AWS – Project management in the Cloud

|  |
| --- |
| **Learning Outcomes** |
| At the end of this practical lesson, students will be able to:   * Setup VPC Public and Private Network * Setup AWS EC2 Instances * Setup Active Directory Domain Controller in Domain Server * Create different users under the domain * Allow client to join Domain Network * Allow RDP Connection on user logon |

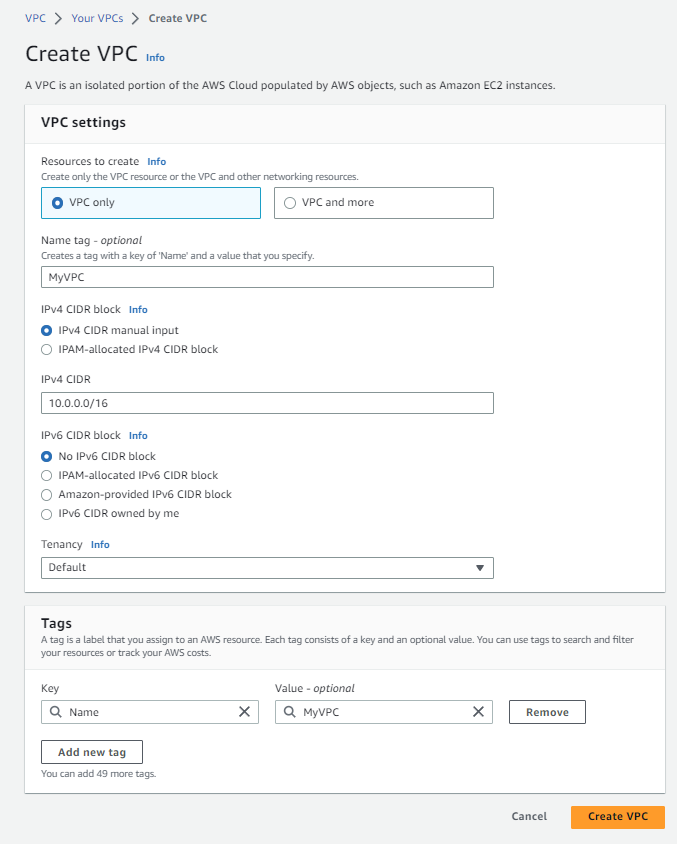
1. Setup VPC Public and Private Network

**Step 1:** search for “VPC” service in the search box on the top left

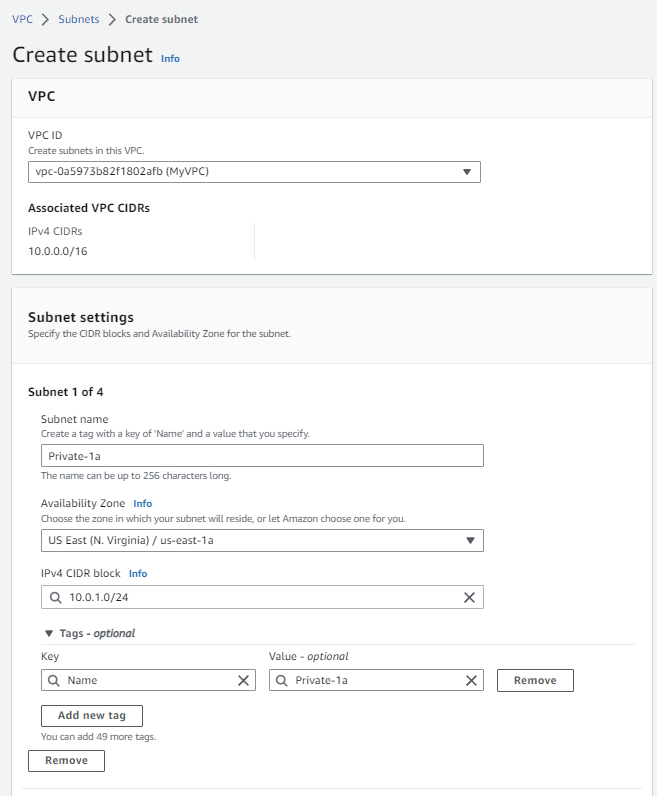
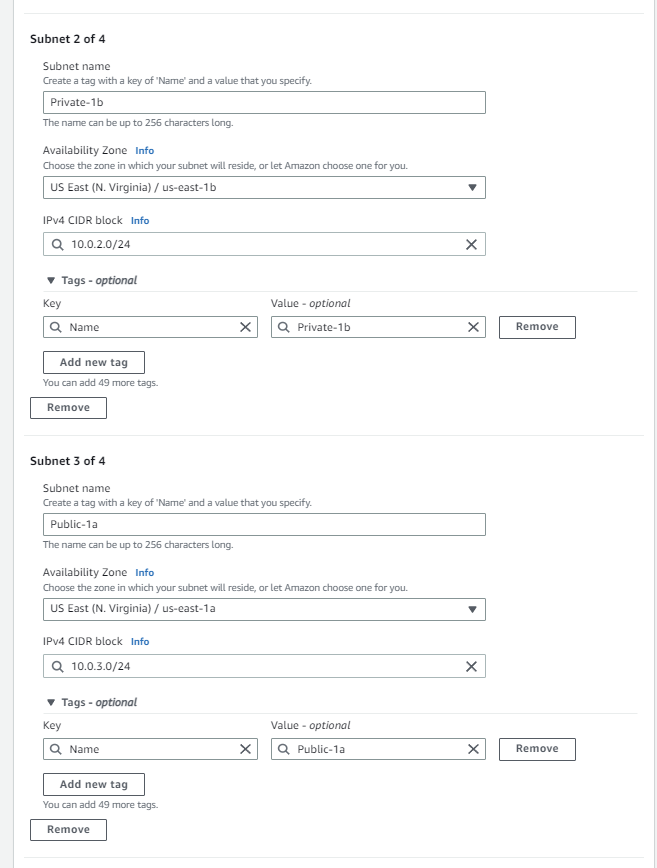
**Step 2:** select “Your VPCs” at the left sidebar

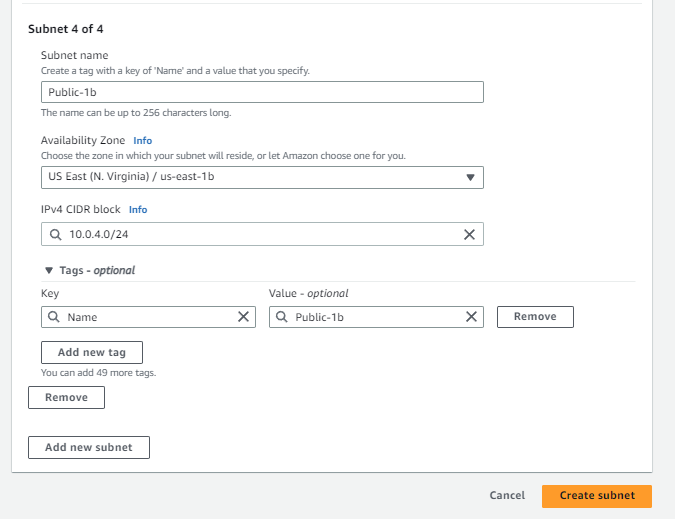
**Step 3:** click “Create VPC” at the right side of your screen

**Step 4:** follow Figure1 which is provided below to create your vpc

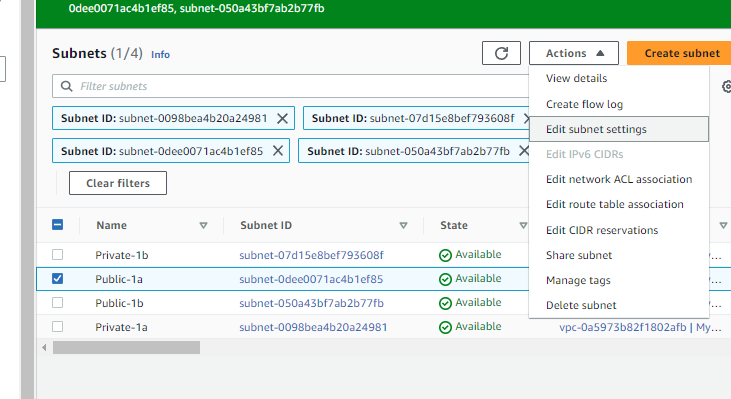
** Figure 1**

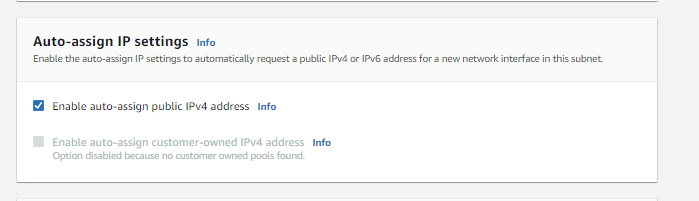
**Step 5:** to create subnets and associate with “MyVPC”, select “Subnets” at the left sidebar and click “Create subnet” at the right side of your screen. Follow Figure2,3,4 which is provided below to create some subnets.

** Figure 2  Figure 3**

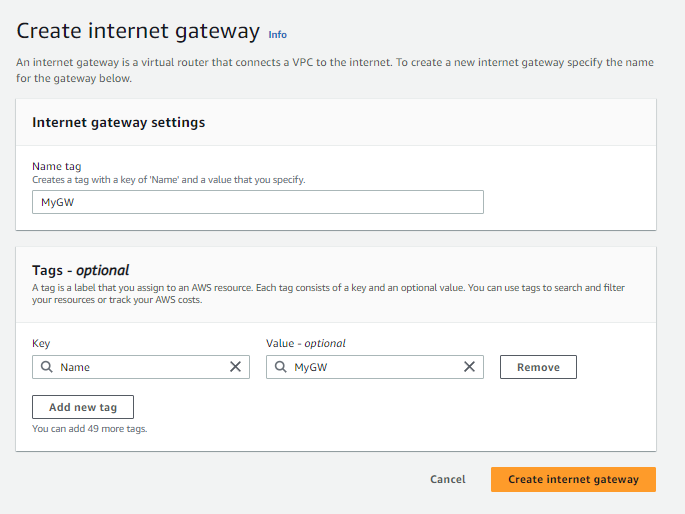
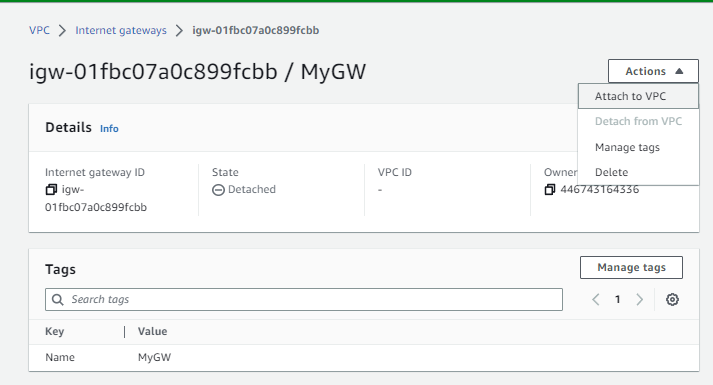
** Figure 4**

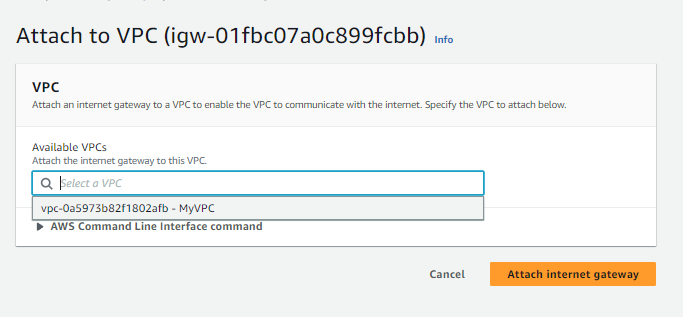
**Step 6:** enable “Auto-assign” for public IPv4 address for “Public-1a” and “Public-1b” subnets. Check “Public-1a” box and click “Create subnet” 🡪 “Edit subnet settings” and check “Enable auto-assign public IPv4 address” box. And do the same for “Public-1b”



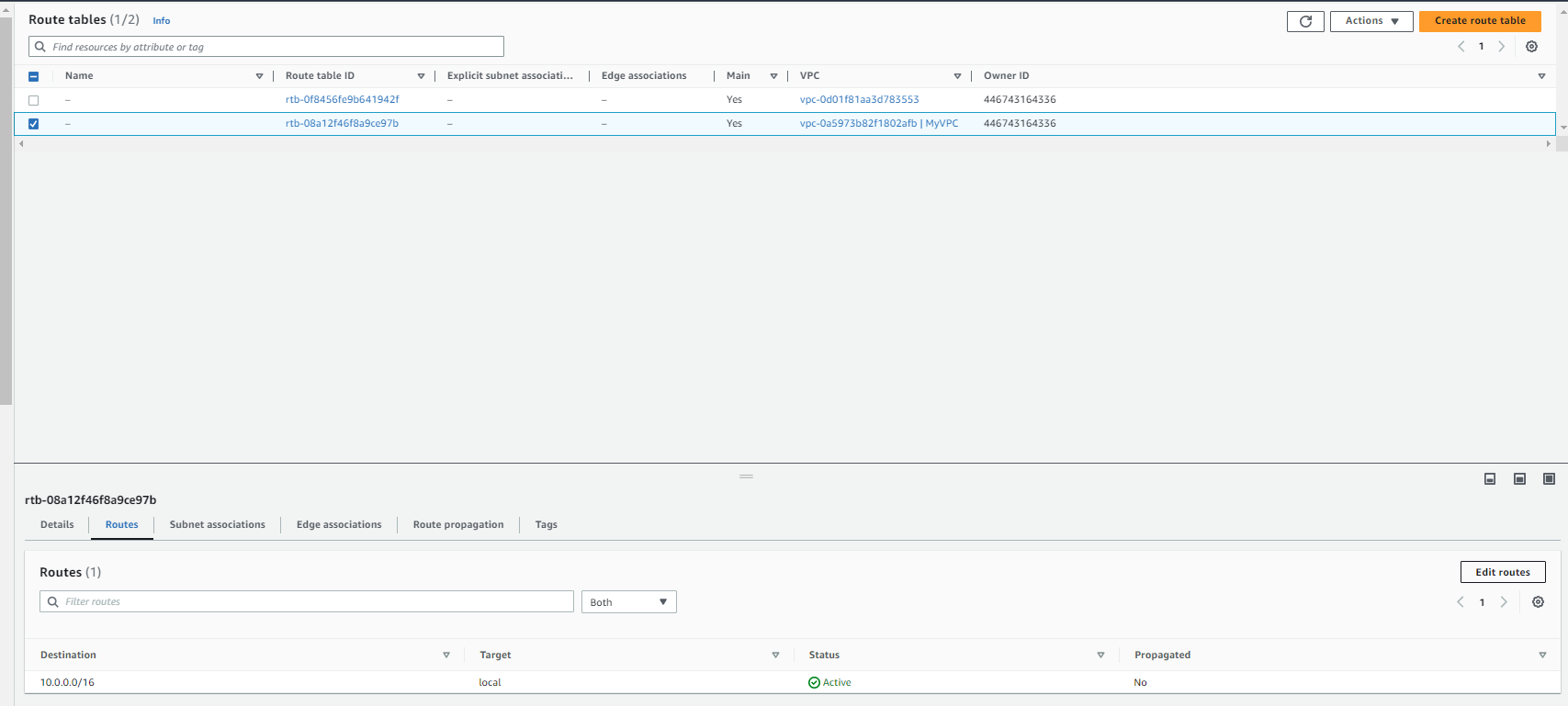


**Step 7:** Create an internet gateway for “MyVPC”. Select “Internet gateways” at the left sidebar and click “Create internet gateway” at the right side of your screen. Follow Figure5,6,7 which is provided below to create some subnets.

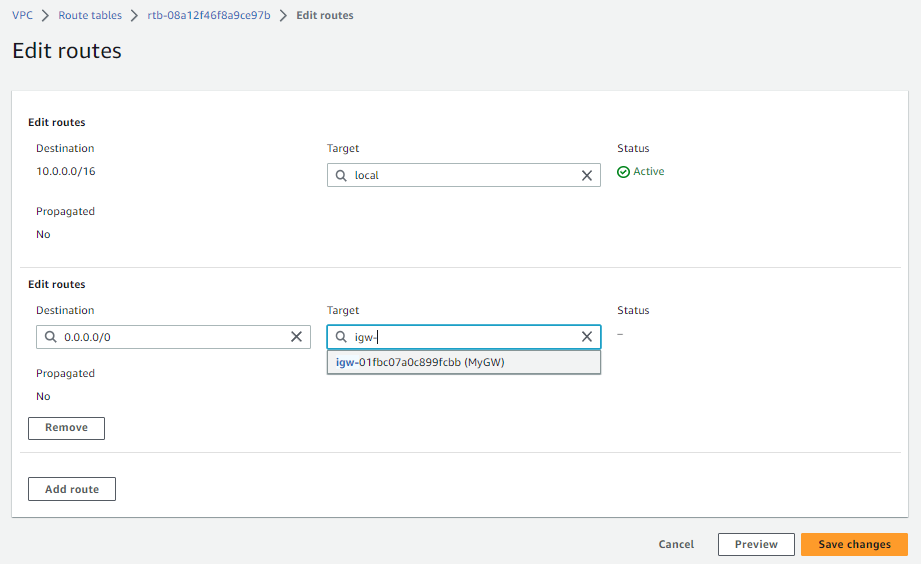
** Figure 5  Figure 6**

** Figure 7**

**Step 8:** To route vpc public subnet to the internet, select “Route tables” at the left sidebar and select the route that is linked with “MyVPC” and select “Edit routes” at the bottom right of the screen Follow Figure8,9 which is provided below to add in an “anywhere” route for IPv4

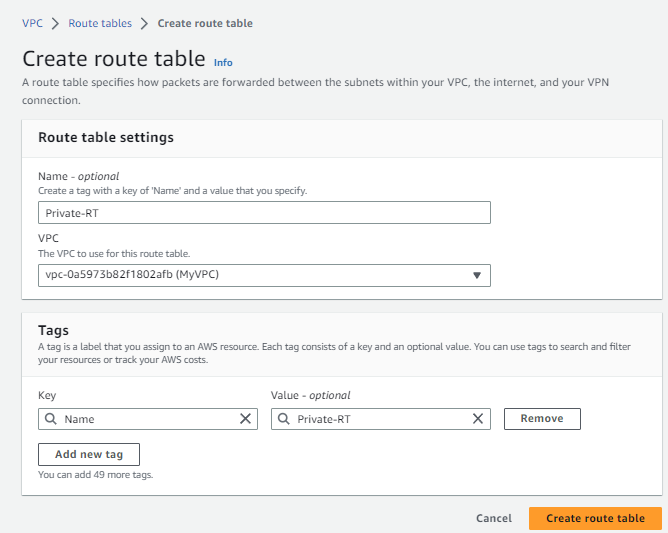
****

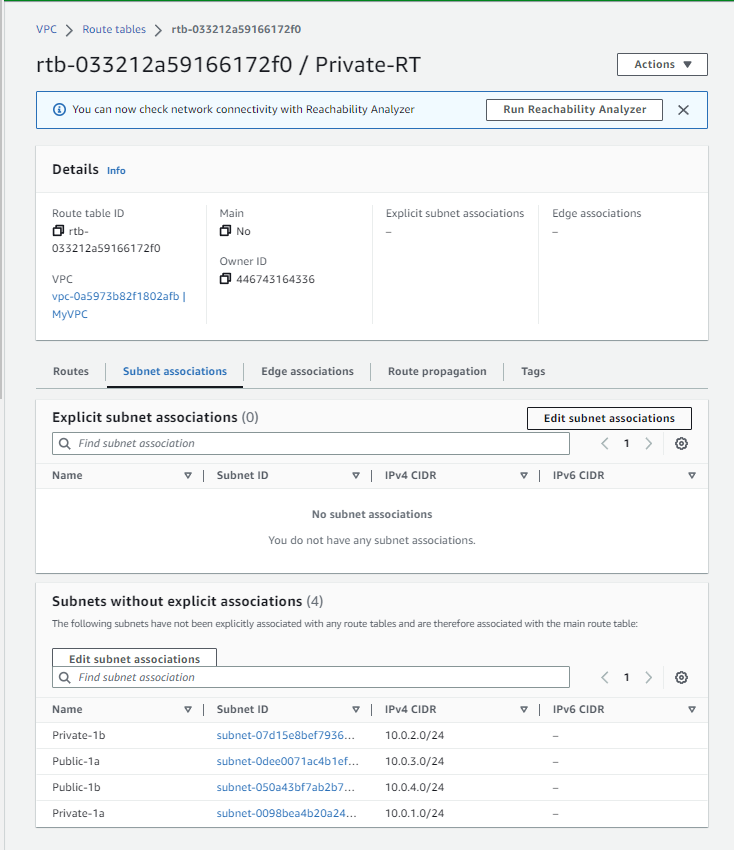
**Figure 8**

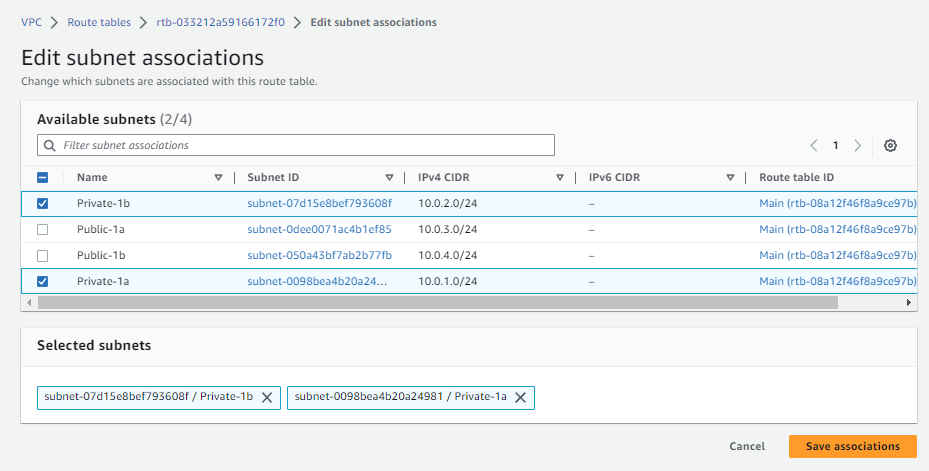
****

**Figure 9**

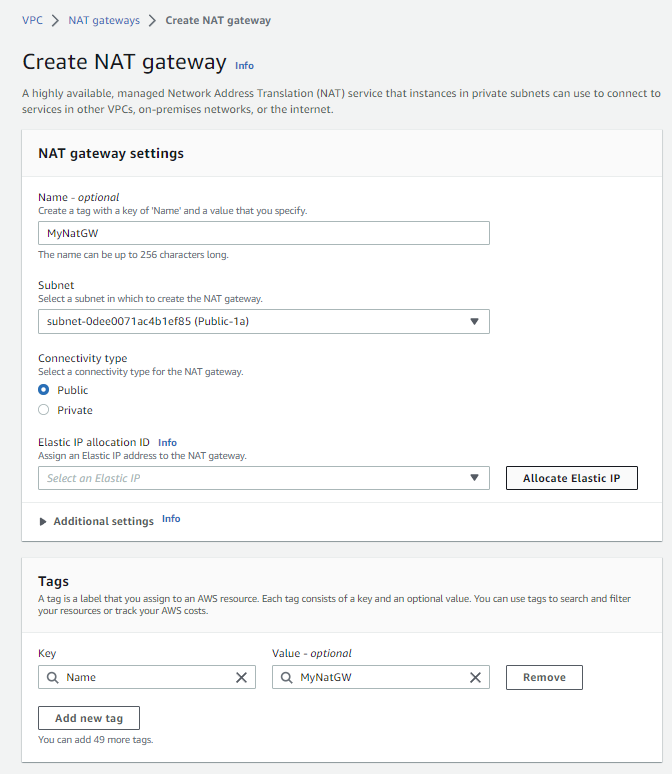
**Step 9:** To route the vpc private subnet separately, select “Route tables” at the left sidebar and click “Create route table” at the right side of your screen. Follow Figure10, 11 and 12 which is provided below.

** Figure 10**

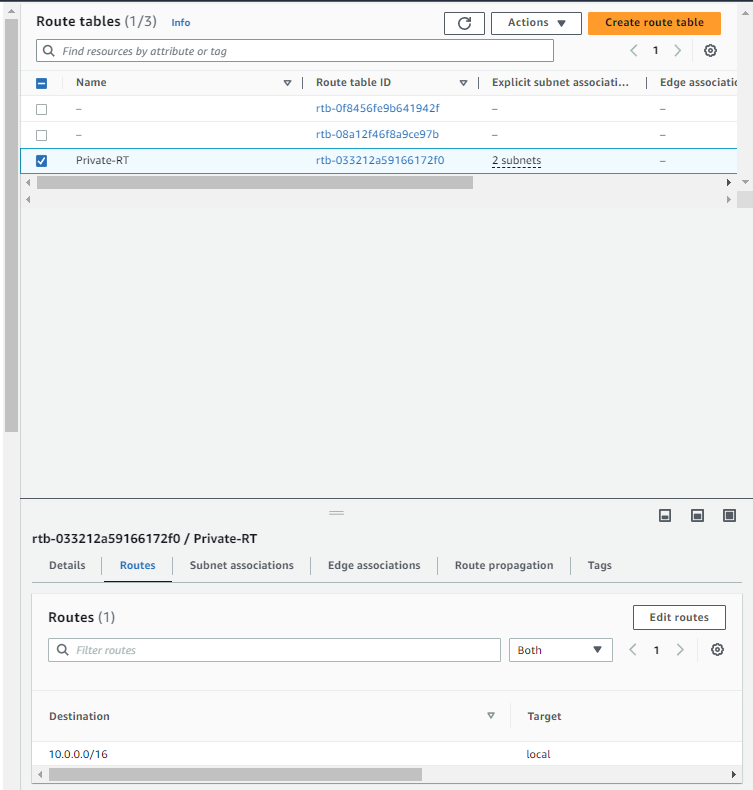
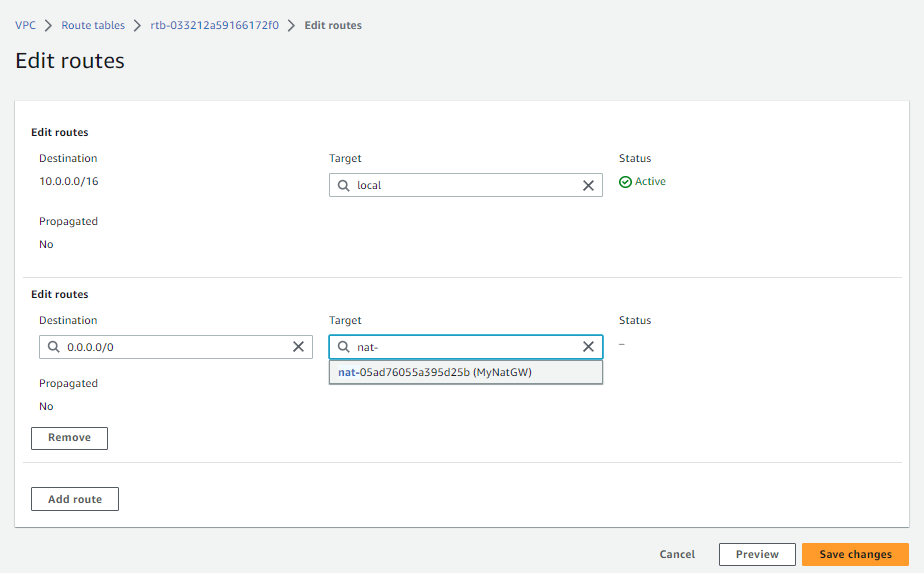
** Figure 11**

** Figure 12**

**Step 10:** to create a NAT gateway for “Public-1a”, select “NAT gateways” at the left sidebar and click “Create NAT gateway” at the right side of your screen. Follow Figure13 which is provided below.

** Figure 13** (Follow and select “allocate elastic ip”, wait for a while and he ip for elastic ip allocation will appear in the box. Click “Create NAT gateway” only after the ip appears)

**Step 11:** To allow Private address to be NAT to any destination, select “Edit routes” at the bottom right after selecting “NAT gateways” at the left sidebar and choose “Private-RT”. Follow Figure 14,15 which is provided below.

** Figure 14 Figure 15**

Reference Video if needed (Create your own):

Video is provided to 🡪 [Create a Custom VPC on AWS](https://youtu.be/AKQ7FdEuWz4)

1. Setup AWS EC2 Instances

**Step 1:** in the search bar at the left of your screen search and select “EC2” amazon services.

**Step 2:** at the left sidebar, scroll down and click on “Network & Security” dropdown button and select “Security Groups” to create 4 Security Groups, name as “SecureWeb”, “SecureDomain” and “SecureBastionHost”, “SecureInternalHost” for “MyVPC” in the VPC box. Inbound and outbound all traffic for now.

**Step 3:** at the left sidebar, click on “Instances” dropdown button and select “Instances” to create five instances. Click on “Launch instances” and name the five hosts as “Bastion Host 1”, “Bastion Host 2”, “WebServer”, “DomainServer” and “Internal Host”. (Refer to Setup AWS Services documentation on how to create a single instance)

**Step 4:** Select “Windows Microsoft” as your Amazon Machine Image Operating System

Under Key pair (login) select “Create new key pair”. Key pair name as “MyKeyPairs”, file format as ‘.pem’. and click “Create key pair”. You will see that a file have been downloaded.

Graphical user interface, text, application

Description automatically generated A picture containing text, rectangle, screenshot, electric blue

Description automatically generated

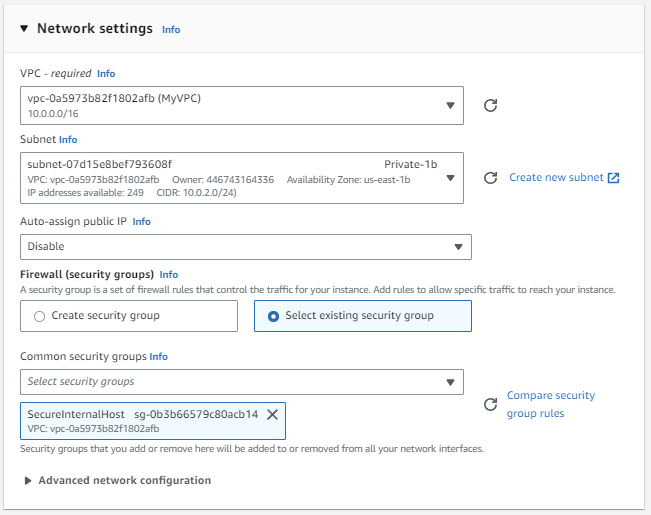
**Step 5:** click “Edit” beside “Network settings” info dropdown

**Step 6:** Select “Select existing security group”. Click on the dropdown button and select “SecureWeb”, “SecureDomain”, “SecureBastionHost”, “SecureInternalHost” security groups for each instances respectively. (Take note of the 4 pictures below to edit the network settings for step 5 and 6)

A screenshot of a network settings

Description automatically generated with medium confidence A screenshot of a network settings

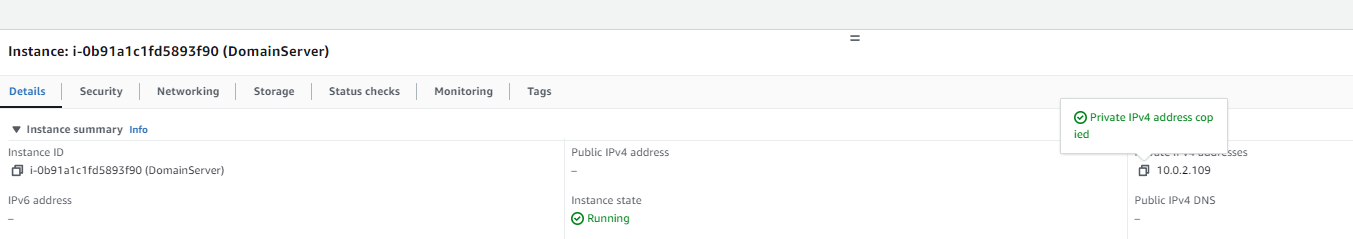
Description automatically generated with medium confidence A screenshot of a computer

Description automatically generated with medium confidence 

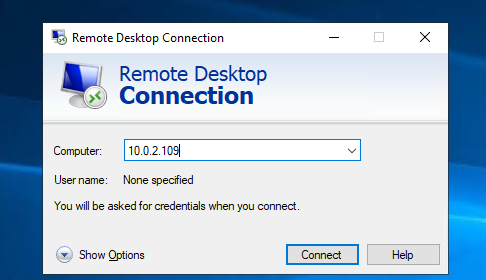
Select “Launch instance” on the right of the screen.

1. Setup Active Directory Domain Controller in Domain Server

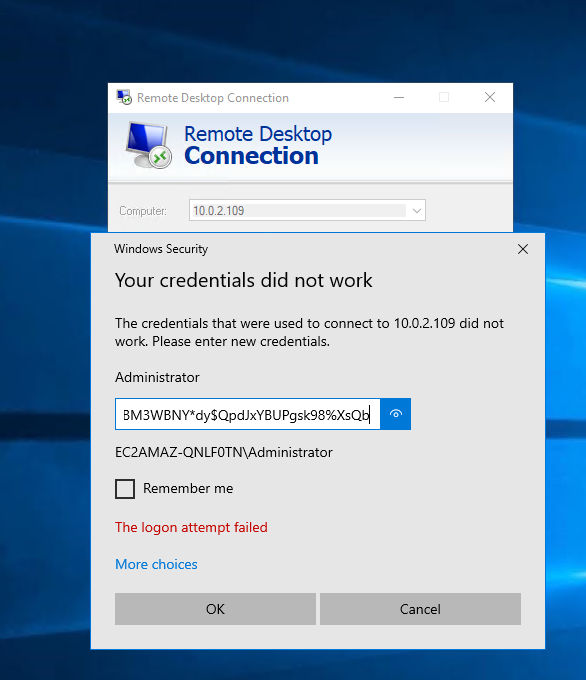
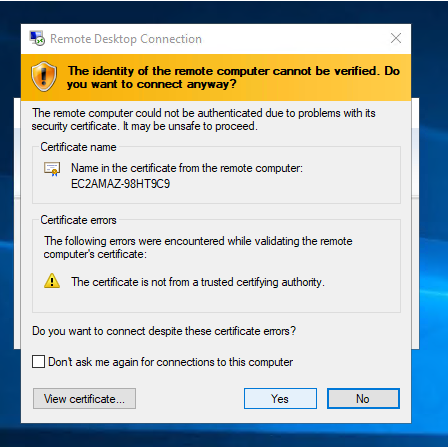
**Step 1:** Login to bastion host 1 and 2 to access domain server and internal host. In bastion host 1 ec2, use Remote Desktop Connection to connect to domain server as Bastion Host is in the same network as Domain Server. Copy the domain server private ip address given in the details of Domain Server EC2 in AWS and input into the box.



And paste in the box and connect



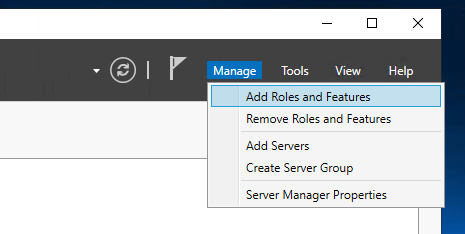
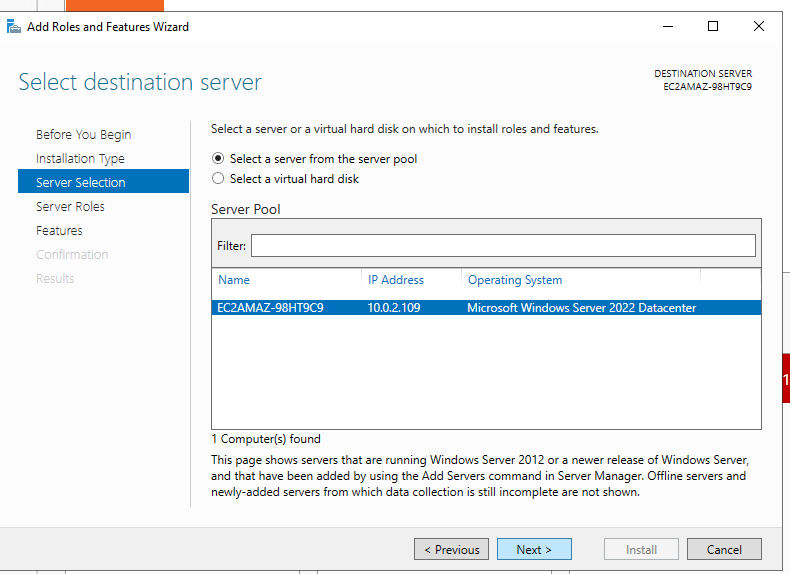
**Step 2:** use the password that is decrypted from the “.pem” key for domain server ec2 and connect by clicking yes afterwards

The bastion host is now in the rdp of domain server



**Step 3:** install AD Domain service by clicking “Add Roles and Features”. In serve role, tick “Active Directory Domain Services”. Follow Figure 16,17,18 which is provided below.

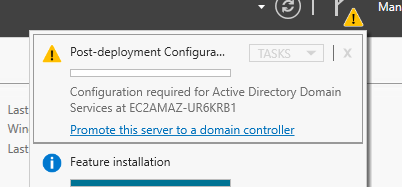
** Figure 16Figure 17**

**A screenshot of a computer

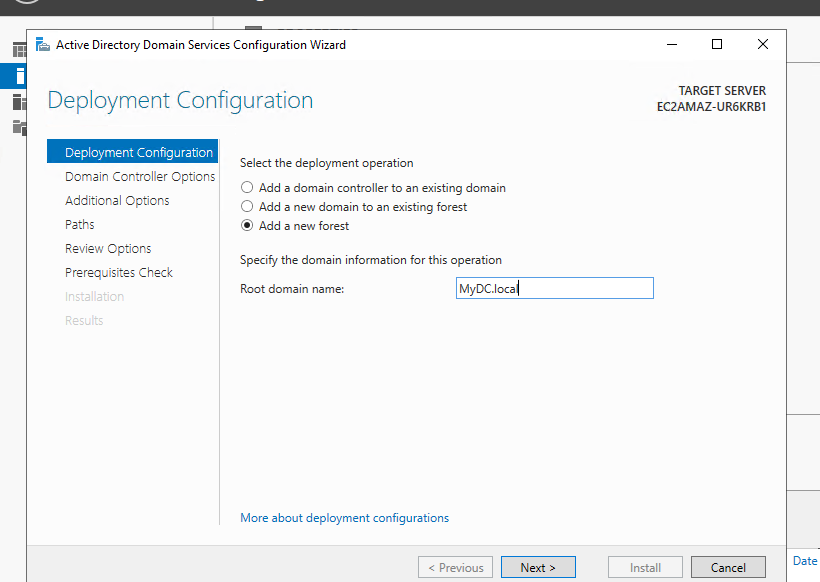
Description automatically generated Figure 18**

Rest of the configuration follow by default and install.

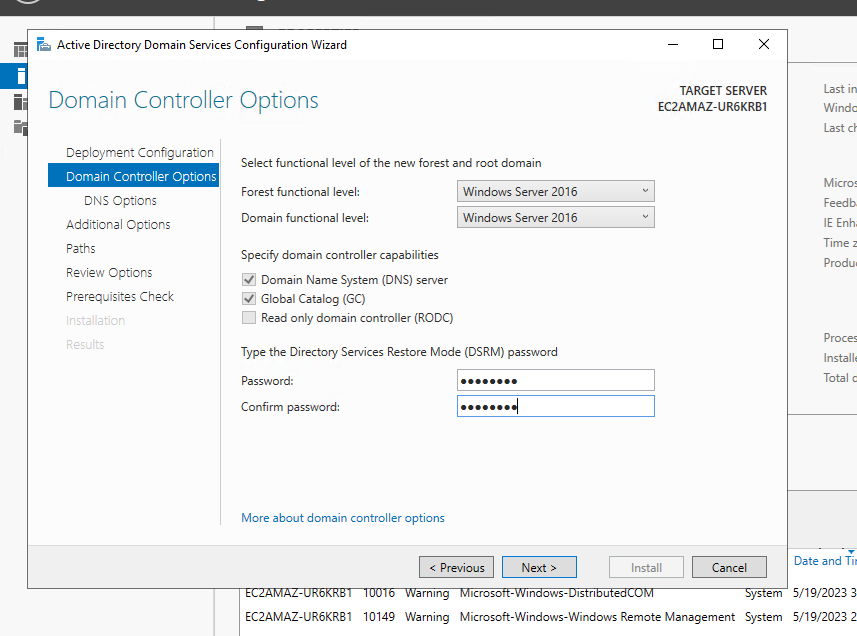
**Step 4:** After installed, navigate to where u see a “warning” sign and select “Promote this server to a domain controller”



**Step 5:** In deployment configuration, select as follows in the picture below



**Step 6:** set your password and select the rest by default and install



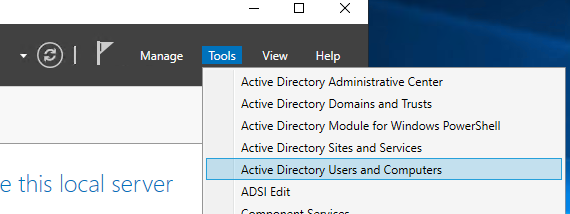
After success installation, the remote desktop connection will log you out automatically. Wait for about 3mins and log back in using rdp again.

Reference Video if needed (Creat your own):

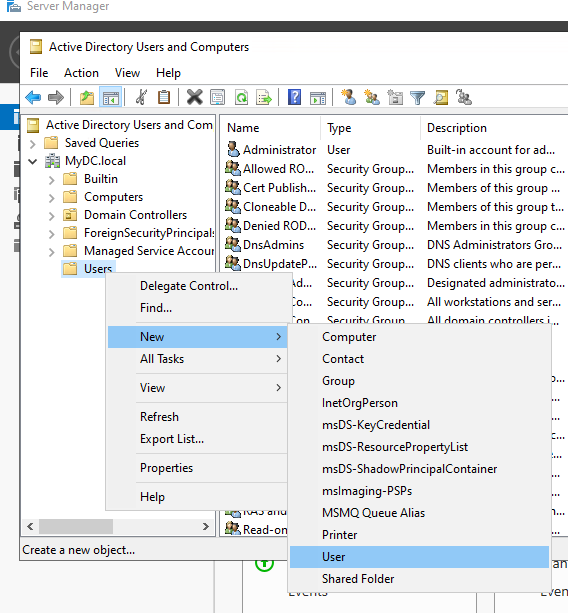
Video is provided to 🡪 [How to Set Up Active Directory in Windows Server 2022 Step by Step Guide #windowsserver2022](https://youtu.be/hfU-uWWIEiQ?t=348)

1. Create different users under the domain

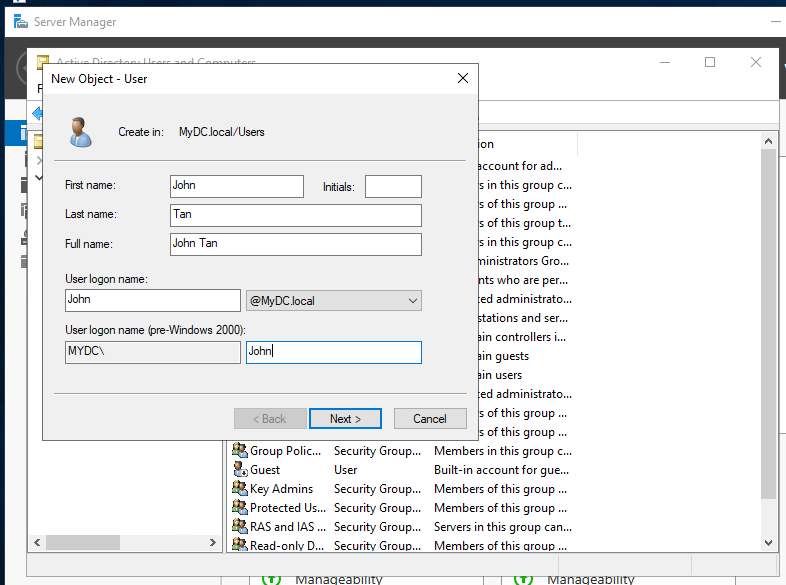
**Step 1:** now we can create user accounts and test them out. Select “AD Users and Computers” in tools dropdown.



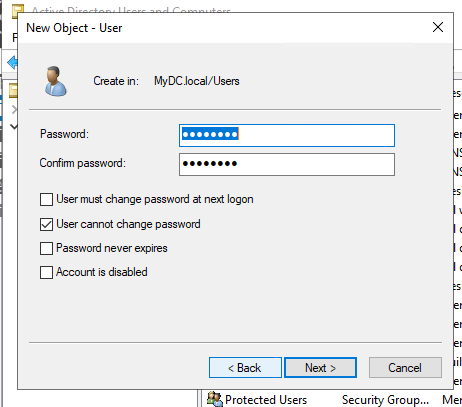
**Step 2:** right click “Users” 🡪 “New” 🡪 “User” to create a user account in “MyDC.local” domain



**Step 3:** create a user name “John”. Follow Figure 19 which is provided below

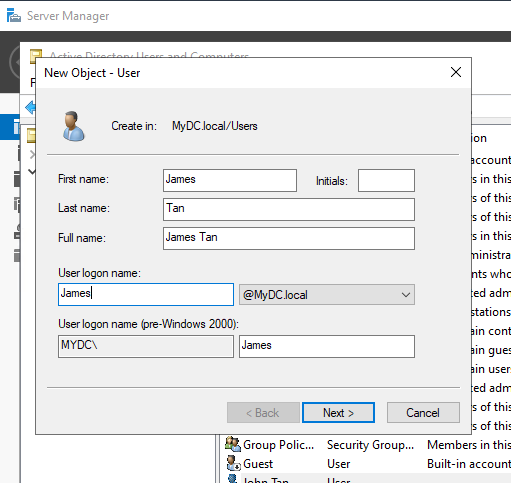
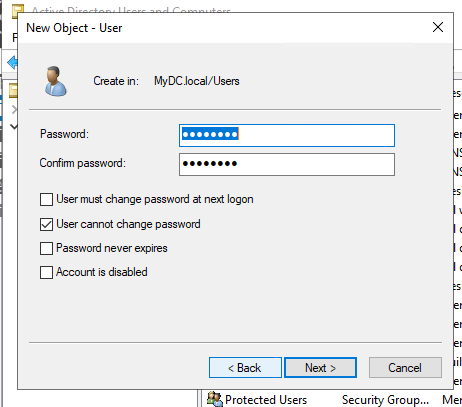
** Figure 19**

**Step 4:** Use “Pa$$w0rd” as the password for that user. And check “user cannot change password”.



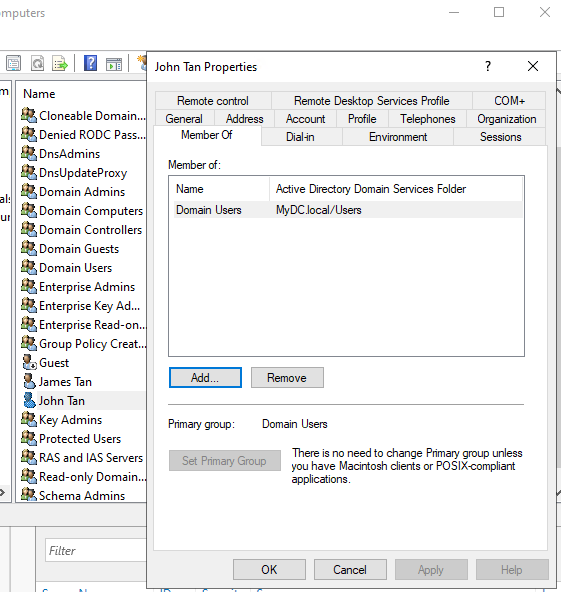
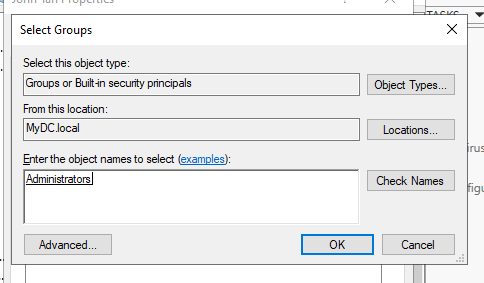
**Step 5:** Press next and click finish

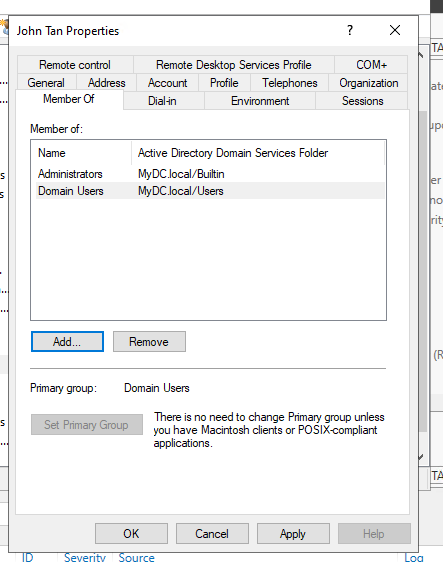
**Step 6:** create another user named “James” and set its password.

**Step 7:** Press next and click finish

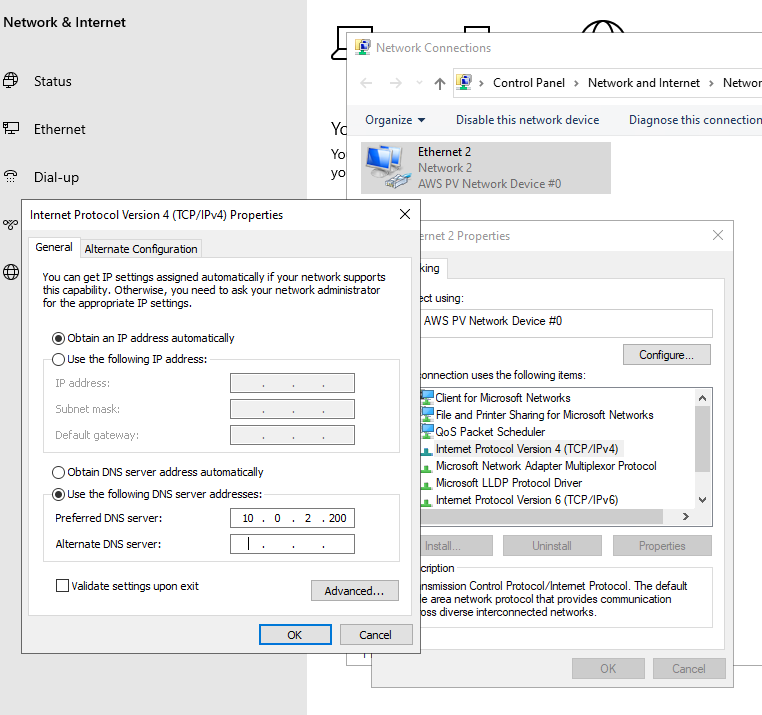
**Step 8:** Make John as an administrator. Right click on “John Tan” 🡪 “Properties” 🡪 “Member Of”. Click “Add…” and add “Administrators”. Click ok and apply and ok. As shown in Figure 20,21,22 below.

** Figure 20  Figure 21**

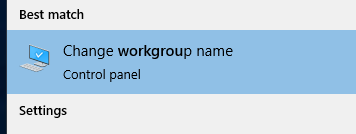
** Figure 22**

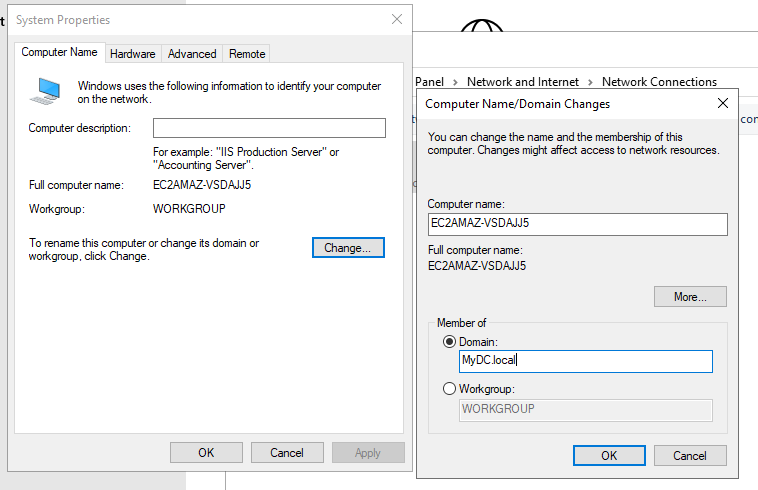
1. Allow client to join Domain Network

**Step 1:** For Internal Host to join Domain, first use Bastion Host 2 and remote desktop connection into Internal Host EC2. Next in control panel, go to “Network and Internet” 🡪 “Network Connections” and right click “Ethernet 2” 🡪 “Properties” 🡪 find “Internet Protocol Version 4 (TCP/IPv4)” and click properties to edit its DNS Server to the Domain Server ip address “x.x.x.x” and click “ok” two times.

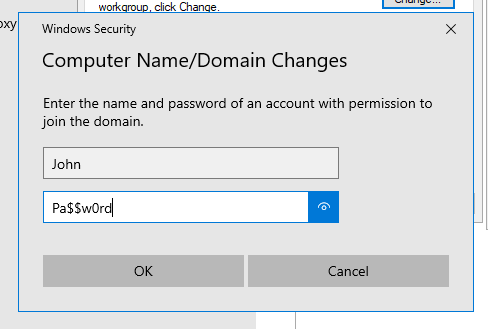
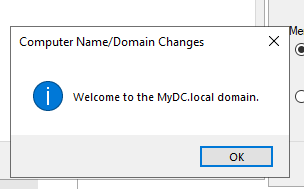
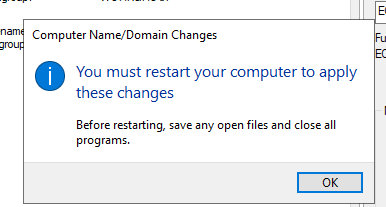
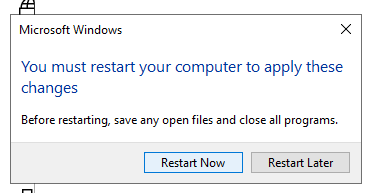


**Step 2:** In the windows search, search for “Change workgroup name”. Click “Change…”. Under Member of, select “Domain” and enter “MyDC.local” in the textbox. And click “ok” two times.



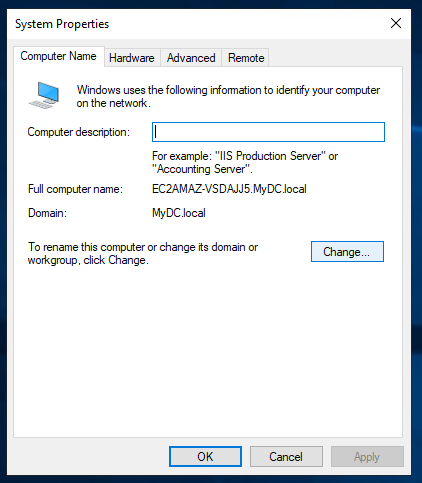


**Step 3:** a pop up will appear to prompt you to enter one of the domains serves username and password for confirmation. In this case, we will use user “John Tan” which we had set as an Administrator. Click “ok” three times and click “Restart Now”.

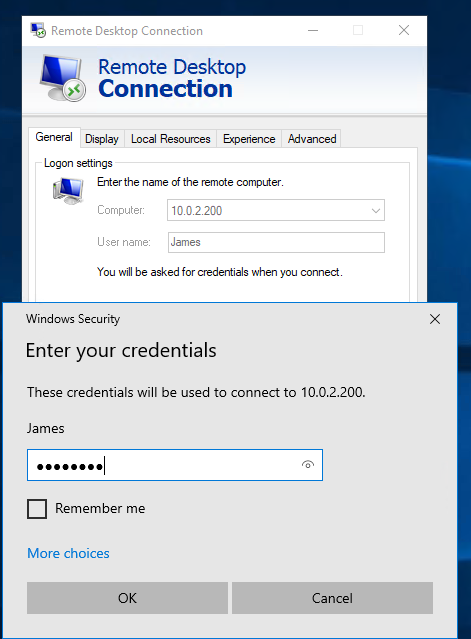
Here, it will close the rdp connection by itself. Wait 3mins and rdp into Internal Host again.

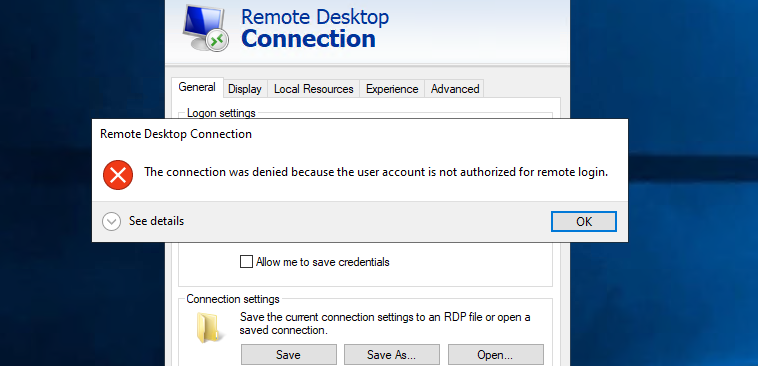
**Step 4:** Go back to the change workgroup. Notice now that u are in the domain already.



1. Allow RDP Connection on user logon

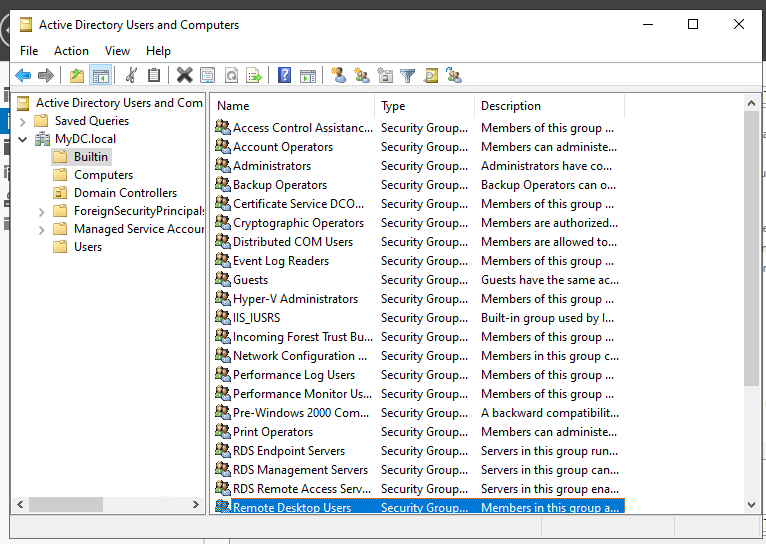
**Step 1:** Try to log in to one of the account, like “James Tan” by sign in out and go to rdp and follow figure 23

** Figure 23**

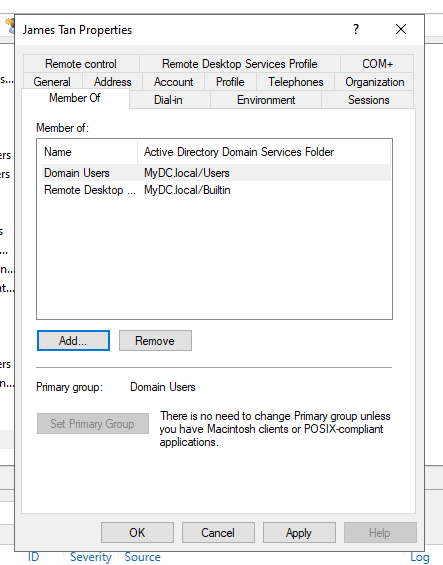


Notice that a pop out appear prompting you that the connection was denied because that account is not authorized.

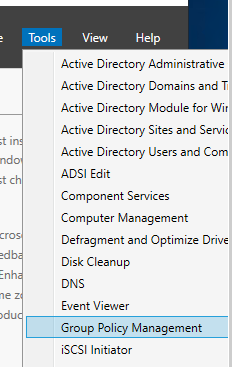
**Step 2:** To allow rdp, go to builtin tabs, u can see the security groups that are available by default



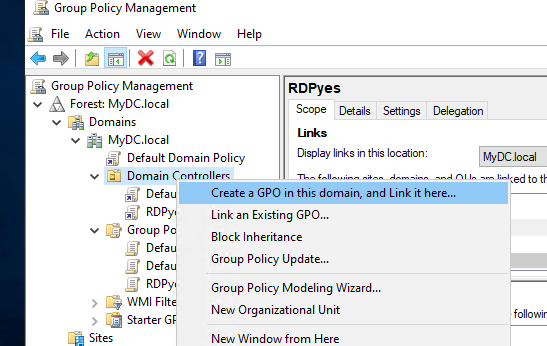
**Step 3:** Go back to James Tan properties and add in “Remote Desktop User” security group



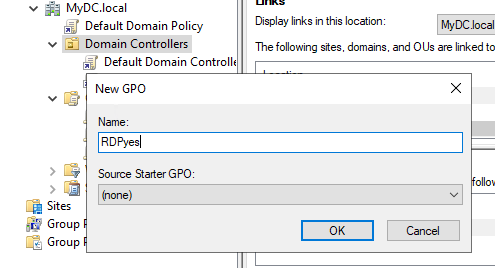
**Step 4:** Select “Group Policy Management” under “Tools” dropdown



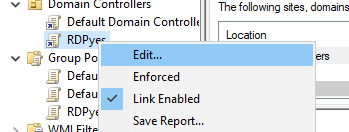
**Step 5:** select “Forest: MyDC.local” 🡪 “Domains” 🡪 “MyDC.local” and right click “Domain Controllers” 🡪 “Create a GPO in this domain, and link it here…”



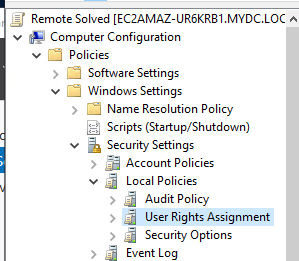
**Step 6:** to create a group policy, under name input “RDPyes” and click ok



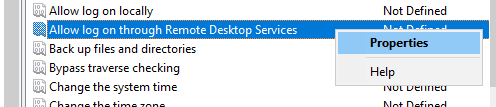
**Step 7:** right click “RDPyes” 🡪 “Edit…”



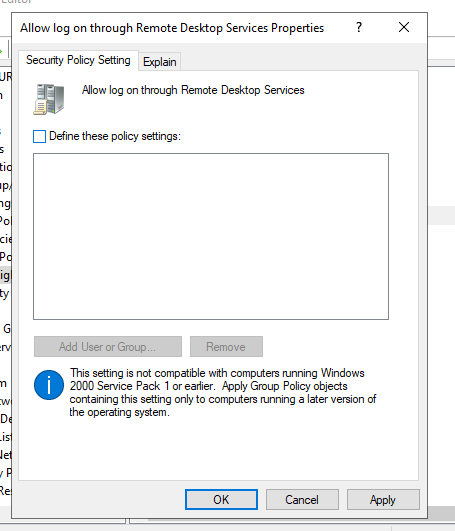
**Step 8:** a windows appear similar to Figure 24 below. Select “Computer Configuration” 🡪 “Policies” 🡪 “Windows Settings” 🡪 “Security Settings” 🡪 “Local Policies” 🡪 “User Rights Assignment”

** Figure 24**

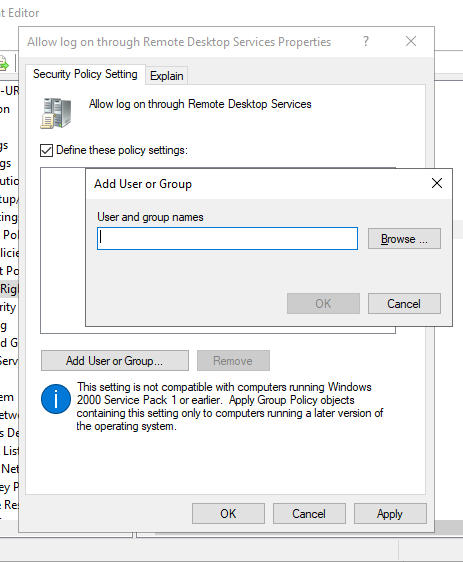
**Step 9:** find “Allow log on through Remote Desktop Services” right click select “Properties”



**Step 10:** to enable “Add User or Group” button, check the “Define these policy settings” checkbox

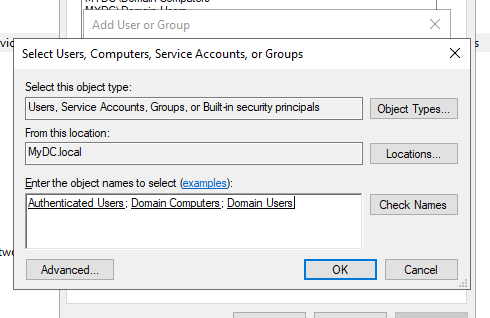


**Step 11:** after clicking “Add User or Group”, a pop up appears. Select “Browse”

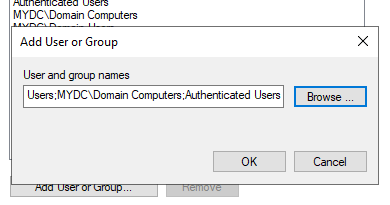


**Step 12:** find “Authenticated Users”, “Domain Computers” and “Domain Users” and click ok

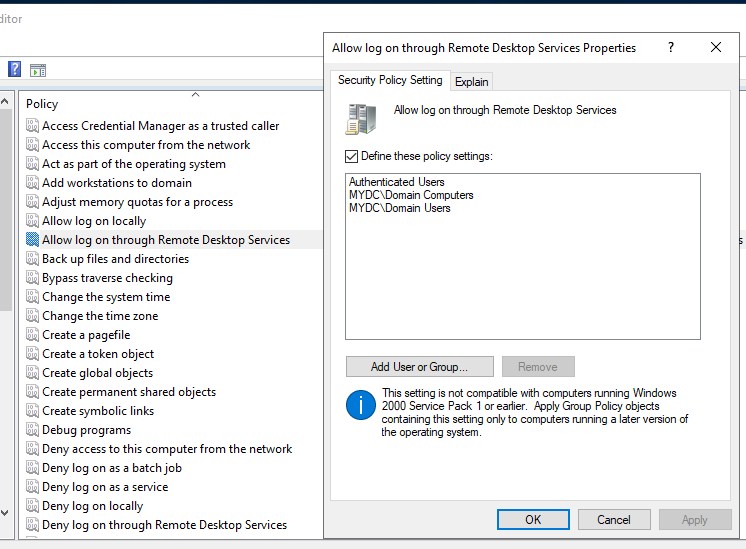
Browse



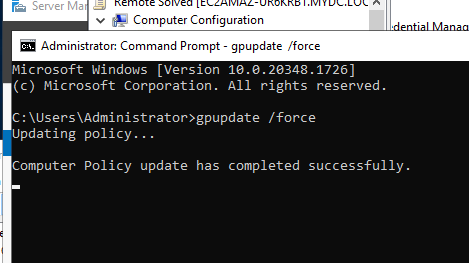
**Step 13:** click ok after the textbox is filled



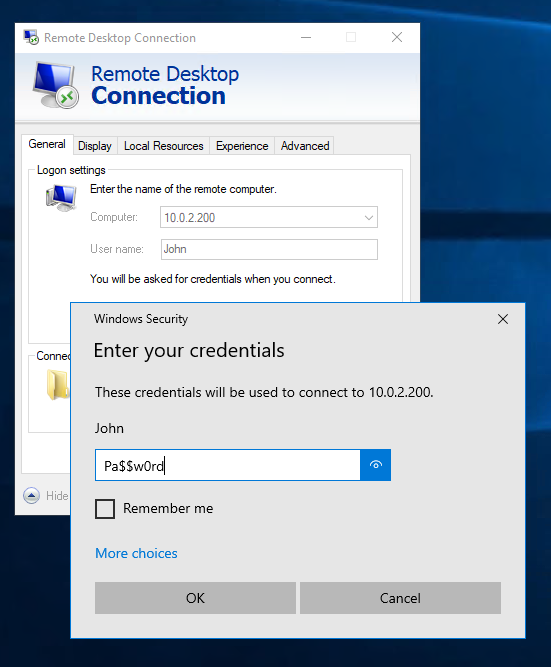
**Step 14:** click Apply and ok



**Step 15:** open Command Prompt as Administrator and type “gpudate /force”



After the message in the command prompt showing that the policy have been updated successfully, now try again to login in from internal host you will see that it is successful



Reference Video if needed (Creat your own):

Video is provided to 🡪 [How to create user in active directory and join a domain](https://youtu.be/NkeplvBcjXE)

A screenshot of a computer

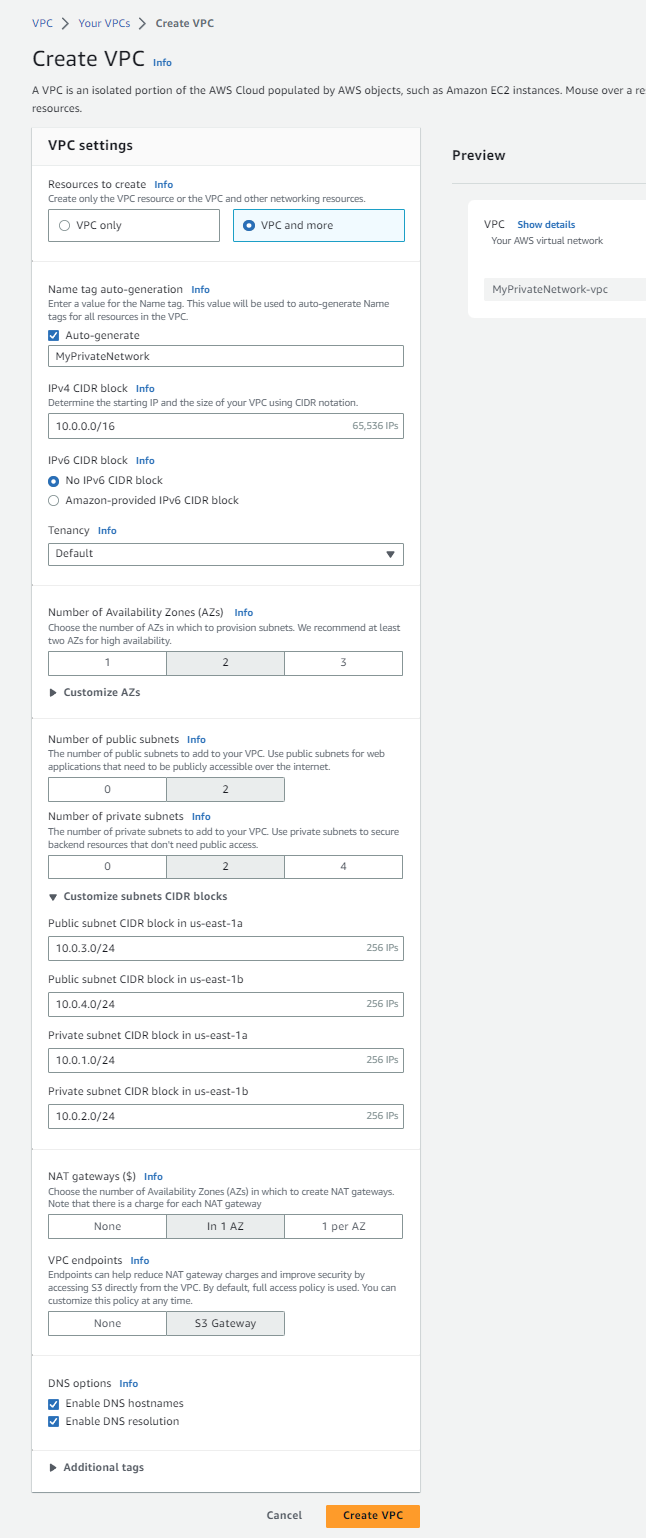
Description automatically generated

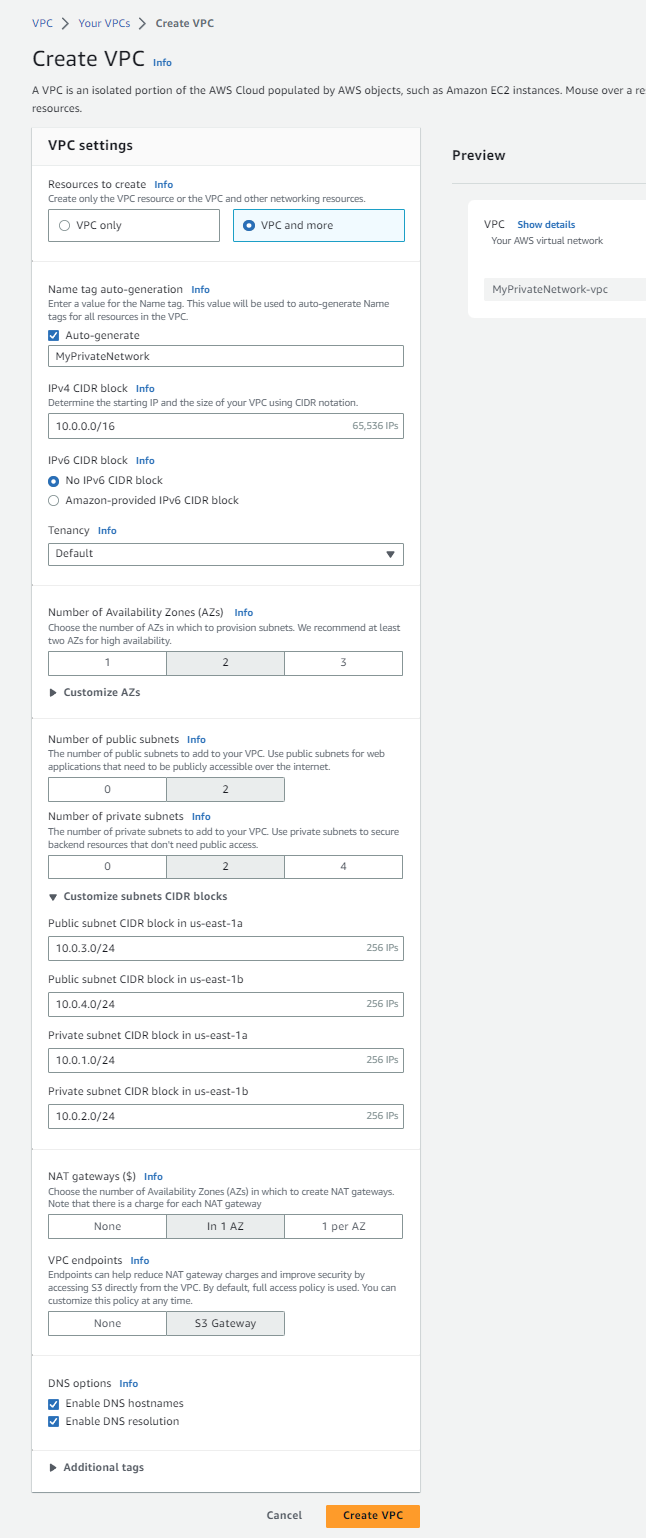
A screenshot of a computer

Description automatically generated

After the route is created, Click on “Edit subnet associations” at the middle right of the screen and save associations.

Step 1: First go to VPC and create one





A screenshot of a computer

Description automatically generated with medium confidence

