Windows Join Client to AD Lab
By Michael Ambeguia

Purpose: A vital step in Active Directory implementation is joining Windows client devices to the domain. The purpose of this lab is to practice joining a Windows client to an AD domain. I will take a 4 step approach to completing this lab. The first step will be doing some preparation on the DC side. I need a domain administrator account to join the client device. In step 2 I will prepare the client by setting the appropriate network configuration for it (DNS server), make sure the client can resolve the Domain Controller's hostname, then make sure the time is synchronized and correct. In step 3 I will join the client to the domain, using the domain administrator account to do so. Lastly, in step 4 I will verify that the connection worked both on the client side (system info) and server side (Computers OU). Learning how devices are connected to an AD domain will help me further expand my Windows system administration skills and my understanding of Active Directory.

Sections:

1. Prepare Domain Controller

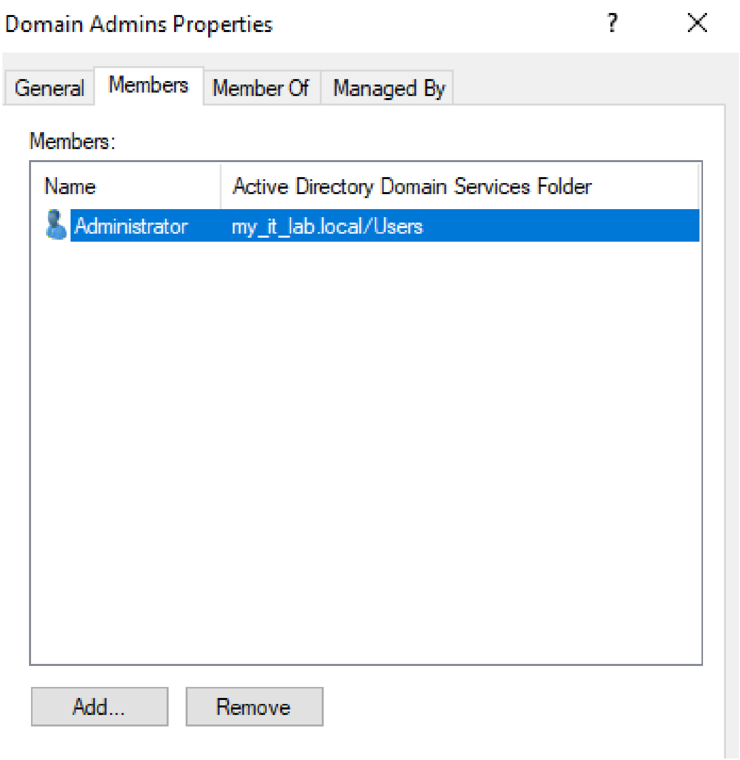
2. Prepare Client

3. Join Client

4. Verify Join

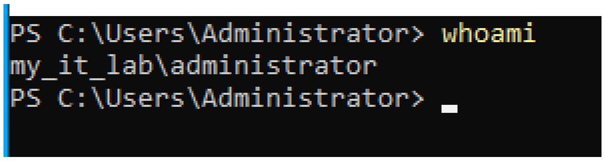
Section #1 Prepare DC:

1.1 Identify Domain Administrator account:



Name	Active Directory Domain Services Folder
Administrator	my_it_lab.local/Users

The Administrator account is part of the Domain Admins security group.

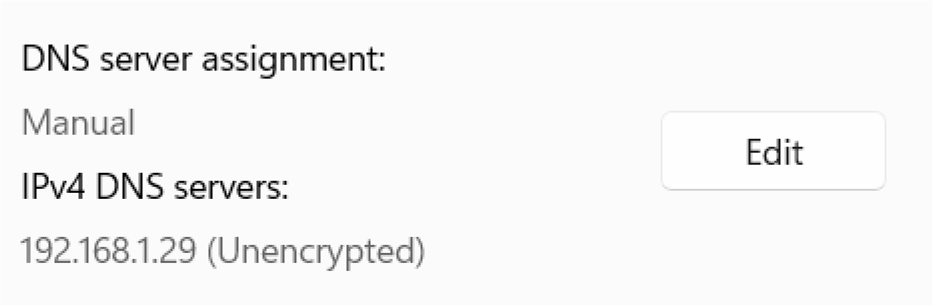


```
PS C:\Users\Administrator> whoami
my_it_lab\administrator
PS C:\Users\Administrator> _
```

Section #2 Prepare Client:

2.1 Verify the DC ip is set as the DNS server address:

The client needs to have the domain controller ip address set as its DNS server. The reason why is that is the only way the client can resolve the hostname for the DC.



DNS server assignment:

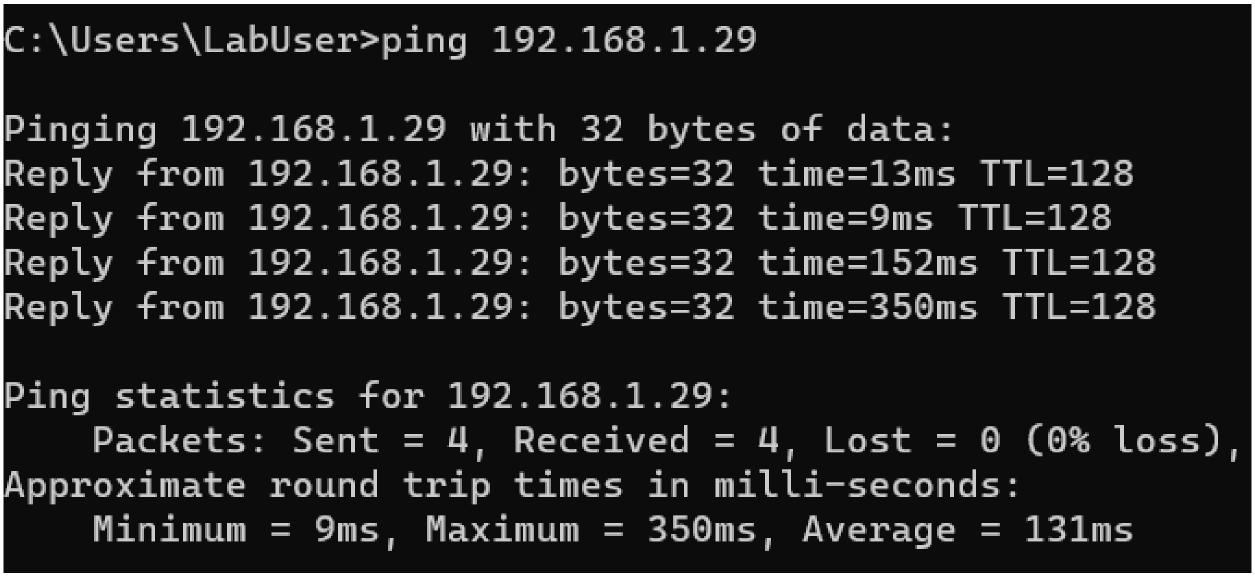
Manual

IPv4 DNS servers:

192.168.1.29 (Unencrypted)

2.2 Ping the DC:

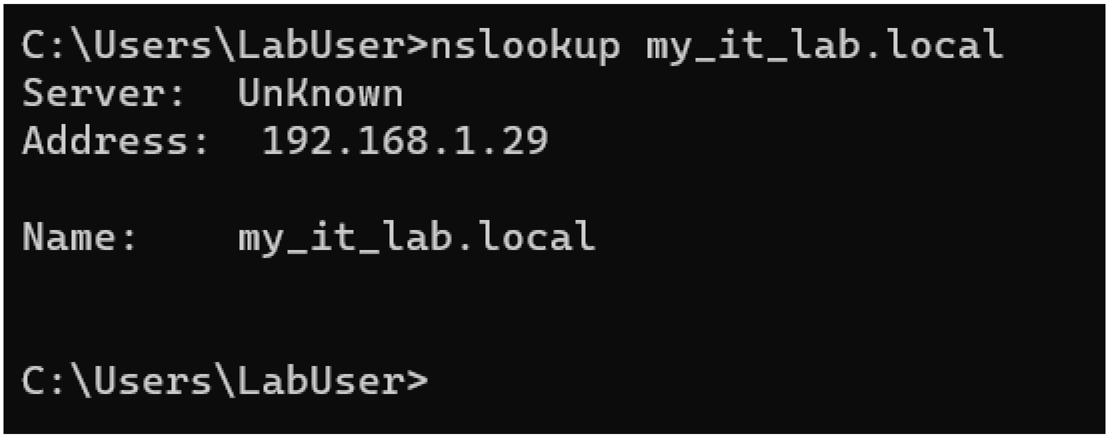
On the client it would be a great idea to ping the DC to check that it can be reached.



```
C:\Users\LabUser>ping 192.168.1.29

Pinging 192.168.1.29 with 32 bytes of data:
Reply from 192.168.1.29: bytes=32 time=13ms TTL=128
Reply from 192.168.1.29: bytes=32 time=9ms TTL=128
Reply from 192.168.1.29: bytes=32 time=152ms TTL=128
Reply from 192.168.1.29: bytes=32 time=350ms TTL=128

Ping statistics for 192.168.1.29:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 9ms, Maximum = 350ms, Average = 131ms
```

2.3 Use nslookup to verify that DNS works:

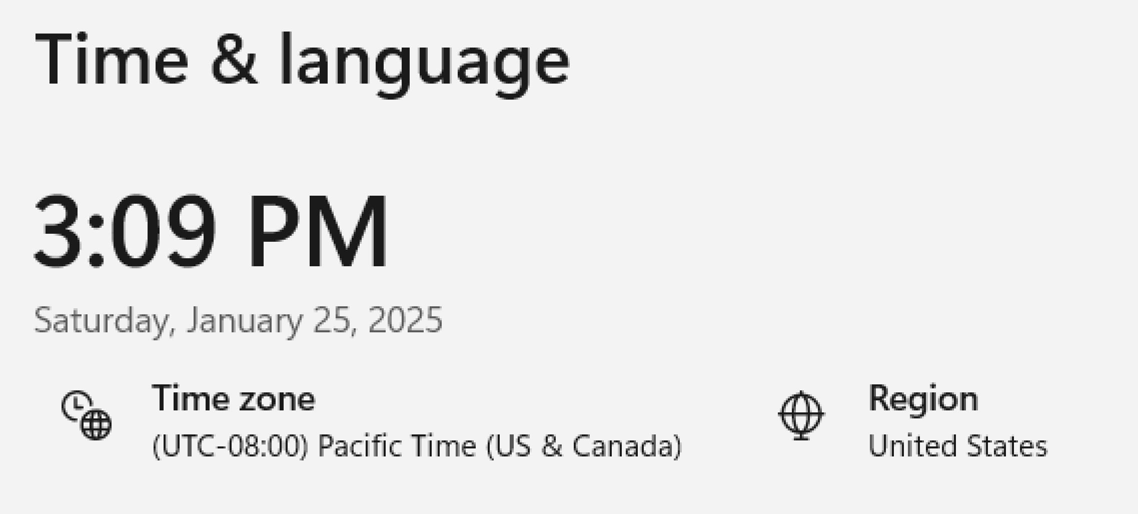
On the client you should also check if the DNS server you configured works and that you can resolve the hostname of the DC.



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

Name:    my_it_lab.local


C:\Users\LabUser>
```

The hostname for the DC is resolved. That means that the DNS configuration on the client is correct.

2.4 Make sure the time is synchronized with the DC:



Time & language

3:09 PM

Saturday, January 25, 2025

Time zone
(UTC-08:00) Pacific Time (US & Canada)

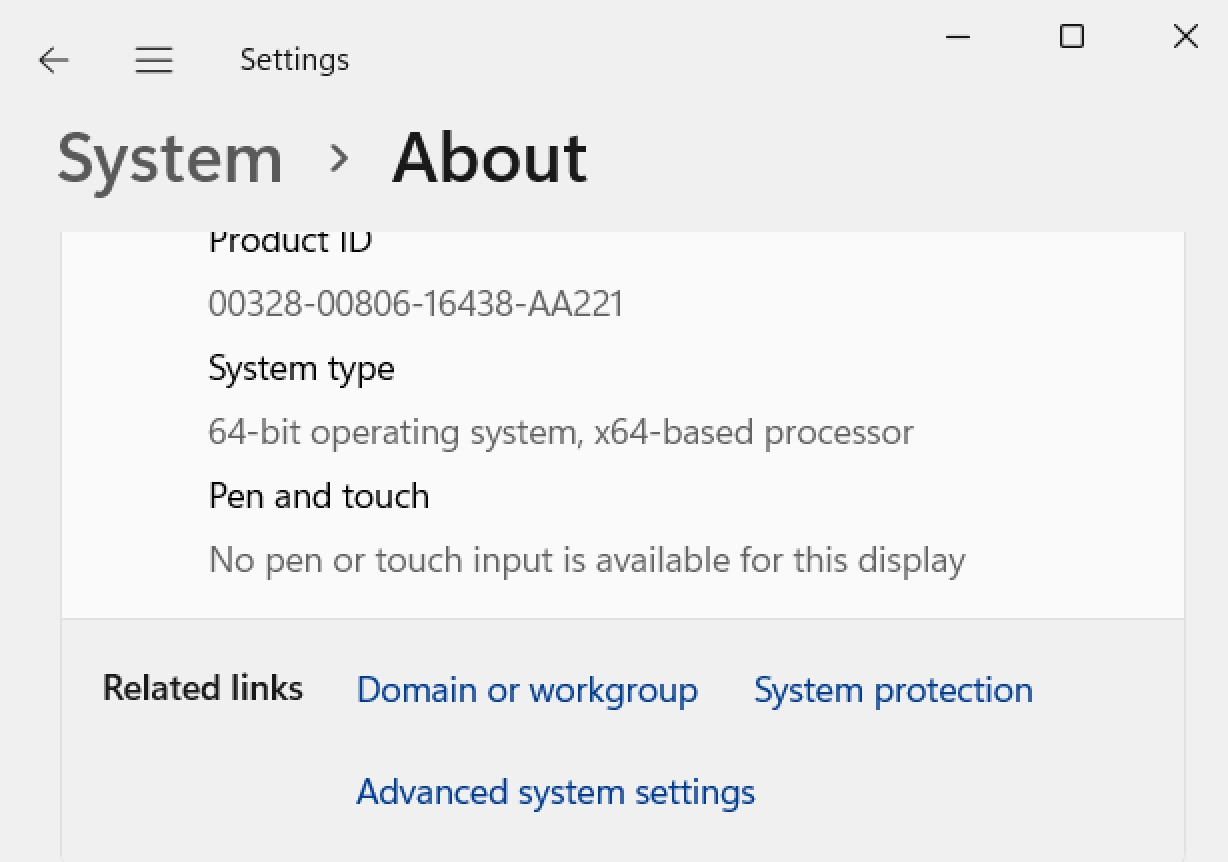
Region
United States

The time zone and time is correct on the client and matches what is on the DC.

Section #3 Join Client:

3.1 Join client to AD using domain admin credentials:

Go to settings/system/about/Domain or workgroup.



System › About

Product ID

00328-00806-16438-AA221

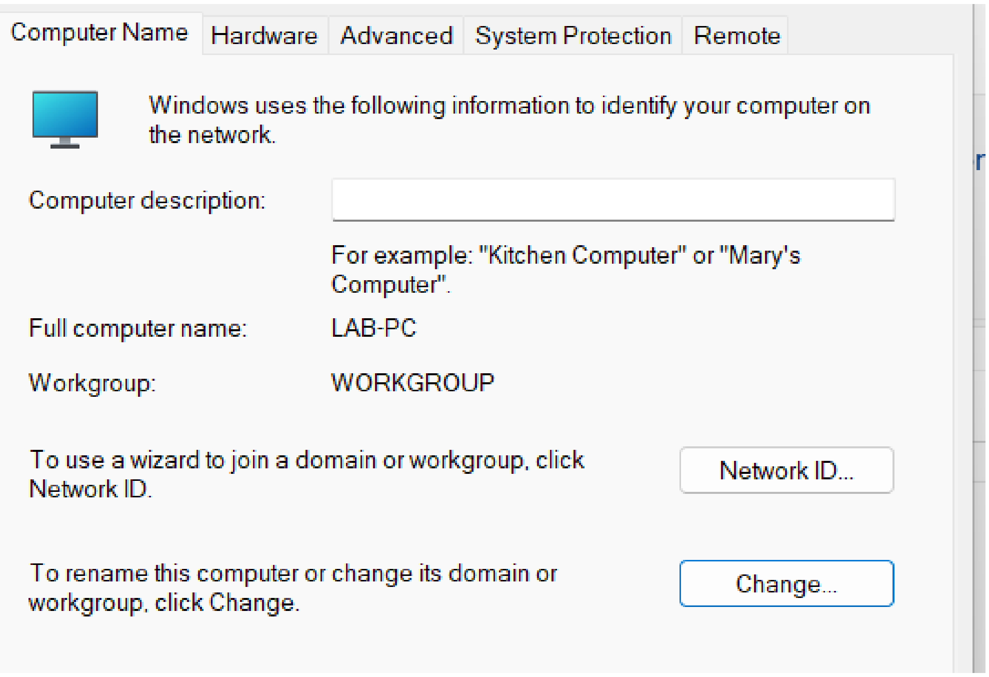
System type

64-bit operating system, x64-based processor

Pen and touch

No pen or touch input is available for this display

Click on Advanced settings then click on change.



Windows uses the following information to identify your computer on the network.

Computer description:

For example: "Kitchen Computer" or "Mary's Computer".

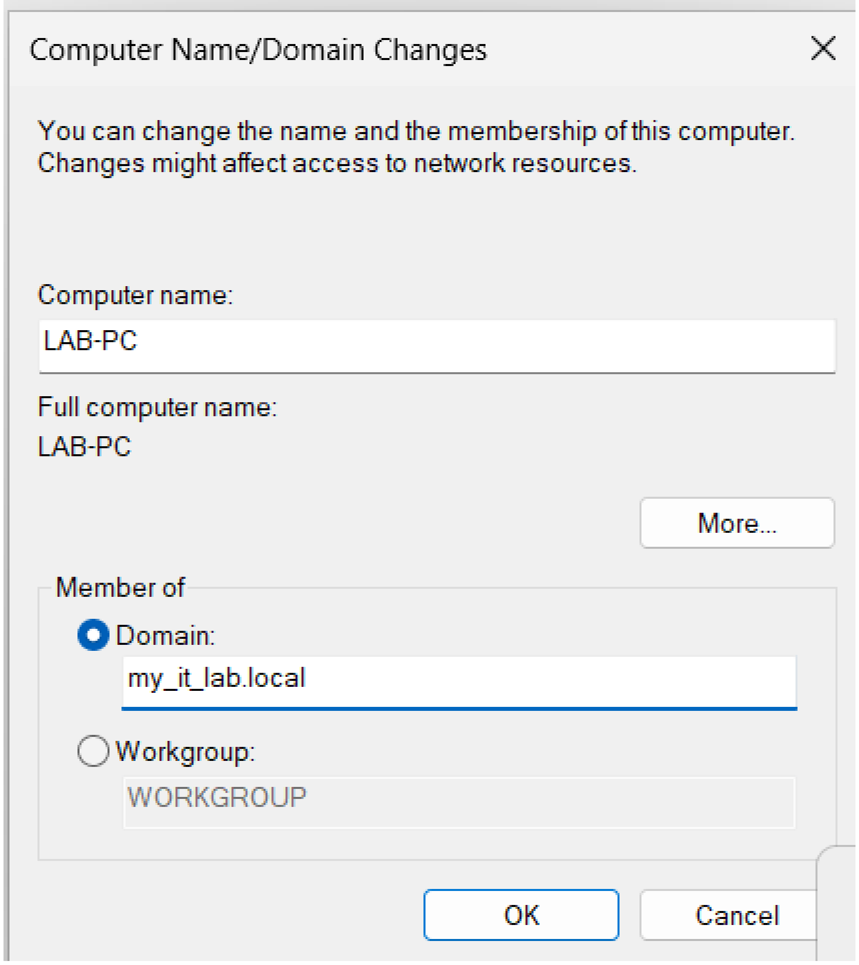
Full computer name: LAB-PC

Workgroup: WORKGROUP

To use a wizard to join a domain or workgroup, click Network ID.

To rename this computer or change its domain or workgroup, click Change.

Enter in the domain you want to join.



Computer Name/Domain Changes

You can change the name and the membership of this computer. Changes might affect access to network resources.

Computer name:
LAB-PC

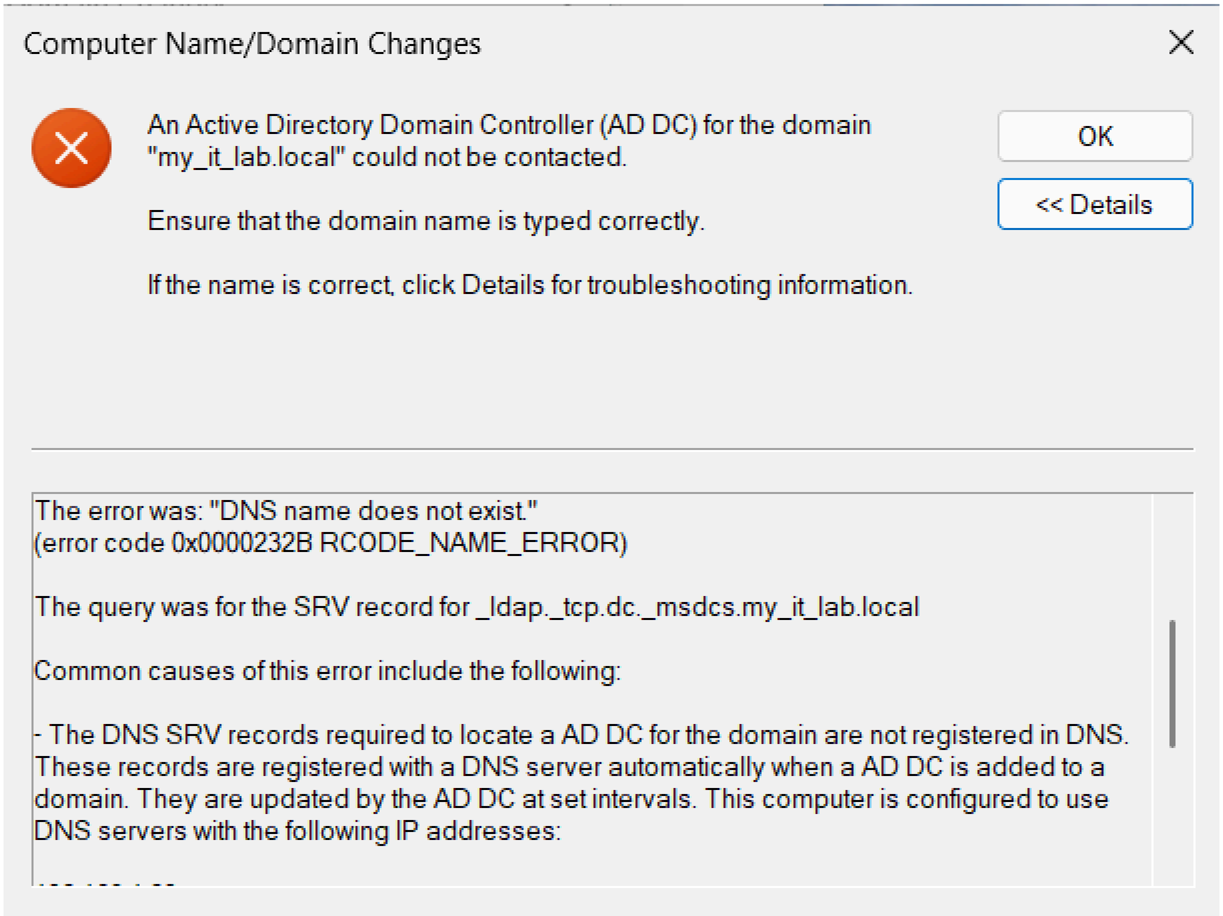
Full computer name:
LAB-PC

Member of

● Domain:
my_it_lab.local

○ Workgroup:
WORKGROUP

Unfortunately after I clicked okay I ran into an error. Apparently I am missing SRV records in my DC’s DNS service. SRV records are needed for allowing the client to find where certain services essential for AD functioning (LDAP) can be found on the DC.



An Active Directory Domain Controller (AD DC) for the domain "my_it_lab.local" could not be contacted.

Ensure that the domain name is typed correctly.

If the name is correct, click Details for troubleshooting information.

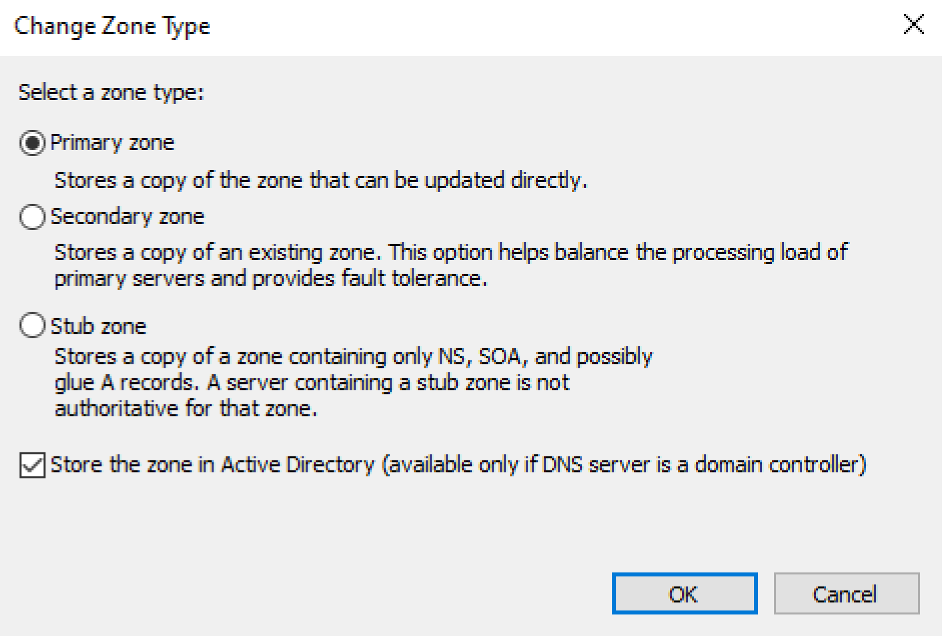
The error was: "DNS name does not exist."
(error code 0x0000232B RCODE_NAME_ERROR)

The query was for the SRV record for _ldap._tcp.dc._msdcs.my_it_lab.local

Common causes of this error include the following:

- The DNS SRV records required to locate a AD DC for the domain are not registered in DNS. These records are registered with a DNS server automatically when a AD DC is added to a domain. They are updated by the AD DC at set intervals. This computer is configured to use DNS servers with the following IP addresses:

In order to resolve this issue I had to integrate my DNS service with AD. To do this, I configured my forward lookup zone to be stored in AD (it is integrated with AD).



Change Zone Type

Select a zone type:

● Primary zone

Stores a copy of the zone that can be updated directly.

○ Secondary zone

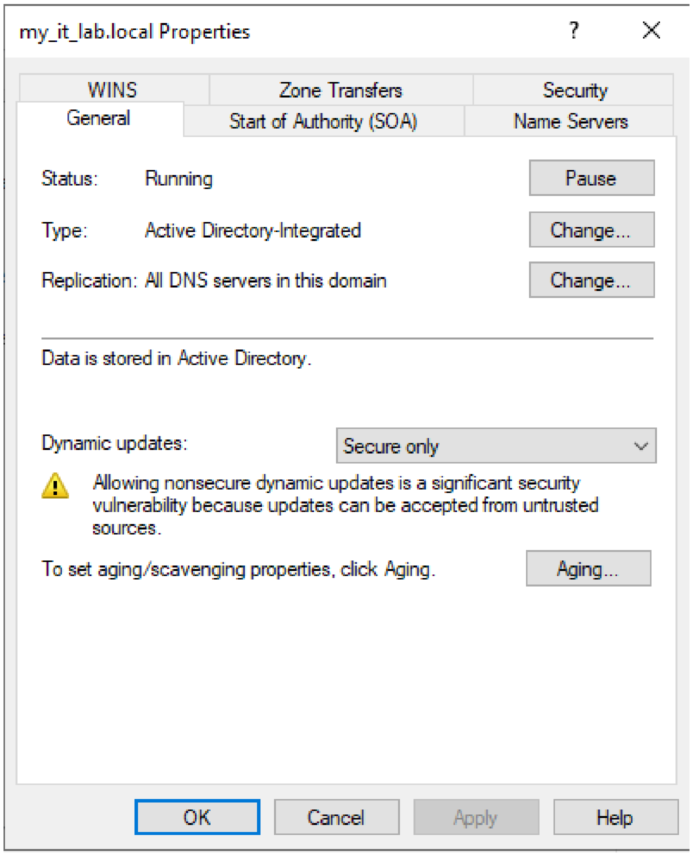
Stores a copy of an existing zone. This option helps balance the processing load of primary servers and provides fault tolerance.

○ Stub zone

Stores a copy of a zone containing only NS, SOA, and possibly glue 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 domain controller)

After I integrated the forward lookup zone with AD I double checked the zone's type. It is AD-Integrated!



my_it_lab.local Properties

Status: Running

Type: Active Directory-Integrated

Replication: All DNS servers in this domain

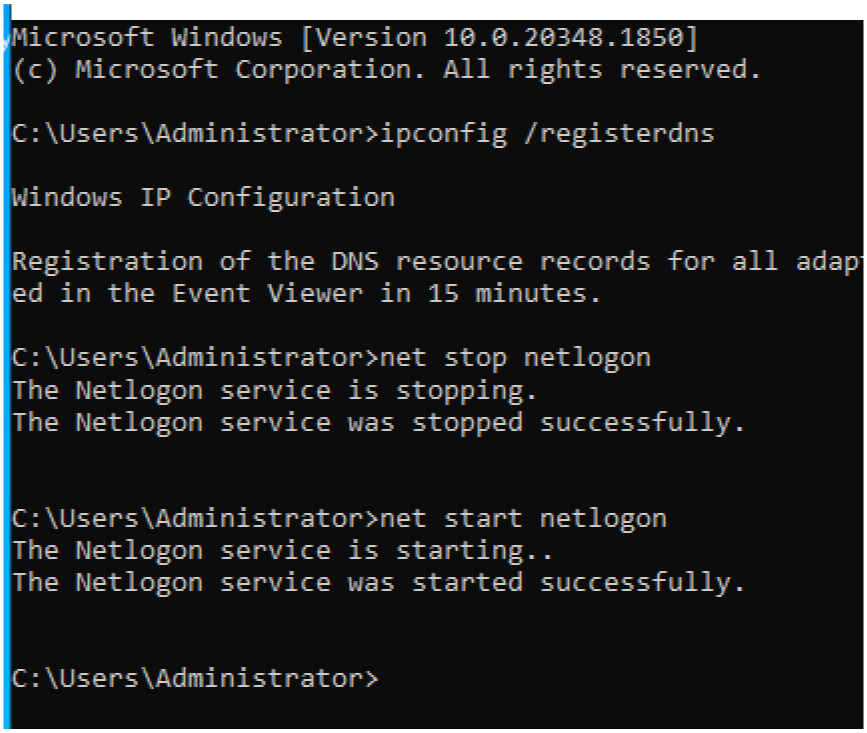
Data is stored in Active Directory.

Dynamic updates: Secure only

Allowing nonsecure dynamic updates is a significant security vulnerability because updates can be accepted from untrusted sources.

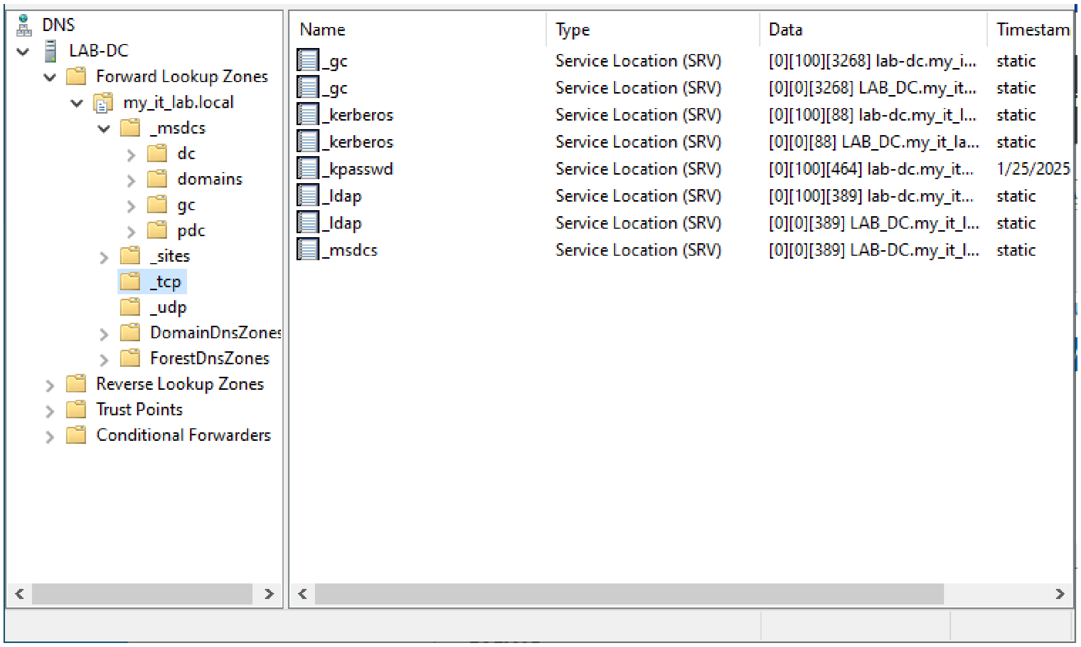
To set aging/scavenging properties, click Aging.

The last thing I had to do was register the dns record via the command prompt.



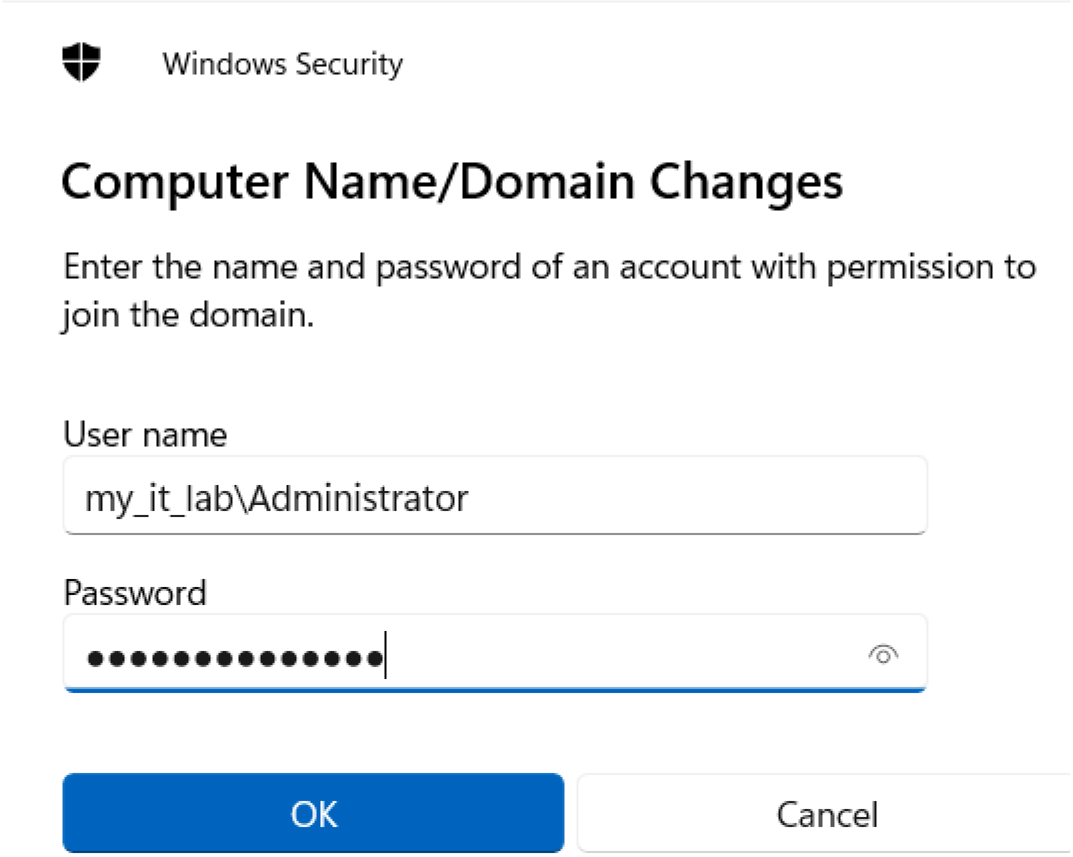
```
Microsoft Windows [Version 10.0.20348.1850]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ipconfig /registerdns

Windows IP Configuration

Registration of the DNS resource records for all adap
ed in the Event Viewer in 15 minutes.

C:\Users\Administrator>net stop netlogon
The Netlogon service is stopping.
The Netlogon service was stopped successfully.


C:\Users\Administrator>net start netlogon
The Netlogon service is starting..
The Netlogon service was started successfully.


C:\Users\Administrator>
```

Now the SRV records necessary for AD functioning are present under my forward lookup zone. There are SRV records for LDAP, Kerberos, GC, and MSDCS.



Name	Type	Data	Timestam
_gc	Service Location (SRV)	[0][100][3268] lab-dc.my_i...	static
_gc	Service Location (SRV)	[0][0][3268] LAB_DC.my_it...	static
_kerberos	Service Location (SRV)	[0][100][88] lab-dc.my_it_l...	static
_kerberos	Service Location (SRV)	[0][0][88] LAB_DC.my_it_la...	static
_kpasswd	Service Location (SRV)	[0][100][464] lab-dc.my_it...	1/25/2025
_ldap	Service Location (SRV)	[0][100][389] lab-dc.my_it...	static
_ldap	Service Location (SRV)	[0][0][389] LAB_DC.my_it_l...	static
_msdcs	Service Location (SRV)	[0][0][389] LAB-DC.my_it_l...	static

Back on the Windows 11 client I am now able to add the device to the domain.



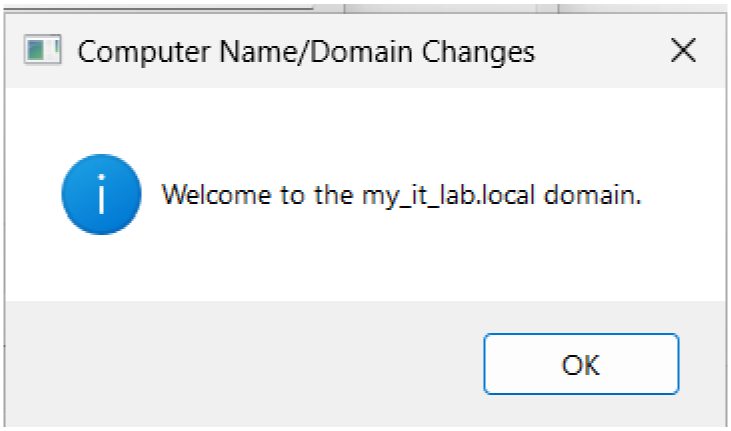
Windows Security

Computer Name/Domain Changes

Enter the name and password of an account with permission to join the domain.

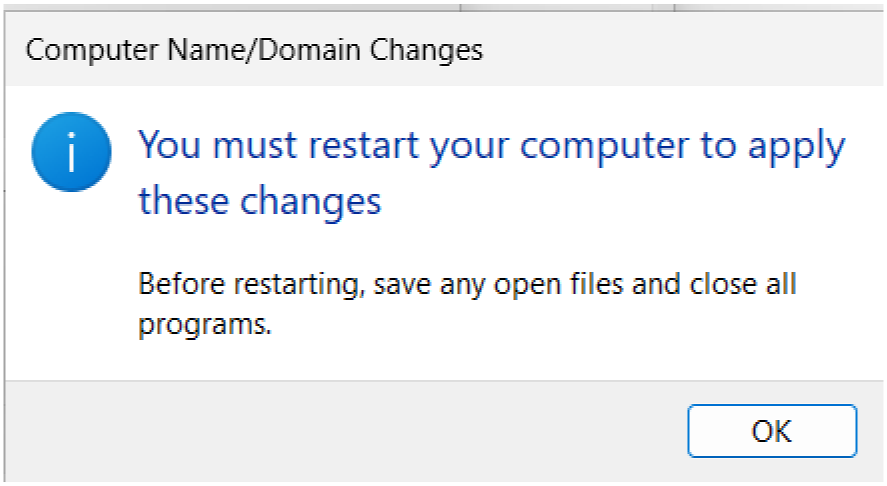
User name: my_it_lab\Administrator

Password: ••••••••••••••



Computer Name/Domain Changes

Welcome to the my_it_lab.local domain.

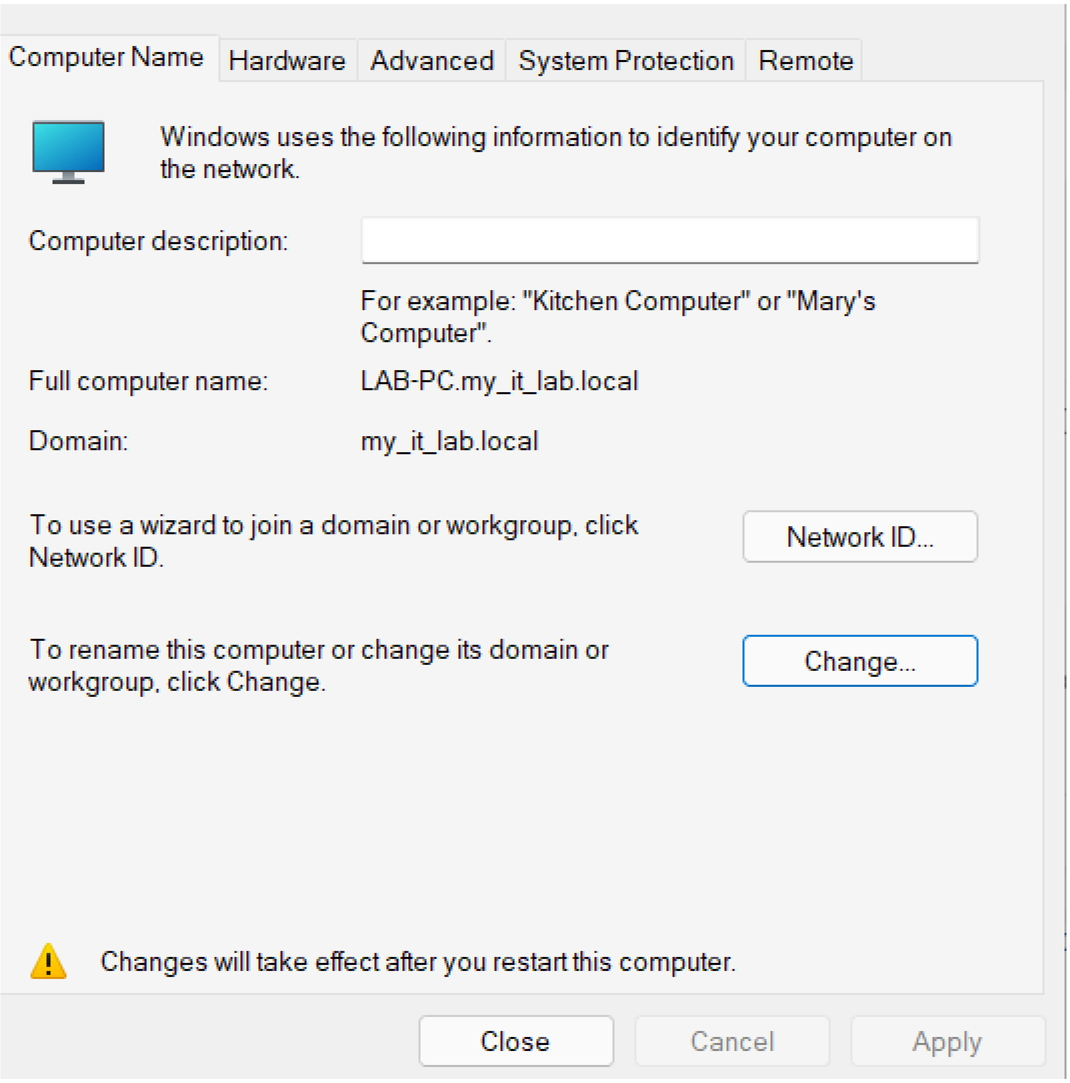


Computer Name/Domain Changes

You must restart your computer to apply these changes

Before restarting, save any open files and close all programs.

Now it shows that the client is a part of the my_it_lab.local domain!



Windows uses the following information to identify your computer on the network.

Computer description:

For example: "Kitchen Computer" or "Mary's Computer".

Full computer name: LAB-PC.my_it_lab.local

Domain: my_it_lab.local

To use a wizard to join a domain or workgroup, click Network ID.

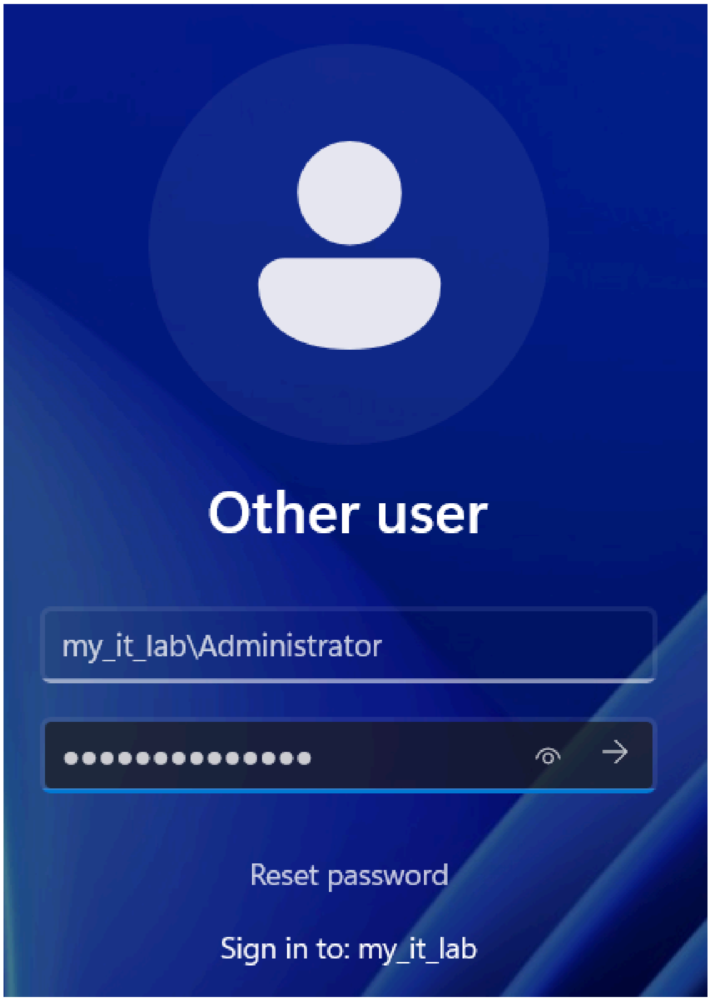
To rename this computer or change its domain or workgroup, click Change.

Changes will take effect after you restart this computer.

Section #4 Verify Join:

4.1 Verify join by using domain admin credentials to log into client:

On the Windows 11 client I signed using the Domain Admin credentials. ***Note that I had to use the name of the domain followed by a \\.***

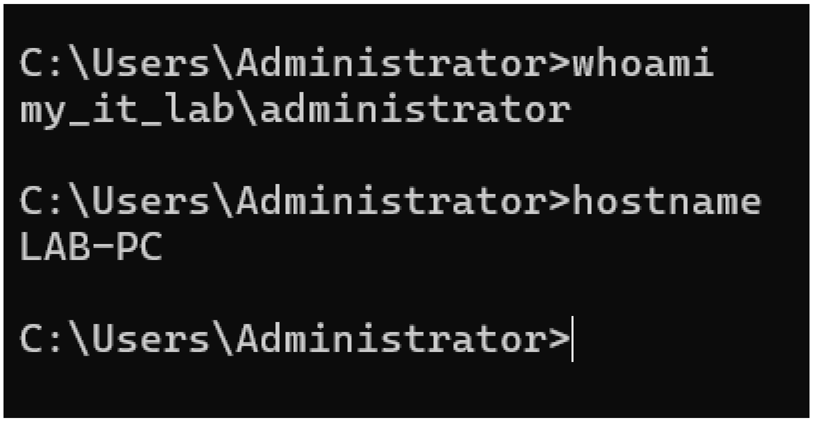


Other user

my_it_lab\Administrator

●●●●●●●●●●●●●●

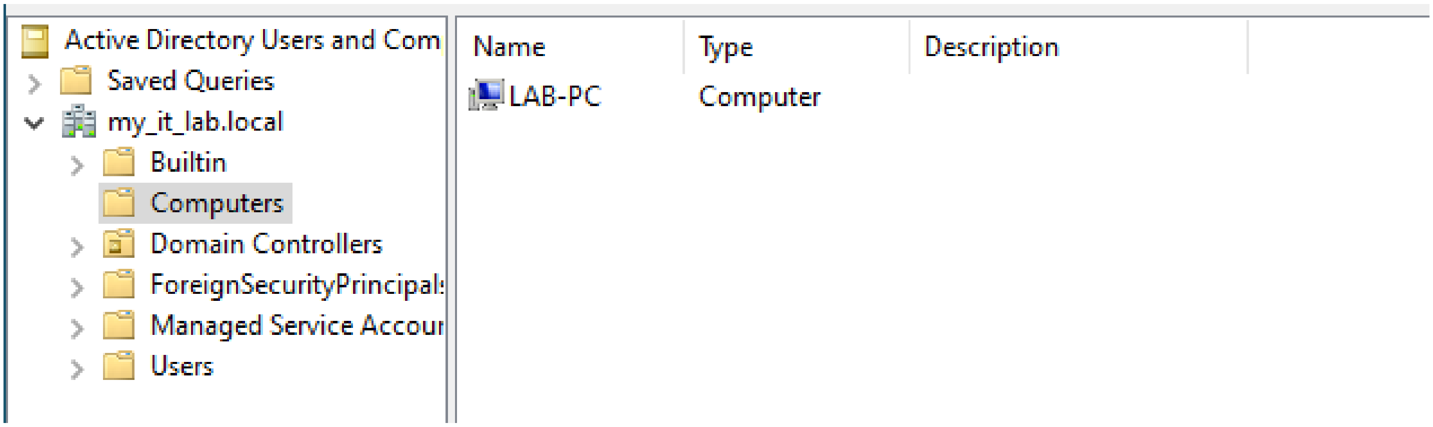
After successful authentication I double checked that the domain admin account is signed in to the client using the domain admin account.



```
C:\Users\Administrator>whoami
my_it_lab\administrator

C:\Users\Administrator>hostname
LAB-PC

C:\Users\Administrator>
```

4.2 Additionally, verify the join by looking at AD Users and Computers on DC:

Now that the client is joined to the domain it is put in the built-in and default container for newly joined devices, the Computers OU.



Name	Type	Description
LAB-PC	Computer	