Deploying an On-Premises Active Directory

Part 1: Deploying an Active Directory using Azure Virtual Machines

1 Introduction **2**
1.1 What is an Active Directory? And why would you set one up with Microsoft Azure? 2
1.2 Resources and Software tools we'll be using 2
2 Setting up the Virtual Machines **3**
2.1 Setting up Windows Server VM on Azure 3
2.2 Setting up Windows 10 VM on Azure 9
3 Setting up Windows Server VM **15**
3.1 Configuring Firewall 16
3.2 Setting up Active Directory 17
3.3 Creating Domain Controller 19
3.4 Creating Organisational Units 22
3.5 Logging in as Admin 25
4 Setting up Client VM **26**
4.1 Matching the DNS server 26
4.2 Observing the DNS changes 28
4.3 Having a Client connect to the Active Directory VM 29
5 Conclusion **33**

1 Introduction

1.1 What is an Active Directory? And why would you set one up with Microsoft Azure?

Setting up an Active Directory (AD) on Microsoft is a valuable exercise in modern enterprise infrastructure management. This project will document my process of establishing an AD environment using Azure Virtual Networks, subnets, and virtual machines running Windows Server 2022 and Windows 10.

Active Directory is a crucial component for organisations, providing centralised authentication, authorisation, and directory services. Implementing AD on Azure offers several compelling benefits:

1. Scalability: Easily adjust resources to meet changing organisational needs.
2. High availability: Leverage Azure's robust infrastructure for improved uptime.
3. Cost-effectiveness: Reduce on-premises hardware and maintenance costs.
4. Global accessibility: Enable secure access to resources from anywhere in the world.
5. Integration: Seamlessly connect with other Azure and Microsoft 365 services.

By creating an AD environment in Azure, organisations can modernise their infrastructure, improve remote work capabilities, and streamline identity management. This project will provide hands-on experience with cloud-based network configuration and virtual machine management within the Azure ecosystem.

Through this endeavour, I aim to gain practical insights into the deployment and management of cloud-based Active Directory services, enhancing my understanding of enterprise-level identity and access management in a cloud environment.

1.2 Resources and Software tools we'll be using

The Azure resources we'll be creating and working with:

- Azure Virtual Networks and Subnets
- Azure Virtual Machines (Windows Server 2022 and Windows 10)

Software/Tools we'll be using to configure Active Directory:

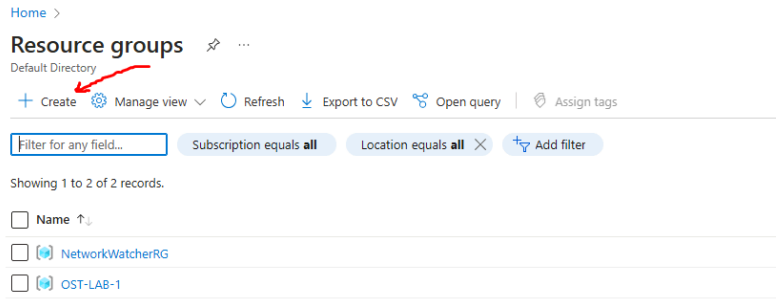
- Server Manager
- Command Prompt

2 Setting up the Virtual Machines

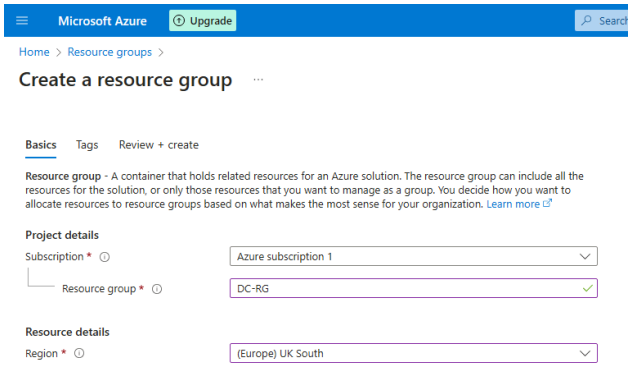
During this section, I'll be setting up the Windows Server and Windows 10 Virtual Machines on Azure. The Windows Server will be made as our Active Directory Domain Controller, and the Windows 10 Machine will be our client machine.

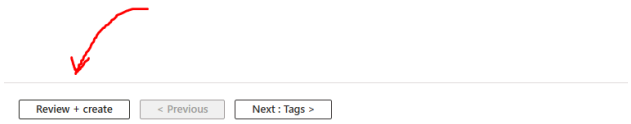
2.1 Setting up Windows Server VM on Azure

Go to portal.azure.com > resource groups



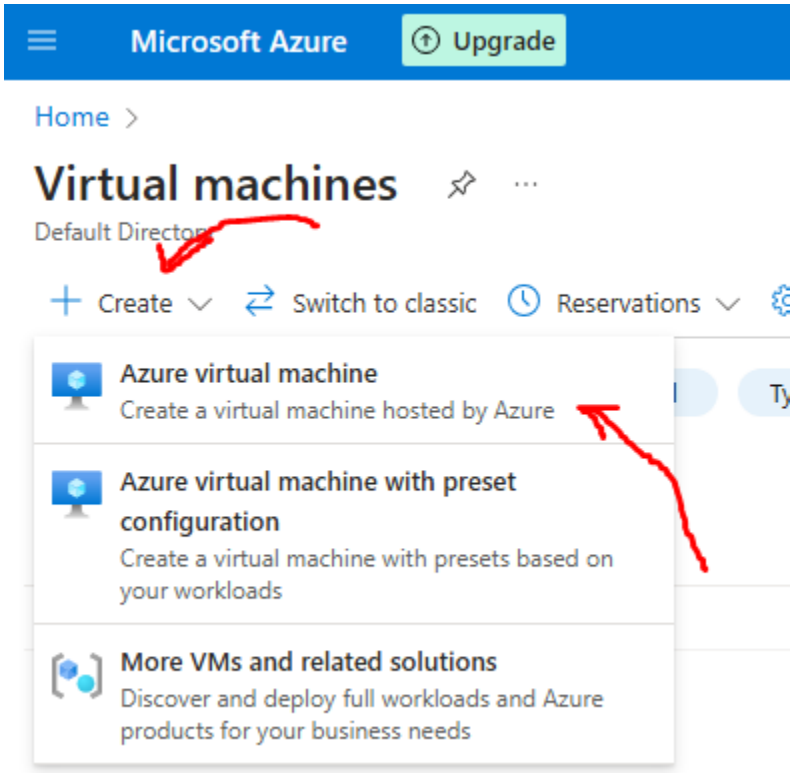
- Select Create



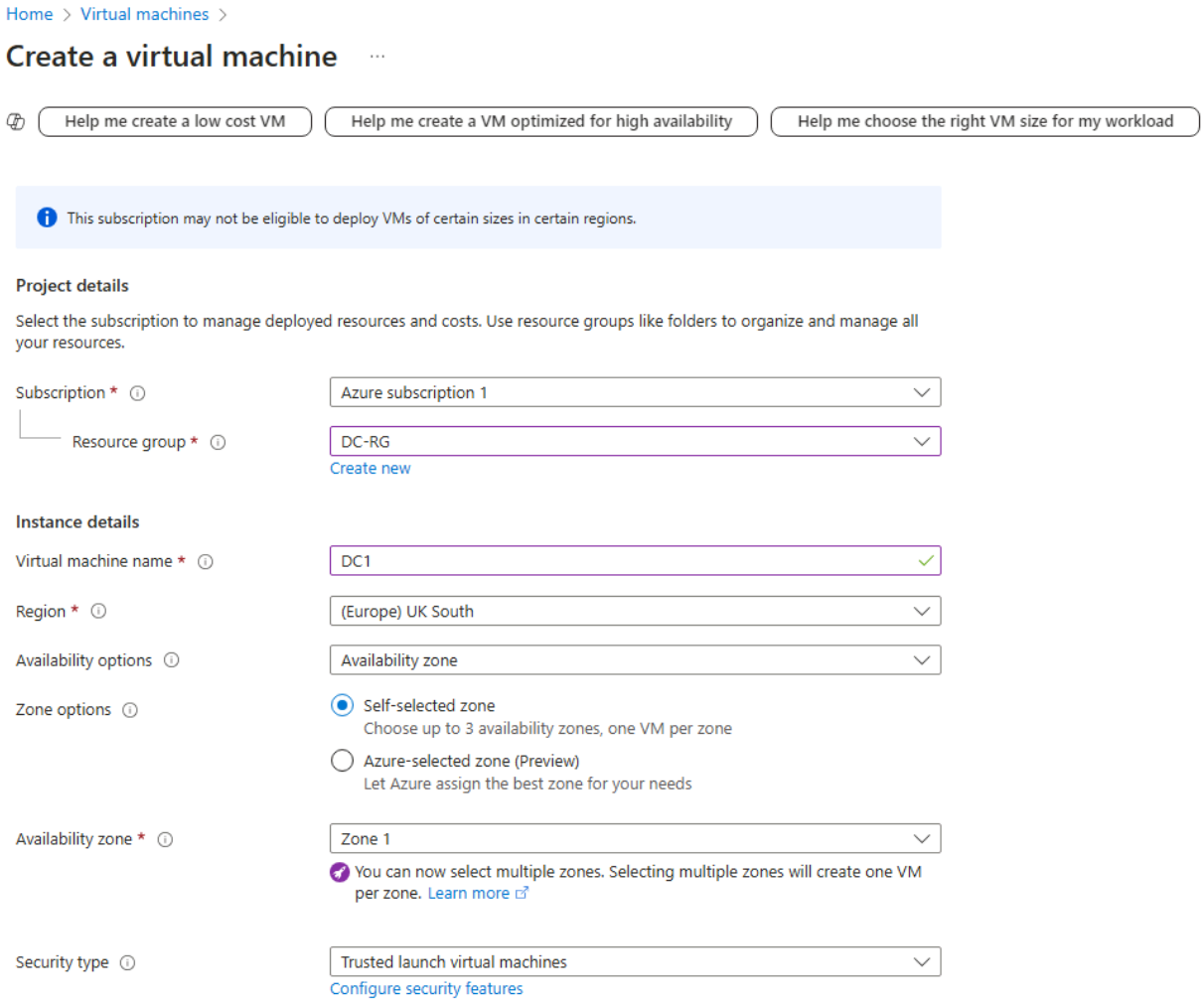


- I'm naming it as DC-RG (Domain Controller - Resource Group)
- Selected UK South as region as it's the closest server to me
- Press Review + Create

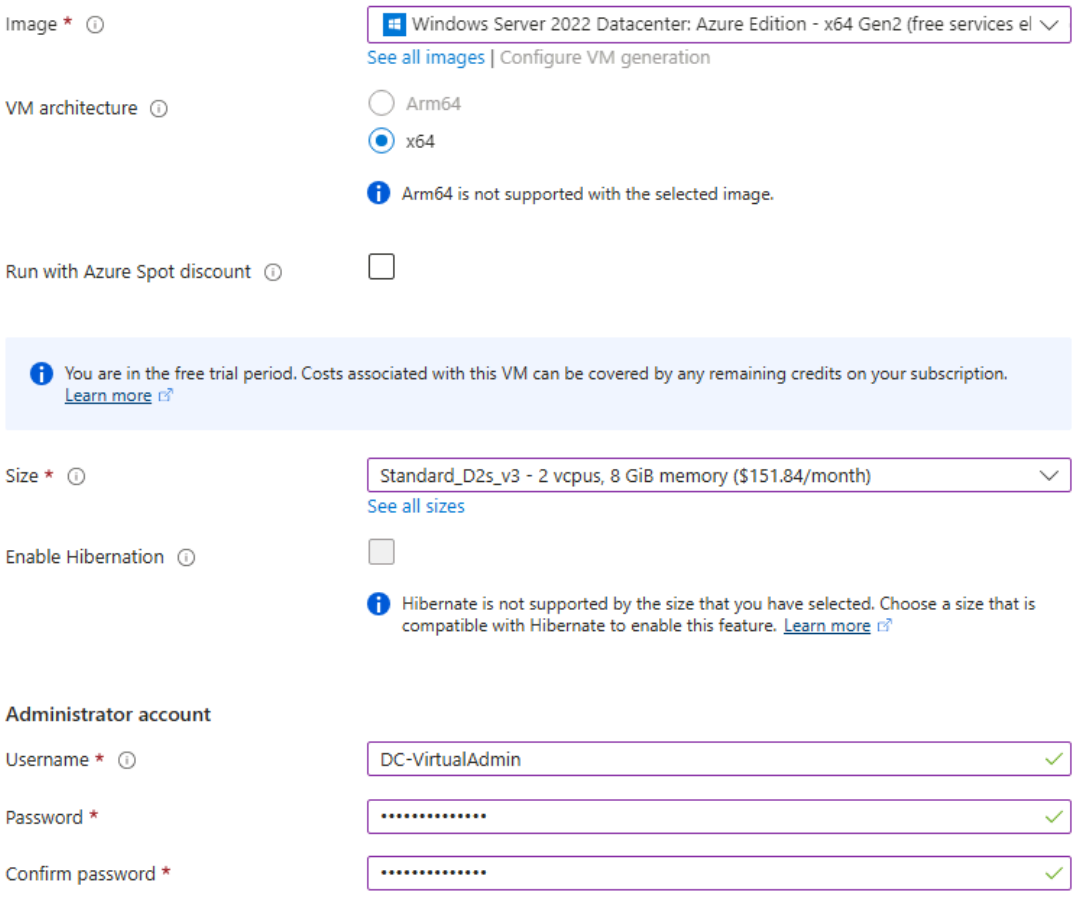
We'll now set up a Virtual Machine. Search for Virtual Machines



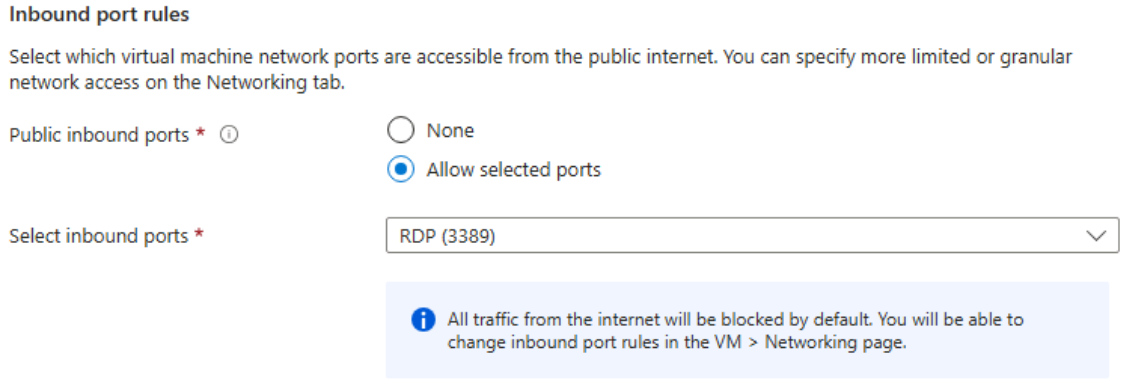
- Select Create
- Azure Virtual Machine



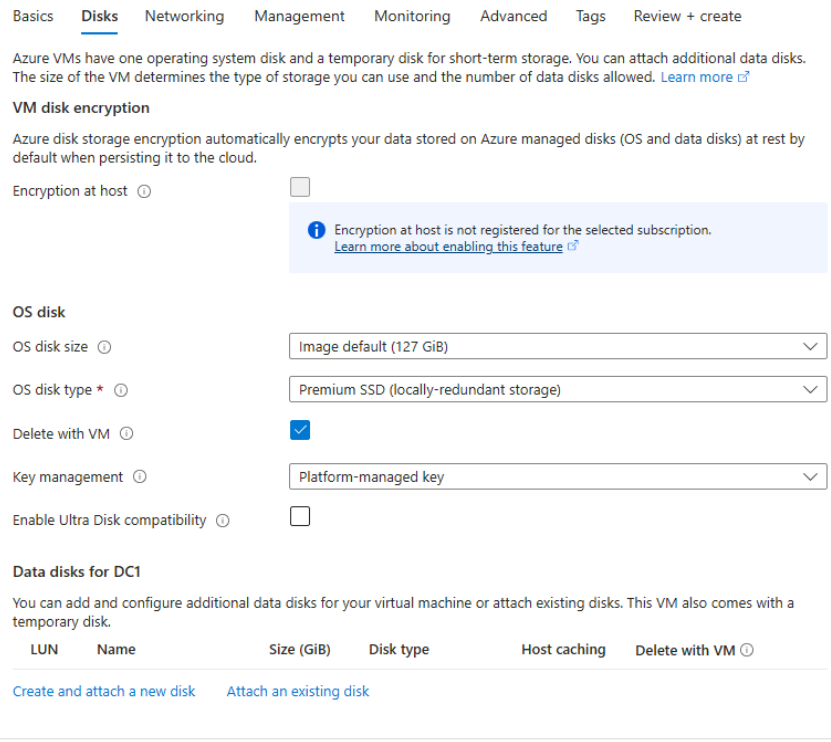
- Fill in the details as shown
- Select DC-RG resource group we made
- You can name the VM what you want, I named it DC1
- Select closest region
- Everything else should be default in this screenshot



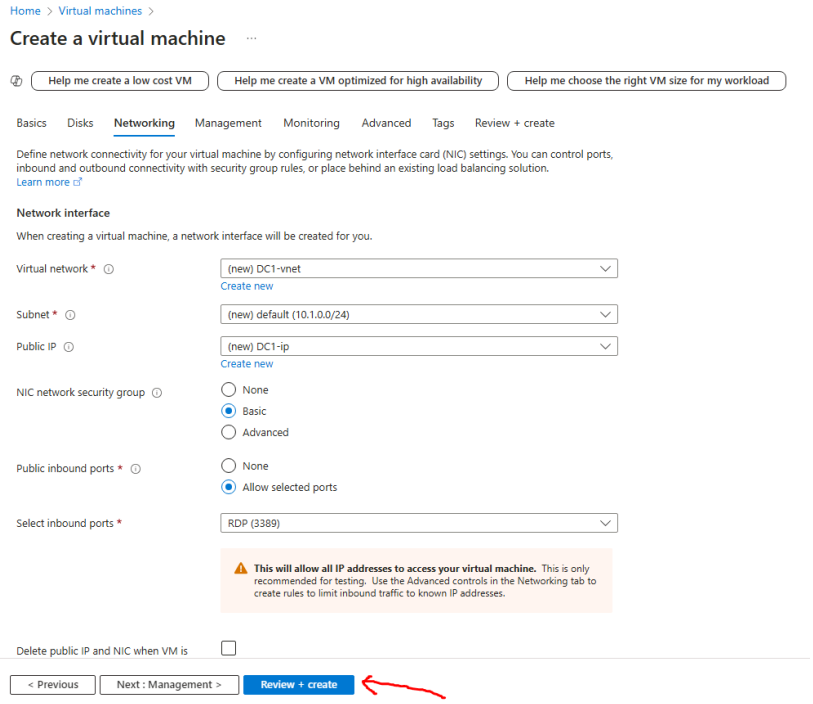
- Image will be Windows Server 2022
- Size can be your choice, I picked 2 cores for demonstration purposes and ease of setting up.
- Username can be whatever you want. I called mine DC-VirtualAdmin
- Make a strong password



- Here I've selected RDP - We need this inbound port as we'll be accessing this VM remotely.
- After this press Next : Disks >



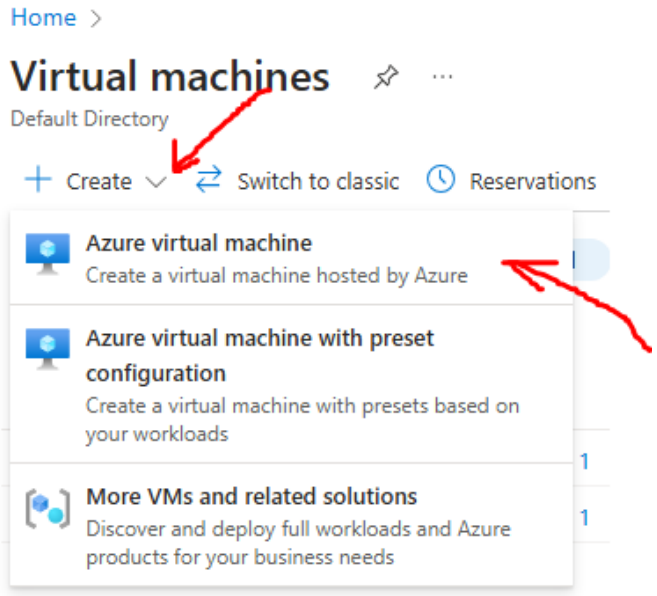
- We can keep this the same. Click Next : Networking >



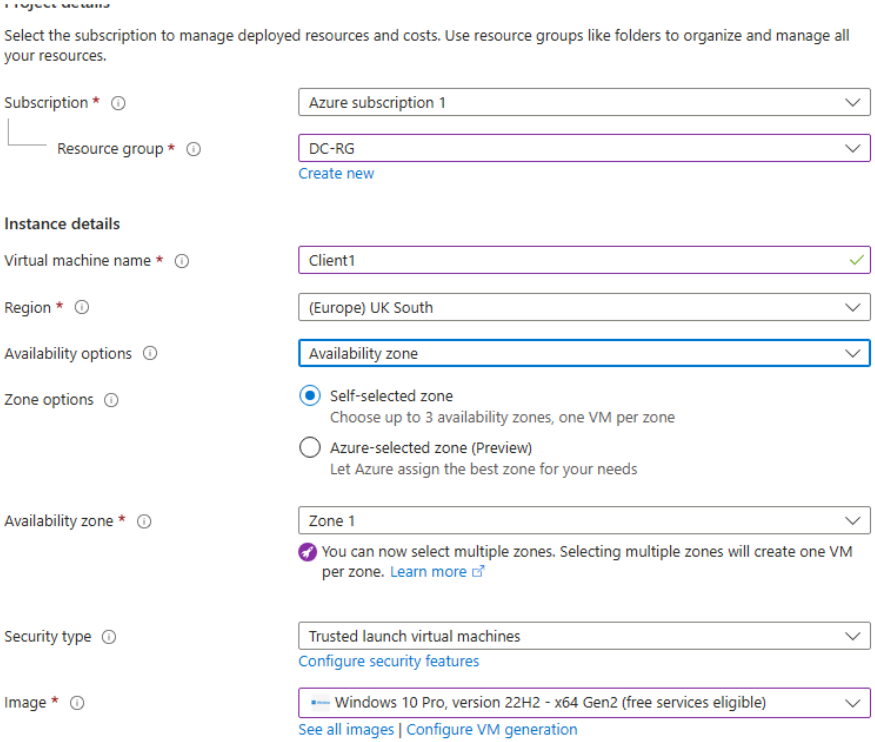
- As long as you have the same settings as I have - which is default - you're good to go
- Click on Review + create

2.2 Setting up Windows 10 VM on Azure

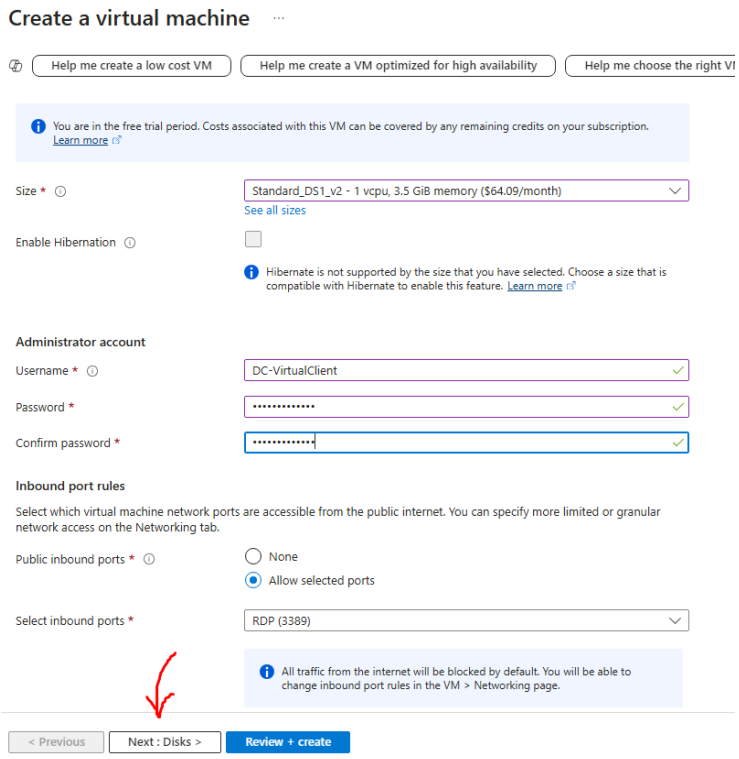
Now we'll be setting up the Windows 10 VM



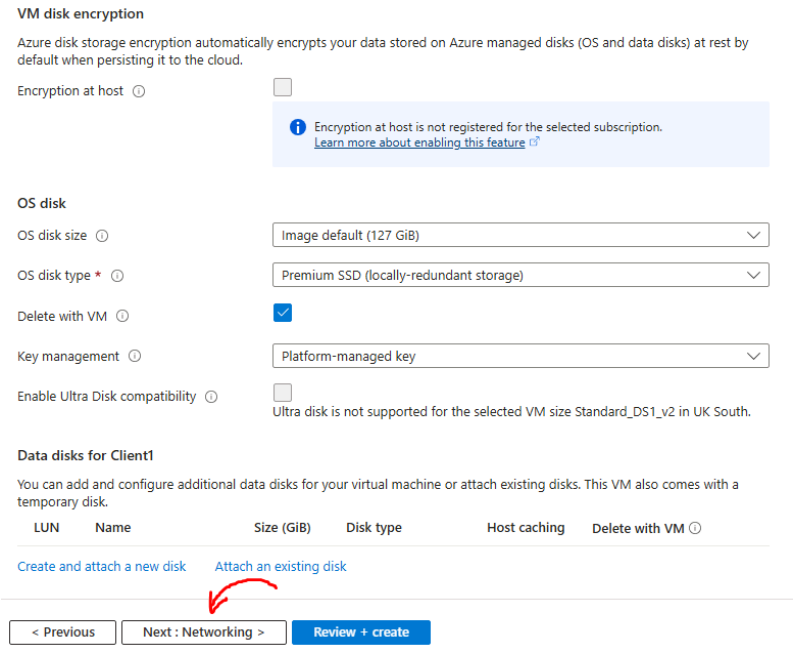
- Create an Azure Virtual Machine



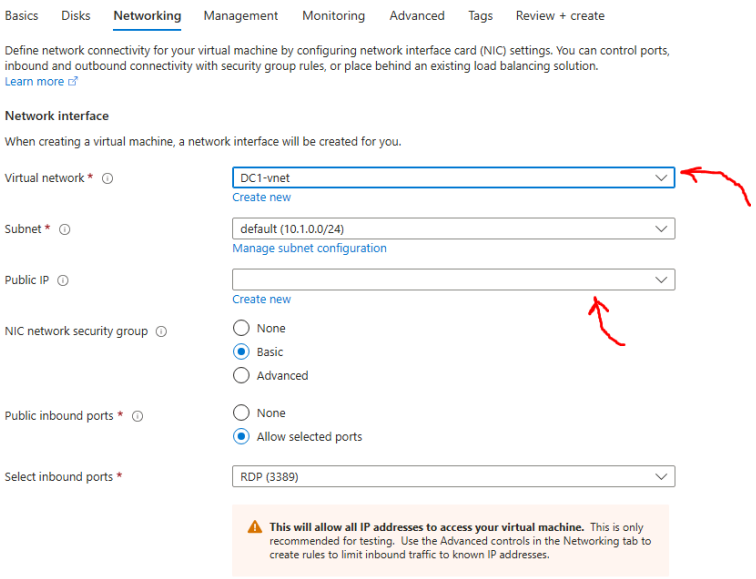
- Select these options. Similar as before, only difference is name & Image
- Name: Client1
- Image: Windows 10 Pro



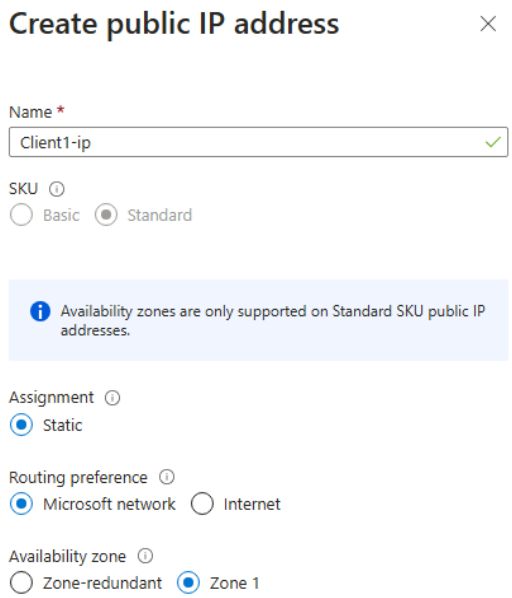
- Select a size, I've gone for a smaller size because I've run out of CPUs for my trial
- Remember your username nas pass
- Select Next : Disks >



- Everything should be as shown.
- Click Next : Networking >

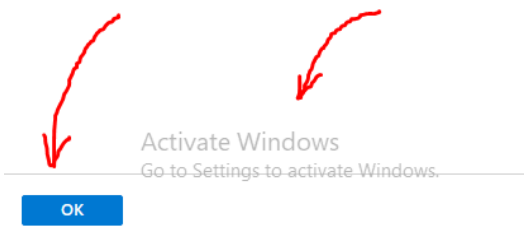


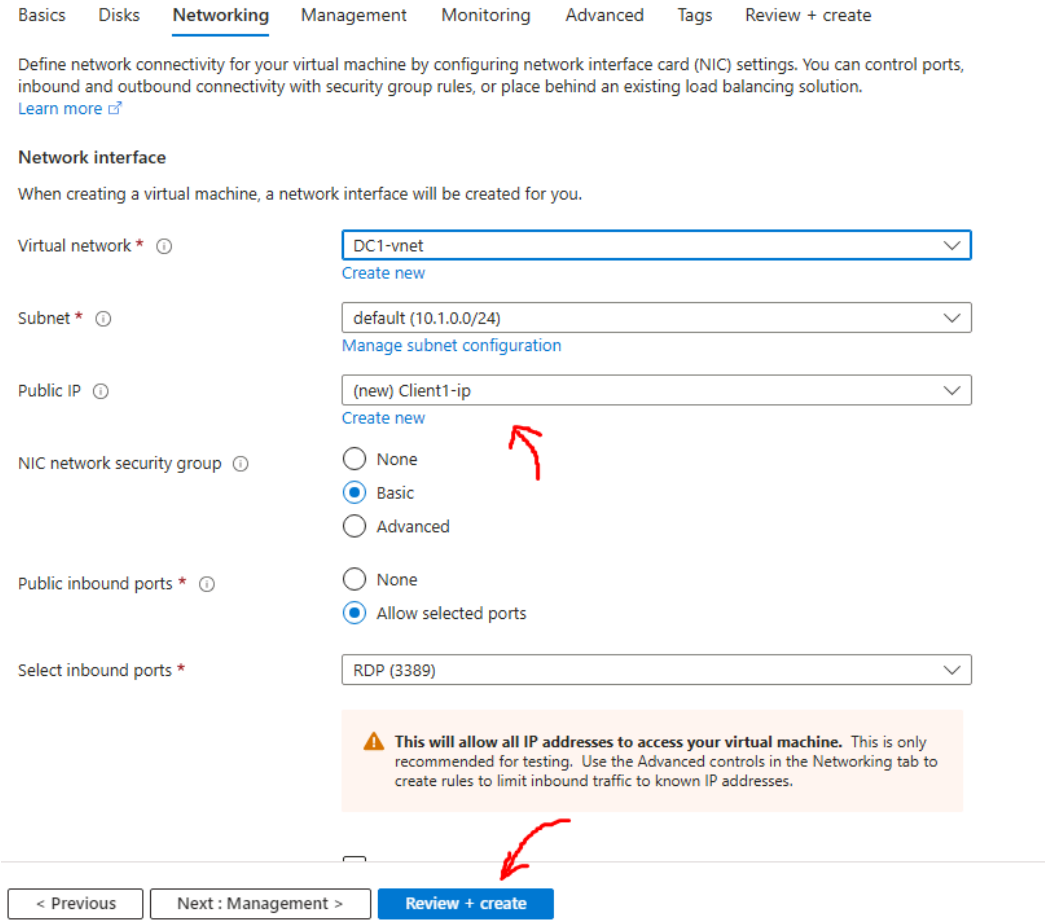
- We want to make sure it's in the same Virtual Network so click on the dropdown and make sure the DC1-vnet is selected
- The public IP may not be shown. If not, we'll make a new one called Client1-ip



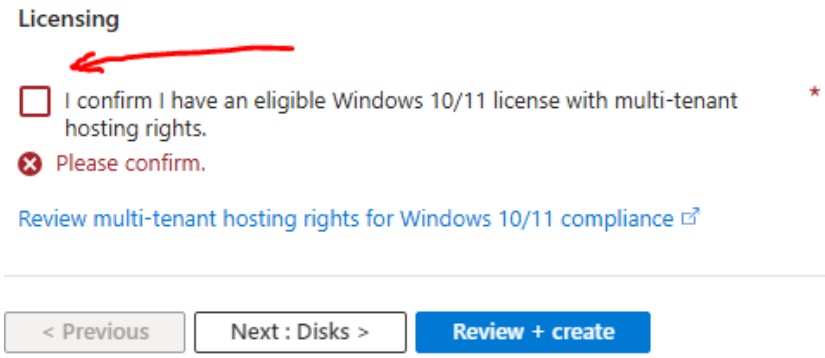
- This should be what is shown by default. If not, just type what is shown and press OK

- Very important, ignore the:
  "Activate Windows logo" 😉

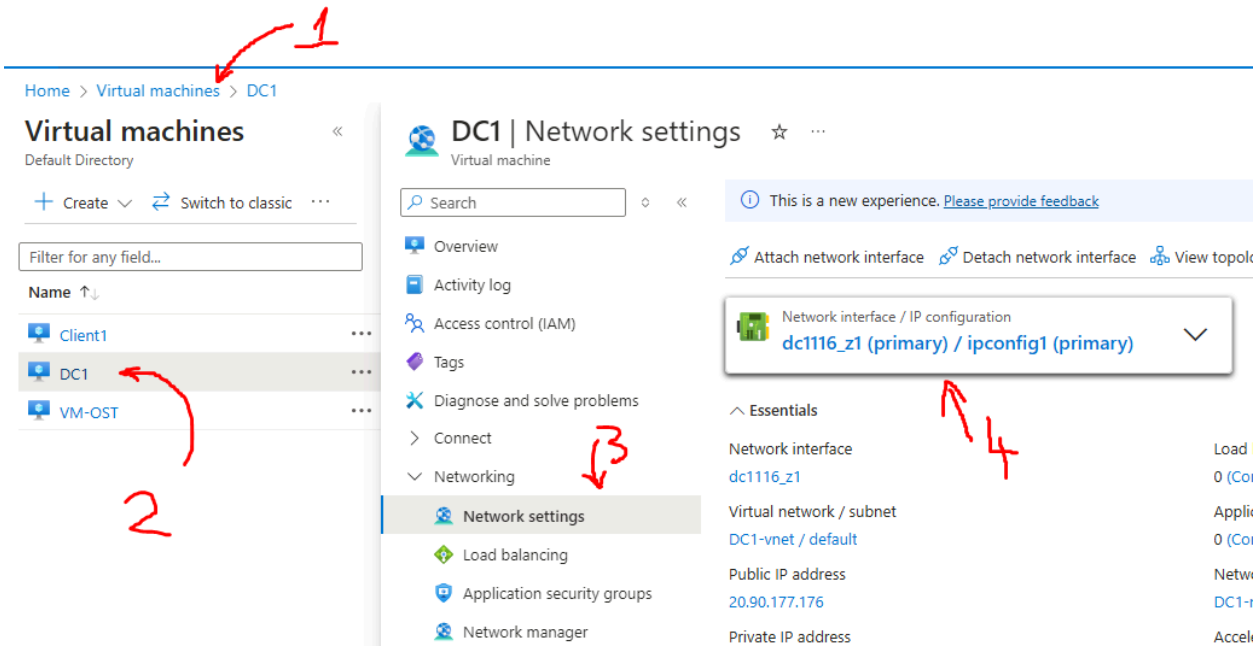




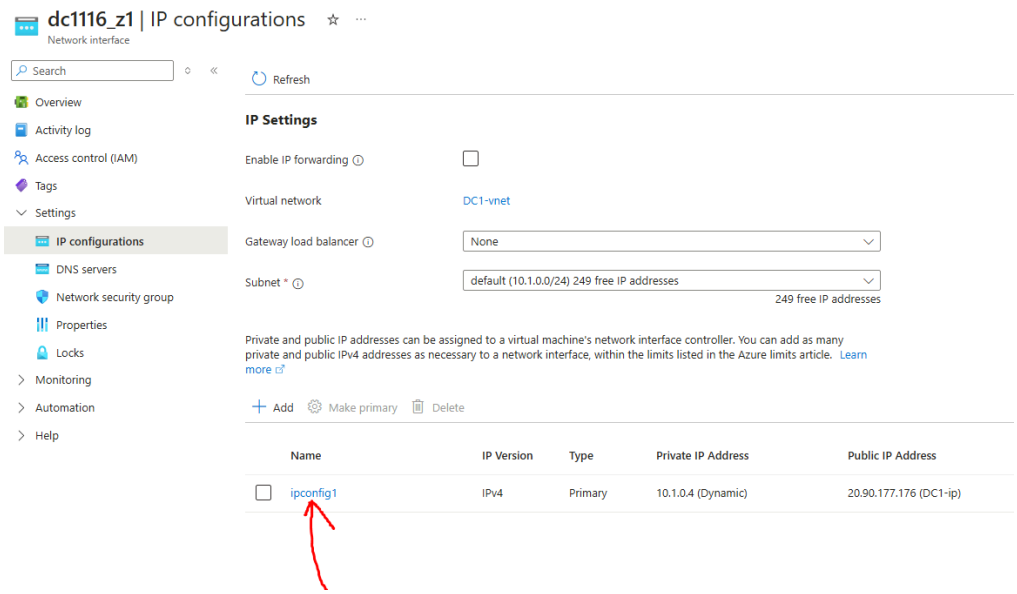
- The Public IP should now be set.
- Click on Review + Create



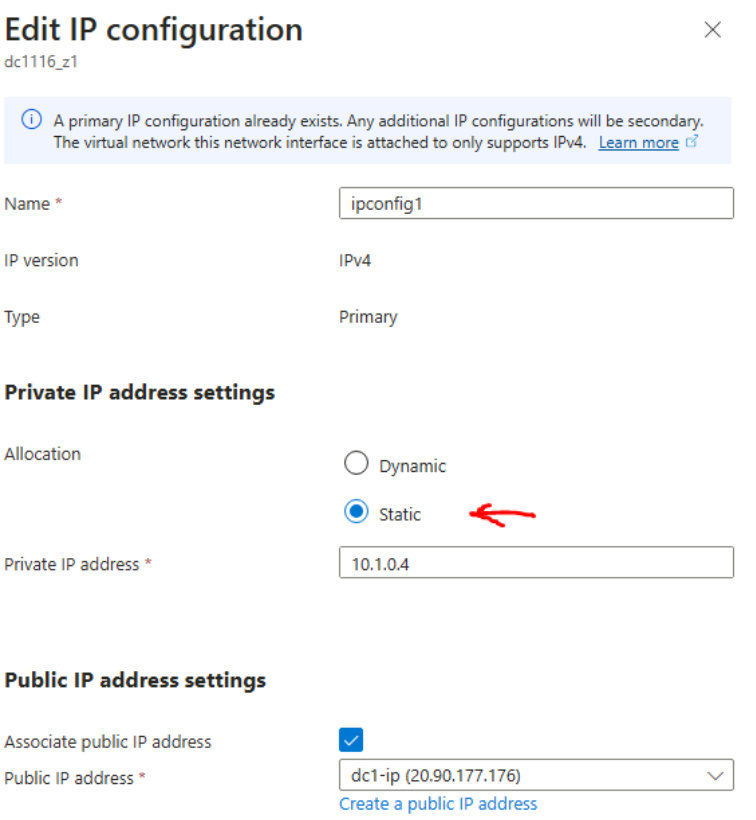
- If you get this error, just tick this. Then Review + Create



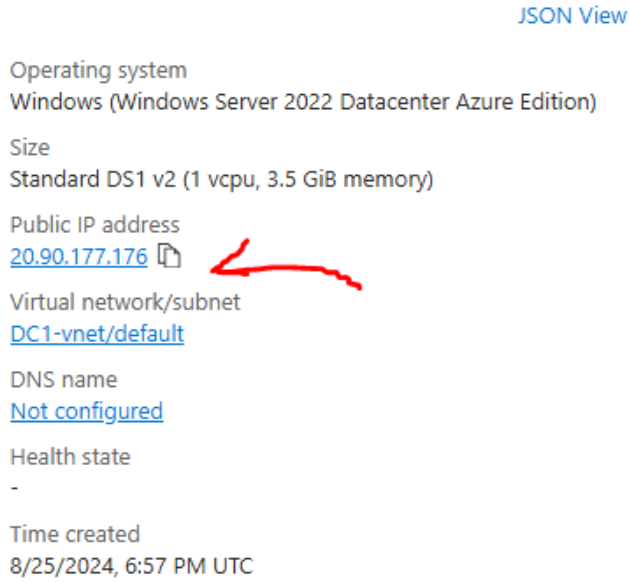
- Next we just want to make sure out DC Server has a static IP address - this way it won't continually change
- 1. Go to your Virtual Machines
- 2. Select DC1
- 3. Go to Networking > Network Settings
- 4. Select Network Interface



- Select "ipconfig1"



- Make sure “Static” is selected
- The private IP address should be given. Mine is 10.1.0.4 but usually it’ll be 10.0.0.4, it’s only because I already have an IP address of 10.0.0.4 running.



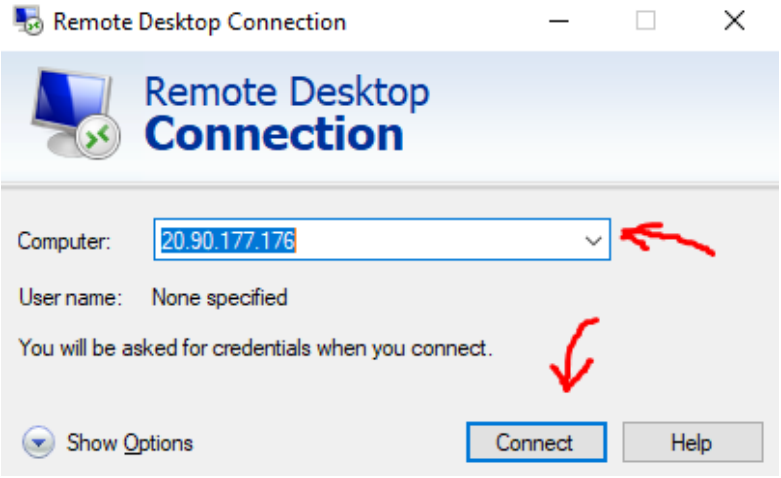
- All you have to do here is copy the Public IP Address given and you’re set to go onto the next stage

3 Setting up Windows Server VM

During this section, I'll be setting up the Active Directory within our Windows Server VM. This will include a number of steps:

- Configuring the Firewall
- Adding Roles and Features
- Creating a Domain Controller
- Creating Organisational Units
- Logging in as an Admin

Before we start, let's remote into our Windows Server Virtual Machine.

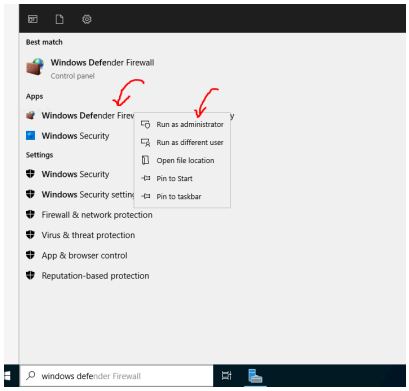


- Paste the IP we copied from earlier
- Connect

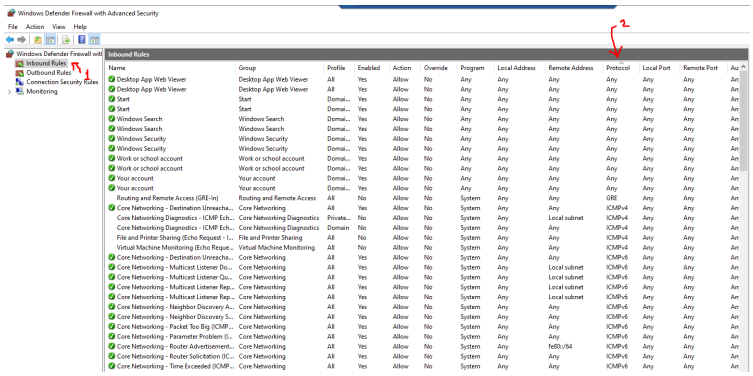
- Use the credentials you made during the setup for Windows Server
- Click OK then on the next pop-up, click Yes

3.1 Configuring Firewall

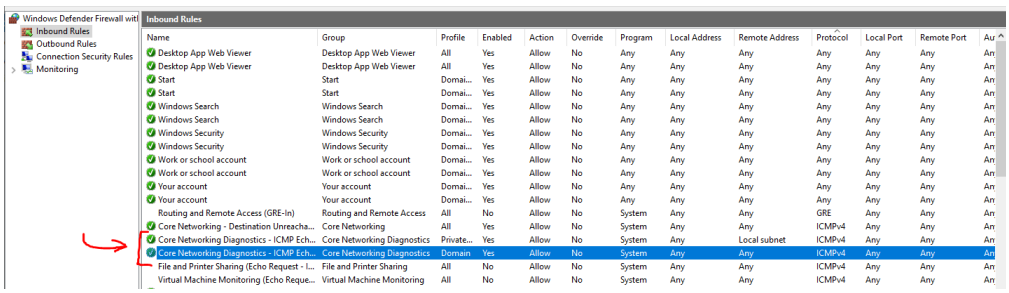
Something that we must do is enable ICMP Echo Request. Enabling ICMP allows you to use ping on the Command Line to check if your server is reachable from other devices on the network - this is important for Active Directories. This can help diagnose connectivity issues or verify that network routes are correctly configured.



- Search for Windows Defender Firewall
- Run as Administrator



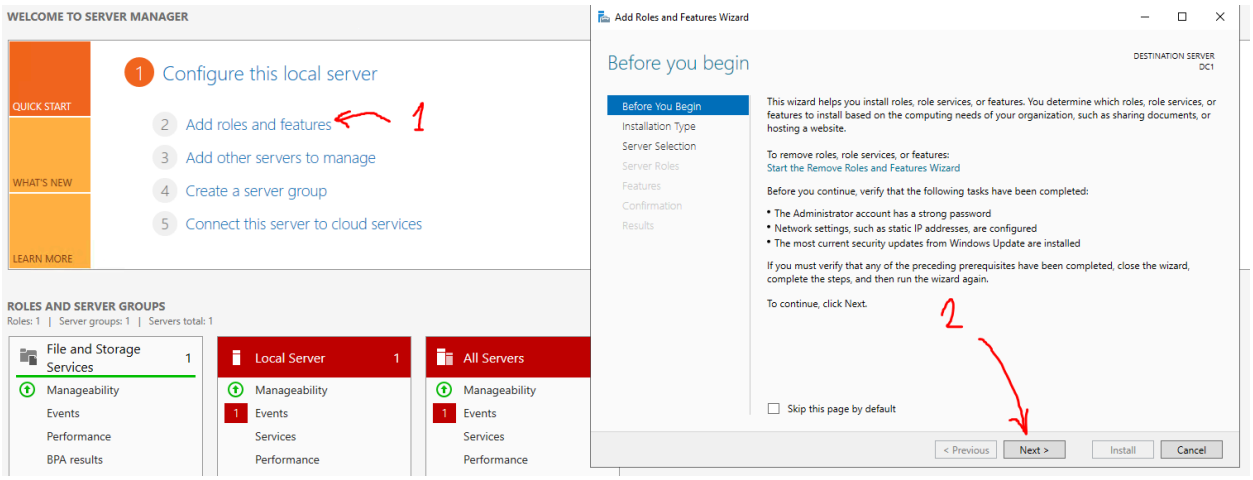
- Select Inbound Rules
- Select Protocol to order Any to the top



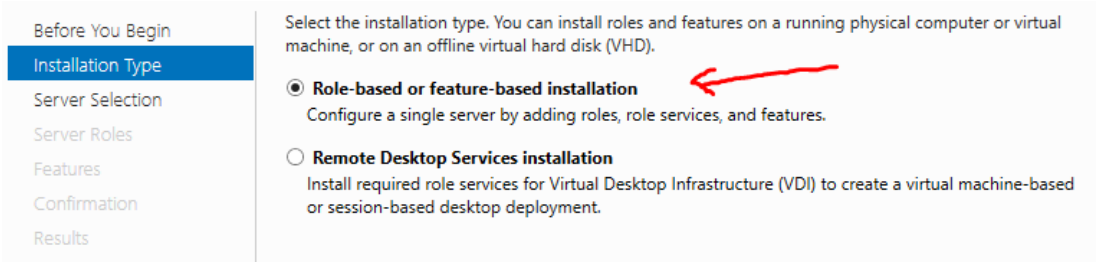
- Enable Core Networking Diagnostics - ICMP. Both the “Private” and “Domain” profiles.

3.2 Setting up Active Directory

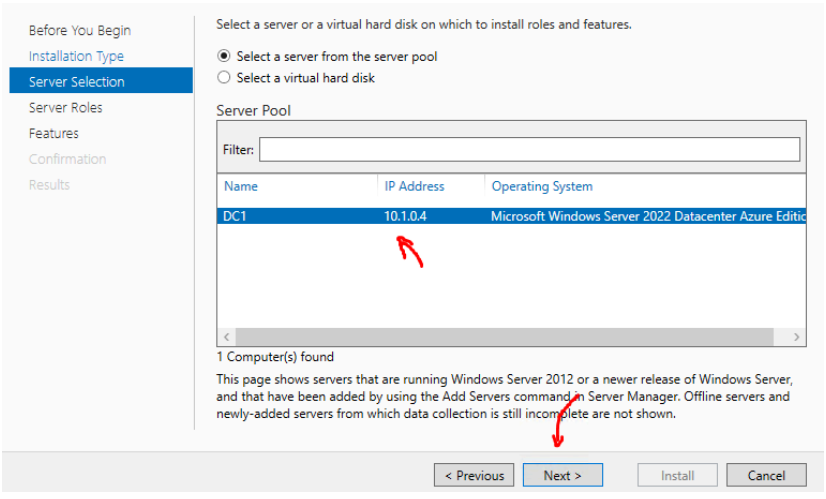
Setting up an Active Directory Domain Services will have us select the “Add Roles and Features” then eventually selecting the Active Directory Domain Services from there. The steps of this will be shown below.



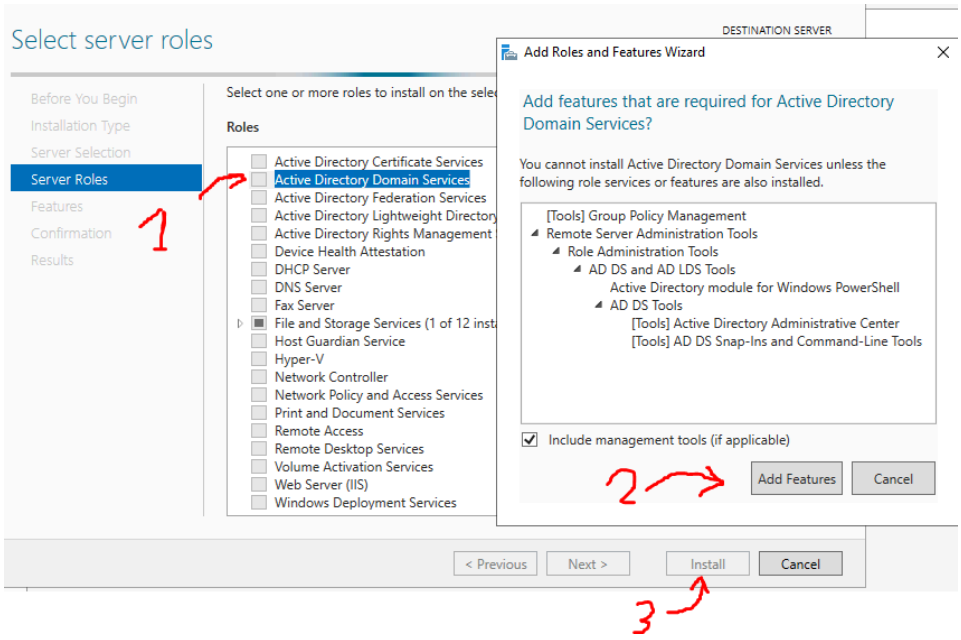
- 1. Select Add roles and Features
- 2. Select Next on the pop-up



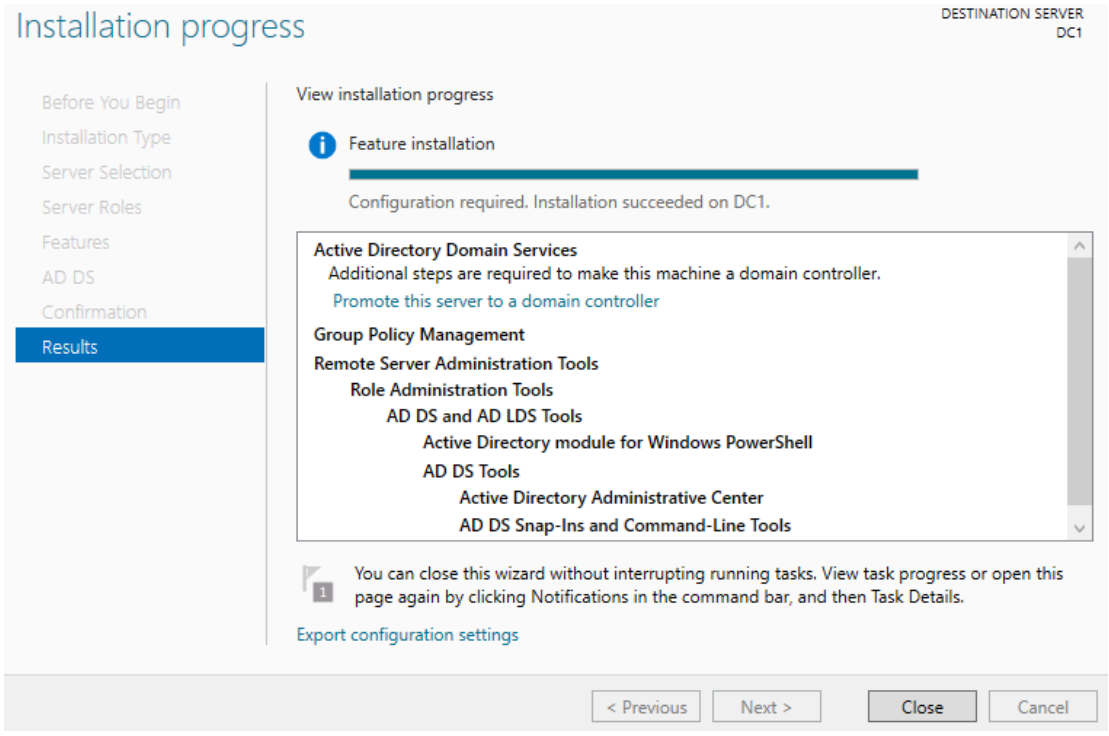
- Select Role-based and click next



- Select the server and click Next



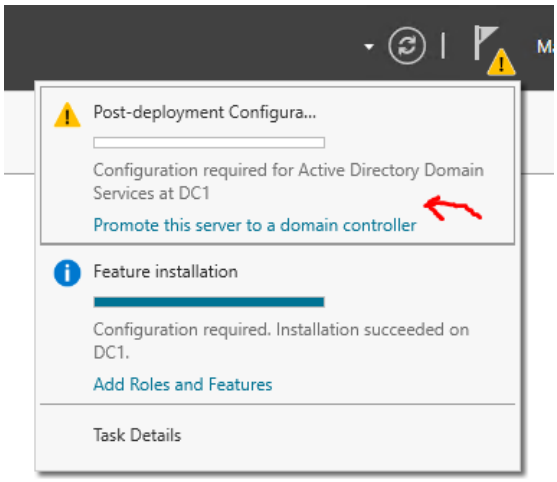
- Select Active Directory Domain Services
- Select Add Features
- Press Next and continue pressing next until you install



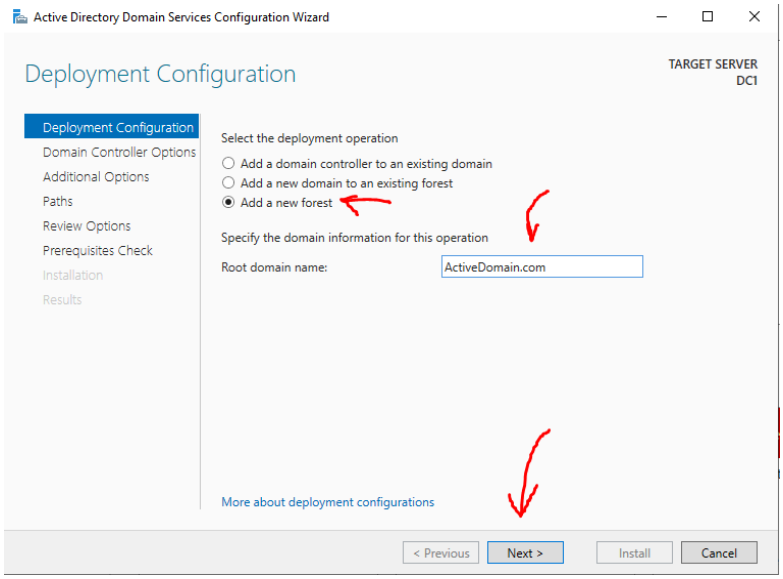
3.3 Creating Domain Controller

A Domain Controller is a server in a network that manages user logins and access to resources like files and applications. It acts as the "gatekeeper," ensuring that only authorised users can access certain parts of the network. It also stores and organises important information about users and devices, making it easier to manage and secure the network.

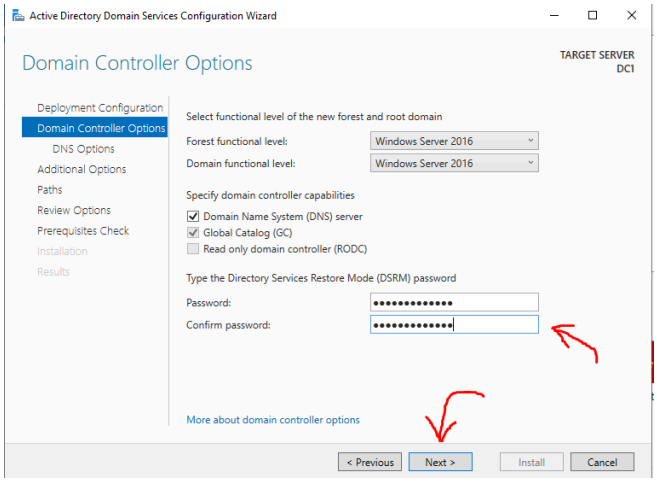
Here we'll be able to promote our server into a domain controller.



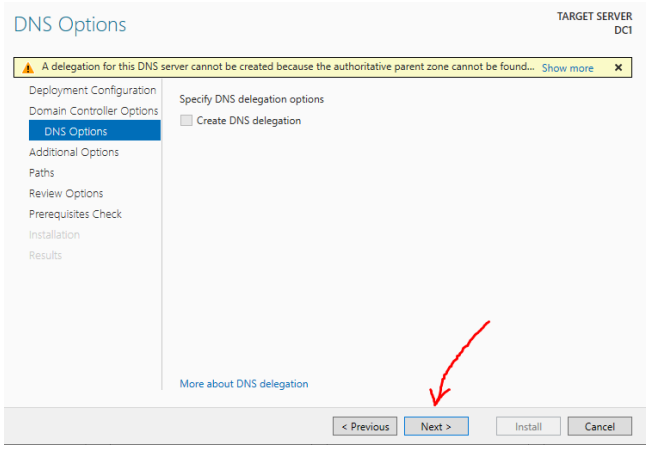
- Click on the arrow on the right
- Select "Promote this server to a domain controller"



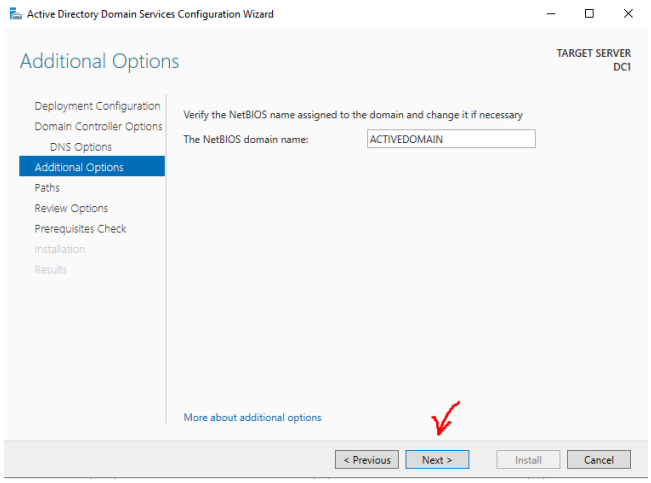
- Select "Add a new forest"
- Root Domain Name: "ActiveDomain.com"
- Click Next



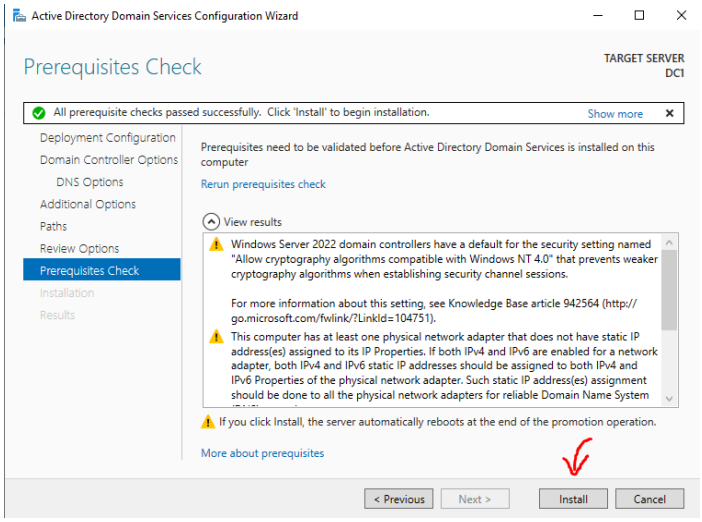
- Set up a password
- Select Next



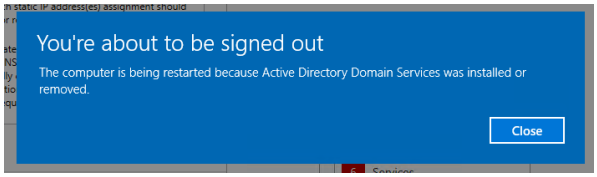
- Next



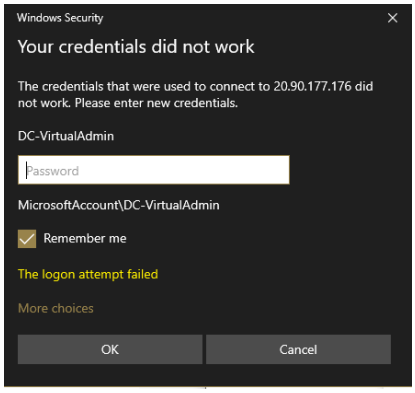
- Wait for awhile
- Then when ready, press Next
- Continue to go next until Prerequisites Check

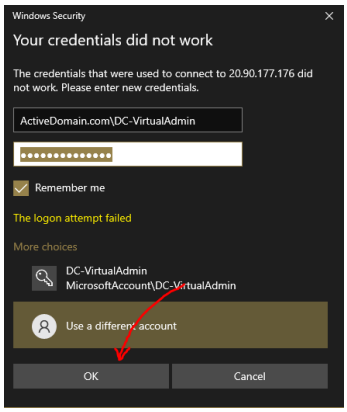


- Install



- The remote access will then reset as the Windows Server VM will restart



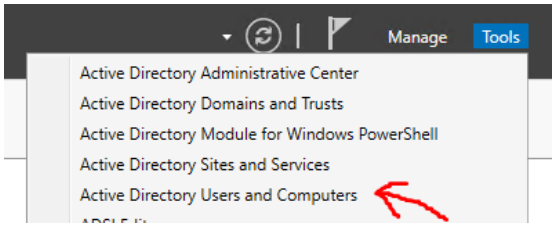


- What should happen here is that you'll be unable to log in. That's because we've set up an Active Domain. So we'll need to log into our active domain.
- Setup the new credentials. It'll be your domainName.com\yourAdminName

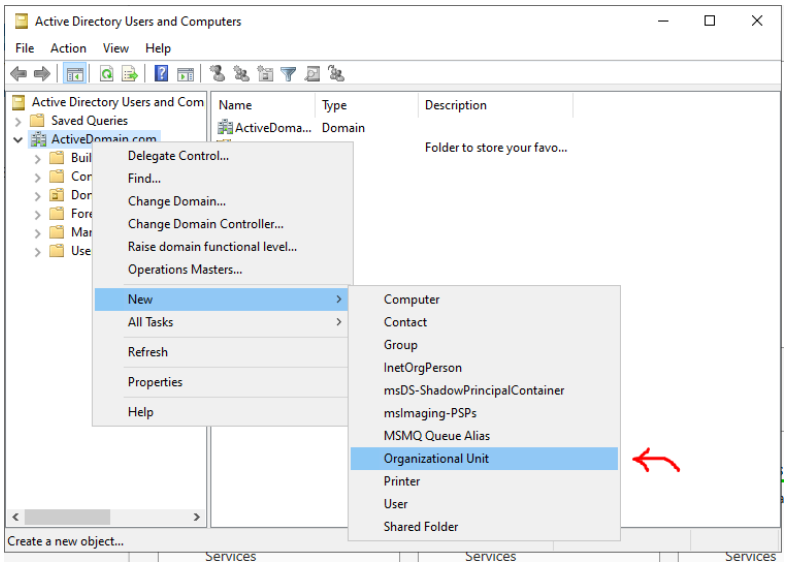
- Wait for this to complete, after this we'll be taken back to our Active Directory

3.4 Creating Organisational Units

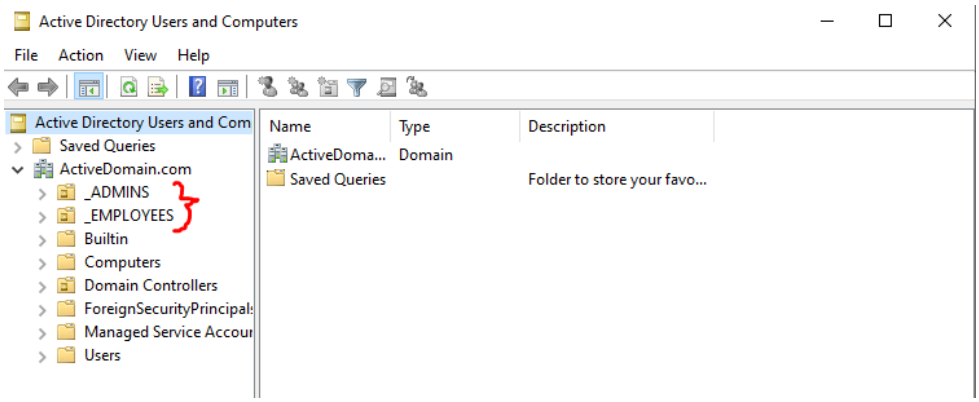
Now we're going to setup some Organisational Units. Think of these as folders for our users. This will allow us to manage our users easier.



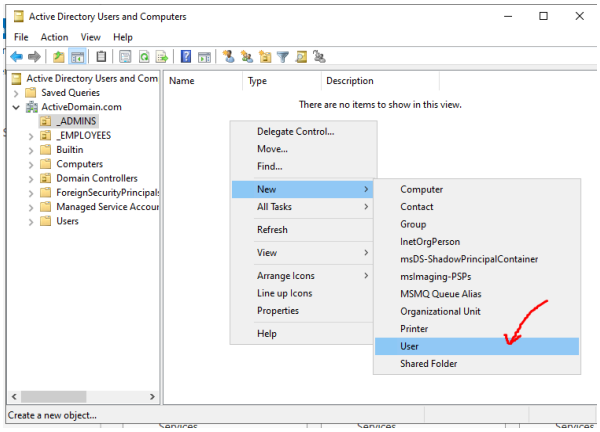
- Select Tools
- Active Directory Users and Computers



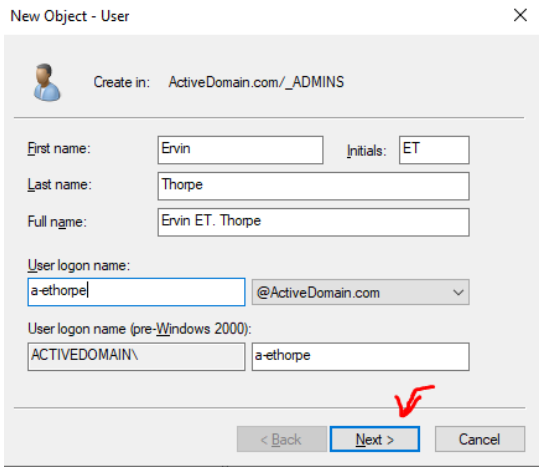
- We'll now create an organisational unit
- GO to ActiveDomain.com > Right click > New > Organisational Unit



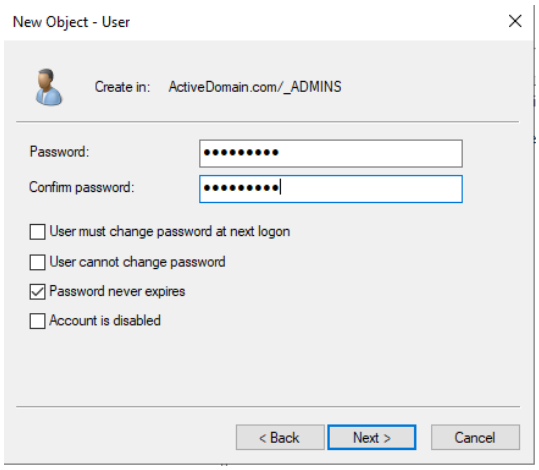
- We've now setup _ADMINS and _EMPLOYEES as two new organisational units



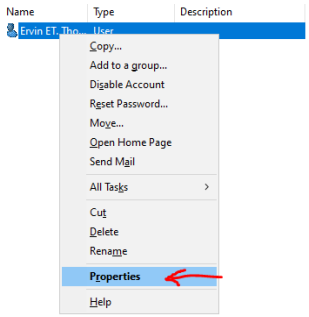
- We'll now set up a new admin user
- Right click > New > User



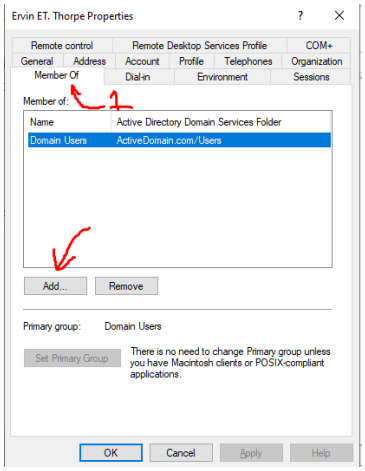
- Set up a new user. I like to use a-FirstLetterLastName. A = Admin



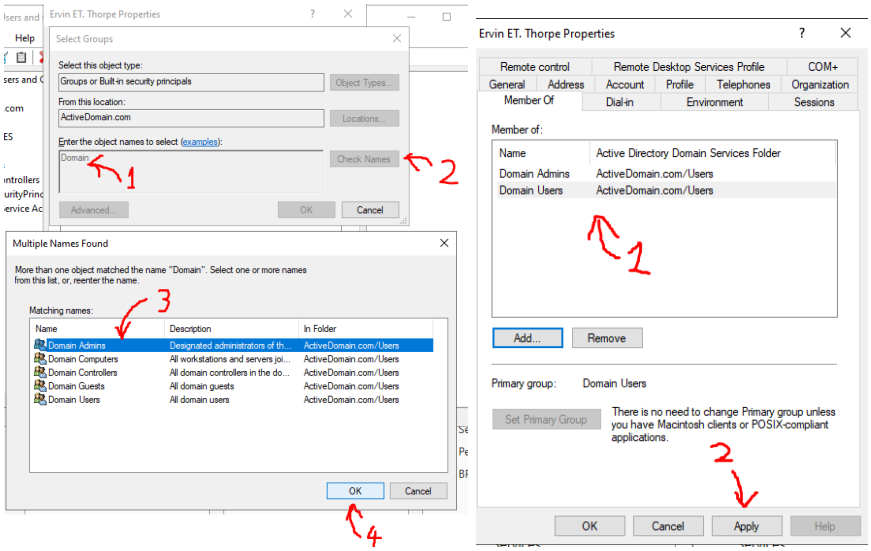
- Setup a password
- then go next
- Tick "Password never expires"



- We'll now setup a domain for this account
- Right click the account > Properties



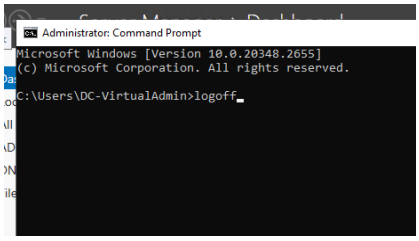
- Go to Member Of
- Then click Add…



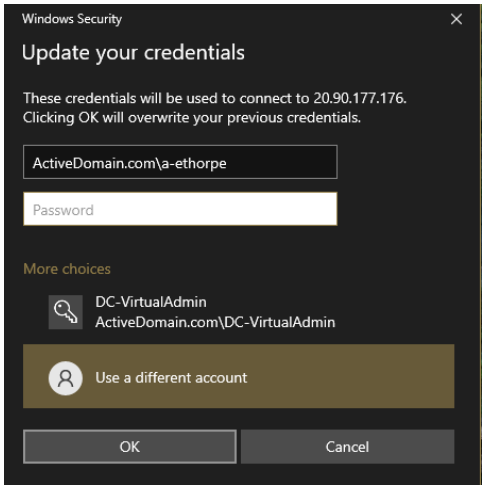
- Type in "Domain"
- Click Check Names
- Look for "Domain Admin"
- Click OK then click OK again
- You will then see that Domain Admin has been added. New user is now a domain admin.

3.5 Logging in as Admin

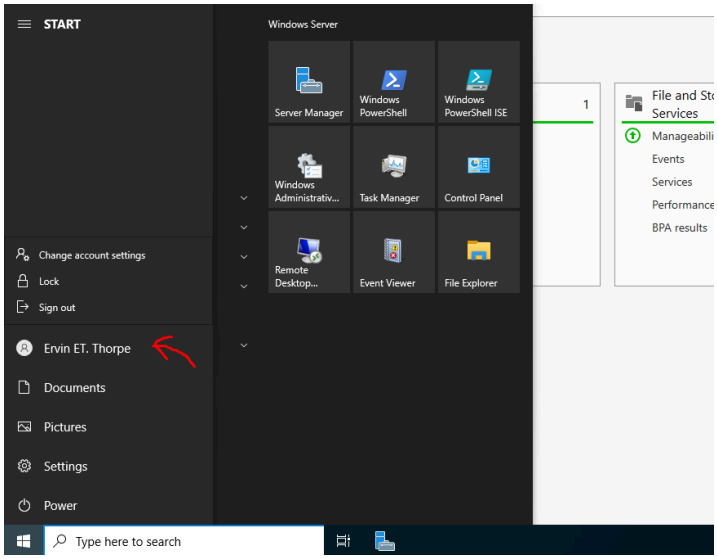
For this section, we're going to test to see if we can log in as our new admin account.



First we'll just log off. We can do this from the command prompt.



- Now we'll want to log in as our admin account. This is done by domainName\adminName

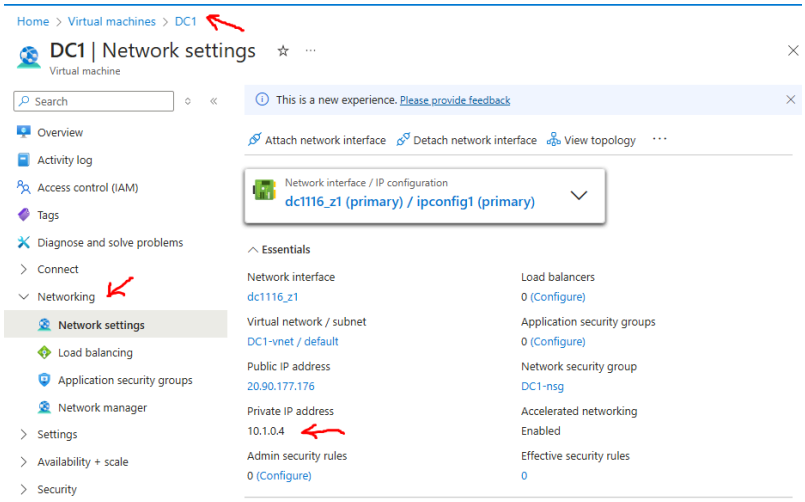


- We're now logged in as our admin account!

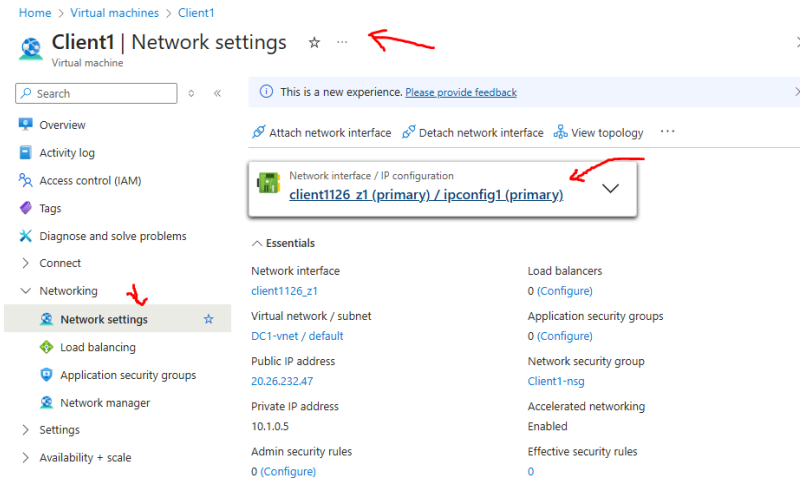
4 Setting up Client VM

For this section, I'll be setting up the Client Virtual Machine. Configuring and testing the DNS of this machine and having this client connect to the active directory virtual machine. In order for this Client's machine to connect to the domain controller, we'll have to have them be the same DNS.

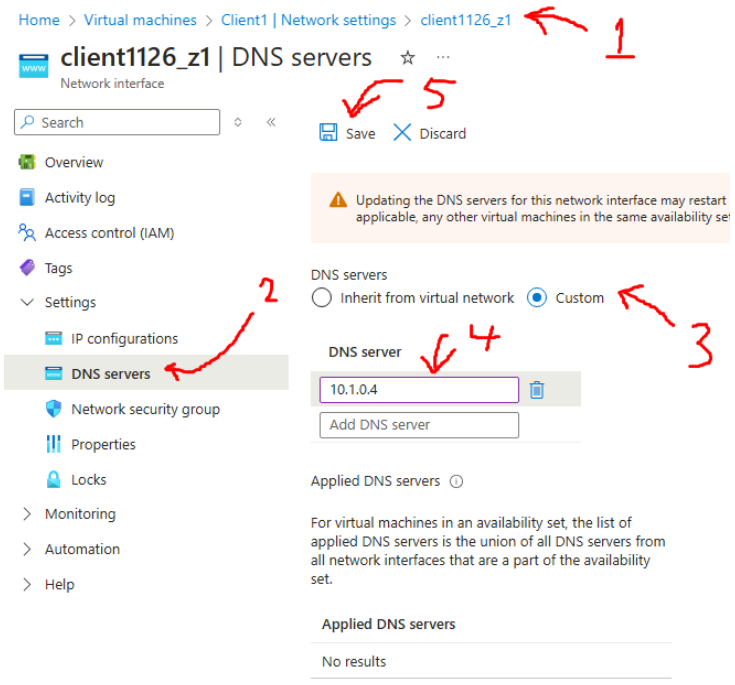
4.1 Matching the DNS server



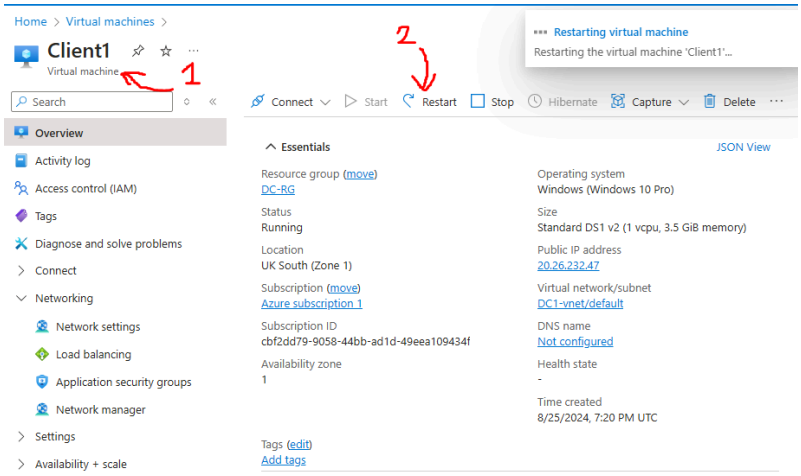
- Go to DC VM
- Go to Networking > Network settings > Copy Private IP Address



- Go to Client1 VM
- Go to Networking > Network settings > Select the Network Interface



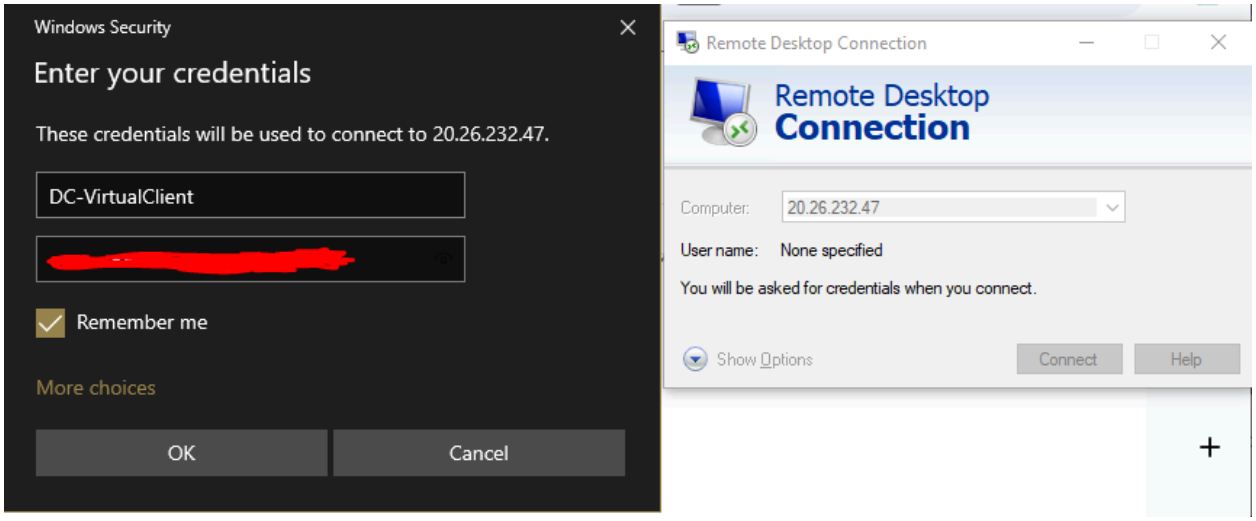
- A number of steps here..
- 1. Make sure you're on the Network Interface
- 2. Go to DNS Servers
- 3. Select Custom
- 4. Type in or paste the private IP address we copied earlier for the DNS server
- 5. Save



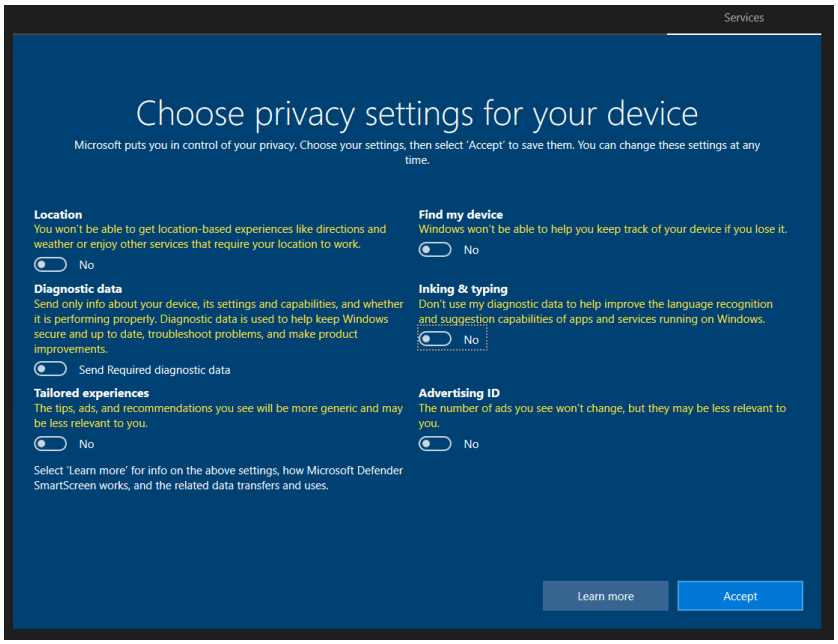
- Now go back to our Client1 VM
- Restart it. This is because we set up a new DNS server. We'll want to restart it to deploy the new changes.

4.2 Observing the DNS changes

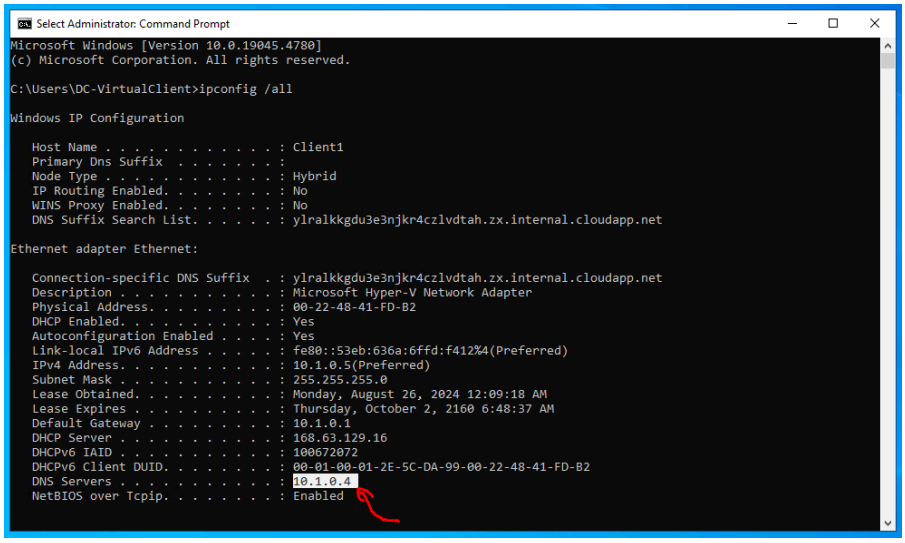
To observe to see if these DNS changes worked, we'll have to now remote access our client VM.



- Type in the client machine username and password
- Click OK



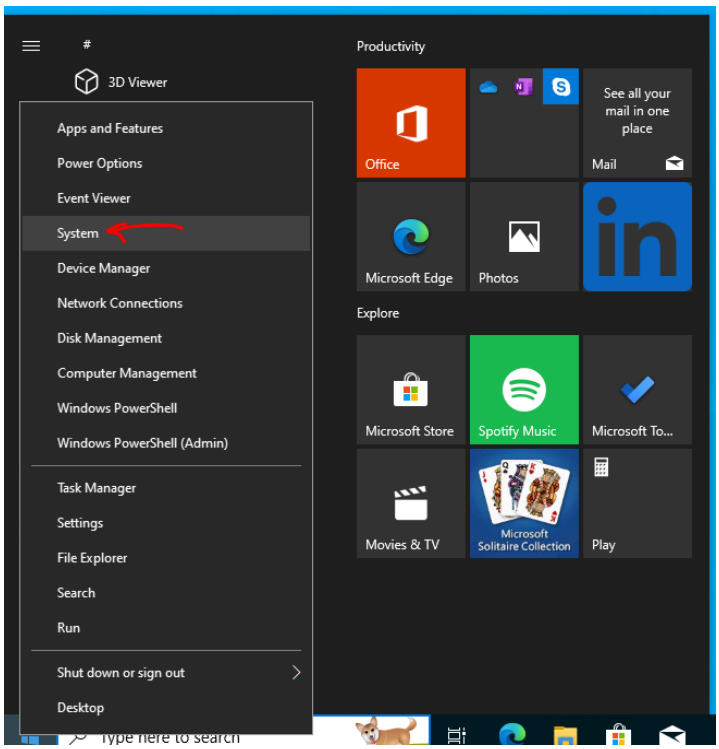
- Select No to all and accept. We don't want to overload our VM when we already have low resources.



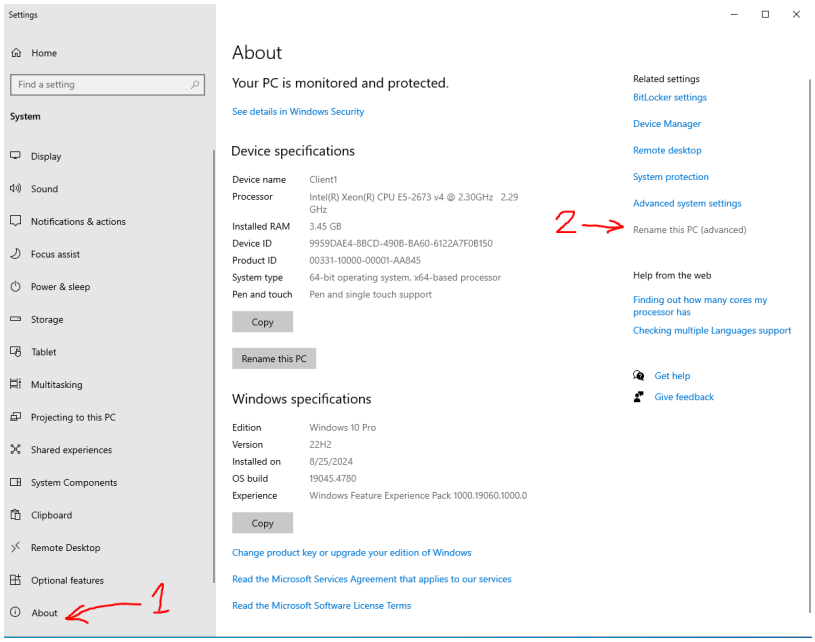
- Open Command Line as Administrator
- Type in “ipconfig /all”
- From here, we can see that the DNS servers have been set the way we intended.

4.3 Having a Client connect to the Active Directory VM

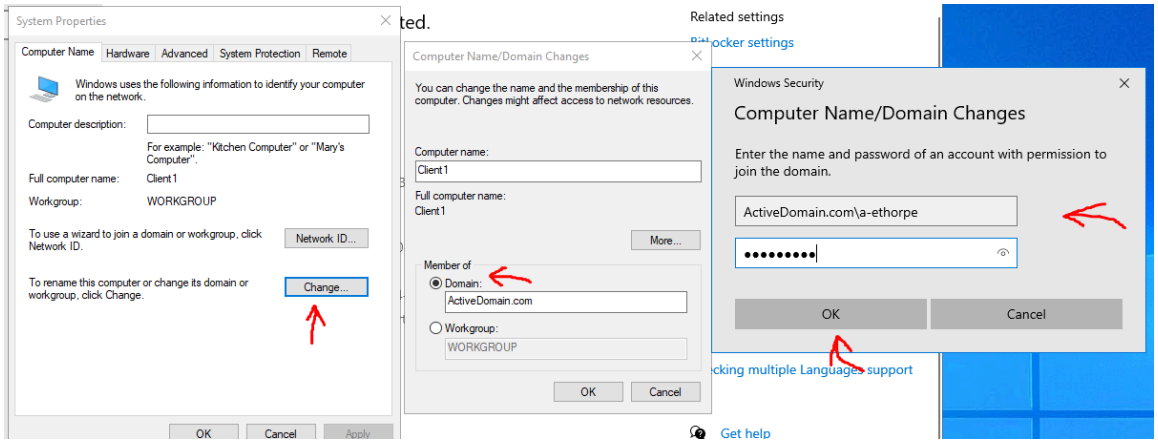
Now we’re going to try to connect the client VM to the Active Directory VM



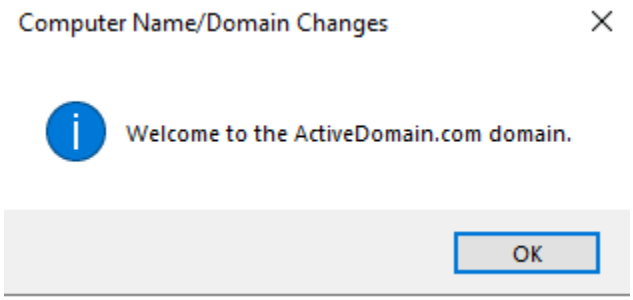
- Right click the Start button > Select System



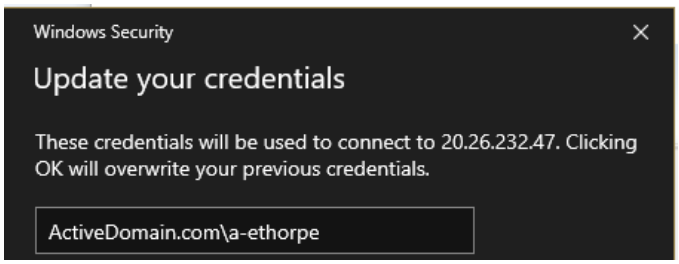
- Select About
- Then Select “Rename this PC (preferred)”



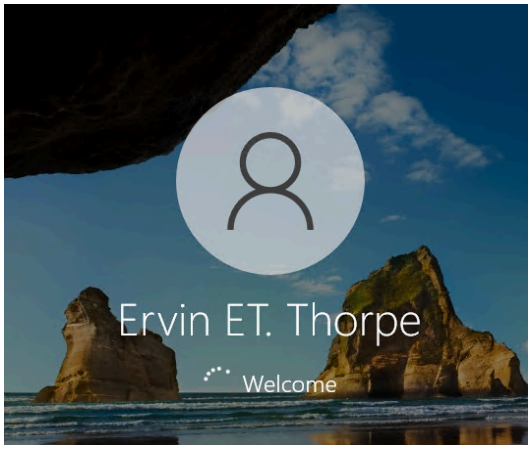
- Select Change
- Select “Domain”, type in the domain, press OK
- Then type in the credentials of one of the accounts. I’ll use the admin account.



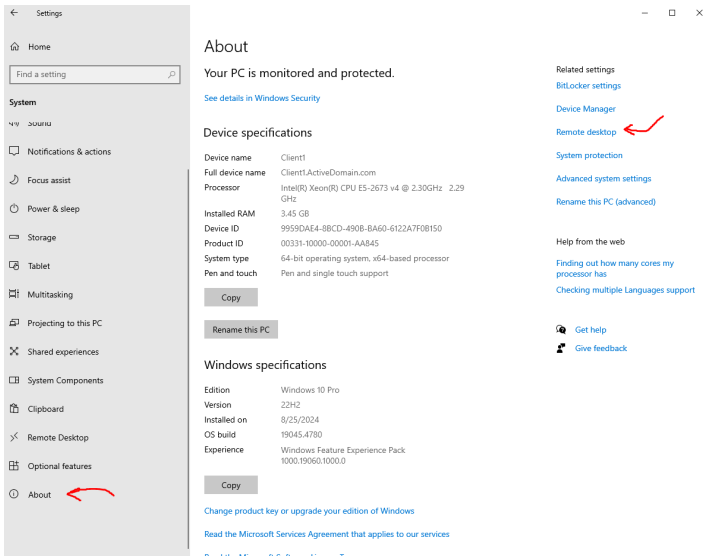
- If done correctly, you’ll get this



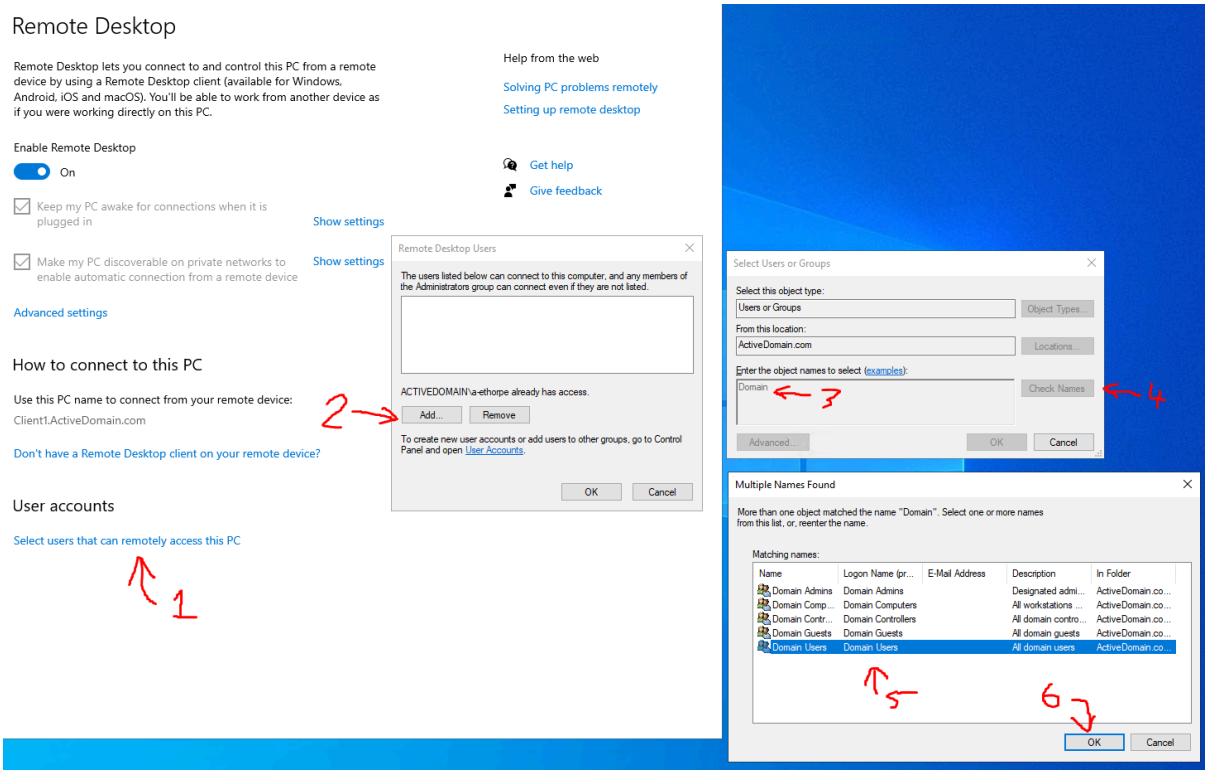
- Now we'll try to access the Active Domain with our admin account that exists in the active directory for the Client1 machine



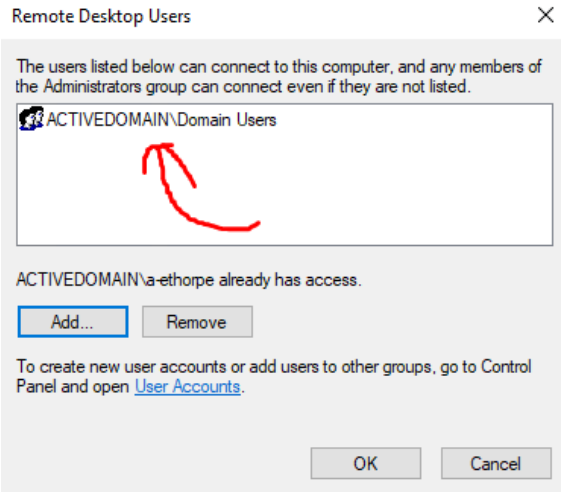
- Now we're logging in as our admin account



- Now we're going to have any user within our Active Directory be able to connect to this client1 machine.
- Go to About > Remote Desktop



- Go to “Select users that can remotely access this PC”
- Then select “Add…”
- Then type “Domain”
- Go to “Check Names”
- Then select “Domain Users” - that will be all users, including admin
- Click OK



- As we can see, our Domain Users has been added.
- The benefits of this is that it allows any user to access this machine. This has plenty of benefits and I plan on building onto this in the distant future to showcase how it can help in a real world case.

5 Conclusion

In this project, I successfully deployed an on-premises Active Directory environment using Microsoft Azure Virtual Machines. The key accomplishments include:

1. Setting up Azure Virtual Networks and creating two Virtual Machines: a Windows Server 2022 for the Domain Controller and a Windows 10 client machine.

2. Configuring the Windows Server VM by enabling necessary firewall rules and installing Active Directory Domain Services.

3. Promoting the server to a domain controller and establishing a new forest with a root domain.

4. Creating organisational units and setting up administrative accounts within the Active Directory structure.

5. Configuring the client VM to connect to the domain by adjusting its DNS settings and joining it to the Active Directory domain.

6. Enabling remote desktop access for domain users on the client machine.

This hands-on experience has provided me with valuable insights into cloud-based infrastructure management, Active Directory deployment, and network configuration within the Azure ecosystem.

Moving forward, I plan to build upon this foundation by exploring DNS management. The next section of this project will focus on configuring and managing DNS services using the existing Azure Virtual Machines (Windows Server 2022 and Windows 10), DNS Manager, and Command Prompt. This will allow me to gain a deeper understanding of name resolution, zone management, and the critical role DNS plays in network infrastructure and Active Directory environments.

By continuing to develop these skills, I am enhancing my expertise in enterprise-level identity and access management, as well as some basic network administration in cloud environments.