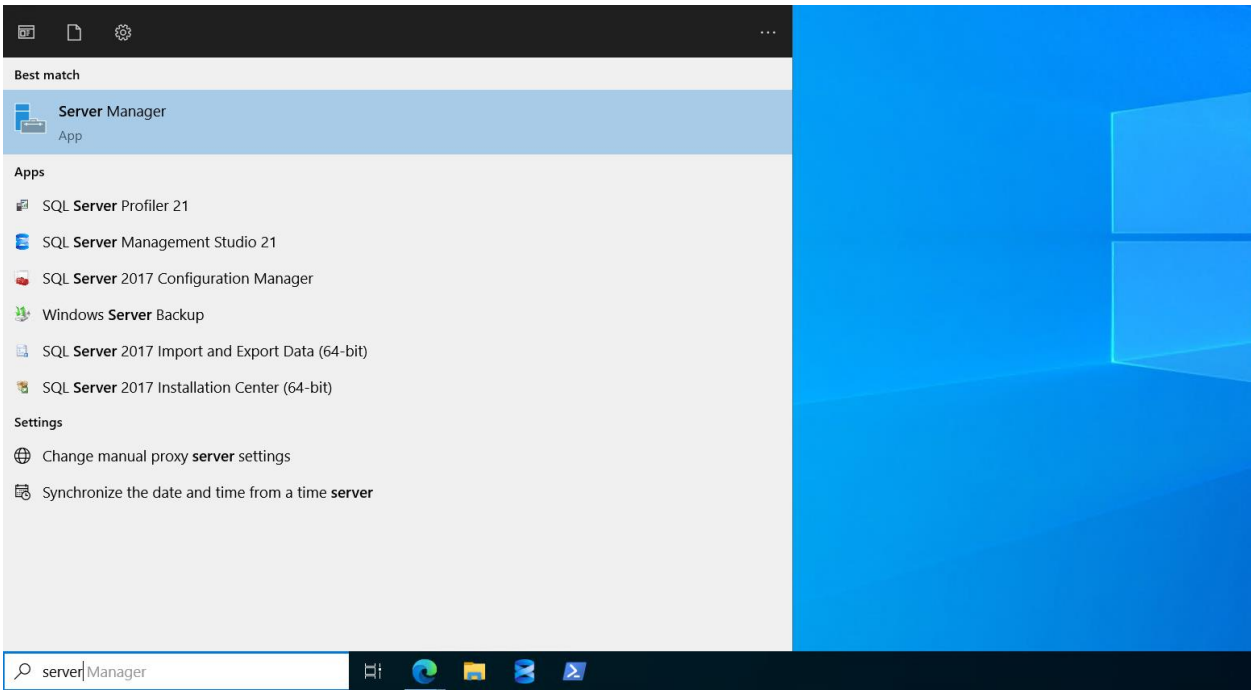
How to config Active Directory on window server 2022 as AD and AD certificate

Mục lục

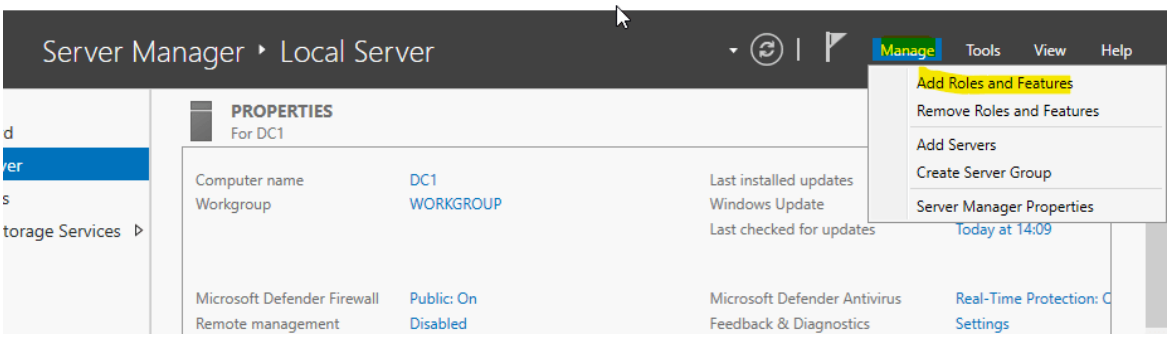
1. Config AD

- 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

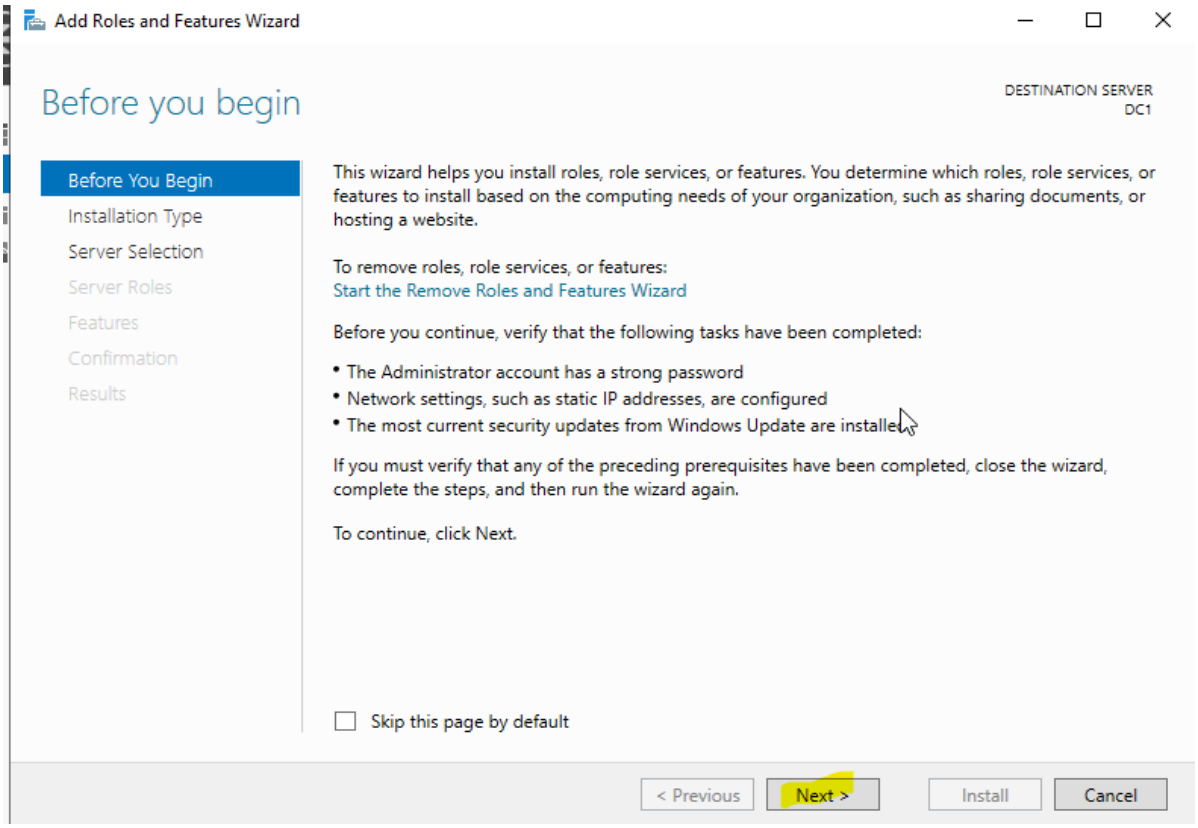
Search Server manager from lookup



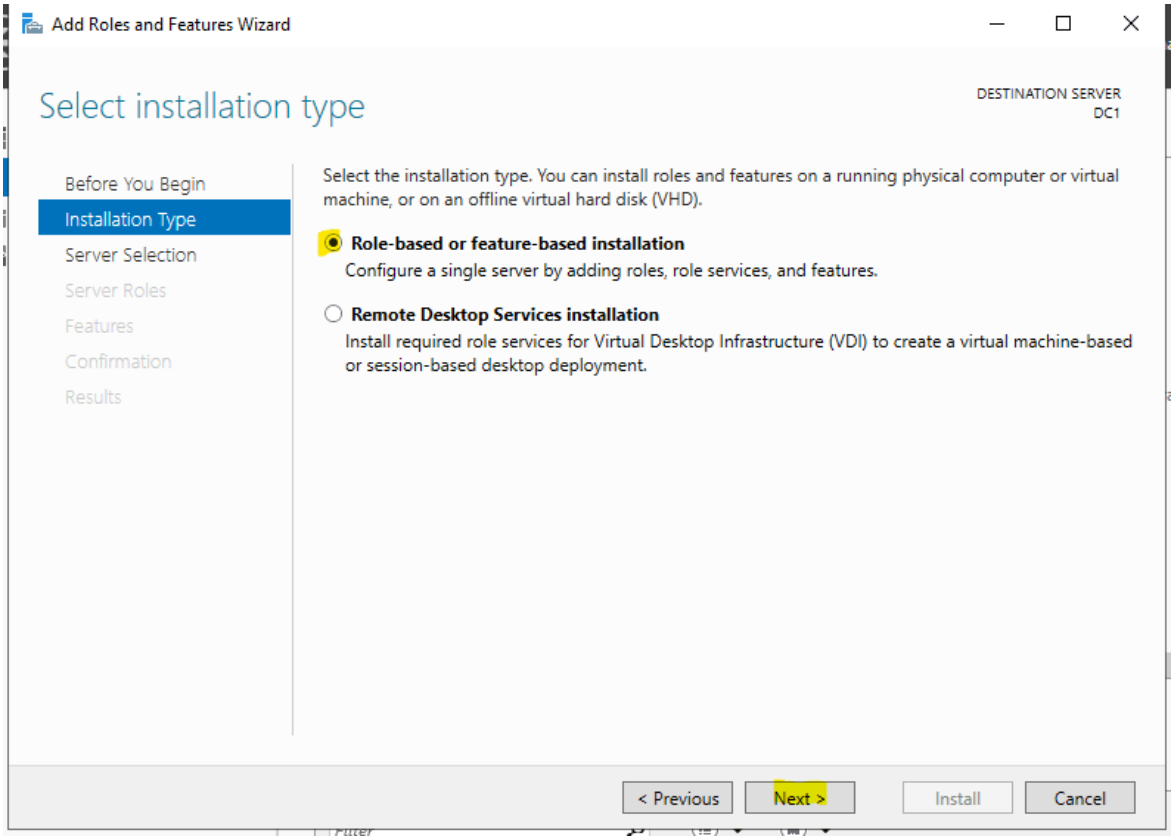
In the Server Manager, select Manage, and then Add Roles and Features



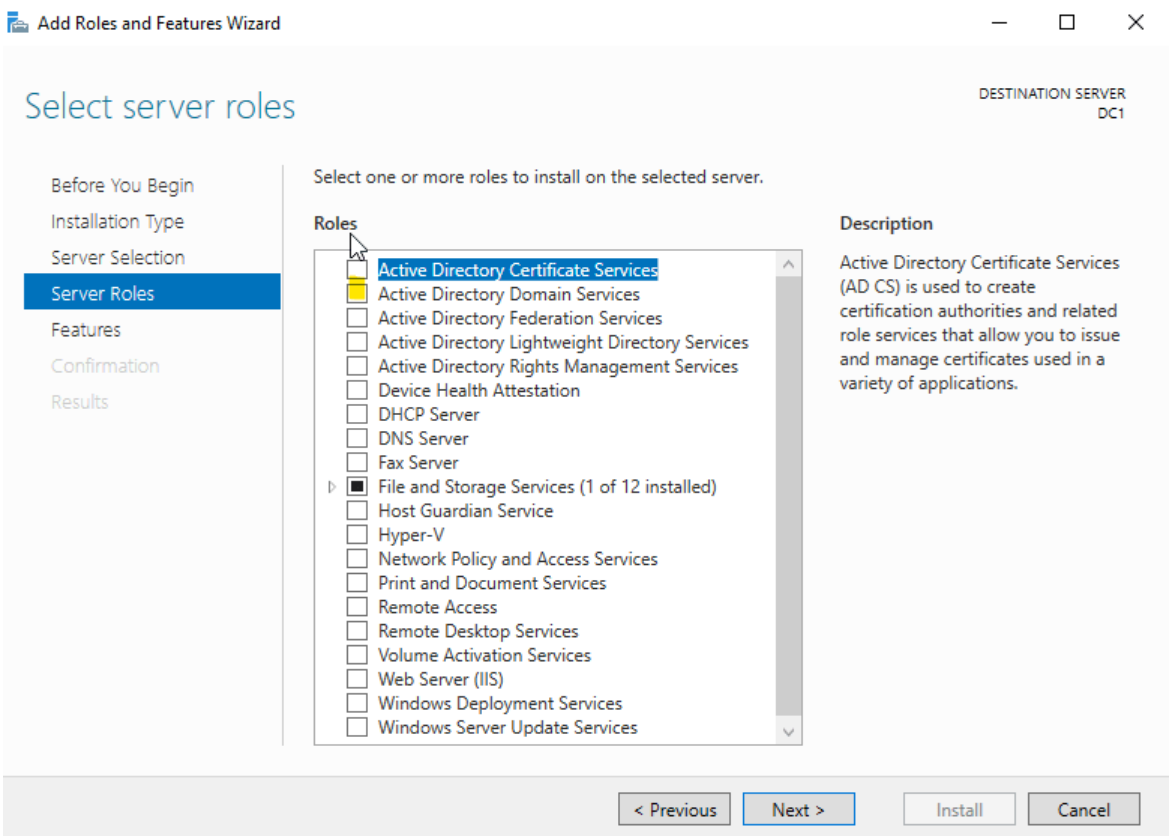
The wizard will give basic information; click Next.



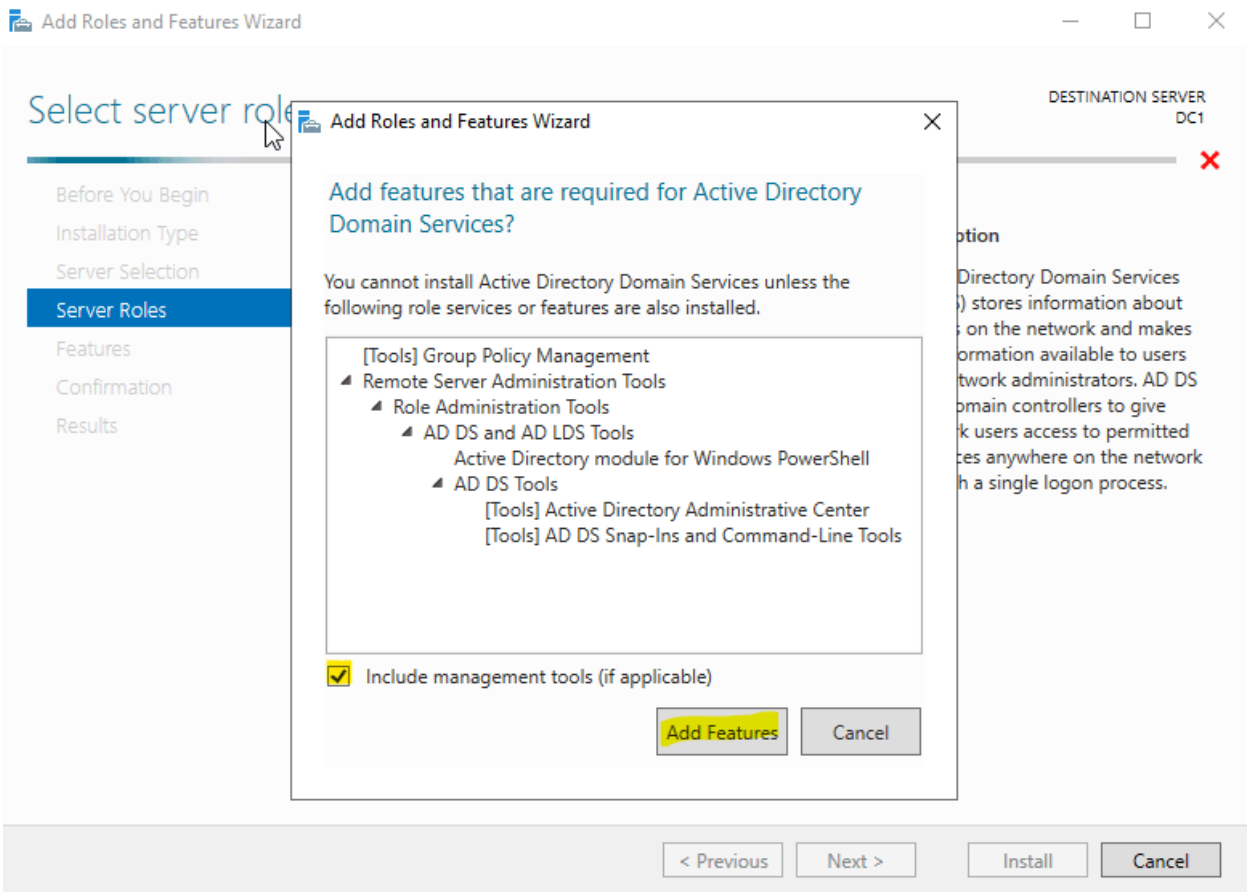
Select Role-based or feature-based installation and click Next



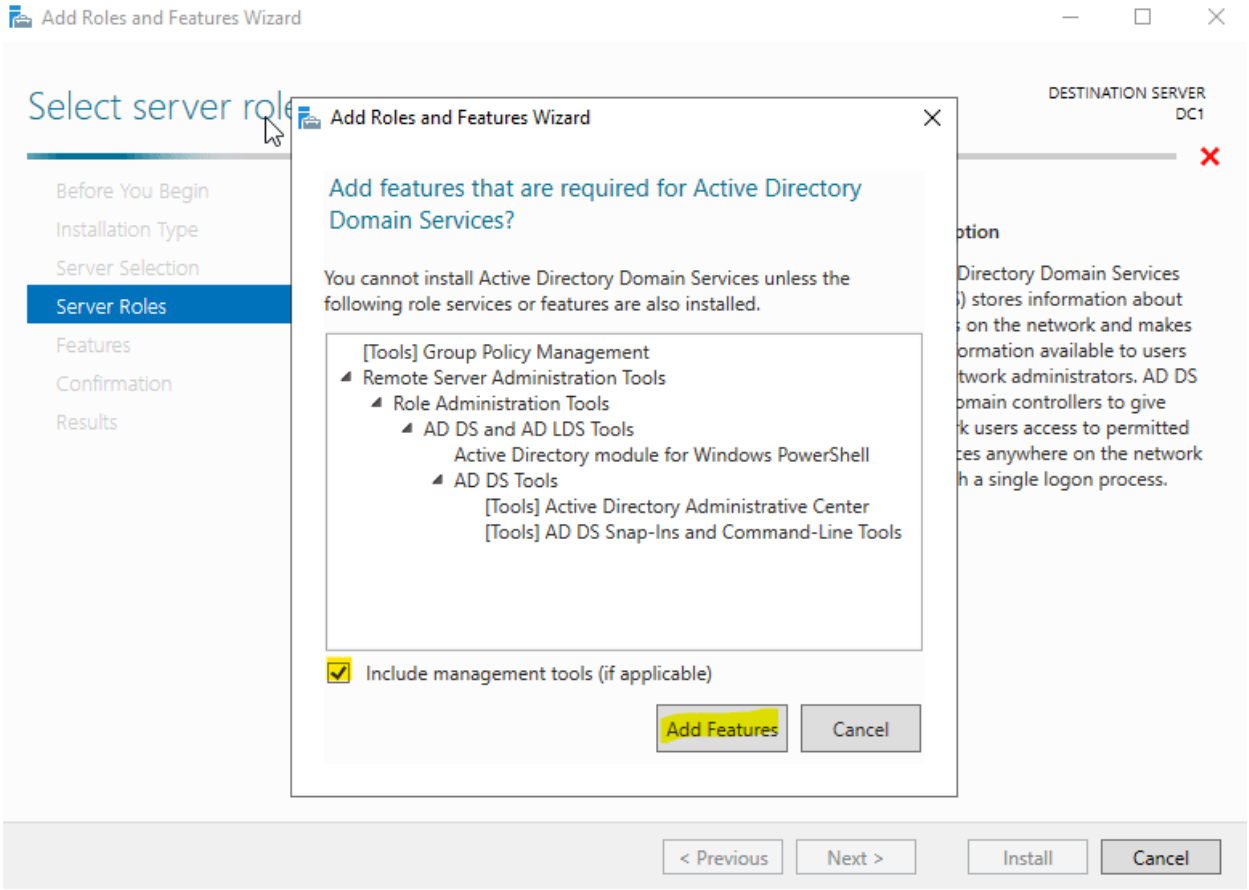
Select Active Directory Certificate Serivce, Active Directory Domain Service, DNS Server



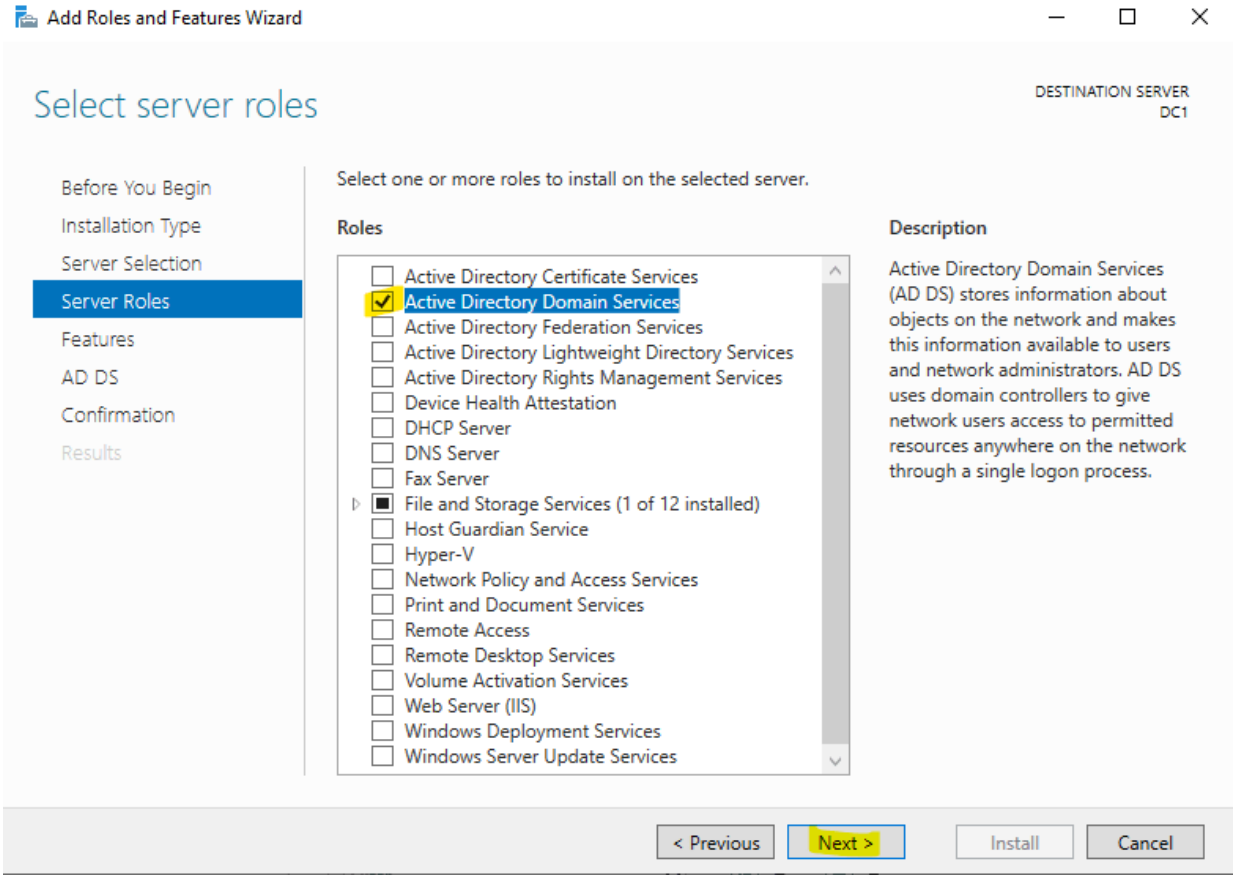
Leave the tick box ticked to Include management tools, and click Add Features.


Add Roles and Features Wizard
Select server role
DESTINATION SERVER
DC1
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
< Previous
Next >
Install
Cancel

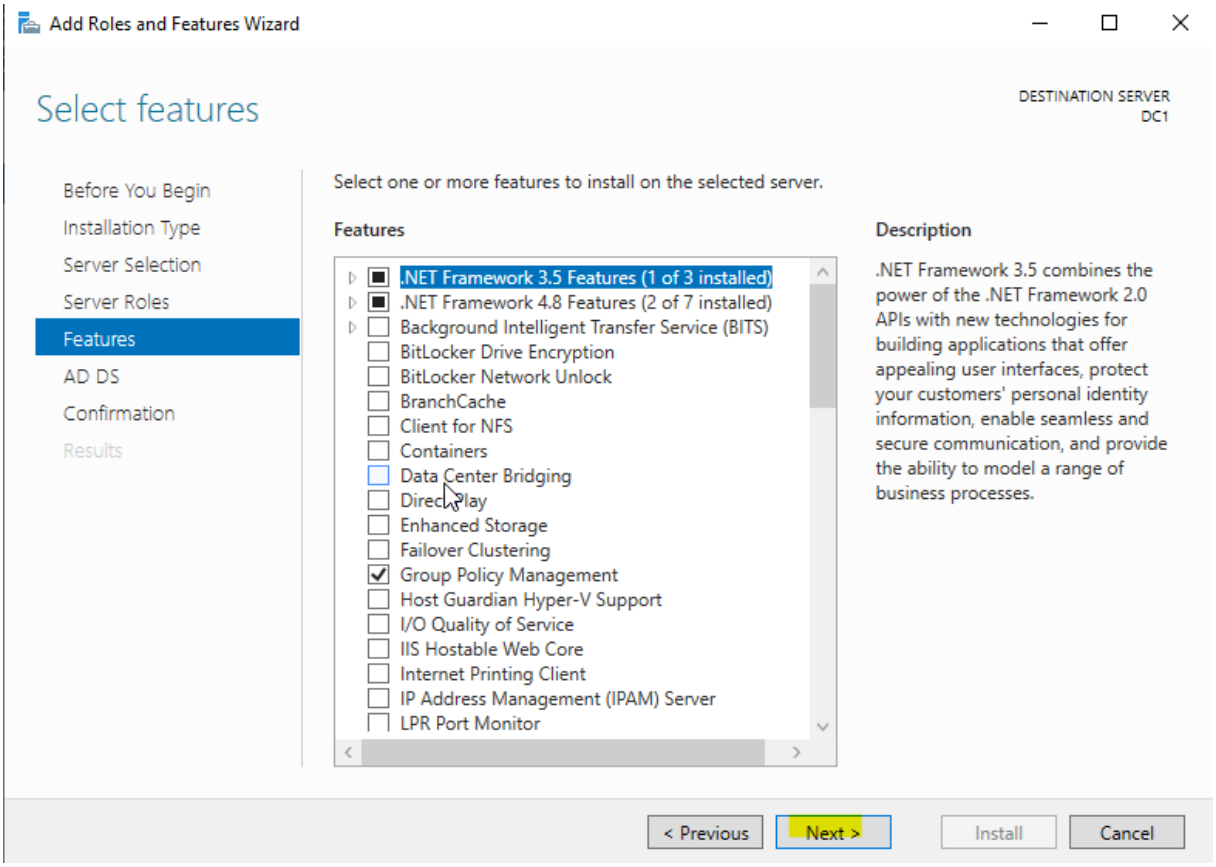
Leave the tick box ticked to Include management tools, and click Add Features.



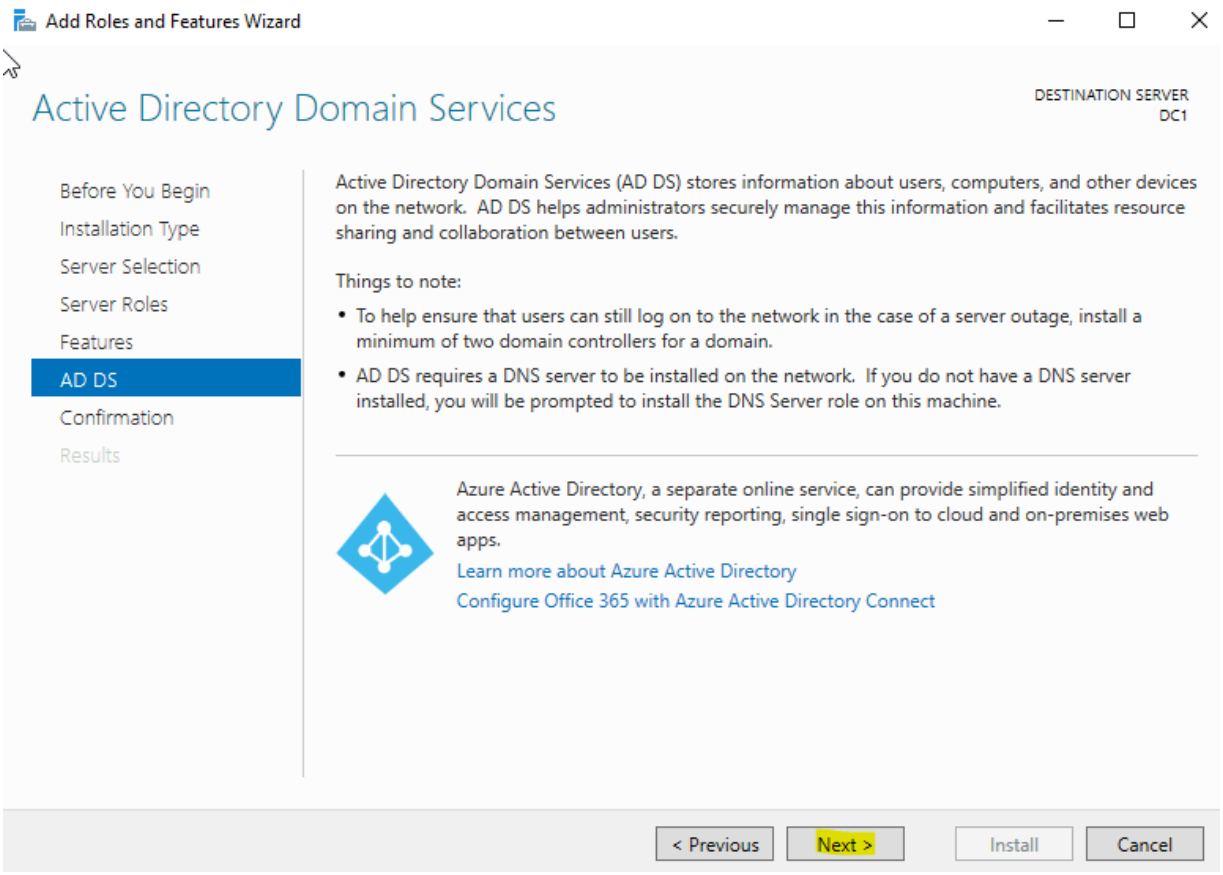
Active Directory Domain Services will now be ticked. Click Next.

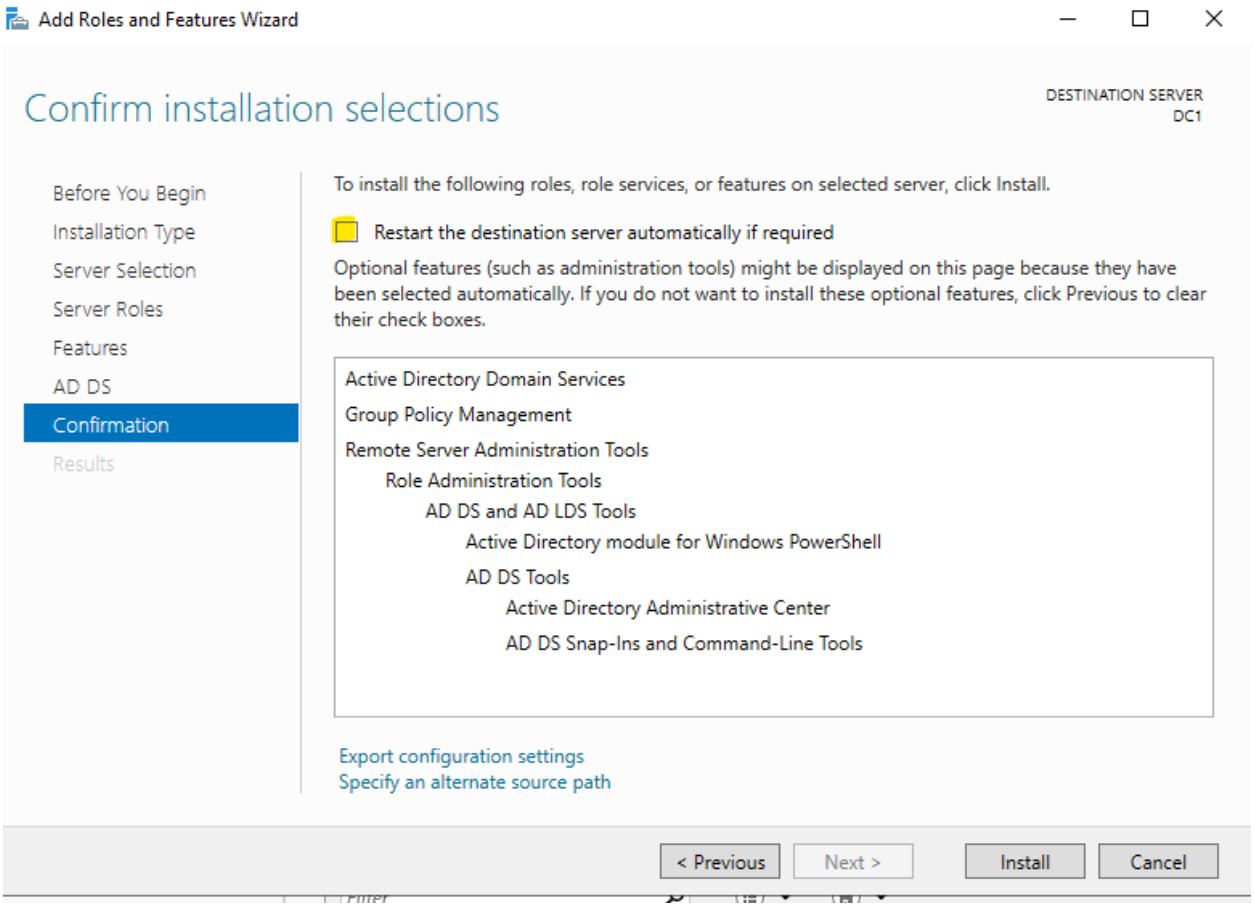


For the Features, click Next with no changes.

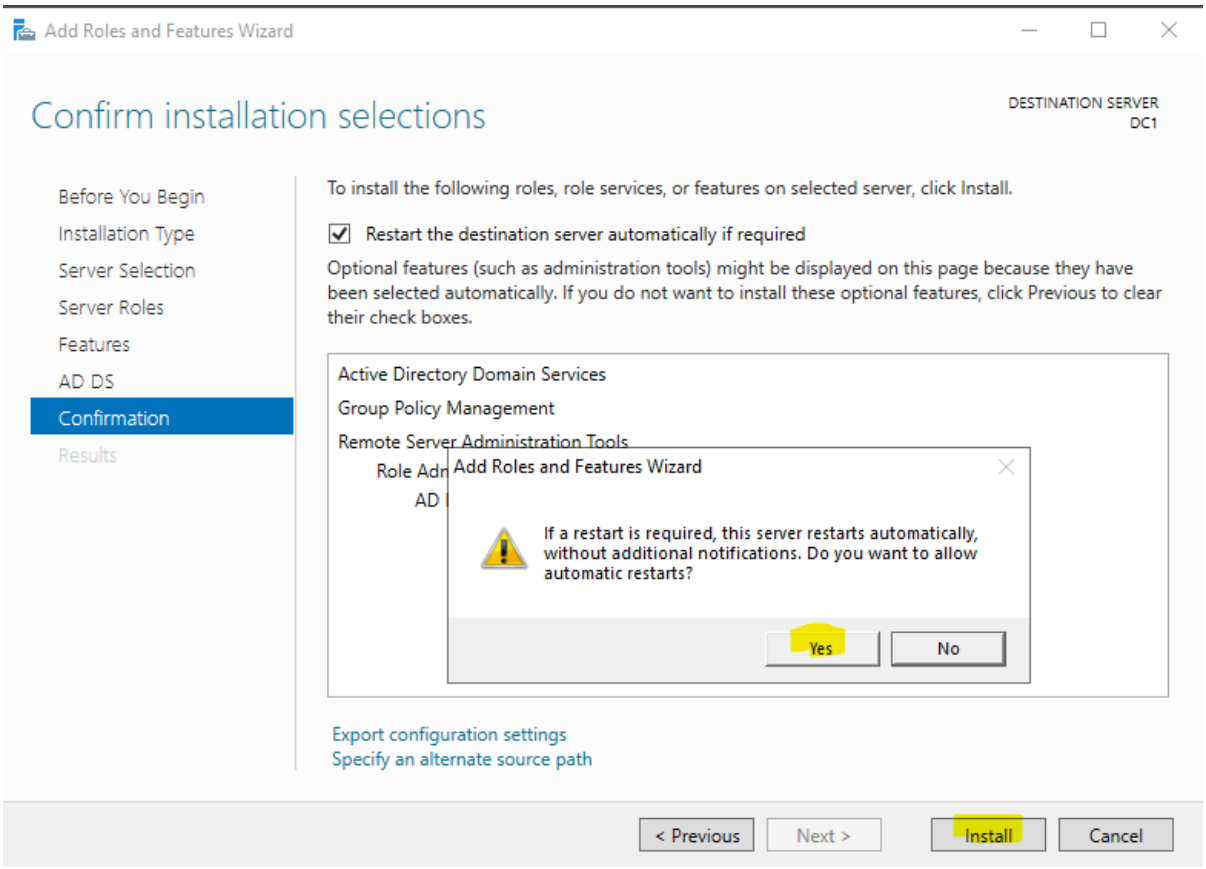


The Active Directory Domain Services will make some suggestions that are very important for production environments, namely:
Install a minimum of two domain controllers so users can log in even if there is a server outage.
A Microsoft DNS server must be set up in the network.
Click Next.


Add Roles and Features Wizard
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

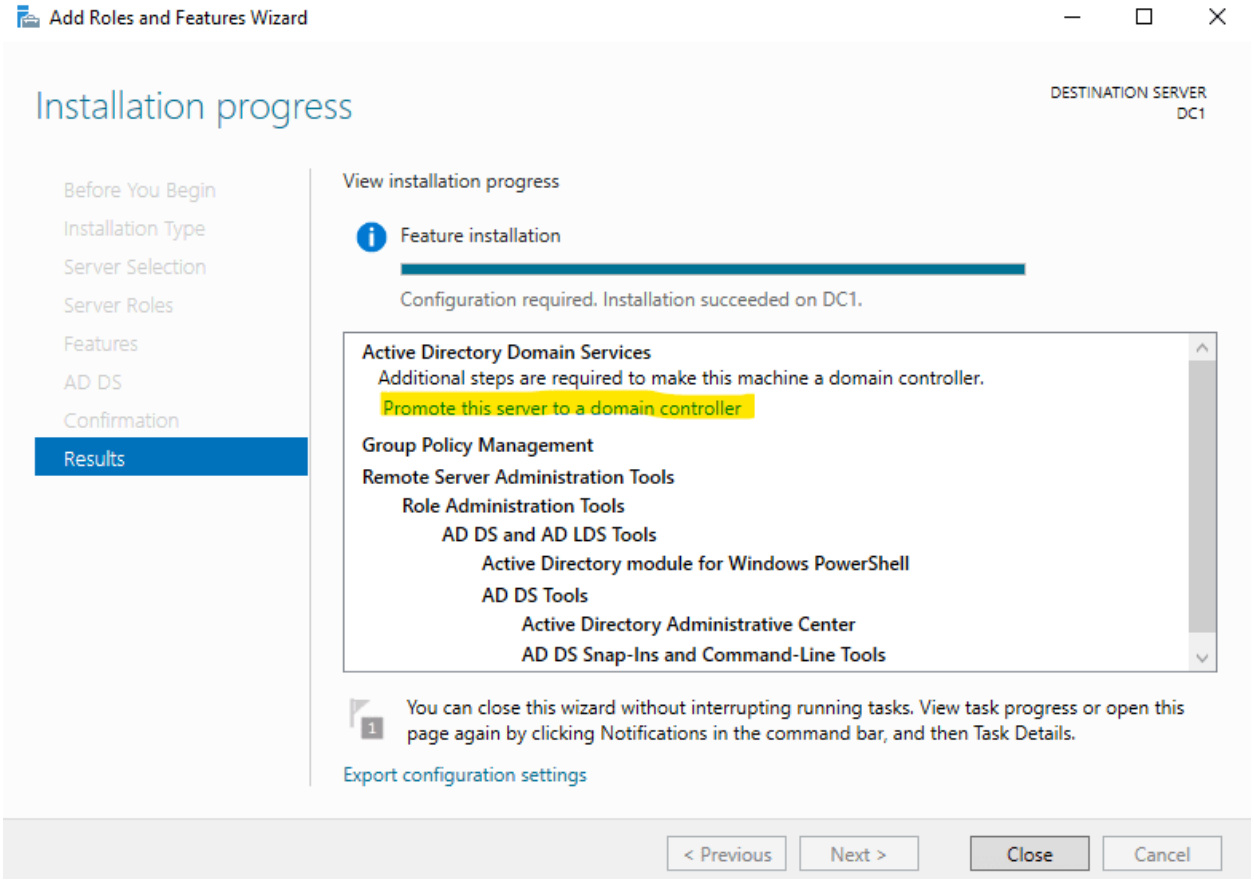


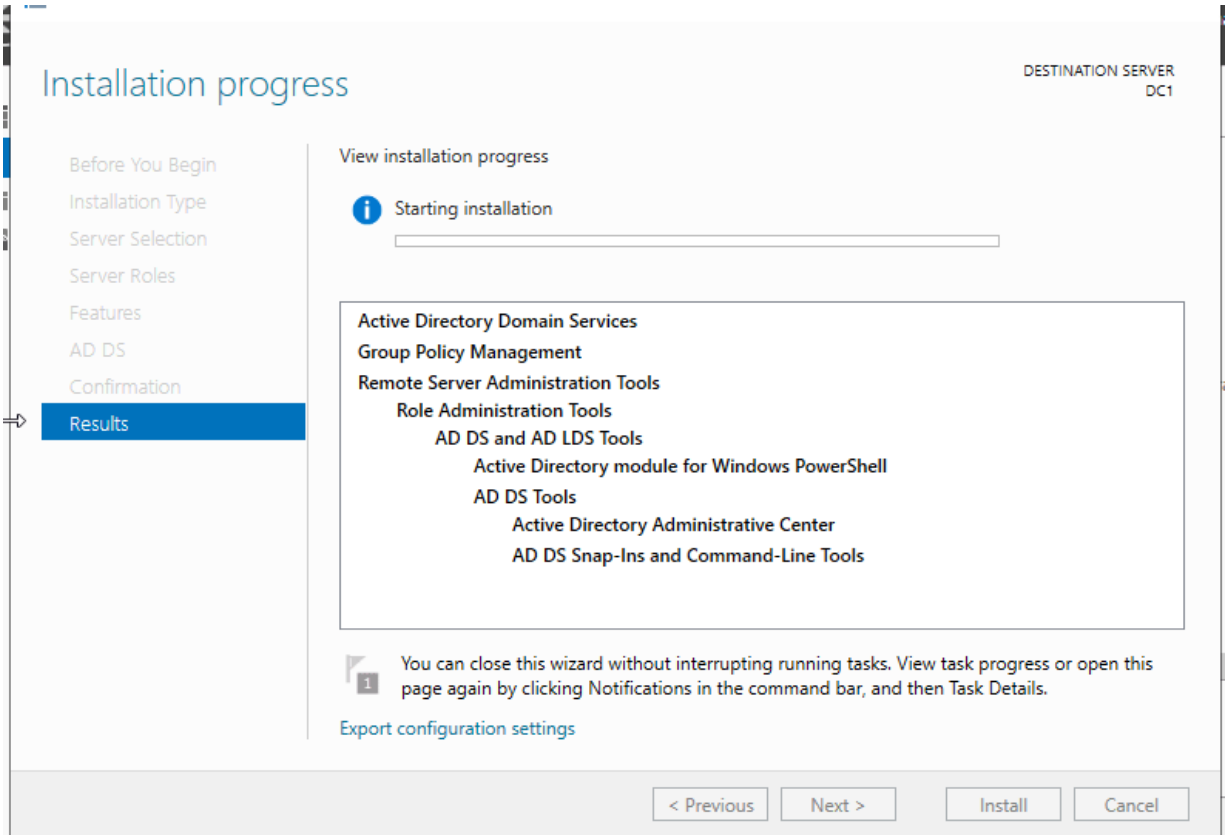
If the option to restart was selected, click Yes to allow the automatic restart.



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.

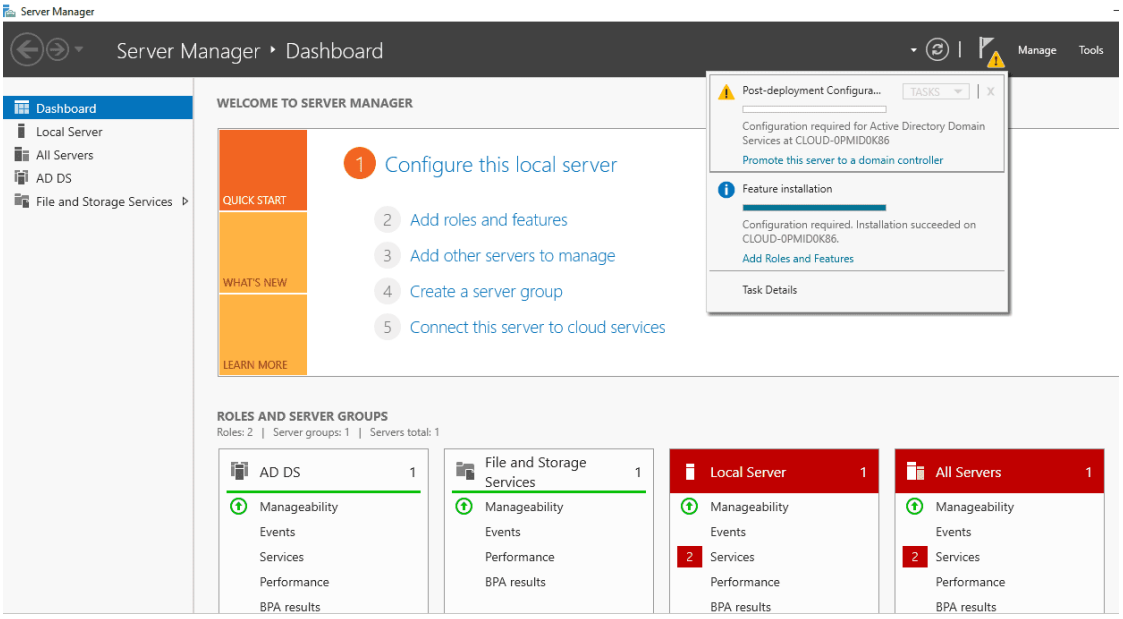




At this point, the Active Directory Domain service has been installed on your server. Now, you will need to set up it on the server.

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**"

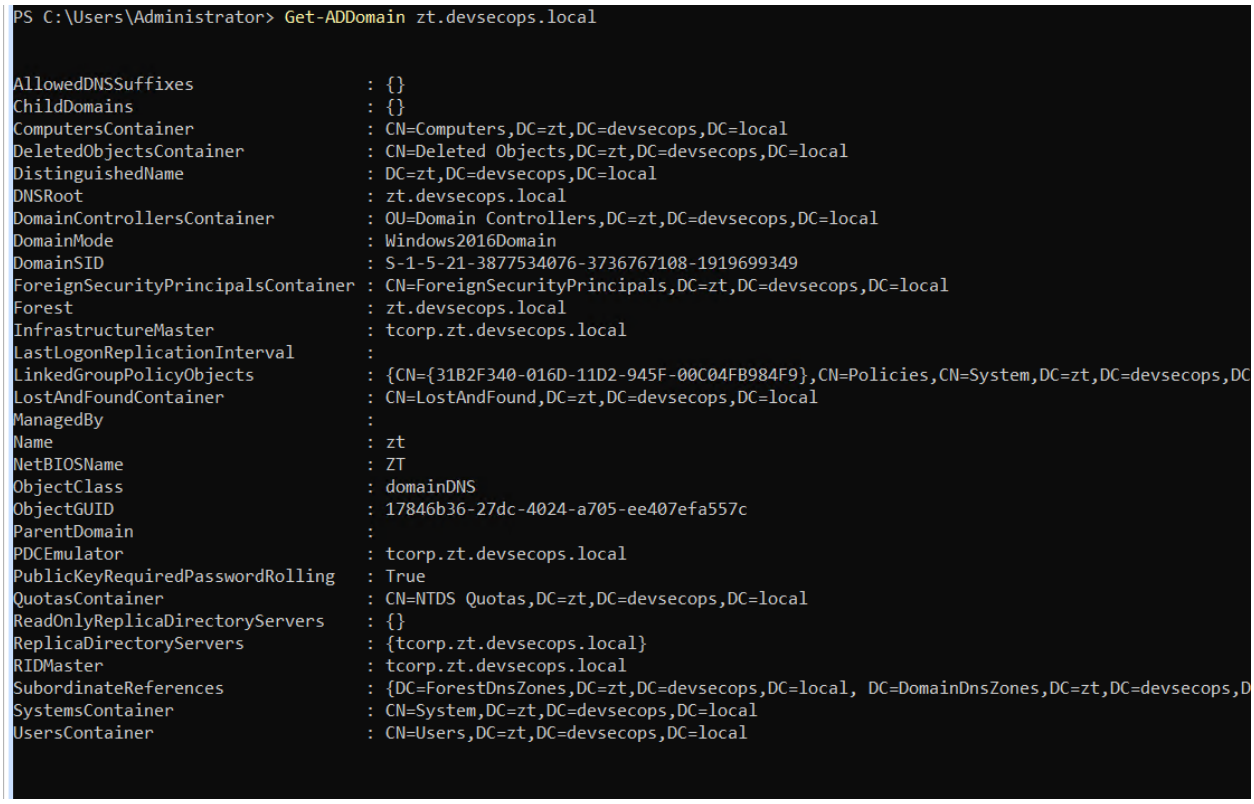
2. Confirm AD running

```
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
```

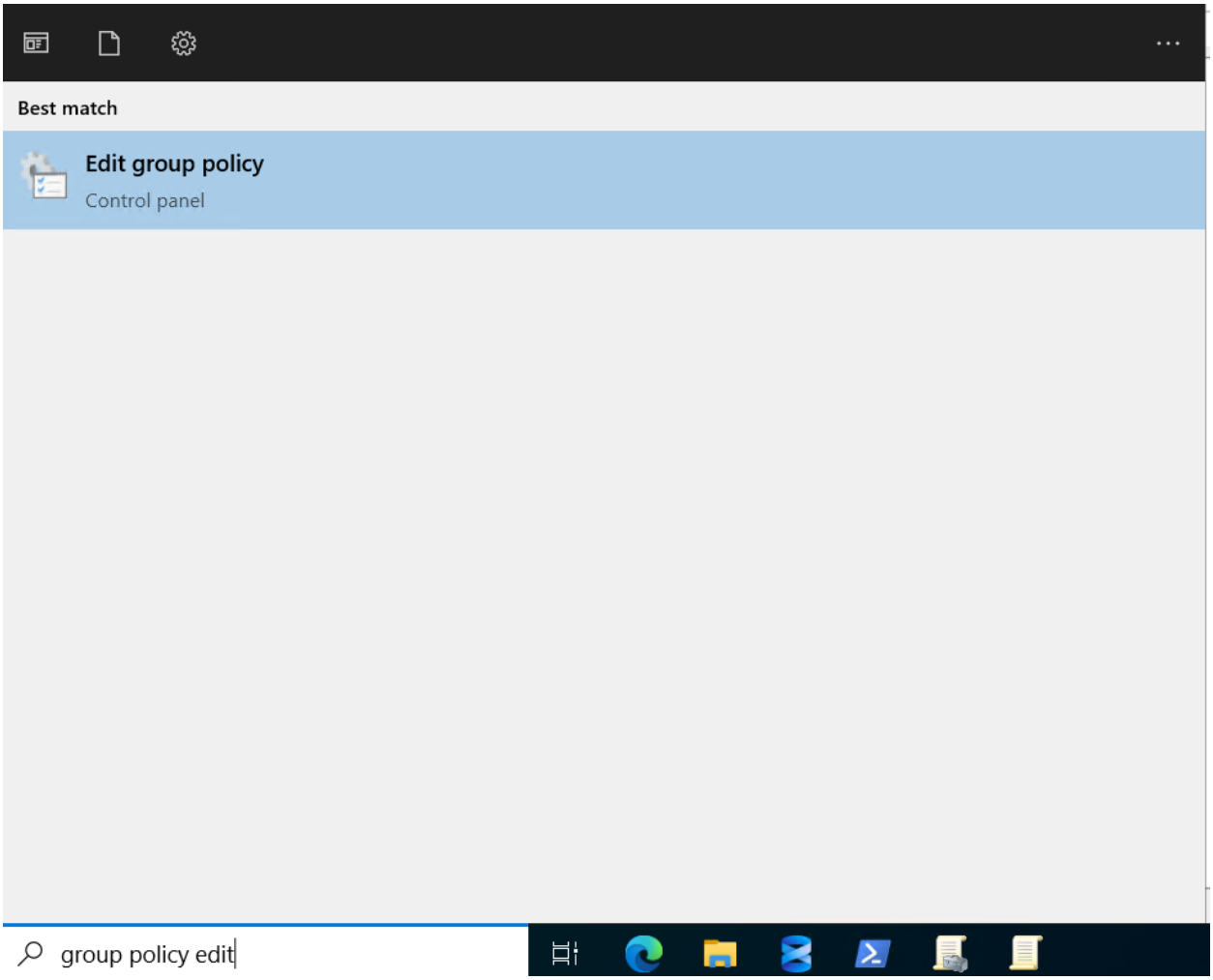
```
PS C:\Users\Administrator> Get-ADDomainController


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=Configura
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
```

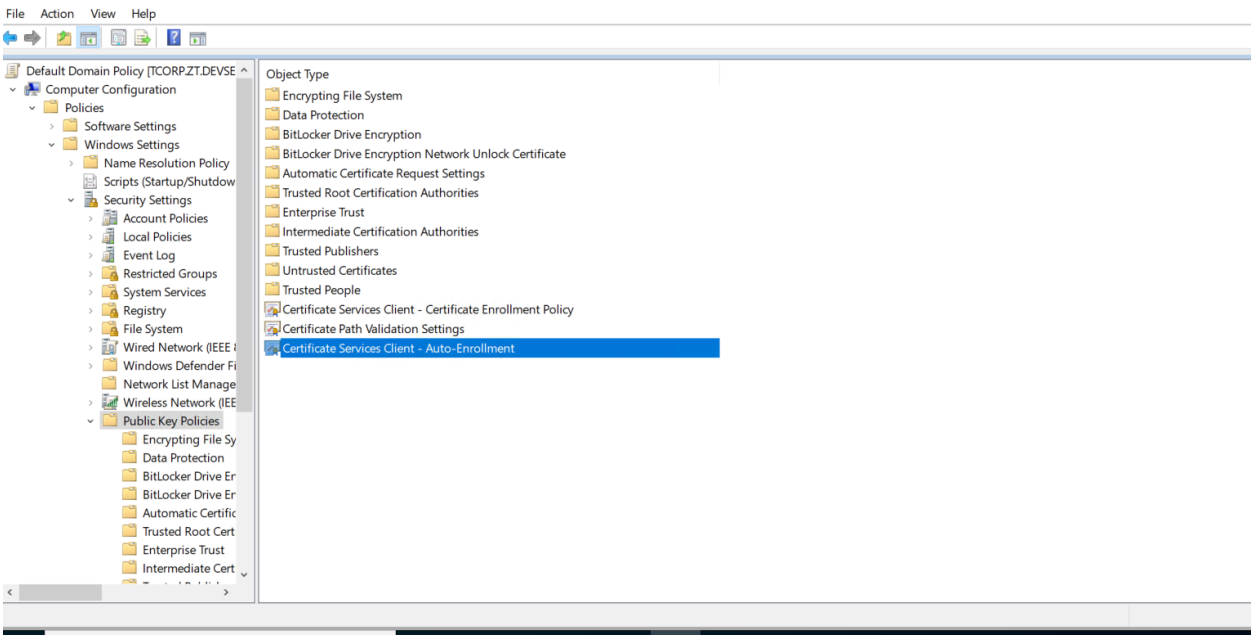


3. Cấp certificate tự động khi máy join vào domain

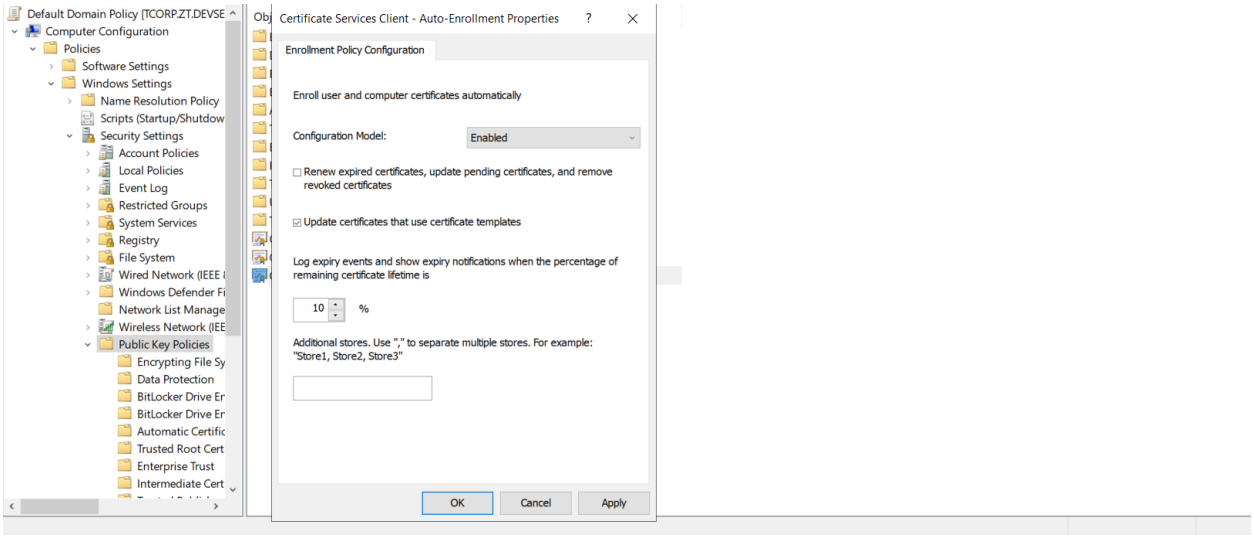
Search “Edit group policy”



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