

How to config Active Directory on window server 2022 as AD and AD certificate

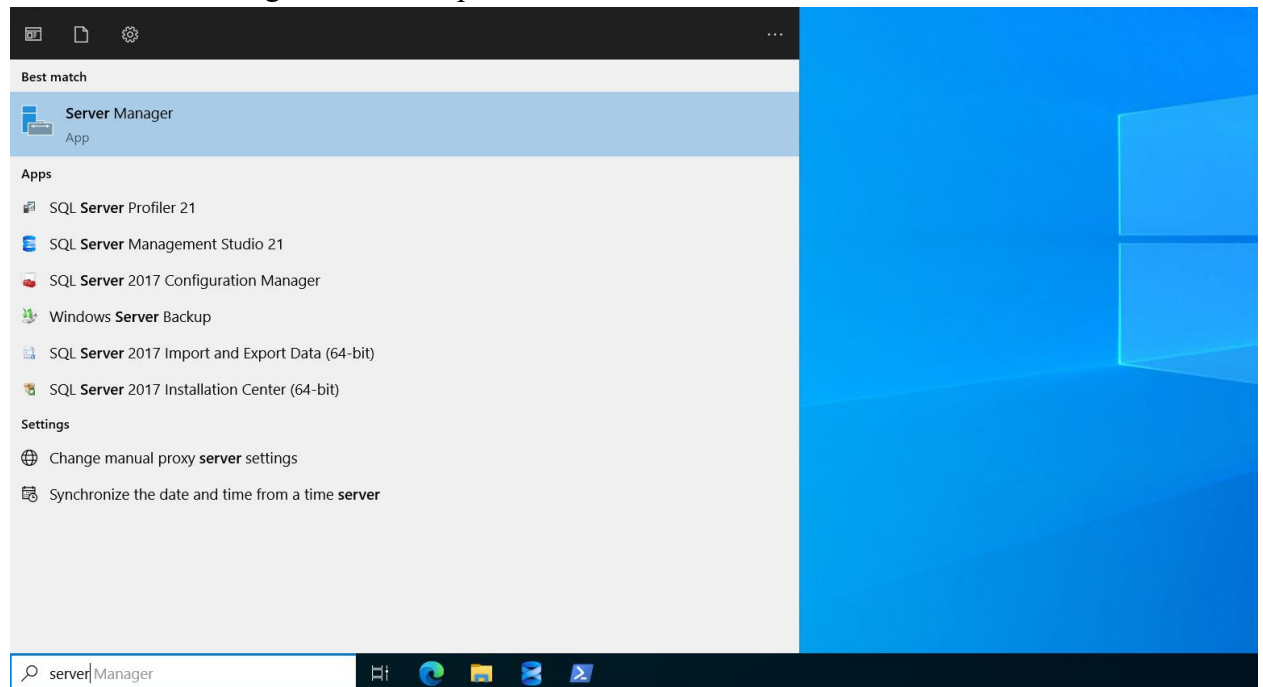
Mục lục

1. Config AD.....	1
2. Confirm AD running.....	14
3. Cấp certificate tự động khi máy join vào domain	15

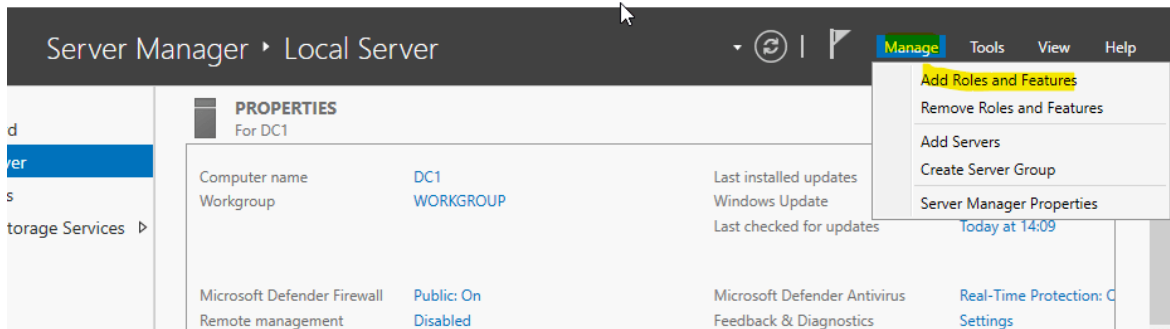
1. Config AD

- The Active Directory had been configured before this project. As a result, no installation backup is available. The previous configuration was reused as a reference for this documentation

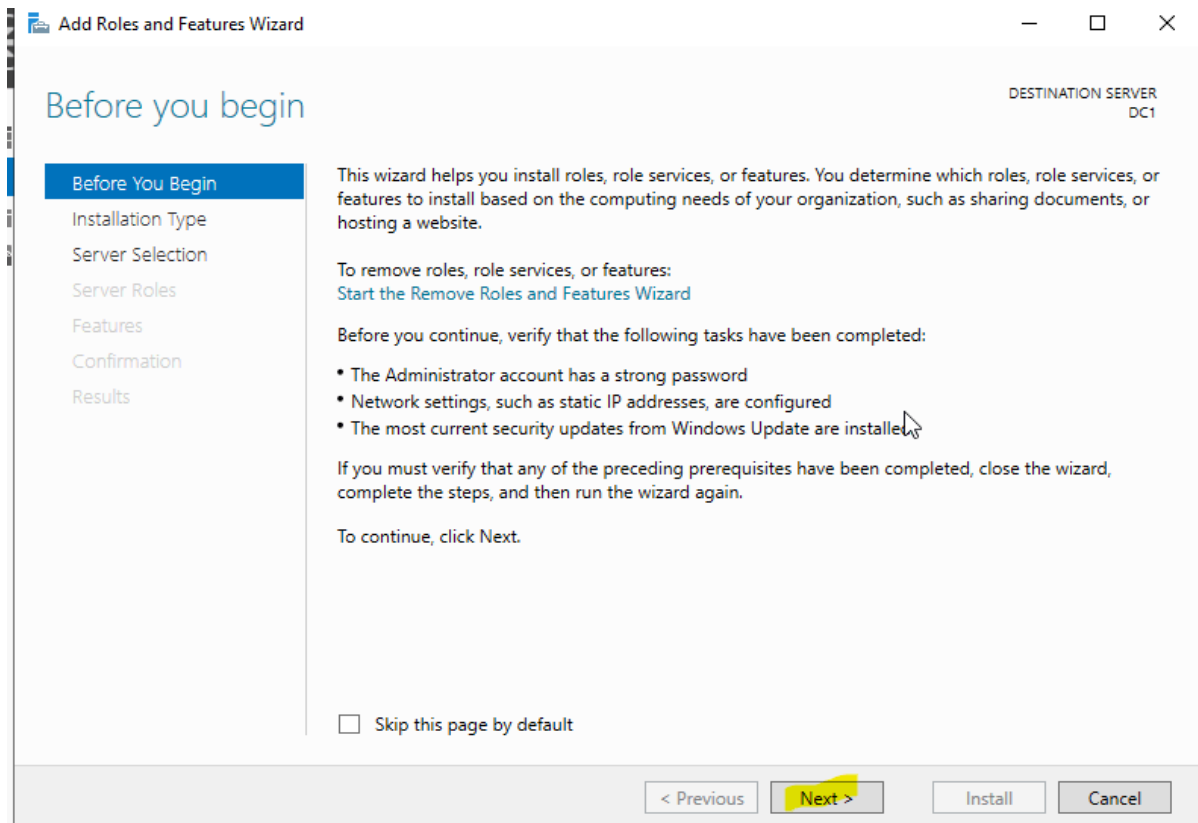
Search Server manager from lookup



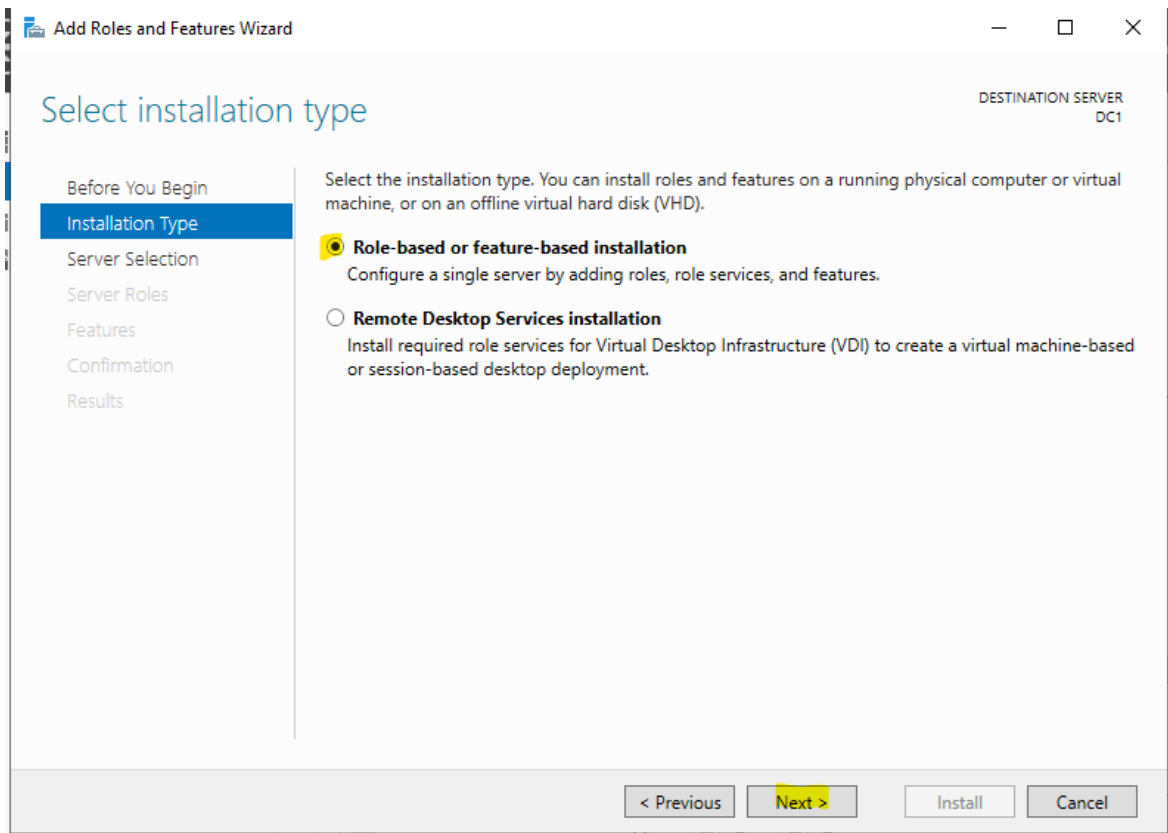
In the Server Manager, select Manage, and then Add Roles and Features



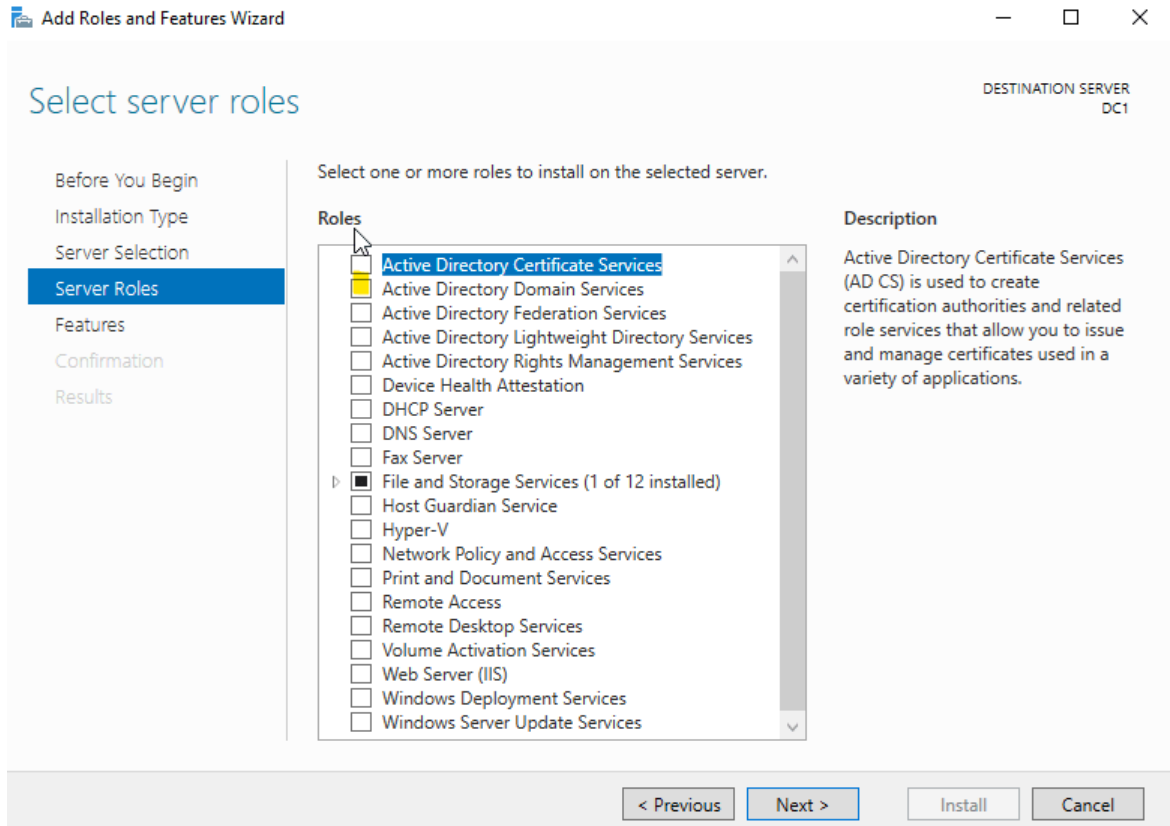
The wizard will give basic information; click Next.



Select Role-based or feature-based installation and click Next



Select Active Directory Certificate Service, Active Directory Domain Service, DNS Server



Leave the tick box ticked to Include management tools, and click Add Features.

Select server role

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Confirmation

Results

Add Roles and Features Wizard

Add features that are required for Active Directory Domain Services?

You cannot install Active Directory Domain Services unless the following role services or features are also installed.

- [Tools] Group Policy Management
- ▲ Remote Server Administration Tools
 - ▲ Role Administration Tools
 - ▲ AD DS and AD LDS Tools
 - Active Directory module for Windows PowerShell
 - ▲ AD DS Tools
 - [Tools] Active Directory Administrative Center
 - [Tools] AD DS Snap-Ins and Command-Line Tools

☒ Include management tools (if applicable)

Add Features **Cancel**

DESTINATION SERVER
DC1

Option

Directory Domain Services (AD DS) stores information about users and groups on the network and makes this information available to users and network administrators. AD DS is used by domain controllers to give users access to permitted resources anywhere on the network through a single logon process.

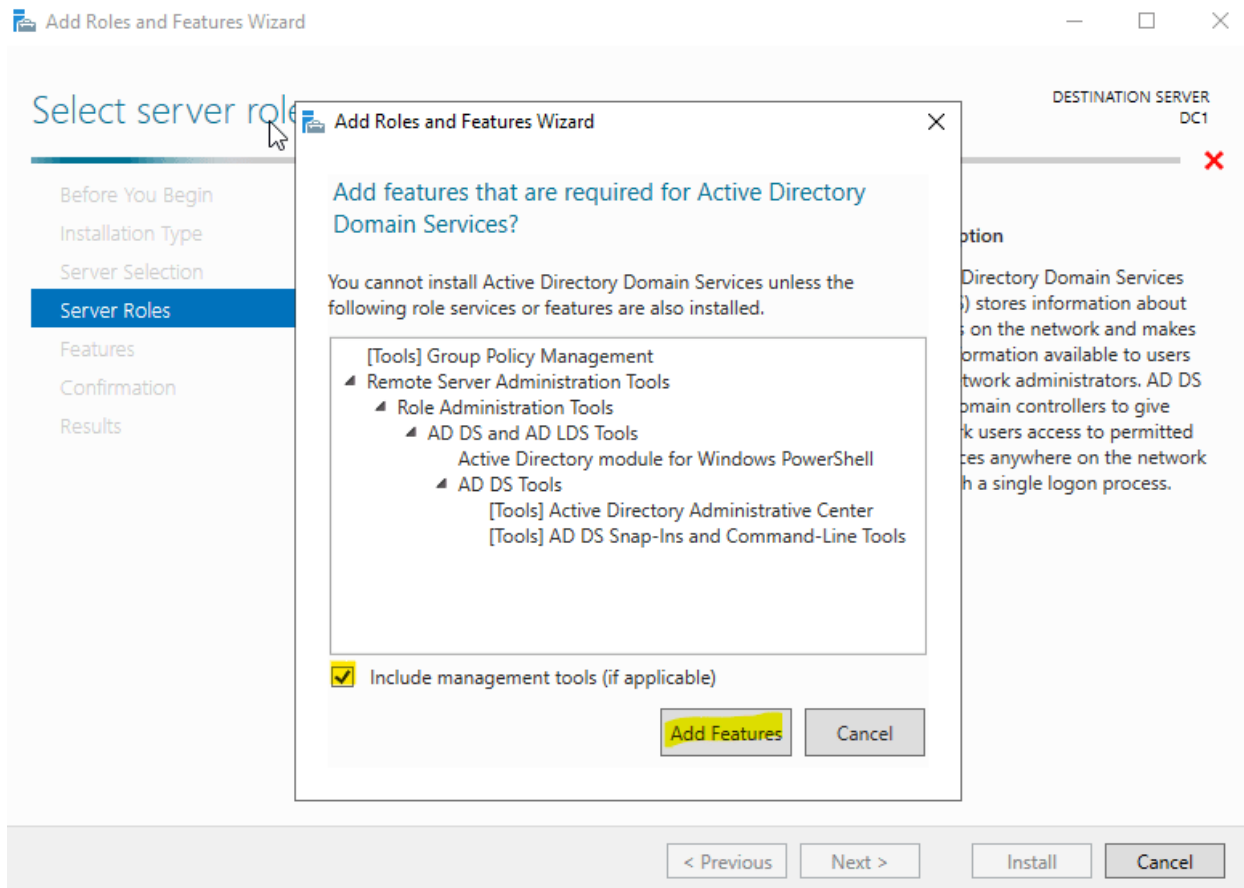
< Previous

Next >

Install

Cancel

Leave the tick box ticked to Include management tools, and click Add Features.



Active Directory Domain Services will now be ticked. Click Next.

Add Roles and Features Wizard

DESTINATION SERVER
DC1

Select server roles

Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
Confirmation
Results

Select one or more roles to install on the selected server.

Roles

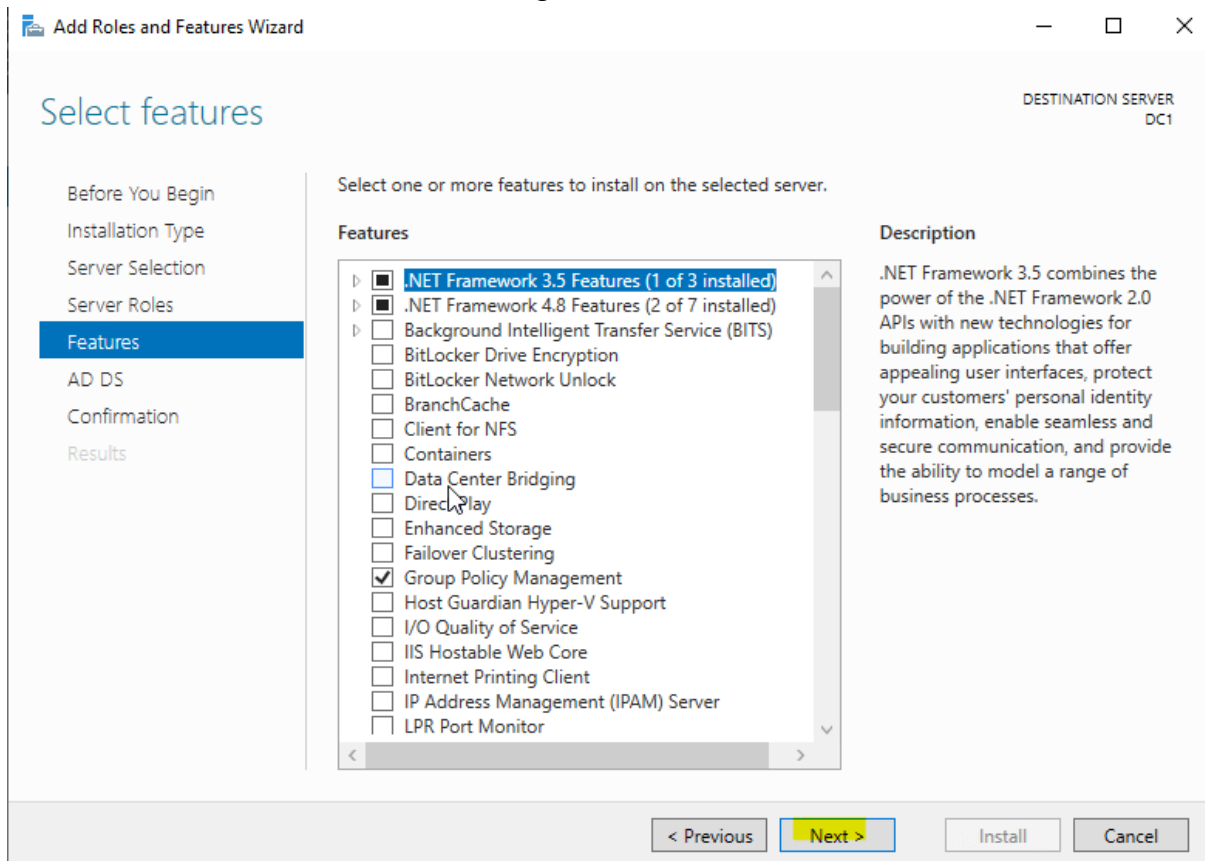
- ☐ Active Directory Certificate Services
- ☒ Active Directory Domain Services
- ☐ Active Directory Federation Services
- ☐ Active Directory Lightweight Directory Services
- ☐ Active Directory Rights Management Services
- ☐ Device Health Attestation
- ☐ DHCP Server
- ☐ DNS Server
- ☐ Fax Server
- ☒ File and Storage Services (1 of 12 installed)
- ☐ Host Guardian Service
- ☐ Hyper-V
- ☐ Network Policy and Access Services
- ☐ Print and Document Services
- ☐ Remote Access
- ☐ Remote Desktop Services
- ☐ Volume Activation Services
- ☐ Web Server (IIS)
- ☐ Windows Deployment Services
- ☐ Windows Server Update Services

Description

Active Directory Domain Services (AD DS) stores information about objects on the network and makes this information available to users and network administrators. AD DS uses domain controllers to give network users access to permitted resources anywhere on the network through a single logon process.

< Previous **Next >** Install Cancel

For the Features, click Next with no changes.



The Active Directory Domain Services will make some suggestions that are very important for production environments, namely:

Install a minimum of two domain controllers so users can log in even if there is a server outage.

A Microsoft DNS server must be set up in the network.

Click Next.



Active Directory Domain Services

DESTINATION SERVER
DC1[Before You Begin](#)[Installation Type](#)[Server Selection](#)[Server Roles](#)[Features](#)**AD DS**[Confirmation](#)[Results](#)

Active Directory Domain Services (AD DS) stores information about users, computers, and other devices on the network. AD DS helps administrators securely manage this information and facilitates resource sharing and collaboration between users.

Things to note:

- To help ensure that users can still log on to the network in the case of a server outage, install a minimum of two domain controllers for a domain.
- AD DS requires a DNS server to be installed on the network. If you do not have a DNS server installed, you will be prompted to install the DNS Server role on this machine.



Azure Active Directory, a separate online service, can provide simplified identity and access management, security reporting, single sign-on to cloud and on-premises web apps.

[Learn more about Azure Active Directory](#)

[Configure Office 365 with Azure Active Directory Connect](#)

< Previous

Next >

Install

Cancel

Confirm installation selections

DESTINATION SERVER
DC1[Before You Begin](#)[Installation Type](#)[Server Selection](#)[Server Roles](#)[Features](#)[AD DS](#)**[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 Domain Services
Group Policy Management
Remote Server Administration Tools
 Role Administration Tools
 AD DS and AD LDS Tools
 Active Directory module for Windows PowerShell
 AD DS Tools
 Active Directory Administrative Center
 AD DS Snap-Ins and Command-Line Tools

[Export configuration settings](#)
[Specify an alternate source path](#)

< Previous

Next >

Install

Cancel

If the option to restart was selected, click Yes to allow the automatic restart.

Confirm installation selections

DESTINATION SERVER
DC1[Before You Begin](#)[Installation Type](#)[Server Selection](#)[Server Roles](#)[Features](#)[AD DS](#)**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 Domain Services

Group Policy Management

Remote Server Administration Tools

Role Administration Add Roles and Features Wizard

AD



If a restart is required, this server restarts automatically, without additional notifications. Do you want to allow automatic restarts?

Yes

No

[Export configuration settings](#)[Specify an alternate source path](#)

< Previous

Next >

Install

Cancel

Installation of the Active Directory Domain Services and certificate will now run. Once

completed, select the option to Promote this server to a domain controller.

Add Roles and Features Wizard

DESTINATION SERVER
DC1

Installation progress

Before You Begin

Installation Type

Server Selection

Server Roles

Features

AD DS

Confirmation

Results

View installation progress

Feature installation

Configuration required. Installation succeeded on DC1.

Active Directory Domain Services

Additional steps are required to make this machine a domain controller.

Promote this server to a domain controller

Group Policy Management

Remote Server Administration Tools

Role Administration Tools

AD DS and AD LDS Tools

Active Directory module for Windows PowerShell

AD DS Tools

Active Directory Administrative Center

AD DS Snap-Ins and Command-Line Tools

You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

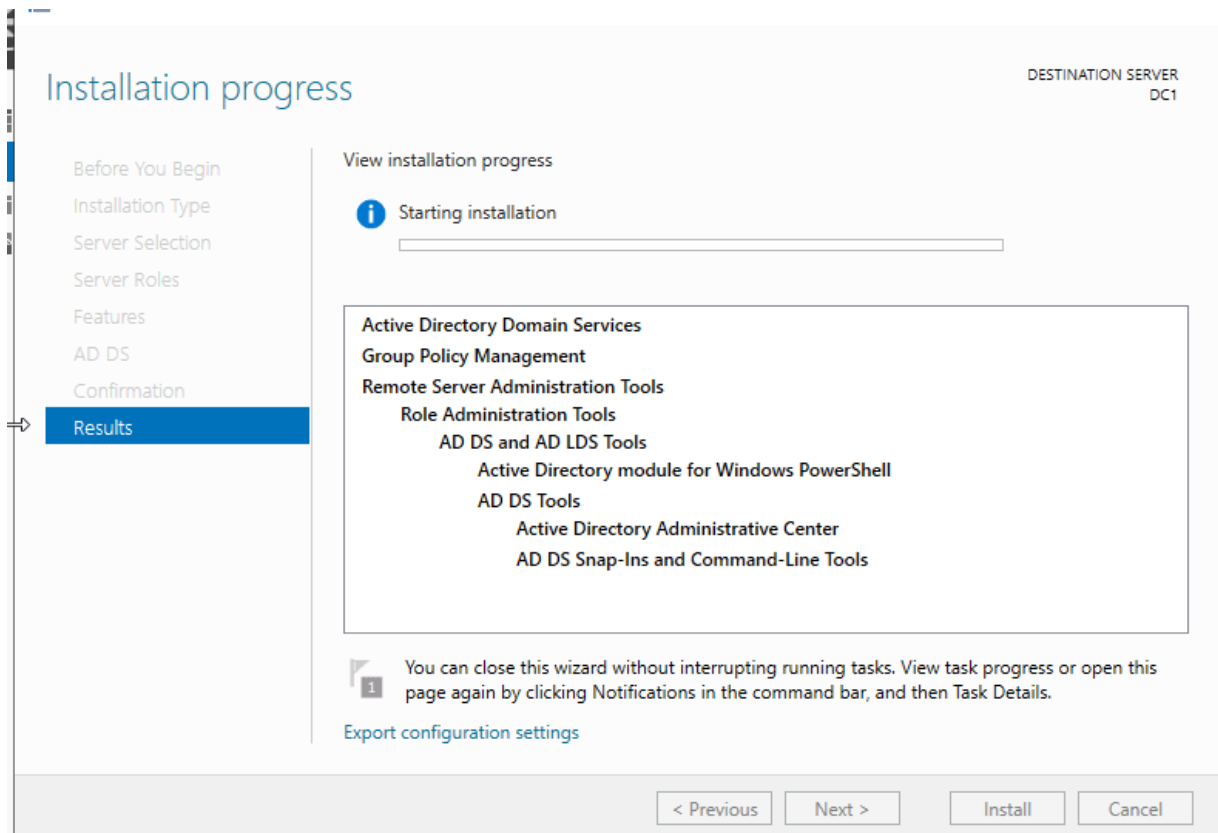
[Export configuration settings](#)

< Previous

Next >

Close

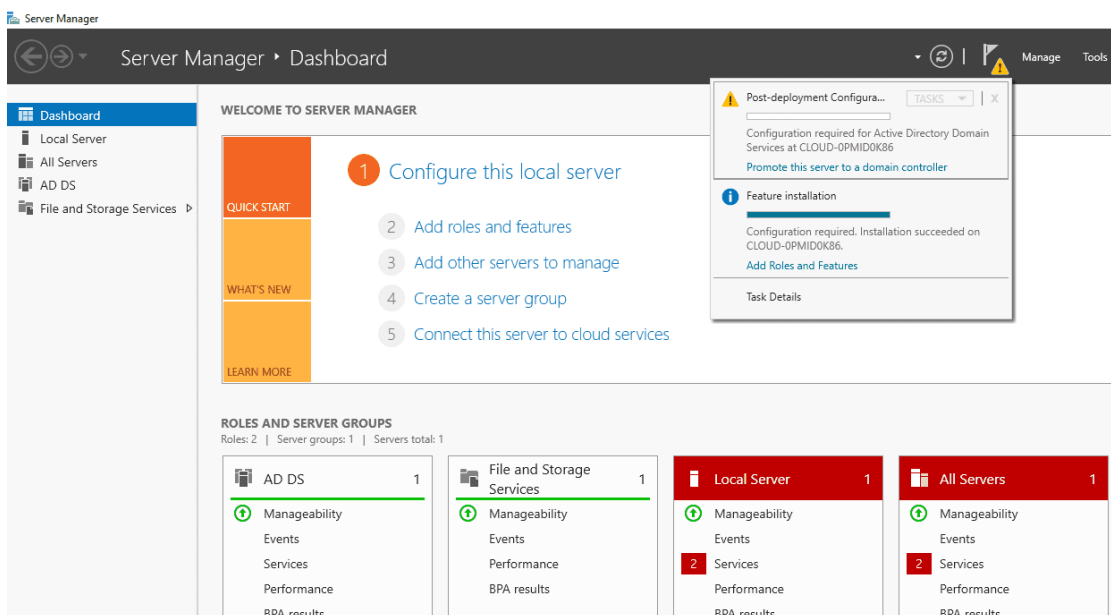
Cancel



At this point, the Active Directory Domain service has been installed on your server. Now, you will need to set up it on the server.

Follow the below steps to set up the Active Directory Domain:

After the Active Directory Domain service installation, you should see the yellow notification icon on the Server Manager:



As this is a new domain, we will create a new forest.

For the root domain name, it is best to use a subdomain of an existing public FQDN (Fully Qualified Domain Name).

For example, adtest.foldersecurityviewer.com. In my case, I use “**zt.devsecops.local**”

2. Confirm AD running

```
PS C:\Users\Administrator> Get-Service adws, kdc, netlogon, dns
```

Status	Name	DisplayName
Running	adws	Active Directory Web Services
Running	dns	DNS Server
Running	kdc	Kerberos Key Distribution Center
Running	Netlogon	netlogon

```
PS C:\Users\Administrator> Get-ADDomainController
```

```
ComputerObjectDN      : CN=TCORP,OU=Domain Controllers,DC=zt,DC=devsecops,DC=local
DefaultPartition      : DC=zt,DC=devsecops,DC=local
Domain                : zt.devsecops.local
Enabled               : True
Forest                : zt.devsecops.local
HostName              : tcorp.zt.devsecops.local
InvocationId          : d53502d0-4683-4da5-9f23-272cf3521da8
IPv4Address           : 10.0.1.4
IPv6Address           :
IsGlobalCatalog       : True
IsReadOnly            : False
LdapPort              : 389
Name                  : TCORP
NTDSSettingsObjectDN  : CN=NTDS Settings,CN=TCORP,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=zt,DC=devsecops,DC=local
OperatingSystem       : Windows Server 2022 Standard Evaluation
OperatingSystemHotfix :
OperatingSystemServicePack :
OperatingSystemVersion : 10.0 (20348)
OperationMasterRoles  : {SchemaMaster, DomainNamingMaster, PDCEmulator, RIDMaster...}
Partitions             : {DC=ForestDnsZones,DC=zt,DC=devsecops,DC=local, DC=DomainDnsZones,DC=zt,DC=devsecops,DC=local, CN=Schema,CN=Configuration,DC=zt,DC=devsecops,DC=local}
ServerObjectDN        : CN=TCORP,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=zt,DC=devsecops,DC=local
ServerObjectGuid       : c8c52209-5b20-4a64-92ad-ec5dc7f3441c
Site                  : Default-First-Site-Name
SslPort               : 636
```

```

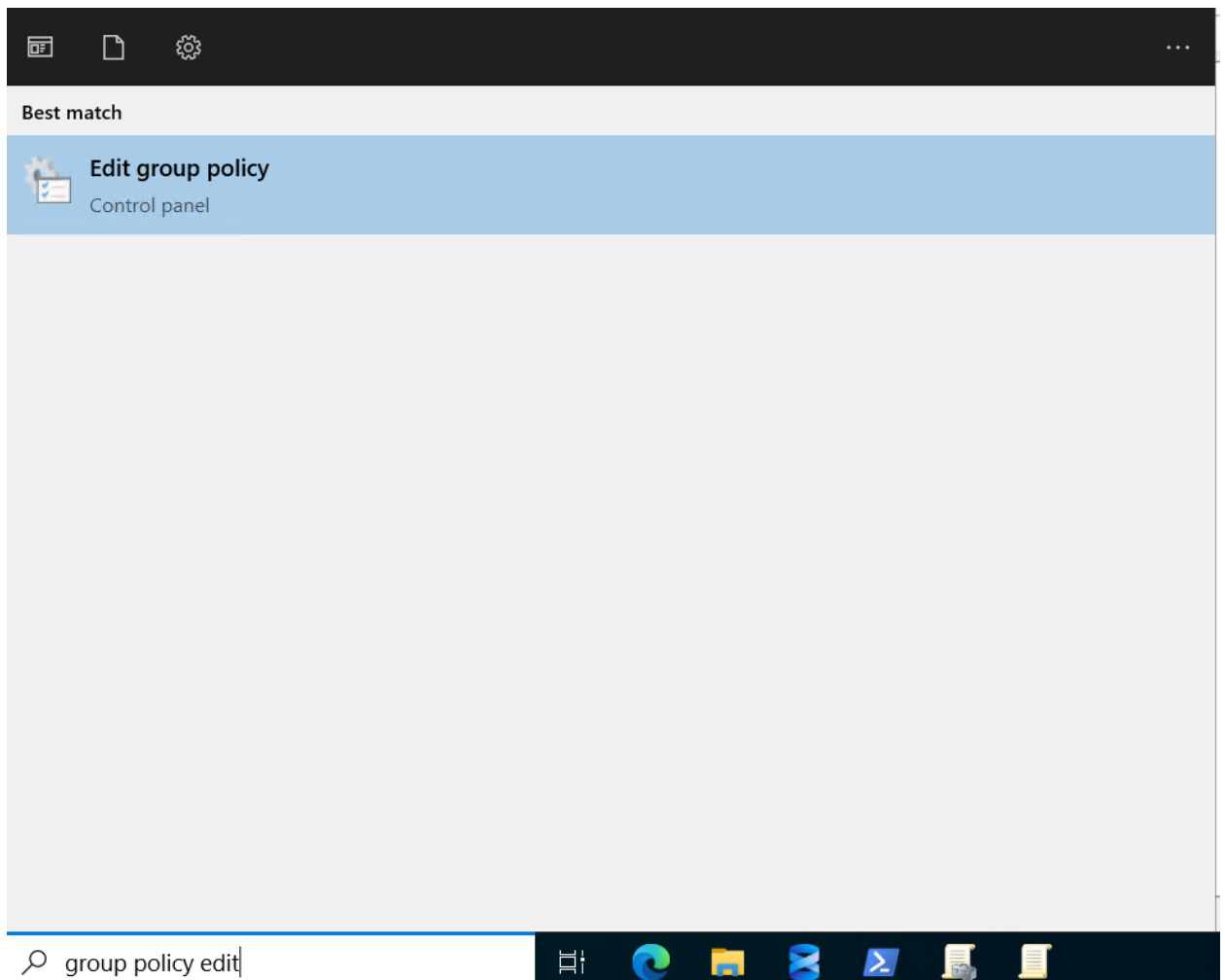
PS C:\Users\Administrator> Get-ADDomain zt.devsecops.local

AllowedDNSSuffixes      : {}
ChildDomains            : {}
ComputersContainer      : CN=Computers,DC=zt,DC=devsecops,DC=local
DeletedObjectsContainer : CN=Deleted Objects,DC=zt,DC=devsecops,DC=local
DistinguishedName       : DC=zt,DC=devsecops,DC=local
DNSRoot                 : zt.devsecops.local
DomainControllersContainer : OU=Domain Controllers,DC=zt,DC=devsecops,DC=local
DomainMode              : Windows2016Domain
DomainSID               : S-1-5-21-3877534076-3736767108-1919699349
ForeignSecurityPrincipalsContainer : CN=ForeignSecurityPrincipals,DC=zt,DC=devsecops,DC=local
Forest                  : zt.devsecops.local
InfrastructureMaster     : tcorp.zt.devsecops.local
LastLogonReplicationInterval : 
LinkedGroupPolicyObjects : {CN={31B2F340-016D-11D2-945F-00C04FB984F9},CN=Policies,CN=System,DC=zt,DC=devsecops,DC=local}
LostAndFoundContainer    : CN=LostAndFound,DC=zt,DC=devsecops,DC=local
ManagedBy               : 
Name                     : zt
NetBIOSName              : ZT
ObjectClass              : domainDNS
ObjectGUID               : 17846b36-27dc-4024-a705-ee407efa557c
ParentDomain             : 
PDCEmulator              : tcorp.zt.devsecops.local
PublicKeyRequiredPasswordRolling : True
QuotasContainer          : CN=NTDS Quotas,DC=zt,DC=devsecops,DC=local
ReadOnlyReplicaDirectoryServers : {}
ReplicaDirectoryServers  : {tcorp.zt.devsecops.local}
RIDMaster                : tcorp.zt.devsecops.local
SubordinateReferences    : {DC=ForestDnsZones,DC=zt,DC=devsecops,DC=local, DC=DomainDnsZones,DC=zt,DC=devsecops,DC=local}
SystemsContainer         : CN=System,DC=zt,DC=devsecops,DC=local
UsersContainer           : CN=Users,DC=zt,DC=devsecops,DC=local

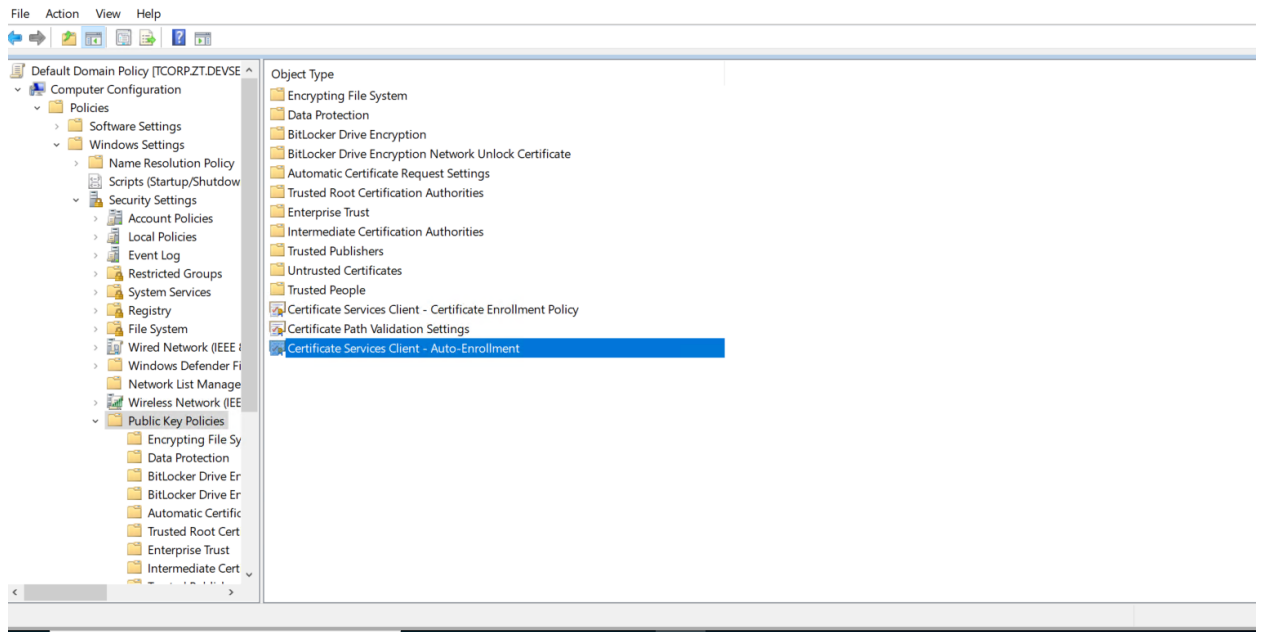
```

3. Cấp certificate tự động khi máy join vào domain

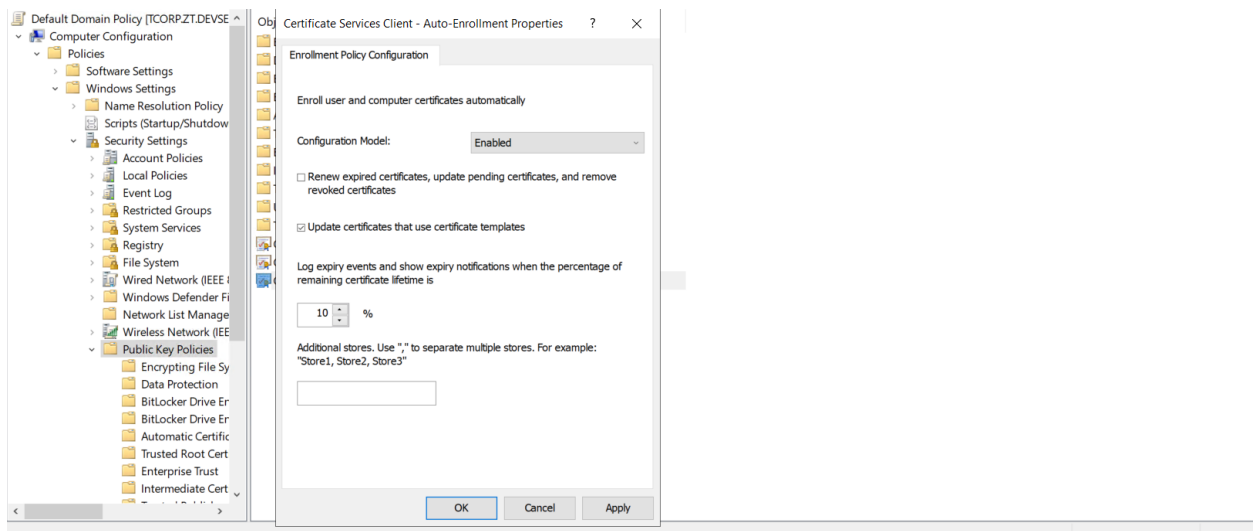
Search “Edit group policy”



Next, find computer configuration -> window settings -> public key policy -> Certificat services client – Auto-Enrollment



Enable and Apply



Go to cert manager -> Personal -> Certificate in the client that to join Domain controller. We'll

sê the certificate

certmgr - [Certificates - Current User\Personal\Certificates]

FileActionViewHelp

Certificates - Current User

Personal

Certificates

Trusted Root Certification Authorities

Enterprise Trust

Intermediate Certification Authorities

Active Directory User Objects

Trusted Publishers

Untrusted Certificates

Third-Party Root Certifications

Trusted People

Client Authentication Issuers

Local NonRemovable Certifications

Certificate Enrollment Request

Smart Card Trusted Roots

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certificate Te...
dev2	zt-TCORP-CA	10/30/2026	Encrypting File Syst...	<None>	User	Basic EFS

Personal store contains 2 certificates.