

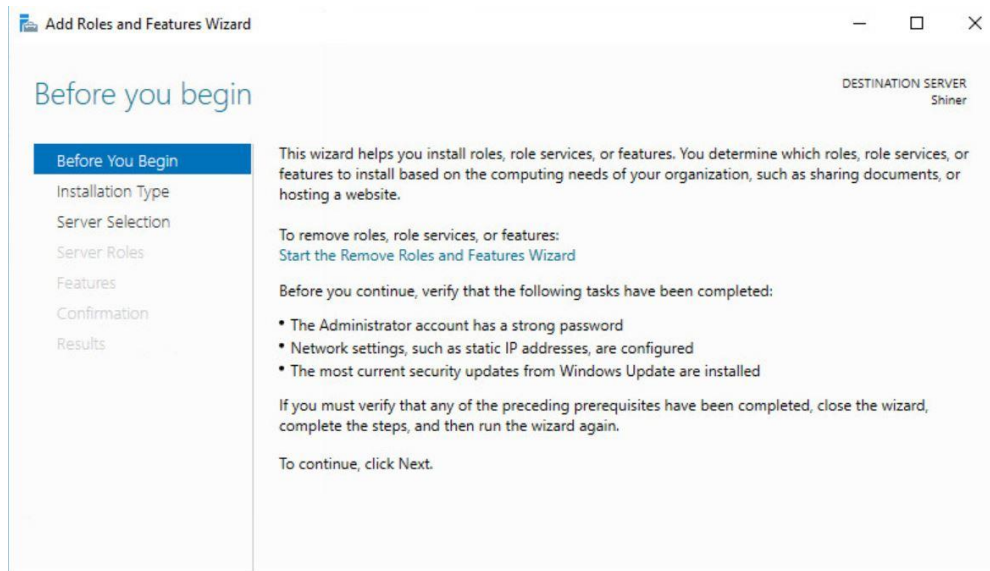
Documentation Mary Server Active Directory (LDAP Protocol)

References:

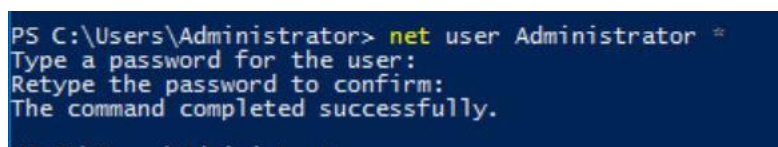
<https://blogs.msdn.microsoft.com/microsoftservertechtips/2017/04/10/step-by-step-guide-to-setup-ldap-on-windows-server/> -Setting up LDAP

Lab3 setting up Domain Controller

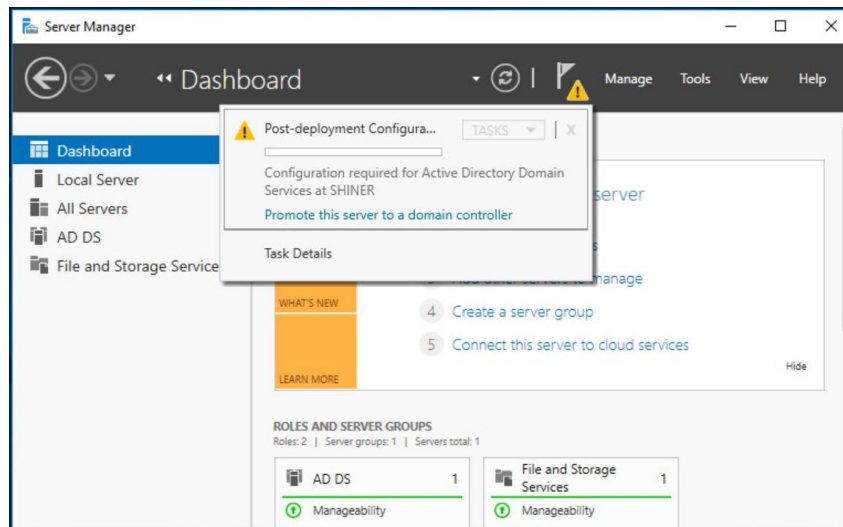
1. Went through Lab 3 in order to set up the domain controller. Installed Active Directory Domain Services.



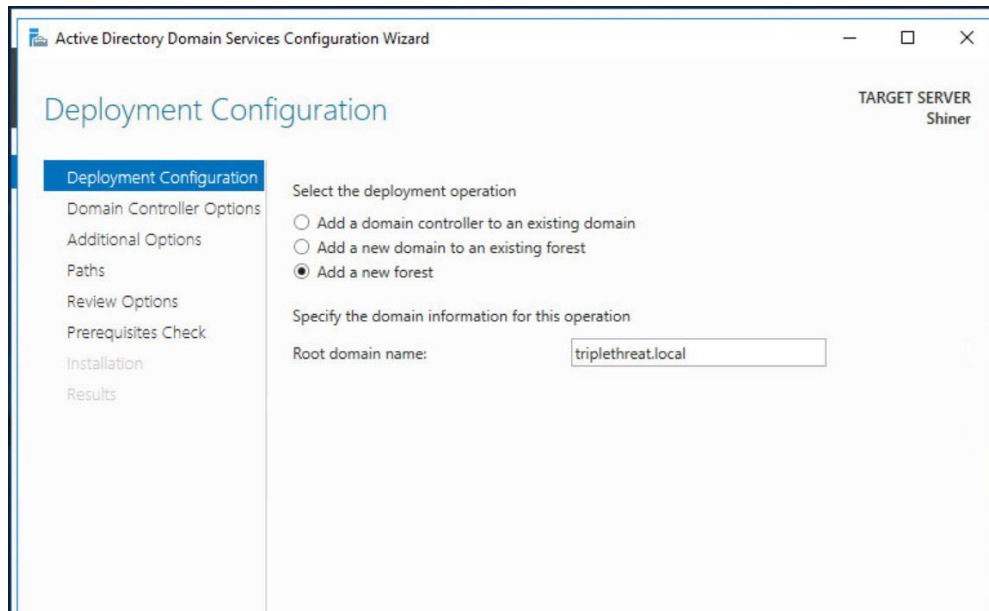
2. Opened up Powershell and set up admin password.



3. Clicked promote this server to a domain controller.

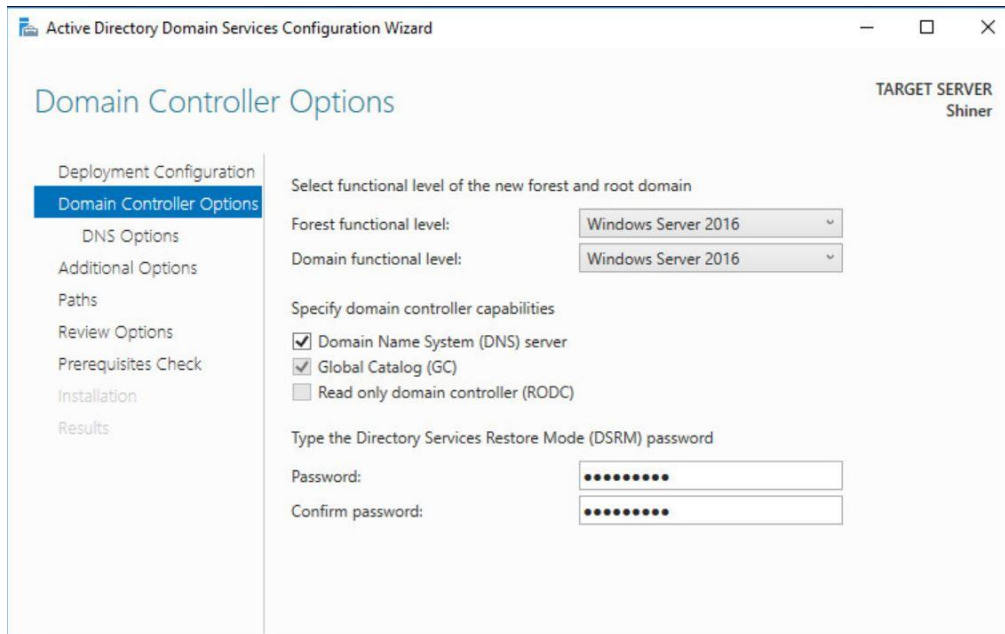


4. Created a new forest.



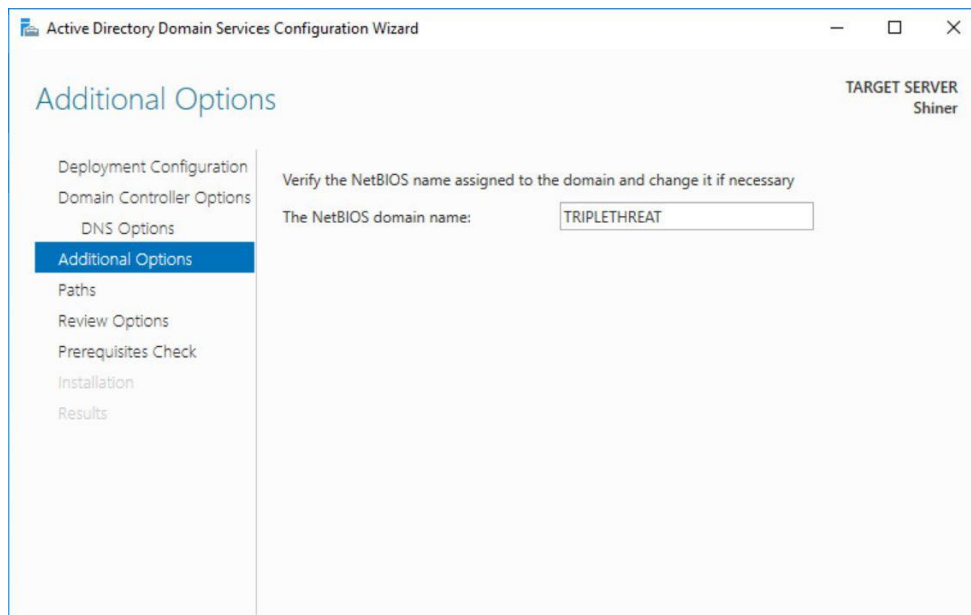
The screenshot shows the 'Active Directory Domain Services Configuration Wizard' window. The title bar includes the Windows logo, the text 'Active Directory Domain Services Configuration Wizard', and standard window controls. The main title is 'Deployment Configuration'. On the right, it says 'TARGET SERVER Shiner'. A left-hand navigation pane lists steps: 'Deployment Configuration' (highlighted), 'Domain Controller Options', 'Additional Options', 'Paths', 'Review Options', 'Prerequisites Check', 'Installation', and 'Results'. The main content area is titled 'Select the deployment operation' and contains three radio buttons: 'Add a domain controller to an existing domain', 'Add a new domain to an existing forest', and 'Add a new forest' (which is selected). Below this, it says 'Specify the domain information for this operation' and has a text box for 'Root domain name:' containing the text 'triplethreat.local'.

5. Set the recovery password for the domain services.

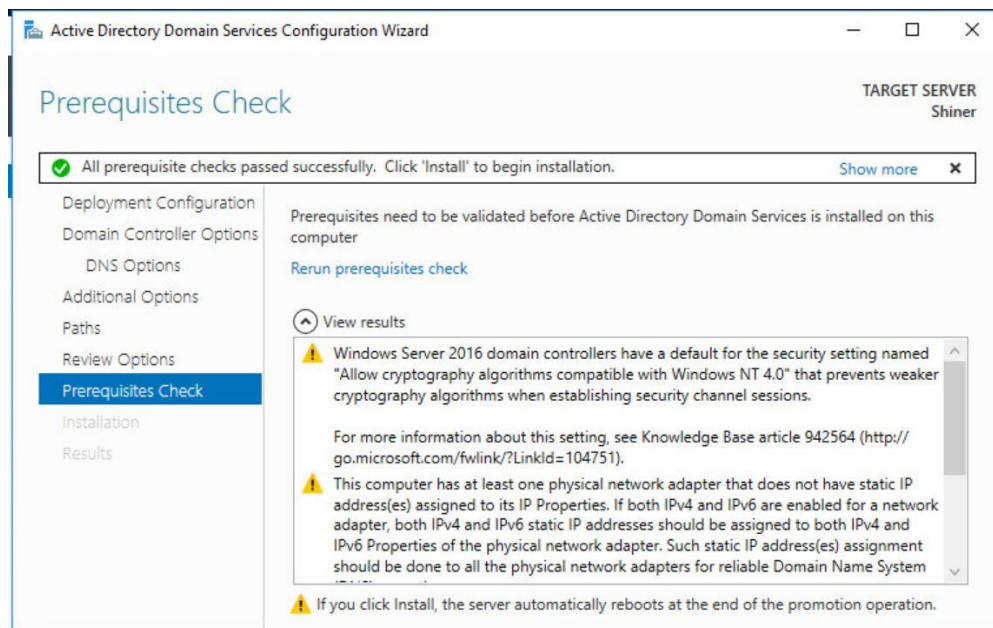


The screenshot shows the 'Active Directory Domain Services Configuration Wizard' window at the 'Domain Controller Options' step. The title bar is the same as the previous screen. The main title is 'Domain Controller Options'. The right-hand text is 'TARGET SERVER Shiner'. The left-hand navigation pane now highlights 'Domain Controller Options'. The main content area is titled 'Select functional level of the new forest and root domain' and contains two dropdown menus: 'Forest functional level:' and 'Domain functional level:', both set to 'Windows Server 2016'. Below this, it says 'Specify domain controller capabilities' and contains three checkboxes: 'Domain Name System (DNS) server' (checked), 'Global Catalog (GC)' (checked), and 'Read only domain controller (RODC)' (unchecked). At the bottom, it says 'Type the Directory Services Restore Mode (DSRM) password' and has two password fields: 'Password:' and 'Confirm password:', both masked with dots.

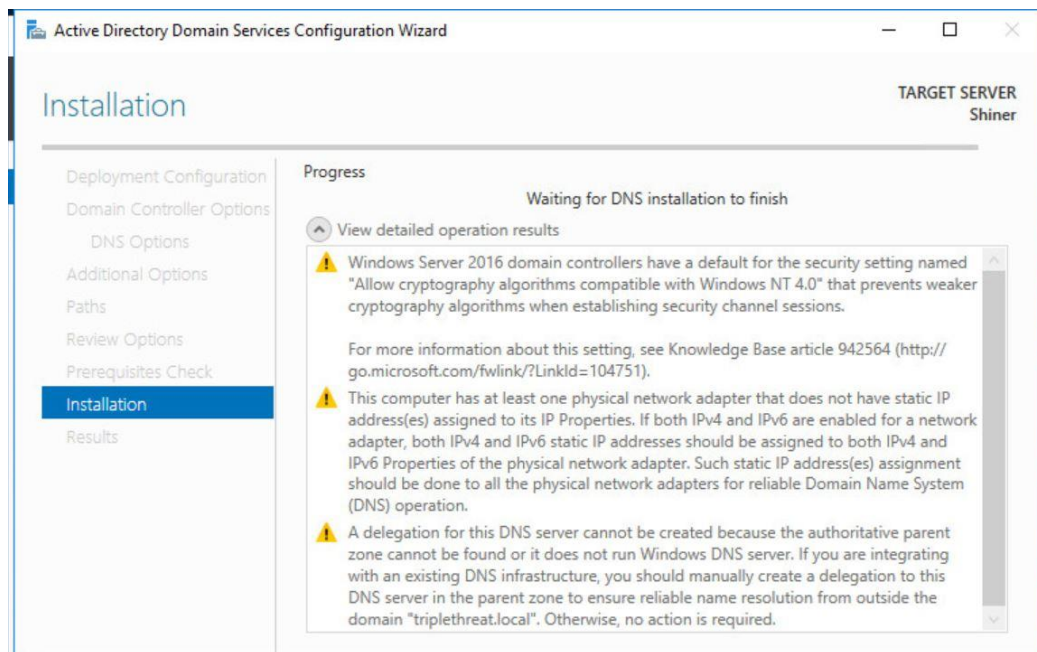
6. Set up the NetBIOS domain name.



7. Checked prerequisites.



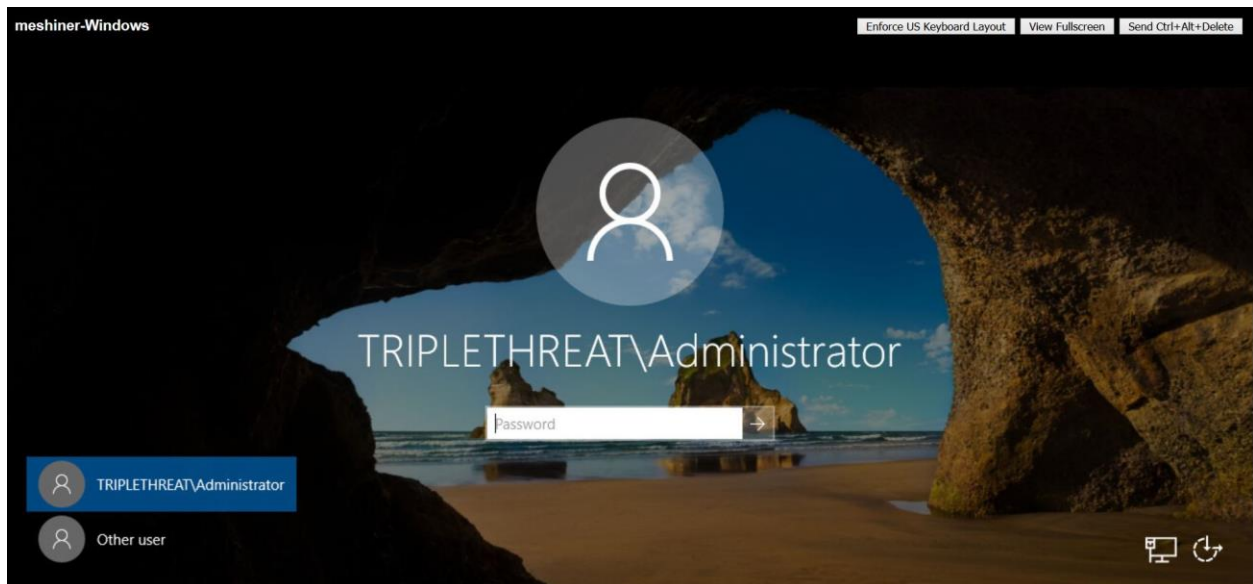
8. Active Directory is being installed.



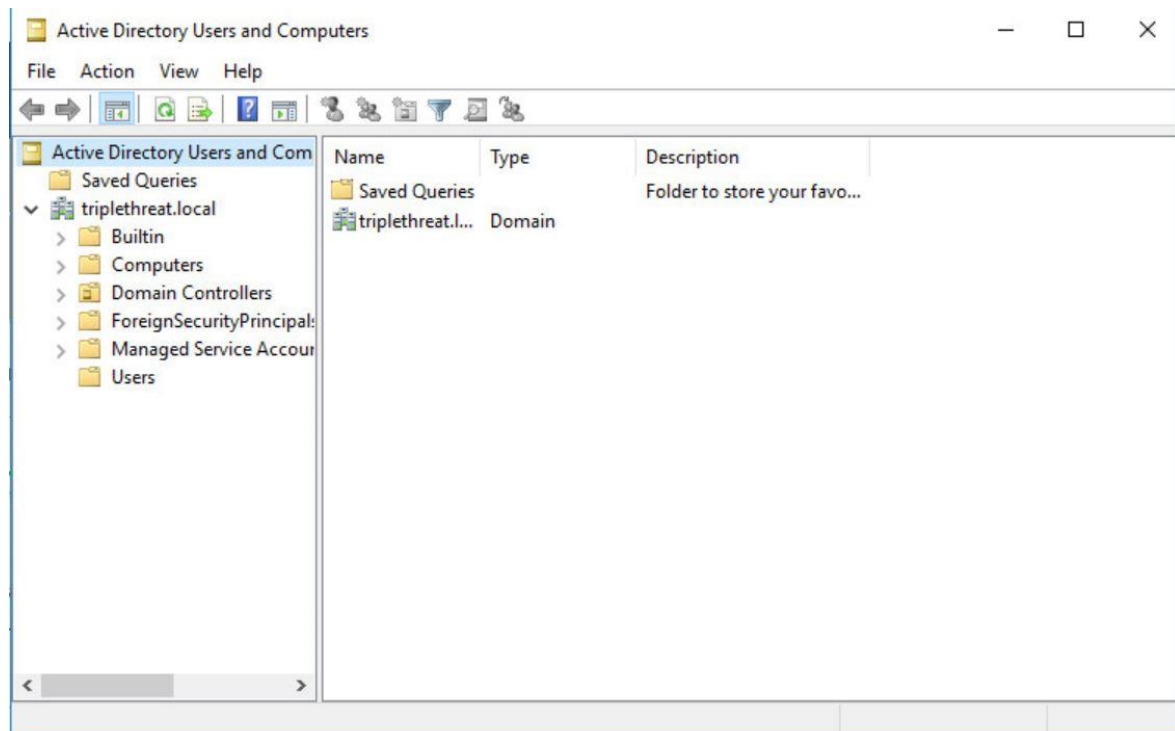
9. VM is restarted.



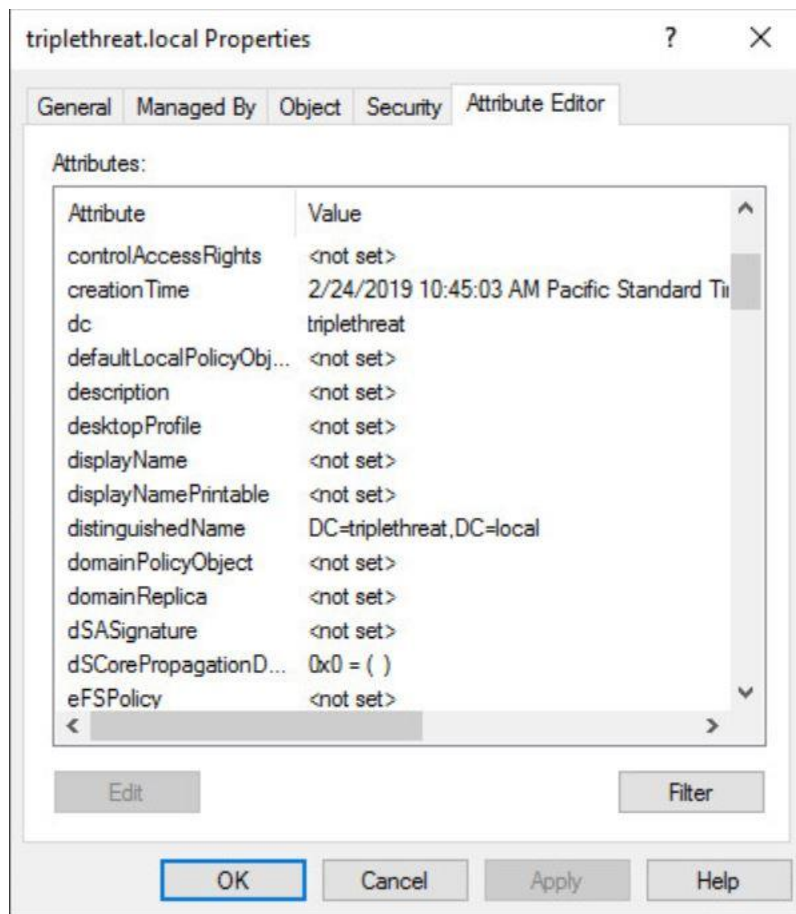
10. Login to new admin account.



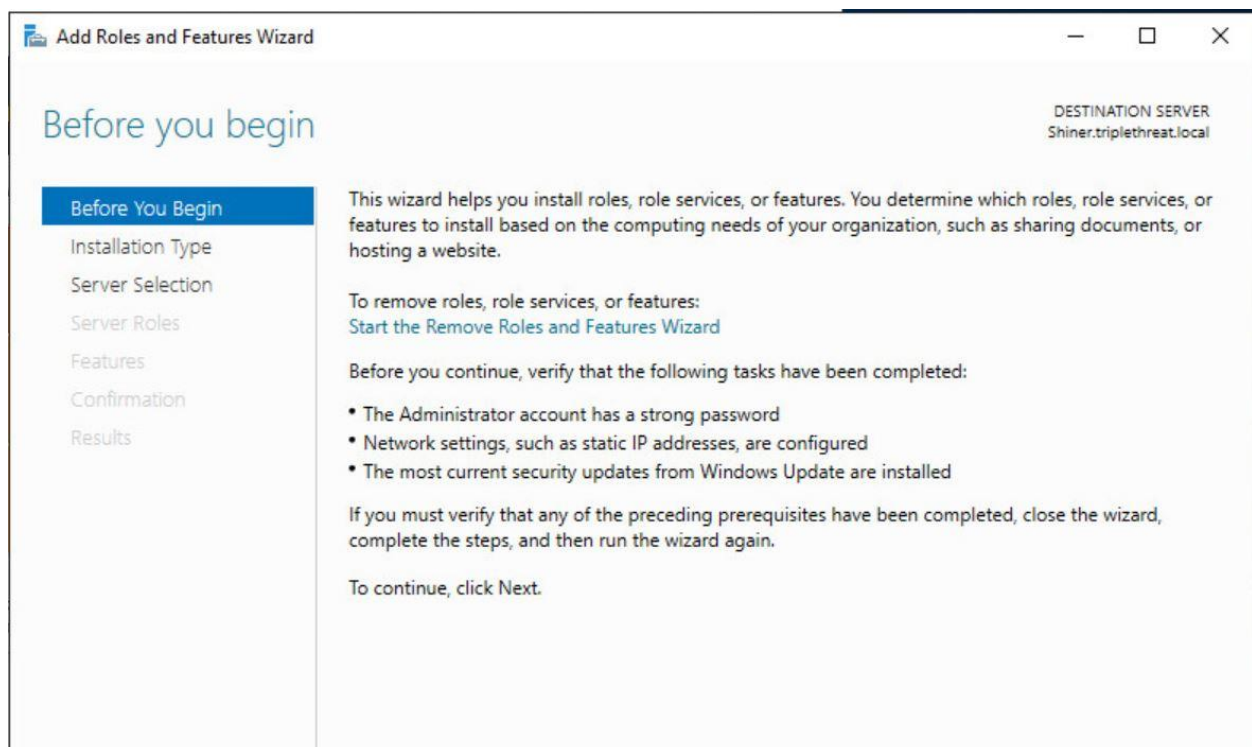
11. Active directory is now installed and shows our forest.



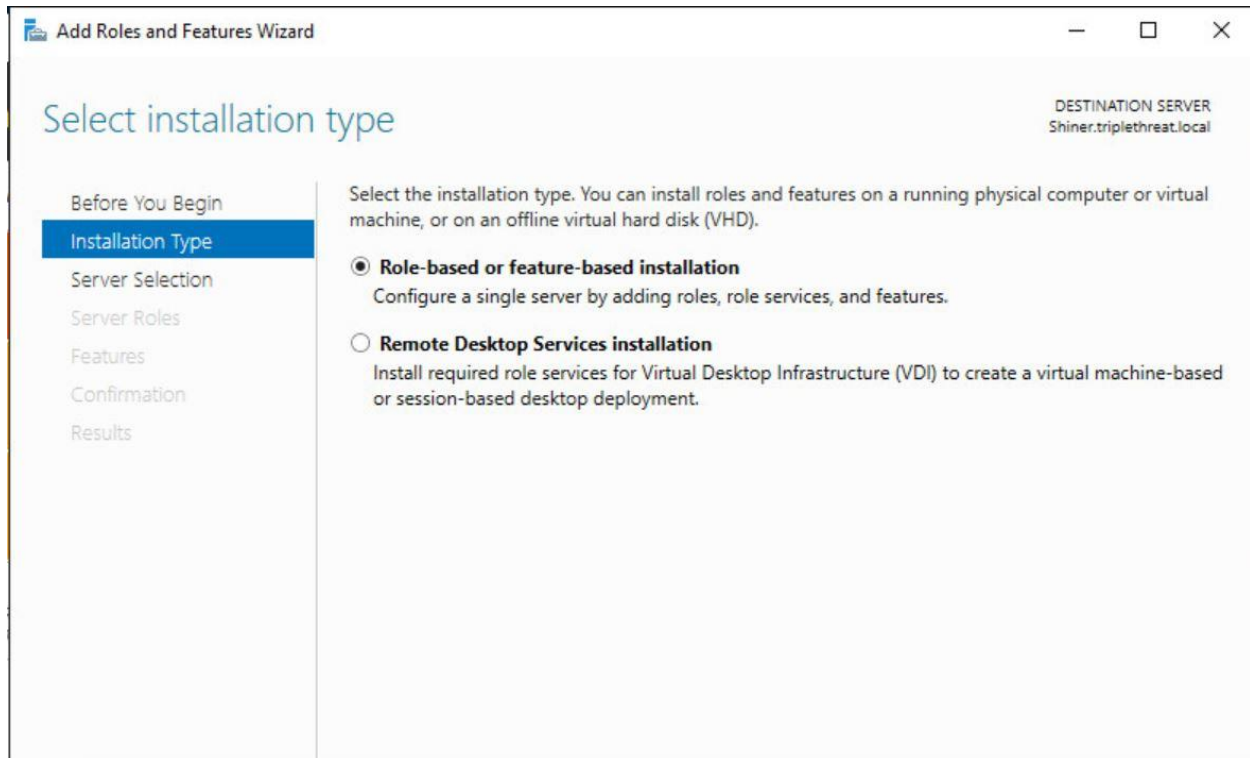
12. Here is our forest properties.



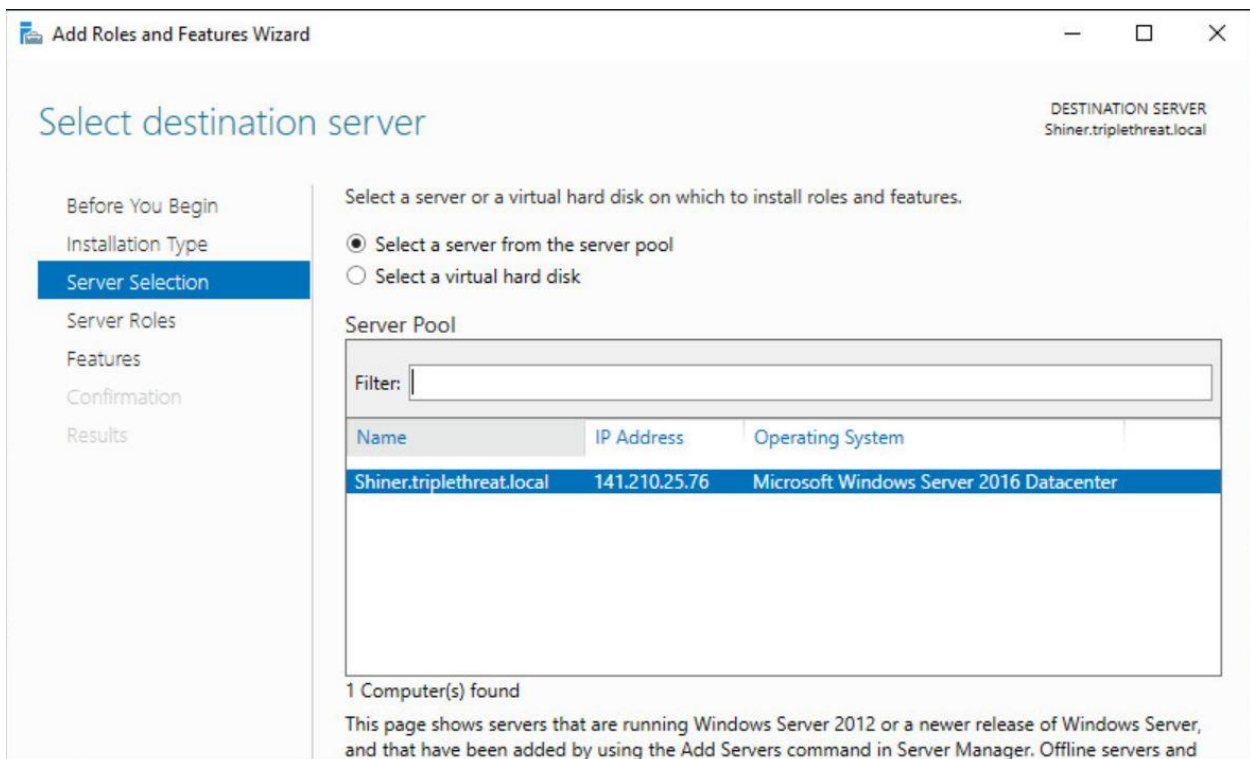
13. We are now going to install LDAP using AD LDS (Active Directory Lightweight Directory Services)



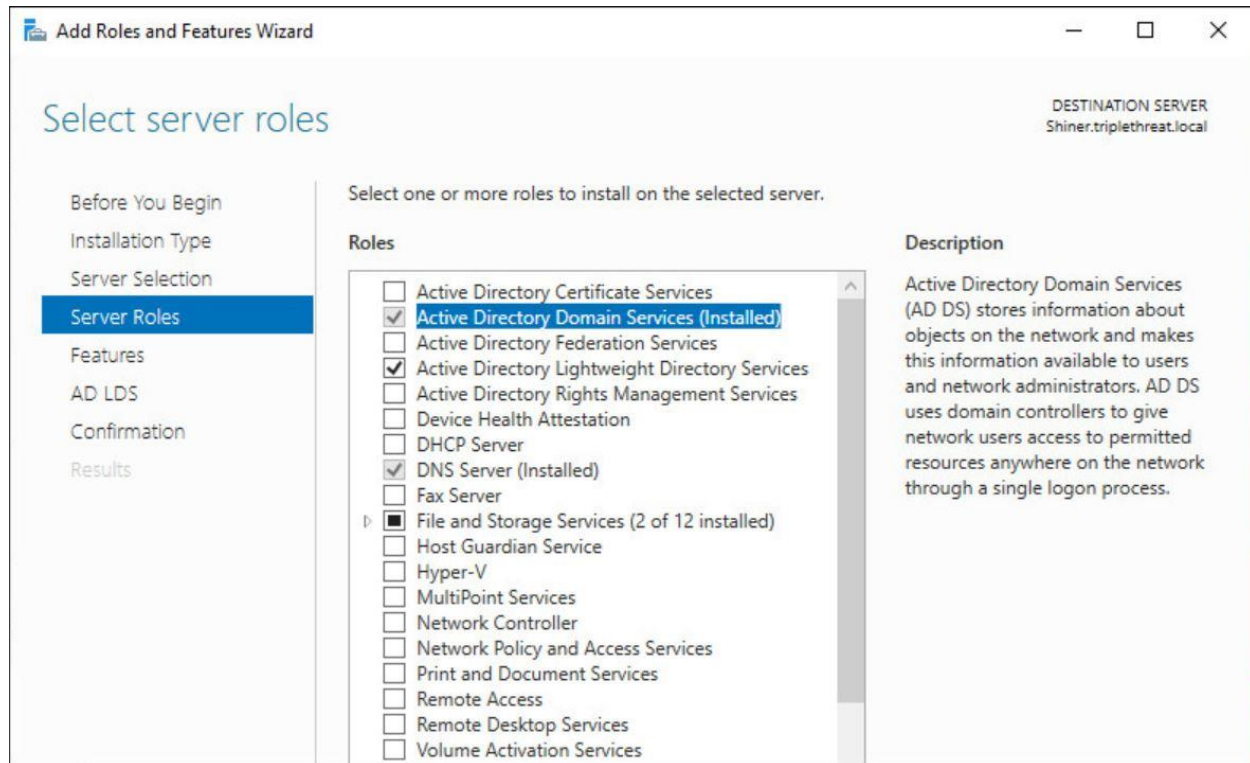
14. We choose Role-based installation.



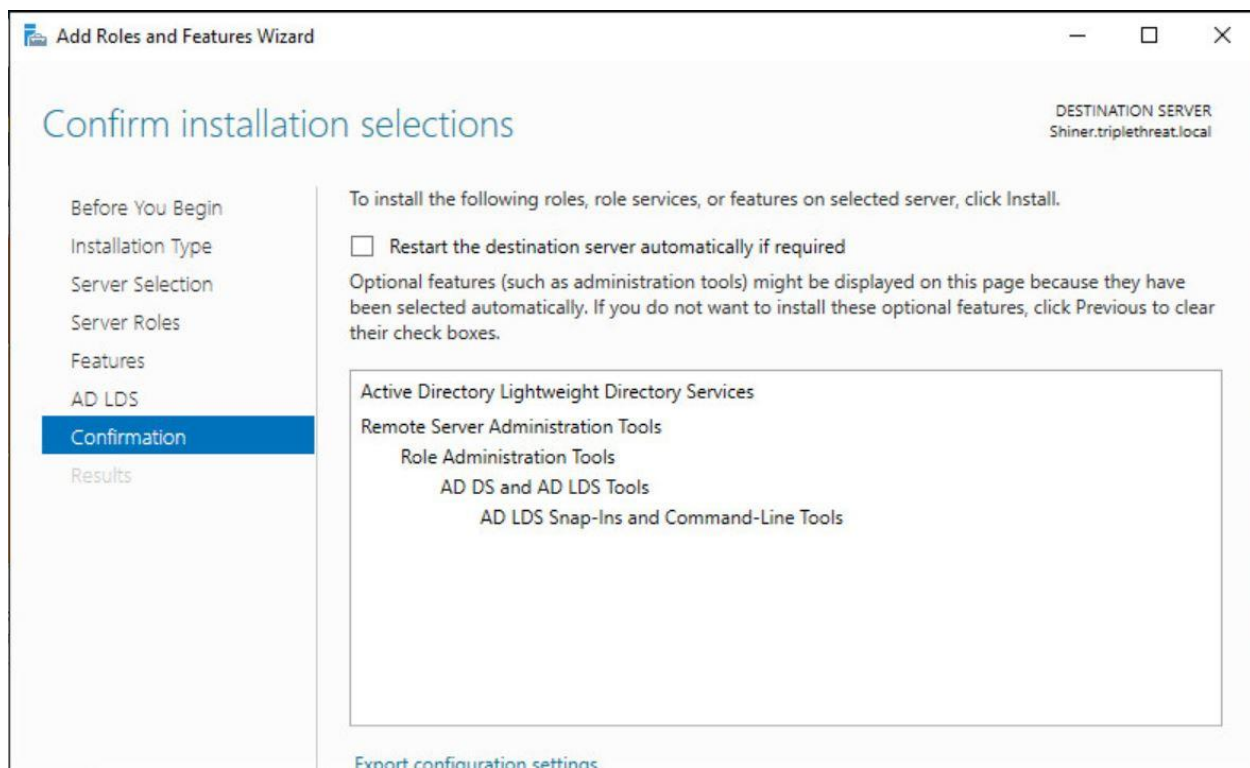
15. We select a server from the server pool.



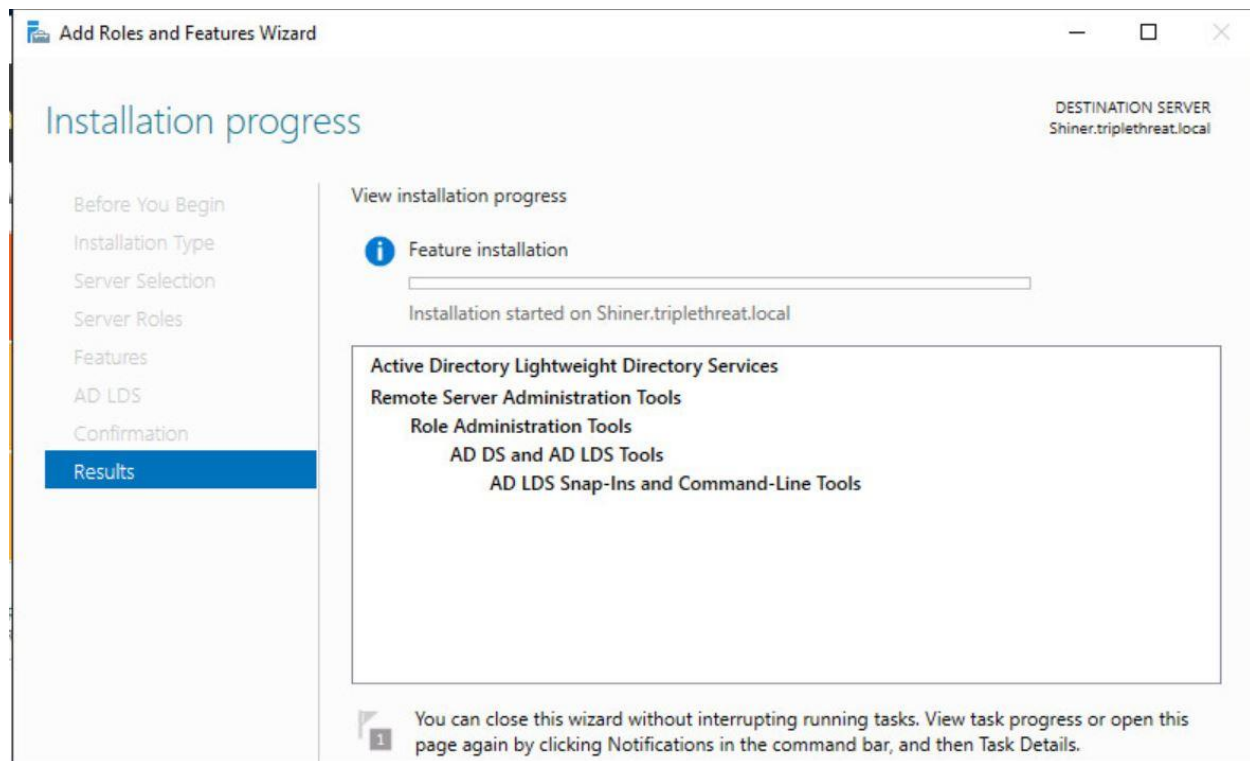
16. We select Active Directory Lightweight Directory Services.



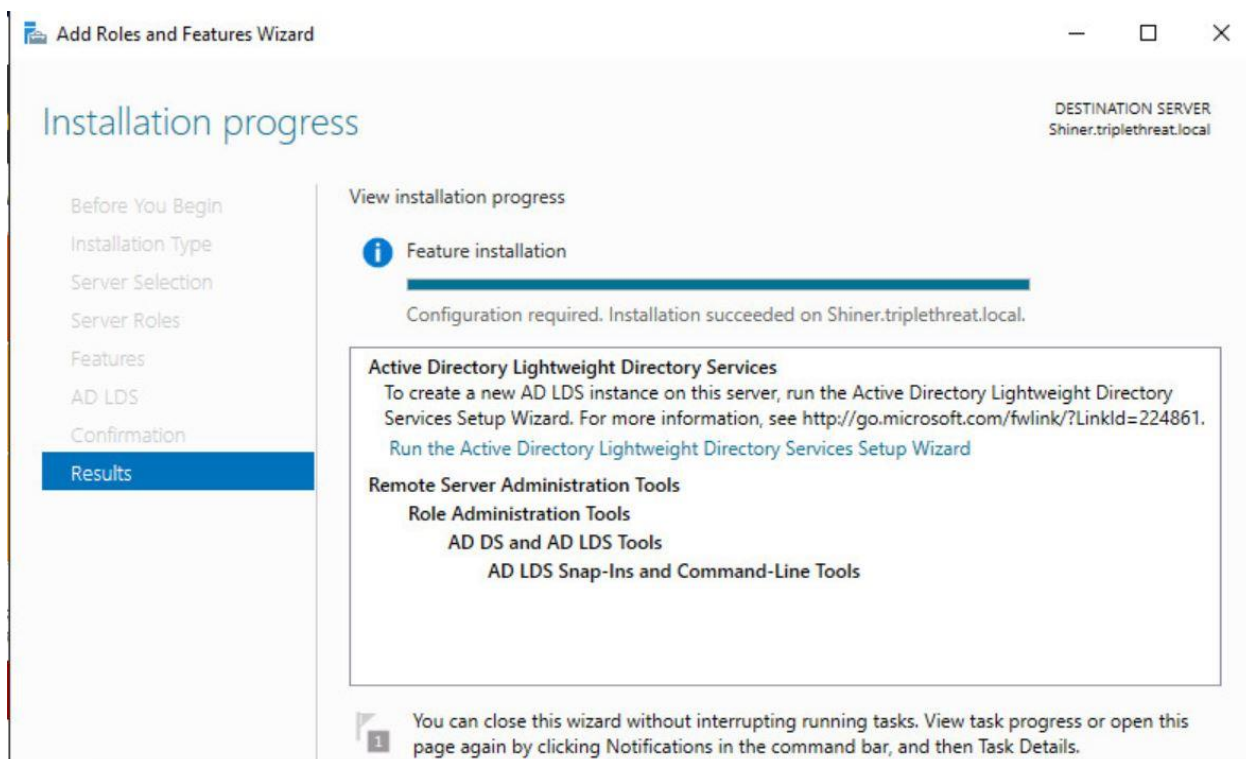
17. We then check our roles, role service and features and then install.



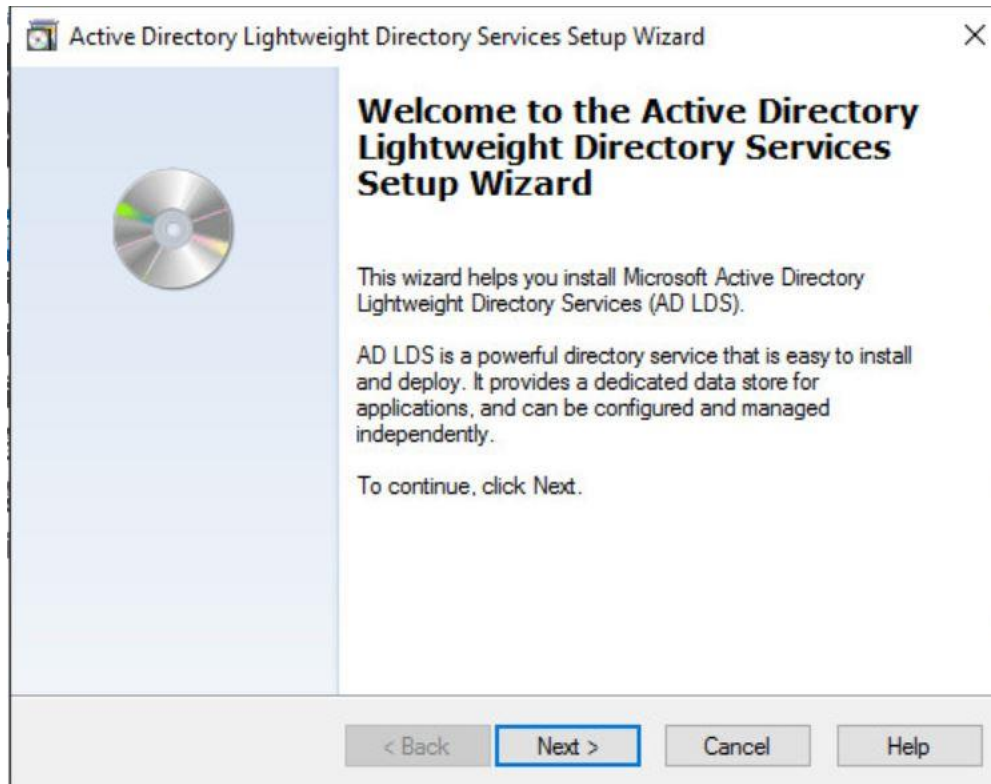
18. It is now installing.



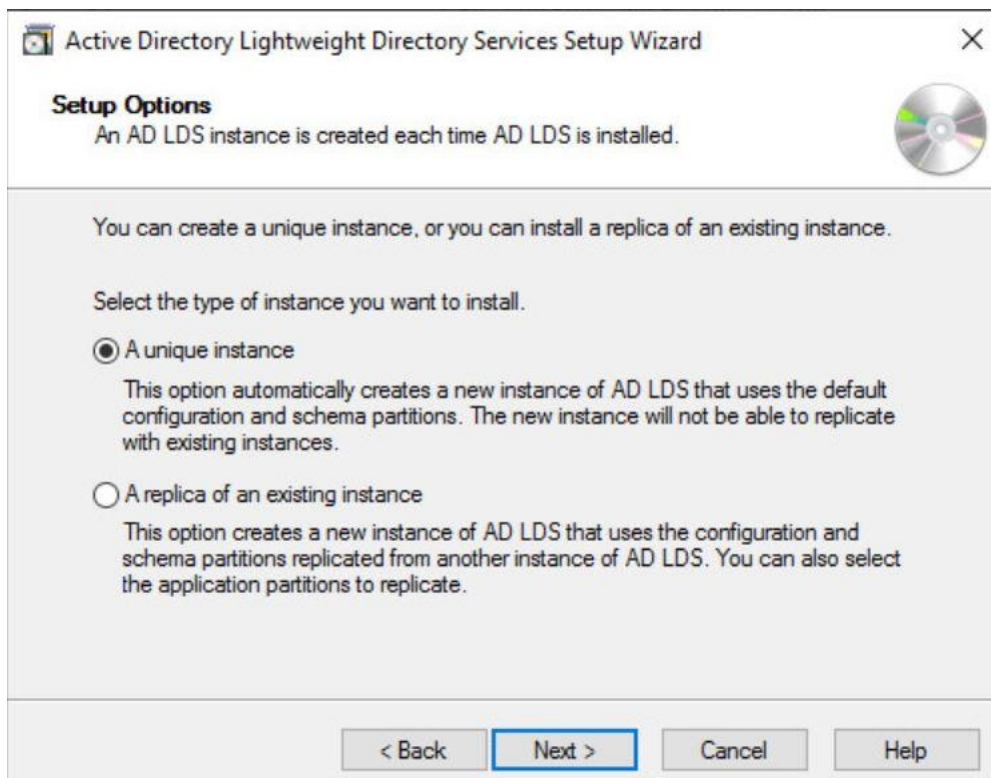
19. Installation of AD LDS Role complete.



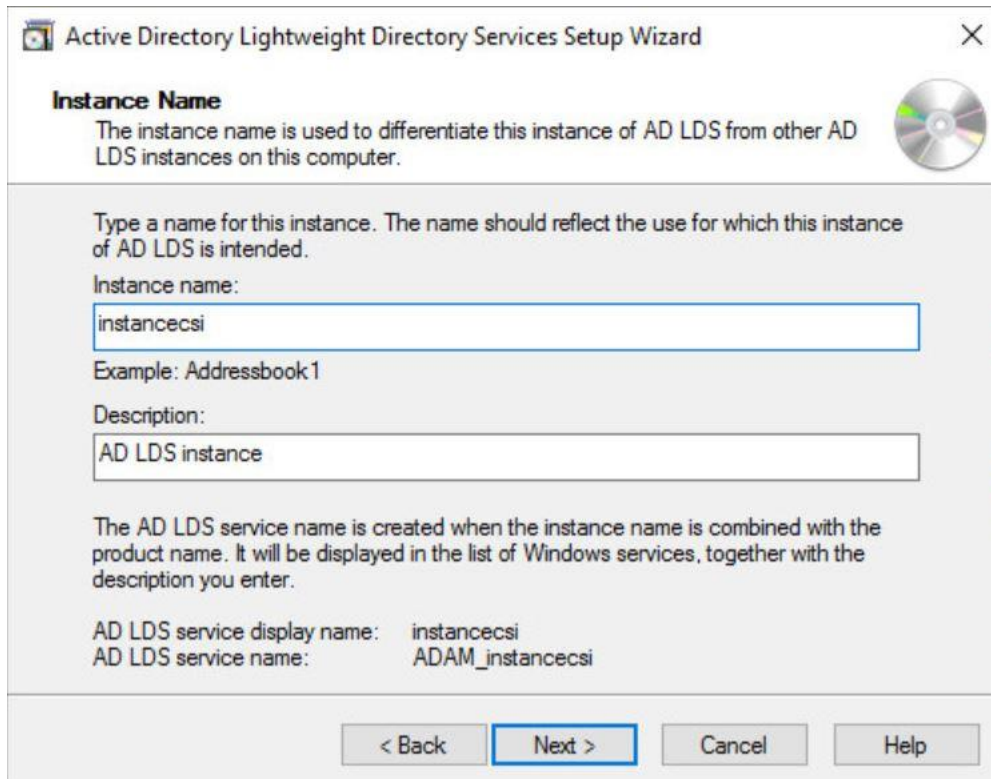
20. Now we are going to create a AD LDS Instance.



21. We choose to set up a unique instance.



22. We name our instance.



The screenshot shows the 'Instance Name' step of the Active Directory Lightweight Directory Services Setup Wizard. The window title is 'Active Directory Lightweight Directory Services Setup Wizard'. The section header is 'Instance Name'. Below it, a text box explains: 'The instance name is used to differentiate this instance of AD LDS from other AD LDS instances on this computer.' To the right of this text is a CD icon. The main instruction says: 'Type a name for this instance. The name should reflect the use for which this instance of AD LDS is intended.' There are two text input fields: 'Instance name:' with the value 'instancecsi' and 'Description:' with the value 'AD LDS instance'. Below these fields, an example is given: 'Example: Addressbook1'. Further down, a paragraph explains: 'The AD LDS service name is created when the instance name is combined with the product name. It will be displayed in the list of Windows services, together with the description you enter.' Below this, two lines of text show the resulting names: 'AD LDS service display name: instancecsi' and 'AD LDS service name: ADAM_instancecsi'. At the bottom, there are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'. The 'Next >' button is highlighted with a blue border.

Instance Name

The instance name is used to differentiate this instance of AD LDS from other AD LDS instances on this computer.

Type a name for this instance. The name should reflect the use for which this instance of AD LDS is intended.

Instance name:
instancecsi

Example: Addressbook1

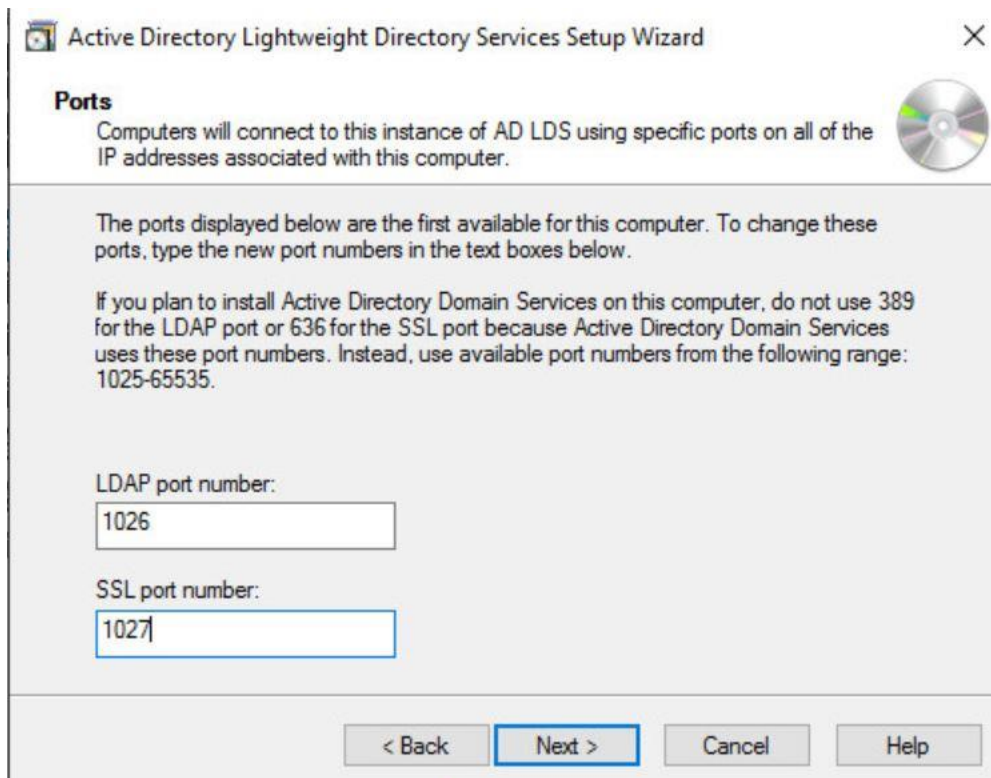
Description:
AD LDS instance

The AD LDS service name is created when the instance name is combined with the product name. It will be displayed in the list of Windows services, together with the description you enter.

AD LDS service display name: instancecsi
AD LDS service name: ADAM_instancecsi

< Back Next > Cancel Help

23. We choose our port numbers.



The screenshot shows the 'Ports' step of the Active Directory Lightweight Directory Services Setup Wizard. The window title is 'Active Directory Lightweight Directory Services Setup Wizard'. The section header is 'Ports'. Below it, a text box explains: 'Computers will connect to this instance of AD LDS using specific ports on all of the IP addresses associated with this computer.' To the right of this text is a CD icon. The main instruction says: 'The ports displayed below are the first available for this computer. To change these ports, type the new port numbers in the text boxes below.' Below this, a paragraph provides a warning: 'If you plan to install Active Directory Domain Services on this computer, do not use 389 for the LDAP port or 636 for the SSL port because Active Directory Domain Services uses these port numbers. Instead, use available port numbers from the following range: 1025-65535.' There are two text input fields: 'LDAP port number:' with the value '1026' and 'SSL port number:' with the value '1027'. At the bottom, there are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'. The 'Next >' button is highlighted with a blue border.

Ports

Computers will connect to this instance of AD LDS using specific ports on all of the IP addresses associated with this computer.

The ports displayed below are the first available for this computer. To change these ports, type the new port numbers in the text boxes below.

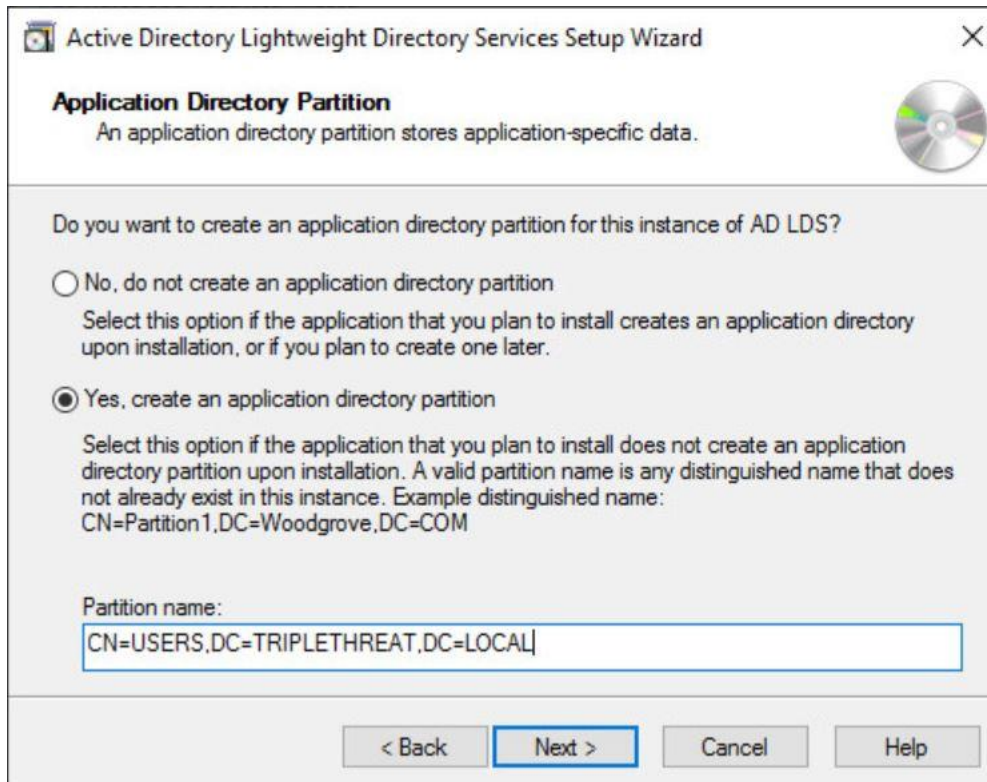
If you plan to install Active Directory Domain Services on this computer, do not use 389 for the LDAP port or 636 for the SSL port because Active Directory Domain Services uses these port numbers. Instead, use available port numbers from the following range: 1025-65535.

LDAP port number:
1026

SSL port number:
1027

< Back Next > Cancel Help

24. We create and name a new Application Directory Partition.



The screenshot shows the 'Application Directory Partition' step of the 'Active Directory Lightweight Directory Services Setup Wizard'. The window title is 'Active Directory Lightweight Directory Services Setup Wizard'. The subtitle is 'Application Directory Partition' with a description: 'An application directory partition stores application-specific data.' There is a CD icon in the top right corner. The main question is 'Do you want to create an application directory partition for this instance of AD LDS?'. There are two radio button options: 'No, do not create an application directory partition' and 'Yes, create an application directory partition'. The 'Yes' option is selected. Below the options, there is a text box for 'Partition name:' containing the text 'CN=USERS,DC=TRIPLETHREAT,DC=LOCAL'. At the bottom, there are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'.

Active Directory Lightweight Directory Services Setup Wizard

Application Directory Partition
An application directory partition stores application-specific data.

Do you want to create an application directory partition for this instance of AD LDS?

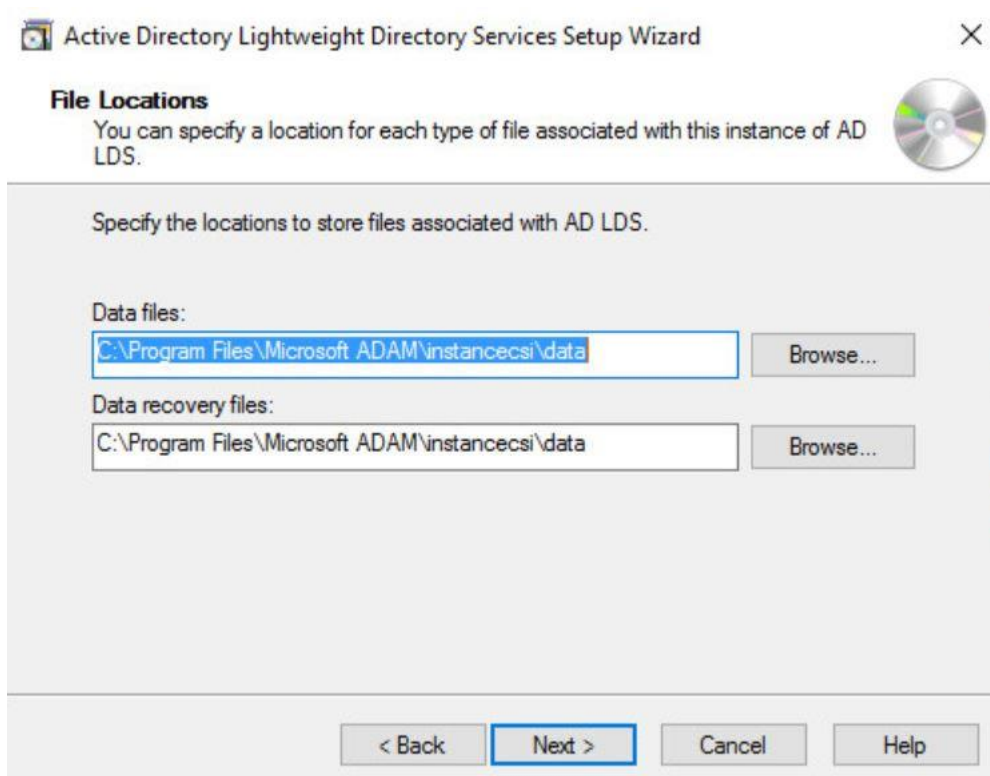
☐ No, do not create an application directory partition
Select this option if the application that you plan to install creates an application directory upon installation, or if you plan to create one later.

☒ Yes, create an application directory partition
Select this option if the application that you plan to install does not create an application directory partition upon installation. A valid partition name is any distinguished name that does not already exist in this instance. Example distinguished name:
CN=Partition1,DC=Woodgrove,DC=COM

Partition name:

< Back Next > Cancel Help

25. We use the default storage locations.



The screenshot shows the 'File Locations' step of the 'Active Directory Lightweight Directory Services Setup Wizard'. The window title is 'Active Directory Lightweight Directory Services Setup Wizard'. The subtitle is 'File Locations' with a description: 'You can specify a location for each type of file associated with this instance of AD LDS.' There is a CD icon in the top right corner. The main instruction is 'Specify the locations to store files associated with AD LDS.' There are two text boxes for file locations. The first is labeled 'Data files:' and contains the text 'C:\Program Files\Microsoft ADAM\instancecsi\data'. The second is labeled 'Data recovery files:' and contains the text 'C:\Program Files\Microsoft ADAM\instancecsi\data'. To the right of each text box is a 'Browse...' button. At the bottom, there are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'.

Active Directory Lightweight Directory Services Setup Wizard

File Locations
You can specify a location for each type of file associated with this instance of AD LDS.

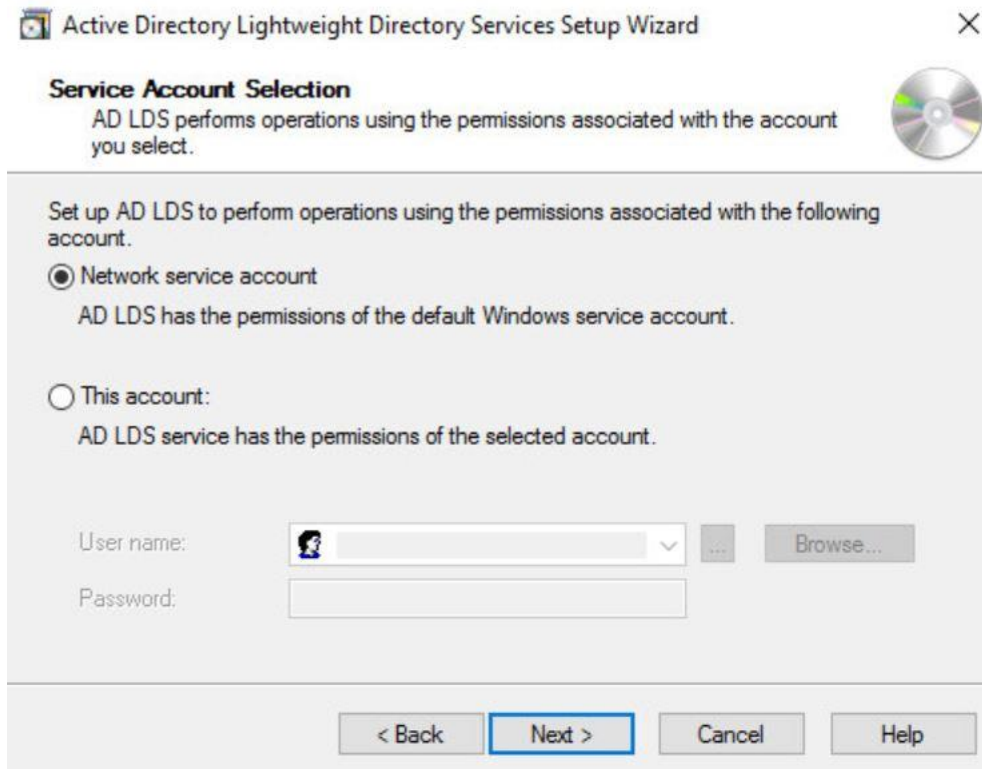
Specify the locations to store files associated with AD LDS.

Data files:
 Browse...

Data recovery files:
 Browse...

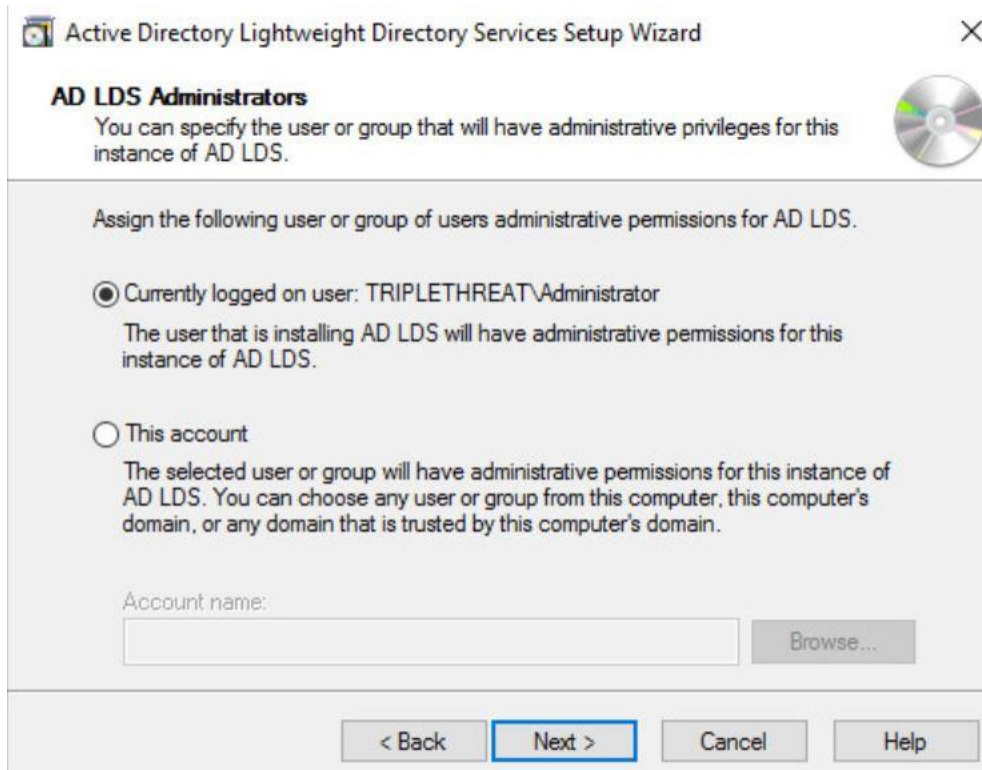
< Back Next > Cancel Help

26. We choose network service account for running AD LDS Service.



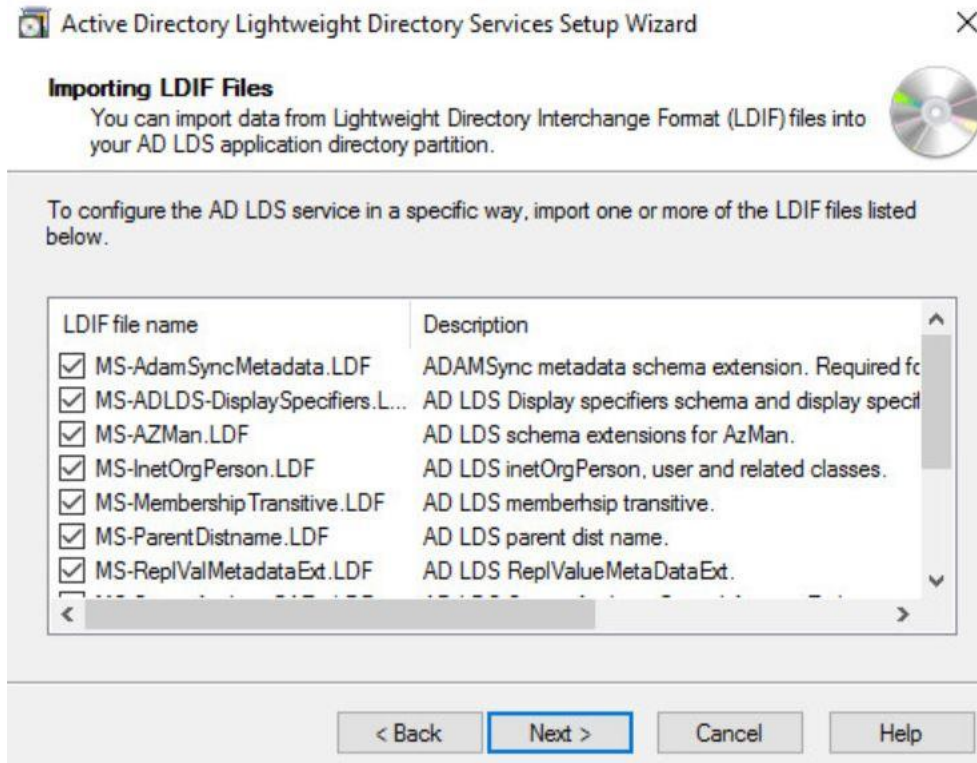
The screenshot shows the 'Service Account Selection' step of the 'Active Directory Lightweight Directory Services Setup Wizard'. The window title is 'Active Directory Lightweight Directory Services Setup Wizard'. The subtitle is 'Service Account Selection'. Below the subtitle, it says 'AD LDS performs operations using the permissions associated with the account you select.' There are two radio button options: 'Network service account' (selected) and 'This account:'. The 'Network service account' option has a description: 'AD LDS has the permissions of the default Windows service account.' The 'This account:' option has a description: 'AD LDS service has the permissions of the selected account.' Below these options, there are input fields for 'User name:' and 'Password:'. The 'User name:' field has a dropdown menu showing a user icon and a 'Browse...' button. The 'Password:' field is empty. At the bottom, there are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'. The 'Next >' button is highlighted with a blue border.

27. We choose the currently logged in user as an admin to for the AD LDS Instance.

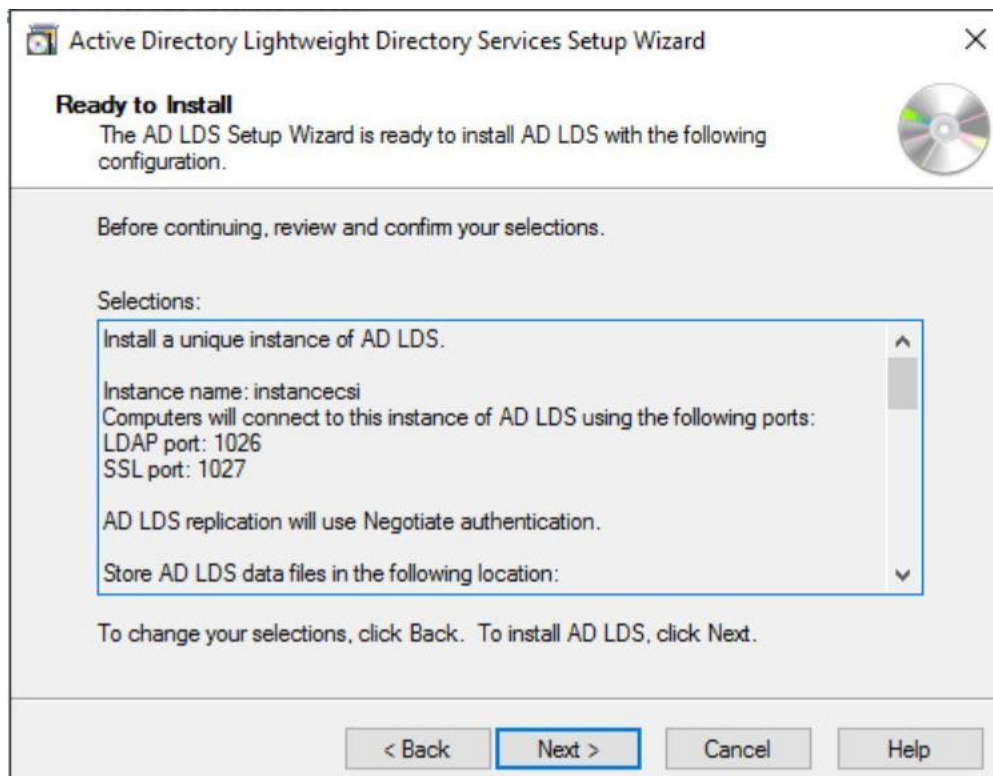


The screenshot shows the 'AD LDS Administrators' step of the 'Active Directory Lightweight Directory Services Setup Wizard'. The window title is 'Active Directory Lightweight Directory Services Setup Wizard'. The subtitle is 'AD LDS Administrators'. Below the subtitle, it says 'You can specify the user or group that will have administrative privileges for this instance of AD LDS.' There are two radio button options: 'Currently logged on user: TRIPLETHREAT\Administrator' (selected) and 'This account'. The 'Currently logged on user: TRIPLETHREAT\Administrator' option has a description: 'The user that is installing AD LDS will have administrative permissions for this instance of AD LDS.' The 'This account' option has a description: 'The selected user or group will have administrative permissions for this instance of AD LDS. You can choose any user or group from this computer, this computer's domain, or any domain that is trusted by this computer's domain.' Below these options, there is an input field for 'Account name:' and a 'Browse...' button. At the bottom, there are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'. The 'Next >' button is highlighted with a blue border.

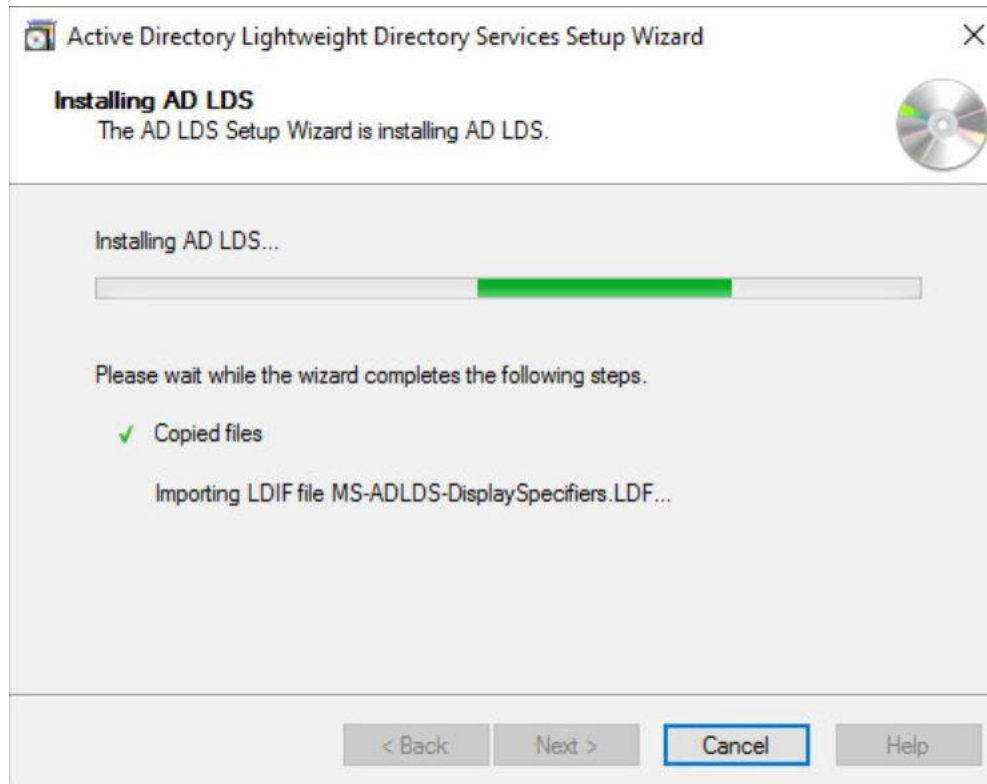
28. Marked all LDIF files to import.



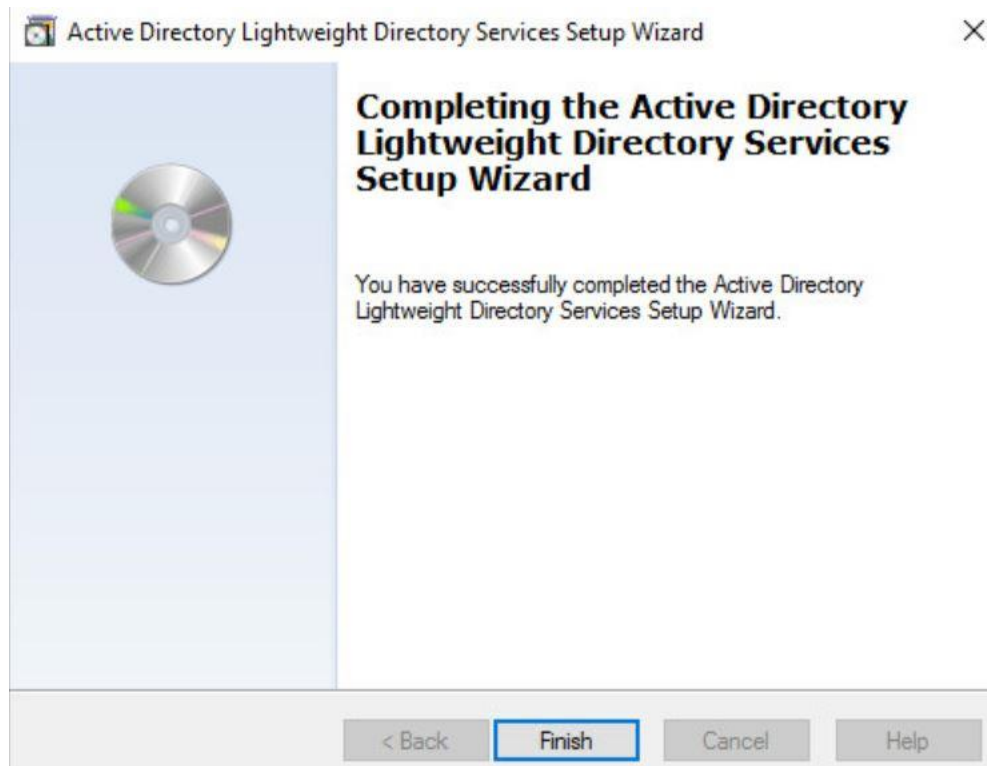
29. Verify our selections and install.



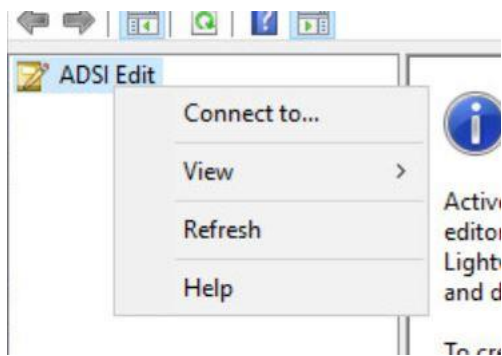
30. AD LDS is installing.



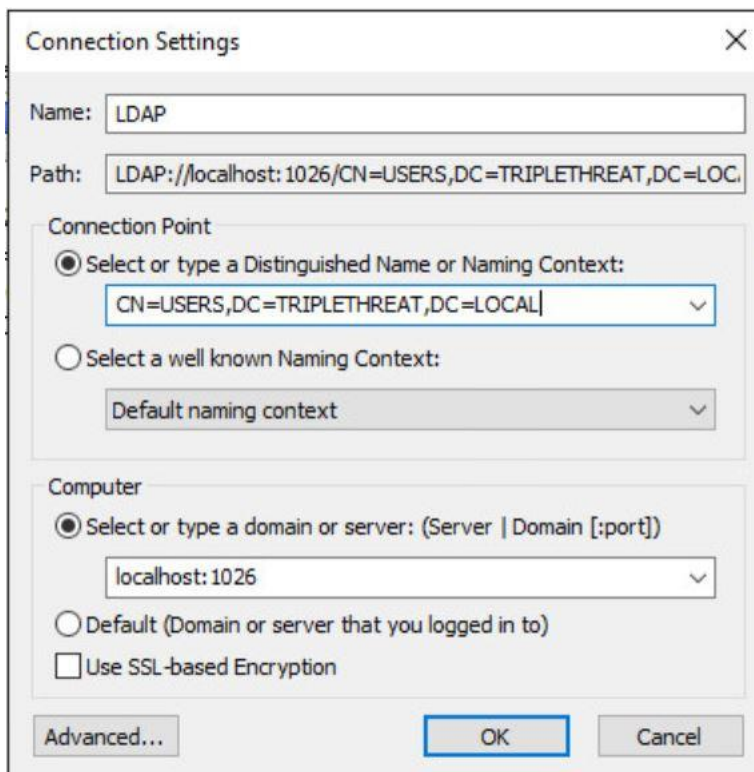
31. AD LDS is installed.



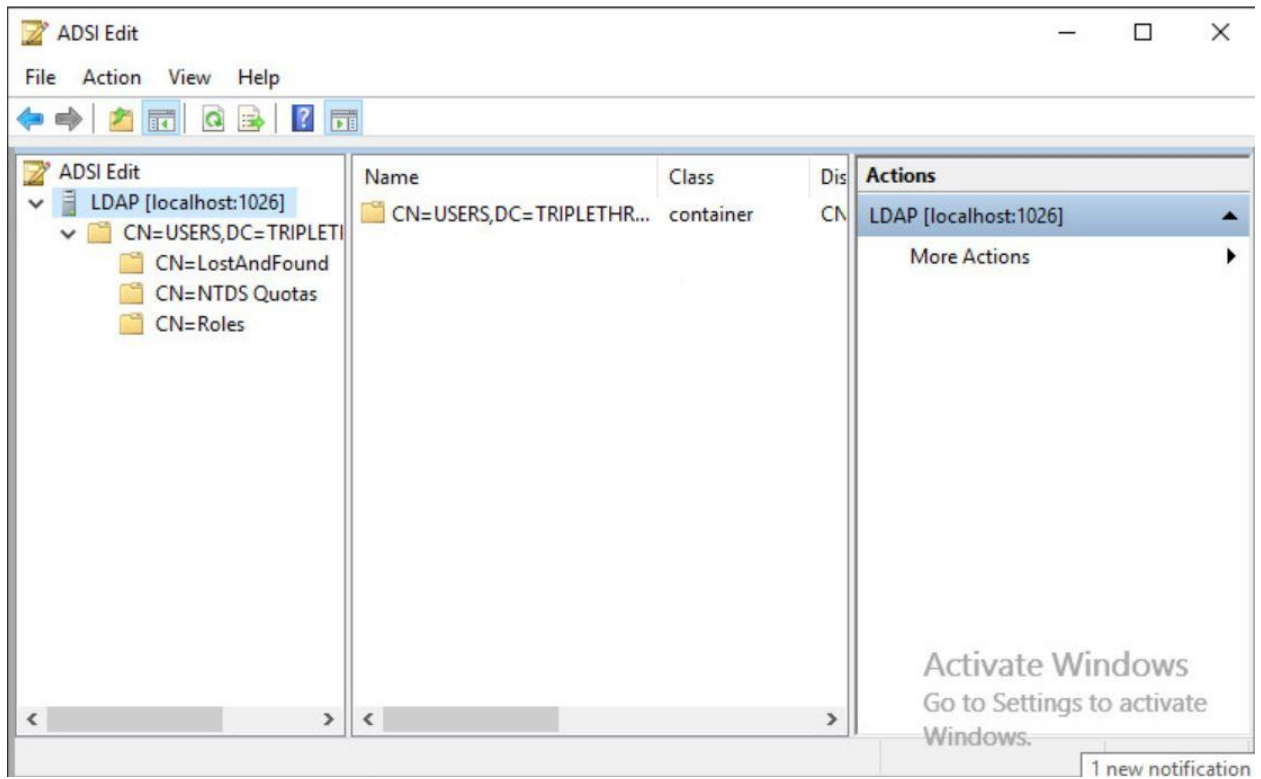
32. We pick ADSI from the menu and open it. Then we choose to connect.



33. We fill out the following.



34. The connection is successful.



35. We add users got to Active directory, right click on users New -> User. Fill out user info with name and password.

Active Directory Users and Computers

File Action

Active Dir

Saved

tripleth

Bu

Co

Do

For

Ke

Lo

Ma

Pro

Sys

Us

NT

TP

New Object - User

Create in: triplethreat.local/Users

First name: bdreher Initials:

Last name:

Full name: bdreher

User logon name: bdreher @triplethreat.local

User logon name (pre-Windows 2000): TRIPLETHREAT\ bdreher

< Back Next > Cancel

New Object - User

Create in: triplethreat.local/Users

Password:

Confirm password:

☐ User must change password at next logon

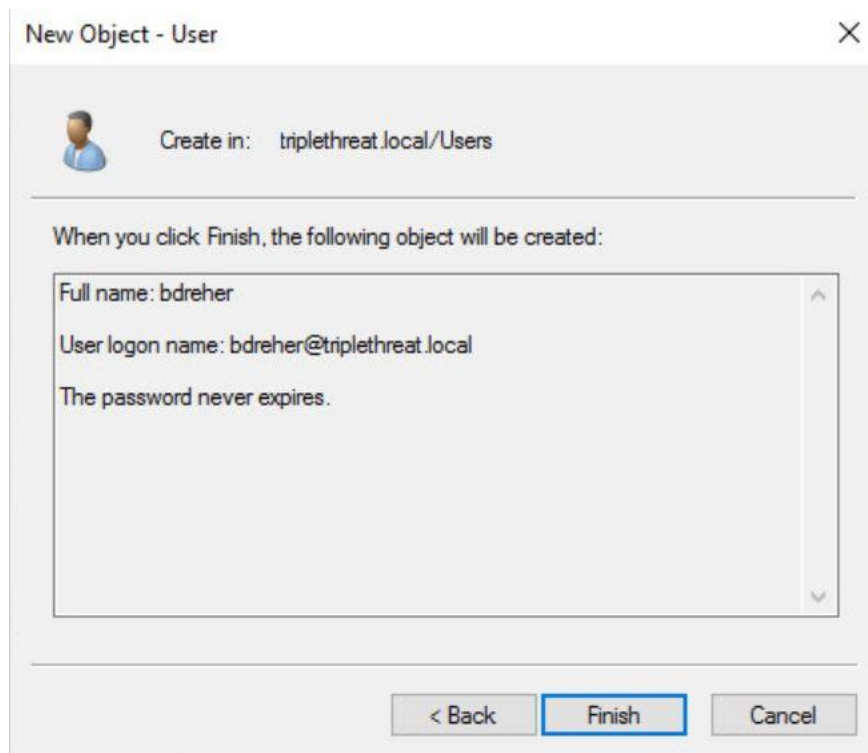
☐ User cannot change password

☒ Password never expires

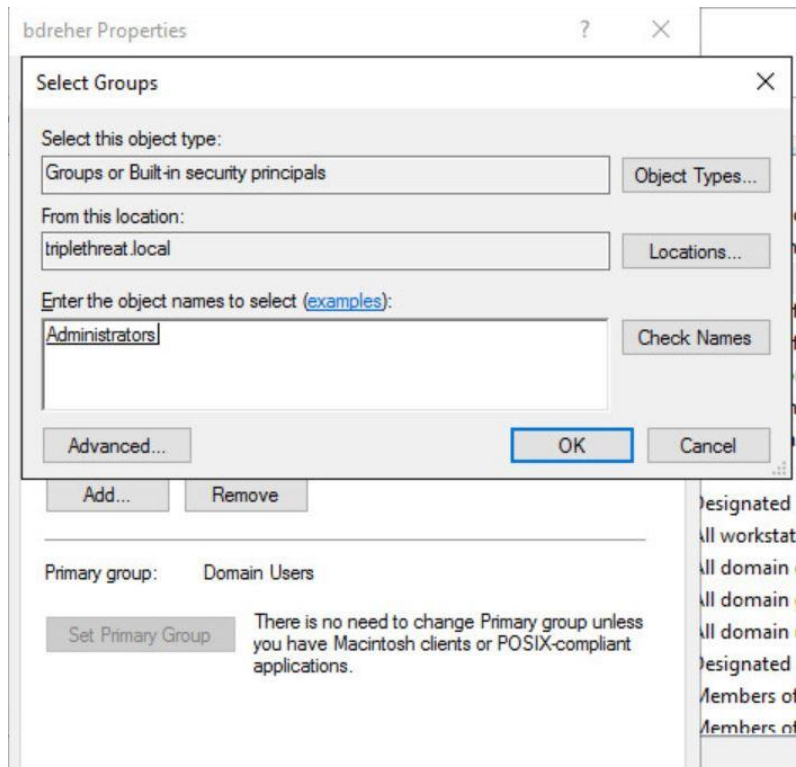
☐ Account is disabled

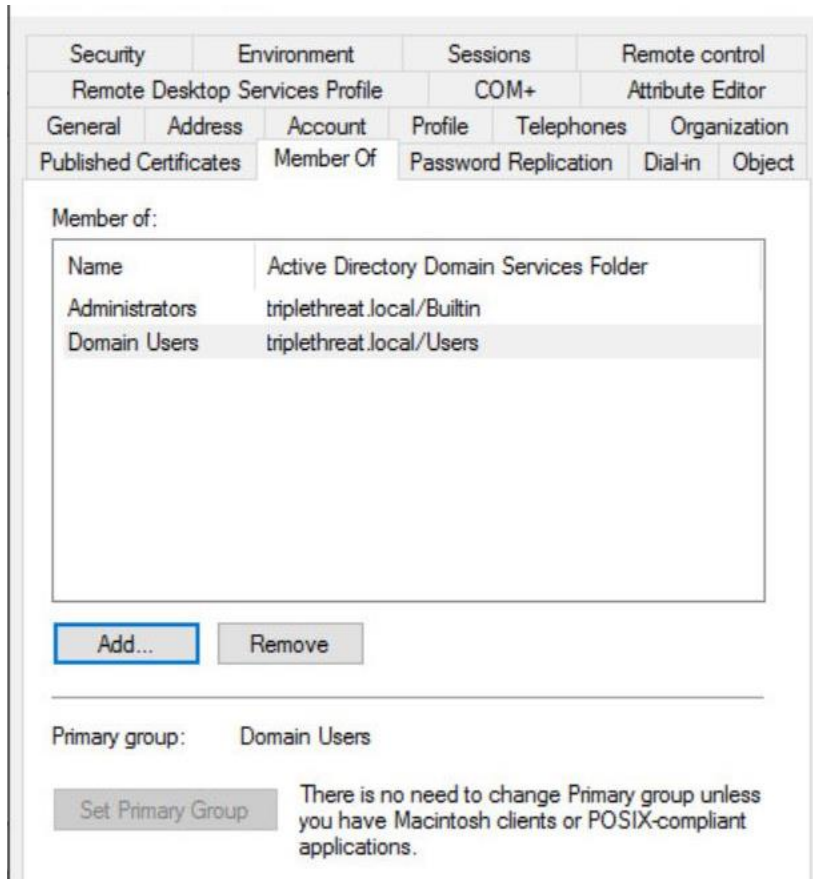
< Back Next > Cancel

36. Check everything is correct and finish.

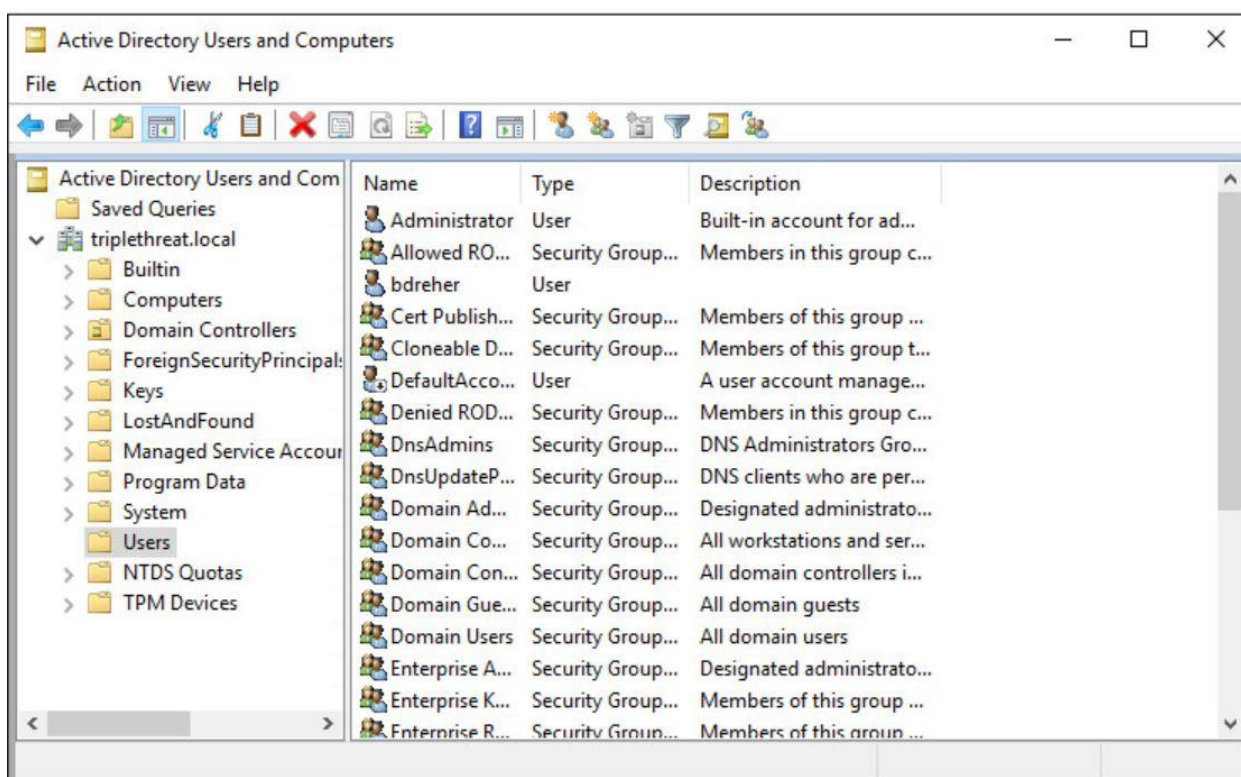


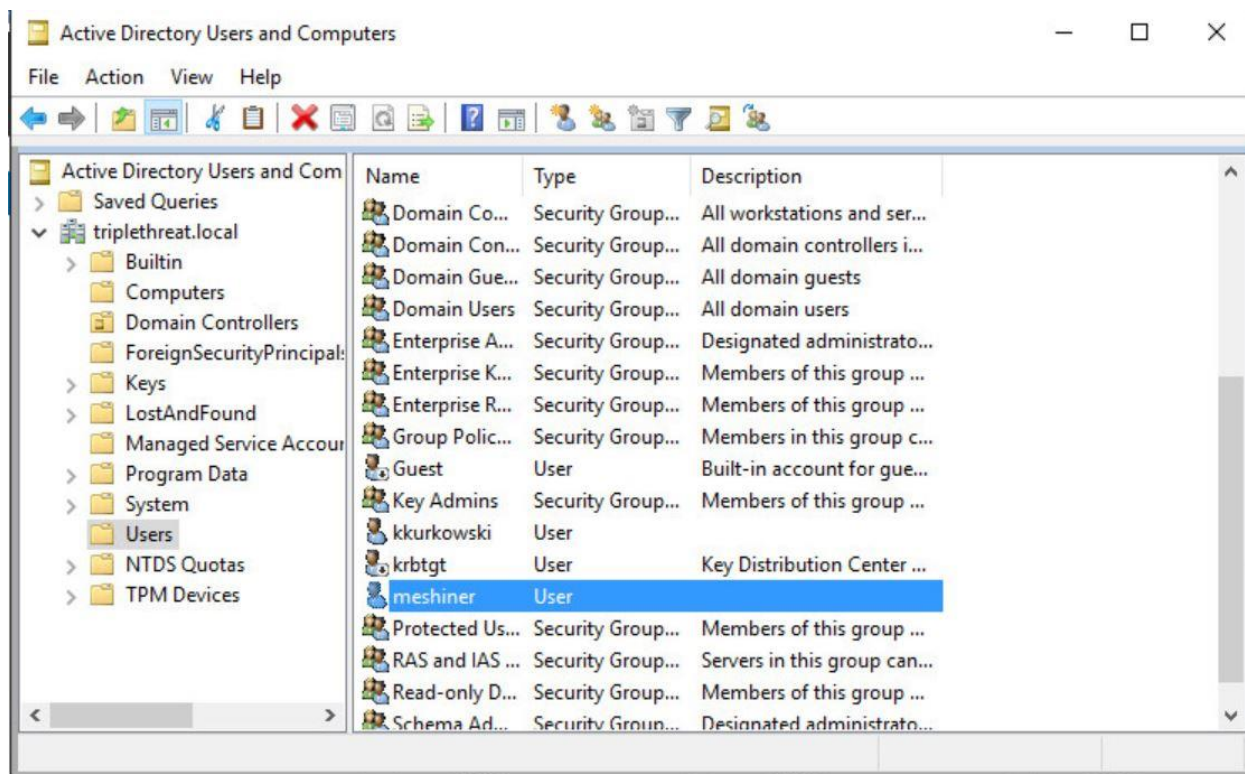
37. Then right click said users and select properties and click the Member Of tab. Then added in Administrators group click Check names and ok and add.



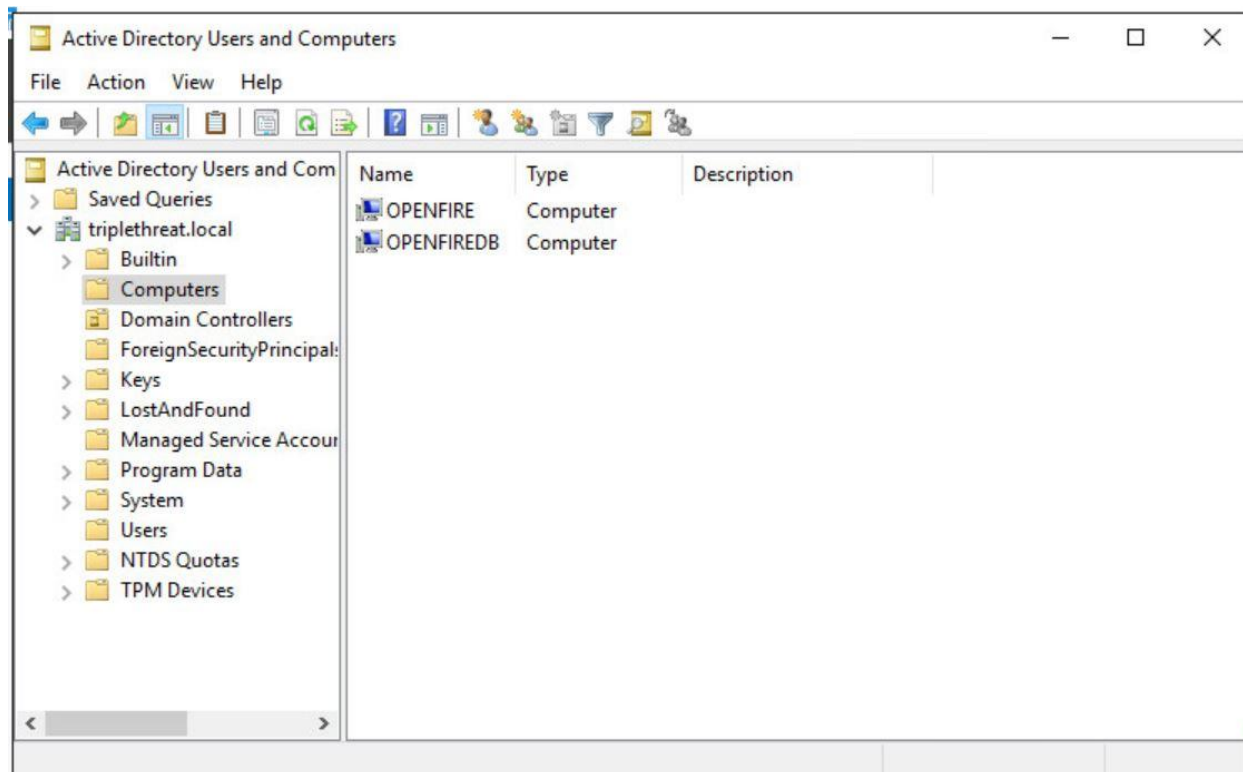


38. Users appear in Users section, bdreher, kkurowski, and meshiner.

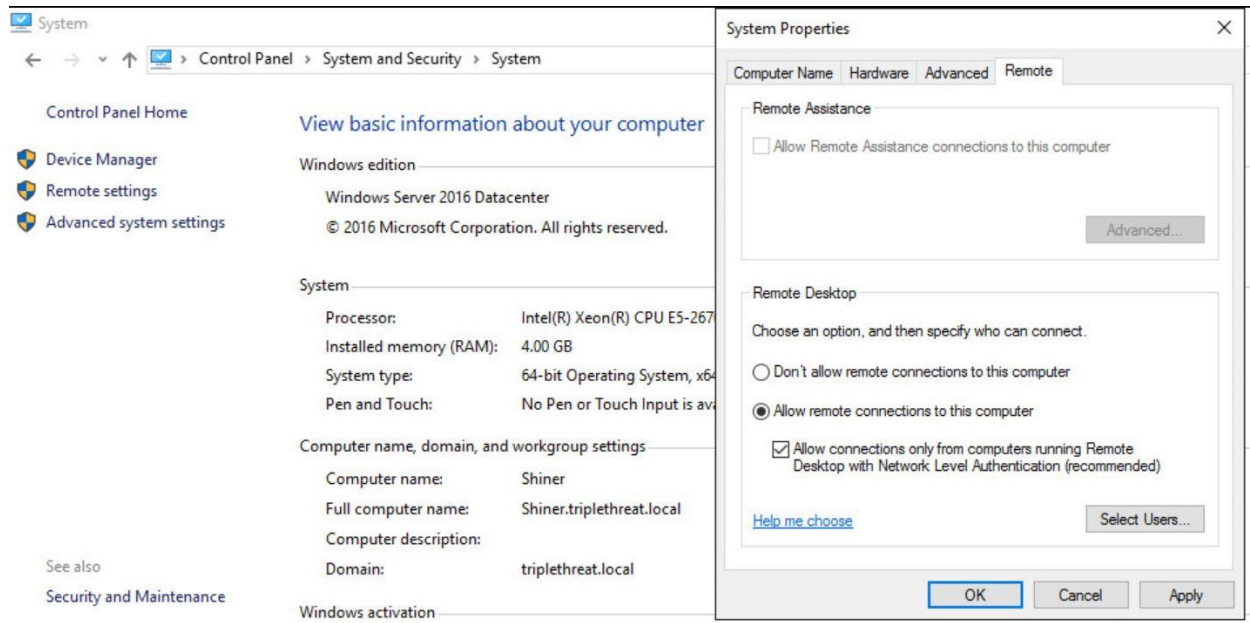




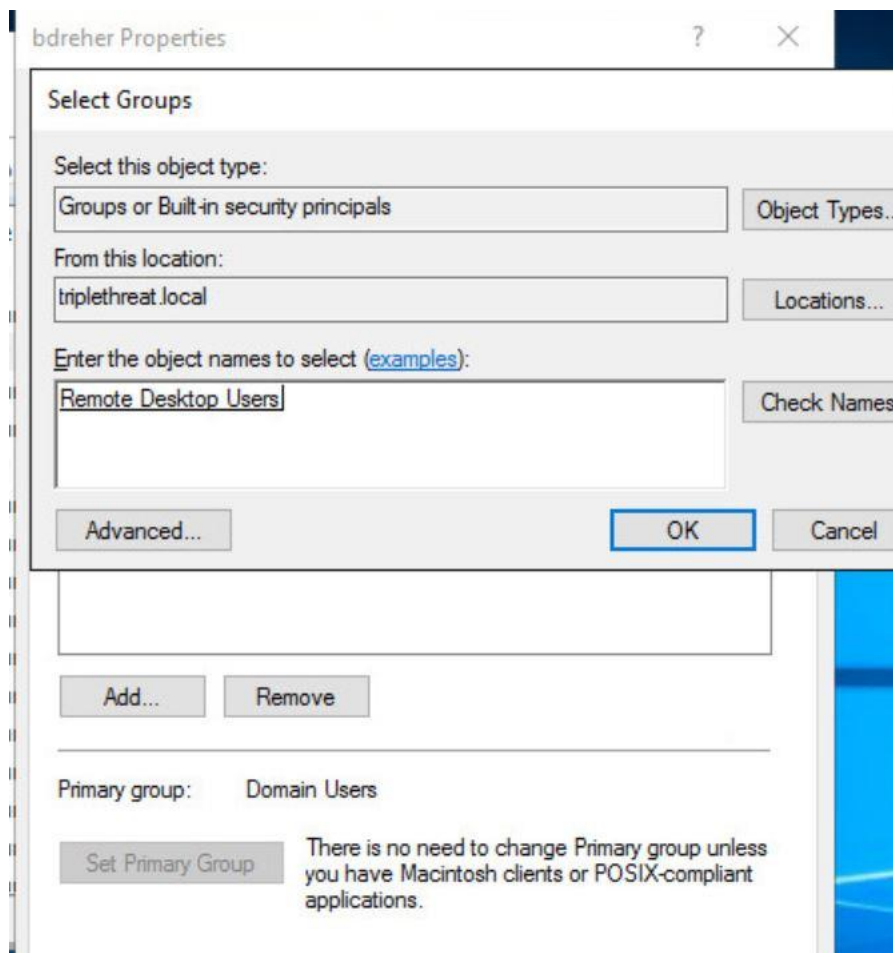
39. Our other computers appeared in active directory.



40. Allowed for remote connections to computer.



41. Put all users in the Remote Desktop Users group.



bdreher Properties



Security	Environment	Sessions	Remote control		
Remote Desktop Services Profile		COM+	Attribute Editor		
General	Address	Account	Profile	Telephones	Organization
Published Certificates	Member Of	Password Replication	Dial-in	Object	

Member of:

Name	Active Directory Domain Services Folder
Administrators	triplethreat.local/Builtin
Domain Users	triplethreat.local/Users
Remote Desktop ...	triplethreat.local/Builtin

Primary group: Domain Users

There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.