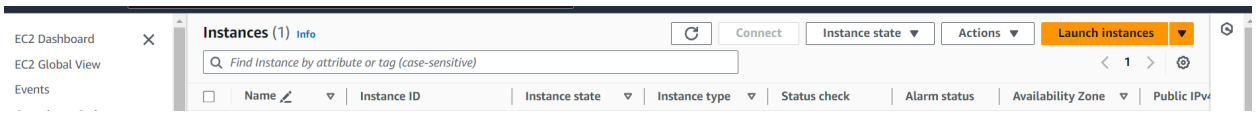
Basic Labs

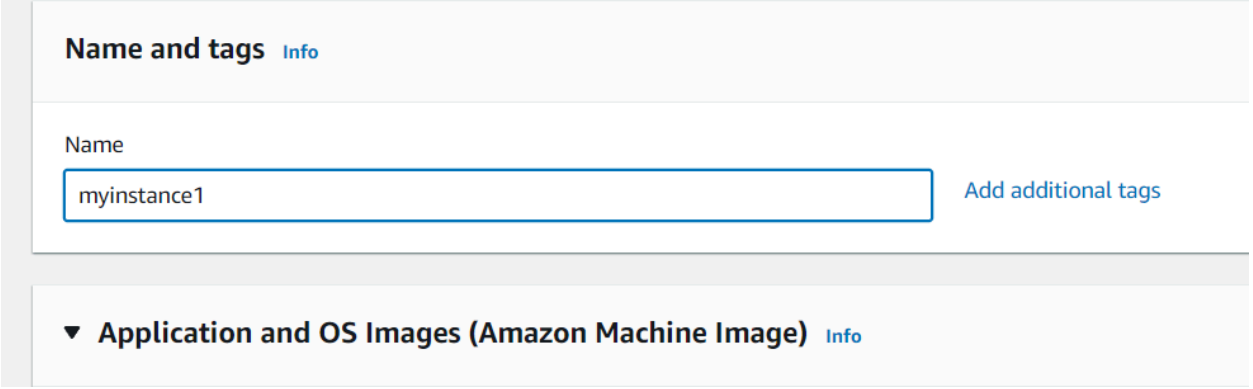
1. **EC2 Basics Lab**
    - **Objective**: To understand the process of setting up and managing an Amazon EC2 instance.
    - **Approach**: Students will start by launching a new EC2 instance, selecting an appropriate instance type and configuring the instance details. They will then create and configure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

EC2 Basics Lab:

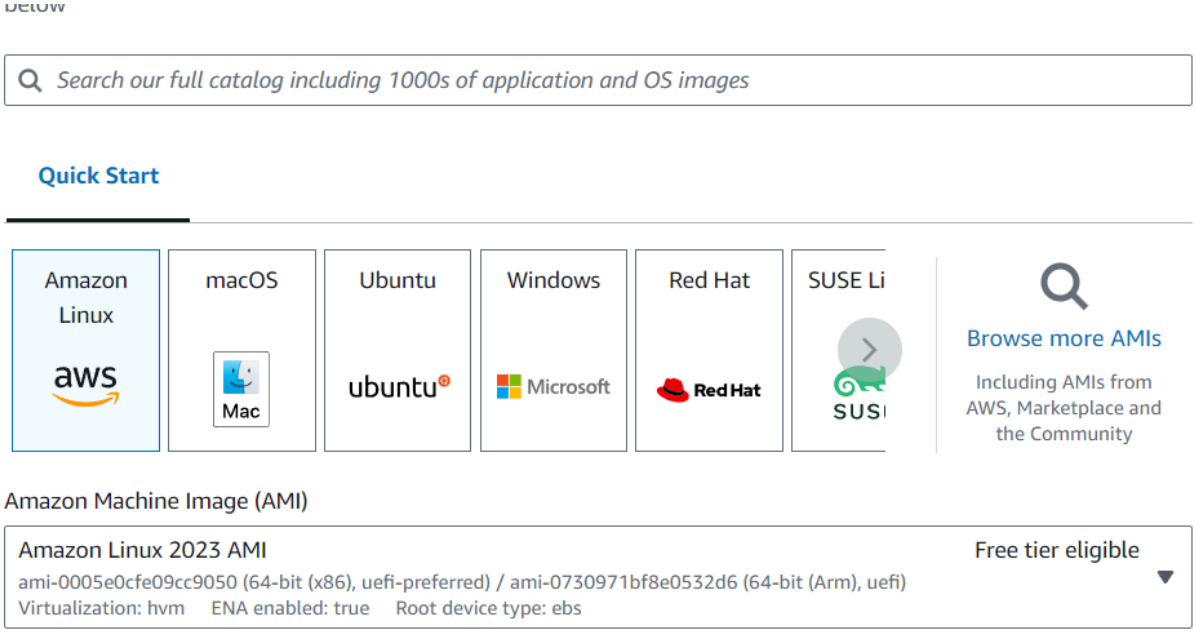
Launching EC2 instance:



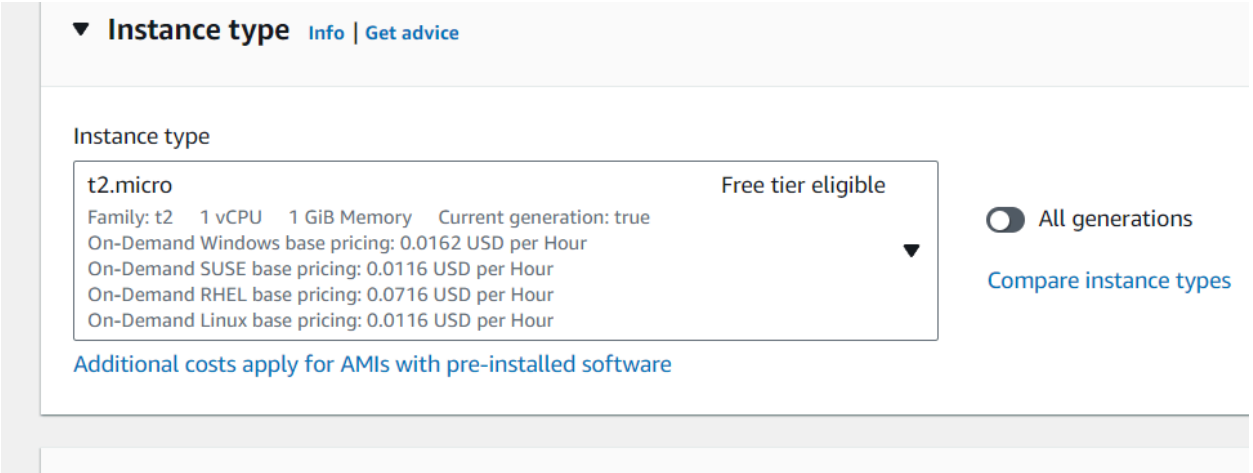
Add name of the instance:



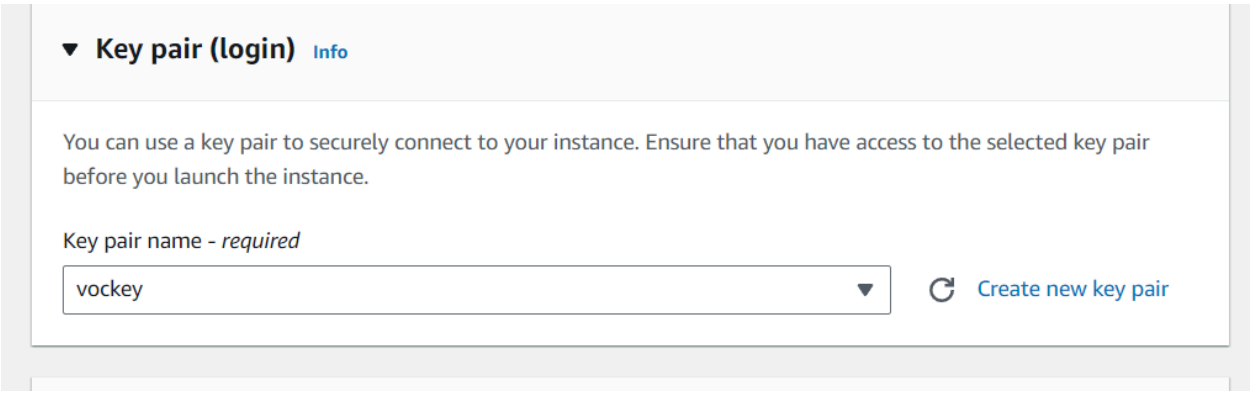
Select required AMI



Select instance type:



Select the default key pair, this will required to connect through the SSH and download the ppm file:



Create the security group:

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

We'll create a new security group called '**launch-wizard-2**' with the following rules:

- [x] Allow SSH traffic from
  Helps you connect to your instance
  Anywhere 0.0.0.0/0
- [ ] Allow HTTPS traffic from the internet
  To set up an endpoint, for example when creating a web server
- [ ] Allow HTTP traffic from the internet
  To set up an endpoint, for example when creating a web server

Required storage configuration:

Configure storage Info Advanced

1x 8 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

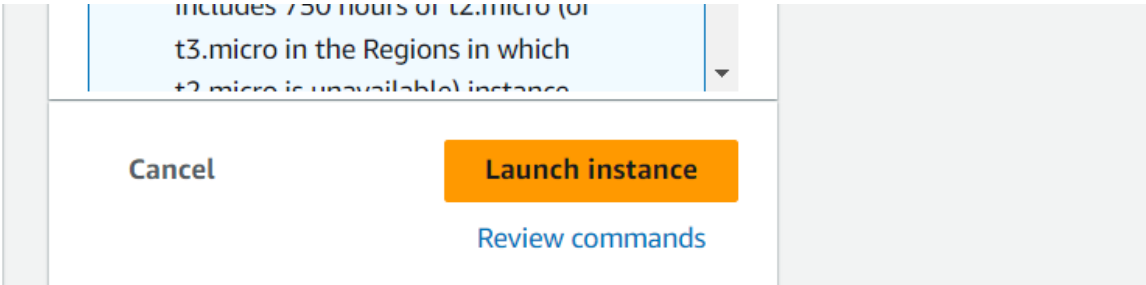
From the network setting disable assign public IP

Auto-assign public IP Info

Disable

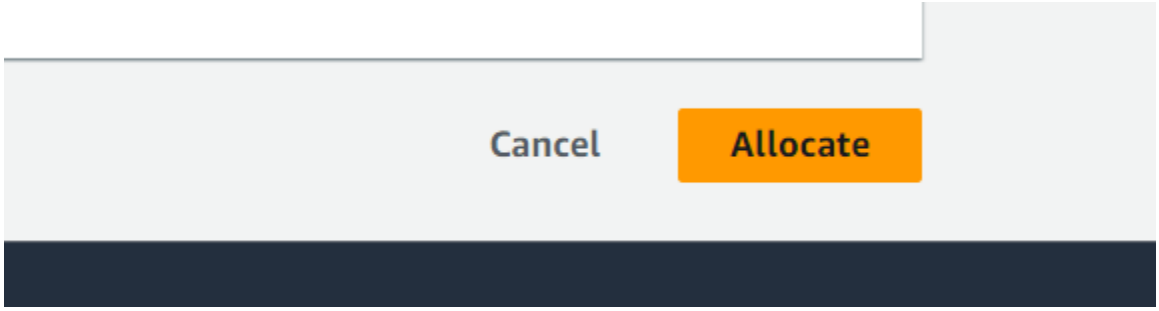
Firewall (security groups) Info

Launching the instance:

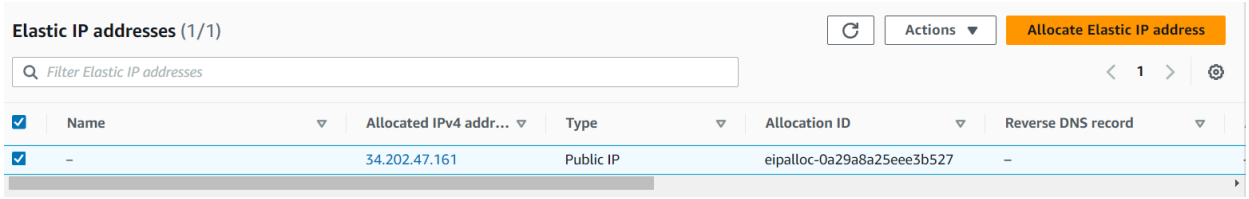


Waiting the instance to be running:

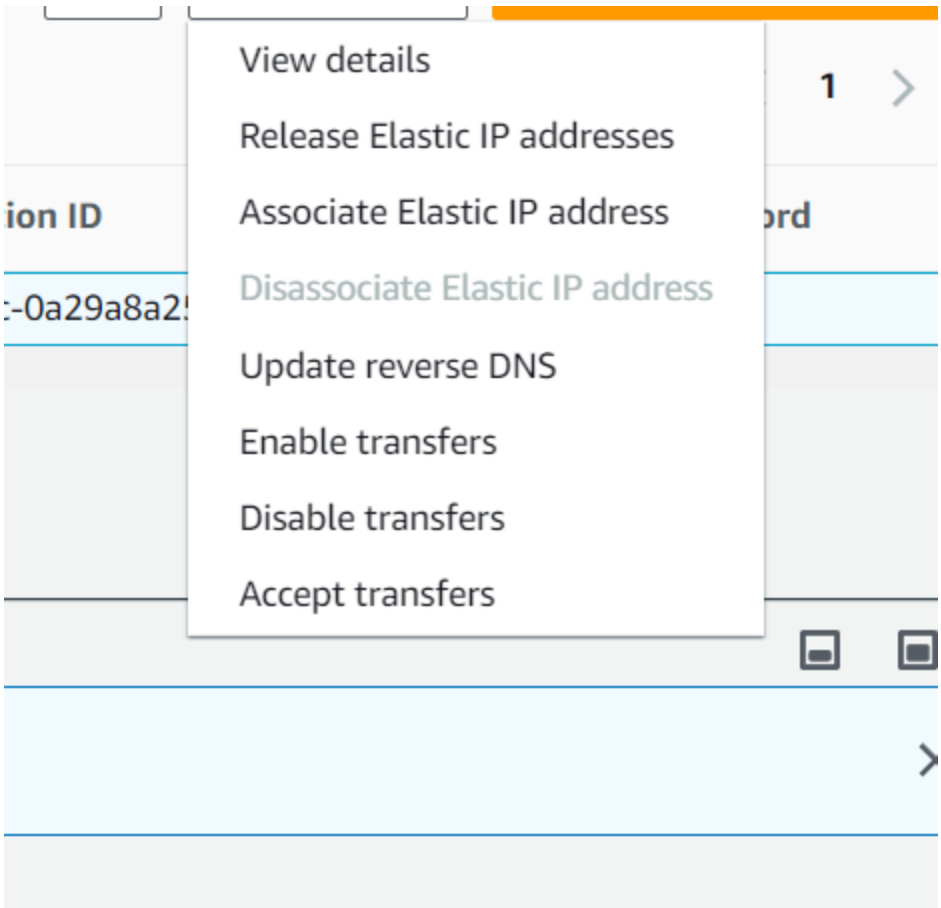
Allocate the default elastic IP:



Now select your allocated elastic IP:

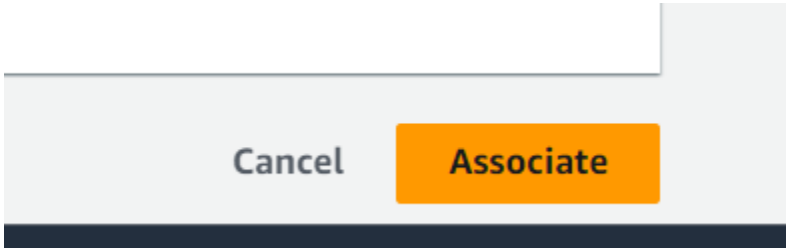


Go to action:
And choose associate elastic IP

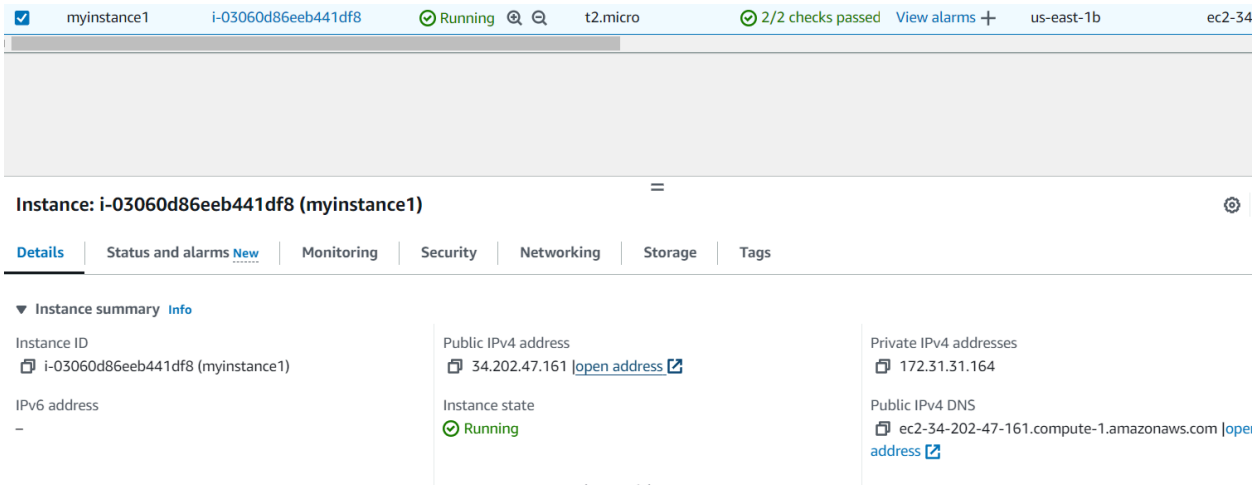


Choose your EC2 instance:

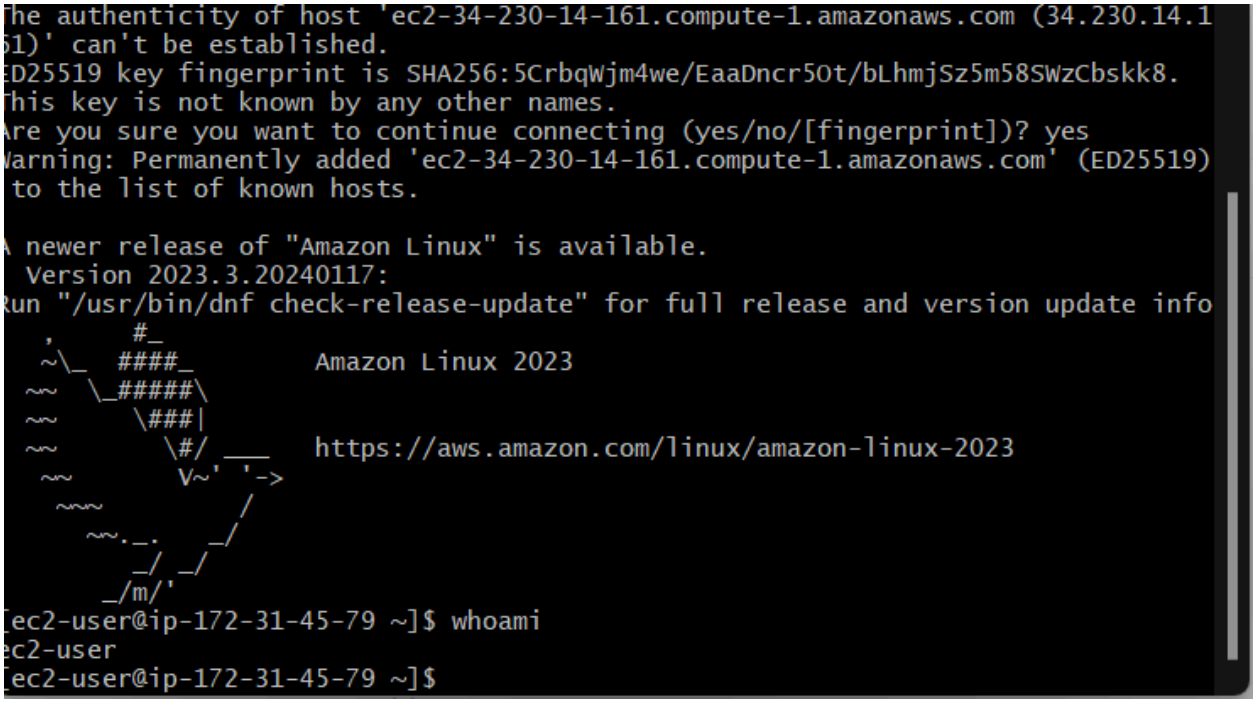
Then associate:



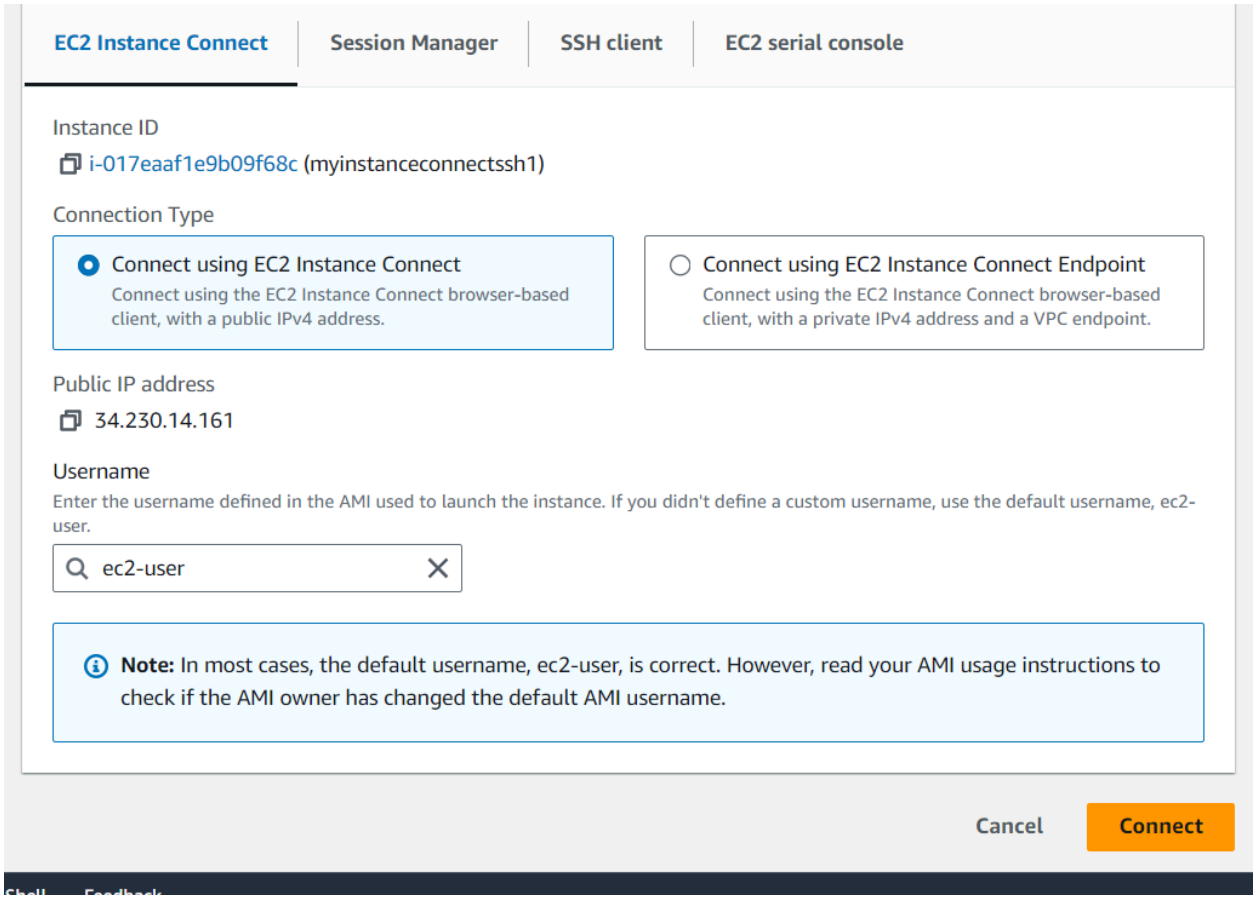
Go to the instance and choose it:



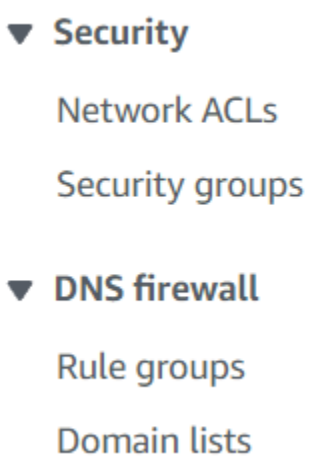
Now connecting through the ssh:

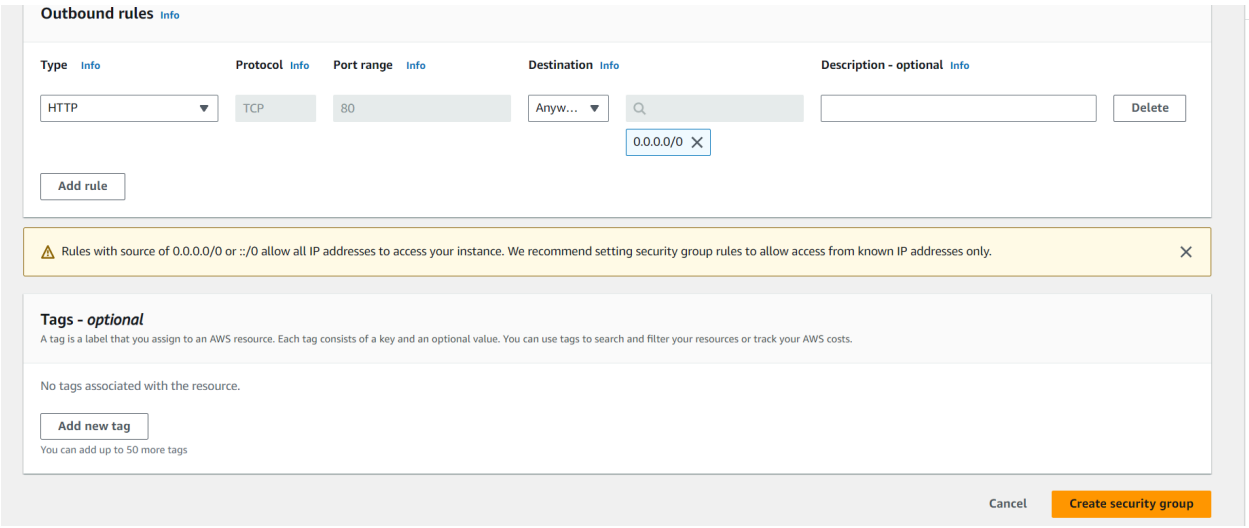


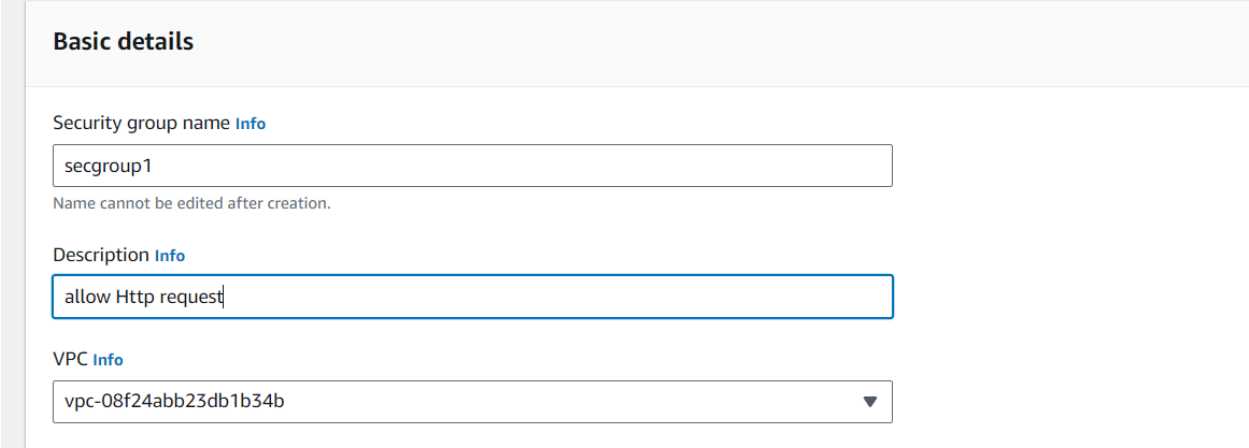
Connection through web browser:



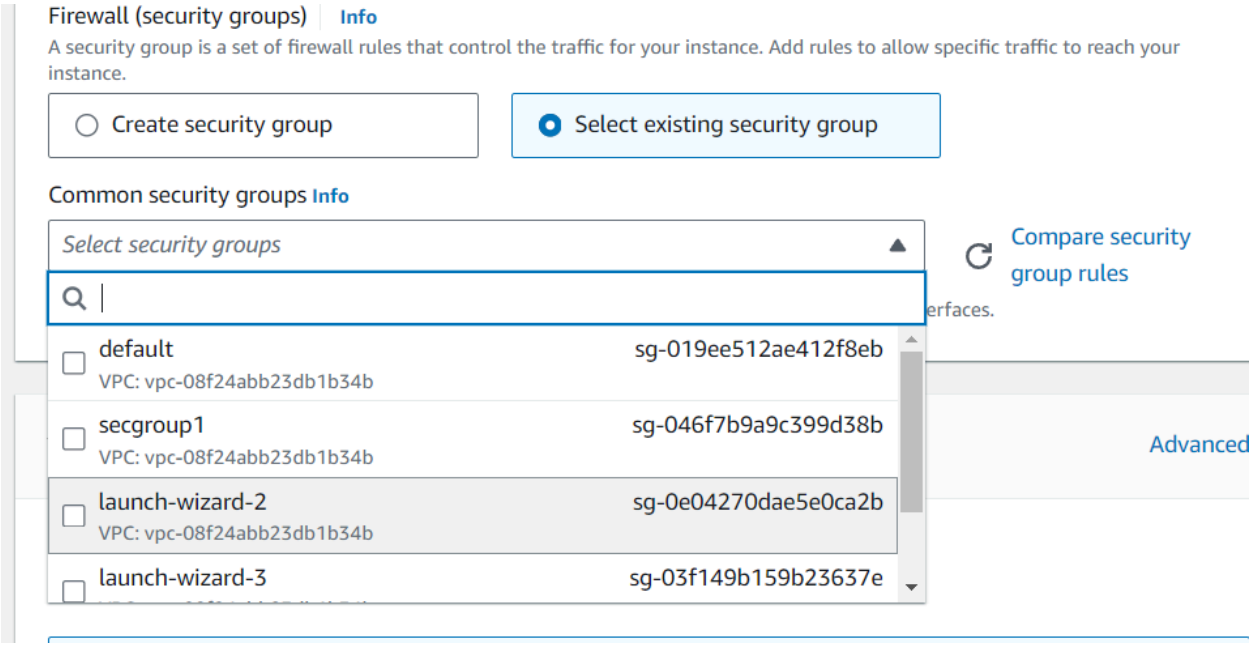
Creating new security group:





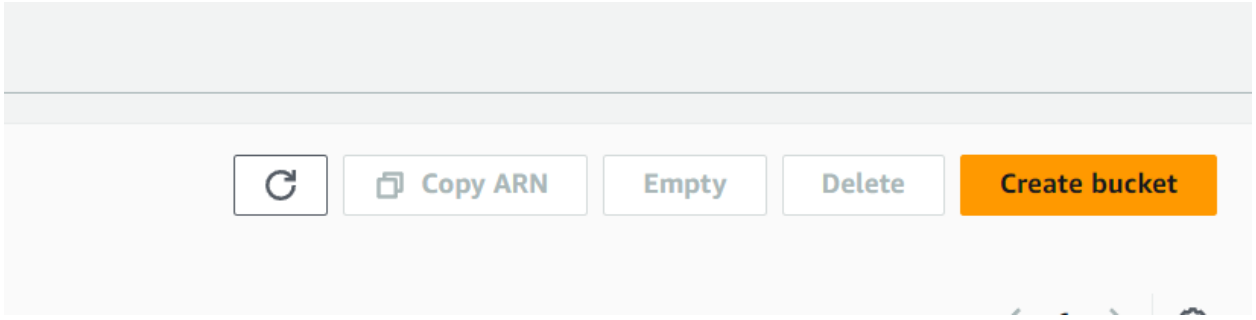


Assigning the security group to ec2:

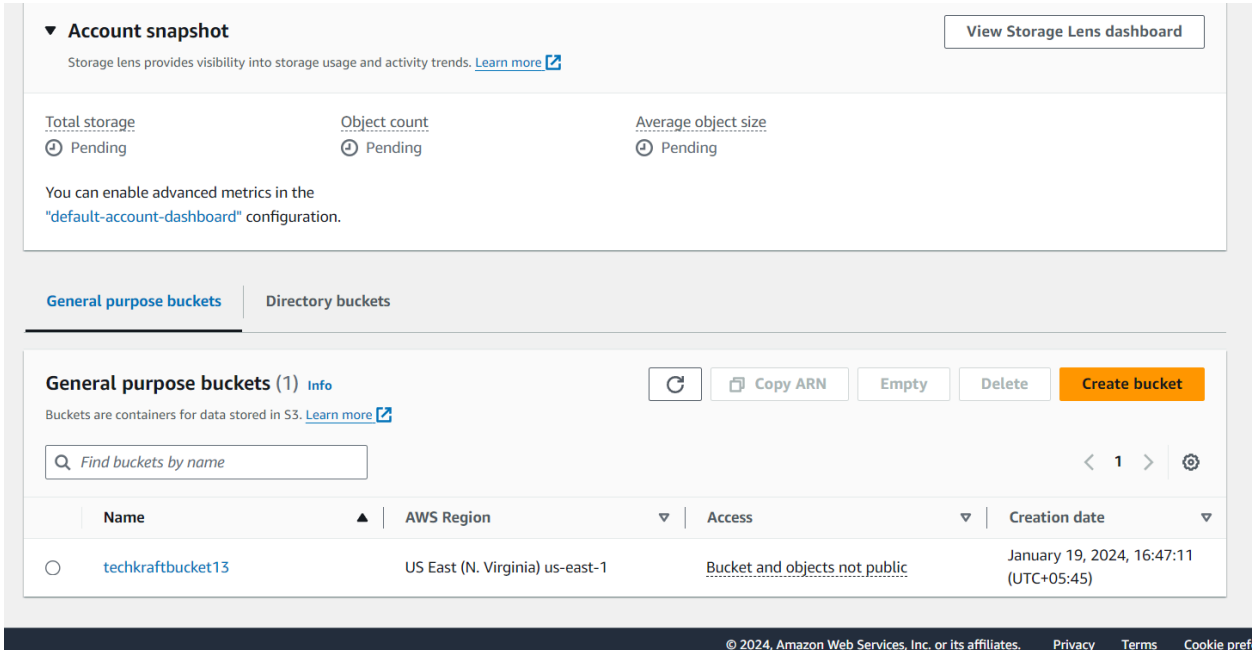


S3 Storage Fundamentals Lab

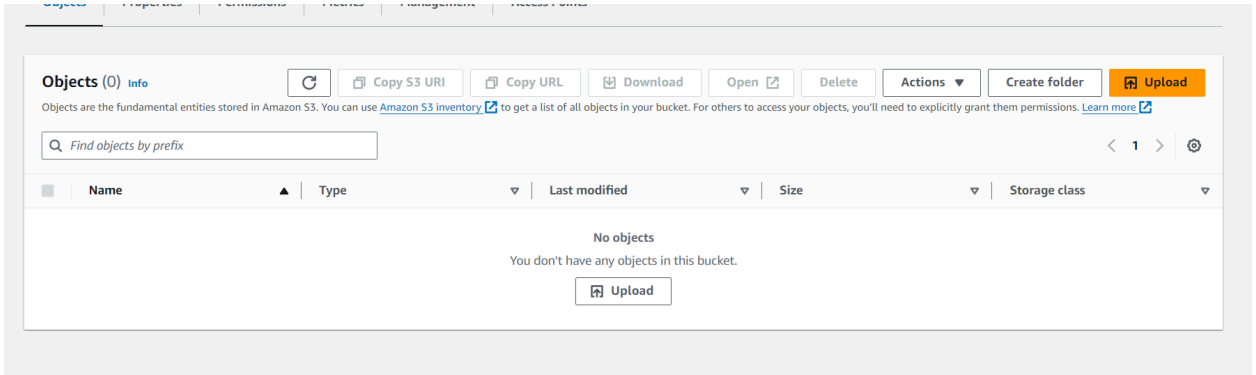
Create S3 bucket:



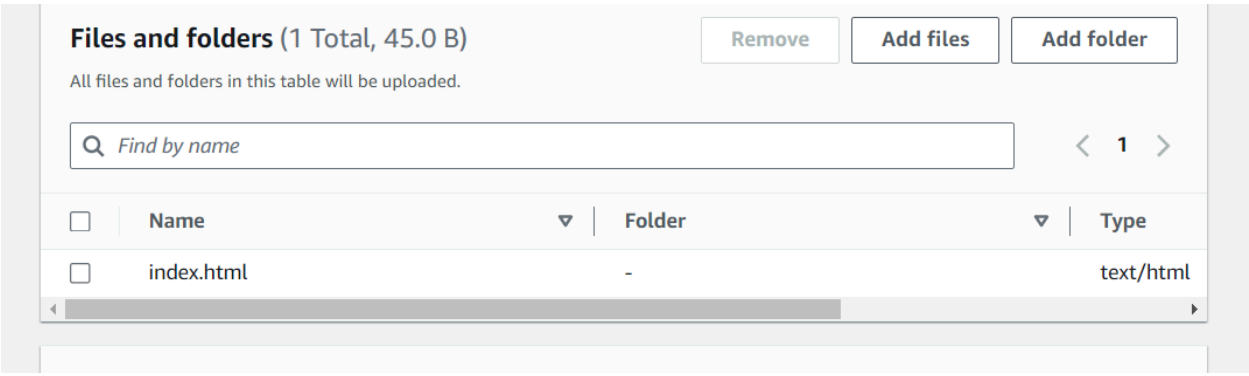
S3 management console:



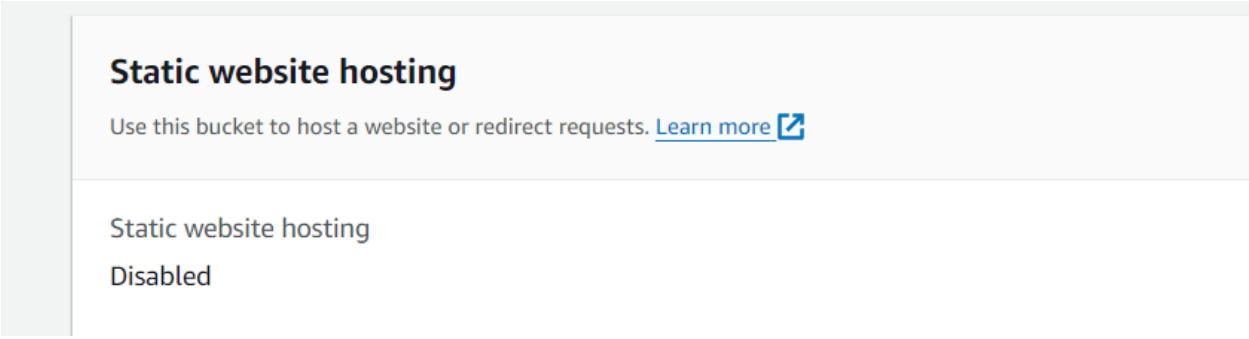
Upload object file to s3 bucket:



Uploaded file:



Enable static website hosting

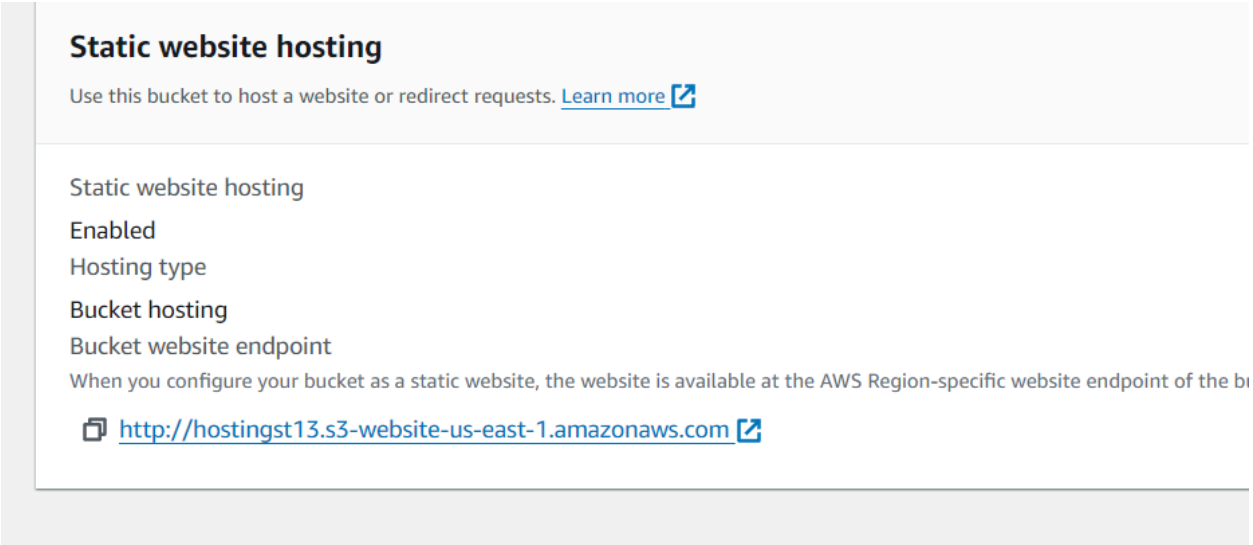


Setting bucket policy:

Policy

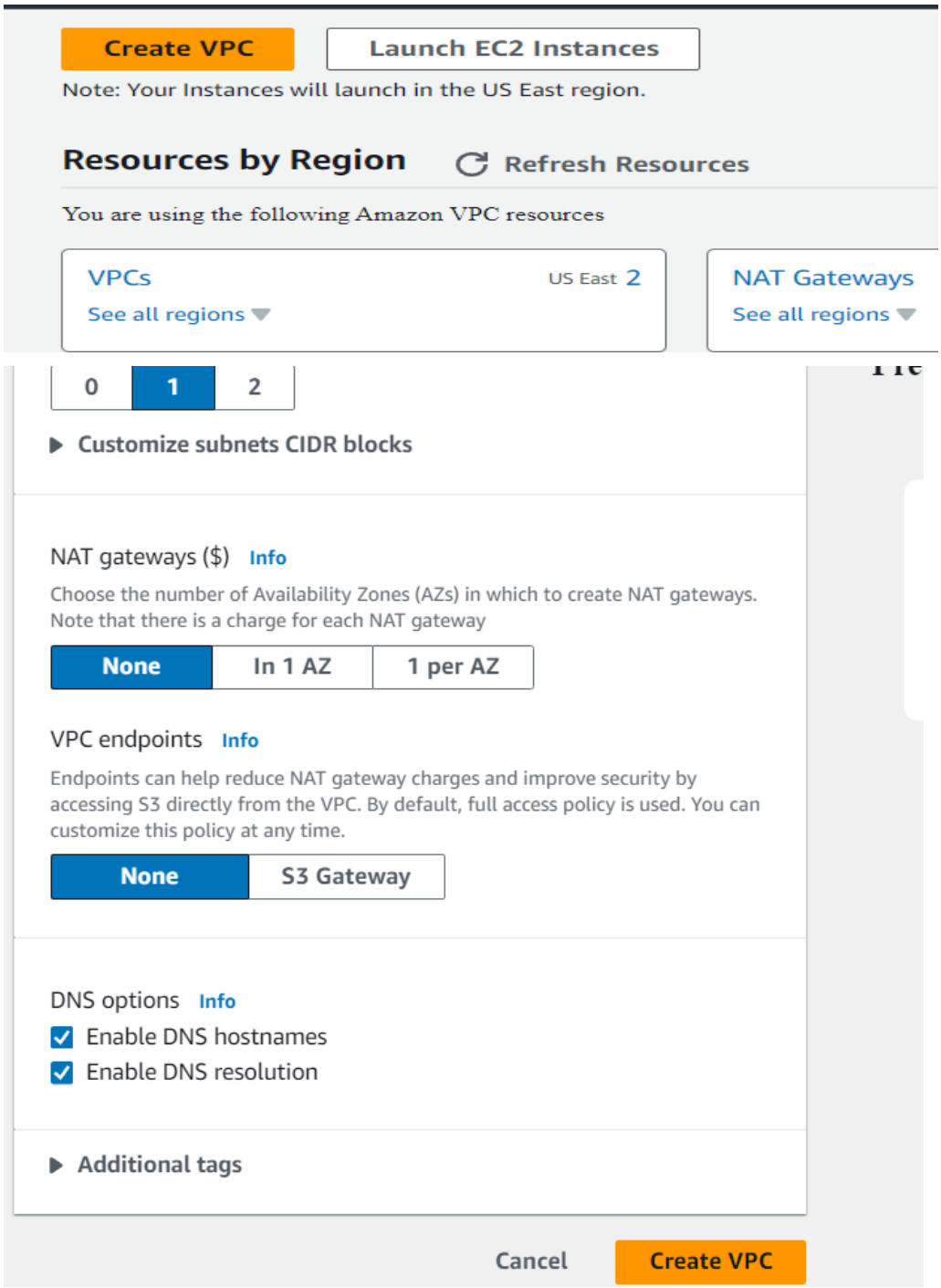
```
1  {
2      "Version": "2012-10-17",
3      "Statement": [
4          {
5              "Sid": "PublicReadGetObject",
6              "Effect": "Allow",
7              "Principal": "*",
8              "Action": [
9                  "s3:GetObject"
10             ],
11             "Resource": [
12                 "arn:aws:s3:::hostingst13/*"
13             ]
14         }
15     ]
16 }
```

HOsted static website:



VPC Configuration Lab:

Creating VPC:



Creating subnet;

VPC dashboard
EC2 Global View
Filter by VPC:
Select a VPC
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways

Subnets (9) Info

Actions | Create subnet

Find resources by attribute or tag

Name	Subnet ID	State	VPC	IPv4 CIDR
-	subnet-04d60bbc2e34d2b75	Available	vpc-035e0434f2845b45b	172.31.48.0/20
Work Public Subnet	subnet-06a45345fbbdf83b2	Available	vpc-019fabf0073781c84 | Work...	10.0.0.0/24
-	subnet-0af93780ed48e4372	Available	vpc-035e0434f2845b45b	172.31.64.0/20
-	subnet-07202f09d432867a2	Available	vpc-035e0434f2845b45b	172.31.16.0/20
-	subnet-01871c80ef1f1c7ae	Available	vpc-035e0434f2845b45b	172.31.0.0/20
-	subnet-04a4b384923f4433e	Available	vpc-035e0434f2845b45b	172.31.80.0/20

Associated VPC CIDRs

IPv4 CIDRs
10.0.0.0/16

Subnet settings

Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

Subnet name
Create a tag with a key of 'Name' and a value that you specify.
subnet-public2
The name can be up to 256 characters long.

Availability Zone Info
Choose the zone in which your subnet will reside, or let Amazon choose one for you.
US East (N. Virginia) / us-east-1b

IPv4 VPC CIDR block Info
Choose the IPv4 VPC CIDR block to create a subnet in.
10.0.0.0/16

IPv4 subnet CIDR block
10.0.2.0/24 256 IPs

Tags - *optional*

Key	Value - *optional*	
Name	subnet-public2	Remove

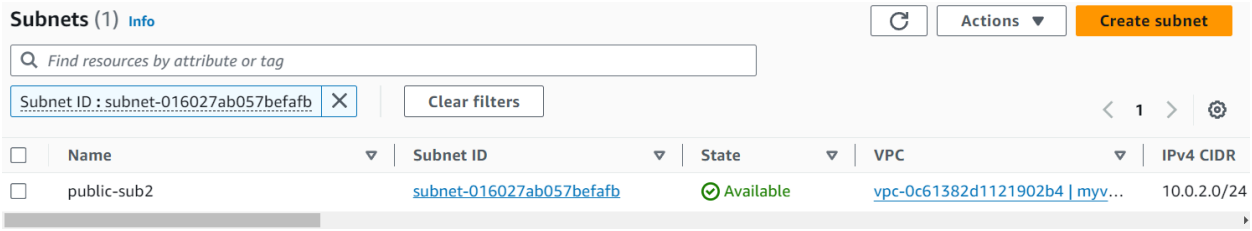
Add new tag
You can add 49 more tags.

Remove

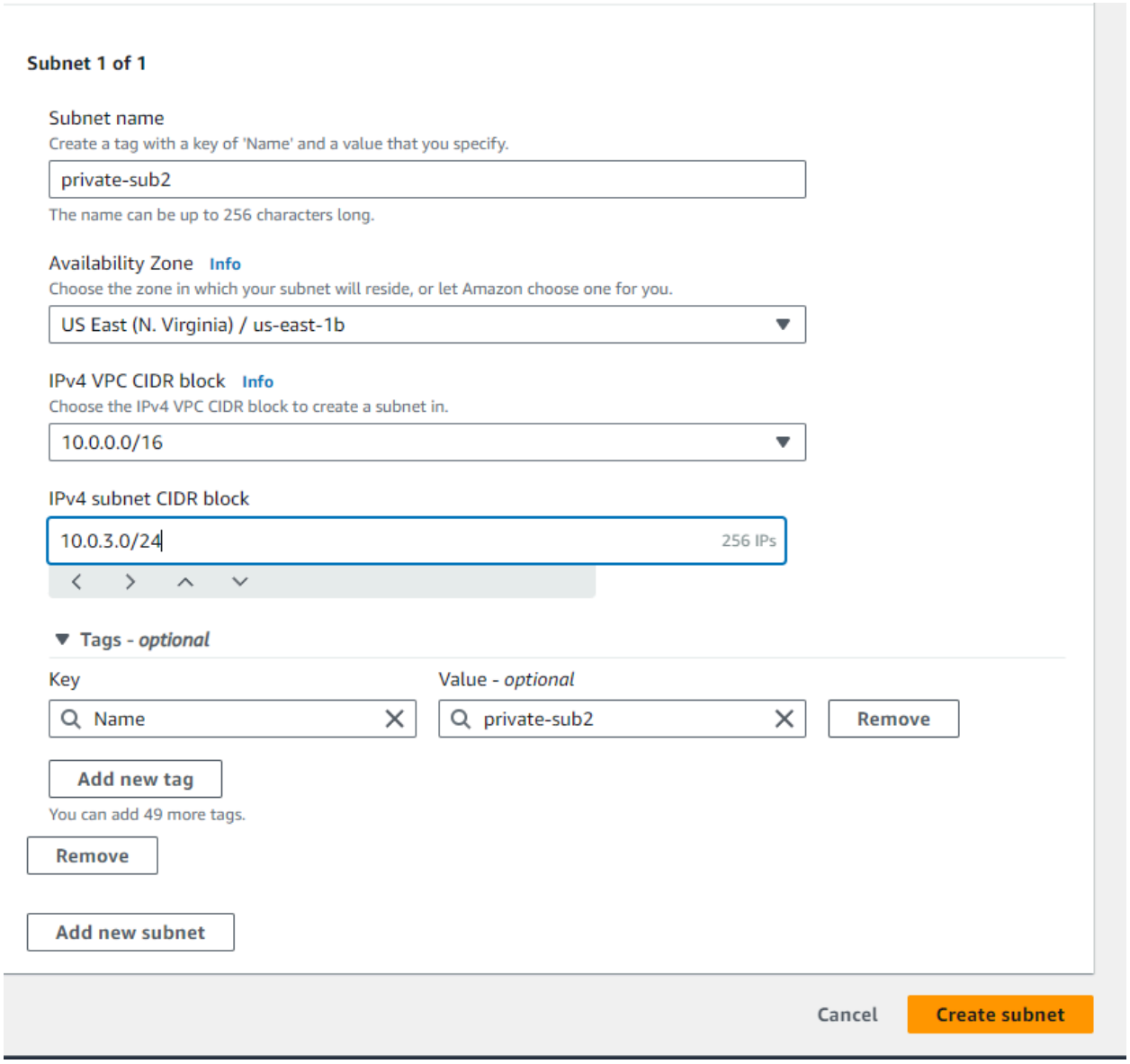
Add new subnet

Cancel | Create subnet

Public subnet created:



Creating private subnet:

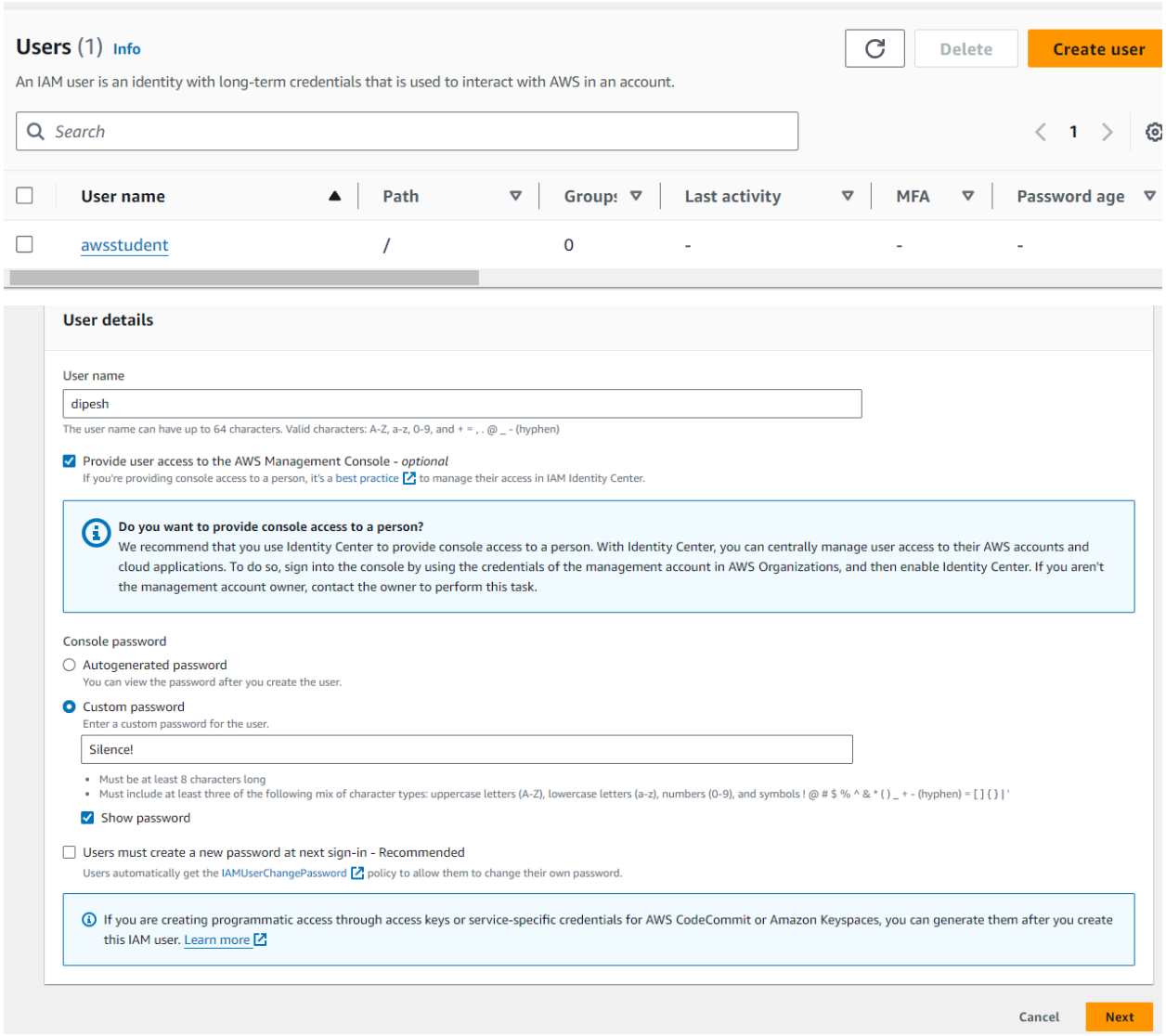


Subnet association:

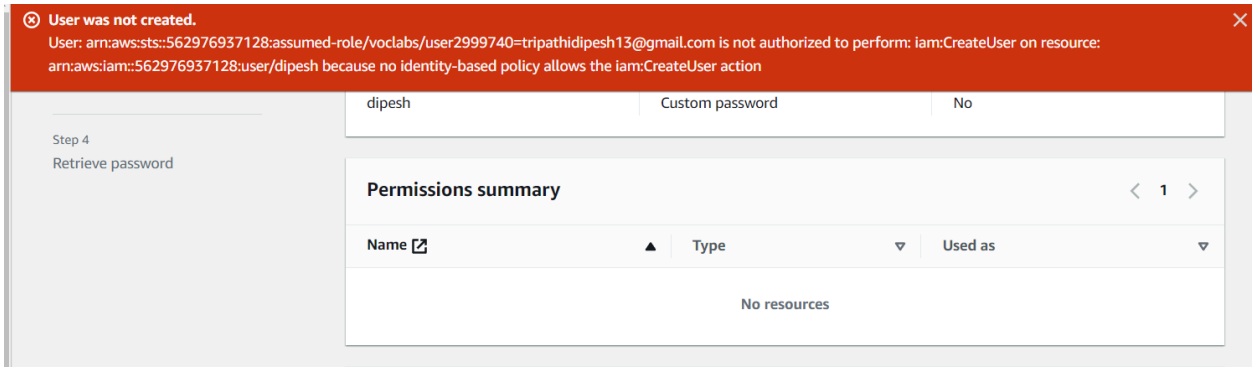
Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
private-sub2	subnet-06ab34a735839e000	10.0.3.0/24	–	Main (rtb-01f47172adde597cd)
public-sub2	subnet-016027ab057befafb	10.0.2.0/24	–	Main (rtb-01f47172adde597cd)
myvpc1-subnet-public1-us-east...	subnet-060e897444a8e8218	10.0.0.0/24	–	rtb-0880ef4c8bba7e6e4 / myvpc1
myvpc1-subnet-private1-us-eas...	subnet-095e08ba67a2935bd	10.0.1.0/24	–	rtb-0fe5035db3565f5ef / myvpc1-

IAM Users and Roles Lab

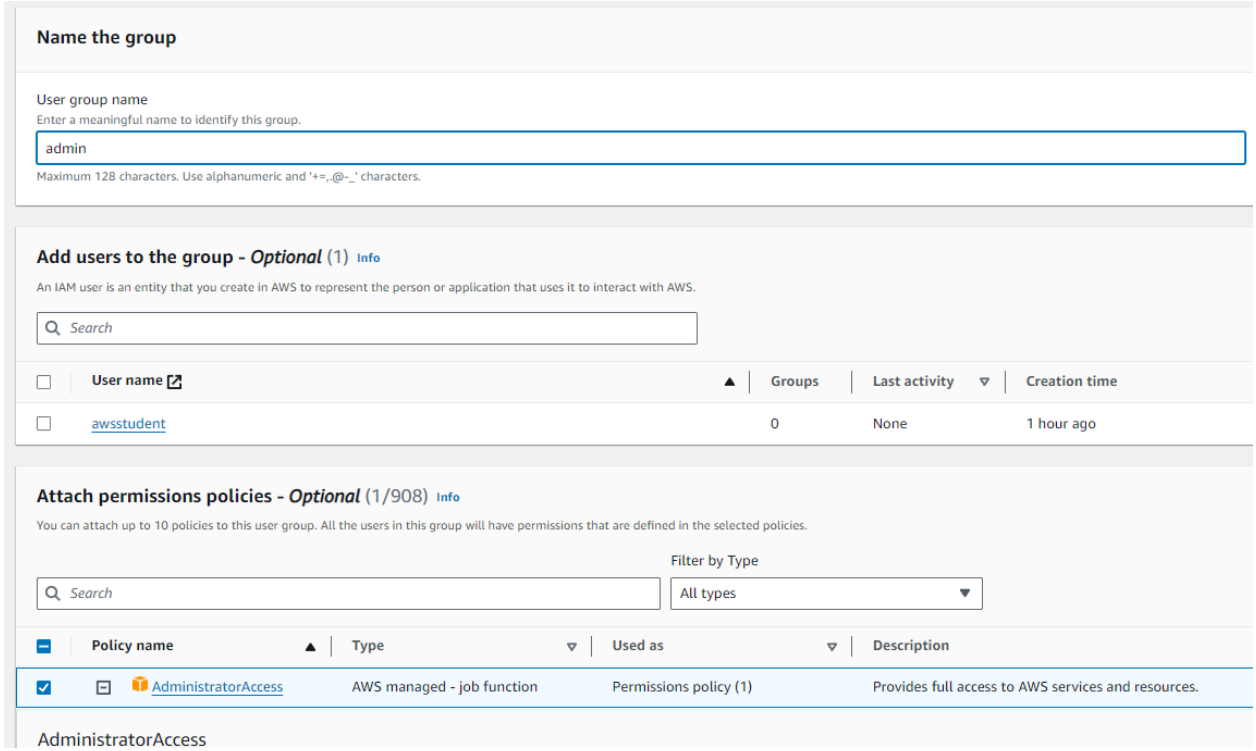
Create user:

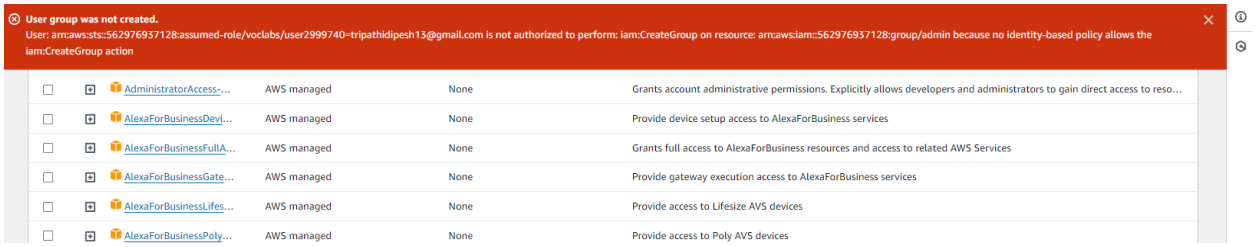


Not authorize to create a user:



Groups


Name the group
User group name
Enter a meaningful name to identify this group.
admin
Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.
Add users to the group - Optional (1) Info
An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.
Search
User name
Groups
Last activity
Creation time
awsstudent
0
None
1 hour ago
Attach permissions policies - Optional (1/908) Info
You can attach up to 10 policies to this user group. All the users in this group will have permissions that are defined in the selected policies.
Filter by Type
Search
All types
Policy name
Type
Used as
Description
AdministratorAccess
AWS managed - job function
Permissions policy (1)
Provides full access to AWS services and resources.
AdministratorAccess


User group was not created.
User: arn:aws:sts::562976937128:assumed-role/voclabs/user2999740=tripathidipesh13@gmail.com is not authorized to perform: iam:CreateGroup on resource: arn:aws:iam::562976937128:group/admin because no identity-based policy allows the iam:CreateGroup action
AdministratorAccess-... AWS managed None Grants account administrative permissions. Explicitly allows developers and administrators to gain direct access to reso...
AlexaForBusinessDevi... AWS managed None Provide device setup access to AlexaForBusiness services
AlexaForBusinessFullA... AWS managed None Grants full access to AlexaForBusiness resources and access to related AWS Services
AlexaForBusinessGate... AWS managed None Provide gateway execution access to AlexaForBusiness services
AlexaForBusinessLifes... AWS managed None Provide access to Lifesize AVS devices
AlexaForBusinessPoly... AWS managed None Provide access to Poly AVS devices

IAM lab with cloud foundation course lab

Here are already created users i.e 3.

☐	user-1	/spl66/	0	-	-	4 minutes	-	Active - AKIAWW43LP...	4 minutes
☐	user-2	/spl66/	0	-	-	4 minutes	-	Active - AKIAWW43LP...	4 minutes
☐	user-3	/spl66/	0	-	-	4 minutes	-	Active - AKIAWW43LP...	4 minutes

Already created user group:

	Group name	Users	Permissions	Creation time
☐	EC2-Admin	0	Defined	5 minutes ago
☐	EC2-Support	0	Defined	5 minutes ago
☐	S3-Support	0	Defined	5 minutes ago

Permission to the EC2-support group is

User group name
EC2-Support

Creation ti
January 20

Users | Permissions | Access Advisor

Permissions policies (1) Info

You can attach up to 10 managed policies.

Search

	Policy name	Type
☐	AmazonEC2ReadOnlyAccess	AWS

JSON written policy:

AmazonEC2ReadOnlyAccess

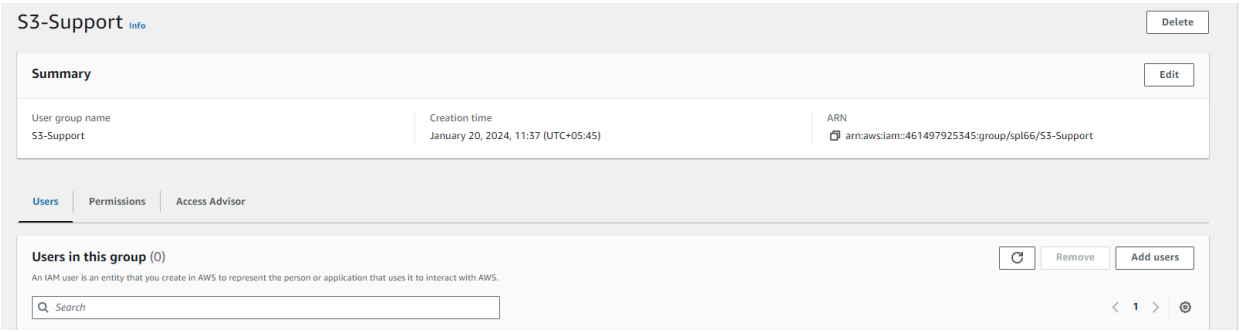
Provides read only access to Amazon EC2 via the AWS Management Console.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:Describe*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "elasticloadbalancing:Describ
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "cloudwatch:ListMetrics",
                "cloudwatch:GetMetricStatistics",
                "cloudwatch:Describe*"
            ],
```

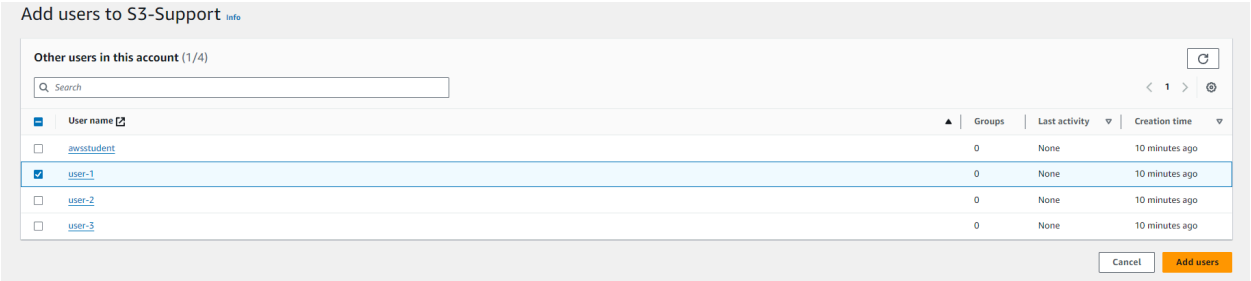
We need to set the following users to the user group:

User	In Group	Permissions
user-1	S3-Support	Read-Only access to Amazon S3
user-2	EC2-Support	Read-Only access to Amazon EC2
user-3	EC2-Admin	View, Start and Stop Amazon EC2 instances

For this add users to the user group:



Select user 1



This Concludes the completion of AWS Basic Labs