

Windows Active Directory Setup Lab

By Michael Ambeguia

Purpose: The purpose of this lab is to gain hands-on experience setting up a Windows Active Directory environment. In this Lab I will set up a Windows domain controller hosted on a Windows 2022 Server and will perform the prerequisite tasks such as setting a static ip address and configuring DNS on the DC. Active Directory is so important for organizations since it simplifies the management of Windows environments and serves as a centralized directory of a company's users, devices, and network resources. Not only this, AD can help organizations configure settings in an organized fashion through the use of Group Policy Objects. By completing this lab I will greatly improve my Windows system administration skills and knowledge as well.

Sections:

1. Introduction to Active Directory:
2. Setting up environment:
3. Installing and Configuring AD:

Section #1 Introduction to Active Directory:

1.1 What is Active Directory? Why is it used?

Microsoft Active Directory is a directory service and database system created by Microsoft to ease the management of a large organization's IT infrastructure and Users. AD has eight main benefits for organizations that choose to adopt it.

1. AD makes configuring a Windows environment easier:
AD helps organizations configure and manage a Windows OS environment by allowing administrators to use baseline policies in the form of GPOs (Group Policy Objects).
2. AD helps organizations manage user accounts:
AD helps organizations manage user accounts by simplifying the provisioning and deprovisioning of user accounts. From an AD domain controller administrators can create new users, set proper permissions for users, update user information, and reset user passwords. Deprovising is easy too. You can delete users from the DC.
3. AD helps organizations manage access to network services and resources:
AD allows organizations to manage access to network services and resources through the use of Kerberos (authentication) and security tokens/acls (authentication). Kerberos is used to verify a user's identity, and once their identity is verified they are granted a security token based on their security group membership. This ticket is then compared against the acl for a network resource

and if the ticket grants permission then the user can access the resource.

4. AD provides easy login capabilities for users:

Active Directory supports single sign on capabilities to make signing into various domain linked applications easier. Using AD credentials once can grant users access to multiple applications without the need to sign in for each one.

5. AD helps organizations logically organize users and devices:

AD can be used to logically organize users and devices in a hierarchical form through the use of organizational units (ous). Ous are containers that are used to store user and device objects. GPOs are applied to OUs. Ous also supports the delegation of administrative permissions. For example, permissions can be given to IT support employees to reset the passwords for a certain OU they are responsible for. ***It should be noted that permissions for users are not based on Ou membership but rather the security group.***

6. AD is scalable:

Active Directory can support high availability since it can be scaled to meet the needs of organizations of any size. Organizations can simply add more DCs to their forests to support growth in their company's size. AD data can be replicated across domain controllers allowing new DCs to start working right away.

7. AD helps organizations configure security policies:

Active Directory GPOS can be used to simplify the deployment of security policies on devices. All you need to do is create the GPO and configure its settings, then apply it to the proper OU.

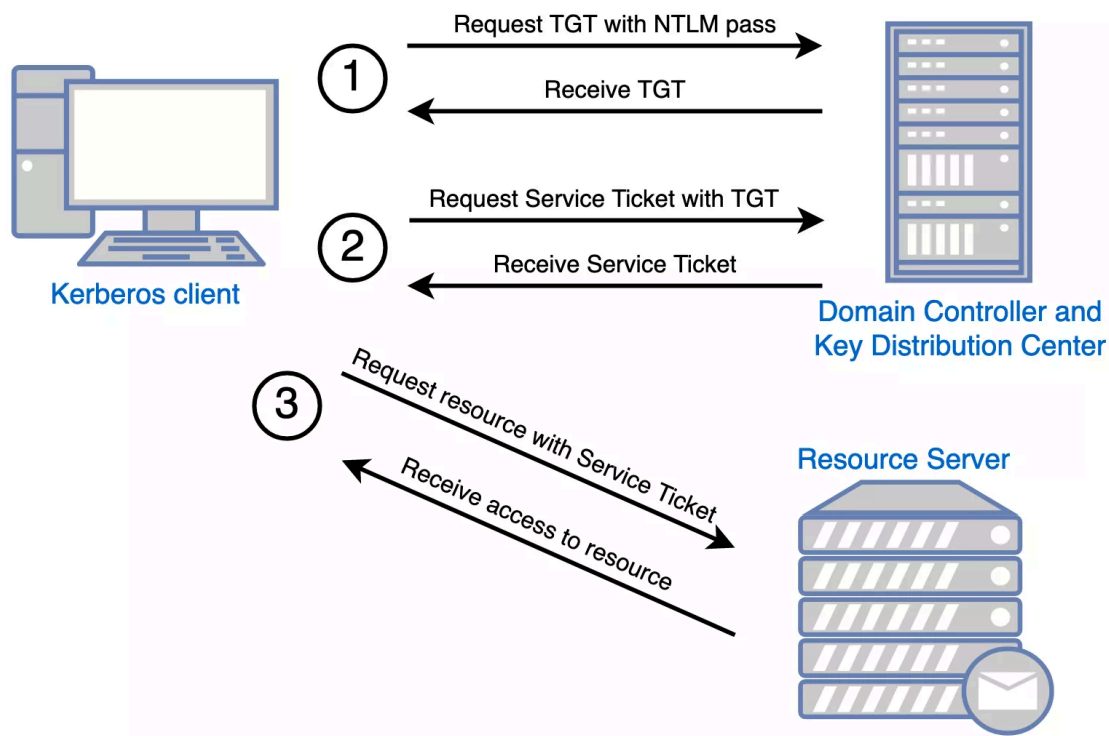
8. AD can be replicated:

Active Directory can be replicated across multiple domain controllers. AD replication serves as a form of fault tolerance, ensuring that if one DC is down the directory data can still be available on another one.

1.2 How does AD handle authentication and authorization?

Active Directory uses Kerberos for authentication, and uses security groups and ACLs for authorization. Here is a nice illustration from

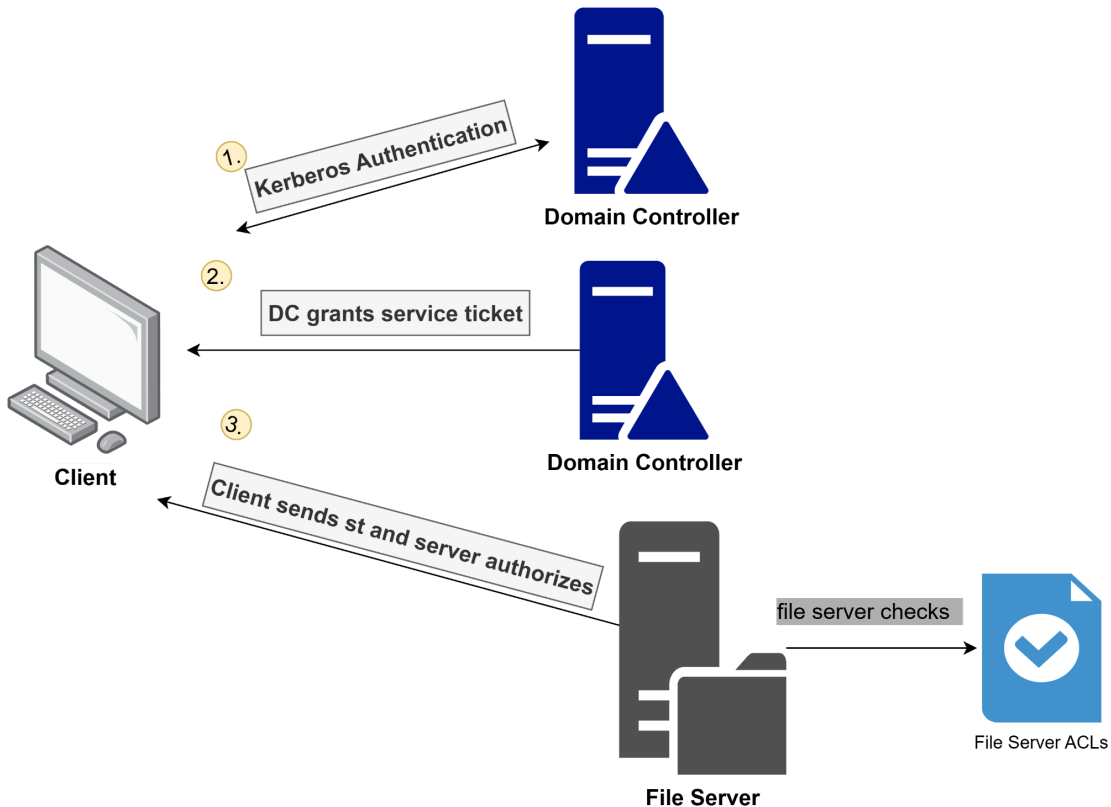
<https://www.optiv.com/insights/source-zero/blog/kerberos-domains-achilles-heel> that demonstrates how Kerberos works.



For AD the domain controller is the ticket granting server and the key distribution center all in one. Kerberos focuses on never sending the password over the network to prevent man in the middle, replay, or credential harvesting. This is possible since a user's password is never sent over the network and is instead used to create a key using PBKDF2 or similar key derivation algorithms. This key is the only data sent from a client to the DC. The DC has a copy of the same key and uses this copy to decrypt data sent from the client. If the DC is able to decrypt the data that means that the password is correct. This is a brilliant and secure method of authentication since the client data is useless to attackers. It is impossible to derive the password from the password derived key.

For authorization AD uses ACLs or access control lists and permissions. The ACLs can dictate whether a user can access, modify, or otherwise interact with a resource. They rely on a user's security group membership rather than OU membership as well. ACLs typically reside on the device hosting the network service or resource as well.

Putting it all together:

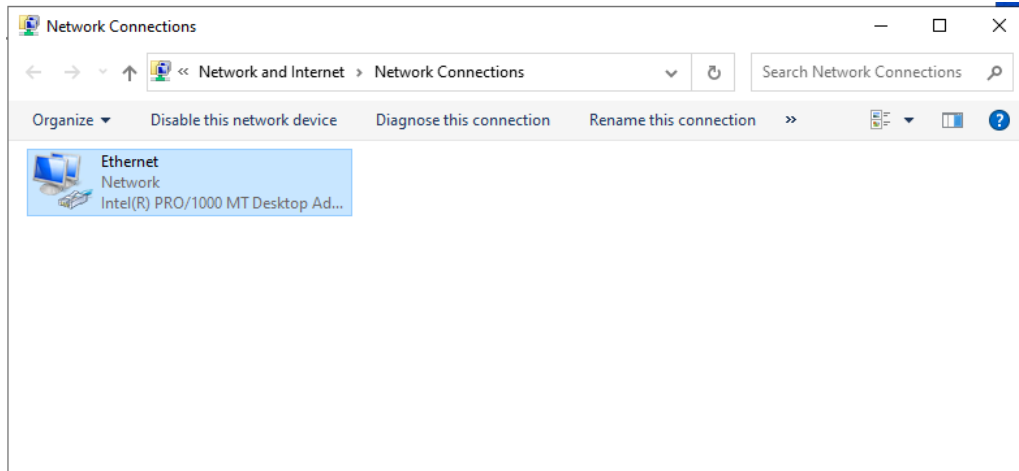


So, to put it all together, a user would sign into their domain joined device (PC/Laptop). Kerberos is used to authenticate them and once they are authenticated they are granted a TGT. Then if a user tries to access a network resource like a file share they send the TGT to the DC. They will ask the DC for access and the DC will send a service ticket in exchange for the TGT. Once the user gets the service ticket they can communicate with the device hosting the resource , which will authorize the action or deny it based on the acl present.

Section #2 Setting up Environment:

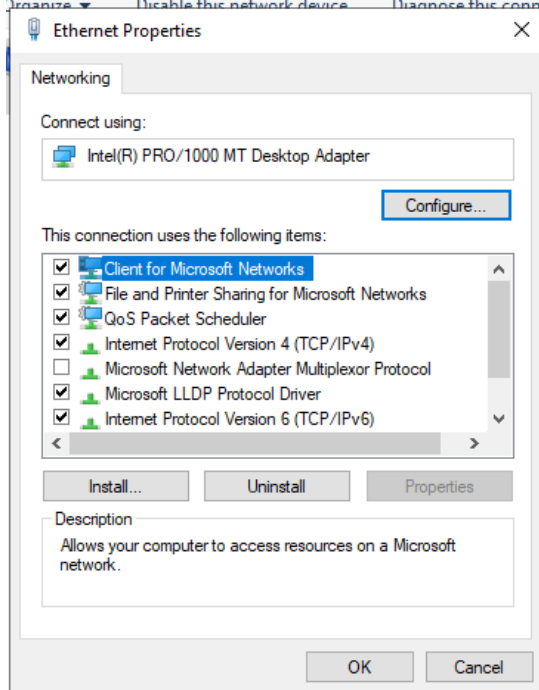
2.1. Assign a static IP address to the server:

To set a static IP address on the server you can go to Control Panel/Network and Internet/Network and Sharing Center/Change Adapter Settings



Then click on the ethernet adapter. After you click on properties.

Under properties click on Internet Protocol Version 4.



Next set the static IP address by choosing “use the following ip address”. First find your current IP address using the command line.

```
Microsoft Windows [Version 10.0.20348.1850]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ipconfig

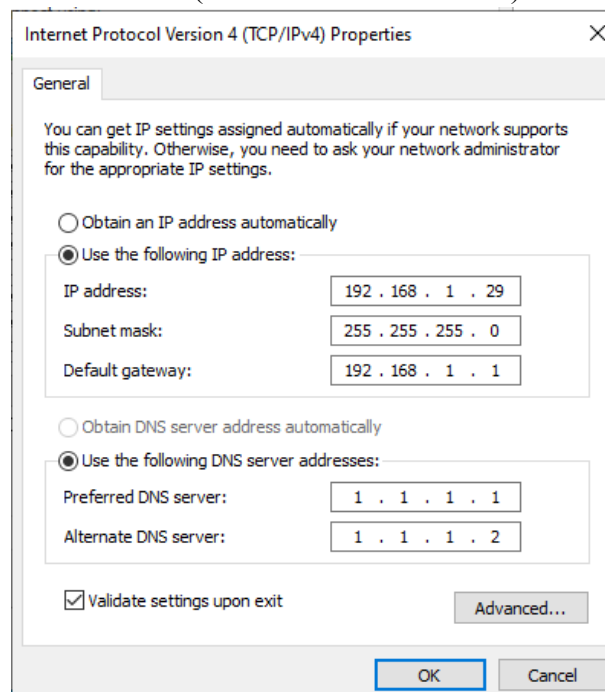
Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::9668:c8cb:44b9:4234%14
    IPv4 Address. . . . . : 192.168.1.29
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

C:\Users\Administrator>
```

Use the same subnet mask and default gateway. For the dns servers I will use 1.1.1.1 and 1.1.1.2 for this server (Cloudflare DNS servers).



Then I tested the network connection using Ping.

```
C:\Users\Administrator>ping 1.1.1.1

Pinging 1.1.1.1 with 32 bytes of data:
Reply from 1.1.1.1: bytes=32 time=14ms TTL=56
Reply from 1.1.1.1: bytes=32 time=36ms TTL=56

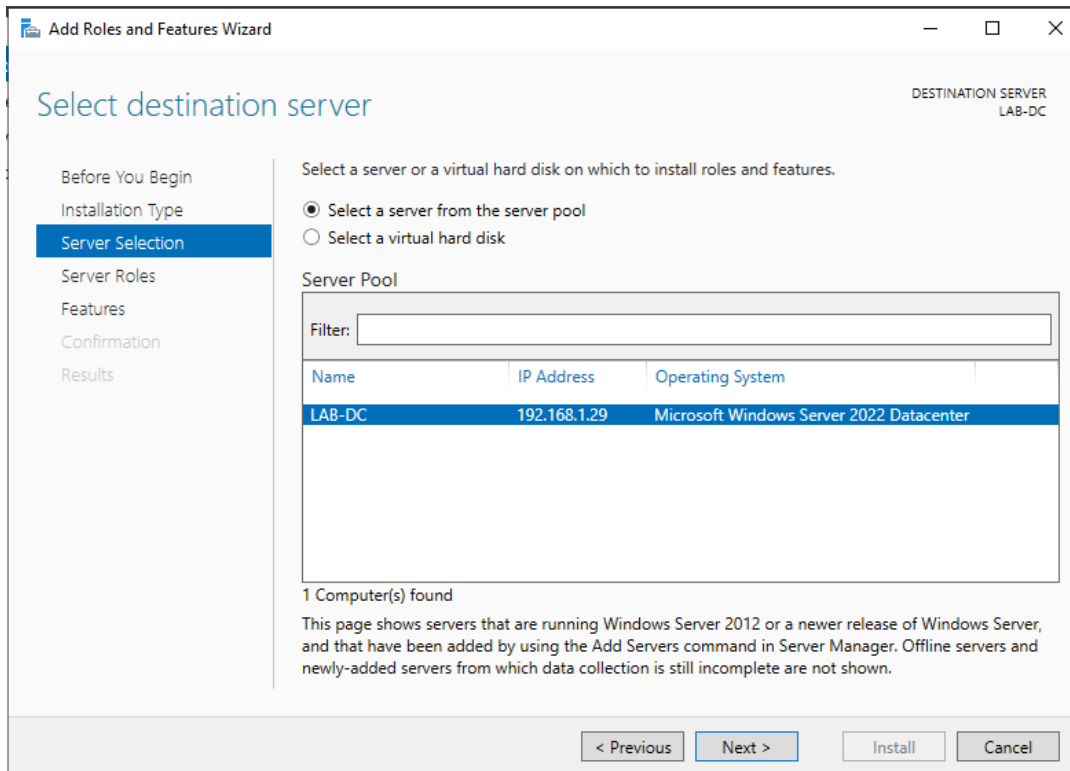
Ping statistics for 1.1.1.1:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 14ms, Maximum = 36ms, Average = 25ms
Reply from 1.1.1.1: Control-C
^C
C:\Users\Administrator>ping Google.com

Pinging Google.com [142.250.72.142] with 32 bytes of data:
Reply from 142.250.72.142: bytes=32 time=63ms TTL=116
Reply from 142.250.72.142: bytes=32 time=307ms TTL=116
Reply from 142.250.72.142: bytes=32 time=60ms TTL=116

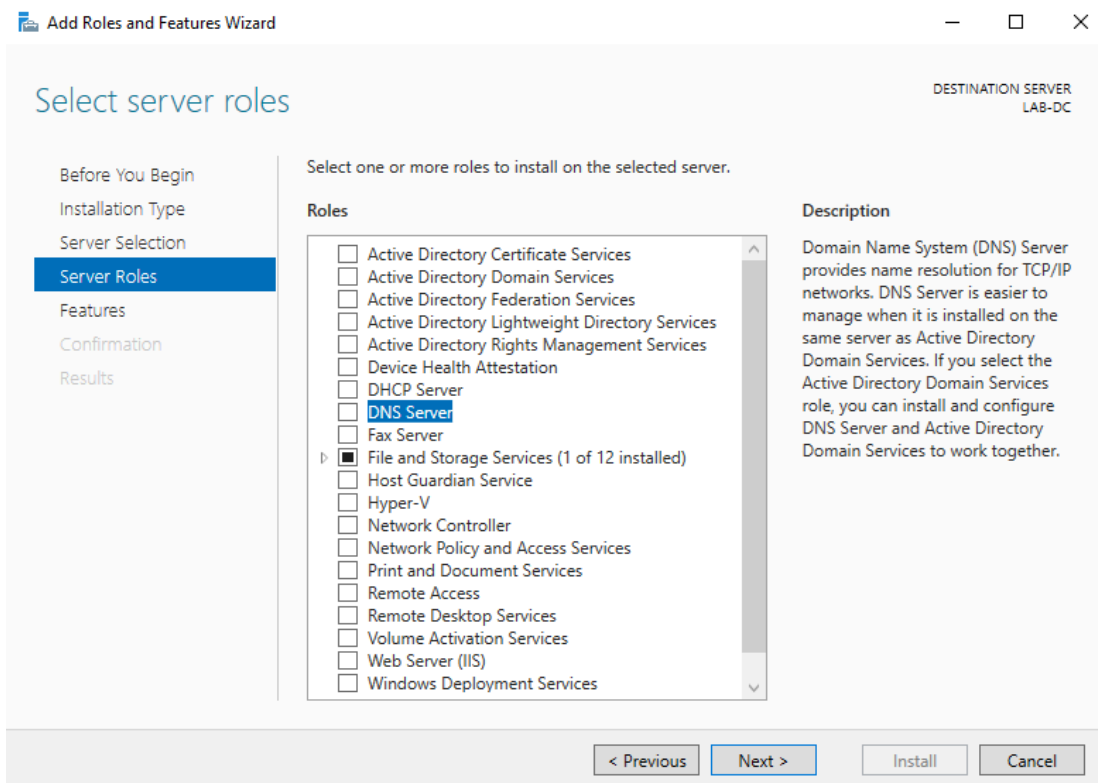
Ping statistics for 142.250.72.142:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 60ms, Maximum = 307ms, Average = 143ms
Control-C
^C
C:\Users\Administrator>
```

2.2 Set up DNS server role on the server:

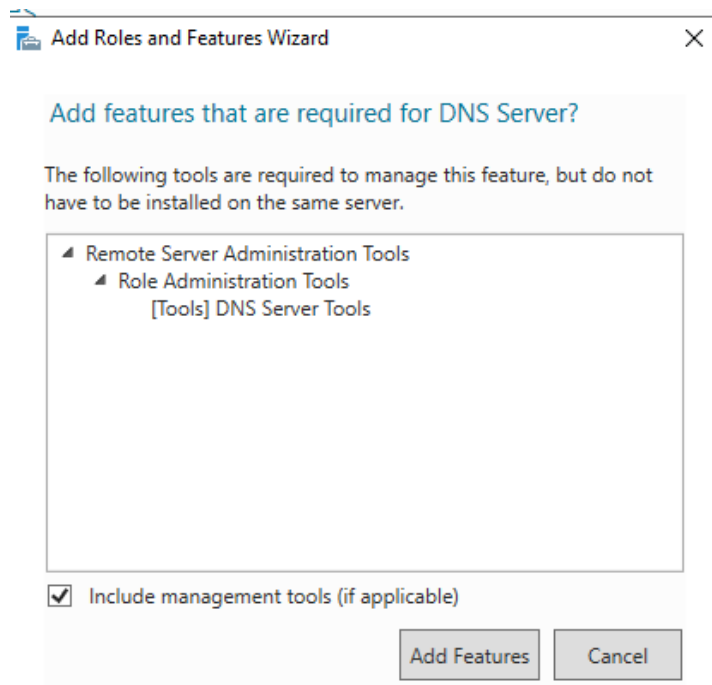
To give the server the DNS server role you need to go to server manager and click manage, then click on add role. Then you need to choose the server you want to add a role to. In my case it is my local server (LAB-DC).



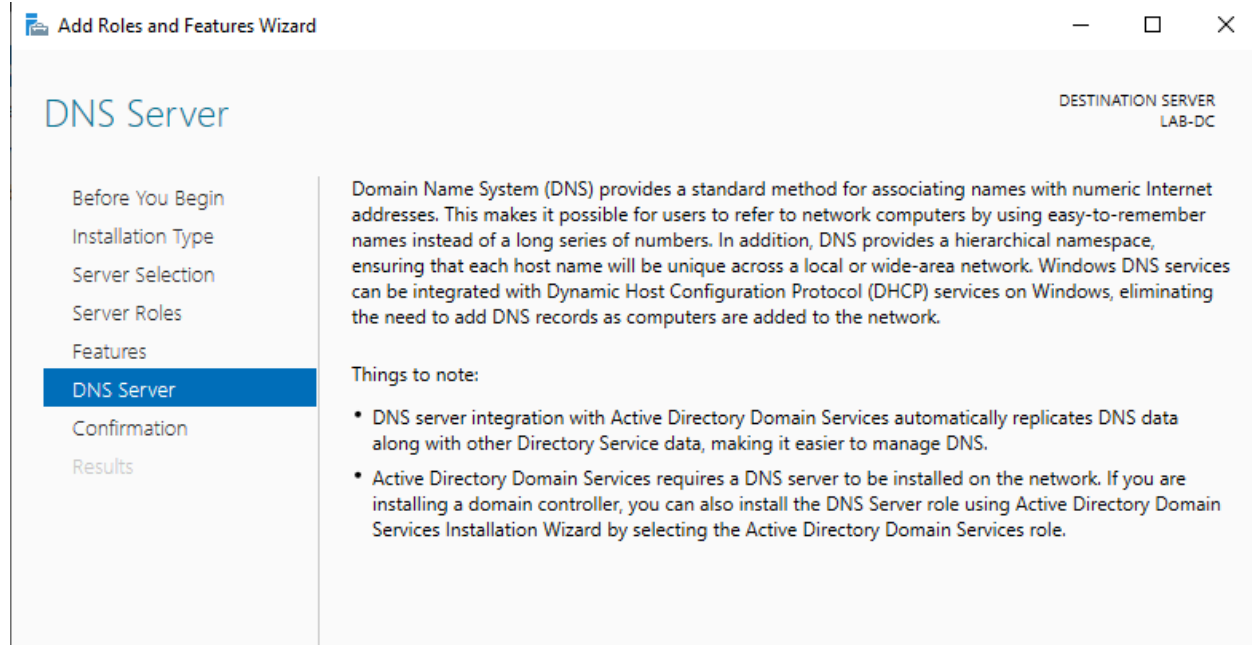
Click next then select the server role (DNS server).



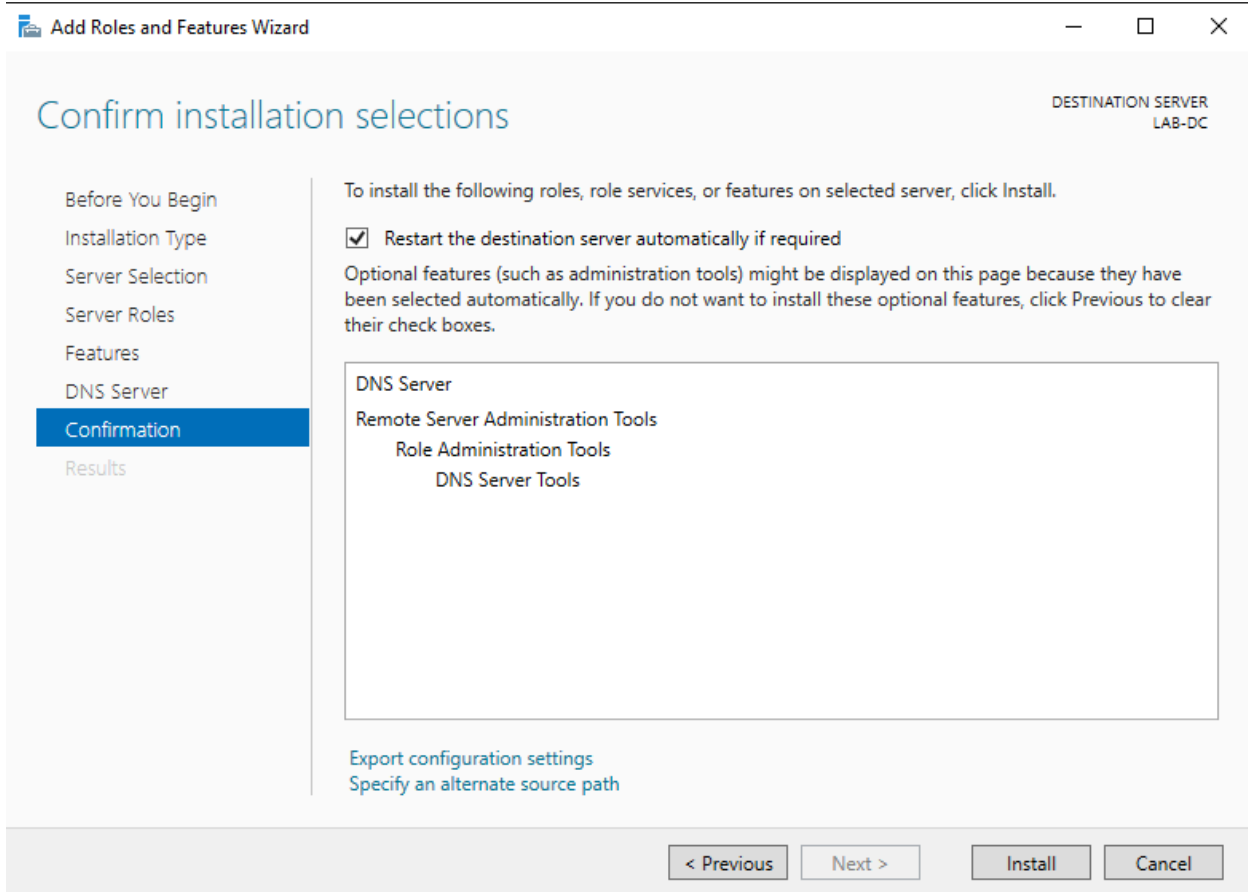
The roles and features associated with this service are shown. Then click add features.



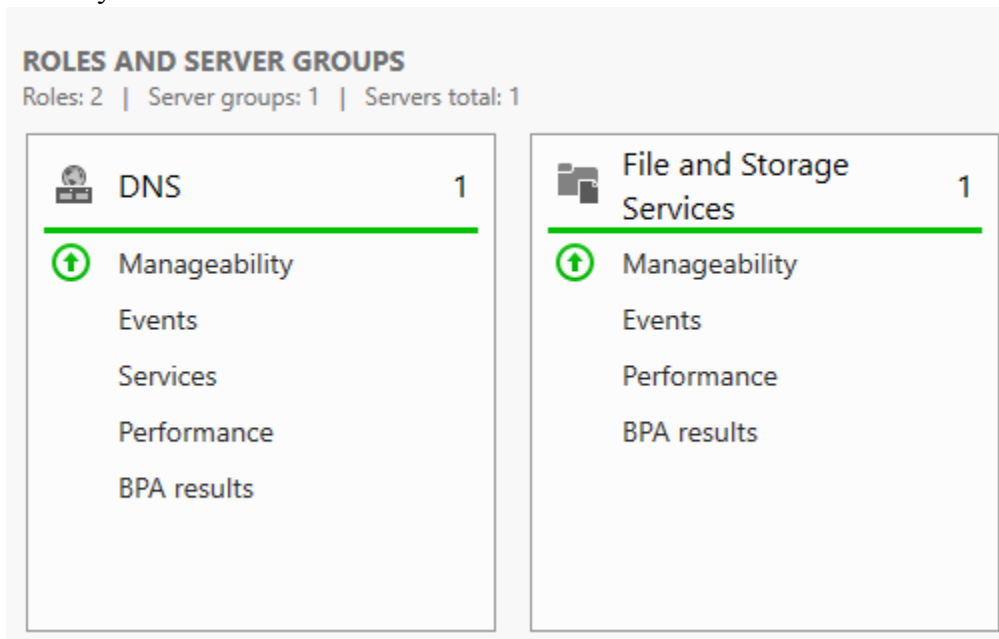
Click next again and skip the features section. Then you will see a page describing the DNS server role.



Then install the service. You want to restart the server right away once the role is installed.



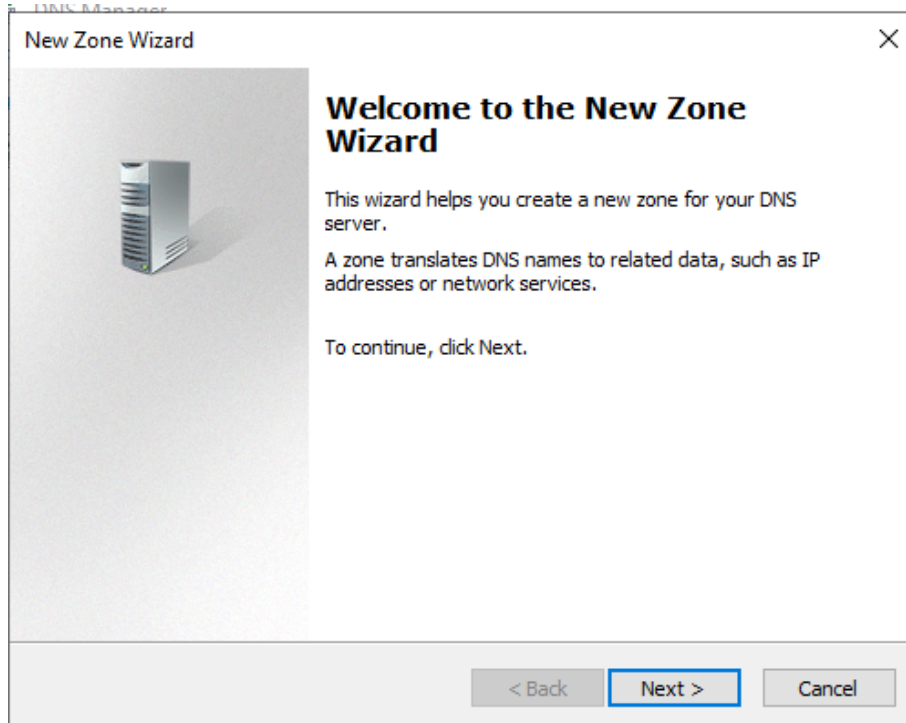
Now my server has the DNS role!



2.3 Configuring DNS

Create a forward lookup zone.

Forward lookup zones are used to translate domain names and urls to their ip address. An active directory controller needs to have a forward lookup zone that points its domain name to the server ip address since without a forward lookup zone the clients won't be able to resolve the domain controller's domain name.



New Zone Wizard ✕

Zone Type
The DNS server supports various types of zones and storage.

Select the type of zone you want to create:

☒ **Primary zone**
Creates a copy of a zone that can be updated directly on this server.

☐ **Secondary zone**
Creates a copy of a zone that exists on another server. This option helps balance the processing load of primary servers and provides fault tolerance.

☐ **Stub zone**
Creates a copy of a zone containing only Name Server (NS), Start of Authority (SOA), and possibly glue Host (A) records. A server containing a stub zone is not authoritative for that zone.

☐ Store the zone in Active Directory (available only if DNS server is a writeable domain controller)

< Back **Next >** Cancel

New Zone Wizard ✕

Forward or Reverse Lookup Zone
You can use a zone for forward or reverse lookups.

Select the type of lookup zone you want to create:

☒ **Forward lookup zone**
A forward lookup zone translates DNS names into IP addresses and provides information about available network services.


☐ **Reverse lookup zone**
A reverse lookup zone translates IP addresses into DNS names.

< Back **Next >** Cancel

Windows Server 2008 R2 DNS Manager

New Zone Wizard

Zone Name
What is the name of the new zone?



The zone name specifies the portion of the DNS namespace for which this server is authoritative. It might be your organization's domain name (for example, microsoft.com) or a portion of the domain name (for example, newzone.microsoft.com). The zone name is not the name of the DNS server.


Zone name:

< Back Next > Cancel

Windows Server 2008 R2 DNS Manager

New Zone Wizard

Zone File
You can create a new zone file or use a file copied from another DNS server.

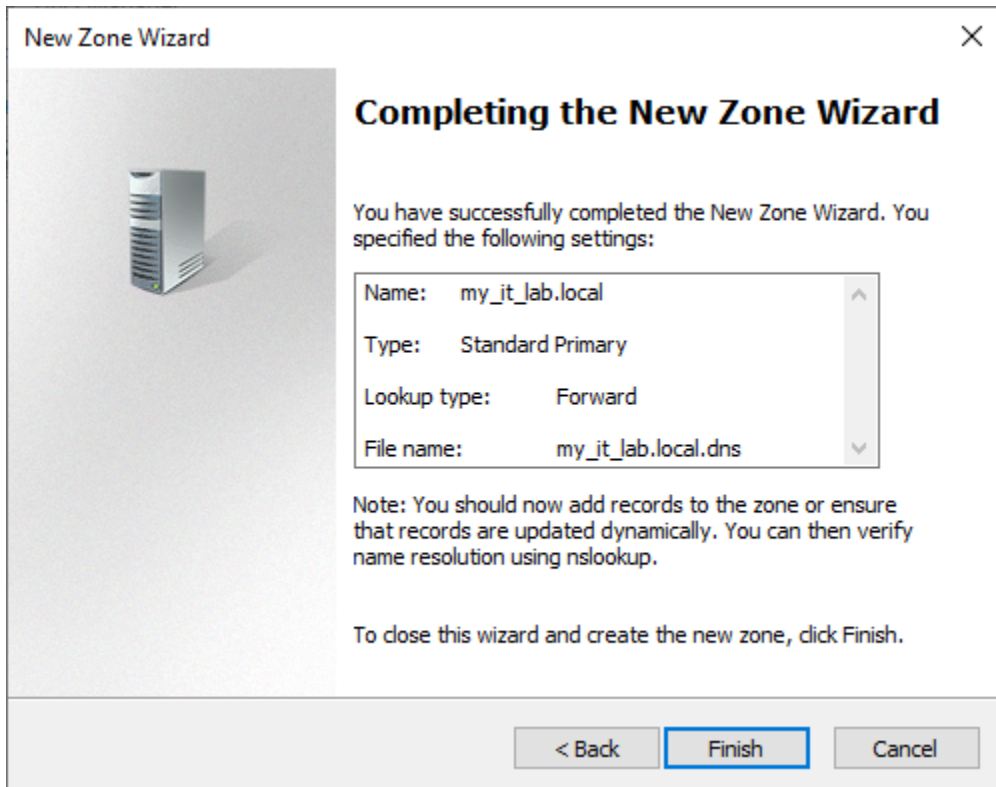
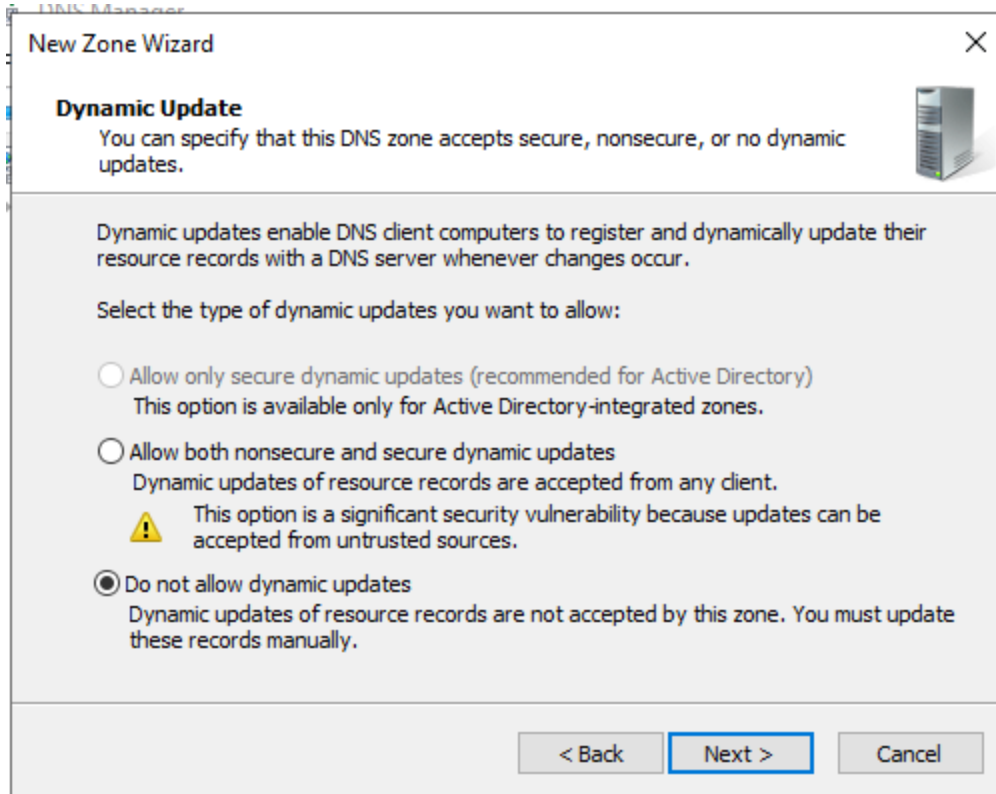


Do you want to create a new zone file or use an existing file that you have copied from another DNS server?

☒ Create a new file with this file name:

☐ Use this existing file:

To use this existing file, ensure that it has been copied to the folder %SystemRoot%\system32\dns on this server, and then click Next.



Now create an A record for the server. The A record is used by the forward lookup zone to resolve the DC domain name to its ip address.

New Host

Name (uses parent domain name if blank):
LAB_DC

Fully qualified domain name (FQDN):
LAB_DC.my_it_lab.local.

IP address:
192.168.1.29

☐ Create associated pointer (PTR) record

Add Host Cancel

Create a reverse lookup zone.

DNS Manager

New Zone Wizard

Forward or Reverse Lookup Zone
You can use a zone for forward or reverse lookups.

Select the type of lookup zone you want to create:

☐ Forward lookup zone
A forward lookup zone translates DNS names into IP addresses and provides information about available network services.

☒ Reverse lookup zone
A reverse lookup zone translates IP addresses into DNS names.

< Back Next > Cancel

Reverse lookup zones are used to translate ip addresses into hostnames. This is vital for Active Directory since knowing what the hostname of a client device is will allow AD to add the hostname in logs and other sources of data.

New Zone Wizard

Reverse Lookup Zone Name
A reverse lookup zone translates IP addresses into DNS names.

Choose whether you want to create a reverse lookup zone for IPv4 addresses or IPv6 addresses.

☒ IPv4 Reverse Lookup Zone
☐ IPv6 Reverse Lookup Zone

< Back Next > Cancel

New Zone Wizard

Reverse Lookup Zone Name
A reverse lookup zone translates IP addresses into DNS names.

To identify the reverse lookup zone, type the network ID or the name of the zone.

☐ Network ID:

The network ID is the portion of the IP addresses that belongs to this zone. Enter the network ID in its normal (not reversed) order.
If you use a zero in the network ID, it will appear in the zone name. For example, network ID 10 would create zone 10.in-addr.arpa, and network ID 10.0 would create zone 0.10.in-addr.arpa.

☒ Reverse lookup zone name:

< Back Next > Cancel

This reverse lookup zone will only work on my home lab network! What this reverse lookup zone will do is tell the DC DNS system what the hostname for a domain joined PC is.

DNS Manager

New Zone Wizard

Zone File

You can create a new zone file or use a file copied from another DNS server.

Do you want to create a new zone file or use an existing file that you have copied from another DNS server?

☒ Create a new file with this file name:

1.168.192.in-addr.arpa.dns

☐ Use this existing file:

To use this existing file, ensure that it has been copied to the folder %SystemRoot%\system32\dns on this server, and then click Next.

DNS Manager

New Zone Wizard


Dynamic Update

You can specify that this DNS zone accepts secure, nonsecure, or no dynamic updates.

Dynamic updates enable DNS client computers to register and dynamically update their resource records with a DNS server whenever changes occur.

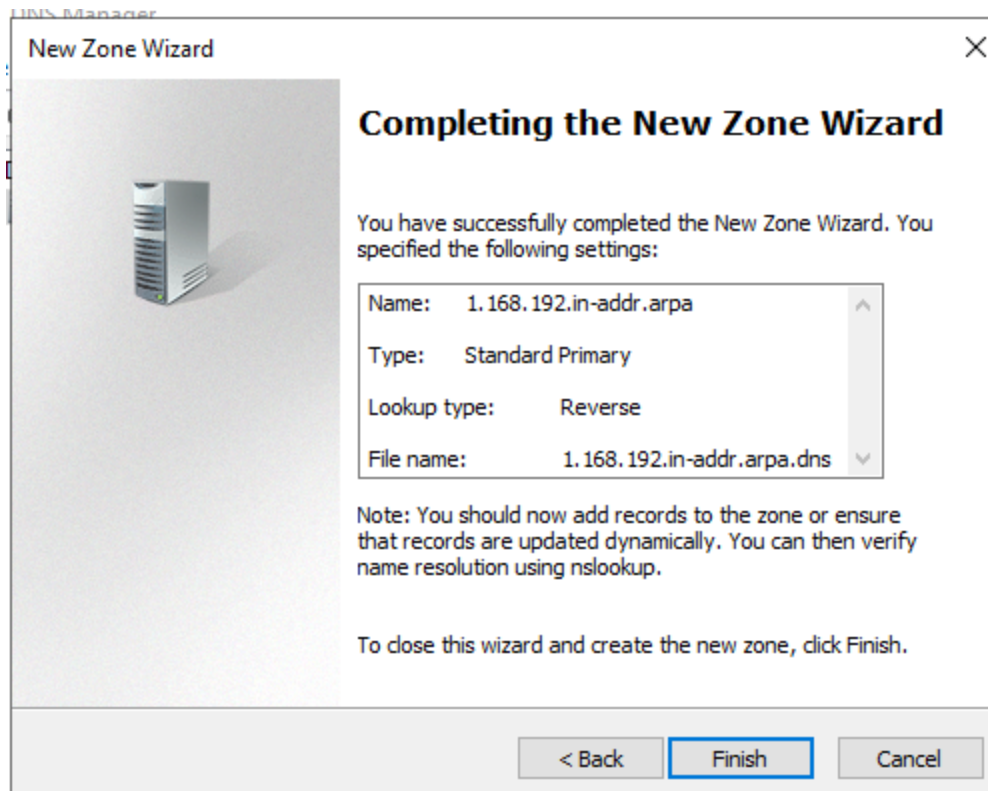
Select the type of dynamic updates you want to allow:

☐ Allow only secure dynamic updates (recommended for Active Directory)
This option is available only for Active Directory-integrated zones.

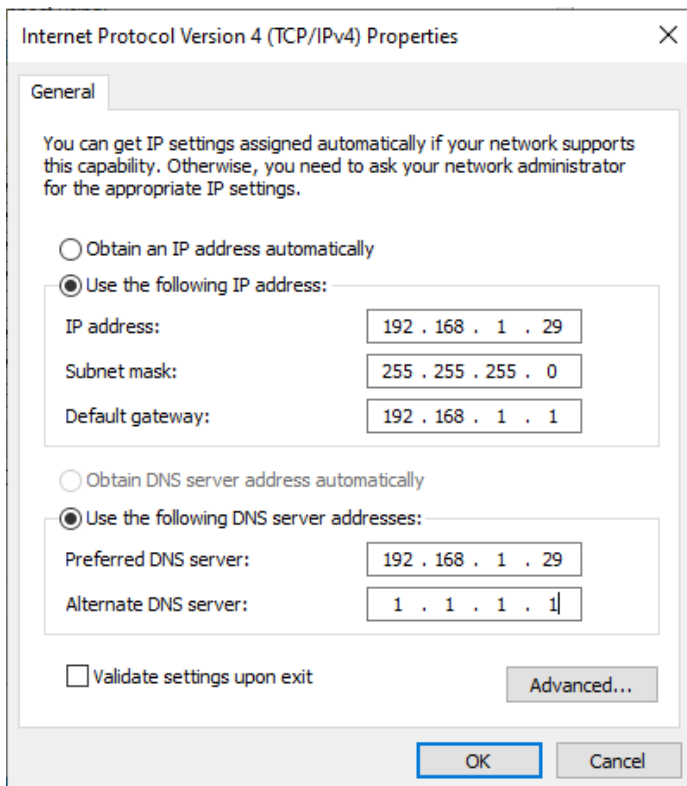
☐ Allow both nonsecure and secure dynamic updates
Dynamic updates of resource records are accepted from any client.
 This option is a significant security vulnerability because updates can be accepted from untrusted sources.

☒ Do not allow dynamic updates
Dynamic updates of resource records are not accepted by this zone. You must update these records manually.

< Back Next > Cancel



Test the DNS server:



Using nslookup I am able to resolve the domain name of the DC to its host name.

```
C:\Users\Administrator>nslookup LAB_DC.my_it_lab.local
Server: UnKnown
Address: 192.168.1.29

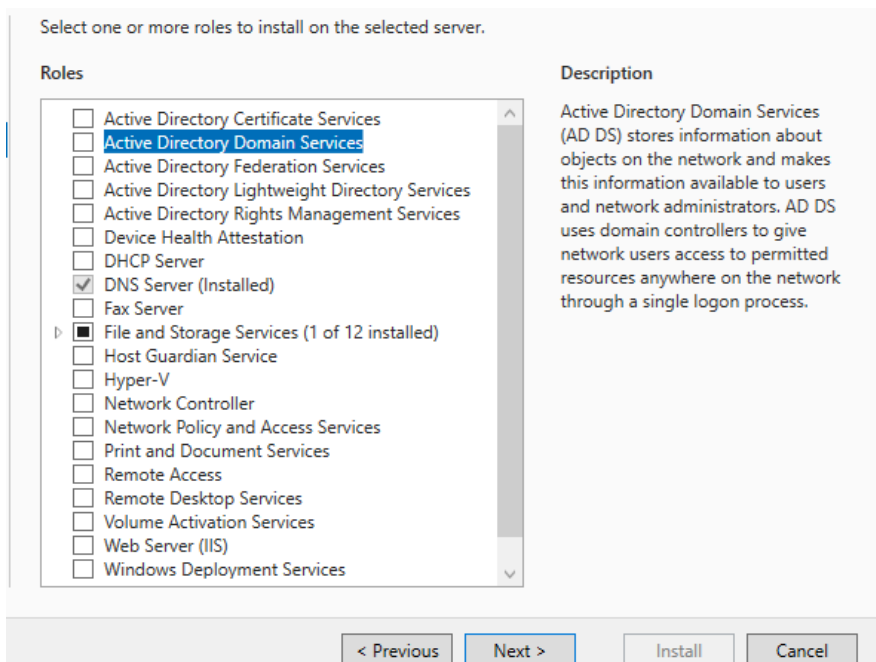
Name: LAB_DC.my_it_lab.local
Address: 192.168.1.29
```

Note: All the clients in my lab will need to use the ip address of the DC as their DNS server. They will still be able to access the internet since my DC has its own dns server and it is also connected to the router as well. If a client tries to access a website on the internet the request will be sent to the DC. The DC will then send the request to its own DNS server.

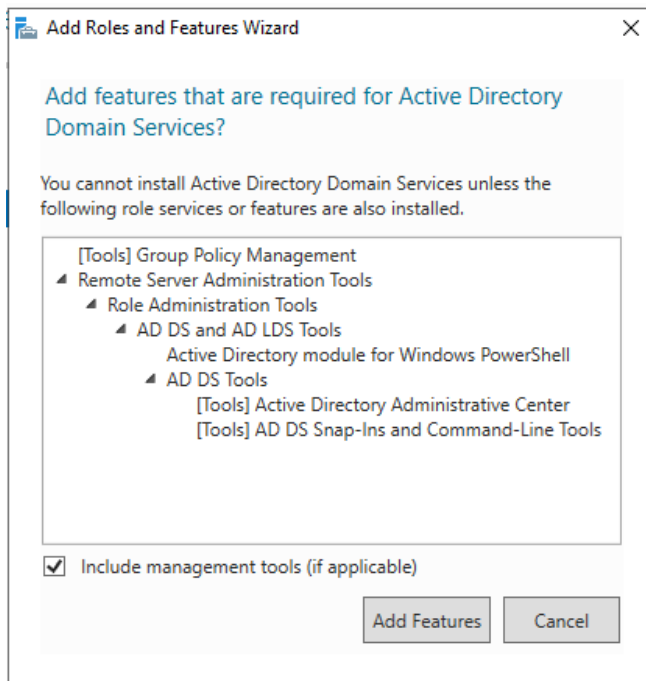
Section #3 Installing and Configuring AD

3.1 Add the AD server role to the server.

Choose the AD DS role



The following are the features that are included with the AD DS service. These features are RSAT (for secure remote management of the DC), AD DS(group policy editor, users and computers), and LDS Tools (LDAP).



I added these features, then a summary about what the AD DS is provided.

Active Directory Domain Services


DESTINATION SERVER
LAB-DC

- 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](#)

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](#)

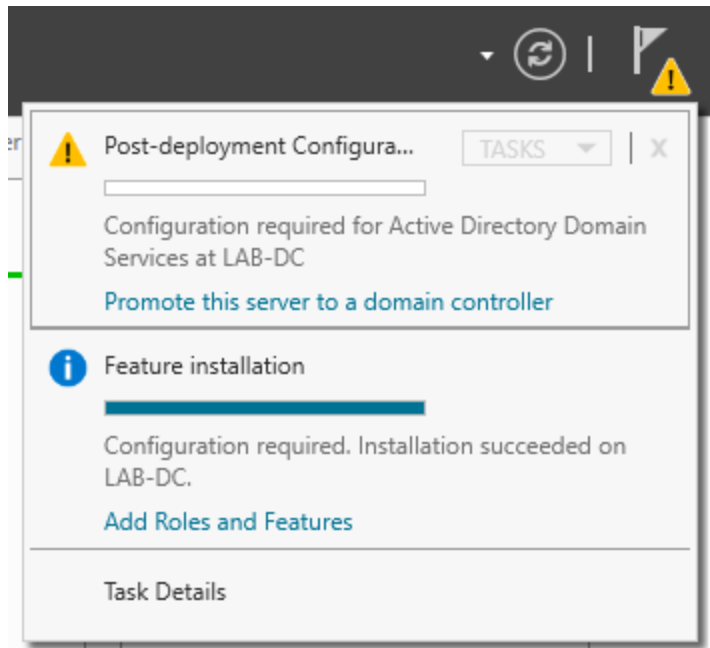
< Previous Next > Install Cancel

I installed the role and its tools. Now the role is up on the server. I still need to configure AD though

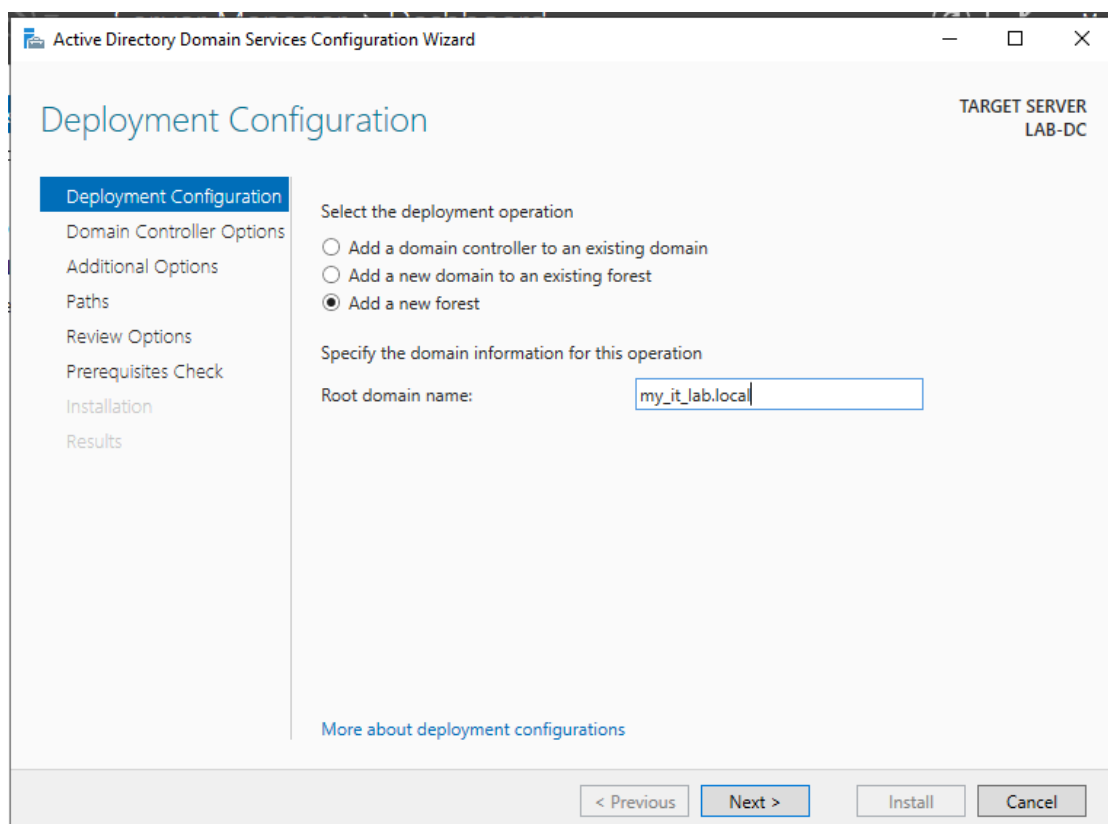
<p> AD DS 1</p> <p> Manageability</p> <p>Events</p> <p>Services</p> <p>Performance</p> <p>BPA results</p>	<p> DNS 1</p> <p> Manageability</p> <p>Events</p> <p>Services</p> <p>Performance</p> <p>BPA results</p>
<p> File and Storage Services 1</p> <p> Manageability</p> <p>Events</p> <p>Performance</p> <p>BPA results</p>	<p> Local Server 1</p> <p> Manageability</p> <p> 2 Events</p> <p> 1 Services</p> <p>Performance</p> <p>BPA results</p> <p>1/19/2025 2:16 PM</p>

3.2 Configure AD

Even though AD is installed on the system it still needs to be configured properly.



This AD DC will create a new forest since this lab is fresh and I don't have any existing forests.



Set the Directory Services Restore Mode password so that I have the ability to restore or repair my Active Directory environment if something goes wrong.

Domain Controller Options

TARGET SERVER
LAB-DC

[Deployment Configuration](#)
Domain Controller Options
[DNS Options](#)
[Additional Options](#)
[Paths](#)
[Review Options](#)
[Prerequisites Check](#)
[Installation](#)
[Results](#)

Select functional level of the new forest and root domain

Forest functional level:

Domain functional level:

Specify domain controller capabilities

☒ Domain Name System (DNS) server

☒ Global Catalog (GC)

☐ Read only domain controller (RODC)

Type the Directory Services Restore Mode (DSRM) password

Password:

Confirm password:

[More about domain controller options](#)

[< Previous](#) [Next >](#) [Install](#) [Cancel](#)

I will set the DNS up later.

DNS Options

TARGET SERVER
LAB-DC



[Deployment Configuration](#)
[Domain Controller Options](#)
DNS Options
[Additional Options](#)
[Paths](#)
[Review Options](#)
[Prerequisites Check](#)
[Installation](#)
[Results](#)

Specify DNS delegation options

☐ Create DNS delegation

[More about DNS delegation](#)

[< Previous](#) [Next >](#) [Install](#) [Cancel](#)

 A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found... [Show more](#) 

Set a NetBIOS name which will be used by certain Windows services.

The screenshot shows the 'Additional Options' page of the Active Directory Domain Services Configuration Wizard. The title bar reads 'Active Directory Domain Services Configuration Wizard'. On the right, it says 'TARGET SERVER LAB-DC'. The left sidebar contains a list of steps: Deployment Configuration, Domain Controller Options, DNS Options, Additional Options (highlighted), Paths, Review Options, Prerequisites Check, Installation, and Results. The main area has the heading 'Additional Options' and a sub-heading 'Verify the NetBIOS name assigned to the domain and change it if necessary'. Below this, it says 'The NetBIOS domain name:' followed by a text box containing 'MY_IT_LAB'. At the bottom, there are buttons for '< Previous', 'Next >', 'Install', and 'Cancel'. A link 'More about additional options' is at the bottom left.

Paths for the AD data. This is a lab so it does not matter where the data is stored.

The screenshot shows the 'Paths' page of the Active Directory Domain Services Configuration Wizard. The title bar is the same as the previous page. On the right, it says 'TARGET SERVER LAB-DC'. The left sidebar is the same, with 'Paths' highlighted. The main area has the heading 'Paths' and a sub-heading 'Specify the location of the AD DS database, log files, and SYSVOL'. Below this, there are three rows: 'Database folder:' with a text box containing 'C:\Windows\NTDS' and a browse button (...); 'Log files folder:' with a text box containing 'C:\Windows\NTDS' and a browse button (...); and 'SYSVOL folder:' with a text box containing 'C:\Windows\SYSVOL' and a browse button (...). At the bottom, there is a link 'More about Active Directory paths'.

Now the system has to do prerequisite checks to ensure that it can be an AD DC.

Prerequisites Check

TARGET SERVER
LAB-DC

Deployment Configuration

Domain Controller Options

DNS Options

Additional Options

Paths

Review Options

Prerequisites Check


Installation

Results

Prerequisites need to be validated before Active Directory Domain Services is installed on this computer

Verifying prerequisites for domain controller operation...

View results

 If you click Install, the server automatically reboots at the end of the promotion operation.

[More about prerequisites](#)

< Previous

Next >

Install

Cancel

Prerequisites Check

TARGET SERVER
LAB-DC

Deployment Configuration

Domain Controller Options

DNS Options

Additional Options



Paths

Review Options

Prerequisites Check

Installation

Results


 All prerequisite checks passed successfully. Click 'Install' to begin installation. [Show more](#) 


Prerequisites need to be validated before Active Directory Domain Services is installed on this computer


[Rerun prerequisites check](#)


View results


go.microsoft.com/fwlink/?Linkid=104731.

 The domain name "my_it_lab.local" contains the underscore character (_). Microsoft DNS servers allow underscore characters in the DNS records. However, other DNS server products may not.

 A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found or it does not run Windows DNS server. If you are integrating with an existing DNS infrastructure, you should manually create a delegation to this DNS server in the parent zone to ensure reliable name resolution from outside the domain "my_it_lab.local". Otherwise, no action is required.

 Prerequisites Check Completed

 All prerequisite checks passed successfully. Click 'Install' to begin installation.

 If you click Install, the server automatically reboots at the end of the promotion operation.

[More about prerequisites](#)

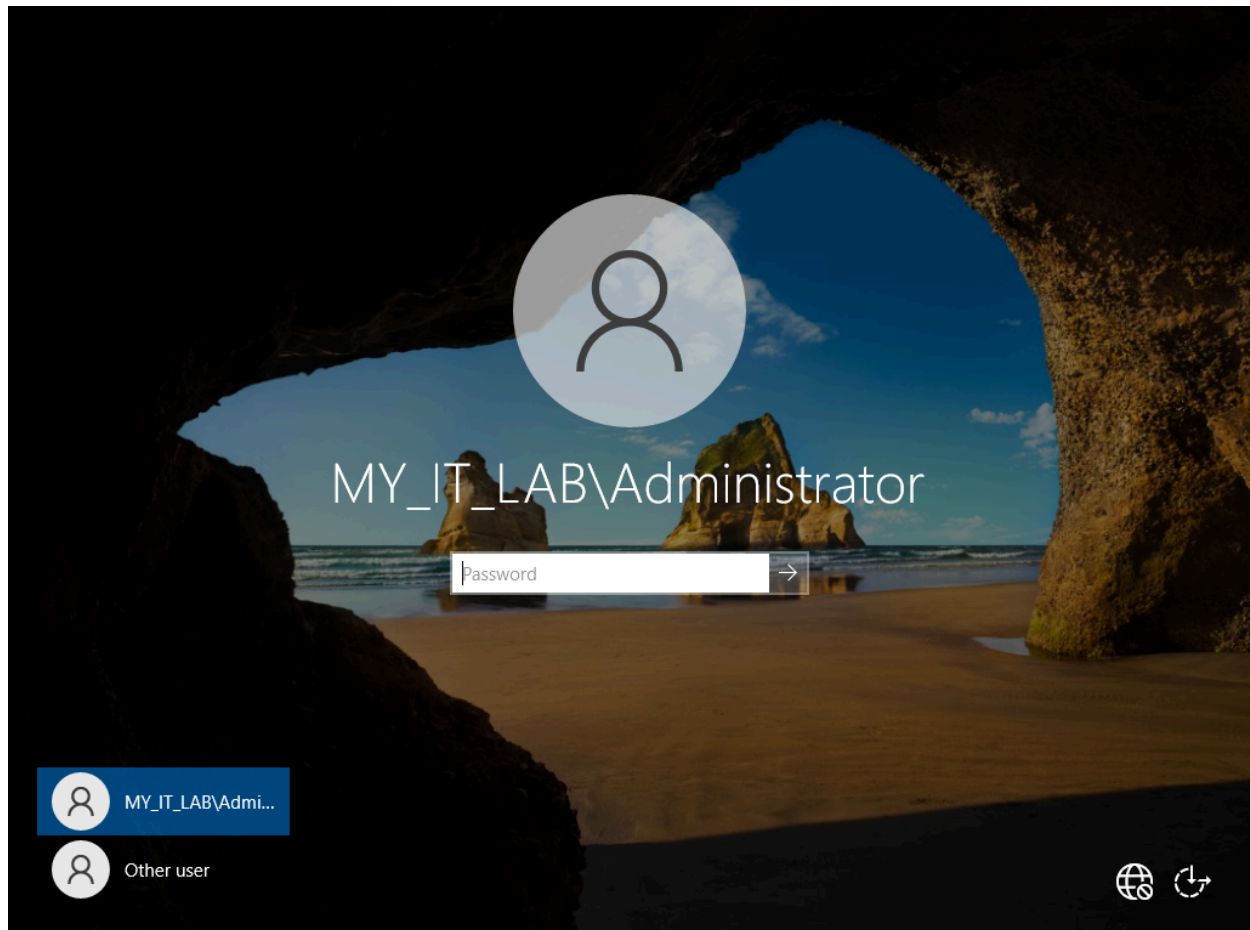
< Previous

Next >

Install

Cancel

All good! Now after the system reboots I can sign into the VM.



The domain has been created. Active Directory has been set up!

