

# AWS EC2 (Elastic Compute Cloud) Task

STEP : Open AWS console and go to EC2.

The screenshot shows the AWS Console Home page. On the left, under 'Recently visited', there are links to CloudWatch, Billing and Cost Management, S3, Lambda, IAM, EC2, VPC, and AWS Health Dashboard. On the right, under 'Applications (0)', it says 'Region: US East (N. Virginia)' and 'us-east-1 (Current Region)'. A search bar says 'Find applications'. Below it, there's a table with columns for Name, Description, Region, and Origin, which is currently empty. At the bottom, there's a 'Create application' button.

STEP : Click on Instance

The screenshot shows the AWS EC2 Dashboard. On the left, the sidebar has sections for EC2 Global View, Events, Console-to-Code (Preview), Instances (with sub-options like Instances, Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity Reservations, and Images). The main area shows 'Resources' with a table of Amazon EC2 resources in the US East (N. Virginia) Region:

Instances (running)	1	Auto Scaling Groups	0	Dedicated Hosts	0
Elastic IPs	0	Instances	1	Key pairs	2
Load balancers	0	Placement groups	0	Security groups	2
Snapshots	0	Volumes	1		

Below the resources, there are two sections: 'Launch instance' (with a note to get started by launching an instance) and 'Service health' (with a link to the AWS Health Dashboard).

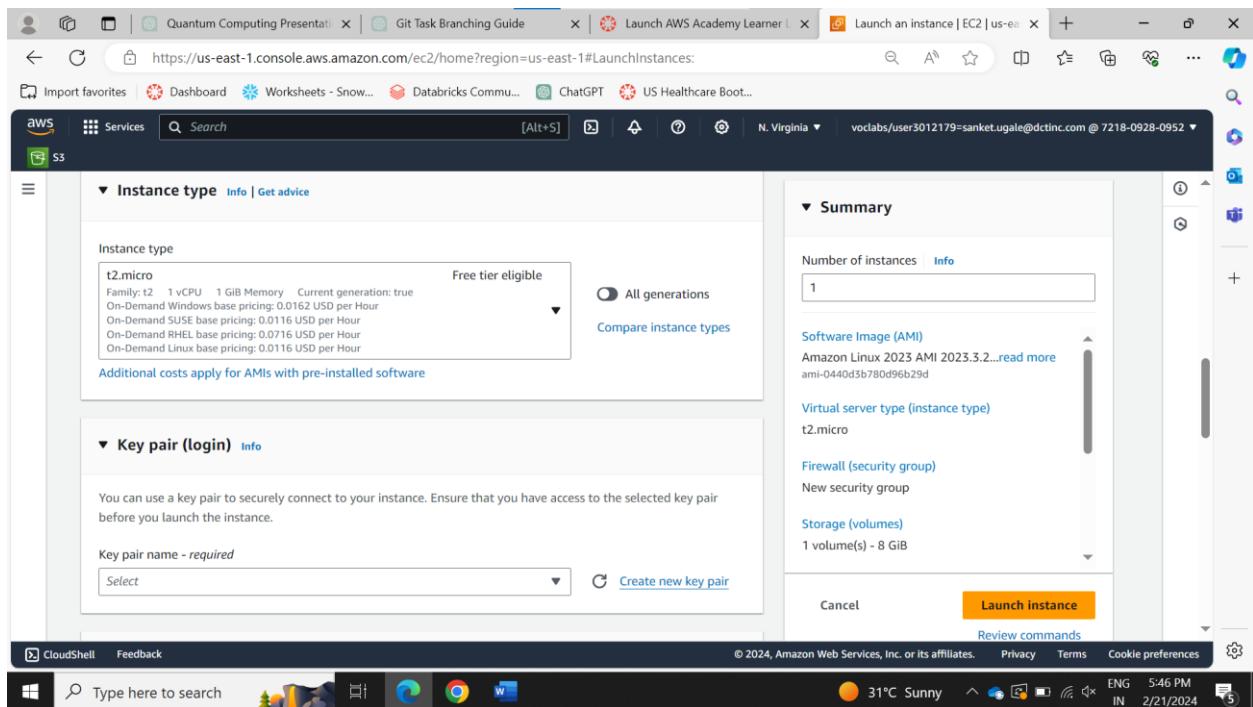
STEP : Click on Launch Instances

The screenshot shows the AWS EC2 Instances page. In the left sidebar, under 'Instances', there is a section titled 'Instances' with various options like Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity Reservations, and Images. The main area displays a table titled 'Instances (1) Info' with one row. The row details an instance named 'my\_instance01' with the ID 'i-0a9914e91306f40cb'. The instance is listed as 'Running' with a status check of '2/2 checks passed' and an alarm status of 'View alarms'. A modal window titled 'Select an instance' is open in the foreground.

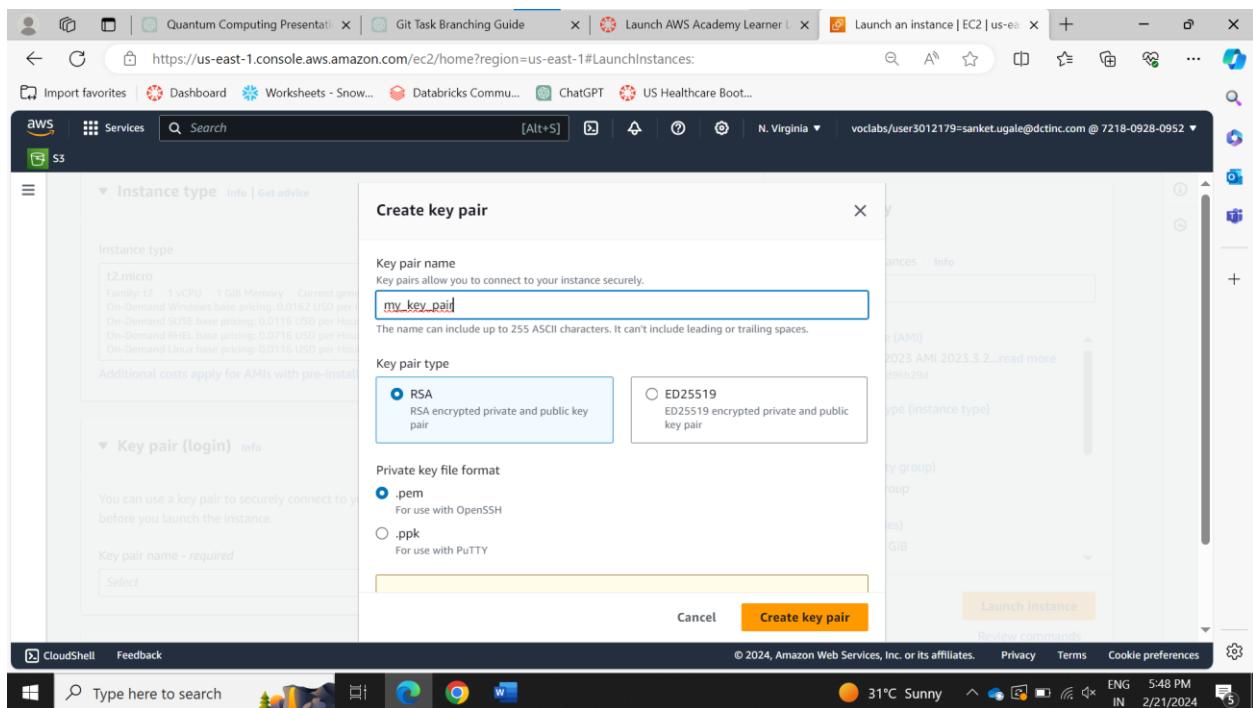
STEP : Give a name to your instance and select the AMI (Amazon Machine Image)

The screenshot shows the 'Launch an instance' wizard. On the left, there's a 'Name and tags' section where the name 'My\_Instance' is entered. Below it is a 'Application and OS Images (Amazon Machine Image)' section. Under 'Software Image (AMI)', the 'Amazon Linux 2023 AMI 2023.3.2...' option is selected. Other options include 'macOS', 'Ubuntu', 'Windows', 'Red Hat', 'SUSE Linux', and 'Browse more AMIs'. A tooltip for the Amazon Linux AMI provides information about free tier usage. On the right, there's a 'Summary' section showing 'Number of instances: 1'. At the bottom, there are 'Cancel', 'Launch instance', and 'Review commands' buttons.

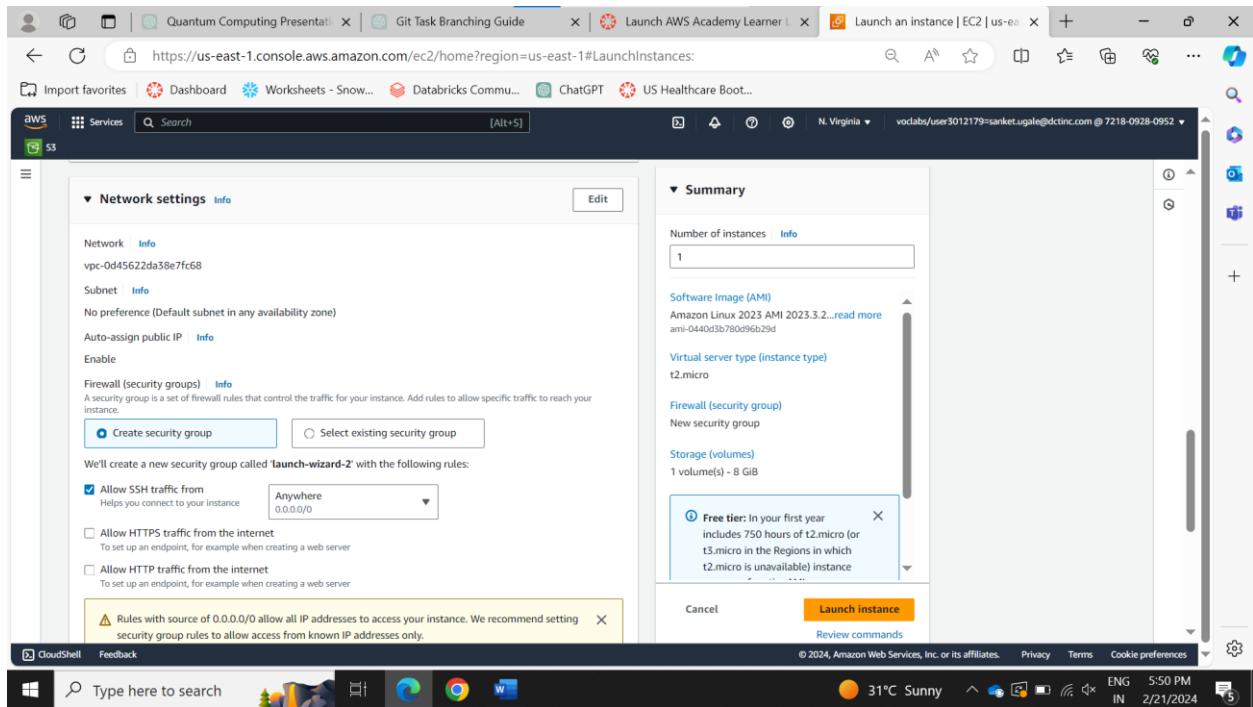
STEP : Select your instance type from the drop down menu and click on the create key pair.



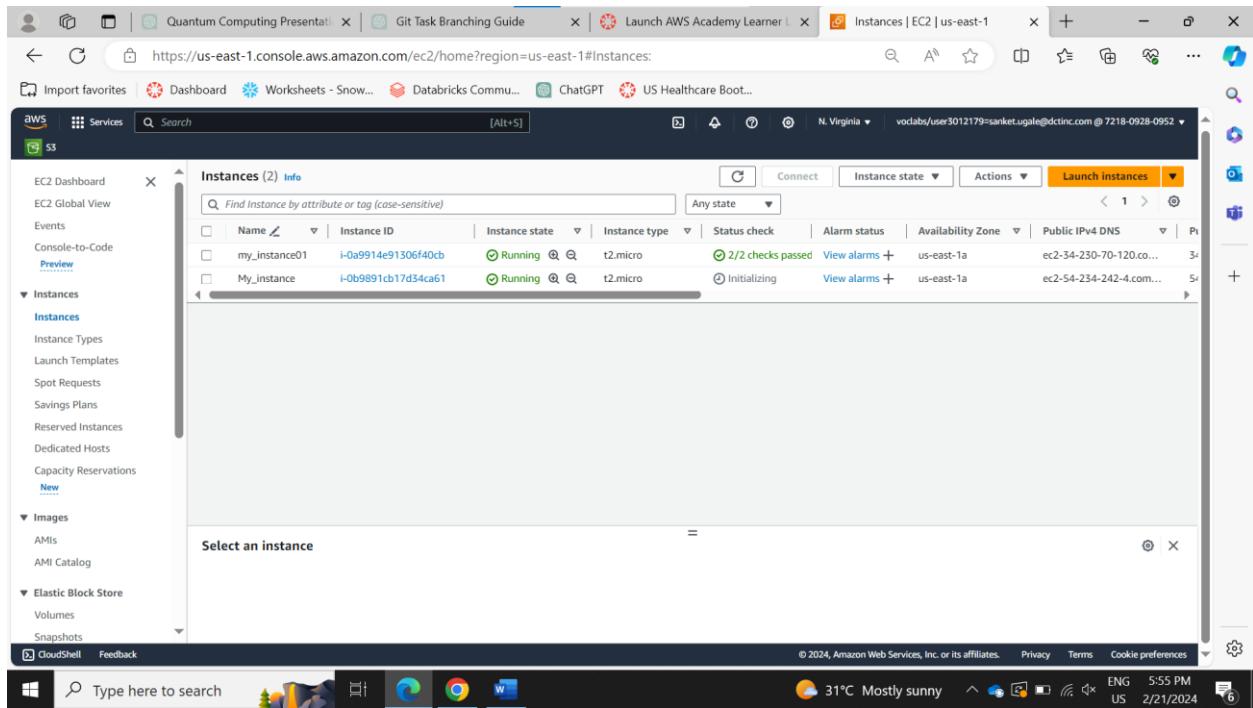
STEP : Name your key pair and select the .pem and click on create key pair and download the key pair.



STEP : tick the create security group and create instance.



STEP : again go to instances and wait until you instance states comes to “Running”



STEP : Go to Elastic IP in network and setting and click on allocate elastic IP.

The screenshot shows the AWS Management Console with the EC2 Dashboard selected. In the center, the 'Elastic IP addresses' section is displayed. A search bar at the top has the URL 'https://us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#Addresses:' entered. Below the search bar, there's a table header with columns: Name, Allocated IPv4 addr..., Type, Allocation ID, Reverse DNS record, and Associated. A message below the table states 'No Elastic IP addresses found in this Region'. At the bottom of the page, a note says 'View IP address usage and recommendations to release unused IPs with Public IP insights.' The status bar at the bottom right shows 'ENG US 5:58 PM 2/21/2024'.

STEP : Click on allocate.

The screenshot shows the 'Allocate Elastic IP address' dialog box. The 'Public IP pool of IPv4 addresses' section contains a note: 'Amazon's pool of IPv4 addresses' with a link to 'Learn more'. Below it, another note says 'Customer-owned pool of IPv4 addresses created from your on-premises network for use with an Outpost. Option disabled because no customer owned pools found.' with a link to 'Learn more'. The 'Tags - optional' section explains what tags are and how they can be used for search and filtering. At the bottom, there are 'Cancel' and 'Allocate' buttons.

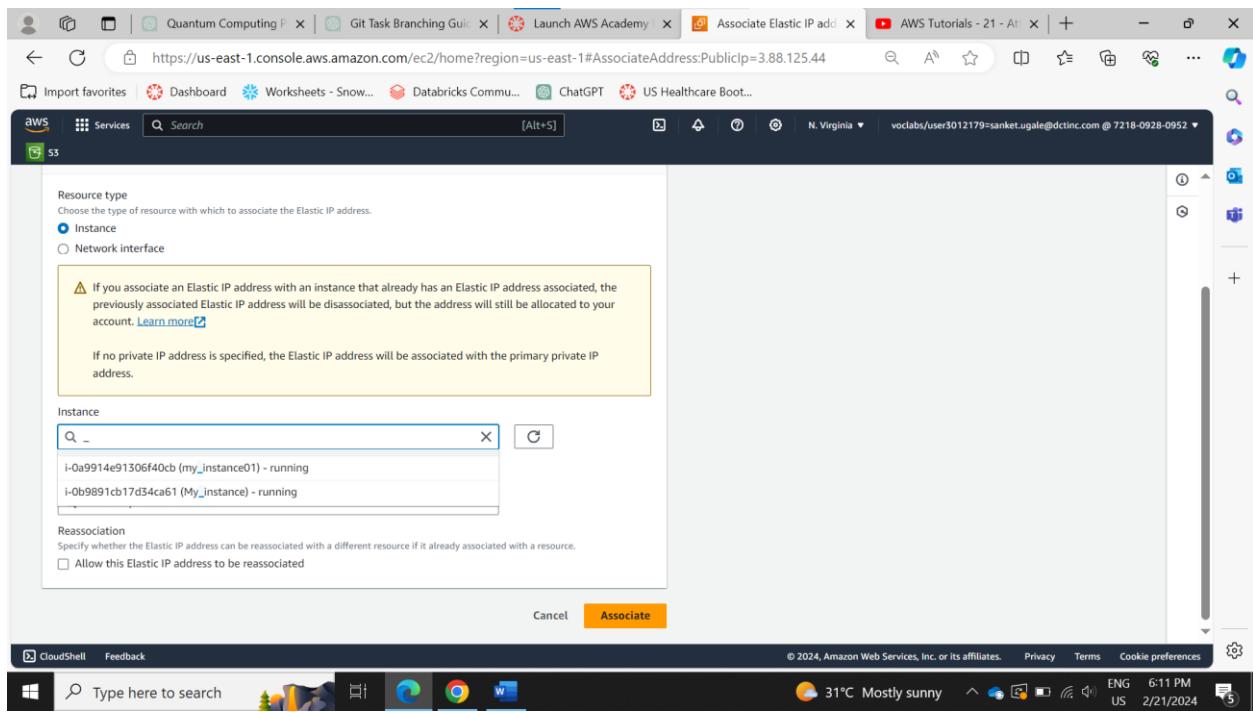
STEP : Your Elastic IP is generated rename it as per your need.

The screenshot shows the AWS Elastic IP addresses page. On the left, there's a sidebar with options like EC2 Dashboard, EC2 Global View, Events, Console-to-Code, Instances, Images, and CloudShell. The main area is titled "Elastic IP addresses (1/1)". It lists one item: "My\_EIP" with the IP address "3.88.125.44". The "Actions" button is highlighted in orange at the top right. Below the table, there's a note about Public IP insights and a summary tab.

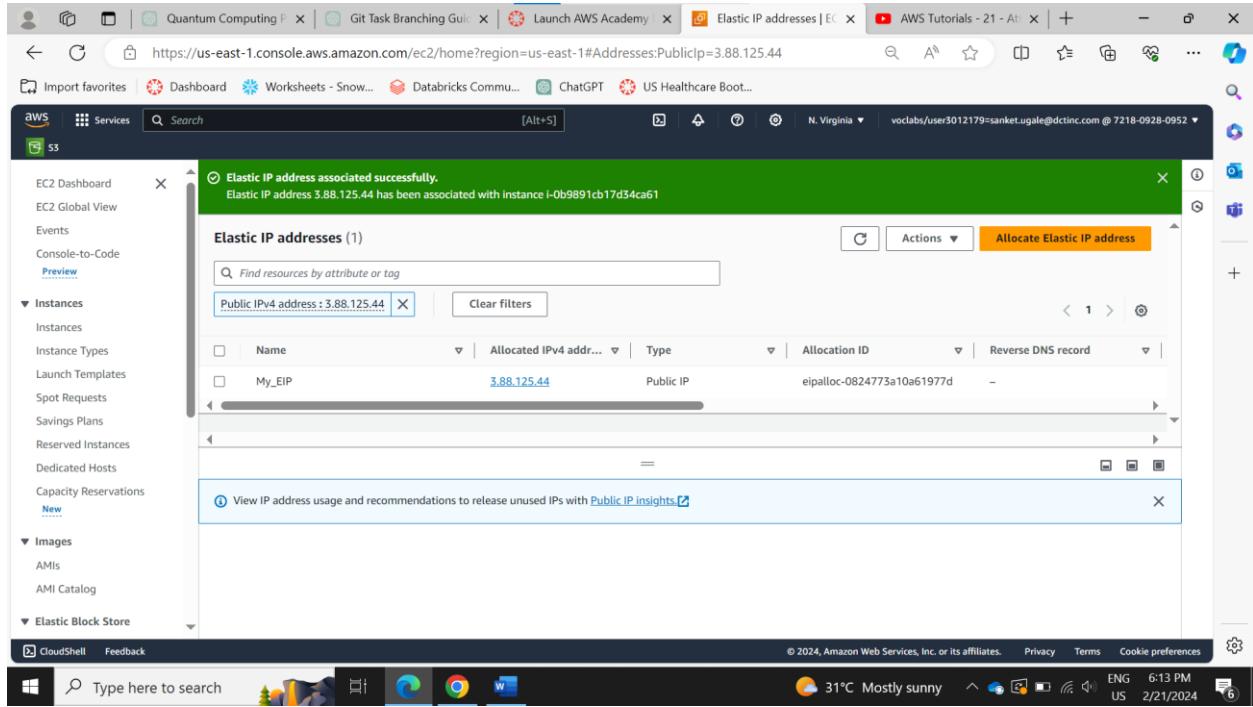
STEP : Select your Elastic IP and click on Actions and click on Associate Elastic IP Address.

This screenshot is similar to the previous one, but the "Actions" dropdown menu is open. The "Associate Elastic IP address" option is highlighted with a blue border. Other options in the menu include View details, Release Elastic IP addresses, Disassociate Elastic IP address, Update reverse DNS, Enable transfers, Disable transfers, and Accept transfers.

STEP : Tick the instance and select your instance from drop down menu and click on associate.



STEP : Congratulations your Elastic IP address is associated with your instance.

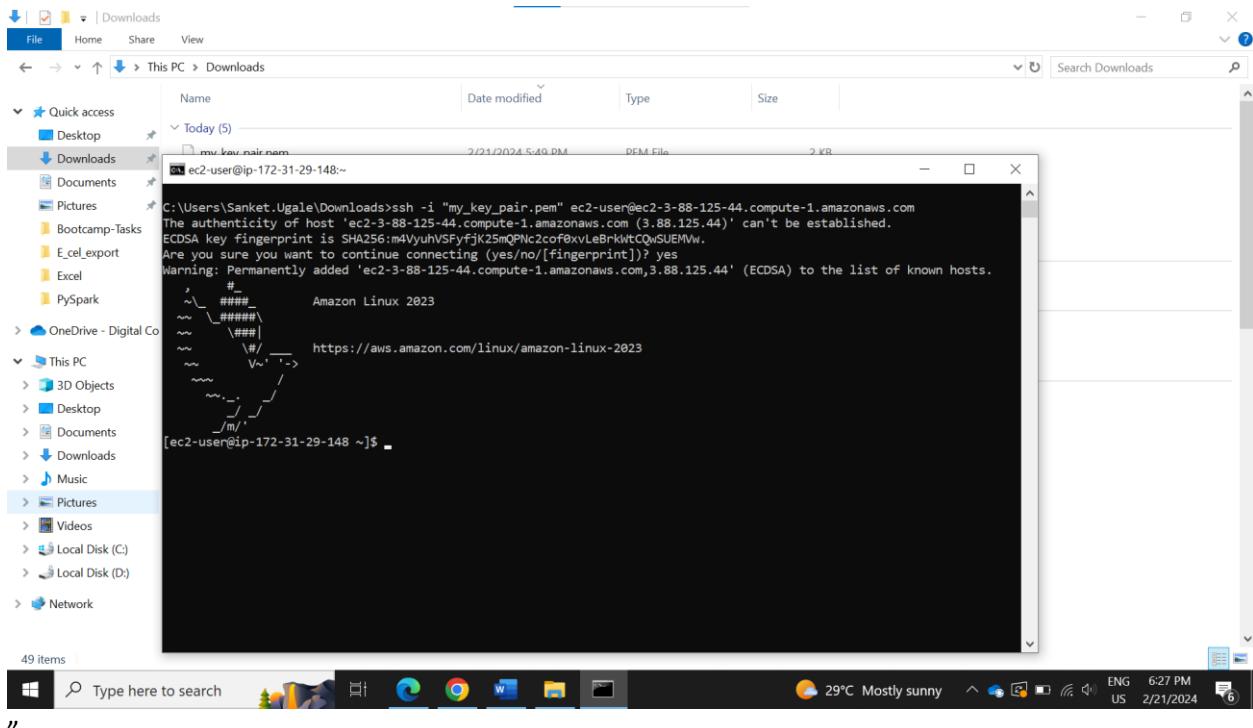


STEP : Now go to instances select your instance and click on connect.

STEP : Go to SSH Client. And Copy your Public DNS.

STEP : Open Command Prompt and Go to location where your key pair is downloaded.

And type the “`ssh -i "my_key_pair.pem" ec2-user@ec2-3-88-125-44.compute-1.amazonaws.com`” and click enter.



STEP : Congratulations you are connected to your EC2 instance by using ssh

## AWS S3 Lab (Simple Storage Service)

STEP 1 : Search S3 and go to s3 Console.

The screenshot shows the AWS Management Console with the S3 service selected. The left sidebar lists various AWS services. The main panel shows the 'Console Home' with sections for 'Recently visited' services (S3, EC2, CloudWatch, Lambda, IAM, VPC, AWS Health Dashboard) and 'Applications' info for the N. Virginia region. The status bar at the bottom indicates 'Activate Windows' and 'Go to Settings to activate Windows.'

STEP 2 : Click on Create Bucket option.

The screenshot shows the AWS S3 console interface. On the left, a sidebar lists various S3 management options like Buckets, Access Grants, and Storage Lens. The main area displays an 'Account snapshot' with metrics: Total storage (101.0 B), Object count (2), and Average object size (50.5 B). Below this, there are tabs for 'General purpose buckets' and 'Directory buckets', with 'General purpose buckets' currently selected. It shows 2 buckets and includes buttons for Copy ARN, Empty, Delete, and a prominent orange 'Create bucket' button. A search bar at the bottom allows finding buckets by name.

STEP 3 : Give a unique name to the bucket ( Globally Unique) and Select a region where you want your bucket to be created.

The screenshot shows the 'Create bucket' configuration page. Under 'General configuration', the 'AWS Region' is set to 'US East (N. Virginia) us-east-1'. The 'Bucket type' section has two options: 'General purpose' (selected) and 'Directory - New'. The 'Bucket name' field contains 'my-s3-task-bucket'. Below it, a note states that the name must be unique within the global namespace and follows specific naming rules. A 'Copy settings from existing bucket - optional' section is present. At the bottom right, there's an 'Activate Windows' message with a link to Settings. The footer includes standard AWS navigation links and system status indicators.

STEP : Untick the “**Block all Public access**” and Simpaly click on the create bucket option.

Launch AWS Academy Learner | Create S3 bucket | S3 | Global

s3.console.aws.amazon.com/s3/bucket/create?region=us-east-1&bucketType=general

Block Public Access settings for this bucket

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to this bucket or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

**Block all public access**  
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

- Block public access to buckets and objects granted through new access control lists (ACLs)**  
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
- Block public access to buckets and objects granted through any access control lists (ACLs)**  
S3 will ignore all ACLs that grant public access to buckets and objects.
- Block public access to buckets and objects granted through new public bucket or access point policies**  
S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.
- Block public and cross-account access to buckets and objects through any public bucket or access point policies**  
S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

Activate Windows  
Go to Settings to activate Windows

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences 19°C Clear 00:40 23-02-2024

Launch AWS Academy Learner | Create S3 bucket | S3 | Global

s3.console.aws.amazon.com/s3/bucket/create?region=us-east-1&bucketType=general

aws Services Search [Alt+S] Global vclabs/user3012179=sanket.ugale@dctinc.com @ 7218-0928-0952

Server-side encryption with Amazon S3 managed keys (SSE-S3)  
 Server-side encryption with AWS Key Management Service keys (SSE-KMS)  
 Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)  
Secure your objects with two separate layers of encryption. For details on pricing, see DSSE-KMS pricing on the Storage tab of the [Amazon S3 pricing page](#).

**Bucket Key**  
Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. [Learn more](#)

Disable  
 Enable

**Advanced settings**

After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.

Create bucket

Activate Windows  
Go to Settings to activate Windows

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences 19°C Clear 00:41 23-02-2024

The screenshot shows the AWS S3 console with the title "Launch AWS Academy Learner" and the URL "s3.console.aws.amazon.com/s3/buckets?region=us-east-1&bucketType=general&region=us-east-1". The main area displays "General purpose buckets (3) Info" with a table listing three buckets:

Name	AWS Region	Access	Creation date
my-bucket0241	US East (N. Virginia) us-east-1	Objects can be public	February 20, 2024, 15:38:17 (UTC+05:30)
my-bucket0249	US East (N. Virginia) us-east-1	Bucket and objects not public	February 20, 2024, 10:42:48 (UTC+05:30)
my-s3-task-bucket	US East (N. Virginia) us-east-1	Objects can be public	February 23, 2024, 00:41:38 (UTC+05:30)

The bottom status bar shows "CloudShell Feedback" and the system tray includes "Activate Windows", "CloudShell", "Feedback", "Type here to search", and various icons.

**STEP : Go to Bucket permissions and edit bucket policy.**

The screenshot shows the AWS S3 bucket "my-s3-task-bucket" with the title "my-s3-task-bucket - S3 bucket" and the URL "s3.console.aws.amazon.com/s3/buckets/my-s3-task-bucket?region=us-east-1&bucketType=general&tab=permissions". The "Permissions" tab is selected. The "Permissions overview" section shows "Access: Objects can be public". The "Block public access (bucket settings)" section has a note: "Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases." Below it, "Block all public access" is set to "OFF". The "Bucket policy" section at the bottom contains the note: "The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts." and includes "Edit" and "Delete" buttons.

The bottom status bar shows "CloudShell Feedback" and the system tray includes "Activate Windows", "CloudShell", "Feedback", "Type here to search", and various icons.

**STEP : Click on policy generator.**

- Select the type of Policy to “**s3 Bucket policy**”
- Allow it to everyone “**\***”
- Select action as “**get object**”
- Copy your bucket ARN (**Amazon Resource Name**) and Paste.
- Click on add statement and then generate Policy.
- Copy the generated policy and then paste in the bucket policy.
- And save the changes.

Launch AWS Academy Learner | Edit bucket policy - S3 bucket | + s3.console.aws.amazon.com/s3/bucket/my-s3-task-bucket/property/policy/edit?region=us-east-1&bucketType=general

Apps YouTube LinkedIn SQL 50 - Study Plan... Placement: Home Python SQL Excel Data Structures And... Linux Tutorials For B...

AWS Services Search [Alt+S]

Amazon S3 > Buckets > my-s3-task-bucket > Edit bucket policy

### Edit bucket policy Info

**Bucket policy**

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. [Learn more](#)

**Bucket ARN**  
arnaws:s3:::my-s3-task-bucket

**Policy**

1

Edit statement

Select a statement  
Select an existing statement in the policy or add a new statement.

Add new statement

Go to Settings to activate Windows.

CloudShell Feedback Type here to search © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences 19°C Clear 00:43 23-02-2024

Launch AWS Academy Learner | Edit bucket policy - S3 bucket | AWS Policy Generator | + awspolicygen.s3.amazonaws.com/policygen.html

CloudShell Feedback Type here to search © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences 19°C Clear 00:45 23-02-2024

A Policy is a container for permissions. The different types of policies you can create are an IAM Policy, an S3 Bucket Policy, an SNS Topic Policy, a VPC Endpoint Policy, and an SQS Queue Policy.

Select Type of Policy **S3 Bucket Policy**

**Step 2: Add Statement(s)**

A statement is the formal description of a single permission. See [a description of elements](#) that you can use in statements.

**Effect**  Allow  Deny

**Principal** \*

Use a comma to separate multiple values.

**AWS Service** Amazon S3  All Services ('\*')

Use multiple statements to add permissions for more than one service.

**Actions** 1 Action(s) Selected  All Actions ('\*')

**Amazon Resource Name (ARN)** arn:aws:s3:::my-s3-task-bu

ARN should follow the following format: arn:aws:s3:::{BucketName}/{Keyname}.  
Use a comma to separate multiple values.

**Add Conditions (Optional)**

**Add Statement**

Activate Windows  
Go to Settings to activate Windows.

**Step 3: Generate Policy**

CloudShell Feedback Type here to search © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences 19°C Clear 00:45 23-02-2024

The screenshot shows the AWS Policy Generator interface for an S3 bucket. The policy document is displayed in a code editor:

```
1  {
2    "Id": "Policy1708629393052",
3    "Version": "2012-10-17",
4    "Statement": [
5      {
6        "Sid": "Stmt1708629345707",
7        "Action": [
8          "s3:GetObject"
9        ],
10       "Effect": "Allow",
11       "Resource": "arn:aws:s3:::my-s3-task-bucket/*",
12       "Principal": "*"
13     }
14   ]
15 }
```

A modal window titled "Edit statement" is open on the right, with the sub-titile "Select a statement". It contains the instruction "Select an existing statement in the policy or add a new statement." and a button "+ Add new statement".

STEP : Go to bucket and upload some file.

The screenshot shows the AWS S3 Objects page for the "my-s3-task-bucket" bucket. The page title is "my-s3-task-bucket - S3 bucket". The main area displays the following information:

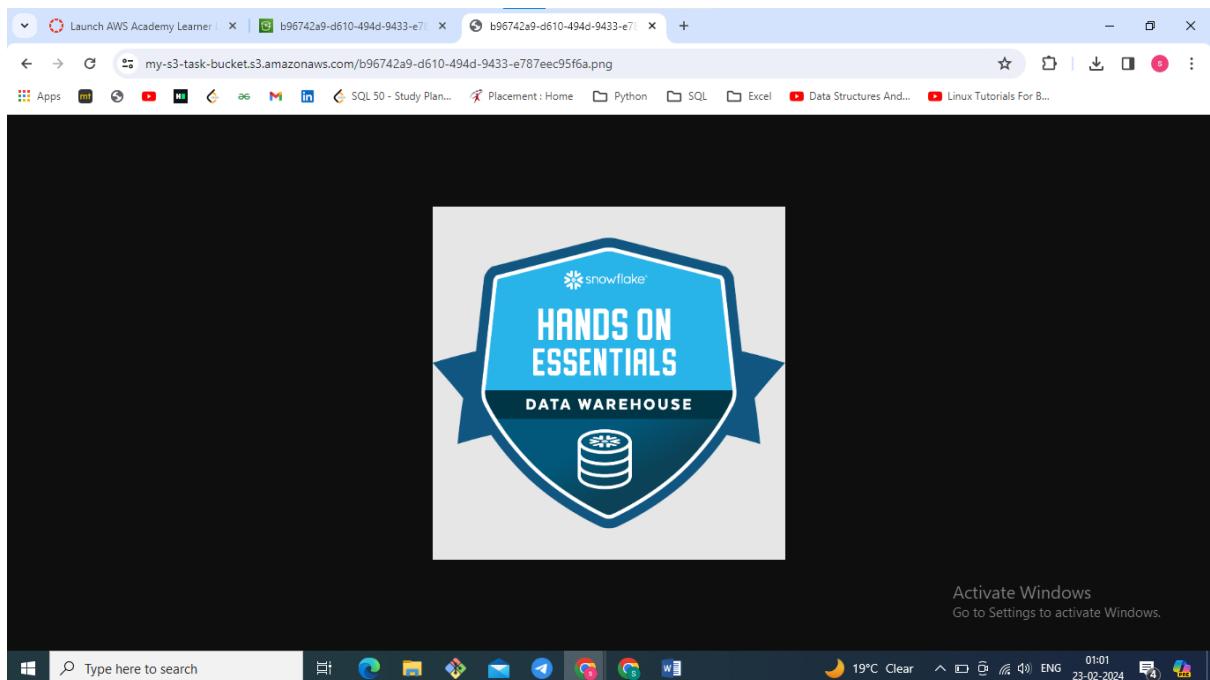
- Objects (0)**
- Info
- Action buttons: Copy S3 URI, Copy URL, Download, Open, Delete, Actions, Create folder, Upload (highlighted).
- Description: "Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)".
- Search bar: "Find objects by prefix".
- Table headers: Name, Type, Last modified, Size, Storage class.
- Message: "No objects" and "You don't have any objects in this bucket."
- Action button: Upload.

A modal window titled "Activate Windows" is partially visible on the right, with the sub-titile "Go to Settings to activate Windows".

The screenshot shows the AWS S3 service in the AWS Management Console. A single object named 'b96742a9-d610-494d-9433-e787eec95f6a.png' is listed in the 'Objects' table. The table includes columns for Name, Type, Last modified, Size, and Storage class. The object is a PNG file from February 23, 2024, at 00:59:08 UTC+05:30, with a size of 48.8 KB and a Standard storage class. Below the table, there are buttons for Actions (Upload, Copy S3 URI, Copy URL, Download, Open, Delete, Create folder) and a search bar for 'Find objects by prefix'. The top navigation bar shows the bucket name 'my-s3-task-bucket' and the region 'us-east-1&bucketType=general&tab=objects'.

STEP : Go to object properties and copy the Object URL and paste it in the new tab.

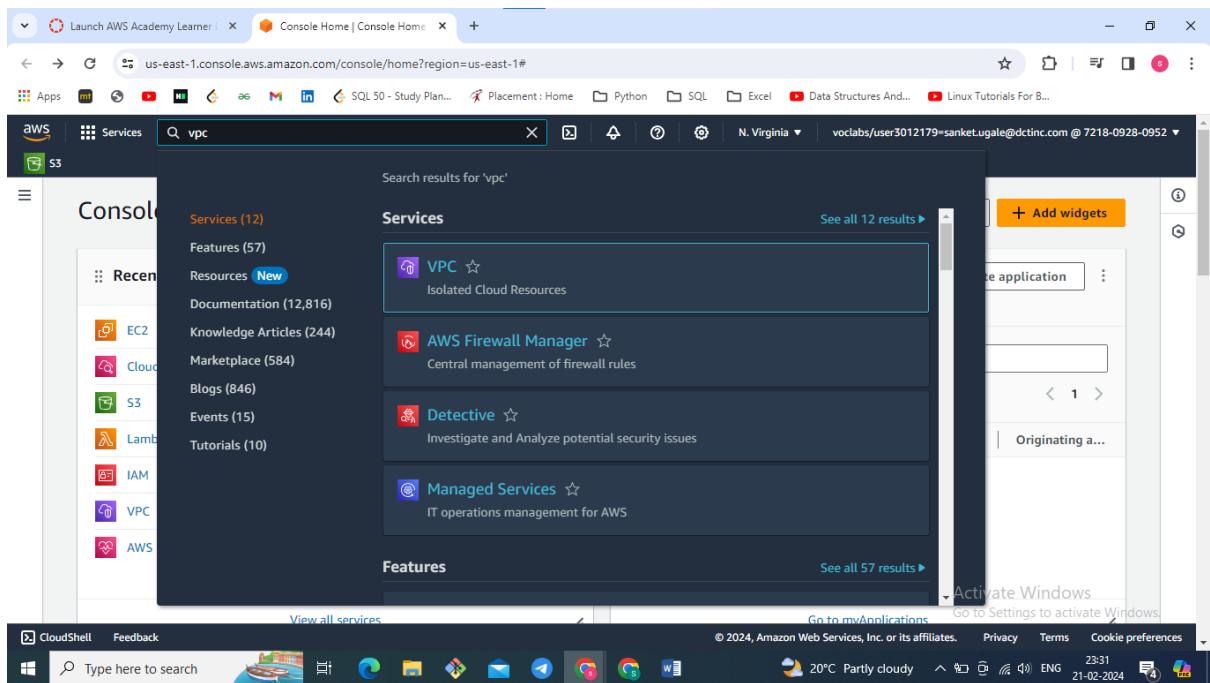
The screenshot shows the 'Object overview' page for the same object. The 'Object URL' field is highlighted, displaying the full URL: <https://my-s3-task-bucket.s3.amazonaws.com/b96742a9-d610-494d-9433-e787eec95f6a.png>. The rest of the page displays various metadata fields such as Owner, AWS Region, Last modified, Size, Type, and Key.



Congratulations now you can access the objects in your buckets Publically

AWS VPC Lab (Virtual Private Cloud)

## STEP 1 : Open AWS and search and select VPC

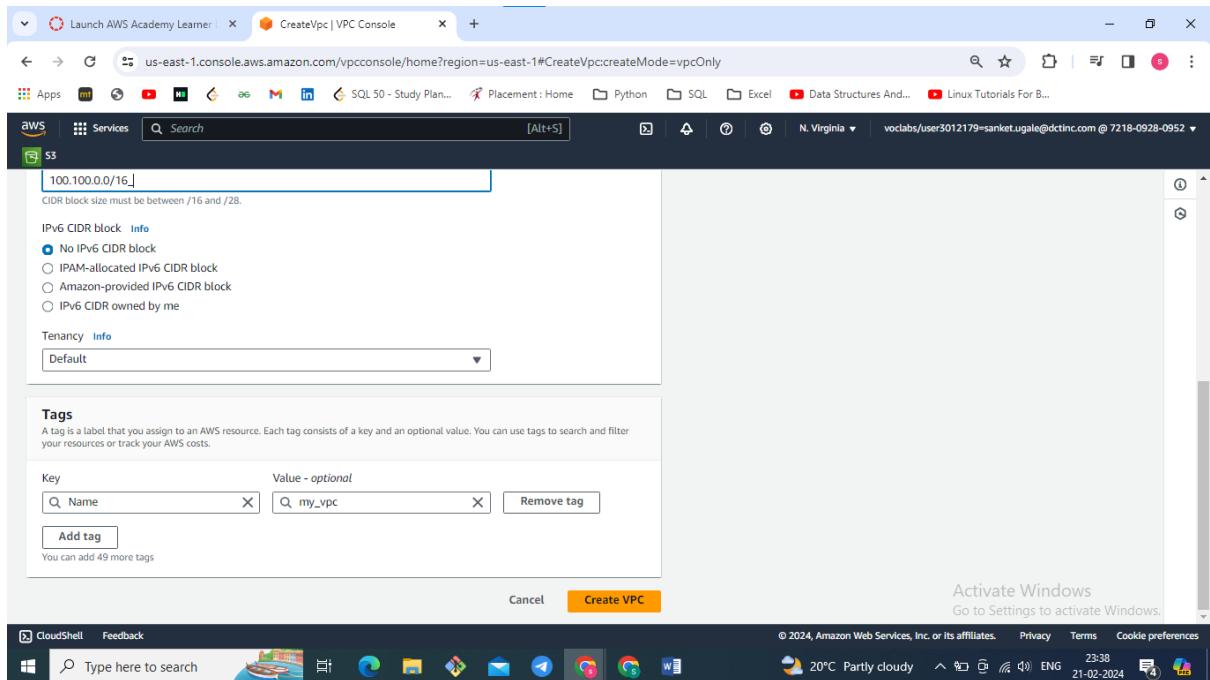


**STEP 2 : Go to VPC and Click on Create VPC (Region Specific)**

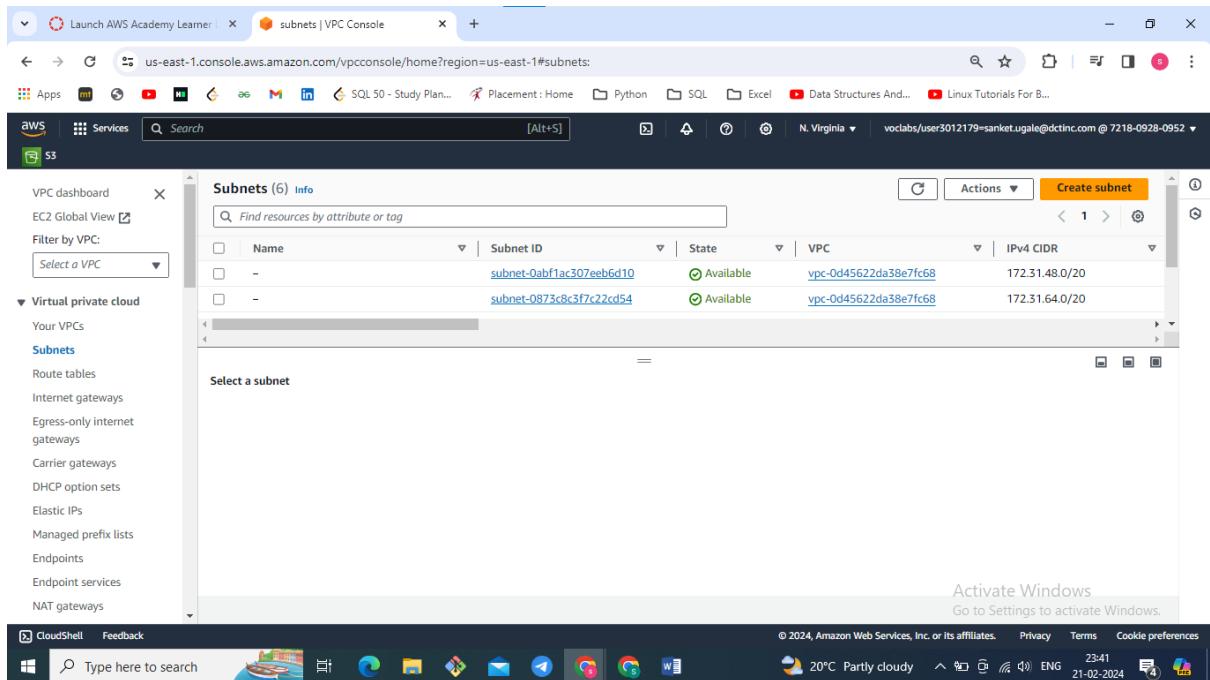
The screenshot shows the AWS VPC Console Home page. On the left, there's a sidebar titled "VPC dashboard" with sections like "Virtual private cloud" (Your VPCs, Subnets, Route tables, Internet gateways, Egress-only internet gateways, Carrier gateways, DHCP option sets, Elastic IPs, Managed prefix lists, Endpoints, Endpoint services) and "Create VPC" (Launch EC2 Instances). The main area is titled "Resources by Region" and shows "You are using the following Amazon VPC resources": VPCs (US East), NAT Gateways (US East), Subnets (US East), VPC Peering Connections (US East), Route Tables (US East, 1 item), Network ACLs (US East), Internet Gateways (US East), Security Groups (US East). To the right, there are "Service Health" and "Settings" sections, and a "Feedback" bar at the bottom.

STEP 3 : Give a name of VPC and Provide IPv4 CIDR (**100.100.0.0/16**) and click on create VPC.

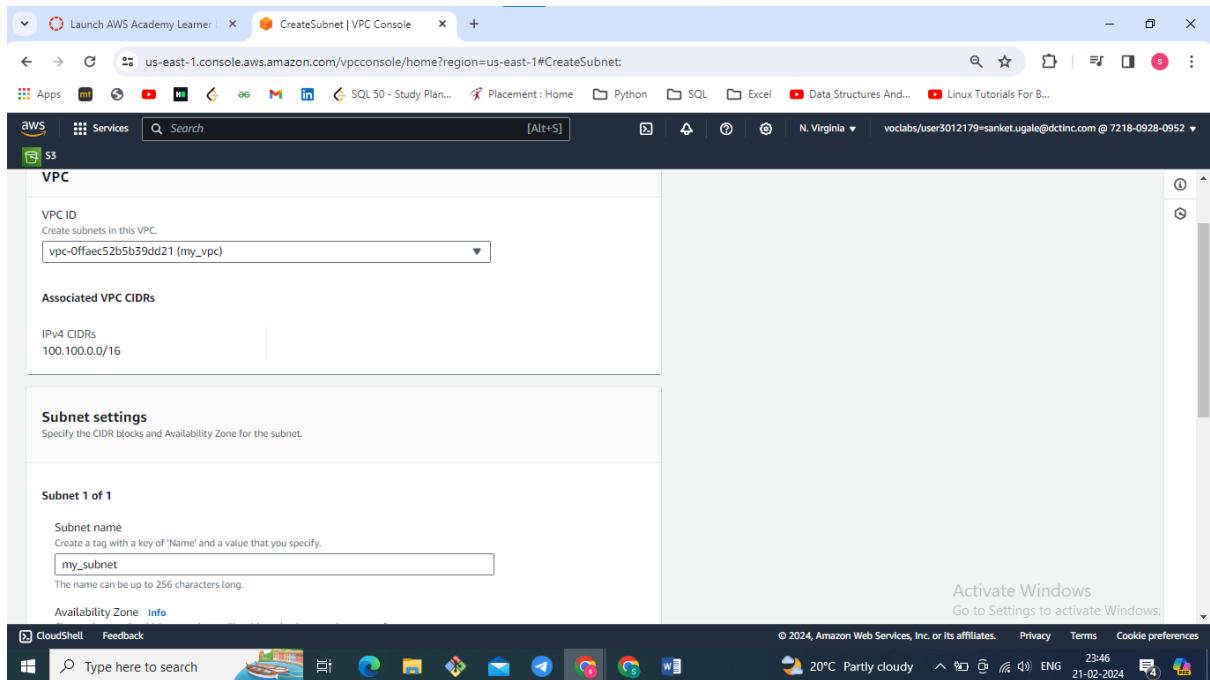
The screenshot shows the "CreateVpc | VPC Console" page. It has a "VPC settings" section with "Resources to create" (radio buttons for "VPC only" and "VPC and more", with "VPC only" selected). There's a "Name tag - optional" input field containing "my\_vpc". Under "IPv4 CIDR block", there's a radio button for "IPv4 CIDR manual input" (selected) and another for "IPAM-allocated IPv4 CIDR block". The "IPv4 CIDR" input field contains "100.100.0.0/16". Below it, a note says "CIDR block size must be between /16 and /28." At the bottom, there's an "Activate Windows" link and a "CloudShell Feedback" bar.



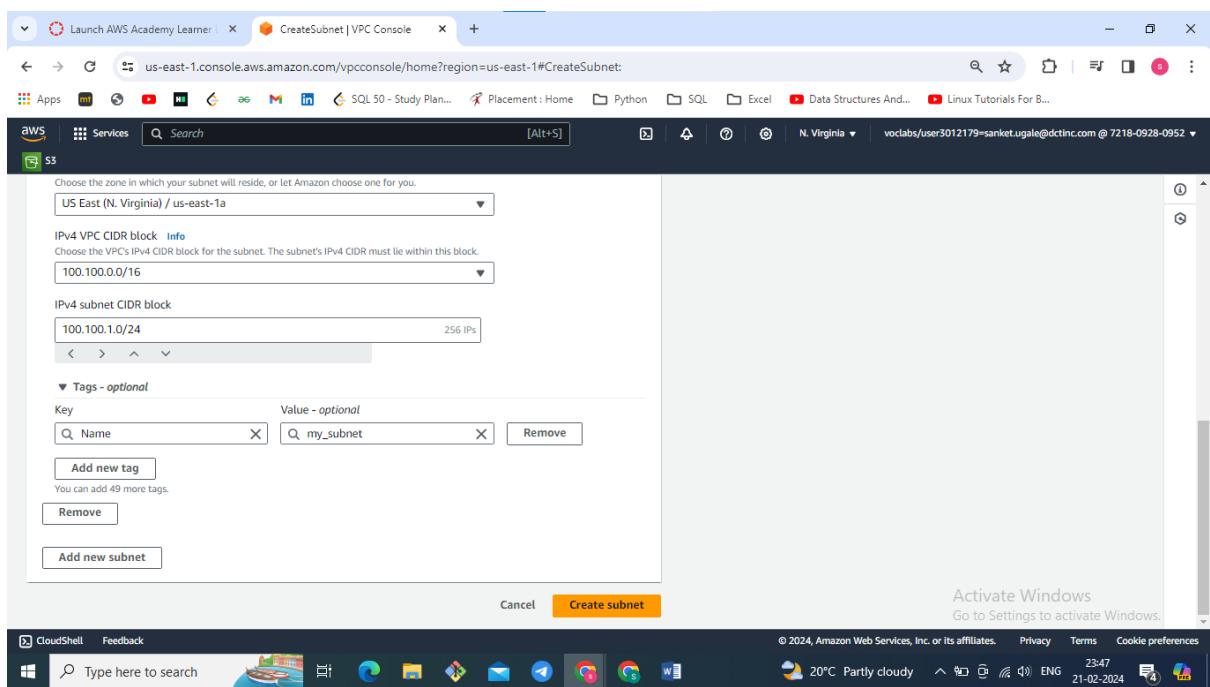
## STEP : Go to Subnets and click on Create subnets (Availability Zone Specific)



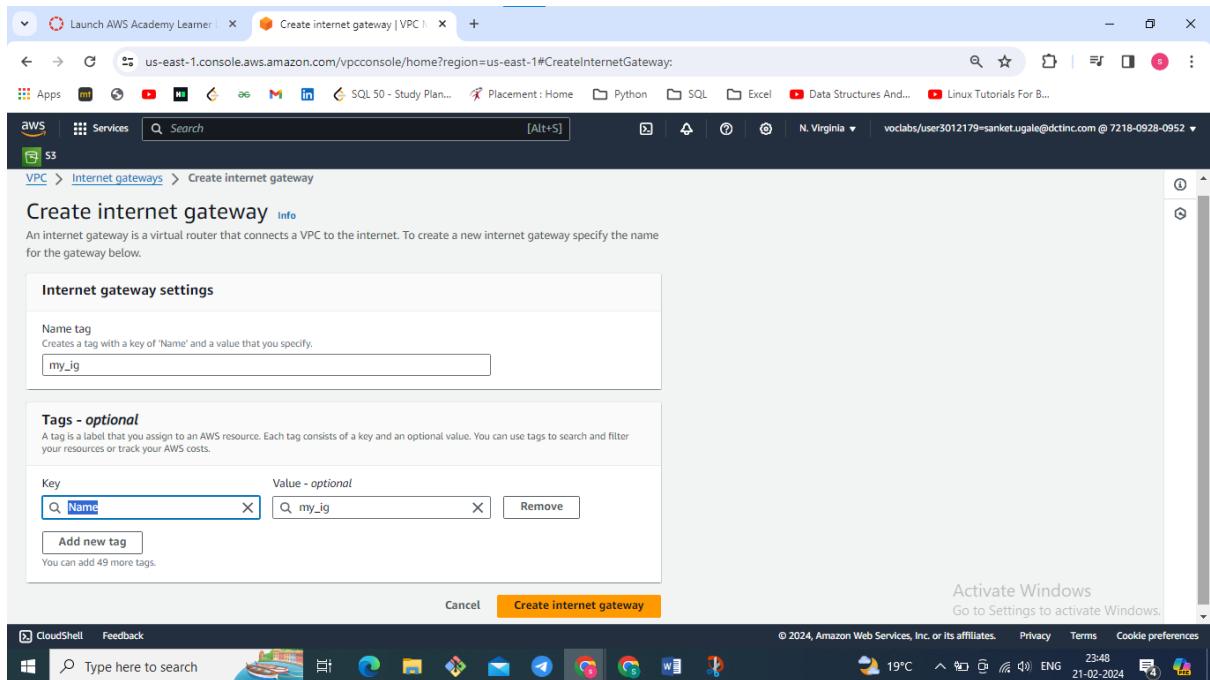
## STEP : Select your vpc ( Which you have already created) and name your subnet



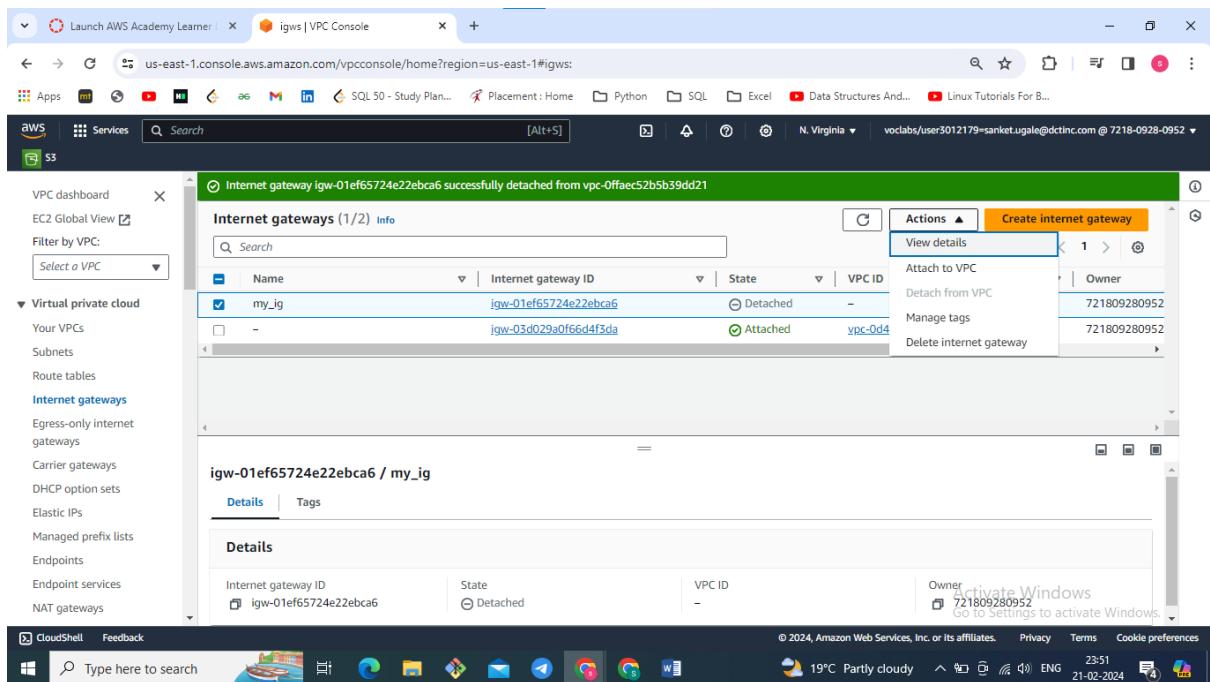
STEP : Select your AZ and Provide IPv4 CIDR (**100.100.1.0/24**)/ (**100.100.2.0/24**) and click on create 2 Subnets.



STEP : Go to internet gateway and give the name to IG and click on Create.



STEP : Select your created IG and go to action and attach it to your VPC.



STEP : Go to route table and select your route table > route > Edit route > add route >  
Destination : 0.0.0.0/0 → my created IG save changes.

The screenshot shows the AWS VPC Console with the 'RouteTables' page open. On the left, a sidebar lists 'Virtual private cloud' options like 'Your VPCs', 'Subnets', and 'Route tables'. The main area displays a table of route tables, with one row selected:

Name	Route table ID	Explicit subnet associations	Edge associations	Main	VPC
-	rtb-02cf4755848e92b00	-	-	Yes	vpc-0d45622da38e7fc

Below the table, a detailed view of the selected route table 'rtb-02cf4755848e92b00' is shown. The 'Routes' tab is selected, displaying the following routes:

Destination	Target	Status	Propagated
0.0.0.0/0	igw-03d029a0f66d4f3da	Active	No
172.31.0.0/16	local	Active	No

At the bottom right of the page, there is a message: "Activate Windows Go to Settings to activate Windows."

The screenshot shows the 'Edit routes' interface for route table 'rtb-03c29bdb642d6a1e8'. The 'Destination' column contains '100.100.0.0/16' and '0.0.0.0/0'. The 'Target' column contains 'local' and 'Internet Gateway'. The 'Status' column shows 'Active' for both, and the 'Propagated' column shows 'No' for both.

Destination	Target	Status	Propagated
100.100.0.0/16	local	Active	No
0.0.0.0/0	Internet Gateway igw-01ef65724e22ebca6	Active	No

At the bottom right, there are 'Cancel', 'Preview', and 'Save changes' buttons. A message at the bottom right says: "Activate Windows Go to Settings to activate Windows."

STEP : Create a instance with the above VPC attached.

Launch AWS Academy Learner | EditRoutes | VPC Console | EC2 | us-east-1

us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#LaunchInstances:

Launch an instance

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags

Name: my\_vpc\_instance

Application and OS Images (Amazon Machine Image)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below.

Search our full catalog including 1000s of application and OS images

Software Image (AMI)

Amazon Linux 2023 AMI 2023.3.2...read more

ami-0440d3b780d96b29d

Virtual server type (instance type)

t2.micro

Firewall (security group)

New security group

Storage (volumes)

1 volume(s) - 8 GiB

Launch instance

CloudShell Feedback Type here to search 19°C Partly cloudy 00:01 22-02-2024

Launch AWS Academy Learner | EditRoutes | VPC Console | EC2 | us-east-1

us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#LaunchInstances:

Network settings

VPC - required

vpc-0ffae52b5b39dd21 (my\_vpc)  
100.100.0.0/16

Subnet

subnet-0dbfef20e4bda9bfb my\_subnet  
VPC: vpc-0ffae52b5b39dd21 Owner: 721809280952 Availability Zone: us-east-1a  
IP addresses available: 251 CIDR: 100.100.1.0/24

Create new subnet

Auto-assign public IP

Disable

Firewall (security groups)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

Create security group Select existing security group

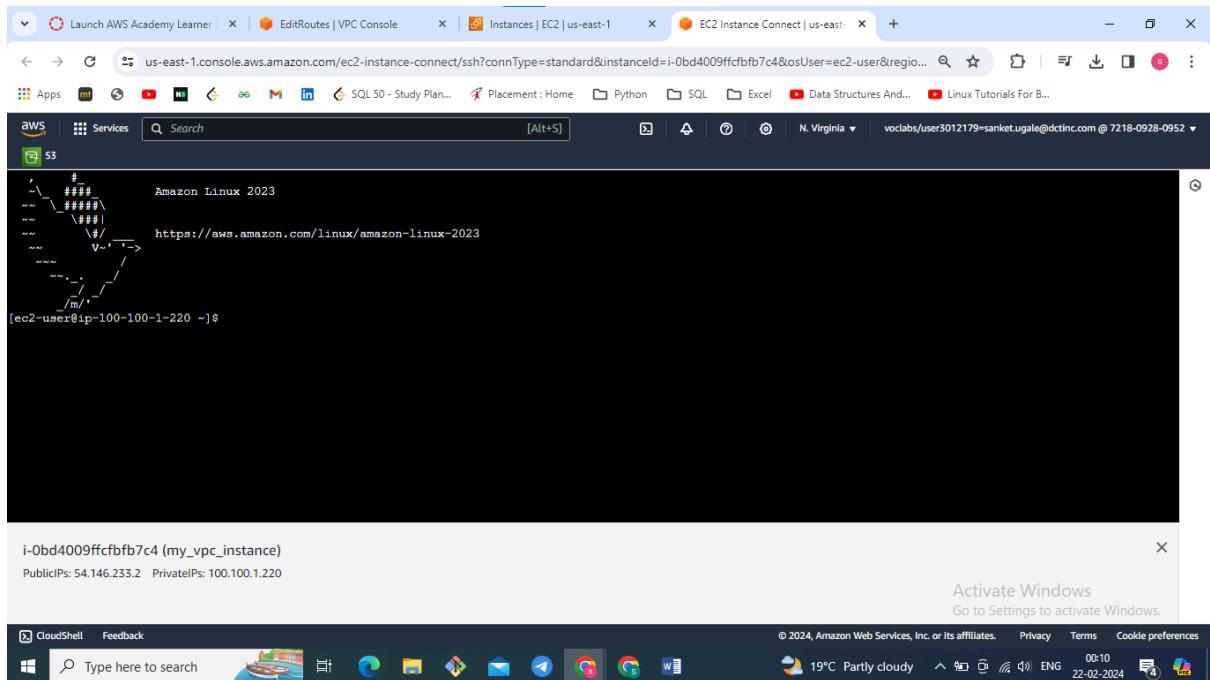
Security group name - required

launch-wizard-4

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and \_~!@#\$%^&{}()

Description - required

CloudShell Feedback Type here to search 19°C 00:01 22-02-2024



Congratulations now you have created a VPC by which your instance can access the internet.

## AWS IAM Lab (Identity and Access Management)

Amazon Web Services Identity and Access Management (AWS IAM) is a web service that enables secure control and management of access to AWS resources. IAM allows you to create and manage users and their permissions within your AWS account, helping you control who can access specific resources and what actions they can perform.

### Key features of AWS IAM include:

1. **Users and Groups:** IAM allows you to create individual IAM users for people accessing your AWS account and organize them into groups for easier management.
2. **Policies:** IAM policies define permissions and specify what actions are allowed or denied on AWS resources. These policies can be attached to users, groups, or roles.
3. **Roles:** IAM roles are similar to users but are meant to be assumed by other AWS entities, such as EC2 instances or Lambda functions. Roles define a set of permissions, and AWS services or users assume these roles to perform specific tasks.

**4. Multi-Factor Authentication (MFA):** IAM supports the use of MFA to add an extra layer of security by requiring users to provide a second form of authentication, in addition to their password, when accessing AWS resources.

**5. Identity Federation:** IAM allows you to integrate with external identity providers, enabling users to sign in using credentials from sources like Active Directory or social identity providers.

**6. Access Advisor:** IAM provides an Access Advisor that helps you identify unused or underutilized permissions within your IAM policies, helping you adhere to the principle of least privilege.

**7. Audit Trail:** IAM maintains an audit trail by logging all API calls made on your account. These logs can be analyzed to track user activity, changes to policies, and other security-relevant events.

By effectively using AWS IAM, organizations can implement strong security practices, ensure least privilege access, and manage access to their AWS resources in a scalable and controlled manner.