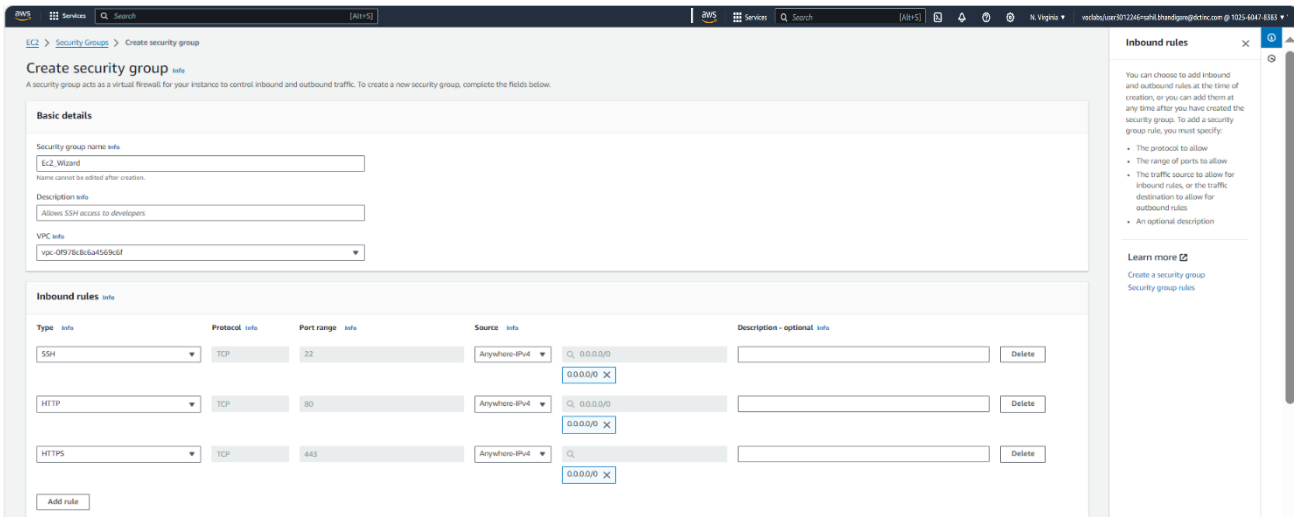
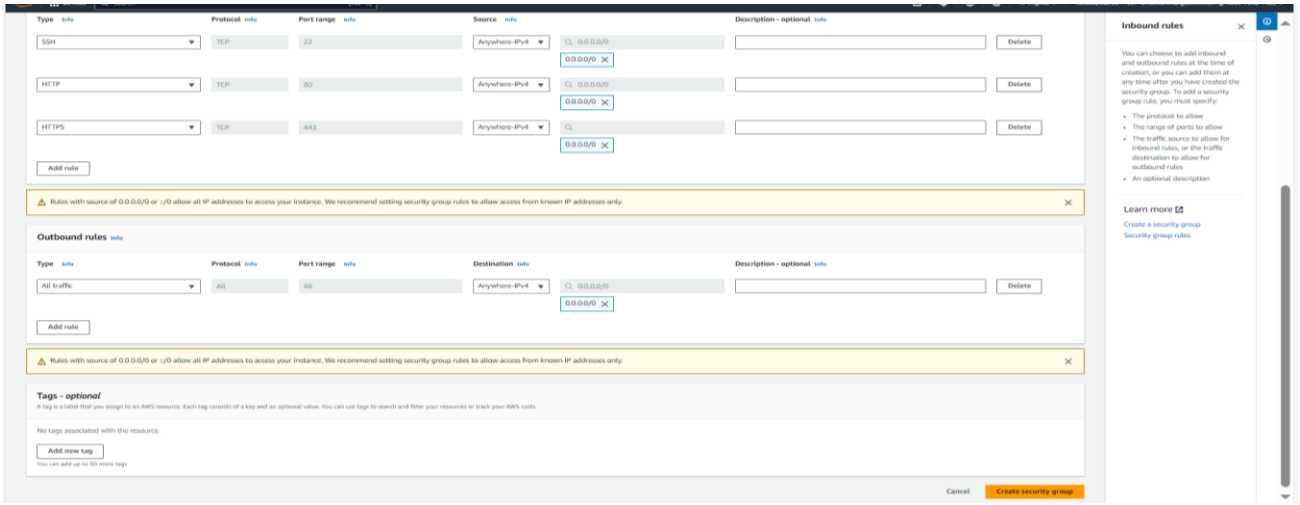
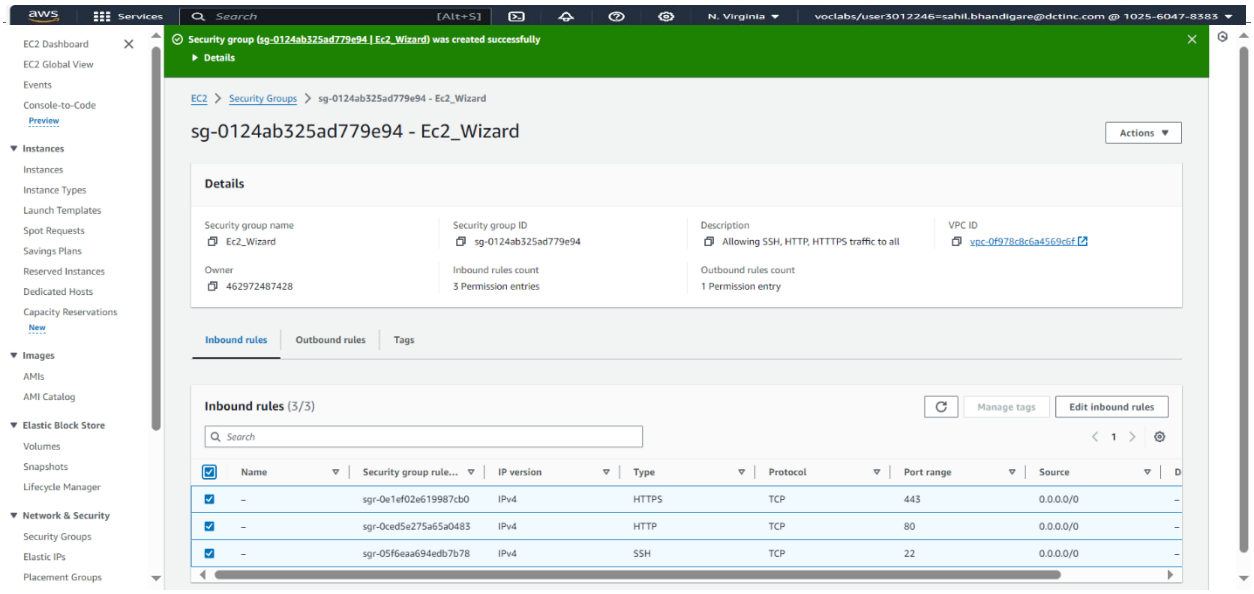
Q1. EC2 Basics Lab

- **Objective**: To understand the process of setting up and managing an Amazon EC2 instance.
- **Approach**: Students will start by launching a new EC2 instance, selecting an appropriate instance type and configuring the instance details. They will then create and configure a new Security Group, and allocate an Elastic IP address to the instance. The lab will also include connecting to the instance via SSH.
- **Goal**: By the end of this lab, students should be able to launch and manage an EC2 instance, understand instance types, security groups, and IP addressing in AWS.

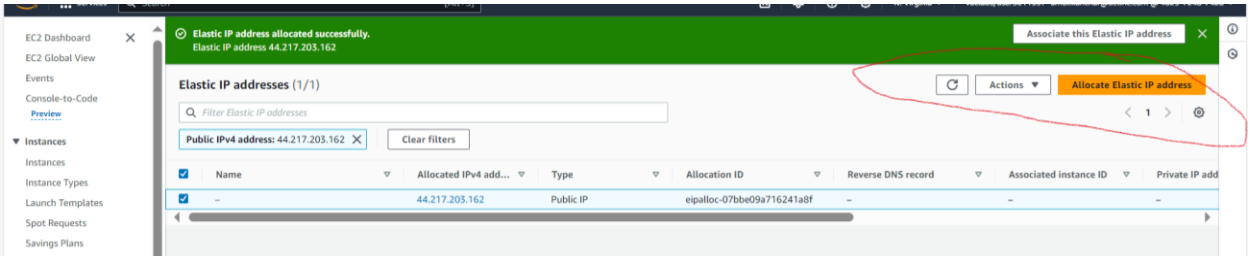
Creating security group



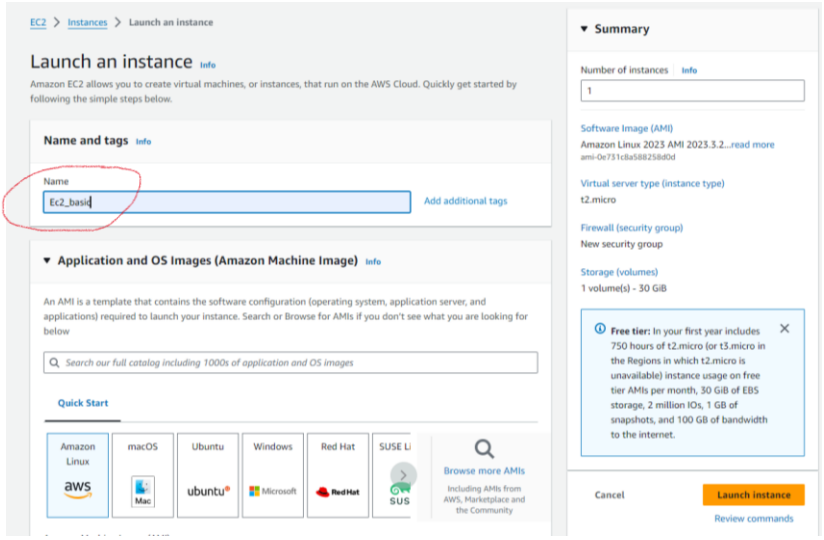


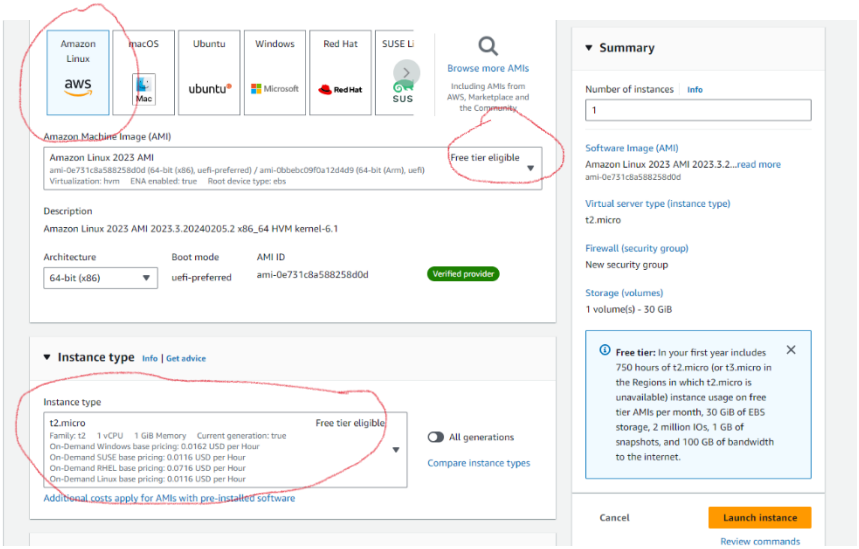


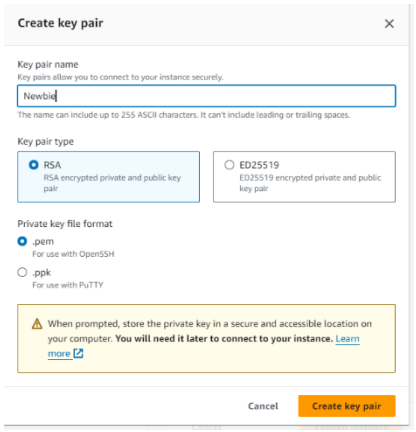
Allocating elastic IP Address

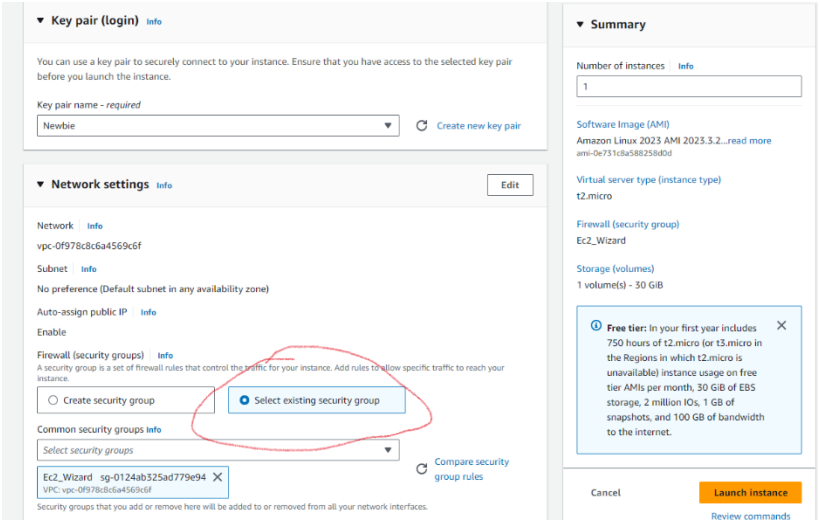


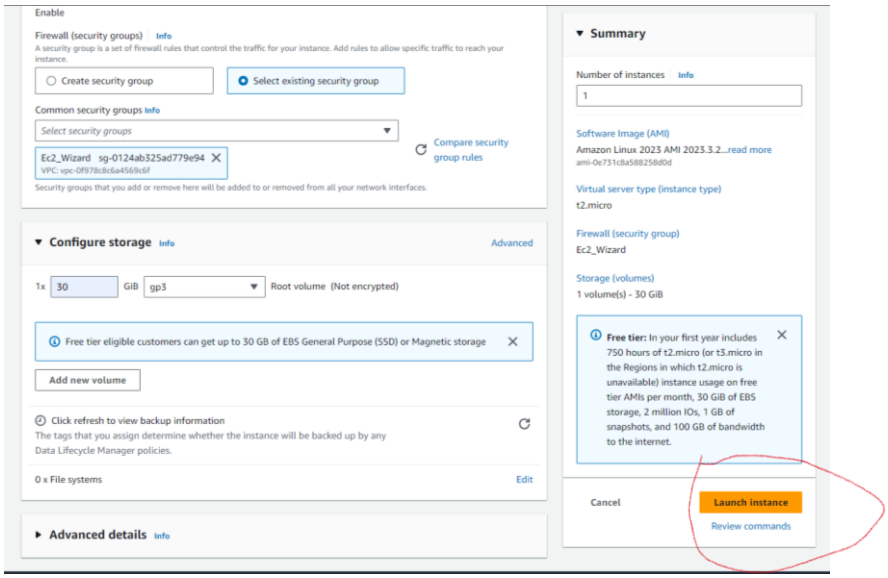
Creating Instance

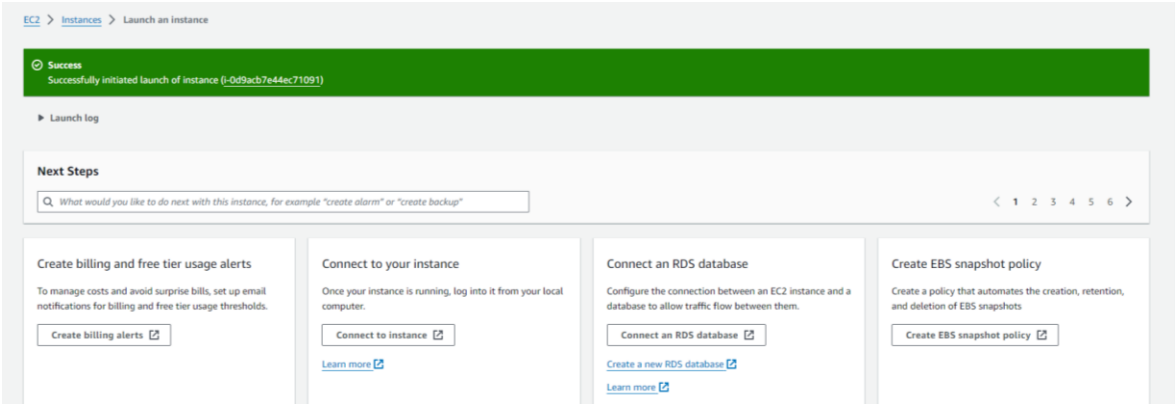


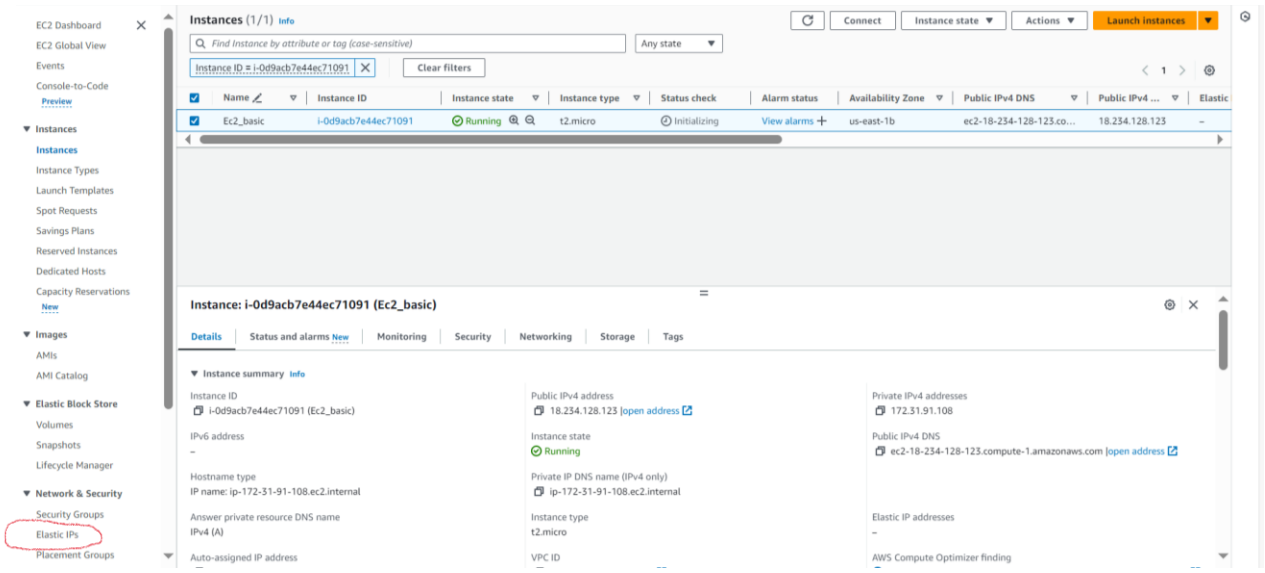


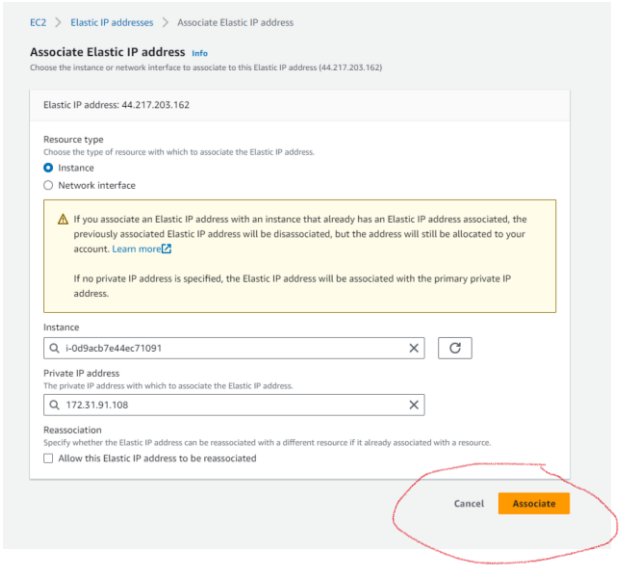

Create key pair
Key pair name
Key pairs allow you to connect to your instance securely.
Newbie
The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.
Key pair type
RSA
RSA encrypted private and public key pair
ED25519
ED25519 encrypted private and public key pair
Private key file format
.pem
For use with OpenSSH
.ppk
For use with PuTTY
When prompted, store the private key in a secure and accessible location on your computer. You will need it later to connect to your instance. Learn more
Cancel
Create key pair

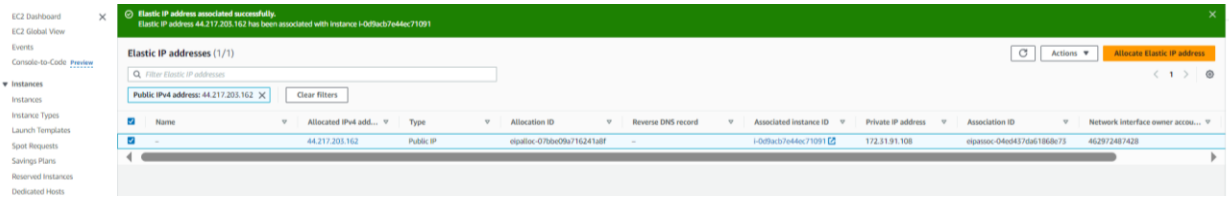

Key pair (login) Info
You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.
Key pair name - required
Newbie
Create new key pair
Network settings Info
Edit
Network Info
vpc-0f978c8c6a4569c6f
Subnet Info
No preference (Default subnet in any availability zone)
Auto-assign public IP Info
Enable
Firewall (security groups) Info
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
Common security groups Info
Select security groups
Ec2_Wizard sg-0124ab325ad779e94
VPC: vpc-0f978c8c6a4569c6f
Compare security group rules
Security groups that you add or remove here will be added to or removed from all your network interfaces.
Summary
Number of instances Info
1
Software Image (AMI)
Amazon Linux 2023 AMI 2023.3.2...read more
ami-0e731c8a588258d0d
Virtual server type (instance type)
t2.micro
Firewall (security group)
Ec2_Wizard
Storage (volumes)
1 volume(s) - 30 GiB
Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet.
Cancel
Launch instance
Review commands


Enable
Firewall (security groups) Info
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
Common security groups Info
Select security groups
Ec2_Wizard sg-0124ab325ad779e94
VPC: vpc-0f978c8c6a4569c6f
Compare security group rules
Security groups that you add or remove here will be added to or removed from all your network interfaces.
Configure storage Info
Advanced
1x 30 GiB gp3 Root volume (Not encrypted)
Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage
Add new volume
Click refresh to view backup information
The tags that you assign determine whether the instance will be backed up by any Data Lifecycle Manager policies.
0 x File systems
Edit
Advanced details Info
Summary
Number of instances Info
1
Software Image (AMI)
Amazon Linux 2023 AMI 2023.3.2...read more
ami-0e731c8a588258d0d
Virtual server type (instance type)
t2.micro
Firewall (security group)
Ec2_Wizard
Storage (volumes)
1 volume(s) - 30 GiB
Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet.
Cancel
Launch instance
Review commands

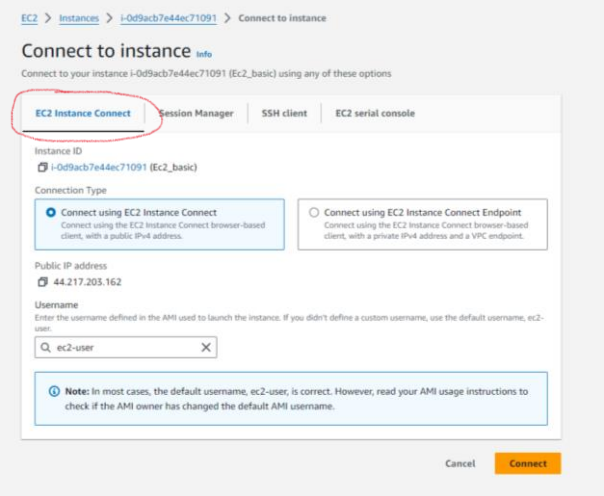

EC2 > Instances > Launch an instance
Success
Successfully initiated launch of instance (i-0d9acb7e44ec71091)
Launch log
Next Steps
What would you like to do next with this instance, for example "create alarm" or "create backup"
1 2 3 4 5 6
Create billing and free tier usage alerts
To manage costs and avoid surprise bills, set up email notifications for billing and free tier usage thresholds.
Create billing alerts
Connect to your instance
Once your instance is running, log into it from your local computer.
Connect to instance
Learn more
Connect an RDS database
Configure the connection between an EC2 instance and a database to allow traffic flow between them.
Connect an RDS database
Create a new RDS database
Learn more
Create EBS snapshot policy
Create a policy that automates the creation, retention, and deletion of EBS snapshots
Create EBS snapshot policy

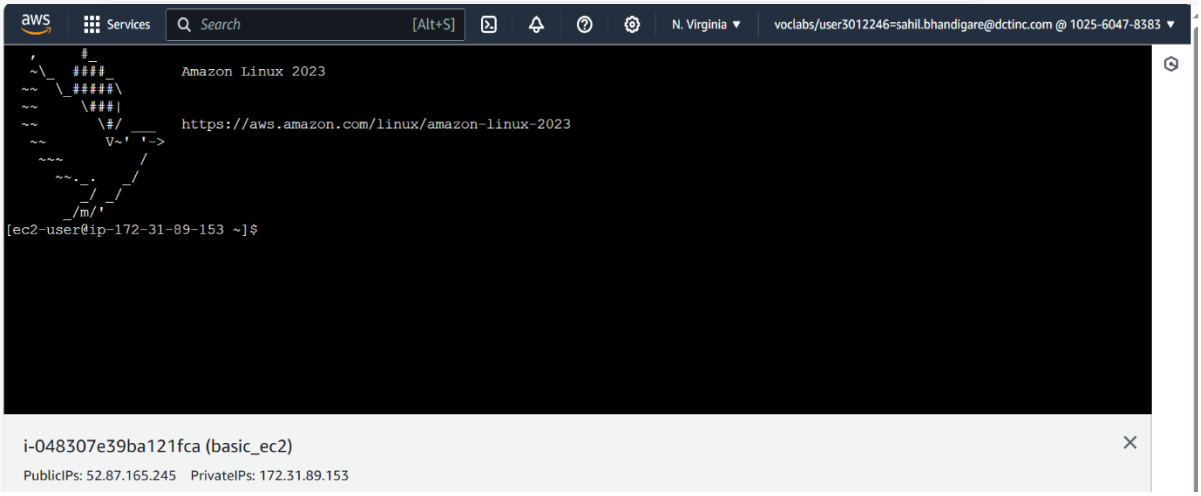

EC2 Dashboard
EC2 Global View
Events
Console-to-Code
Preview
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations
New
Images
AMIs
AMI Catalog
Elastic Block Store
Volumes
Snapshots
Lifecycle Manager
Network & Security
Security Groups
Elastic IPs
Placement Groups
Instances (1/1) Info
Find Instance by attribute or tag (case-sensitive)
Any state
Instance ID = i-0d9acb7e44ec71091
Clear filters
Connect
Instance state
Actions
Launch instances
Name
Instance ID
Instance state
Instance type
Status check
Alarm status
Availability Zone
Public IPv4 DNS
Public IPv4 ...
Elastic
Ec2_basic
i-0d9acb7e44ec71091
Running
t2.micro
Initializing
View alarms
us-east-1b
ec2-18-234-128-123.co...
18.234.128.123
Instance: i-0d9acb7e44ec71091 (Ec2_basic)
Details
Status and alarms New
Monitoring
Security
Networking
Storage
Tags
Instance summary Info
Instance ID
i-0d9acb7e44ec71091 (Ec2_basic)
IPv6 address
-
Hostname type
IP name: ip-172-31-91-108.ec2.internal
Answer private resource DNS name
IPv4 (A)
Auto-assigned IP address
Public IPv4 address
18.234.128.123 |open address
Instance state
Running
Private IP DNS name (IPv4 only)
ip-172-31-91-108.ec2.internal
Instance type
t2.micro
VPC ID
Private IPv4 addresses
172.31.91.108
Public IPv4 DNS
ec2-18-234-128-123.compute-1.amazonaws.com |open address
Elastic IP addresses
-
AWS Compute Optimizer finding


EC2 > Elastic IP addresses > Associate Elastic IP address
Associate Elastic IP address Info
Choose the instance or network interface to associate to this Elastic IP address (44.217.203.162)
Elastic IP address: 44.217.203.162
Resource type
Choose the type of resource with which to associate the Elastic IP address.
Instance
Network interface
If you associate an Elastic IP address with an instance that already has an Elastic IP address associated, the previously associated Elastic IP address will be disassociated, but the address will still be allocated to your account. Learn more
If no private IP address is specified, the Elastic IP address will be associated with the primary private IP address.
Instance
i-0d9acb7e44ec71091
Private IP address
The private IP address with which to associate the Elastic IP address.
172.31.91.108
Reassociation
Specify whether the Elastic IP address can be reassociated with a different resource if it already associated with a resource.
Allow this Elastic IP address to be reassociated
Cancel
Associate


Elastic IP address associated successfully.
Elastic IP address 44.217.203.162 has been associated with instance i-0d9acb7e44ec71091
EC2 Dashboard
EC2 Global View
Events
Console-to-Code Preview
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Elastic IP addresses (1/1)
Actions
Allocate Elastic IP address
Public IPv4 address: 44.217.203.162
Clear filters
Name
Allocated IPv4 add...
Type
Allocation ID
Reverse DNS record
Associated instance ID
Private IP address
Association ID
Network interface owner accou...
44.217.203.162
Public IP
eipalloc-07bbe09a716241a8f
i-0d9acb7e44ec71091
172.31.91.108
eipassoc-04ed437da61868e73
462972487428

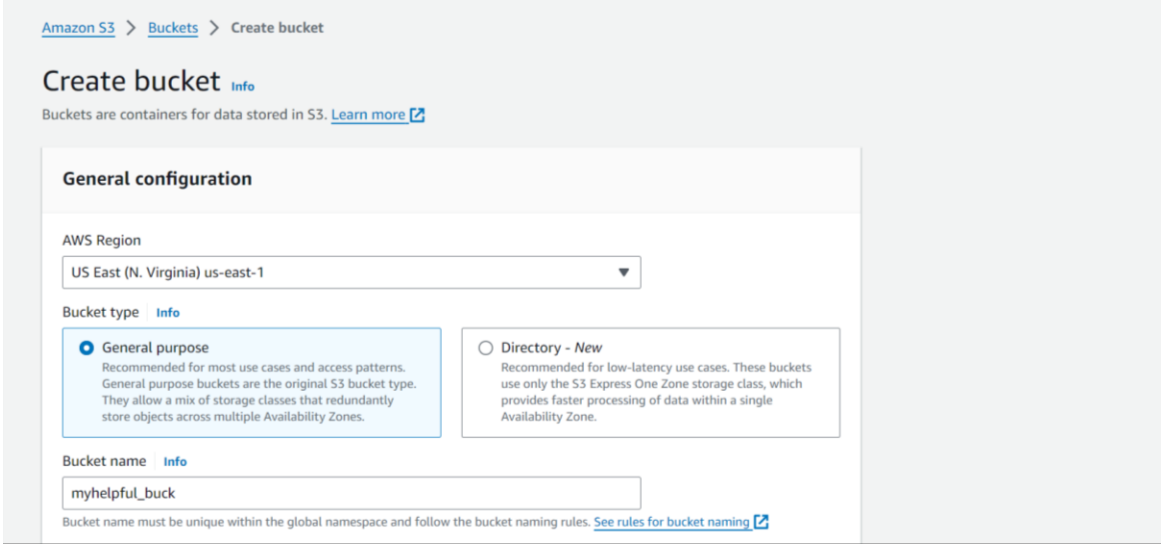
Connecting EC2 instance

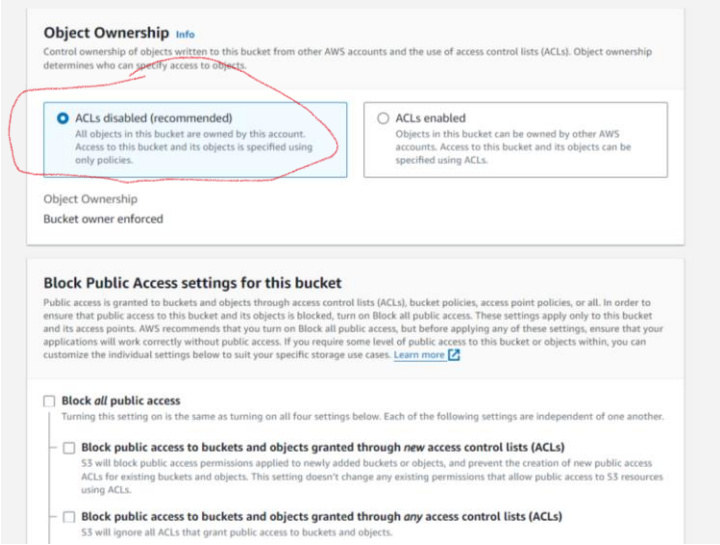


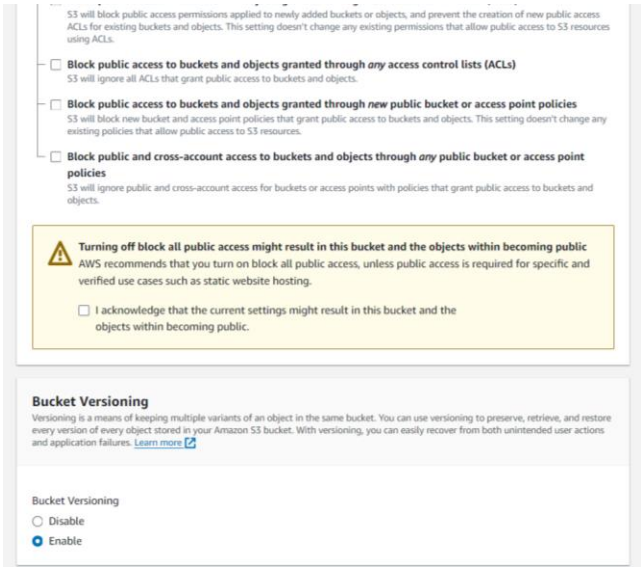


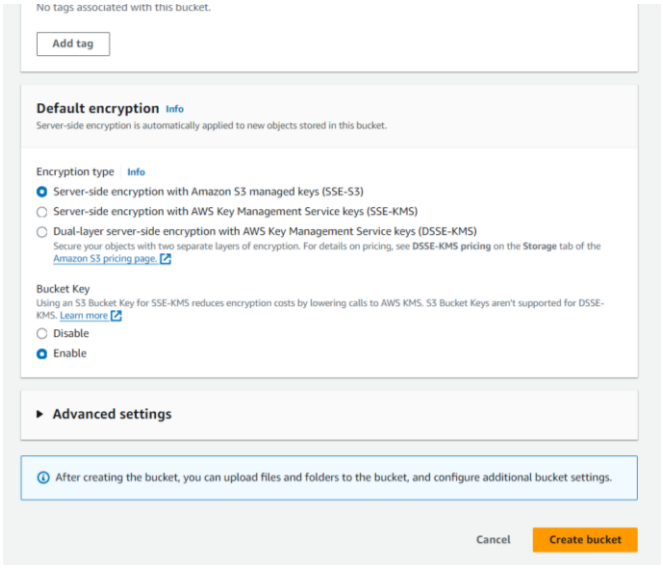
Q2. S3 Storage Fundamentals Lab

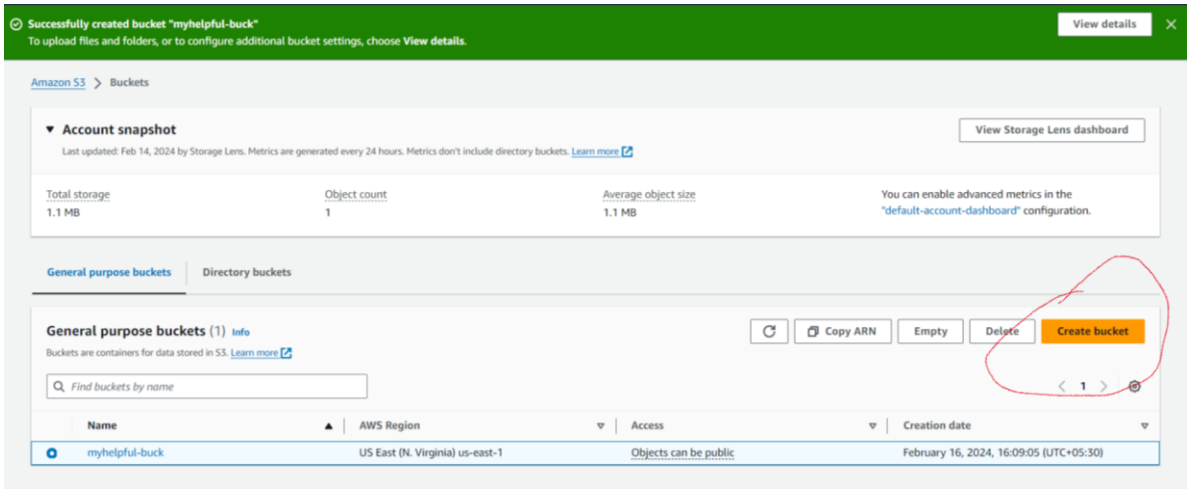
- **Objective**: To gain hands-on experience with Amazon S3 by performing basic storage operations.
- **Approach**: This lab involves creating an S3 bucket, uploading files to it, and setting up bucket policies for access control. Students will explore the S3 management console, learn about object storage, and understand the concepts of buckets and objects.
- **Goal**: Students will understand how to use S3 for storing and managing data, learn about S3 security and permissions, and become familiar with S3's user interface.

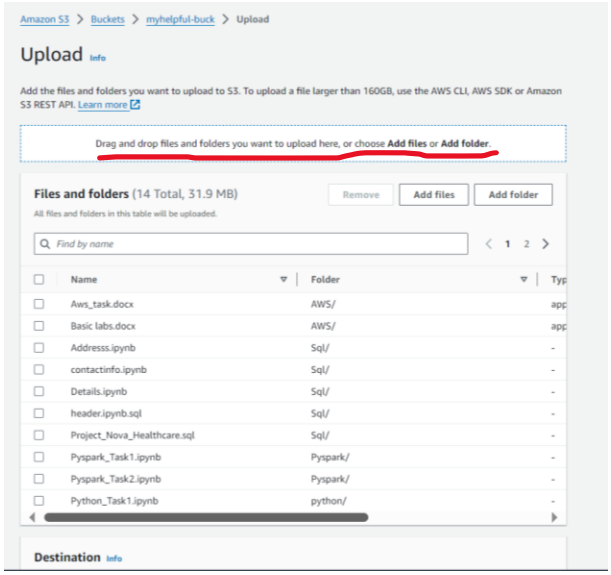


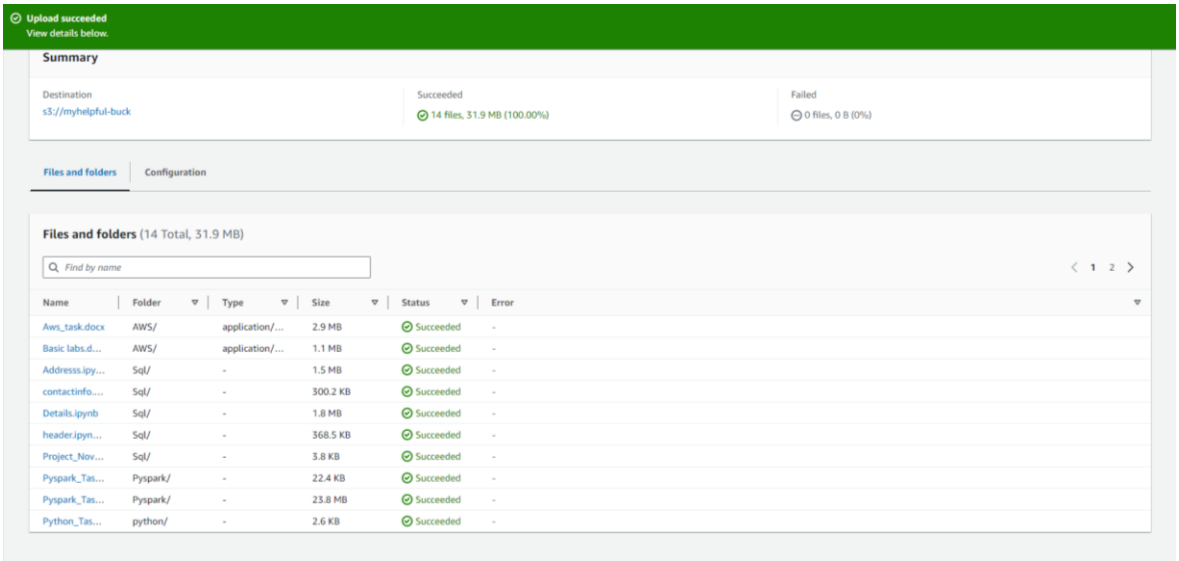



S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
Block public access to buckets 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.
Turning off block all public access might result in this bucket and the objects within becoming public
AWS recommends that you turn on block all public access, unless public access is required for specific and verified use cases such as static website hosting.
I acknowledge that the current settings might result in this bucket and the objects within becoming public.
Bucket Versioning
Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. Learn more
Bucket Versioning
Disable
Enable


No tags associated with this bucket.
Add tag
Default encryption Info
Server-side encryption is automatically applied to new objects stored in this bucket.
Encryption type Info
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.
Cancel
Create bucket


Successfully created bucket "myhelpful-buck"
To upload files and folders, or to configure additional bucket settings, choose View details.
View details
Amazon S3 > Buckets
Account snapshot
Last updated: Feb 14, 2024 by Storage Lens. Metrics are generated every 24 hours. Metrics don't include directory buckets. Learn more
View Storage Lens dashboard
Total storage
1.1 MB
Object count
1
Average object size
1.1 MB
You can enable advanced metrics in the "default-account-dashboard" configuration.
General purpose buckets
Directory buckets
General purpose buckets (1) Info
Buckets are containers for data stored in S3. Learn more
Copy ARN
Empty
Delete
Create bucket
Find buckets by name
Name
AWS Region
Access
Creation date
myhelpful-buck
US East (N. Virginia) us-east-1
Objects can be public
February 16, 2024, 16:09:05 (UTC+05:30)


Amazon S3 > Buckets > myhelpful-buck > Upload
Upload Info
Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDK or Amazon S3 REST API. Learn more
Drag and drop files and folders you want to upload here, or choose Add files or Add folder.
Files and folders (14 Total, 31.9 MB)
All files and folders in this table will be uploaded.
Remove
Add files
Add folder
Find by name
Name
Folder
Aws_task.docx
AWS/
Basic labs.docx
AWS/
Addresss.ipynb
Sql/
contactinfo.ipynb
Sql/
Details.ipynb
Sql/
header.ipynb.sql
Sql/
Project_Nova_Healthcare.sql
Sql/
Pyspark_Task1.ipynb
Pyspark/
Pyspark_Task2.ipynb
Pyspark/
Python_Task1.ipynb
python/
Destination Info



Q3. IAM Users and Roles Lab

- **Objective**: To understand AWS Identity and Access Management (IAM) by creating and managing users, groups, and roles.
- **Approach**: Students will create new IAM users, assign them to groups, and apply policies to manage permissions. The lab will also involve creating roles for AWS services and understanding the use of IAM roles for cross-service access.
- **Goal**: Students will learn about user and permission management in AWS, the importance of roles for security and best practices for IAM.

IAM stands for Identity Access Management. Its purpose if to create sub-users under 1 root users and give them specific permissions according to their roles. This helps in Access Control, Least Privilege Principle, Security, Managing and Delegating the tasks and getting the tasks done with a single account.