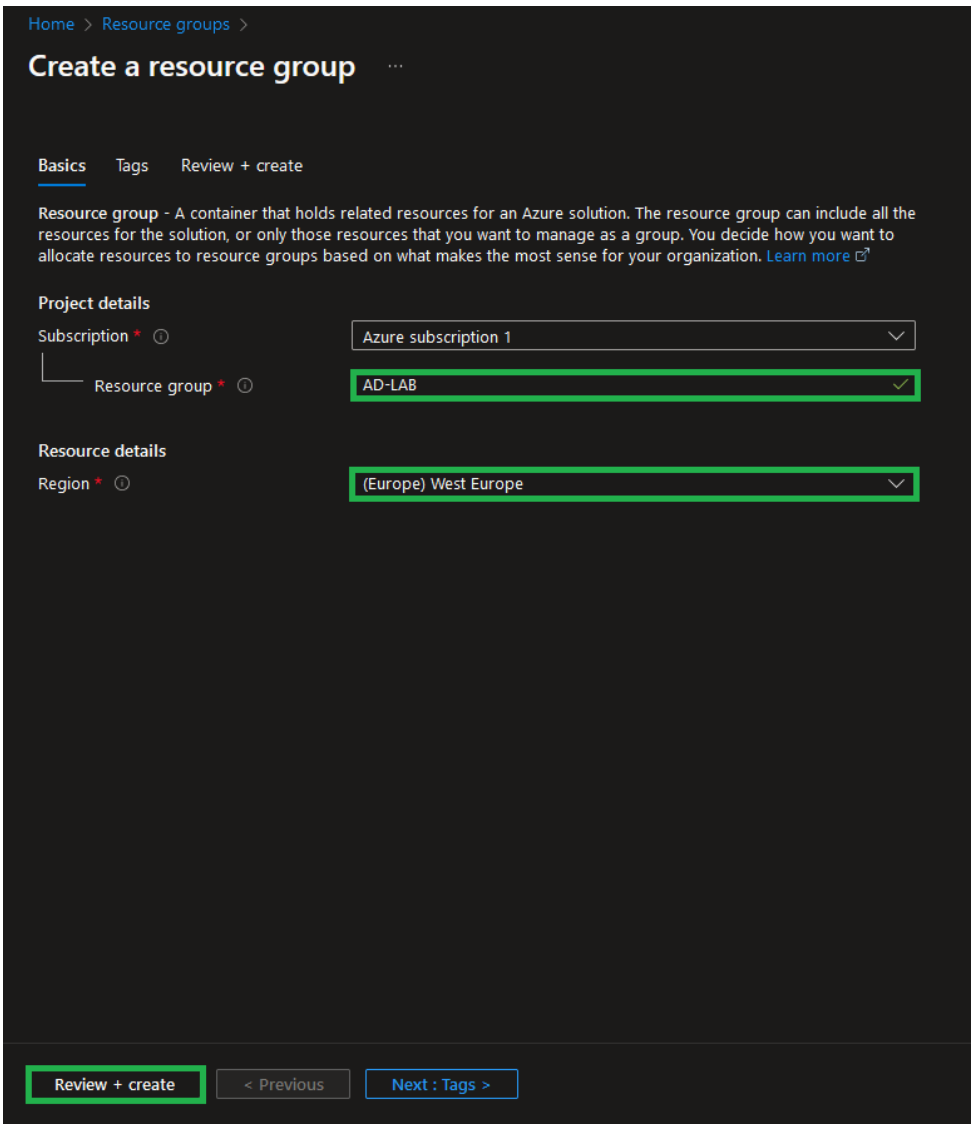
Deploying a Traditional Active Directory Setup in Azure

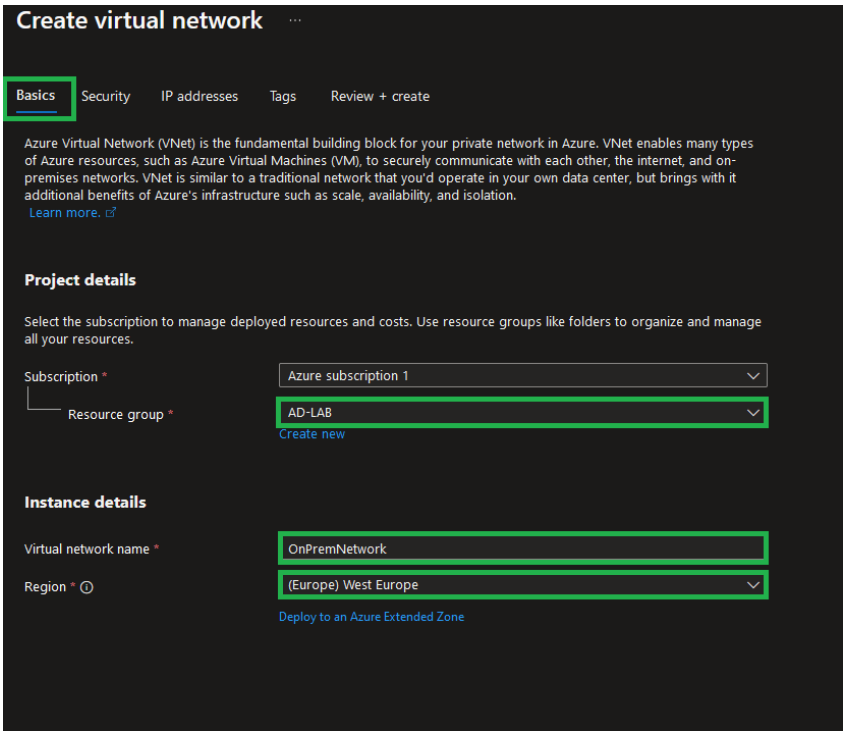
In this project I will simulate the creation of an on premises Active Directory setup with two domain controllers (DCs) for redundancy, all hosted within the Azure Cloud. We will be using the DNS settings of our Server, instead of the Azure settings, so that the two DCs can communicate. When we create users and groups using one domain controller, they will be replicated over to the other which will ensure that our users can maintain access to the resources they need to do continue their work uninterrupted.

Task 1: Creating and configuring the necessary resources in Azure

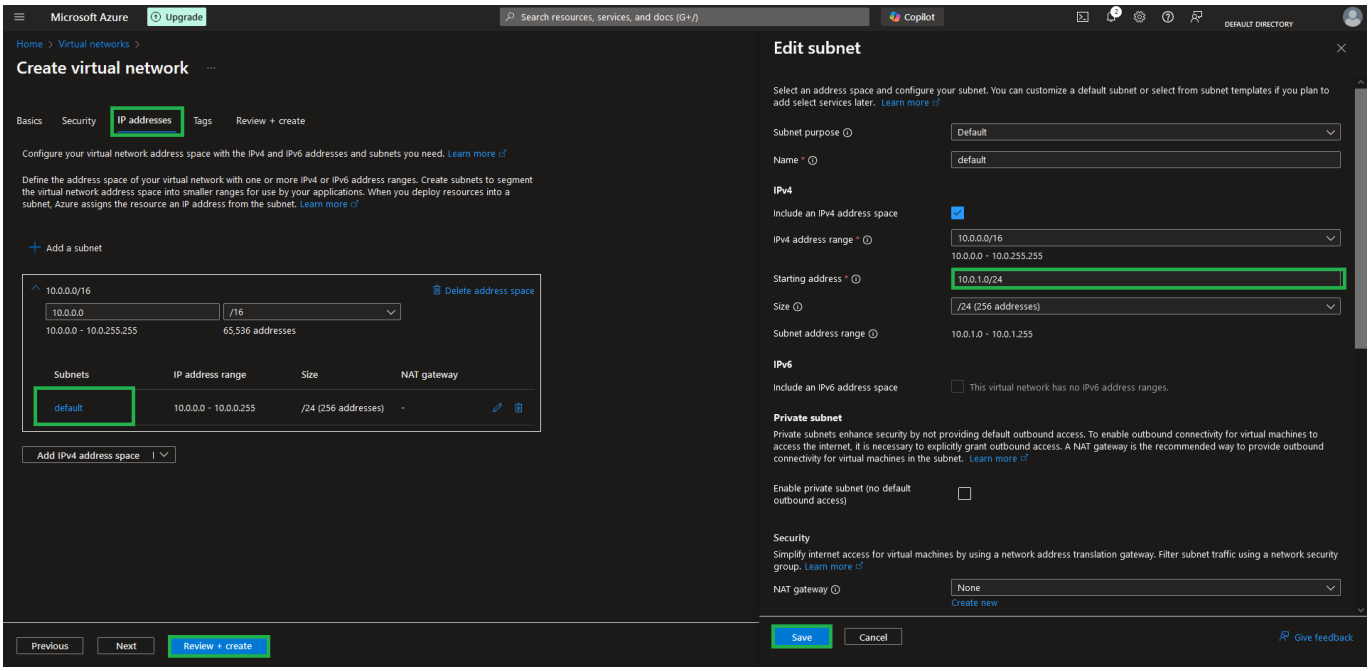
1. We first create a resource group called AD-LAB located in the highest availability region closest to us.



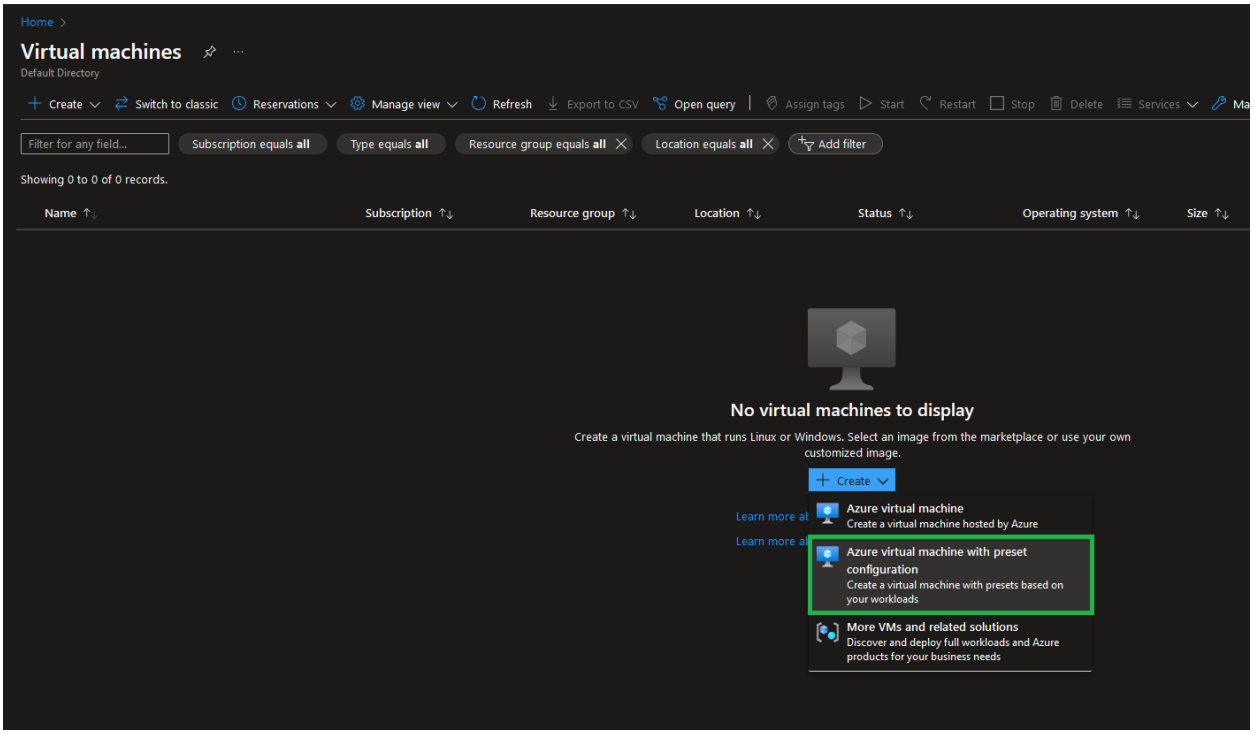
2. We then create a Virtual Network for our AD domain controllers with the following configuration:
    I. On the **Basics** tab we select the resource group we just created, name our virtual network, and select the same region as our resource group.



    II. On the **IP addresses** tab, we click on the *default* subnet, input 10.0.1.0/24 as our starting address, select **Save**, leave the other tabs to their default values, and click on the **Review + Create button.**

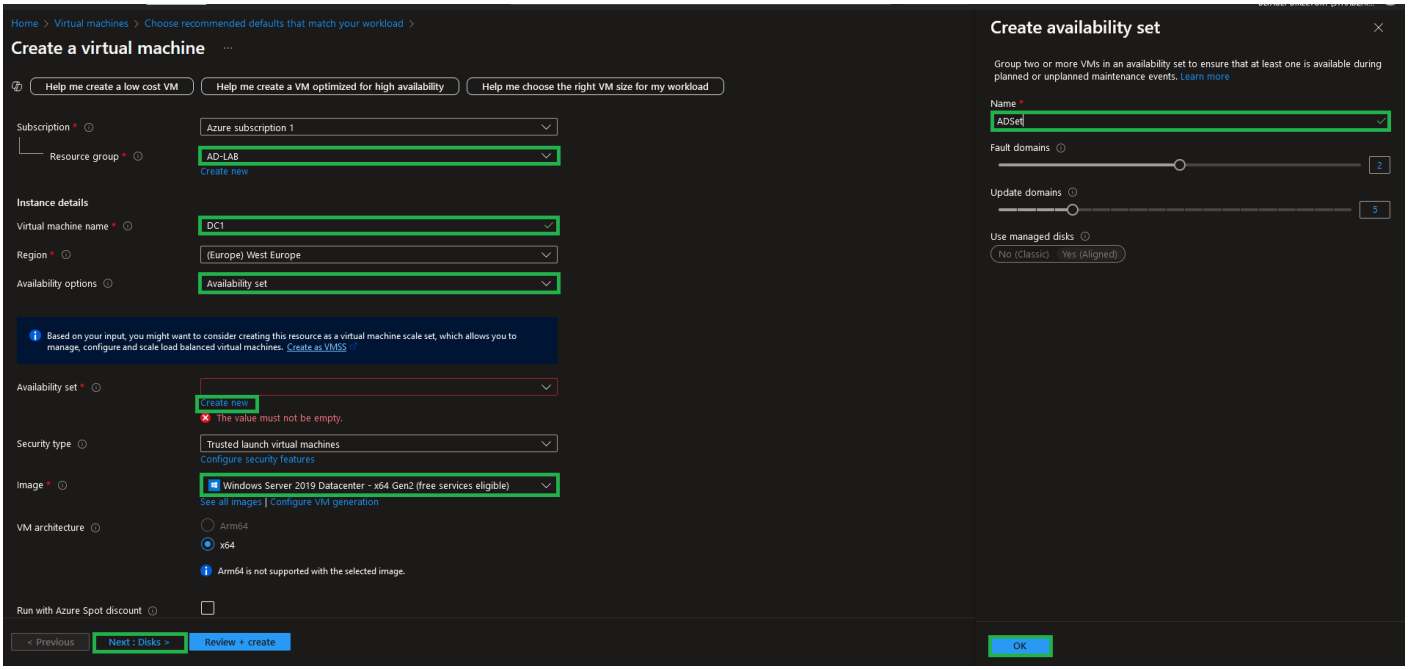


3. We then choose the **Create virtual machine with preset configuration** option from the Virtual machines page and select a *Dev/Test* workload environment with a *General Purpose (D-Series)* workload type.

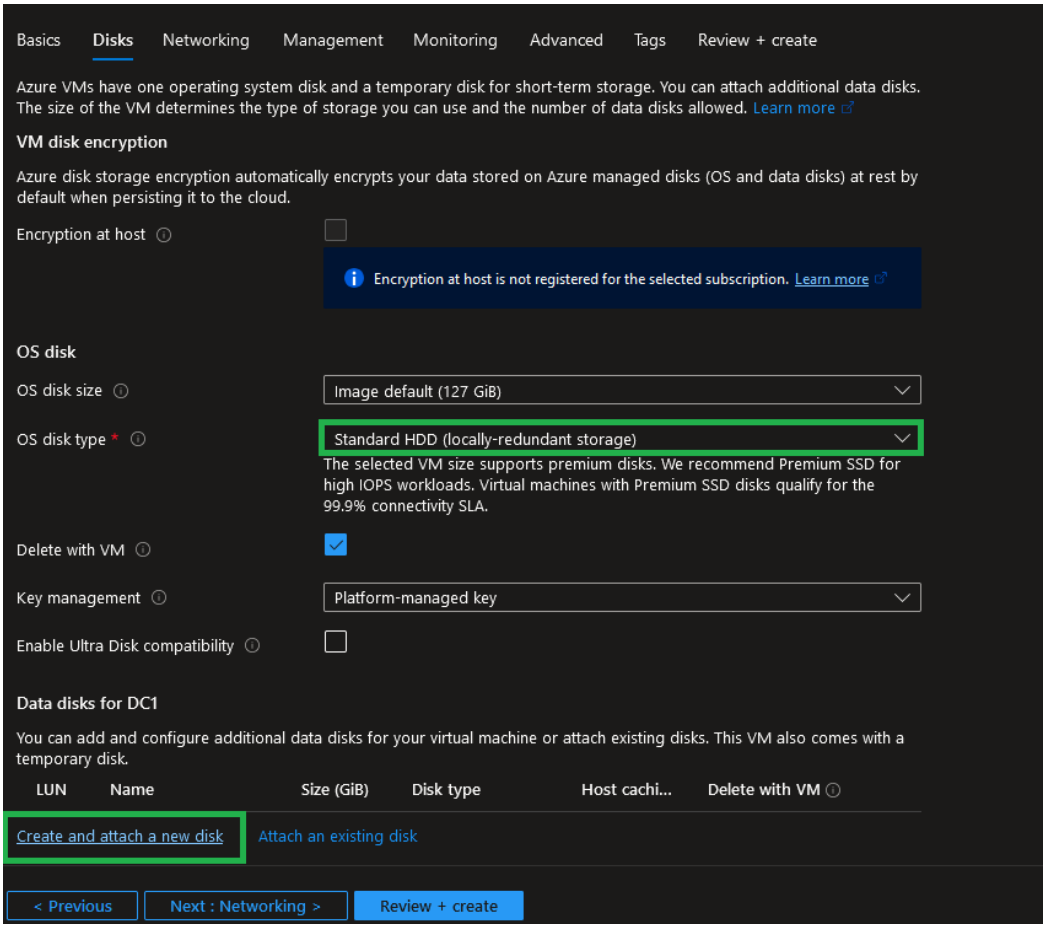


4. and create our Windows Server 2019 virtual machine with the following configuration on the **Basics** tab:

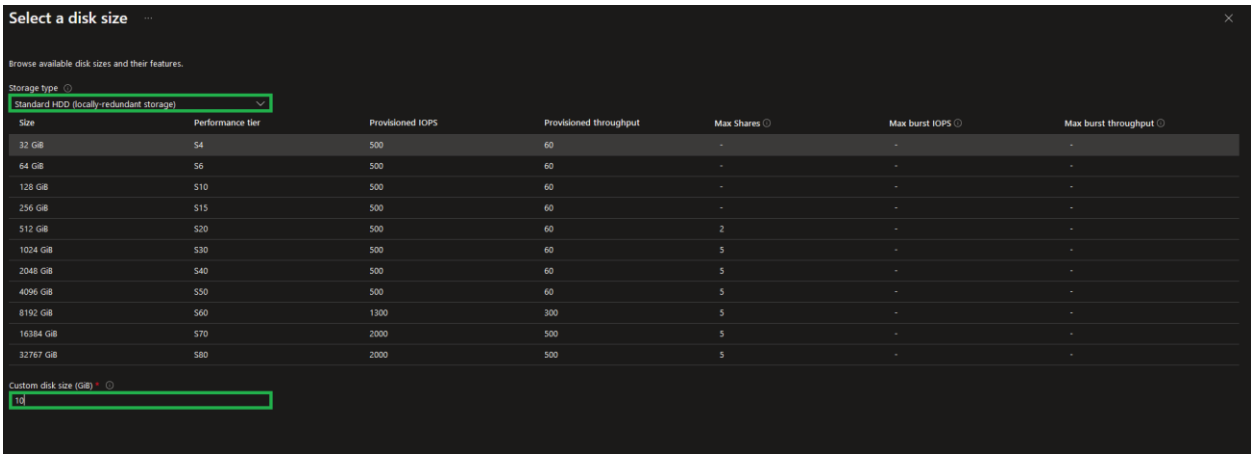
Field	**Value**
Subscription	Our current subscription.
Resource group	**AD-LAB**
Virtual machine name	Enter a unique VM name, such as **DC1**.
Region	Select the same region as before.
Availability options	Select **Availability set**.
Availability set	Create new called **ADSet**.
Image	Select **Windows Server 2019 Datacenter**
Size	**D2s_v3 – 2vcpus, 8GiB memory**



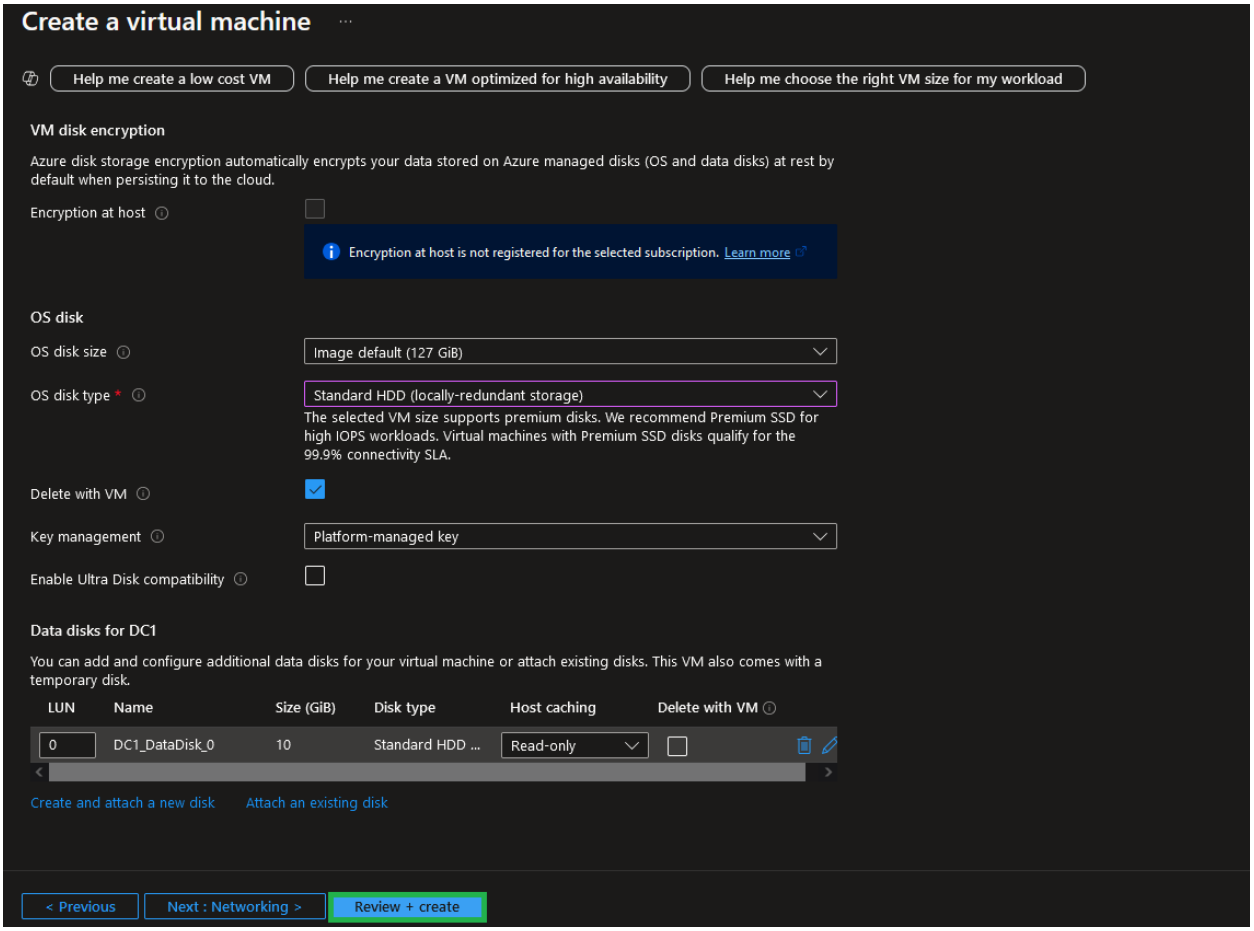
5. We then click on **Next : Disks**, select the **Standard HDD** OS disk type, and click on **Create and attach a new disk**.



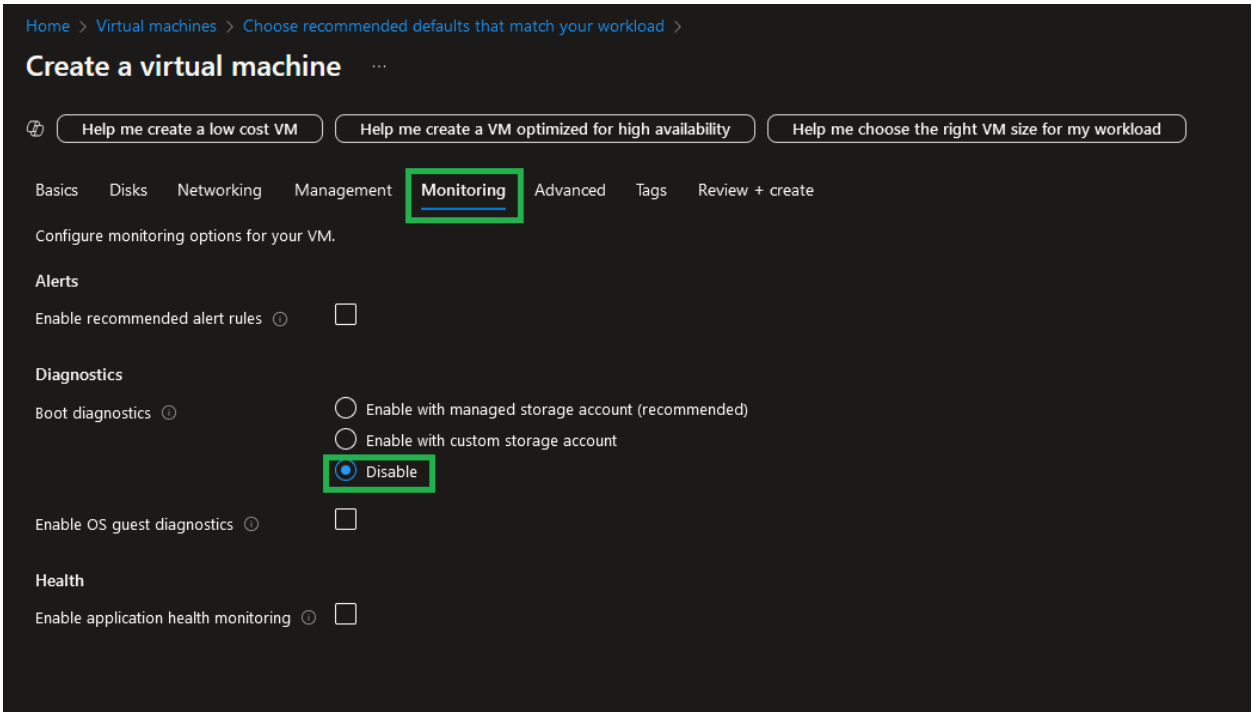
6. On the **Create a new disk page**, we click on **Change Size**, and create a *Standard HDD 10GB GiB* disk.



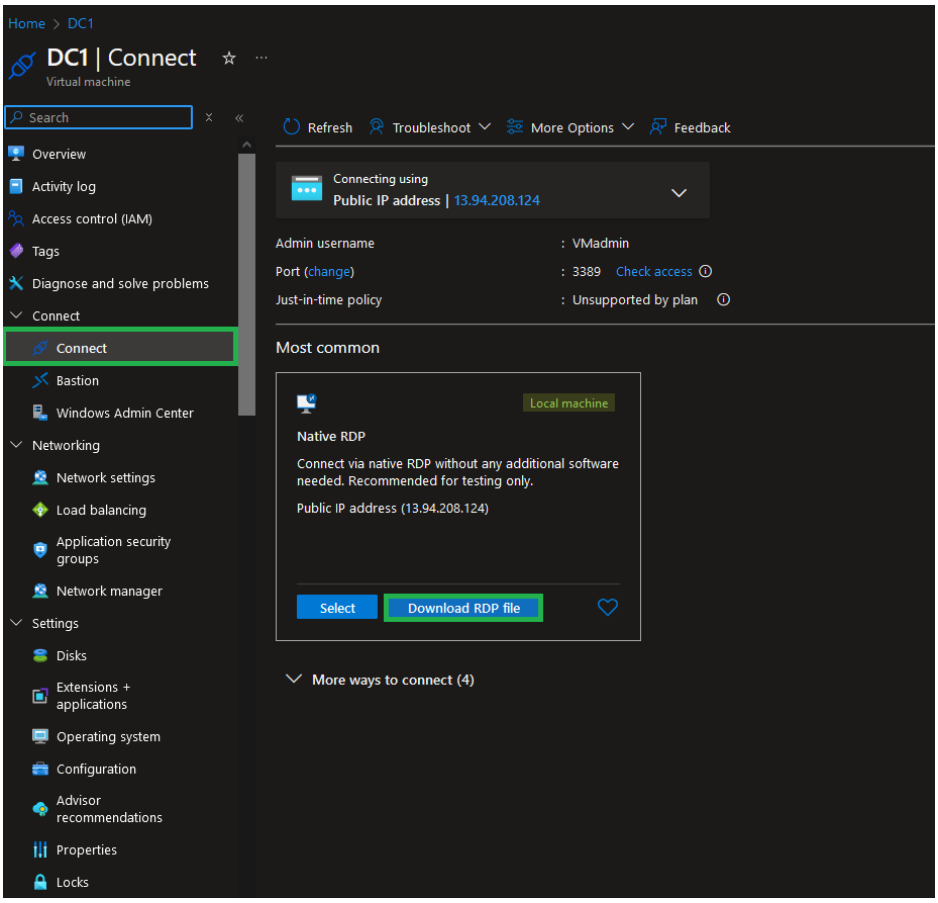
7. Once our disk is created, we can click on **Review + Create**, leaving the rest of the configuration at default values and then deploy our resource with the **Create** button.



Note: Since this is a lab, we can also disable **Boot diagnostics** from the **Management** tab as we do not really need it for the purposes of this project.

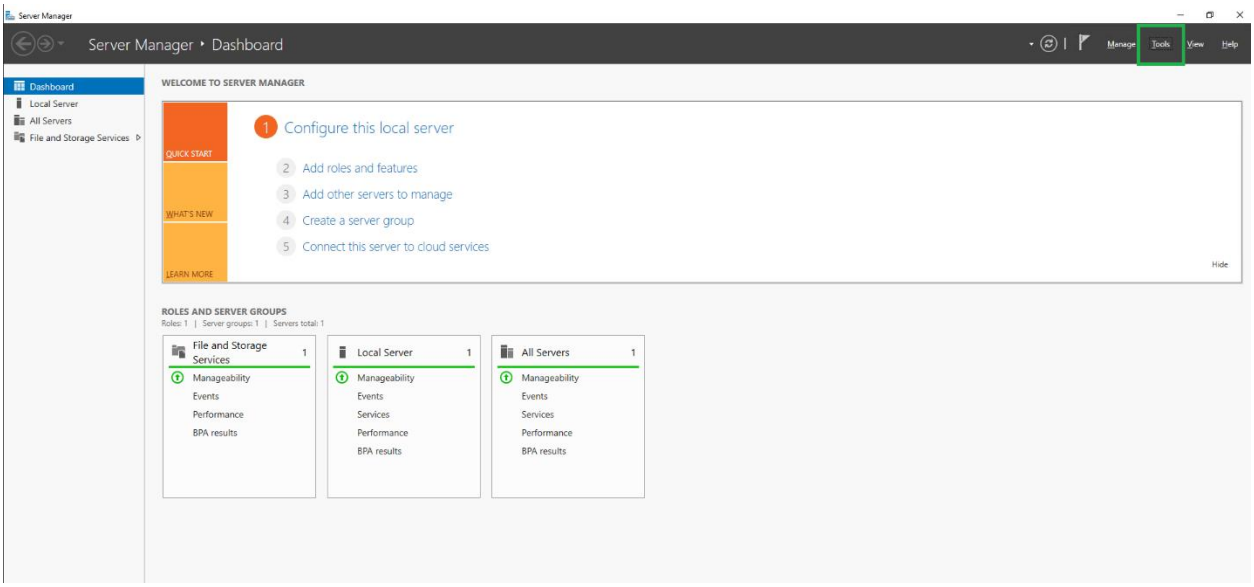


8. Once the VM is deployed, we click on **Go to Resource**, select the *Connect* blade, and download the RDP file.

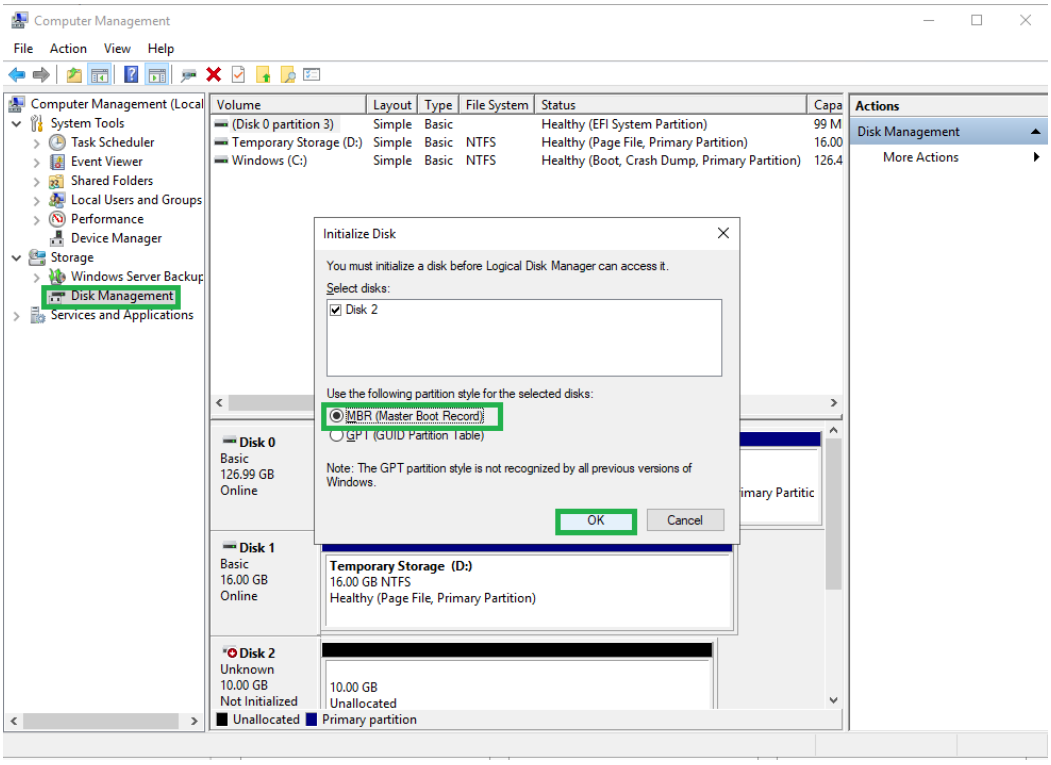


Task 2: Setting up our domain controllers

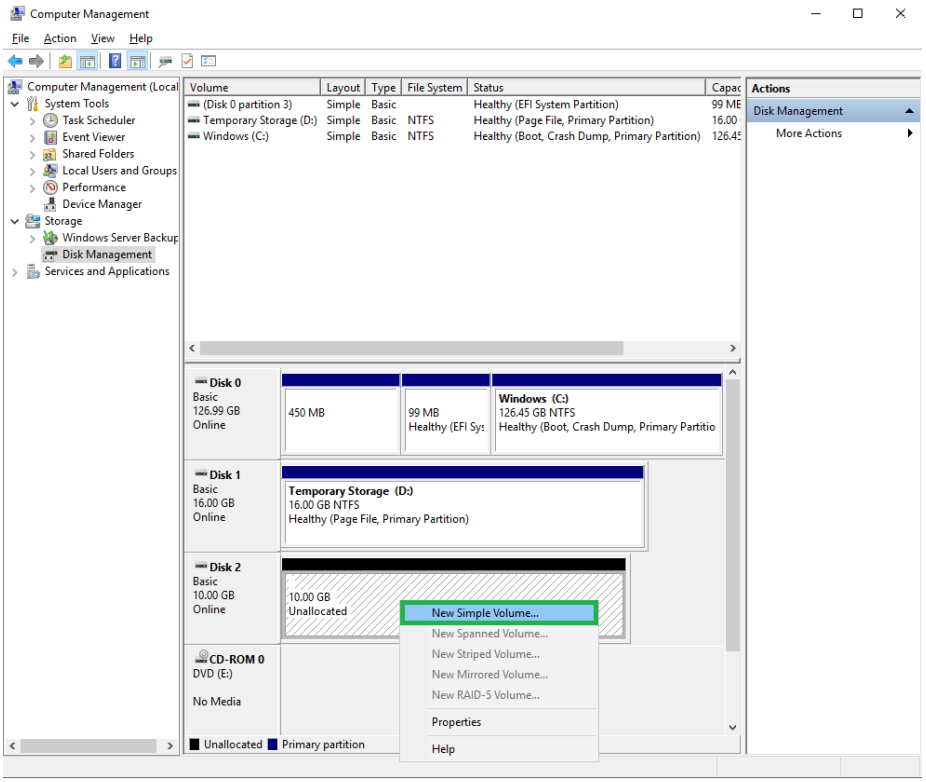
1. Once our we've logged into **DC1**, we click on **Yes** when asked whether we want this PC to be discoverable by other PCs and devices on this network. We then go to **Tools** within the newly loaded Server Manager window, and select **Computer Management**.



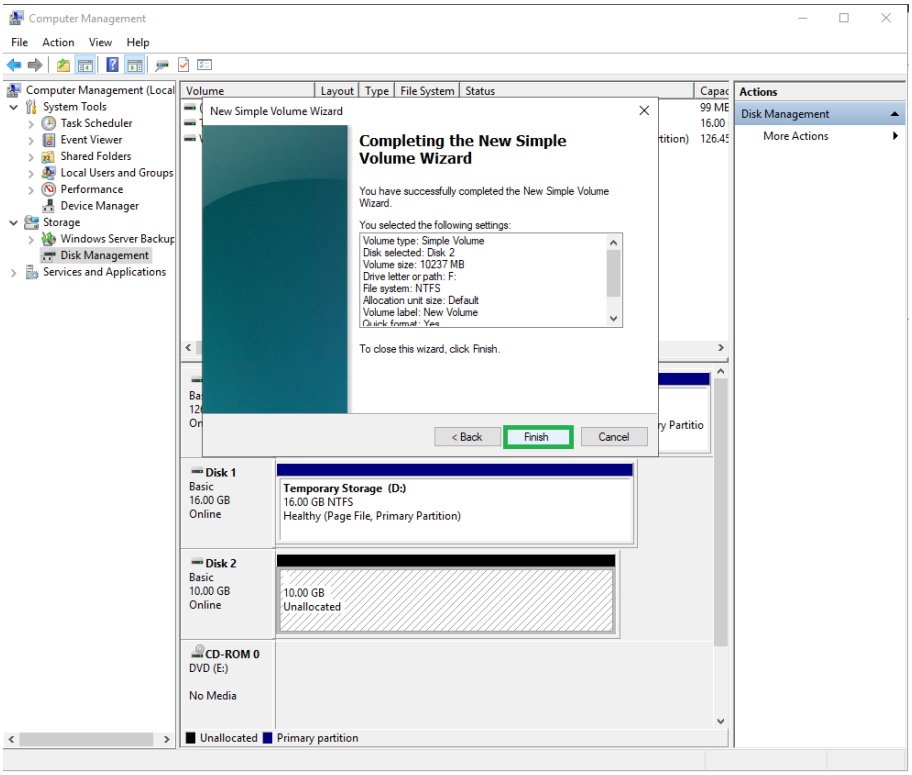
2. We then select **Disk Management**, choose the **MBR** partition style when the **Initialize Disk** window pops up, and select **OK**.



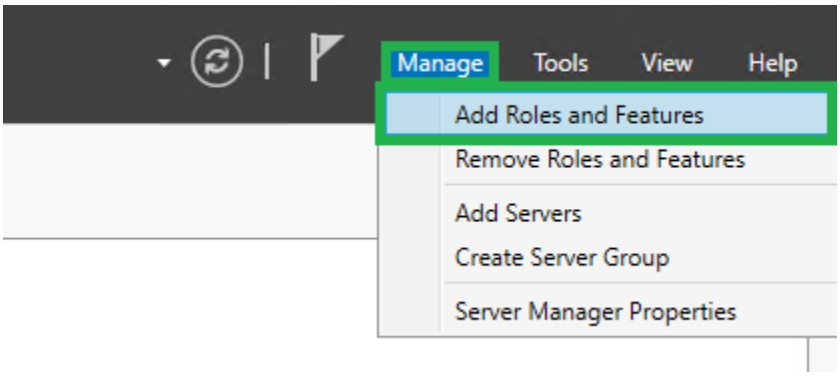
3. We then right click on Disk 2, which is the disk we created in Azure during our VM's initial configuration, and select **New Simple Volume**.



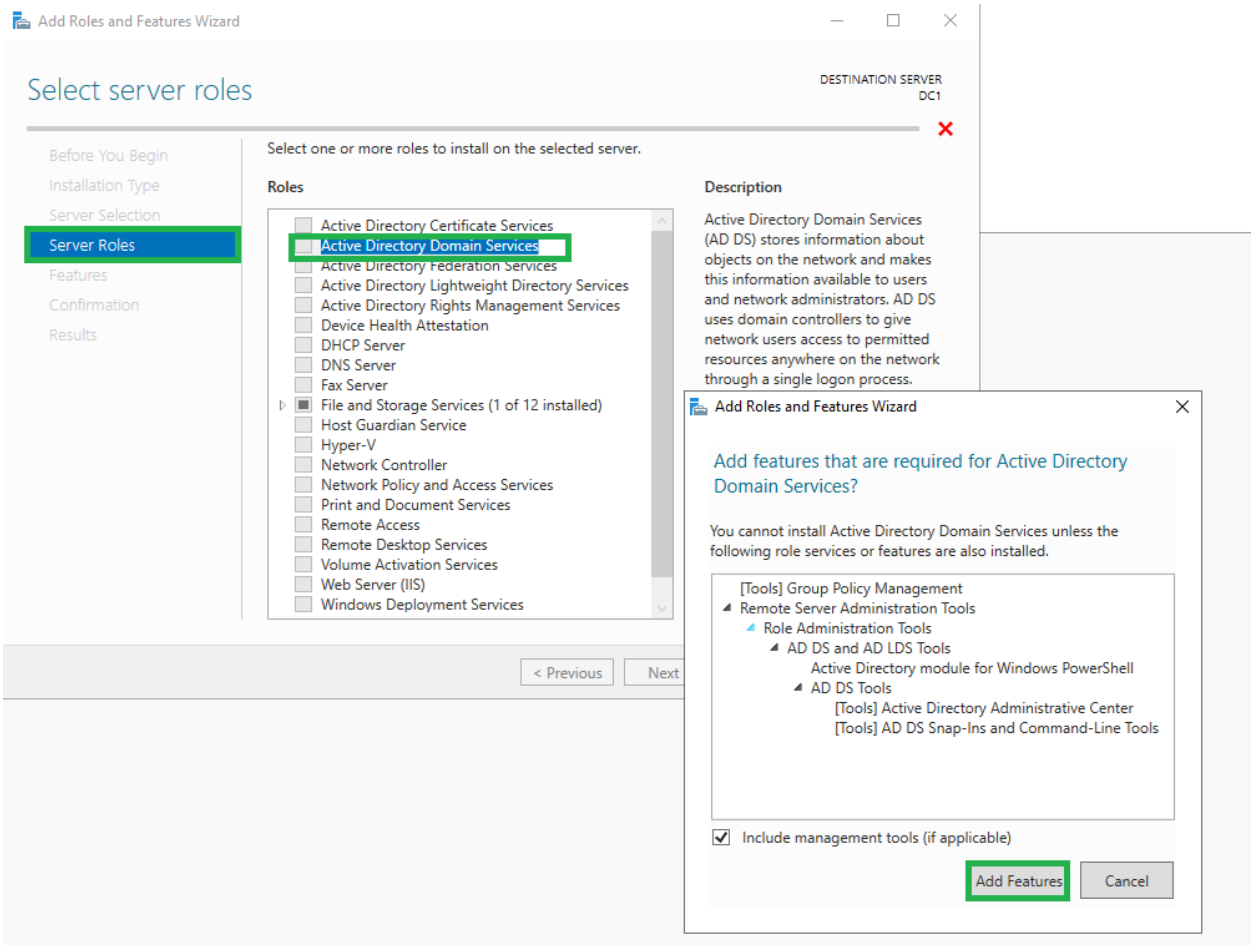
4. We click though all default settings in the Wizard and select **Finish**.



5. We then need to install Active Directory. We do so by clicking on **Manage** and selecting **Add Roles and Features**.

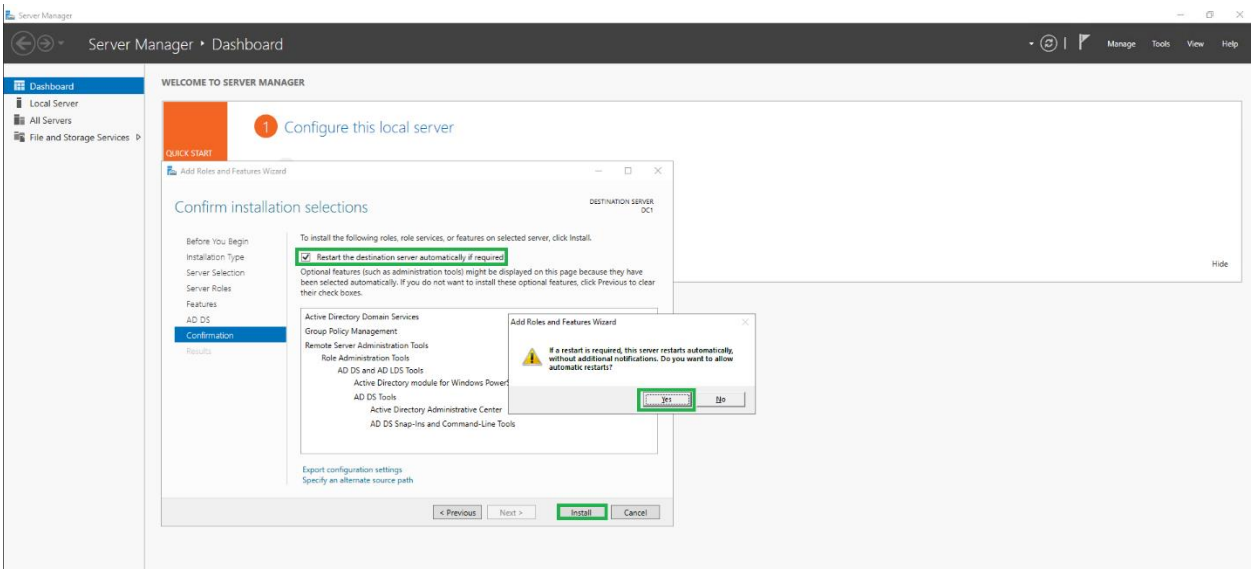


6. In the Wizard that pops up, we select **Role-based or feature-based installation**, leave in the defaults until we reach the **Server Roles** page, where we select the **Active Directory Domain Services** box and click on the **Add Features** button in the new window that will appear.

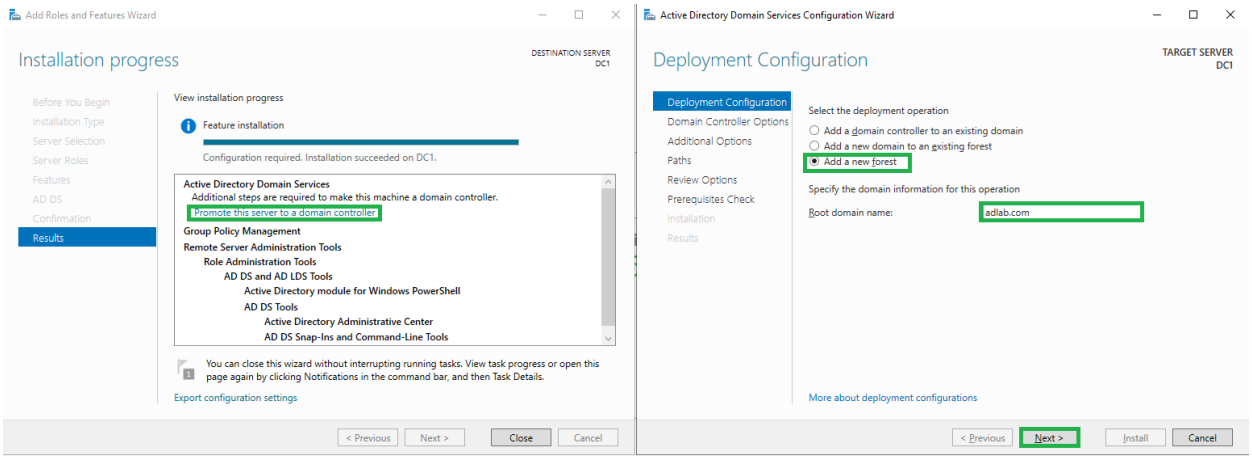


7. We then click through the rest of the defaults using the **Next** button until we reach the **Confirmation** page, where we select the **Restart the destination server automatically if**

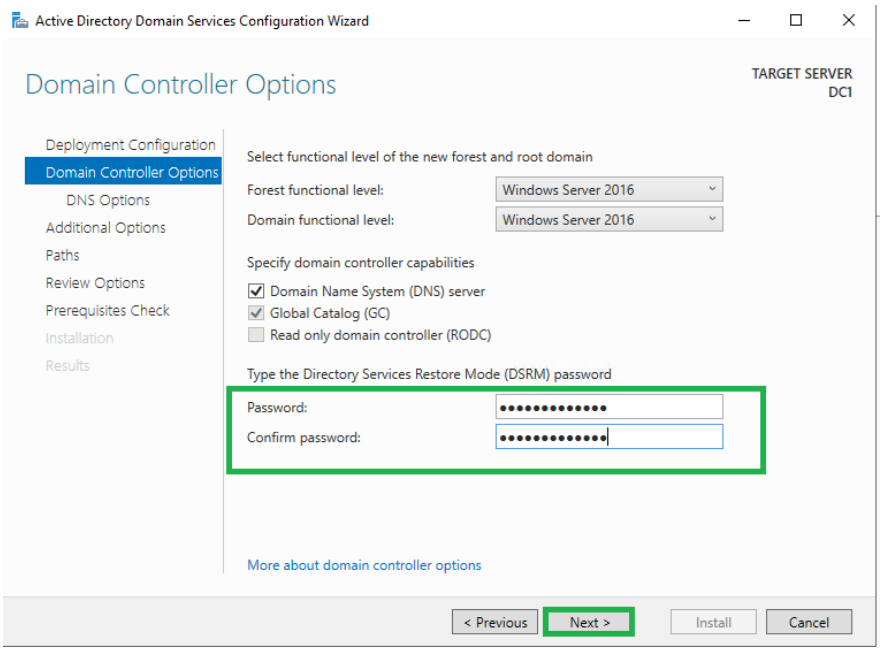
required box, confirm our choice on the pop-up window by choosing **Yes**, and then finalize the process by clicking on **Install**.



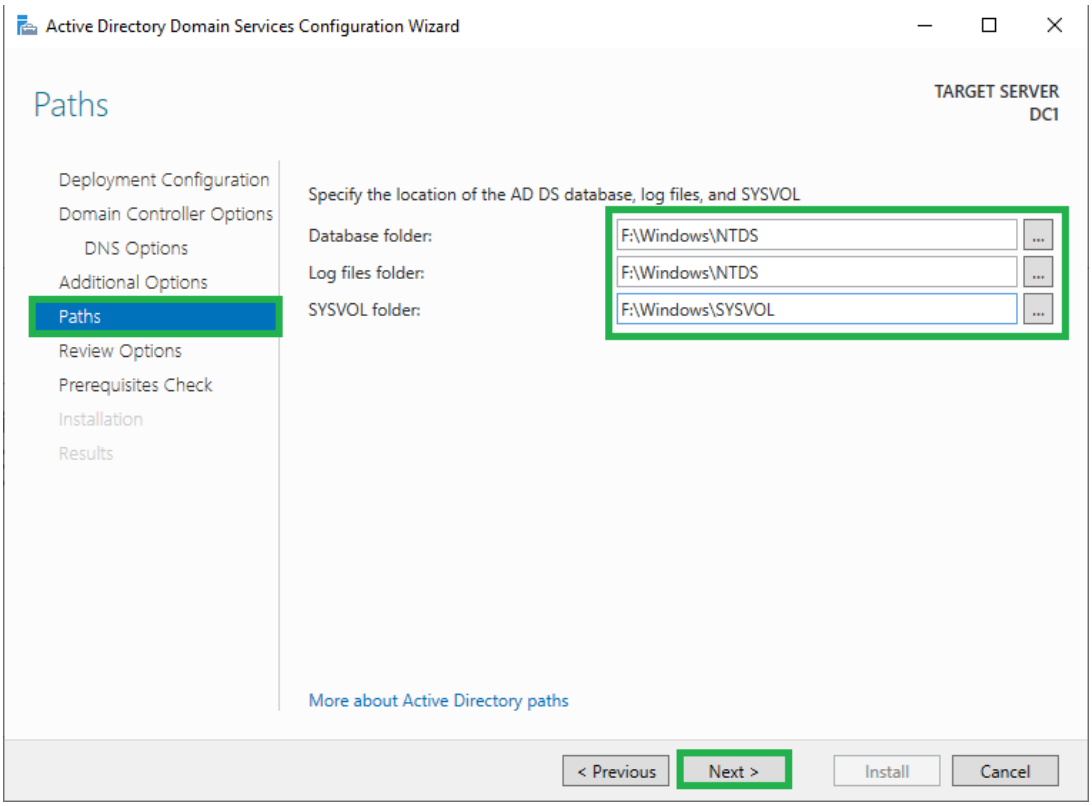
8. Once this is done, we click on **Promote this server to a domain controller** and select the **Create a new forest** radio button, and specify a domain name of our choice.



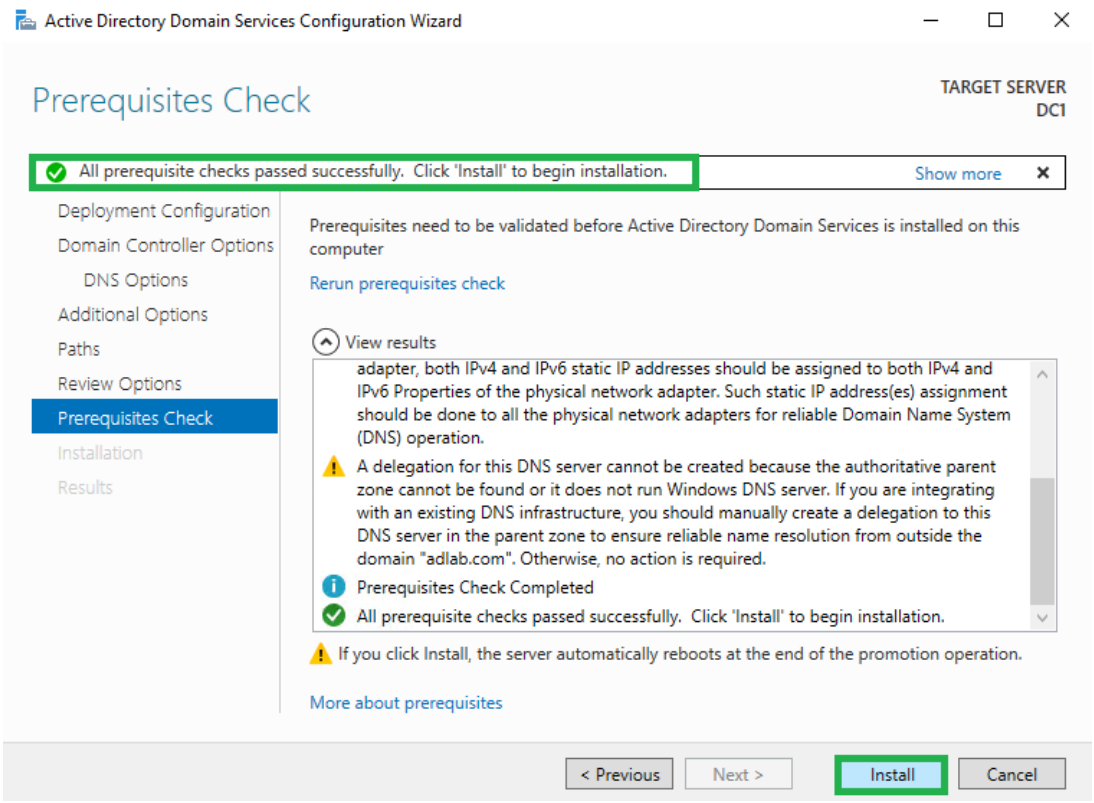
9. We create a password on the following page and click **Next**, as we can in leave the other options at their defaults.



10. We leave the **DNS Options** and **Additional Options** pages as they are and then go to **Paths**, where we switch the default C Drive paths to our Azure Storage, so that we avoid the risk of losing our AD settings by keeping the cache stored safely in the cloud.



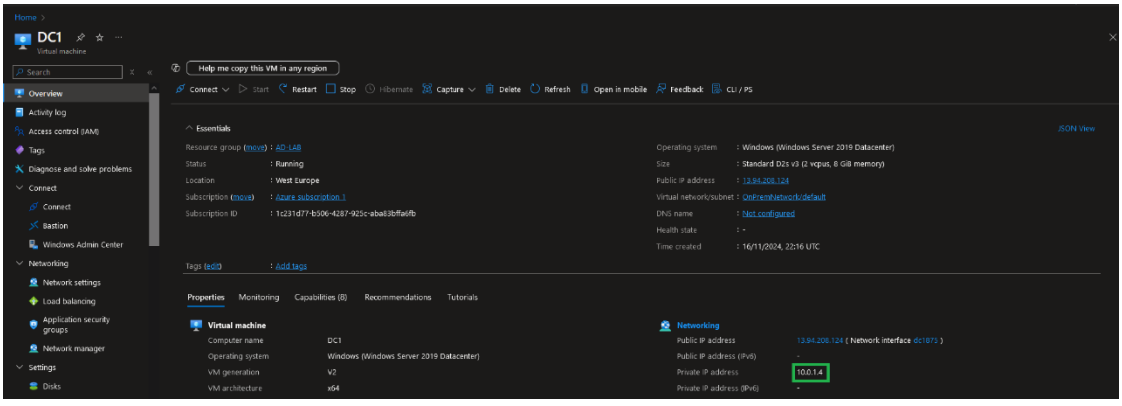
11. We click through the **Review Options** page and select **Install** after the Prerequisites Check is complete. When the install is complete, the VM will reboot.



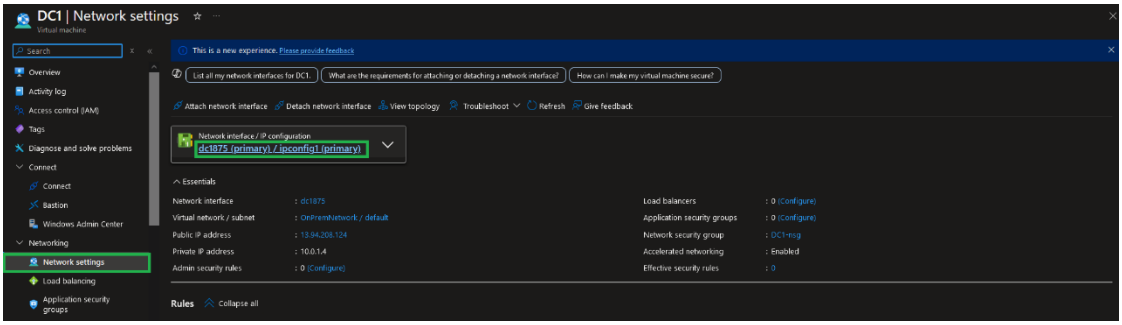
Note: We will configure the DNS settings later because we want to use the DNS of the server itself instead of the Azure DNS, so that our two domain controllers can talk to each other.

12. We then repeat this process by create a second VM called **DC2** in Azure with the exact same configuration settings.
    Note: Make sure to use the same resource group, region, virtual network, subnet, and availability set, as well as creating another Standard HDD 10GiB disk.

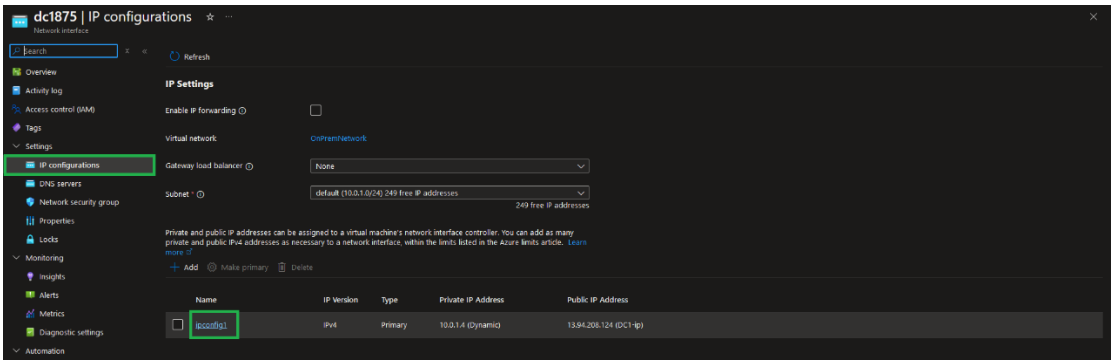
13. We now need to go **DC1**'s Azure page and take a note of its Private IP address.



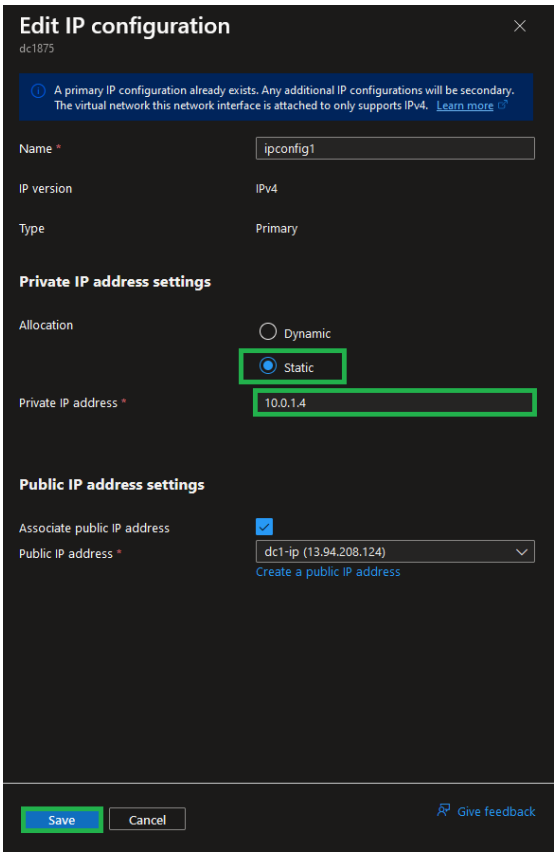
14. We then navigate to the VM's network adapter by selecting the Network settings blade and clicking on underlined name of the network interface.



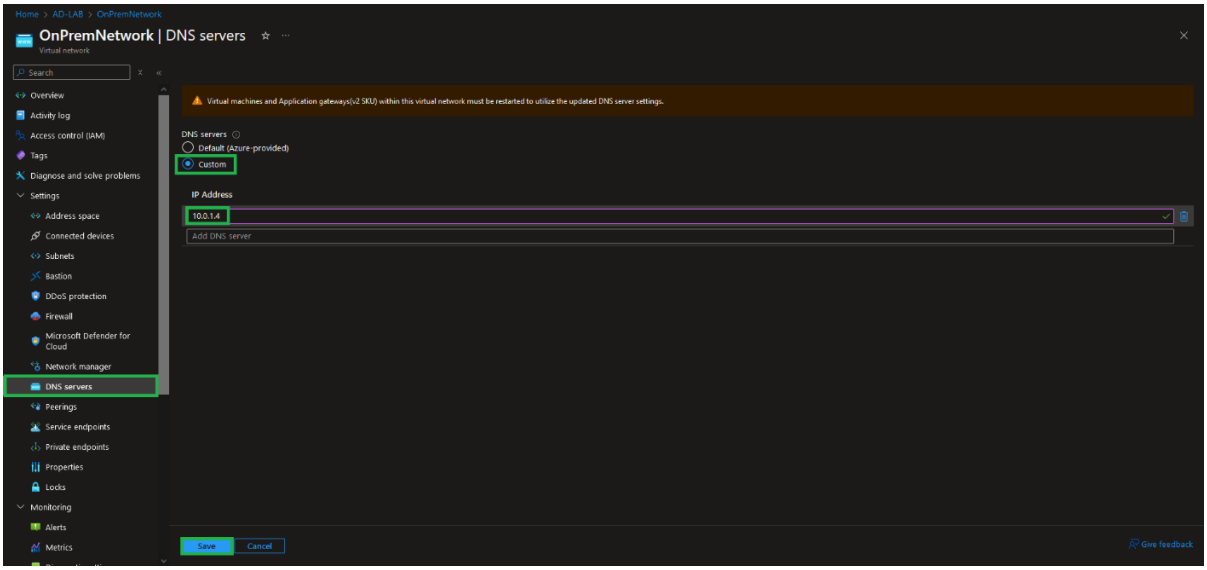
15. On the IP configurations blade, we select **ipconfig1**.



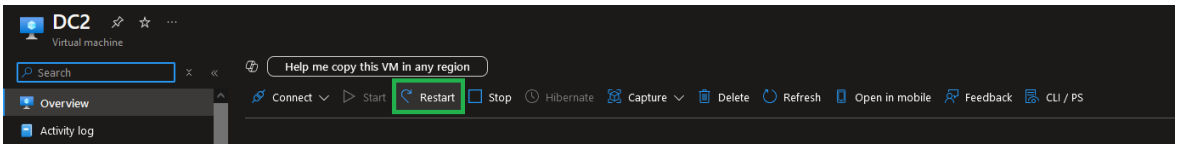
16. We then assign it a static IP and click **Save**.



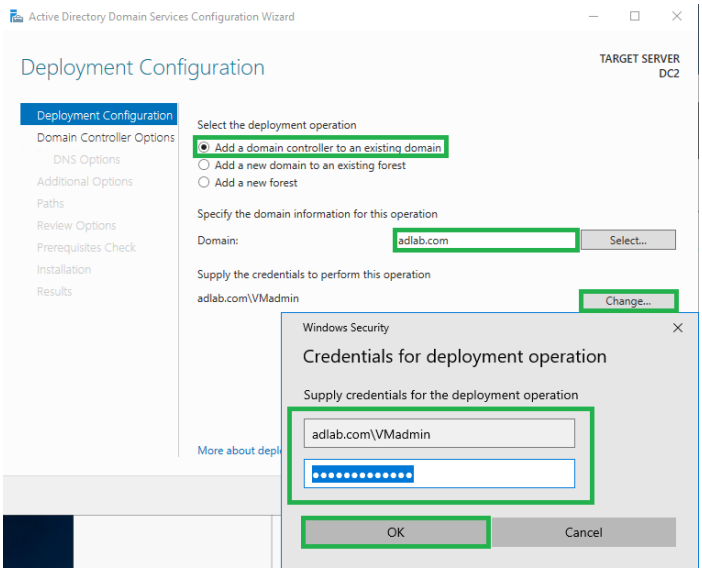
17. The next step is to go to our virtual network's page and change it to the deployed Active Directory's DNS. We navigate to the *DNS servers* blade, select the **Custom** radio button, paste **DC1**'s private IP address, and select **Save**.



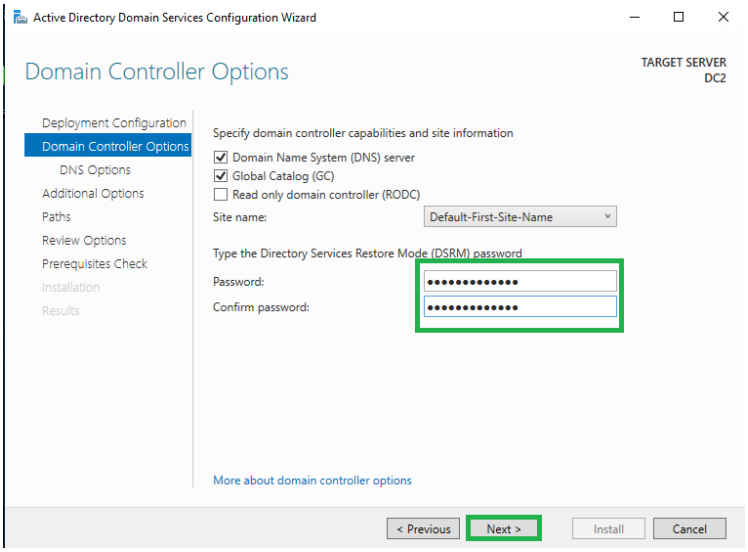
18. The **DC2** VM should now be restarted, so that it can get it's DNS from **DC1**'s AD instead of Azure.



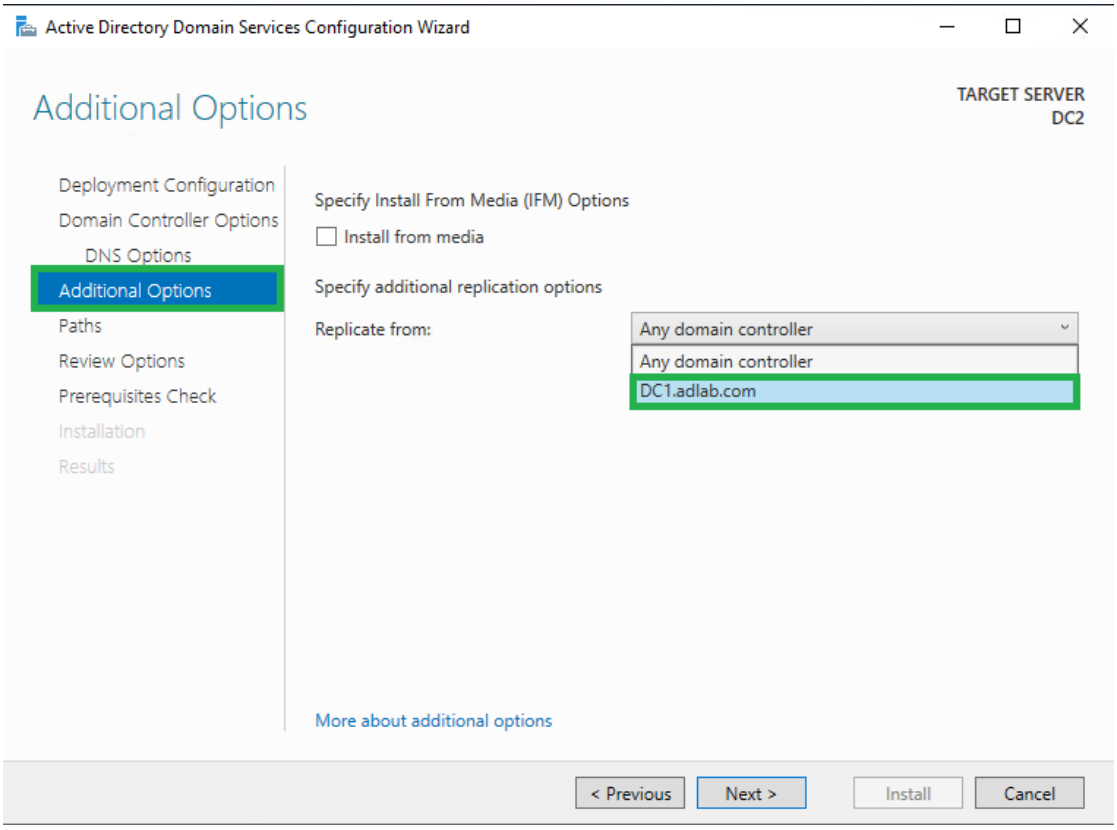
19. We can now install Active Directory to **DC2** using the exact same way as we did on **DC1** up to the point at which we reach the **Deployment Configuration** page where we select the **Add a domain controller to an existing domain** radio button, type in our domain and click on **Change** under the *Supply the credentials to perform the operation* section. We then input **adlab.com\VMadmin** as the username and type-in our password.



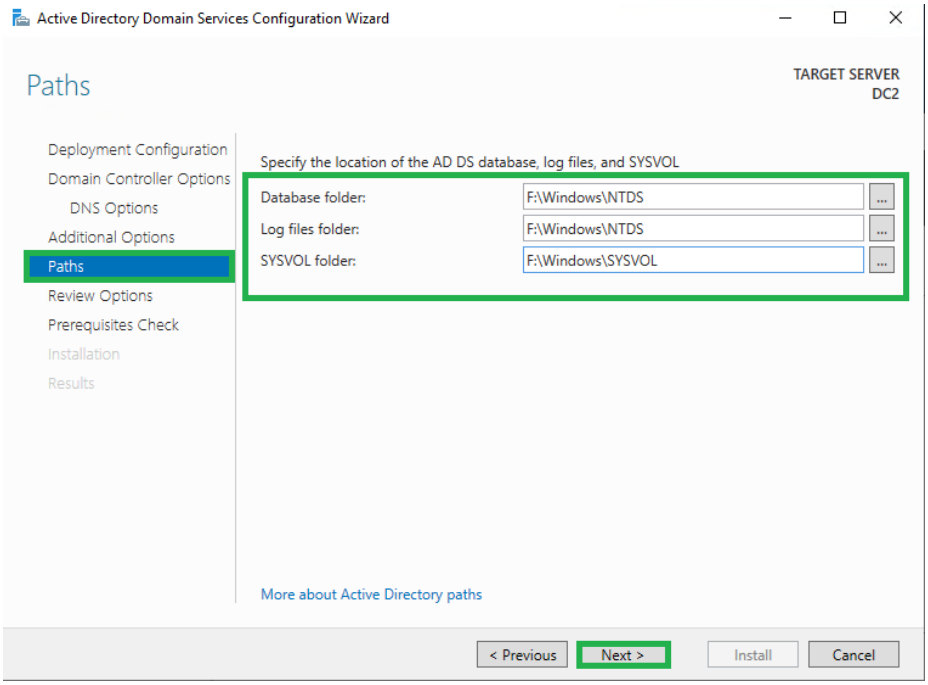
20. We then retype the DSRM password we created earlier during **DC1**'s configuration and click **Next**.



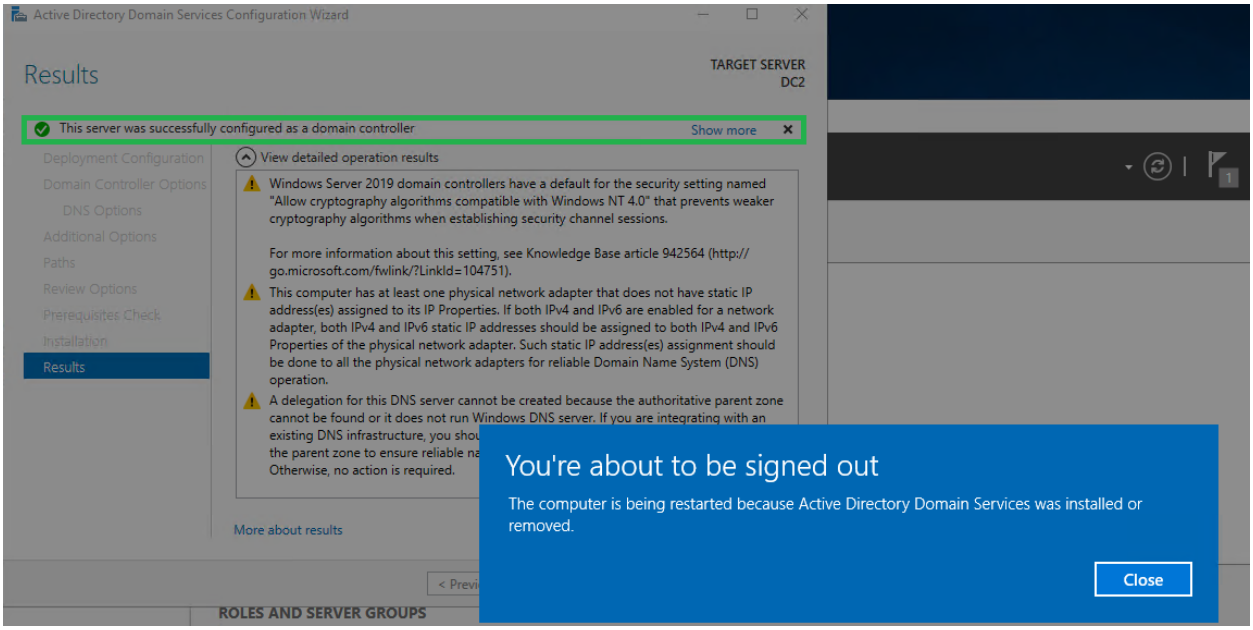
21. We click through the **DNS Options** page and on the **Additional Options** page, we select to replicate from the domain controller that we created earlier – **DC1**.



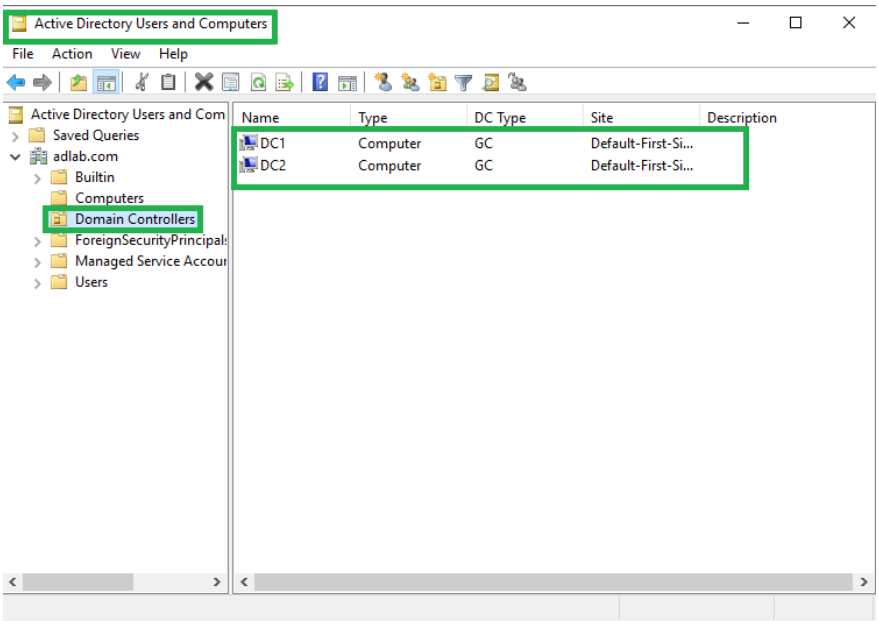
22. On the next page, we once again change the location to the F drive we created in Azure, so that our AD information is not lost in the case of a server crash.



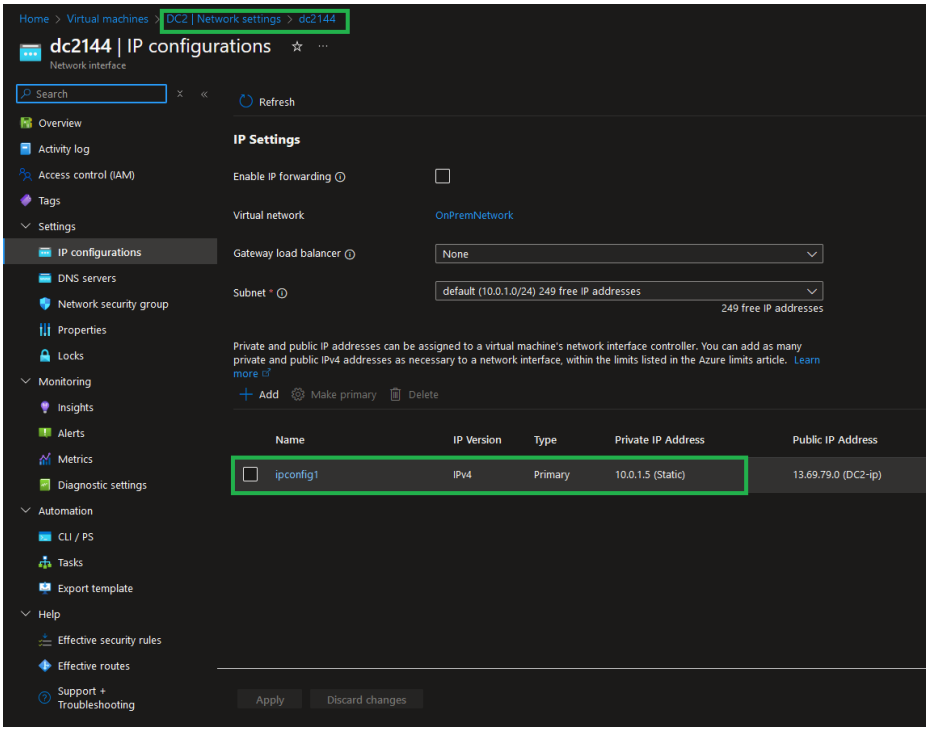
23. We click through the following pages and install Active Directory just like before. The VM will reboot after the installation is completed.



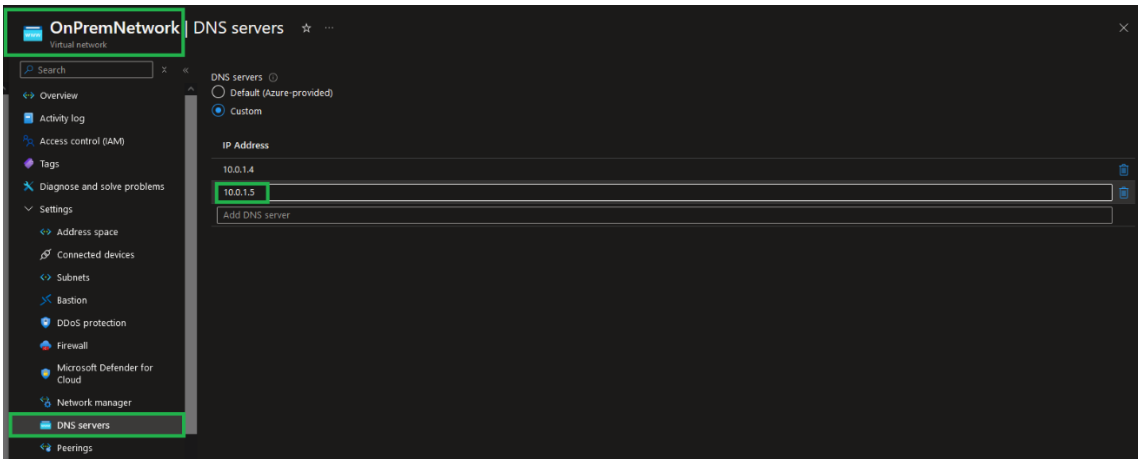
24. If we now go to **Tools** and click on **Active Directory Users and Computers** on **DC2**, we should see both VMs in the **Domain Controllers** section.



25. Now, just like before, we go back into Azure and assign a static IP to **DC2**'s network interface.

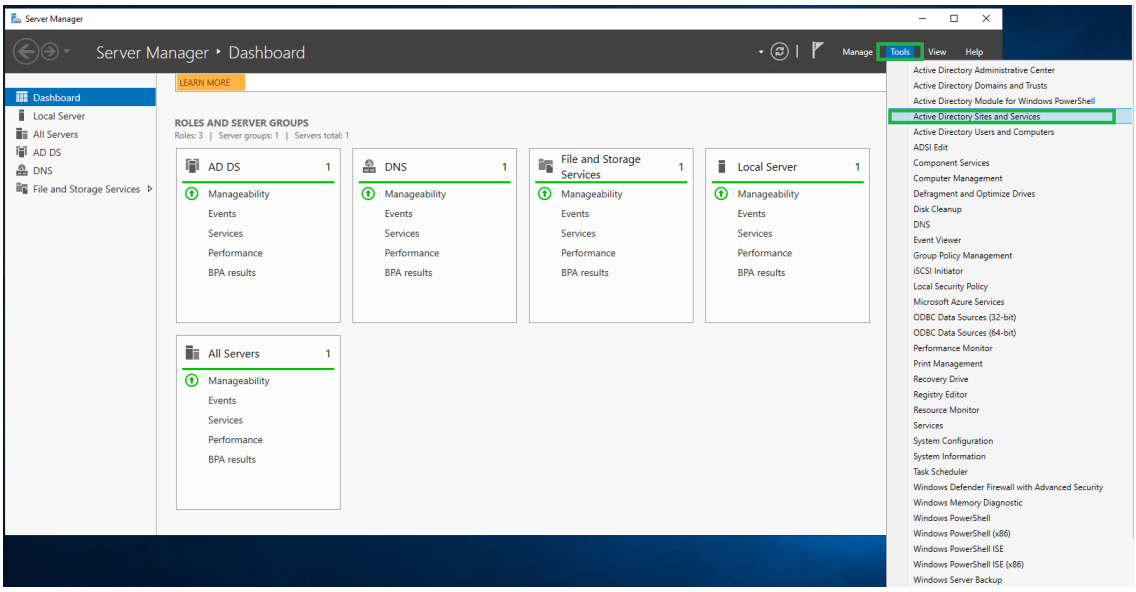


26. We also repeat the process of adding the new domain controller – **DC2**'s IP address as a DNS server on our virtual network, same as with **DC1** earlier.

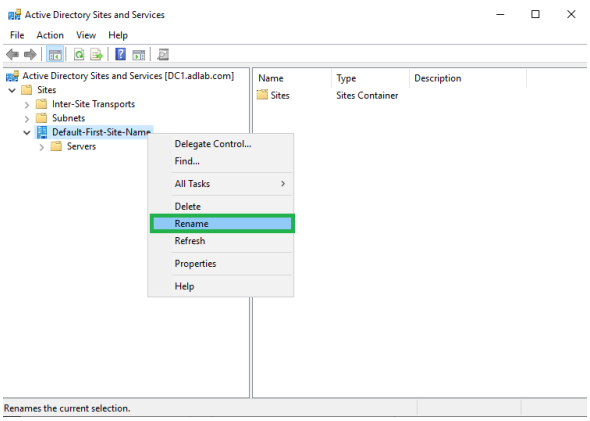


Task 3: Finalizing and testing the Active Directory configuration

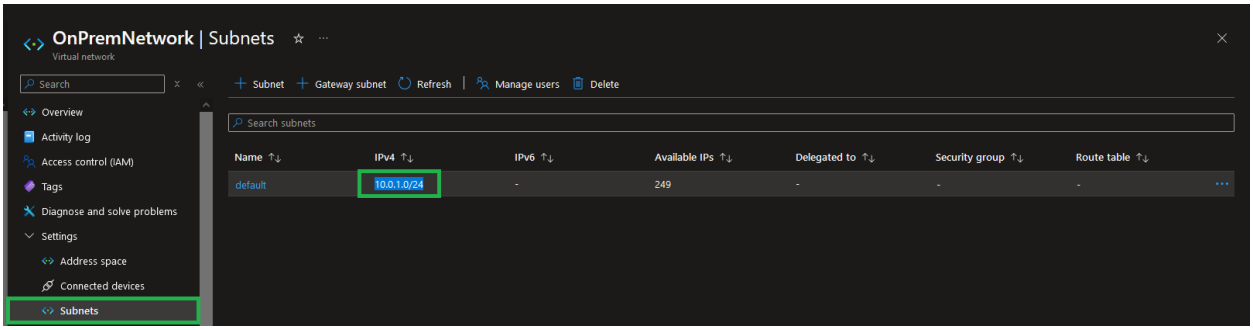
1. We open Server Manager on **DC1**, go to Tools and click on **Active Directory Sites and Services**.



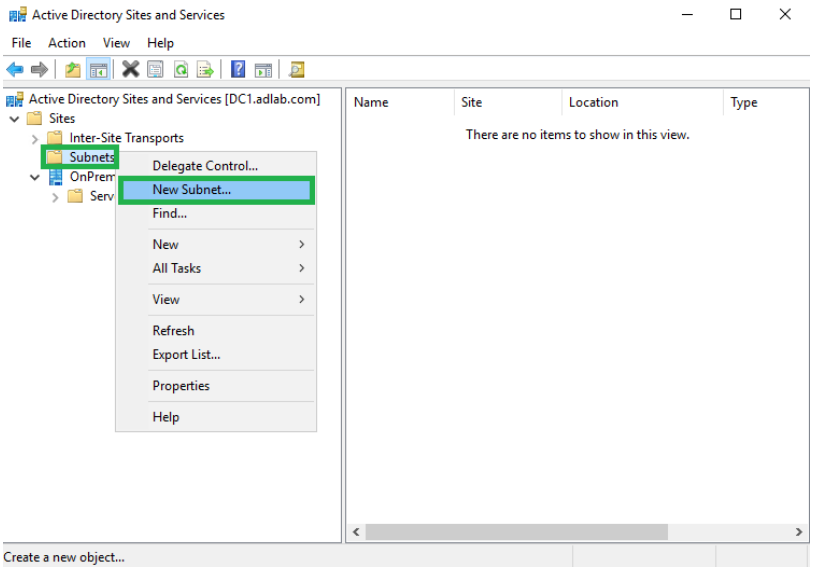
2. We scroll down to our site called Default-First-Site-Name and rename it to something like **OnPrem**, for example.



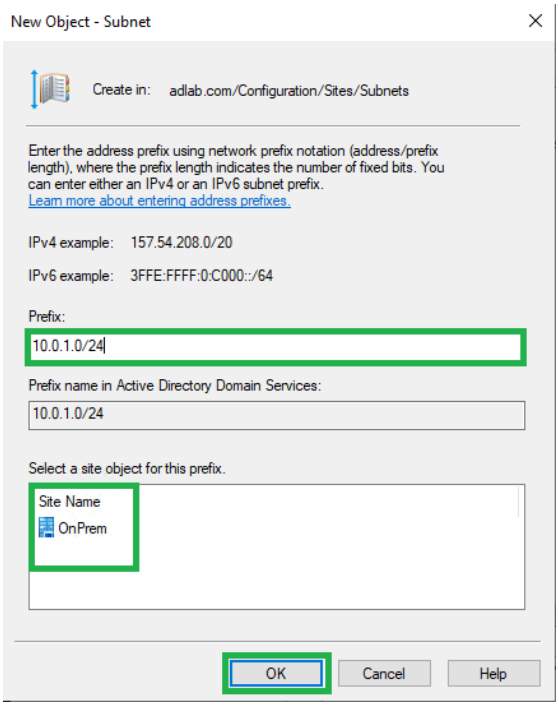
3. We then want to add our virtual network's subnet address to the **Subnets** section. We do this by going back to our Azure virtual network page and selecting the *Subnets* blade where we can view and copy our subnet's IPv4 address.



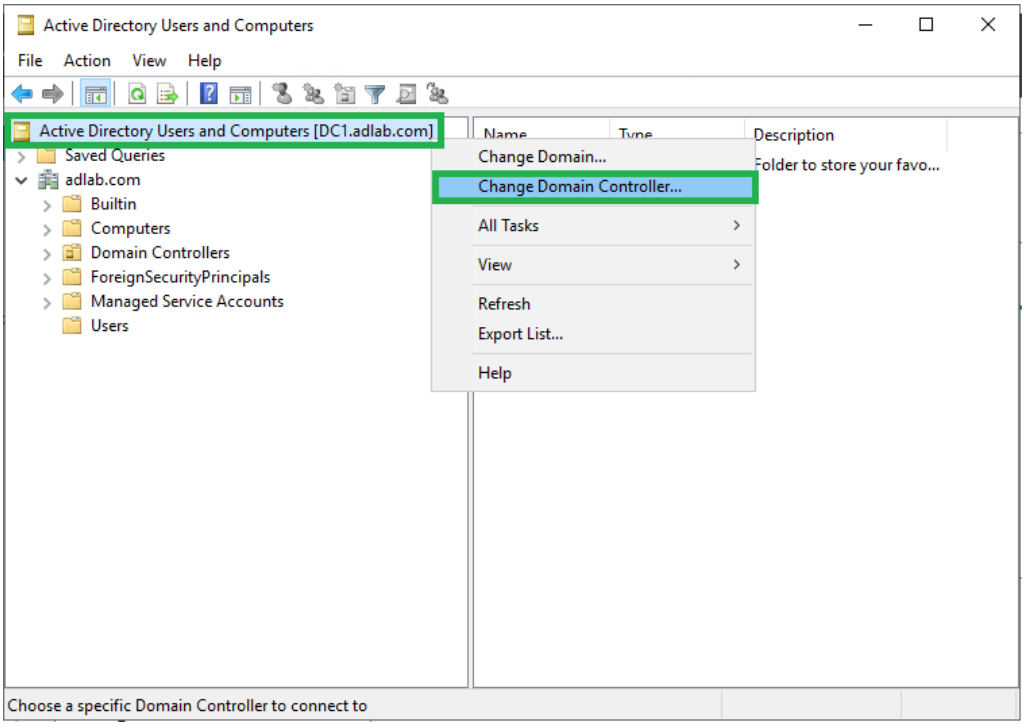
4. We go back to the **DC1** VM, where we right click on **Subnets** and select **New Subnet…**



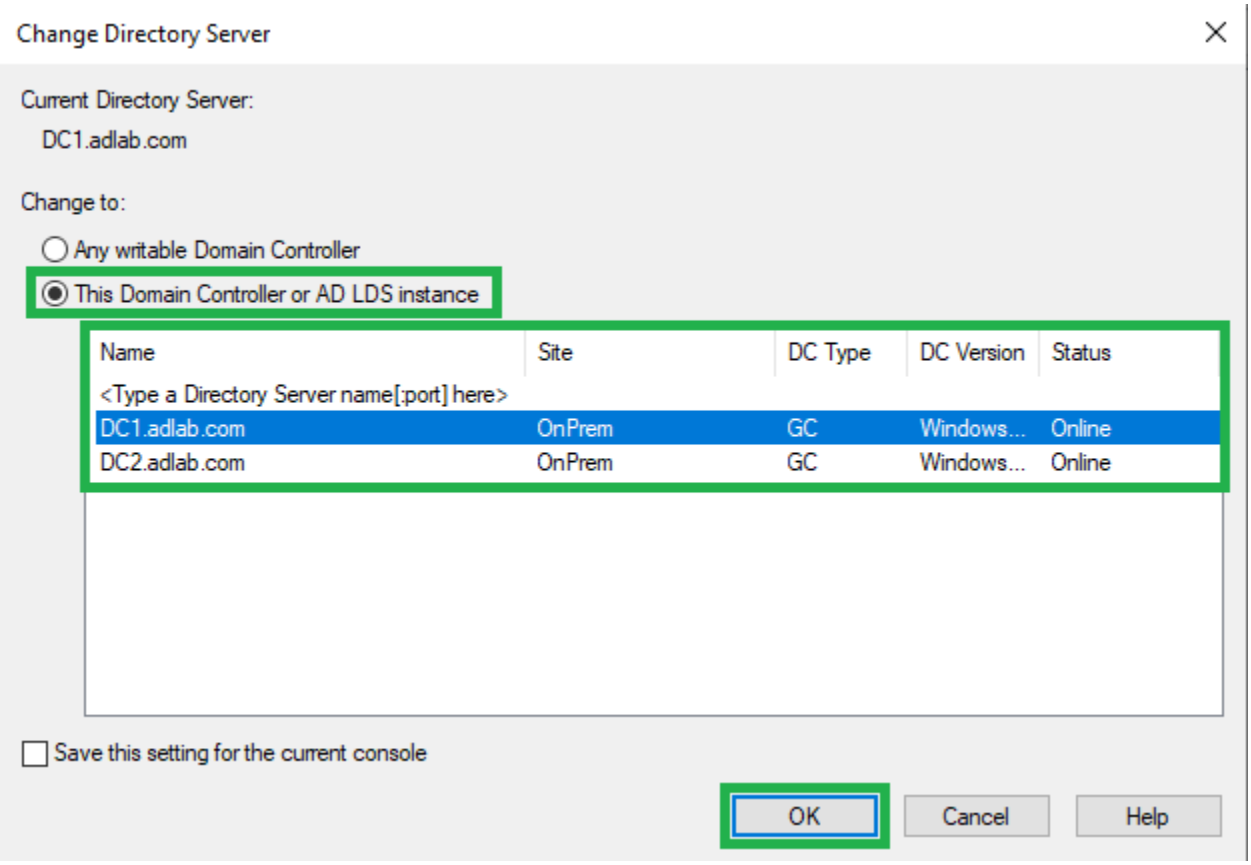
5. In the window that appears, we paste the subnet address that we copied from Azure virtual network page to the **Prefix** section, click on our site's name at the bottom, and confirm with **OK**.



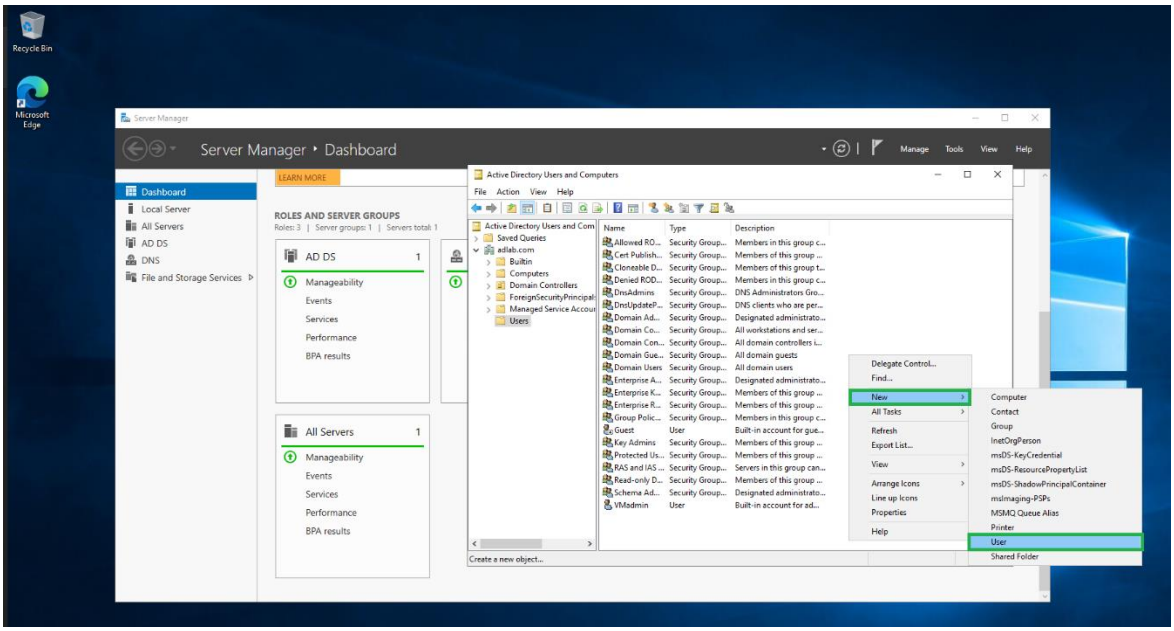
6. We then go to **Tools**, select **Active Directory Users and Computers**, right click on the first section and select **Change Domain Controller…**



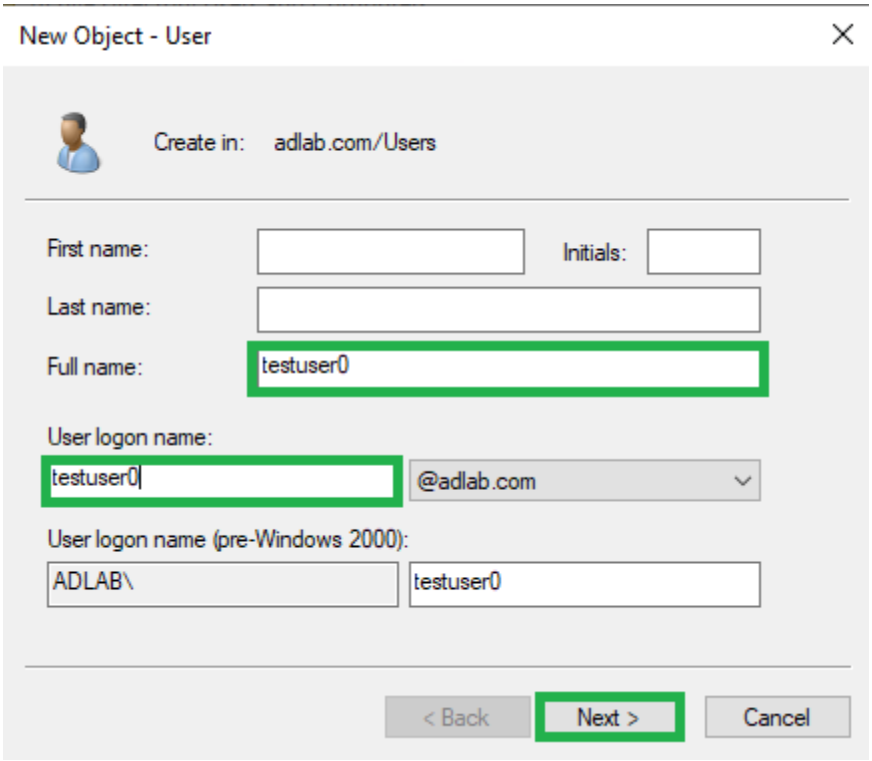
7. We can now see that both domain controllers are available and we have the option to switch between them. We select one and click on **OK**.



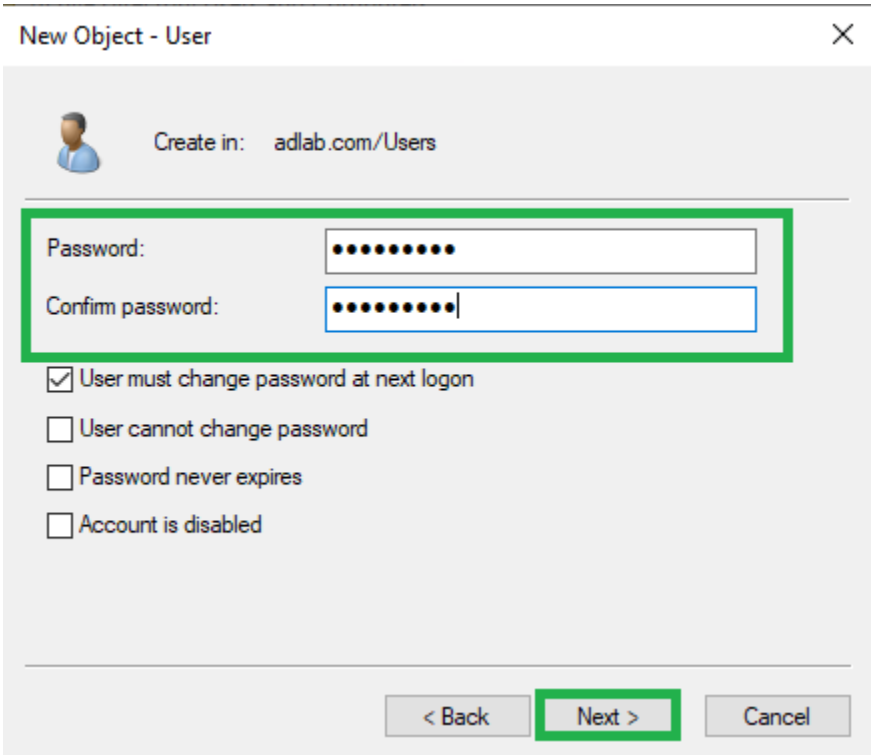
8. We now go to **Users** and create a **New User** by right clicking in the **Users** window to test out that the setup and configuration were successful.

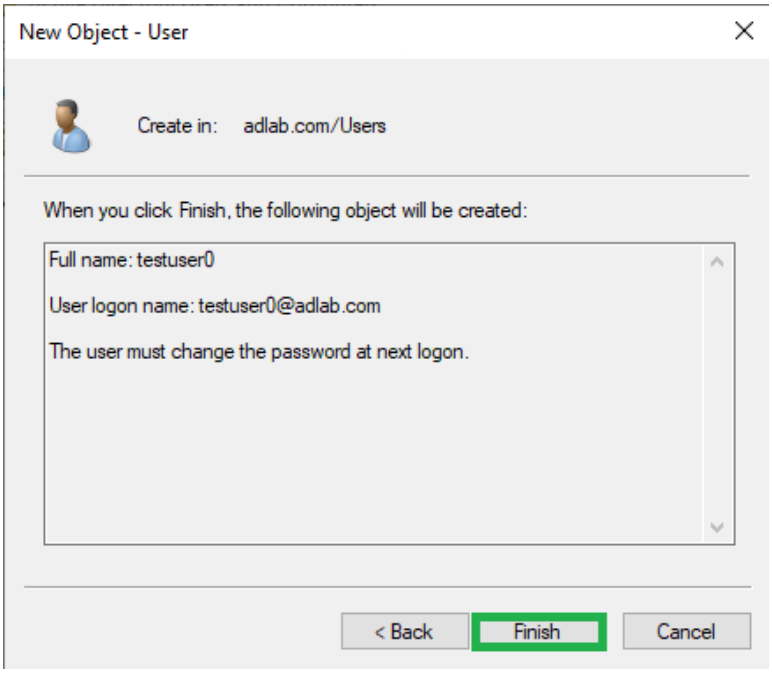


9. We think of a name for our new user – for example, **testuser0**, type it into the **Full name** and **User logon name** sections, and click on **Next**.

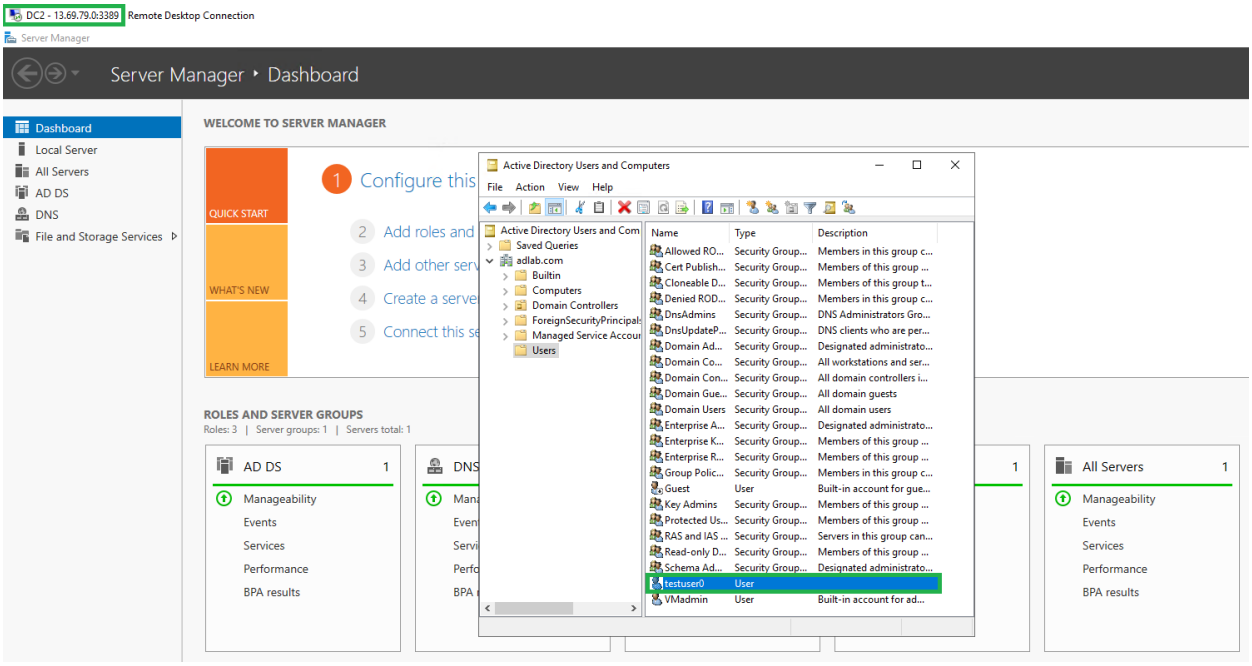


10. We create a password for the user and select **Next**, then click on **Finish** in the following window.





11. To confirm user replication works properly, we now log back into **DC2**, go to **Tools** and select **Active Diretory Users and Computers**. If we go to **Change Domain Controller…** again and switch between **DC1.adlab.com** or **DC2.adlab.com**, testuser0 should appear regardless of our selection.



We have successfully deployed a dual domain controller in Azure and are using the domain controller's Active Directory and DNS (instead of the Azure DNS) to do all of the work. This lab can now be used for any other resources that we would like to test (Site-to-Site VPN/Point-to-Site VPN/Hub-and-Spoke VPN and others, user creation, work policies, installing Azure's Entra Connect to synchronize with Microsoft Entra ID for a hybrid identity setup etc.).