****

**Cloud Computing**

**MCQ Questions:**

**1**.- A VPC peering connection is a networking connection between two VPCs that enables you route traffic between them using private IPv4 addresses or IPv6 addresses. Following is correct with regards to VPC peering: -

1. Instances in either VPC can communicate with each other
2. EFS can be used for common file sharing
3. Can create a VPC peering connection between your own VPC, or with a VPC in another AWS account
4. Amazon’s Content Delivery Network (CDN)

**2**.- Following security standards are not relevant to Amazon Cloud security: -

1. IPSec
2. PCI DSS Level 1
3. ISO-27001
4. RFC 1918

**3.-** Security group is a virtual firewall that works at ENI level. This is achieved by configuring following services: -

1. Stateful permit rules
2. Auto Scaling
3. Lambda

****

**4** – CloudFront is Amazon’s distributed global content delivery network (CDN). Following doesn’t form part of this service: -

1. Edge location
2. Origin
3. Distribution
4. Groups

**5.-** Principal is an IAM entity which interacts to AWS resources. Following is not considered as principal: -

1. MFA
2. Tag
3. Group
4. Roles/temporary security tokens

**6**.- File storage stores the files in hierarchical structure of directories. Main application of file storage includes: -

1. NAS
2. SAN
3. DAS
4. None of these

**7.-** Storage classes (S3) not suitable for data archiving are: -

1. S3 Standard
2. S3 Glacier
3. S3 - IA
4. S3 Glacier Deep Archive

****

**8**.- Following services are not provided by BIG-IP F5 Local traffic manager: -

1. Backup and restore
2. Programmable L7 loading balancing
3. Anti-DDOS
4. L4 Firewall

**9**.- Fusion Cloud is brand name for Huawei cloud computing solutions. Following doesn’t form part of Fusion Cloud: -

1. Fusion Access
2. OceanStore
3. Fusion Insight
4. Fusion Sphere

**10**.- How many types are available in azure subscriptions: -

1. 2
2. 4
3. 3
4. None of these

**11**.- from which option user can assign license for mailbox: =

1. Office365 console
2. Azure portal
3. None of these
4. By default license’s are assigned

**12**.- which of the storage type is used in storage account: -

1. Blob storage
2. SQL storage
3. Cosmos Database
4. Simple storage

**13**.- Apps in licenses of office365 are: -

1. 12
2. 16
3. 28
4. 26

**14**. - To create vm’s in Hyper-V virtualization minimum processers cores are required.

1. 8
2. 6
3. 4
4. 2

**15**. – Which portal is used to authorized the users to login with cloud credential.

1. Office365
2. Azure AD
3. Local server
4. Active directory domain services

****

Date: 19 November 2023 Time: 2-Hours

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Marks: 80

**Part 2 (Lab)**

**Q.1:** Build below virtual private cloud (VPC) using AWS free tier. You may choose Region/Availability zones of your own choice. Essential requirements for different subnets are as under: -

a. **Subnet 1 (Public):**

(1). Build one EC2 instance (windows server 2019 based) and ensure that it is accessible from Internet.

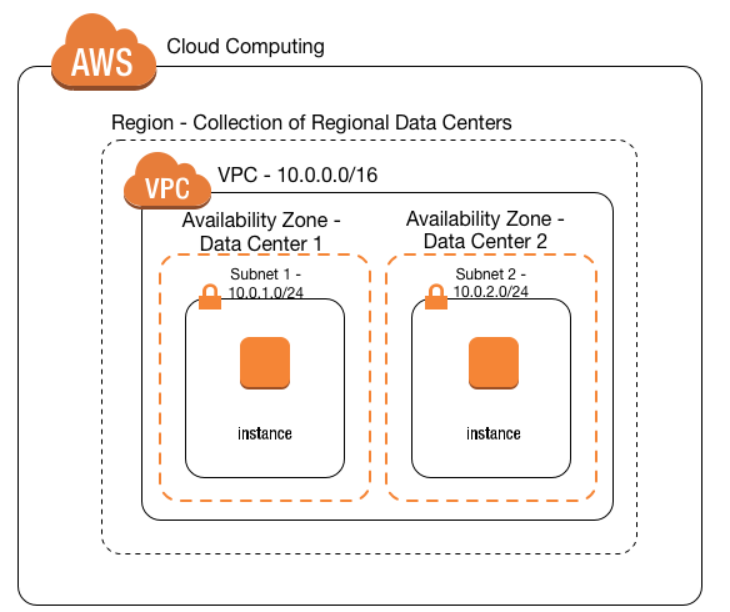
(2). You can add essential components needed to achieve your task.

b. **Subnet 2 (Private):**

(1). Build one EC2 instance (Linux based).

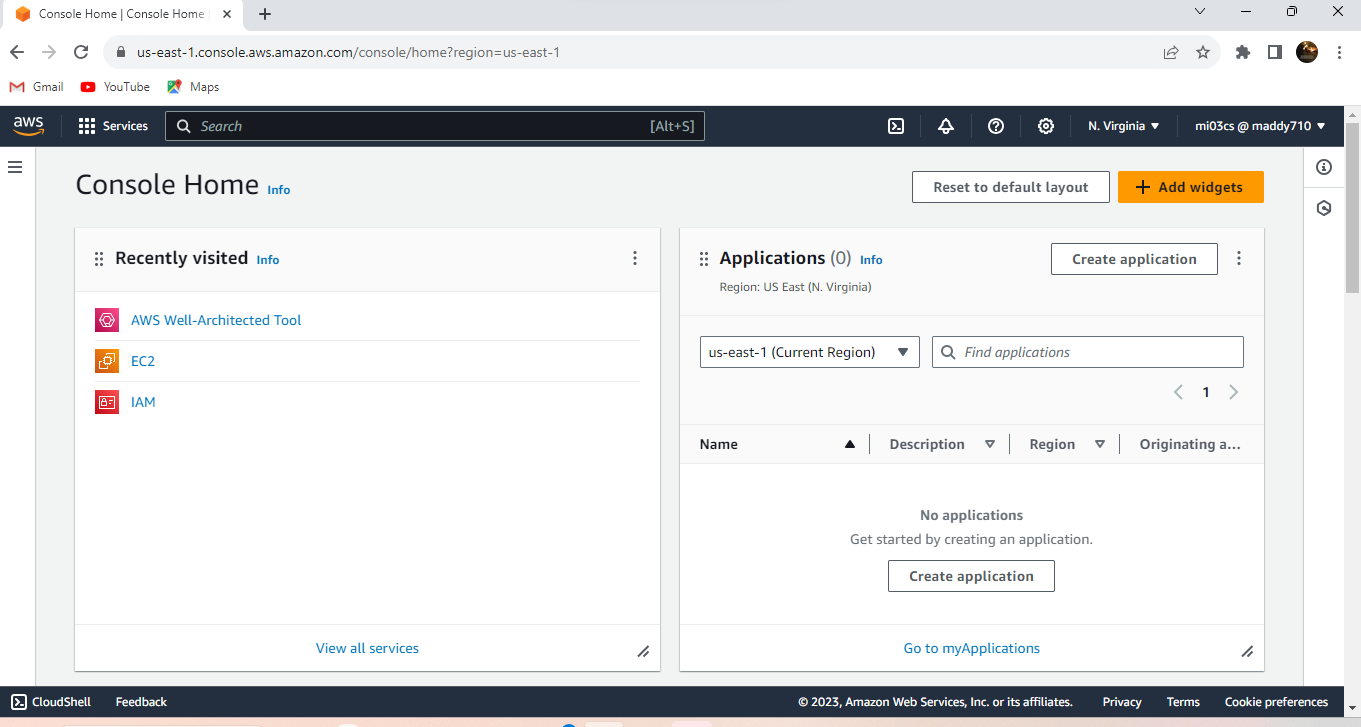
(2). Ensure that there should be any internet reachability.

(3). You may configure essential components required to achieve your requirement.



**Answer**

Login to aws managment and sing in as a iam user and come to the dashboard of aws.



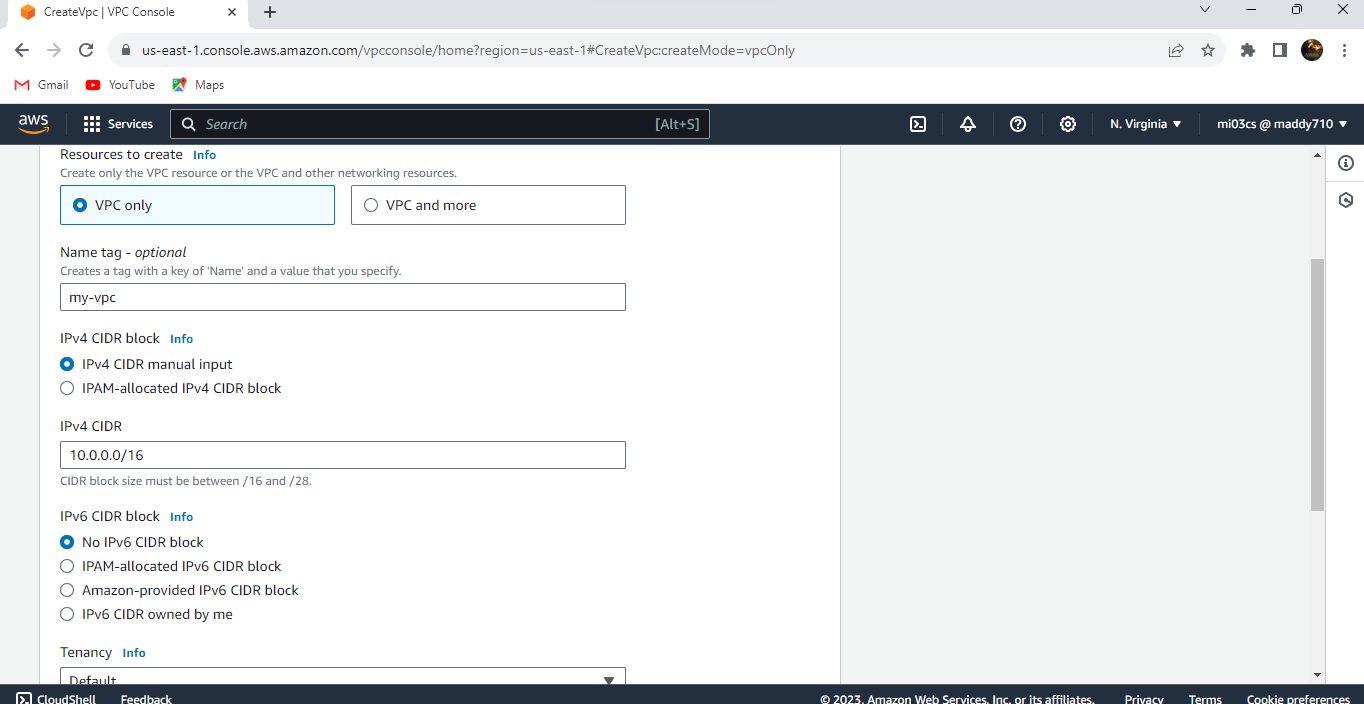
**Steps**

1-Create a vpc in aws concole in any region or in any availability zone.

2-Enter vpc name e.g my-vpc

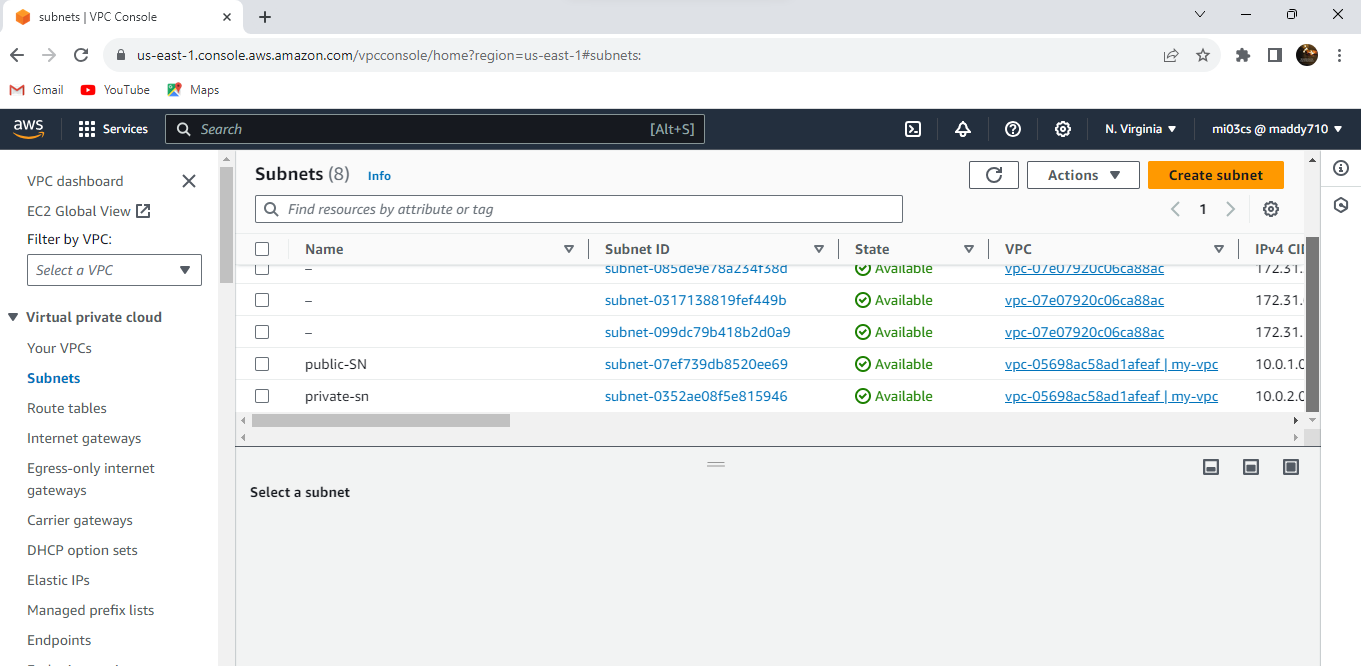
2-give ip to vpc (10.0.0.0/16)

3- Don’t change Tenancy saty it as default .

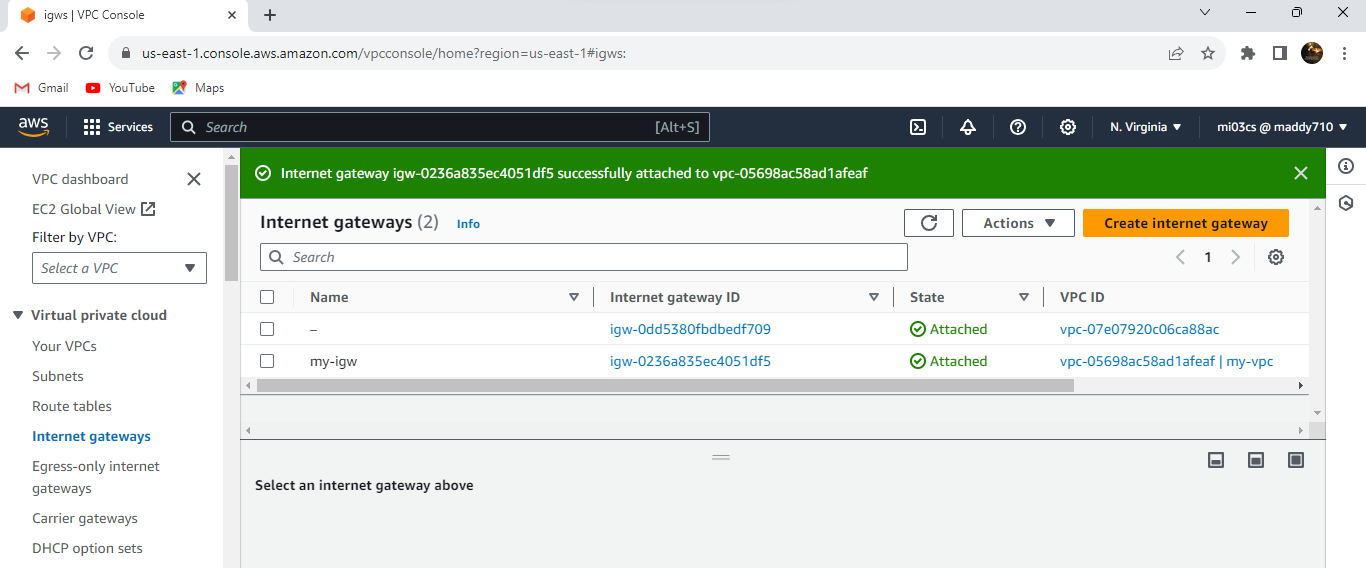
****

4- Create subnet 🡪 move to subnet dashboard and create subnet name public-sn subnet🡪choice the vpc that created in previous step🡪 select a availability zone 🡪enter a subnet🡪(10.0.1.0/24)🡪create subnet

5- Follow the same steps as above for creating a subnet, but choose a different CIDR block (e.g., 10.0.2.0/24) and a different name (e.g., Private-sn).

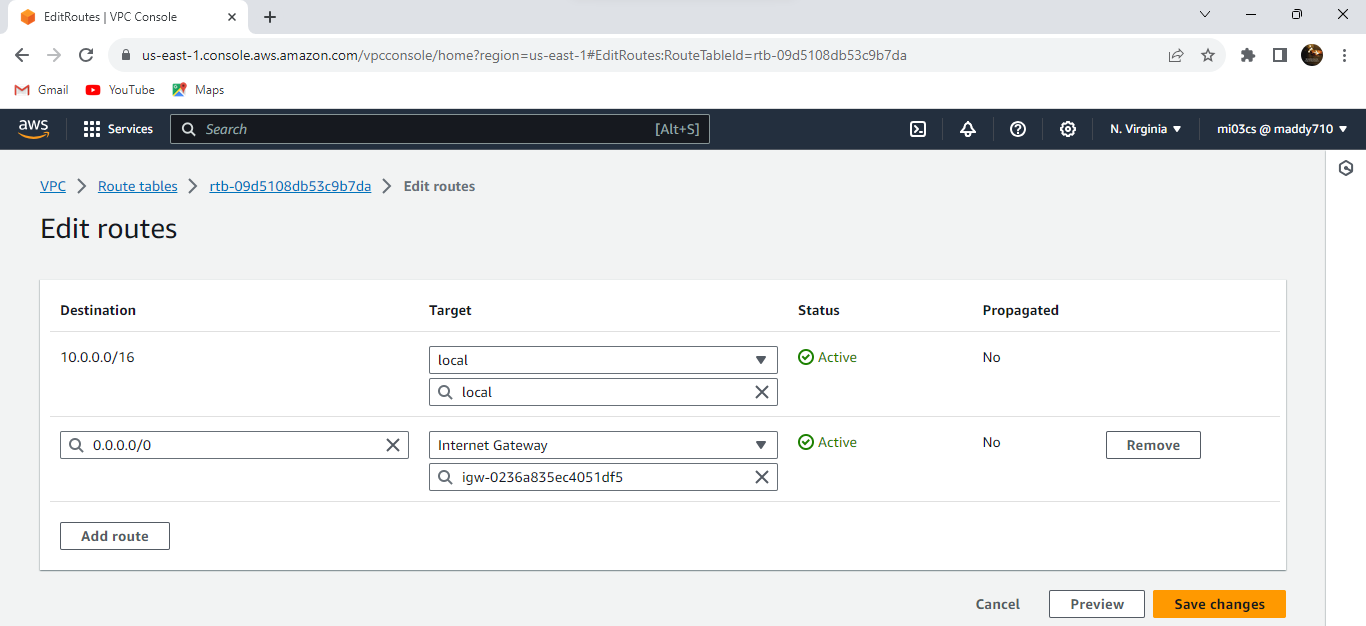


6- Now go to internet gateway and create a internet gateway🡪 name (my-igw)🡪 create gateway🡪 attach to vpc that was created in previous steps .



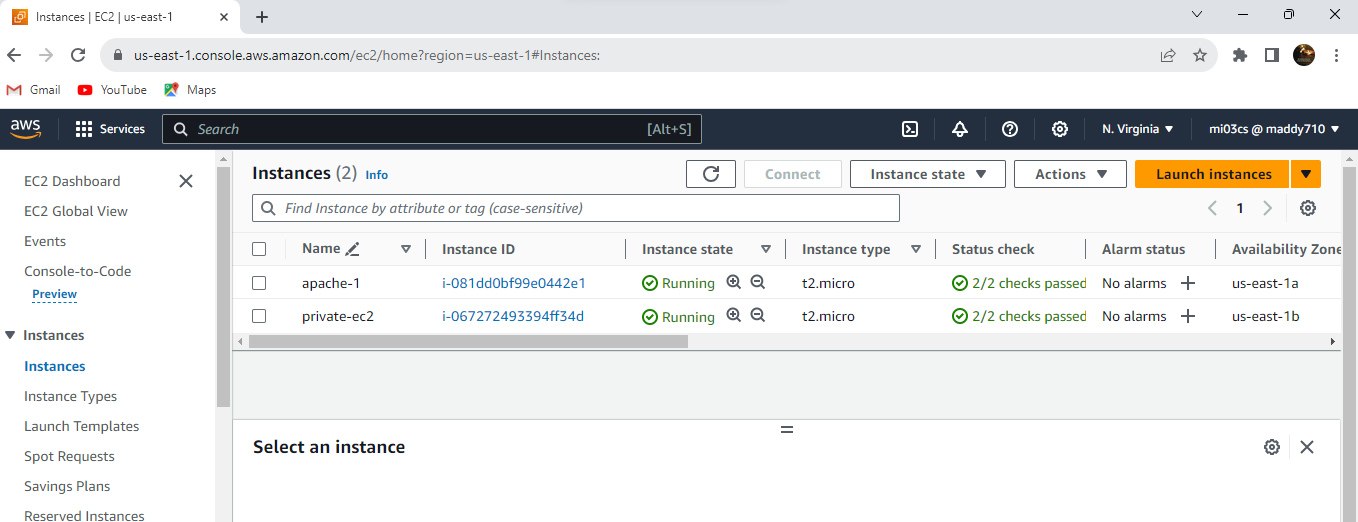
7- Go to route table tab and create a route table name public-rt🡪select vpc 🡪 create route table 🡪 select created route table and associate it with public subnet🡪Then 🡪 create a new route table name private-rt🡪select vpc 🡪 create route table 🡪 select created route table and associate it with private subnet.

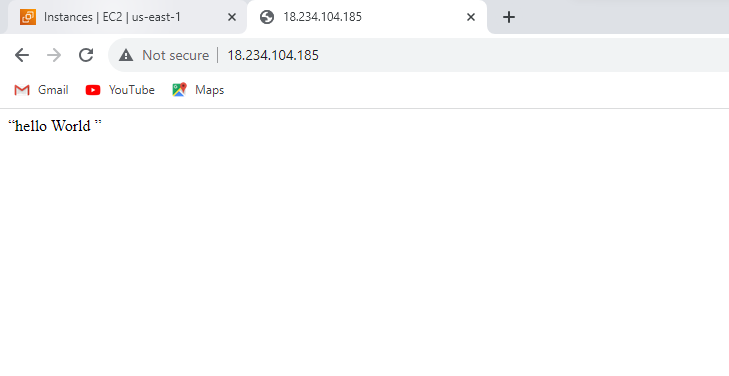
8- Edit the main route table and add a route: - Destination: 0.0.0.0/0 - Target: Choose the internet gateway created in the previous step.



9- Create an ec2 instance🡪go to ec2 dashboard 🡪 launch Instance🡪Select t2 micro instance type🡪 select your created vpc 🡪select public subnet-🡪add a security group and allow ssh any where to access it through mobaxterm.

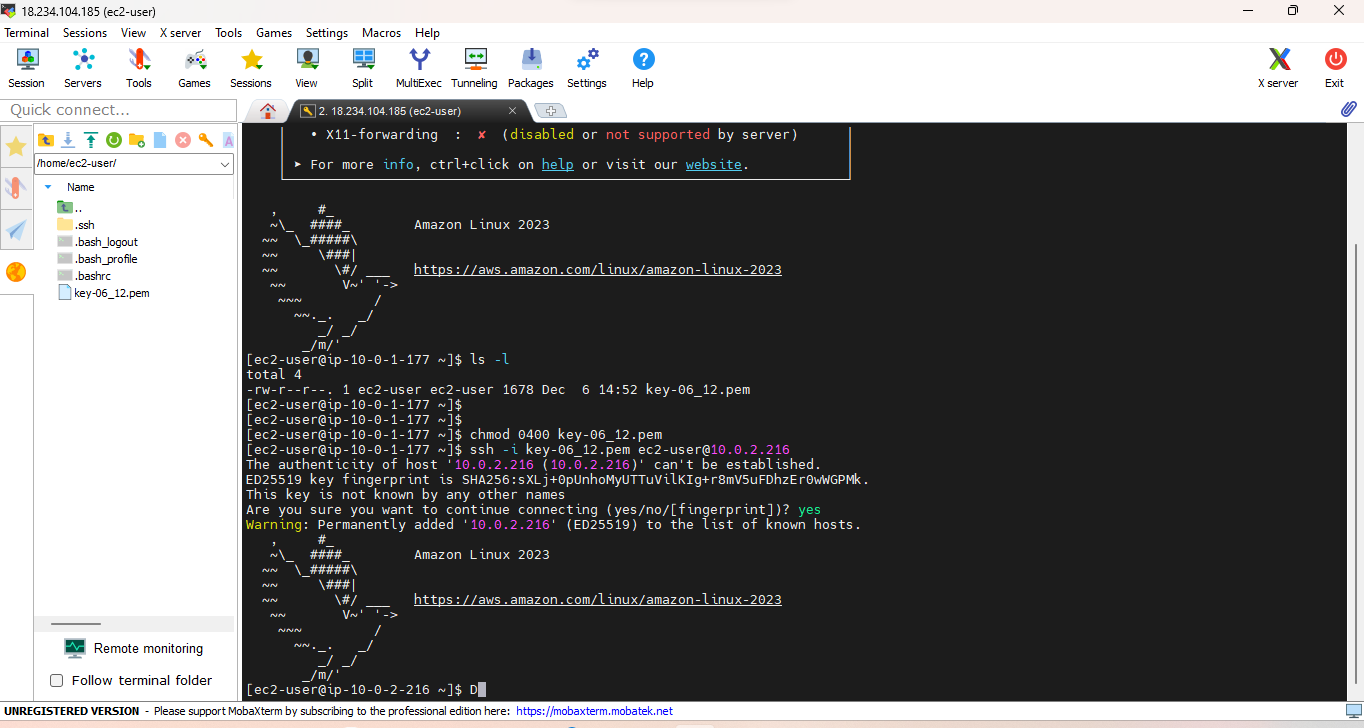
Create another ec2 instance name private-ec2🡪 instance t2 micro 🡪 choose your created vpc and private subnet🡪select security group that was selected by public subnet ec2 to access it or for a baston host.



9- check the public ip machine online with appache server 

10- Go to mobaxterm 🡪 session 🡪 start new session🡪 give public machine ip 🡪username (ec2-user) 🡪 advance setting 🡪 upload key that was created at time of creation 🡪 ok

Machine accessed 🡪 upload private-ec2 key and change its permissions using command (chmod 0400)🡪 now type the command to access the private-ec2 key (ssh -i key-06-12 [ec2-user@10.0.2.216](mailto:ec2-user@10.0.2.216)) 🡪 press enter 🡪 type yes 🡪 your private machine accessed through public machine in a with different availability zone .



Lab Performed

Q 2: Build the azure virtual machine in one private VNET and migrate it to other private VNET In same zone or different zone .

I do not have azure account my account are expire so I am sorry I can not take screen short of azure lab but I can write down the steps of lab below here according to virtualization.

**Steps**

1.Prepare the Source VM: Stop the VM:\*\* Ensure the VM is in a stopped (deallocated) state before proceeding with the migration. –

2-Move or Copy Data (if applicable):\*\* - If your VM relies on data stored locally, you may need to move or copy the data to a shared location or Azure Storage, depending on your use case.

3. Capture VM Image (Optional):\*\* - If you want to create a custom image of the VM, use the Azure CLI or PowerShell to capture the VM image. ```bash az vm deallocate --resource-group --name az vm generalize --resource-group --name az image create --resource-group --name --source ```

4. Remove VM from Source VNet:\*\* - Navigate to the Azure Portal. - Deallocate and deallocate the VM (if not already done). - In the VM settings, navigate to "Networking" and remove the NIC from the source VNet.

5. Delete or Keep Resources (Optional):\*\* - Depending on your requirements, you can either delete the VM, keep the disks, or deallocate and deallocate the VM for later use.

6. Create VM in Destination VNet:\*\* - Navigate to the Azure Portal. - Create a new VM in the destination VNet. - Use the captured image or create a new VM with the desired configuration.

7. Configure Networking:\*\* - In the VM settings, navigate to "Networking" and attach the NIC to the destination VNet.

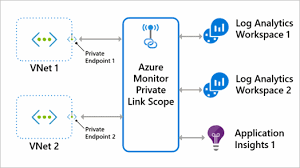
8. Start the VM:\*\* - Start the VM in the destination VNet.

9. Verify Connectivity:\*\* - Ensure that the VM in the new VNet is functioning correctly. - Test network connectivity, and update DNS or other configurations if necessary.

**Lab Performed**

**Q 2:** Build the azure virtual machine in one private VNET and migrate it to other private VNET

In same zone or different zone.



**Answer**

Sure, I can guide you through the process of creating an Azure Virtual Machine (VM) in one private Virtual Network (VNET) and then migrating it to another private VNET, either in the same availability zone or a different one.

Here are the steps:

**Step 1:** Create the Initial Virtual Machine and Virtual Network

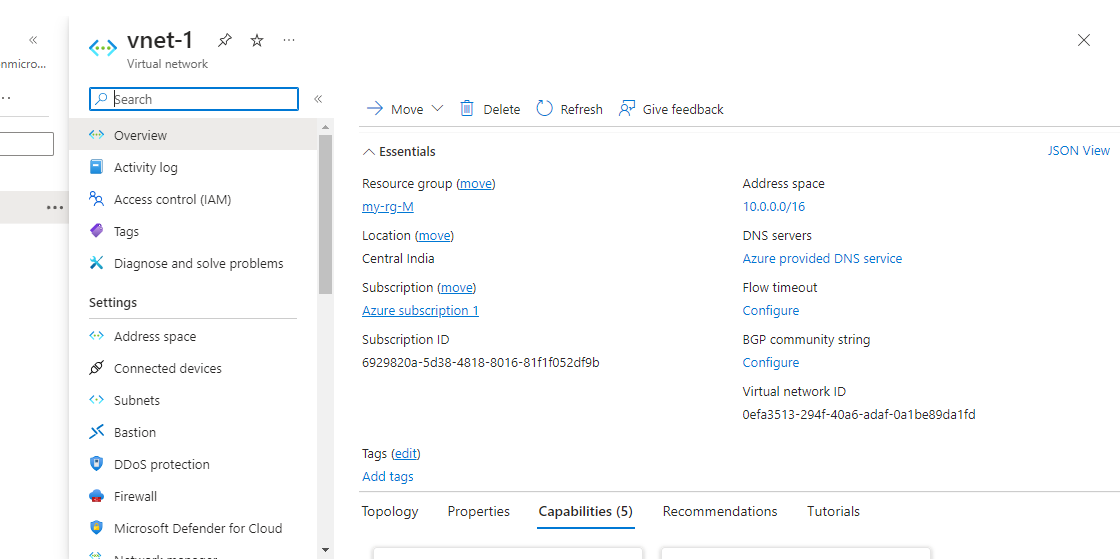
1.1. Sign in to Azure Portal

- Navigate to the [Azure Portal](https://portal.azure.com/).

1.2. Create a Virtual Network (VNET)

- Go to "Create a resource" > "Networking" > "Virtual network."

- Set up the necessary configurations for your VNET, including address space and subnets.

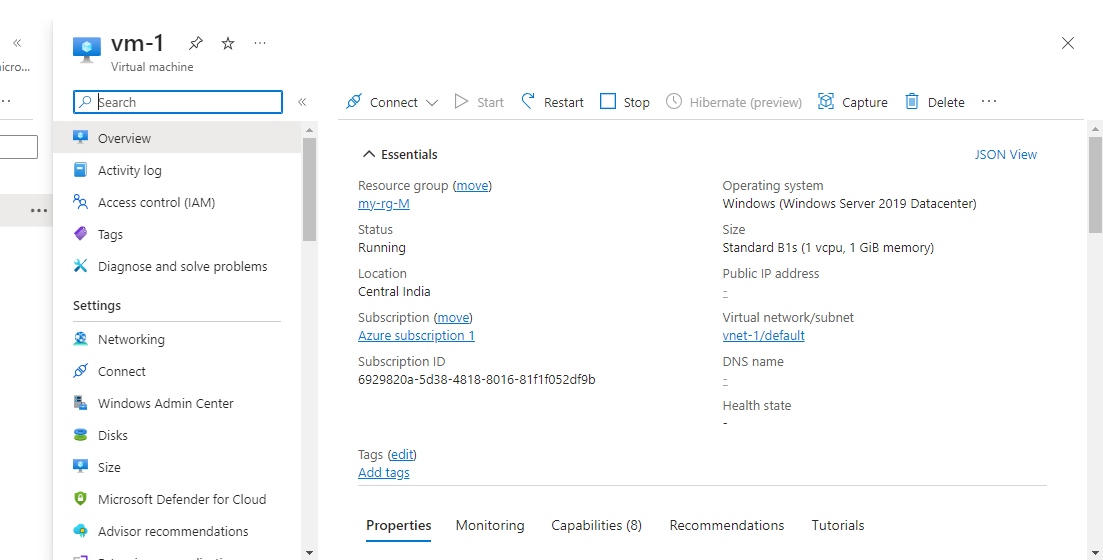


1.3. Create a Virtual Machine

- Go to "Create a resource" > "Compute" > "Virtual machine."

- Configure the VM settings, including the operating system, size, authentication, and networking.

- Select the VNET you created in step 1.2.



**Step 2:** Prepare for Migration

2.1. Review VM Configuration

- Ensure that you have documented the VM configuration, including OS settings, disk configurations, and any additional settings.

2.2. Back Up Data

- If necessary, back up any data on the VM to ensure you don't lose important information during the migration.

**Step 3:** Capture VM Image

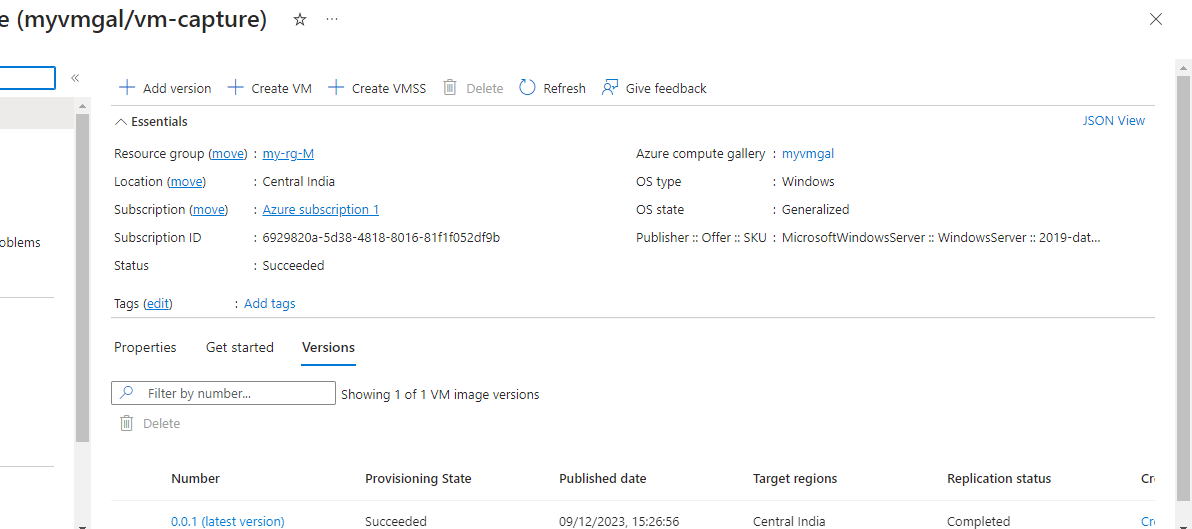
3.1. Deallocate the VM

- Stop (deallocate) the VM to prepare it for image capture. This can be done in the Azure Portal.

3.2. Capture VM Image

- Once the VM is deallocated, navigate to the VM settings, go to "Operations," and select "Capture."

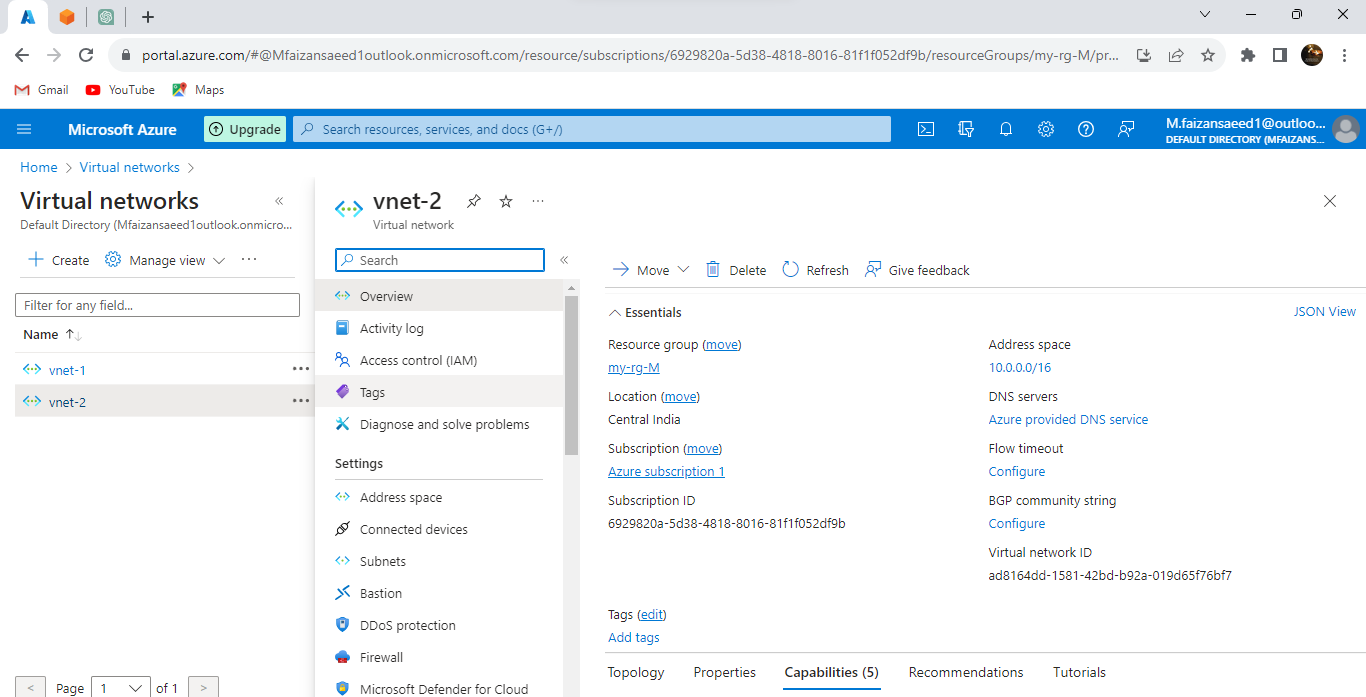
- Follow the prompts to create an image of the VM.



**Step 4:** Create a New Virtual Machine in the Target VNET

4.1. Create a New Virtual Network (VNET)

- If you haven't already, create a new VNET in the target zone.



4.2. Create a New Virtual Machine

- Go to "Create a resource" > "Compute" > "Virtual machine."

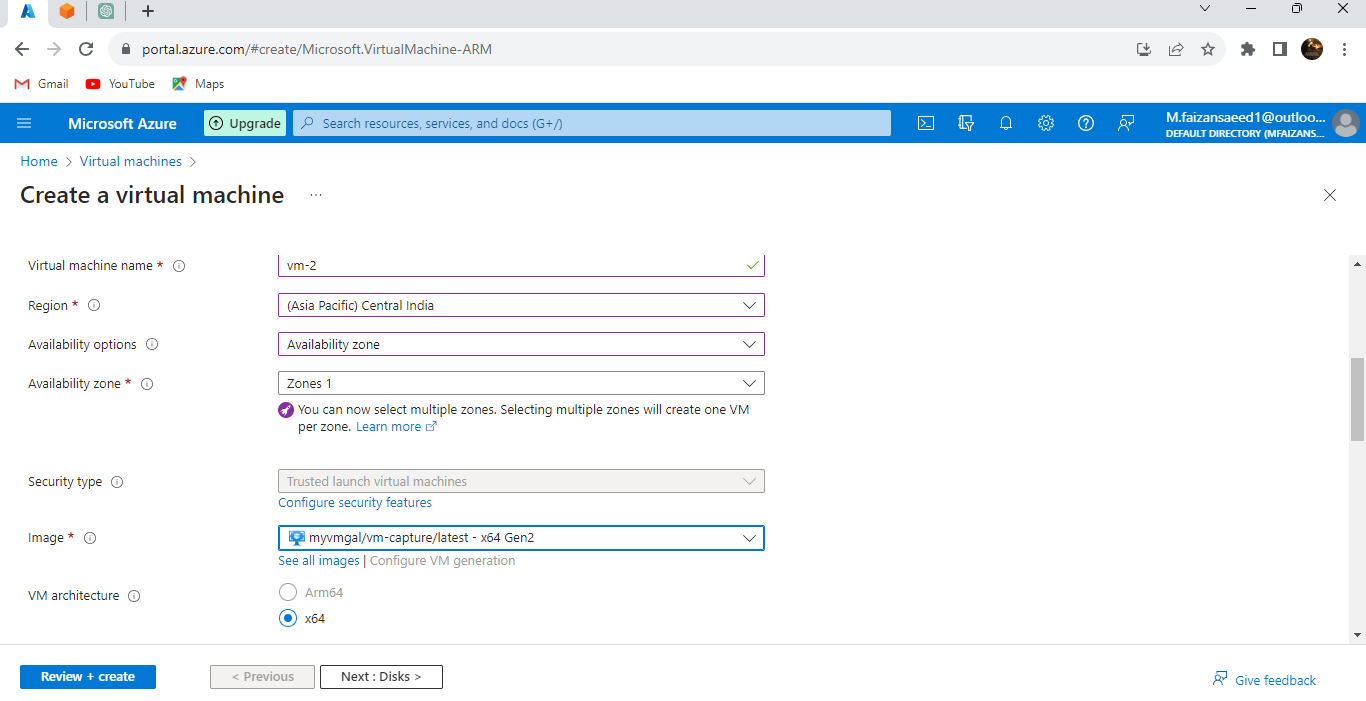
- Configure the VM settings, including the operating system, size, authentication, and networking.

- In the networking section, select the new VNET created in step 4.1.

**Step 5:** Deploy VM Image to the New VM

5.1. Deploy Image

- Once the new VM is created, navigate to its settings, go to "Image," and select the captured image from step 3.2.



.2. Configure Networking

- Ensure that the networking configurations match those of the original VM, including private IP addresses, subnets, and security groups.

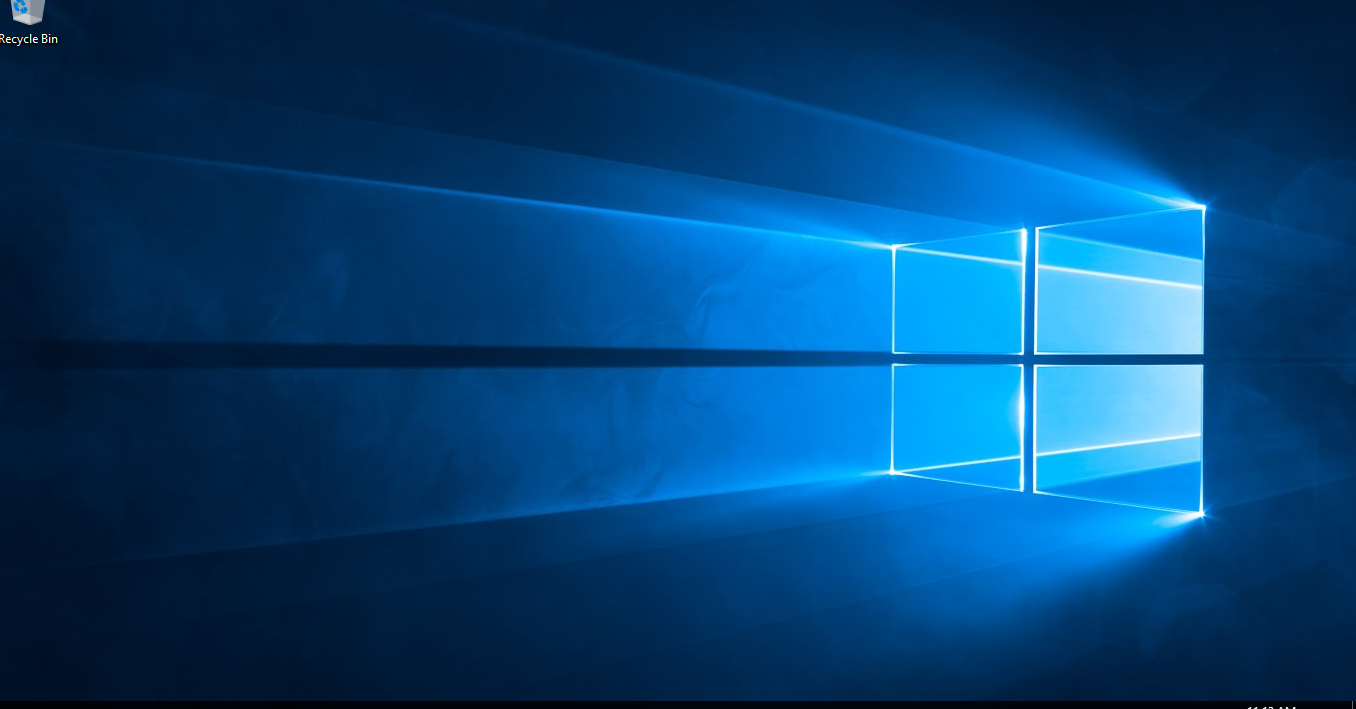
**Step 6:** Verify and Test

6.1. Verify VM Configuration

- Review the new VM's configuration to ensure it matches the original VM.

6.2. Test Connectivity

- Test connectivity to and from the VM to ensure that networking is correctly configured.



**Lab Performed**

**END**