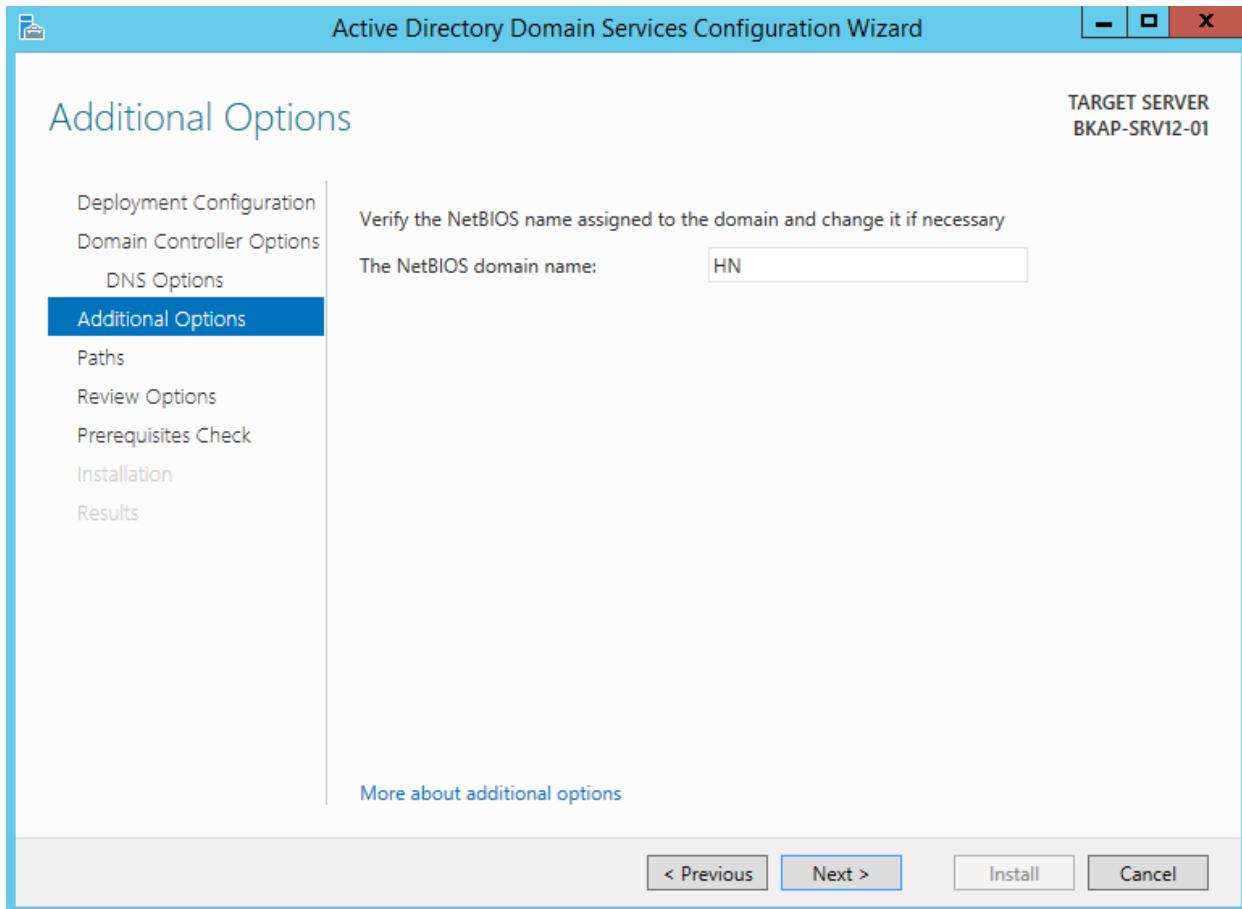
- Tại cửa sổ **Domain Controller Options**, nhập vào *Password DSRM*.
Click vào Next.



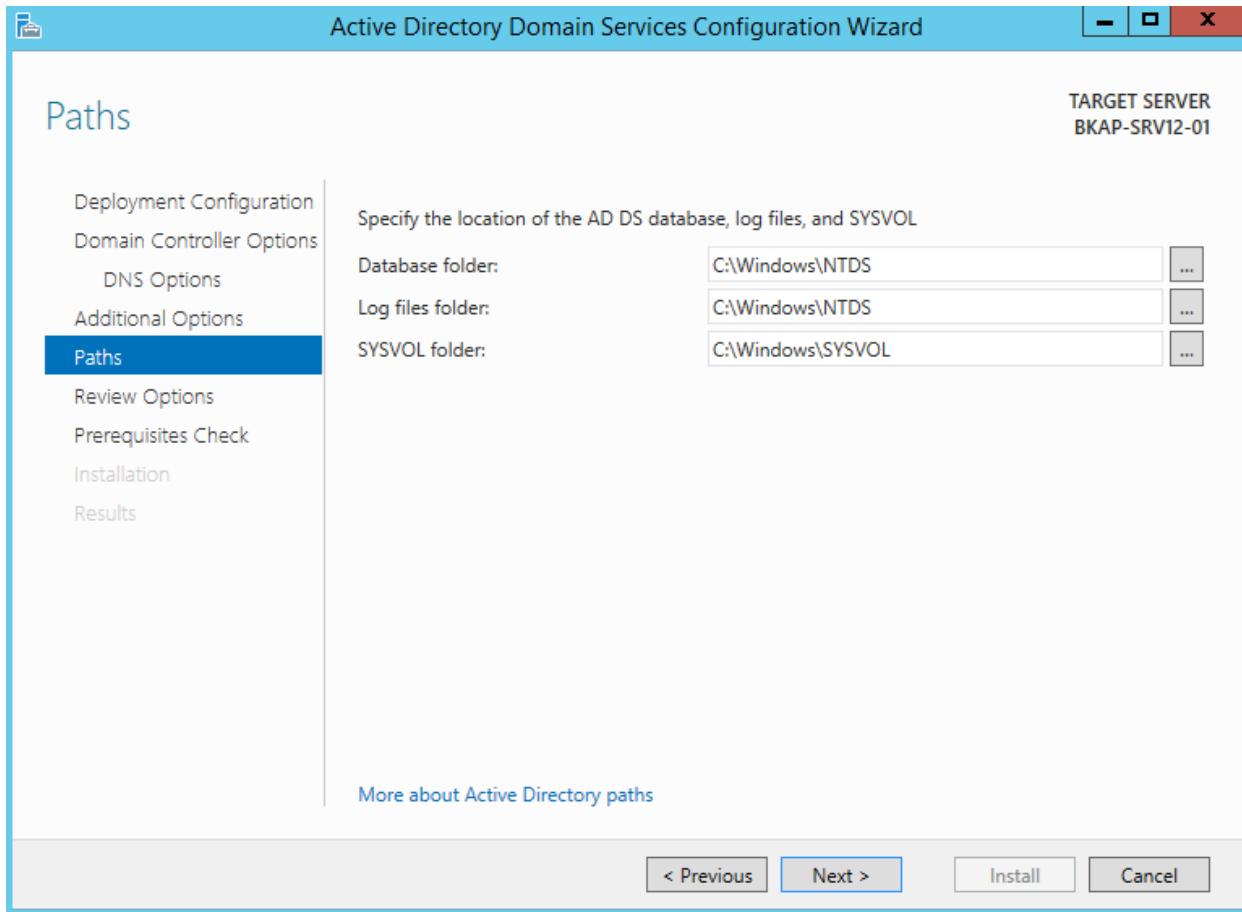
- Tại cửa sổ **DNS Options**, click vào **Next**.



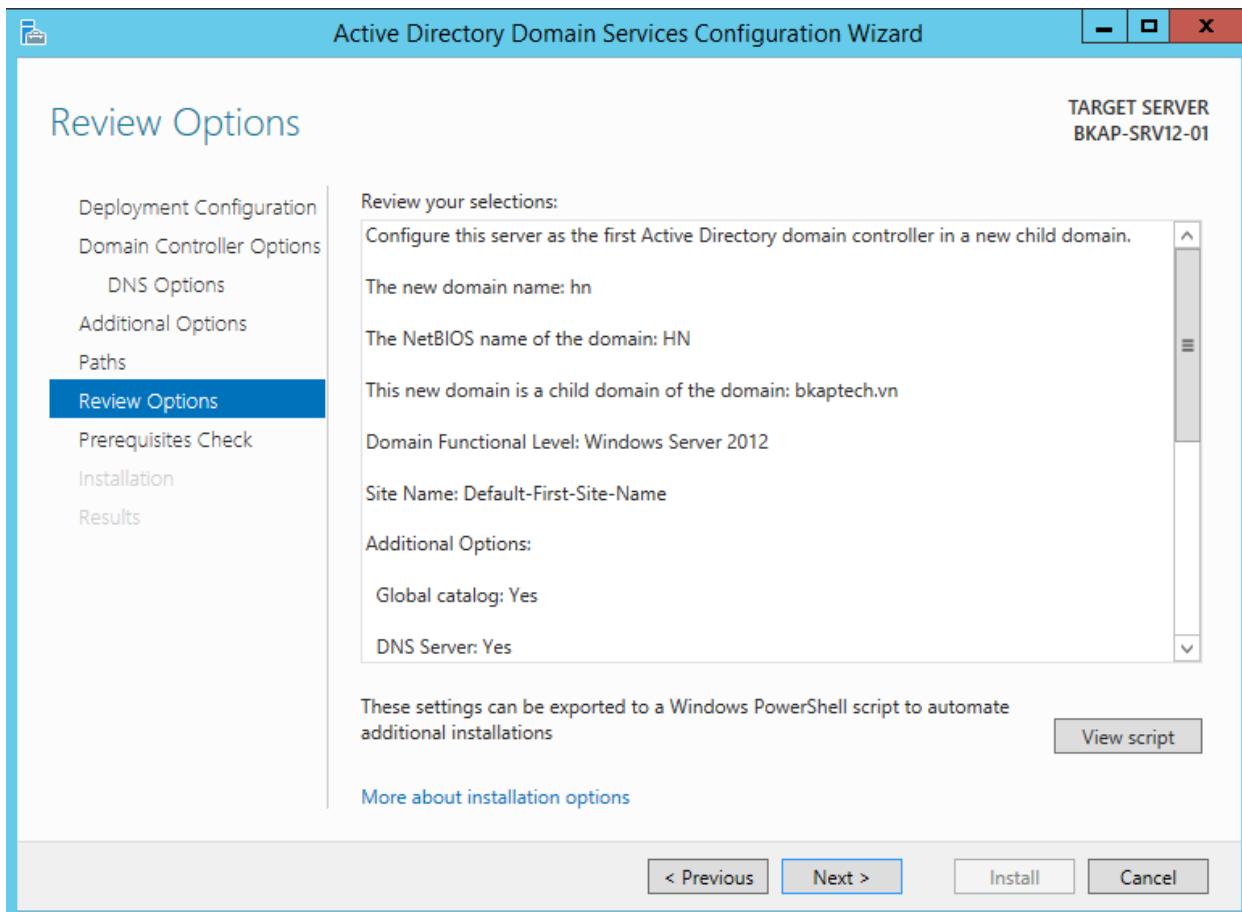
- Tại cửa sổ **Additional Options**, kiểm tra **The NetBIOS domain name: HN**, click vào **Next**.



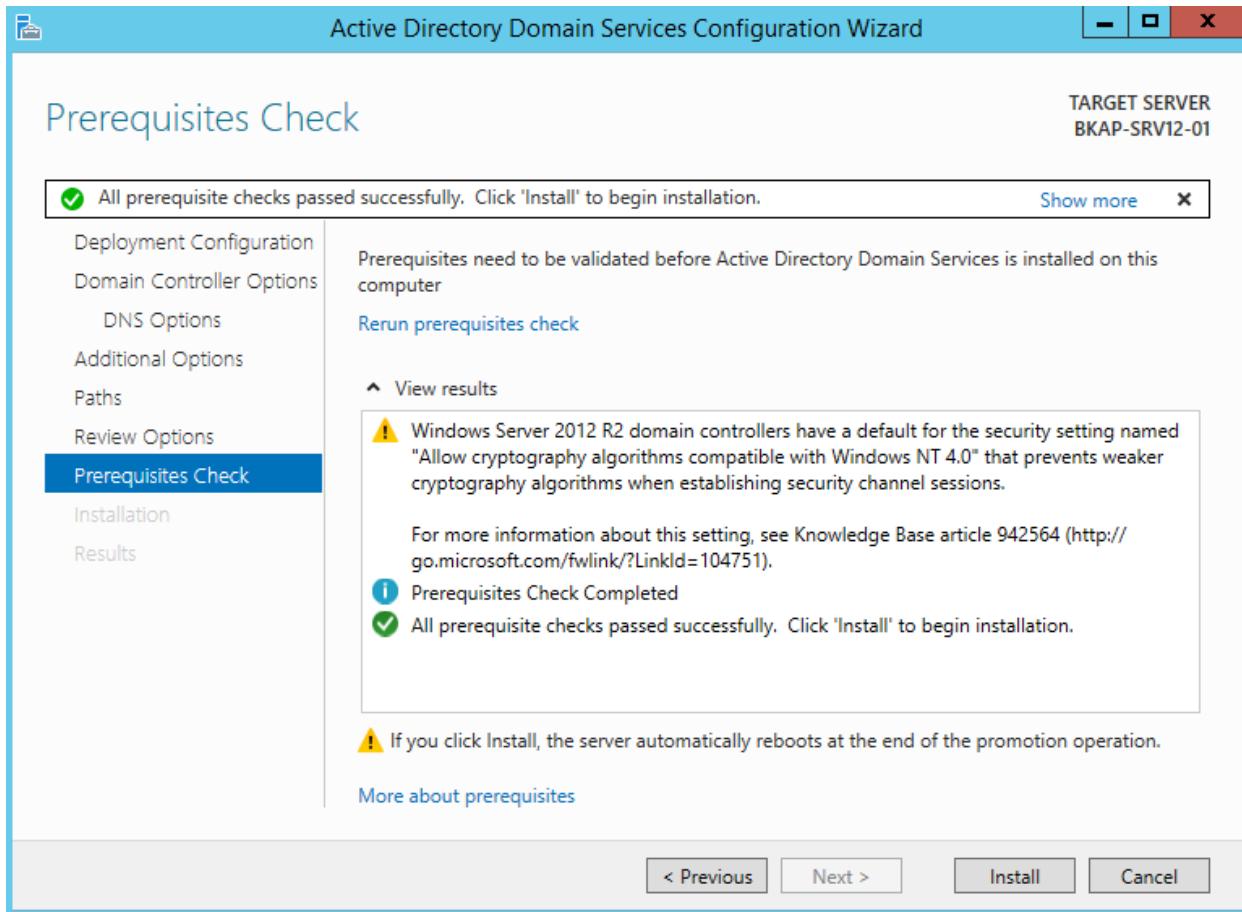
- Tại cửa sổ **Paths**, click vào **Next**.



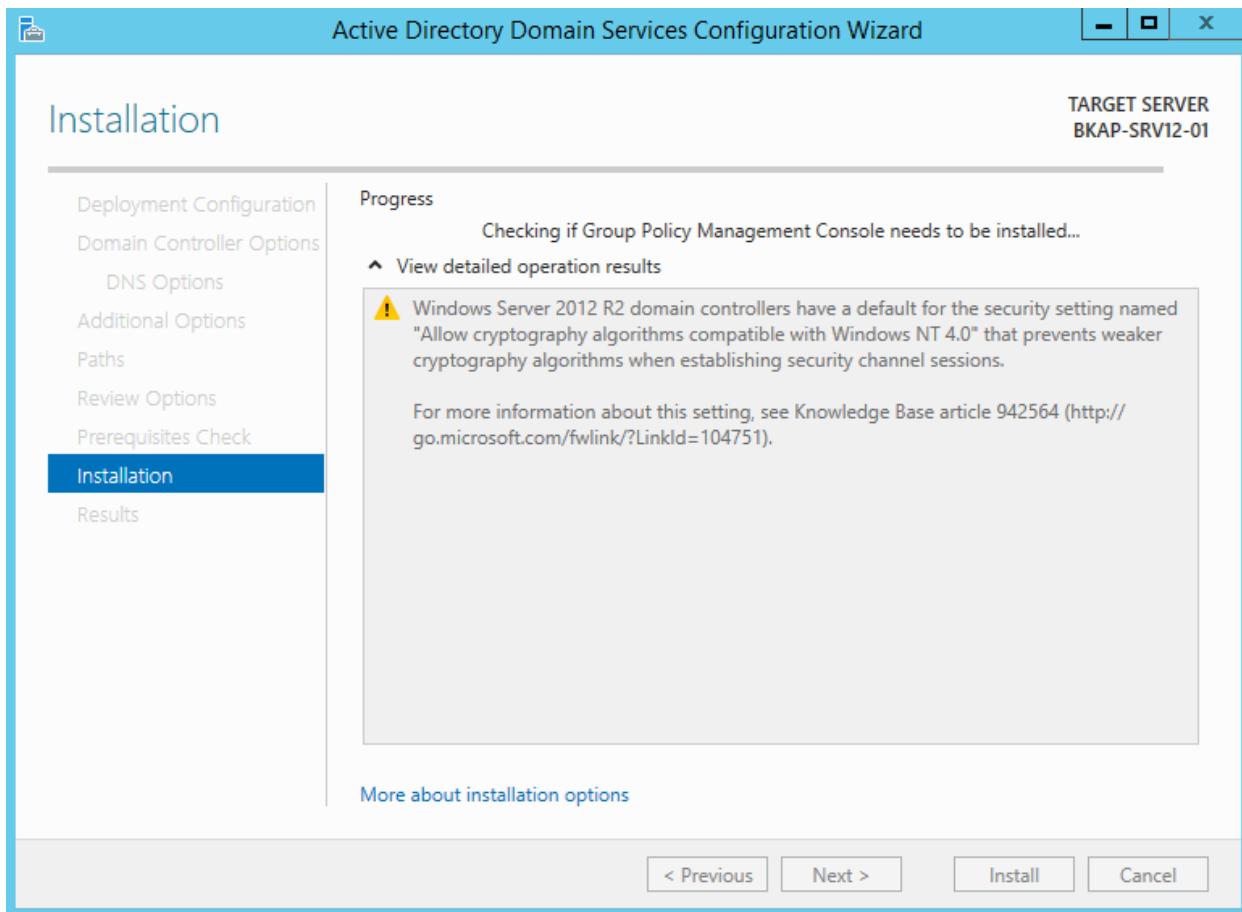
- Tại cửa sổ **Review Options**, click vào **Next**.



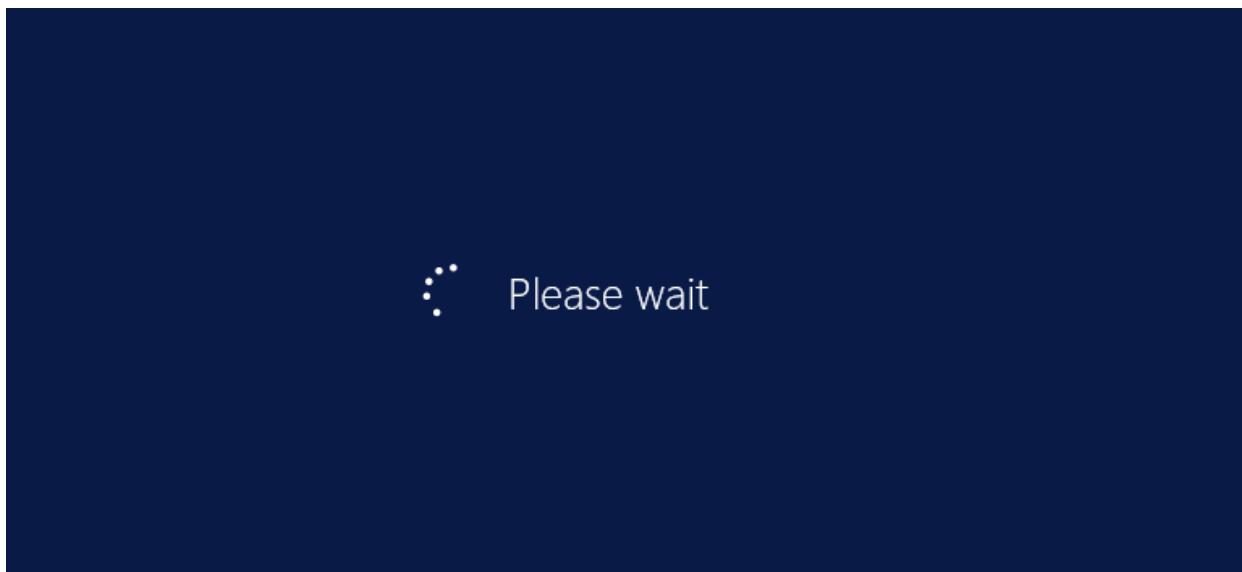
- Tại cửa sổ **Prerequisites Check**, click vào **Install**.



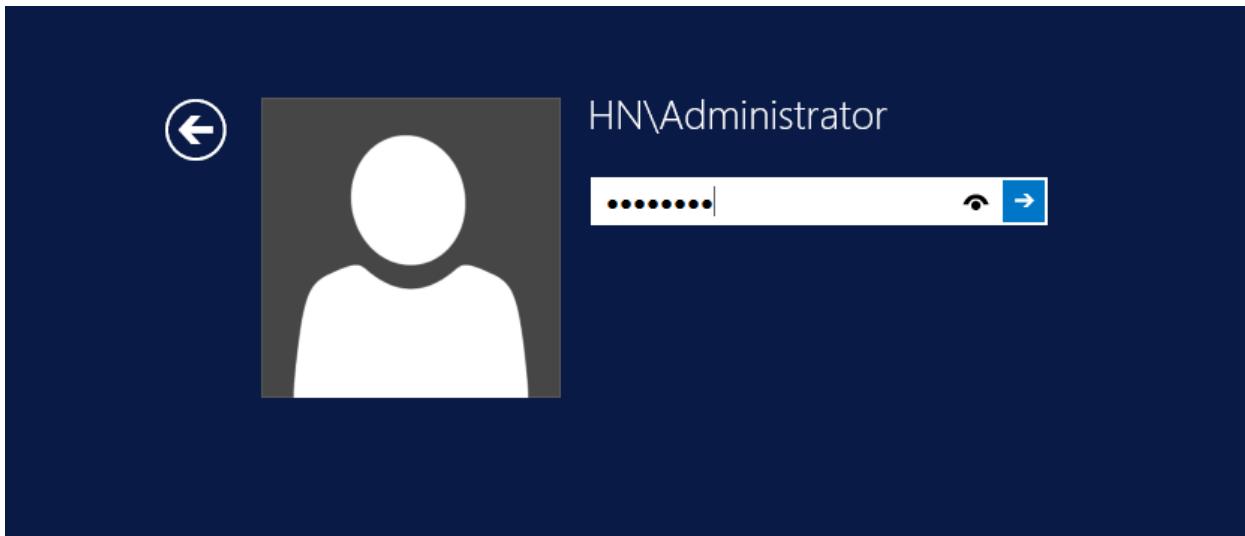
- Server tiến hành kiểm tra và cài đặt.



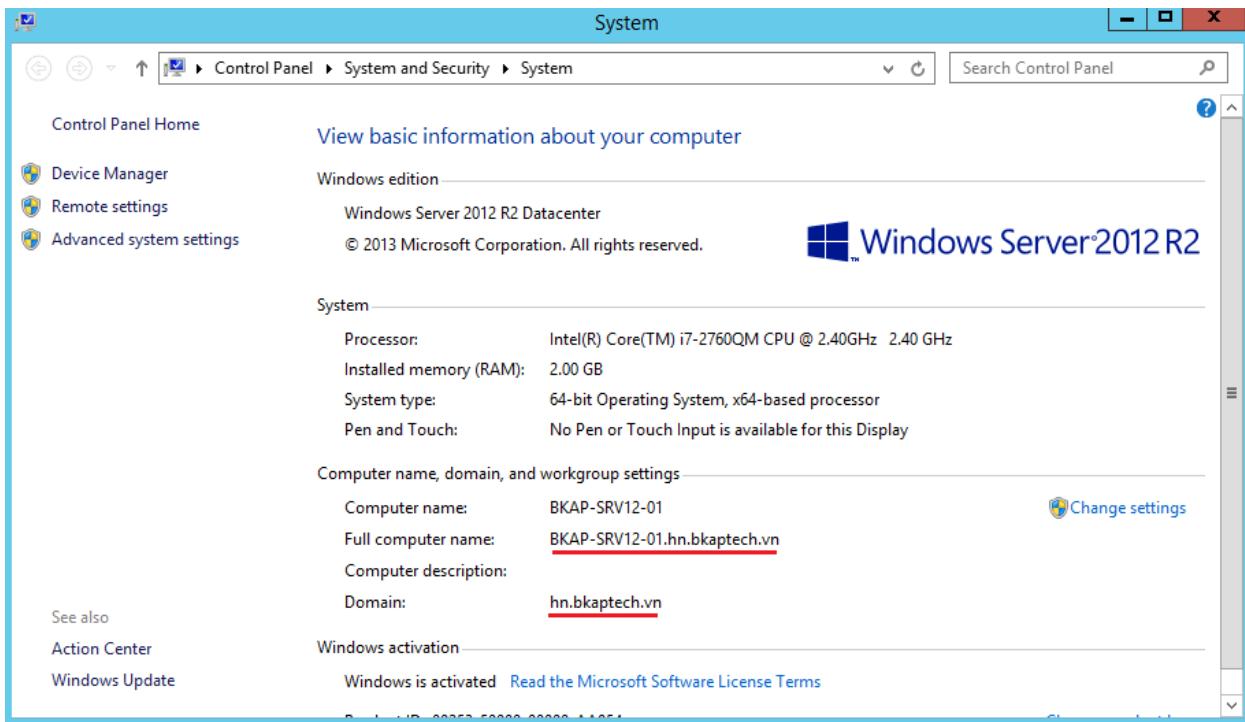
- Máy chủ tự động reset.



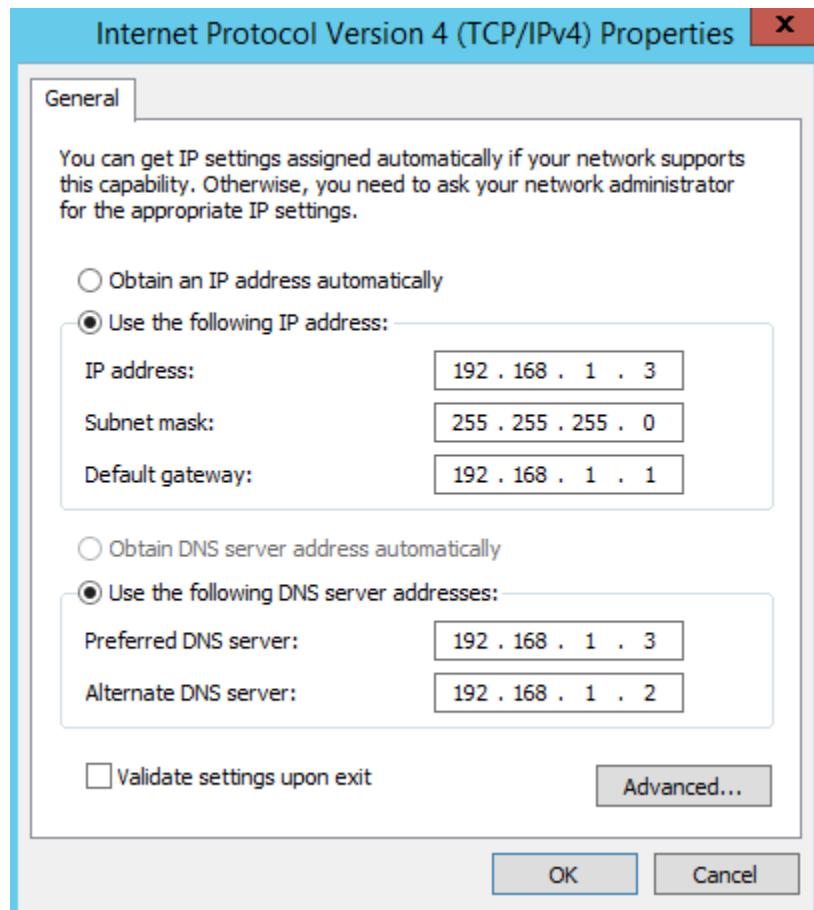
- Đăng nhập lại vào hệ thống.



- Kiểm tra tên domain, tên máy.



- Kiểm tra địa chỉ IP của máy *BKAP-SRV12-01*.

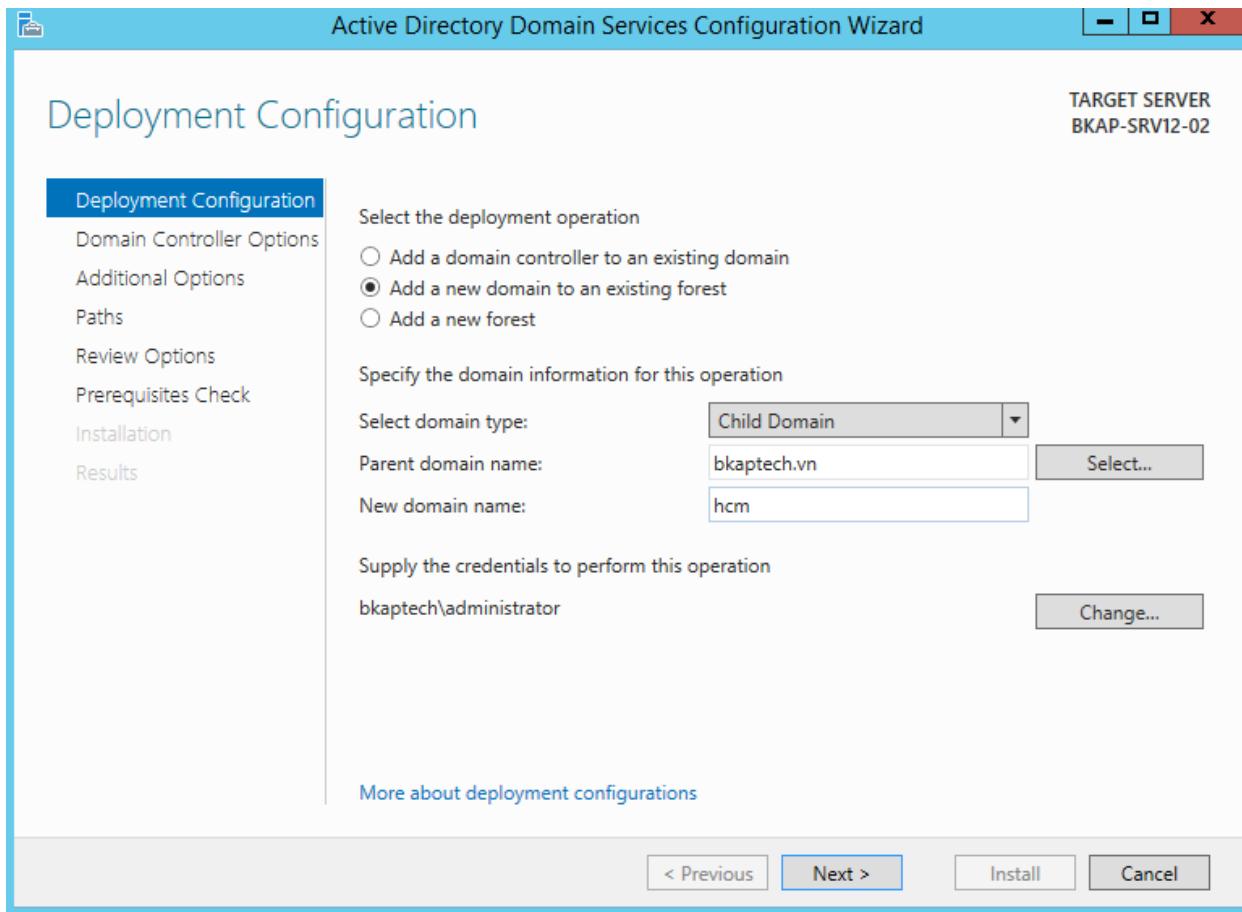


- Cấu hình **DNS Server** trên máy *BKAP-SRV12-01*:

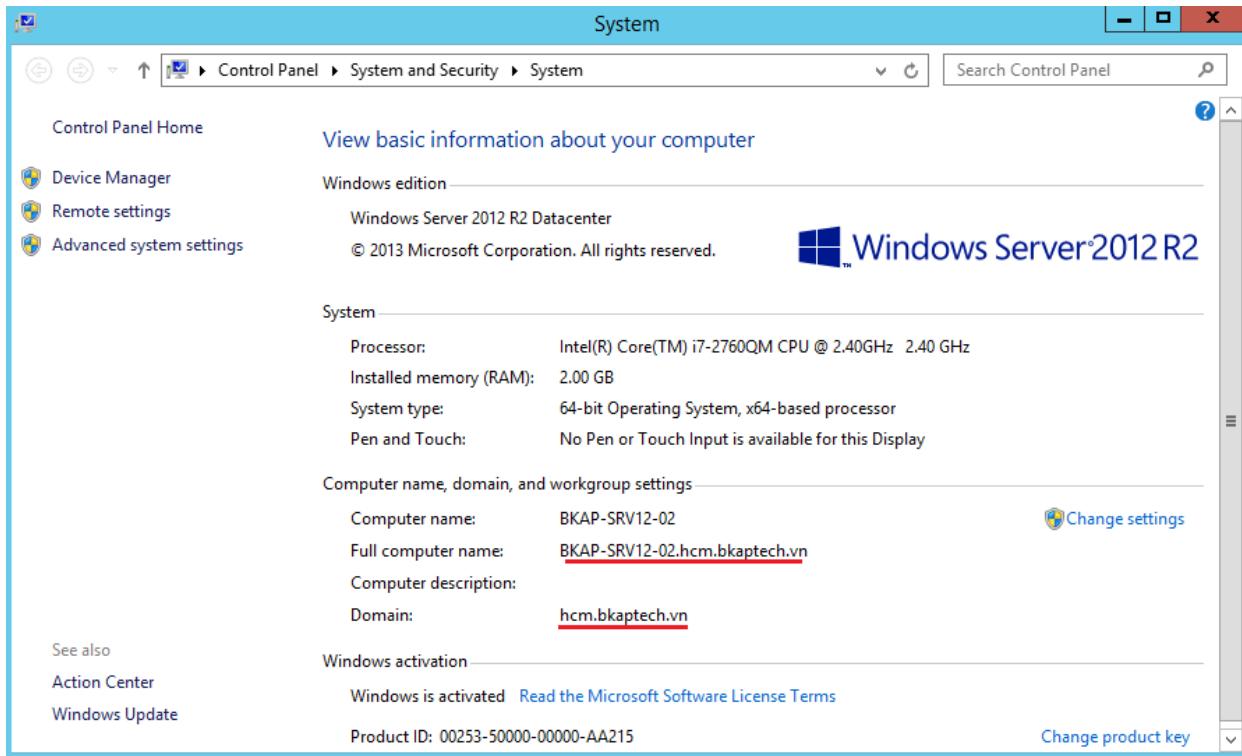
- Kết quả như sau:

The screenshot shows a Windows Command Prompt window titled "Administrator: C:\Windows\system32\cmd.exe - nslookup". The window displays the following text:
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.
C:\Users\Administrator>nslookup
Default Server: bkap-srv12-01.hn.bkaptech.vn
Address: 192.168.1.3
> -

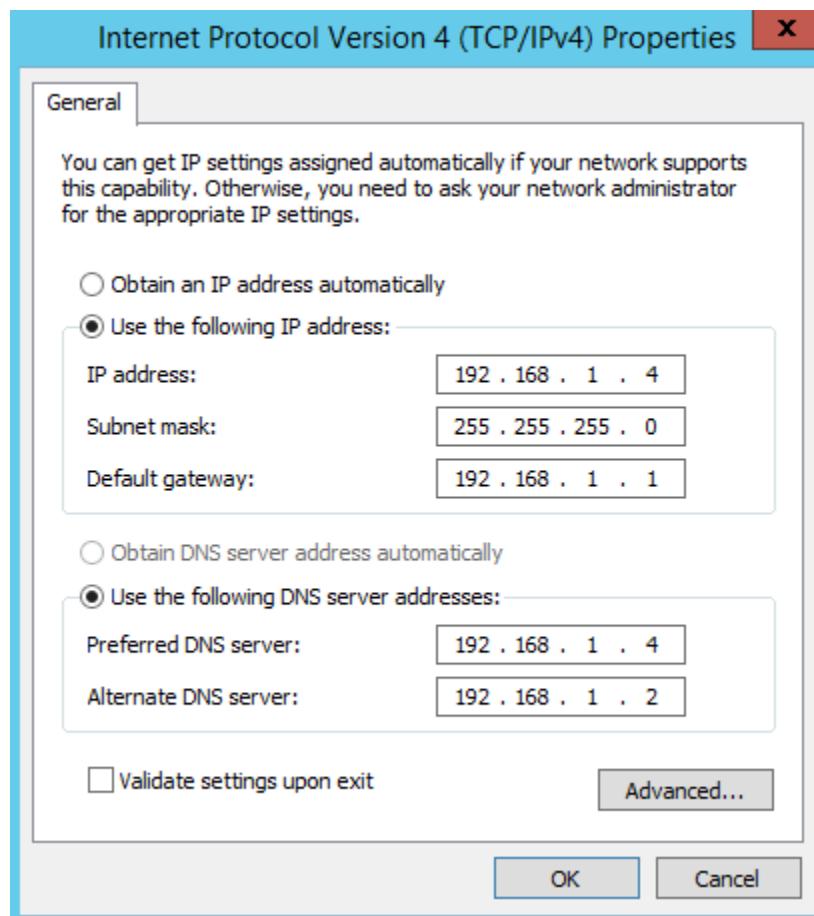
- Chuyển sang máy *BKAP-SRV12-02*, thực hiện các bước tương tự như trên, nâng cấp máy *BKAP-SRV12-02* lên **Child Domain** với tên miền là *hcm.bkaptech.vn*.



- Kiểm tra kết quả.



- Kiểm tra địa chỉ IP của máy *BKAP-SRV12-02*.

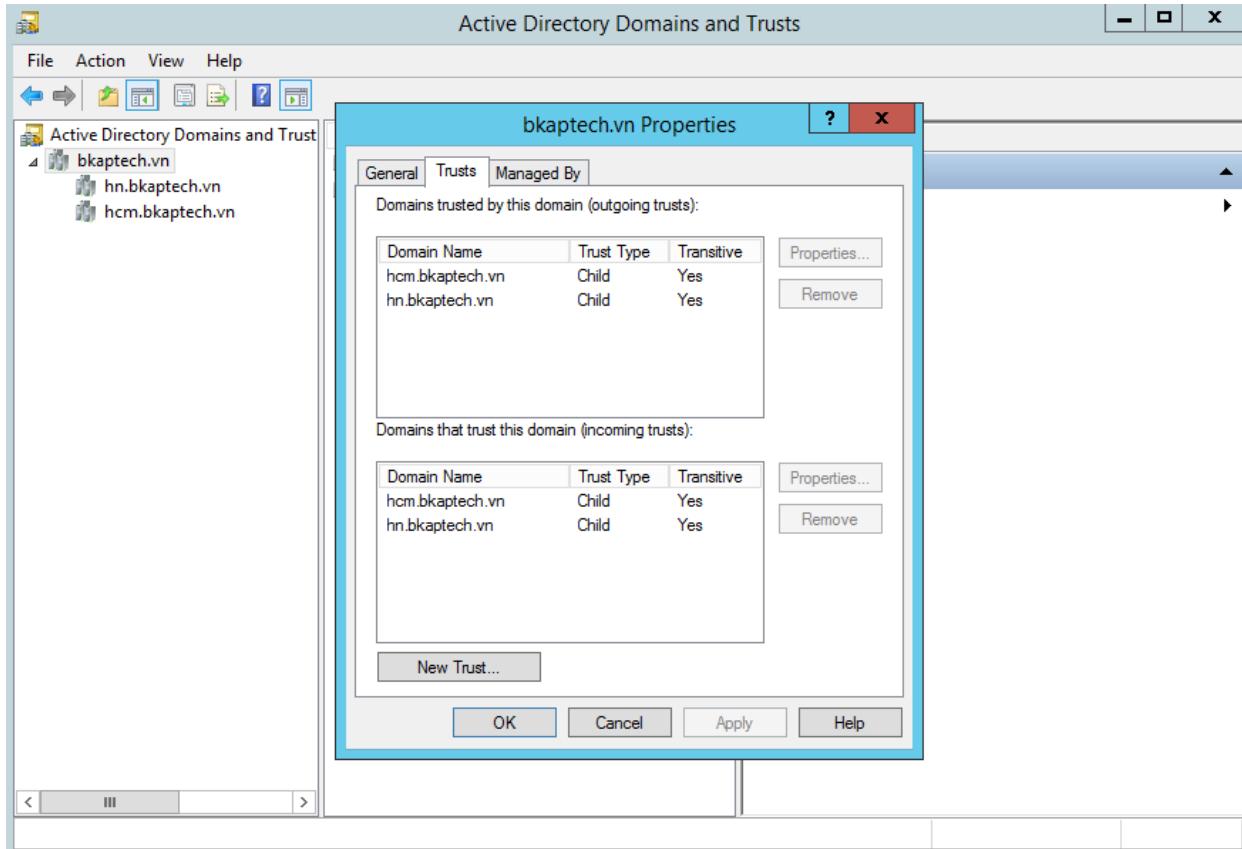


- Cấu hình **DNS Server** trên máy *BKAP-SRV12-02*.

- Kết quả như sau:

The screenshot shows a Windows Command Prompt window titled "Administrator: C:\Windows\system32\cmd.exe - nslookup". The window displays the following text:
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.
C:\Users\Administrator>nslookup
Default Server: bkap-srv12-02.hcm.bkaptech.vn
Address: 192.168.1.4
>

- Chuyển về máy *BKAP-DC12-01*, vào **Active Directory Domains and Trusts**, kiểm tra trust giữa 2 miền.



- Kiểm tra ping giữa các miền trong forest.

The screenshot shows a Windows PowerShell window titled "Administrator: Windows PowerShell". The command PS C:\Users\Administrator> ping hn.bkaptech.vn is run, followed by PS C:\Users\Administrator> ping hcm.bkaptech.vn. Both commands return successful ping results with 0% loss and low round-trip times. The window has a standard Windows title bar and a blue background.

```
Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> ping hn.bkaptech.vn
Pinging hn.bkaptech.vn [192.168.1.3] with 32 bytes of data:
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

PS C:\Users\Administrator>
PS C:\Users\Administrator> ping hcm.bkaptech.vn

Pinging hcm.bkaptech.vn [192.168.1.4] with 32 bytes of data:
Reply from 192.168.1.4: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

4.2 Thực hiện Trust Forest

1.Yêu cầu bài Lab:

- + BKAP-DC12-01: Cấu hình hệ thống tên miền DNS.
- + BKAP-DC12-02: Cấu hình hệ thống tên miền DNS.
- + Cấu hình *Trust Forest Domain* giữa 2 máy.
- + Kiểm tra share folder giữa 2 máy thuộc 2 miền.

2.Yêu cầu chuẩn bị:

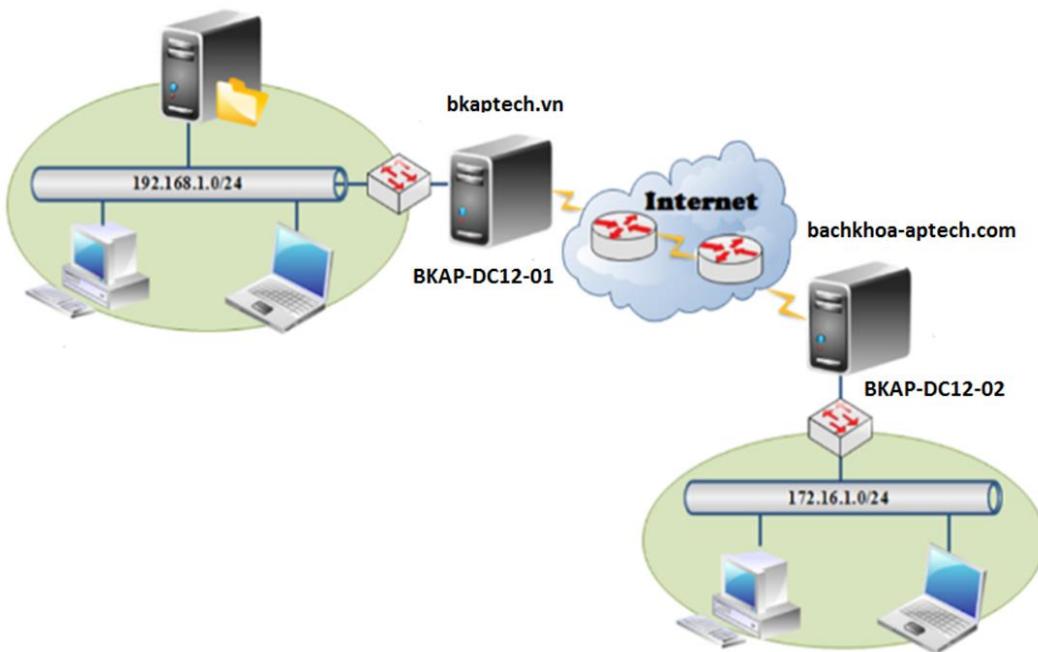
- + Máy **BKAP-DC12-01**: đã nâng cấp lên Domain Controller quản lý miền **bkaptech.vn**.
- + Máy **BKAP-DC12-02**: đã nâng cấp lên Domain Controller quản lý miền **bachkhoa-aptech.com**.

3.Mô hình Lab:

HỆ THỐNG ĐÀO TẠO CNTT QUỐC TẾ BACHKHOA-APTECH



Triển khai thực hiện Trust Forest

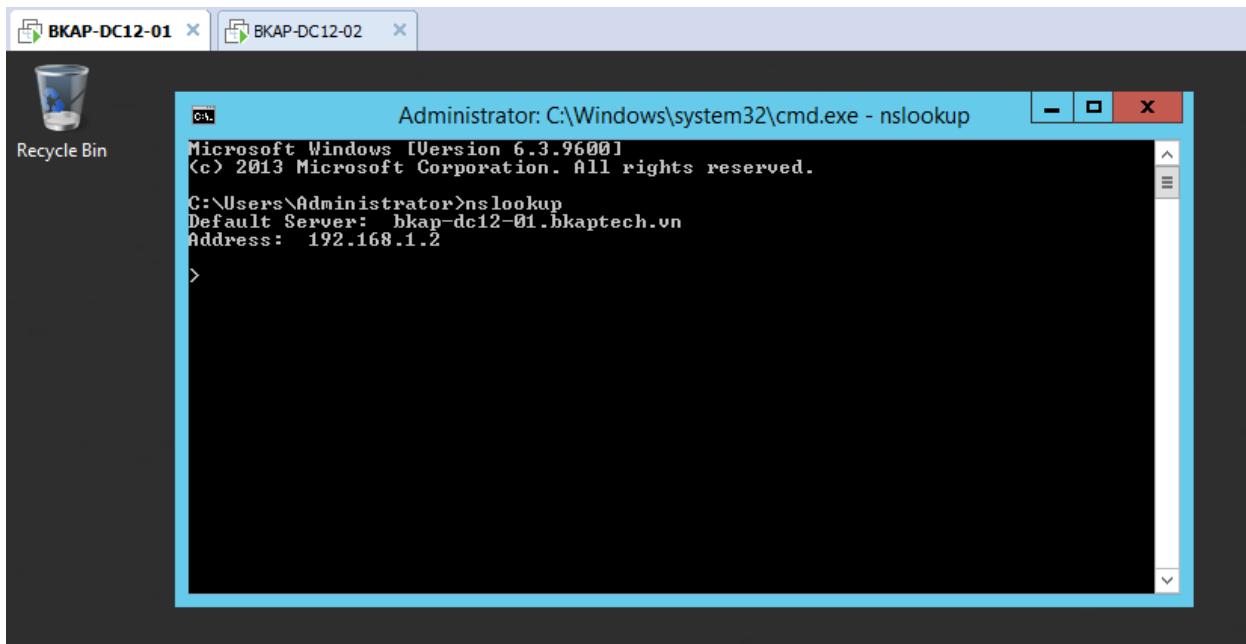


Sơ đồ địa chỉ sau:

Thông số	BKAP-DC12-01	BKAP-DC12-02
<i>IP address</i>	192.168.1.2	192.168.1.3
<i>Subnet Mask</i>	255.255.255.0	255.255.255.0
<i>Default Gateway</i>	192.168.1.1	192.168.1.1
<i>DNS Server</i>	192.168.1.2	192.168.1.3

Hướng dẫn chi tiết:

- Thực hiện cấu hình **DNS Server**, kiểm tra phân giải địa chỉ IP sang tên miền trên 2 máy Server **BKAP-DC12-01** và **BKAP-DC12-02**.
 - Máy **BKAP-DC12-01**.



- Máy BKAP-DC12-02.

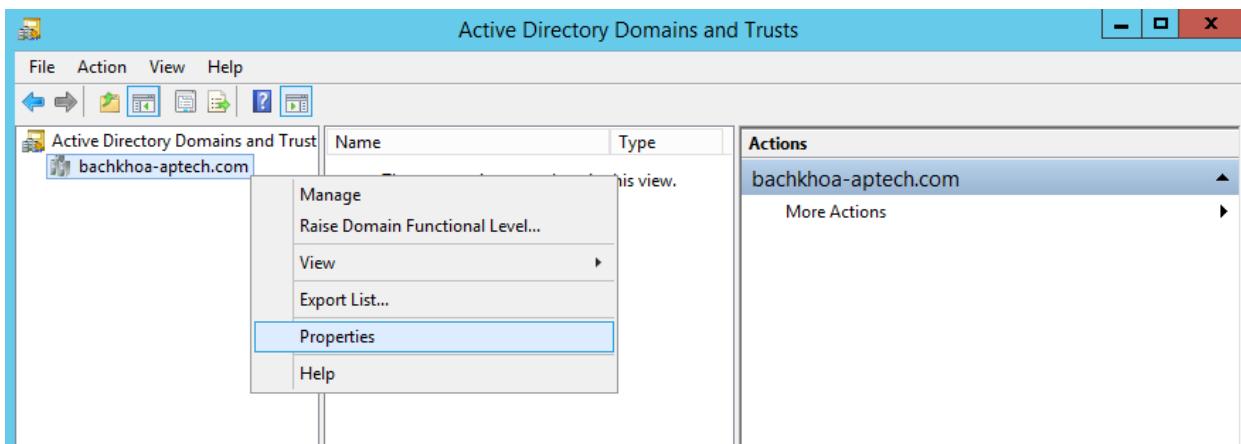
```
Administrator: C:\Windows\system32\cmd.exe - nslookup
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>nslookup
Default Server: bkap-dc12-01.bkaptech.vn
Address: 192.168.1.2

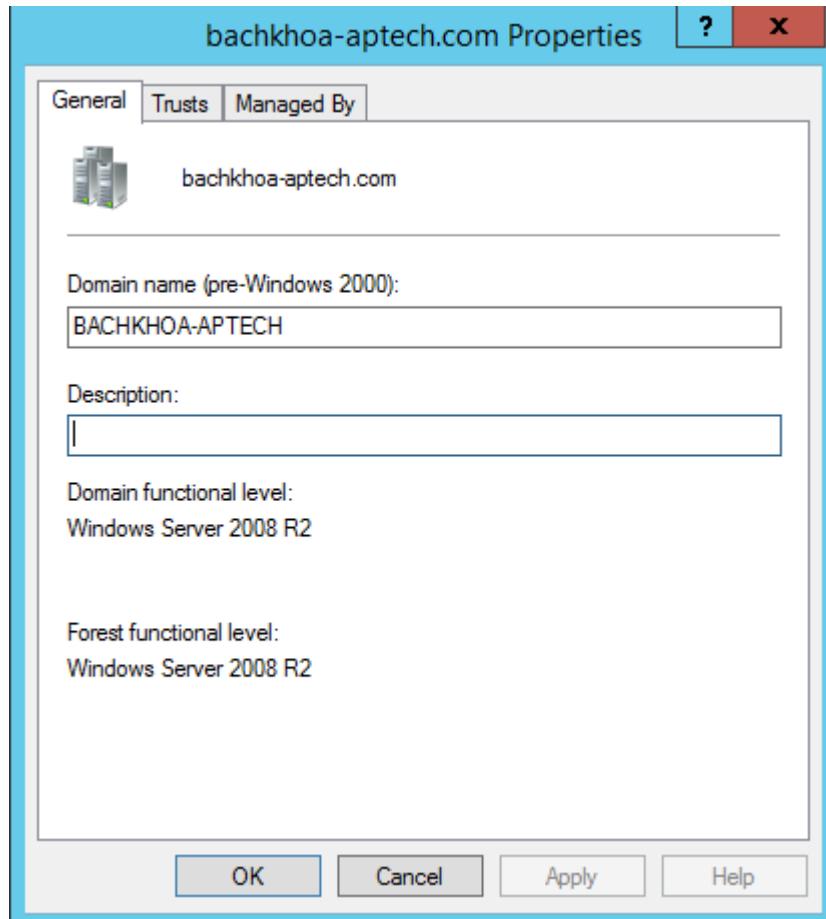
>
```

- Thực hiện Trust Forest.

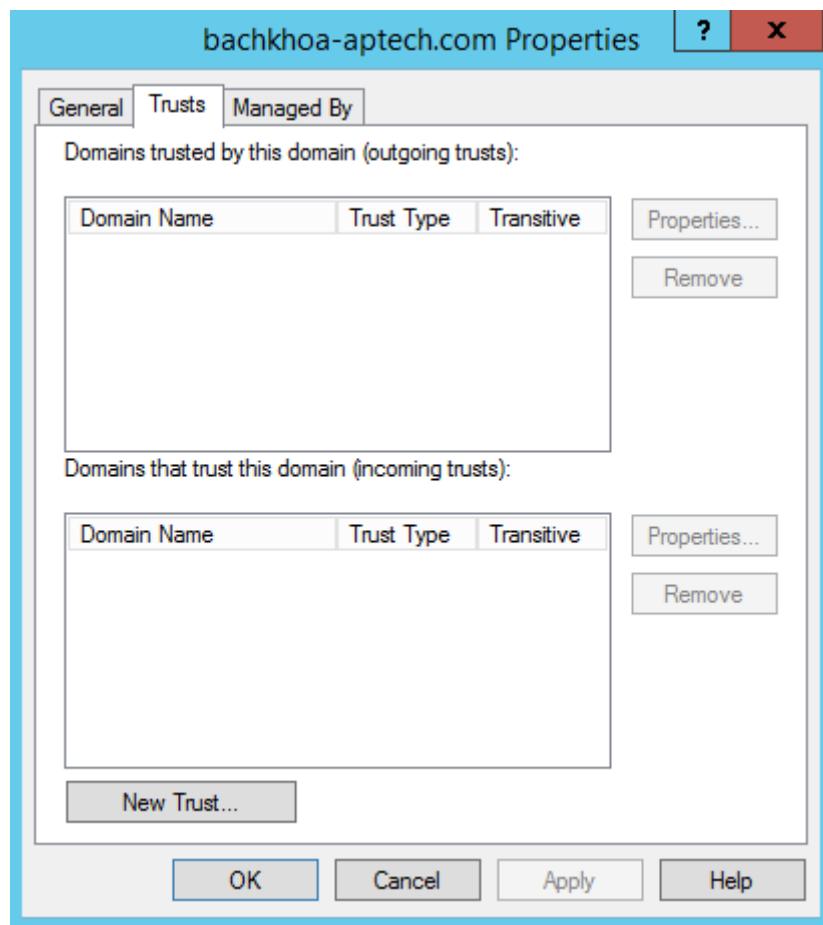
- Trên máy BKAP-DC12-02 , vào **Server Manager / Tools / Active Directory Domains and Trusts**.
- Trong cửa sổ **Active Directory Domains and Trusts**, click chuột phải tại tên domain **bachkhoa-aptech.com** , chọn **Properties**.



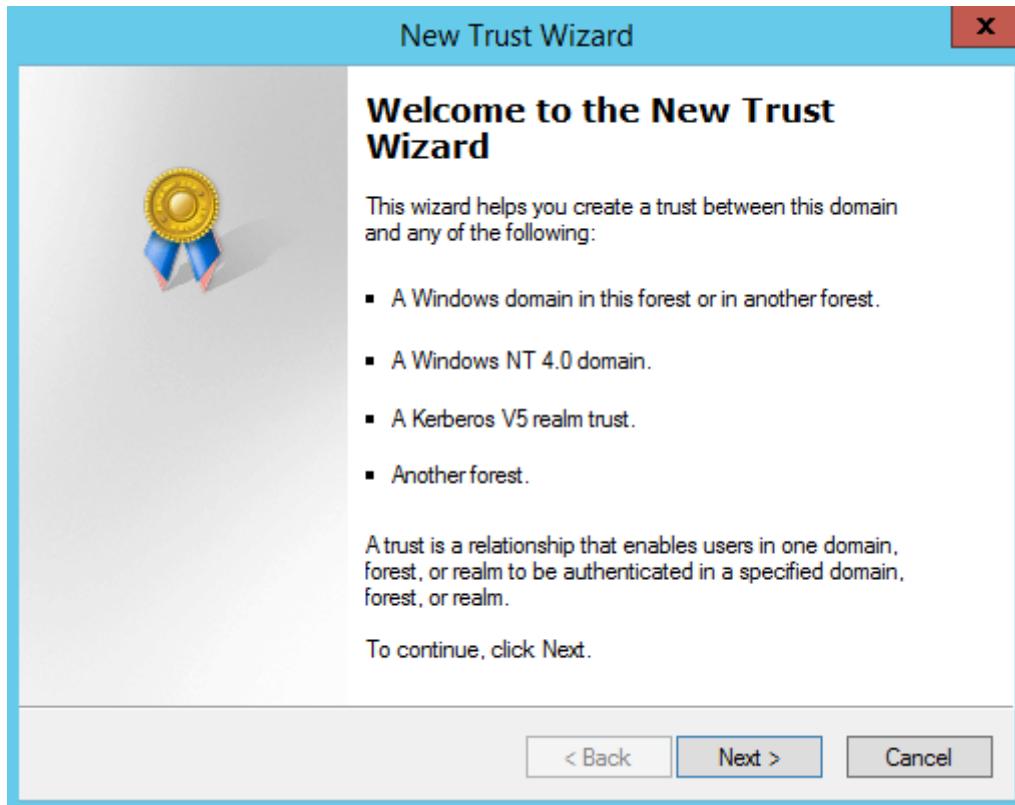
- Trong cửa sổ **bachkhoa-aptech.com Properties**, tại tab **General**, kiểm tra tên *Domain name*: **BACHKHOA-APTECH**.



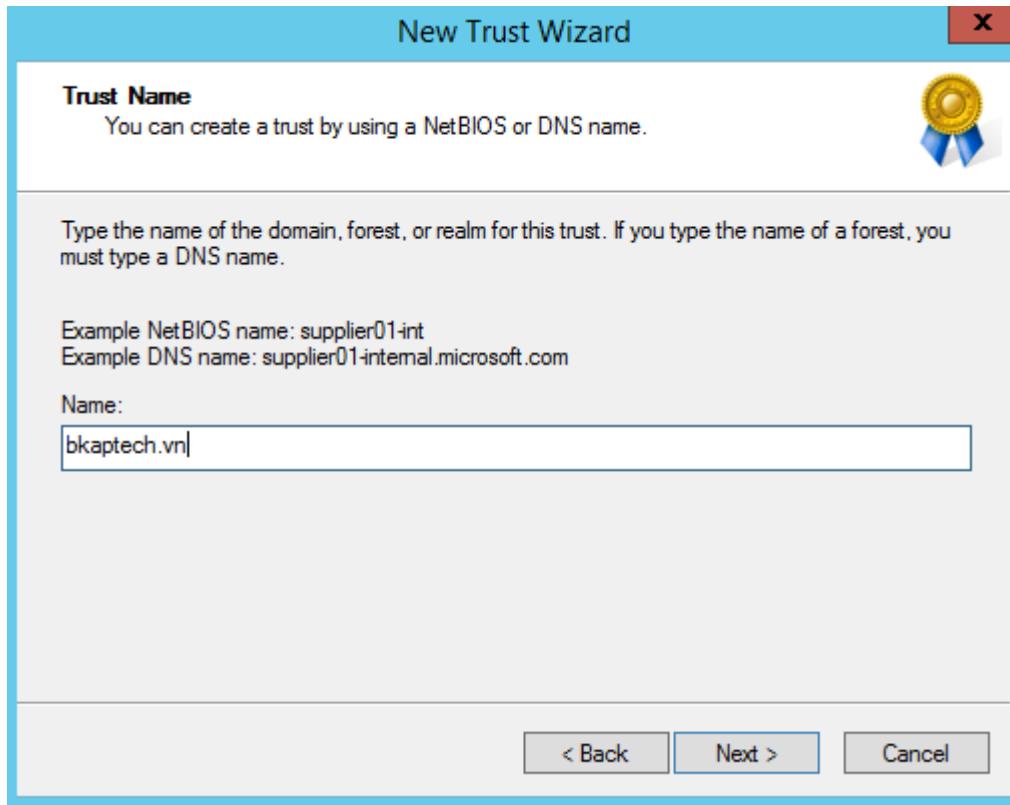
- Chuyển sang tab **Trusts** , click chọn vào **New Trust...**



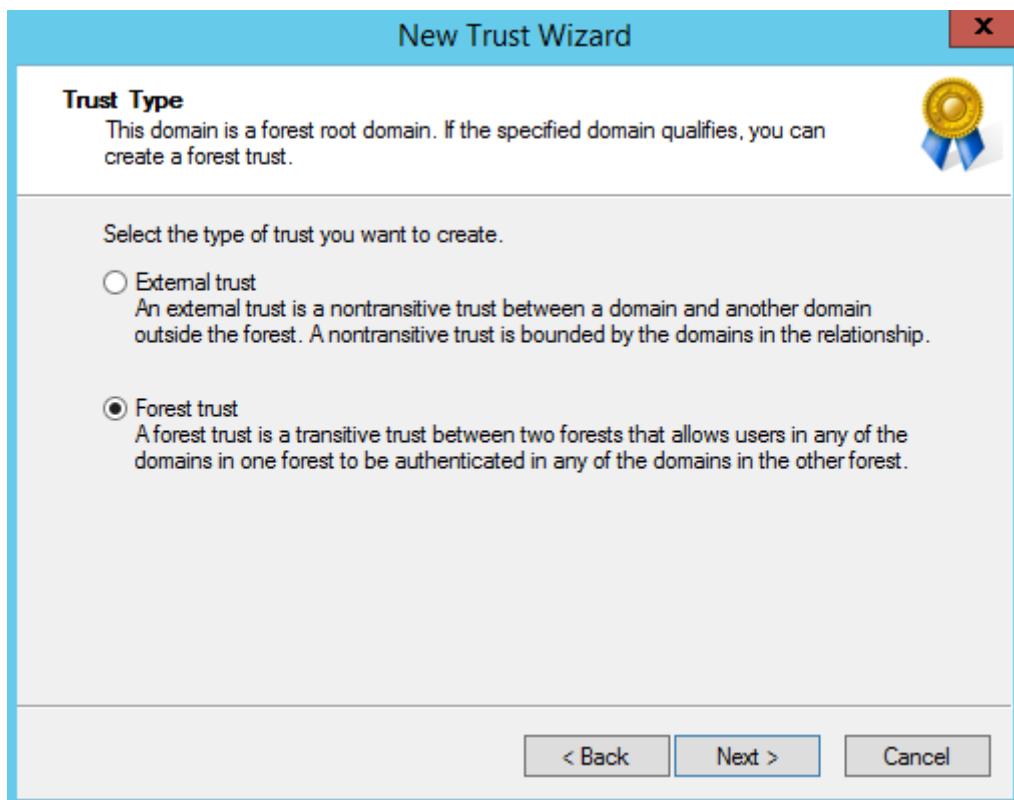
- Tại cửa sổ **Welcome to the New Trust Wizard**, click vào **Next**.



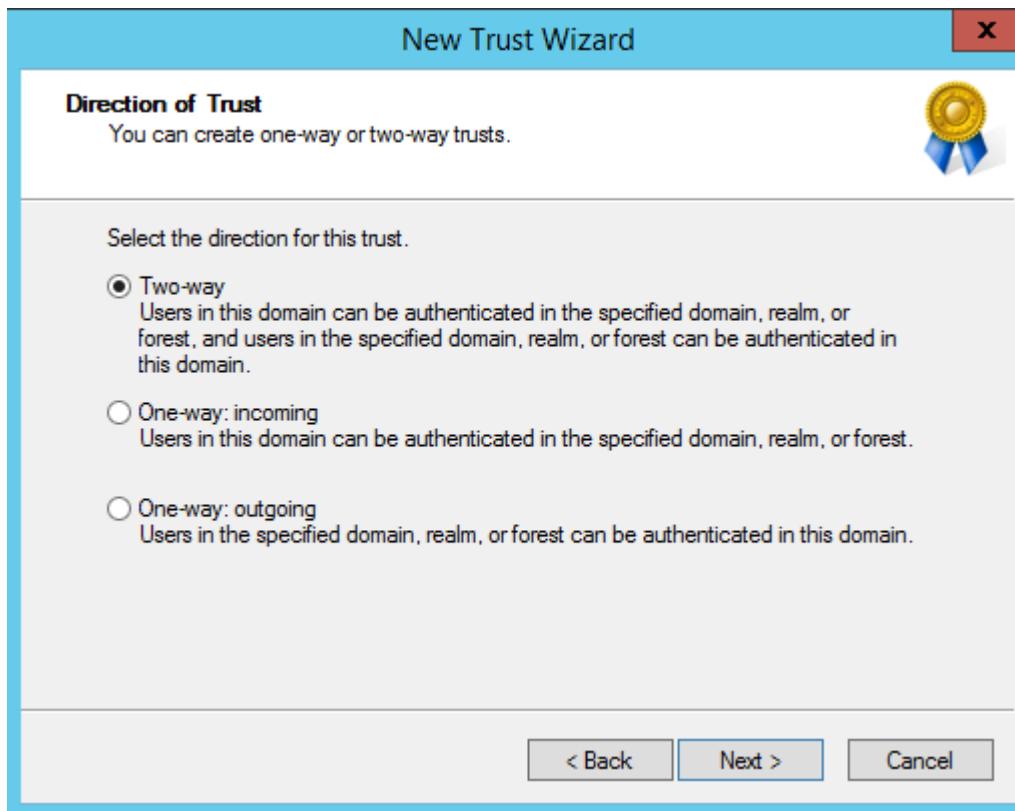
- Tại cửa sổ **Trust Name**, trong mục **Name**, nhập vào tên domain **bkaptech.vn** , Next.



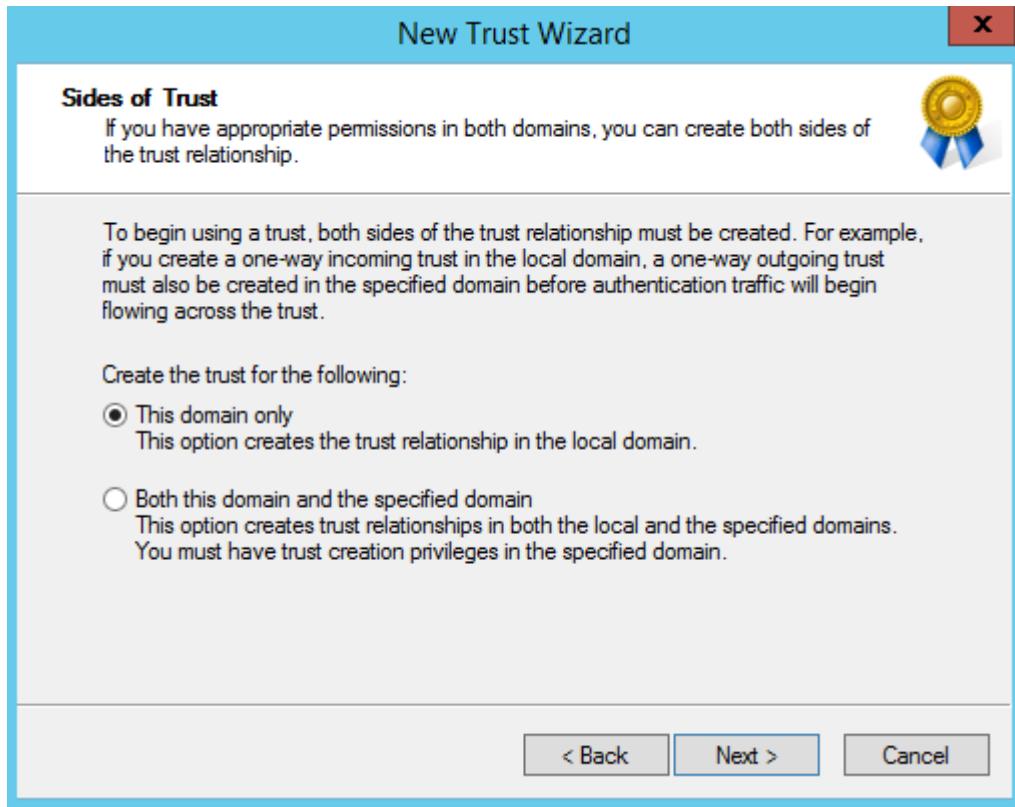
- Tại cửa sổ Trust Type, click chọn vào Forest trust, Next.



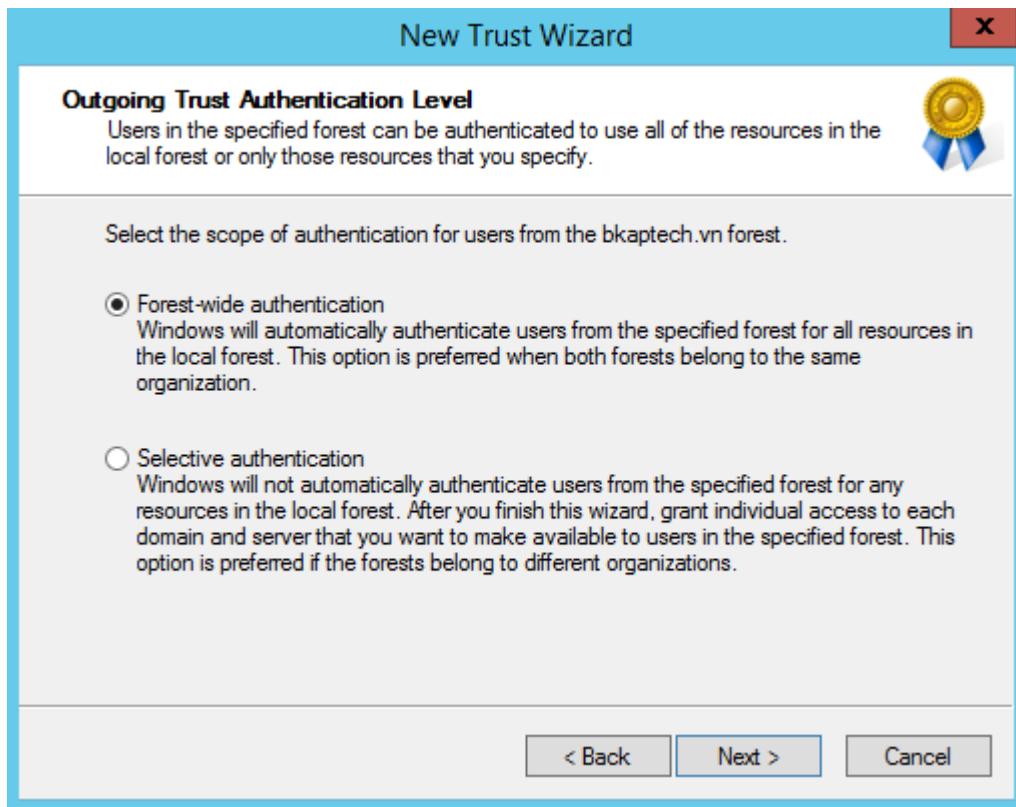
- Tại cửa sổ **Direction of Trust**, click chọn vào **Two-way , Next**.



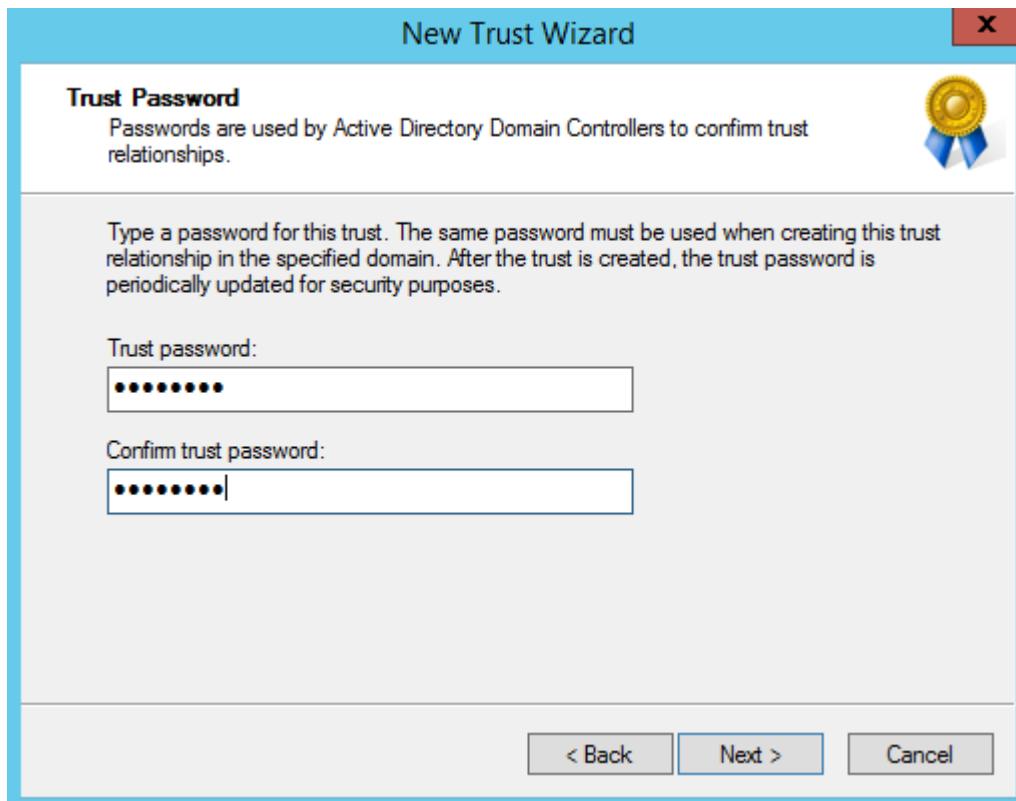
- Tại cửa sổ **Sides of Trust**, click chọn vào **This domain only**, **Next**.



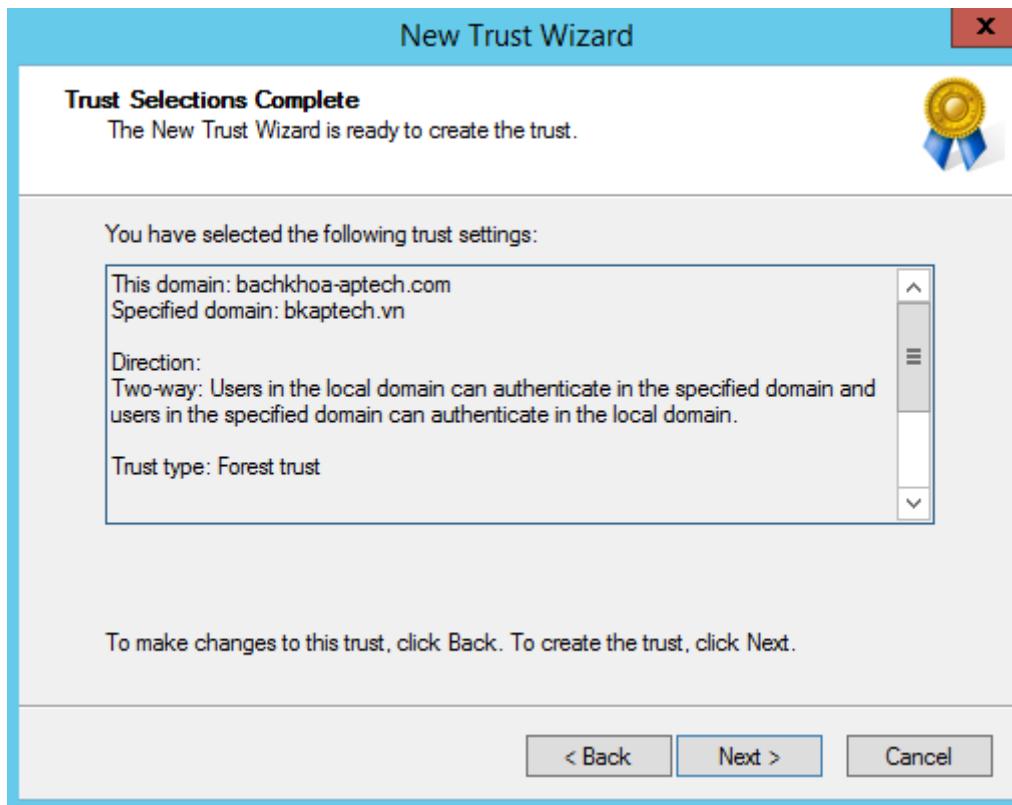
- Tại cửa sổ **Outgoing Trust Authentication Level**, click chọn vào **Forest-wide authentication**, Next.



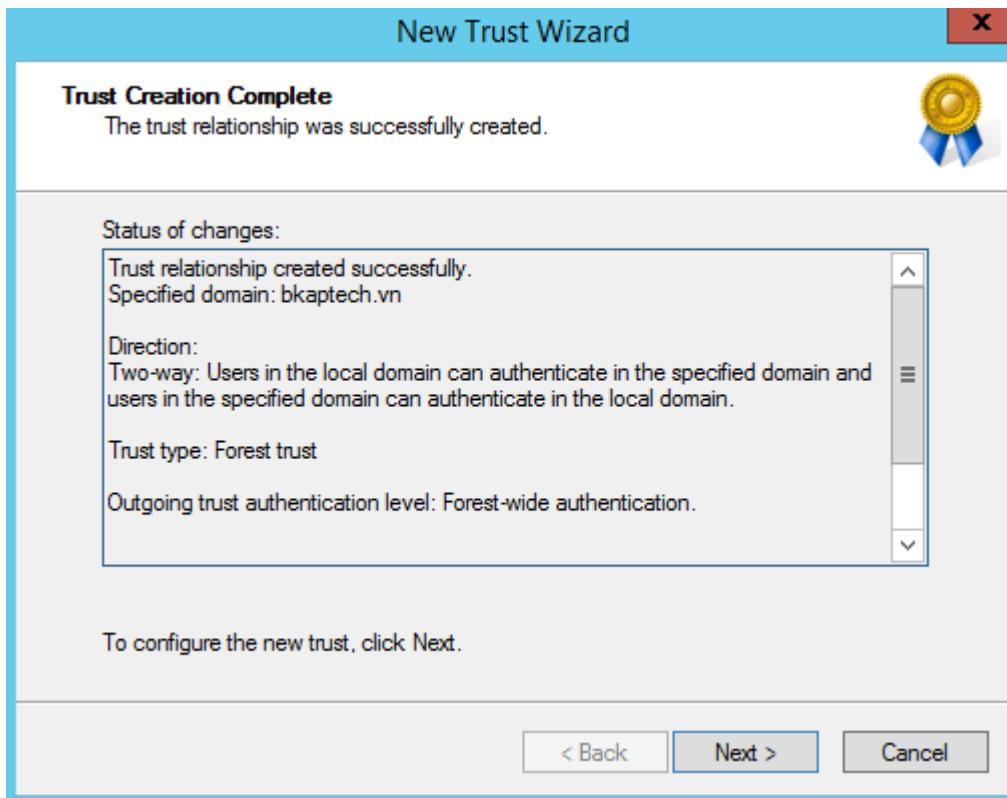
- Tại cửa sổ **Trust Password**, nhập vào password, click vào **Next**.



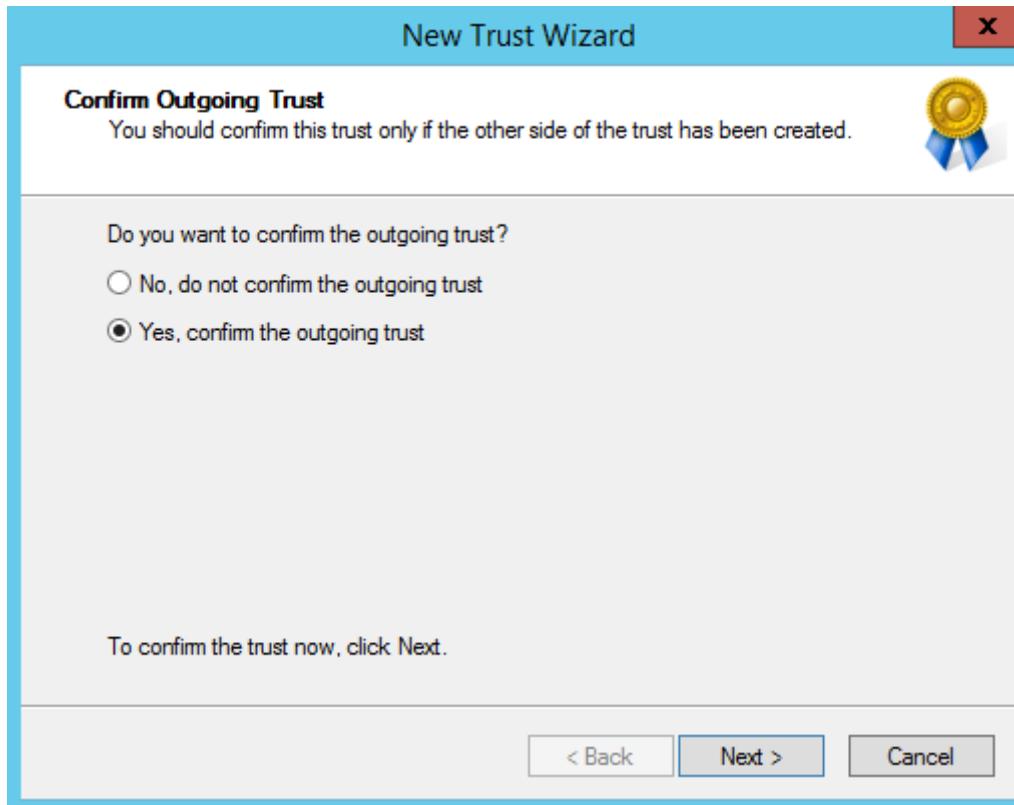
- Tại cửa sổ Trust Selections Complete, click vào Next.



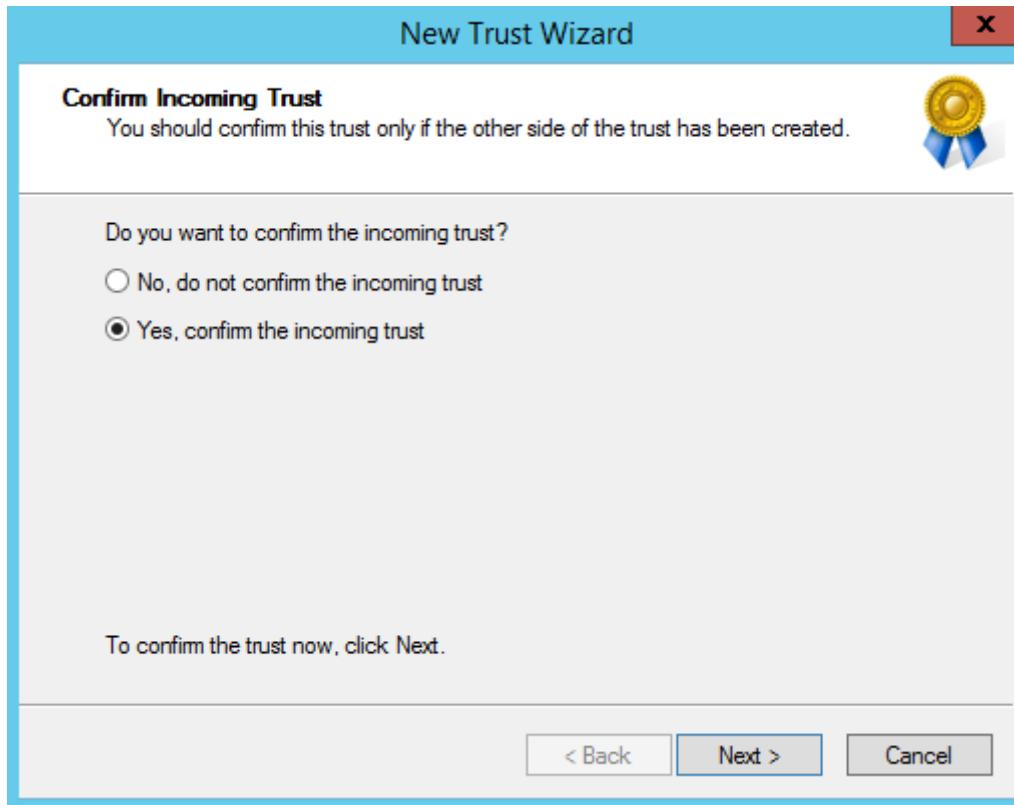
- Tại cửa sổ **Trust Creation Complete**, click vào **Next**.



- Tại cửa sổ **Confirm Outgoing Trust**, click chọn **Yes, confirm the outgoing trust** , click vào **Next**.



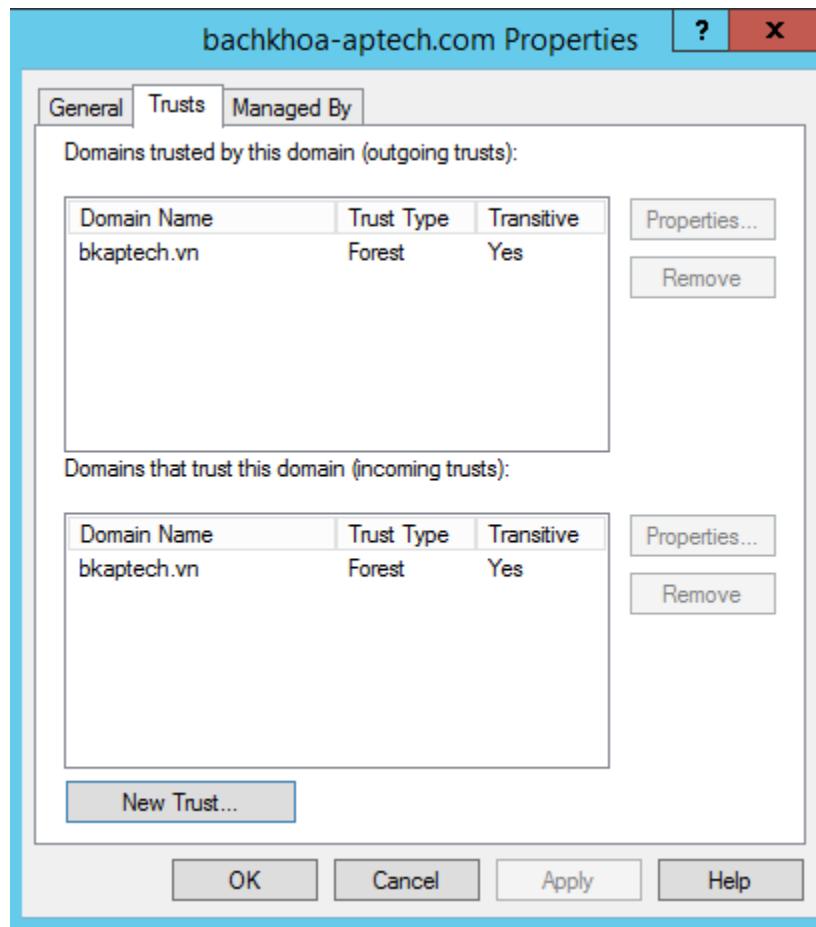
- Tại cửa sổ **Confirm Incoming Trust**, click chọn vào **Yes, confirm the incoming trust**, click vào **Next**.



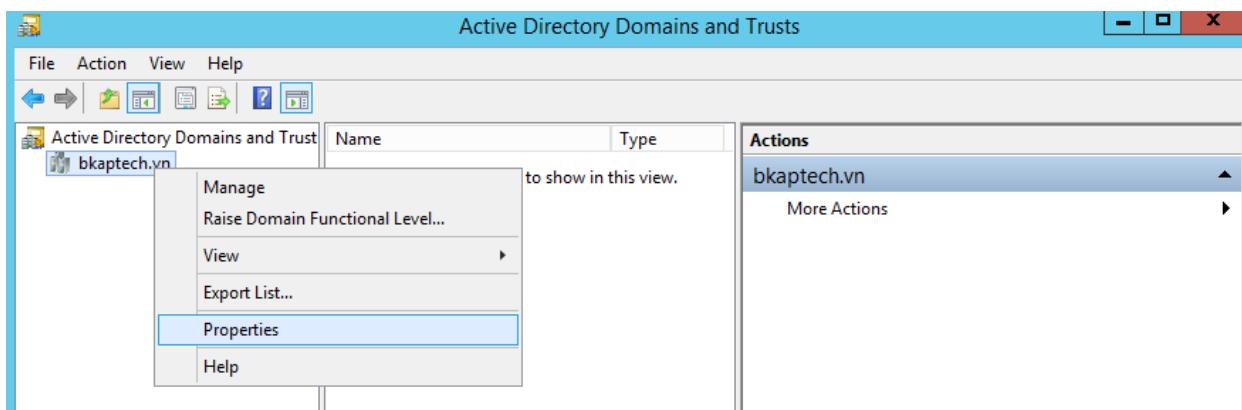
- Tại cửa sổ **Completing the New Trust Wizard**, click vào **Finish**.



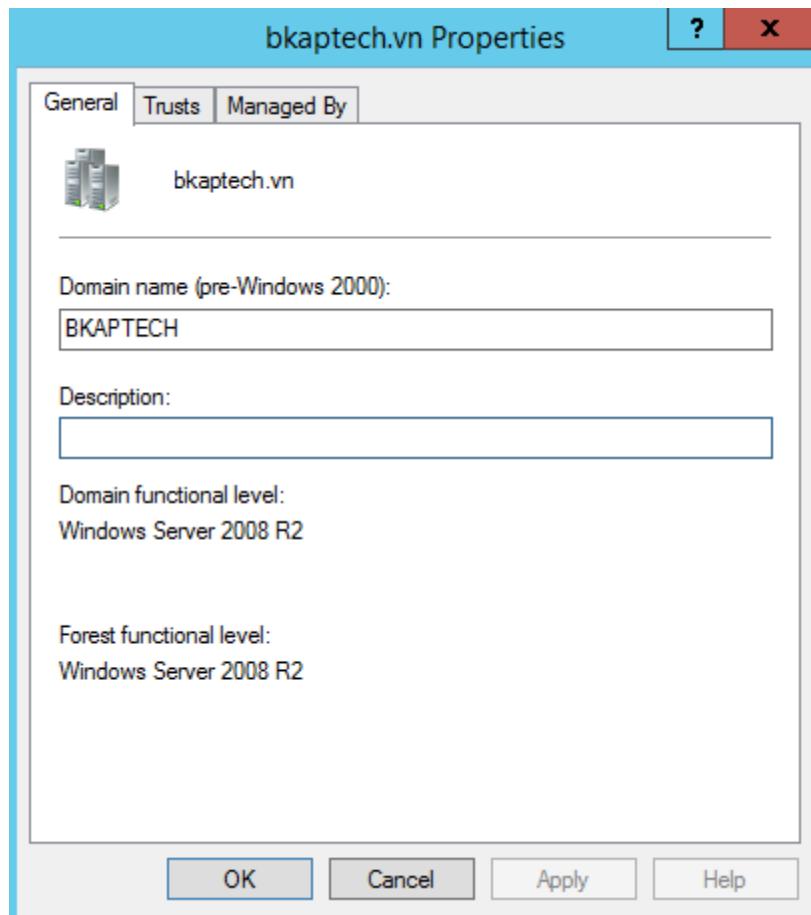
- Trong cửa sổ **bachkhoa-aptech.com Properties**, click chọn **OK**.



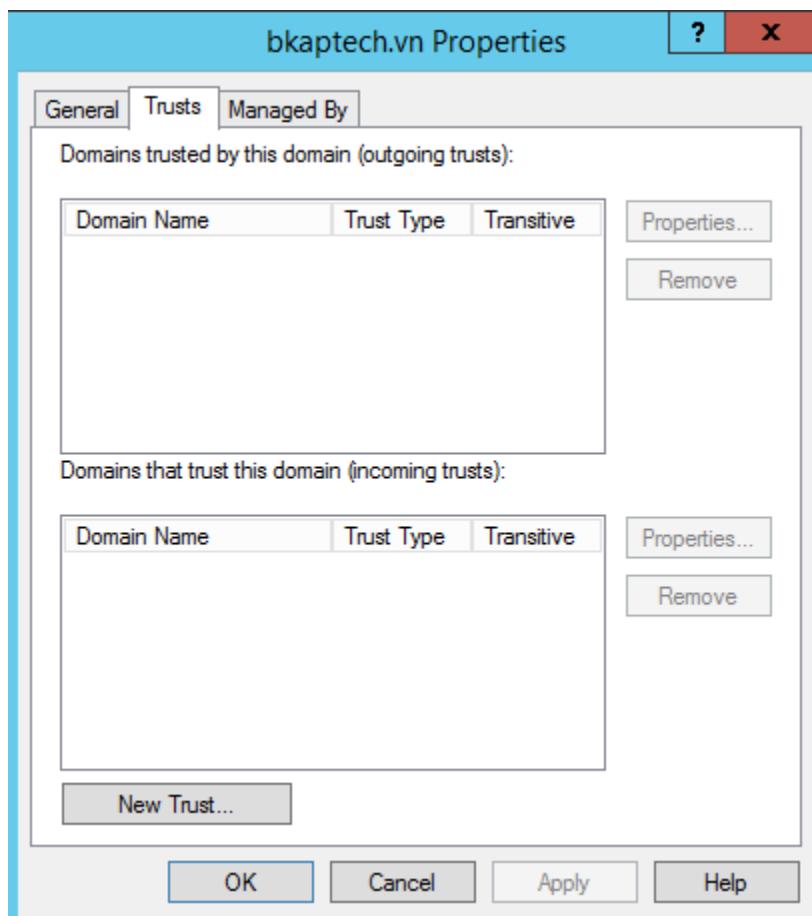
- Chuyển sang máy **BKAP-DC12-01**, thực hiện **Trust Forest**.
 - Vào **Server Manager / Tools / Active Directory Domain and Trusts**.
 - Trong cửa sổ **Active Directory Domains and Trusts**, click chuột phải tại tên domain **bkaptech.vn**, chọn **Properties**.



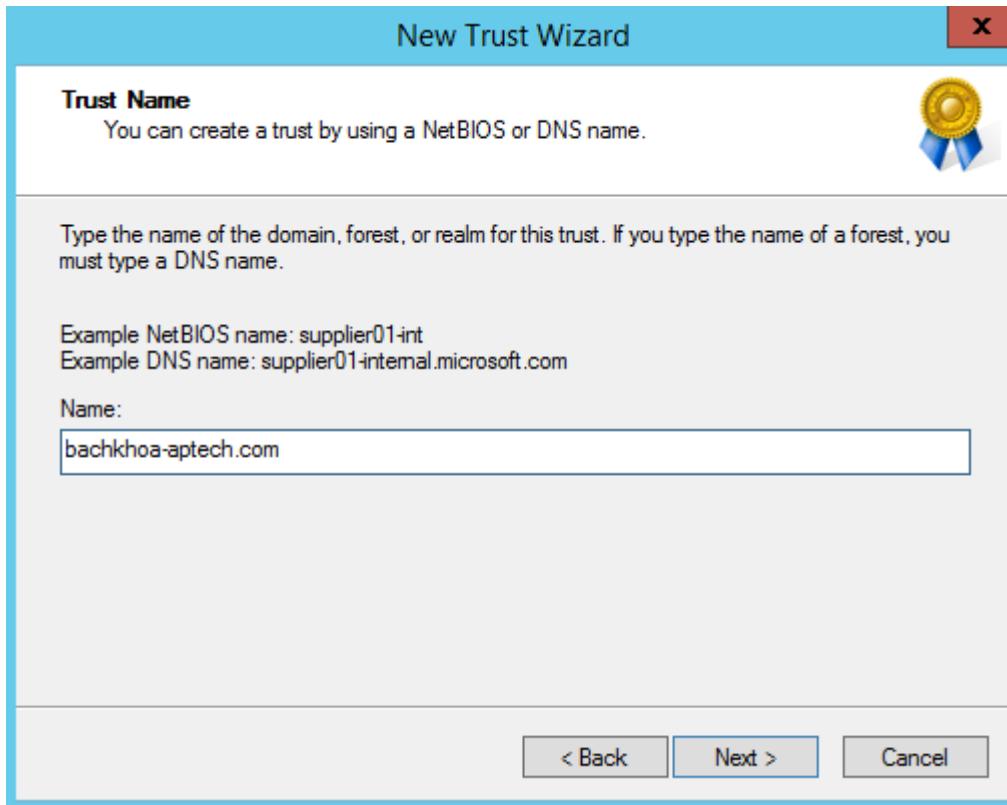
- Tại cửa sổ **bkaptech.vn Properties**, trong tab **General**, kiểm tra tại mục *Domain name : BKAPTECH*.



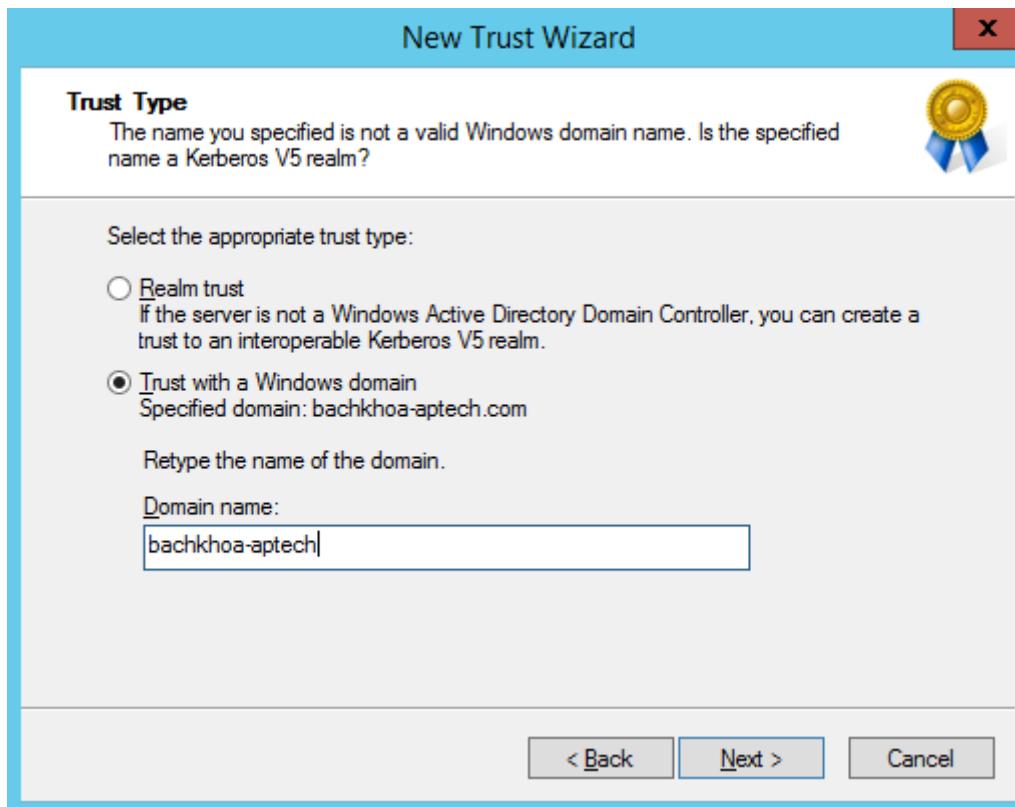
- Chuyển sang tab **Trust**, click chọn vào **New Trust...**



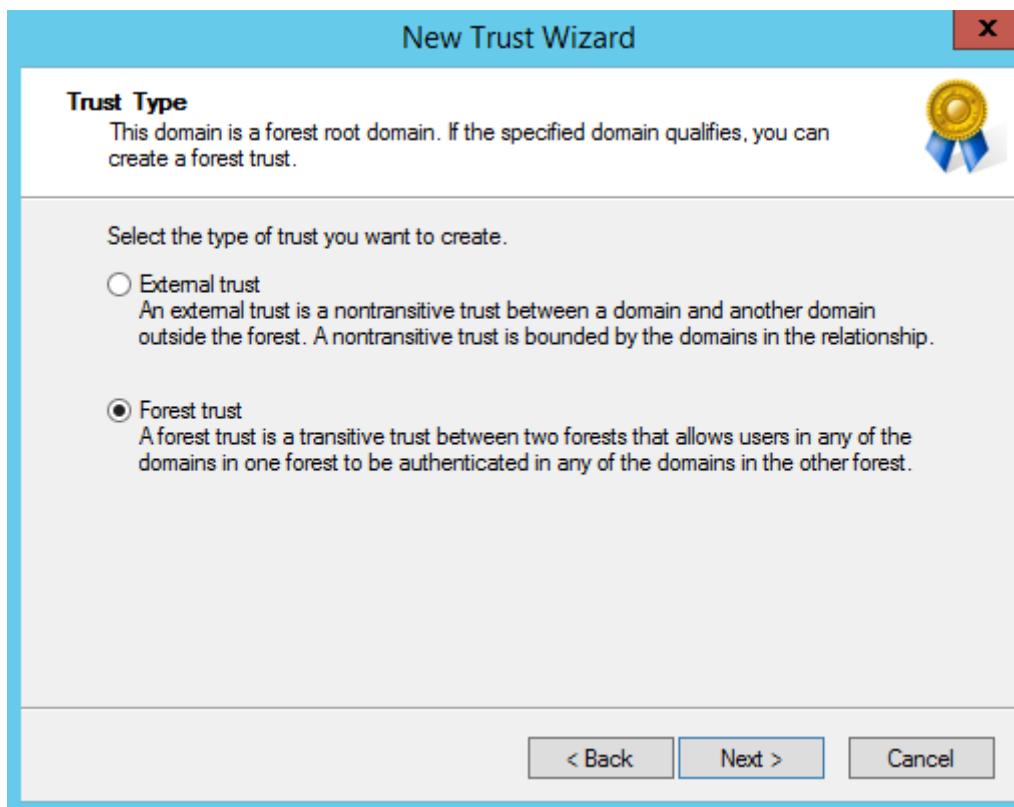
- Trong cửa sổ **Trust Name**, tại mục **name**, nhập vào tên **bachkhoa-aptech.com**.



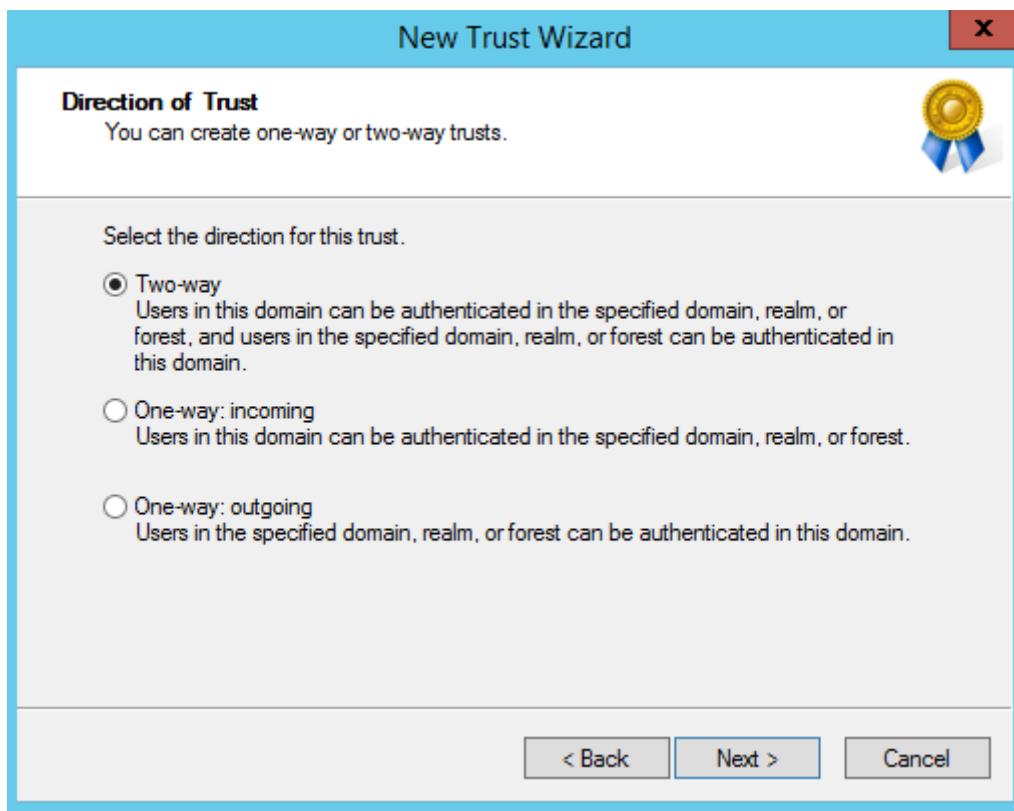
- Tại cửa sổ **Trust Type**, click chọn vào **Trust with a Windows domain**, kiểm tra tại mục **Domain name: bachkhoa-aptech** , **Next.**



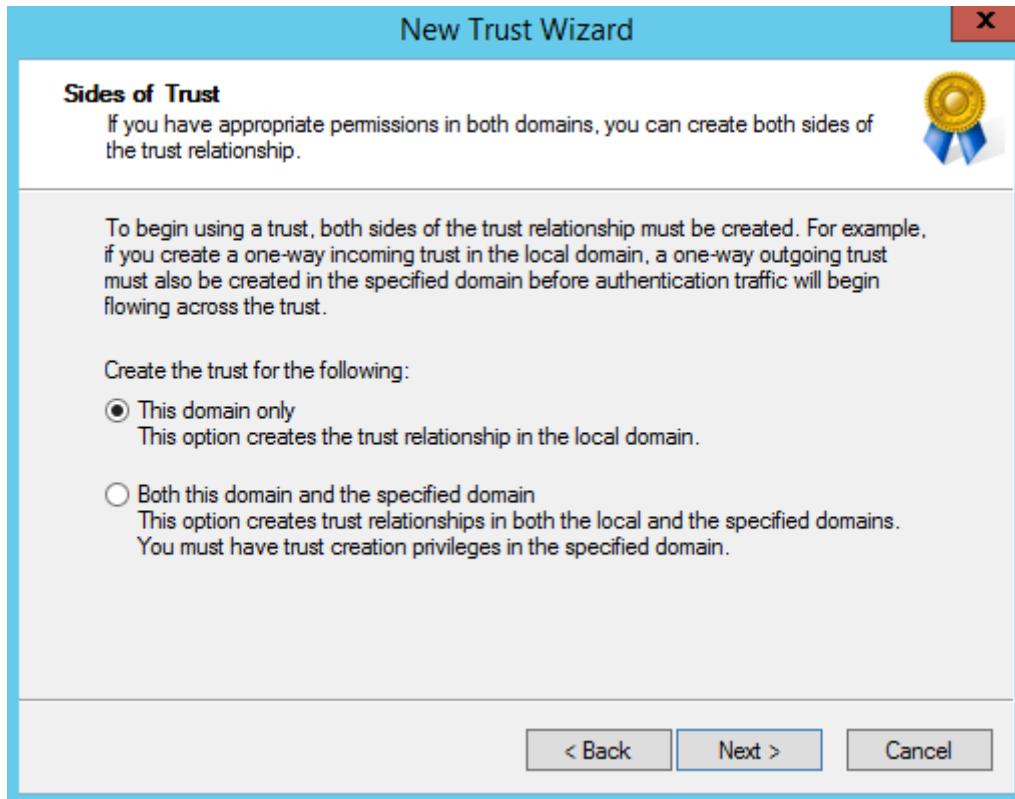
- Tại cửa sổ Trust Type, click chọn vào Forest Trust , Next.



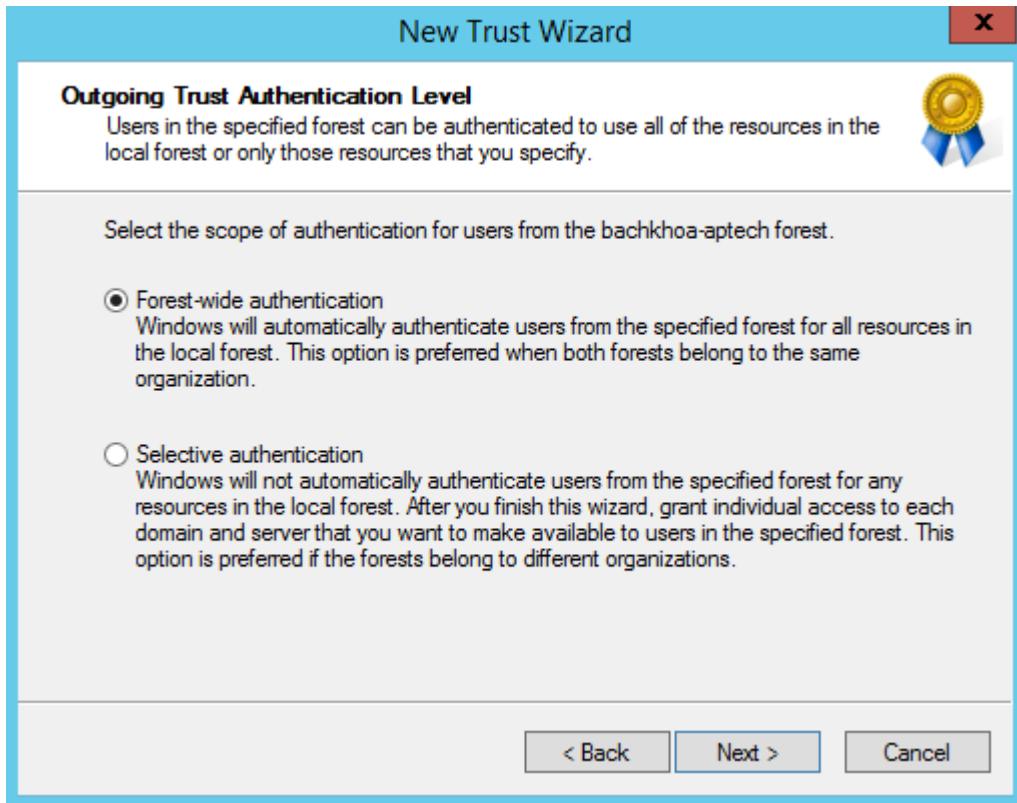
- Tại cửa sổ **Direction of Trust**, click chọn vào **Two-way , Next**.



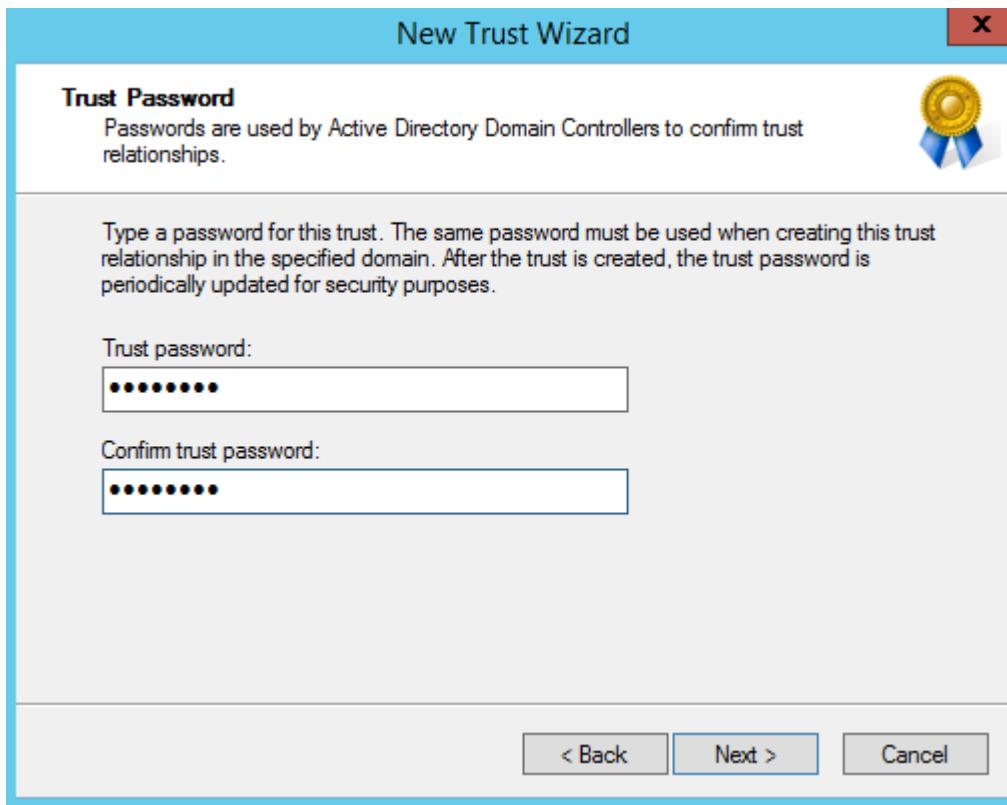
- Tại cửa sổ **Sides of Trust**, click vào **This domain only**, click vào **Next**.



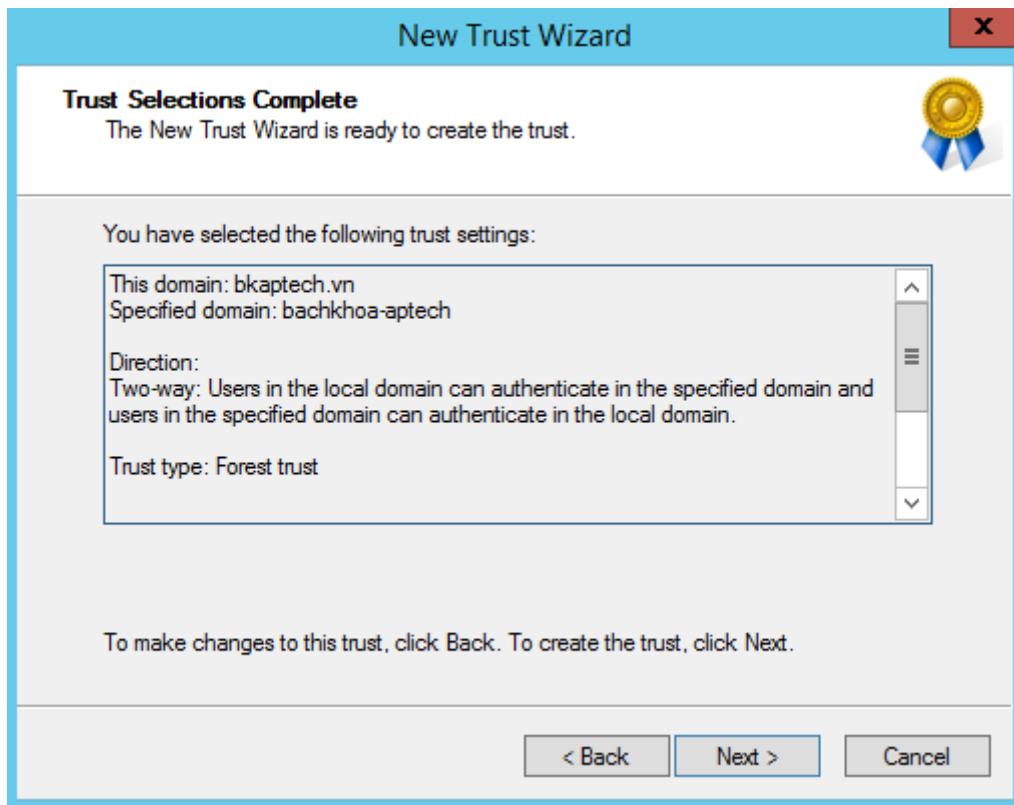
- Tại cửa sổ **Outgoing Trust Authentication Level**, click vào Forest-wide authentication, Next.



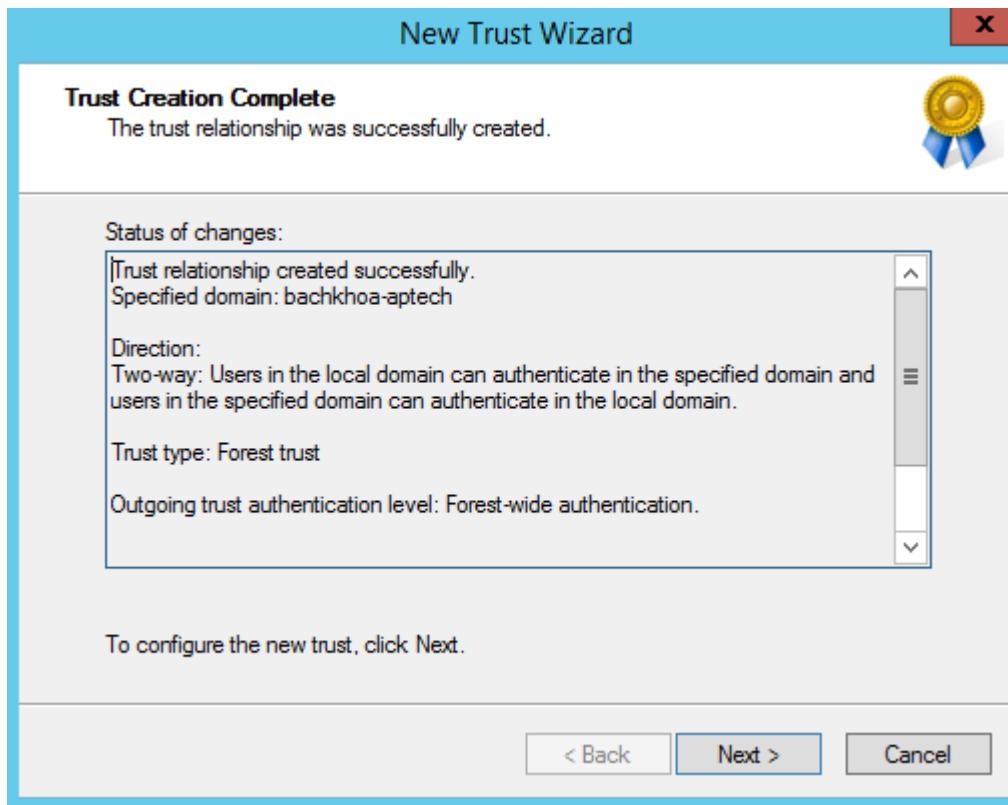
- Tại cửa sổ Trust Password, nhập vào Password.



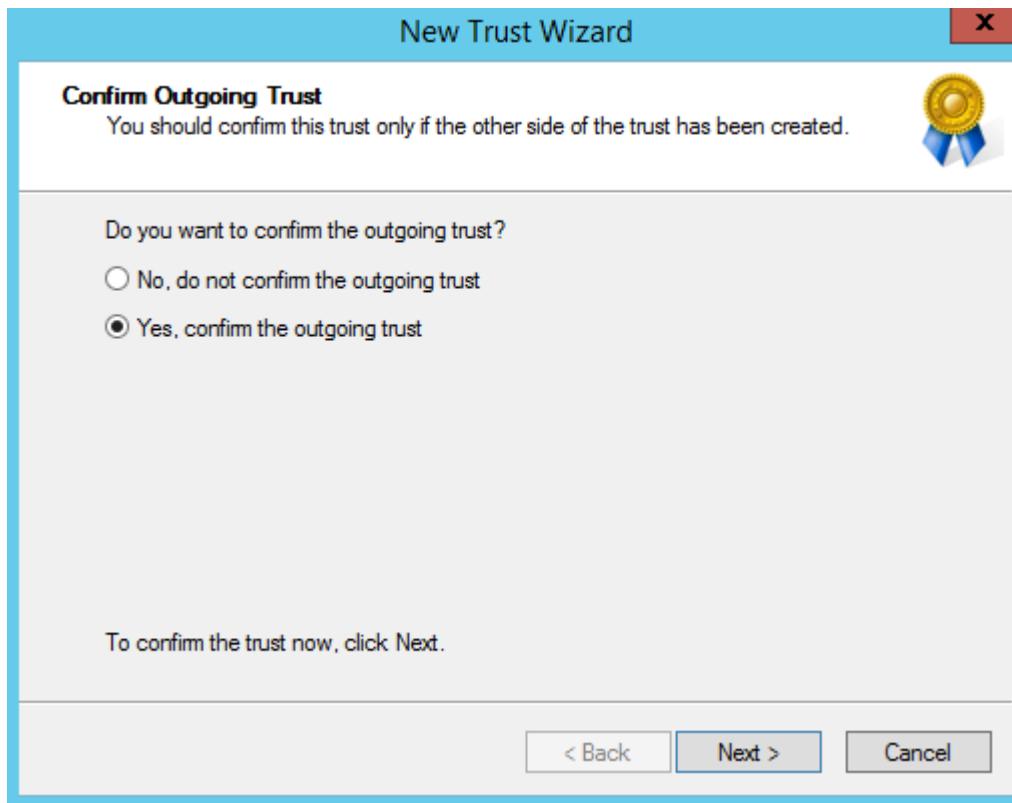
- Tại cửa sổ Trust Selections Complete, click vào Next.



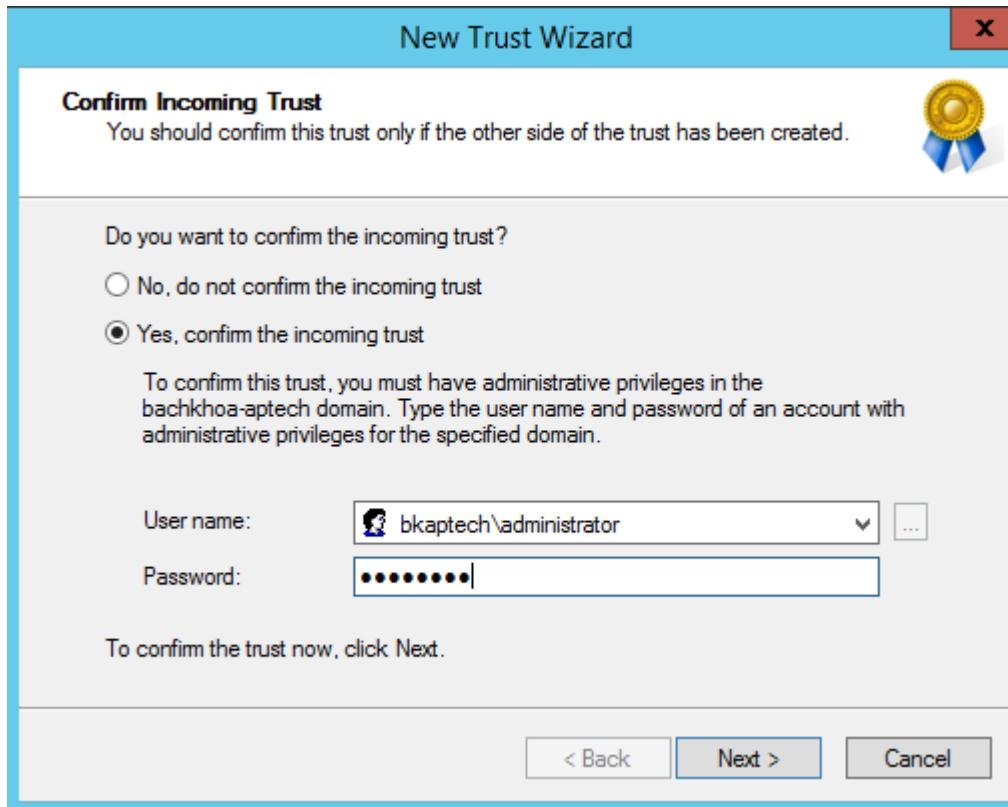
- Tại cửa sổ **Creation Complete**, click vào **Next**.



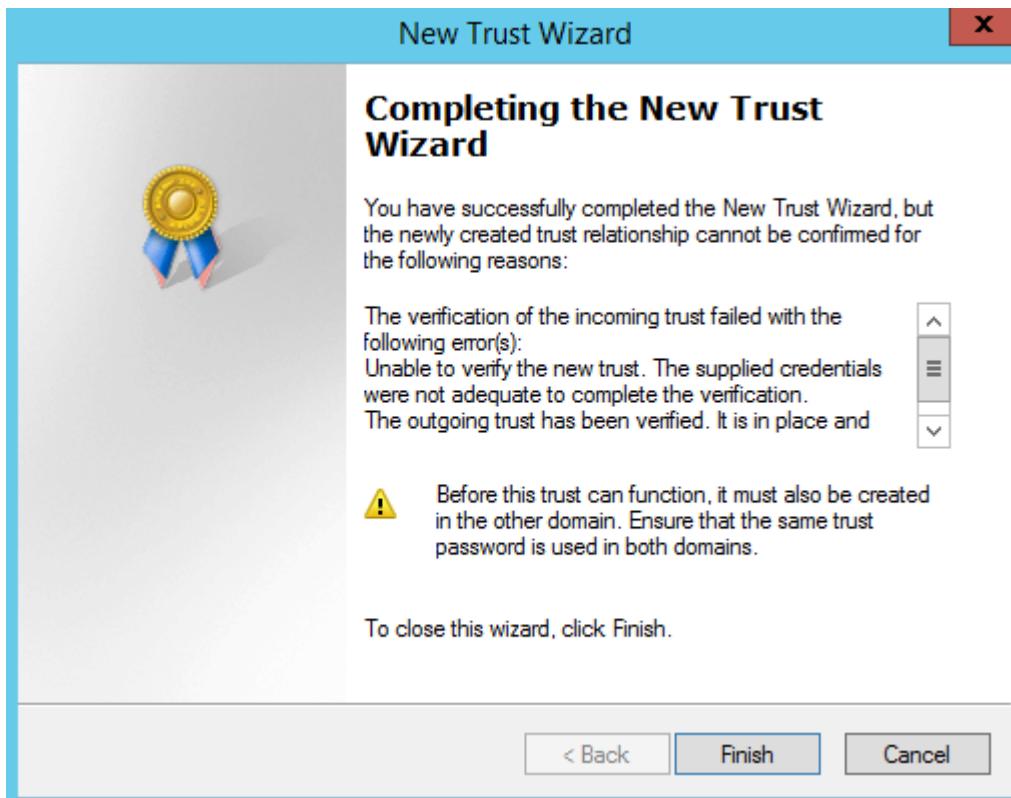
- Tại cửa sổ **Confirm Outgoing Trust**, click chọn vào **Yes, confirm the outgoing trust.**



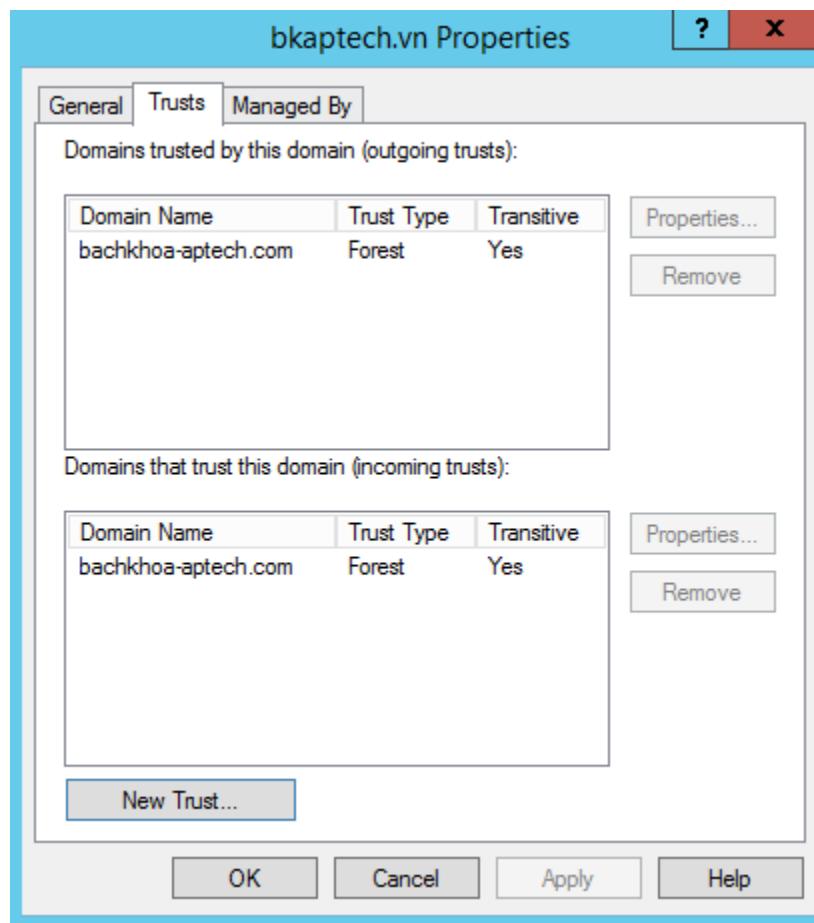
- Tại cửa sổ **Confirm Incoming Trust**, click chọn **Yes, confirm the incoming trust**, nhập vào user *bkaptech\administrator*.



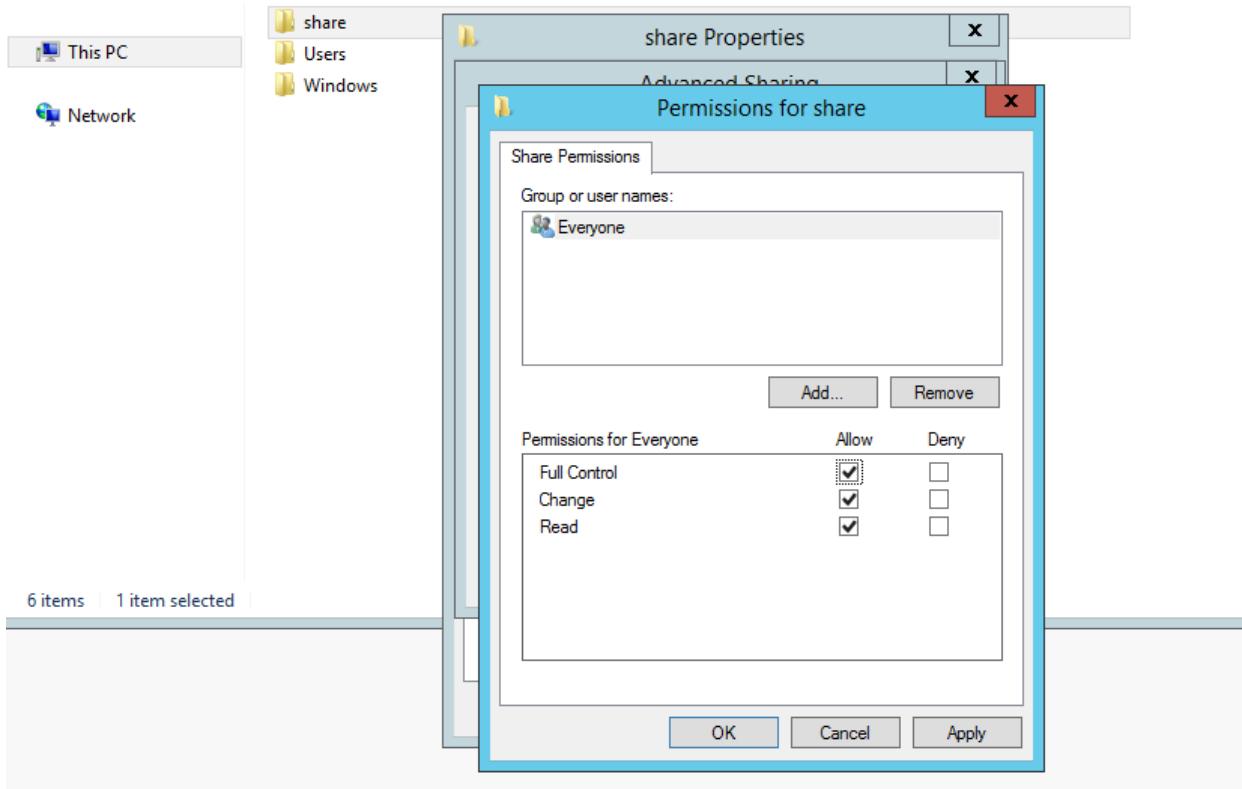
- Tại cửa sổ Completing.... Click vào Finish.



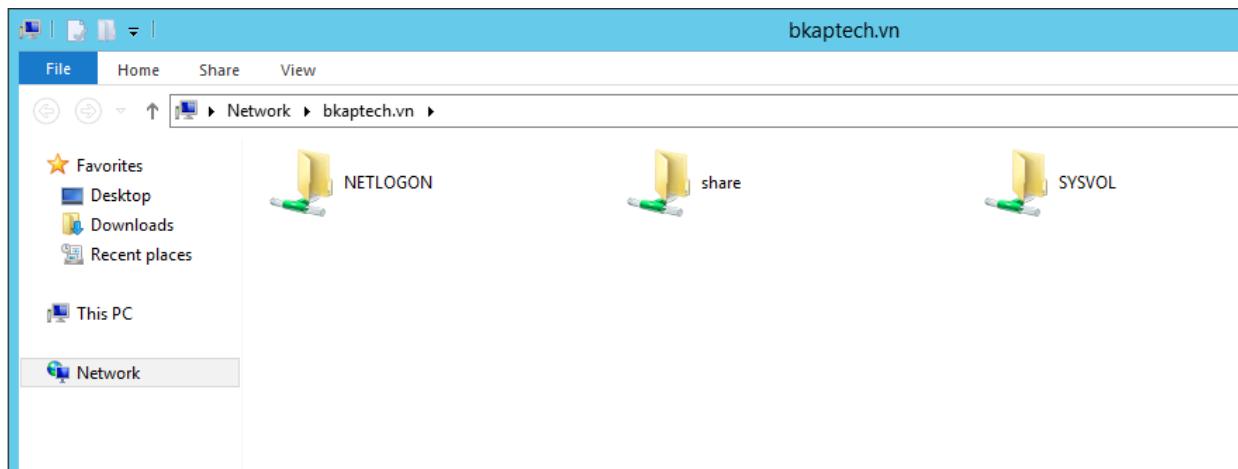
- Tại cửa sổ **bkaptech.vn Properties** ,click vào **OK**.



- Vào ổ C, tạo thư mục **share**, chia sẻ thư mục này cho **everyone** với quyền **Full Control**.



- Chuyển sang máy *BKAP-DC12-02*, truy cập thành công thư mục **share**.



4.3 Cấu hình Active Directory Domain Services Sites and Replication.

1.Yêu cầu bài Lab:

+ Cấu hình Active Directory Domain Services Sites và đồng bộ dữ liệu giữa các site và khắc phục sự cố khi hệ thống xảy ra lỗi.

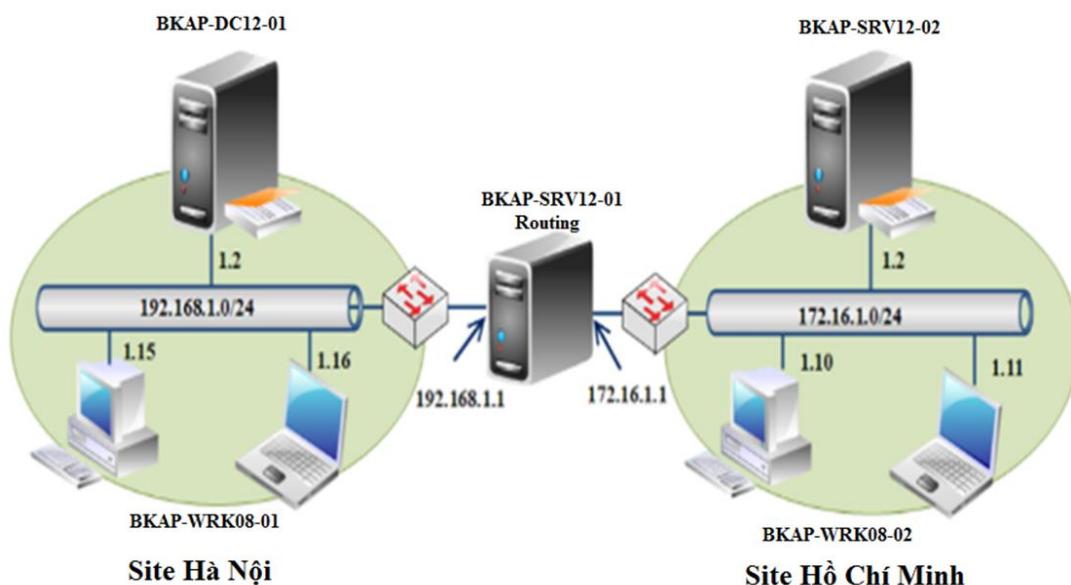
2.Yêu cầu chuẩn bị:

- + Máy Server **BKAP-DC12-01**: đã nâng cấp lên Domain Controller quản lý miền **bkaptech.vn**.
- + Máy Client **BKAP-WRK08-01** : Join vào miền **bkaptech.vn**.
- + Máy Server **BKAP-SRV12-02**: Member Domain.
- + Máy Server **BKAP-SRV12-01**: làm Routing.

3.Mô hình Lab:

HỆ THỐNG ĐÀO TẠO CNTT QUỐC TẾ BACHKHOA-APTECH

Cấu hình Active Directory Domain Services Sites and Replication

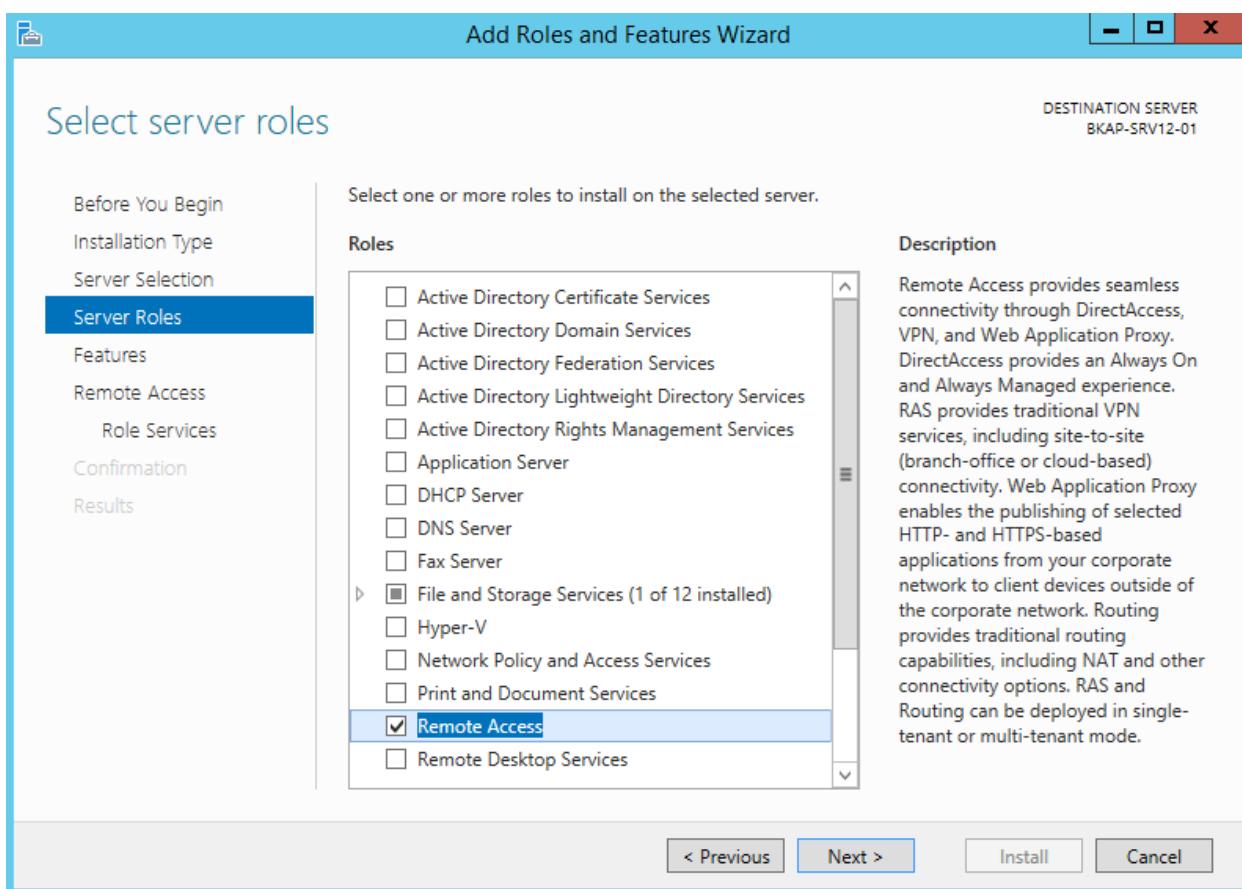


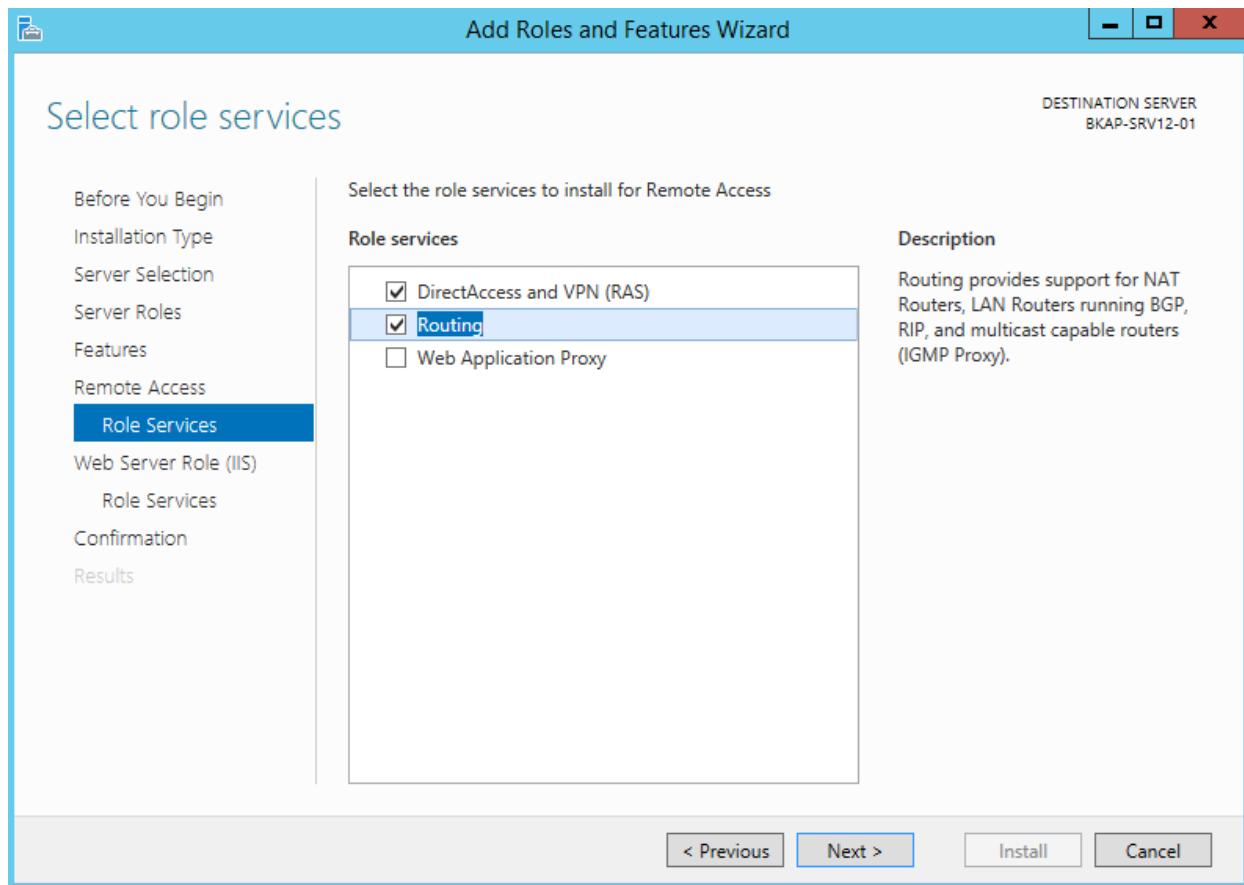
Sơ đồ địa chỉ sau:

Thông số	BKAP-DC12-01	BKAP-SRV12-01	BKAP-SRV12-02
<i>IP address</i>	192.168.1.2	NIC1: 192.168.1.1 NIC2: 172.16.1.1	172.16.1.2
<i>Subnet Mask</i>	255.255.255.0	255.255.255.0	255.255.255.0
<i>Default Gateway</i>	192.168.1.1	--	172.16.1.1
<i>DNS Server</i>	192.168.1.2	--	192.168.1.2

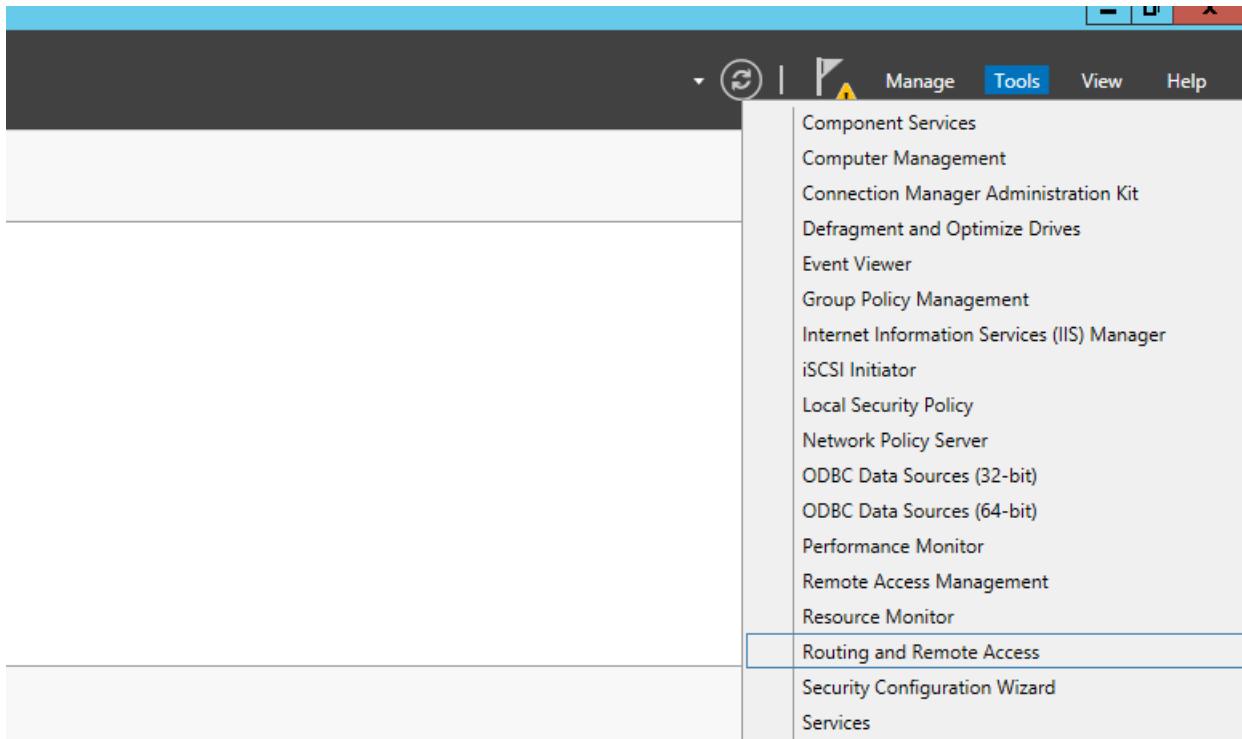
Hướng dẫn chi tiết:

- Mở các máy ảo, kết nối như mô hình trên, đặt địa chỉ IP cho các máy theo sơ đồ, thực hiện ping thông giữa các card mạng kết nối trực tiếp.
- Trên máy *BKAP-SRV12-01*, thực hiện cài đặt **Remote Access**.

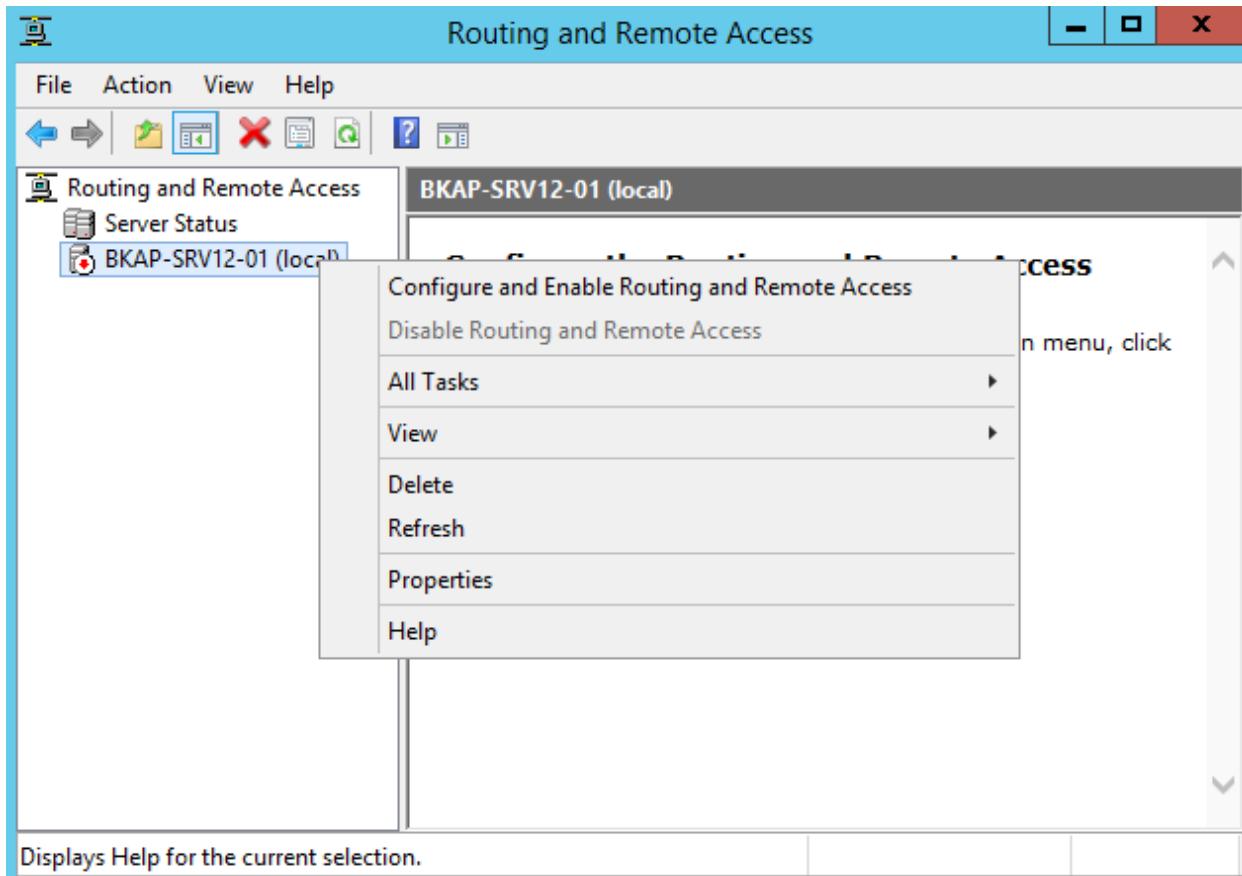




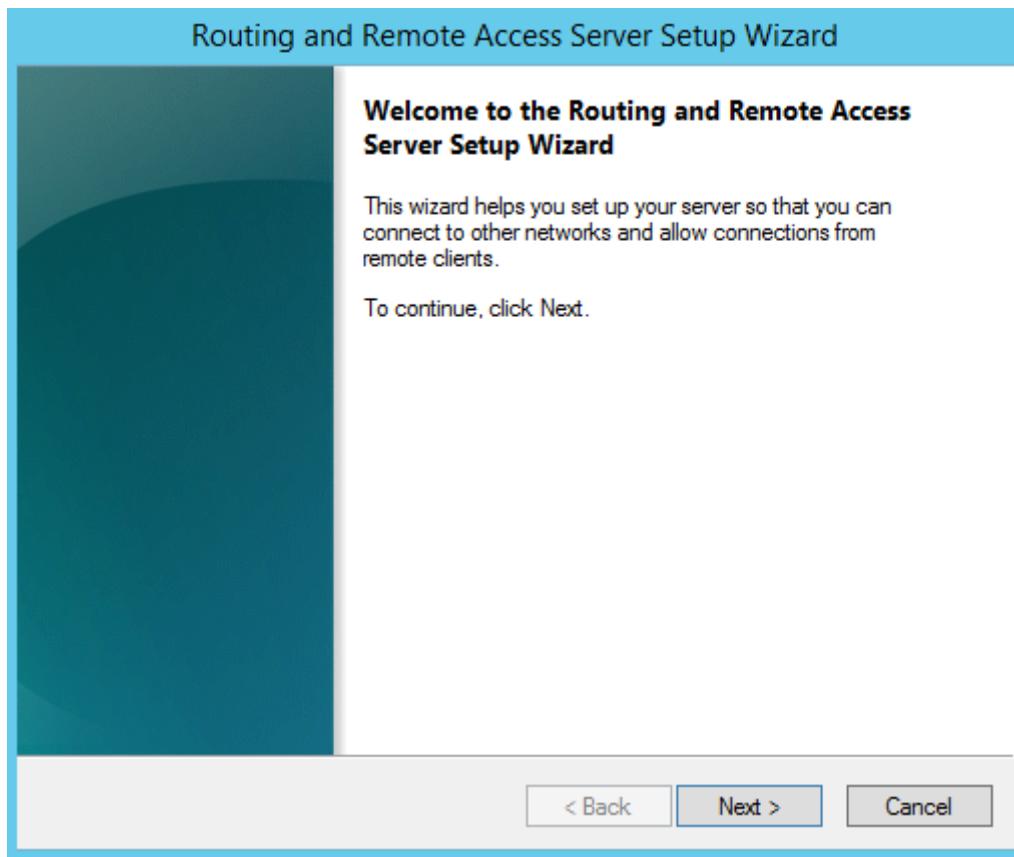
- Thực hiện cấu hình định tuyến giữa 2 mạng.
 - Trong cửa sổ **Server Manager**, click vào **Tools / Routing and Remote Access**.



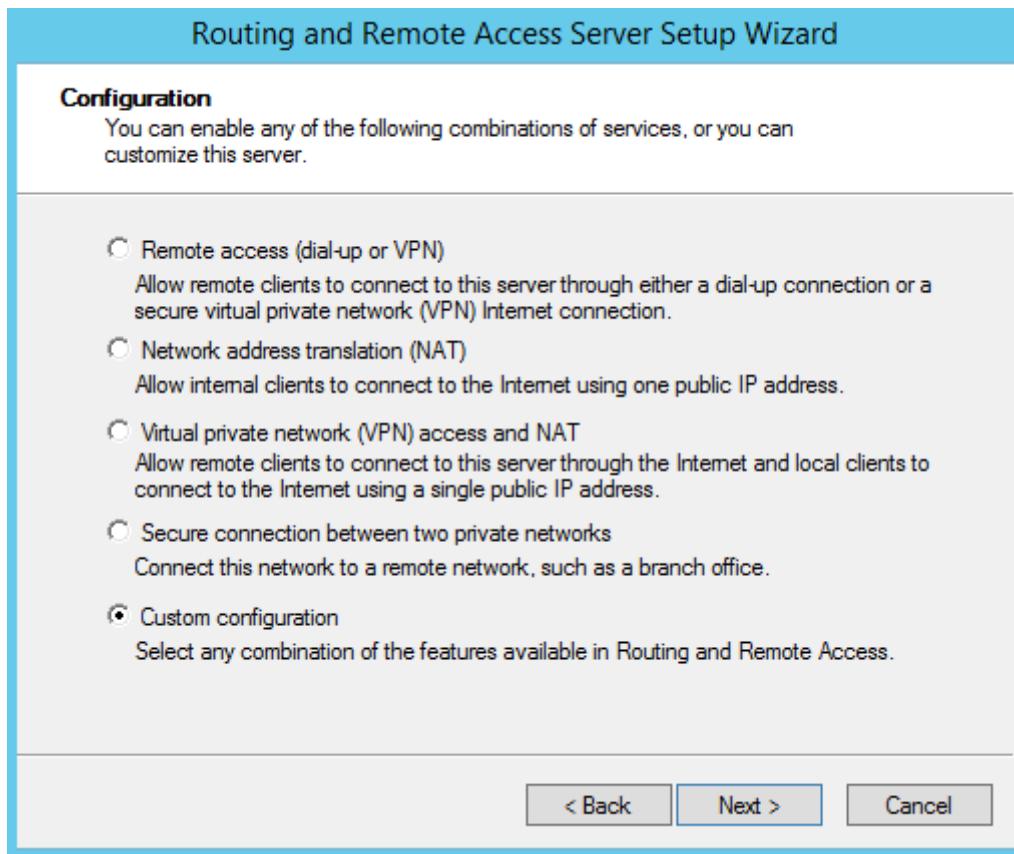
- Trong cửa sổ **Routing and Remote Access**, click chuột phải tại **BKAP-SRV12-01 (local)** , chọn vào **Configure and Enable Routing and Remote Access**.



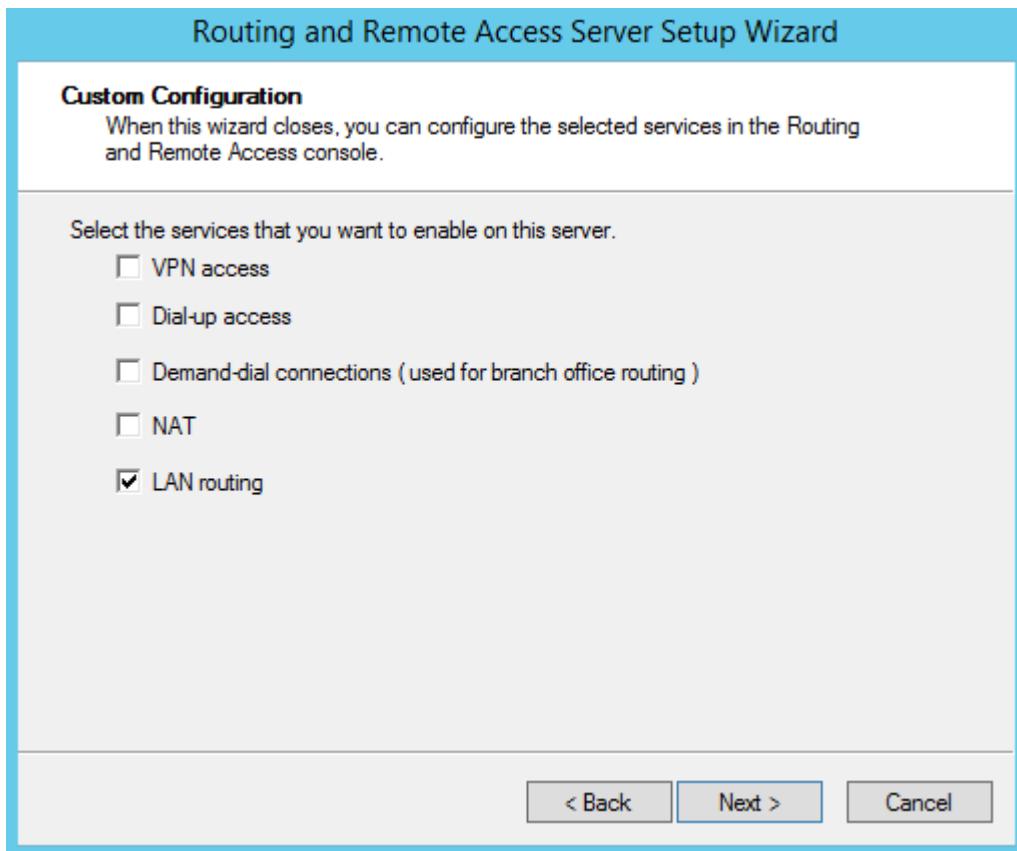
- Tại cửa sổ **Welcome to the Routing....**, click vào **Next**.



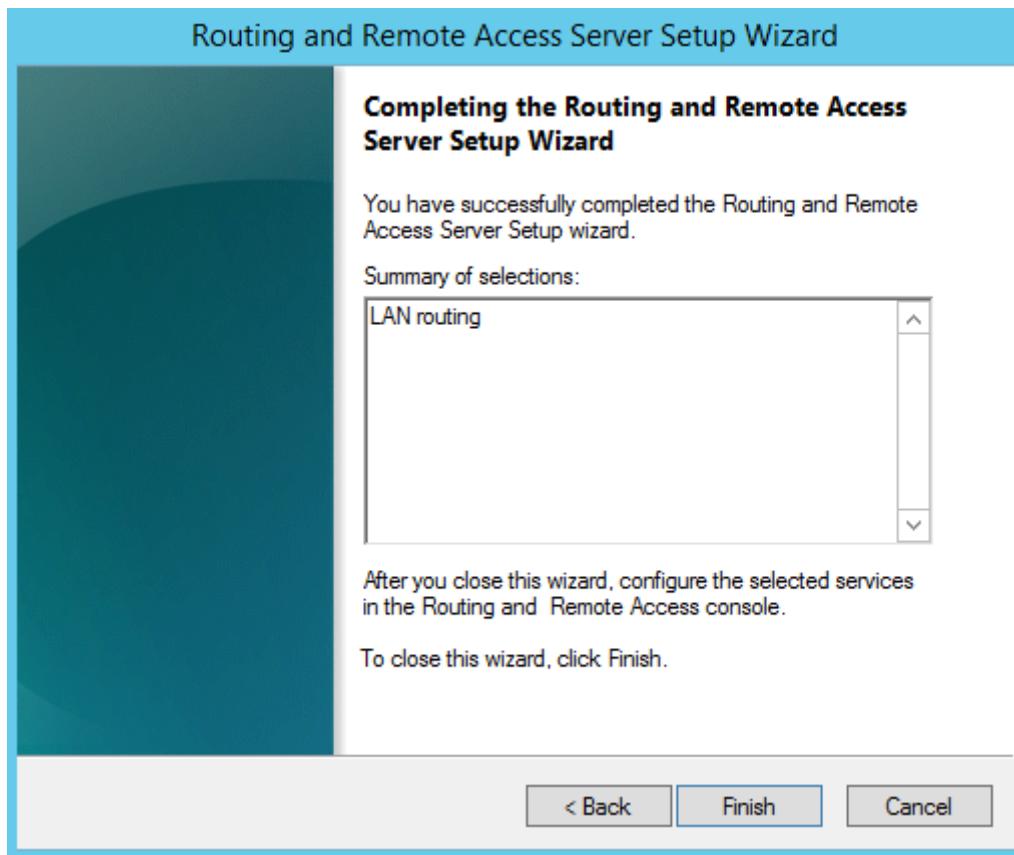
- Tại cửa sổ **Configuration**, click chọn vào **Custom configuration**.



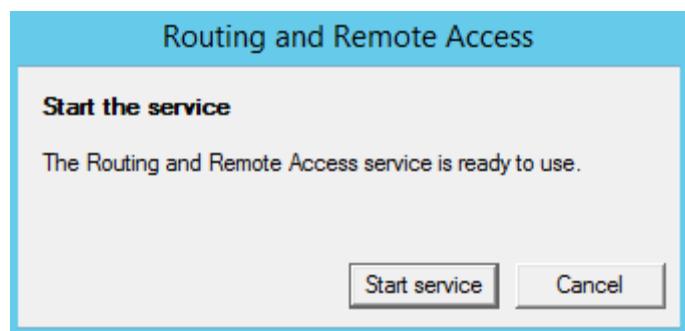
- Tại cửa sổ **Custom Configuration**, click chọn vào **LAN routing**.



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



- Click vào **Start services.**



- Chuyển sang máy *BKAP-SRV12-02*, kiểm tra kết nối từ máy *BKAP-SRV12-02* đến máy *BKAP-DC12-01*.

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

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 = 0ms, Average = 0ms

C:\Users\Administrator>
```

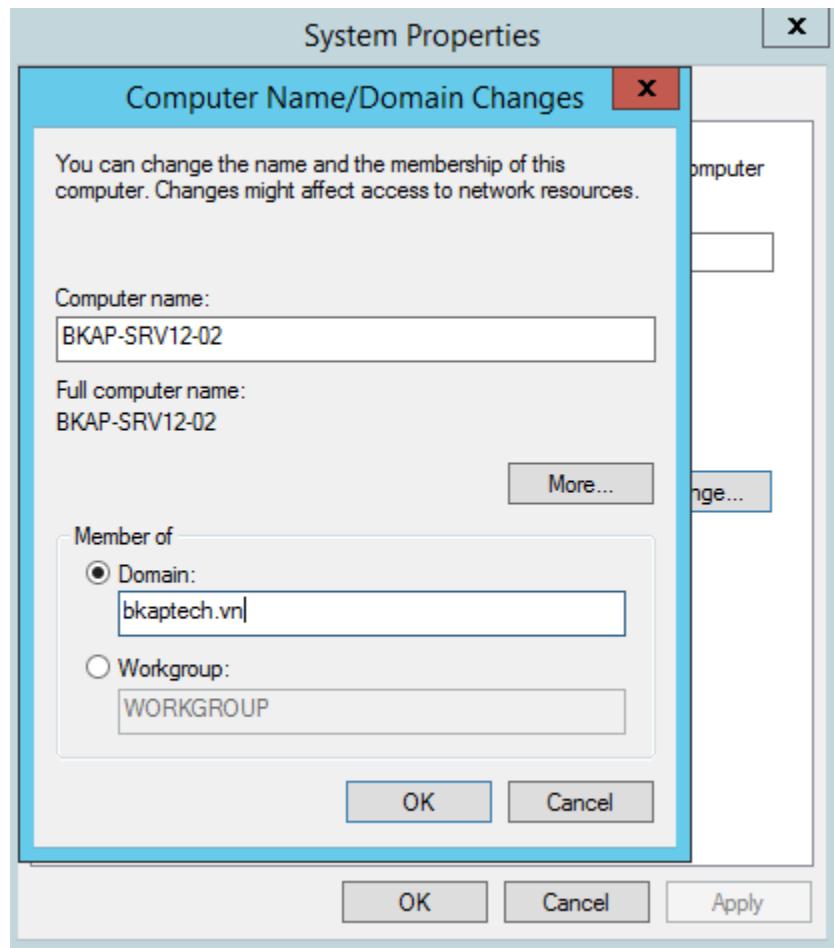
- Kiểm tra phân giải từ IP sang tên miền:

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

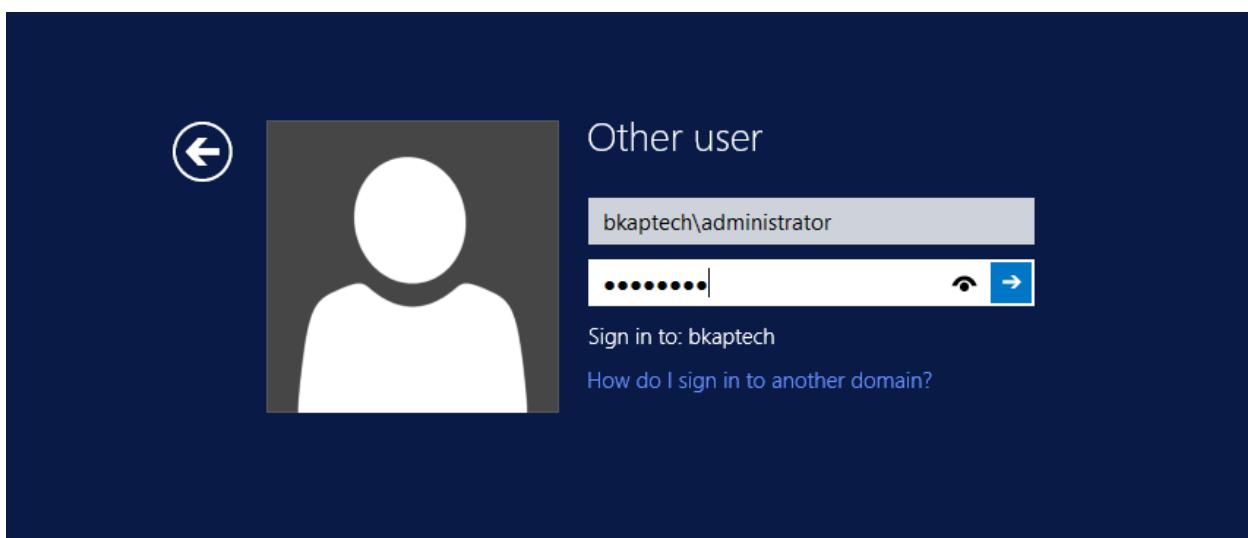
C:\Users\Administrator>nslookup
Default Server: bkap-dc12-01.bkaptech.vn
Address: 192.168.1.2

>
```

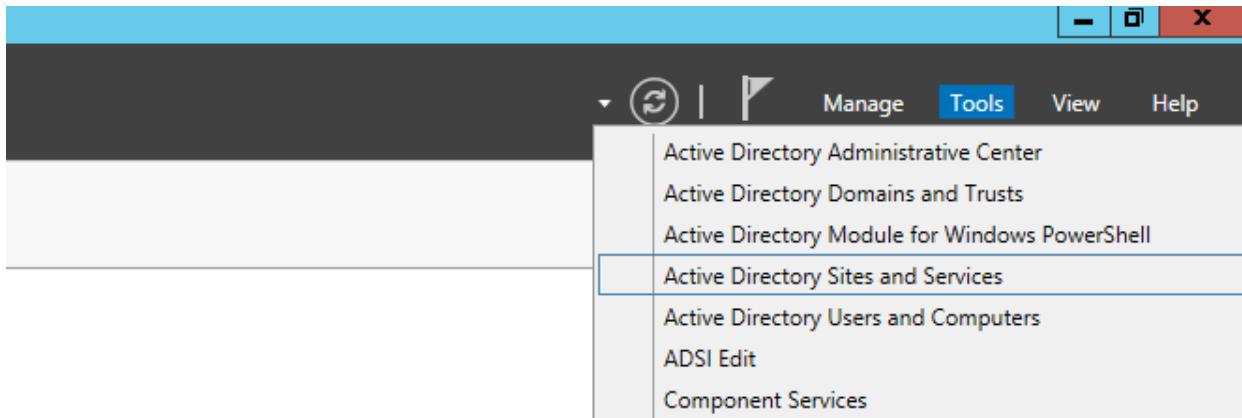
- Thực hiện Join vào domain:



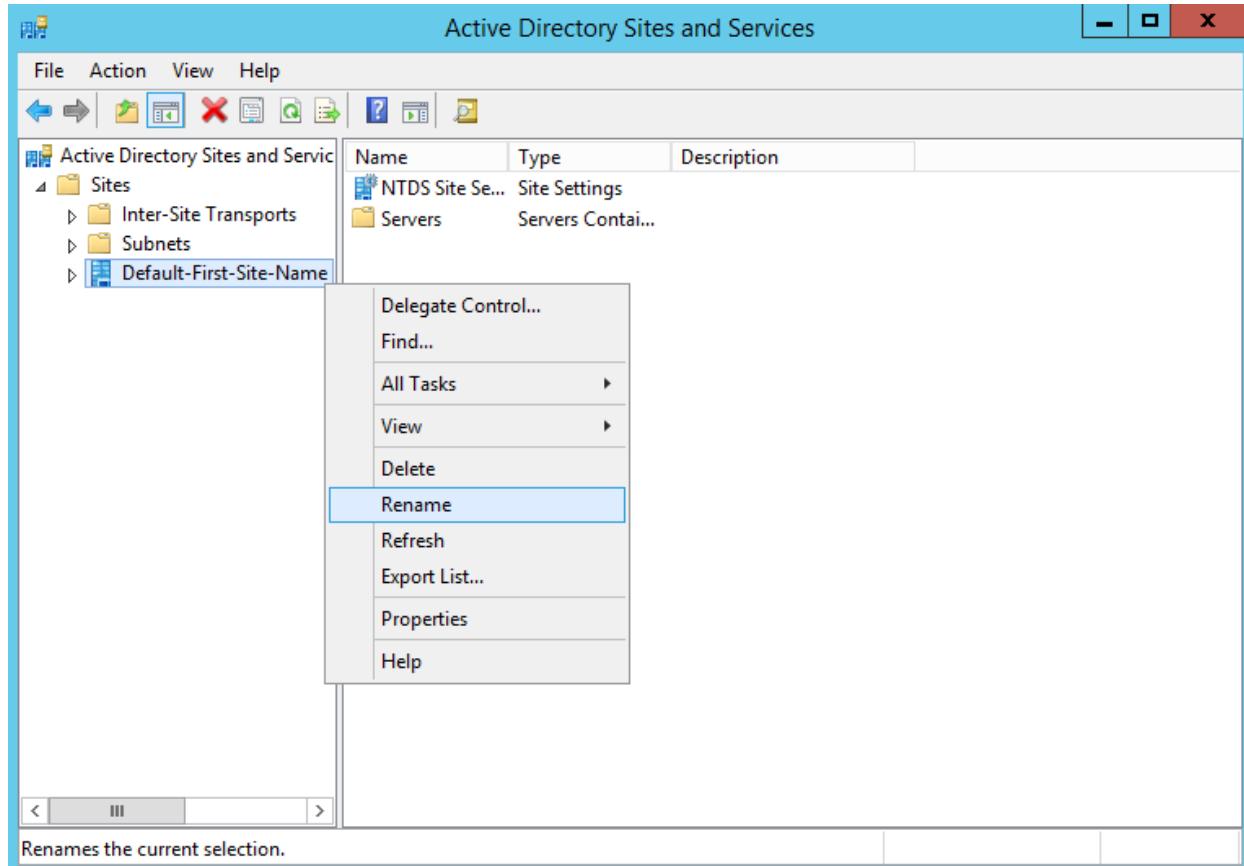
- Đăng nhập bằng user **bkaptech\administrator** .



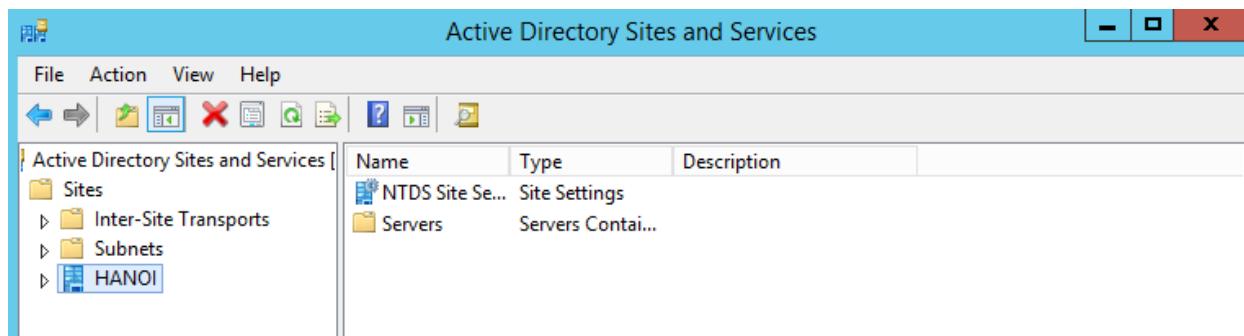
- Thực hiện nâng cấp máy *BKAP-SRV12-02* lên **Additional Domain Controller**. (xem lại bài **lab 2.3** trong sách **QUẢN TRỊ HỆ THỐNG MẠNG WINDOWS SERVER 2012 PHẦN 1**).
- Chuyển qua server *BKAP-DC12-01*, thực hiện đổi tên Site.
 - Trong **Server Manager**, click chọn vào **Tools / Active Directory Sites and Services**.



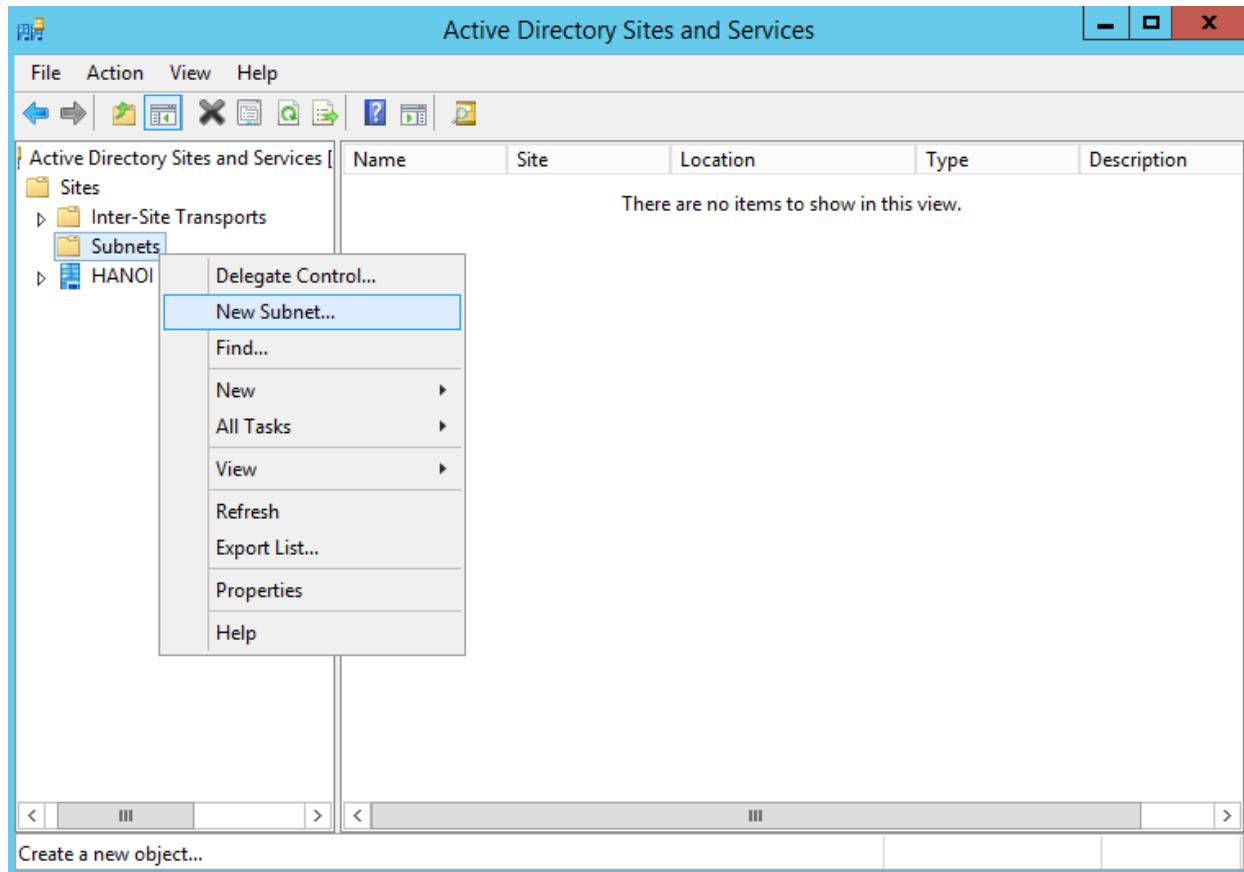
- Đổi tên site “Default-First-Site-Name” thành HANOI.
 - Trong cửa sổ Active Directory Sites and Services, click chuột phải tại Default-First-Site-Name, chọn Rename.



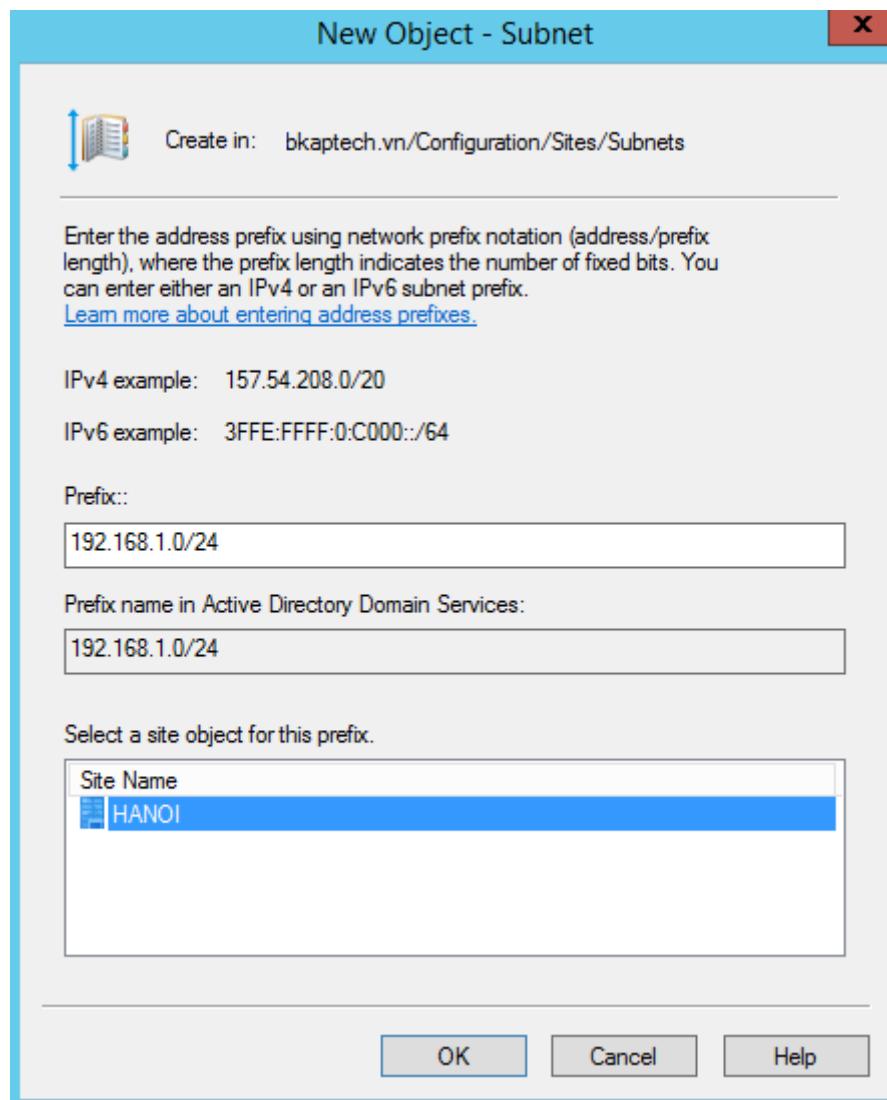
- Thực hiện đổi tên thành HANOI.



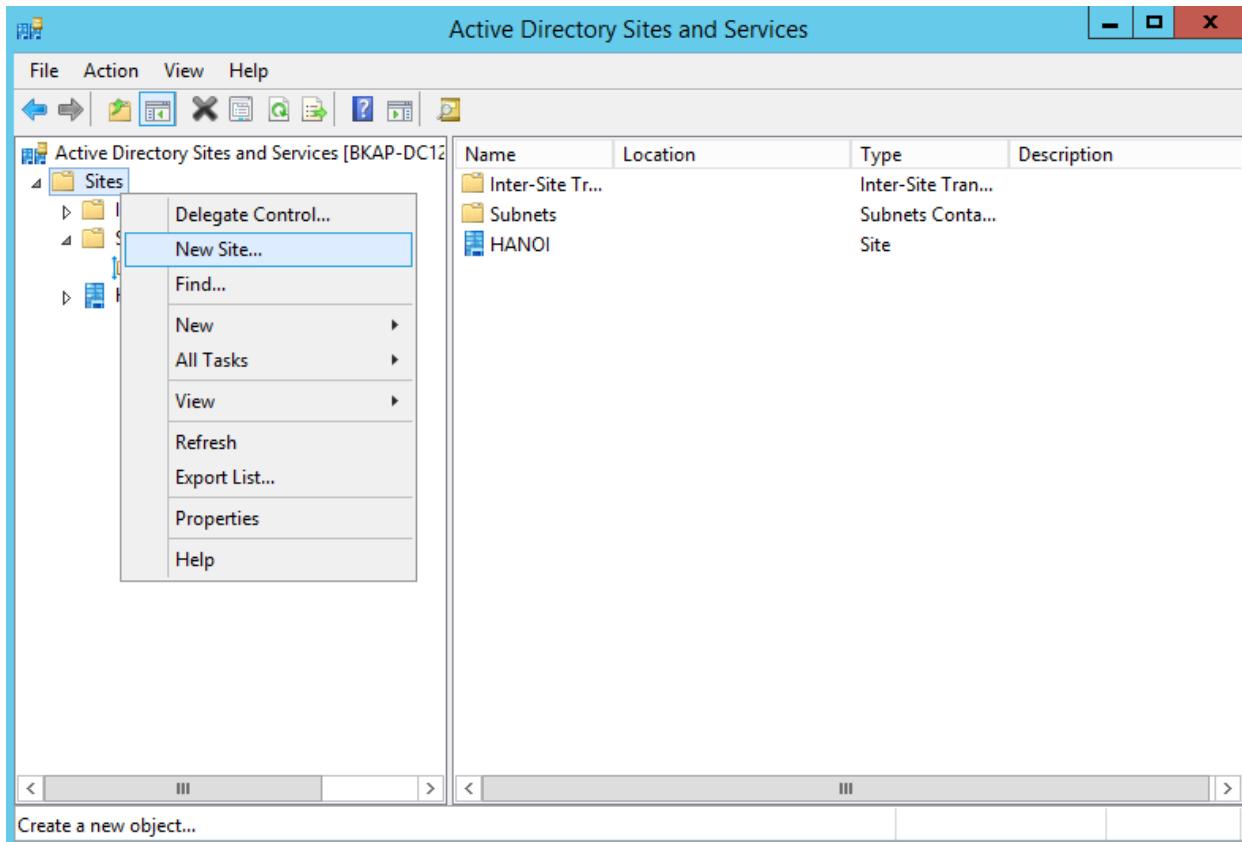
- Cấu hình IP subnets cho site **HANOI**.
 - Trong cửa sổ **Active Directory Sites and Services**, click chuột phải tại **Subnets** , chọn vào **New Subnet...**



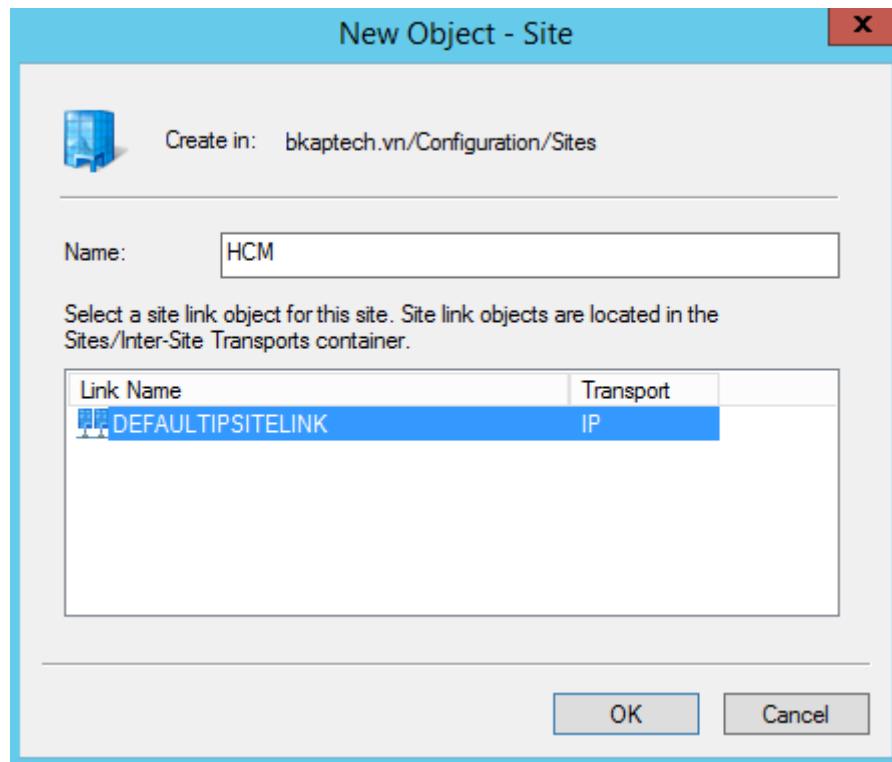
- Tại cửa sổ **New Object – Subnet**, tại mục **Prefix**, nhập vào dải địa chỉ **192.168.1.0/24**, chọn vào Site Name **HANOI**, click vào **OK**.



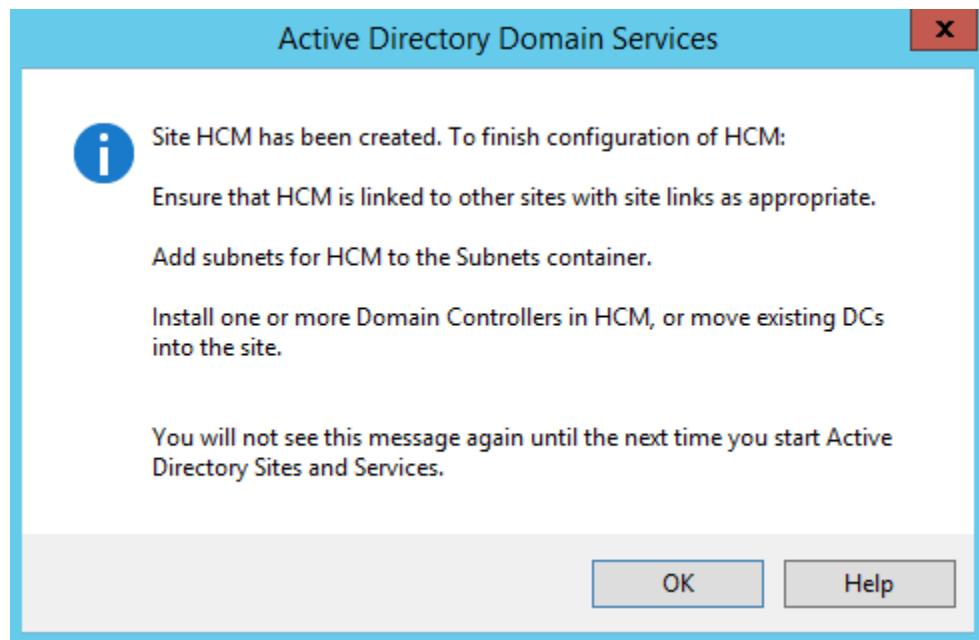
- Tạo Additional Sites and Subnets.
 - Click chuột phải vào **Sites**, chọn **New Site...**



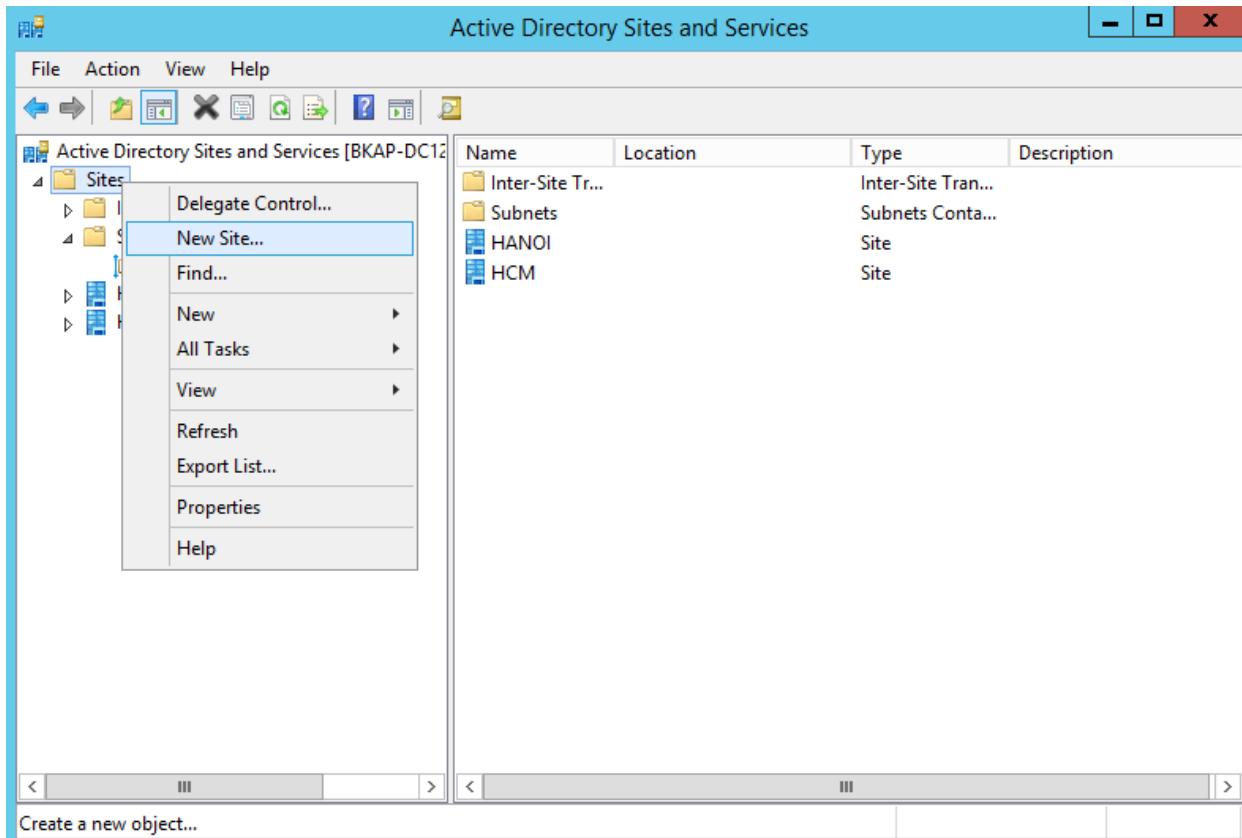
- Trong cửa sổ **New Object – Site**, nhập vào tên tại mục **Name: HCM**, click chọn vào **Link Name: DEFAULTSITELINK**, click vào **OK**.



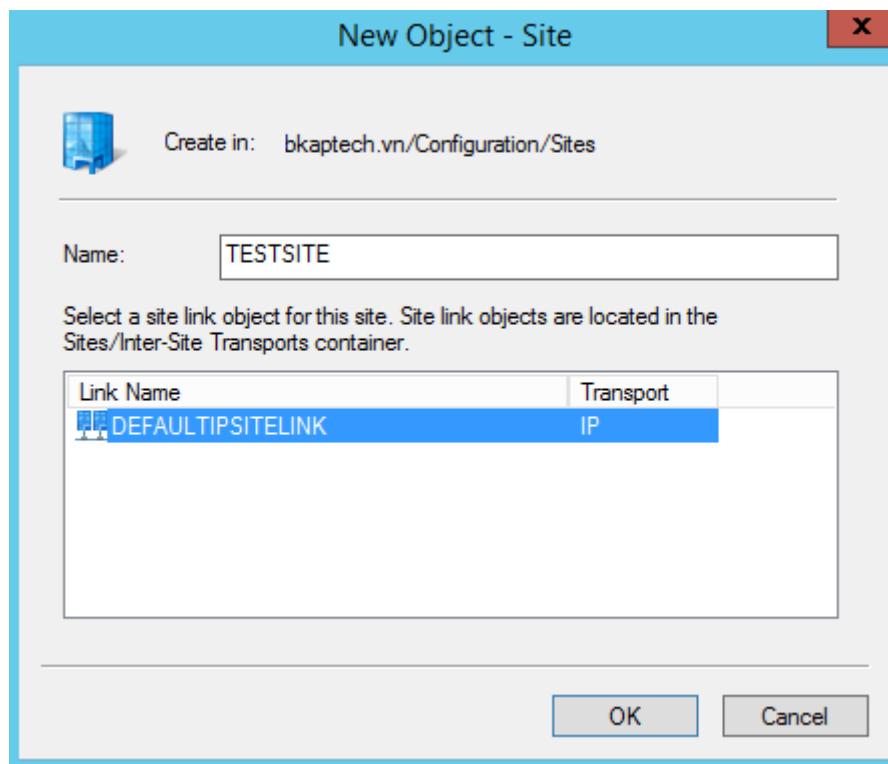
- Tại cửa sổ **ADDS**, click vào **OK**.



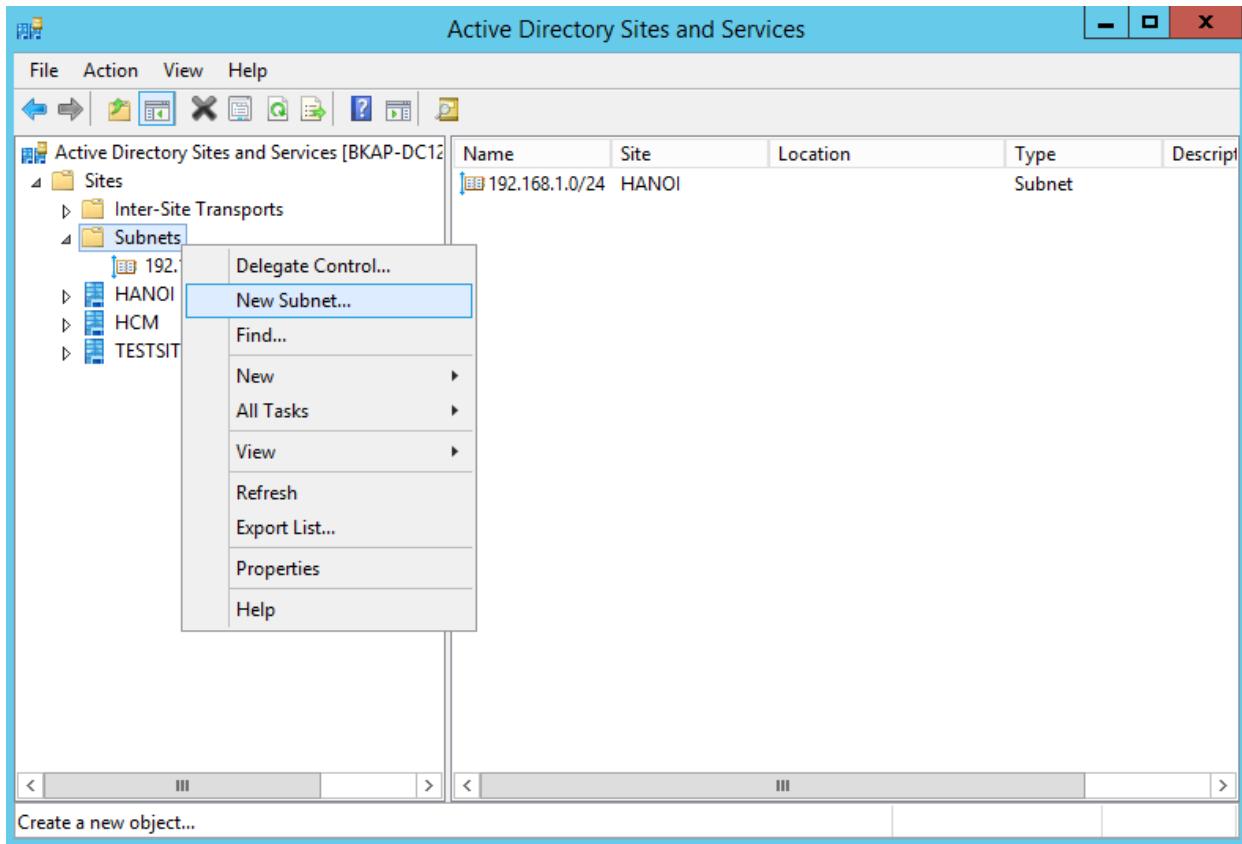
- Click chuột phải vào **Sites**, chọn **New Site...**



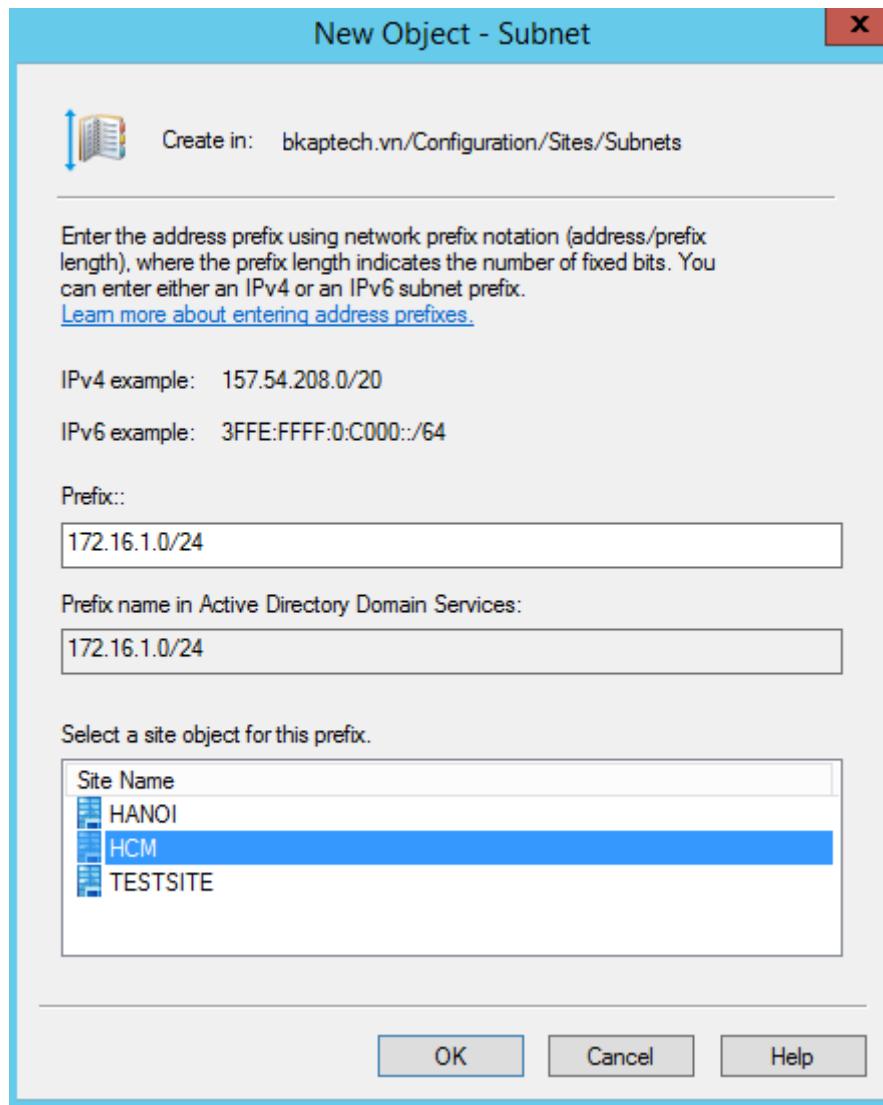
- Trong cửa sổ **New Object – Site**, nhập vào tên tại mục **Name: TESTSITE** , click chọn vào **DEFAULTSITELINK**, click vào **OK**.



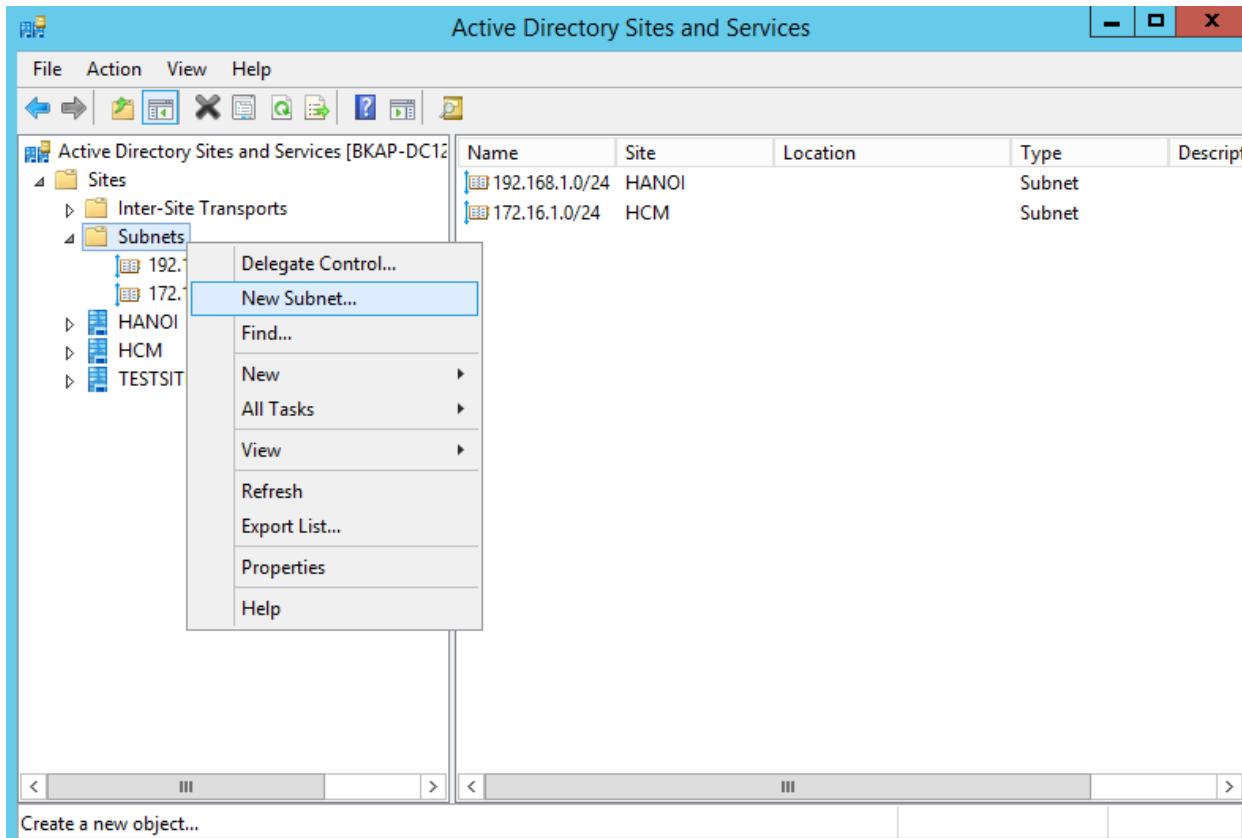
- Thực hiện tạo IP subnets liên kết với site **HCM**.
 - Click chuột phải tại **Subnets**, chọn **New Subnet...**



- Trong cửa sổ **New Object – Subnet**, tại mục **Prefix**, nhập vào dải địa chỉ **172.16.1.0/24**, chọn vào Site **HCM**, click vào **OK**.



o Tạo Subnets mới:



New Object - Subnet X

Create in: bkaptech.vn/Configuration/Sites/Subnets

Enter the address prefix using network prefix notation (address/prefix length), where the prefix length indicates the number of fixed bits. You can enter either an IPv4 or an IPv6 subnet prefix.
[Learn more about entering address prefixes.](#)

IPv4 example: 157.54.208.0/20

IPv6 example: 3FFE:FFFF:0:C000::/64

Prefix:::

131.107.1.0/24

Prefix name in Active Directory Domain Services:

131.107.1.0/24

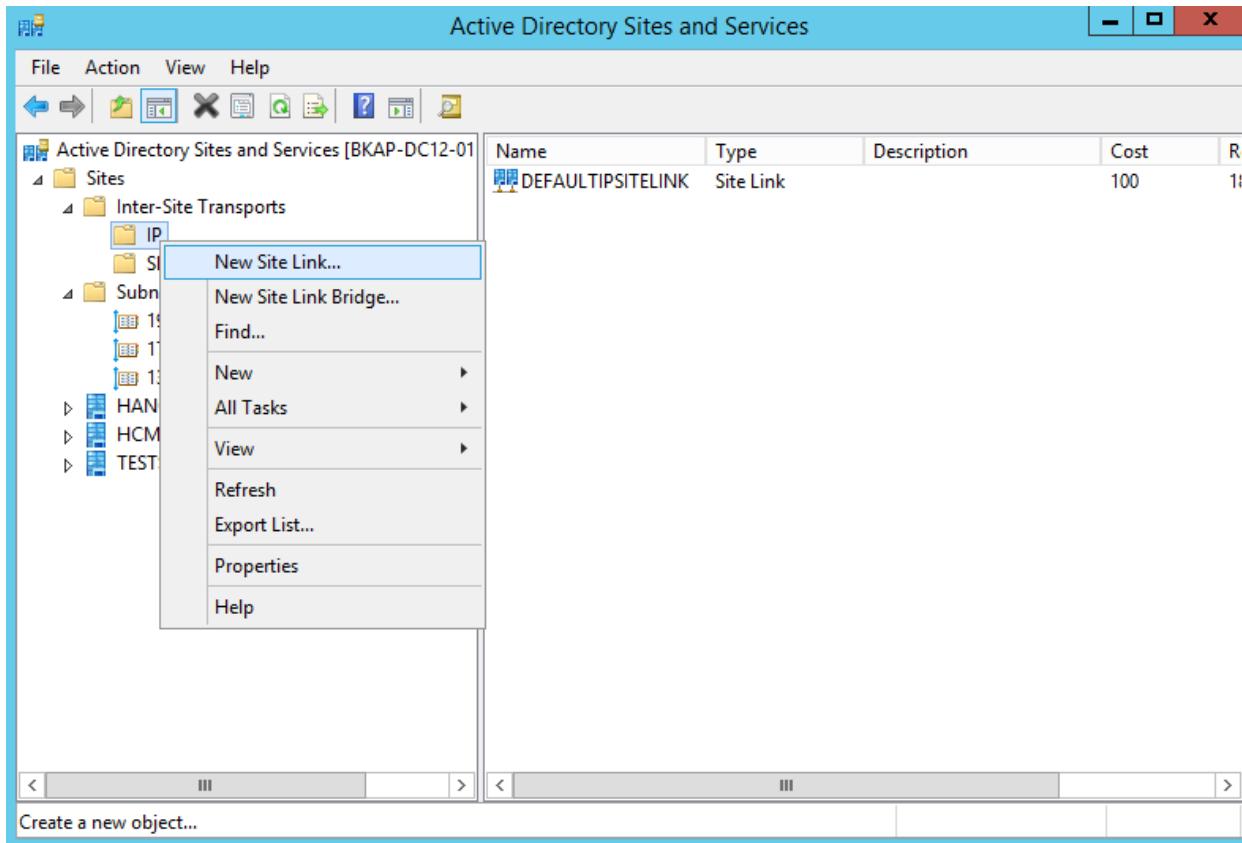
Select a site object for this prefix.

Site Name

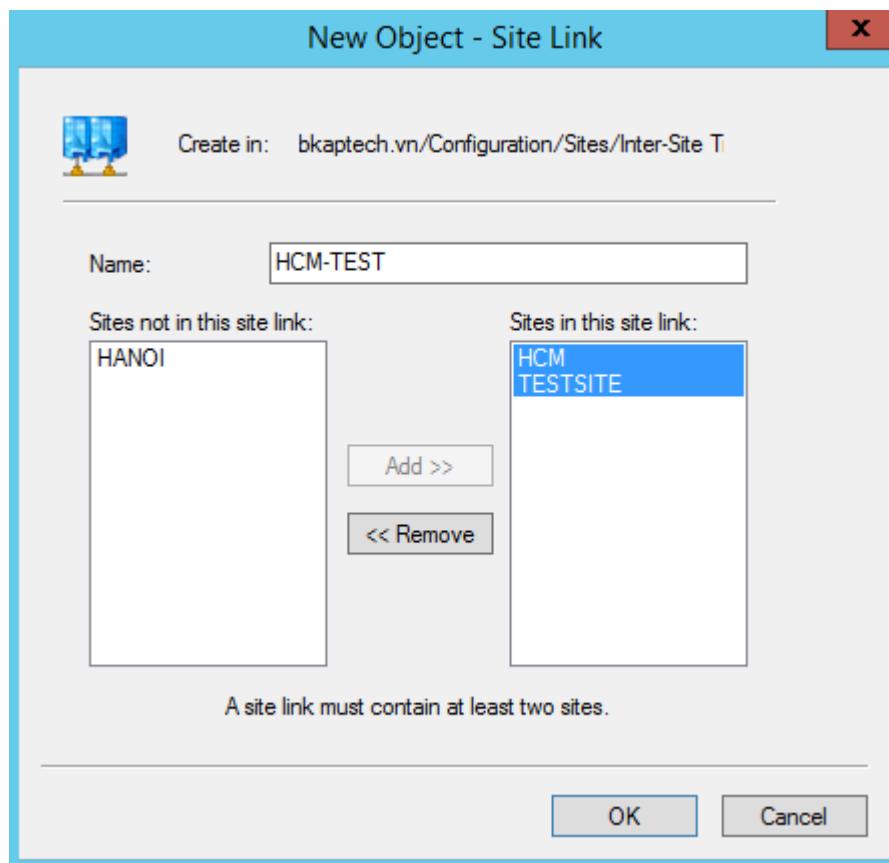
HANOI
HCM
TESTSITE

OK Cancel Help

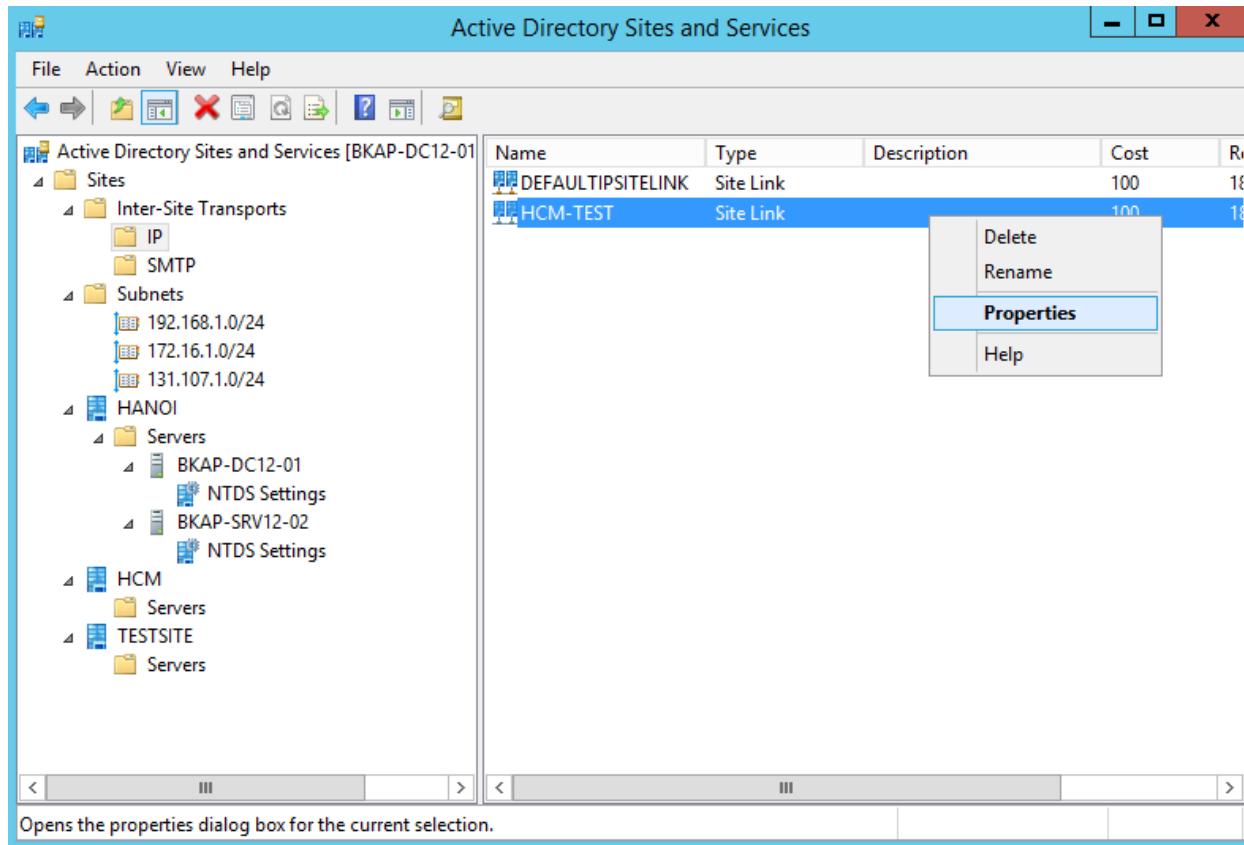
- Cấu hình ADDS Replication.
 - Thực hiện cấu hình Site links between AD DS sites.
 - Trong cửa sổ Active Directory Sites and Services, chọn vào **Sites / Inter-Site Transports / IP**.
 - Click chuột phải tại IP, chọn **New Site Link...**



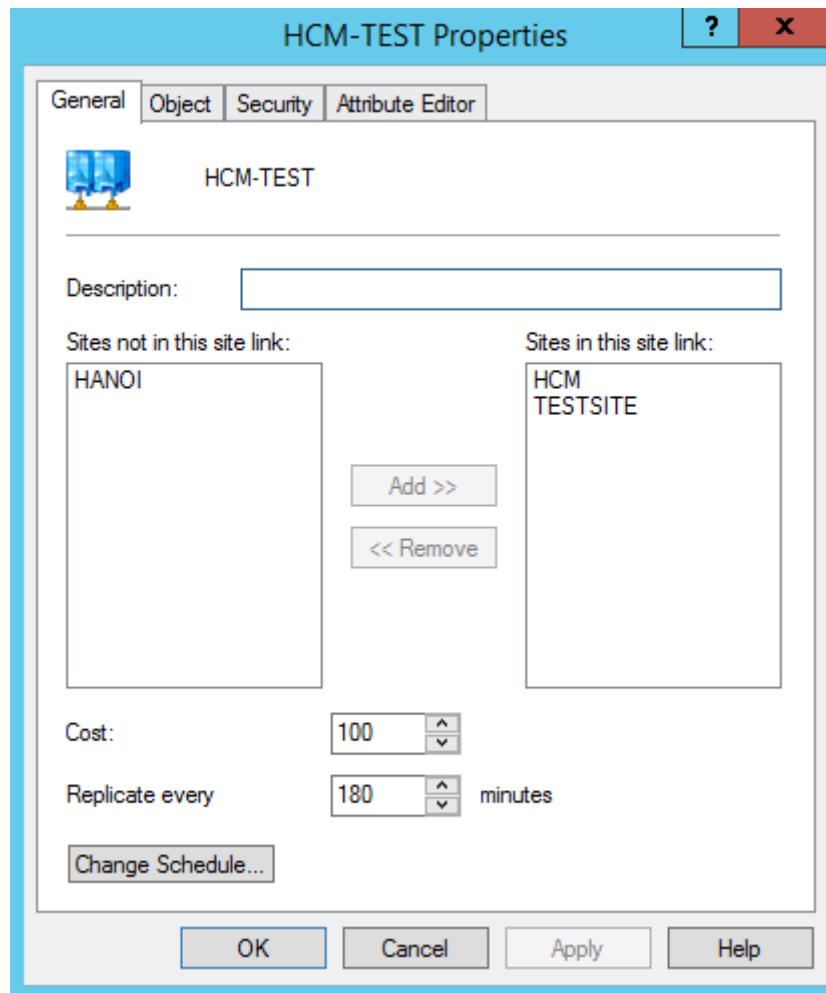
- Tại cửa sổ **New Object – Site Link**, nhập vào tên tại mục **Name: HCM-TEST**, tại khung **Sites not in this site link**, click chọn vào **HCM** và **TESTSITE**, click vào **Add >>**, click **OK**.



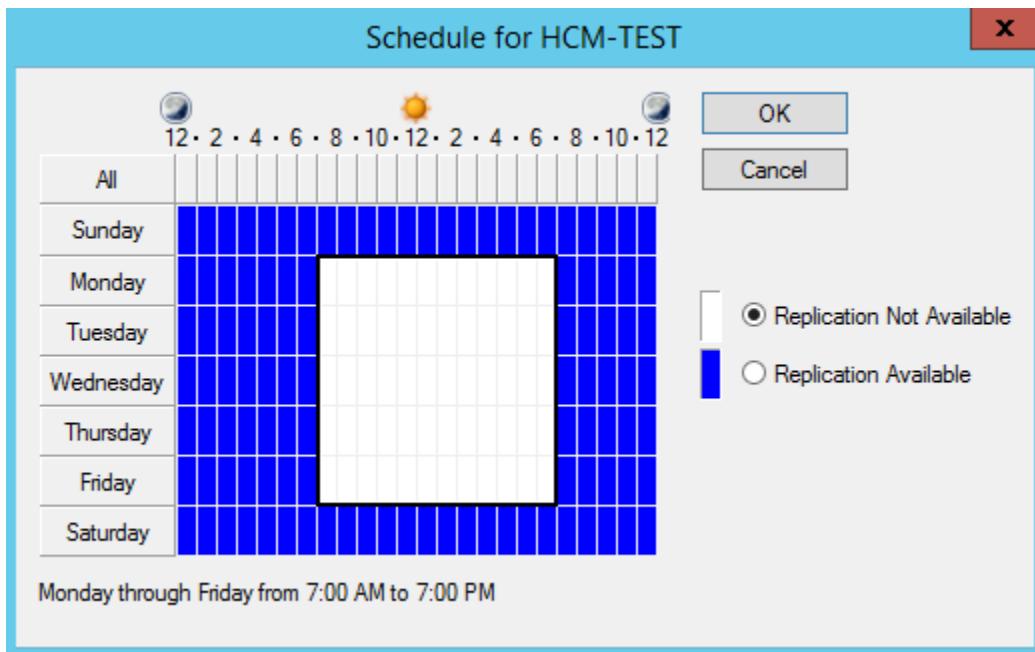
- Click chuột phải tại HCM-TEST, chọn Properties.



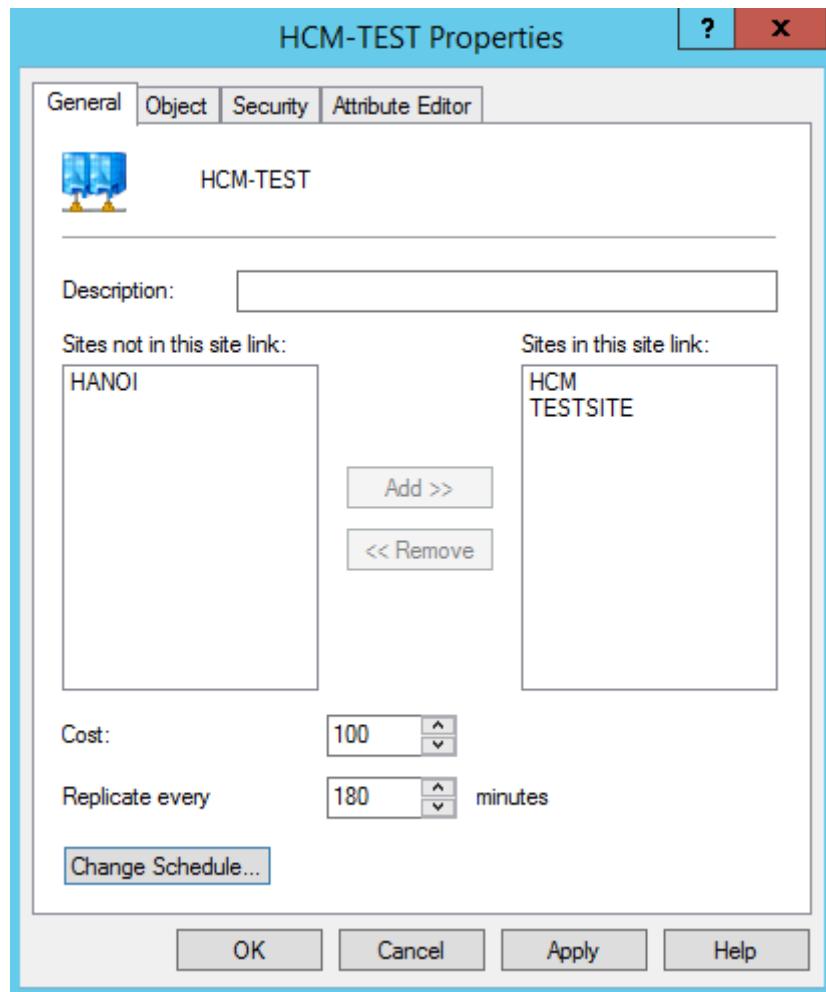
- Trong cửa sổ **HCM-TEST Properties**, click vào **Change Schedule...**



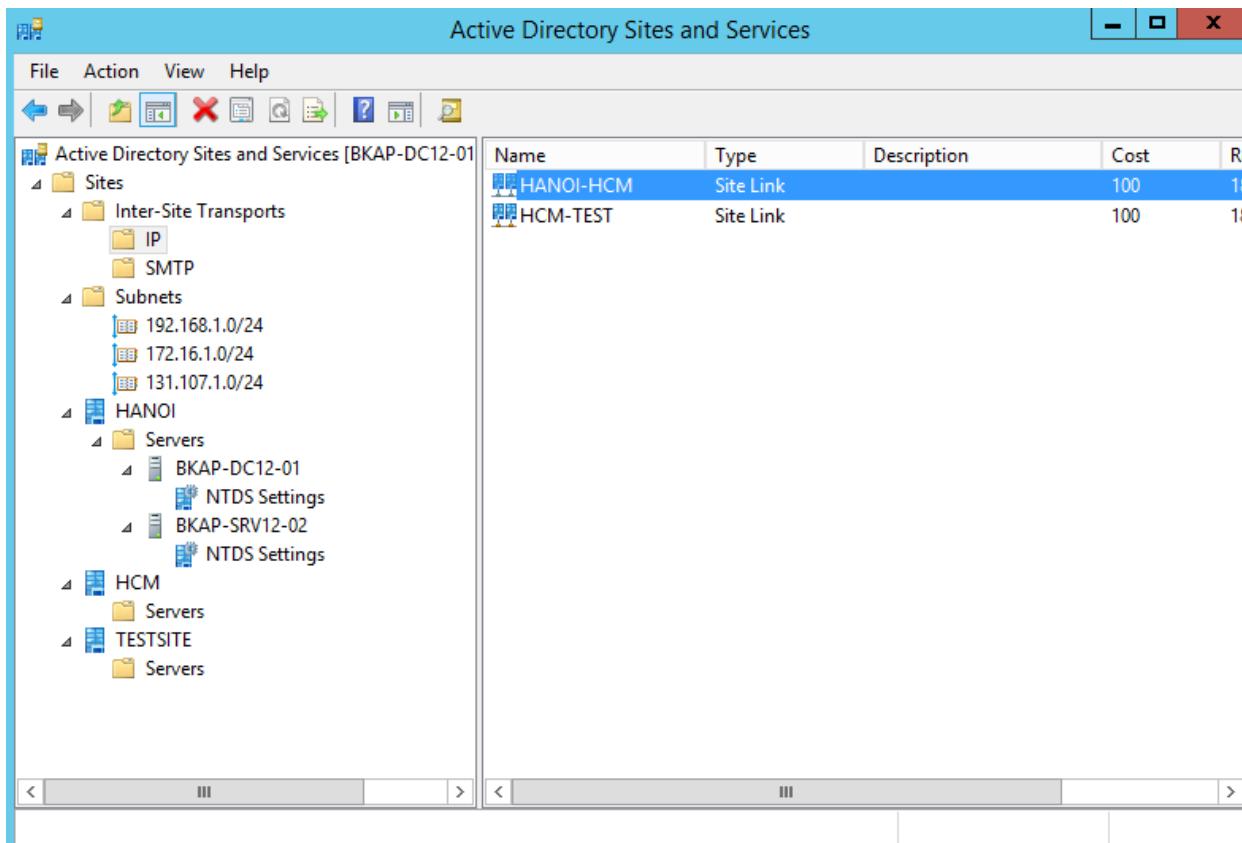
- Trong cửa sổ **Schedule for HCM-TEST**, chọn thời gian.



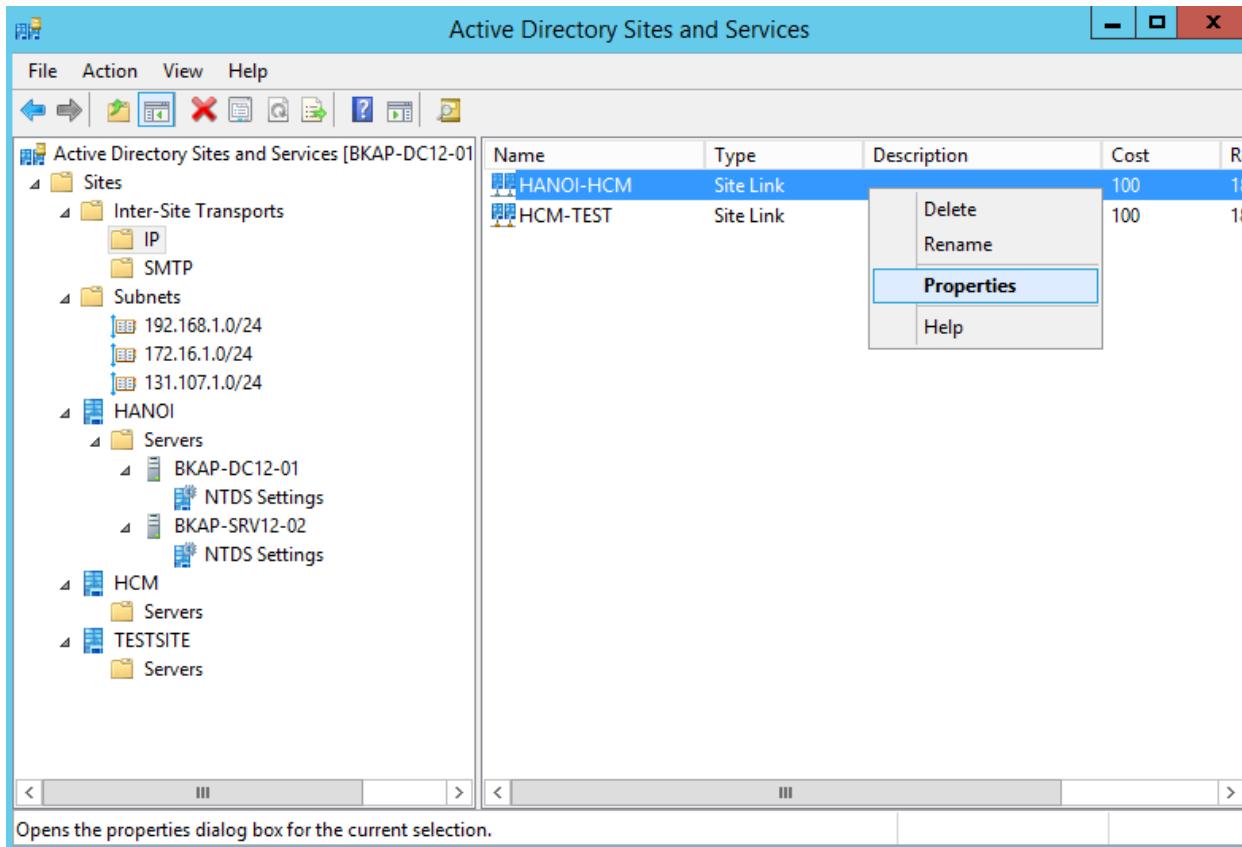
- Click **Apply/OK** tại cửa sổ **HCM-TEST Properties**.



▪ Sửa đổi tên **DEFAULTIPSITELINK** thành **HN-HCM**.

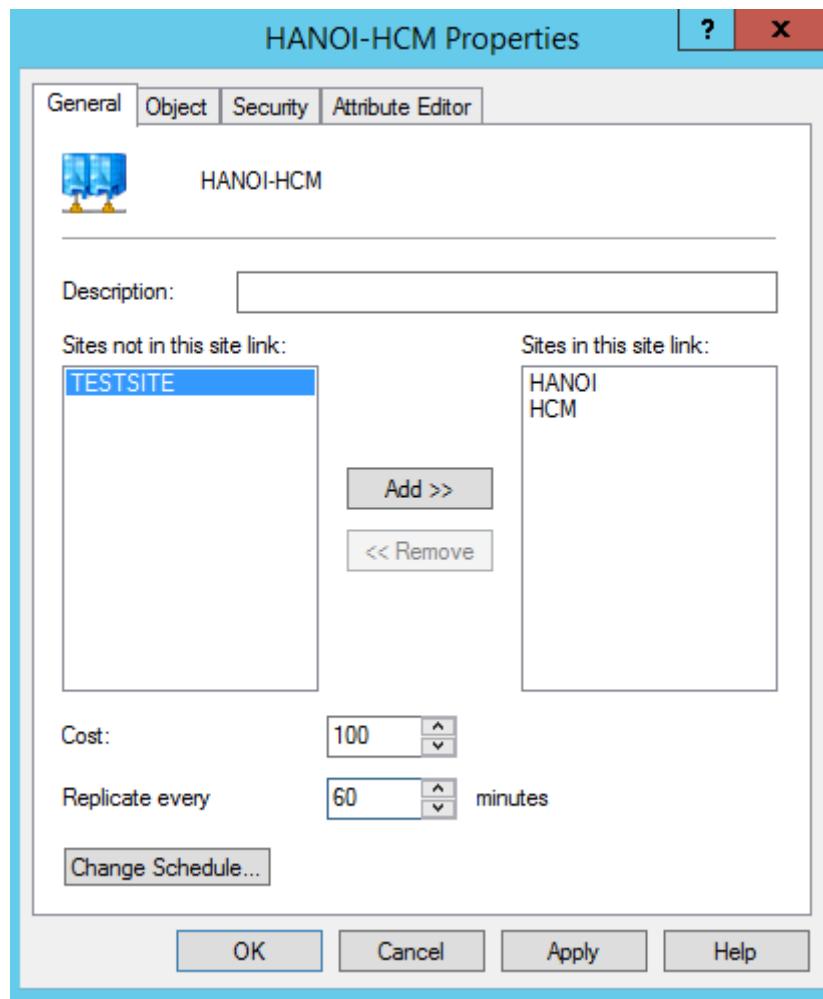


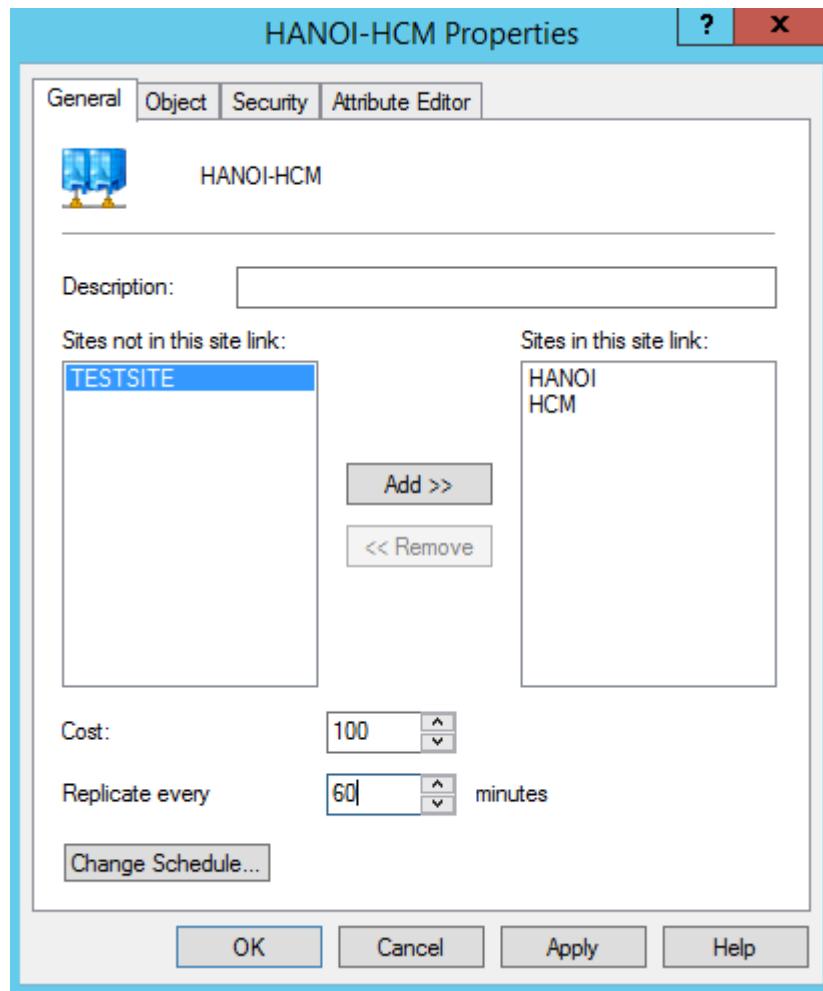
- Click chuột phải tại Site-Link HANOI-HCM, chọn Properties.



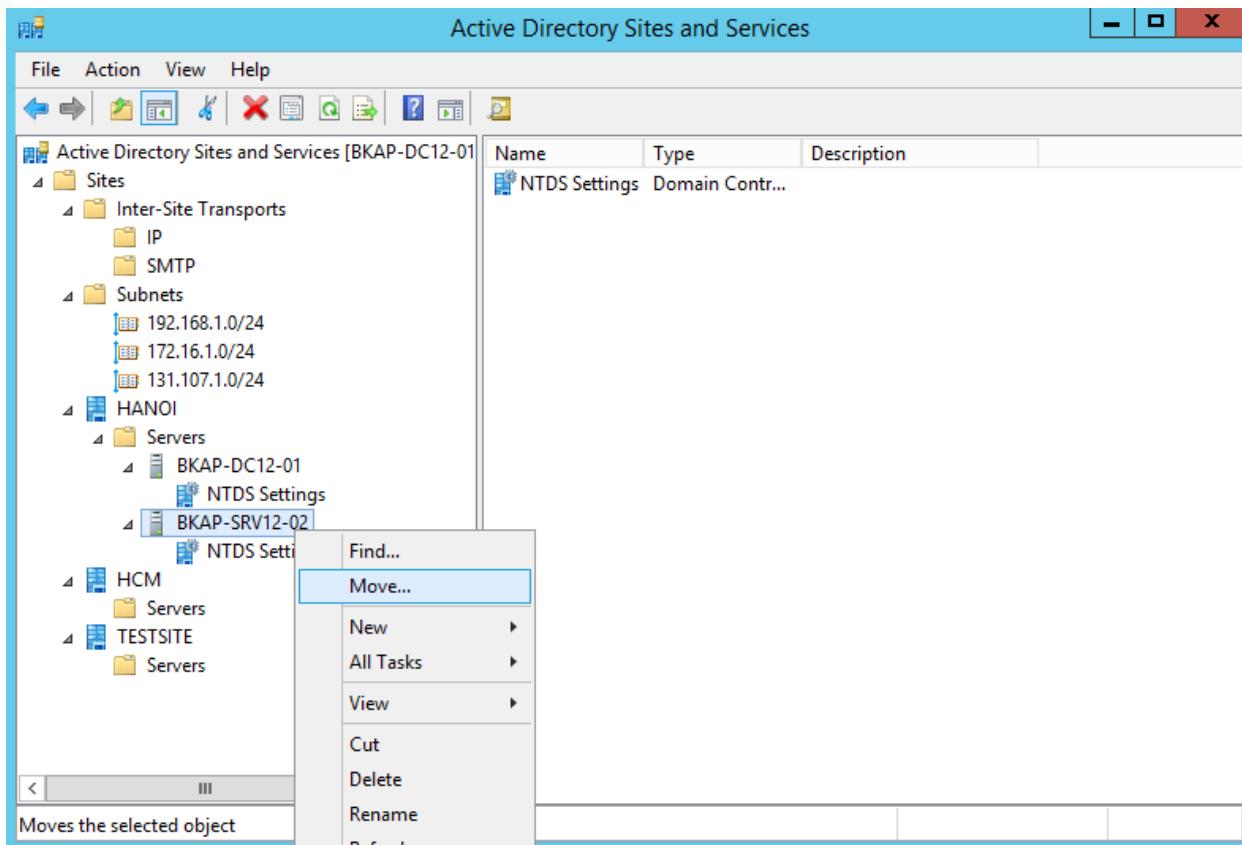
- Tại cửa sổ **HANOI-HCM Properties**, trong khung **Sites in this site link**, chọn vào **TESTSITE**, click vào << Remove.

- Điều chỉnh thông số **Replicate every : 60 minutes**.
- Click vào **Apply/OK**.

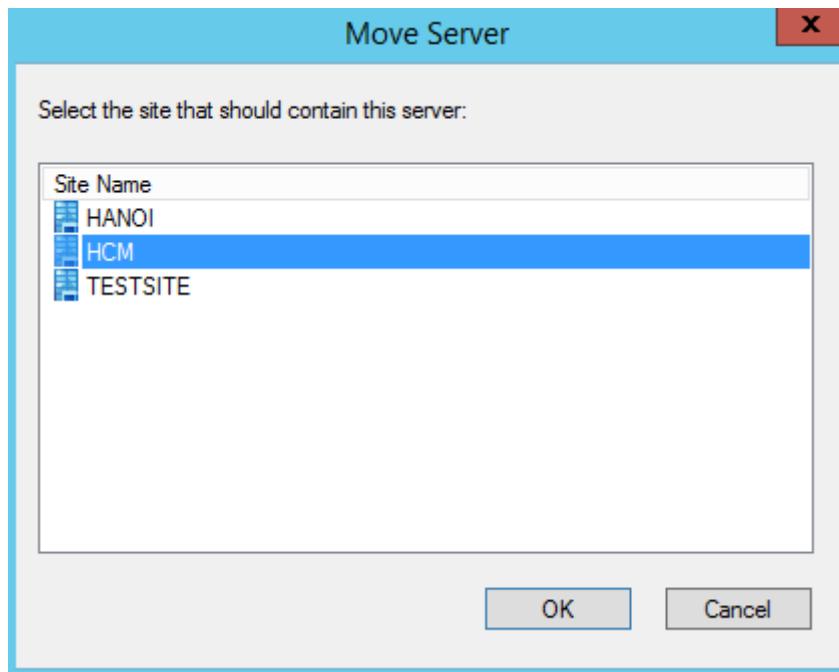




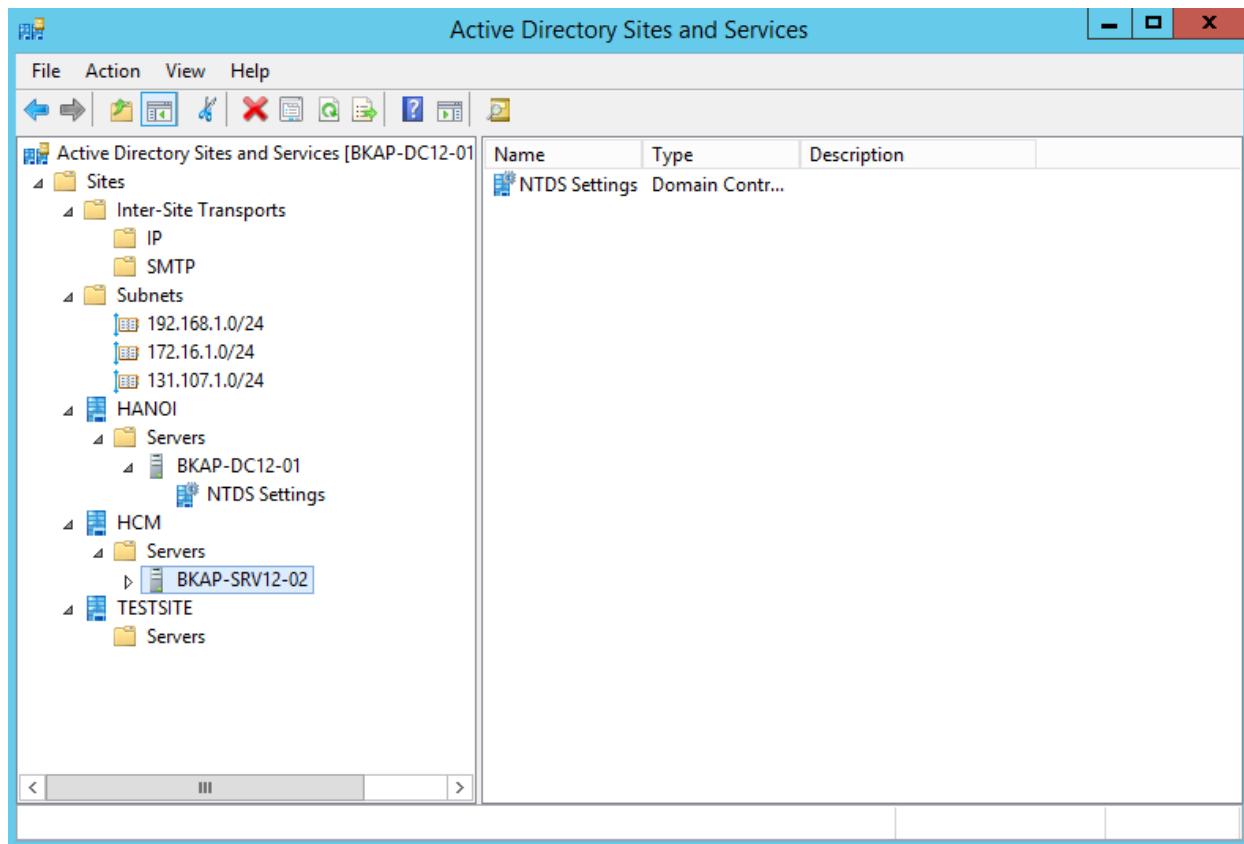
- Thực hiện di chuyển Server *BKAP-SRV12-02* về site **HCM**.
 - Trong cửa sổ **Active Directory Sites and Services**, click chuột phải tại máy *BKAP-SRV12-02* trong Sites **HANOI**, chọn vào **Move...**



- Trong cửa sổ **Move Server**, chọn vào Site **HCM**, click vào **OK**.



- Kiểm tra tại site **HCM**.



- Thực hiện giám sát *AD DS site replication*.
 - Vào **Windows PowerShell**, nhập vào các câu lệnh:
 - **repadmin /kcc**

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> repadmin /kcc

Repadmin: running command /kcc against full DC localhost
HANOI
Current Site Options: (none)
Consistency check on localhost successful.

PS C:\Users\Administrator>
```

- **repadmin /showrepl**

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> repadmin /kcc

Repadmin: running command /kcc against full DC localhost
HANOI
Current Site Options: (none)
Consistency check on localhost successful.

PS C:\Users\Administrator> repadmin /showrepl

Repadmin: running command /showrepl against full DC localhost
HANOI\BKAP-DC12-01
DSA Options: IS_GC
Site Options: (none)
DSA object GUID: 674da08c-36c4-4fa7-969e-68315b721de4
DSA invocationID: 5420cd4a-de1c-4163-be3c-16c8a7ab5703

===== INBOUND NEIGHBORS =====

DC=bkaptech,DC=vn
    HCM\BKAP-SRV12-02 via RPC
        DSA object GUID: 29353c5c-bf2b-4584-908c-fb5534947752
        Last attempt @ 2016-06-28 01:49:14 was successful.

CN=Configuration,CN=Configuration,DC=bkaptech,DC=vn
    HCM\BKAP-SRV12-02 via RPC
        DSA object GUID: 29353c5c-bf2b-4584-908c-fb5534947752
        Last attempt @ 2016-06-28 02:28:56 was successful.

CN=Schema,CN=Configuration,DC=bkaptech,DC=vn
    HCM\BKAP-SRV12-02 via RPC
        DSA object GUID: 29353c5c-bf2b-4584-908c-fb5534947752
        Last attempt @ 2016-06-28 01:49:14 was successful.

DC=DomainDnsZones,DC=bkaptech,DC=vn
    HCM\BKAP-SRV12-02 via RPC
        DSA object GUID: 29353c5c-bf2b-4584-908c-fb5534947752
        Last attempt @ 2016-06-28 02:29:13 was successful.

DC=ForestDnsZones,DC=bkaptech,DC=vn
    HCM\BKAP-SRV12-02 via RPC
        DSA object GUID: 29353c5c-bf2b-4584-908c-fb5534947752
        Last attempt @ 2016-06-28 02:29:16 was successful.

PS C:\Users\Administrator>
```

▪ *repadmin /bridgeheads*

```
Administrator: Windows PowerShell

Repadmin: running command /showrepl against full DC localhost
HANOI\BKAP-DC12-01
DSA Options: IS_GC
Site Options: (none)
DSA object GUID: 674da08c-36c4-4fa7-969e-68315b721de4
DSA invocationID: 5420cd4a-de1c-4163-be3c-16c8a7ab5703

===== INBOUND NEIGHBORS =====

DC=bkaptech,DC=vn
    HCM\BKAP-SRV12-02 via RPC
        DSA object GUID: 29353c5c-bf2b-4584-908c-fb5534947752
        Last attempt @ 2016-06-28 01:49:14 was successful.

CN=Configuration,DC=bkaptech,DC=vn
    HCM\BKAP-SRV12-02 via RPC
        DSA object GUID: 29353c5c-bf2b-4584-908c-fb5534947752
        Last attempt @ 2016-06-28 02:28:56 was successful.

CN=Schema,CN=Configuration,DC=bkaptech,DC=vn
    HCM\BKAP-SRV12-02 via RPC
        DSA object GUID: 29353c5c-bf2b-4584-908c-fb5534947752
        Last attempt @ 2016-06-28 01:49:14 was successful.

DC=DomainDnsZones,DC=bkaptech,DC=vn
    HCM\BKAP-SRV12-02 via RPC
        DSA object GUID: 29353c5c-bf2b-4584-908c-fb5534947752
        Last attempt @ 2016-06-28 02:29:13 was successful.

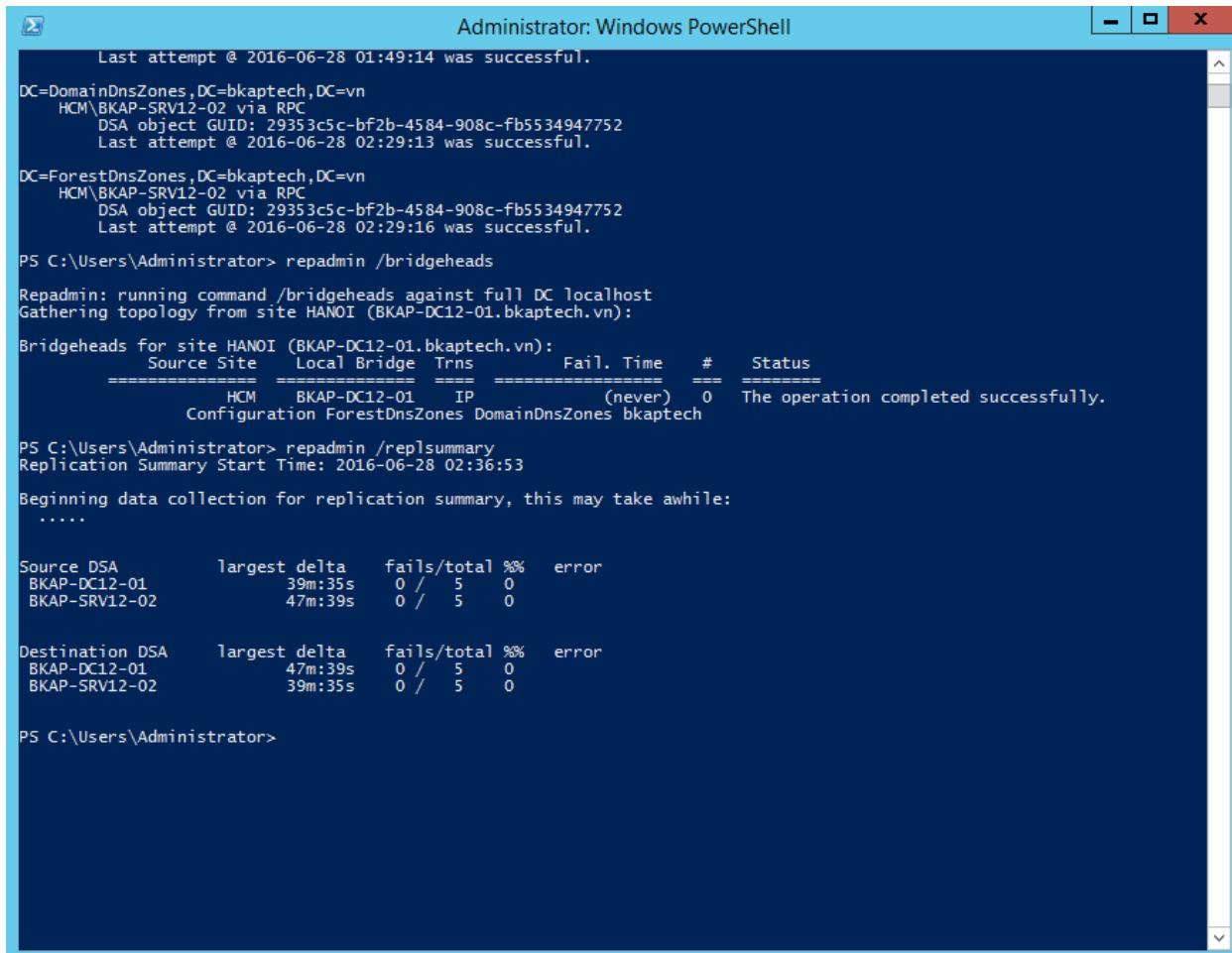
DC=ForestDnsZones,DC=bkaptech,DC=vn
    HCM\BKAP-SRV12-02 via RPC
        DSA object GUID: 29353c5c-bf2b-4584-908c-fb5534947752
        Last attempt @ 2016-06-28 02:29:16 was successful.

PS C:\Users\Administrator> repadmin /bridgeheads

Repadmin: running command /bridgeheads against full DC localhost
Gathering topology from site HANOI (BKAP-DC12-01.bkaptech.vn):

Bridgeheads for site HANOI (BKAP-DC12-01.bkaptech.vn):
Source Site Local Bridge Trns Fail. Time # Status
===== ===== = = ===== = = =====
HCM BKAP-DC12-01 IP (never) 0 The operation completed successfully.
Configuration ForestDnsZones DomainDnsZones bkaptech

PS C:\Users\Administrator>
```

■ *repadmin /replsummary*

```
Last attempt @ 2016-06-28 01:49:14 was successful.

DC=DomainDnsZones,DC=bkaptech,DC=vn
HCM\BKAP-SRV12-02 via RPC
DSA object GUID: 29353c5c-bf2b-4584-908c-fb5534947752
Last attempt @ 2016-06-28 02:29:13 was successful.

DC=ForestDnsZones,DC=bkaptech,DC=vn
HCM\BKAP-SRV12-02 via RPC
DSA object GUID: 29353c5c-bf2b-4584-908c-fb5534947752
Last attempt @ 2016-06-28 02:29:16 was successful.

PS C:\Users\Administrator> repadmin /bridgeheads

Repadmin: running command /bridgeheads against full DC localhost
Gathering topology from site HANOI (BKAP-DC12-01.bkaptech.vn):

Bridgeheads for site HANOI (BKAP-DC12-01.bkaptech.vn):
Source Site Local Bridge Trns Fail. Time # Status
===== ===== = == ===== = == =====
HCM BKAP-DC12-01 IP (never) 0 The operation completed successfully.
Configuration ForestDnsZones DomainDnsZones bkaptech

PS C:\Users\Administrator> repadmin /replsummary
Replication Summary Start Time: 2016-06-28 02:36:53

Beginning data collection for replication summary, this may take awhile:
.....
Source DSA      largest delta    fails/total %%   error
BKAP-DC12-01        39m:35s     0 / 5      0
BKAP-5RV12-02        47m:39s     0 / 5      0

Destination DSA      largest delta    fails/total %%   error
BKAP-DC12-01        47m:39s     0 / 5      0
BKAP-5RV12-02        39m:35s     0 / 5      0

PS C:\Users\Administrator>
```

■ *dcdiag /test:replications*

```
Administrator: Windows PowerShell
BKAP-DC12-01      39m:35s  0 /  5  0
BKAP-SRV12-02      47m:39s  0 /  5  0

Destination DSA      largest delta    fails/total %%   error
BKAP-DC12-01          47m:39s      0 /  5  0
BKAP-SRV12-02          39m:35s      0 /  5  0

PS C:\Users\Administrator> dcdiag /test:replications
Directory Server Diagnosis
Performing initial setup:
  Trying to find home server...
  Home Server = BKAP-DC12-01
  * Identified AD Forest.
  Done gathering initial info.

Doing initial required tests
  Testing server: HANOI\BKAP-DC12-01
    Starting test: Connectivity
      ..... BKAP-DC12-01 passed test Connectivity

Doing primary tests
  Testing server: HANOI\BKAP-DC12-01
    Starting test: Replications
      ..... BKAP-DC12-01 passed test Replications

  Running partition tests on : ForestDnsZones
  Running partition tests on : DomainDnsZones
  Running partition tests on : Schema
  Running partition tests on : Configuration
  Running partition tests on : bkaptech
  Running enterprise tests on : bkaptech.vn
PS C:\Users\Administrator>
```

Bài 5:**TRIỂN KHAI DỊCH VỤ ACTIVE DIRECTORY RIGHTS MANAGEMENT SERVICES****Các nội dung chính được đề cập:**

- ✓ Cấu hình Active Directory Rights Management Services – Phần 1.
- ✓ Cấu hình Active Directory Rights Management Services – Phần 2.
- ✓ Cấu hình Active Directory Rights Management Services – Phần 3.

5.1 Cấu hình Active Directory Rights Management Services – P1**1.Yêu cầu bài lab:**

+ Cài đặt và cấu hình **AD RMS** để phân quyền và bảo vệ các tài liệu quan trọng trong tổ chức, phân quyền cho người dùng thuộc tổ chức khác và tích hợp với Dynamic Access Control (DAC) để tự động bảo vệ các tài liệu nhạy cảm dựa trên các điều kiện xác định.

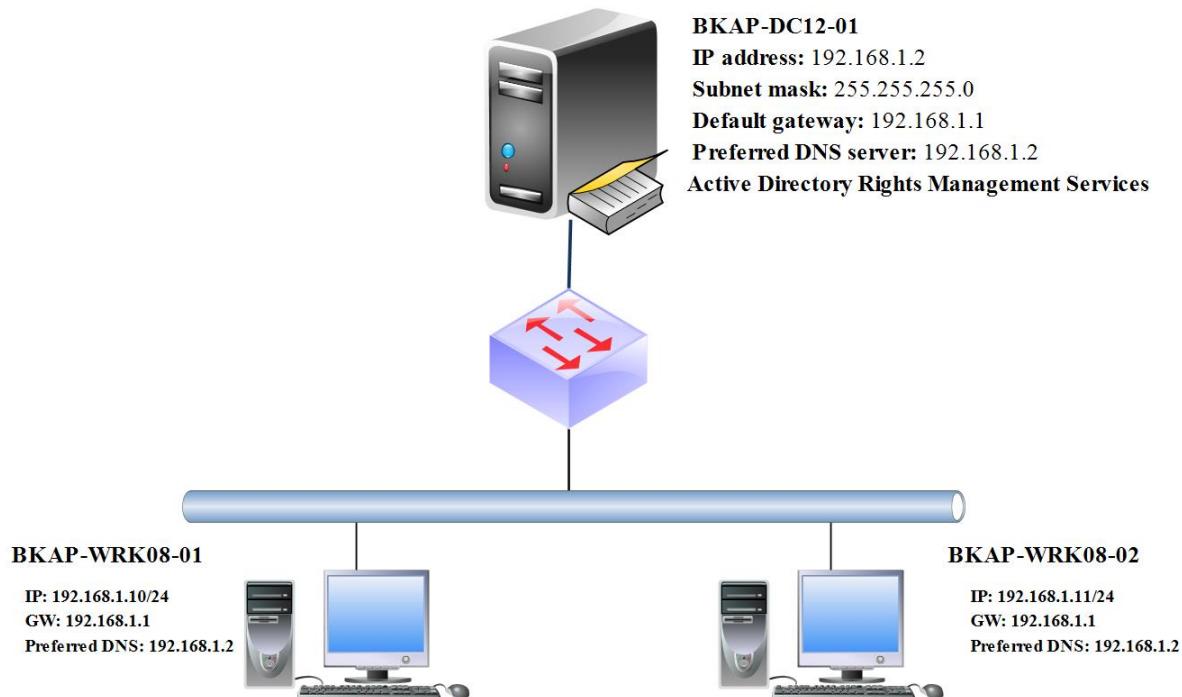
2.Yêu cầu chuẩn bị:

- + BKAP-DC12-01: Domain Controller quản lý miền **bkaptech.vn**.
- + BKAP-WRK08-01: Join vào domain, cài đặt *Office 2013*.

3.Mô hình Lab:

HỆ THỐNG ĐÀO TẠO CNTT QUỐC TẾ BACHKHOA-APTECH

Cài đặt và cấu hình AD RMS (Phân 1)



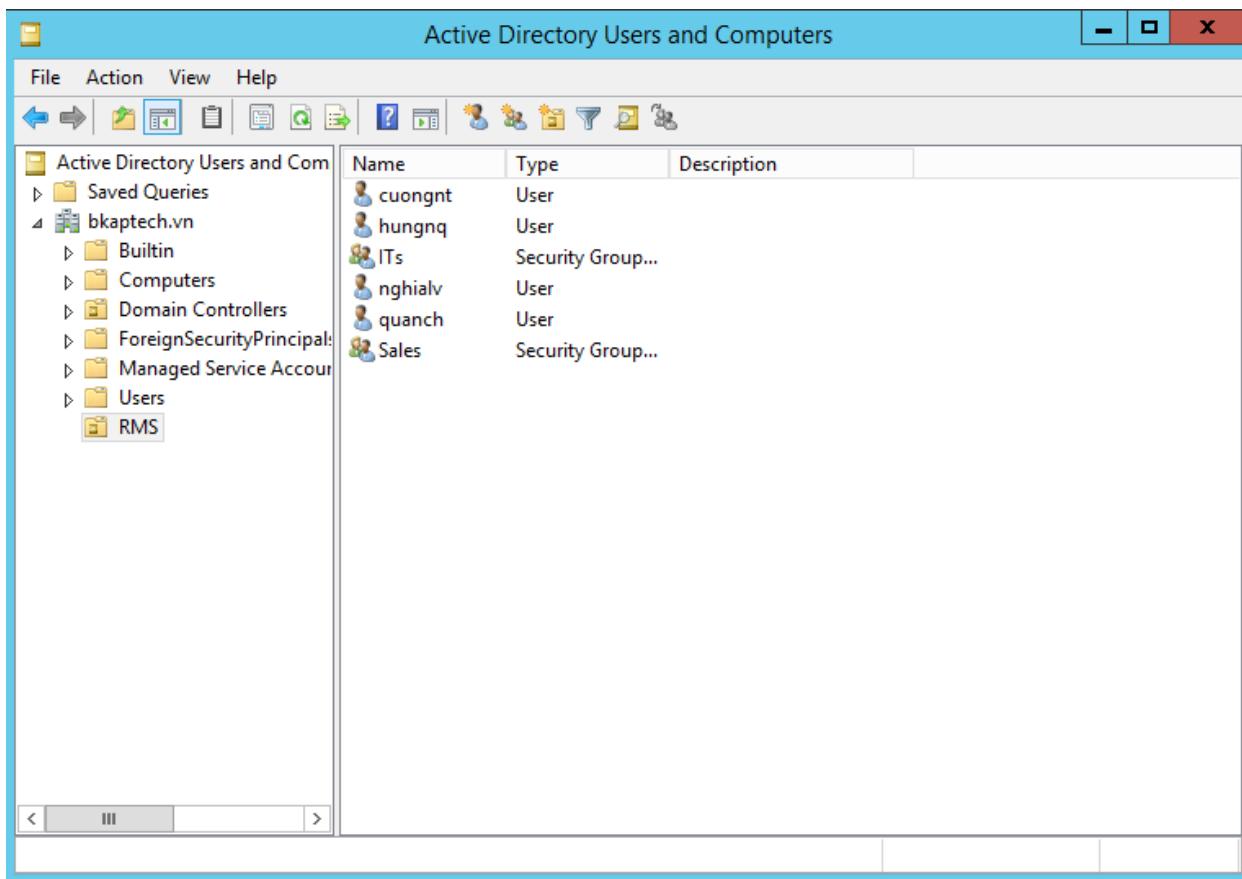
Sơ đồ địa chỉ như sau:

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

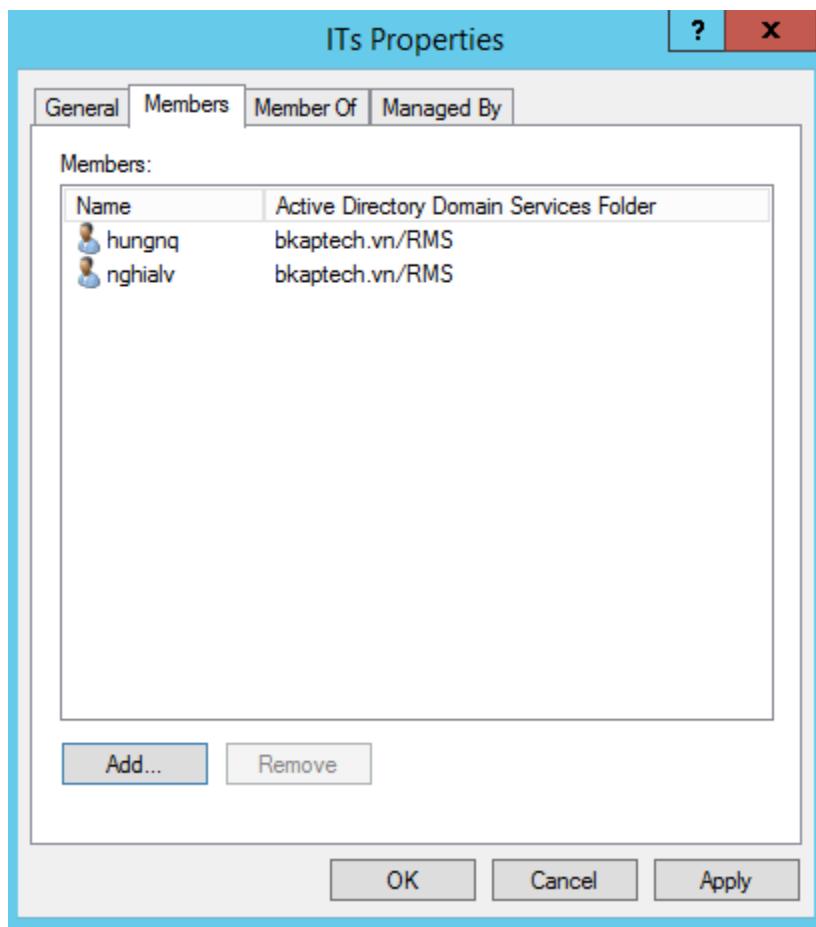
Hướng dẫn chi tiết:

Mở các máy ảo, kết nối như mô hình, đặt địa chỉ IP, ping thông giữa các máy.

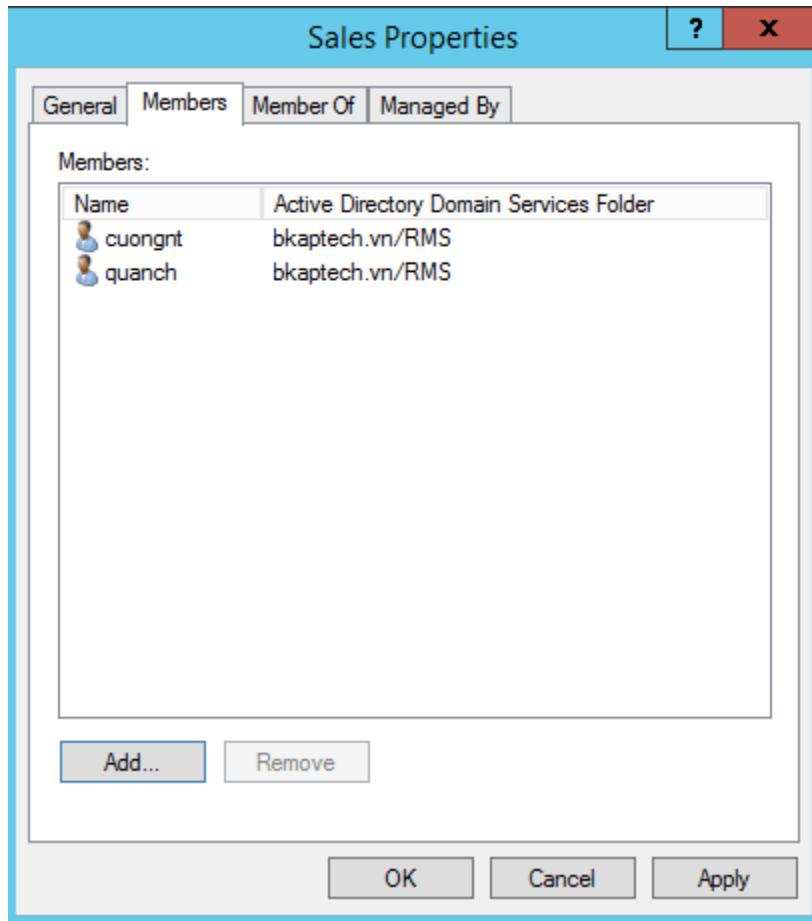
- Trên BKAP-DC12-01, thực hiện tạo các tài khoản người dùng và cấu hình thuộc tính *Email Address*.
 - Vào **Active Directory User and Computers**, tạo ou **RMS**, tạo user **hungnq, nghialv, quanch, cuongnt** trong ou **RMS**, tạo Group **ITs, Sales** trong ou **RMS**.



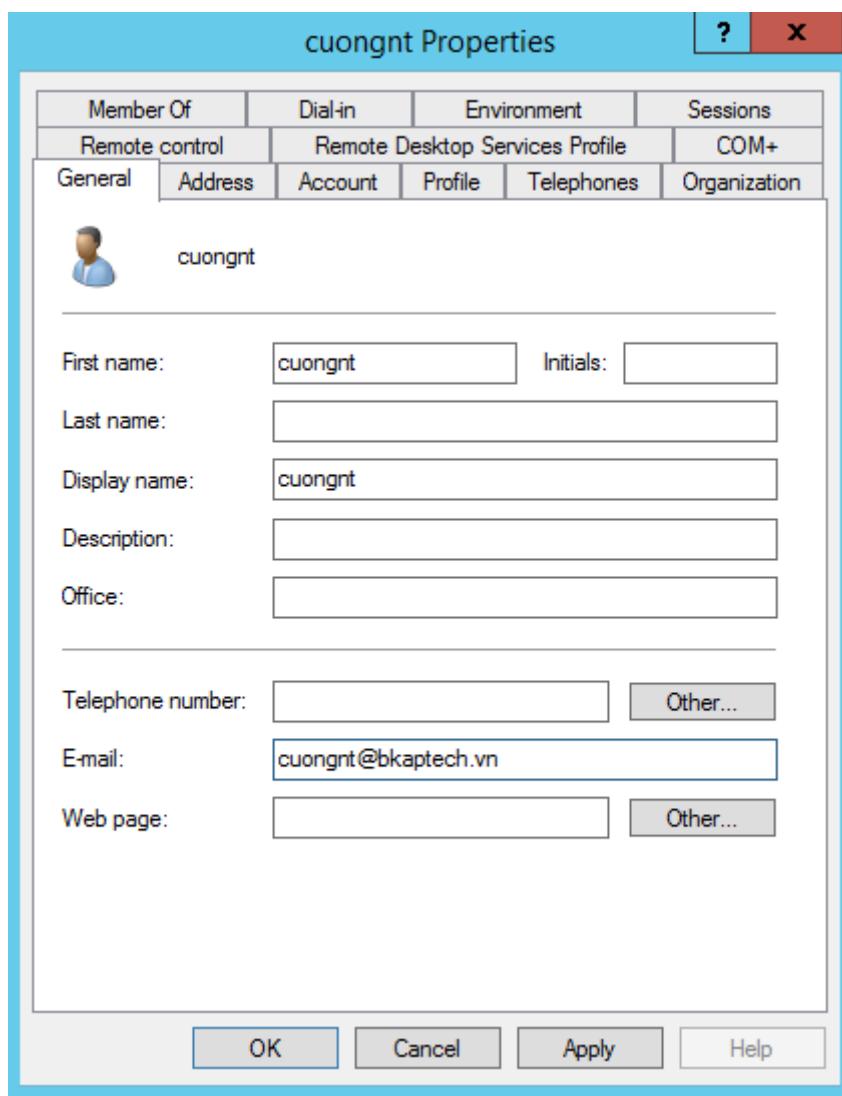
- Add user **hungnq, nghialv** vào group **ITs**.



- Add user **cuongnt, quanch** vào group **Sales**.



- Tạo thông tin mail cho các user:



hungnq Properties

Member Of	Dial-in	Environment	Sessions
Remote control	Remote Desktop Services Profile	COM+	
General	Address	Account	Profile Telephones Organization

hungnq

First name: Initials:

Last name:

Display name:

Description:

Office:

Telephone number: Other...

E-mail:

Web page: Other...

OK Cancel Apply Help

nghialv Properties

Member Of	Dial-in	Environment	Sessions		
Remote control	Remote Desktop Services Profile		COM+		
General	Address	Account	Profile	Telephones	Organization

 nghialv

First name: Initials:

Last name:

Display name:

Description:

Office:

Telephone number: Other...

E-mail:

Web page: Other...

quanch Properties

Member Of	Dial-in	Environment	Sessions
Remote control	Remote Desktop Services Profile	COM+	
General	Address	Account	Profile
		Telephones	Organization

quanch

First name: Initials:

Last name:

Display name:

Description:

Office:

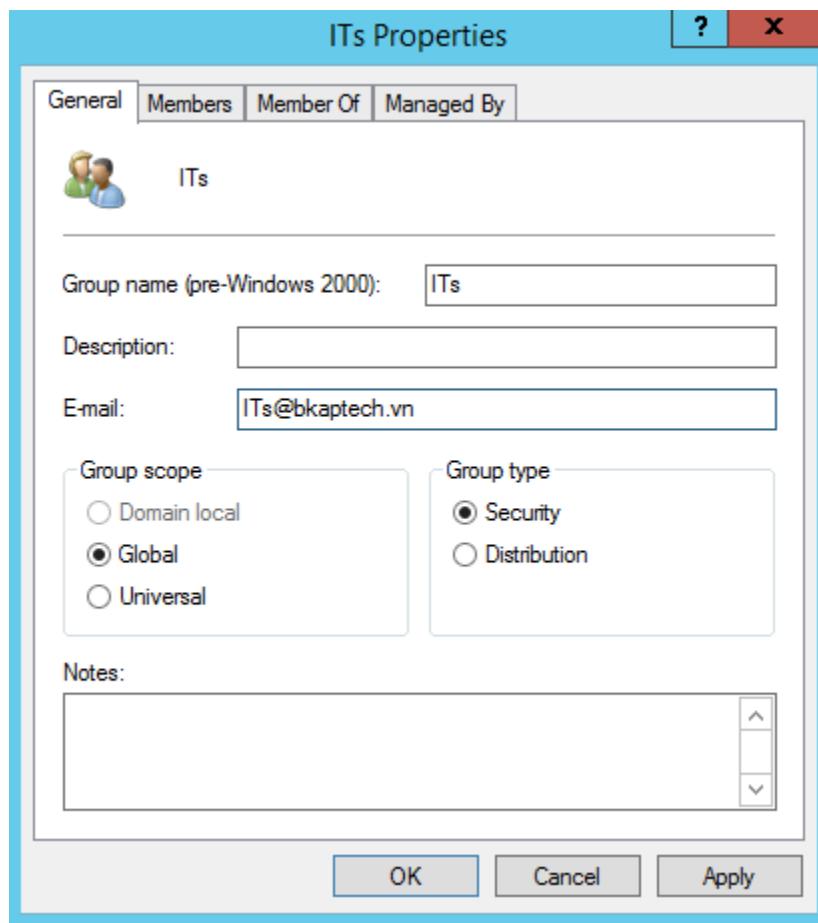
Telephone number: Other...

E-mail:

Web page: Other...

OK Cancel Apply Help

- Tạo thông tin *mail* cho group ITs và group Sales:



Sales Properties

General Members Member Of Managed By

 Sales

Group name (pre-Windows 2000):

Description:

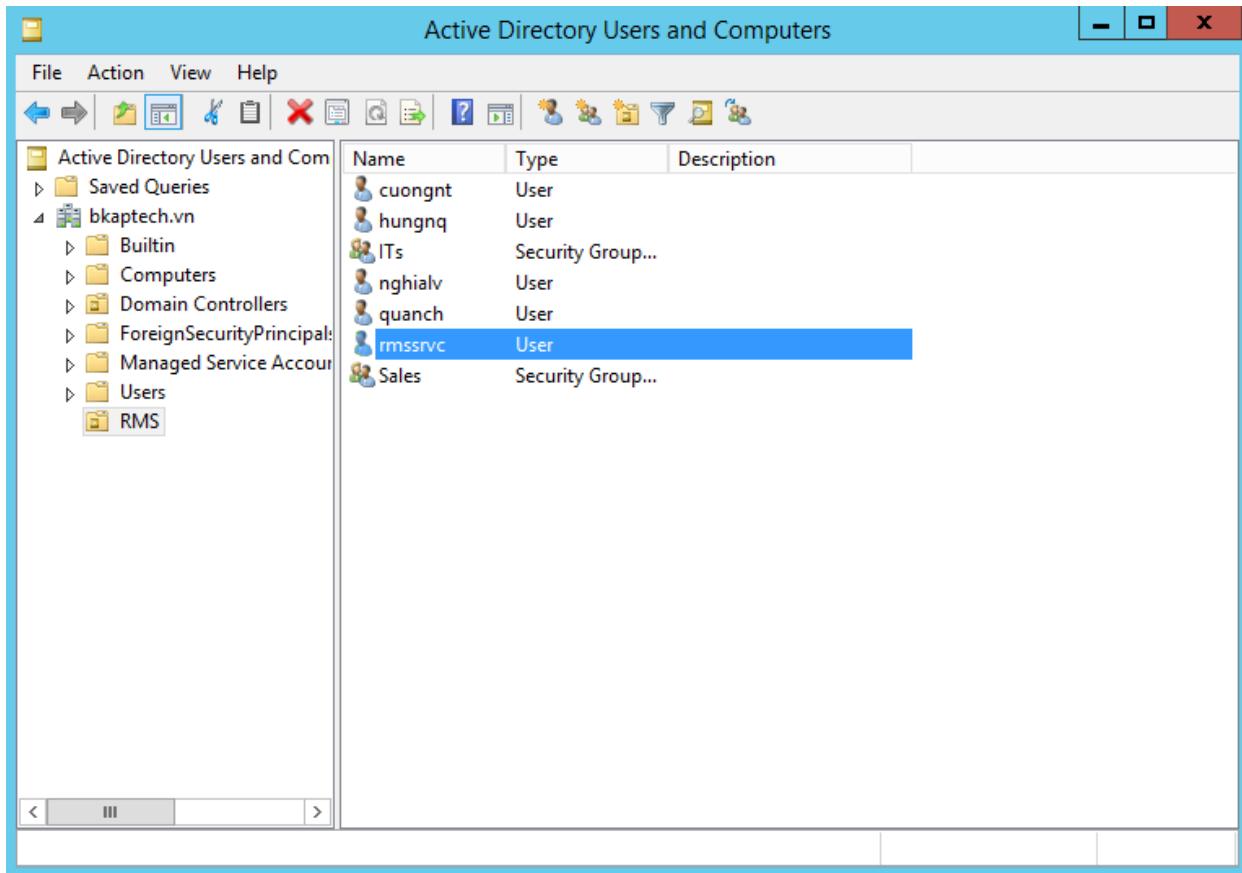
E-mail:

Group scope Domain local Global Universal

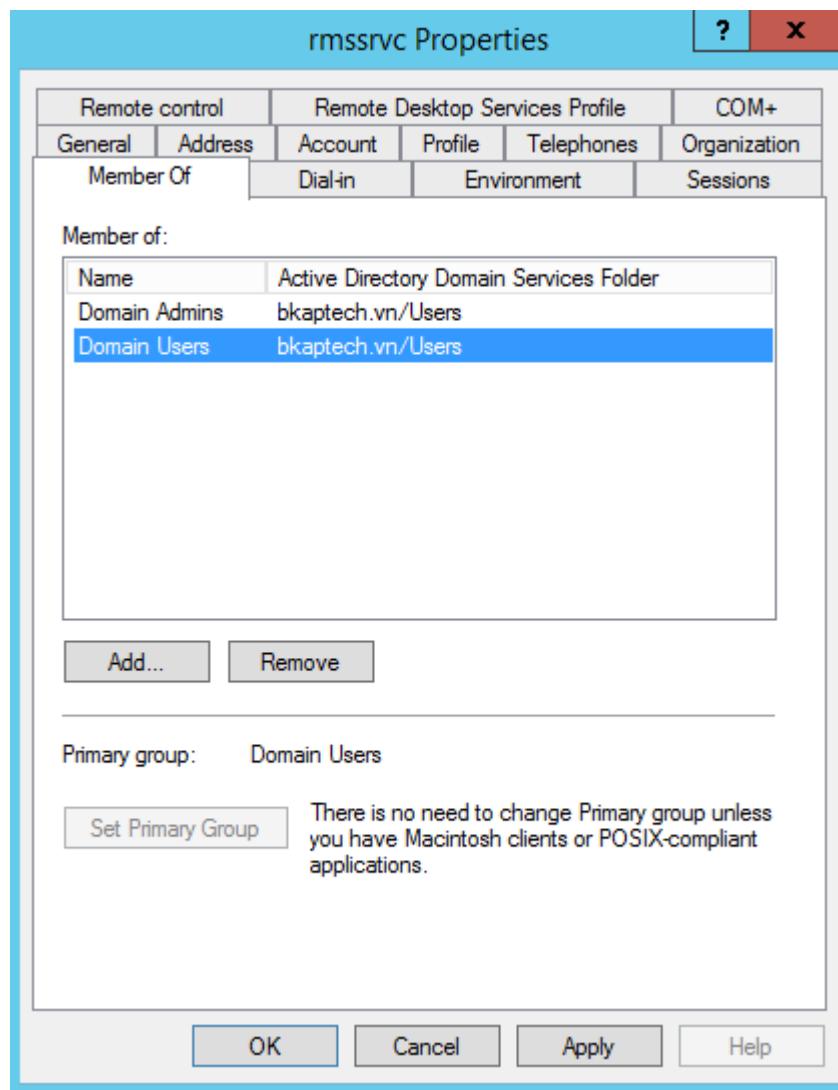
Group type Security Distribution

Notes:

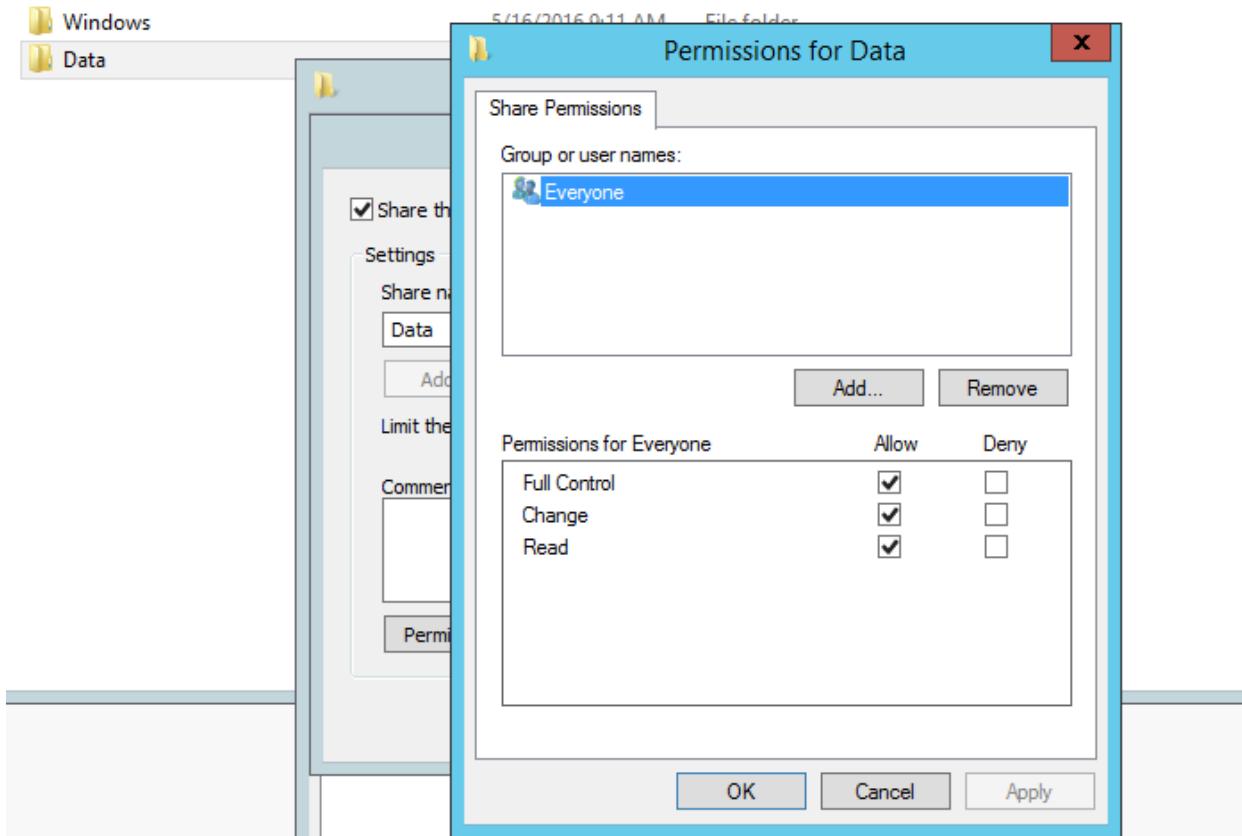
- Trong ou RMS, tạo user **rmssrvc**, add user này vào Group **Domain Admins**.



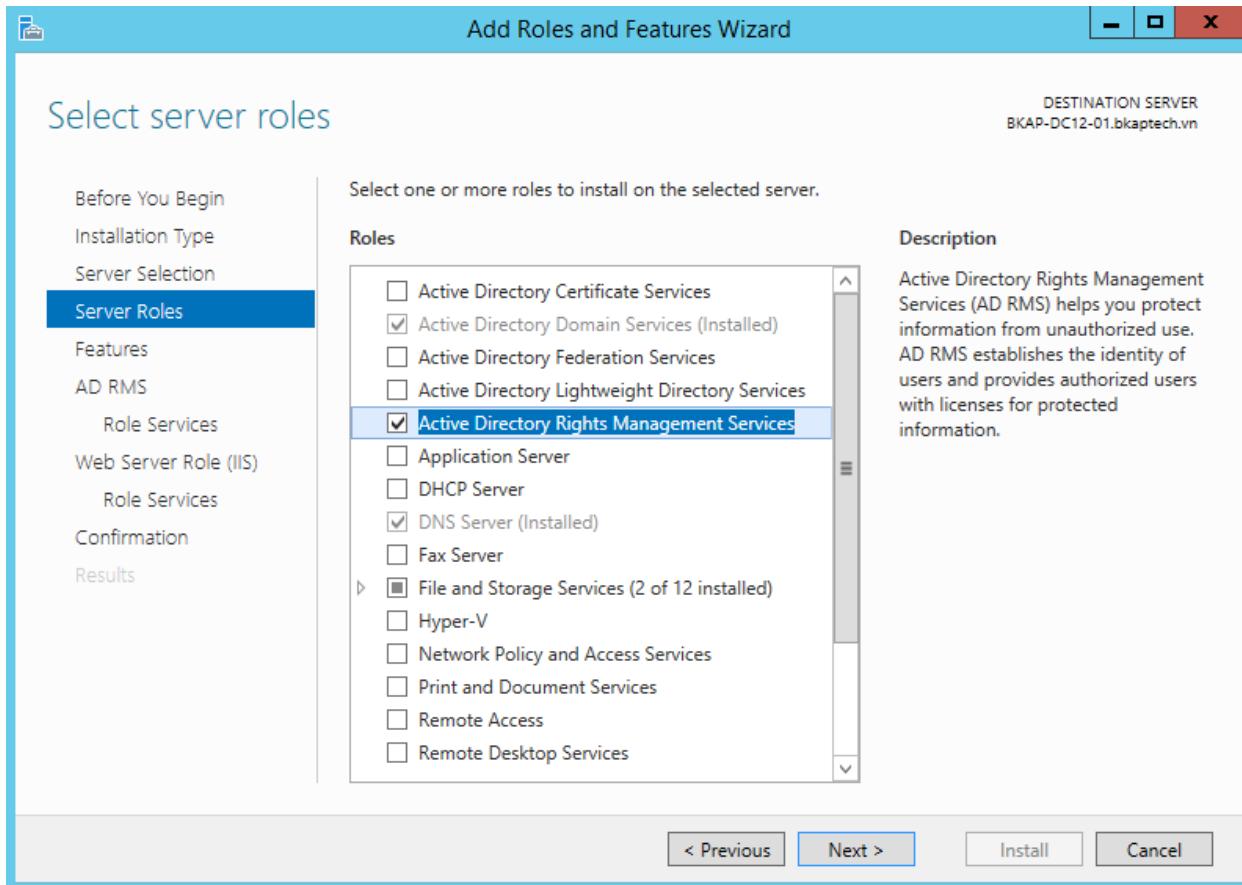
- Add user **rmssrvc** vào group **Domain Admins**.



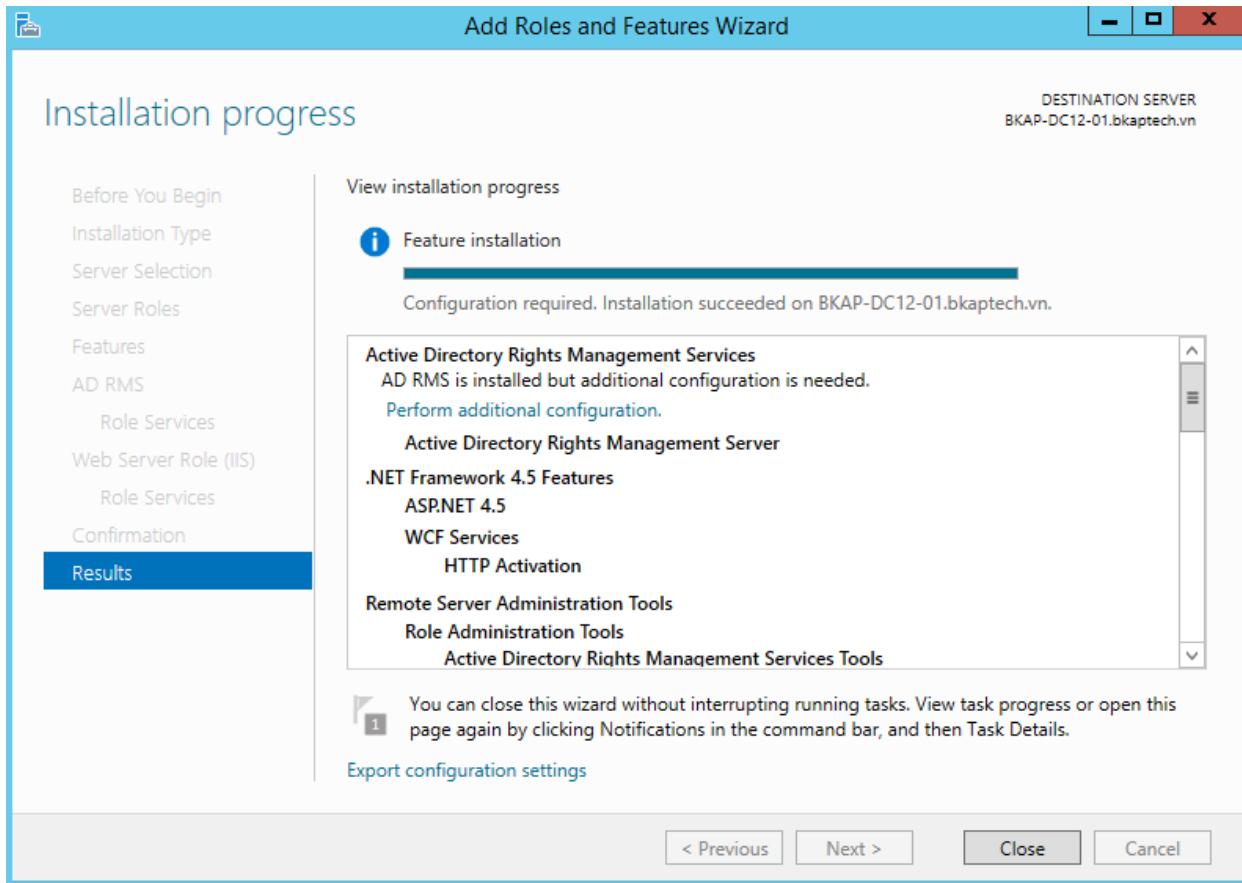
- Tạo thư mục **Data** trong ổ *C*, share thư mục này với quyền *Full Control* cho *Everyone*.



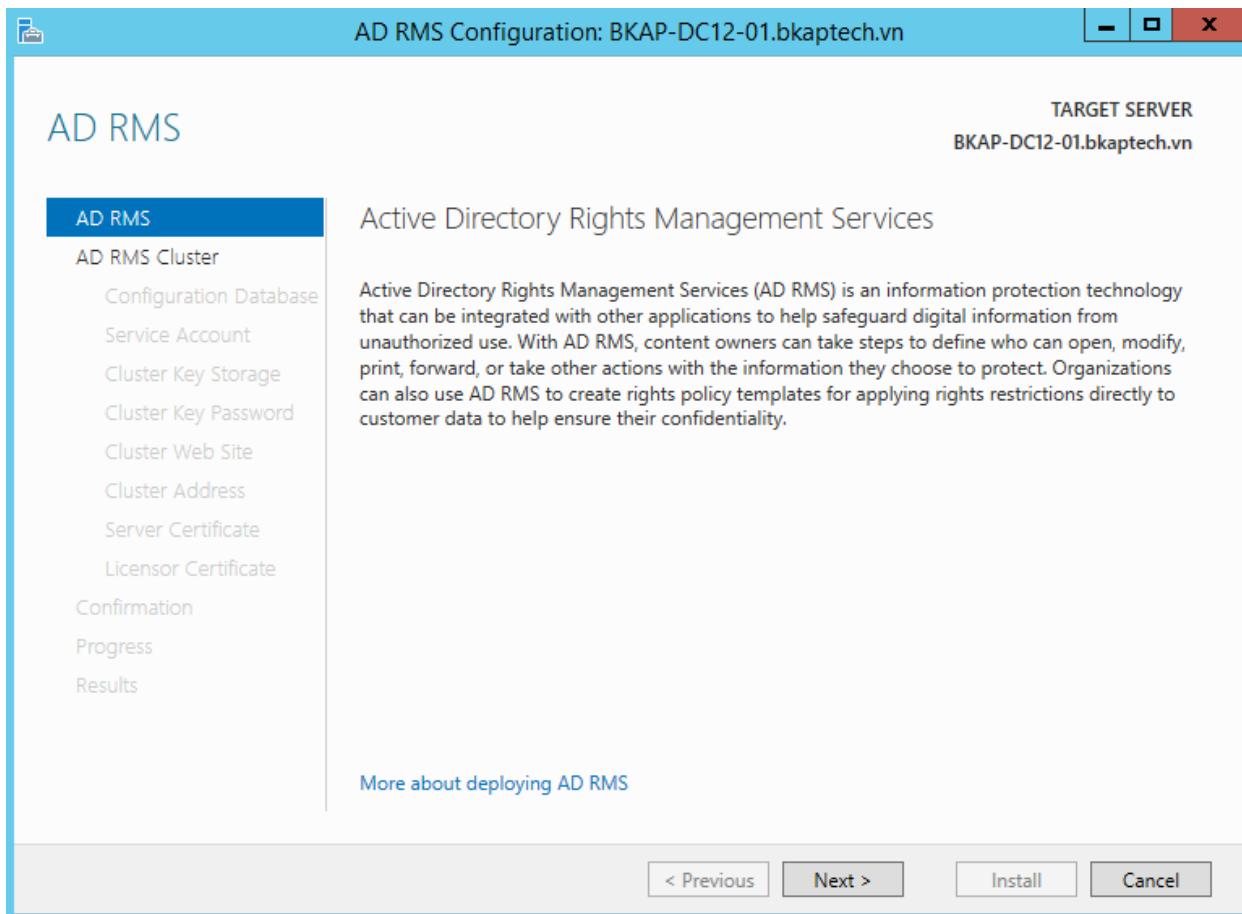
o Cài đặt AD RMS.



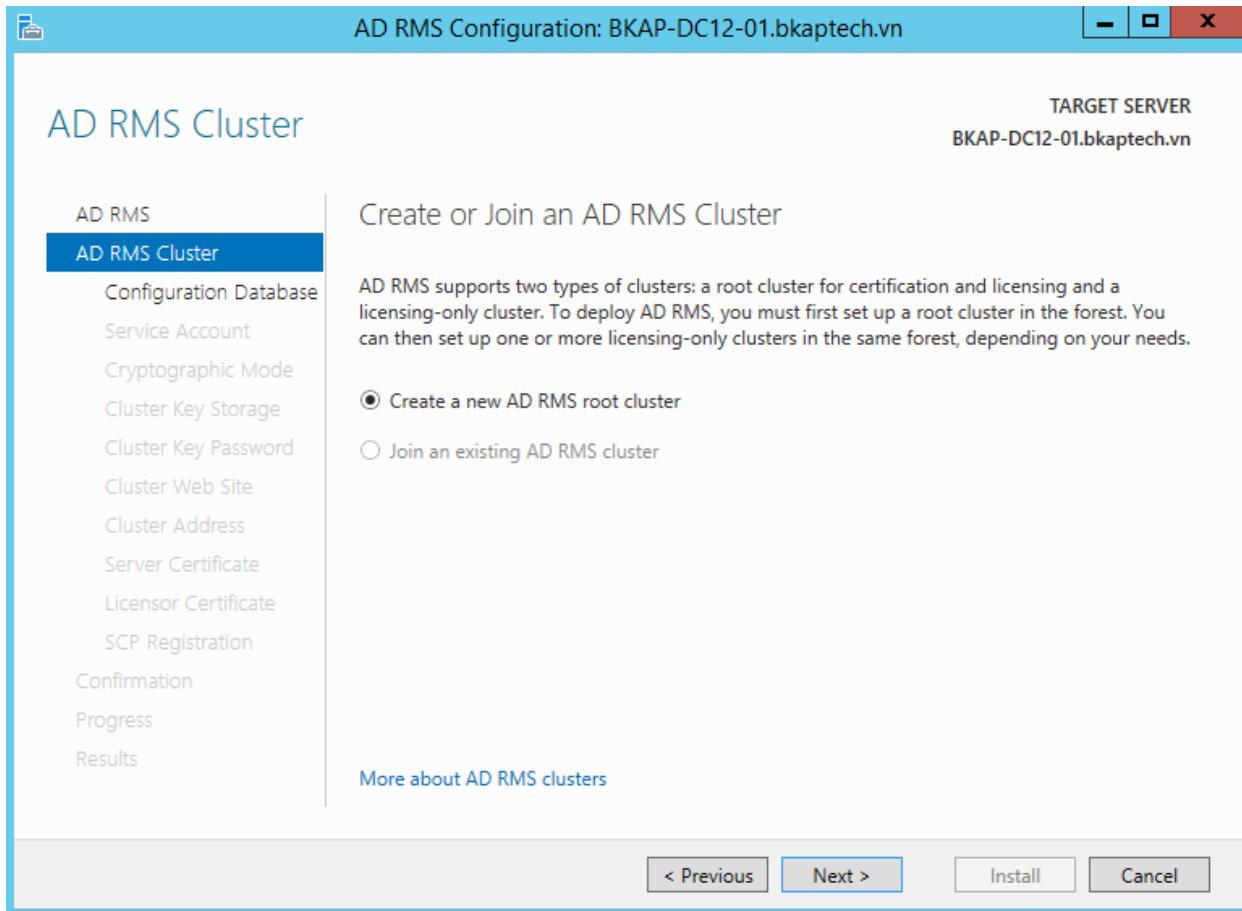
- Chờ đợi dịch vụ kết thúc cài đặt, chọn “*Perform additional configuration*”.



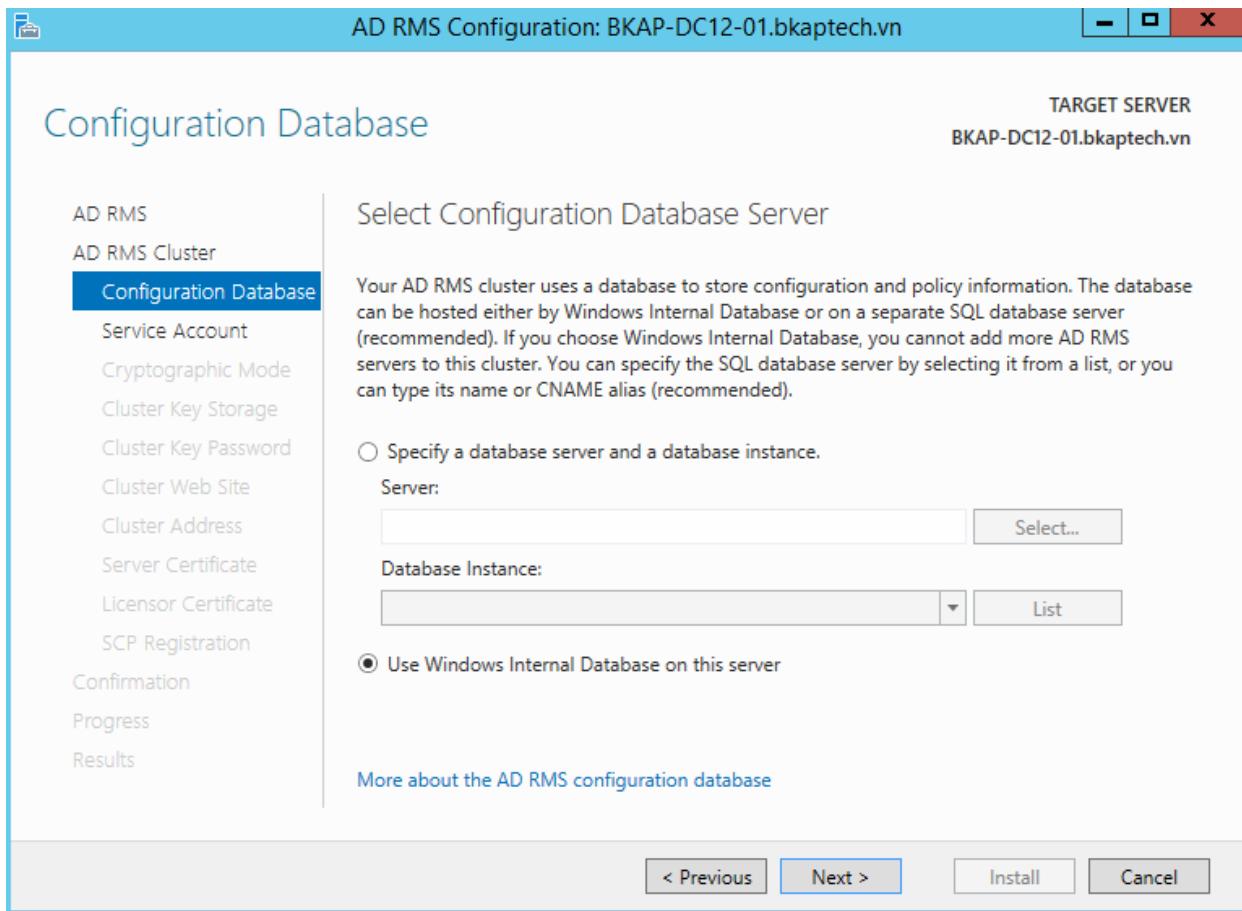
- Tại cửa sổ **AD RMS**, click vào **Next**.



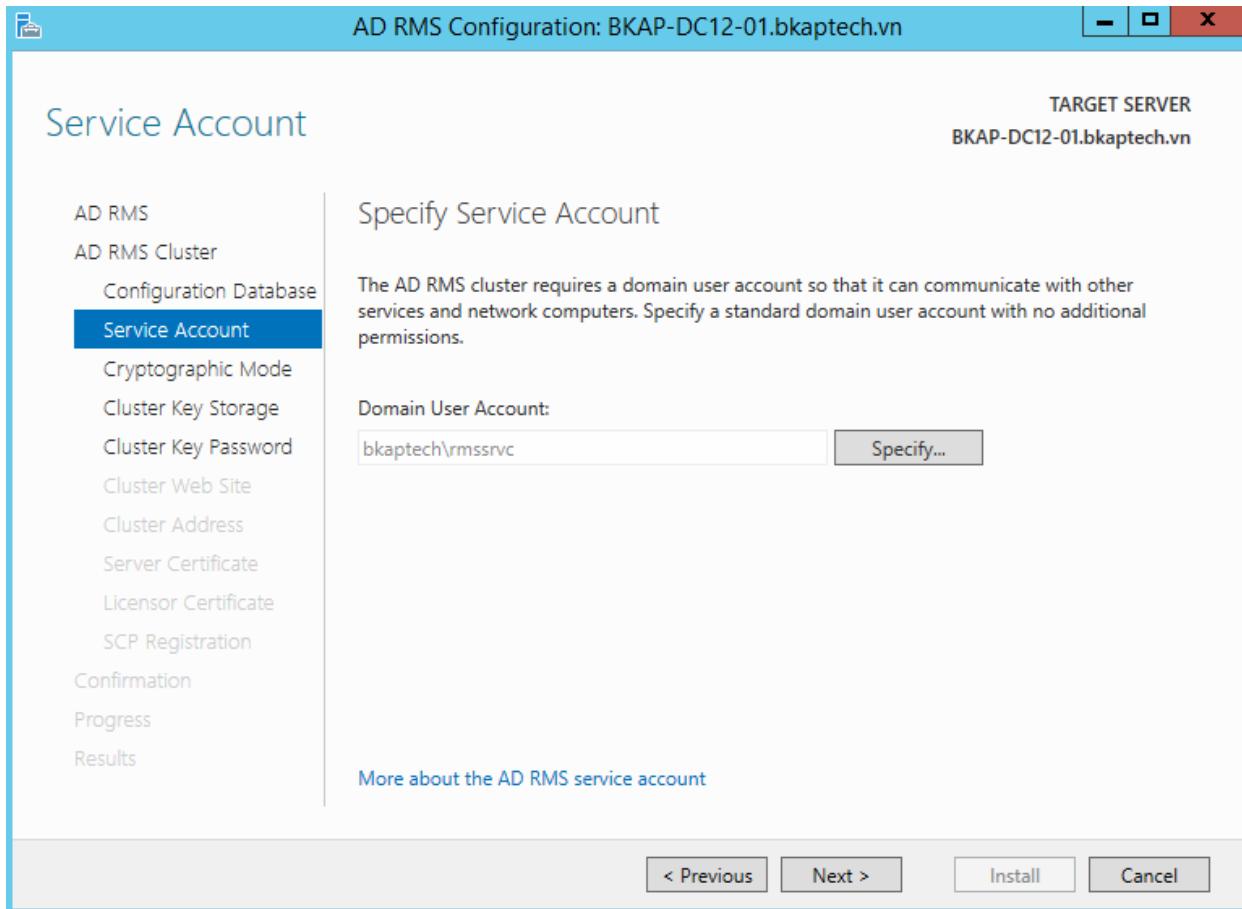
- Tại cửa sổ **AD RMS Cluster**, chọn *Create a new AD RMS root cluster*, sau đó click vào **Next**.



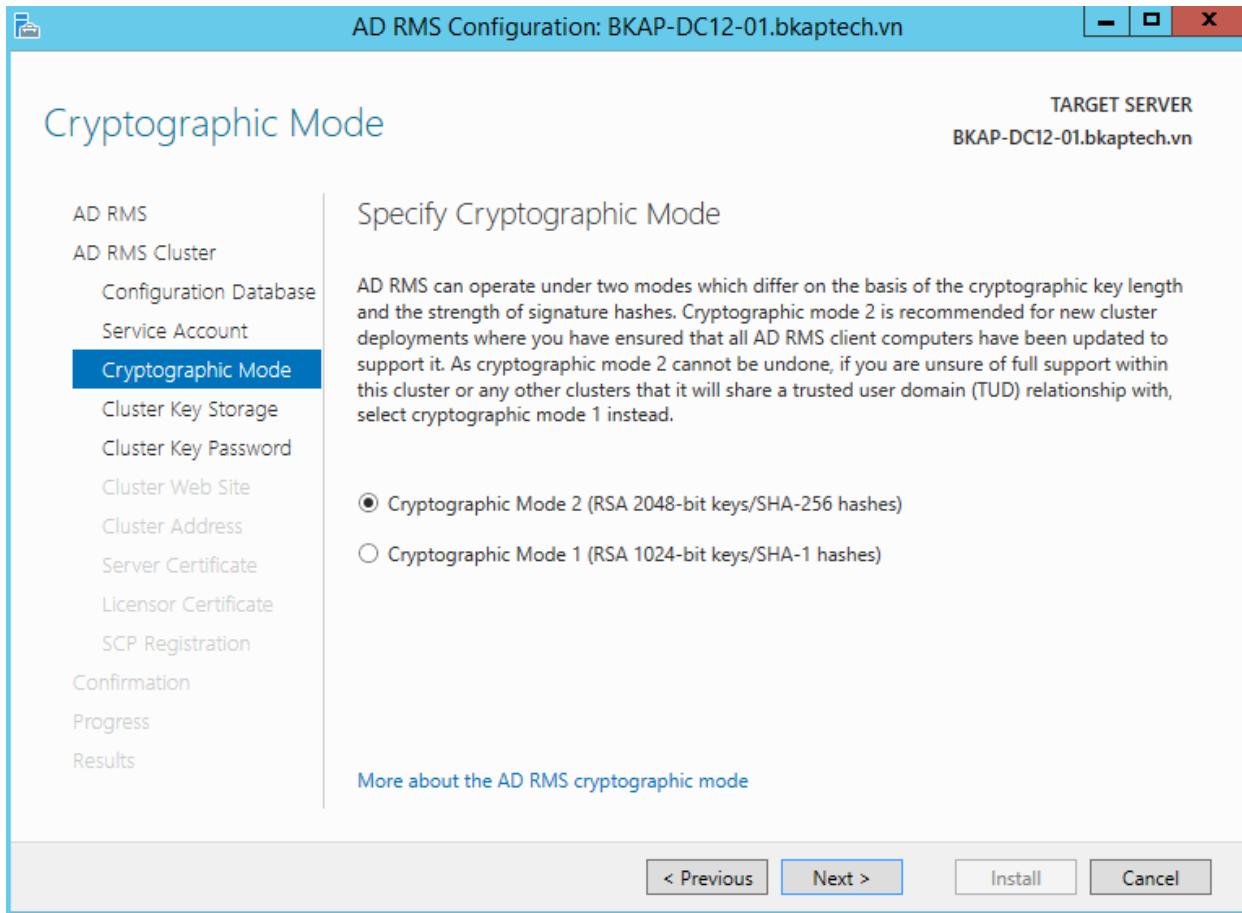
- Tại cửa sổ **Configuration Database**, chọn vào *Use Windows Internal Database on this server.*



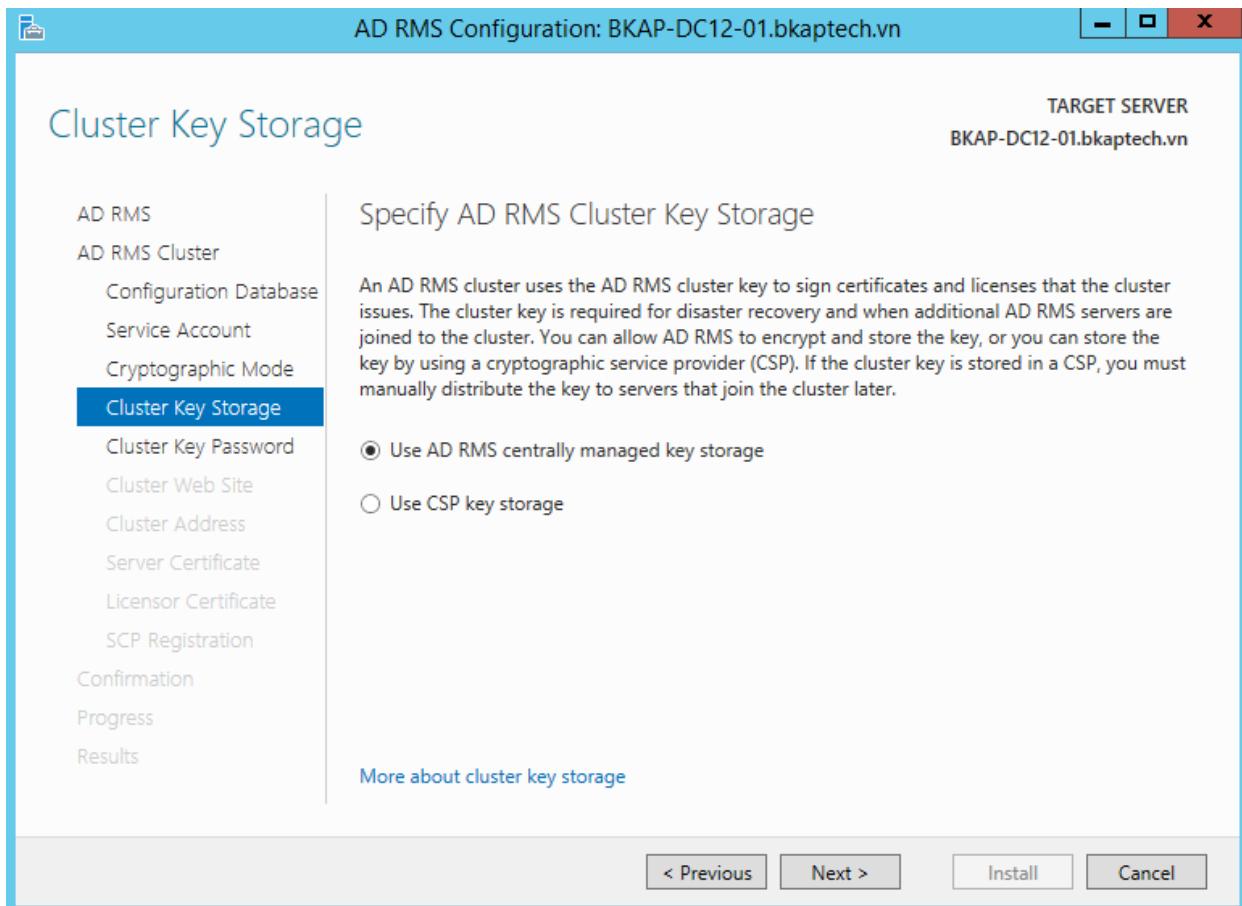
- Tại cửa sổ **Service Account**, click vào nút **Specify...** nhập vào user **bkaptech\rmssrvc** , sau đó click vào **Next**.



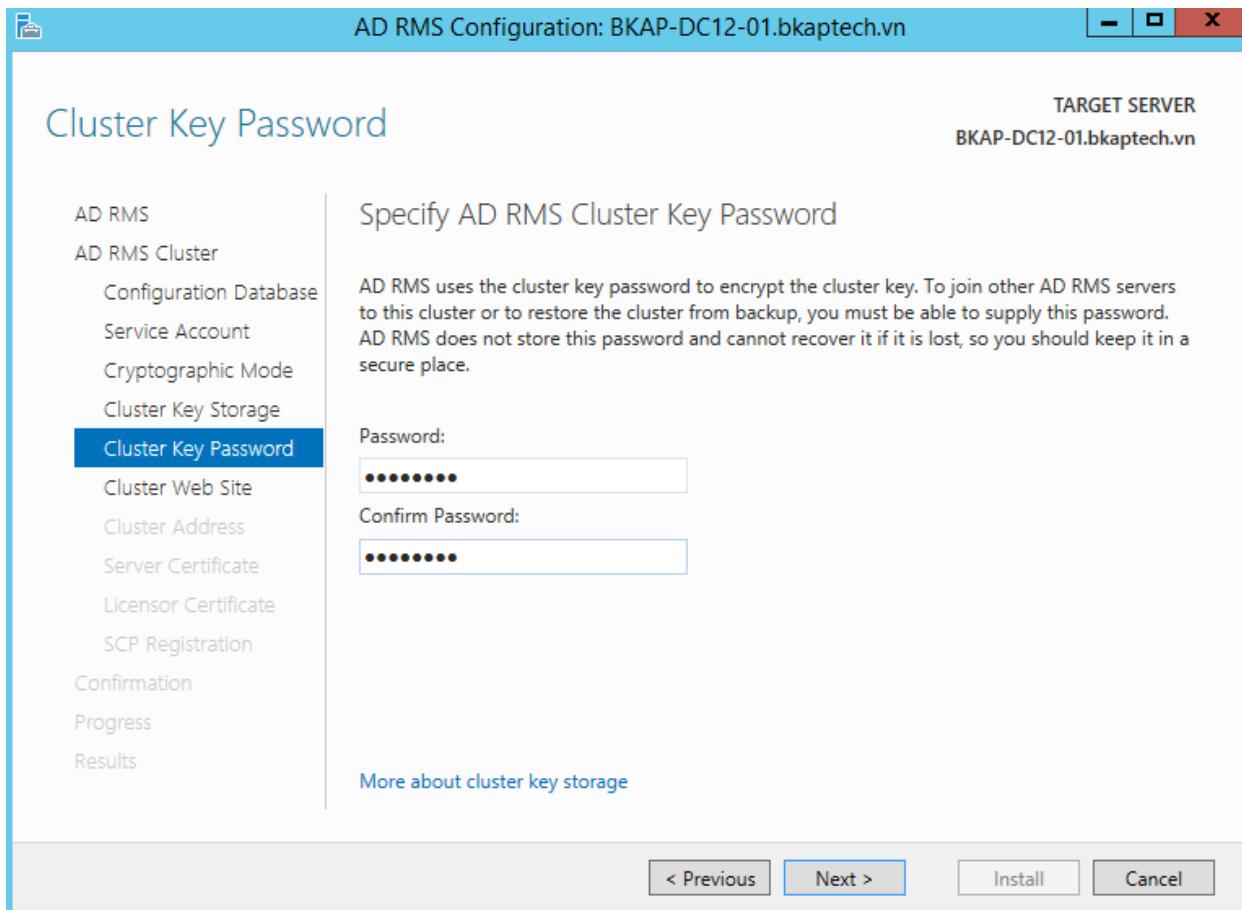
- Tại cửa sổ **Cryptographic Mode**, chọn vào **Cryptographic Mode 2 (RSA 2048-bit keys/SHA-256 hashes)**, sau đó click vào **Next**.



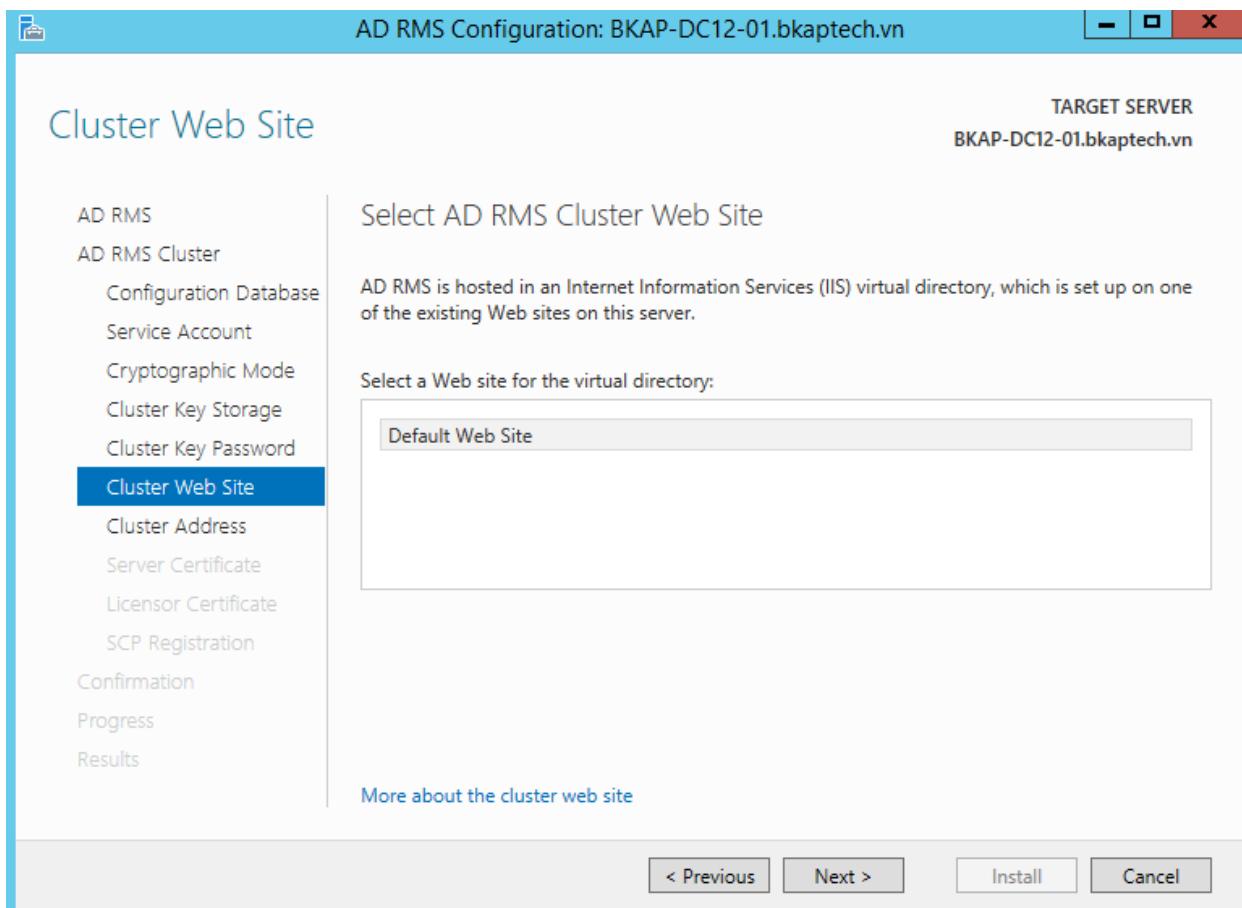
- Tại cửa sổ **Cluster Key Storage**, chọn vào **Use AD RMS centrally managed key storage**.



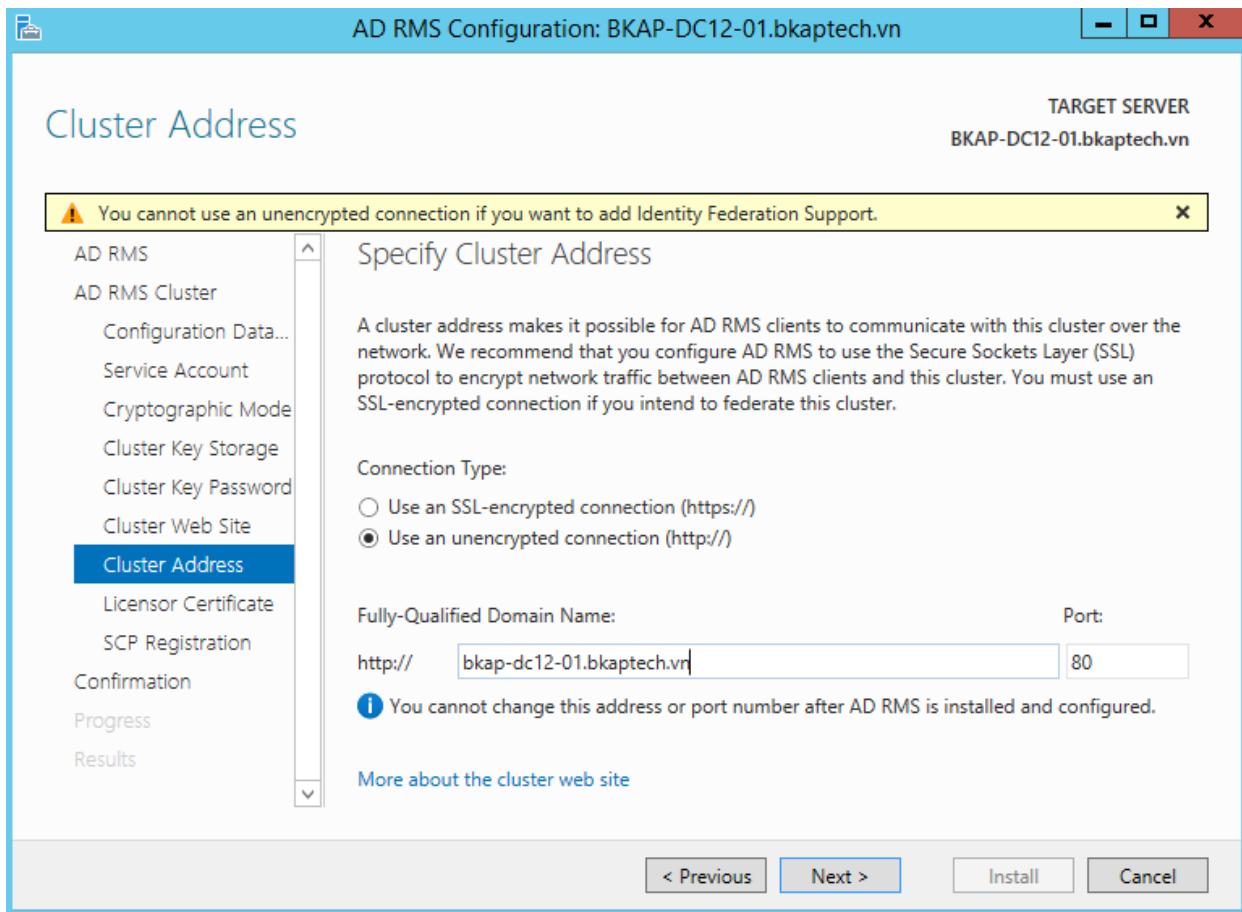
- Tại cửa sổ **Cluster Key Password**, nhập *password*:



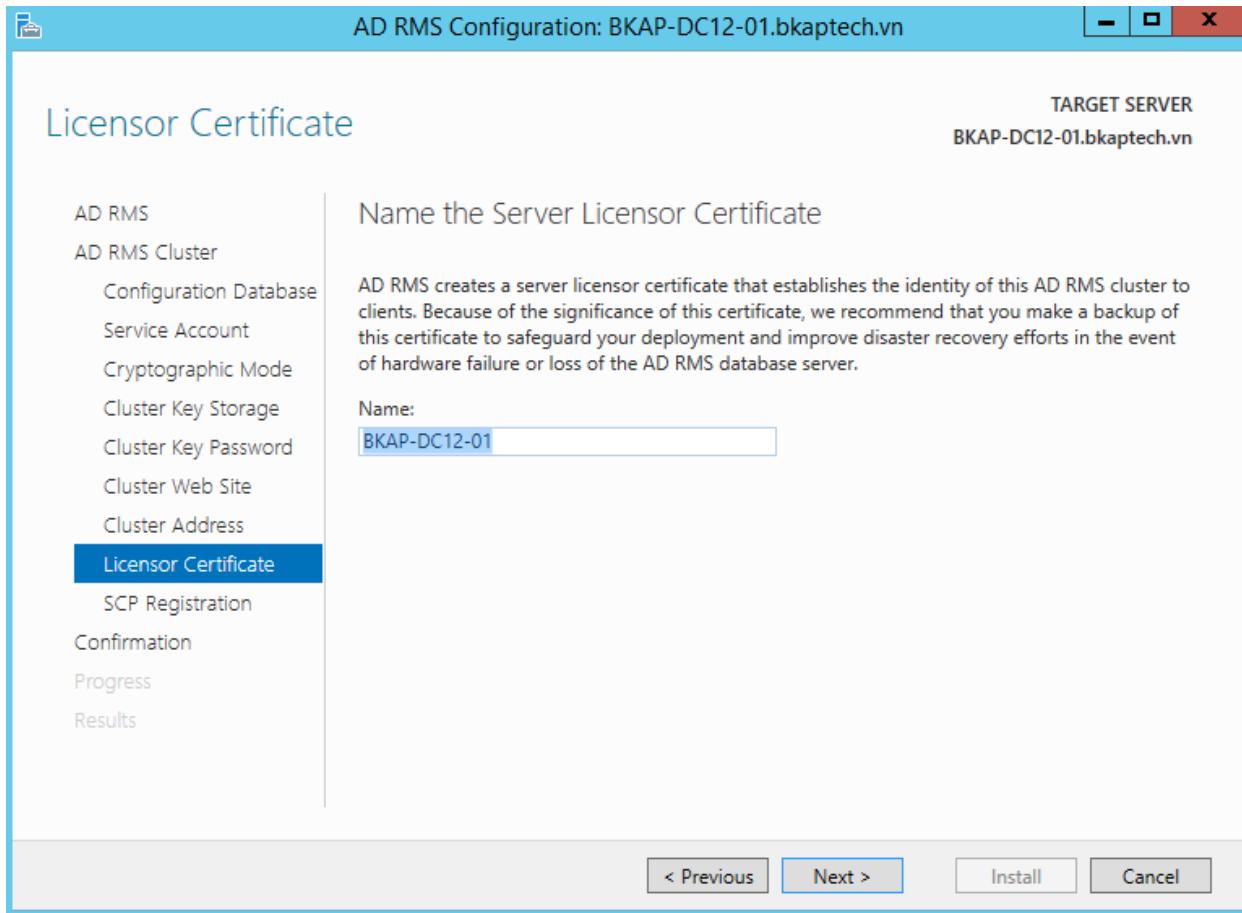
- Tại cửa sổ **Cluster Web Site**, click vào **Next**.



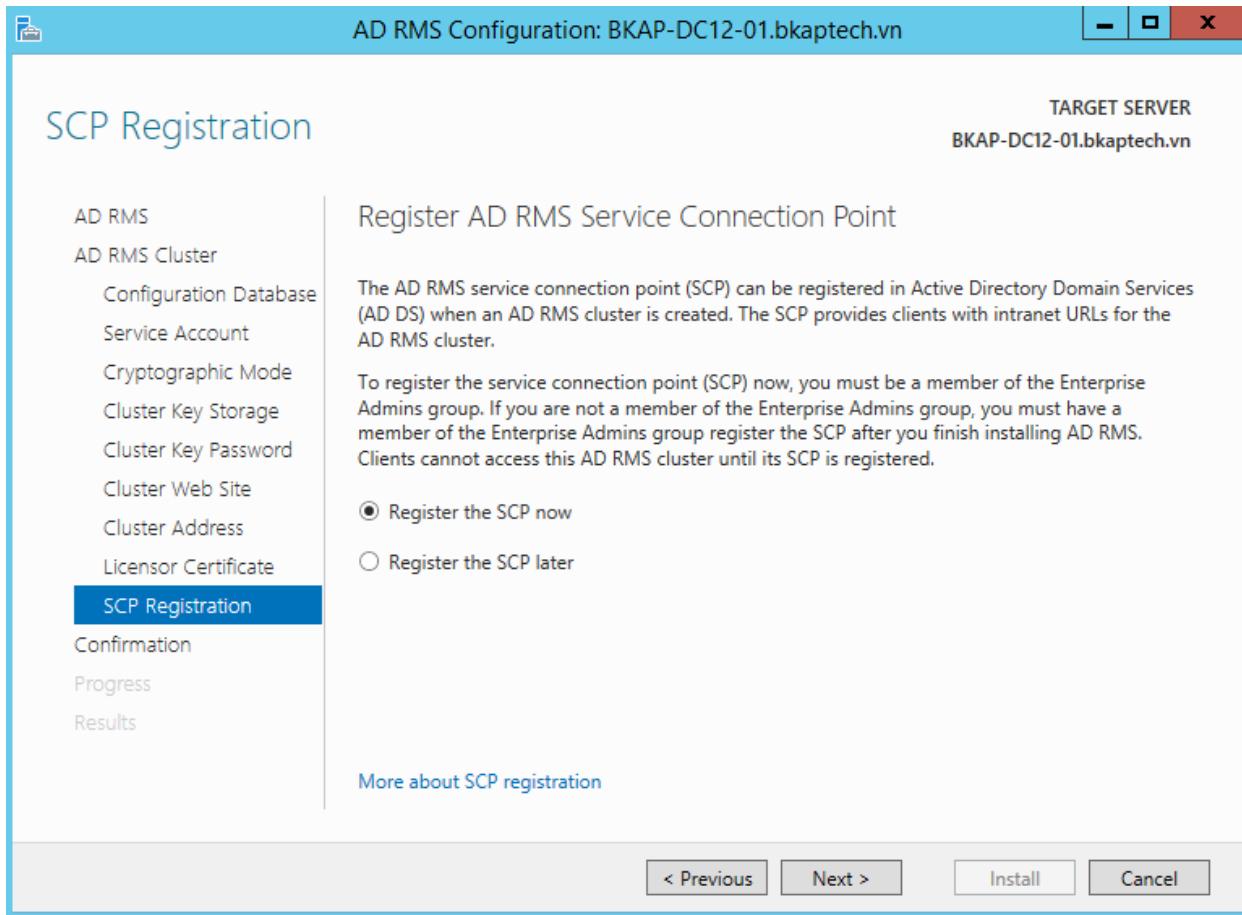
- Tại cửa sổ **Cluster Address**, tại mục **Connection Type**, chọn **Use an unencrypted connection (http://)** , tại mục **Fully-Qualified Domain Name** , nhập vào **bkap-dc12-01.bkaptech.vn**, sau đó click vào **Next**.



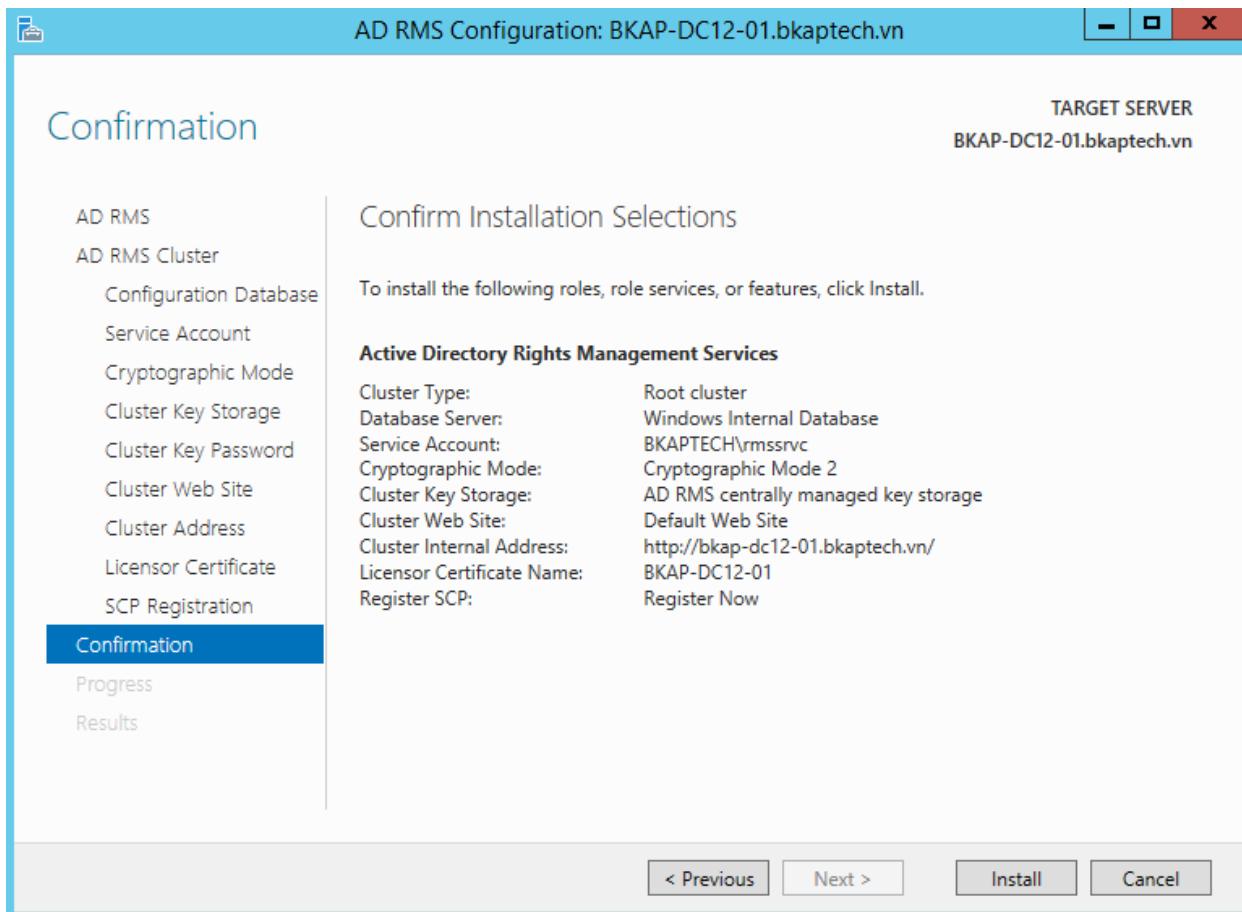
- Tại cửa sổ **Licensor Certificate**, kiểm tra tên tại mục Name phải là: **BKAP-DC12-01**, click vào **Next**.



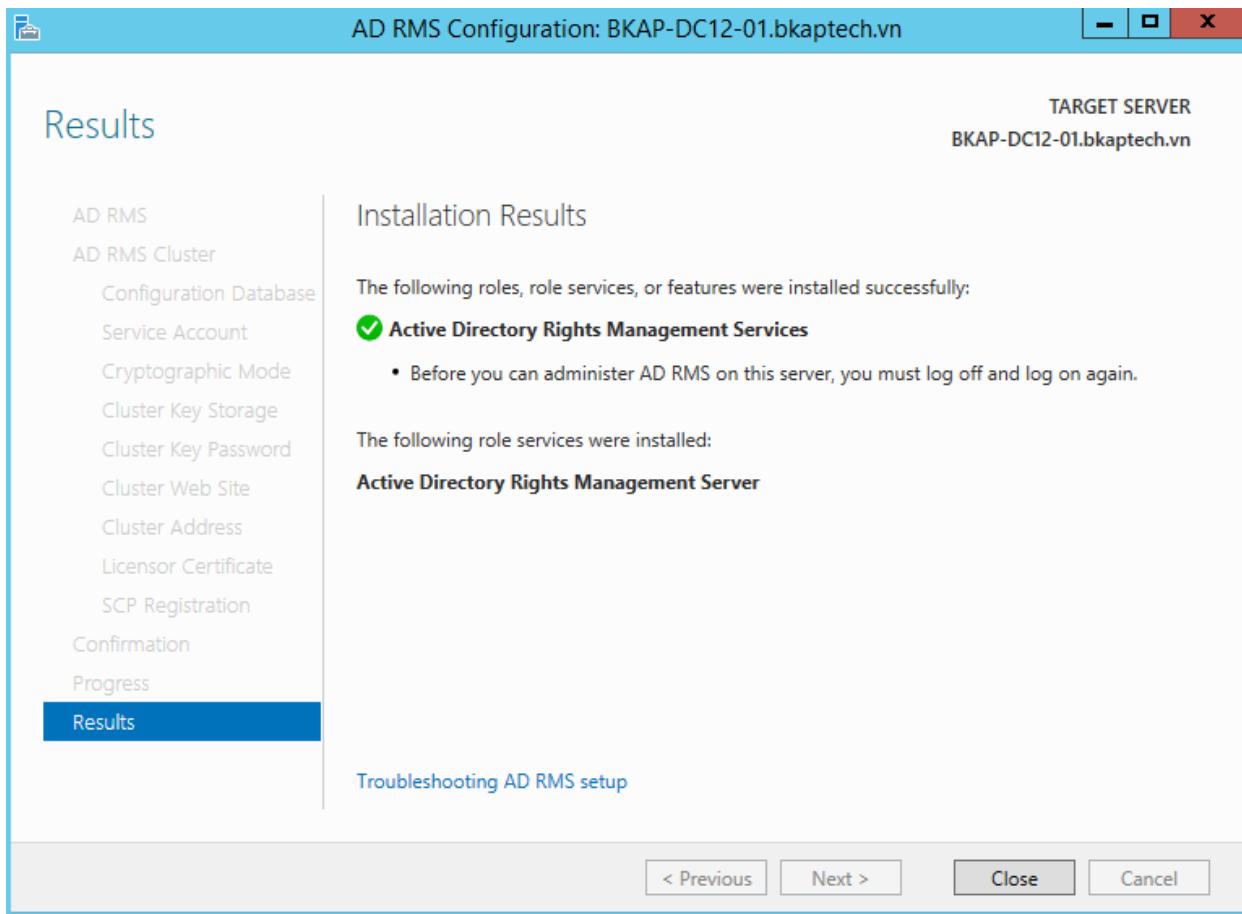
- Tại cửa sổ **SCP Registration**, chọn vào **Register the SCP now**, click vào **Next**.



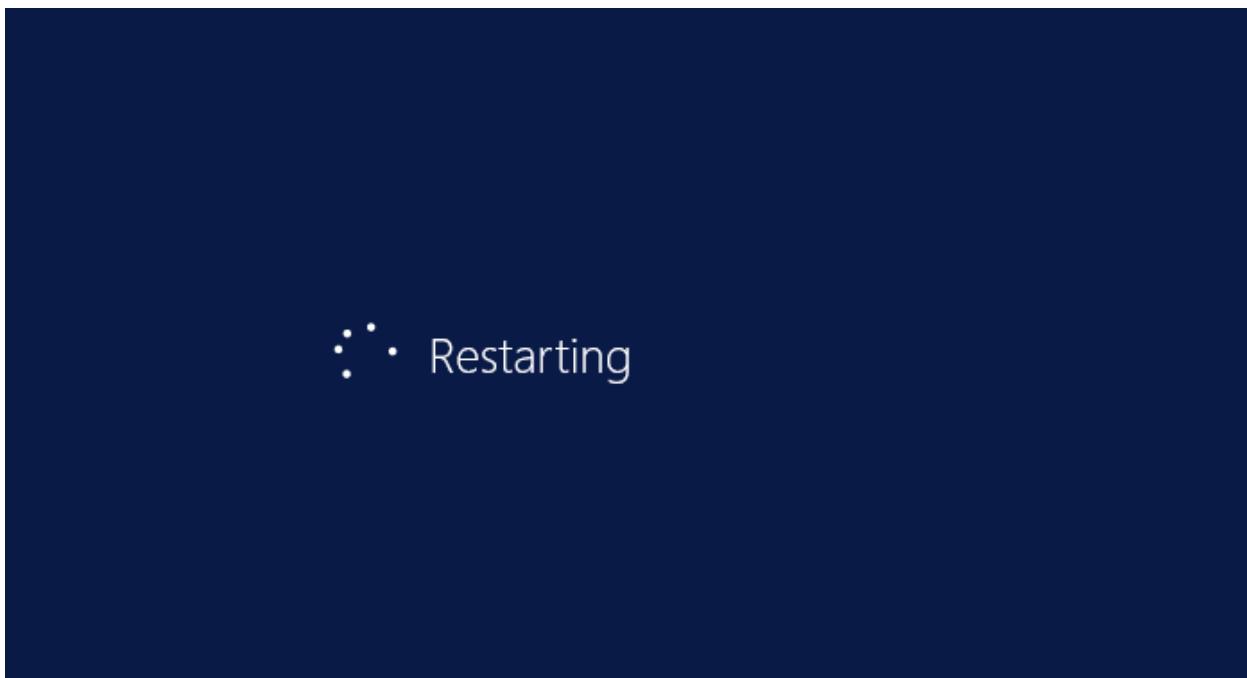
- Click **Install** để cài đặt dịch vụ:



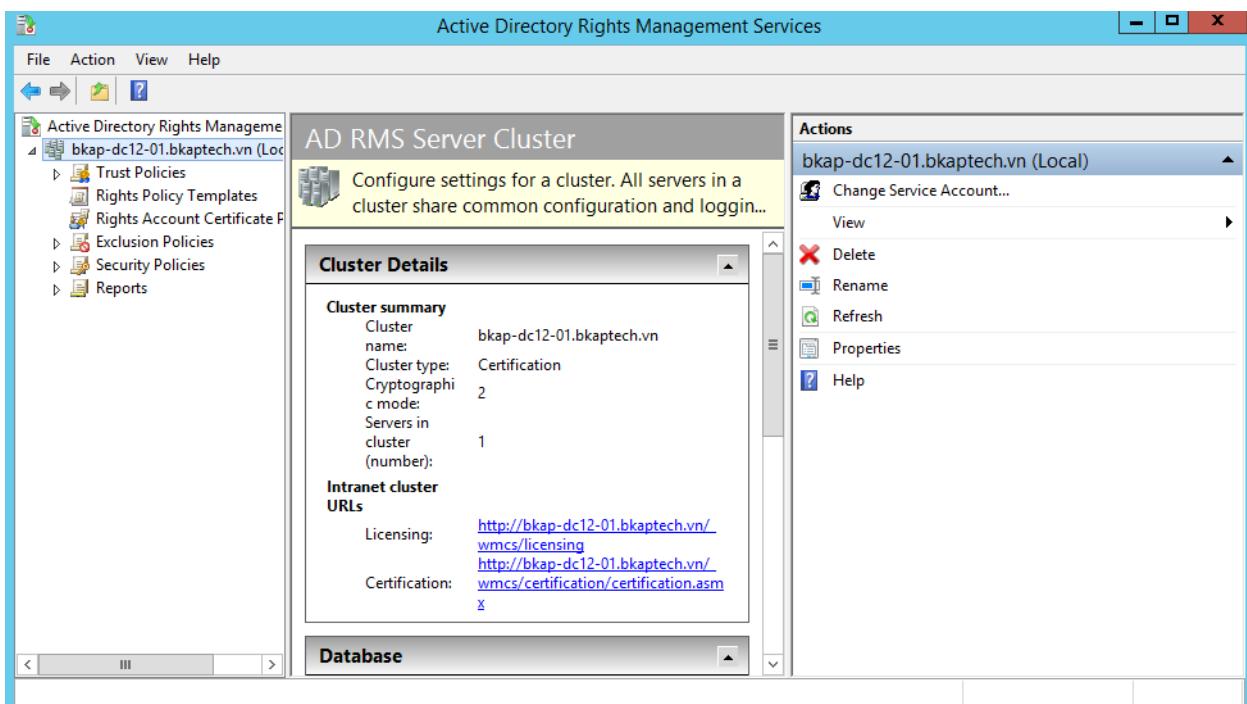
- Chờ đợi quá trình cài đặt kết thúc, click **Close** để kết thúc.



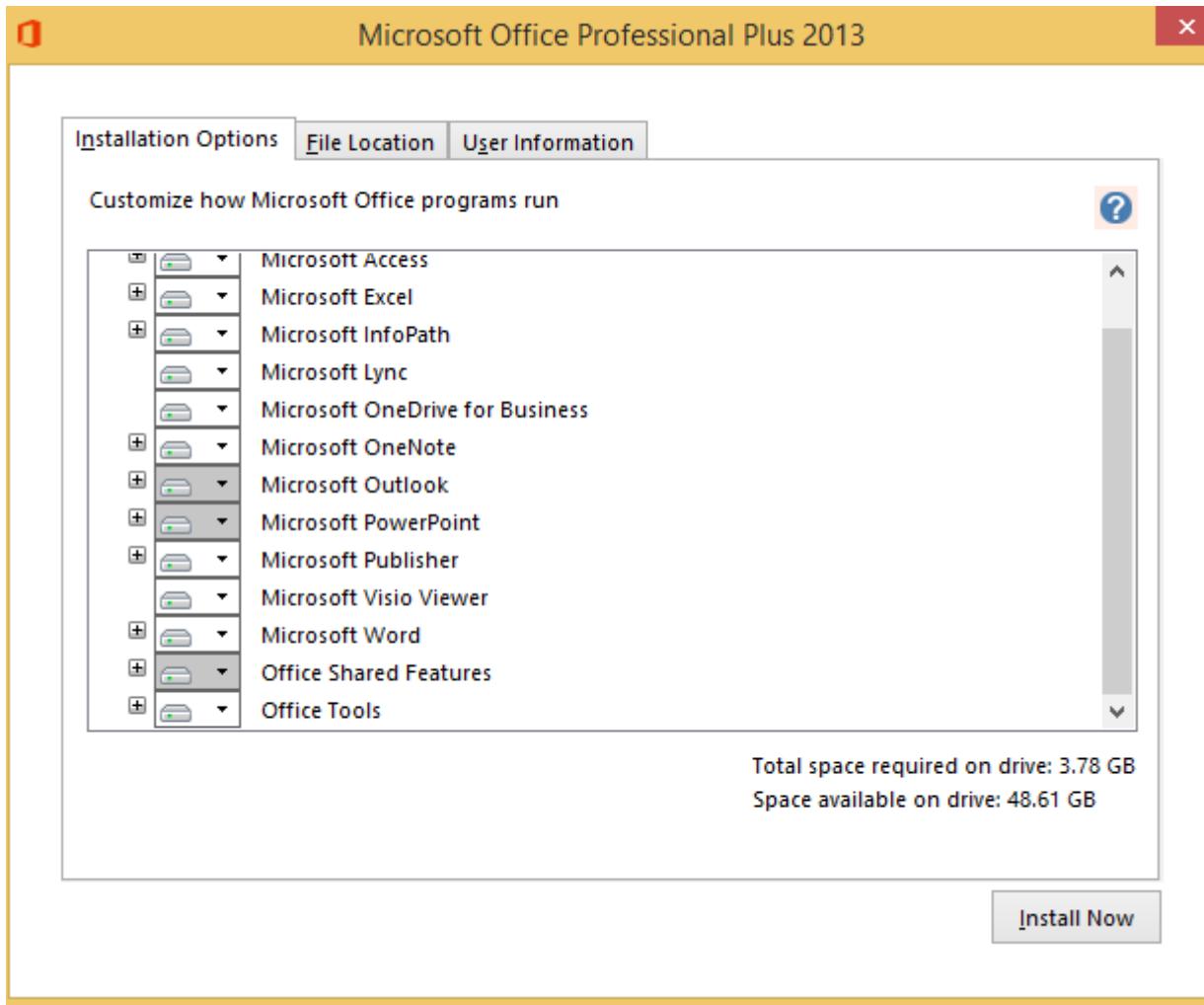
- Thực hiện **Restart** lại server.



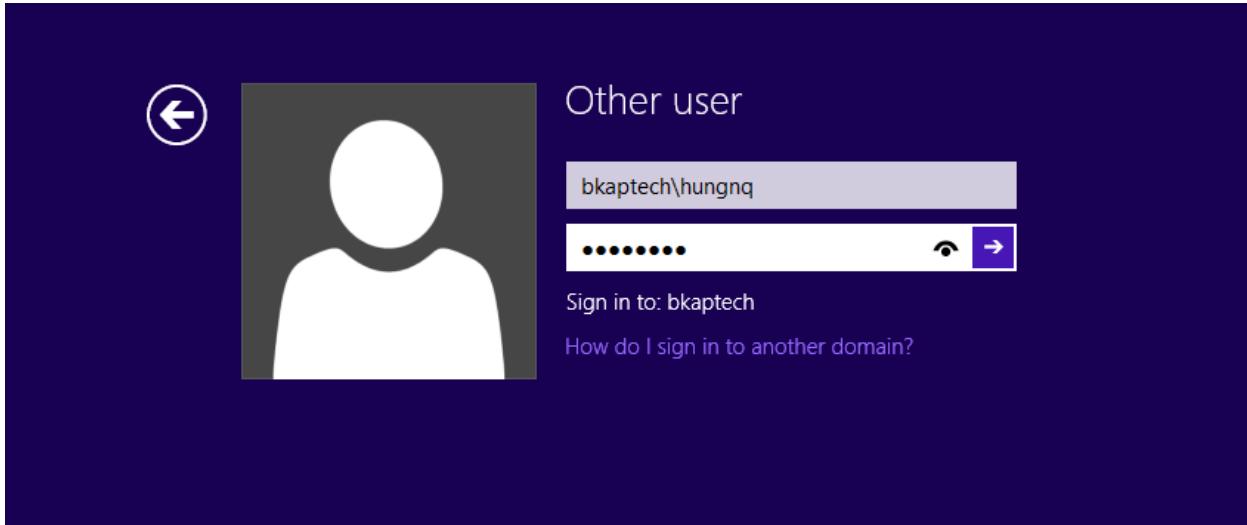
- Kiểm tra lại dịch vụ **AD RMS**.



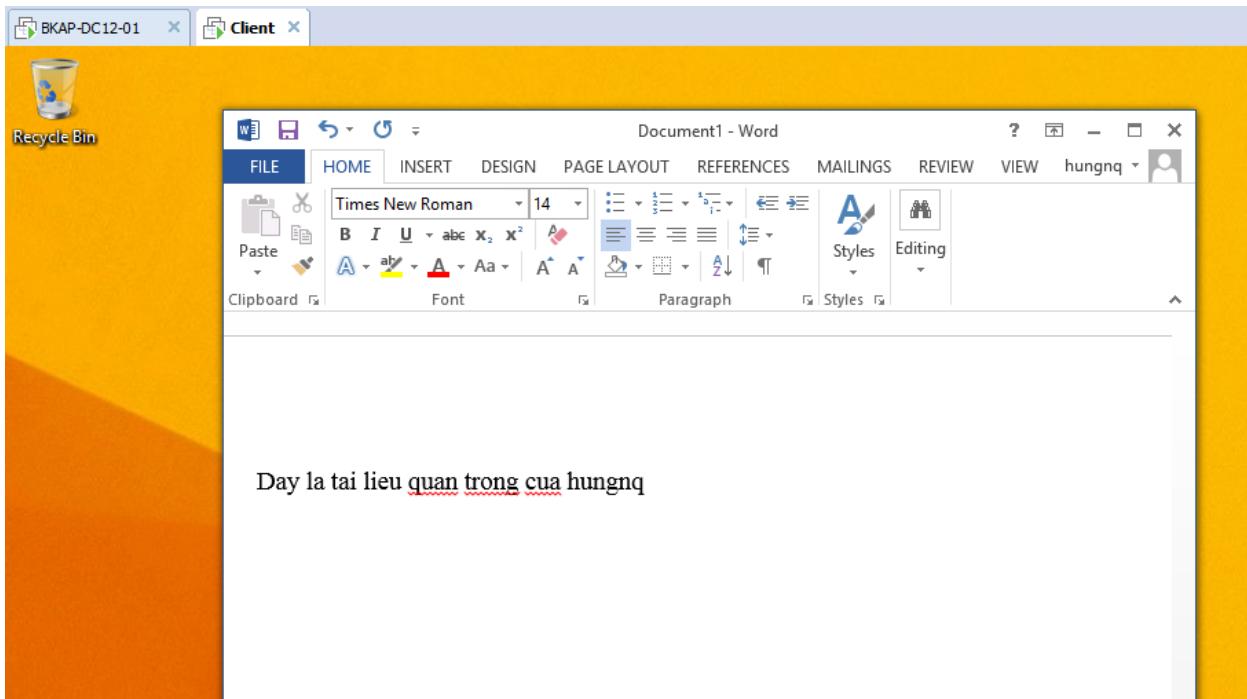
- Chuyển qua Client WRK08-01 thực hiện kiểm tra hoạt động của **AD RMS**.
 - Cài đặt phần mềm *Office 2013*:



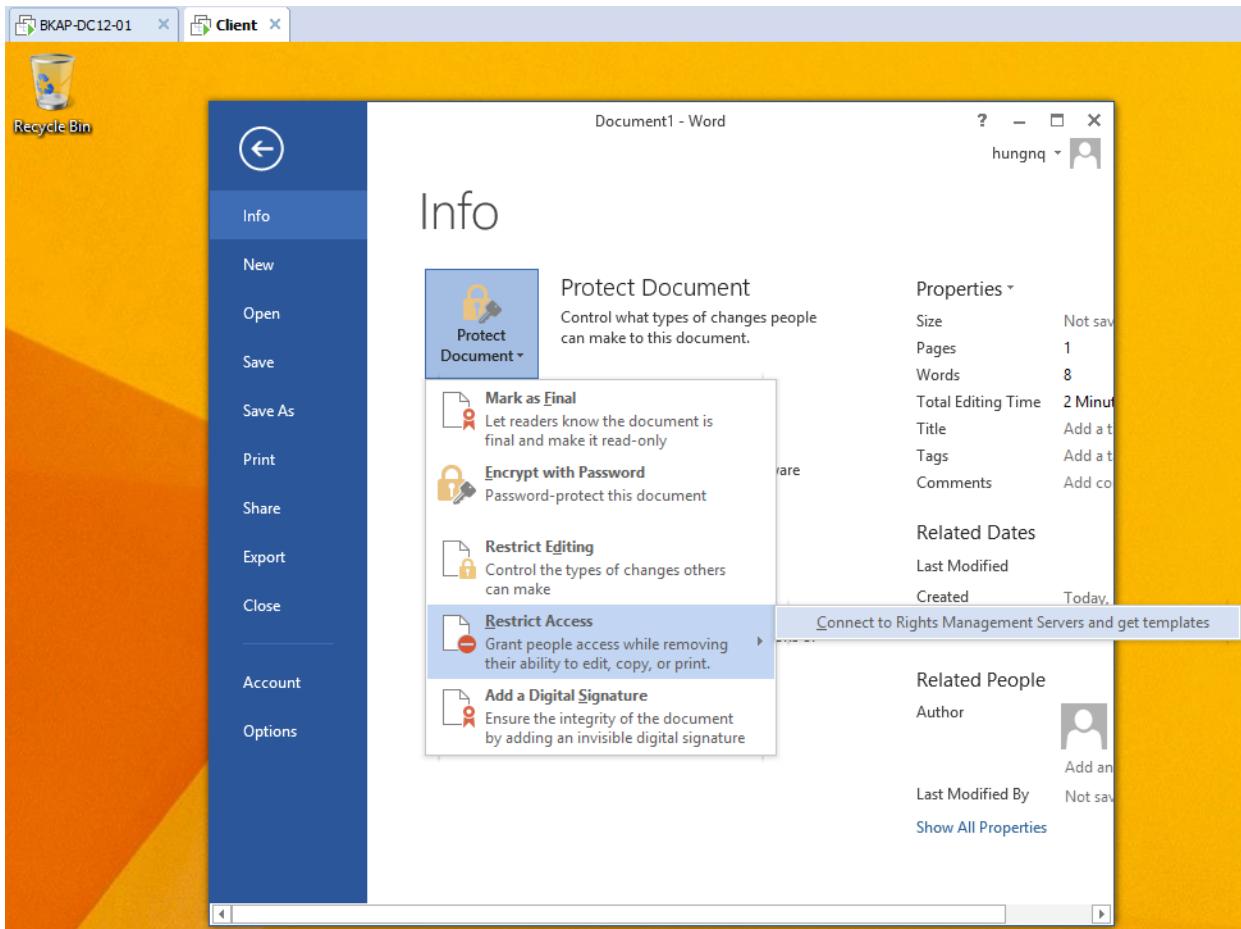
- Join Client vào Domain, đăng nhập bằng user **hungnq** trong group ITs.



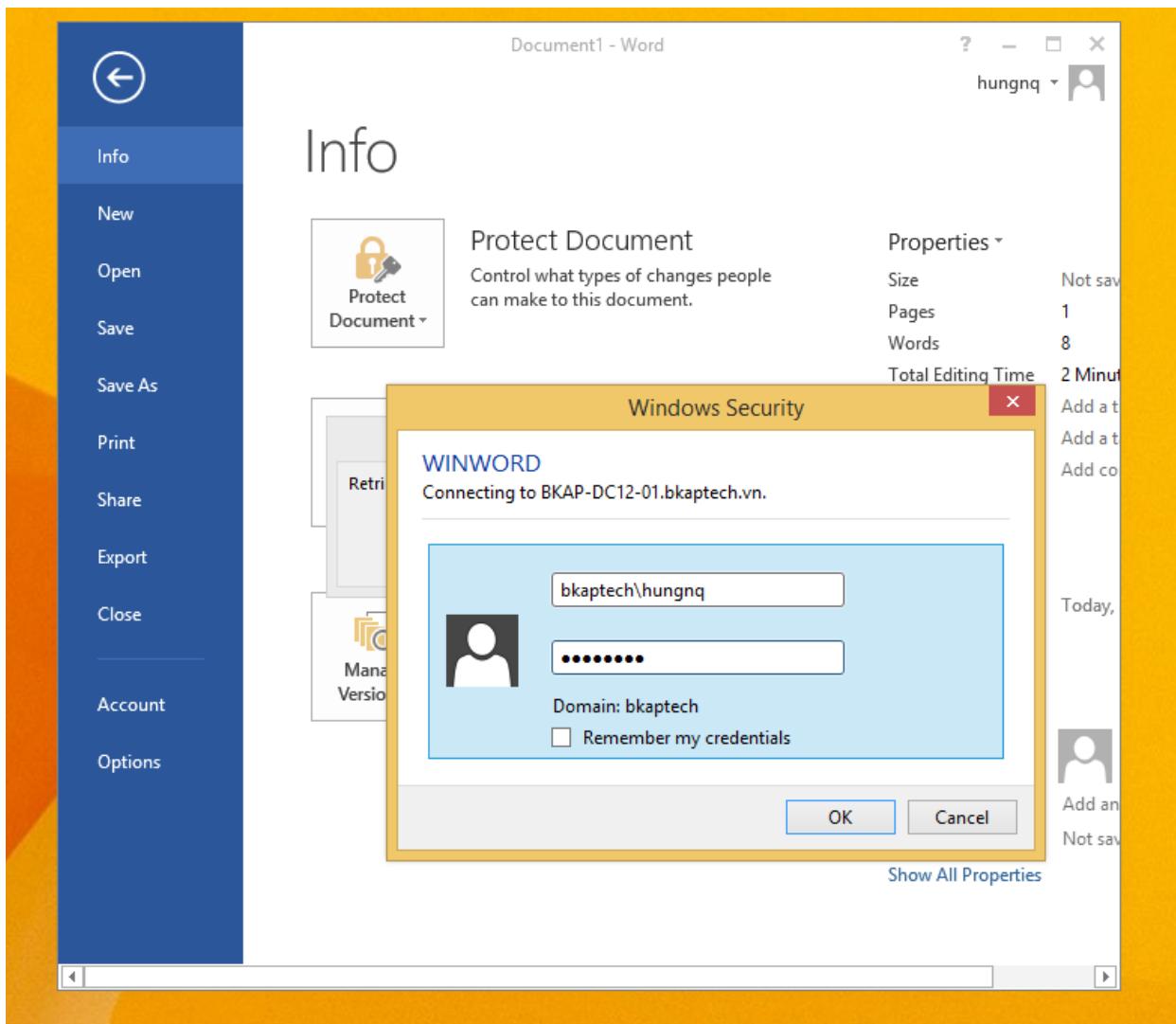
- Thực hiện soạn thảo 1 văn bản bất kì bằng Microsoft Word:



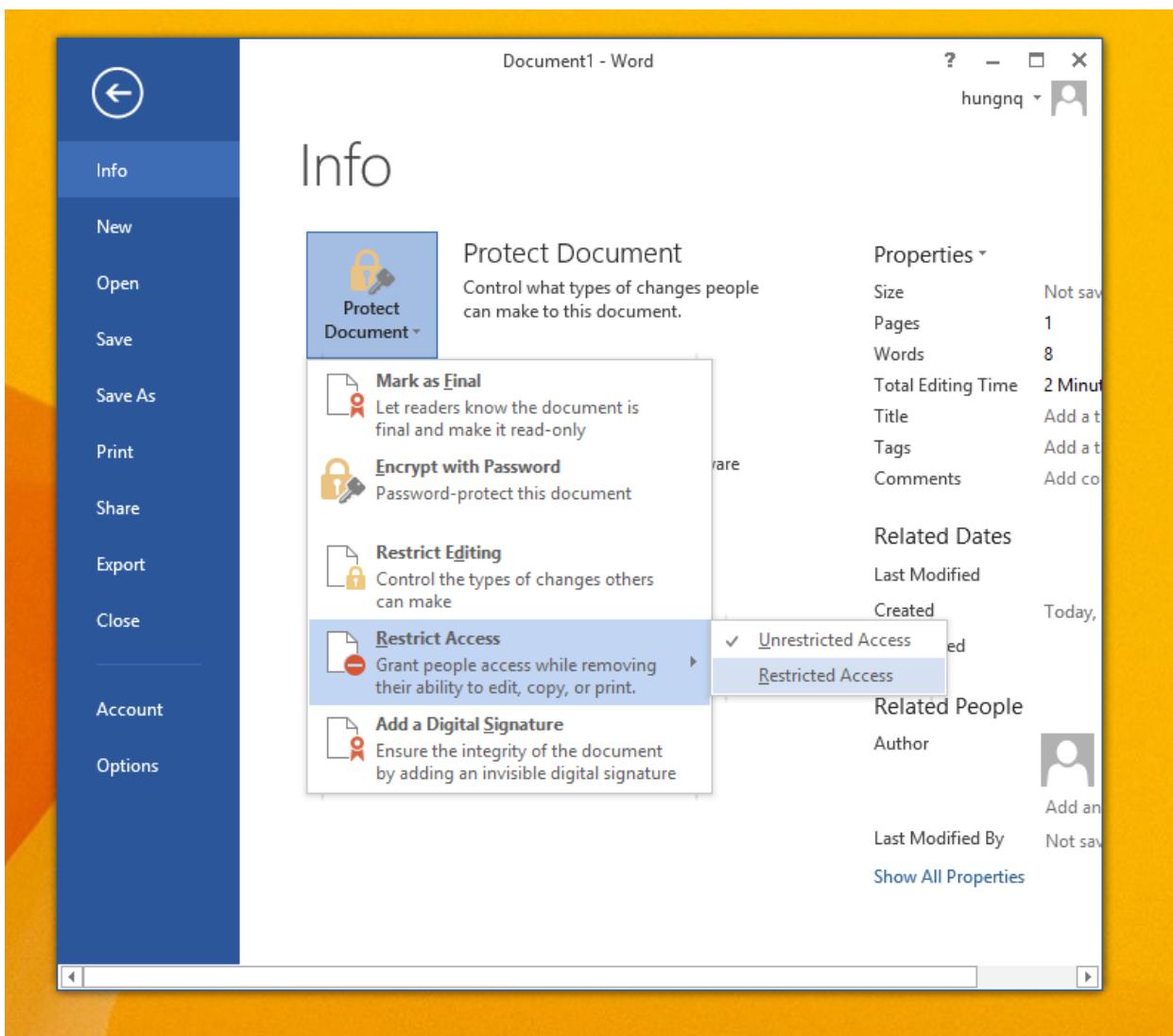
- Trong cửa sổ Word , chọn vào **File** , chọn vào **Info / Protect Document / Restrict Access / Connect to Rights Management Servers and get templates.**



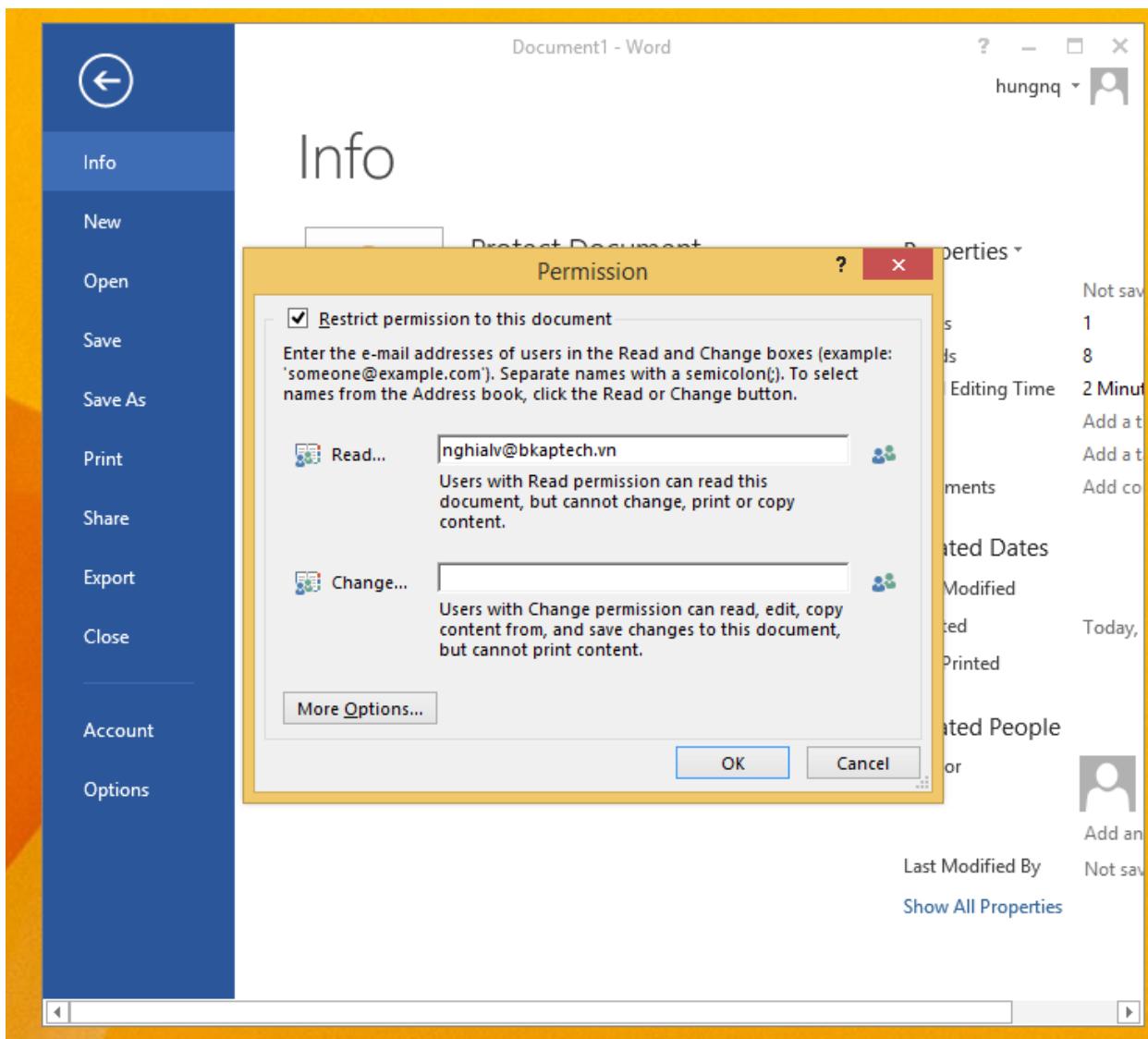
- Nhập vào user **hungnq**:



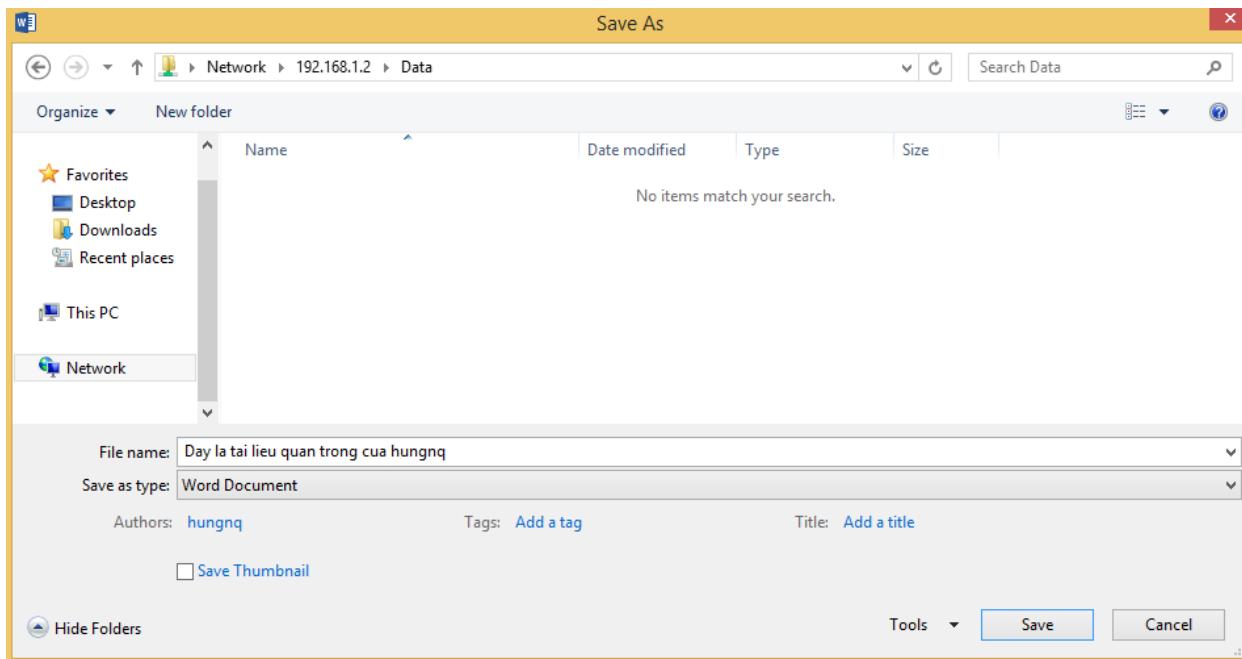
- Click chọn lại vào **Info / Restrict Access / => Restricted Access.**



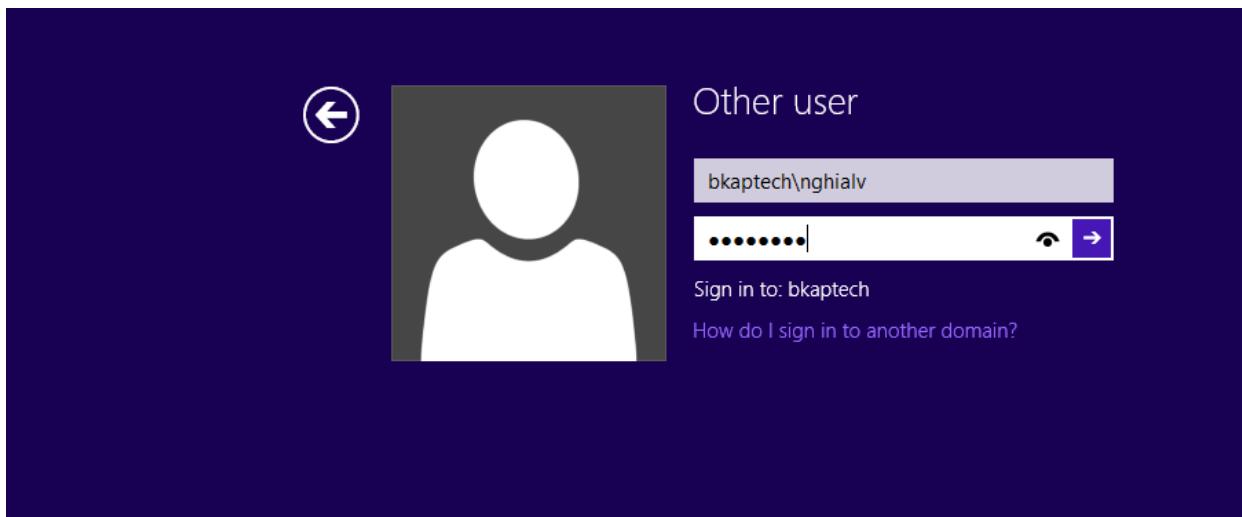
- Tại cửa sổ **Permission**, tích chọn vào **Restrict permission to this document**.
 - Tại quyền **Read...** nhập vào user nghialv trong group **ITs**.
 - **OK.**



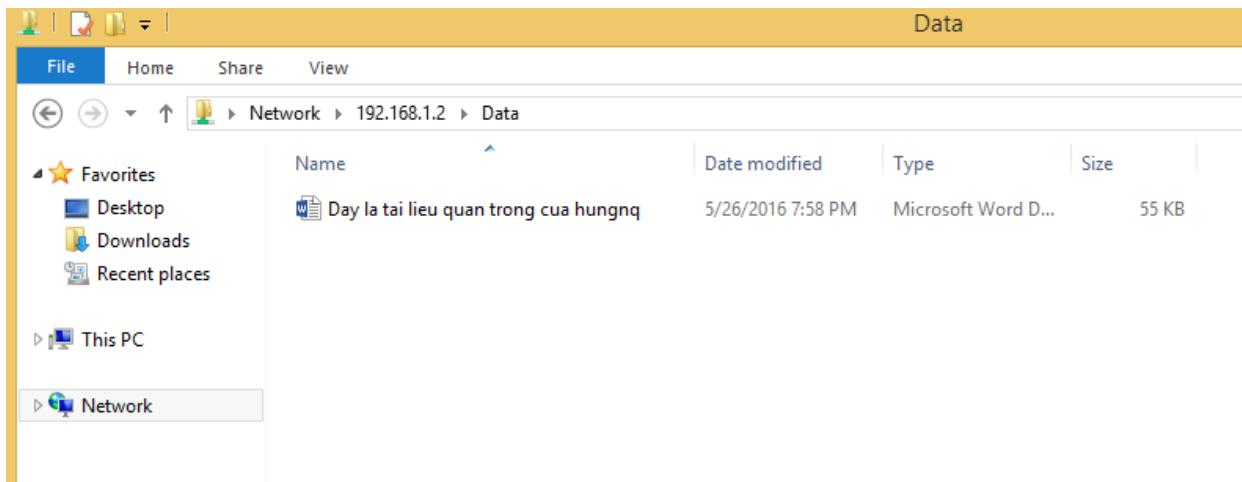
- **Save as file document** vừa tạo vào thư mục **Data** trên **DC12-01**:



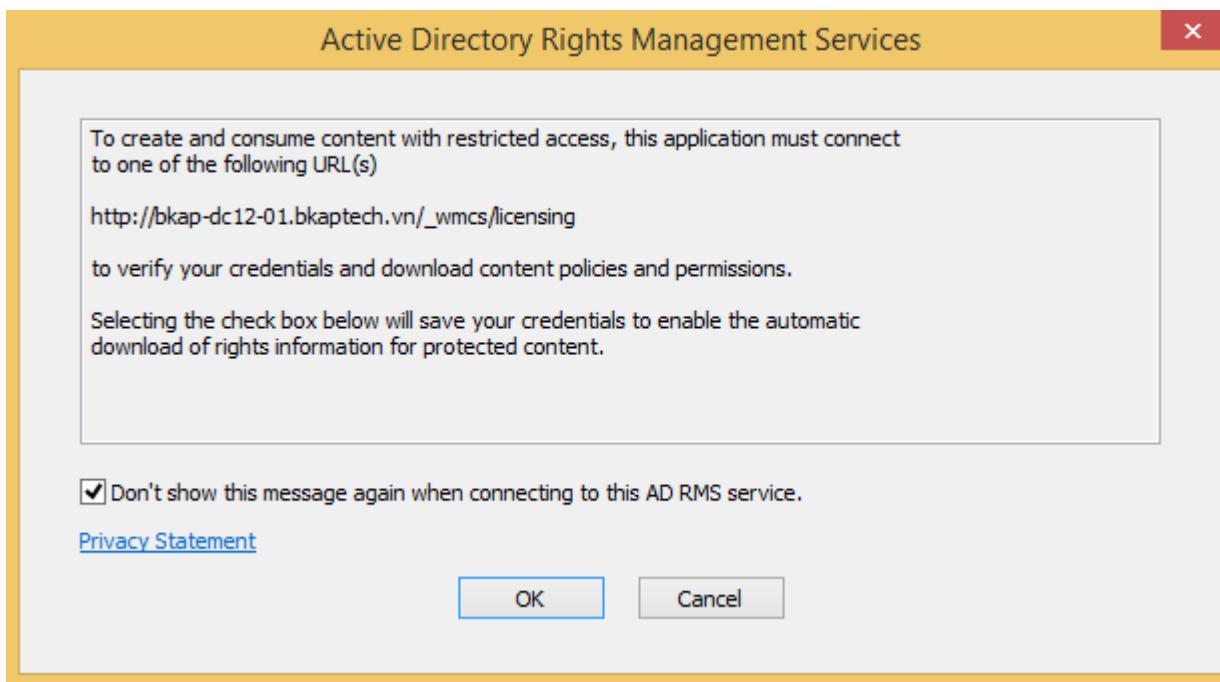
- Đăng nhập lại bằng tài khoản **nghialv** trong group **ITs** để kiểm tra.



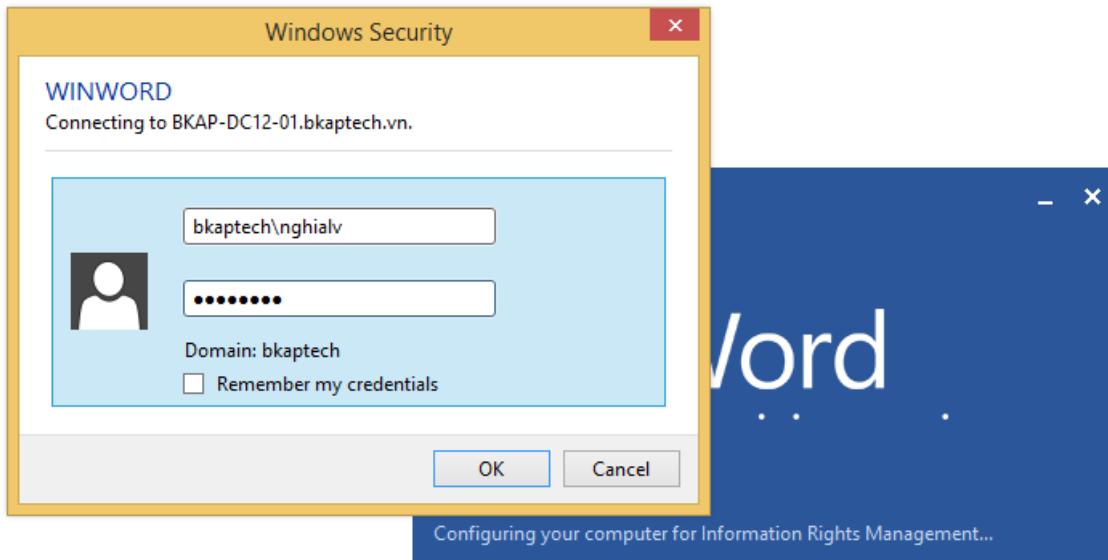
- Truy cập file *document* vừa lưu trong thư mục **Data** trên máy *DC12-01* để kiểm tra permission.



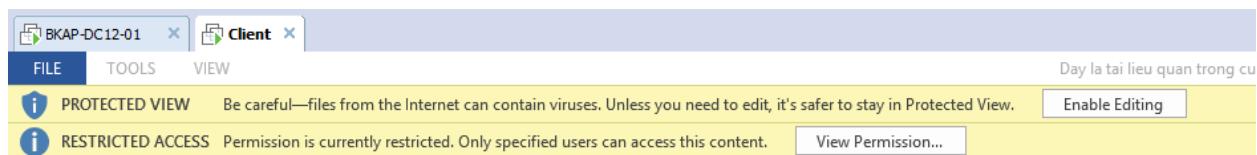
- Tại cửa sổ **Active Directory Rights Management Services**, click **OK**.



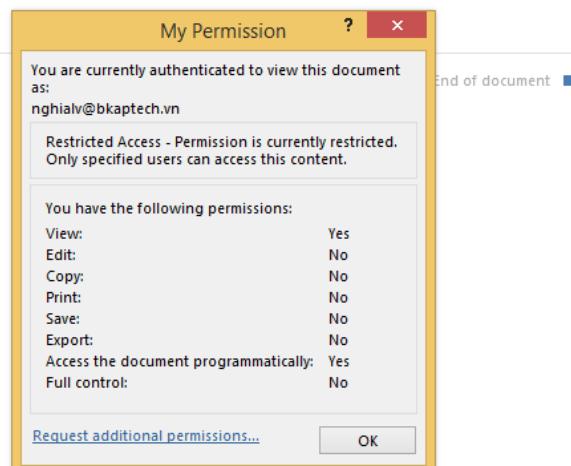
- Nhập vào user **nghialv**:



- Trong file Word vừa mở, click vào **View Permission**, theo dõi permission trong cửa sổ **My Permission**.

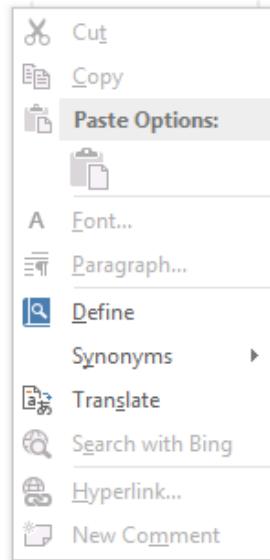


Day la tai lieu quan trong cua hungnq

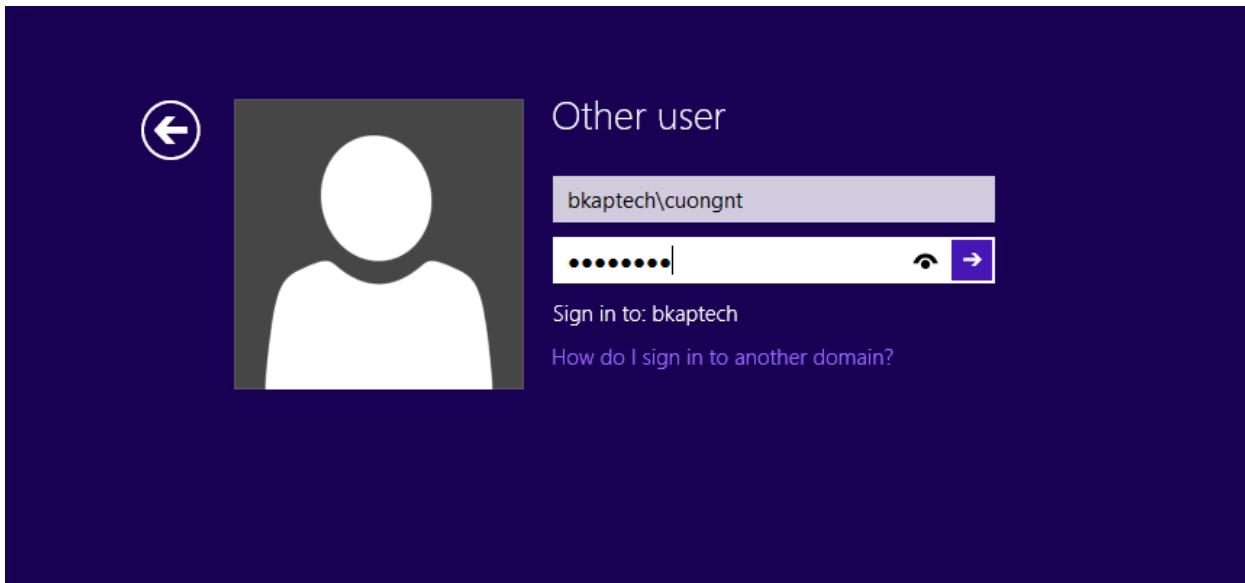


⇒ User nghialv ko có quyền **copy, chỉnh sửa tài liệu.**

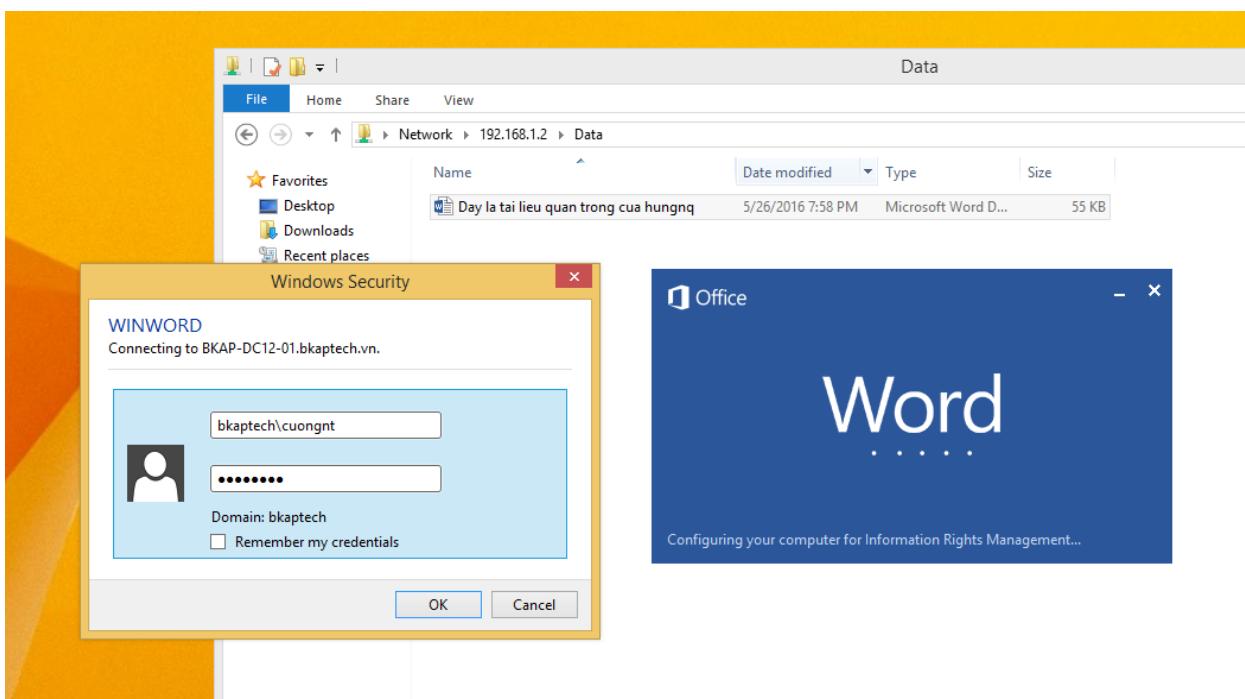
Day la tai lieu quan trong cua hungnq



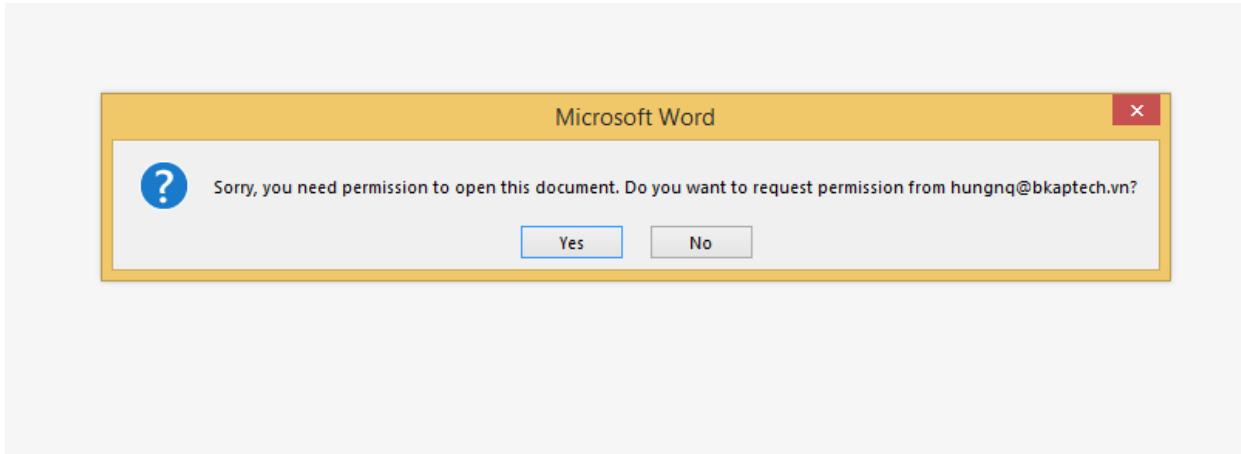
- Đăng nhập bằng user **cuongnt** trong group **Sales** để kiểm tra truy cập file *word* đã tạo bởi user **hungnq** trong group **ITs**.



- Truy cập file *word* đã được lưu trong thư mục **Data** trên máy *DC12-01*:



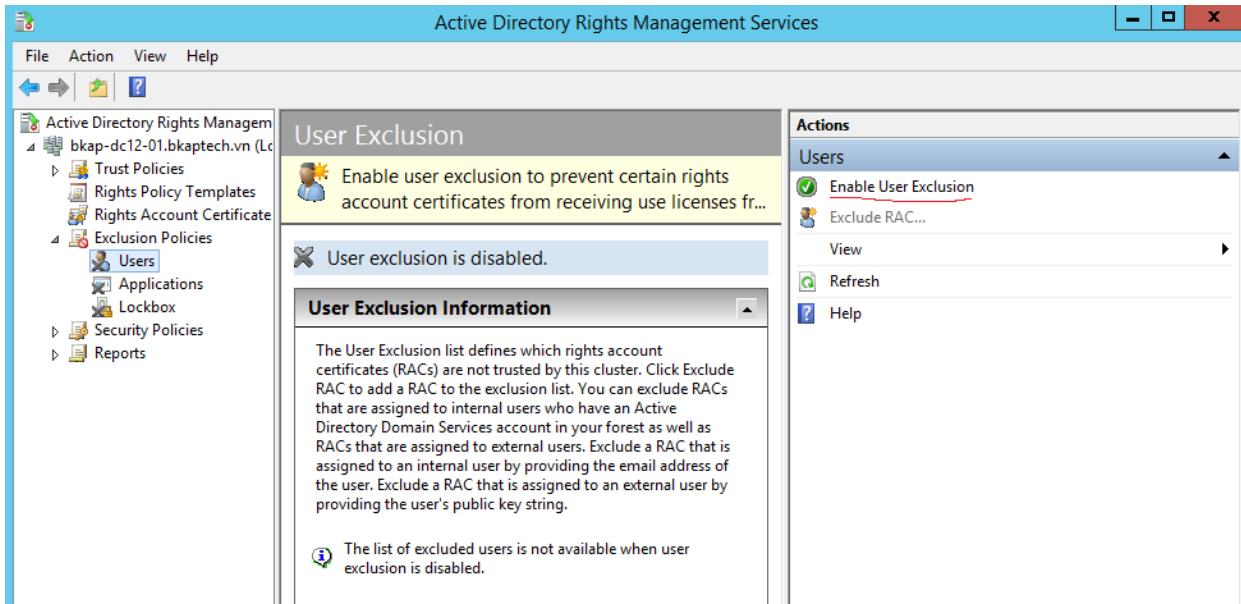
⇒ User cuongnt không được quyền truy cập vào file word này:



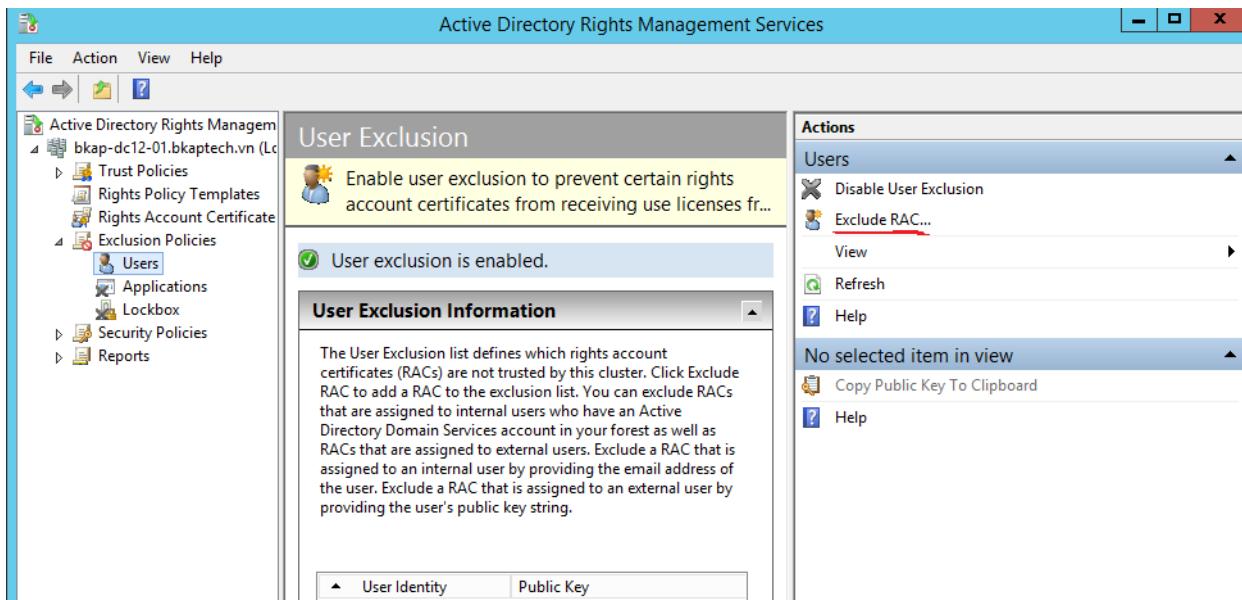
- Qua máy **DC12-01**, thực hiện cấu hình **RAC (Rights Account Certificate)** và **User Exclusion Policy**.

Ngoài việc người dùng có thể phân quyền trên tài liệu của mình, **RMS** cho phép dùng **RAC** và **User Exclusion Policy** để loại trừ quyền truy cập của người dùng chỉ định.

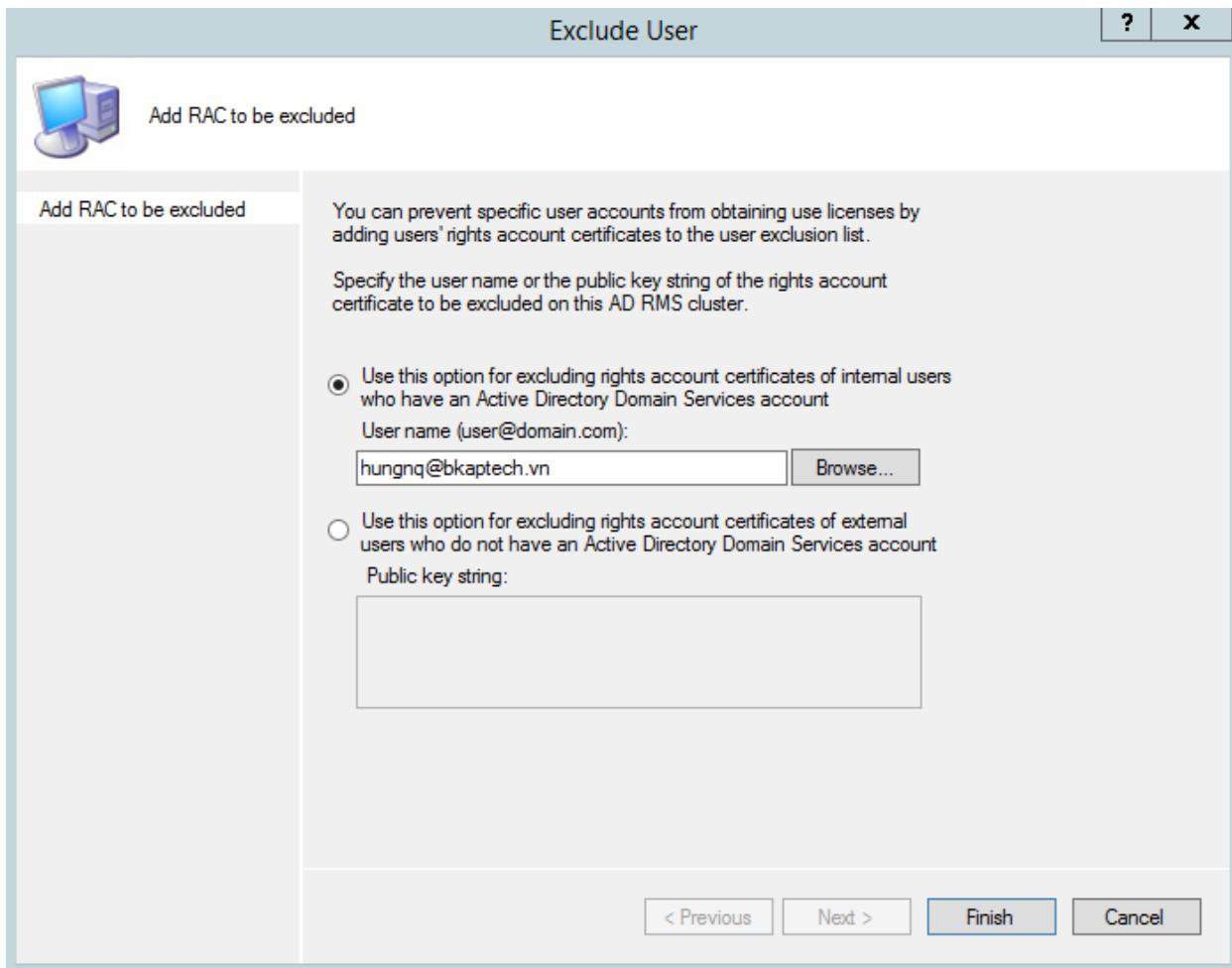
- Trong **AD RMS**, chọn **Exclusion Policies / Users**, click vào **Enable User Exclusion**.



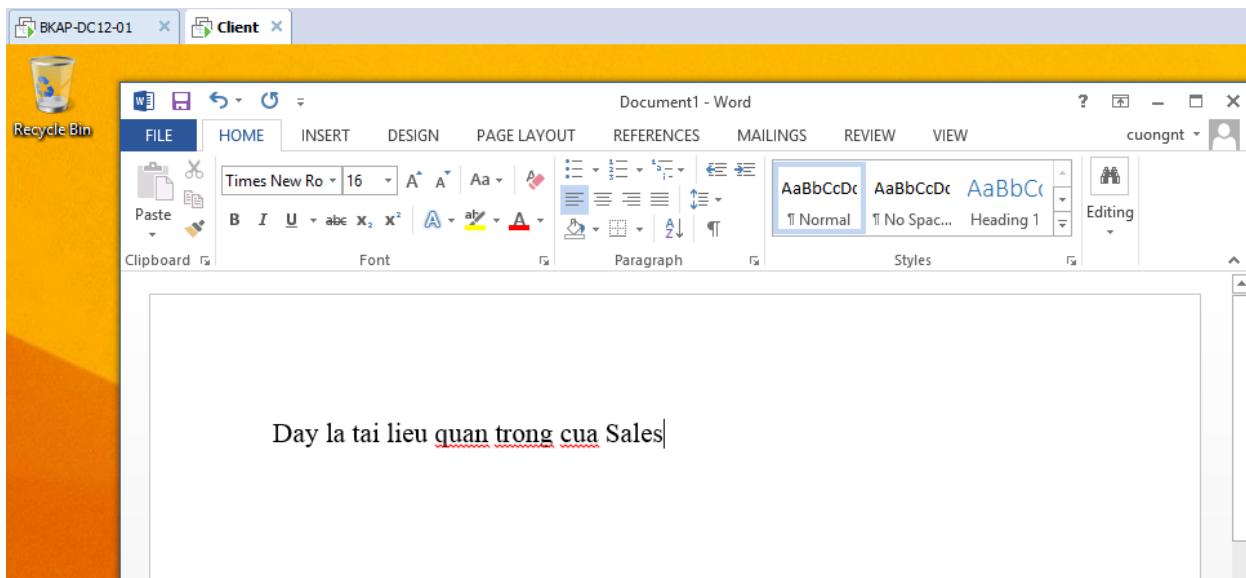
- Click vào **Exclude RAC**.



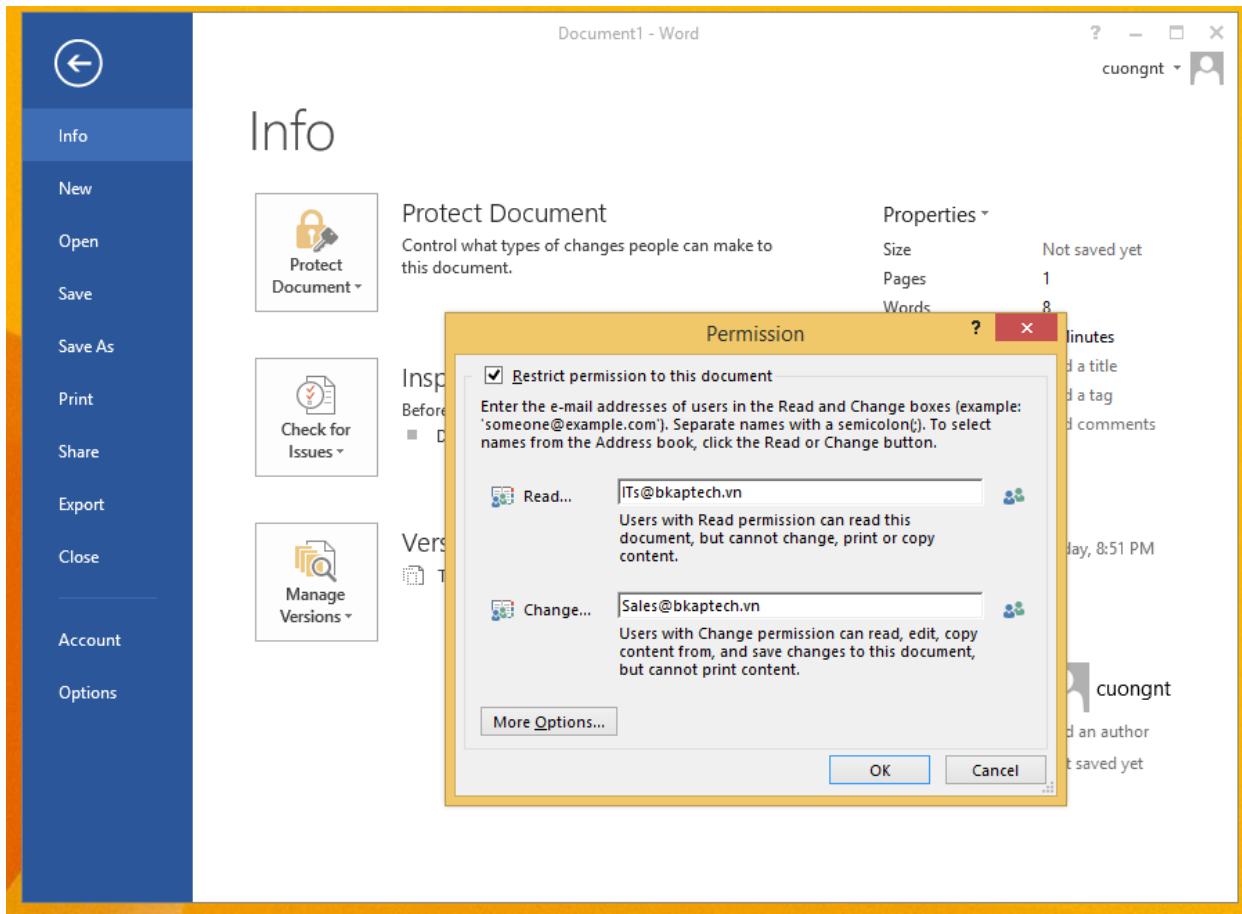
- Trong cửa sổ **Exclude User**, chọn vào *Use this option for excluding rights account certificates of internal..*
 - Nhập vào user hungnq@bkaptech.vn , click vào **Finish**.



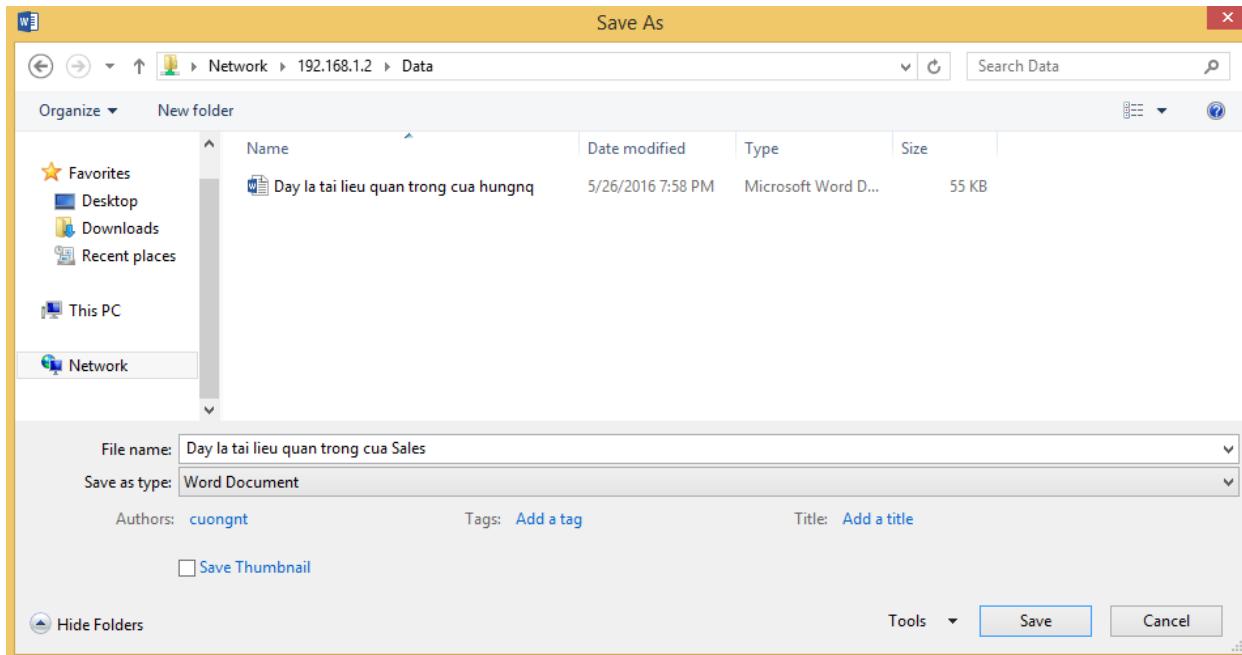
- Chuyển sang *Client*, đăng nhập user **cuongnt** trong group **Sales**.
 - Tạo 1 văn bản mới.



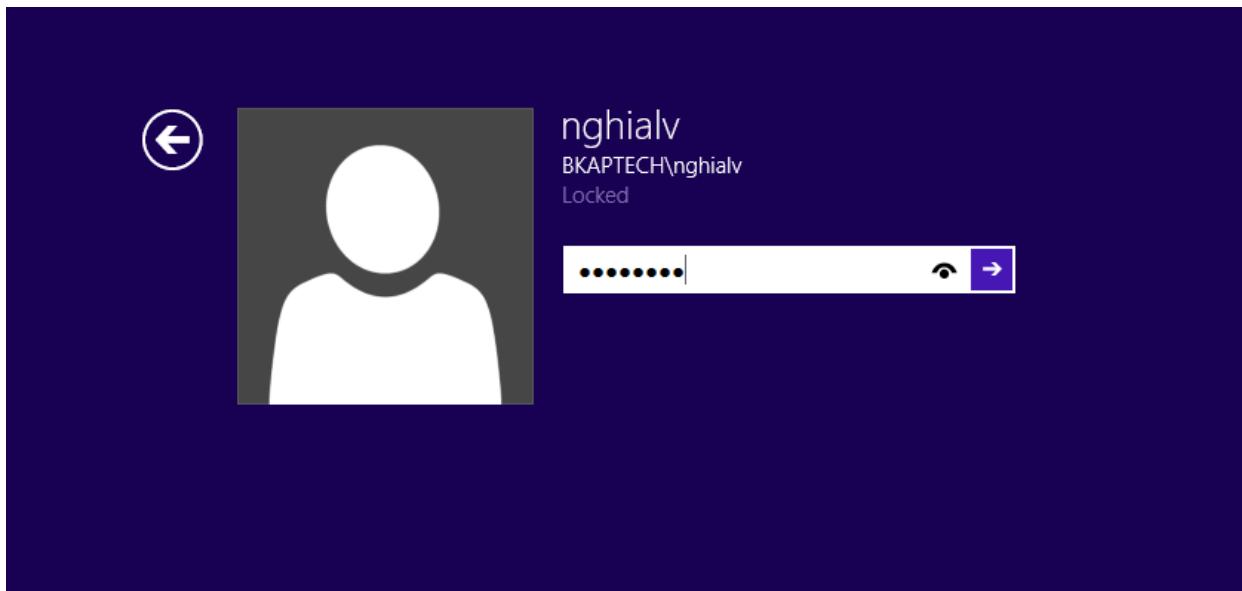
- Chọn vào **Restrict Permission / Restricted Access** (*tương tự như trên*).
 - Trong cửa sổ **Permission**, tích chọn vào **Restrict permission to this document**.
 - Trong khung **Read...** nhập vào mail **ITs@bkaptech.vn**
 - Trong khung **Change...** nhập vào mail **Sales@bkaptech.vn**



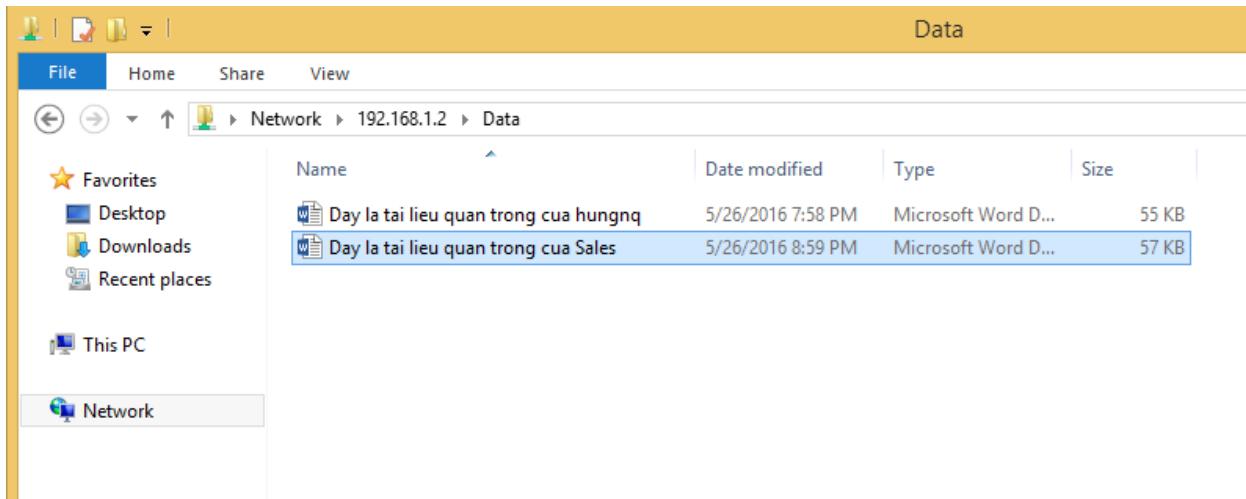
- Lưu file này vào thư mục **Data** trên máy *DC12-01*:



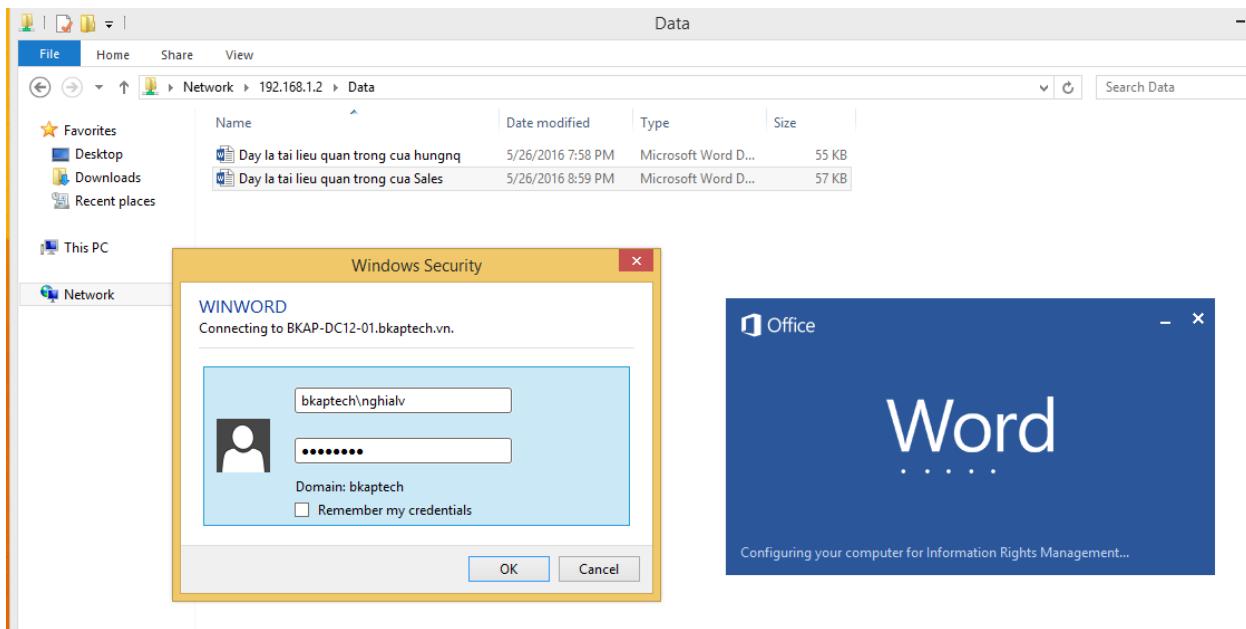
- Đăng nhập lại bằng user **nghialv** thuộc group **ITs** để kiểm tra.



- Truy cập thư mục **Data** trên máy *DC12-01*, mở file *Document* vừa được tạo bởi user **cuongnt**.



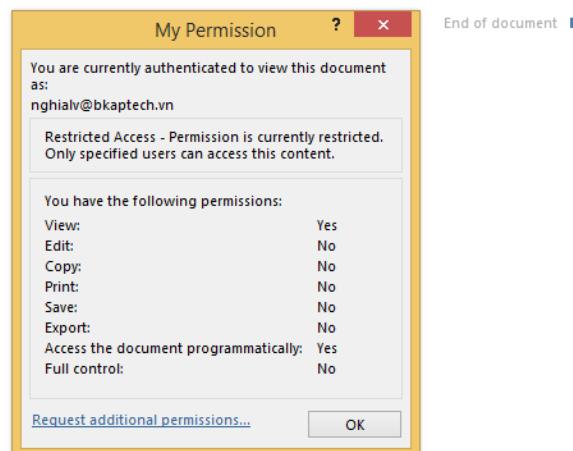
- Nhập vào user **nghialv**.



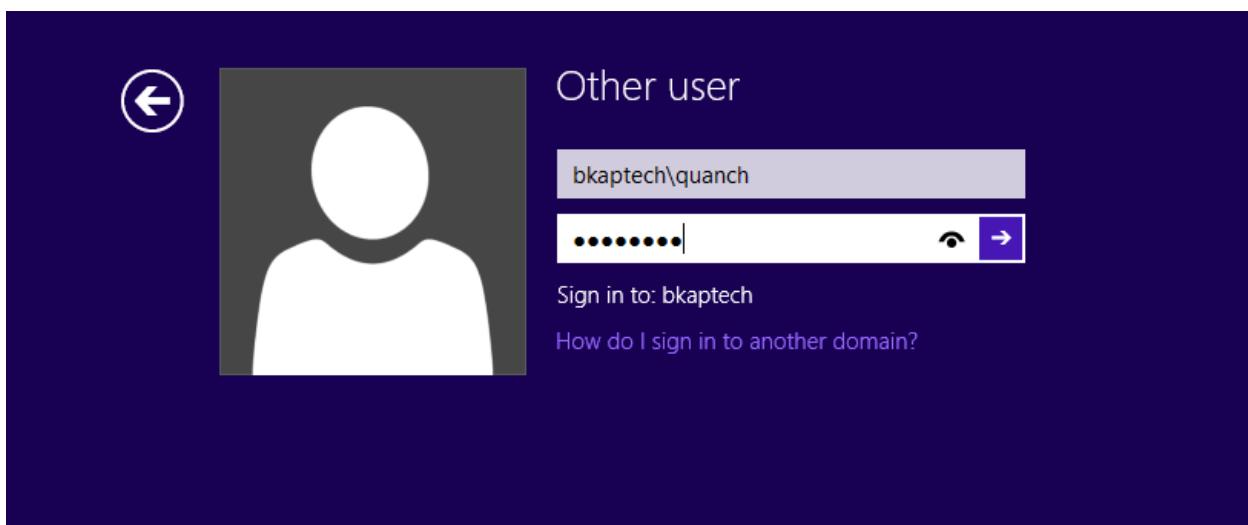
⇒ User **nghialv** chỉ được quyền xem tài liệu này.



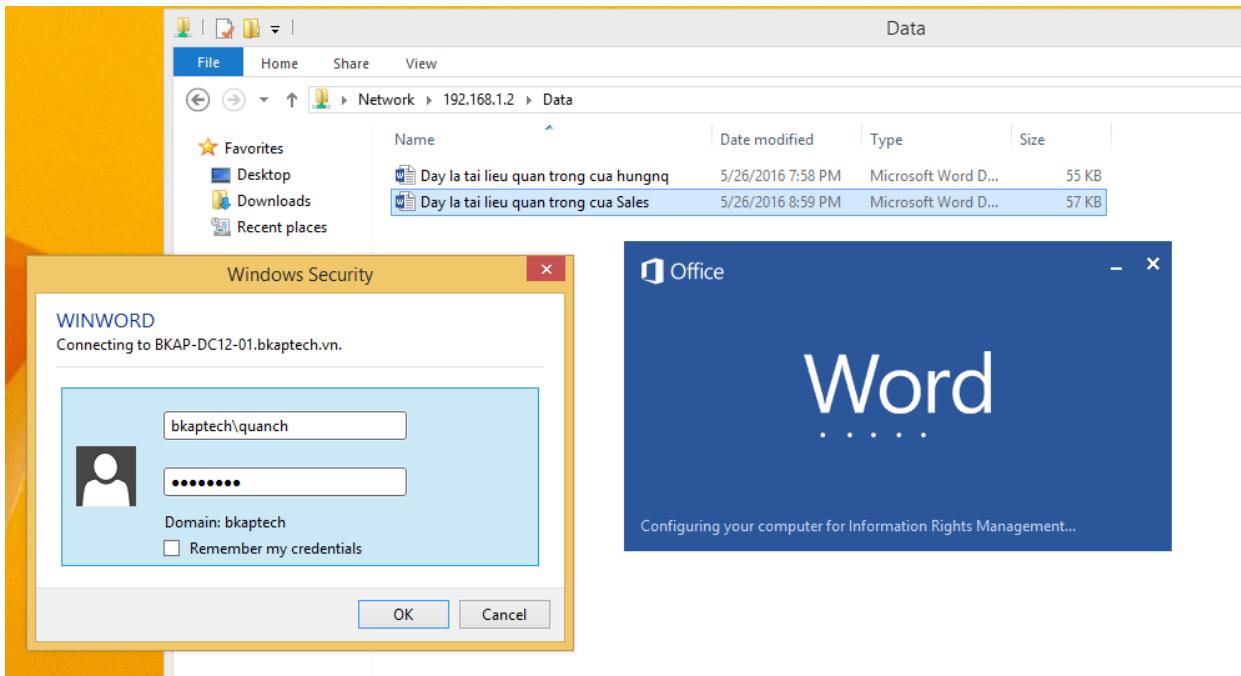
Day la tai lieu quan trong cua Sales



- Đăng nhập lại bằng user **quanch** thuộc group **Sales** để kiểm tra.



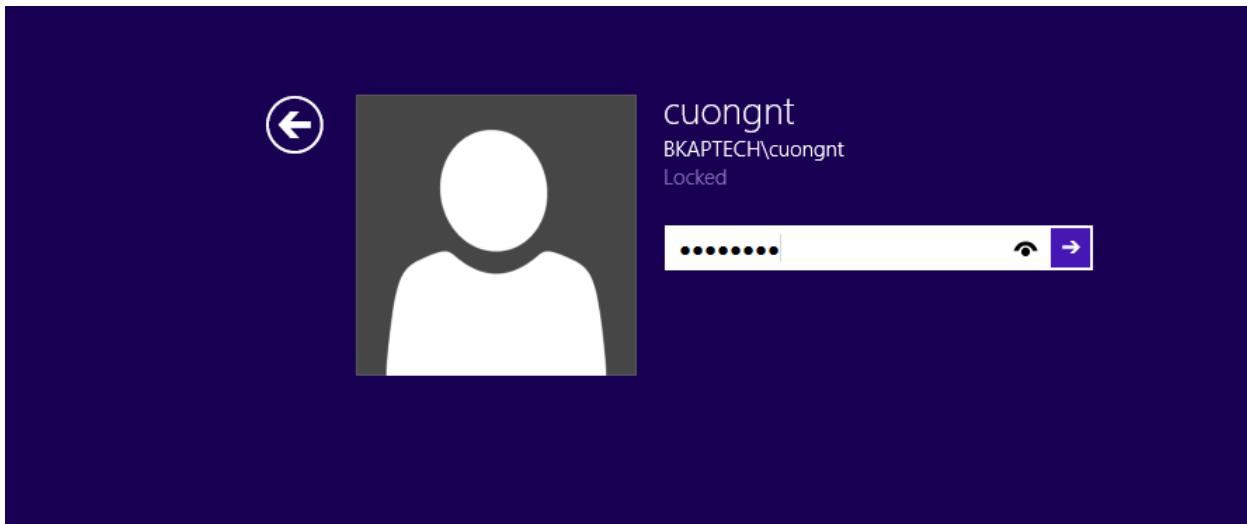
- Truy cập, mở file *Document* vừa được tạo ra bởi user **cuongnt** trong group **Sales**, nhập vào user **quanch**.



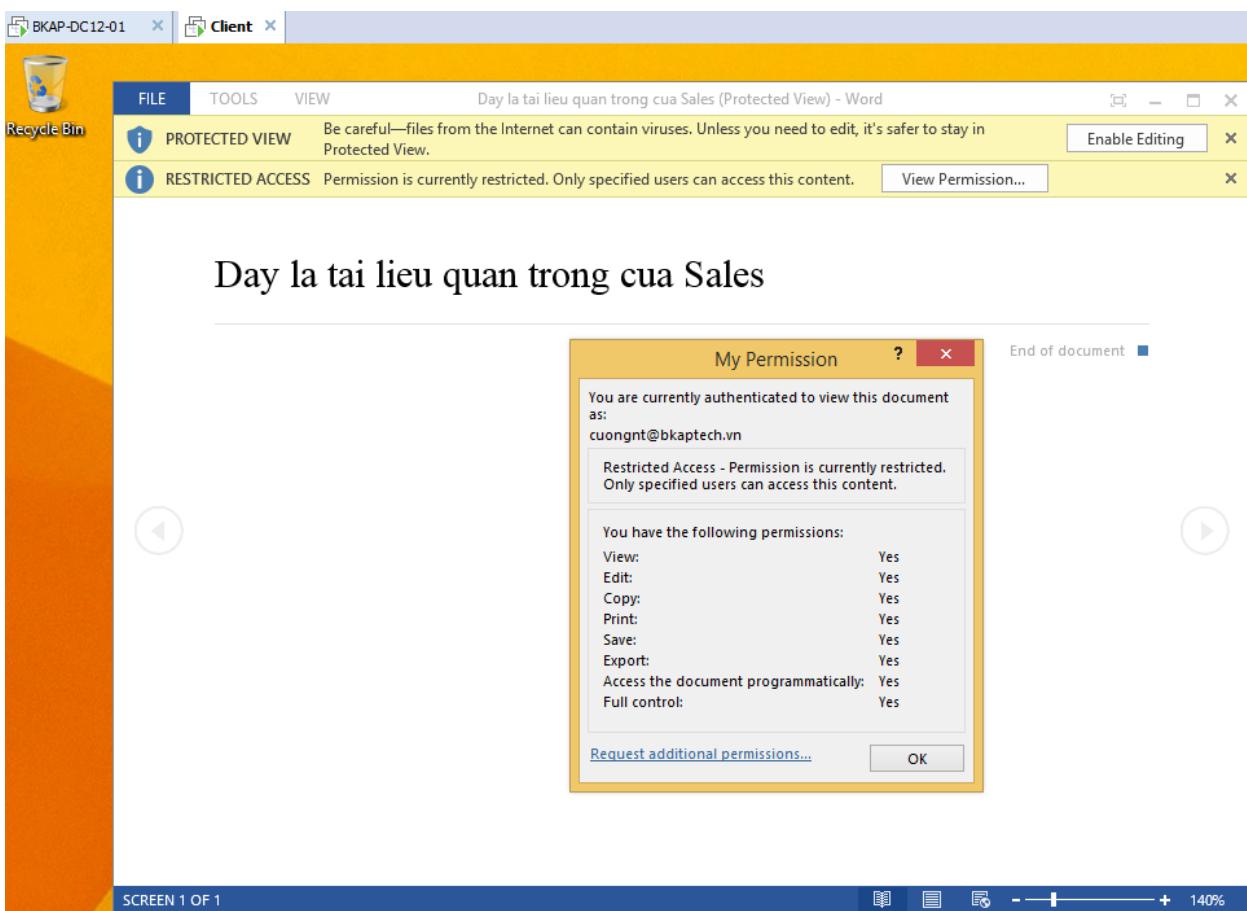
⇒ User **quanch** thuộc group **Sales** (cùng nhóm với user **cuongnt**) nên có thêm các quyền *Copy*, *chỉnh sửa* trong văn bản này.

Permission	Status
View:	Yes
Edit:	Yes
Copy:	Yes
Print:	No
Save:	Yes
Export:	No
Access the document programmatically:	Yes
Full control:	No

- Đăng nhập lại user **cuongnt** trong group Sale:



- User **cuongnt** có toàn quyền trong file Document này.



5.2 Cấu hình Active Directory Rights Management Services – P2

1.Yêu cầu bài lab:

- + Cho phép người dùng thuộc domain **bkaptech.vn** có thể phân quyền trên các tài liệu nhạy cảm cho người dùng thuộc domain **bachkhoa-aptech.com** .

2.Yêu cầu chuẩn bị:

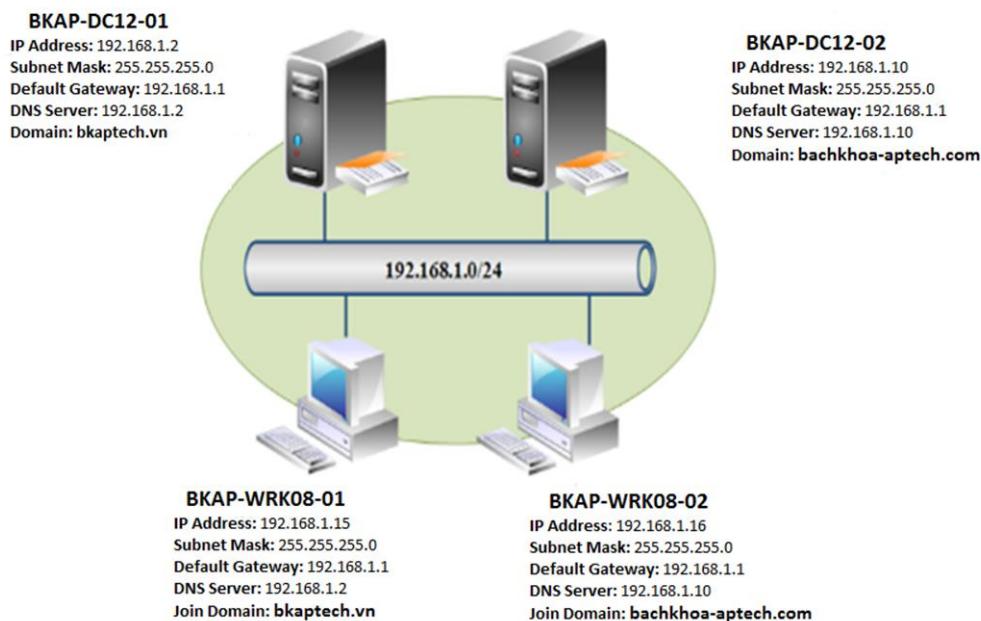
- + Máy **BKAP-DC12-01**: đã nâng cấp lên *Domain Controller* quản lý miền **bkaptech.vn**.
- + Máy **BKAP-DC12-02**: đã nâng cấp lên *Domain Controller* quản lý miền **bachkhoa-aptech.com**.
- + Máy **BKAP-WRK08-01**: Client đã join vào miền **bkaptech.vn** , cài đặt **Office 2013**.
- + Máy **BKAP-WRK08-02**: Client đã join vào miền **bachkhoa-aptech.com** , cài đặt **Office 2013**.

3.Mô hình Lab:

HỆ THỐNG ĐÀO TẠO CNTT QUỐC TẾ BACHKHOA-APTECH



Cài đặt và cấu hình AD RMS (Phần 2)

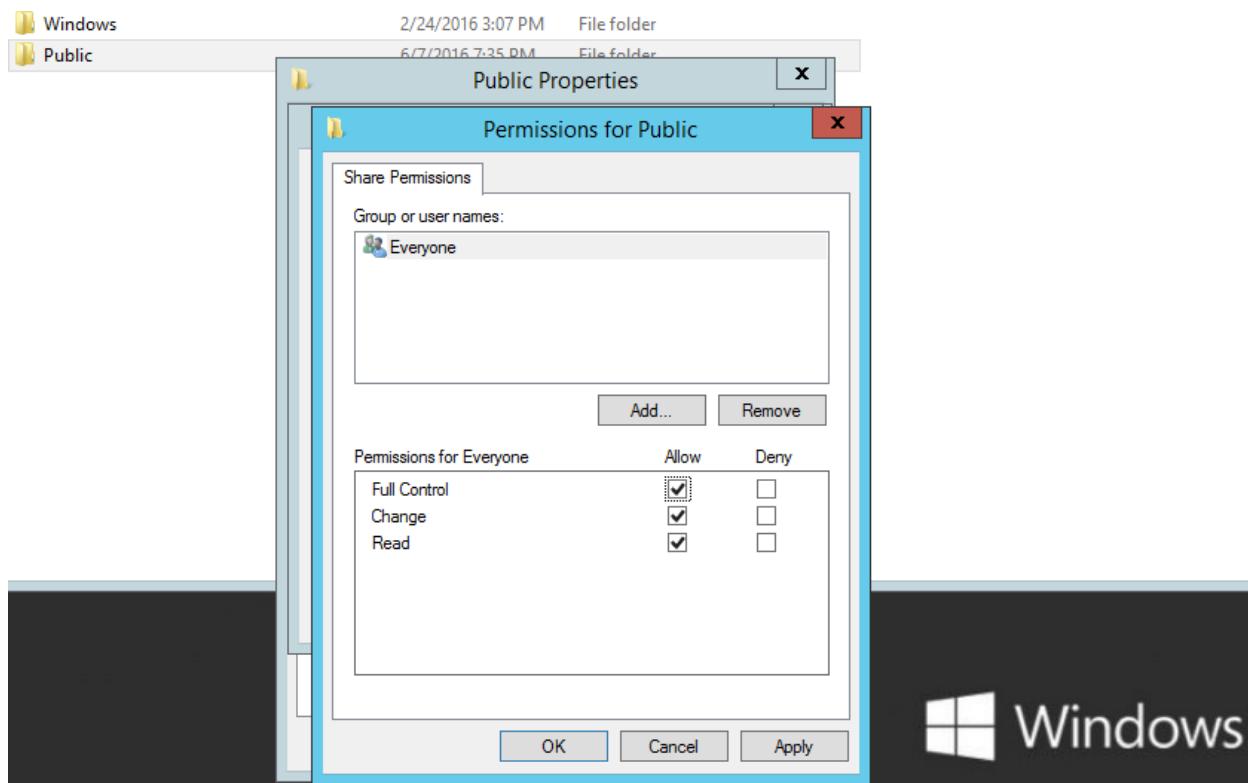


Sơ đồ địa chỉ như sau:

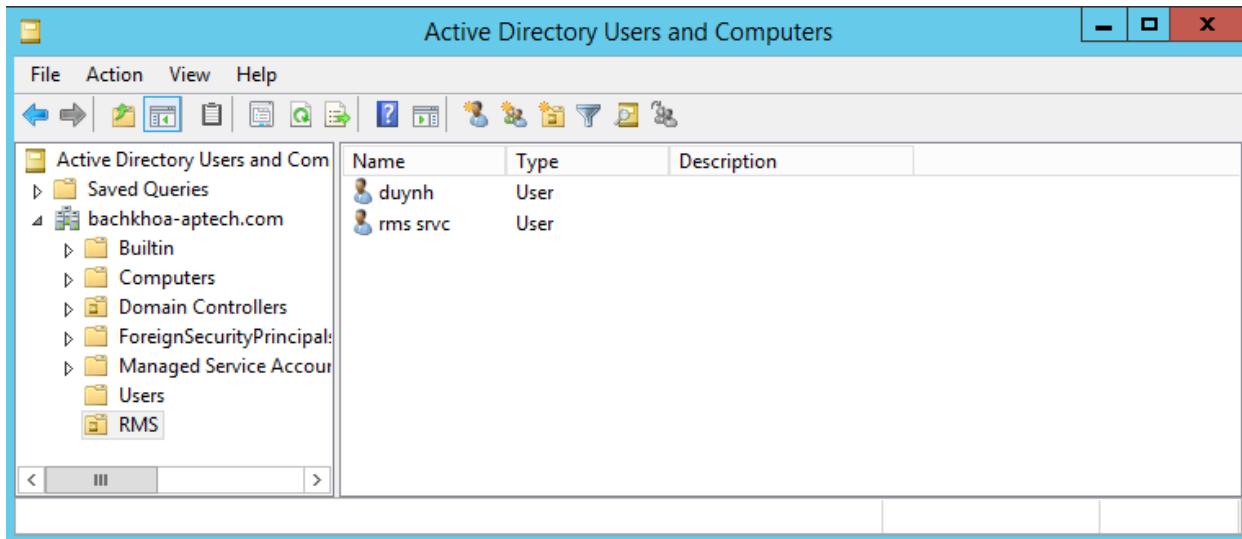
Thông số	DC12-01	DC12-02	WRK08-01	WRK08-02
IP Address	192.168.1.2	192.168.1.110	192.168.1.15	192.168.1.16
Subnet Mask	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
Default Gateway	192.168.1.1	192.168.1.1	192.168.1.1	192.168.1.1
DNS Server	192.168.1.2	192.168.1.110	192.168.1.2	192.168.1.110

Hướng dẫn chi tiết:

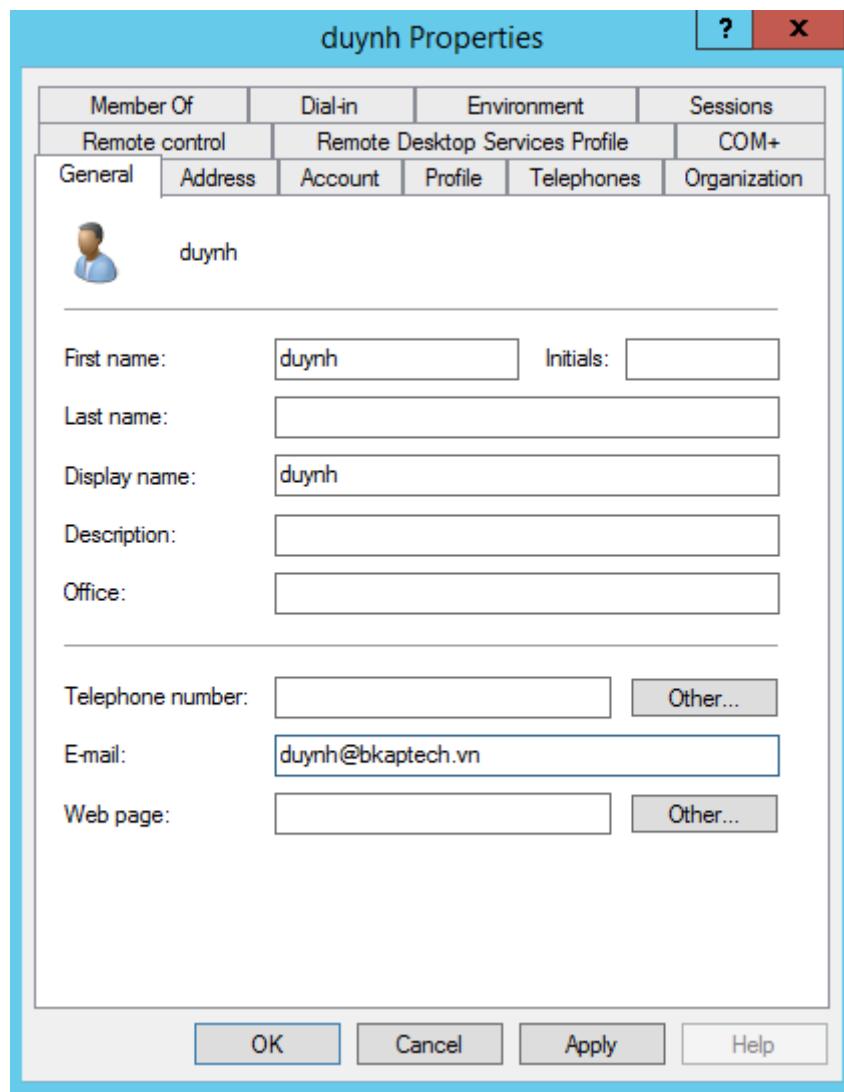
- Trên máy server BKAP-DC12-02 thực hiện tạo thư mục **C:\Public** , share thư mục này cho *Everyone* quyền **Full Control**.



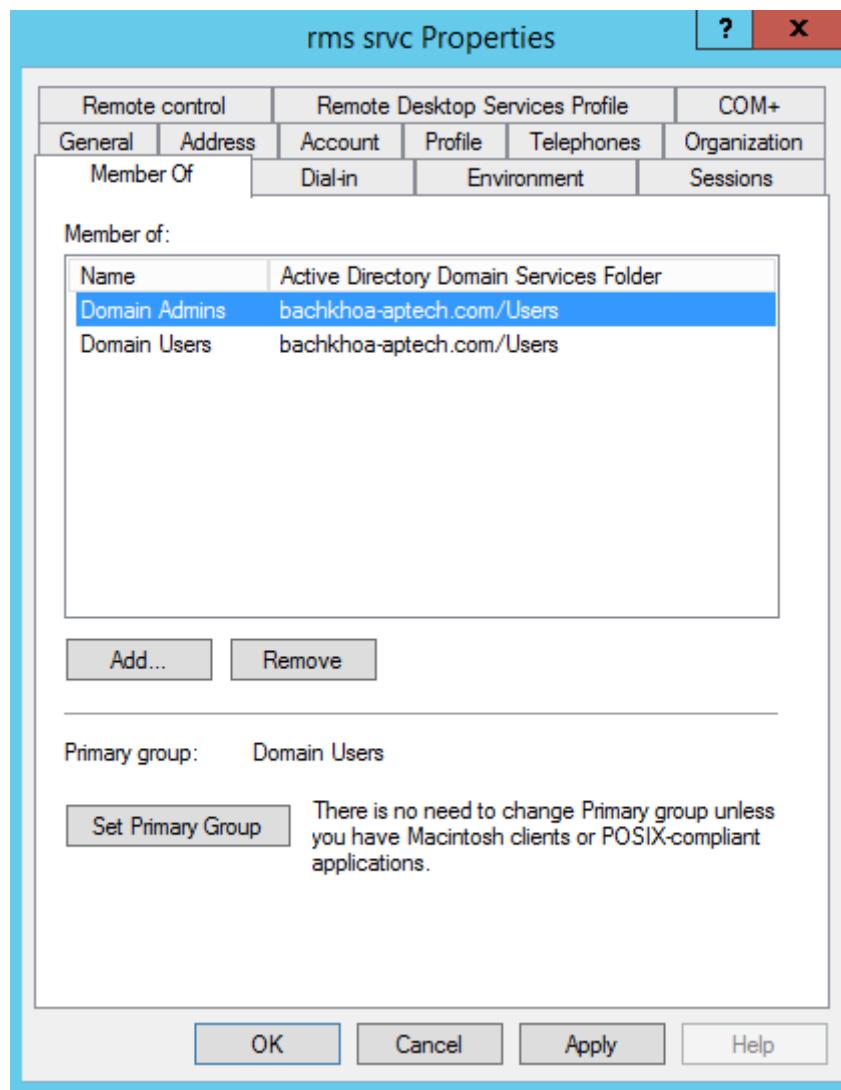
- Tạo OU tên RMS, trong OU này, tạo 2 user tên rmssrvc và duynh.



- Tạo thuộc tính *email* cho user **duynh**.



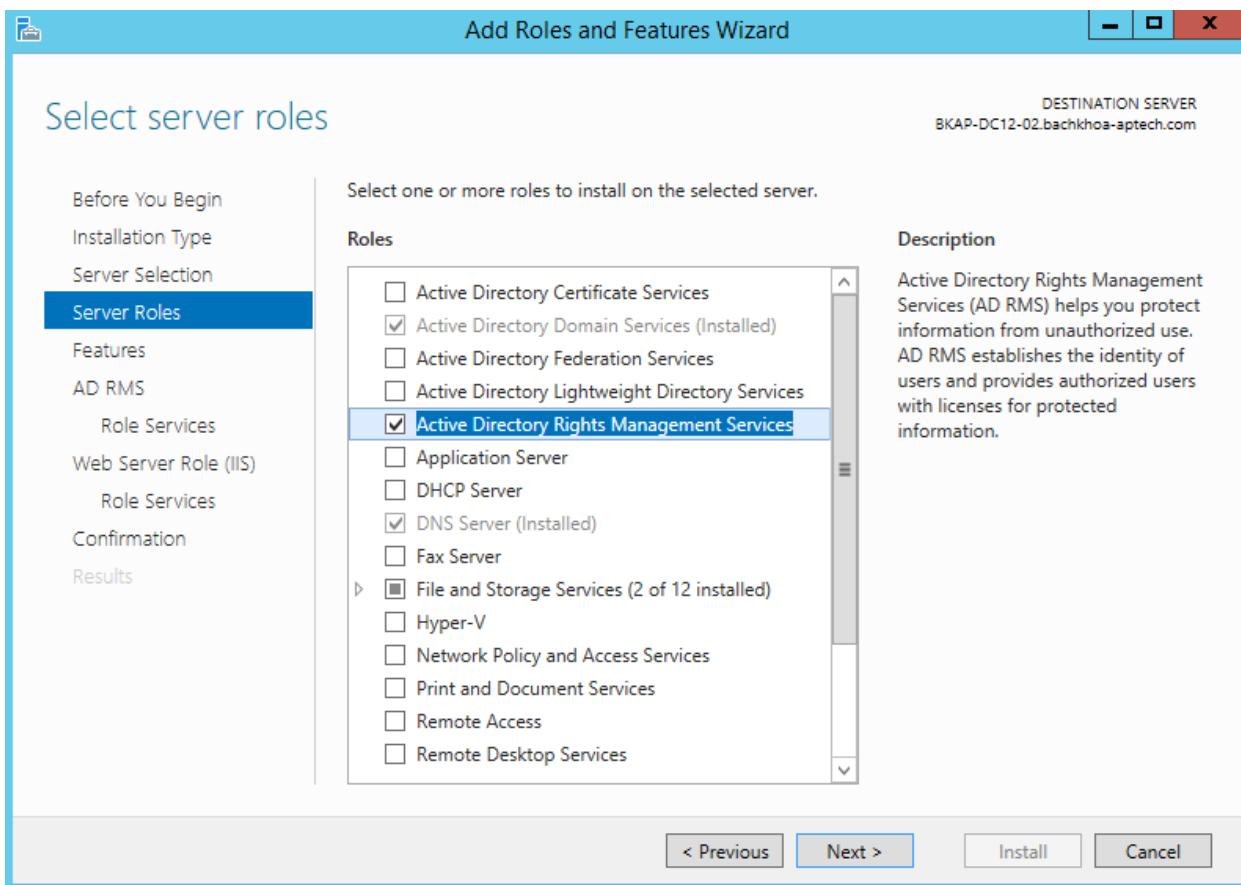
- Đưa user **rmssrvc** vào thành viên của group **Domain Admins**.



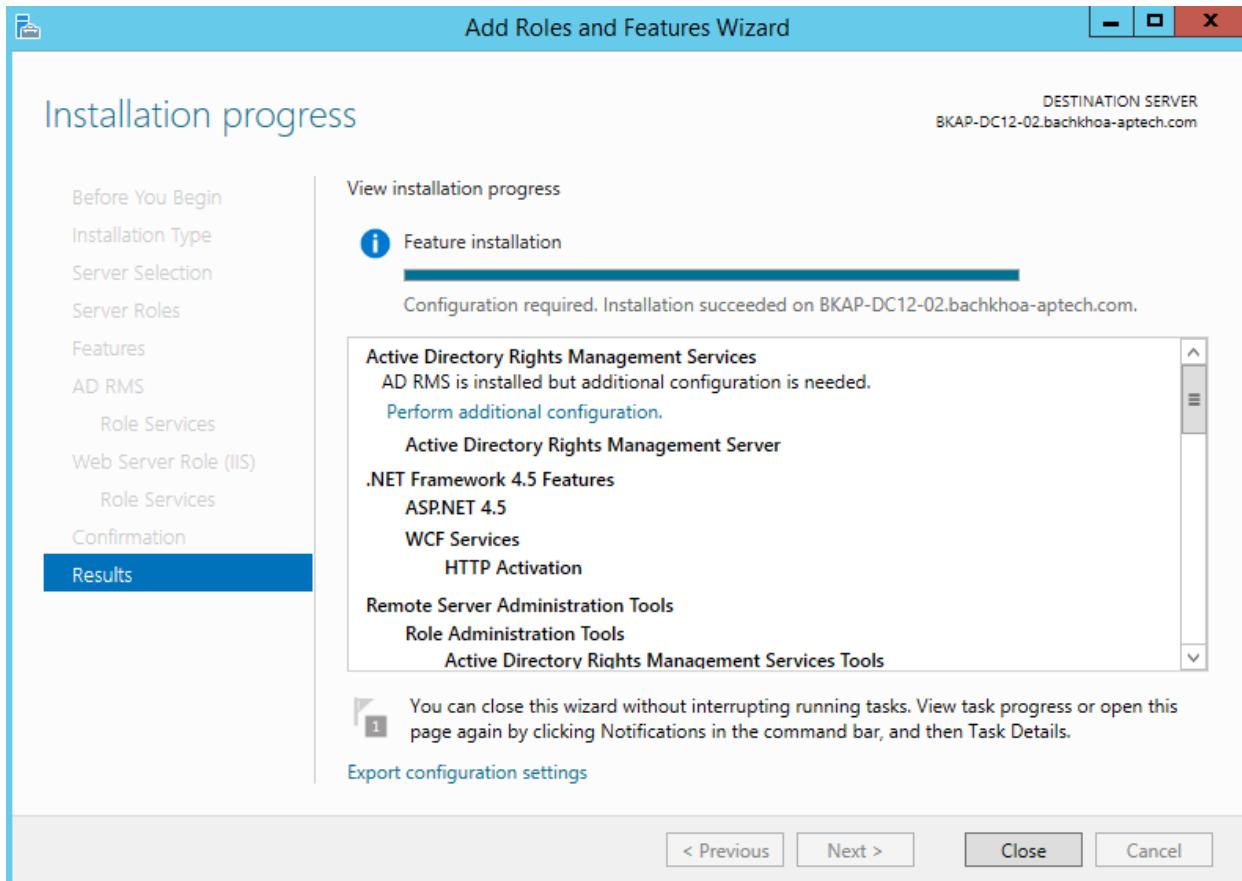
- Chuyển qua máy Client *BKAP-WRK08-02*, join vào *domain*, đăng nhập bằng user **duynh**.



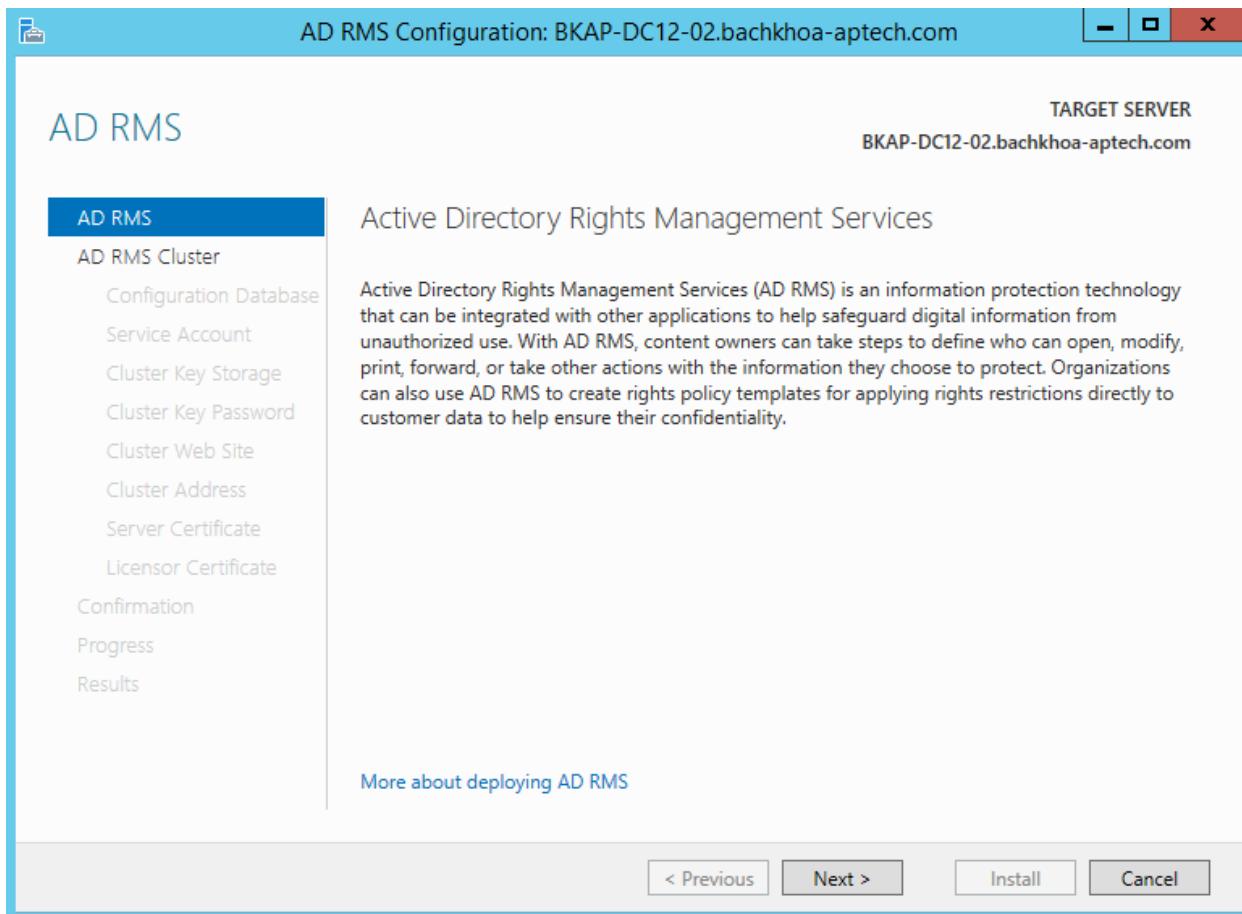
- Chuyển sang máy *BKAP-DC12-02* thực hiện cài đặt **Active Directory Rights Management**.



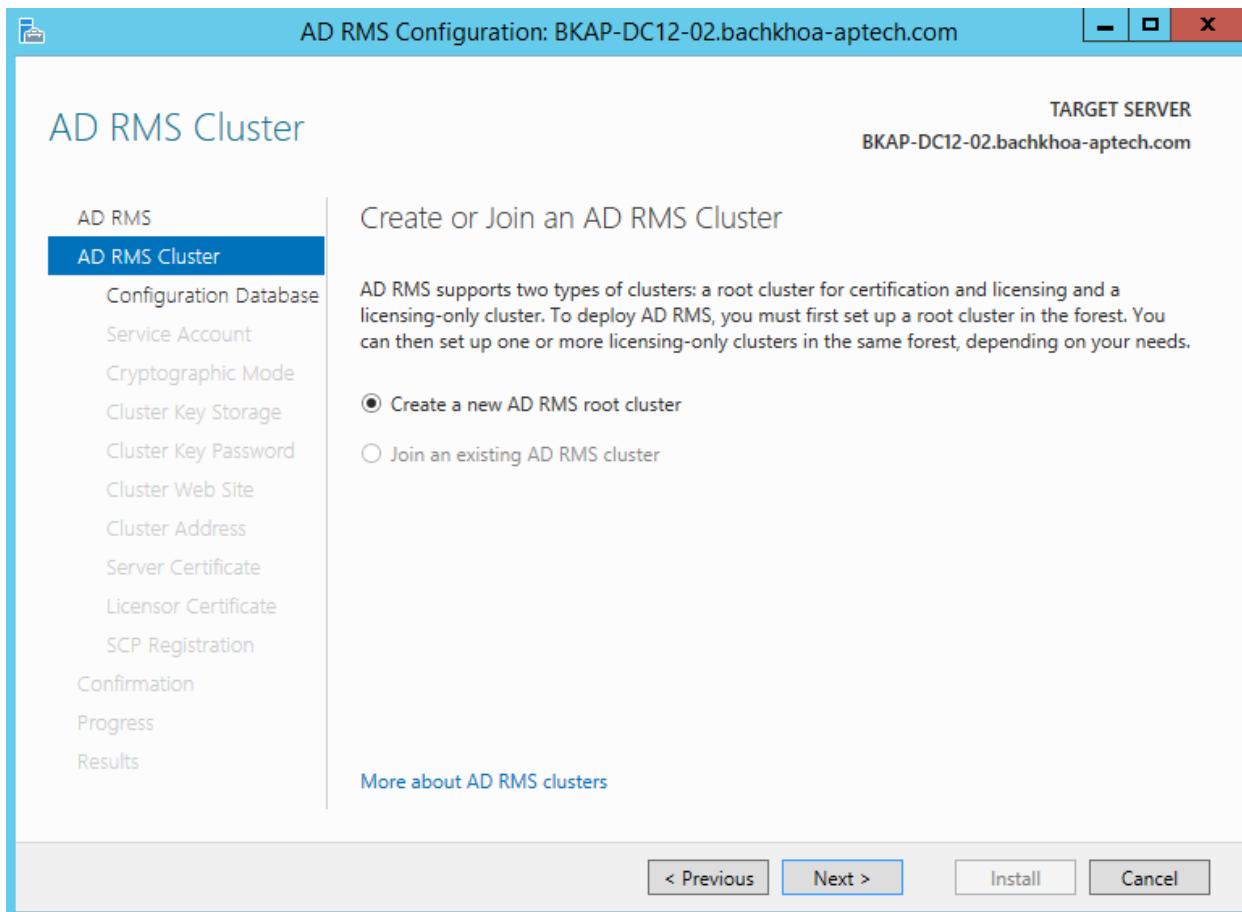
- Tại cửa sổ **Installation progress**, click vào dòng chữ **Perform additional configuration**.



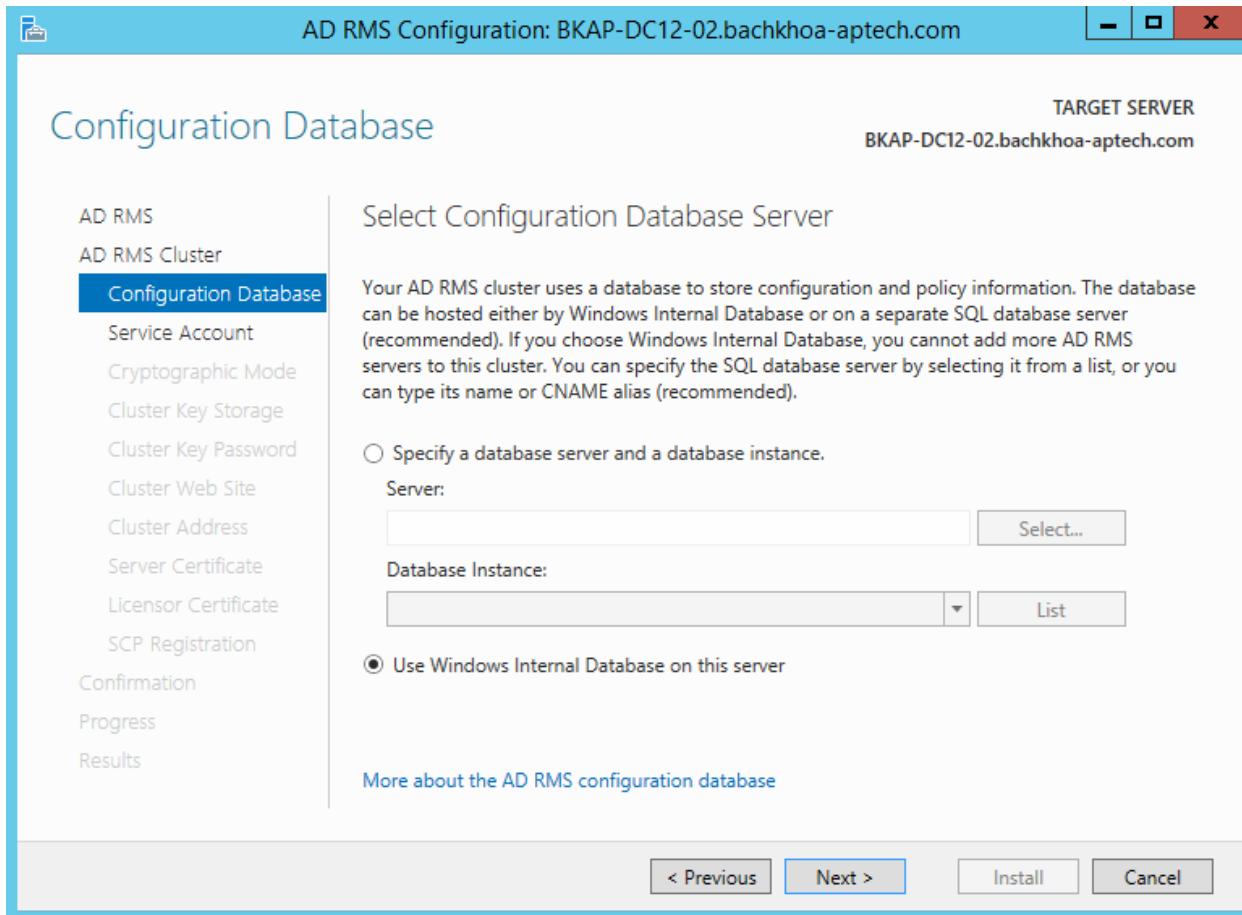
- Tại cửa sổ **AD RMS**, click vào **Next**.



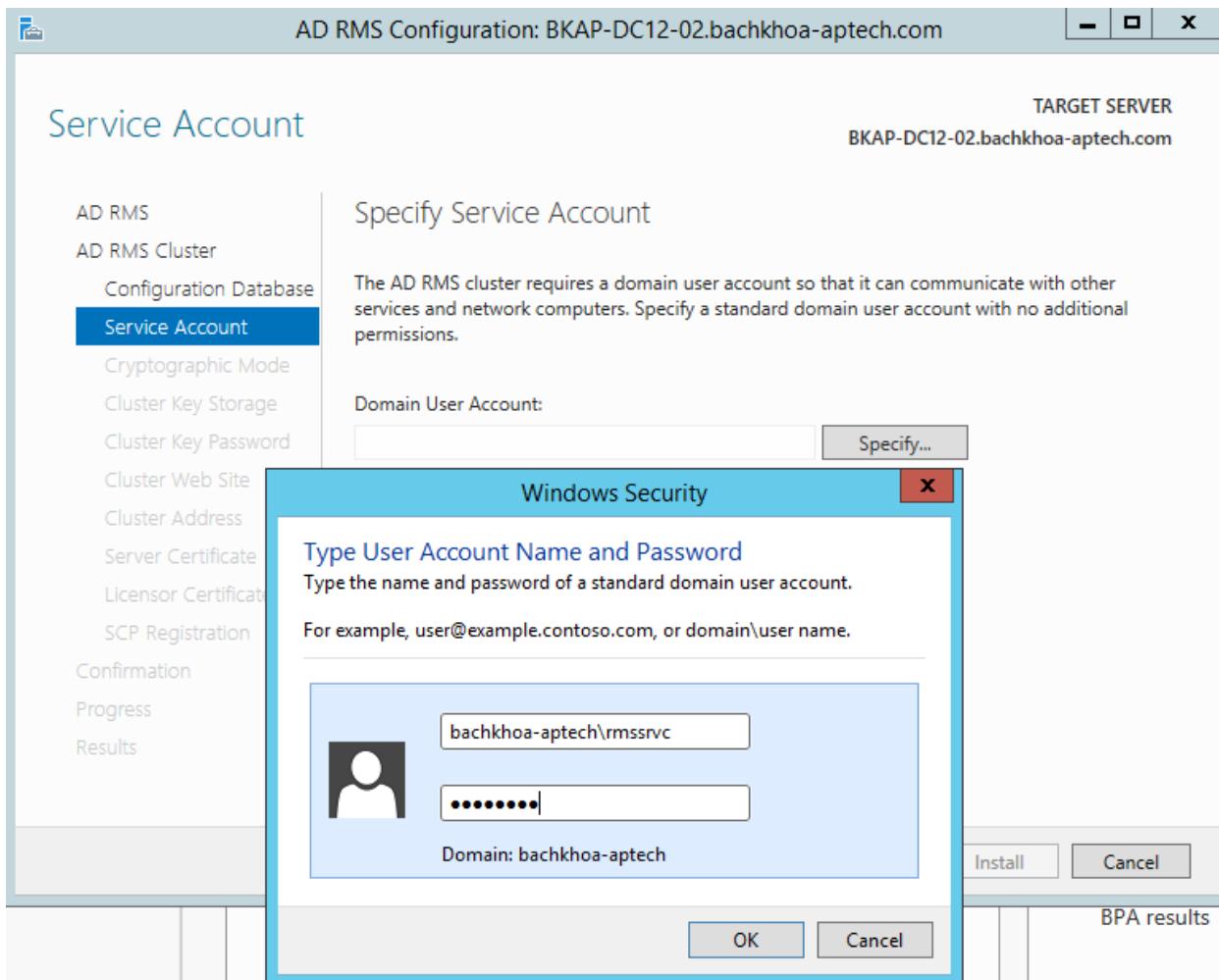
- Tại cửa sổ **AD RMS Cluster**, click vào **Next**.



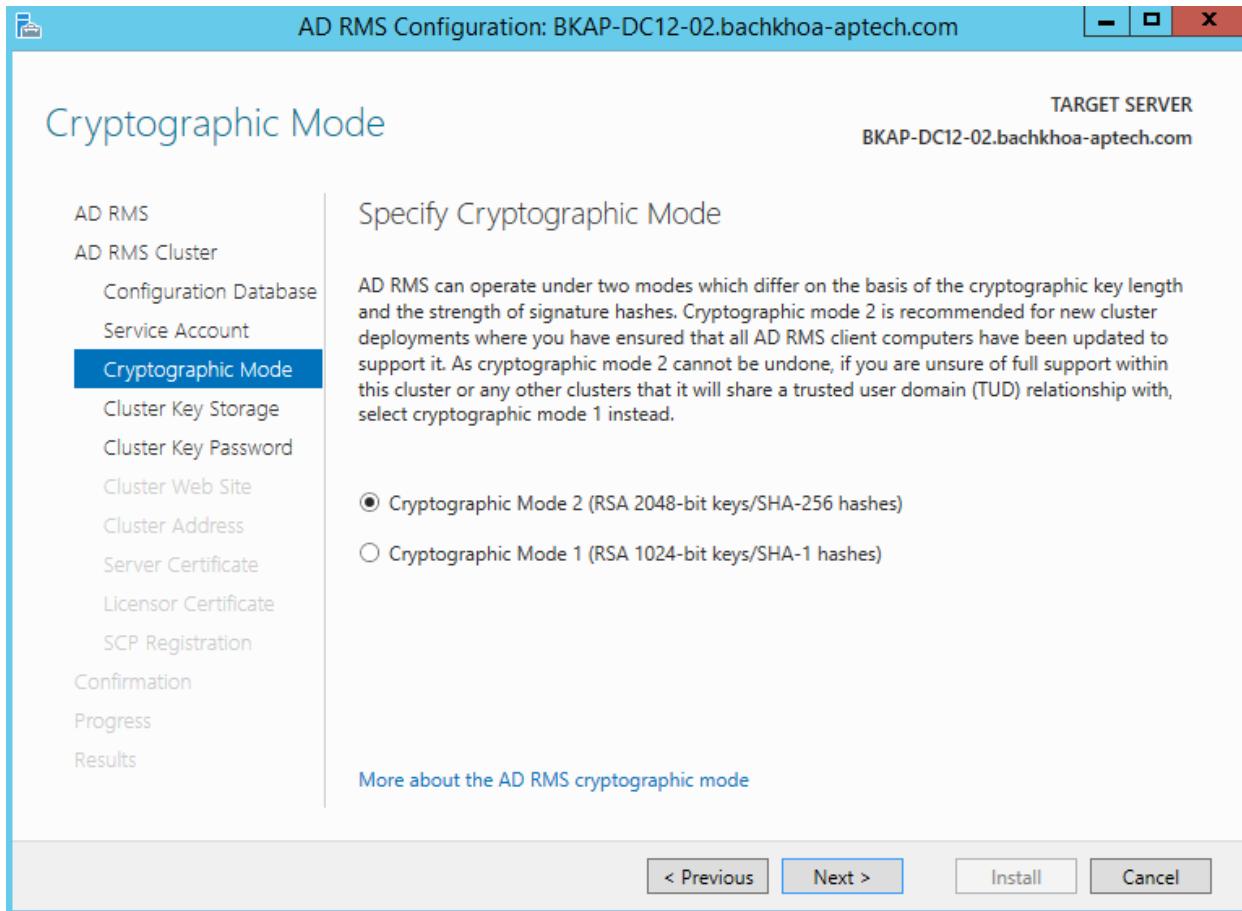
- Tại cửa sổ **Configuration Database**, click chọn vào **Use Windows Internal Database on this server**.



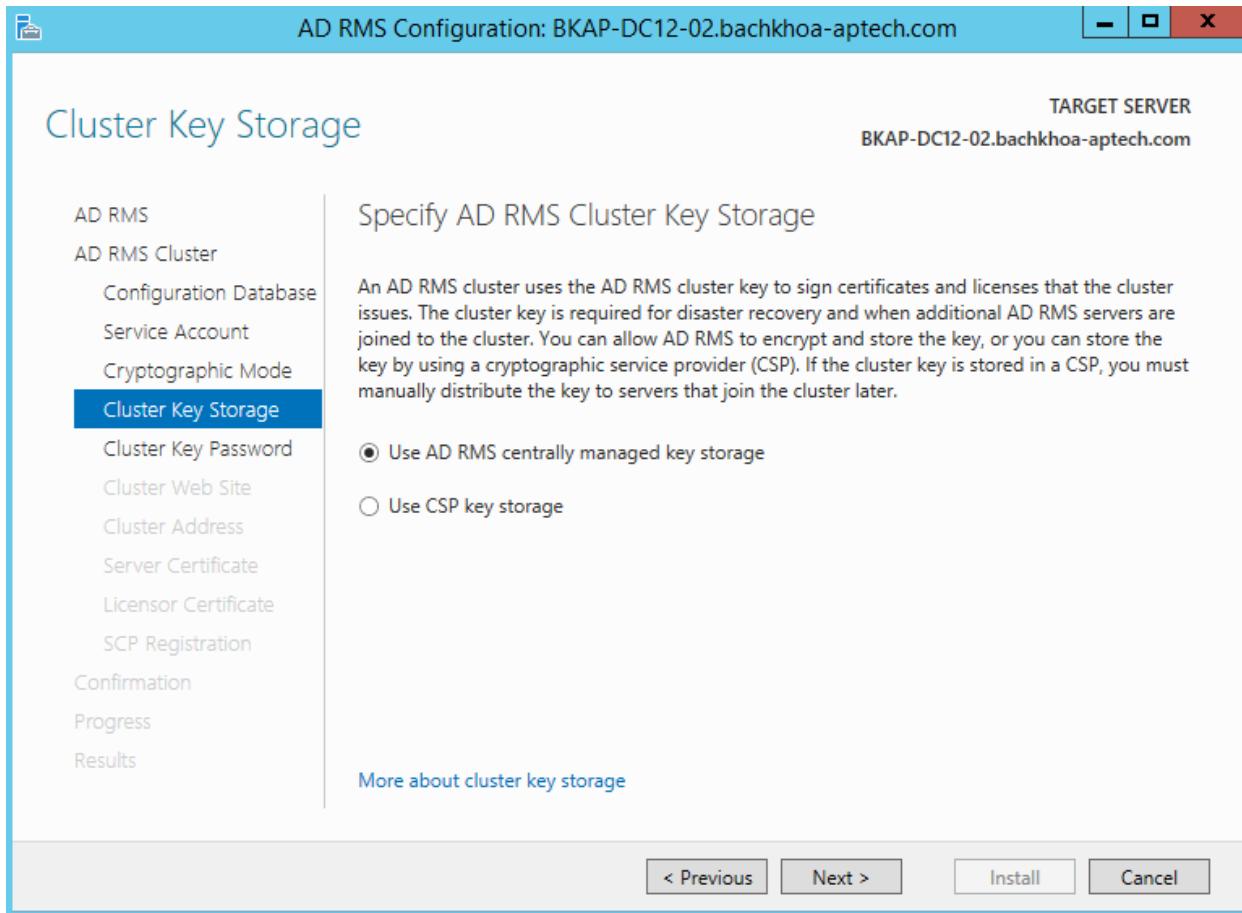
- Tại cửa sổ **Service Account**, nhập vào user **rmssrvc**, click vào **Next**.



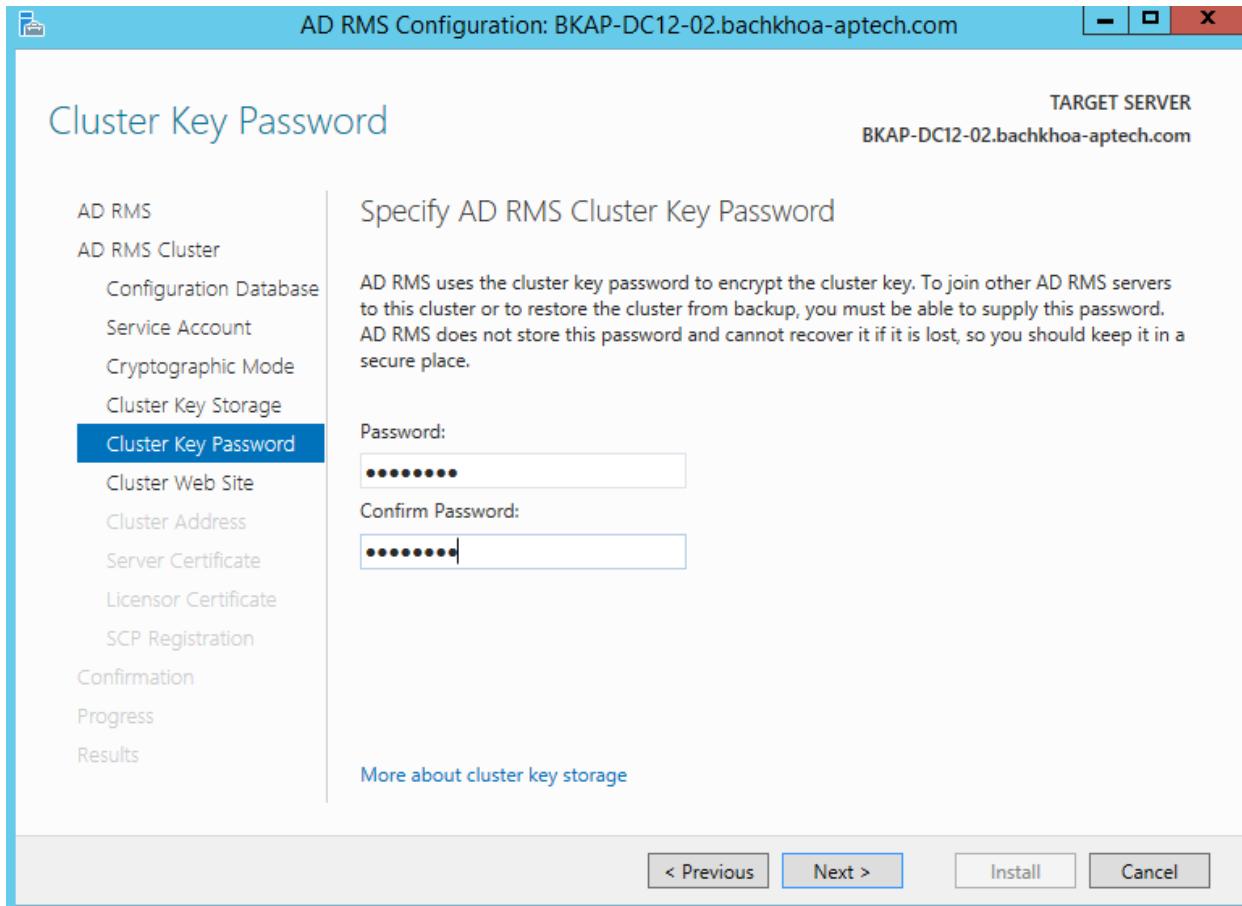
- Tại cửa sổ **Cryptographic Mode**, chọn vào **Cryptographic Mode 2...**



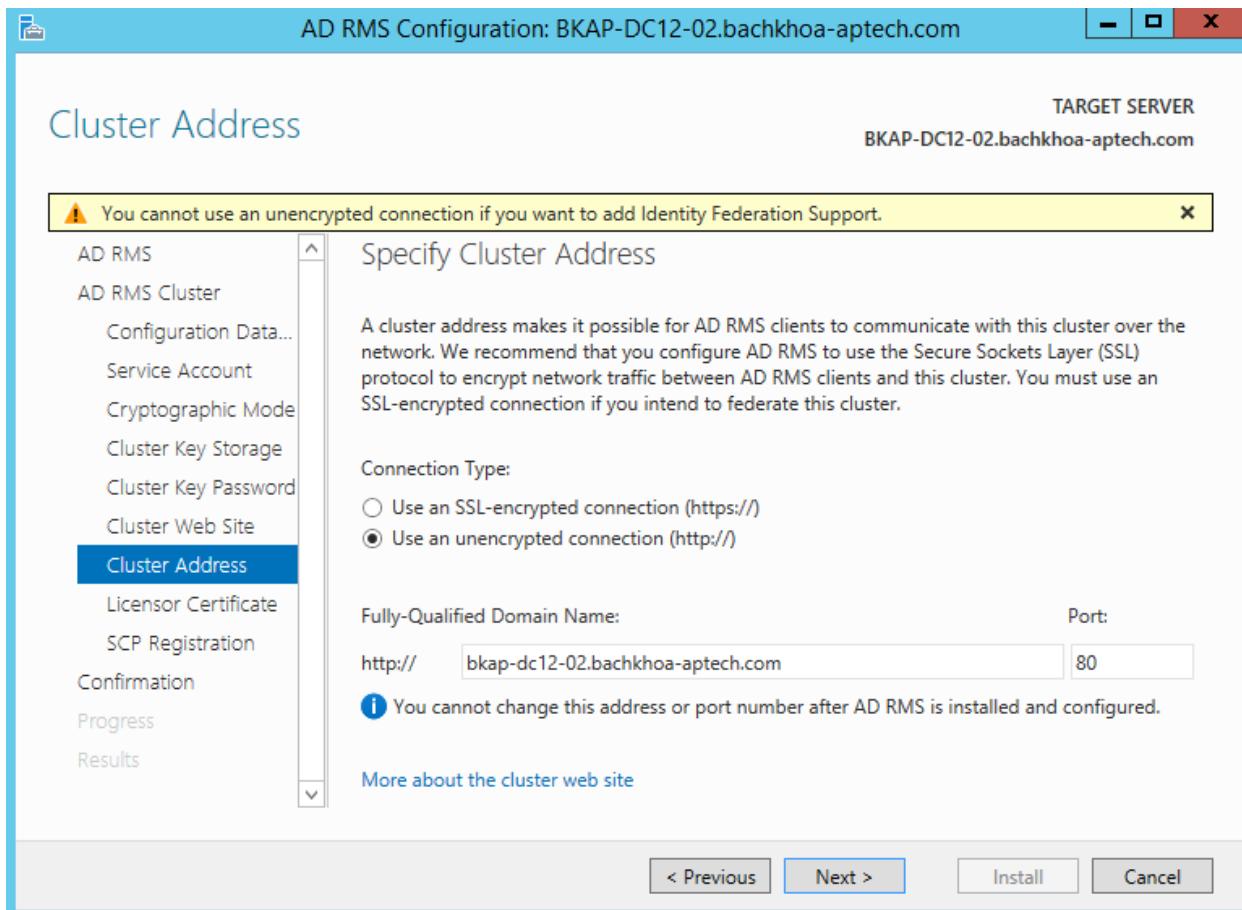
- Tại cửa sổ **Cluster Key Storage**, click chọn vào **Use AD RMS centrally managed key storage**.



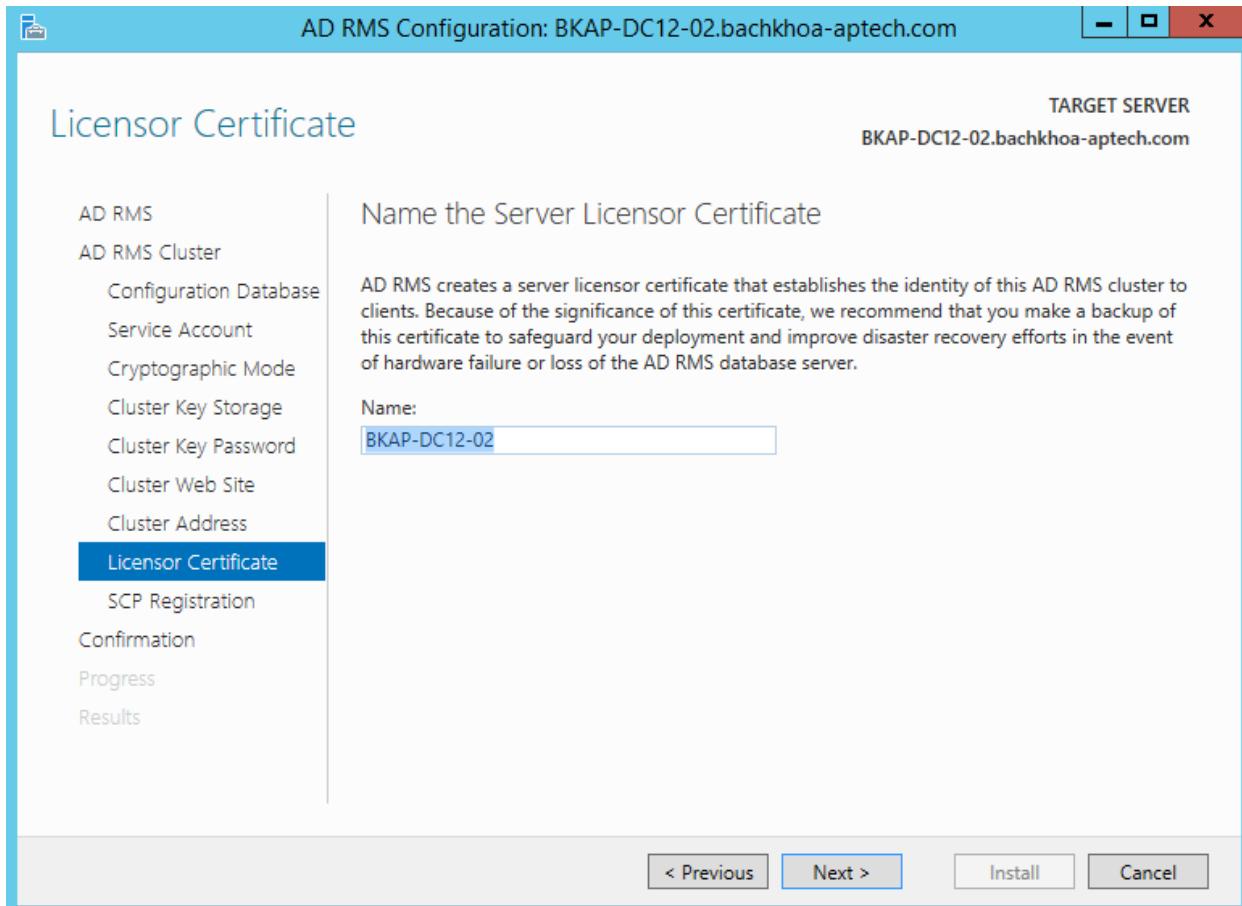
- Tại cửa sổ **Cluster Key Password**, nhập vào mật khẩu, click vào **Next**.



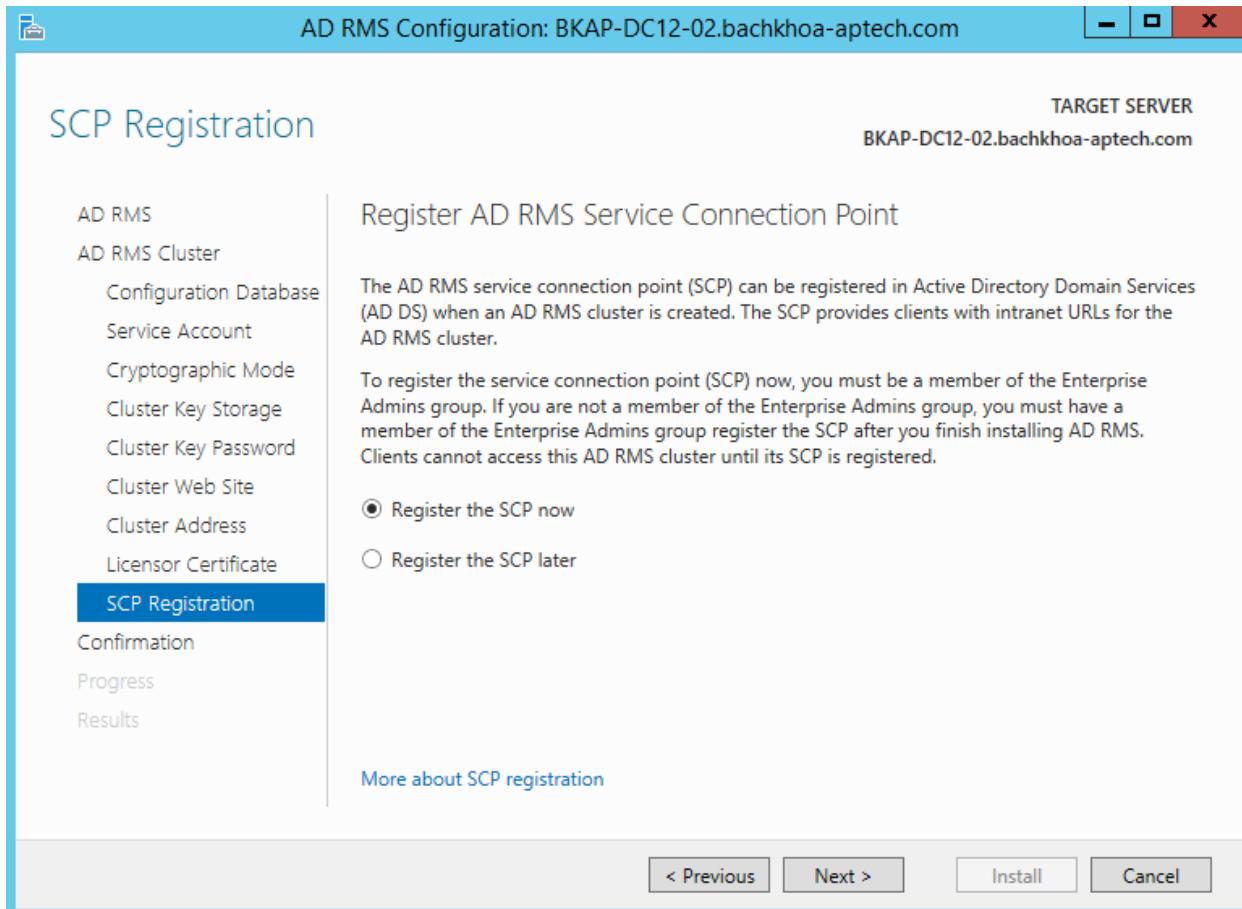
- Tại cửa sổ **Cluster Address**, click chọn vào **Use an unencrypted connection (http://)**, tại mục **http://** nhập vào tên đầy đủ của server **bkap-dc12-02.bachkhoa-aptech.com**.



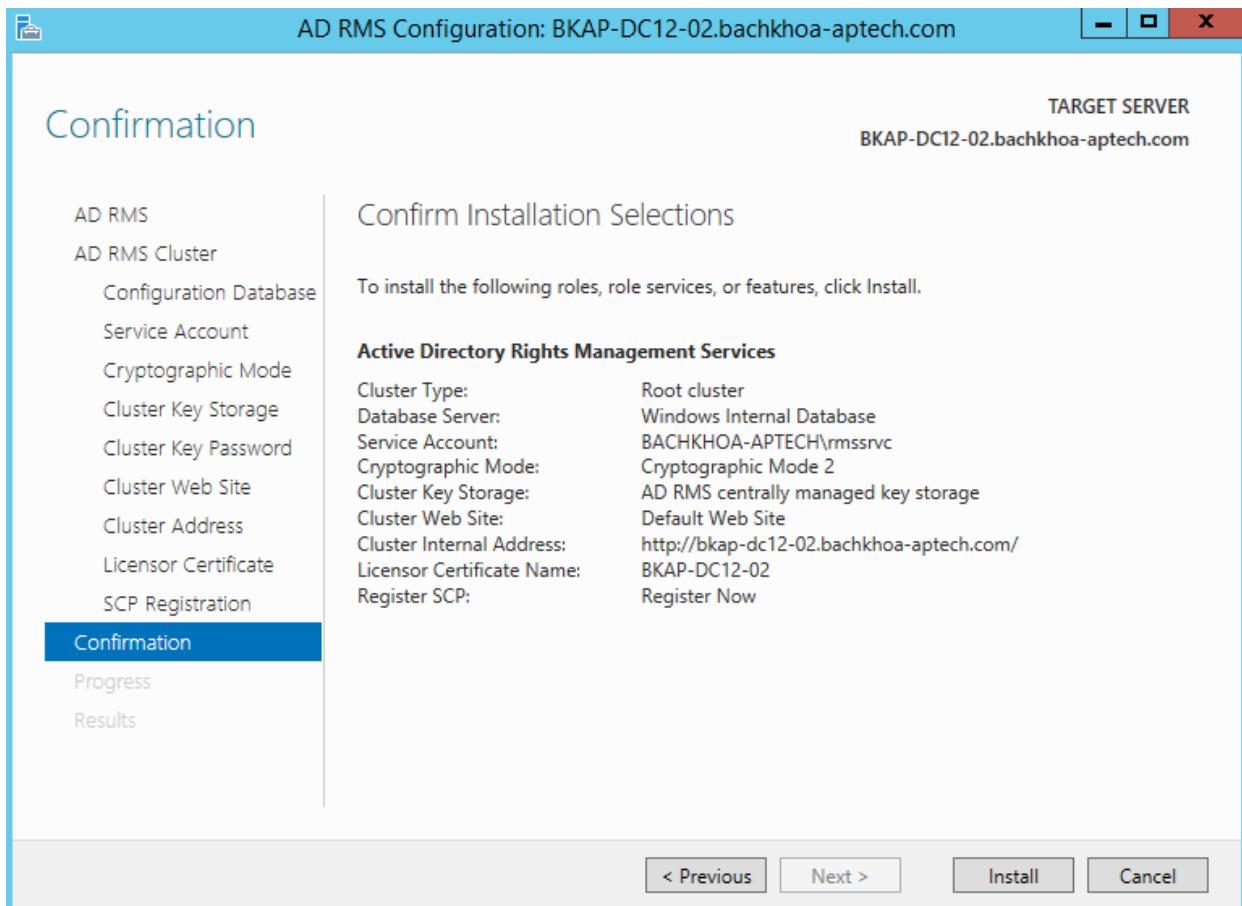
- Tại cửa sổ **Licensor Certificate**, kiểm tra tên server tại mục Name: **BKAP-DC12-02**, click vào **Next**.



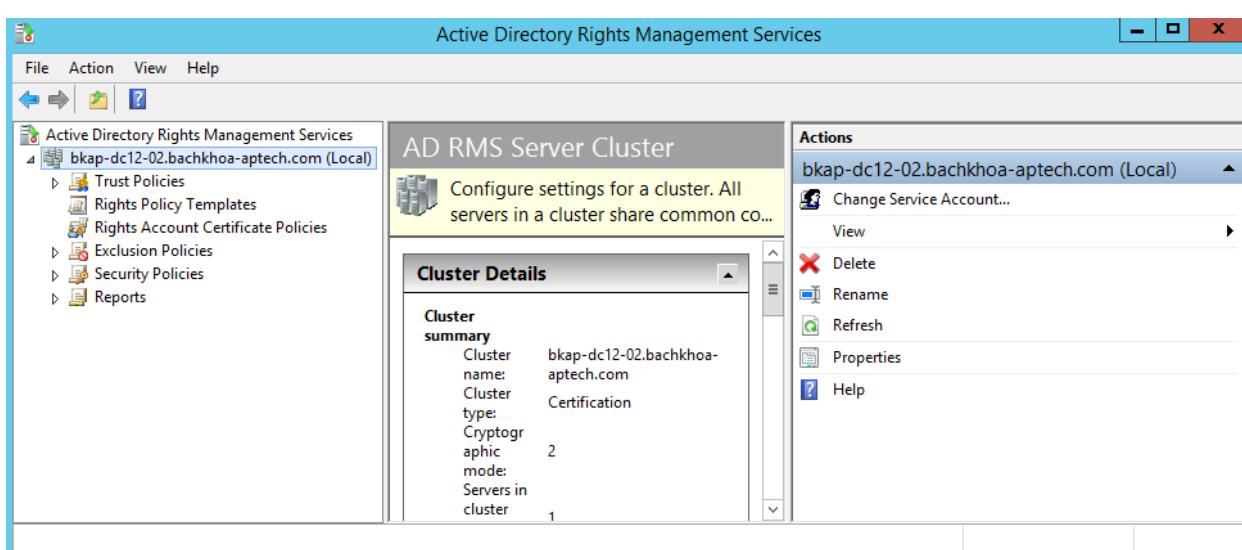
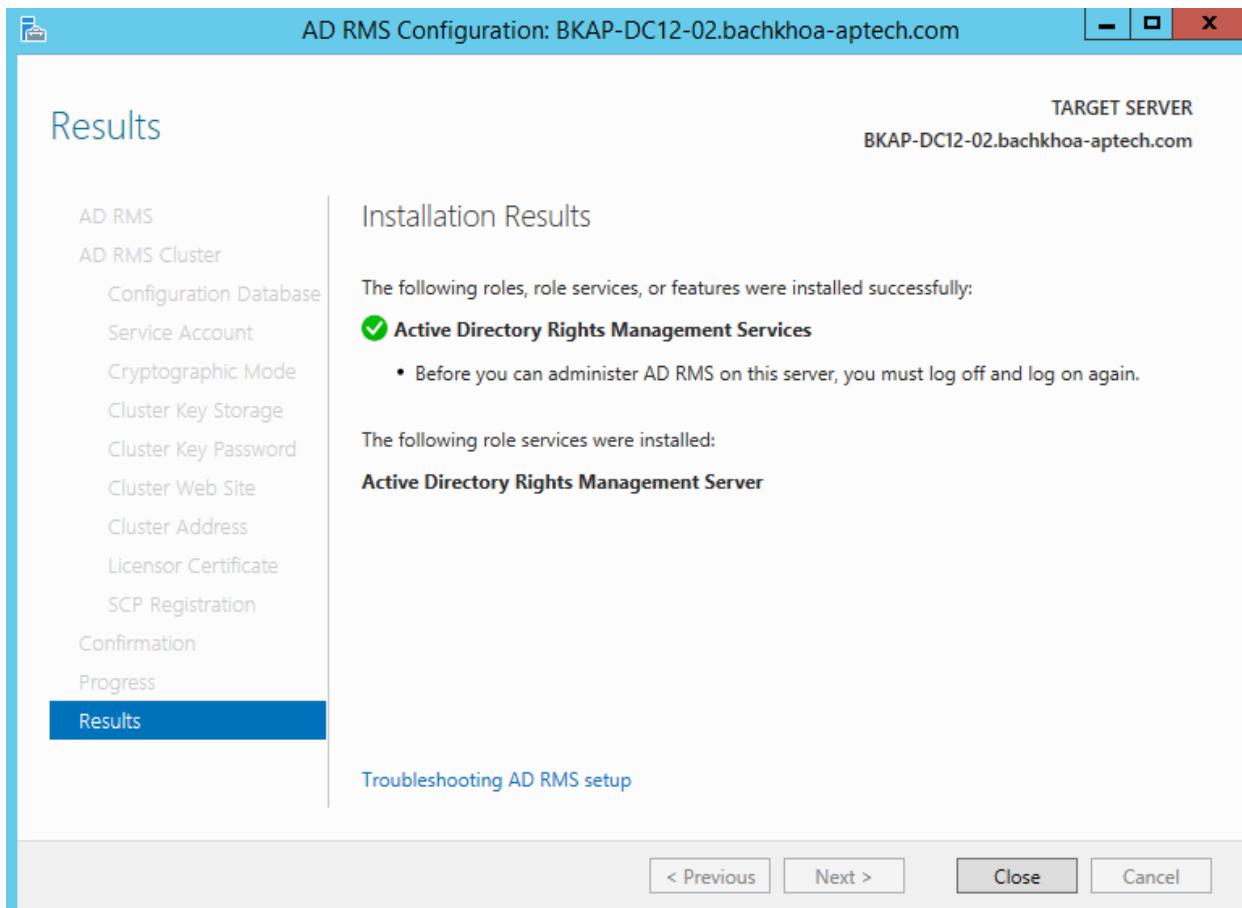
- Tại cửa sổ **SCP Registration**, click chọn vào **Register the SCP now**, click vào **Next**.



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

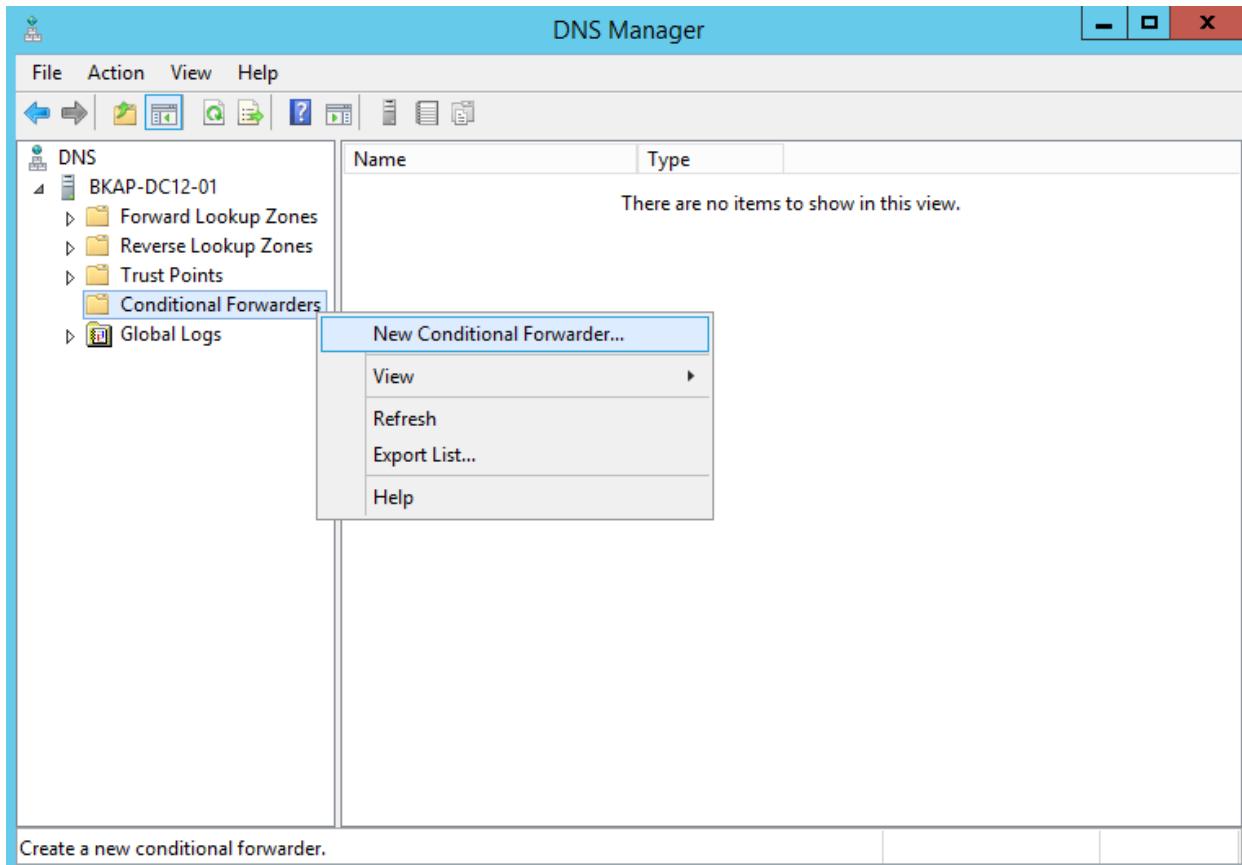


- Tại cửa sổ **Results**, click vào **Close, restart** lại máy , kiểm tra dịch vụ **AD RMS** vừa cài đặt.

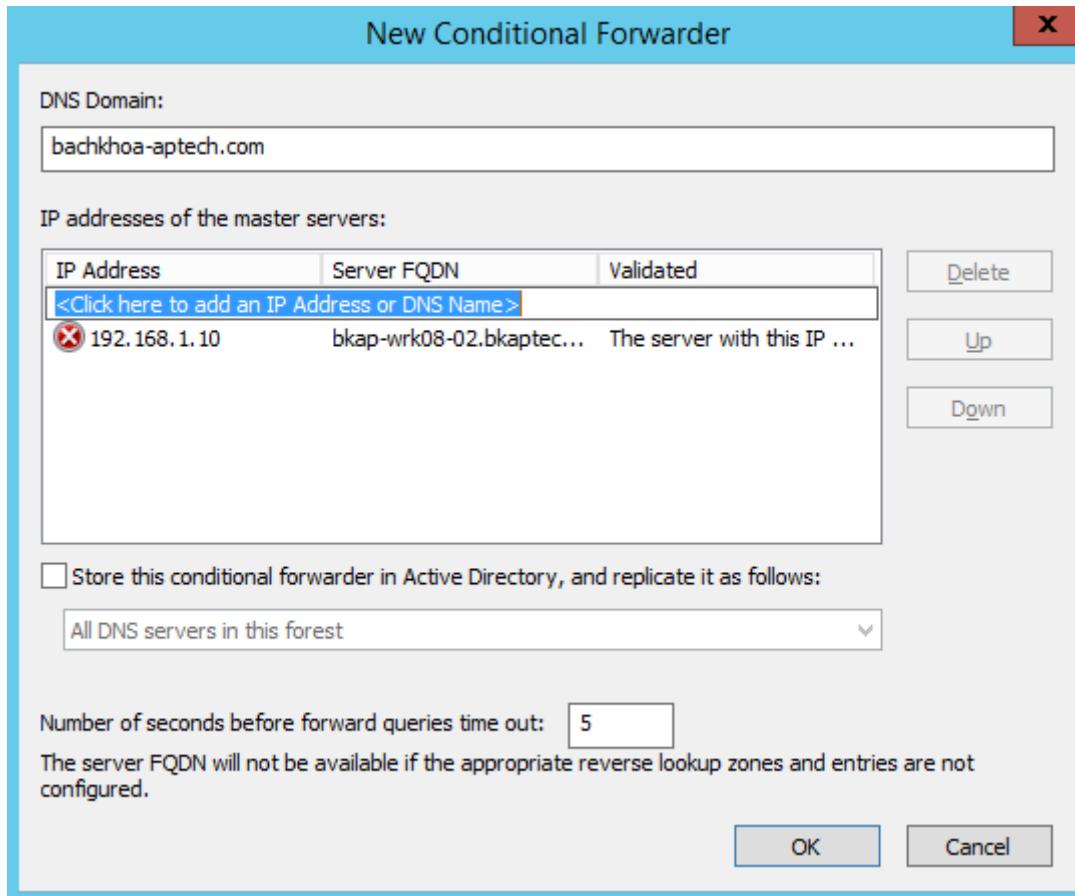


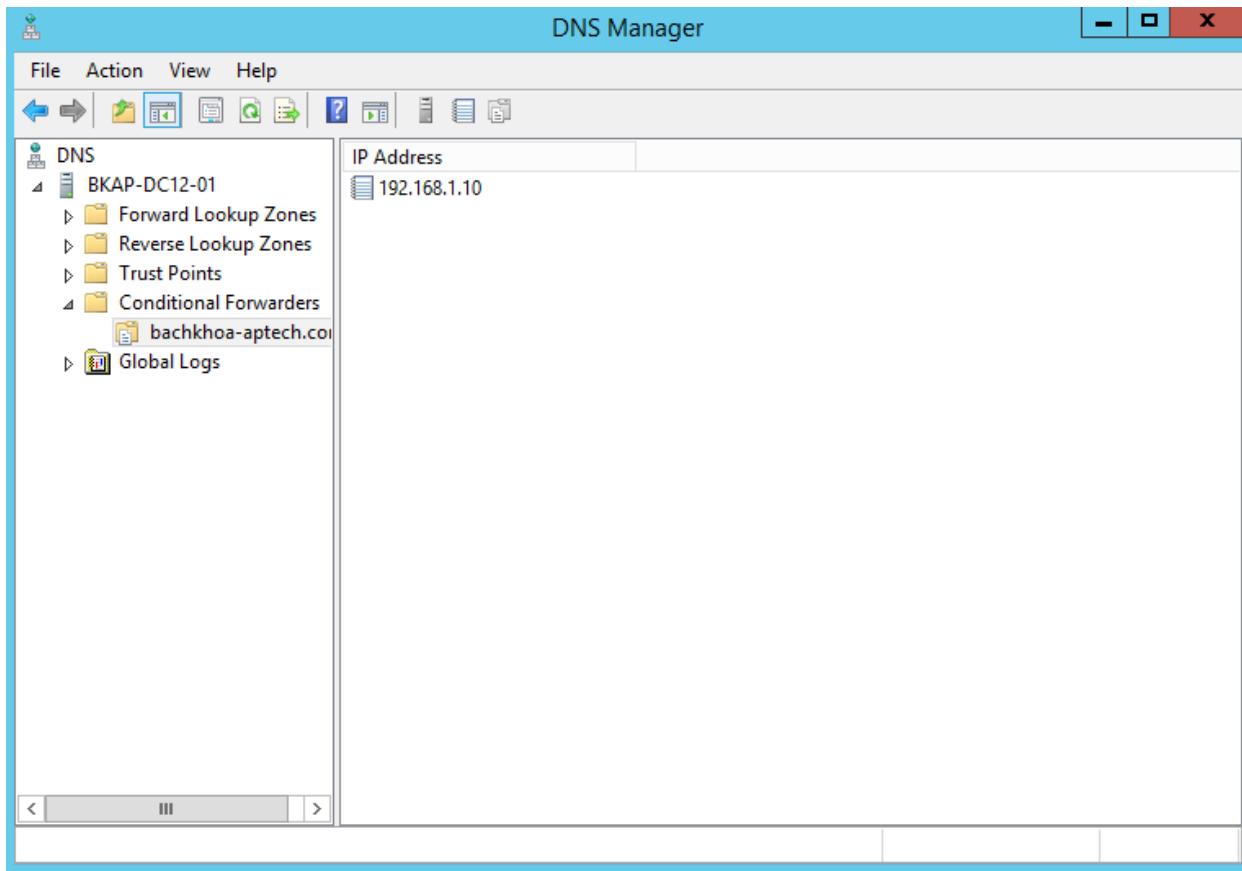
- Chuyển qua máy **BKAP-DC12-01**, vào dịch vụ **DNS**, thực hiện cấu hình **Conditional Forwarders**.

- Trong cửa sổ **DNS Manager**, click chuột phải vào **Conditional Forwarders**, chọn **New Conditional Forwarder...**



- Tại cửa sổ **New Conditional Forwarder**, tại mục **DNS Domain**, nhập vào tên **bachkhoa-aptech.com** , tại mục **IP address**, nhập vào địa chỉ **192.168.1.110** (địa chỉ IP của máy *BKAP-DC12-02*), click vào **OK**.





- Thực hiện kiểm tra phân giải bằng câu lệnh **nslookup bachkhoa-aptech.com**.

```

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

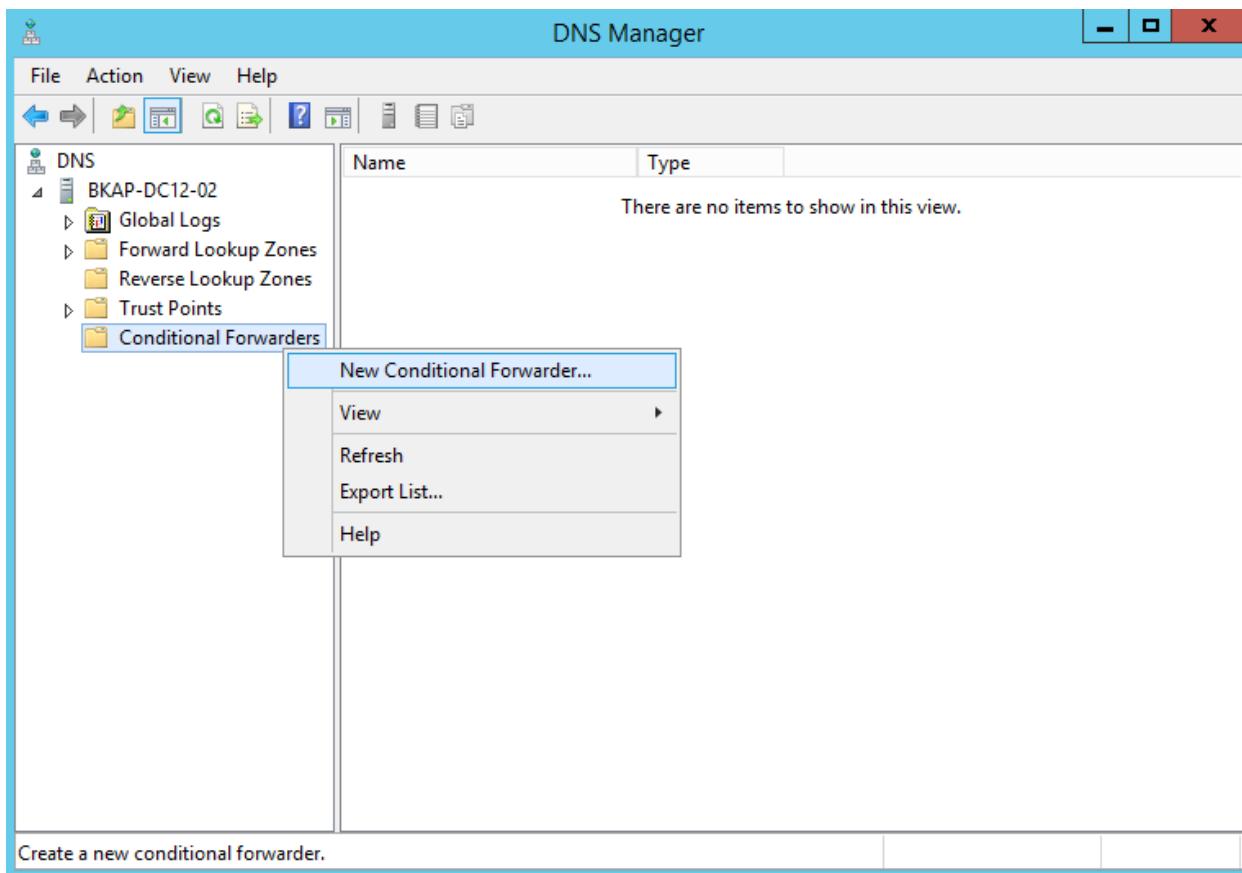
C:\Users\Administrator>nslookup bachkhoa-aptech.com
Server: bkap-dc12-01.bkaptech.vn
Address: 192.168.1.2

Non-authoritative answer:
Name: bachkhoa-aptech.com
Address: 192.168.1.10

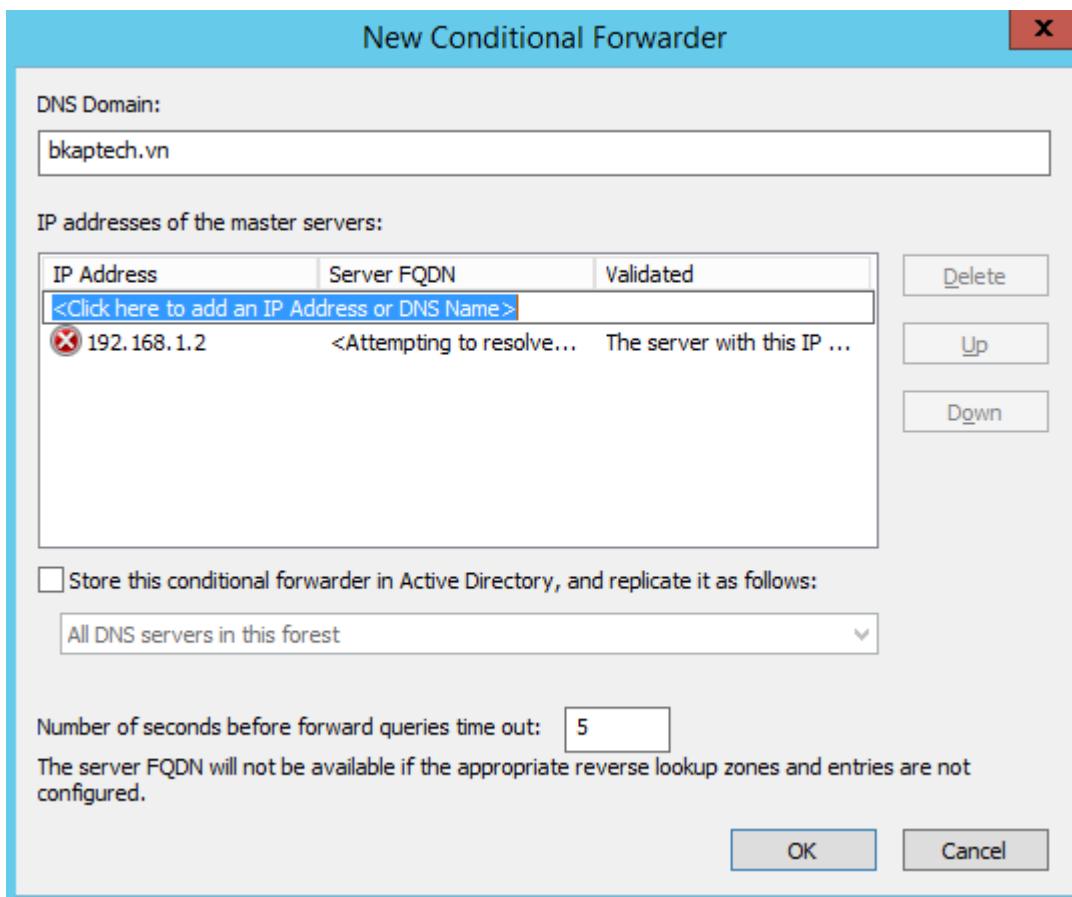
C:\Users\Administrator>

```

- Chuyển sang máy **BKAP-DC12-02**, thực hiện cấu hình **Conditional Forwarders**.
 - Trong cửa sổ **DNS Manager**, click chuột phải tại **Conditional Forwarder** , chọn **New Conditional Forwarder...**



- Tại cửa sổ **New Conditional Forwarder**, tại mục **DNS Domain**, nhập vào tên **bkaptech.vn** , tại mục **IP address**, nhập vào địa chỉ **192.168.1.2** (địa chỉ IP của máy *BKAP-DC12-01*), click vào **OK**.



- Thực hiện kiểm tra phân giải bằng câu lệnh nslookup bkaptech.vn.

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

C:\Users\Administrator>nslookup bkaptech.vn
Server: bkap-dc12-02.bachkhoa-aptech.com
Address: 192.168.1.10

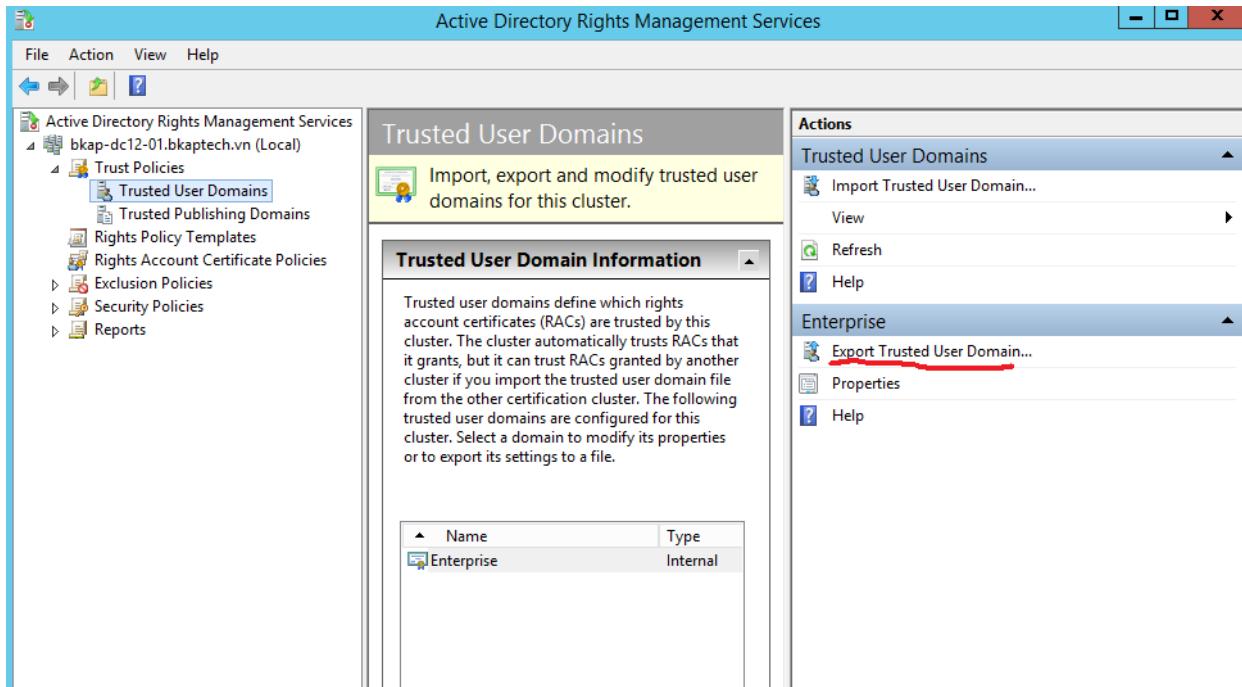
Non-authoritative answer:
Name: bkaptech.vn
Address: 192.168.1.2

C:\Users\Administrator>
```

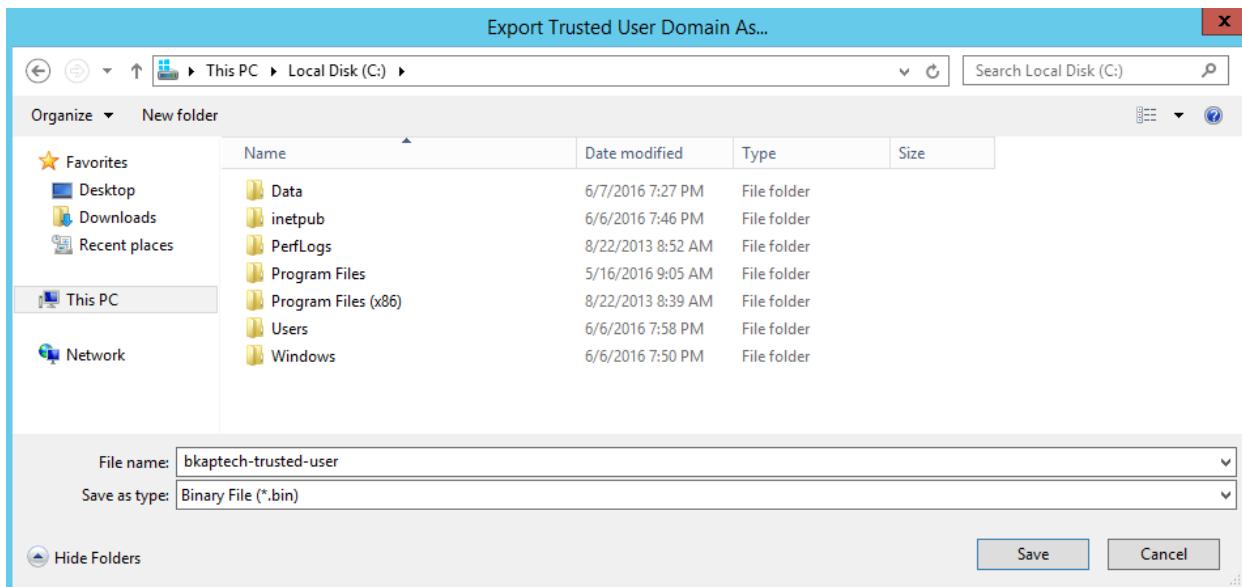
- Chuyển qua máy *BKAP-DC12-01* thực hiện cấu hình **Export Trusted User Domain Policy** và **Trusted Publishing Domain Policy**.

Để 2 RMS Server thuộc 2 domain có thể thiết lập quan hệ "trust" với nhau, trên mỗi RMS Server ta cần Import 2 Policy là *Trusted User Domain* và *Trusted Publishing Domain* được export từ *RMS Server đối tác*.

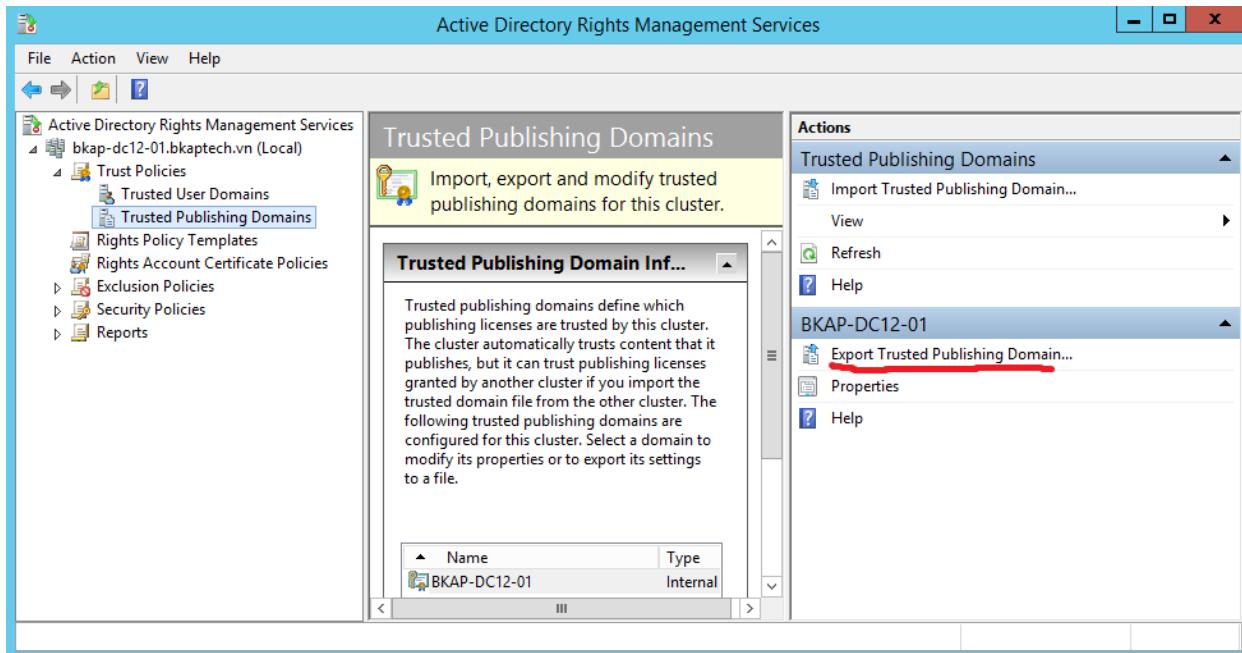
- Mở dịch vụ **AD RMS**, chọn vào **Trusted User Domains**, chọn vào **Export Trusted User Domain...**



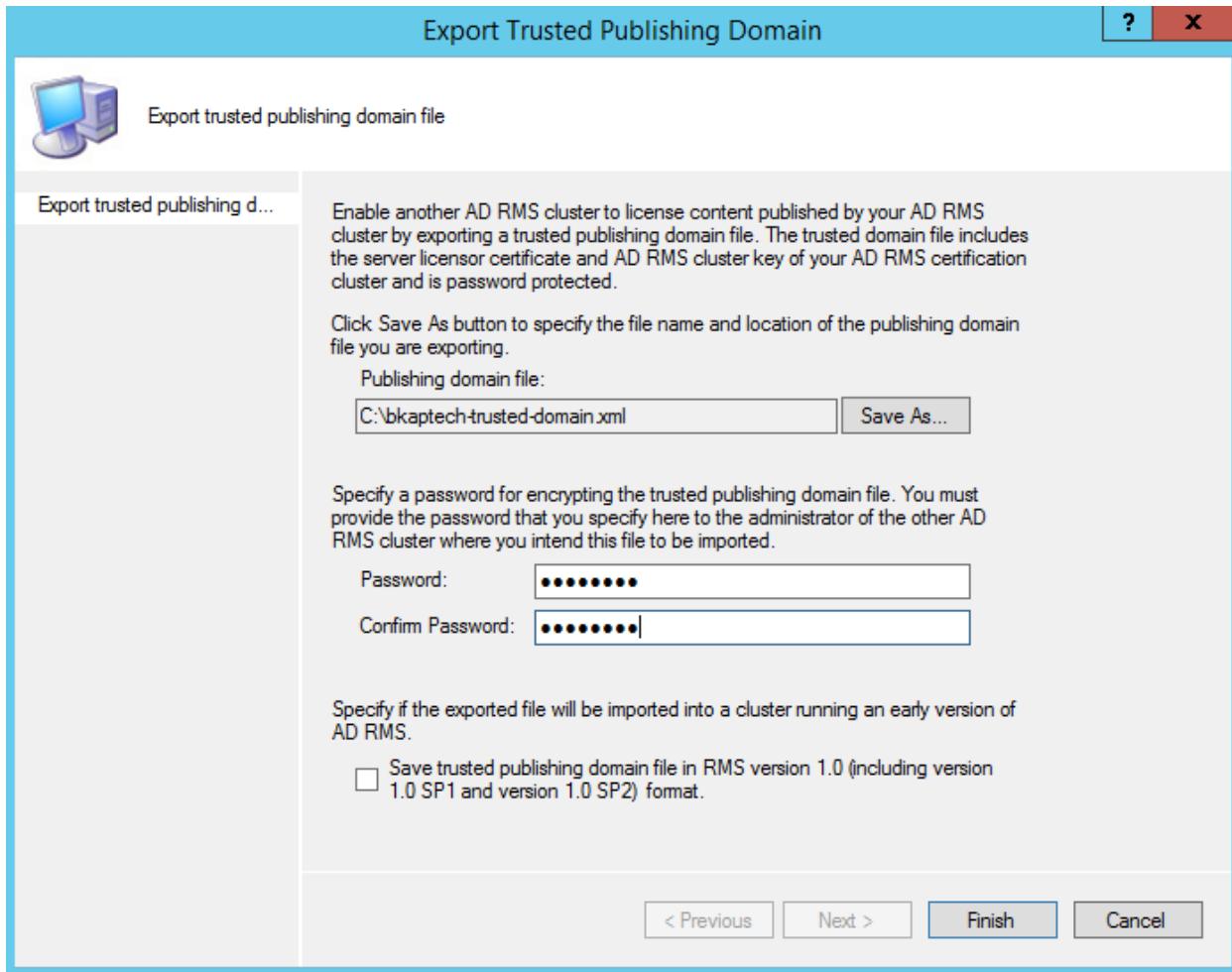
- Tại cửa sổ **Export Trusted User Domain...**, browse đến ô C, nhập vào tên *File name* : **bkaptech-trusted-user**, click vào **Save**.



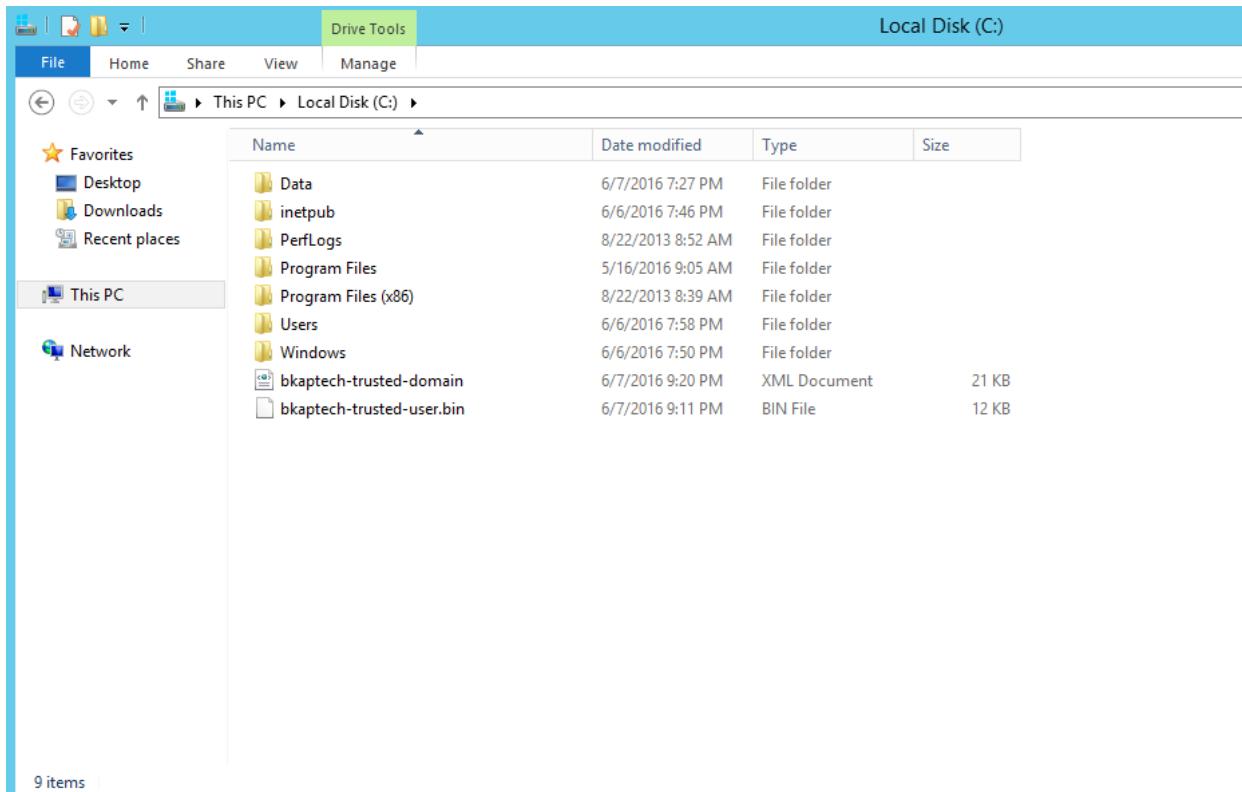
- Tại cửa sổ **AD RMS**, click chọn vào **Trusted Publishing Domains**, click vào **Export Trusted Publishing Domain...**



- Tại cửa sổ **Export Trusted Publishing Domain** , click vào **Save As...** , Browse đến ổ C , nhập vào tên tại mục *File name* : **bkaptech-trusted-domain** , click vào **Save** , nhập vào **Password => Finish.**

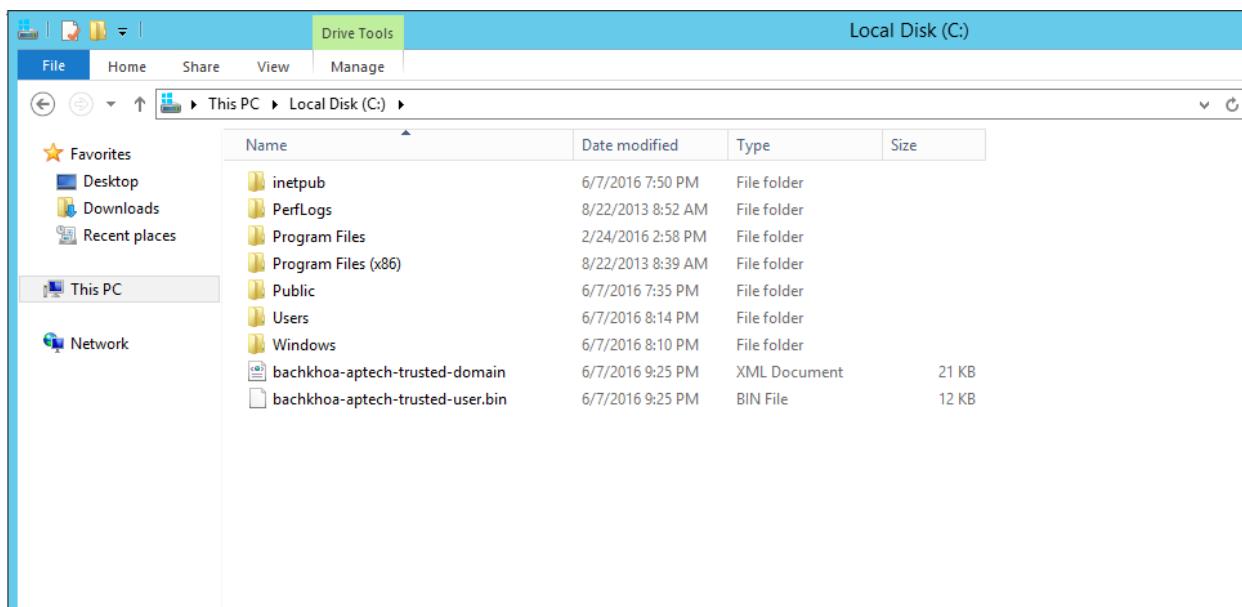


- Vào ô C kiểm tra.

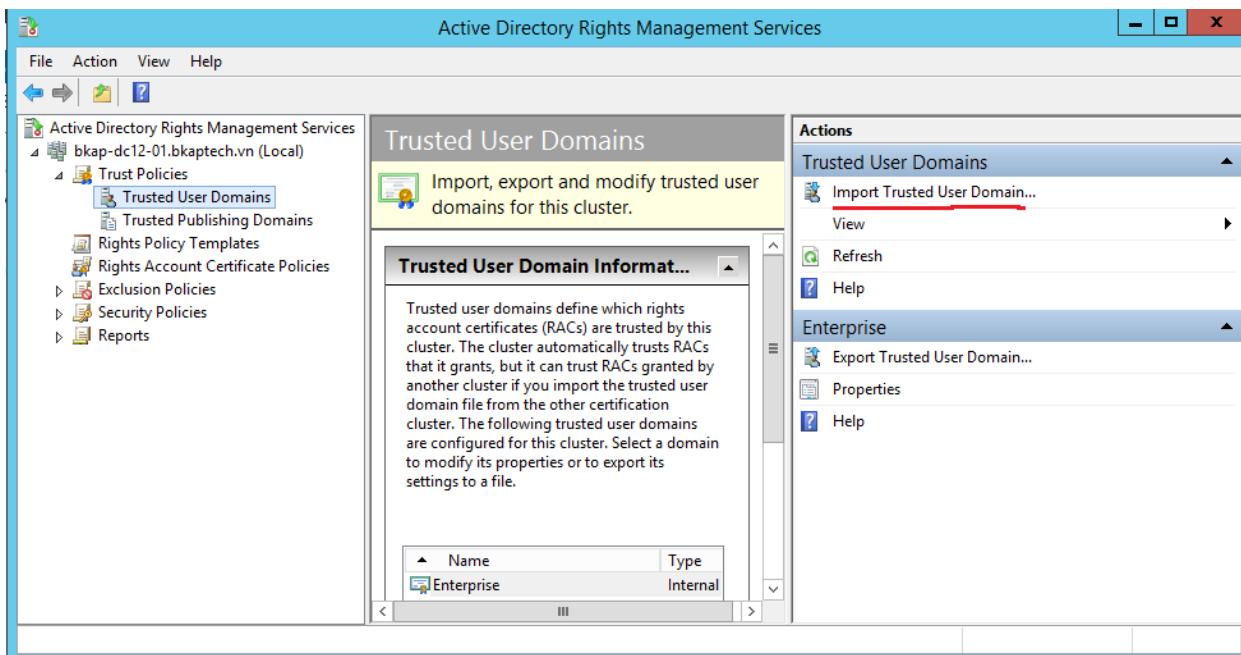


- Chuyển qua máy *BKAP-DC12-02*, thực hiện **Export Trusted User Domain Policy** và **Trusted Publishing Domain Policy**.(làm tương tự các bước ở trên).

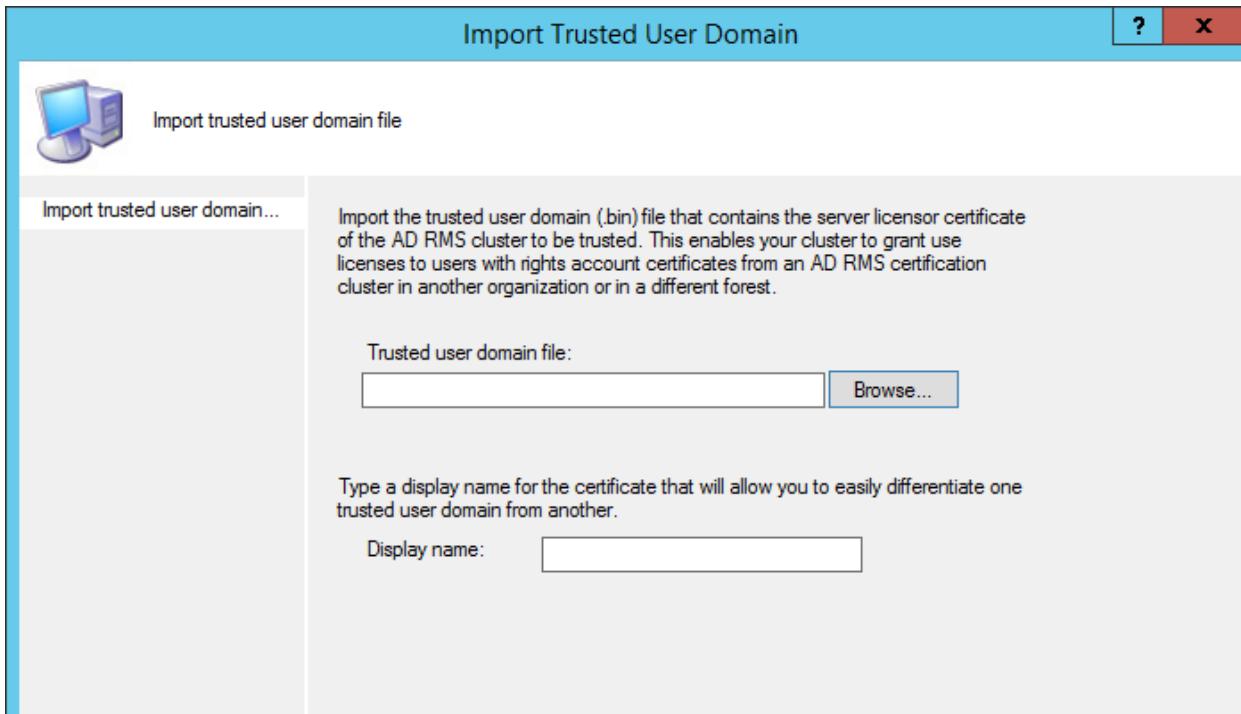
⇒ Kết quả như sau:



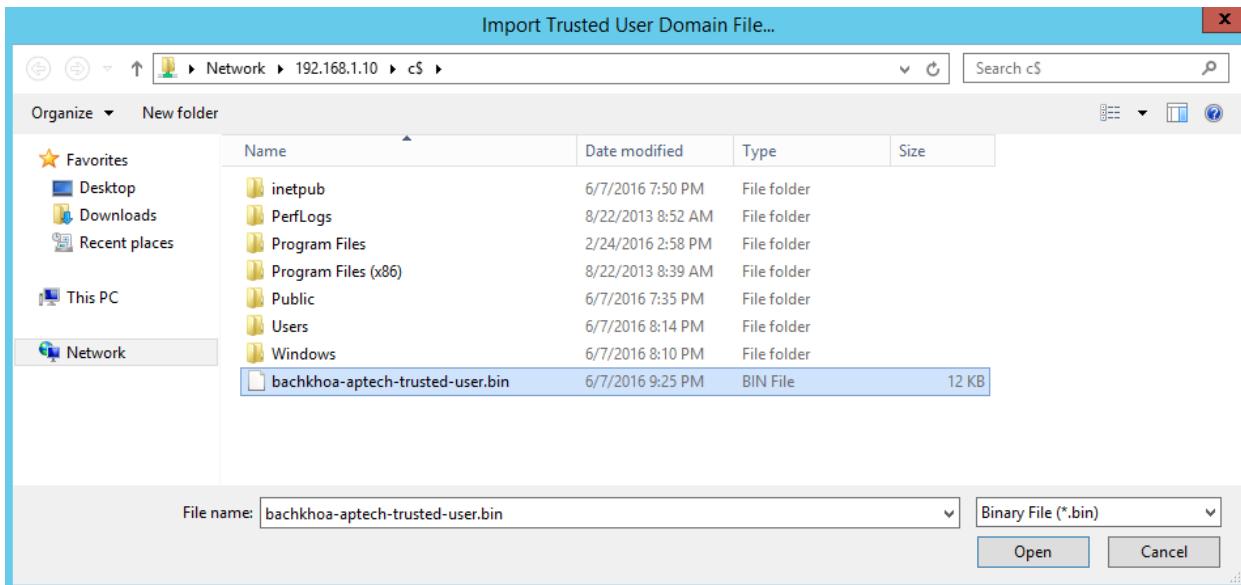
- Chuyển sang máy *BKAP-DC12-01* , thực hiện **Import Trusted User Domain Policy** và **Trust Publishing Domain Policy**.
 - Trong cửa sổ **AD RMS**, click chọn vào **Trusted User Domains**, chọn vào **Import Trusted User Domain...**



- Tại cửa sổ Import Trusted User Domain , click vào Browse...

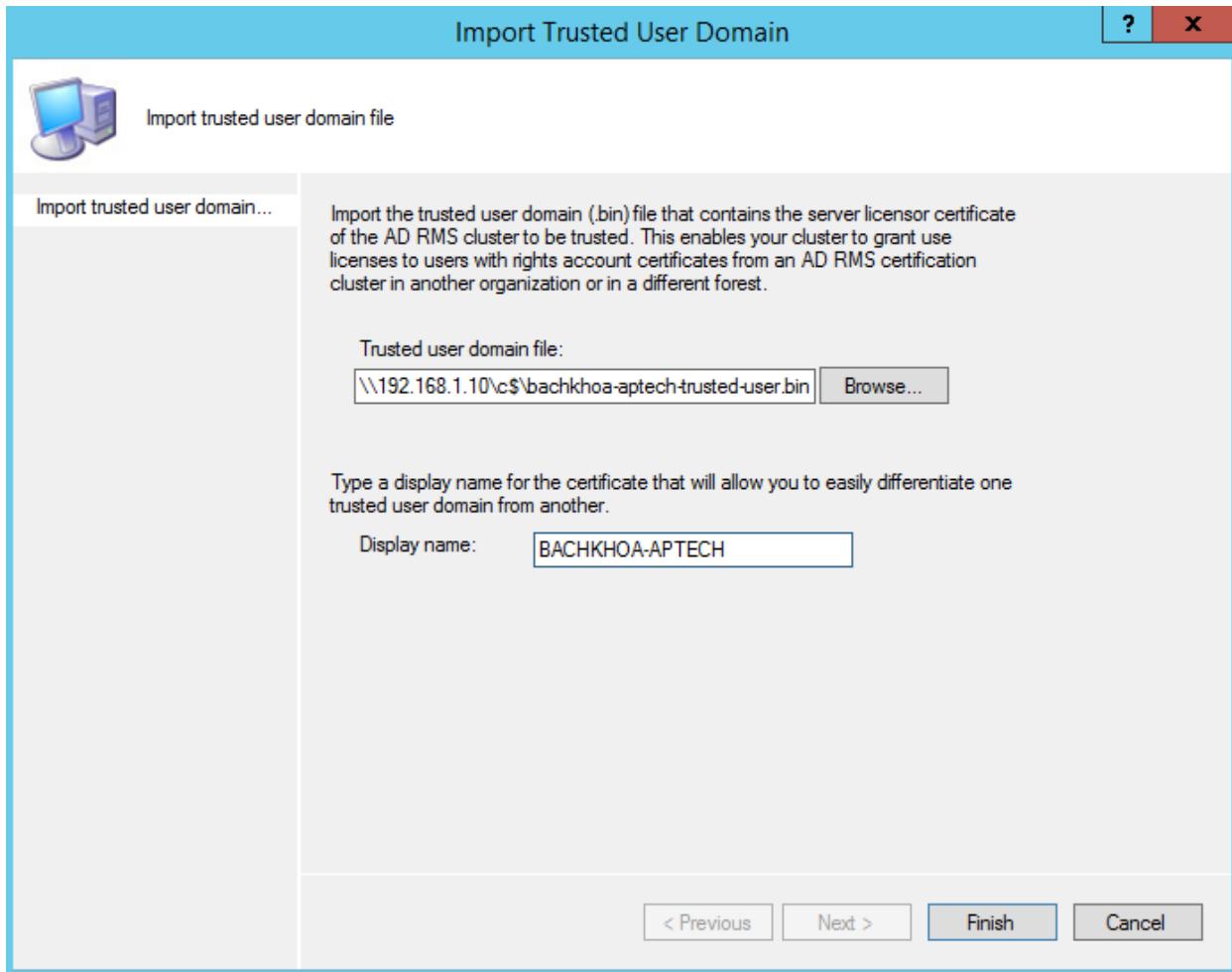


- Tại cửa sổ Import Trusted User Domain File...., nhập vào đường dẫn \\192.168.1.10\C\$ (địa chỉ IP của máy BKAP-DC12-02) , chọn file **bachkhoa-aptech-trusted-user.bin** => Open.

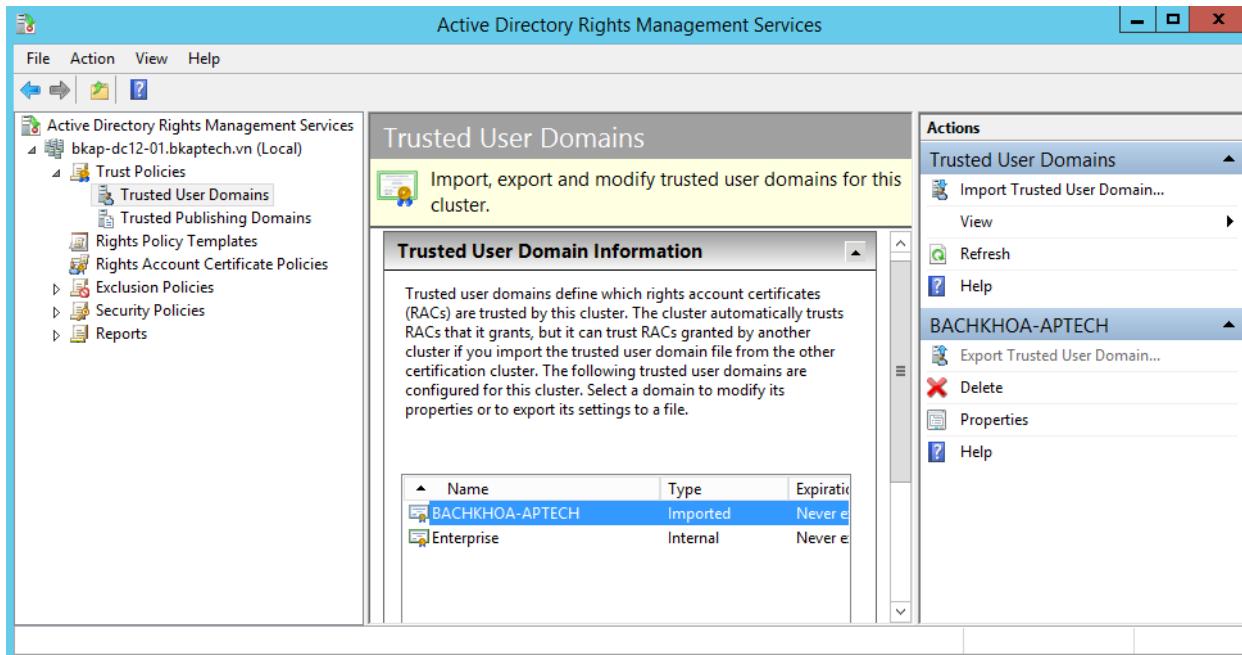


- Tại mục **Display name** , nhập vào tên **BACHKHOA-APTECH**.

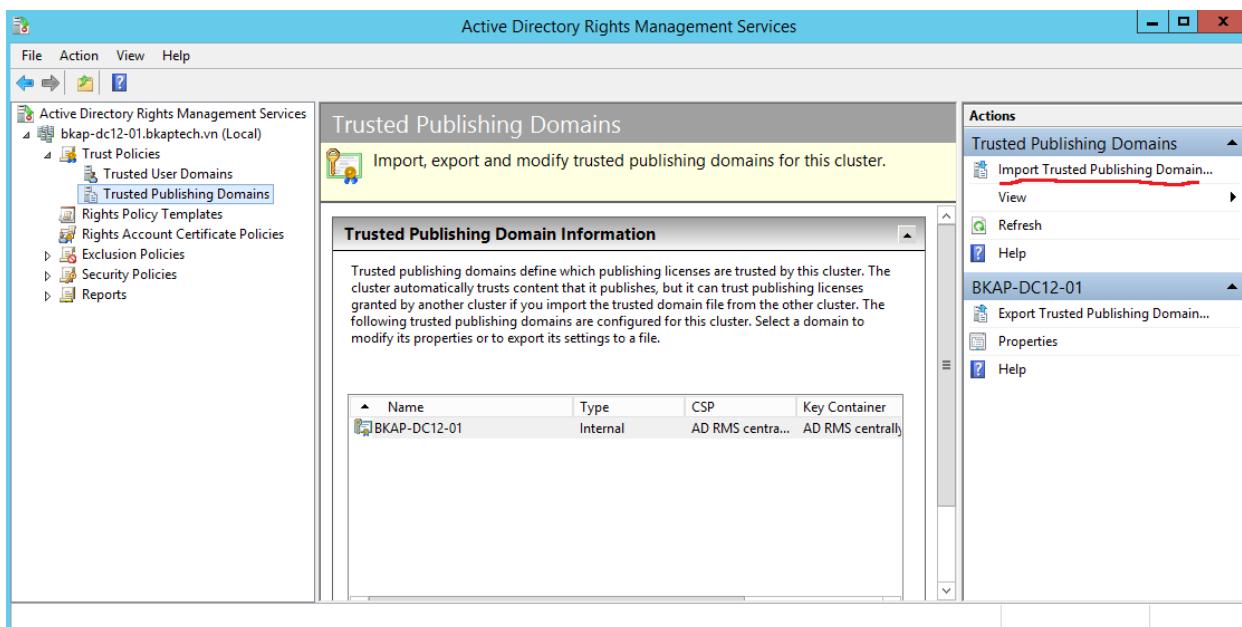
⇒ **Finish.**



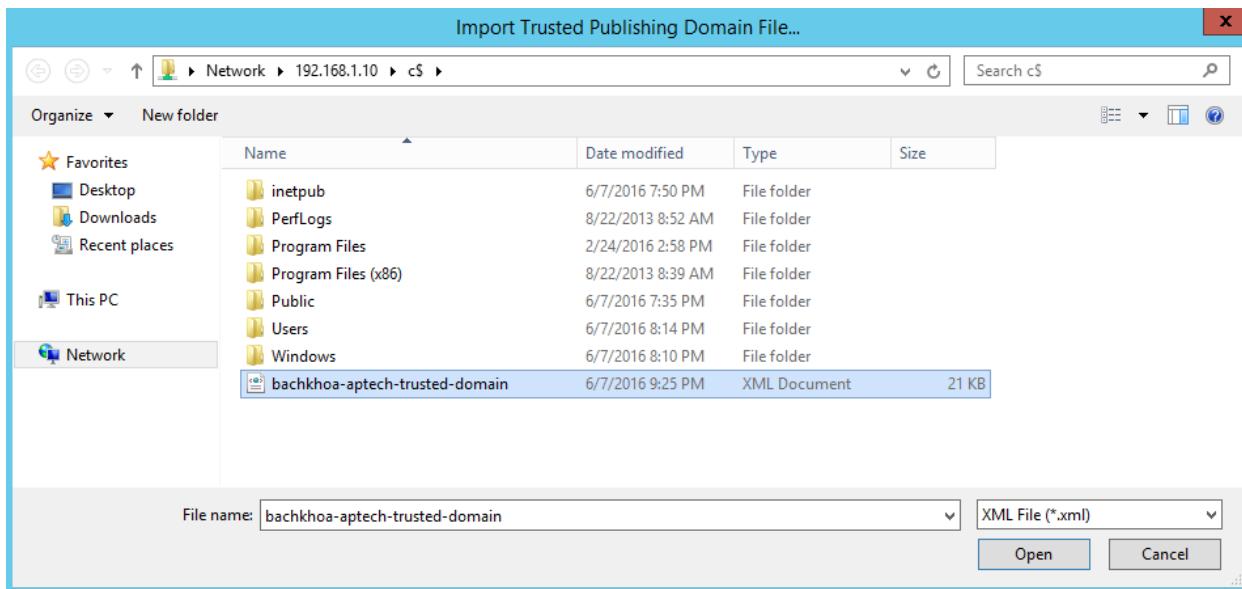
- Kiểm tra Trusted User Domain đã được *import* thành công.



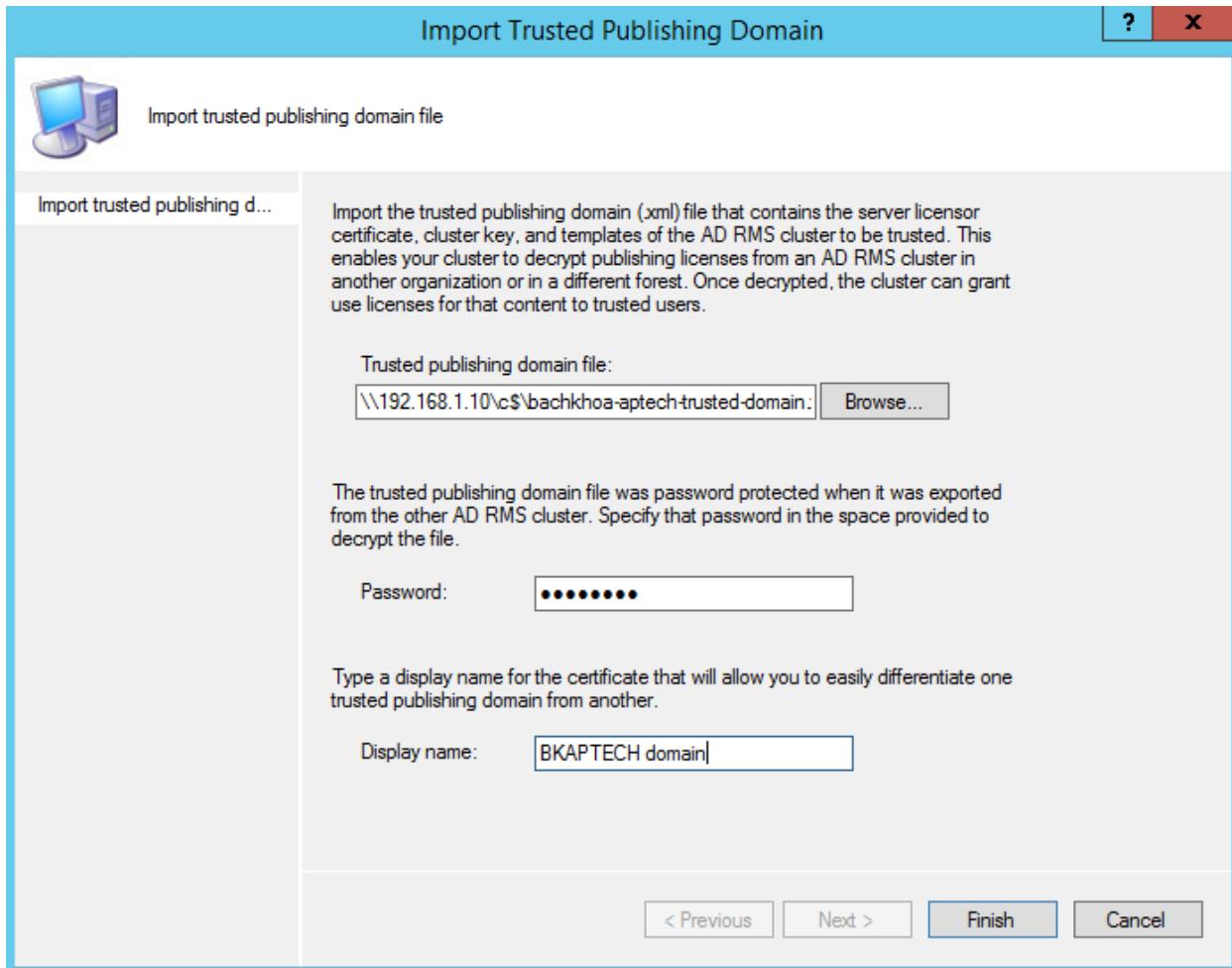
- Tại cửa sổ AD RMS, click chọn vào Trusted Publishing Domains , click chọn vào Import Trusted Publishing Domains.



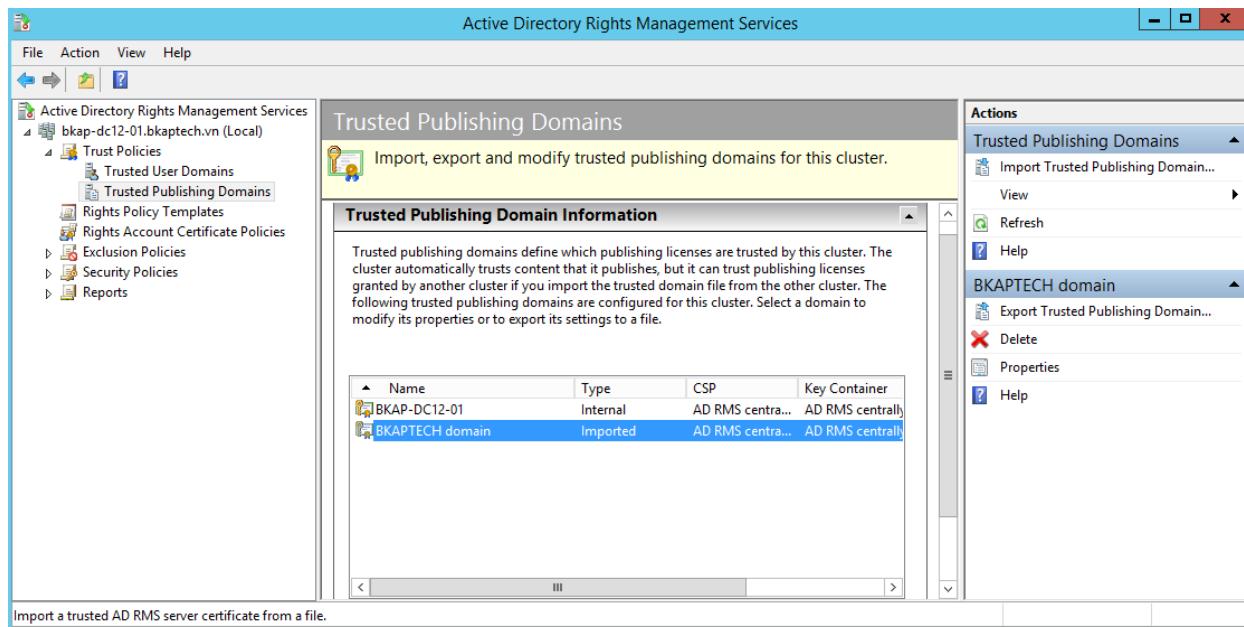
- Tại cửa sổ **Import Trusted Publishing Domain**, click vào **Browse...**, chọn đến file **bachkhoa-aptech-trusted-domain**, click vào **Open**.



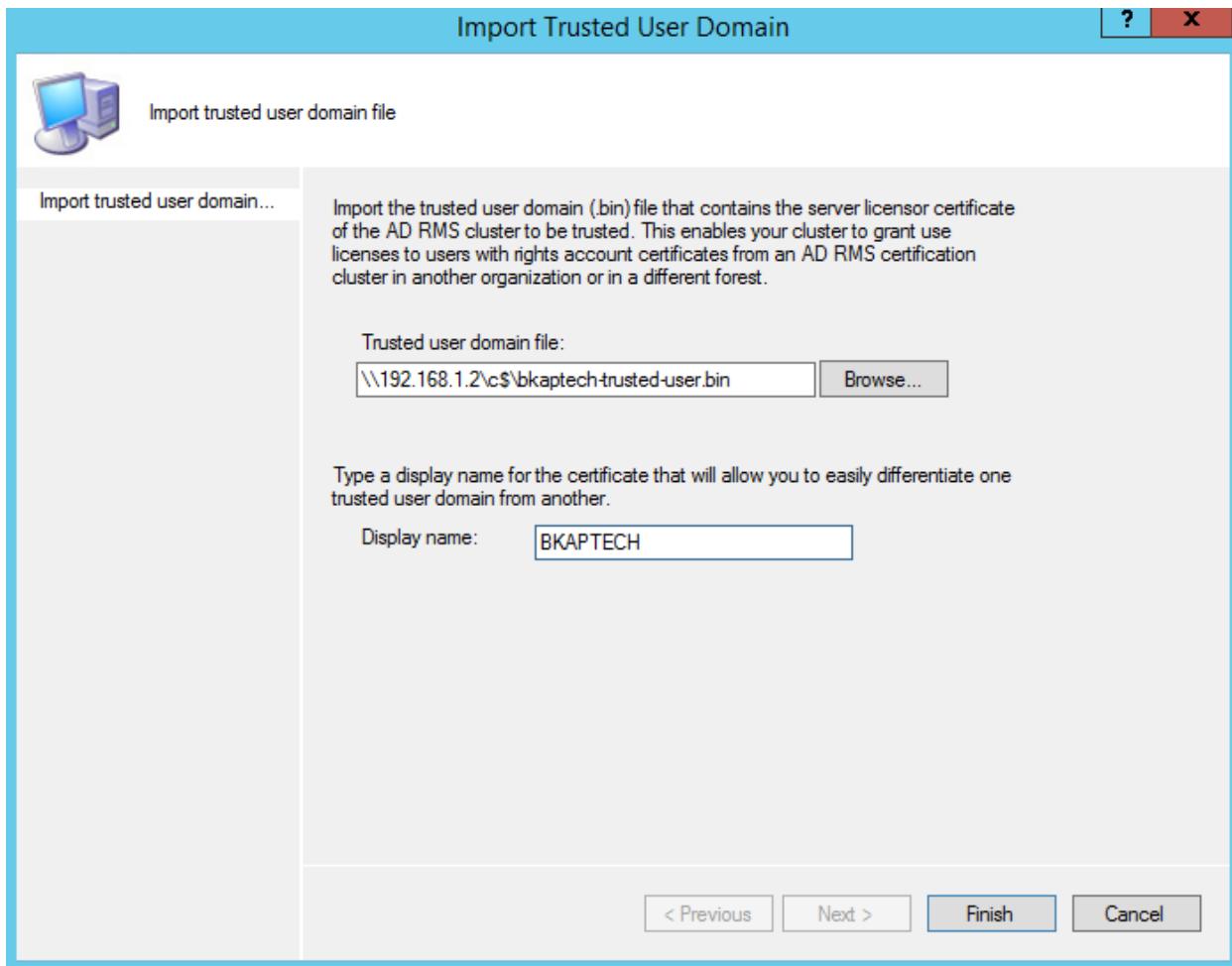
- Tại cửa sổ **Import Trusted Publishing Domain**, nhập vào *password* và tên tại **Display name**.



- Kiểm tra Trusted Publishing Domain đã được *import* thành công.



- Chuyển qua máy BKAP-DC12-02, thực hiện cấu hình **Import Trusted User Domain Policy** và **Trust Publishing Domain Policy**.(làm tương tự các bước trên).



Import Trusted Publishing Domain

 Import trusted publishing domain file

Import trusted publishing d...

Import the trusted publishing domain (xml) file that contains the server licensor certificate, cluster key, and templates of the AD RMS cluster to be trusted. This enables your cluster to decrypt publishing licenses from an AD RMS cluster in another organization or in a different forest. Once decrypted, the cluster can grant use licenses for that content to trusted users.

Trusted publishing domain file:

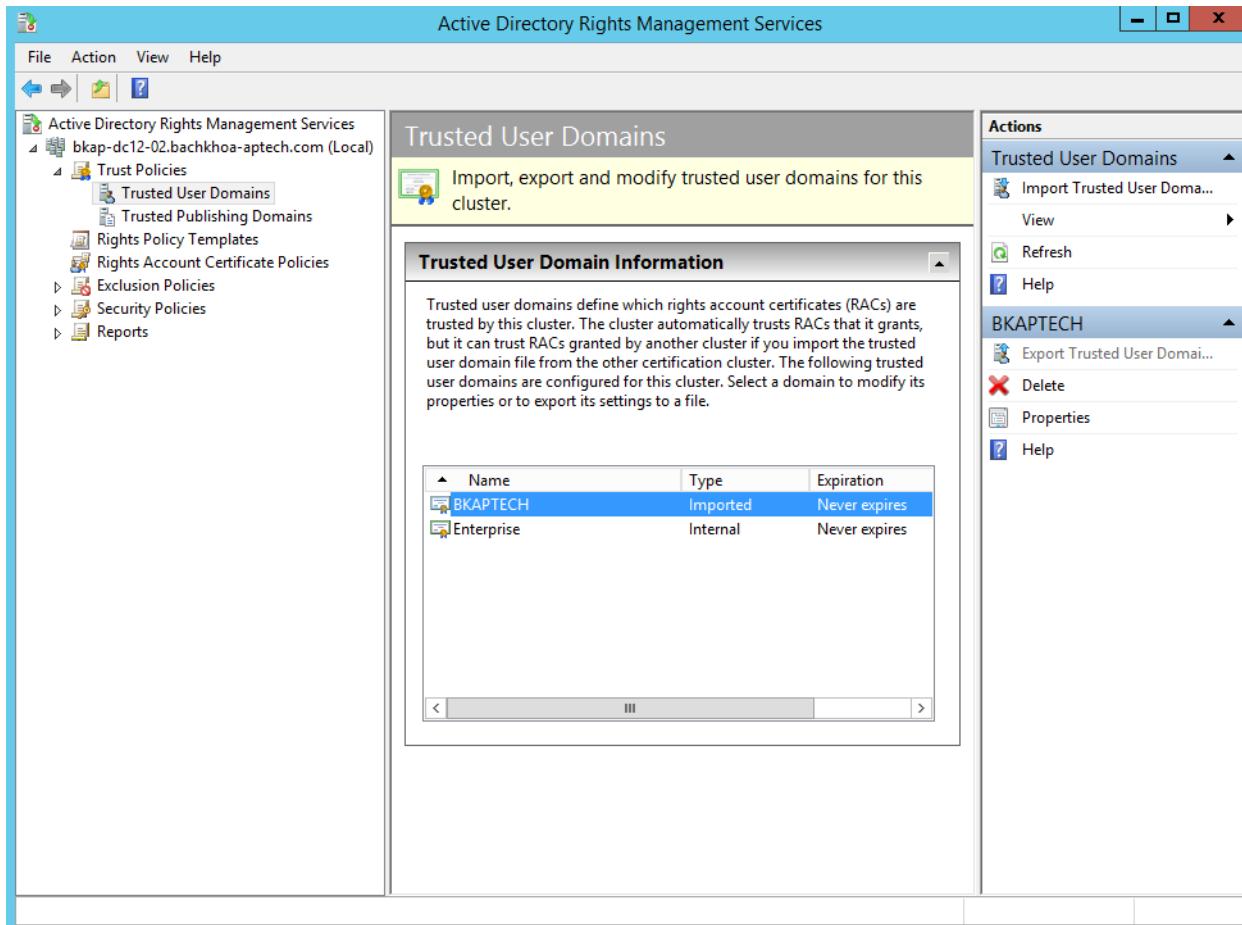
The trusted publishing domain file was password protected when it was exported from the other AD RMS cluster. Specify that password in the space provided to decrypt the file.

Password:

Type a display name for the certificate that will allow you to easily differentiate one trusted publishing domain from another.

Display name:

⇒ Kết quả như sau:

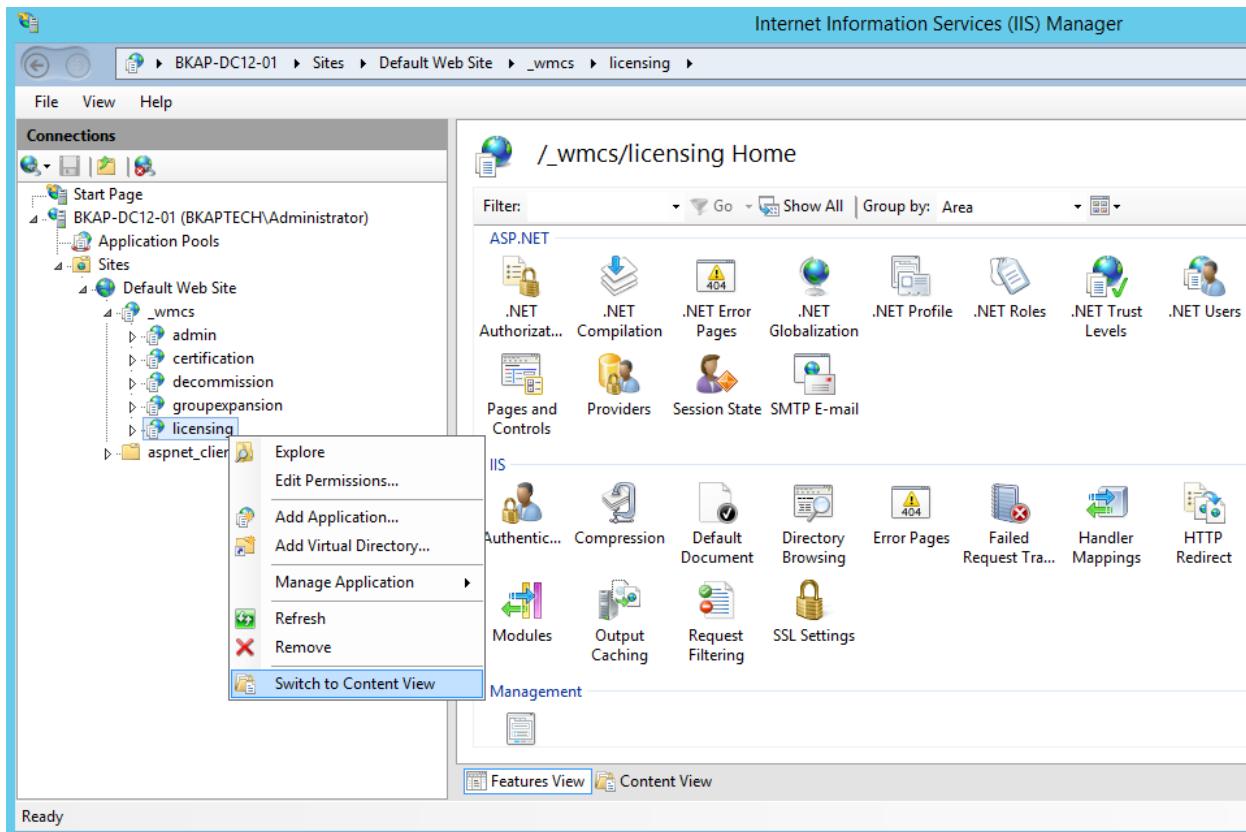


The screenshot shows the 'Trusted Publishing Domains' section of the AD RMS management console. The left navigation pane shows a tree structure with 'Active Directory Rights Management Services' selected, followed by 'bkap-dc12-02.bachkhoa-aptech.com (Local)' and 'Trust Policies'. Under 'Trust Policies', 'Trusted Publishing Domains' is selected. The main pane displays the 'Trusted Publishing Domain Information' table:

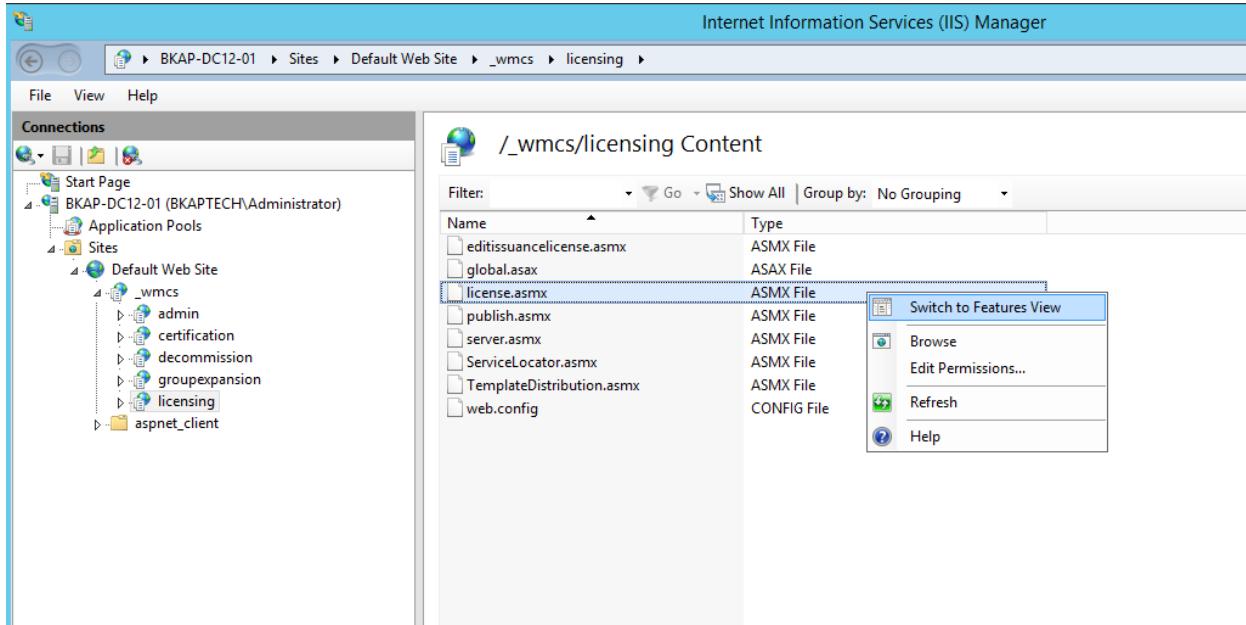
Name	Type	CSP
BACHKHOA-APTECH domain	Imported	AD RMS centra...
BKAP-DC12-02	Internal	AD RMS centra...

The right pane contains an 'Actions' menu with options like 'Import Trusted Publishing ...', 'View', 'Refresh', 'Help', 'Export Trusted Publishing ...', 'Delete', 'Properties', and 'Help'.

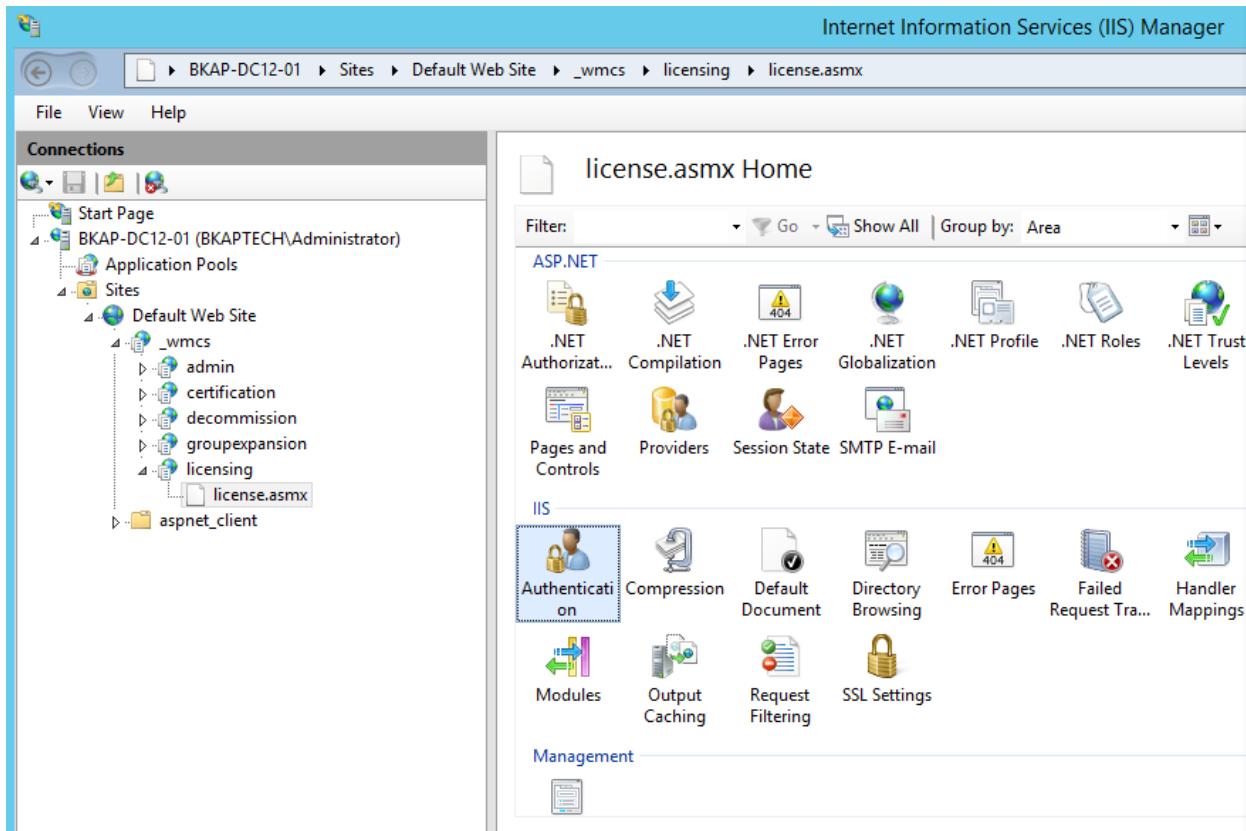
- Chuyển sang máy BKAP-DC12-01, thực hiện cấu hình **Anonymous access** cho RMS Licensor Server.
 - Mở **Internet Information Service (IIS) Manager**, click vào **Default Web Site** / chọn tiếp vào **_wmcs / licensing** , click chuột phải tại đây, chọn **Switch to Content View**.



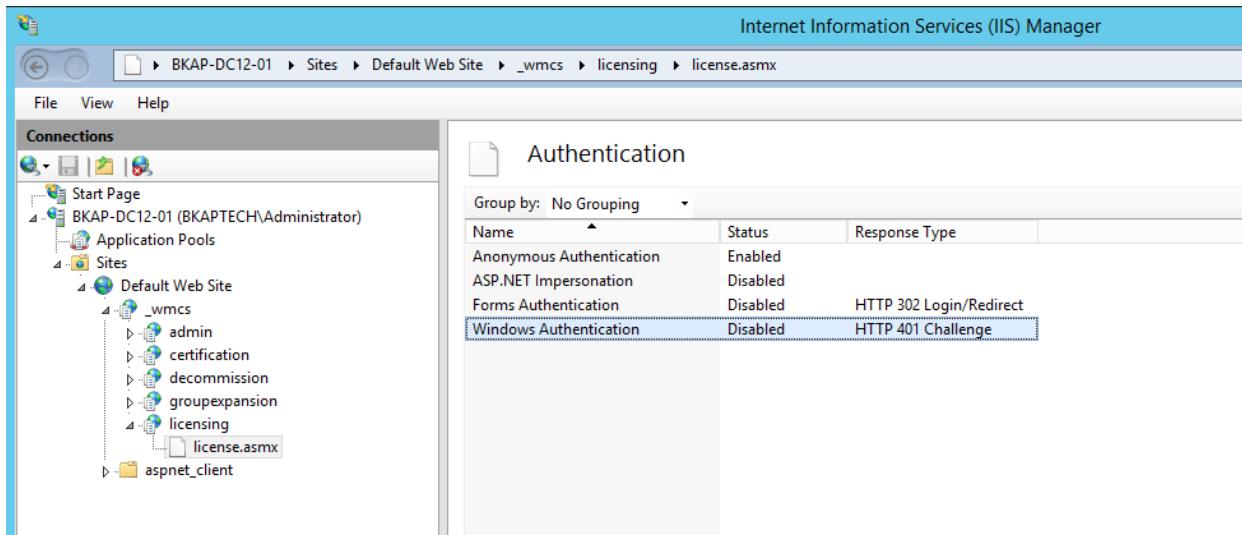
- Trong cửa sổ **/_wmcs/licensing Content**, click chuột phải vào **license.ashx**, chọn **Switch to Features View**.



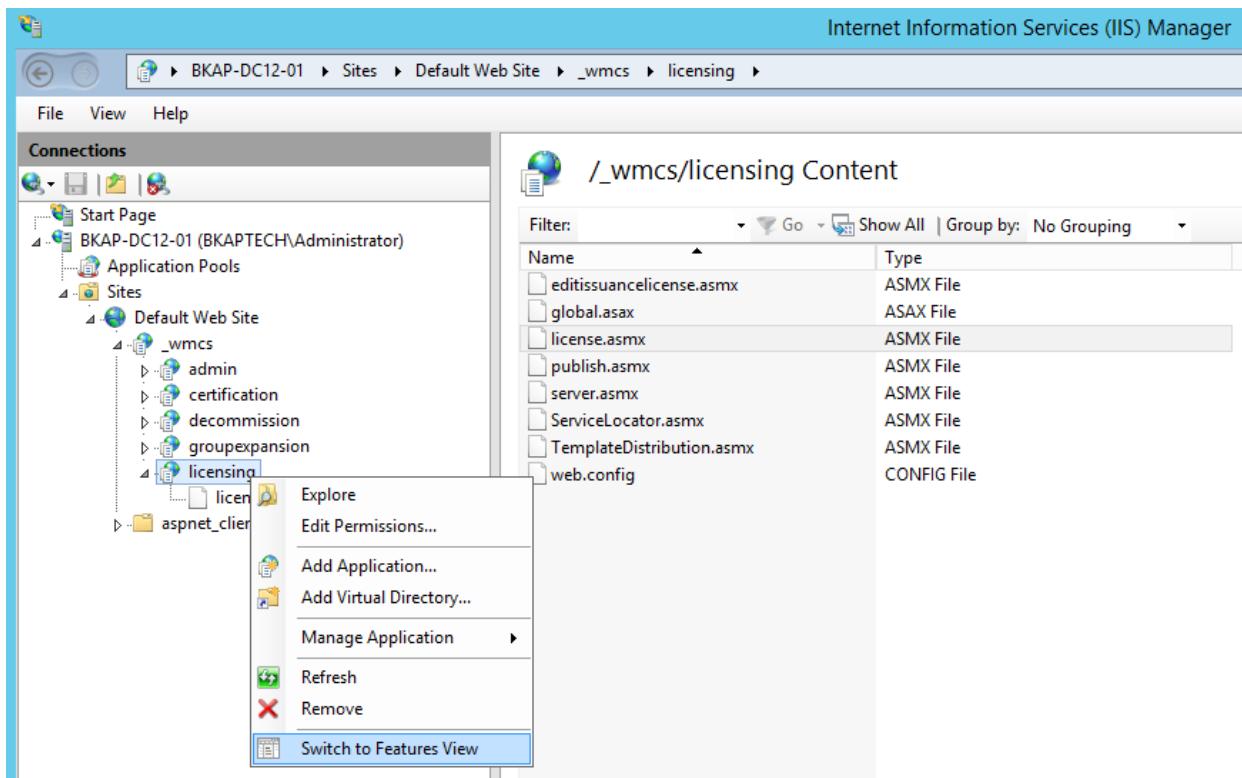
- Tại cửa sổ **license.ashx Home**, chọn vào **Authentication**.



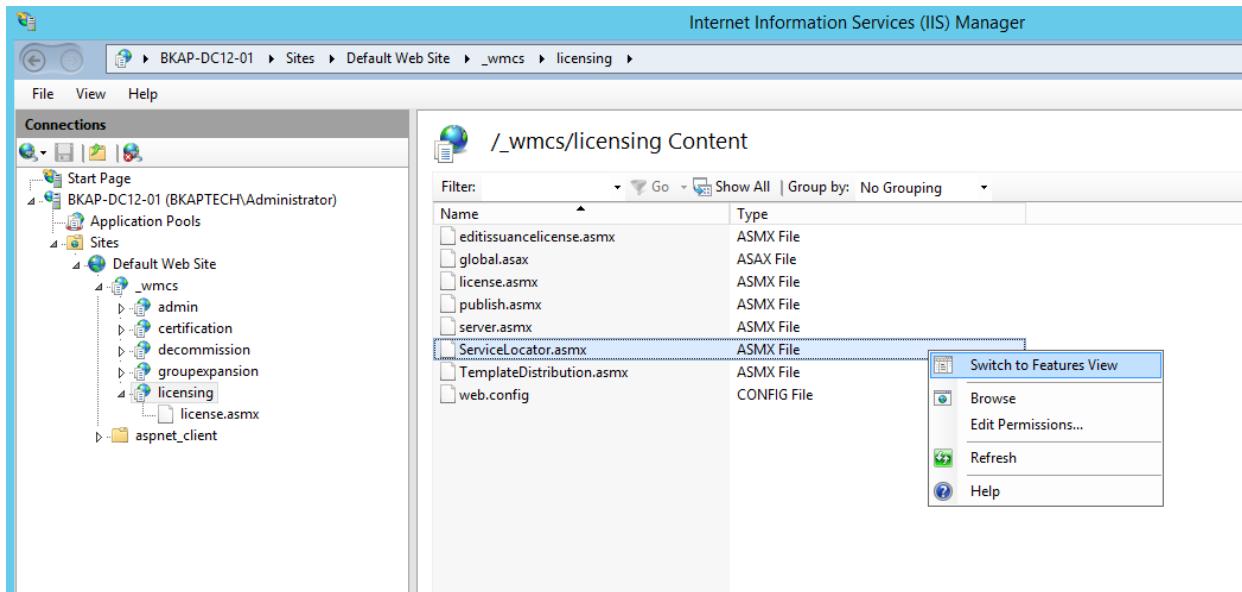
- Tại cửa sổ **Authentication**, thực hiện **Enable Anonymous Authentication, Disable Windows Authentication.**



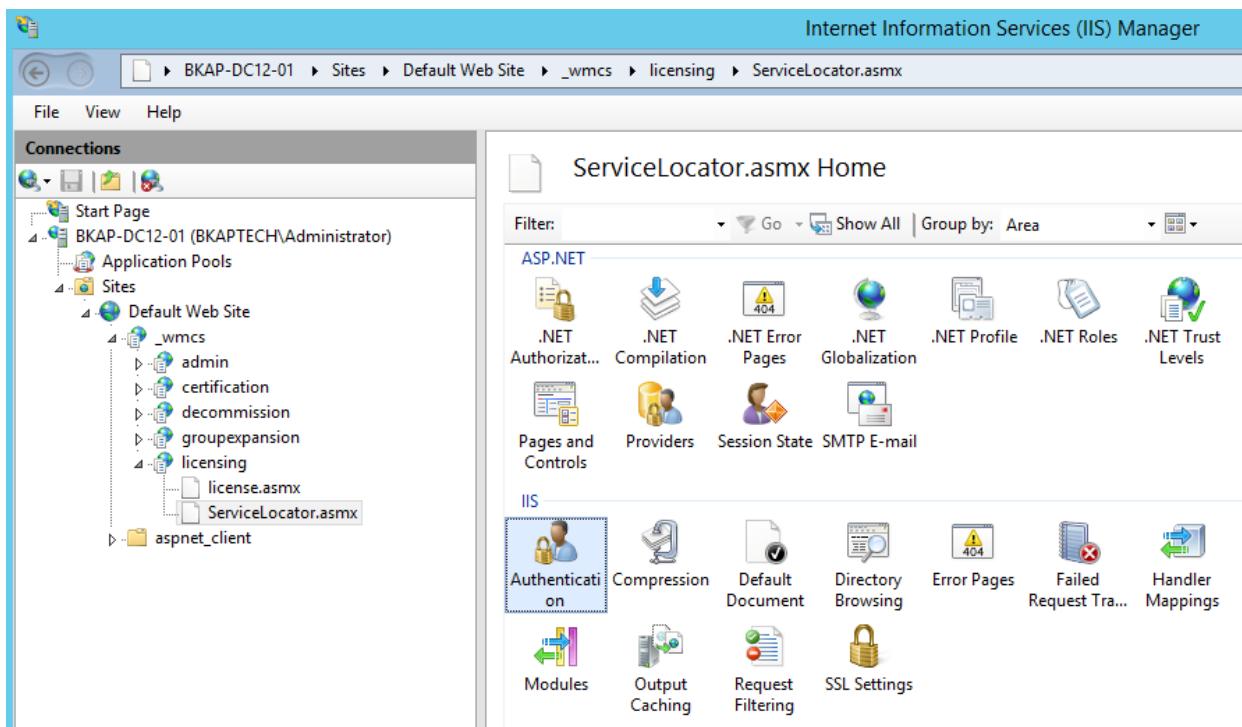
- Click chuột phải tại **licensing** , chọn **Switch to Features View**.



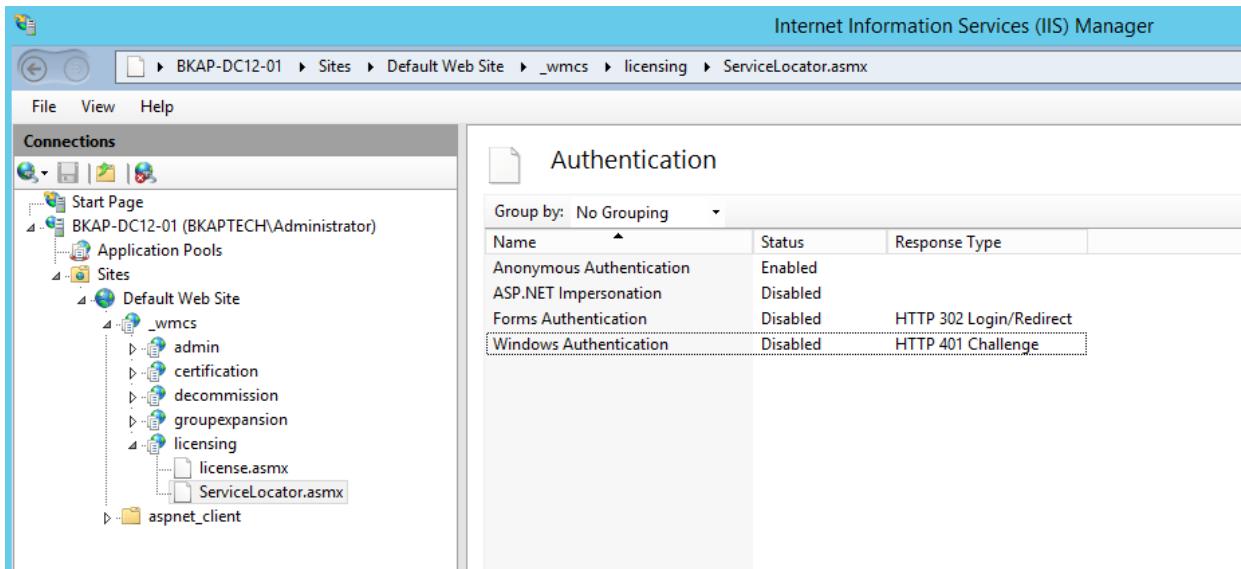
- Trong cửa sổ **_wmcs/licensing Content**, click chuột phải tại **ServiceLocator.ashx**, chọn vào **Switch to Features View**.



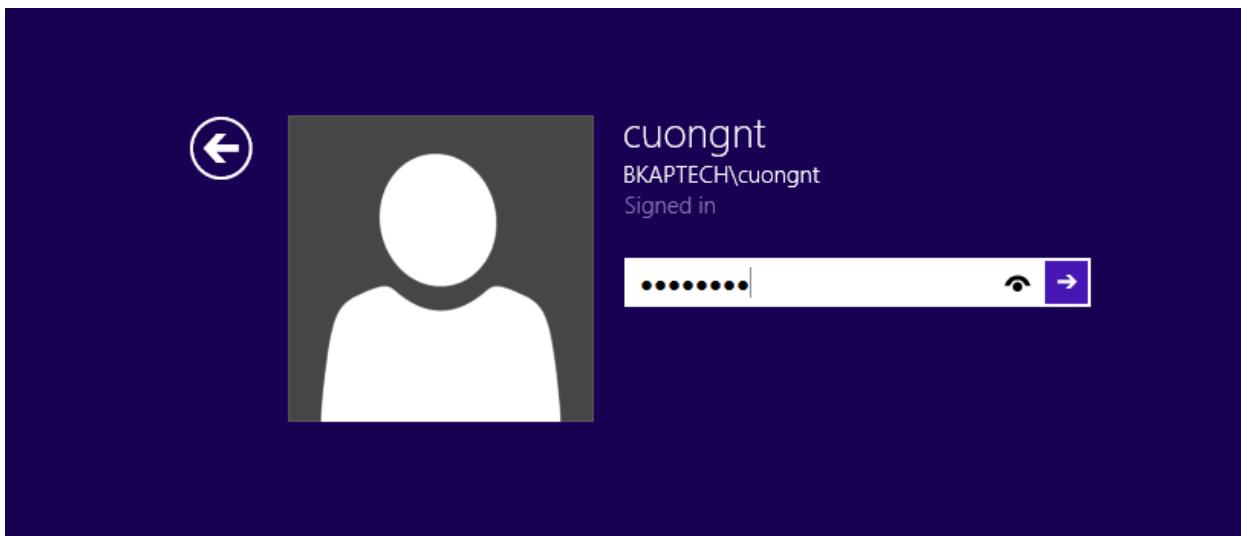
- Tại cửa sổ **ServiceLocator.ashx Home**, chọn vào **Authentication**.



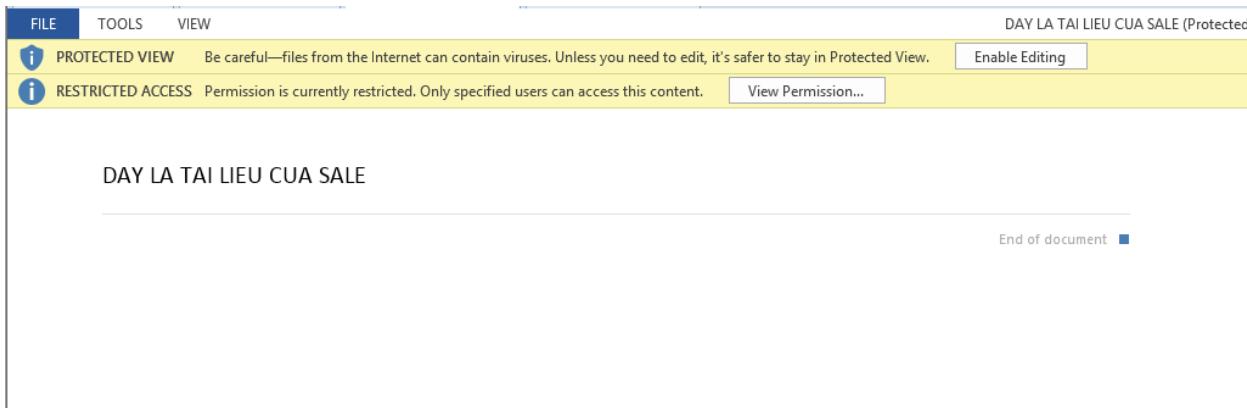
- Trong cửa sổ **Authentication**, thực hiện **Enable Anonymous Authentication, Disable Windows Authentication**.



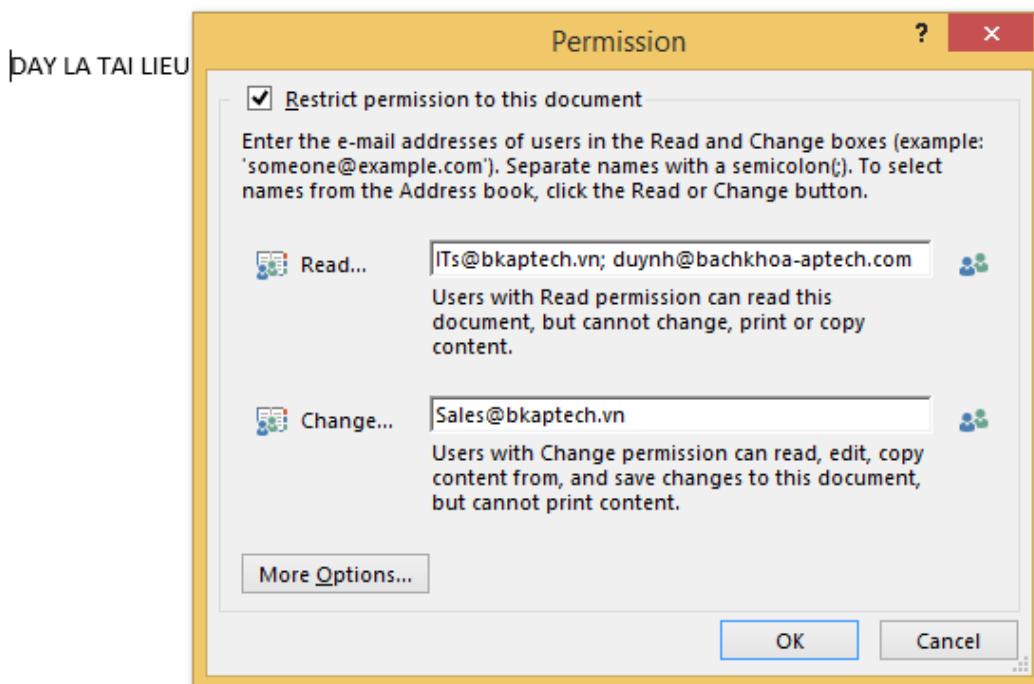
- Chuyển sang máy Client *BKAP-WRK08-01*, đăng nhập lại bằng user **cuongnt**.



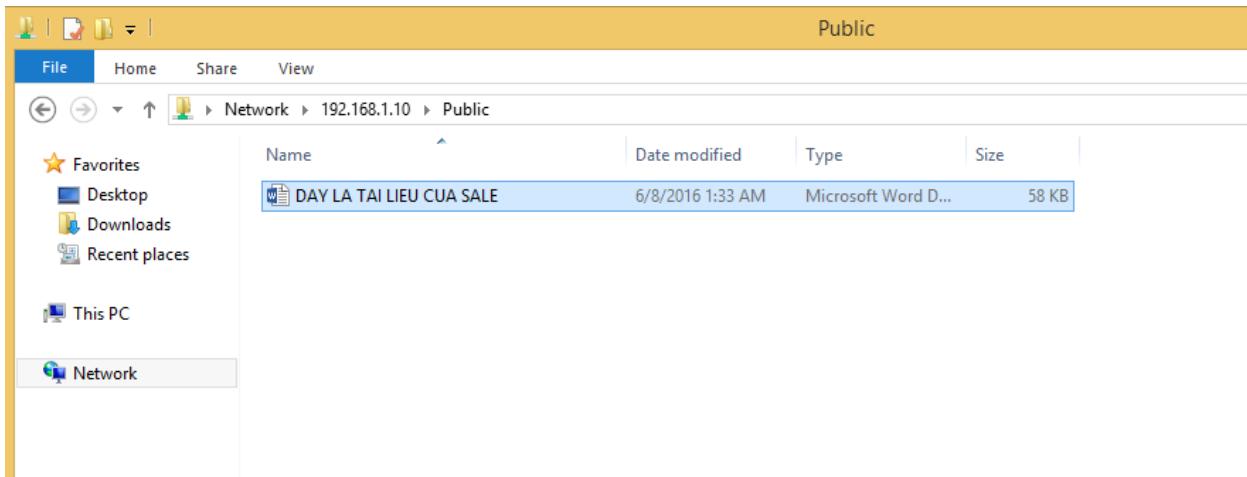
- Mở tài liệu do user **cuongnt** tạo ra (xem lại Phần 1).



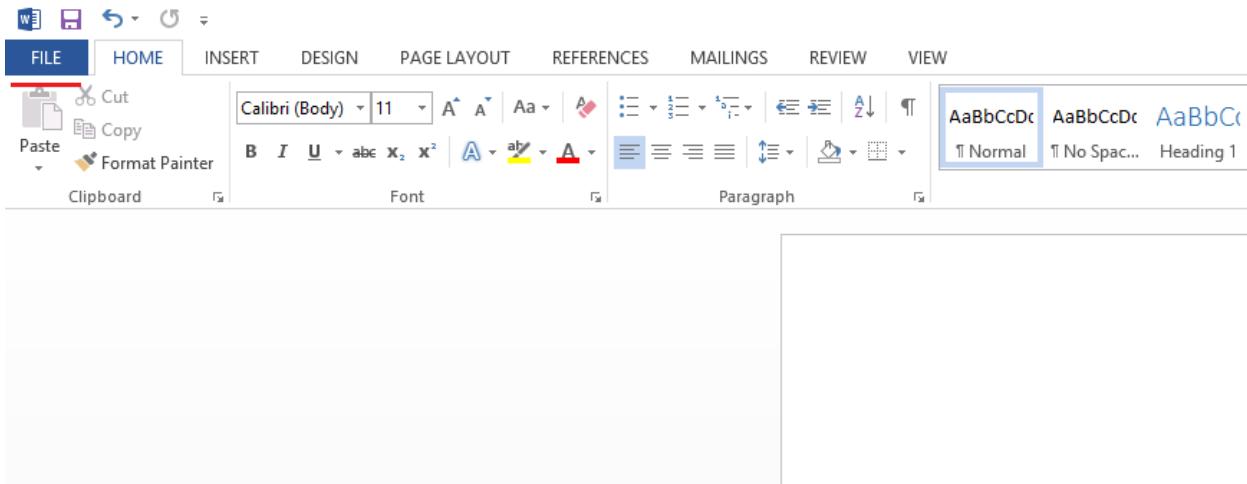
- Điều chỉnh **Permission**, gán thêm user **duynh** thuộc domain **bachkhoa-aptech.com**. Thực hiện *save* lại tài liệu này.



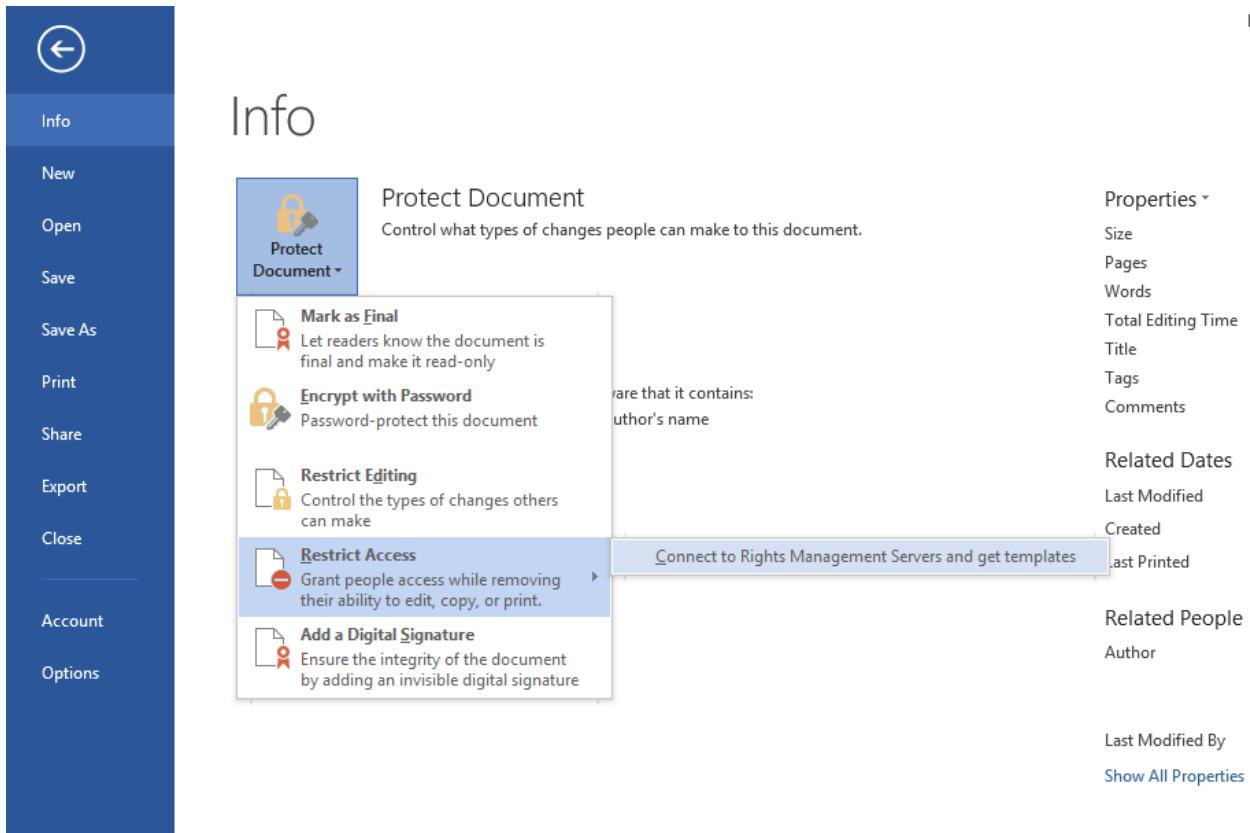
- Truy cập vào thư mục **Public** trên máy *BKAP-DC12-02*.
 - Copy file *Tai lieu cua Sale* qua máy *BKAP-DC12-02*.



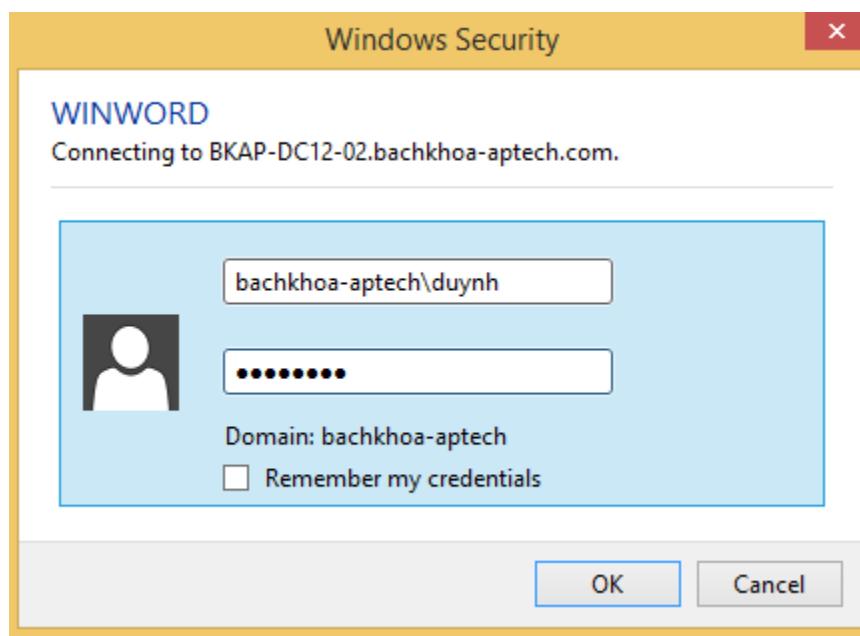
- Chuyển qua máy Client *BKAP-WRK08-02*, đăng nhập tài khoản **duynh**, thực hiện kiểm tra.
- Mở **Microsoft Office**, chọn vào **File**.



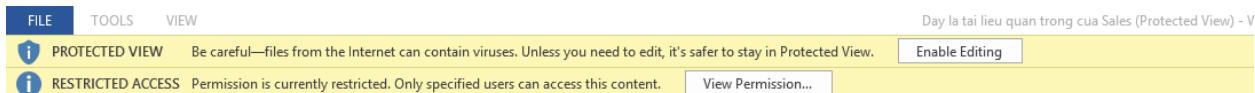
- Trong mục **Info**, chọn vào **Protect Document / Restrict Access / Connect to Rights Management Servers and get templates**.



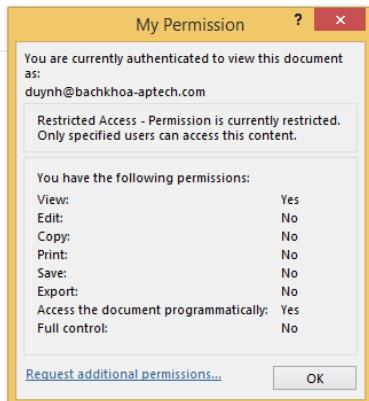
- Nhập vào user **duynh**.



- Truy cập vào thư mục **Public** trên máy *BKAP-DC12-02* , thực hiện mở file tài liệu đã được copy từ bước trên.
 - Kiểm tra **permission** của user **duynh**. (user **duynh** có quyền xem tài liệu này).



Day la tai lieu quan trong cua Sales



5.3 Cấu hình Active Directory Rights Management Services – P3

1.Yêu cầu bài Lab:

+ Cấu hình AD RMS kết hợp với **Dynamic Access Control (DAC)** để tự động bảo vệ các tài liệu nhạy cảm trong doanh nghiệp.

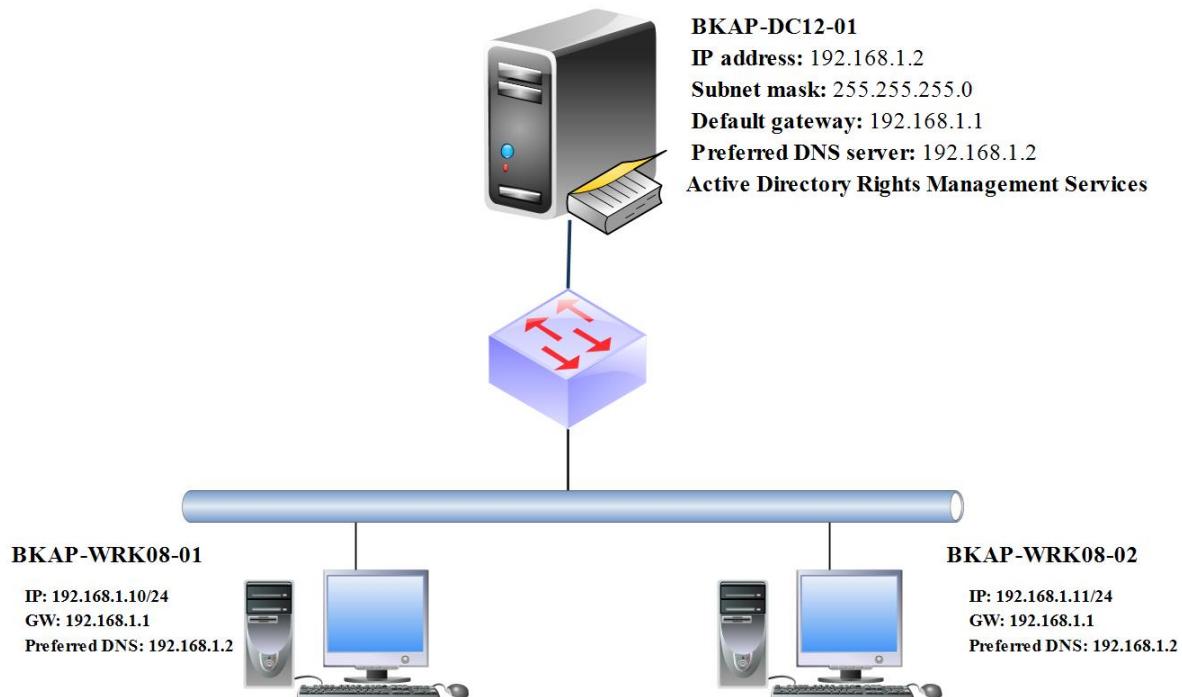
2.Yêu cầu chuẩn bị:

- + Máy *BKAP-DC12-01*: đã nâng cấp lên *Domain Controller* quản lý miền **bkaptech.vn**.
- + Máy Client *BKAP-WRK08-01*: đã Join vào miền **bkaptech.vn** , cài đặt phần mềm **Office 2013**.

3.Mô hình Lab:

HỆ THỐNG ĐÀO TẠO CNTT QUỐC TẾ BACHKHOA-APTECH

Cài đặt và cấu hình AD RMS (Phân 3)

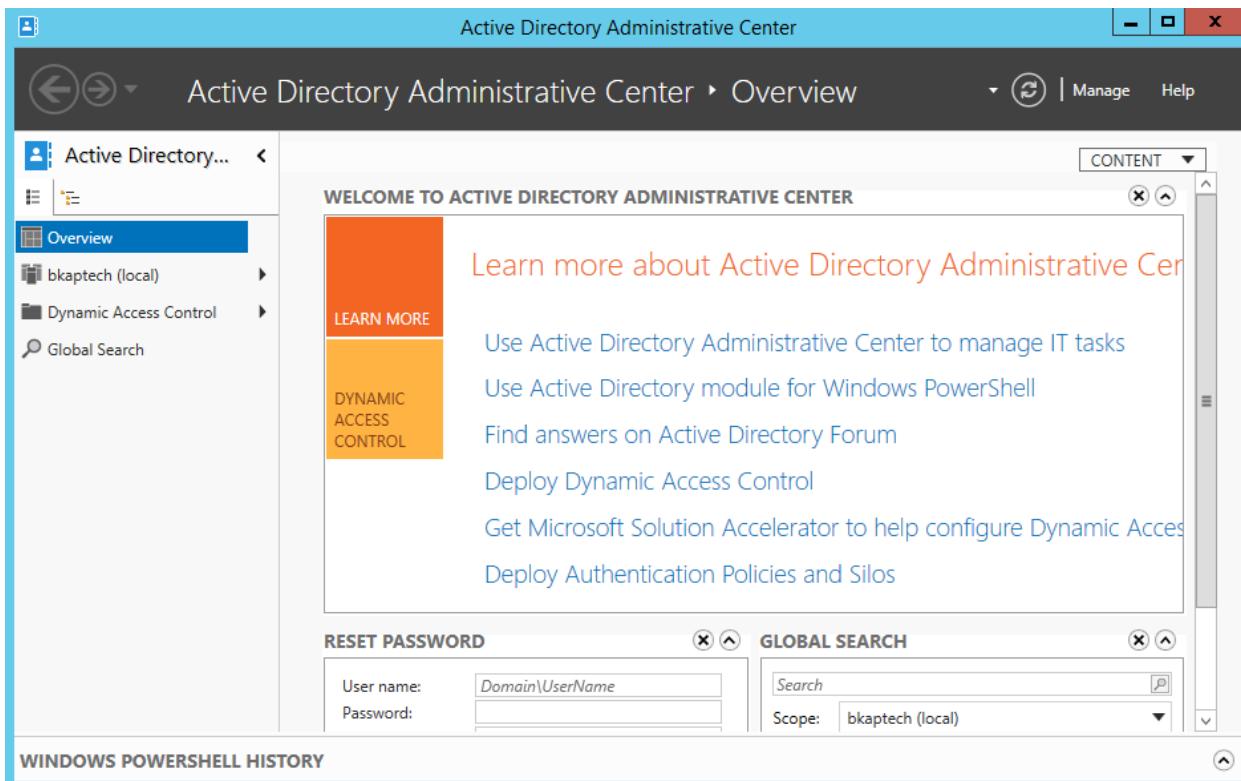


Sơ đồ địa chỉ như sau:

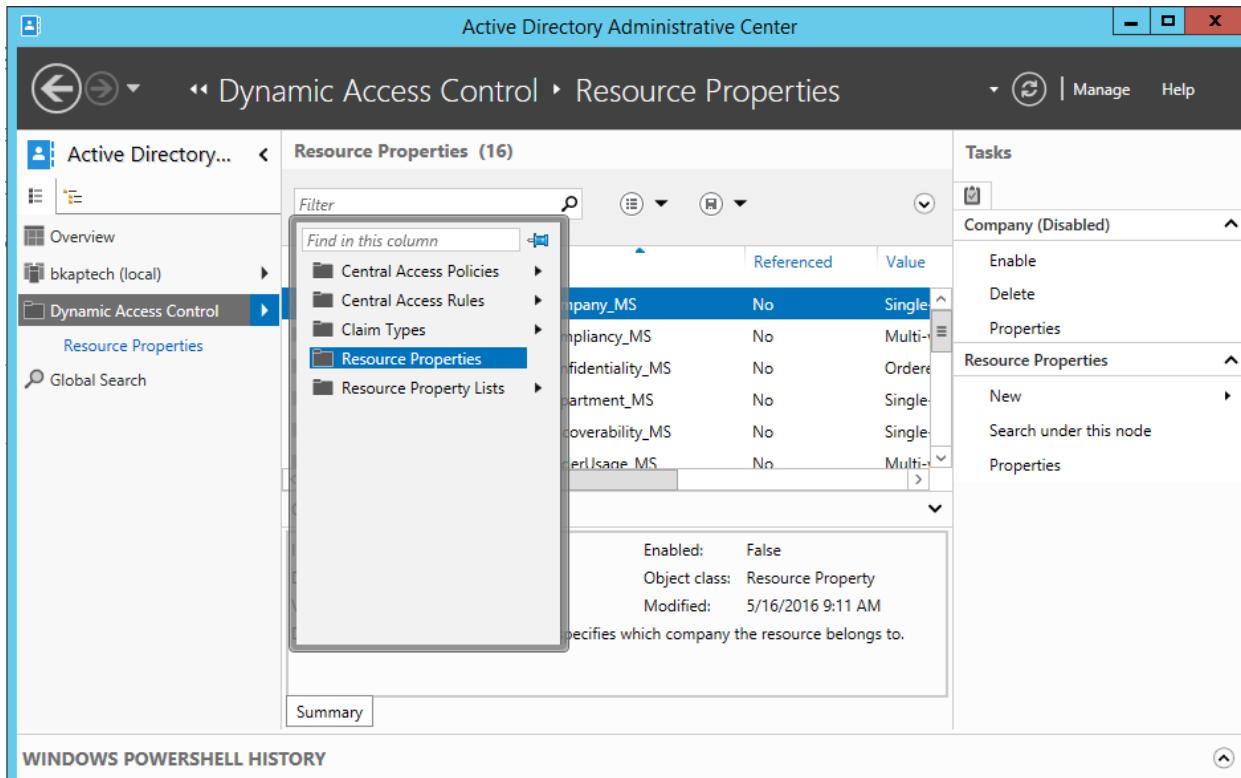
Thông số	BKAP-DC12-01	BKAP-WRK08-01
IP address	192.168.1.2	192.168.1.10
Subnet Mask	255.255.255.0	255.255.255.0
Gateway	192.168.1.1	192.168.1.1
DNS Server	192.168.1.2	192.168.1.2

Hướng dẫn chi tiết:

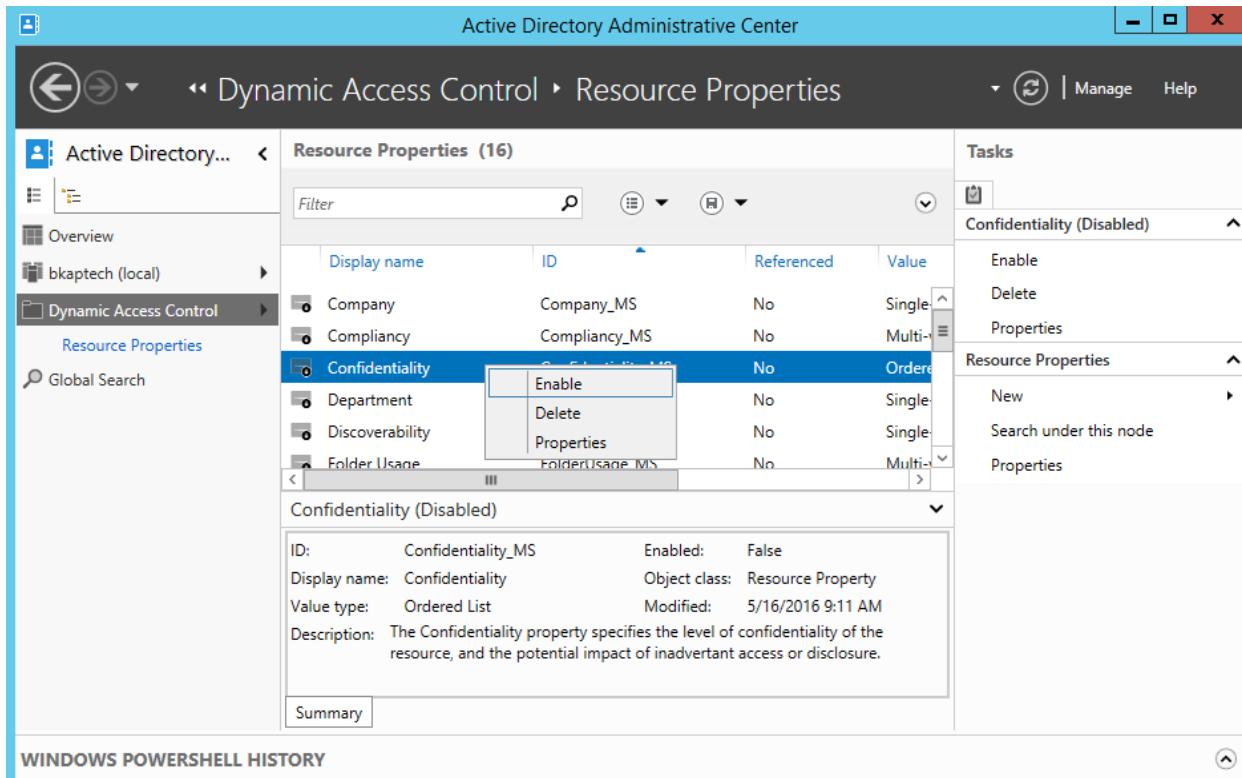
- Trên máy *BKAP-DC12-01*, thực hiện cấu hình **Enable Resource Properties**.
 - Vào **Server Manager / Tools / Active Directory Administrative Center**.



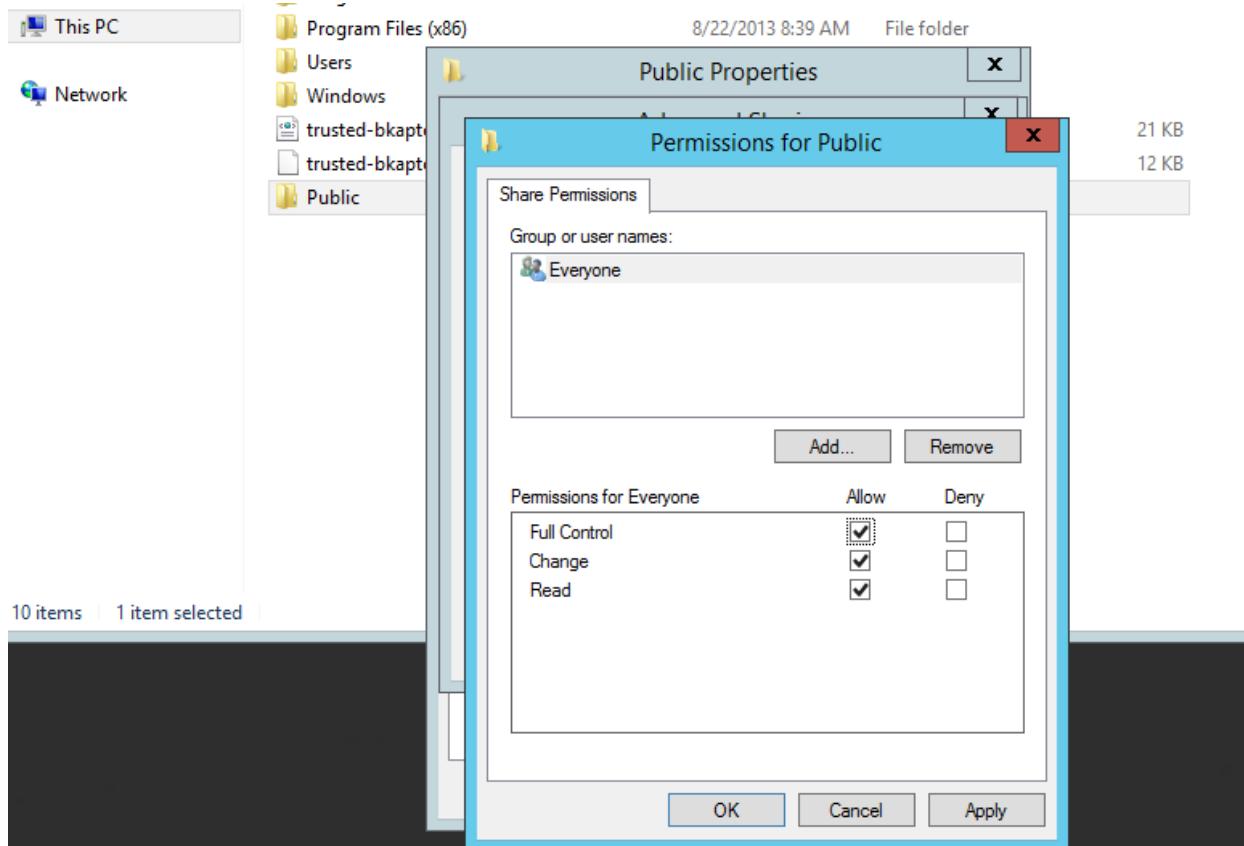
- Trong cửa sổ **Active Directory Administrative Center**, chọn vào **Dynamic Access Control / Resource Properties**.



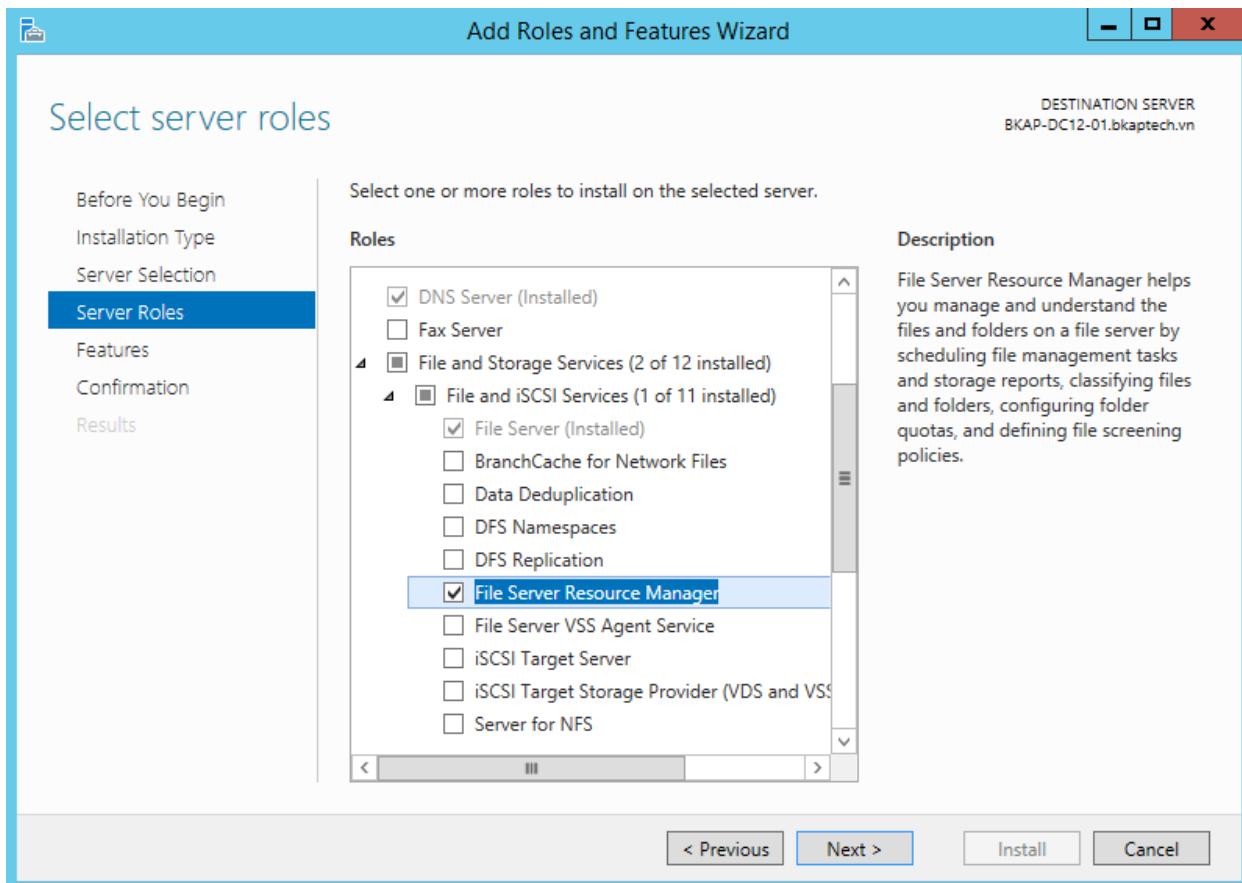
- Trong cửa sổ **Resource Properties**, click chuột phải vào **Confidentiality**, chọn **Enable**.



- Tạo thư mục “**Public**” và chia sẻ dữ liệu với quyền ‘**Full control**’ cho *Everyone*.

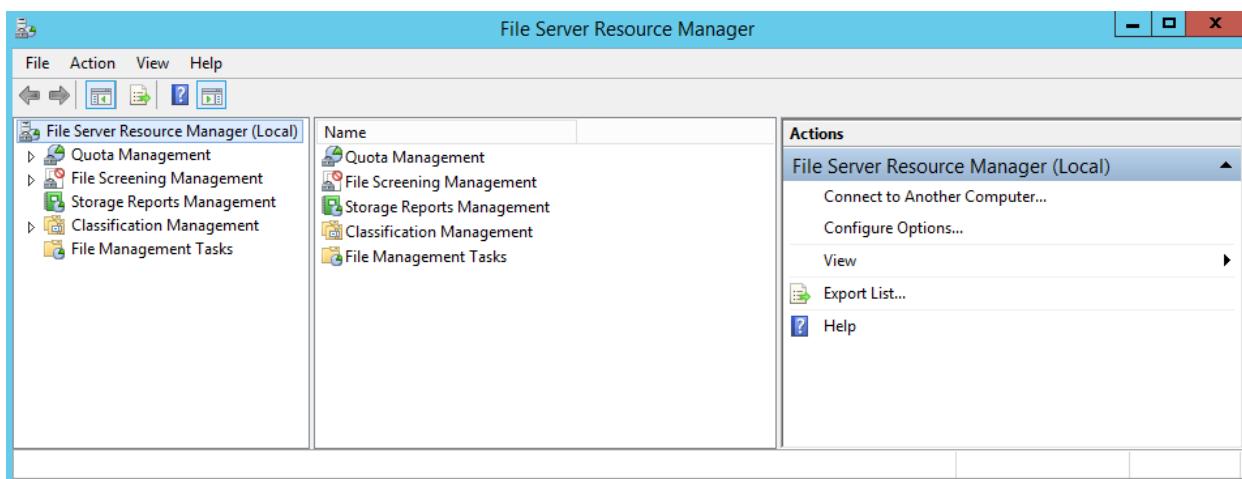


- Thực hiện cài đặt **File Server Resource Manager**.

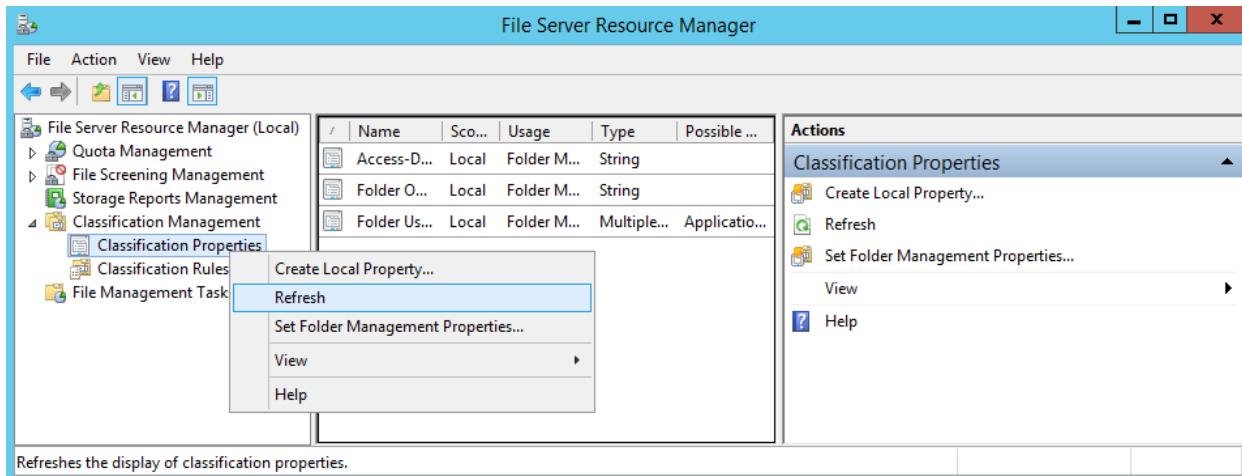


- Thực hiện cấu hình phân loại File bằng **Classification Rule**.

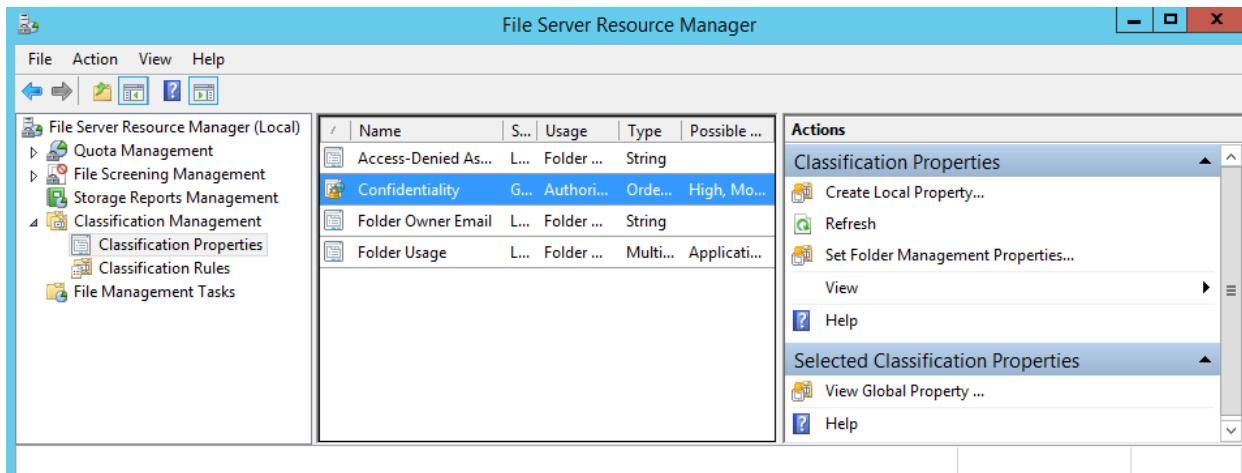
- Vào **Server Manager / Tools / Server Manager**.



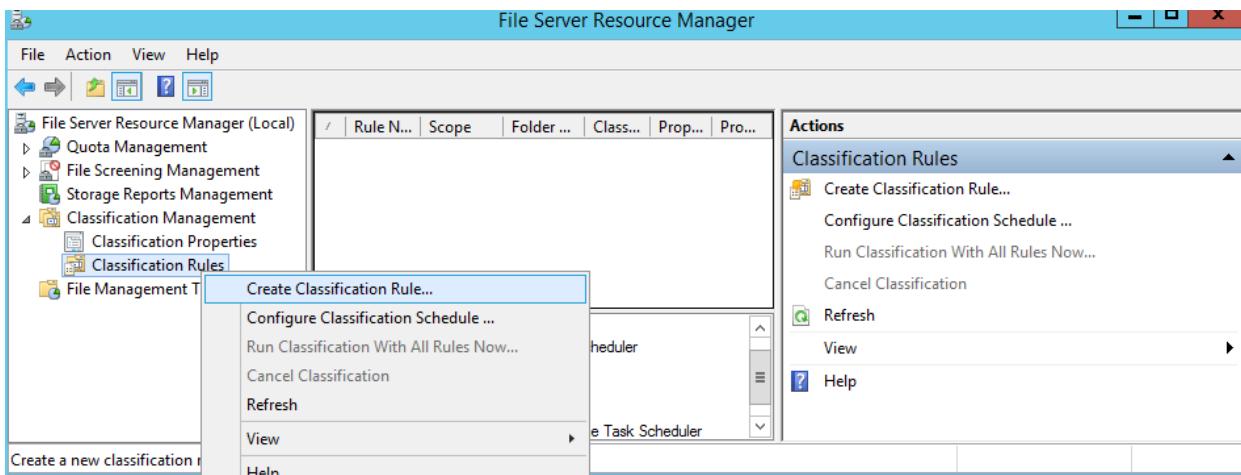
- Click vào Classification Management / Classification Properties / Refresh.



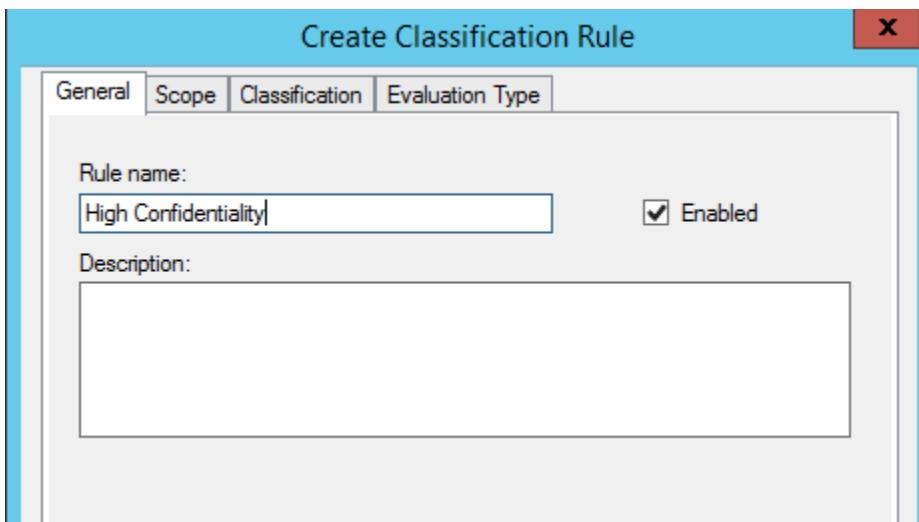
- Sau khi Refresh, kiểm tra thuộc tính Confidentiality.



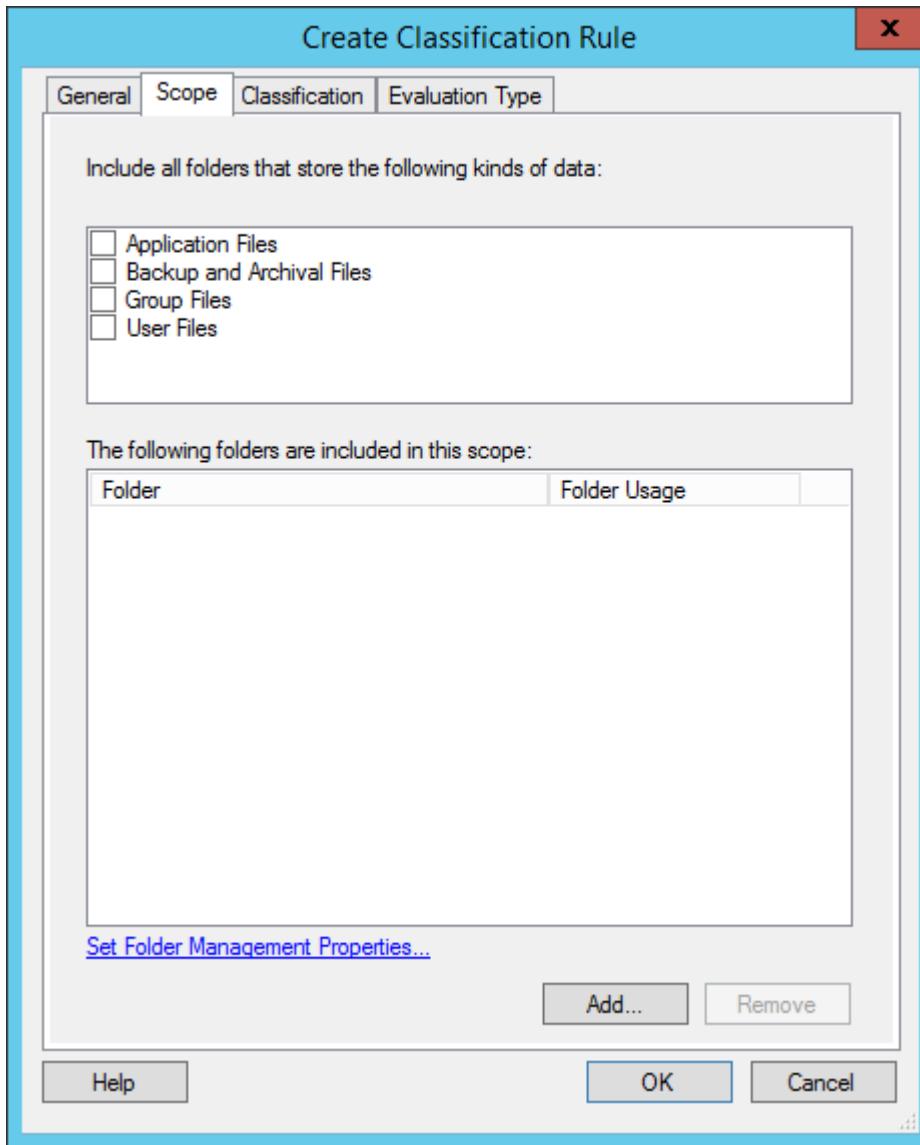
- Click chuột phải vào **Classification Rules**, chọn **Create Classification Rule...**



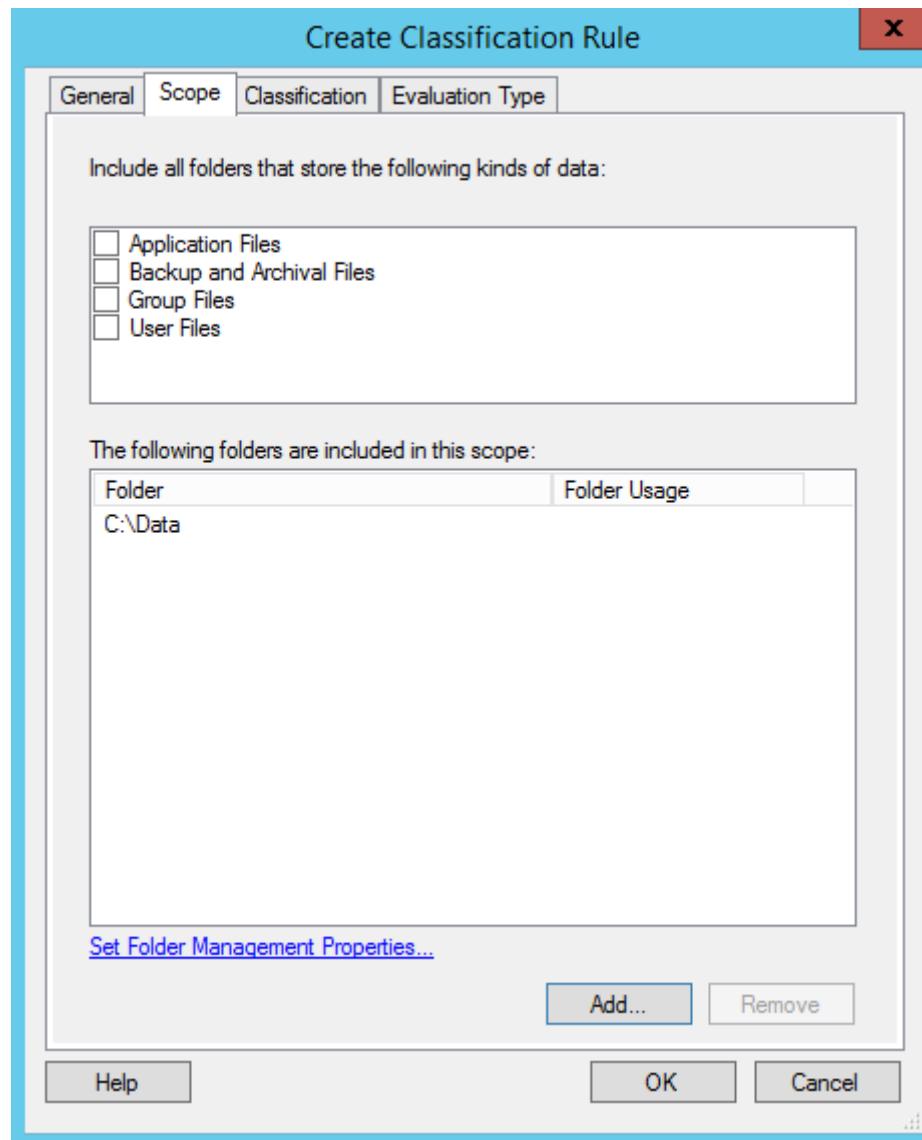
- Trong cửa sổ **Create Classification Rule**, tại tab **General**, nhập vào tên tại mục *Rule name* : **High Confidentiality**.



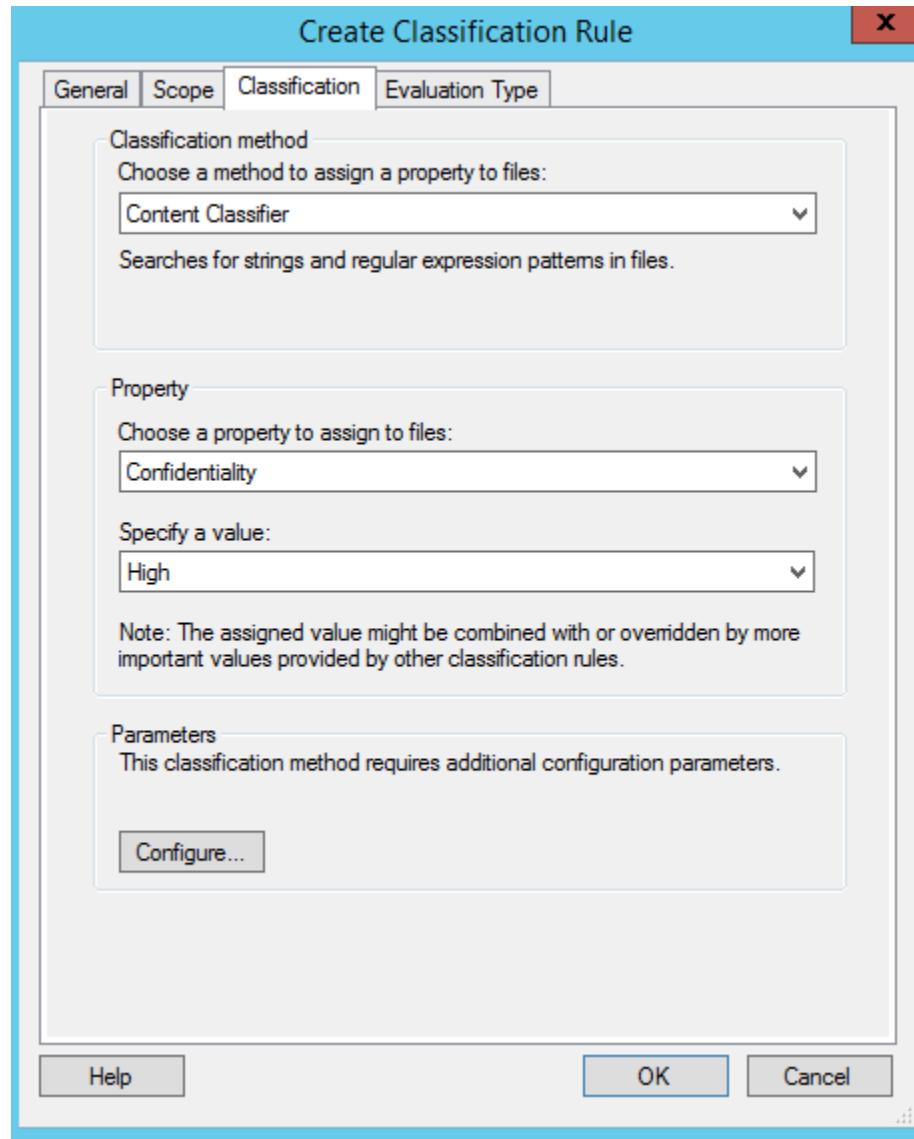
- Chuyển sang tab Scope, click vào Add...



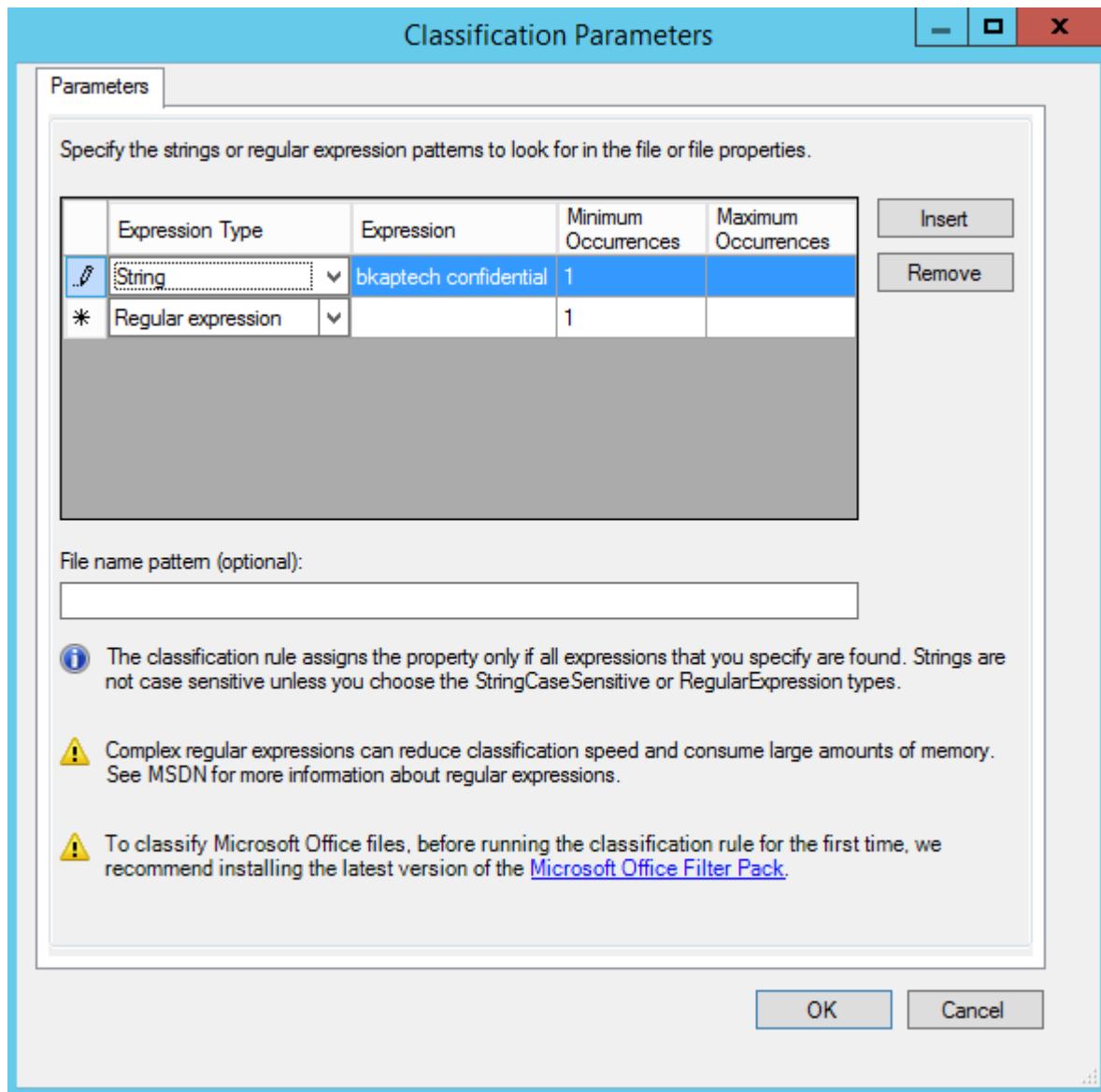
- Thực hiện add vào thư mục **Data** (đã tạo ở phần 1).



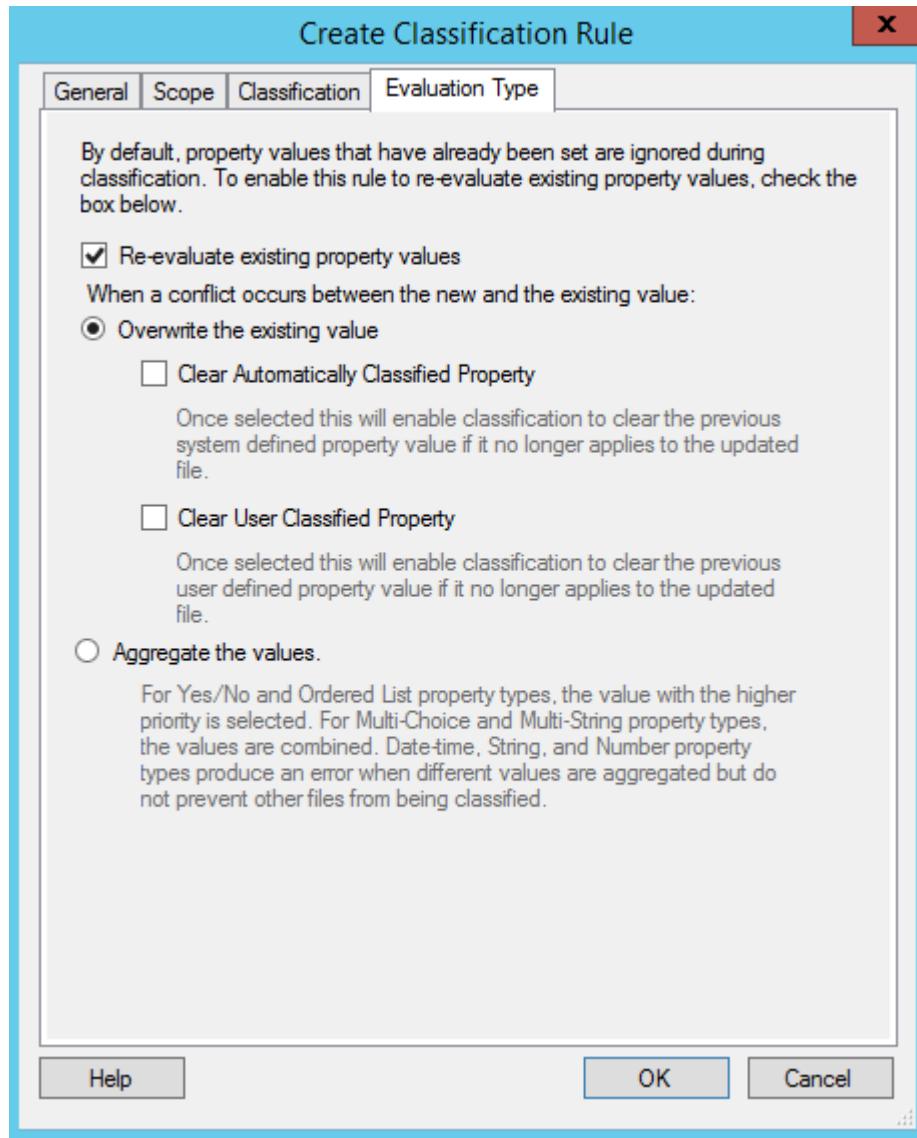
- Chuyển sang Tab **Classification**, kiểm tra các tùy chọn như hình dưới, click vào **Configure...**



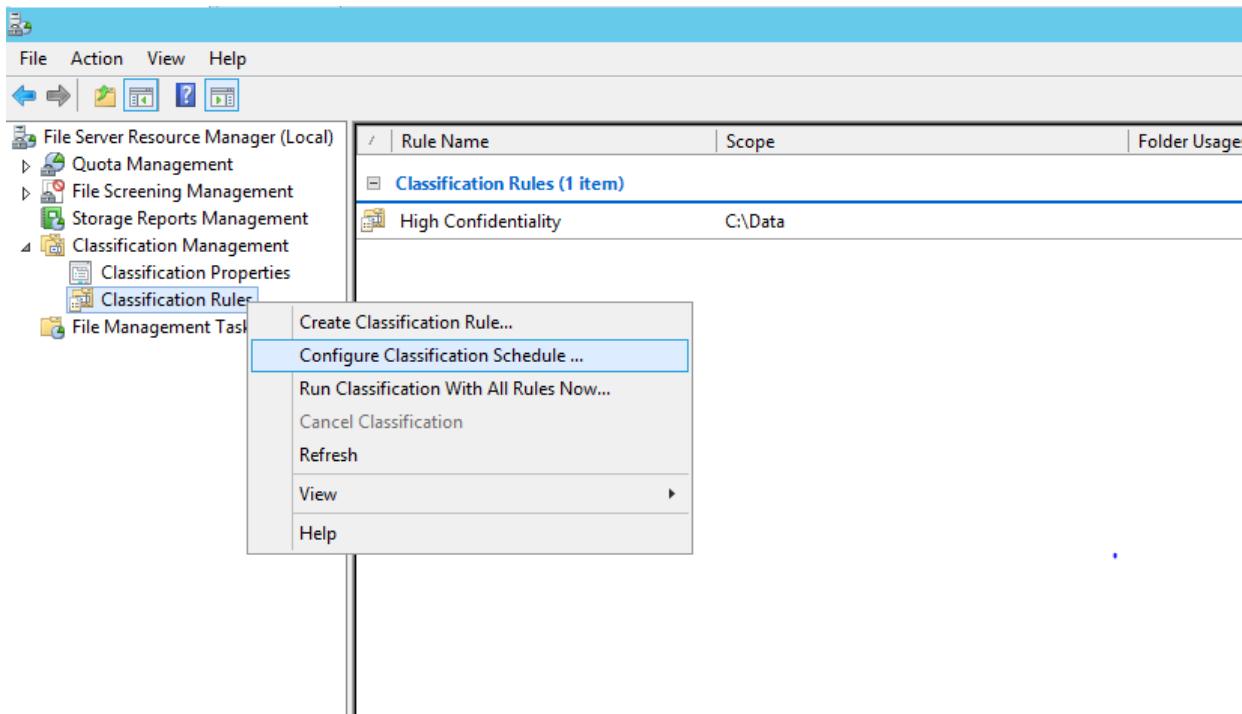
- Trong cửa sổ **Classification Parameters**, trong mục **Expression Type**, chọn vào **String**, trong mục **Expression**, nhập vào **bkaptech confidential**. => **OK**.



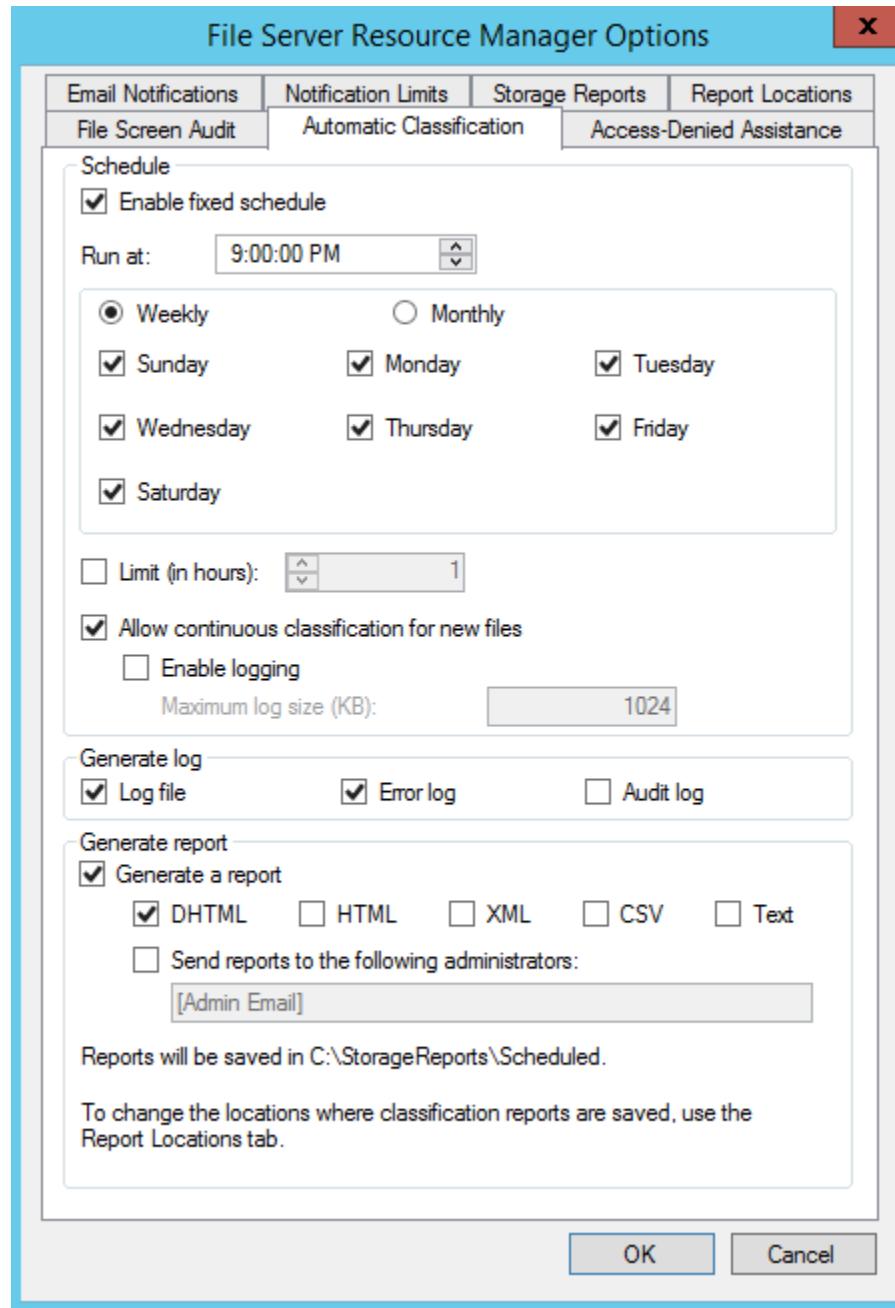
- Tại cửa sổ **Create Classification Rule**, chuyển sang Tab **Evaluation Type**, tích chọn vào **Re-evaluate existing property values** và **Overwrite the existing value => OK.**



- Trong cửa sổ **File Server Resource Manager**, click chuột phải tại **Classification Rules**, chọn **Configure Classification Schedule...**

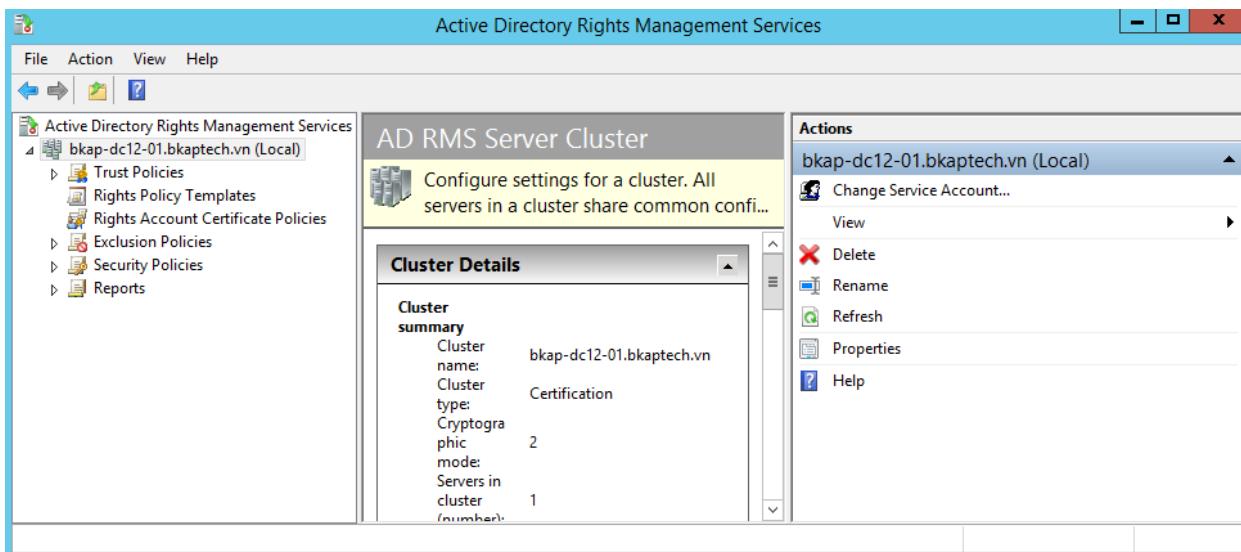


- Tại cửa sổ **File Server Resource Manager Options**, tích chọn vào **Enable fixed schedule**, thực hiện điều chỉnh thời gian như hình dưới , tích chọn vào **Allow continuous classification for new files => OK.**

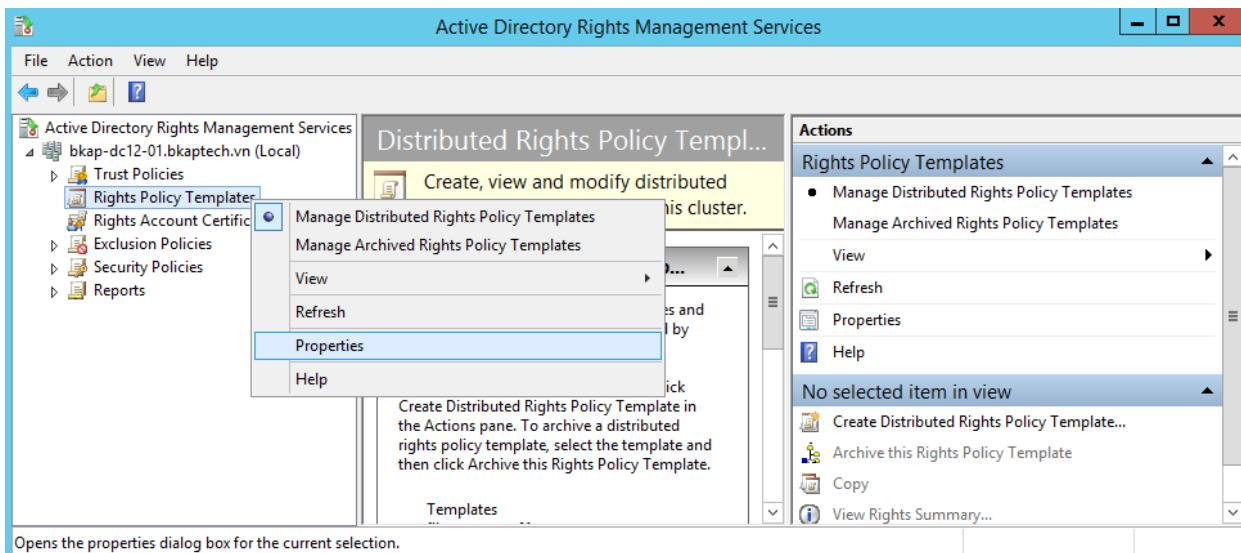


- Thực hiện cấu hình phân quyền bằng RMS Template.

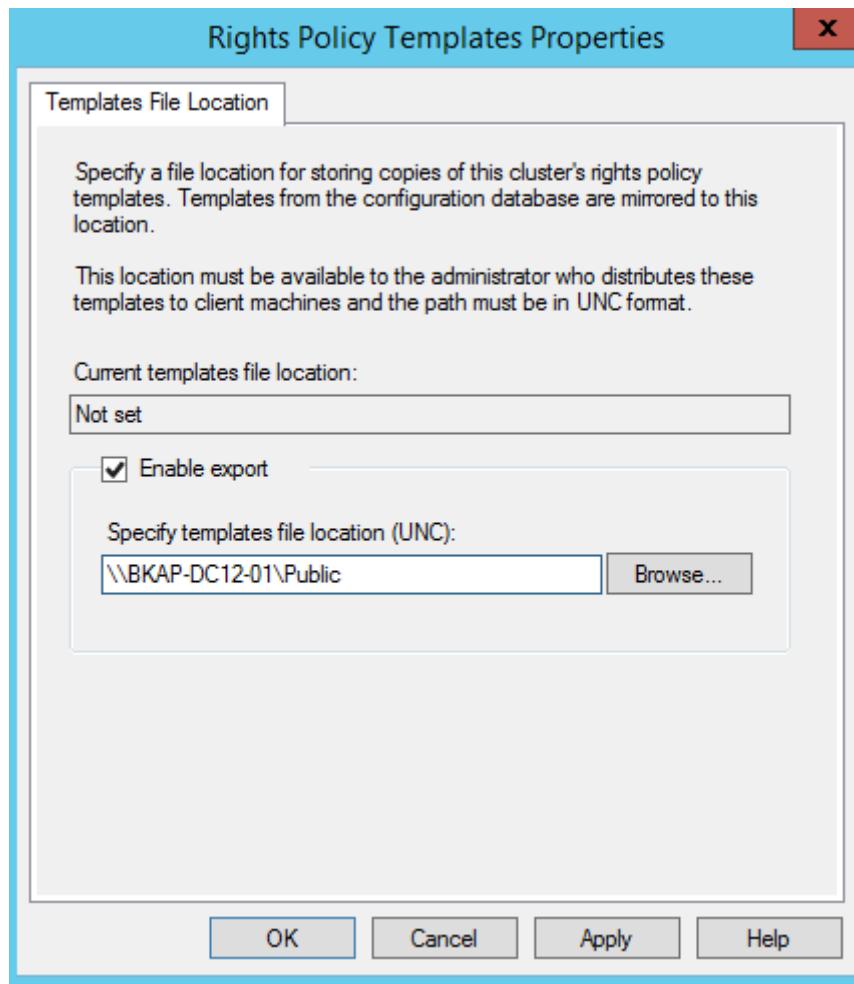
- Vào AD RMS.



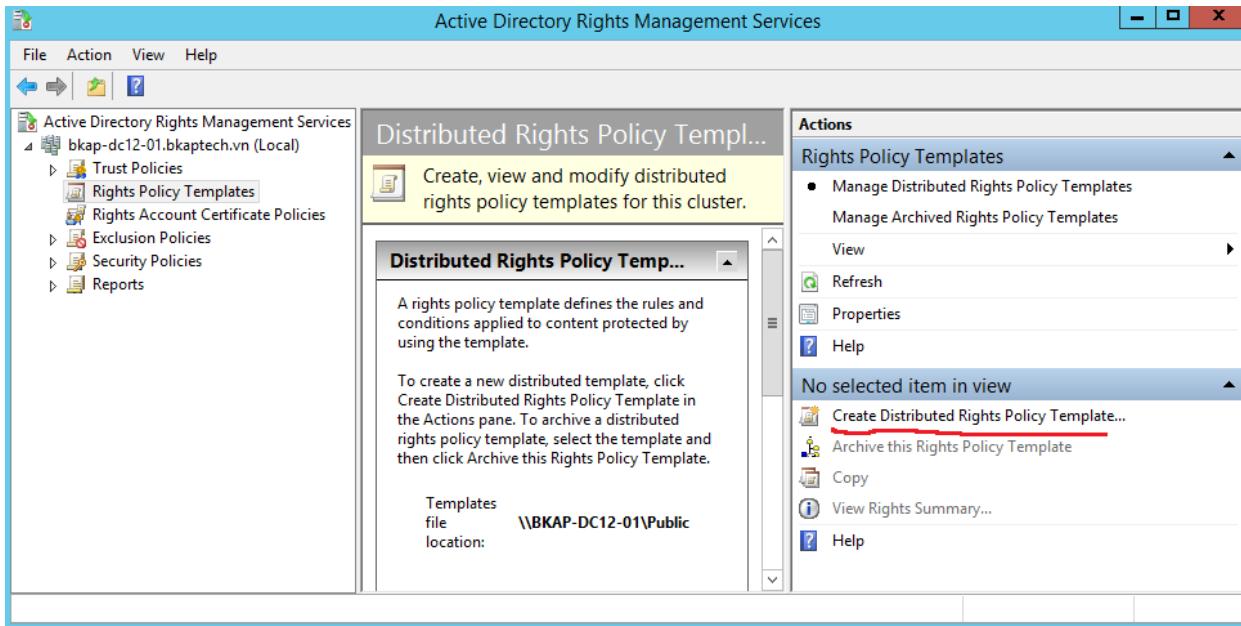
- Trong cửa sổ AD RMS Services , click chuột phải tại Rights Policy Templates chọn Properties.



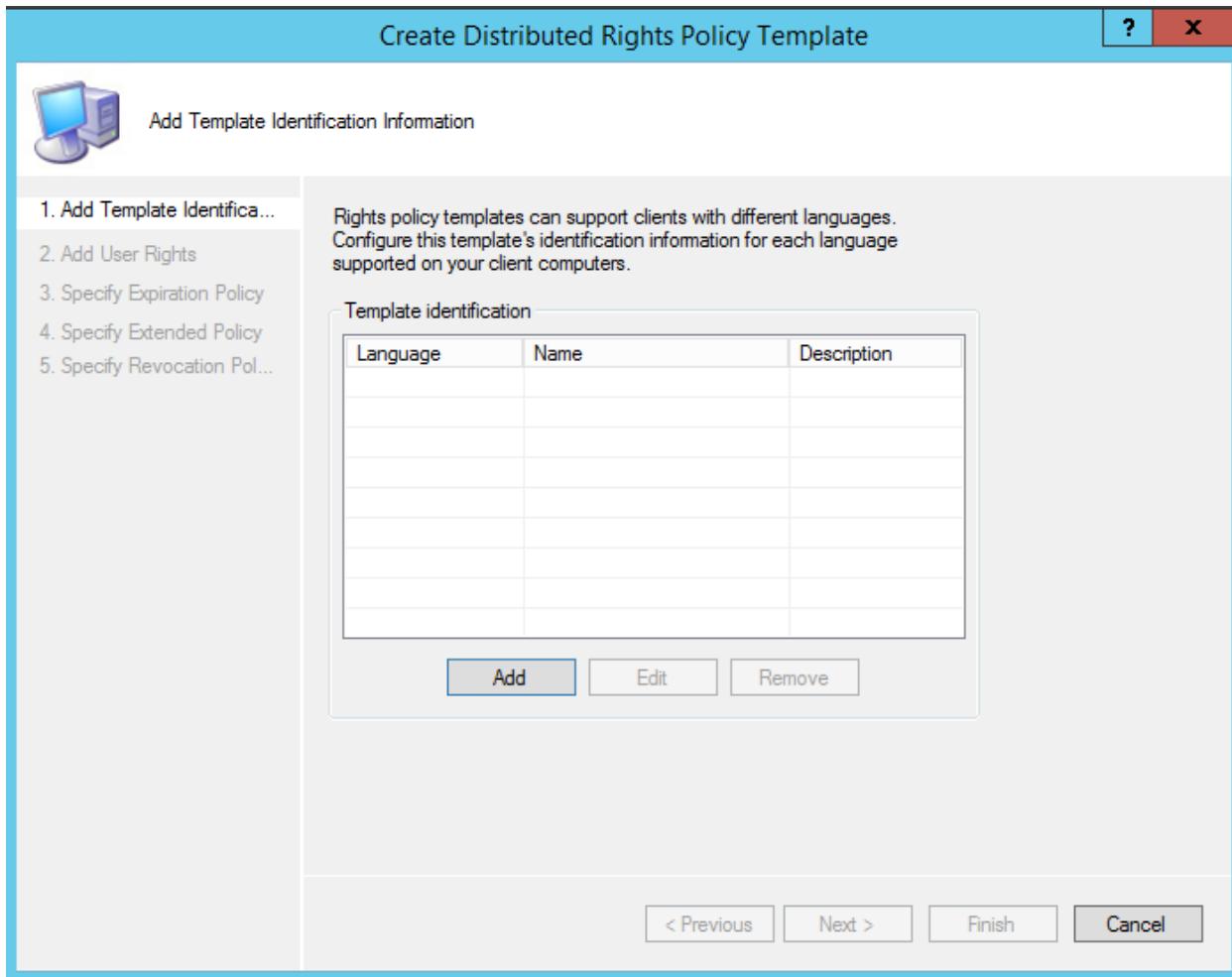
- Trong cửa sổ **Right Policy Templates Properties**, tích chọn vào **Enable export**, tại mục **Specify templates file location (UNC)**, nhập vào <\\BKAP-DC12-01\Public> => **Apply / OK**.



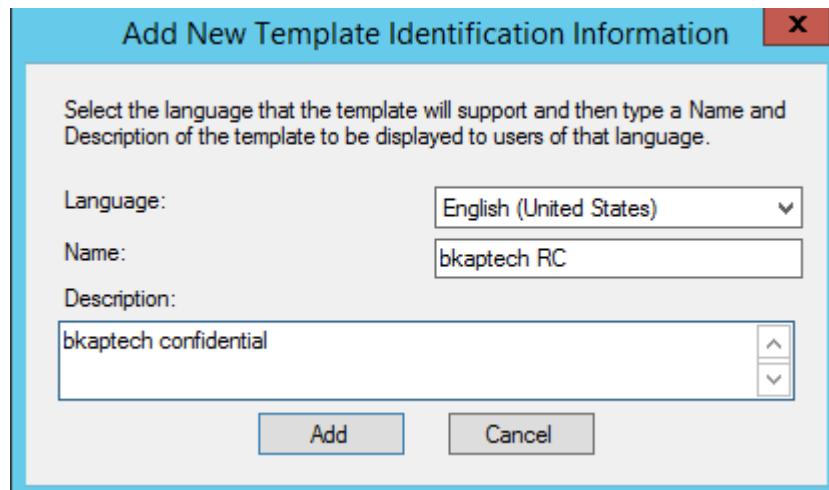
- Trong cửa sổ **Distributed Rights Policy Templates**, click chọn vào **Create Distributed Rights Policy Template...**



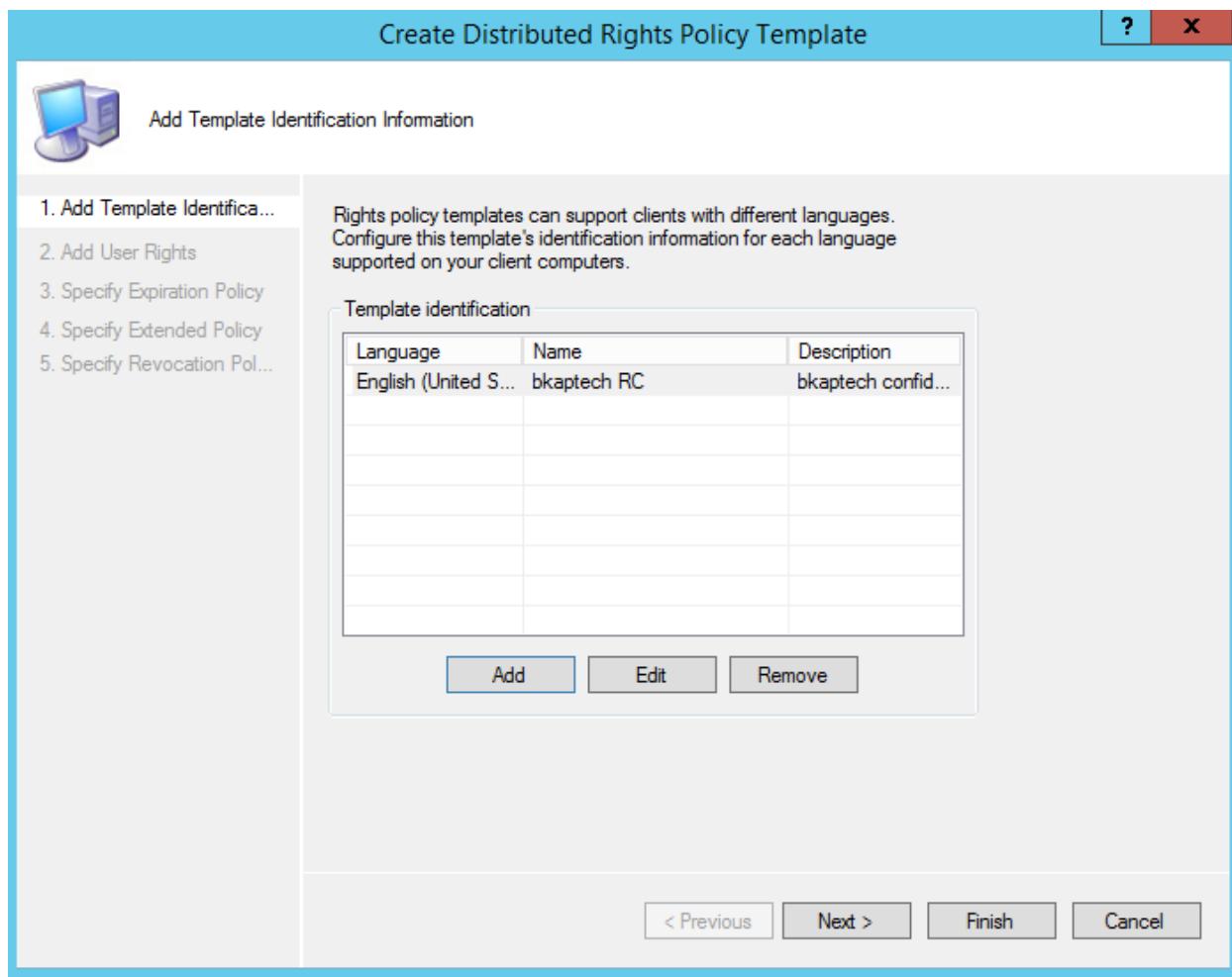
- Tại cửa sổ **Create Distributed Rights Policy Template**, click vào **Add**.



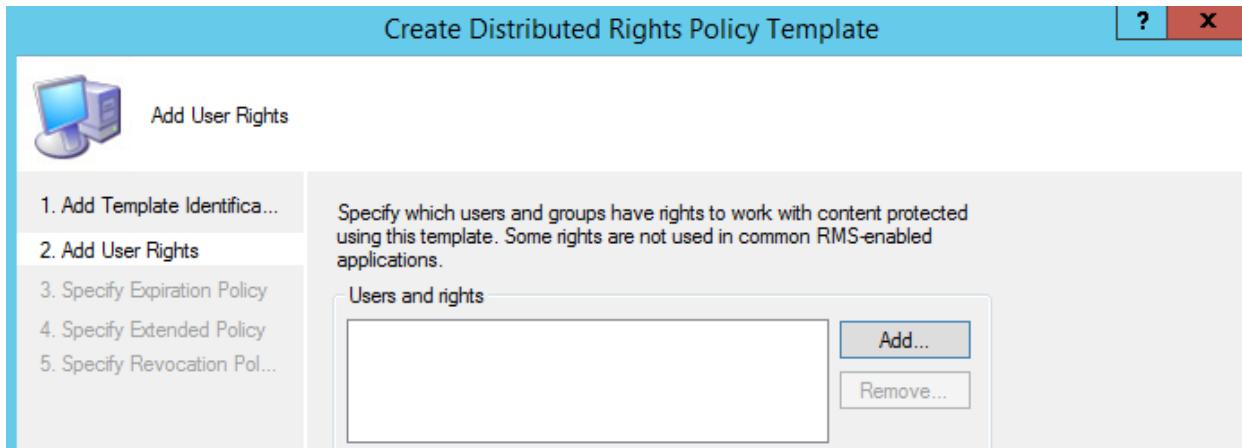
- Trong cửa sổ **Add New Template Identification Information**, nhập vào tên tại mục **Name** : **bkaptech RC** , nhập vào tại **Description** : **bkaptech confidential**.



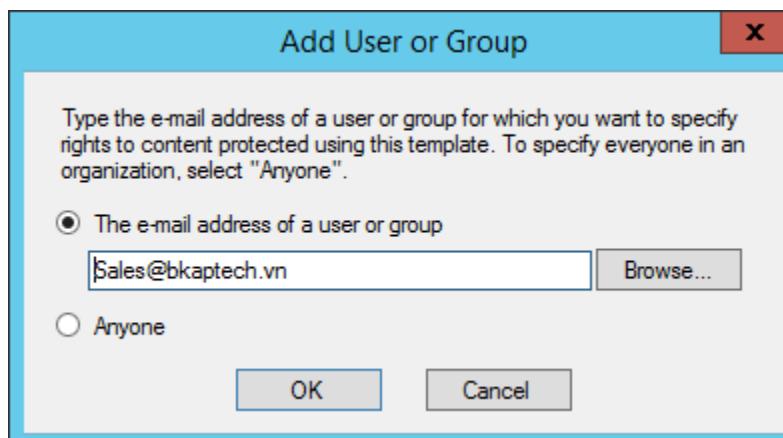
- Click vào **Next**.



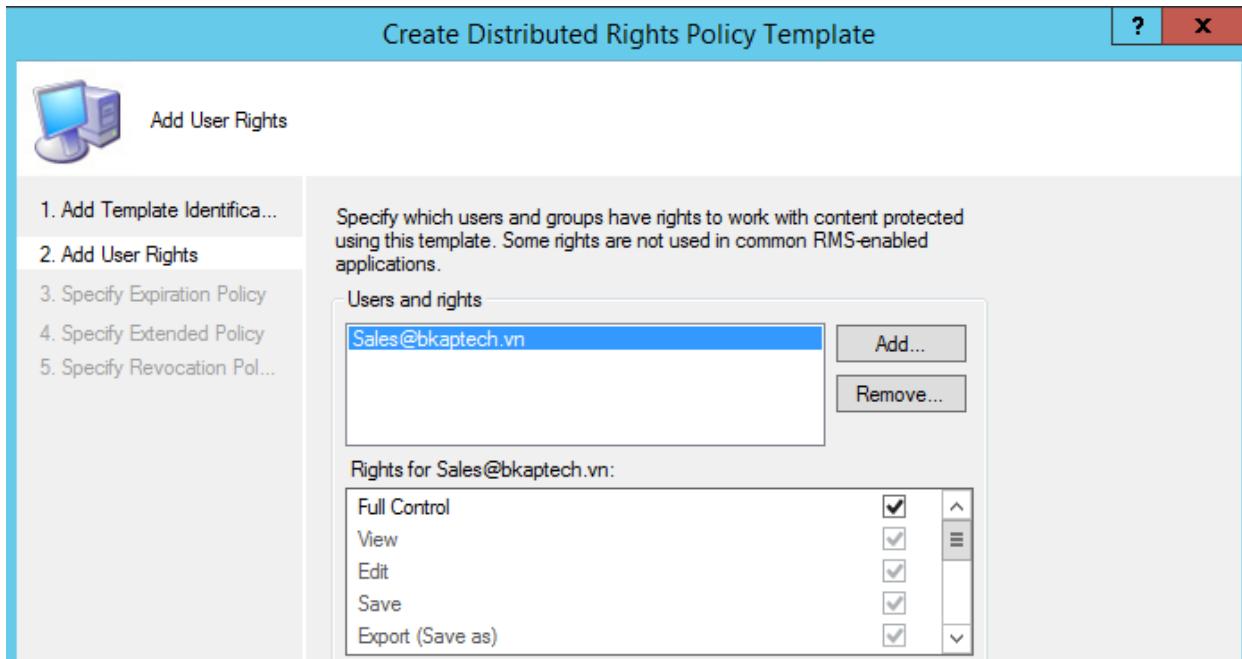
- Tại cửa sổ **Add User rights**, tại mục **Users and rights**, click vào **Add...**.



- Tại cửa sổ **Add User or Group**, click vào **Browse...** tiến hành add vào group **Sales** (Sales@bkaptech.vn).



- Tại mục **Rights for Sales@bkaptech.vn**, click chọn **Full Control**.



- Thực hiện add vào group **ITs** (ITs@bkaptech.vn), chọn vào View.

⇒ **Finish.**

Create Distributed Rights Policy Template

Add User Rights

Specify which users and groups have rights to work with content protected using this template. Some rights are not used in common RMS-enabled applications.

Users and rights

ITs@bkaptech.vn	Add...
Sales@bkaptech.vn	Remove...

Rights for ITs@bkaptech.vn:

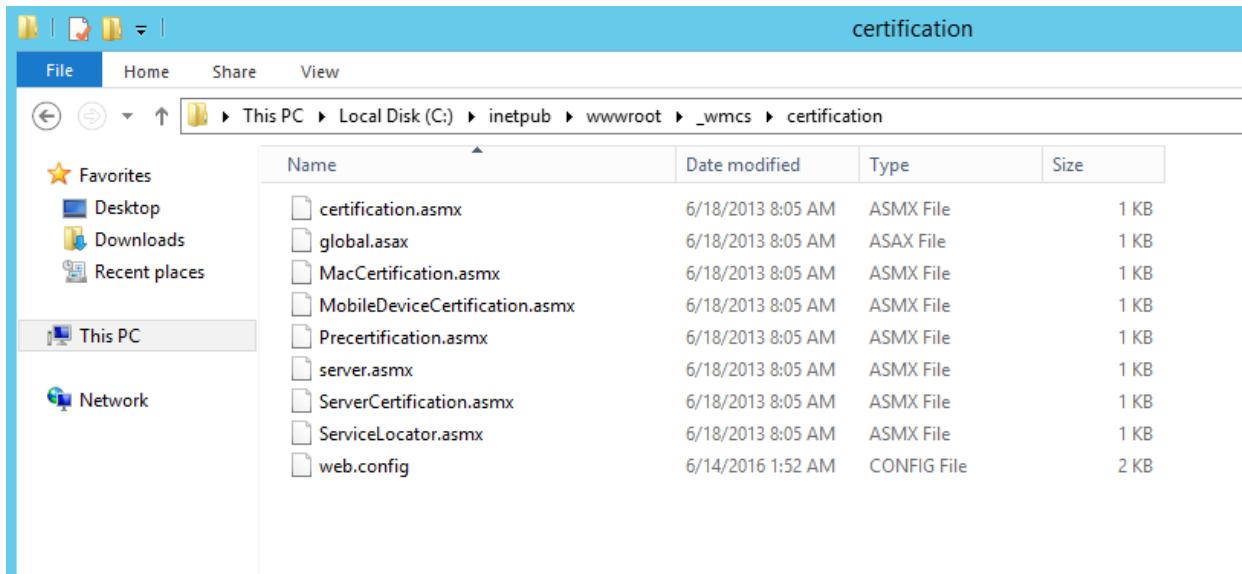
Full Control	<input type="checkbox"/>
View	<input checked="" type="checkbox"/>
Edit	<input type="checkbox"/>
Save	<input type="checkbox"/>
Export (Save as)	<input type="checkbox"/>

Grant owner (author) full control right with no expiration

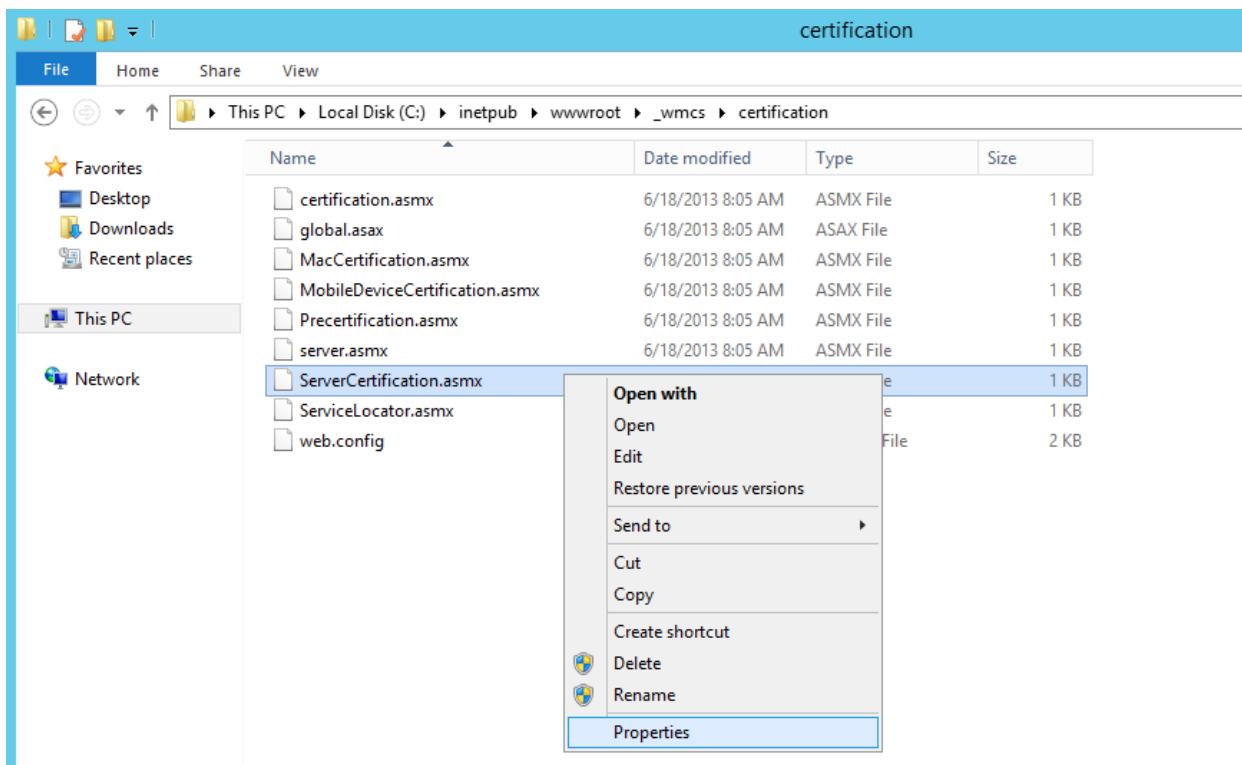
Rights request URL:

< Previous Next > Finish Cancel

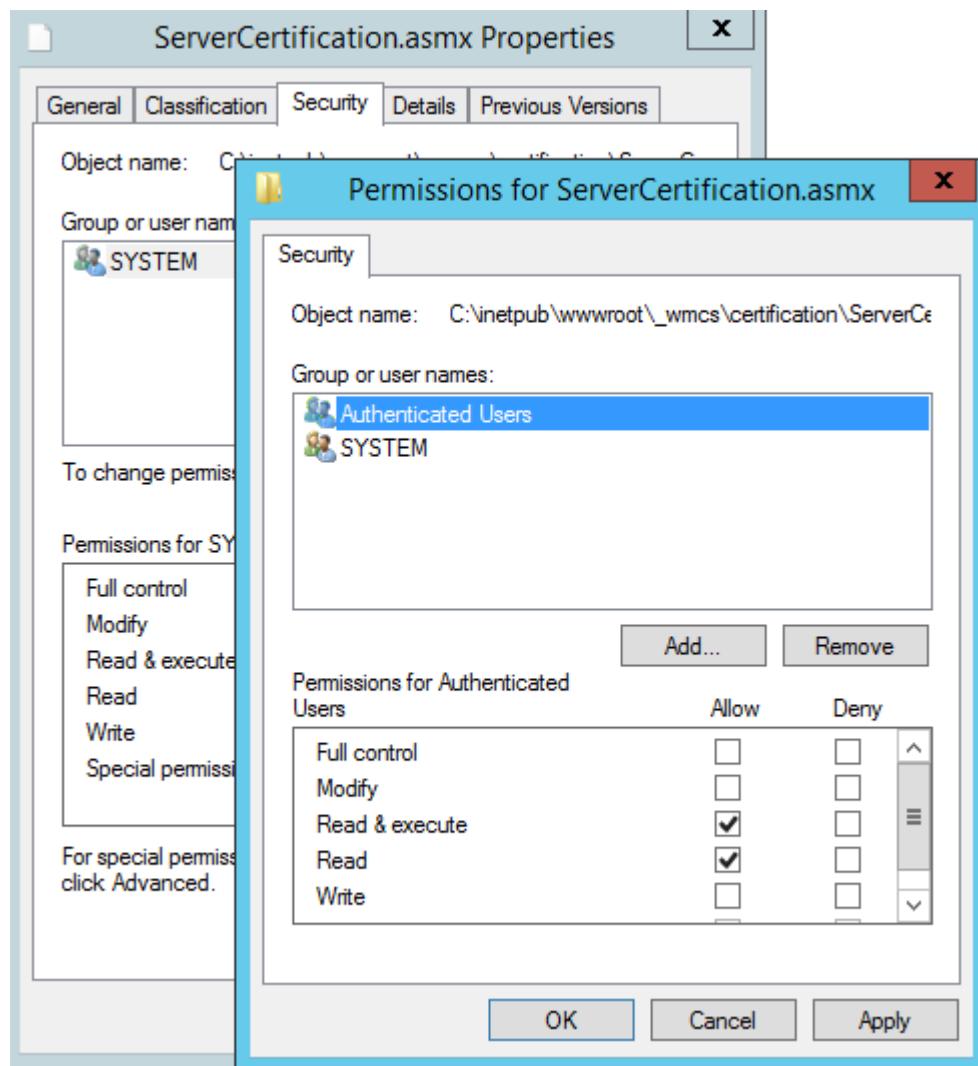
- Thực hiện cấu hình phân quyền truy cập RMS.
- Vào **C:\inetpub\wwwroot_wmcs\certification**.



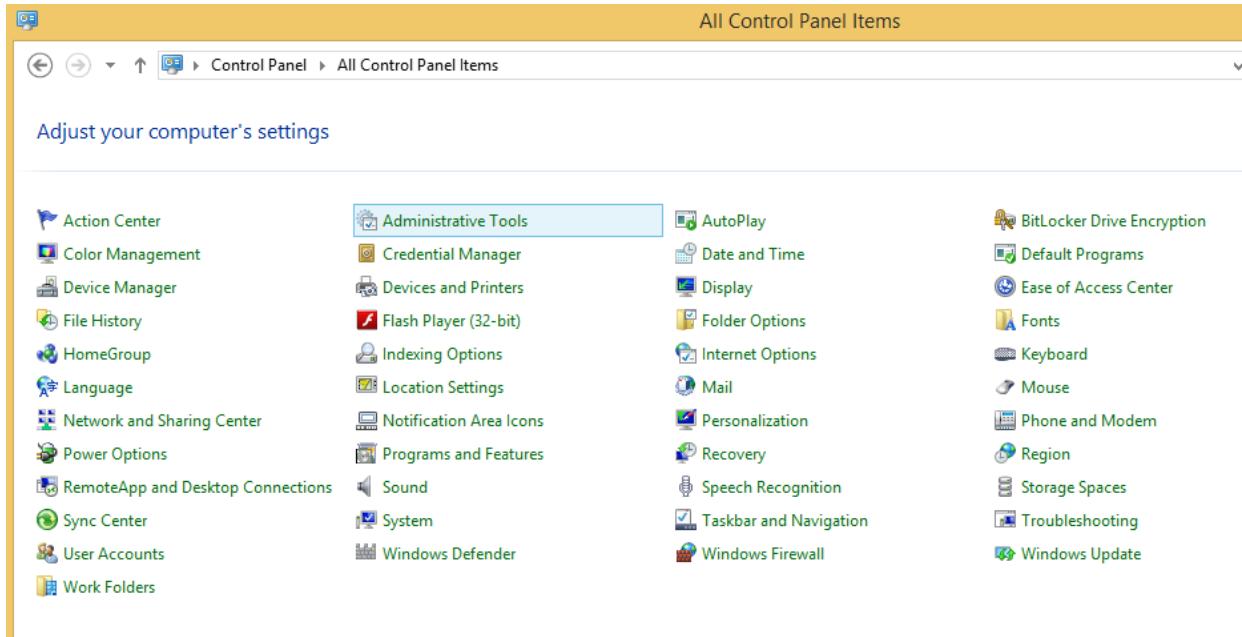
- Trong thư mục **certification**, click chuột phải tại **ServerCertification.asmx**, chọn **Properties**.



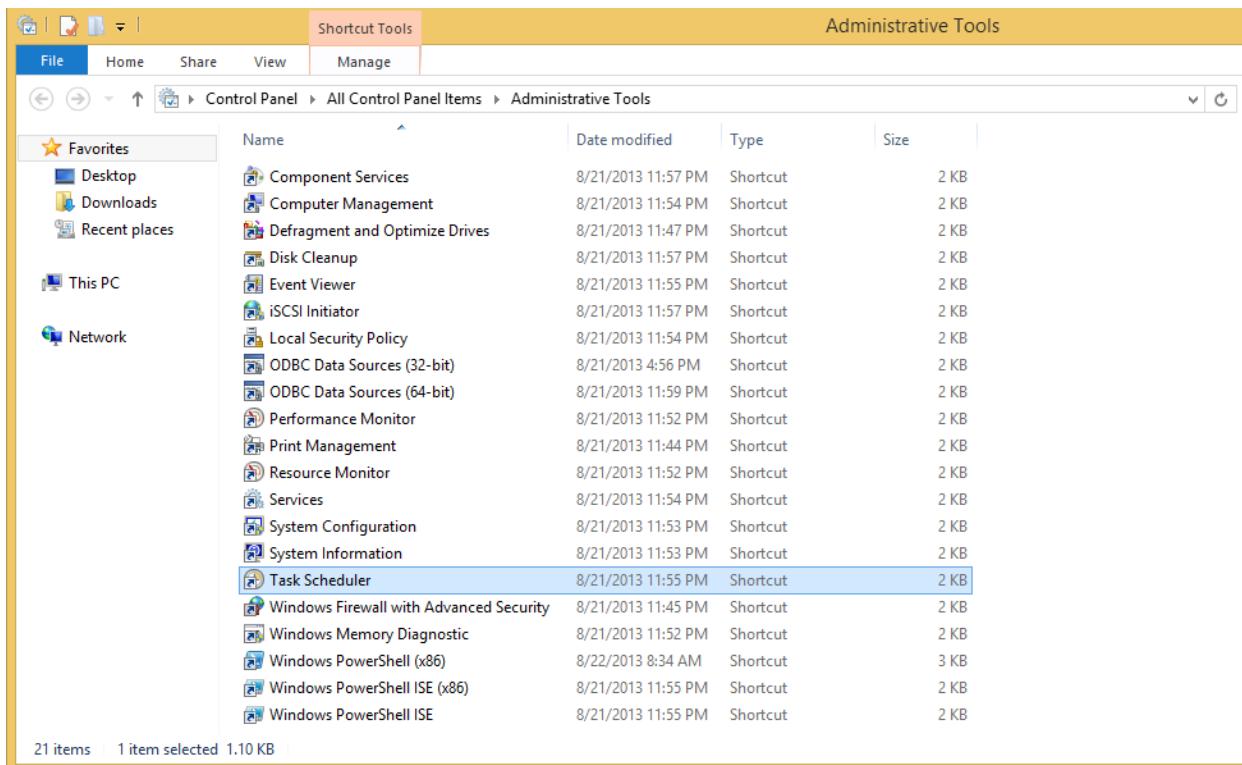
- Tại cửa sổ **ServerCertification.asmx Properties**, chuyển sang tab **Security**, click vào **Edit**, thực hiện *add* vào **Authenticated User**, chọn các *permission* như hình dưới.



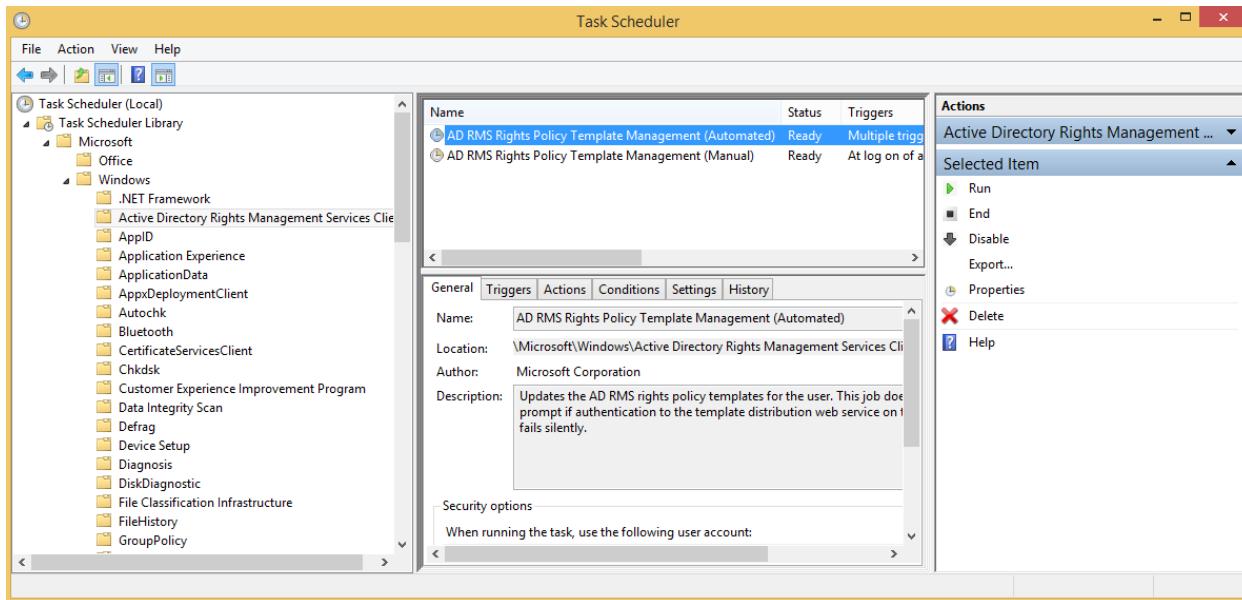
- Chuyển sang máy Client BKAP-WRK08-01, đăng nhập tài khoản **bkaptech\administrator**, vào **Control Panel**, vào **Administrative Tools**.



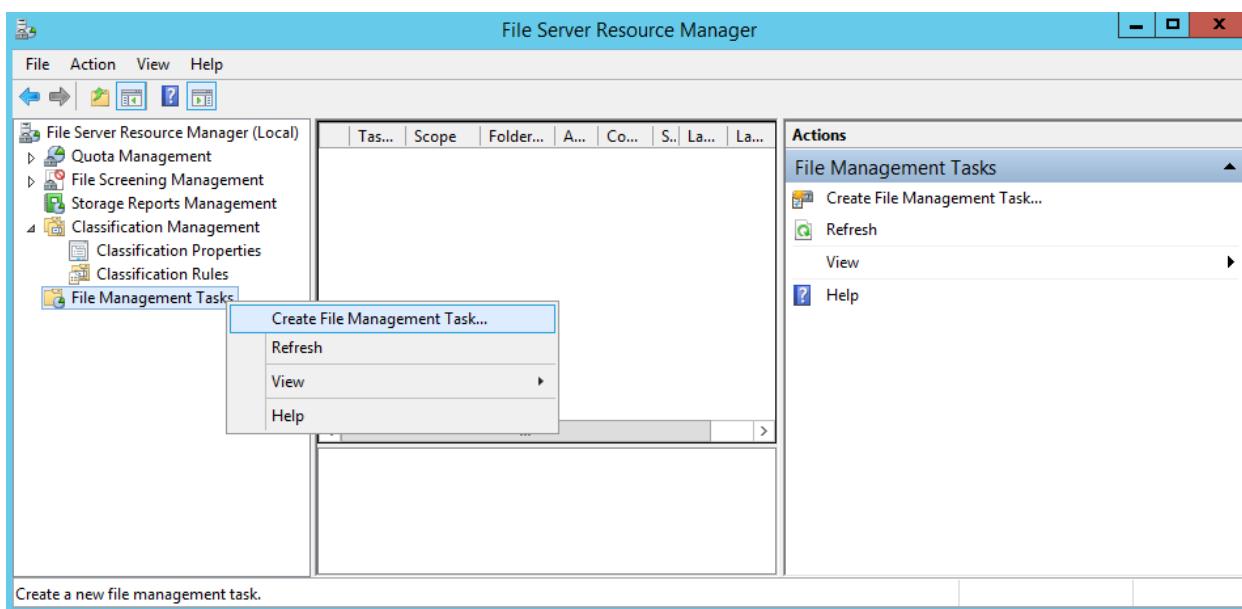
- Trong cửa sổ **Administrative Tools**, chọn vào **Task Scheduler**.



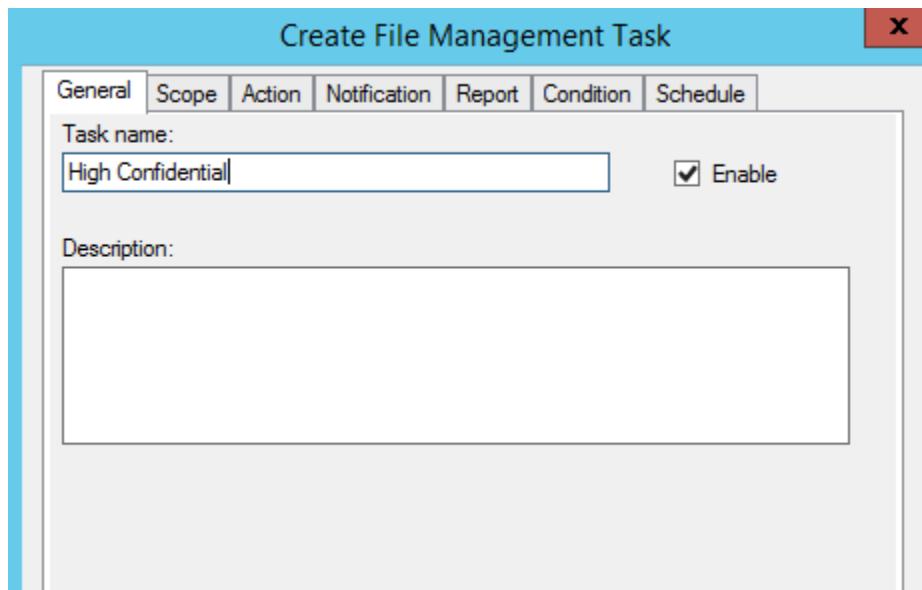
- Trong cửa sổ **Task Scheduler**, chọn vào **Task Scheduler (Local) / Task Scheduler Library / Microsoft / Windows / Active Directory Right Management Services Client**, thực hiện **Enable AD RMS Rights Policy Template Management (Automated)**.



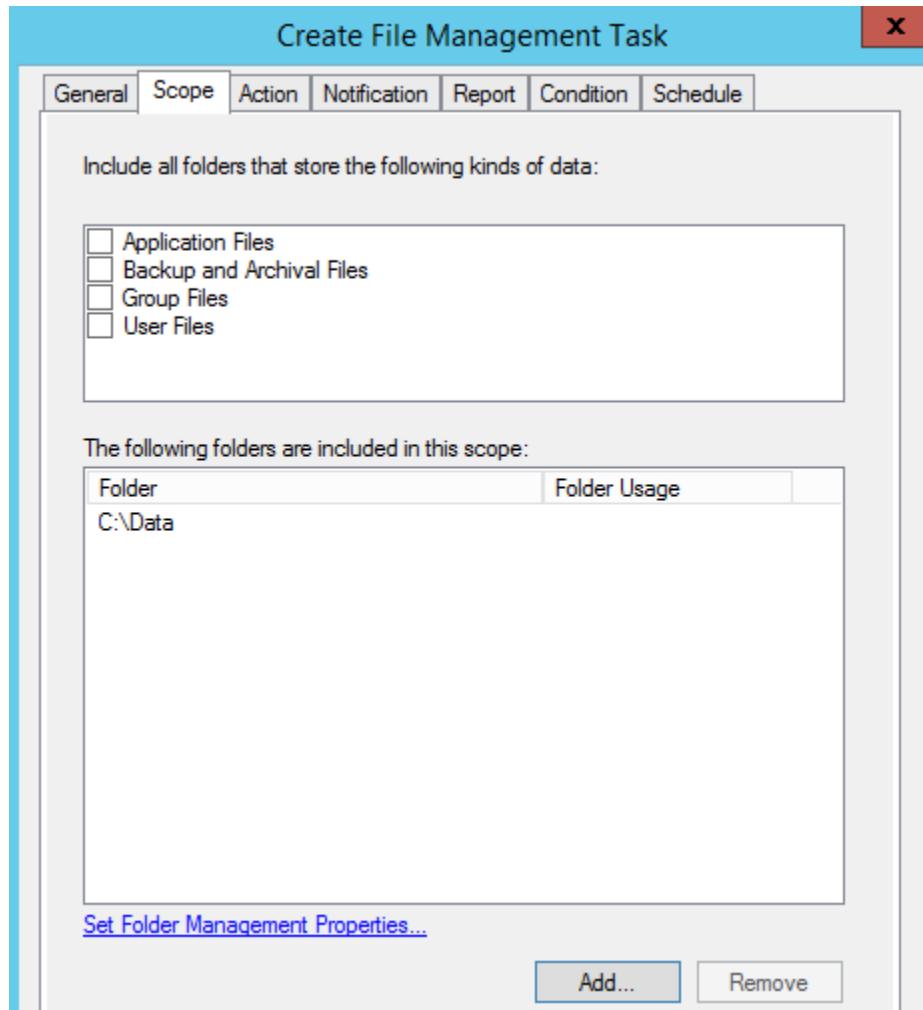
- Chuyển qua server *BKAP-DC12-01*, thực hiện lập lịch phân quyền bằng **File Management Task**.
 - Trong cửa sổ **File Server Resource Manager**, click chuột phải tại **File Management Tasks**, chọn **Create File Management Task...**



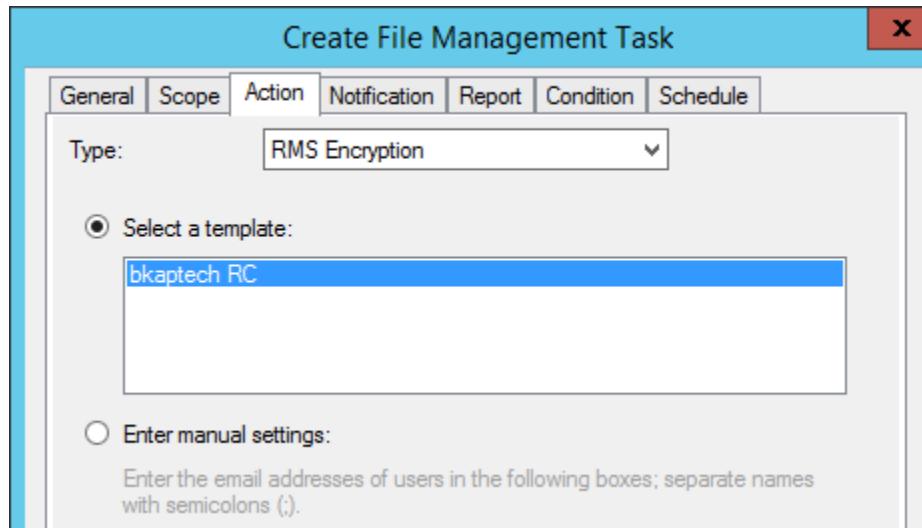
- Trong cửa sổ **Create File Management Task**, tại Tab **General**, nhập vào tại mục Task name : **High Confidential**.



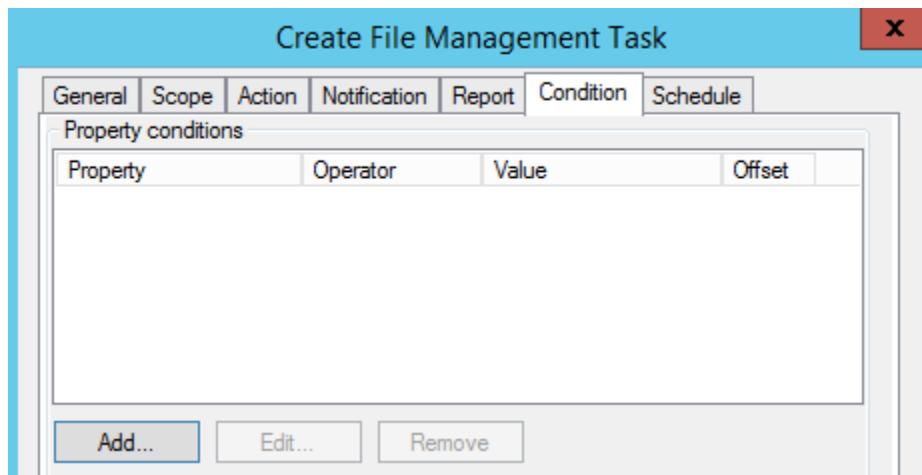
- Chuyển sang Tab Scope, thực hiện Add... vào thư mục C:\Data.



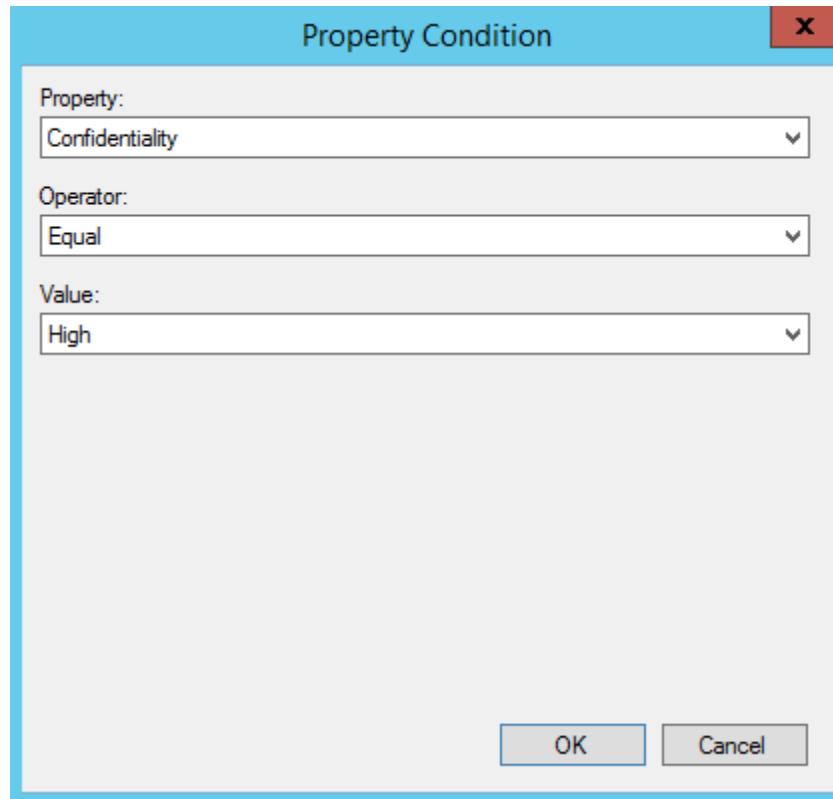
- Chuyển sang Tab **Action**, tại mục **Type** , chọn **RMS Encryption**, chọn vào Template **bkaptech RC**.



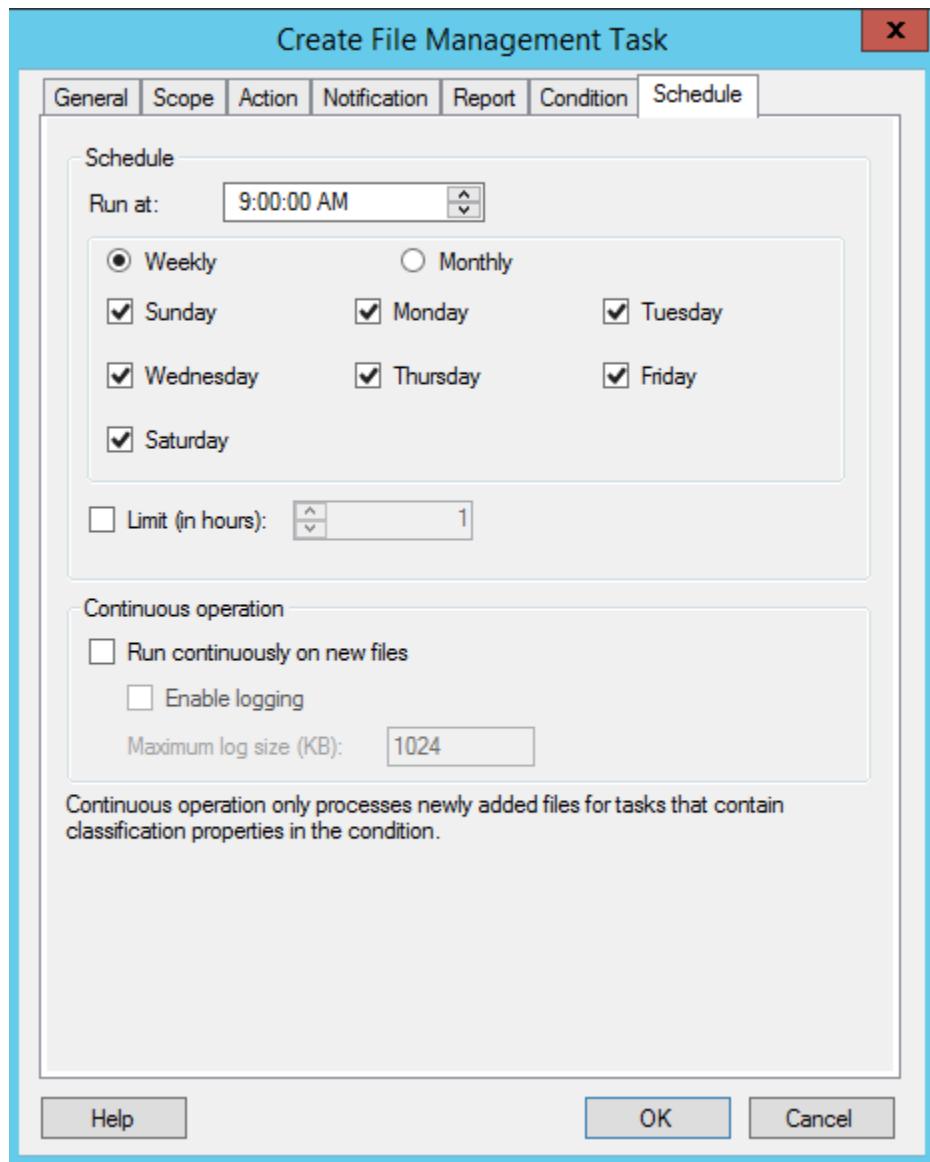
- Chuyển sang Tab **Condition**, click vào **Add...**



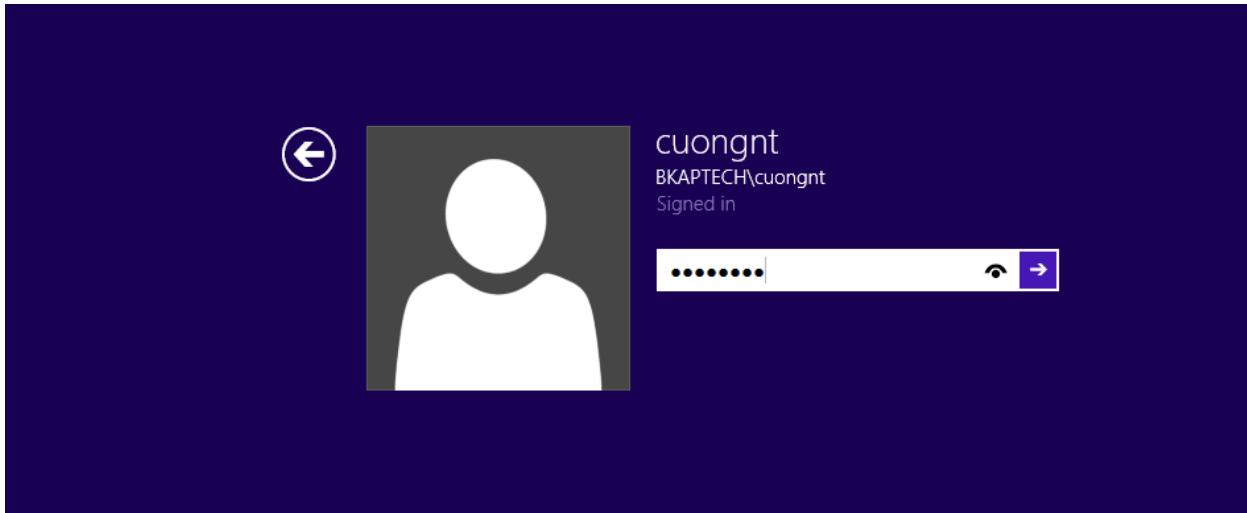
- Tại cửa sổ **Property Condition**, kiểm tra các thuộc tính như hình dưới, OK.



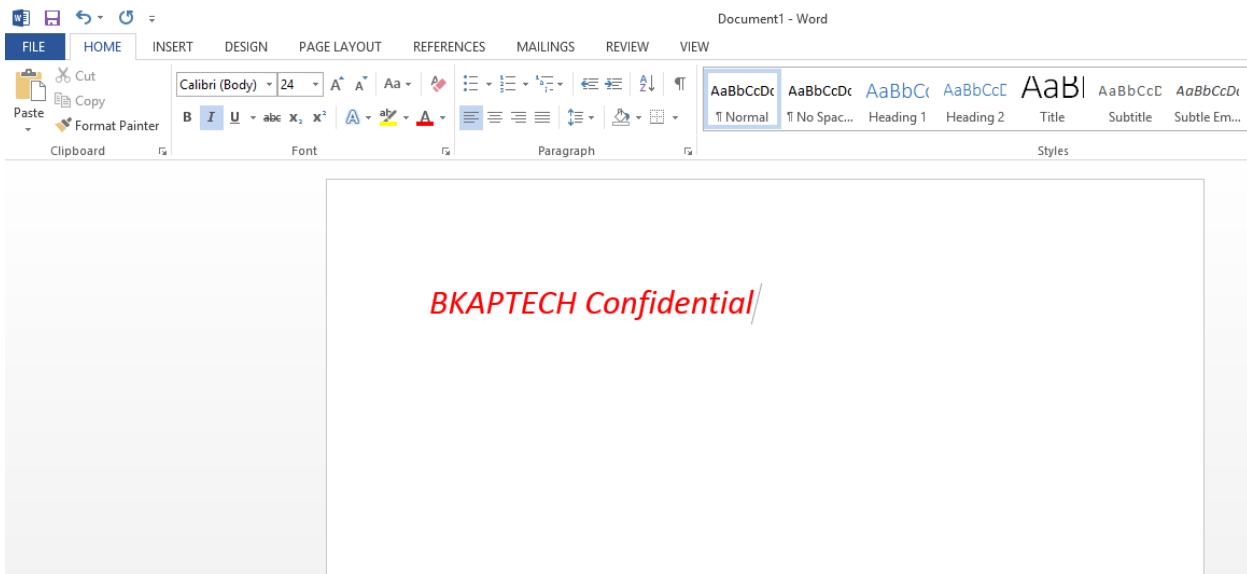
- Chuyển sang Tab **Schedule**, nhập vào thời gian như hình dưới , OK.



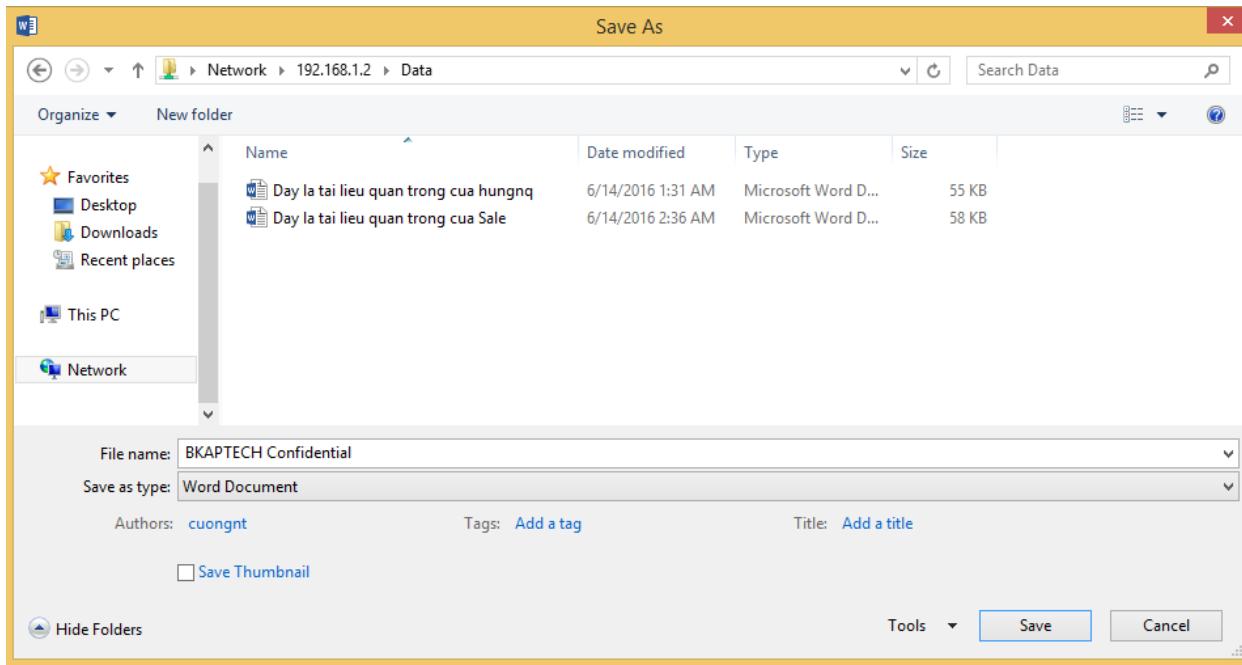
- Chuyển sang máy BKAP-WRK08-01 để kiểm tra.
 - Đăng nhập bằng tài khoản **cuongnt** trong group Sales.



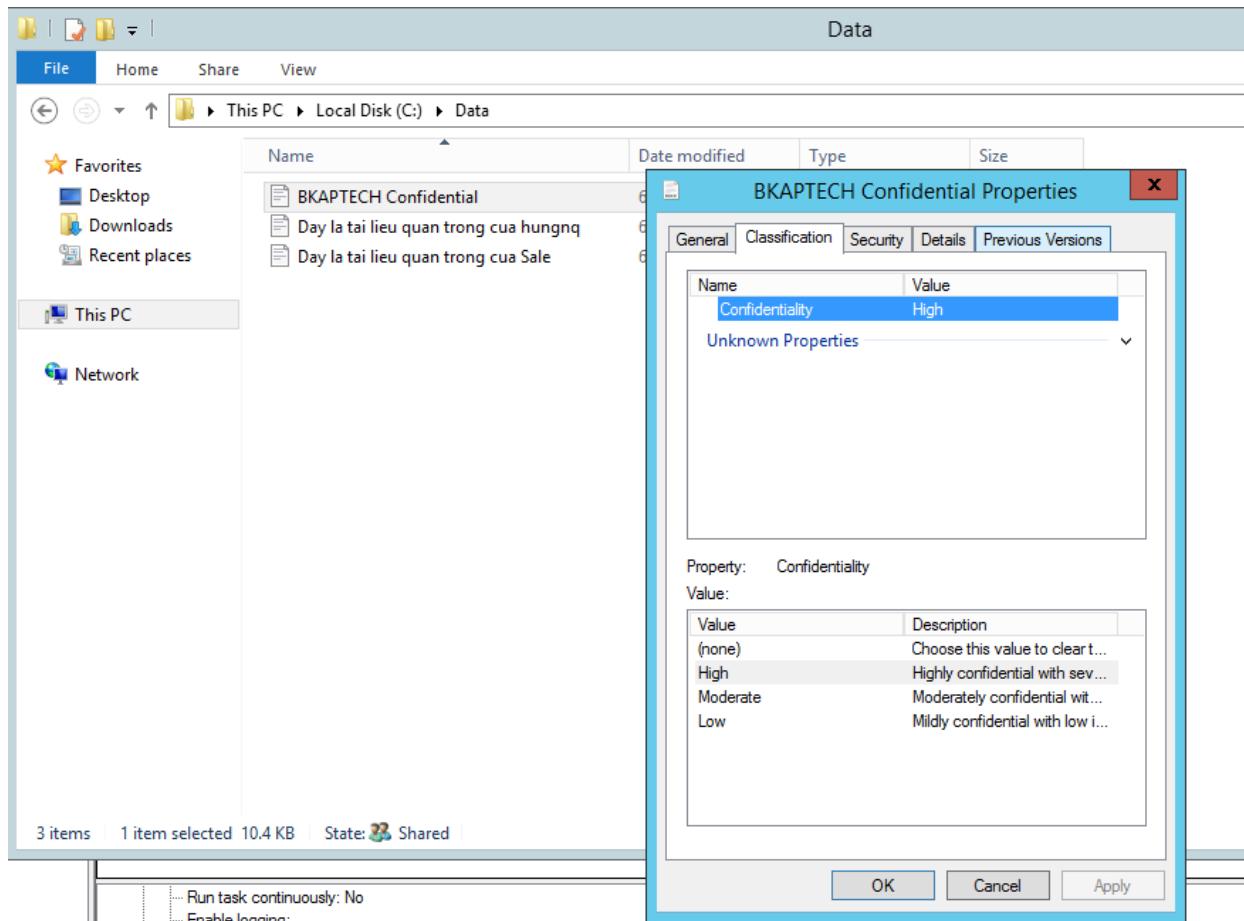
- Thực hiện soạn thảo 1 văn bản bất kì.



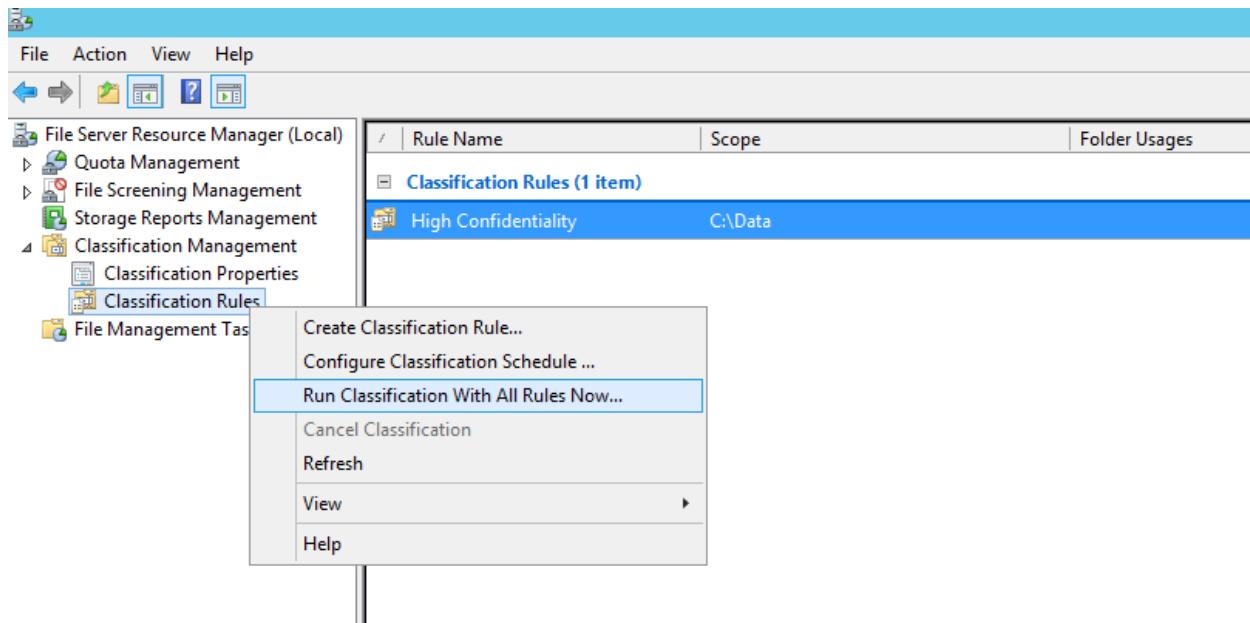
- Save as văn bản này vào thư mục Data trên máy BKAP-DC12-01.



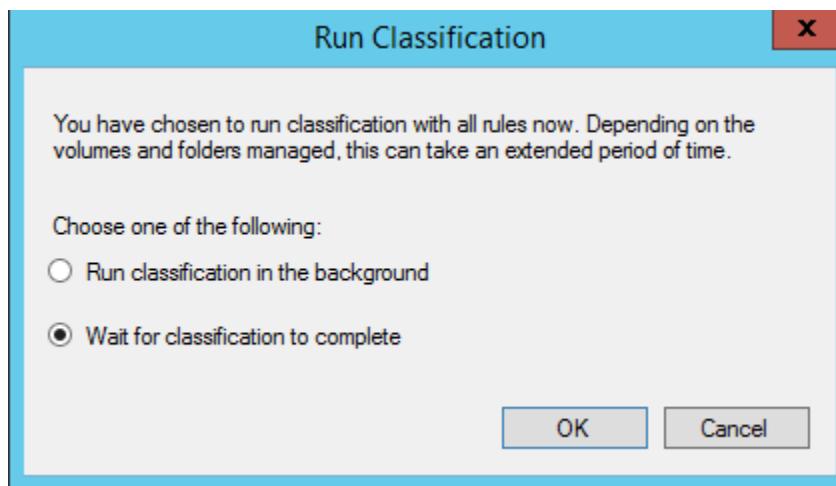
- Chuyển sang máy BKAP-DC12-01, truy cập thư mục **Data** để kiểm tra.



- Vào **File Server Resource Manager**, click chuột phải tại **Classification Rules**, chọn **Run Classification With All Rules Now...**



- Tại cửa sổ **Run Classification**, click chọn vào **Wait for classification to complete, OK**.



- Kiểm tra bảng báo cáo.

Automatic Classification Report
Generated at: 6/15/2016 1:11:09 AM

Report Description: Lists files that were acted on by the classification policy. Use this report to understand how files were classified by the classification policy rules.

Machine: BKAP-DC12-01

Report Folders: 'C:\Data'

Automatic Classification Report Table of Contents

- [Report Totals](#)
- [Size by Owner](#)
- [Size by File Group](#)
- [Size by Property](#)

Report Totals					
Files shown in the report			All files matching report criteria		
Properties	Files	Total size on Disk	Properties	Files	Total size on Disk
0	0	0.00 MB	0	0	0.00 MB

[To top of the current report](#)

Size by Owner		
Owner	Total size on Disk	Files

[To top of the current report](#)

Size by File Group		
File Group	Total size on Disk	Files

- Trong cửa sổ **File Server Resource Manager**, chọn vào **File Management Tasks**, click chuột phải vào **High Confidential** , chọn **Run File Management Task Now...**

File Action View Help

File Server Resource Manager (Local)

- Quota Management
- File Screening Management
- Storage Reports Management
- Classification Management
 - Classification Properties
 - Classification Rules
- File Management Tasks

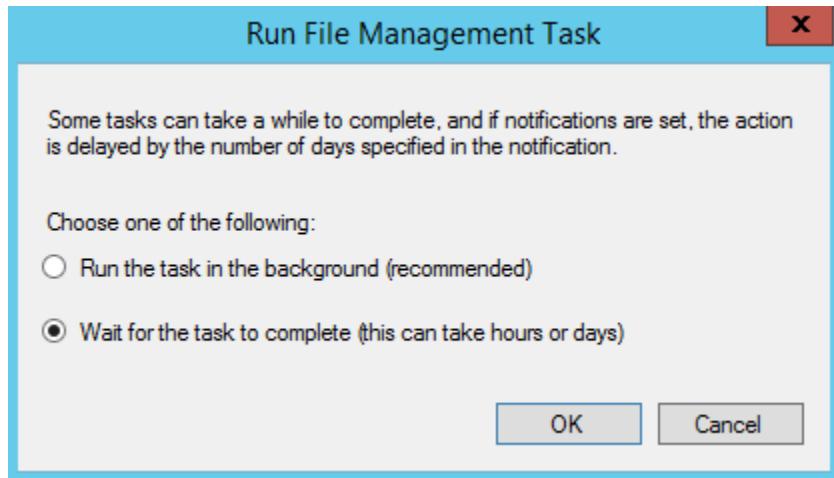
Task Name	Scope	Action
High Confidential	C:\Data	Rms

Scope: C:\Data (1 item)

Right-click context menu for 'High Confidential':

- Edit File Management Task Properties...
- Enable File Management Tasks
- Disable File Management Tasks
- Run File Management Task Now...** (highlighted)
- Cancel File Management Tasks
- Delete
- Help

- Tại cửa sổ **Run File Management Task**, click chọn vào **Wait for the task to complete (this can take hours or days)**, OK.



▪ Kiểm tra báo cáo.



File Management Task Report	
Generated at: 6/15/2016 1:16:03 AM	
Report Description:	Report for the following File Management Task: High Confidential
Action Type:	rms - template = bkaptech RC
Machine:	BKAP-DC12-01
Report Folders:	'C:\Data'

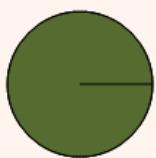
[File Management Task Report Table of Contents](#)

[Report Totals](#)
[Size by Owner](#)
[Size by File Group](#)
[Report statistics](#)
[Report Error for Files](#)

Report Totals			
Files shown in the report		All files matching report criteria	
Files	Total size on Disk	Files	Total size on Disk
1	0.01 MB	1	0.01 MB

[To top of the current report](#)

Size By Owner



Size by Owner		
Owner	Total size on Disk	Files
BKAPTECH\cuongnt	0.01 MB	1

[To top of the current report](#)

Size By File Group



Size by File Group		
File Group	Total size on Disk	Files
Office Files	0.01 MB	1

[To top of the current report](#)

Report statistics

File name	Folder						
	Owner	Size on Disk	Size	Created	Last accessed	Last modified	
BKAPTECH Confidential.docx	C:\Data	BKAPTECH\cuongnt	0.01 MB	0.01 MB	6/15/2016 1:06:02 AM	6/15/2016 1:06:03 AM	6/15/2016 1:06:03 AM

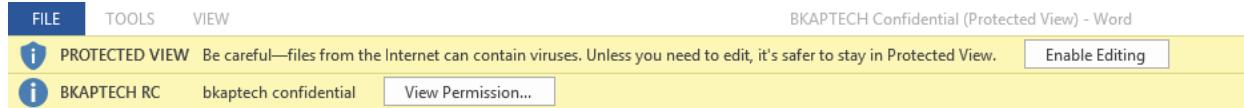
[To top of the current report](#)

Error for files

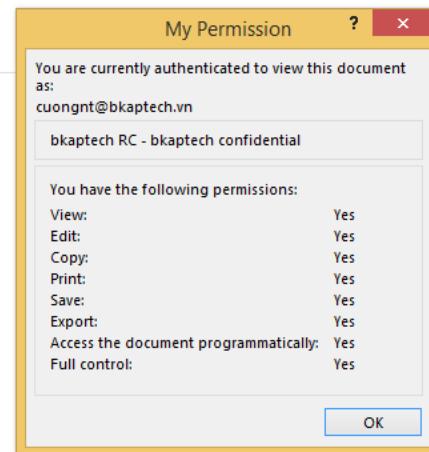
File name	Folder	
	Error	Owner

[To top of the current report](#)

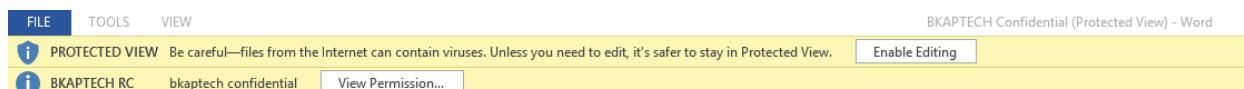
- Chuyển sang máy Client BKAP-WRK08-01, đăng nhập lại bằng user **cuongnt**.
 - Truy cập thư mục **Data**, mở lại file Word vừa tạo ở trên, kiểm tra **permission** của user **cuongnt**.



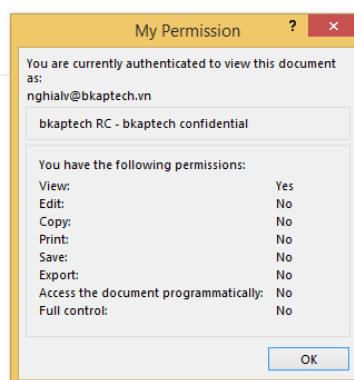
BKAPTECH Confidential



- Đăng nhập bằng user **nghialv** của group **ITs** để kiểm tra permission.



BKAPTECH Confidential



Bài 6:**TRIỂN KHAI DỊCH VỤ DIRECT ACCESS SERVER**

Các nội dung chính được đề cập:

- ✓ Cài đặt và cấu hình dịch vụ Direct Access Server.

6. Cài đặt và cấu hình Direct Access Server**I.Giới thiệu:**

Direct Access là chức năng được *Microsoft* giới thiệu từ *Windows Server 2008 R2* hỗ trợ các máy tính Client chạy Windows 7 kết nối vào hệ thống mạng nội bộ mà không cần thiết lập kết nối VPN. **Direct Access** giúp người dùng có thể kết nối vào mạng nội bộ từ *Internet* mà không cần thực hiện bất cứ thao tác cấu hình nào và giúp người quản trị có thể quản lý các máy tính Client khi các máy tính này ở ngoài *Internet*.

Direct Access Client sử dụng IPv6 để kết nối đến **Direct Access Server** phục vụ cho việc truy cập mạng nội bộ, tuy nhiên nếu hệ thống mạng nội bộ đang sử dụng IPv4, **Direct Access** sẽ dùng các phương pháp để chuyển đổi IPv6, giúp các gói tin IPv6 có thể truyền trong hệ thống mạng nội bộ sử dụng IPv4, các phương pháp sau đây:

- **ISATAP:** Được sử dụng trong mạng nội bộ để các máy tính liên lạc với nhau bằng IPv6. Protocol này sẽ tạo một adapter *ISATAP tunnel* có địa chỉ IPv6, đóng gói dữ liệu trong *IPv4 header* và truyền trong mạng nội bộ. Khi đến đích sẽ giải mã gói tin và sử dụng IPv6.
- **6to4 Protocol:** Hỗ trợ các máy *Direct Access Client* sử dụng địa chỉ IP Public. Protocol này cũng sử dụng 1 adapter *6to4 tunnel* để đưa gói tin IPv6 vào bên trong gói tin IPv4 cho phép truyền gói tin trong mạng nội bộ sử dụng IPv4.
- **Teredo Protocol:** Teredo đóng gói các gói tin IPv6 theo dạng gói tin IPv4 để chuyển tiếp qua các *NAT Server* chạy IPv4 và mạng nội bộ IPv4. Các gói tin IPv6 này sẽ được gửi bằng giao thức **UDP (User Datagram Protocol)** port 3544. Windows Vista, Windows 7 và Windoww 8 mặc định đã được hỗ trợ sử dụng Teredo.

- **IP-HTTPS Protocol:** Đây là protocol do Microsoft phát triển cho phép các **Direct Access Client** kết nối với **Direct Access Server** bằng port 443 (nếu port này được mở trên Server)

Để triển khai dịch vụ **Direct Access** có 2 cách:

a. **Simplified Direct Access:** Theo cách này **Direct Access Server** và **Network Location Server** sẽ tích hợp chung trên 1 Server và sử dụng *Certificate* tự phát sinh (*Self-Signed Certificate*), do đó ta không cần triển khai dịch vụ *Active Directory Certificate Service (ADCS)* trong hệ thống. Tuy nhiên cách triển khai này chỉ không hỗ trợ dịch vụ NAP và các phương pháp chứng thực two-factor như smartcard...

b. **Full PKI Direct Access:** Theo cách này thì việc cấu hình sẽ phức tạp hơn, ta cần triển khai cơ sở hạ tầng **PKI** trong hệ thống bằng cách cài đặt và cấu hình dịch vụ *Active Directory Certificate Service (ADCS)* để cấp các *Certificate* cần thiết cho các **Server** và **Client**.

Bài này sẽ trình bày thao tác cấu hình **Direct Access** theo cách *Full PKI* trên *Windows Server 2012* hỗ trợ các máy **Client** chạy *Windows 8* kết nối vào mạng nội bộ từ bên ngoài *Internet*.

II. Yêu cầu chuẩn bị:

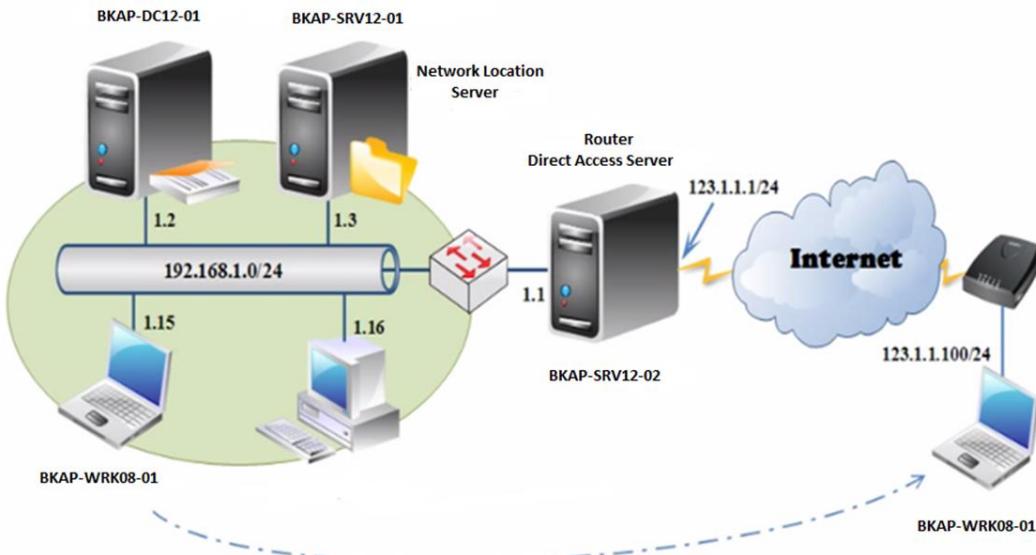
Bài lab gồm 4 máy:

- + **BKAP-DC12-01:** máy Domain Controller chạy Windows Server 2012 (quản lý miền **bkaptech.vn**).
- + **BKAP-SRV12-01:** Domain member đóng vai trò **Network Location Server (NLS)** chạy Windows Server 2012. Đây là Server giúp các **Direct Access Client** xác định vị trí của nó. Nếu **Direct Access Client** liên lạc được với **Network Location Server** thì **Direct Access Client** xác định nó đang ở trong mạng nội bộ và sử dụng **DNS** của hệ thống để phân giải.
- + **BKAP-SRV12-02:** Domain Member đảm nhận vai trò **Direct Access Server** chạy Windows Server 2012.
- + **BKAP-WRK08-01:** **Client** (Domain member) chạy Windows 8.

III, Mô hình Lab:

HỆ THỐNG ĐÀO TẠO CNTT QUỐC TẾ BACHKHOA-APTECH

Lab Cấu hình Direct Access Server trên Windows Server 2012

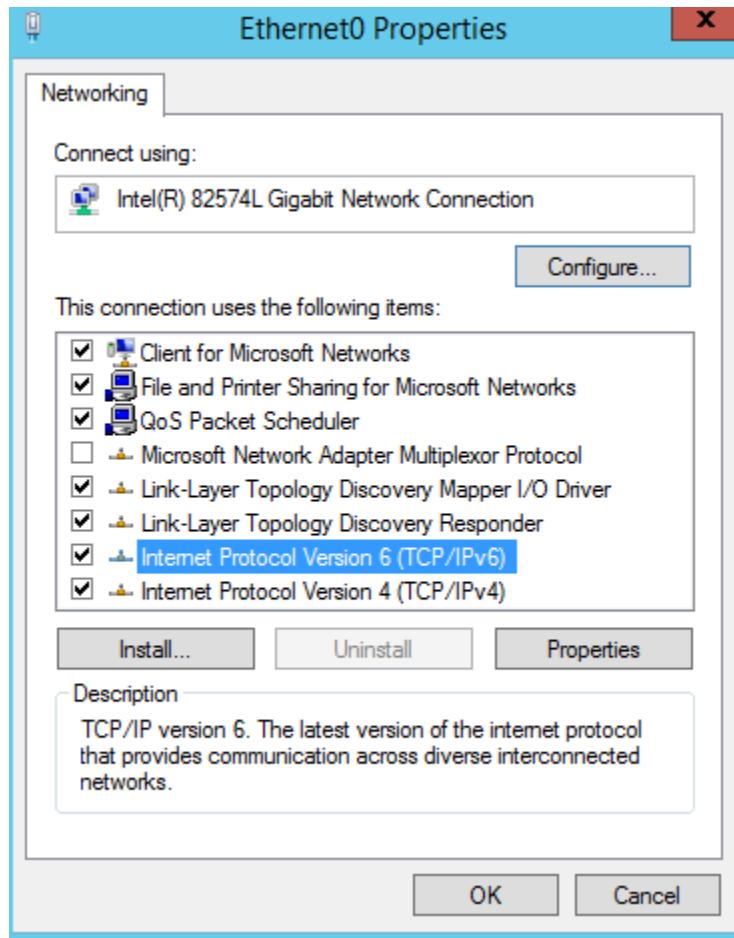


Sơ đồ địa chỉ như sau:

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	192.168.1.10
Subnet Mask	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
Gateway	192.168.1.1	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	192.168.1.2

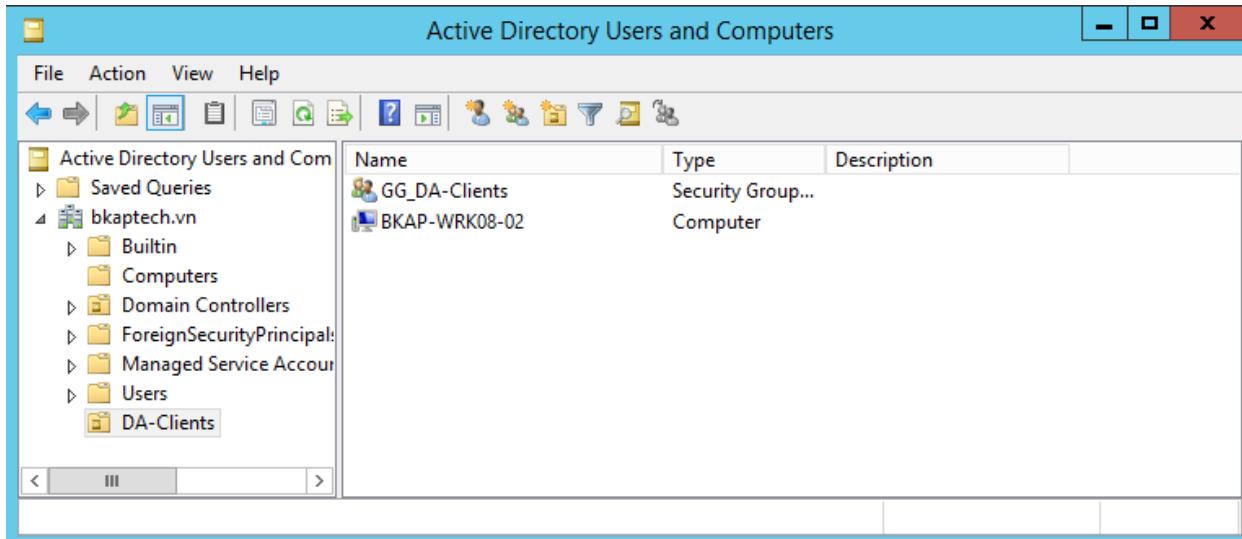
IV, Các bước triển khai:

- Mở các máy ảo, kết nối như mô hình, đặt địa chỉ IP các máy theo sơ đồ trên, thực hiện **enable** địa chỉ *IPv6* trên tất cả các máy.

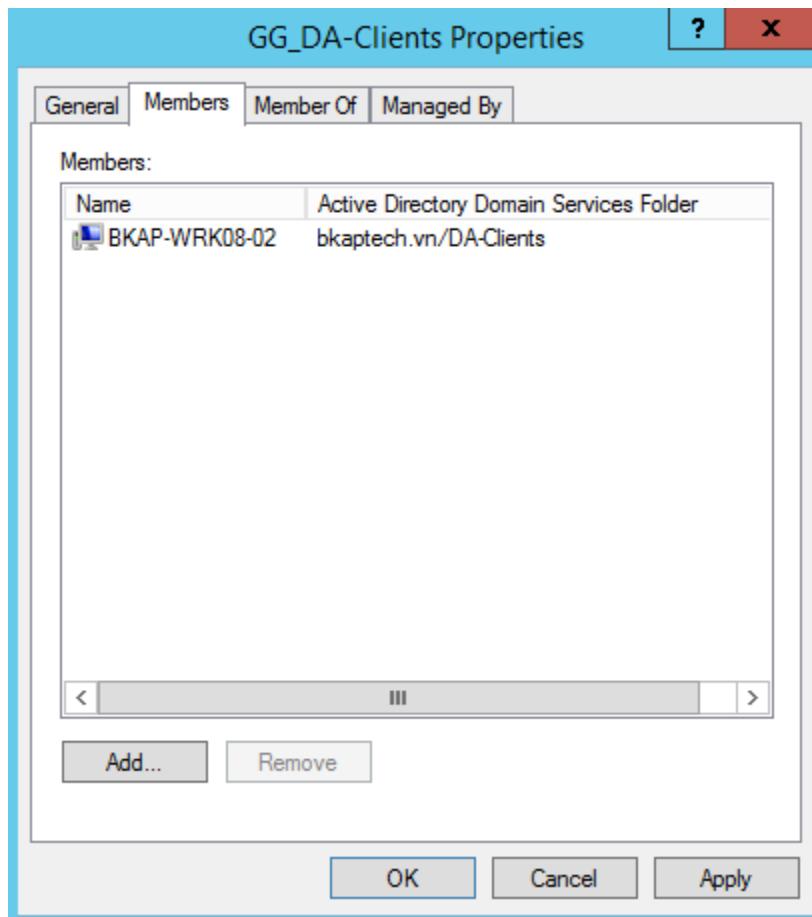


- Trên DC12-01:

- Tạo OU tên **DA-Clients** , trong OU **DA-Clients** tạo group tên **GG_DA-Clients** , move máy Client **WRK08-01** vào OU này.

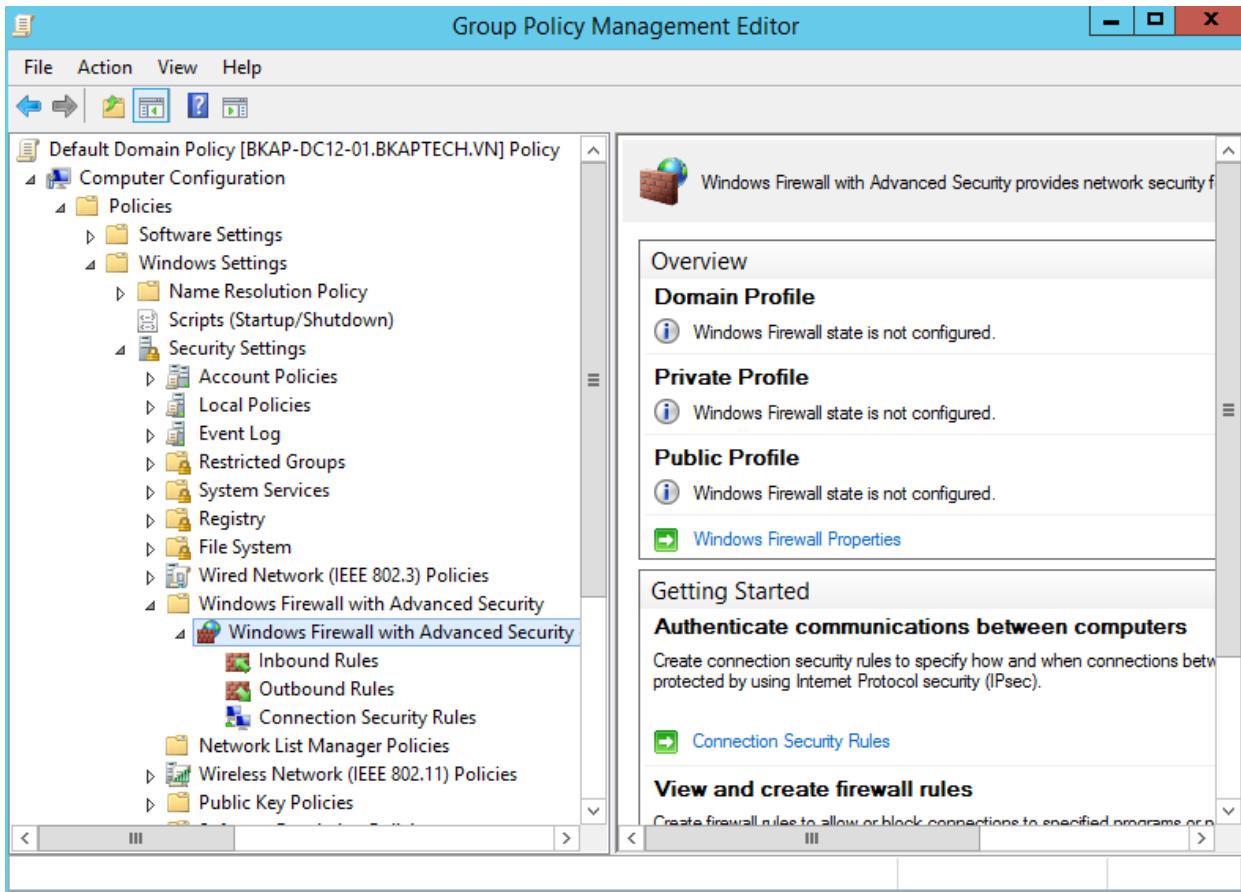


- Thêm máy Client WRK08-01 vào danh sách thành viên group **GG_DA-Clients**.

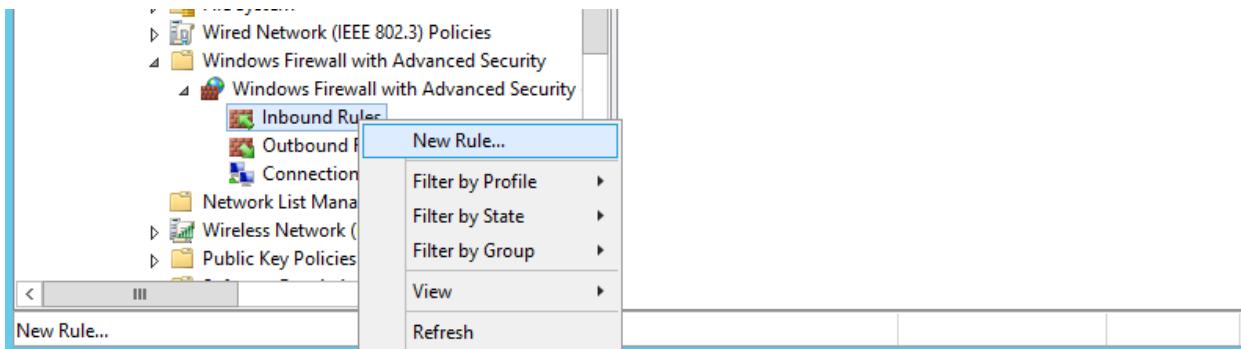


- Do **Direct Access** sử dụng nền tảng IPv6, ta cần tạo 2 rule (**In** và **Out**) cho phép chấp nhận các gói tin ICMPv6 => chỉnh **Default Domain Policy** để tạo 2 Rule này và áp dụng trên tất cả các máy tính trong domain.
 ⇒ Mở *Group Policy Management*, điều chỉnh GPO **Default Domain Policy** / Edit.

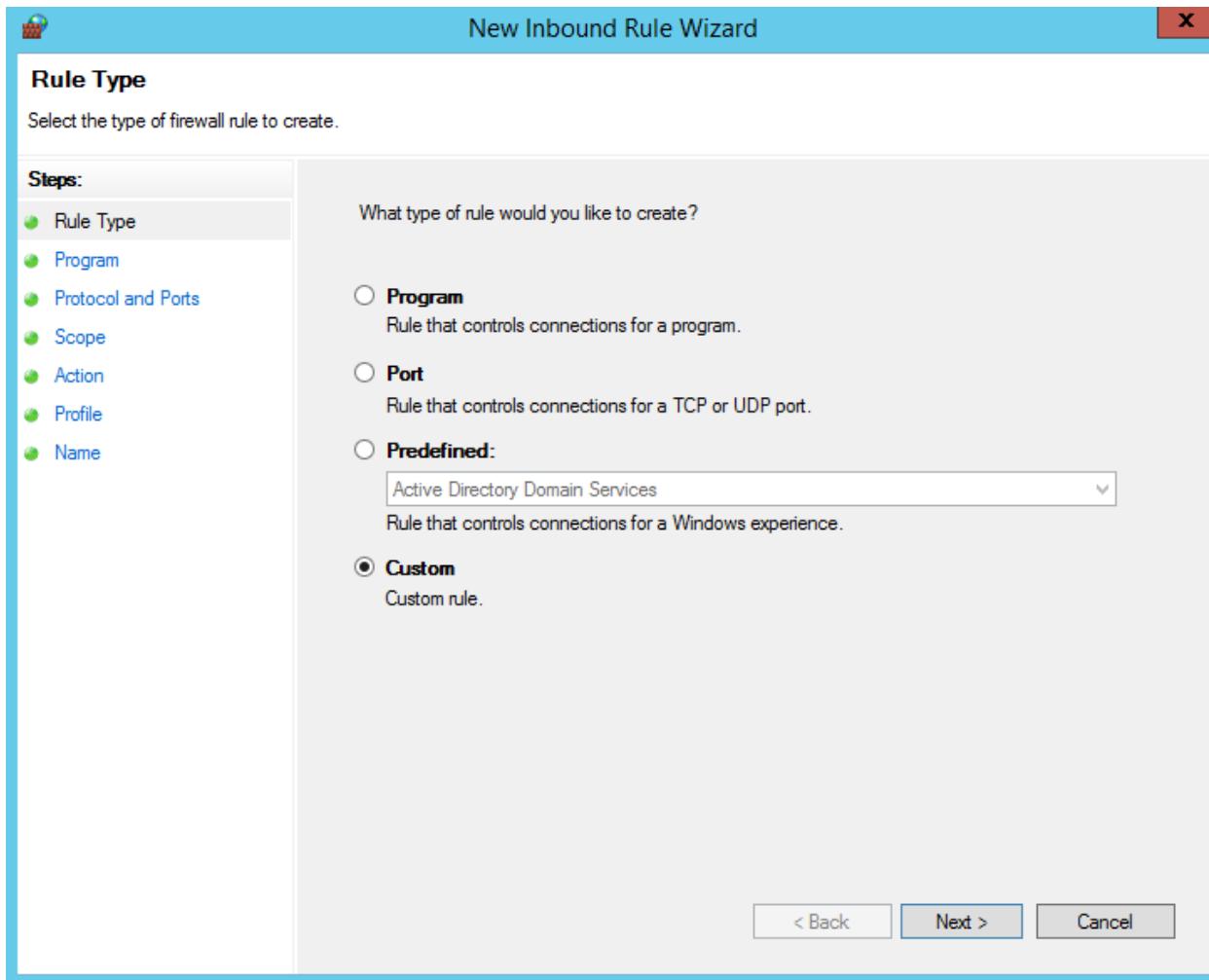
- Trong cửa sổ **Group Policy Management Editor**, chọn vào **Computer Configuration / Policies / Windows Settings / Security Settings / Windows Firewall with Advanced Security / Windows Firewall with Advanced Security**.



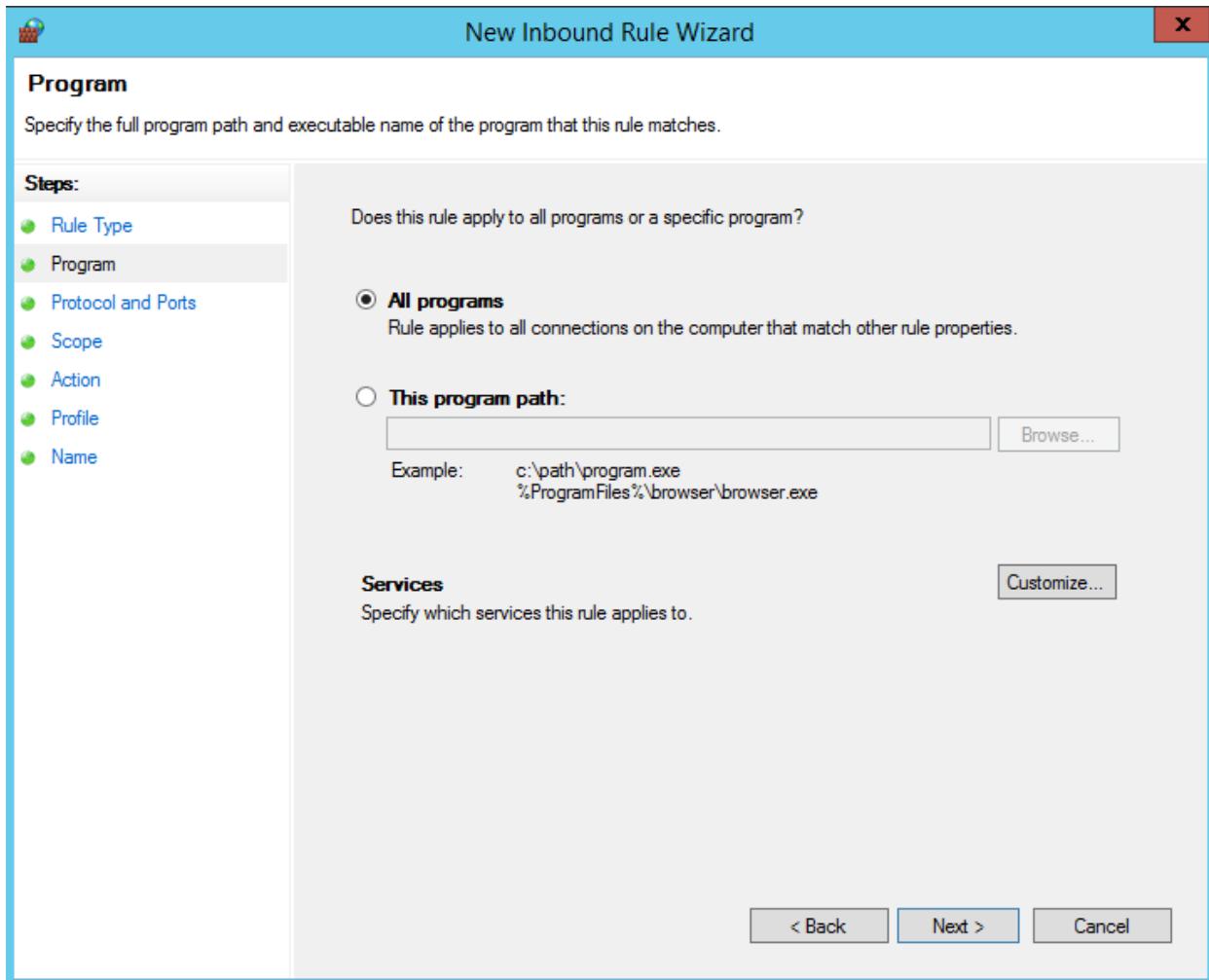
- Tạo *Inbound Rule*:
 - Chọn vào **Inbound Rules / New Rule...**



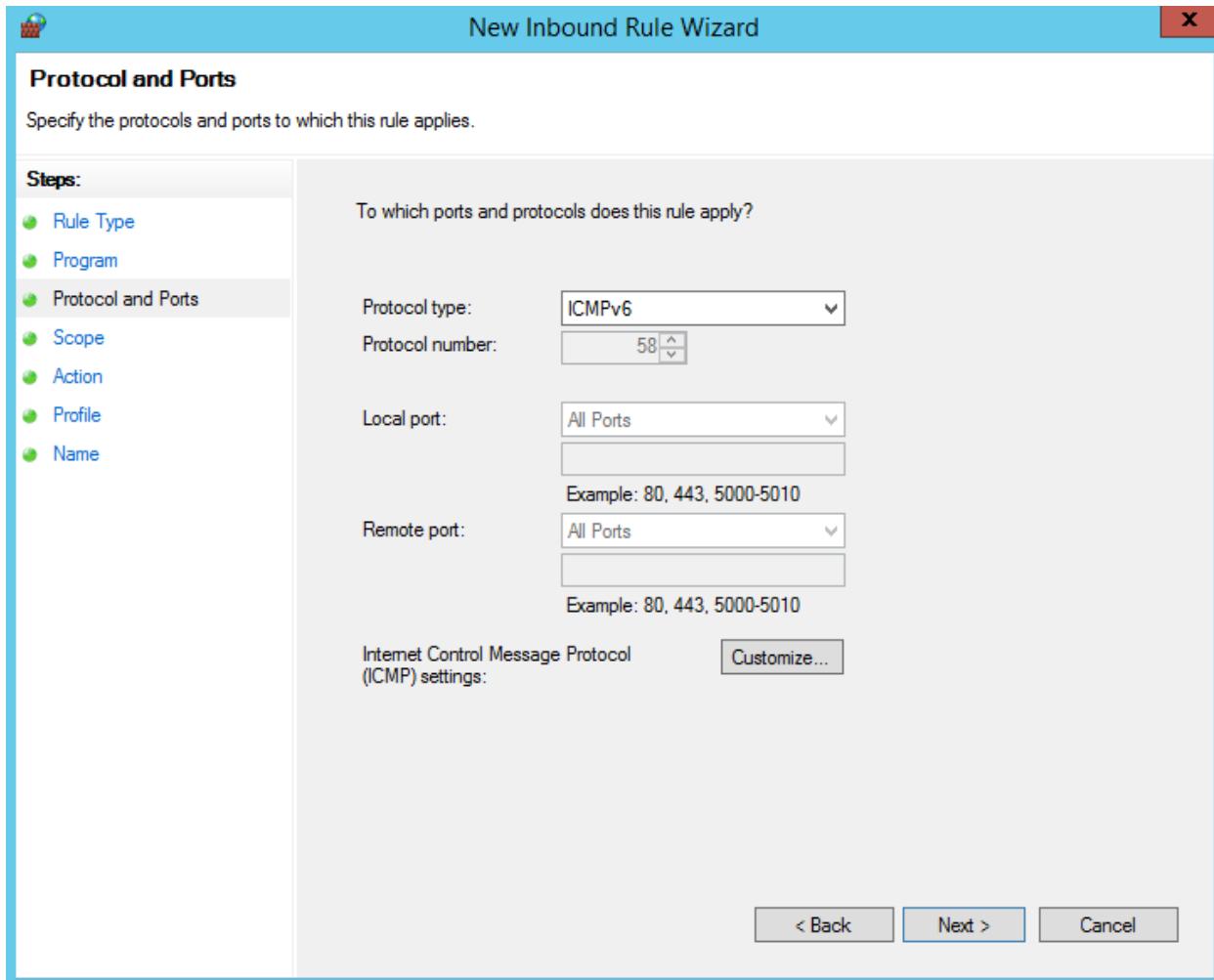
- Tại cửa sổ **Rule Type**, chọn vào **Custom**:



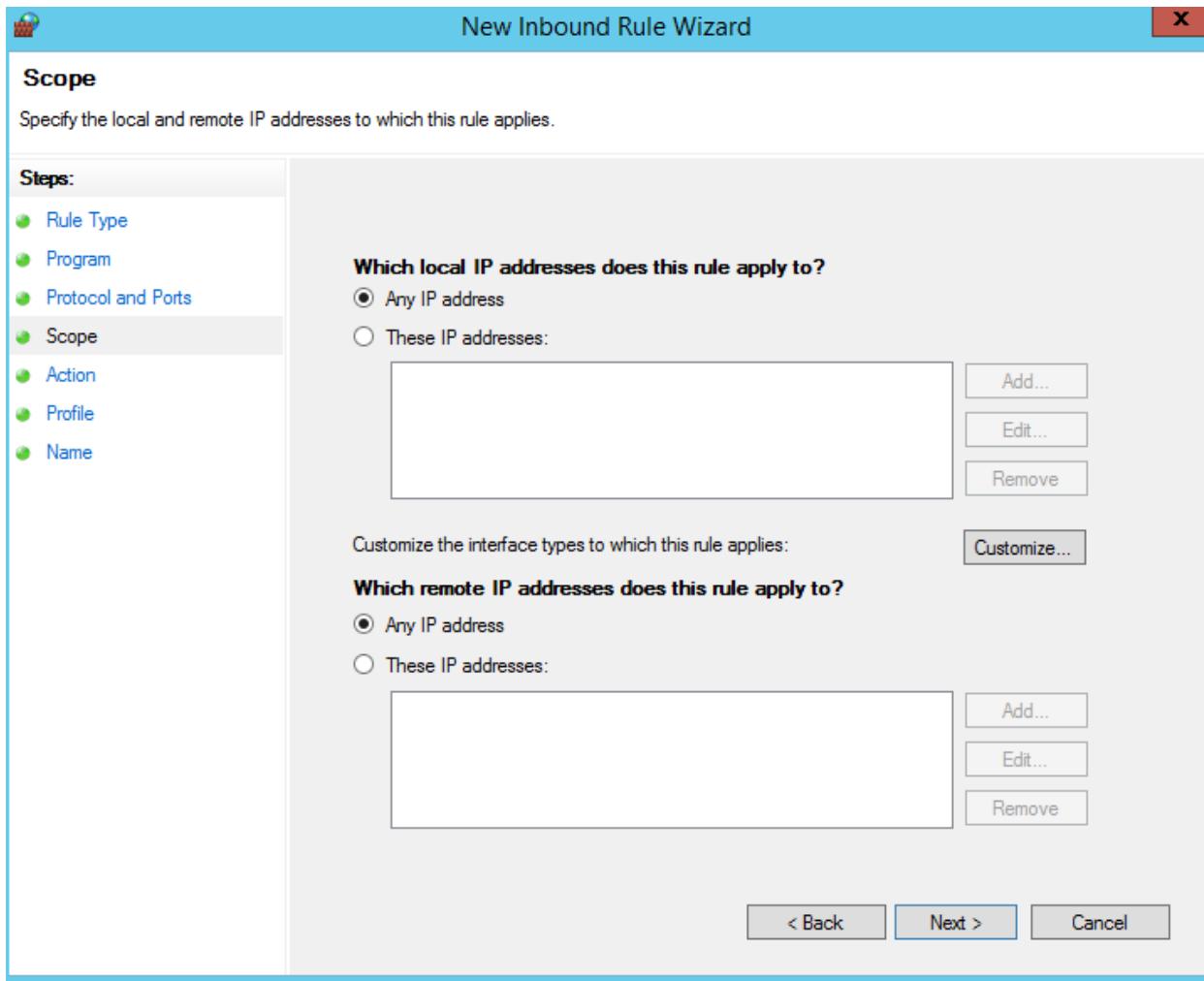
- Tại cửa sổ **Program**, chọn **All programs**, click vào **Next**.



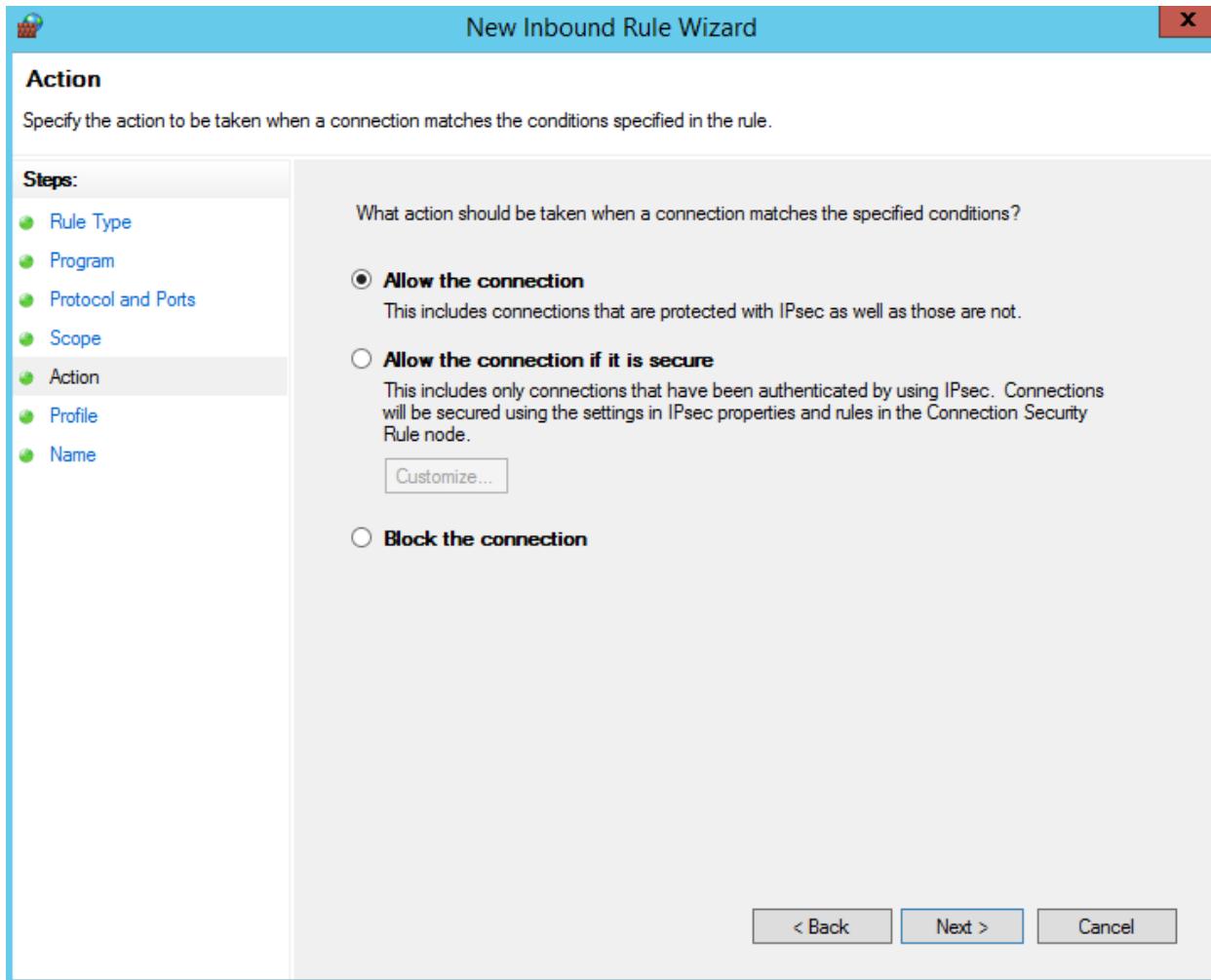
- Tại cửa sổ **Protocol and Ports**, trong mục **Protocol type**, chọn **ICMPv6**, click vào **Next**.



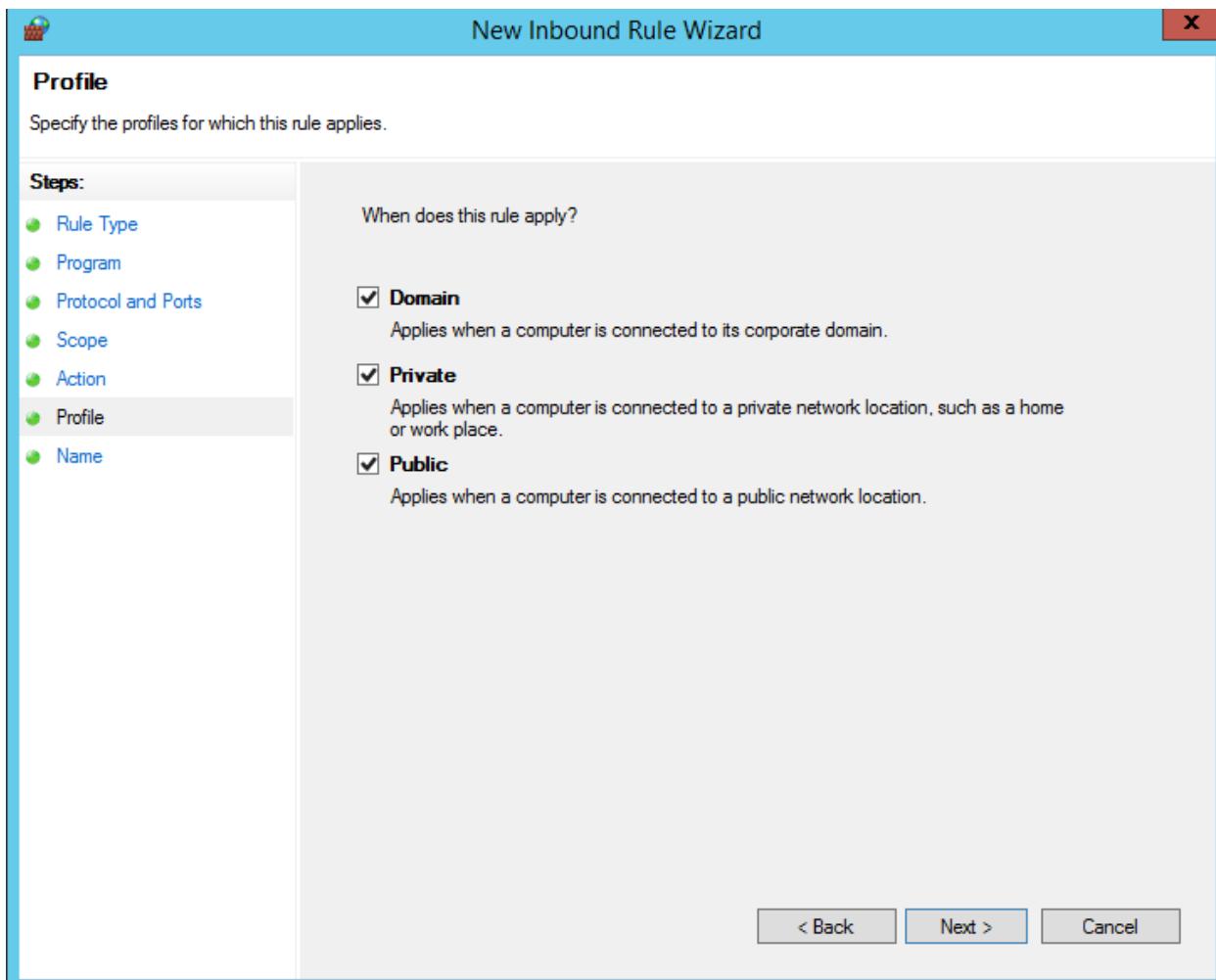
- Tại cửa sổ **Scope**, click vào **Next**.



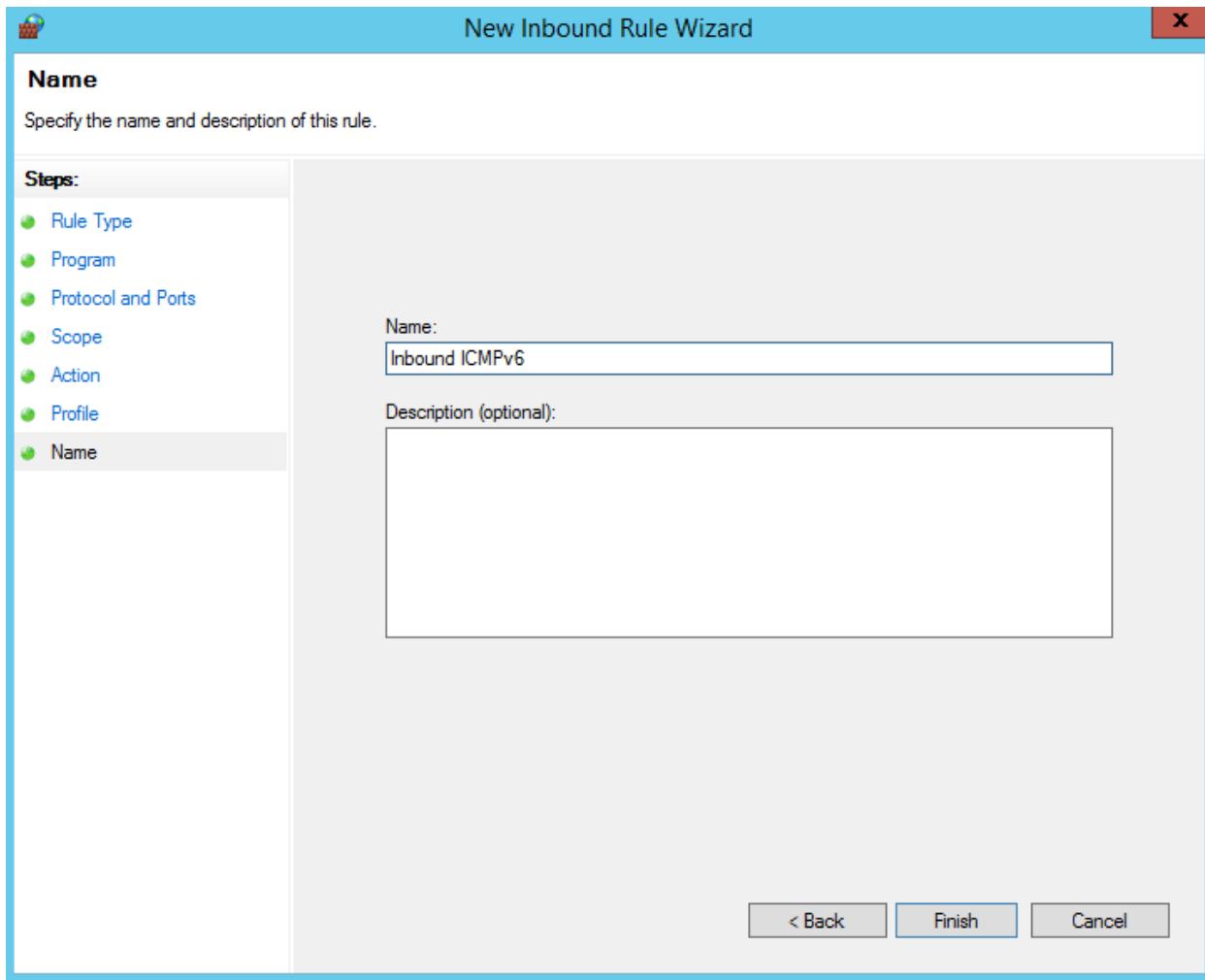
- Chọn **Allow the connection** để chấp nhận các gói tin **ICMPv6** đi vào.



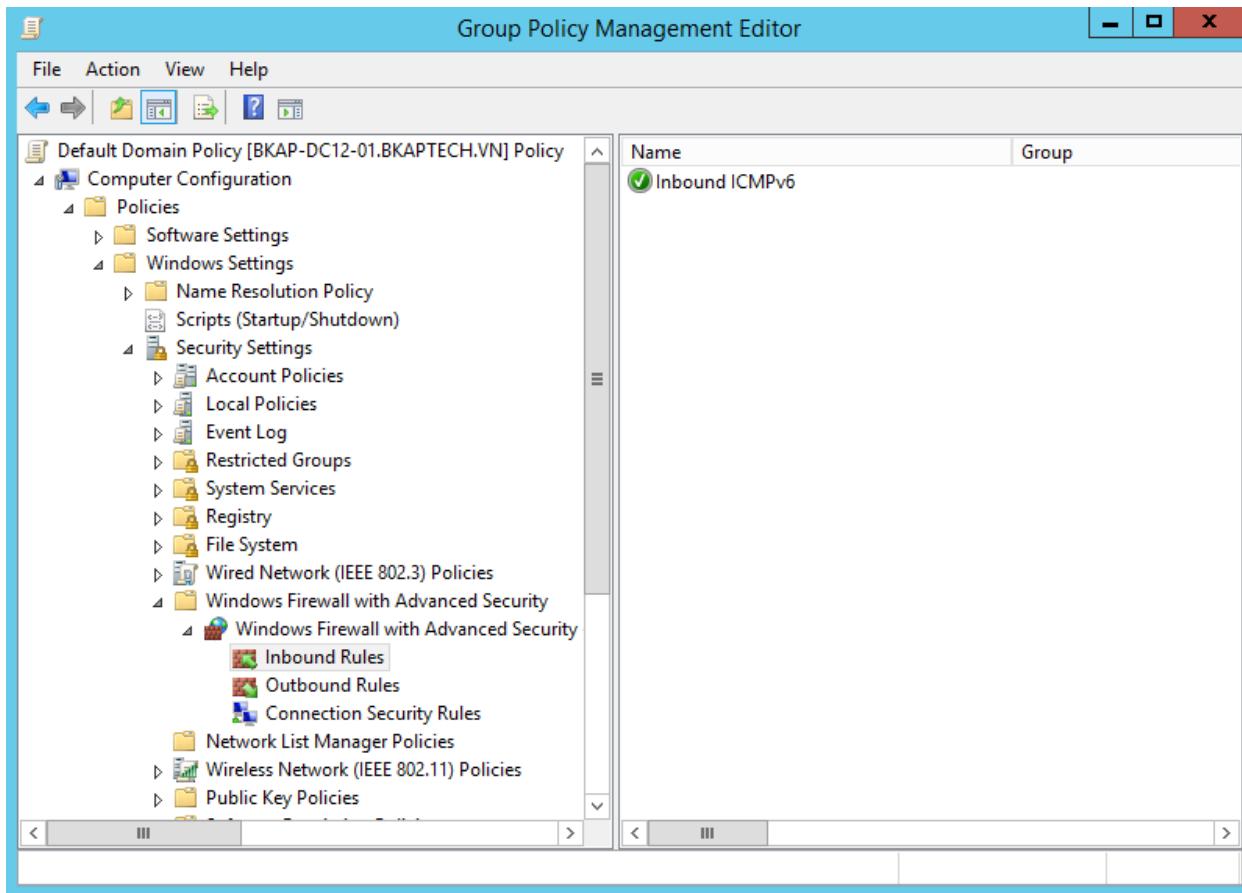
- Tại cửa sổ **Profile**, click vào **Next**.



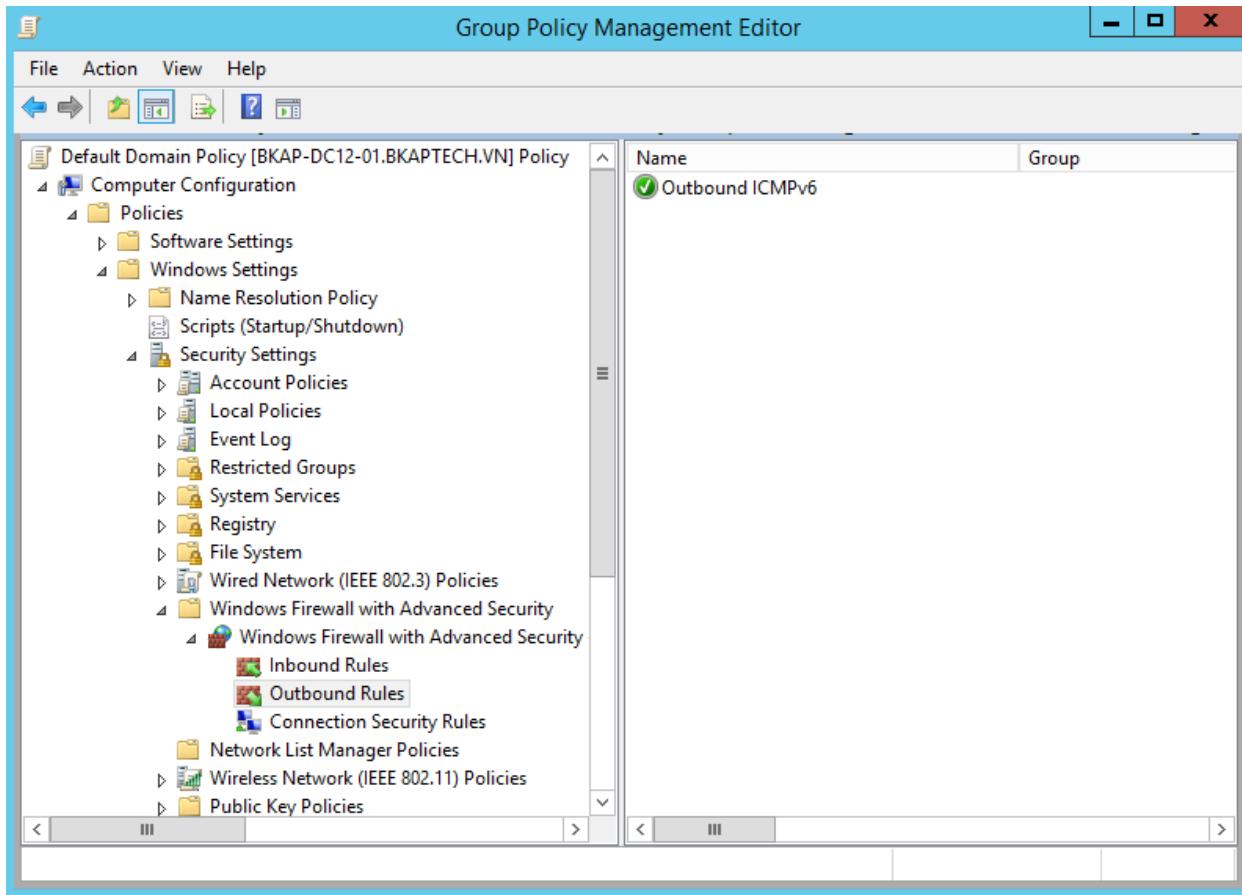
- Đặt tên cho rule là **Inbound ICMPv6 / Finish** :



- Tạo thành công Rule Inbound ICMPv6:



- Tạo Outbound Rule tương tự như các bước trên:



- Cập nhật Policy:

```

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

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

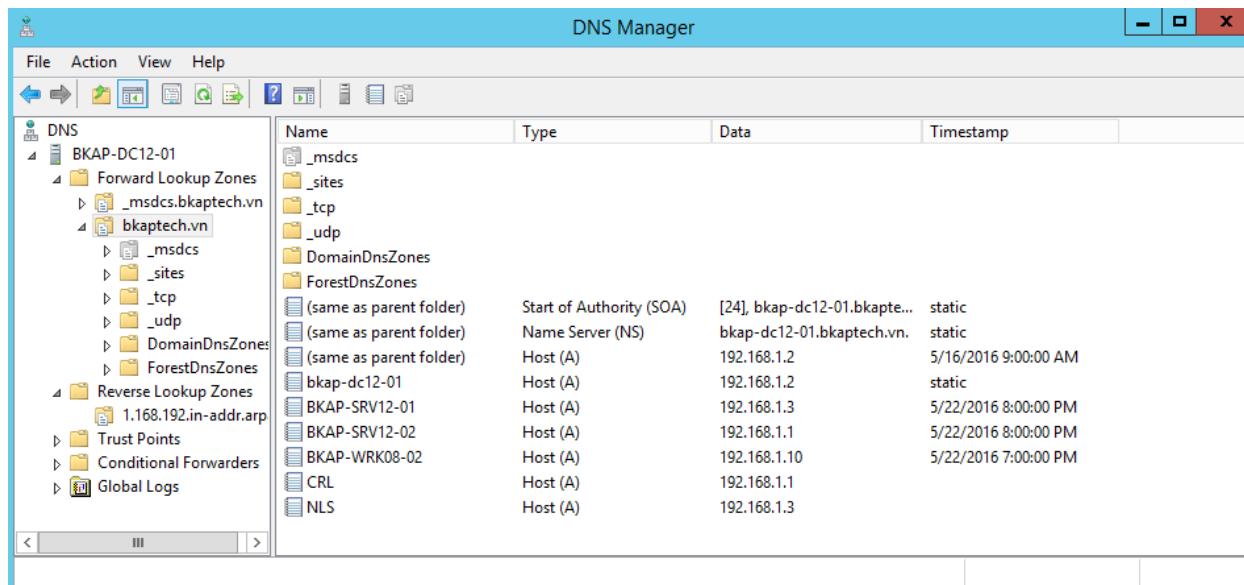
C:\Users\Administrator>gpupdate /force
Updating policy...

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

C:\Users\Administrator>

```

- Mở **DNS**, tạo 2 *host (A)* như sau:
 - **CRL** có IP là **192.168.1.1** (đây là tên của máy sẽ chứa Revocation List là máy **Direct Access Server**).
 - **NLS** có IP là **192.168.1.3** (đây là máy **Network Location Server**).



- Mặc định **DNS** chặn các yêu cầu phân giải **ISATAP** và **WPAD**, ta dùng lệnh “**dnscmd /info /GlobalQueryBlockList**” để kiểm tra:

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

C:\Users\Administrator>dnscmd /info /GlobalQueryBlockList
Query result:
String: wpad
String: isatap

Command completed successfully.

C:\Users\Administrator>
```

- Do Direct Access cần sử dụng **ISATAP**, do đó ta cần loại bỏ **ISATAP** khỏi danh sách chặn của **DNS** bằng lệnh

“**dnscmd /Config /GlobalQueryBlockList wpad**”

```

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

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

C:\Users\Administrator>dnscmd /info /GlobalQueryBlockList

Query result:
String: wpad
String: isatap

Command completed successfully.

C:\Users\Administrator>dnscmd /Config /GlobalQueryBlockList wpad

Registry property GlobalQueryBlockList successfully reset.
Command completed successfully.

C:\Users\Administrator>

```

- Kiểm tra lại ta thấy **DNS** chỉ còn **WPAD** , không chặn **ISATAP**.

```

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

C:\Users\Administrator>dnscmd /info /GlobalQueryBlockList

Query result:
String: wpad
String: isatap

Command completed successfully.

C:\Users\Administrator>dnscmd /Config /GlobalQueryBlockList wpad

Registry property GlobalQueryBlockList successfully reset.
Command completed successfully.

C:\Users\Administrator>dnscmd /info /GlobalQueryBlockList

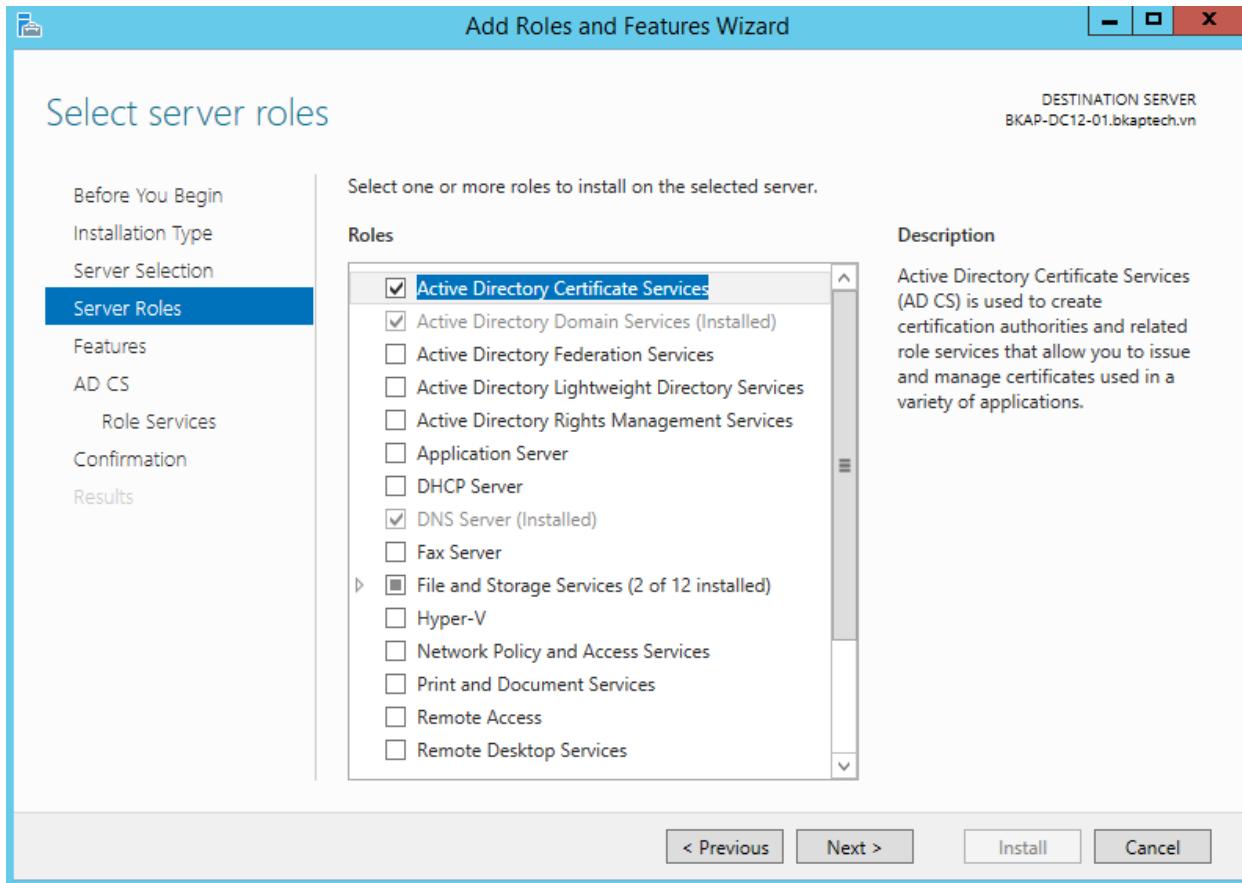
Query result:
String: wpad

Command completed successfully.

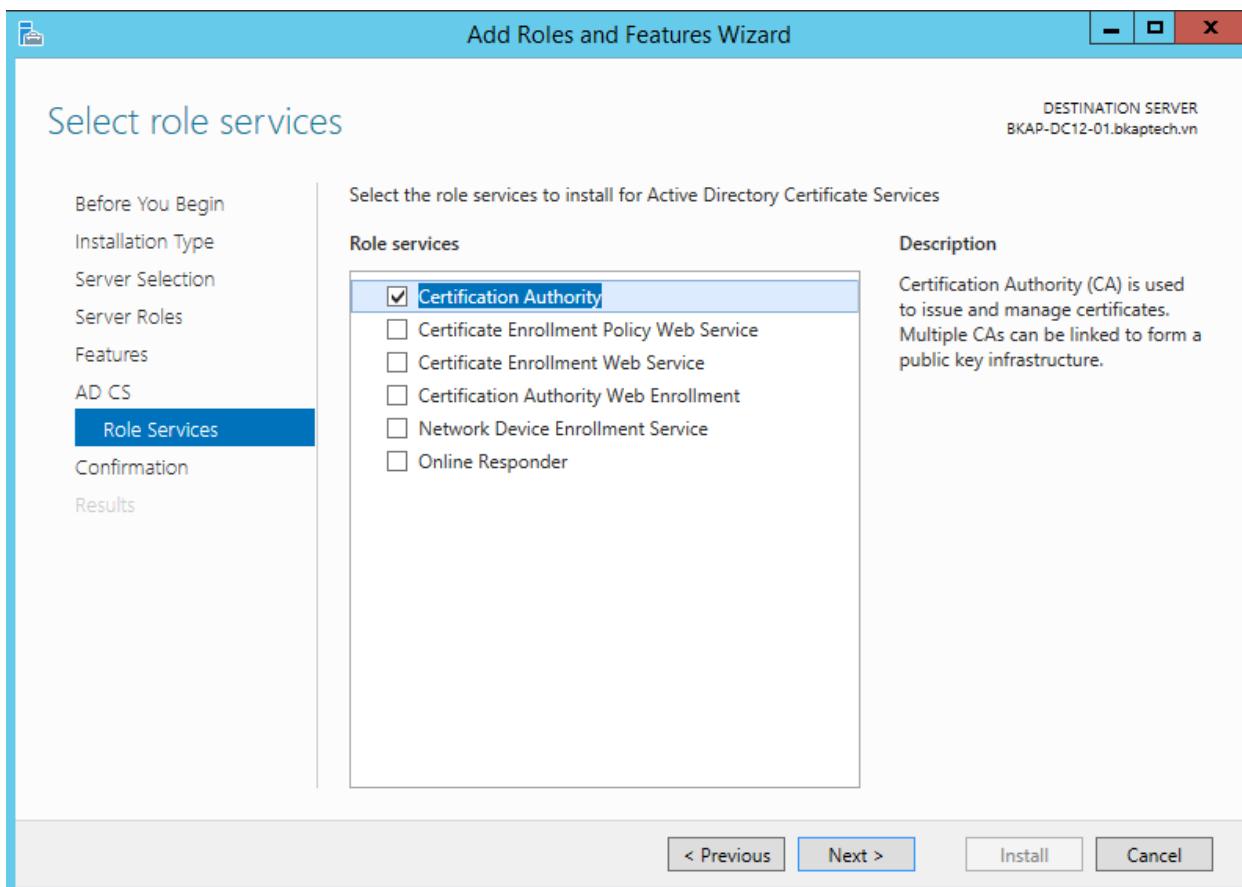
C:\Users\Administrator>

```

- Cài đặt và cấu hình CA Server : trên máy **DC12-01** , mở **Server Manager**, cài đặt dịch vụ *Active Directory Certificate Services*.



- Chọn vào **Certificate Authority** và click vào **Install** để cài đặt.



Add Roles and Features Wizard

Confirm installation selections

DESTINATION SERVER
BKAP-DC12-01.bkaptech.vn

Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD CS
Role Services
Confirmation
Results

To install the following roles, role services, or features on selected server, click Install.

Restart the destination server automatically if required

Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.

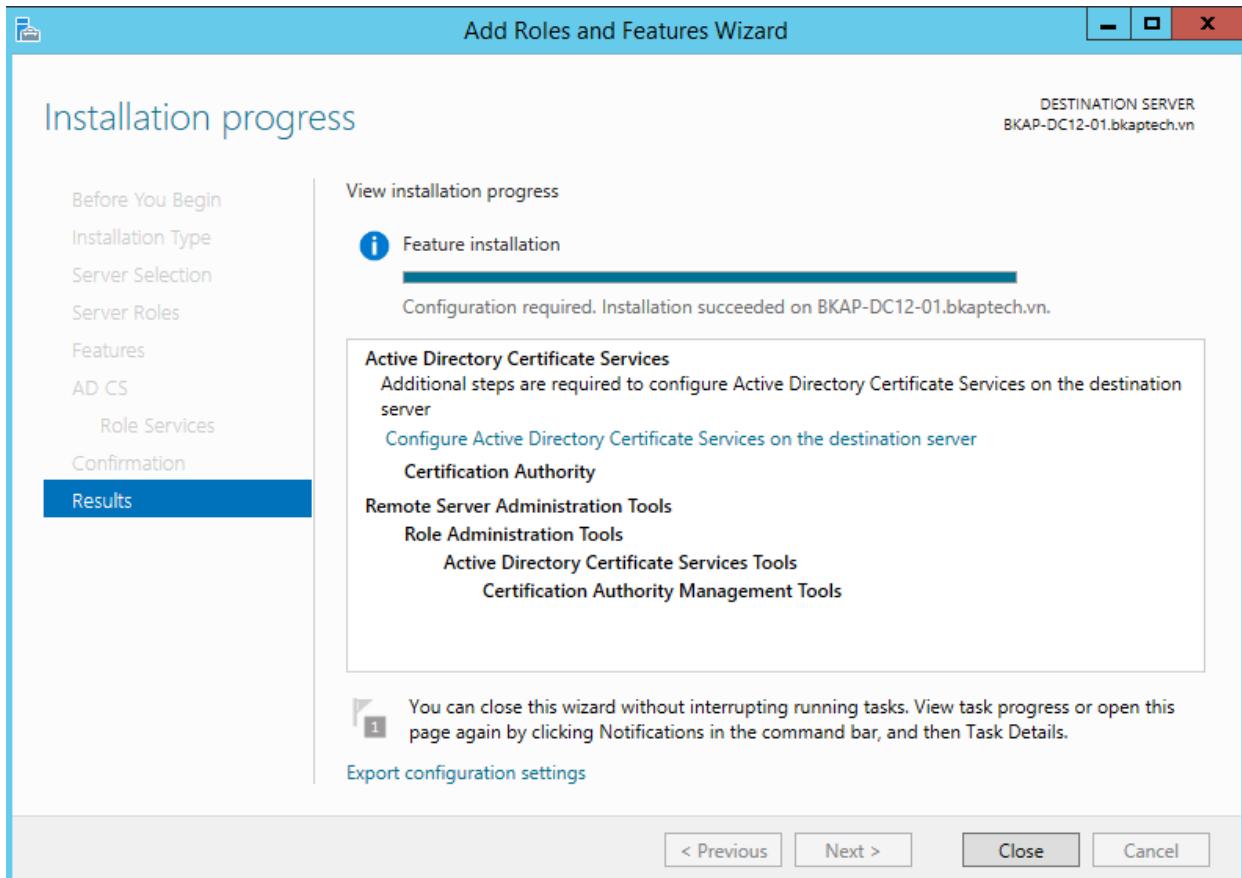
Active Directory Certificate Services
 Certification Authority

Remote Server Administration Tools
 Role Administration Tools
 Active Directory Certificate Services Tools
 Certification Authority Management Tools

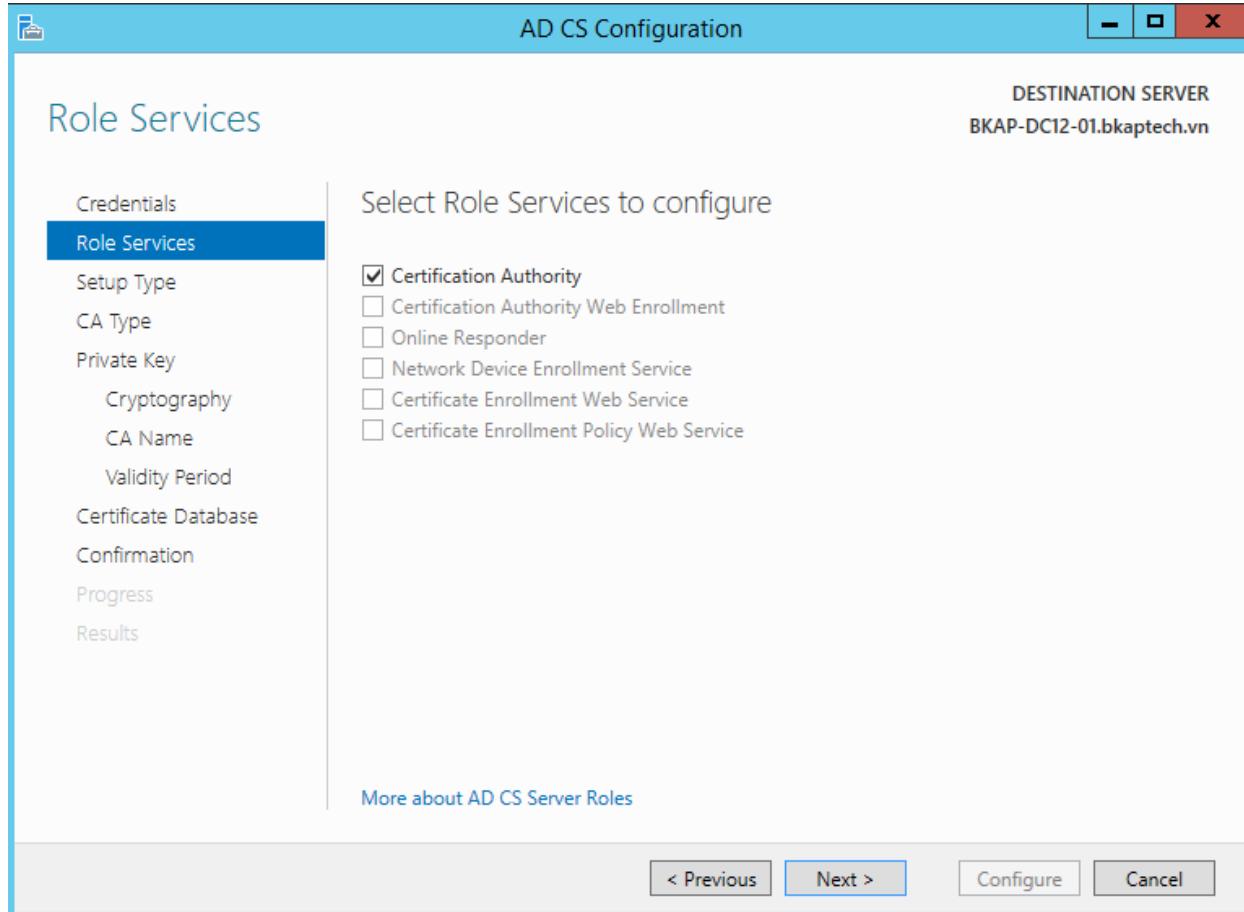
Export configuration settings
Specify an alternate source path

< Previous Next > **Install** Cancel

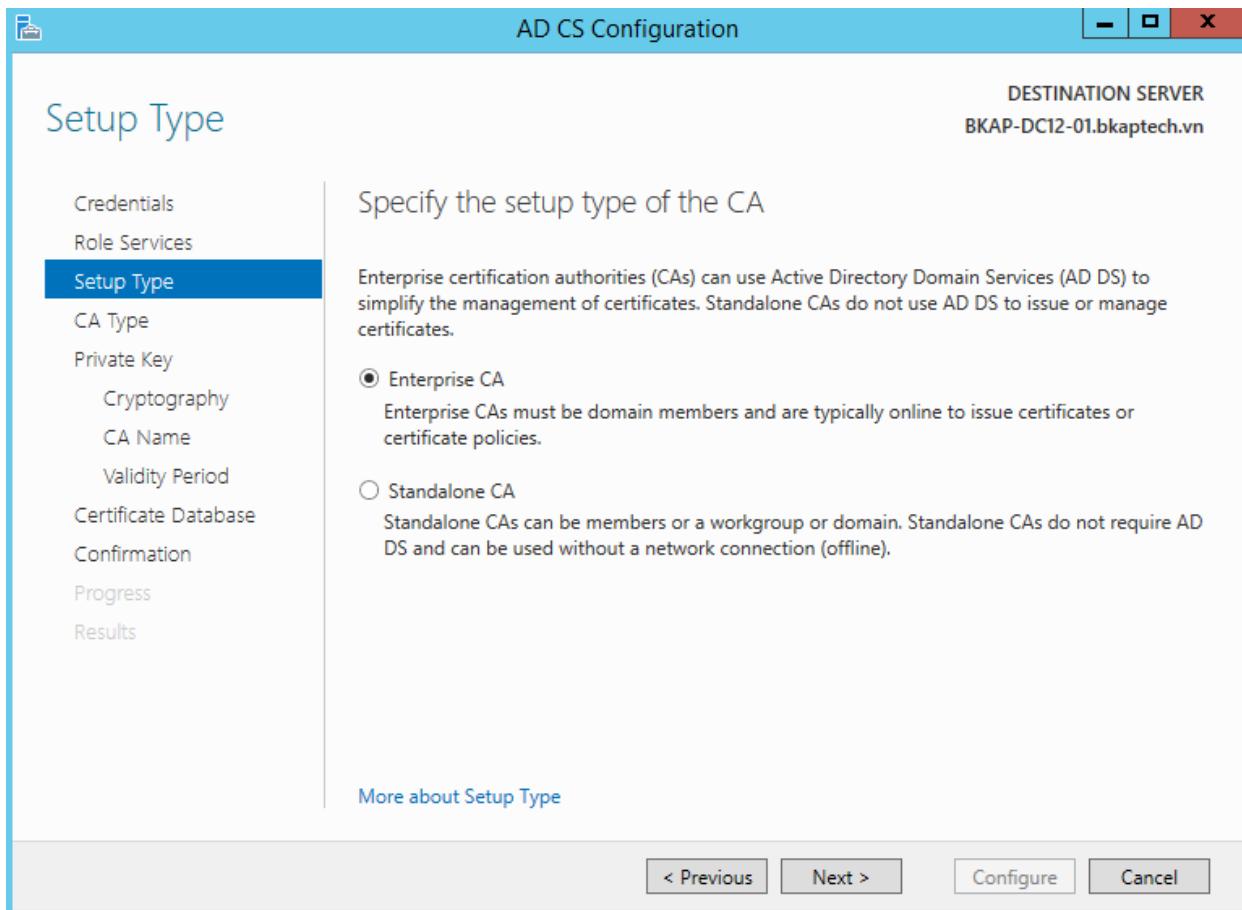
- Khi quá trình cài đặt hoàn tất, nhấn chọn **Configure Active Directory Certificate Service on the destination server** để thực hiện thao tác cấu hình cho dịch vụ.



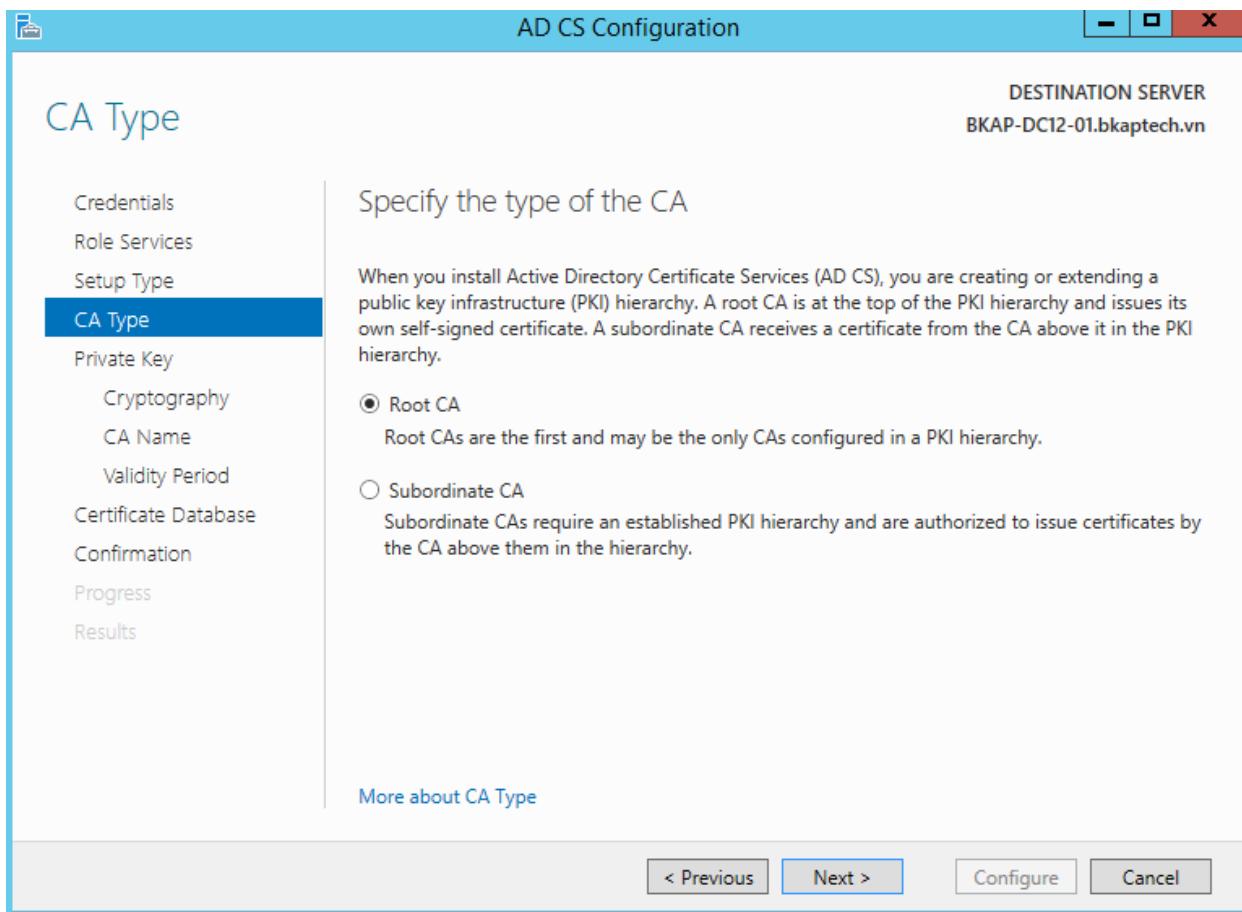
- Tại cửa sổ **Role Services**, tích chọn vào **Certification Authority**.



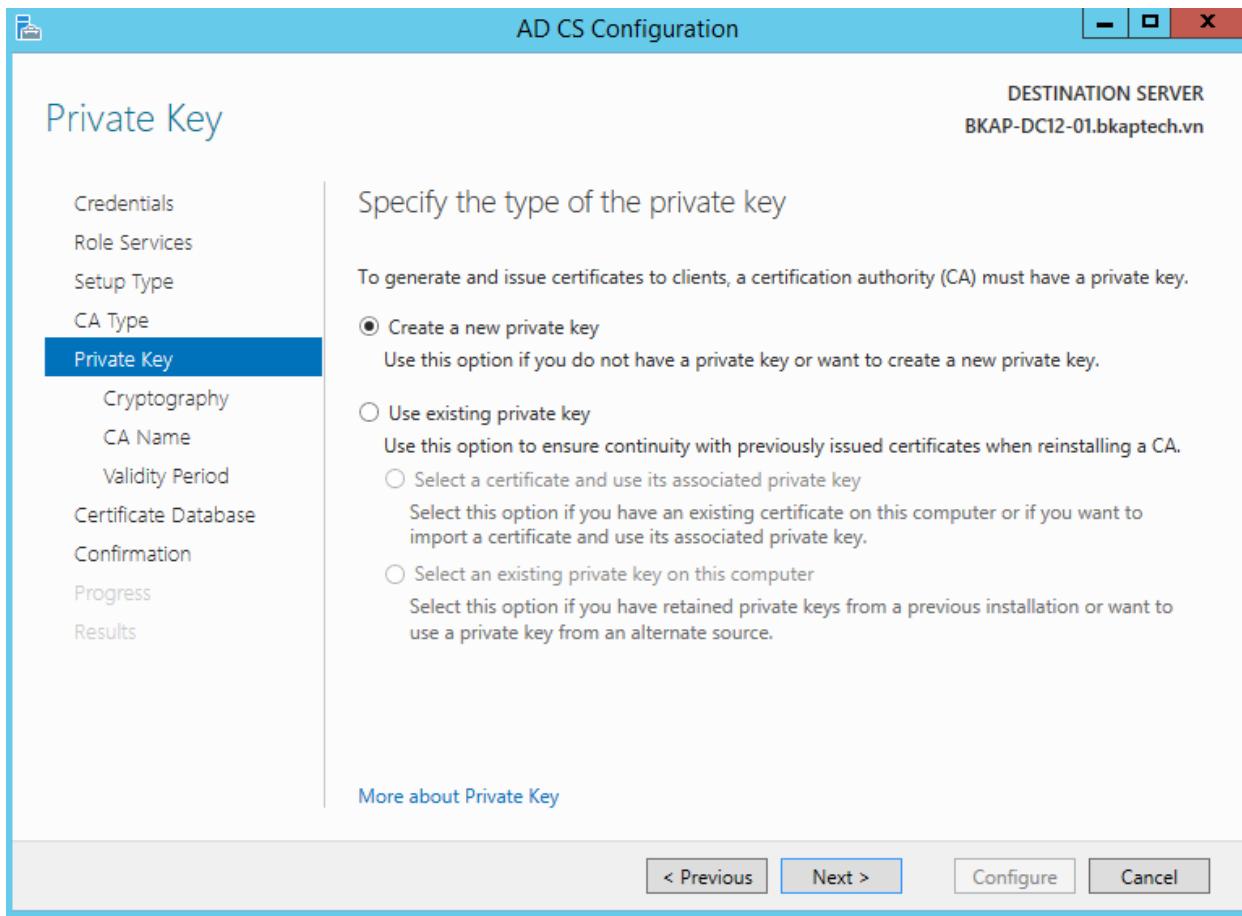
- Chọn loại CA là **Enterprise CA**.

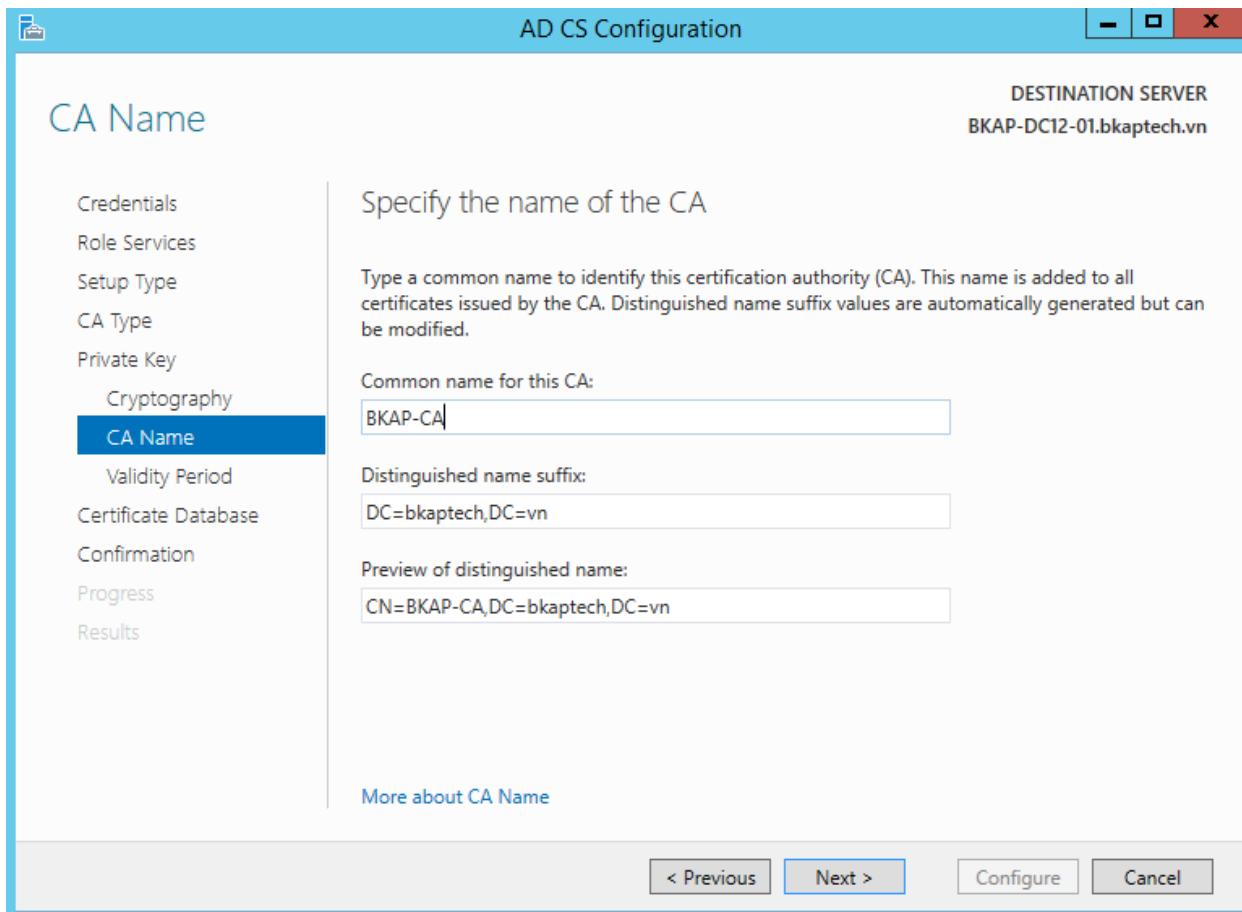


▪ Chọn Root CA:

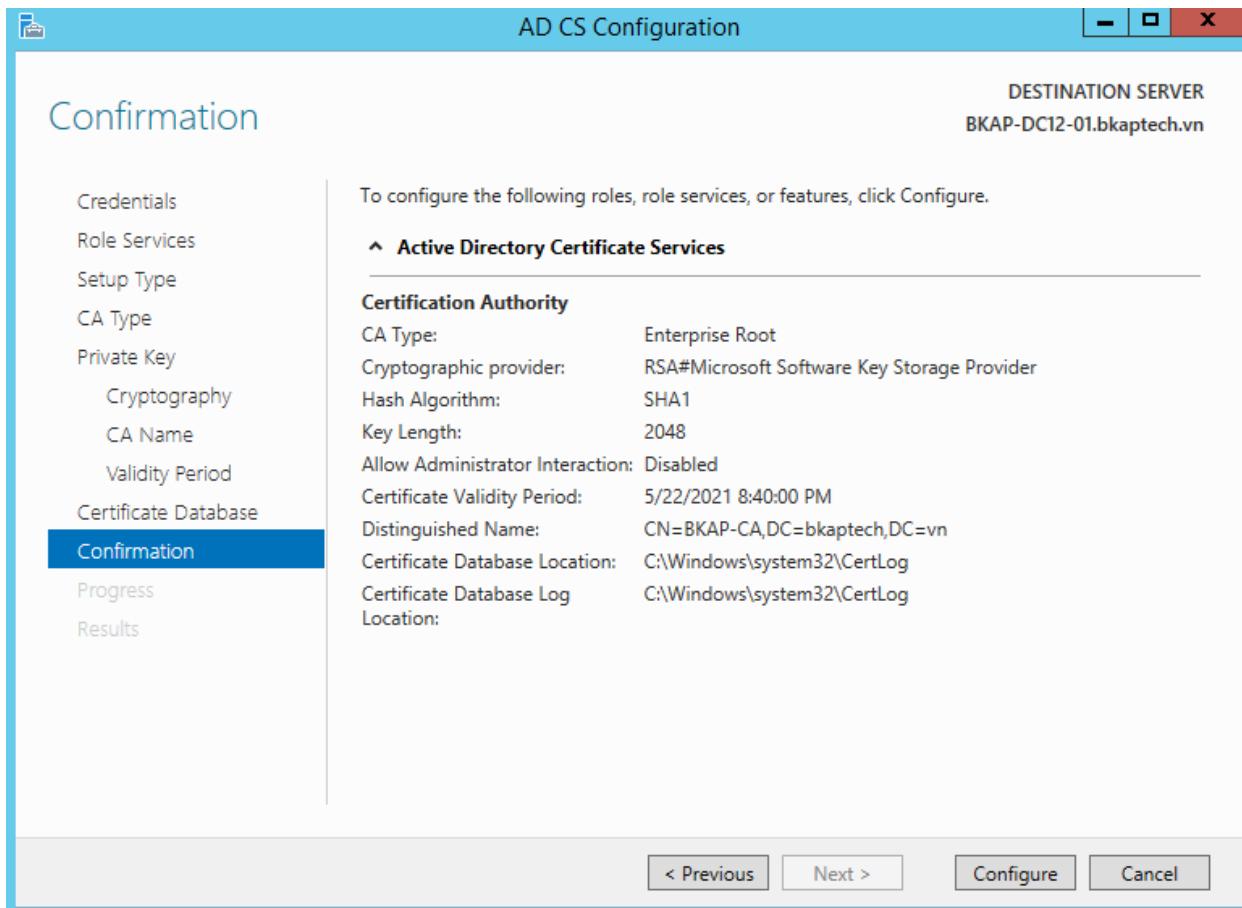


▪ Chọn Create a new private key:

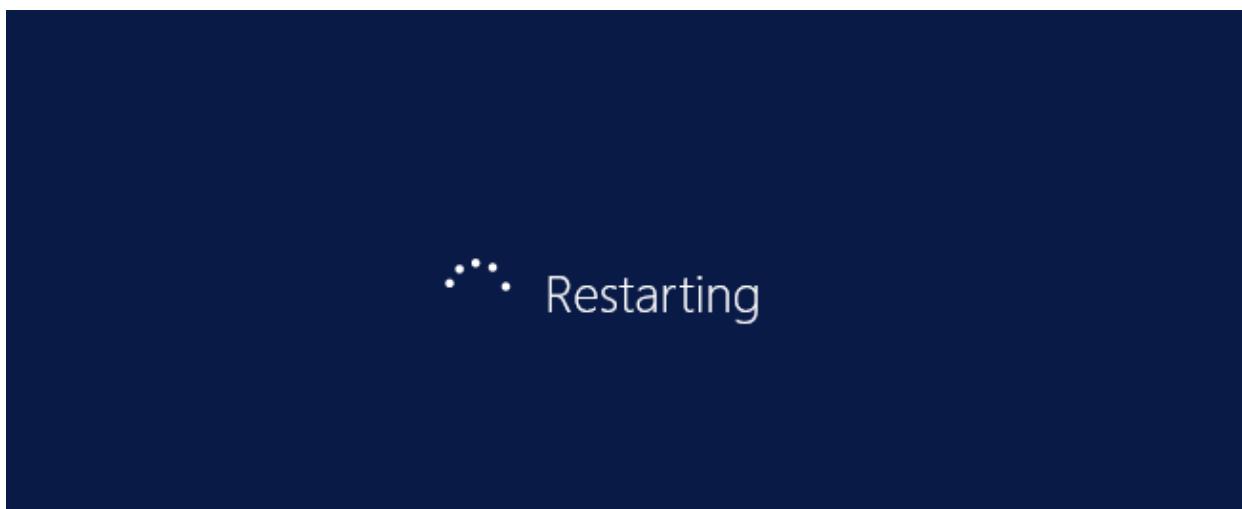


▪ Đặt tên cho CA là **BKAP-CA**:

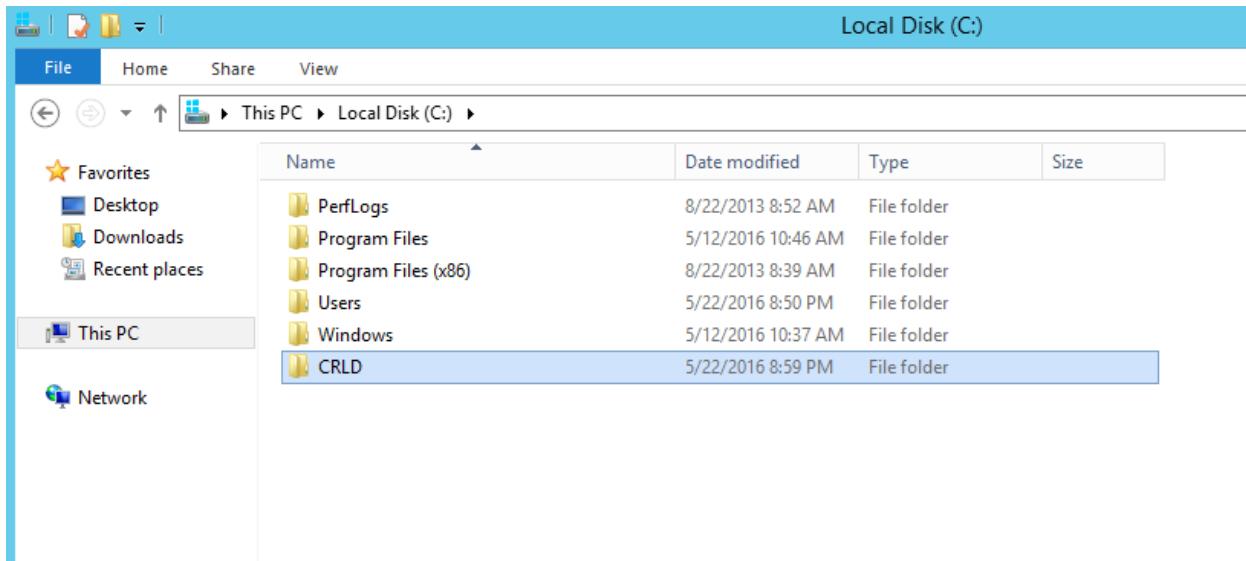
- Chọn vào **Configure** để tiến hành cấu hình:

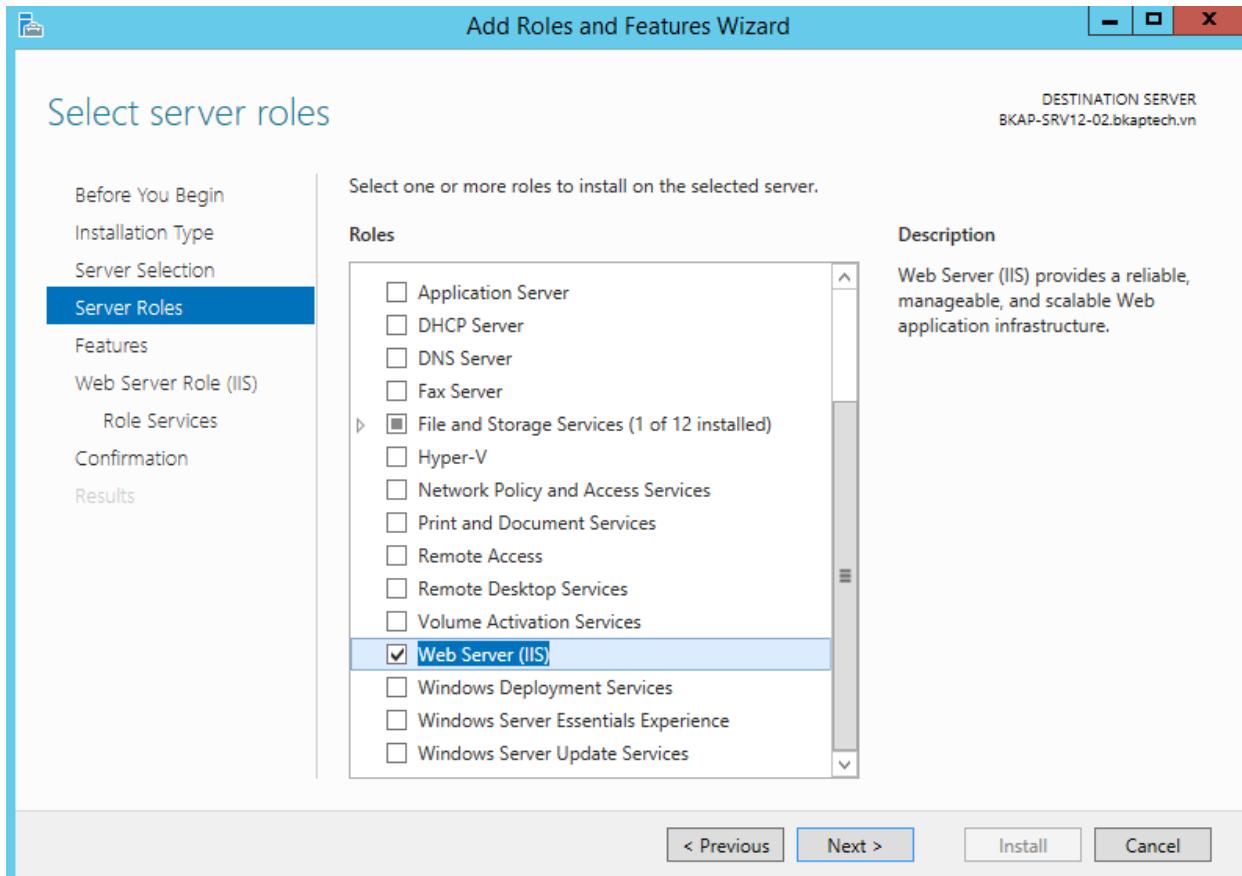


Sau khi cấu hình **CA Server**, thực hiện restart các máy trong hệ thống mạng để các máy này tự động **trust** CA Server trên máy **DC12-01**.

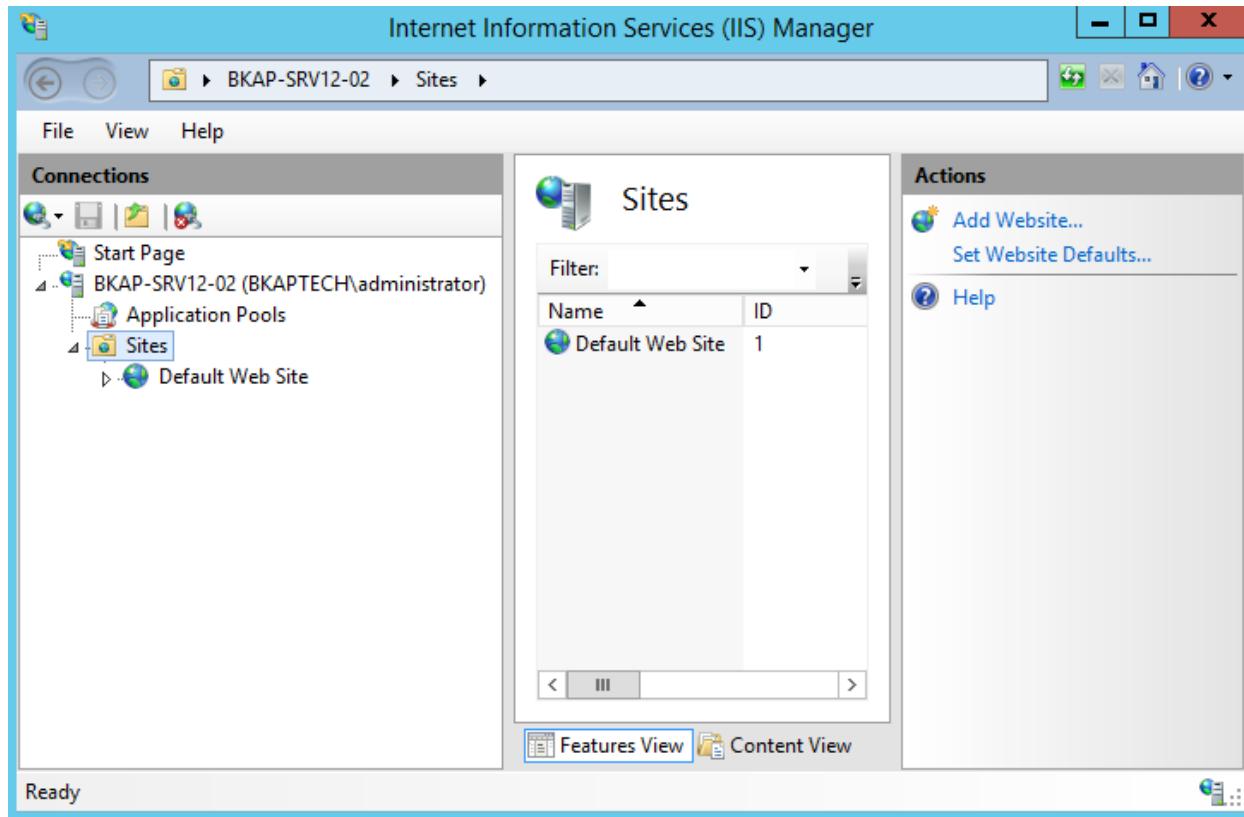


- Cài đặt Web Server (IIS) và chuẩn bị CRL Distribution Point trên Direct Access Server (SRV12-02).
 - Do các Direct Access Client cần truy cập vào **Certificate Revocation List (CRL)** để kiểm tra tính xác thực của **Certificate**, nên ta cần Publish CRL sang Direct Access Server.
 - Trên máy SRV12-02, tạo sẵn 1 thư mục tên tùy ý (ví dụ **C:\CRLD**), thư mục này sẽ chứa **Certificate Revocation List (CRL)** được publish từ CA Server.

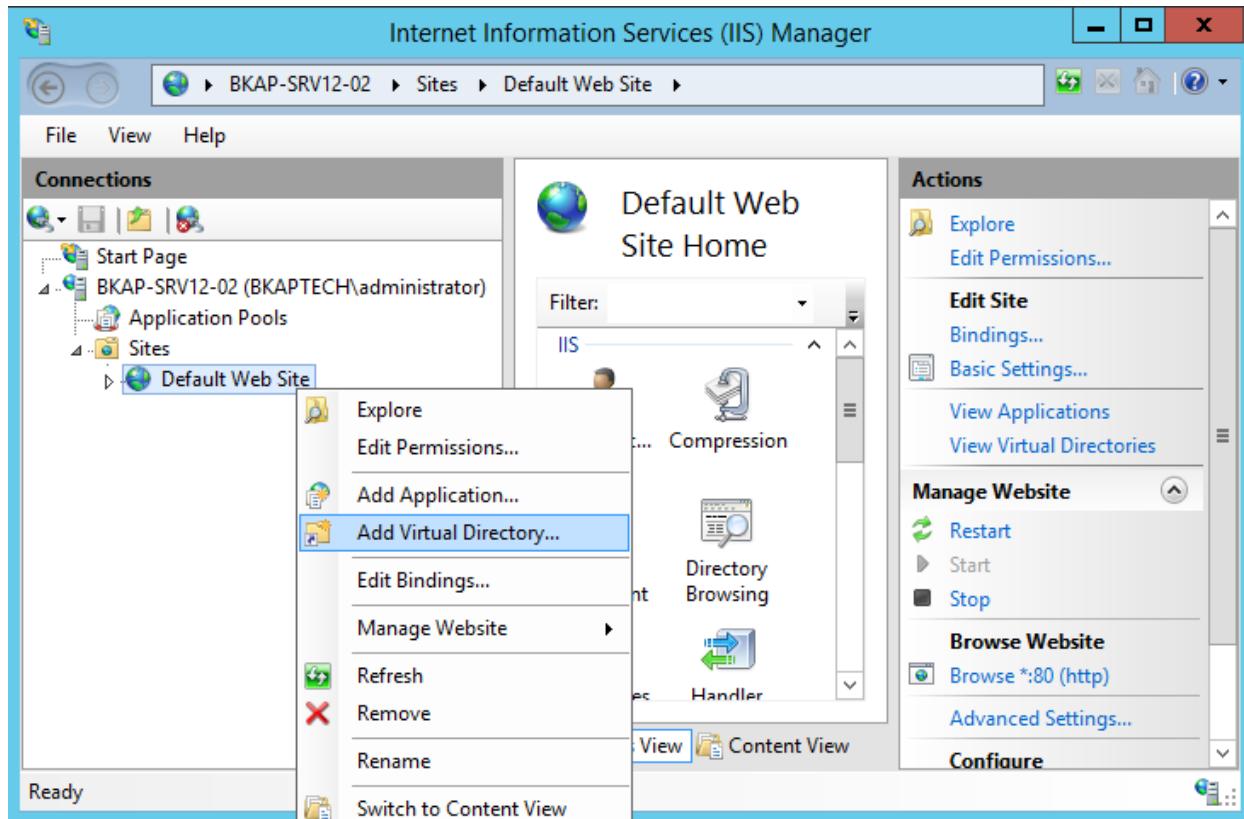


o Cài đặt Web Server (IIS) trên *SRV12-02 (Direct Access Server)*:

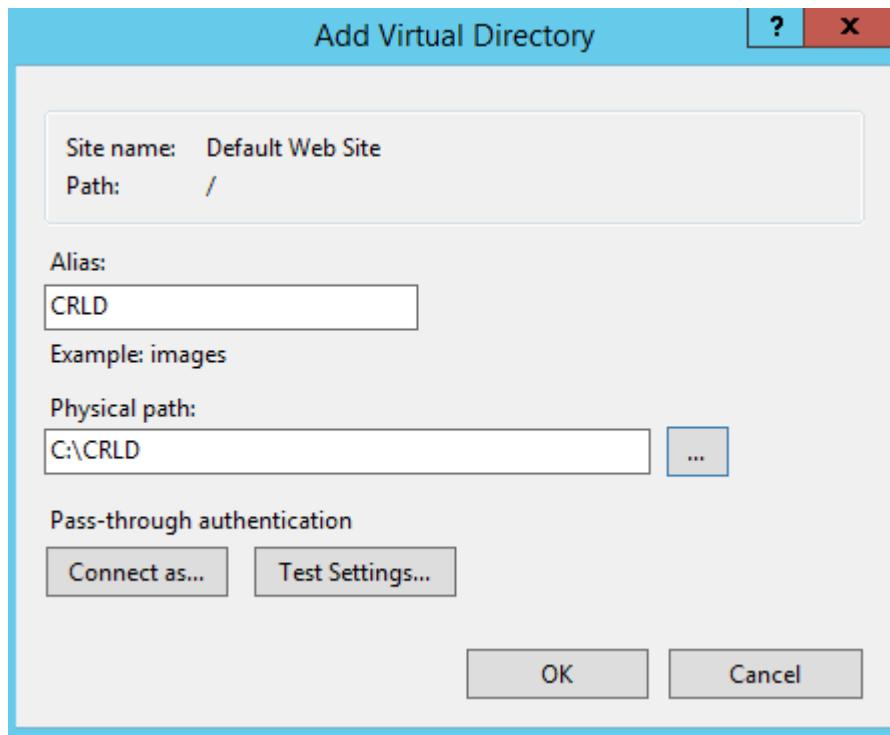
- Mở dịch vụ IIS cấu hình nơi chứa CRL :



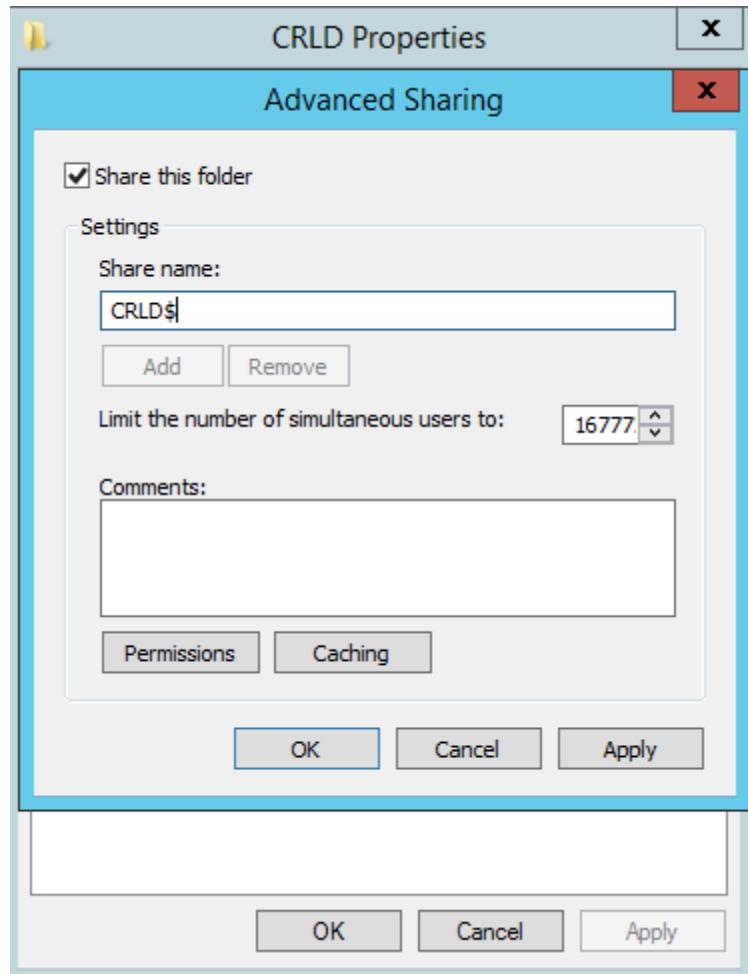
- Tạo một **Virtual Directory** bên dưới trang Web mặc định (*Default Web Site*): click chuột phải tại **Default Web Site**, chọn **Add Virtual Directory...**



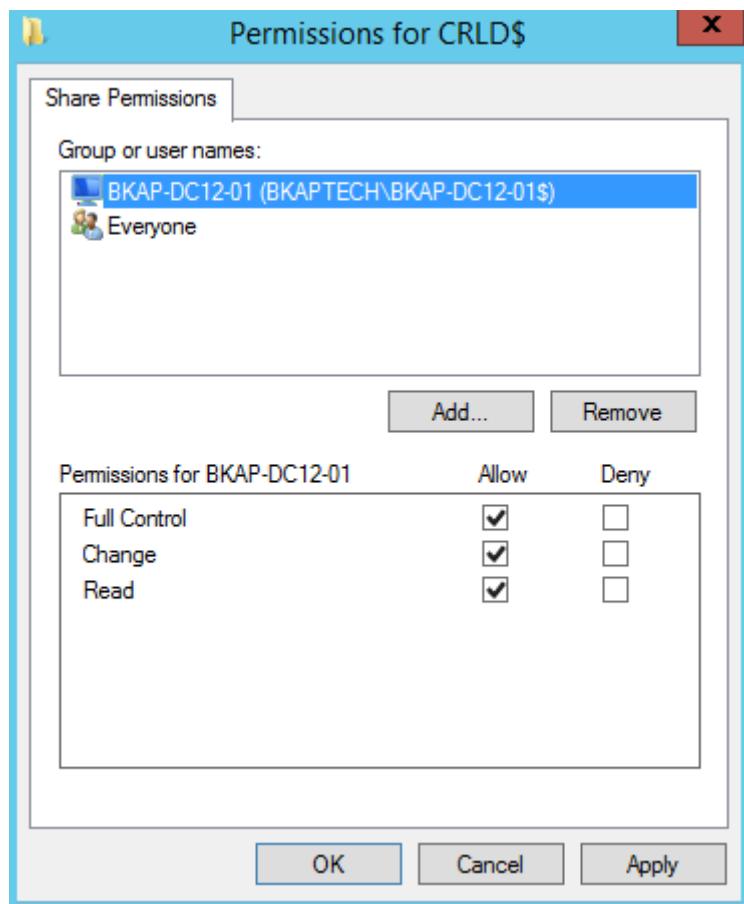
- Trong cửa sổ **Add Virtual Directory**, đặt tên là **CRLD** và chỉ định thư mục **C:\CRLD** đã tạo trước đó.



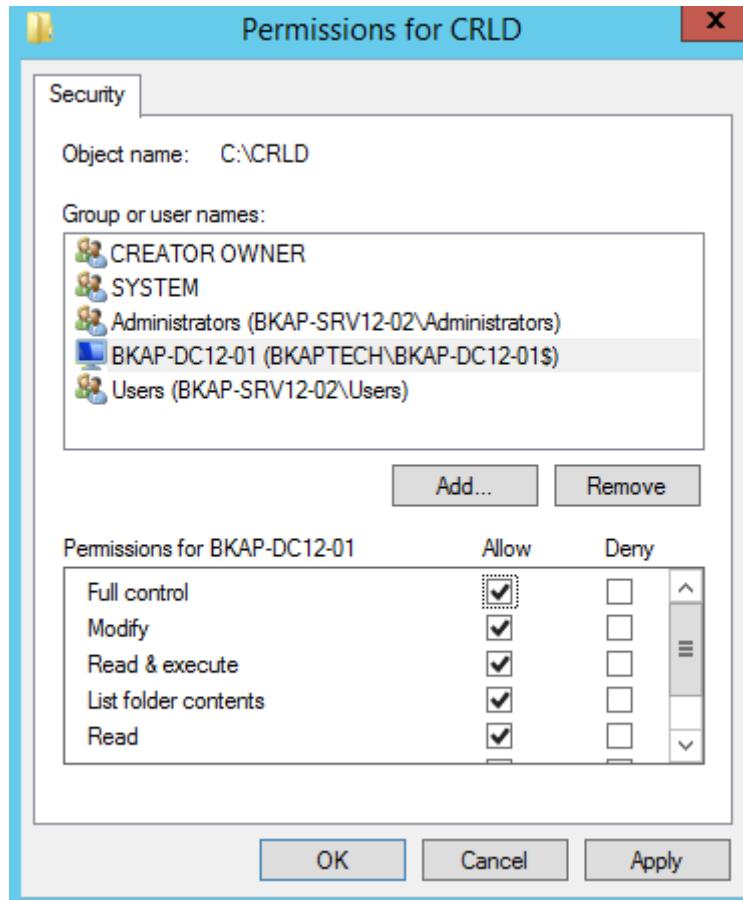
- Thực hiện share ẩn thư mục **CRLD** để CA Server có thể *Publish CRLs* vào thư mục này.



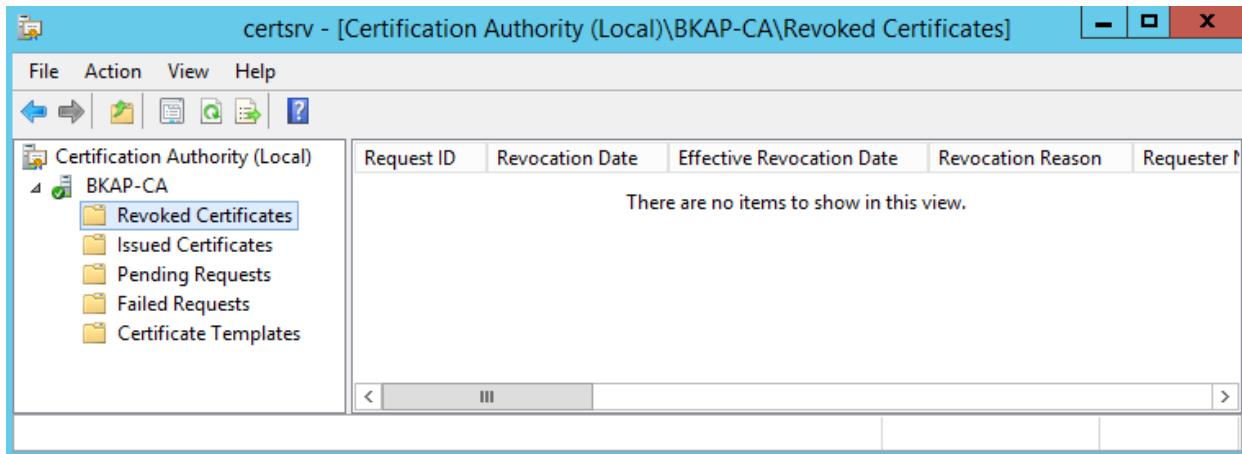
- Click vào *Permissions* để phân quyền , đưa máy *DC12-01* vào danh sách phân quyền, và phân quyền *Full Control* cho *Everyone* và *DC12-01*.



- Sang tab **Security**, phân quyền NTFS bằng cách click vào nút **Edit**, nhấn nút **Add** để phân quyền, chọn máy **DC12-01 (CA Server)** và phân quyền **Full Control**.

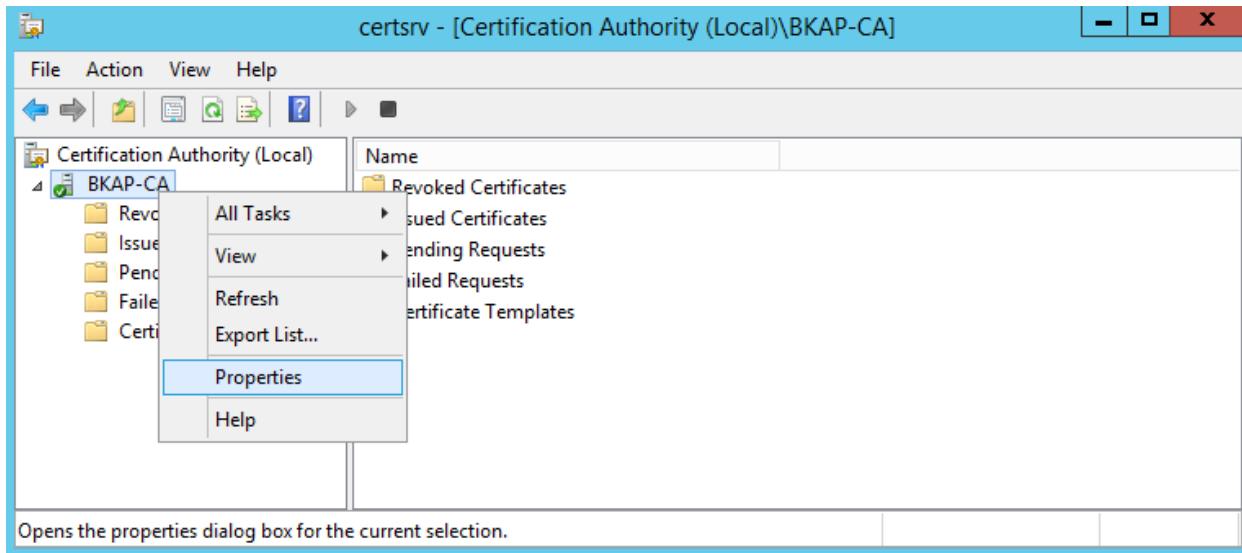


- Thực hiện **Publish CRL**, trên **DC12-01**, mở **Certificate Authority**.

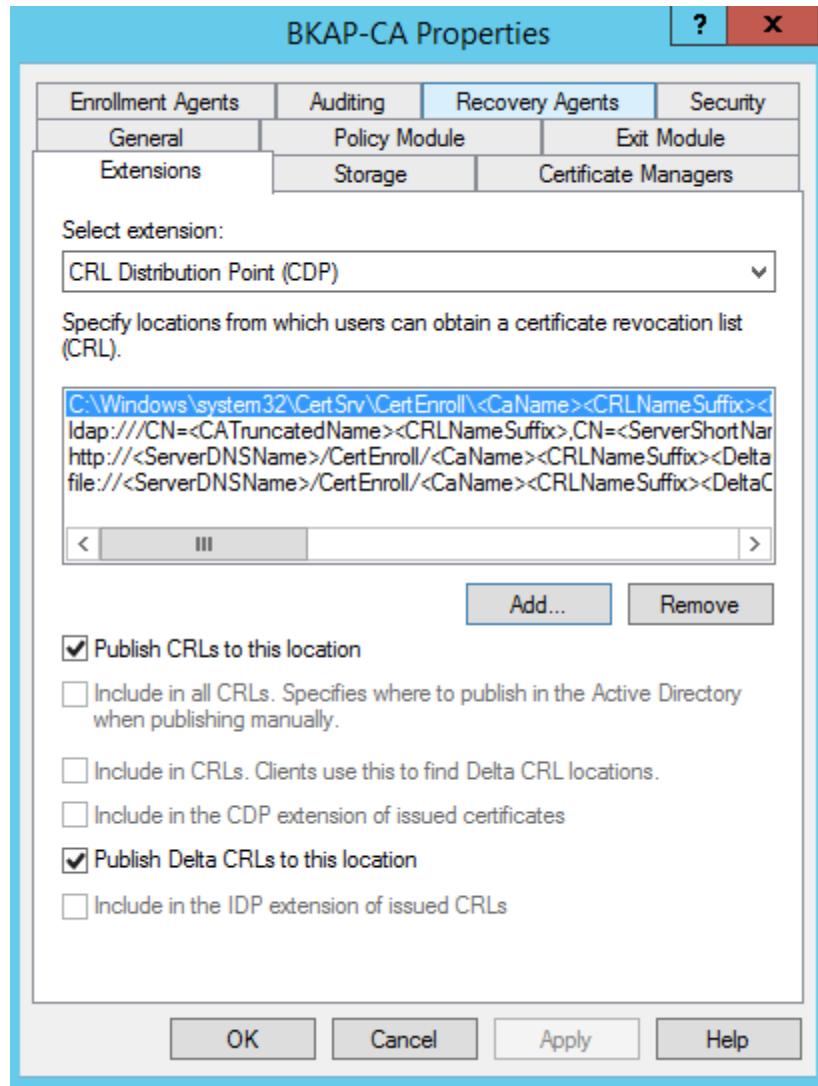


⇒ Ta cần *Publish CRL* và *Delta CRL* sang *Direct Access Server (SRV12-02)*.

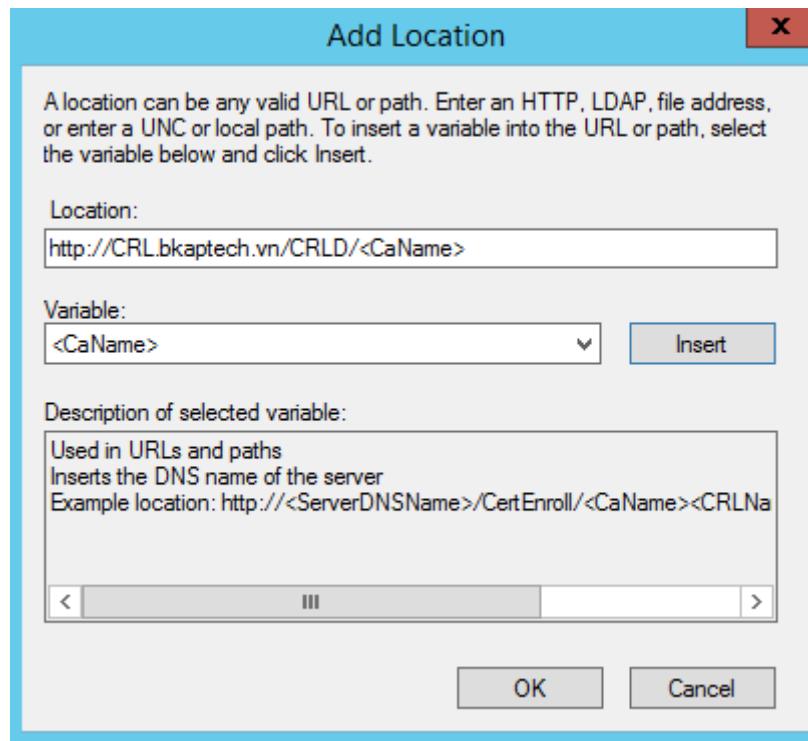
- Chọn **BKAP-CA / Properties**.



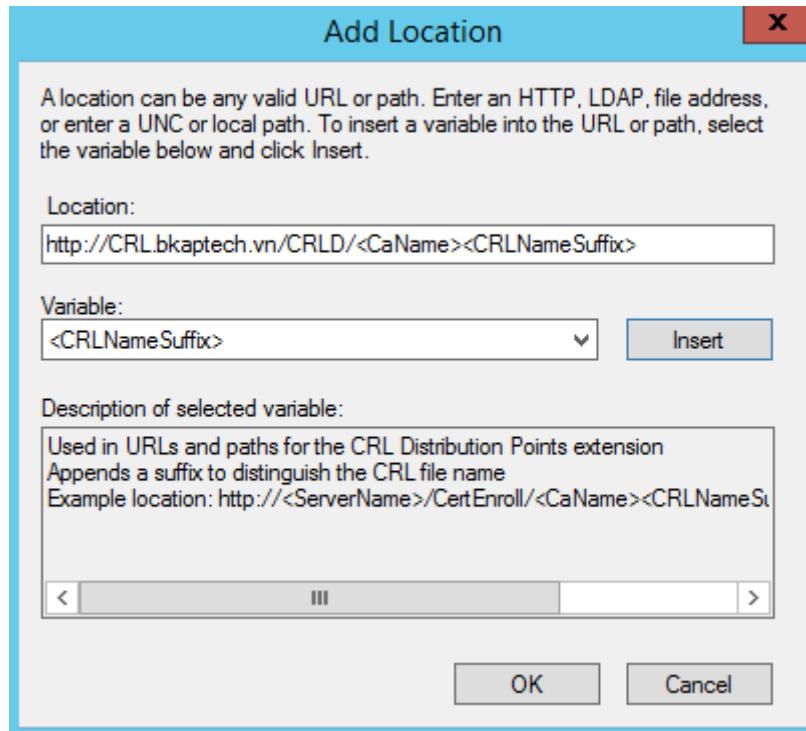
- Tại cửa sổ **BKAP-CA Properties**, chuyển sang tab **Extensions**, click vào **Add...** để thêm *CRL Distribution Point (CDP)*.



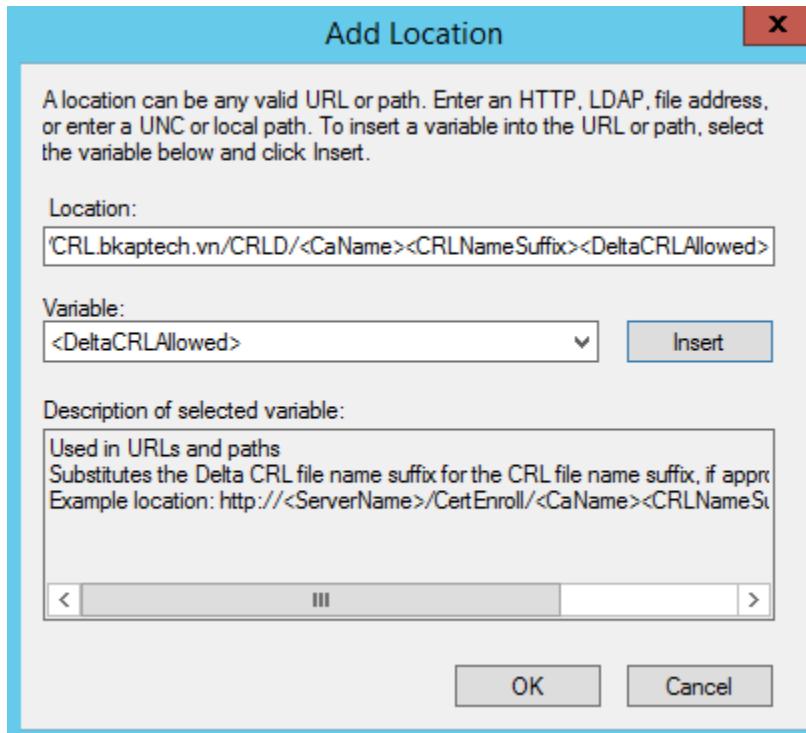
- Trong cửa sổ **Add Location**, tại mục **Location**, nhập vào <http://CRL.bkaptech.vn/CRLD/>, tiếp theo trong mục **Variable**, chọn **<CaName>**, click vào **Insert**.



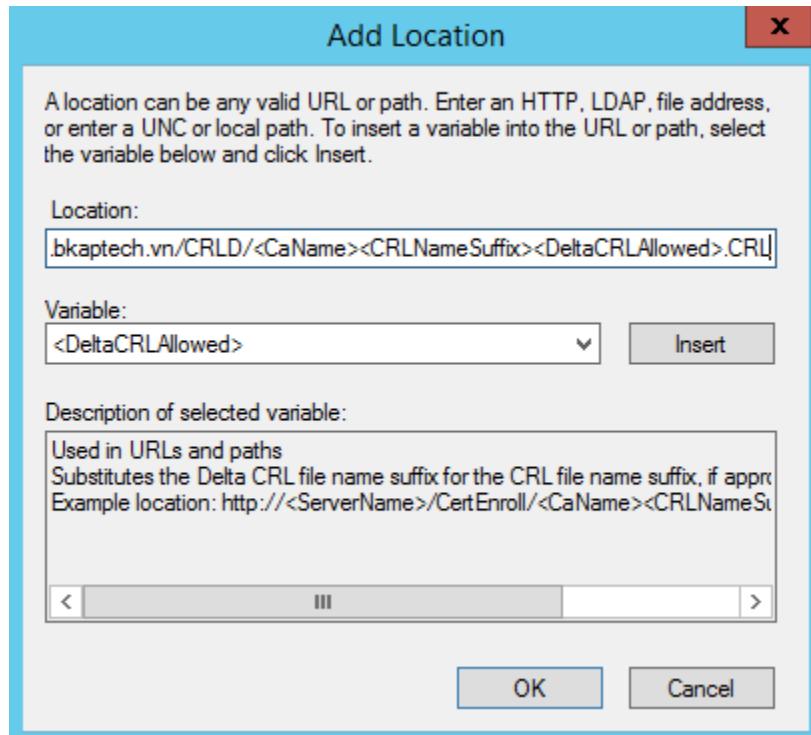
- Tiếp theo trong khung **Variable**, chọn <CRLNameSuffix> và nhấn **Insert**.



- Tiếp theo trong khung **Variable**, chọn <DeltaCRLAllowed> và nhấn **Insert**.



- Trong khung **Location**, đưa con trỏ ra cuối dòng và gõ thêm **.CRL**

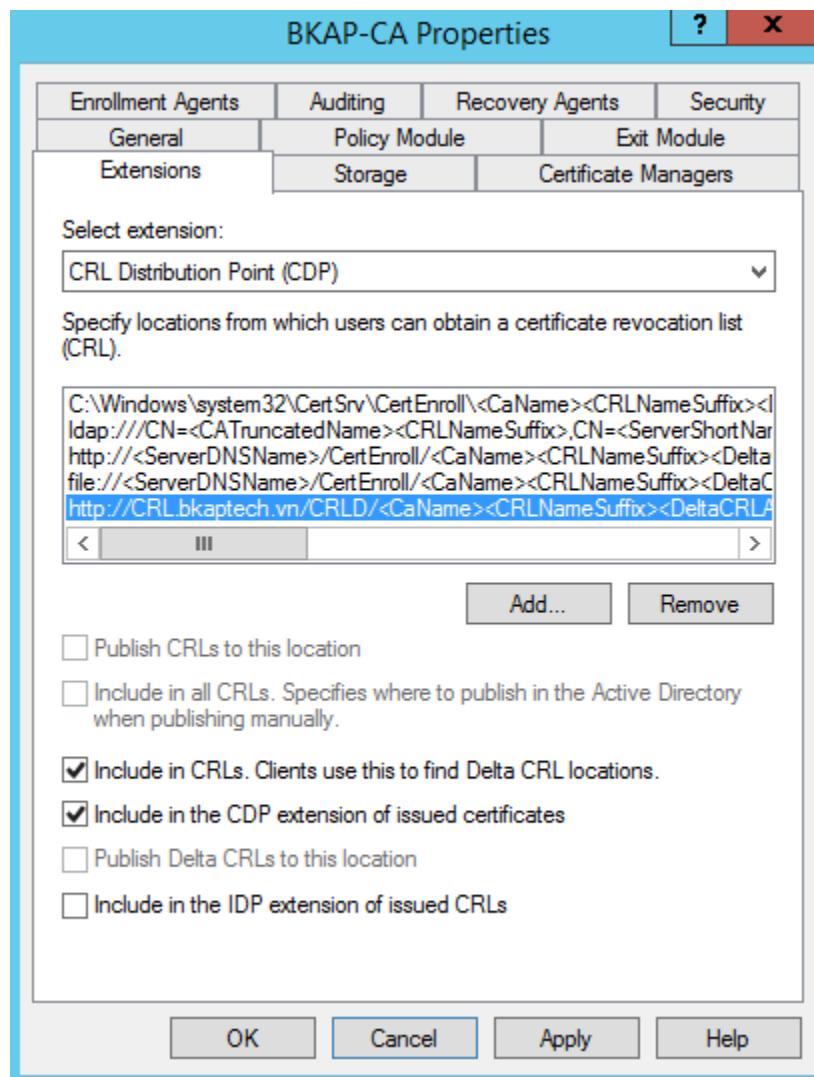


⇒ Kiểm tra lại trong khung **Location** phải là:

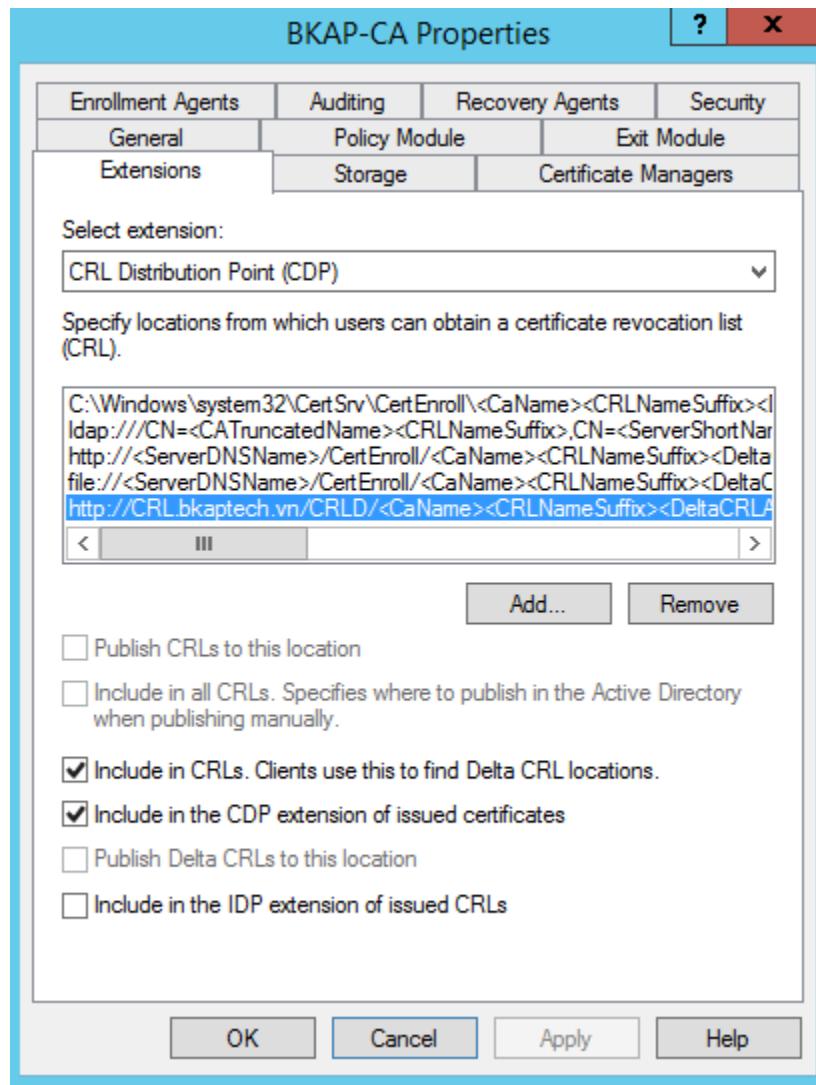
<http://CRL.bkaptech.vn/CRLD/<CaName><CRLNameSuffix><DeltaCRLAllowed>.CRL>

- Click vào OK để xác nhận.

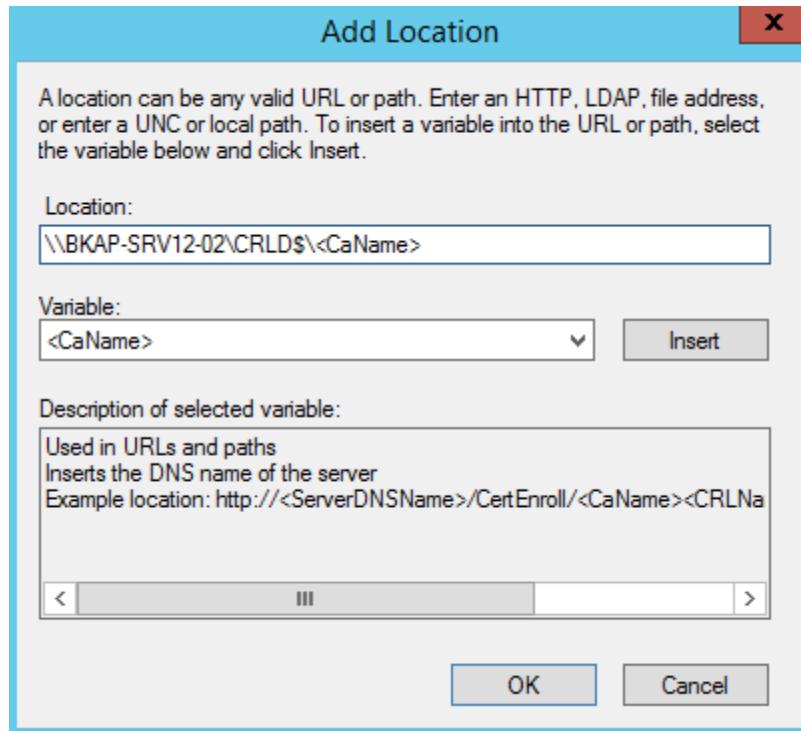
- Đánh 2 dấu check ***Include in CRLs. Client use this to find Delta CRL locations*** và ***Include in the CDP extension of issued certificates***. Nhấn nút **Apply**.



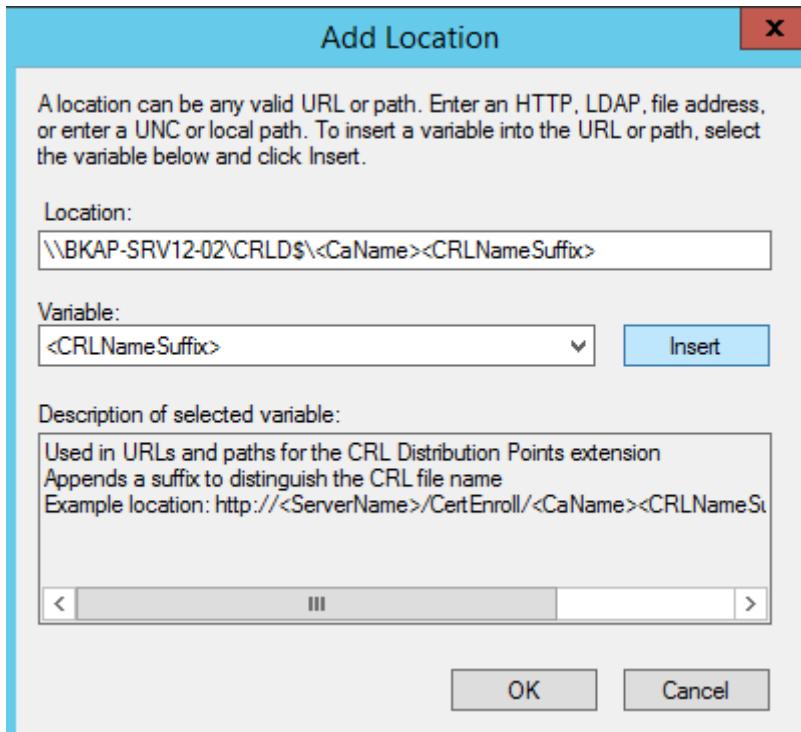
- Hệ thống yêu cầu *restart* dịch vụ, chọn *No* để tiếp tục thêm CDP.
- Click vào **Add...**



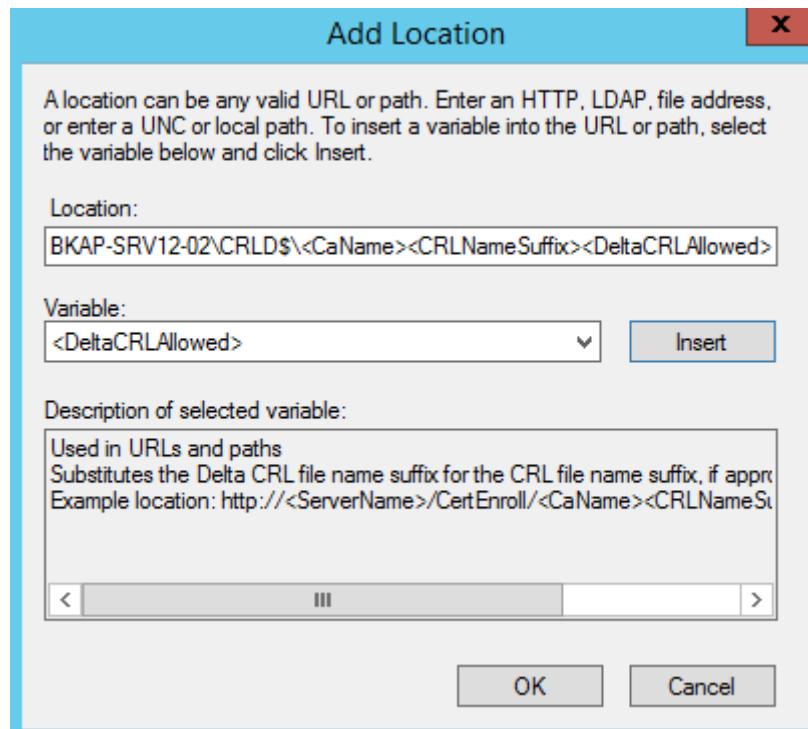
- Trong khung **Location**, nhập `\BKAP-SRV12-02\CRLD$`, sau đó trong khung **Variable** chọn `<CaName>` và nhấn **Insert**.



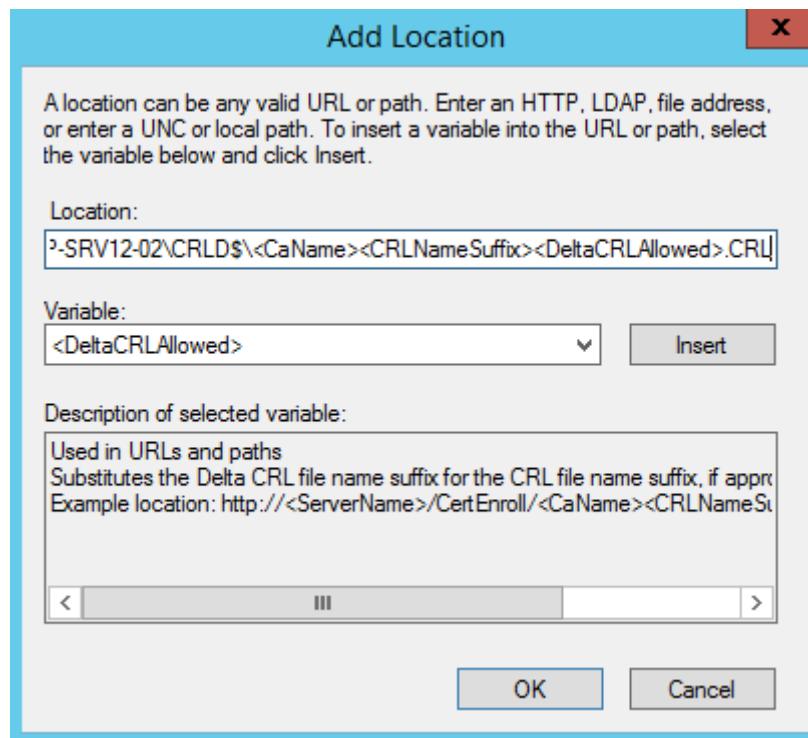
- Trong khung **Variable** chọn `<CRLNameSuffix>` và nhấn **Insert**.



- Trong khung **Variable** chọn **<DeltaCRLAllowed>** và nhấn **Insert**.



- Trong khung **Location**, đưa con trỏ ra cuối dòng và gõ thêm **.CRL**

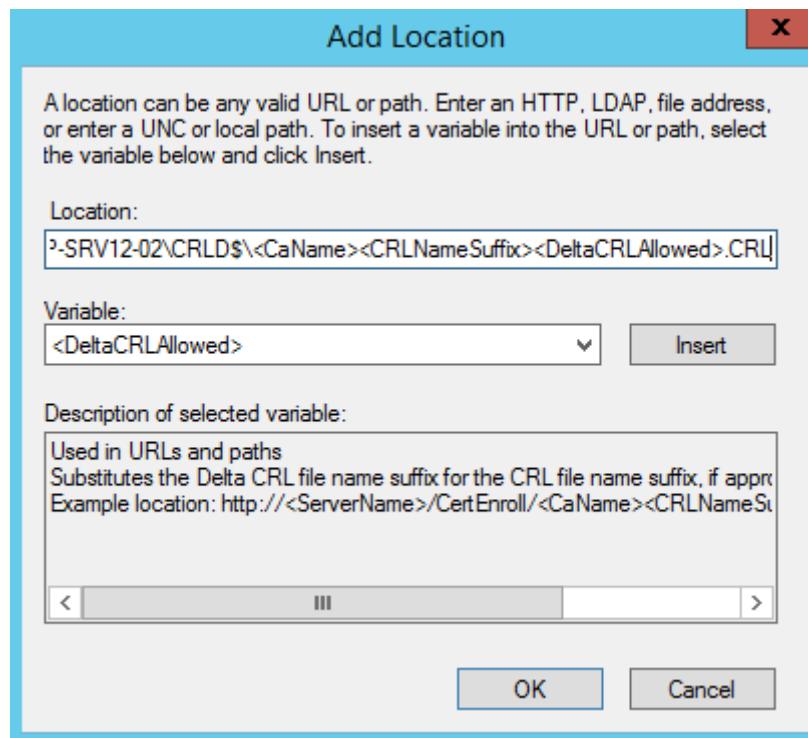


- Kiểm tra lại trong khung **Location** phải là:

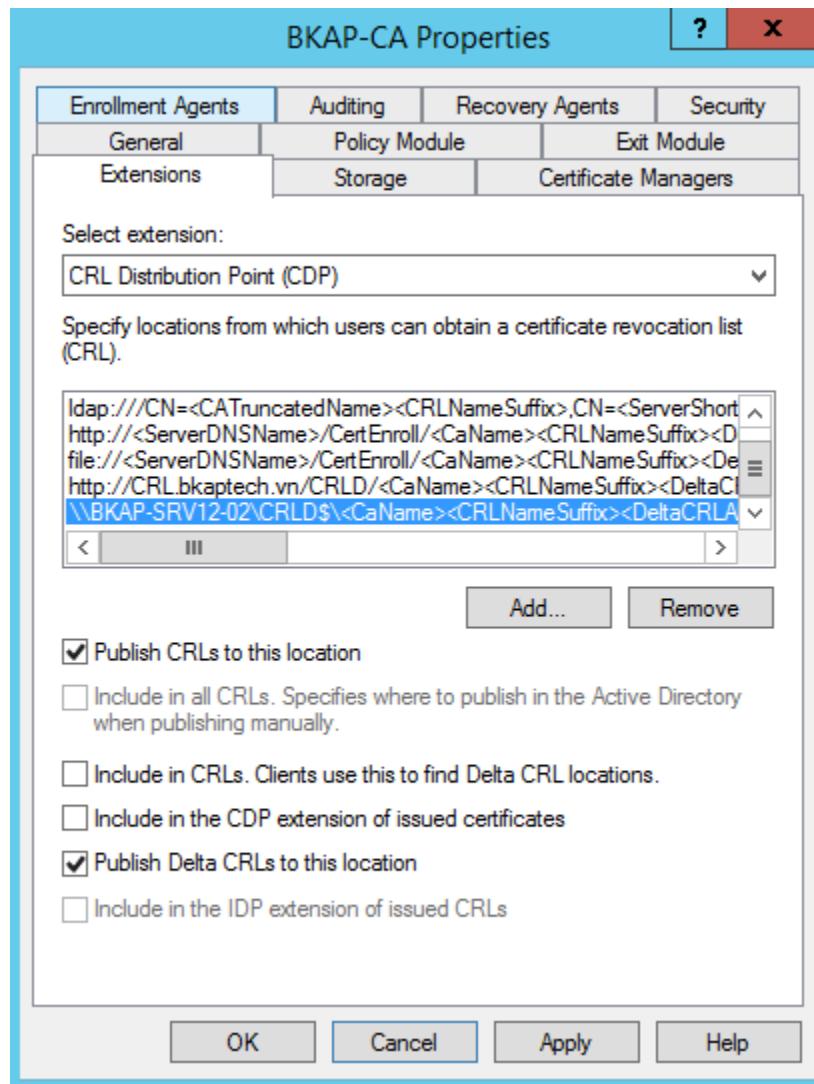
\BKAP-SRV12-

02\CRLD\$<CaName><CRLONameSuffix><DeltaCRLAllowed>.CRL

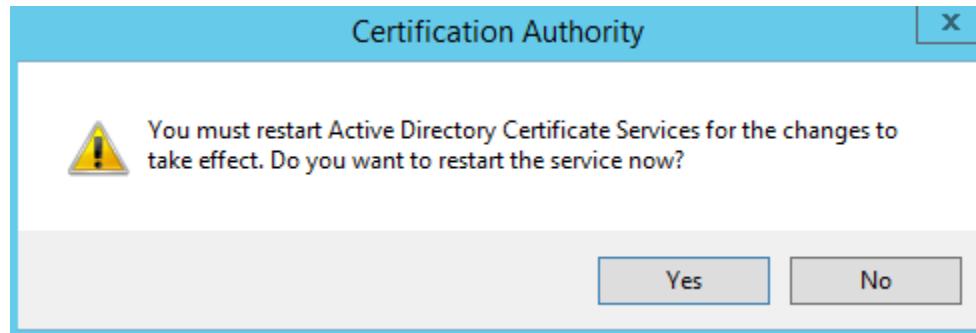
- Click vào OK để xác nhận.

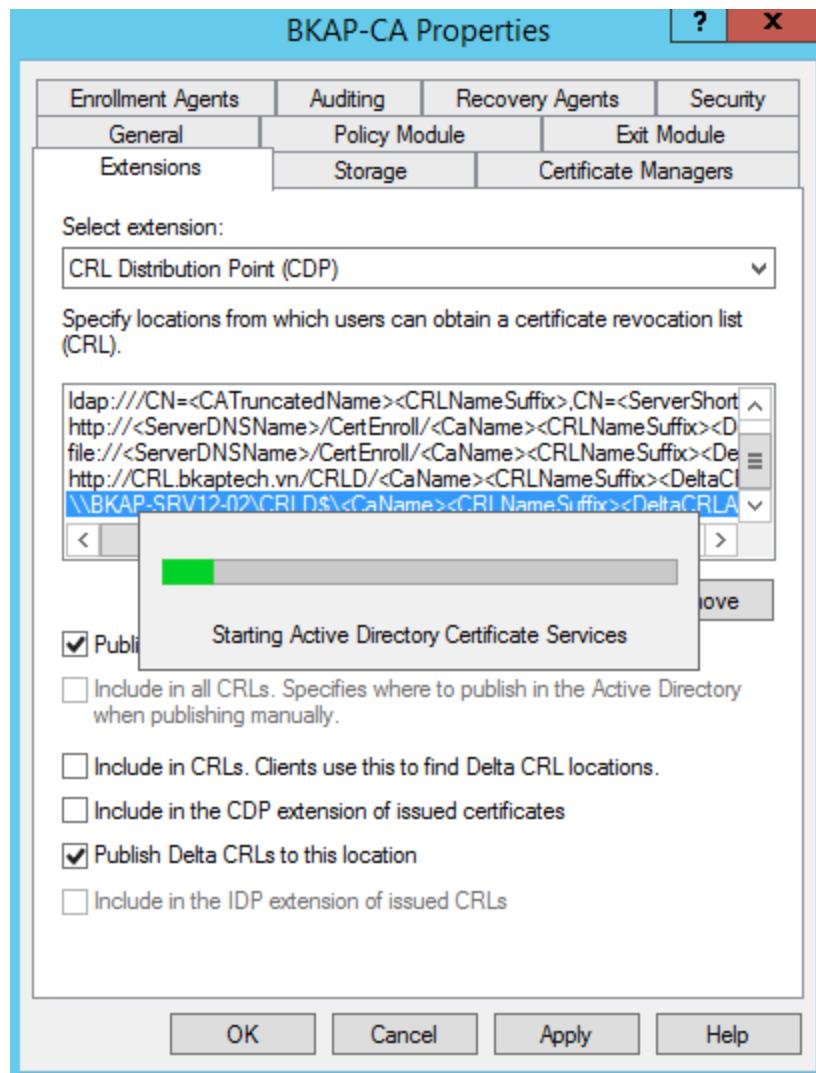


- Đánh 2 dấu check **Publish CRLs to this location** và **Publish Delta CRLs to this location**. Nhấn OK.



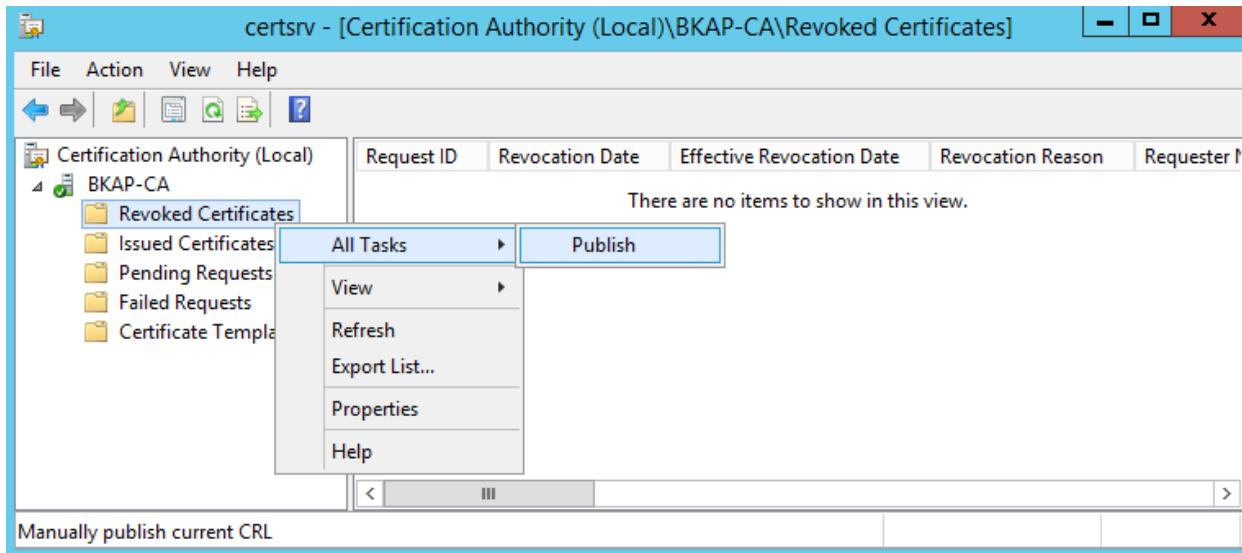
- Click **Apply / Yes** để *restart* dịch vụ.



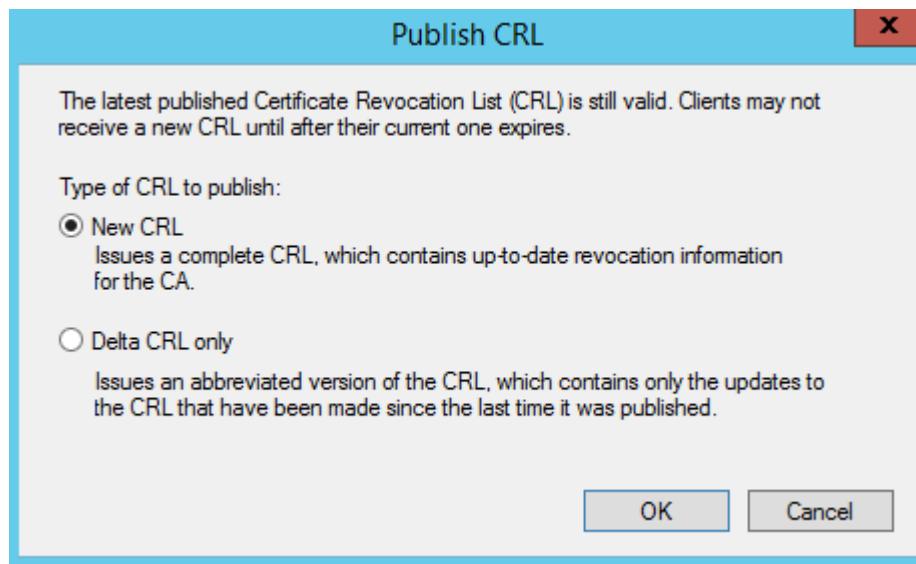


- *Publish CRL:*

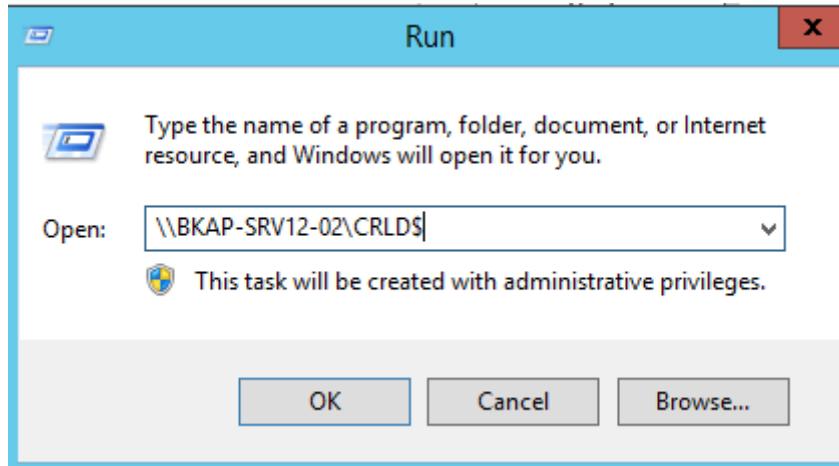
- Tại cửa sổ Certsrv... , click chuột phải tại **Revoked Certificates / All Tasks / Publish.**



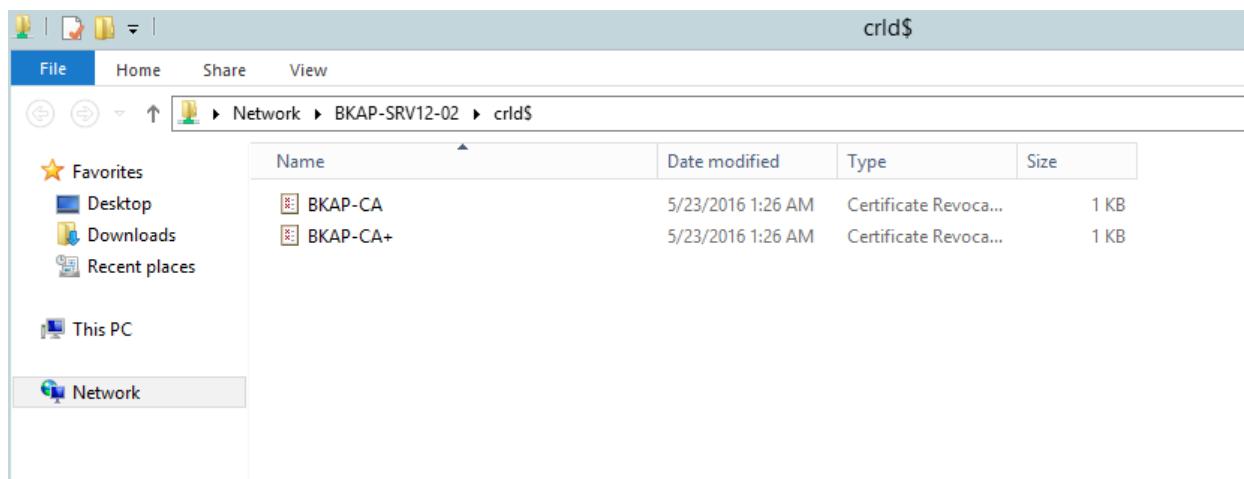
- Trong cửa sổ **Publish CRL** , chọn vào **New CRL / OK.**



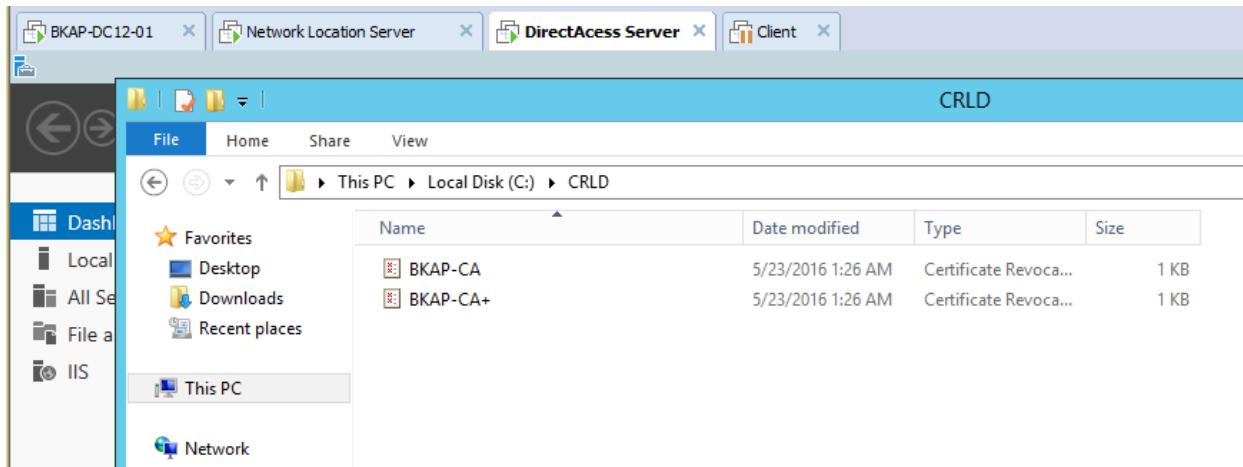
- ⇒ Kiểm tra kết quả **Publish CRL** bằng cách truy cập sang thư mục **CRLD\$** trên máy **BKAP-SRV12-02**.



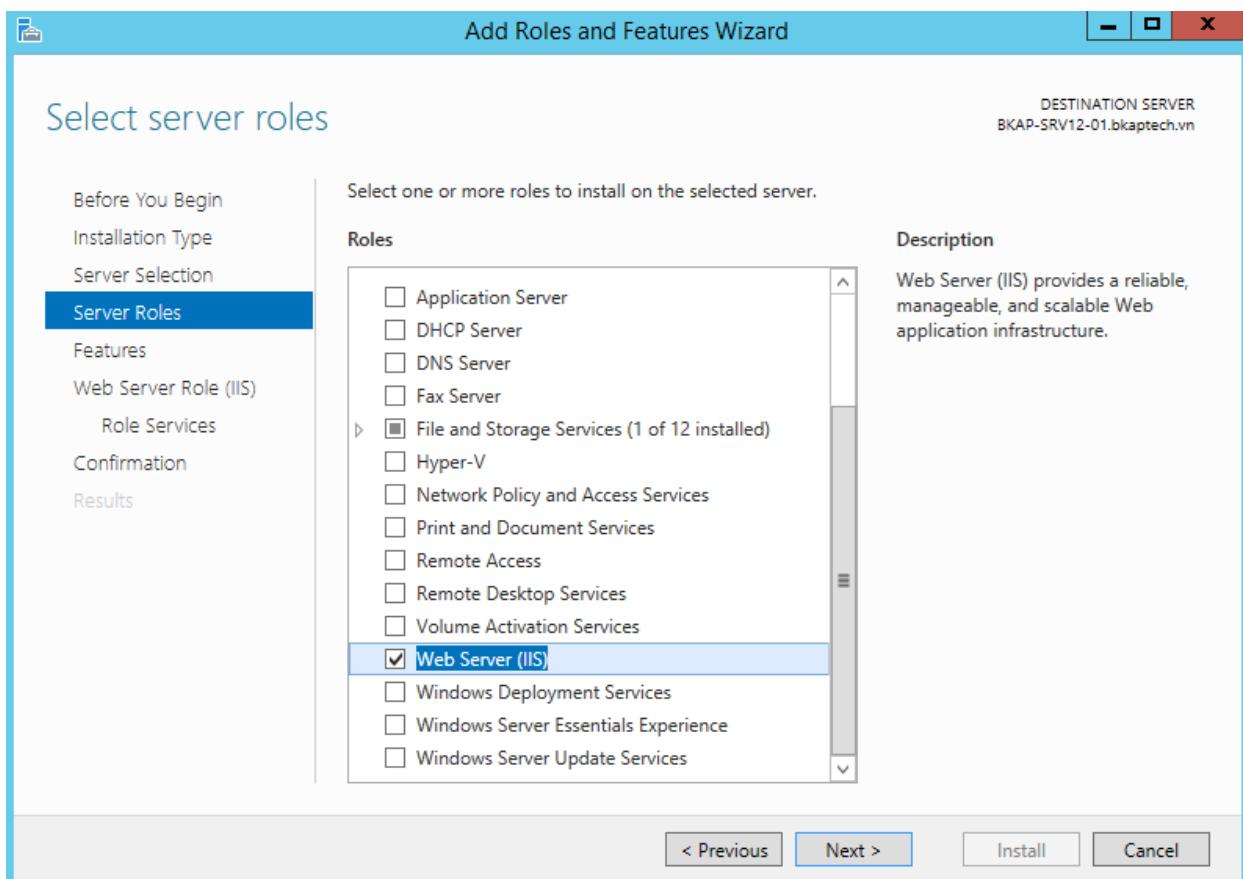
- Ta sẽ thấy 2 File như hình dưới, đó chính là **CRLs** và **Delta CRLs**.



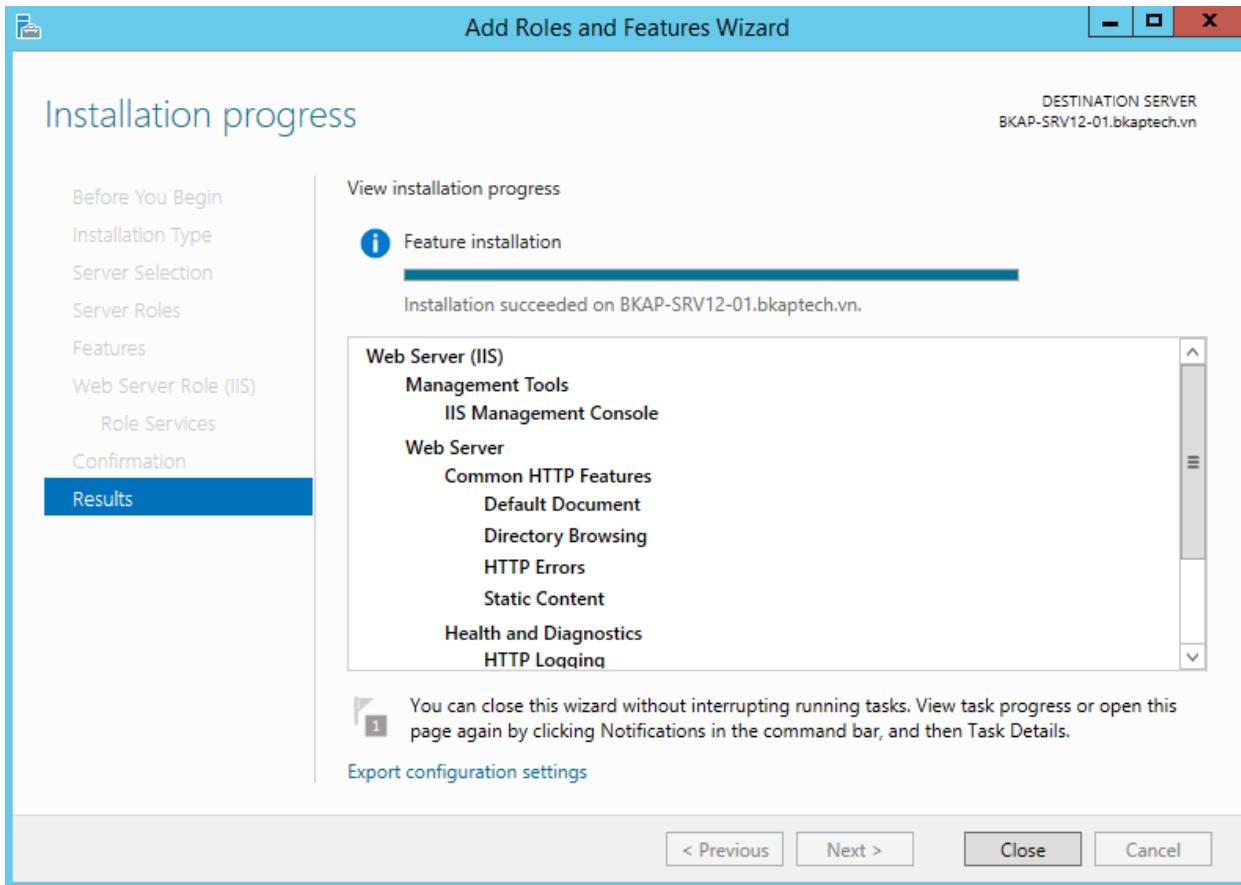
- Sang máy **DirectAccess Server**, ta sẽ thấy 2 file trong thư mục **C:\CRLD**.



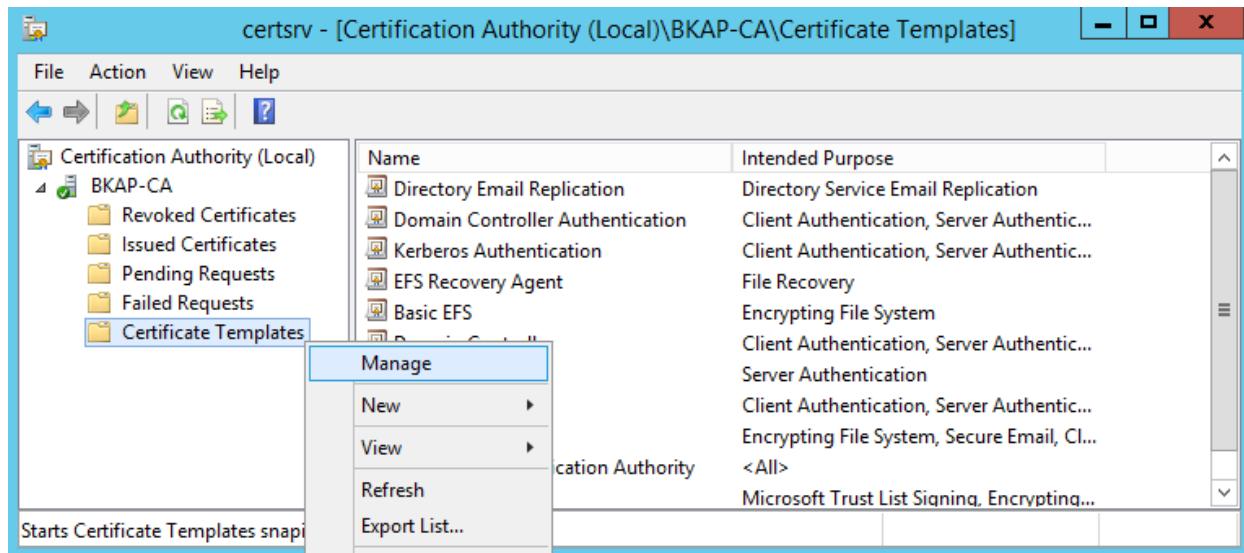
- Thực hiện cài đặt **Web Server (IIS)** trên **Network Location Server (BKAP-SRV12-01)**:



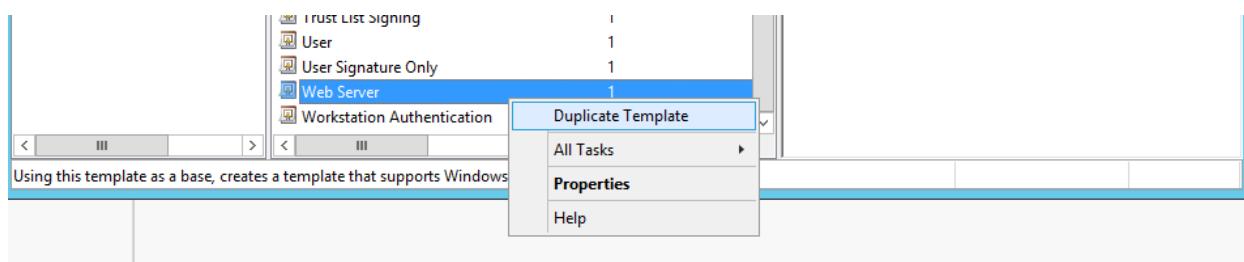
- Click vào **Close** để kết thúc quá trình cài đặt.



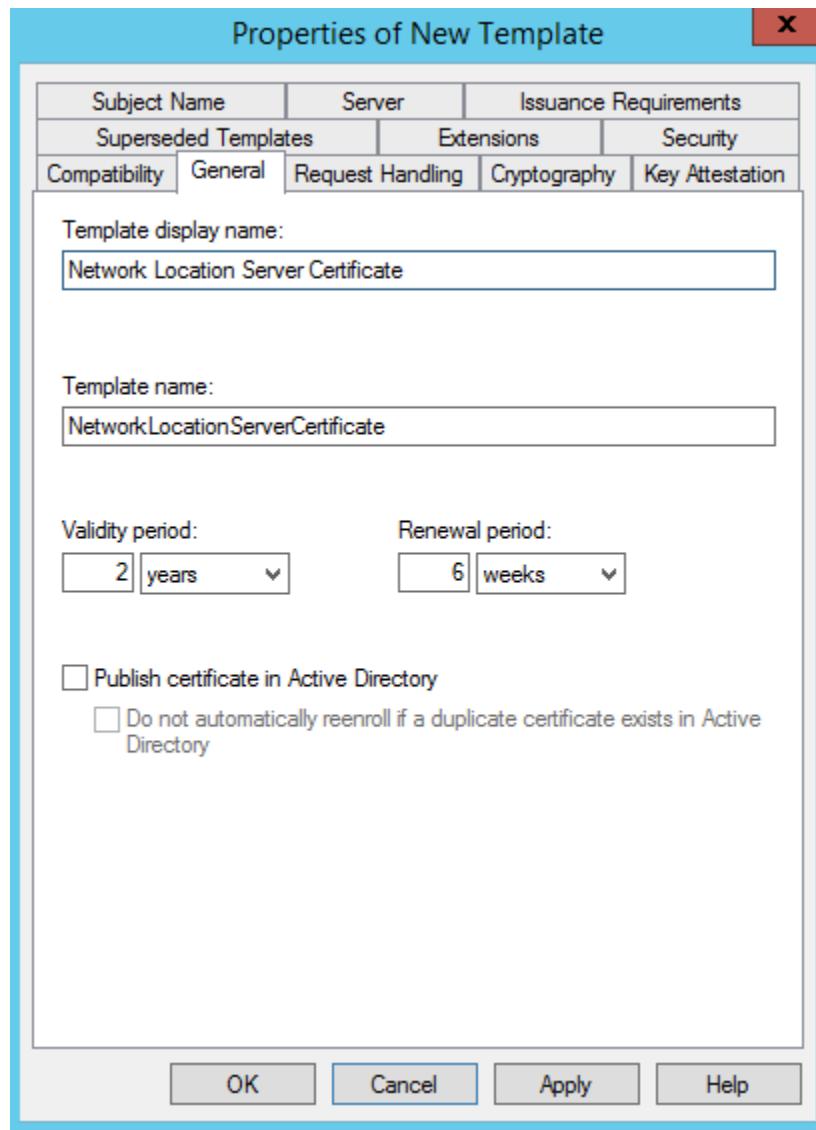
- Trên máy **DC12-01 (CA Server)**, Thực hiện tạo và phát hành **Certificate Template** cho **Network Location Server (SRV12-01) & Direct Access Server(SRV12-02)**.
 - Trong cửa sổ **certsrv**, click chuột phải tại **Certificate Templates**, chọn **Manage**.



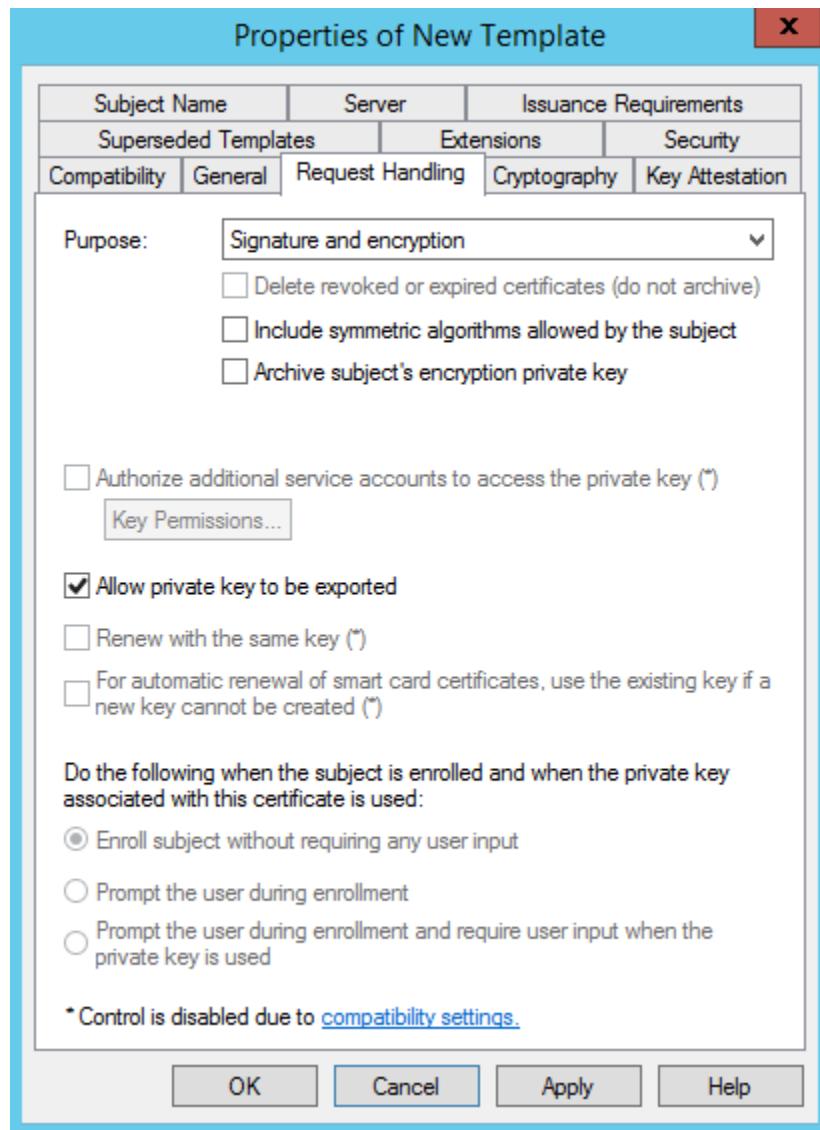
- Trong cửa sổ **Certificate Templates Console**, chọn **Web Server**, click chuột phải tại đây, chọn **Duplicate Template**.



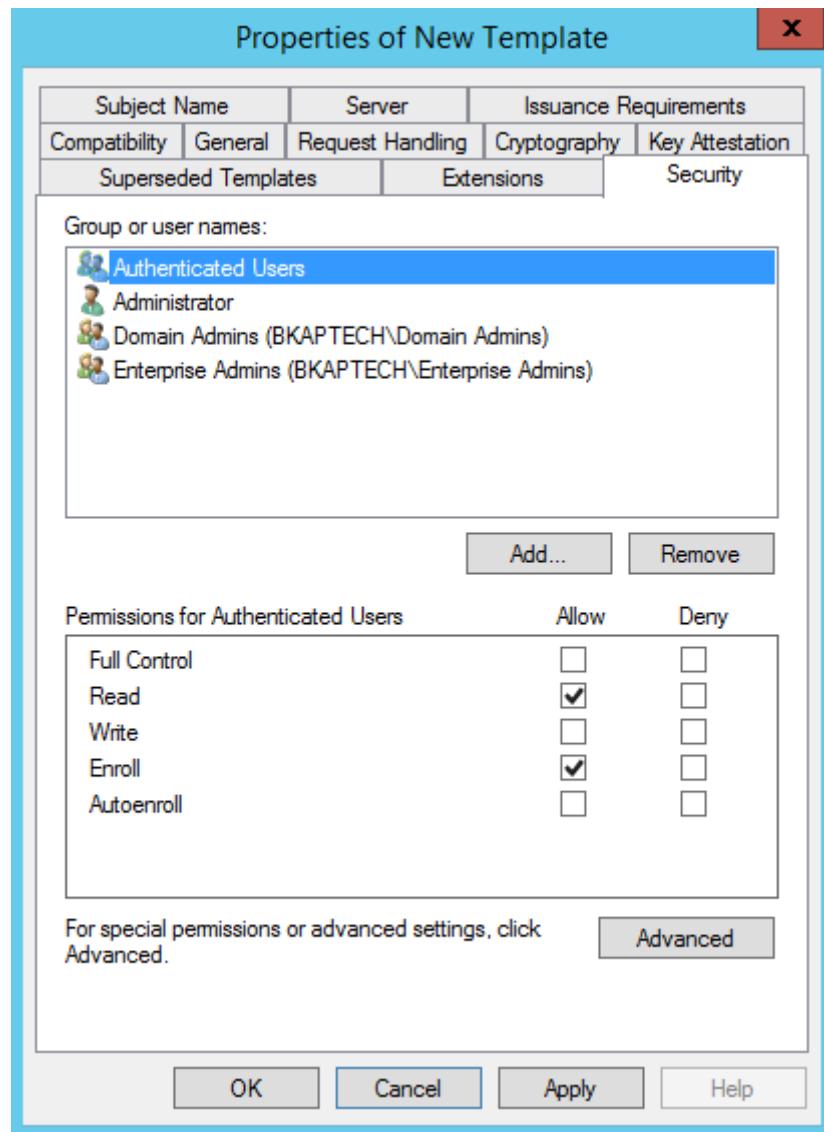
- Trong cửa sổ **Properties of New Template**, tab **General**, trong mục **Template display name**, đặt tên cho **Certificate Template** mới : *Network Location Server Certificate*



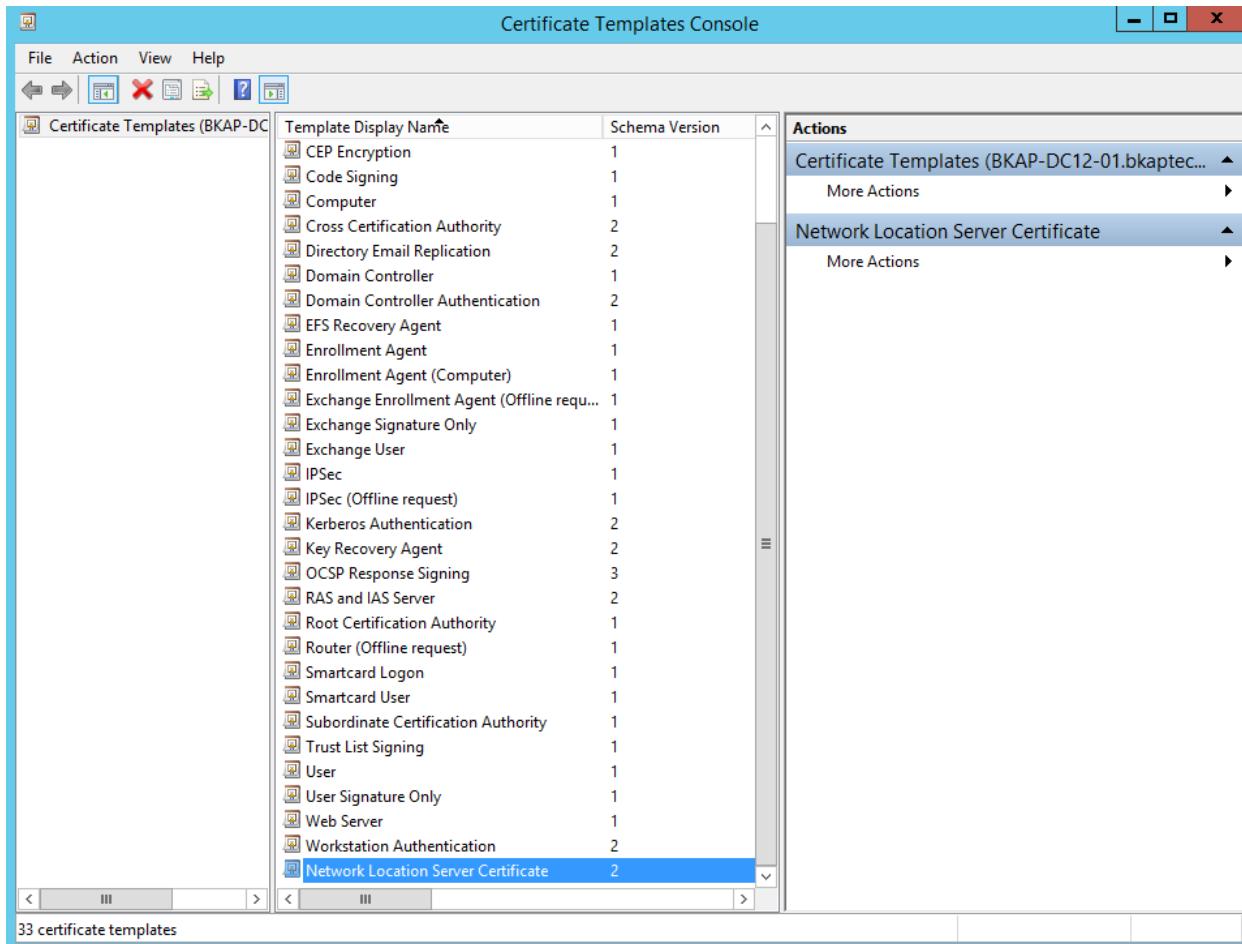
- Sang tab **Request Handling** đánh dấu tại *Allow private key to be exported* để có thể **Export Certificate** để phòng trường hợp bị mất **Certificate**.



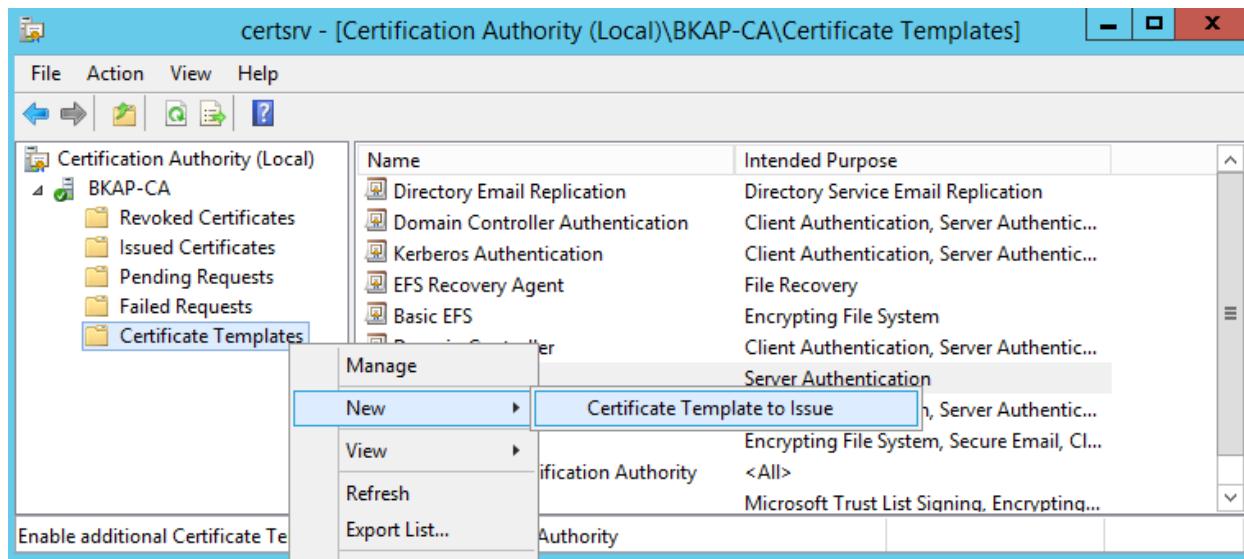
- Sang Tab **Security**, phân quyền **Enroll** cho group **Authenticated Users**. Nhấn nút OK để xác nhận tạo **Certificate Templates** mới.



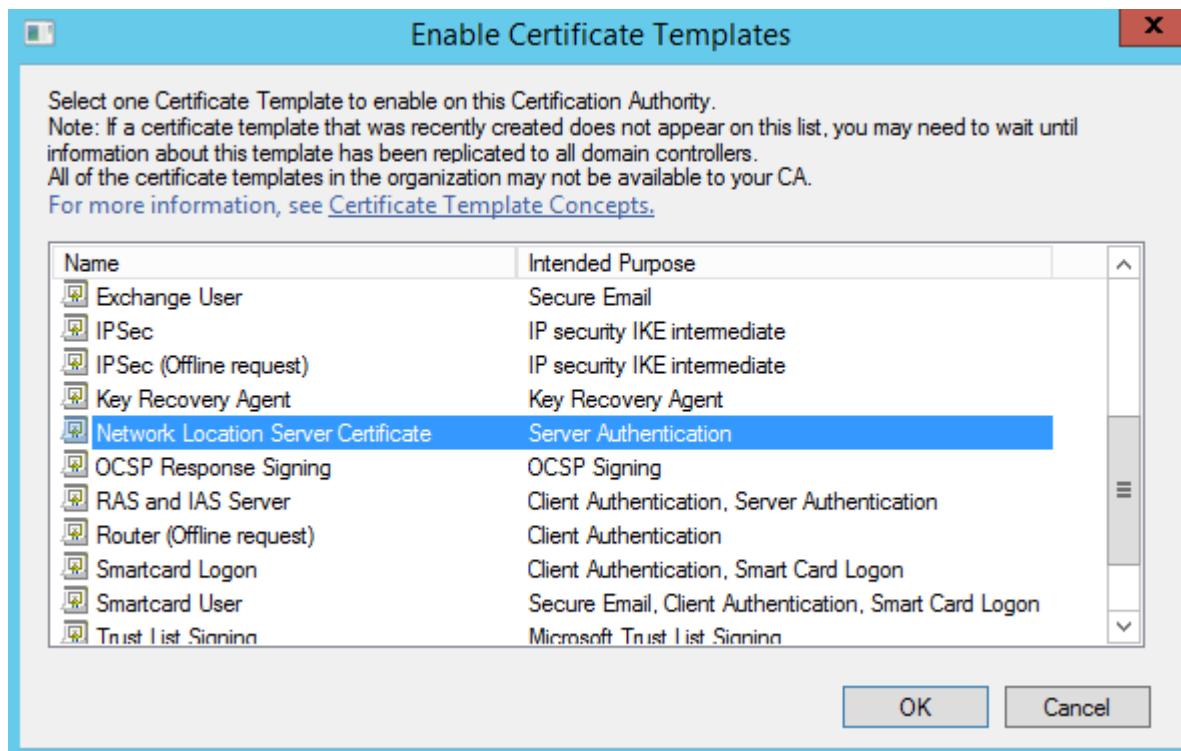
- Kiểm tra Certificate Templates mới đã được tạo.



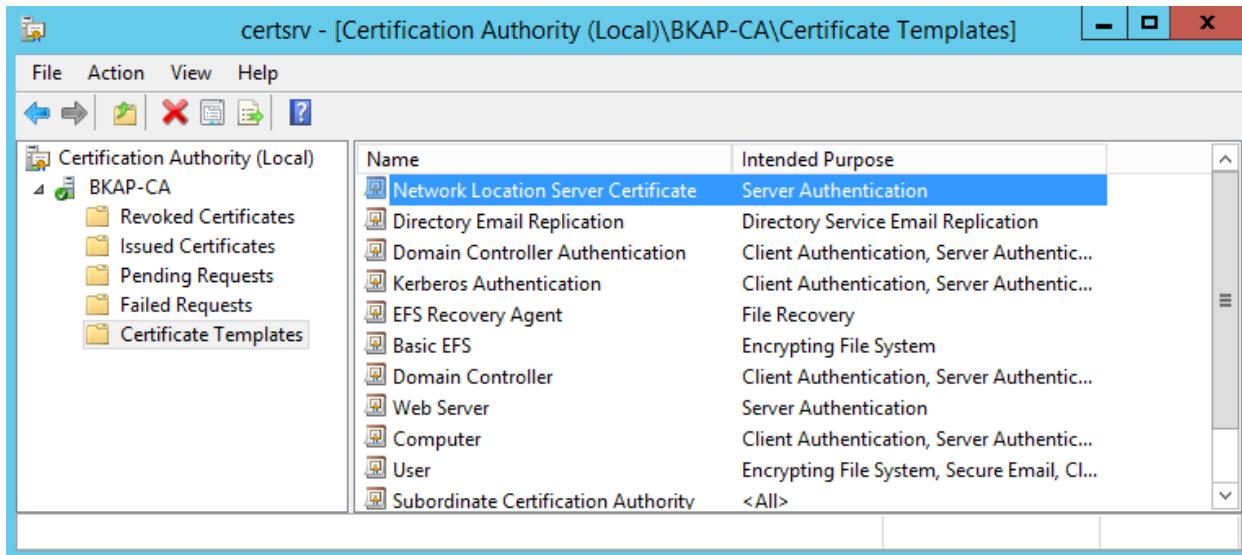
- Phát hành **Certificate Templates** vừa tạo: tại cửa sổ `certsrv...`, chọn vào **Certificate Templates / New / Certificate Template to Issue**.



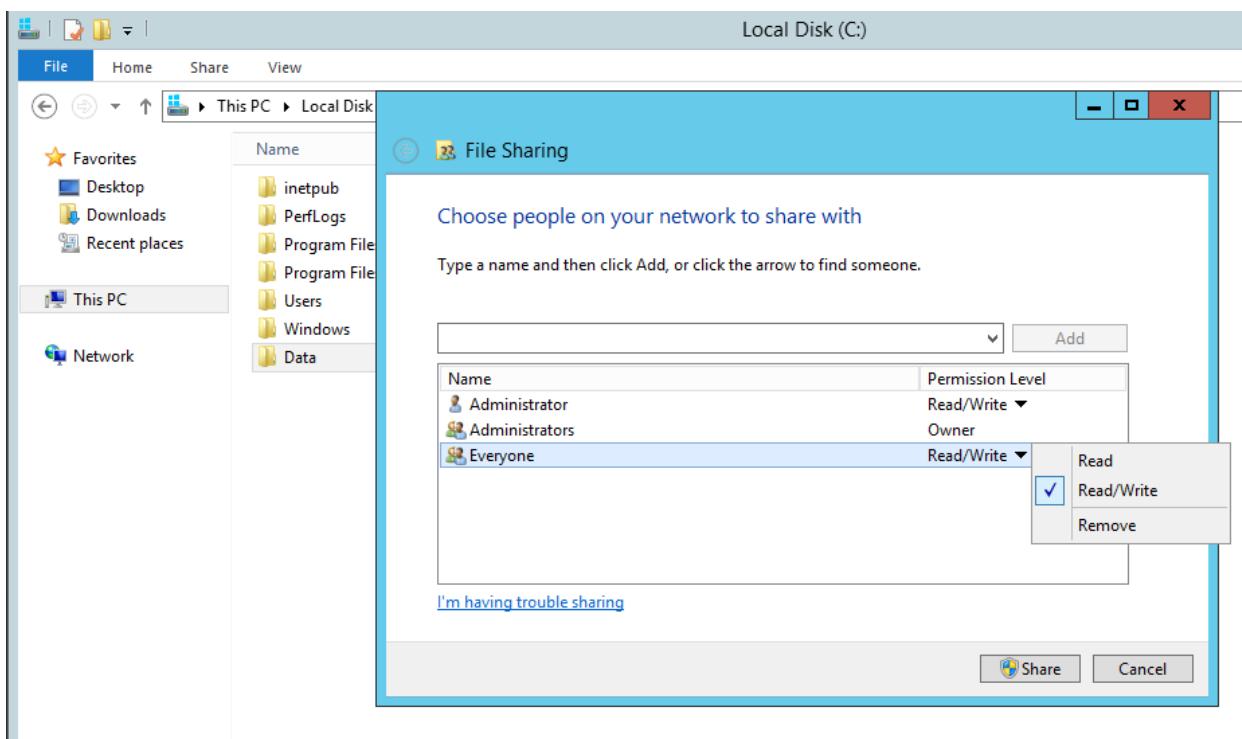
- Chọn Certificate Templates **Network Location Server Certificate** đã tạo trước đó – OK.



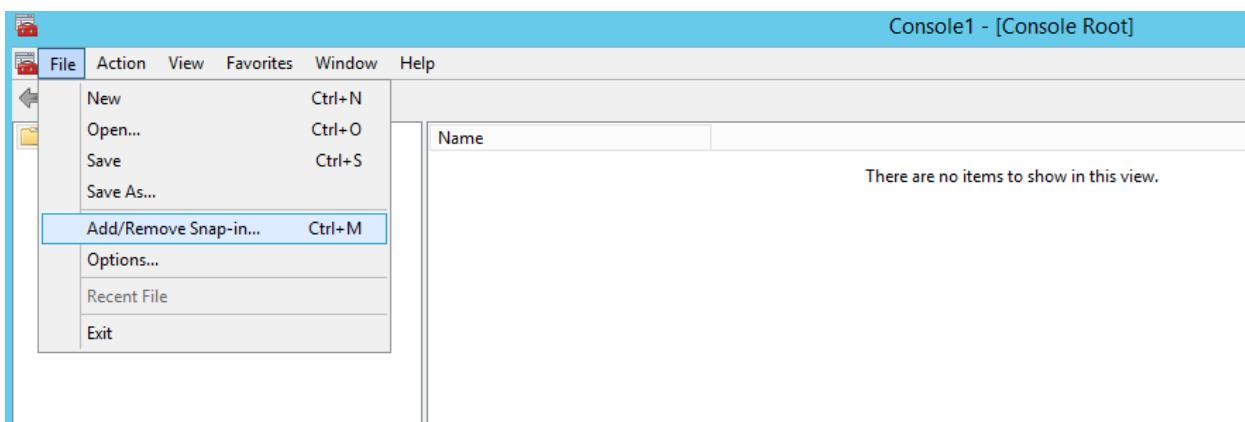
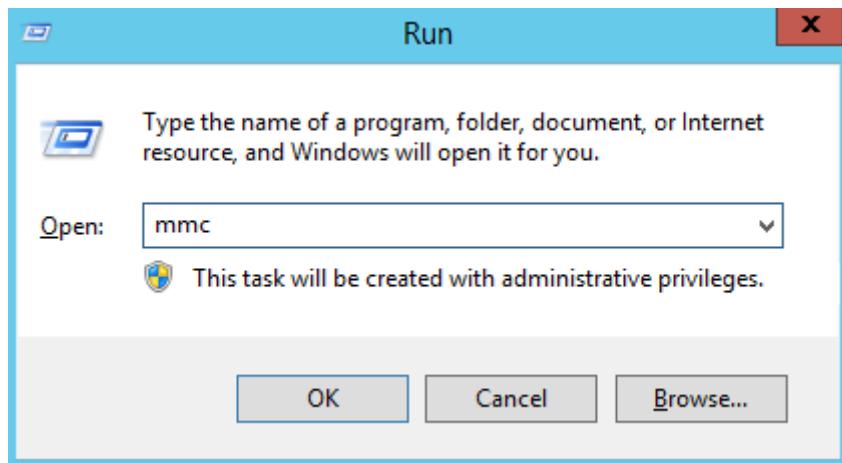
- Kiểm tra **Certificate Templates** mới đã được phát hành.

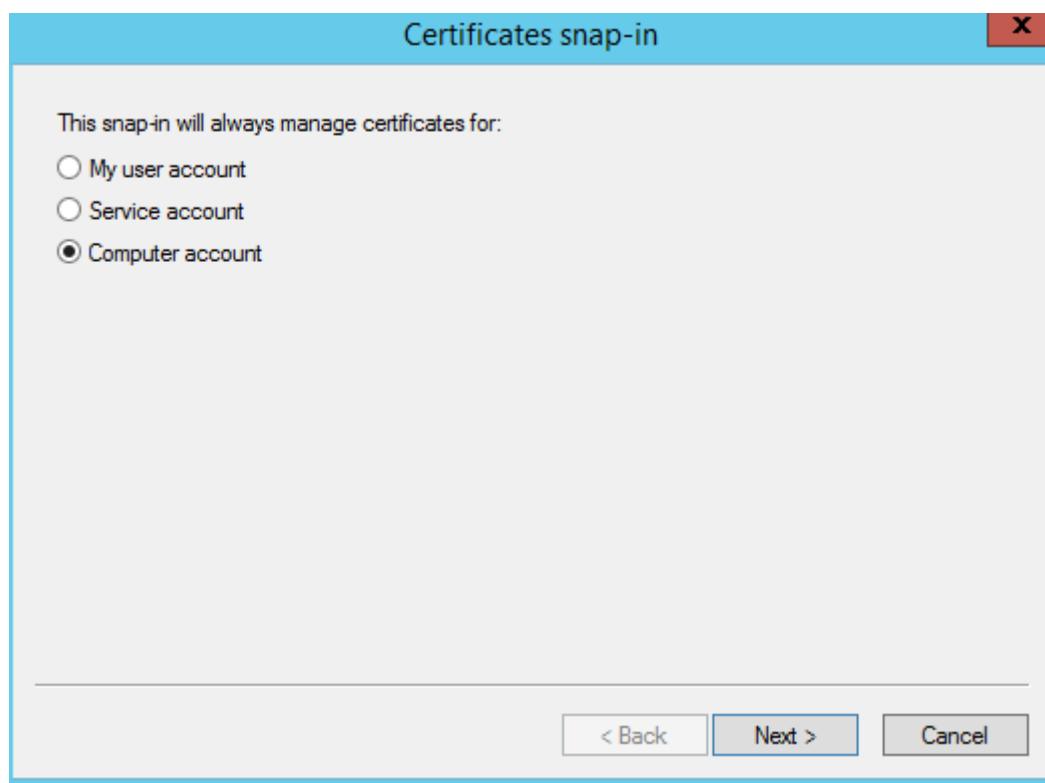
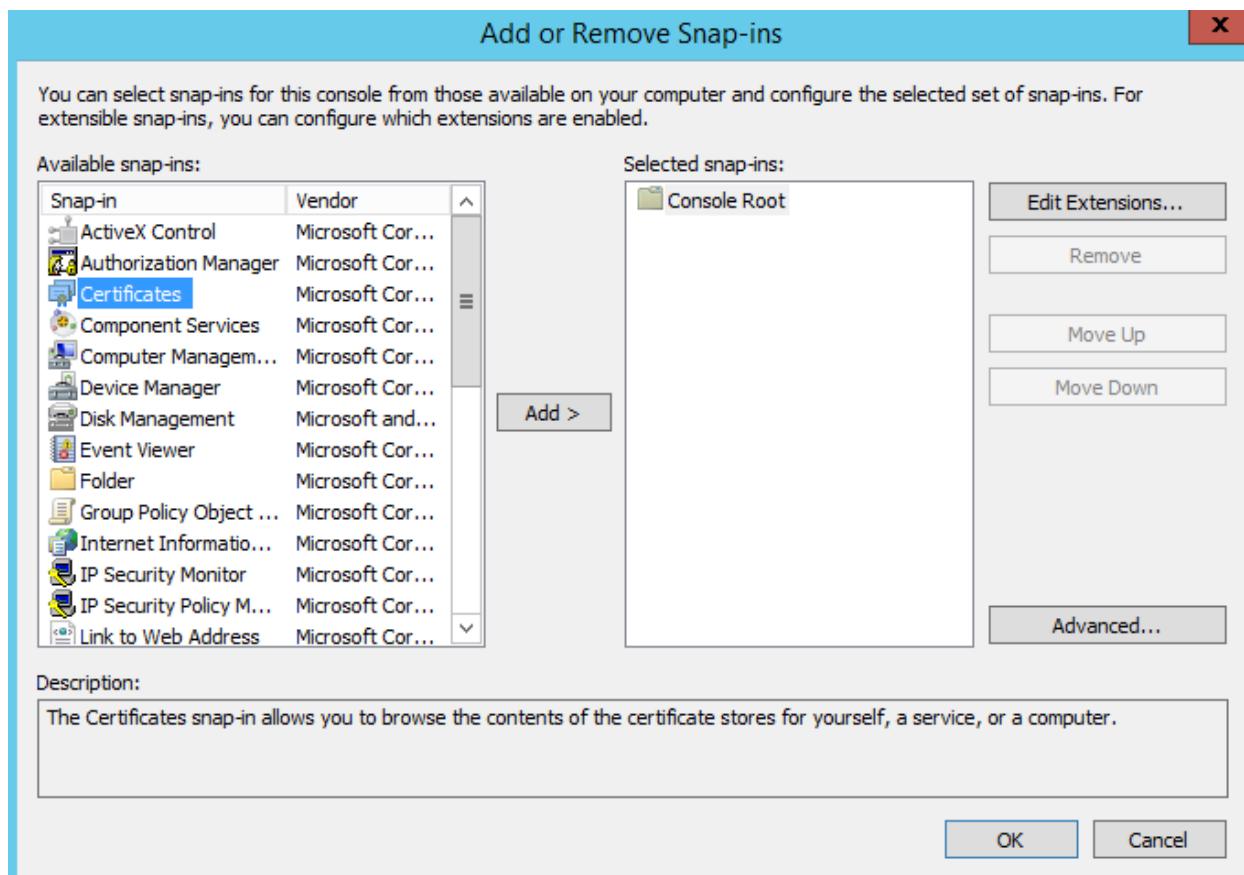


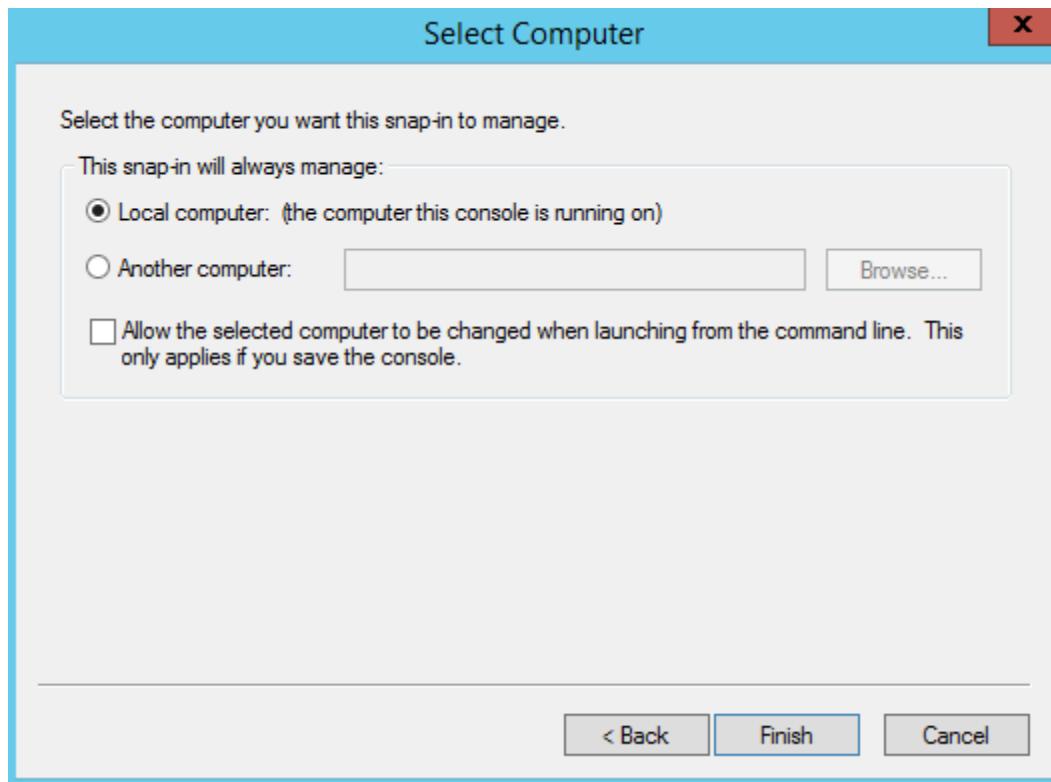
- Chuyển sang máy **BKAP-SRV12-01**, chuẩn bị tài nguyên nội bộ và gán vào **Default Web Site**.
 - Tạo một thư mục tên **Data** để kiểm tra sau đó share thư mục này cho **Everyone** quyền **Read/Write**.



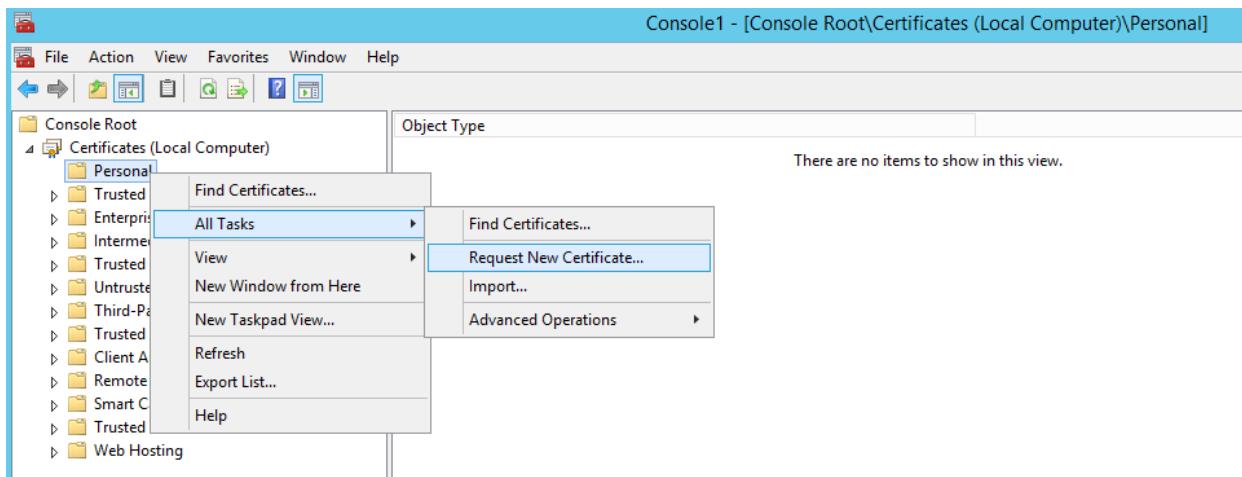
- Sử dụng **MMC** tạo một Console để quản lý *Certificate* cho Local Computer.



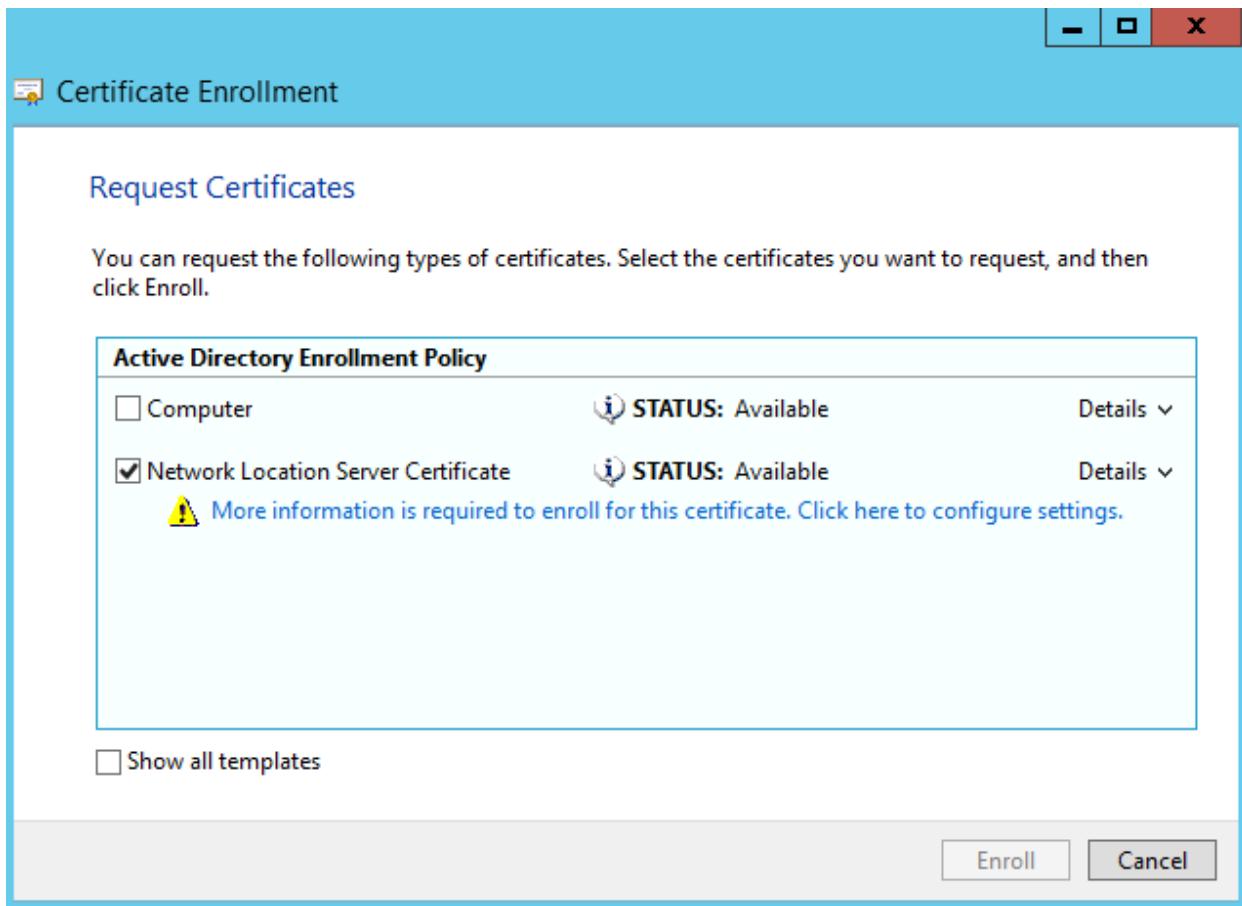




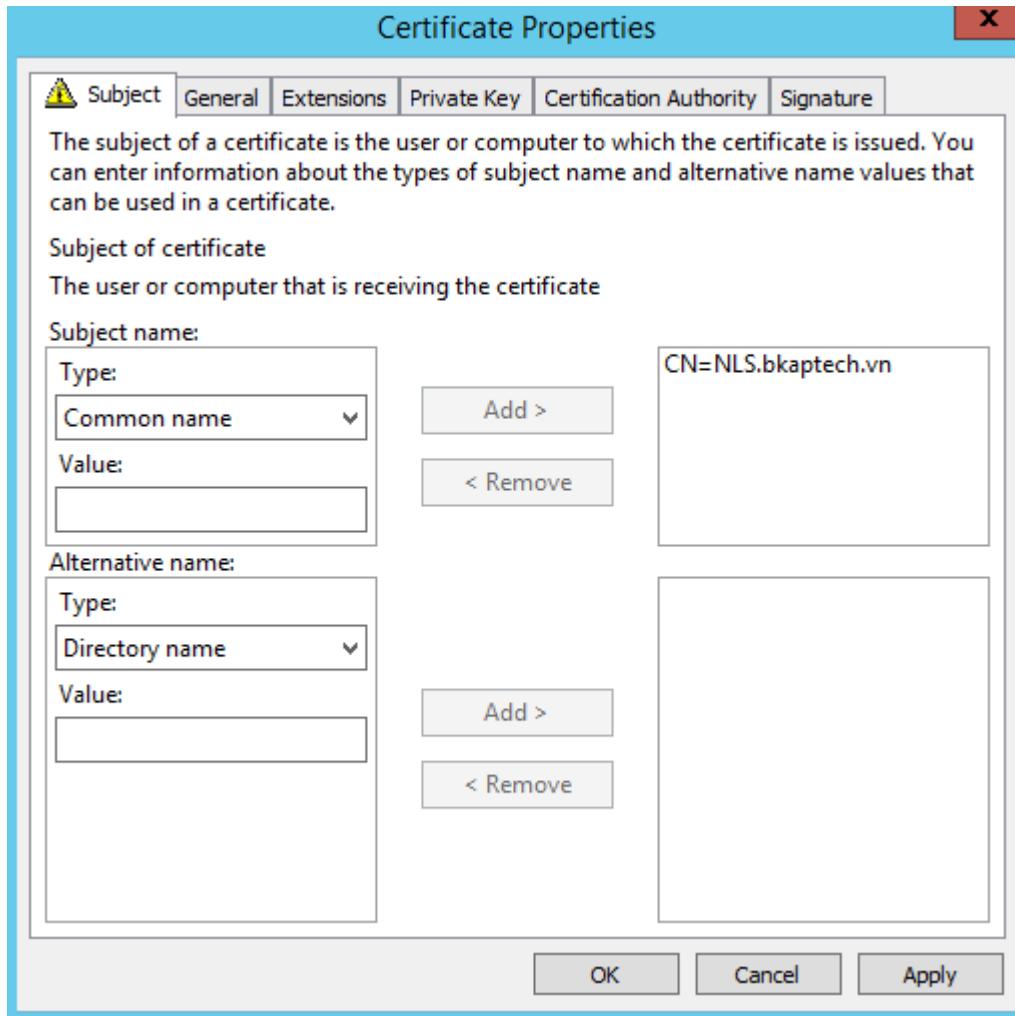
- Xin **Certificate** để thực hiện chức năng **Network Location Server**.
 - Tại cửa sổ **Console1**, chọn vào **Personal / All Tasks / Request New Certificate...**



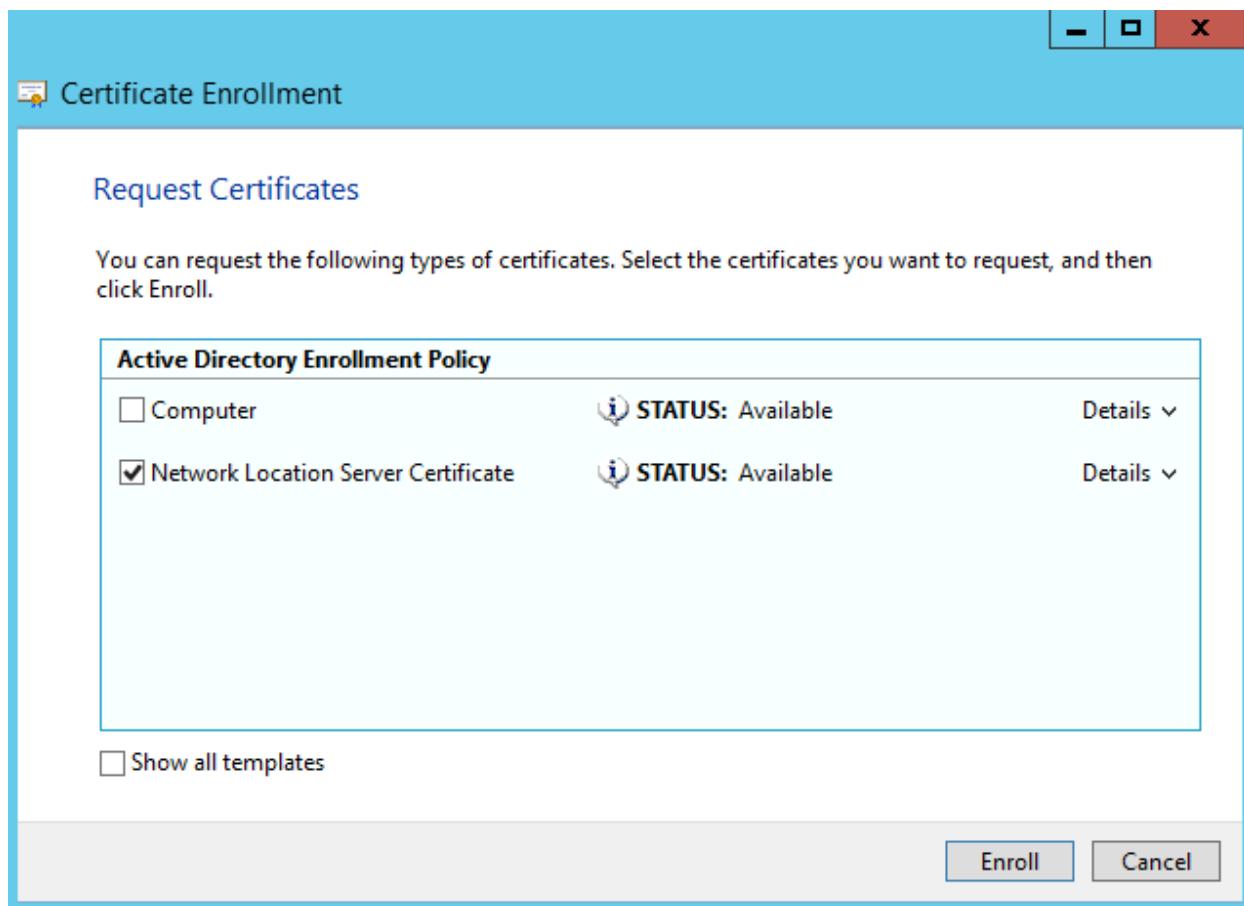
- Chọn *Certificate Templates* đã phát hành, chọn *More information* ... để thêm thông tin cho *Certificate*.



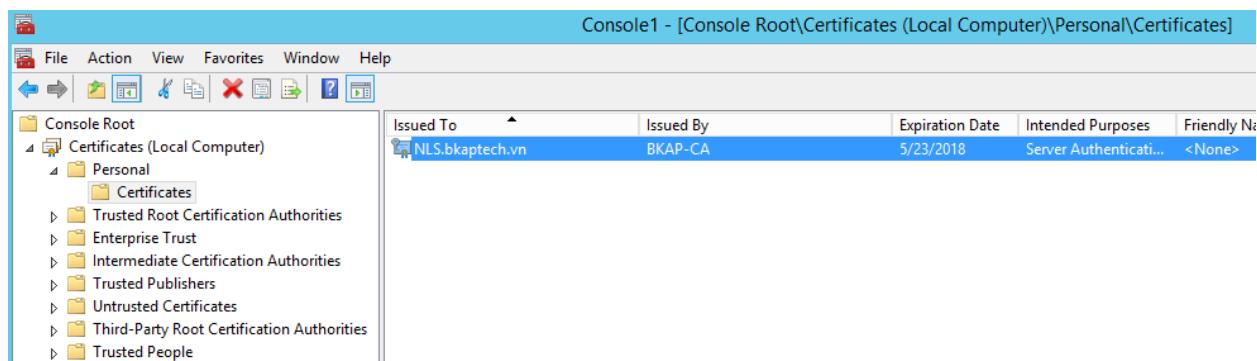
- Tại cửa sổ **Certificate Properties**, trong tab **Subject**, tại khung **Type**, chọn **Common Name**, trong khung **Value** nhập tên nội bộ của **Network Location Server** là **NLS.bkaptech.vn** và nhấn nút **Add=> OK**.

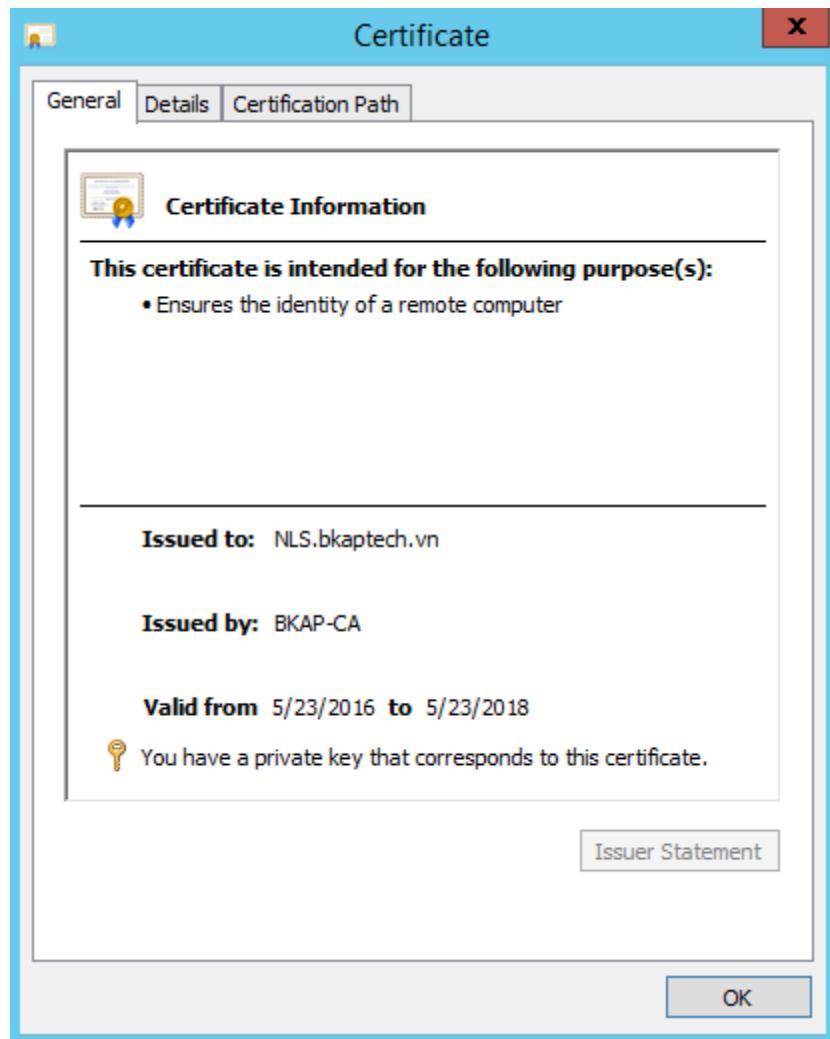


- Tại cửa sổ **Request Certificates**, click chọn vào **Enroll**.

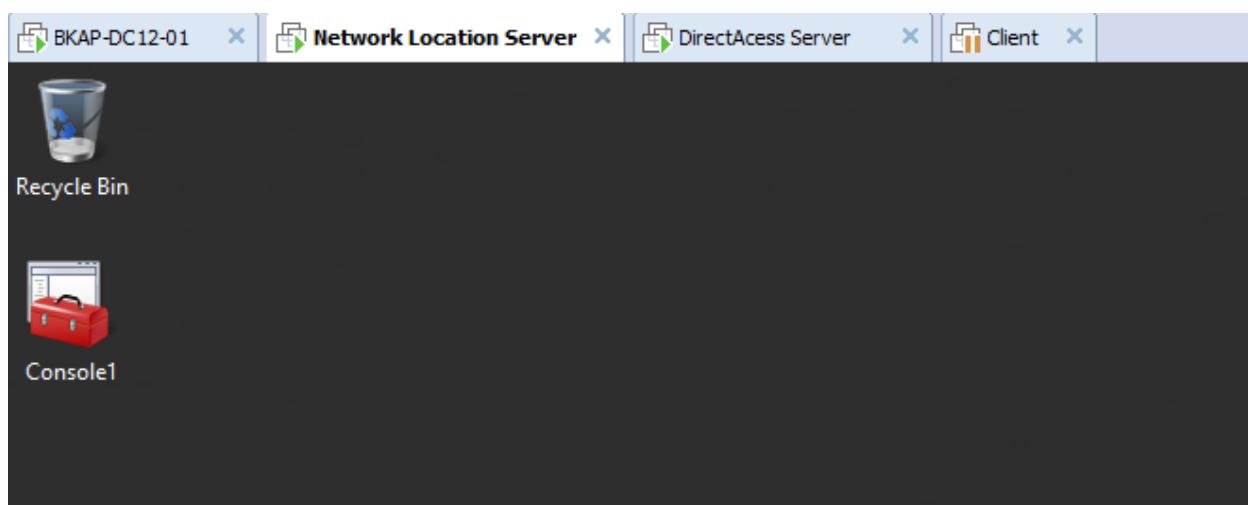


- Kiểm tra **Certificate**.

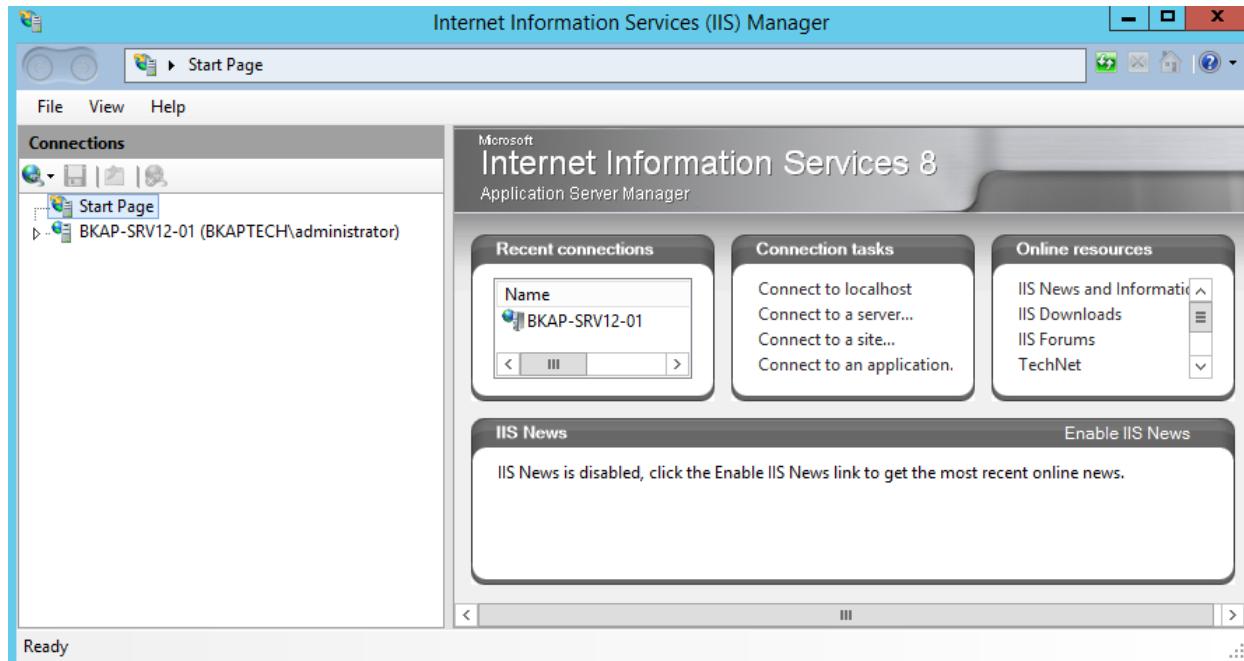




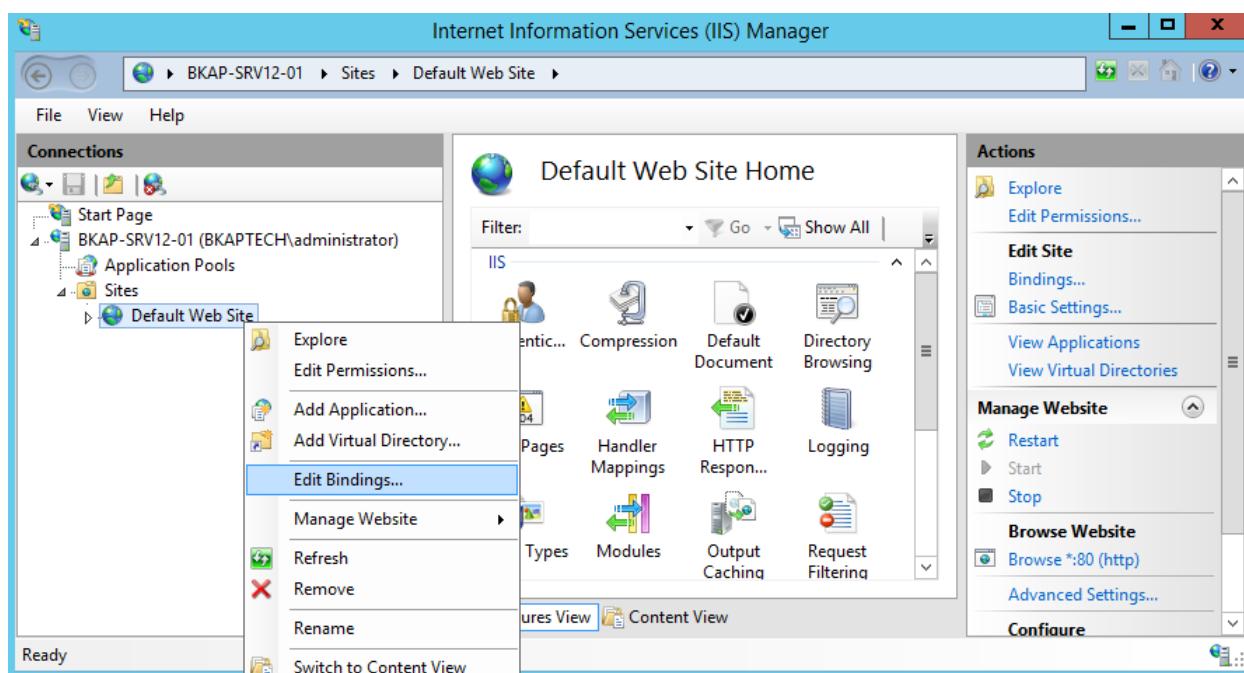
- Lưu Console này lên Desktop.



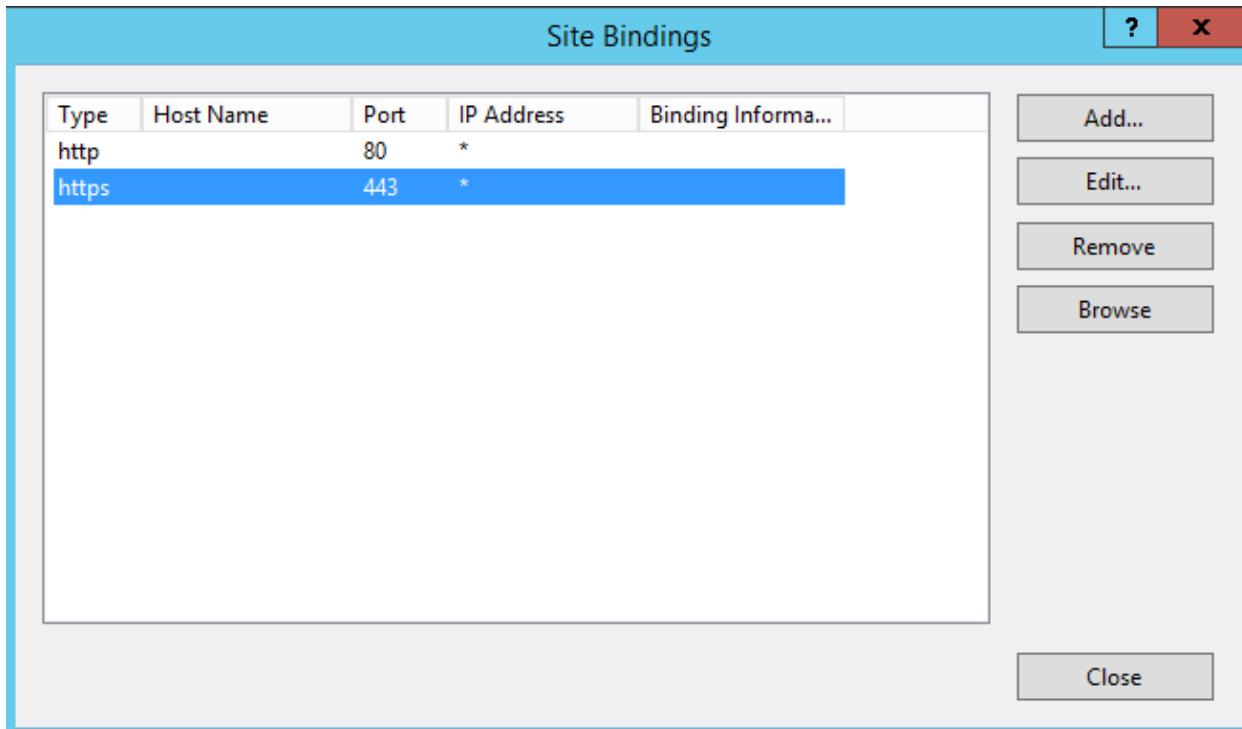
- Mở Web Server (IIS) cấu hình Certificate cho **Default Website**.



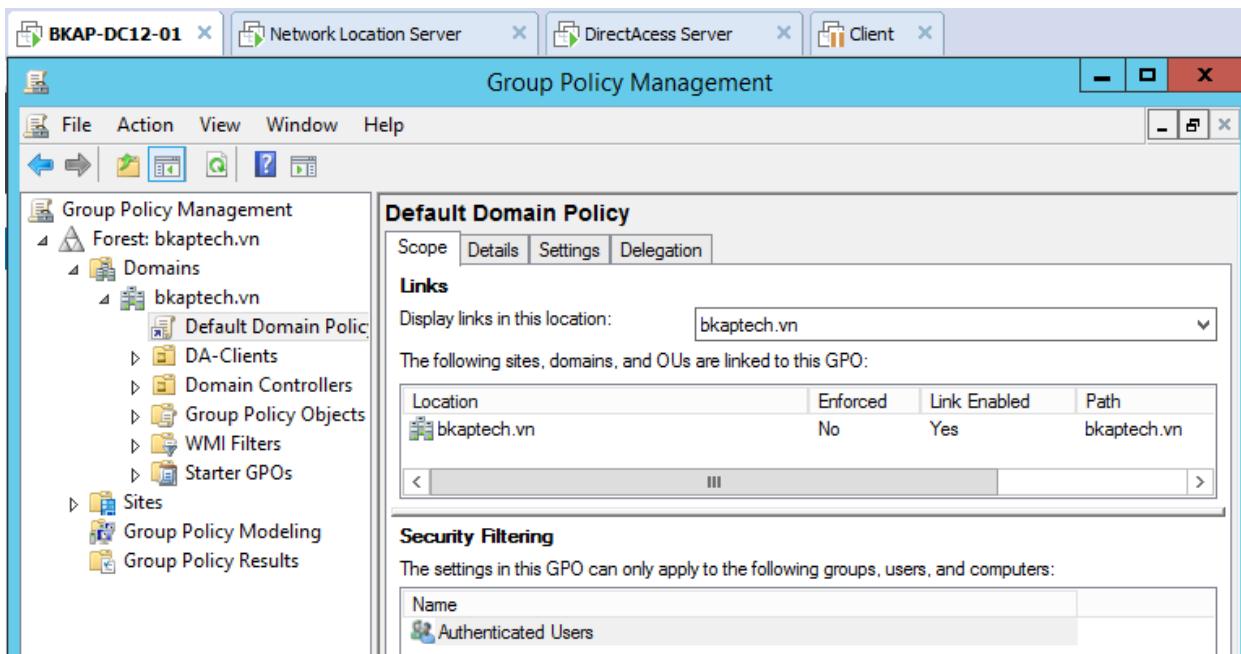
- Gán *Certificate* cho **Default Web Site** để Website này có thể chạy bằng **HTTPS**.
 - Tại **Default Web Site**, chọn **Edit Bindings...**



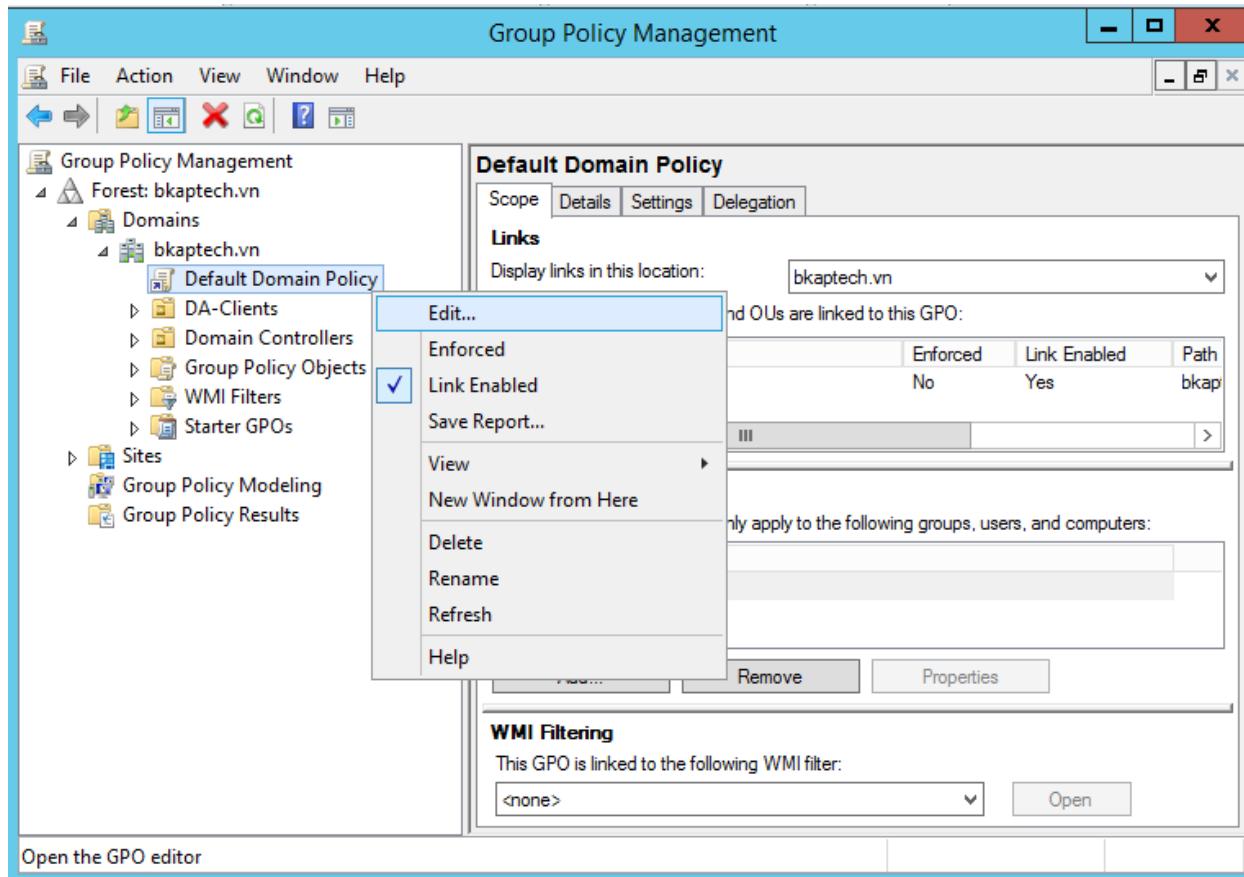
- Tại cửa sổ Site Bindings , Add thêm giao thức HTTPS.



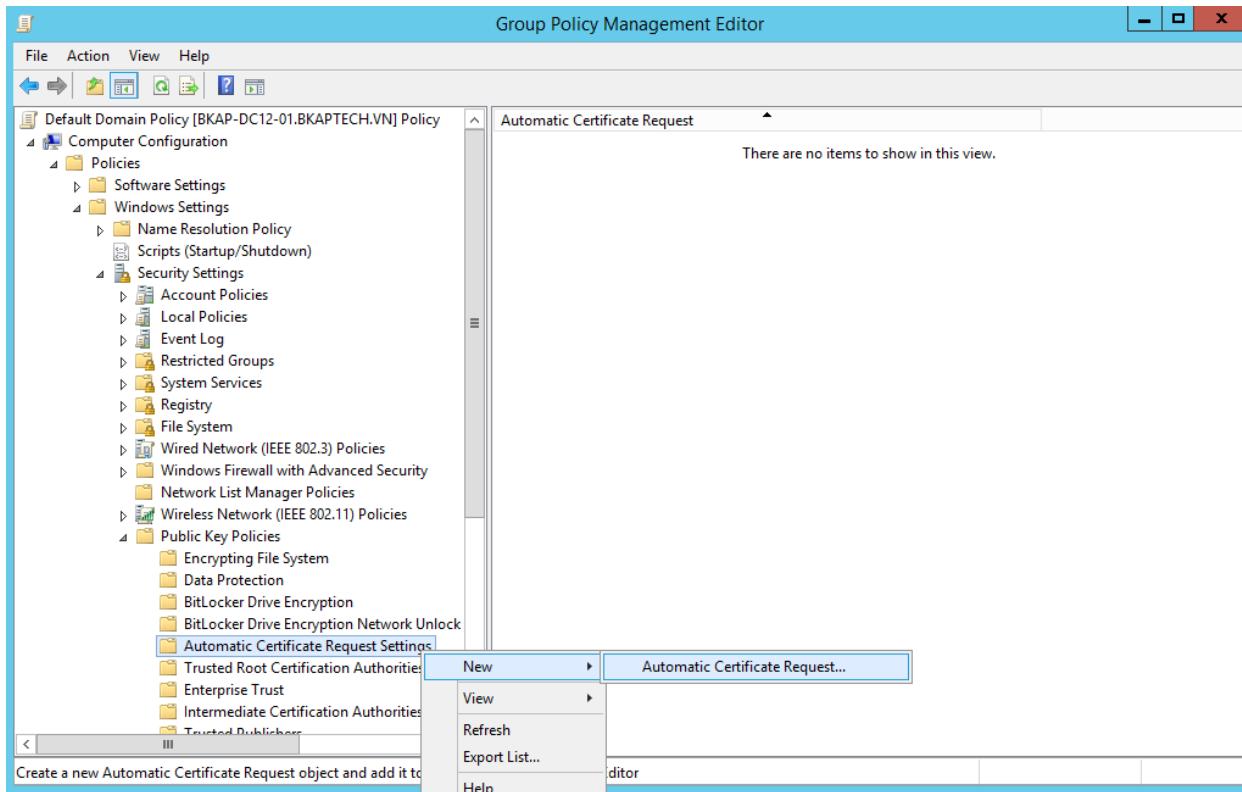
- Chính **GPO** để tự động cấp *Certificate Computer* cho tất cả các **Clients** trong *domain*.
 - ⇒ Do các **Direct Access Client** cần có một *Certificate Computer*. Thay vì để các máy **Client** tự xin *Certificate*, ta có thể dùng **GPO** để cho phép các **Client** tự động xin *Certificate* này.
 - Trên *DC12-01*, vào **Tools / Group Policy Management**.



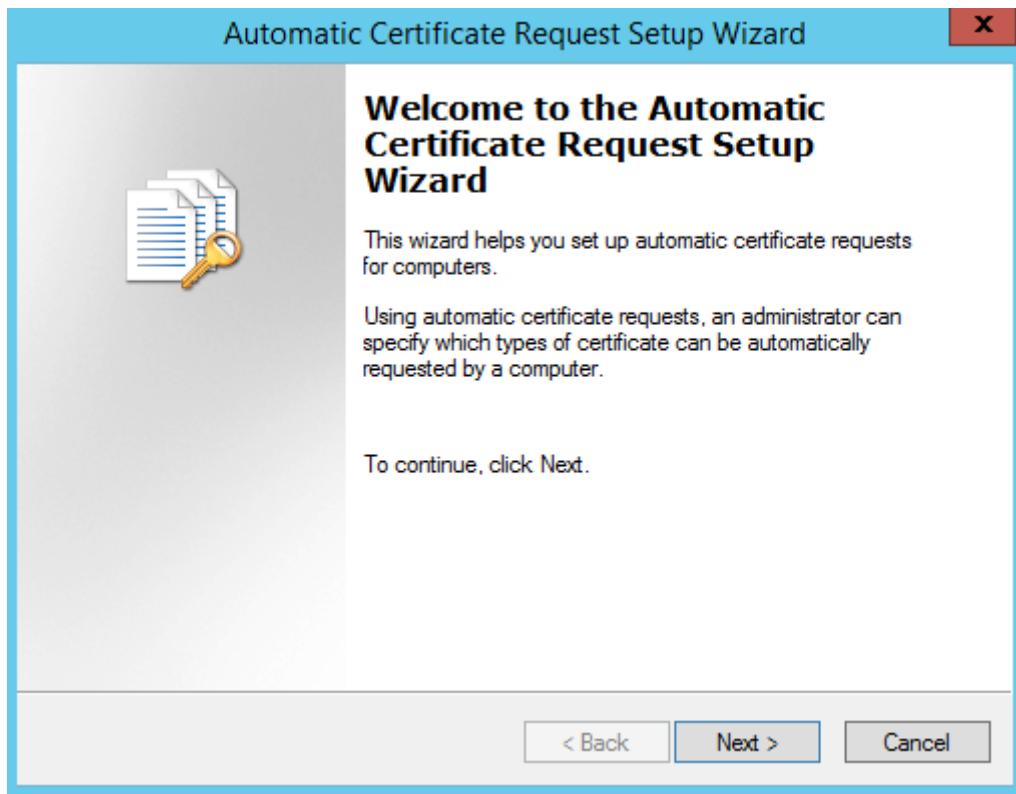
▪ Chọn Default Domain Policy / Edit.

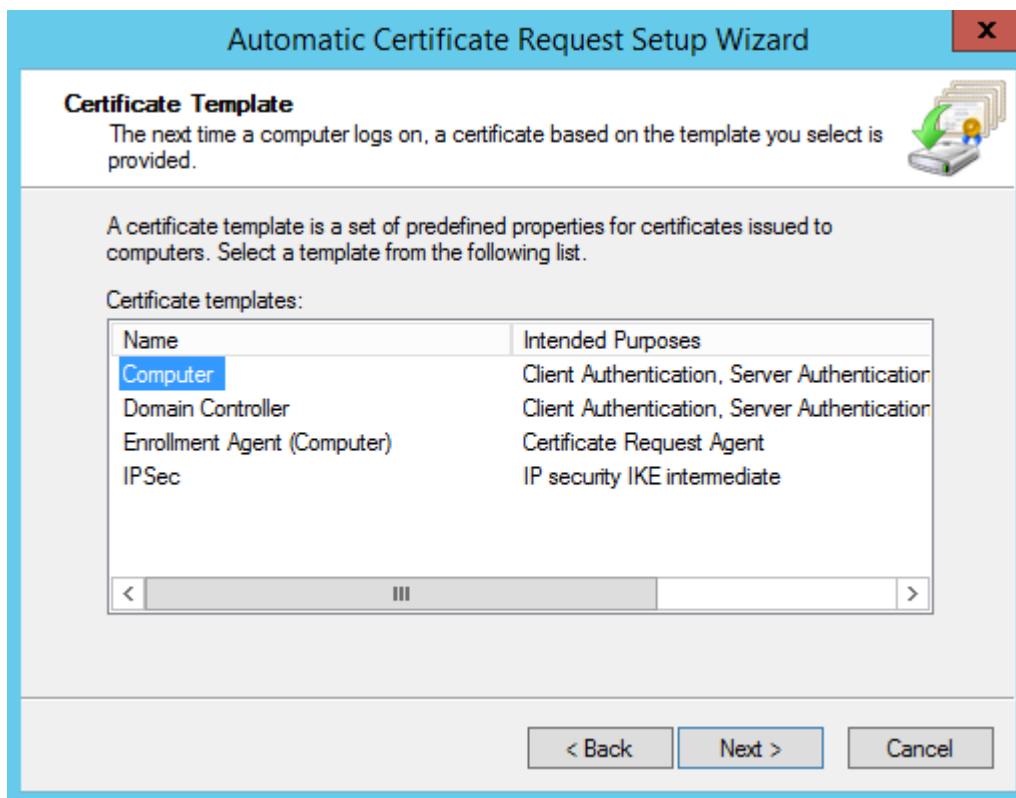


- Trong cửa sổ **Group Policy Management Editor**, chọn vào **Computer Configuration / Policies / Windows Settings / Security Settings / Public Key Policies / Automatic Certificate Request Settings / New / Automatic Certificate Request...**

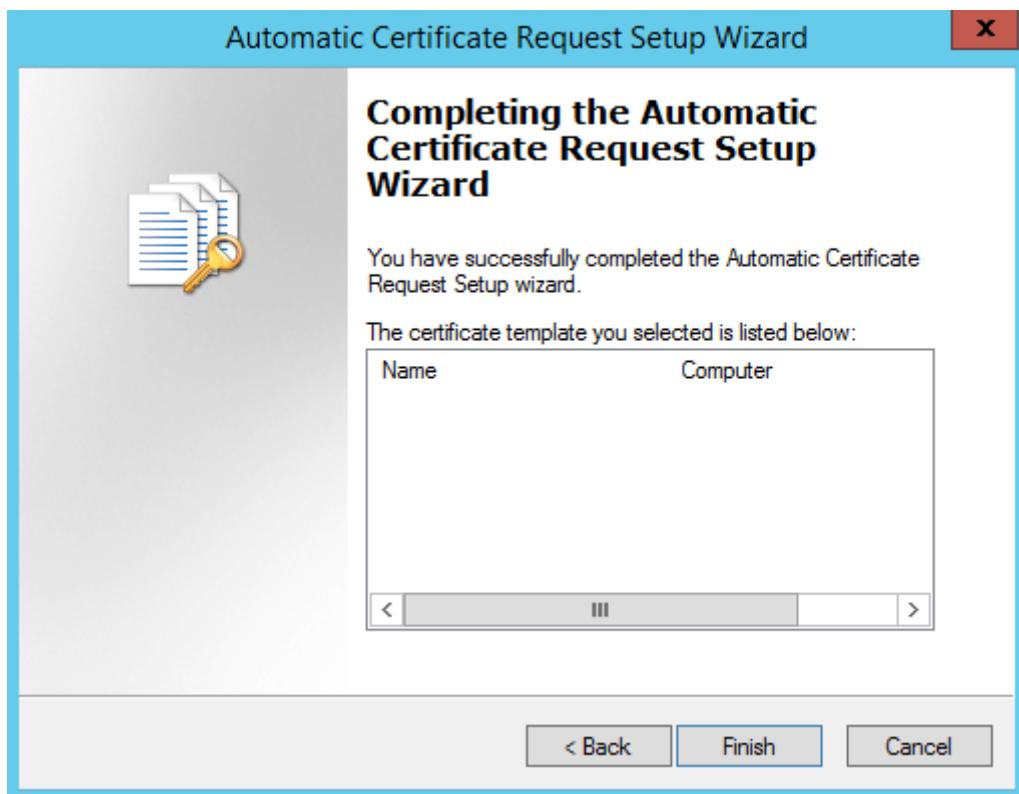


- Tại cửa sổ *Welcome to Automatic...* click vào **Next**.

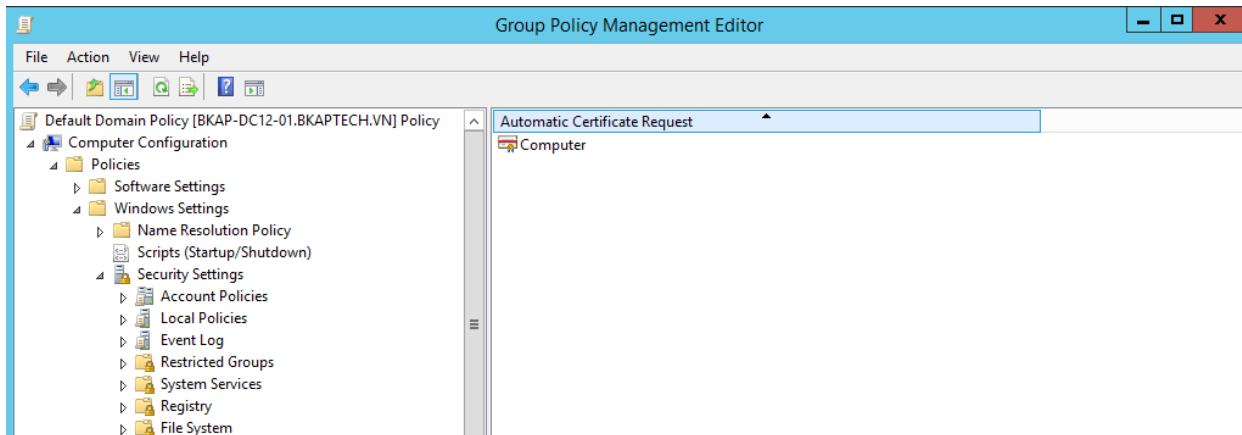


▪ Chọn Certificate Templates *Computer*

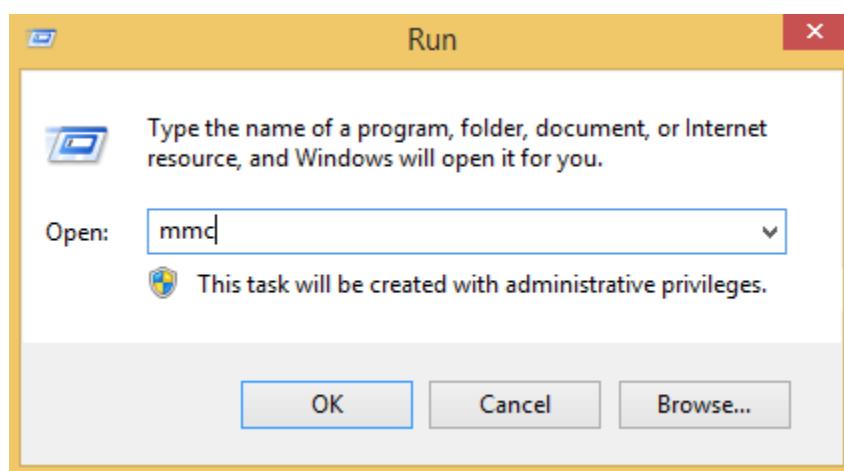
- Finish.

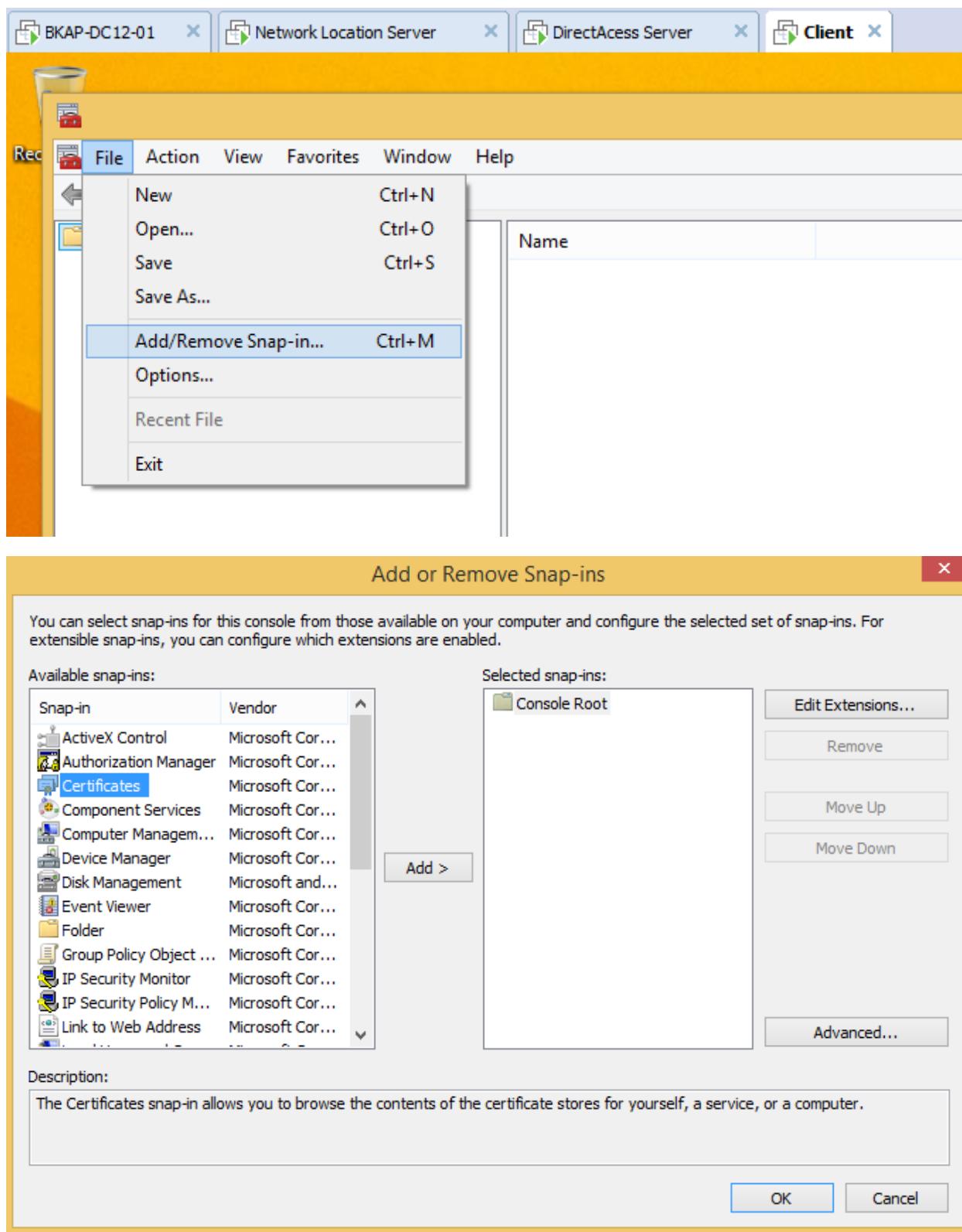


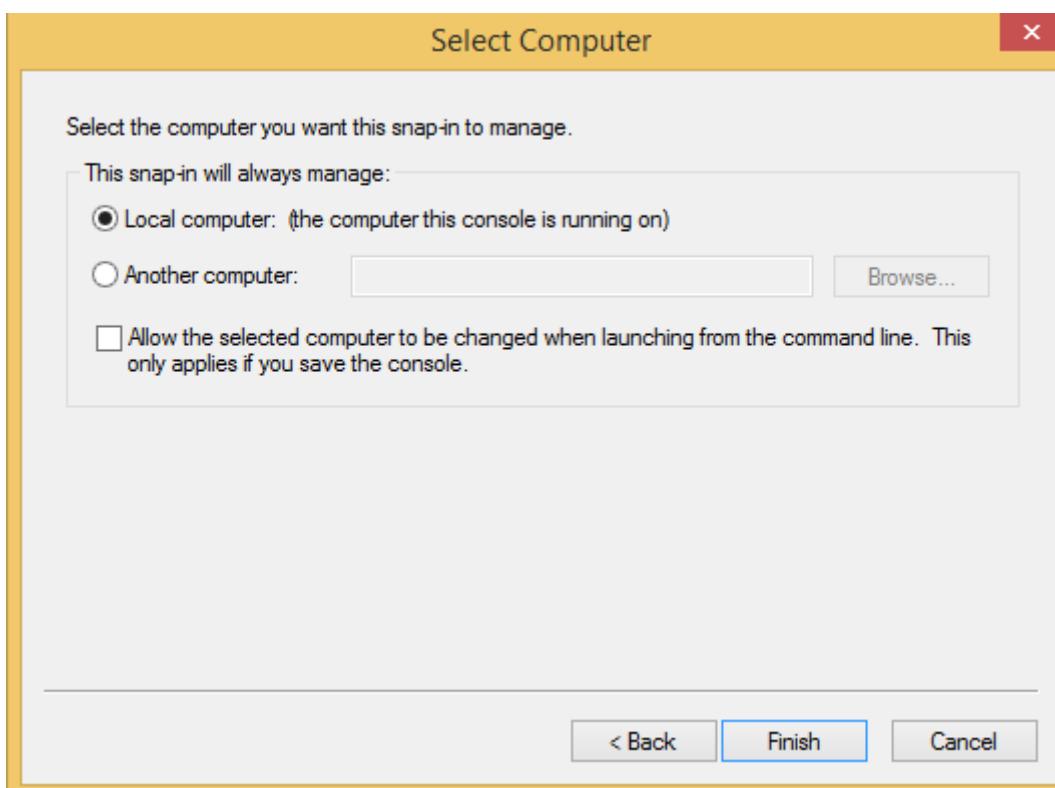
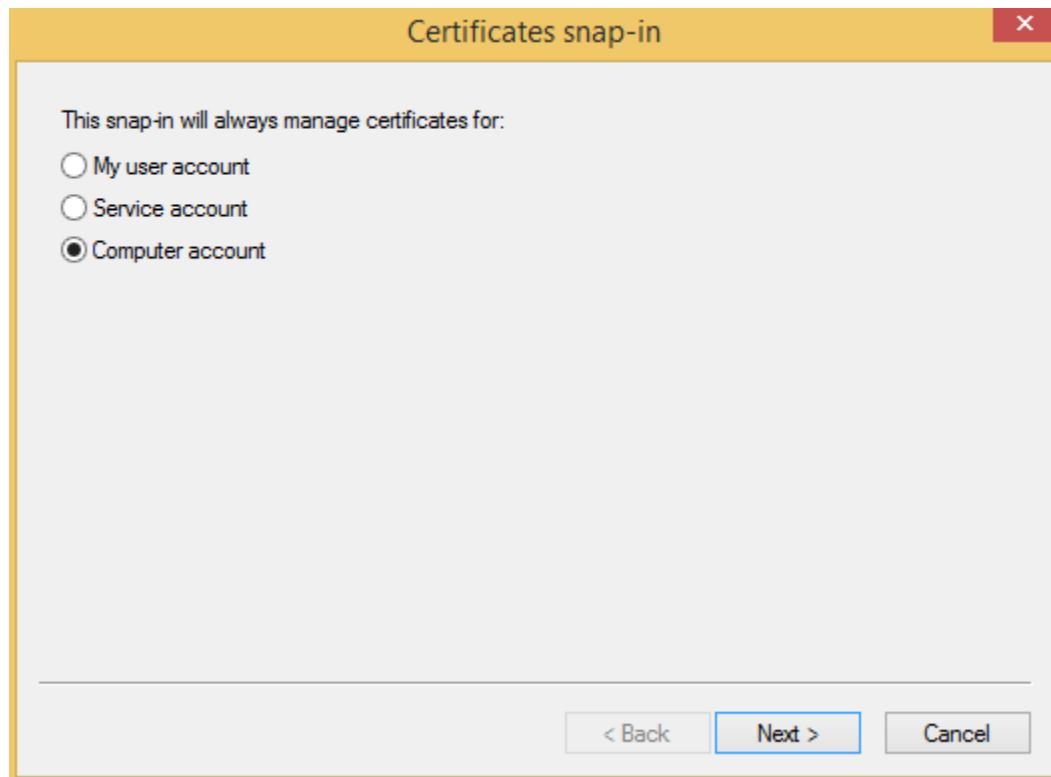
▪ Kiểm tra Policy.



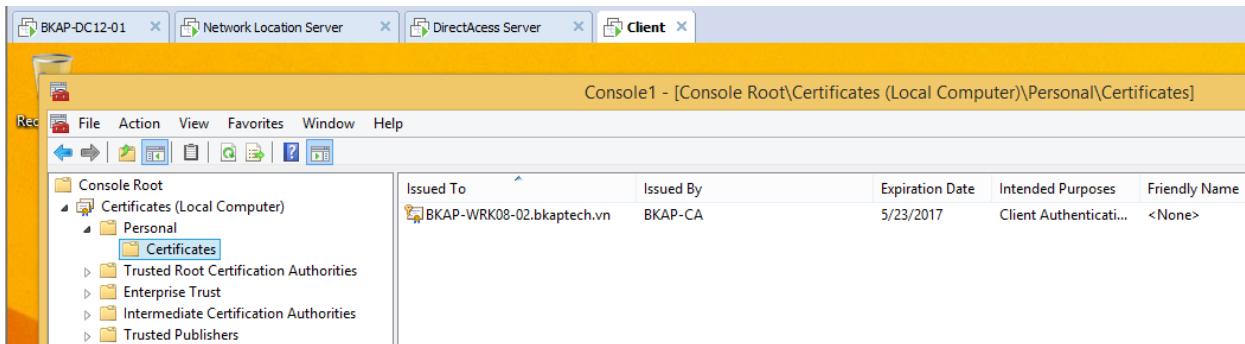
- Chuyển sang máy **Client WRK08-01**, **Restart** để áp dụng Policy.
 - Dùng **MMC** tạo một Console để kiểm tra Certificate.



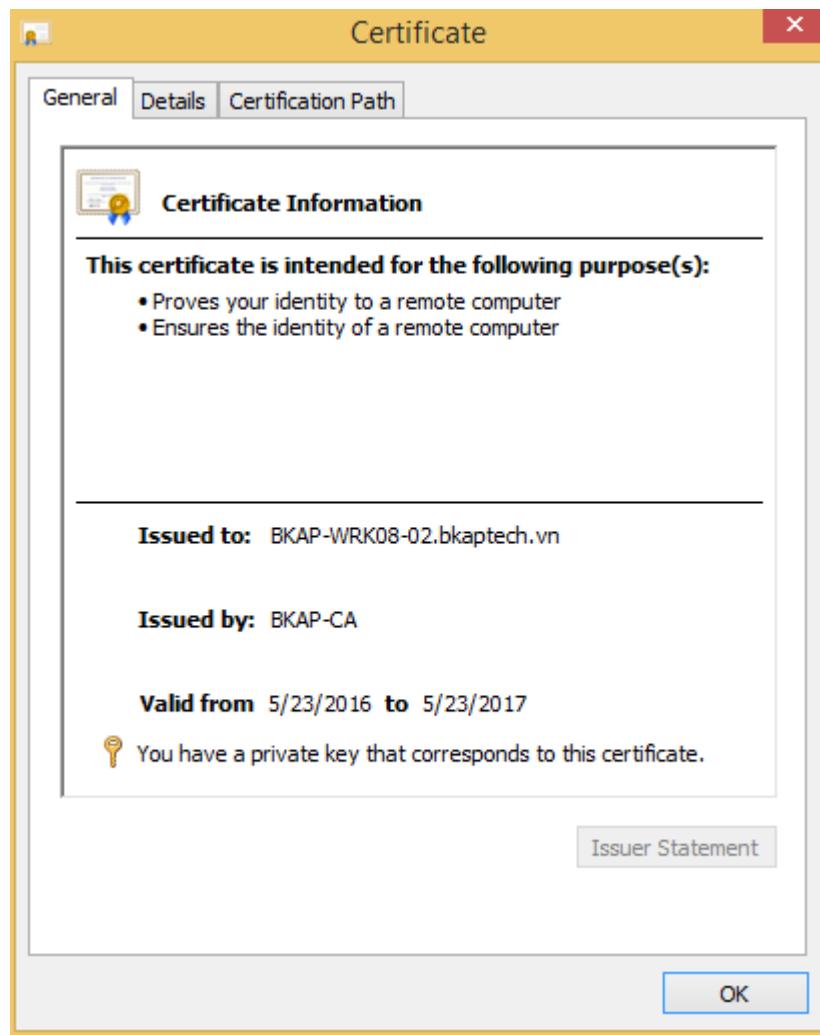




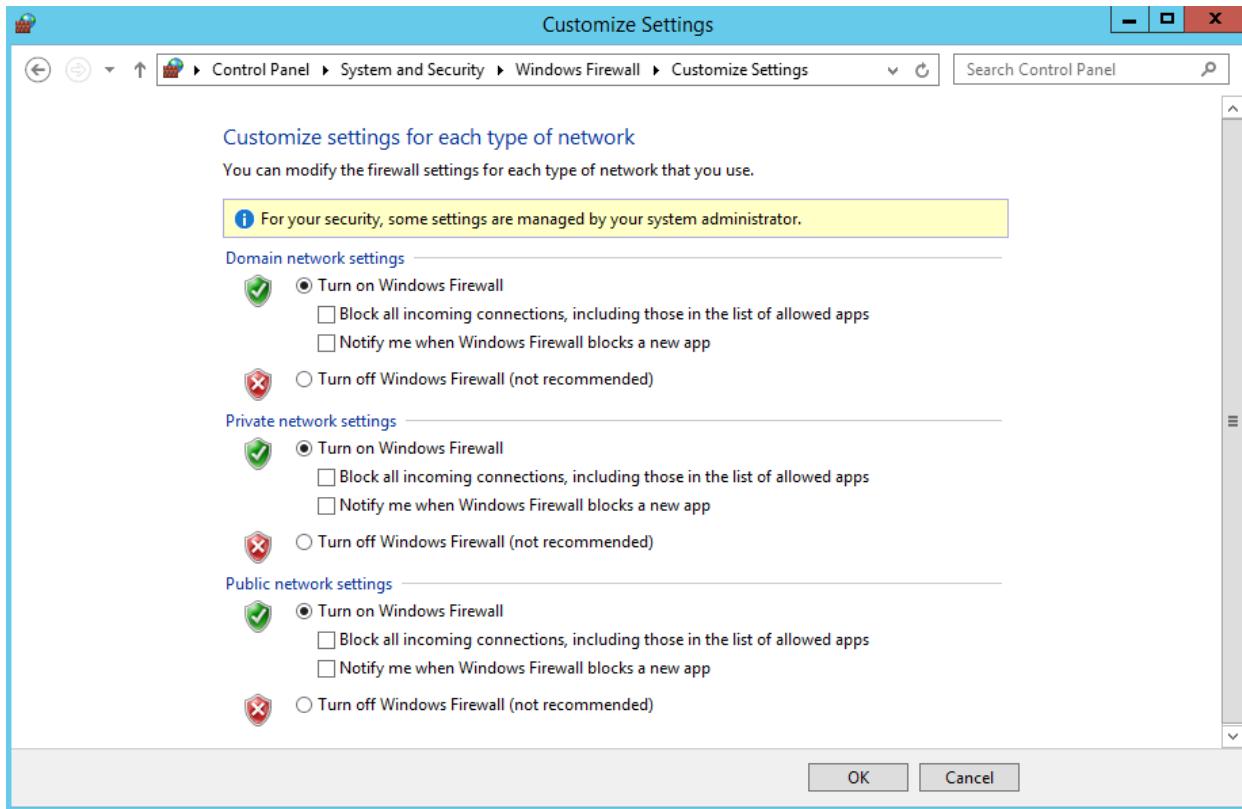
- Kiểm tra máy *Clients* đã có *Certificate*.



- Kiểm tra thông tin *Certificate*.



- Cấu hình Direct Access Server trên máy *SRV12-02*:
 - Trên máy *SRV12-02*, kiểm tra bật *Windows Firewall* nếu đang tắt.



The screenshot shows the Windows Firewall settings window. At the top, it says "Windows Firewall". Below that, the breadcrumb navigation shows "Control Panel > System and Security > Windows Firewall". A search bar is on the right. On the left, there's a sidebar with links like "Allow an app or feature through Windows Firewall", "Change notification settings", "Turn Windows Firewall on or off", "Restore defaults", "Advanced settings", and "Troubleshoot my network". The main content area has a heading "Help protect your PC with Windows Firewall" and a note: "Windows Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network." It shows three network types: "Domain networks" (Not connected), "Private networks" (Not connected), and "Guest or public networks" (Connected). Below this, it lists "Windows Firewall state: On", "Incoming connections: Block all connections to apps that are not on the list of allowed apps", "Active public networks: Unidentified network", and "Notification state: Do not notify me when Windows Firewall blocks a new app". At the bottom left, there's a "See also" section with links to "Action Center" and "Network and Sharing Center".

- Kiểm tra IP address của 2 card mạng:

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

C:\Users\administrator.BKAPTECH>ipconfig /all

Windows IP Configuration

 Host Name . . . . . : BKAP-SRV12-02
 Primary Dns Suffix . . . . . : bkaptech.vn
 Node Type . . . . . : Hybrid
 IP Routing Enabled. . . . . : No
 WINS Proxy Enabled. . . . . : No
 DNS Suffix Search List. . . . . : bkaptech.vn

Ethernet adapter Ethernet1:

 Connection-specific DNS Suffix . . . . . : Intel(R) 82574L Gigabit Network Connection
 Description . . . . . : Intel(R) 82574L Gigabit Network Connection
 Physical Address. . . . . : 00-0C-29-82-F3-81
 DHCP Enabled. . . . . : No
 Autoconfiguration Enabled . . . . . : Yes
 Link-local IPv6 Address . . . . . : fe80::4464:a97e:4517:f2a6%16(PREFERRED)
 IPv4 Address. . . . . : 123.1.1.1(PREFERRED)
 Subnet Mask . . . . . : 255.255.255.0
 Default Gateway . . . . . :
 DHCPv6 IAID . . . . . : 419433513
 DHCPv6 Client DUID. . . . . : 00-01-00-01-1E-C6-77-CD-00-0C-29-82-F3-77
 DNS Servers . . . . . : fec0:0:0:ffff::1%1
                         fec0:0:0:ffff::2%1
                         fec0:0:0:ffff::3%1
 NetBIOS over Tcpip. . . . . : Enabled

Ethernet adapter Ethernet0:

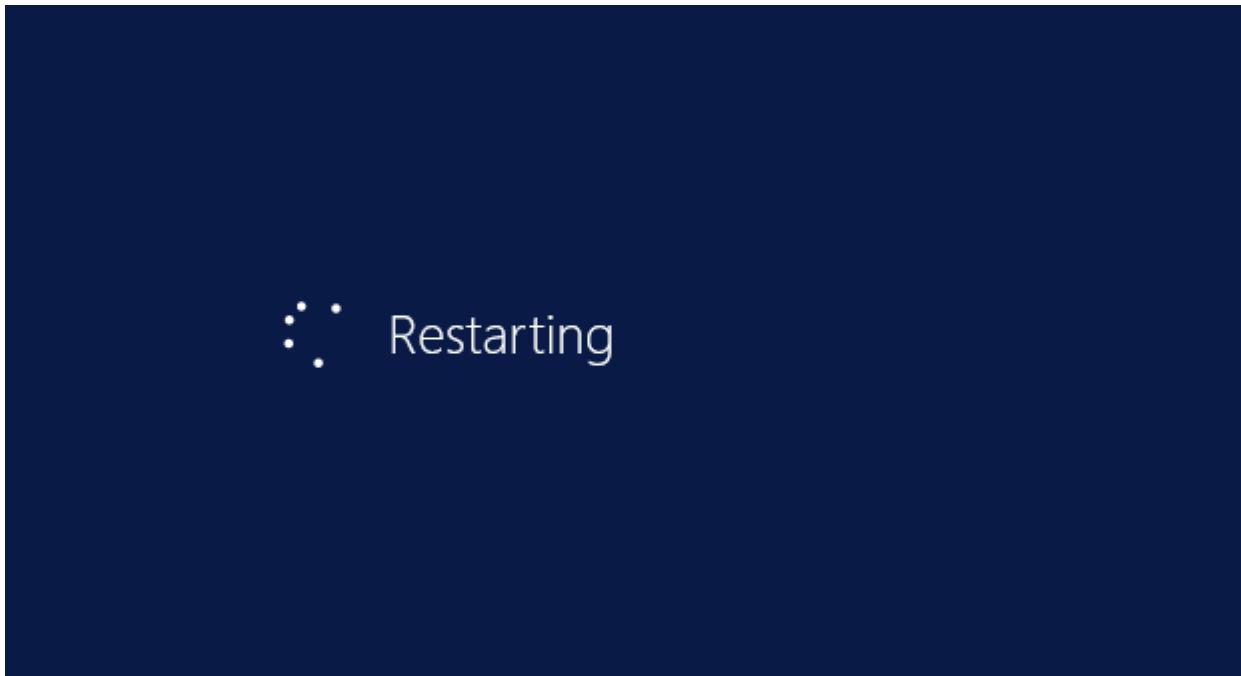
 Connection-specific DNS Suffix . . . . . : Intel(R) 82574L Gigabit Network Connection
 Description . . . . . : Intel(R) 82574L Gigabit Network Connection
 Physical Address. . . . . : 00-0C-29-82-F3-77
 DHCP Enabled. . . . . : No
 Autoconfiguration Enabled . . . . . : Yes
 Link-local IPv6 Address . . . . . : fe80::186f:87a7:c048:cb01%12(PREFERRED)
 IPv4 Address. . . . . : 192.168.1.1(PREFERRED)
 Subnet Mask . . . . . : 255.255.255.0
 Default Gateway . . . . . :
 DHCPv6 IAID . . . . . : 301993001
 DHCPv6 Client DUID. . . . . : 00-01-00-01-1E-C6-77-CD-00-0C-29-82-F3-77
 DNS Servers . . . . . : 192.168.1.2
 NetBIOS over Tcpip. . . . . : Enabled
```

- Dùng lệnh **gpupdate /force** và **restart** lại máy tính để đảm bảo cập nhật **Policy**.

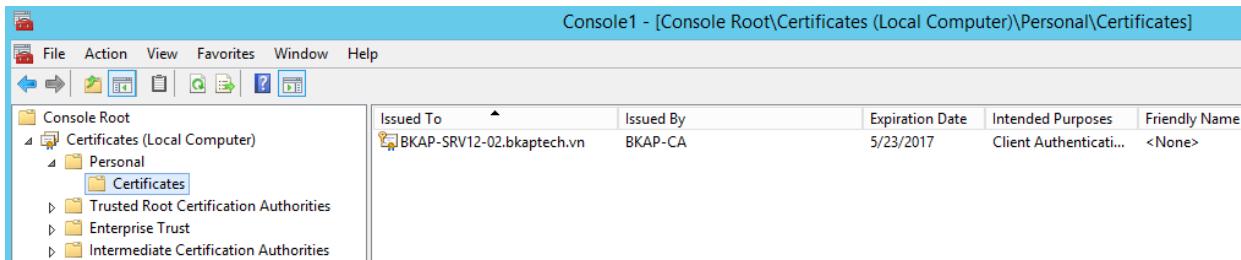
```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\administrator.BKAPTECH>gpupdate /force
Updating policy...
Computer Policy update has completed successfully.
User Policy update has completed successfully.

C:\Users\administrator.BKAPTECH>_
```

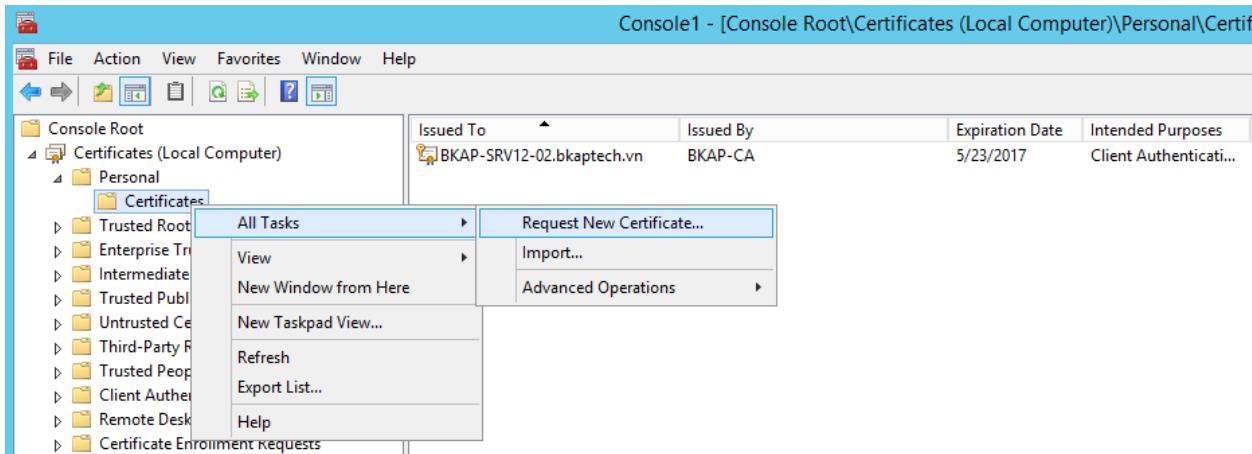


- Dùng **MMC** tạo Console kiểm tra *Certificate* như các bước trước đó.

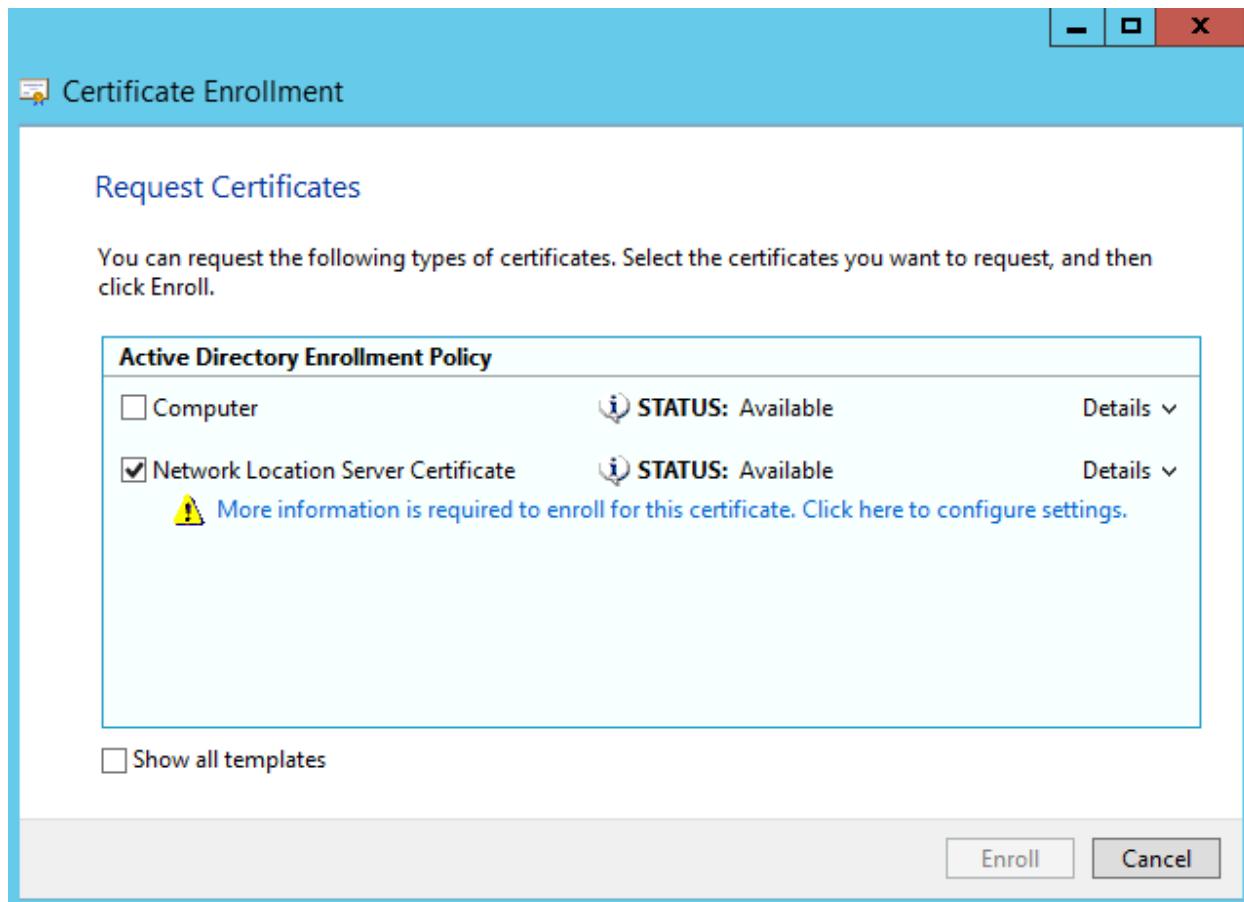


⇒ Máy này đã có một *Certificate* đã cấu hình tự động xin *Certificate* ở bước trước, ta cần xin một *Certificate* mới để đảm nhận vai trò **Direct Access Server**.

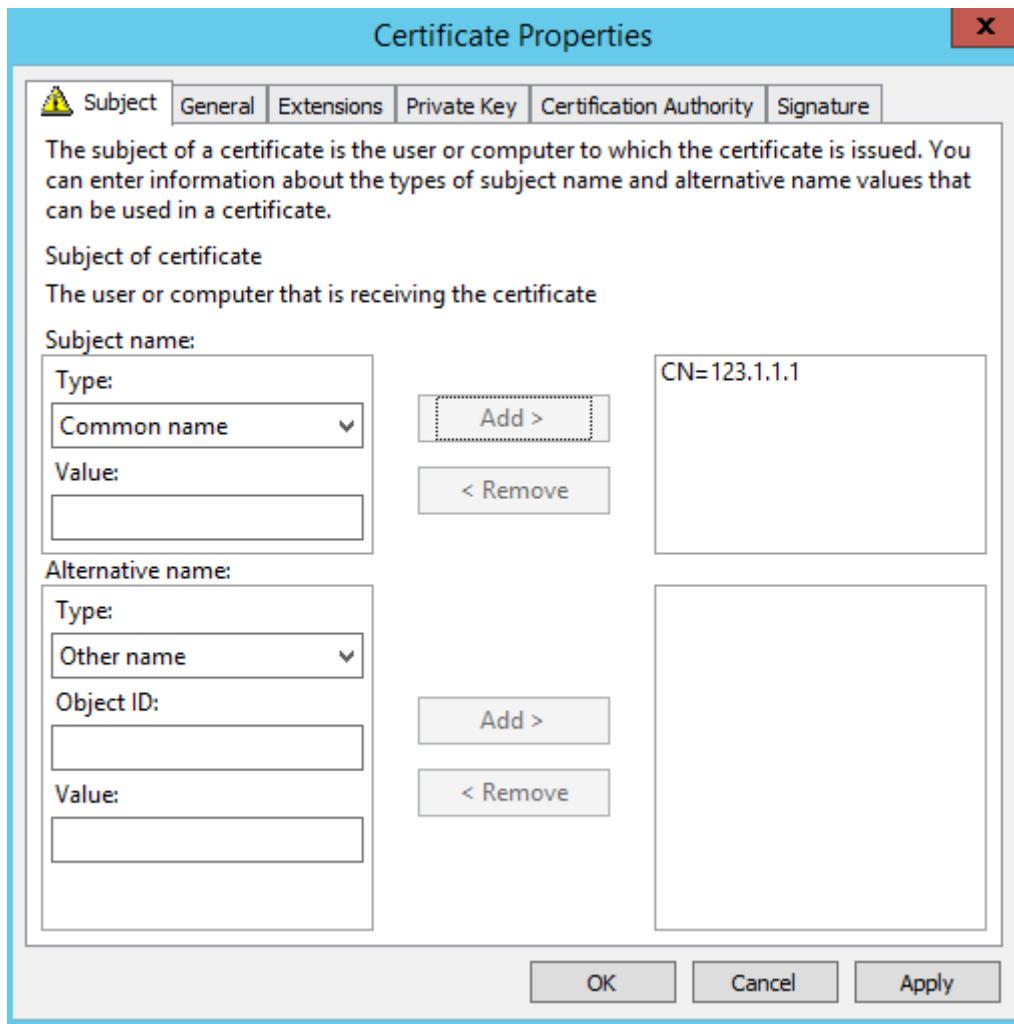
- Trong cửa sổ **Console1..**, click chuột phải tại **Personal / Certificates / All Tasks / Request New Certificate...**



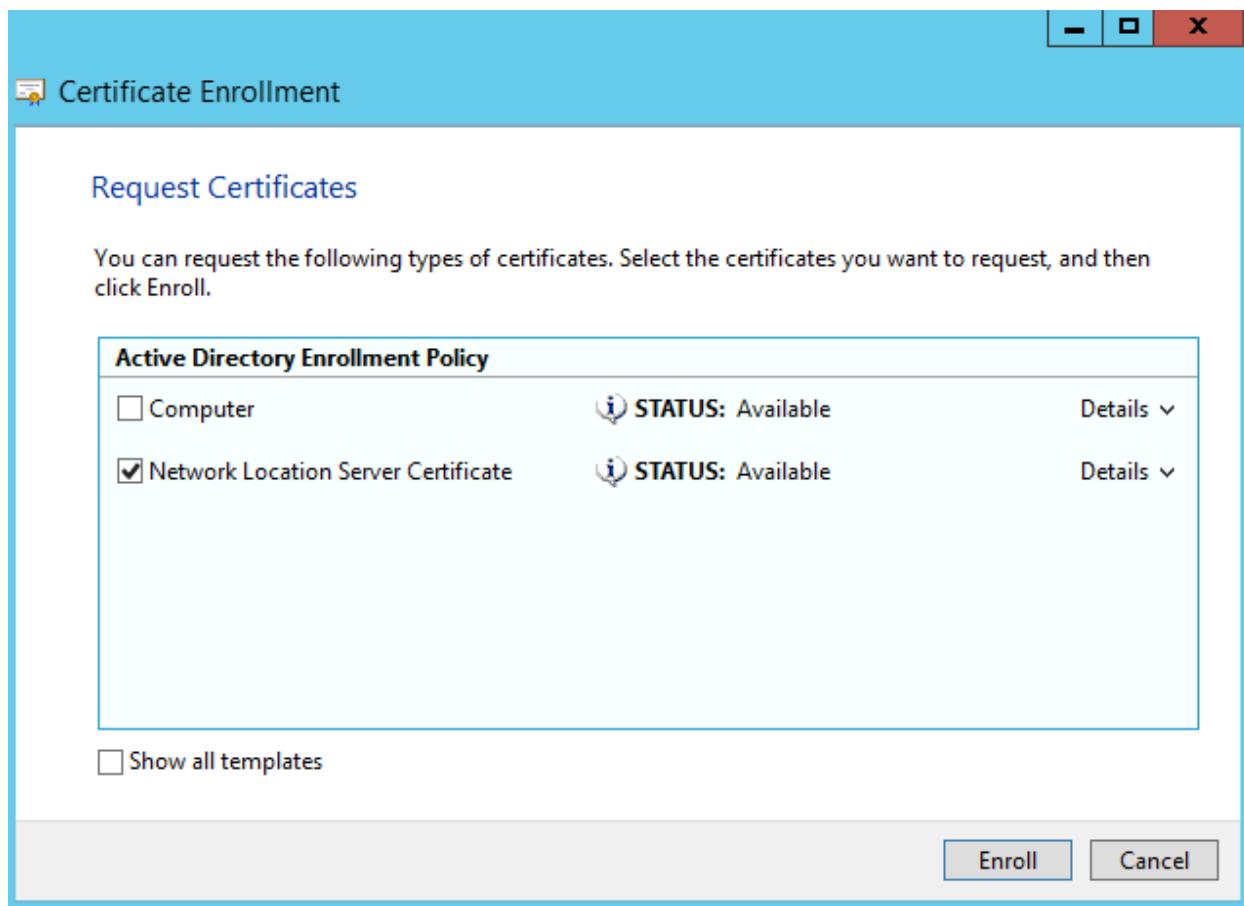
- Tại cửa sổ **Request Certificates**, tích chọn **Network Location Server Certificate**, click vào *More information...* để thêm thông tin cho *Certificate*.



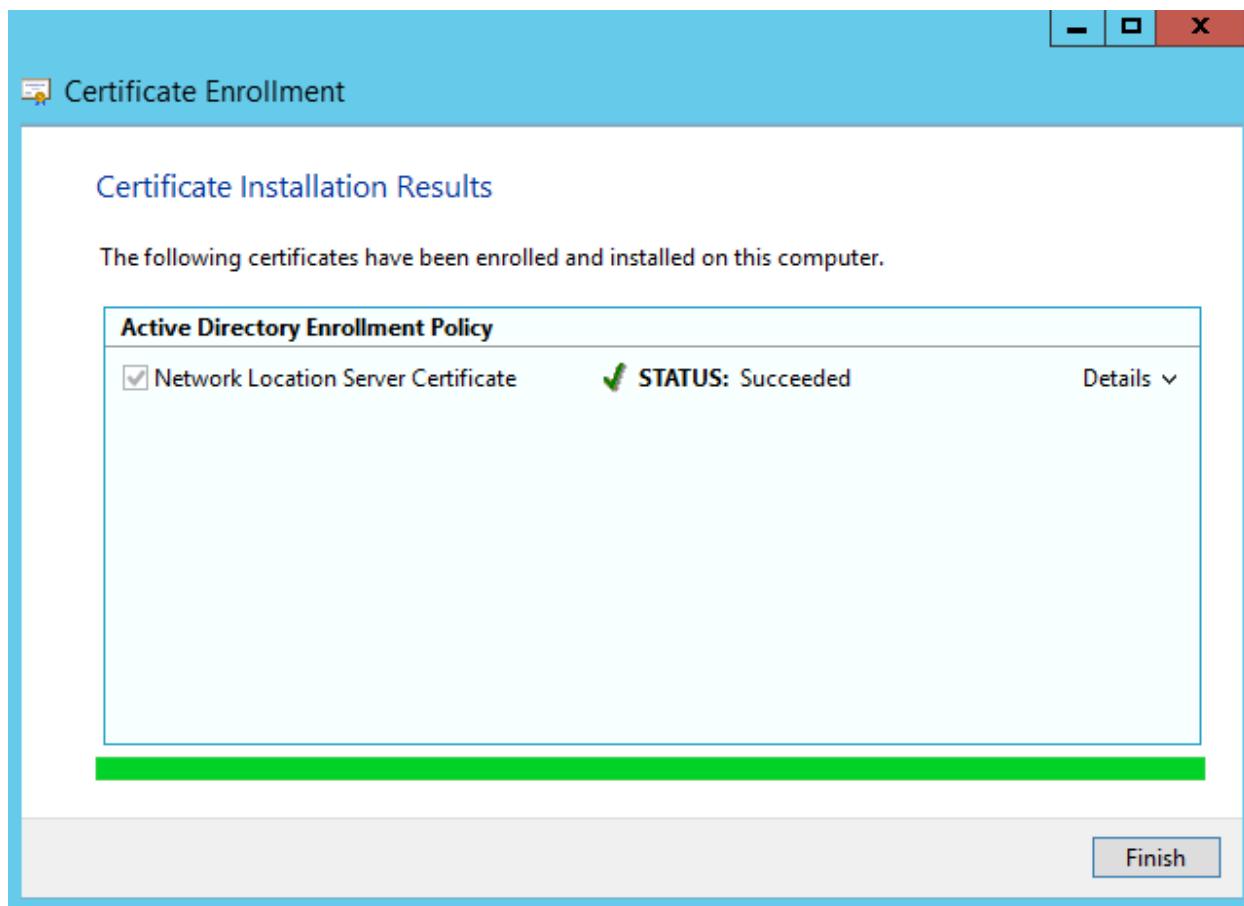
- Trong khung Type, chọn **Common Name**, trong khung Value , nhập IP của card bên ngoài là **123.1.1.1**, click vào **Add**, sau đó nhấn **OK** để xác nhận thông tin *Certificate*.



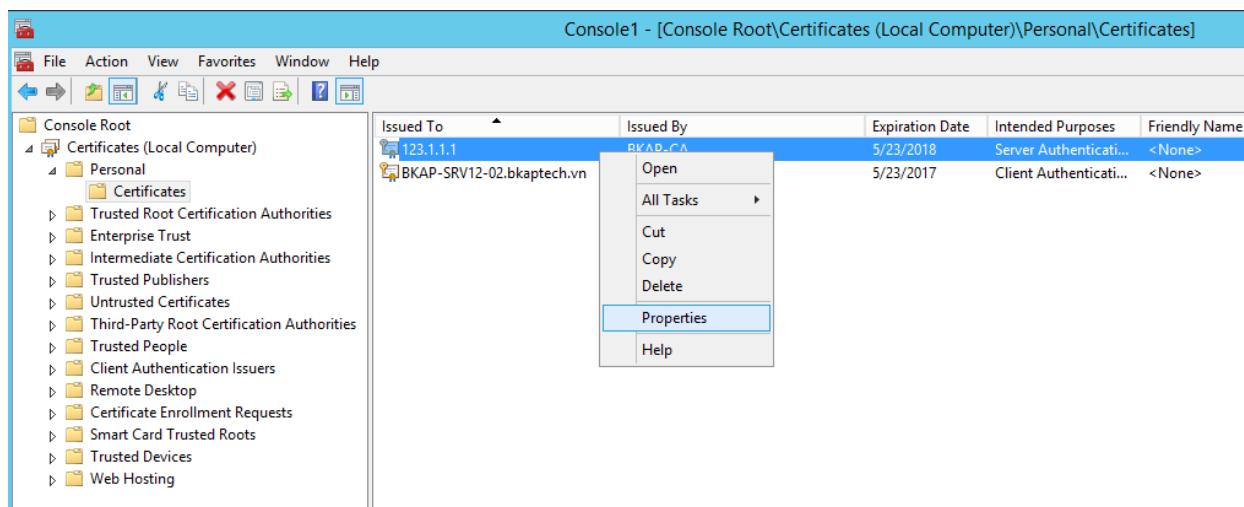
- Click nút **Enroll**.

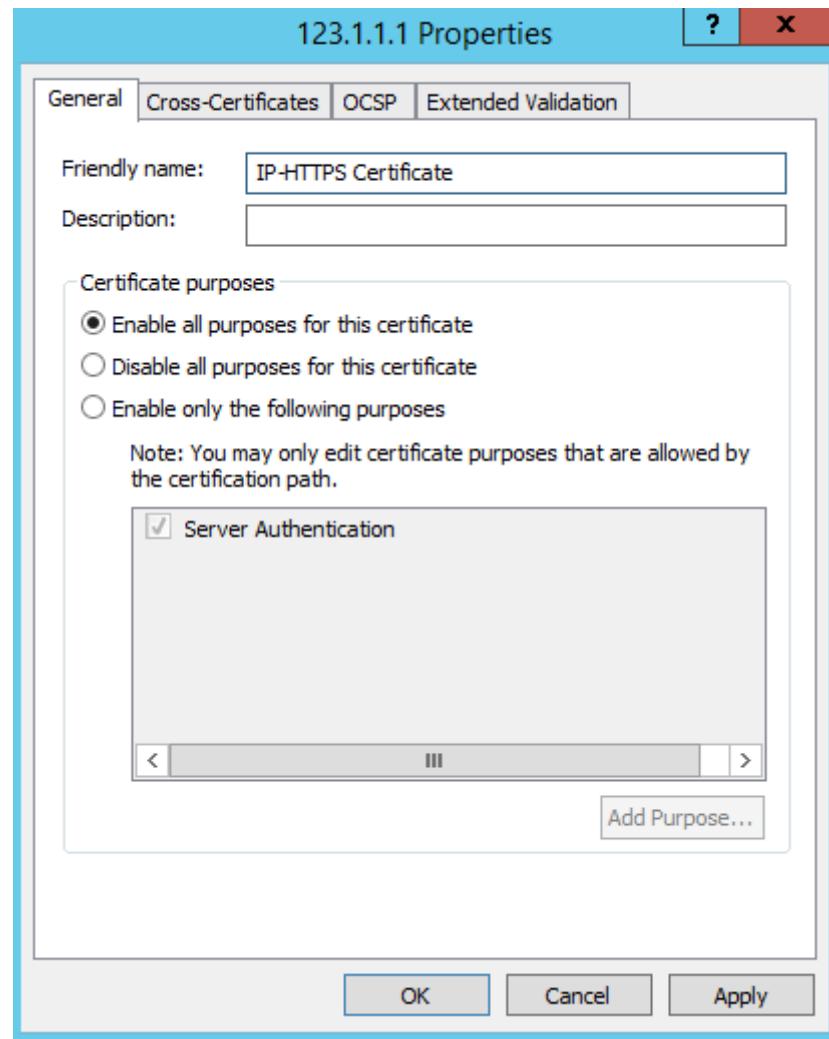


- Kiểm tra kết quả xin *Certificate* thành công và nhấn nút *Finish*.

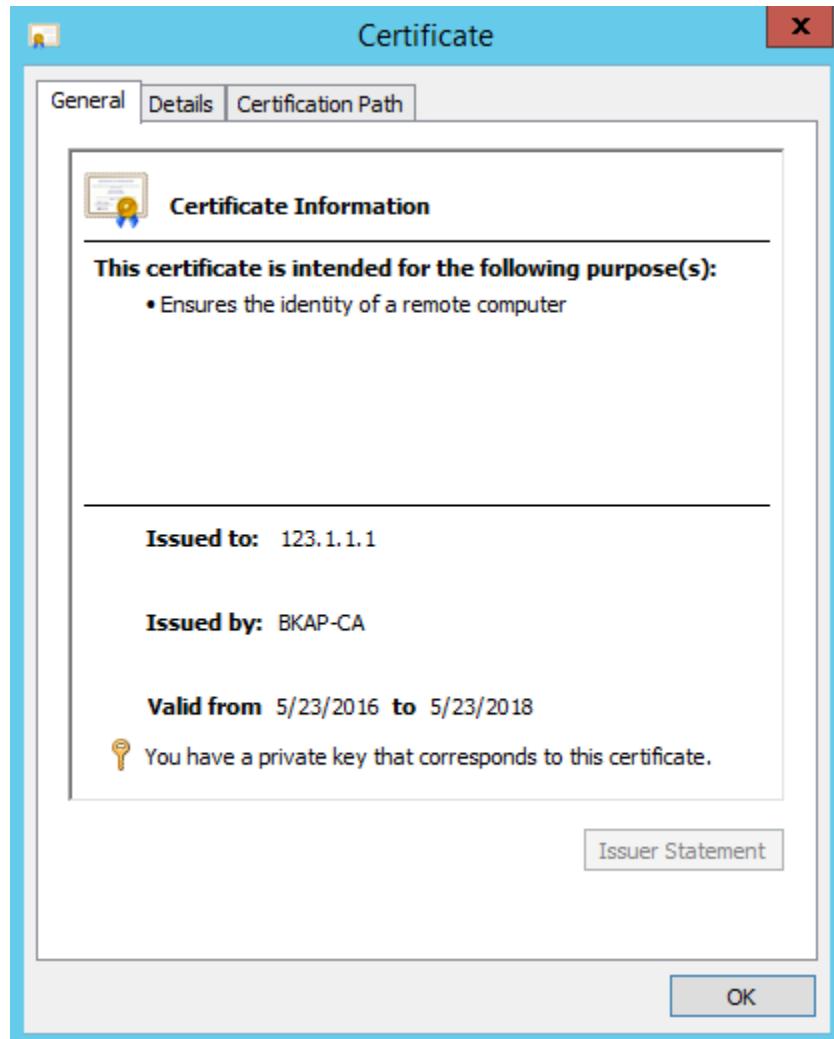


- Đặt *Friendly Name* cho *Certificate* mới là **IP-HTTPS Certificate**.

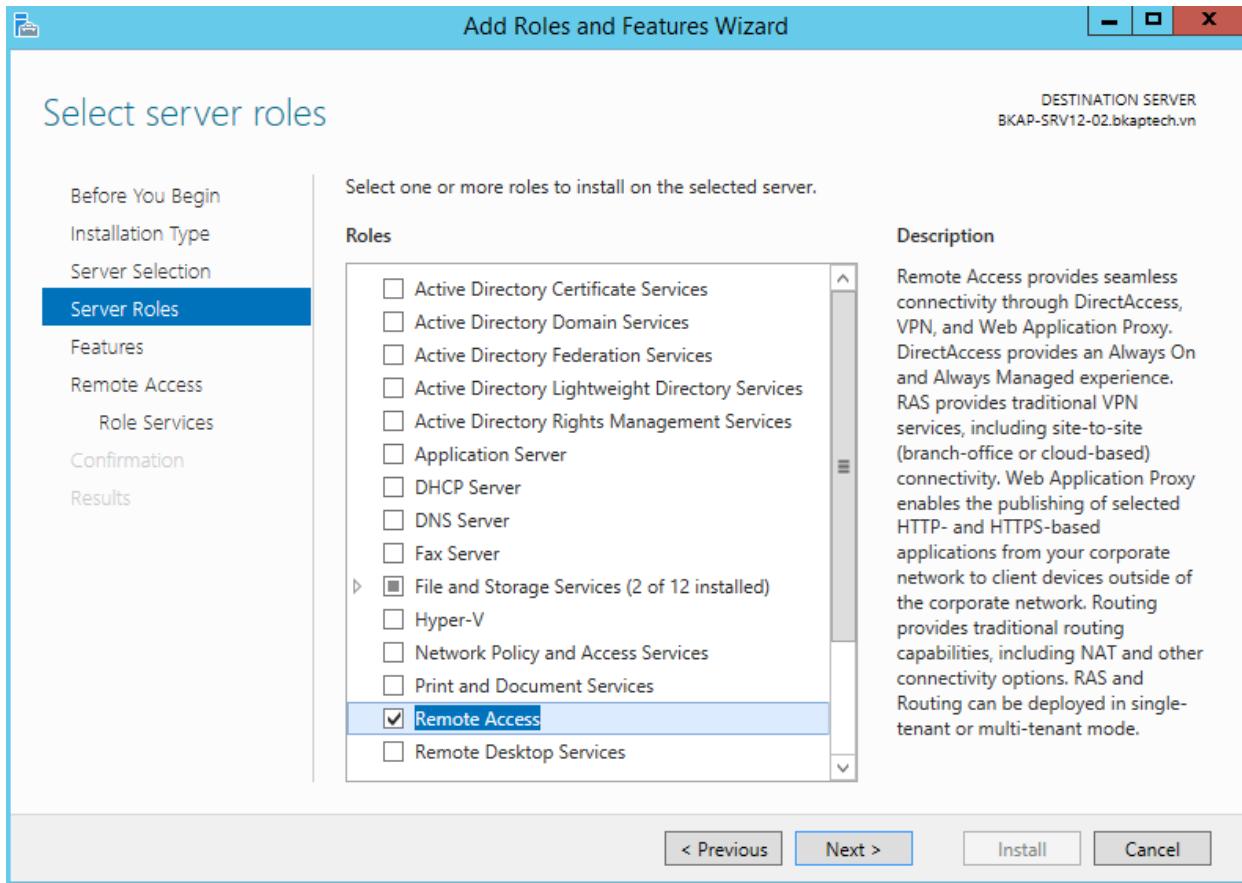


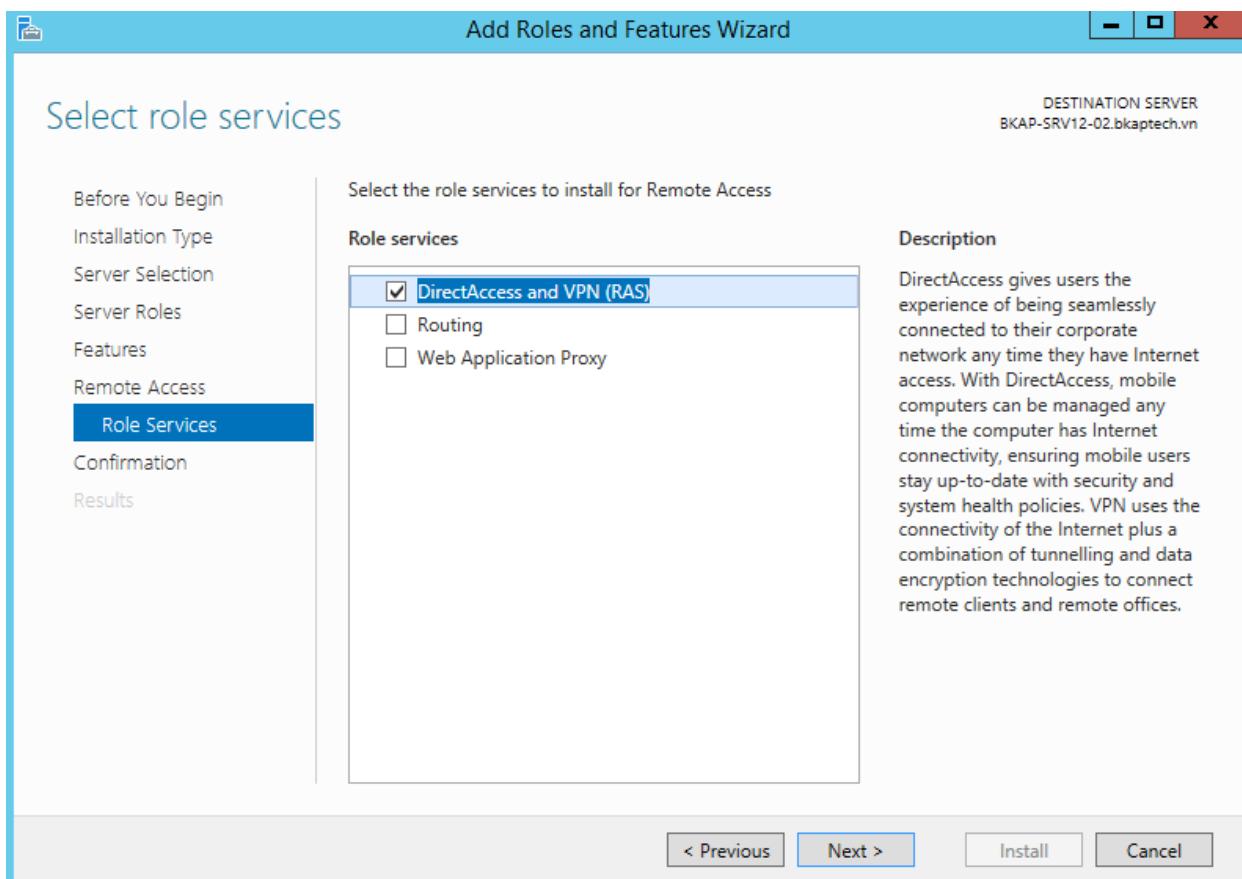


- Kiểm tra thông tin *Certificate*.

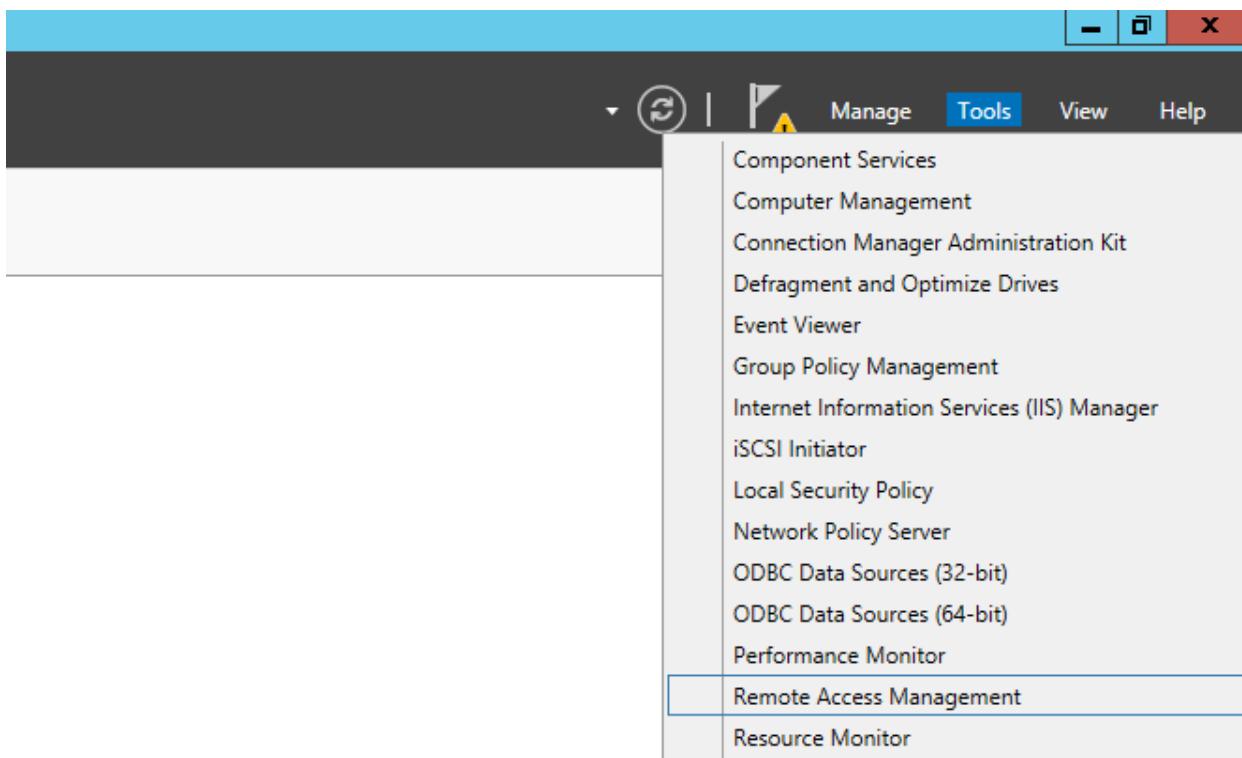


- Cài đặt Role **Remote Access** để có thể đảm nhận chức năng **Direct Access Server**. Mở Server Manager tiến hành cài đặt.

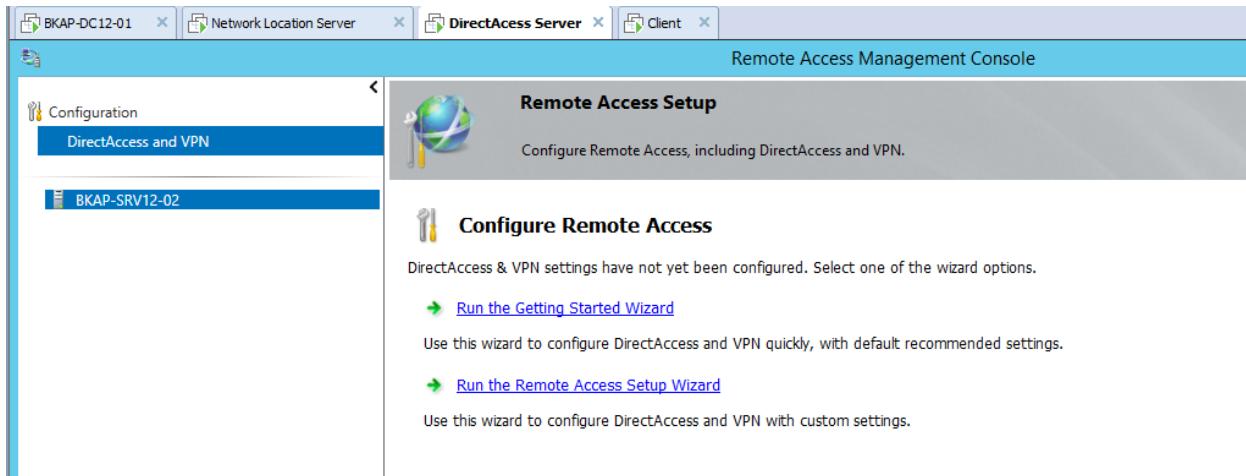




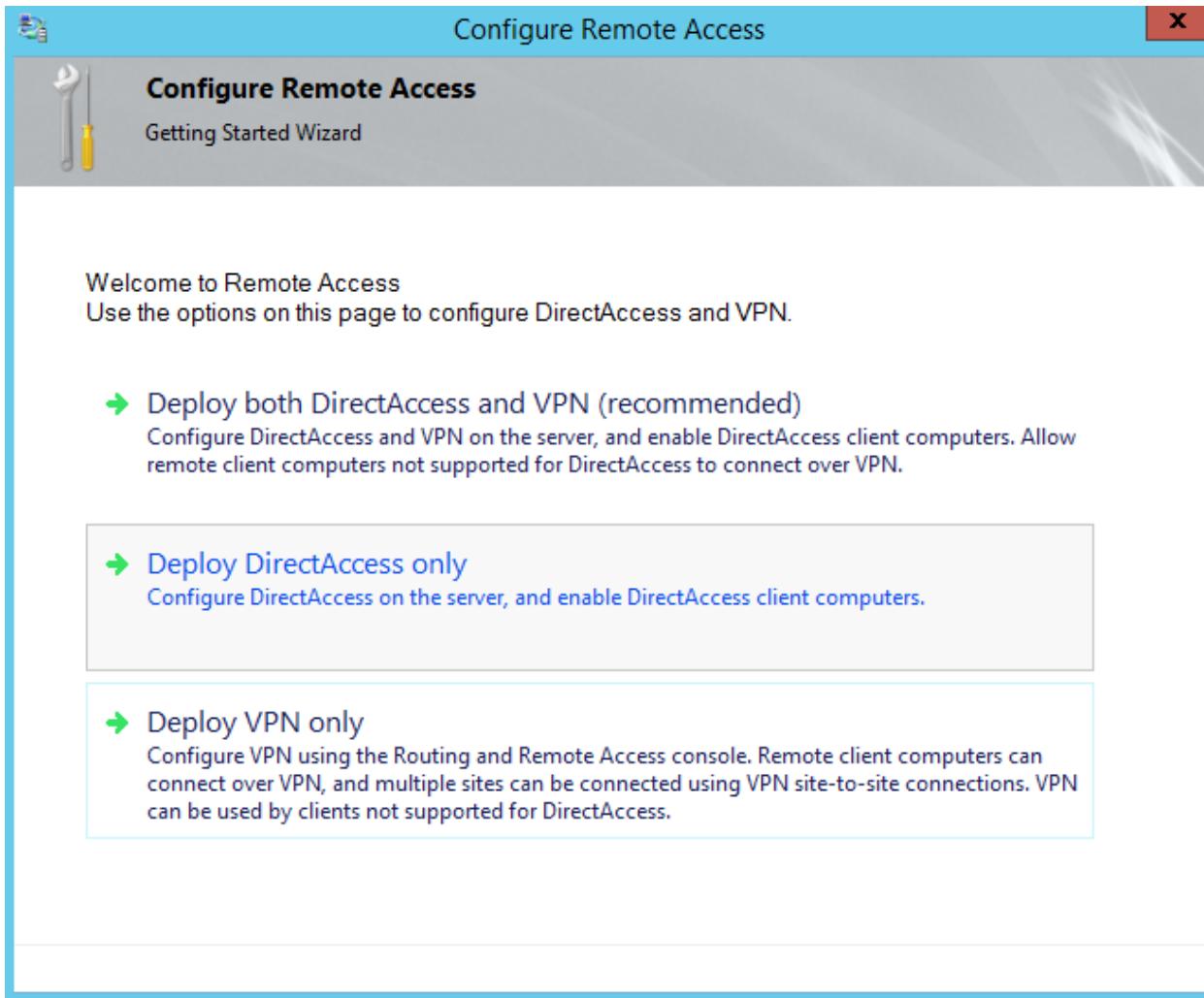
- Cấu hình *Direct Access*: Mở Tools / *Remote Access Management*.



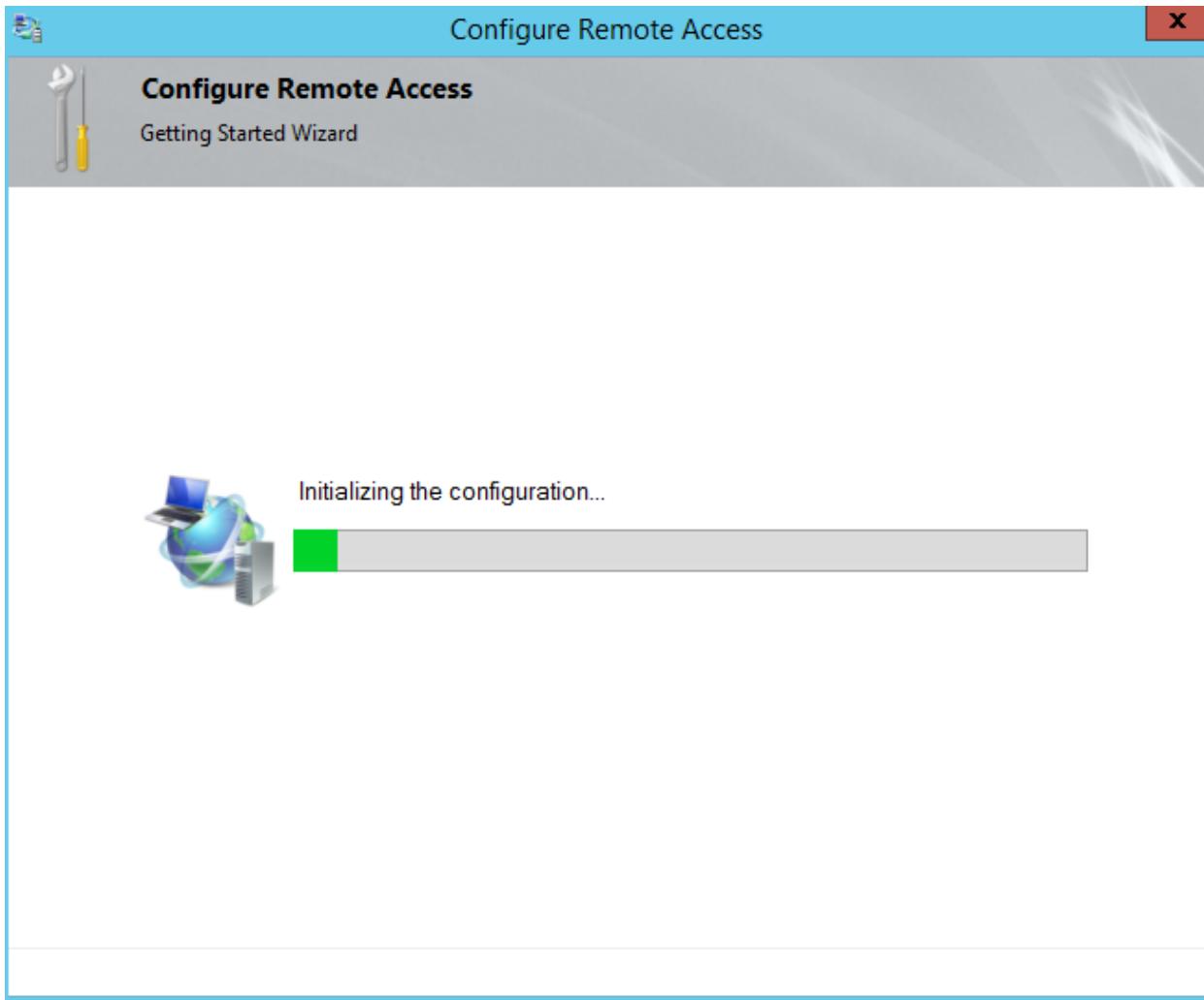
- Trong cửa sổ **Remote Access Management Console**, chạy giao diện cấu hình nhanh: Chọn *Run the Getting Started Wizard*.



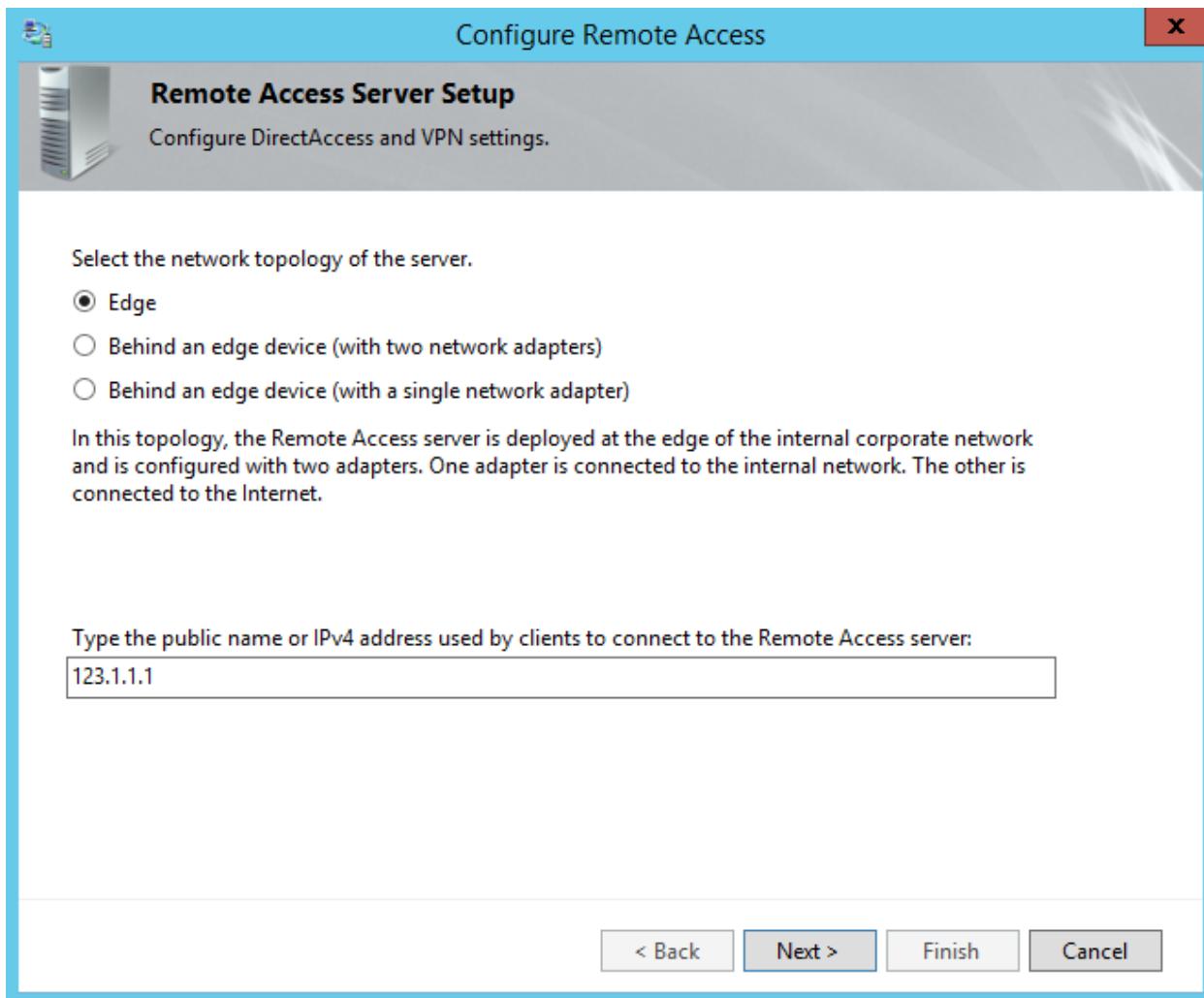
- Trong cửa sổ **Configure Remote Access**, chọn **Deploy DirectAccess Only**.



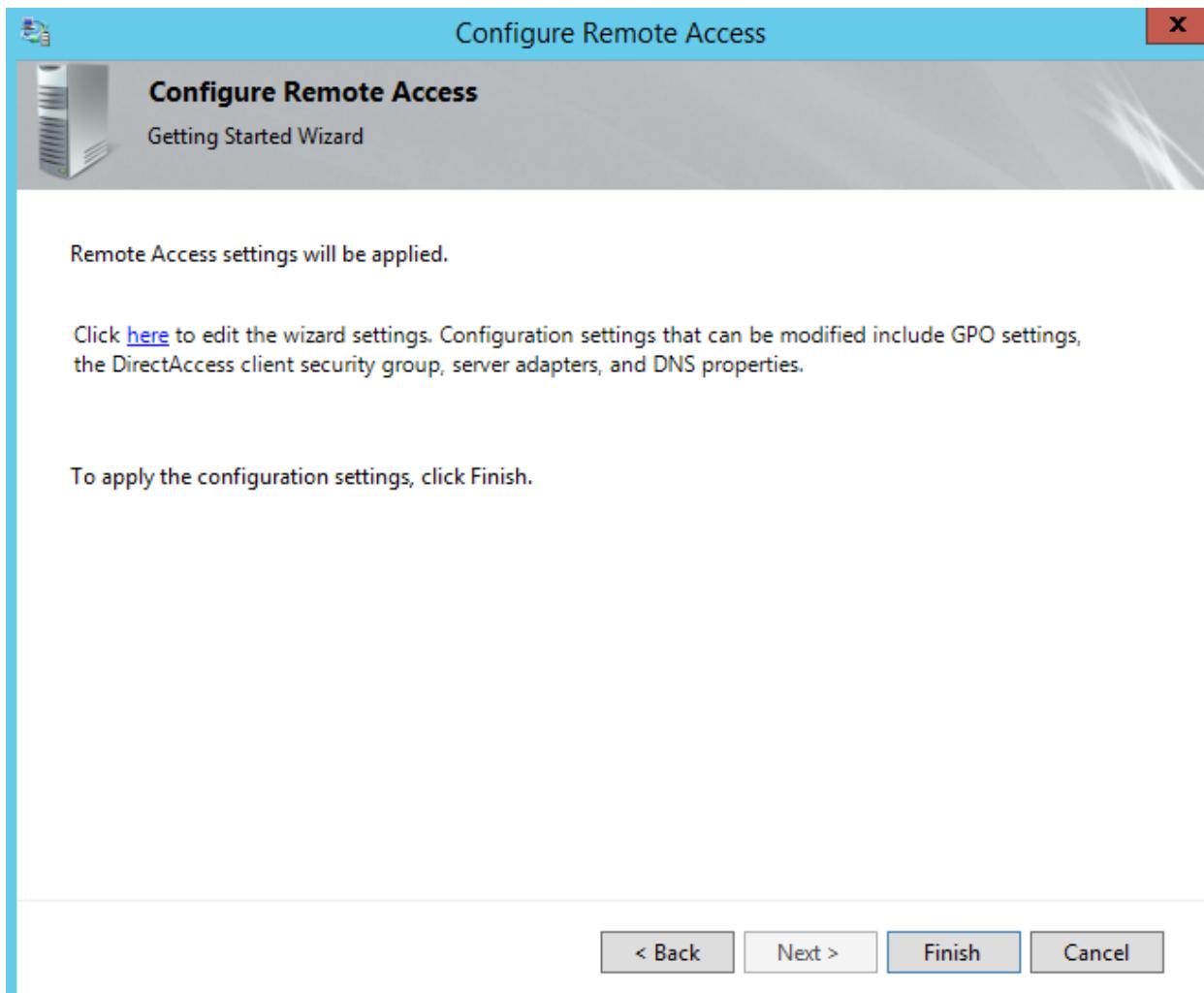
- Chờ đợi quá trình cấu hình. (*Lưu ý nếu bước này bị báo lỗi thì disable card External, sau đó Enable lại và chạy lại Getting Started Wizards.*)



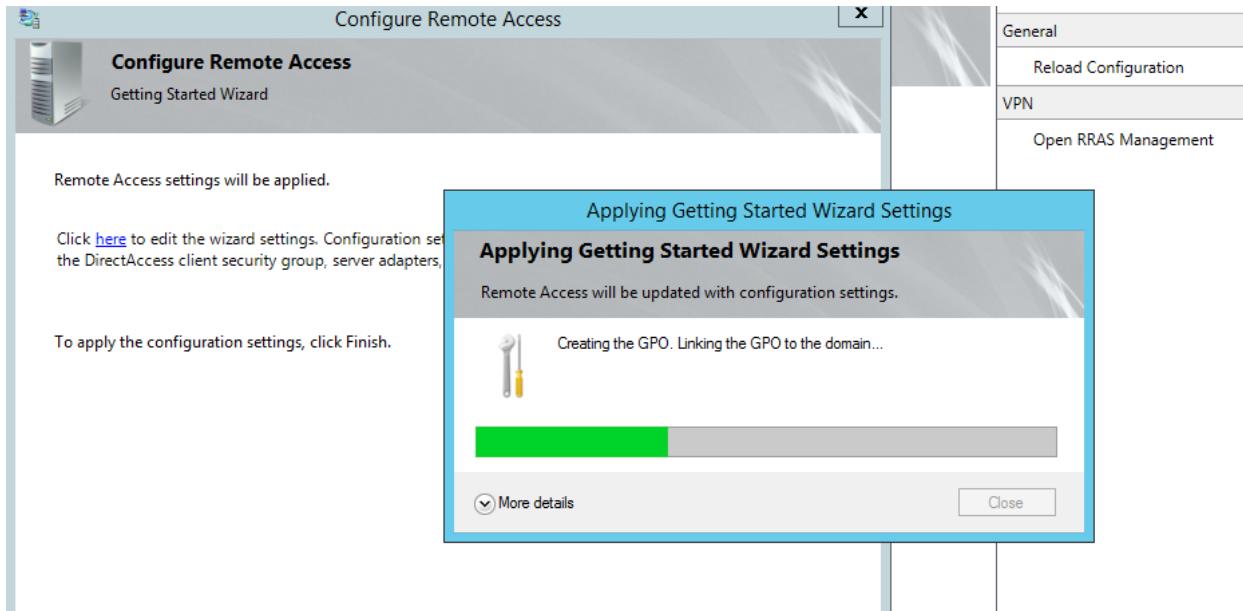
- Dịch vụ **Direct Access** hỗ trợ mô hình **Direct Access Server** nằm phía sau một *NAT Server* (**Direct Access Sever** có thể có 2 Card mạng hoặc 1 Card mạng). Trong mô hình này **Direct Access Server** không nằm sau một *NAT Server* nào nên ta chọn mô hình **Edge**, kiểm tra *IP Public* ở khung **Type the public or IPv4....**



- Nhấn nút **Finish** để hoàn tất cấu hình **Direct Access**.



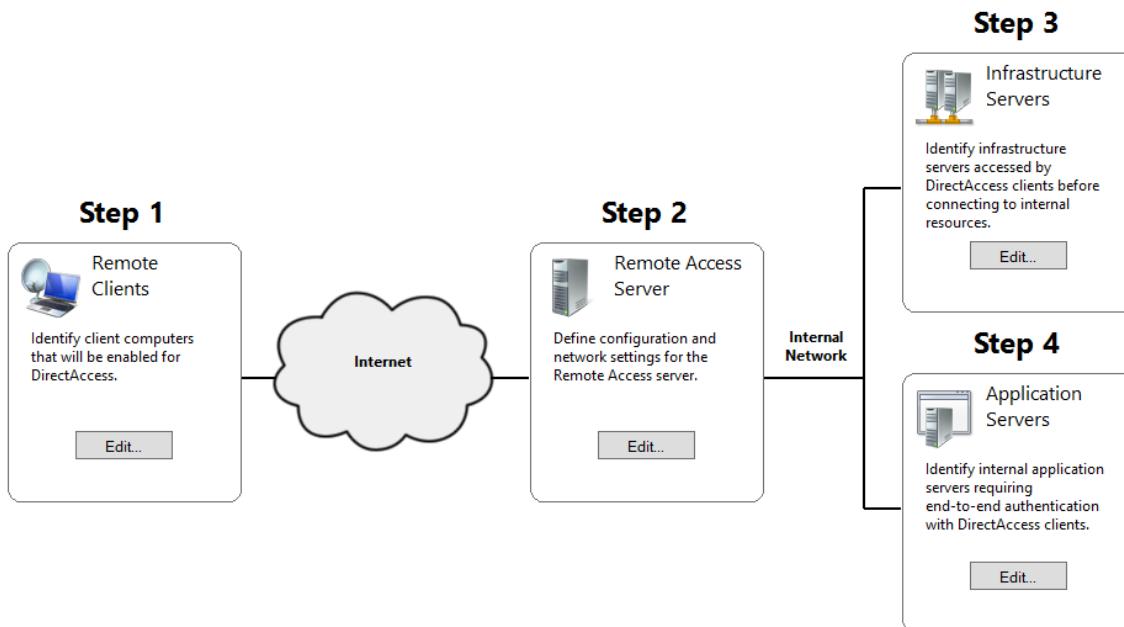
- Giao diện cấu hình này sẽ tạo **2 GPO**, chỉnh các **Policy** cần thiết là **Direct Access Server Settings** và **Direct Access Client Settings** và link **2 GPO** này vào domain. Ta chờ đợi quá trình cấu hình.



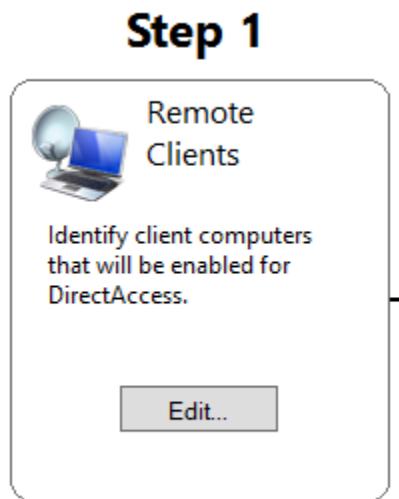
- Kiểm tra quá trình thành công và nhấn nút **Close**.



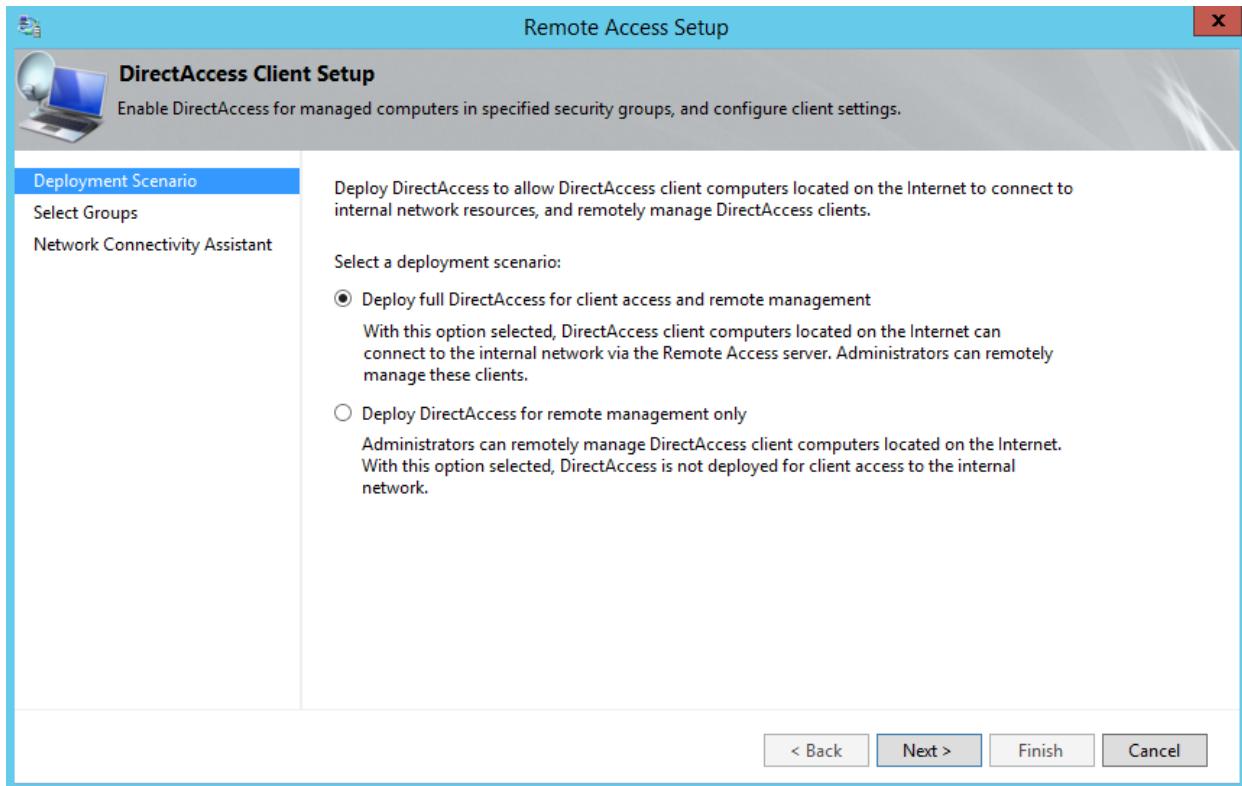
- Tiếp theo, ta cần cấu hình **Direct Access** theo 4 bước bao gồm: Cấu hình **Client**, cấu hình **Remote Access Server**, cấu hình **Infrastructure Server** và cấu hình **Application Server**.



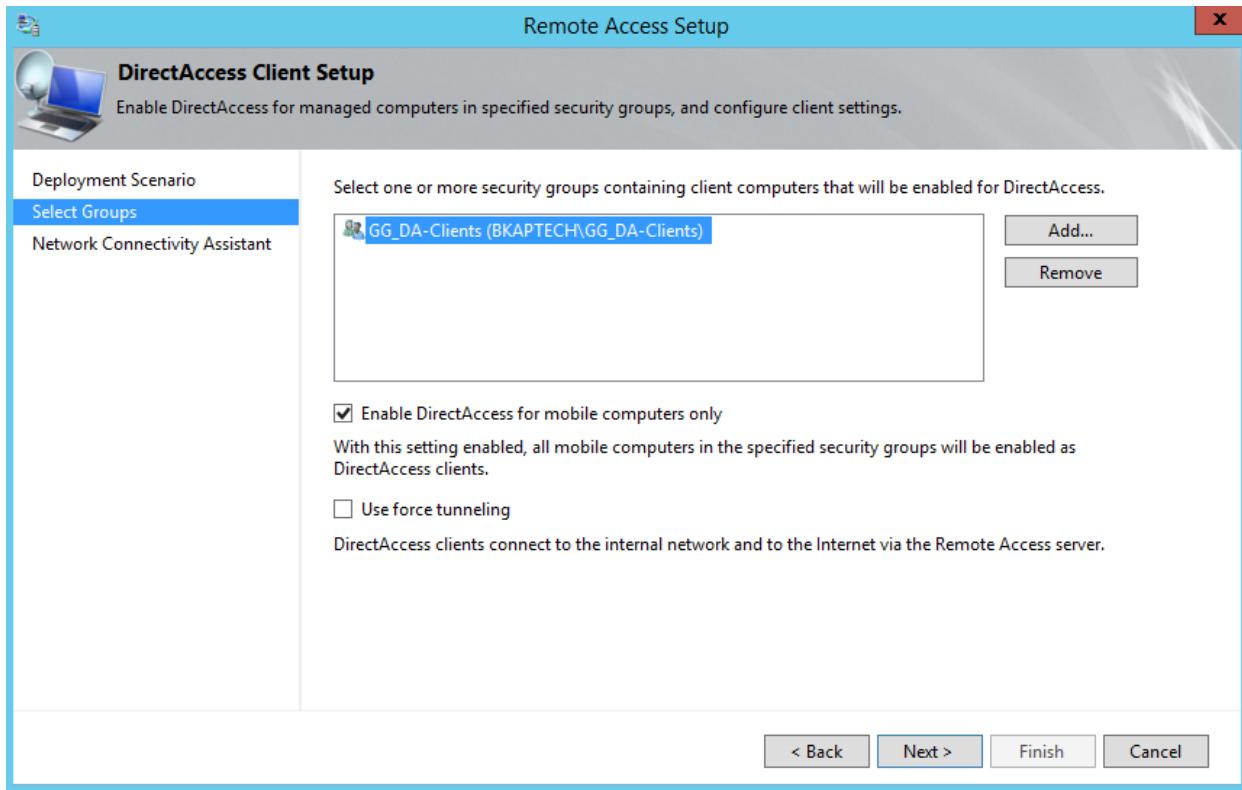
- Ta bắt đầu cấu hình **Client** bằng cách nhấn nút **Edit** trong khung **Step 1**.



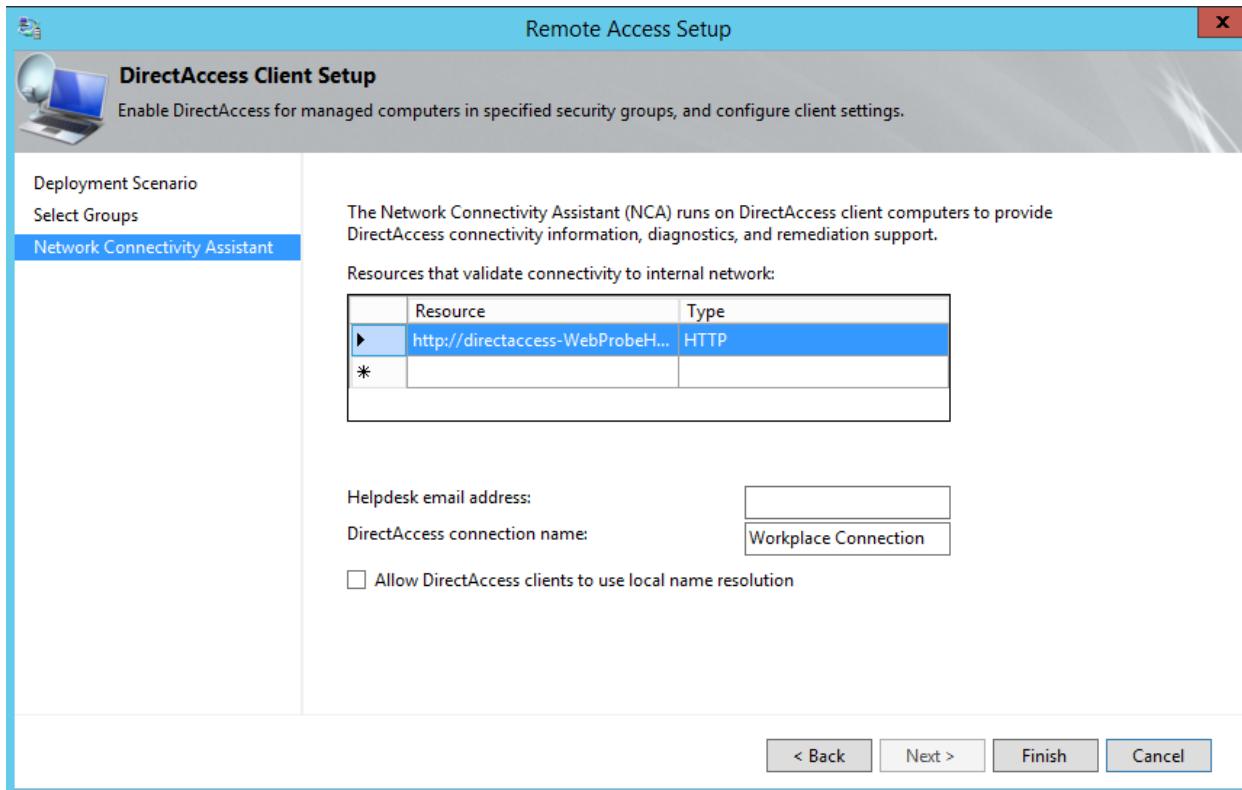
- Trong cửa sổ **DirectAccess Client Setup**, click chọn vào **Deploy full DirectAccess for client access and remote management.**



- Chỉ định các **Client** được phép kết nối **Direct Access** là các **Client** thuộc group **GG_DA-Clients** đã tạo ở trên. Ta xóa group **Domain Computer** khỏi danh sách được phép kết nối sau đó thêm group **GG_DA-Clients** vào danh sách được phép kết nối.

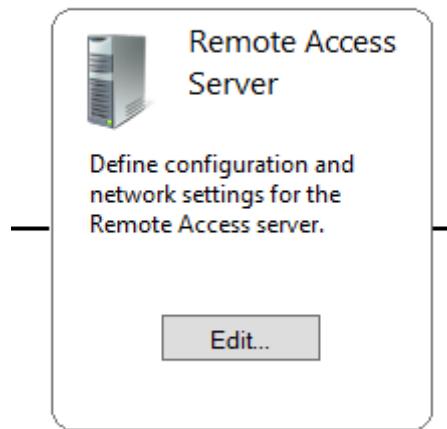


- Chấp nhận các giá trị mặc định và nhấn nút **Finish**.

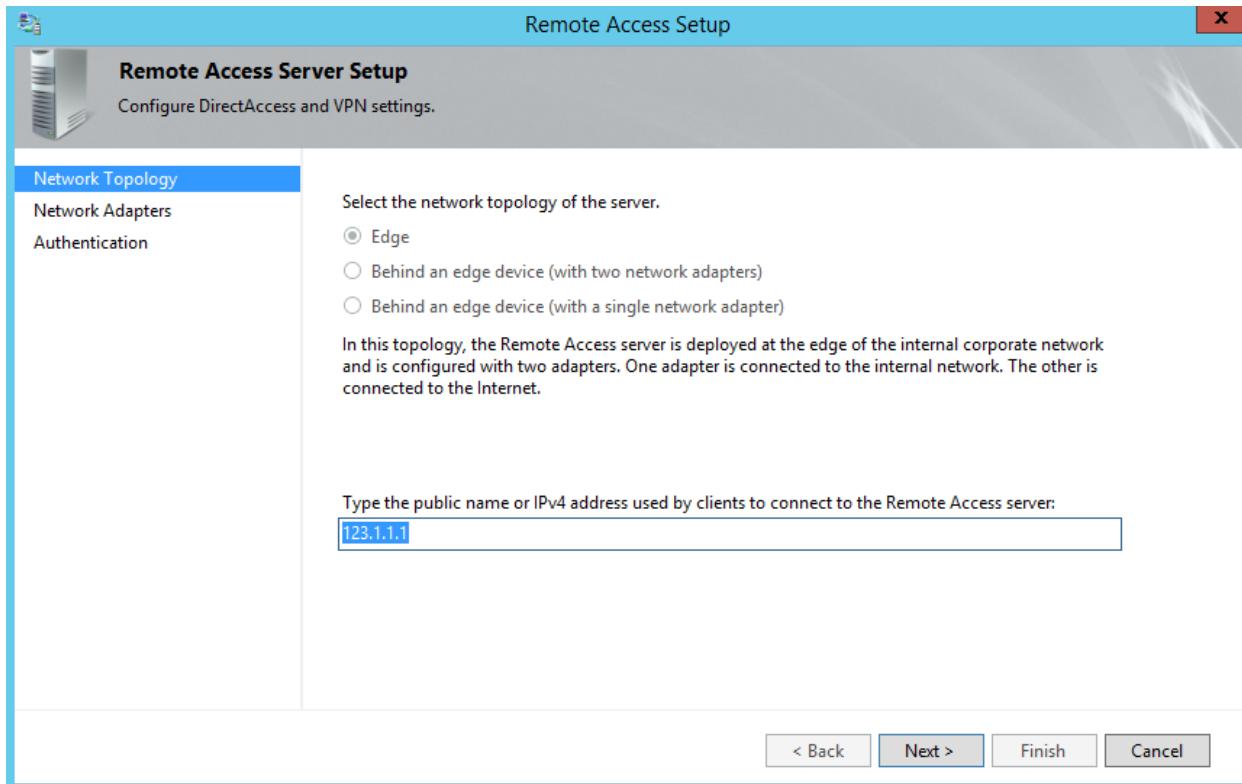


- Cấu hình Remote Access Server: Nhấn nút **Edit** trong khung Step 2.

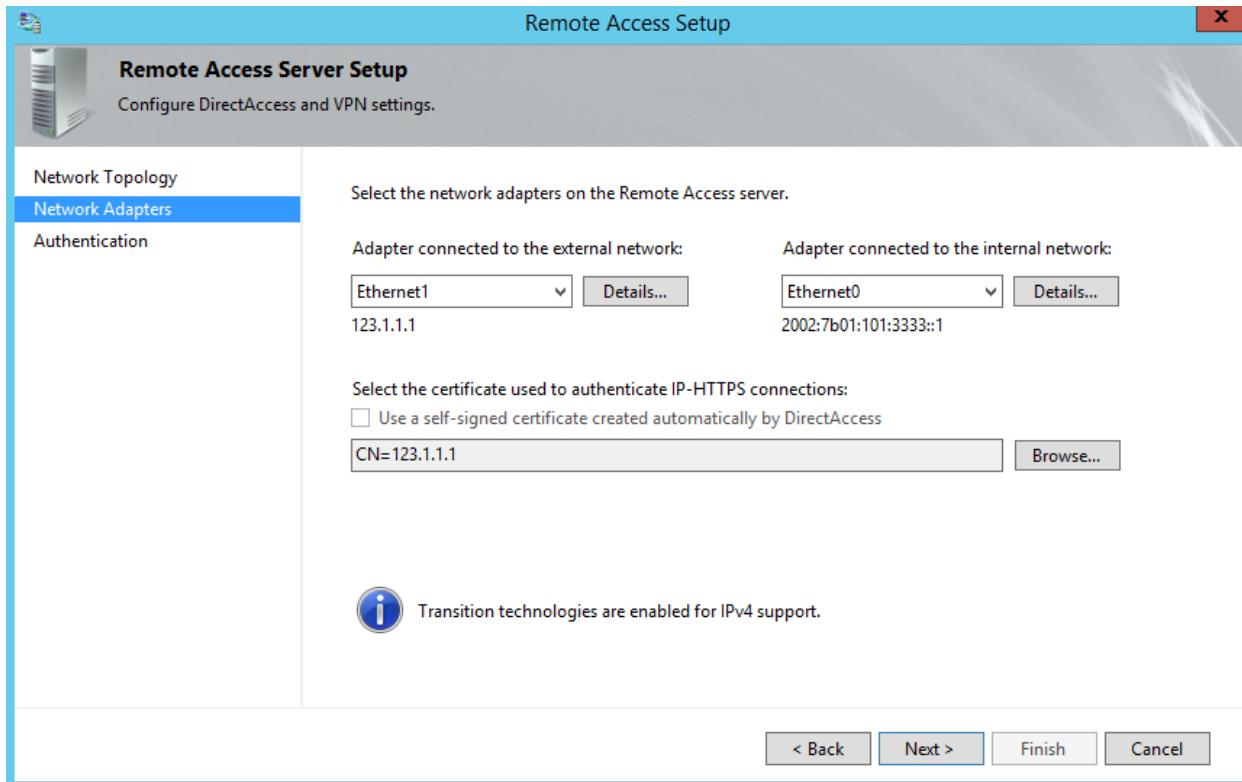
Step 2



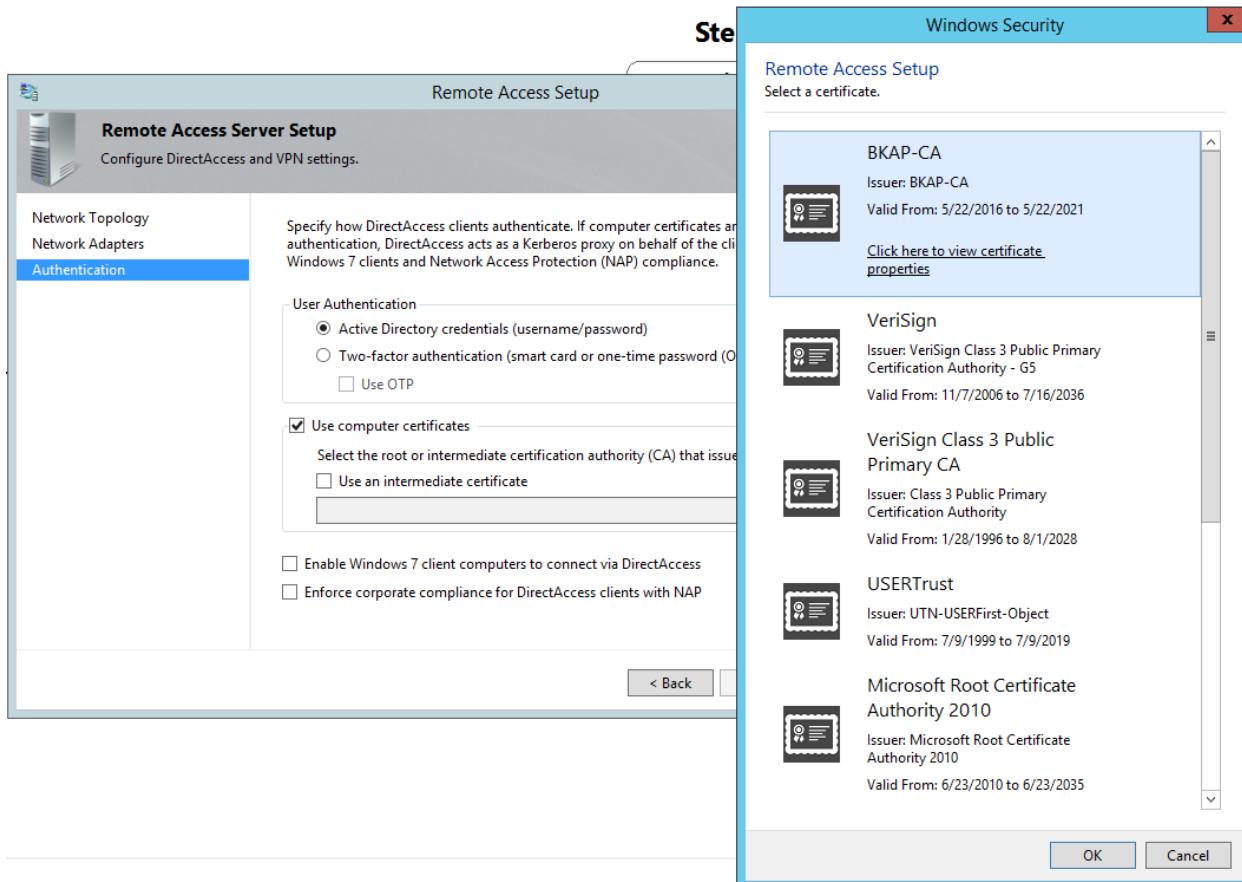
- Trong cửa sổ **Remote Access Server Setup**, kiểm tra *IP Public* của **Direct Access Server** - nhấn *Next*.



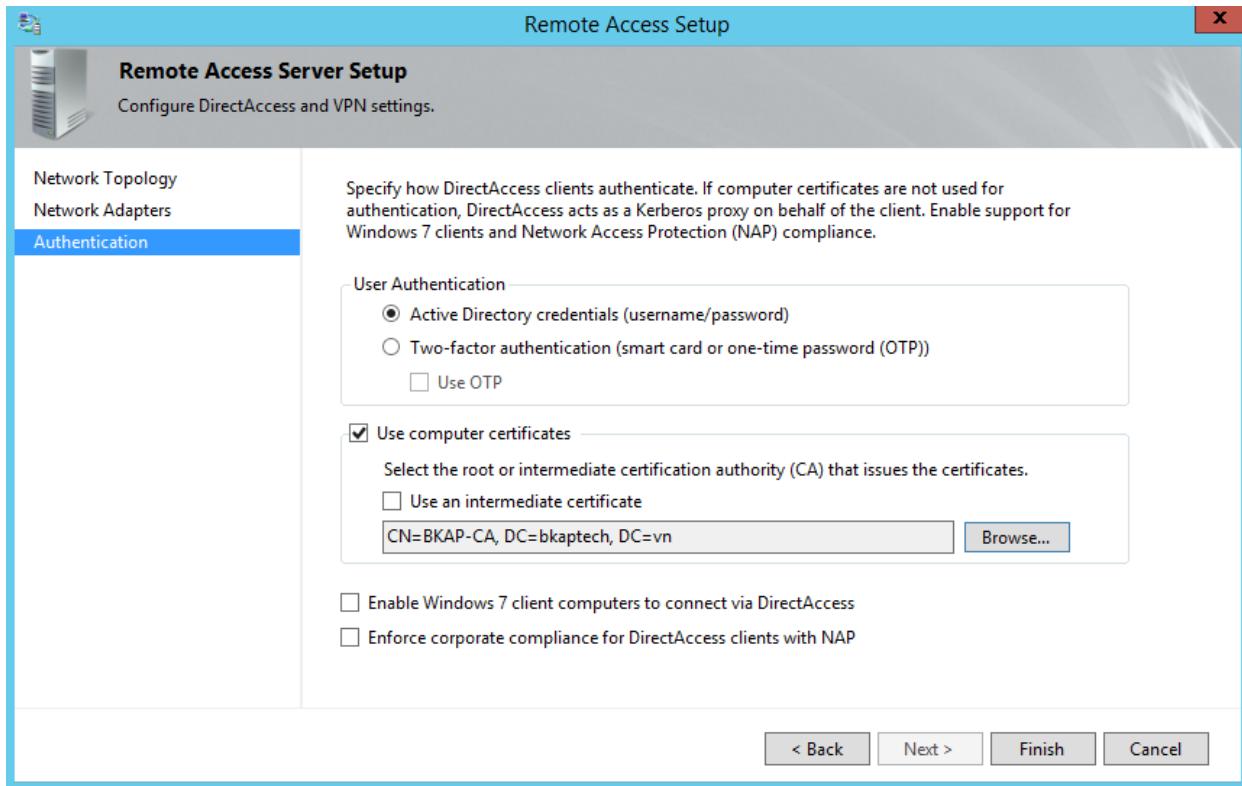
- Tại cửa sổ tiếp theo, chọn card mạng kết nối với bên ngoài là **Ethernet1**, card mạng kết nối với mạng nội bộ là **Ethernet0**.



- Tại cửa sổ tiếp theo, Chọn **Use computer certificates**, nhấn **Browse** để chọn CA Server.

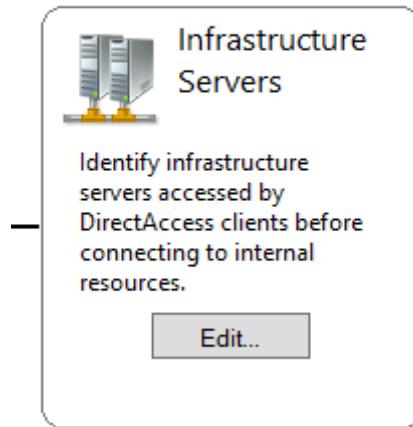


- Nhấn nút **Finish** để hoàn tất.

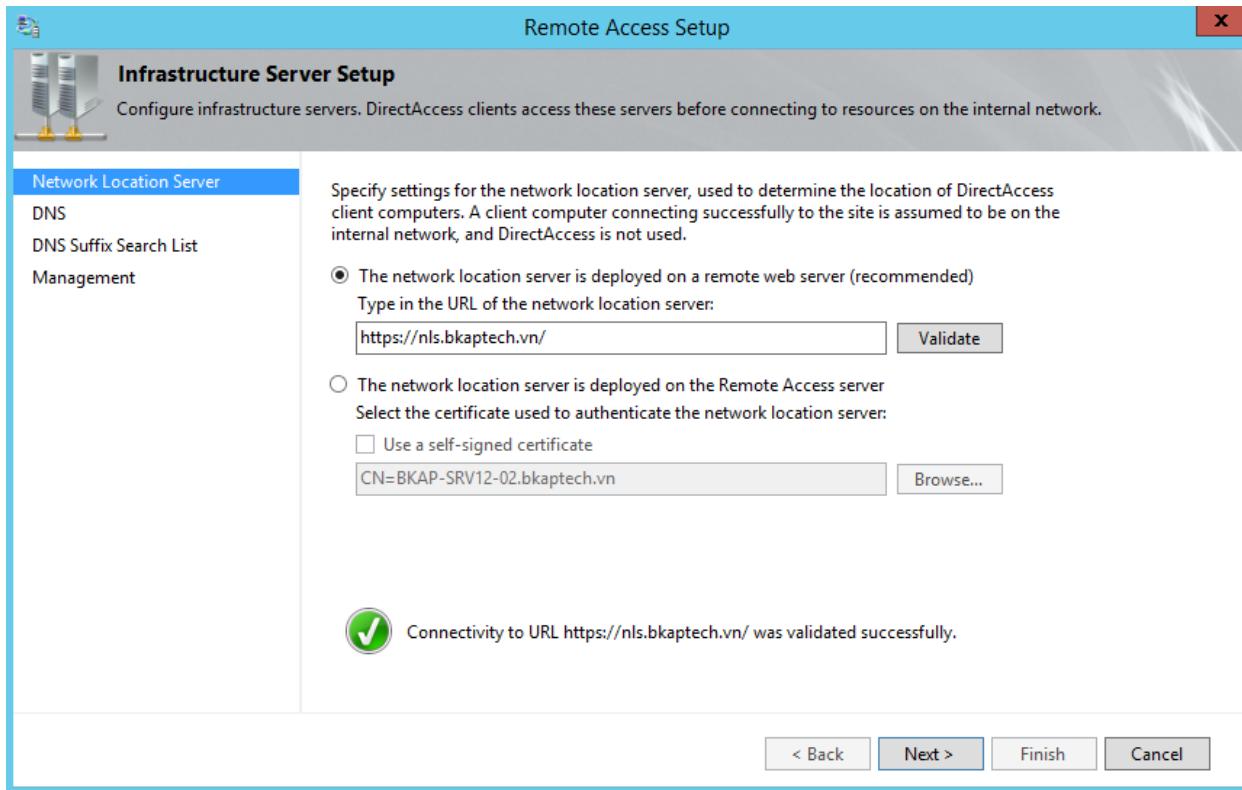


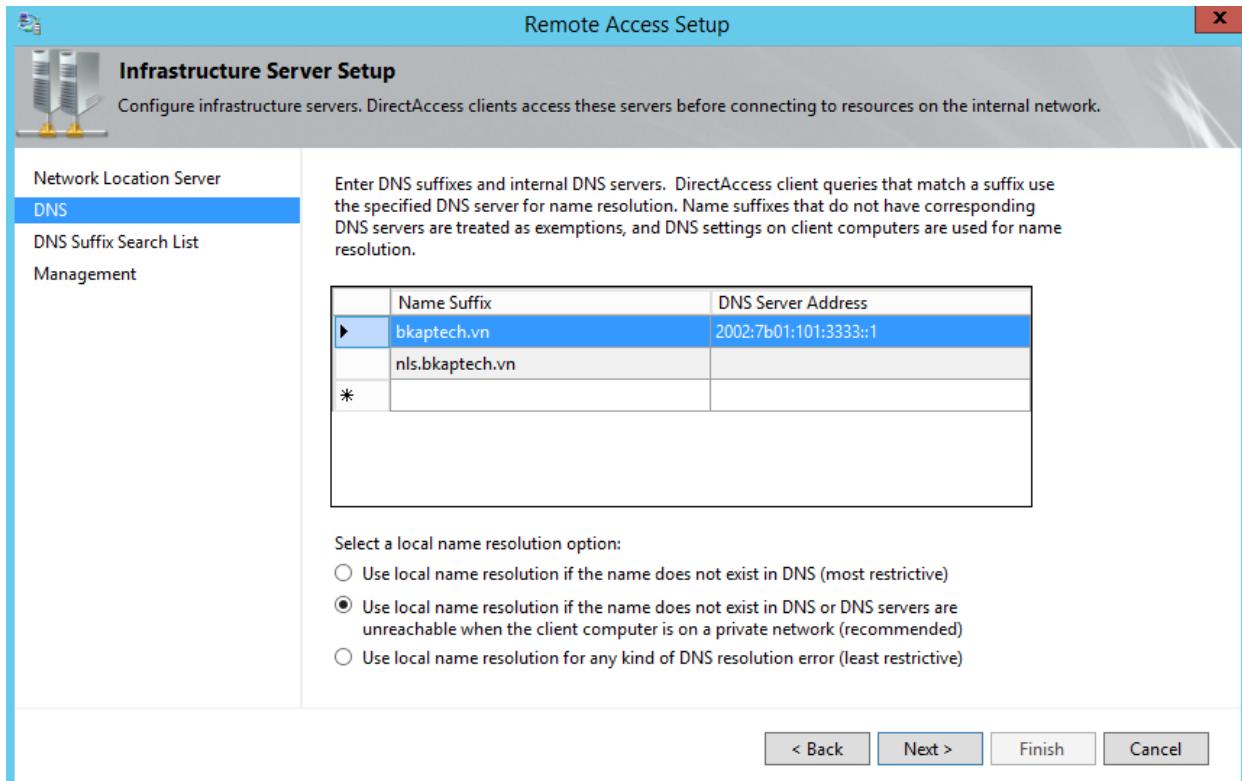
- Cấu hình **Infrastructure Server** bằng cách nhấn nút **Edit** trong khung *Step 3*.

Step 3

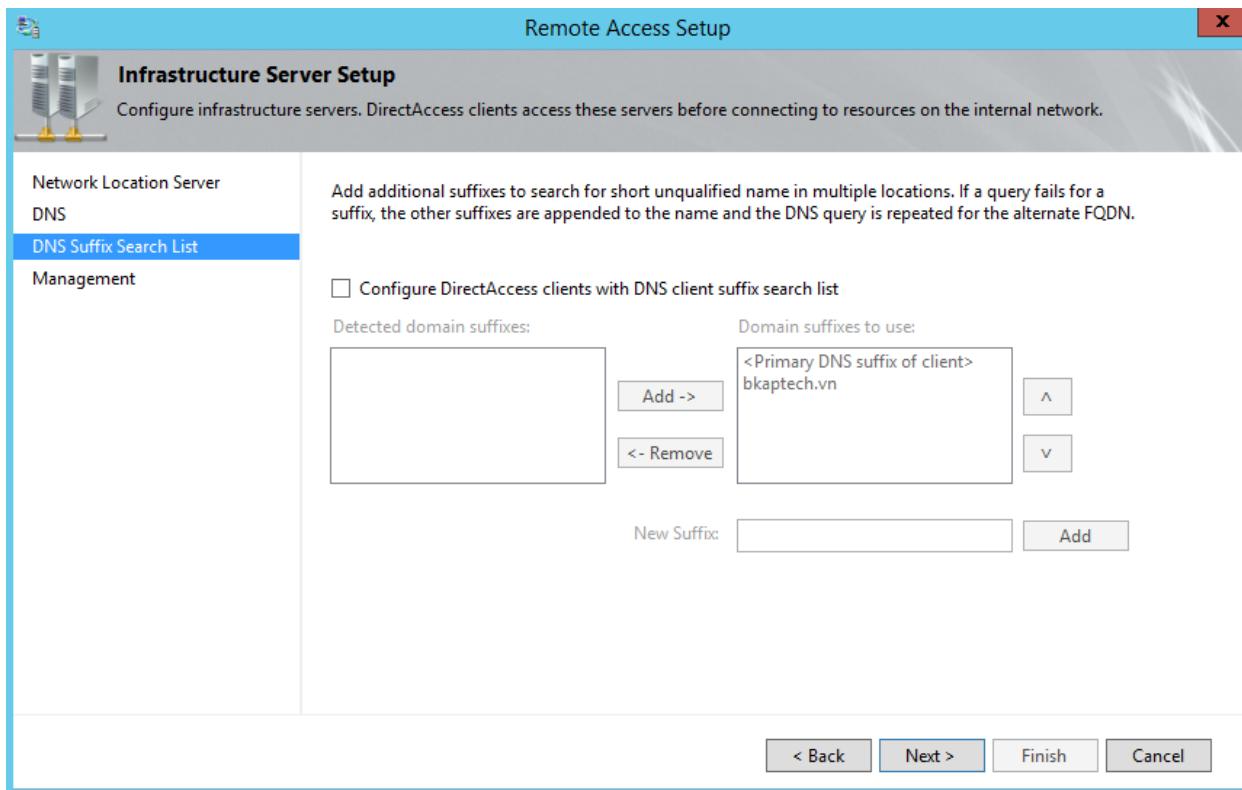


- Trong cửa sổ **Infrastructure Server Setup**, chọn vào **The network location server is deployed...**, nhập URL **httpS://NLS.bkaptech.vn**. Nhấn nút **Validate** để kiểm tra URL, kiểm tra trạng thái thành công và nhấn **Next**.

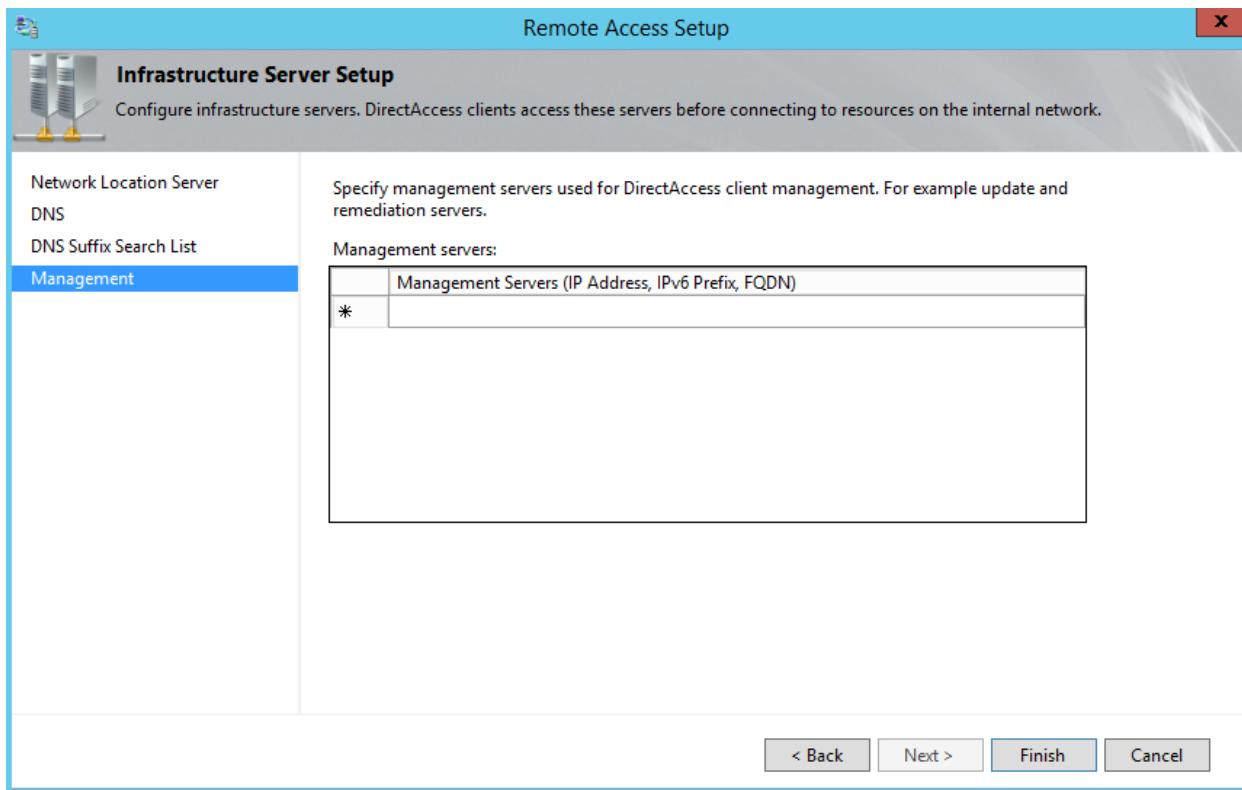


▪ Chấp nhận tên và *IPv6* của *DNS Server* - Nhấn *Next*

- Click vào Next.

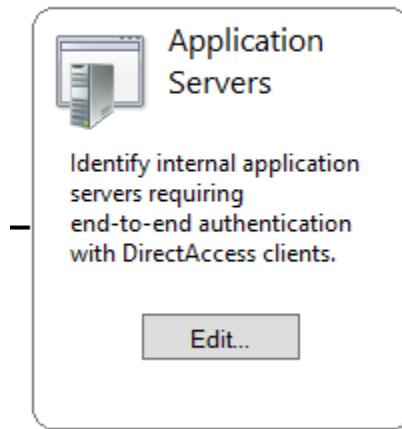


- Nhấn nút **Finish** để hoàn tất.

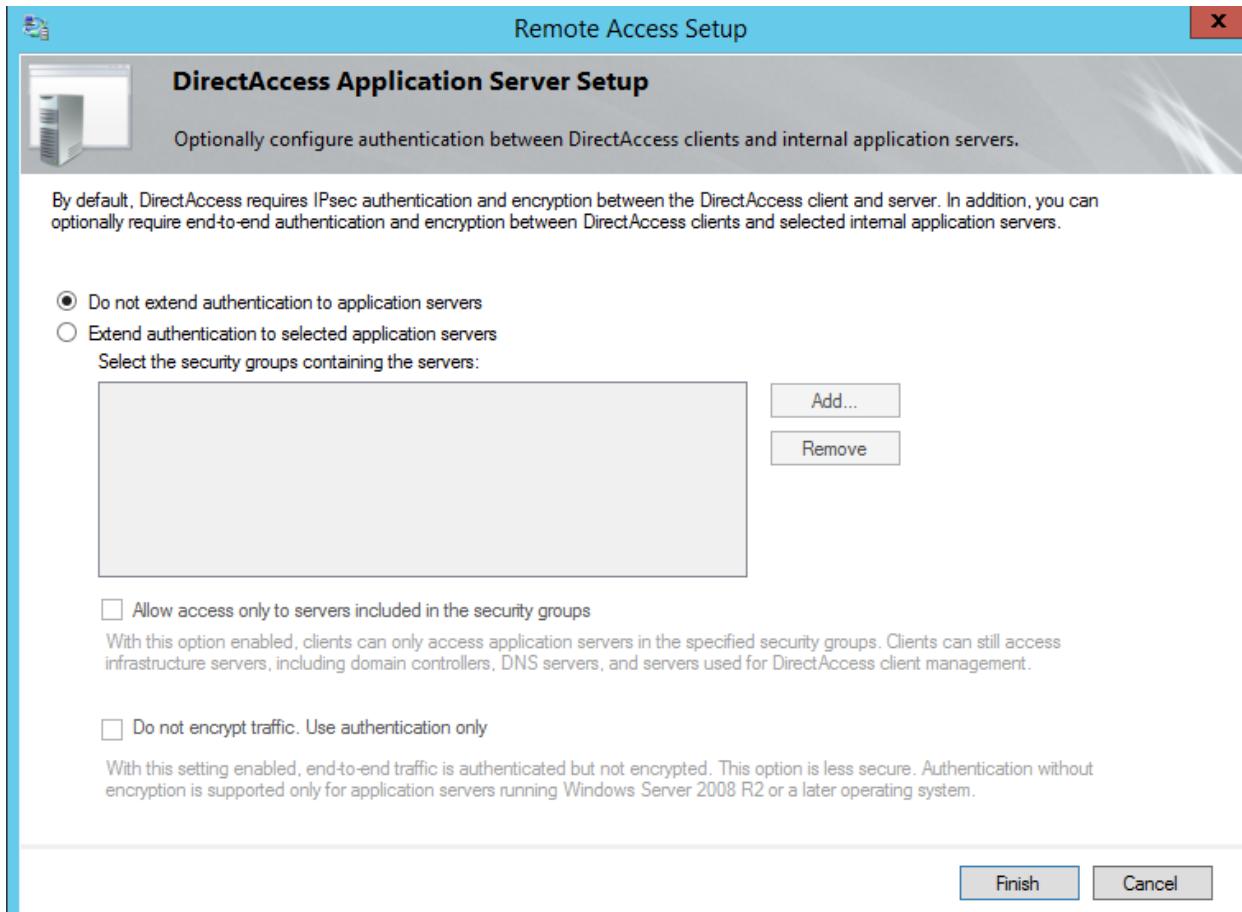


- Cấu hình **Application Server** bằng cách nhấn nút **Edit** trong khung **Step 4**.

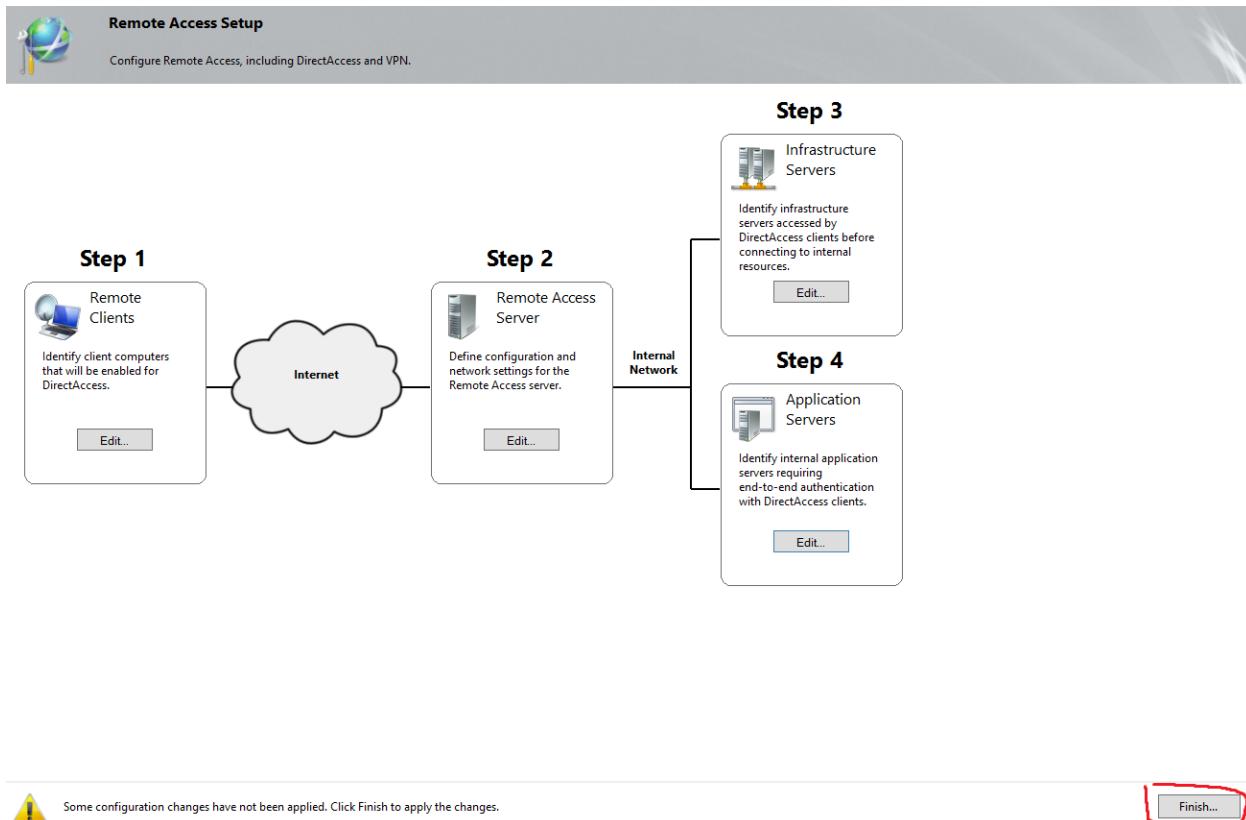
Step 4



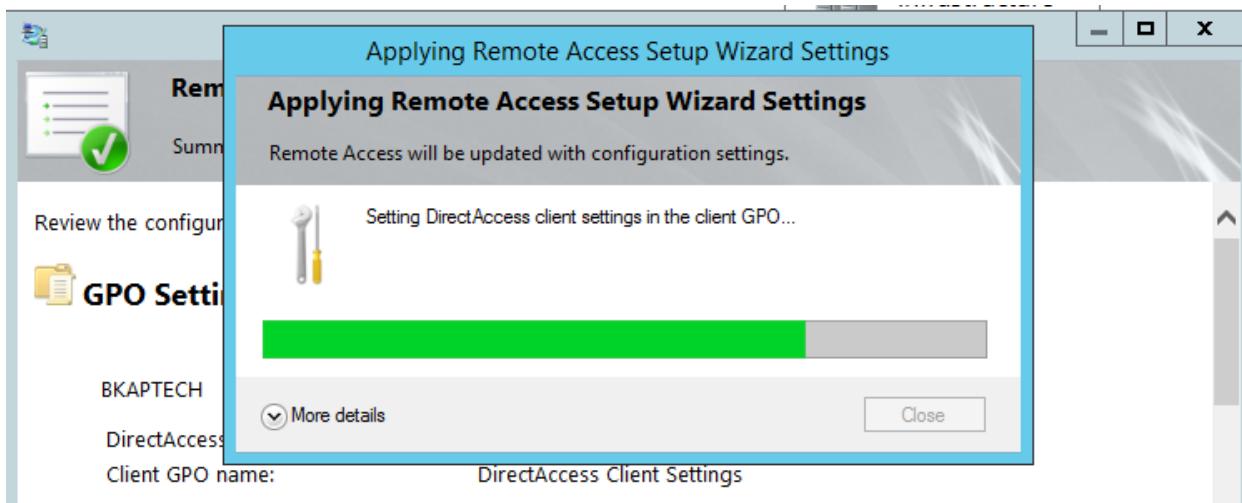
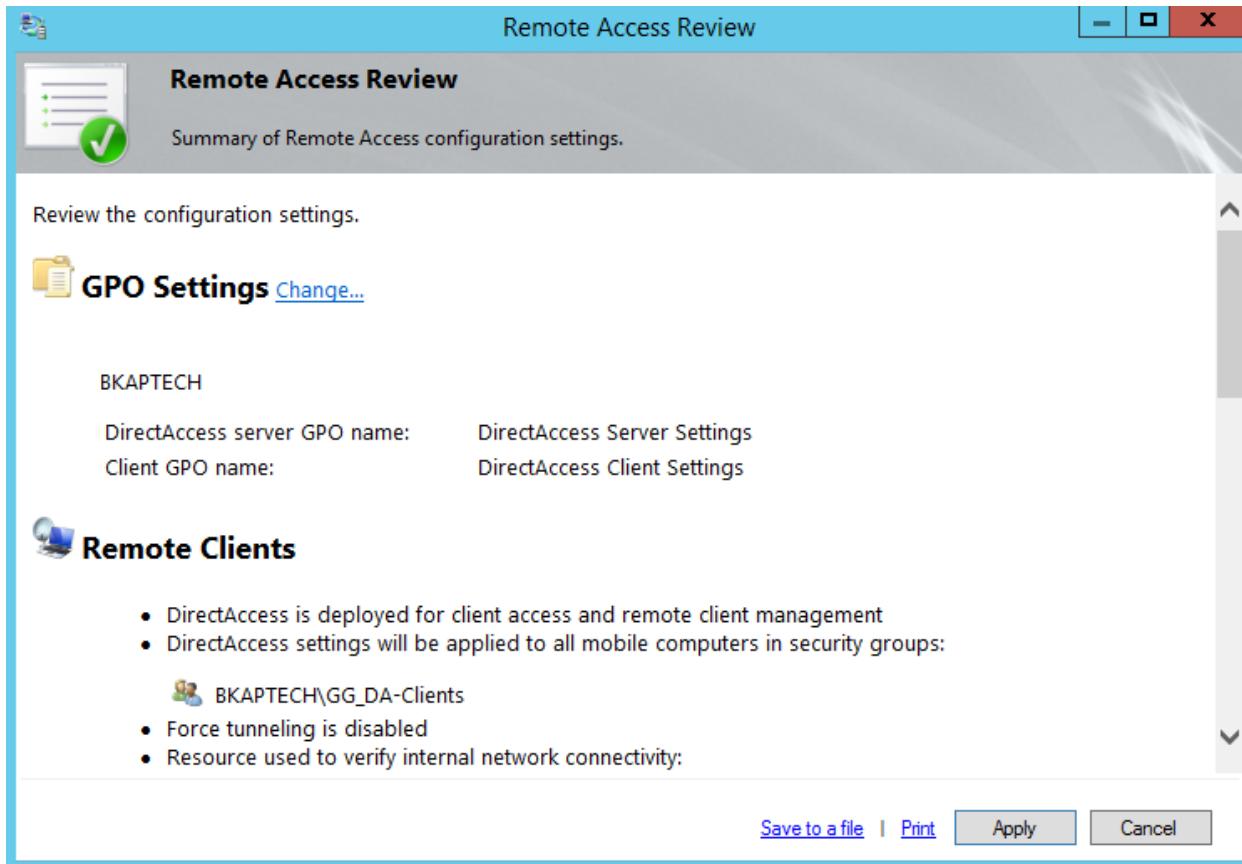
- Chấp nhận các giá trị mặc định và nhấn **Finish**.



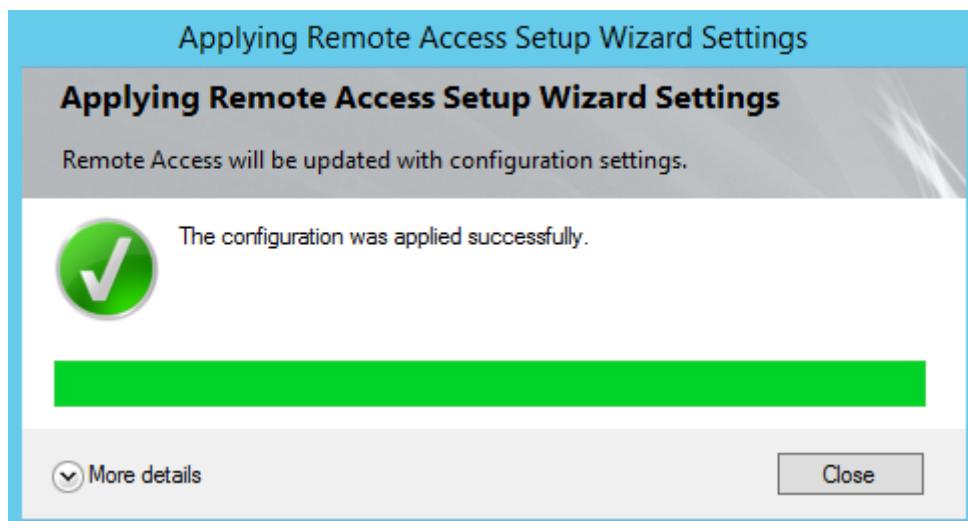
- Sau khi hoàn tất 4 bước cấu hình, bạn cần lưu lại cấu hình bằng cách nhấn nút **Finish** ở khung bên dưới.



- Nhấn nút **Apply** để xác nhận áp dụng cấu hình.



- Kiểm tra kết quả cấu hình thành công và nhấn **Close**.



- Chọn **Preration Status** để kiểm tra trạng thái hoạt động của Server. Nhấn **Refresh**.

- Kiểm tra tất cả các dịch vụ phải có biểu tượng màu xanh lá cây và status là **Working**.

Operations Status

Operations Status

Name	Status	Since
BKAP-SRV12-02.bkaptech.vn	Working	25 minutes, 22 seconds
DirectAccess	Working	25 minutes, 22 seconds
6to4	Working	30 minutes, 22 seconds
DNS	Working	25 minutes, 22 seconds
DNS64	Working	30 minutes, 22 seconds
Domain controller	Working	30 minutes, 22 seconds
IP-HTTPS	Working	30 minutes, 22 seconds
IPsec	Working	30 minutes, 22 seconds
Kerberos	Working	30 minutes, 22 seconds
NAT64	Working	30 minutes, 22 seconds
Network adapters	Working	30 minutes, 22 seconds
Network location server	Working	25 minutes, 22 seconds
Network security	Working	30 minutes, 22 seconds
Services	Working	30 minutes, 22 seconds

Details

(✓) DNS: Working properly

- Thực hiện cập nhập Policy.

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>
```

- Dùng lệnh **IPCONFIG /ALL** và khảo các các Adapter **IPv6** là **ISATAP, 6to4** và **IPHTTPS**.

```

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

Tunnel adapter isatap.{614C2F3C-1586-4E0E-A3A1-E1792B798B2A}:
  Connection-specific DNS Suffix . . . . . : Microsoft ISATAP Adapter #3
  Description . . . . . : Microsoft ISATAP Adapter #3
  Physical Address . . . . . : 00-00-00-00-00-00-E0
  DHCP Enabled. . . . . : No
  Autoconfiguration Enabled . . . . . : Yes
  Link-local IPv6 Address . . . . . : fe80::200:5efe%123.1.1.1%17(PREFERRED)
  Default Gateway . . . . . :
  DHCPv6 IAID . . . . . : 285212672
  DHCPv6 Client DUID. . . . . : 00-01-00-01-1E-C6-77-CD-00-0C-29-82-F3-77

  DNS Servers . . . . . : fec0::0:0:ffff%1
                           fec0::0:0:ffff%2
                           fec0::0:0:ffff%3

  NetBIOS over Tcpip. . . . . : Disabled

Tunnel adapter 6TO4 Adapter:
  Connection-specific DNS Suffix . . . . . : Microsoft 6to4 Adapter
  Description . . . . . : Microsoft 6to4 Adapter
  Physical Address . . . . . : 00-00-00-00-00-00-E0
  DHCP Enabled. . . . . : No
  Autoconfiguration Enabled . . . . . : Yes
  IPv6 Address. . . . . : 2002:7b01:101%1(PREFERRED)
  IPv6 Address. . . . . : 2002:7b01:101%5(PREFERRED)
  Default Gateway . . . . . :
  DHCPv6 IAID . . . . . : 503316480
  DHCPv6 Client DUID. . . . . : 00-01-00-01-1E-C6-77-CD-00-0C-29-82-F3-77

  DNS Servers . . . . . : fec0::0:0:ffff%1
                           fec0::0:0:ffff%2
                           fec0::0:0:ffff%3

  NetBIOS over Tcpip. . . . . : Disabled

Tunnel adapter IPHTTPSInterface:
  Connection-specific DNS Suffix . . . . . : Microsoft IP-HTTPS Platform Adapter
  Description . . . . . : Microsoft IP-HTTPS Platform Adapter
  Physical Address. . . . . : 00-00-00-00-00-00-E0
  DHCP Enabled. . . . . : No
  Autoconfiguration Enabled . . . . . : Yes
  IPv6 Address. . . . . : 2002:7b01:101:1000:d40:87cb:14e5:ab32(PREFERRED)
  Link-local IPv6 Address . . . . . : fe80::d40:87cb:14e5:ab32%31(PREFERRED)
  Default Gateway . . . . . :
  DHCPv6 IAID . . . . . : 520093696
  DHCPv6 Client DUID. . . . . : 00-01-00-01-1E-C6-77-CD-00-0C-29-82-F3-77

  NetBIOS over Tcpip. . . . . : Disabled

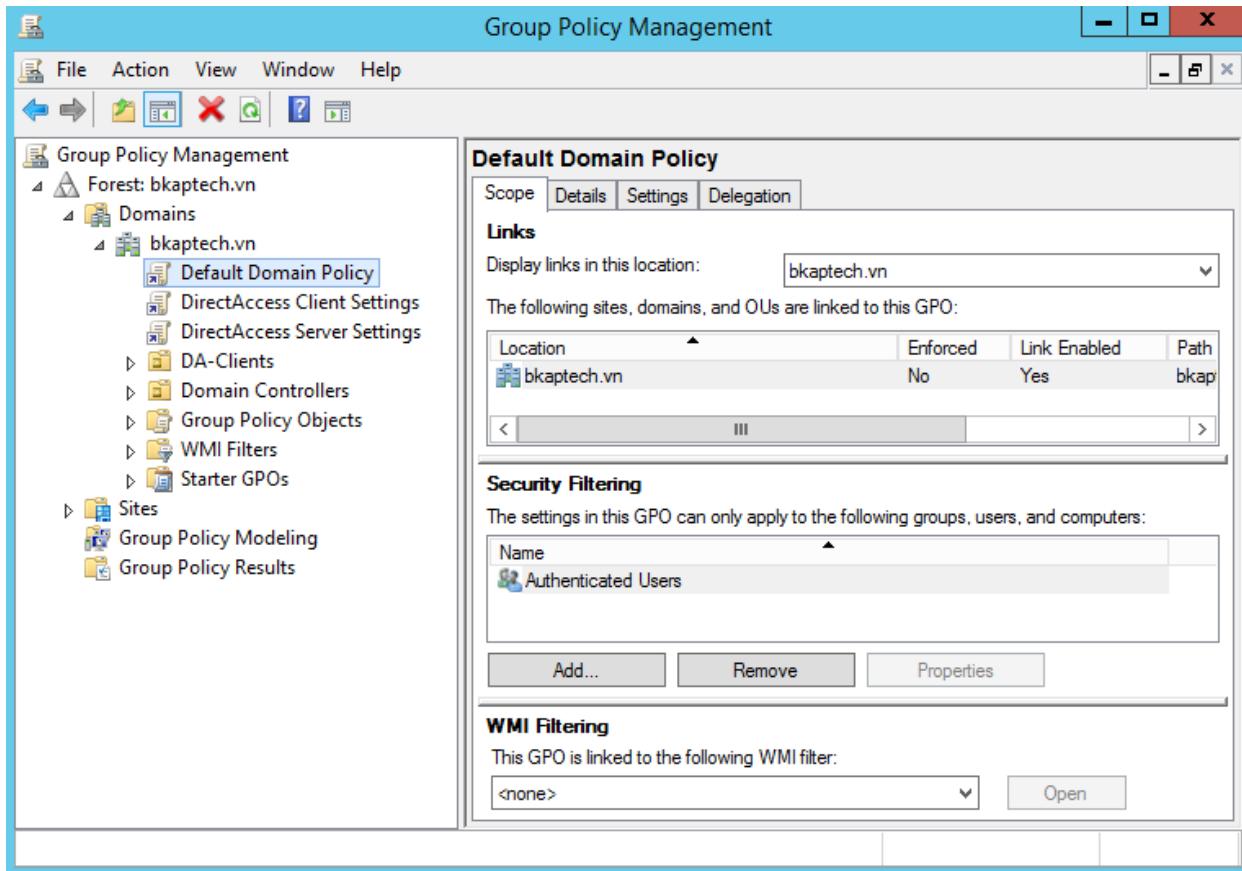
C:\Users\administrator.BKAPTECH>_

```

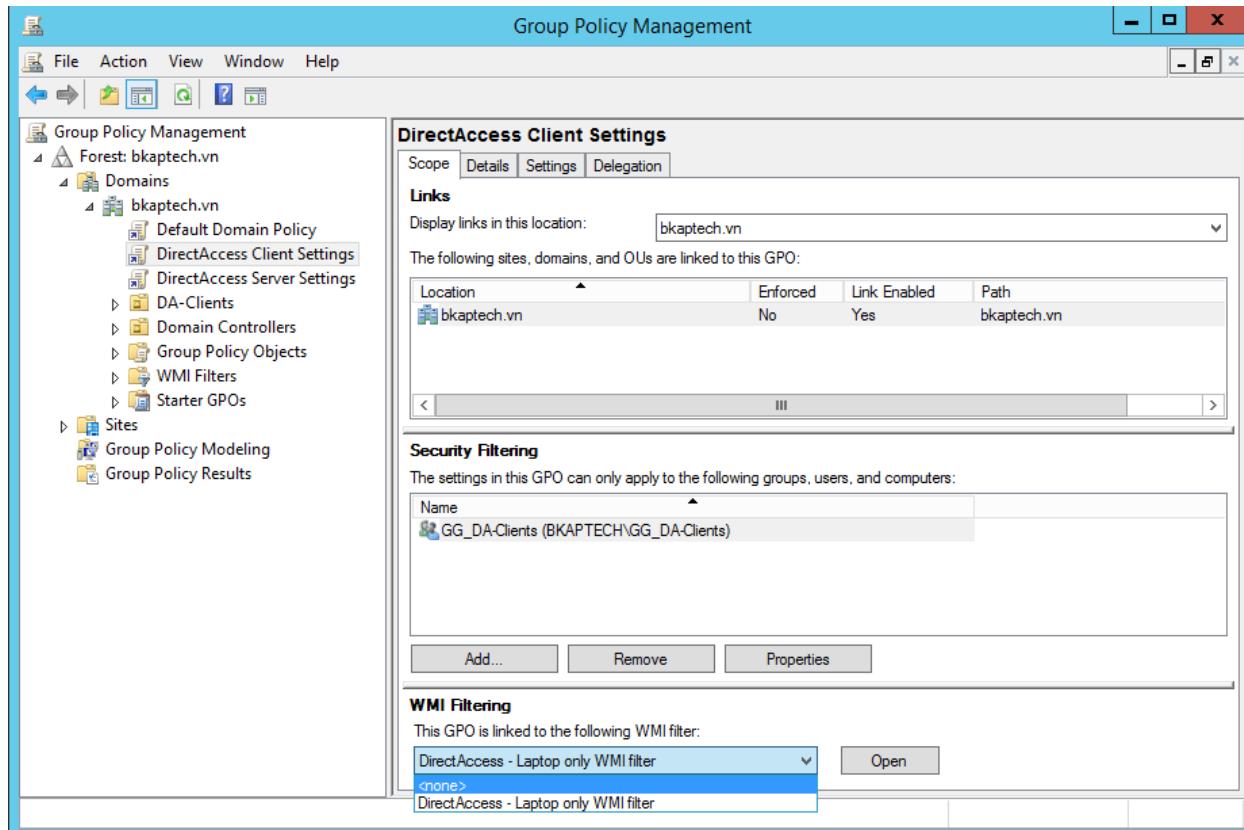
- Cấu hình GPO hỗ trợ tất cả các loại Client (thay vì chỉ hỗ trợ Laptop).

Mặc định, **Direct Access** chỉ hỗ trợ các *Laptop Client* do nhu cầu di chuyển của Laptop. Tuy nhiên trong mô hình này **WRK08-01** không phải là *Laptop* nên ta cần cấu hình **WMI Filter** của **GPO** để áp dụng cho tất cả các loại Client.

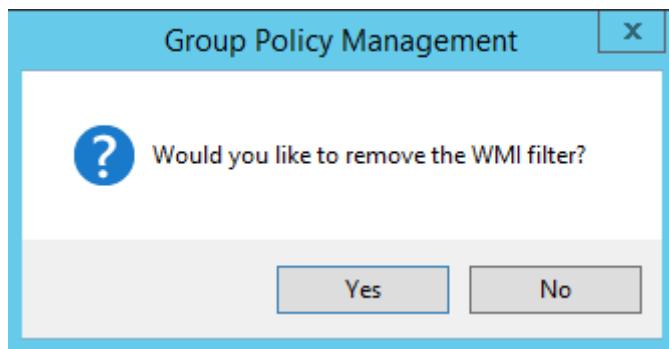
- Trên máy **DC12-01**. Mở *Group Policy Management*. Refresh màn hình (có thêm 2 GPO mới).

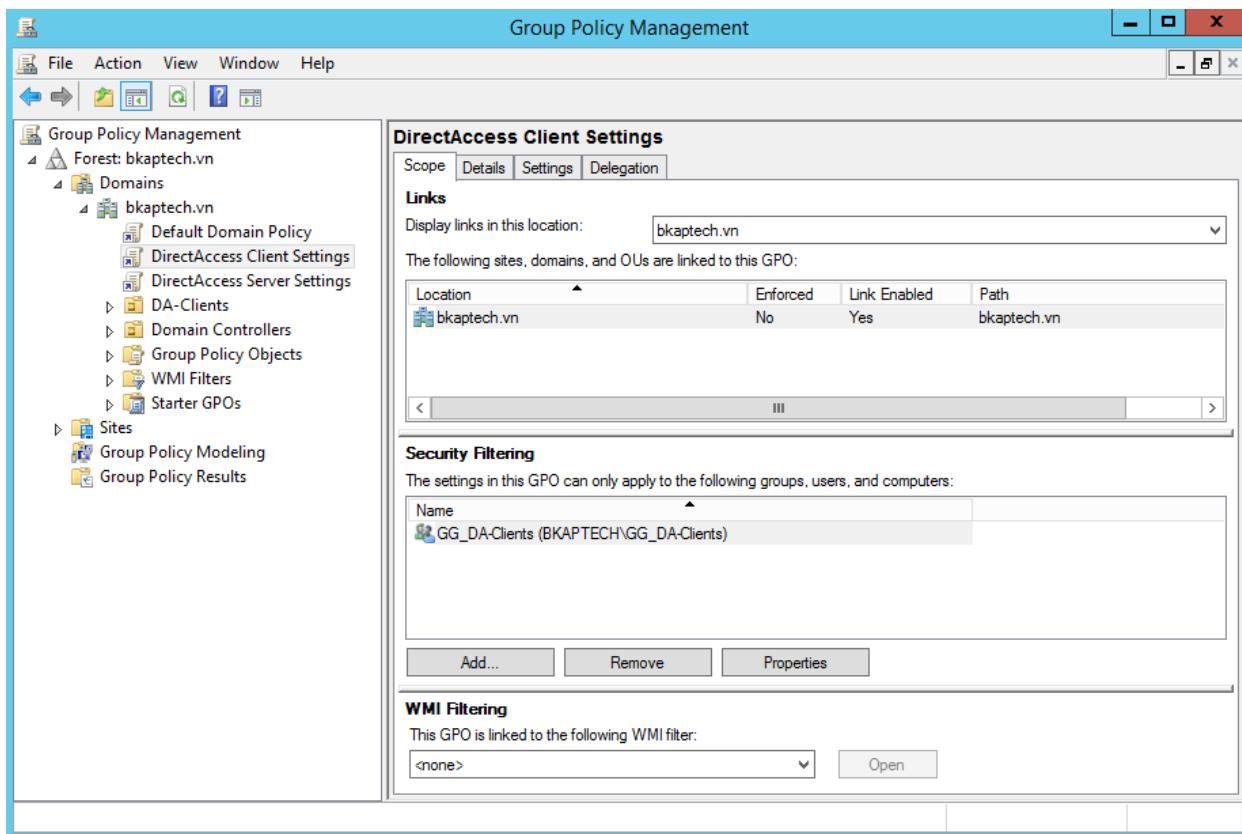


- Chọn GPO **DirectAccess Client Settings**. Trong khung **WMI Filtering**: chọn <none>

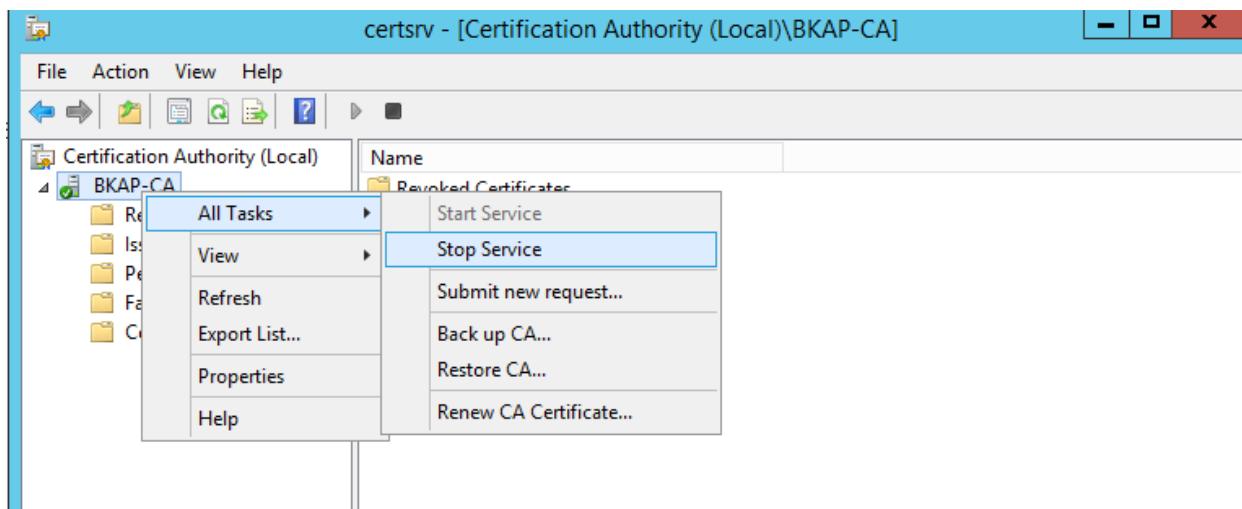


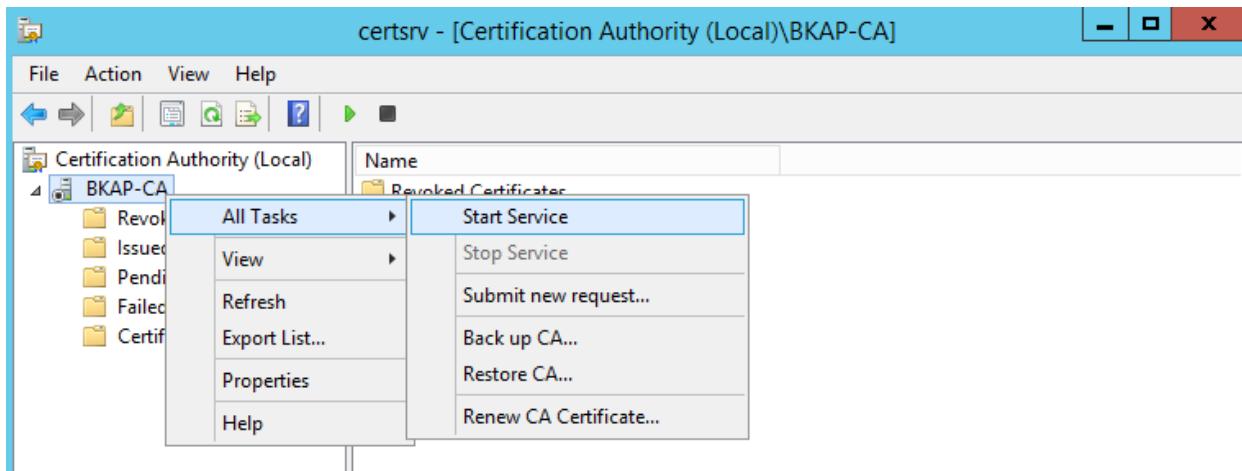
- Nhấn nút **Yes** để xác nhận gỡ bỏ **WMI Filtering**.



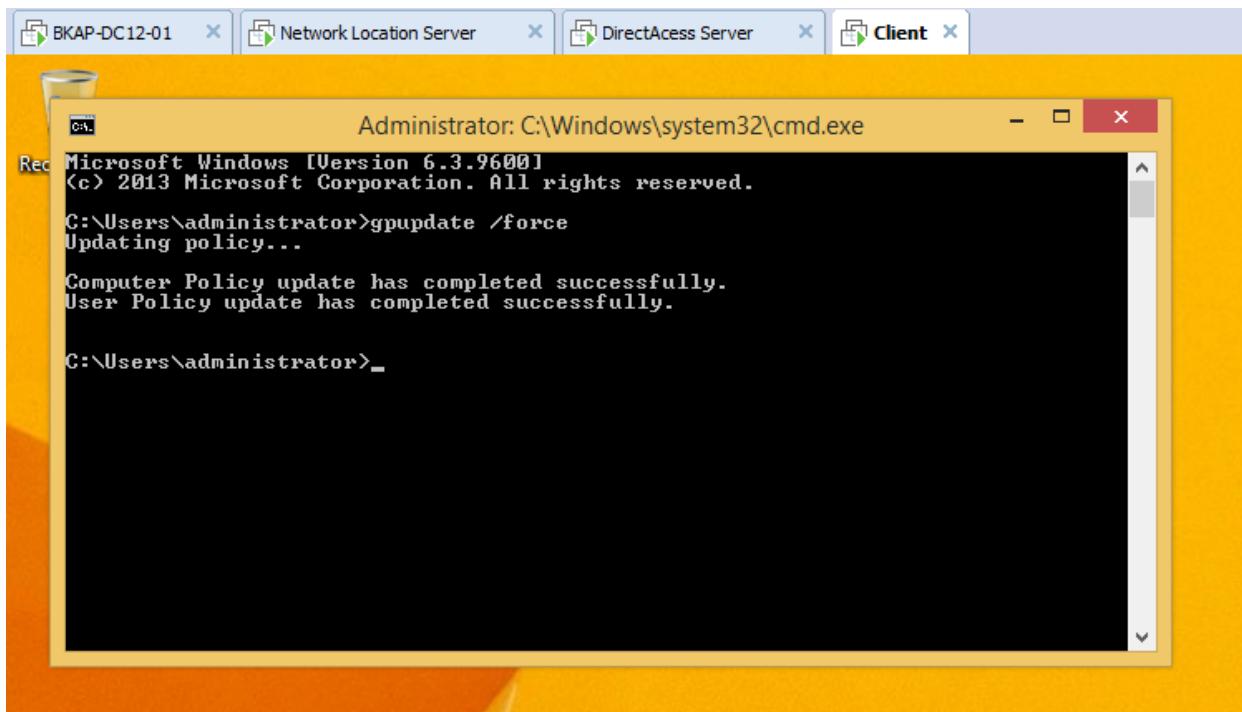


- Thực hiện restart lại dịch vụ *Active Directory Certificate Service*.





- Chuyển sang máy Clients WRK08-01, cập nhật GPO.



- Kiểm tra kết quả cập nhật bằng lệnh **GPRESULT /R**. Quan sát phần **COMPUTER SETTINGS**, bảo đảm client này phải được áp dụng GPO **DirectAccess Client Settings**.

```
Select 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>gpresult /r

Microsoft (R) Windows (R) Operating System Group Policy Result tool v2.0
c 2013 Microsoft Corporation. All rights reserved.

Created on 5/23/2016 at 9:03:51 PM

RSOP data for BKAPTECH\administrator on BKAP-WRK08-02 : Logging Mode

OS Configuration: Member Workstation
OS Version: 6.3.9600
Site Name: Default-First-Site-Name
Roaming Profile: N/A
Local Profile: C:\Users\administrator
Connected over a slow link?: No

COMPUTER SETTINGS

CN=BKAP-WRK08-02,OU=DA-Clients,DC=bkaptech,DC=vn
Last time Group Policy was applied: 5/23/2016 at 9:02:51 PM
Group Policy was applied from: BKAP-DC12-01.bkaptech.vn
Group Policy slow link threshold: 500 kbps
Domain Name: BKAPTECH
Domain Type: Windows 2008 or later

Applied Group Policy Objects
    DirectAccess Client Settings
        Default Domain Policy

The following GPOs were not applied because they were filtered out
    DirectAccess Server Settings
        Filtering: Denied <Security>

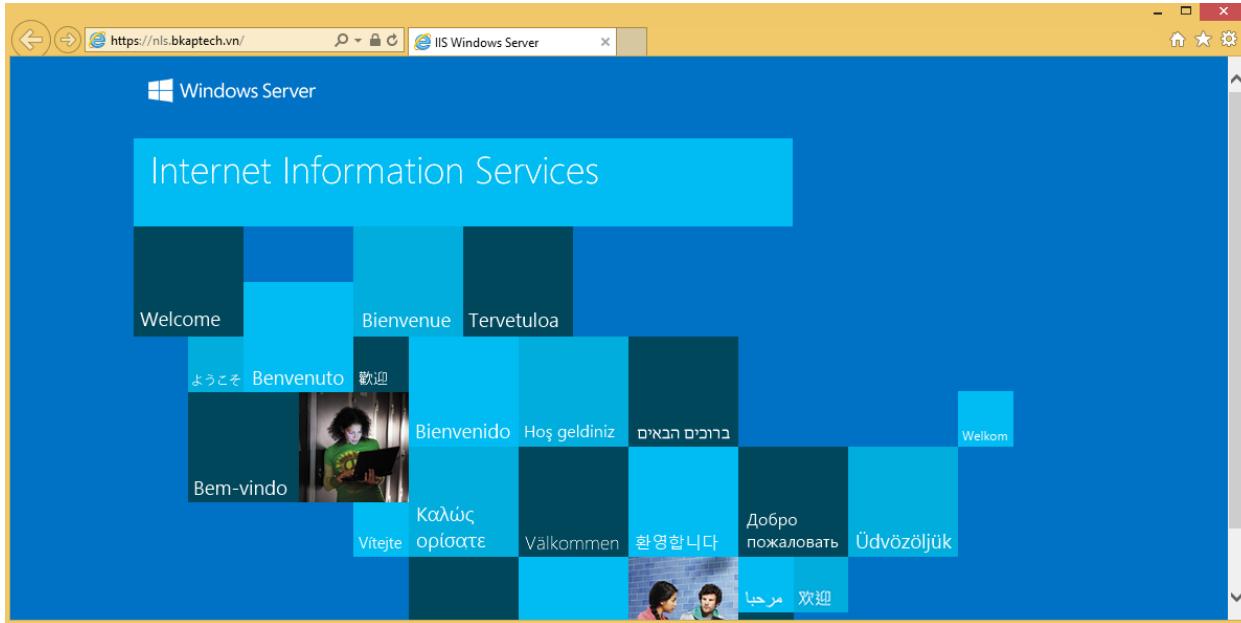
    Local Group Policy
        Filtering: Not Applied <Empty>

The computer is a part of the following security groups
    BUILTIN\Administrators
    Everyone
    BUILTIN\Users
    NT AUTHORITY\NETWORK
    NT AUTHORITY\Authenticated Users
    This Organization
    BKAP-WRK08-02$
    GG_DA-Clients
    Domain Computers
    Authentication authority asserted identity
    System Mandatory Level

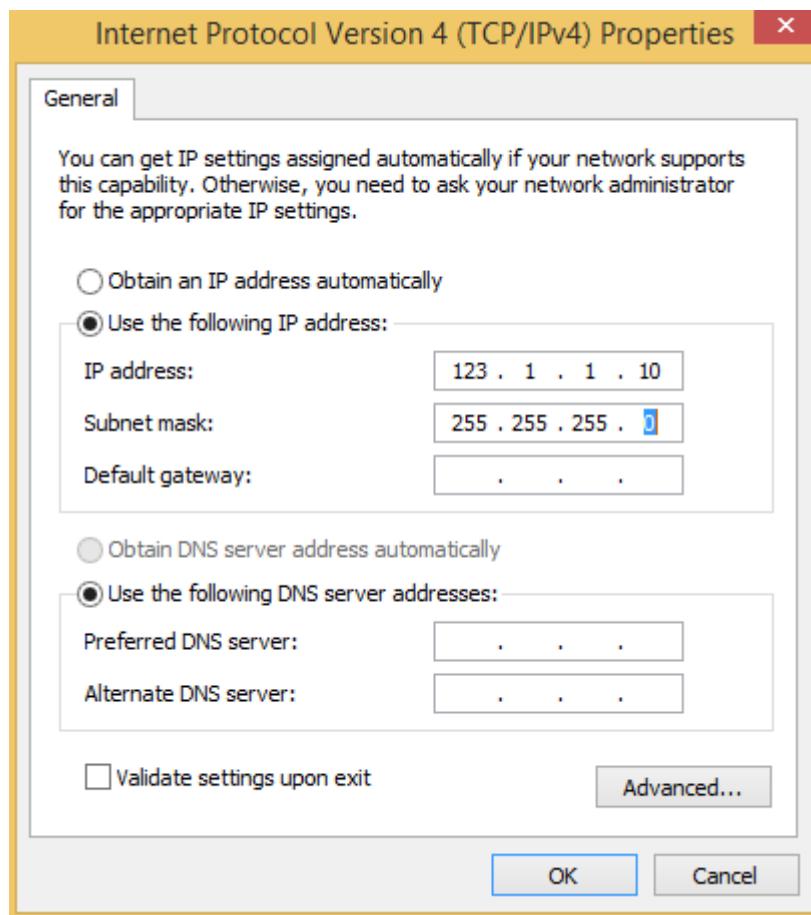
USER SETTINGS

CN=Administrator,CN=Users,DC=bkaptech,DC=vn
Last time Group Policy was applied: 5/23/2016 at 9:02:52 PM
```

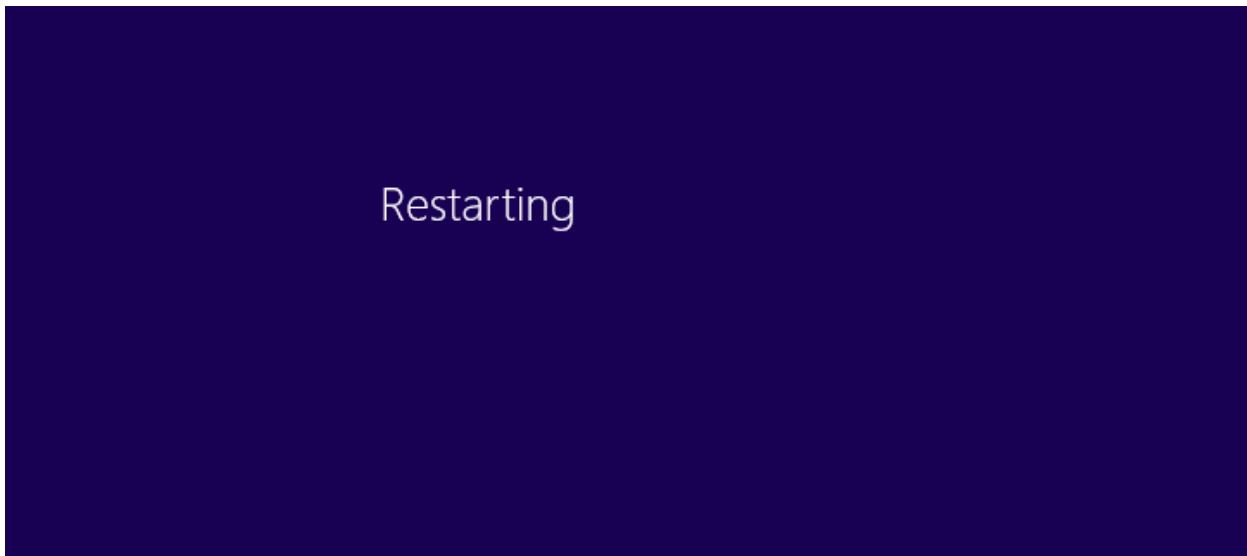
- Kiểm tra truy cập vào Website của **Network Location Server** bằng **HTTPS**.



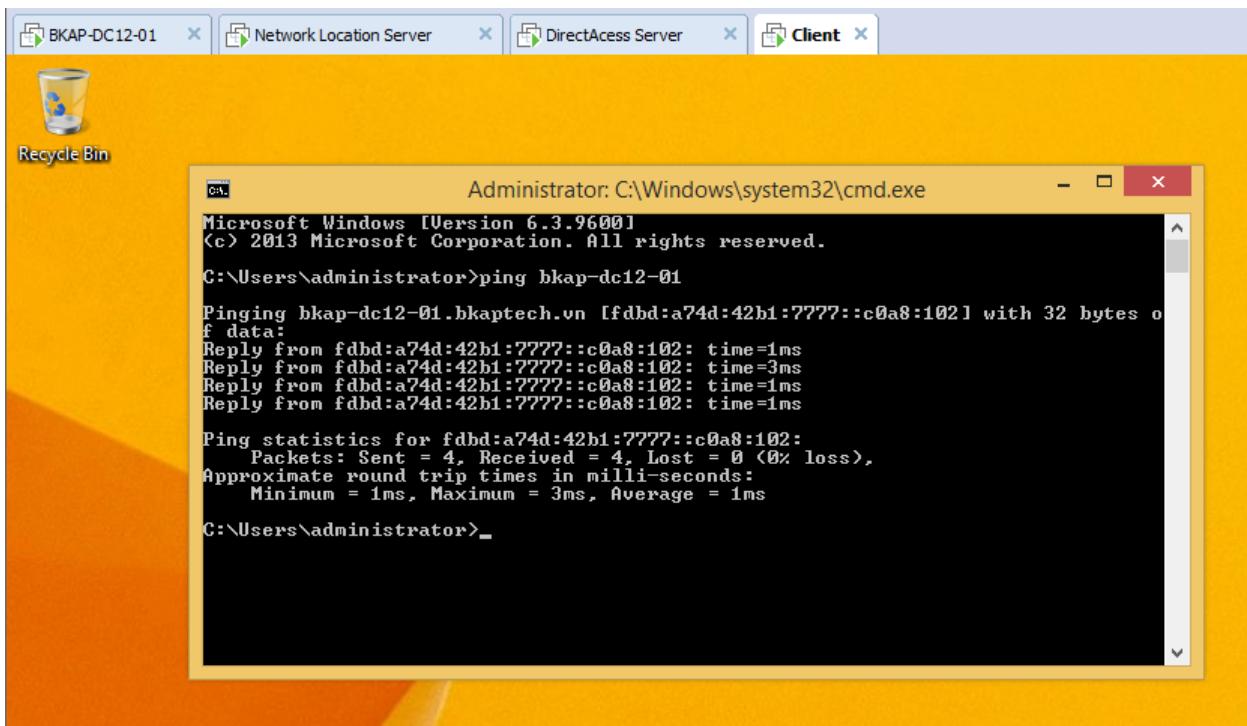
- Kiểm tra kết nối bằng **Direct Access**.
 - Chính lại card mạng của máy Client WRK08-01 là VMnet3 và IP là *public*.(Đặt IP cùng mạng với card VMnet3 của **Direct Access Server**).

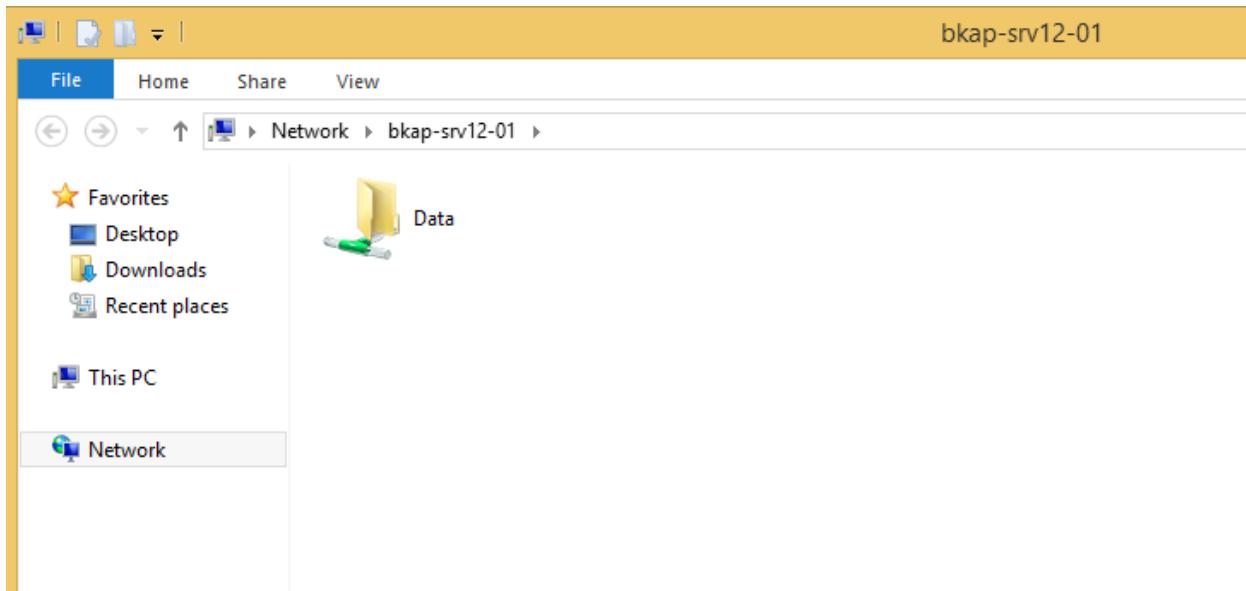


- Thực hiện reset lại máy **Client**.(bật giao thức *IPv6* và *Firewall* trên **Client**).



- Kiểm tra bằng cách **ping** vào một máy trong mạng nội bộ (ví dụ **PING bkap-dc12-01**) ta sẽ thấy kết quả reply bằng *IPv6*.



▪ Truy cập dịch vụ File trên **BKAP-SRV12-01**:

- Dùng lệnh **IPCONFIG /ALL** để khảo sát các Adapter IPv6:

```
Administrator: C:\Windows\system32\cmd.exe
WINS Proxy Enabled . . . . . : No
DNS Suffix Search List . . . . . : bkaptech.vn

Ethernet adapter Ethernet0:
Connection-specific DNS Suffix . . . . . : Intel(R) 82574L Gigabit Network Connection
Description . . . . . : Intel(R) 82574L Gigabit Network Connection
Physical Address . . . . . : 00-0C-29-07-3E-6D
DHCP Enabled . . . . . : No
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::a98e:6fd1:b904:12a4%3(PREFERRED)
IPv4 Address . . . . . : 123.1.1.10(PREFERRED)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 123.1.1.1
DHCPv6 IAID . . . . . : 50334761
DHCPv6 Client DUID . . . . . : 00-01-00-01-1E-86-2D-40-00-0C-29-07-3E-6D
DNS Servers . . . . . : fec0:0:0:ffff::1%1
                         fec0:0:0:ffff::2%1
                         fec0:0:0:ffff::3%1
NetBIOS over Tcpip . . . . . : Enabled

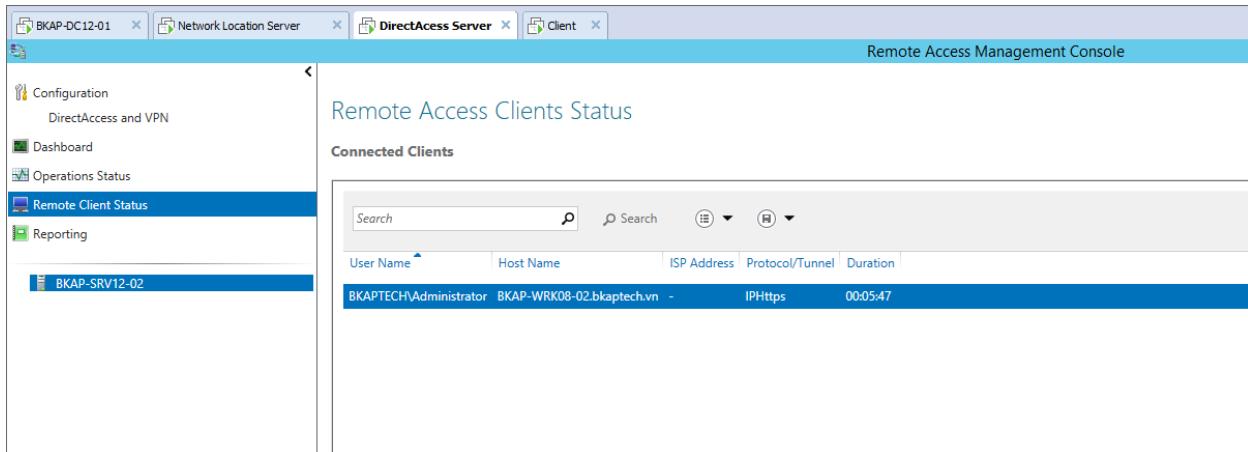
Tunnel adapter 6TO4 Adapter:
Connection-specific DNS Suffix . . . . . : Microsoft 6to4 Adapter
Description . . . . . : Microsoft 6to4 Adapter
Physical Address . . . . . : 00-00-00-00-00-00-E0
DHCP Enabled . . . . . : No
Autoconfiguration Enabled . . . . . : Yes
IPv6 Address . . . . . : 2002:7b01:10a::7b01:10a(PREFERRED)
Default Gateway . . . . . :
DHCPv6 IAID . . . . . : 150994944
DHCPv6 Client DUID . . . . . : 00-01-00-01-1E-86-2D-40-00-0C-29-07-3E-6D
DNS Servers . . . . . : fec0:0:0:ffff::1%1
                         fec0:0:0:ffff::2%1
                         fec0:0:0:ffff::3%1
NetBIOS over Tcpip . . . . . : Disabled

Tunnel adapter isatap.{28989327-657D-4472-B2D4-43254223B842}:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . . . . : Microsoft ISATAP Adapter #2
Description . . . . . : Microsoft ISATAP Adapter #2
Physical Address . . . . . : 00-00-00-00-00-00-E0
DHCP Enabled . . . . . : No
Autoconfiguration Enabled . . . . . : Yes

Tunnel adapter iphttpsinterface:
Connection-specific DNS Suffix . . . . . : iphttpsinterface
Description . . . . . : iphttpsinterface
Physical Address . . . . . : 00-00-00-00-00-00-E0
DHCP Enabled . . . . . : No
Autoconfiguration Enabled . . . . . : Yes
IPv6 Address . . . . . : 2002:7b01:101:1000:9cf0:b5b0:438a:de1b(PREFERRED)
Temporary IPv6 Address . . . . . : 2002:7b01:101:1000:bcfd:ee37:feb8:1ab2(PREFERRED)
Link-local IPv6 Address . . . . . : fe80::9cf0:b5b0:438a:de1b%10(PREFERRED)
Default Gateway . . . . . :
DHCPv6 IAID . . . . . : 167772160
DHCPv6 Client DUID . . . . . : 00-01-00-01-1E-86-2D-40-00-0C-29-07-3E-6D
NetBIOS over Tcpip . . . . . : Disabled

C:\Users\administrator>
```

- Sang máy *DirectAccess Server*, kiểm tra trạng thái kết nối của Client.



Bài 7:

TRIỂN KHAI NETWORK LOAD BALANCING

Các nội dung chính được đề cập:

- ✓ Cài đặt và cấu hình dịch vụ Network Load Balancing.

7. Triển khai Network Load Balancing

1.Yêu cầu bài Lab:

+ Trên Server *BKAP-SRV12-01* và *BKAP-SRV12-02*:

- Tạo dữ liệu và nội dung Website đặt trên ổ C.
- Cài đặt **Web Server (IIS) role**.
- Tạo **Hosting Website** trên IIS.
- Cài đặt và cấu hình **Network Load Balancing**.

+ Trên Server *BKAP-DC12-01*:

- Cài đặt, cấu hình **DNS Server**.
- Tạo bản ghi trên **DNS Server** để phân giải Website với tên miền www.bkaptech.vn có địa chỉ là 192.168.1.100

+ Kiểm tra sau khi thiết lập:

- Trên máy Client *BKAP-WRK08-01* truy cập vào website www.bkaptech.vn.
- Thực hiện tắt máy *BKAP-SRV12-01*, trên Client vẫn truy cập lại Website thành công.

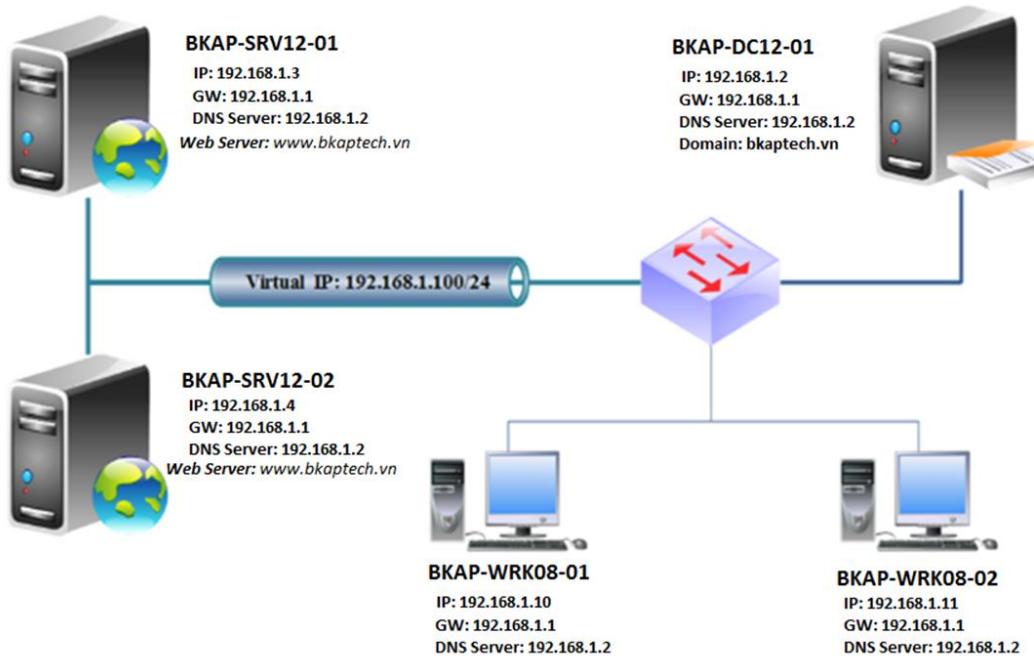
2.Yêu cầu chuẩn bị:

- + Máy Server *BKAP-DC12-01* đã nâng cấp lên **Domain Controller**, quản lý miền **bkaptech.vn**.
- + Máy Server *BKAP-SRV12-01* cài đặt và cấu hình Web IIS.
- + Máy Server *BKAP-SRV12-02* cài đặt và cấu hình Web IIS.
- + Máy Client *BKAP-WRK08-01* dùng để kiểm tra.

3.Mô hình Lab:

HỆ THỐNG ĐÀO TẠO CNTT QUỐC TẾ BACHKHOA-APTECH

Triển khai Network Load Balancing

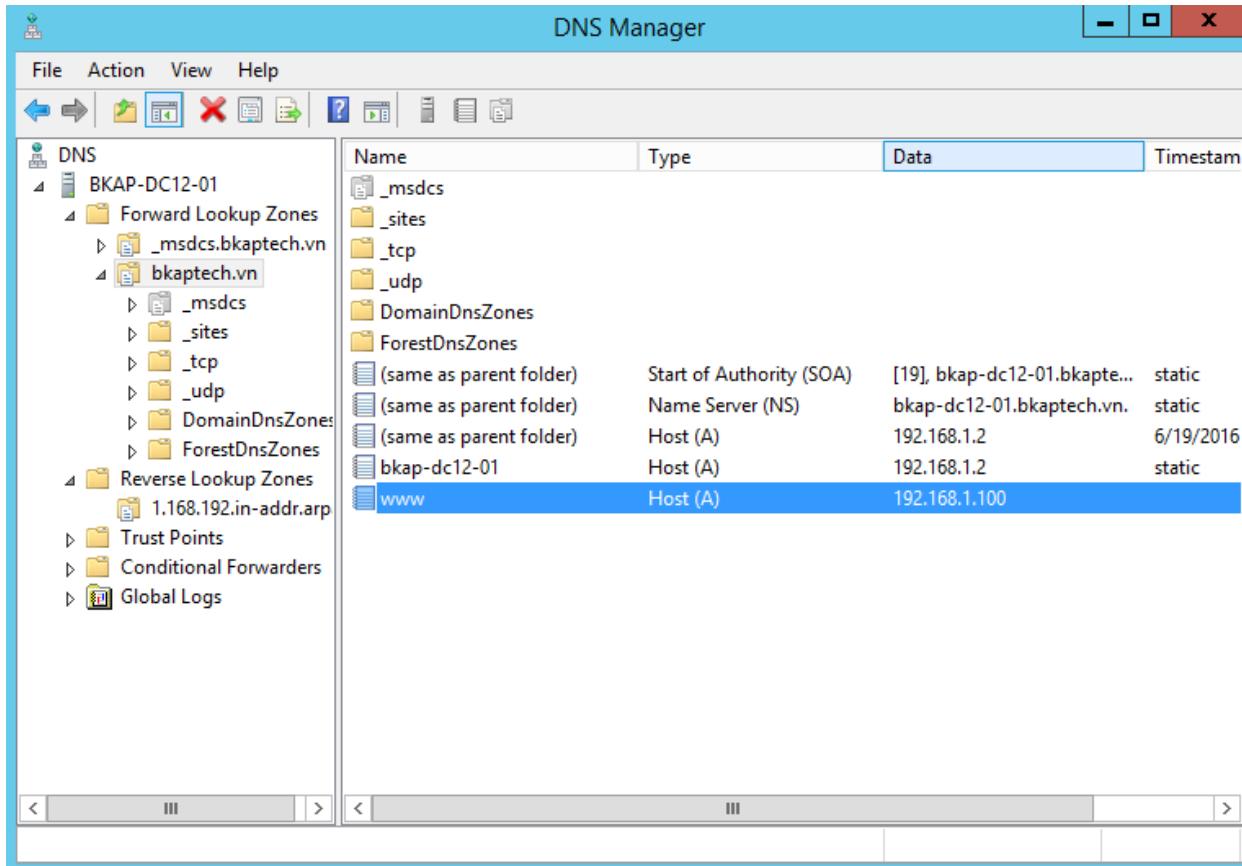


Sơ đồ địa chỉ như sau:

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>Default Gateway</i>	192.168.1.1	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	255.255.255.0
<i>DNS Server</i>	192.168.1.2	192.168.1.2	192.168.1.2	192.168.1.2

Hướng dẫn chi tiết:

- Trên máy **BKAP-DC12-01**, thực hiện cấu hình **DNS Server** , tạo bản ghi phân giải tên miền Web Server www.bkaptech.vn ⇔ **192.168.1.100**.



○ Kiểm tra:

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

C:\Users\Administrator>nslookup
Default Server: bkap-dc12-01.bkaptech.vn
Address: 192.168.1.2

> www.bkaptech.vn
Server: bkap-dc12-01.bkaptech.vn
Address: 192.168.1.2

Name: www.bkaptech.vn
Address: 192.168.1.100

>
```

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

○ Kiểm tra địa chỉ IP:

- Kiểm tra phân giải DNS:

```

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

C:\Users\Administrator>nslookup
Default Server: bkap-dc12-01.bkaptech.vn
Address: 192.168.1.2

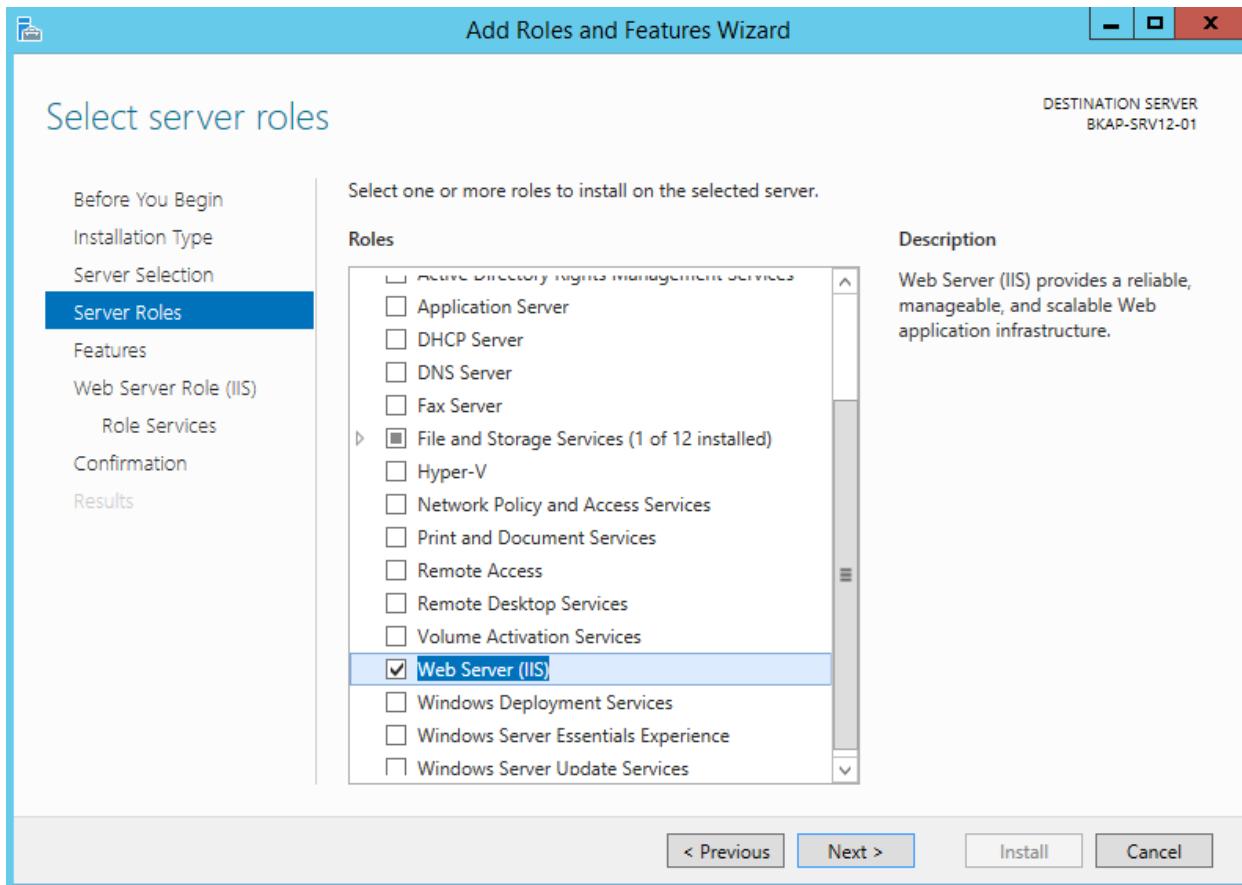
> www.bkaptech.vn
Server: bkap-dc12-01.bkaptech.vn
Address: 192.168.1.2

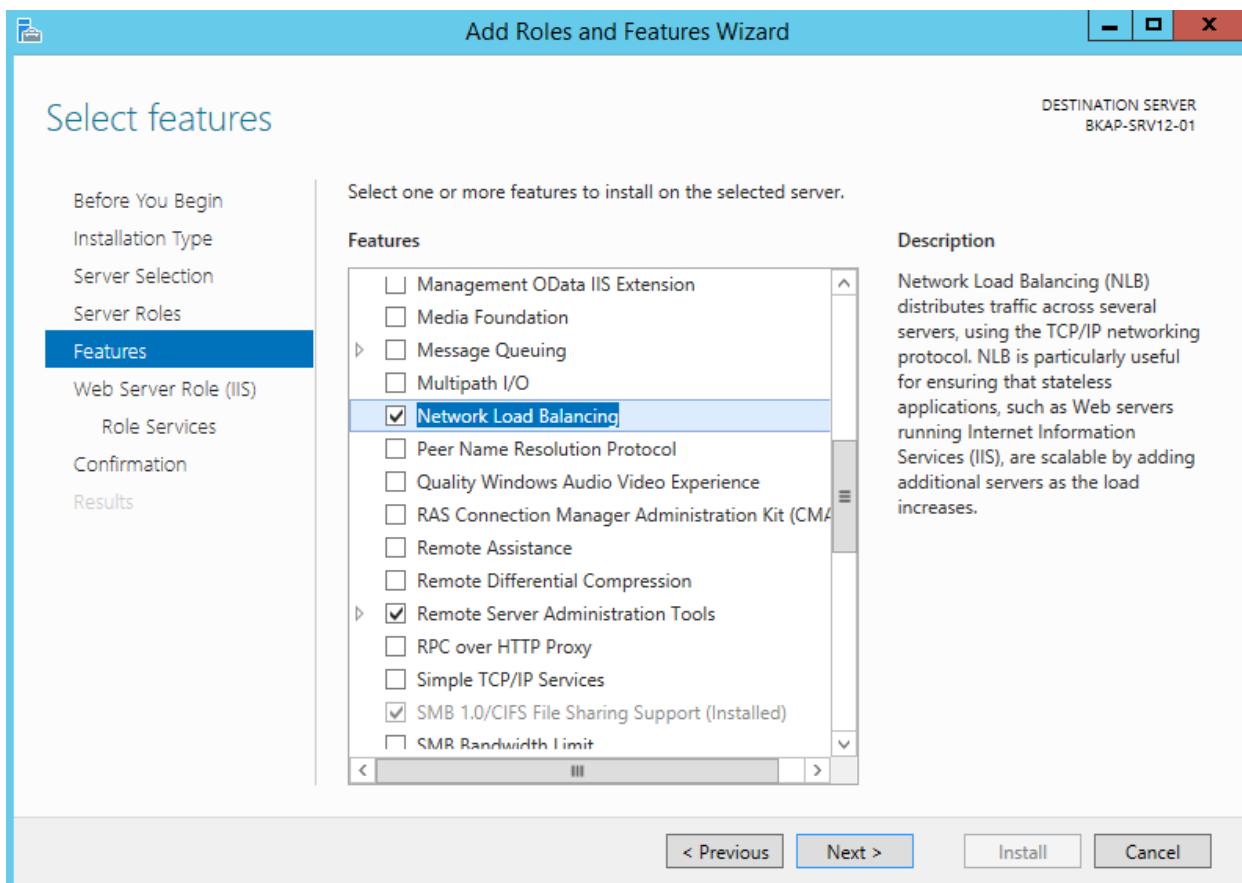
Name: www.bkaptech.vn
Address: 192.168.1.100

>

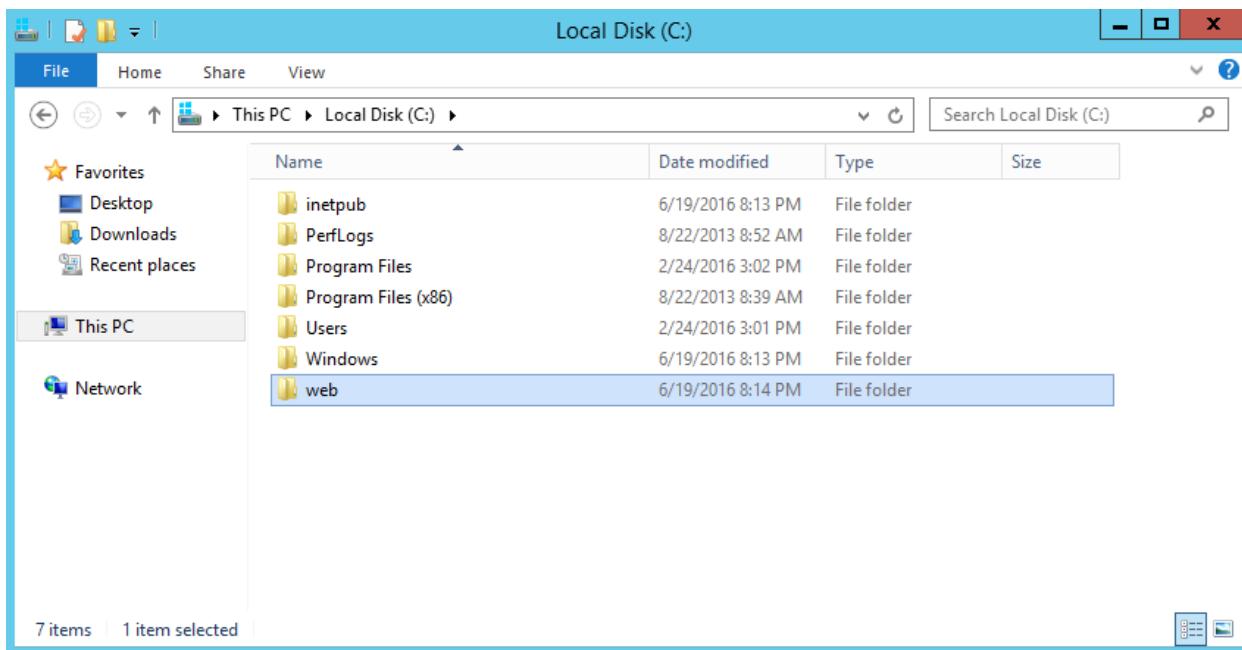
```

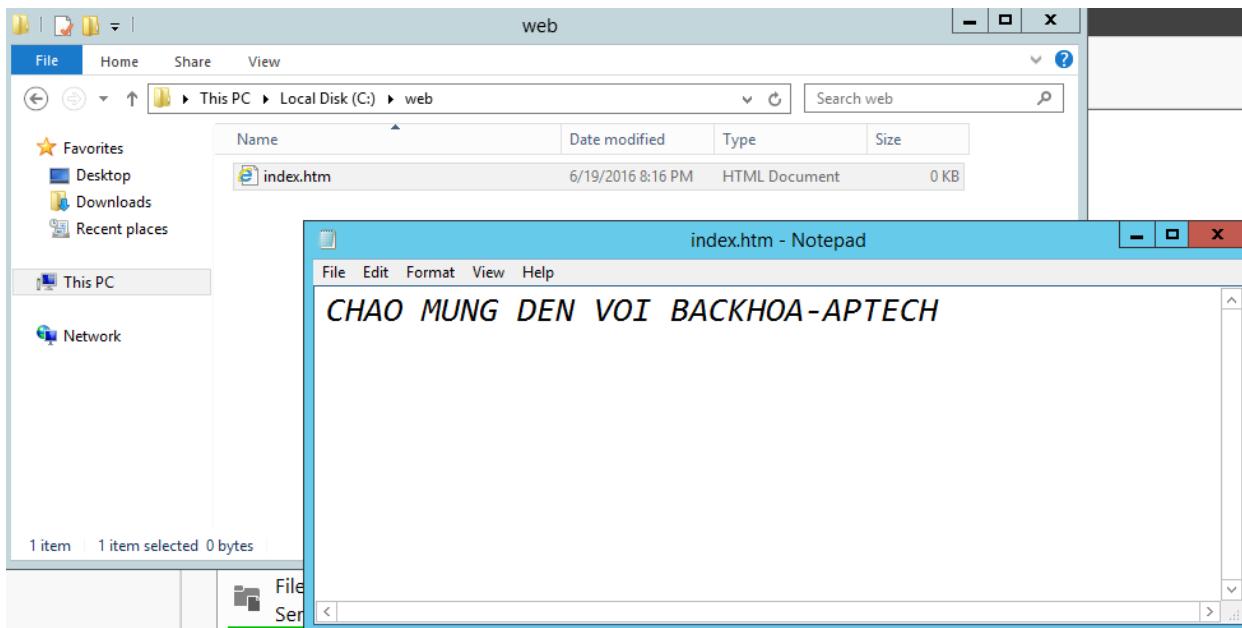
- Cài đặt dịch vụ Web (IIS) và Network Load Balancing.



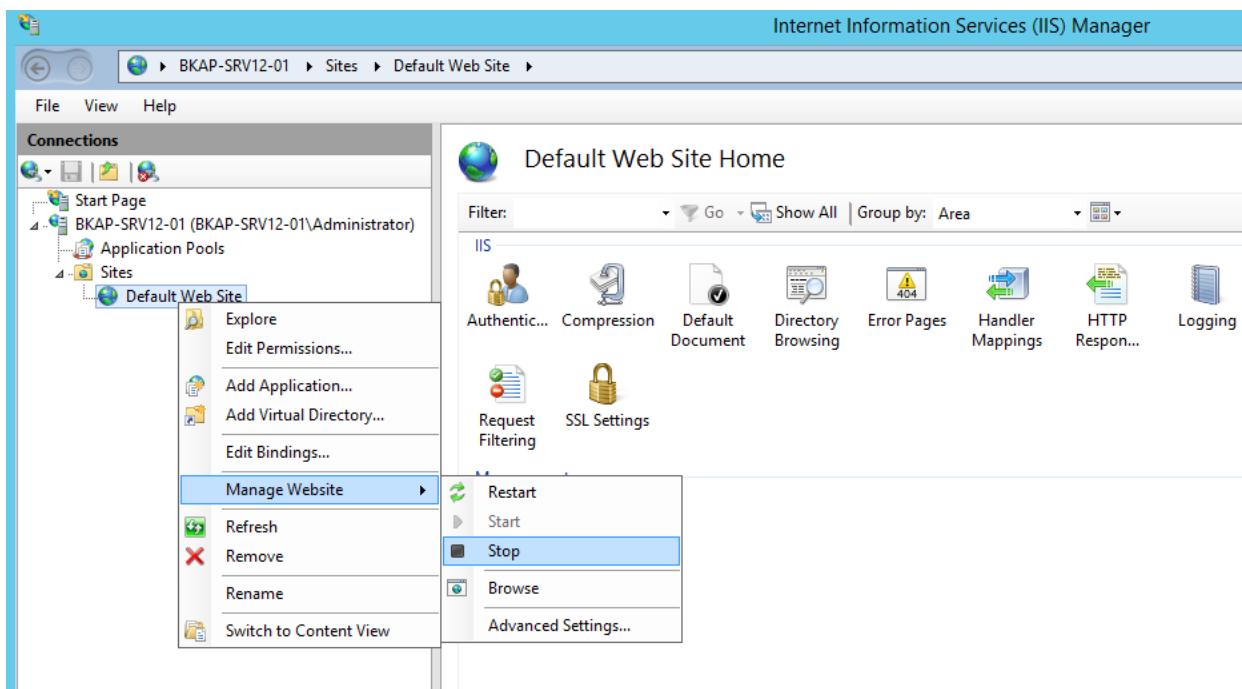


- Tạo thư mục và nội dung Website đặt trên ổ C.

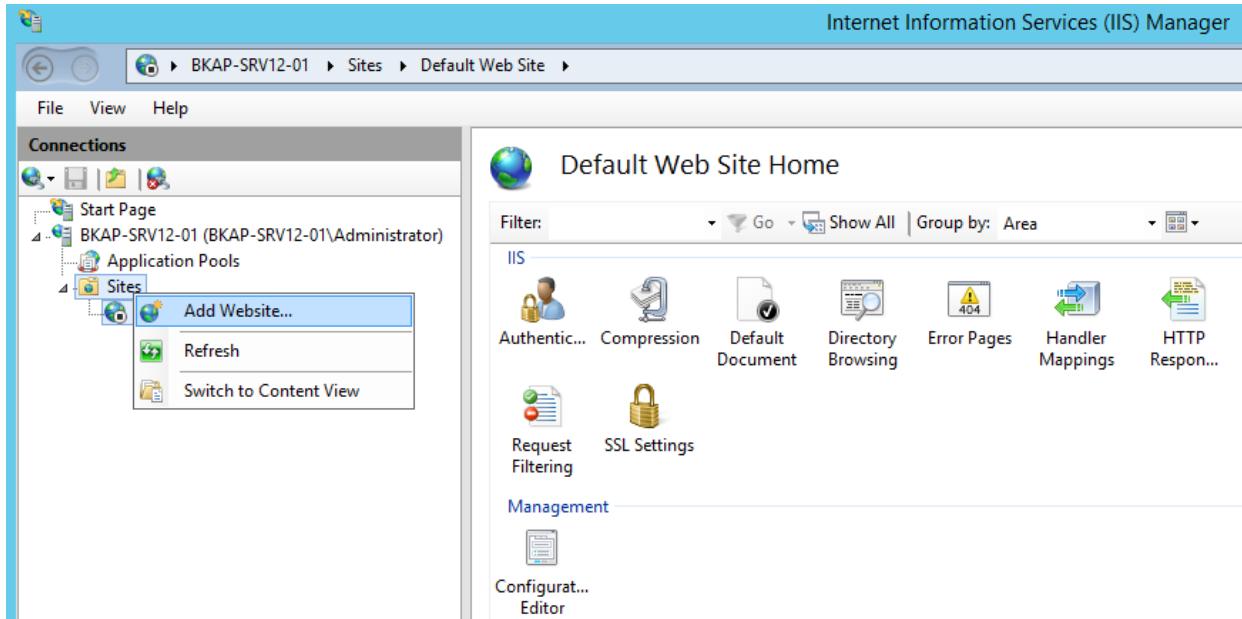




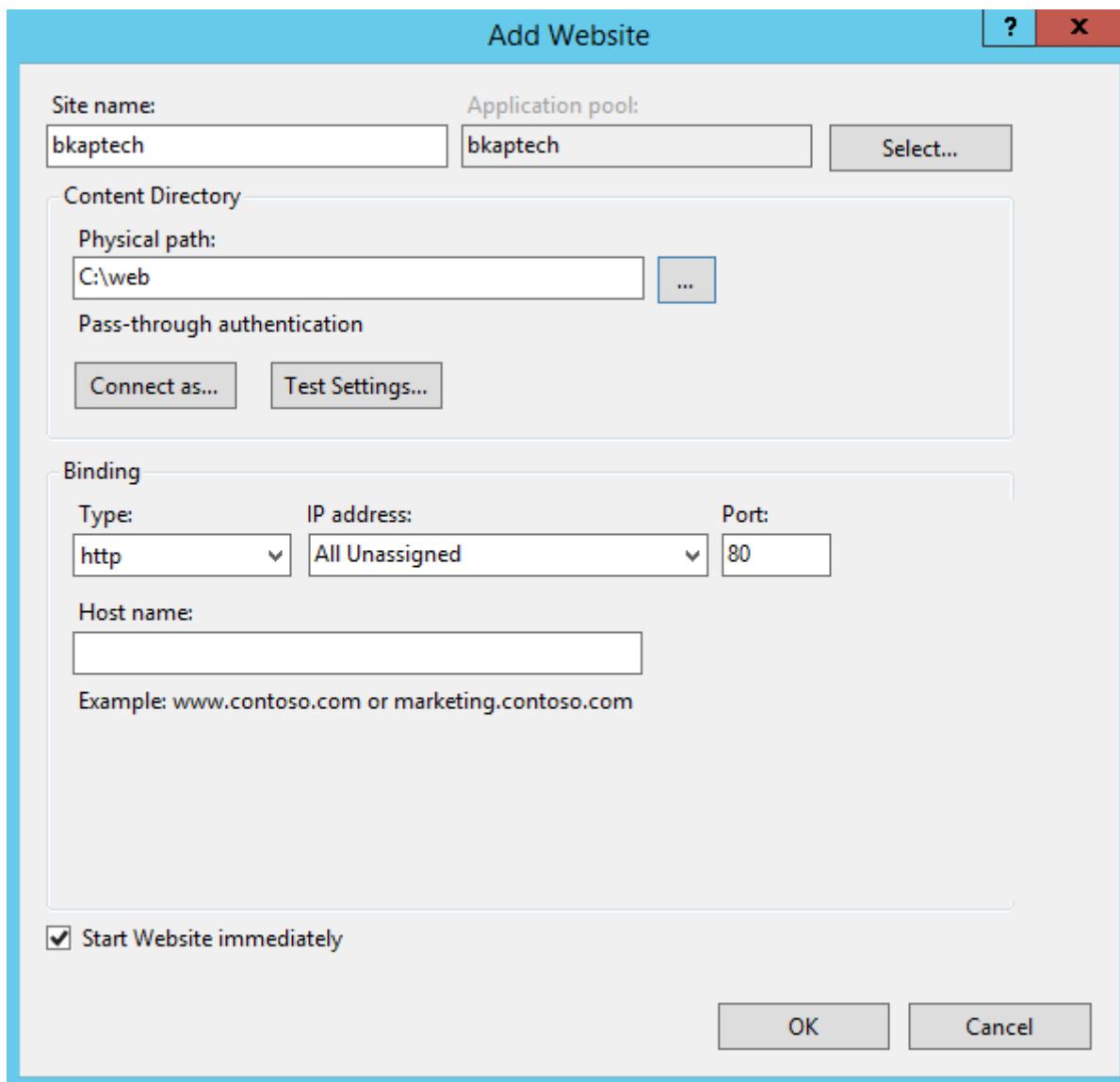
- Cấu hình Web Server (IIS).
 - Trong cửa sổ Internet Information Services (IIS) Manager , thực hiện Stop Default Web Site.



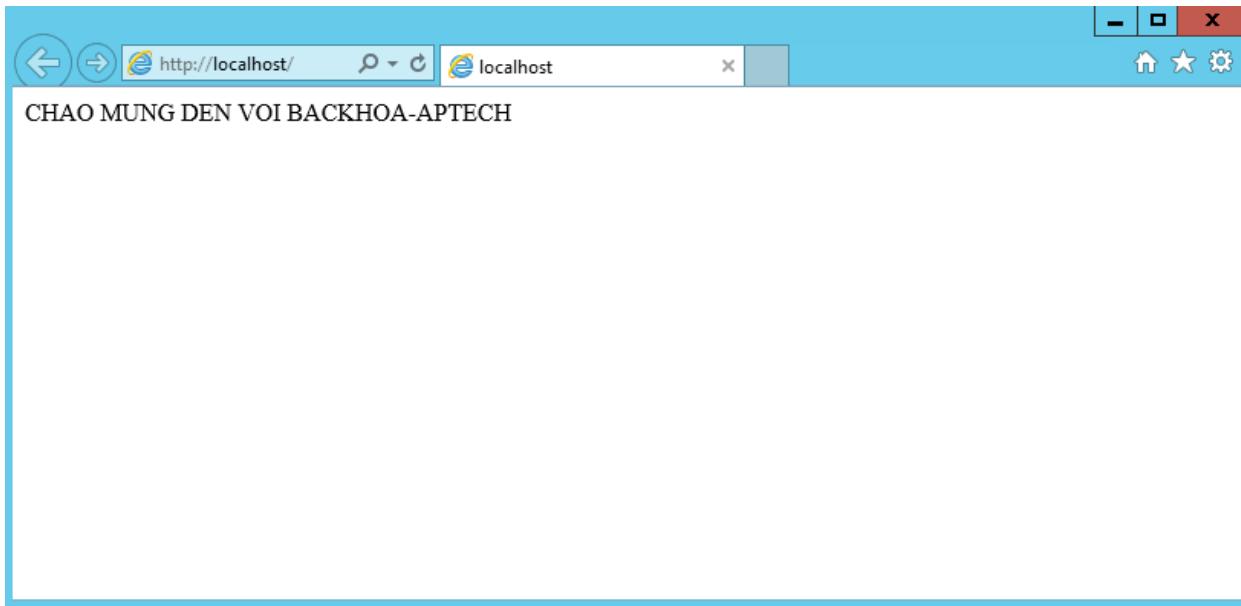
- Tạo Hostname mới:
 - Click chuột phải vào **Sites** , chọn **Add Website...**



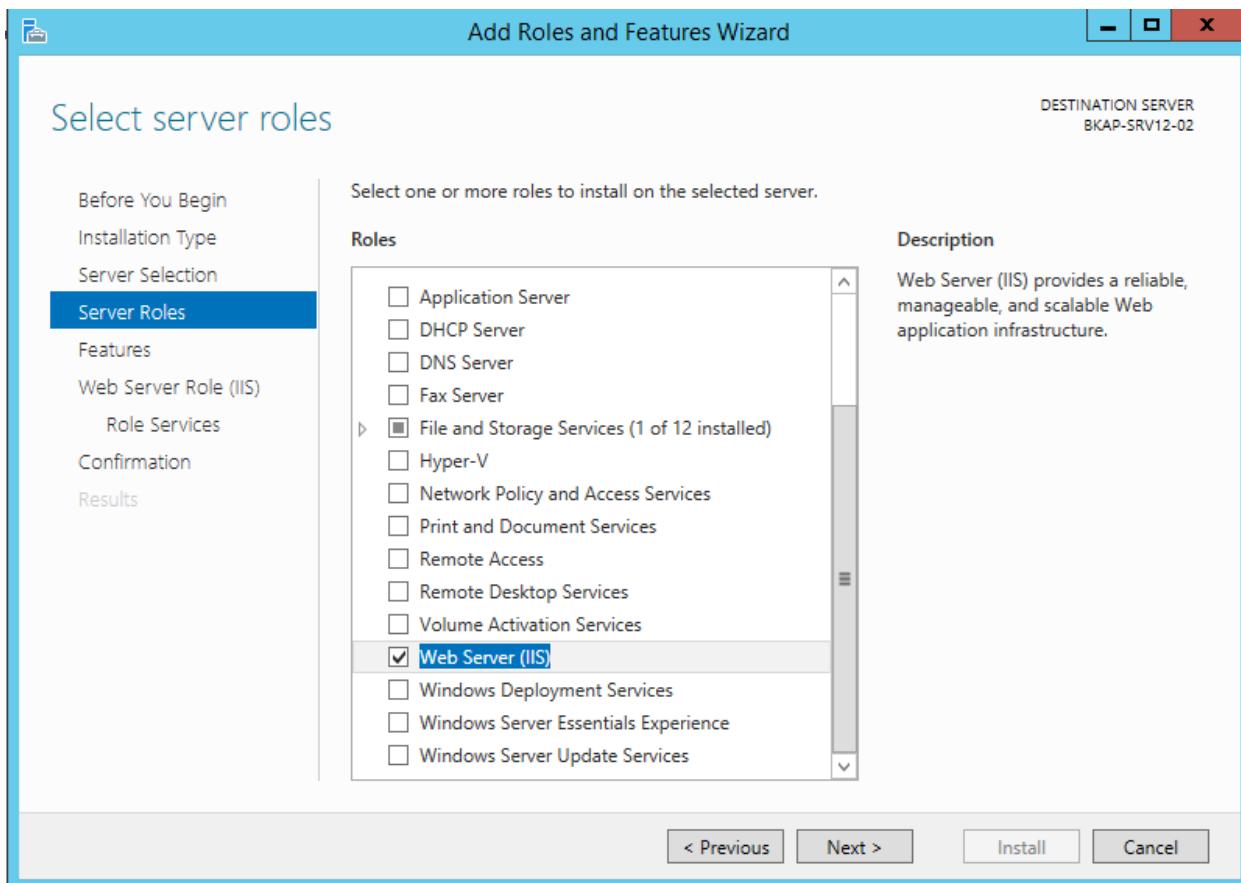
- Trong cửa sổ **Add Website**, tại mục **Site name**, nhập vào tên **bkaptech**.
 - Tại mục **Physical path**, *Browse* đến thư mục *Web* trong ô C.
 - **OK**.

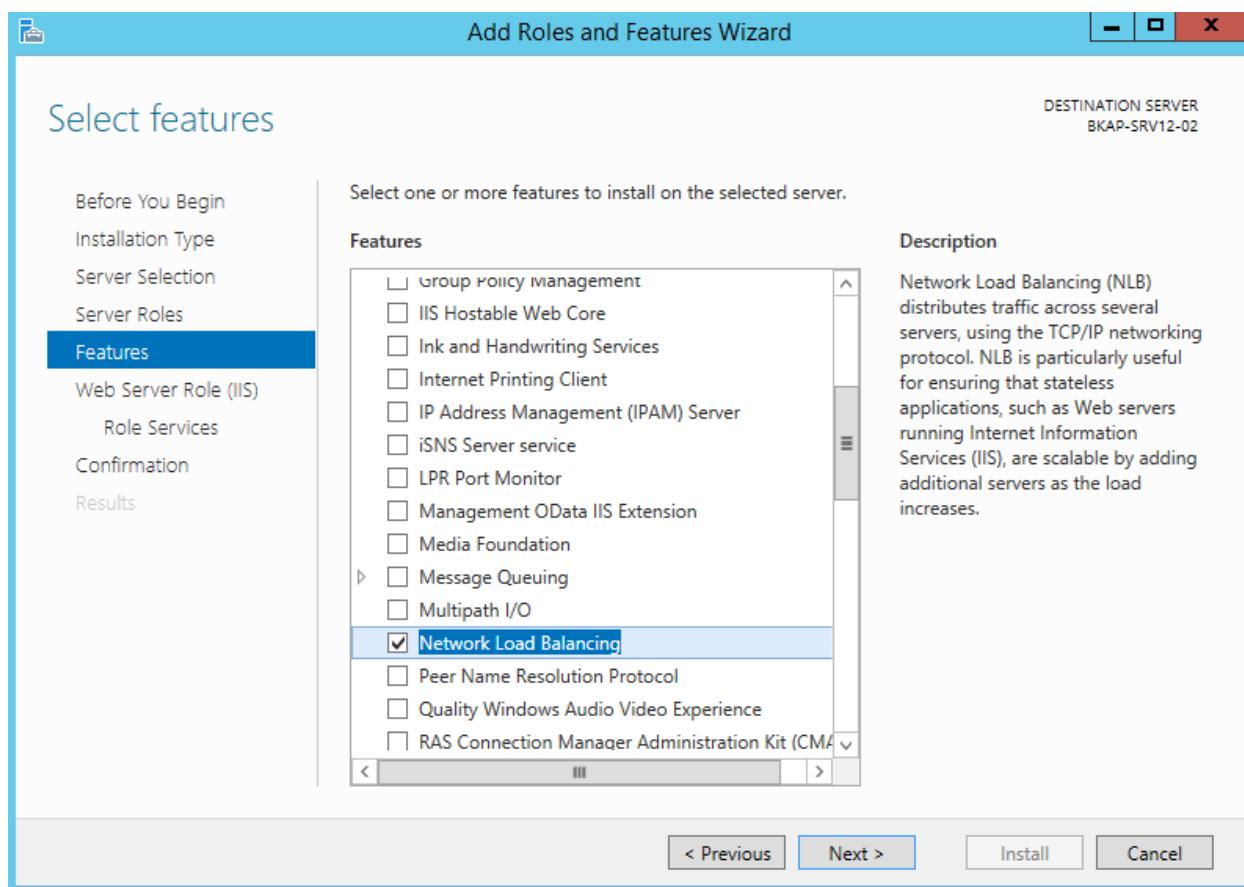


- Kiểm tra website chạy trong local.

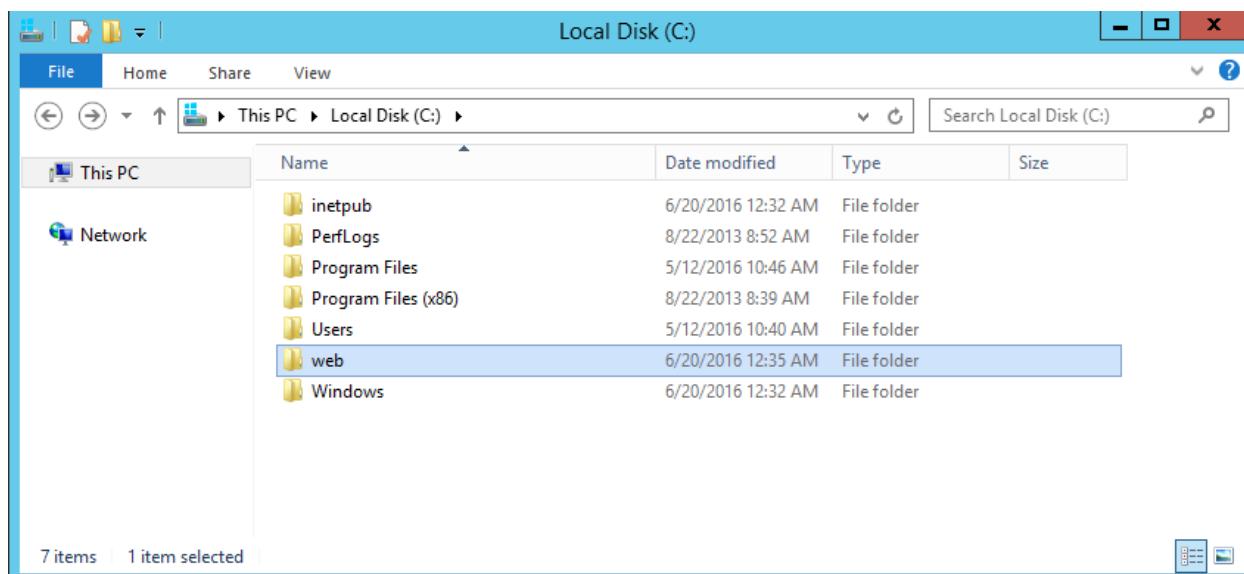


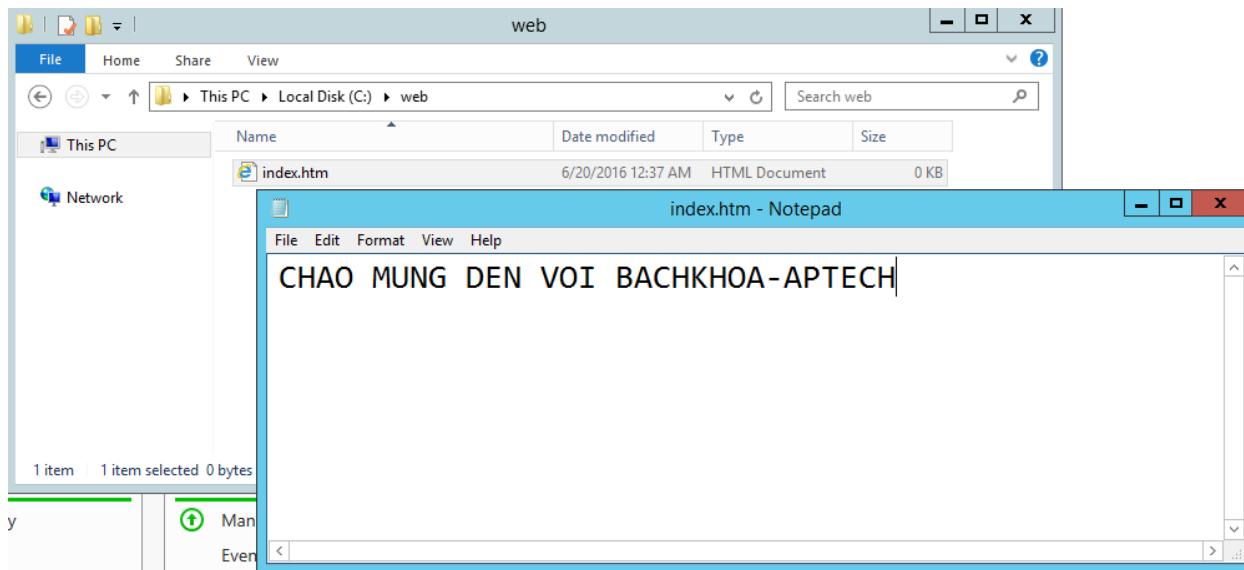
- Chuyển sang máy BKAP-SRV12-02 cài đặt và cấu hình IIS và Network Load Balancing.



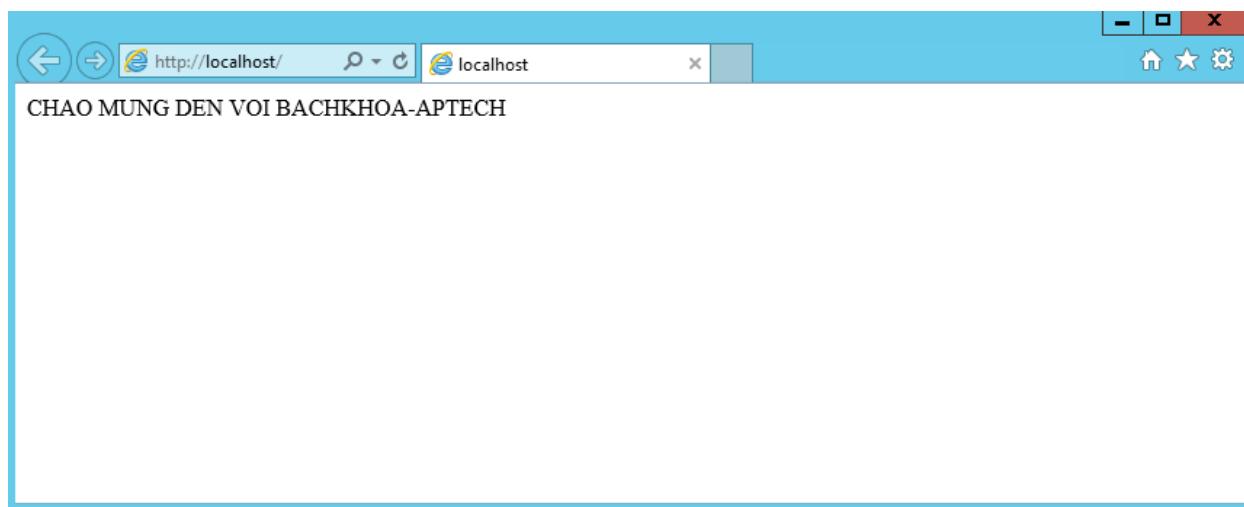


- Tạo thư mục vào nội dung Website đặt trong ổ C.

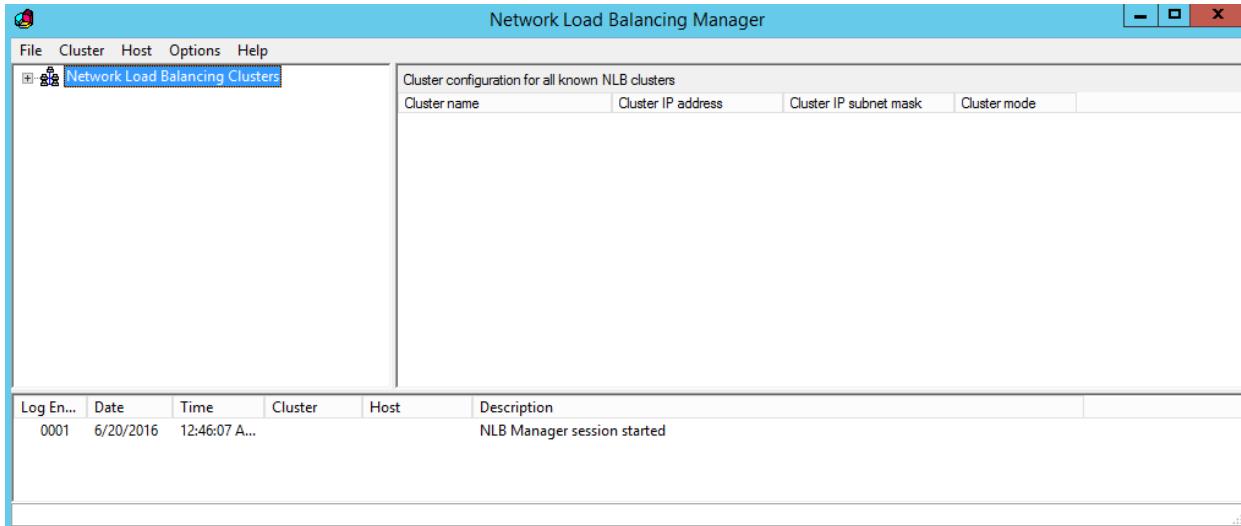




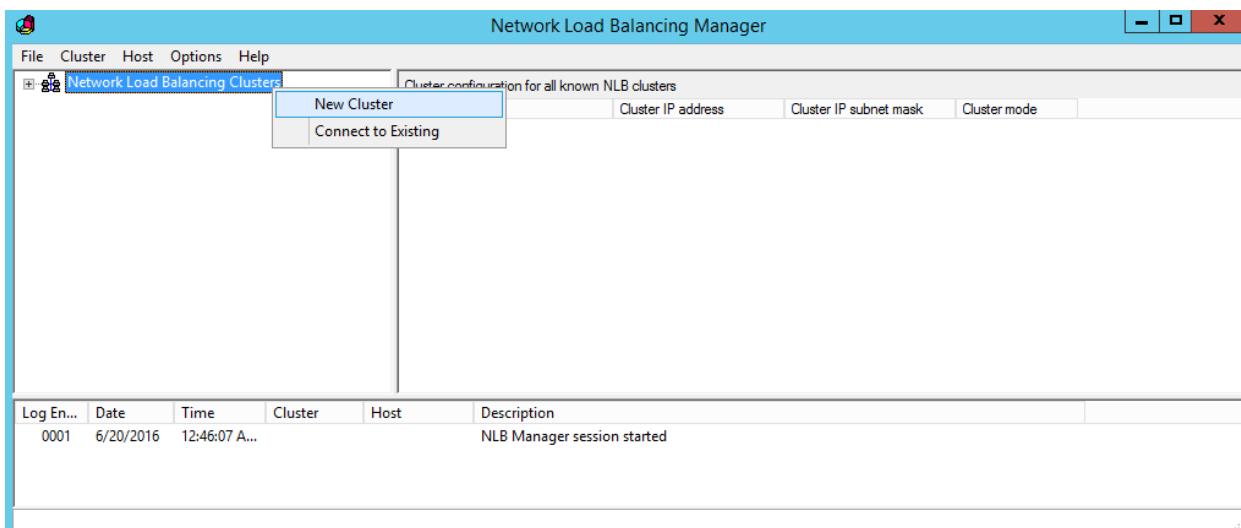
- Cấu hình Web Server (IIS). (Làm tương tự giống trên máy BKAP-SRV12-01).
 - Kết quả như sau:



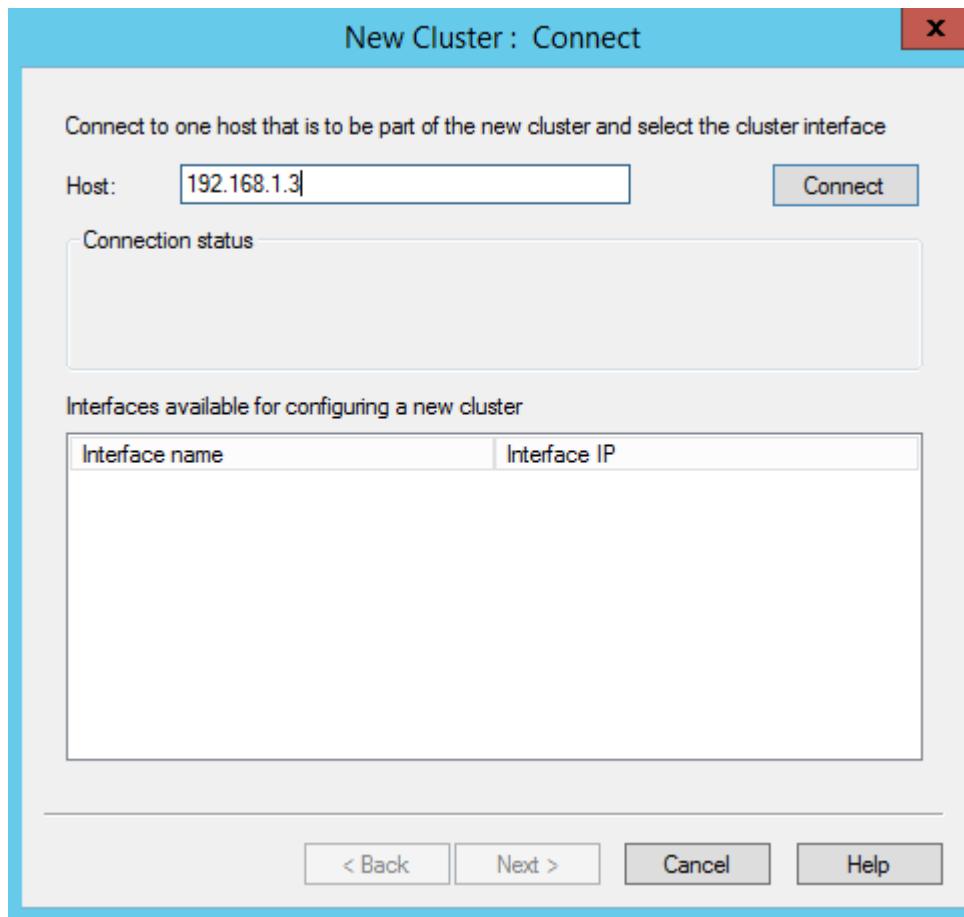
- Chuyển qua máy *BKAP-SRV12-01*, cấu hình Network Load Balancing.
 - Vào Server Manager / Tools / Network Load Balancing Manager.



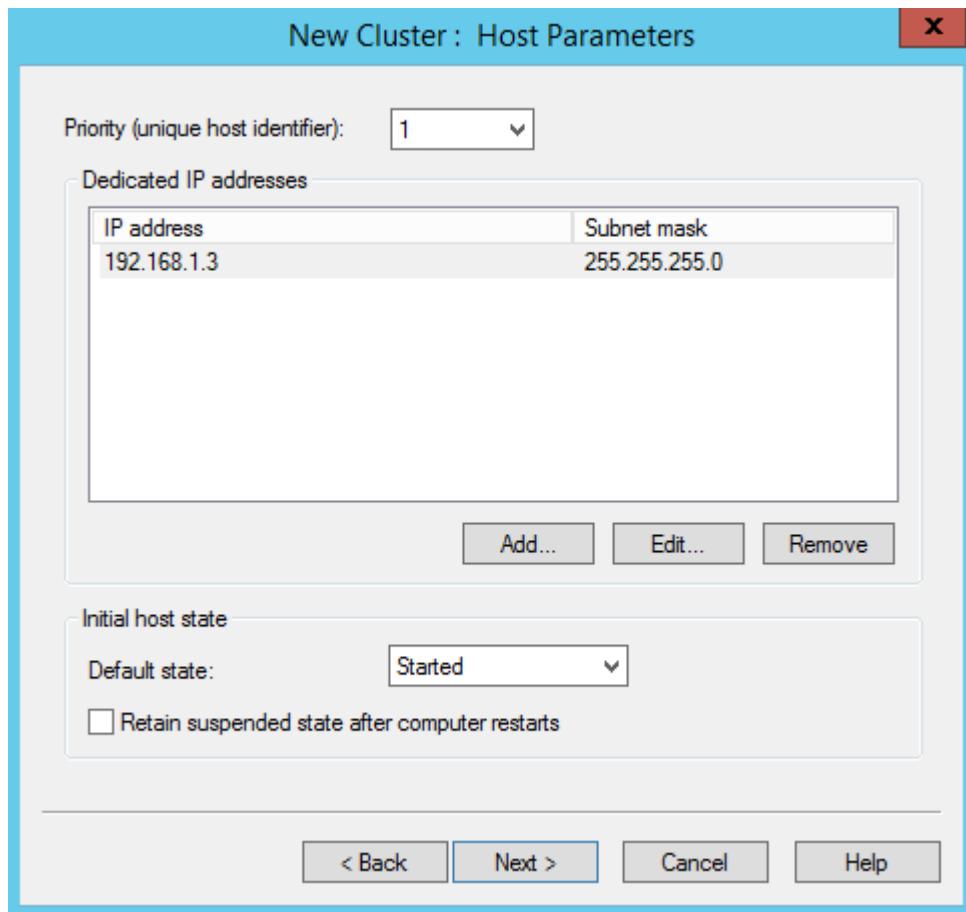
- Trong cửa sổ Network Load Balancing Manager, click chuột phải tại Network Load Balancing Cluster, chọn New Cluster.



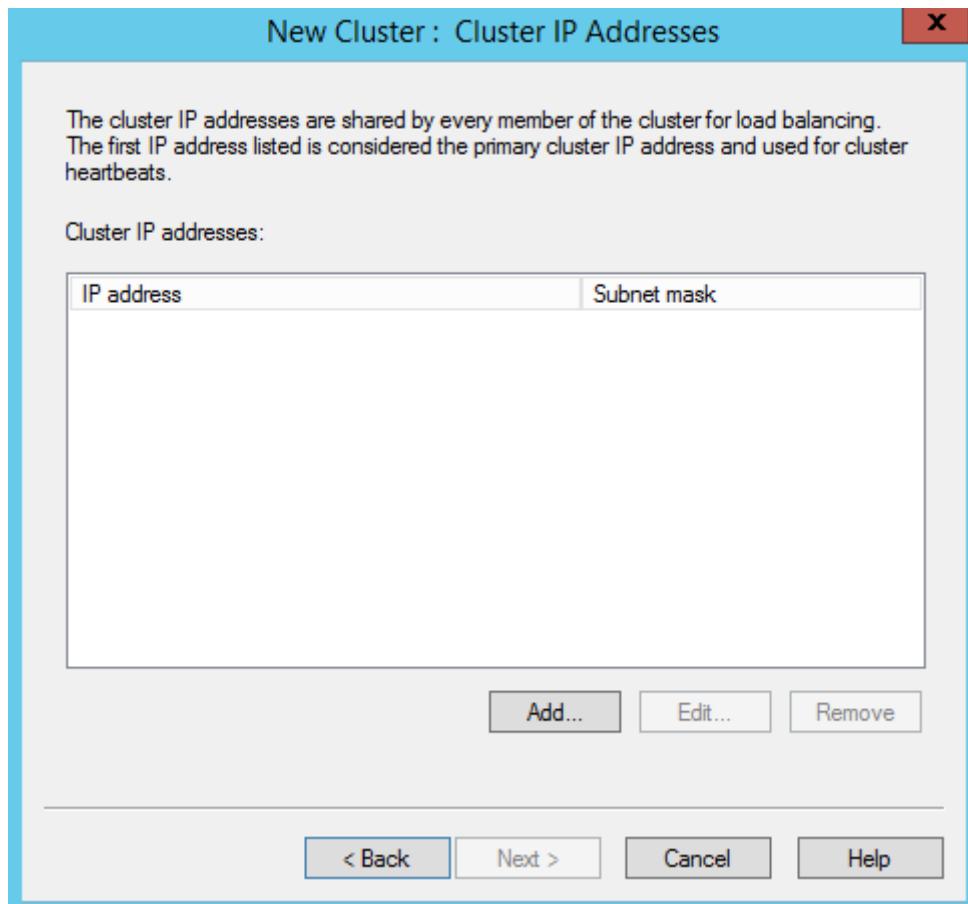
- Trong cửa sổ **New Cluster : Connect** , tại mục **Host** , nhập vào địa chỉ IP **192.168.1.3** (IP address của máy *BKAP-SRV12-01*) , click vào **Connect**.



- Tại cửa sổ **New Cluster : Host Parameters**, click vào *Next*.

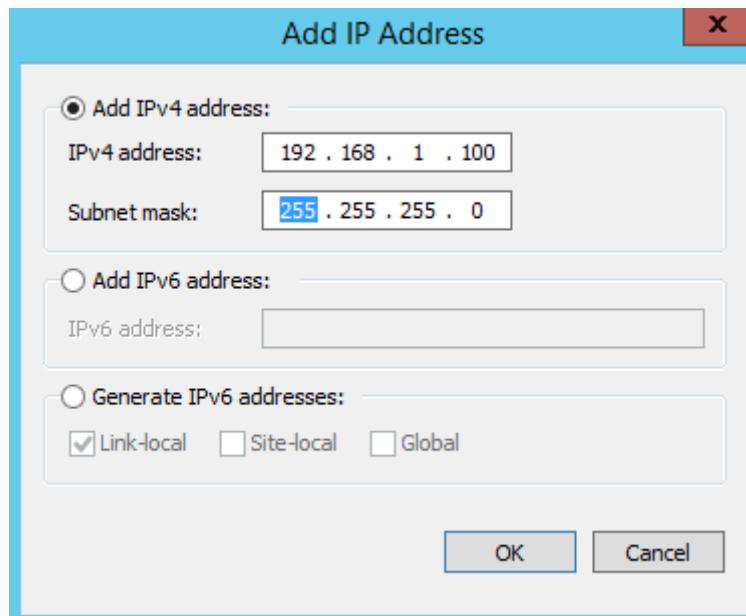


- Tại cửa sổ New Cluster : Cluster IP Address, Click vào Add...

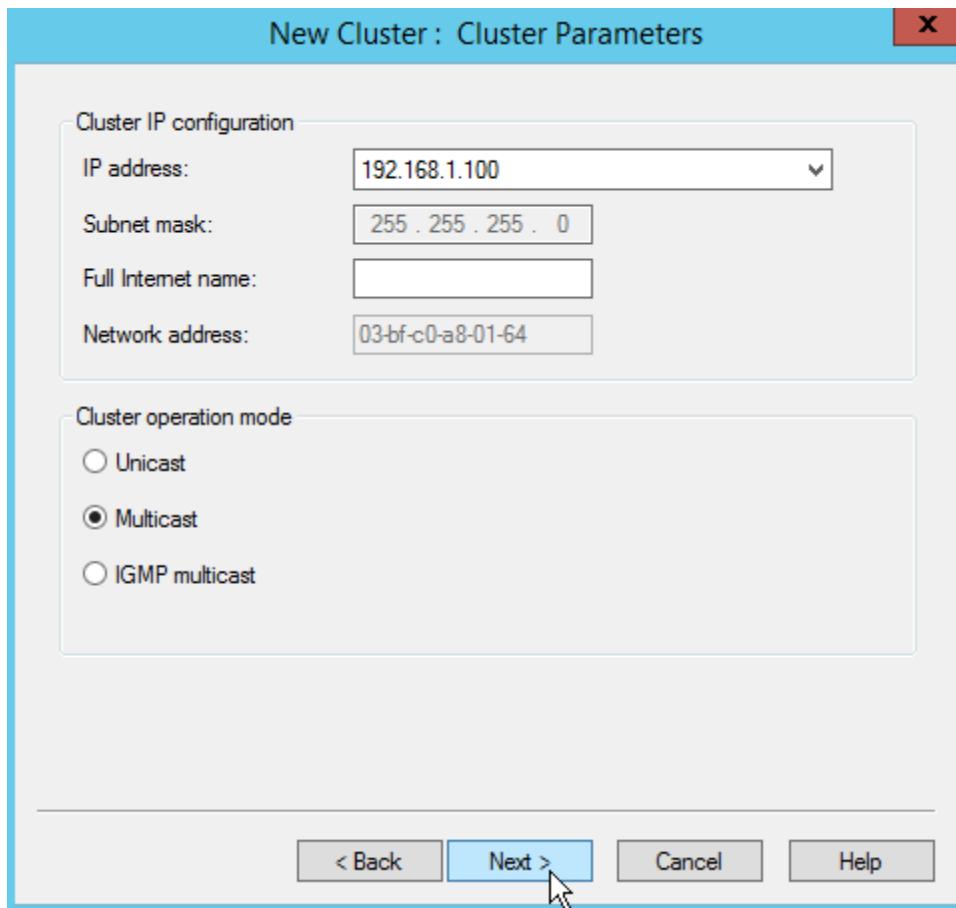


- Tại cửa sổ **Add IP Address**, tại mục **Add IPv4 address**, nhập vào:
 - **IPv4 address:** **192.168.1.100**
 - **Subnet mask:** **255.255.255.0**

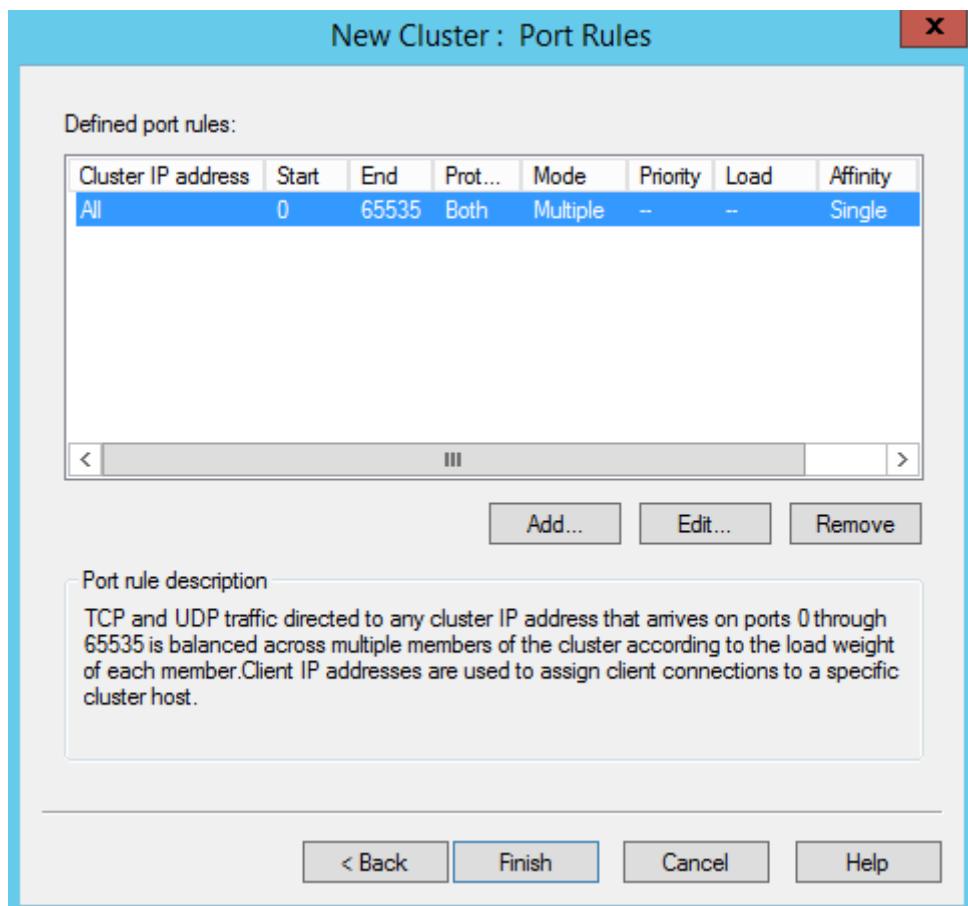
=> **OK.**



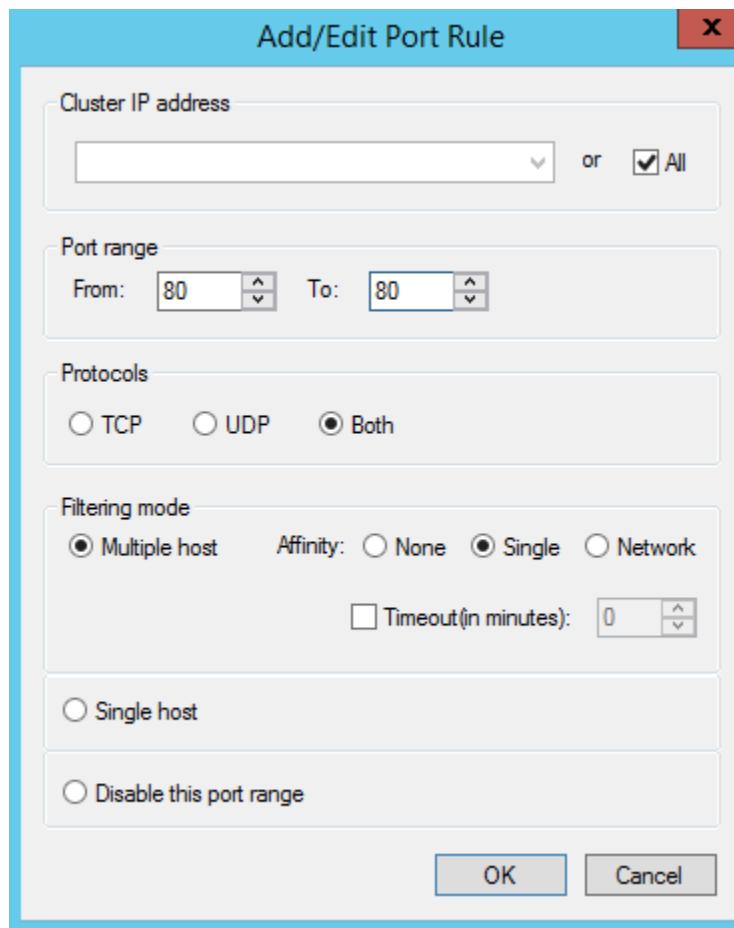
- Tại cửa sổ **New Cluster : Cluster Parameters**, tại mục **Cluster operation mode**, chọn vào **Multicast**. **Next**.



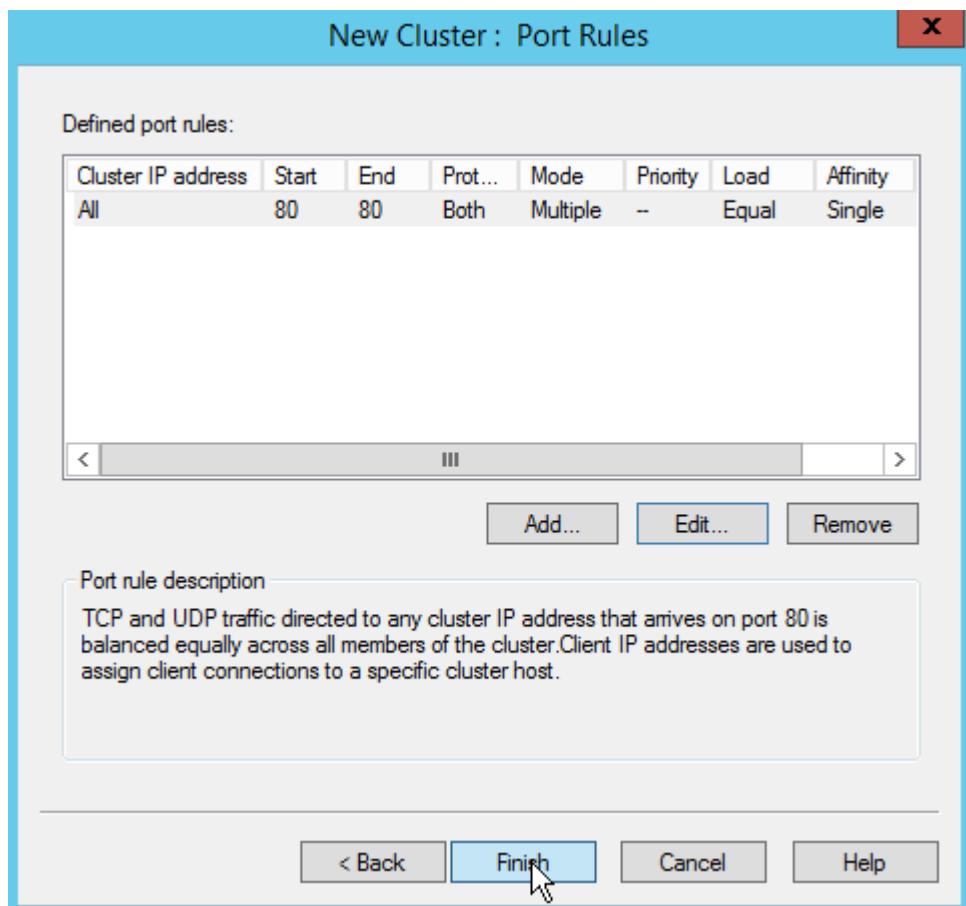
- Tại cửa sổ New Cluster : Port Rules, click vào Edit.



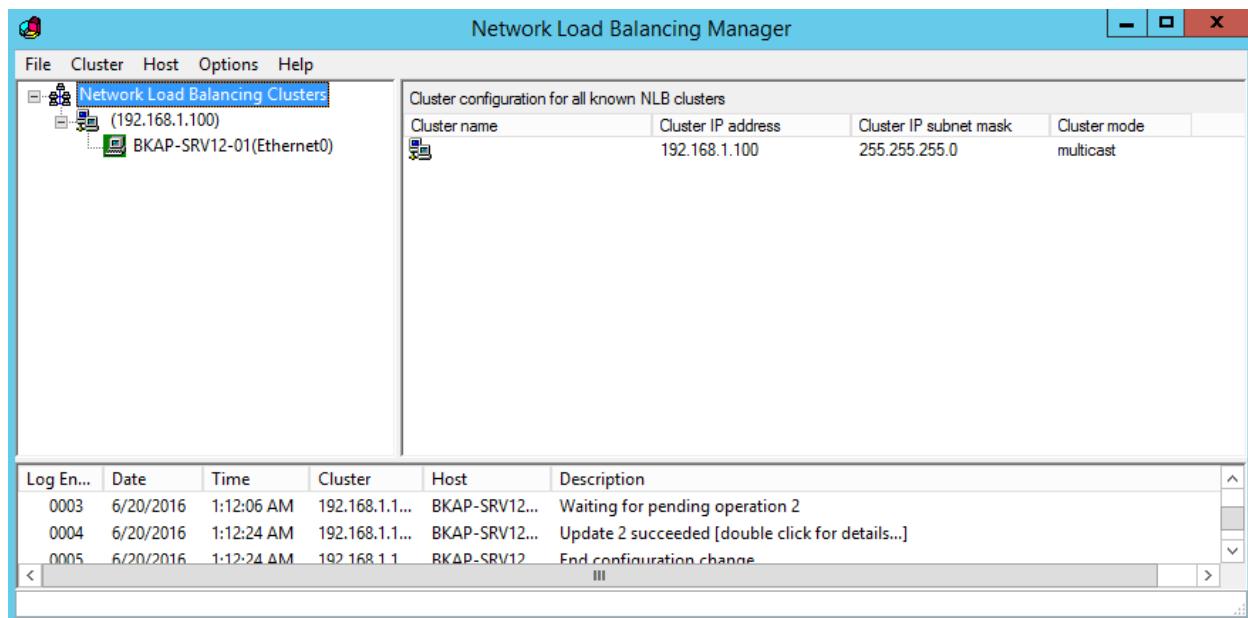
- Tại cửa sổ **Add/Edit Port Rule**, tại mục **Port range**, nhập vào Port : **80**.
 - Kiểm tra **Filtering mode** : **Multiple host** và **Single**.
 - Click vào **OK**.



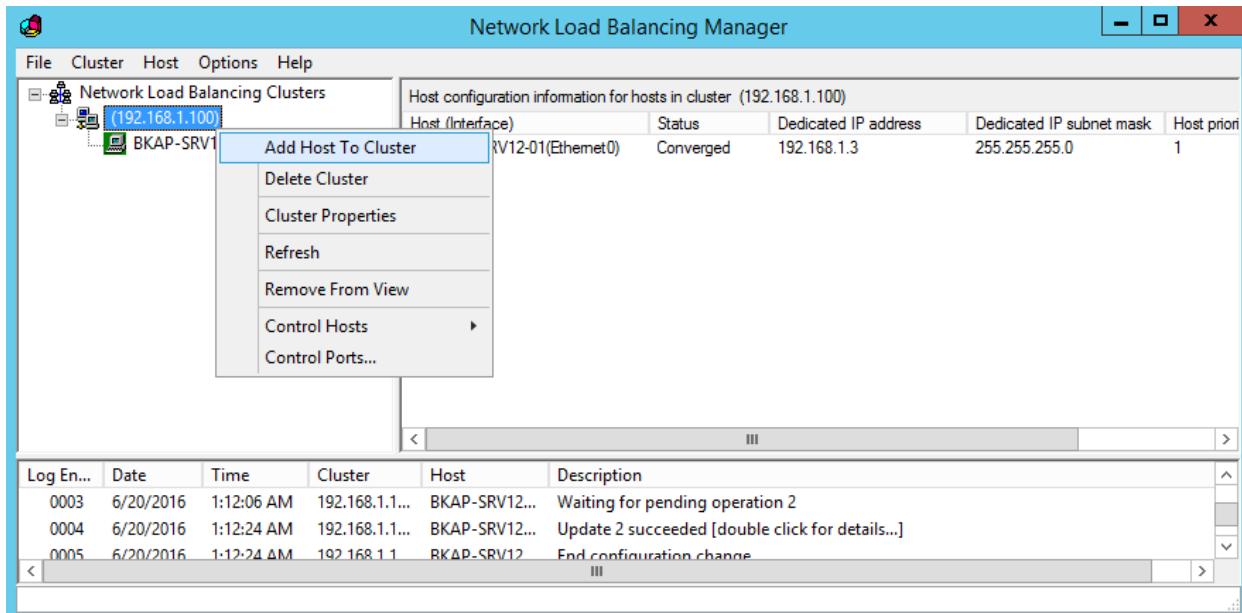
- Click vào **Finish**.



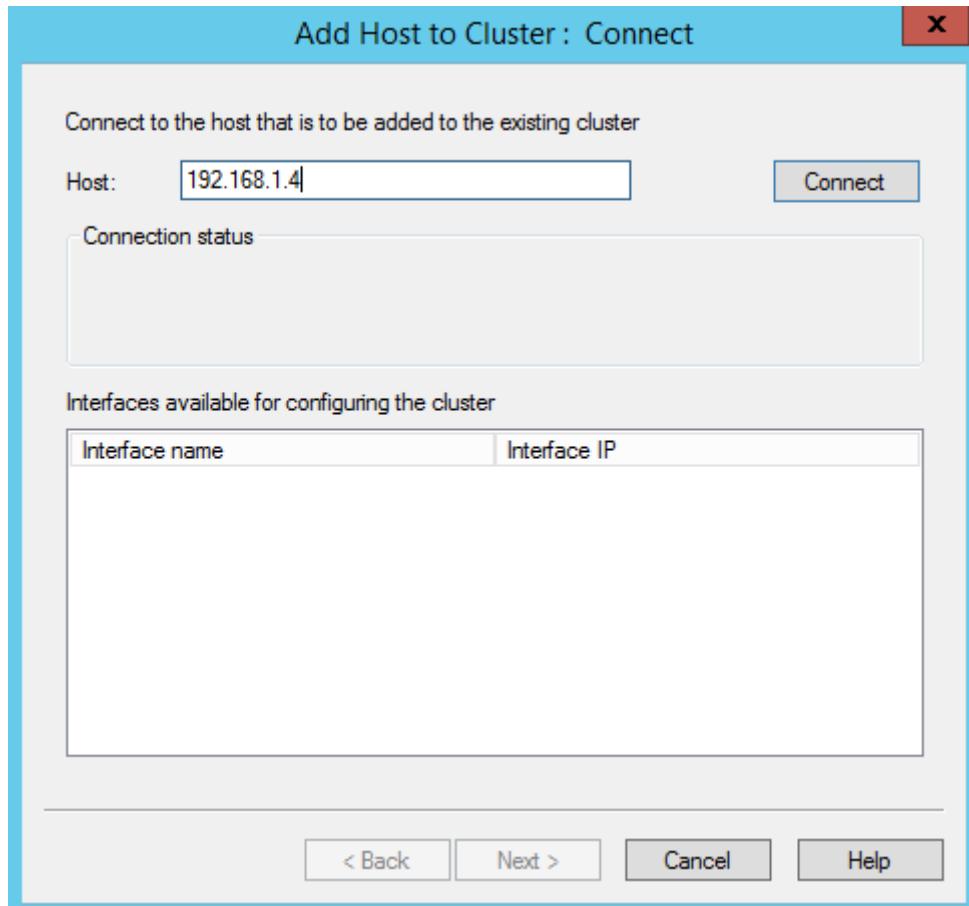
- Kiểm tra lại cấu hình.



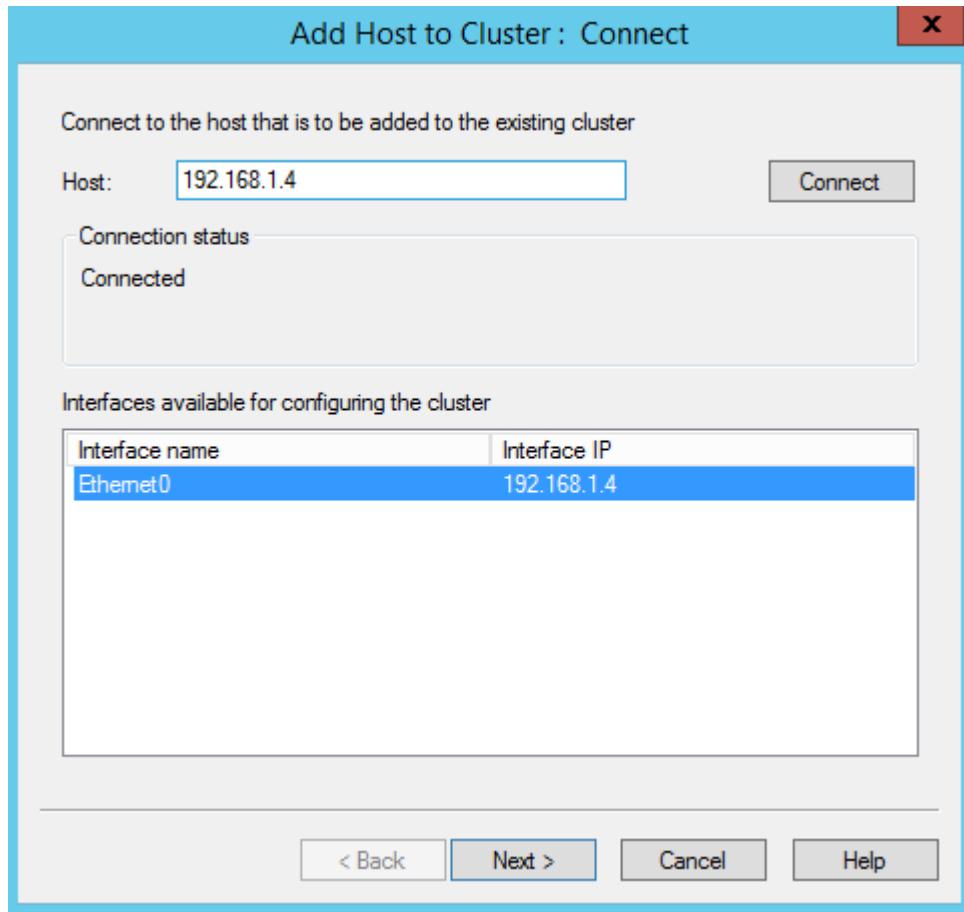
- Tại cửa sổ **Network Load Balancing Manager**, click chuột phải tại host **192.168.1.100** , chọn **Add Host To Cluster**.



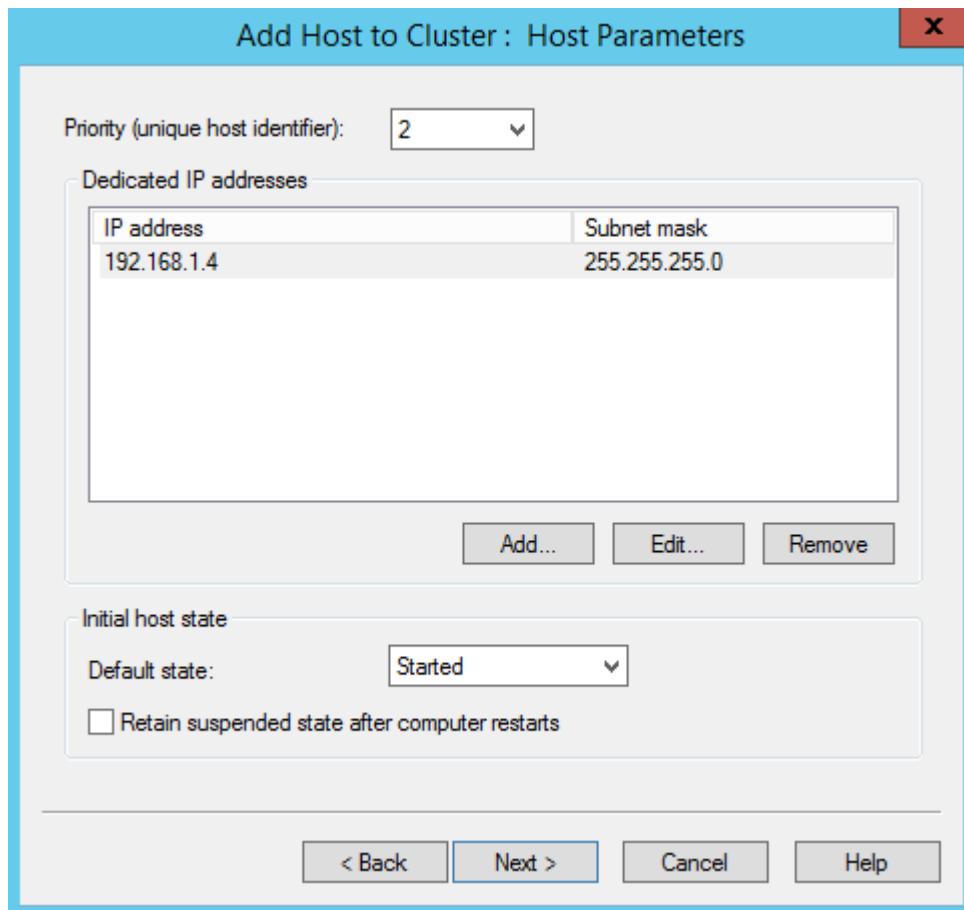
- Tại cửa sổ **Add Host to Cluster : Connect**, tại mục **Host**, nhập vào **192.168.1.4**, click vào **Connect**.



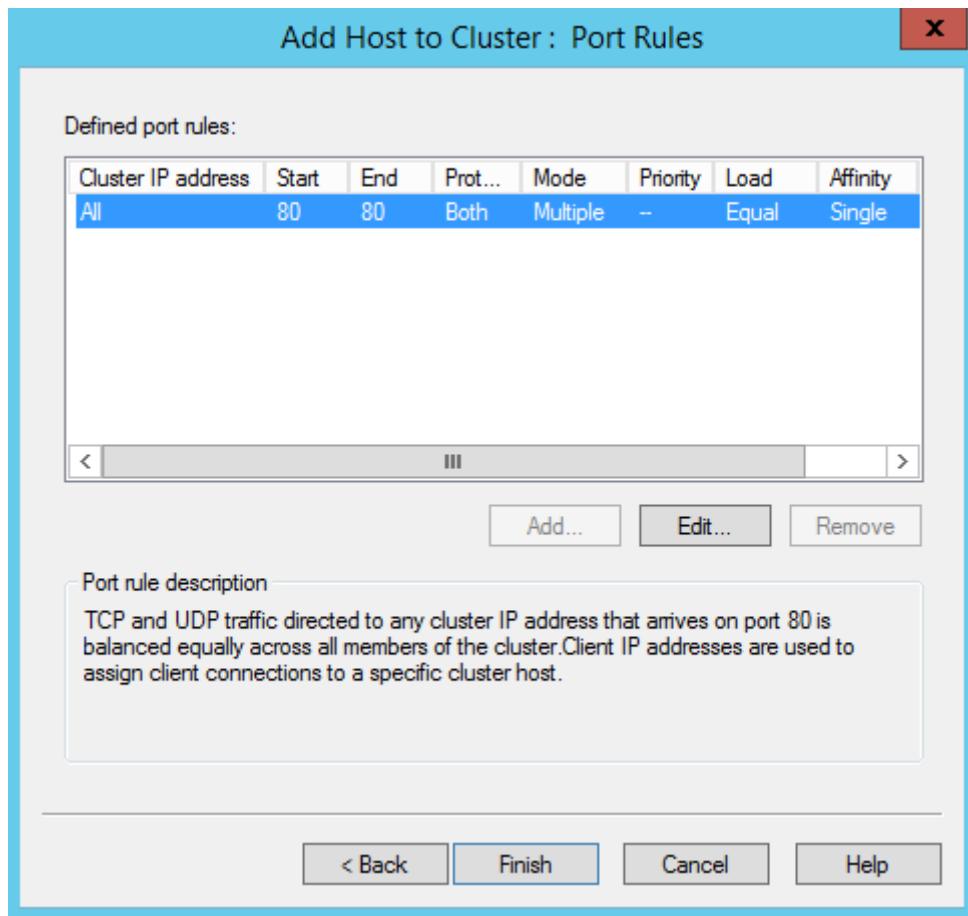
- Click vào Next.



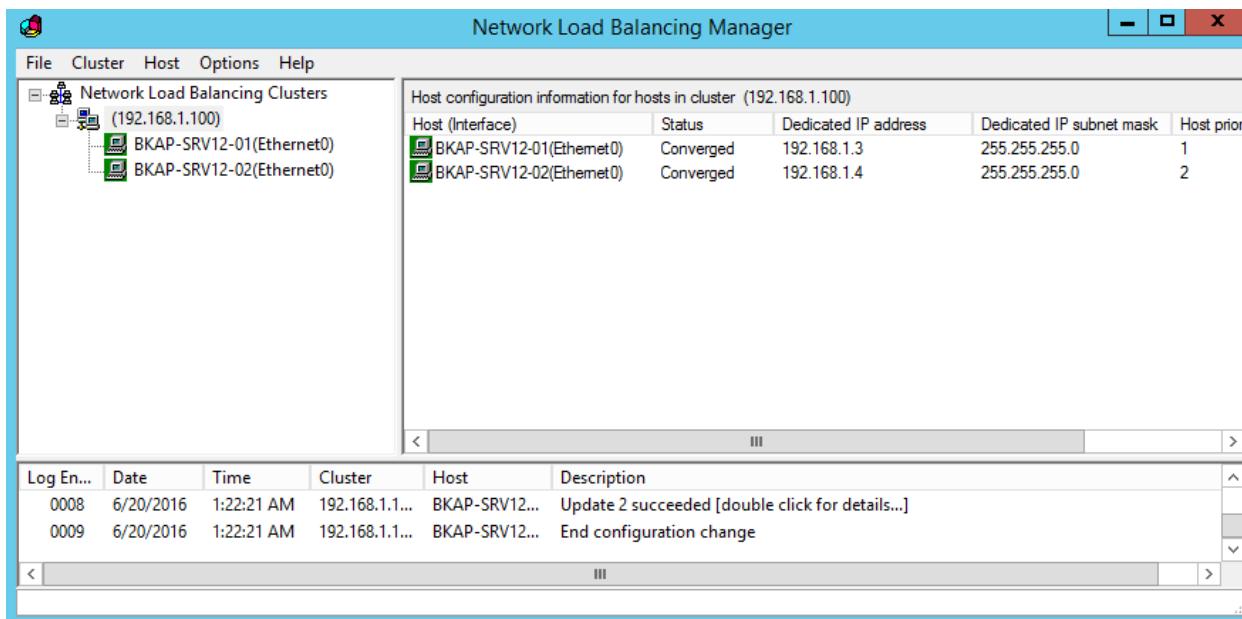
- Tại cửa sổ **Add Host to Cluster : Host Parameters** , click vào Next.



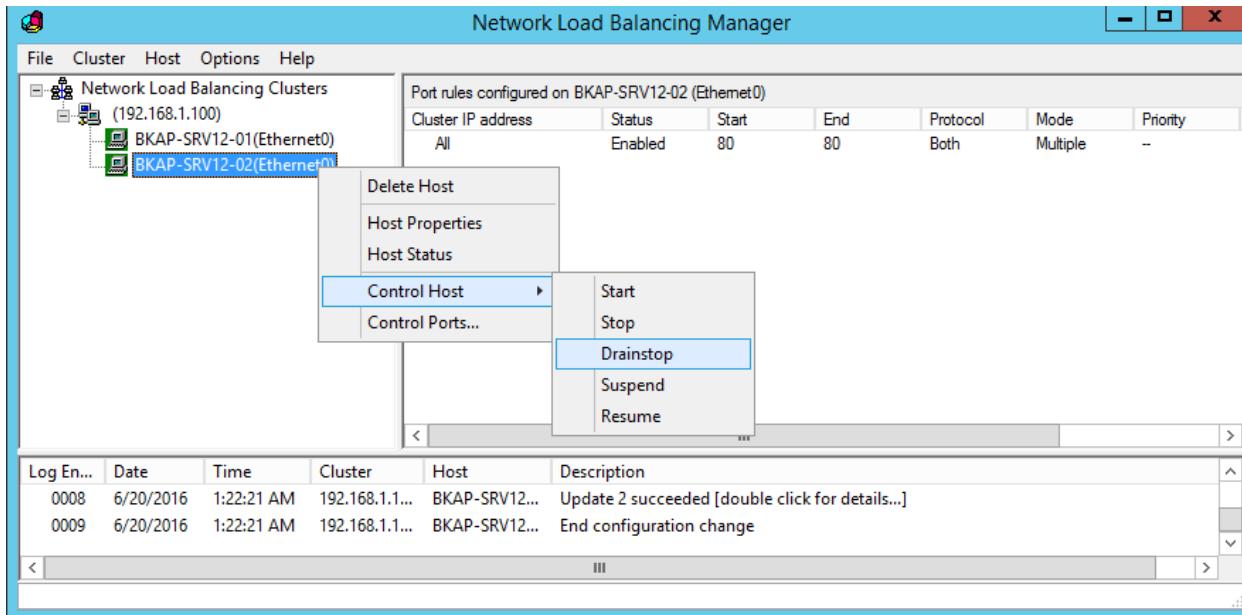
- Tại cửa sổ **Add Host to Cluster : Port Rules**, click vào **Finish**.



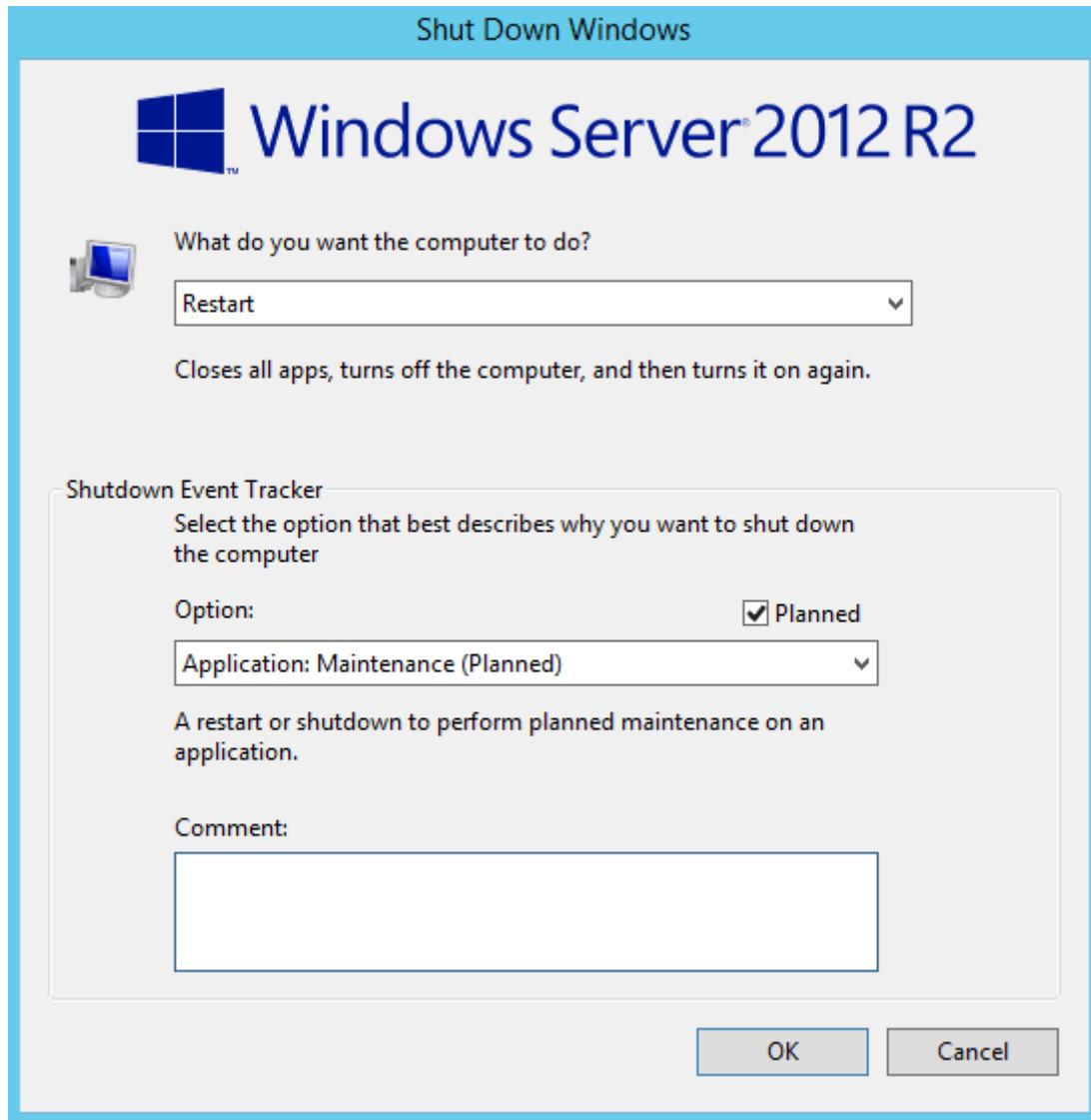
- Kiểm tra cấu hình.



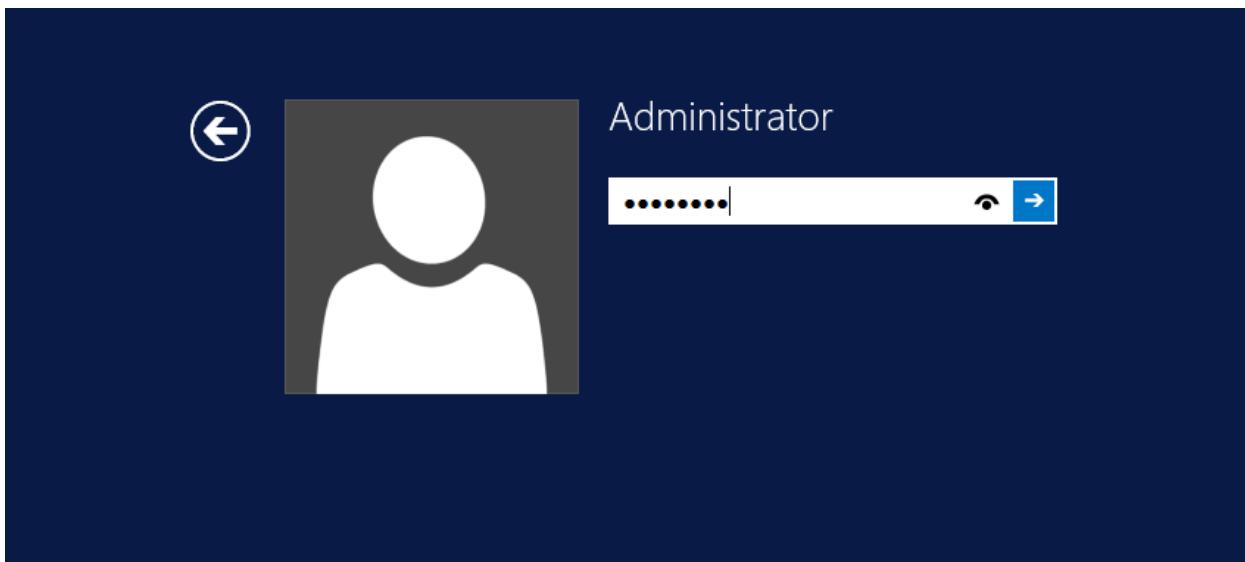
- Tại cửa sổ **Network Load Balancing Manager**, click chuột phải tại **BKAP-SRV12-02(Ethernet0)** , chọn **Control Host / Drainstop**.



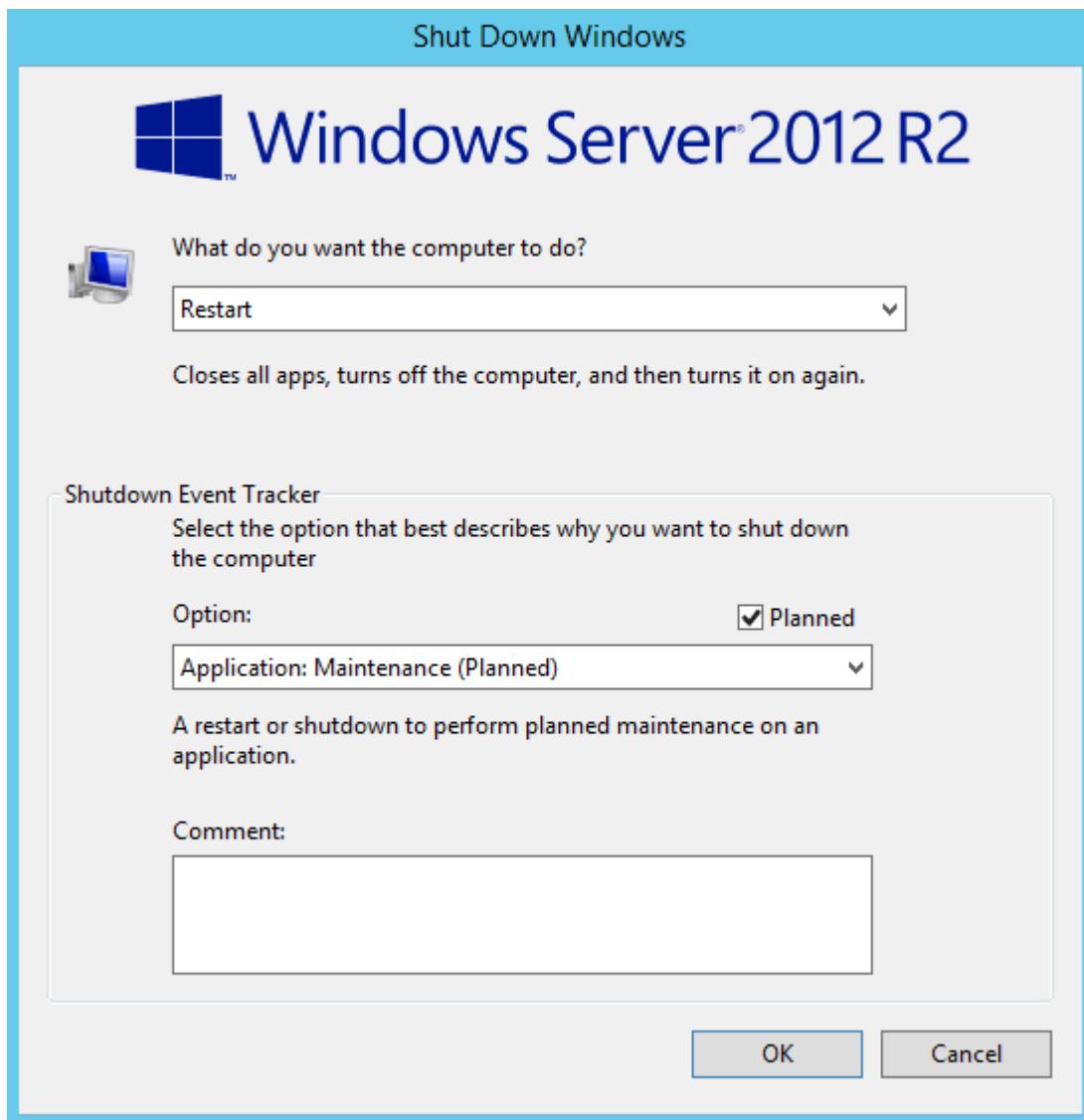
- Sau khi cấu hình dịch vụ ta khởi động lại hệ thống (chỉnh Options ở dạng **Application: Maintenance (Planned)**).



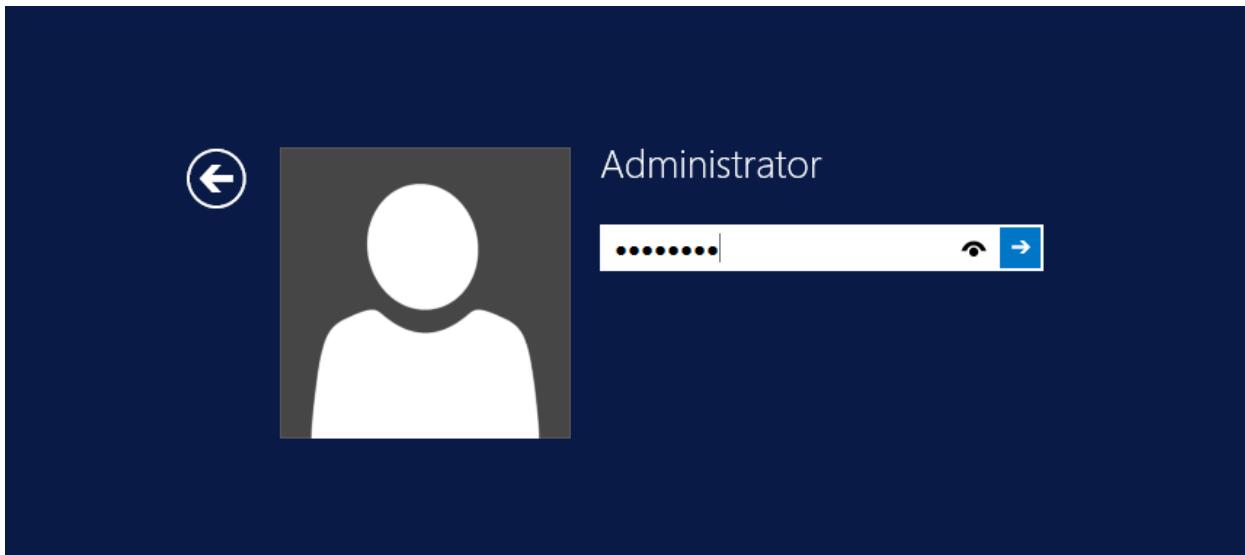
- Đăng nhập lại vào hệ thống.



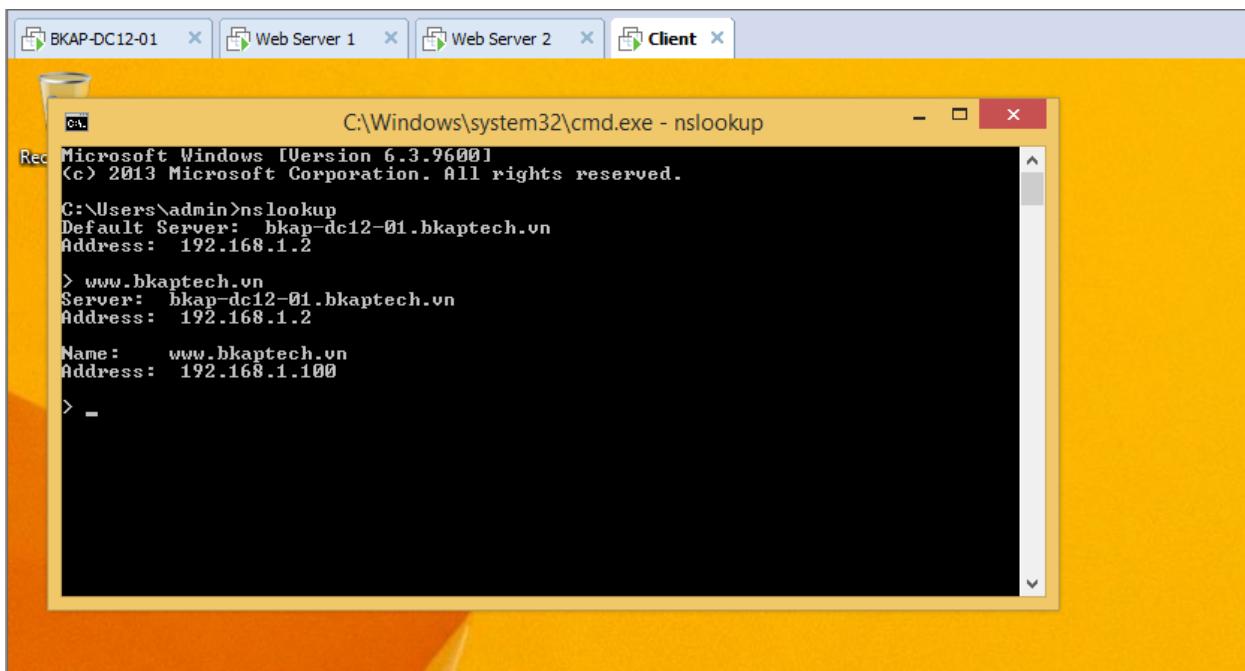
- Chuyển sang máy BKAP-SRV12-02, khởi động lại hệ thống. (*tương tự BKAP-SRV12-01*).



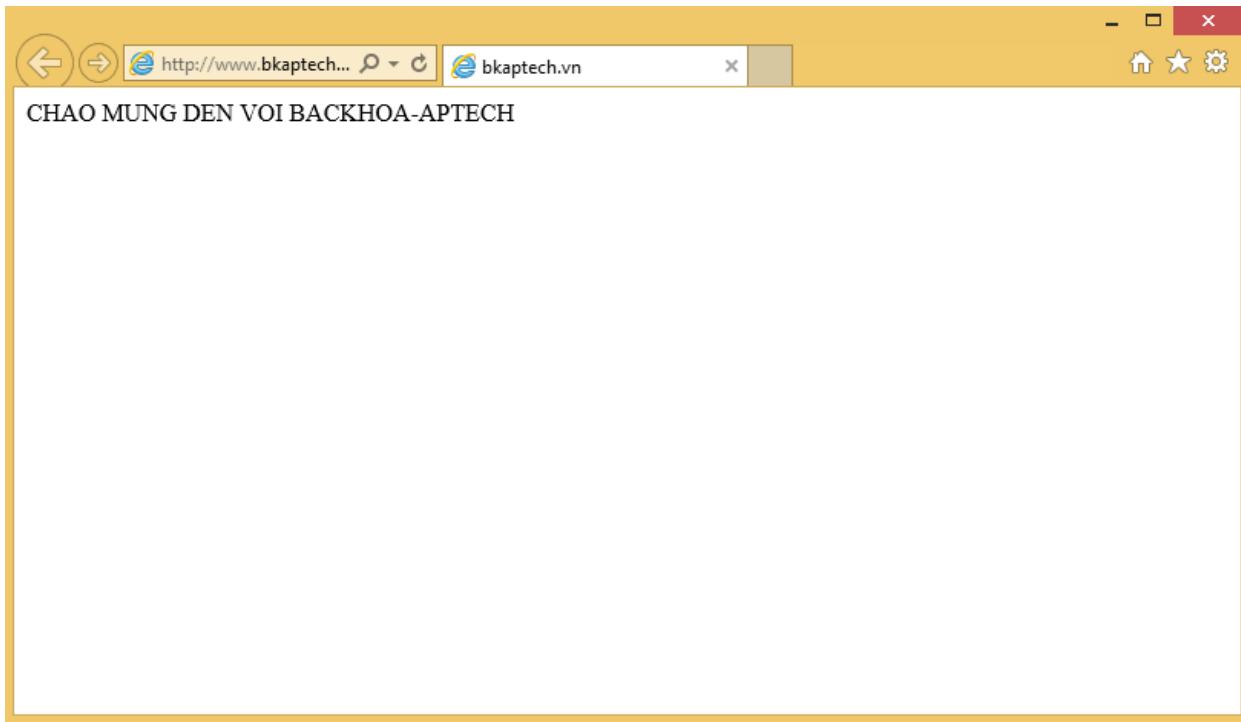
- Đăng nhập lại hệ thống:



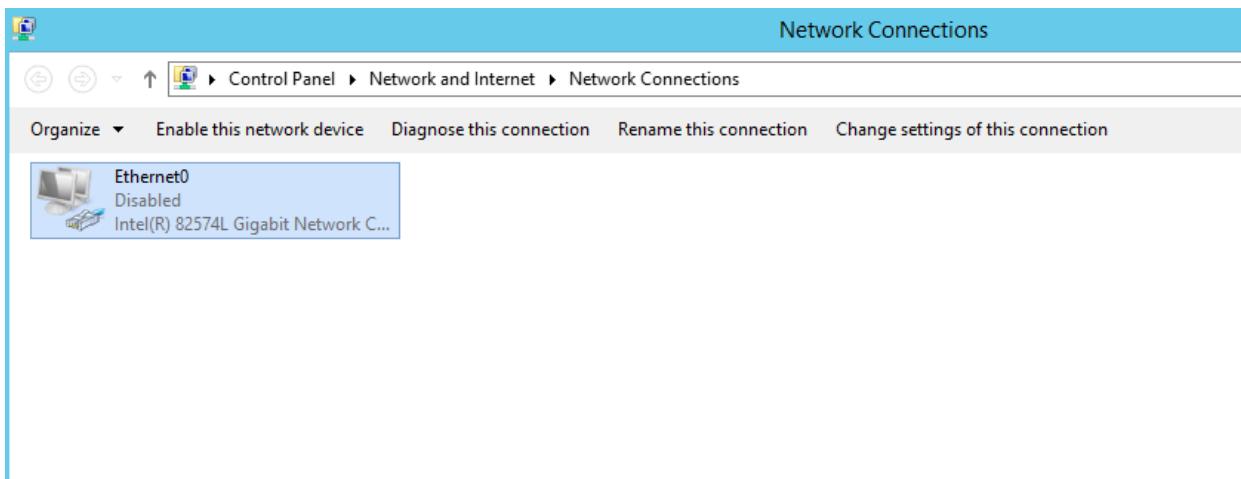
- Chuyển sang máy *BKAP-WRK08-01*, truy cập Website để kiểm tra.
 - Kiểm tra phân giải DNS.



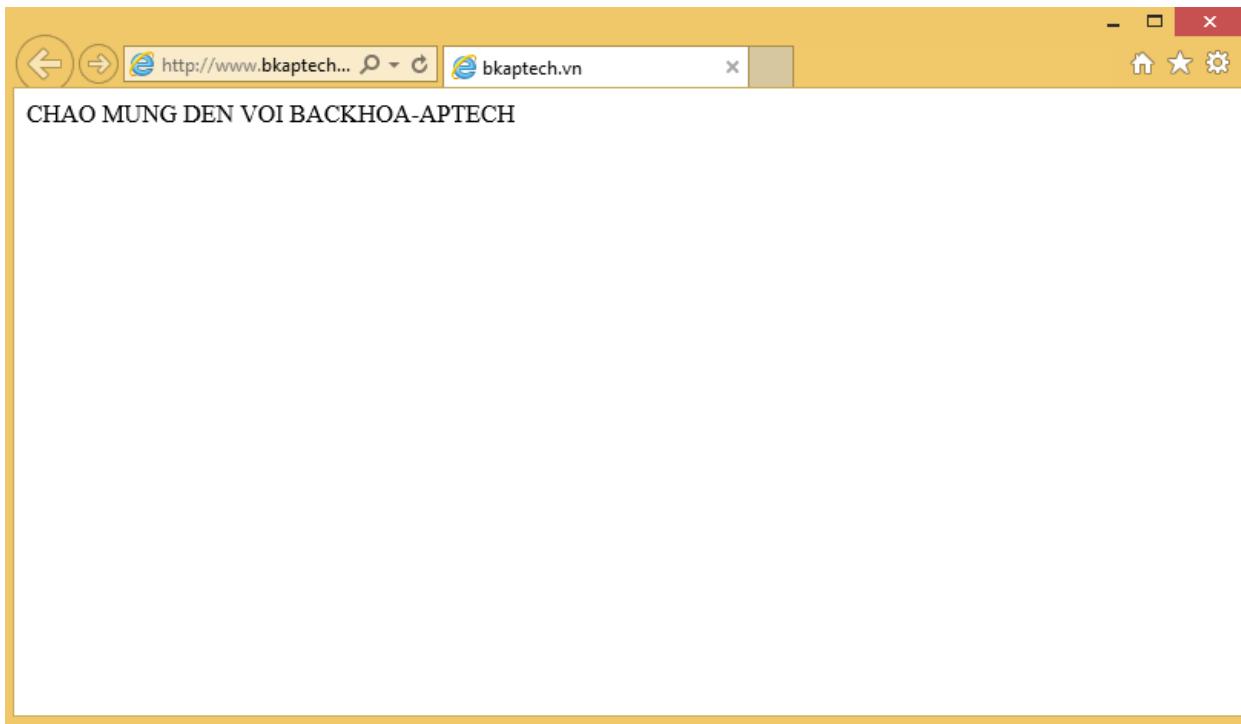
- Truy cập trang Web:



- Chuyển qua máy Server BKAP-SRV12-02, tắt card mạng.



- Chuyển qua máy *Client*, truy cập Website để kiểm tra.



Bài 8:

TRIỀN KHAI FAILOVER CLUSTERING

Các nội dung chính được đề cập:

- ✓ Cài đặt và cấu hình Failover Clustering.

8. Cấu hình Failover Clustering

1. Yêu cầu bài Lab:

+ Trên Server *BKAP-DC12-01*:

- Cài đặt và cấu hình iSCSI Server.
- Tạo tài khoản người dùng theo phòng ban **IT, Sale**.

+ Trên Server *BKAP-SRV12-01* và *BKAP-SRV12-02*:

- Cấu hình nhận ổ từ iSCSI Server.
- Cài đặt và cấu hình Failover Clustering.

- Cài đặt **File Server** và phân quyền truy cập thư mục.
- + Kiểm tra sau khi thiết lập:
 - Đứng trên **Client** truy cập vào **File Server** chia sẻ theo địa chỉ :
<\\192.168.1.100>
 - Tắt máy **BKAP-SRV12-01**, trên **Client** vẫn truy cập **File Server** thành công.

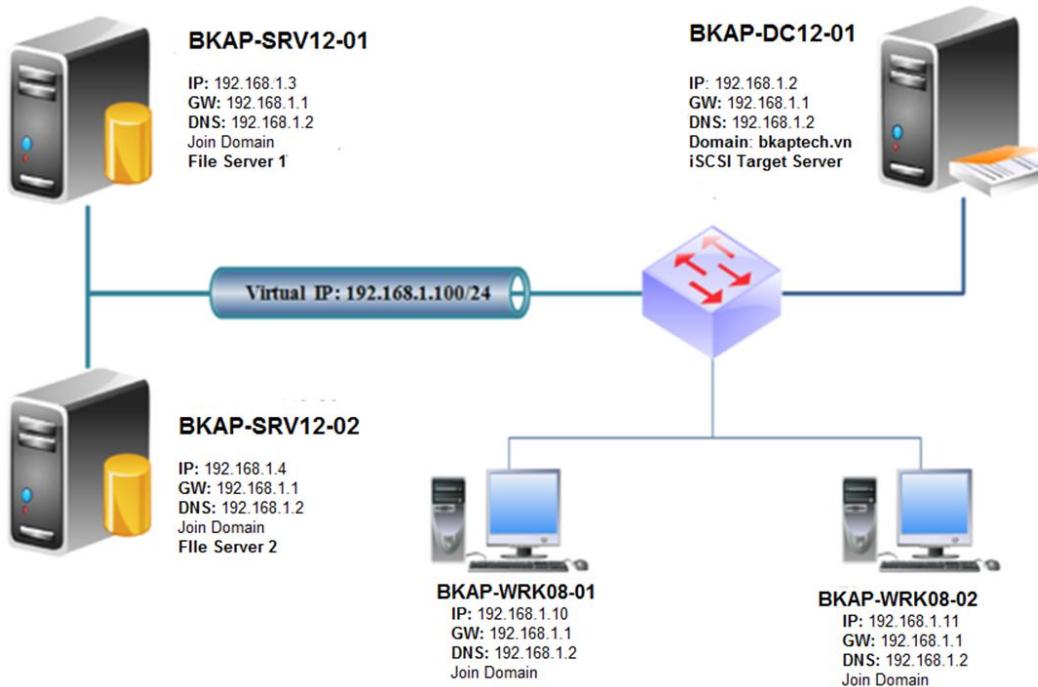
2.Yêu cầu chuẩn bị:

- + Máy Server **BKAP-DC12-01** đã nâng cấp lên **Domain Controller** đã cấu hình **DNS Server** và 1 ổ cứng để cài **iSCSI**.
- + Máy Server **BKAP-SRV12-01** và **BKAP-SRV12-02**.
- + Máy Client **BKAP-WRK08-01**.

3.Mô hình lab:

HỆ THỐNG ĐÀO TẠO CNTT QUỐC TẾ BACHKHOA-APTECH

Cấu hình Failover Clustering

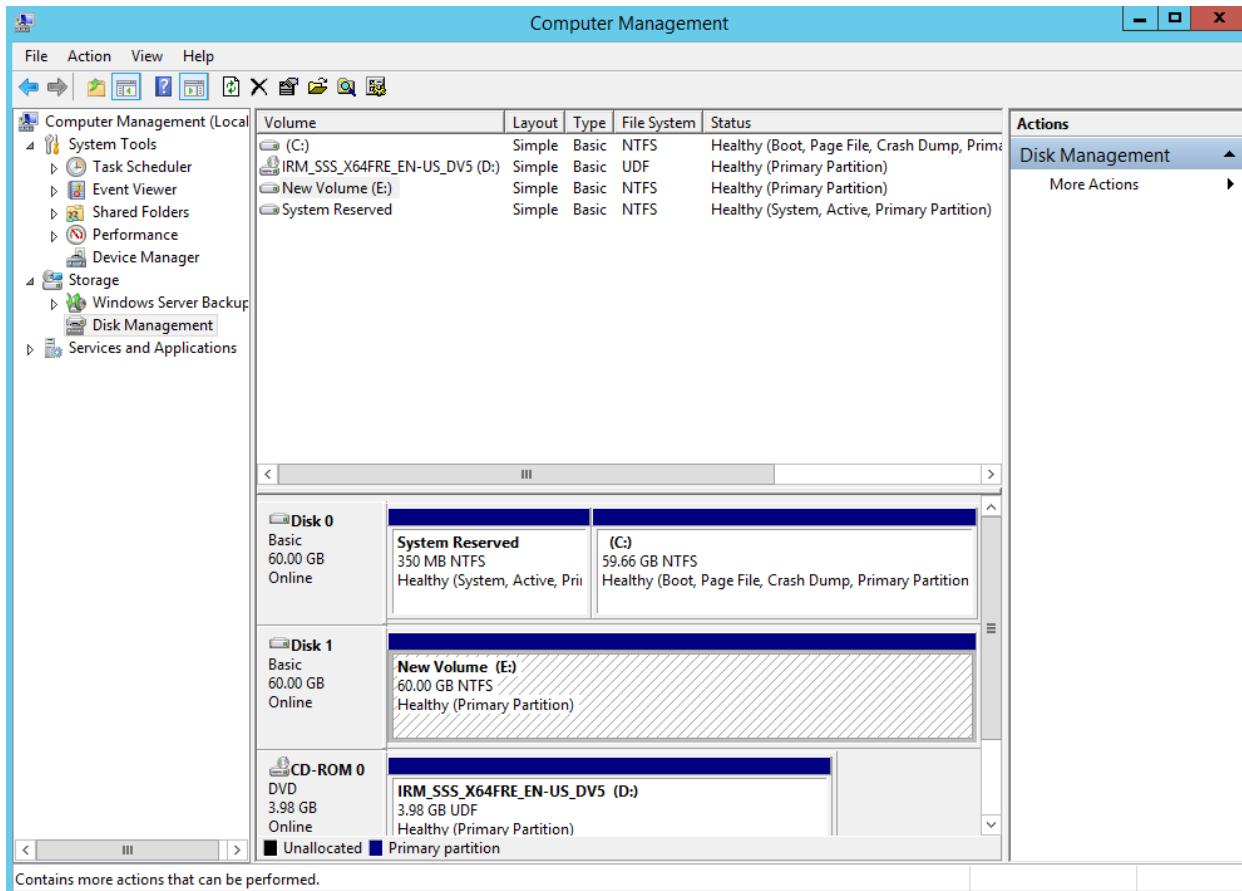


Sơ đồ địa chỉ như sau:

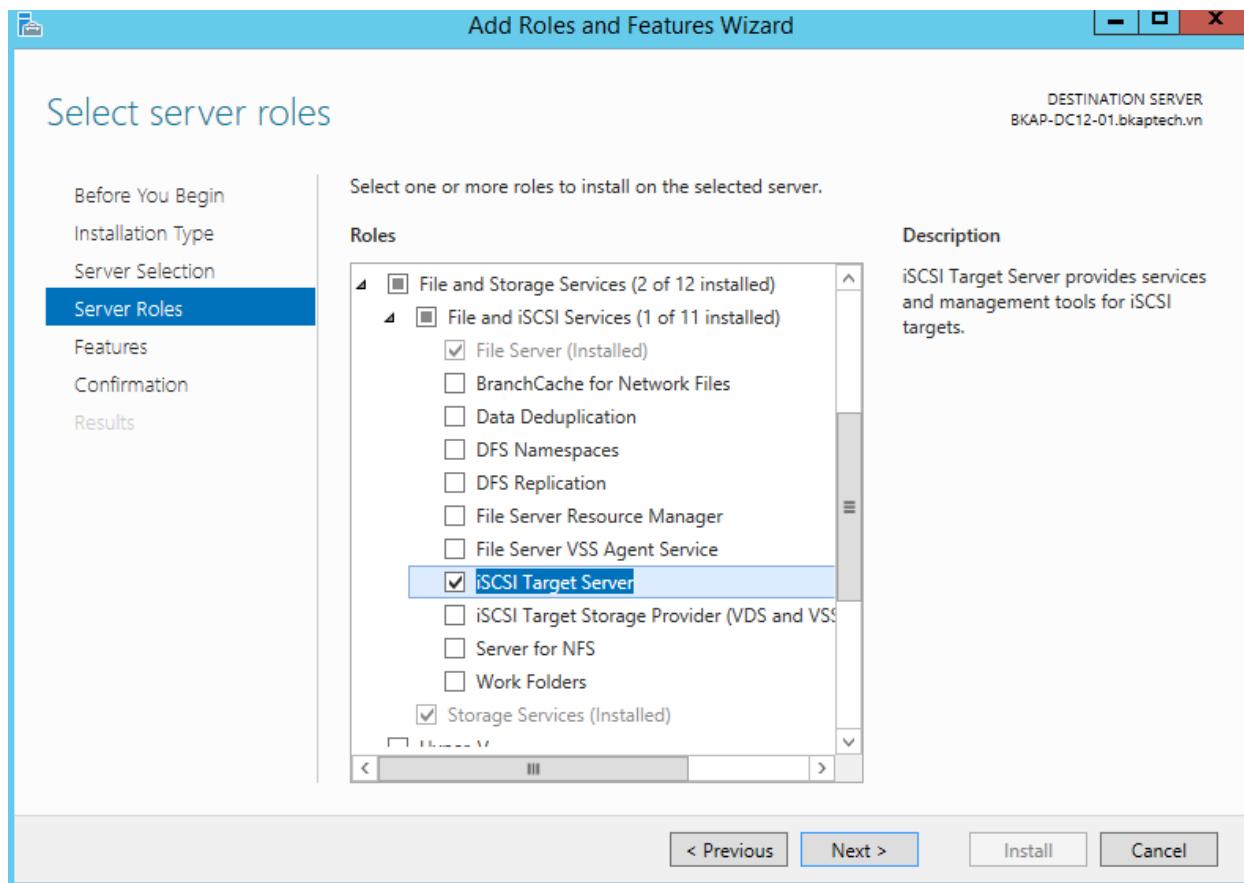
Thông số	DC12-01	SRV12-01	SRV12-02	WRK08-01
<i>IP address</i>	192.168.1.2	192.168.1.3	192.168.1.4	192.168.1.10
<i>Gateway</i>	192.168.1.1	192.168.1.1	192.168.1.1	192.168.1.1
<i>Subnet Mask</i>	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
<i>DNS Server</i>	192.168.1.2	192.168.1.2	192.168.1.2	192.168.1.2

Hướng dẫn chi tiết:

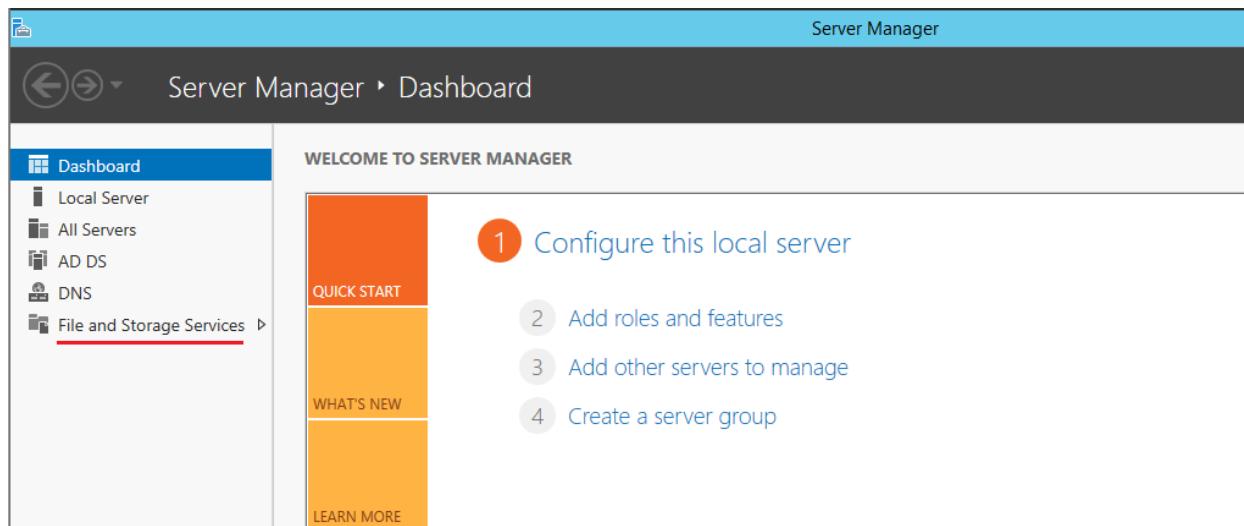
- Trên máy BKAP-DC12-01, add thêm 1 ổ cứng.



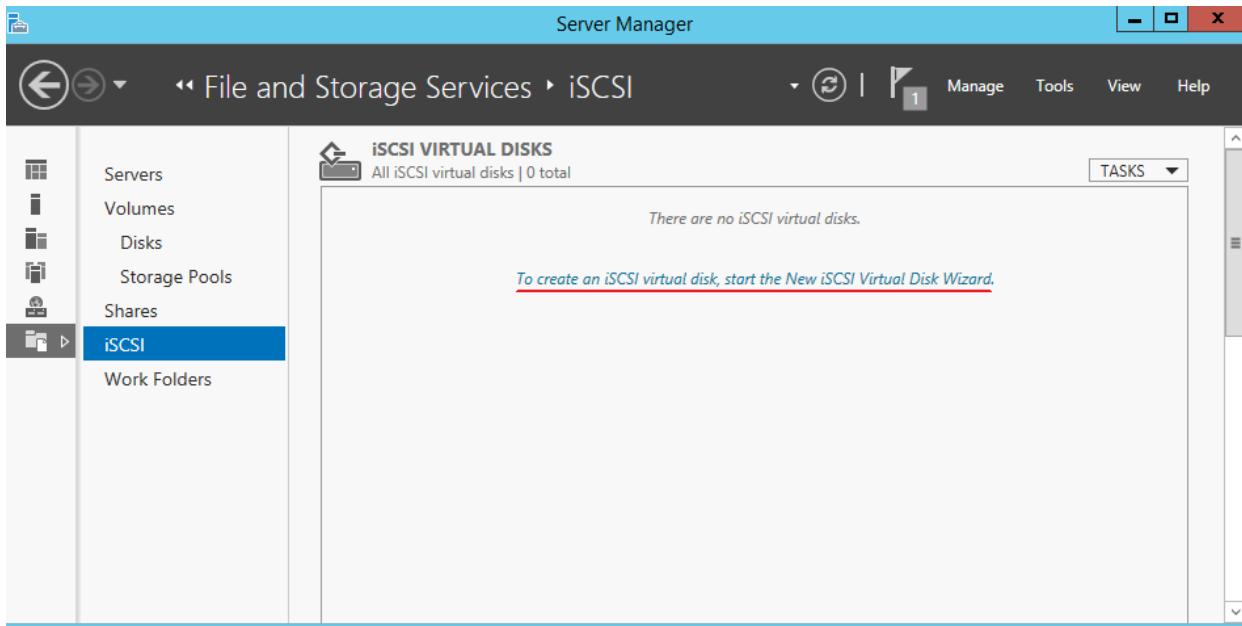
- Cài đặt iSCSI Target Server.



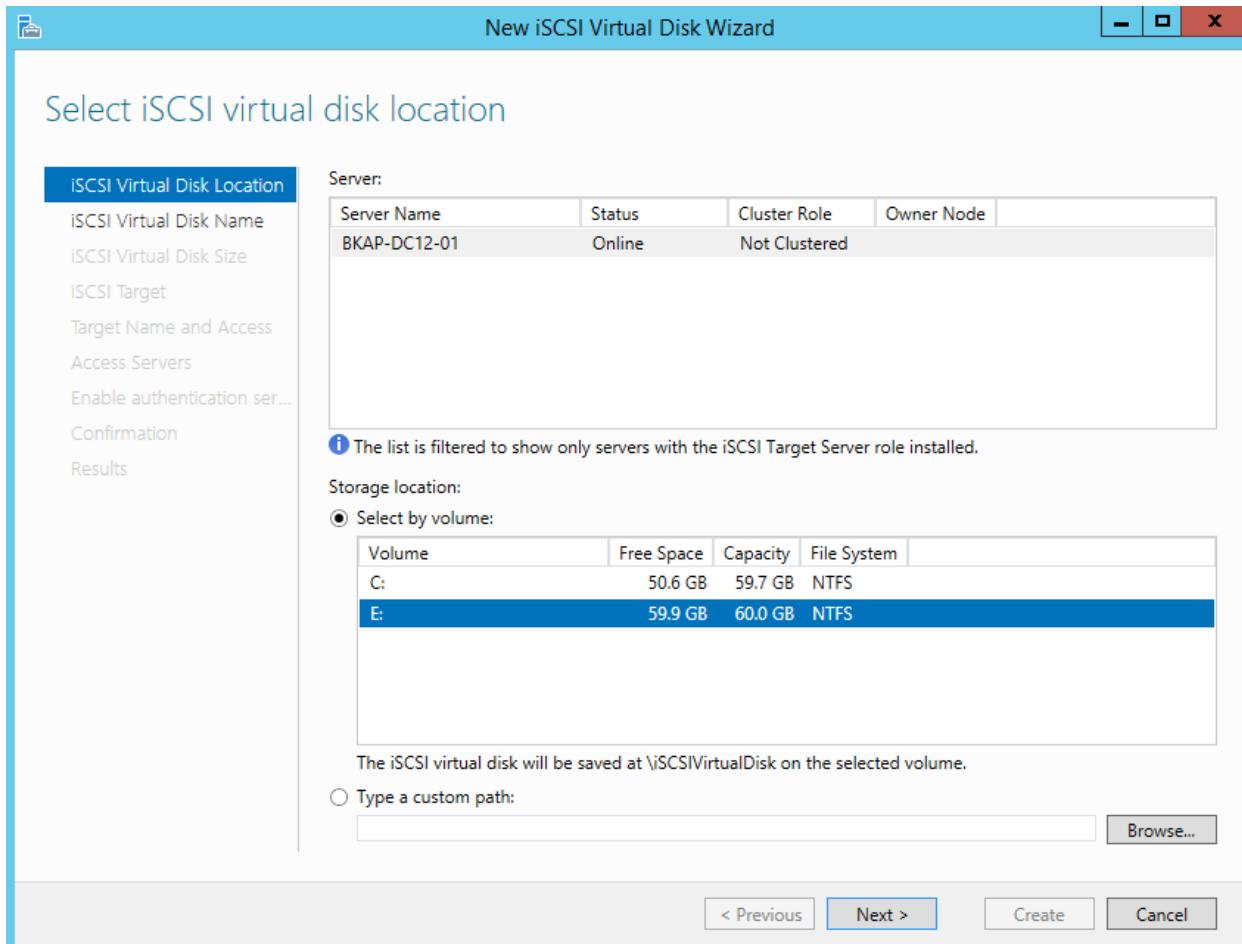
- Trong Server Manager, click chọn vào File and Storage Services.



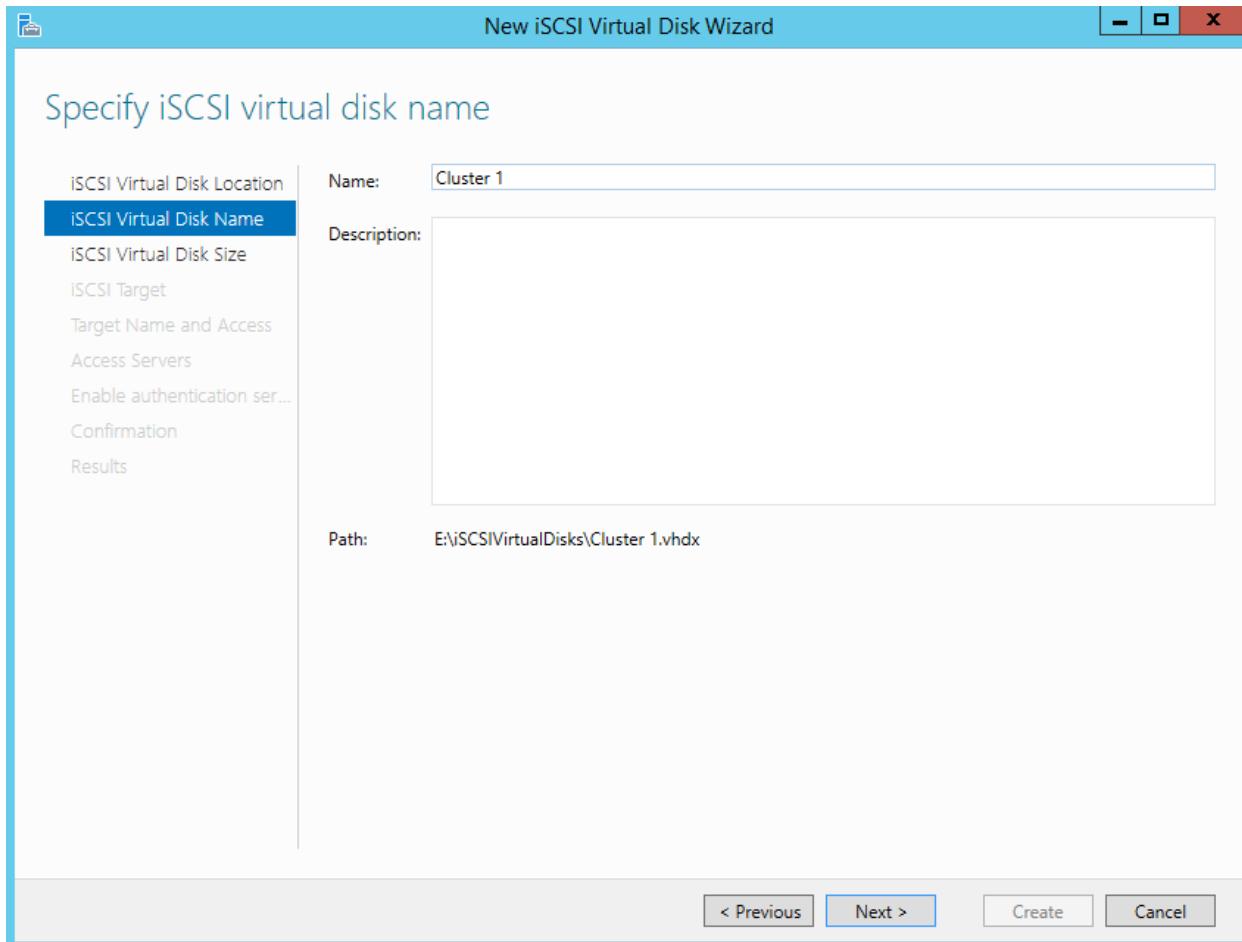
- Chọn vào **iSCSI**, click vào dòng *To Create an iSCSI virtual disk, start the New iSCSI Virtual Disk Wizard.*



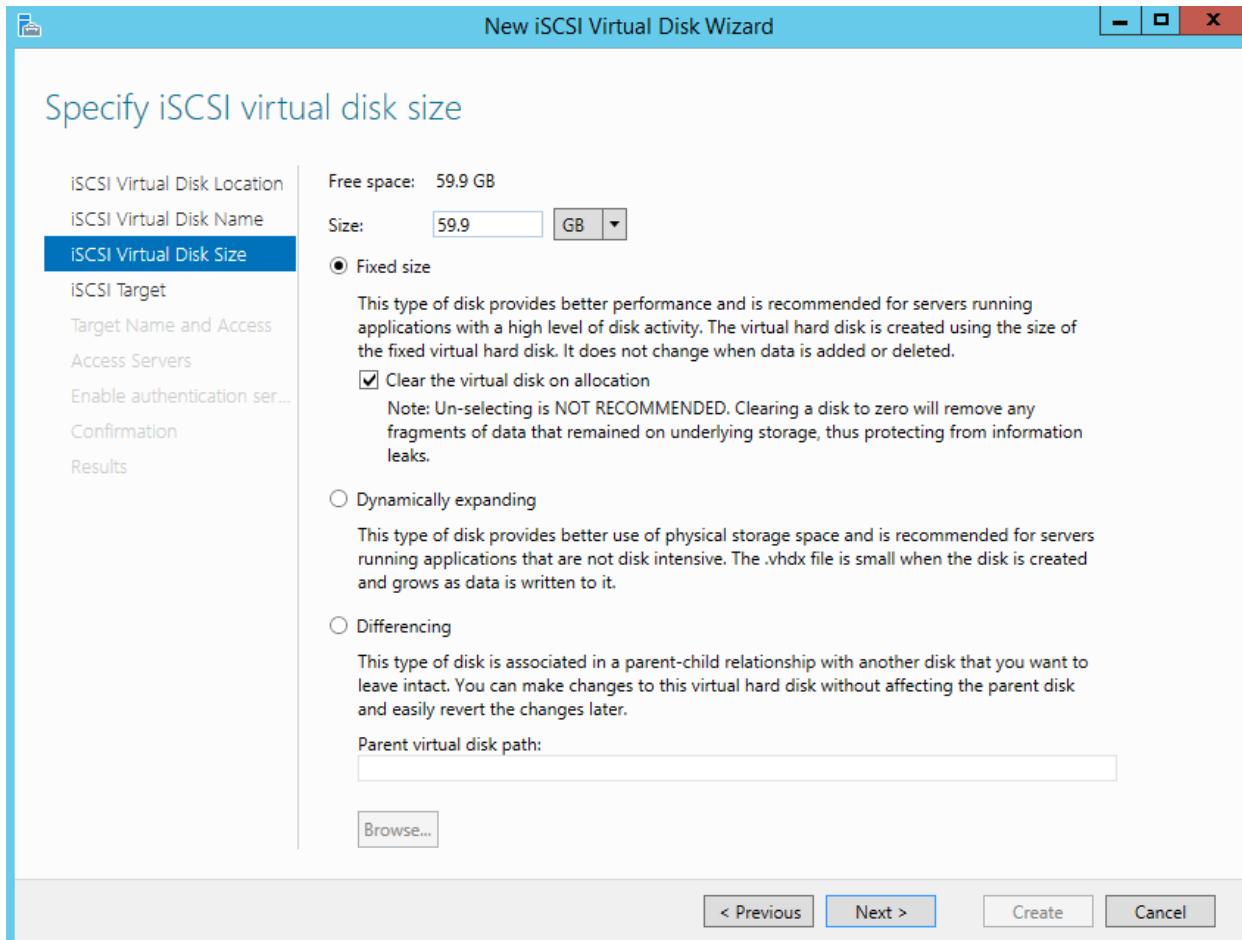
- Tại cửa sổ **Select iSCSI virtual disk location**, chọn vào ô **E** , click vào **Next**.



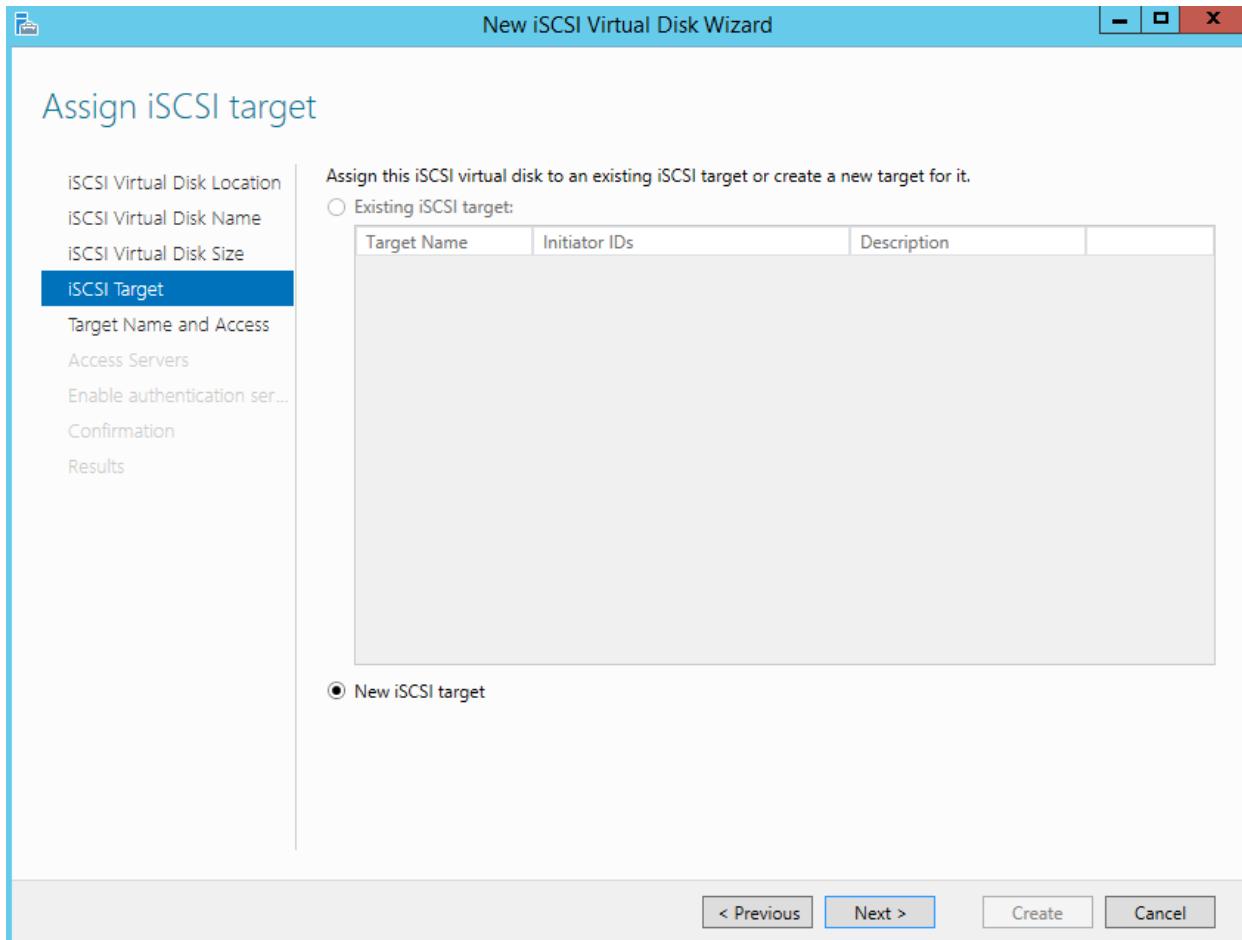
- Tại cửa sổ **Specify iSCSI virtual disk name**, nhập vào tại mục Name: **Cluster 1** , click vào **Next**.



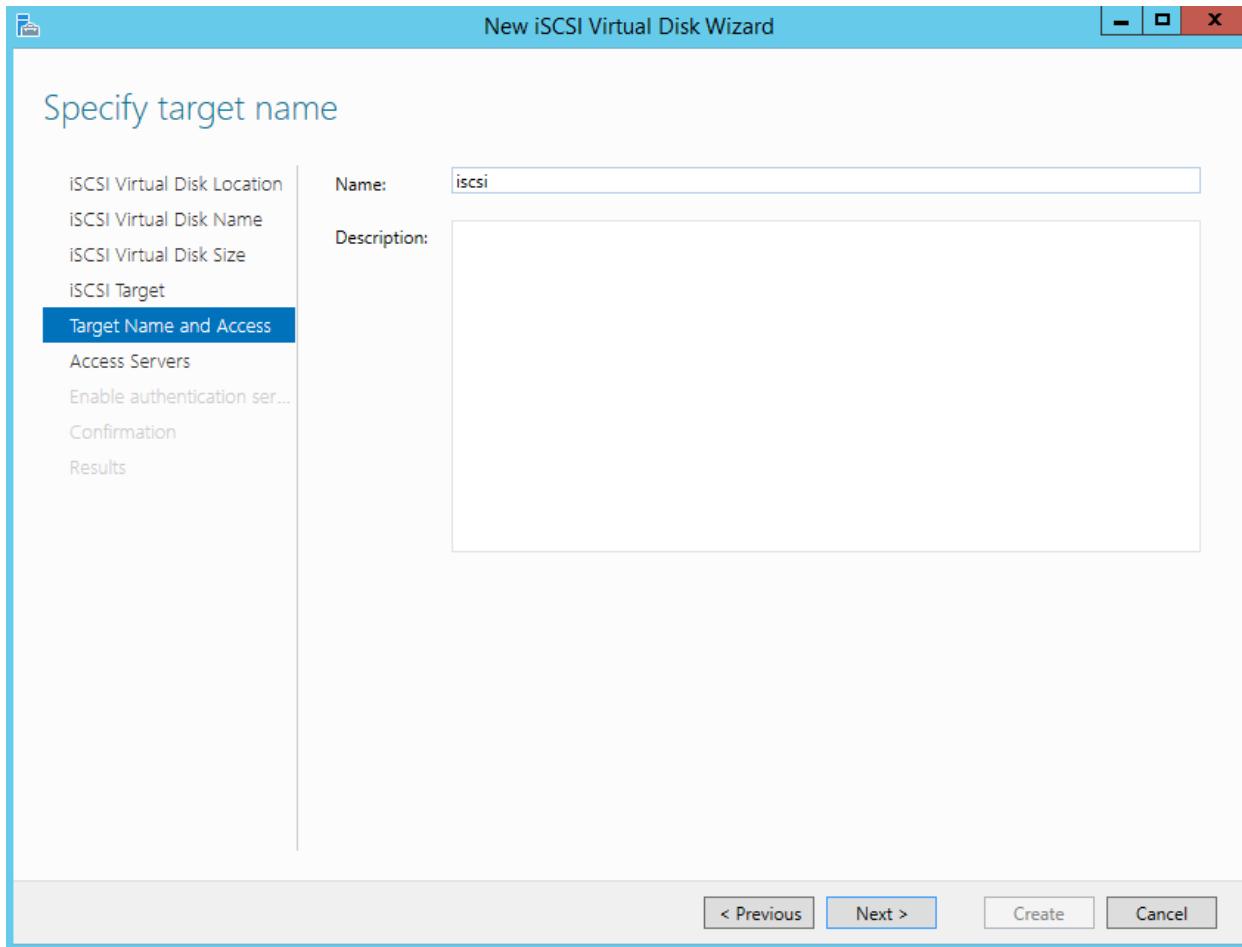
- Tại cửa sổ **Specify iSCSI virtual disk size**, nhập vào dung lượng ổ cứng tại mục **Size** , click vào **Next**.



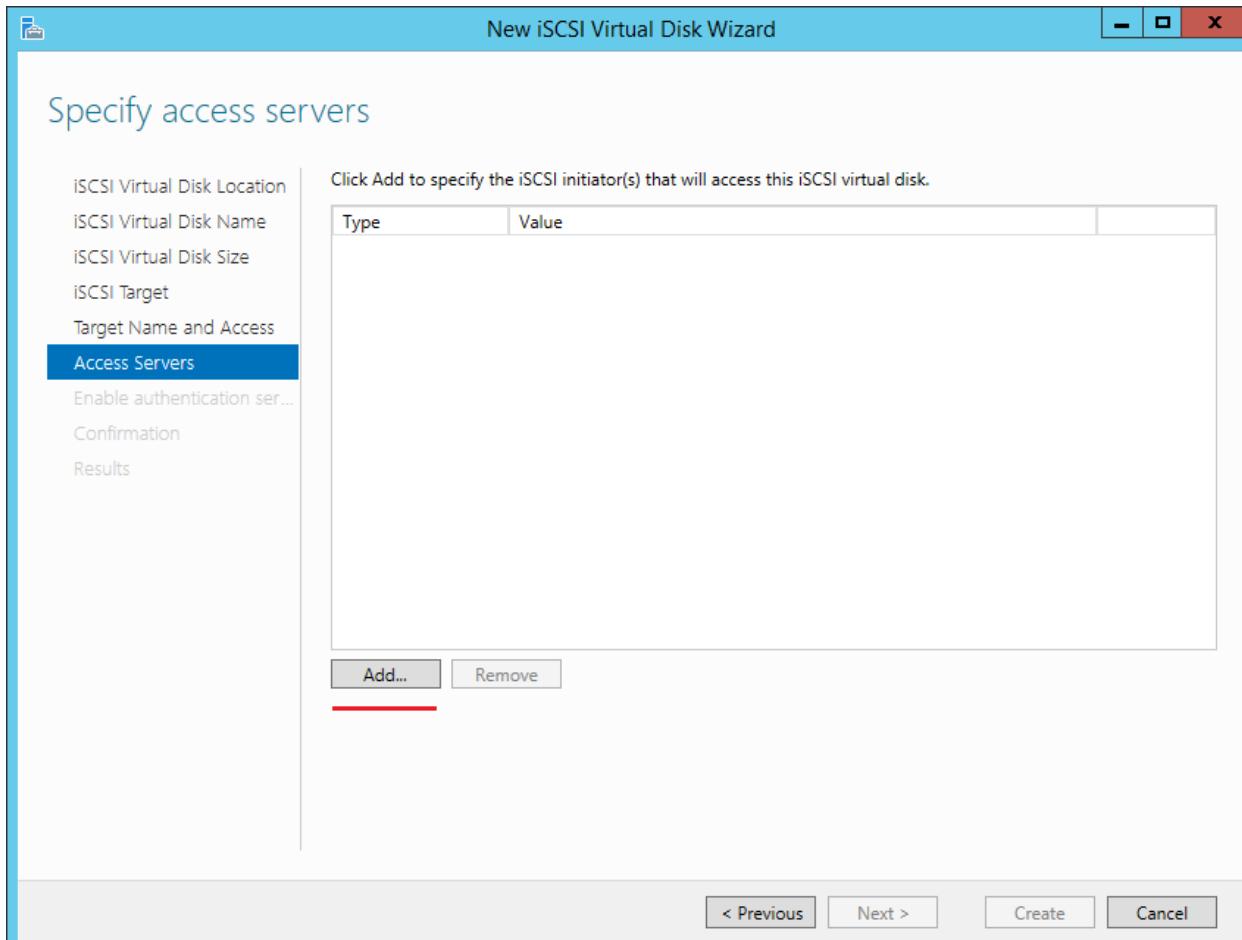
- Tại cửa sổ **Assign iSCSI target**, kiểm tra lựa chọn **New iSCSI target**, click vào **Next**.



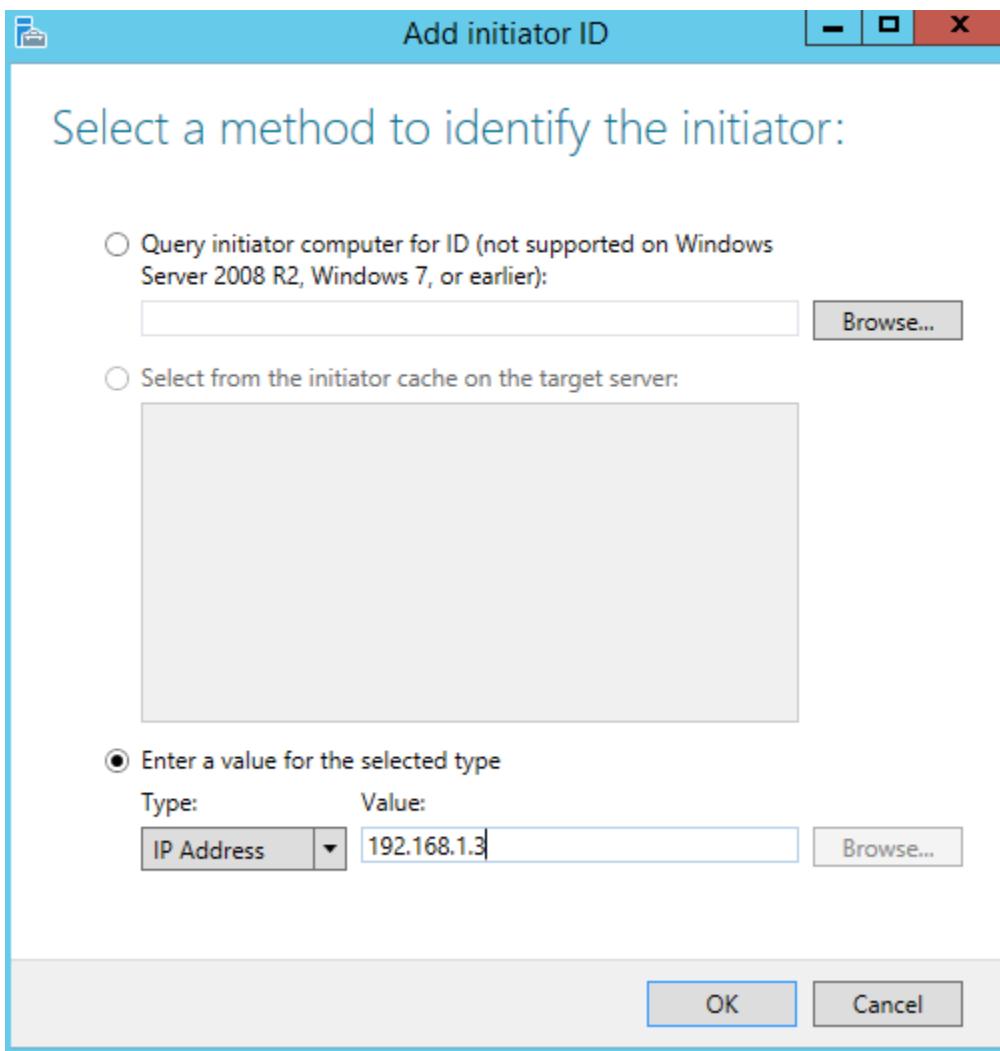
- Tại cửa sổ **Specify target name**, nhập vào tại mục **Name: iscsi**, click vào **Next**.



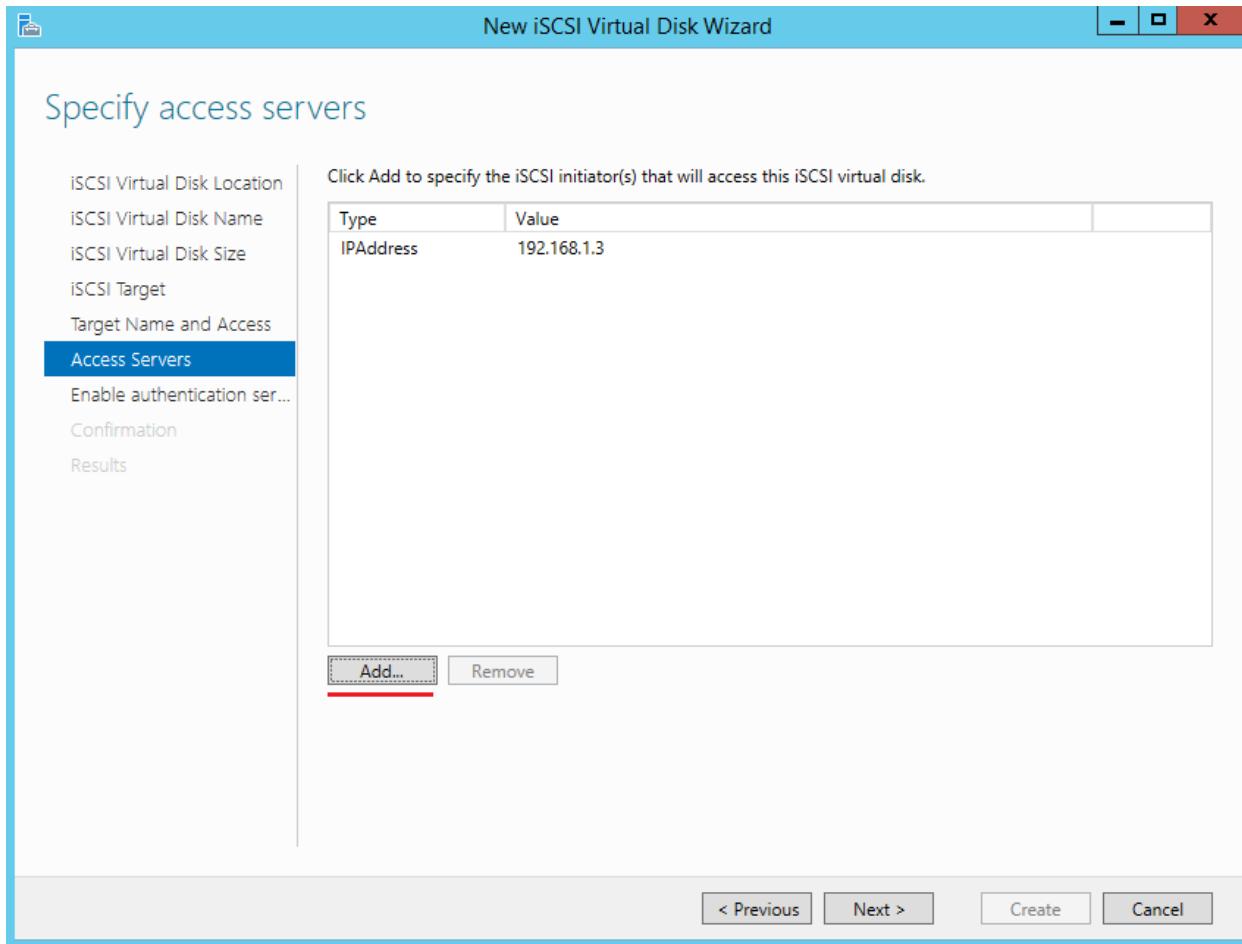
- Tại cửa sổ **Specify access servers**, click vào **Add...**



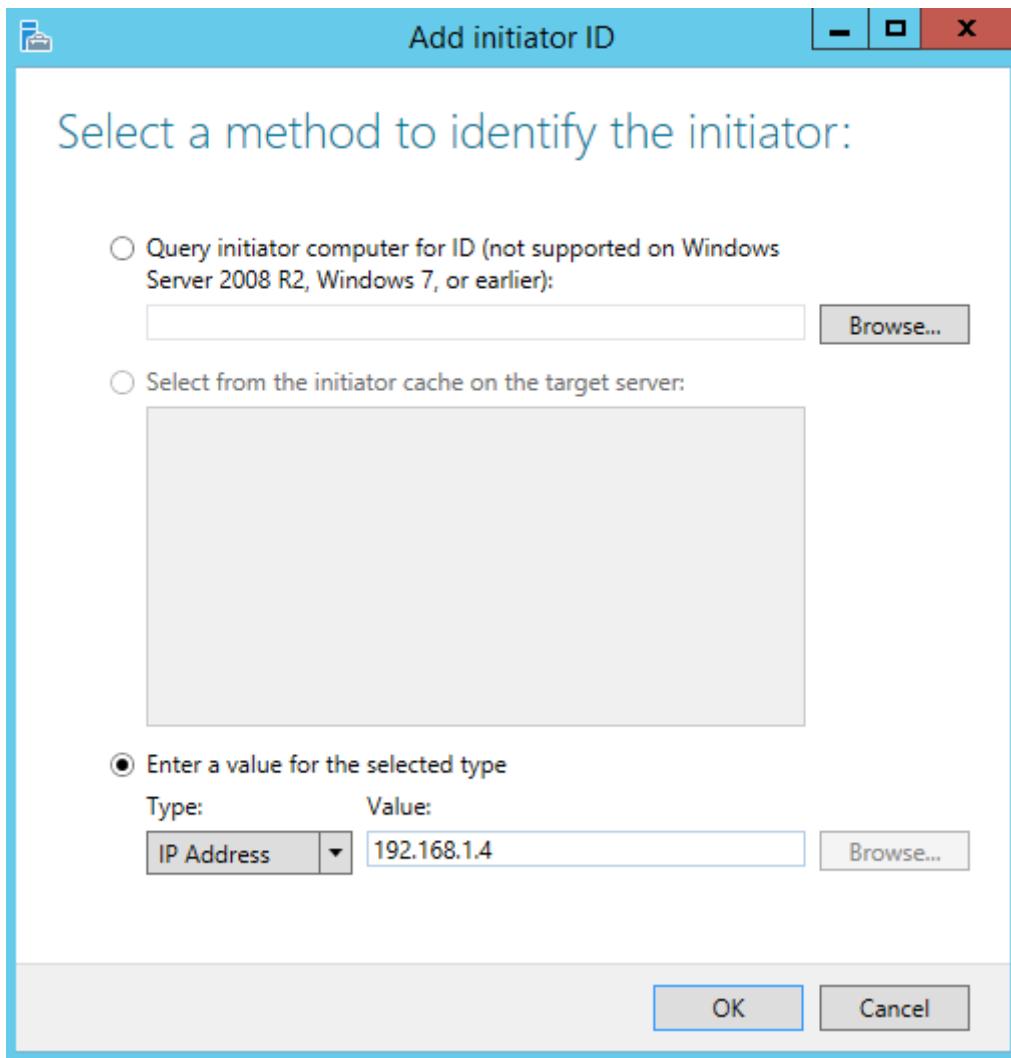
- Tại cửa sổ **Select a method to identify the initiator**, click chọn vào dòng **Enter a value for the selected type**, tại mục **Type** , chọn vào **IP Address**, tại mục **Value** , nhập vào **IP 192.168.1.3**.



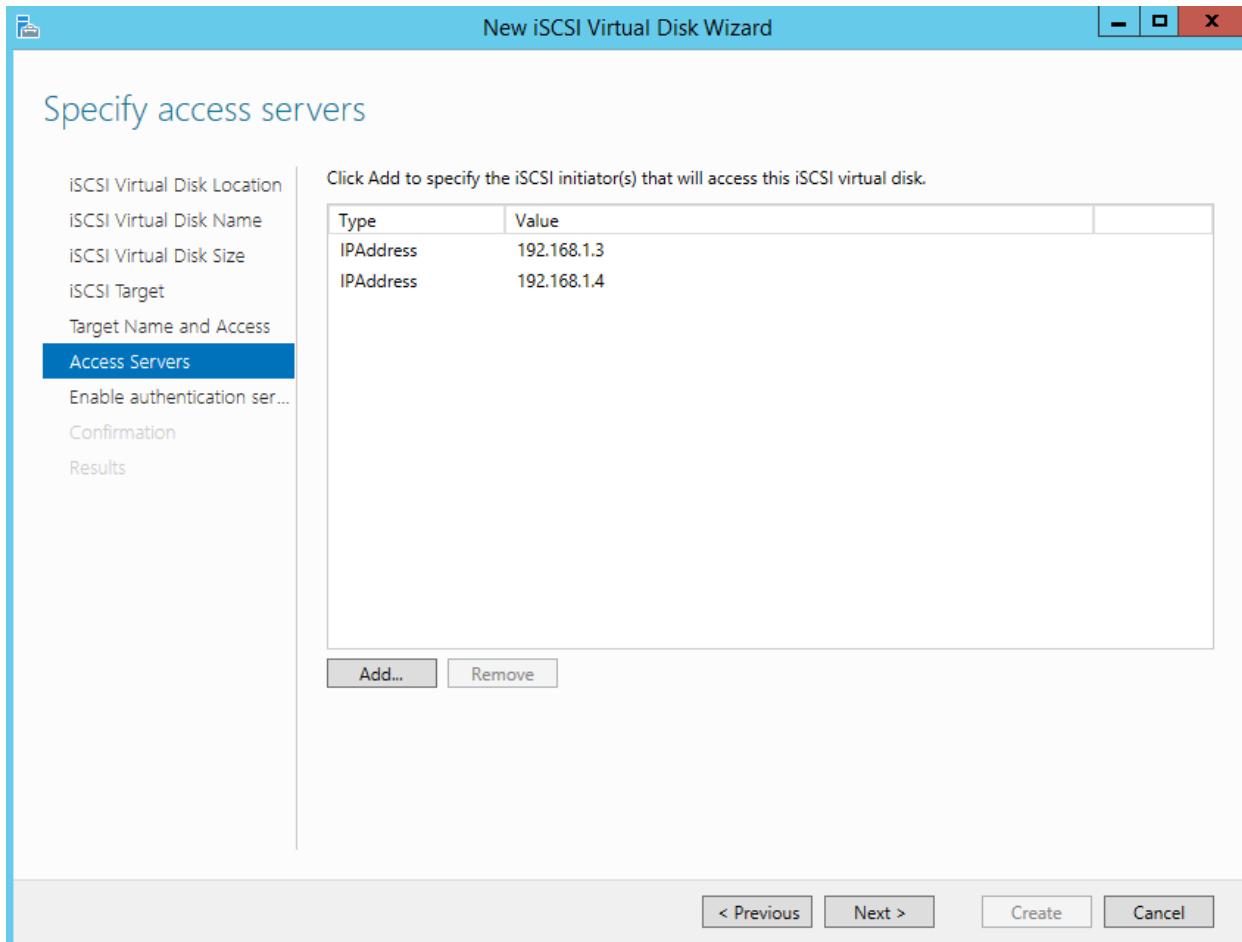
- Tại cửa sổ **Specify access servers** , tiếp tục click vào **Add...**



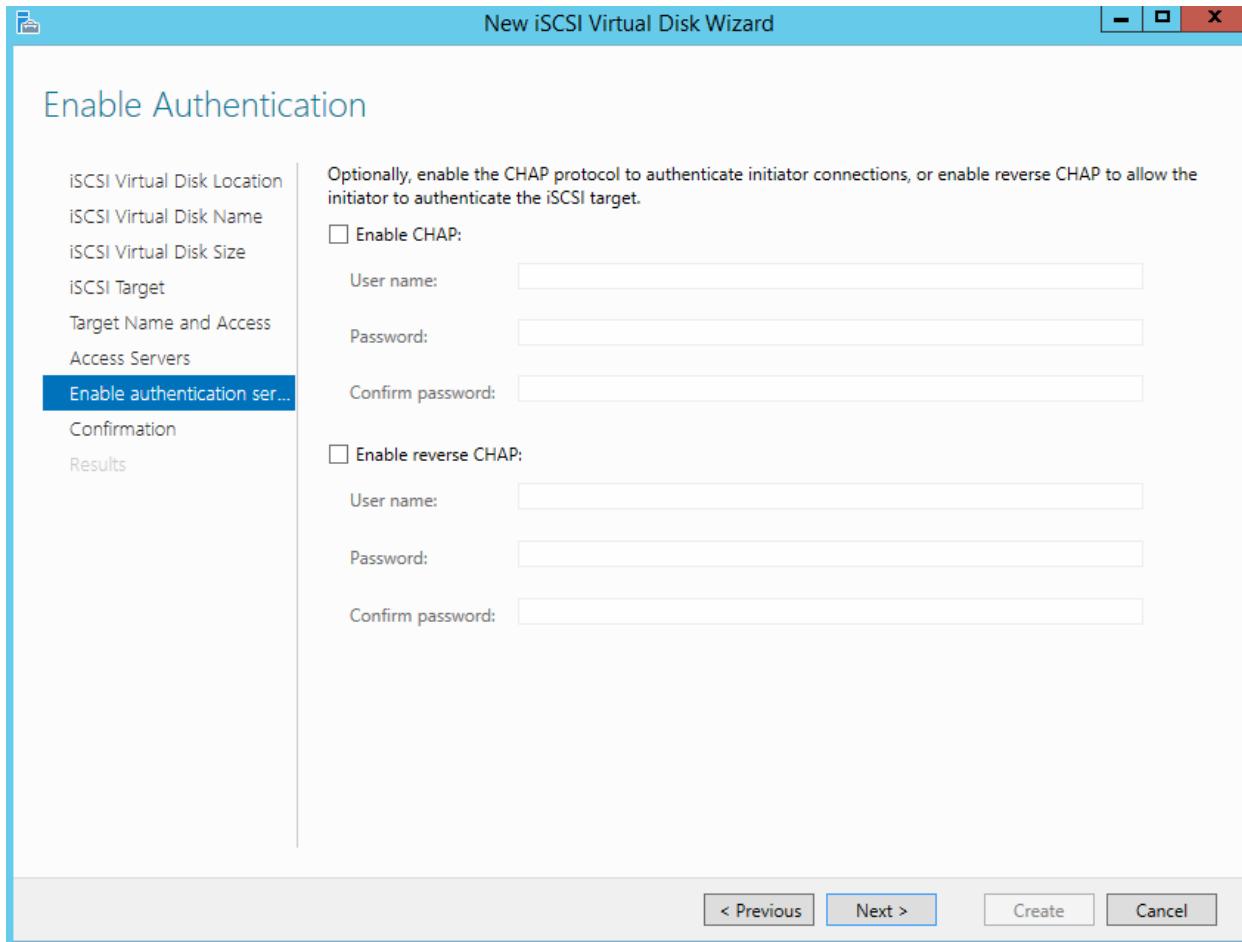
- Thực hiện add thêm địa chỉ IP **192.168.1.4**.



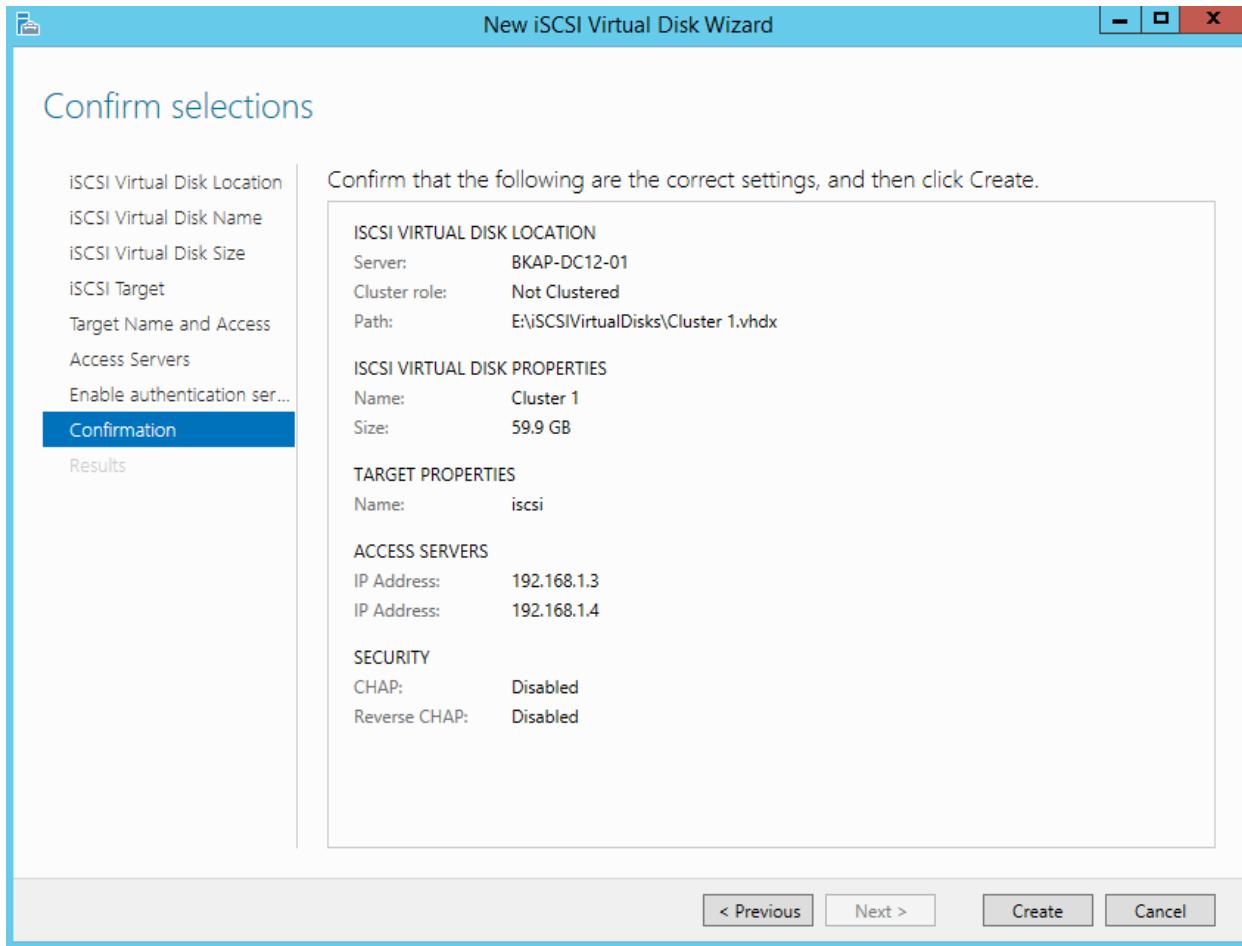
- Click vào **Next** tại cửa sổ **Specify access servers**.



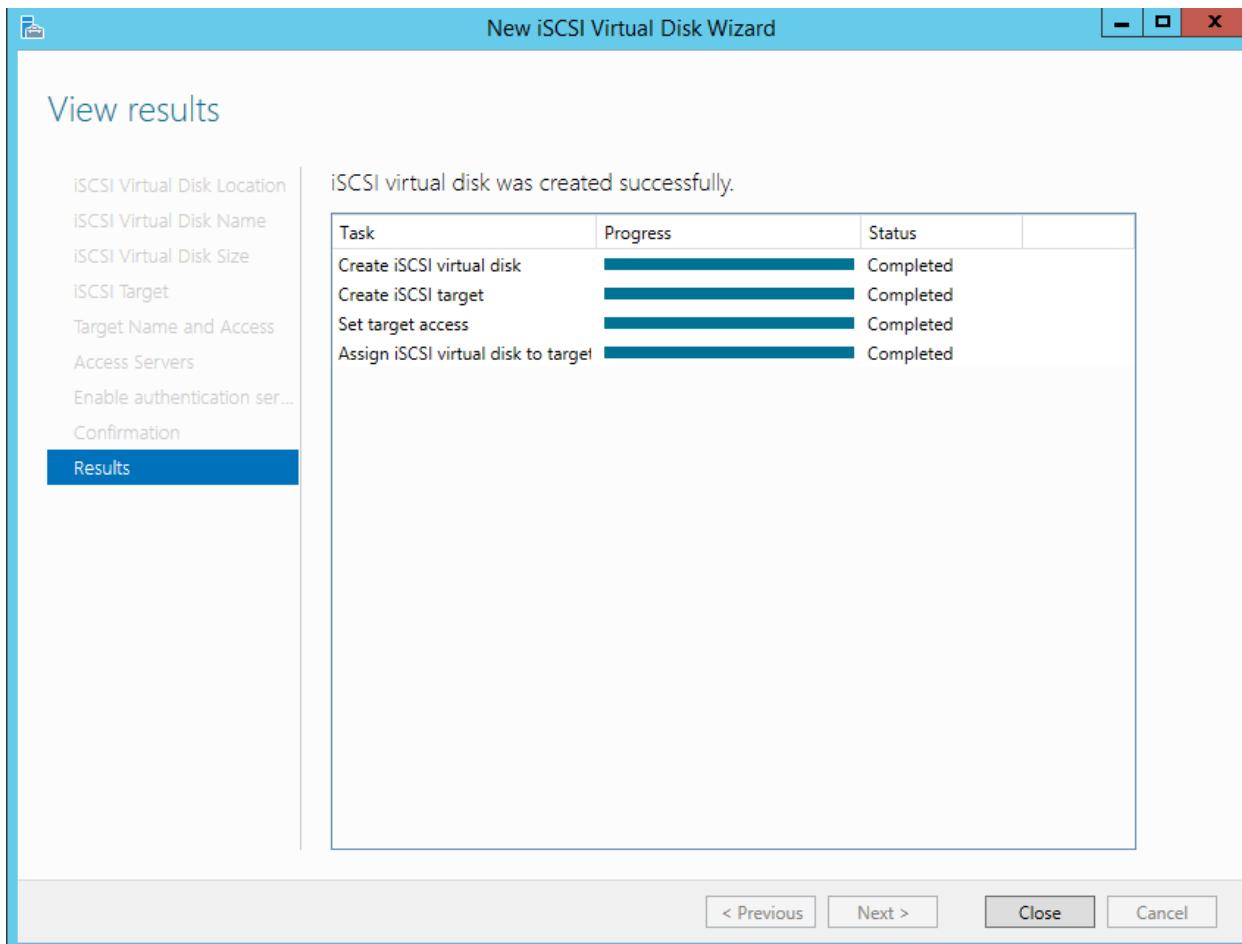
- Click vào **Next** tại cửa sổ **Enable Authentication**.



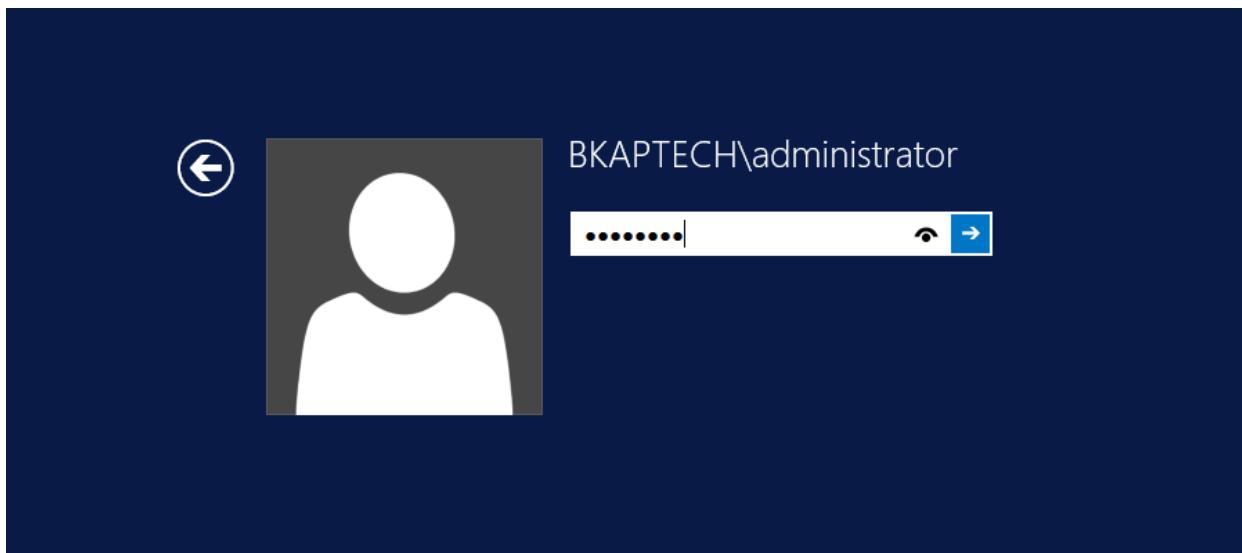
- Tại cửa sổ **Confirm selections**, click vào **Create**.



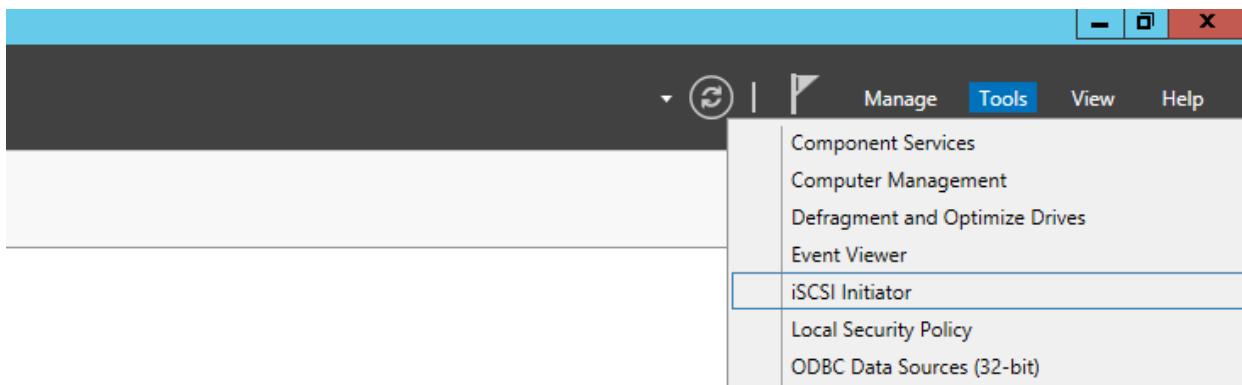
- Tại cửa sổ **View results**, kiểm tra kết quả, click vào **Close**.



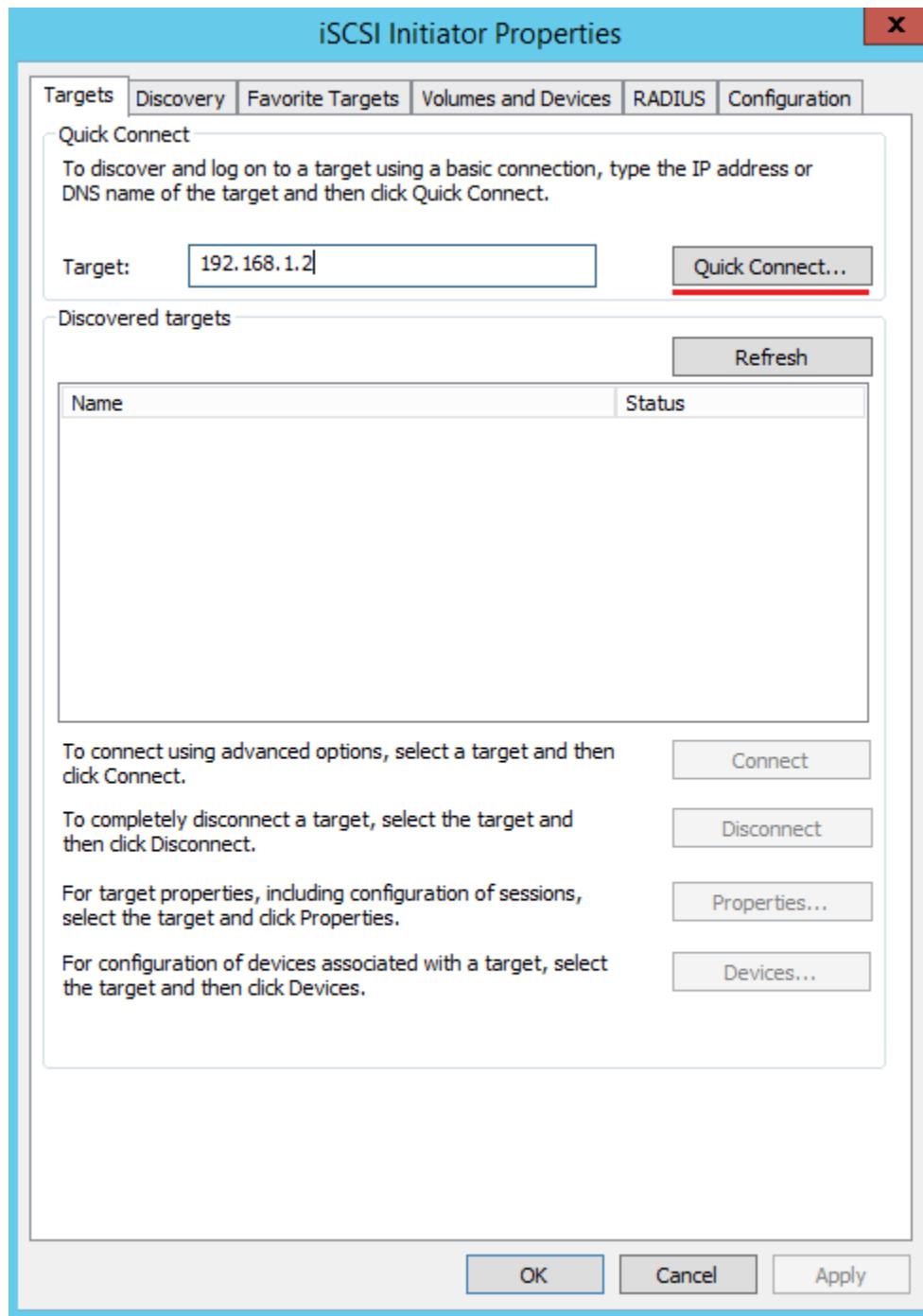
- Chuyển sang máy **BKAP-SRV12-01**:
 - Join vào Domain, đăng nhập bằng tài khoản **bkaptech\administrator**.



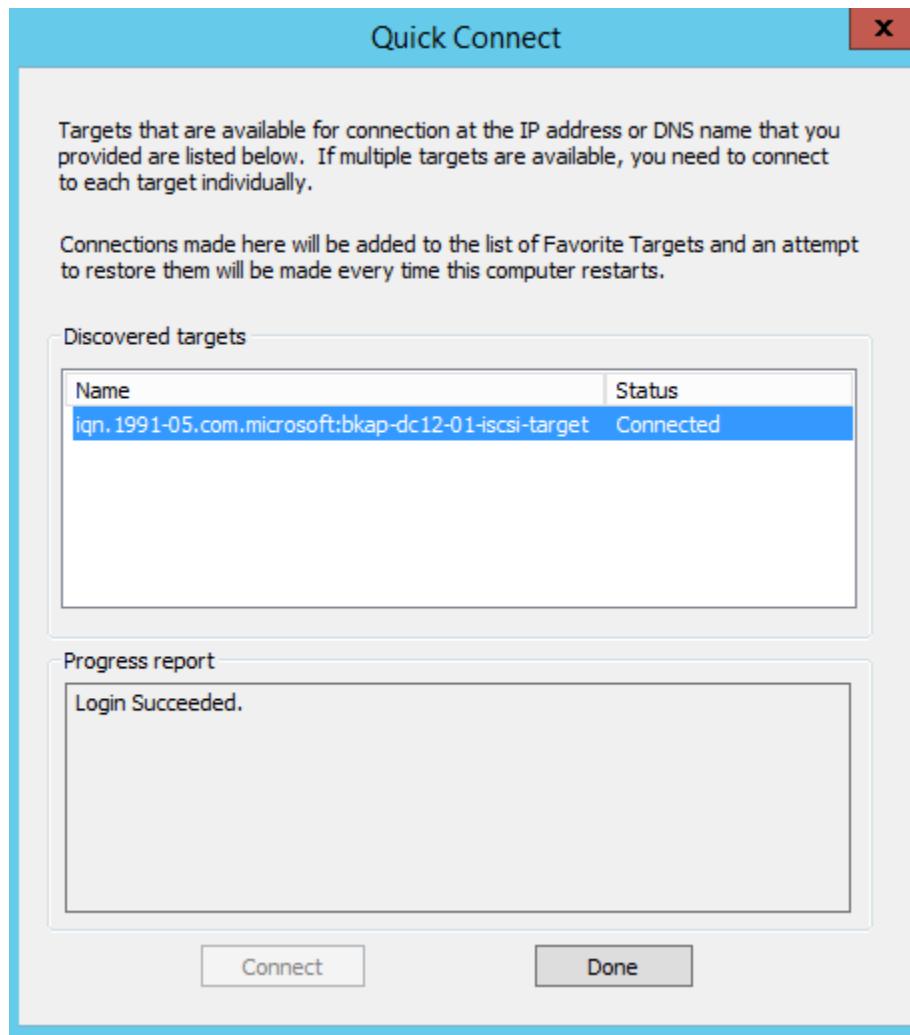
- Cấu hình nhận ổ từ iSCSI Server.
 - Vào Server Manager / Tools / iSCSI Initiator.



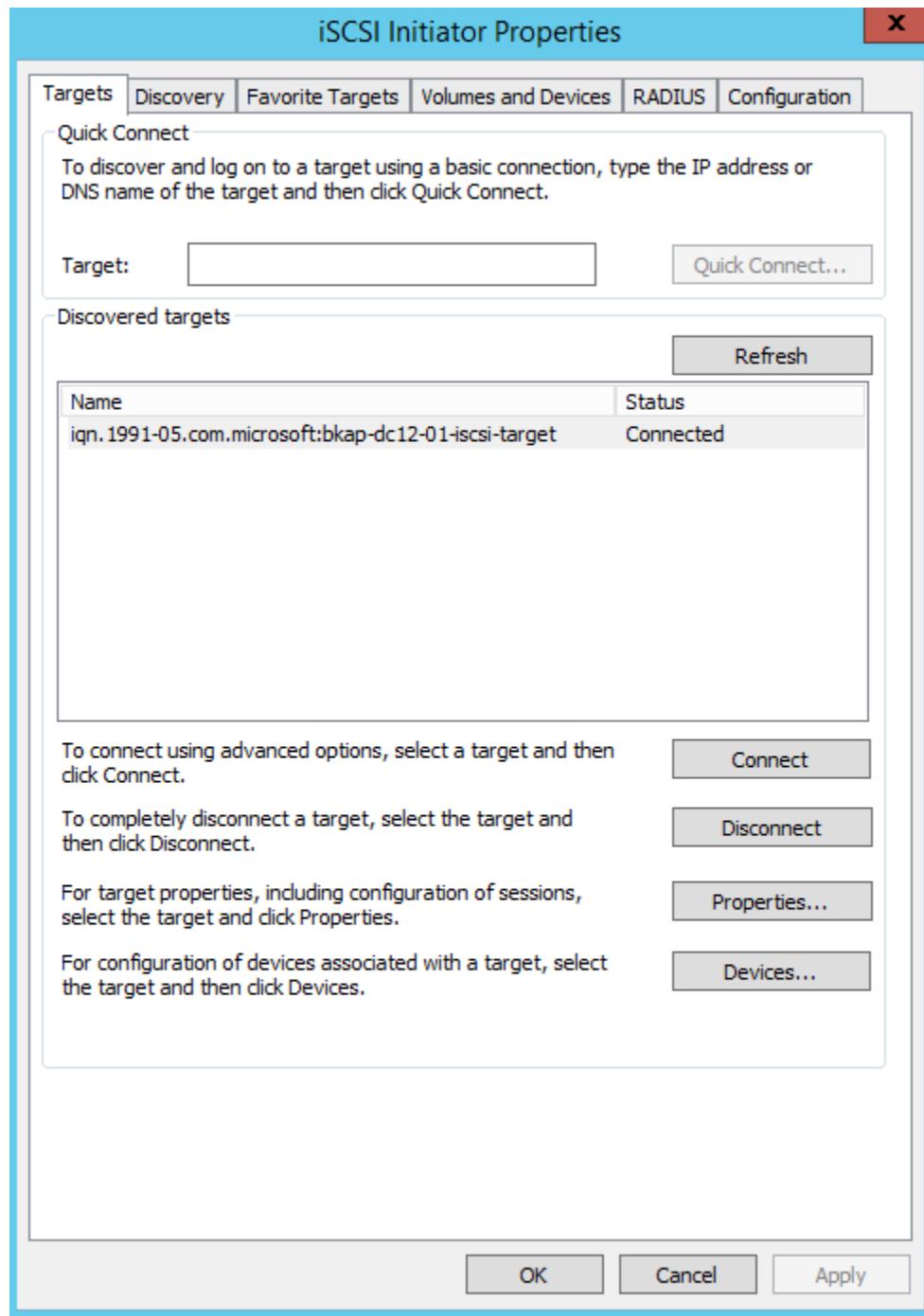
- Trong cửa sổ iSCSI Initiator Properties, trong tab Targets, nhập vào tại mục Target: 192.168.1.2, click vào Quick Connect...



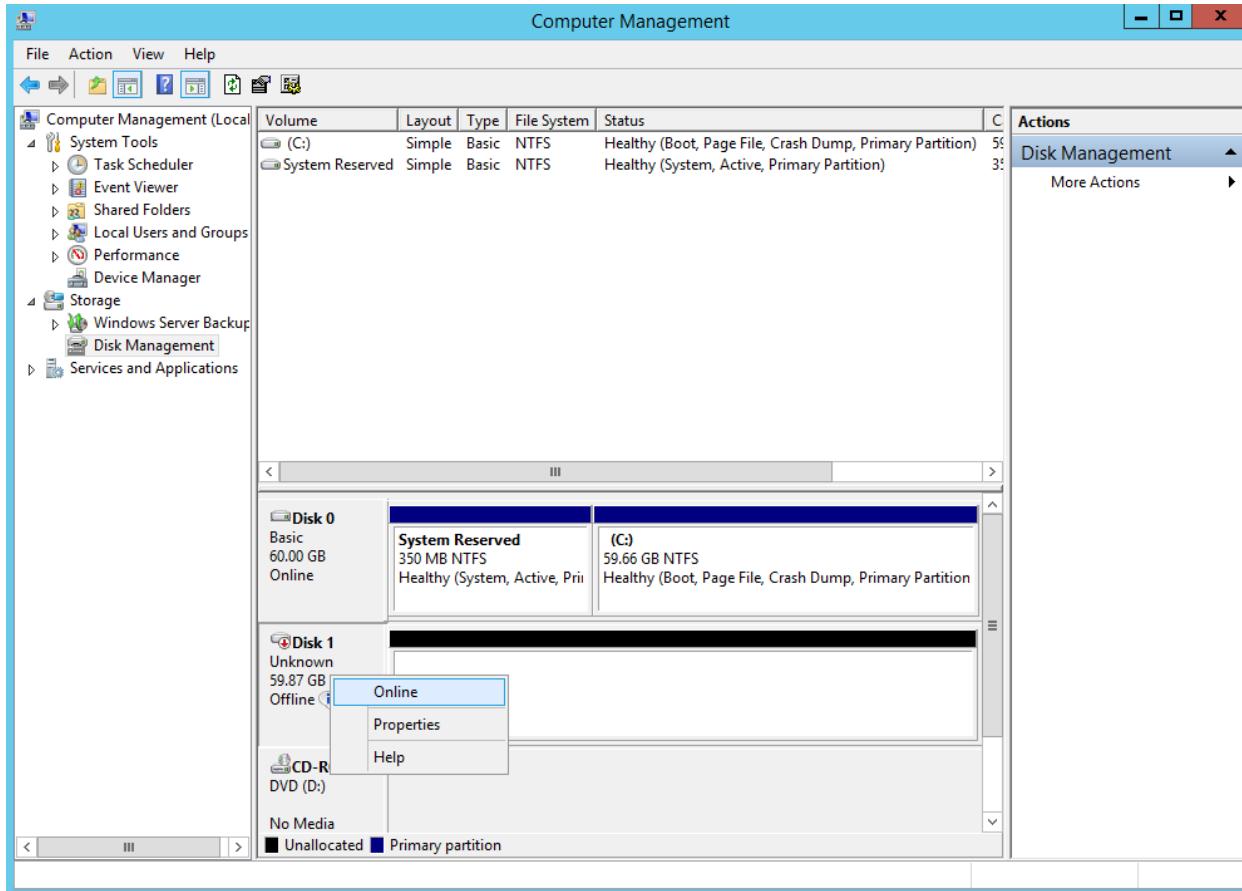
- Tại cửa sổ **Quick Connect**, click vào **Done**.



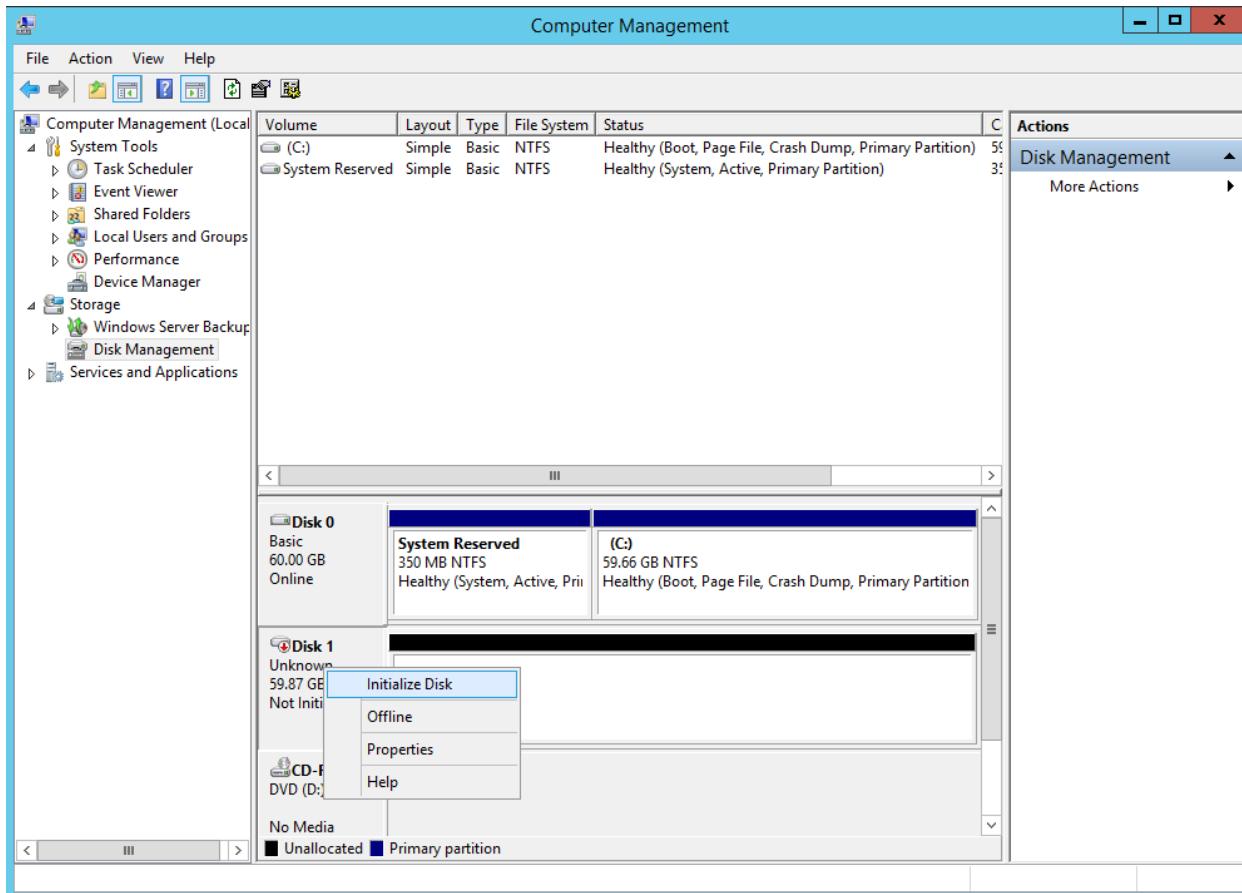
- Click vào **OK** tại cửa sổ iSCSI Initiator Properties.



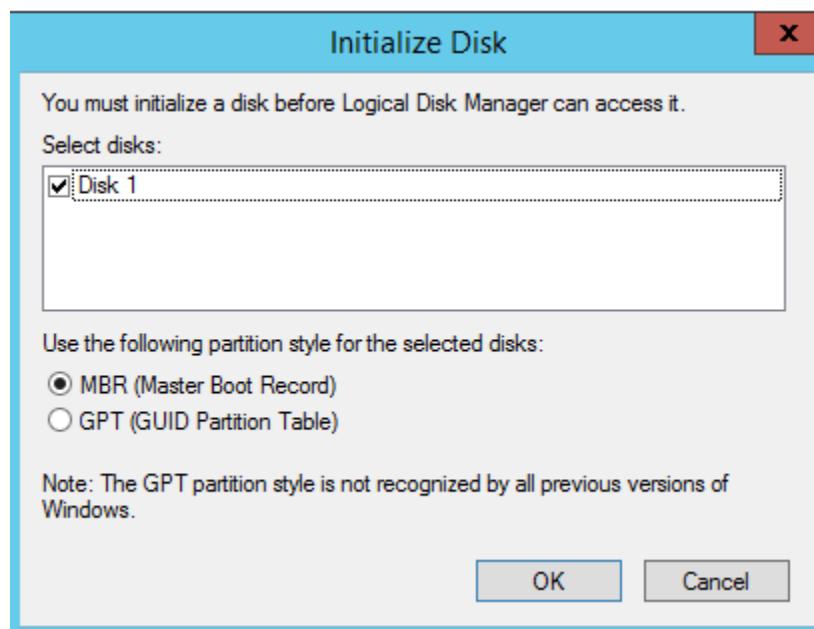
- Vào **Computer Management** cấu hình ổ đĩa:
 - Click chọn vào **Disk Management**, click chuột phải vào **Disk 1**, chọn **Online**.



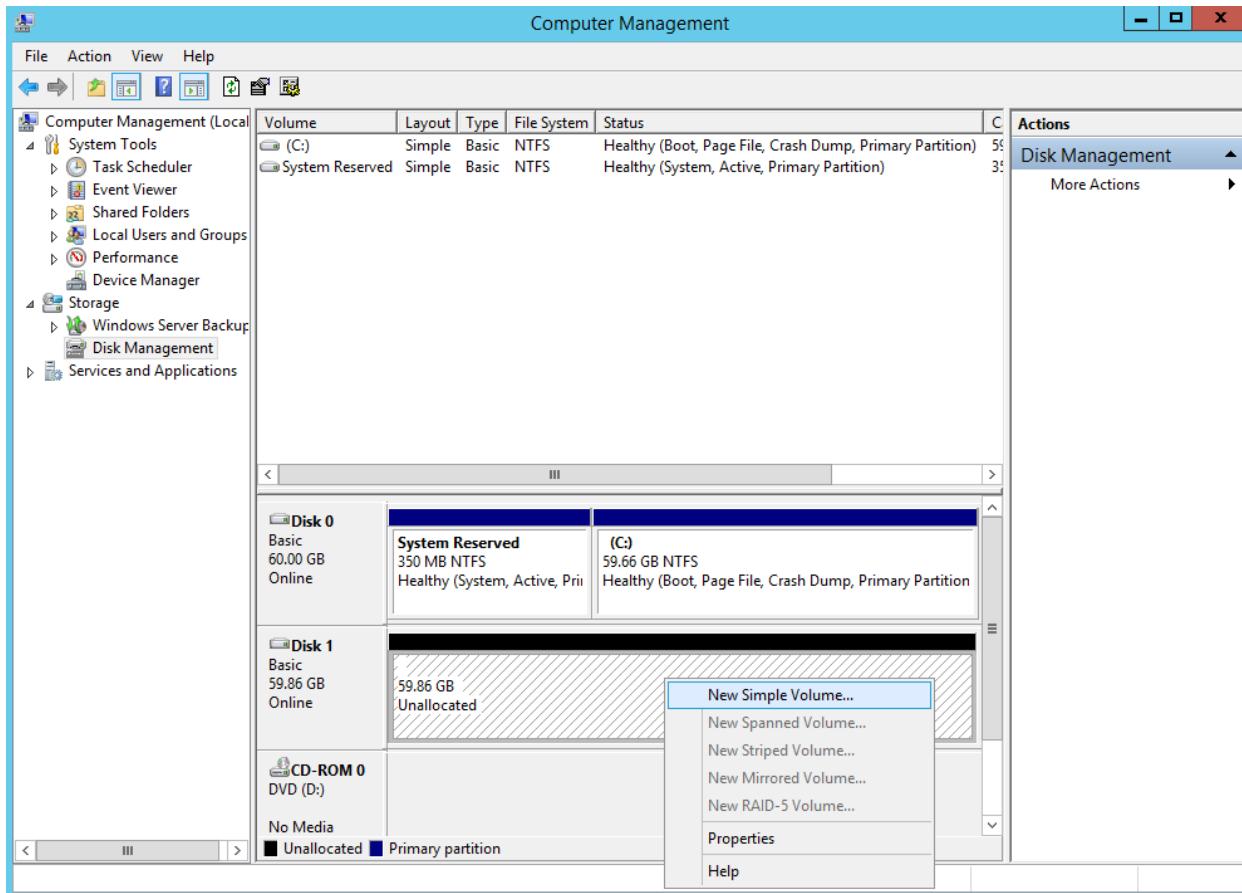
- Tiếp tục click chuột phải tại **Disk 1**, chọn **Initialize Disk**.



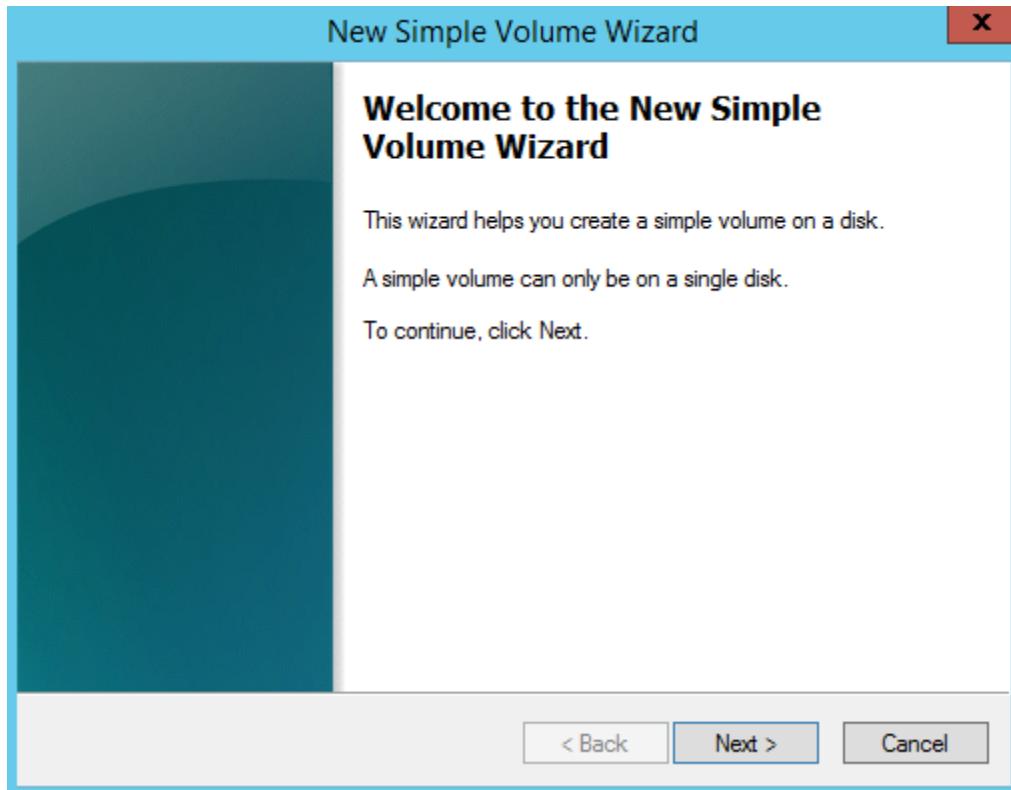
- Tại cửa sổ **Initialize Disk**, kiểm tra lự chọn **Disk 1 / MBR** , click **OK**.



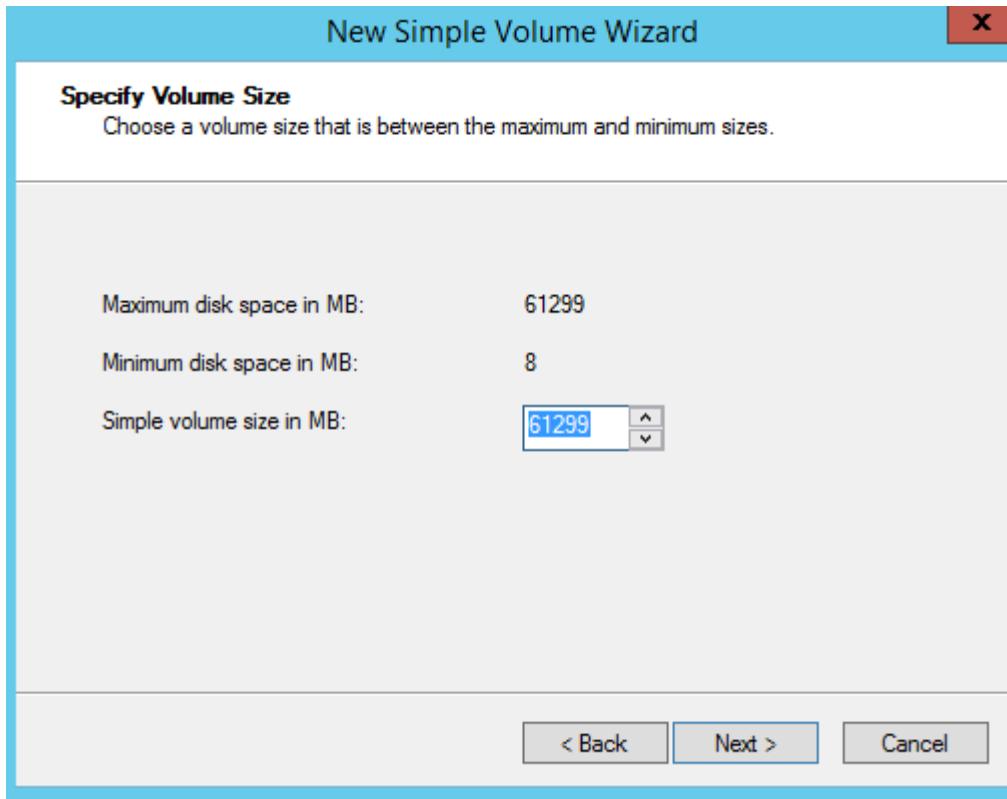
- Click chuột phải tại **Unallocated**, chọn **New Simple Volume...**



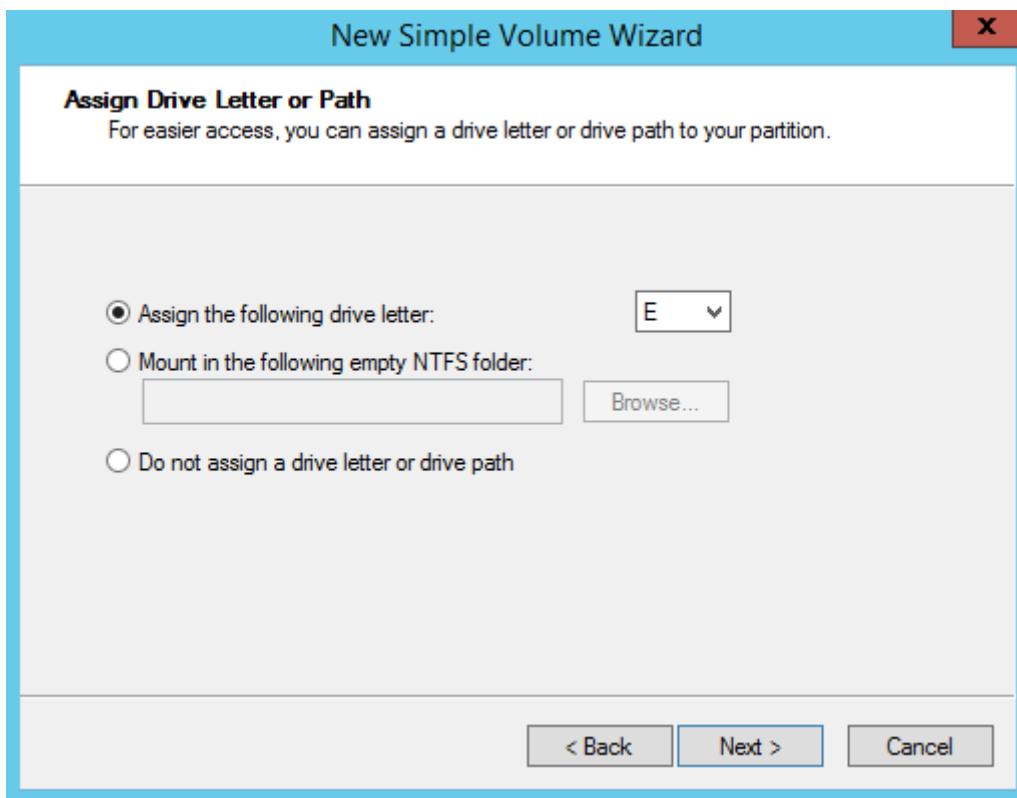
- Tại cửa sổ **Welcome to the New Simple Volume Wizard**, click vào **Next**.



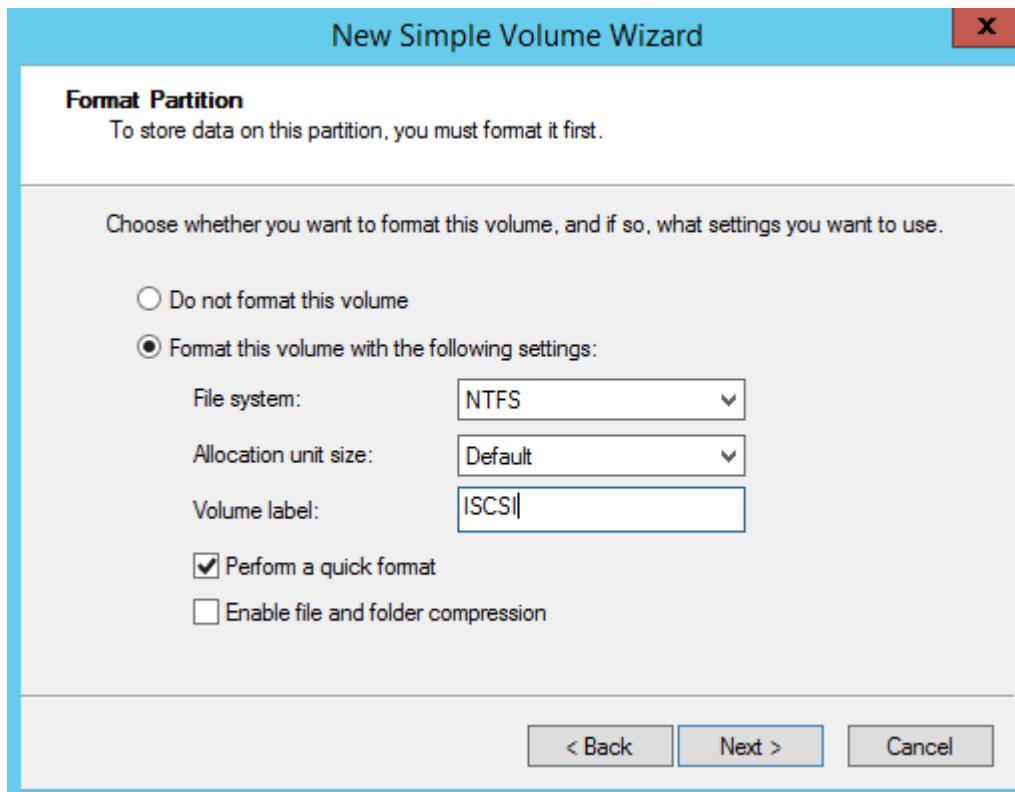
- Tại cửa sổ **Specify Volume Size**, kiểm tra dung lượng ổ đĩa, click vào **Next**.



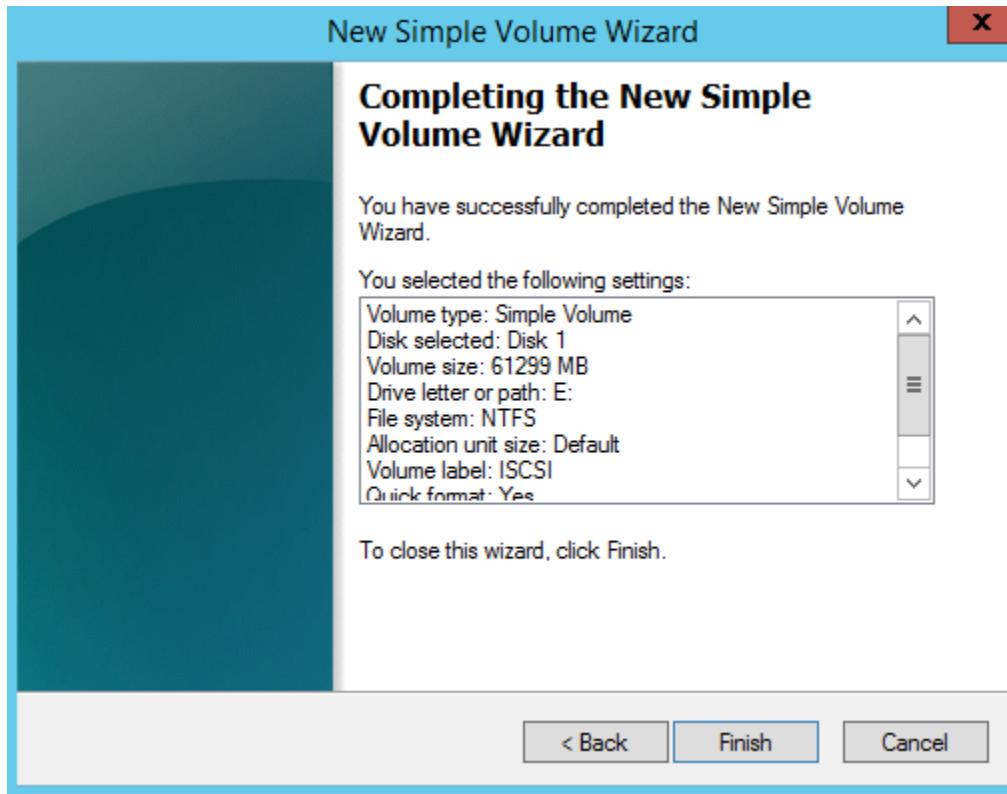
- Tại cửa sổ **Assign Drive Letter or Path**, click vào **Next**.



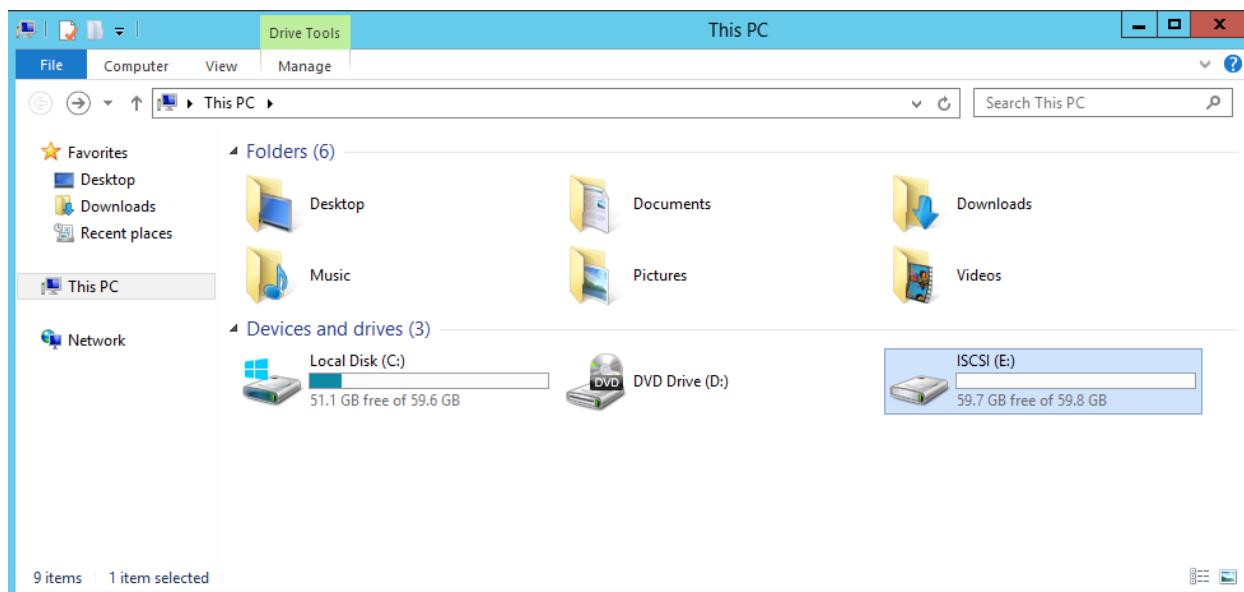
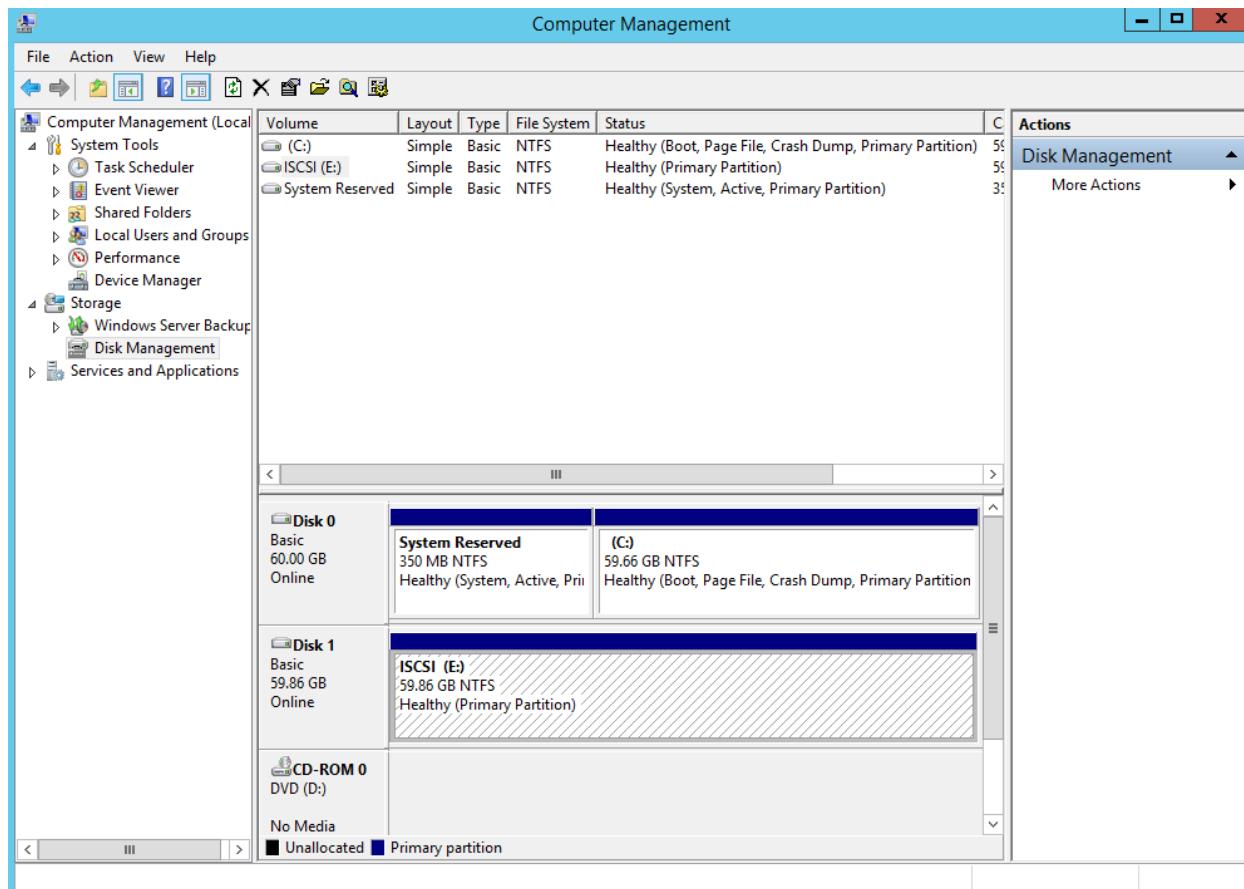
- Tại cửa sổ **Format Partition**, tại mục **Volume label**, nhập vào tên **ISCSI**, click vào **Next**.



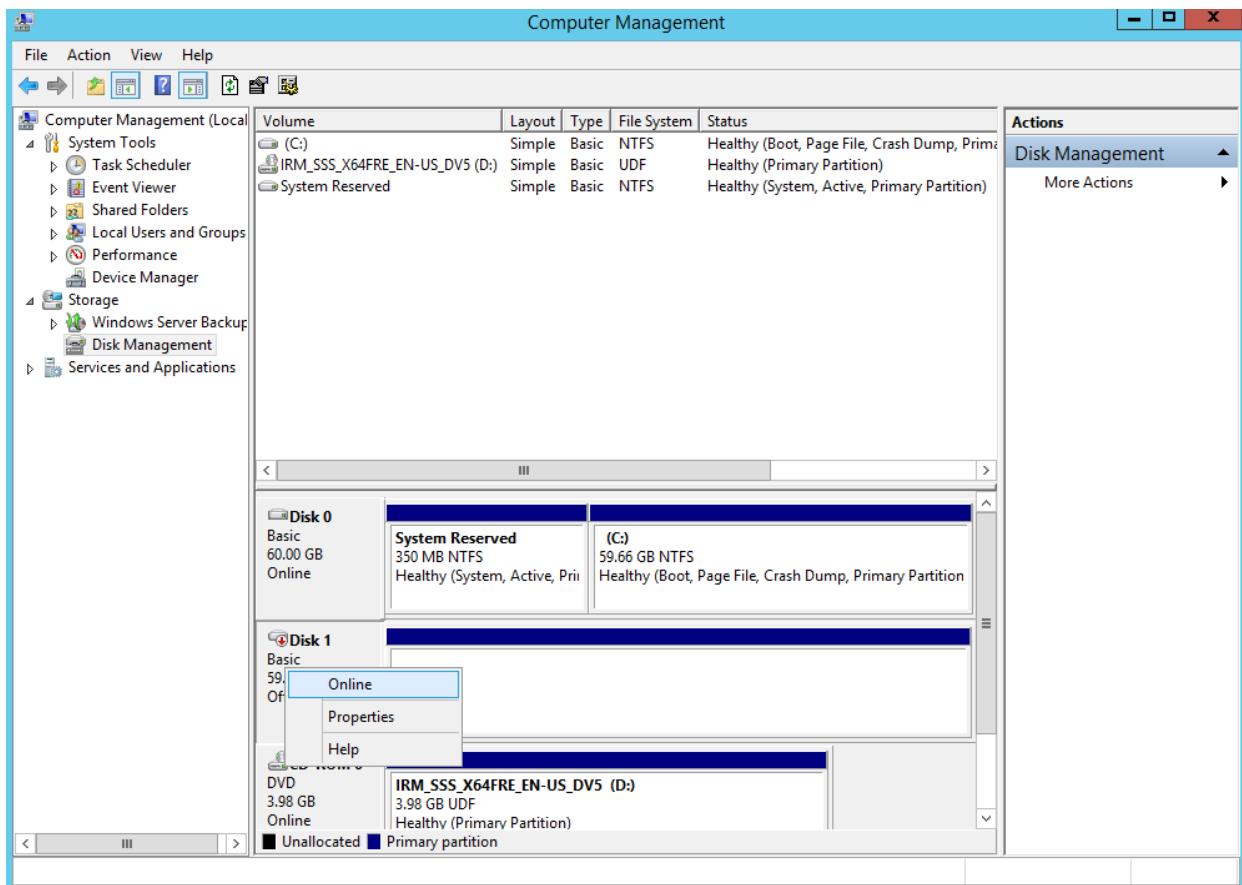
- Tại cửa sổ **Completing the New Simple...** click vào **Finish**.



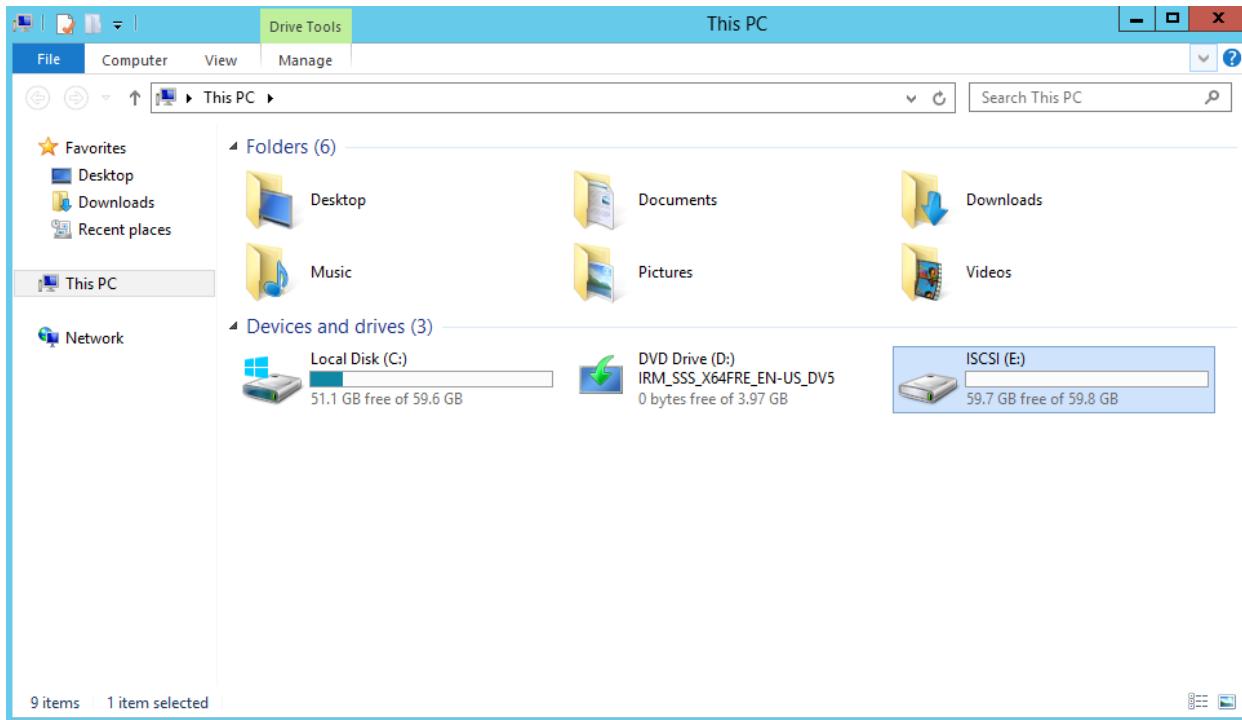
■ Kiểm tra ổ đĩa đã được tạo:



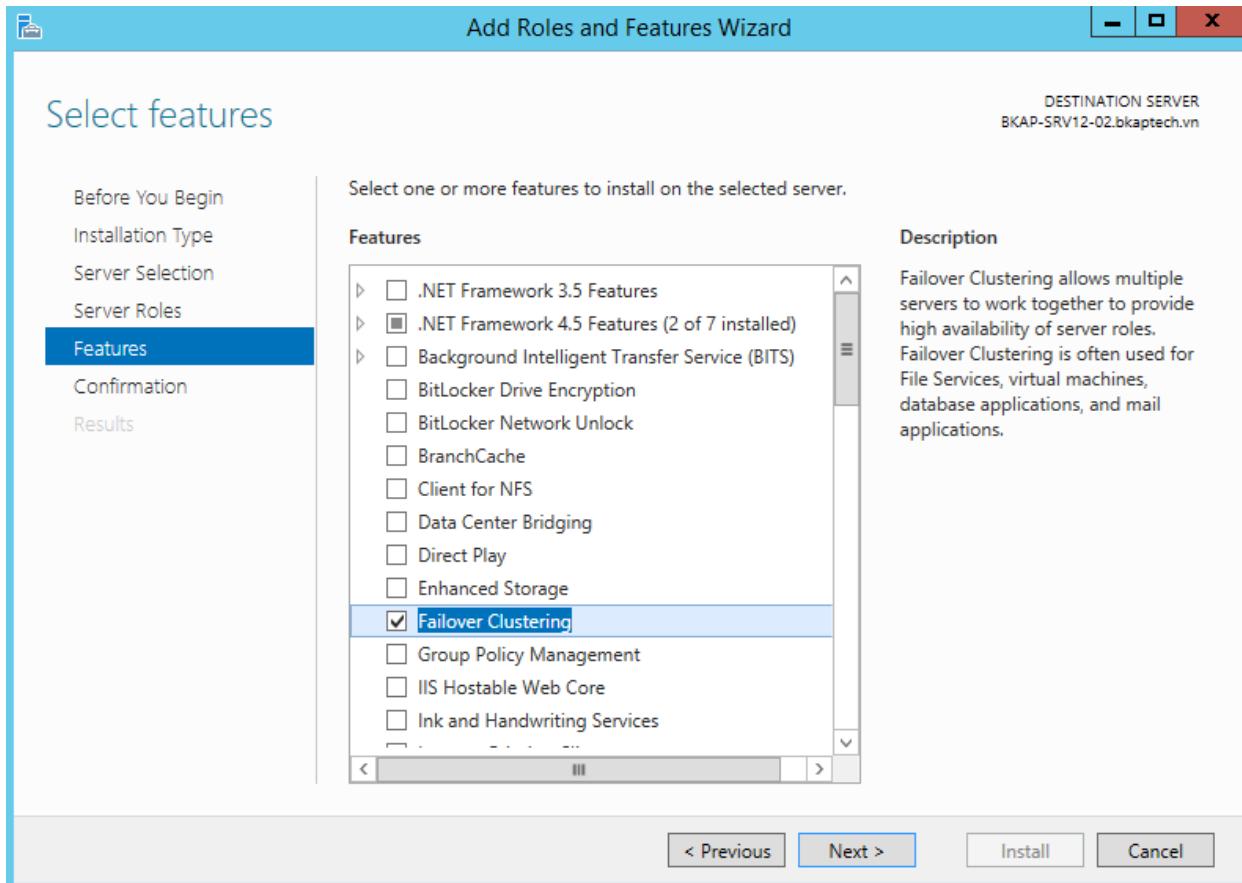
- Chuyển sang máy **BKAP-SRV12-02**, Join vào Domain, đăng nhập bằng tài khoản **bkaptech\administrator**, cấu hình nhận ổ từ **iSCSI Server**.(làm tương tự giống trên máy **BKAP-SRV12-01**).
 - Trong cửa sổ **Computer Management**, click vào **Disk 1**, chọn **Online**.



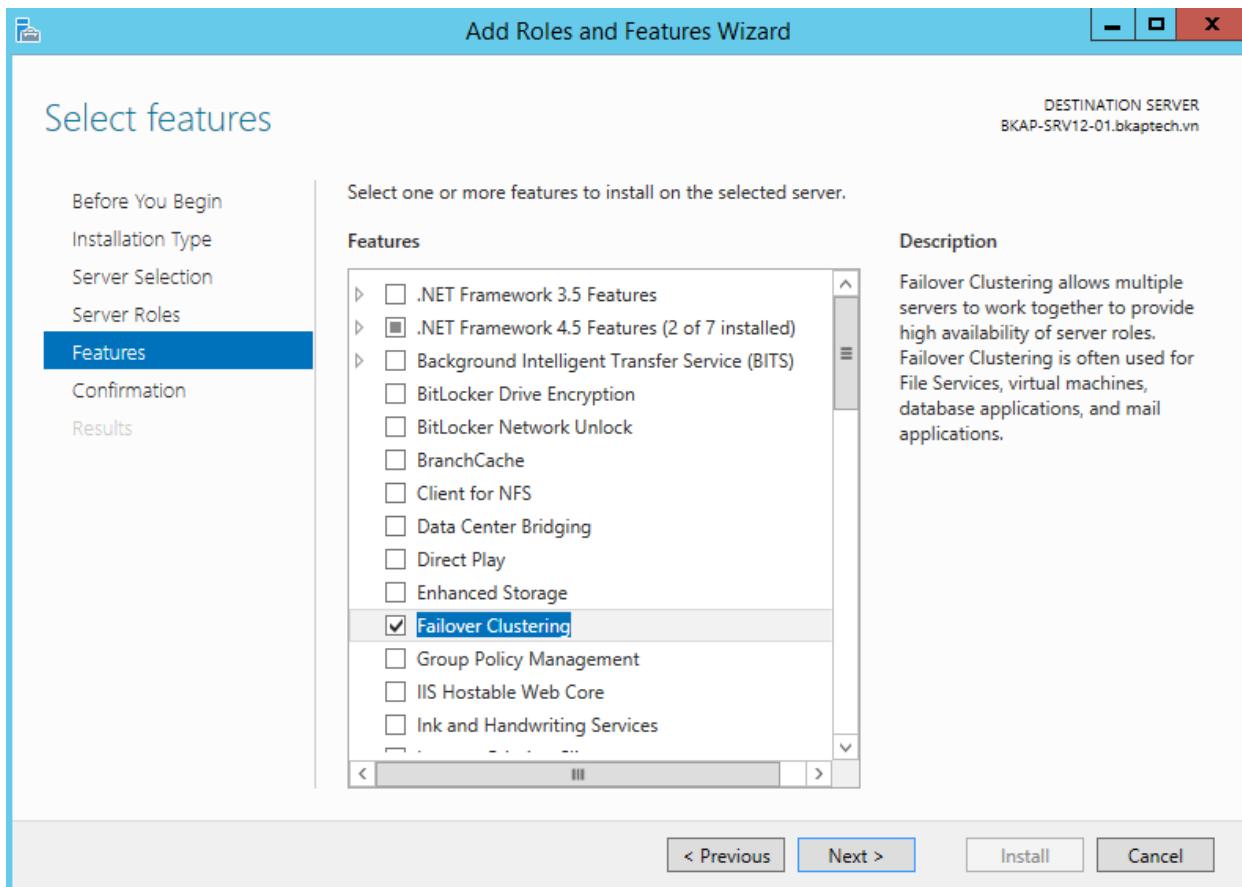
■ Kiểm tra ổ đĩa:



o Cài đặt Failover Cluster:

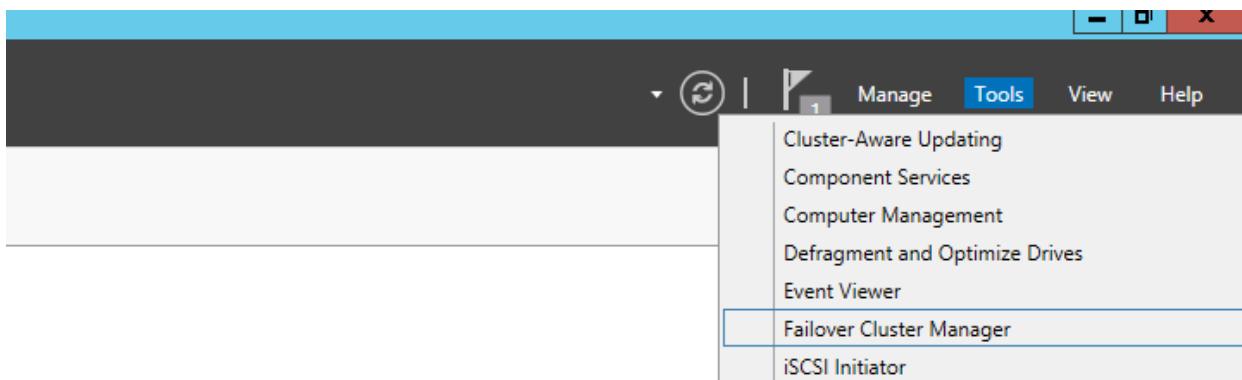


- Chuyển sang máy **BKAP-SRV12-01**, cài đặt và cấu hình **Failover Cluster**.
 - Cài đặt **Failover Cluster**

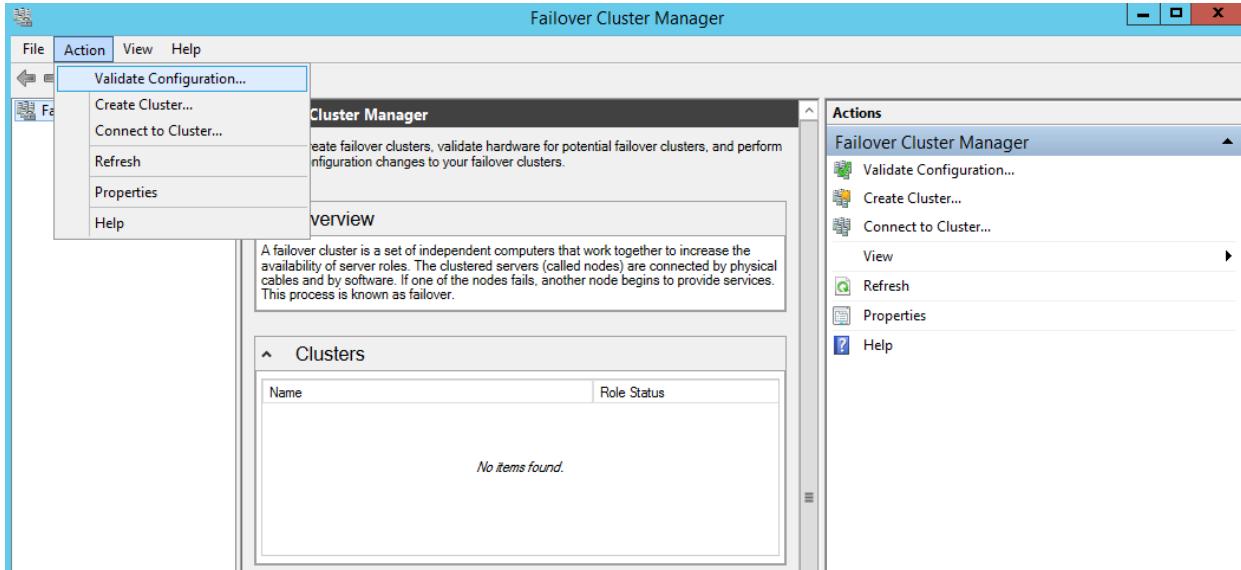


○ Cấu hình Failover Cluster:

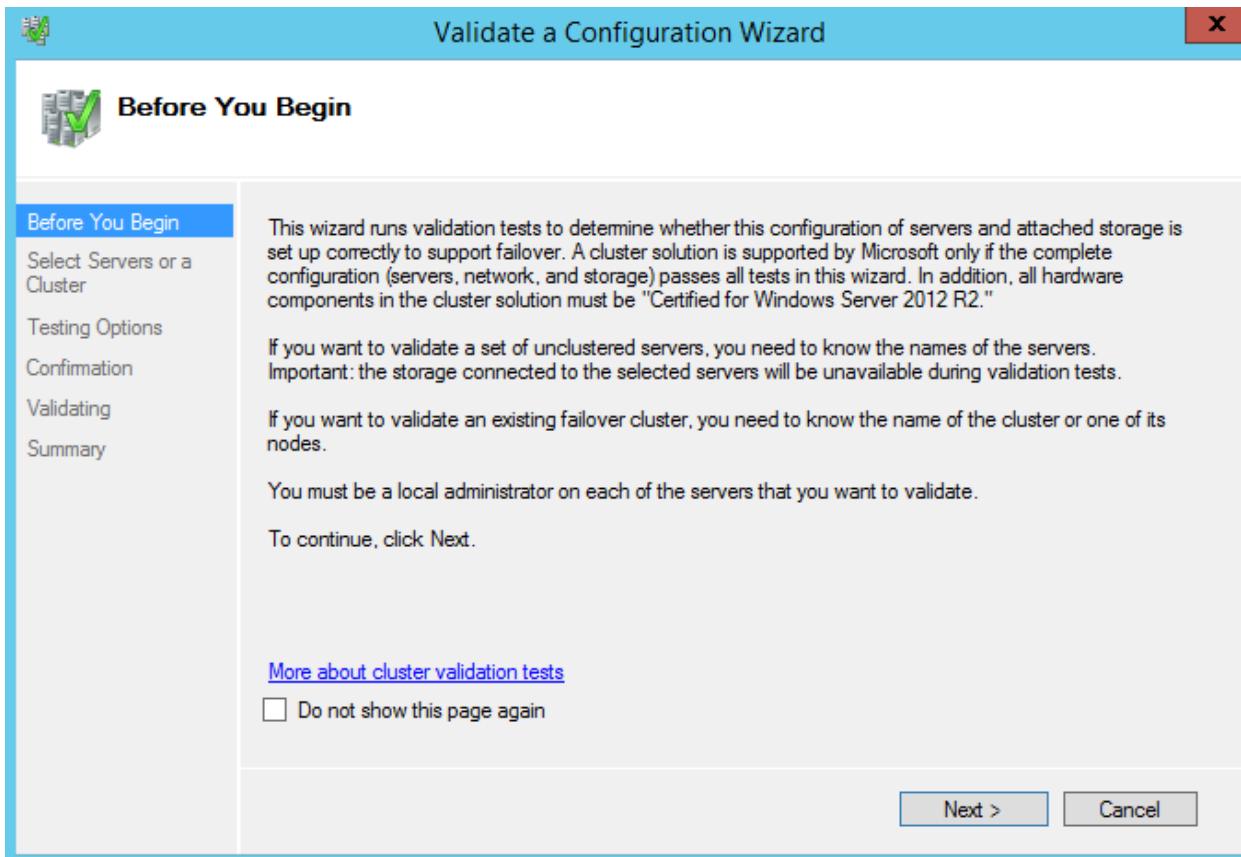
- Trong **Server Manager**, chọn vào **Tools / Failover Cluster Manager**.



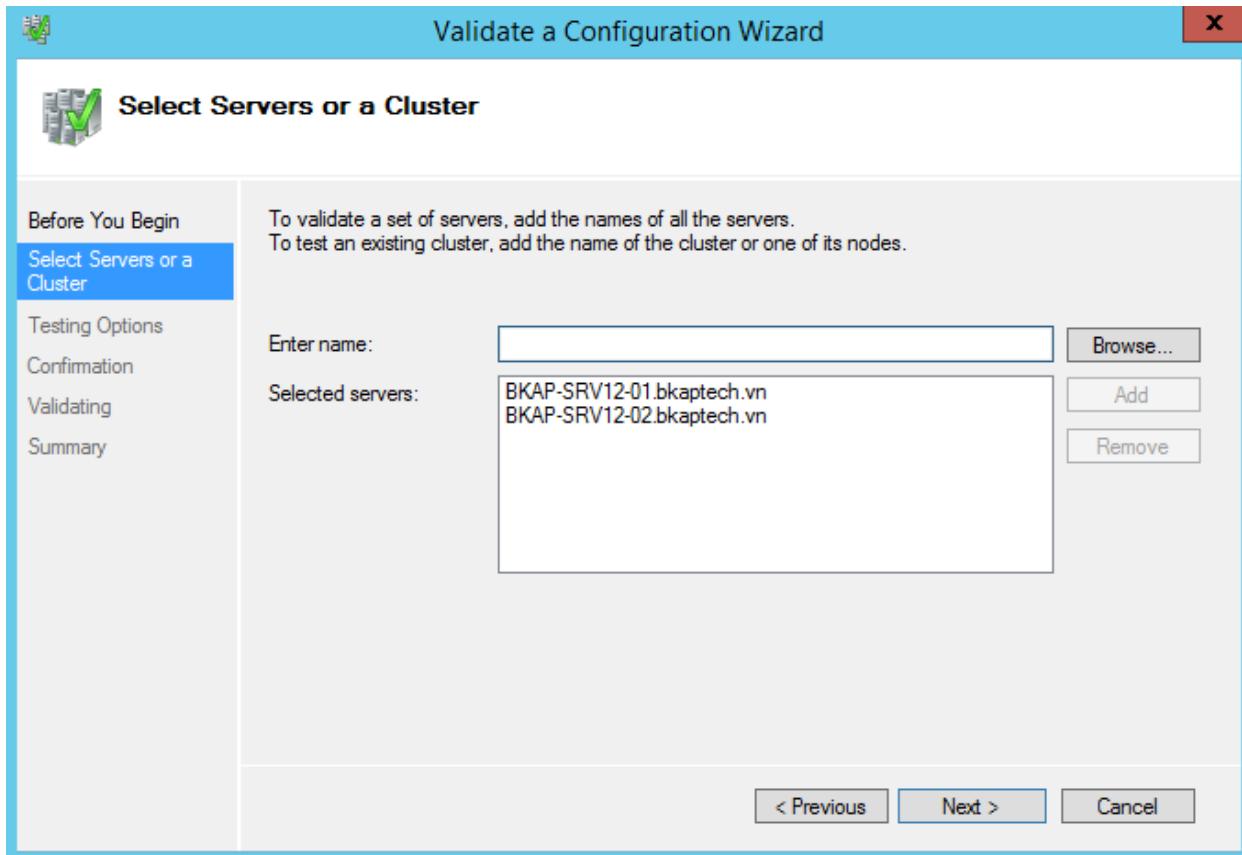
- Trong cửa sổ **Failover Cluster Manager**, click vào **Action / Validate Configuration...**



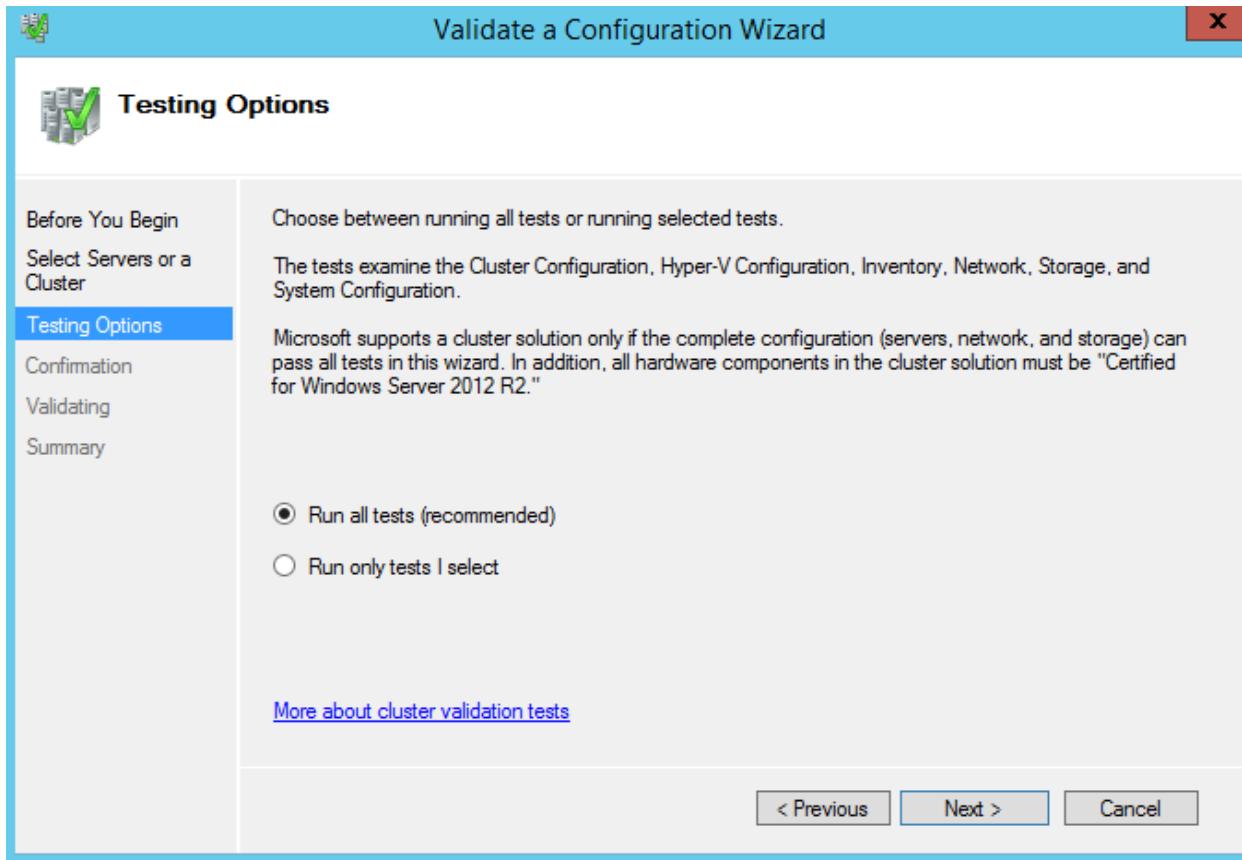
- Tại cửa sổ **Before You Begin**, click vào **Next**.



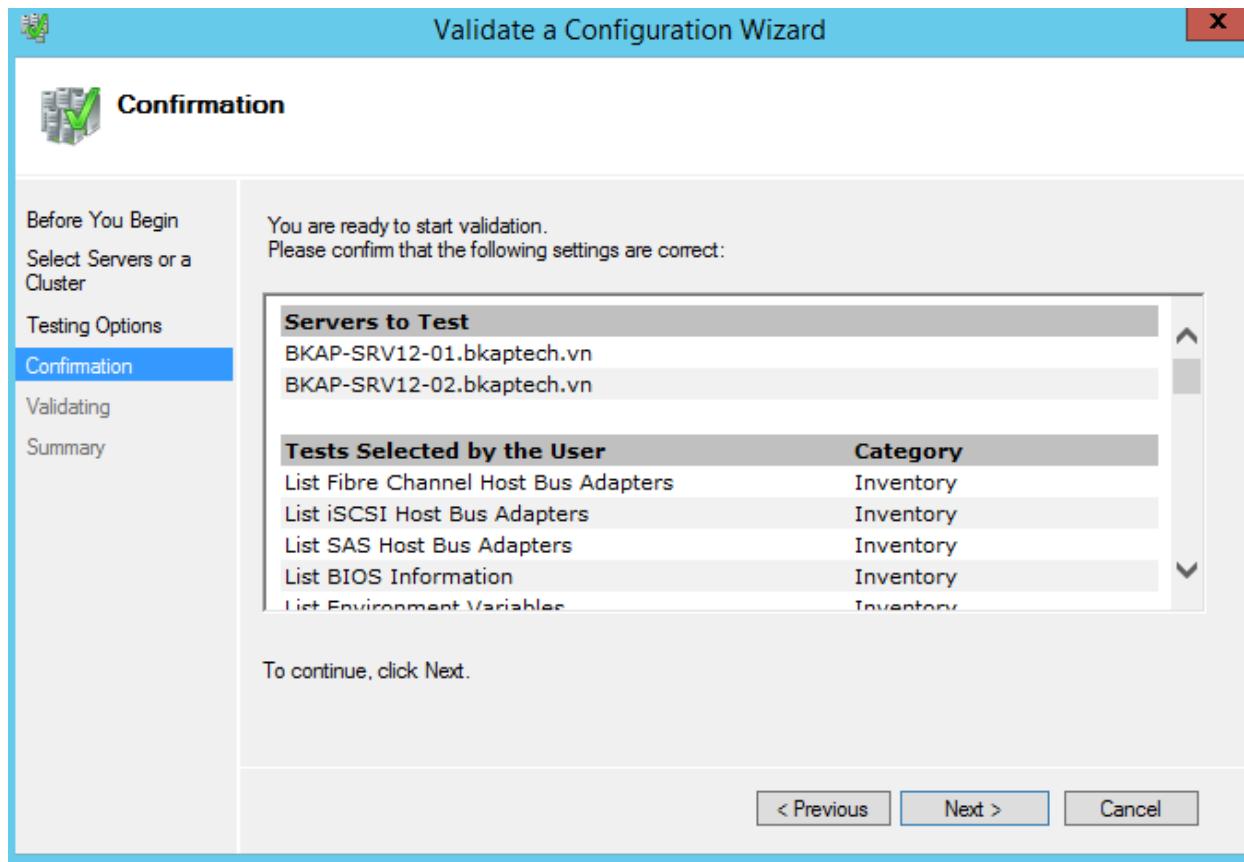
- Tại cửa sổ **Select Servers or a Cluster**, thực hiện **Browse** đến 2 Server *BKAP-SRV12-01* và *BKAP-SRV12-02* , click vào **Next**.



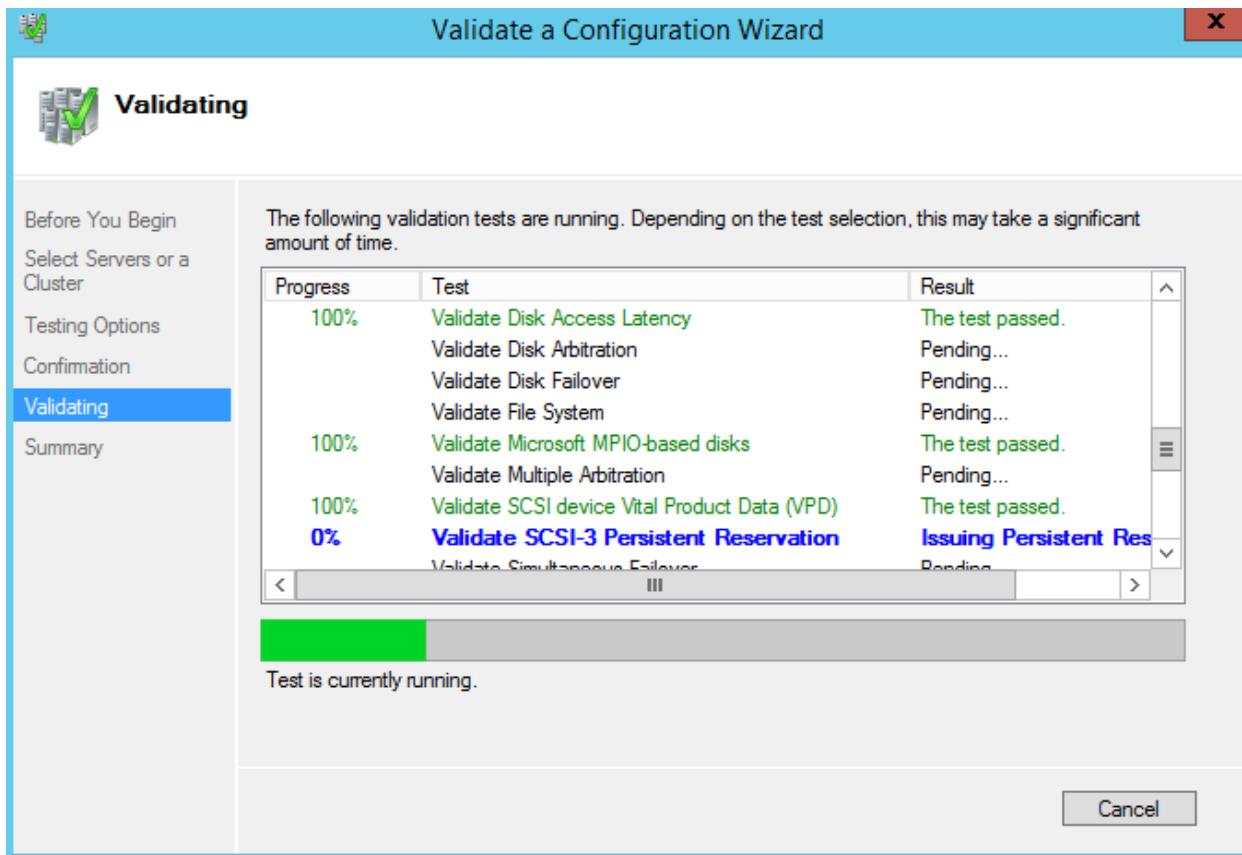
- Tại cửa sổ **Testing Options**, click chọn vào **Run all tests (recommended)**, click vào **Next**.

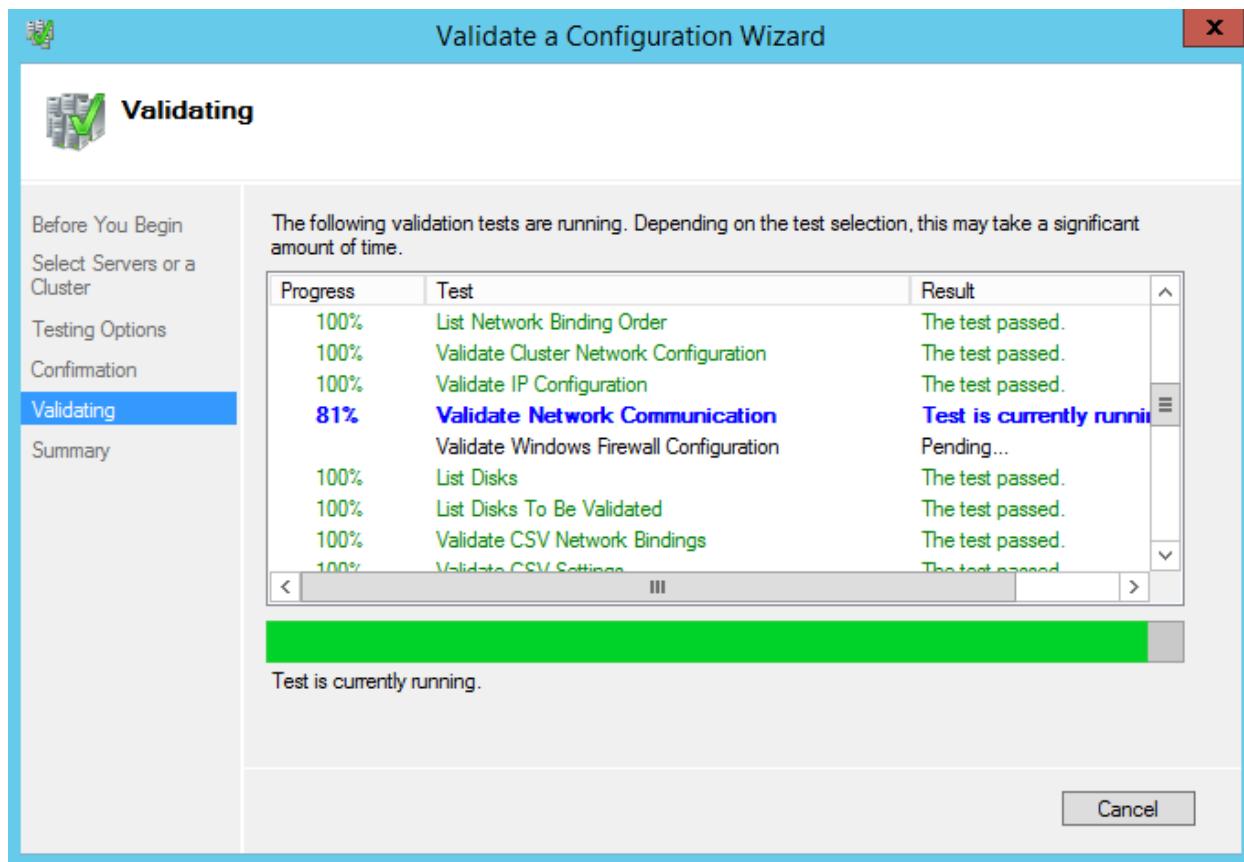


- Tại cửa sổ **Confirmation**, click vào **Next**.

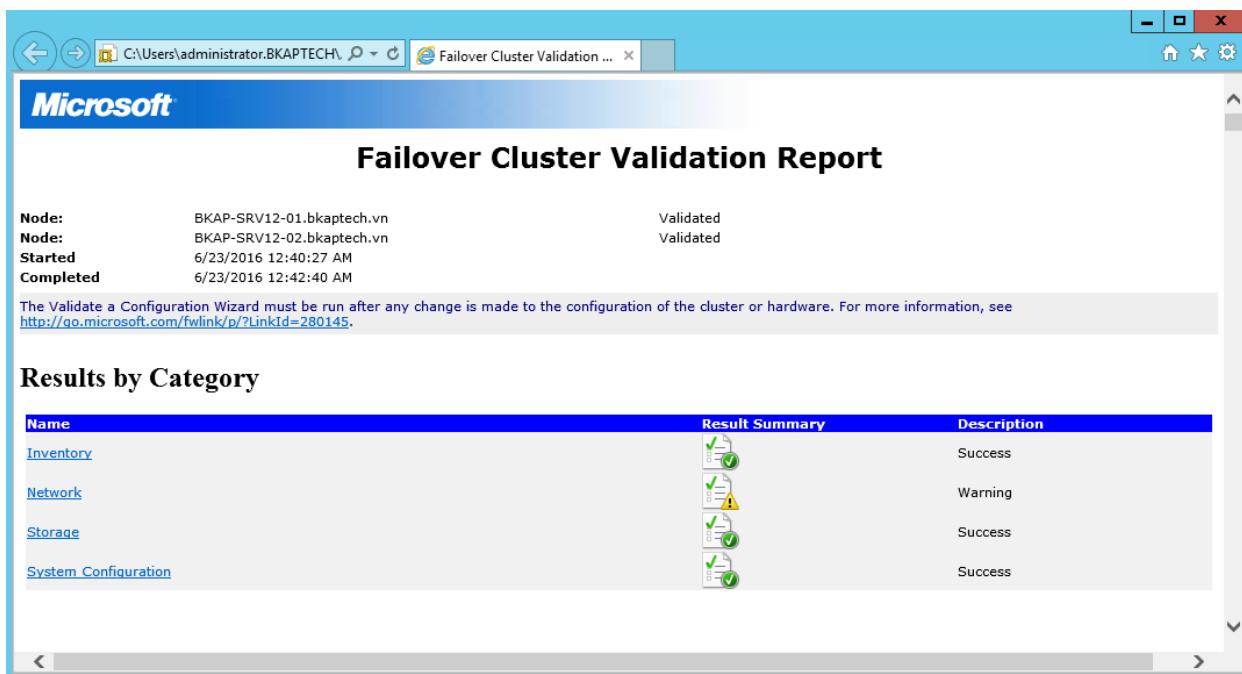
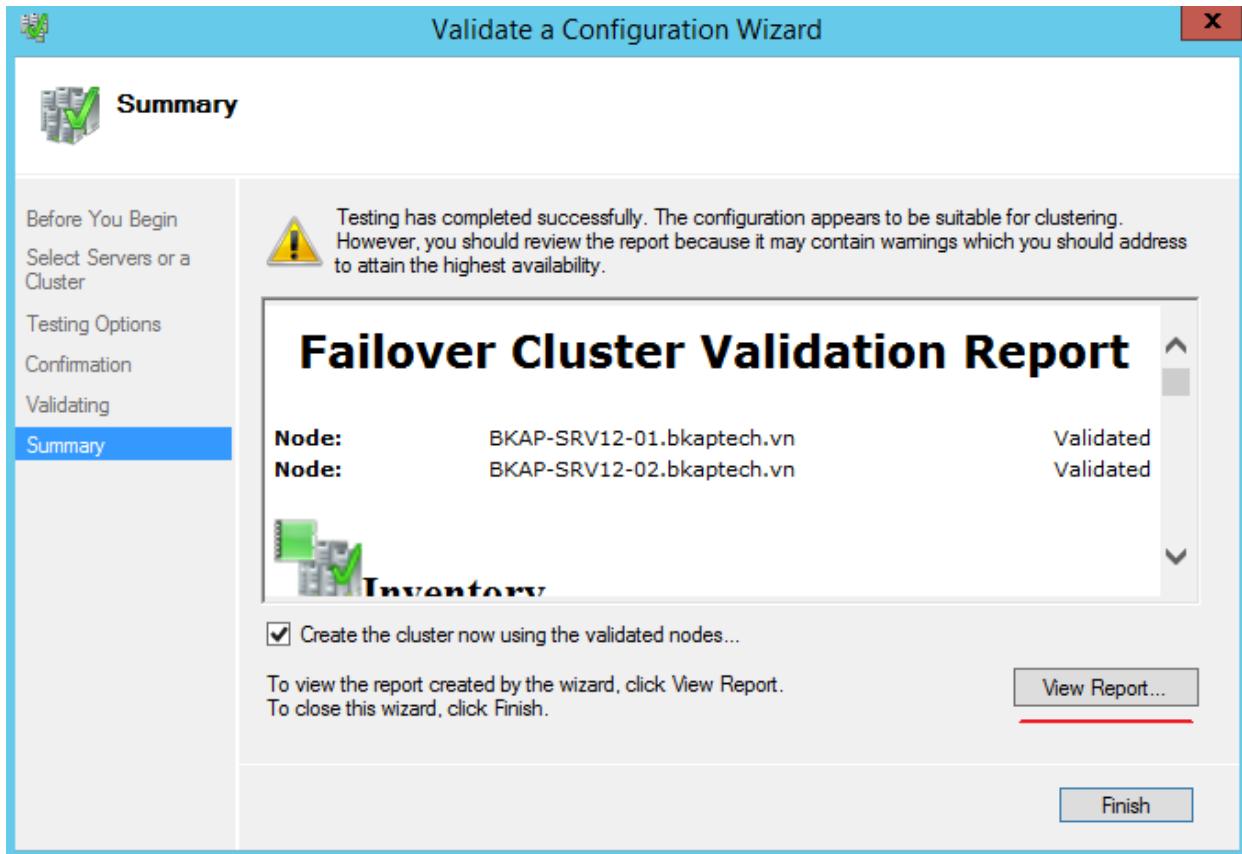


- Server tiến hành kiểm tra.

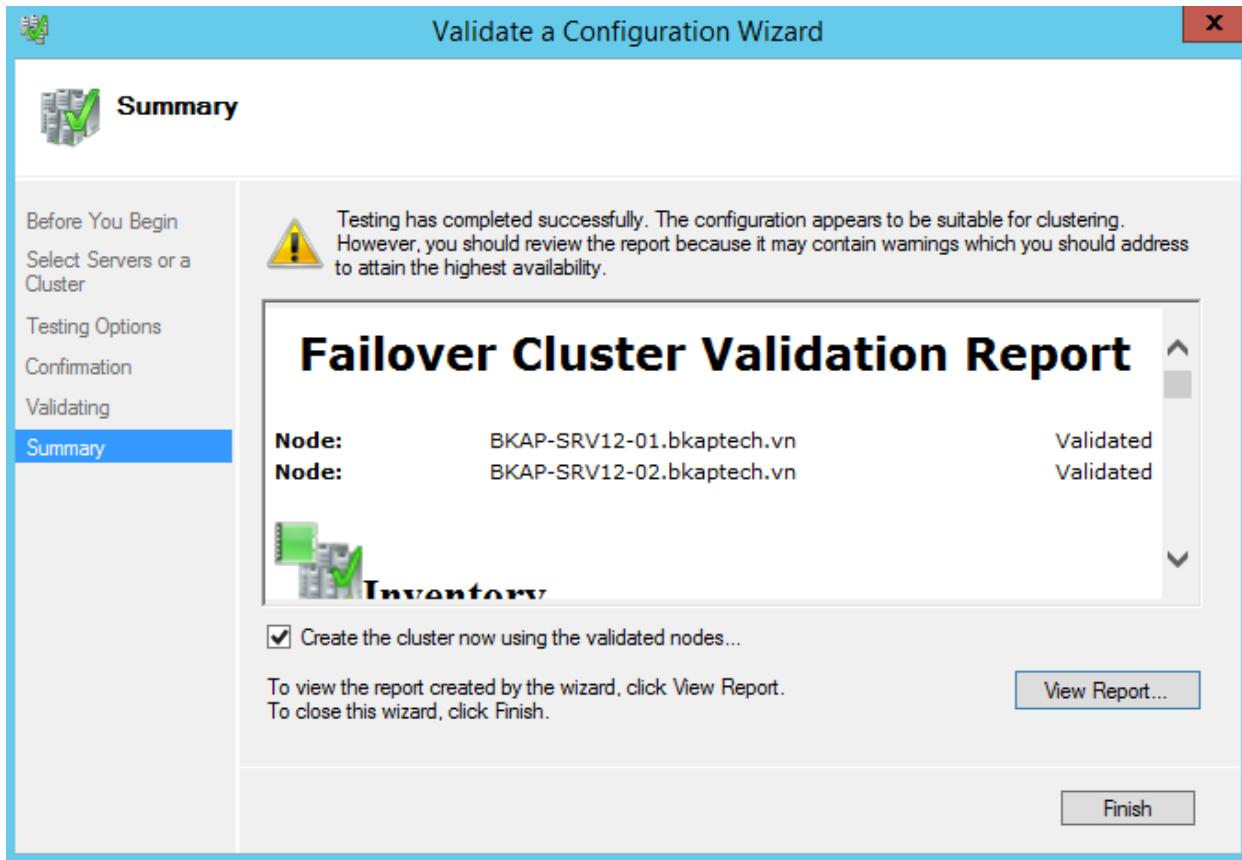




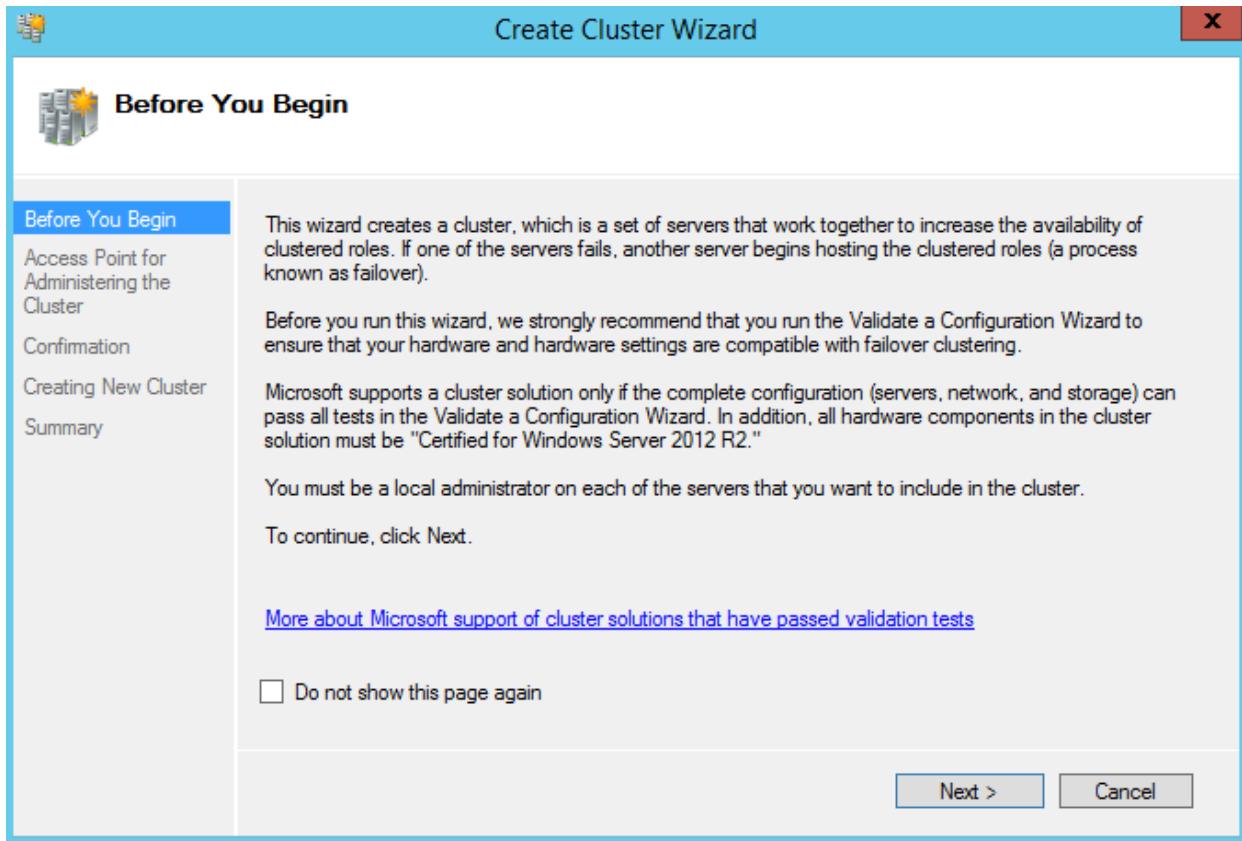
- Tại cửa sổ **Summary**, click vào **View Report...** để xem báo cáo.



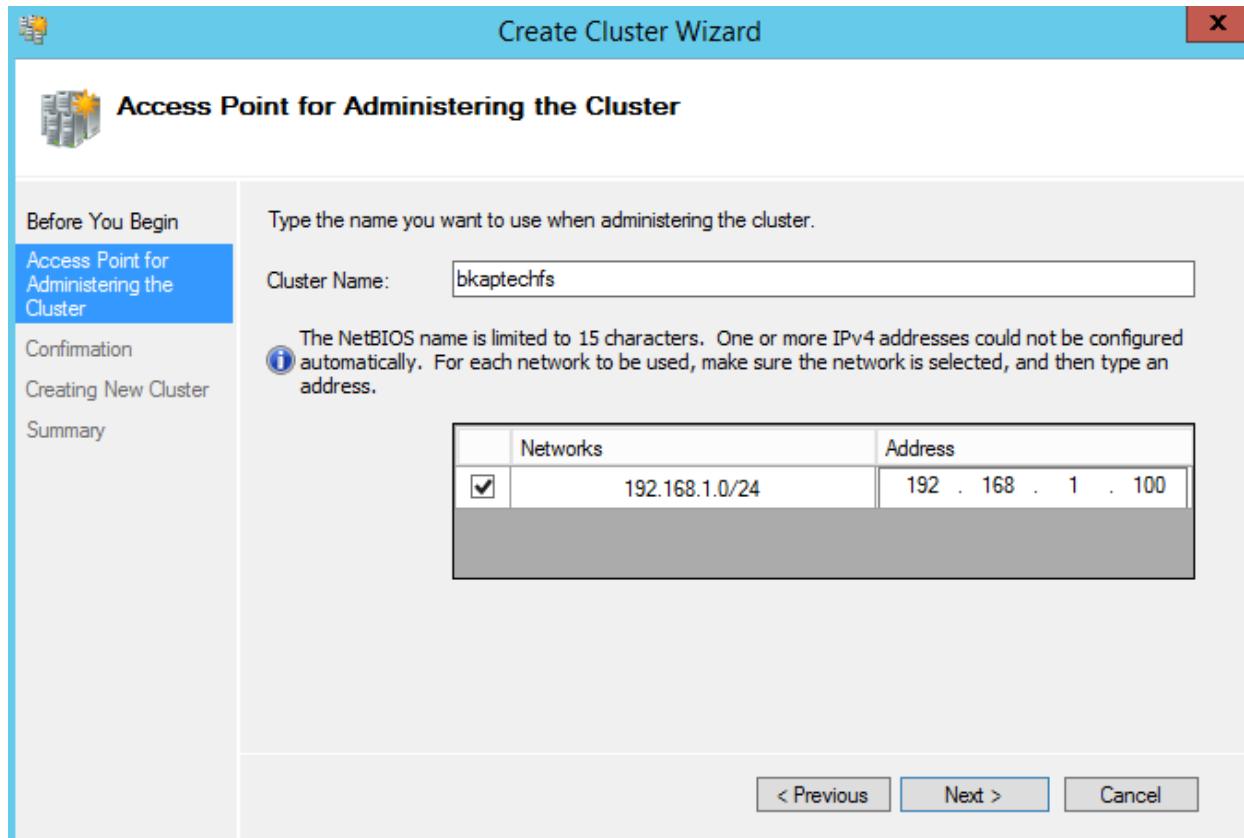
- Click vào **Finish** tại cửa sổ **Summary**.



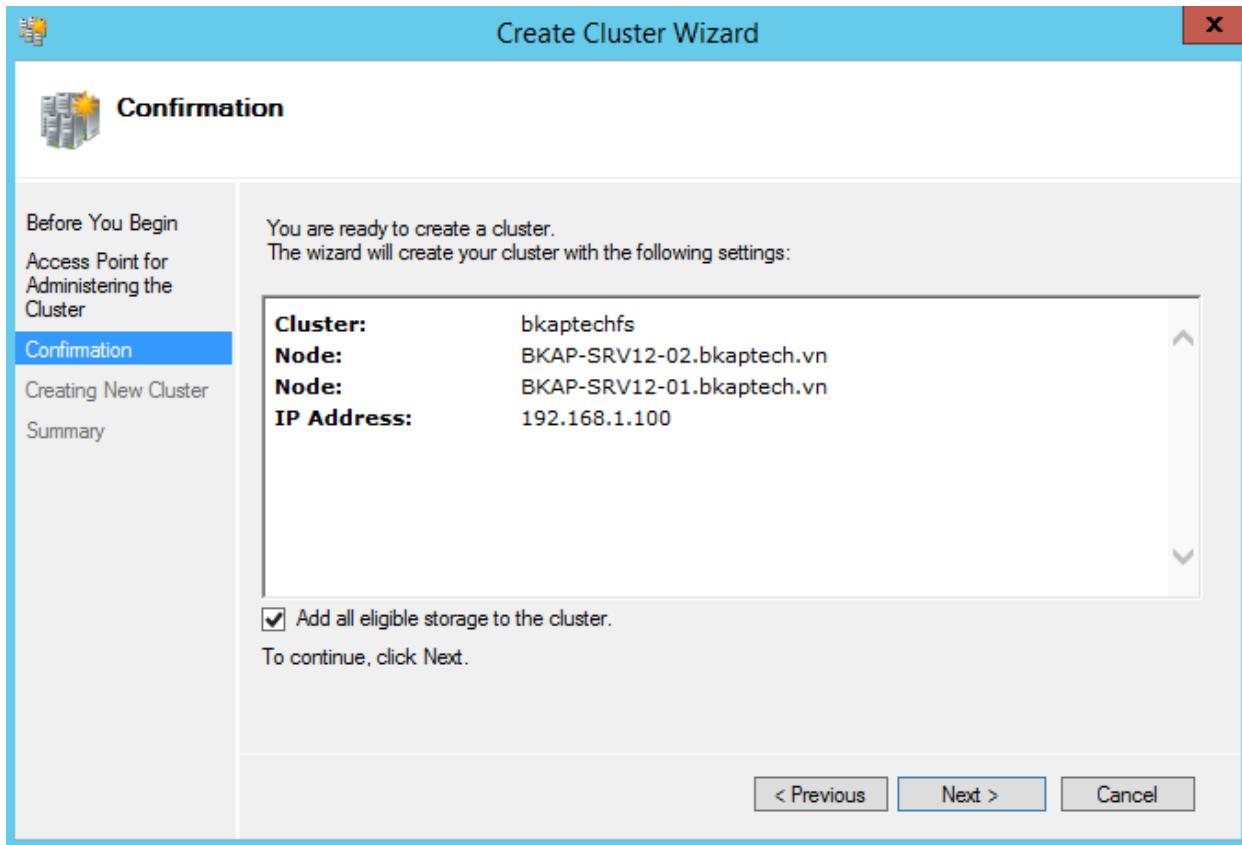
- Tại cửa sổ **Create Cluster Wizard / Before You Begin**, click vào **Next**.



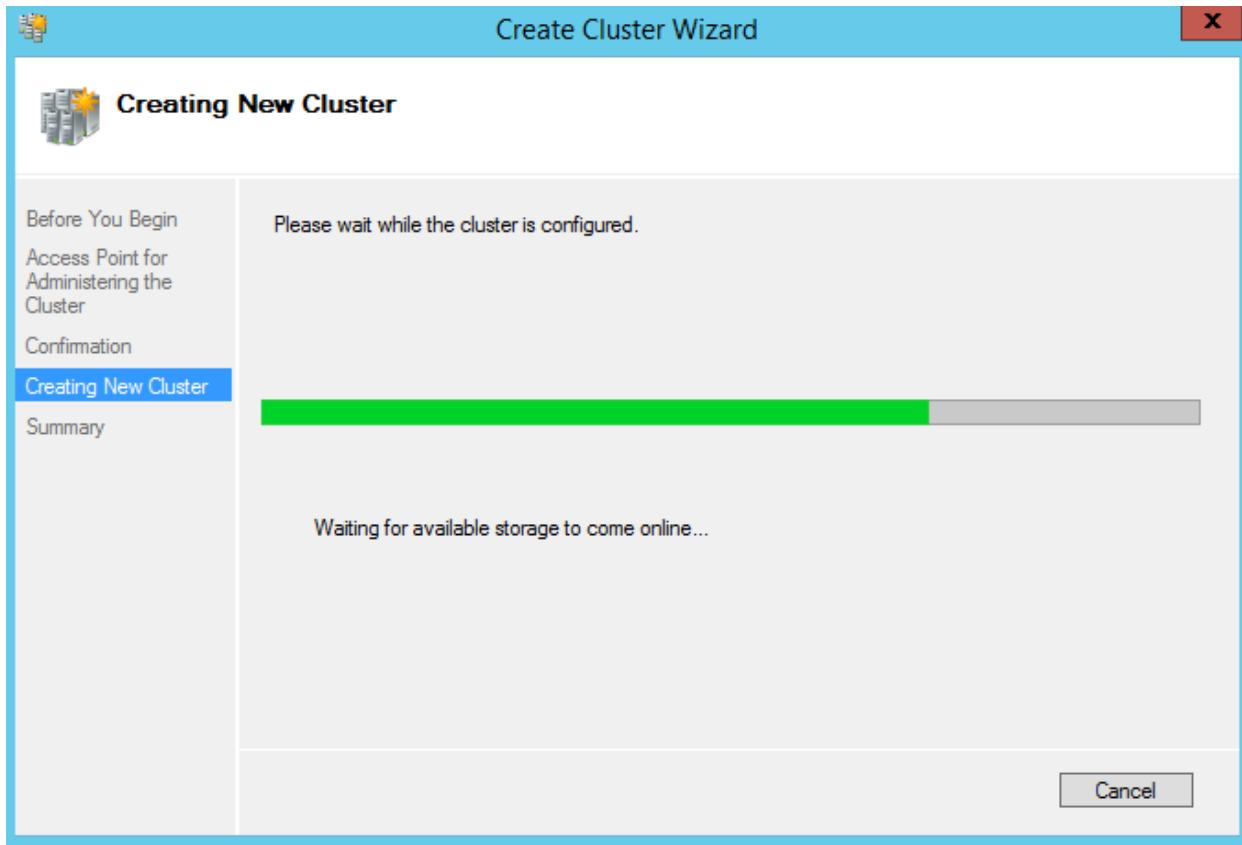
- Tại cửa sổ **Access Point for Administering the Cluster**, tại mục **Cluster Name**, nhập vào tên **bkaptechfs** , tại khung bên dưới, nhập vào địa chỉ IP **192.168.1.100**, click vào **Next**.



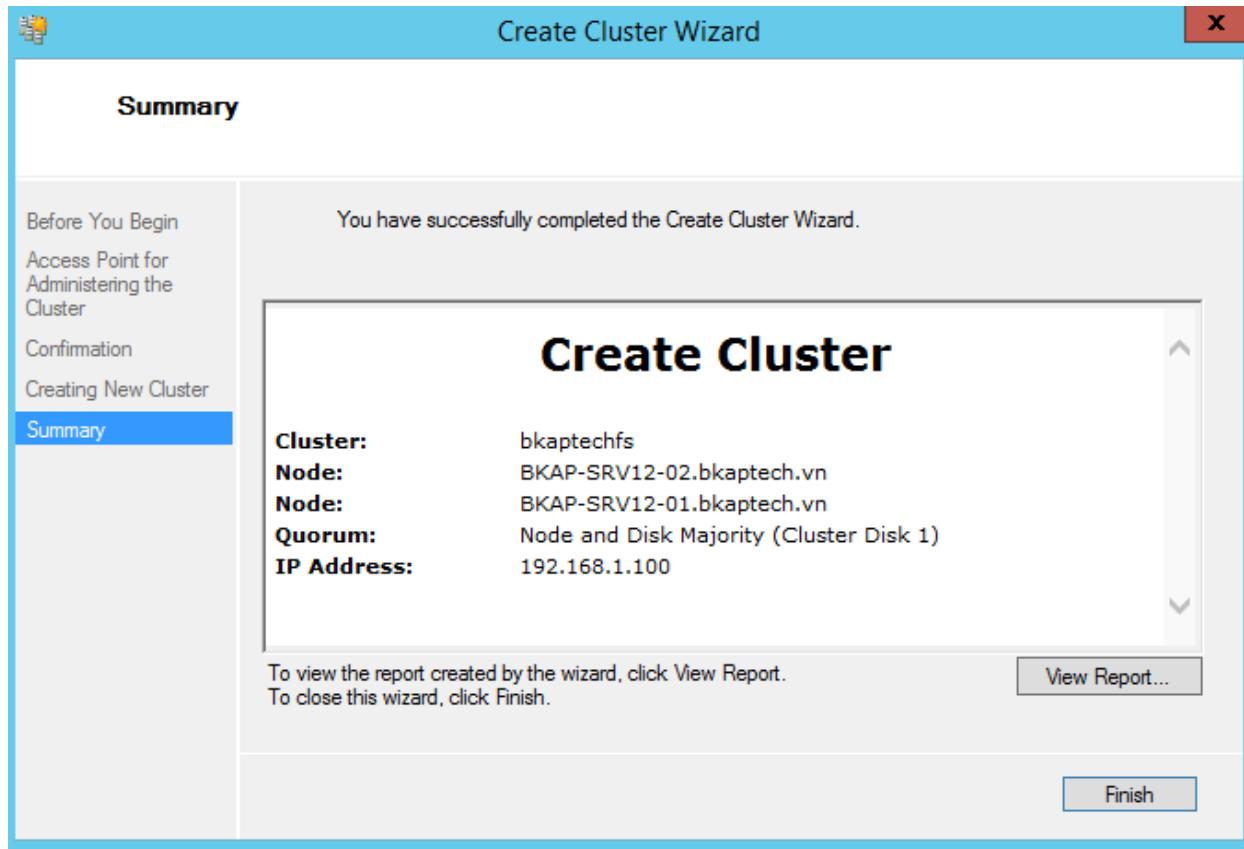
- Tại cửa sổ **Confirmation**, click vào **Next**.



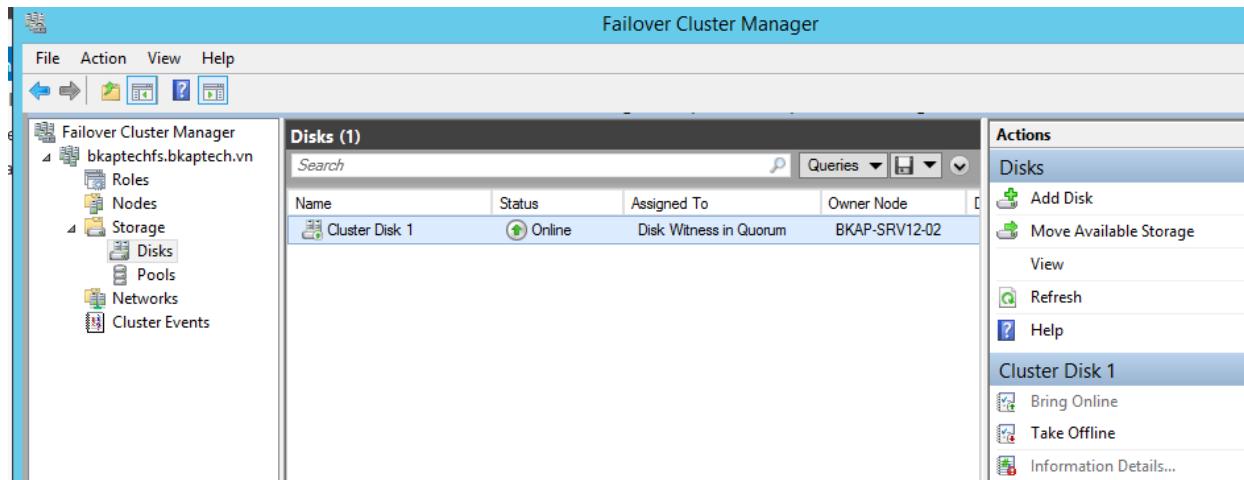
- Chờ đợi Server cấu hình:



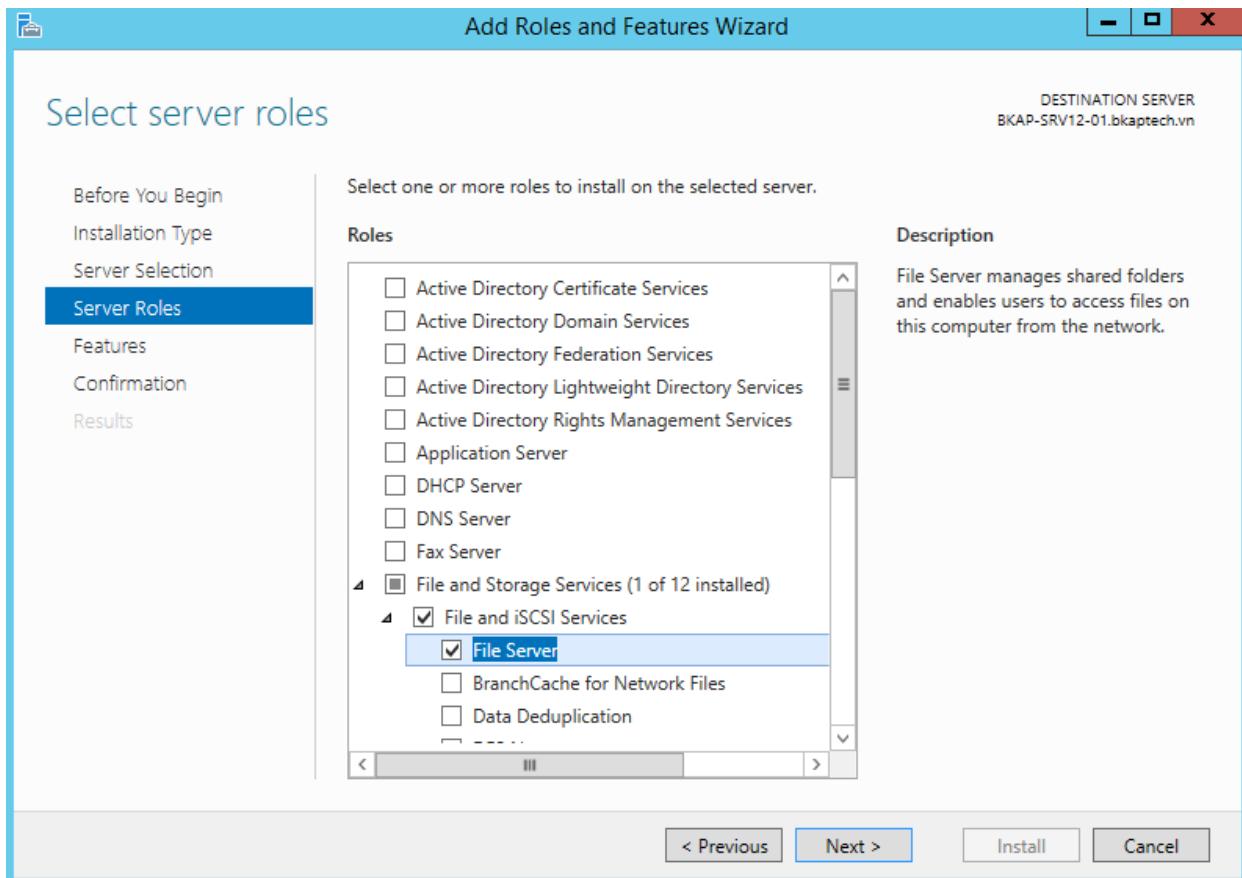
- Tại cửa sổ **Summary**, click vào **Finish**.



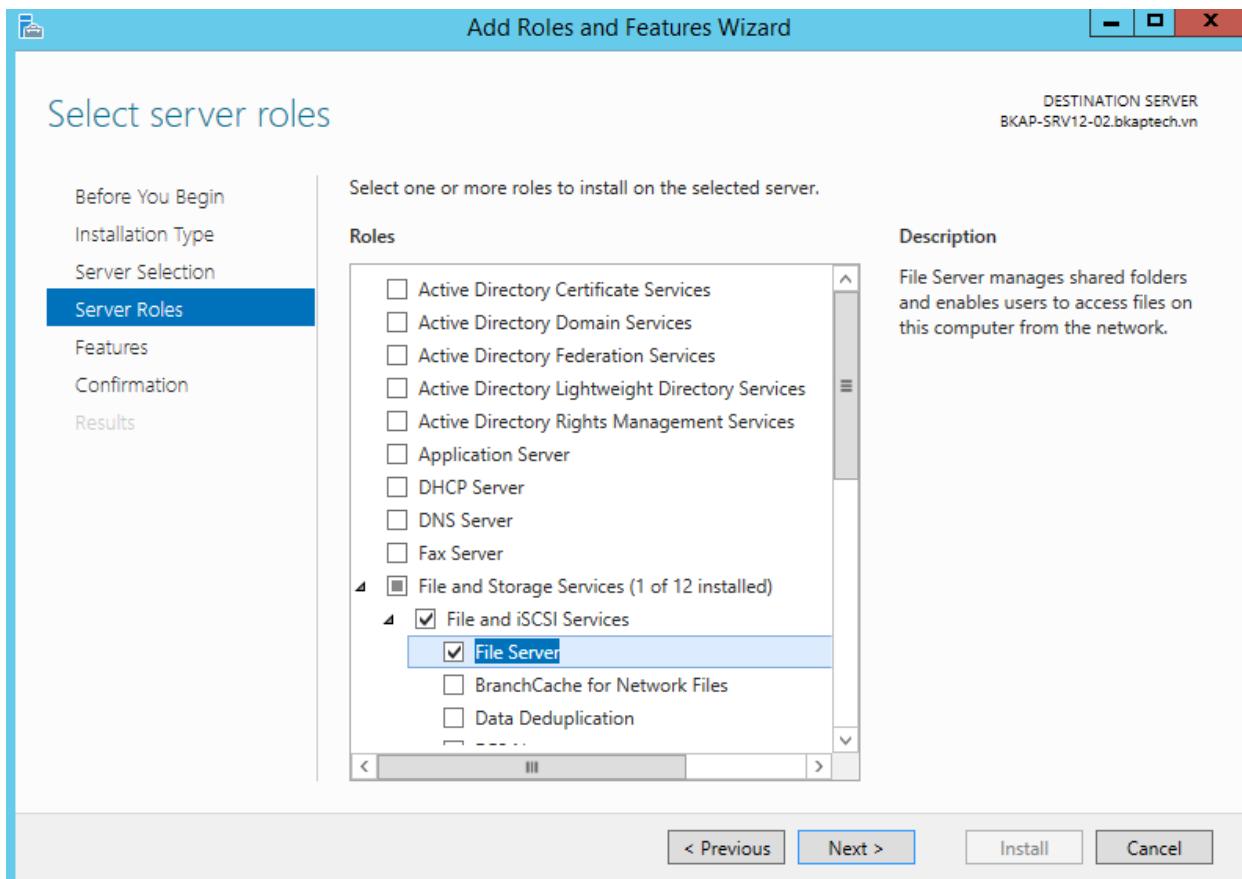
- Trong cửa sổ **Failover Cluster Manager**, click vào **Storage / Disks**, kiểm tra **Cluster Disk 1** đã được tạo.



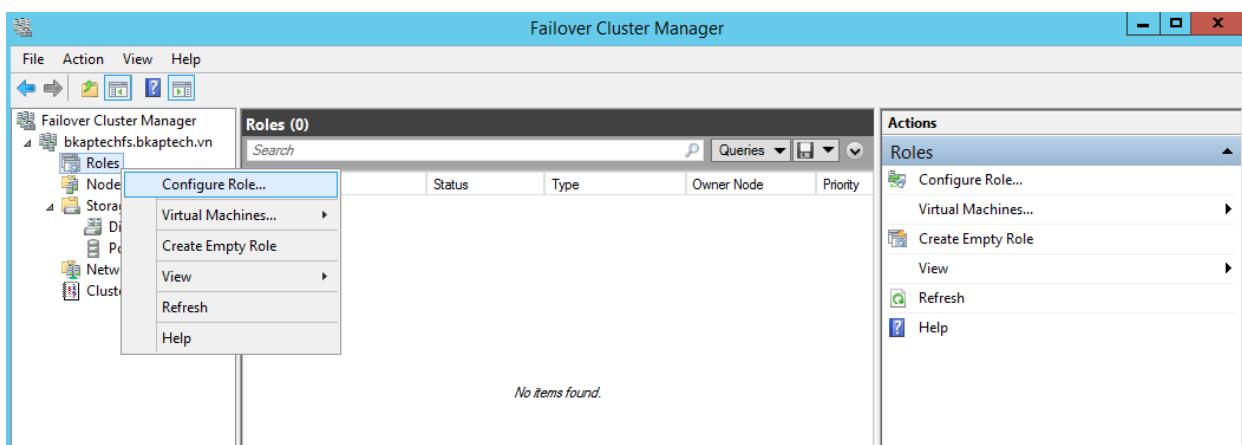
- Thực hiện cài đặt File Server.



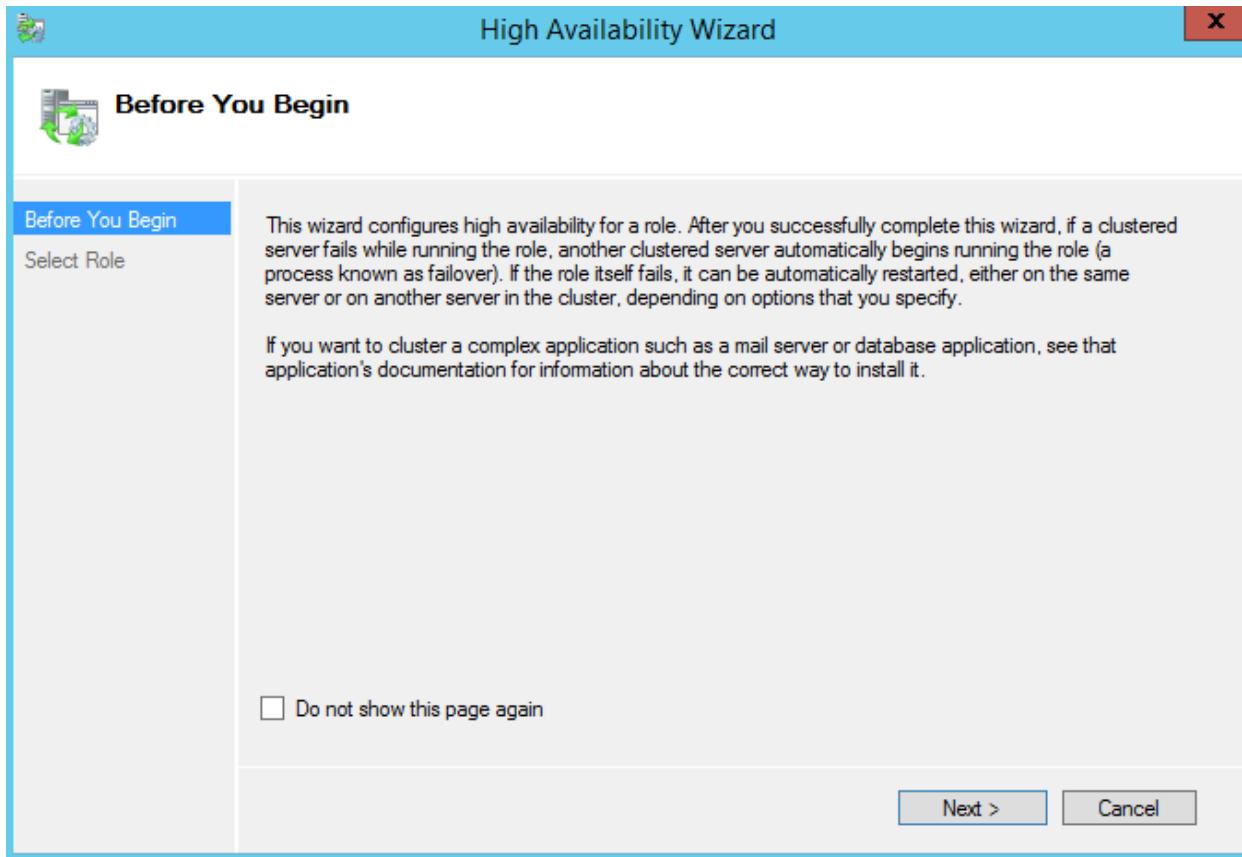
- Chuyển sang máy BKAP-SRV12-02, thực hiện cài đặt **File Server**.



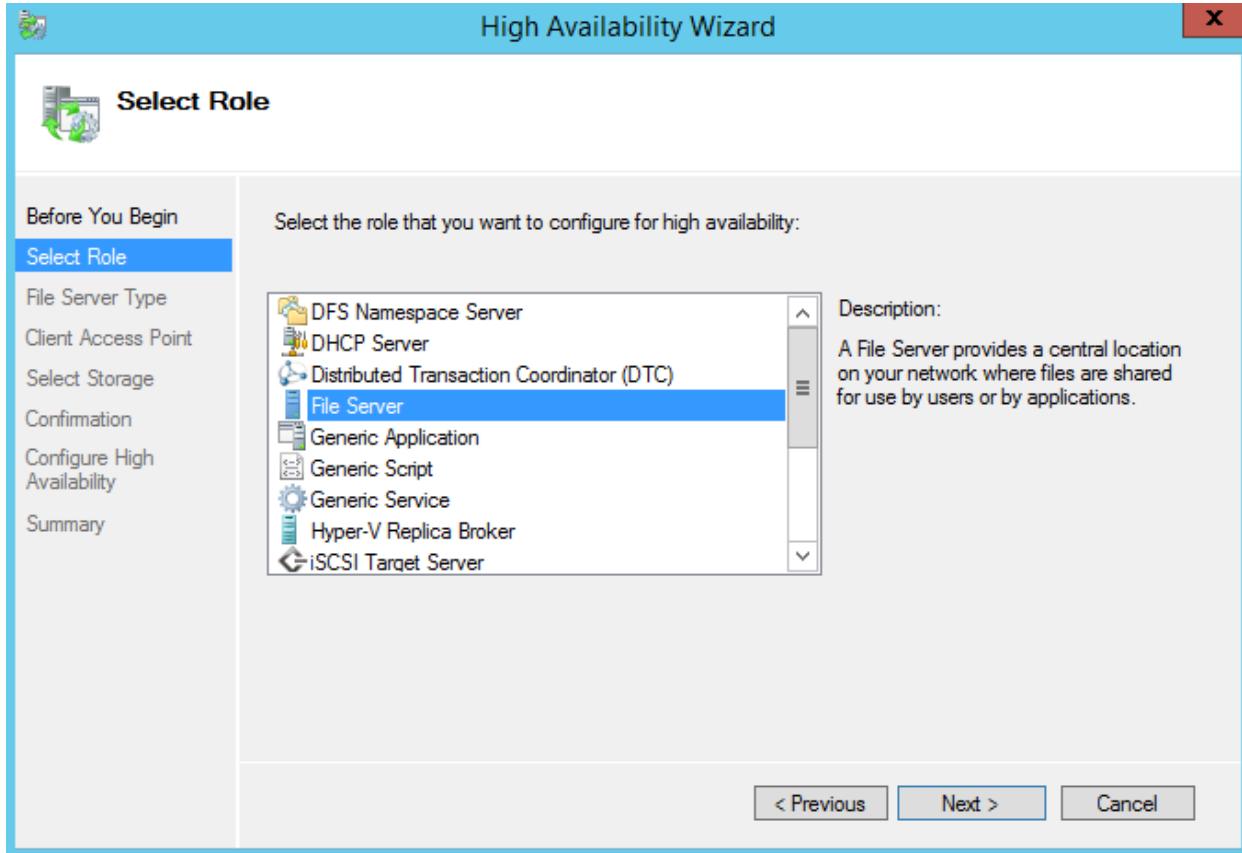
- Chuyển về máy BKAP-SRV12-01, cấu hình đồng bộ **File Server**.
 - Trong cửa sổ **Failover Cluster Manager**, click vào **Roles / Configure Role...**



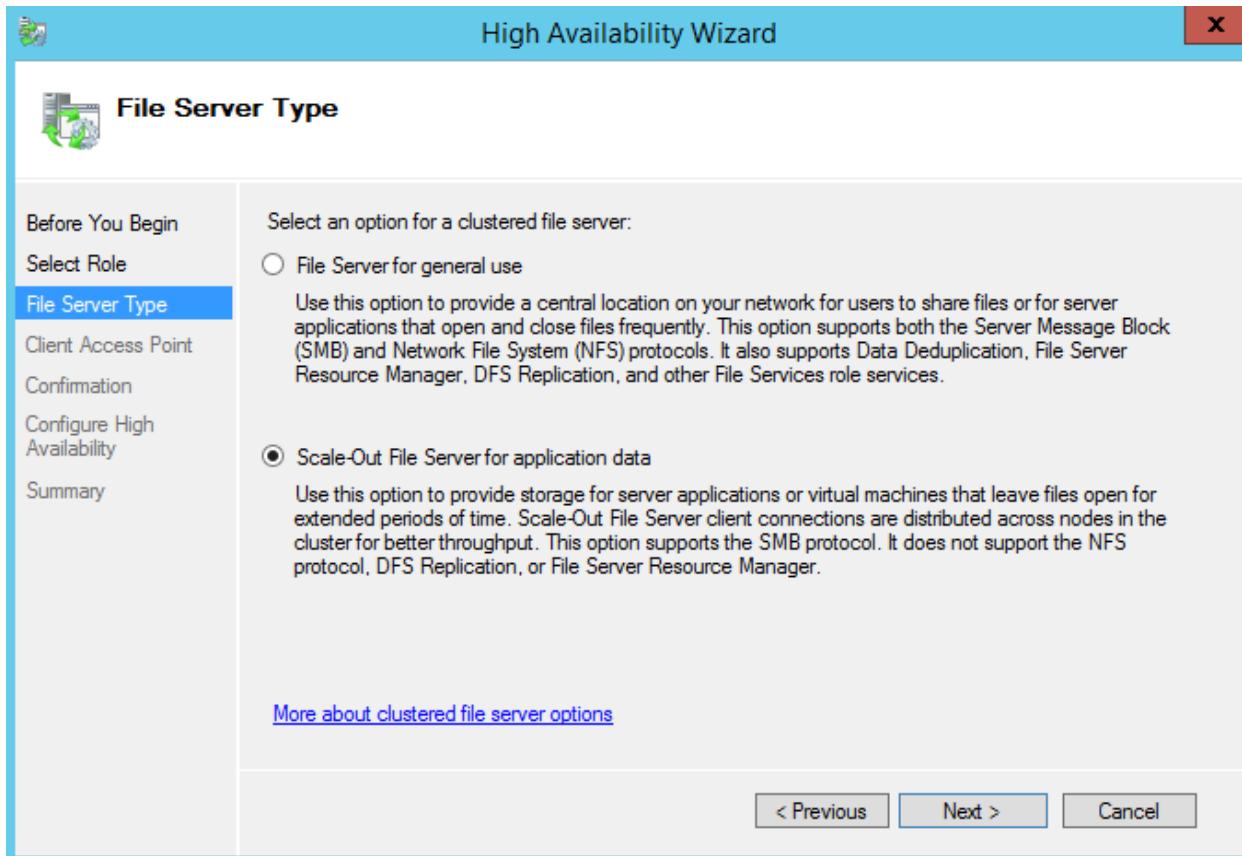
- Trong cửa sổ **Before You Begin**, click vào **Next**.



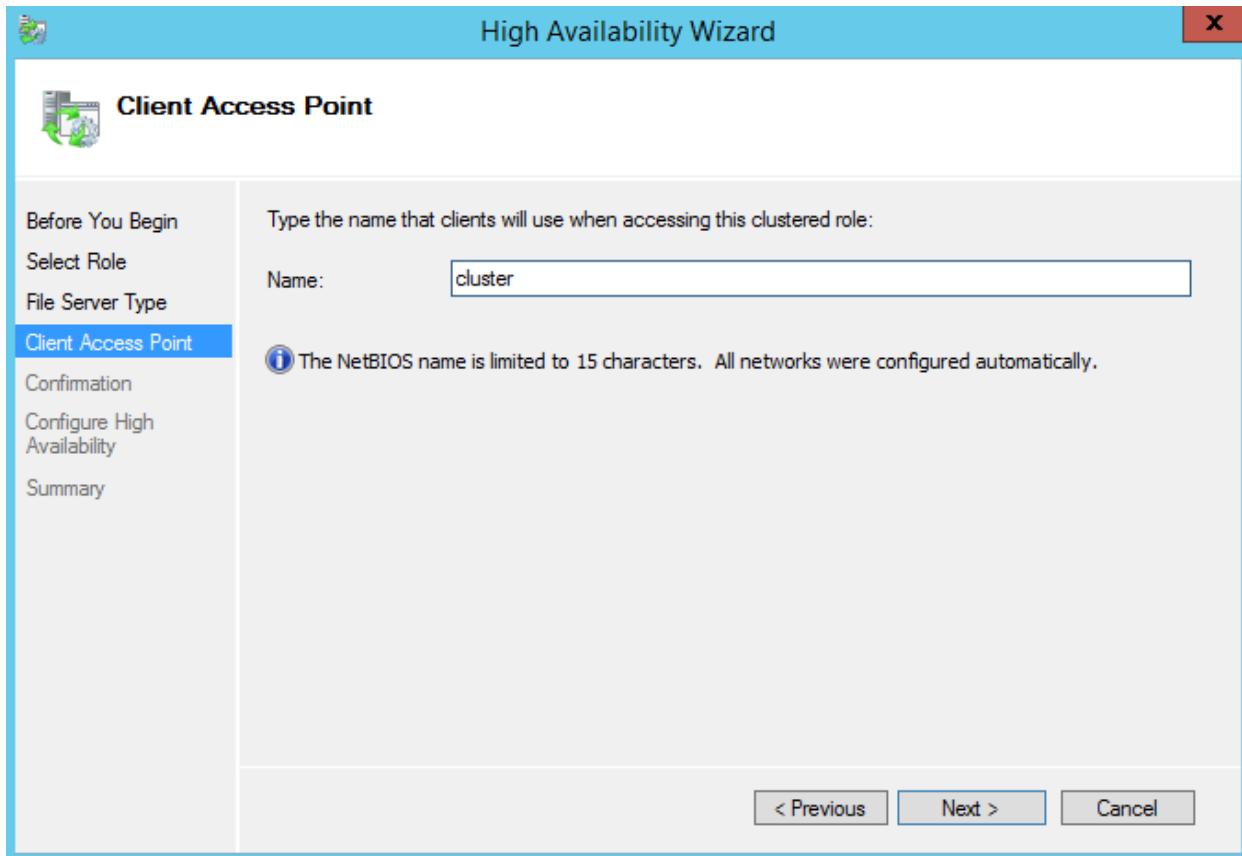
- Tại cửa sổ **Select Role**, click chọn vào **File Server**, click vào **Next**.



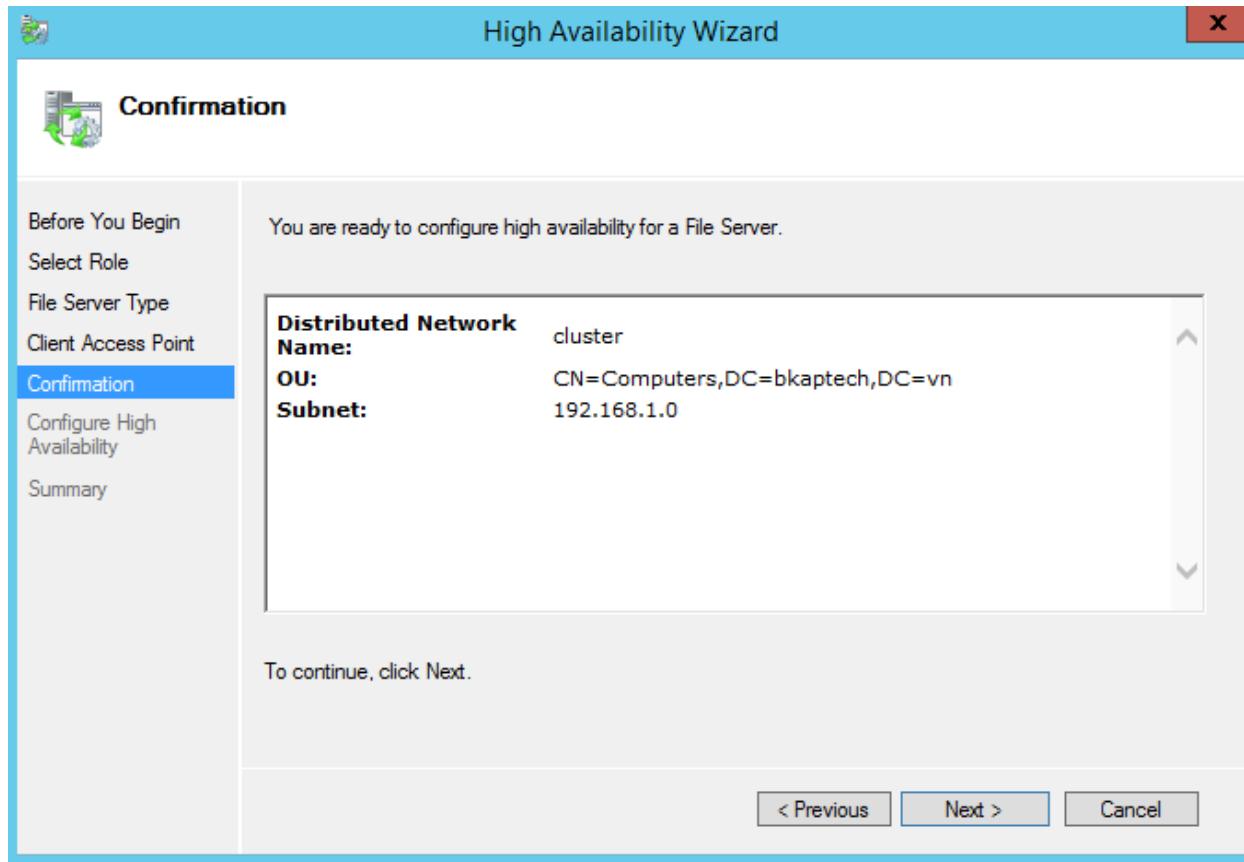
- Tại cửa sổ **File Server Type**, click vào **Scale-Out File Server for application data**, click vào **Next**.



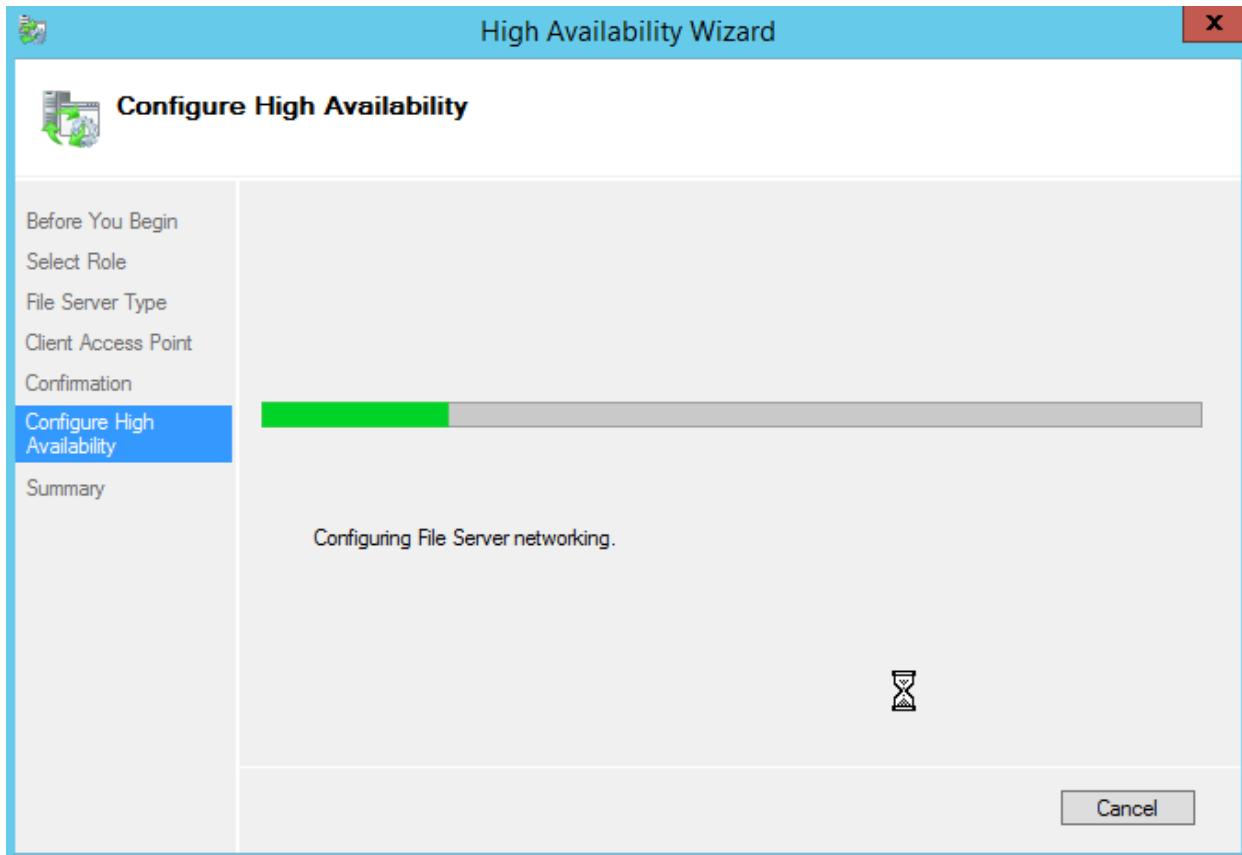
- Tại cửa sổ **Client Access Point**, nhập vào tại mục **Name:** cluster, click vào **Next**.



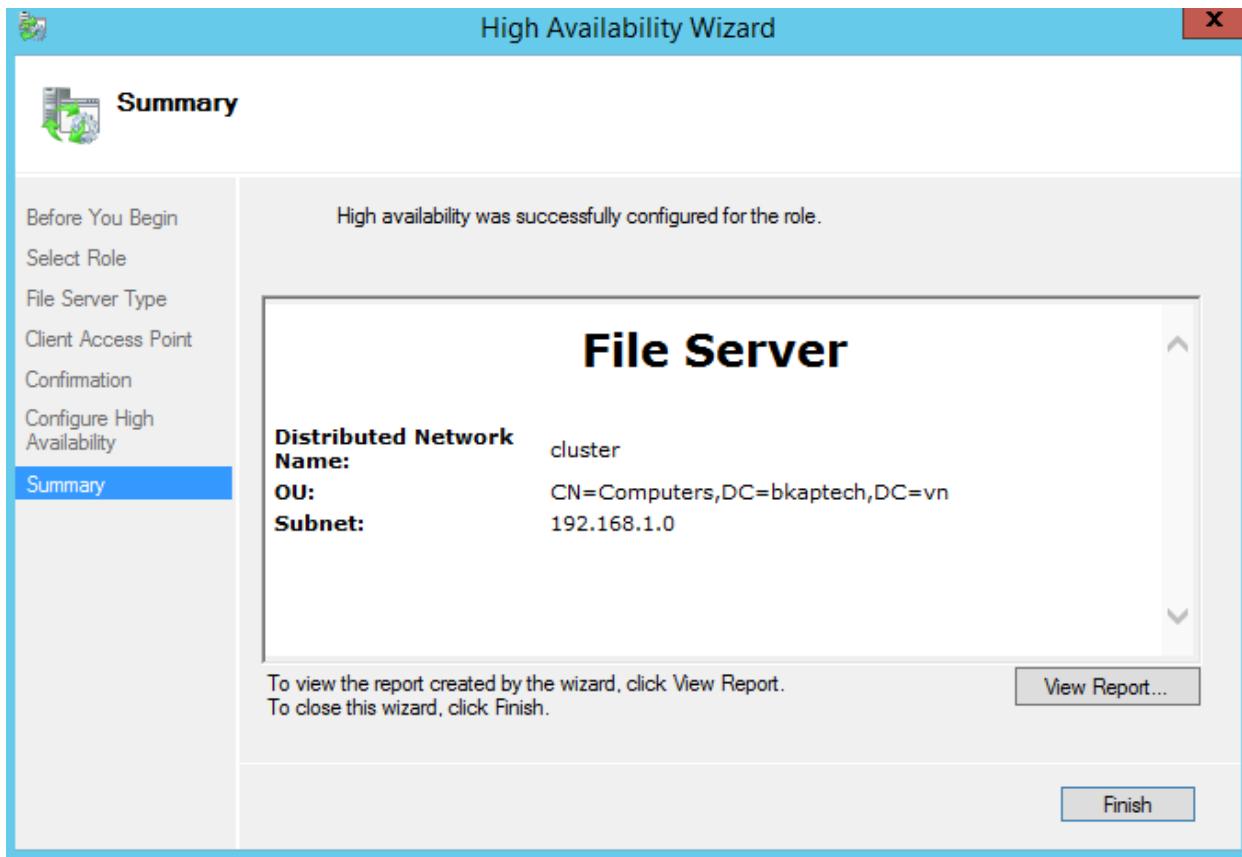
- Tại cửa sổ **Confirmation**, click vào **Next**.



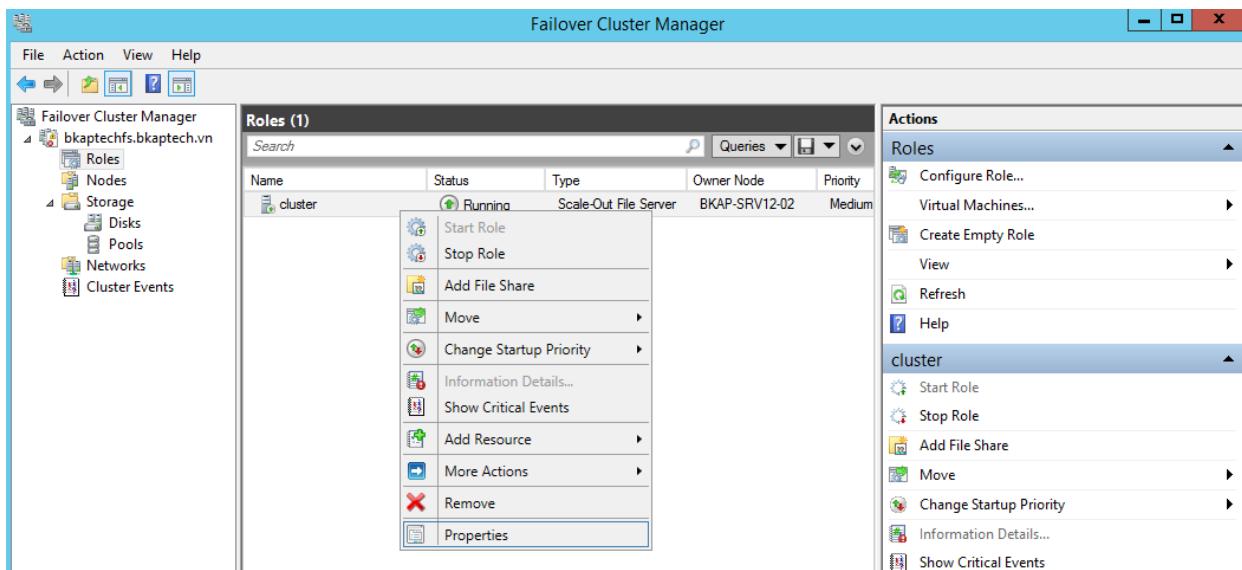
- Chờ đợi Server cấu hình.



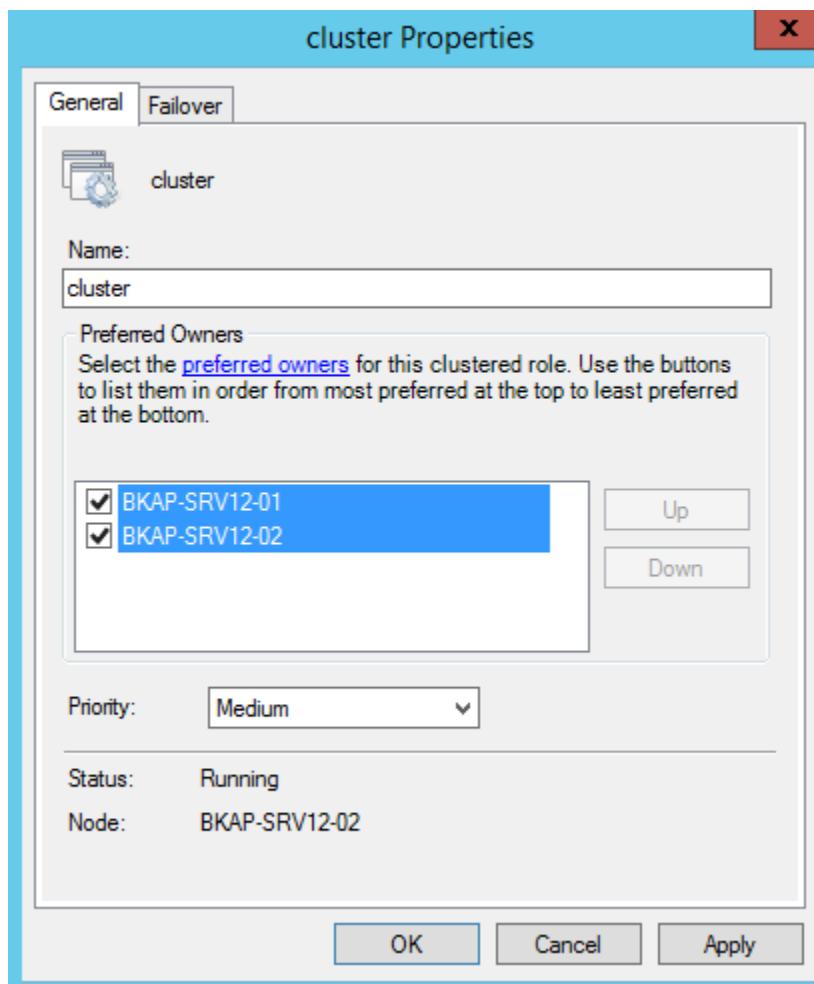
- Tại cửa sổ **Summary**, click vào **Finish**.



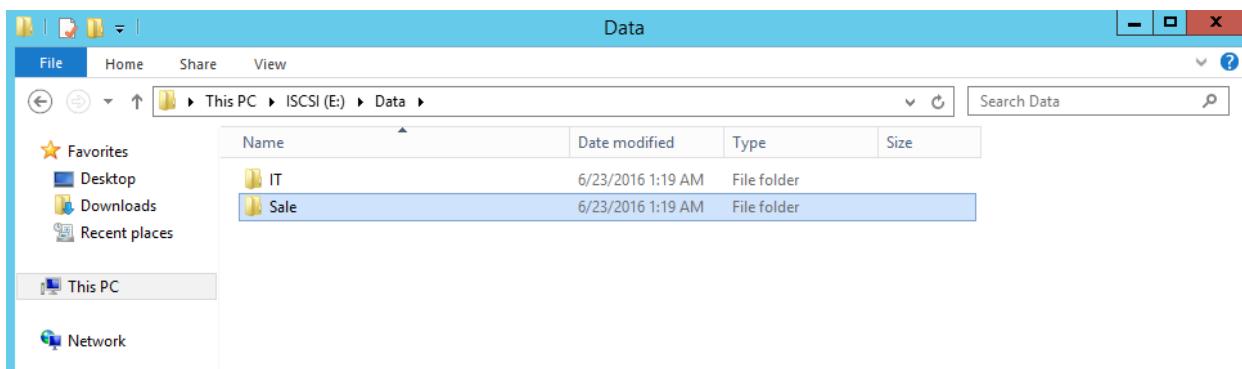
- Click chuột phải tại cluster, chọn **Properties**.



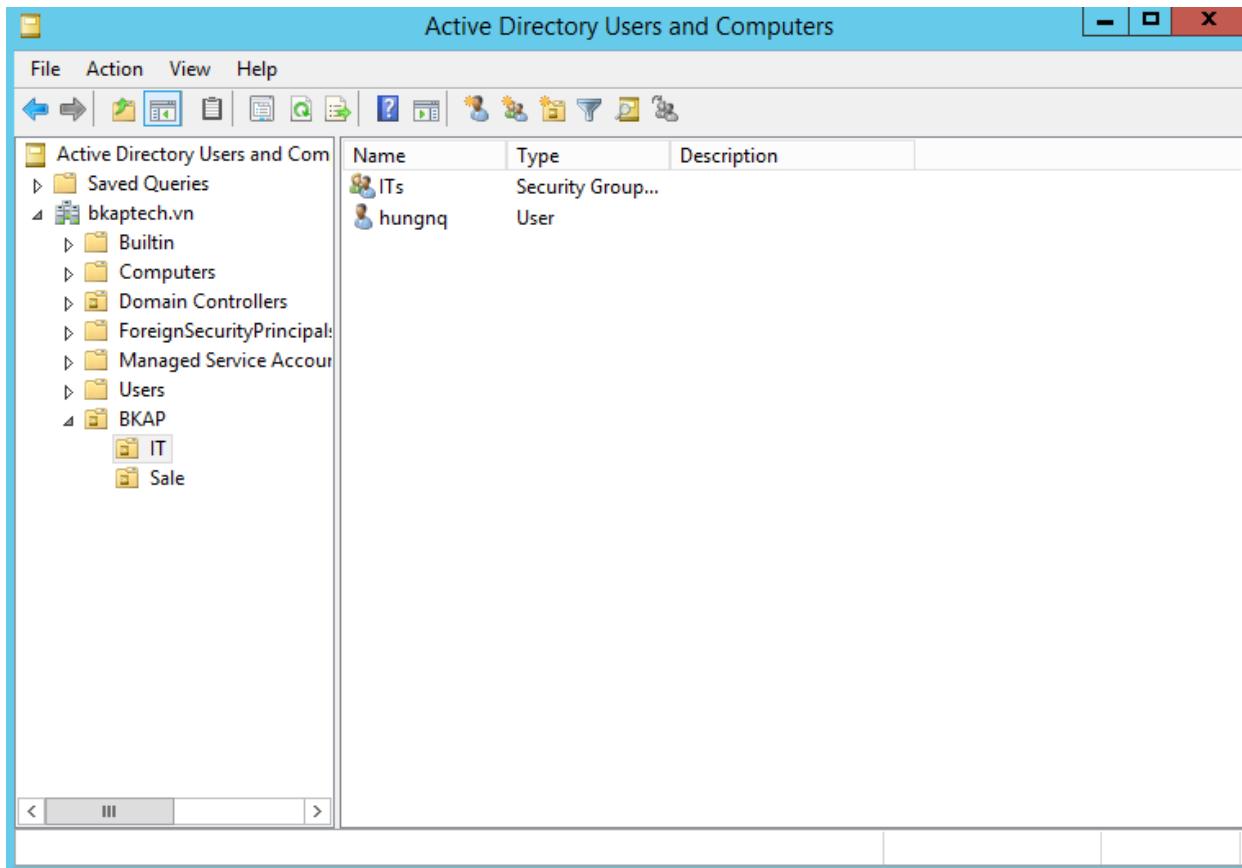
- Tại cửa sổ **cluster Properties**, click chọn vào cả 2 Server, click **OK**.



- Chuyển sang máy **BKAP-SRV12-02**, vào ổ đĩa **ISCSI**, tạo folder **Data**, trong folder **Data**, tạo 2 folder **IT** và **Sale**, tạo các tài liệu bên trong folder **IT** và **Sale**.



- Chuyển về máy *BKAP-DC12-01*, tạo OU theo hình dưới.



Active Directory Users and Computers

File Action View Help

Active Directory Users and Com

Saved Queries

bkaptech.vn

Builtin

Computers

Domain Controllers

ForeignSecurityPrincipal

Managed Service Account

Users

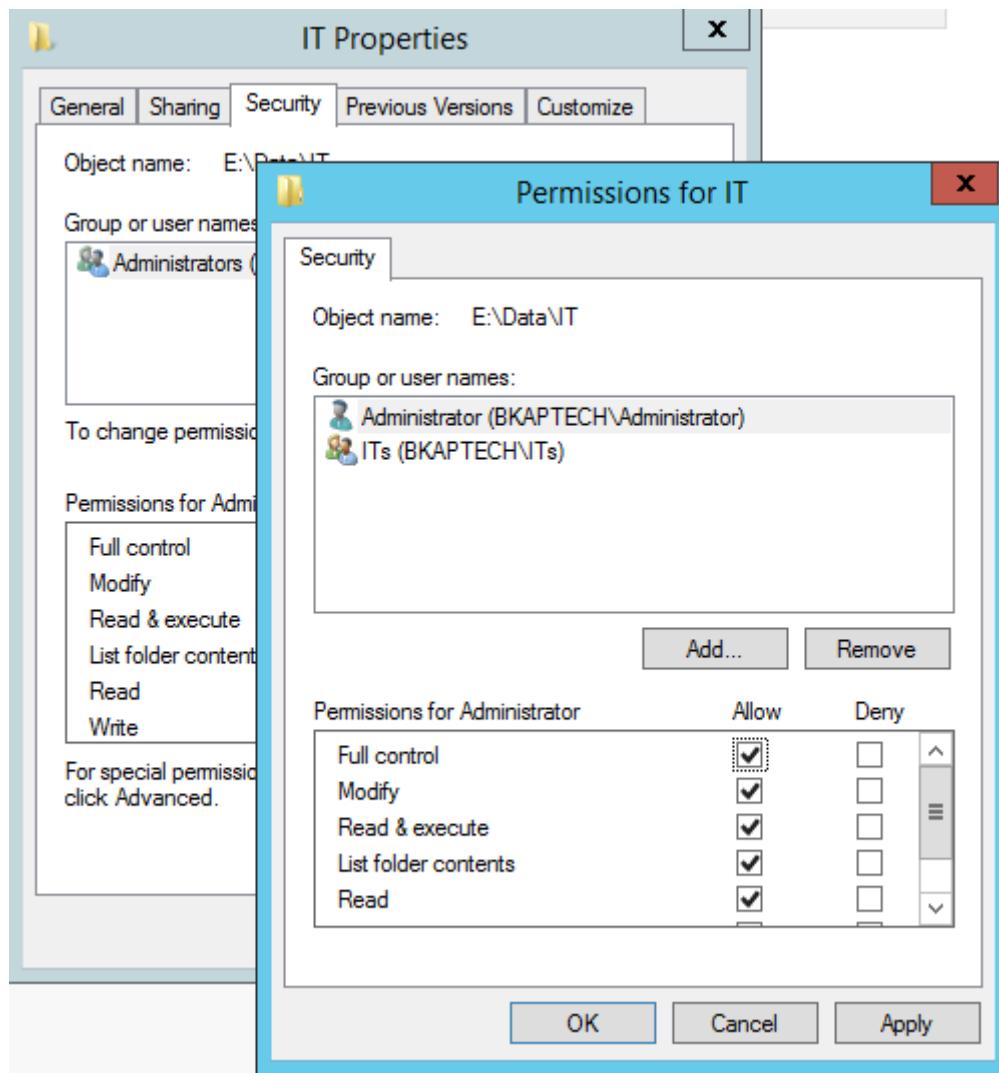
BKAP

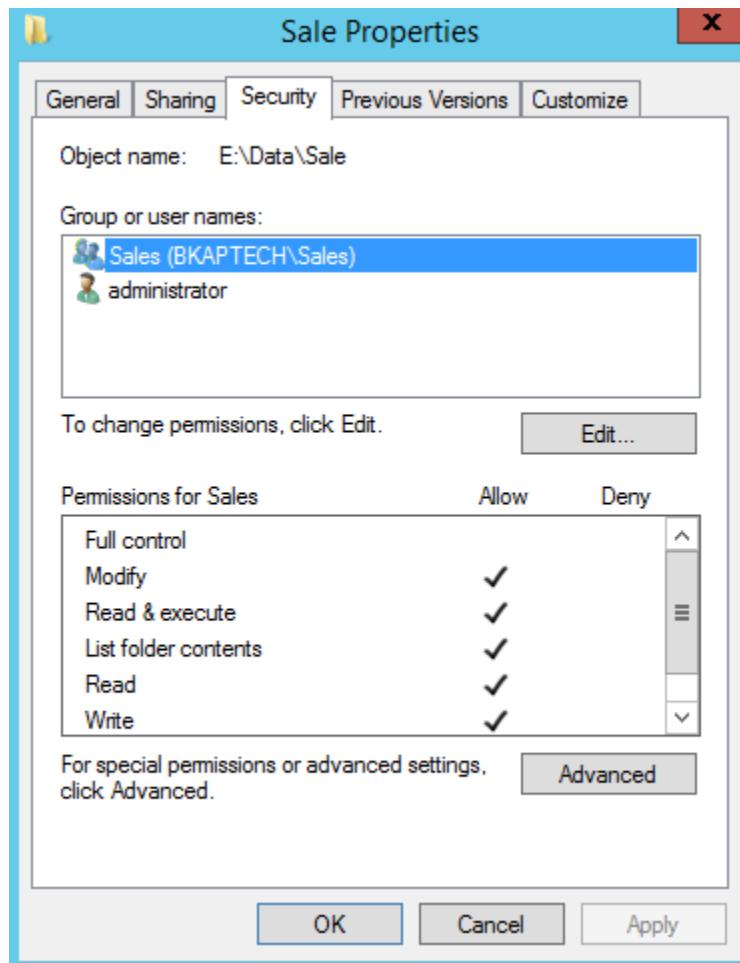
IT

Sale

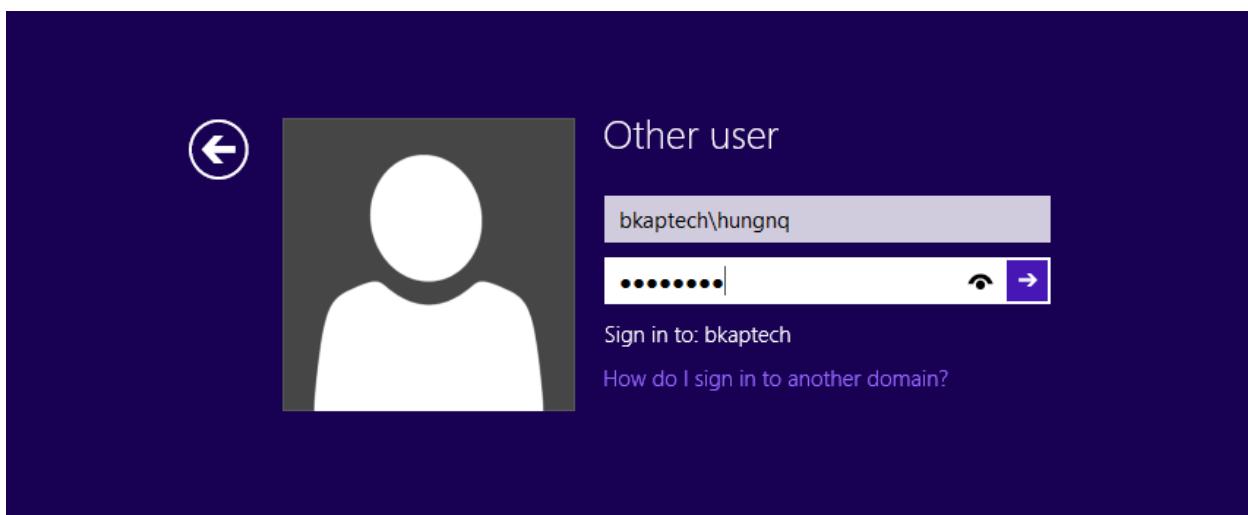
Name	Type	Description
Sales	Security Group...	
nghialv	User	

- Phân quyền chia sẻ trên thư mục Data / IT / Sale.

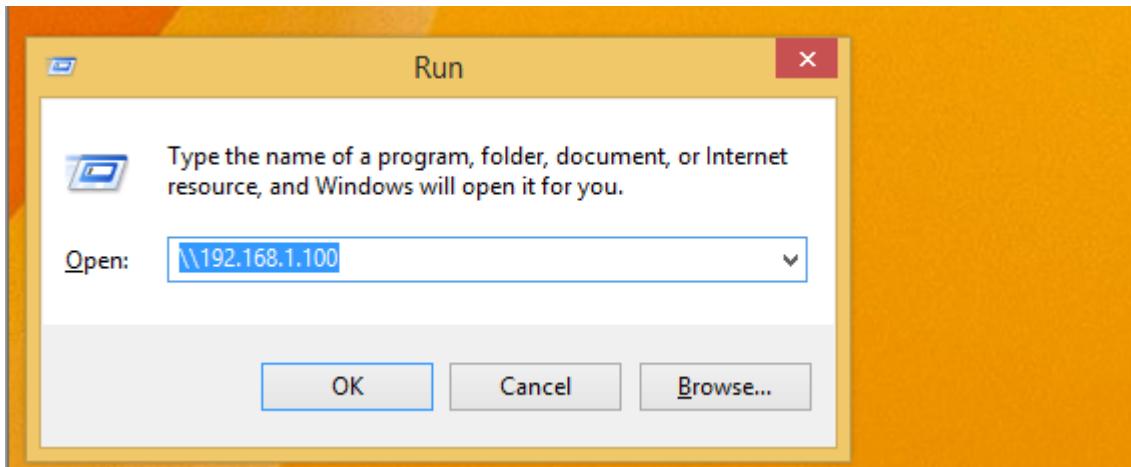




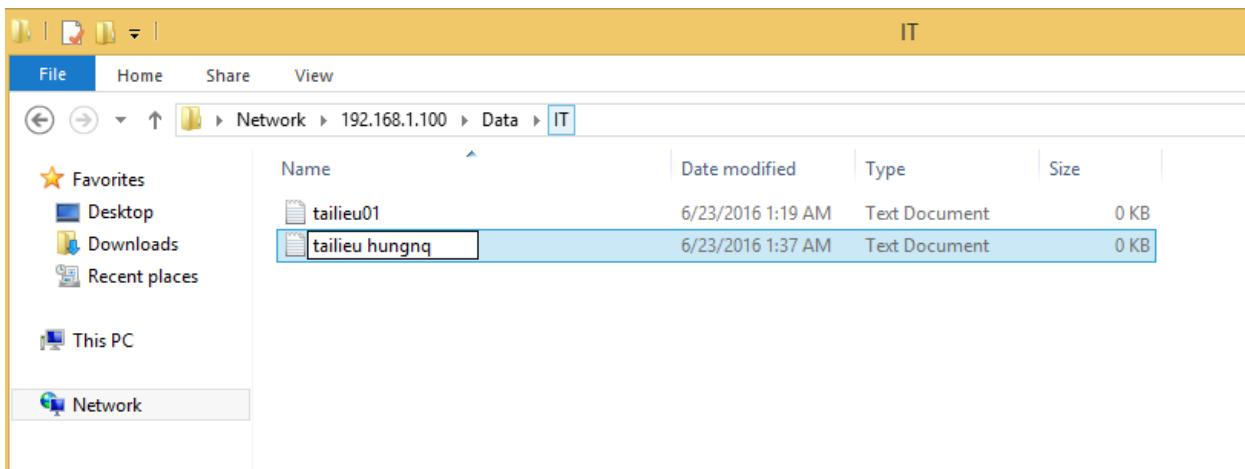
- Chuyển sang máy Client *BKAP-WRK08-01*, Join vào Domain, đăng nhập bằng user **hungnq** trong ou IT.



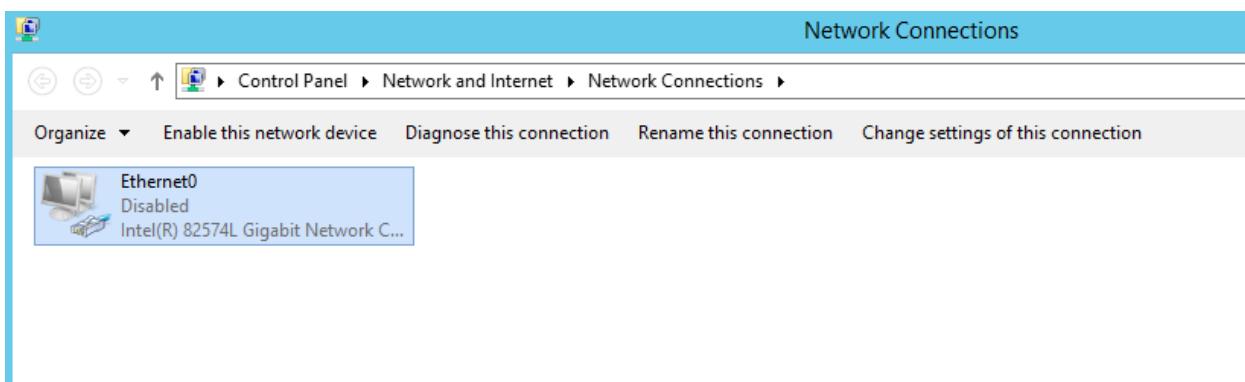
- Truy cập file bằng địa chỉ <\\192.168.1.100>



- Tạo thêm tài liệu trong thư mục IT.



- Chuyển về máy BKAP-SRV12-02, tắt card mạng để kiểm tra.



- Chuyển sang máy BKAP-WRK08-01 kiểm tra.

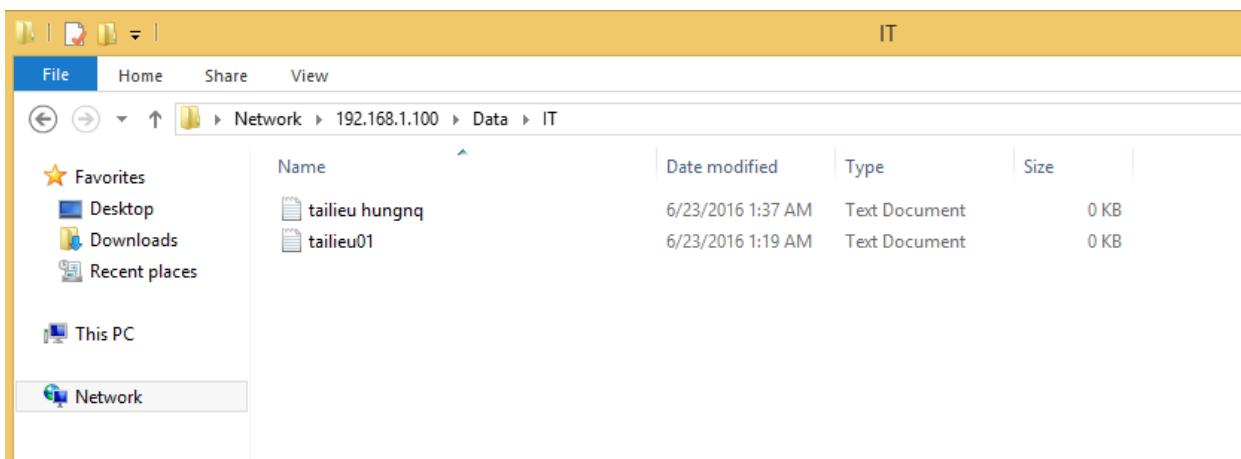
```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\hungnq>ping 192.168.1.100

Pinging 192.168.1.100 with 32 bytes of data:
Reply from 192.168.1.100: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\hungnq>
```



Bài 9 :**SAO LUU VÀ PHỤC HỒI DỮ LIỆU SỬ DỤNG WINDOWS SERVER BACKUP****Các nội dung chính được đề cập:**

- ✓ Cấu hình sao lưu và phục hồi dữ liệu sử dụng Windows Server Backup.

9. Sao lưu và phục hồi dữ liệu sử dụng Windows Server Backup**1.Yêu cầu bài lab:**

+ Trên Server *BKAP-SRV12-01*:

- Cài đặt **Windows Server Backup**.
- Thực hiện **Backup** và **Restore File**.
- Kiểm tra sau khi xóa File và khôi phục lại.

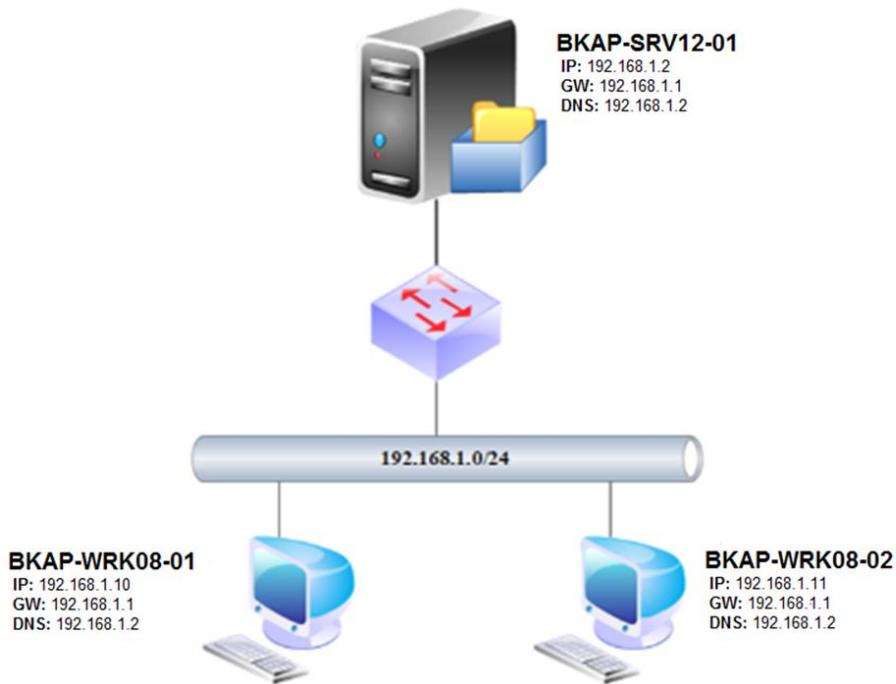
2.Yêu cầu chuẩn bị:

+ Máy Server *BKAP-SRV12-01* có 3 ổ **C , D , E**.

3.Mô hình lab:

HỆ THỐNG ĐÀO TẠO CNTT QUỐC TẾ BACHKHOA-APTECH

Sao lưu và phục hồi dữ liệu sử dụng Windows Server Backup

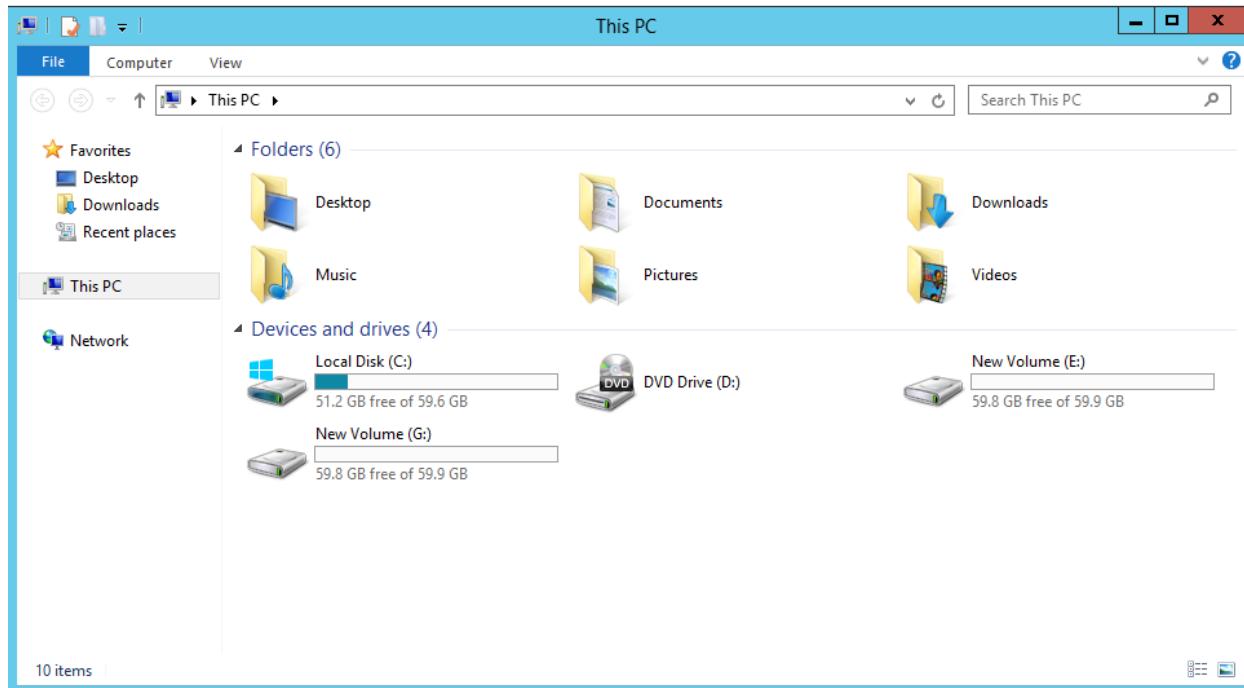


Sơ đồ địa chỉ như sau:

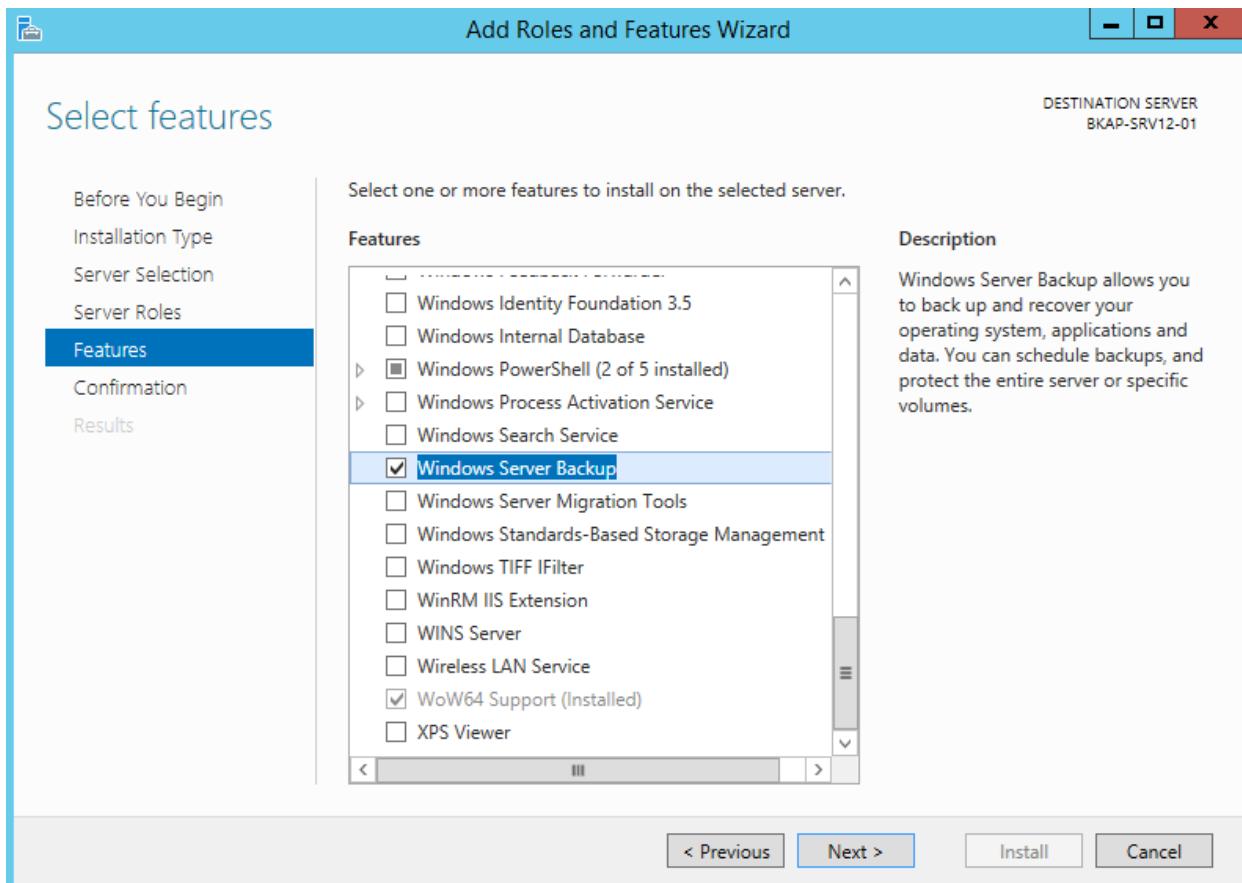
Thông số	BKAP-SRV12-01	BKAP-WRK08-01
<i>IP address</i>	192.168.1.2	192.168.1.10
<i>Subnet Mask</i>	255.255.255.0	255.255.255.0
<i>Gateway</i>	192.168.1.1	192.168.1.1
<i>DNS Server</i>	192.168.1.2	192.168.1.2

Hướng dẫn chi tiết:

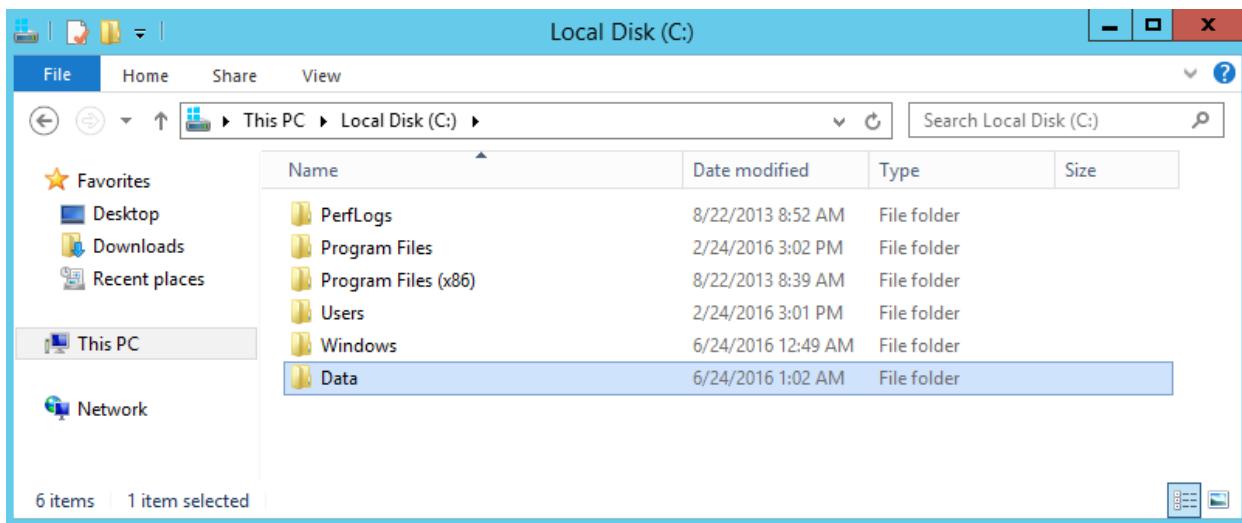
- Trên máy BKAP-SRV12-01, add thêm 2 ổ cứng.



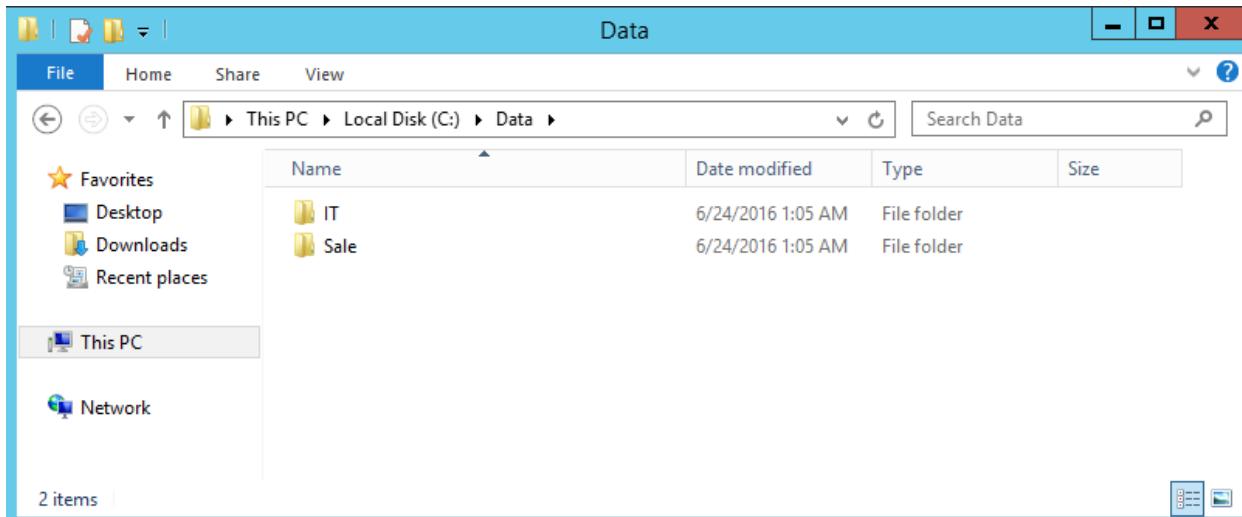
- Cài đặt Windows Server Backup.



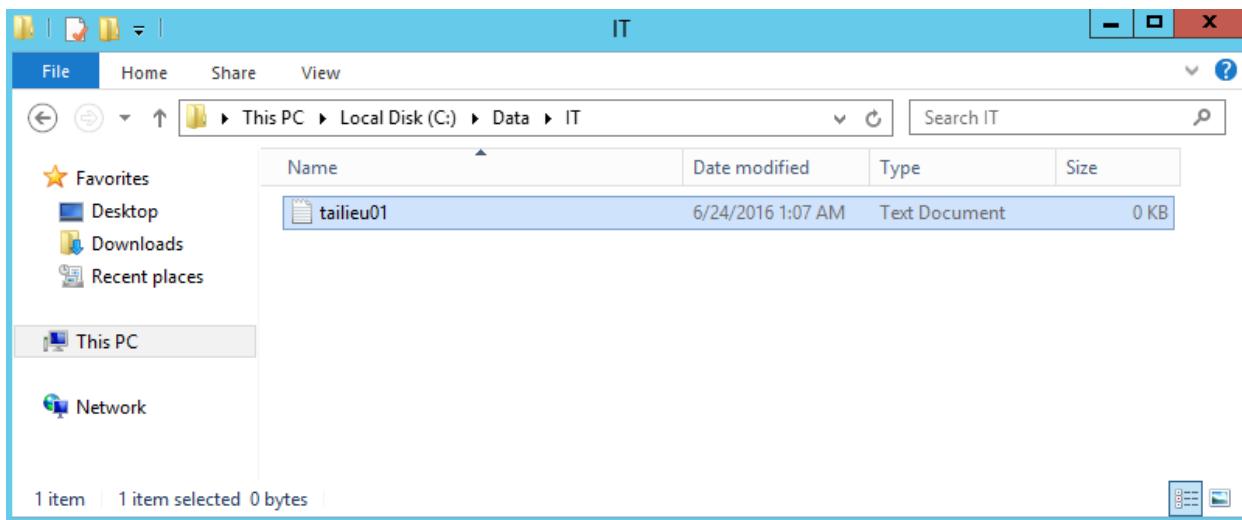
- Tạo thư mục Data trong ổ C.



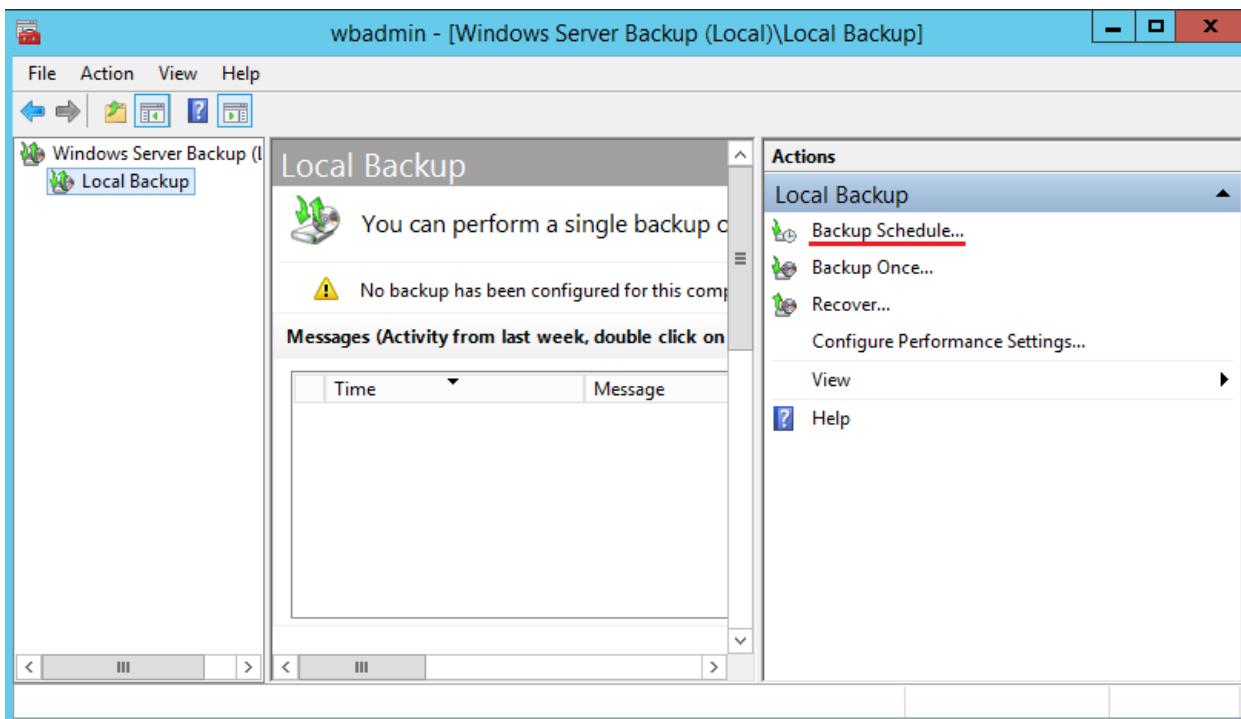
- Tạo thư mục **IT, Sale** trong thư mục **Data**.



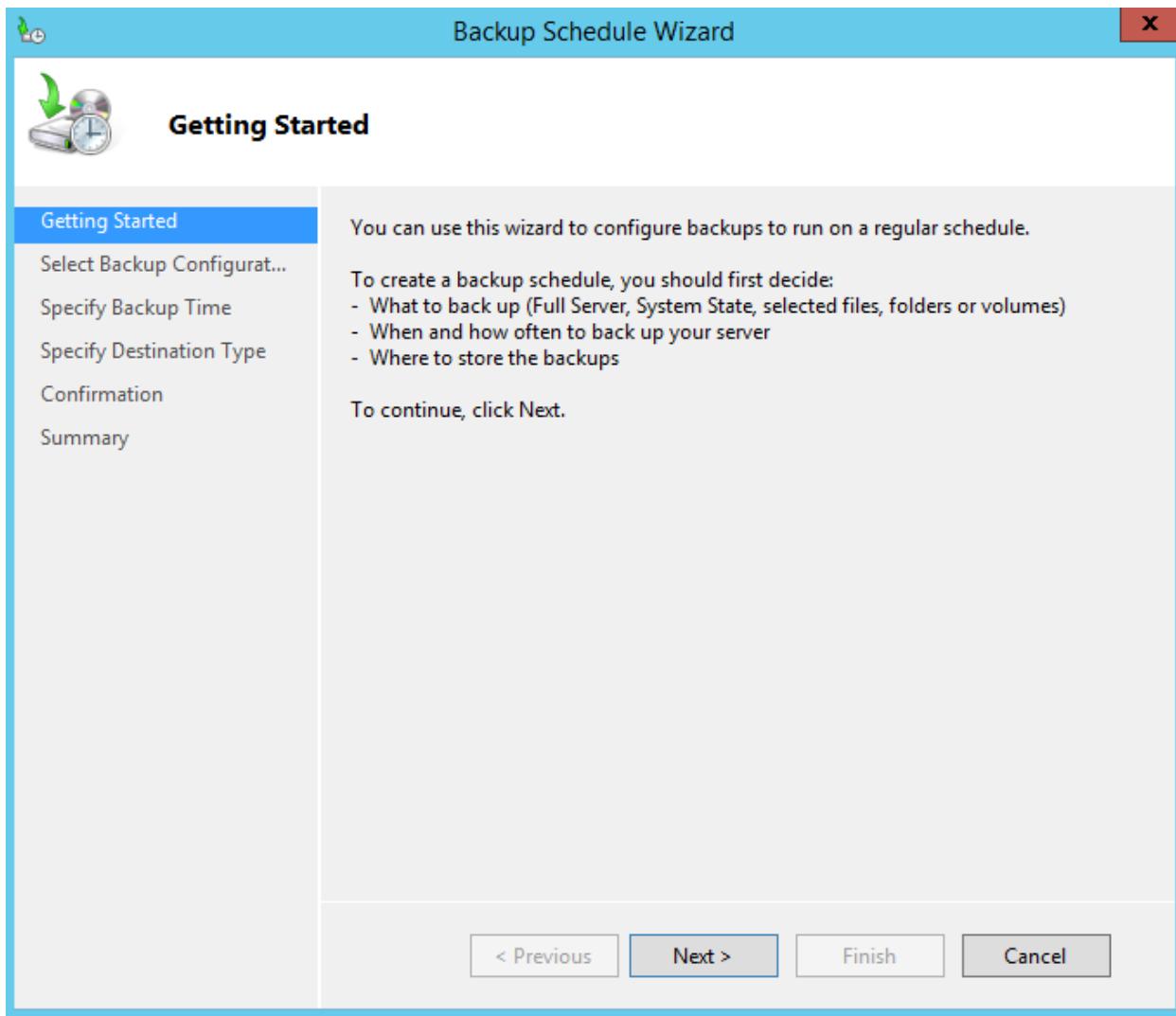
- Tạo 1 tài liệu tên **tailieu01** trong folder **IT**.



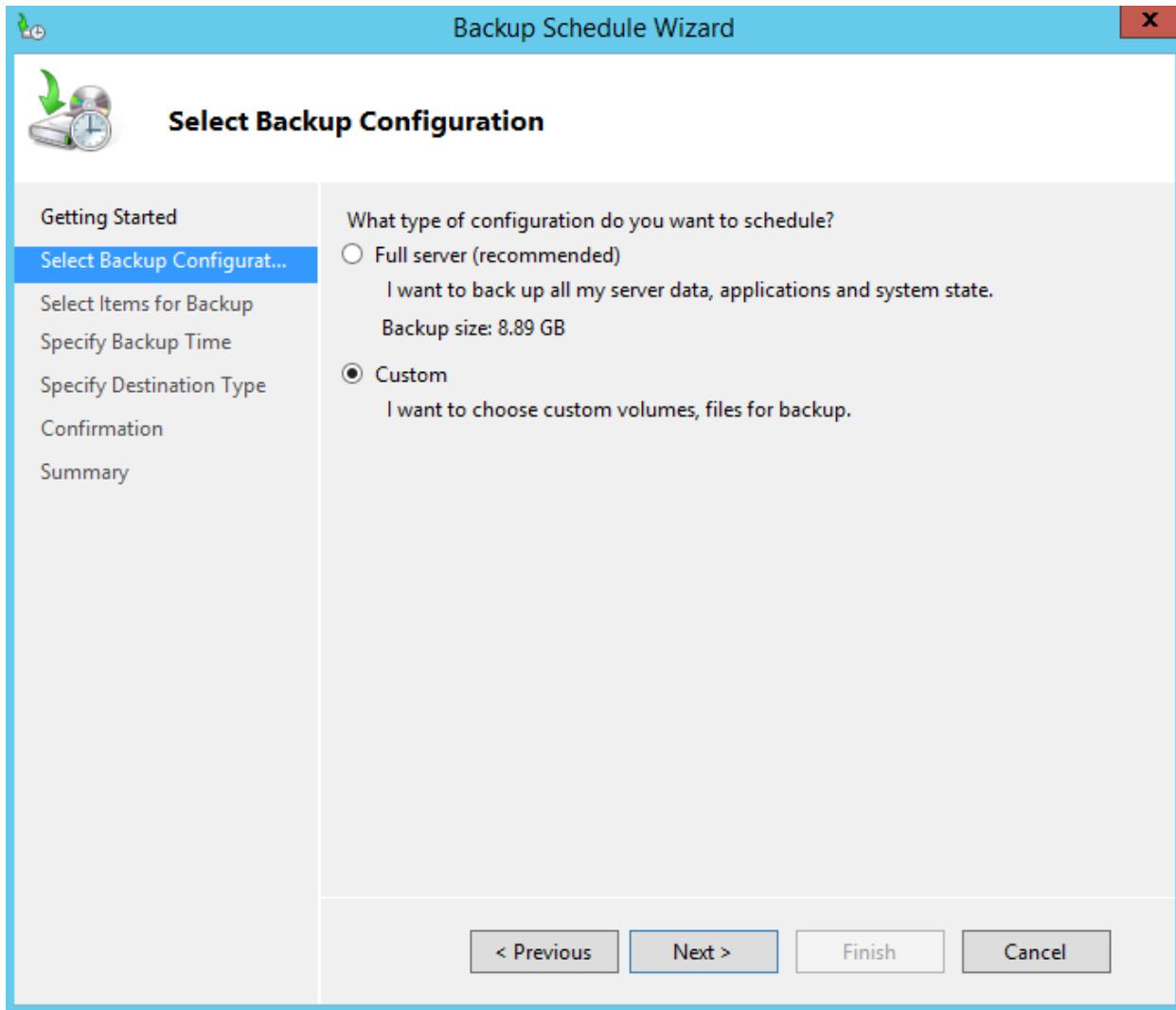
- Cấu hình Windows Server Backup, thực hiện **đặt lịch** và tạo **Backup** bằng tay để kiểm tra.
 - Trong cửa sổ **wbadmin – [Windows Server Backup (Local)\Local Backup]** , click vào **Backup Schedule...**



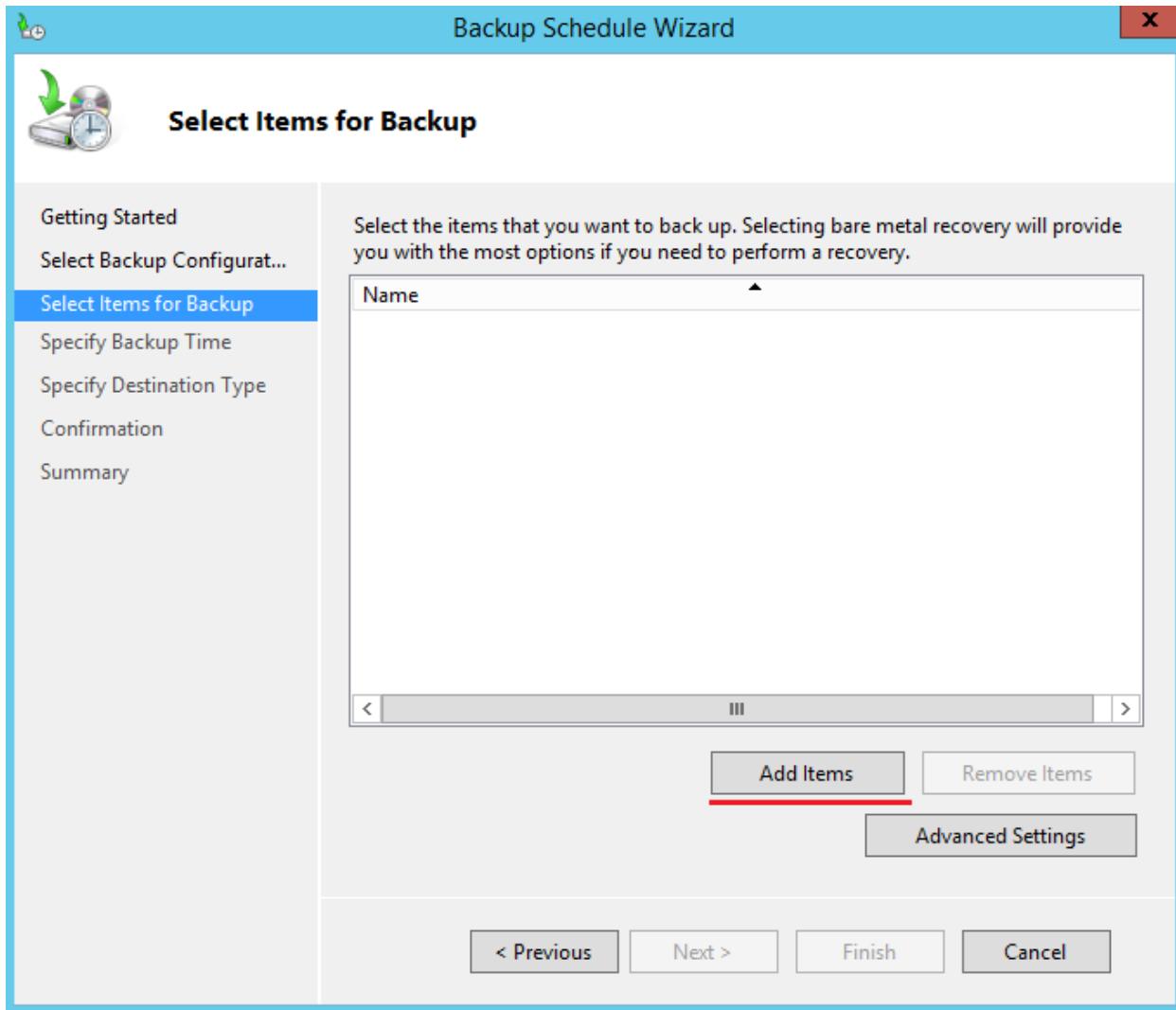
- Tại cửa sổ **Getting Started**, click vào **Next**.



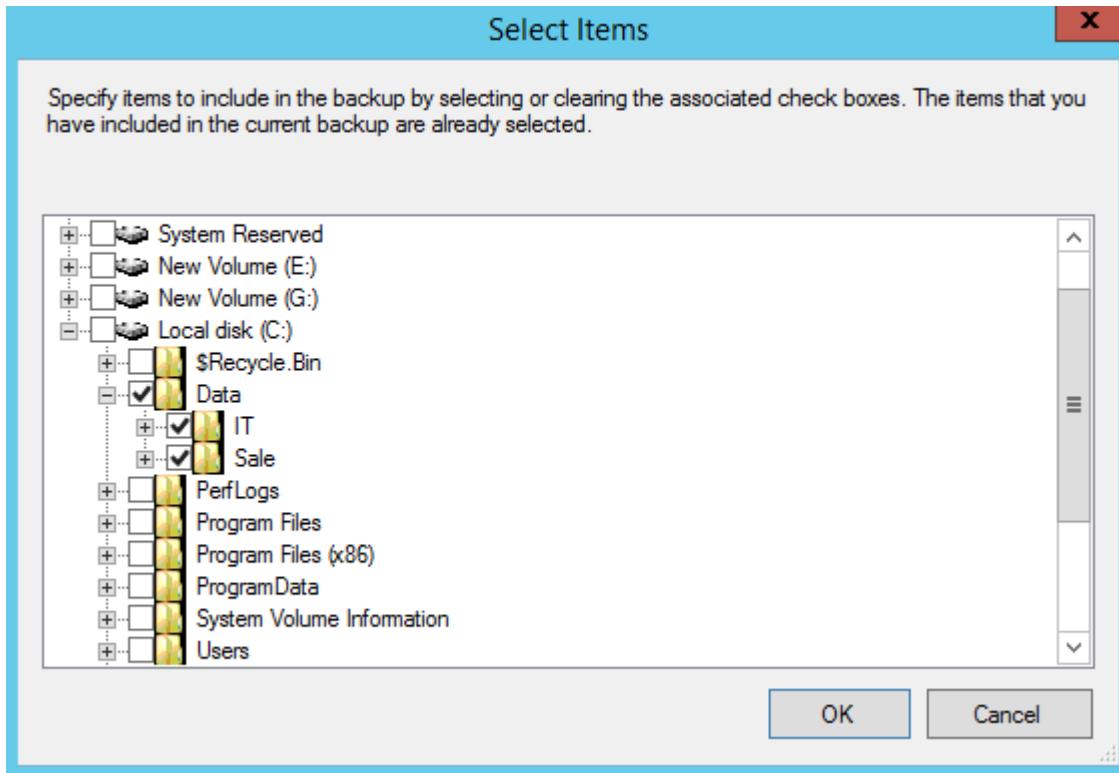
- Tại cửa sổ **Select Backup Configuration**, click chọn vào **Custom**, click vào **Next**.



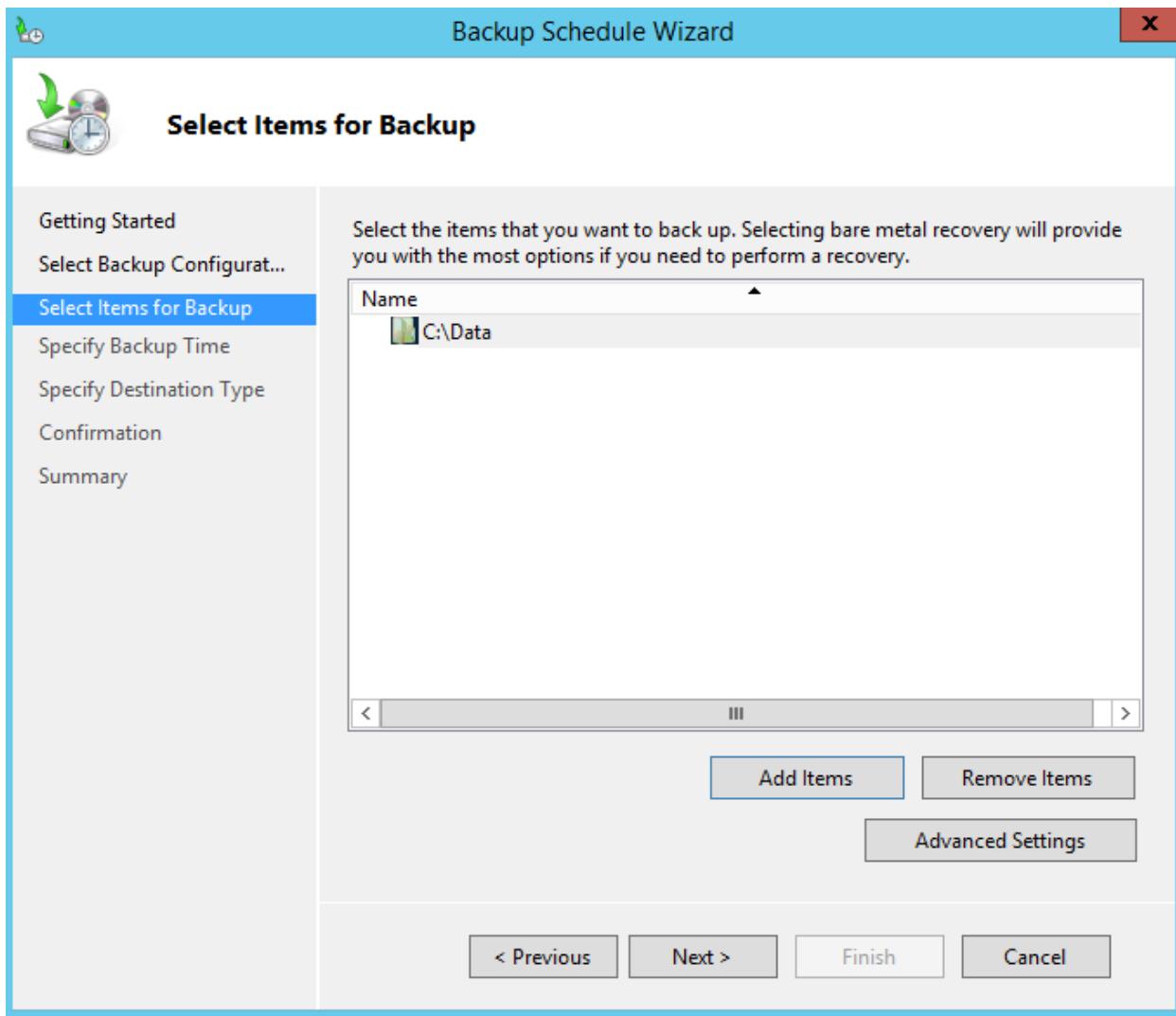
- Tại cửa sổ **Select Items for Backup**, click chọn vào **Add Items**.



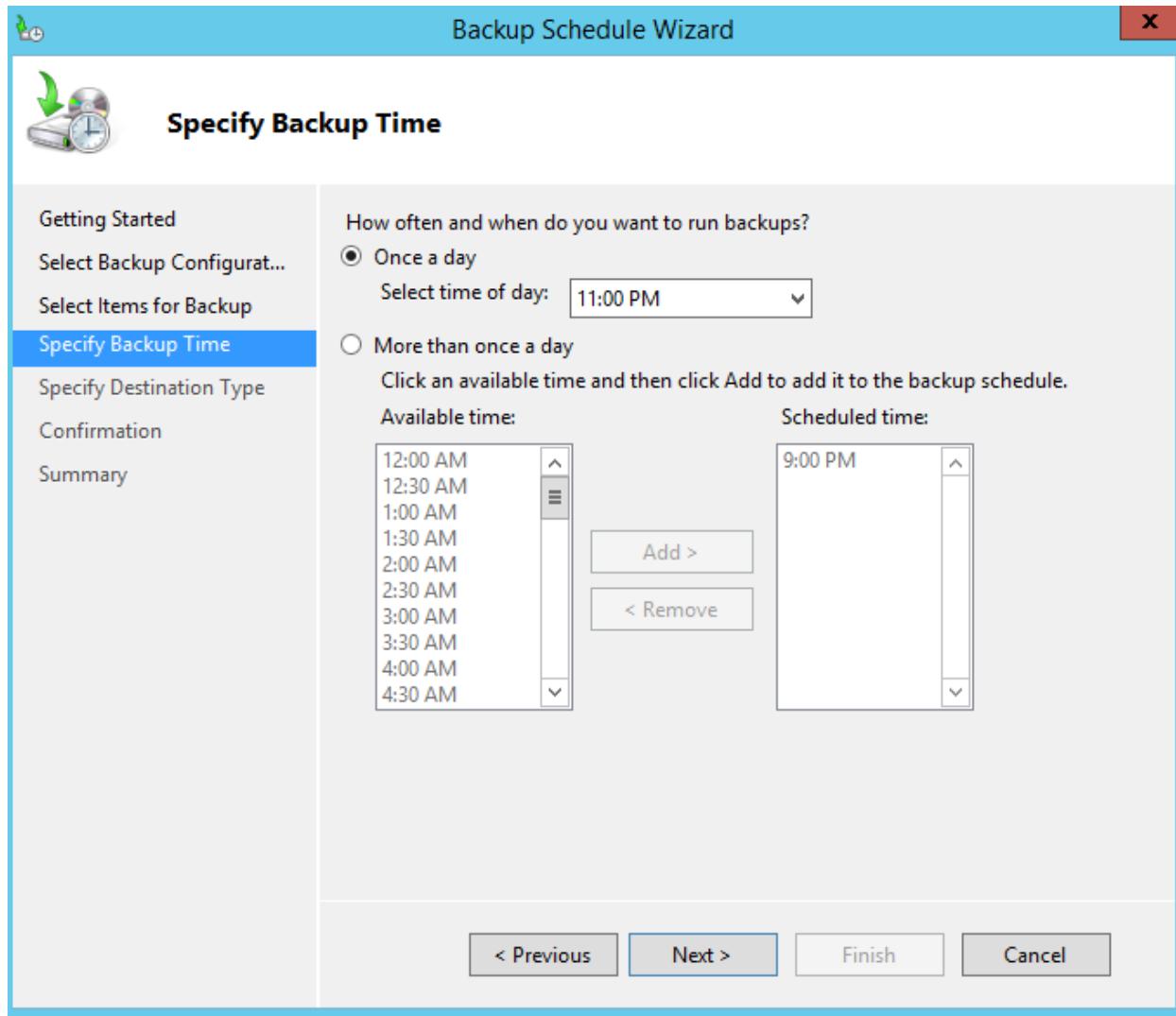
- Trong cửa sổ **Select Items**, click chọn vào ô **C** , thư mục **Data**, click vào **OK**.



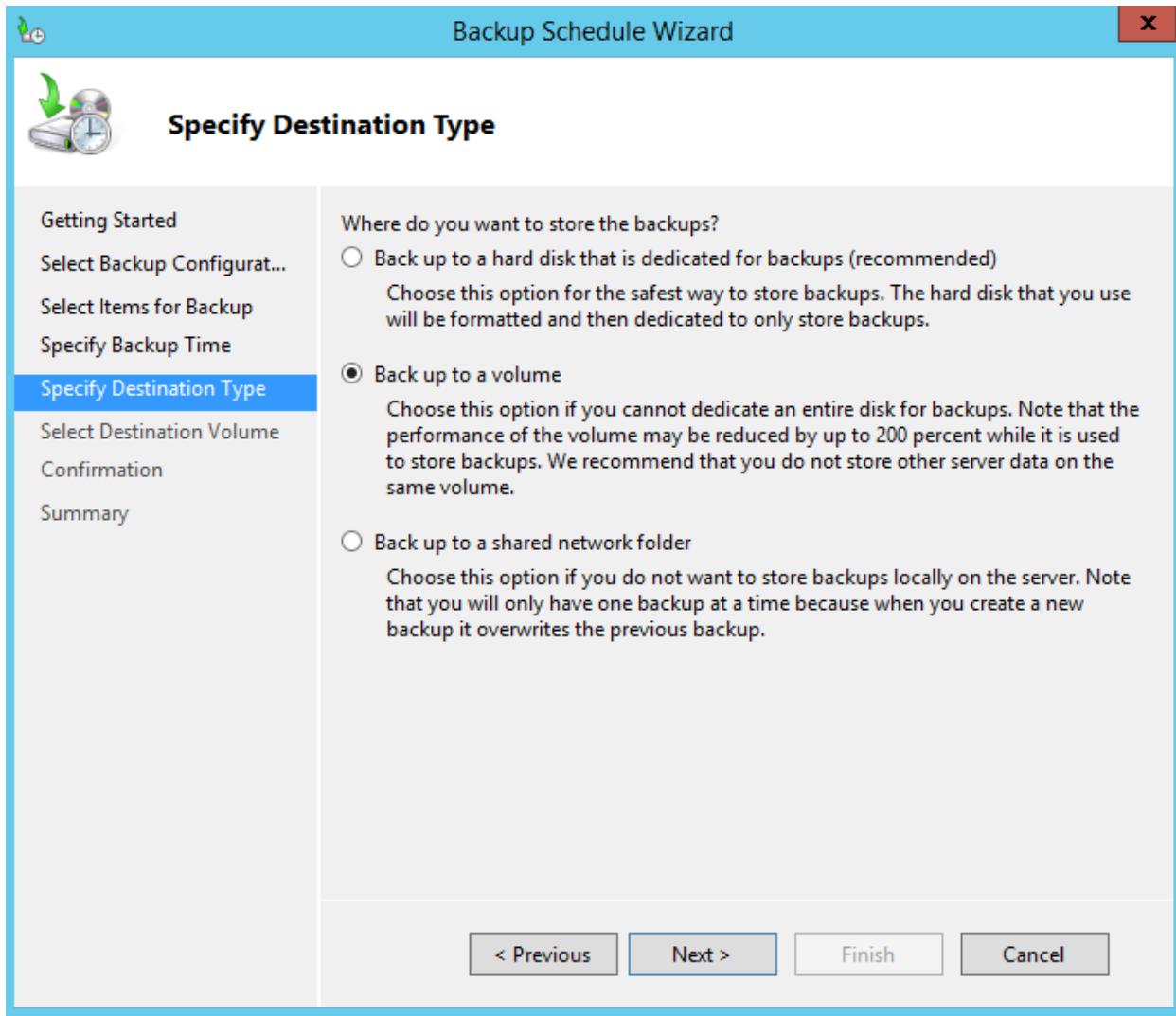
- Tại cửa sổ **Select Items for Backup**, click vào **Next**.



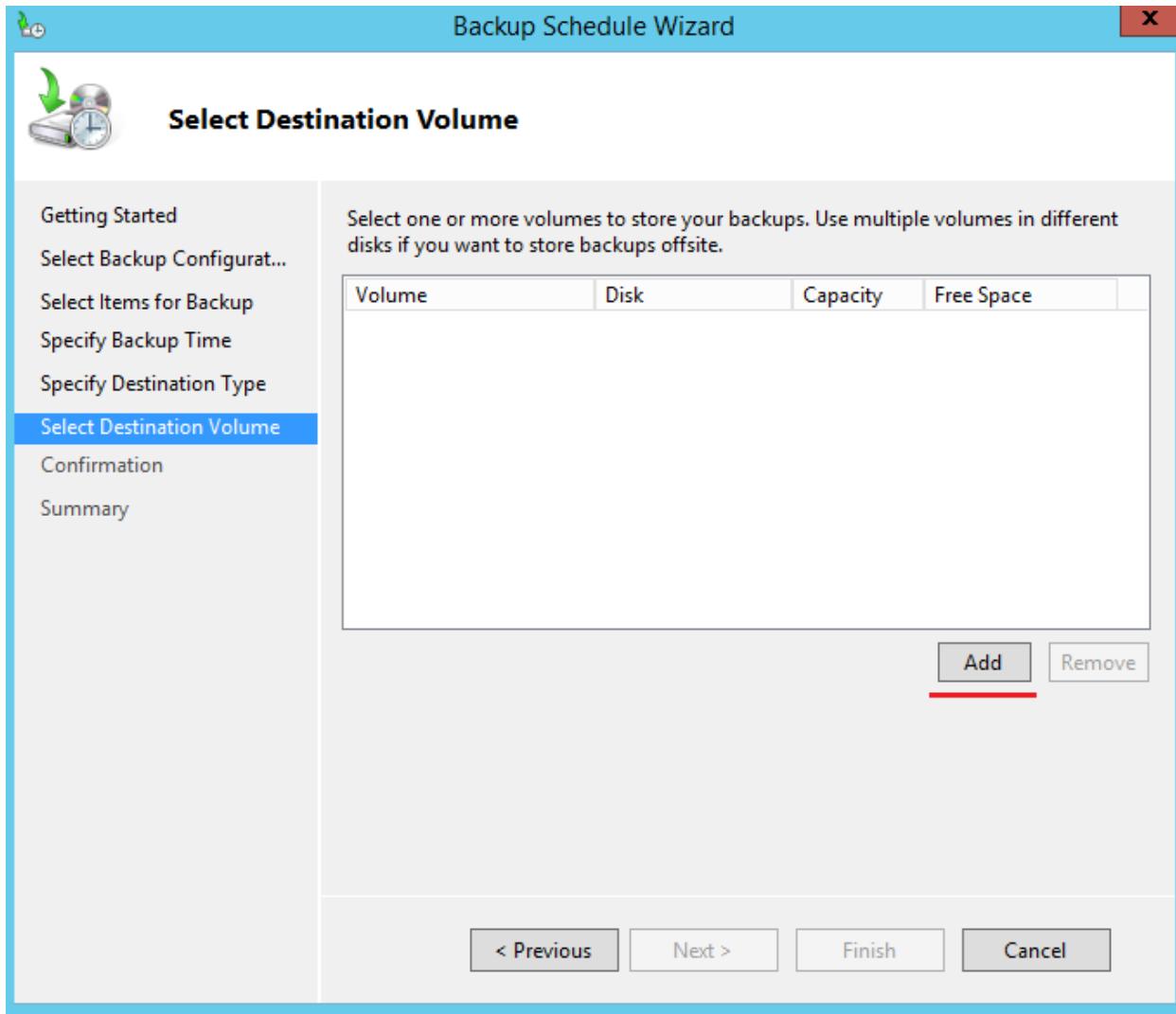
- Tại cửa sổ **Specify Backup Time**, đặt thời gian, click vào **Next**.



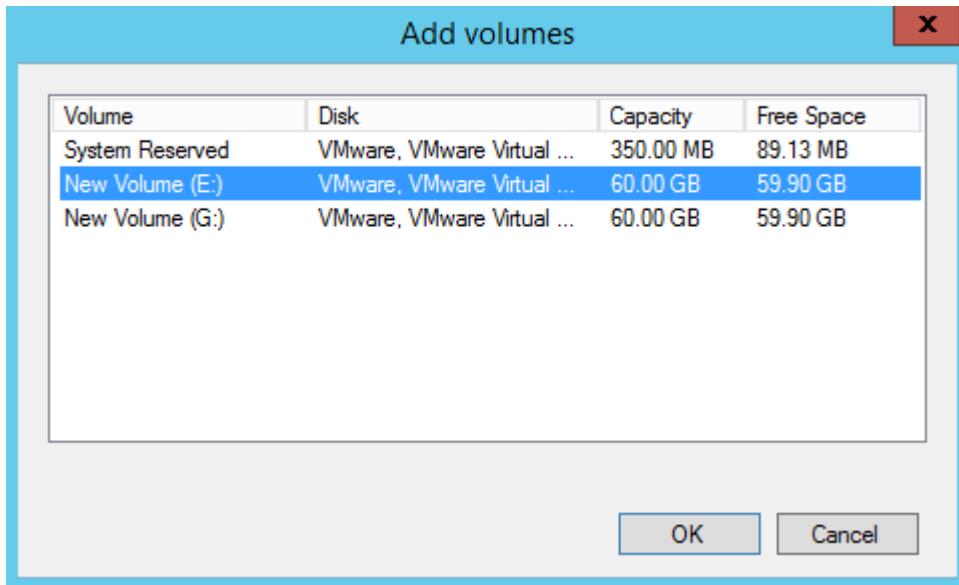
- Tại cửa sổ **Specify Destination Type**, click chọn vào **Back up to a volume**, click vào **Next**.



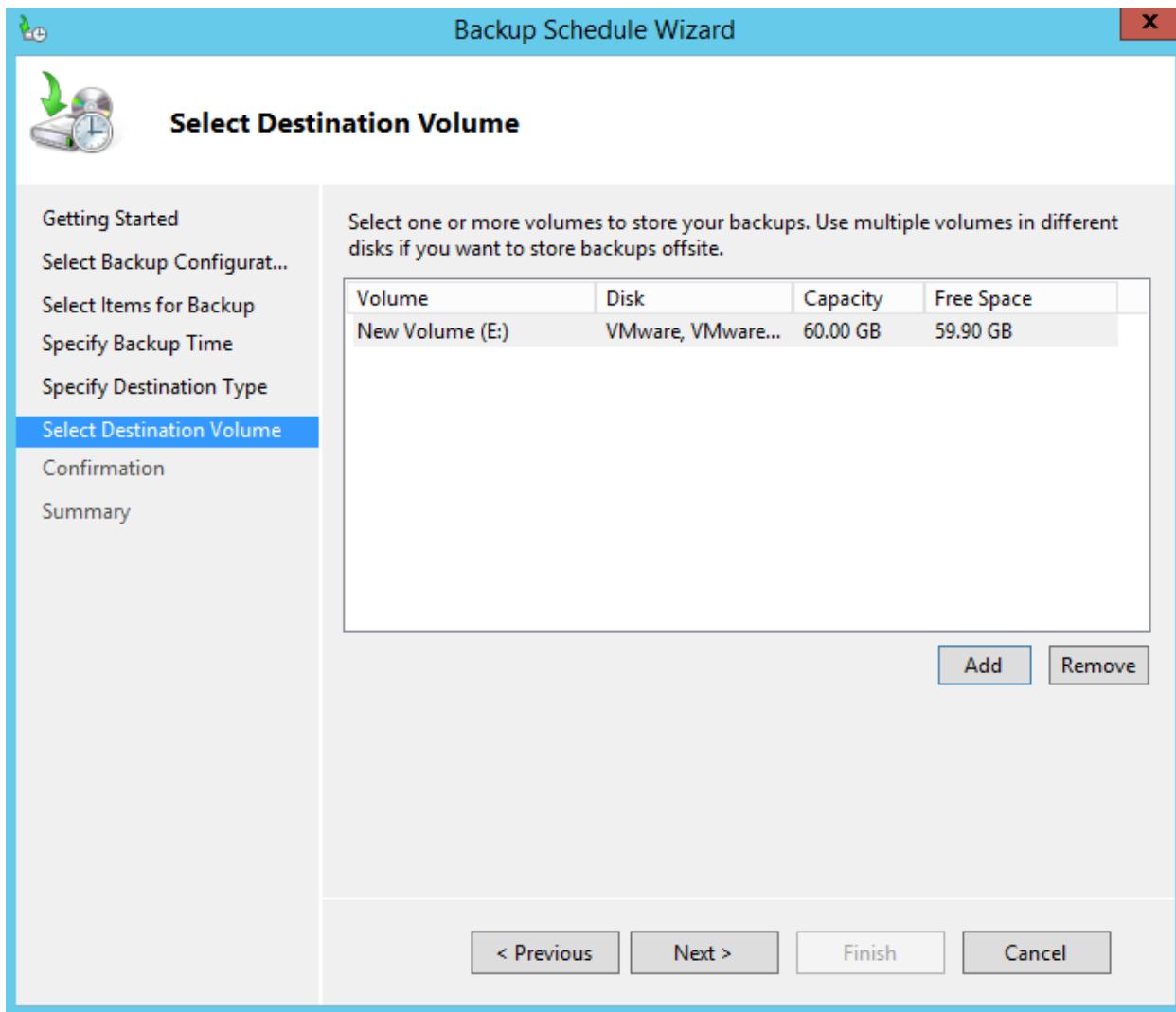
- Tại cửa sổ **Select Destination Volume**, click vào **Add**.



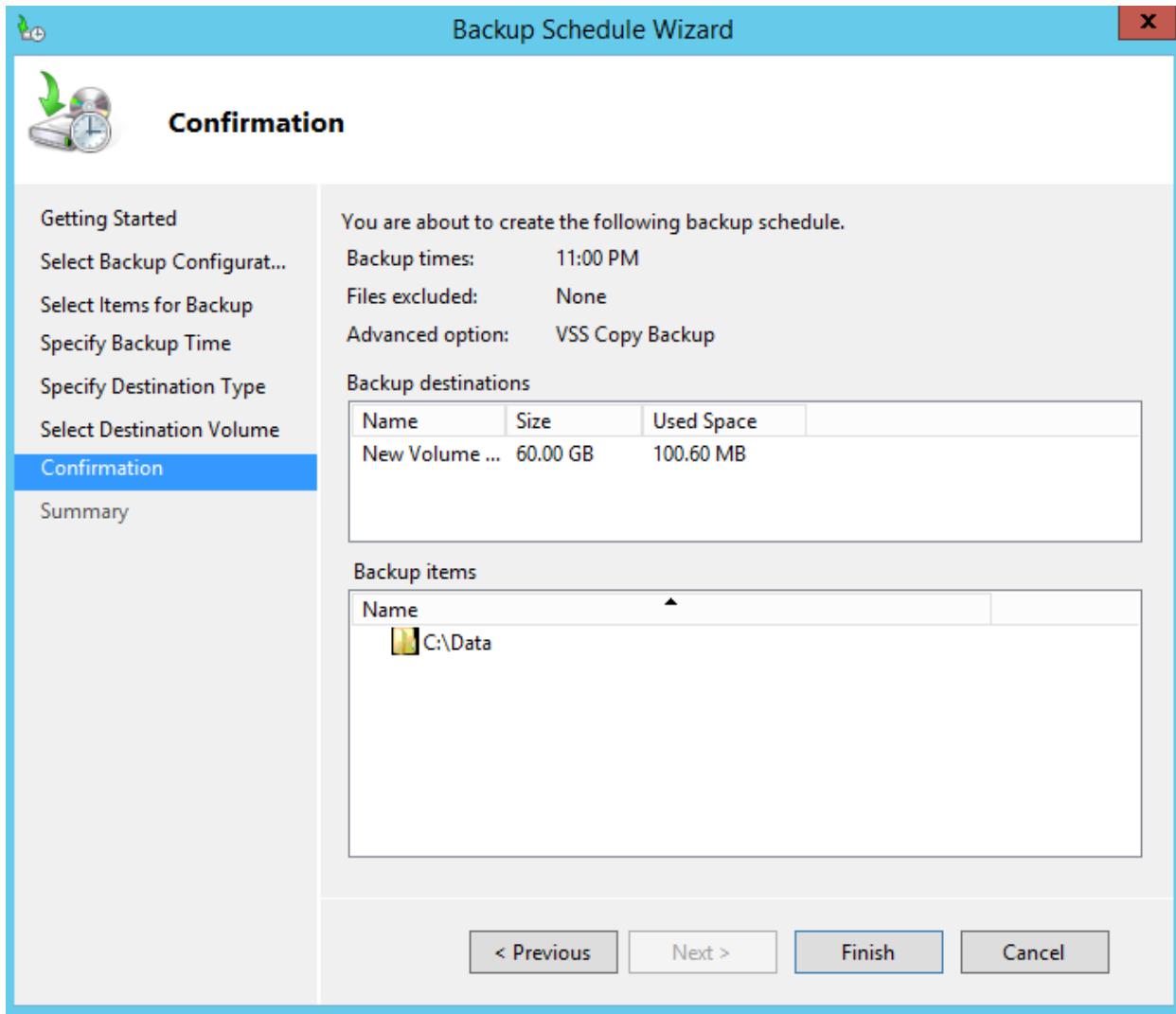
- Tại cửa sổ **Add volumes**, click chọn vào ô E.



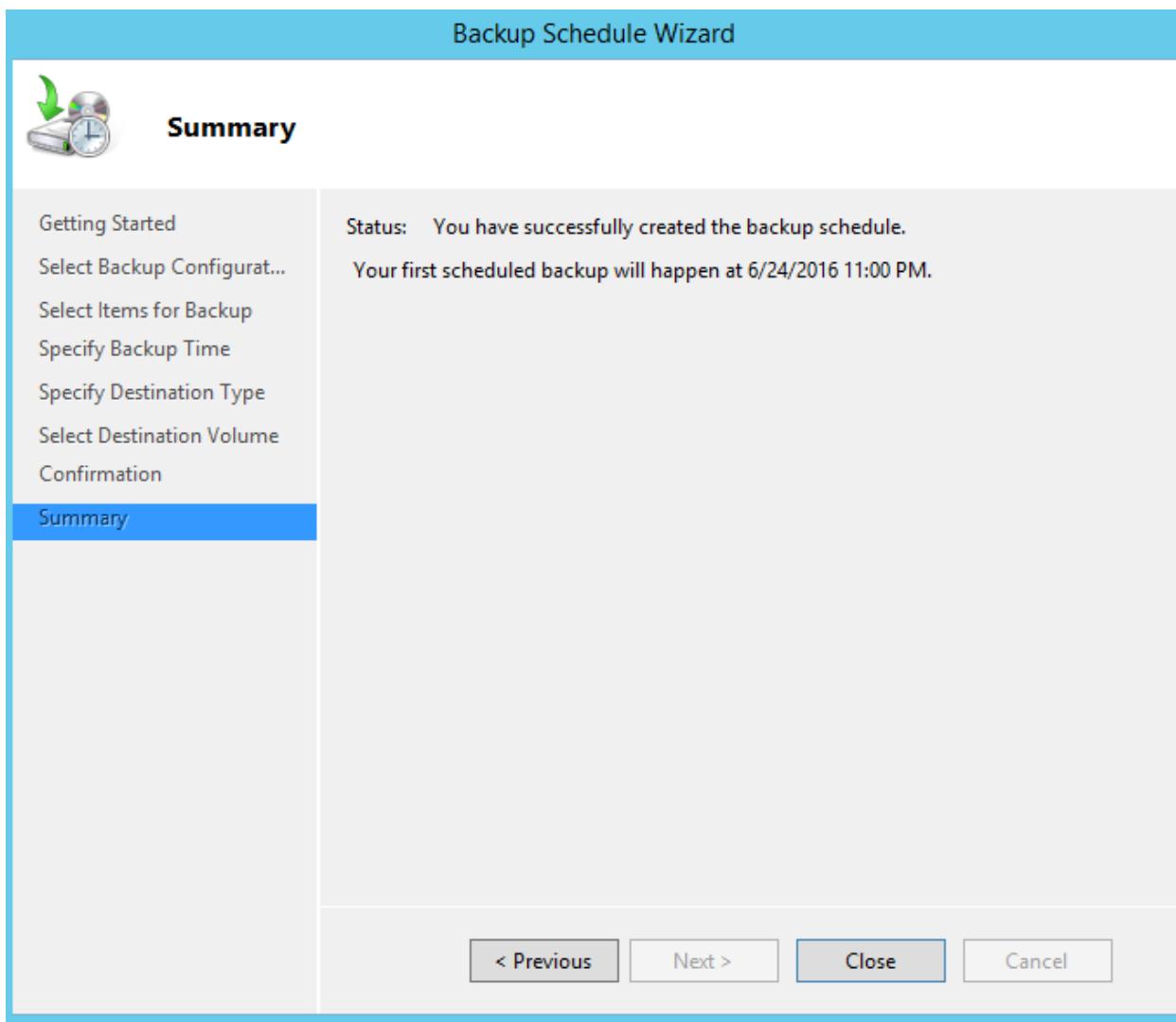
- Tại cửa sổ **Select Destination Volume**, click vào **Next**.



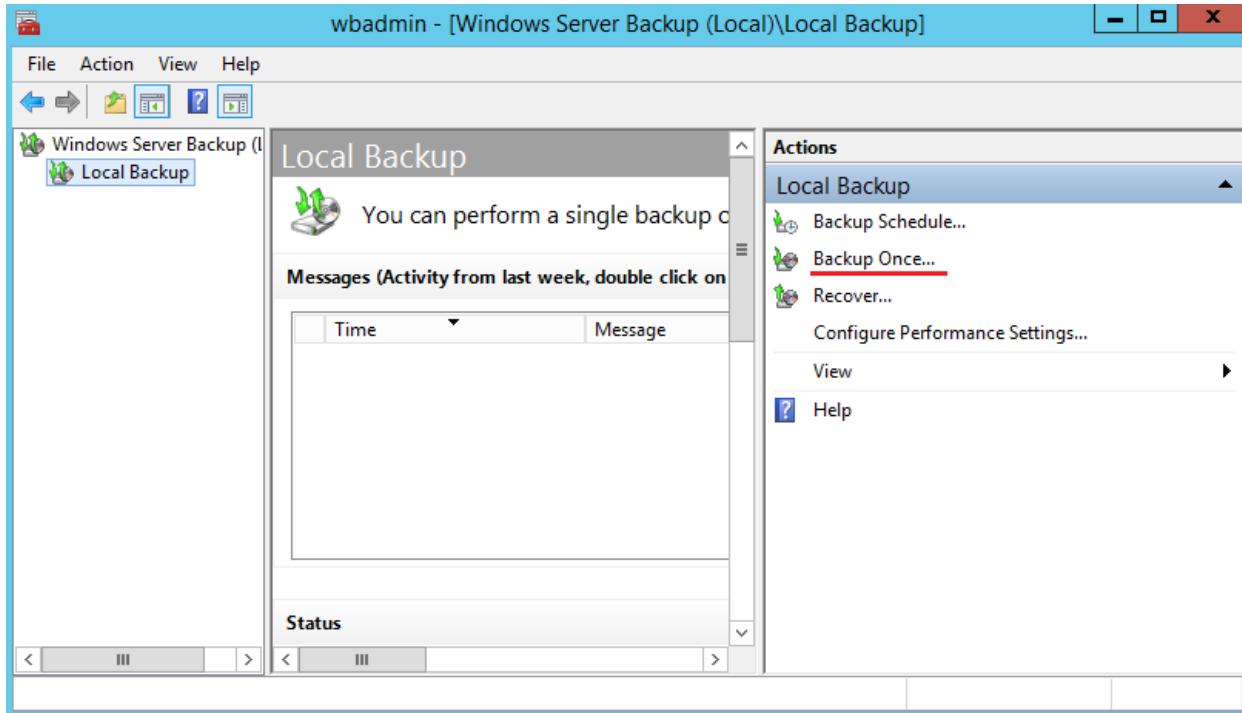
- Tại cửa sổ **Confirmation**, click vào **Finish**.



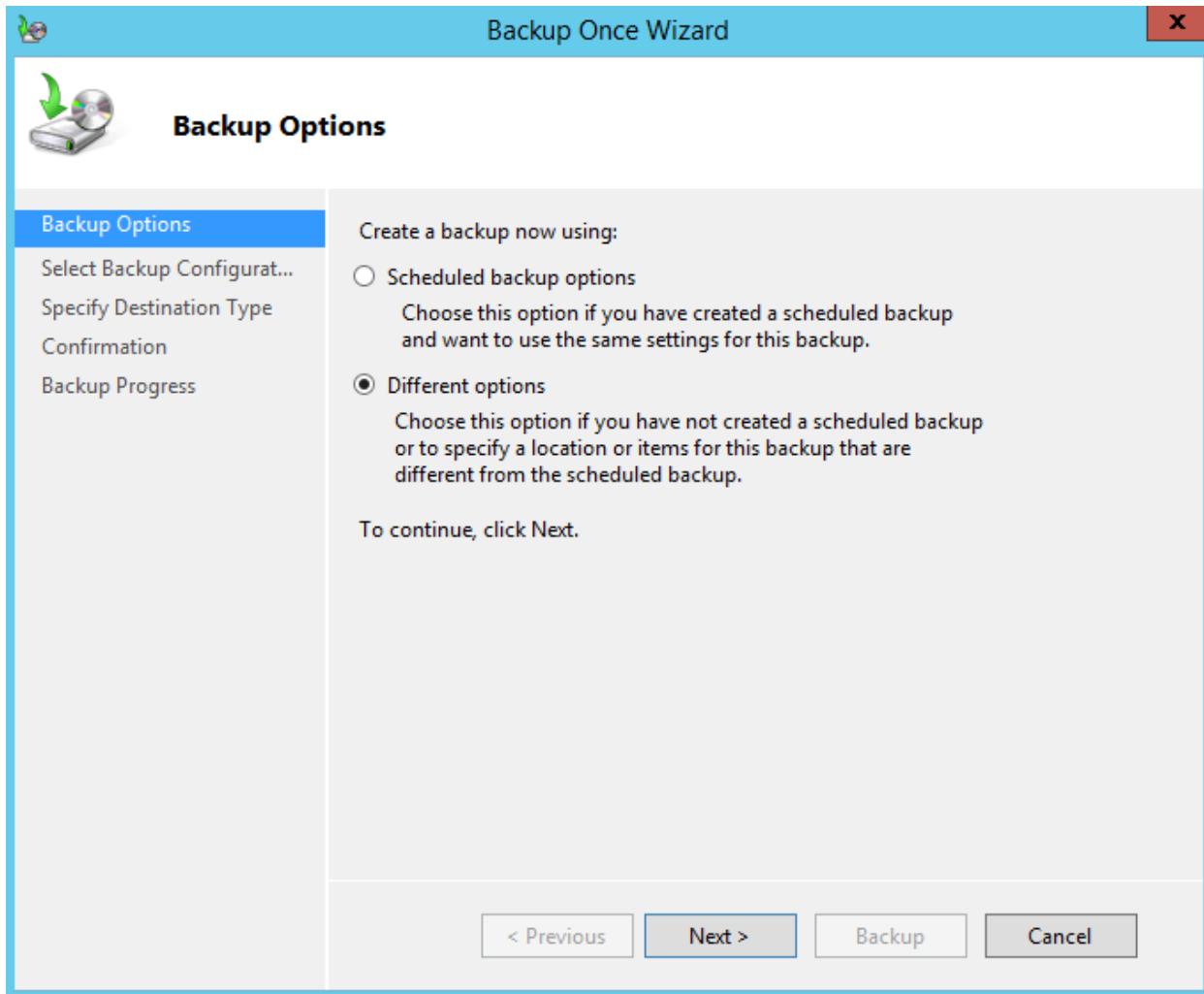
- Tại cửa sổ **Summary**, click vào **Close**.



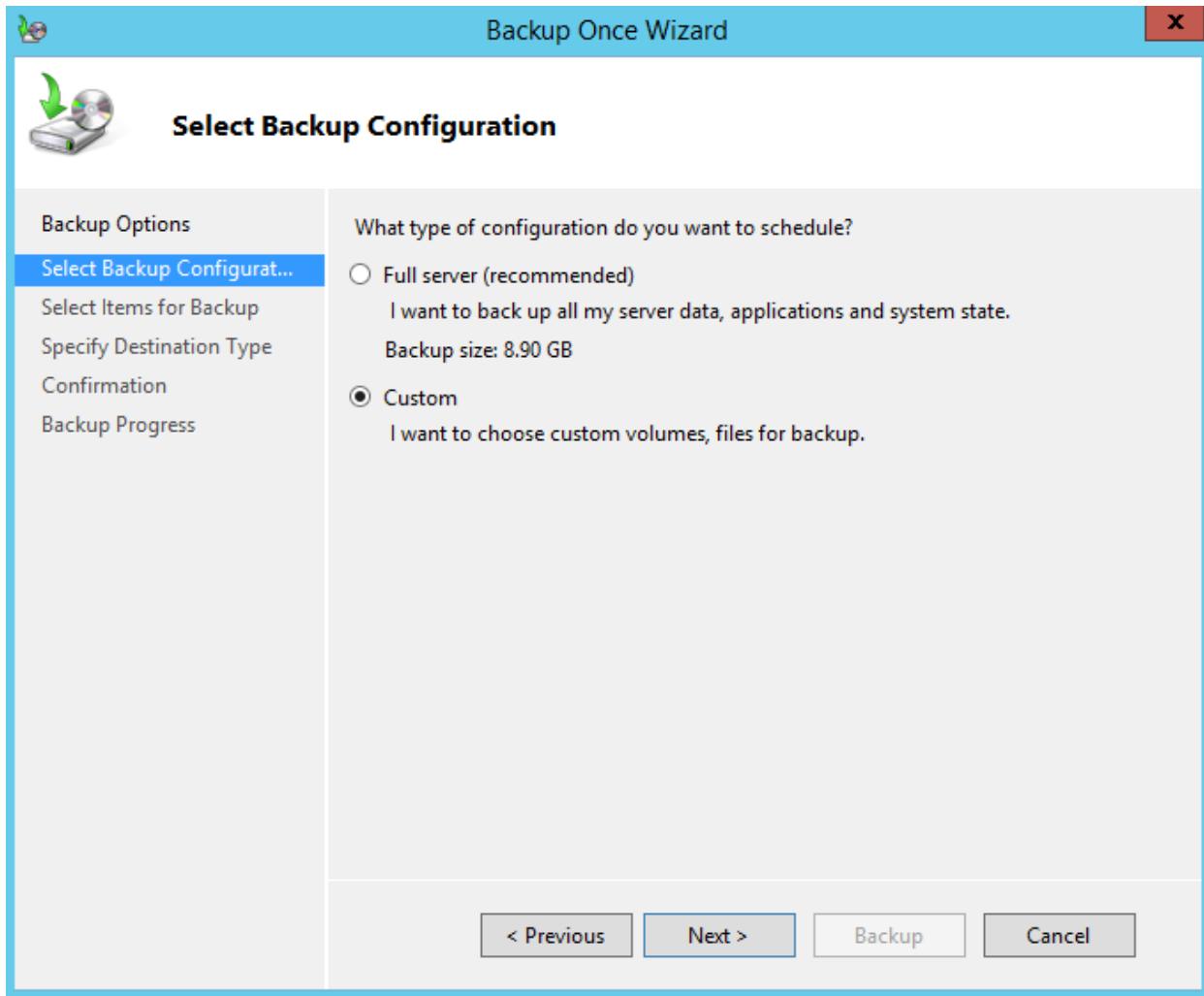
- Tại cửa sổ wbadmin – [Windows Server Backup (Local)\Local Backup] , click chọn vào **Backup Once...**



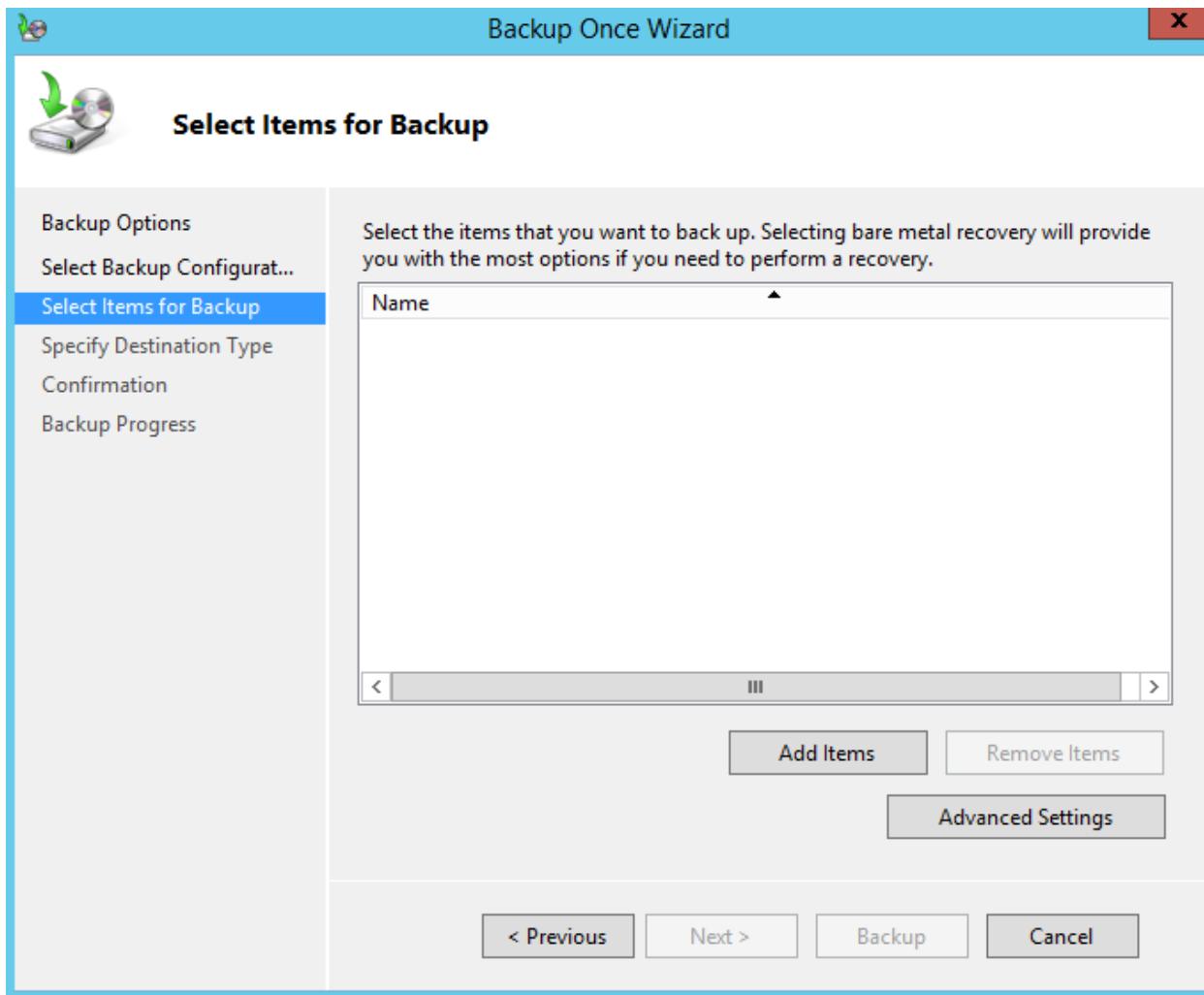
- Tại cửa sổ **Backup Options**, click vào **Different options**, click vào **Next**.



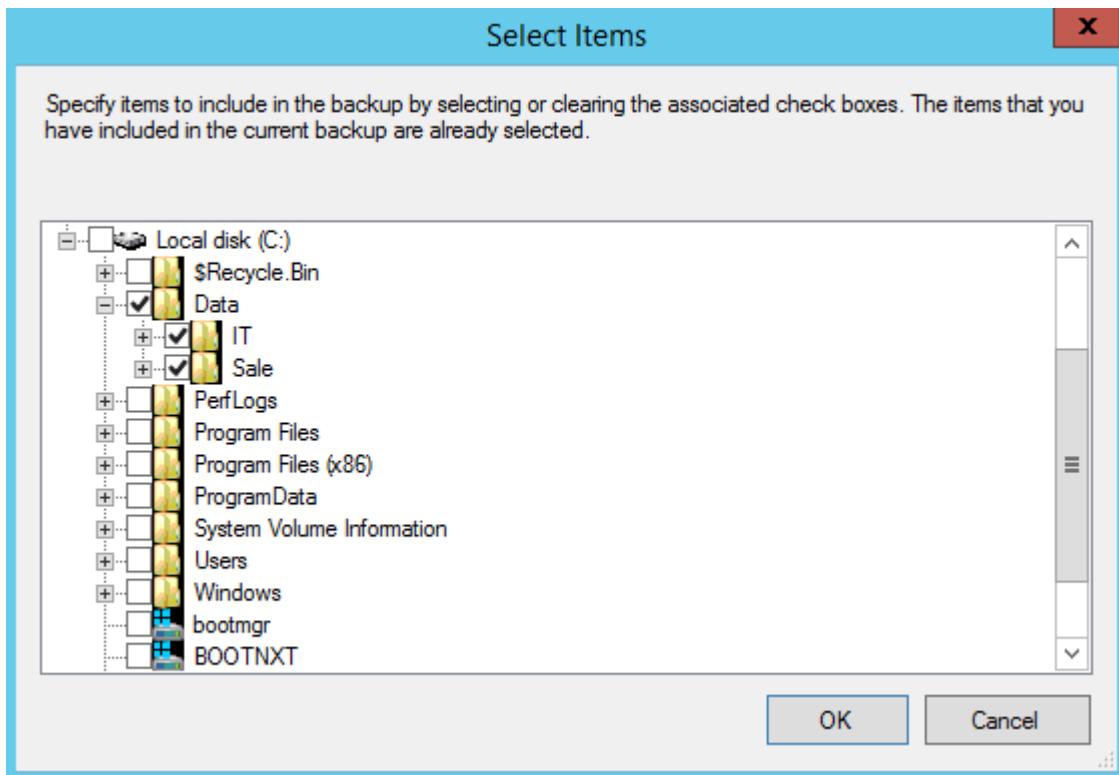
- Tại cửa sổ **Select Backup Configuration**, click chọn vào **Custom**, click vào **Next**.



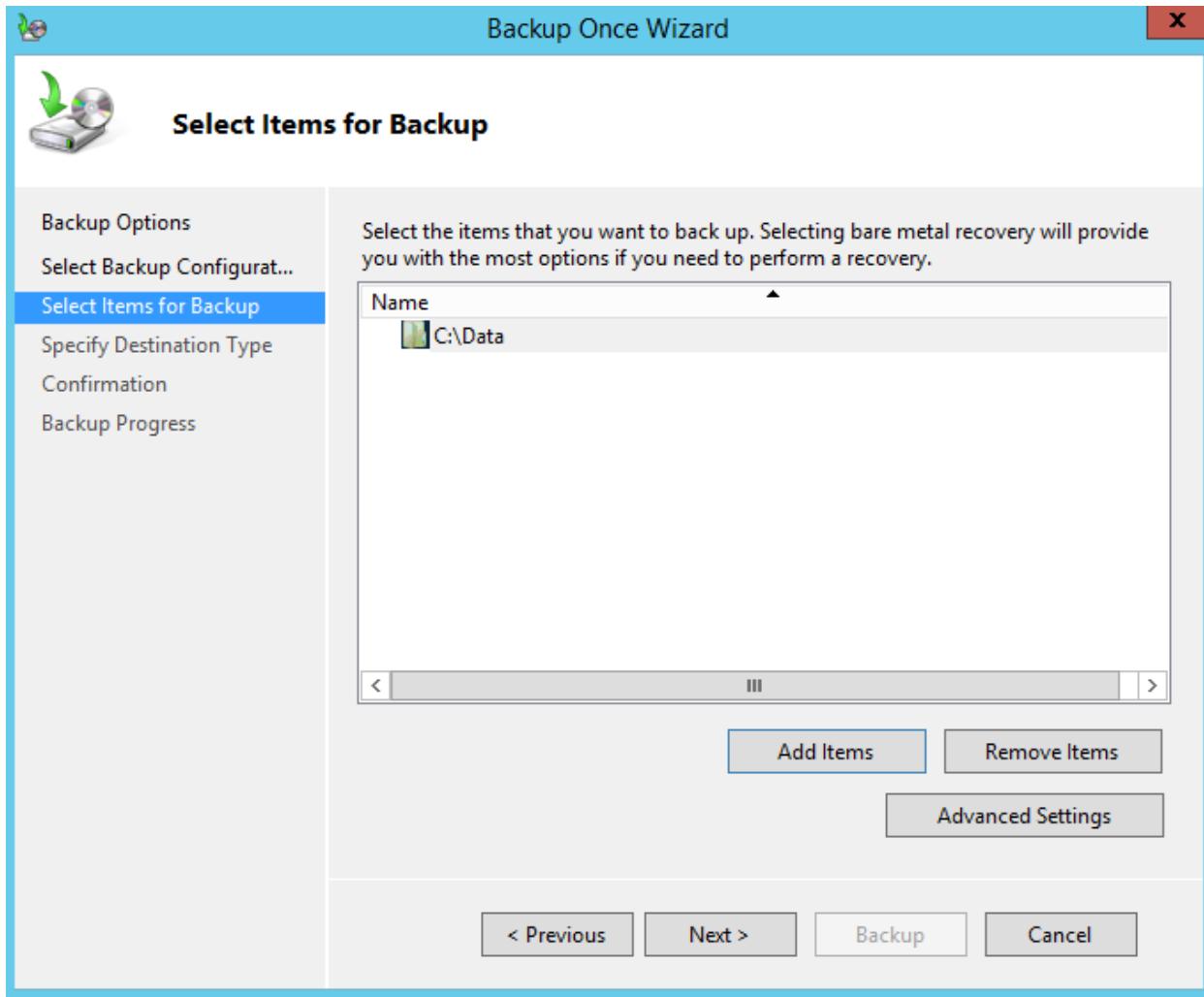
- Tại cửa sổ **Select Items for Backup**, click vào **Add Items**.



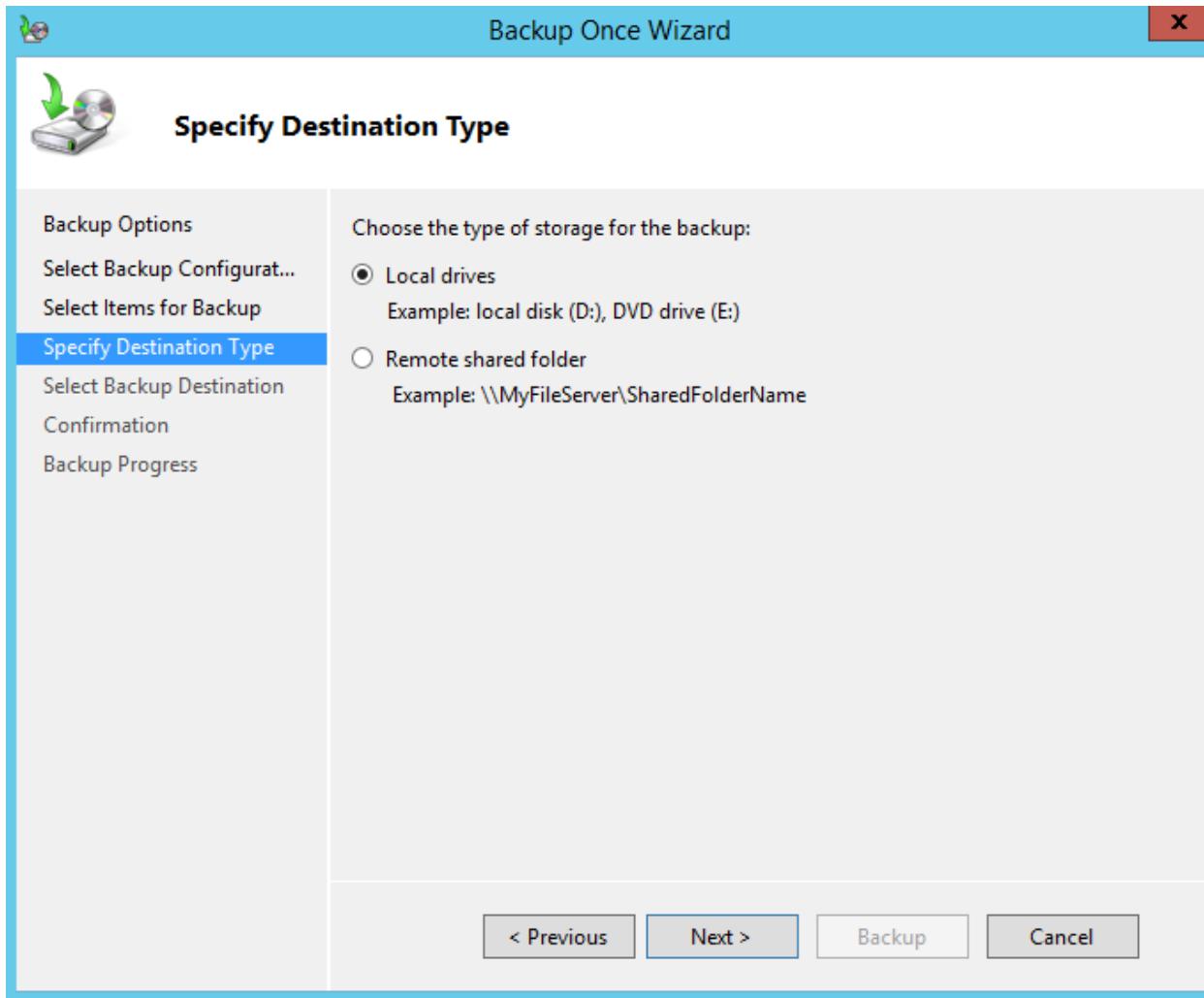
- Tại cửa sổ **Select Items**, chọn vào thư mục **Data**.



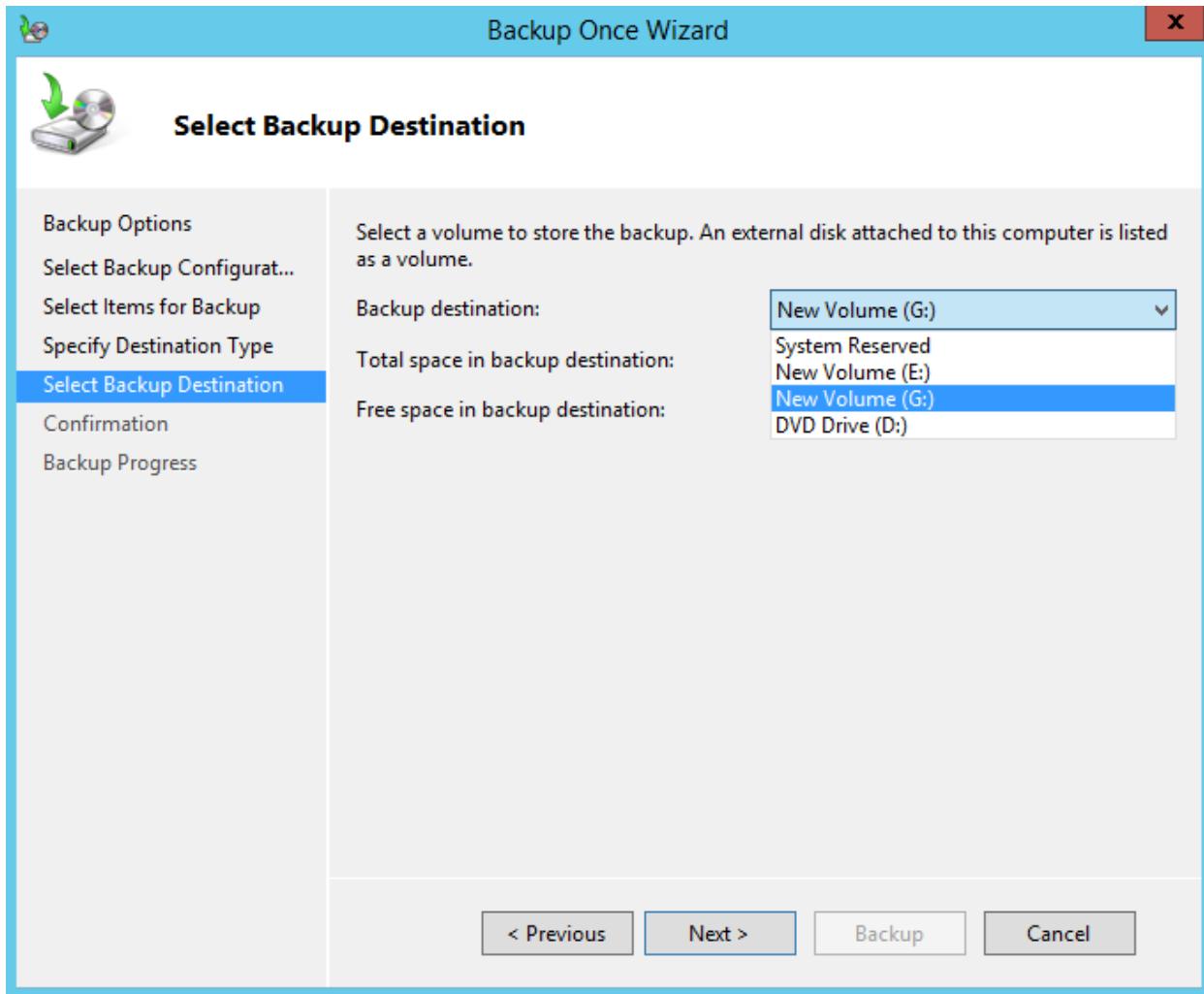
- Tại cửa sổ **Select Items for Backup**, click vào **Next**.



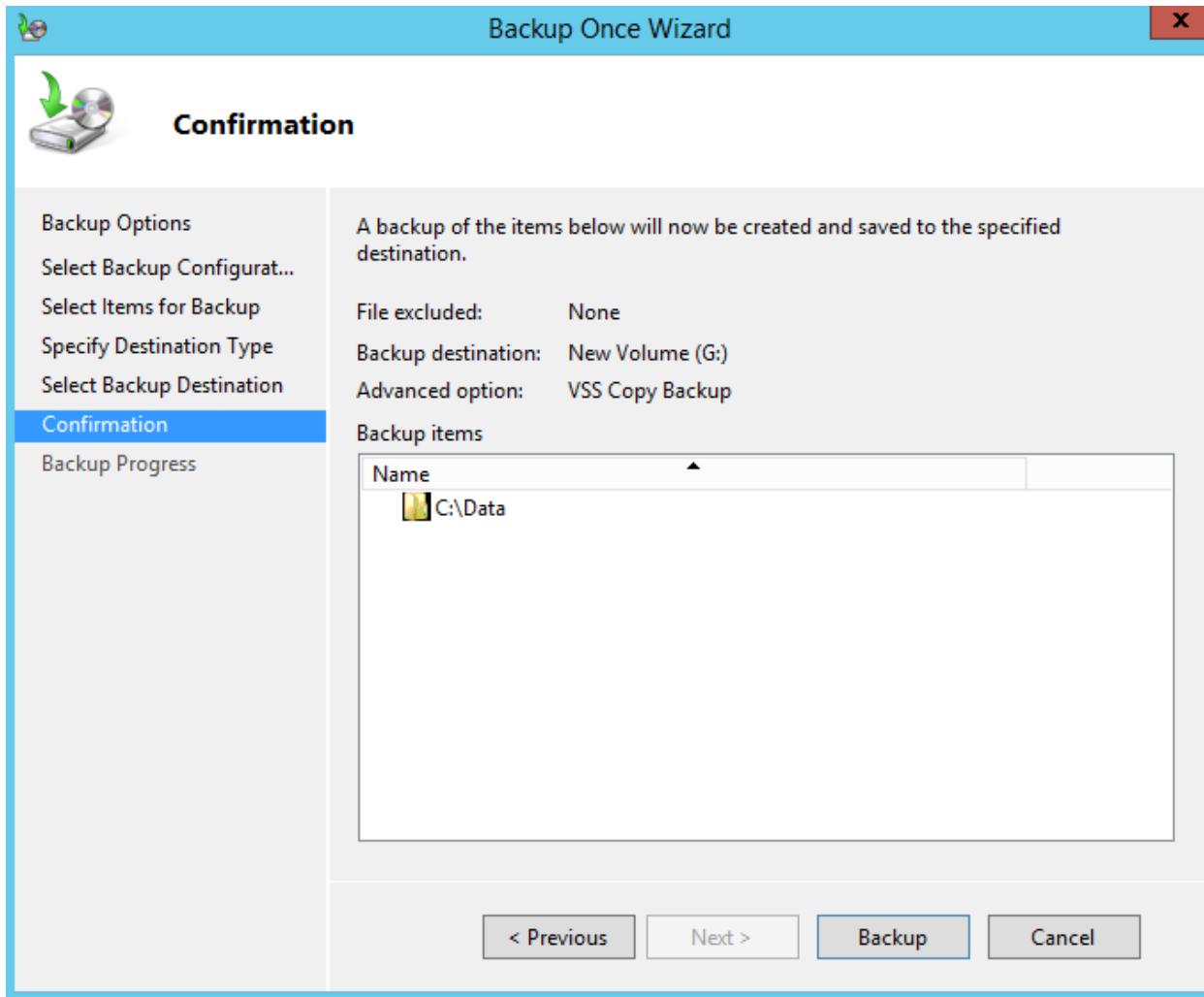
- Tại cửa sổ **Specify Destination Type**, click chọn **Local drives**, click vào **Next**.



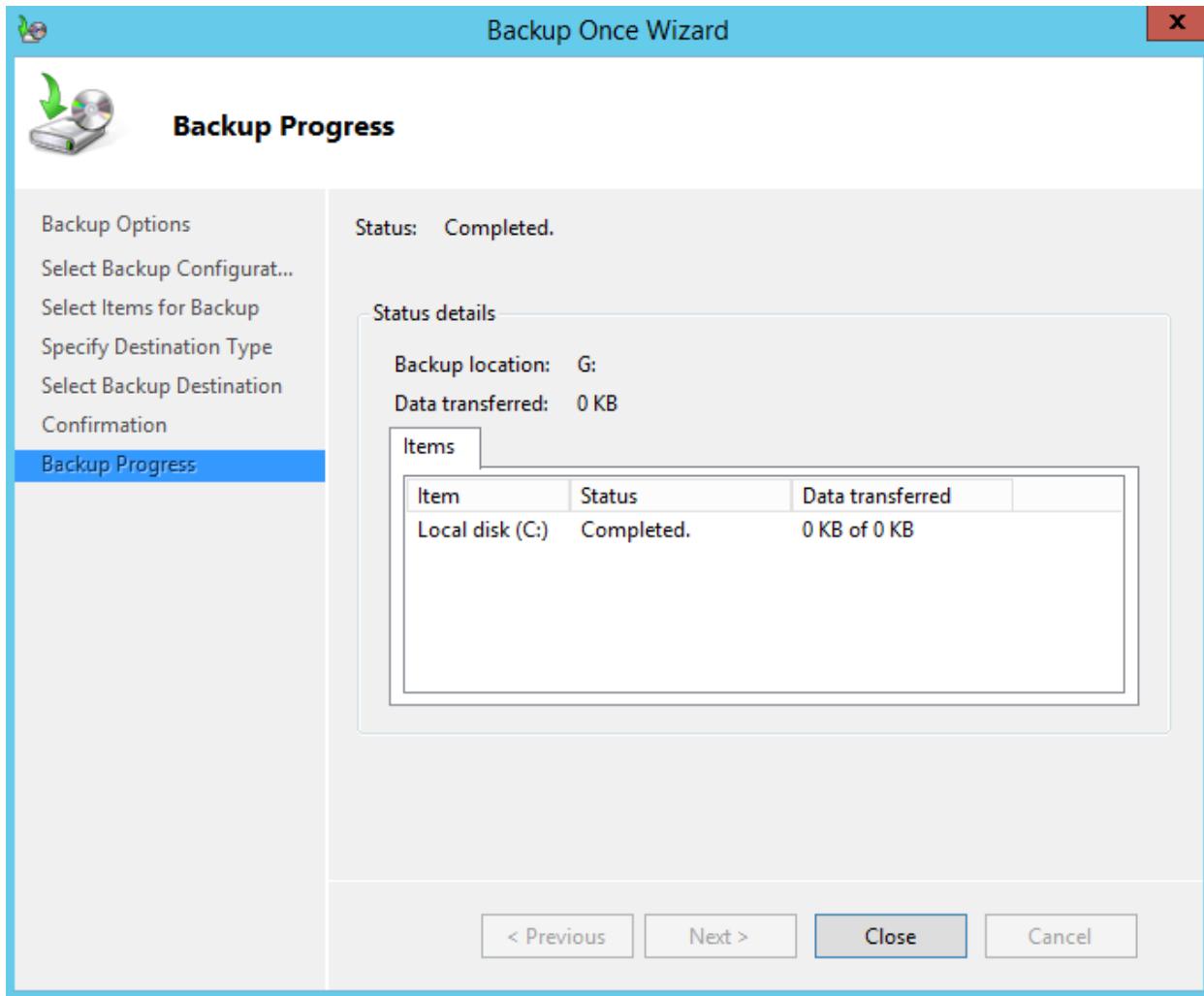
- Tại cửa sổ **Select Backup Destination**, tại mục **Backup destination**, chọn vào ô **G**, click vào **Next**.



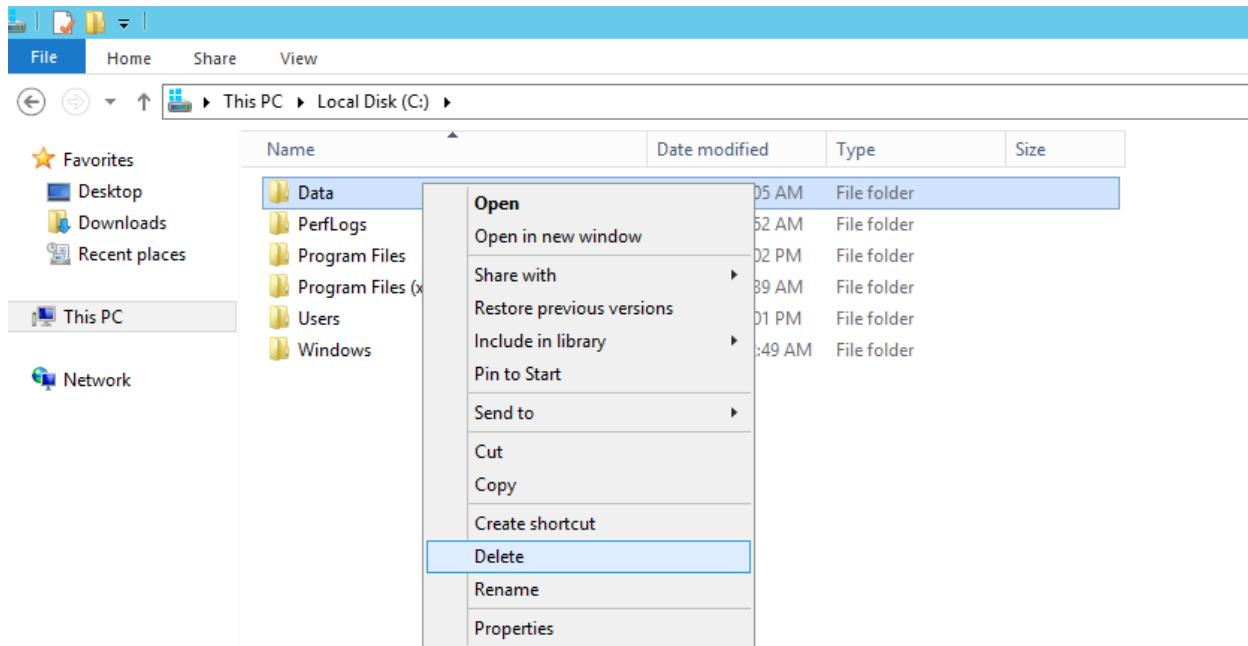
- Tại cửa sổ **Confirmation**, click vào **Backup**.



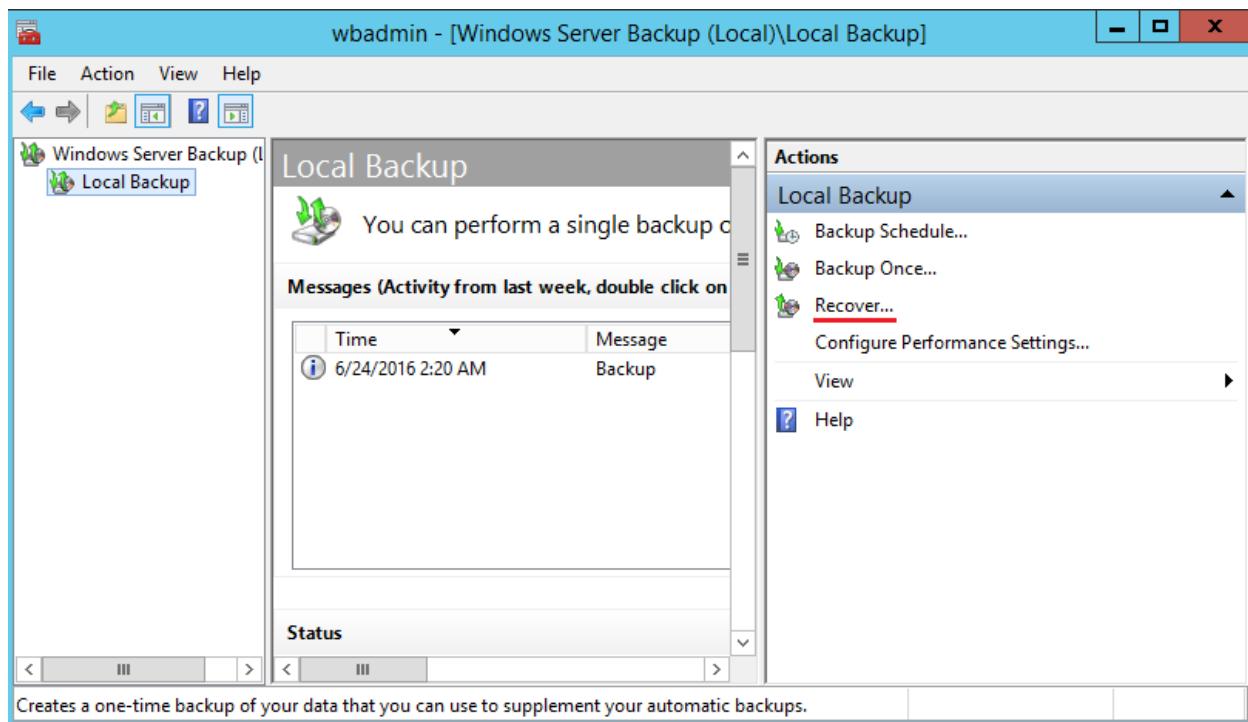
- Máy chủ tiến hành backup dữ liệu, tại cửa sổ **Backup Progress**, click vào **Close**.



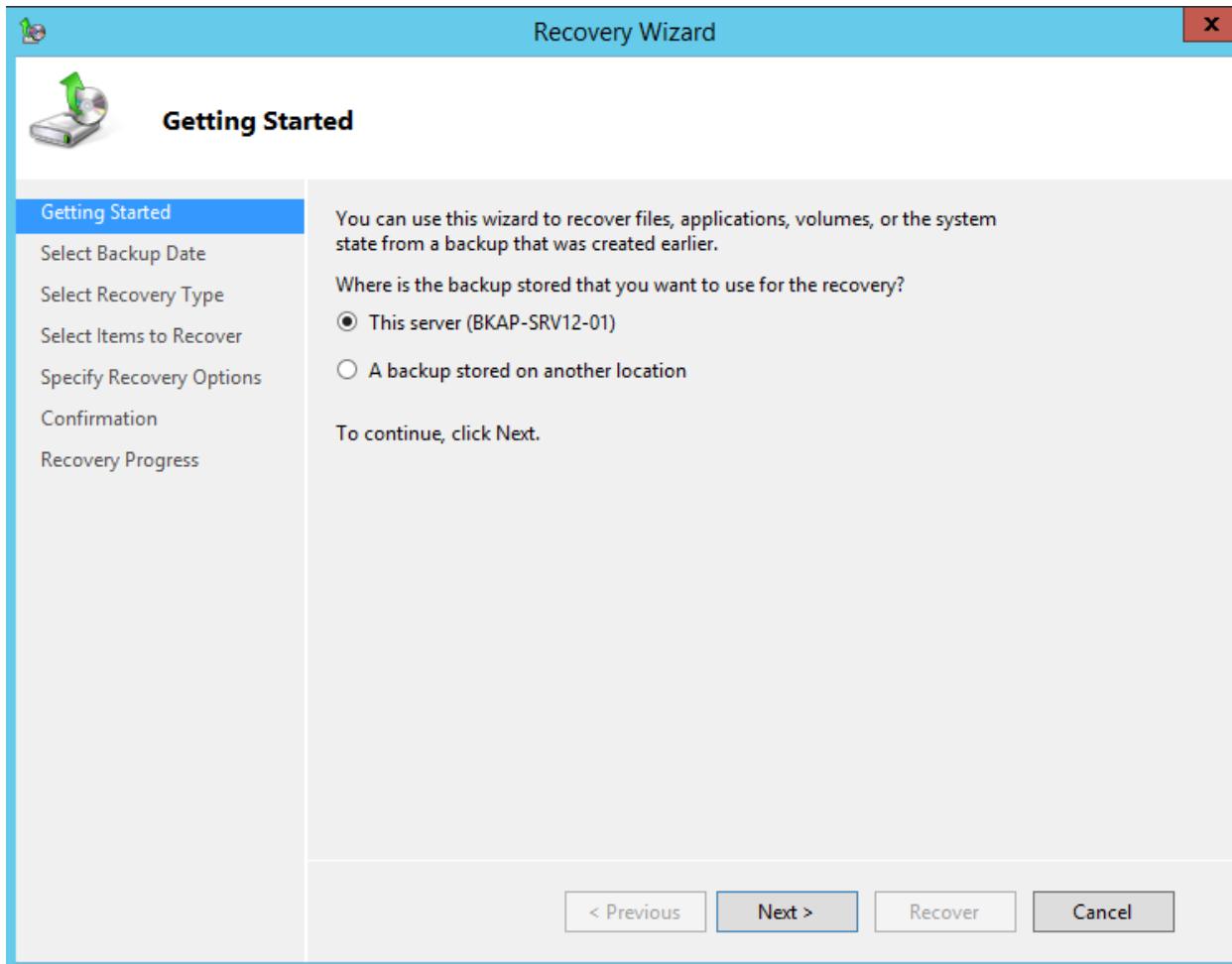
- Vào ô C, xóa thư mục Data.



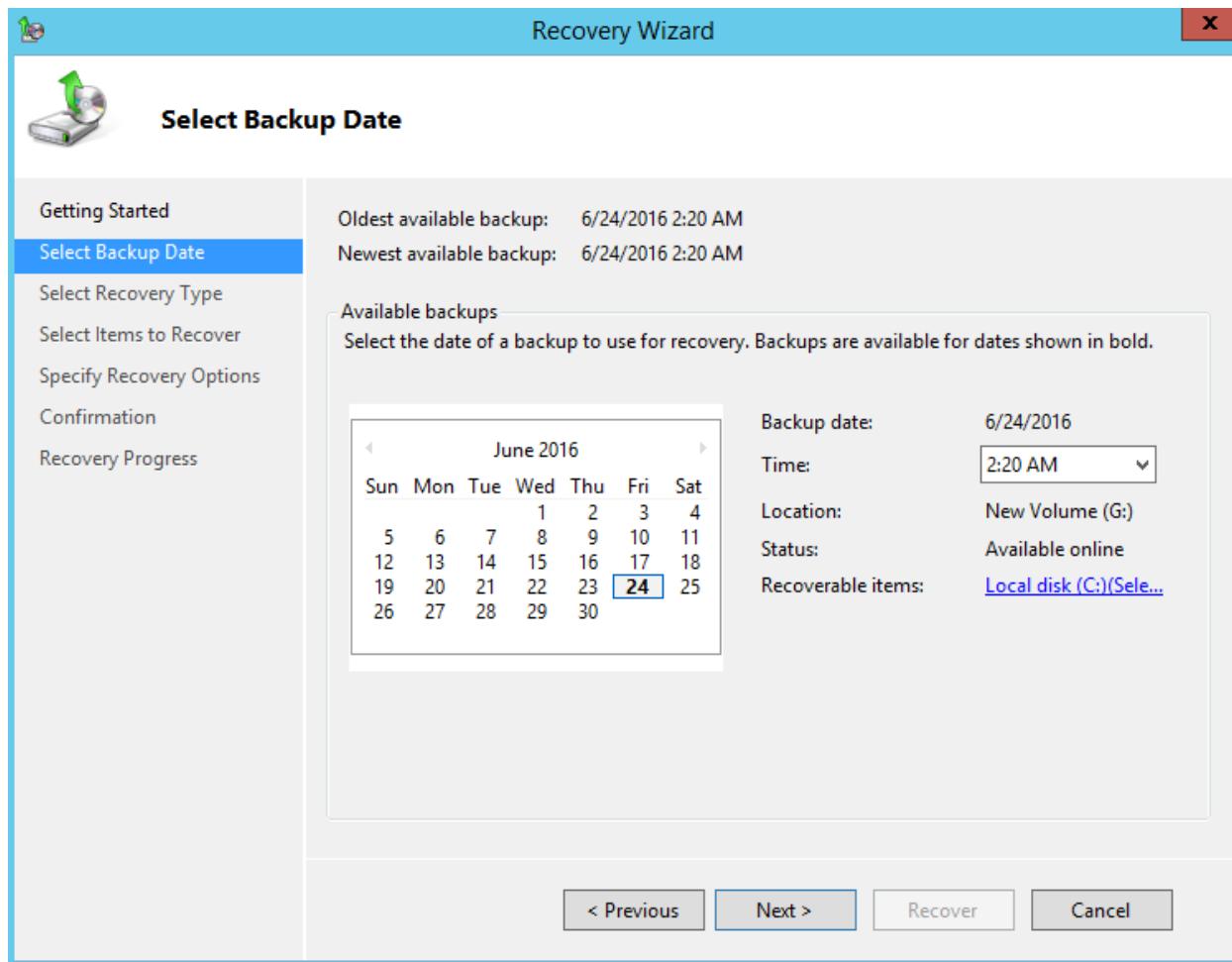
- Khôi phục lại dữ liệu:
 - Tại cửa sổ wbadmin – [Windows Server Backup (Local)\Local Backup] , click vào Recover...



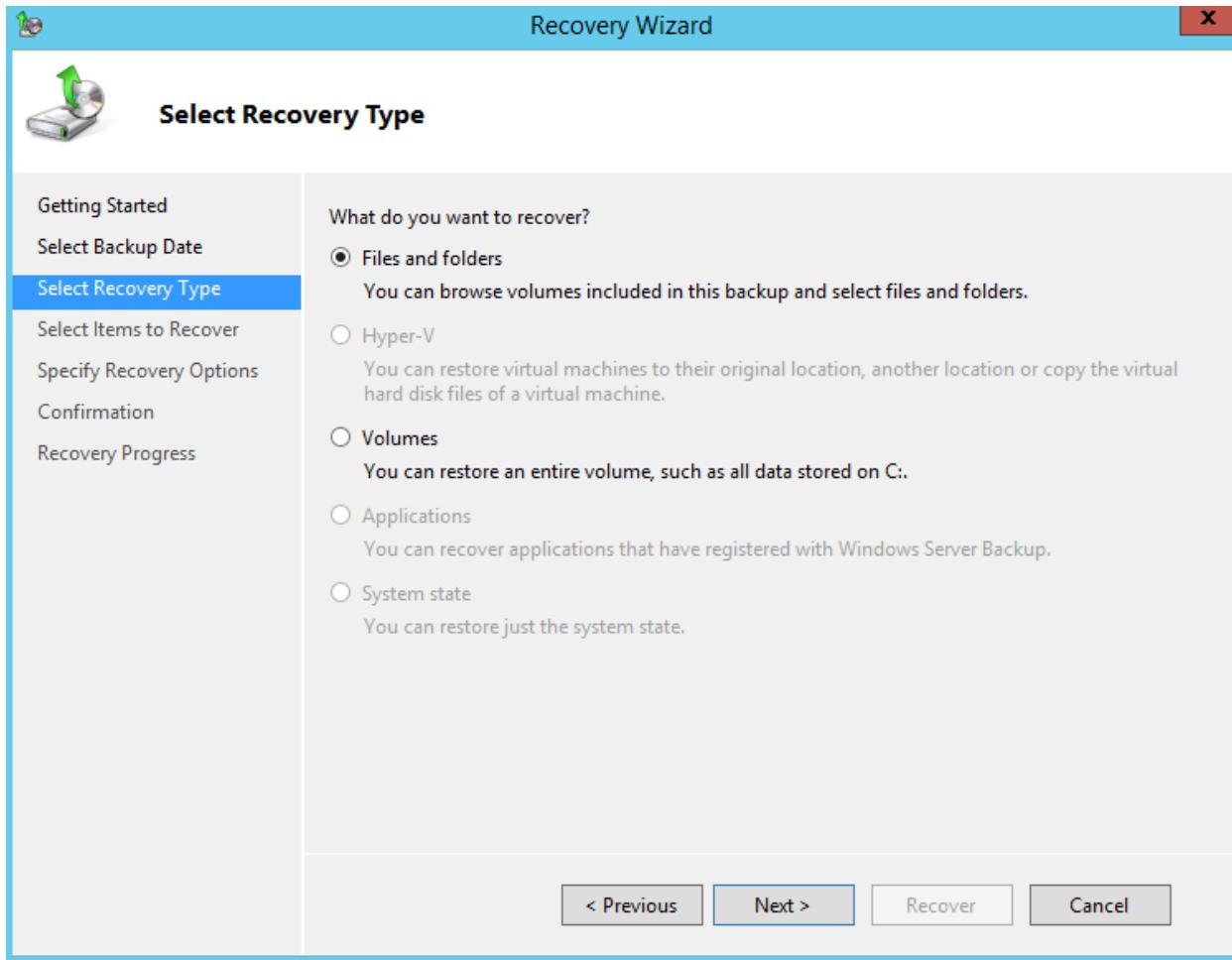
- Tại cửa sổ **Getting Started**, click chọn vào dòng **This server (BKAP-SRV12-01)**, click vào **Next**.



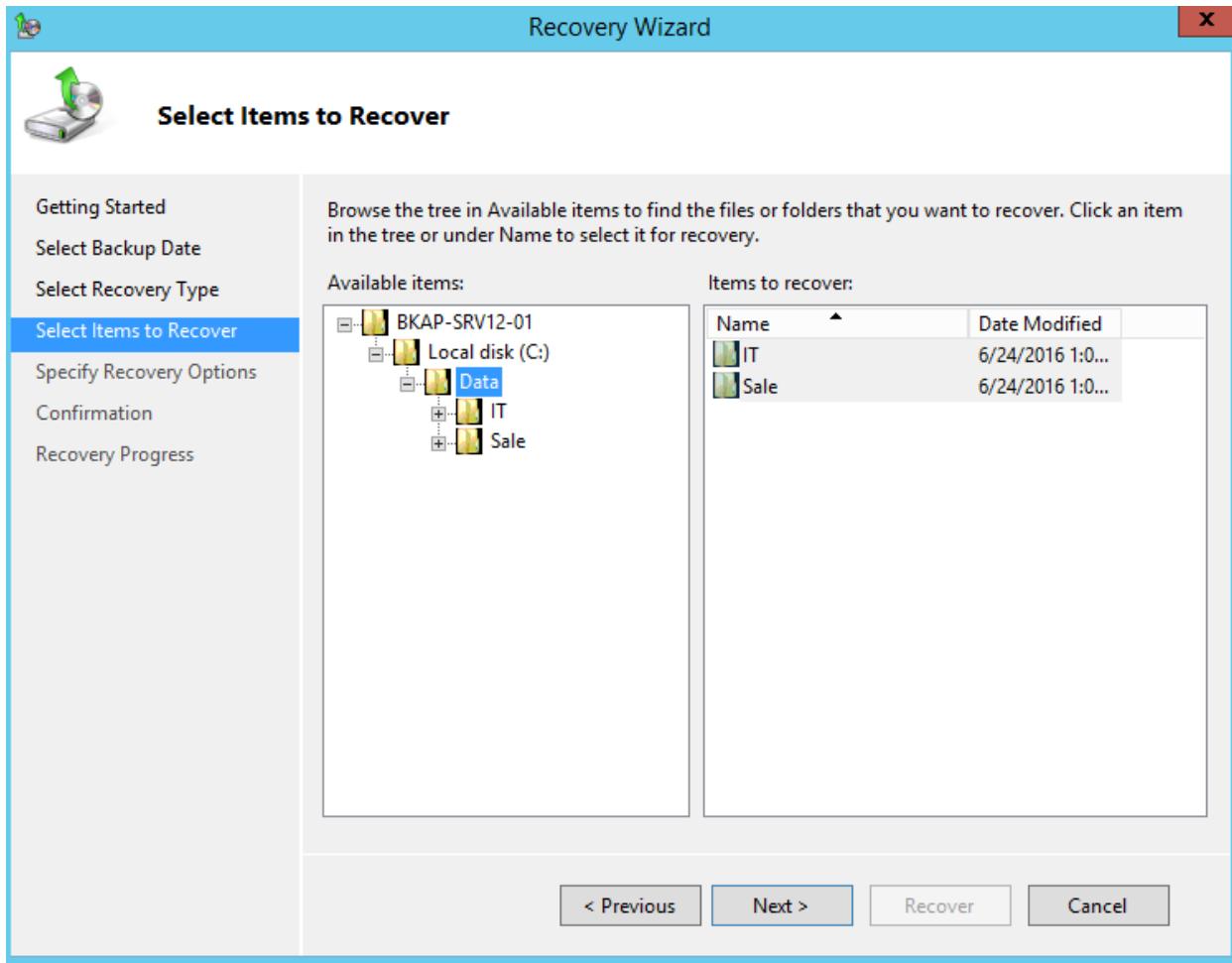
- Tại cửa sổ **Select Backup Date**, click vào **Next**.



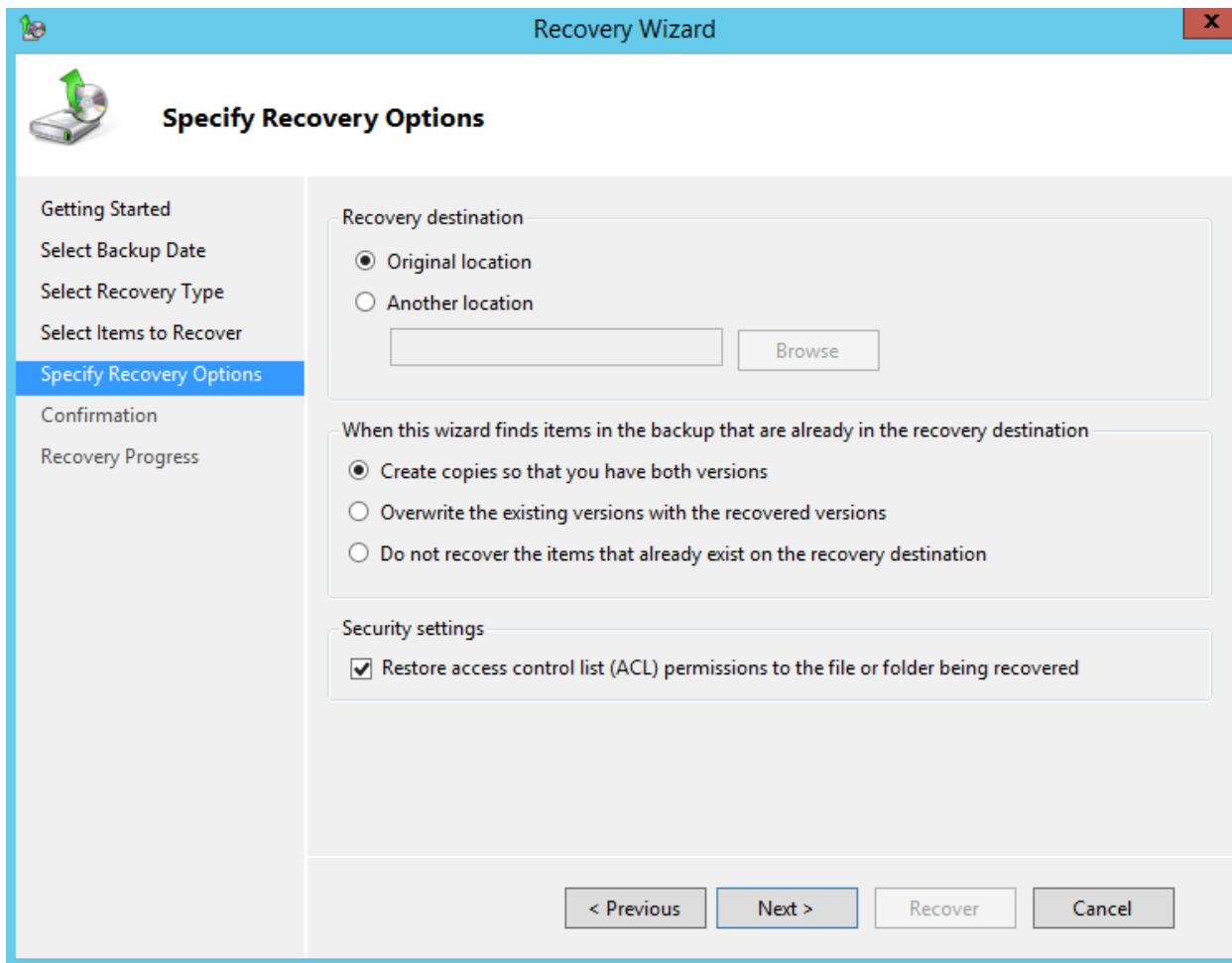
- Tại cửa sổ **Select Recovery Type**, click chọn vào **Files and folders**, click vào **Next**.



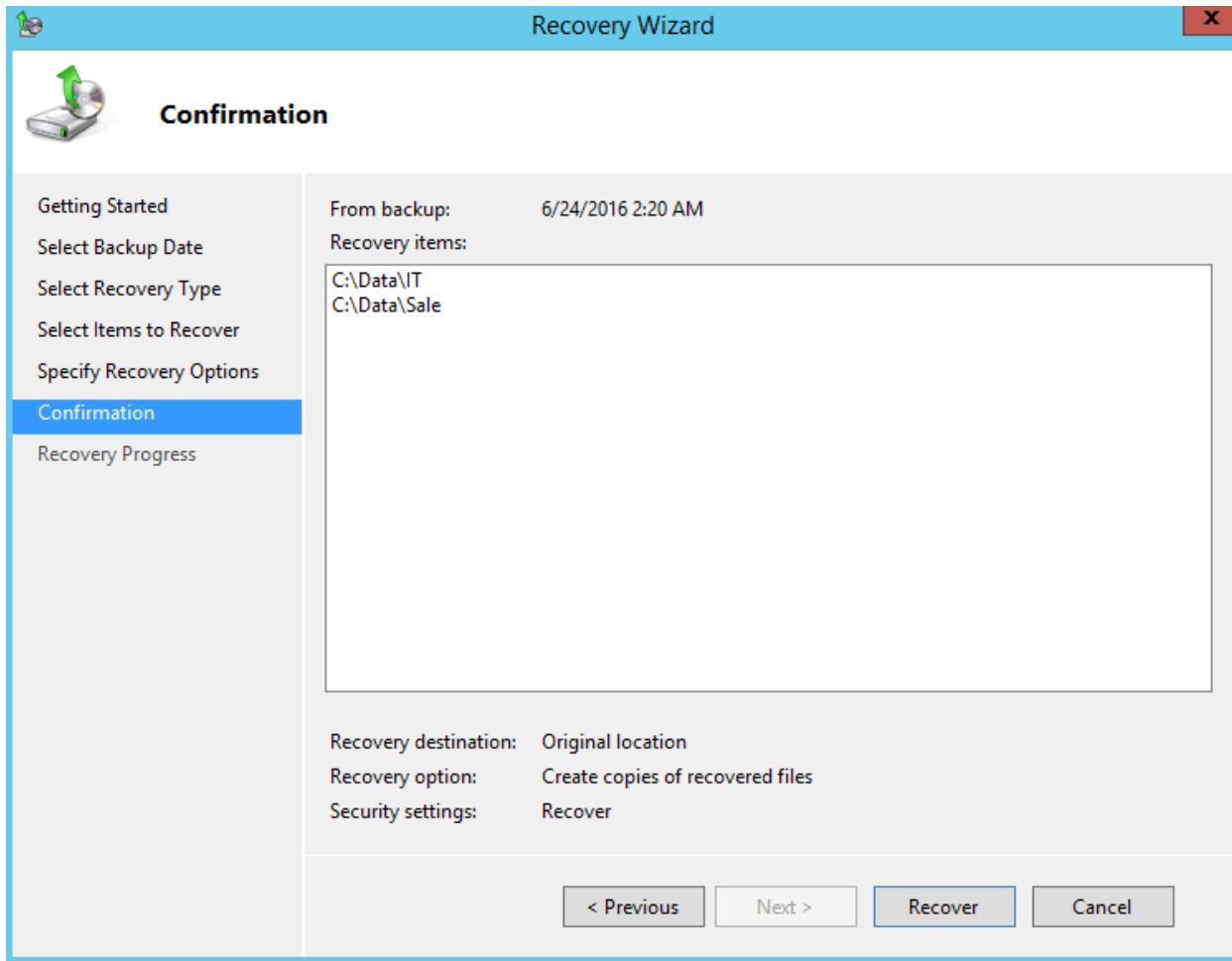
- Tại cửa sổ **Select Items to Recover**, trong mục Available items, click chọn vào **BKAP-SRV12-01 / Local disk (C:) / Data**. Click vào **Next**.



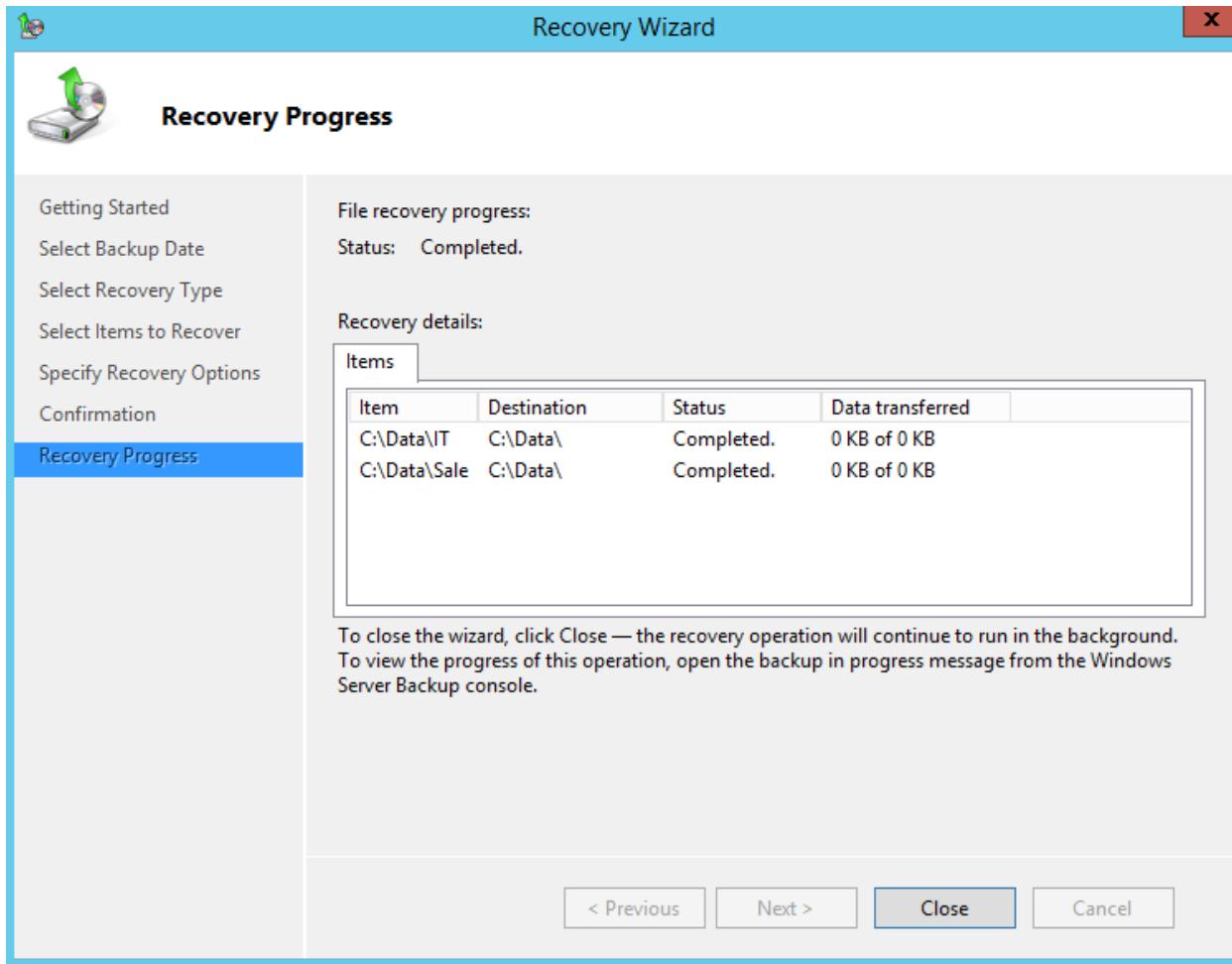
- Tại cửa sổ **Specify Recovery Options**, click vào **Next**.



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



- Máy chủ tiến hành phục hồi dữ liệu, click vào **Close** tại cửa sổ **Recovery**.



- Kiểm tra dữ liệu đã được phục hồi.

