Rawad Youssef

Windows Server course

# Windows SERVER 2025 Course

## Setup

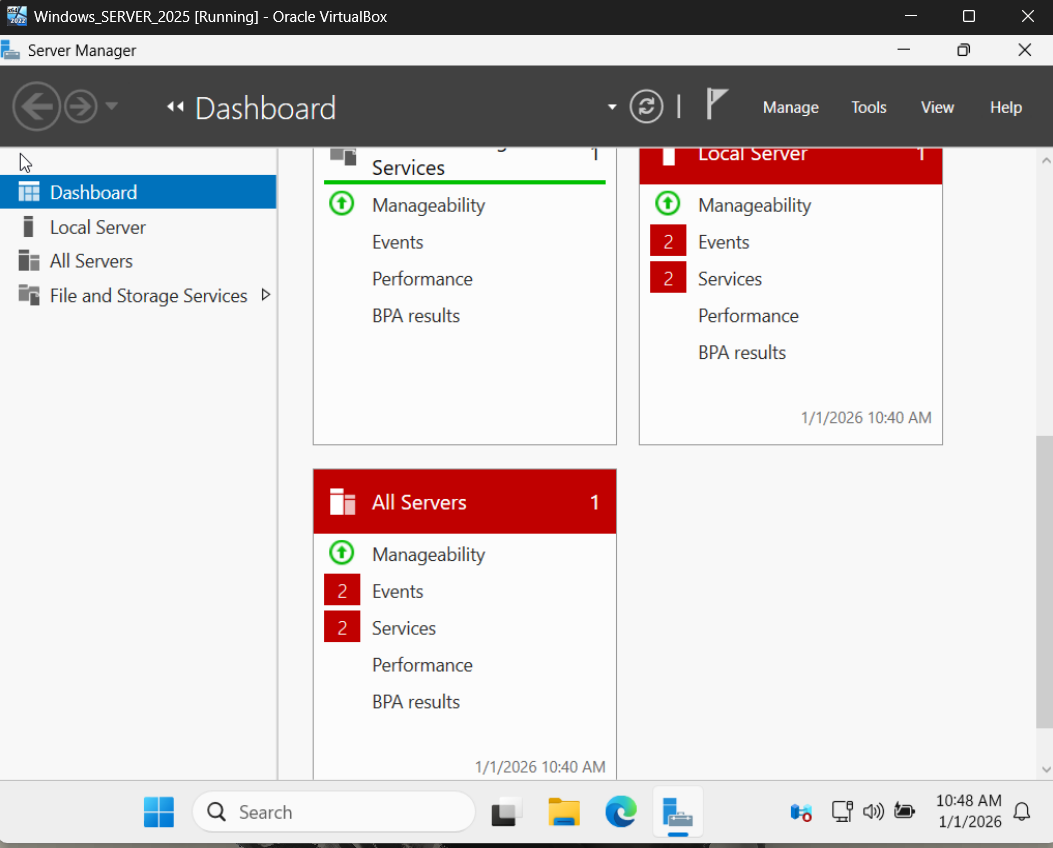
2 VM instances

* Windows 10 VM to simulate users
* Windows SERVER 2025 VM

Both latest ISO images

VM used: VirtualBox

## Basic Server Configuration



By default, the server manager app open on the server

Server manager is a tool to manage everything in the server , including roles and other tasks

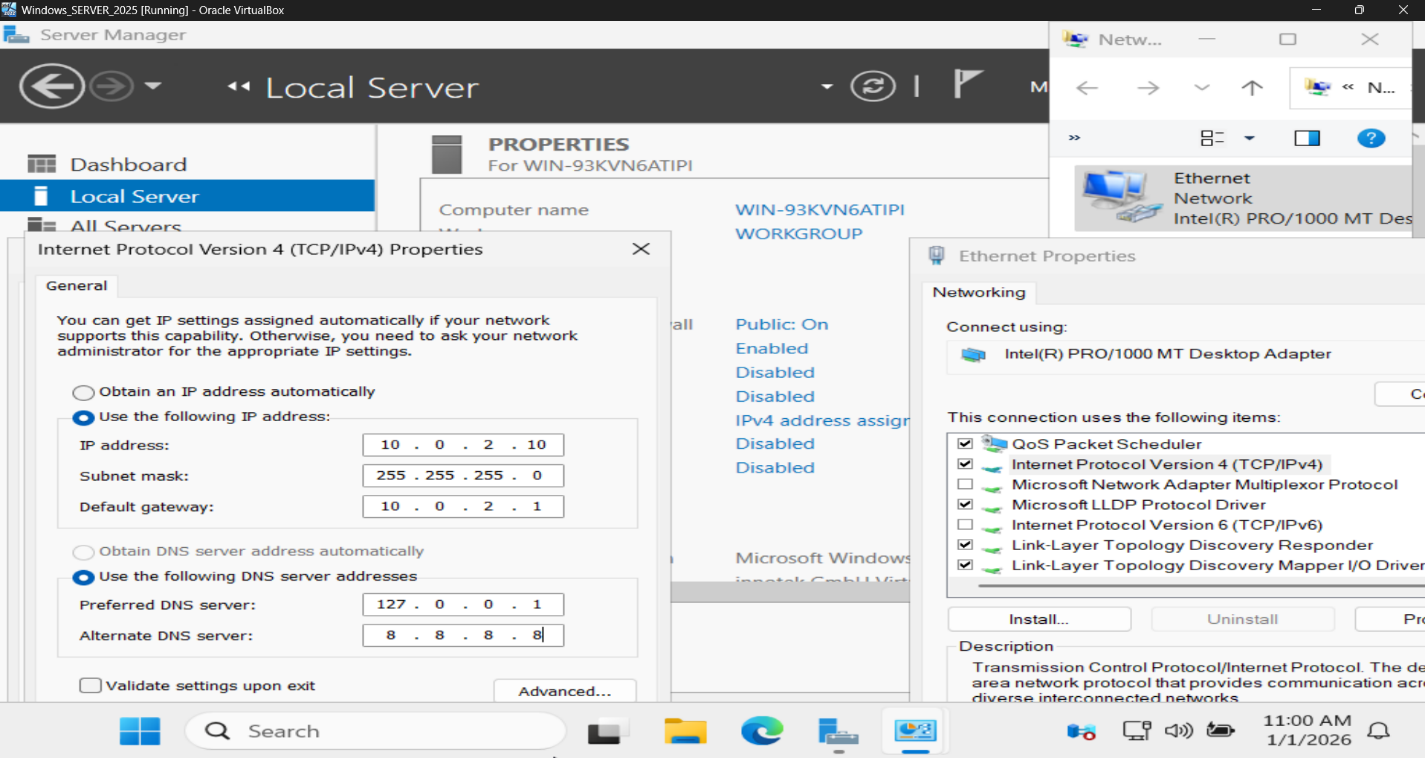
1. Add a static IP

Go to Local Server TAB

It show info about : Services , roles and features

Also shows logs with SEVERITY levels

And Local SERVER properties eg. Static IP



To add the IP in Local SERVER TAB, CLICK on ETHERNET

And configure the IP as if on normal windows 10

IP here must match the NAT network created in the VM

DNS address 1: 127.0.0.1 Since the server will act as the domain controller

Backup DNS: 8.8.8.8 googles DNS, also resolve domain name to reach out to the internet

1. Change the computer Name

Click in Local Server tab, computer Name

And change it to a readable Name(LABDC01)

## Windows Servers Fundamentals

All windows Servers have server manager (All version)

It allows to manage the local server and the servers on the local network

Like a server and network management tool

We can manage Ip addresses, view events and services, firewall setting and much more

Depending on the version of the server it may have 4 or 3 tabs:

1. Dashboard is the general info (Local or remote server info)
2. Local server is the server we are using
3. All server to see and manage other servers
4. The 4th tab is a role that may be preinstalled on newer version:

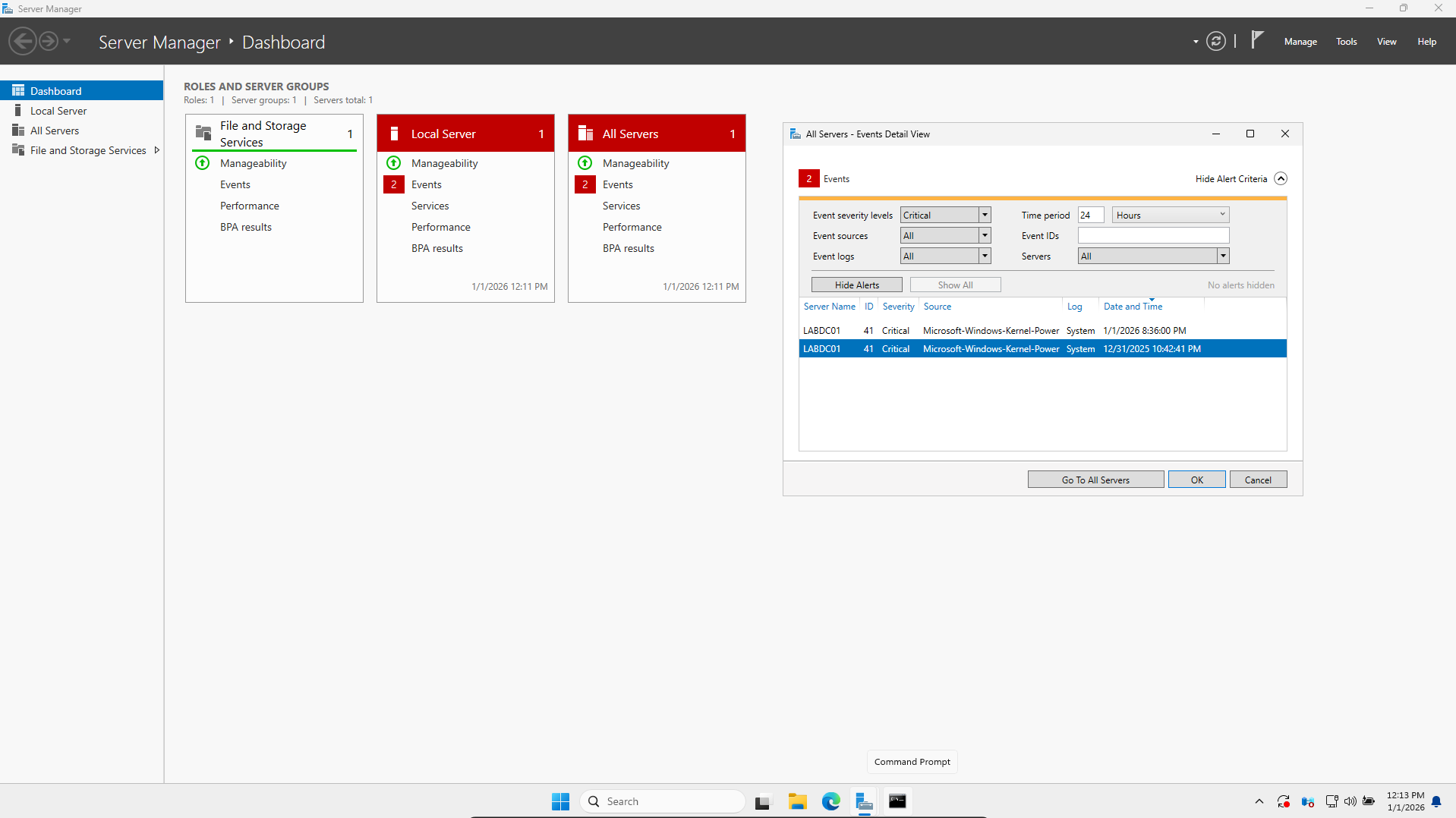
The files and storage services

If we add any role to the server, it shows a new tab for it on the left

1. Dashboard

Gives a quick overview of the server and allows quick access to roles, local or remote servers for quick configurations

Also, dashboard will show errors, like a service that failed to start:



Here we can see a critical log error, due to system randomly shutting down

Local errors will also show on All server’s events.

To see events of remote server they must be remotely manageable

(Added as a remotely managed server)

1. Local server Tab

Gives Detailed info of the current server logged on to.

Allow to modify the servers network info, firewall settings (remote access) e.g., IP, Computer Name

Show logs(events) with much more detail

Also shows much more Info like services and roles

1. All servers

Show the same Info as the local server tab, except does not allow to change any settings like the local server

Will show events, services, roles of the local and remote servers

1. File and storage Services

Includes technologies to setup one or more file servers which allows user to access configured file remotely from the file servers

Important key terminology:

Roles and Features

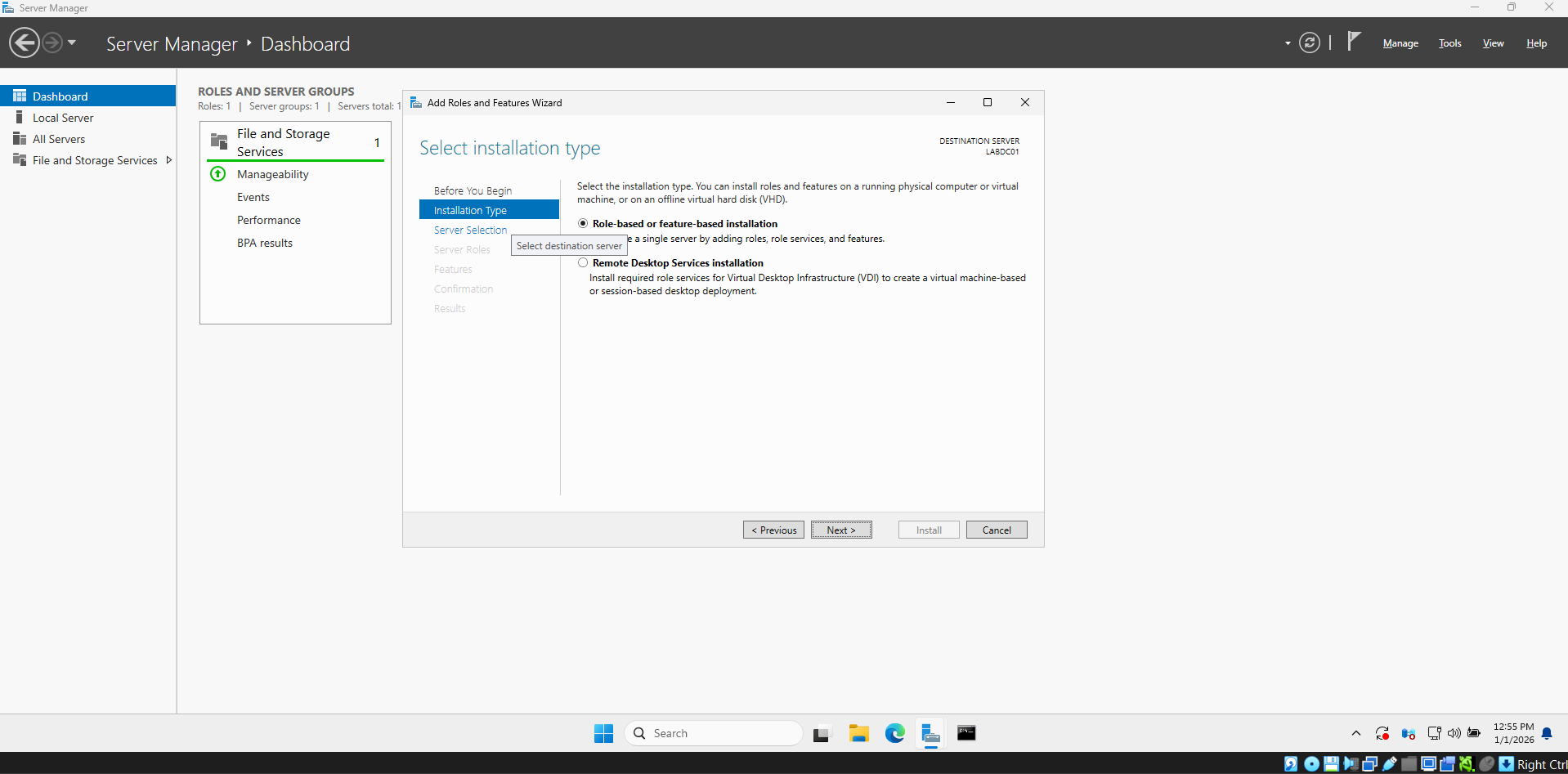
Roles: A set of software program, a set of tools that allows the server to provide a specific service to its network. (e.g., DHCP role for the server to act as a DHCP server)

Features: A single software program that also allows the server to provide a certain service. Some features may be needed to be installed with roles and also, they can be installed independently.

To access them on the Top left menu, click on the Manage tab.

This allows us to:

1. Add roles and features



We have two installation types:

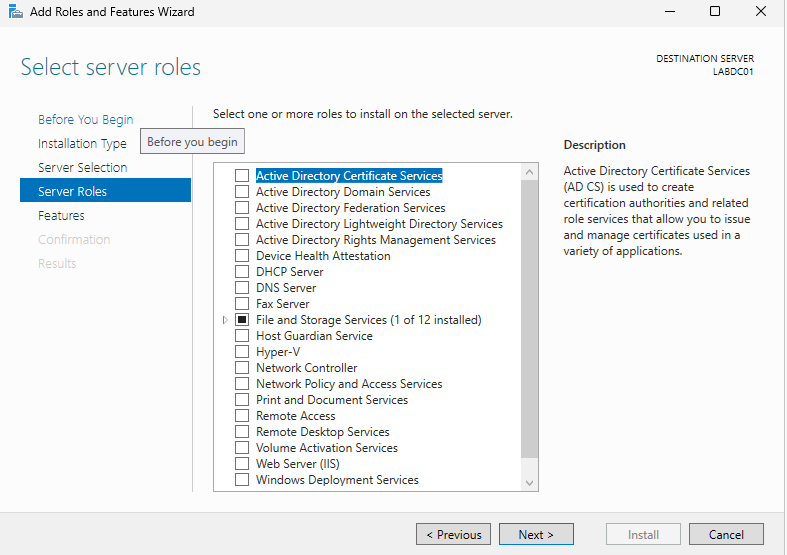
1. Installation on the server we are using
2. Installation for VDI (To create a virtual machine-based program for this role)

Then we Select the location of the installation

Our options are:

1. On the chosen server from the server pool(might be remote or local server)
2. On virtual hard disk (Used in case of Hyper-V/Type 1 Hypervisor)

Then onto the roles TAB(if we are only add/remove features then we can skip this)



If we check a role, it will open a window that allow us to automatically check all the features needed for that role.

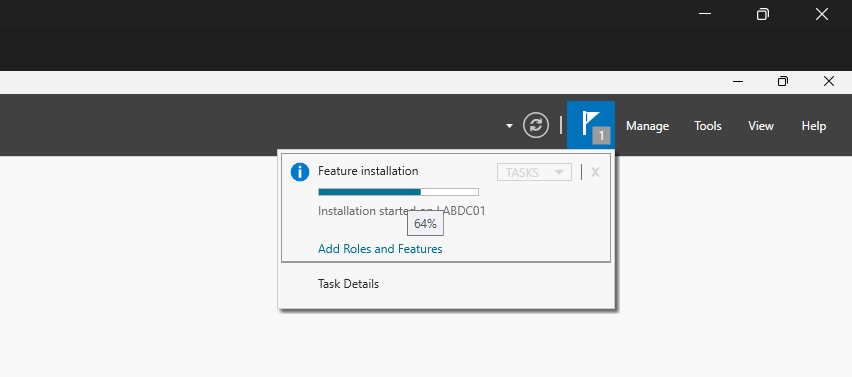
After clicking next, we are now in the features tab.

The features that are needed for the role we have just checked will be checked automatically.

If no role has been chosen since it can be skipped, we can still add features and which we must at least do to complete the requirements of the wizard.

After clicking next, some info about the role will be provided with recommended roles to install

After we can finally install the role.



After the installation, for any role , we must do the post deployment configuration to truly deploy the role on the server.

1. Remove server roles and features

Same exact process as adding

Uncheck the desired roles.

If no role to be removed then skip

But at least features must be unchecked.

If a role is unchecked it also does the same to its related features.

And finally remove.

## Active Directory Domain Service basic deployment

We will install the ADDS role.

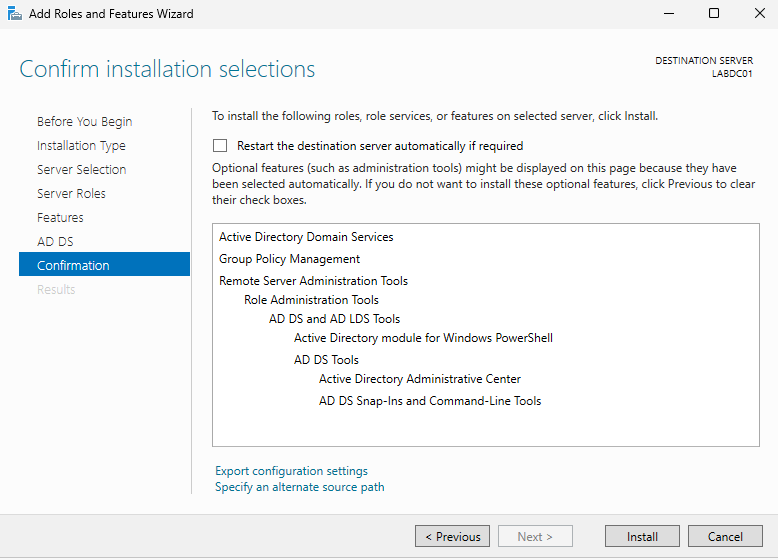
Any Server that has the ADDS role installed is a domain controller.

AD DS allows a Domain Controller to centrally manage users, computers, and resources that have joined the domain, assign them permissions and policies, and authenticate them, all under a shared domain identity identified by the domain name.

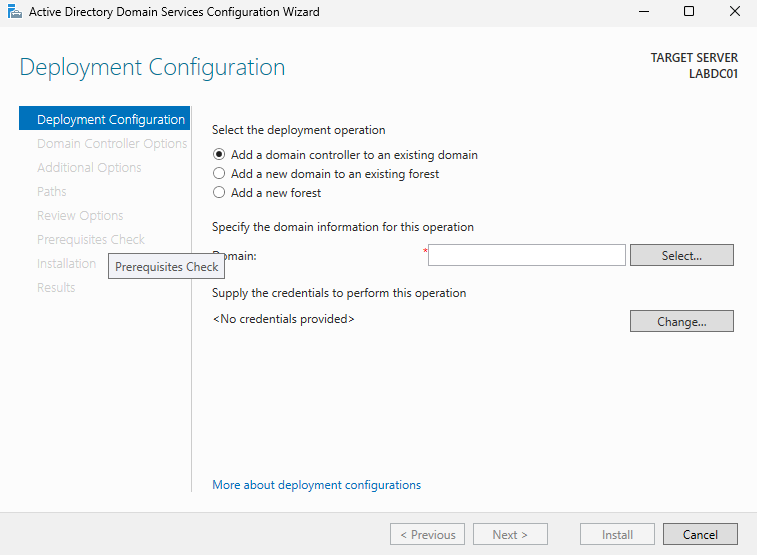
**One server (Domain Controller) usually belongs to ONE domain.**  
Multiple domains exist for **administrative, security, or organizational reasons**, not because of networking limits.

Which means the best and latest practice is one server=one domain.

Now we Install the ADDS role:



After the installation, we must do the post deployment configuration.



Here we have 3 options:

1. Add a domain controller to an existing domain
2. Add a new domain to an existing forest

In this case forest is the main domain and the domain to this forest is the subdomain. E.g.: students.school.com

School is the forest, students is the subdomain

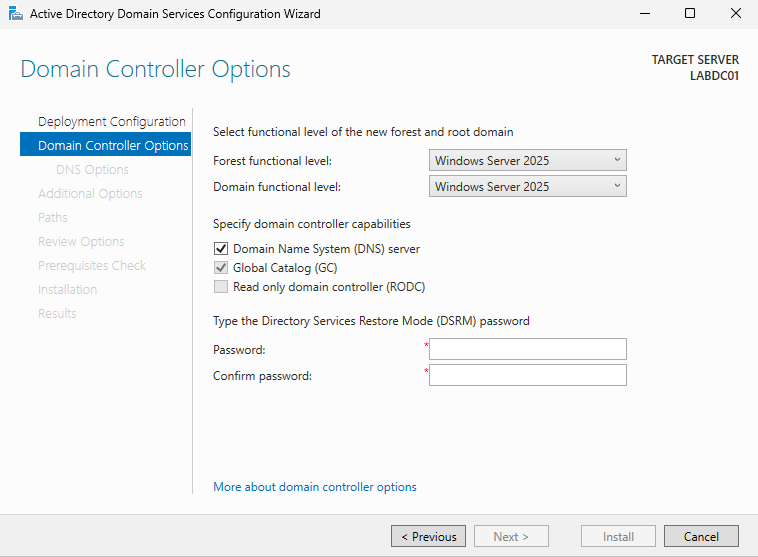
This allows the subdomains to be isolated and cannot reach out.

But the main forest can reach in the subdomain.

1. Add a new forest, allow us to add a new domain. This is the choice in our case for post deployment configuration.

Forest format: name.extension e.g.: wslab.com

Onto the next Tab:



Functional level is the OS that the domain controller will use.

In our case, its same as the local server.

Make sure DNS is checked so the domain name can be resolved.

And set the DSRM password

(DRSM is used to take an instance of AD offline in cases of troubleshooting/maintenance)

Uncheck the DNS delegation box.

This means that people on the internet won’t be able to access the domain and subdomains.

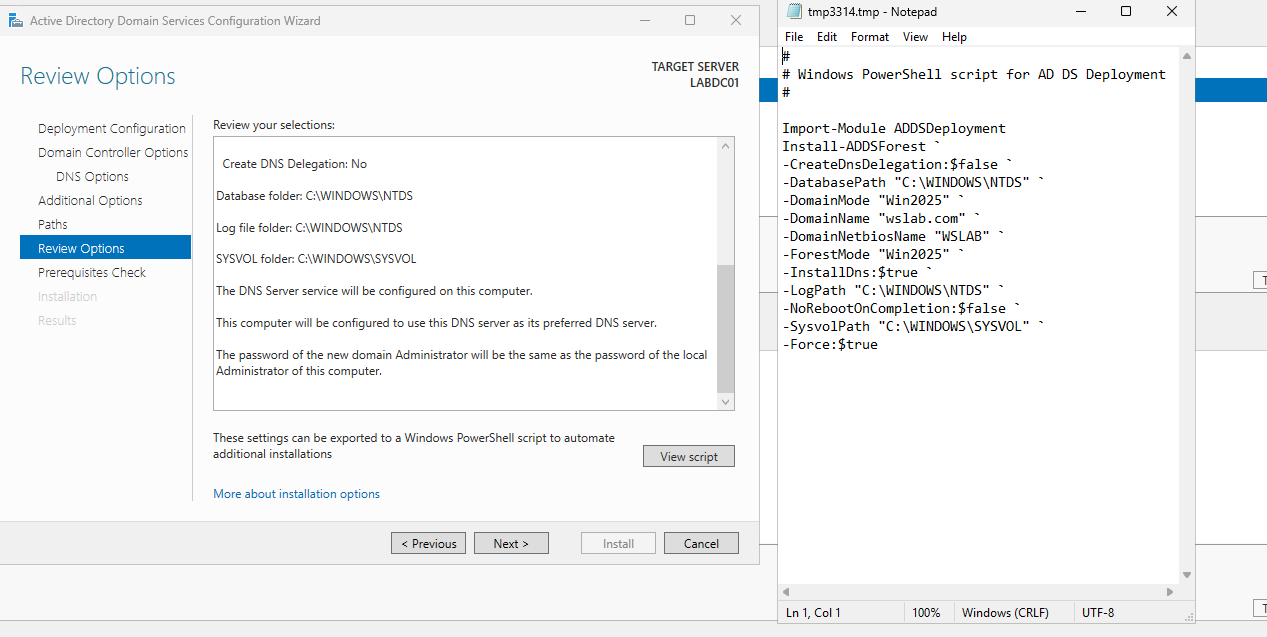
In our case its fine because we only access it inside our network and don’t want to cause issue for website with same domain.

We can change the NetBIOS domain name too, this is the name that will show on the devices that represents the domain.

In our case keep it.

Same for AD path where ADDS path for files are stored.

We can change them to the desired drive.



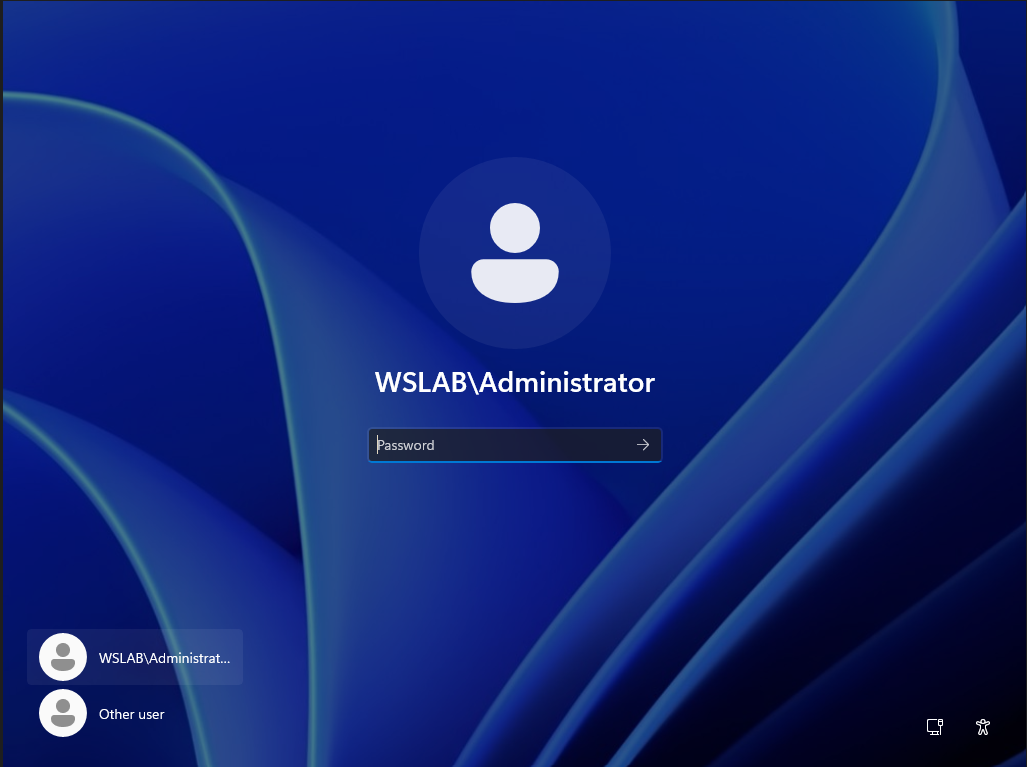
An overview of our setup, with a provided script.

After run prerequisite check.

If an error appears then it is best then check it out, fix it and then install.

After its installed, we have to login into the server as the domain controller administrator.

So as WSLAB\ADMINISTRATOR where WSLAB is the BIOS domain name.

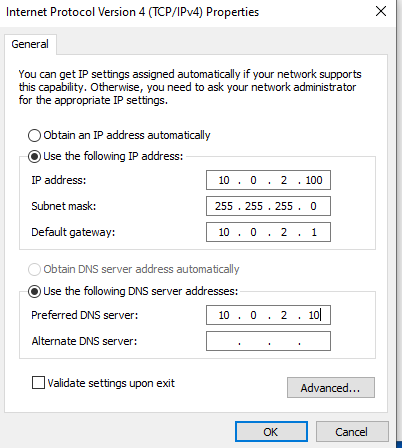


And Now ADDS and DNS roles is installed.

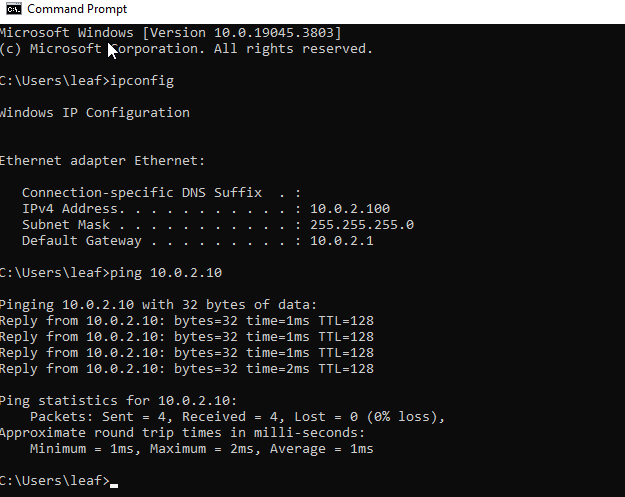
## Joining our domain from a window 10 VM

Since we have not installed the DHCP role yet we have to manually configure the windows 10 IP on the VM to make sure they are on the same network.

Both of the VM are in the same NAT network 10.0.2.0/24



Now we check for connectivity



We have an IP and we are able to ping the server.

Now we join the domain.

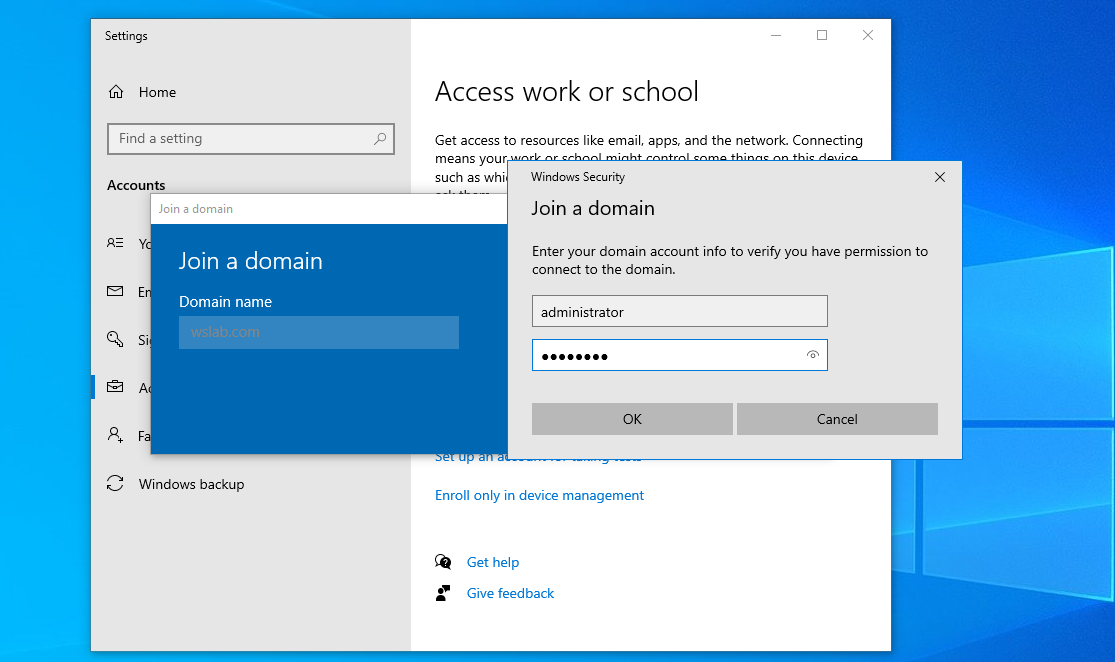
The PC name is LABWS01.

In setting ->system ->About->Rename (to change name)

A good PC name is important, later on it is used to login.

In setting->Accounts->Access work or school->connect->Join this device to a local AD domain

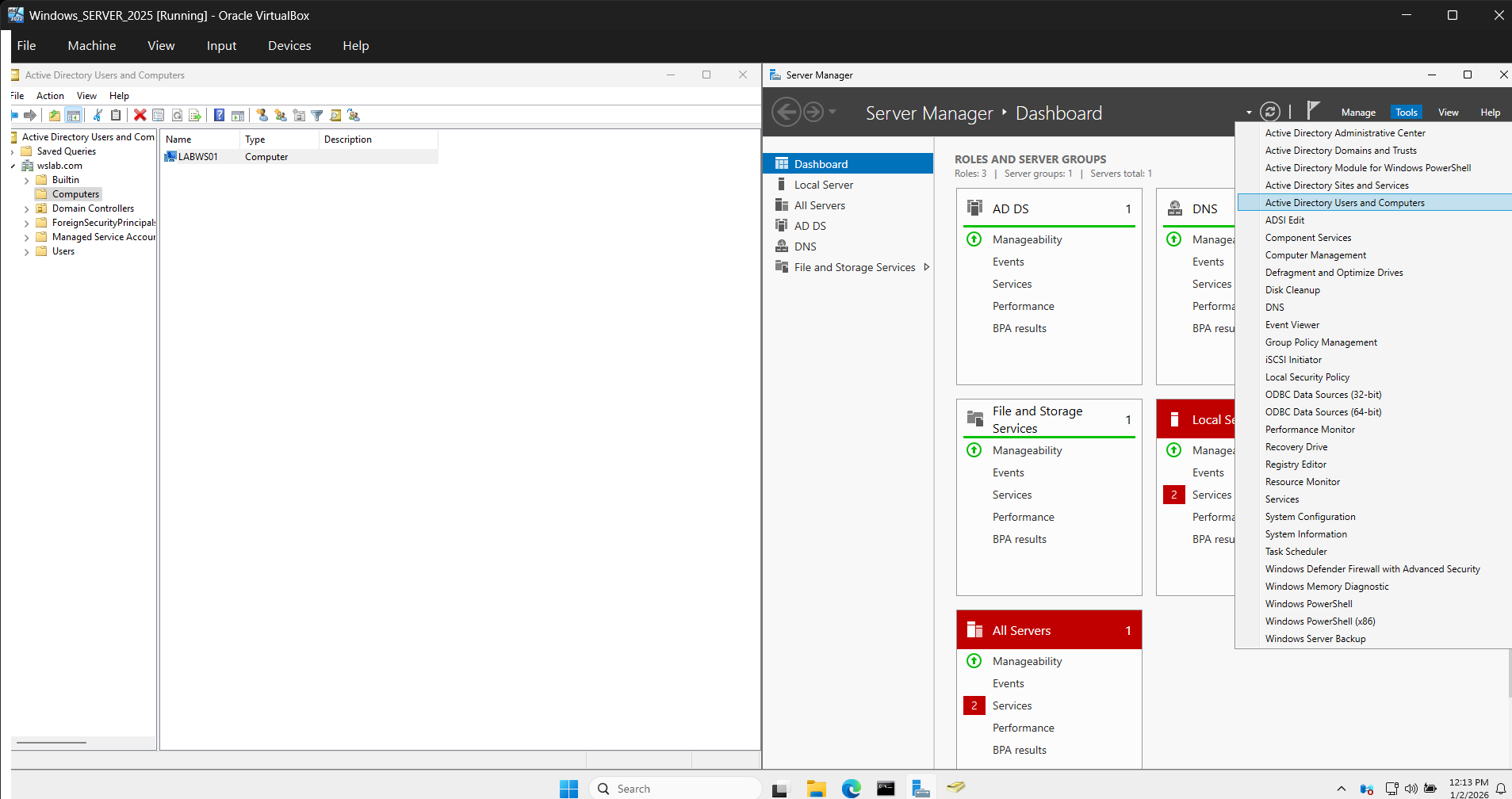
It will open the connection window which will allow us to join the domain.



We provide the domain, and login as administrator.

And then we restart.

Now we login into the domain controller.



We can see in ADDS users and computers->WSLAB (domain name)->computers.

We can see a new computer instance have been added.

## Windows domain and domain controller

Windows domain: Allows administrators (Domain controllers/DC) to manage a large group of computers on the same network.

A windows domain can have more than one DC, but there is always a primary DC the rest is backup for redundancy.

Domain controller: Any server that has the ADDS service installed.

The server Job is to:

1. Manage the computers in the domain, give privileges, and more using the tools AD and Group policy.
2. Handle authentication request across the domain, all request done from/to a user inside the domain are passed to the server to be checked.

The Active directory users and computers tool:

Used to manage the AD objects which are users accounts (windows users), computers that joined the domain, groups and acts as a directory service for resources on the network (printers, file shares …) so that users can find all services on the network easily using AD.

Group objects: Groups contain members which can be any AD object (user, computer, printer, …). By default, there are several groups already made with AD, e.g., domain Admins, domain users, and more.

The folders that store AD objects are called organizational units (OUs).

An important AD tool is GP (Group policy):

Group policy management tool: Allows to manage all the domain users and domain computers remotely.

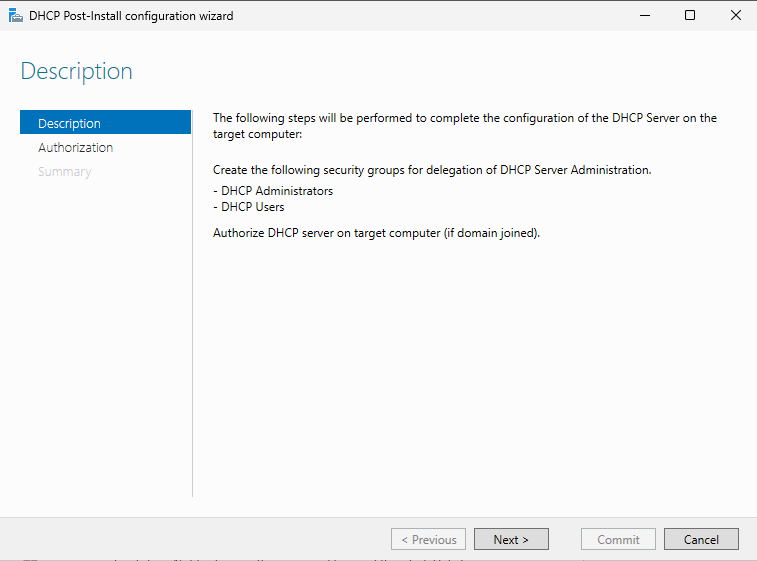
Uses group policy objects to remotely manage the settings of AD objects.

GPOs allows to configure anything like desktops, privileges, and more remotely from the DC.

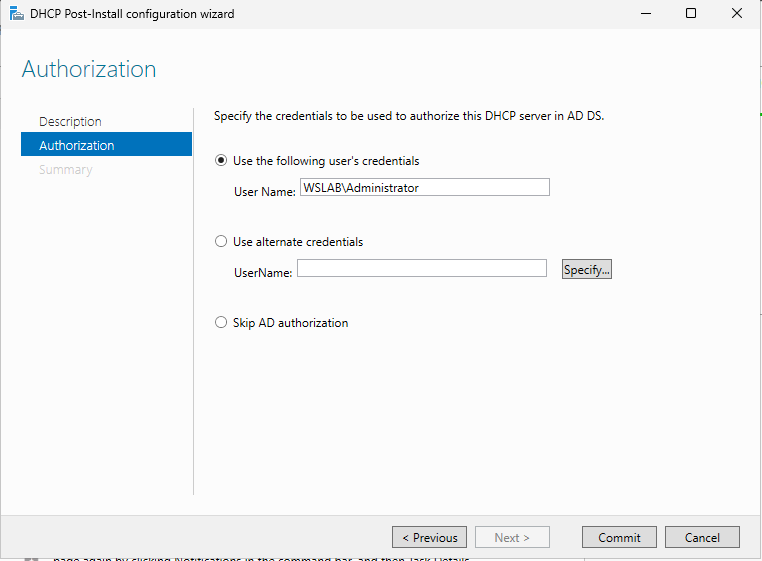
## Adding DHCP to the DC

We will follow the same process to add the roles and features for DHCP on our server.

After the installation we complete the DHCP configuration from the DHCP config wizard.



We will need to create the administrators and users’ security groups which will be done automatically, and authorize the desired device in our ADDS domain.

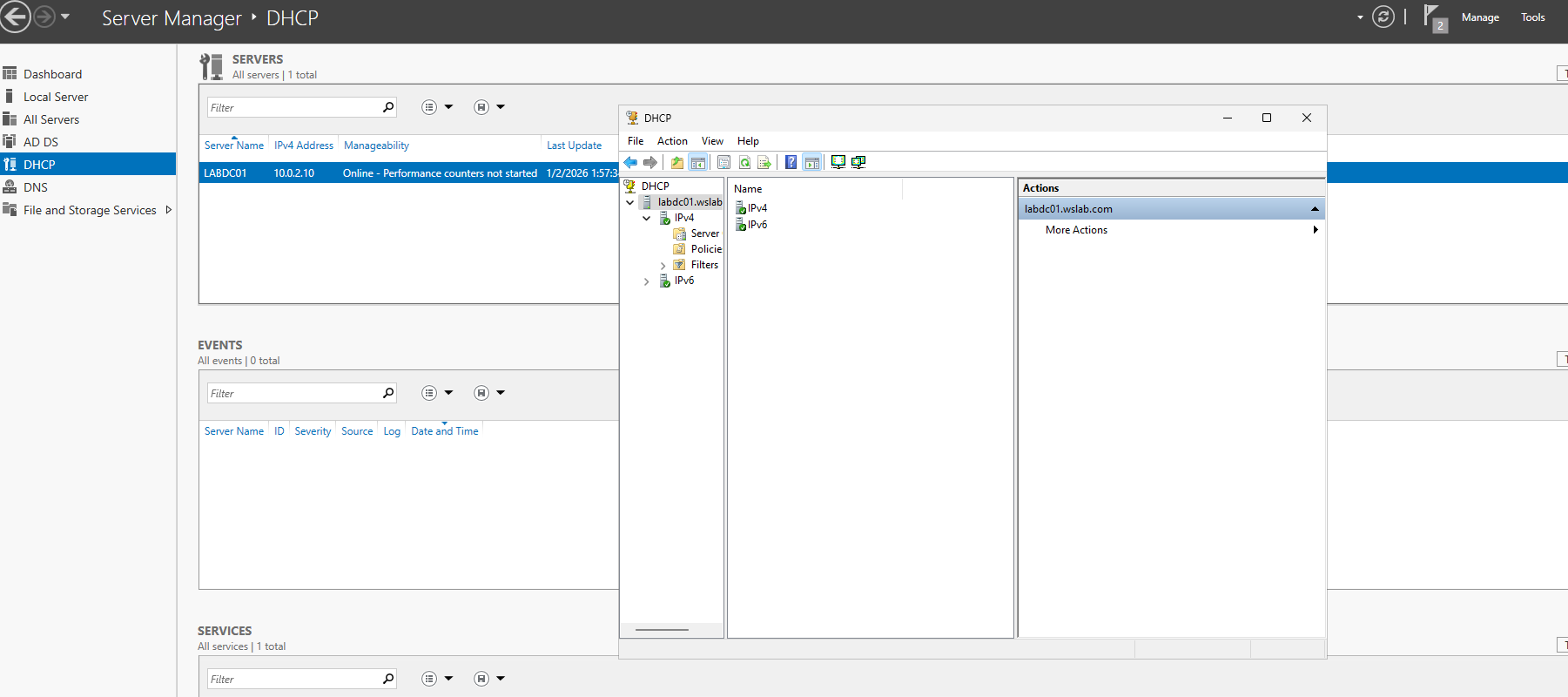


Here we must specify a user within a domain that have administrative permission.

Here we gave it the user administrator in the WSLAB domain.

We click commit, it finishes checking and installing and now we have DHCP.

To access DHCP go to, tools->DHCP



In this Tab we will be able to fully manage and configure DHCP.

Now we will specify the DHCP scope and exclusions.

The scope is the ranges of IP for the DHCP pool.

1 subnet, 1 scope.

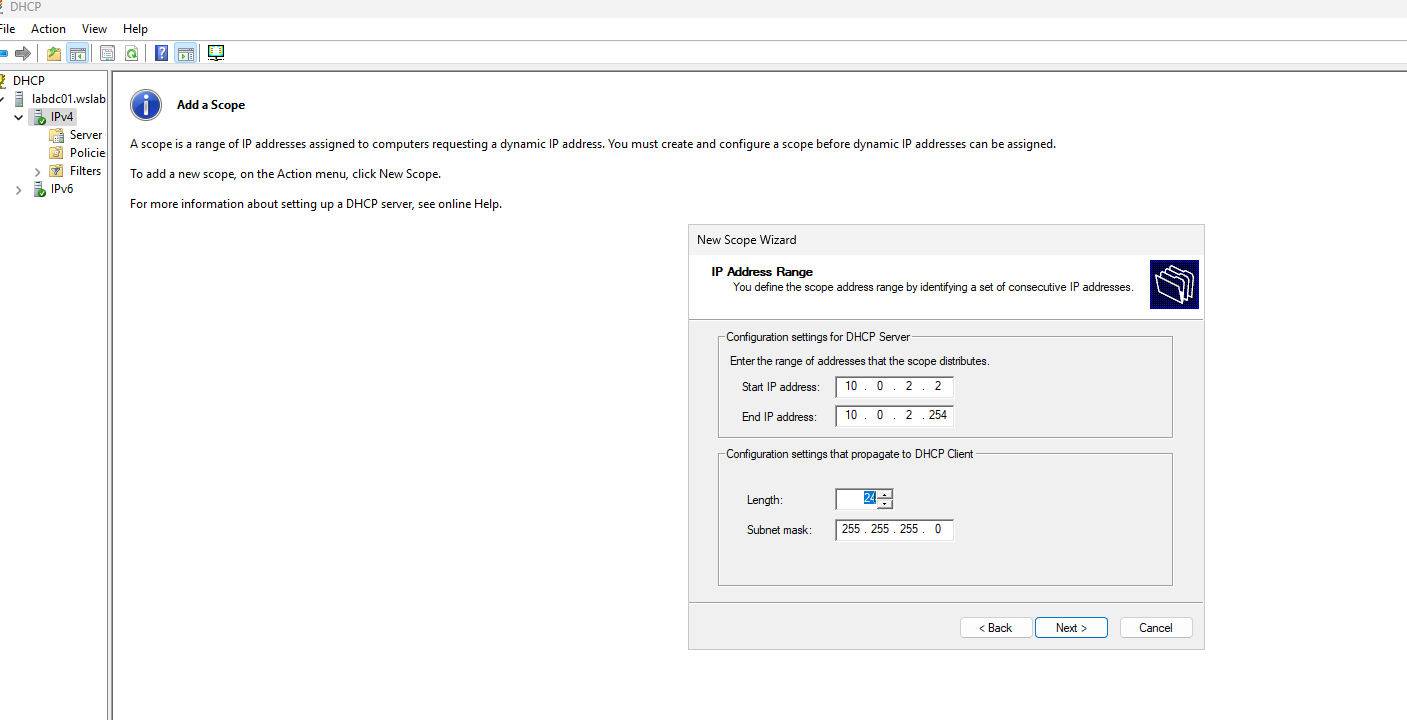
Exclusions are the IP that must not be dynamically assigned like the network address, broadcast address the server address itself, the default gateway, and statically configured addresses.

In tools->DHCP->select the server->IPV4

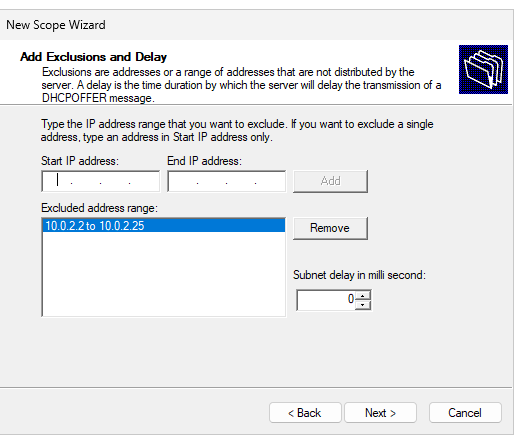
Right click->new scope

Now specify the needed info to complete the wizard.

We will do from 10.0.2.2 to .254



After we specify the basic pool info, we specify the exclusions.



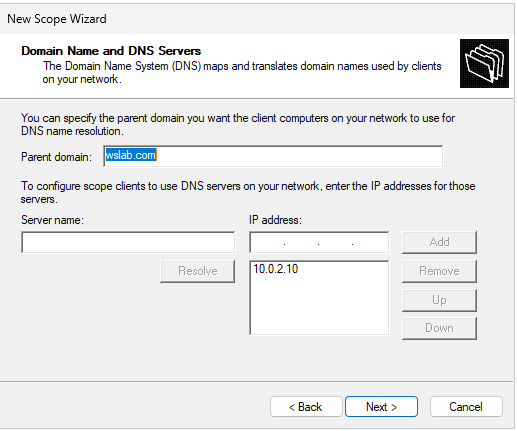
The excluded addresses MUST be a range WITHIN the previously specified range.

Here we excluded from .2 to .25 (Our server is .10)

After we asked to specified the lease time, which is the duration, the device that has taken an IP from the DHCP server pool.

When the lease time ends, the IP will no longer be assigned to this device. (Might be reassigned if “preferred”).

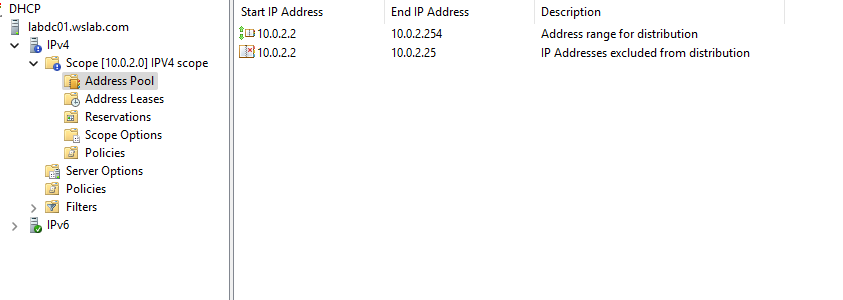
After we can choose to specify now or not the DG, DNS server and more.



We specify the info as usual.  
Our server also handles DNS since the role DNS is installed with ADDS so we give the servers IP and our domain.

We are also tasked about WINS which is like an older version of DNS. (Skip this one since DNS outdated it).

We will now have this:



We have many scope options:

1. Address Pool: List of available Ips and all exclusions
2. Address leases: Shows all devices that have received a TCP/IP configuration from DHCP (devices that have requested an IP).
3. Reservations: All devices that have a DHCP reservation (devices that received and took an IP).
4. Scope options: Allows to change settings like DG, DNS server and domain configurations.
5. Policies: Allows to assign certain range within our range to a group of devices e.g., Range 1 for IP phones only.

## DHCP basics

Before understanding DHCP we must understand static IPs

Static Ips are manually assigned addresses, and cannot change unless manually changed.

To configure a static IP address, we must know and understand what subnet mask, IP subnet, DG IP and DNS server IP.

What is DHCP?

Dynamic host configuration protocol: Allow a server to automatically assign TCP/IP configuration to device in the network. This saves time and eliminates human error.

So, on a windows server we must have the DHCP role.

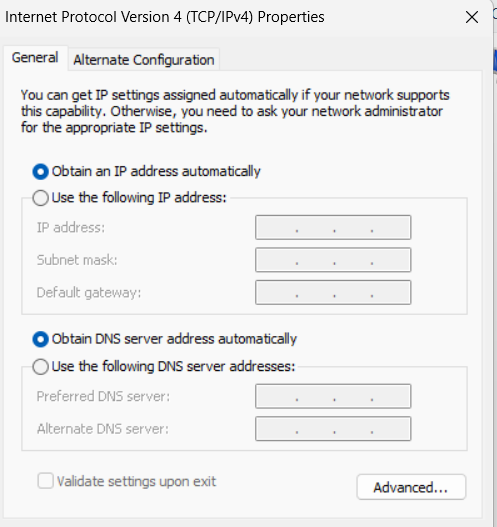
DHCP client will be any device in the network, in our case in our domain that is attempting DHCP automatic configuration.

DHCP have scopes which is the addresses range of the DHCP pool.

Within that scope we have exclusion which are Ips that must not be assigned from the pool. They can be used later for static configurations.

Reservations are also within the scope, and they are IP reservation for a certain device. E.g., 192.168.1.100 for MAC AAA: FFF.

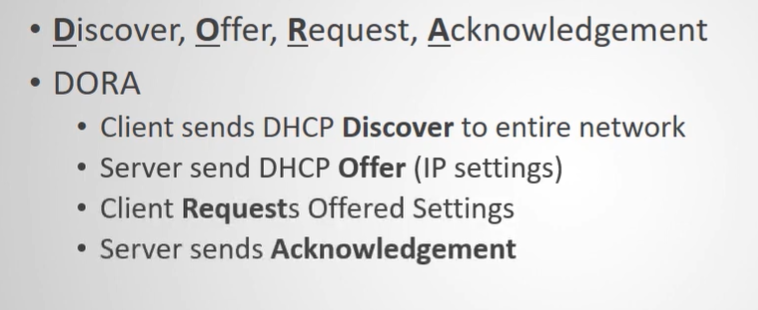
Reservations are not static they are configured to dynamically assigned the given device with the specified info.



The configuration given to the client is not permanent, it is leased for a period of time.

If lease expires, the client can renew the lease to receive the same preferred info again or receive entirely new configurations.

DHCP uses DORA:



This is the process that allows the device to use DHCP.

The DNS server, Default Gateway, Domain controllers, printers, scanners, and any server providing a service must all have a static IP configured.

Because they need a fixed IP.

If it was by DHCP then it would cause problem since they are configured inside DHCP or their service was mapped to the IP like printers.

We can make a DHCP reservation instead but it’s not recommended since they will depend on the DHCP server, if it crashes, then no more connectivity through the network.

## More DHCP configurations

Now we are going to do some more DHCP configurations.

We will start by making a reservation.

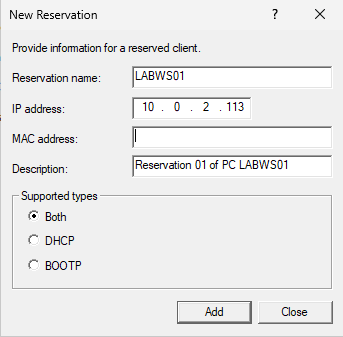
In our windows 10 VM that join the ADDS domain we will need to find its MAC address so we can map this address with the TCP/IP configuration that will be reserved for this MAC on our DHCP server.

In windows 10 open command prompt, and use the following command to obtain the MAC address->getmac

Now we have the MAC address of the device, we proceed to the server to make the reservation.

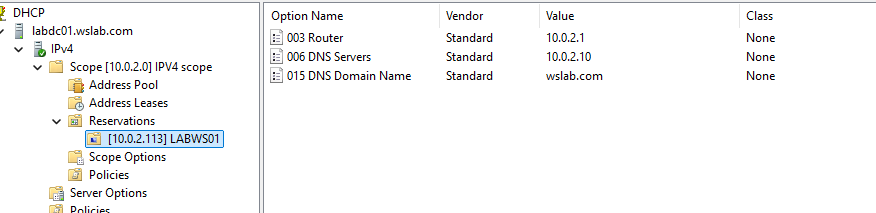
Now on the server->server manager->tools->DHCP->ipv4->scope->reservations->right click->new reservation

Now on the reservation wizard->



We provide all info, the desired IP within the DHCP scope that we want to assign to the desired MAC.

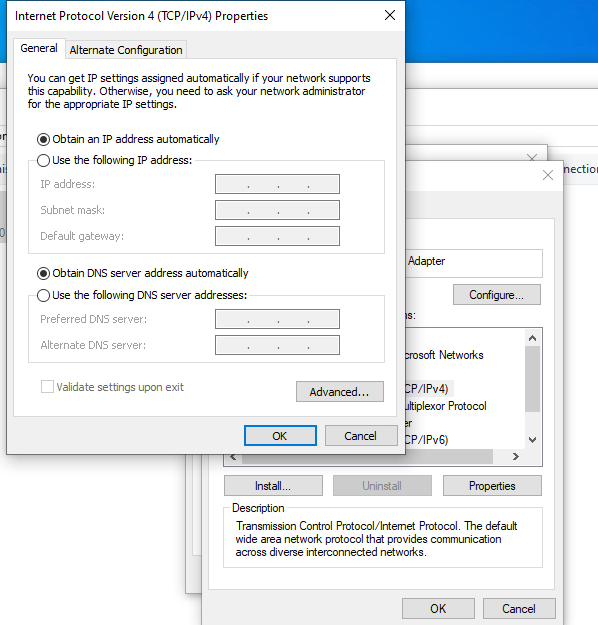
Supported types is kept as both, where BOOTP (Bootstrap protocol) is to dynamically assign Ips when computer boot up/powered up.



Now we have made the reservation.

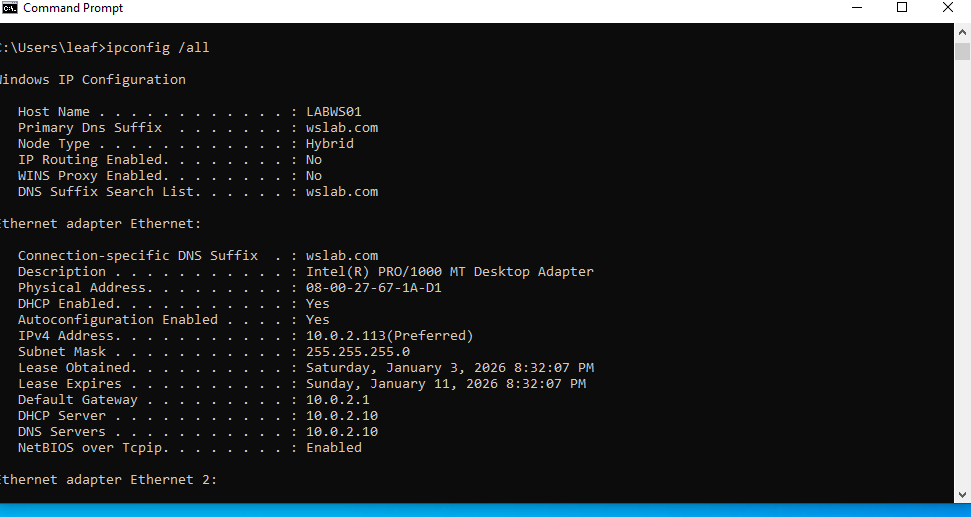
If we want to change anything we can find many options when we right click the [10.0.2.113] LABWS01 reservation.

Now we turn on DHCP on the client.



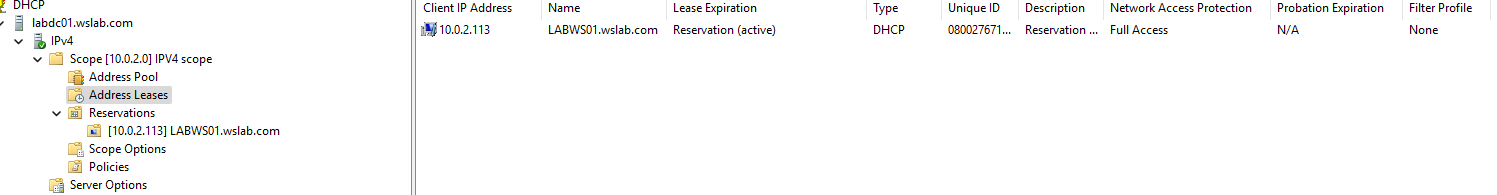
This will allow the client to get all TCP/IP config from the DHCP server.

Now we check, open command prompt and type->ipconfig /all



We can see that now we have the configured info.

We can also check on the server->



## DNS Zones

A DNS zone is a collection of DNS records.

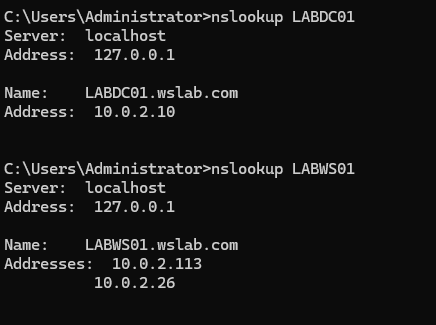
DNS records are mapping for each host name to IP addresses.

Two types of zones:

1. Forward Lookup zones: Most common, and they translate host names to IP addresses.
2. Reverse Lookup zones: Less common, they translate IP addresses to host names.

On command prompt we use the command->nslookup [{host name} ||{Ip address}] , and it will give us its result.

This will ask the DNS server configured on the device for the hostname or IP of the given device.



Both forward and reverse Zones have subzones.

The Subzones are:

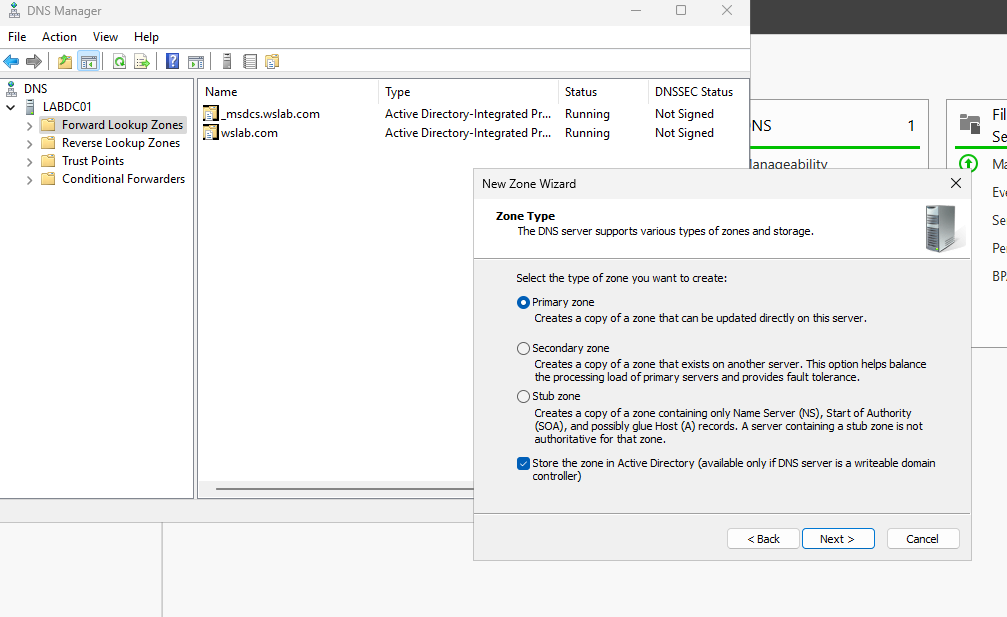
1. Primary zones: Primary source of info on the DNS server, Is located in the folder->%windir%\system32/dns, Or It can be stored in AD if the DC is writable, store in AD can be useful since we can use AD duplication and security features on it. Also, this is the only zone that can be edit or updated (write).
2. Secondary Zones: Read Only zones, cannot be edited, it is stored onto another remote DNS server connected to the primary DNS. Its purpose is to simply provide redundancy if the primary server is unavailable (require a lot of copying so its intensive on large networks). Ant change/edit request is sent back to the primary server. Cannot be stored in AD.
3. Stub Zones: Stored on remote DNS server. But it only stores mapping of host names to IP of DNS server only.

It is used to be less network intensive, and still does its purpose by pointing the user to the DNS server from the stub zone so they can resolve the host names.

Now let’s create a Zone on our DNS server.

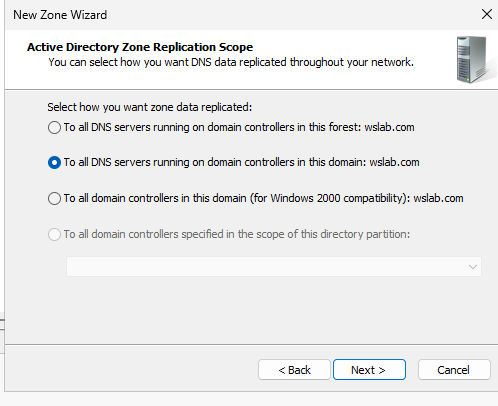
Go to server manager->tools->DNS.

Choose the server->right click forward zone or the zone that will need to add->new zone.



Choose zone type.

If its primary or stub zone we might as well store it in AD since this server has ADDS enabled. (Check the box to do so)



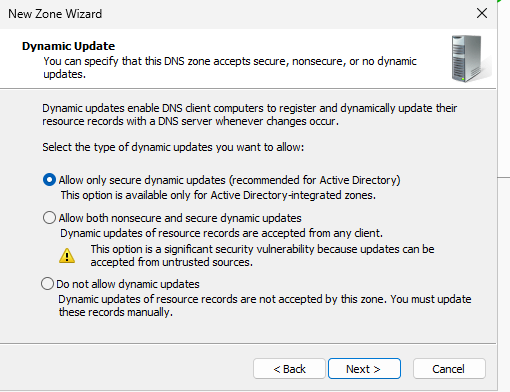
Since we have chosen to store in AD we have to choose where to replicate it.

WE can replicate across the whole forest(domain) or across the subdomain or the option for WS2000.

The last option needs the server to be enlisted in a DNS application directory partition to be available.

If it is, this will allow to choose which domain controllers to replicate to.

Now we set the zone name.



This step is very important, it is best to keep as the first option, because we need dynamic updates so we do not manually do it ourselves which will need maintenance and nonsecure updates is a huge security risk.

Click finish and now we have a new forward lookup zone.

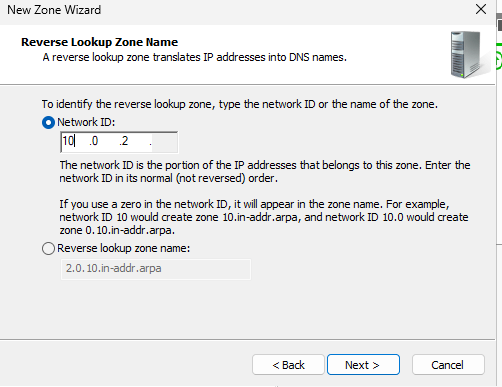
Now let’s do a reverse lookup zone, its nearly the same but has some subtle differences.

We set the subzone type, and store in AD as usual.

We choose type of IP protocol used. (IPV4)

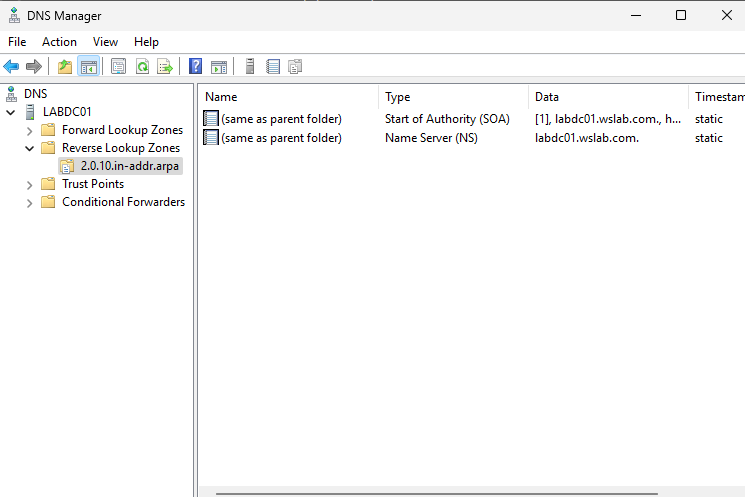
So, the reverse zone can identify we must specify the network ID.

In our case its 10.0.2.



Now allow dynamic secure updates, next and finish.

Now we have our reverse Zone.



The zone will contain two records, SOA and NS.

These are called resource record and will be automatically populated to be used to resolve names or Ips.

DNS servers have different type of entries which are resource records. (files)

These records have DNS based data (like a host name and its IP) about devices on a network.

In this lecture we will cover the following records->

SOA, NS, A, PTR, CNAME, MX and SRV.

1. SOA: Start of authority, every zone contains it, contains info about the DNS server that provide data for this zone.
2. NS: Name server, every zone has an NS record, it indicates the zones authoritative DNS server or simply info about the DNS server, every zone have at least one NS.
3. A: Address, maps an FQDN (Fully qualified domain name) to an IP address, an example of a fully qualified domain name is wsdc01.wslab.com which Is the hostname. domain. schema
4. PTR: Pointer, maps an IP address to an FQDN.
5. CNAME: Canonical Name, Stores mapping for FQDN, if we have updated the FQDN to wsdomaincontroller01.wslab.com then it will be mapped to the old FQDN so devices can know which is it.
6. MX: Mail Exchange, will list the mail server for the domain, this file will not exist if Mail is not installed.
7. SRV: Service Record, allows us to map the specified server to the specific service, so we make an FQDN to a server and point it to its port allowing its services to be easily accessible.

## AD users and computers

Active directory users and computers is a tool installed when the role ADDS is installed.

AD is a live directory, a live database that stores users accounts, computers, printers, file shares, security groups and the respective permissions.

So, it stores AD objects, and security groups also technically is a group of objects, so its purpose is simply for security, to control group permission for example.

Purpose of AD is to handle security authentication across the domain, one of the ways of doing so, is to only allow the authorized users to login into the network and access its services.

It also provides centralized security management of network resources, which means it stores usernames, passwords and more in one location instead of storing this information on each computer.

The most common task using AD is resetting user passwords, create and delete user accounts.

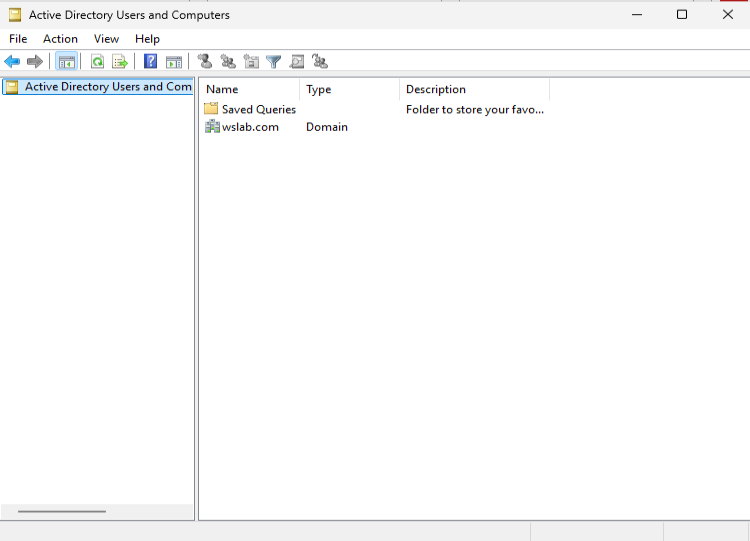
When a user tries to login to a domain/workstation, the DC of that domain will check the entered credentials by the user and compare them with the ones stored in AD.

So, data is centralized in one place, which makes work easier for daily tasks.

Now onto the interface.

Go to server manager->tools-> AD users and computers.

This is the AD tool that allows us to fully configure and manage AD.



This is the AD tools manager.

We can access the data within a folder or a domain to manage or view the data.

We have 4 tabs:

1. File: either to exit the tool or to simply open option that only have one thing which allow us to delete the changes made to the view of the console.
2. Action: literally does the same thing as right click and will show the same exact output when we right click on the specified directory.
3. View: have multiple option, like removing certain columns to make it easier to see, also has filtering and more options to remove items or columns. Most importantly is the advanced features option, this one allows us to see hidden and important information that can be only seen when this option is on.
4. Help: contains resources to learn, troubleshoot, and more info if needed on Microsoft website or other resources. Also, it contains some info about the current server.

Under the tabs we have a toolbar, which have many purposes based on the folder or object selected.

Using the toolbar we can add users, groups or manage them if a domain is selected.

For example, the second last tool in the toolbar allow to find objects in the AD.



It allows us to choose many options to search for an AD object that we do not know its exact location.

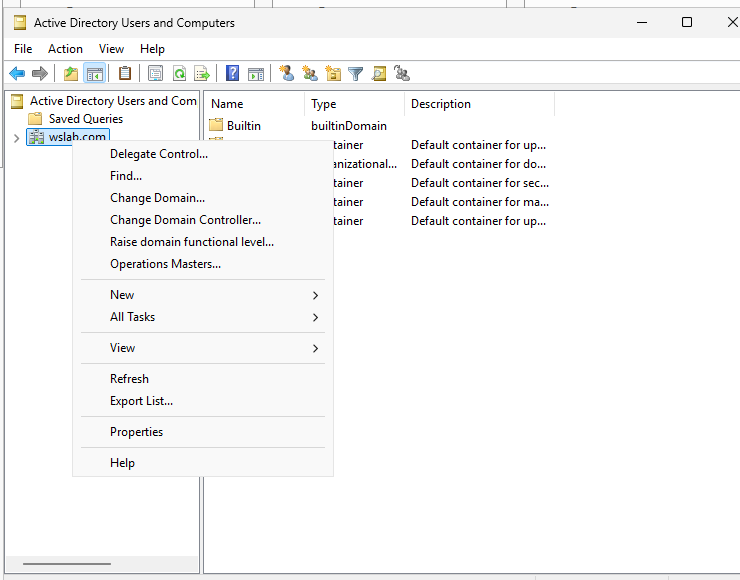
On the top left, on the navigation we have Saved Queries.

This one allows us to save process that we do many times to make it faster an easier.

For example, delete users who have not logged in the past 30 days.

We simply add the queries in this folder to be instantly used.

Now onto the things we can do within the domain.



We can do the following things:

1. Delegate control: Allows us to choose additional users who may manage the domain.
2. Find: Allows us to local objects, same as the find button in the toolbar.
3. Change domain: It works only if we have subdomains or another trusted domain on the network.
4. Change domain controller: This one allows us to swap to another domain controller in our network.
5. Raise domain functional level: This one is used when we have many domain controllers using AD. If one DC is 2016 and another is 2025 then the 2016 windows server won’t be able to support the latest AD features, and we need all DC to support a feature to use it properly, so when we update the DC to 2025, we can raise the functional level so it can function based on the latest supported version.
6. Operations masters: Allow us to choose the master DC of a certain operation. For example, primary domain controller or PDC, we must choose a server as this one, and in case we want to delete/remove the server we must change the PDC before it is deleted.
7. New: Allows us to add new objects to the AD, like users, groups and more.

## OUs and containers

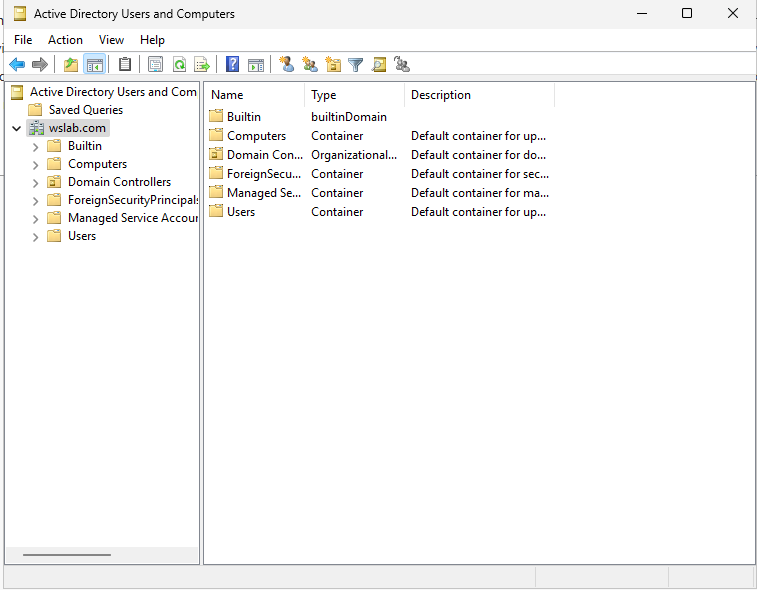
A container is a structural object that is included by default within AD.

The main difference between organizational units and containers is that we cannot apply GPOs directly to containers.

Also, we cannot create container in AD, its not possible unless we use ADSI, but we rarely need to do this unless we launch a new program.

1. **AD Containers:** Default, system-created folders in Active Directory used to hold objects, but **you can’t link Group Policies to them**.
2. **AD Organizational Units (OUs):** Admin-created folders used to organize objects **and apply Group Policies and delegate administration**.

By default, we have the following AD containers.



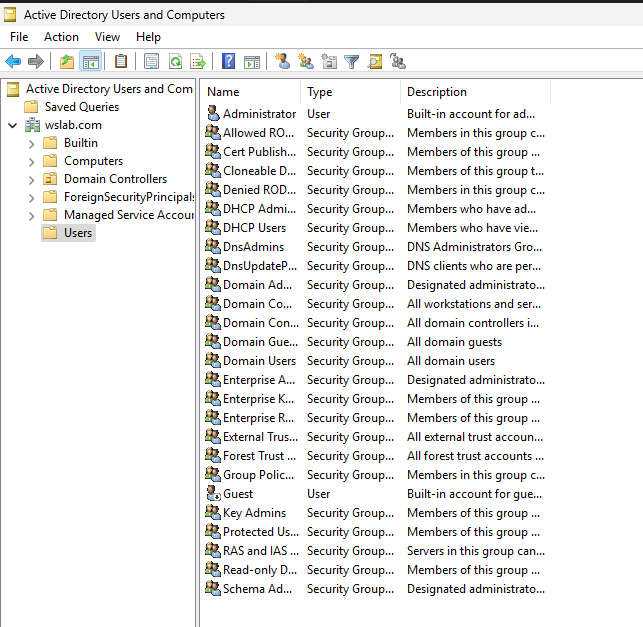
We can see in the type column which are containers, which are premade storage for AD to store objects.

Computer container: Default location for computers that joined the domain, this location can be changed using PowerShell. Also, GPOs applied to the domain like the default domain policy will be also applied to the container but we cannot apply GPOs directly to it.

Foreign Security Principals container: Holds proxy objects for security principles from other trusted domains. A security principal from another domain could be a user account or security groups that reside in the other domain. A trust between our domain or another must be established to use this container.

Managed service accounts container: Holds account that are used to run service or applications that are run on servers. They do not need to have passwords since they are handled automatically and are supposed to be used for service and not by end users, and that is to solve the problem of expiring service accounts password which is a headache so that’s what MSAs hopes to solve. To create an MSA the PowerShell command line must be used.

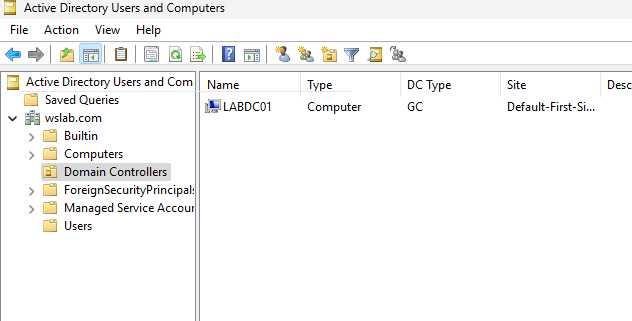
Users’ container: Inside the container we can see many default accounts like admin and guest user.



Other than the Users there are all the default security groups that are used by the domain.

The Built-in domain contains the security groups that are required for the DC to operate.

Now onto OUs.



We have by default the Domain controllers OU, which inside we can see our DC which is the device we are working on.

Also, by default, there is a GPO created and applied on this OU.

OU is used to organize and separate objects within active directory.

Also, OUs can be used to assign permission, for example we create an OU that stores only the marketing team users of a domain.

Then we apply the permission to this OU which will be applied to all the users inside it.

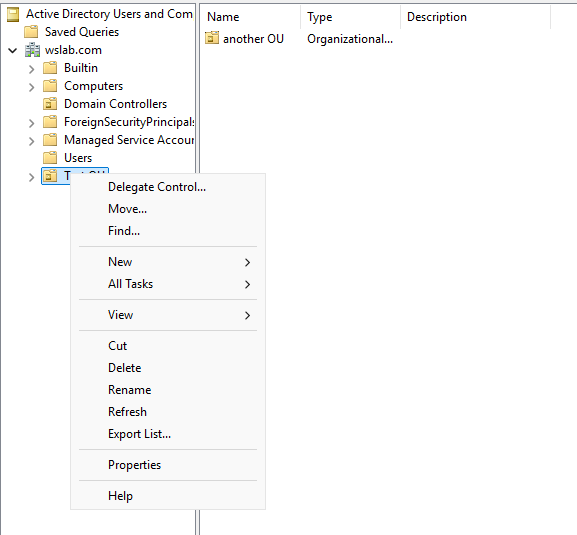
Let’s create a new OU:

Choose location inside domain-> right click->new->Organizational Unit.

Then set the OU name, and keep protect from deletion checked which protects it and needs many steps to delete it.

We can make another OU inside an OU.

Now we can do many things to it if we right click on it.



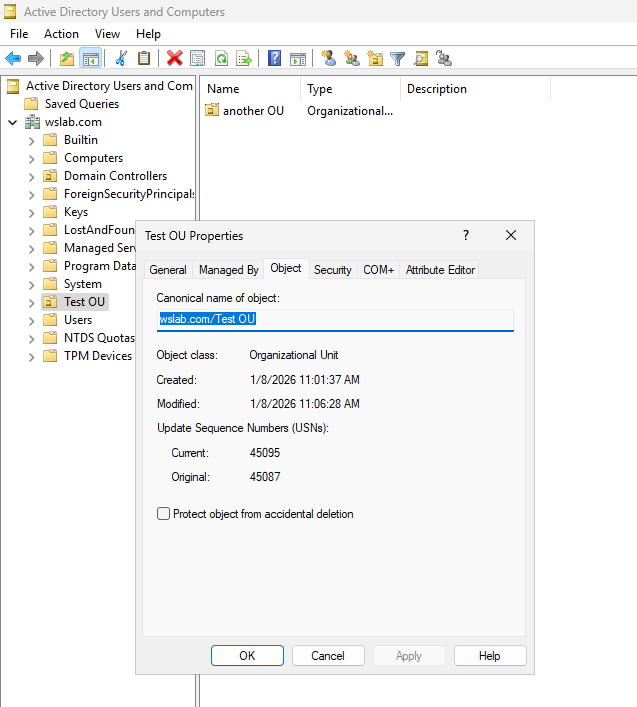
Export list will show all files, folders, objects and more and export it into a text file.

If we try to delete, we will have an error since we checked to prevent deletion.

To fix that we do the following:

Go to View->Advanced features

Then right click the OU ->properties -> a new tab will show called object since we turned on advanced features->uncheck delete protection.



And now we can delete it.

## Create and manage user accounts

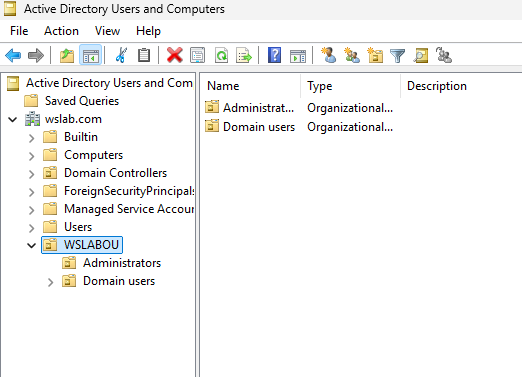
We have two options to manage, either from the AD users and computers interface or from the command line.

Now we will use the interface in tools->AD users and computers.

Now we will simulate a company server.

We create an OU for the company.

Now inside this OU we will put OUs, one for administrators and one for users of the company.

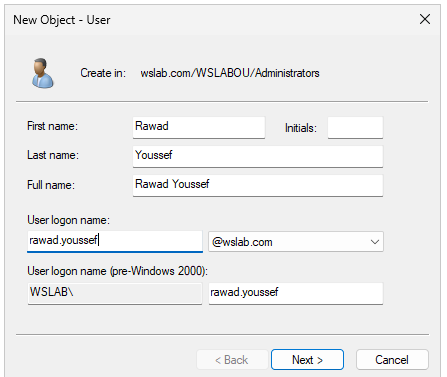


Now we have our structure, we simply add objects to the OUs.

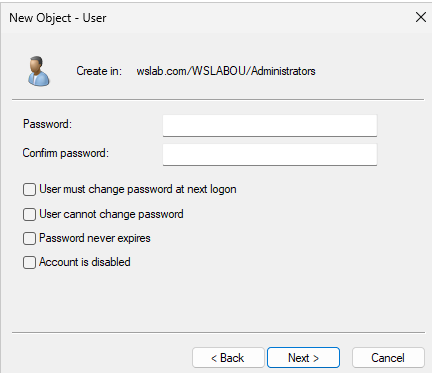
Let’s add an admin, go to administrators->right click->new -> user.

Important note: The user account we are using right now is called the shared administrator account and it is not a good security practice.

It is best to use a made account like the ones we will create.



We fill the info as usual.



Now we set the password.

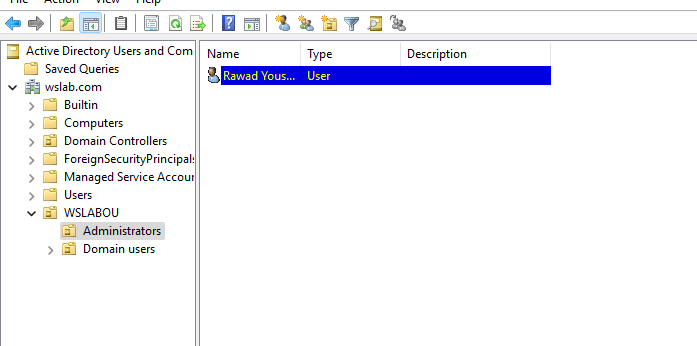
Then we have some options that we can choose for the password, like user must change password at next logon, this option is useful is the user is for someone other than the server administrator.

User cannot change password is not to recommend because is unsecure and barely used, sometimes used in service accounts.

Same for password never expires, best for service account that run an application.

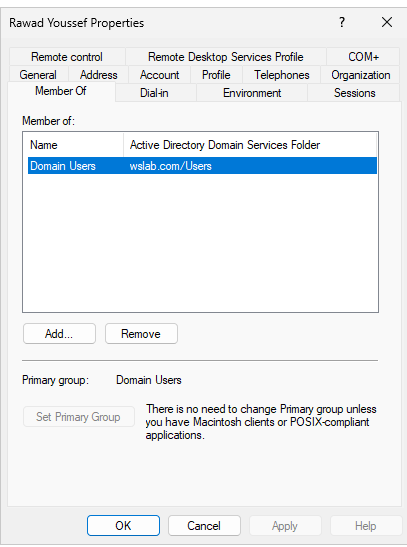
Account is disabled, this one is used to pre create an account, and then make it available when we need to.

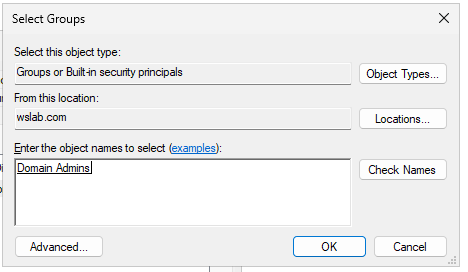
And now we have a new user:



Now this account is still a user, we need to make it an admin.

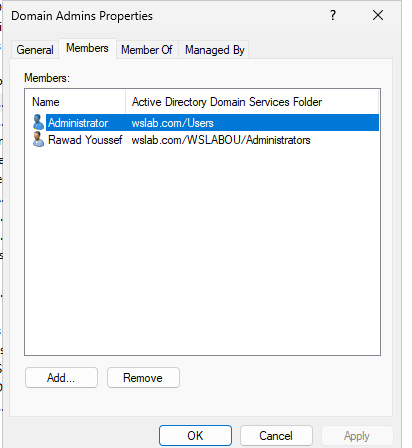
Double click the account -> member of

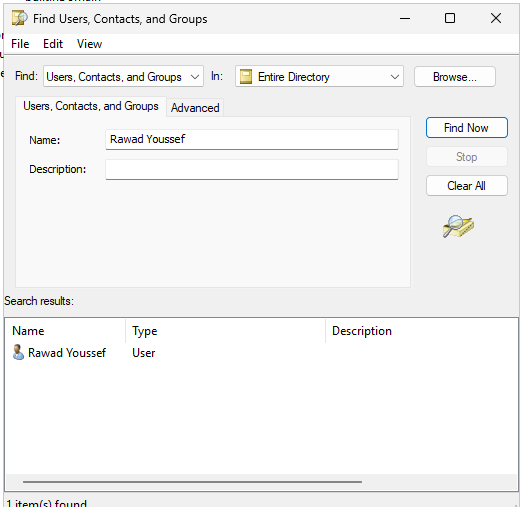
We can see that the account is part of the Domain user’s security group in the user’s container.

 So, we simply add the user to the Domain admin security group.

Go to Add->type domain admins ->check names (to make sure it found it) -> add

Now we have added the users to the group.

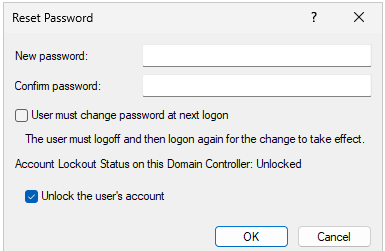




If we go to ->toolbar top left->find->search entire directory

And we try to search for the new user, we can add more advanced filtering option in Advanced tab of find wizard to filter or remove columns.

Let’s reset the user’s password, in the search result or in the OU, find the user and right click-> reset password

 We enter the new password, check user must change if we need to.

If Account lockout status was locked then it’s a good practice to unlock it so it can be used.

Now we can finally login to our new user and use it like we were using the shared admin account.

## Groups and memberships

Everything here will be completed from the AD users and computers console.

Now, we will need to create a group first.

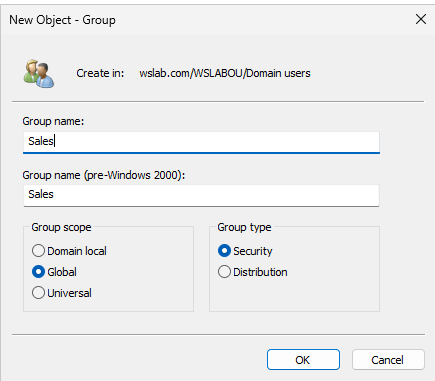
So, we will add it to the OU Domain users previously made, but we can still create the group anywhere we want.

This group will allow us to store multiple objects at once.

Go to the desired OU ->right click->NEW->group

Now enter the required info.

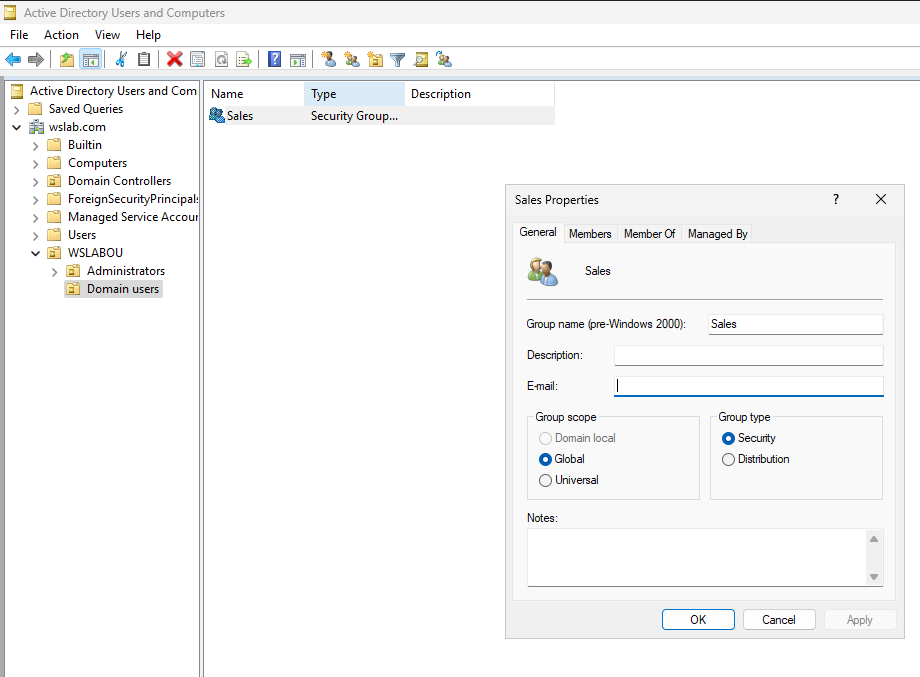
We will name it sales as it will represent the sales branch of the company.



Now we have group scope and group type.

1. Group scope:
   * 1. Domain local: The least accessible scope, only accessed by the domain that it is inside. No one from other domains can access it, even if trust was established between the domains.
     2. Global: Same as domain local, but also the group can now be access by outside trusted domains within the same forest.
     3. Universal: Same as global, but now it can be accessed between forests other than the one that the group is located in.
2. Group Type:
   1. Security: Make such group for authentication, to add and modify privileges of the objects of that group.
   2. Distribution: Only used when we have an exchange server setup on the network. So, it is only used for emails, when we create a group for example, and we send an email to that group, the email will be then sent to all users of that group.

Now we will keep the scope as global and the type security.

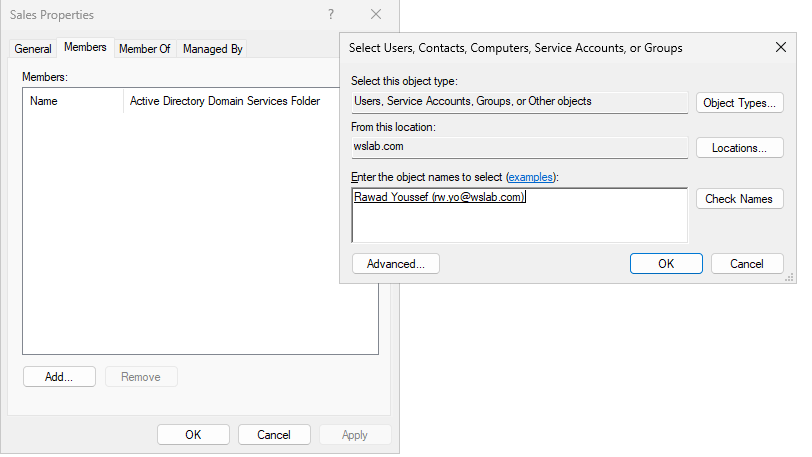


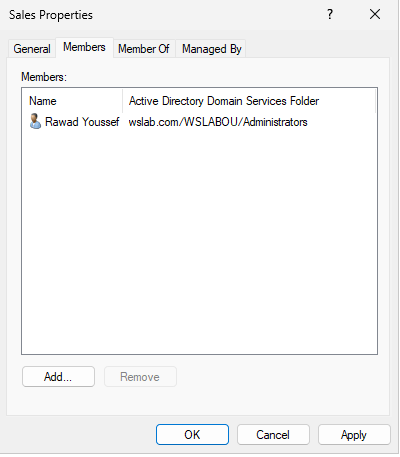
Now we have created the group, notice that we can expand the scope but no shrink it.

We can modify and add some info too.

The most important tabs here are members and member of.

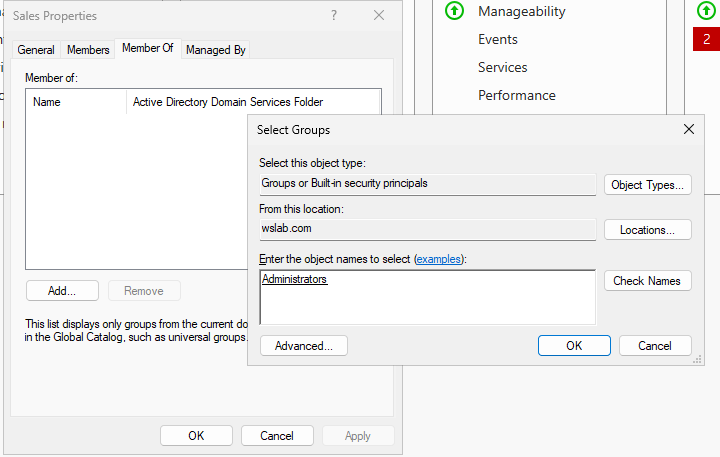
In members, we can add object to the groups.





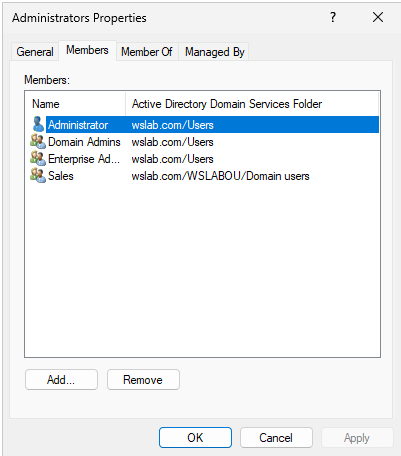
The member of tab allows us to join another existing group.

We will join the administrators group located in the Built-in domain.



Now the group is inside the group administrators.

This means that the users inside this group, is also inside administrators, which means they will have admin privileges.



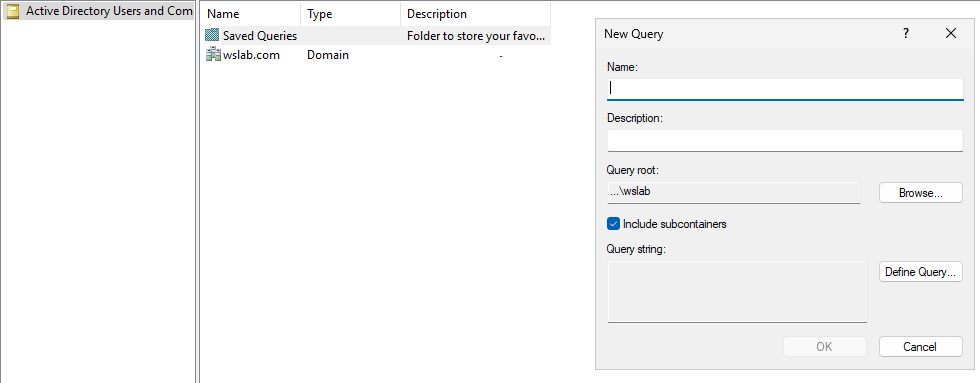
Here we can sales in inside the group.

## Saved queries

Saved queries allows us to make redundant task way faster.

The saved queries folder is located inside the AD users and computers console.

To add a query, go to Saved queries->right click->New->Query



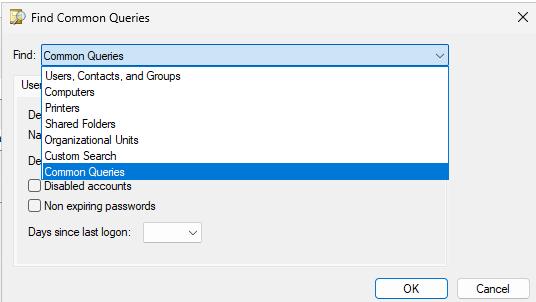
Enter the name and description.

We will do a query that handles users who have not logon the last 30 days.

The query root is where it will affect/do what it should do.

Include sub container should be checked at least 90% of the time, since without it the query won’t be able to see the sub container, like the OUs we made inside the OU WSLABOU.

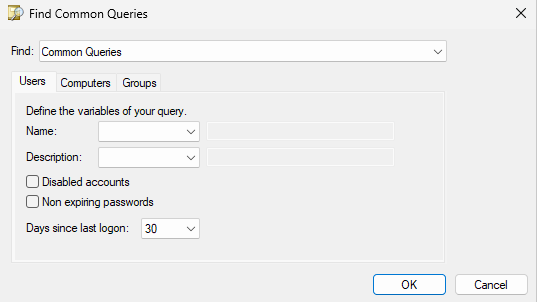
Now click define query to write the action of that query.

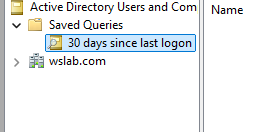
We are able to find any AD object like the first 5 options.

The custom search allows us to search based on something that an object has, like the office location of the user.

We can also search using LDAP queries, but we must understand LDAP syntax to do so.

We will set it to common queries, which will allow us to easily create queries for users, computers and groups.

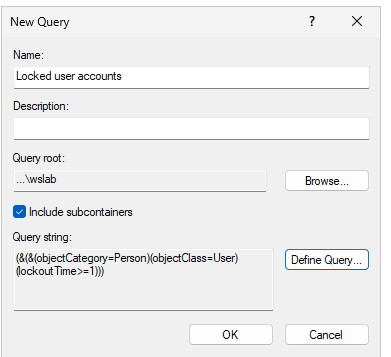
Now we also set the days since last logon to 30, then click OK.  
Now, users that have not logged in the last 30 days will show up in the following folder.

 We can later on, right click the folder, export list to txt file to send a text file containing the users.

Now, we will create another query, this one will handle users that are locked. We will be using LDAP.

We will enter the following query-> (objectCategory=Person)(objectClass =User)(lockoutTime > =1)

This query will search and return for all the users that are in the person category, so normal users that have a lockout Time greater or equal to 1.



We can later on create a GP that locks accounts if they try to login and fail 3 times in a row.

## Group policy

Group policy is a tool used in AD.

Used to quickly and easily make configuration changes to users and computers within AD.

We can apply security configurations quickly and easily, like restrict certain users to login into certain computers, allow certain users to access certain files, give specific users or all users a specific desktop background, or deploy software to the workstation.

Group policy works by applying groups policy objects (GPOs) to the OU structure that we have created.

A GPO contains configurations for both users and computers.

So, when we apply a GPO to an OU, the configurations of that GPO are applied to that OU.

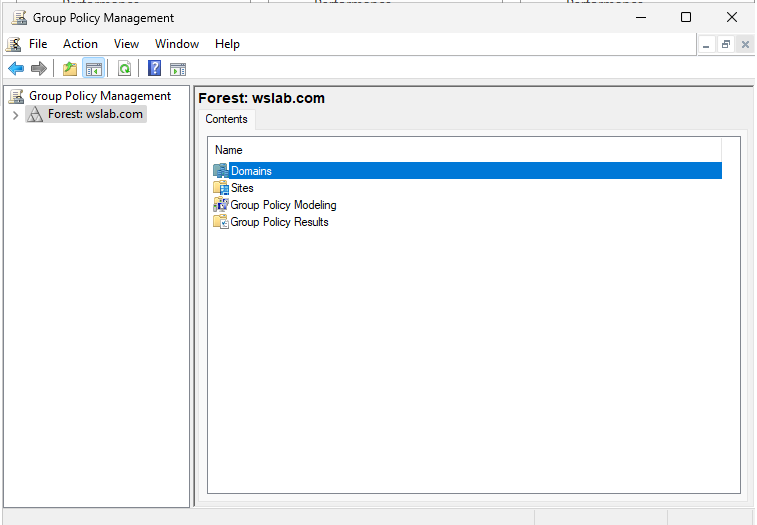
Its like instantly giving a group specific permission.

We can also apply the GPO on specific user by defining the security filtering, most default choice is the authenticated user’s group (Any valid user or PC within AD).

GPOs are applied recursively which means it can detect sub containers.

Now onto the technical part.

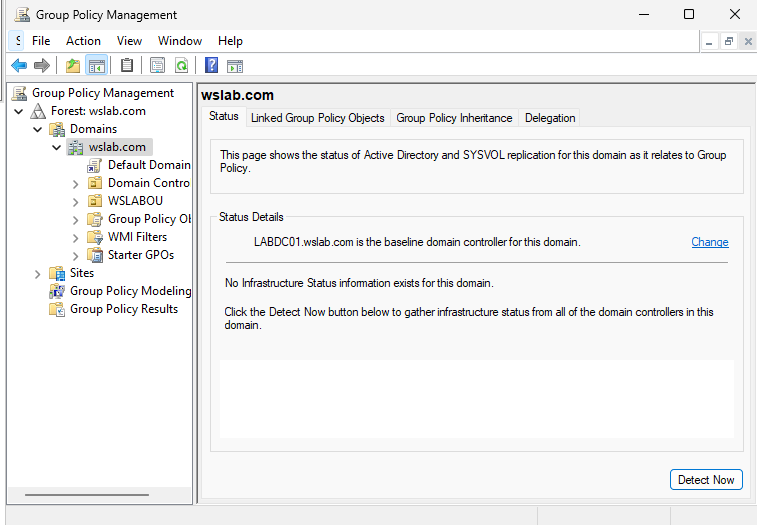
Go to server manager->tools->Group policy management.



In this tool we will see all our forests.

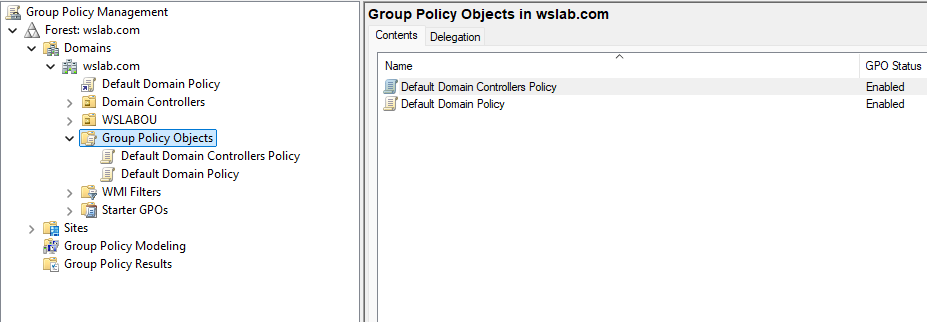
The wslab.com forest has the following folders:

1. Domains: All domains within the forest.
2. Sites: All the sites that may have been configured through AD sites and services. (Used for servers in a different physical location).
3. Group policy modeling and Group policy results: Both of them are tools to troubleshoot Group policy.



Inside the desired domain, we will see a similar structure to AD, but it does not contain the AD containers like users. It will still have the OUs we made.

We can also see that it has a Default domain policy, this policy is created an applied when we create the domain, it is applied under the domain wslab.com, so it will affect all objects that are within this domain, including all objects in the OUs and the sub-OUs.



The group policy objects contain all the GPOs inside our domain, whether they are currently in use or not.

WMI filters allows us to apply specific rules of when a GPO should be applied or not.

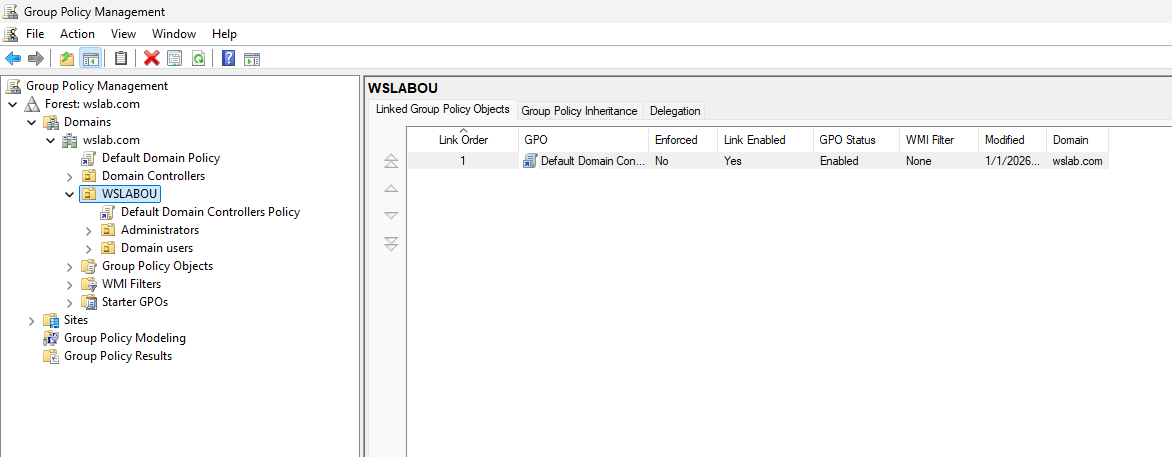
Starter GPOs is used to when we want to export GPOs for distribution or other environments.

A domain may contain many GPO and a GPO may be applied to multiple OUs within its scope that it is applied to.

Let’s apply the existing GPOs to the OU we created.

Right click the OU->Link an existing GPO.

Choose the GPO and apply.

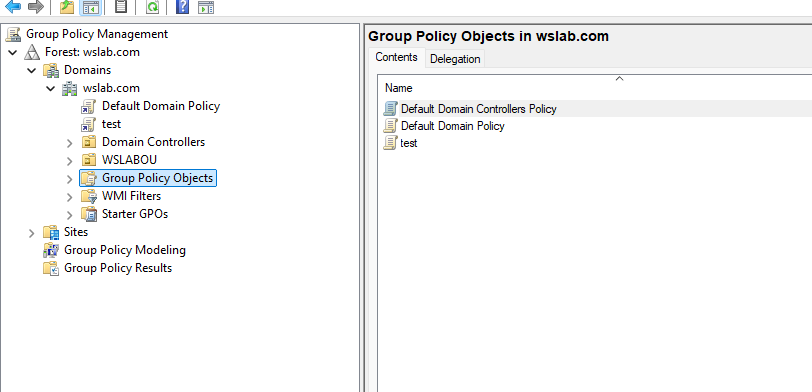


Now we can see the GPO have been applied to the OU.

To delete the link that we just made simply right click the GPO link inside the OU we applied and click delete.

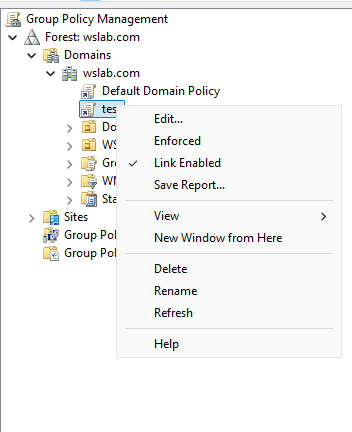
Now let’s make a GPO.

To make one right click on the domain->create a GPO and link->set the name and click OK.



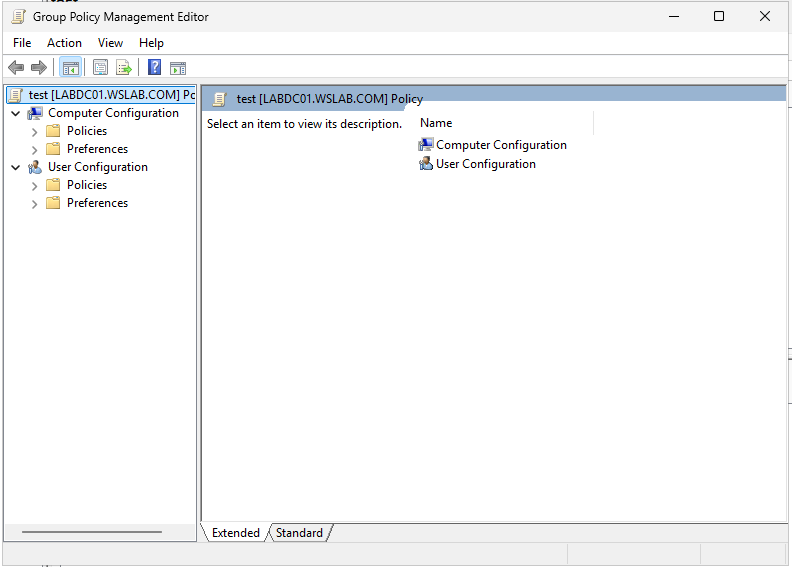
The new GPO test is now created and applied the whole wslab.com domain.

Now we can do many things with that GPO.



We can edit, we can make it enforced, which means it will take priority in its task more than the others, link enabled means its applied and can be disabled, we can save a report that is well formatted an contain info about the GPO and we can also modify the view.

Now click on edit.



Here we can make all the configuration changes for the test GPO.

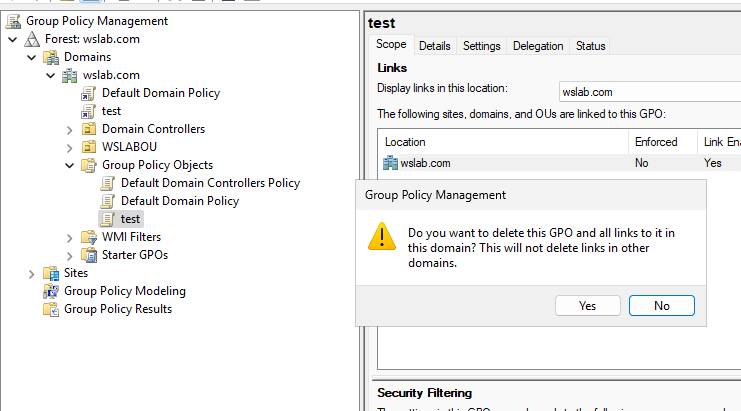
There are two types of configurations, users and computers.

Users’ configurations will only be applied on user’s objects.

Computer’s configurations will only be applied on computer objects.

So, if the OU contains users, then we must modify the users’ configurations.

Now we will see how to delete the GPO itself, and not only the link.



To delete it, we must simply right click-> delete from the Group policy objects folder.

## Group policy precedence

GPOs work in a certain order since there may be multiple GPOs trying to apply the same settings.

The first applied GPO is the local GP. It is applied when the computer is booted and it is the most ignore, it handles computer configurations. We can see it my searching gpedit.msc

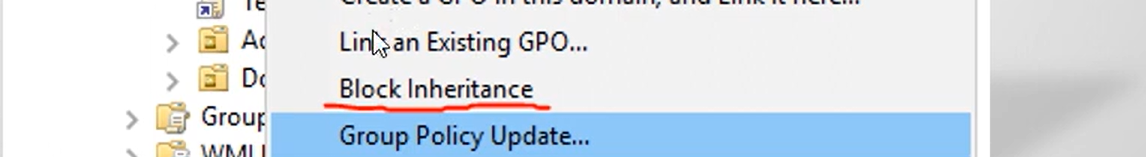
After there are the Site policies, this one overwrites anything in the local policy. So, if we do the same task on both the site policy will take precedence and do it after so it can overwrite.

Next is the domain policy, the policy applied on the domain will take precedence and be applied after the site policies.

Next is the OU policy, it takes precedence over the domain, so it will be applied after it. Also, sub-OUs will take precedence on the outer OUs.

Finally, we have the Enforced GPOs, they are the GPOs that we have right clicked and choose to enforce, this one is the most important one and is always executed last so it can overwrite them.

Now within the GPO we have configuration, the computer configuration is applied first and then the user configuration is applied second.



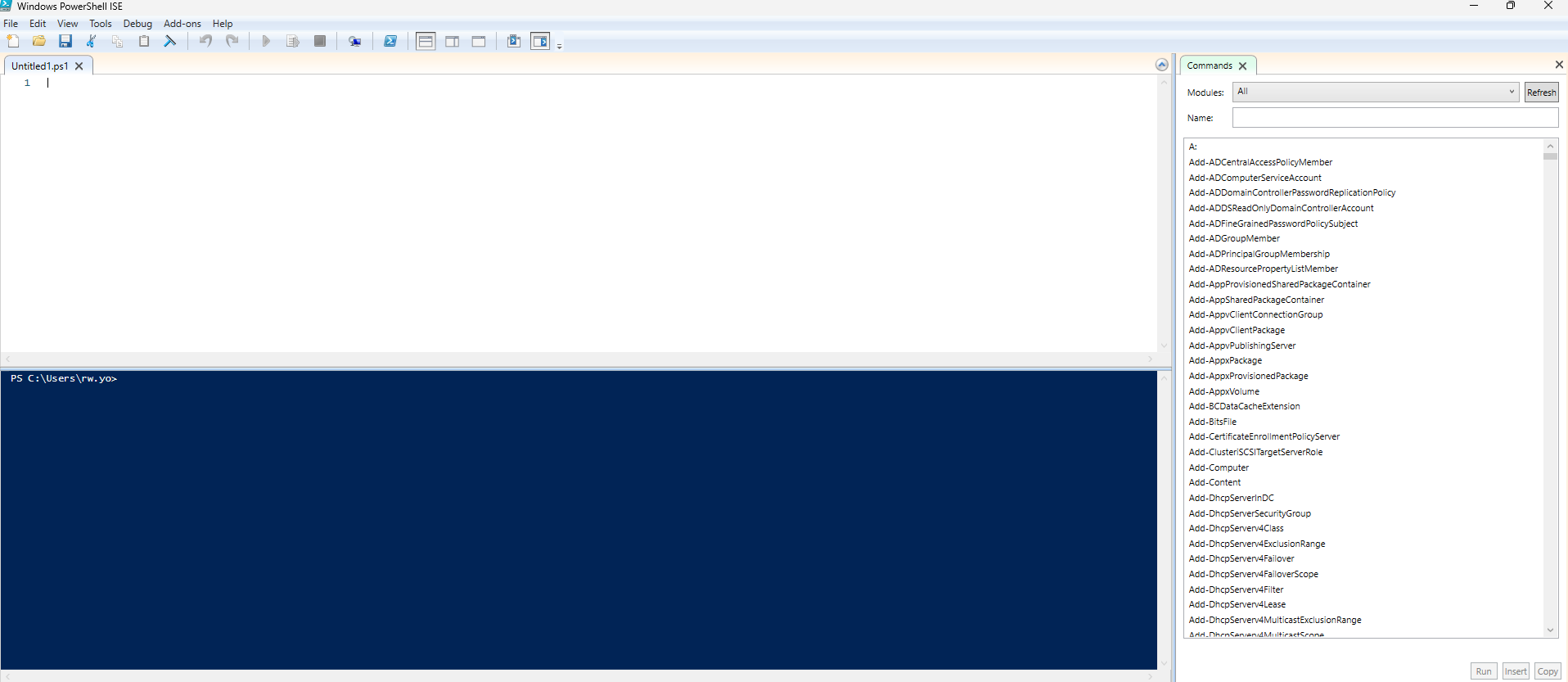
Also, we can choose an OU and block inheritance.

This will make only the GPOs inside the OU to be applied. The one outside will be ignored unless they are enforced GPOs.

## Using PowerShell

On the DC, all prerequisites to use PowerShell are met.

Go to server manager->tools->PowerShell ISE or search for it.



Like CMD we can type in command normally in the blue block.

The white block can be shown by clicking the top left arrow, and here we can write scripts, which is a sequence of commands to save and use for later.

Now onto the scripting syntax.

Comment: use # to write comments

Now we are going to try to store the users first name into a variable.

To create a variable use $, example: $var = “username”

This way we are initializing the variable statically.

We can take the user input using the following command

$var = Read-Host

We can also add to it some things like prompt for the name

$username = Read-Host -Prompt “Enter name”

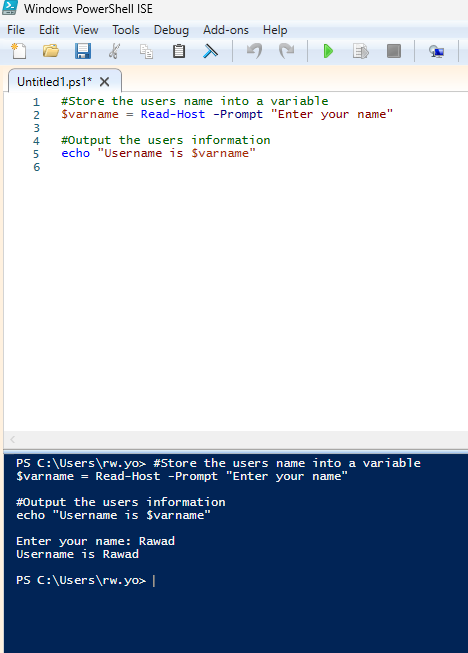
We can also print the information that we took.

Use the echo command.

Echo “Username is $username”

This will print the user input.

Now to run the code click the green arrow.



We can see that the executed script will be pasted and will run in the blue block.

Such simple scripts can be later on used to take user info as input to create AD users.

Now we will write a script that takes user input and pass it on to AD.

First, we have to import modules that allows us to use special commands.

To import use the Import-Module command.

So, we do -> Import-Module ActiveDirectory

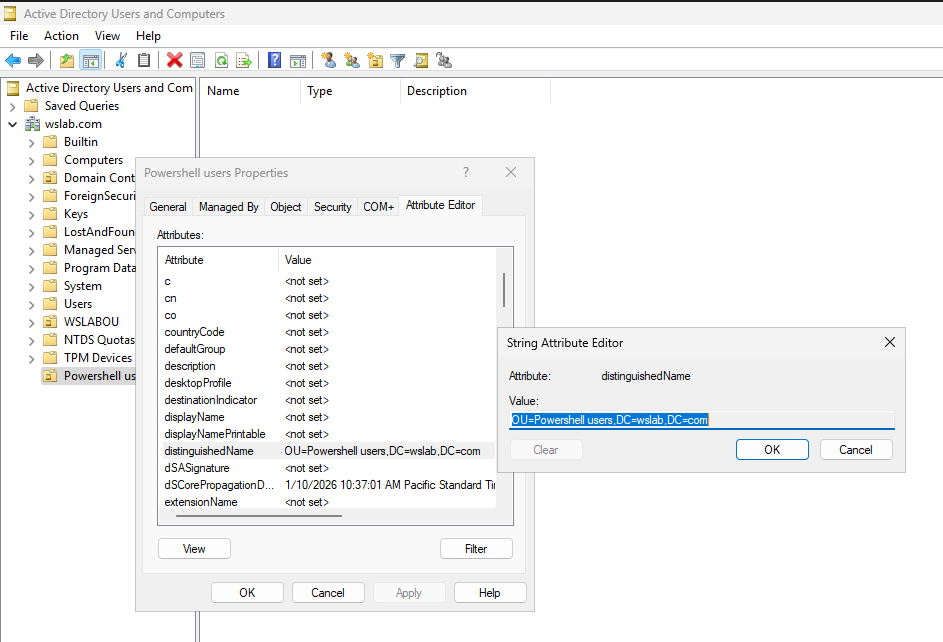
Now we have to specify where to store the user account.

So, we create $OUpath and we store the path of our OU.

To get the path go to server manager->tools->AD users and computers.

Turn on the advanced view.

Choose the OU-> properties->attribute editor->distinguished name



Copy that name and past it into the variable.

Now the password that we are taking as input need to be converted into a secure format.

So, we make a secure variable.

$securePassword = ConvertTo-SecureString $pass -AsPlainText -Force

So, this will convert the $pass variable into a secure String which is the format needed for the AD account to be created.

-Force will make sure it is converted.

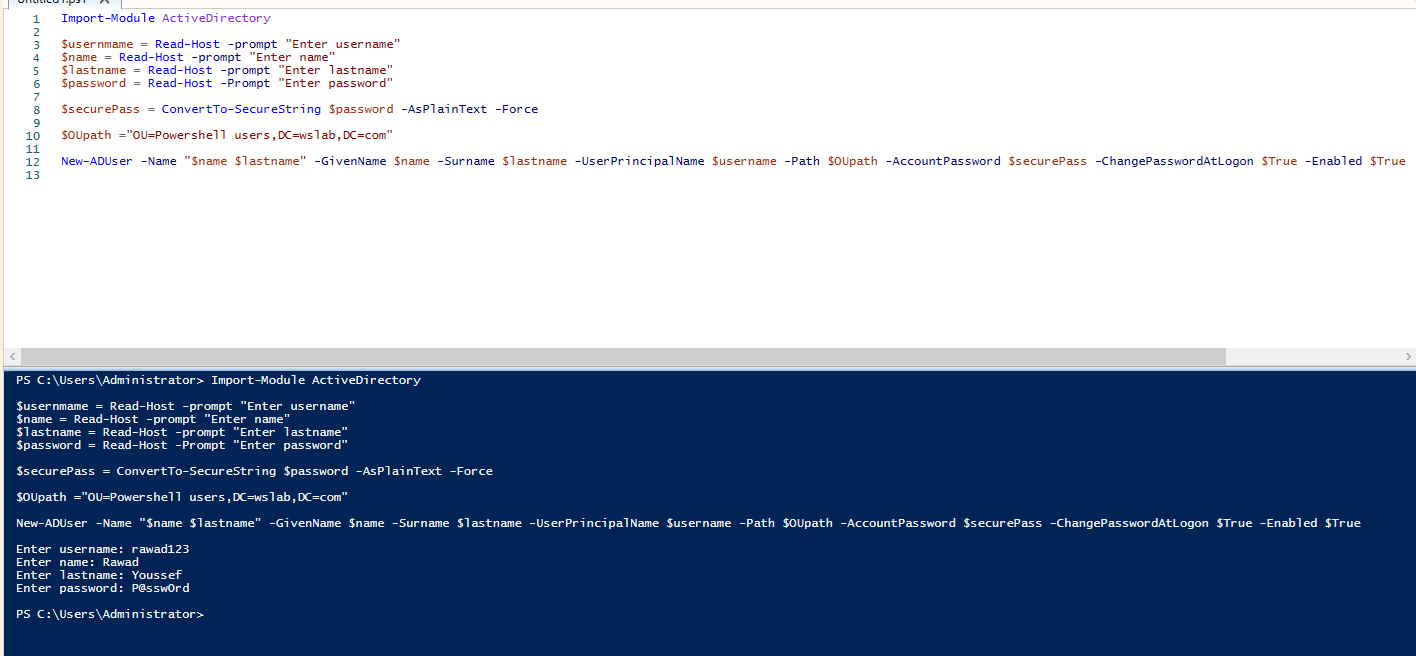
Now we are ready to create the user account.

This command will make use of the previously imported library.

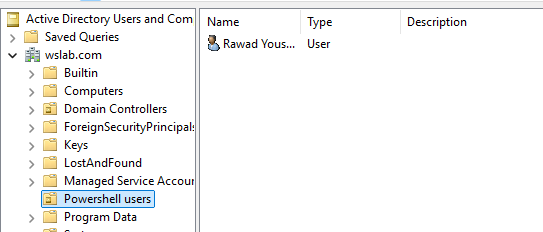


This command will create a new user and store the user into the specified OU in AD.

Change pass at logon is set to true so its activated and same for enabled so the user can be used.



And now we check inside the OU.



We can see the account have been created.

Now let’s make another script, same goal but we will make it inside a loop and this loop will allow us to created multiple users.

Here is the basic while loop syntax.

$exit =””

While($exit -ne “q”){

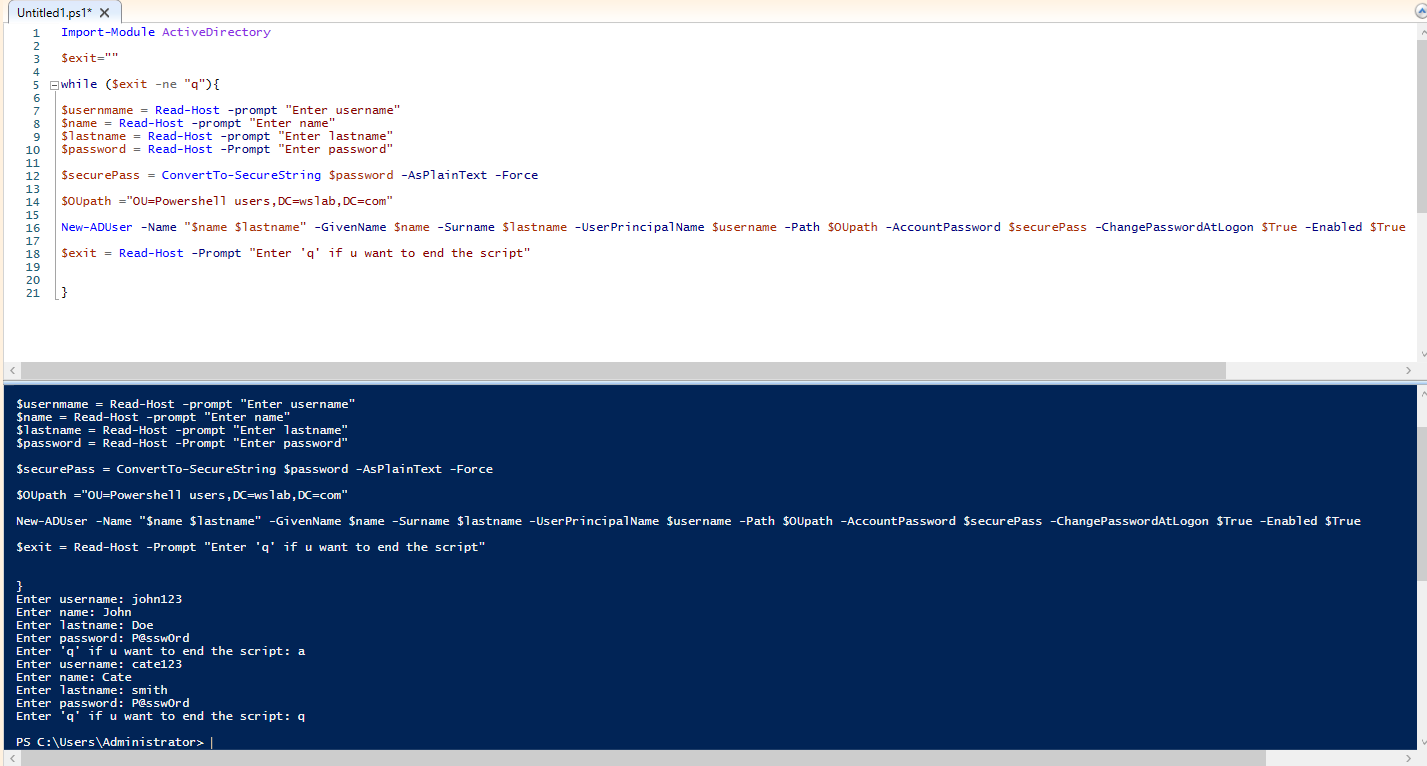
#some code to create accounts

$exit =Read-Host -prompt “Type q to exit”

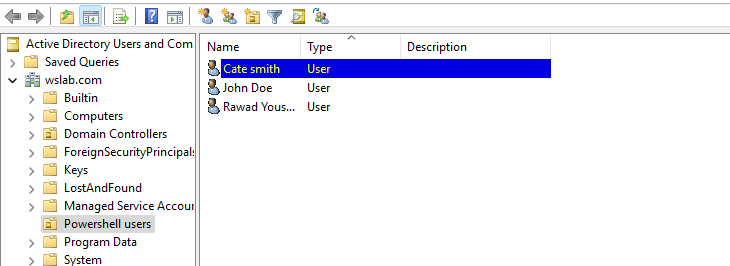
}

This script will now loop and ask to user to enter q to leave, if we want to add another account just enter something else other than q.

Now we test, we will create 2 in one try.



It ran well, we check in the OU.



We can see it worked well.

Now we will save the script, for later use.

Go to file on top left->FILE->Save

And save it in the desired location.



We can right click->run with PowerShell and the same script will be executed.

Now we will create user account, by taking the info from a CSV spreadsheet and using that info to create the accounts.

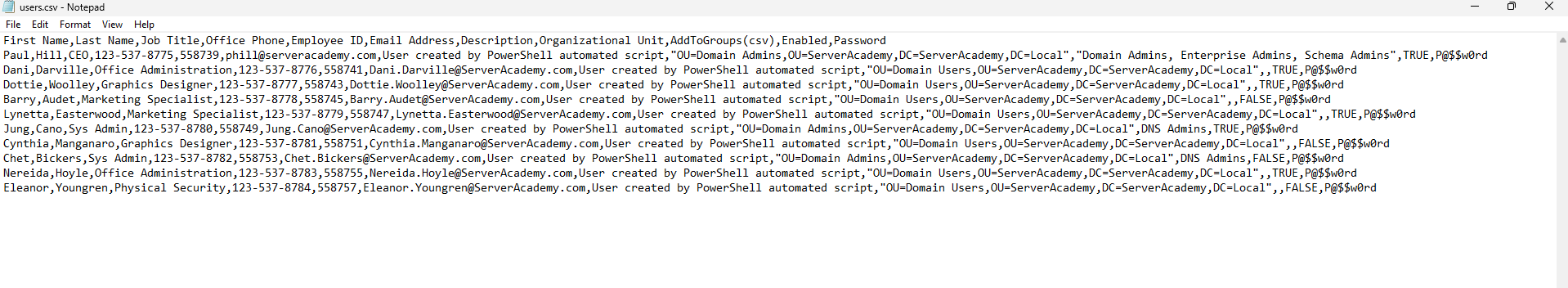
Any file type that is exported to CSV, contains data.

This data is structured and separated in a readable format.

To be able to parse this data from PowerShell we must understand the format.

Most importantly, that CSV files data are comma separated.

Such script is used when large amount of data is involved, to make the process faster and easier.



Here is the actual structure of the CSV file, we can see its comma separated.

Now we will write the same script, but instead of prompting the user for info we will simply take it from the CSV.



Now we make a variable file path, it will contain the path of the csv file.

We can either directly initialize it or make it so the user chooses which file by using Read-Host.

Now we must import the data of the CSV into a variable.

Now we have the data stored into users.

Now we must loop, thought the data and create each user in each loop.

We can see from the format of the CSV file, each line is a user, we must skip the first line since it’s a header for the data, and the commas are used to identify the attributes/columns of each lines/row.

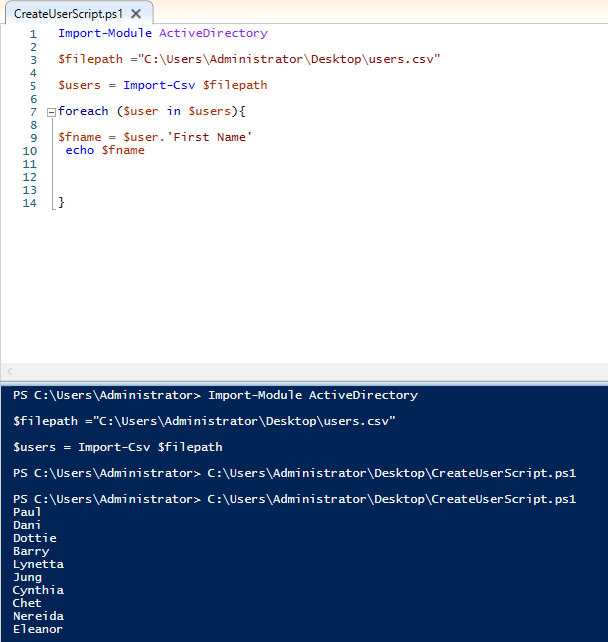
Currently the users variable work as an array since it contains more than one user.

We will use foreach to loop through them.

Since the $users is imported form a CSV, the array can detect that each line as many attributes.

So, it’s an array of objects.

Also, the first line is automatically skipped based on the standard CSV format.



In each row, the user variable takes a line from the user’s array.

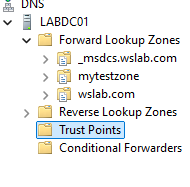
And we are initializing the fname variable with the value of the First Name column of each row.

Now we will parse the whole file, all the column and use the New-ADUser command to create users as usual and that’s most of it.

## DNS

We will create DNS resource record for forward and reverse lookup zones.

We will use the previously created zone in the forward zones.



Now lets add records of the type CNAME to the mytestzone forward zone.

Right click the zone->other new records->Alias(CNAME)->create

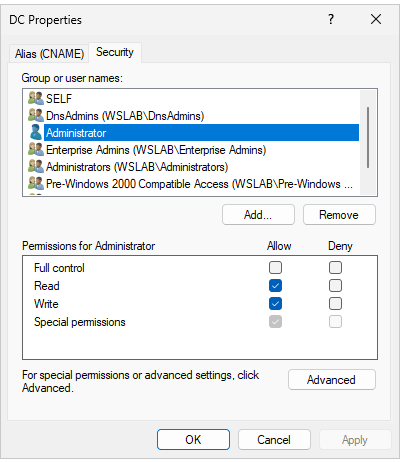
Set the record name and specify the FQDN.

Since CNAME record maps FQDNs.

We can right click on the record to delete or access properties to modify.

Under properties there is some basic info like the record name, FQDN and more.

And the security tab.

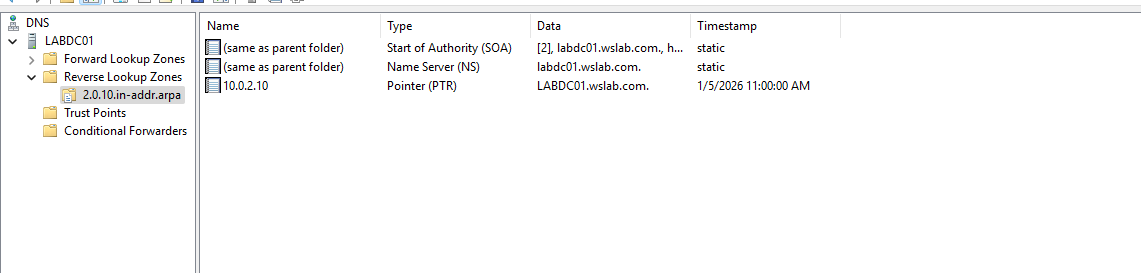


In this tab, we can modify who can have which access to these records.

We can allow the shared admin to have full access, write only, maybe read only or special permissions.

Now onto the reverse lookup zones.

We will create a new record as type PTR(Pointer).



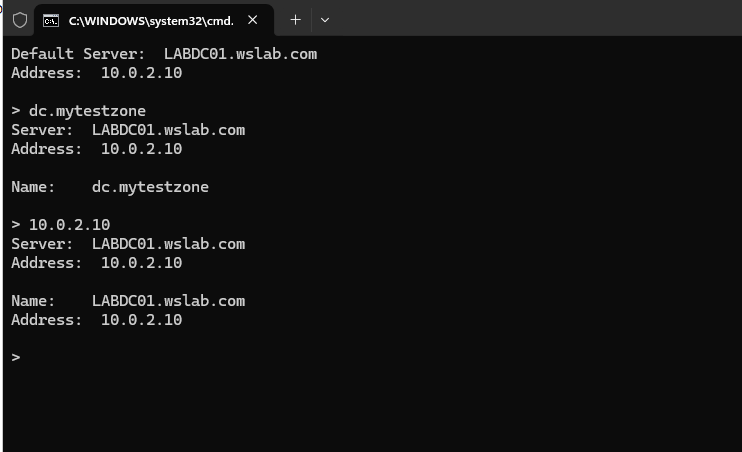
In this zone we will create a new PTR.

Right click the zone->new PTR

Create the new PTR record, in our case its 10.0.2.10 like the one in the image.

On the top left right click the DC name->launch ns lookup.

Now we are going to test the records we just made to see if they map the data properly.



We can see that it is working.

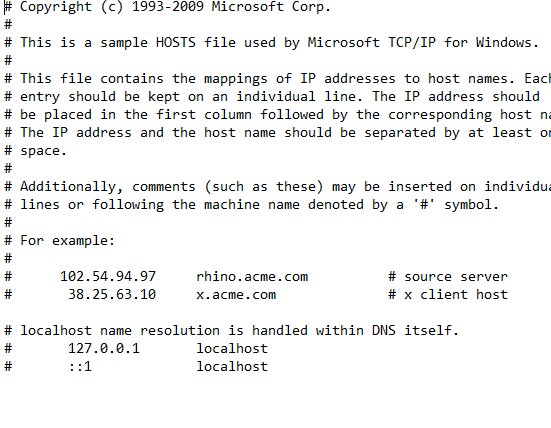
Now here are some more info about the DNS console tool.

We can access remote DNS server by right click on top left DNS->connect to DNS server->then choose the server’s name.

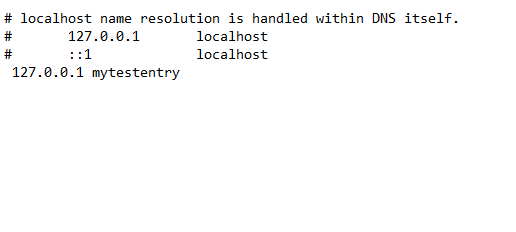
Now for our final thing we will look for the windows host file.

Host file were used before DNS to map info, and it still exits, open the files->C drive->windows->system32->drivers->etc.

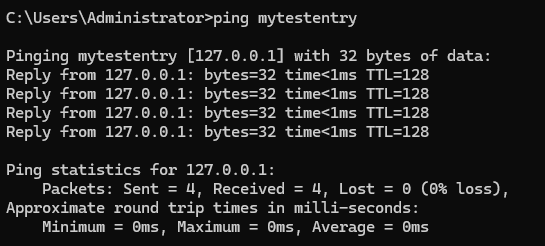
Inside etc there is a file called hosts.

It needs admin permissions so we open notepad as admin, then drag the hosts file inside.

Now we are going to add a loopback entry 127.0.0.1 to a test entry.



Now we test in nslookup.



We can see that our server is able to map mytestentry to a loopback address.