😊 Azure AD Application Proxy

Azure AD Application Proxy is a feature of Azure Active Directory (AD) that enables users to access on-premises web applications securely from anywhere. It acts as a middleman between users outside your network and your on-premises applications, providing secure remote access without requiring VPNs or complex network configurations.

Here's how it works:

1. **Authentication:** When a user attempts to access an on-premises web application, they are first authenticated by Azure AD. This can involve single sign-on (SSO) if configured.
2. **Authorization:** Once authenticated, Azure AD determines if the user has the necessary permissions to access the application.
3. **Proxying:** If the user is authorized, Azure AD Application Proxy establishes a secure tunnel between the user's device and the on-premises application server, allowing the user to access the application securely.
4. **Traffic Management:** All traffic between the user and the on-premises application is routed through Azure AD, providing additional security and monitoring capabilities.

Azure AD Application Proxy offers several benefits:

1. **Secure Remote Access:** Users can securely access on-premises applications from anywhere, without the need for a VPN.
2. **Single Sign-On (SSO):** Users can access multiple applications with a single set of credentials, enhancing user experience and reducing the need for multiple logins.
3. **Conditional Access Policies:** Administrators can enforce access policies based on various factors such as user location, device compliance, and application sensitivity.
4. **Monitoring and Logging:** Azure AD provides comprehensive logging and monitoring capabilities, allowing administrators to track access attempts and identify potential security threats.

Overall, Azure AD Application Proxy simplifies remote access to on-premises applications while enhancing security and user experience.

😄 Use cases:

Azure AD Application Proxy can be used in various scenarios across different industries. Here are some common use cases:

1. **Remote Workforce Access:** With the rise of remote work, organizations need secure ways for employees to access on-premises applications from anywhere. Azure AD Application Proxy enables employees to securely access internal tools, such as HR portals, intranet sites, or financial systems, without the need for a VPN.

2. **Partner and Contractor Access:** Organizations often collaborate with external partners or contractors who require access to specific on-premises applications. Azure AD Application Proxy allows organizations to securely extend access to these external users without exposing internal networks or compromising security.
3. **Legacy Application Modernization:** Many organizations still rely on legacy on-premises applications that are not easily migrated to the cloud. Azure AD Application Proxy can help modernize access to these applications by providing a secure and scalable way for users to access them from any location, using modern authentication methods.
4. **BYOD (Bring Your Own Device) Scenarios:** In bring-your-own-device environments, ensuring secure access to on-premises applications can be challenging. Azure AD Application Proxy enables organizations to provide secure access to internal resources while maintaining control over which devices are allowed to connect.
5. **Secure Customer Access:** Some organizations may need to provide customers or clients with access to certain on-premises applications, such as self-service portals or customer support tools. Azure AD Application Proxy allows organizations to securely extend access to these applications to external users, while maintaining control over authentication and authorization.
6. **Compliance and Regulatory Requirements:** Industries such as healthcare, finance, and government have strict compliance and regulatory requirements for data access and security. Azure AD Application Proxy helps organizations meet these requirements by providing secure access controls, audit logs, and compliance reporting for on-premises applications.
7. **High Availability and Disaster Recovery:** Azure AD Application Proxy offers built-in high availability and disaster recovery capabilities, ensuring continuous access to on-premises applications even in the event of an outage or disaster.

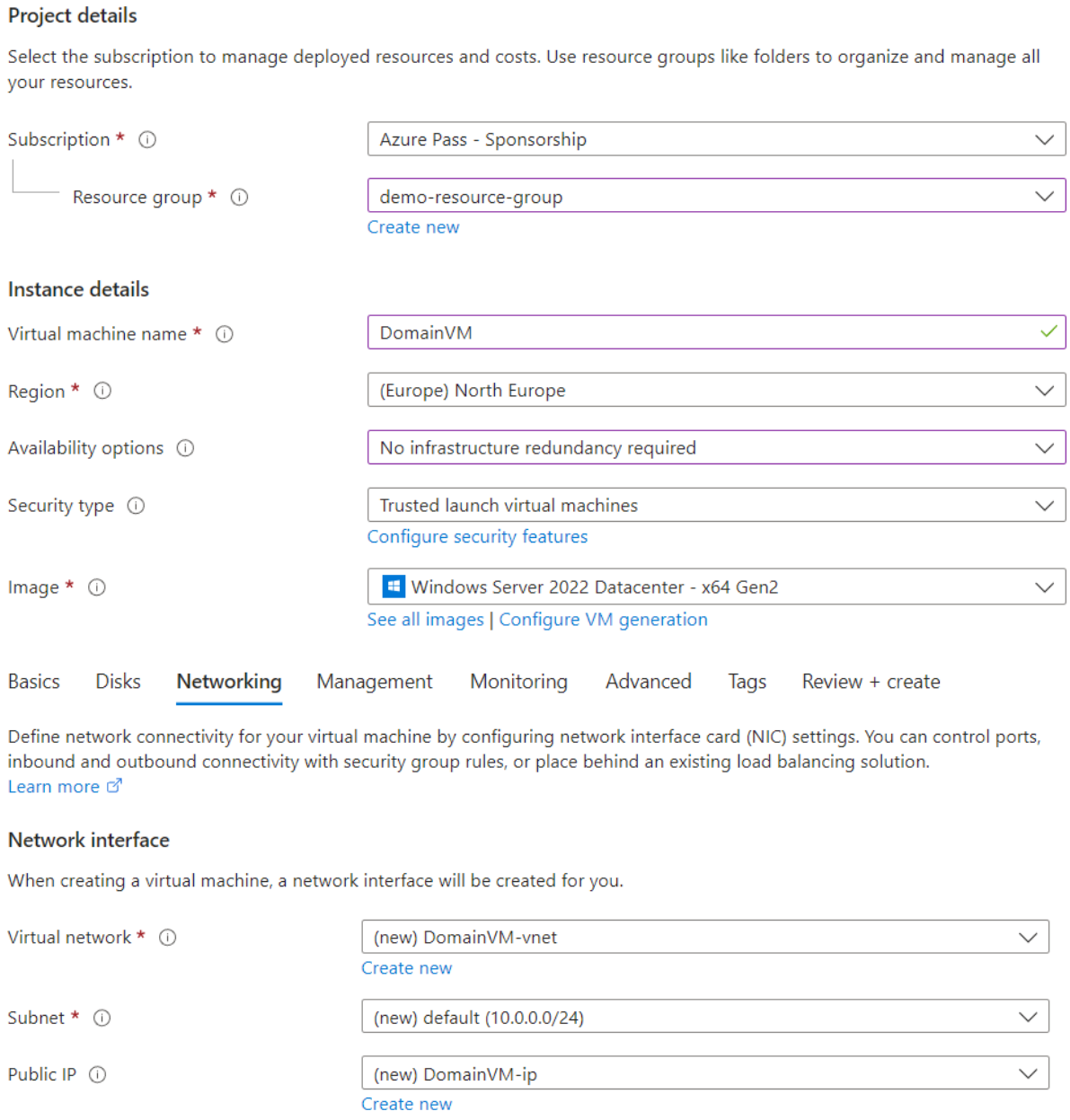
In this lab, we are setting up a virtual environment using Azure resources to demonstrate the configuration and usage of Azure AD Application Proxy. The end goal is to showcase how Azure AD Application Proxy enables secure remote access to on-premises web applications for users outside the corporate network, facilitating scenarios like remote workforce access, partner access, and secure customer access. We'll configure a domain server, set up additional virtual machines, install and configure IIS, and ultimately demonstrate secure access to the web application through Azure AD Application Proxy.

😄 To begin with the Lab:

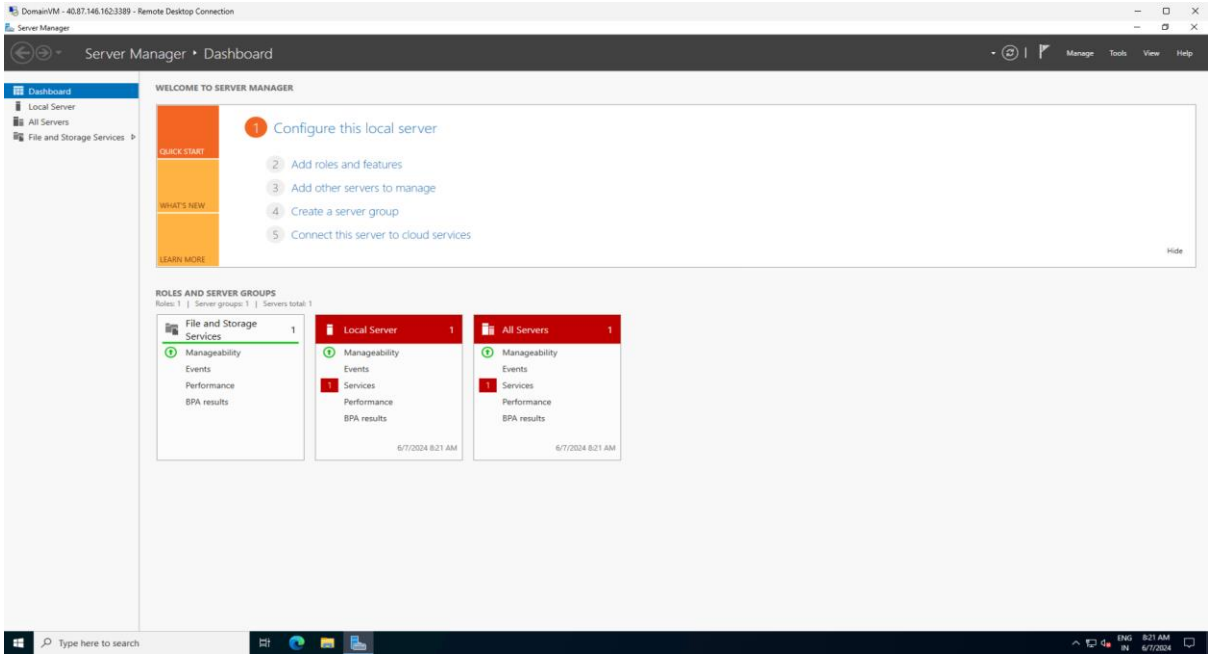
😁 Building the domain server

1. Here in this lab, we are going to create a setup in which we will create three Virtual Machines.

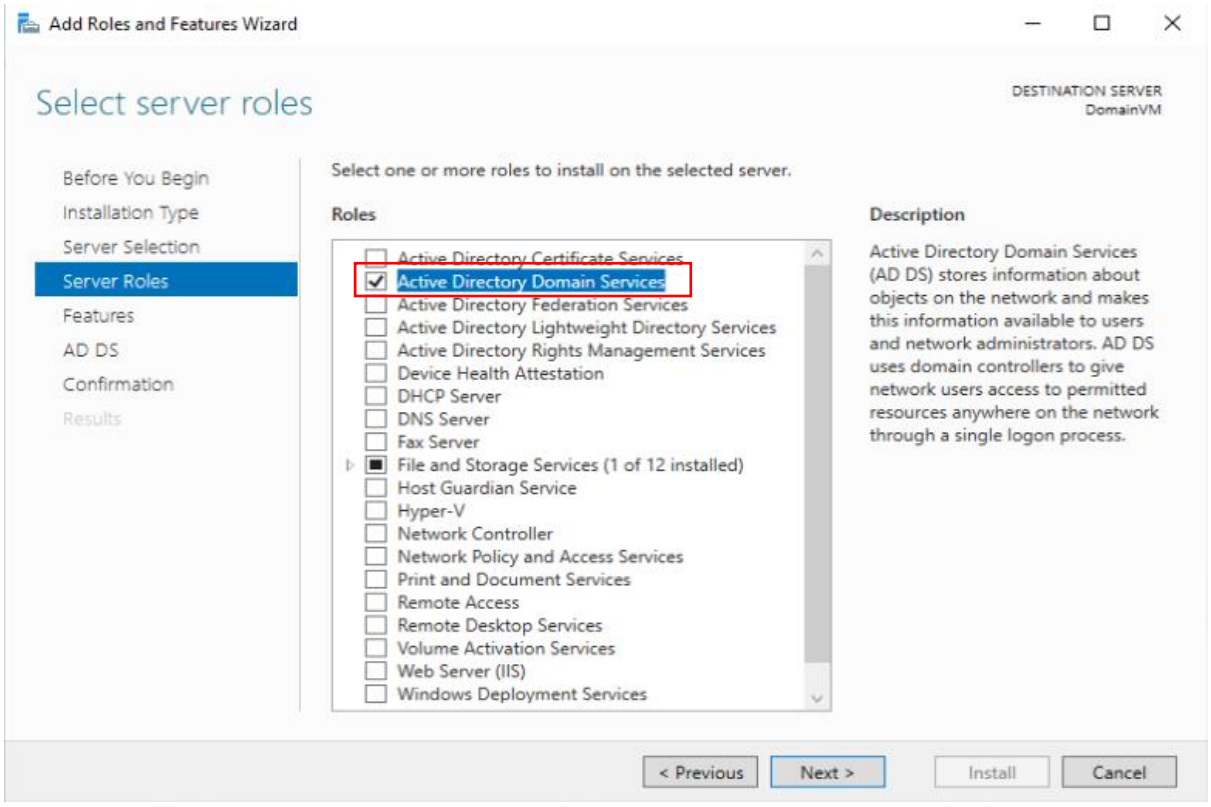
2. Now in your Azure Portal, go to Virtual Machines and create a VM based on Windows Server 2022.
3. You can follow the snapshot below to make sure you have a public IP address for your VM.
4. Afterwards go ahead and create your VM. Once your VM is deployed, download the RDP file and you need to login to your VM.



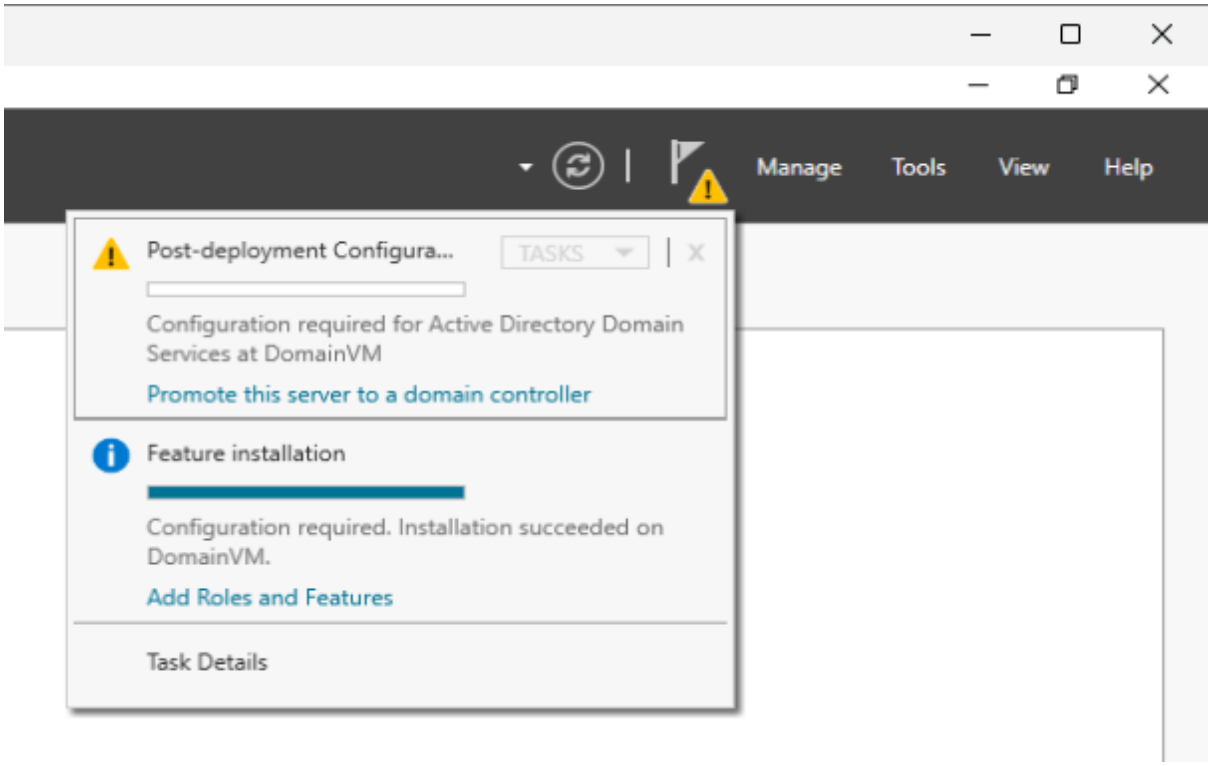
5. Once you are in the Server Manager of the VM you need to click on add roles and features and then install Azure Active Directory on your VM.



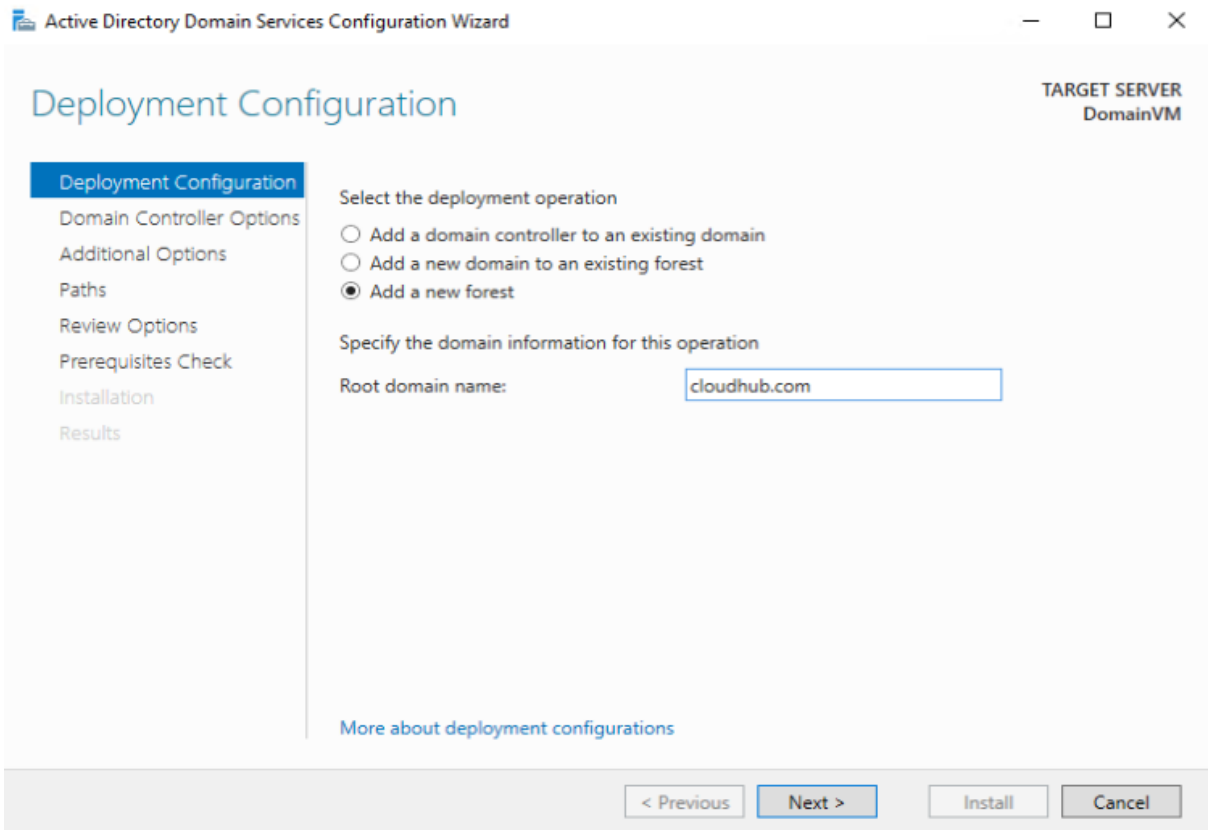
6. Now you need to install Active Directory Domain Services on your VM as you can see below.



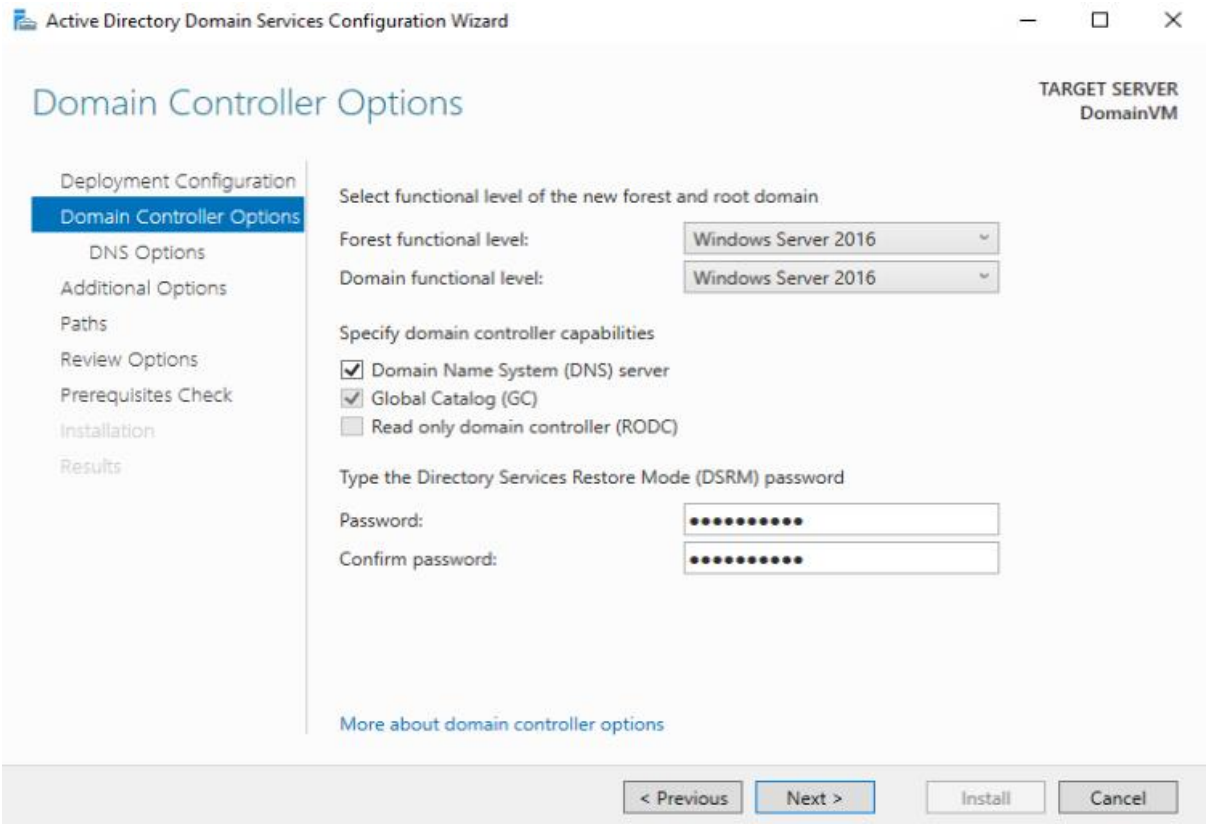
7. After that you will see that we got a notification to promote the server to become a domain controller.



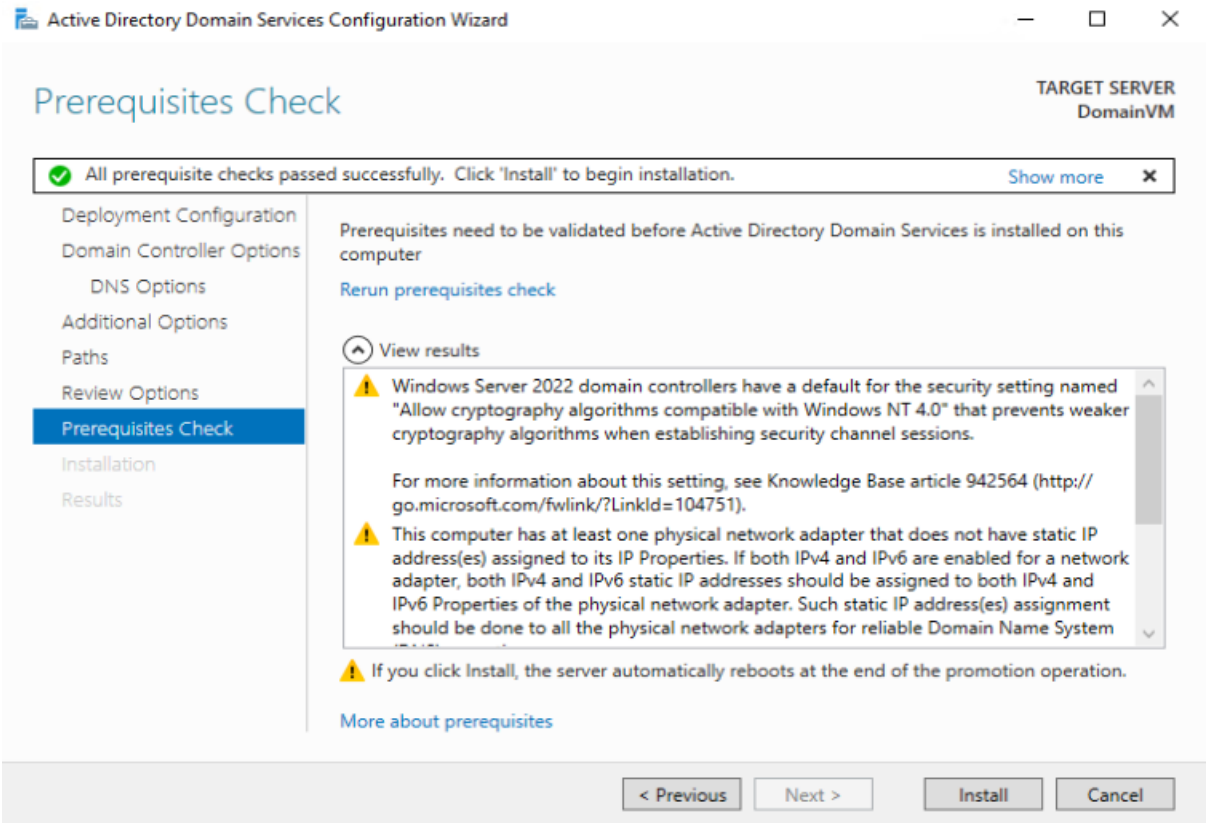
8. Now we need to choose to add a new forest and then give a domain name, you can give any random name, then click on next.



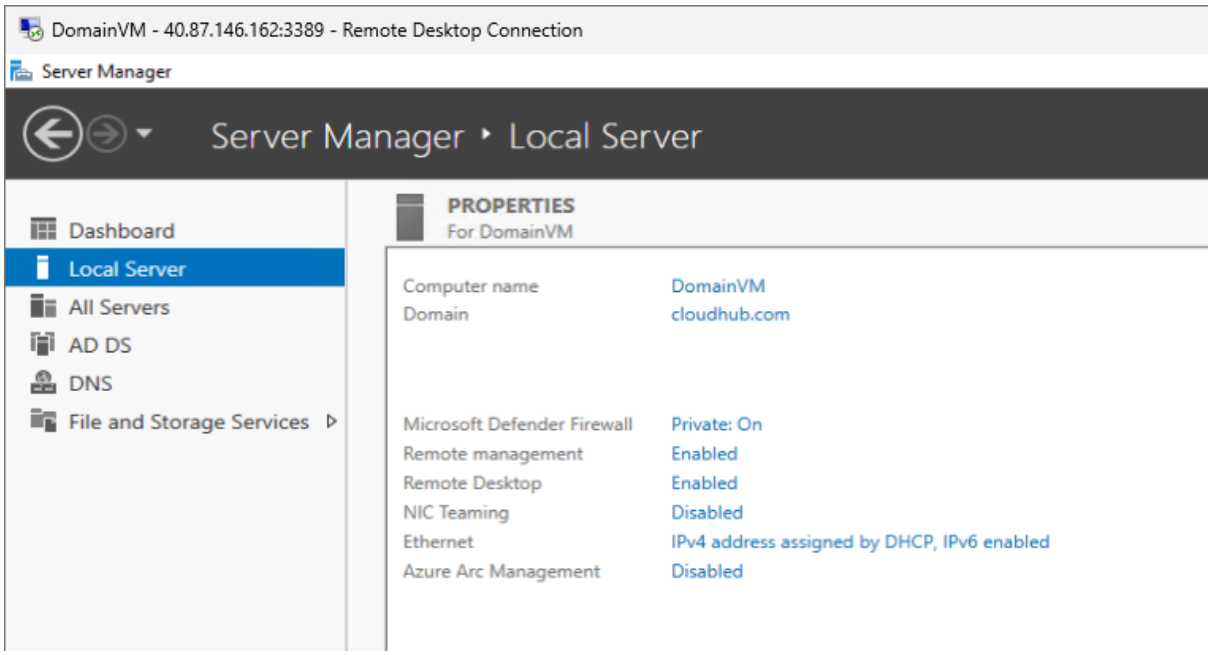
9. Now you need to provide a password for directory services restore mode.



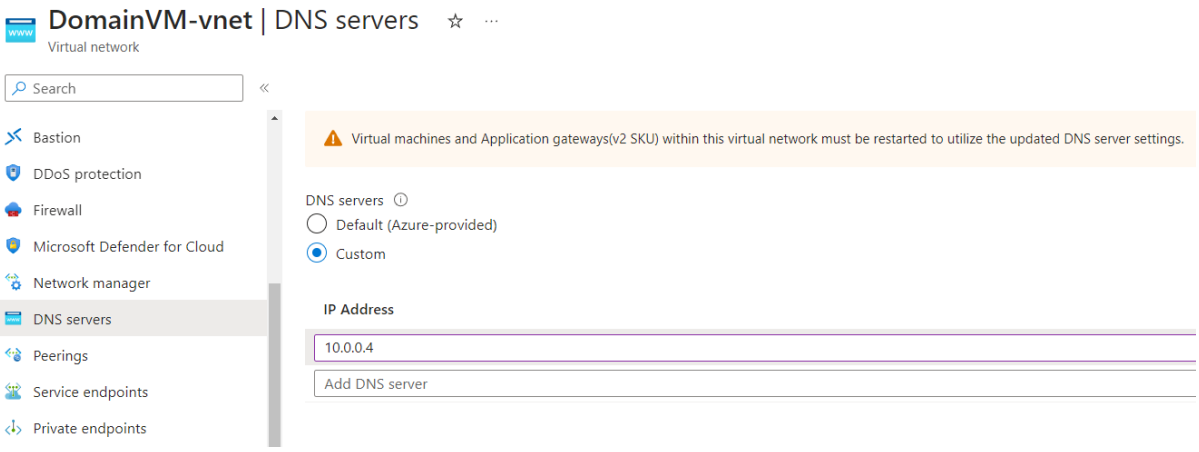
10. Now you need to click on next until you reach the installation part and just install it. Once the installation is complete, it will restart the server and you will lose connectivity.



11. After that, once the installation is complete, you need to log in to your VM again and if you go to the local server, you will see that it is a part of the domain cloudhub.com



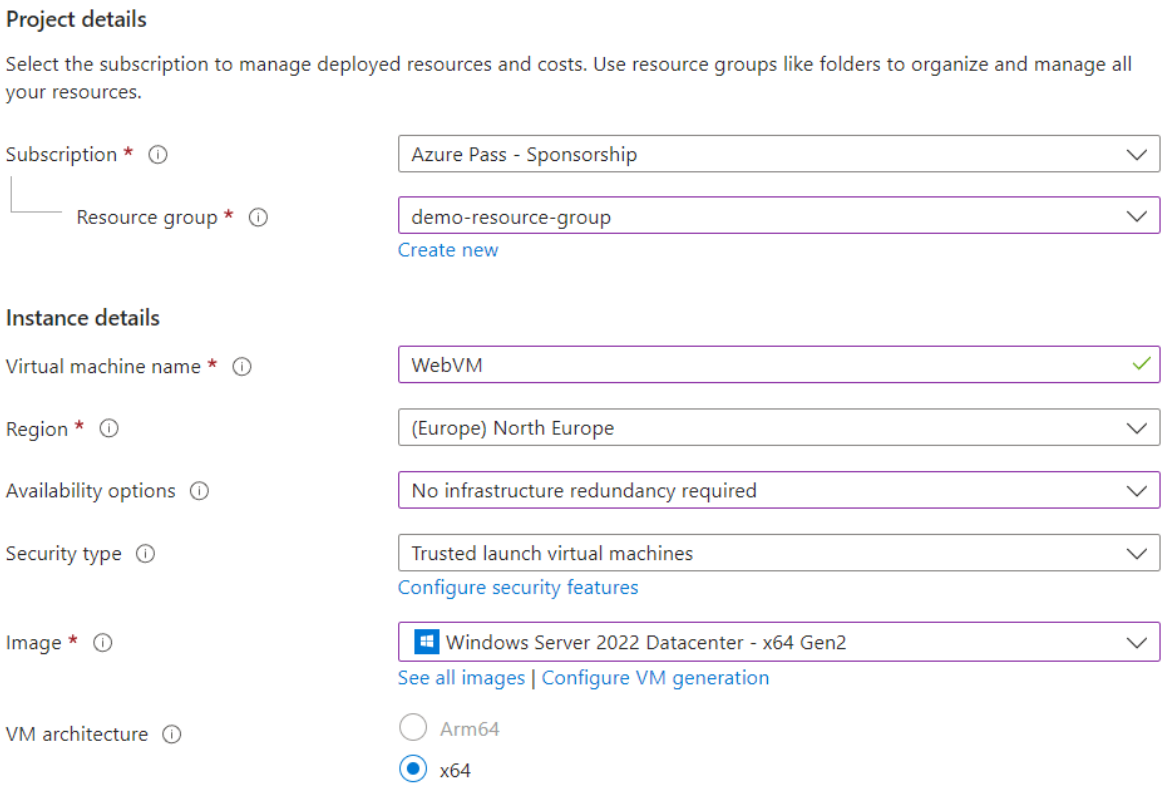
12. Now we are going to create another two Virtual Machines but we want all of them to be a part of this Domain.
13. So, for that we need to change the DNS settings of our Virtual Network. Now from your VM open Virtual Network.
14. Now from the left pane choose DNS servers and then choose Custom and give the Private IP address of your VM (domain VM).



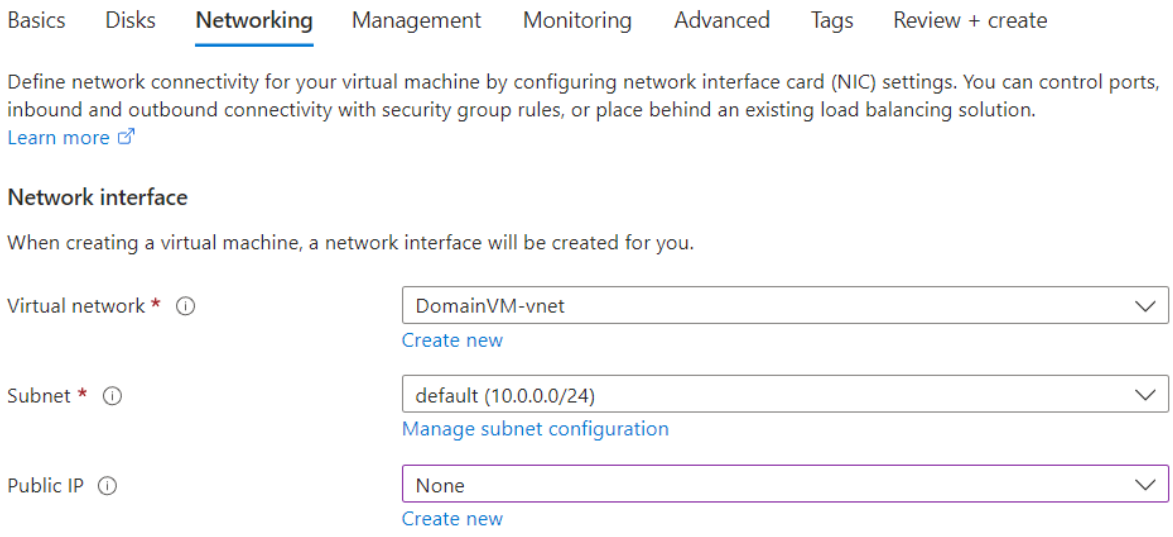
15. After that you need to restart your Virtual Machine.

😄 Setting up Another Virtual Machine

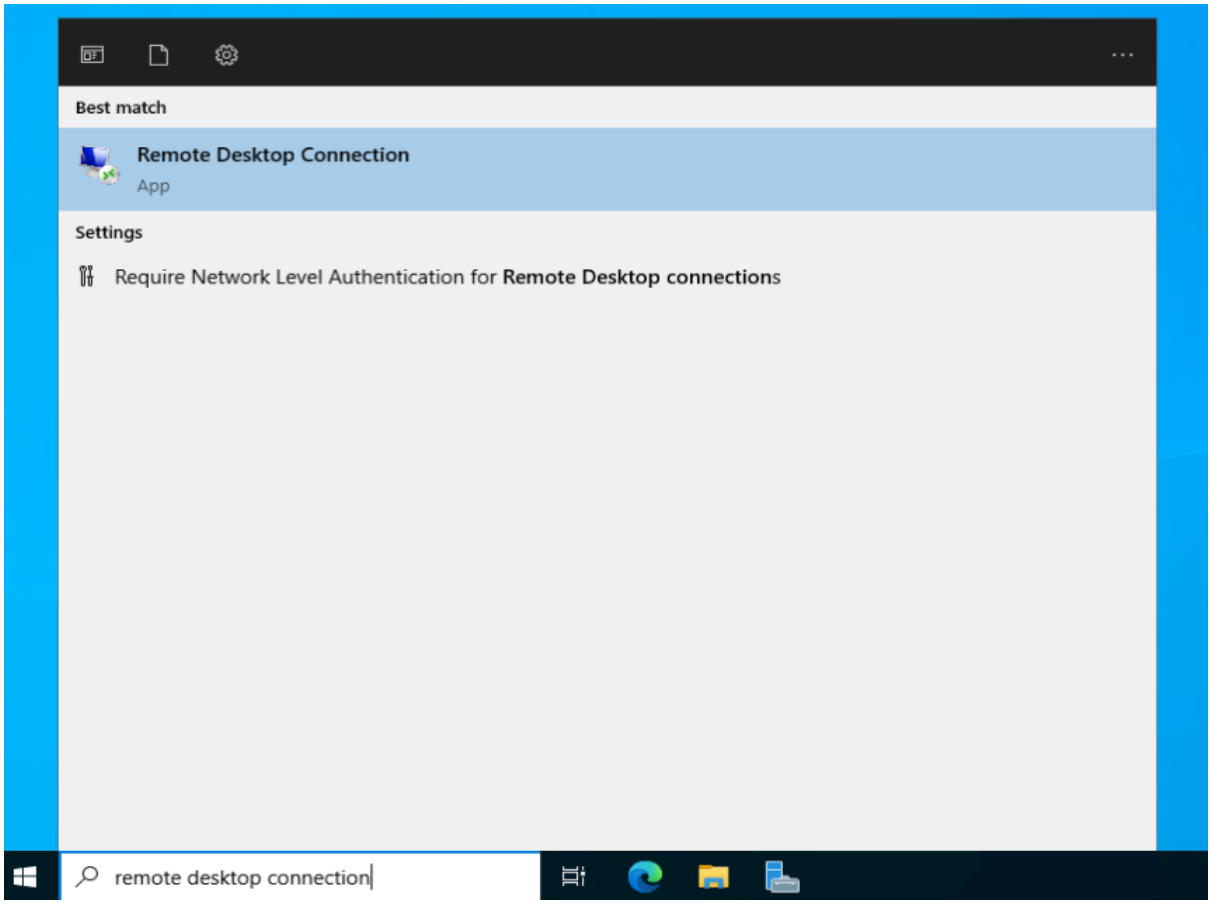
1. Now we are going to spin up another Virtual Machine.



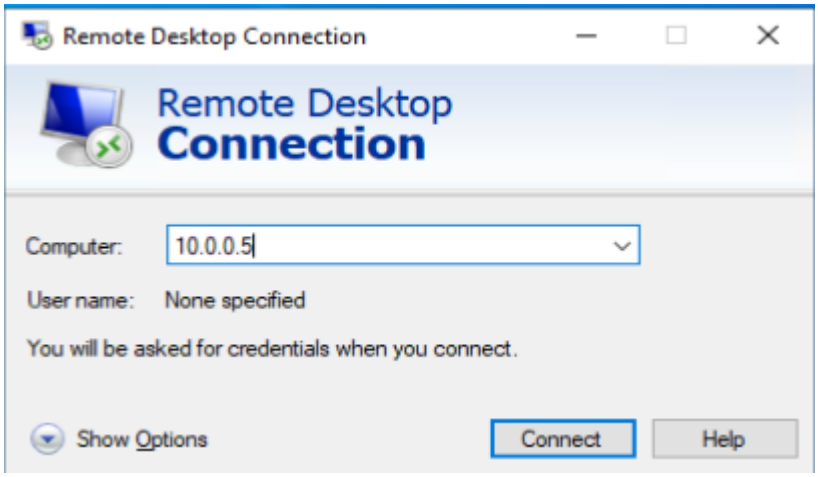
2. In the networking you need to choose none for a public IP address because we don't want to have a public IP address for this machine. After that just go ahead and create your virtual machine.



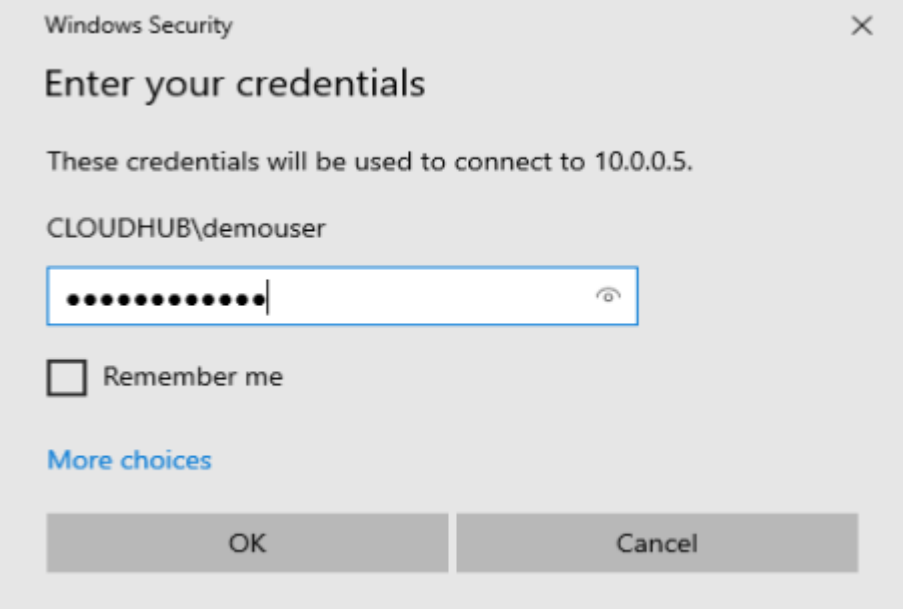
3. Now we are going to install IIS on this VM but to do that we need to login to this machine, but we don't have any public IP address.
4. So, first we will login with our Domain VM, also copy the private IP address of your Web VM.
5. Now in our domain VM we will open a remote desktop connection and open it.



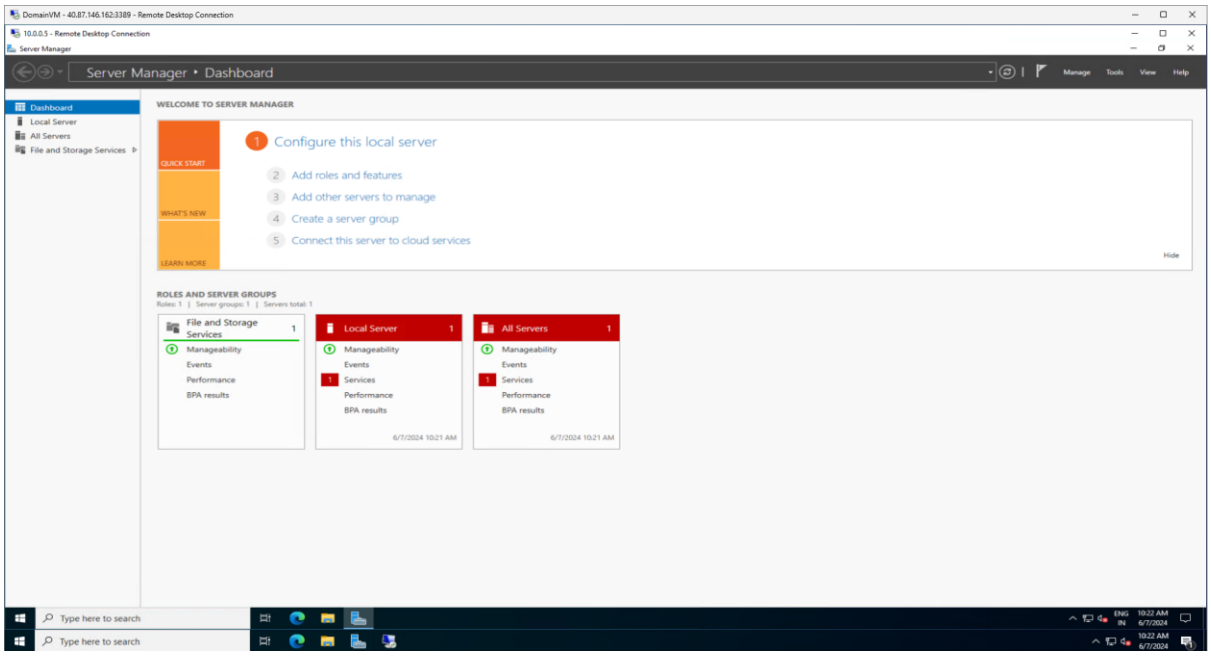
6. Then we will enter the private IP address of our web VM and click on connect.



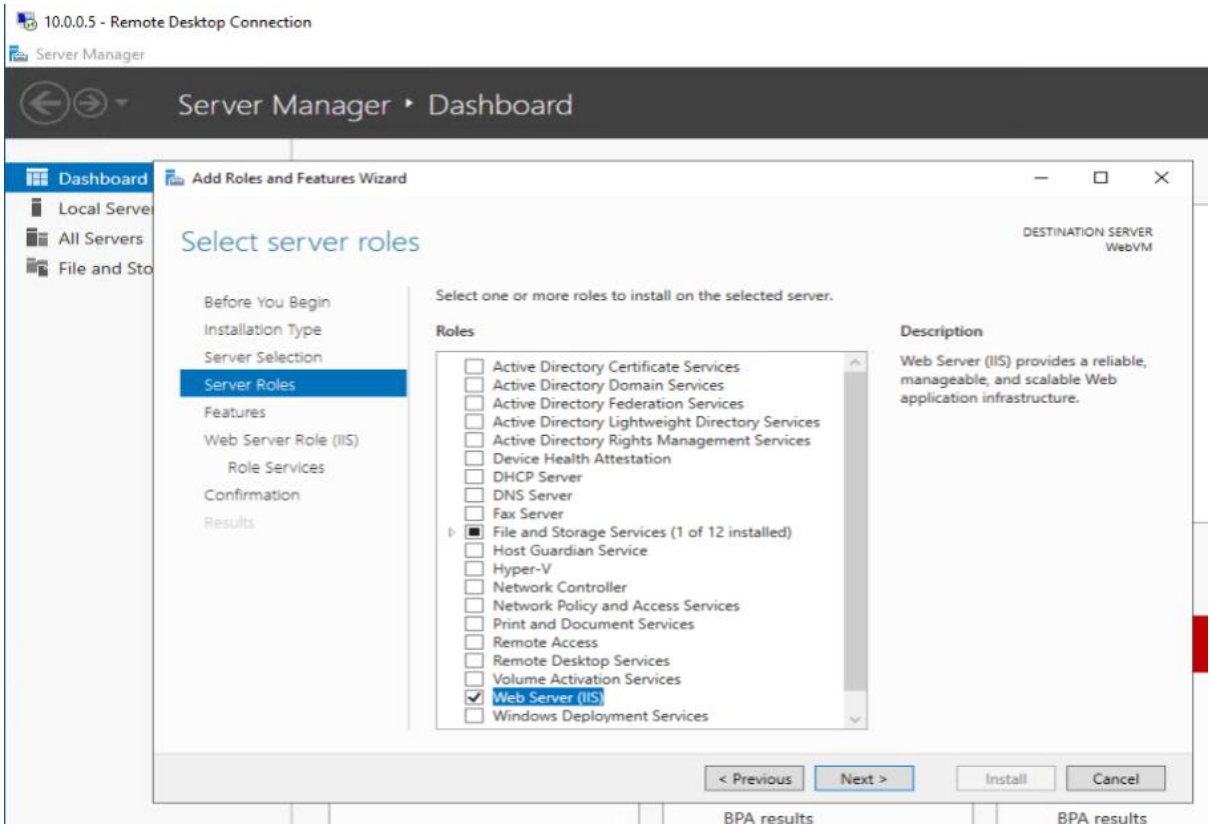
7. After that it will ask you for the password, enter that and click on OK. Then you will see that you are connected to your web VM using its private IP address.



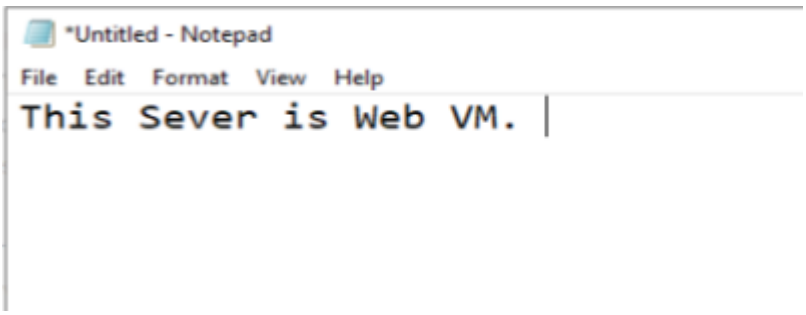
8. Below you can see that you have a VM inside of a VM.
9. Now you need to install IIS on the web VM for that click on add roles and features.

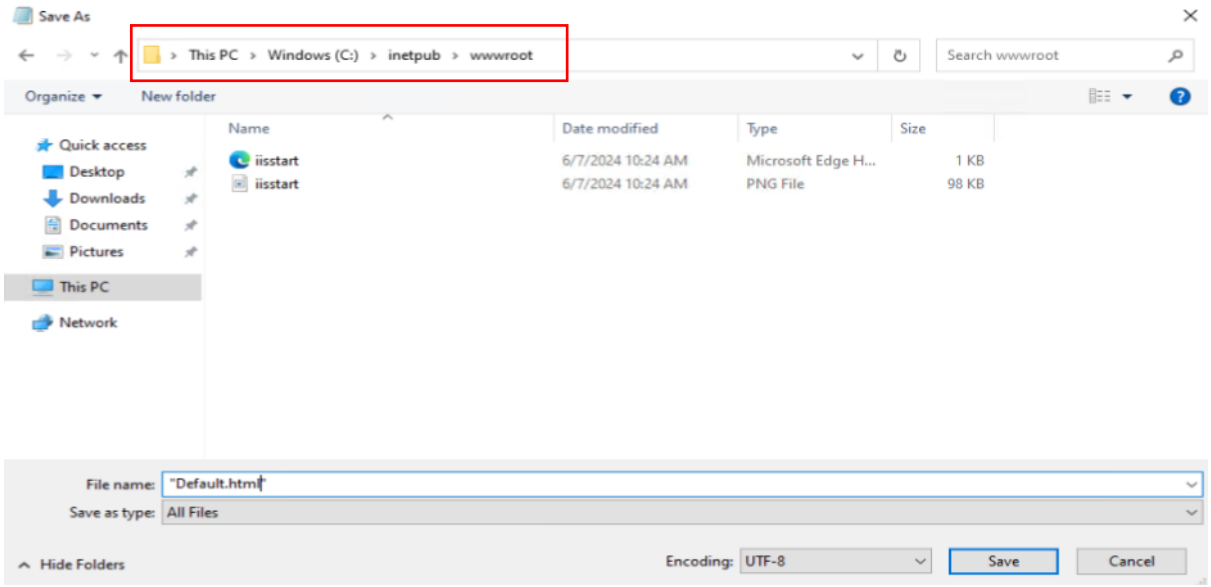


10. Choose the web server to install and then install it. After that wait for the installation to complete and open the notepad.

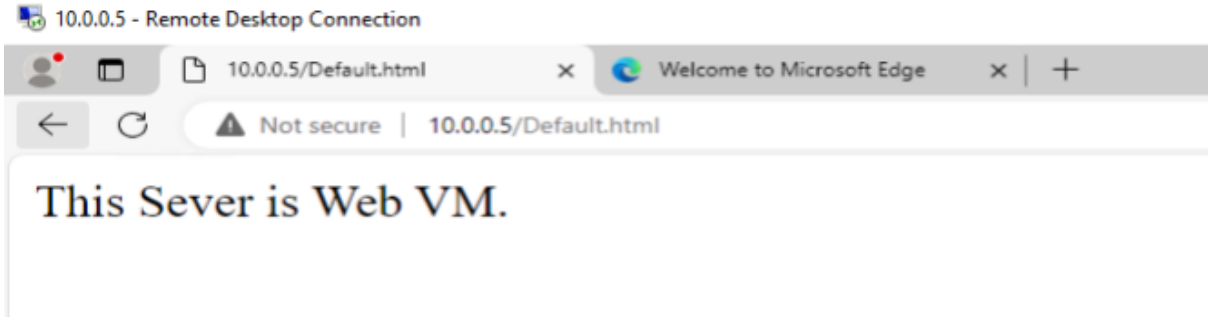


11. Once the installation is complete, write something in Notepad and save it at the exact same location as shown below.

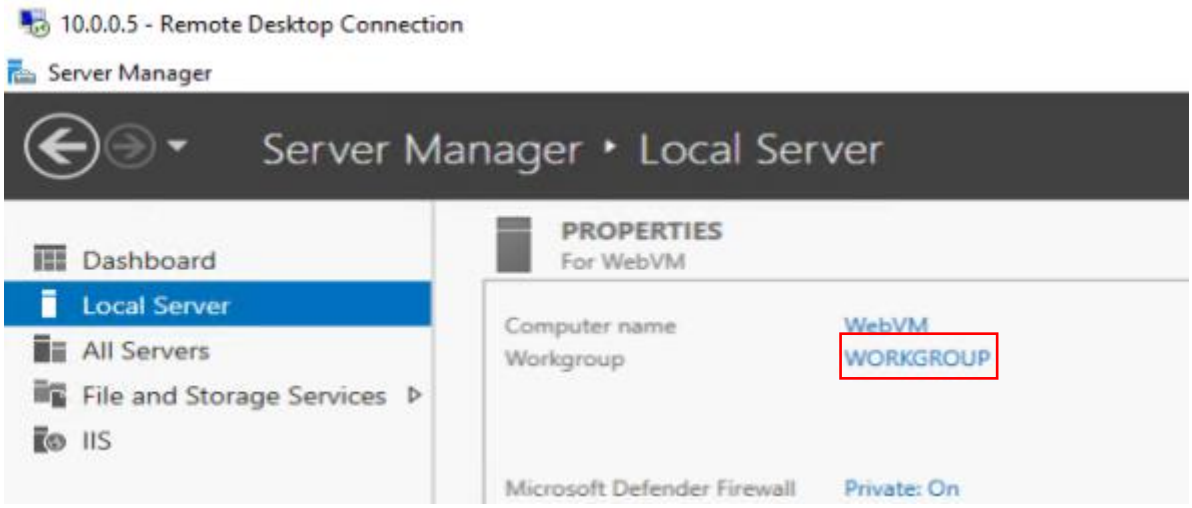




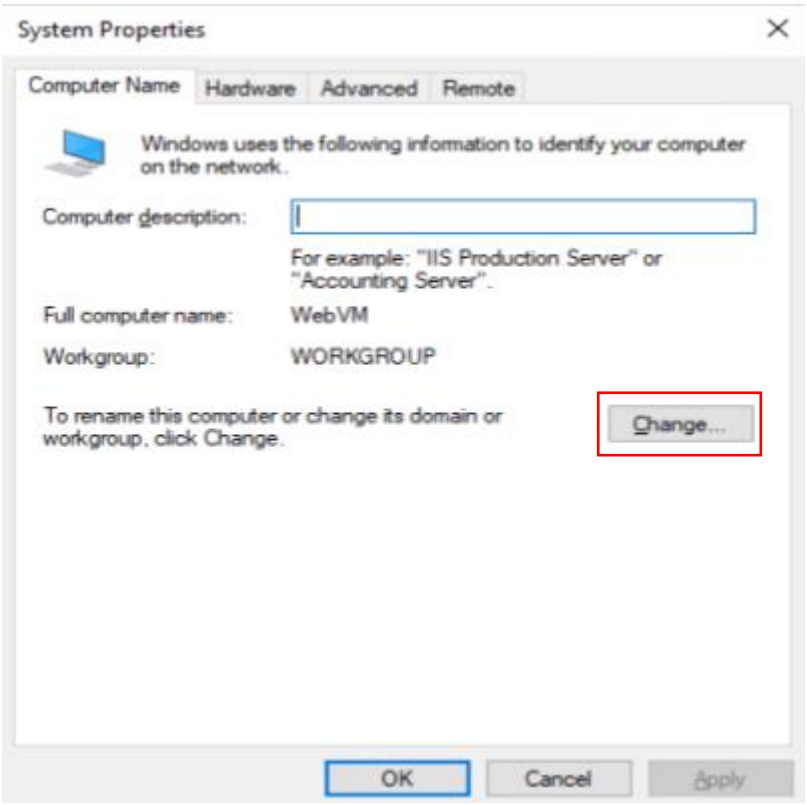
12. After that, open the Edge Browser, in your web VM and write the Private IP address of the VM and append it with default.html as shown below then you can see the webpage.



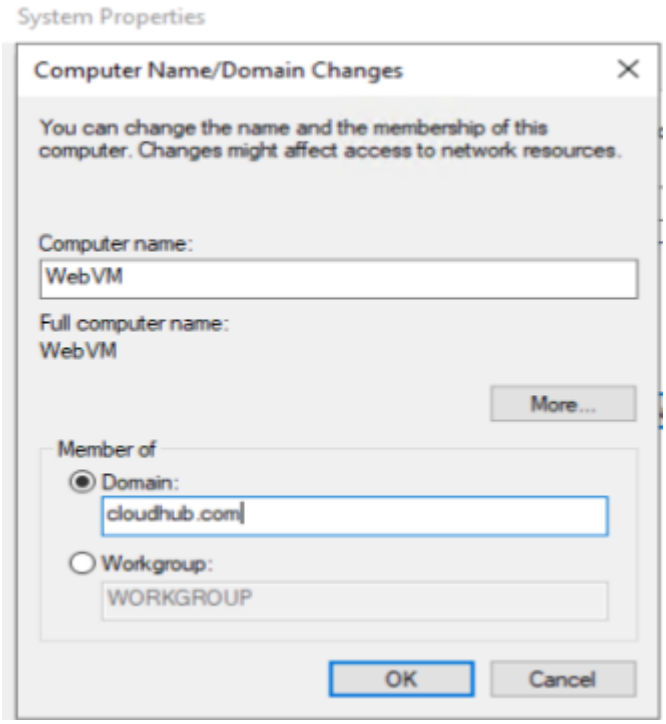
13. Now we will make this web VM part of our domain. For that in server manager go to the local server and here you can see that your web VM is a part of work group. Click on this work group.



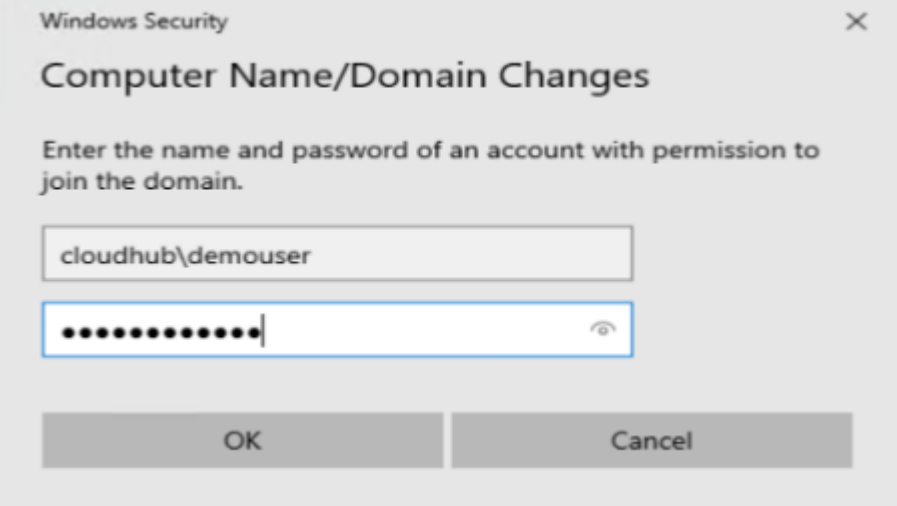
14. Then you need to click on change.



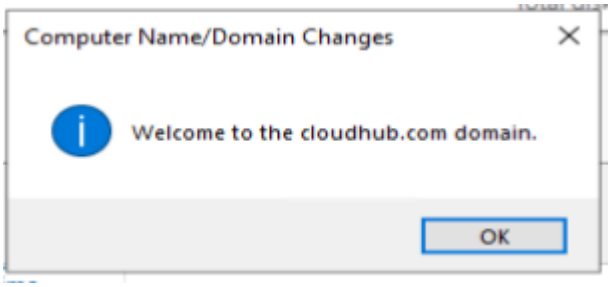
15. And we will choose a domain then we need to give the name of our internal domain which is cloudhub.com and click on Ok.



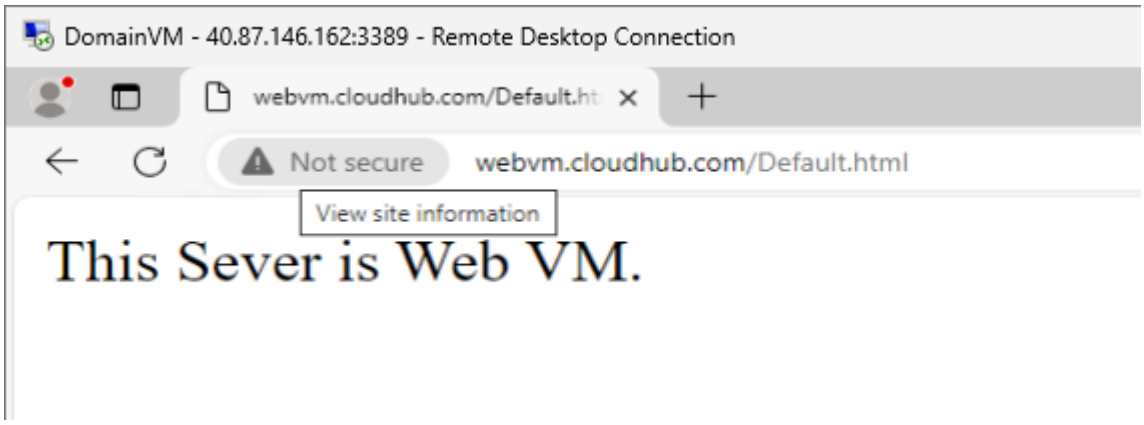
16. Then you need to enter the credentials of your Domain VM. The username and password which you use while logging into the VM, also need to give the domain name as shown below. Then just click OK.



17. If you successfully logged in then you will get this message and then it will ask you to restart your VM. Do that.

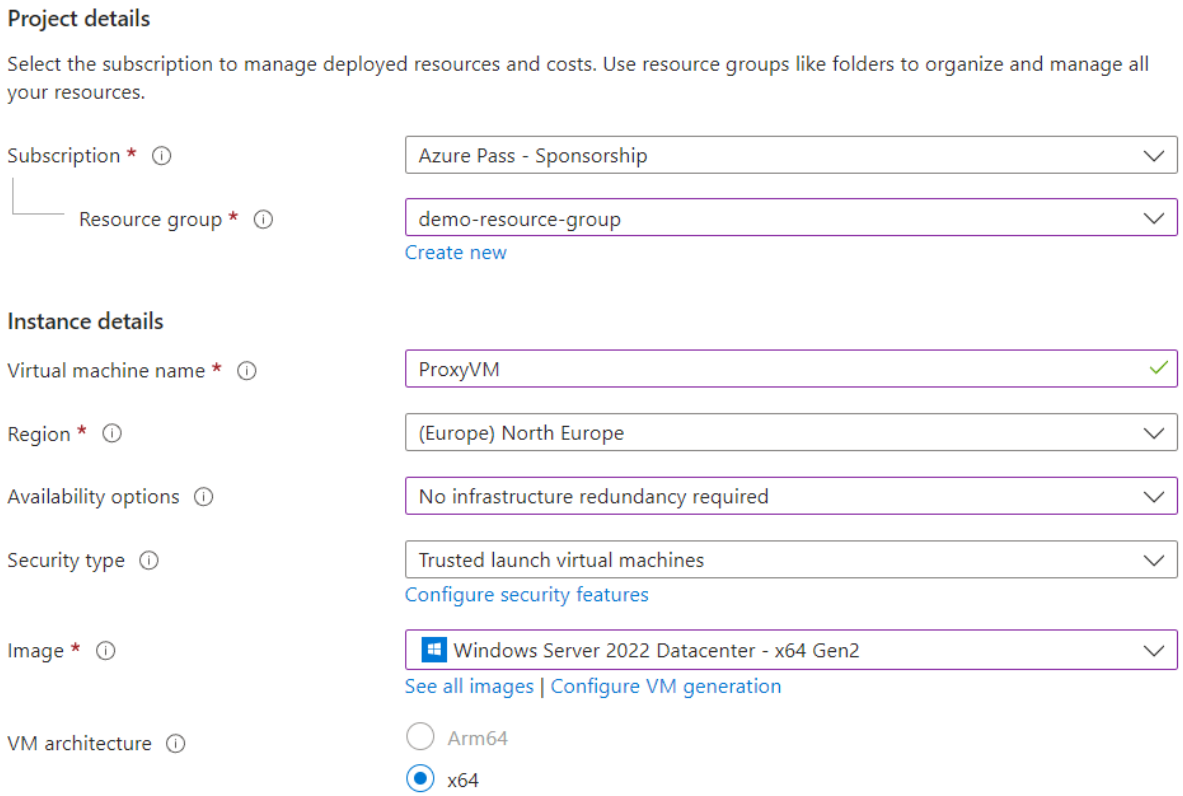


18. Now in your domain VM open the Edge browser and as our web VM is a part of our domain now, so, we will use the domain name along with the web VM name as you can see in the snapshot and we will get the web page as expected.

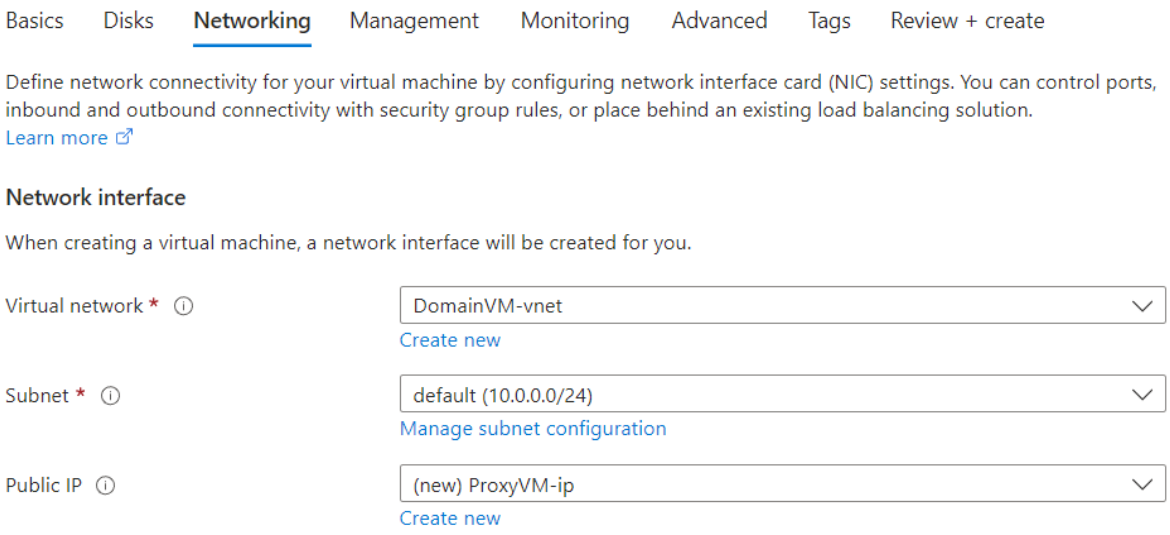


😄 Setting up the Proxy Virtual Machine

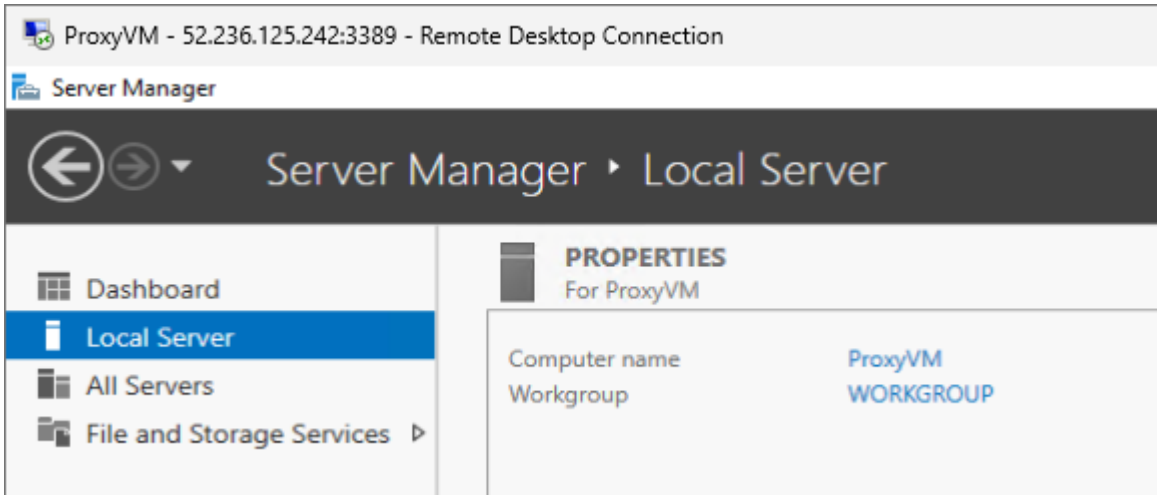
1. Now create a VM like you did before.



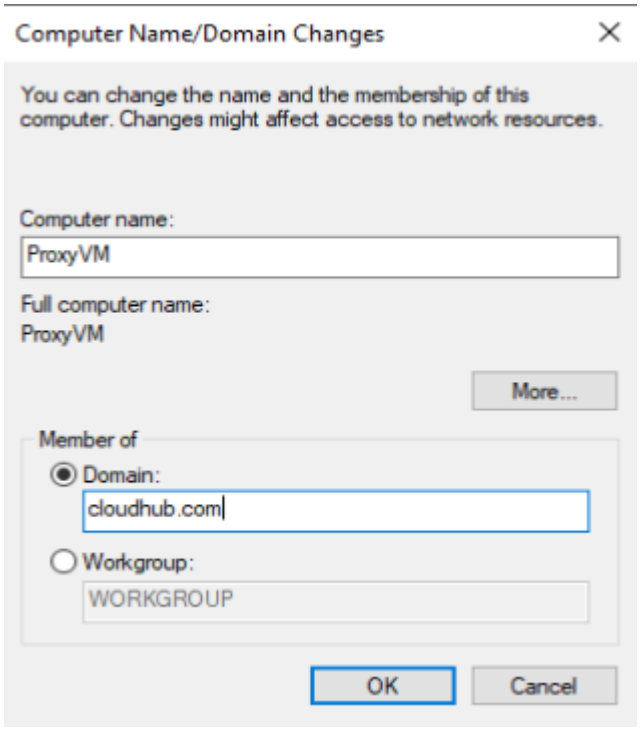
2. Just make sure that our Proxy VM should have a public IP address and it should be in the same Virtual network as the last two were. After that go ahead and create your VM.



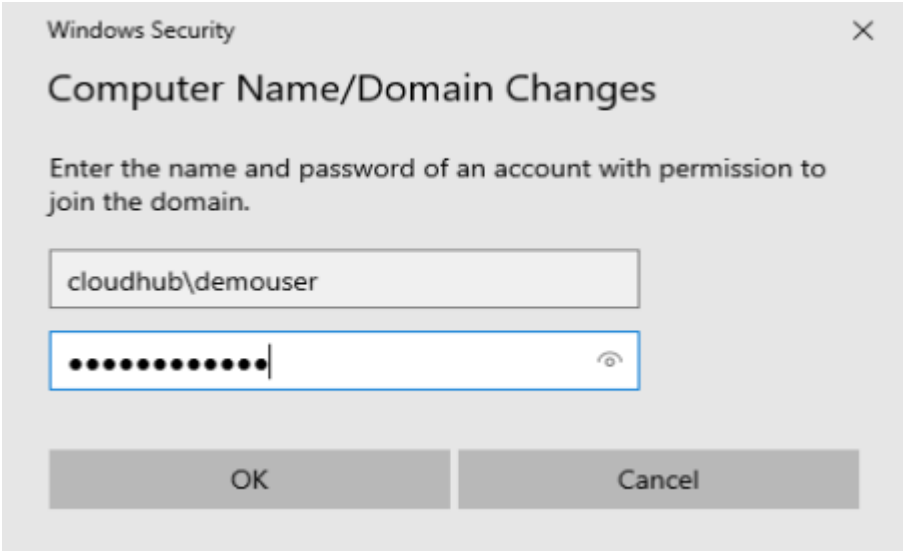
3. Once your machine is deployed, you need to download the RDP file and login to your VM. Then we will make this VM a part of our Domain.
4. Again, you need to follow the same steps as before, in server manager go to local server. You can see it is a part of some workgroup click on it.



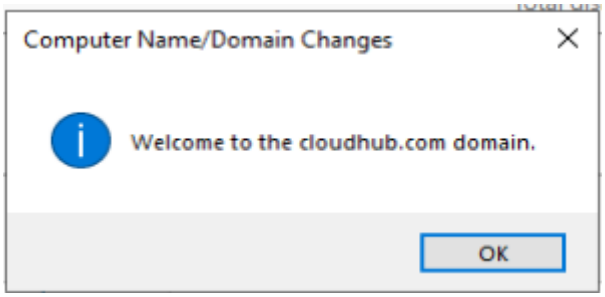
5. Now you need choose domain and write our domain name and click on Ok.



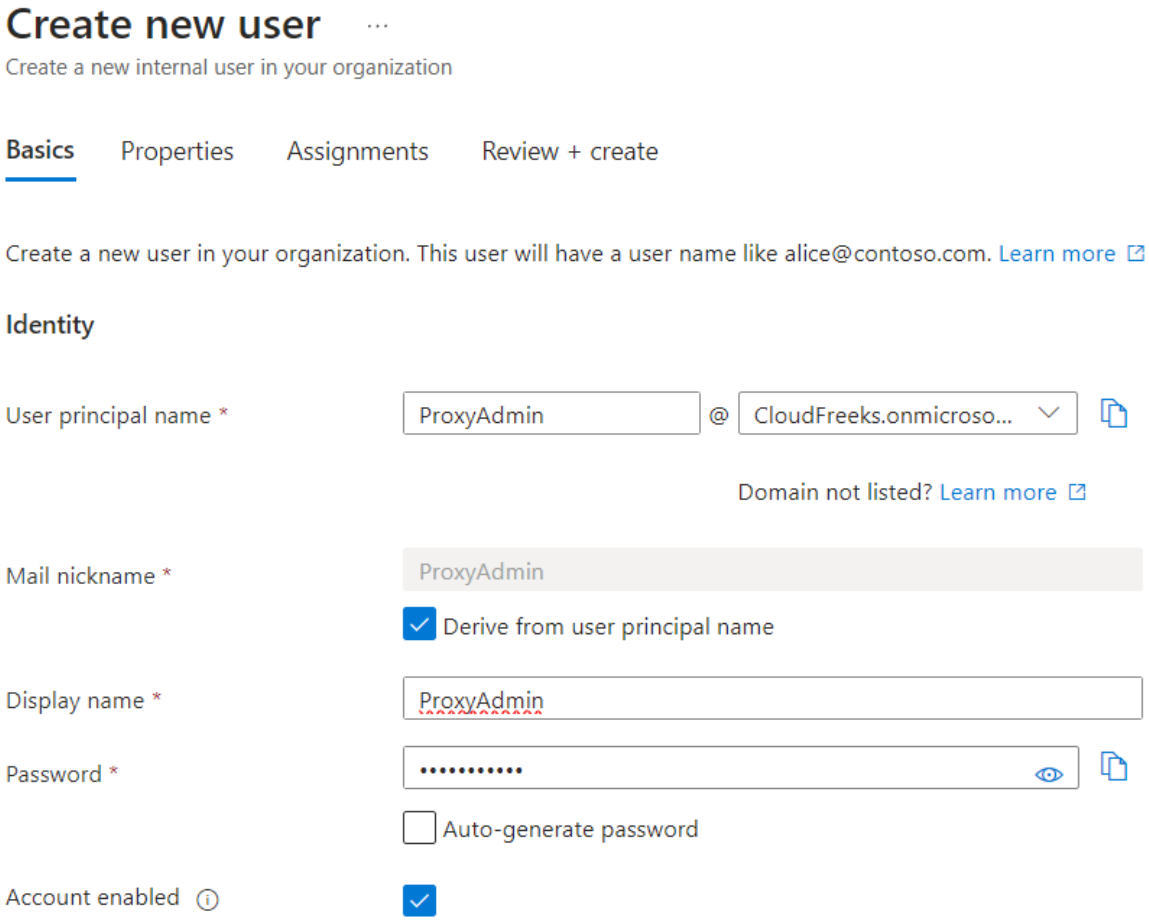
6. Then give the username and password of the domain VM as we did before.



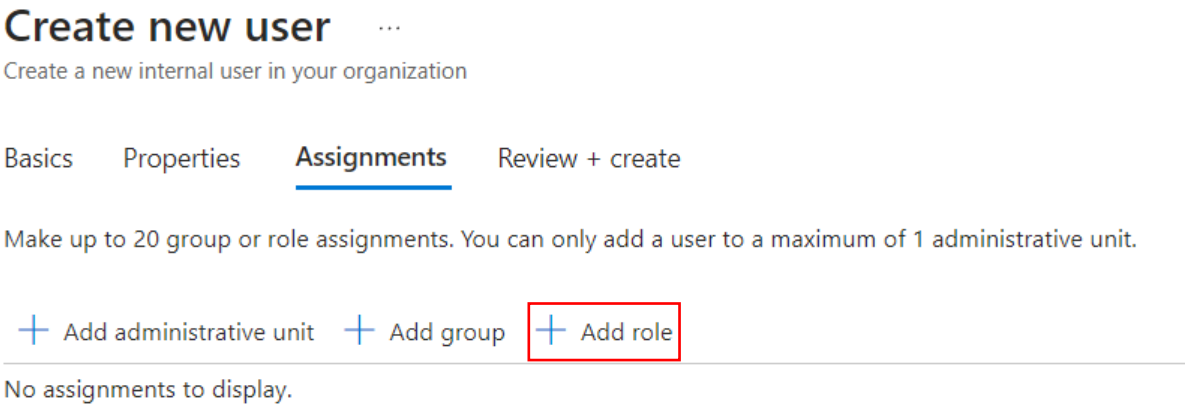
7. Once you have logged in successfully then you will see the welcome message then just restart your VM.

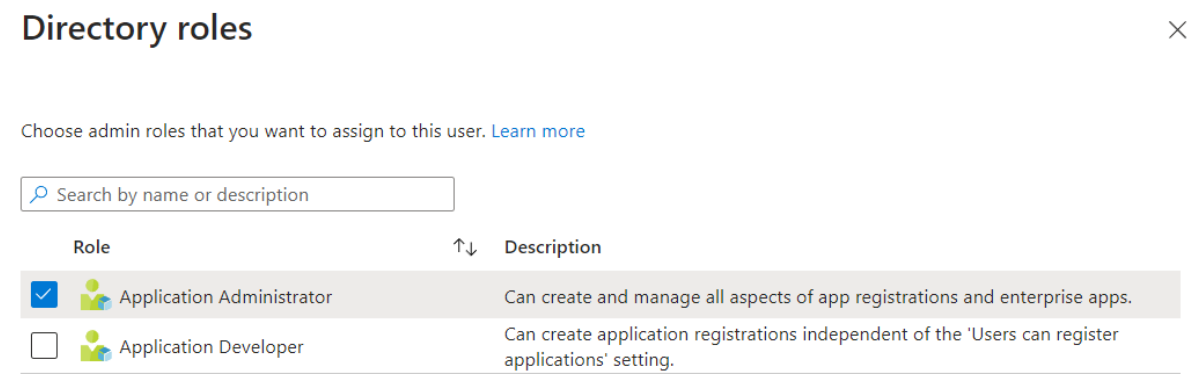


8. Now we need to go to Microsoft Entra ID because in order to configure Application Proxy we need to have a user in place. So, we will create a new user.
9. Now you need to name it and give your own password or use auto-generated password.



10. Then in the assignment we are going to add a role. We will choose the Application Administrator.
11. Then move to review page and create your user.



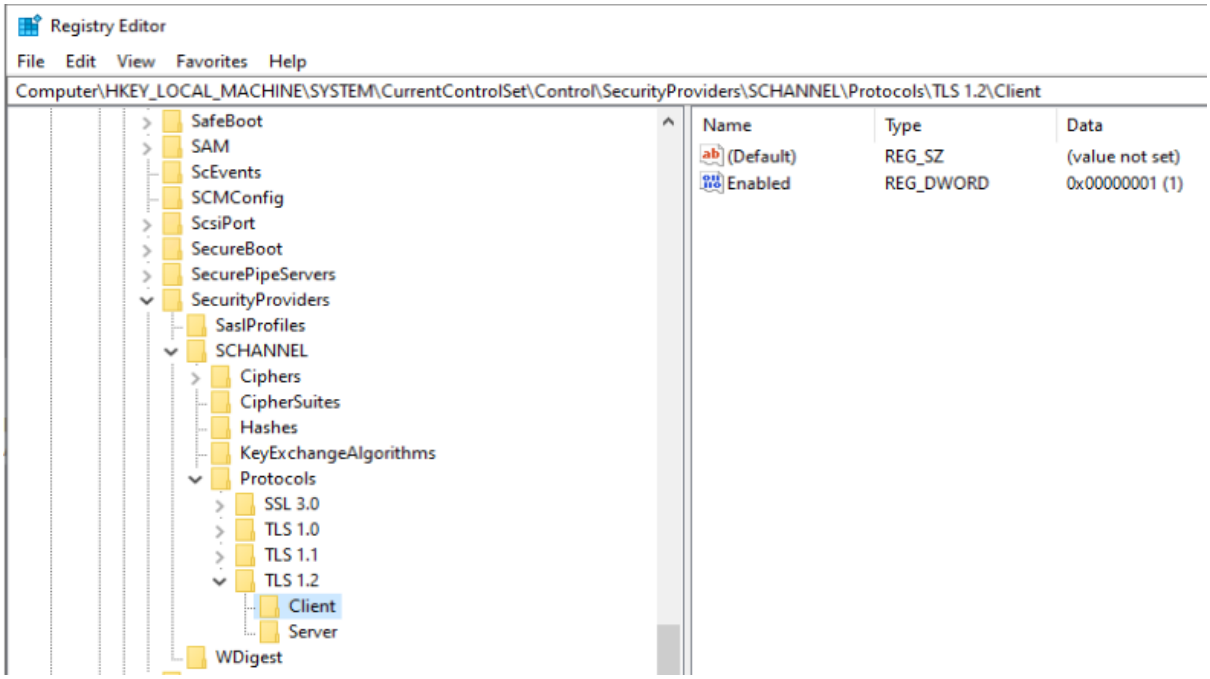


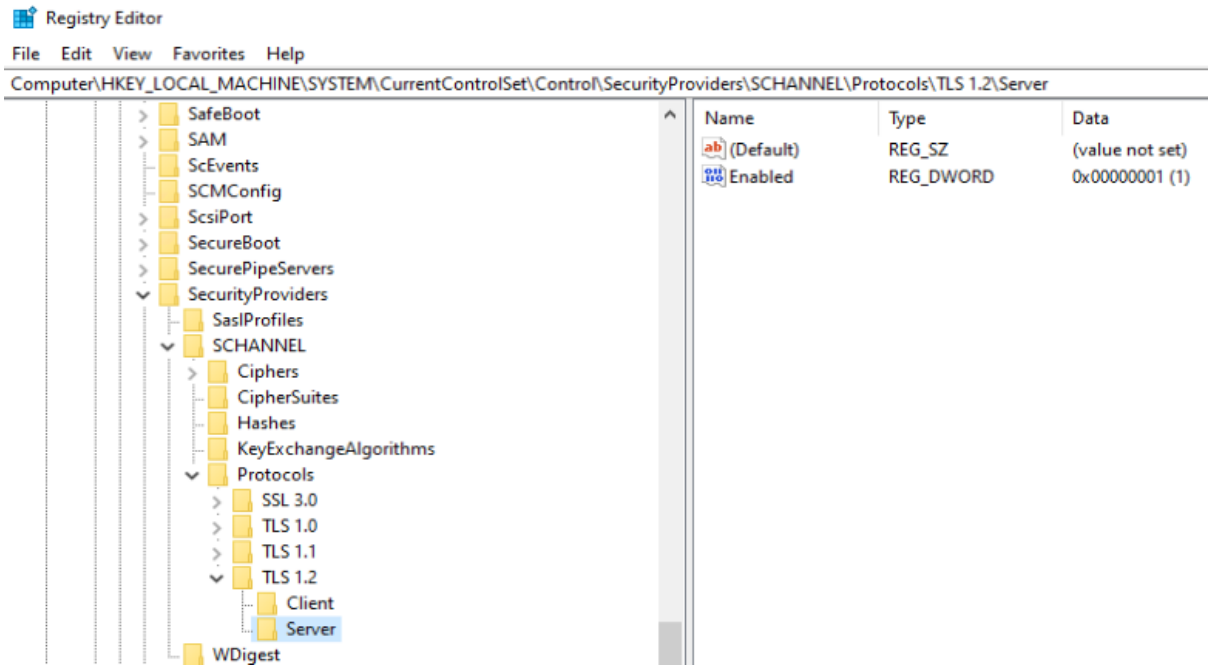
12. After that we need to login to the proxy VM and open the registry editor in our VM.

13. In the Registry Editor you need to follow the below path given and go to TLS 1.2

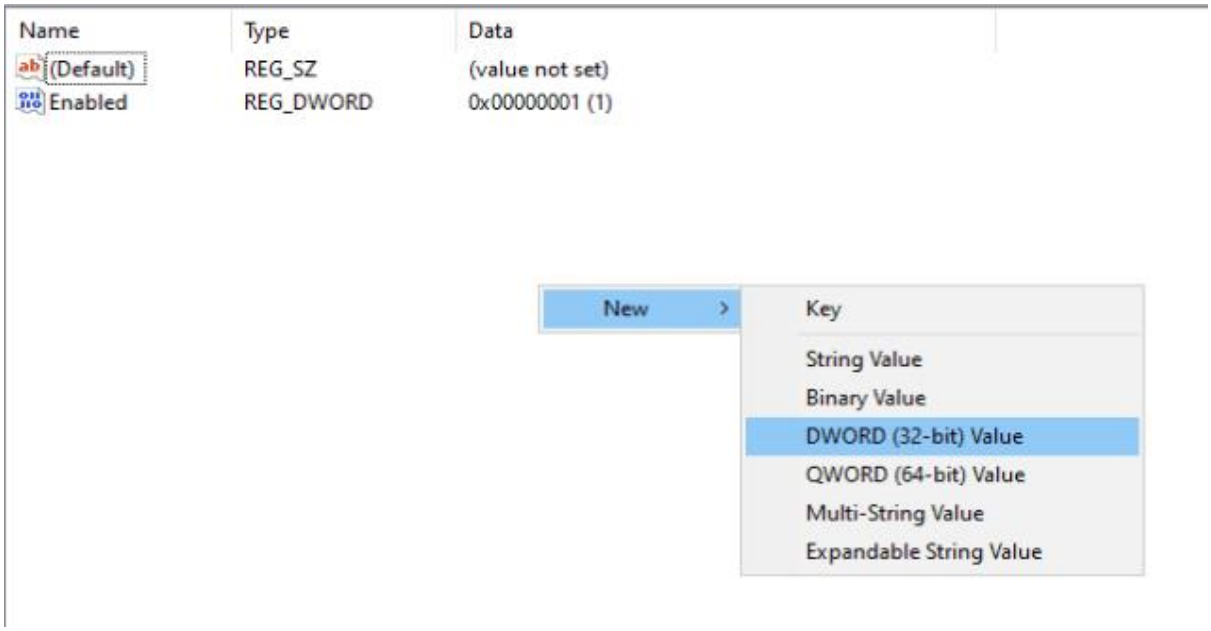
HkeyLocalMachine\System\CurrentControlSet\Control\SecurityProviders\SChannel\Protocols\TLS1.2

14. Here in TLS 1.2 we have two things client and server you can see that in both of them, the REG_DWORD is enabled. So, we need to create a new DWORD.

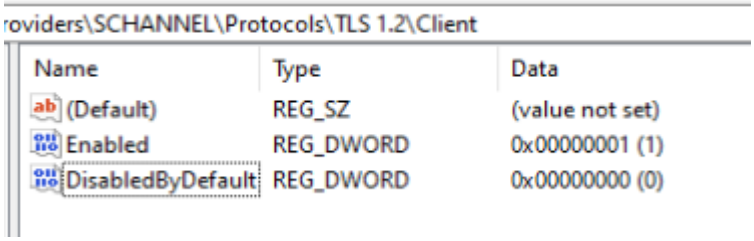


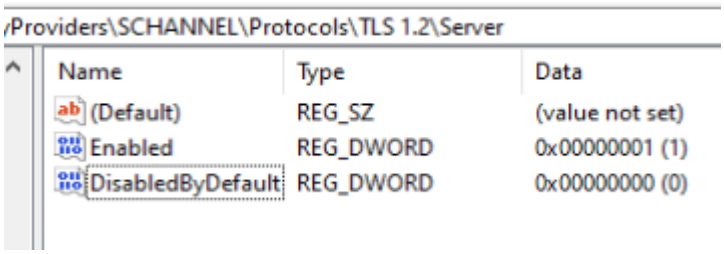


15. For that right-click in the empty space and choose DWORD.



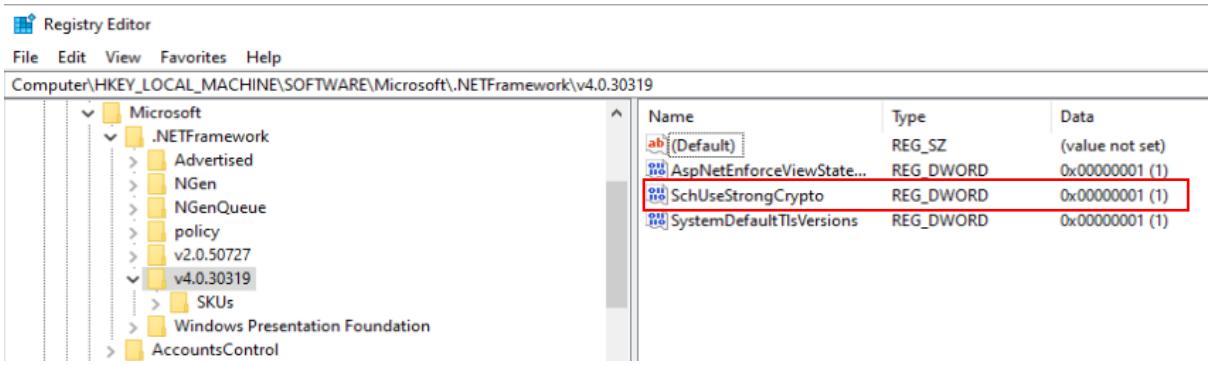
16. And we will name it DisabledByDefautl and its value is zero. We need to do the same thing for the Server too.



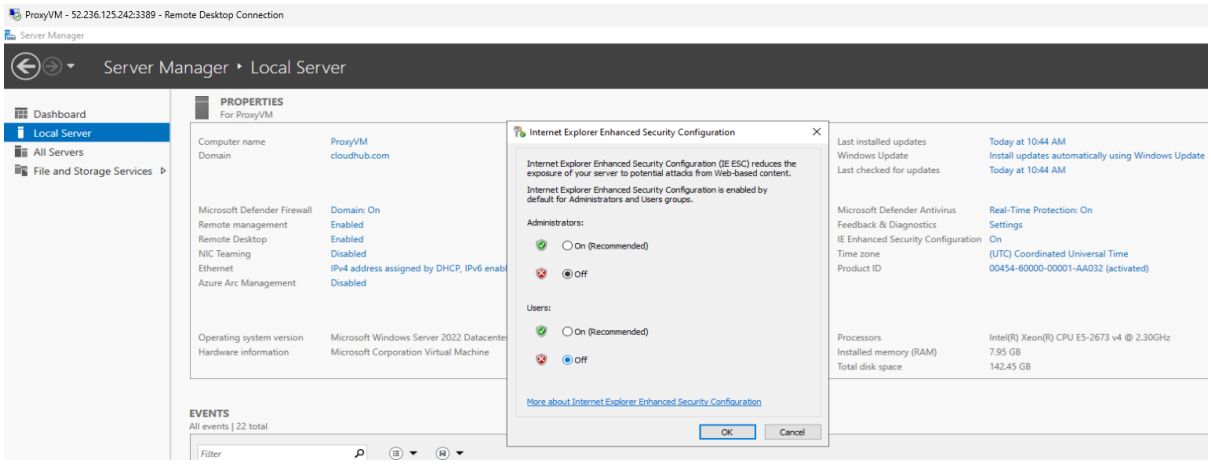


17. After that you need to go to this location and check that there is an entry for this highlighted name, and it should be set to 1.

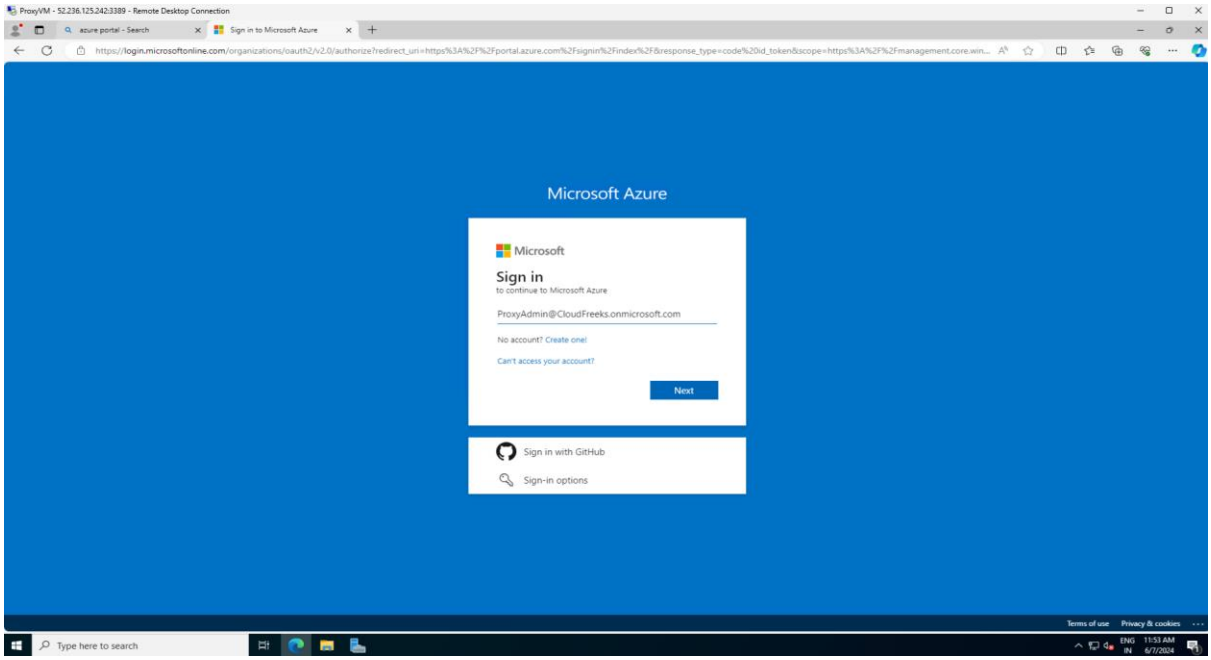
HkeyLocalMachine\Software\Microsoft\.NETFramework\v4.0



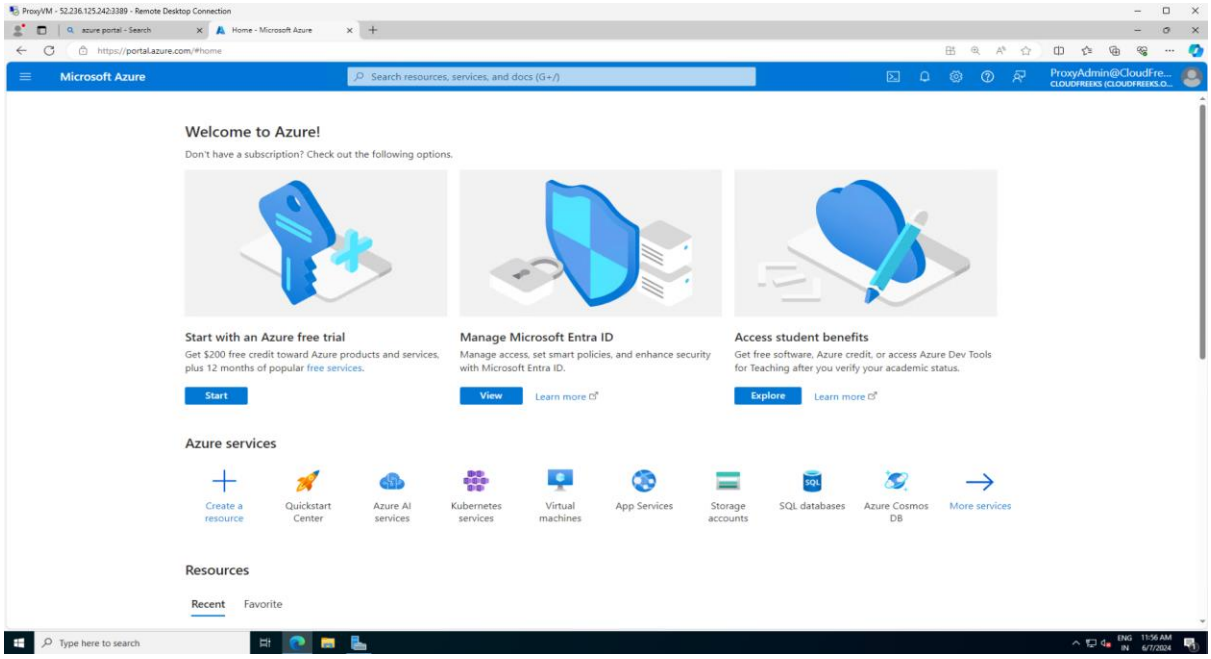
18. Now we need to restart the server. After some time you need to login to your Proxy VM.
19. Then you need to go to the local server and turn off the IE-enhanced security configuration. So, we can download certain things from the internet.



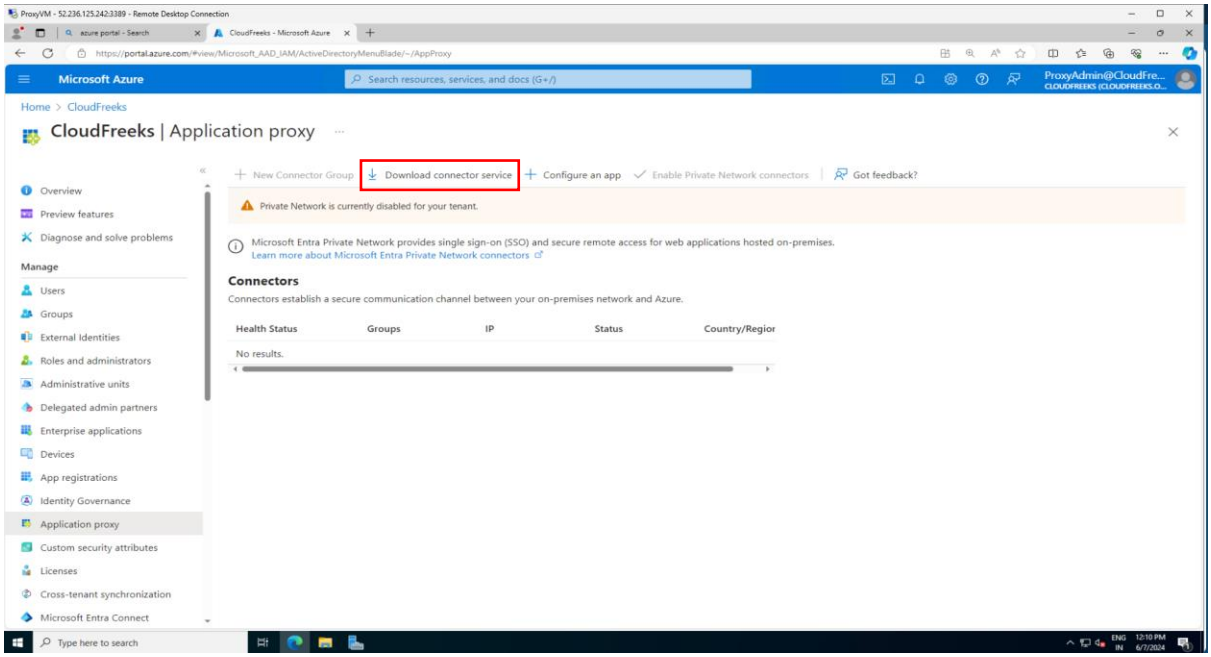
20. Now you need to open the Edge browser. Then you need to open the Azure Portal and log in as your new Proxy user you created earlier.
21. First you need to copy the user principal name from Azure Portal and then paste it in the VM and click on next.
22. Then you need to enter the password, after that, you need to change the password because we are logging in for the first time with this user.



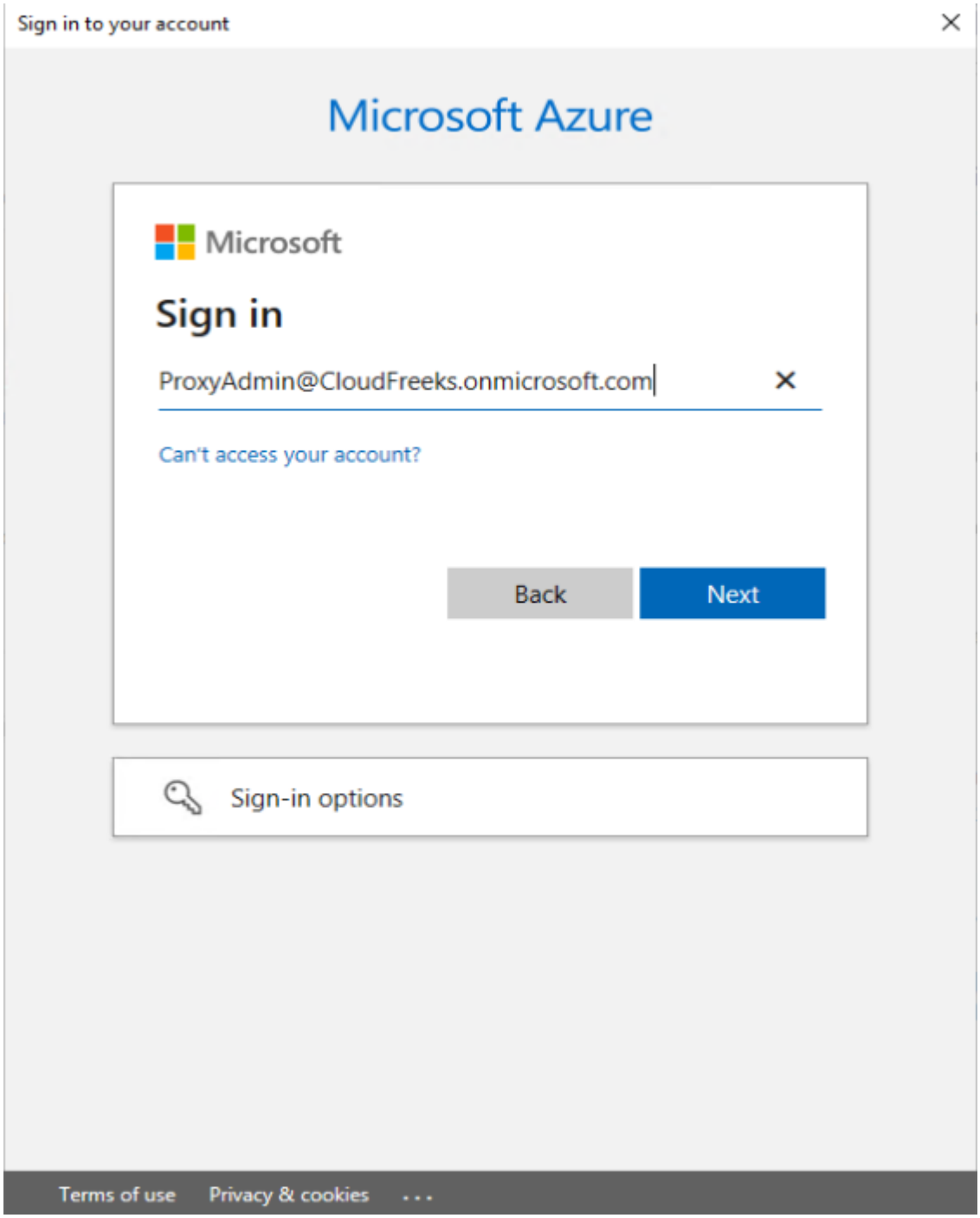
23. Once you are logged in the you need to go to Microsoft Entra ID.



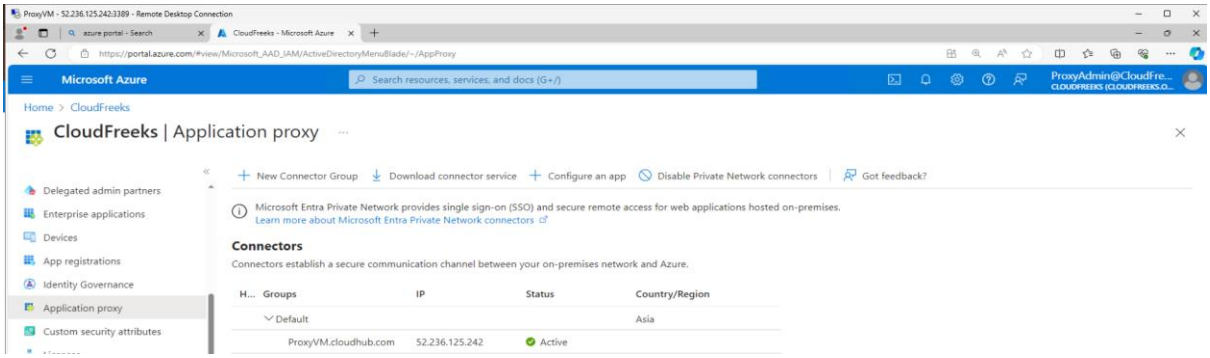
24. Now you need to go to Application Proxy and click on download connector service.



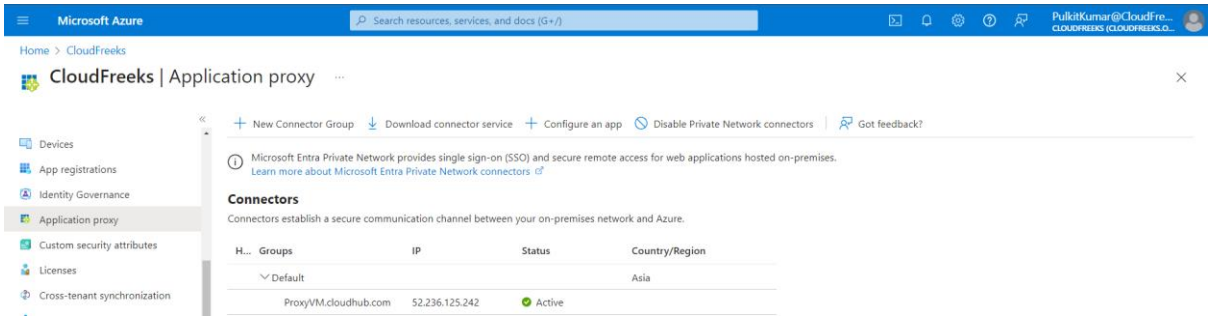
25. Once it is downloaded then you need to install it, while installing it will ask you to sign in. So, you need to sign in as Proxy admin user.



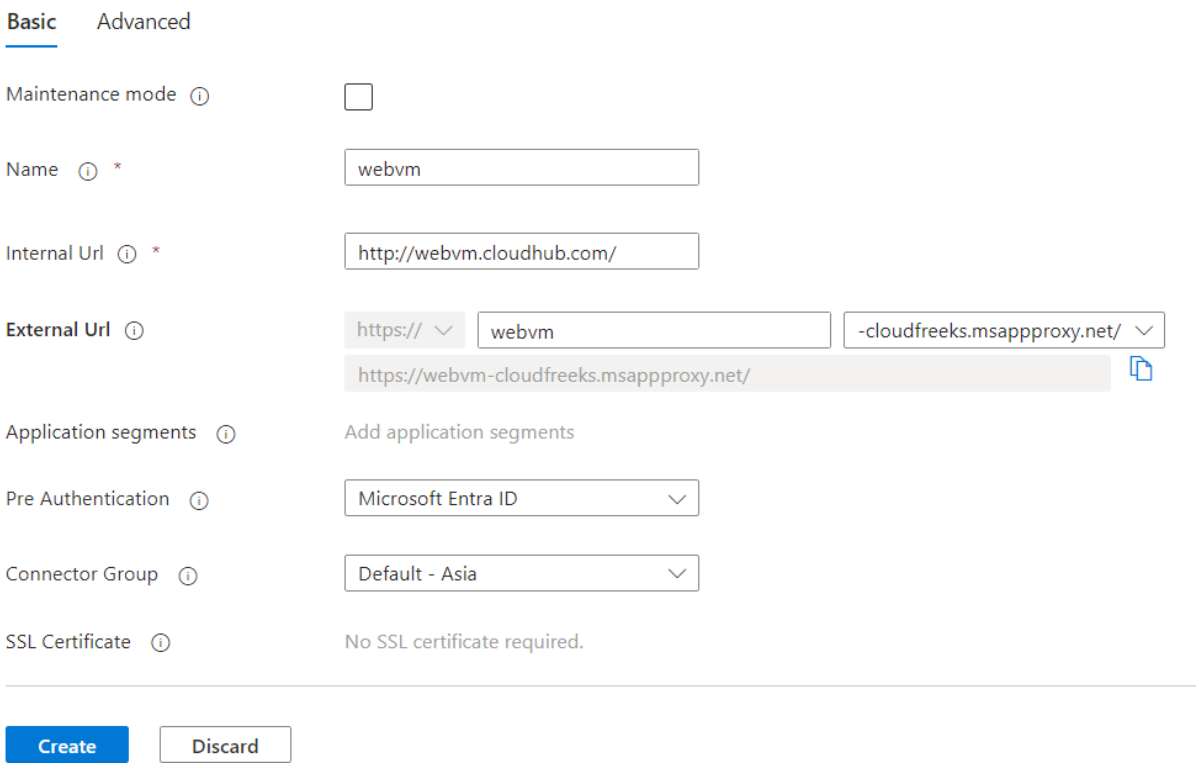
26. After everything is done refresh the page in your VM and you will see your proxy VM.



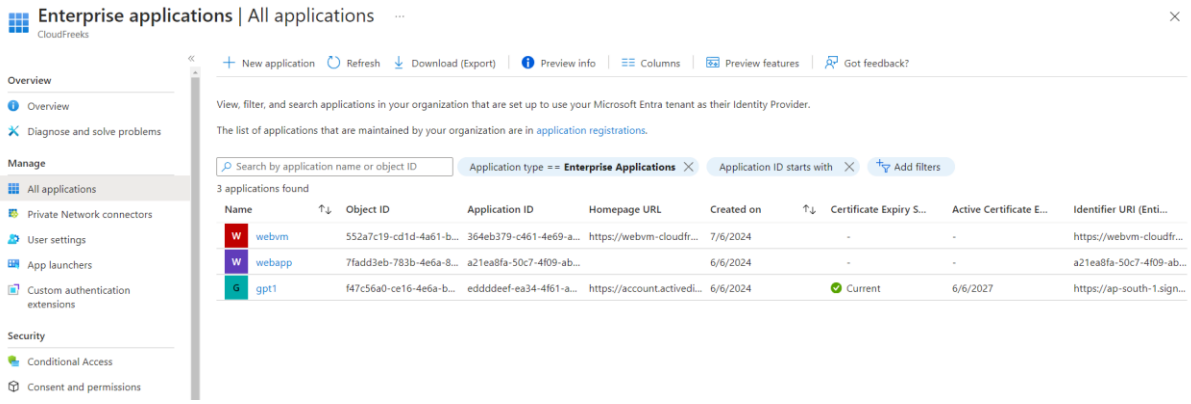
27. After that you need to sign out of this account from your VM.
28. Then go to Application Proxy in your main Admin account and choose to configure an app.



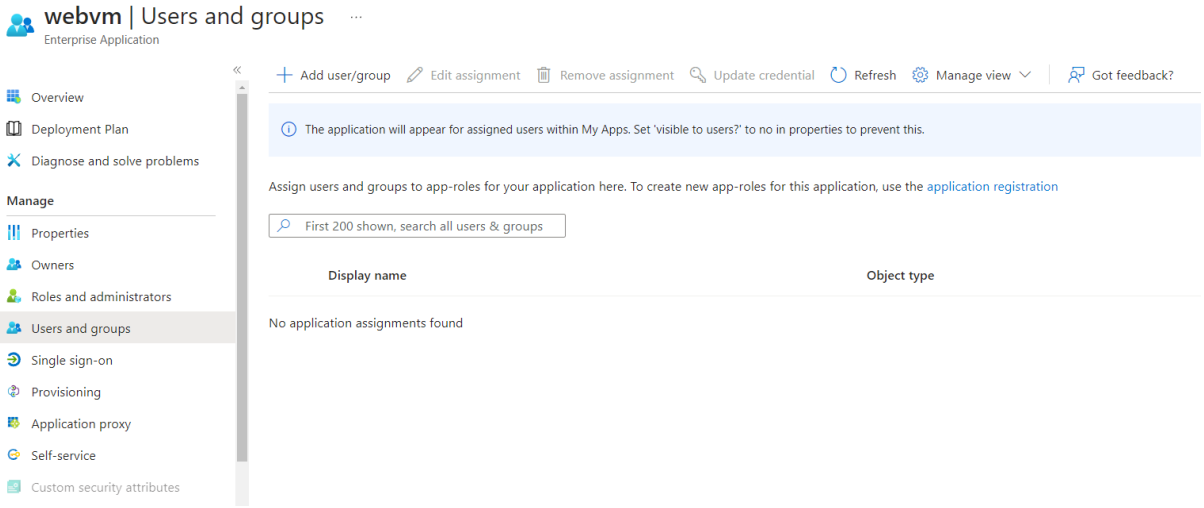
29. Now you need to give the name of your web VM where you have installed IIS and then give the internal URL as you can see below. Then you will get this External URL copy it to someplace then just create it.



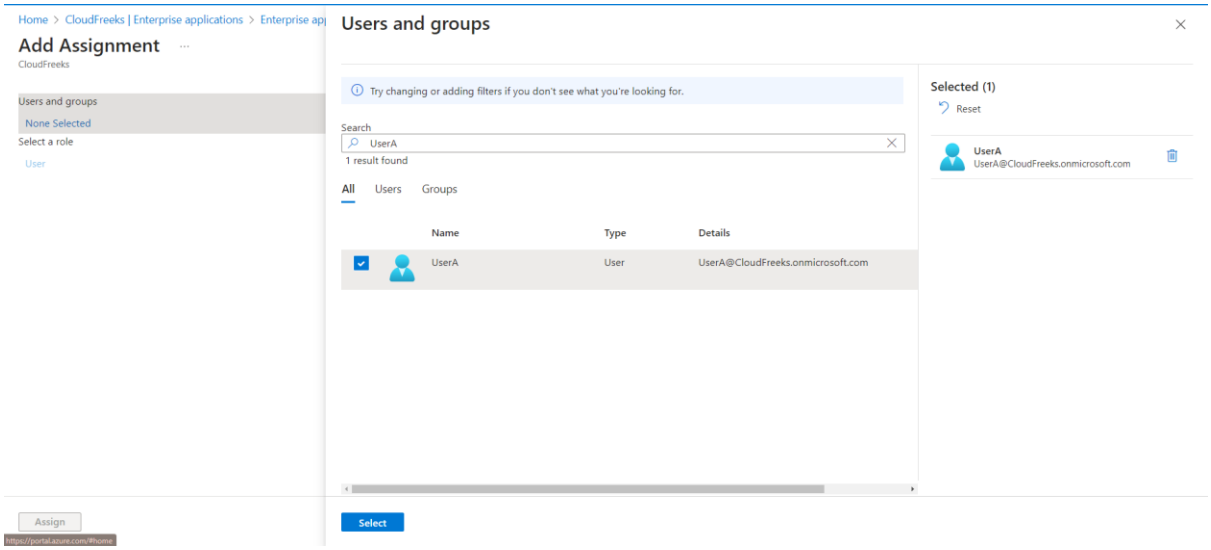
30. Now in your Microsoft Entra ID from the left pane go to Enterprise application and here you can see the Web VM. So, open it.



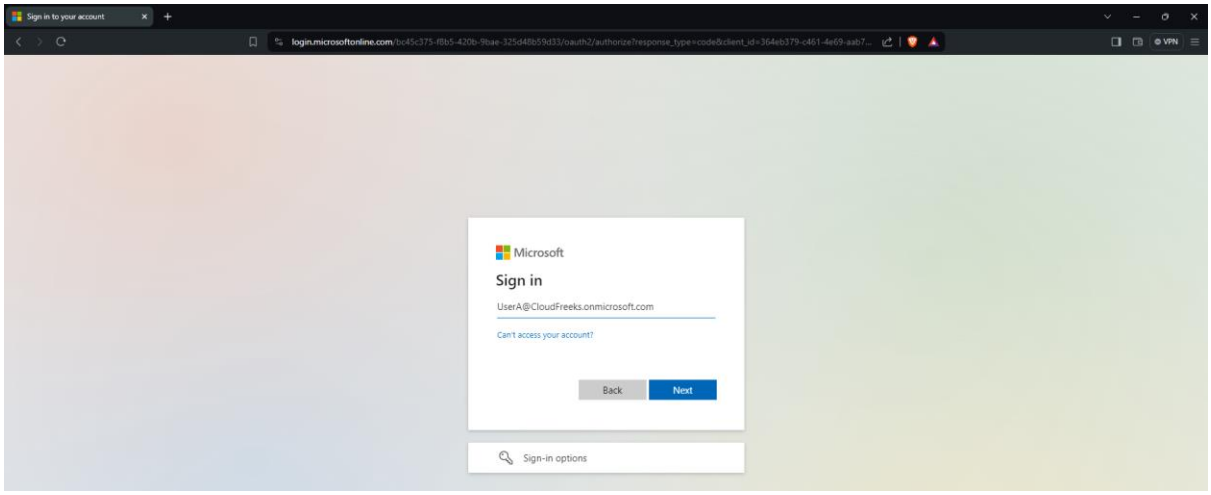
31. Here we can add users which are defined in our Microsoft Entra ID. Click on Add user.



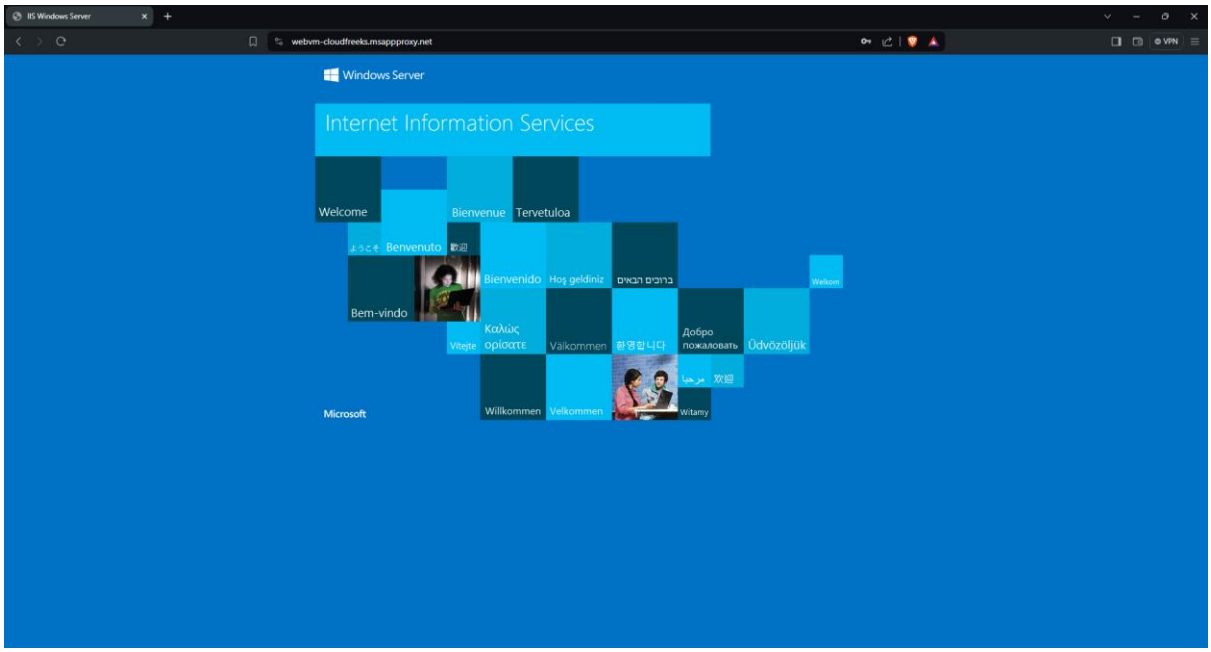
32. Now we will add a new username User A. If you don't have any user other than the Proxy admin user, then you can create a new one and then come back and add that user.



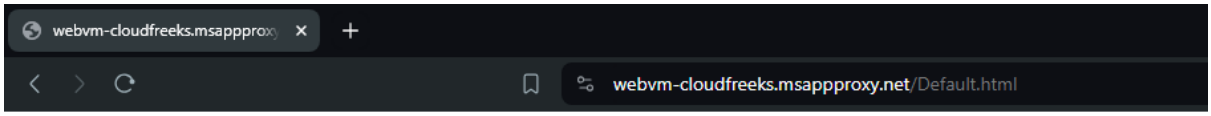
33. Now in Microsoft Entra ID go to User A and copy its user principal name and open up a new browser.
34. Then in the new browser you need to paste the URL that we copied while configuring an app in the application proxy.
35. Once you have pasted the URL it will ask you to sign in, you have to sign in as User A.



36. After entering the password, you will directly be on the Web Server IIS page.



37. And if you append it with default.html then you will see your web page.



This Sever is Web VM.

38. We can now access the web server running on Web VM, while the use of Azure AD application proxy. At the same time, we are now giving access to users defined in Azure Active directory to access the web server running on the Web VM.
39. Once you are done just delete all of the resources.