

# Building a Traditional Active Directory 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.

Home > Resource groups >

### Create a resource group

Basics Tags Review + create

Resource group - A container that holds related resources for an Azure solution. The resource group can include all the resources for the solution, or only those resources that you want to manage as a group. You decide how you want to allocate resources to resource groups based on what makes the most sense for your organization. [Learn more](#)

**Project details**

Subscription \* ⓘ Azure subscription 1 ✓

Resource group \* ⓘ AD-LAB ✓

**Resource details**

Region \* ⓘ (Europe) West Europe ✓

Review + create < Previous Next : Tags >

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.

The screenshot shows the 'Create virtual network' page in the Azure portal. The 'Basics' tab is selected. The 'Project details' section shows 'Subscription' as 'Azure subscription 1' and 'Resource group' as 'AD-LAB'. The 'Instance details' section shows 'Virtual network name' as 'OnPremNetwork' and 'Region' as '(Europe) West Europe'. A 'Deploy to an Azure Extended Zone' link is visible below the region dropdown.

**Create virtual network** ...

**Basics** Security IP addresses Tags Review + create

Azure Virtual Network (VNet) is the fundamental building block for your private network in Azure. VNet enables many types of Azure resources, such as Azure Virtual Machines (VM), to securely communicate with each other, the internet, and on-premises networks. VNet is similar to a traditional network that you'd operate in your own data center, but brings with it additional benefits of Azure's infrastructure such as scale, availability, and isolation. [Learn more.](#)

**Project details**

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription \* Azure subscription 1

Resource group \* AD-LAB [Create new](#)

**Instance details**

Virtual network name \* OnPremNetwork

Region \* (Europe) West Europe [Deploy to an Azure Extended Zone](#)

- 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.

The screenshot shows the 'Create virtual network' page in the Azure portal, with the 'IP addresses' tab selected. On the left, a table lists subnets, with the 'default' subnet highlighted. On the right, the 'Edit subnet' panel is open, showing configuration for the 'default' subnet. The 'Starting address' is set to '10.0.1.0/24'. The 'Save' button is highlighted in green.

Microsoft Azure Upgrade Search resources, services, and docs (G+V) Copilot

Home > Virtual networks > Create virtual network ...

**Create virtual network** ...

Basics Security **IP addresses** Tags Review + create

Configure your virtual network address space with the IPv4 and IPv6 addresses and subnets you need. [Learn more.](#)

Define the address space of your virtual network with one or more IPv4 or IPv6 address ranges. Create subnets to segment the virtual network address space into smaller ranges for use by your applications. When you deploy resources into a subnet, Azure assigns the resource an IP address from the subnet. [Learn more.](#)

+ Add a subnet

Subnets	IP address range	Size	NAT gateway
default	10.0.0.0 - 10.0.0.255	/24 (256 addresses)	

+ Add IPv4 address space

**Edit subnet**

Select an address space and configure your subnet. You can customize a default subnet or select from subnet templates if you plan to add select services later. [Learn more.](#)

Subnet purpose: Default

Name: default

IPv4

Include an IPv4 address space: ☒

IPv4 address range: 10.0.0.0 - 10.0.255.255

Starting address: 10.0.1.0/24

Size: /24 (256 addresses)

Subnet address range: 10.0.1.0 - 10.0.1.255

IPv6

Include an IPv6 address space: ☐ This virtual network has no IPv6 address ranges.

**Private subnet**

Private subnets enhance security by not providing default outbound access. To enable outbound connectivity for virtual machines to access the internet, it is necessary to explicitly grant outbound access. A NAT gateway is the recommended way to provide outbound connectivity for virtual machines in the subnet. [Learn more.](#)

Enable private subnet (no default outbound access): ☐

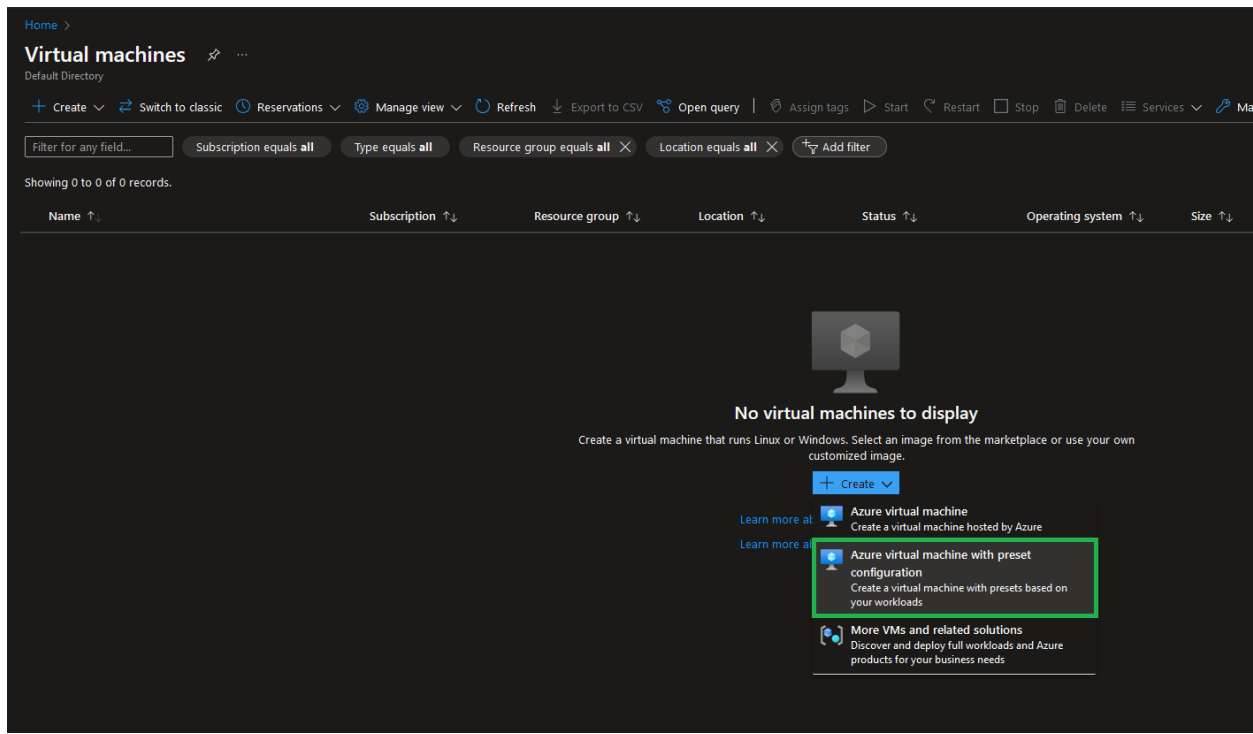
**Security**

Simply internet access for virtual machines by using a network address translation gateway. Filter subnet traffic using a network security group. [Learn more.](#)

NAT gateway: None [Create new](#)

**Save** Cancel [Give feedback](#)

- 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.



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

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

Home > Virtual machines > Choose recommended defaults that match your workload >

## Create a virtual machine

Help me create a low cost VM Help me create a VM optimized for high availability Help me choose the right VM size for my workload

Subscription \* Azure subscription 1

Resource group \* AD-LAB  
Create new

Instance details

Virtual machine name \* DC1

Region \* (Europe) West Europe

Availability options \* Availability set

Based on your input, you might want to consider creating this resource as a virtual machine scale set, which allows you to manage, configure and scale load balanced virtual machines. [Create as VMSS](#)

Availability set \*  
Create new  
The value must not be empty.

Security type \* Trusted launch virtual machines  
Configure security features

Image \* Windows Server 2019 Datacenter - x64 Gen2 (free services eligible)  
See all images | Configure VM generation

VM architecture \*  
Arm64  
x64  
Arm64 is not supported with the selected image.

Run with Azure Spot discount ☐

< Previous Next : Disks > Review + create

### Create availability set

Group two or more VMs in an availability set to ensure that at least one is available during planned or unplanned maintenance events. [Learn more](#)

Name \* ADSet

Fault domains 2

Update domains 5

Use managed disks \*  
No (classic) Yes (Aligned)

OK

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

Basics Disks Networking Management Monitoring Advanced Tags Review + create

Azure VMs have one operating system disk and a temporary disk for short-term storage. You can attach additional data disks. The size of the VM determines the type of storage you can use and the number of data disks allowed. [Learn more](#)

### VM disk encryption

Azure disk storage encryption automatically encrypts your data stored on Azure managed disks (OS and data disks) at rest by default when persisting it to the cloud.

Encryption at host ☐

Encryption at host is not registered for the selected subscription. [Learn more](#)

### OS disk

OS disk size \* Image default (127 GiB)

OS disk type \* Standard HDD (locally-redundant storage)  
The selected VM size supports premium disks. We recommend Premium SSD for high IOPS workloads. Virtual machines with Premium SSD disks qualify for the 99.9% connectivity SLA.

Delete with VM ☒

Key management \* Platform-managed key

Enable Ultra Disk compatibility ☐

### Data disks for DC1

You can add and configure additional data disks for your virtual machine or attach existing disks. This VM also comes with a temporary disk.

LUN	Name	Size (GiB)	Disk type	Host cachi...	Delete with VM
<a href="#">Create and attach a new disk</a> <a href="#">Attach an existing disk</a>					

< Previous Next : Networking > Review + create

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

Select a disk size

Browse available disk sizes and their features.

Storage type: Standard HDD (locally-redundant storage)

Size	Performance tier	Provisioned IOPS	Provisioned throughput	Max Shares	Max burst IOPS	Max burst throughput
32 GiB	S4	500	60	-	-	-
64 GiB	S6	500	60	-	-	-
128 GiB	S10	500	60	-	-	-
256 GiB	S15	500	60	-	-	-
512 GiB	S20	500	60	2	-	-
1024 GiB	S30	500	60	5	-	-
2048 GiB	S40	500	60	5	-	-
4096 GiB	S50	500	60	5	-	-
8192 GiB	S60	1300	300	5	-	-
16384 GiB	S70	2000	500	5	-	-
32767 GiB	S80	2000	500	5	-	-

Custom disk size (GiB): 10

- 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.

Create a virtual machine

Help me create a low cost VM | Help me create a VM optimized for high availability | Help me choose the right VM size for my workload

VM disk encryption

Azure disk storage encryption automatically encrypts your data stored on Azure managed disks (OS and data disks) at rest by default when persisting it to the cloud.

Encryption at host: ☐

OS disk

OS disk size: Image default (127 GiB)

OS disk type: Standard HDD (locally-redundant storage)

Delete with VM: ☒

Key management: Platform-managed key

Enable Ultra Disk compatibility: ☐

Data disks for DC1

You can add and configure additional data disks for your virtual machine or attach existing disks. This VM also comes with a temporary disk.

LUN	Name	Size (GiB)	Disk type	Host caching	Delete with VM
0	DC1_DataDisk_0	10	Standard HDD ...	Read-only	<input type="checkbox"/>

Create and attach a new disk | Attach an existing disk

< Previous | Next : Networking > | Review + create

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 purposed of this project.

Home > Virtual machines > Choose recommended defaults that match your workload >


## Create a virtual machine

Help me create a low cost VM   Help me create a VM optimized for high availability   Help me choose the right VM size for my workload


Basics   Disks   Networking   Management   **Monitoring**   Advanced   Tags   Review + create


Configure monitoring options for your VM.

### Alerts


Enable recommended alert rules  ☐

### Diagnostics

Boot diagnostics  ☐ Enable with managed storage account (recommended)  
☐ Enable with custom storage account  
☒ **Disable**

Enable OS guest diagnostics  ☐

### Health

Enable application health monitoring  ☐

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

Home > DC1

## DC1 | Connect

Virtual machine

Search



Refresh   Troubleshoot   More Options   Feedback

Overview  
Activity log  
Access control (IAM)  
Tags  
Diagnose and solve problems  
Connect  
**Connect**  
Bastion  
Windows Admin Center

Networking  
Network settings  
Load balancing  
Application security groups  
Network manager

Settings  
Disks  
Extensions + applications  
Operating system  
Configuration  
Advisor recommendations  
Properties  
Locks


Connecting using  
Public IP address | 13.94.208.124

Admin username : VMadmin  
Port (change) : 3389  Check access  
Just-in-time policy : Unsupported by plan 

### Most common

**Local machine**

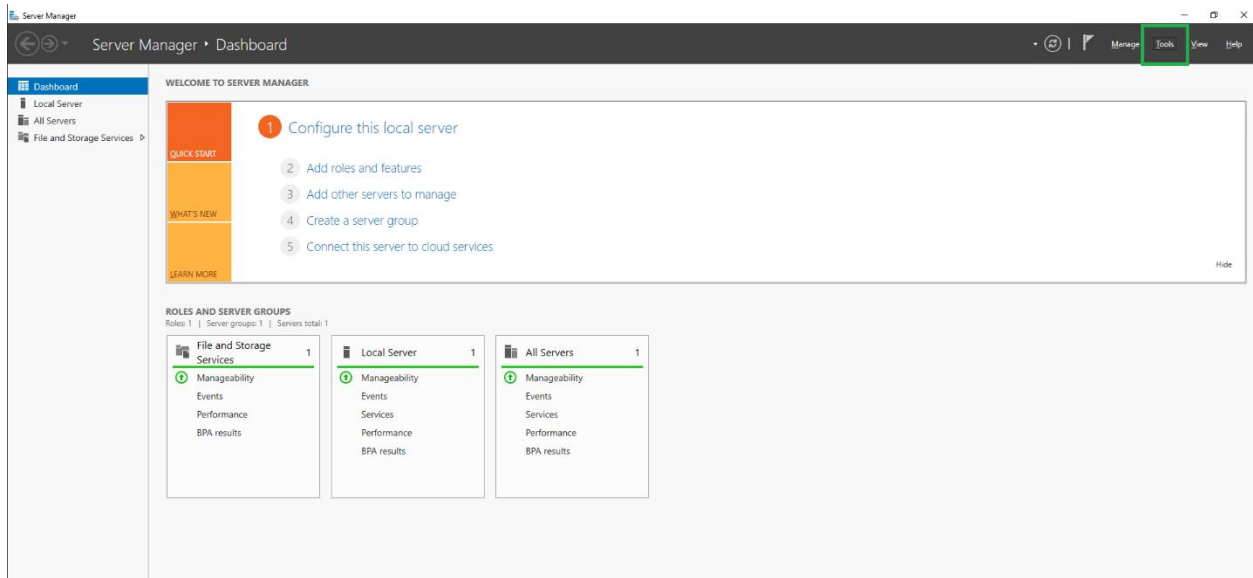
**Native RDP**  
Connect via native RDP without any additional software needed. Recommended for testing only.  
Public IP address (13.94.208.124)

Select   **Download RDP file**   

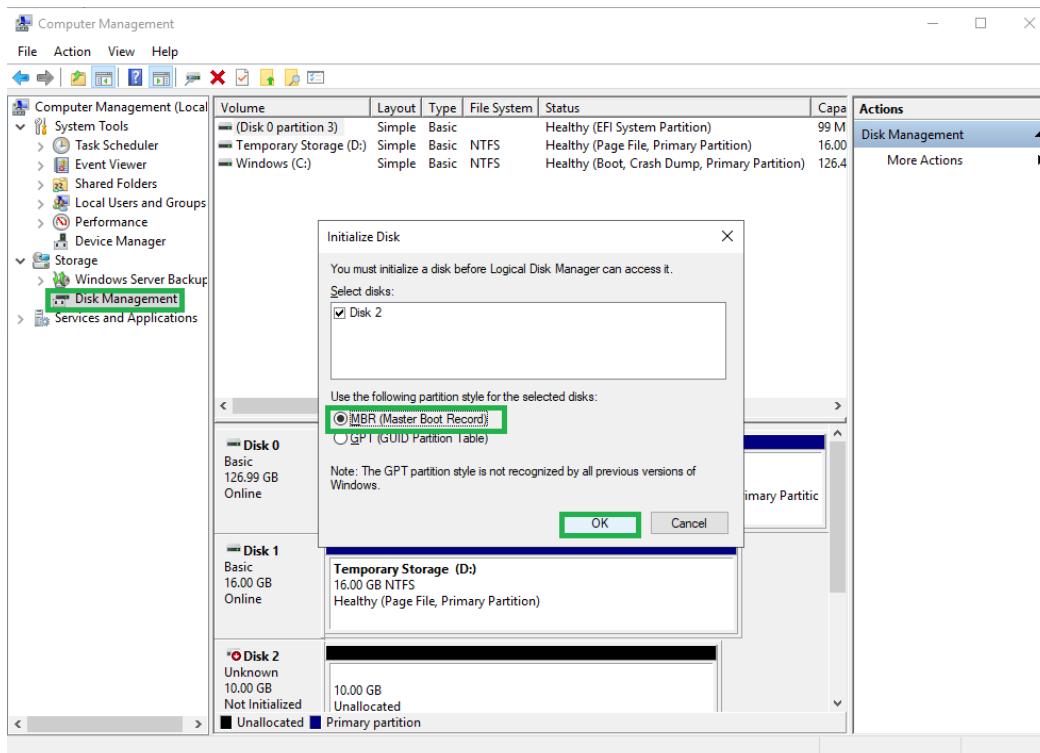
More ways to connect (4)

## Task 2: Setting up our domain controllers

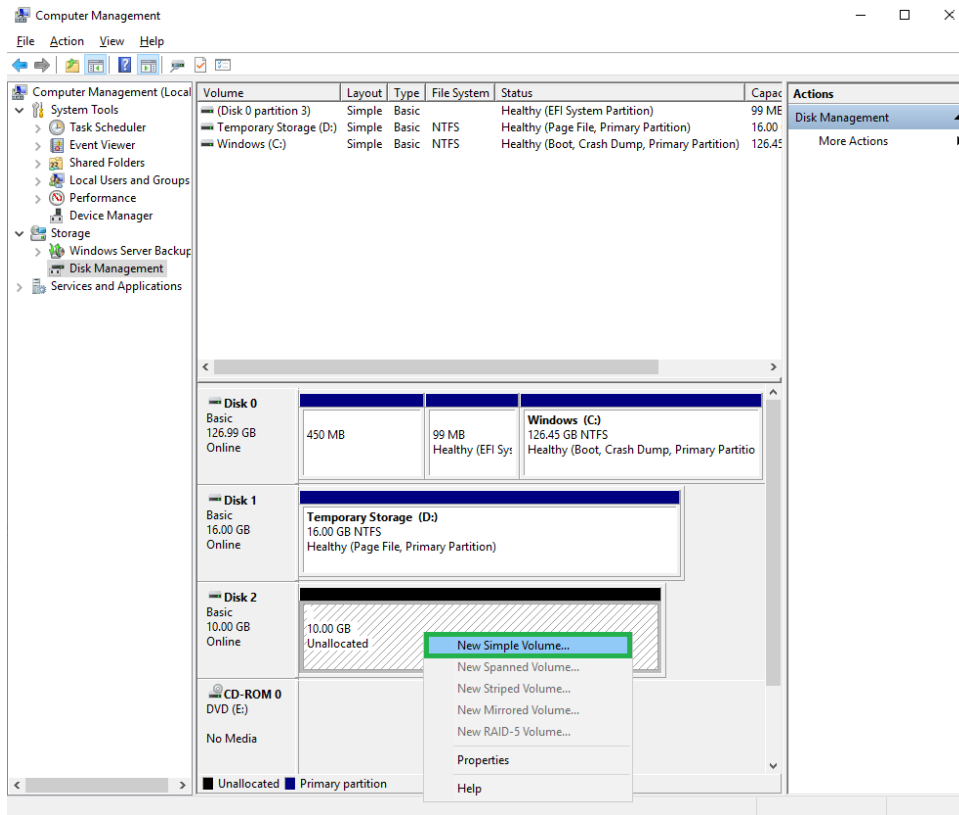
1. Once we've logged into **DC1**, we click on **Yes** when asked whether we want this PC to be discoverable by other PCs and devices on this network. We then go to **Tools** within the newly loaded Server Manager window, and select **Computer Management**.



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

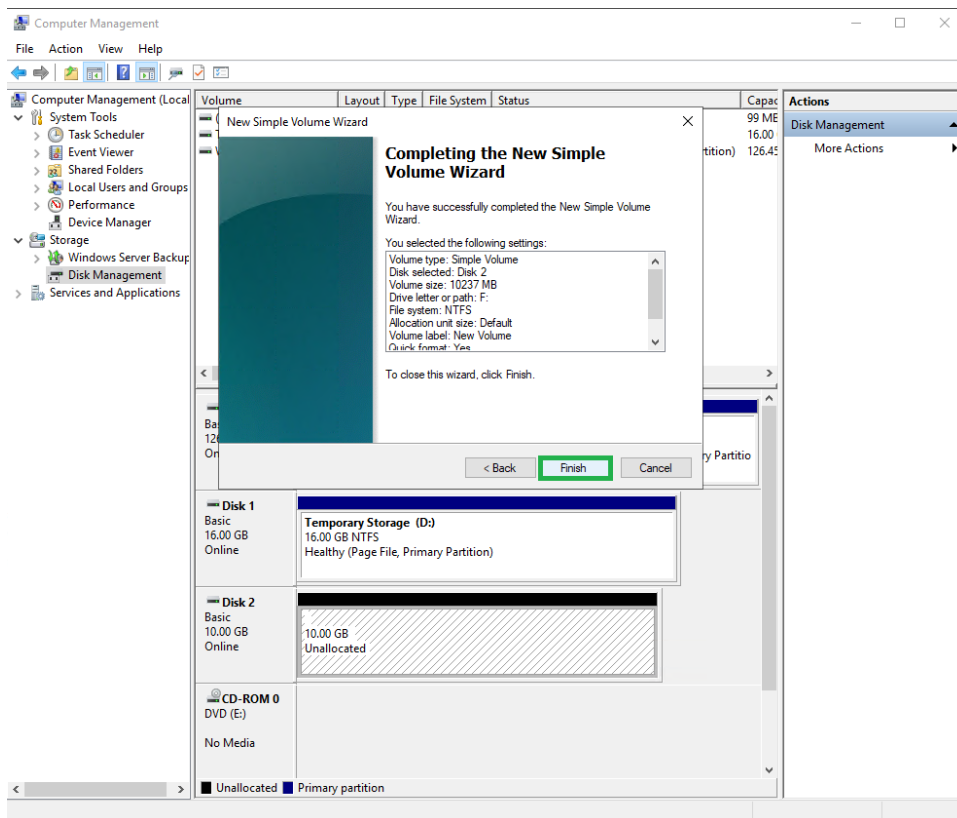


3. We then right click on Disk 2, which is the disk we created in Azure during our VM's initial configuration, and select **New Simple Volume**.

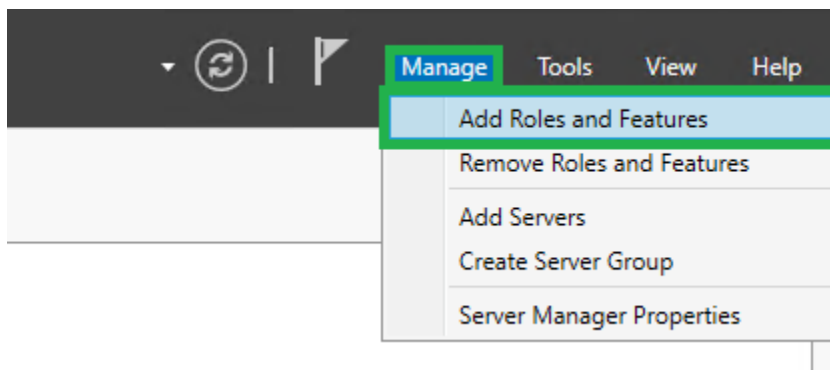


4. We click through all default settings in the Wizard and select **Finish**.

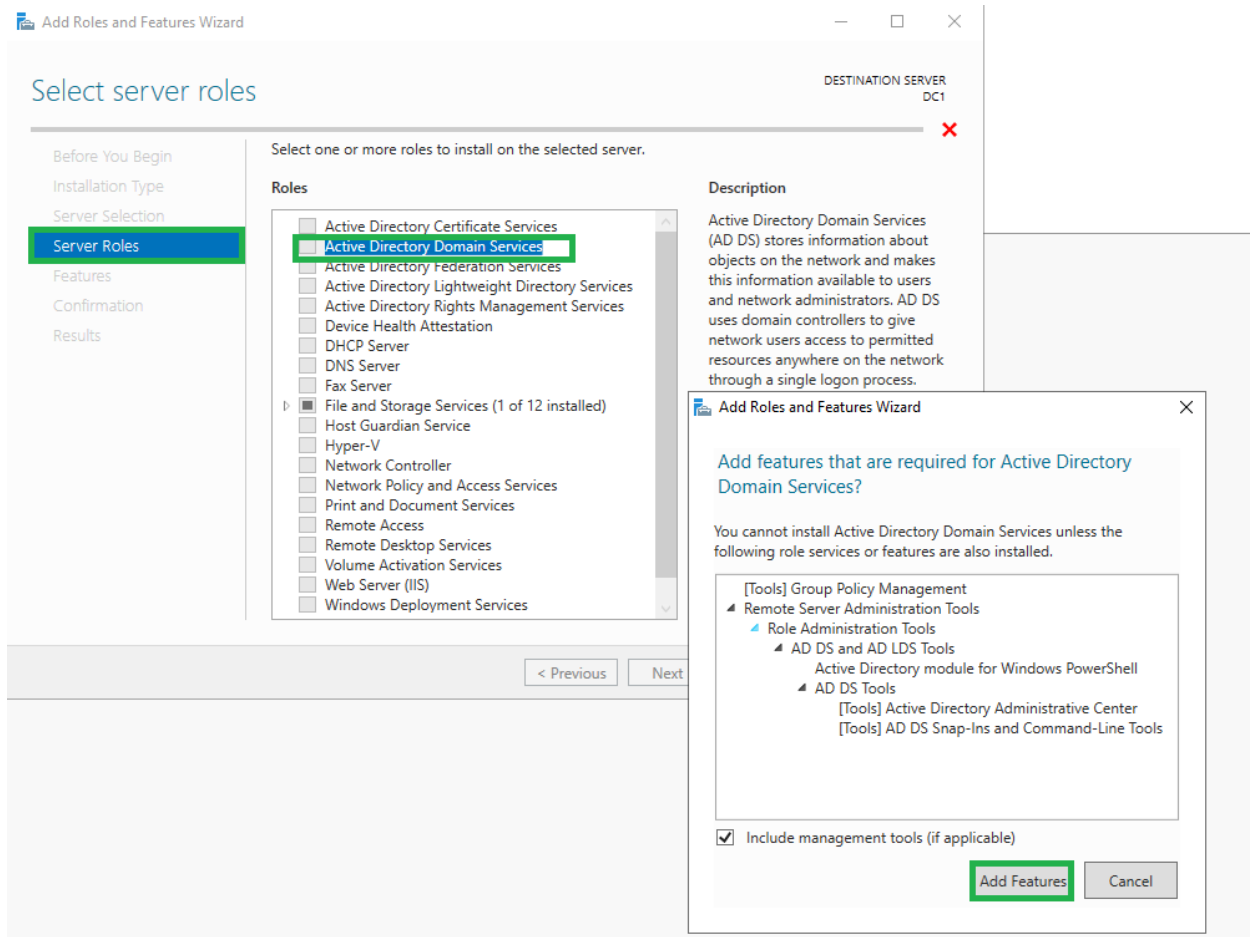




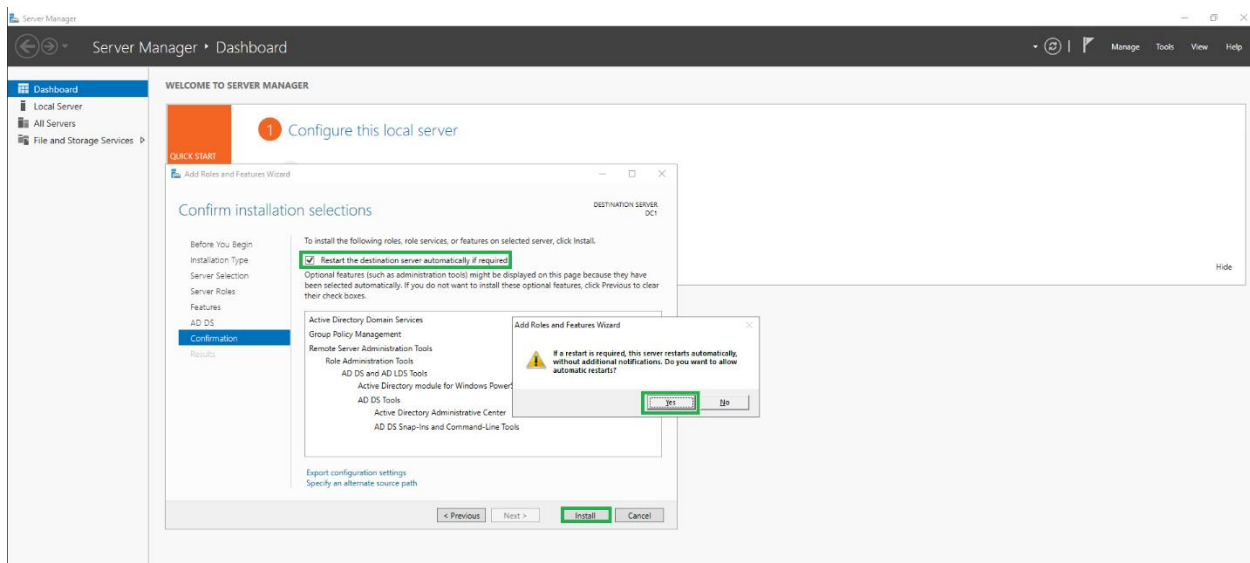
5. We then need to install Active Directory. We do so by clicking on **Manage** and selecting **Add Roles and Features**.



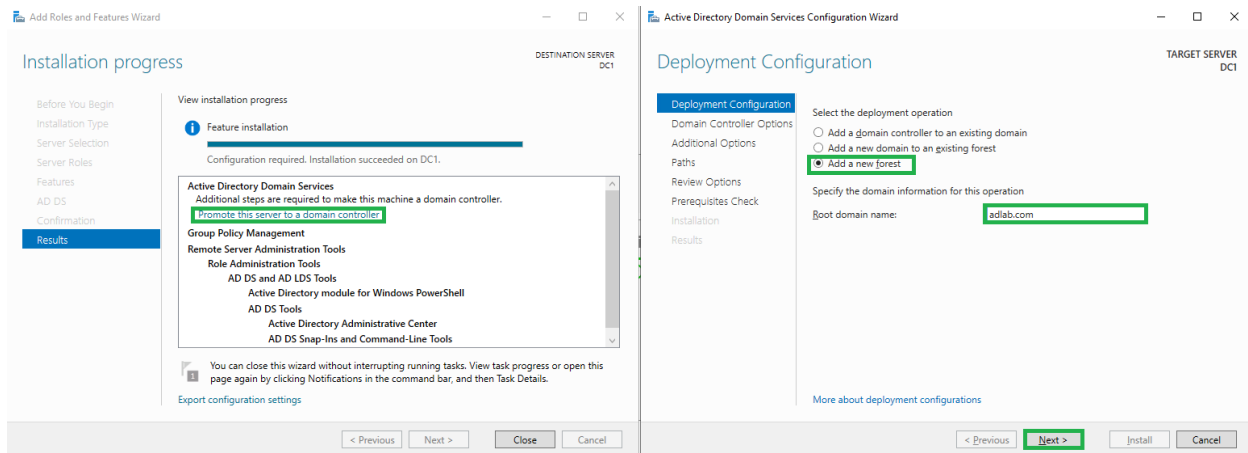
6. In the Wizard that pops up, we select **Role-based or feature-based installation**, leave in the defaults until we reach the **Server Roles** page, where we select the **Active Directory Domain Services** box and click on the **Add Features** button in the new window that will appear.



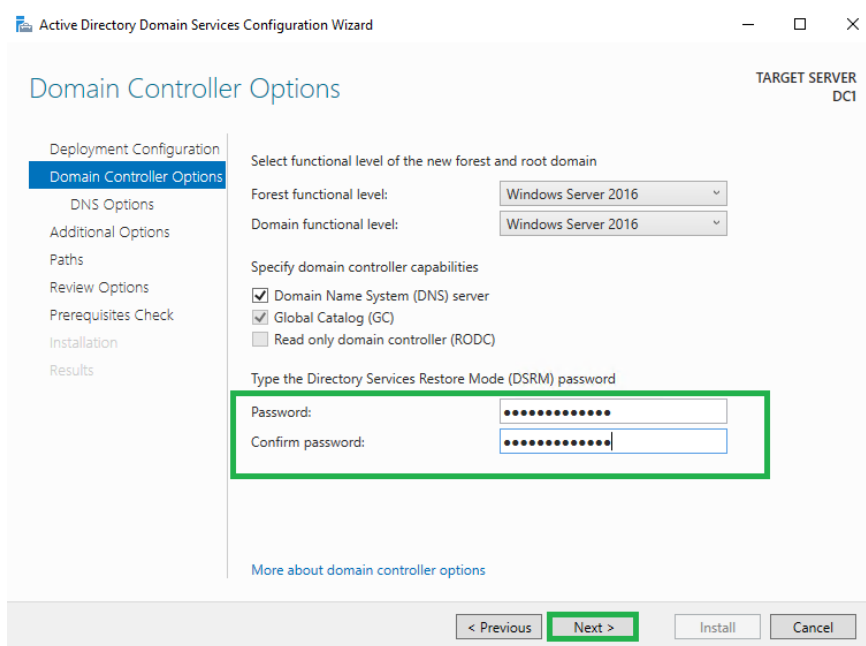
- We then click through the rest of the defaults using the **Next** button until we reach the **Confirmation** page, where we select the **Restart the destination server automatically if required** box, confirm our choice on the pop-up window by choosing **Yes**, and then finalize the process by clicking on **Install**.



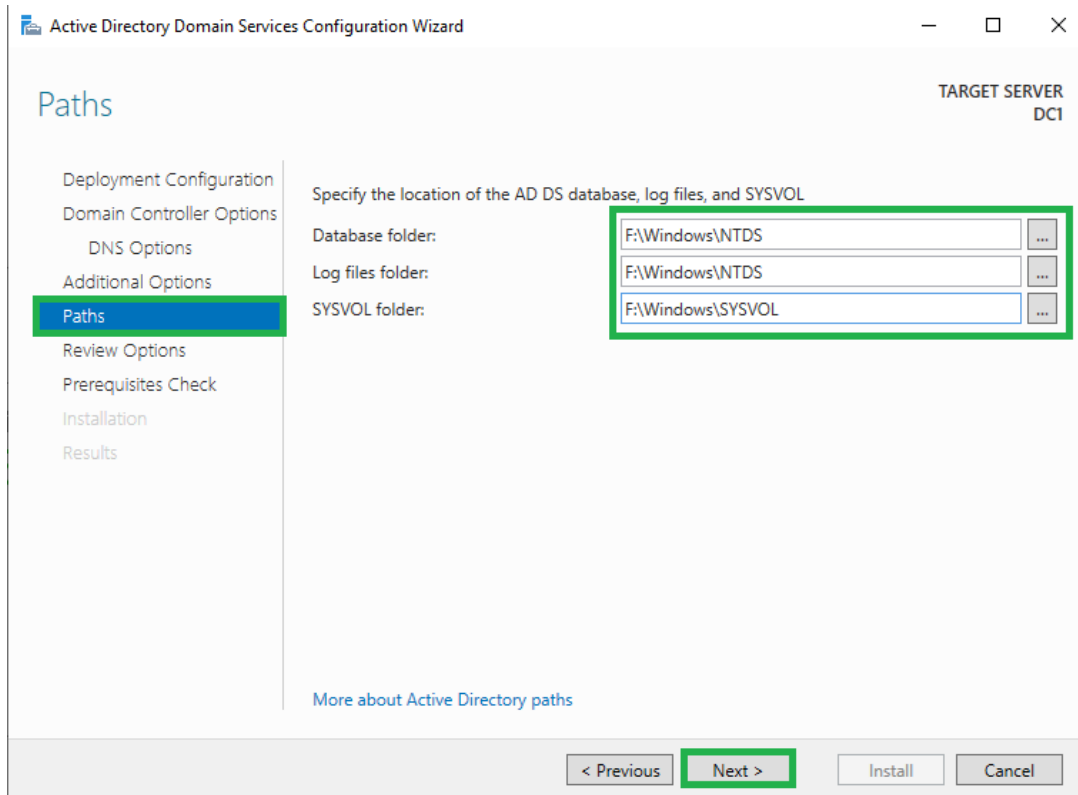
8. Once this is done, we click on **Promote this server to a domain controller** and select the **Create a new forest** radio button, and specify a domain name of our choice.



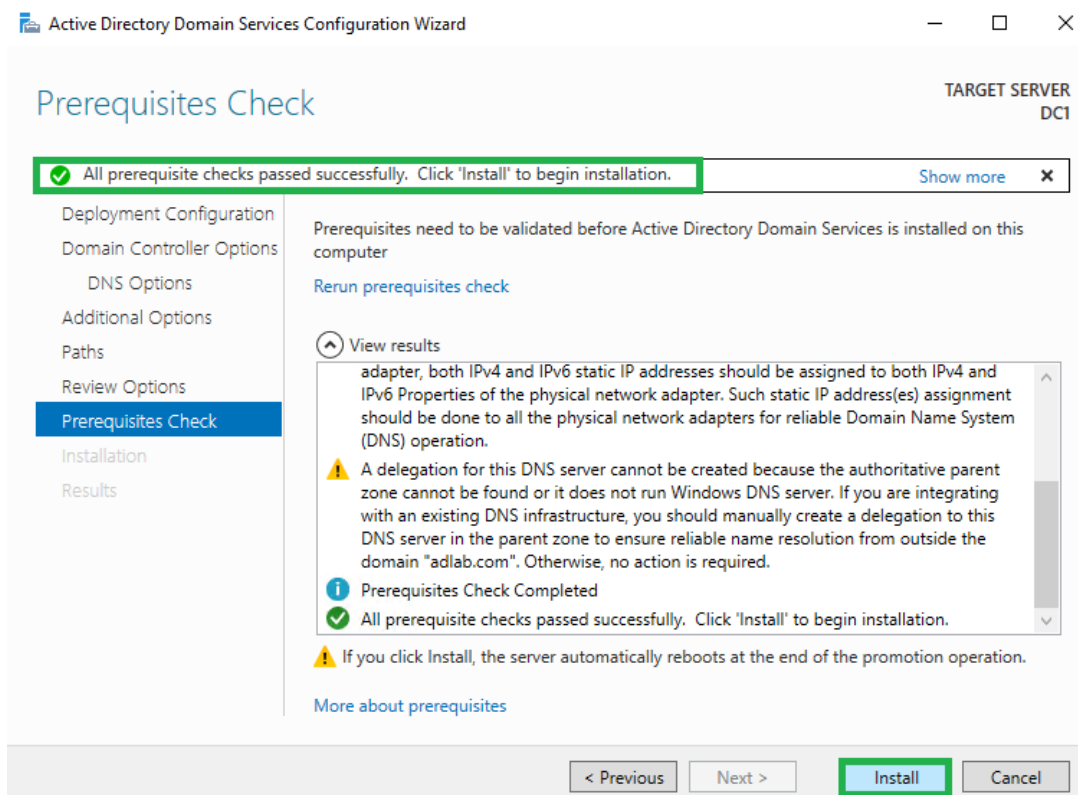
9. We create a password on the following page and click **Next**, as we can leave the other options at their defaults.



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.

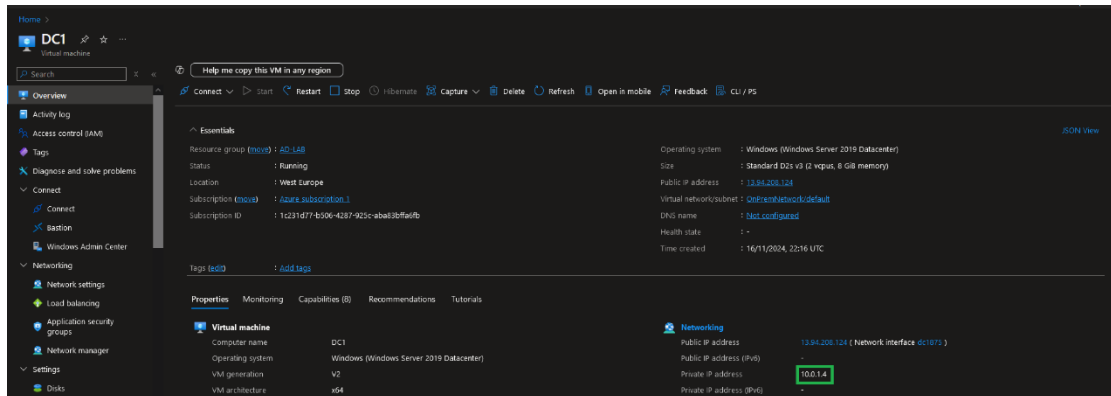


**Note:** We will configure the DNS settings later because we want to use the DNS of the server itself instead of the Azure DNS, so that our two domain controllers can talk to each other.

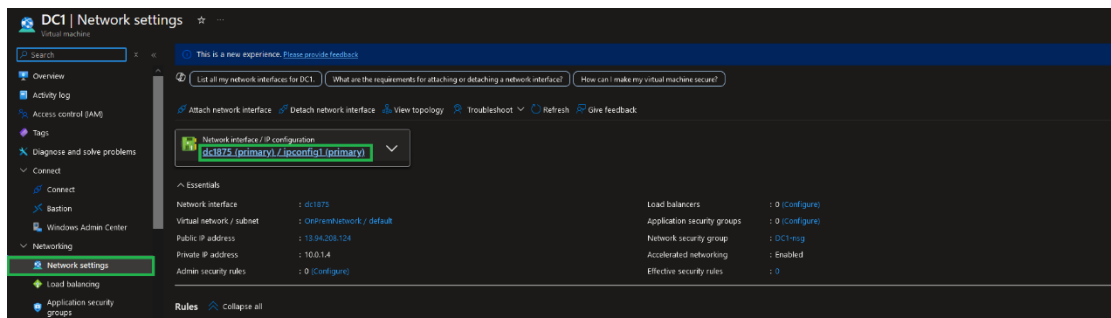
12. We then repeat this process by create a second VM called **DC2** in Azure with the exact same configuration settings.

**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.

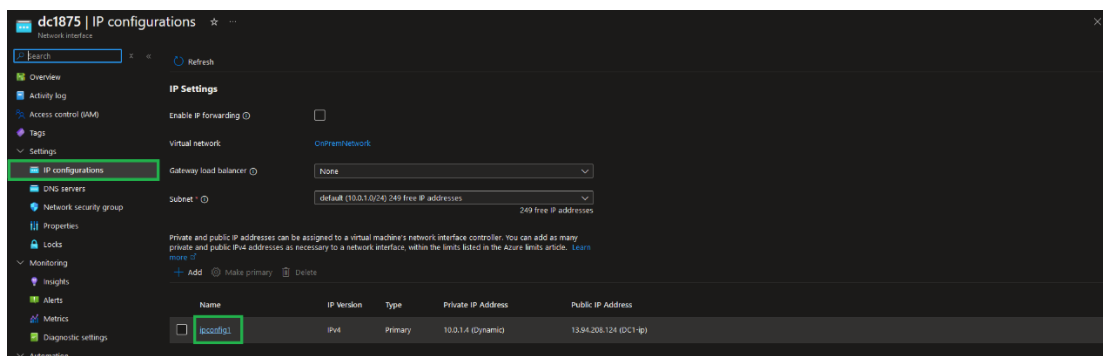
13. We now need to go **DC1**'s Azure page and take a note of its Private IP address.



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**.

**Edit IP configuration** dc1875

❗ A primary IP configuration already exists. Any additional IP configurations will be secondary. The virtual network this network interface is attached to only supports IPv4. [Learn more](#)

Name \*

IP version IPv4

Type Primary

**Private IP address settings**

Allocation ☐ Dynamic ☒ **Static**

Private IP address \*

**Public IP address settings**

Associate public IP address ☒

Public IP address \*  [Create a public IP address](#)

**Save** **Cancel** [Give feedback](#)

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**.

Home > AD-LAB > OnPremNetwork

**OnPremNetwork | DNS servers** Virtual network

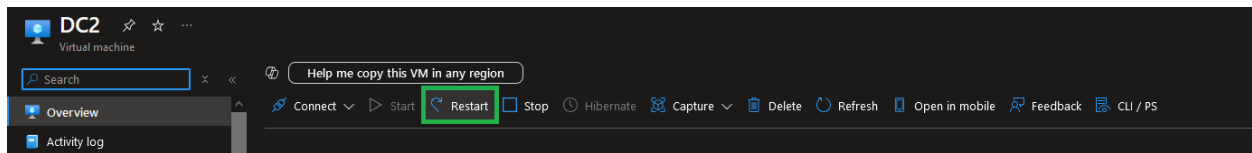
Virtual machines and Application gateways (v2.3KJ) within this virtual network must be restarted to utilize the updated DNS server settings.

DNS servers ☐ Default (Azure-provided) ☒ **Custom**

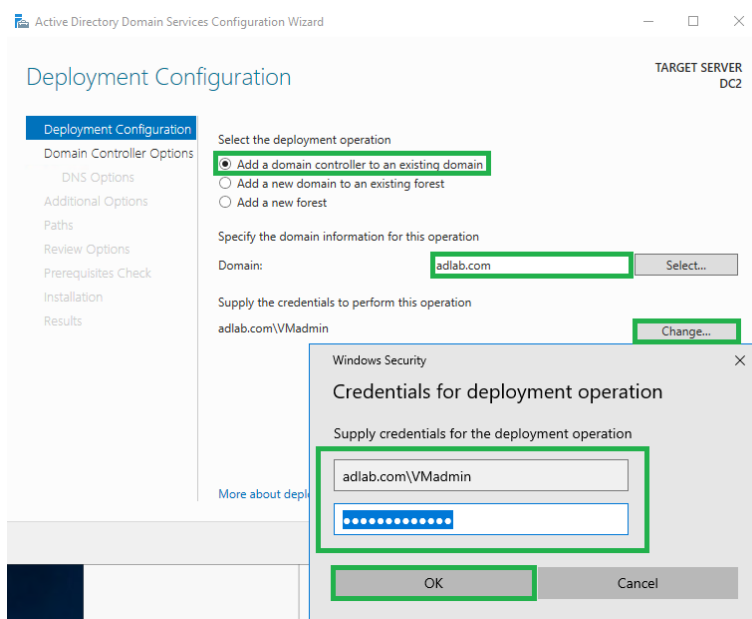
IP Address  [Add DNS server](#)

**Save** **Cancel** [Give feedback](#)

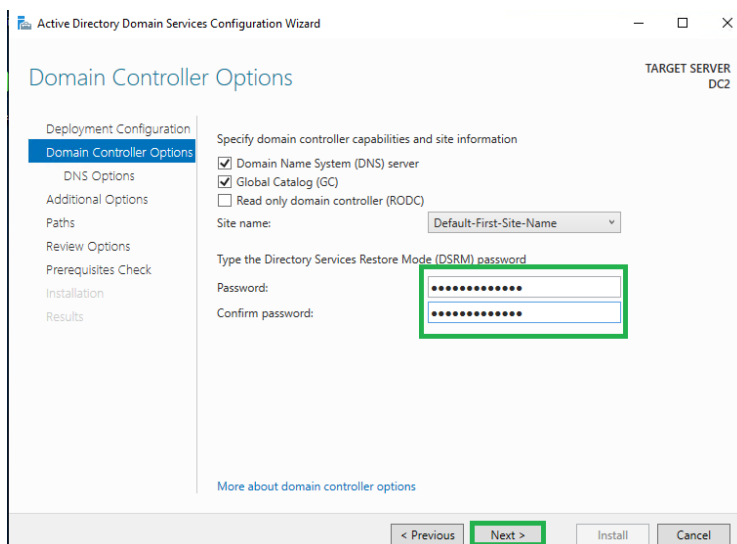
18. The **DC2** VM should now be restarted, so that it can get it's DNS from **DC1**'s AD instead of Azure.



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**.

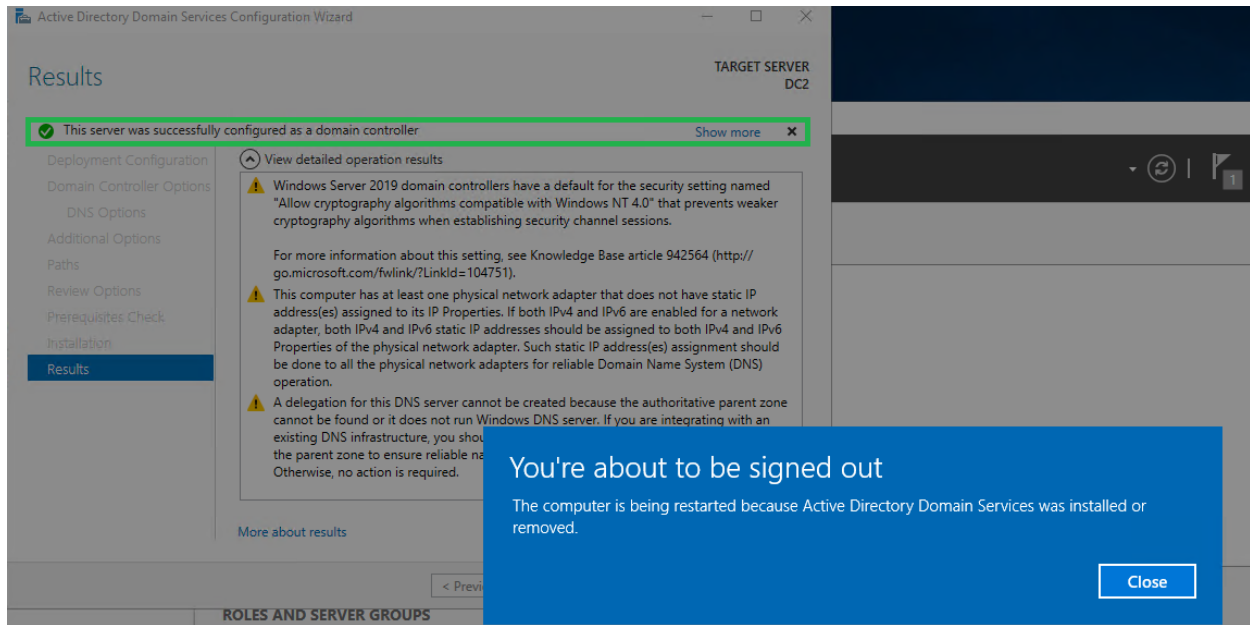
The screenshot shows the 'Additional Options' page of the Active Directory Domain Services Configuration Wizard. The left-hand navigation pane lists several steps: Deployment Configuration, Domain Controller Options, DNS Options, Additional Options (highlighted in blue), Paths, Review Options, Prerequisites Check, Installation, and Results. The main content area is titled 'Additional Options' and includes a 'Specify Install From Media (IFM) Options' section with an unchecked 'Install from media' checkbox. Below this is the 'Specify additional replication options' section, which contains a 'Replicate from:' label and a dropdown menu. The dropdown menu is open, showing three options: 'Any domain controller', 'Any domain controller', and 'DC1.adlab.com' (which is highlighted in blue). At the bottom of the wizard, there are four buttons: '< Previous', 'Next >' (highlighted in blue), 'Install', and 'Cancel'. The top right corner of the window indicates 'TARGET SERVER DC2'.

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.

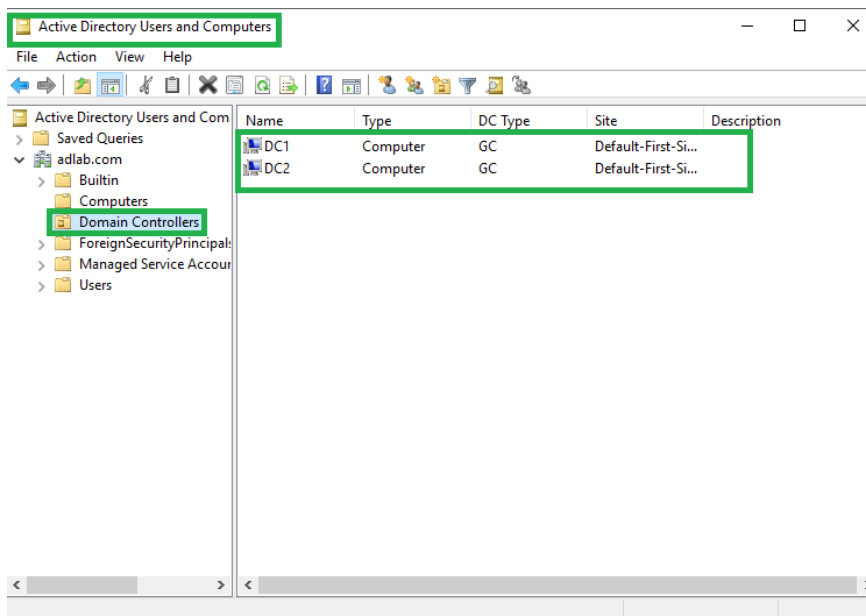
The screenshot shows the 'Paths' page of the Active Directory Domain Services Configuration Wizard. The left-hand navigation pane lists several steps: Deployment Configuration, Domain Controller Options, DNS Options, Additional Options, Paths (highlighted in blue), Review Options, Prerequisites Check, Installation, and Results. The main content area is titled 'Paths' and includes a section titled 'Specify the location of the AD DS database, log files, and SYSVOL'. This section contains three input fields: 'Database folder:', 'Log files folder:', and 'SYSVOL folder:'. Each field has a text box containing 'F:\Windows\NTDS' or 'F:\Windows\SYSVOL' and a browse button (three dots) to the right. The entire section is highlighted with a green border. At the bottom of the wizard, there are four buttons: '< Previous', 'Next >' (highlighted in blue), 'Install', and 'Cancel'. The top right corner of the window indicates 'TARGET SERVER DC2'.



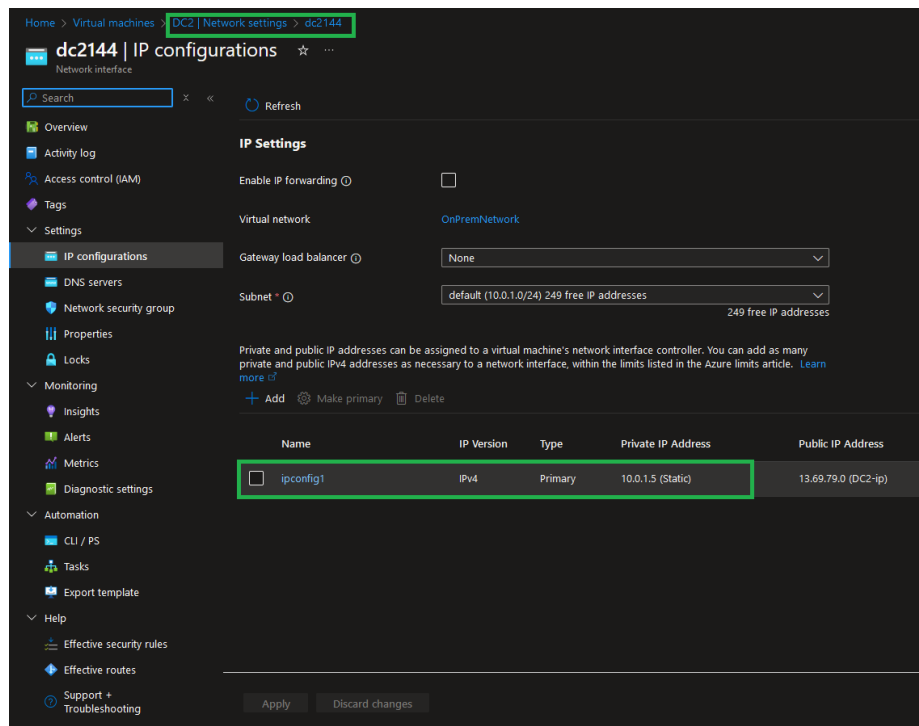
23. We click through the following pages and install Active Directory just like before. The VM will reboot after the installation is completed.



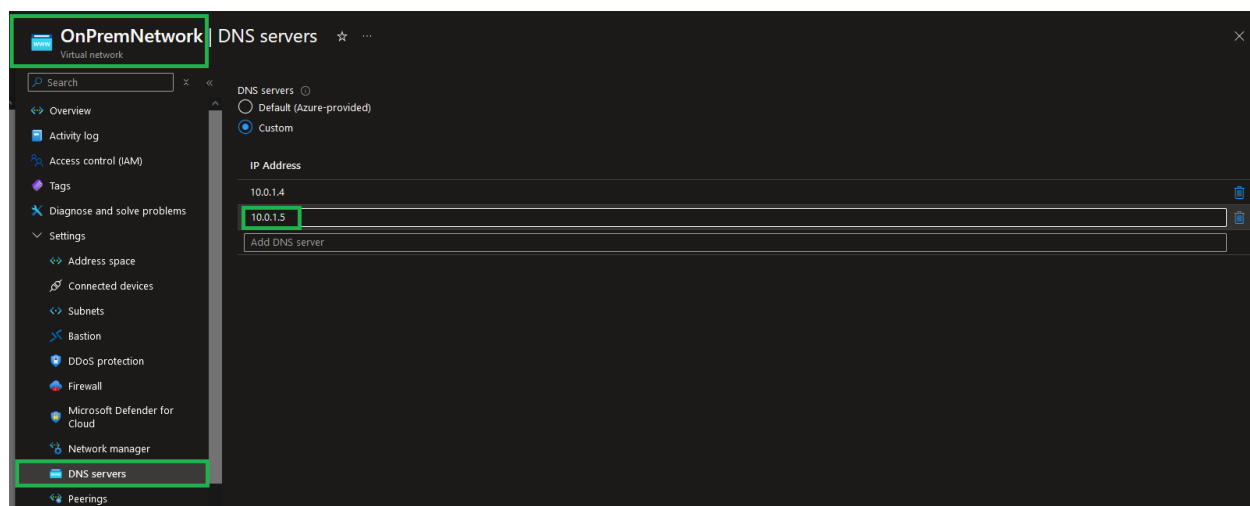
24. If we now go to **Tools** and click on **Active Directory Users and Computers** on **DC2**, we should see both VMs in the **Domain Controllers** section.



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

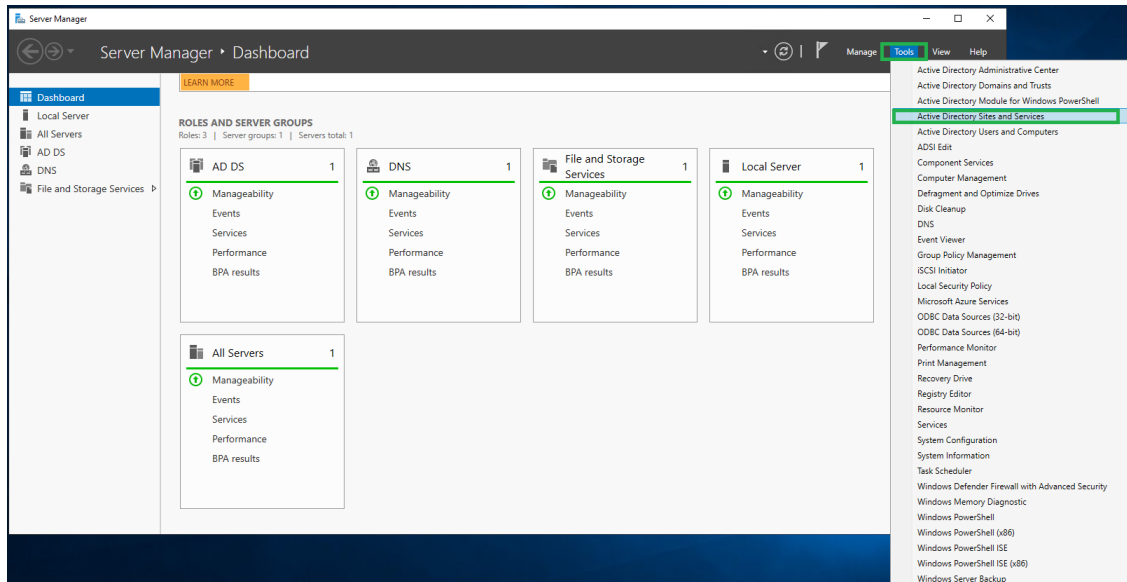


26. We also repeat the process of adding the new domain controller – **DC2**’s IP address as a DNS server on our virtual network, same as with **DC1** earlier.

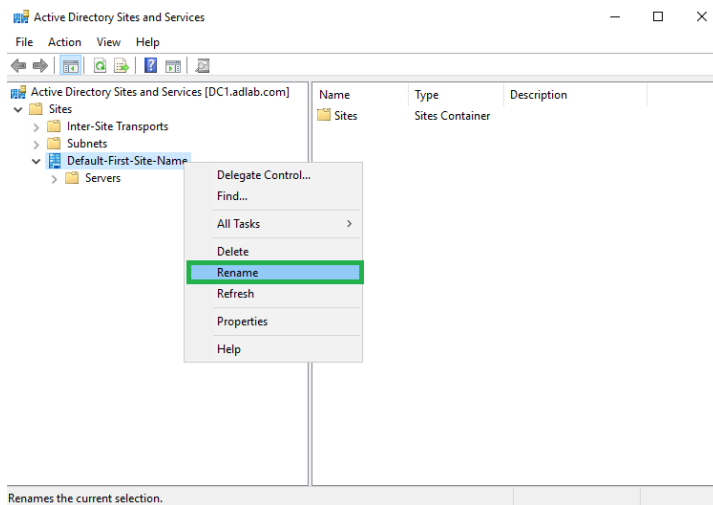


## Task 3: Finalizing and testing the Active Directory configuration

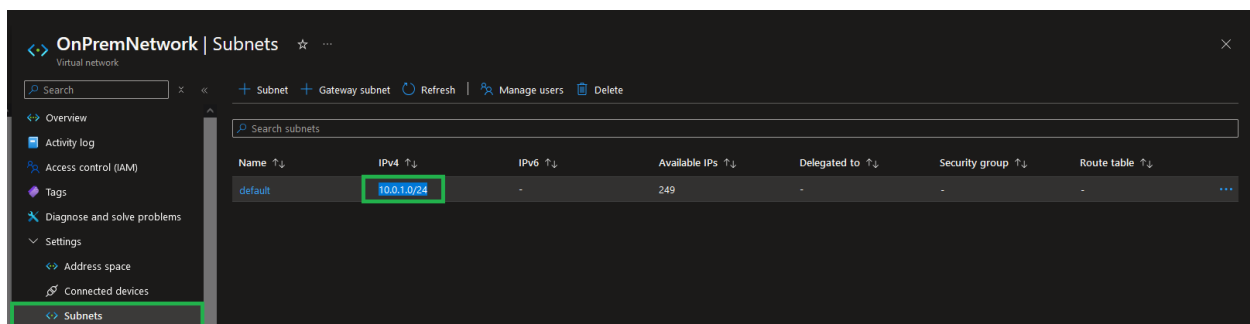
1. We open Server Manager on **DC1**, go to Tools and click on **Active Directory Sites and Services**.



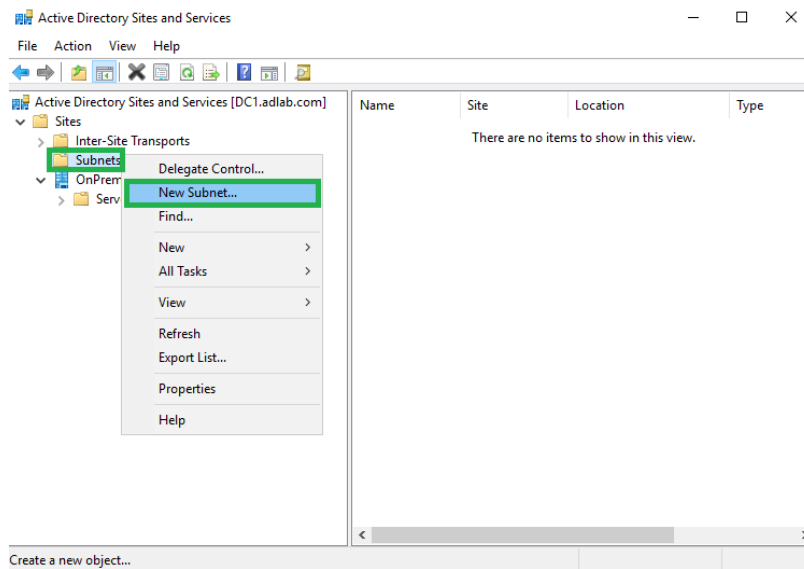
2. We scroll down to our site called Default-First-Site-Name and rename it to something like **OnPrem**, for example.



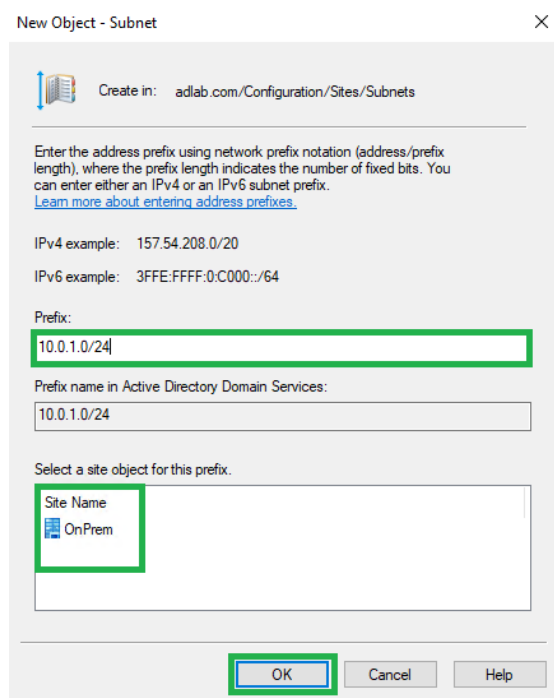
3. We then want to add our virtual network's subnet address to the **Subnets** section. We do this by going back to our Azure virtual network page and selecting the *Subnets* blade where we can view and copy our subnet's IPv4 address.



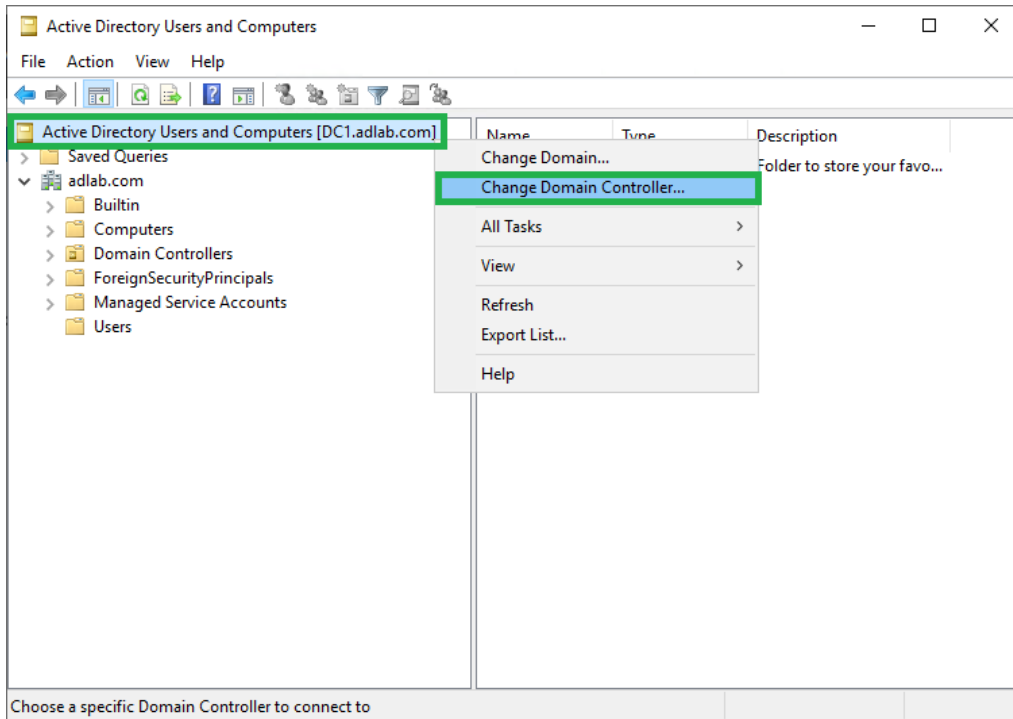
4. We go back to the **DC1 VM**, where we right click on **Subnets** and select **New Subnet...**



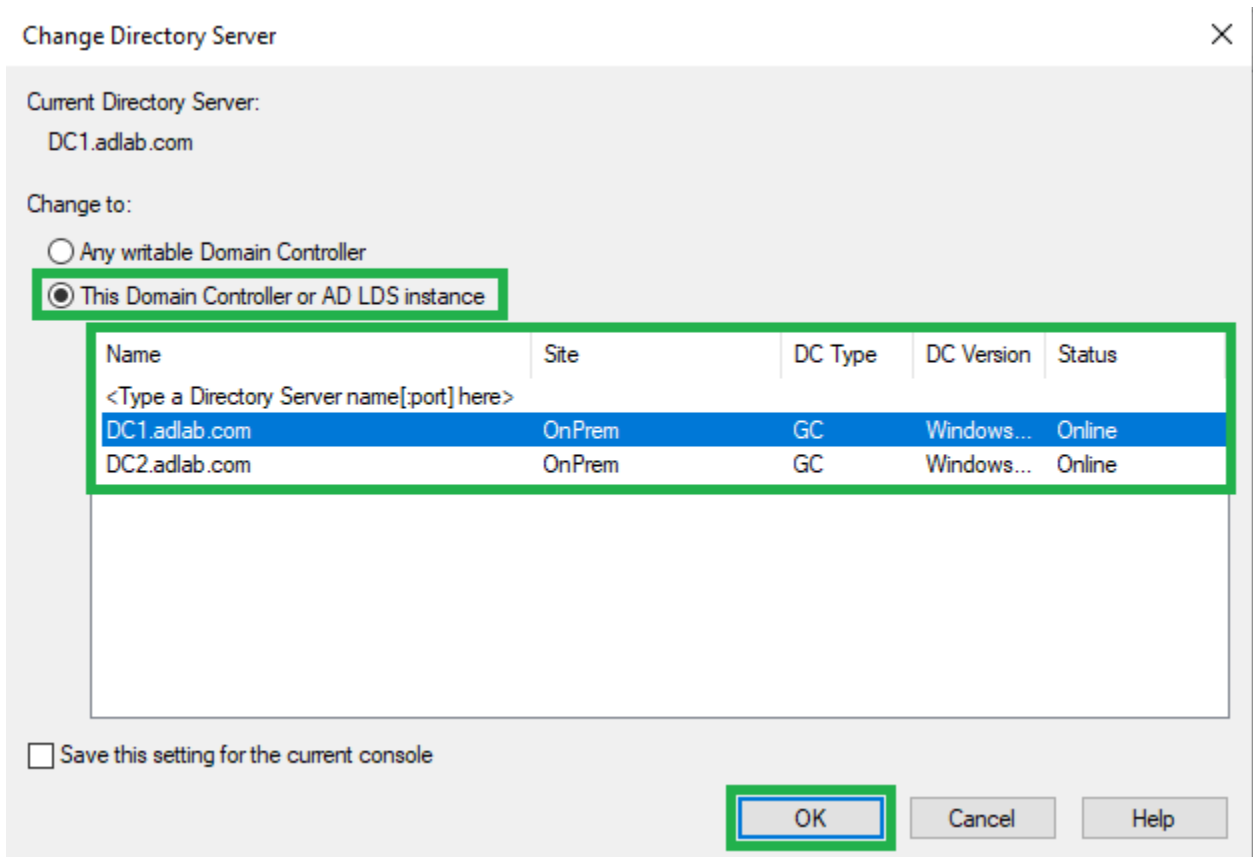
5. In the window that appears, we paste the subnet address that we copied from Azure virtual network page to the **Prefix** section, click on our site's name at the bottom, and confirm with **OK**.



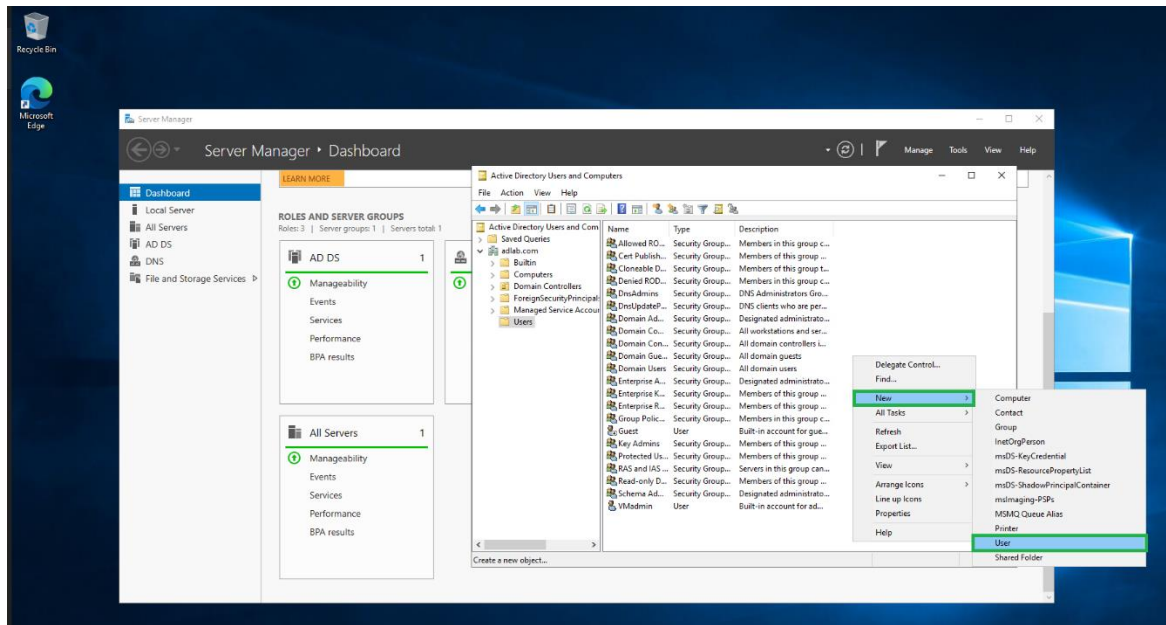
6. We then go to **Tools**, select **Active Directory Users and Computers**, right click on the first section and select **Change Domain Controller...**



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 login name** sections, and click on **Next**.

New Object - User

Create in: adlab.com/Users

First name:  Initials:

Last name:

Full name:


User login name:  @adlab.com

User login name (pre-Windows 2000):

< Back Next > Cancel

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

New Object - User ×

 Create in: adlab.com/Users

---

Password:

Confirm password:

☒ User must change password at next logon

☐ User cannot change password


☐ Password never expires

☐ Account is disabled

---

< Back Next > Cancel

New Object - User ×

 Create in: adlab.com/Users

---

When you click Finish, the following object will be created:

Full name: testuser0

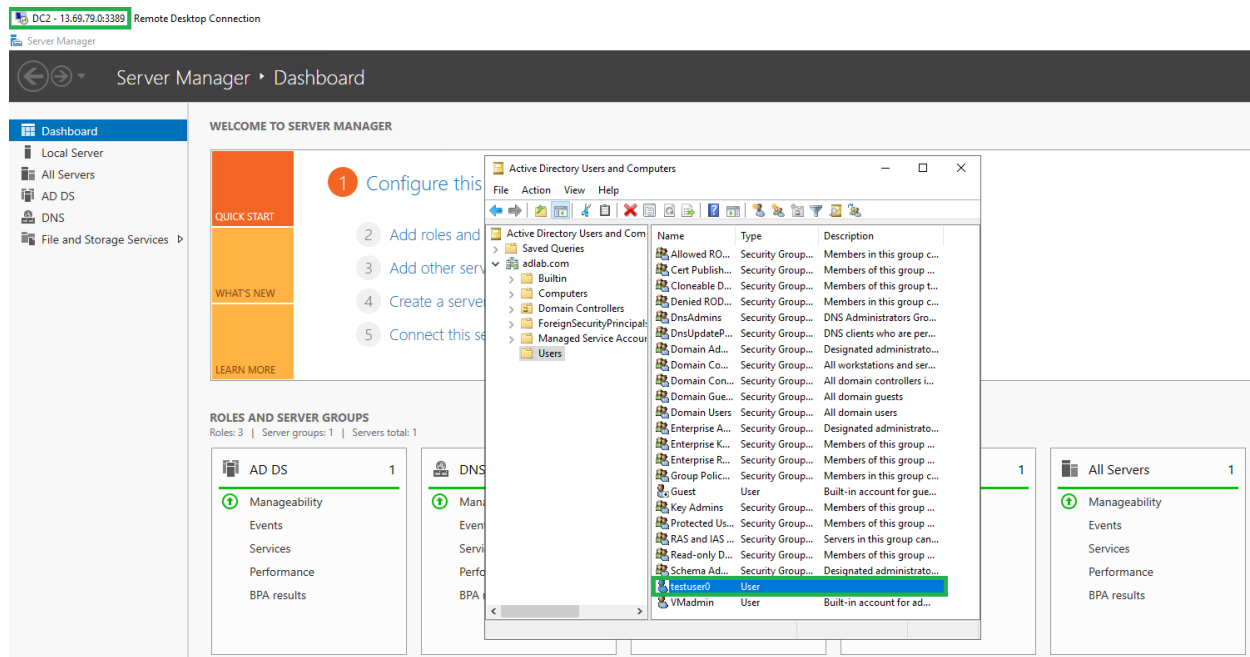
User logon name: testuser0@adlab.com

The user must change the password at next logon.

---

< Back Finish Cancel

11. To confirm user replication works properly, we now log back into **DC2**, go to **Tools** and select **Active Directory 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.).