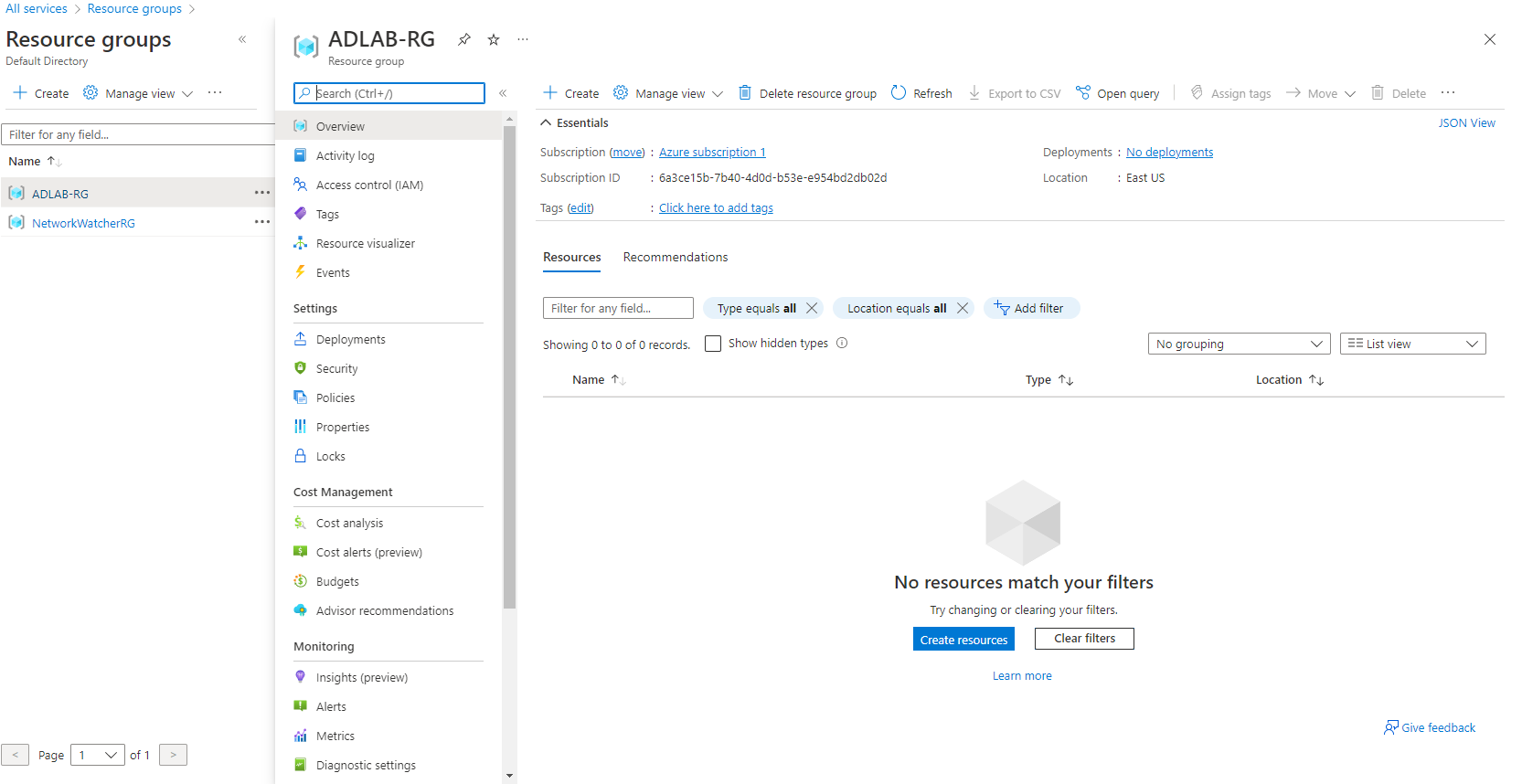
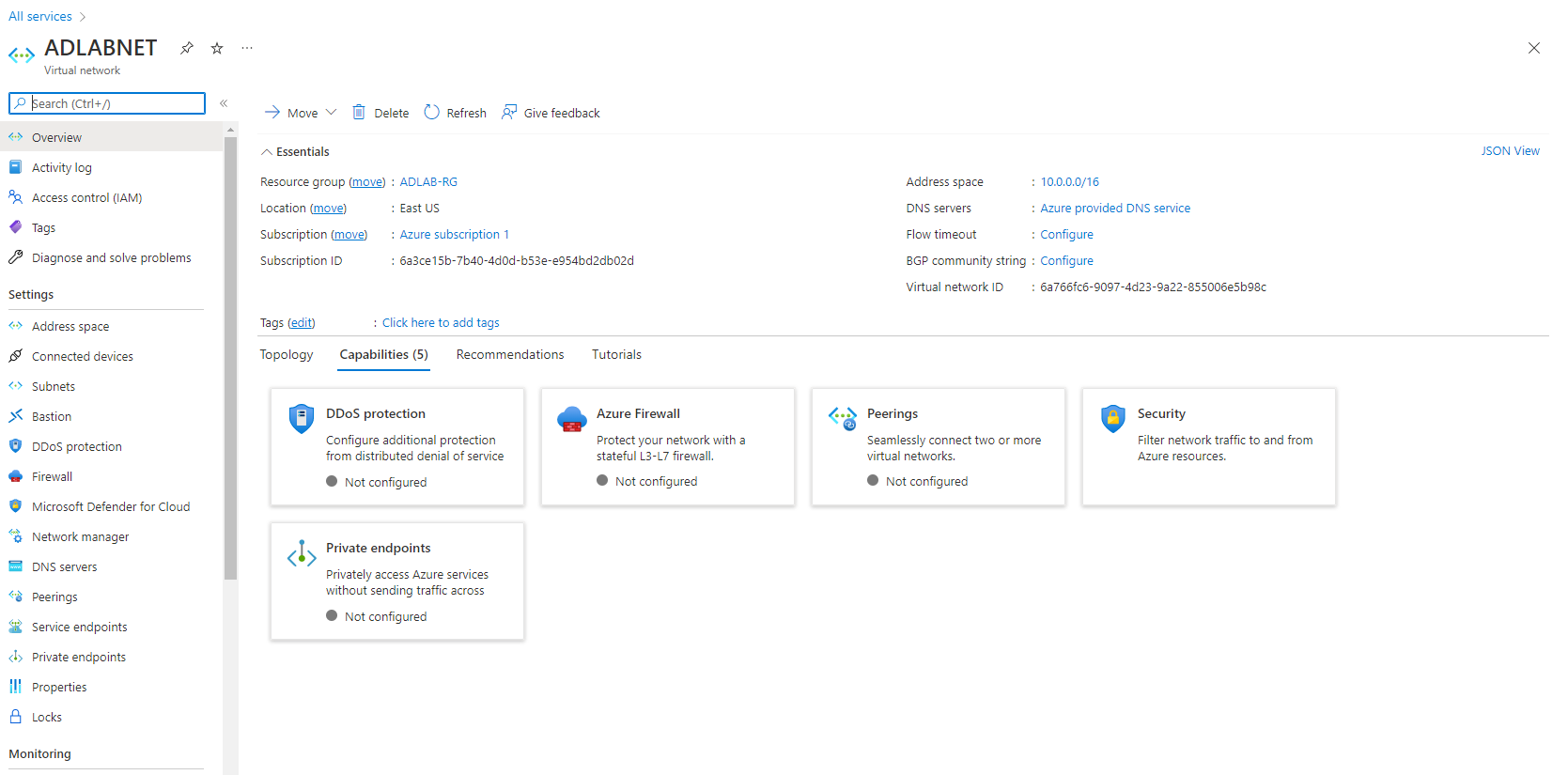
Creating Active Directory LAB

Objective: Creating an Active Directory Lab environment from scratch in Azure.

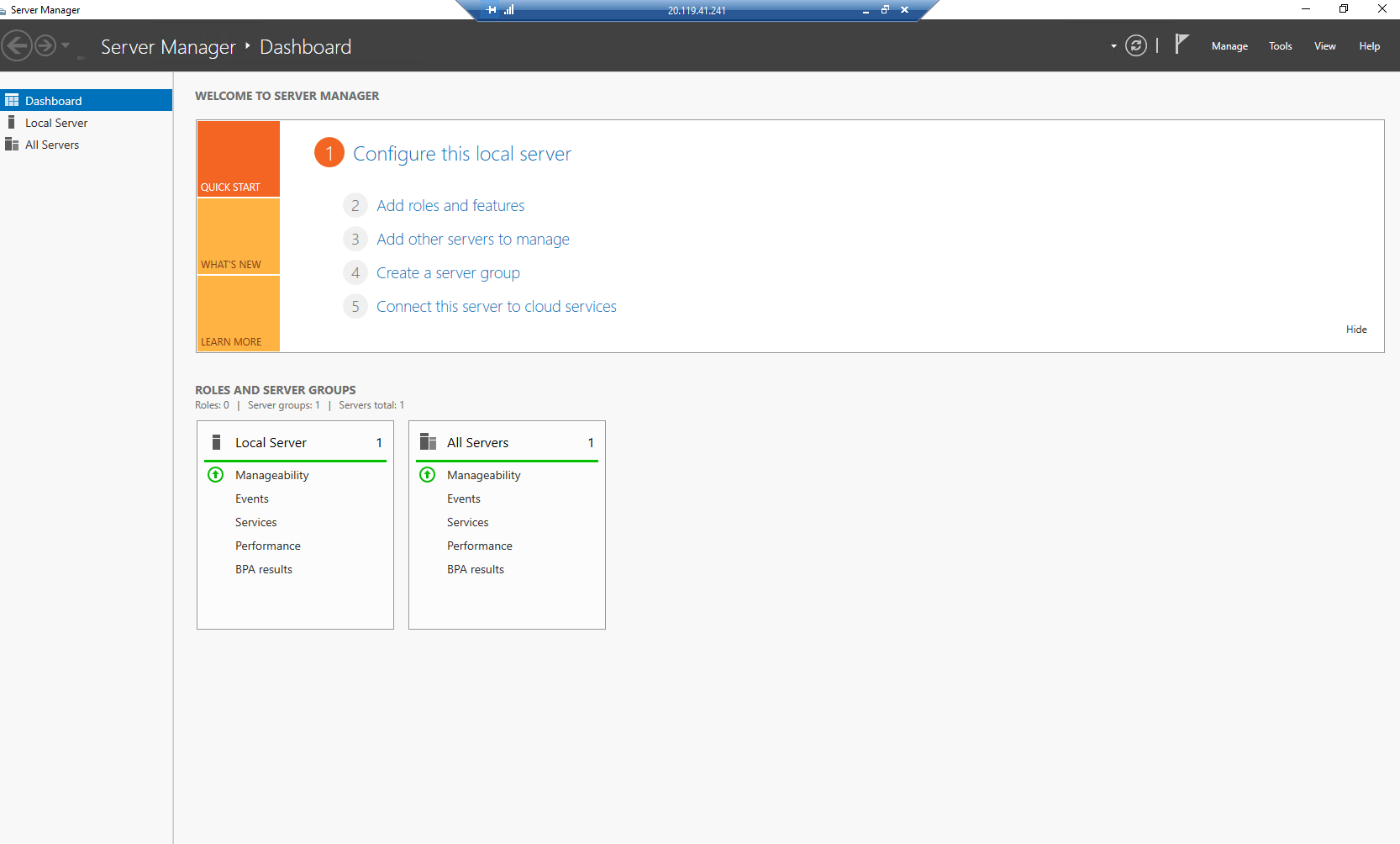
* To start this project off I had to make a Resource group. A resource group is a container that houses all resources used in a project. I named my resource group ADLAB to keep on topic with the objective of the project, but it could be anything.



* Step-2 creating a resource that allows communication securely within in/outside networks. I created a Virtual Network to handle this task.
  + Requirements:
    - Name: ADLAB-NET
    - Address Space/ IP Range: 10.0.1.0 /24
    - Subscription: Select your Subscription
    - Resource Group: ADLAB Note: you must use the resource group you previously created
    - Location: Select your region
    - Subnet Name: AD-SUBNET
    - Address Range: 10.0.1.0/24
    - Everything else I left as Default and selected Create



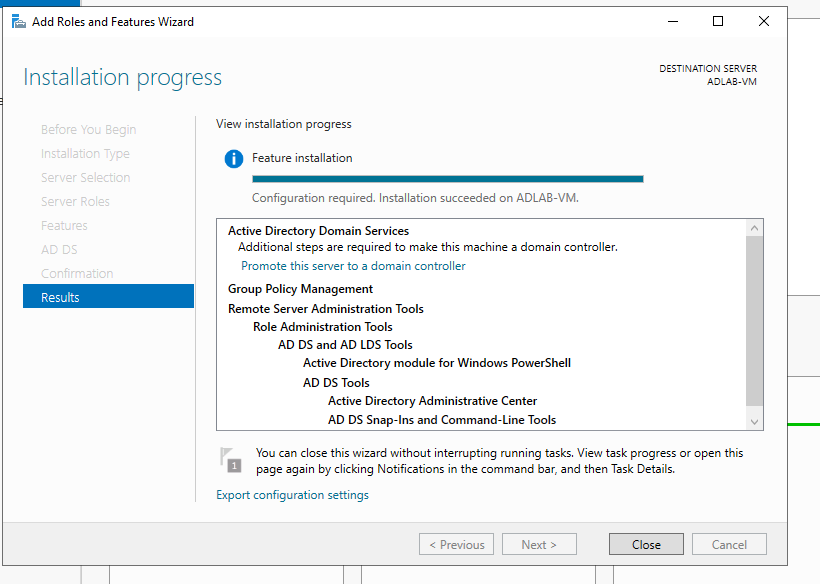
* Step-3 Creating the Domain Controller VM.
  + Step -01 Configuring Connection to DC
    - I had to create a Virtual Machine (VM) as I have yet to so.
      * Subscription and Resource Group must be the same as above
      * VM Name: ADLAB-VM
      * Region: Select your region
      * Availability options: Default
      * Image: I used windows server 2019 datacenter which I had to obtain from the marketplace. Marketplace 🡪 Compute🡪 Windows Server 2019 Datacenter
      * Azure Spot Instance: Default
      * Size: I used B2ms, but you can choose whatever that is available
      * Administrator Account: User Ghost Password 1 down 3 down
      * Disks: I used Standard for this Lab as this isn’t going into production since its lab environment with no need worrying of SLAs
      * Network: VNET, Subnet = 10.0.1.0/24, Create new Public IP holder = AD-DC-IP, NIC NSG Basic, Public inbound port = Allow Selected ports, Selected Inbound Ports = 3389 (RDP) and rest is default.
      * Review and Create VM Note: Creation can take a little bit 5-10 minutes enough time to go get a snack
      * Verify that the VM was Successfully Created. Go to Virtual Machines, selected your Machine, once inside go ahead and connect to it using RDP. Credentials is the set you created for the Administrator account.



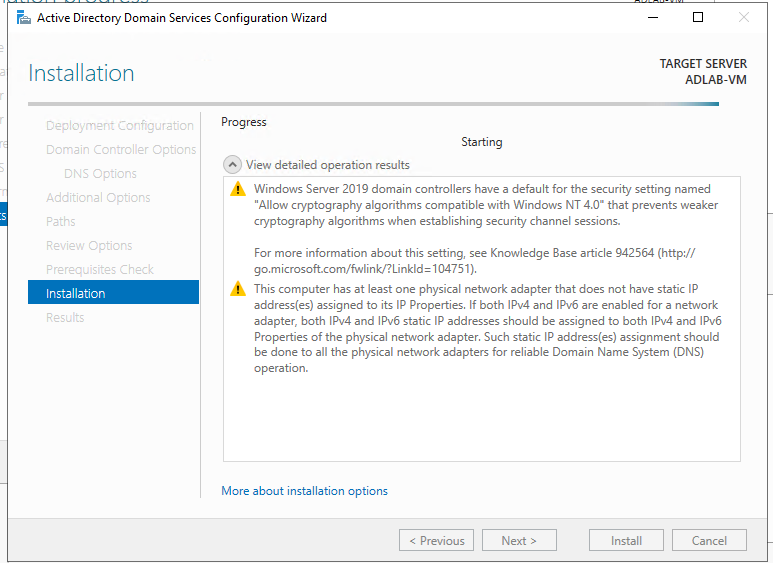
* + Step -02 Configuring the DC (Domain Controller)
    - I had to launch the Server Manager and select Add Roles and Features
      * Install Type: Role-Based
      * Server Selection: Select a sever from sever pool and I selected AD-VM. Note: you must select your VM you created as the DC
      * Server Roles: Check the box for Active Directory Domain Services 🡪 hit next and a pop up window should appear. Select add features

Note: I selected this role because it what allows a network user access to the permitted resources

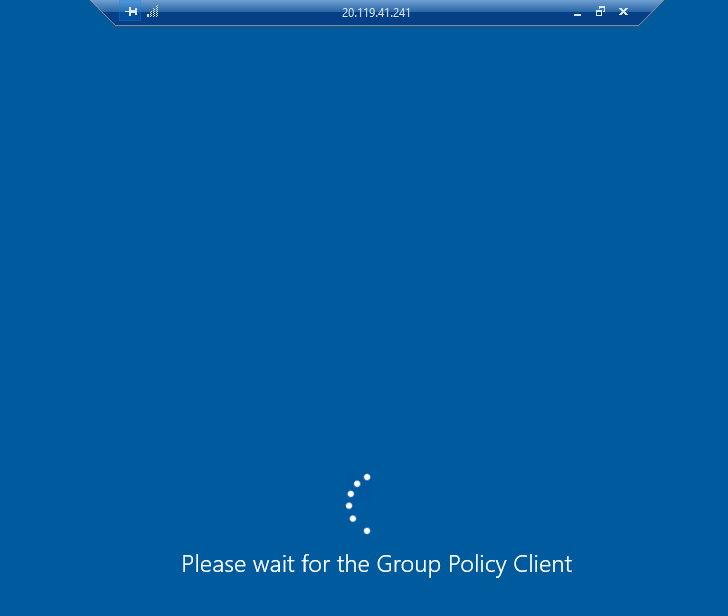
* + - * Features: Default
      * AD-DS: Default
      * Confirm and install



* + Step -03 Promote VM to DC
    - After configuring the DC I received a warning flag to promote server to DC and was provided a link. Clicking a link brings me a Wizard to configure the Domain Services.
    - Choose Add a new forest
  + Step -04
    - Create a Domain name, I’m going to use GhostTown.local
    - Give the Directory Services Restore Mode a password
    - NetBios domain name should be recognized and populate
    - Agree to defaults for the path
    - Review and Install
    - Note: The install is going to take a minute, and your machine is going to restart during the process. After the restart, I was able to login in with my domain credentials
    - Reminder: Administrator Account: User Ghost Password 1 down 3 down

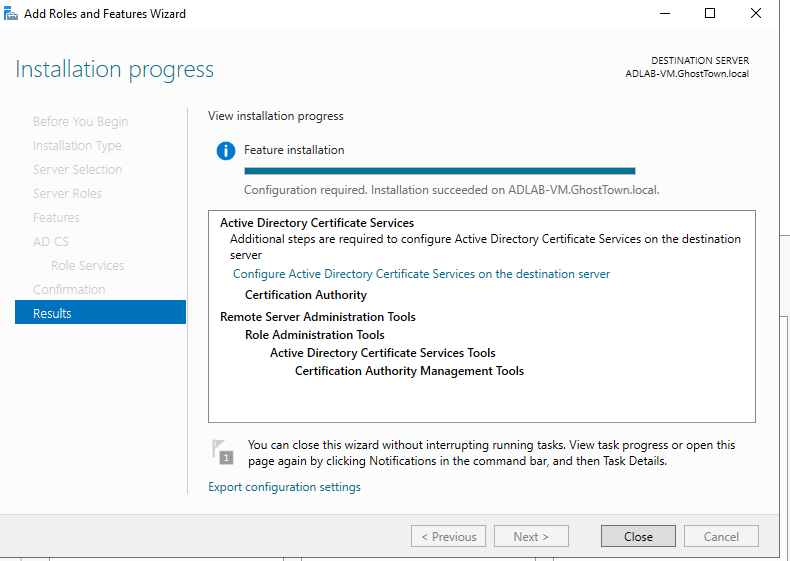


Completing Domain controller configurations and Installing the DC.

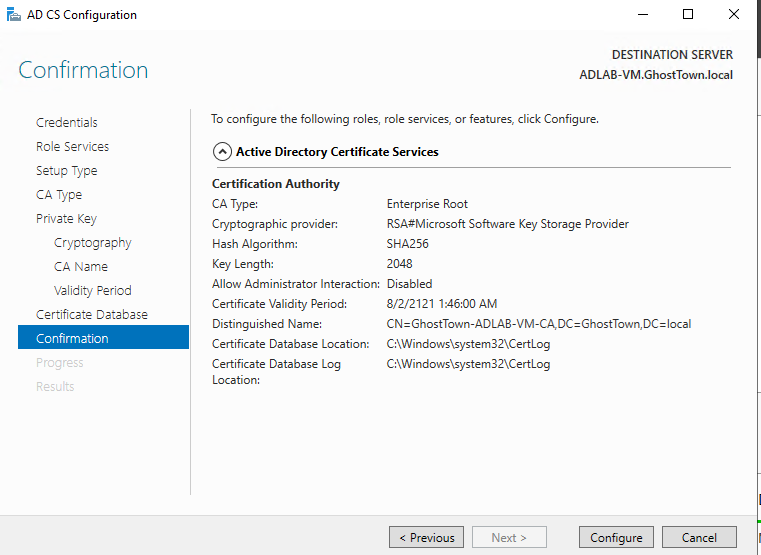


After Rebooting and signing back in using the domain name Ghosttown\Ghost password 1 down 3 down This take some time for your machine to complete the changes

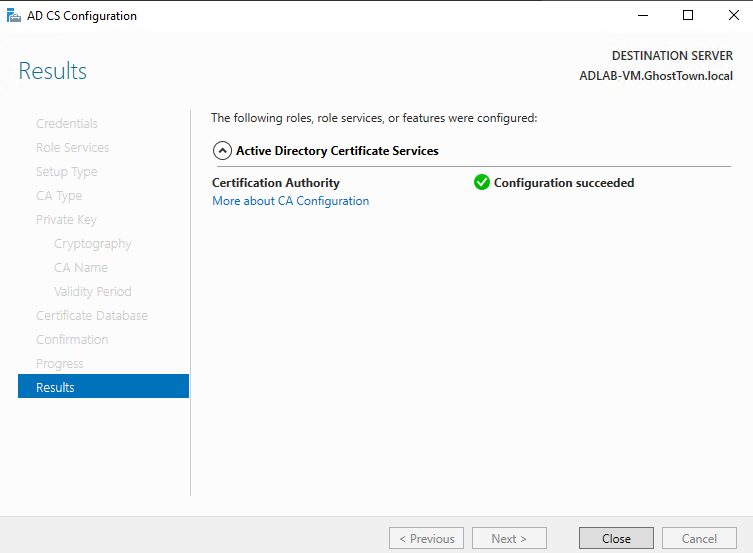
* + Step -05
  + Configuring Certificate Services:
    - I began by launching the Windows Sever 2019 and going to add roles and features.
    - Everything is default in the wizard until you reach the Server Roles tab. On the Server Roles tab select Active Directory Certificate Services (ADCS) to add feature
    - Once ADCS is installed, selected its table and select the Certification Authority check box
    - When the confirmation tab pops up go ahead and check the Restart destination Server automatically if required. By doing this the necessary components for Active Directory Certificates Services



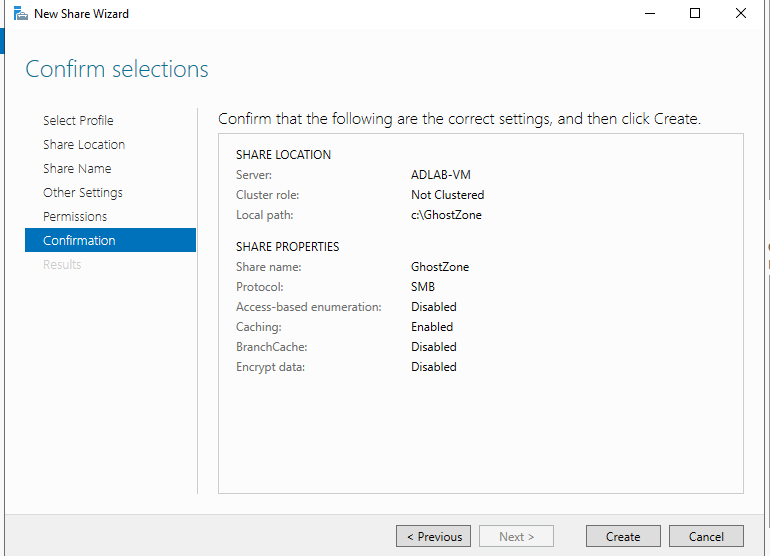
* + - After doing all this, I still was receiving a warning flag notification. Therefore, I decided to click on the link given to configure ADCS on the destination server.
    - On the ADCS configuration wizard, hit next on the Credentials tab
    - On Role Services, Check Certification Authority and hit next
    - On setup type for CA select Enterprise CA, Root CA
    - Private key tab I had to make a new private key. I had to use default options on the cryptography tab
    - Use Default names on the CA NAME tab
    - I selected 99 years on the validity period. This ensures the CA never expires
    - Certificate Database tab is default

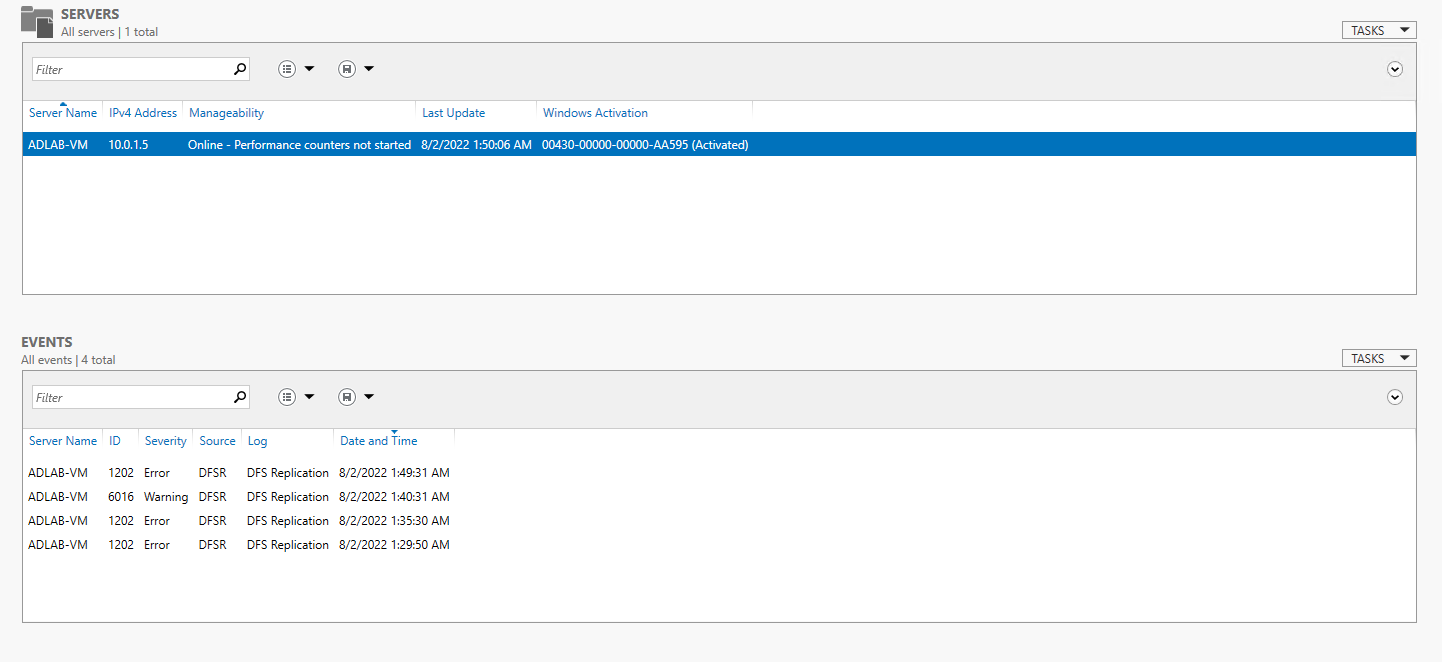


* + - On the confirmation tab select the configure table. Once you see Configuration Succeeded close dialog window and restart VM for changes to go into effect.



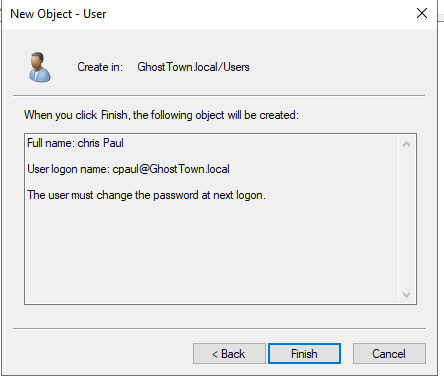
* + Step -06
    - Setting up a share path. Created folder called Ghostzone on the C drive.
    - On the Server Manager I had to select File and Storage from the services tab, and I had to hit Shares
    - From there I had to select New Share under Tasks
    - On the pop-up wizard menu, I selected SMB Share -Quick
    - Share Location tab I had to select Type a custom Path (C://Ghostzone) and hit next
    - Share name = Ghostzone and hit next
    - Other settings tab, and Permissions is left as default
    - Create and once you get a created successfully in the window. Close Window Out



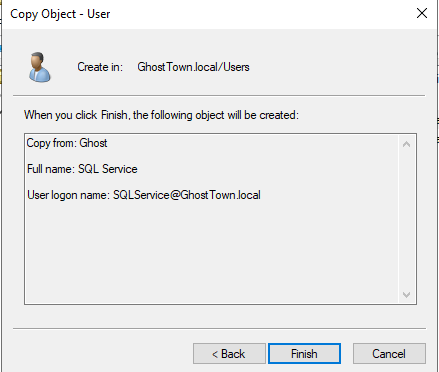


Here looking at my different servers I see I successfully activated my VM to manage the Ghost town Domain. I do see there is Some events in the Event Categories which is showing nothing major currently.

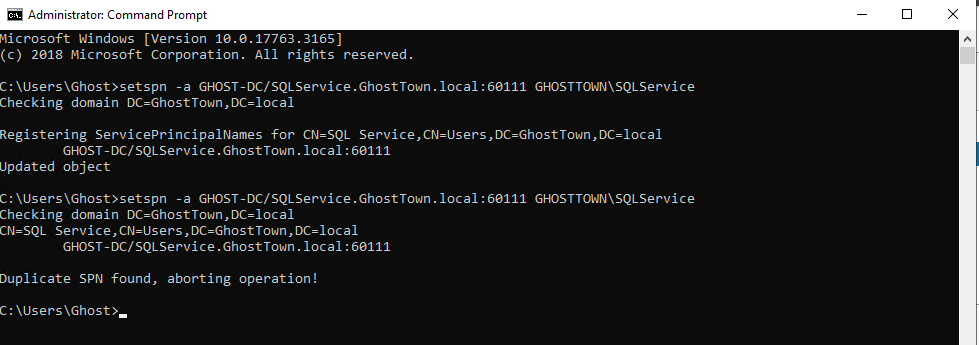
* + Step -07
  + Now onto the meat and potatoes of creating some domain users.
    - In the Server Manager, locate Tools and select AD Users and Computers
    - Right Click on your domain (Ghost.local) and select create new Organization Unit (OU)
    - Name the OU something simple as Groups and hit ok. This now created a new folder called Groups
    - Go to your user folder and move all the users except for Guest and TestUser1 to the new Groups folder previously created.
    - Now back in the users Folder its time to create a few users. Right Click 🡪 New 🡪User and follow the prompts
    - Create a Domain-Admin Type User by copying Ghost Properties by right clicking and selecting Copy. First name SQL Last name Service, User logon SQLService and create password
    - Once SQLService User was created I had to edit its properties by Right clicking go to General and provide a Description of Password is “Insert Password”
    - Setting up a Service Principal Name (SPN) for the SQLService using setspn command in command prompt. Note: The CMD prompt needs to be ran as Administrator
    - I have now completed the Domain User Creation along with all the required configurations.
    - No Machines have been added to the domain I just created, therefore next is to add some. Note: Knowing the Machines IP will be needed



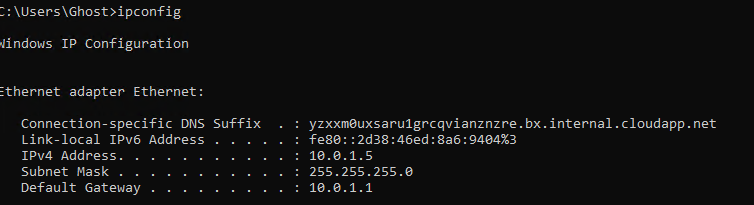
Created a new user profile for Chris Paul to the user group. To go with enterprise nature, I assigned Chris a temporary password where he is going to have to change when he logins.



Created a domain-admin type user using the properties from my admin user account.

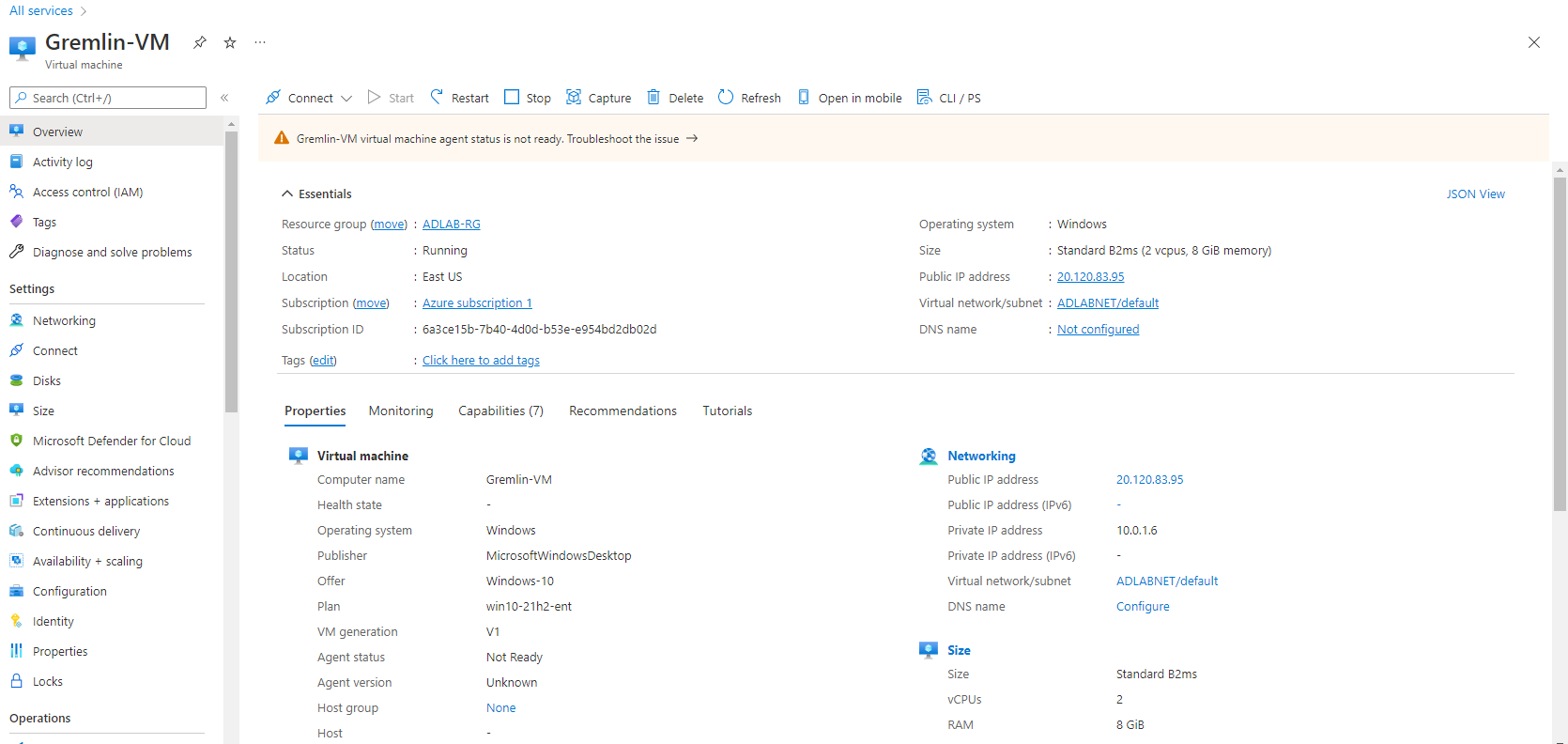


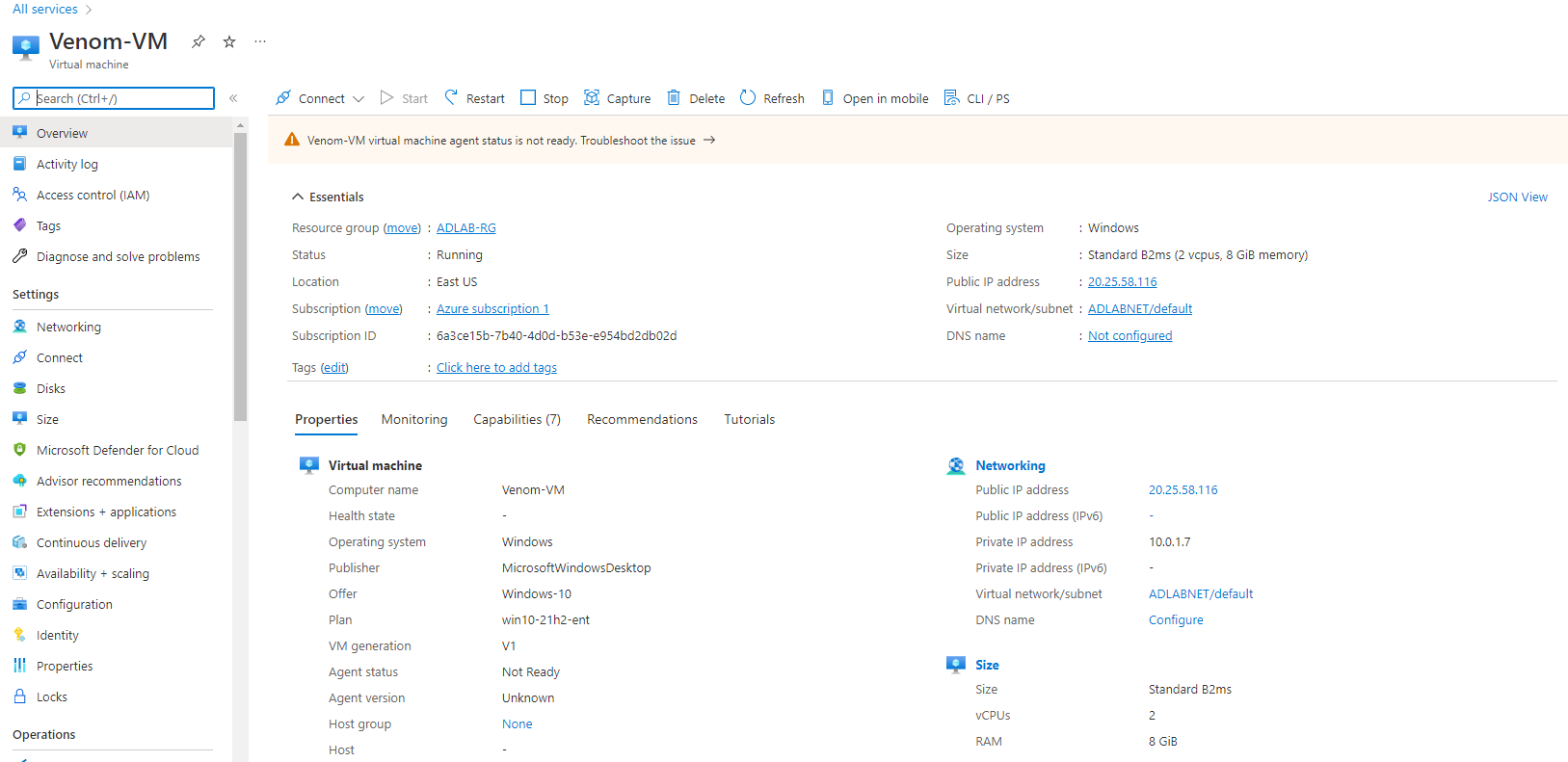
Configured the Service Principal Name for the SQLService account using the setspn operator.



Issued the ipconfig command to determine my network information for further configurations.

* Step -08 Setting up User Machines

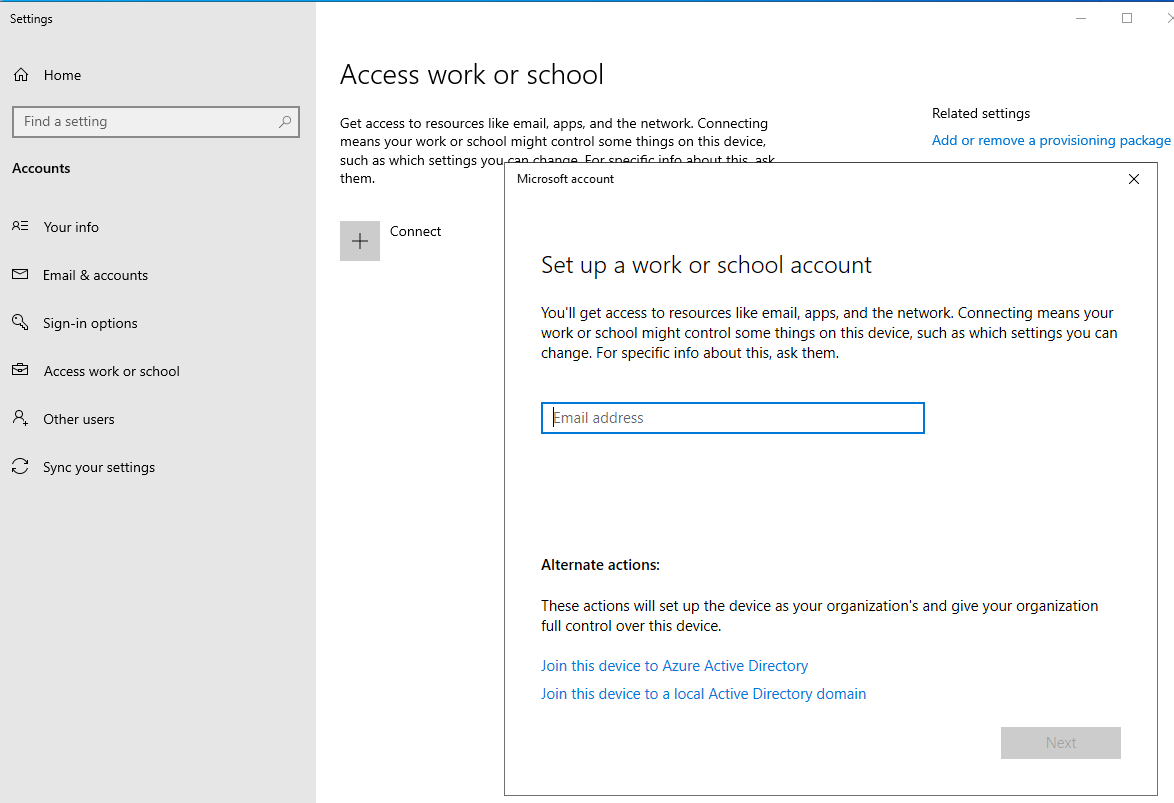




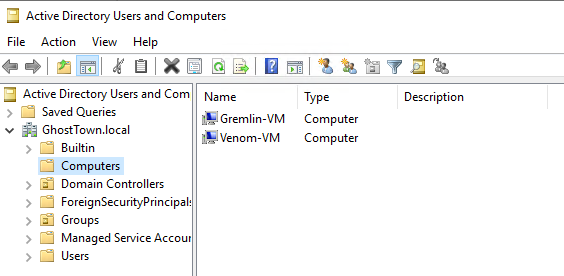
Next is to join to the users to the Domain. Starting off with my Gremlin VM as its my primary I had to go into the network settings and configure the ethernet adaptor to find my domains DNS controller which for this lab was 10.0.1.5.

NOTE: After configuring the DNS server for each Computer you must restart the VM for the changes to take effect.

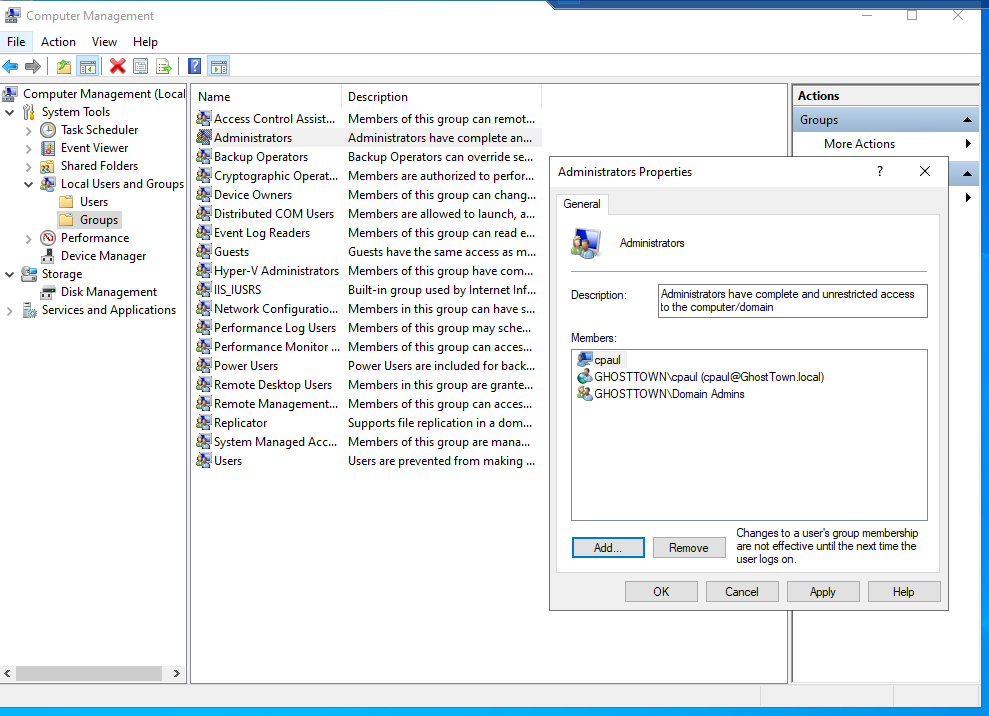
To join them to the domain, go to access work or school in the search. Click Connect 🡪 Join this device to a local Active Directory domain and input the domain information. For example, for this lab my domain is GhostTown.local Domain Admin- Ghost and password.



As mention above all that is next is selecting the Join this Active Directory Domain fill in your information. Reboot your Domain Controller VM and it should be populated under computers Organizational Unit.



Indeed, my computer VMs populated successfully



Assigned User Chris Paul to the user machines. The above process started out going into my Gremlin VM or Domain user VM going adding myself an Administrator user machine and we are complete for this lab.

NOTE: To add Venom as an administrator user account you would just repeat the above steps