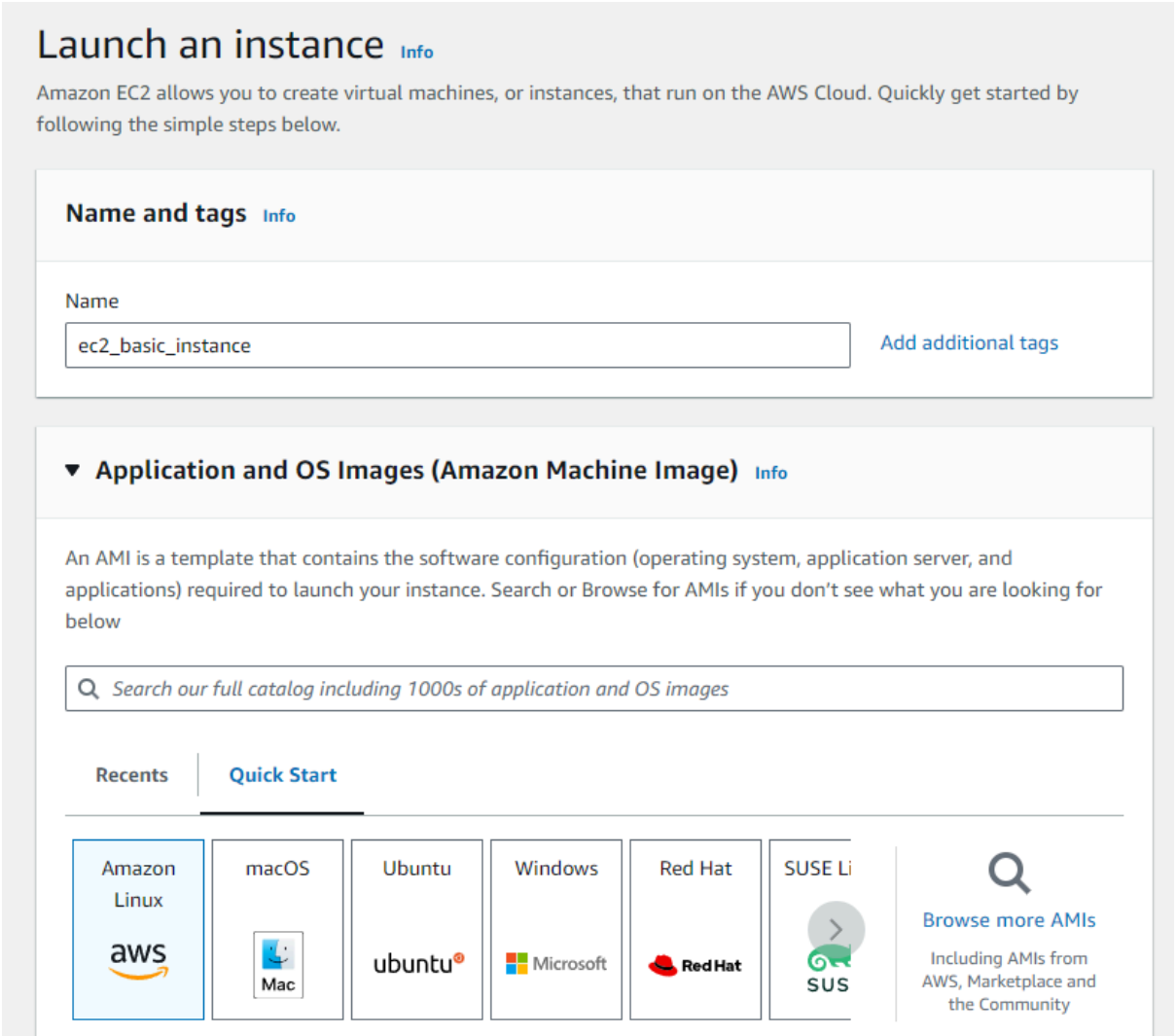
1. **EC2 Basics Lab**
    - **Objective**: To understand the process of setting up and managing an Amazon EC2 instance.
    - **Approach**: Students will start by launching a new EC2 instance, selecting an appropriate instance type and configuring the instance details. They will then create and configure 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.

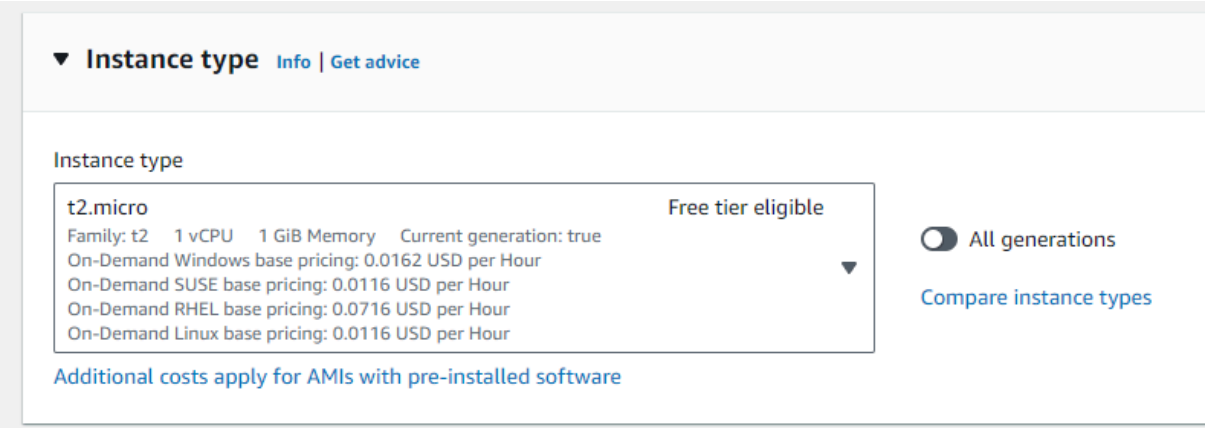
Process:

- Open Aws Console inside learners lab
- Search and find EC2 feature and launch instance

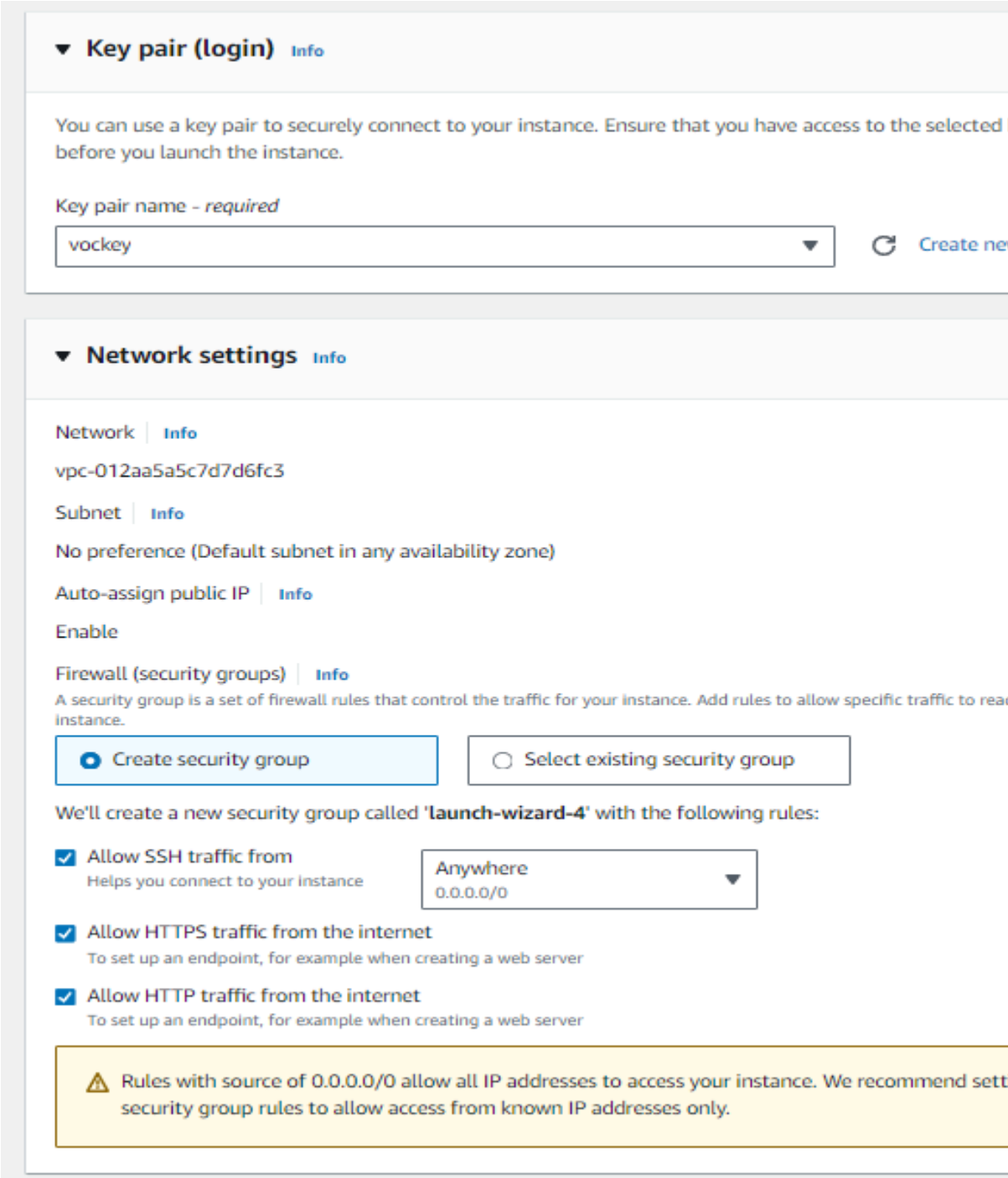


- Name was given and Os images was assigned as linux

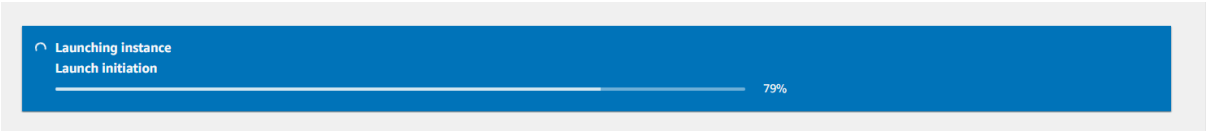
- T2 micro was selected as instance type to cut down cost for the bootcamp



  - Keyvalue was given and security was assigned



- Finally launching



- Allocating elastic IP

Allocate Elastic IP address Info

Elastic IP address settings Info

Network border group Info

us-east-1

Public IPv4 address pool

- Amazon's pool of IPv4 addresses
- Public IPv4 address that you bring to your AWS account with BYOIP. (option disabled because no pools found) Learn more
- 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) Learn more

Global static IP addresses

AWS Global Accelerator can provide global static IP addresses that are announced worldwide using anycast from AWS edge locations. This can help improve the availability and latency for your user traffic by using the Amazon global network. Learn more

Create accelerator

Tags - *optional*

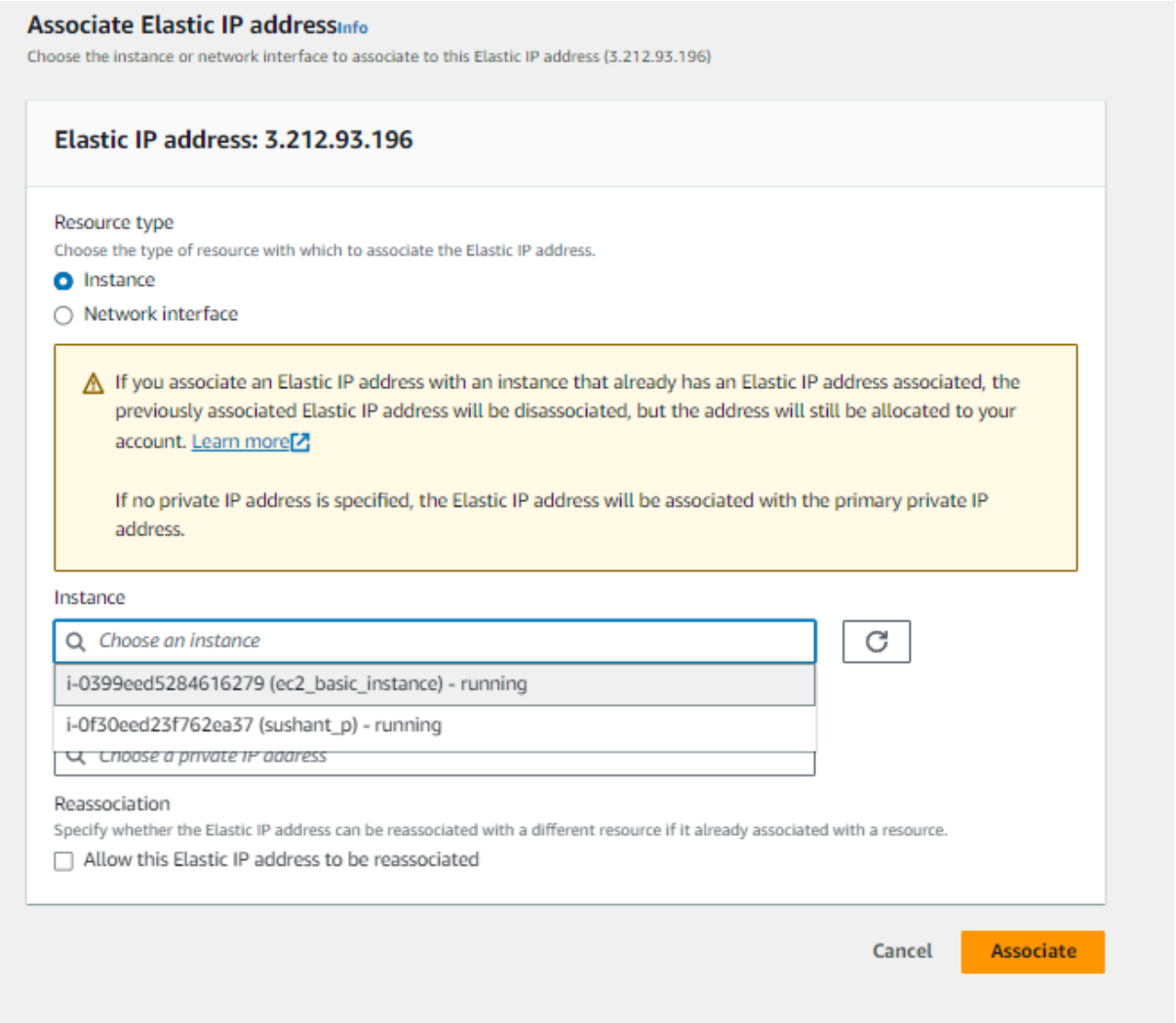
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

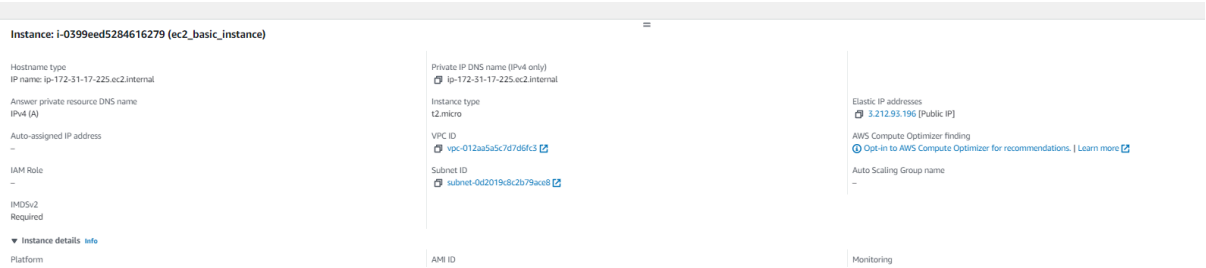
No tags associated with the resource.

Add new tag

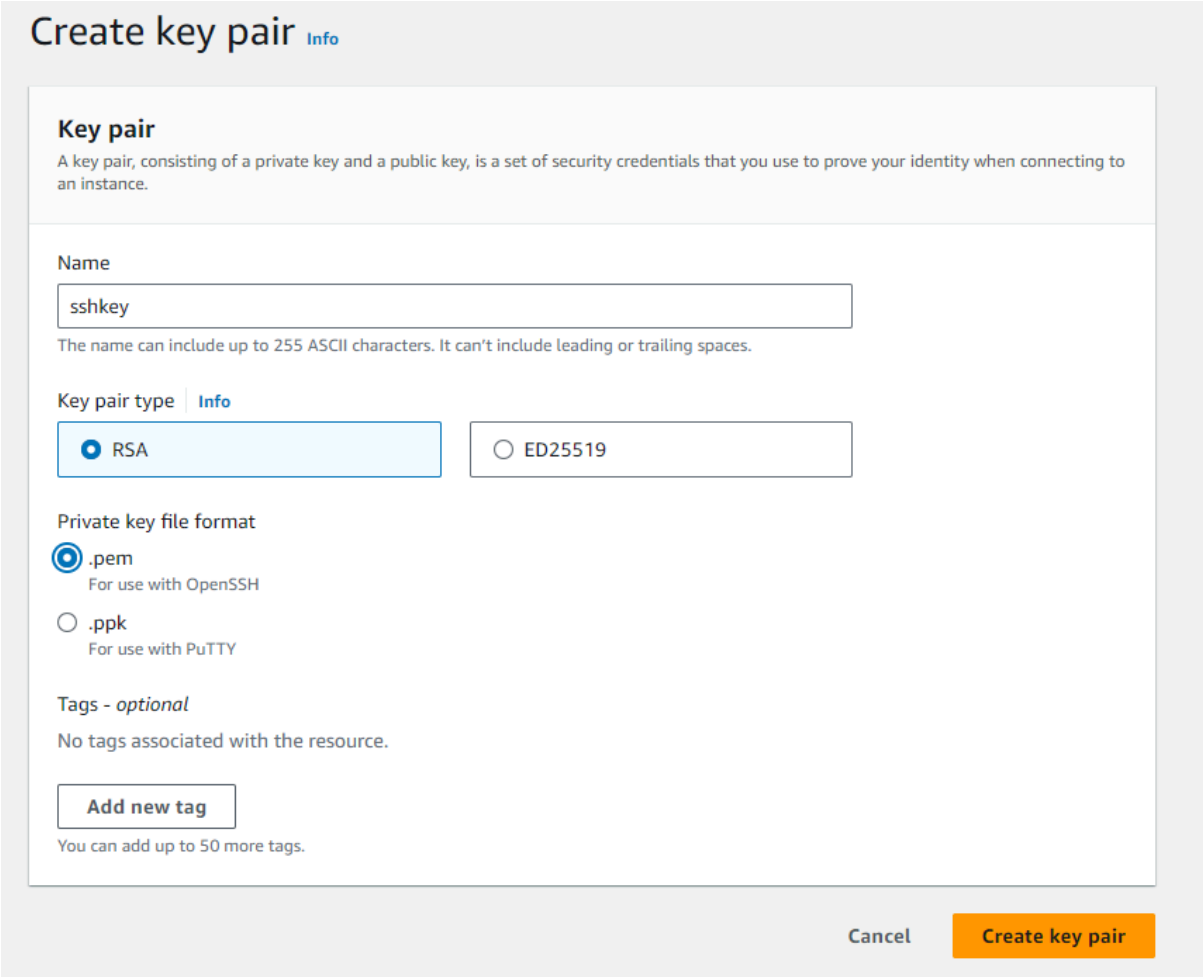
You can add up to 50 more tag

Cancel Allocate





- Connecting to the instance via SSH



chmod 400 /path/to/your/private-key-file.pem

ssh -i /path/to/your/private-key-file.pem ec2-user@your-instance-public-dns

AWS CloudShell

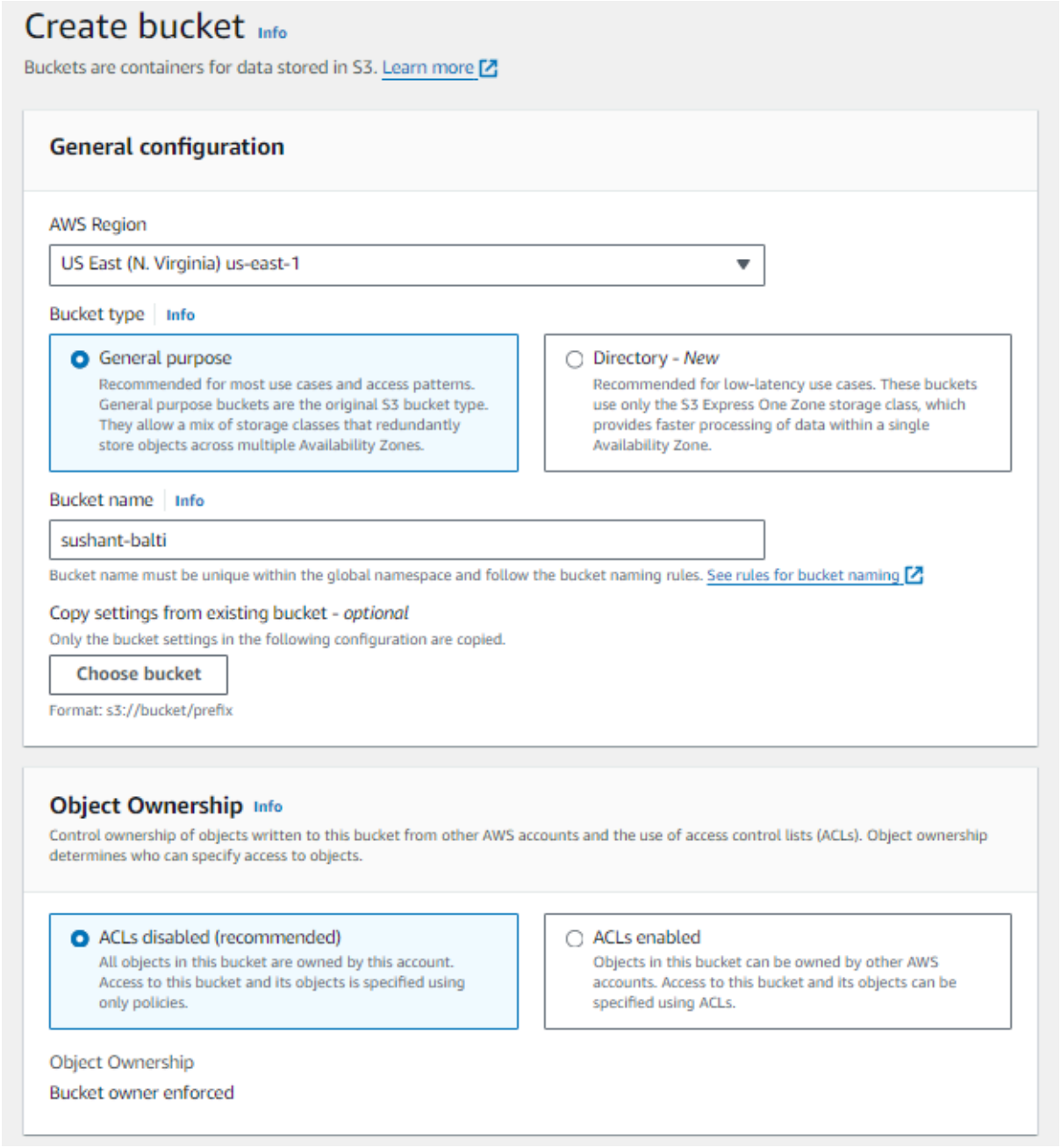
us-east-1

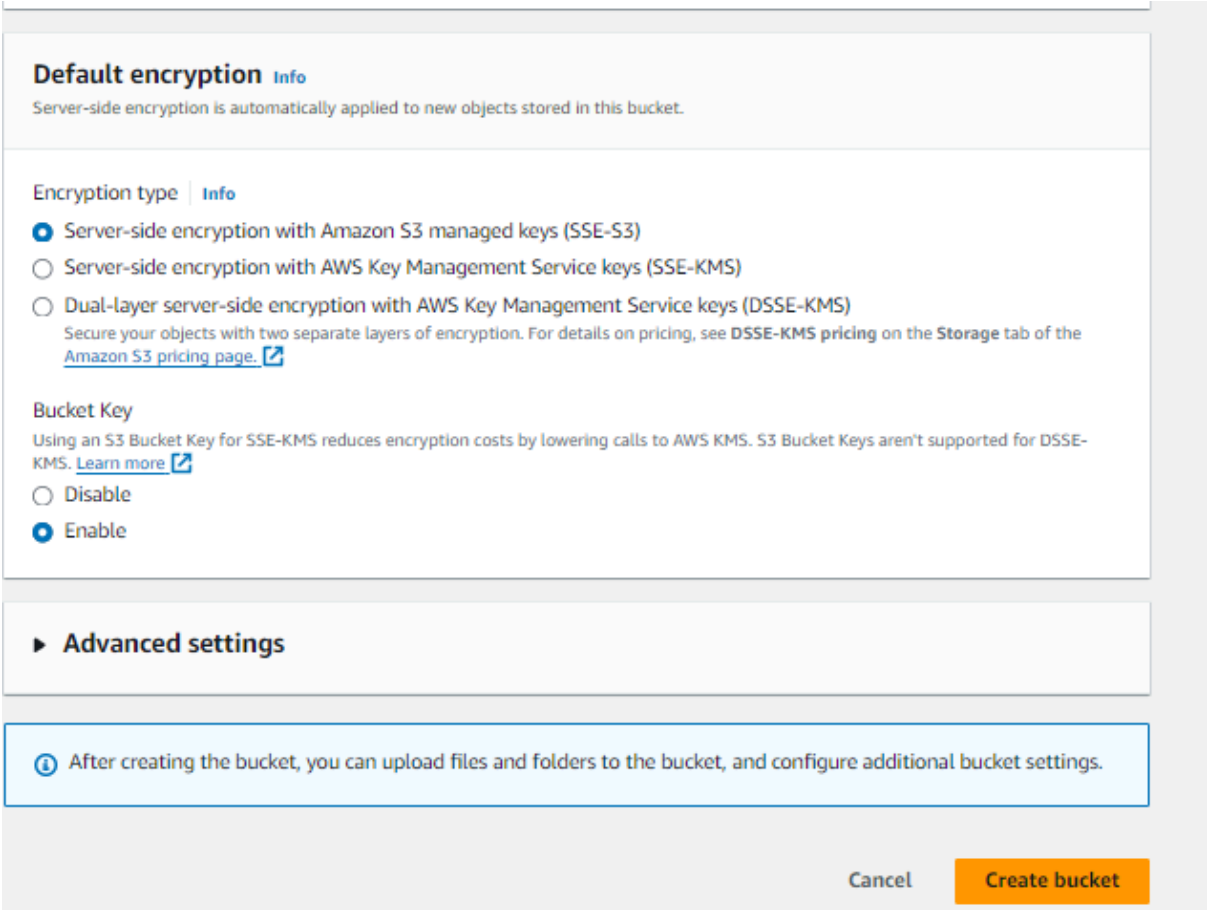
```
[cloudshell-user@ip-10-132-44-197 ~]$ chmod 400 new-key.pem
[cloudshell-user@ip-10-132-44-197 ~]$ ssh -i "new-key.pem" ec2-user@ec2-3-212-93-196.compute-1.amazonaws.com

ssh: connect to host ec2-3-212-93-196.compute-1.amazonaws.com port 22: Connection timed out
[cloudshell-user@ip-10-132-44-197 ~]$
[cloudshell-user@ip-10-132-44-197 ~]$ ssh -i "new-key.pem" ec2-user@ec2-3-212-93-196.compute-1.amazonaws.com
^C
[cloudshell-user@ip-10-132-44-197 ~]$ ssh -i "new-key.pem" ec2-user@ec2-54-90-80-47.compute-1.amazonaws.com
The authenticity of host 'ec2-54-90-80-47.compute-1.amazonaws.com (54.90.80.47)' can't be established.
ED25519 key fingerprint is SHA256:f5nrVihjJ4SJuCsMAeGzhH8I9rsLyzdpEu15jW+HrsE.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'ec2-54-90-80-47.compute-1.amazonaws.com' (ED25519) to the list of known hosts.
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Tue Feb 20 10:28:40 2024 from 18.206.107.27
[ec2-user@ip-172-31-25-67 ~]$ whoami
ec2-user
[ec2-user@ip-172-31-25-67 ~]$
```

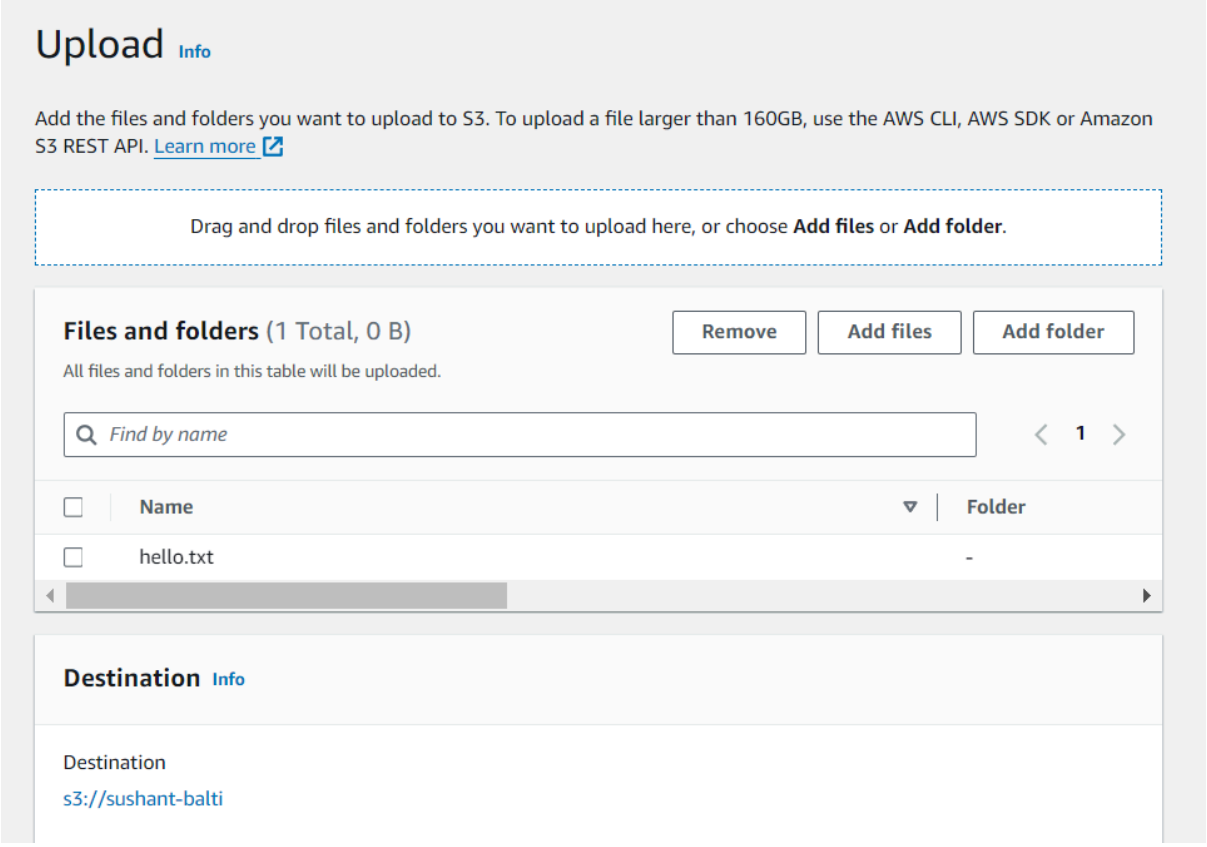
2. S3 Storage Fundamentals Lab

- **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.

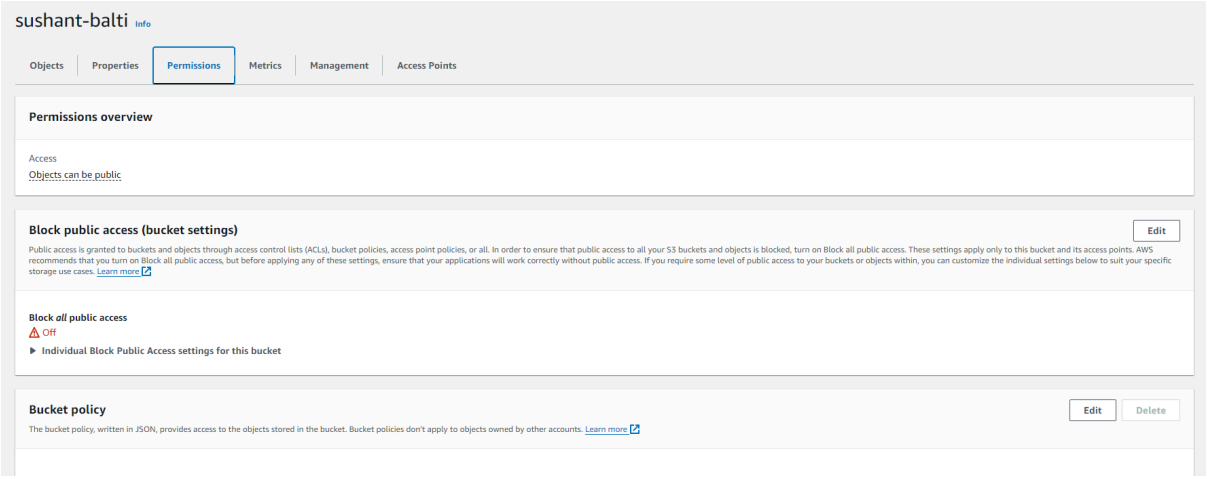


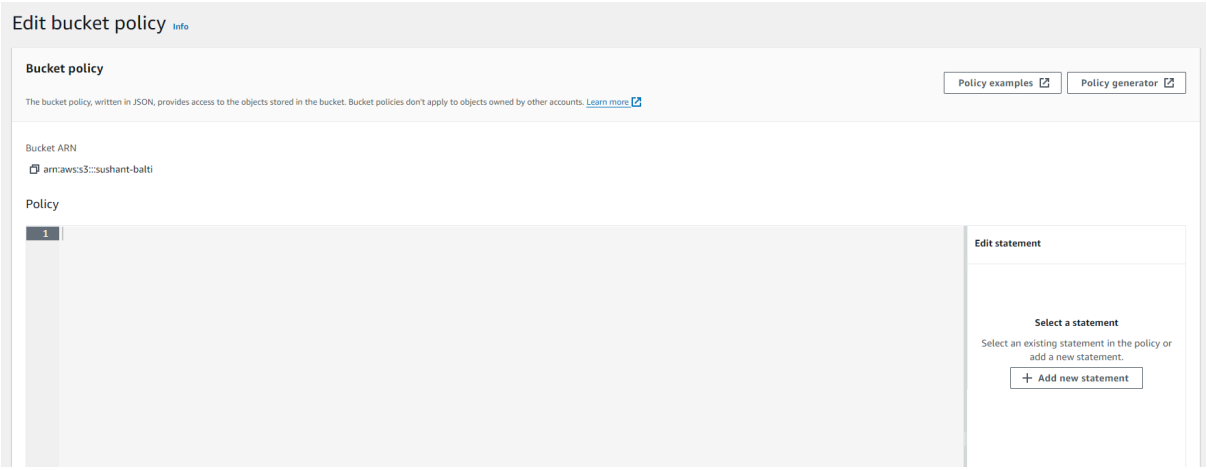


Uploading files to the bucket.

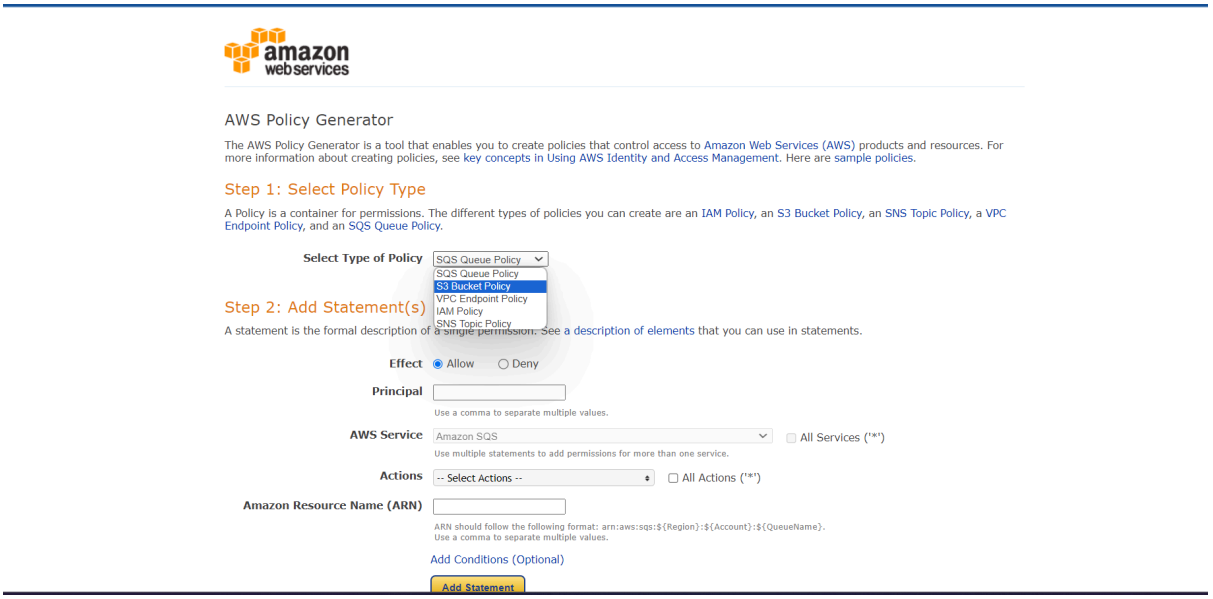


Setting up bucket policies for access control.





Click policy generator



AWS Policy Generator

The AWS Policy Generator is a tool that enables you to create policies that control access to Amazon Web Services (AWS) products and resources. For more information about creating policies, see key concepts in Using AWS Identity and Access Management. Here are sample policies.

Step 1: Select Policy Type

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:::sushant-balti

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

Add Conditions (Optional)

Add Statement

Now pasting the generated 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

arn:aws:s3:::sushant-balti

Policy

```
1  {
2    "Id": "Policy1708535146418",
3    "Version": "2012-10-17",
4    "Statement": [
5      {
6        "Sid": "Stmt1708535145290",
7        "Action": "s3:*",
8        "Effect": "Allow",
9        "Resource": "arn:aws:s3:::sushant-balti",
10       "Principal": "*"
11     }
12   ]
13 }
```

Accessing the uploaded content

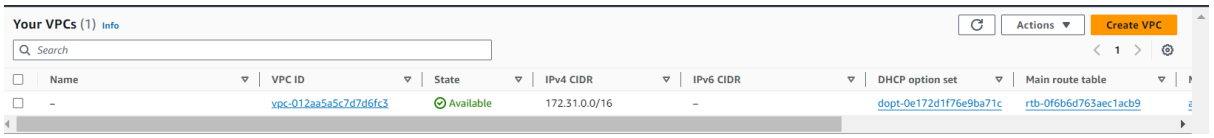
sushant-balti.s3.us-east-1.amazonaws.com/hello.html

This is a heading

This is a paragraph.

3. **VPC Configuration Lab**
    - **Objective**: To understand the fundamentals of AWS networking through the configuration of a Virtual Private Cloud (VPC).
    - **Approach**: Students will create a new VPC, add subnets, set up an Internet Gateway, and configure route tables. The lab might also include setting up a simple EC2 instance within this VPC to demonstrate how resources are deployed in a custom network environment.
    - **Goal**: By the end of this lab, students should be able to create and configure a VPC, understand subnetting, and the role of route tables and internet gateways in AWS.

Creating a new VPC.



VPC > Your VPCs > Create VPC

Create VPC Info

A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such a

VPC settings

Resources to create Info

Create only the VPC resource or the VPC and other networking resources.

- ○ VPC only
- ● VPC and more

Name tag auto-generation Info

Enter a value for the Name tag. This value will be used to auto-generate Name tags for all resources in the VPC.

☑ Auto-generate

basiclab

IPv4 CIDR block Info

Determine the starting IP and the size of your VPC using CIDR notation.

10.0.0.0/16 65,536 IPs

CIDR block size must be between /16 and /28.

IPv6 CIDR block Info

- ● No IPv6 CIDR block
- ○ Amazon-provided IPv6 CIDR block

Tenancy Info

Default

Number of Availability Zones (AZs) Info

Choose the number of AZs in which to provision subnets. We recommend at least two AZs for high availability.

1	2	3

▶ Customize AZs

Number of public subnets Info

The number of public subnets to add to your VPC. Use public subnets for web applications that need to be publicly accessible over the internet.

0	1

Number of private subnets Info

The number of private subnets to add to your VPC. Use private subnets to secure backend resources that don't need public access.

0	1	2

▶ Customize subnets CIDR blocks

NAT gateways ($) Info

Choose the number of Availability Zones (AZs) in which to create NAT gateways. Note that there is a charge for each NAT gateway

None	In 1 AZ	1 per AZ

VPC endpoints Info

Endpoints can help reduce NAT gateway charges and improve security by accessing S3 directly from the VPC. By default, full access policy is used. You can customize this policy at any time.

None	S3 Gateway

▼ **Customize subnets CIDR blocks**

Public subnet CIDR block in us-east-1a

10.0.0.0/24 256 IPs

Private subnet CIDR block in us-east-1a

10.0.1.0/24 256 IPs

NAT gateways ($) Info

Choose the number of Availability Zones (AZs) in which to create NAT gateways. Note that there is a charge for each NAT gateway

None	In 1 AZ	1 per AZ

VPC endpoints Info

Endpoints can help reduce NAT gateway charges and improve security by accessing S3 directly from the VPC. By default, full access policy is used. You can customize this policy at any time.

None	S3 Gateway

Create VPC workflow

Wait for NAT Gateways to activate

70%

Details

- Create VPC: vpc-0e9fea6024ce8f27b
- Enable DNS hostnames
- Enable DNS resolution
- Verifying VPC creation: vpc-0e9fea6024ce8f27b
- Create S3 endpoint: vpce-0b33f11d7154ed7a0
- Create subnet: subnet-071aa08374f7720e2
- Create subnet: subnet-0ef1986e8d4dae2ee
- Create internet gateway: igw-09800f1d52e55189b
- Attach internet gateway to the VPC
- Create route table: rtb-0a71f9920ec0a1c5e
- Create route
- Associate route table
- Allocate elastic IP: eipalloc-0f49544c45410339f
- Create NAT gateway: nat-0972249f2a3242231
- Wait for NAT Gateways to activate
- Create route table
- Create route
- Associate route table
- Verifying route table creation
- Associate S3 endpoint with private subnet route tables: vpce-0b33f11d7154ed7a0

vpc-0e9fea6024ce8f27b / basiclab-vpc

Actions

Details Info

VPC ID vpc-0e9fea6024ce8f27b	State Available	DNS hostnames Enabled	DNS resolution Enabled
Tenancy Default	DHCP option set dopt-0e172d1f76e9ba71c	Main route table rtb-0a5fcad5c08c2b377	Main network ACL acl-0fce440351d314619
Default VPC No	IPv4 CIDR 10.0.0.0/16	IPv6 pool –	IPv6 CIDR (Network border group) –
Network Address Usage metrics Disabled	Route 53 Resolver DNS Firewall rule groups Failed to load rule groups	Owner ID 133852355281	

Adding subnets.

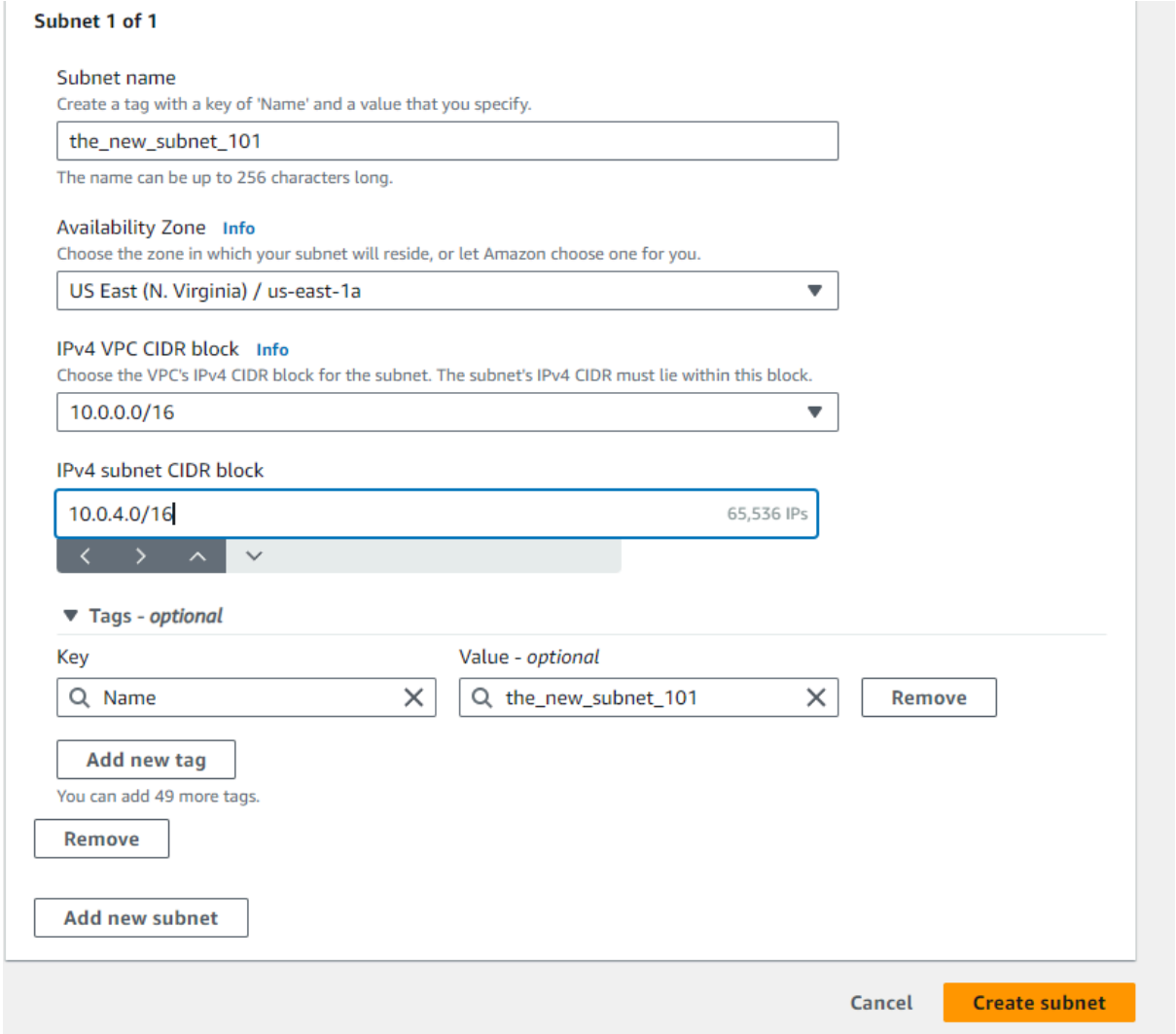
VPC dashboard
EC2 Global View
Filter by VPC:
Select a VPC
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only internet gateways
Carrier gateways
DHCP option sets
Elastic IPs

Subnets (6) Info

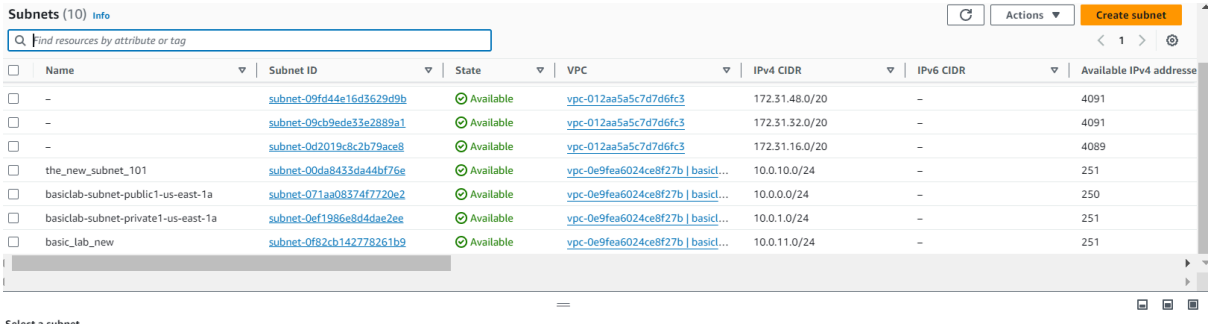
Actions | Create subnet

Find resources by attribute or tag

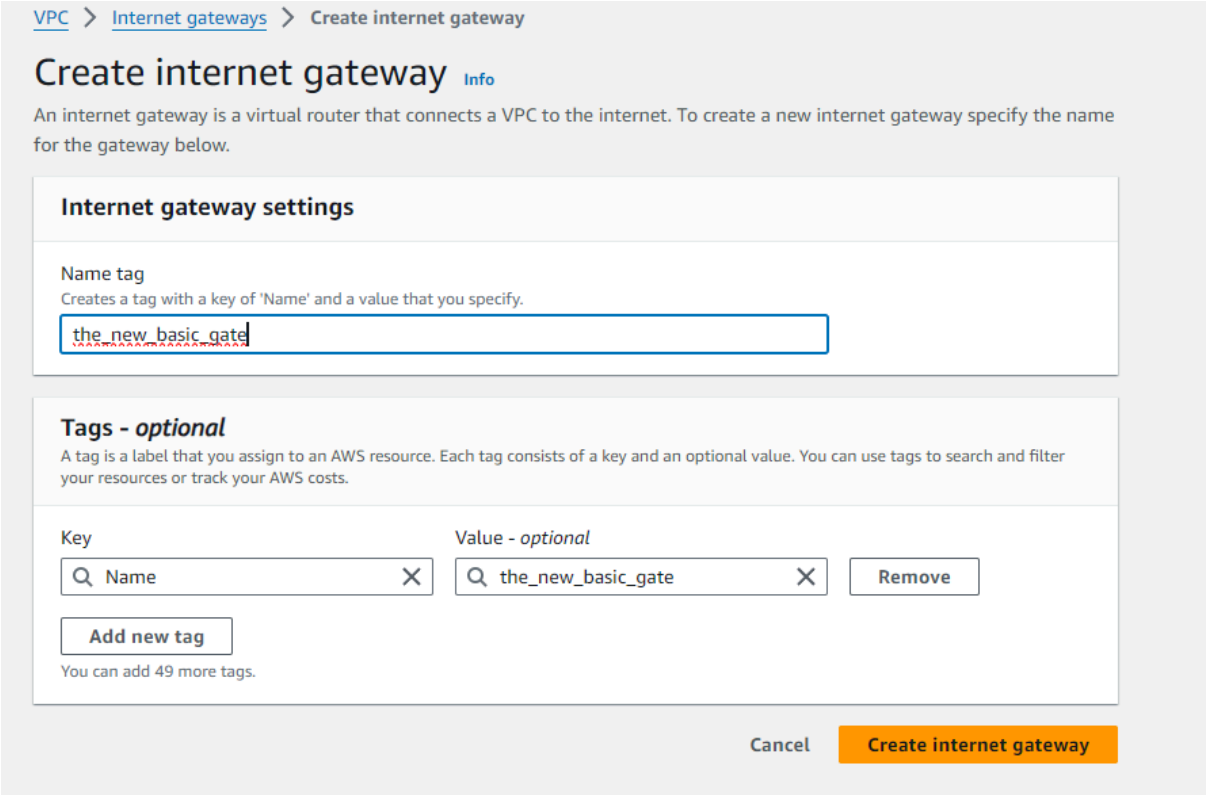
Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR	Available IPv4 addresse
–	subnet-0d18fa231dd2bb593	Available	vpc-012aa5a5c7d7d6fc3	172.31.64.0/20	–	4091
–	subnet-00bcbf13e09e72fcc	Available	vpc-012aa5a5c7d7d6fc3	172.31.80.0/20	–	4091
–	subnet-0da709092523209a9	Available	vpc-012aa5a5c7d7d6fc3	172.31.0.0/20	–	4091
–	subnet-09fd44e16d3629d9b	Available	vpc-012aa5a5c7d7d6fc3	172.31.48.0/20	–	4091
–	subnet-09cb9ede33e2889a1	Available	vpc-012aa5a5c7d7d6fc3	172.31.32.0/20	–	4091
–	subnet-0d2019c8c2b79ace8	Available	vpc-012aa5a5c7d7d6fc3	172.31.16.0/20	–	4089



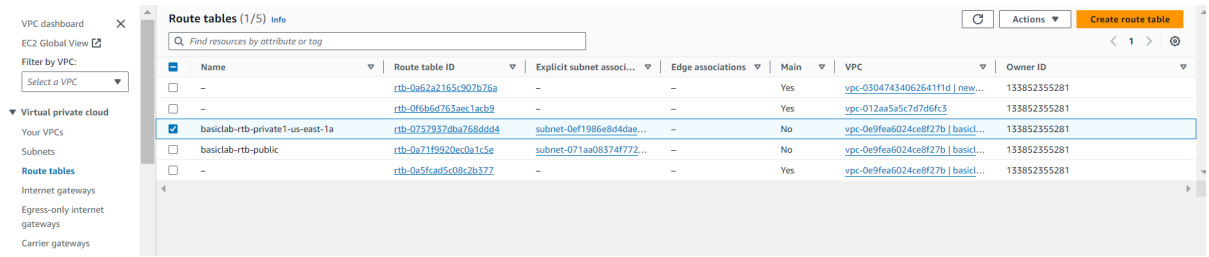
Create multiple subnets



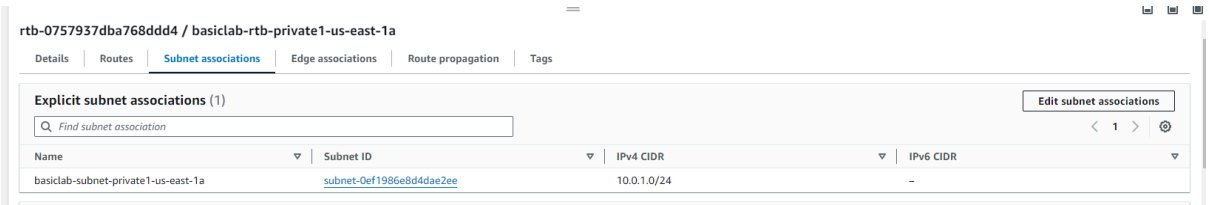
Setting up an Internet Gateway.



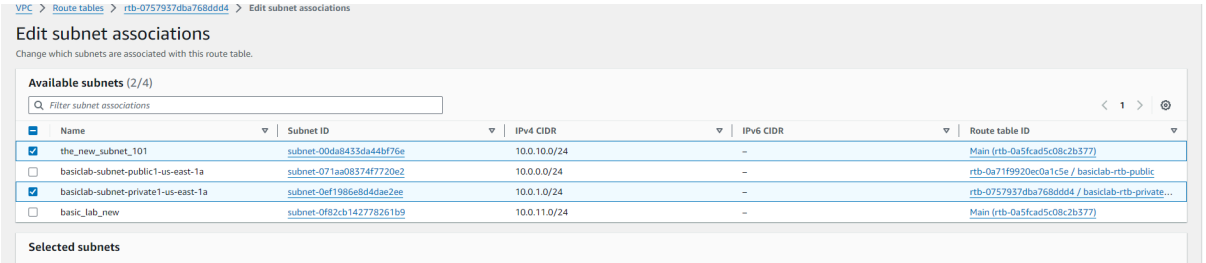
Configuring route tables.



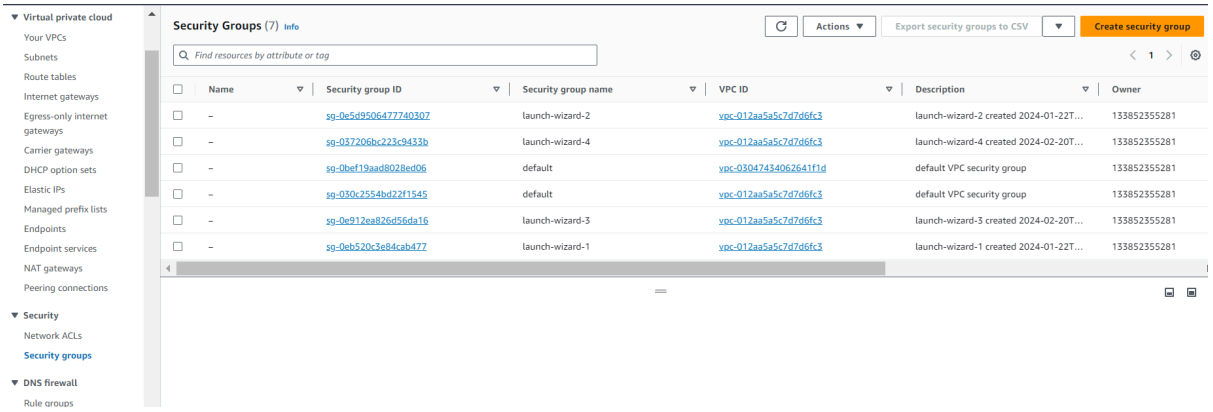
Select edit subnet association in the bottom panel

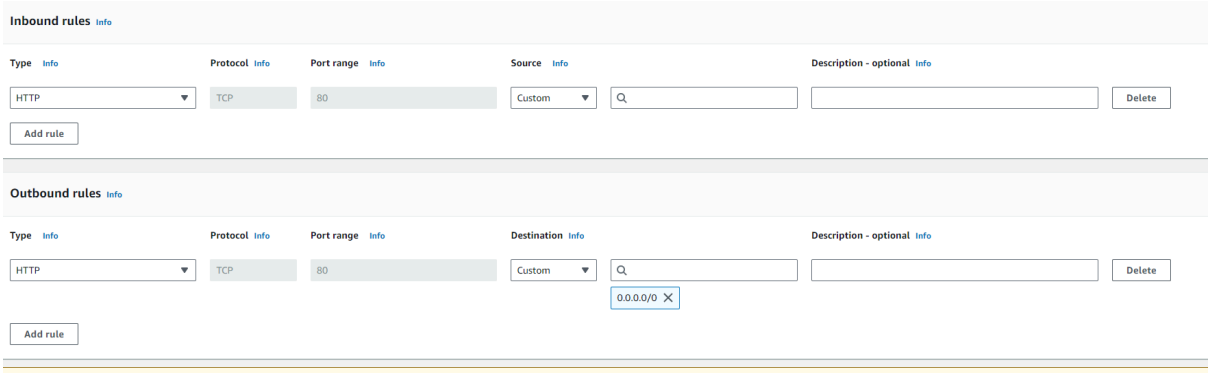


Select the new subnet too



Creating the security group





Setting up a simple EC2 instance within the VPC.

Network settings Info

VPC - *required* Info

vpc-0e9fea6024ce8f27b (basiclab-vpc)
10.0.0.0/16

Subnet Info

subnet-00da8433da44bf76e the_new_subnet_101
VPC: vpc-0e9fea6024ce8f27b Owner: 133852355281 Availability Zone: us-east-1a
IP addresses available: 251 CIDR: 10.0.10.0/24)

Create new subnet

Auto-assign public IP Info

Disable

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

vpc-security sg-0724c5cd84287e744
VPC: vpc-0e9fea6024ce8f27b

Compare security group rules

Security groups that you add or remove here will be added to or removed from all your network interfaces.

▶ **Advanced network configuration**

Instances (1) Info

Connect | Instance state | Actions | Launch instances

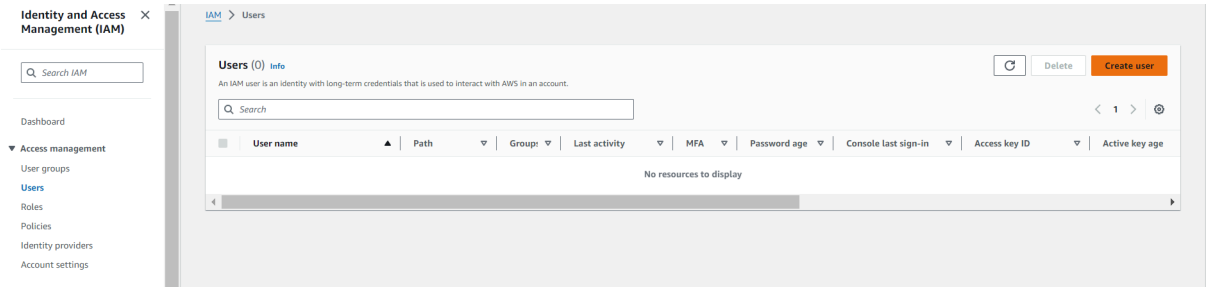
Find Instance by attribute or tag (case-sensitive) | Any state

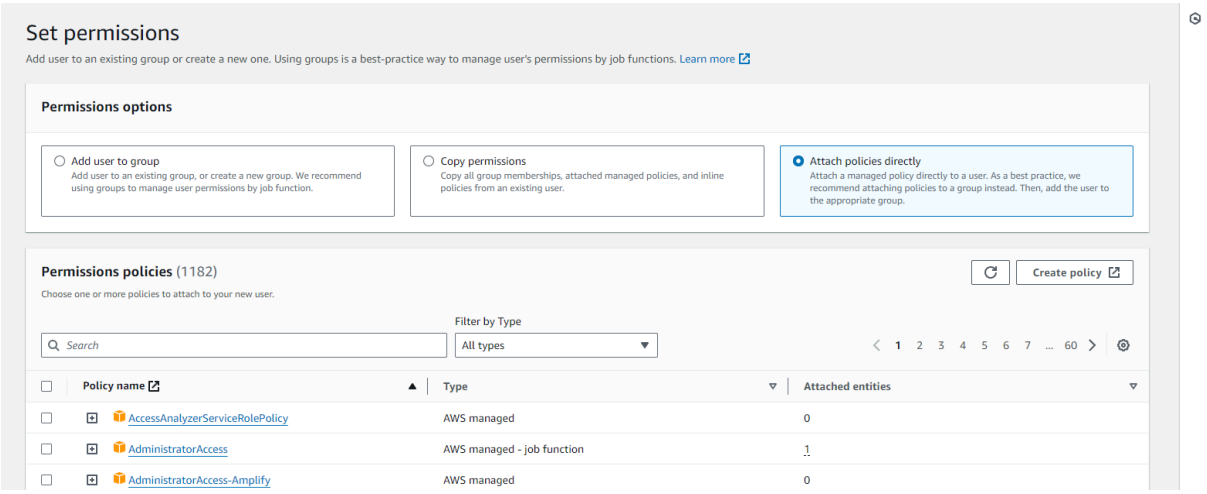
Instance ID = i-0aa85f6ee583fe7ea | Clear filters

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP
New VPC instance	i-0aa85f6ee583fe7ea	Running	t2.micro	2/2 checks passed	View alarms	us-east-1a	–	–	–

4. **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.

Creating new IAM users.





Review and create

Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.

User details

User name	Console password type	Require password reset
sushant	None	No

Permissions summary

1

Name	Type	Used as
No resources		

Tags - *optional*

Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.

No tags associated with the resource.

Add new tag

You can add up to 50 more tags.

Cancel | Previous | Create user