Kamran Bilgrami Follow
Jan 6, 2020 · 21 min read ★ · Listen

Ethical Hacking Lessons — Building Free Active Directory Lab in Azure

Motivation

The majority of IT experts concur that Active Directory is the dominant approach for managing the Windows domain networks. This is why adversaries get attracted to discover and exploit vulnerabilities within the Active Directory echo system. In order to defend against those types of attacks, there is a need for practice grounds where Pen Testers, Security Researchers and Ethical hackers can practice offensive and defensive methodologies.

therefore, decided to look into building a similar low-cost lab (free in this case) in Azure while following his videos. This article basically follows steps from How to Build an Active Directory Hacking Lab video but in a Windows Azure environment.

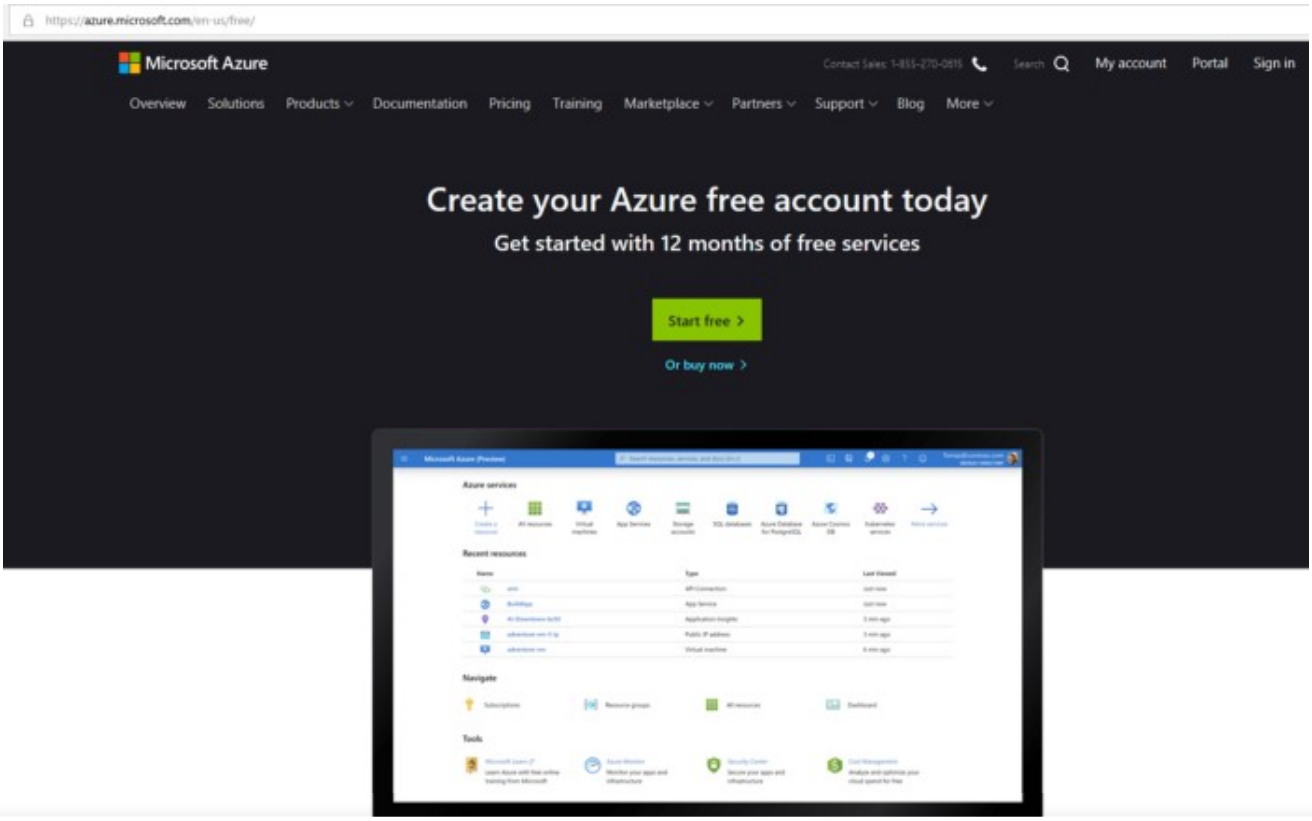
First Things First

It is important to note that some of the practices used during the creation of this lab are intentionally weak to better just to describe the possible attack vectors. You should do the necessary research before using any practices described here into your production or any other network(s).

Microsoft Azure

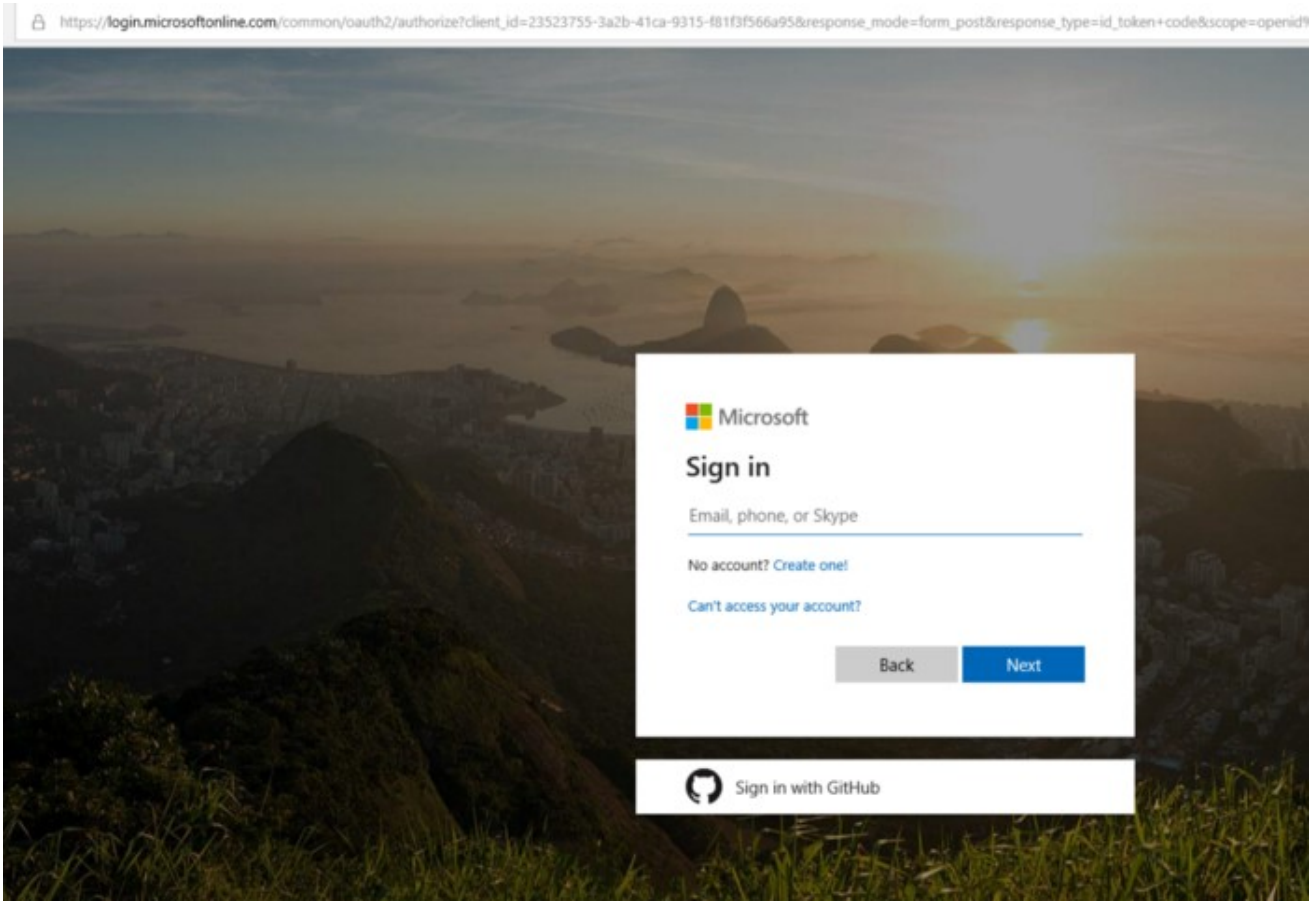
Its highly unlikely that you have not heard about the Microsoft Cloud platform — Azure. This article by no means is an intro to Azure. There are plenty of resources available if you want to learn it.

Microsoft offers a free Azure trial that includes free access to popular Azure products for 12 months, $200 credit to spend for the first 30 days of sign up, and access to more than 25 products that are always free.

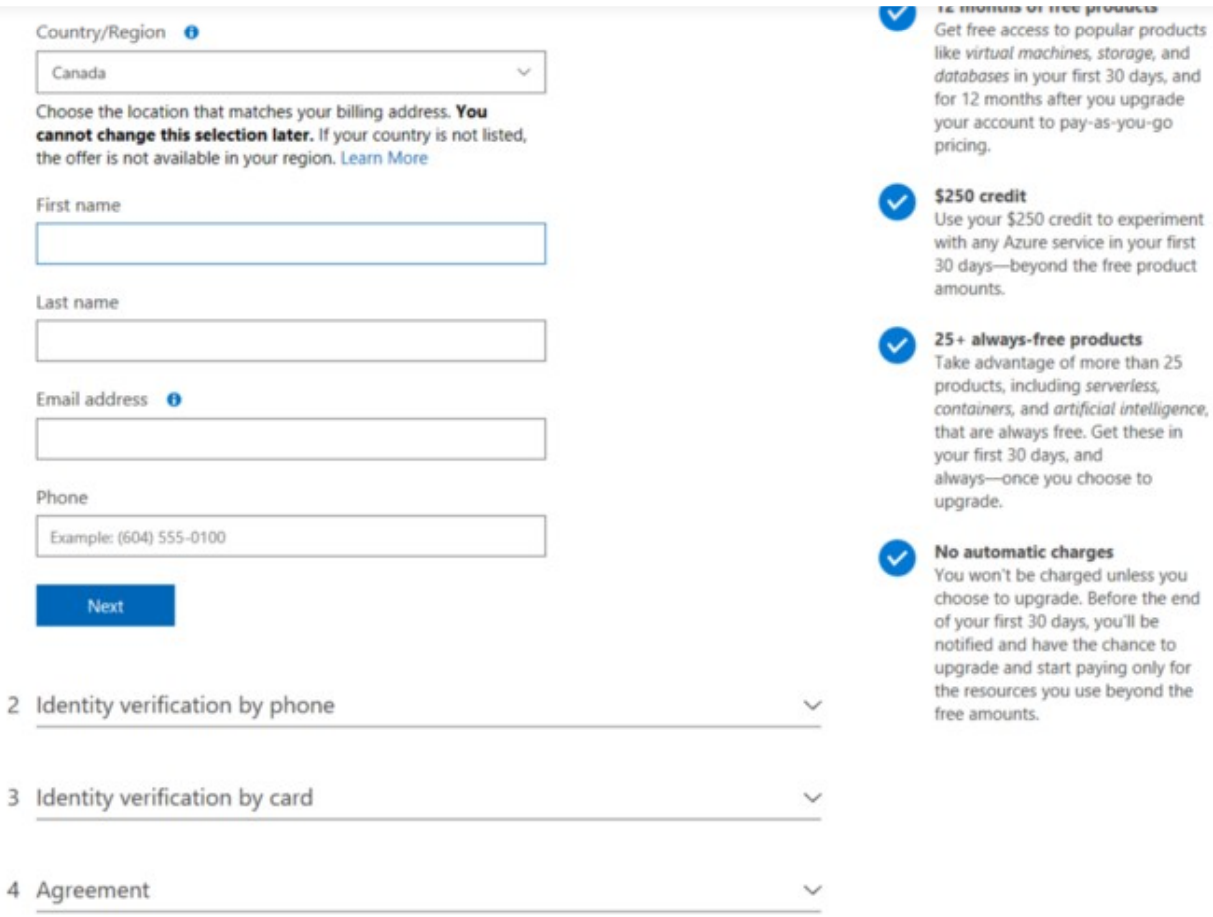


Account Creation

Let's click on the **Start Free** button. If you have an existing Microsoft account, you can log in through the page shown below.

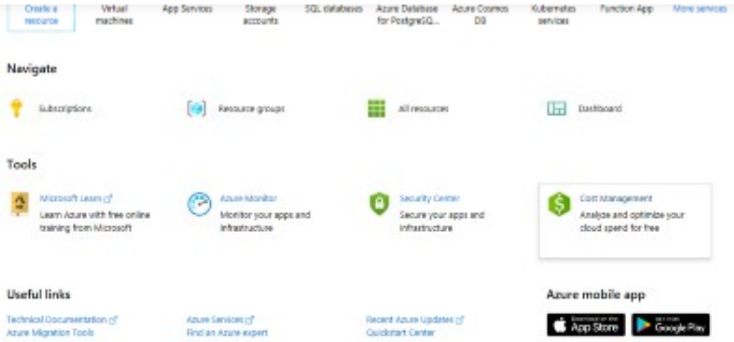


Otherwise, you will have to signup for an account.



Note that the signup process requires to provide user's phone number and credit card information. The credit card is not charged unless the user decides to upgrade to a service such as Pay-As-You-Go. I found the FAQ for the free Azure services quite informative and useful.

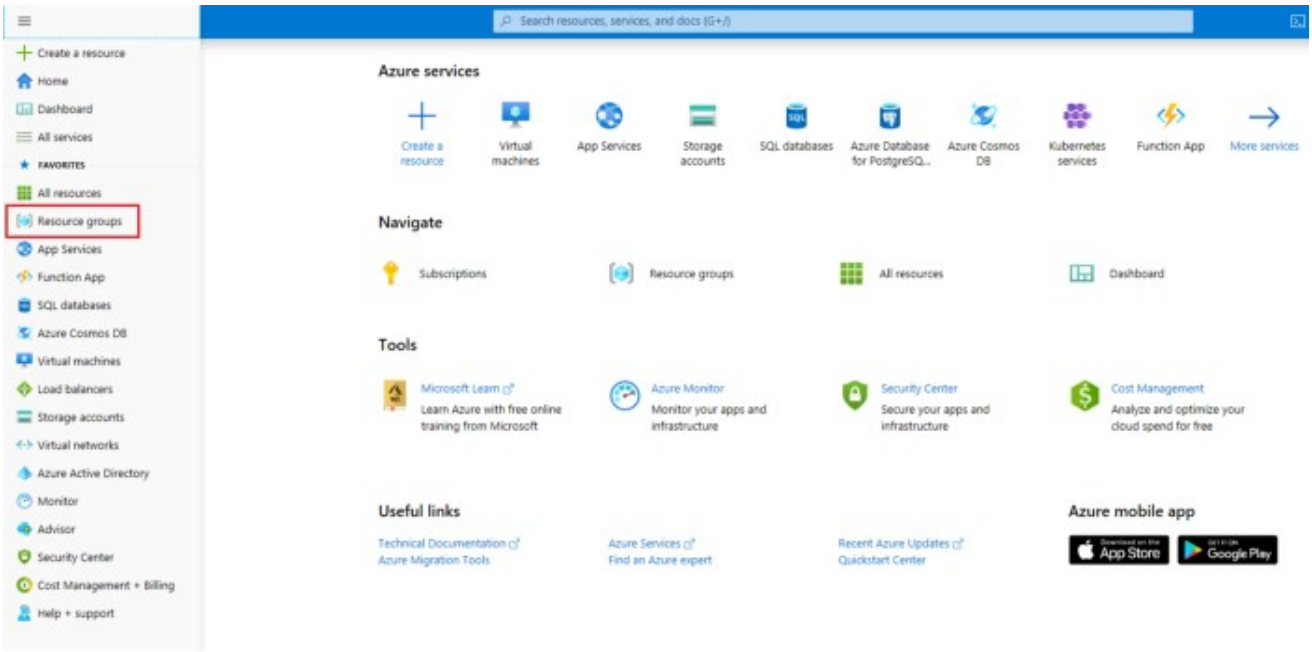
Let's assume that we have signed up for the free Azure service. Let's proceed with the Active Directory lab setup. In your favorite browser, go to Azure portal and login to your account.



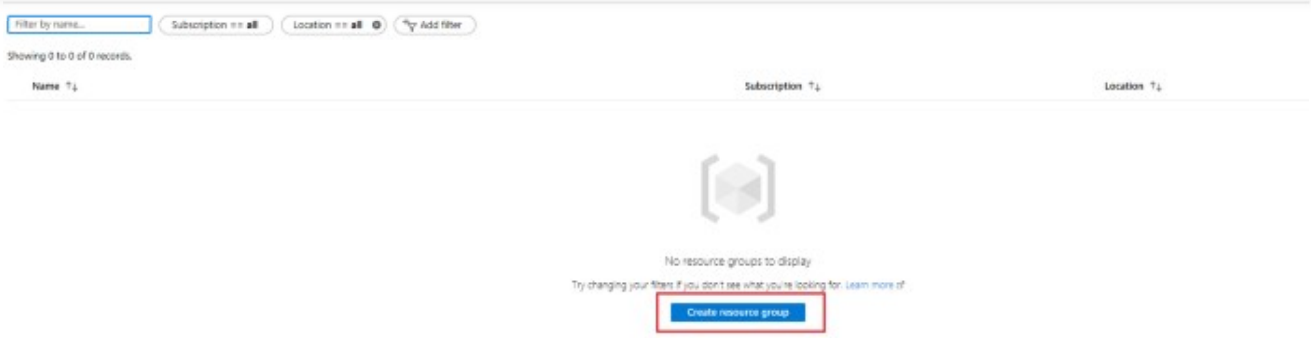
Resource Group Creation

Let's start by creating a dedicated Resource Group for all the lab related resources. A Resource group acts as a container to hold all the related resources for an Azure solution.

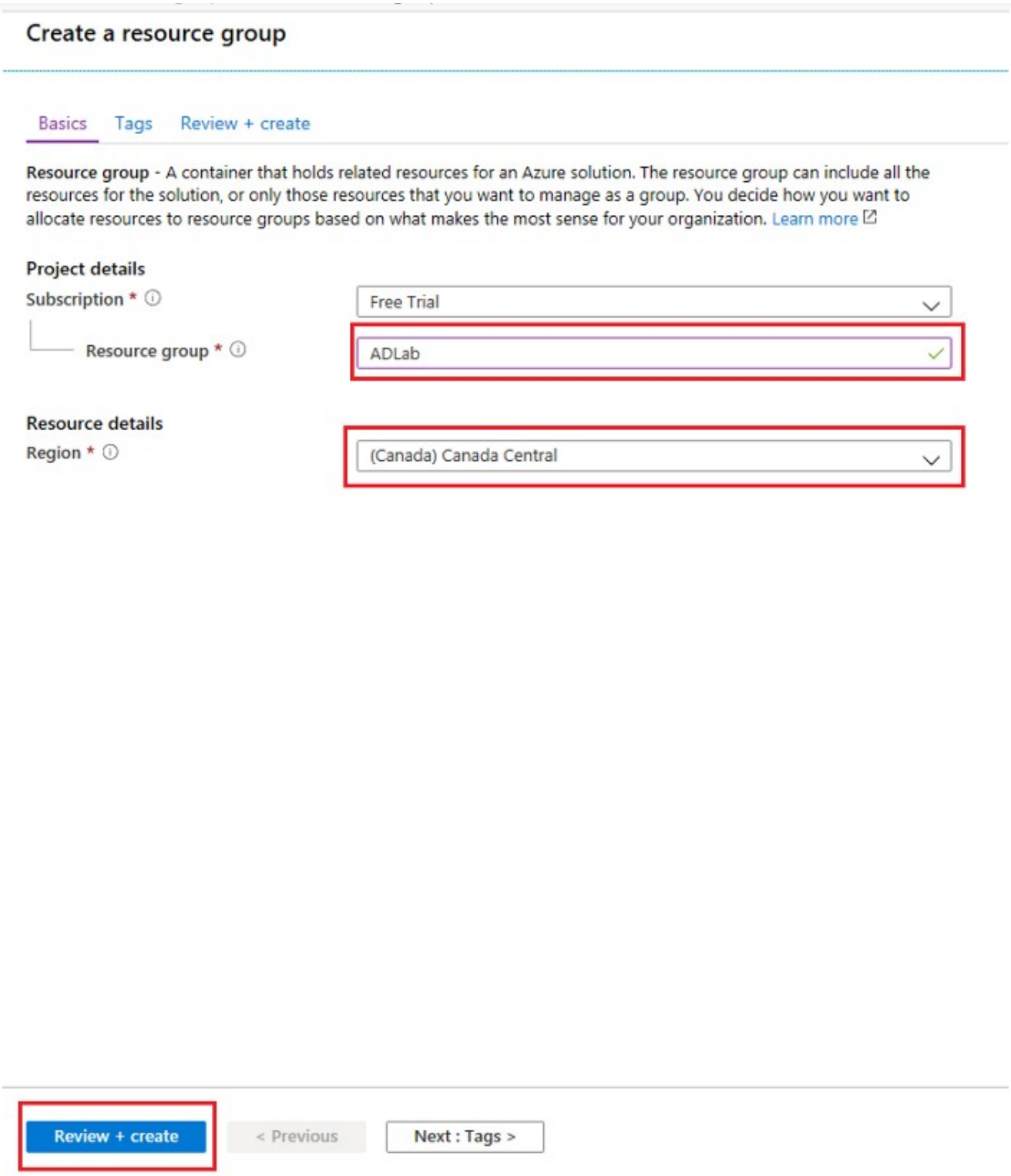
Click on Resource Groups under the Left navigation menu as shown below.



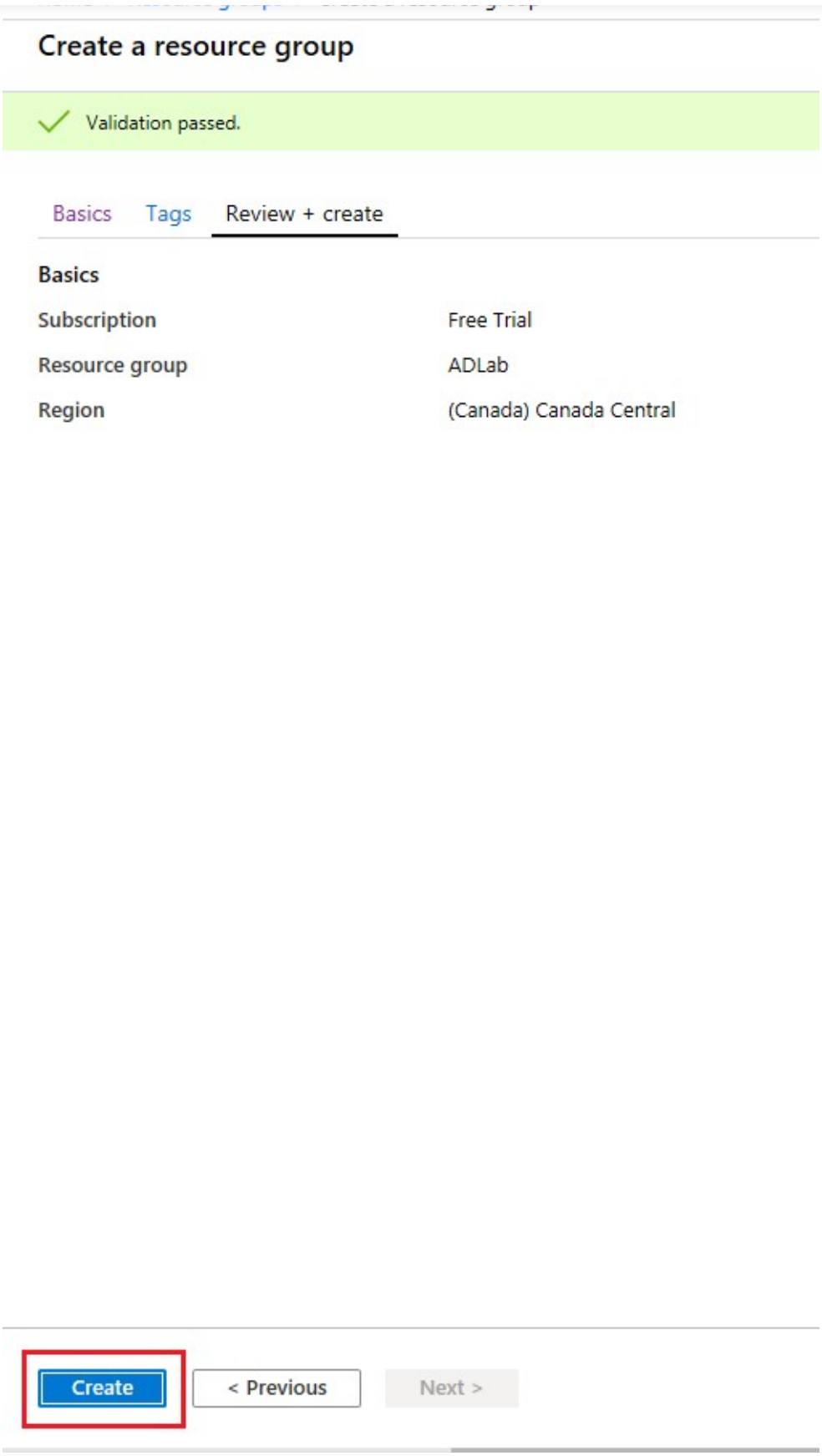
The resource group list is empty. Let's click on the **Create resource group** button as shown below.



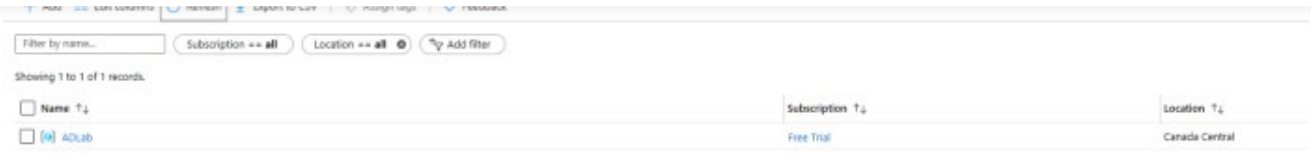
You will be presented with a form like the following. Let's name this Resource group as **ADLab**. I chose **Canada Central** as the Region. You can choose whatever region that makes sense for your geography. Then click on the **Review + create** button.



Necessary validation will be performed and its result will be shown. Its a success in our case. Click on the **Create** button to complete the resource group creation process.

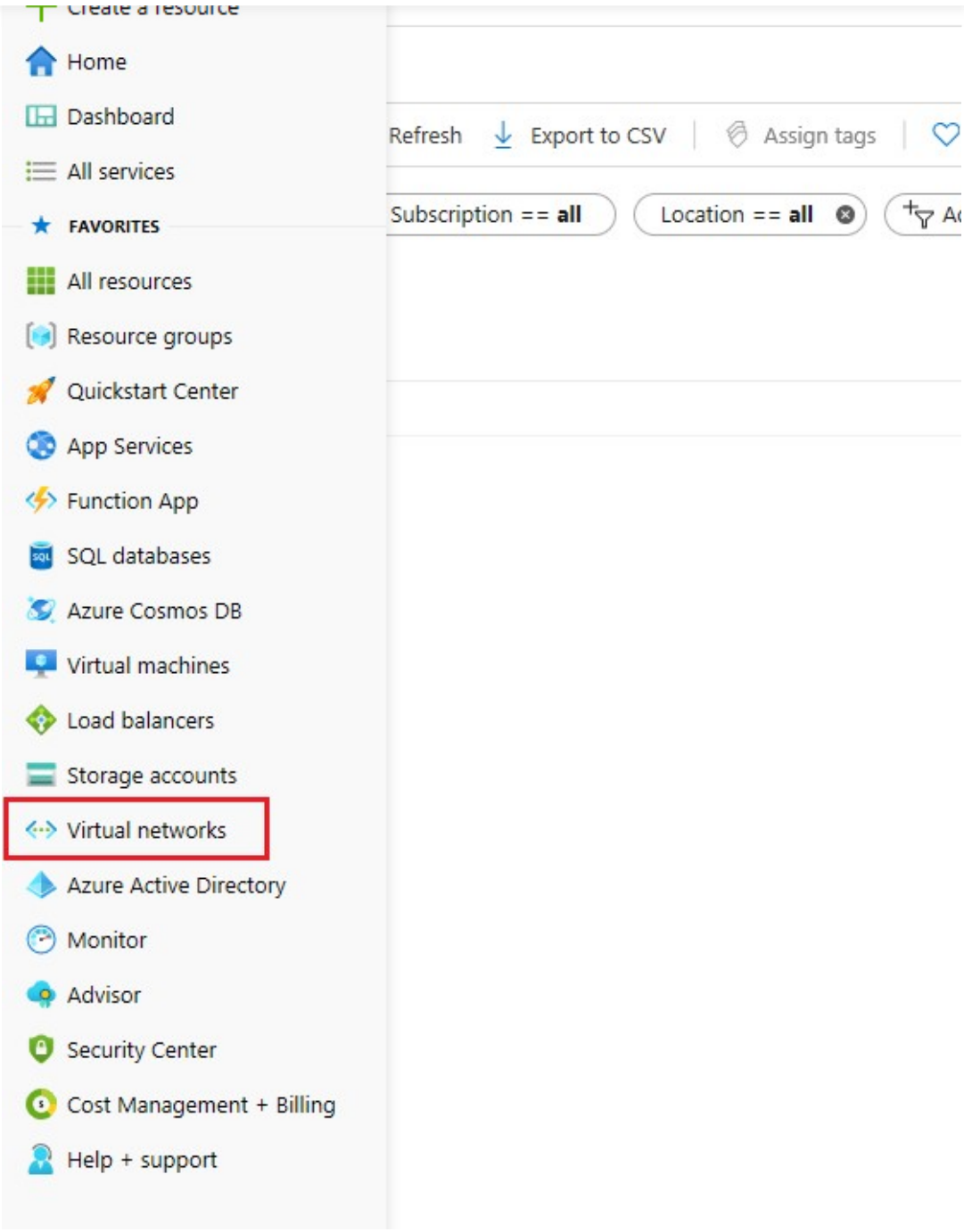


The newly created Resource group now shows up in the list.

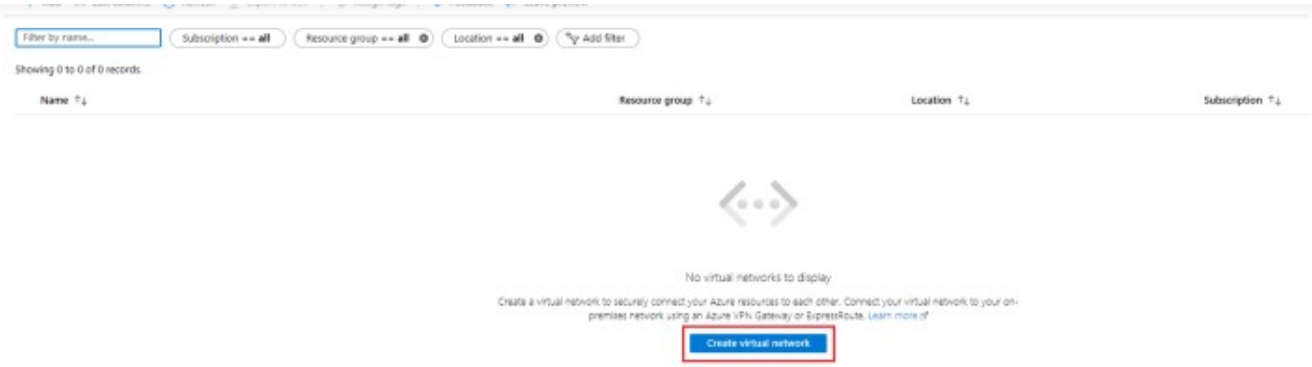


Virtual Network Creation

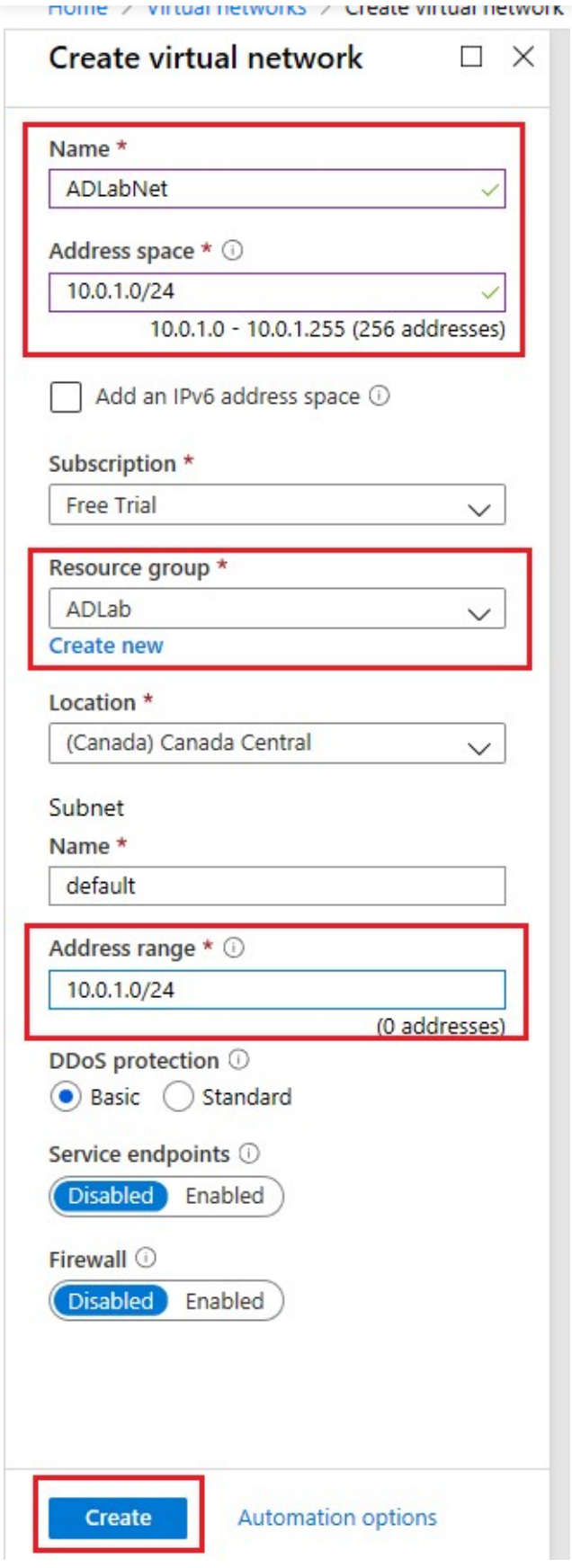
The next step is to create a Virtual Network that will enable Azure resources (such as Virtual Machines) to securely communicate within the network or outside networks. In order to do that, click on the **Virtual networks** in the navigation menu.



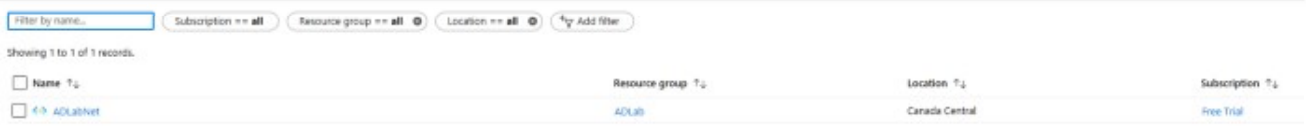
Next, click on the **Create virtual network** button.



Fill in the fields related to Creating that virtual Network. I used **ADLabNet** as the name of the virtual network. Further, I also used **10.0.1.0/24** as the address space and subnet address range. Make sure, you select the resource group **ADLab** that we created earlier. For the rest of the fields, I just used default values. Finally, click on the **Create** button.



That's it with Virtual Network creation. It should show up in the list as shown below.

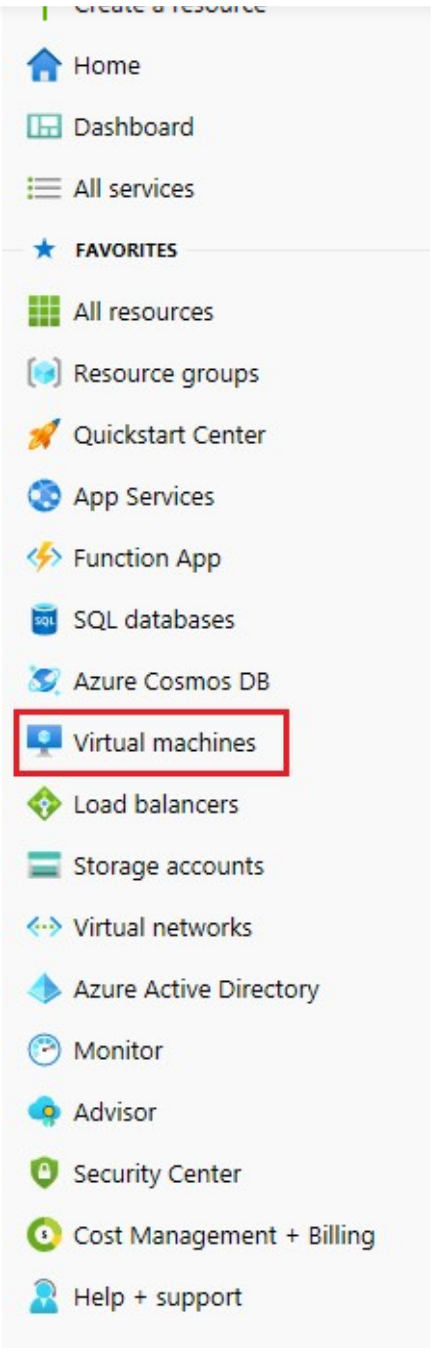


Domain Controller

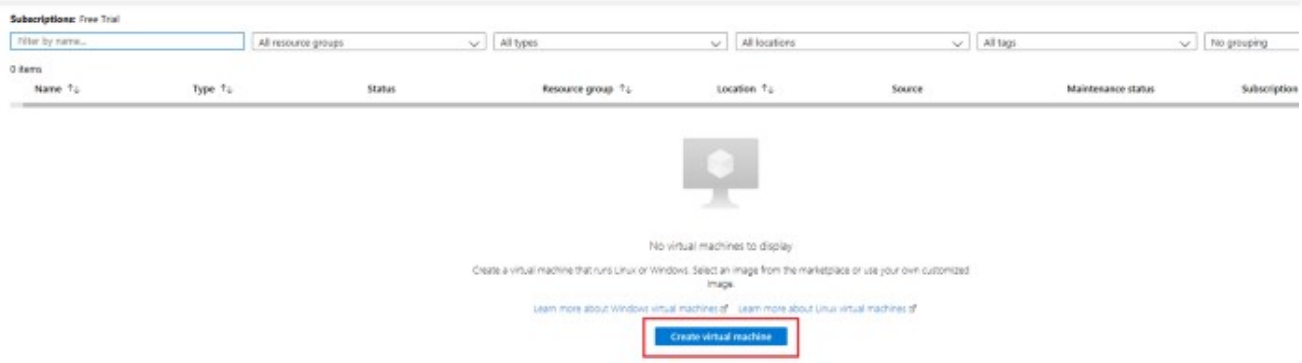
Creation of Domain Controller (DC) machine consists of few steps including creation of Virtual machine, making necessary configuring changes, promoting machine as DC, etc. Let's go over all these steps one by one.

Virtual Machine Creation

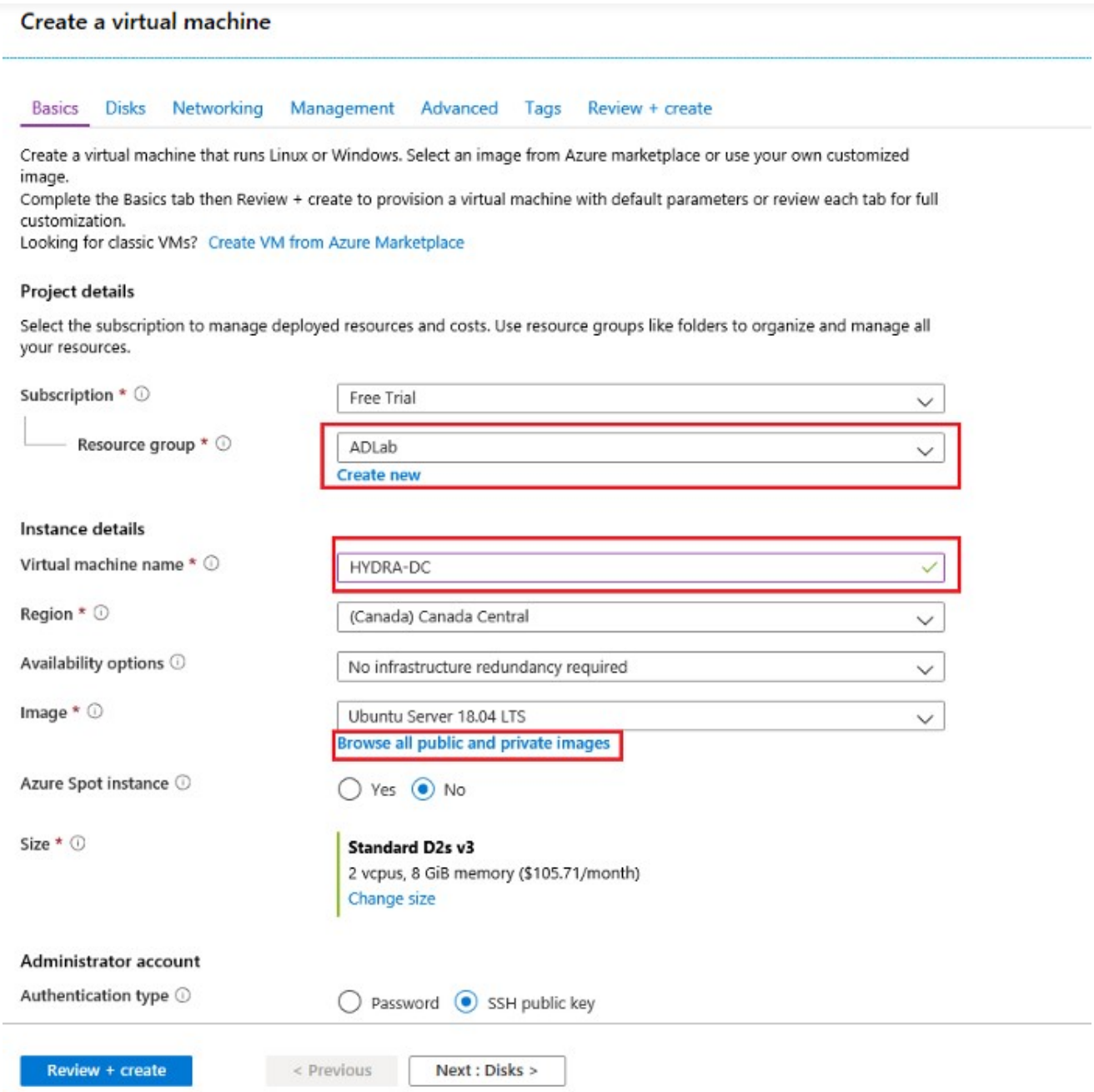
Let's start with the creation of the first Virtual Machine. This will be our Active Directory Domain Controller. I am going to use a Windows Server 2019 image for it. First of all, click on the **Virtual machines** menu item.



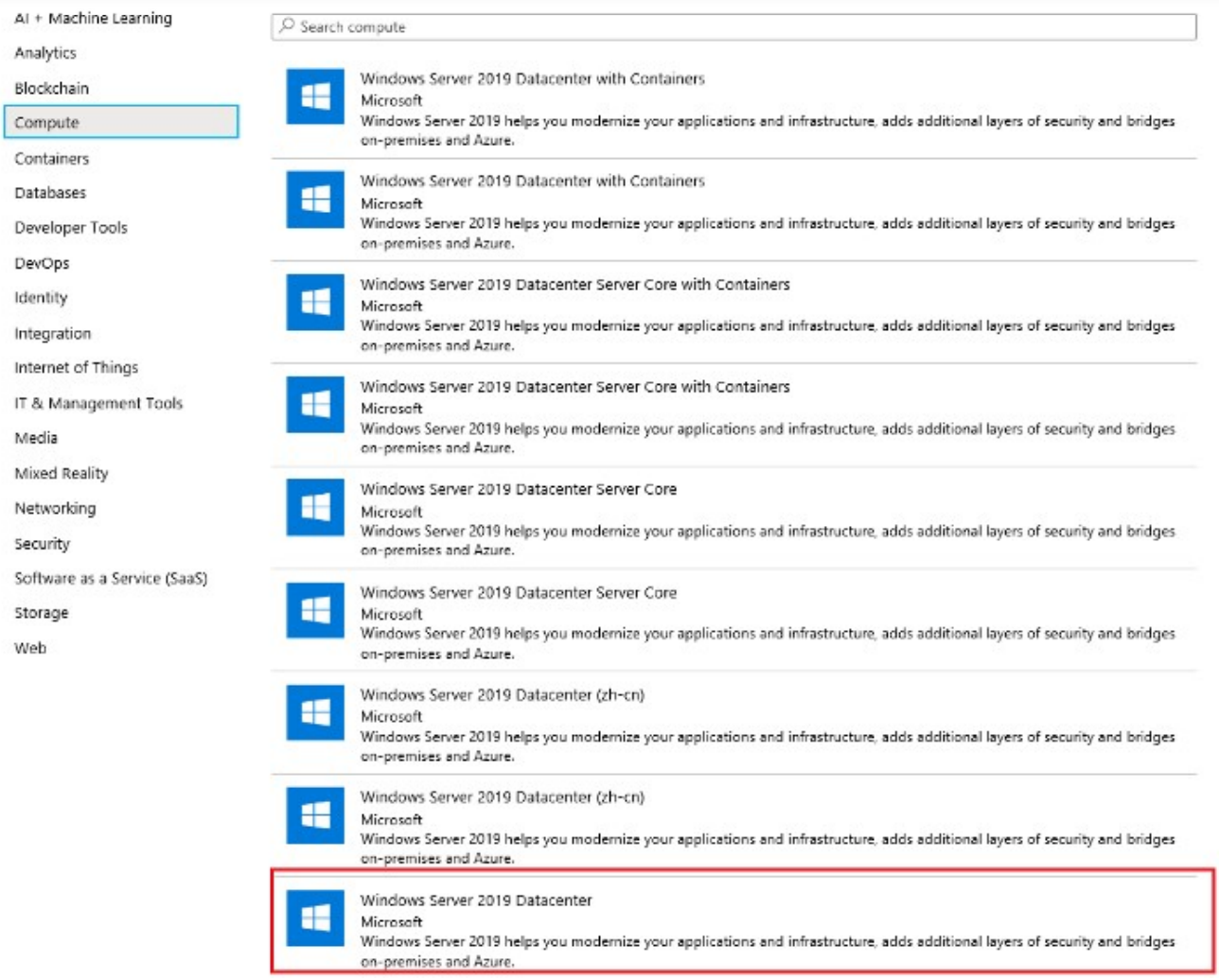
No virtual machines yet on this list. Just click on the **Create virtual machine** button.



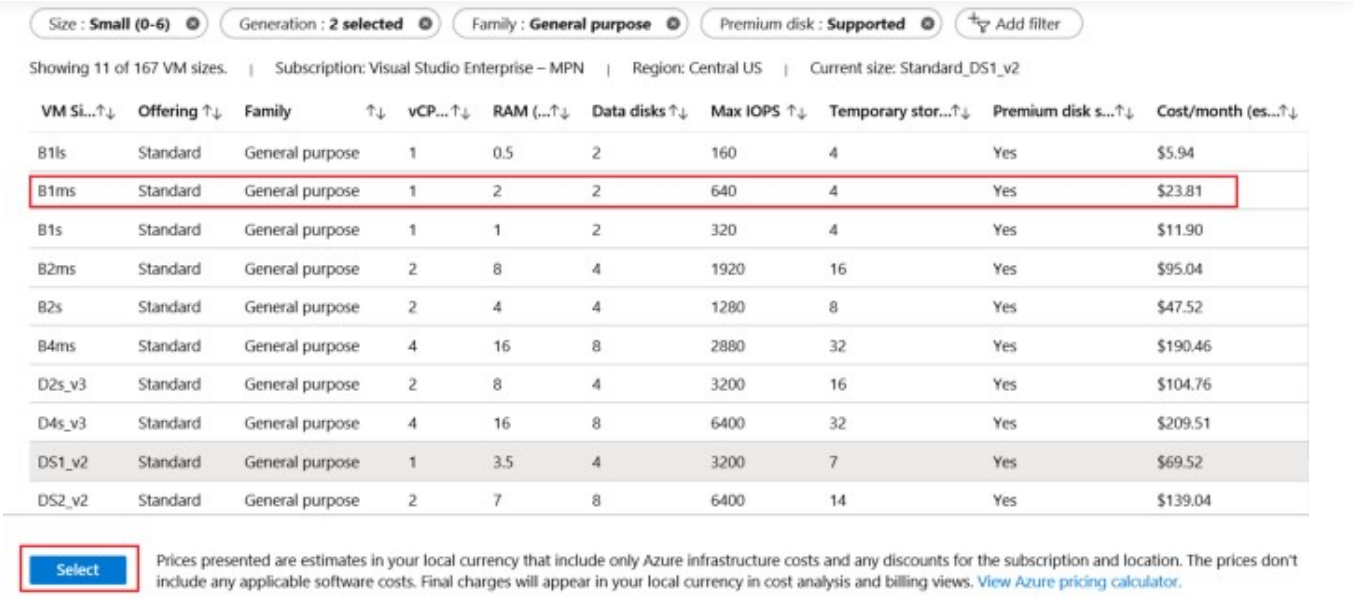
You will be presented with the following page. Make sure you select the **ADLab** resource group created earlier. Let's name the virtual machine **HYDRA-DC**. Click on the Browse all public and private images link to select the right image for our VM.



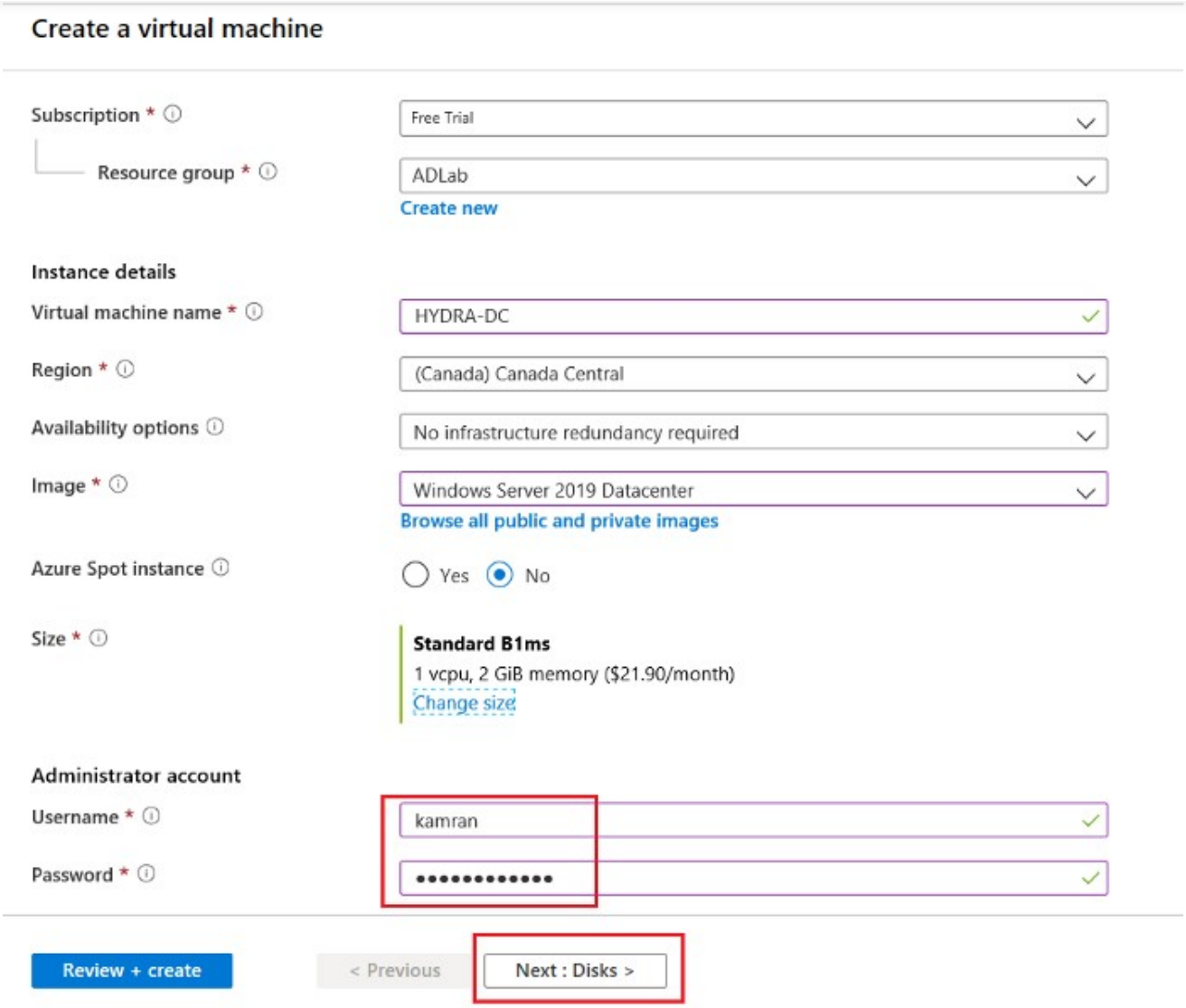
Click on the **Compute** item under the **Marketplace** tab and choose the **Windows Server 2019 Datacenter** image.



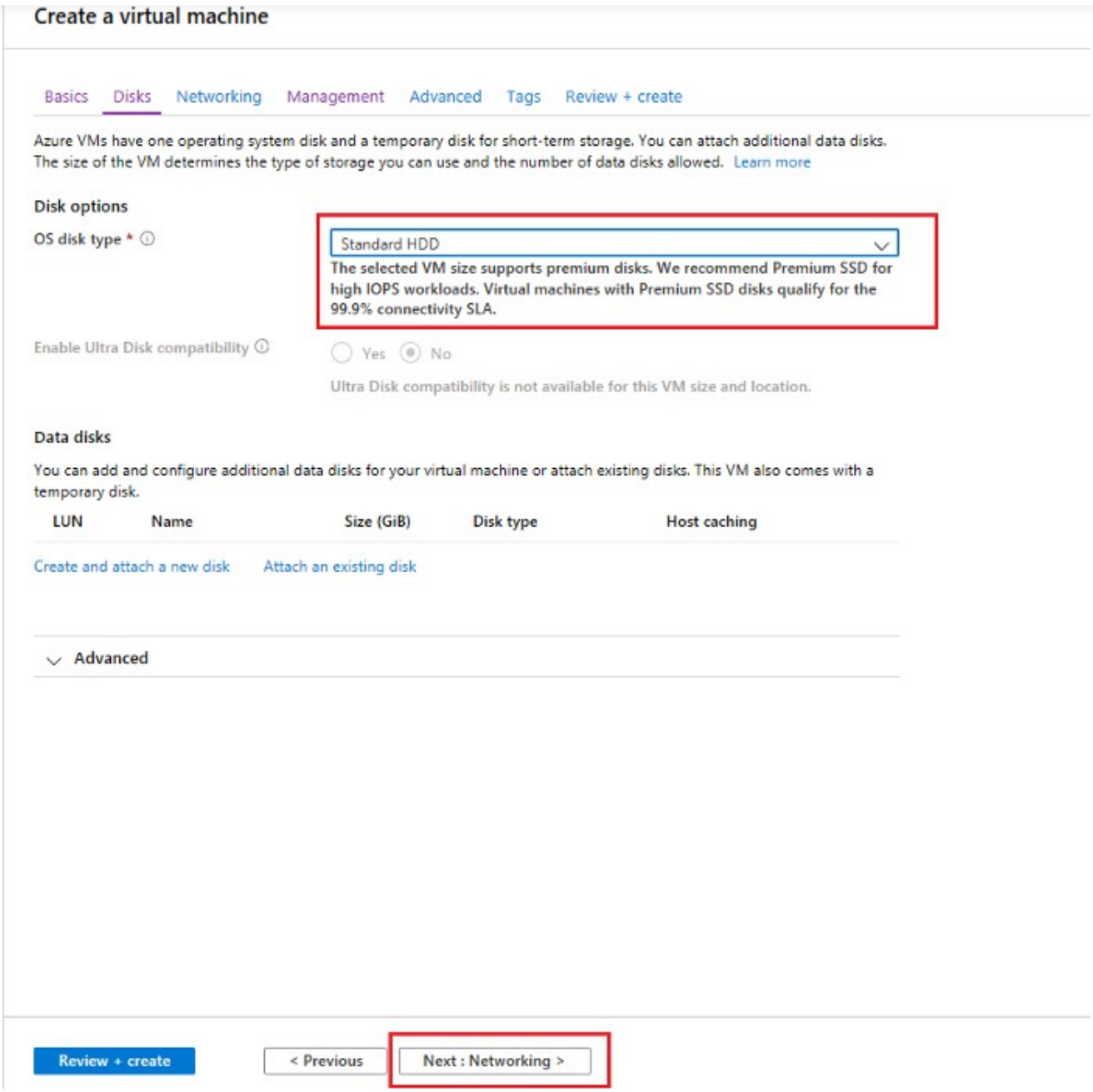
Now that the appropriate image is selected, from the **Create Virtual Machine** page, click on the **Change size** link. I am going to use the **B1ms** for this machine as shown below.



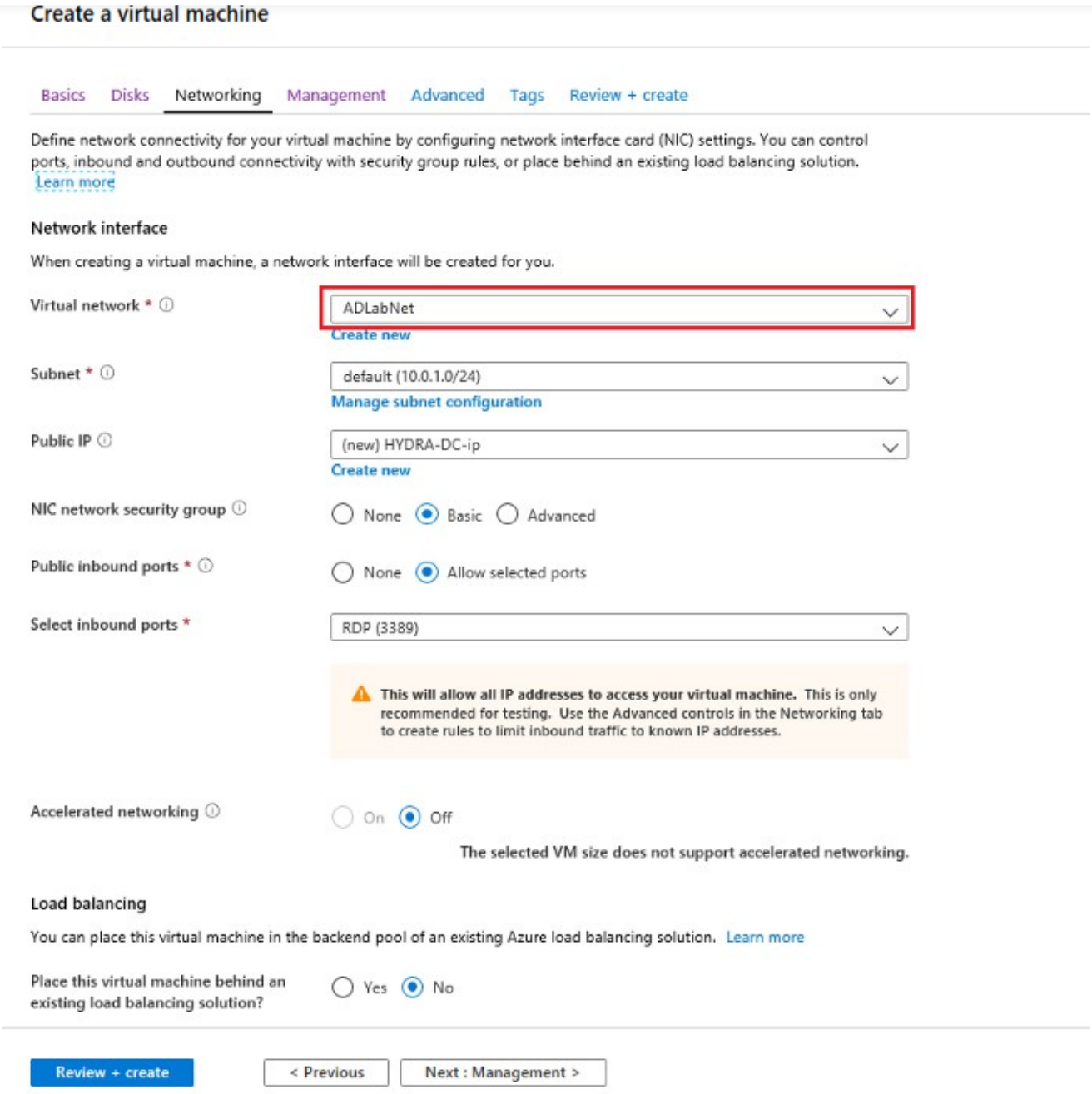
Now, we need to create an Administrator account. I used **kamran** as the username and **Password1234** as the password. Definitely not a strong password for an administrator account. Click on **Next: Disks** button.



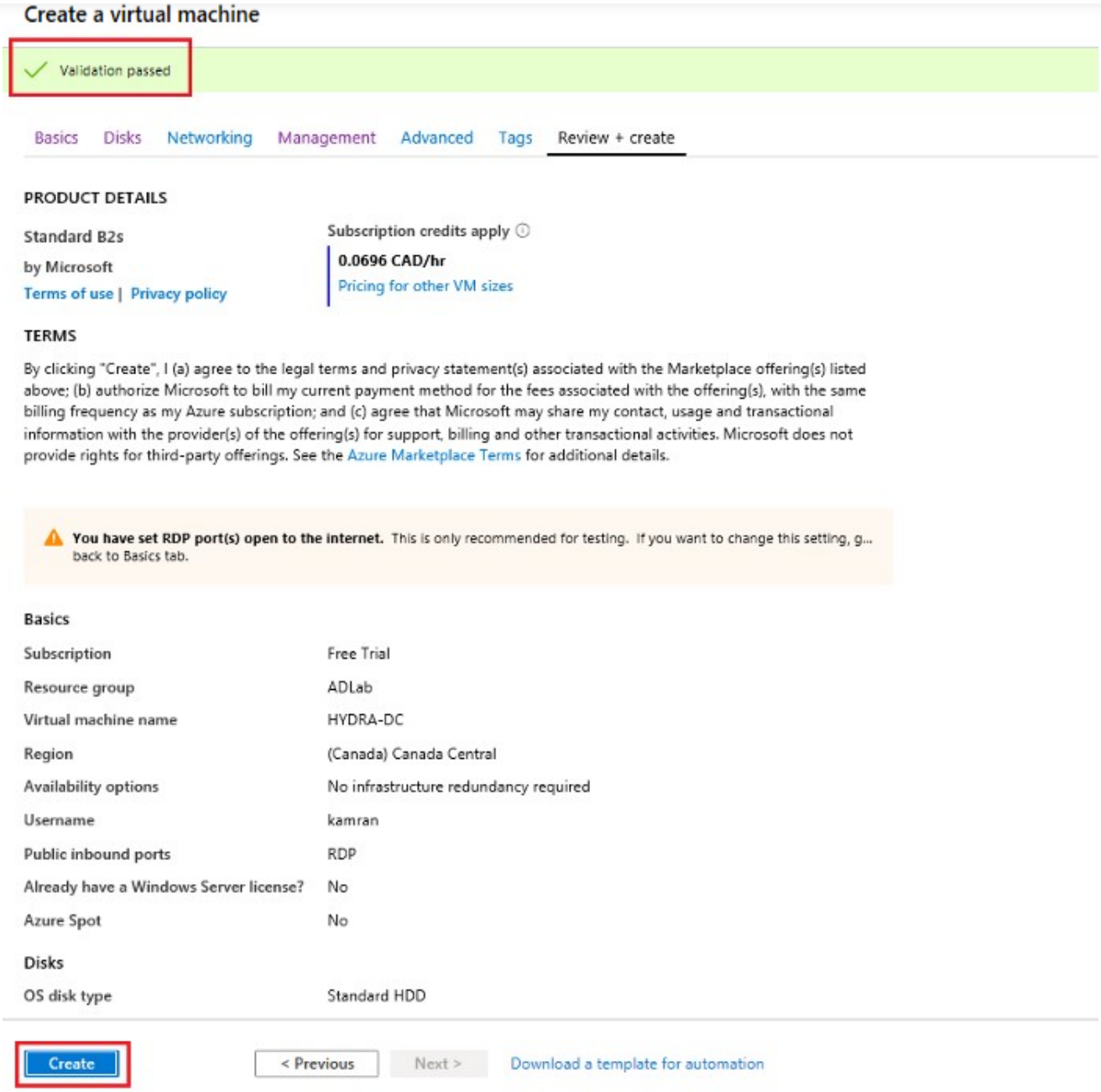
I chose **Standard HDD** OS disk type here. You can certainly go with the Premium SSD also but for the purpose of this lab, the Standard HDD is good enough. Click on **Next: Networking** button.



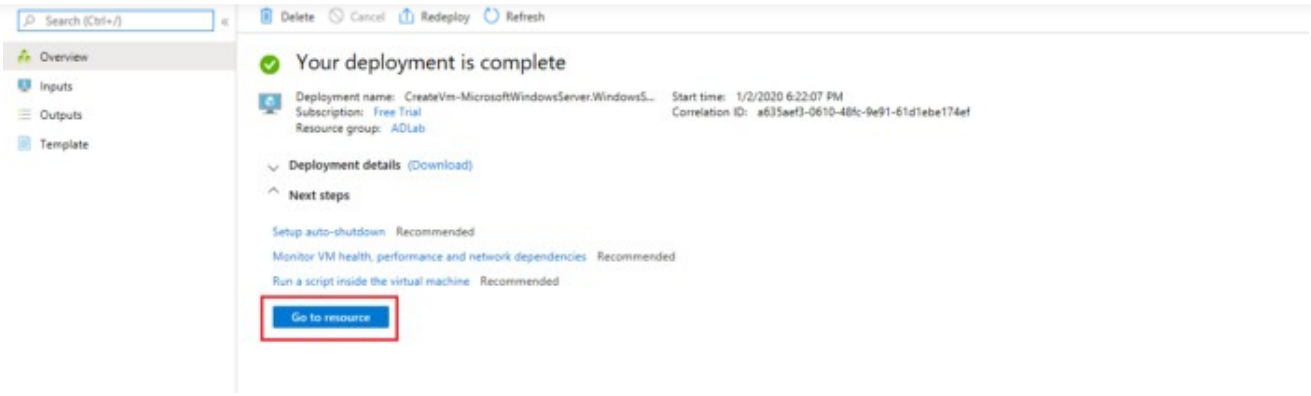
In the Networking tab, make sure the Virtual network is set to **ADLabNet** that we created earlier. For the rest of the steps, we just accept all the defaults and click on **Review + create** button.



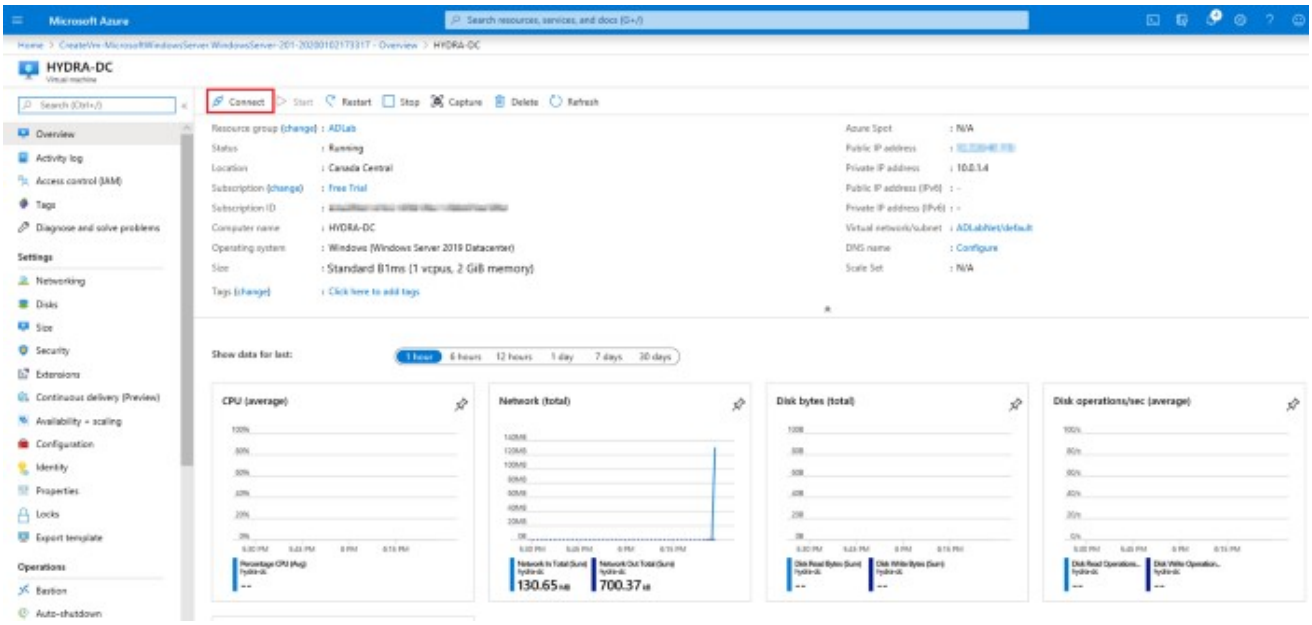
Once getting the successful validation, click on the **Create** button to create the Virtual Machine.



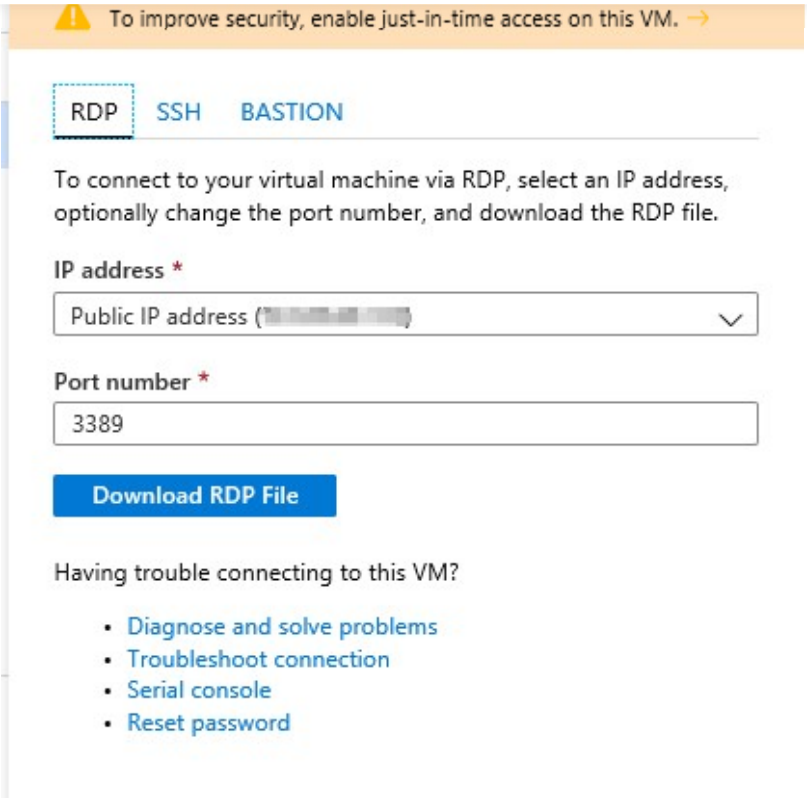
It will take a few minutes but if everything goes well, you should see a message stating that deployment is completed as shown below. You can click on the **Go to resource** button to navigate to the page for this newly created Virtual machine.



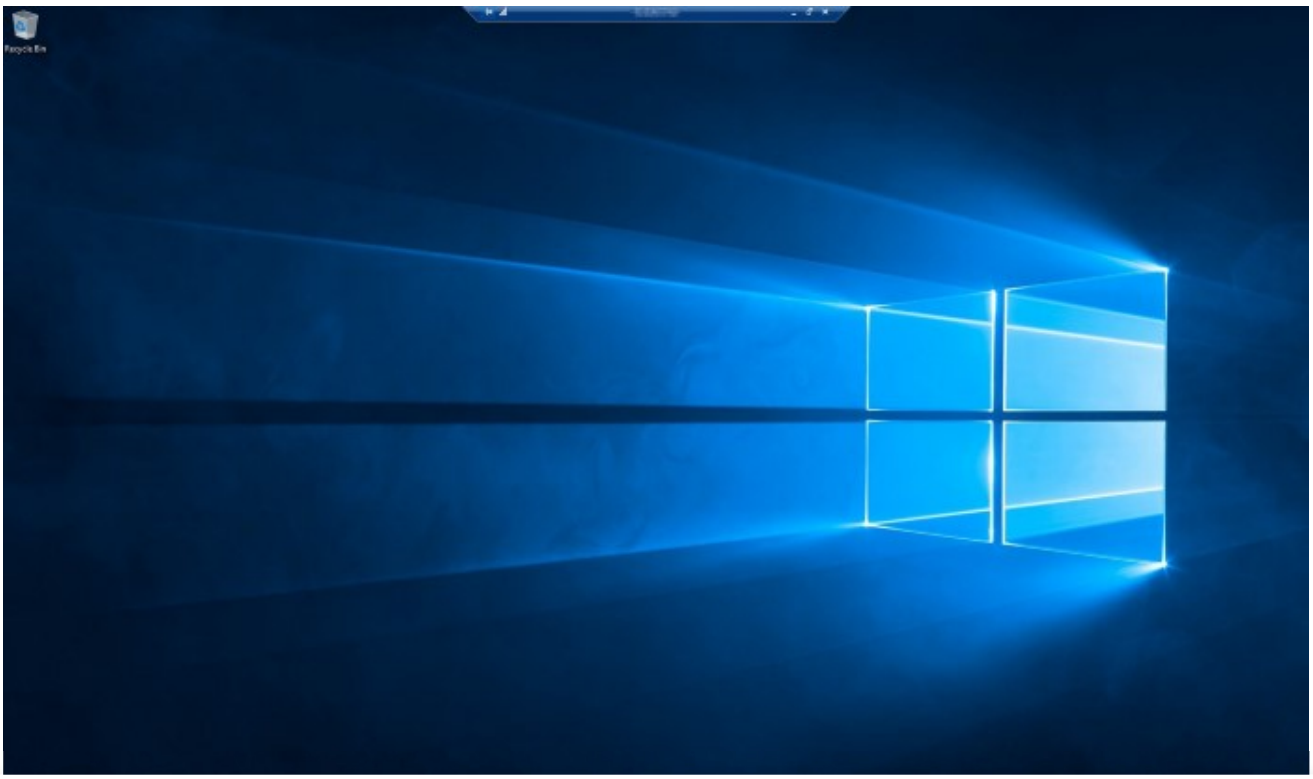
You can click on the **Connect** button to see various options for connecting to this machine.



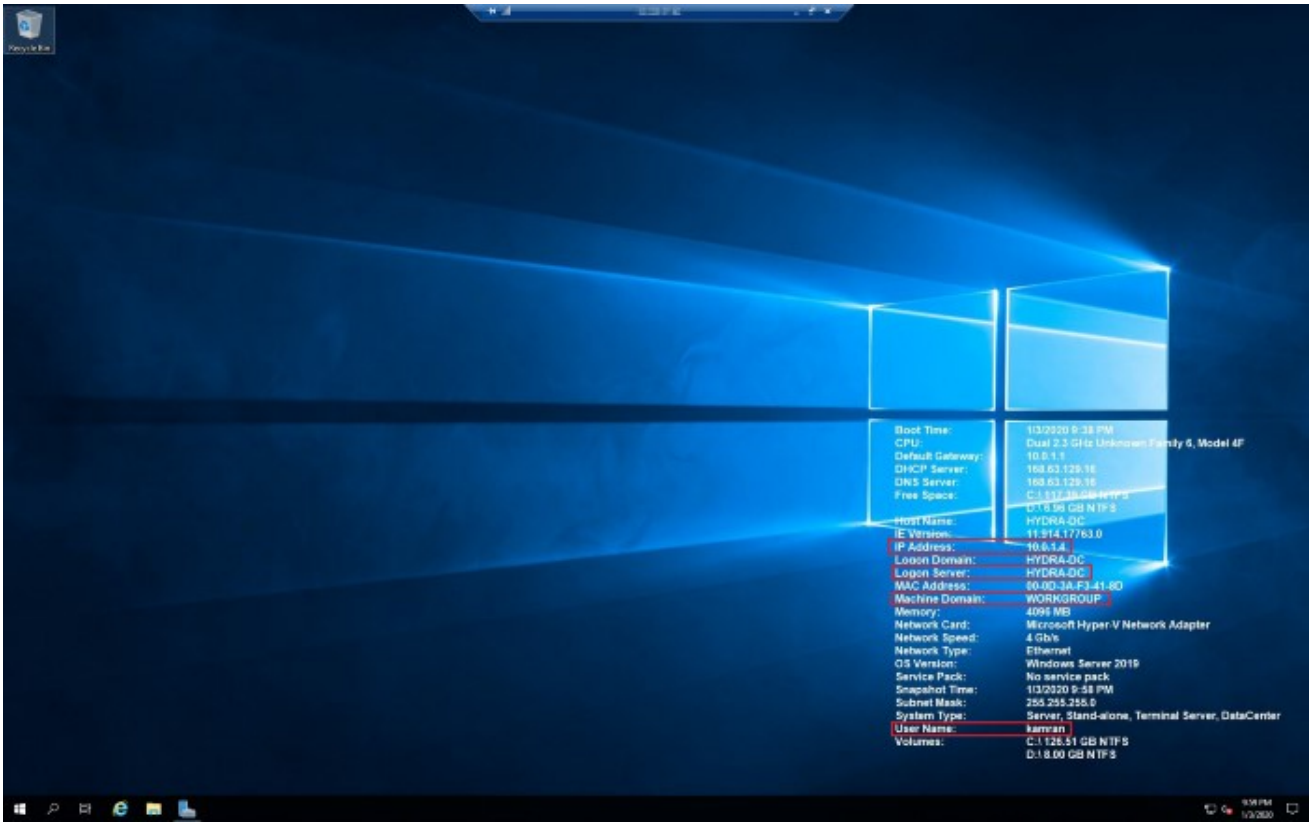
Let's choose **RDP** and download the appropriate file for connecting to the VM.



You should be able to login using the username **kamran** and password **Password1234** that we set up earlier in the process. After RDP into this box, you will see a Desktop like the following.

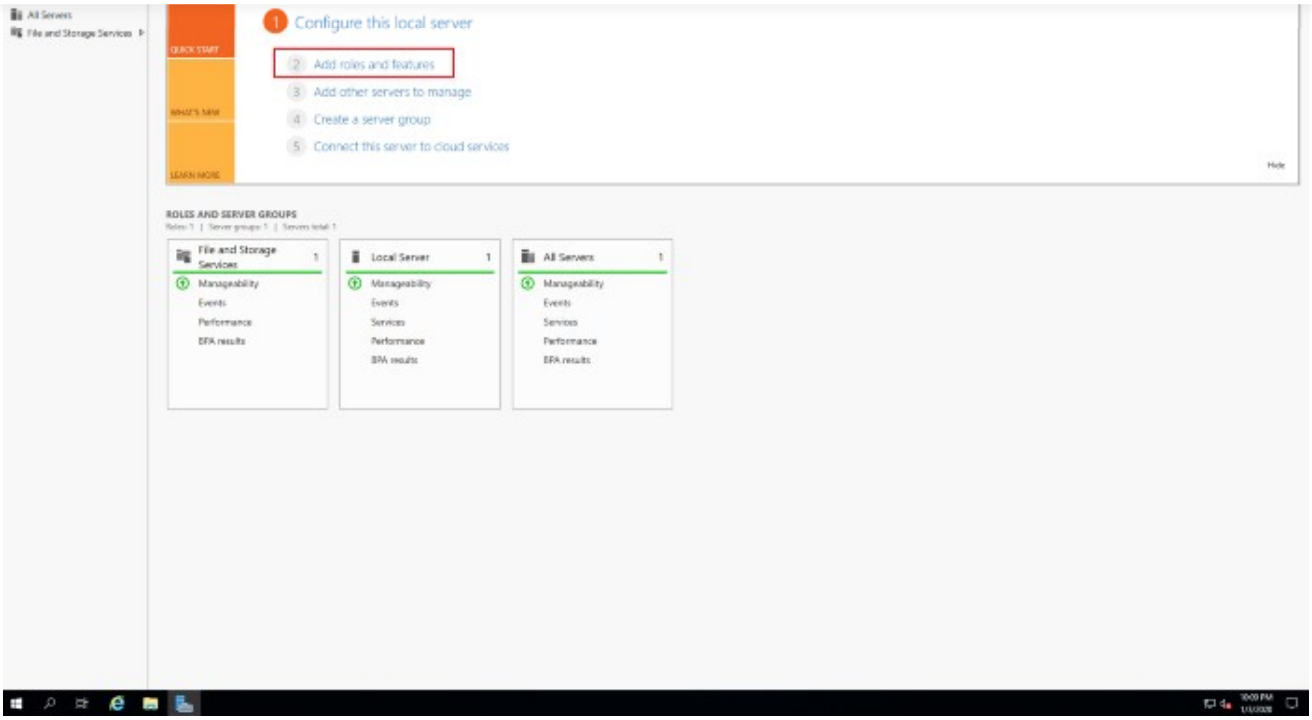


BgInfo utility that setups your desktop background with an image with some useful information such as IP address, machine name/domain, Username, etc. as shown below.

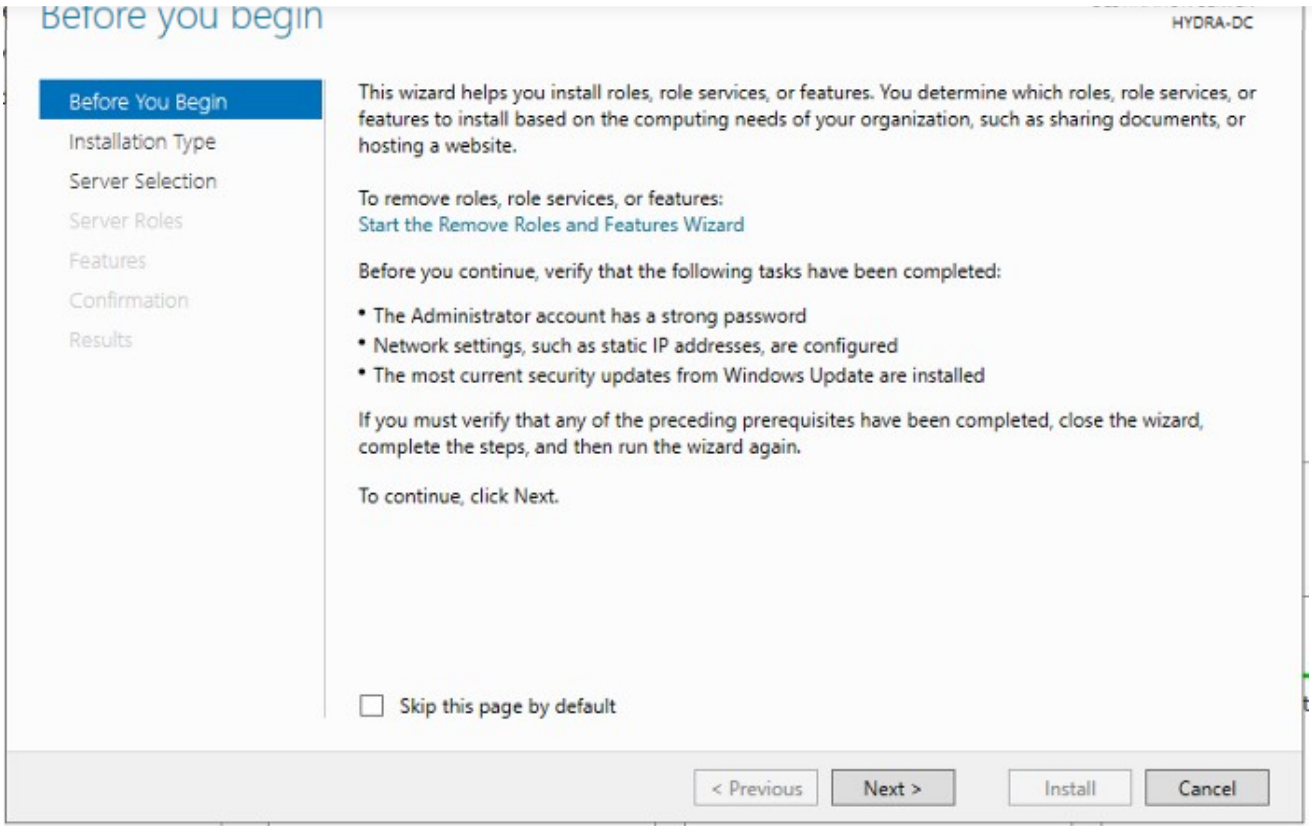


Configuring Services

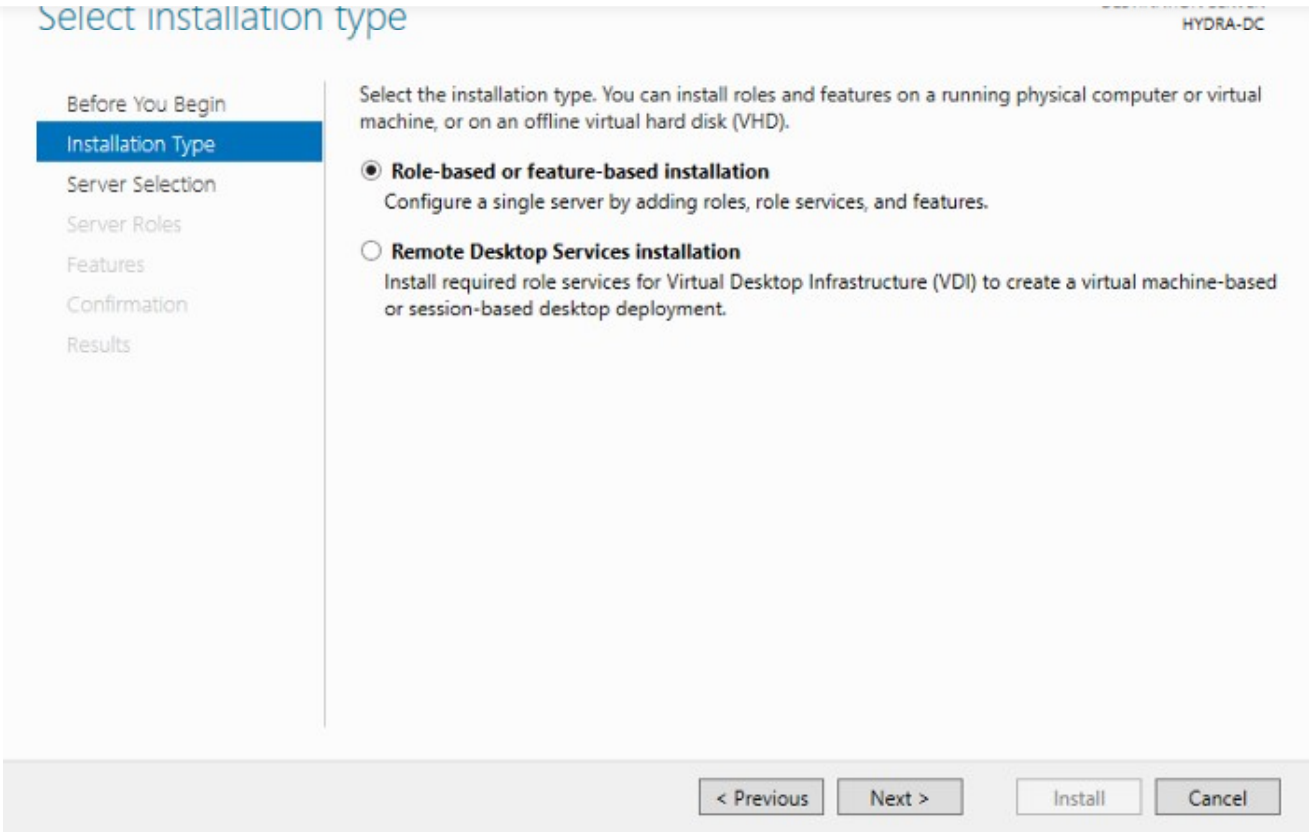
Now that we are connected to the machine, its time to configure it as a Domain Controller. Let's launch the Server Manager and click on **Add roles and features** option.



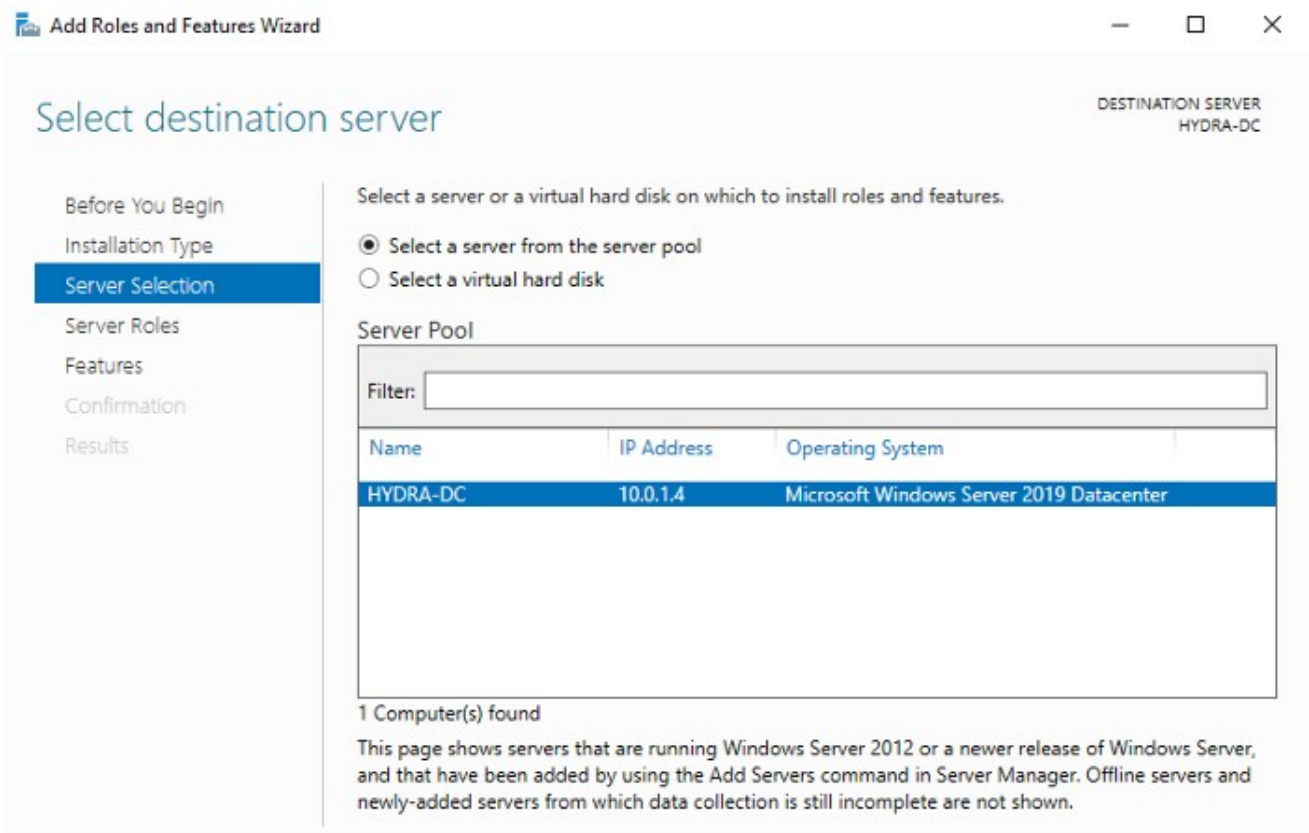
This will start the **Add Roles and Features Wizard**. The first tab **Before you begin** simply provides some information about the wizard and a few suggestions about tasks that should be completed before continuing with this wizard. Make sure you read and understand it and then click Next.

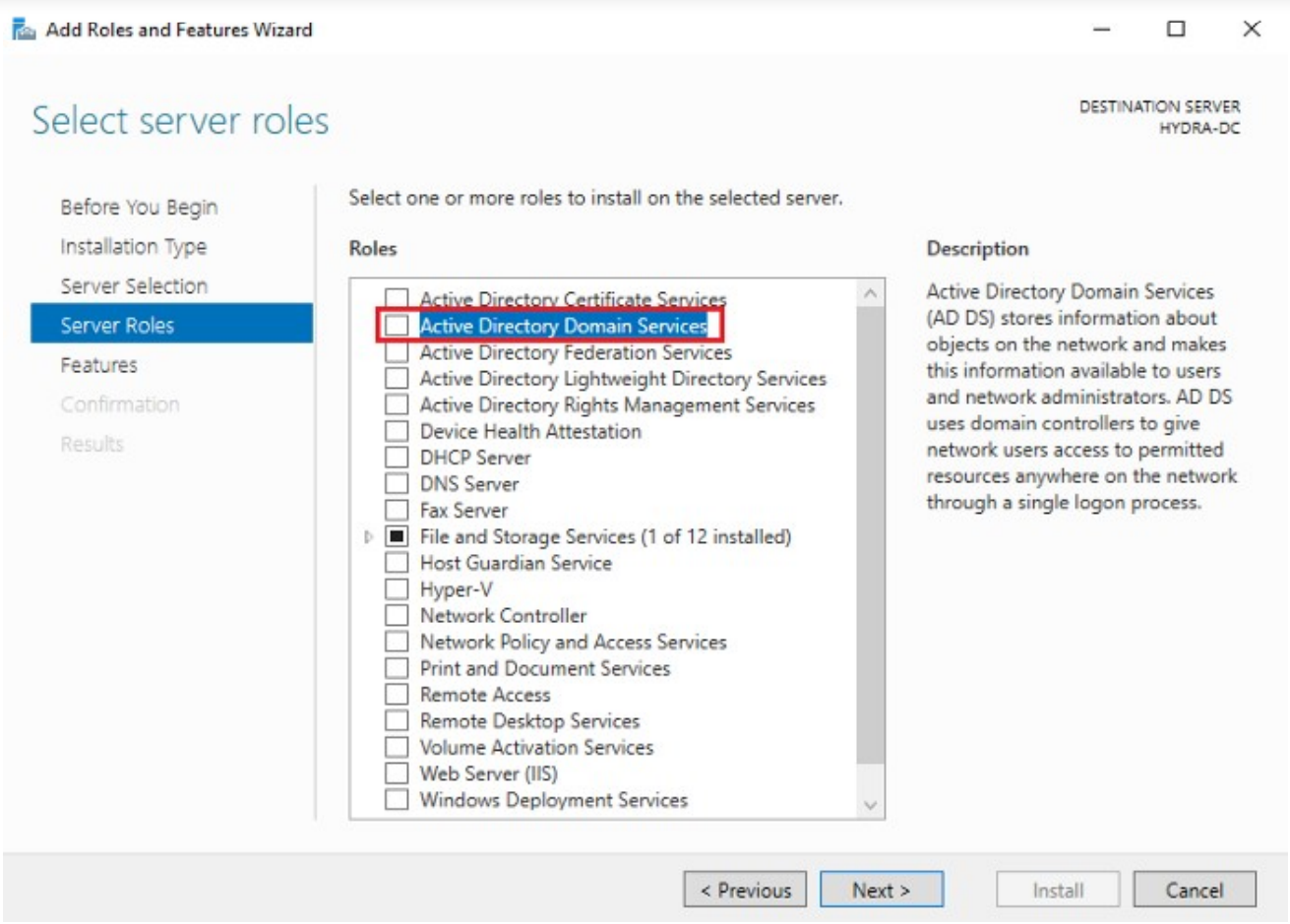


On the next tab **Installation Type**, we just choose **Role-based or feature-based installation** option and click Next.

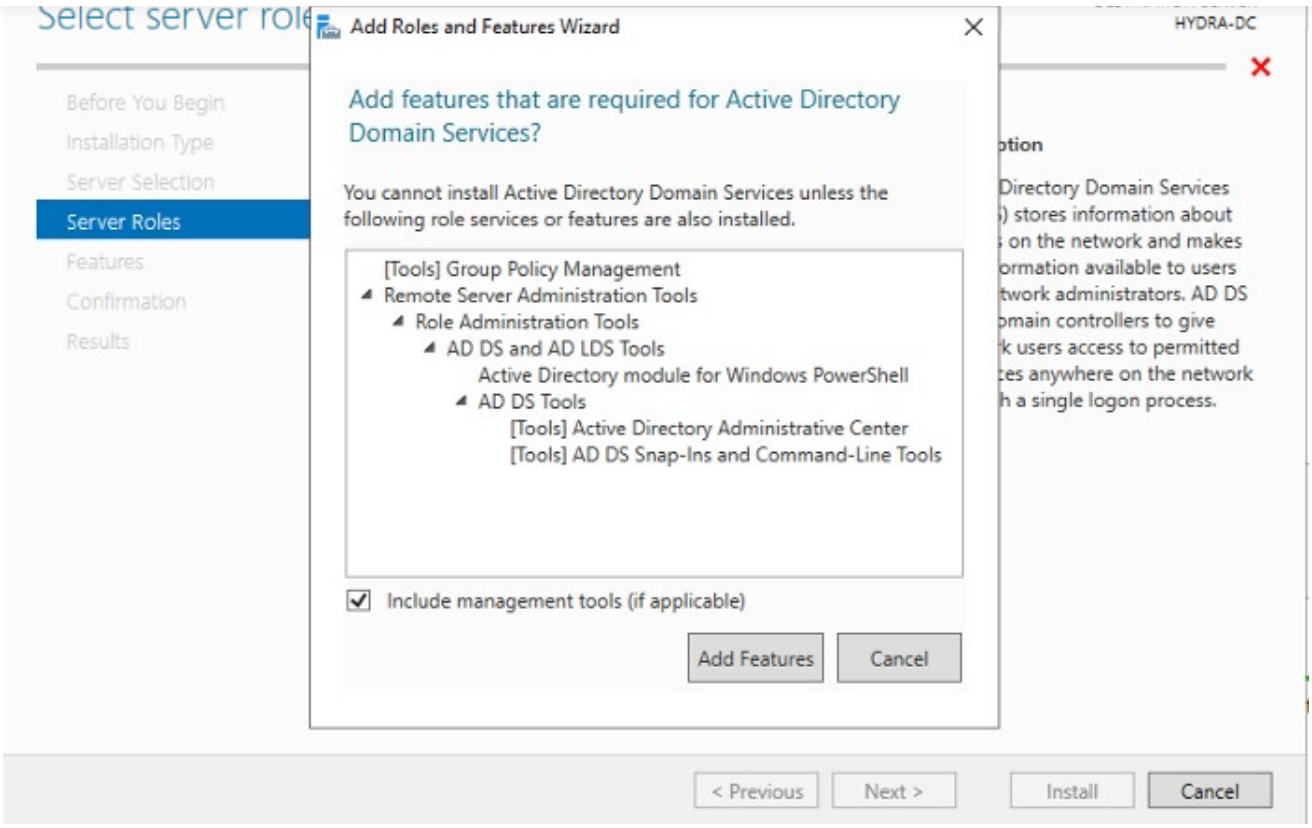


On the next tab **Server Selection**, we can just choose **Next**.

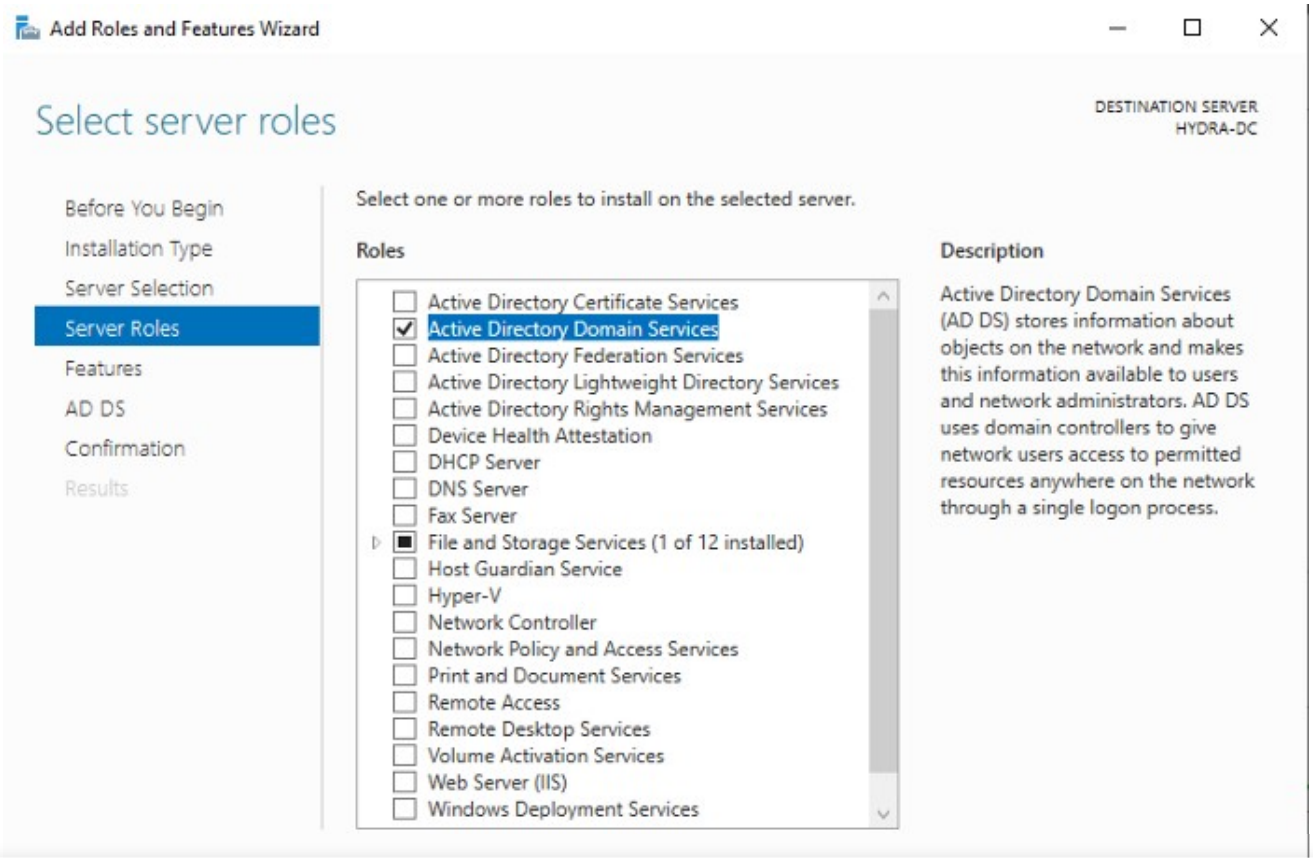


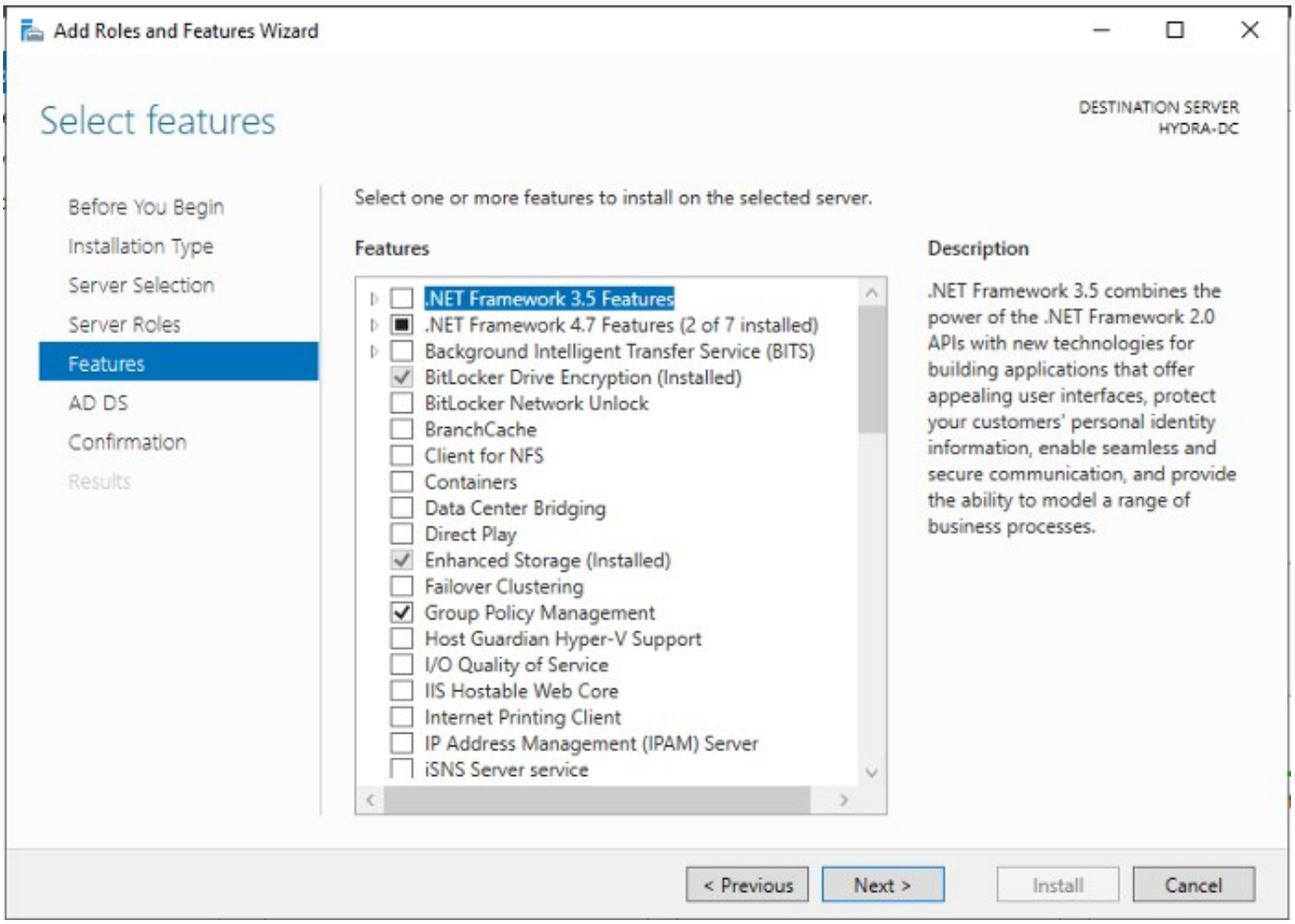


This will bring up following dialog where you simply confirm that you are ok installing other features that Active Directory Domain Services (ADDS) will have to install as well. Click on **Add Features** button.

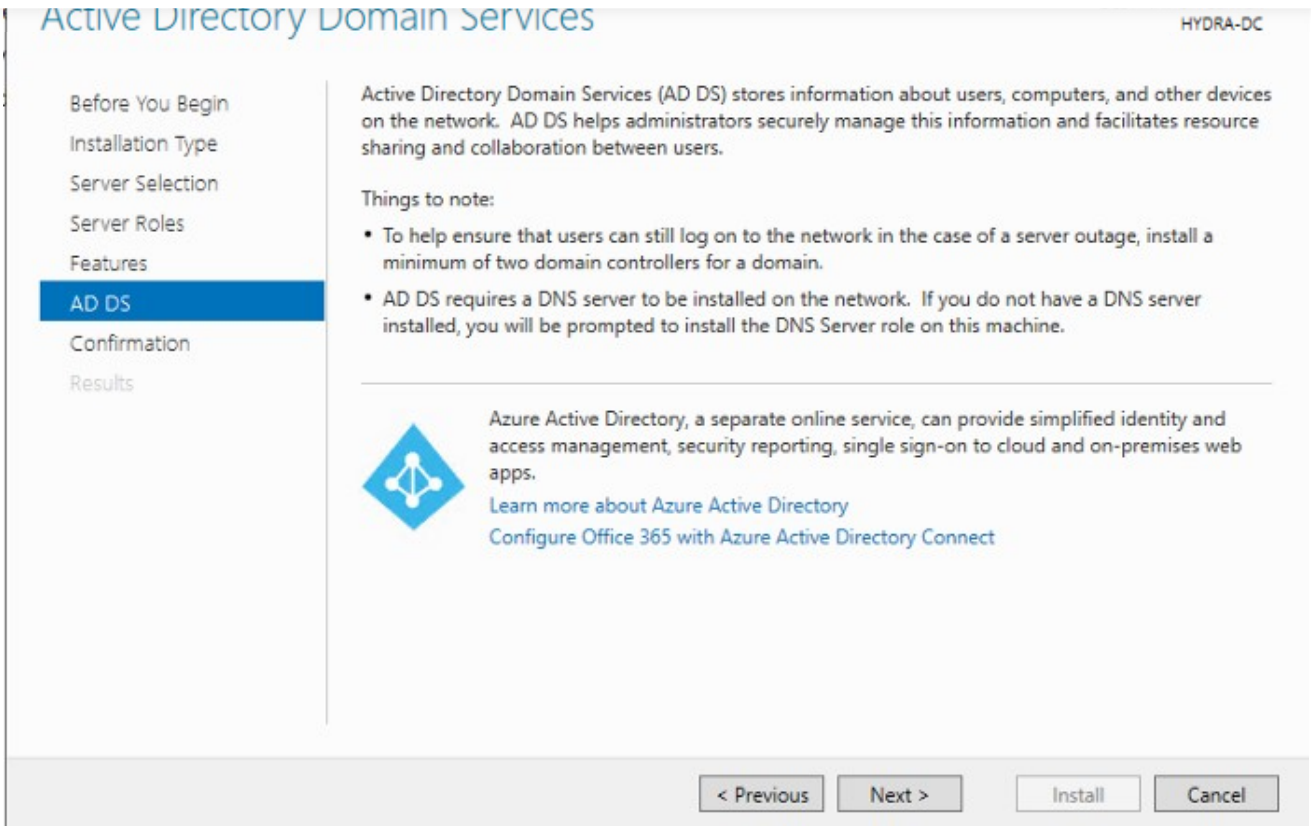


Click Next.

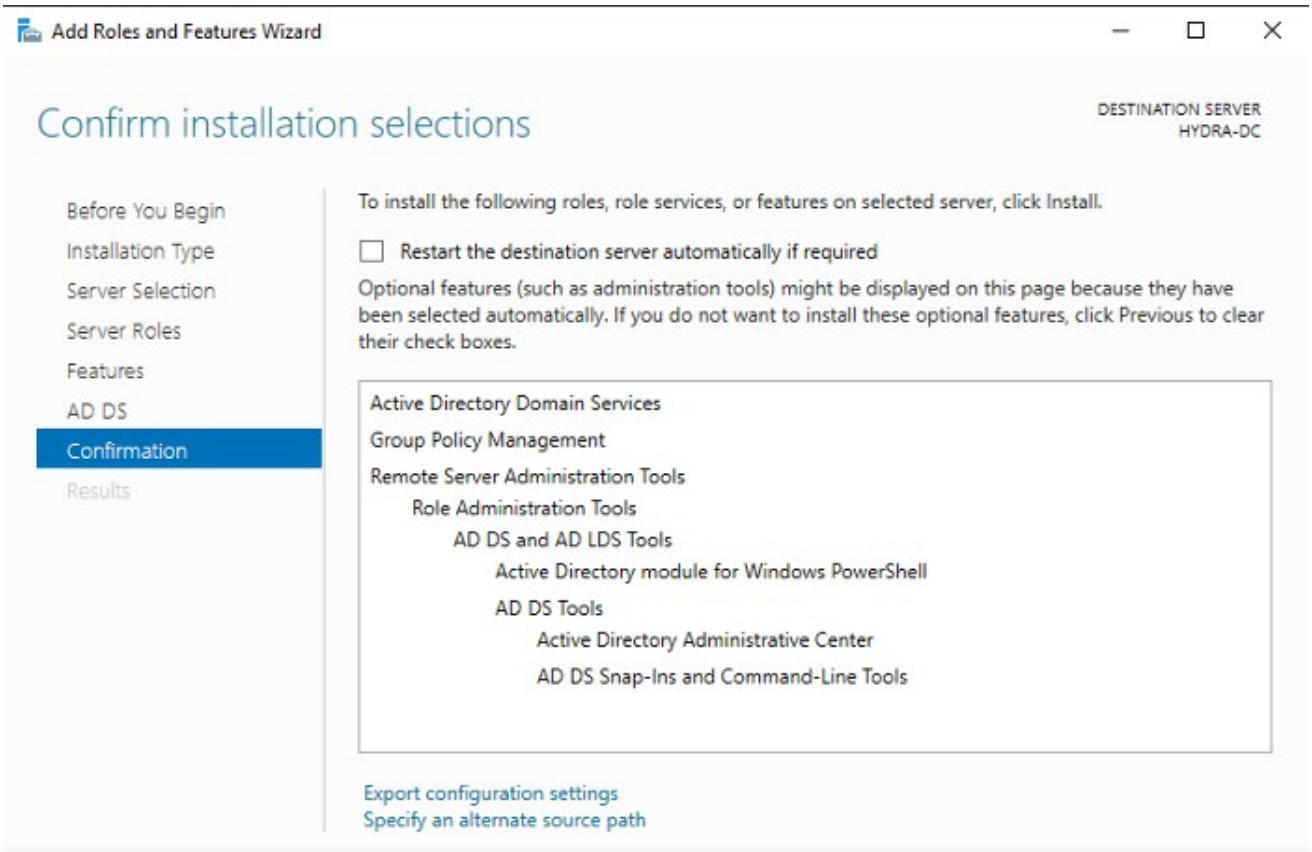


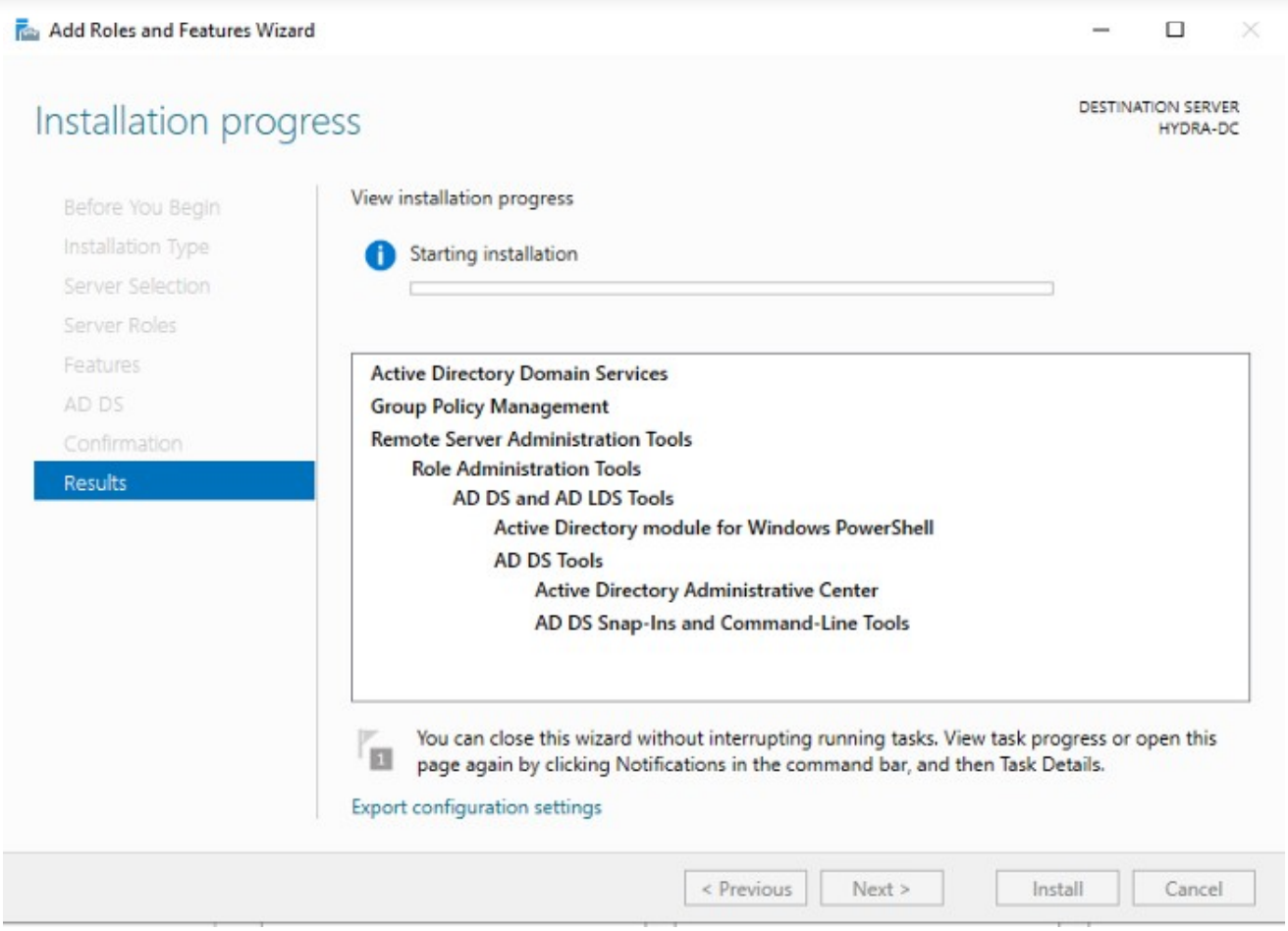


You can click Next on the **AD DS** tab.

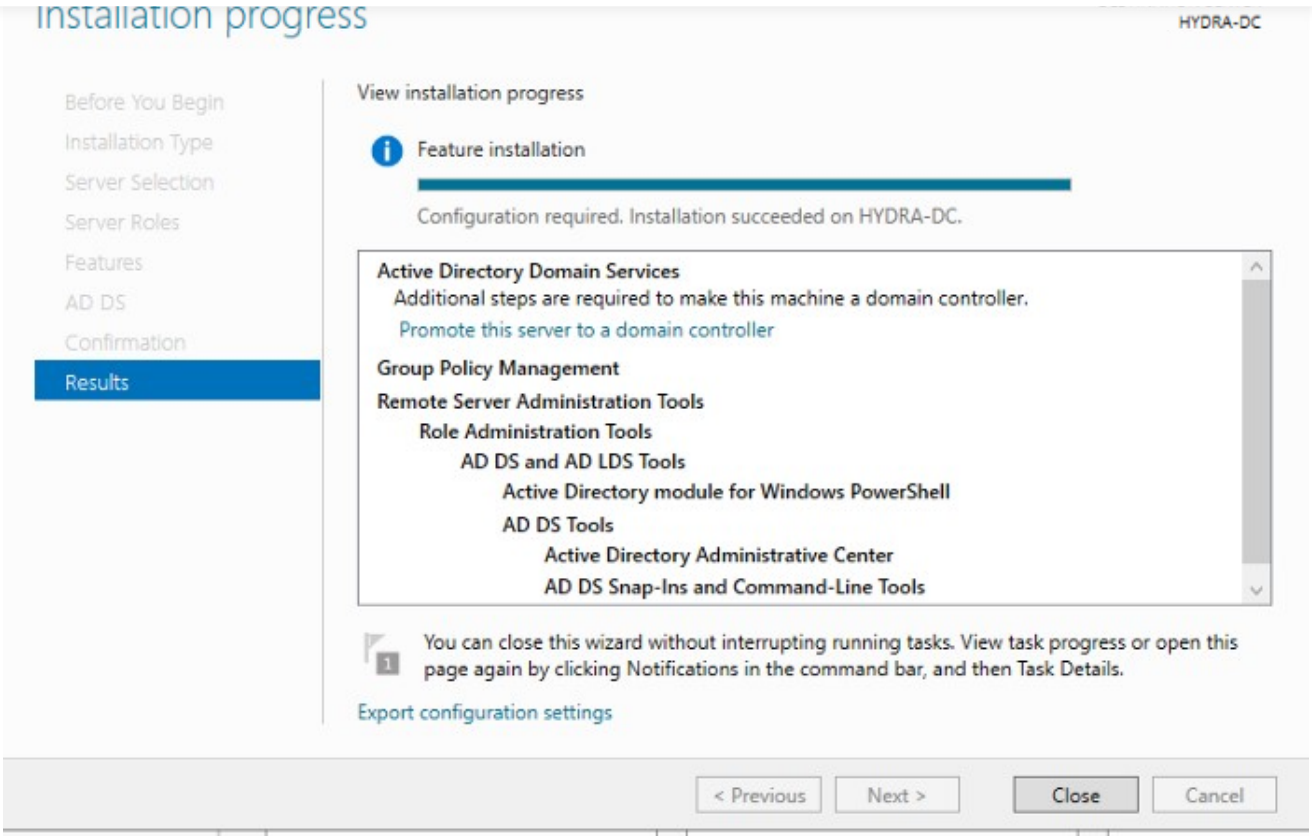


Click **Install** on the **Confirmation** tab.

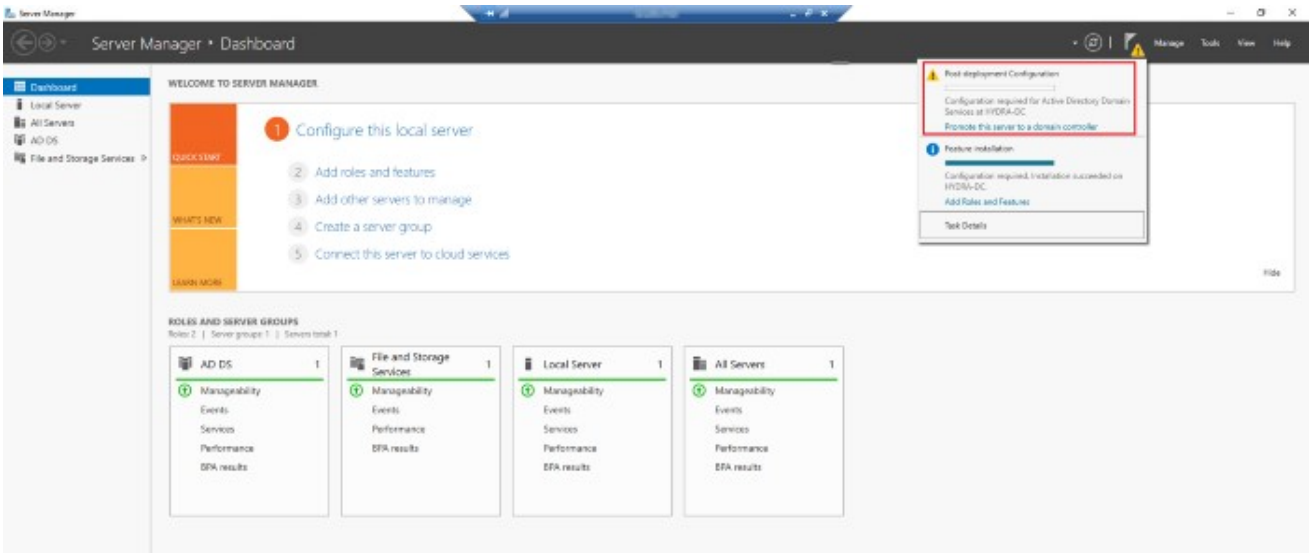




Once the installation is complete, you can just click the Close button.

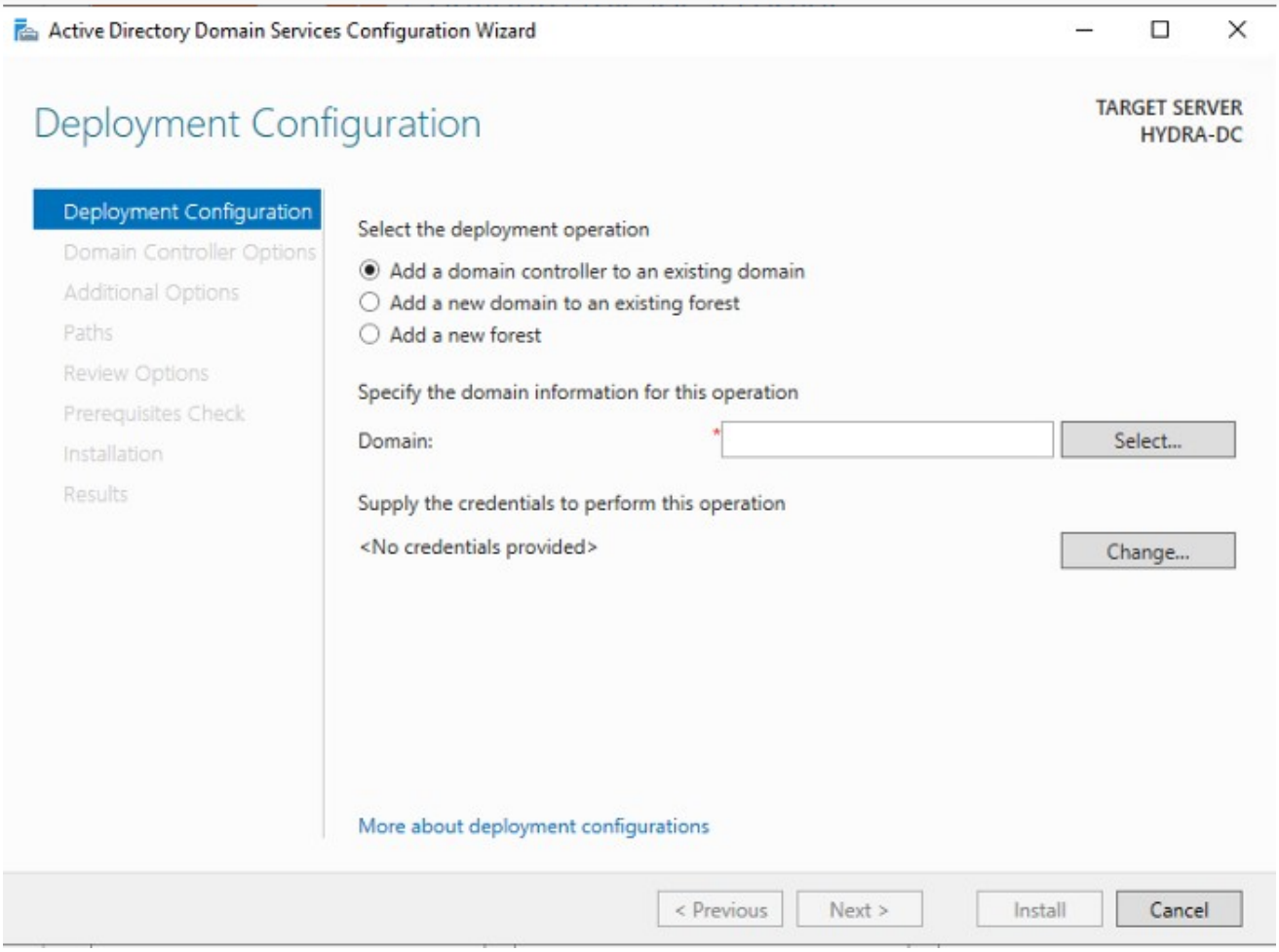


At this point, it will show you a warning flag as shown in the image below. Clicking on the flag will show you the link for **Promote this server to a domain controller**. Click on that link.

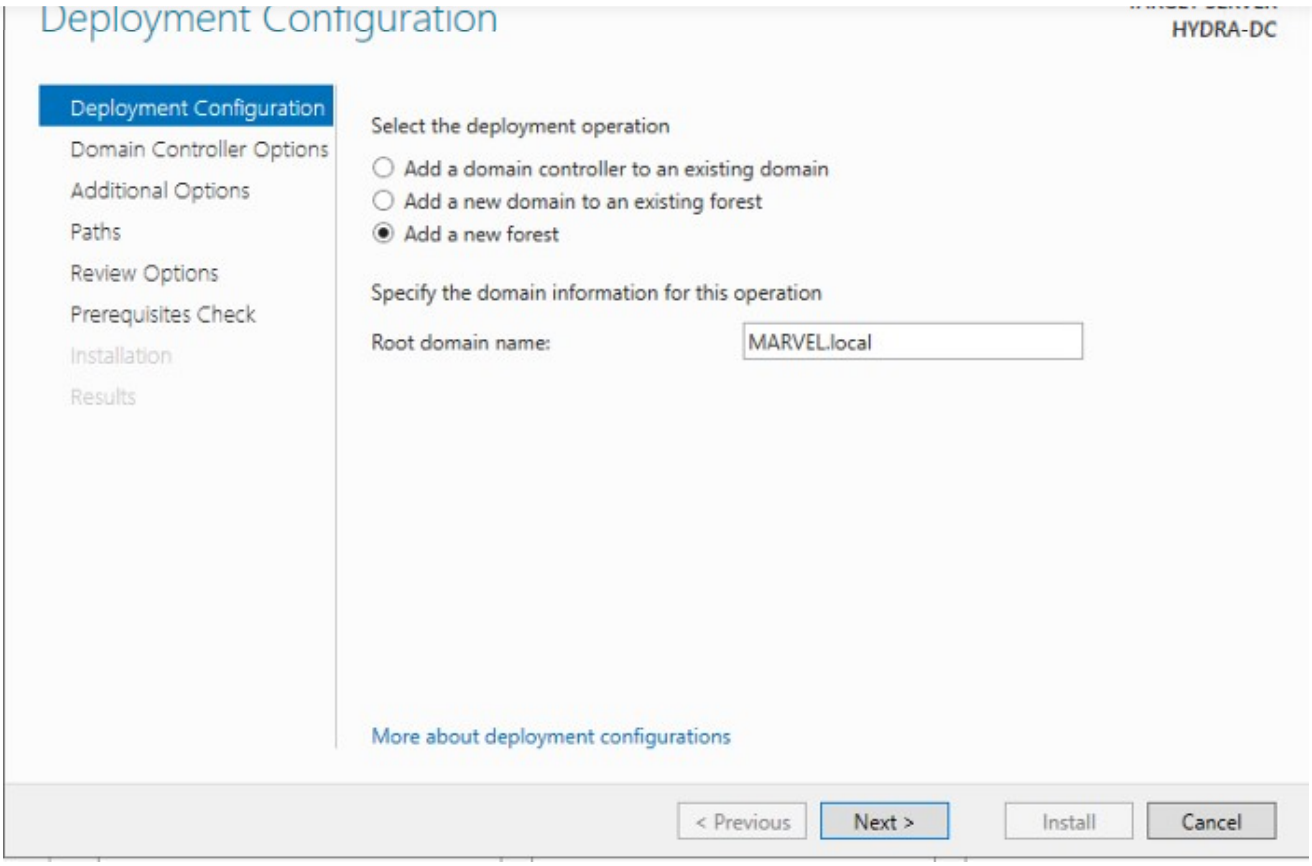


Promote VM to Domain Controller

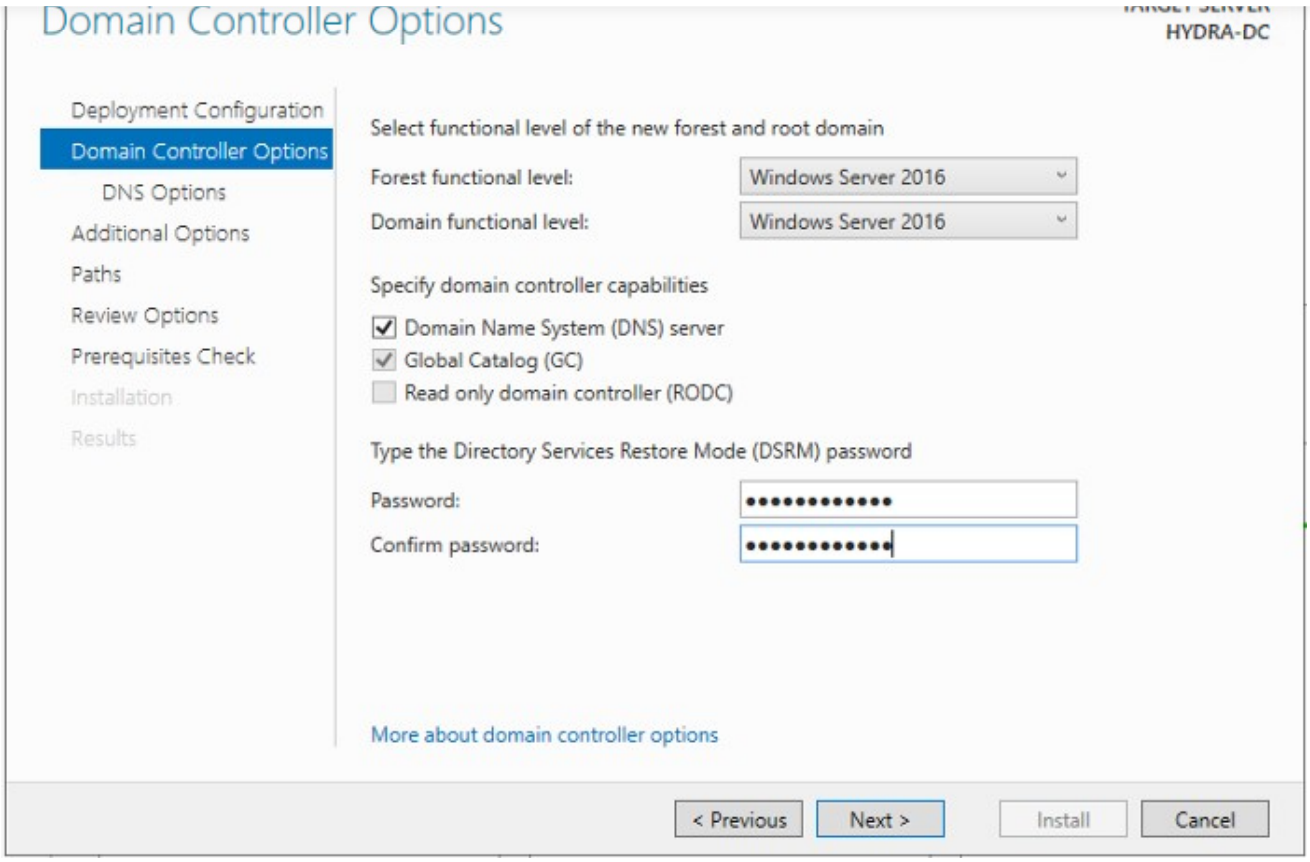
Clicking on the **Promote this server to a domain controller** link will launch **Active**



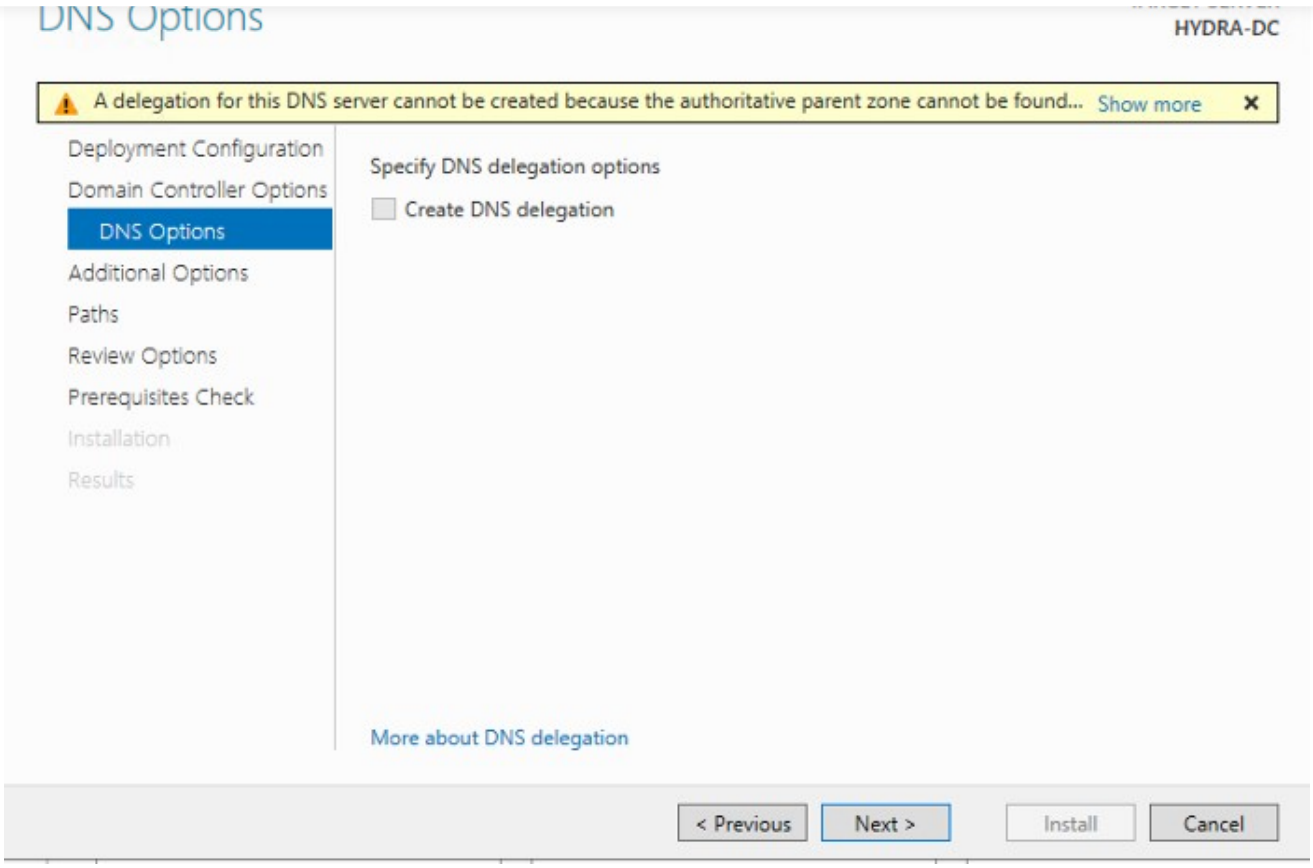
Enter **MARVEL.local** as the domain name and click Next.



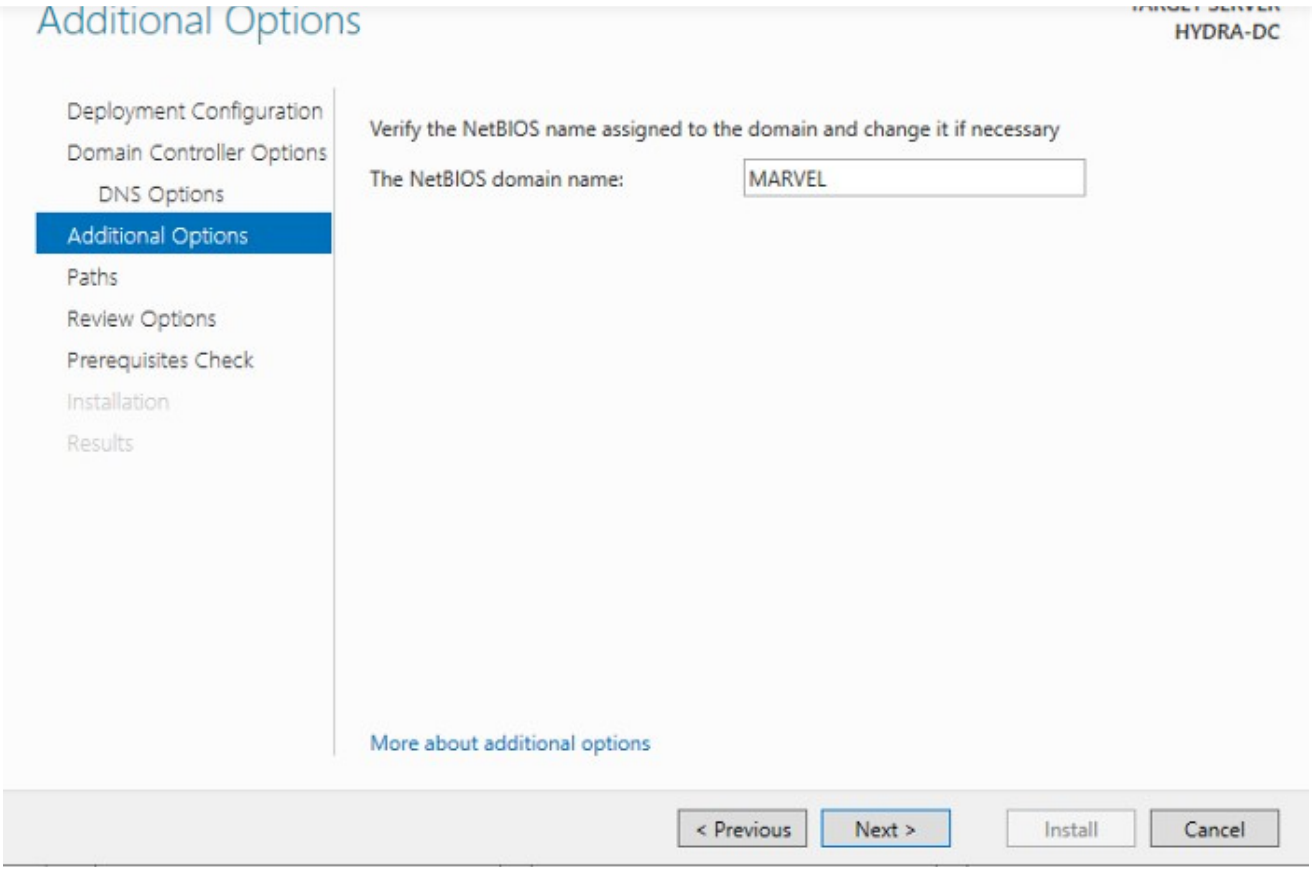
On the **Domain Controller Options** tab, enter a password for DSRM and click Next.



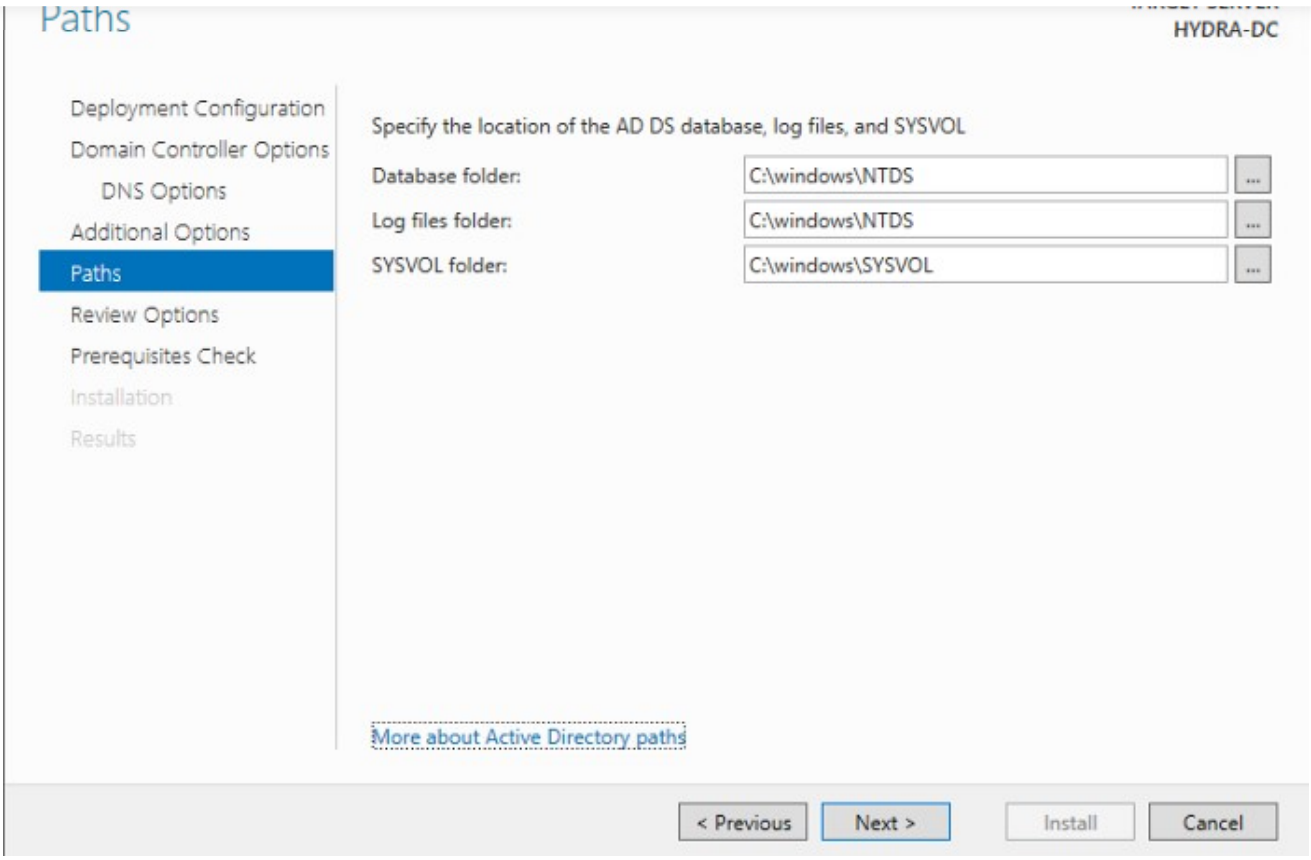
Click Next on **DNS Options** tab.



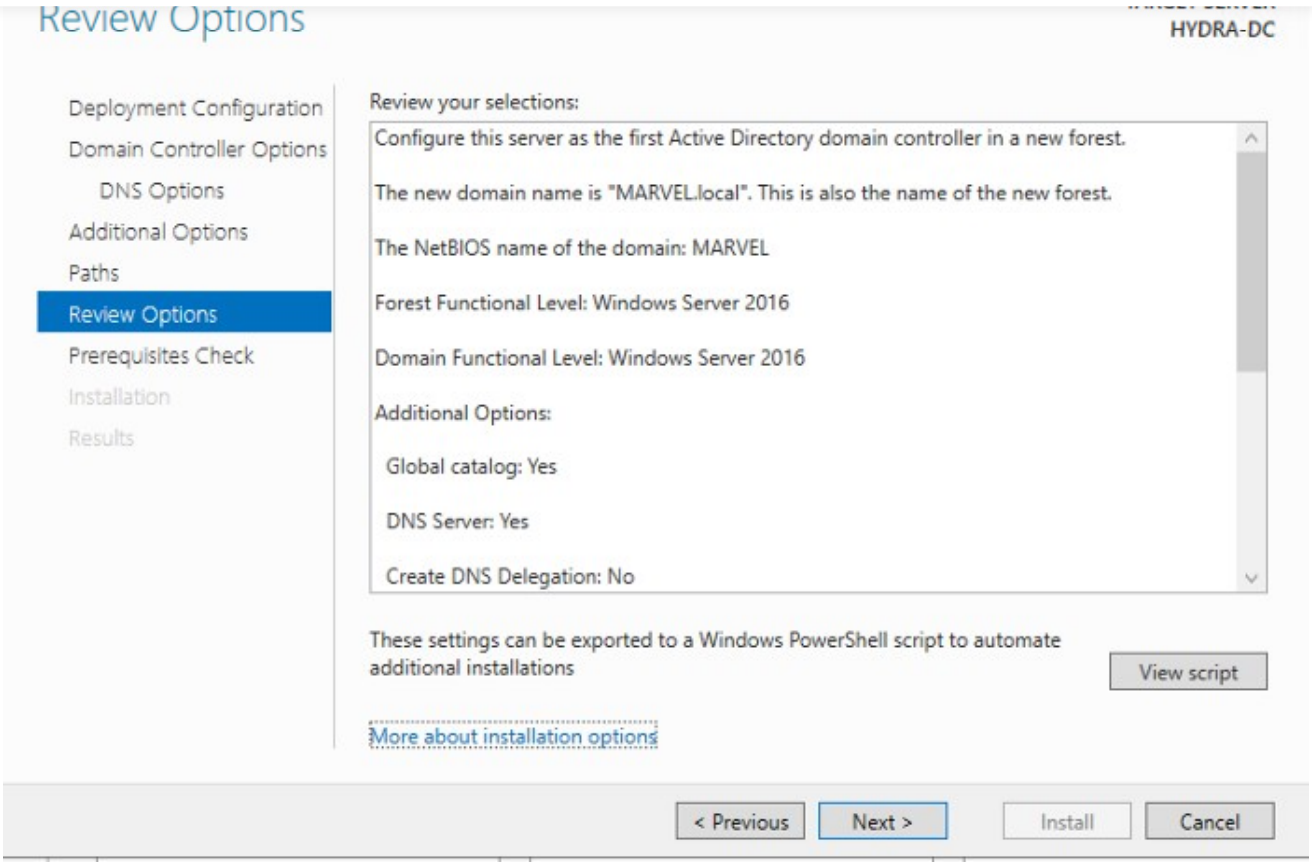
The NetBIOS domain name should populate automatically. Click Next.



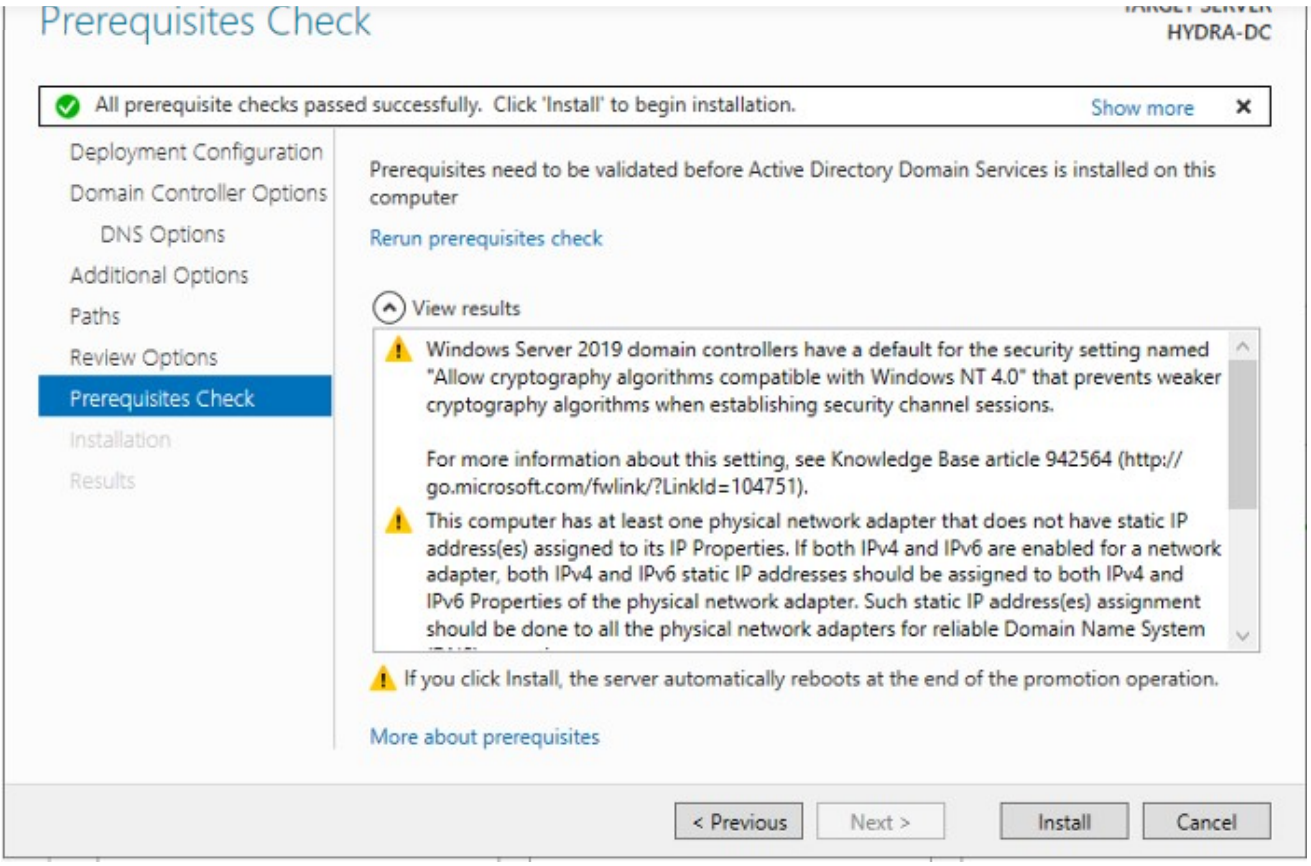
Accept all the defaults on the **Paths** tab and just click Next.



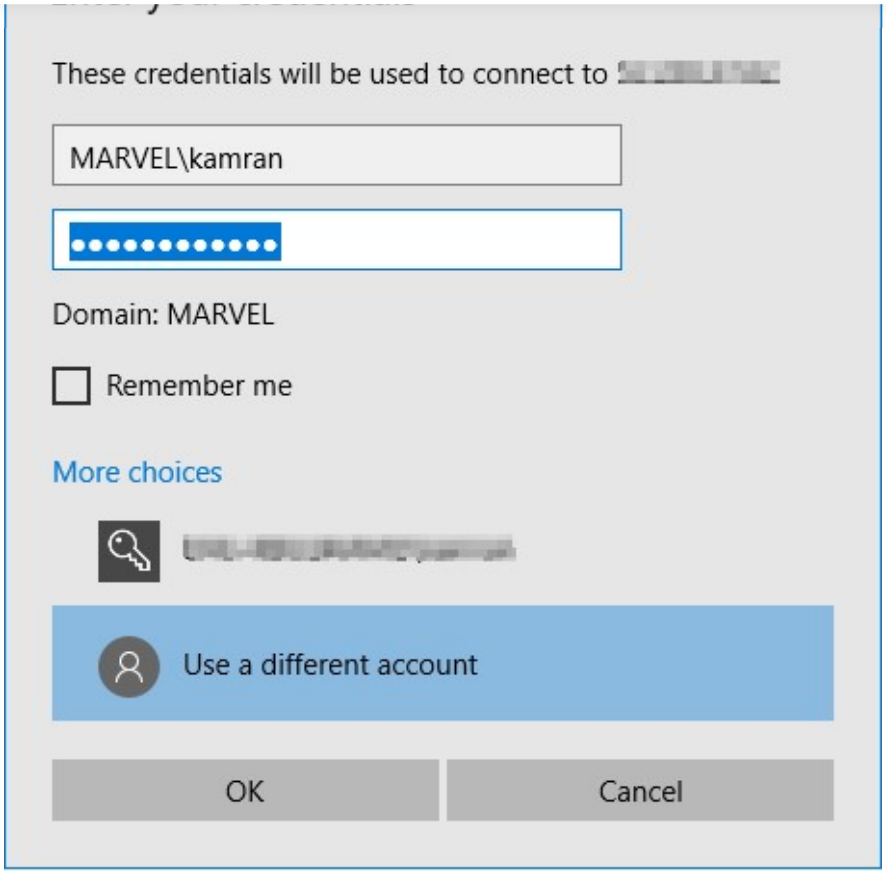
Review the options and click Next.



On the final step, click Install button.

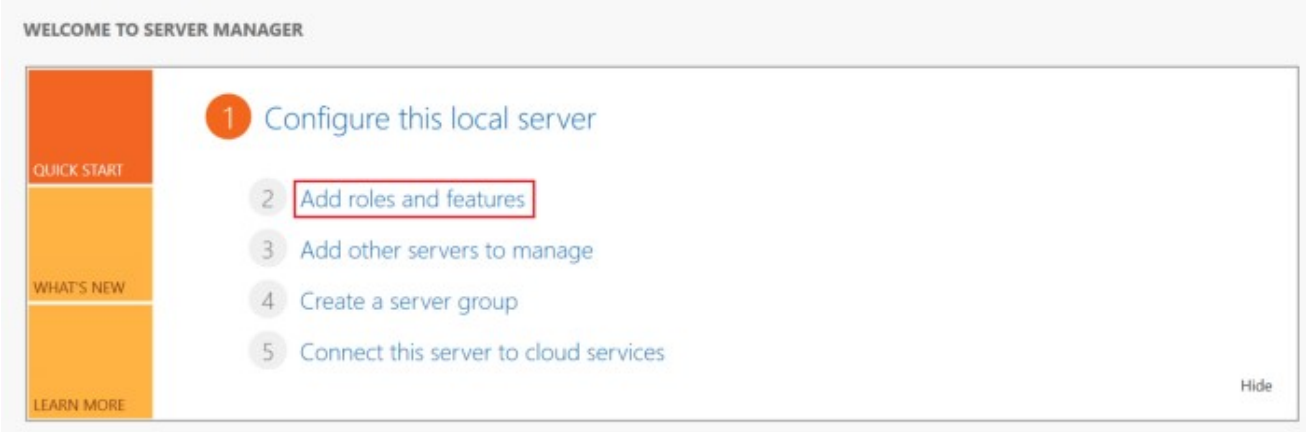


It will take a few minutes for this installation to complete. This will cause a reboot of the machine as well. After that, you can log in with the domain credentials.

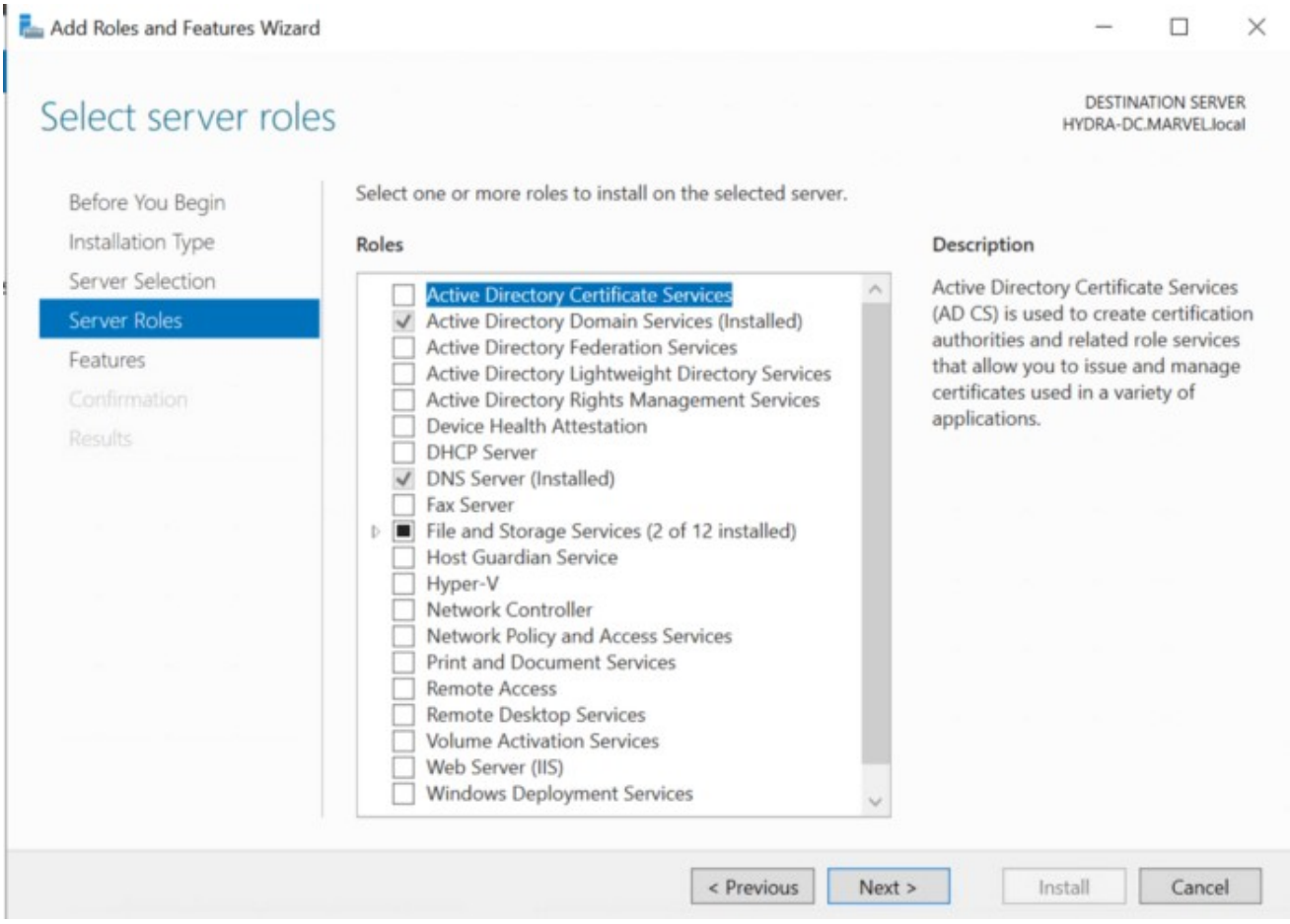


The desktop background image showing that we log in to the newly created MARVEL domain.

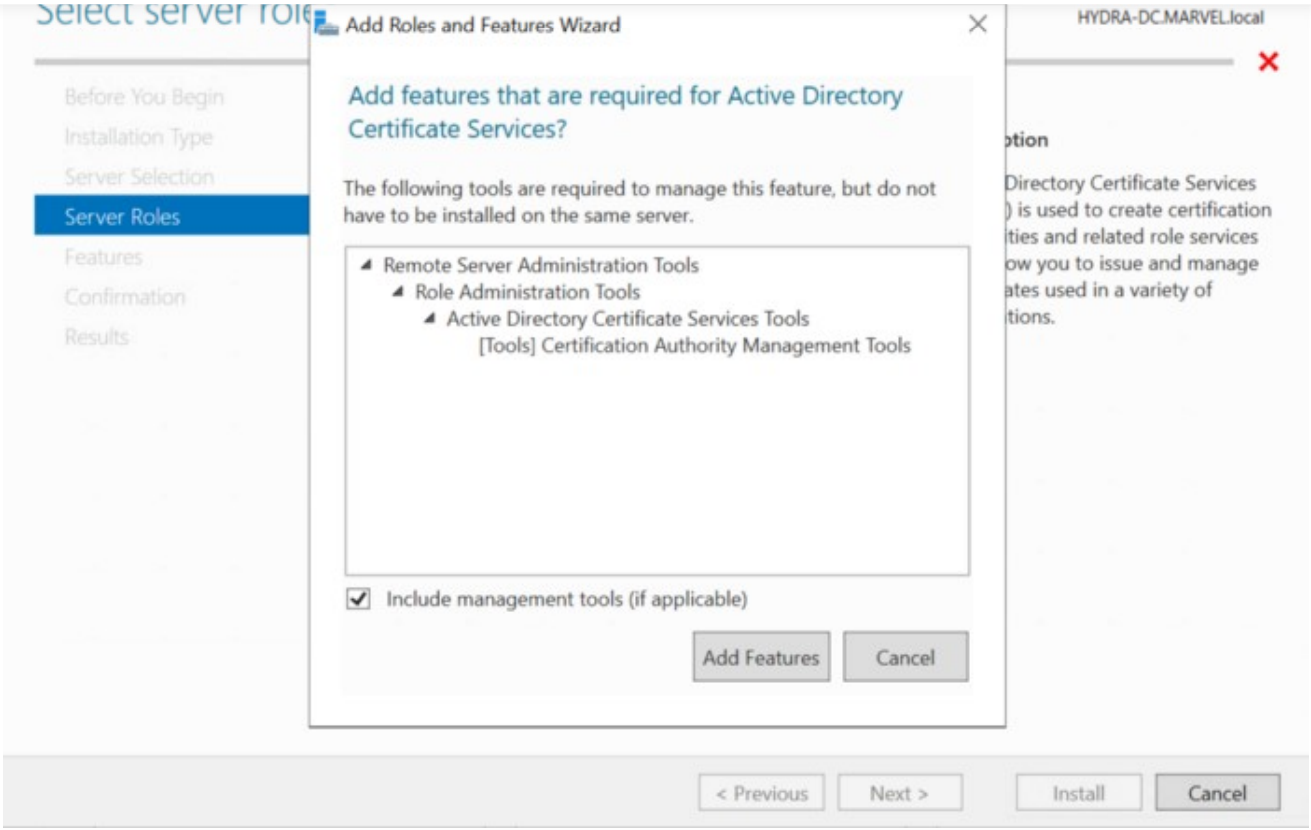
click on the **Add roles and features**.



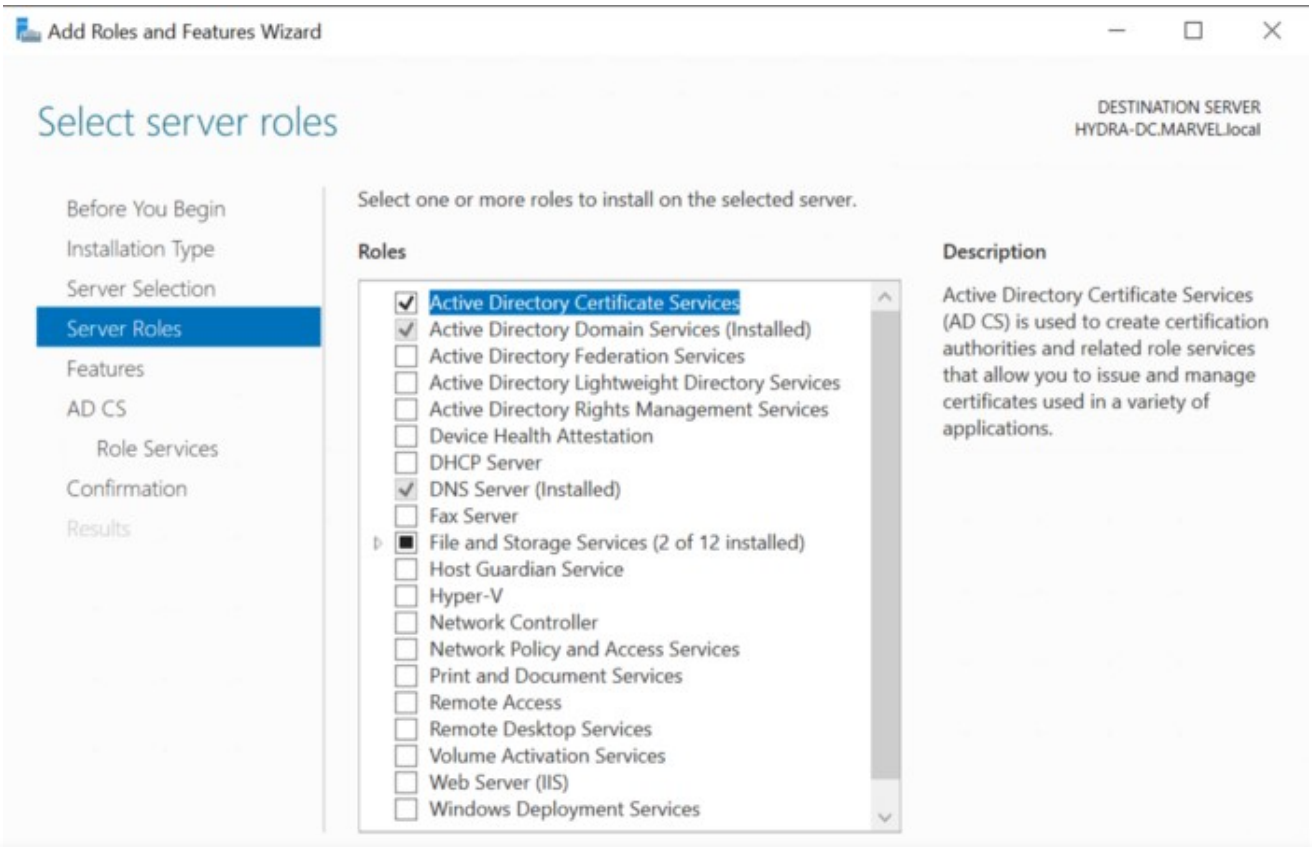
This will launch the **Add Roles and Features** Wizard that we used before too. Just keep clicking Next until you are on the Server Roles tab. Check the **Active Directory Certificate Services** (ADCS) here.

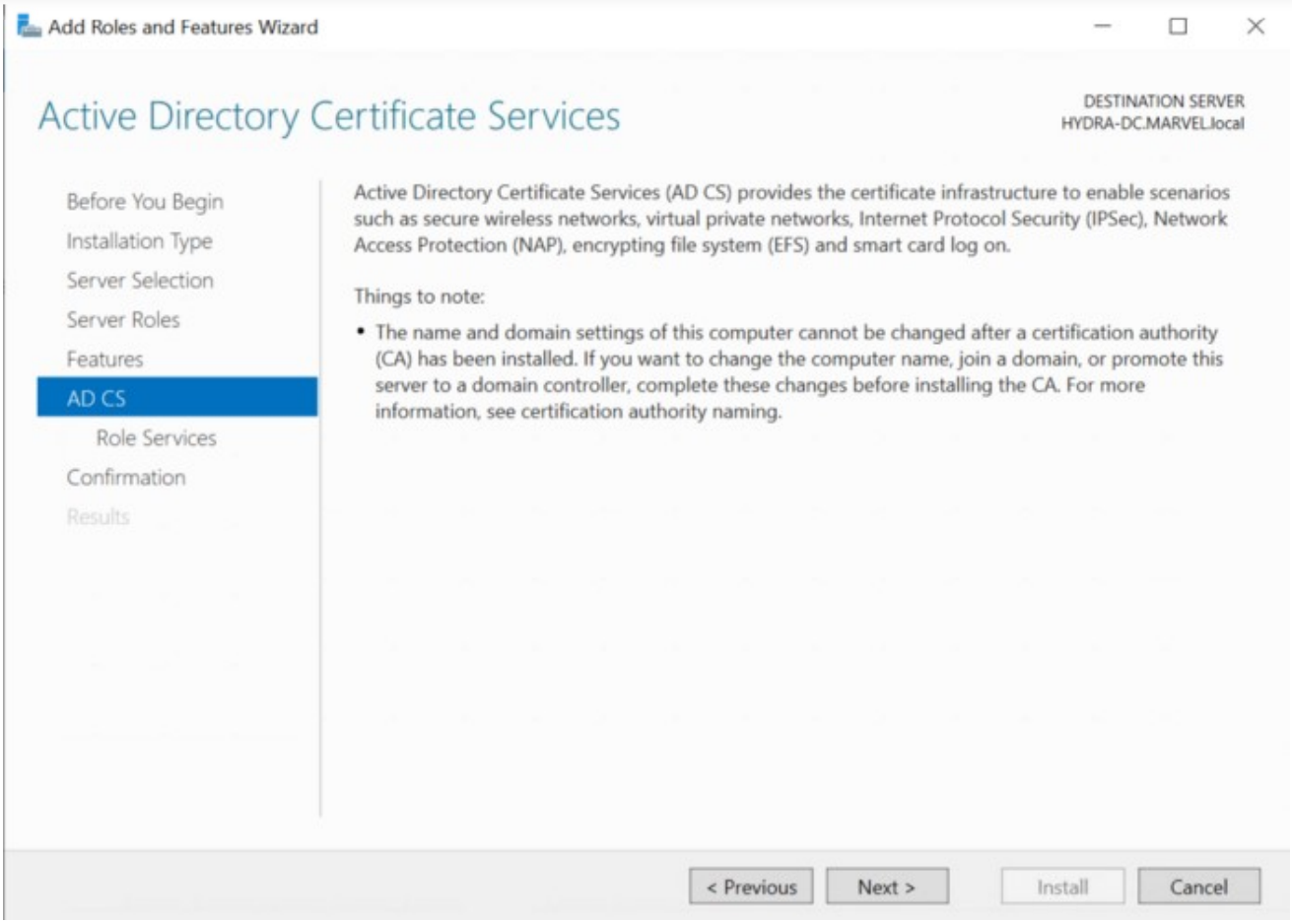


That will pop-up the following dialog with the information about the required features

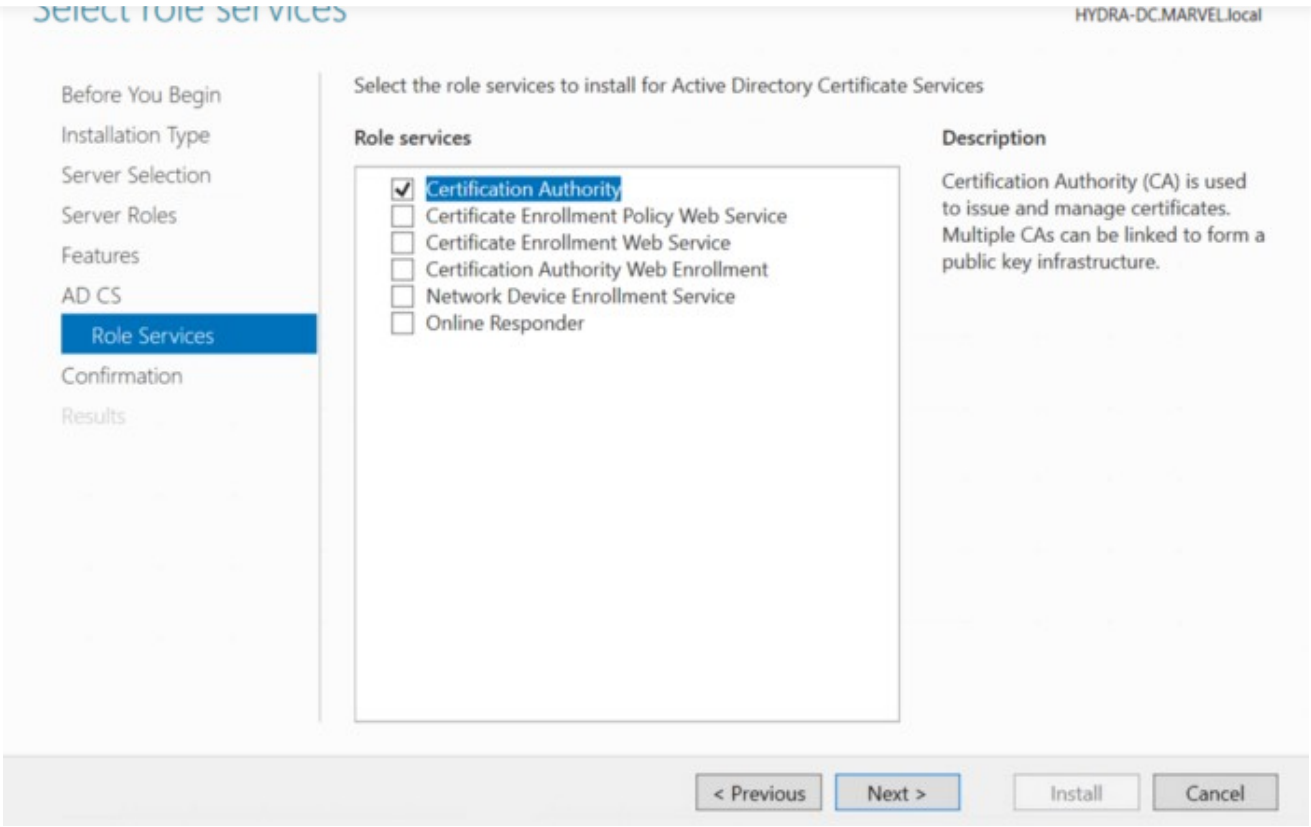


Click on the Next button.

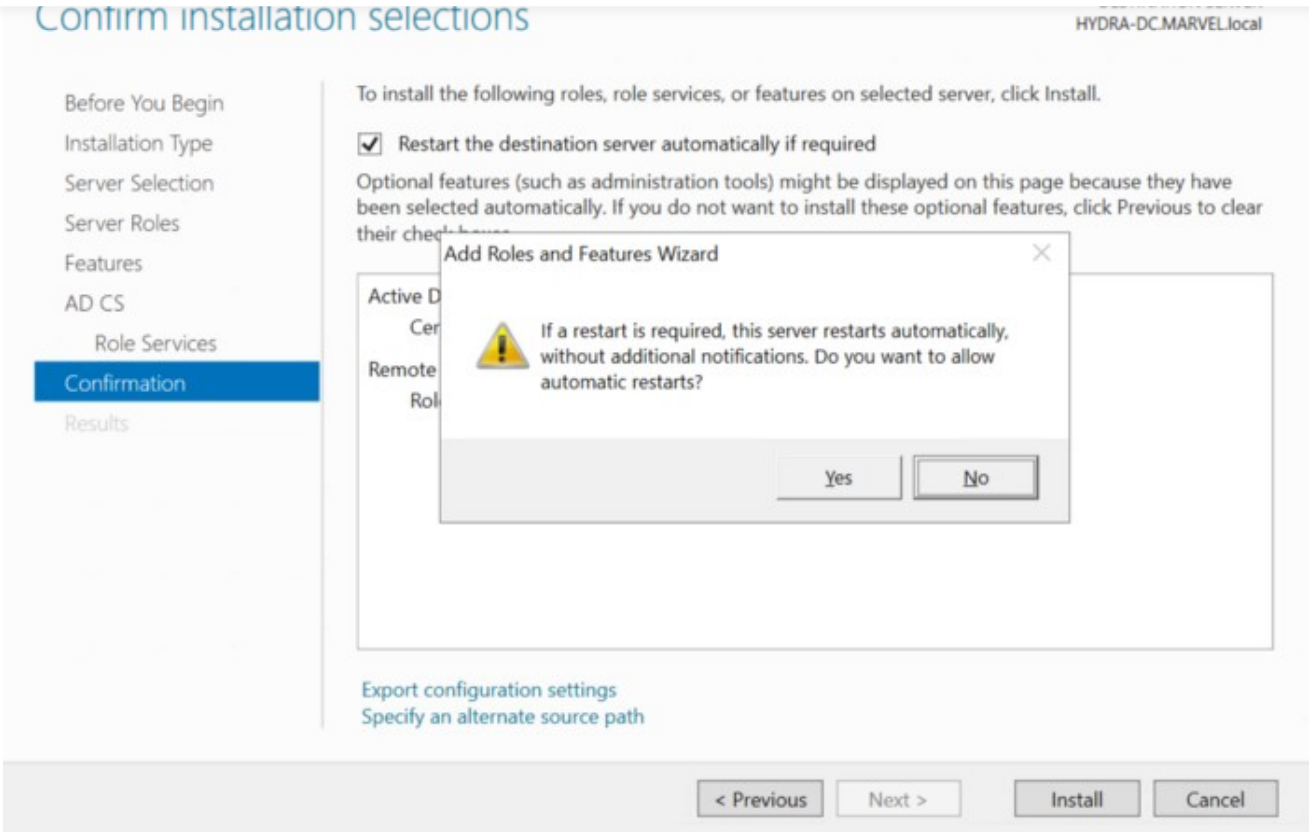




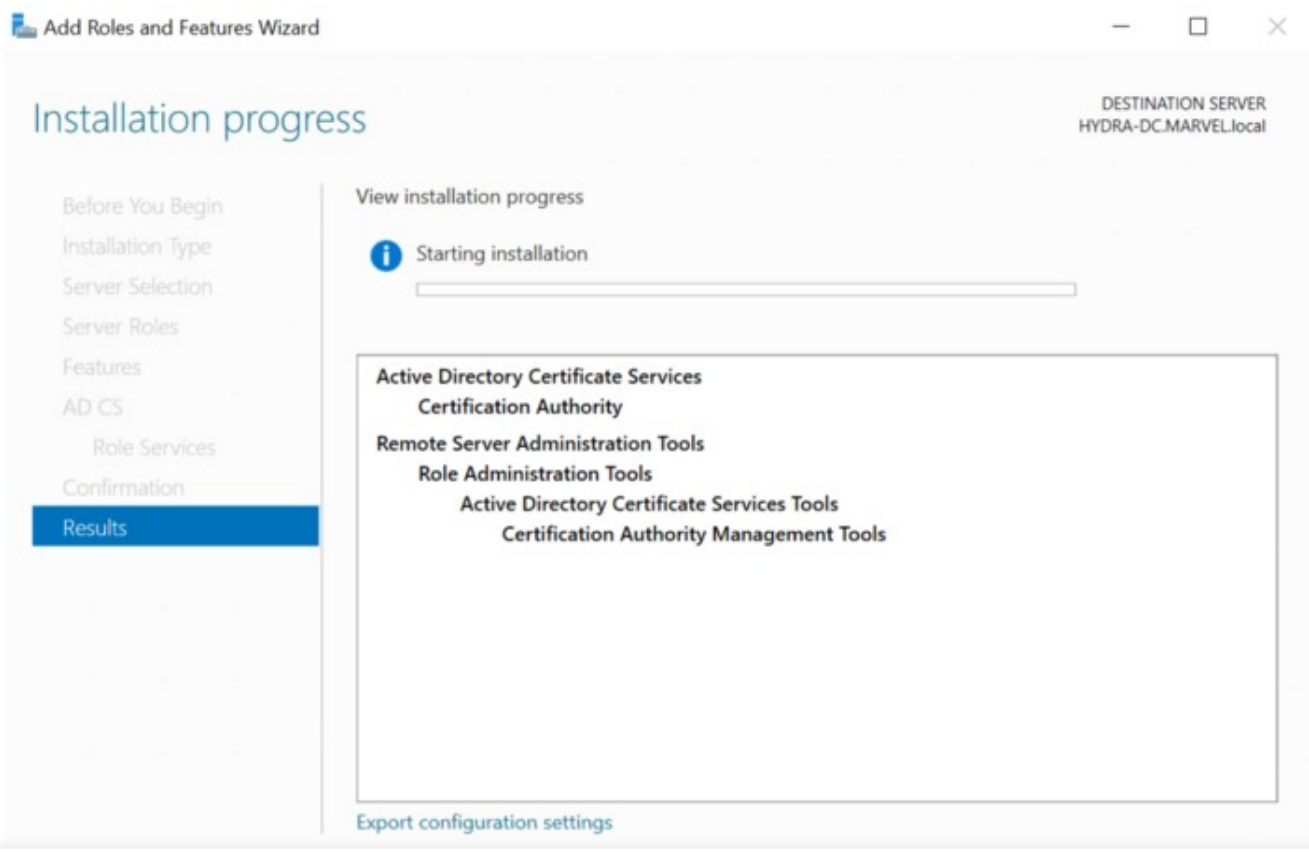
Check the **Certification Authority** checkbox and click Next.

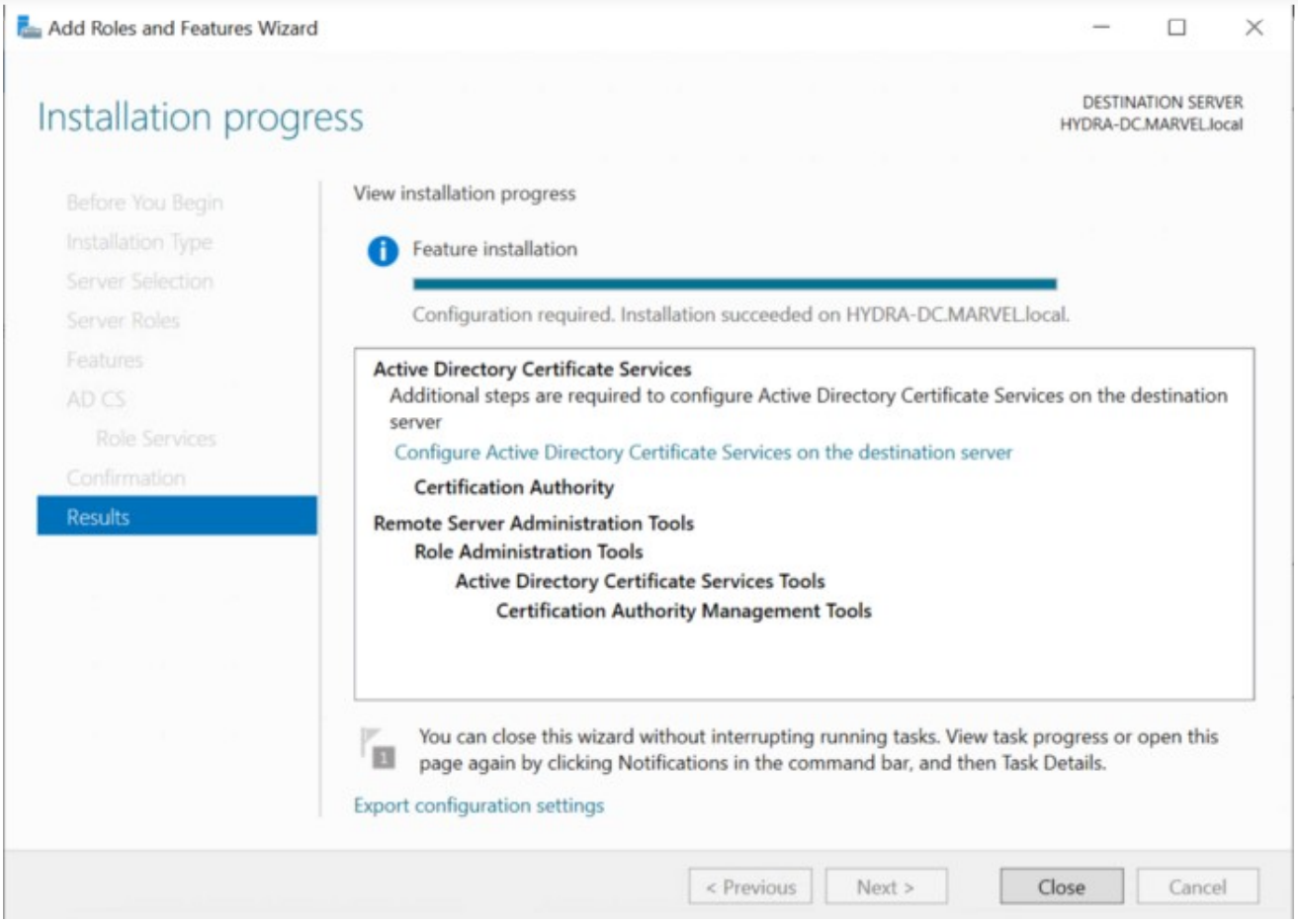


On the **Confirmation** tab, check the **Restart the destination server automatically if required** checkbox. This will prompt a confirmation dialog. Select Yes and then click on Next.

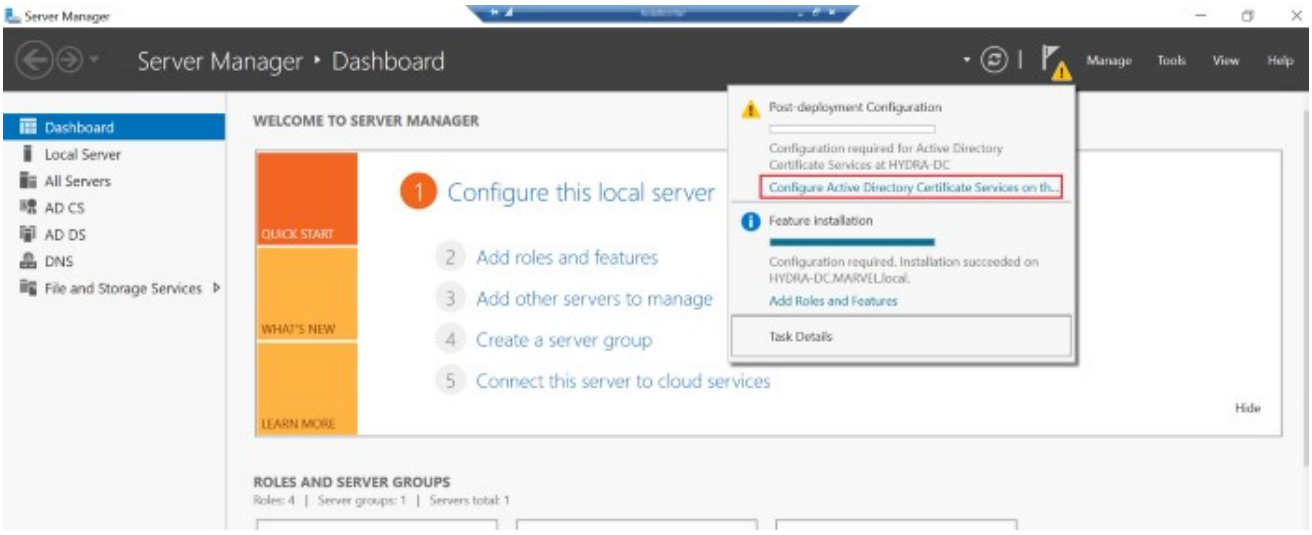


This will start the installation process for ADCS and the required components.

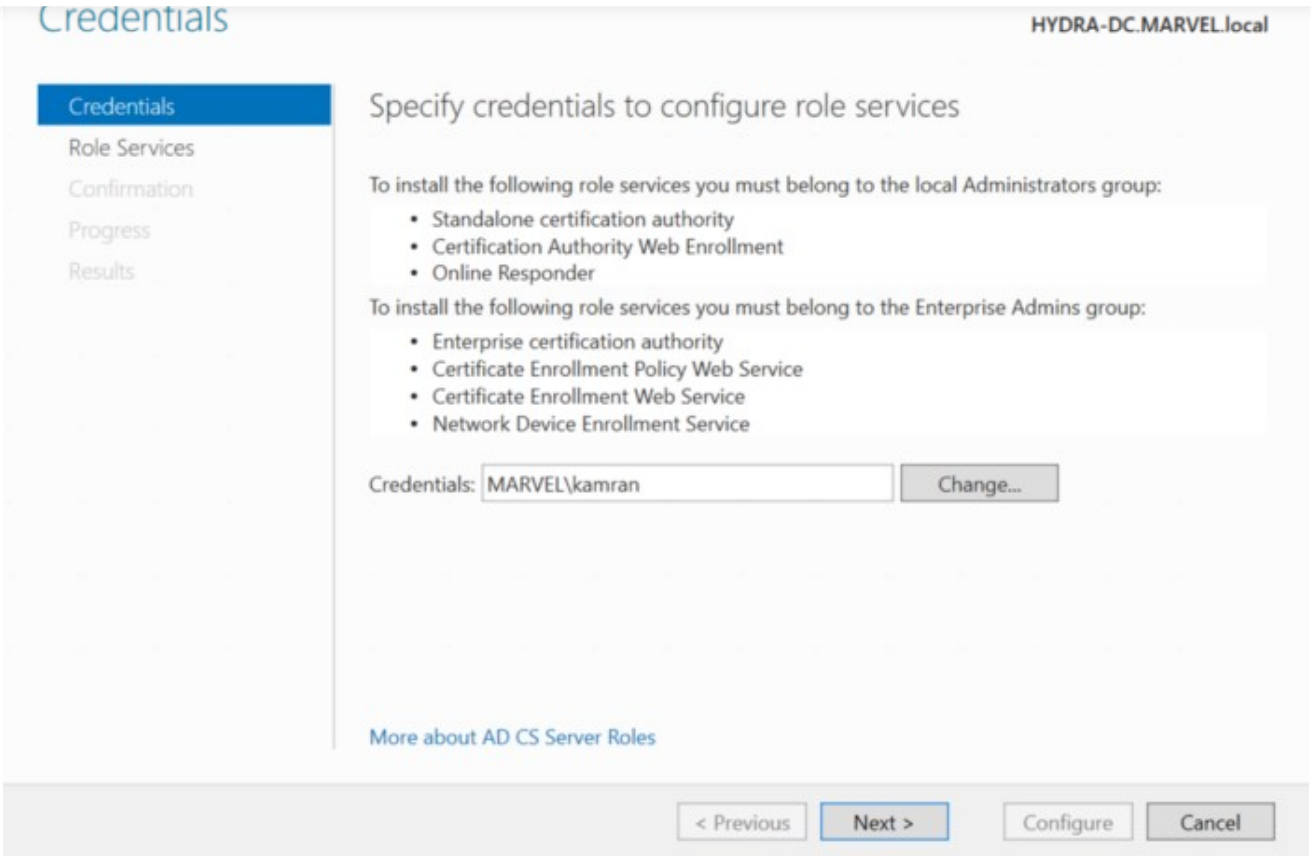




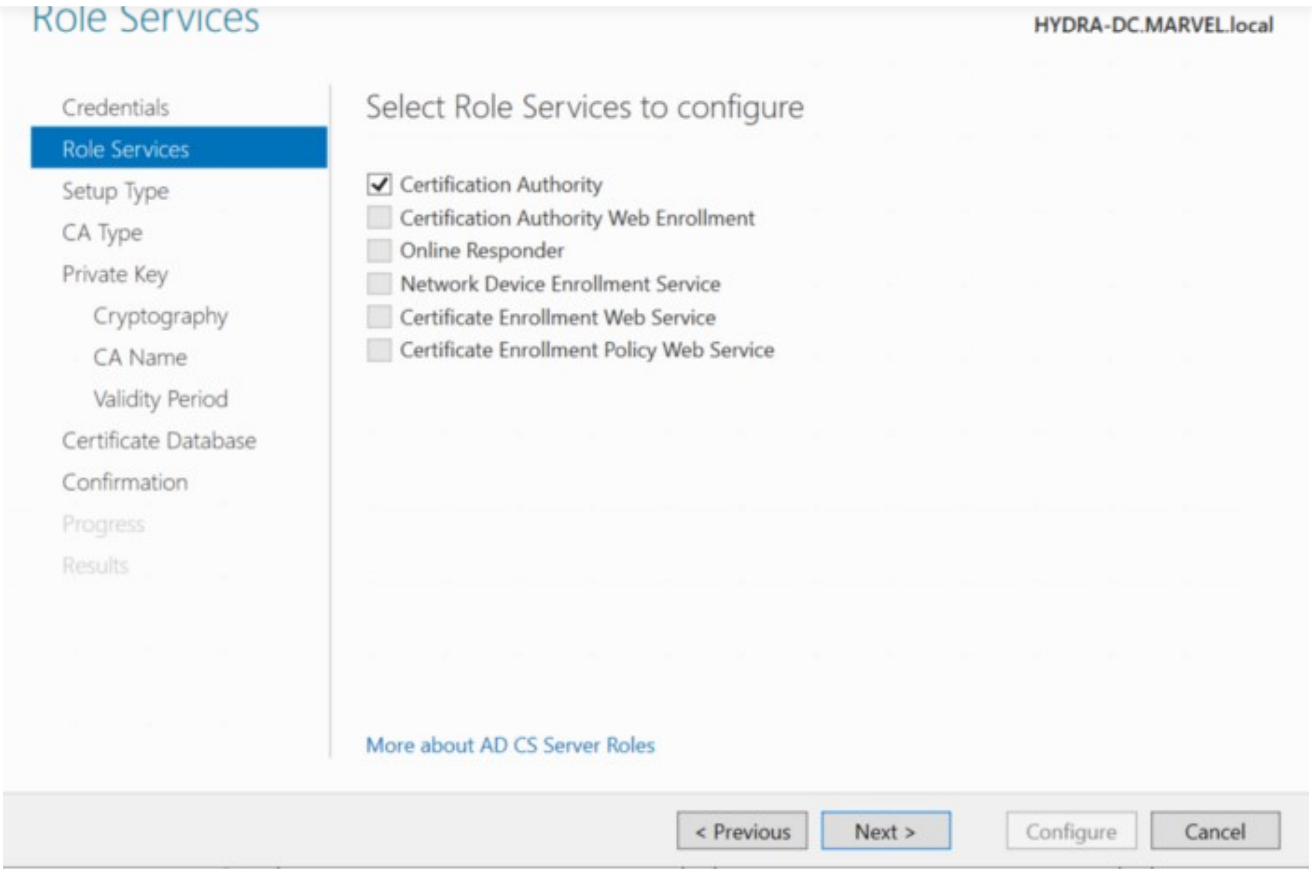
At this point, you will see a warning flag. Click on that flag and then click on the link for **Configure Active Directory Certificate Services on the destination server**.



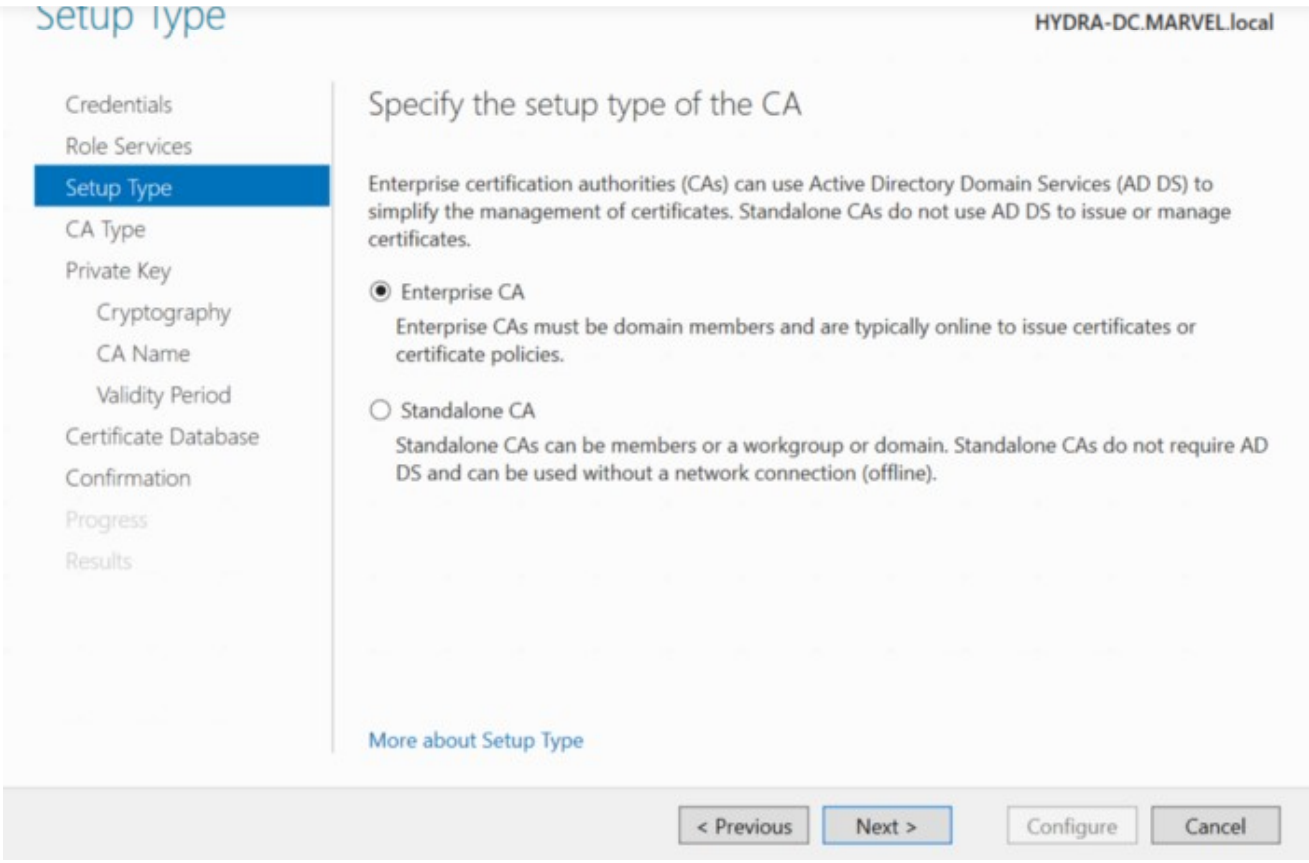
This will launch the **AD CS Configuration** wizard. Click next on the **Credentials** tab.



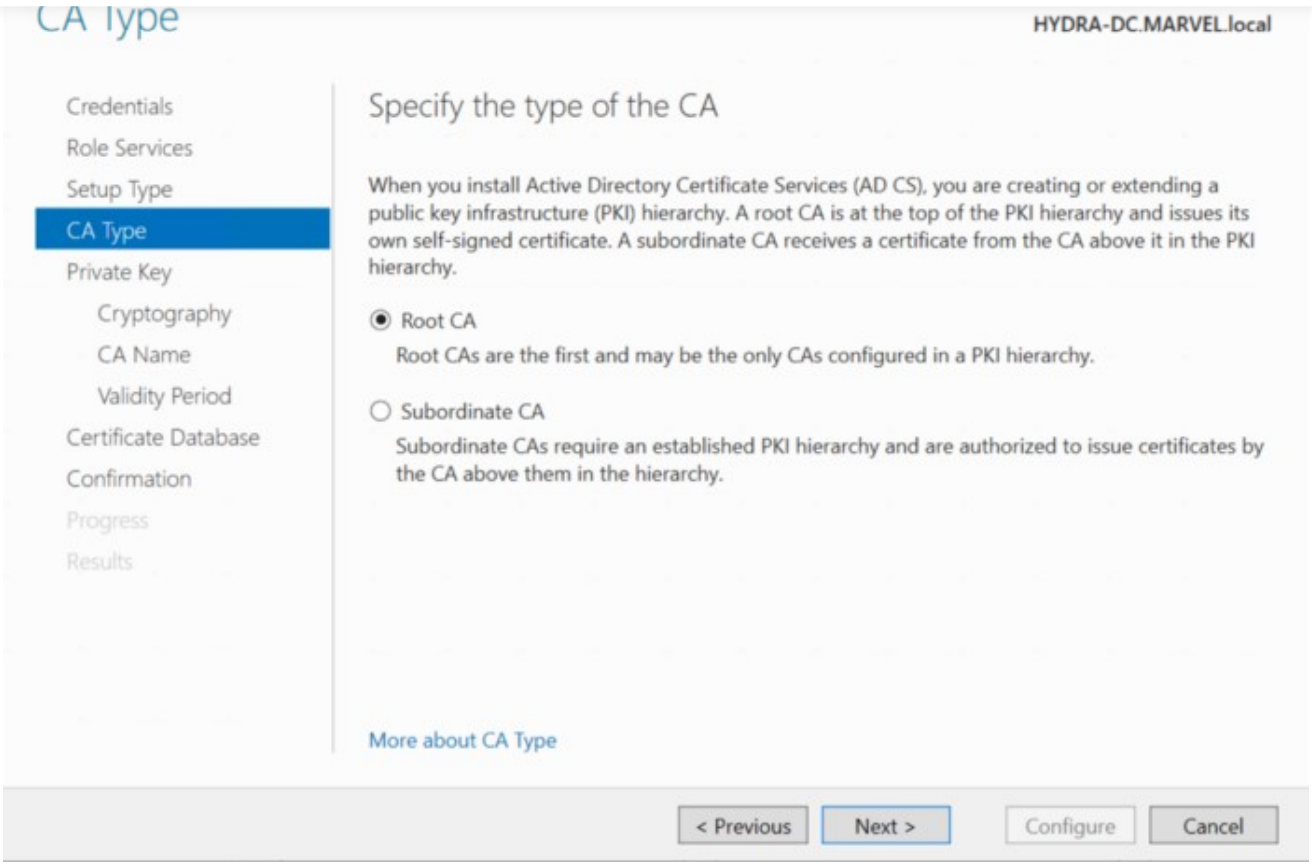
On the **Role Services** tab, check the **Certification Authority** check box and click Next.



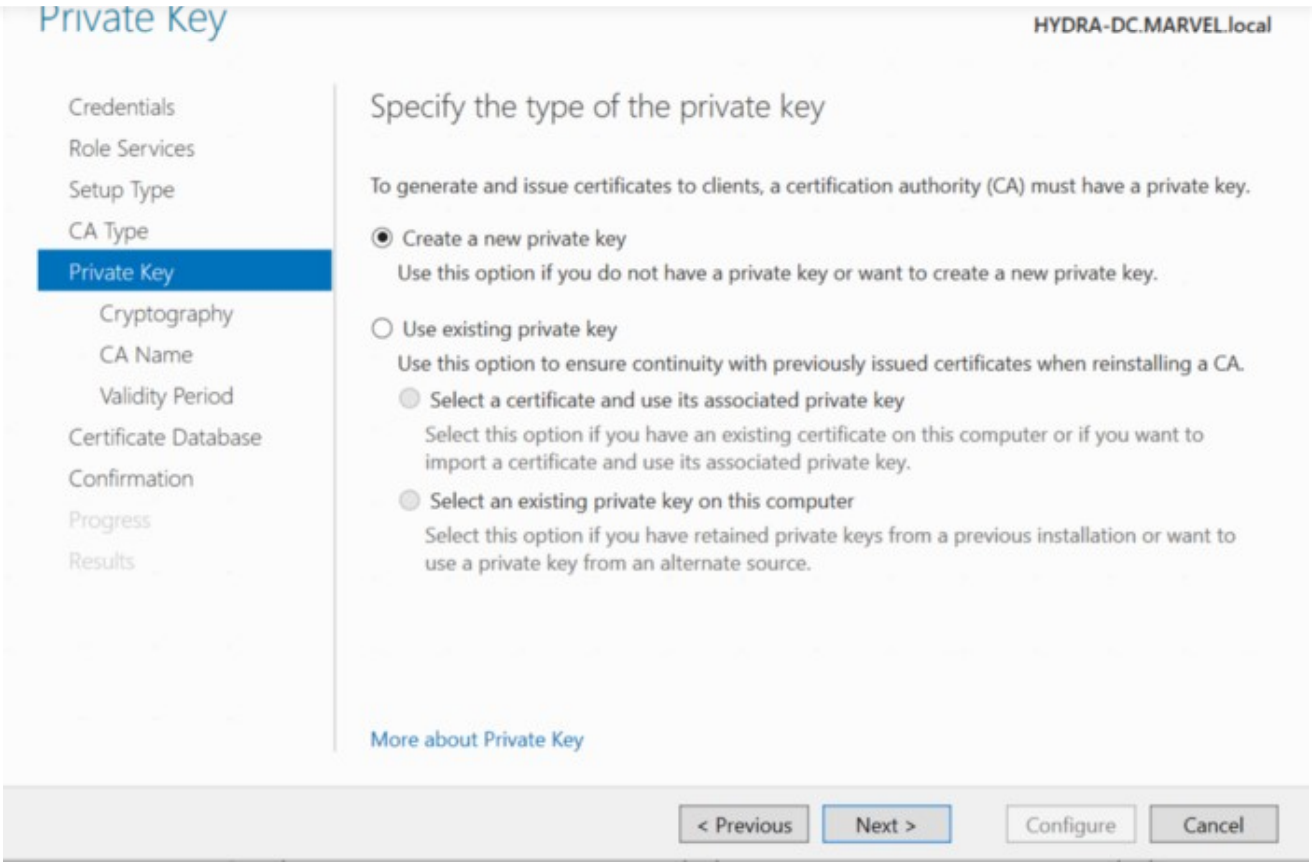
Make sure to select **Enterprise CA** on the **Setup Type** tab and click Next.



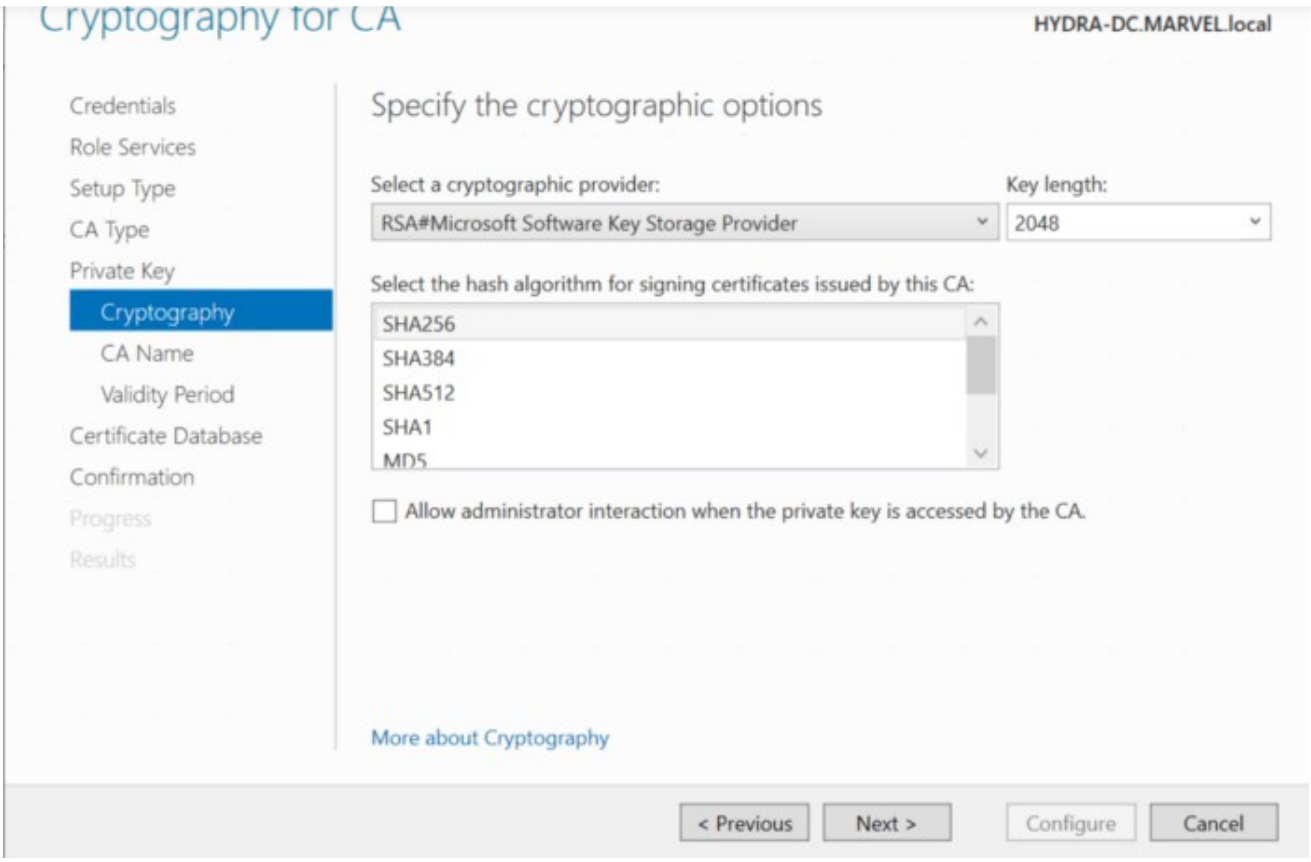
Make sure to select **Root CA** on the **CA Type** tab and click Next.



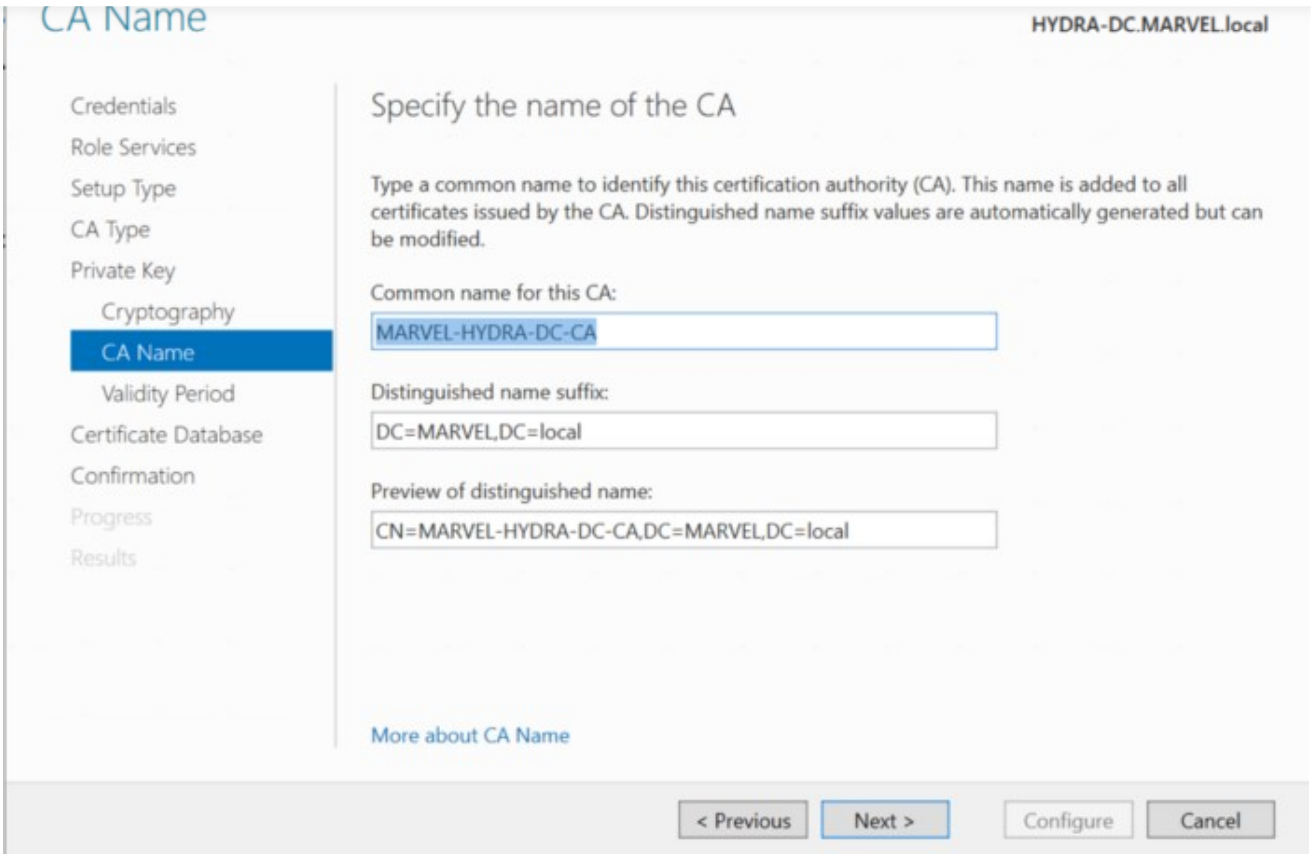
Select **Create a new private key** on the **Private Key** tab and click Next.



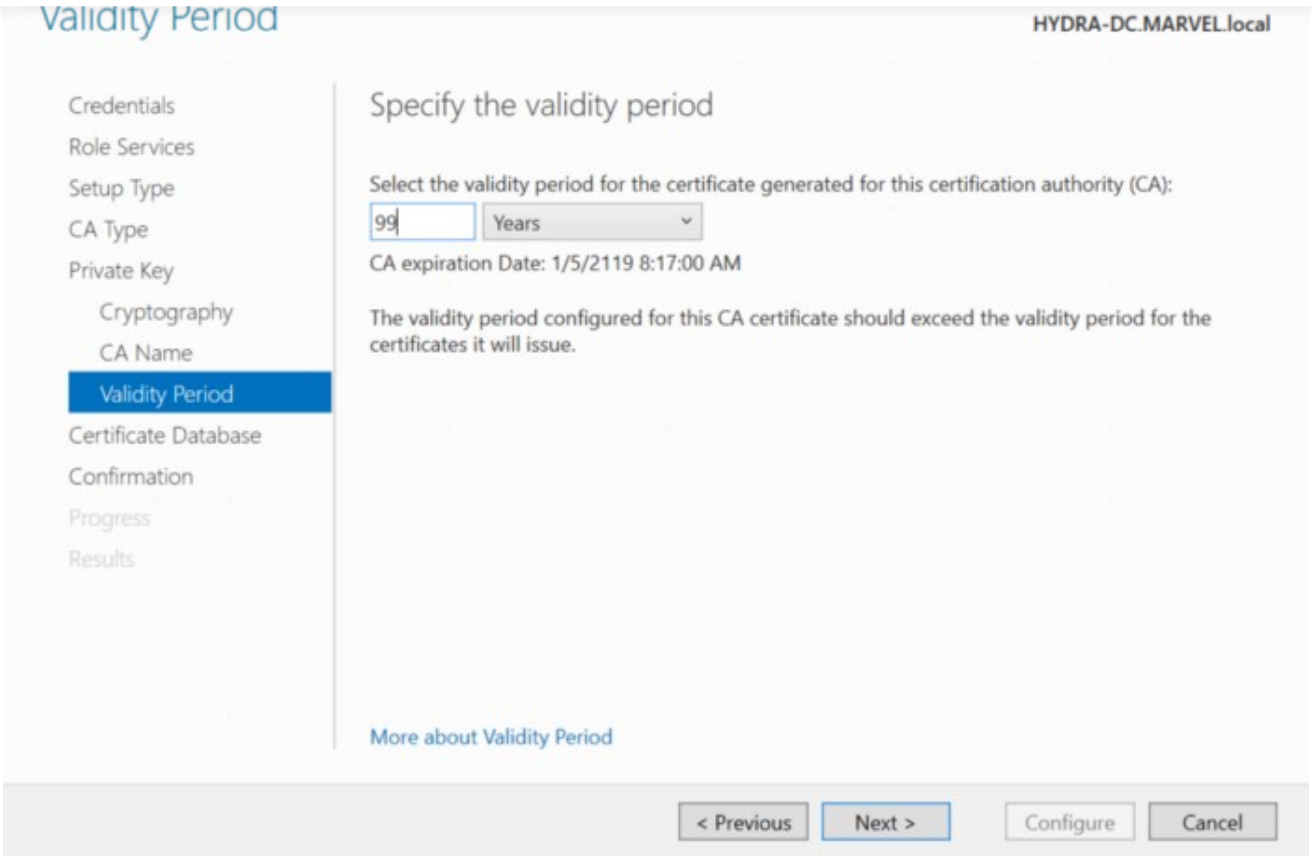
Stick with the default options on the **Cryptography** tab and click Next.



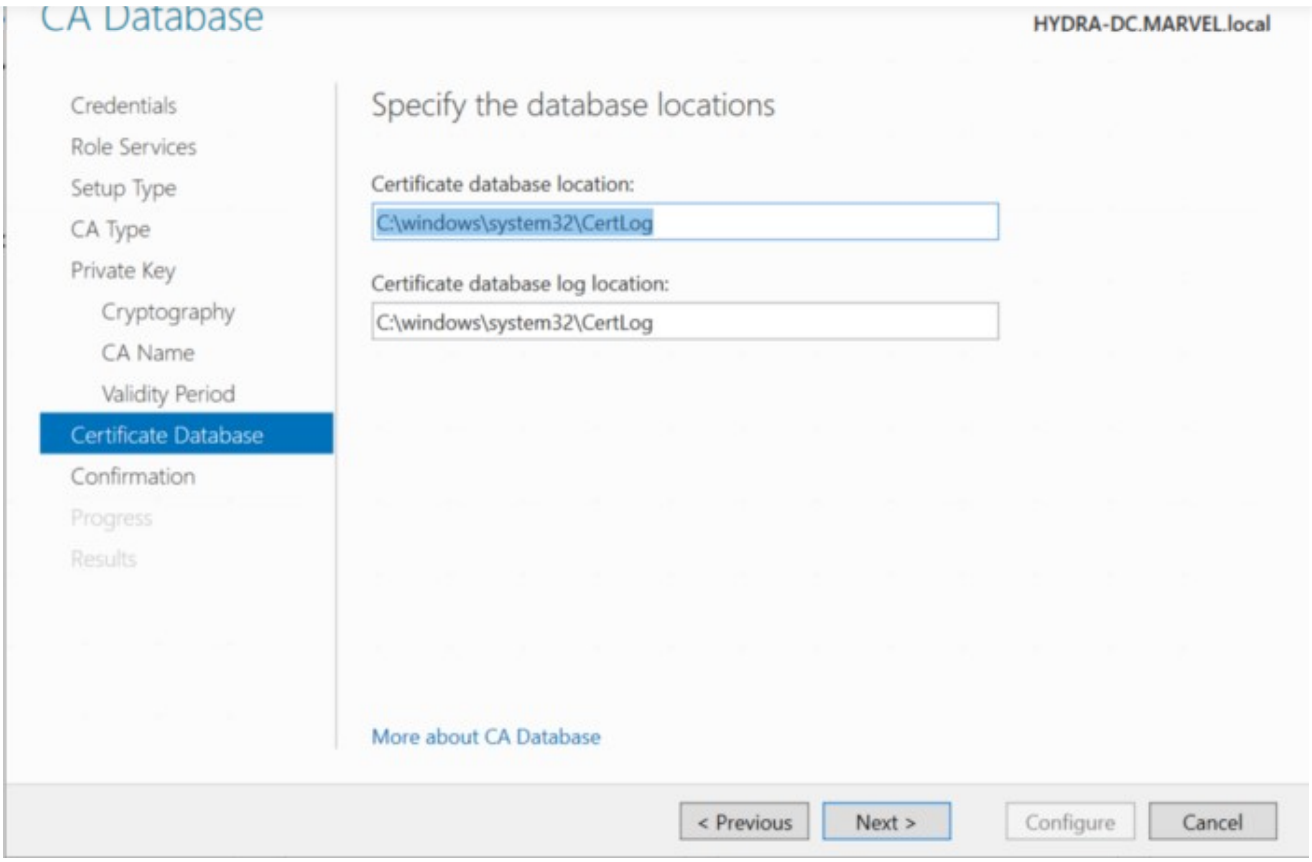
Stick with all the default names of **CA Name** tab and click Next.



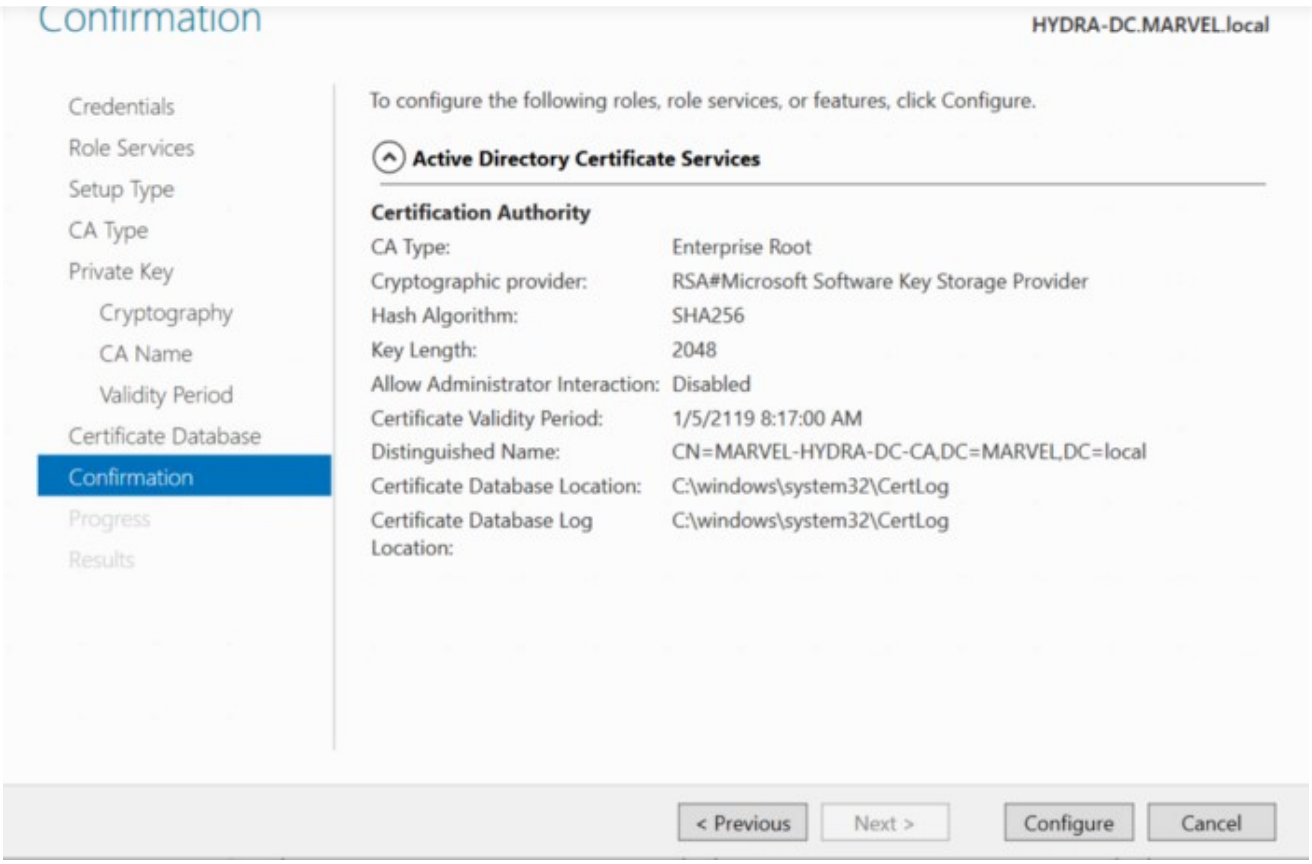
On the **Validity Period**, change it **99** years and click Next.



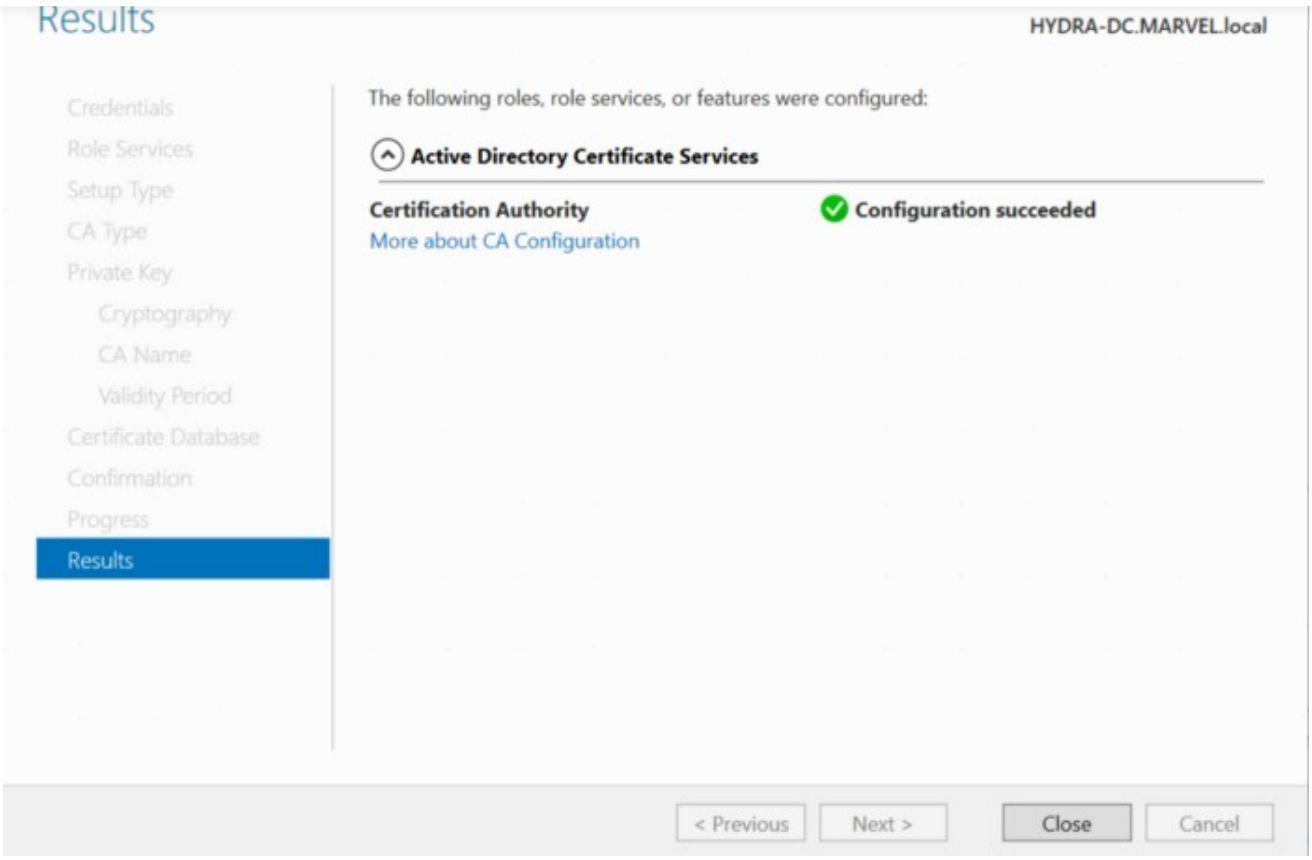
Stick with the default database and log location and click Next.



Click the Configure button on the **Confirmation** tab.



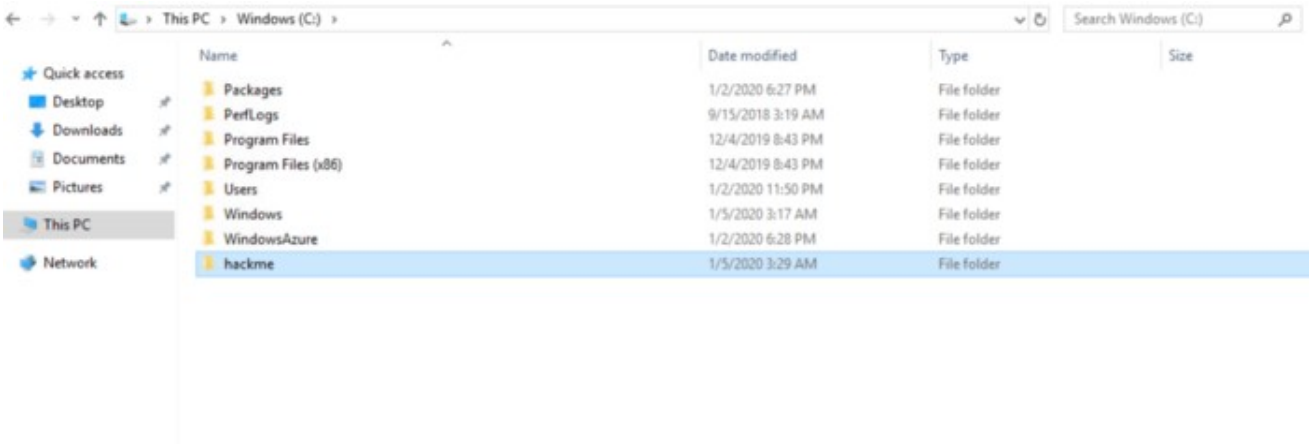
Shortly after you will see the message about Configuration succeeded. You can close this dialog now.



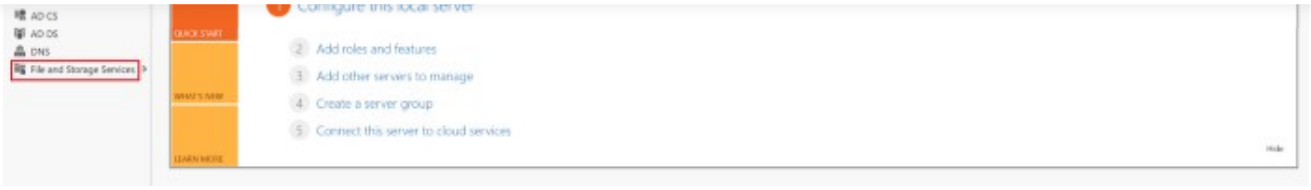
Restart the VM now so the changes take effect.

Setting up a Share

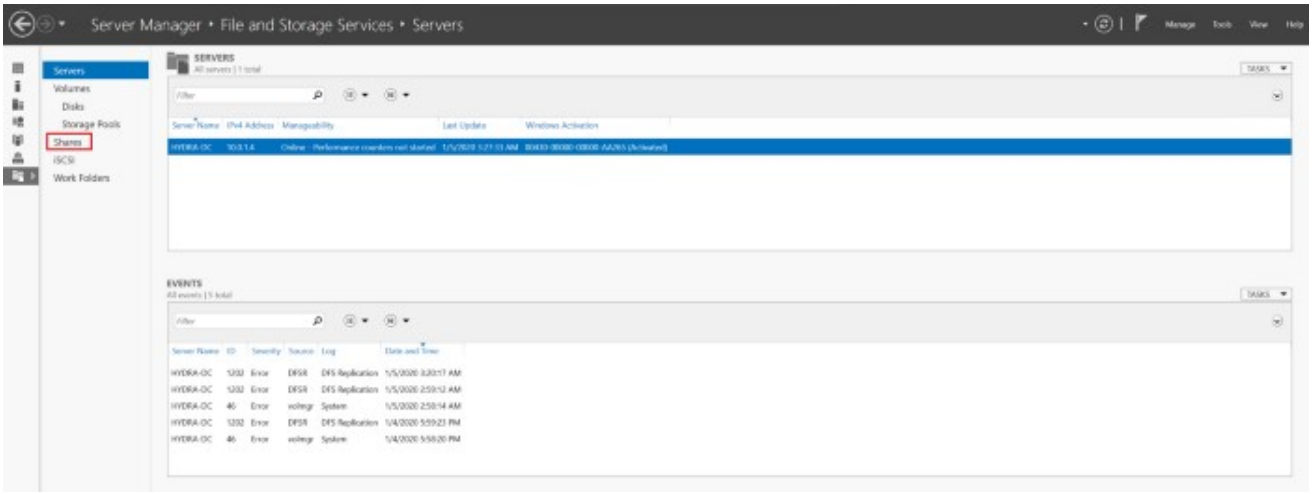
Create a folder **hackme** on the C drive.



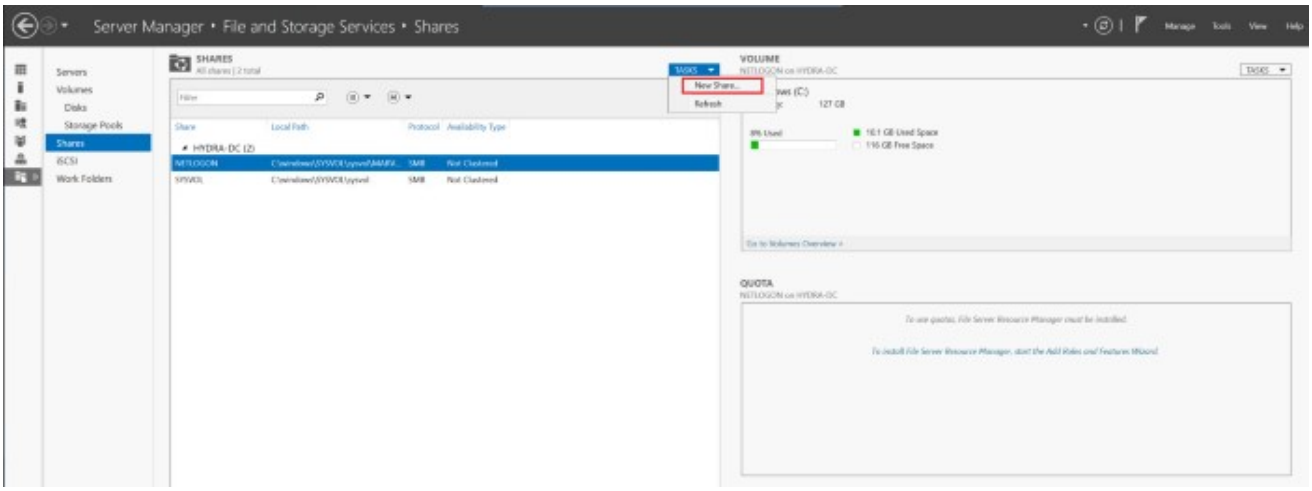
Launch the Server Manager and click on the **File and Storage** Services tab.



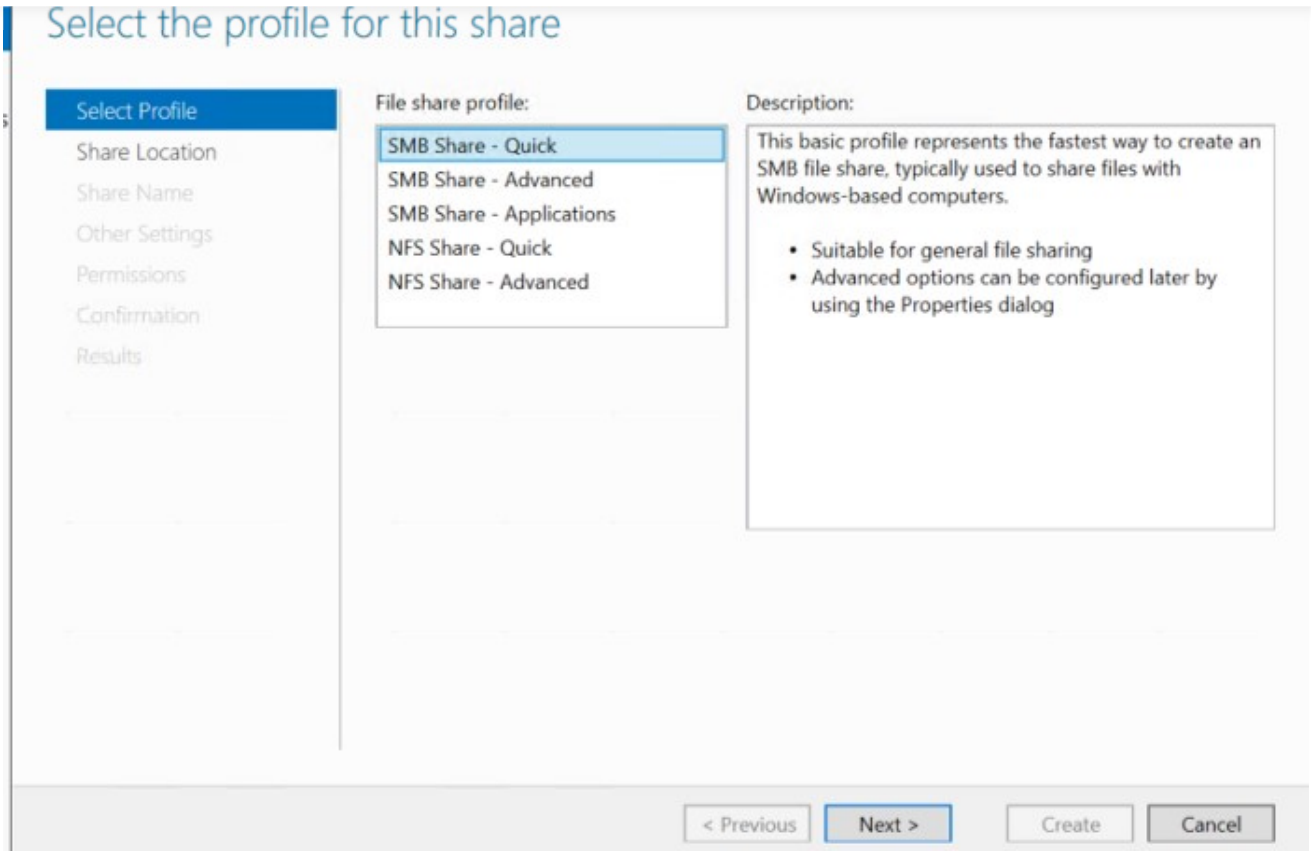
Click on the **Shares** as shown below.



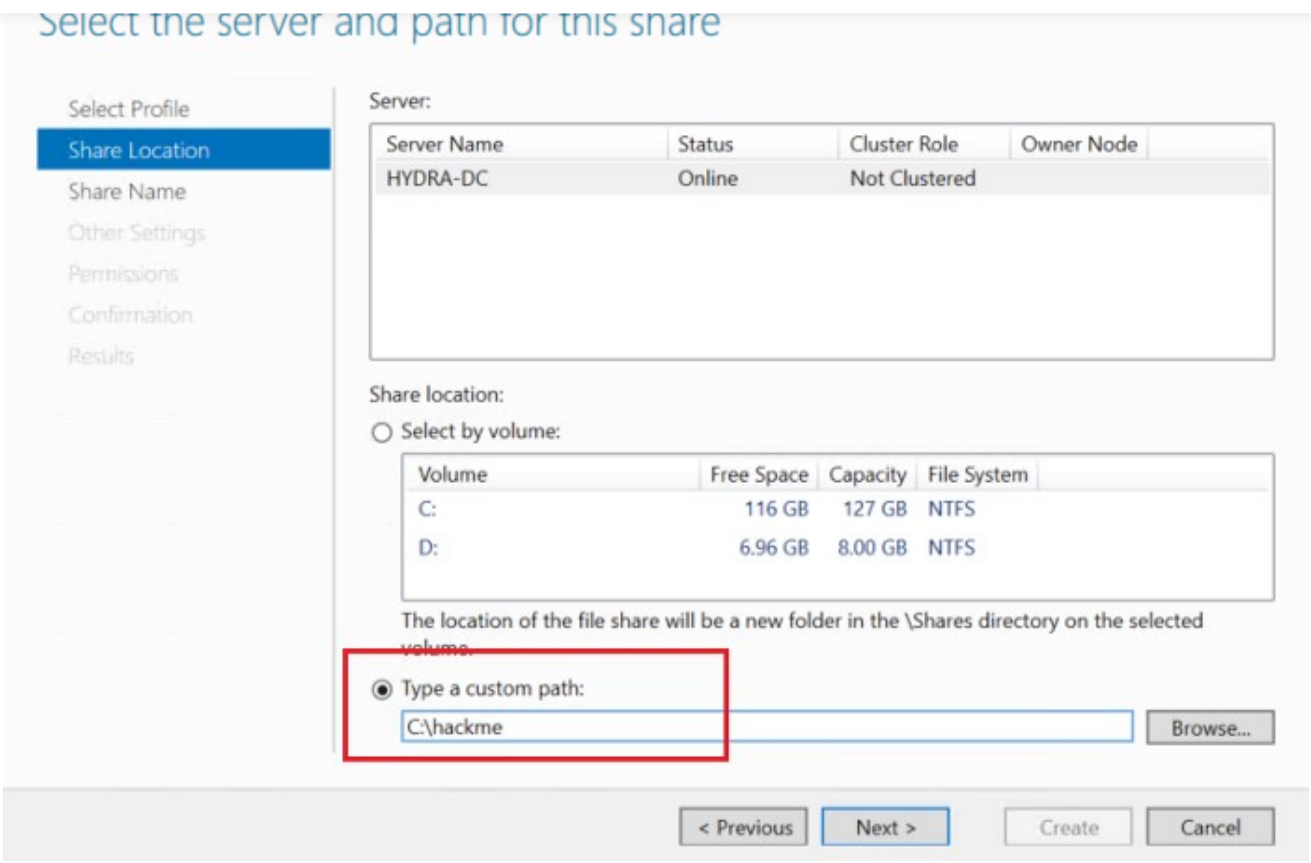
Click on the **New Share** menu item under **Tasks** as shown below.



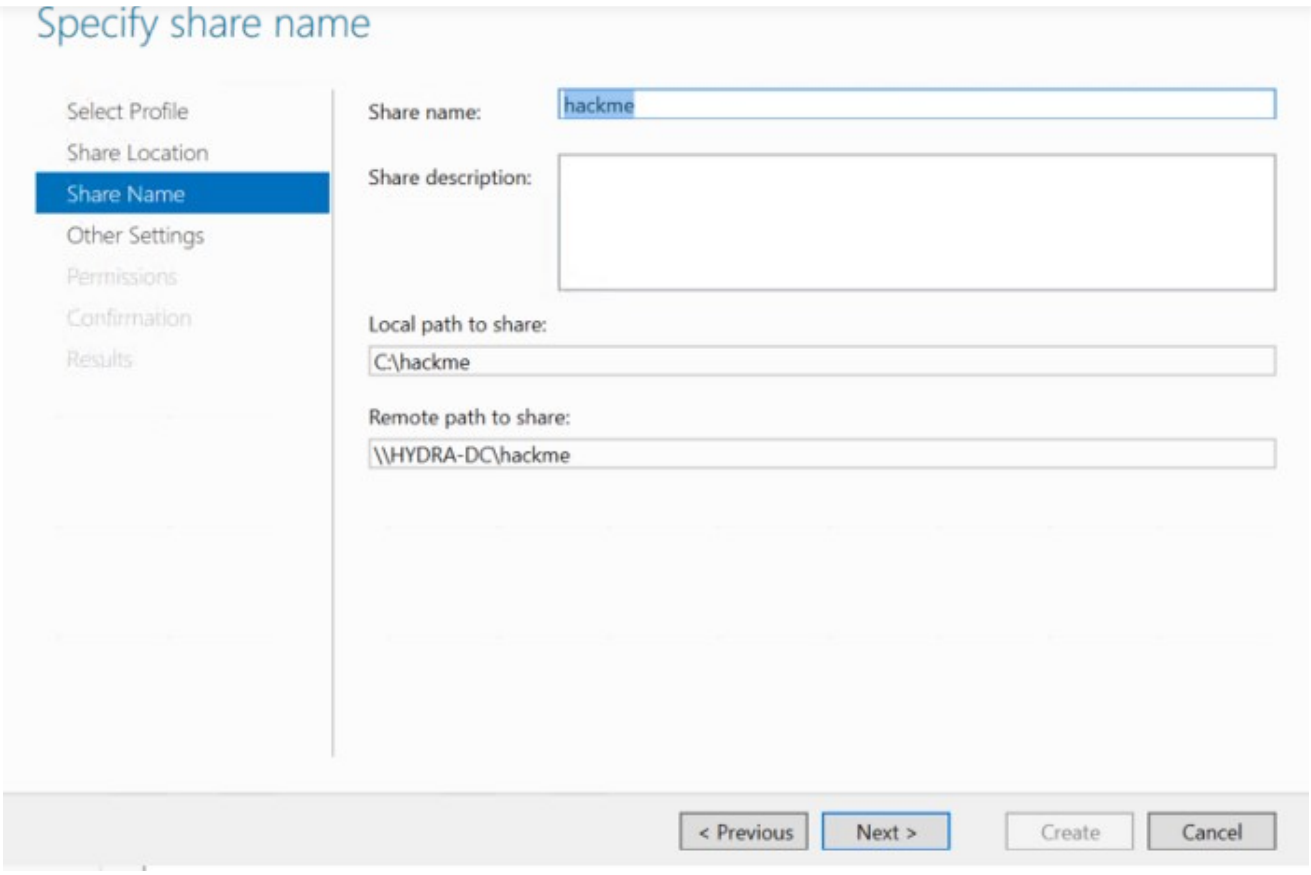
This will launch the **New Share Wizard**. Make sure **SMB Share — Quick** File share profile is selected and click Next.



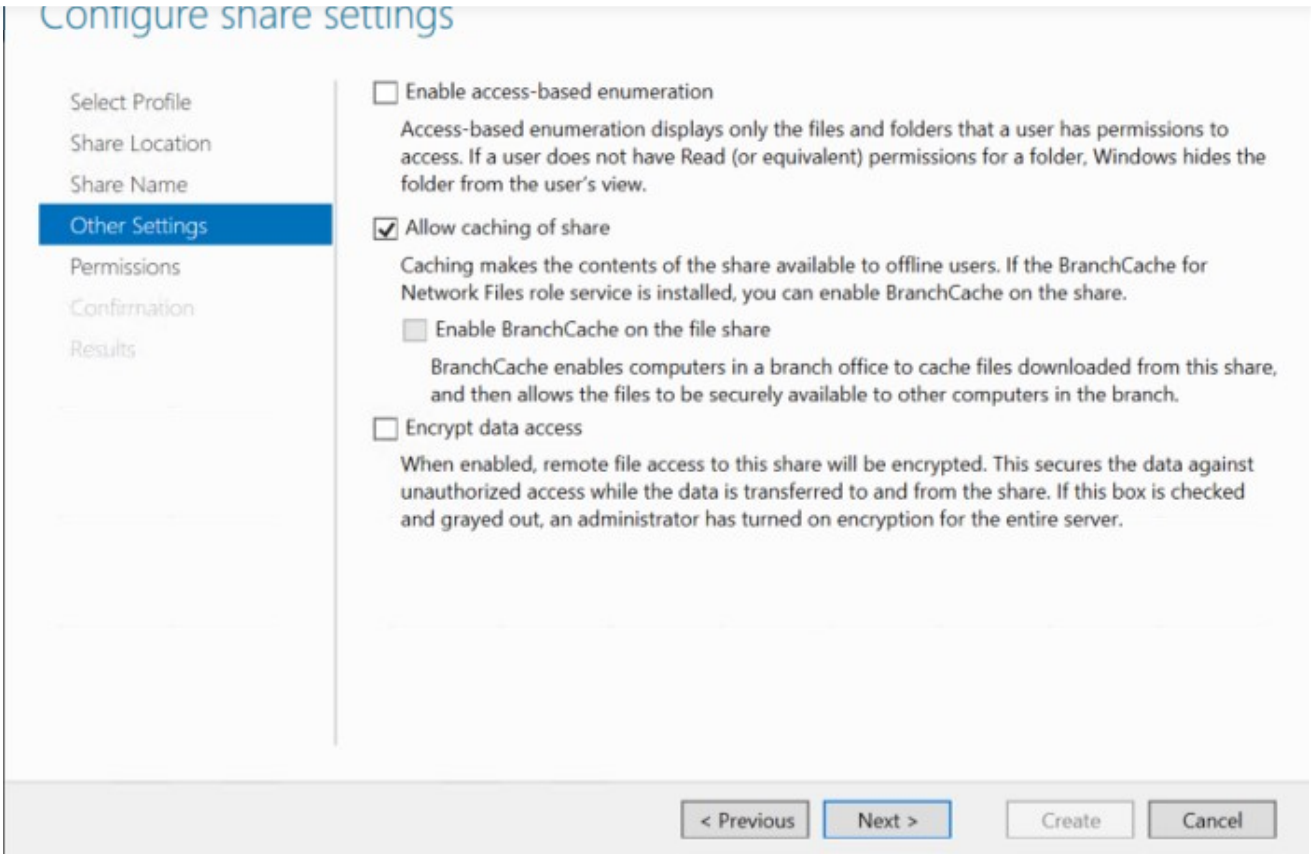
Select **Type a Custom path** option and enter **c:\hackme** folder path and click Next.



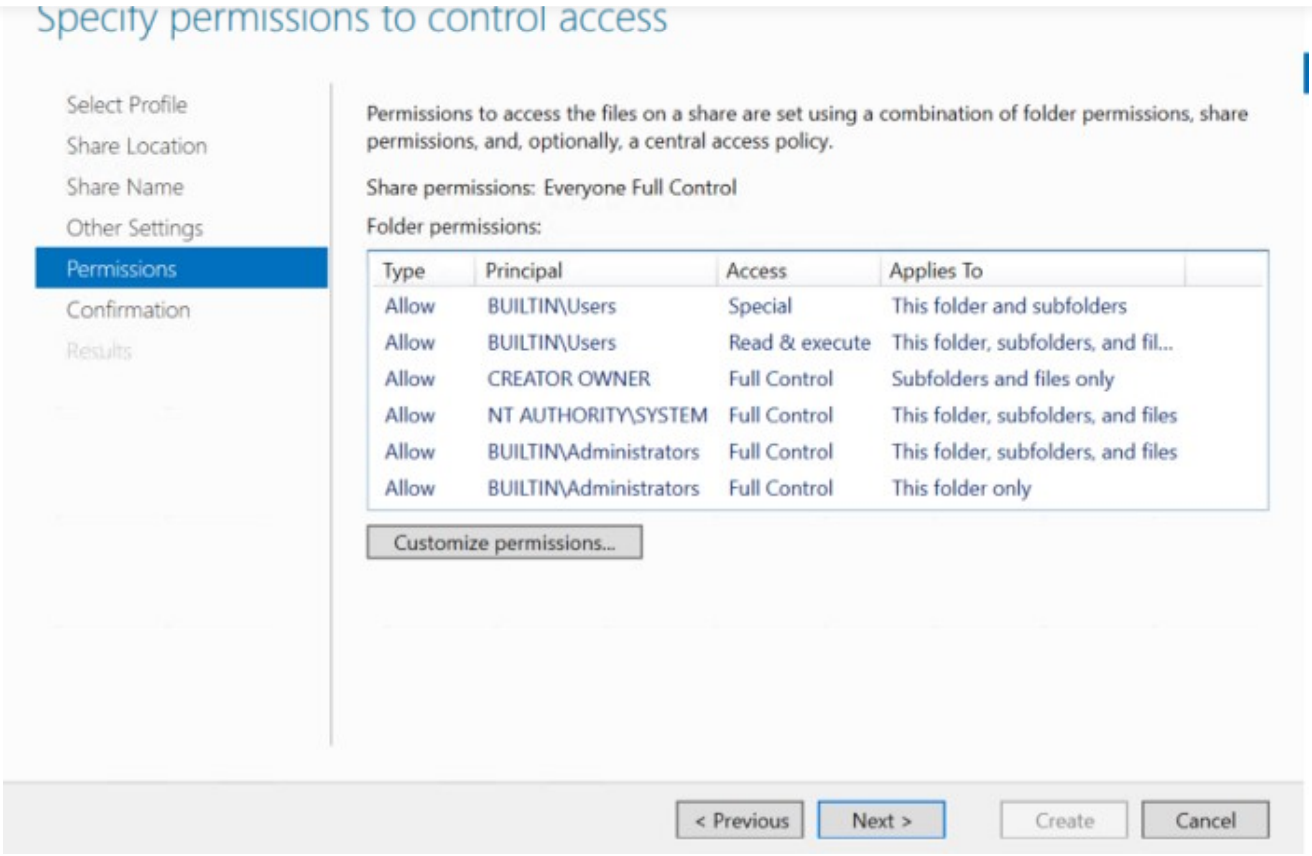
Stick with **hackme** as the Share name and click Next.



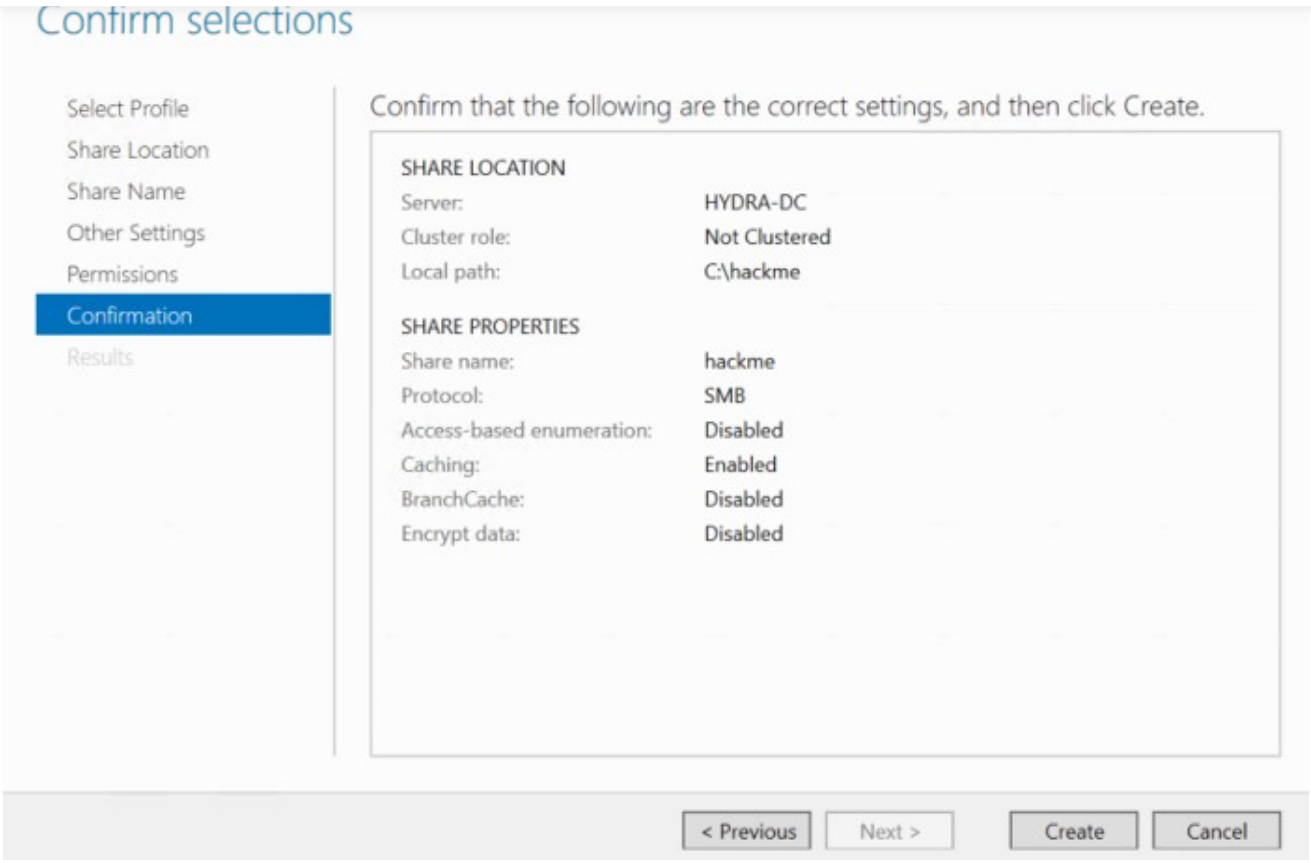
Stick with the defaults on the **Other Settings** tab and click Next.



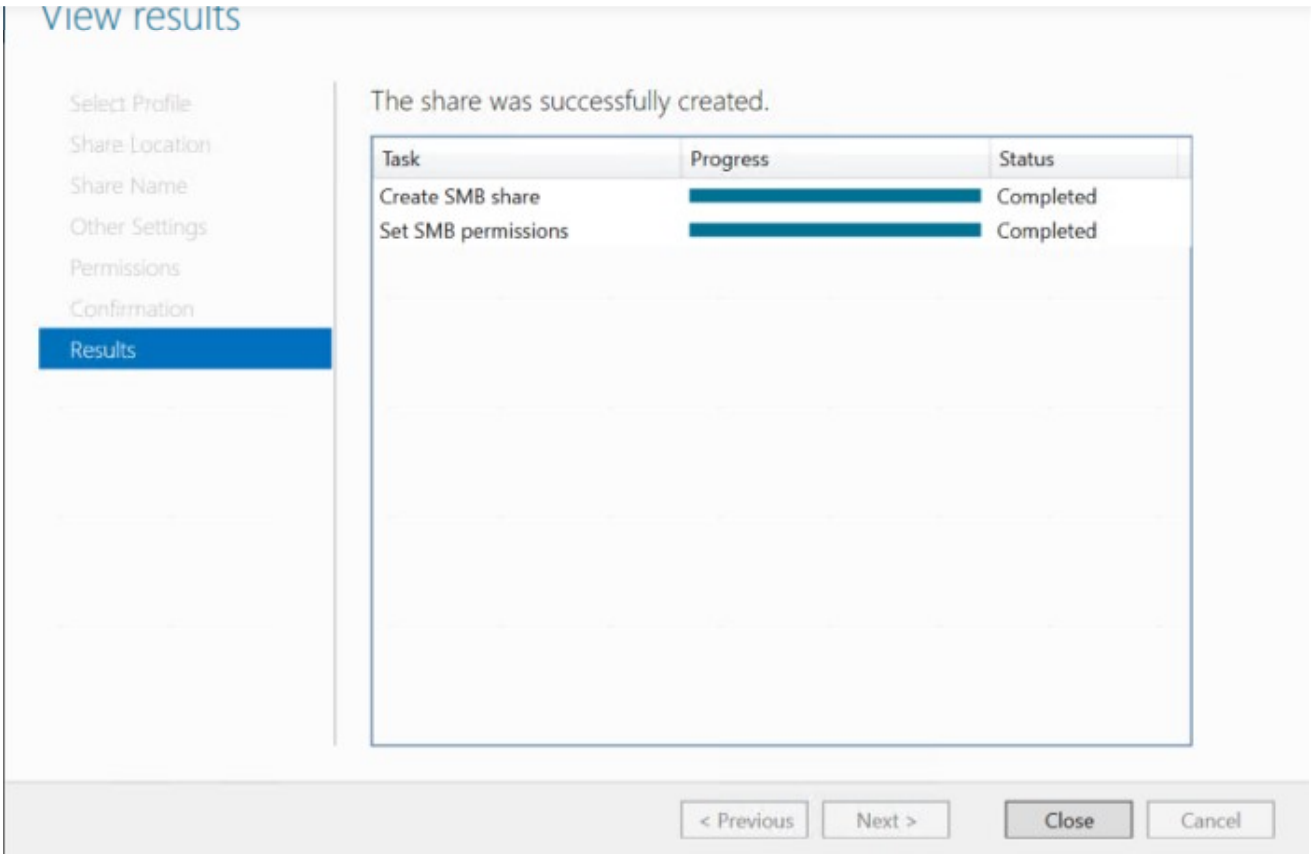
Stick with the defaults on the **Permissions** tab and click Next.



Click on the **Create** button on the **Confirmation** tab.

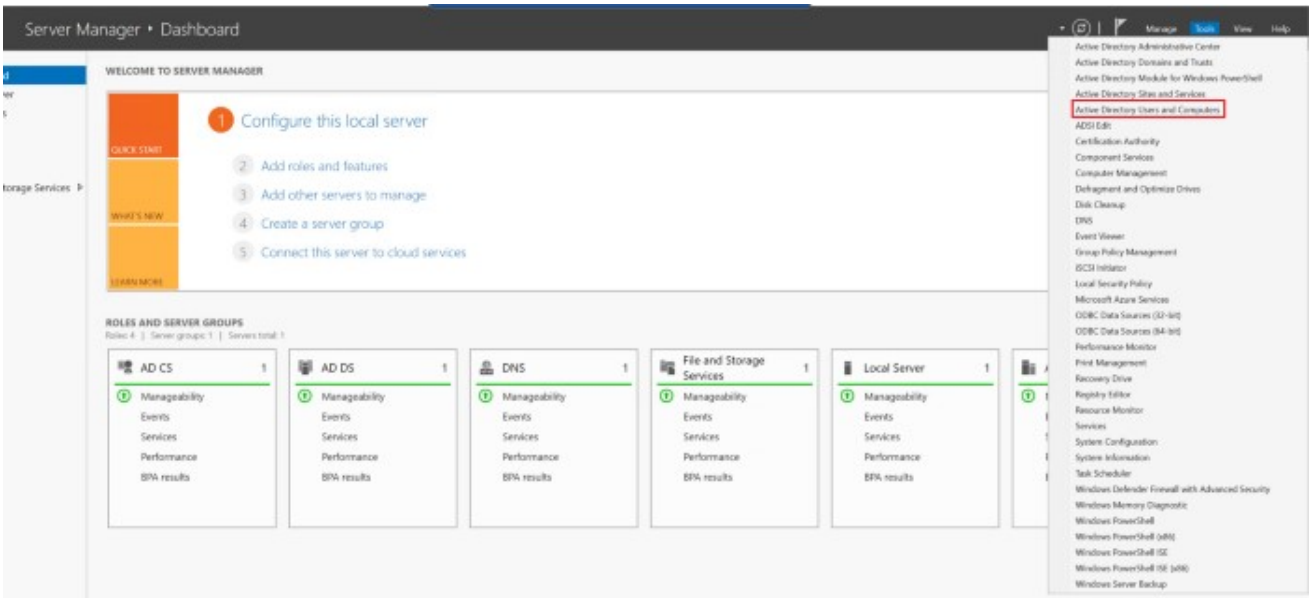


Shortly after you will see the message about share created successfully. You can close this dialog now.

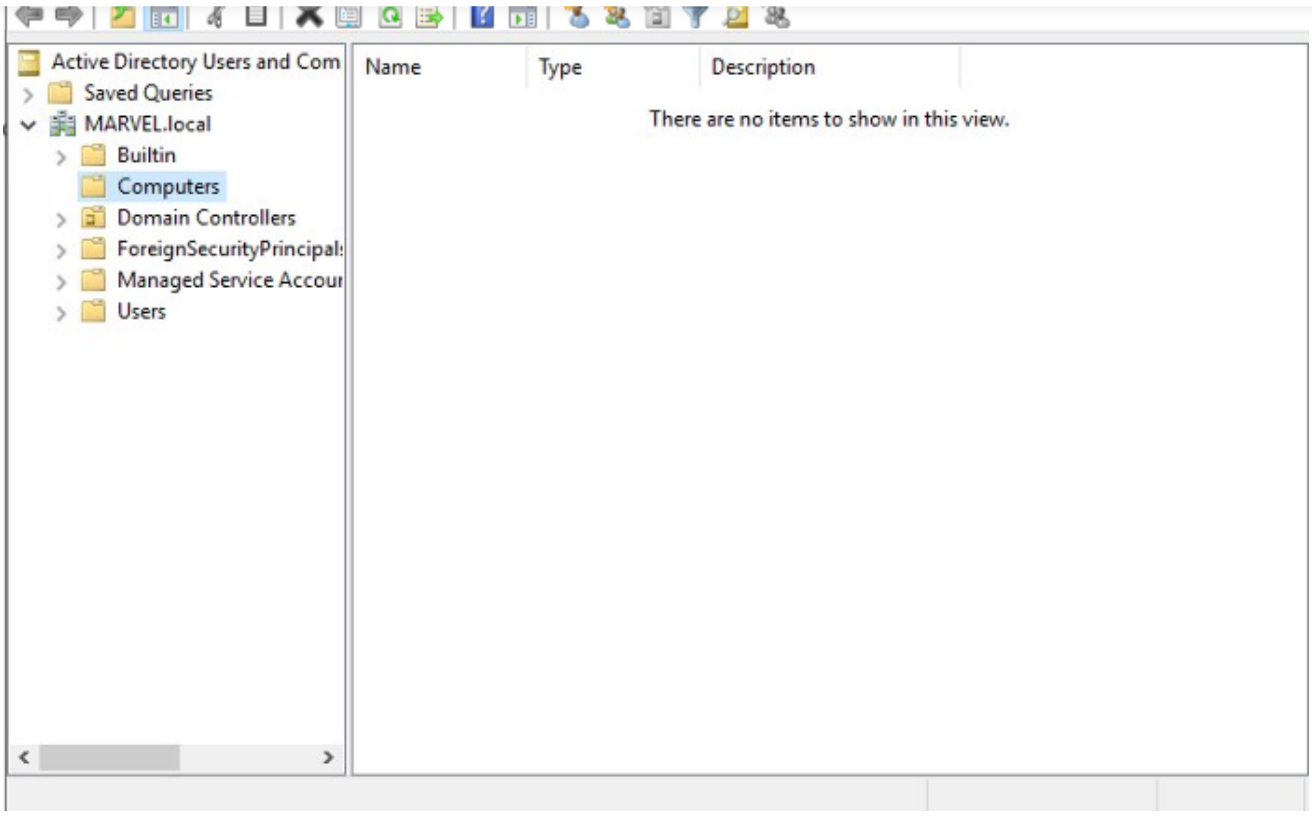


Creating Domain Users

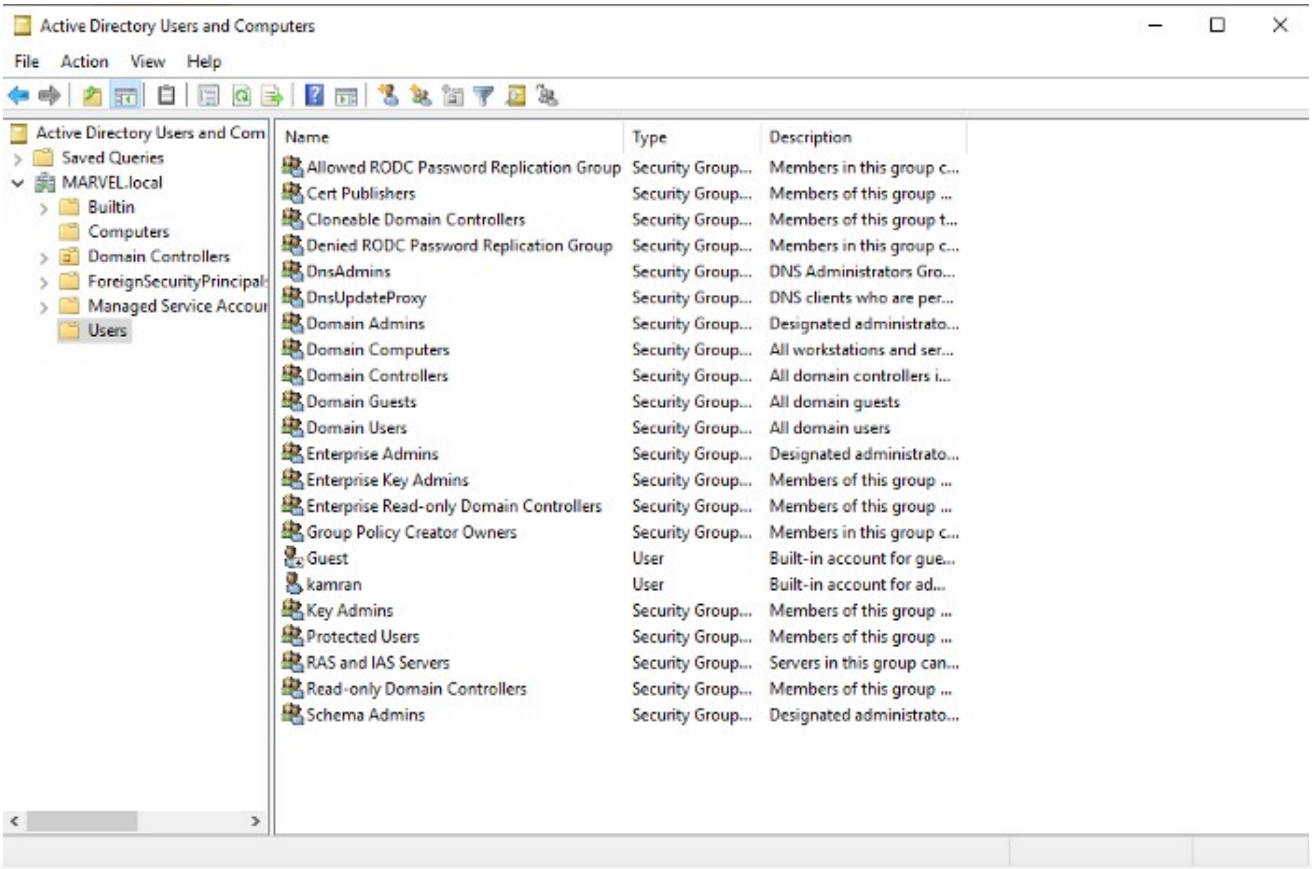
Let's create a few domain users now. Launch the Server Manager and click on the **Active Directory Users and Computers** menu option as shown below.

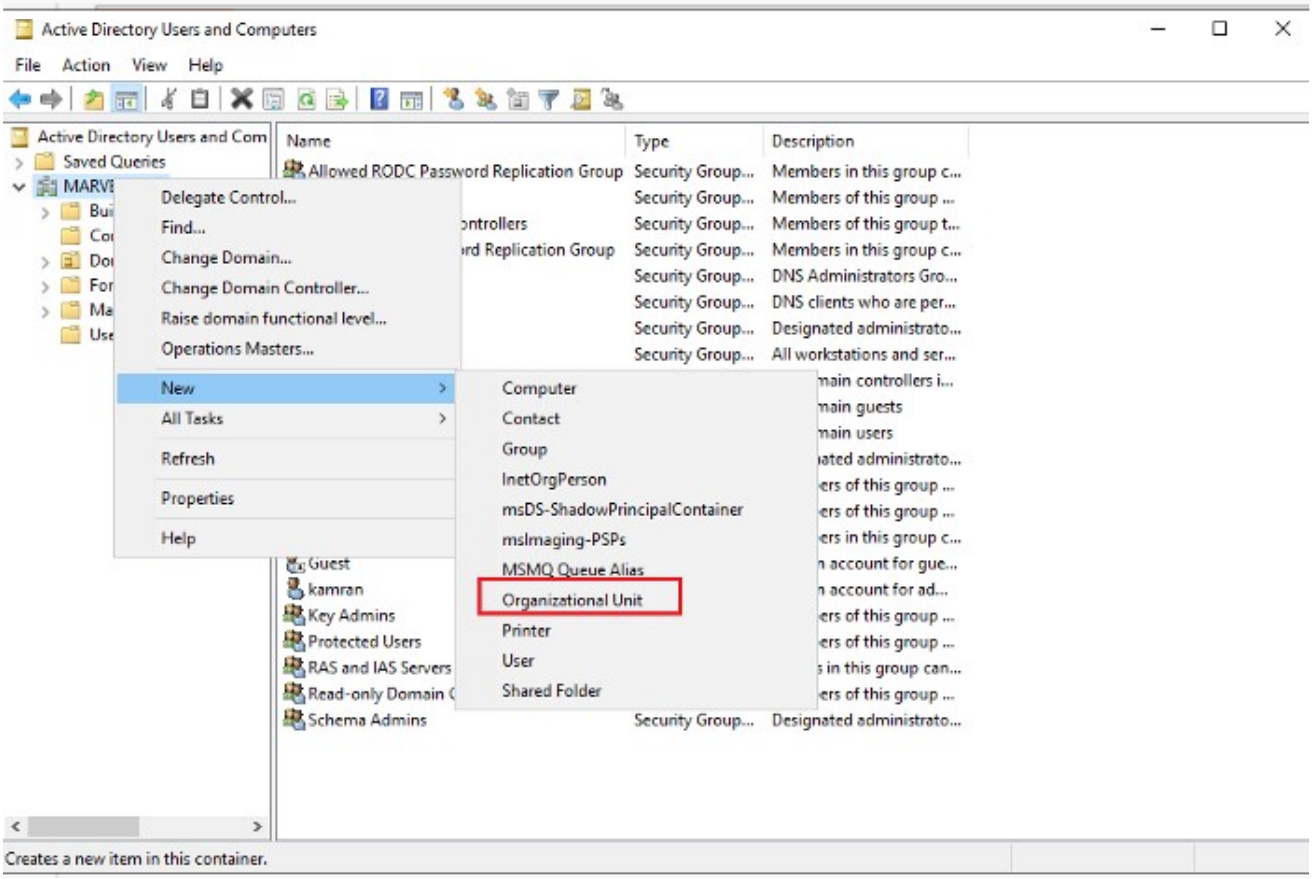


This will launch the **Active Directory Users and Computer** application as shown

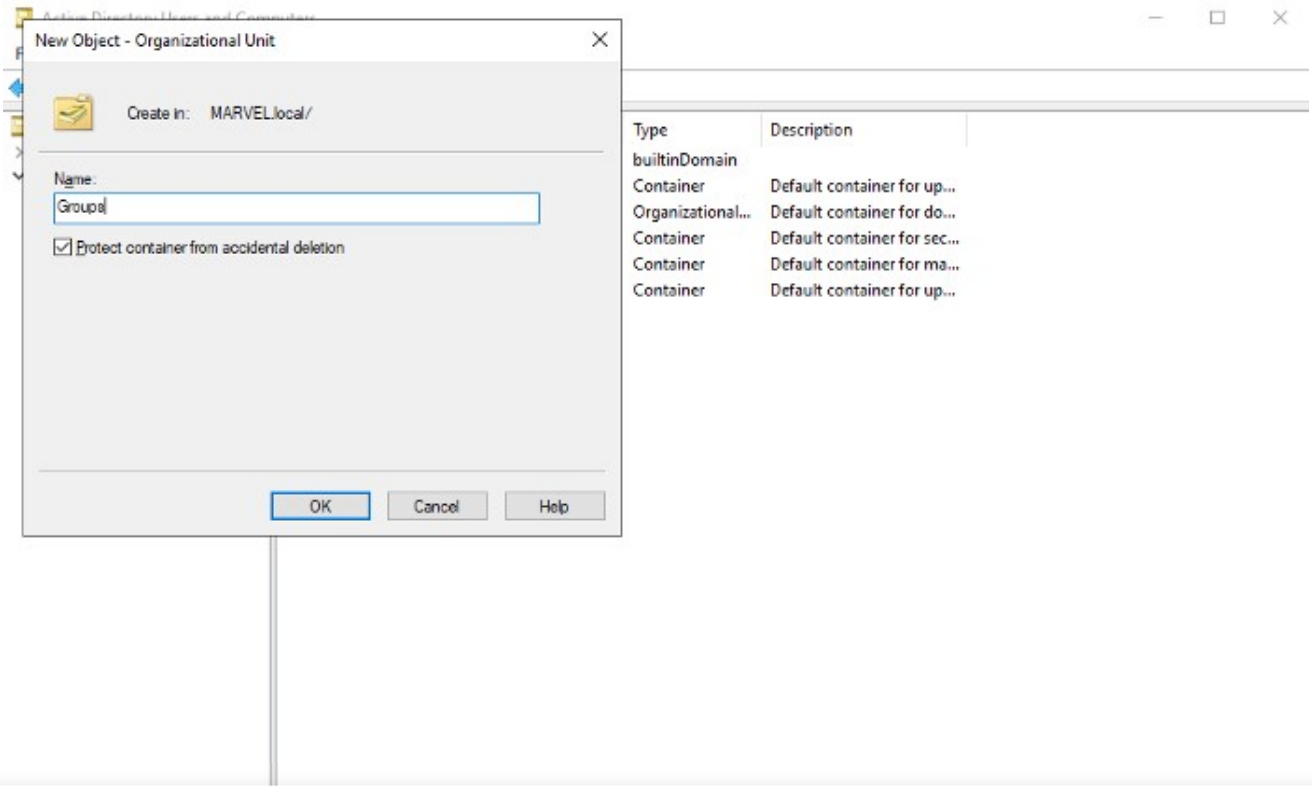


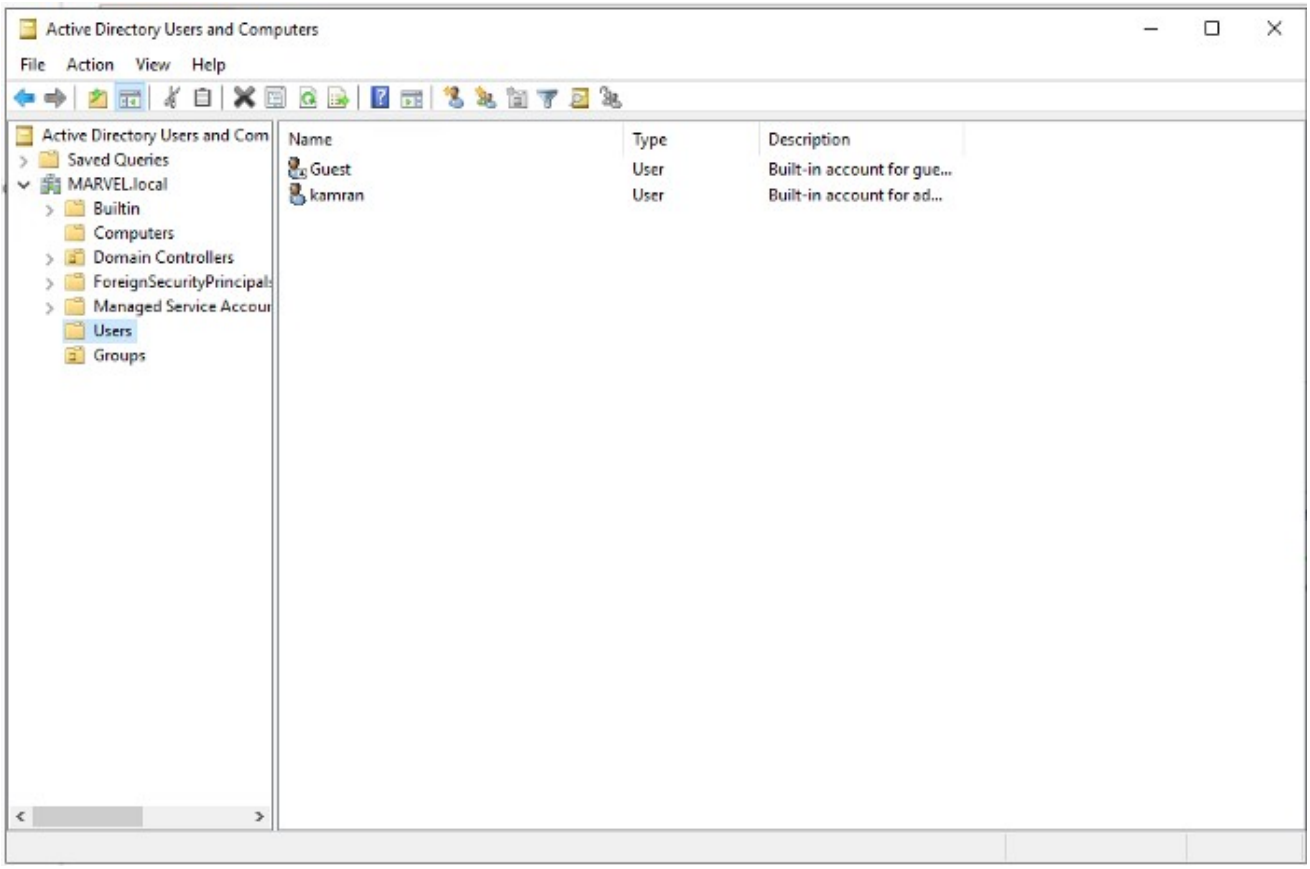
Click on the **Users** node. Let's clean up the entries here a little for ease of management.



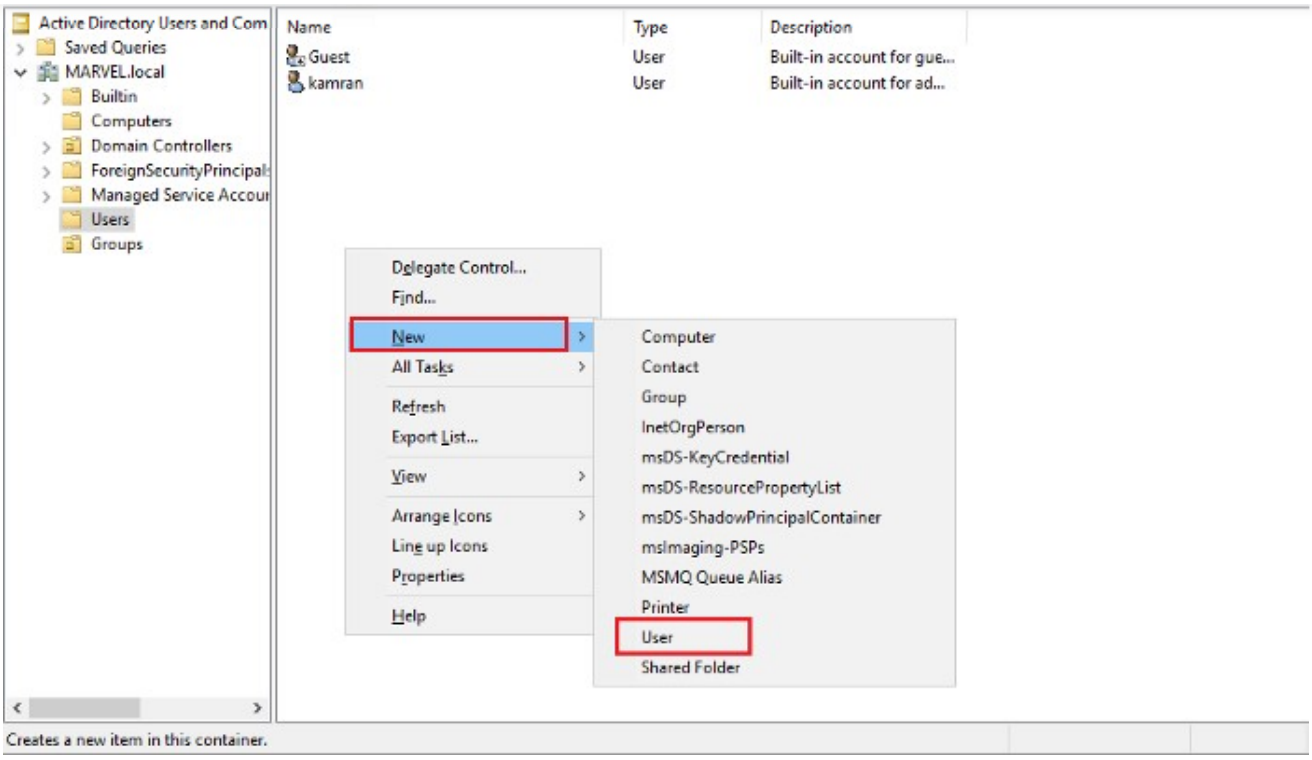


Following dialog will be prompted. Let's name this OU as **Groups**.

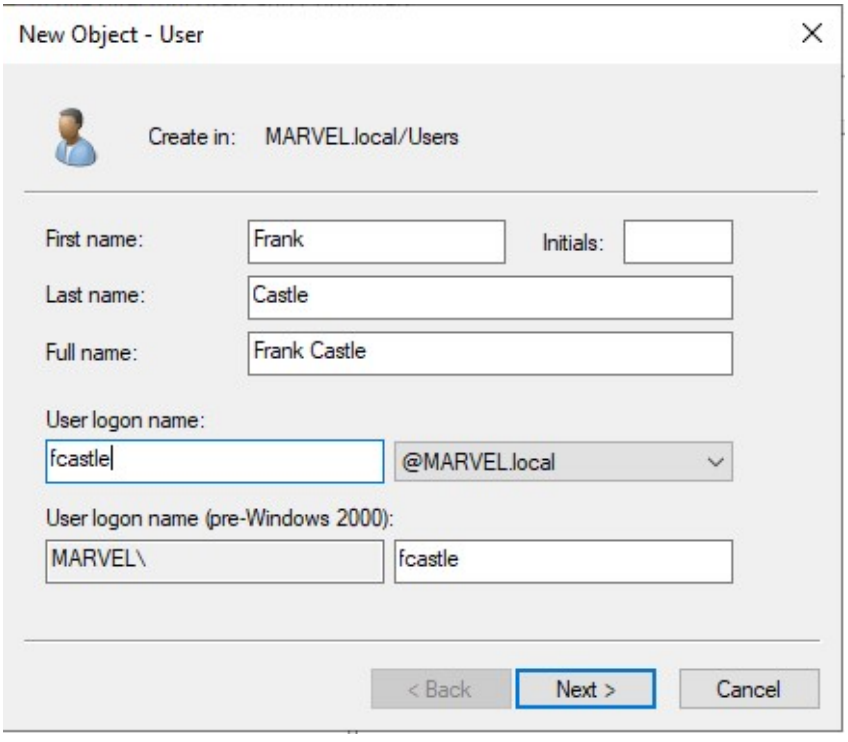




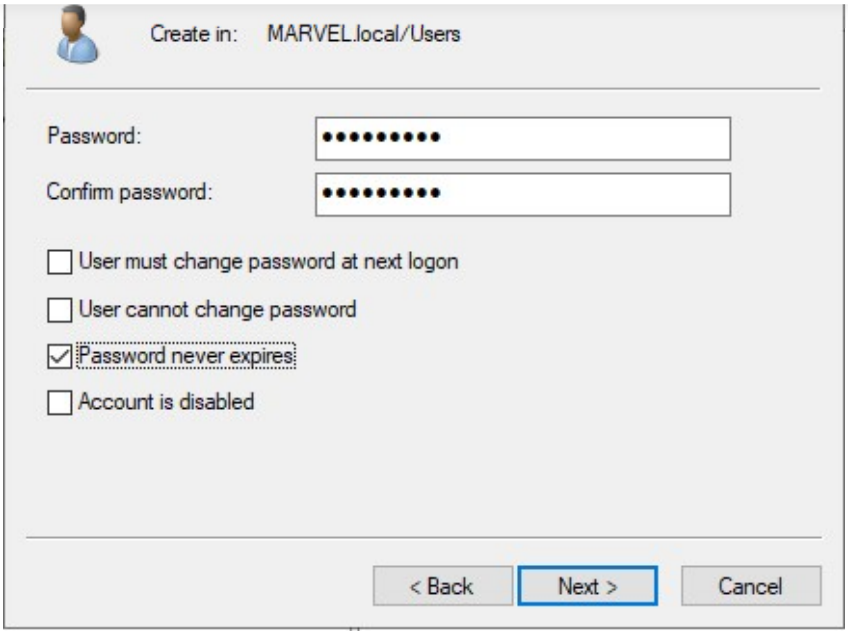
Right-click and select the option for creating a new user.



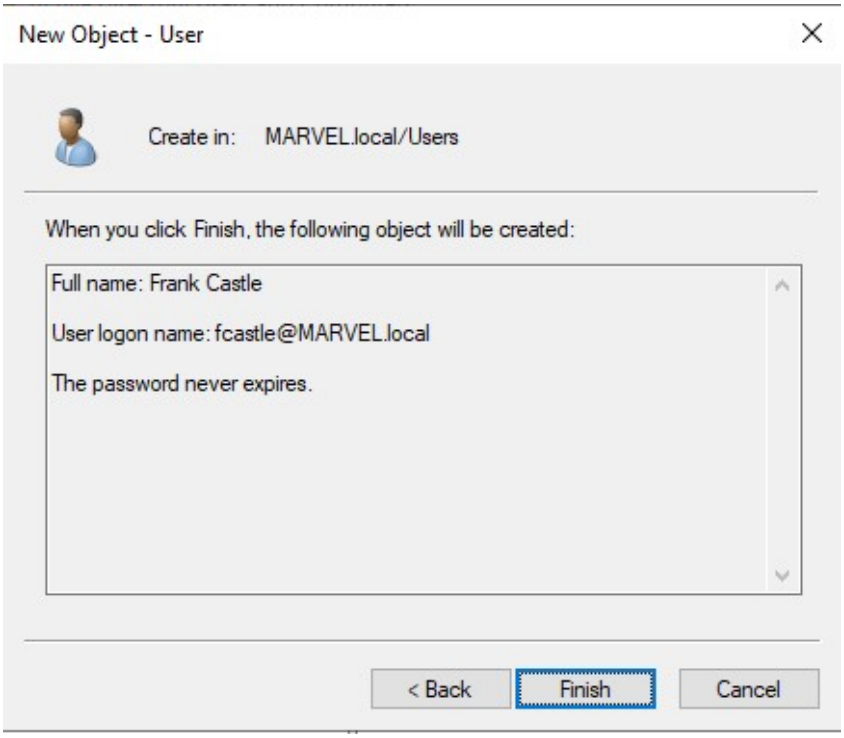
Let's create the first user with First name **Frank**, Last name **Castle** and logon name as **fcastle** as shown below. Click on Next.



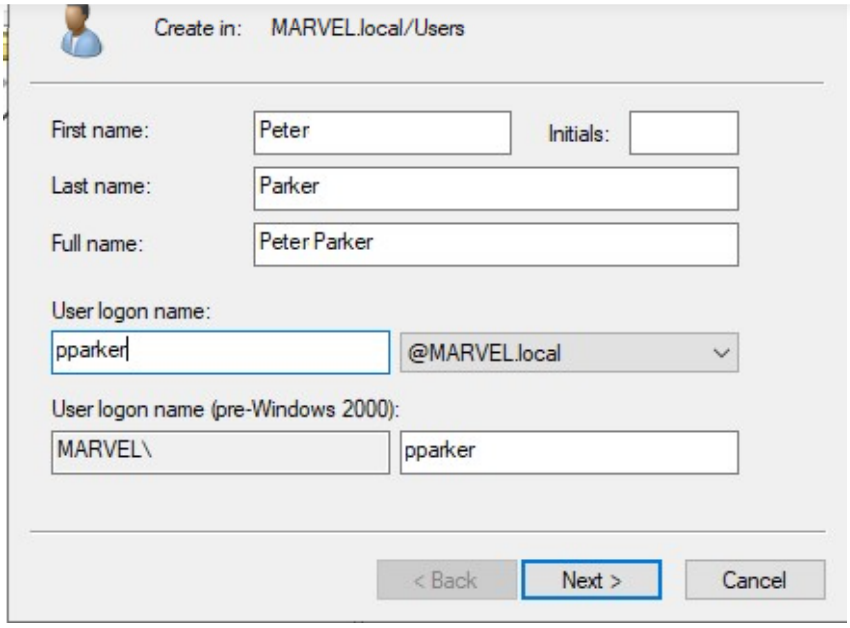
I used a kind of weak password **Password1**. Uncheck **User must change password at next logon** and check the option for **Password never expires**. Click Next.



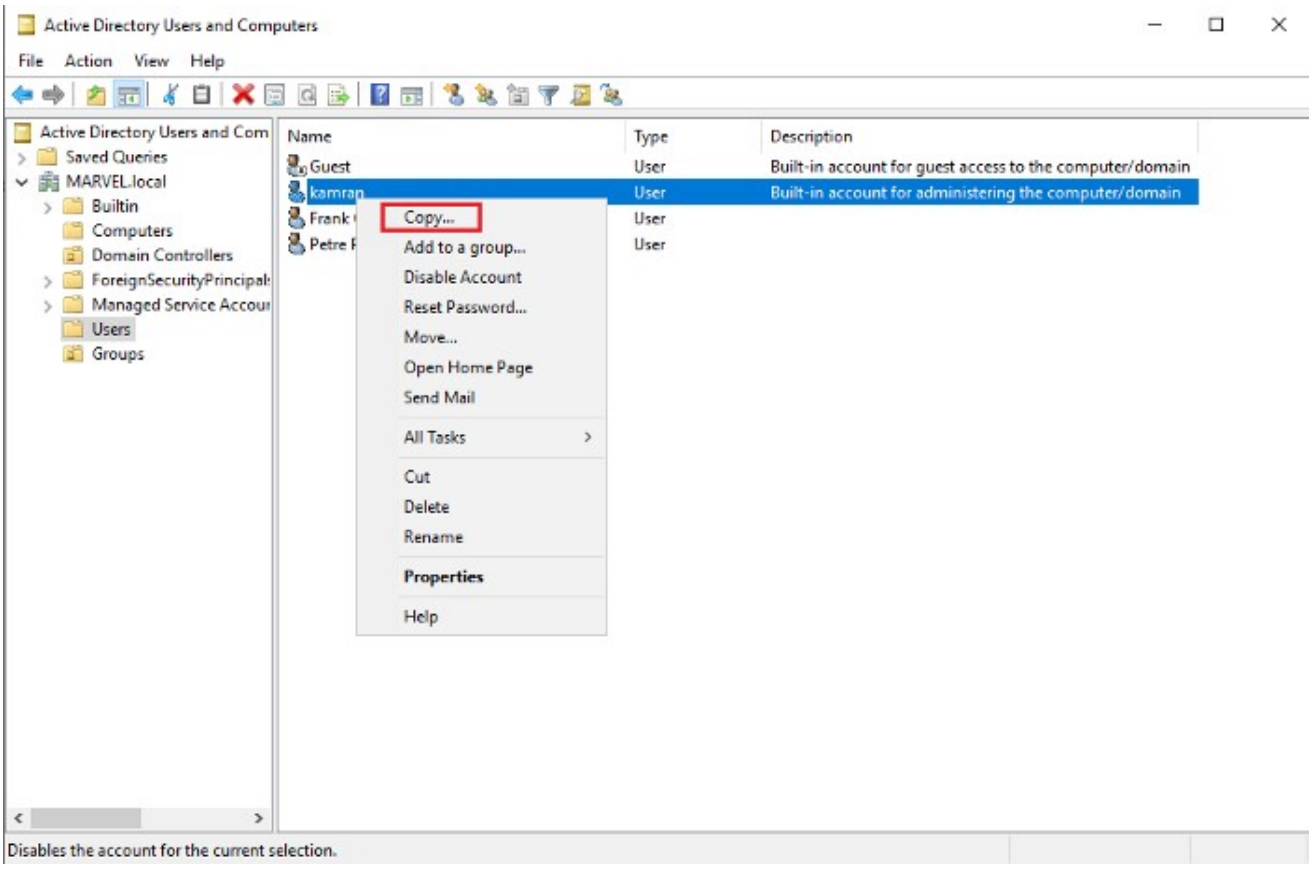
Click Finish here.



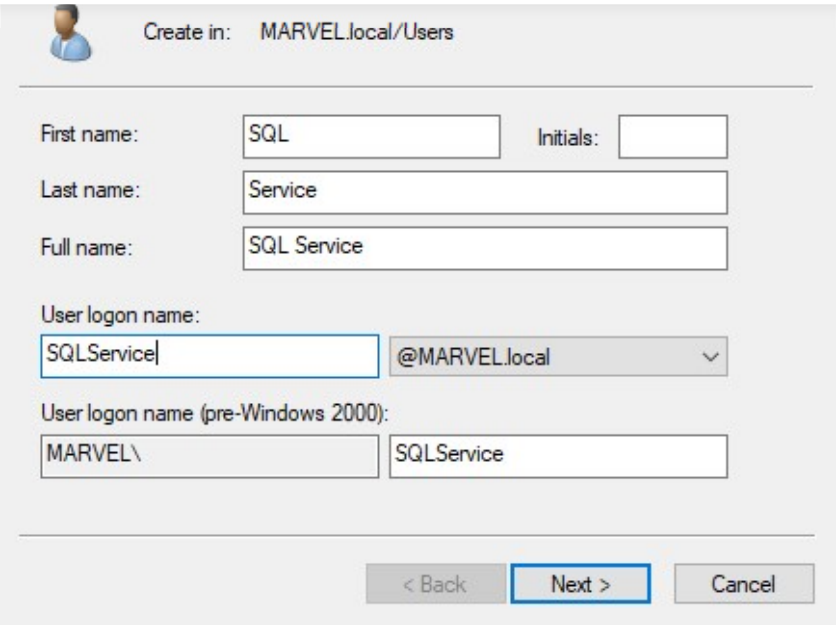
Repeat same steps to create another user with First name **Peter**, Last name **Parker** and logon name as **pparker** as shown below. I used the same password **Password1** for this user as well.



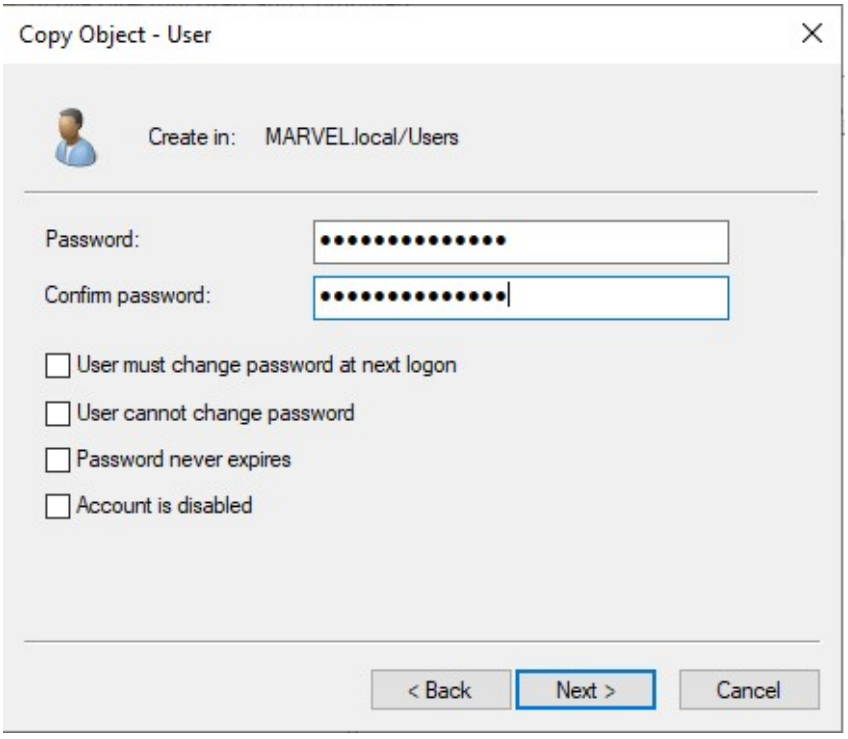
Finally, create a domain-admin type user. For that, we just copy the existing admin user **kamran** by right-clicking on its username and click on the **Copy…** menu option as shown below.



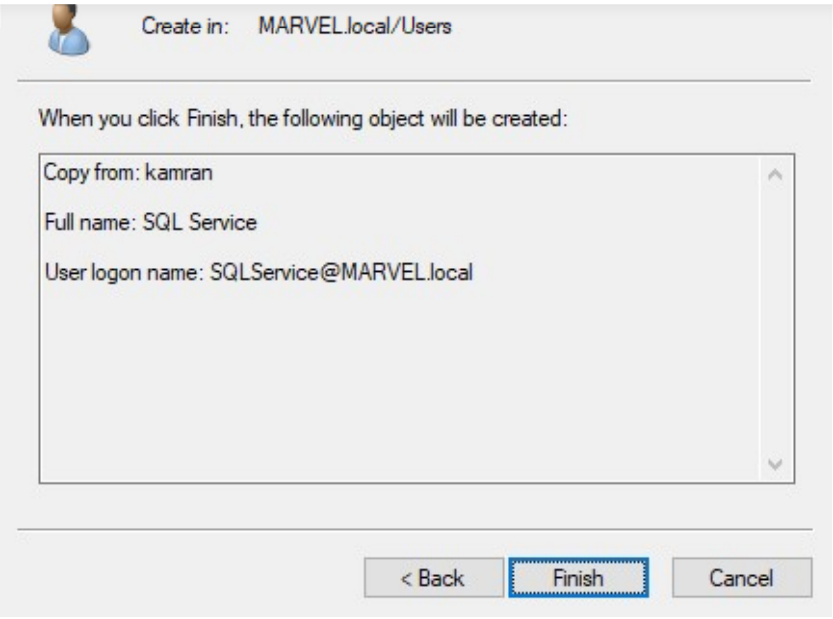
Let's give this user first name **SOL**, last name **Service** and logon name of **SOL Service**



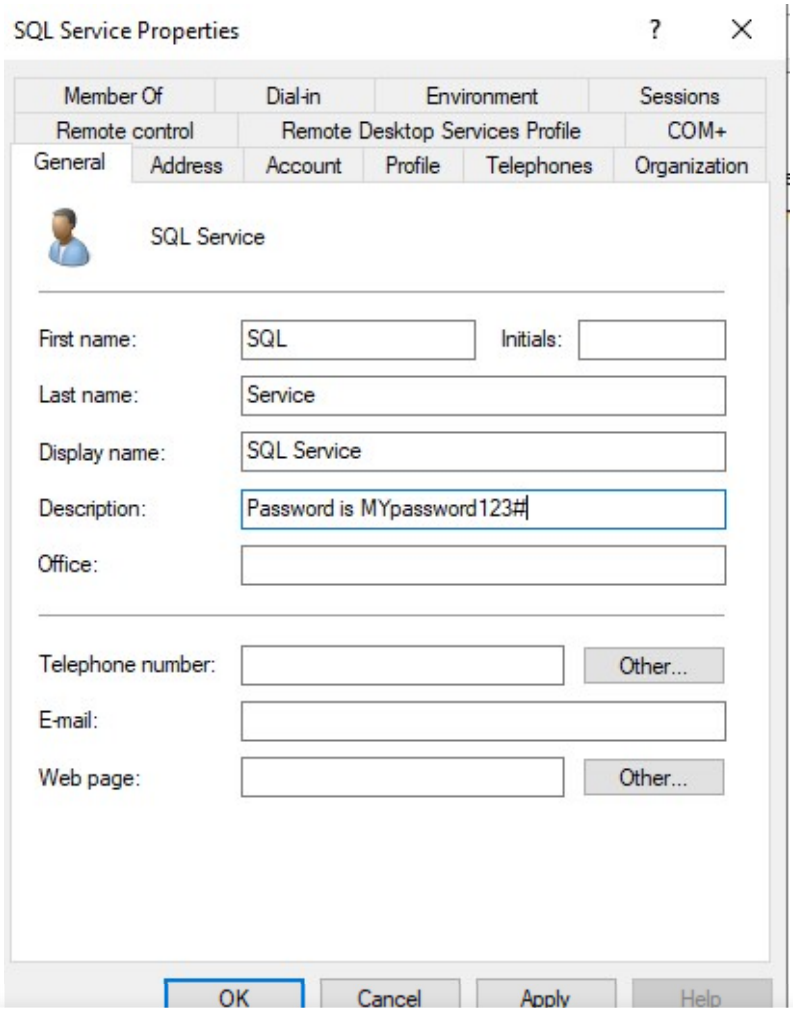
Let's set the password for this user as **MYpassword123#** with settings as shown below. Click Next then.



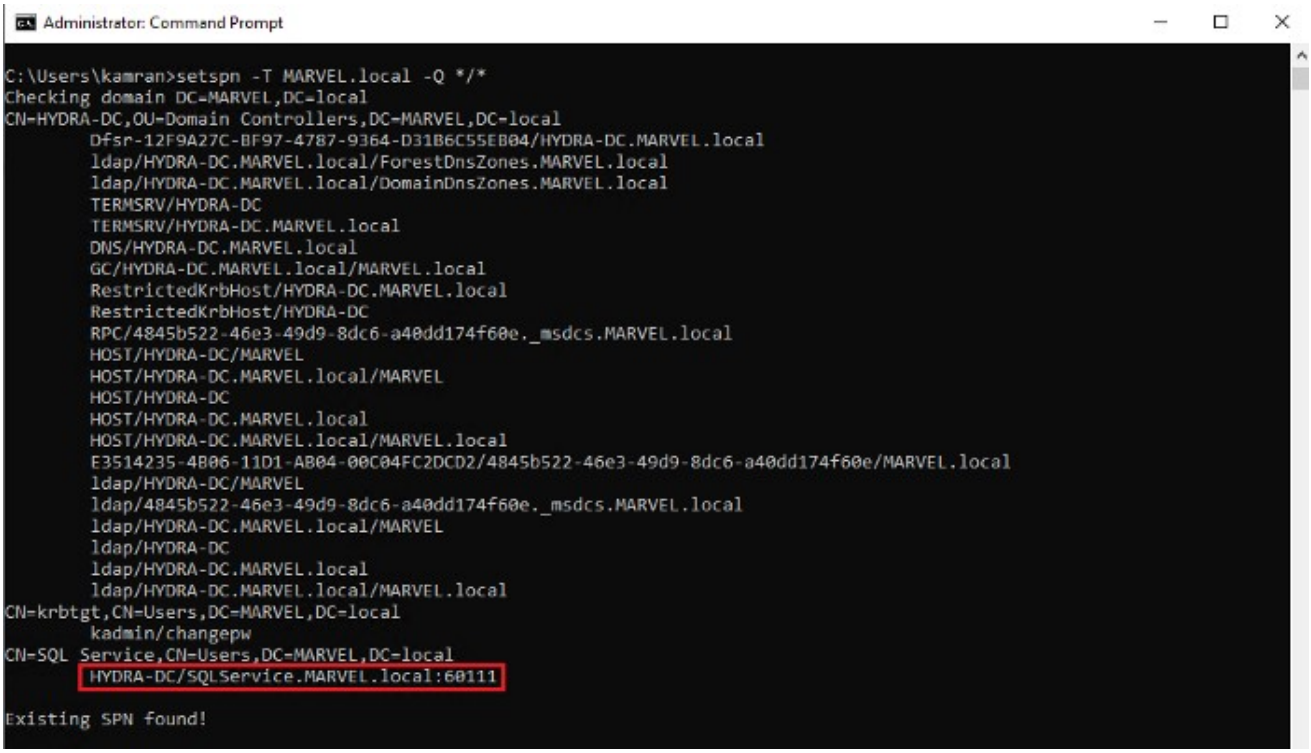
Click Finish here.



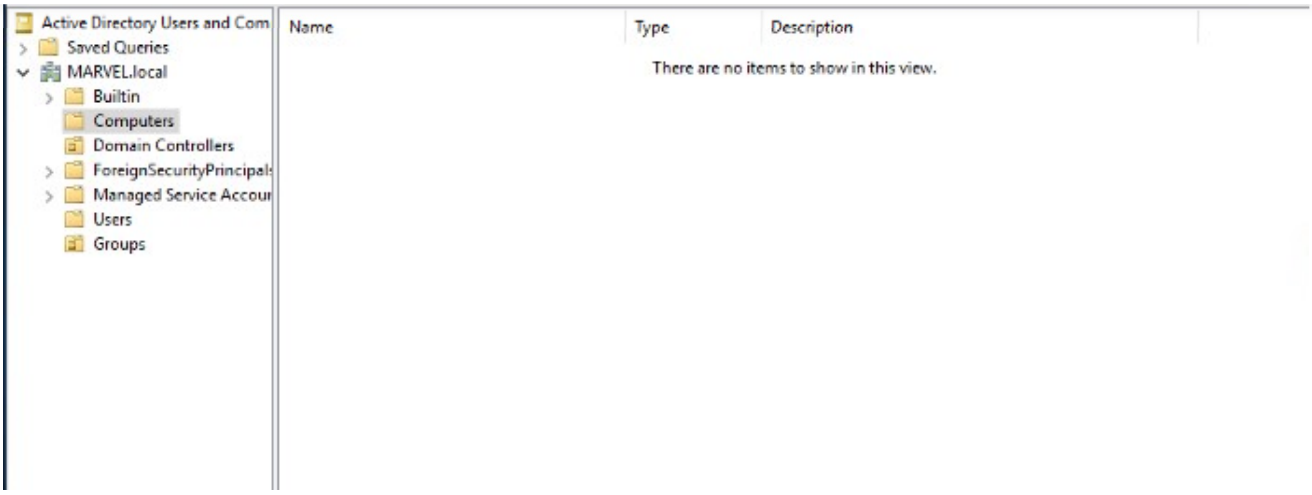
Go back on the properties for SQLService user and set Description as Password is **MYpassword123#** as shown below.



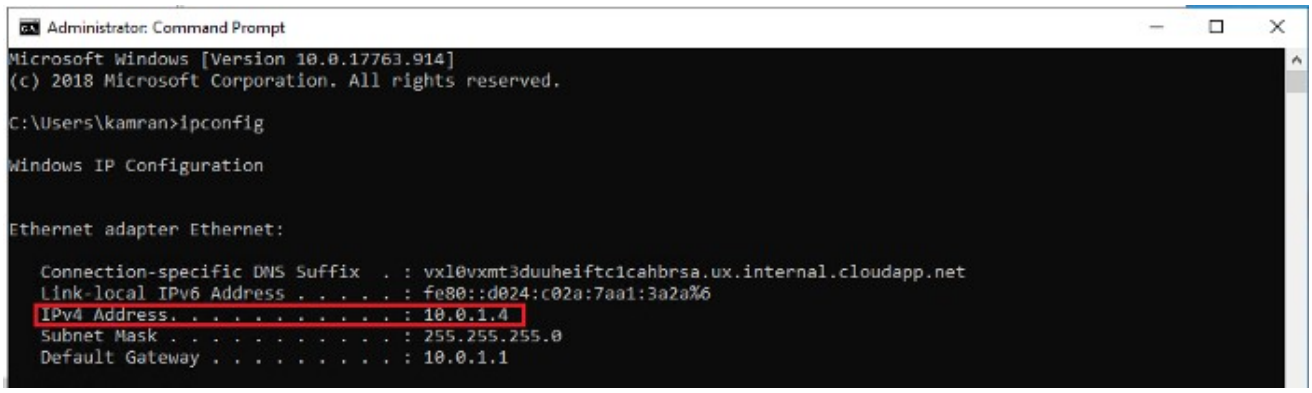
We can run setspn again to confirm the domain for existing SPN as shown below.



This basically completes the creation of domain users and required configuration. As of now, no computers have joined the domain.

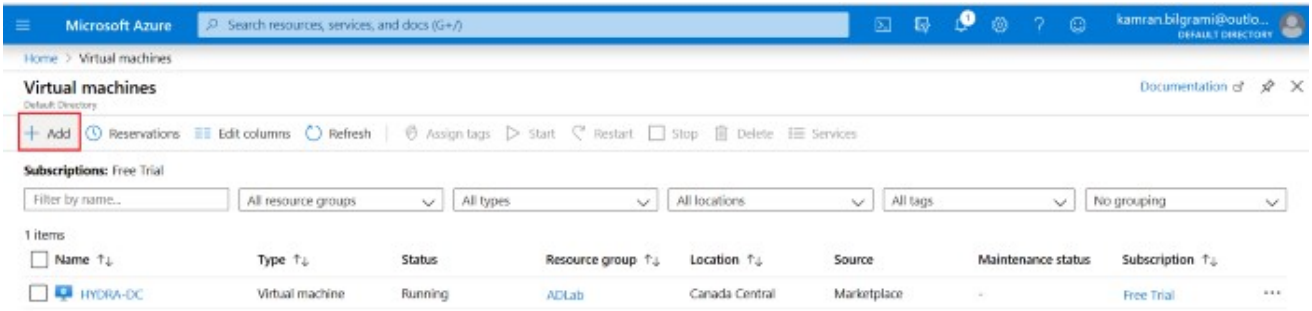


Important to note the IP address of the domain machine as this will be used when joining user computers to the domain.

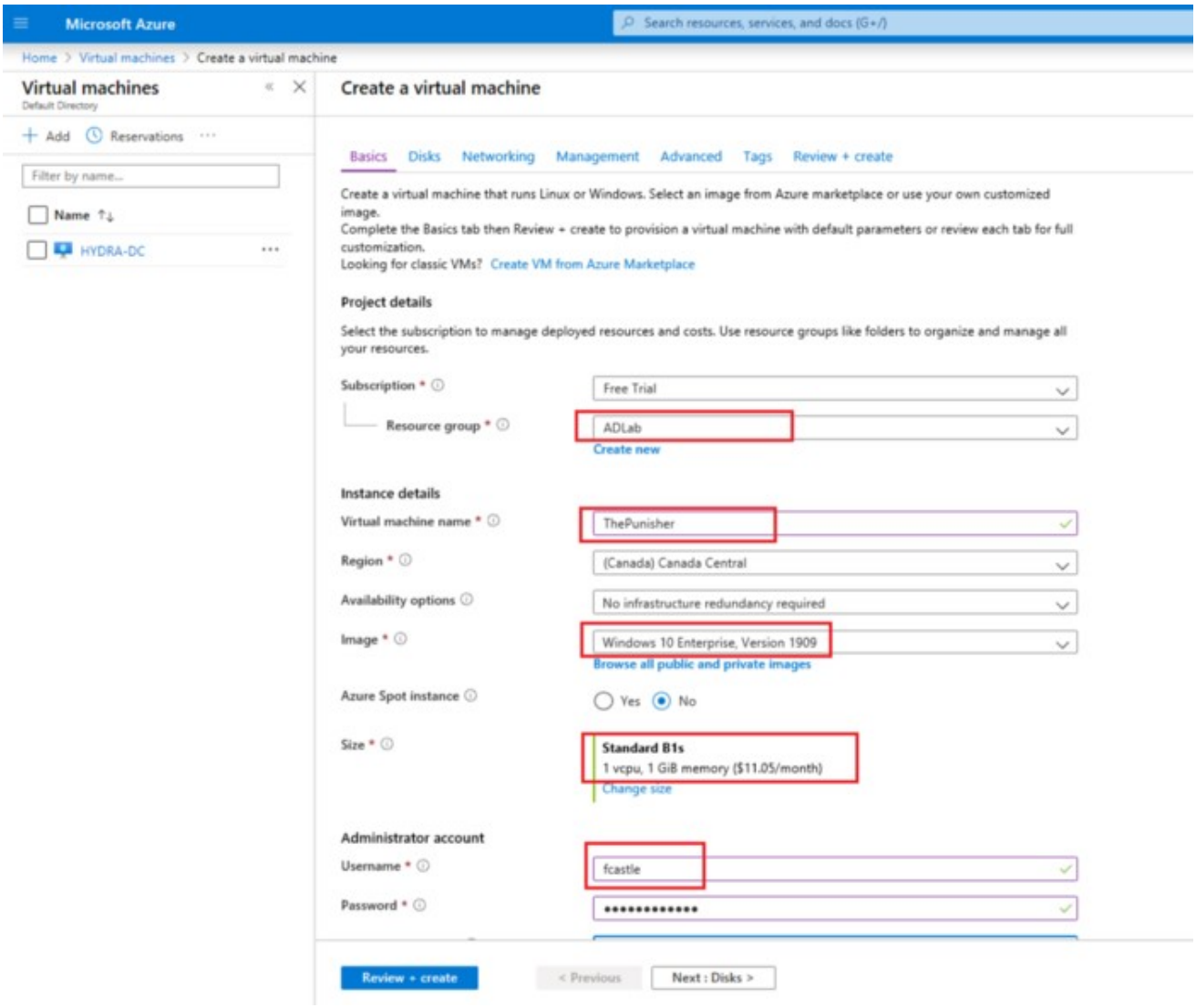


Setting up first User Machine

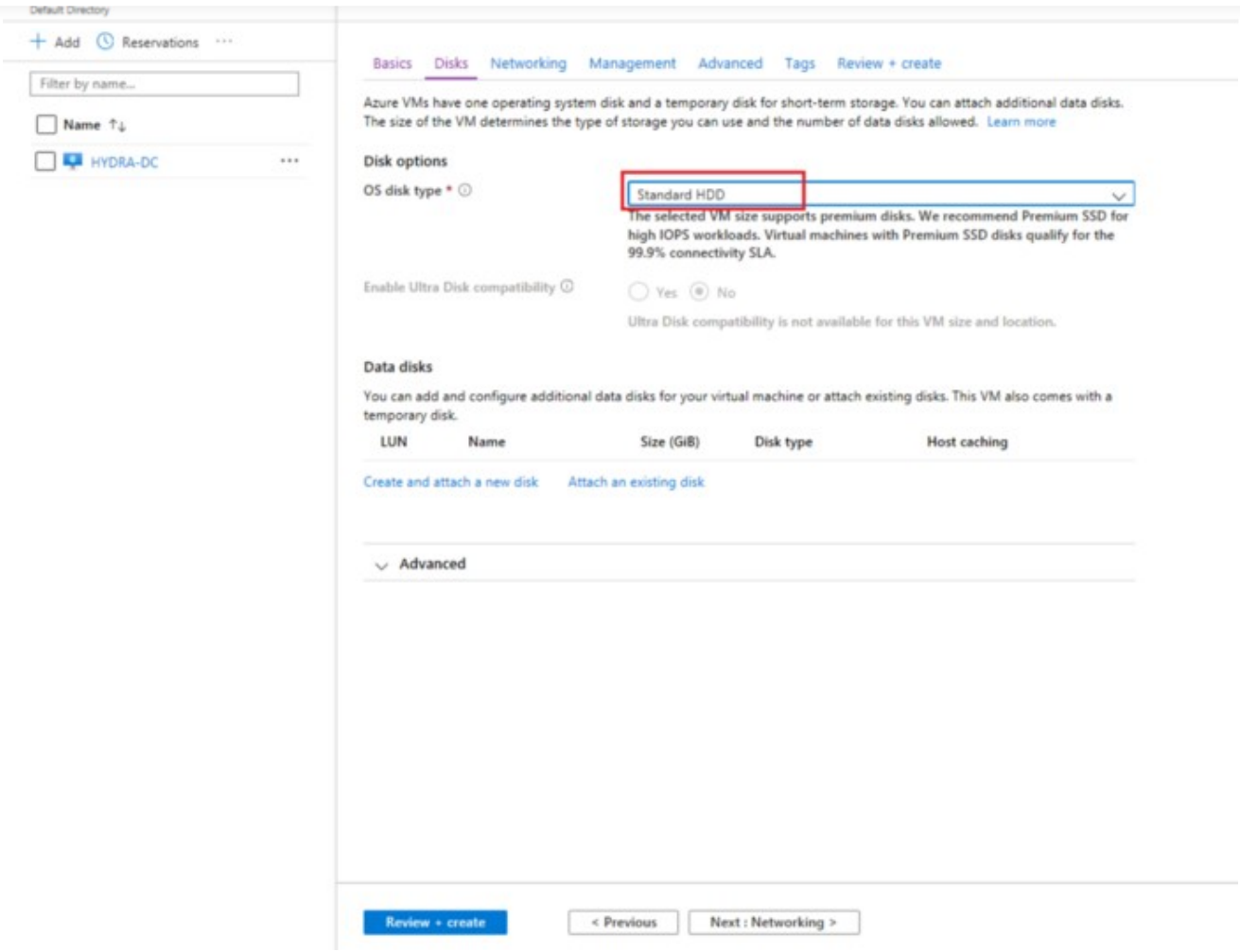
Let's start setting up our first user machine. Under the Virtual machines page, click on the **Add** button.



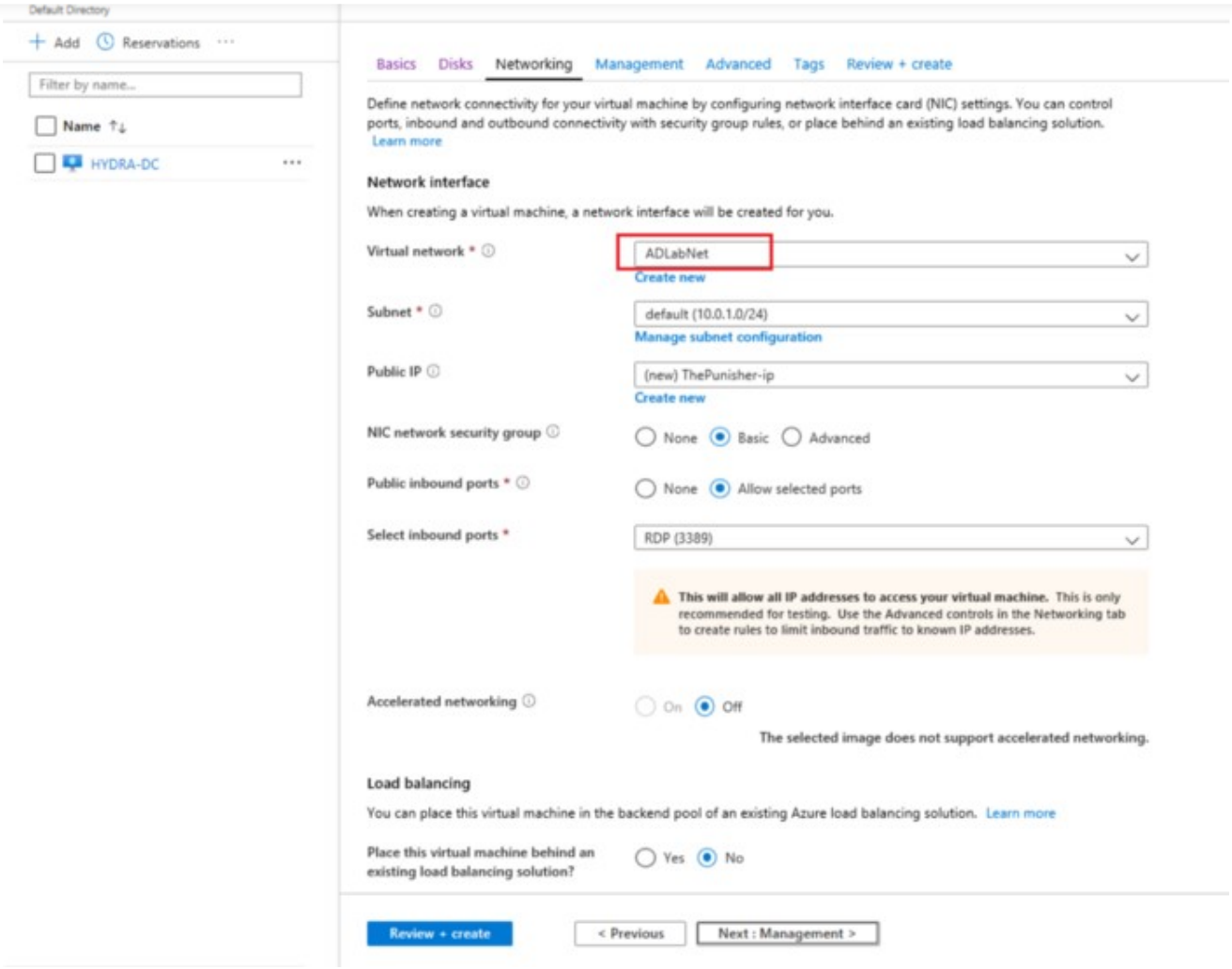
- Set machine name as **ThePunisher**
- Choose **Windows 10 Enterprise Version 1909** image.
- Choose **Standard B1s** machine size
- Name username as **fcastle**. Give it a weak password. I use **myPassword01**



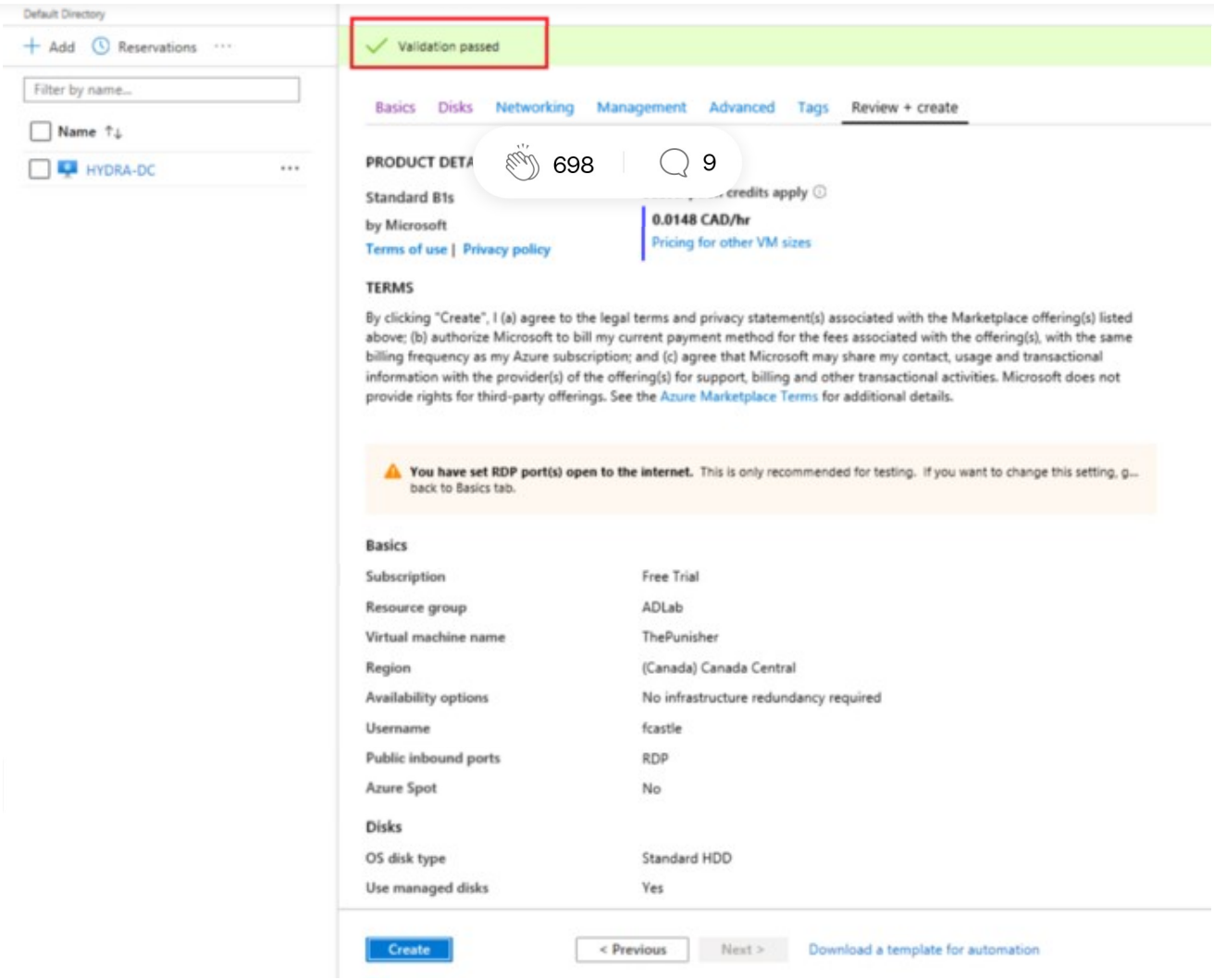
Choose **Standard HDD** for this VM as well.



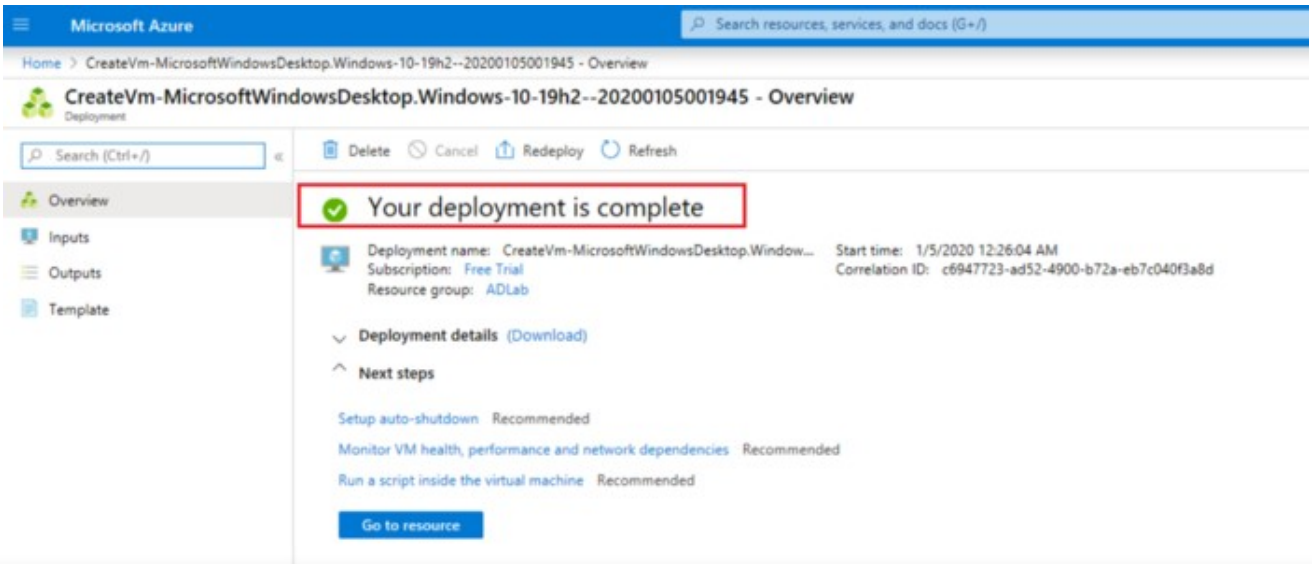
Make sure this VM is also using the **ADLabNet** Virtual network. For the rest of the options, just use defaults and click on the **Review + create** button.

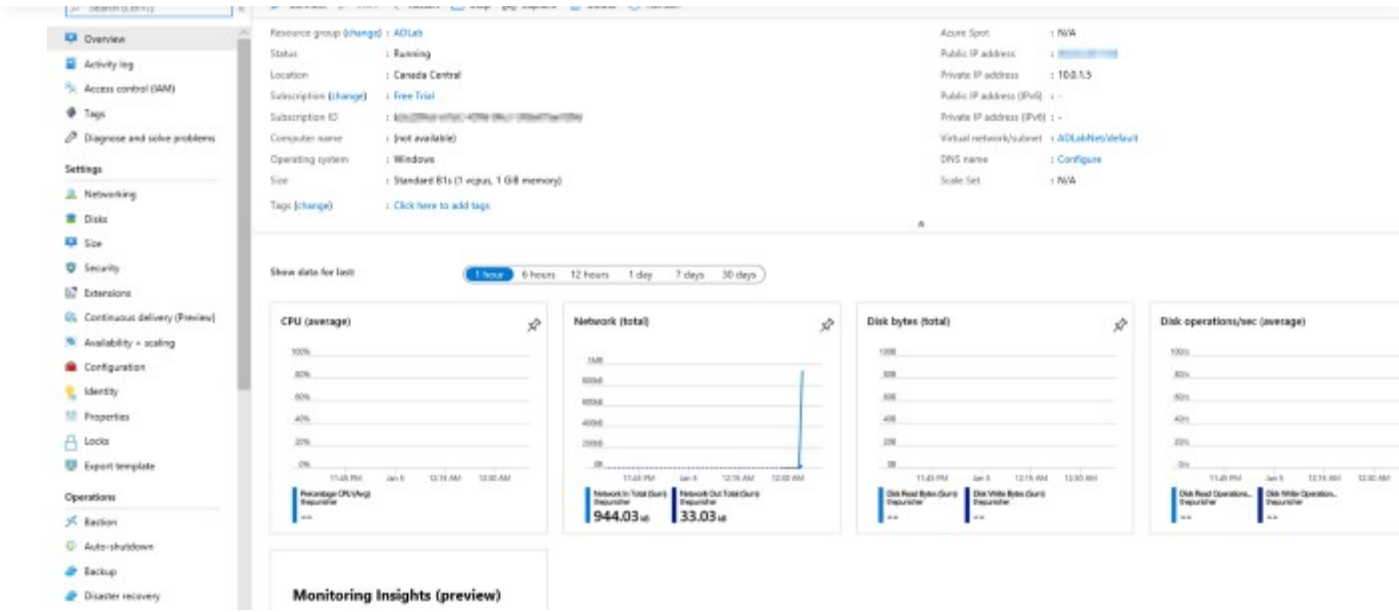


You should see a message about validations succeeded. Click on **Create** button here.

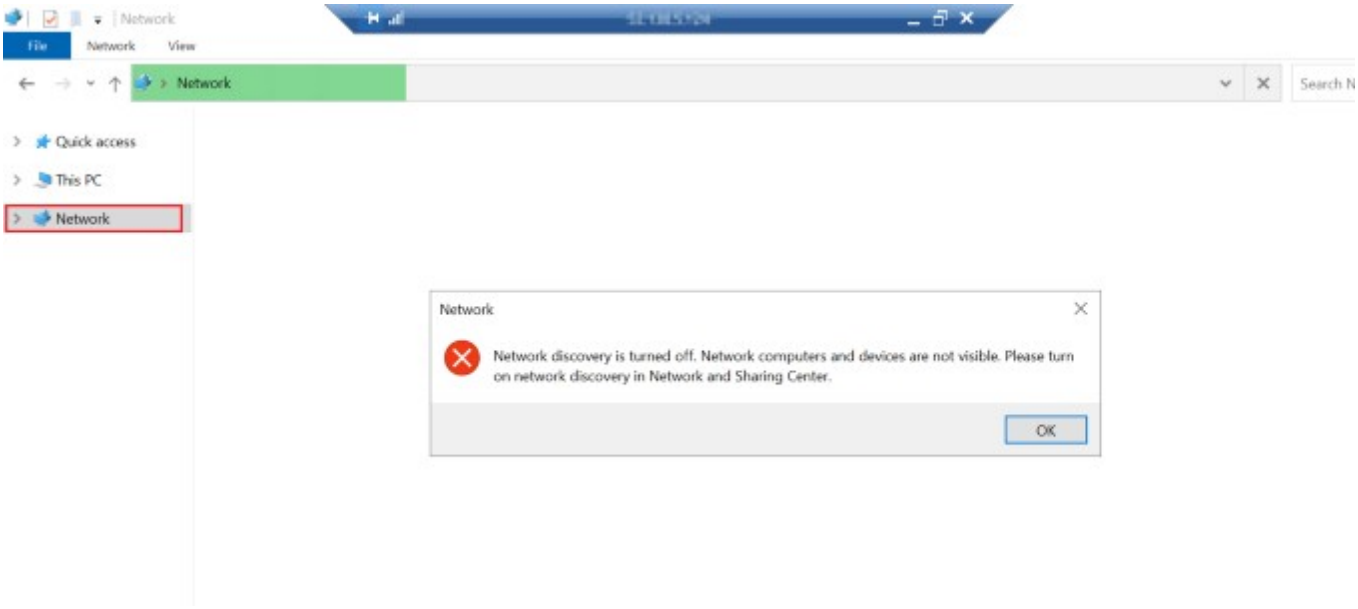


Shortly after you see the message that deployment is complete. You can just click on the Go to resource button to view the newly created VM.

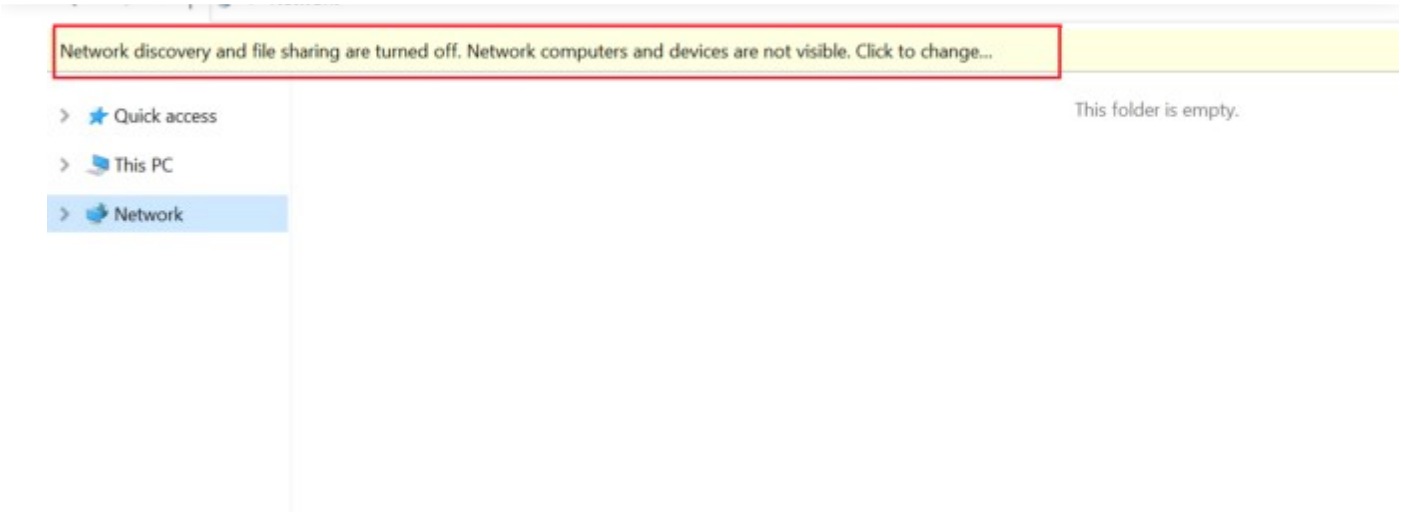




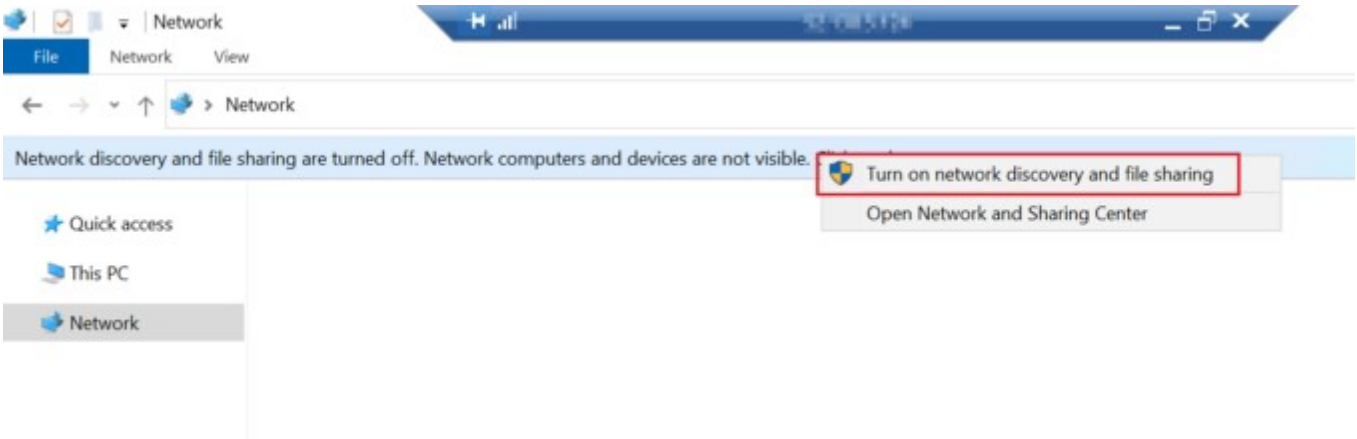
Remote Desktop into this box using the local user account we just setup **fcastle** (password **myPassword01**). Launch File Explorer and click on the **Network** node. You will be prompte with a message box stating Network Discovery is turned off. Click OK here.



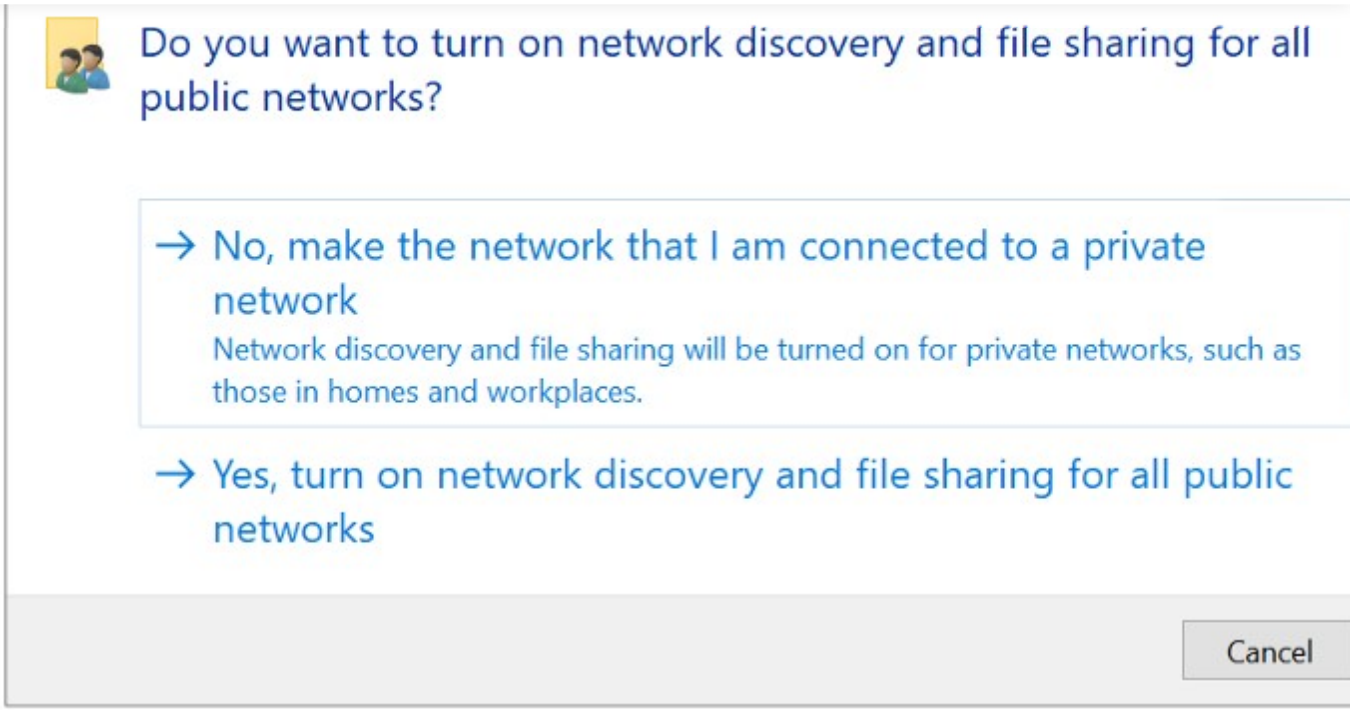
Click on the message below to change the Network discovery and file sharing settings.



Click on **Turn on network discovery and file sharing** option.



You will be prompted with the following options. Click on the first one.



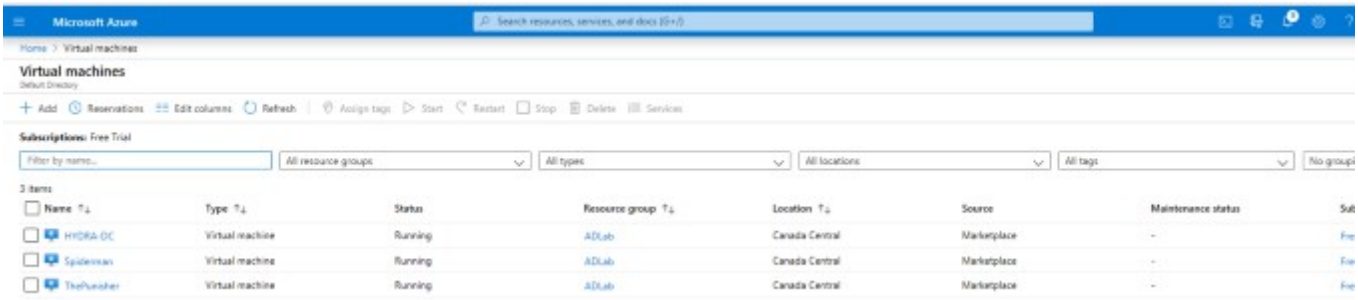
Use the Sysinternals's BgInfo utility on this box as well just like we did for the domain controller earlier.

Setting up the second User Machine

The steps for creating the second User-machine are exactly the same as for the first user

setting up BgInfo utility. This machine should look as follows. Some info may be different (such as IP address depending upon the setting you used etc.).

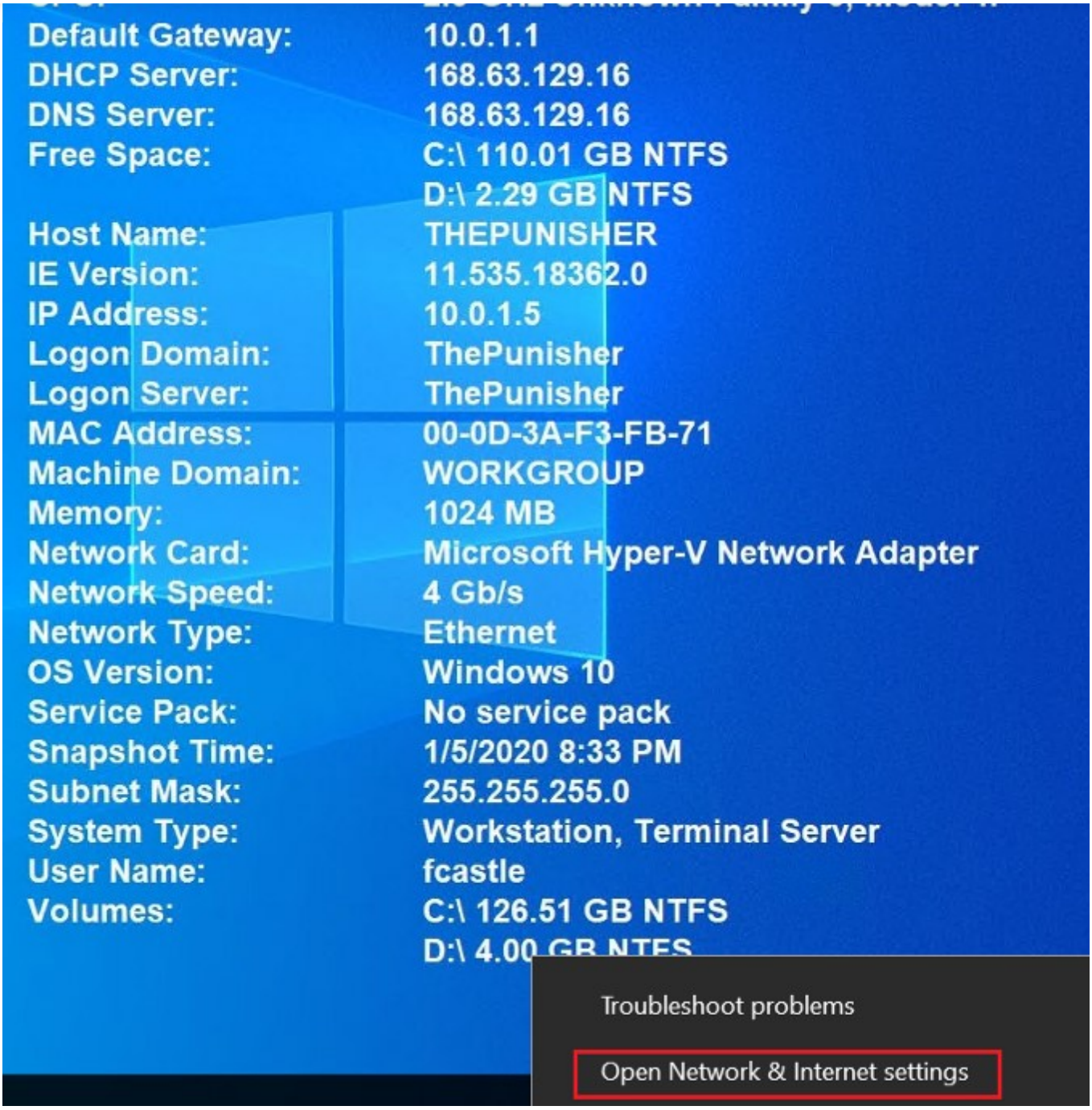
At this point, if we browse to the Virtual Machines page in the Azure portal, it should look as follows.



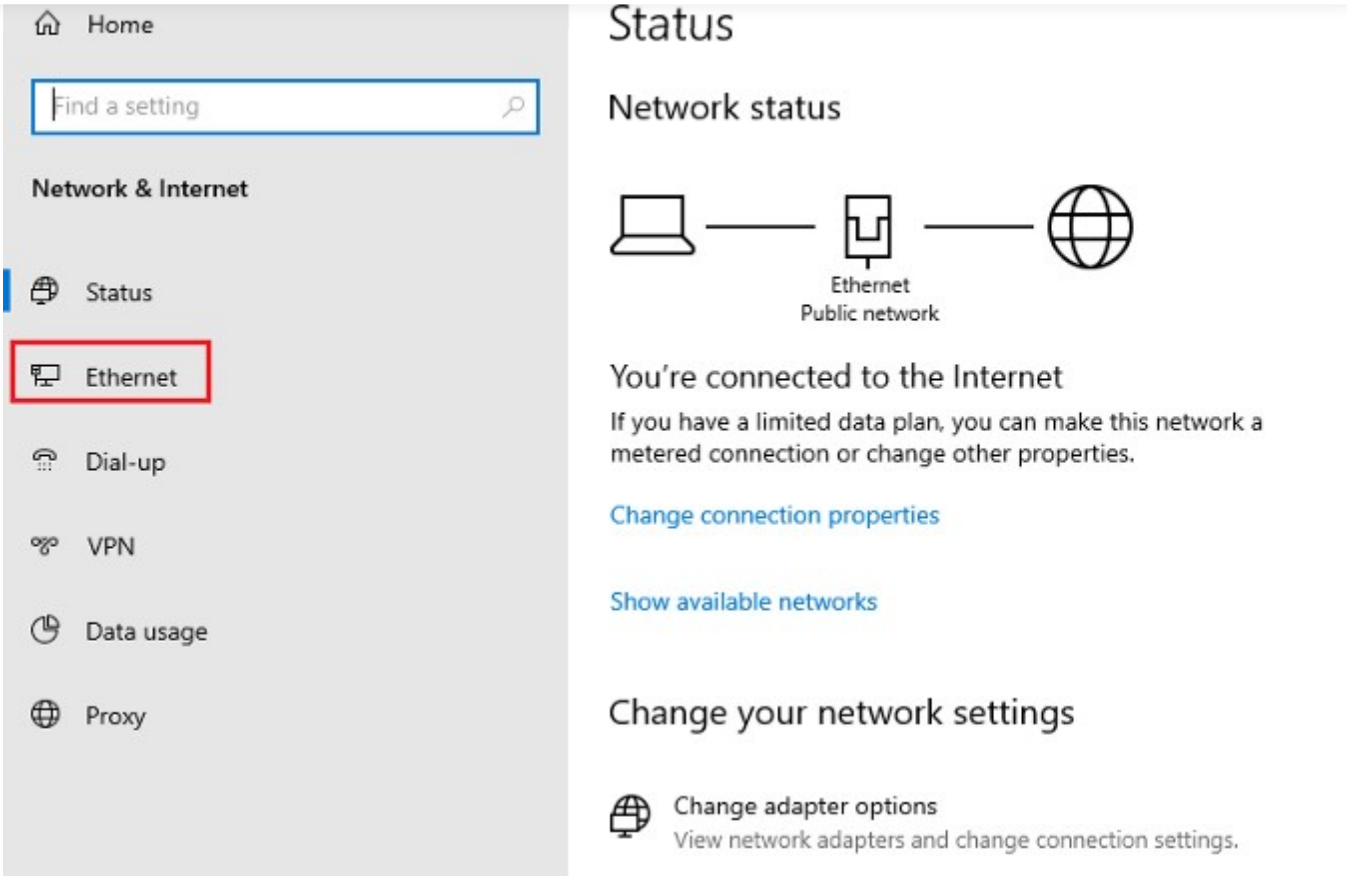
User Machines Join Domain

Now its time to have these machines join the domain. I will show the steps for **ThePunisher** The same steps will have to be done on the other user machine **Spiderman**.

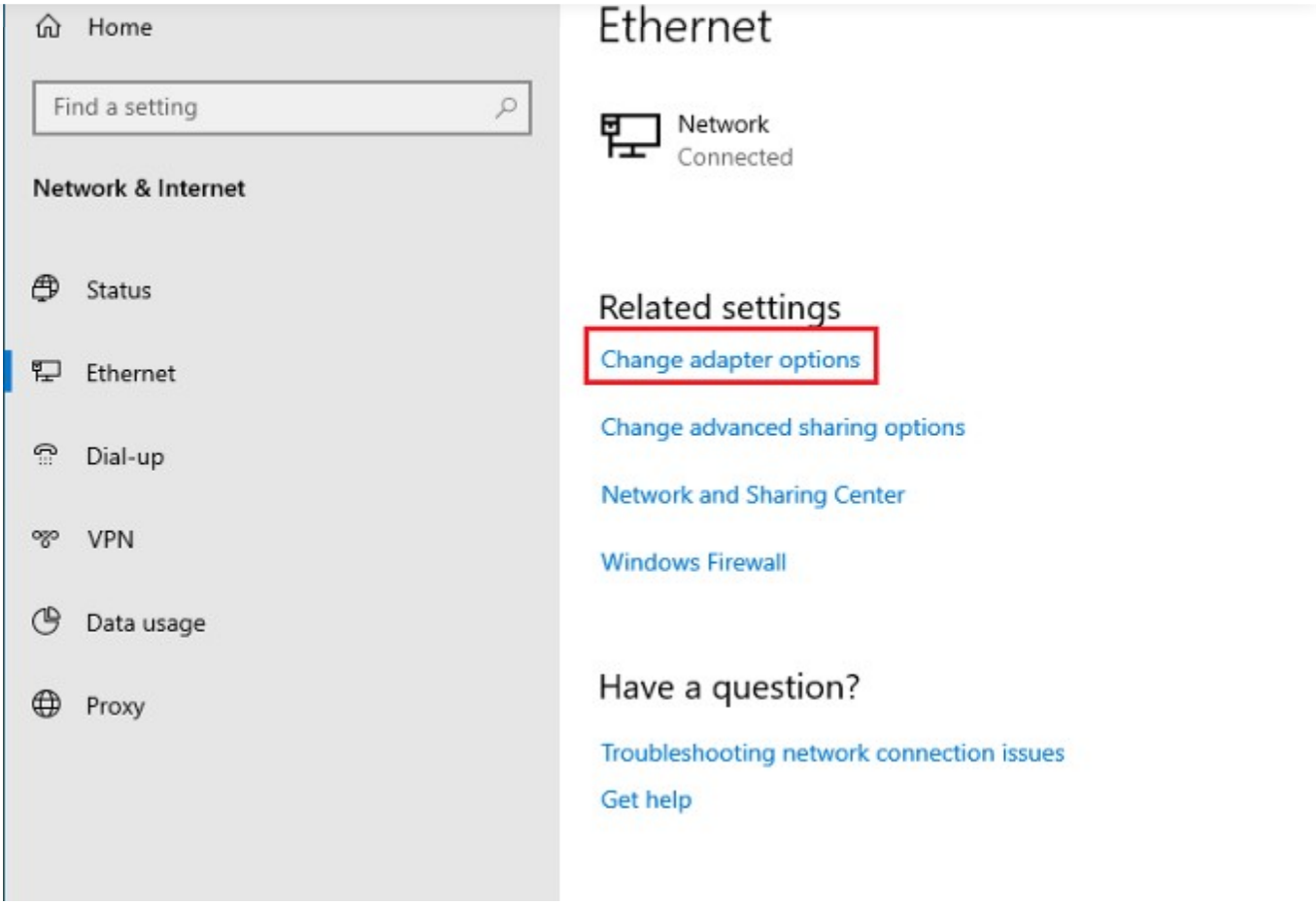
While in **ThePunisher** machine, right-click on the Network icon in the system tray. You will see two options here. Click on the **Open Network & Internet Settings** as shown below.



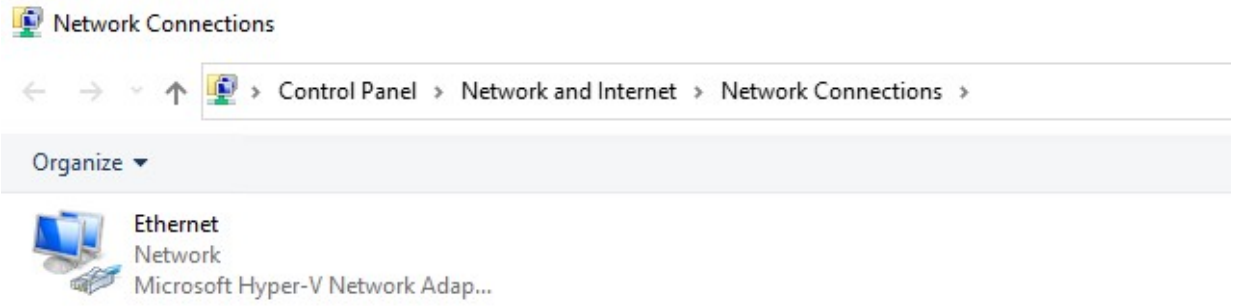
This will open the **Settings** dialog. Click on the **Ethernet** item in left navigation as shown below.



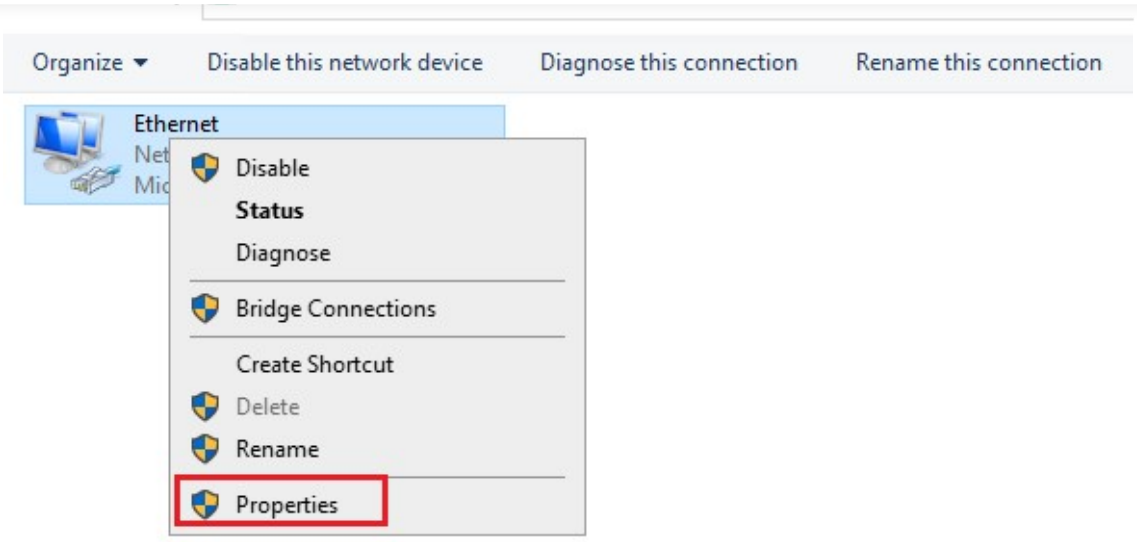
Click on the **Change adapter options**.



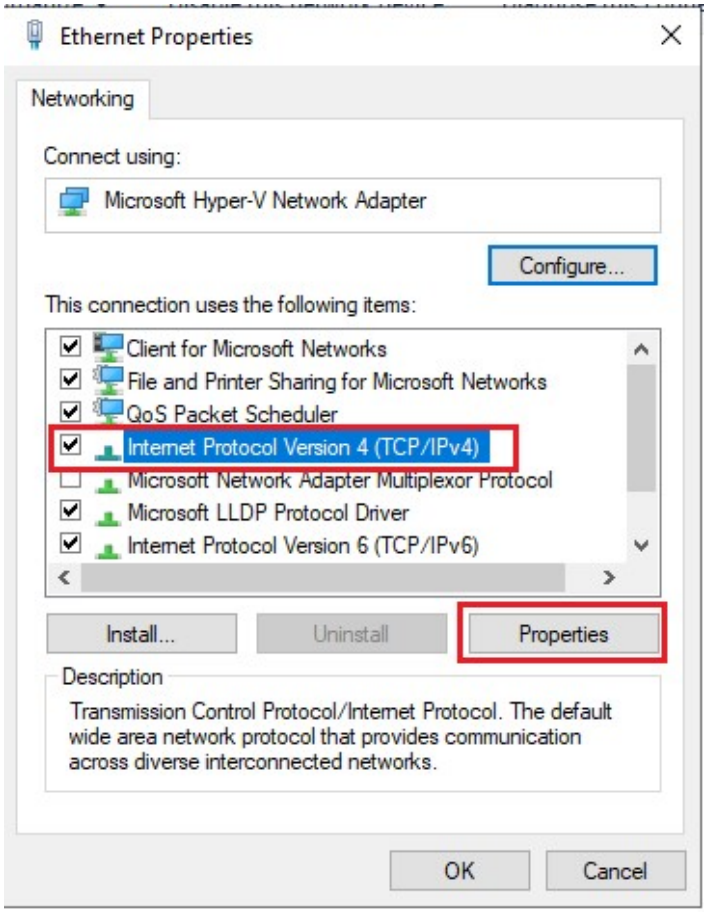
This will bring up the Network Connection dialog showing the Ethernet connection.



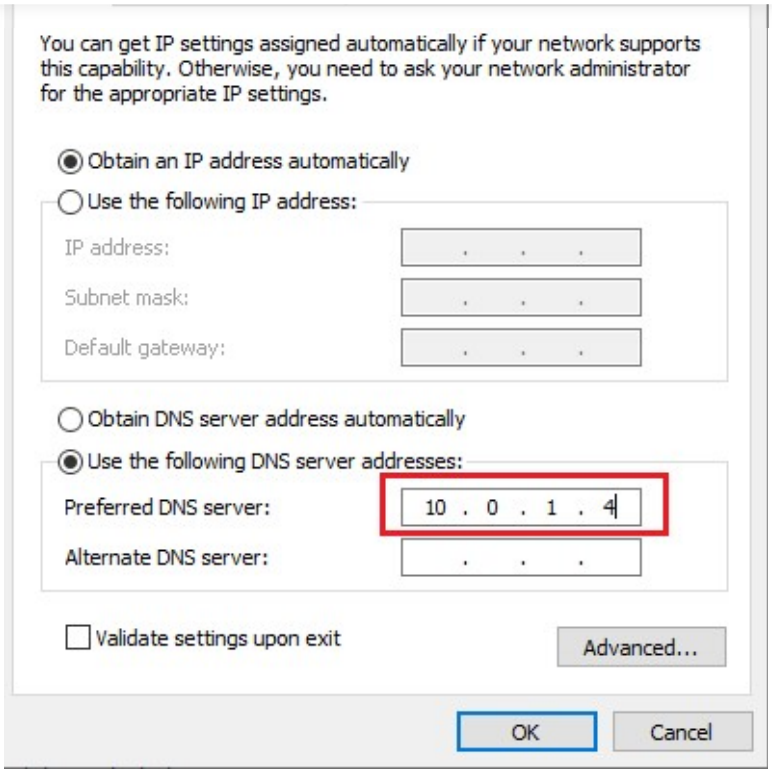
Right-click on the Ethernet and click on the properties menu item.



Select the IP4 from the list and click properties.

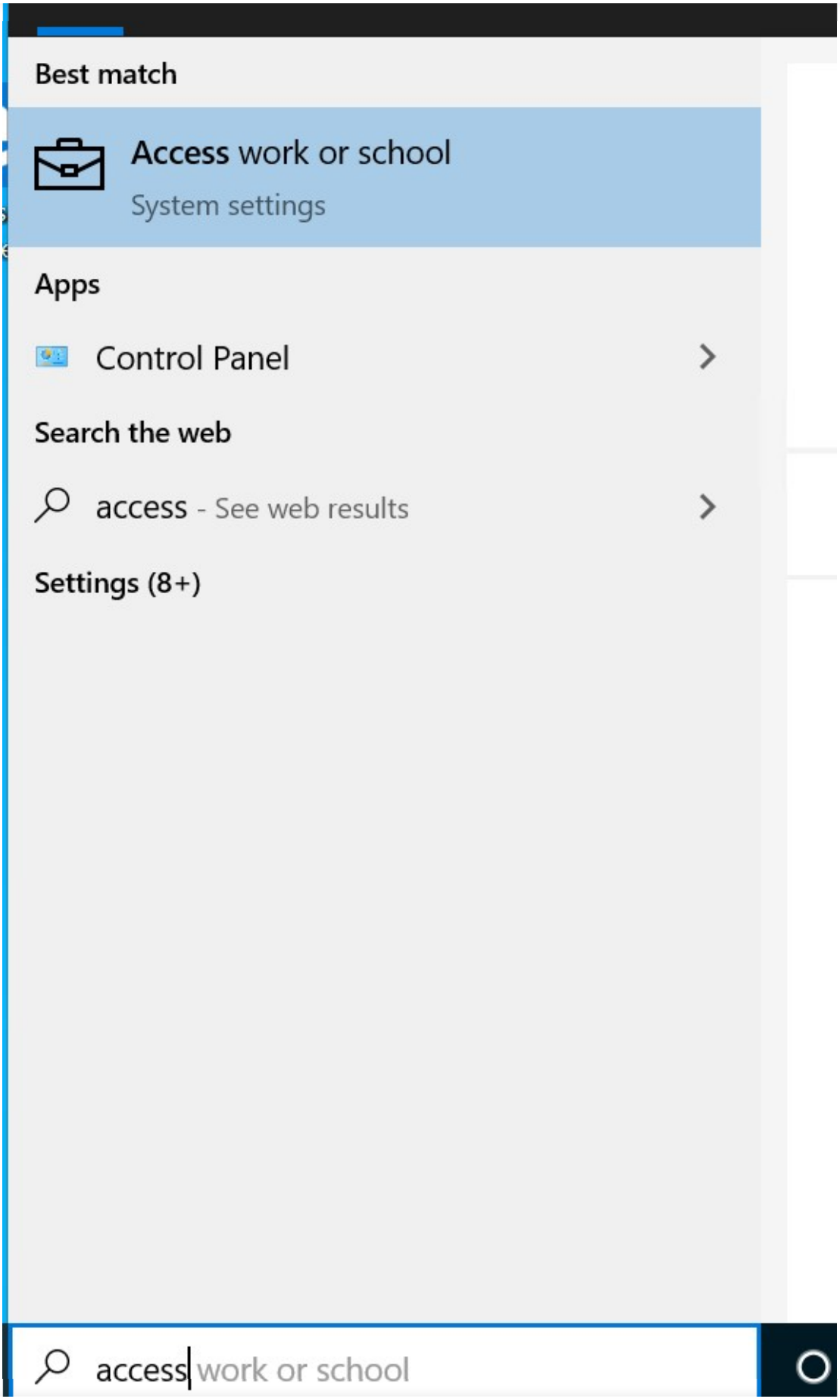


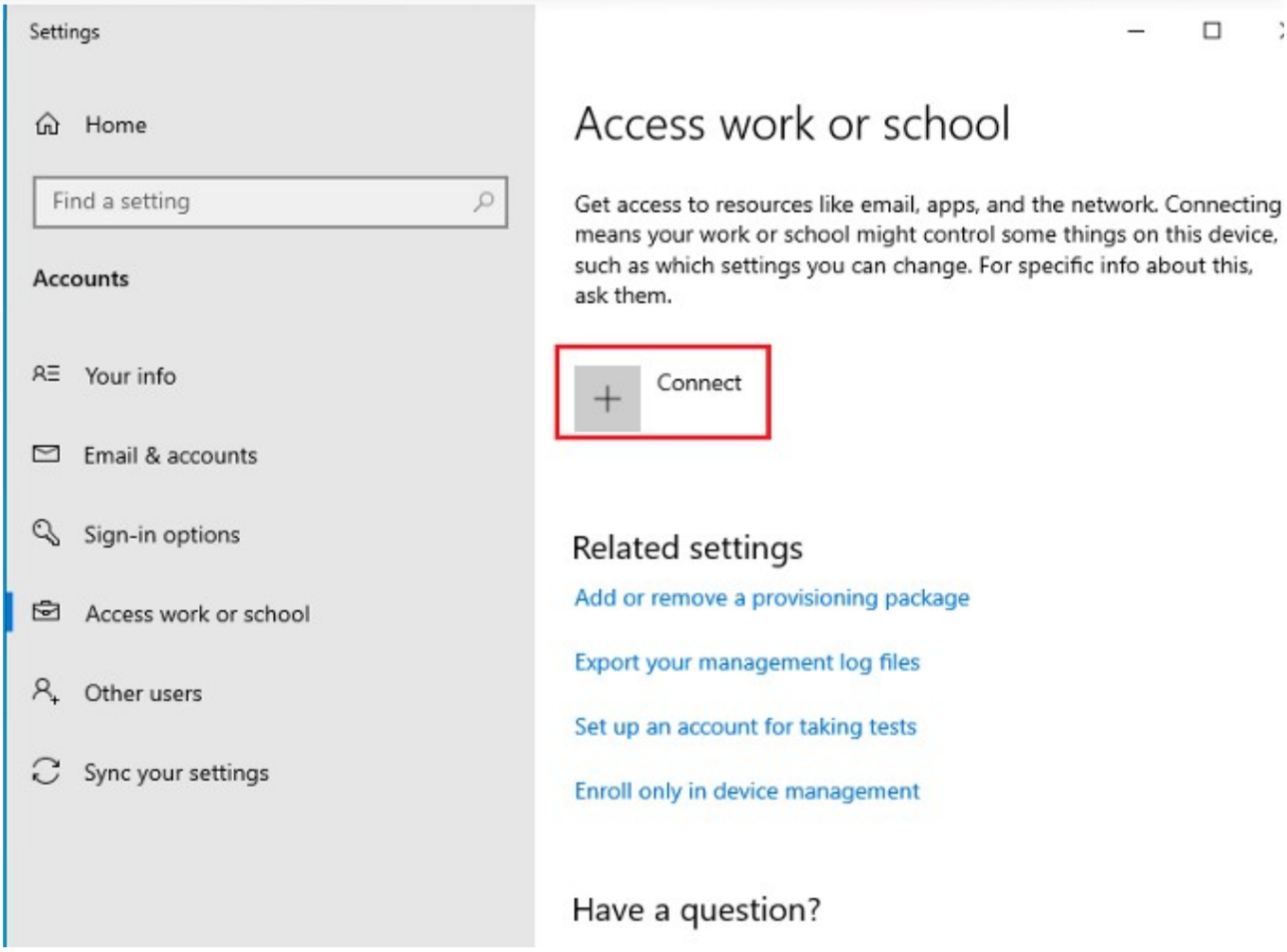
This is where we use the IP address of the domain controller (**10.0.1.4** in my case) as the DN address for this machine.



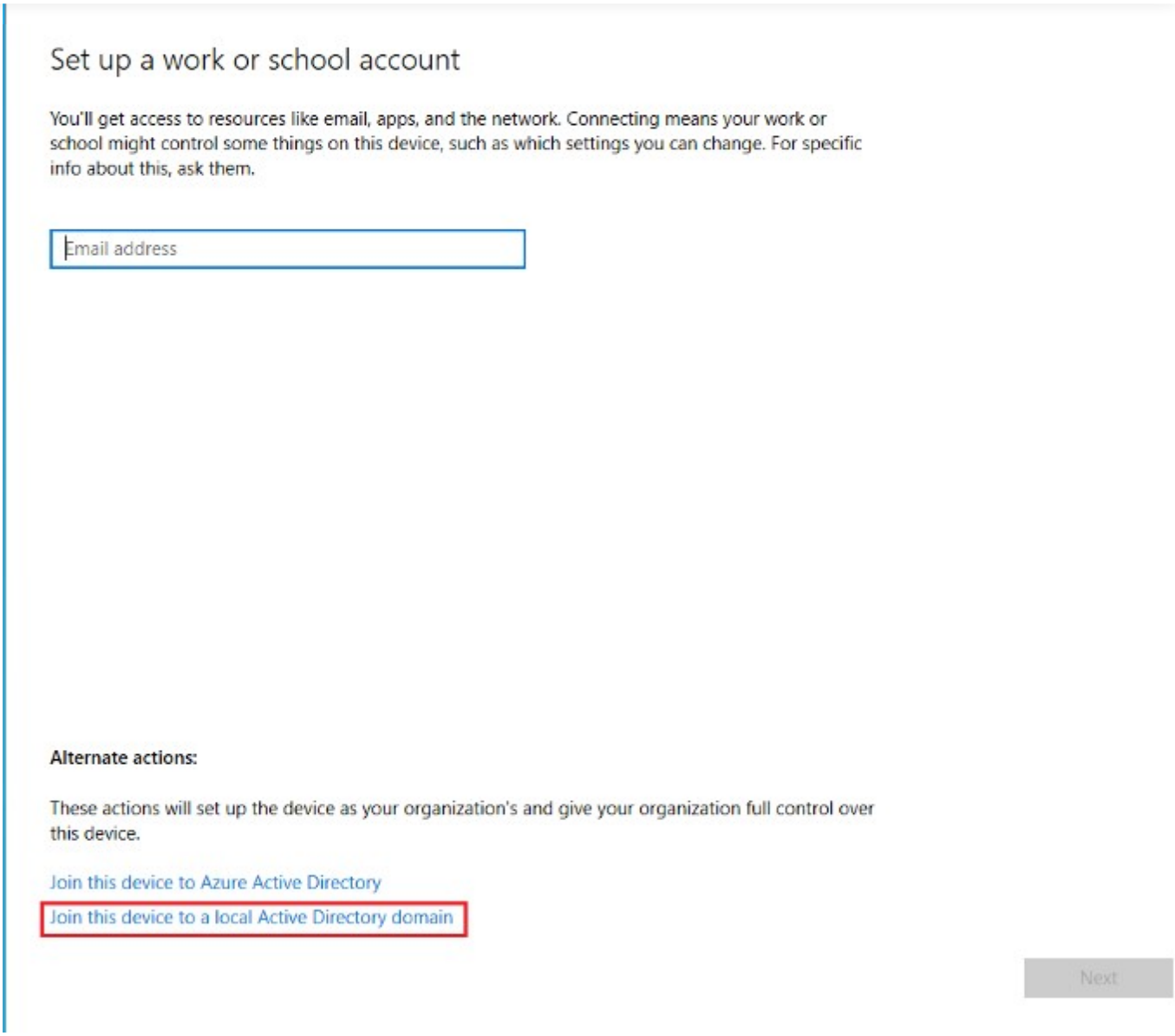
Click OK and close this dialog. At this point, my RDP connection to the VM was lost. I had to restart the VM from Azure portal and log back into the VM using the same local user accoun

Find the **Access work or school** system setting and launch it.

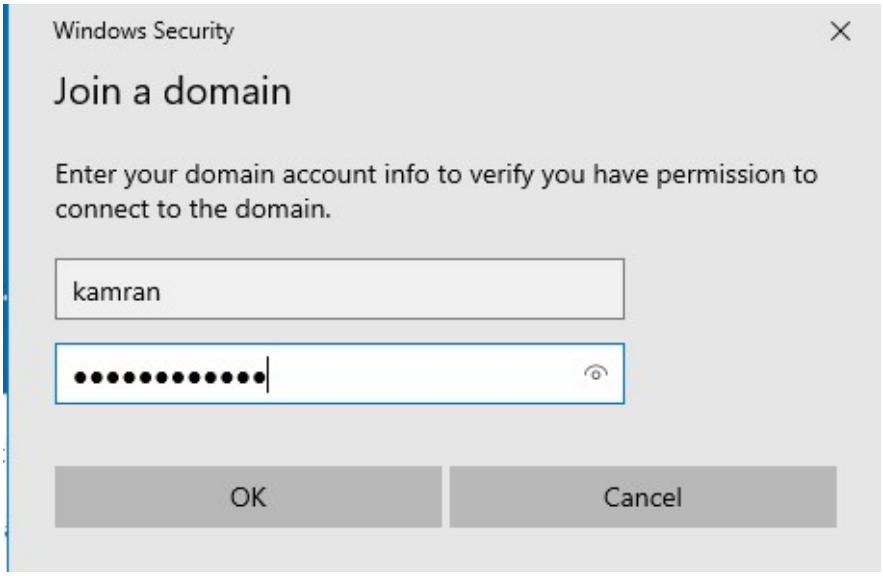




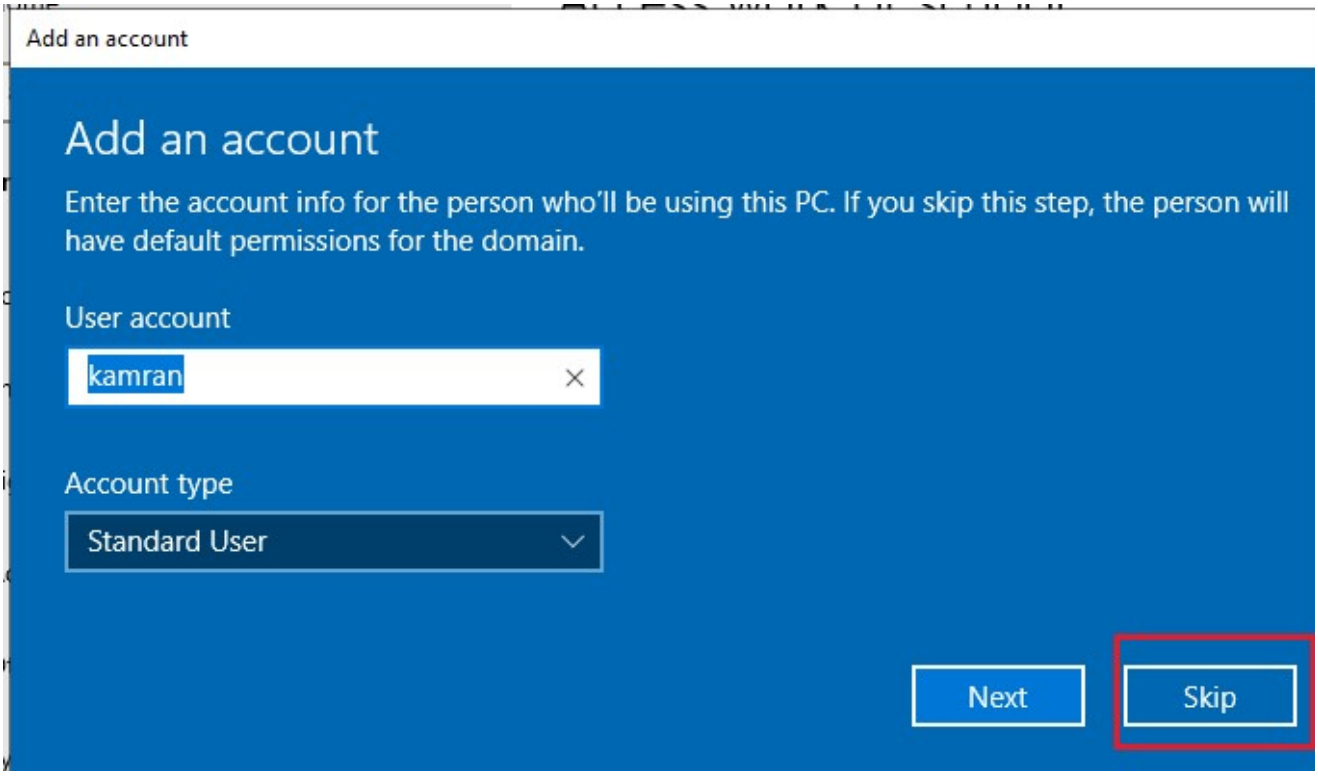
From the next dialog, click the link for **Join this device to a local Active Directory domain**



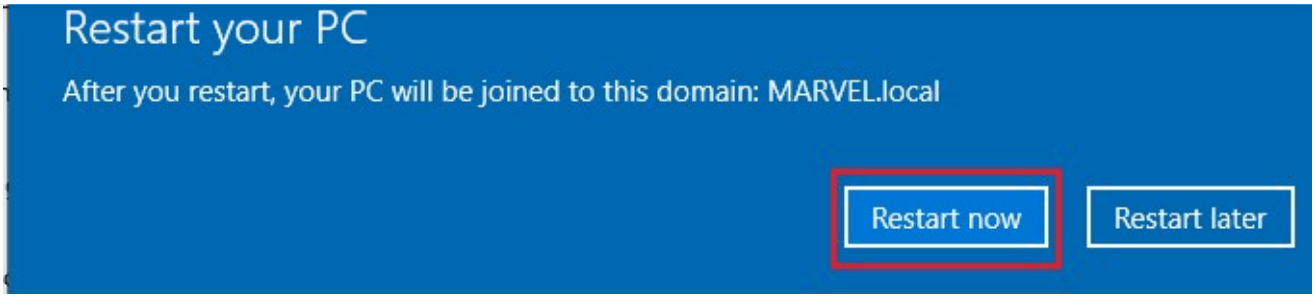
Following dialog will be prompted. Enter **MARVEL.local** as the domain name and click on Next.



Click on the Skip on the next dialog.

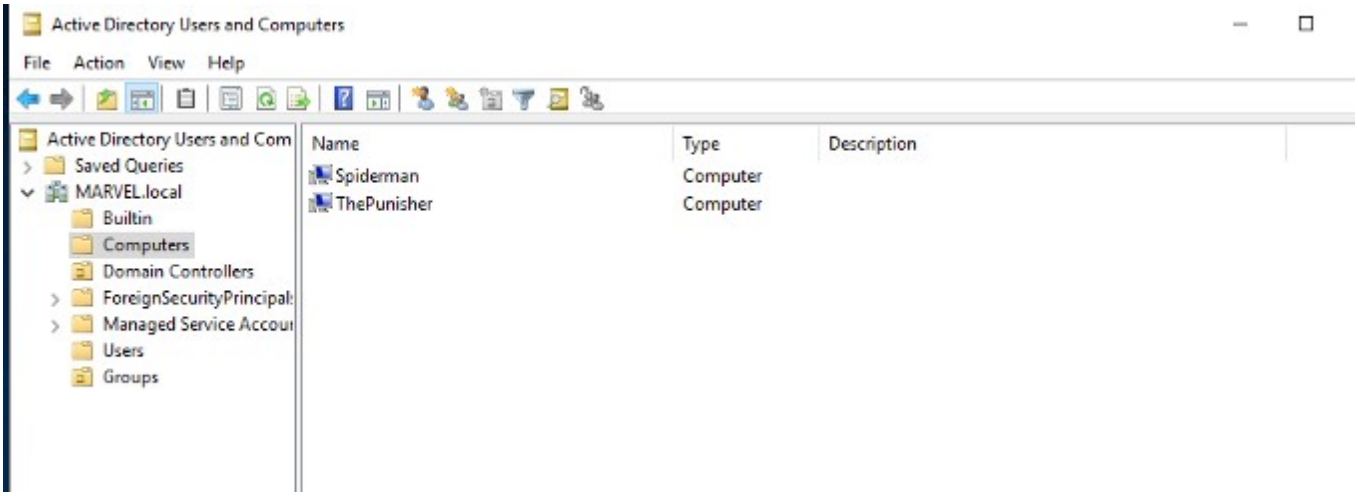


Finally choose to **Restart now**.



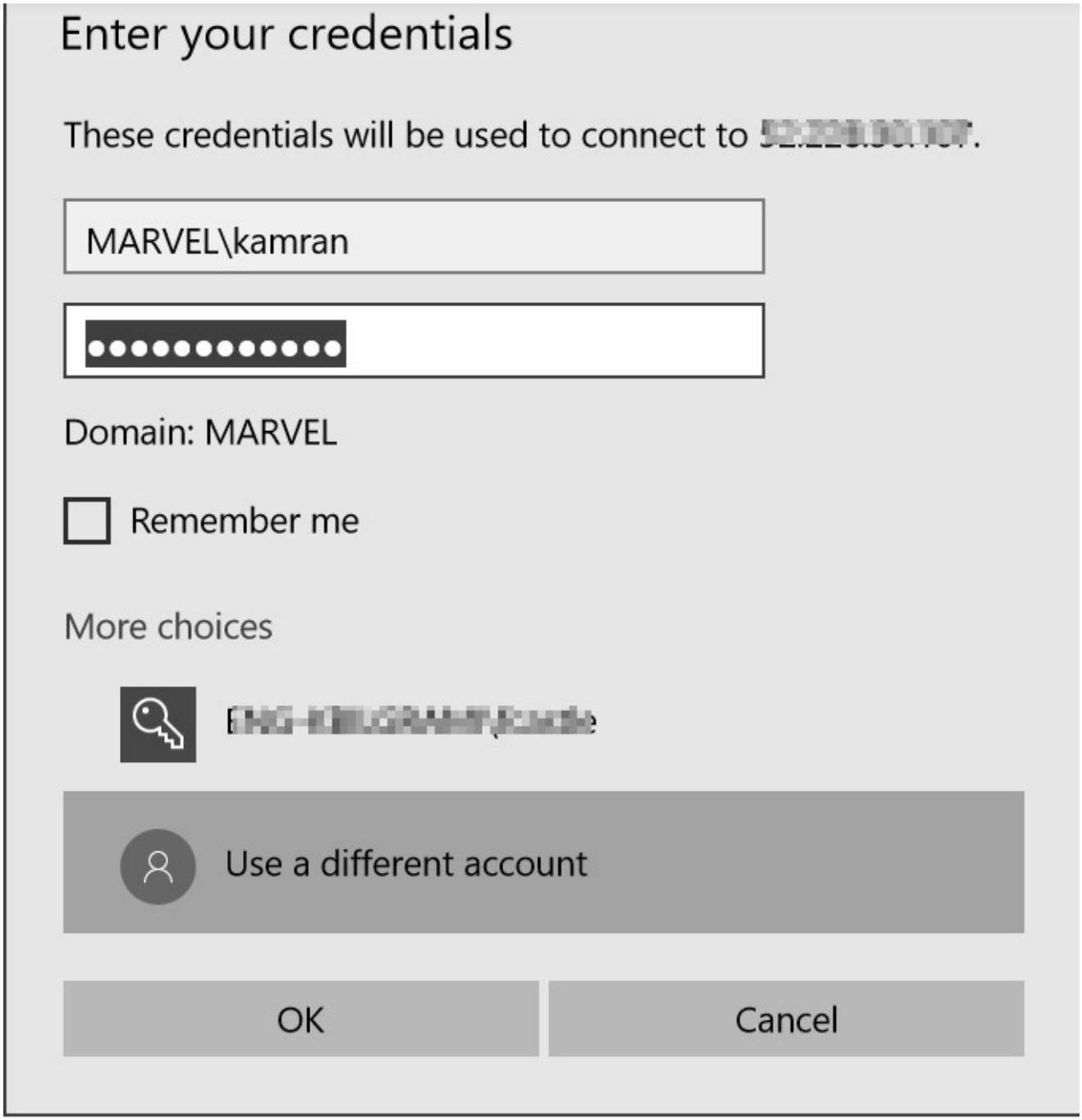
Now repeat the same steps for the other user machine Spiderman to have it join the domain

At this point, if we login to the Domain Controller, we should see both the user computers listed under the **MARVEL.local** domain as shown below.

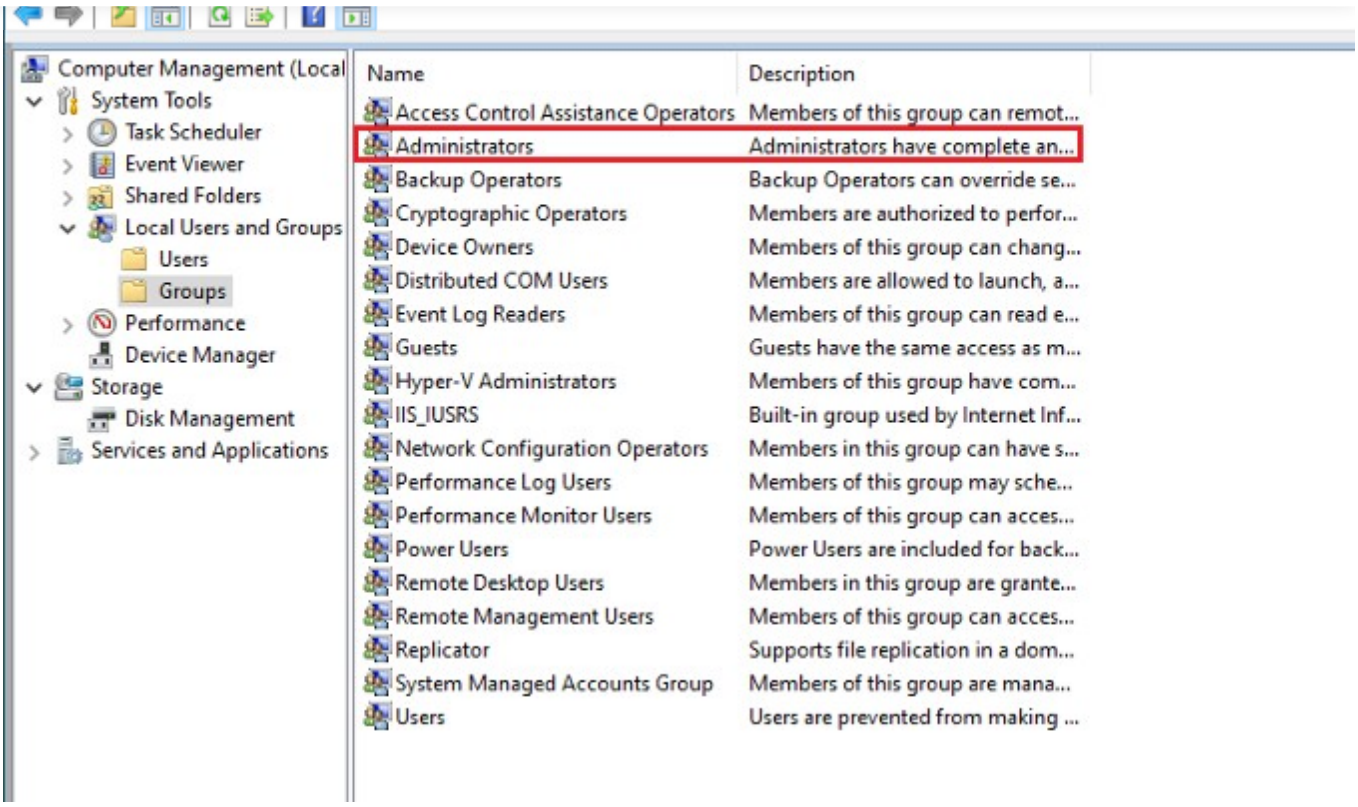


Configuring Domain Users to User-Machines

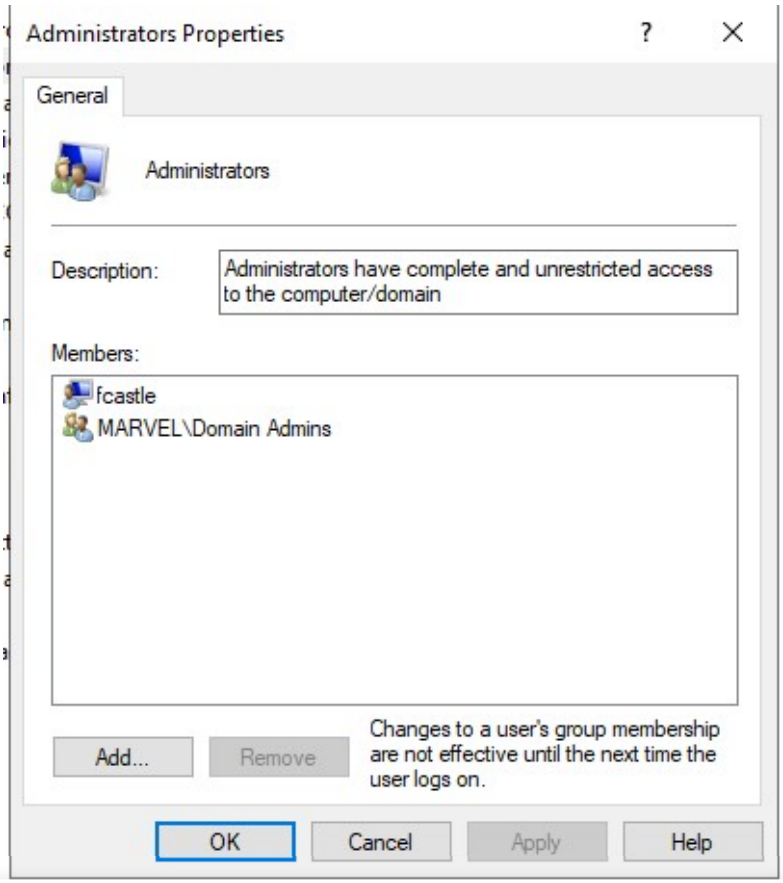
We have created domain users but not yet set up these against any user machines yet. Let's login to the **ThePunsiher** first as a domain administrator to do that.

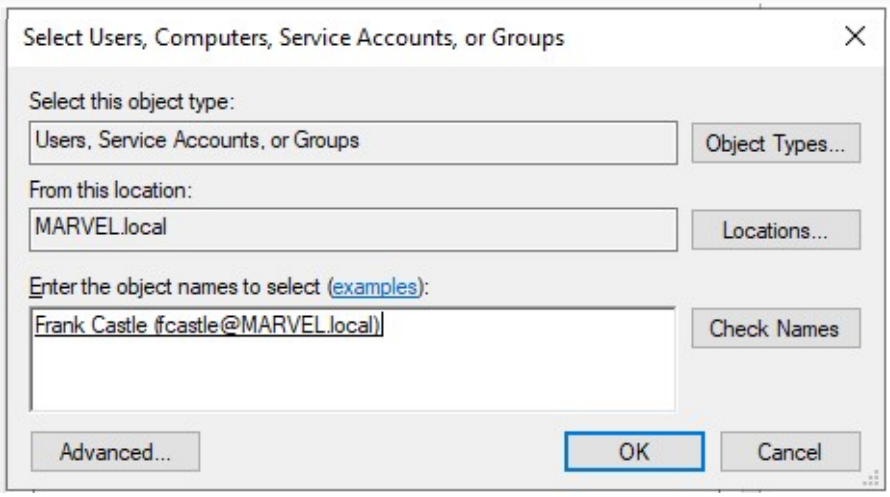


Go to Computer Management -> Groups -> Administrators and double click.

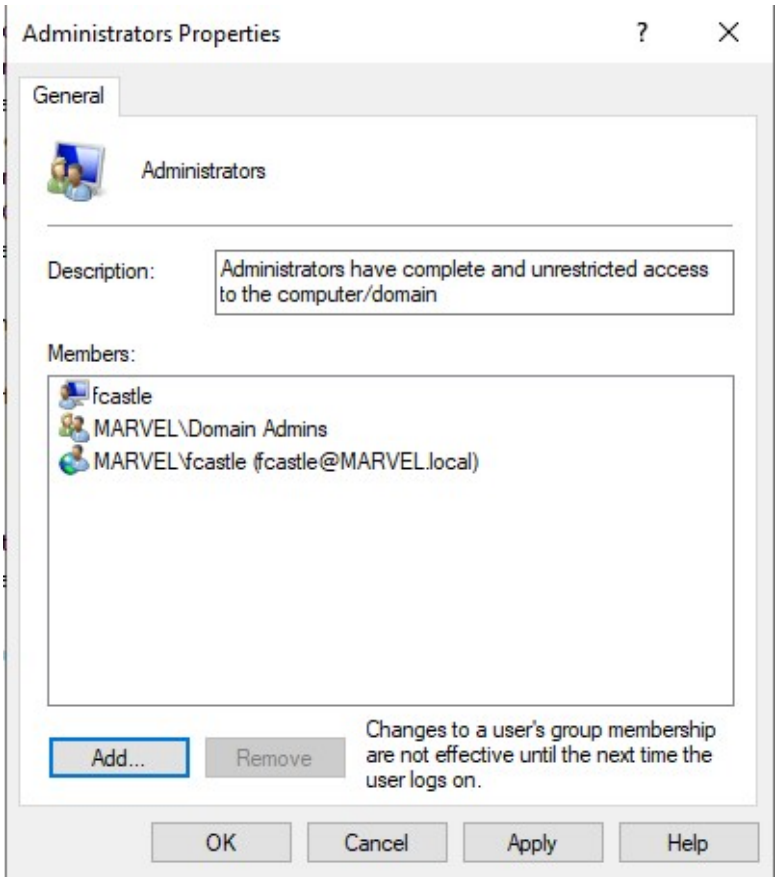


It will show existing users in this group. Click **Add** here.

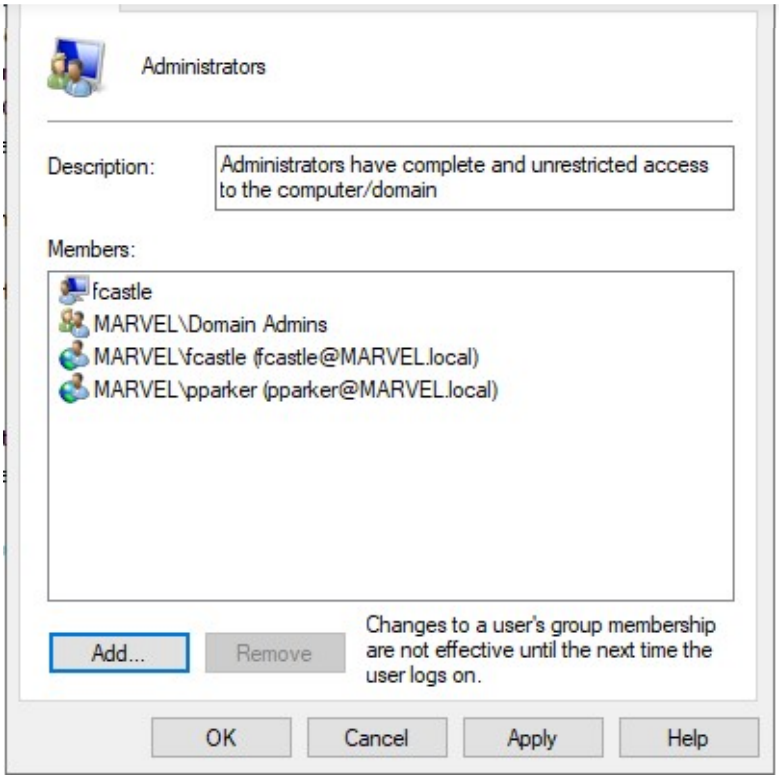




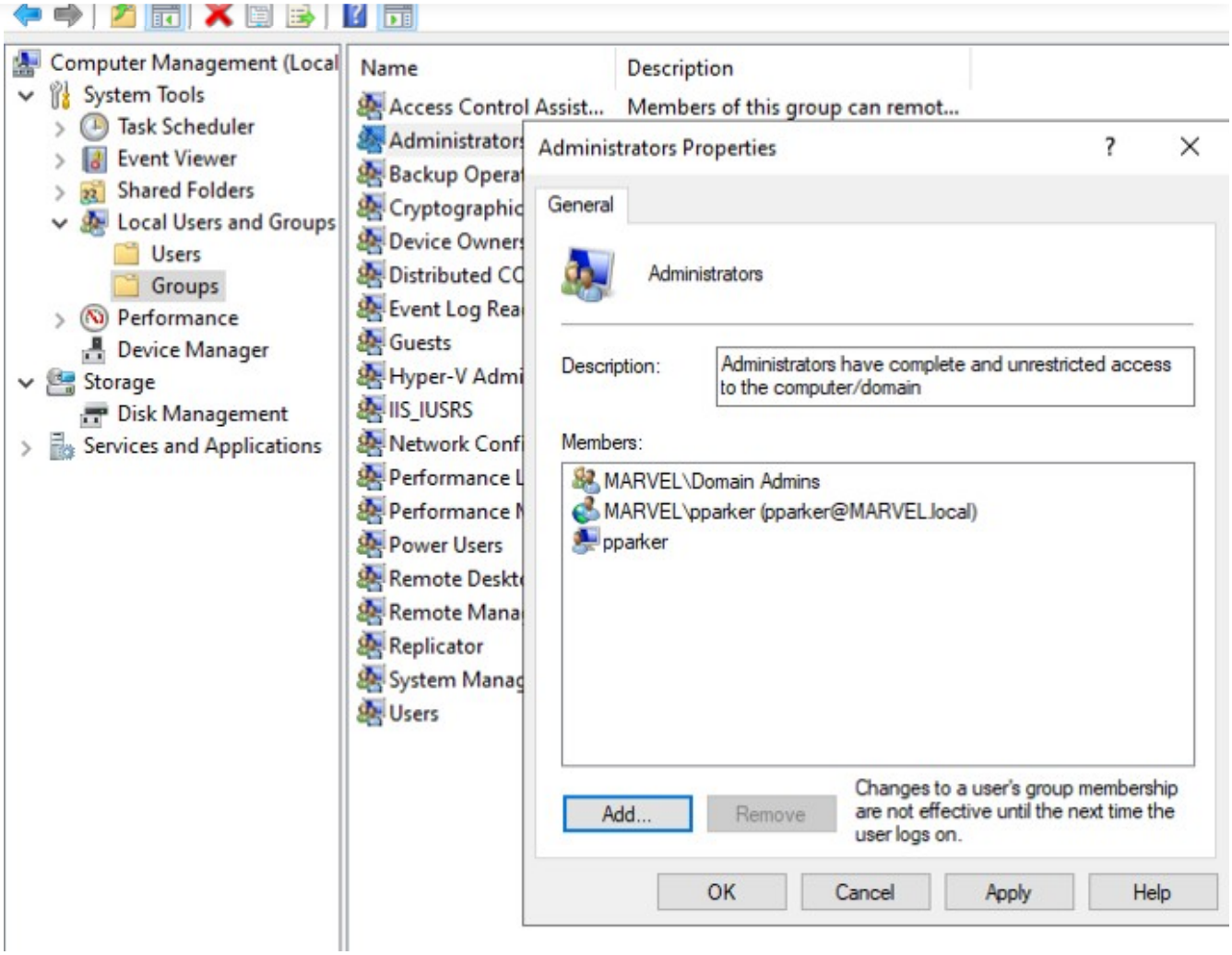
This will add that user as local Administrator.



Repeat the same steps for domain user Petre Parker.



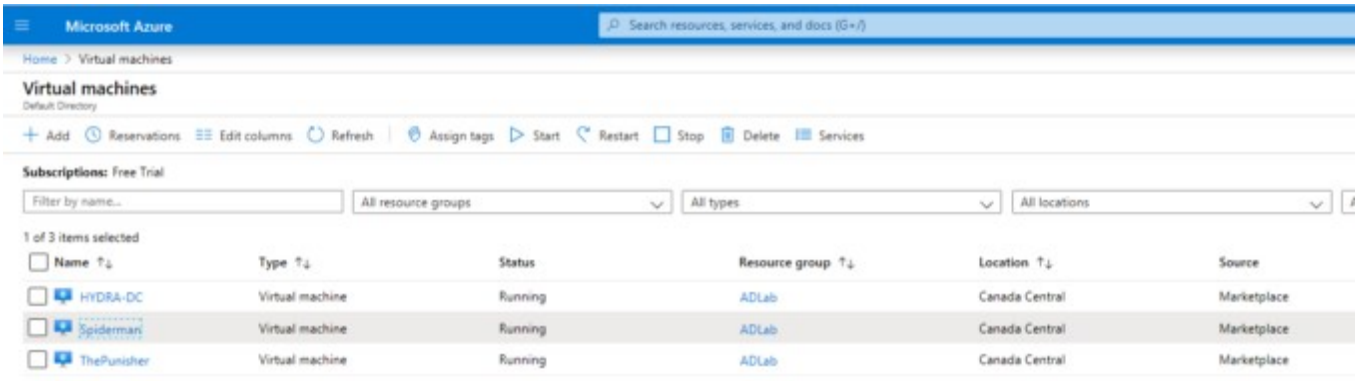
Let's login to the **spiderman** machine as a domain administrator and add the **Marvel\ppar** as the local admin.

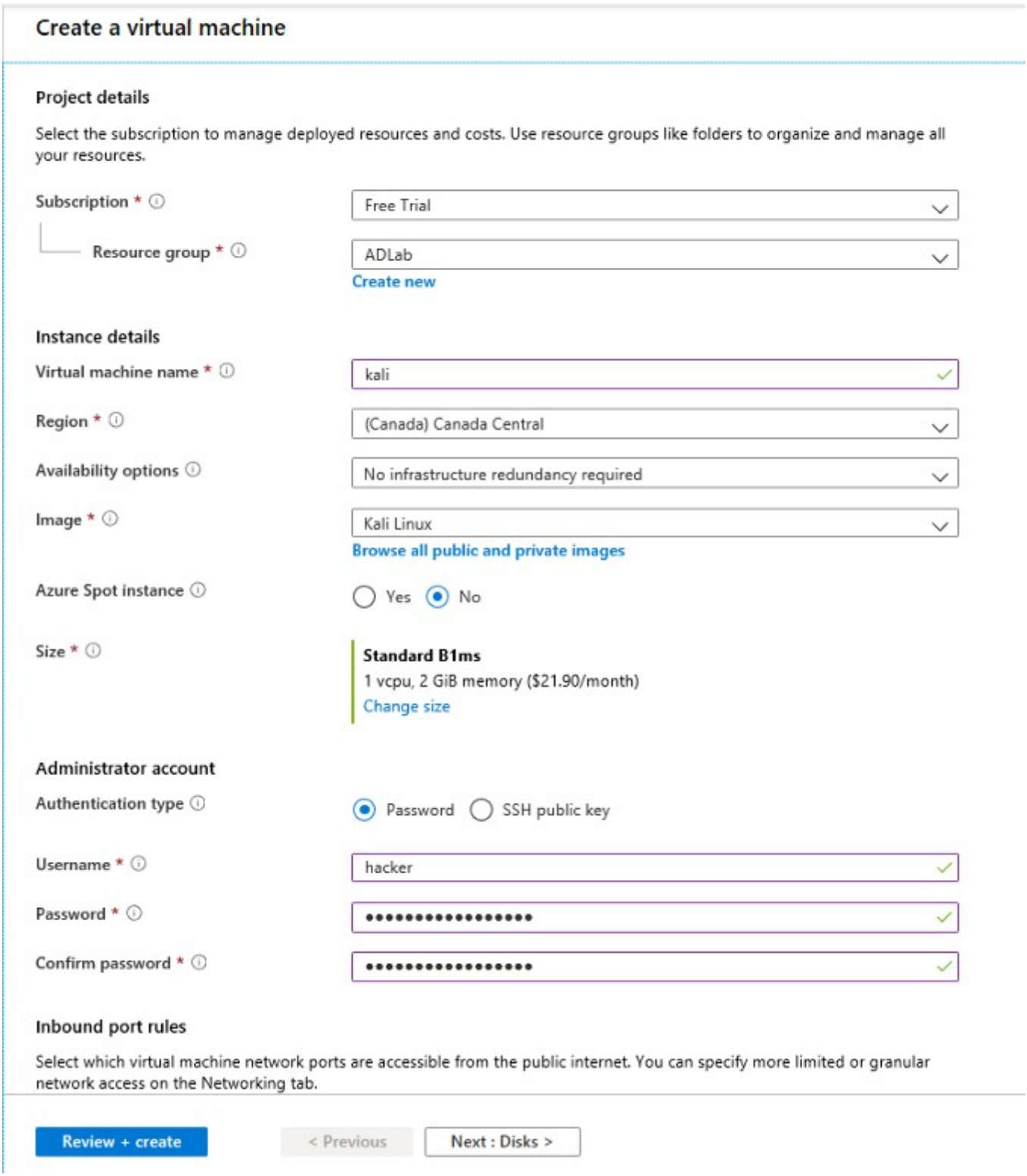


Our Domain setup is all complete now. Last thing to do it add a Kali Linux machine here too.

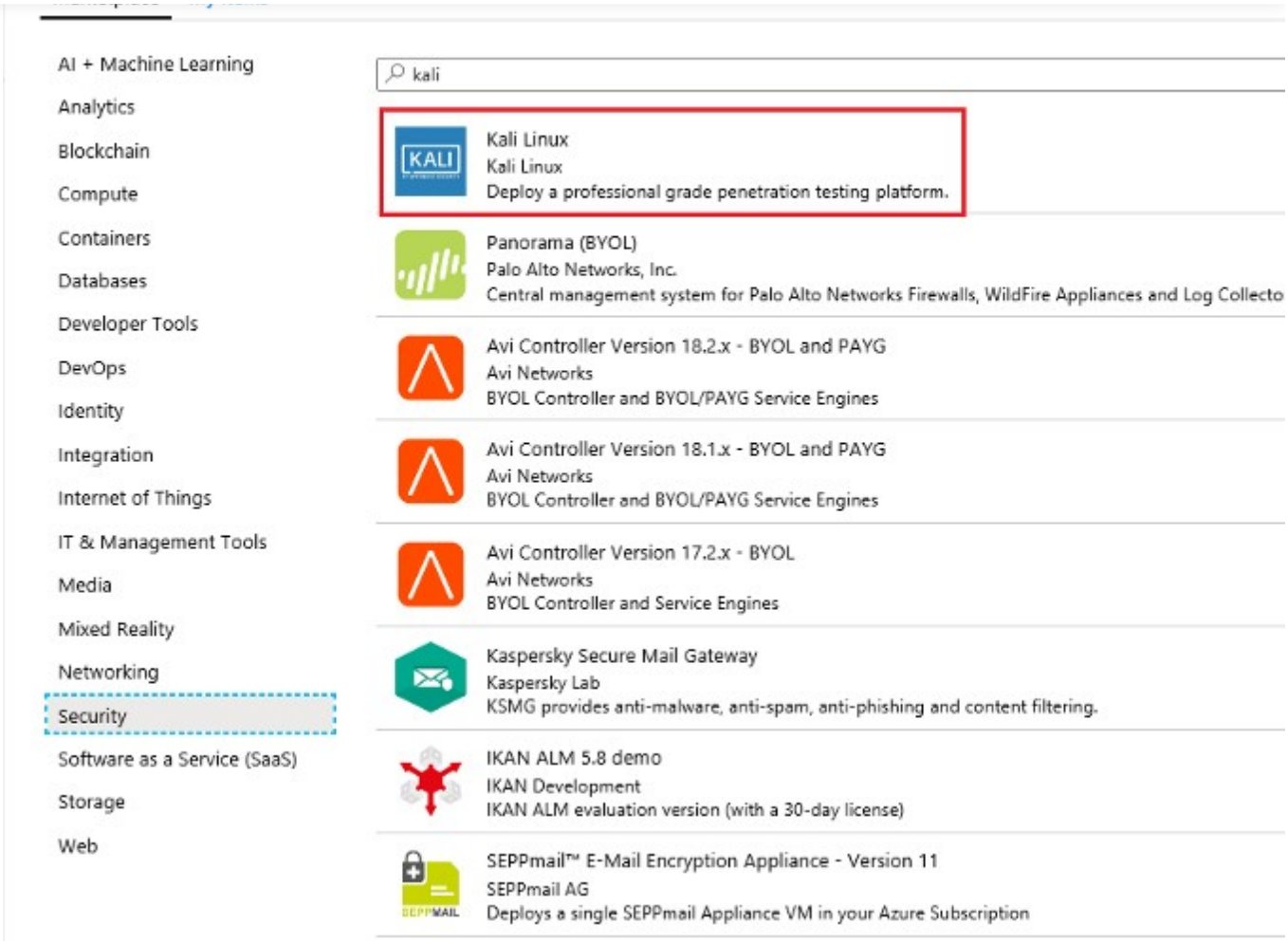
Setting up Kali Linux

Log in to the Azure Portal, browse to Virtual machines section and click on Add button.

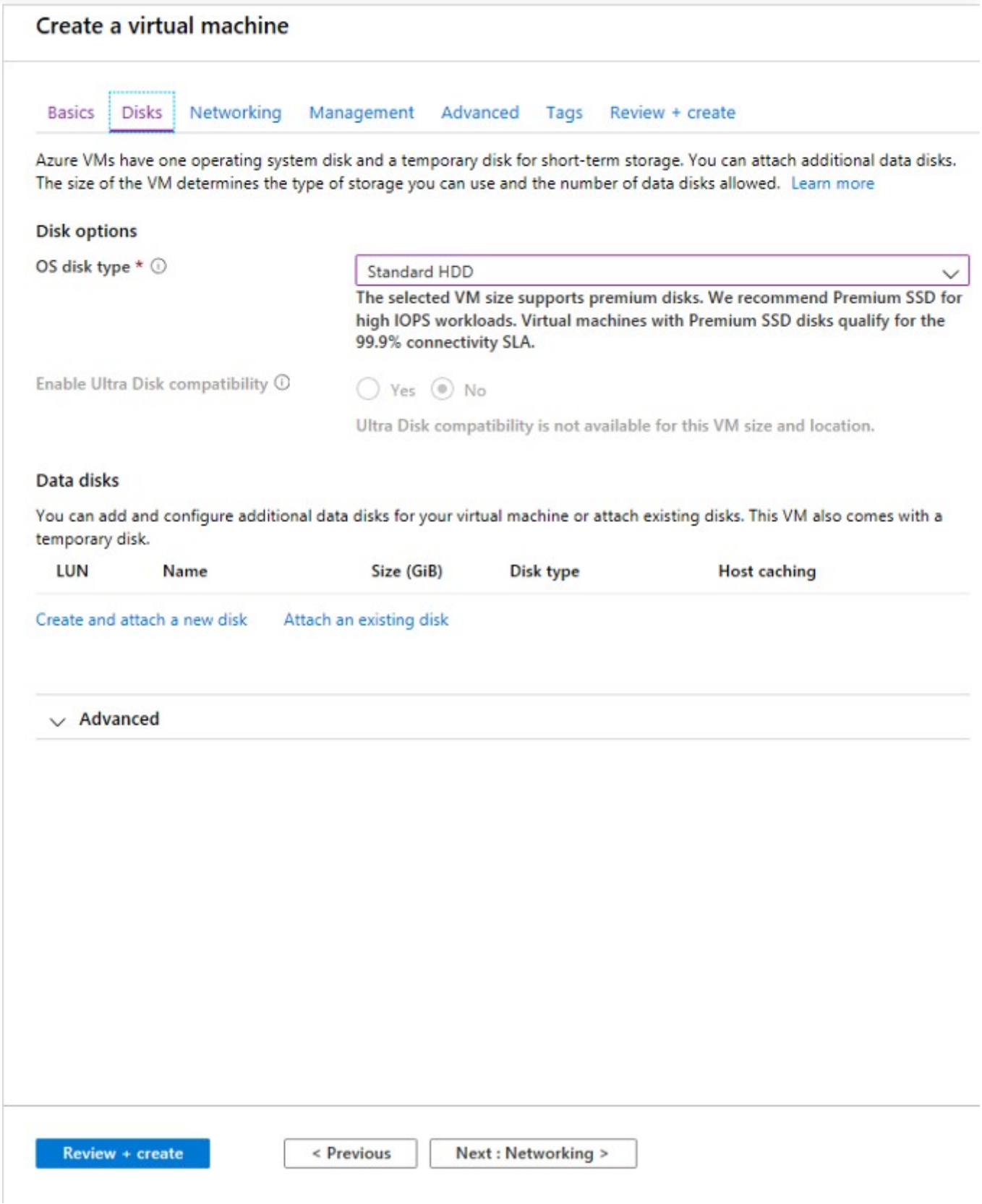




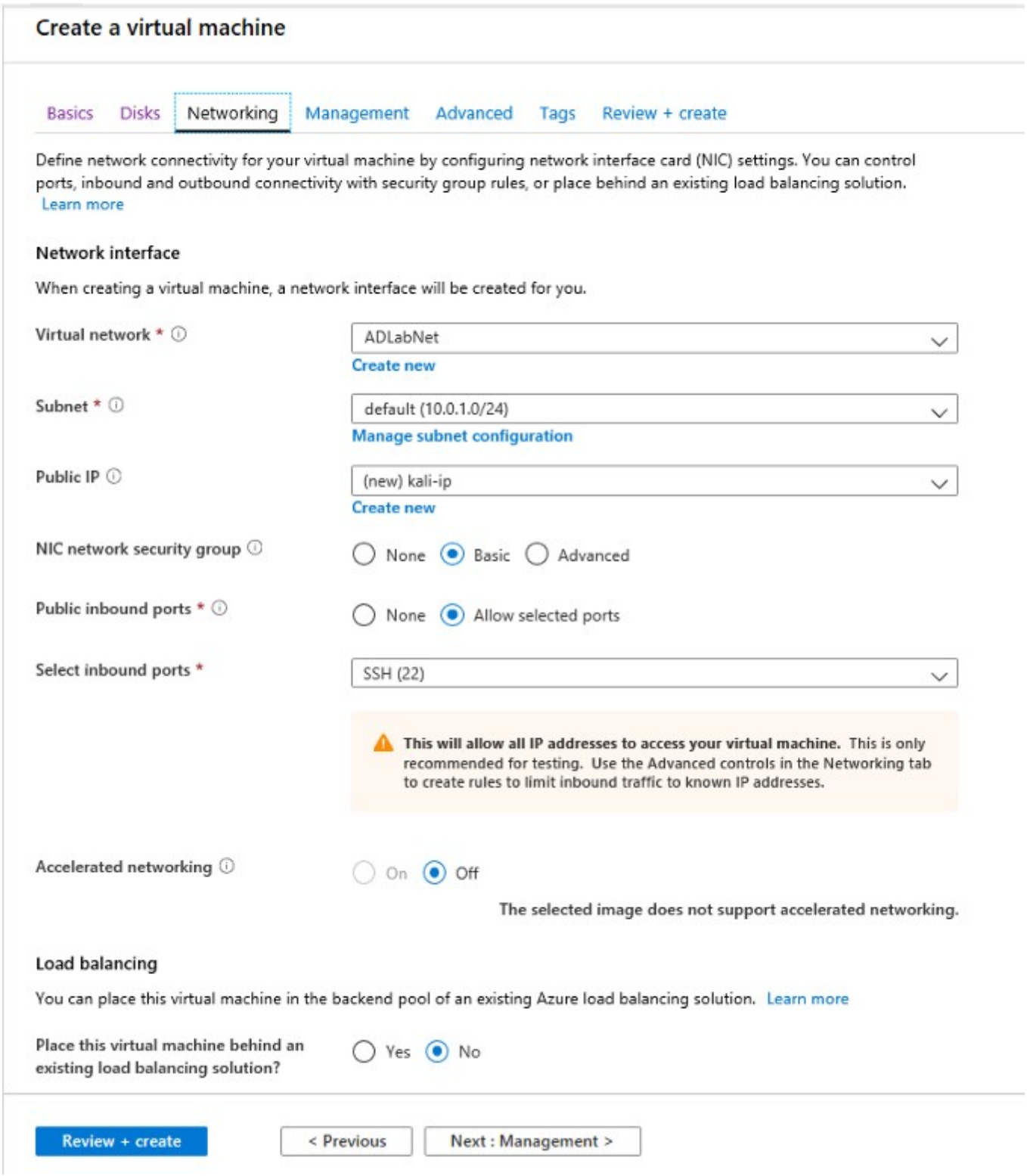
Important thing to note is that there is a Kali Linux image available in the market place that can use.



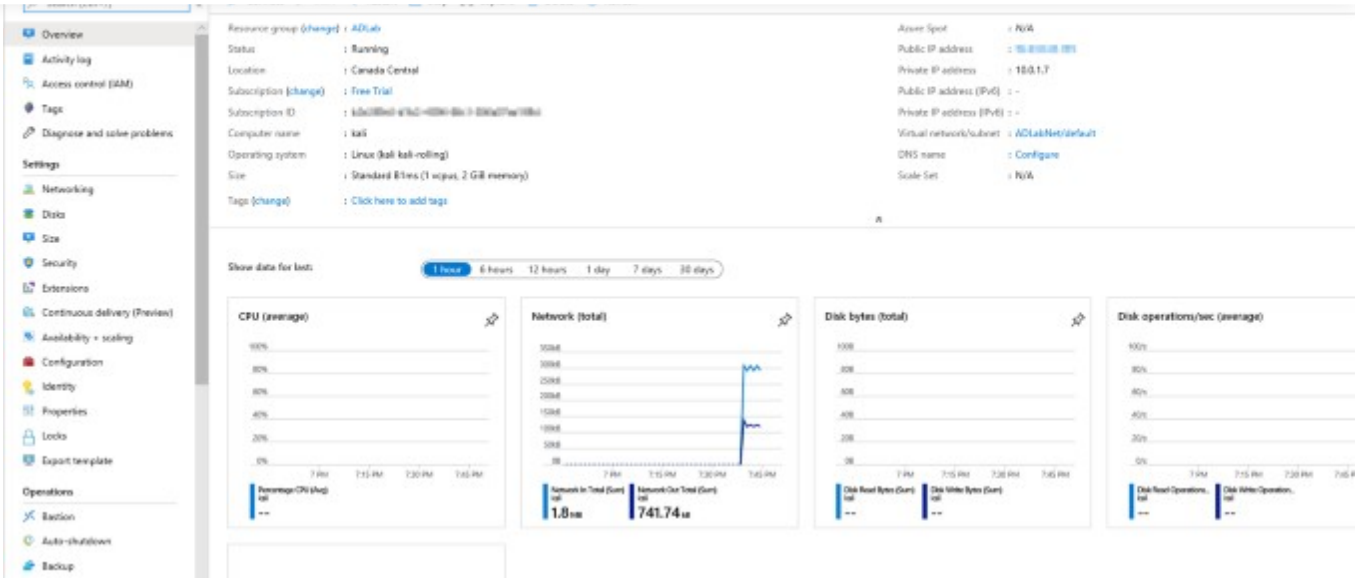
Use the Standard HDD disk.



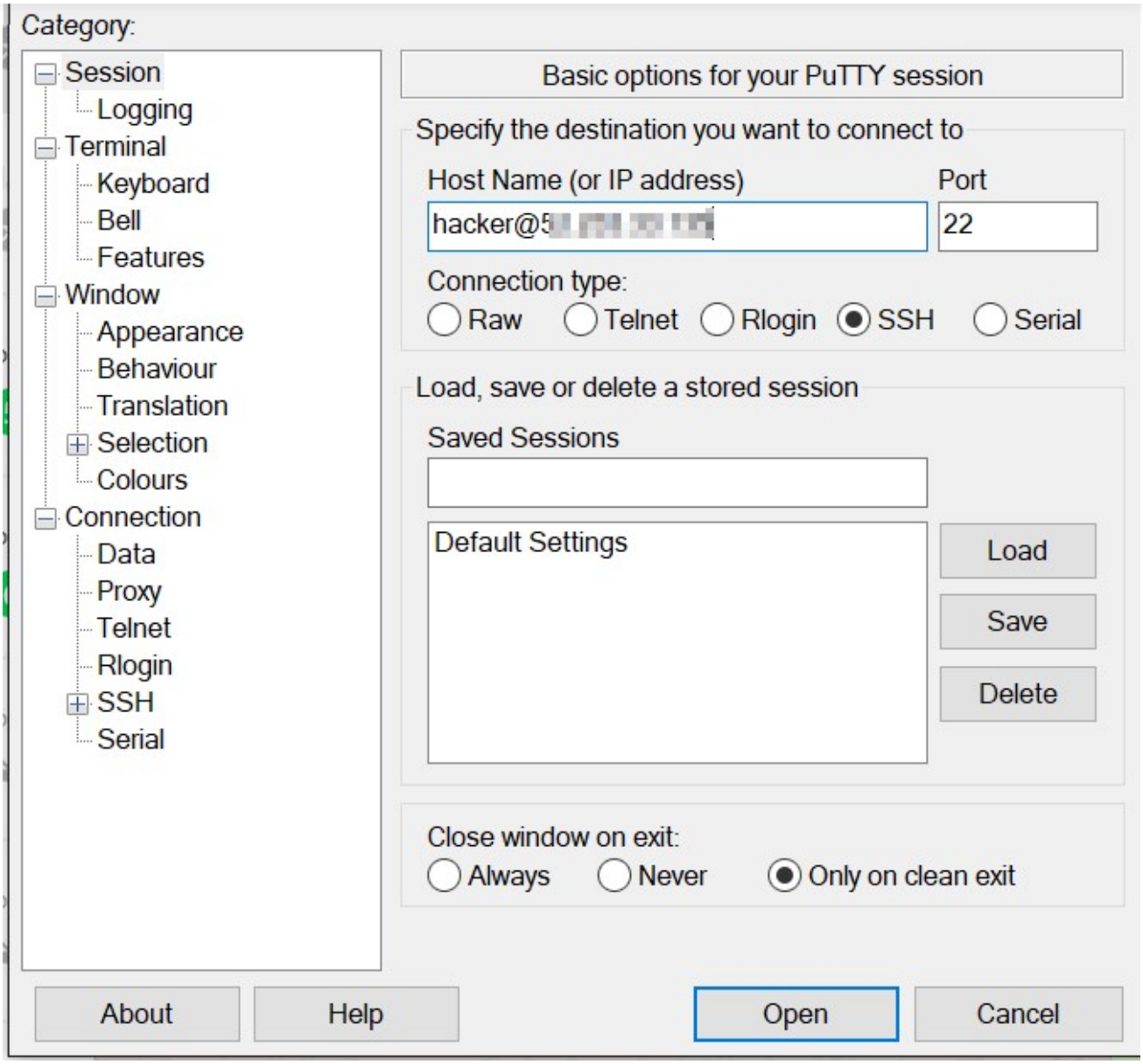
Use the existing Virtual network ADLabNet.



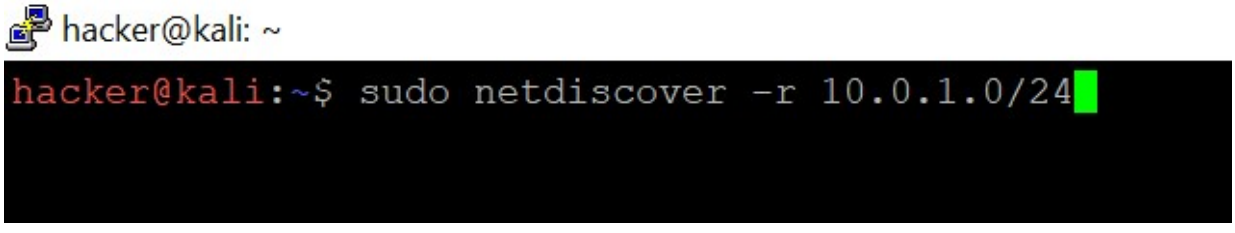
Following the rest of the steps we should have a Kali Linux virtual machine.



I use putty to connect to the Kali machine using SSH.



Once I logged in, I ran netdiscover utility to find the machines.



Its results, as expected, came back with the IP addresses of the domain controller and two u
machines.

```
4 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 168

  IP            At MAC Address      Count      Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
10.0.1.1        12:34:56:78:9a:bc       1       42  Unknown vendor
10.0.1.4        12:34:56:78:9a:bc       1       42  Unknown vendor
10.0.1.5        12:34:56:78:9a:bc       1       42  Unknown vendor
10.0.1.6        12:34:56:78:9a:bc       1       42  Unknown vendor
```

Nmap scan against the domain controller is shown below.

```
hacker@kali: ~
hacker@kali:~$ nmap -A -T4 10.0.1.4 -Pn
Starting Nmap 7.70 ( https://nmap.org ) at 2020-01-05 19:51 EST
Nmap scan report for 10.0.1.4
Host is up (0.0020s latency).
Not shown: 988 filtered ports
PORT     STATE SERVICE       VERSION
53/tcp   open  domain?
| fingerprint-strings:
|   DNSVersionBindReqTCP:
|     version
|_    bind
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2020-01-06 00:52:10Z)
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: MARVEL.local0., Site: Default-First-Site-Name)
| ssl-cert: Subject: commonName=HYDRA-DC.MARVEL.local
| Subject Alternative Name: othername:<unsupported>, DNS:HYDRA-DC.MARVEL.local
| Not valid before: 2020-01-05T08:10:30
|_Not valid after:  2021-01-04T08:10:30
|_ssl-date: 2020-01-06T00:54:22+00:00; 0s from scanner time.
445/tcp  open  microsoft-ds?
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp  open  ssl/ldap      Microsoft Windows Active Directory LDAP (Domain: MARVEL.local0., Site: Default-First-Site-Name)
| ssl-cert: Subject: commonName=HYDRA-DC.MARVEL.local
| Subject Alternative Name: othername:<unsupported>, DNS:HYDRA-DC.MARVEL.local
| Not valid before: 2020-01-05T08:10:30
|_Not valid after:  2021-01-04T08:10:30
|_ssl-date: 2020-01-06T00:54:21+00:00; 0s from scanner time.
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP (Domain: MARVEL.local0., Site: Default-First-Site-Name)
| ssl-cert: Subject: commonName=HYDRA-DC.MARVEL.local
| Subject Alternative Name: othername:<unsupported>, DNS:HYDRA-DC.MARVEL.local
| Not valid before: 2020-01-05T08:10:30
|_Not valid after:  2021-01-04T08:10:30
|_ssl-date: 2020-01-06T00:54:21+00:00; 0s from scanner time.
3269/tcp open  ssl/ldap      Microsoft Windows Active Directory LDAP (Domain: MARVEL.local0., Site: Default-First-Site-Name)
| ssl-cert: Subject: commonName=HYDRA-DC.MARVEL.local
| Subject Alternative Name: othername:<unsupported>, DNS:HYDRA-DC.MARVEL.local
| Not valid before: 2020-01-05T08:10:30
|_Not valid after:  2021-01-04T08:10:30
|_ssl-date: 2020-01-06T00:54:21+00:00; 0s from scanner time.
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| ssl-cert: Subject: commonName=HYDRA-DC.MARVEL.local
| Not valid before: 2020-01-02T22:43:42
|_Not valid after:  2020-07-03T22:43:42
```

Nmap scan for the two user machines is shown below.

```
Host is up (0.0029s latency).
Not shown: 998 filtered ports
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| ssl-cert: Subject: commonName=ThePunisher.MARVEL.local
| Not valid before: 2020-01-04T21:28:52
|_Not valid after:  2020-07-05T21:28:52
|_ssl-date: 2020-01-06T00:56:54+00:00; 0s from scanner time.
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.33 seconds
hacker@kali:~$ nmap -A -T4 10.0.1.6 -Pn
Starting Nmap 7.70 ( https://nmap.org ) at 2020-01-05 19:57 EST
Nmap scan report for 10.0.1.6
Host is up (0.0022s latency).
Not shown: 998 filtered ports
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| ssl-cert: Subject: commonName=Spiderman.MARVEL.local
| Not valid before: 2020-01-04T21:25:15
|_Not valid after:  2020-07-05T21:25:15
|_ssl-date: 2020-01-06T00:57:38+00:00; 0s from scanner time.
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.84 seconds
```

Until next, happy ethical hacking!!!