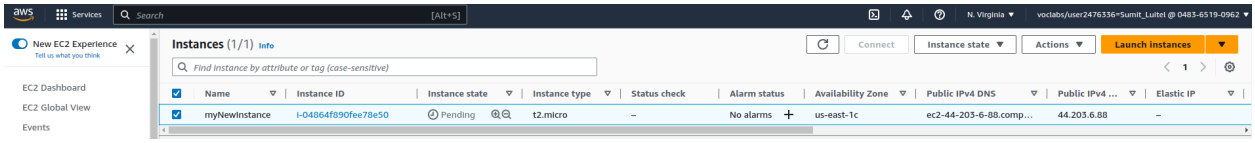
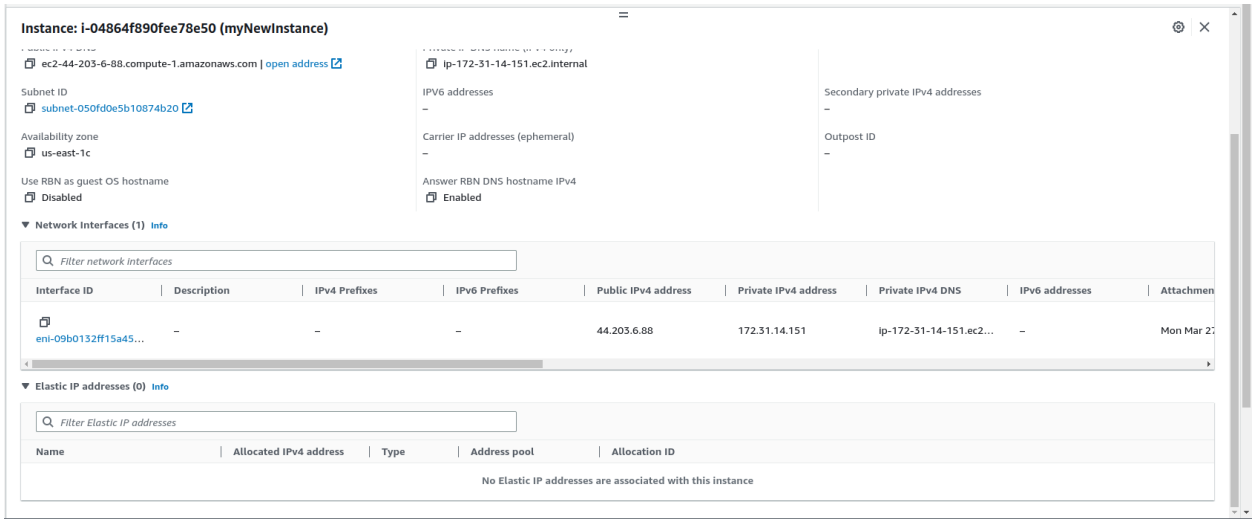
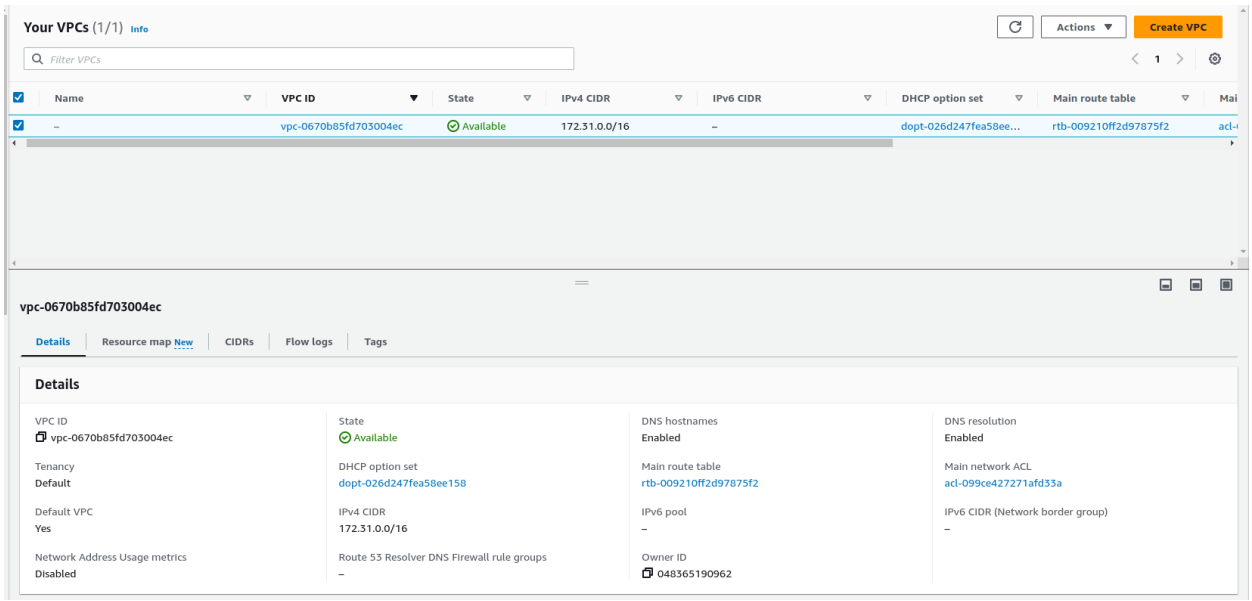
Lab 2:

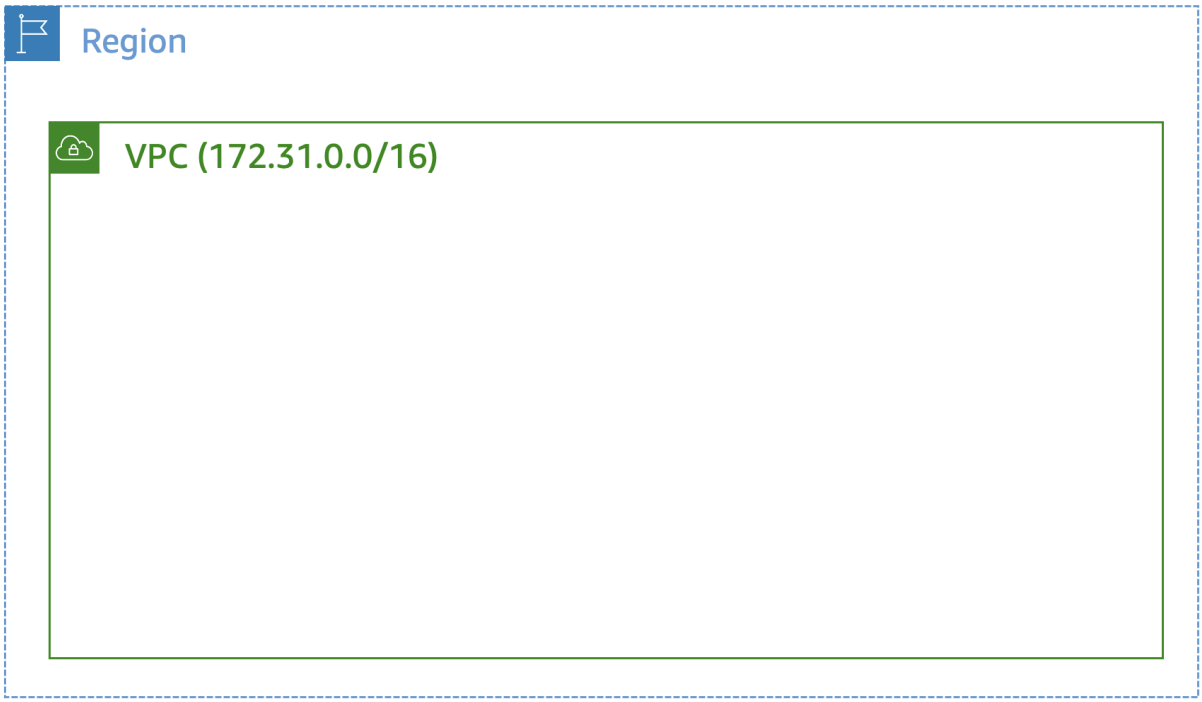
1. Launch a new instance in the default VPC in a particular subnet(AZ). Note the different network resources attached to it.







VPC deployed in AWS region.



CIDR - Classless Inter-Domain Routing (CIDR) is a range of IP addresses a network uses. A CIDR address looks like a normal IP address, except that it ends with a slash followed by a number. The number after the slash represents the number of addresses in the range. Example: **172.31.0.0/16**

This CIDR range includes all addresses from **172.31.0.0** through **172.31.255.255**, which is a total of **65,536 addresses**.

Public Subnet - A subnet is a subrange of IP addresses in the VPC. AWS resources can be launched into a specified subnet. Use a ***public subnet*** for resources that must be connected to the internet, and use a ***private subnet*** for resources that must remain isolated from the internet.

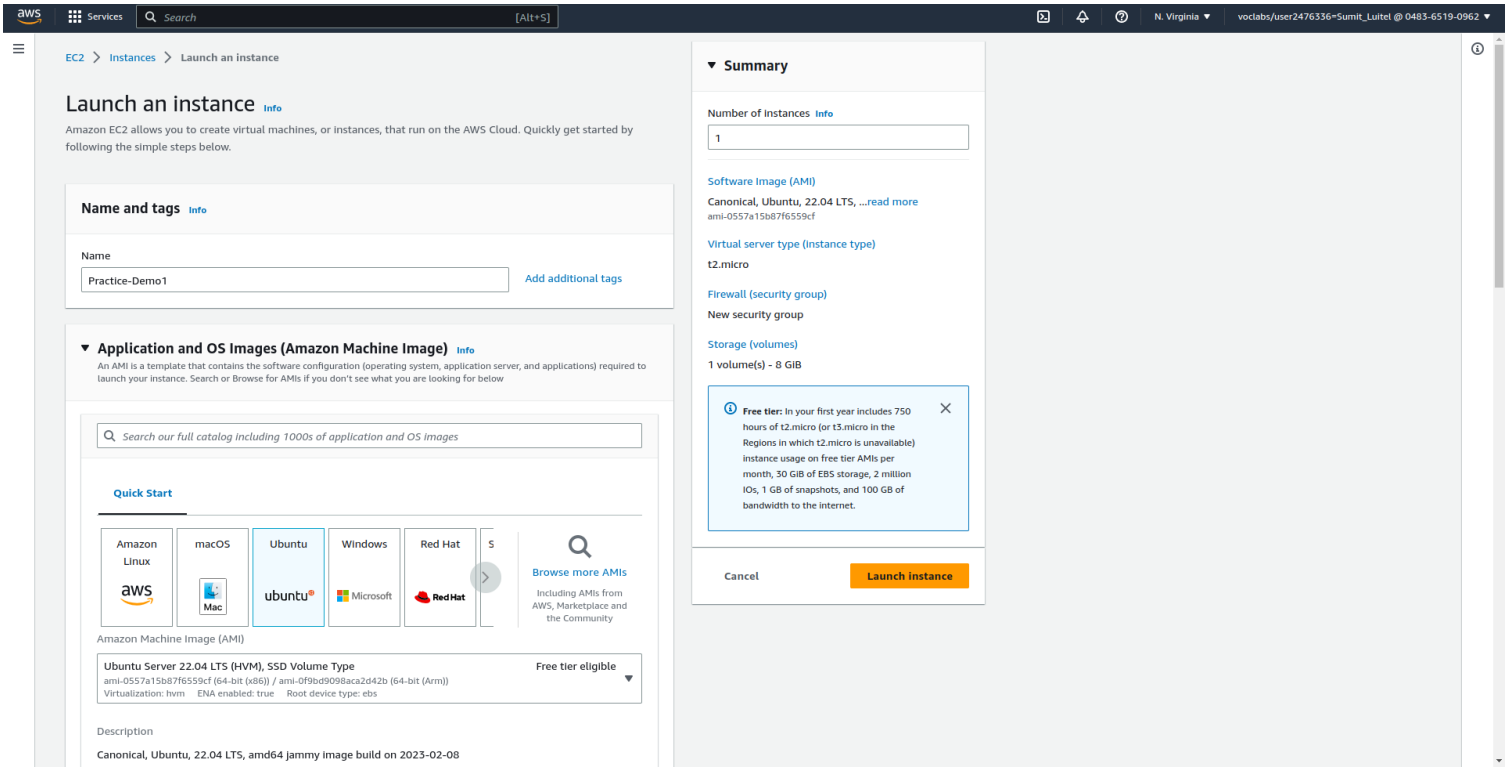
All of the default subnets are associated with the same VPC

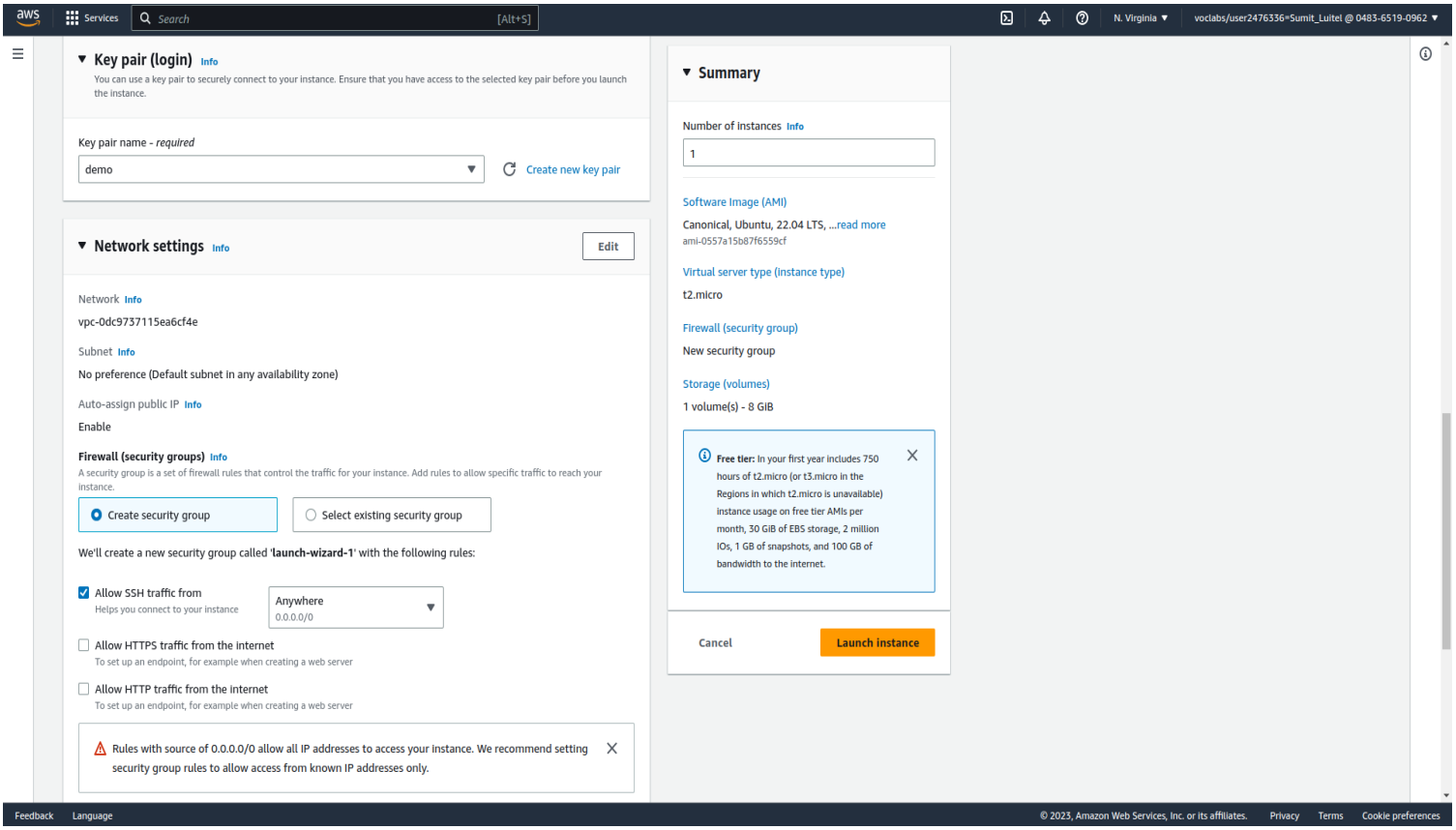
Security group - A *security group* controls the traffic that is allowed to reach and leave the resources that it is associated with. For example, after you associate a security group with an EC2 instance, it controls the inbound and outbound traffic for the instance.

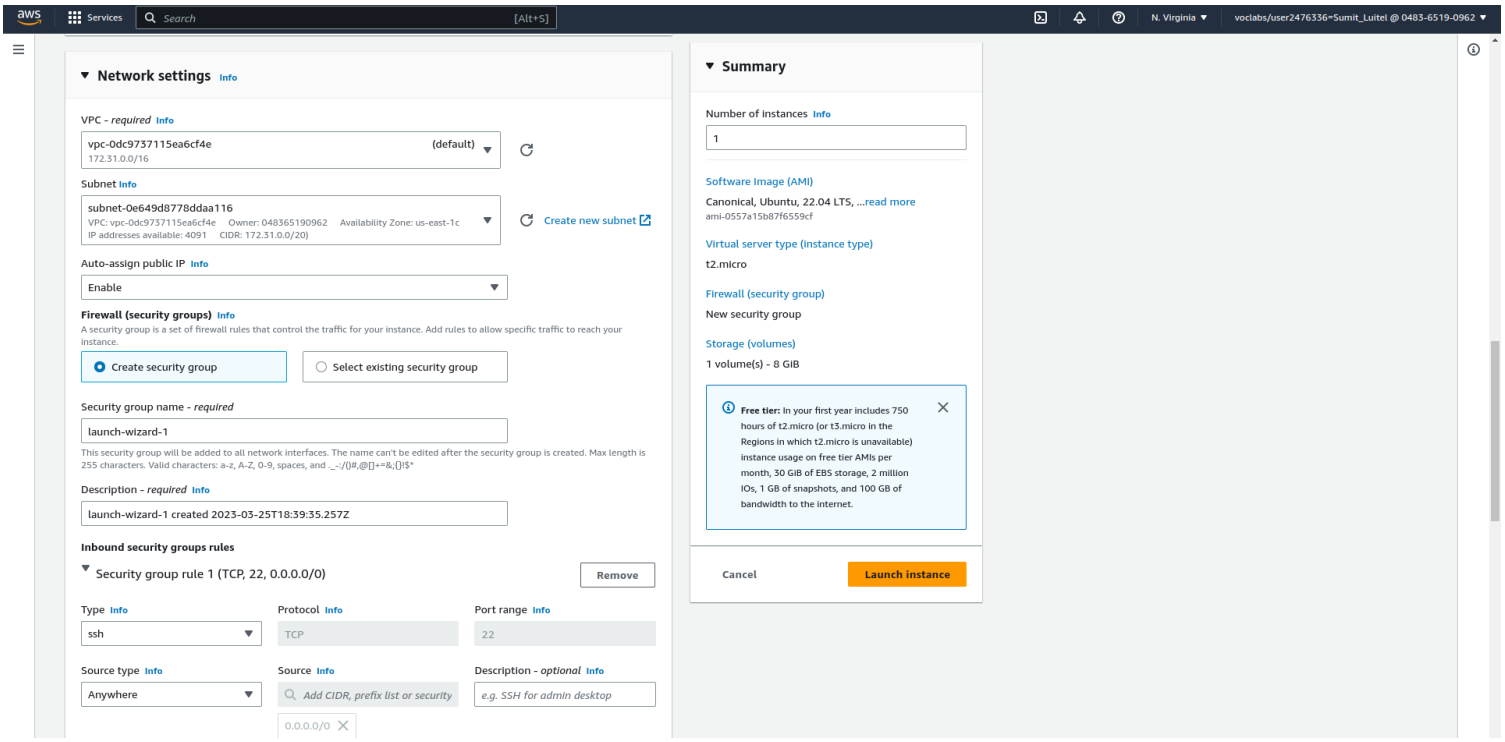
VPC's internet gateway - An *internet gateway* allows communication between the resources in a VPC and the internet. Status - Attached meaning, Internet Gateway exists and that it is attached it to the default VPC.

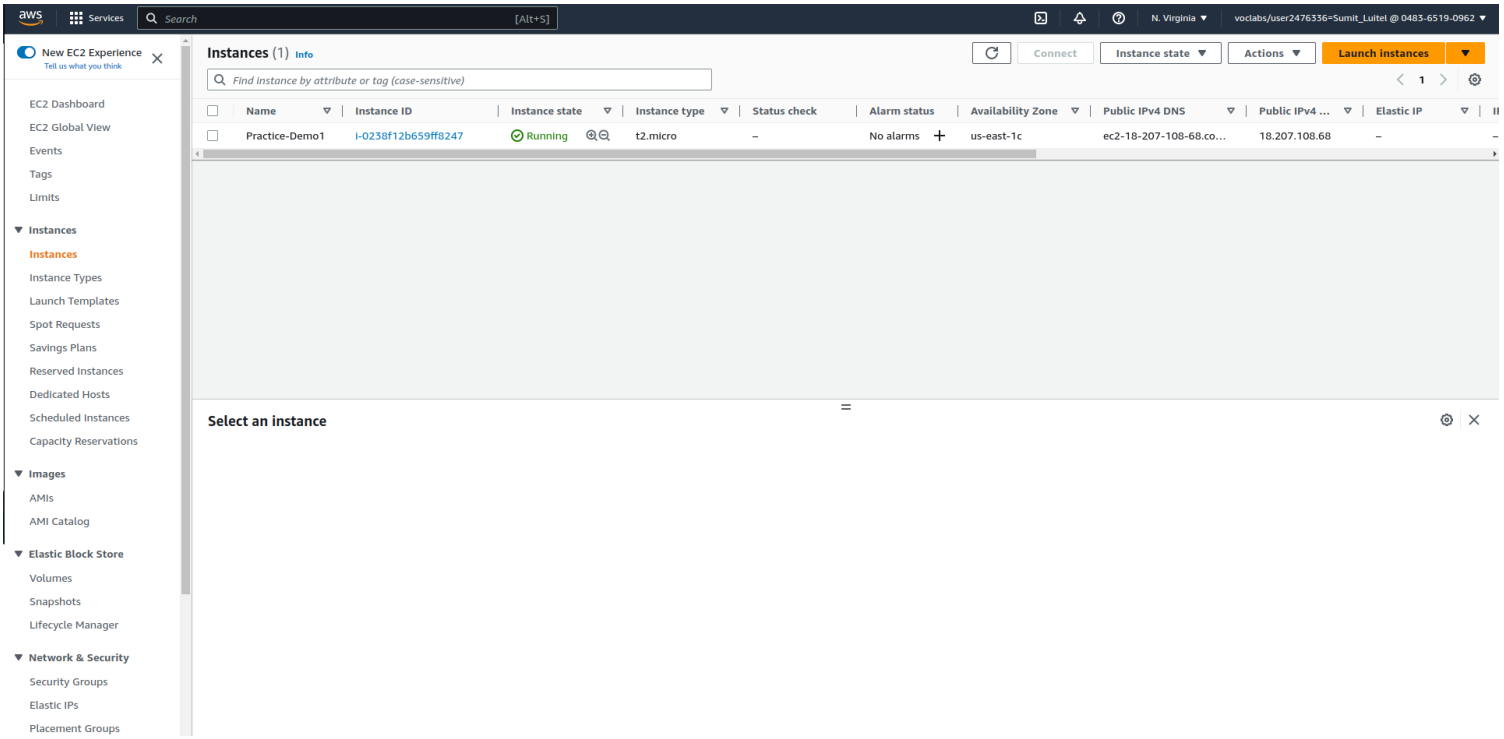
Routes Table - Route table are used to determine where network traffic is directed. Each subnet in a VPC must be associated with a route table. A subnet can be associated with only one route table at a time, but we can associate multiple subnets with the same route table.

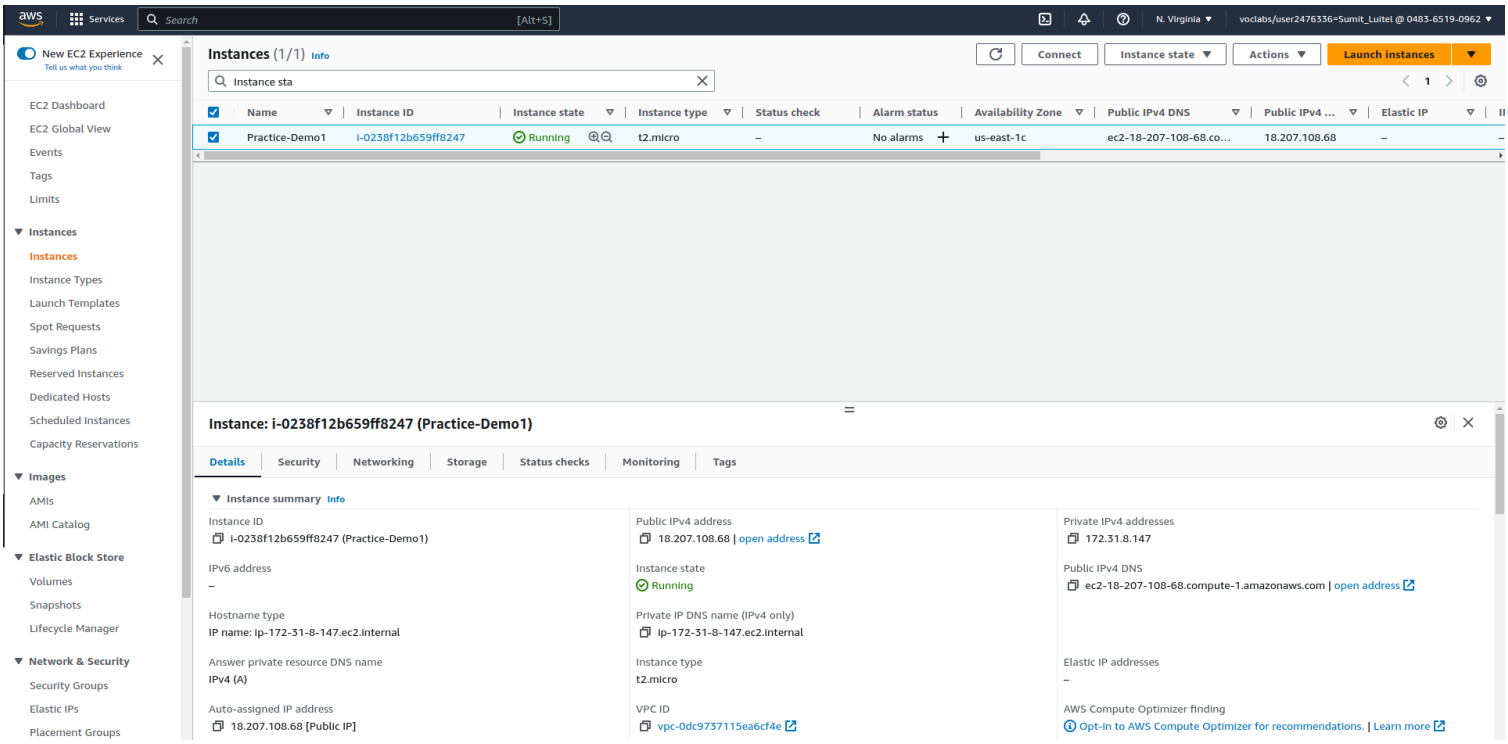
2. Launch 3 instances, 2 in the same region and 1 in another region. Try to access the instances from the other using public and private IPS and note down which connections were successful.
   (Hint: You can connect using http – by launching a webserver, or you can ping one server from another - by allowing ICMP protocol and executing ping command)



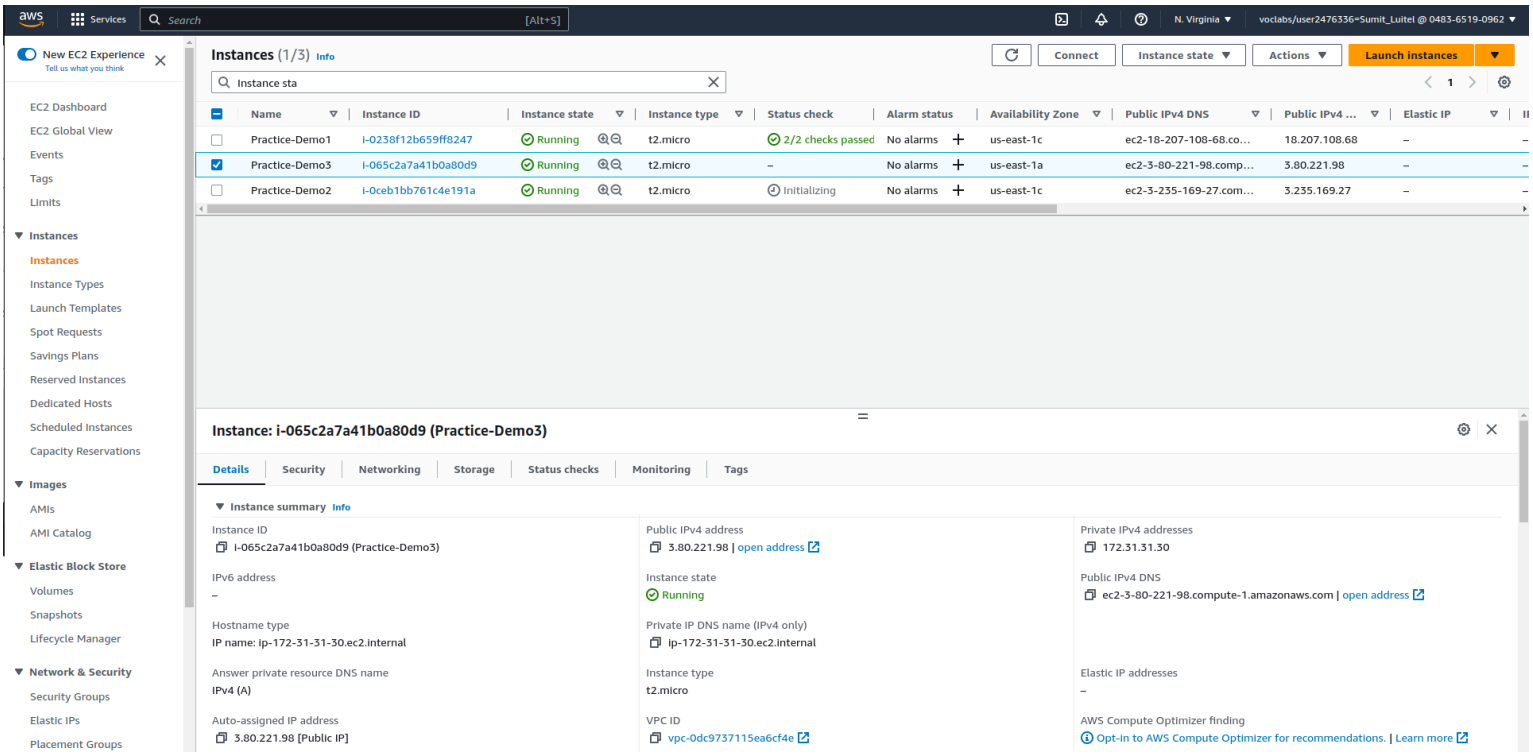

Services
Search
[Alt+S]
N. Virginia
voclabs/user2476336=Sumit_Luitel @ 0483-6519-0962
Key pair (login) Info
You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.
Key pair name - required
demo
Create new key pair
Network settings Info
Edit
Network Info
vpc-0dc9737115ea6cf4e
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
We'll create a new security group called 'launch-wizard-1' with the following rules:
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
Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.
Summary
Number of instances Info
1
Software Image (AMI)
Canonical, Ubuntu, 22.04 LTS, ...read more
ami-0557a15b87f6559cf
Virtual server type (instance type)
t2.micro
Firewall (security group)
New security group
Storage (volumes)
1 volume(s) - 8 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
Feedback
Language
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

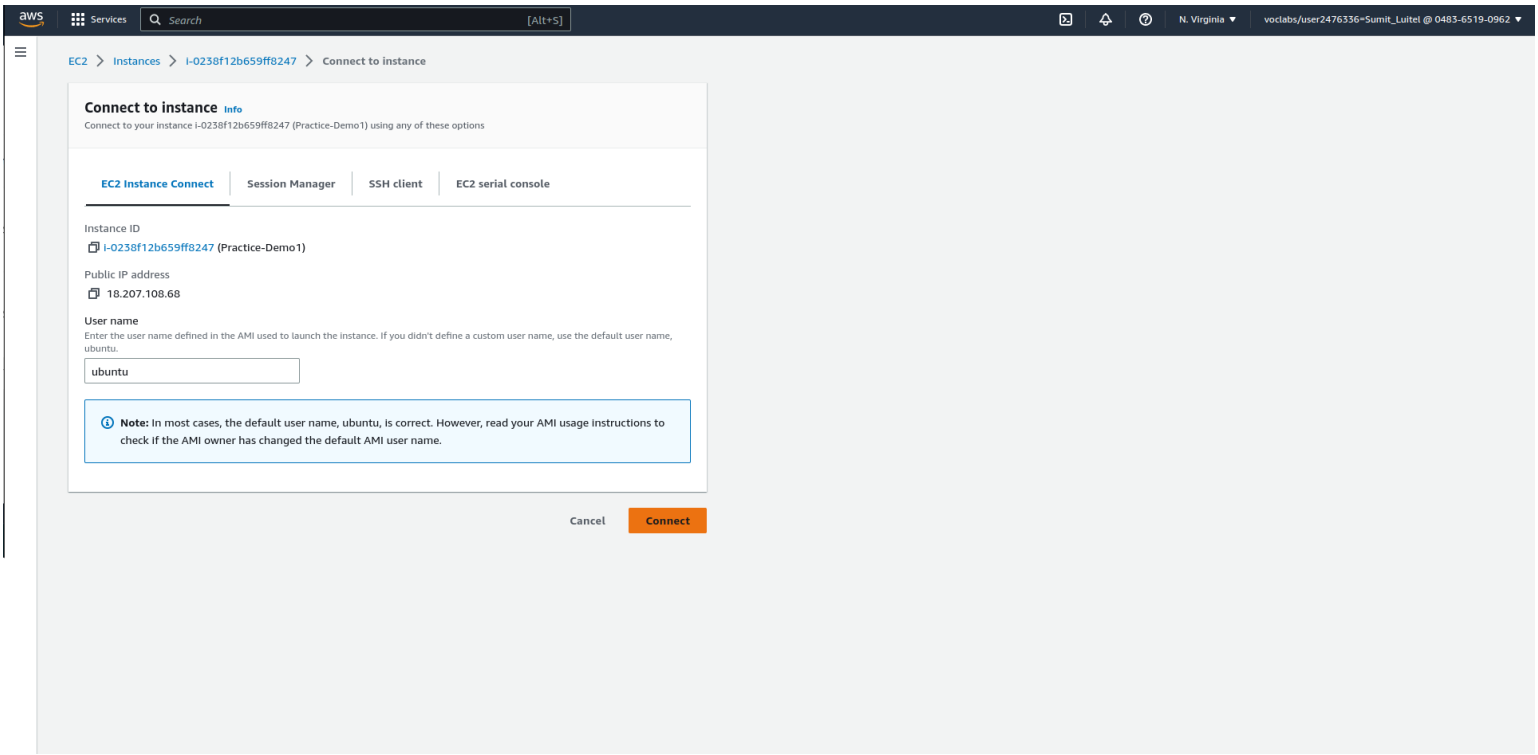

Services
Search
[Alt+S]
N. Virginia
voclabs/user2476336=Sumit_Luitel @ 0483-6519-0962
Network settings Info
VPC - required Info
vpc-0dc9737115ea6cf4e (default)
172.31.0.0/16
Subnet Info
subnet-0e649d8778ddaa116
VPC: vpc-0dc9737115ea6cf4e Owner: 048365190962 Availability Zone: us-east-1c
IP addresses available: 4091 CIDR: 172.31.0.0/20)
Create new subnet
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
Security group name - required
launch-wizard-1
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 Info
launch-wizard-1 created 2023-03-25T18:39:35.257Z
Inbound security groups rules
Security group rule 1 (TCP, 22, 0.0.0.0/0)
Remove
Type Info
ssh
Protocol Info
TCP
Port range Info
22
Source type Info
Anywhere
Source Info
Add CIDR, prefix list or security
0.0.0.0/0
Description - optional Info
e.g. SSH for admin desktop
Summary
Number of instances Info
1
Software Image (AMI)
Canonical, Ubuntu, 22.04 LTS, ...read more
ami-0557a15b87f6559cf
Virtual server type (instance type)
t2.micro
Firewall (security group)
New security group
Storage (volumes)
1 volume(s) - 8 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

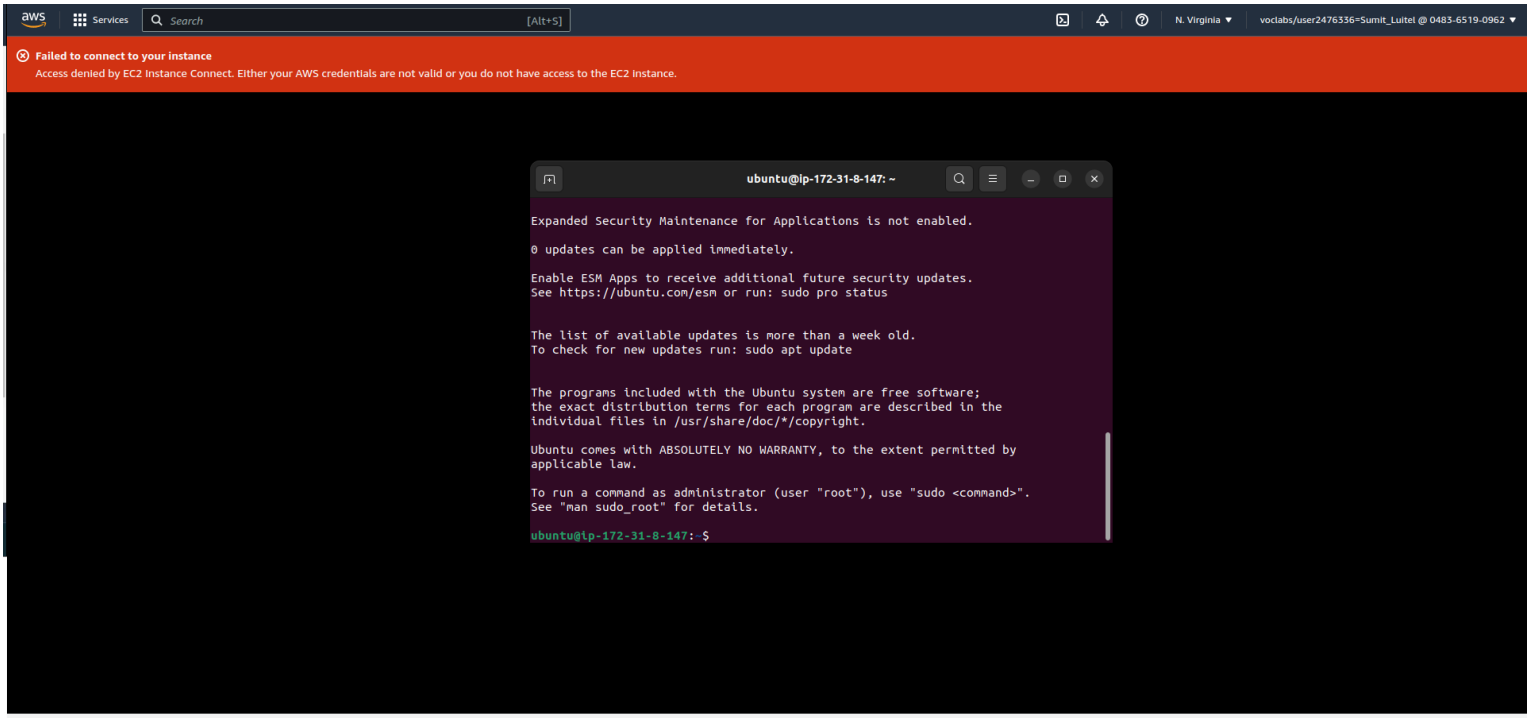

Services
Search
[Alt+S]
N. Virginia
voclabs/user2476336=Sumit_Luitel @ 0483-6519-0962
New EC2 Experience
Tell us what you think
EC2 Dashboard
EC2 Global View
Events
Tags
Limits
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Scheduled Instances
Capacity Reservations
Images
AMIs
AMI Catalog
Elastic Block Store
Volumes
Snapshots
Lifecycle Manager
Network & Security
Security Groups
Elastic IPs
Placement Groups
Instances (1) Info
Find instance by attribute or tag (case-sensitive)
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 IP
Practice-Demo1
i-0238f12b659ff8247
Running
t2.micro
–
No alarms
us-east-1c
ec2-18-207-108-68.co...
18.207.108.68
Select an instance


Services
Search
[Alt+S]
N. Virginia
voclabs/user2476336=Sumit_Luitel @ 0483-6519-0962
New EC2 Experience
Tell us what you think
Instances (1/1) Info
Instance sta
Connect
Instance state
Actions
Launch instances
Practice-Demo1
i-0238f12b659ff8247
Running
t2.micro
No alarms
us-east-1c
ec2-18-207-108-68.co...
18.207.108.68
Instance: i-0238f12b659ff8247 (Practice-Demo1)
Details
Security
Networking
Storage
Status checks
Monitoring
Tags
Instance summary Info
Instance ID
i-0238f12b659ff8247 (Practice-Demo1)
Public IPv4 address
18.207.108.68 | open address
Private IPv4 addresses
172.31.8.147
IPv6 address
–
Instance state
Running
Public IPv4 DNS
ec2-18-207-108-68.compute-1.amazonaws.com | open address
Hostname type
IP name: ip-172-31-8-147.ec2.internal
Private IP DNS name (IPv4 only)
ip-172-31-8-147.ec2.internal
Answer private resource DNS name
IPv4 (A)
Instance type
t2.micro
Elastic IP addresses
–
Auto-assigned IP address
18.207.108.68 [Public IP]
VPC ID
vpc-0dc9737115ea6cf4e
AWS Compute Optimizer finding
Opt-in to AWS Compute Optimizer for recommendations. | Learn more

Created 3 instances in the same region (N.virginia)

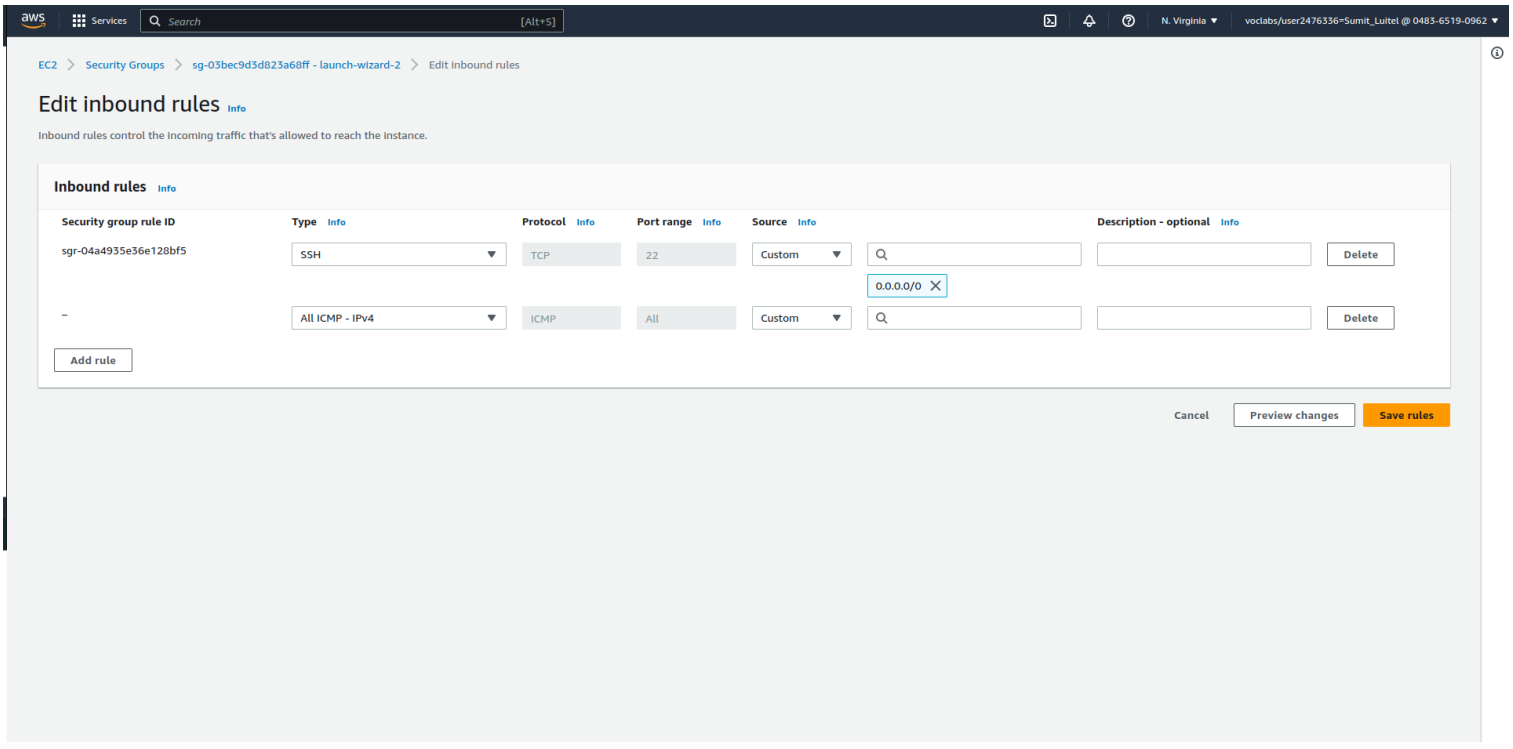




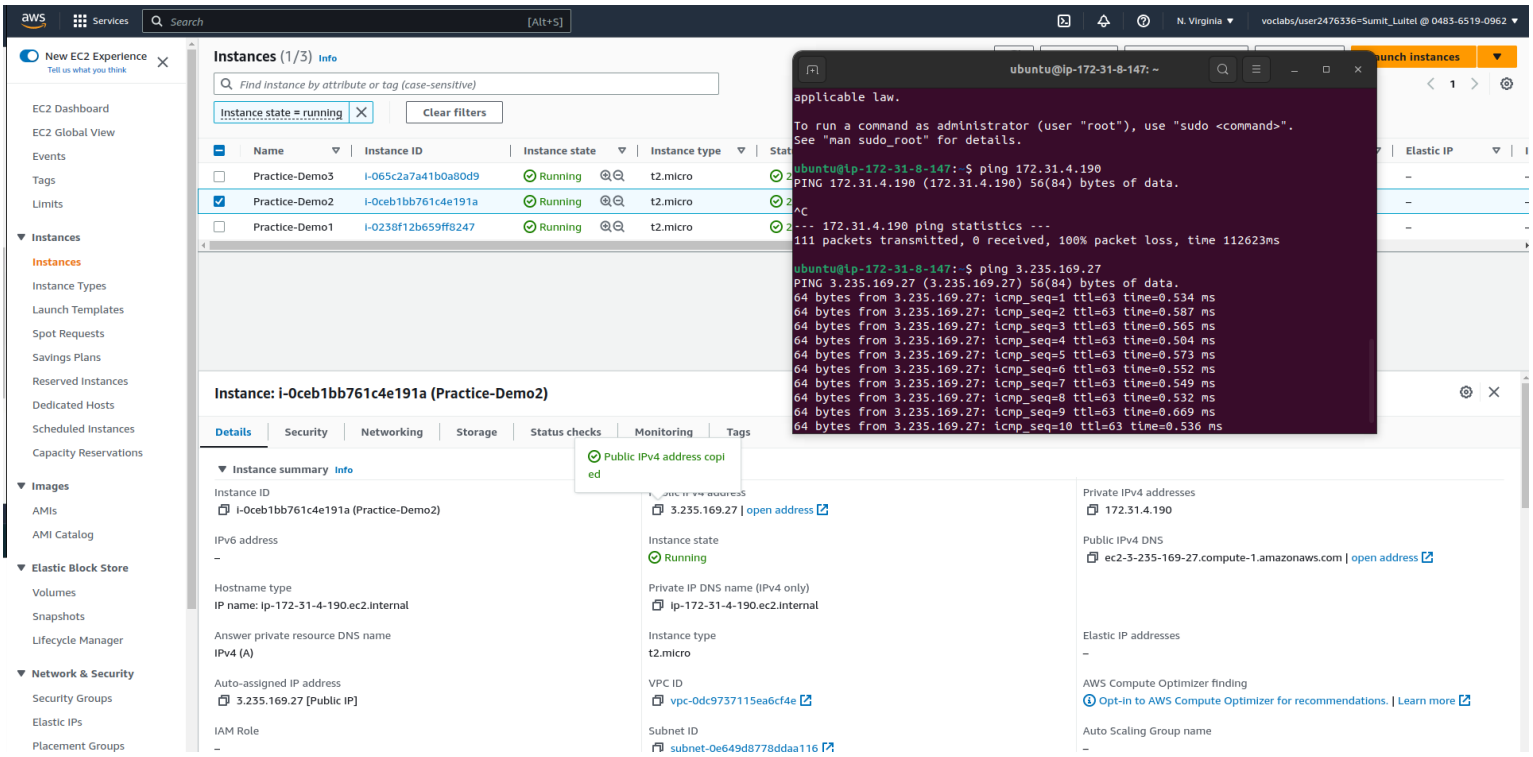


Add Inbbound rule.

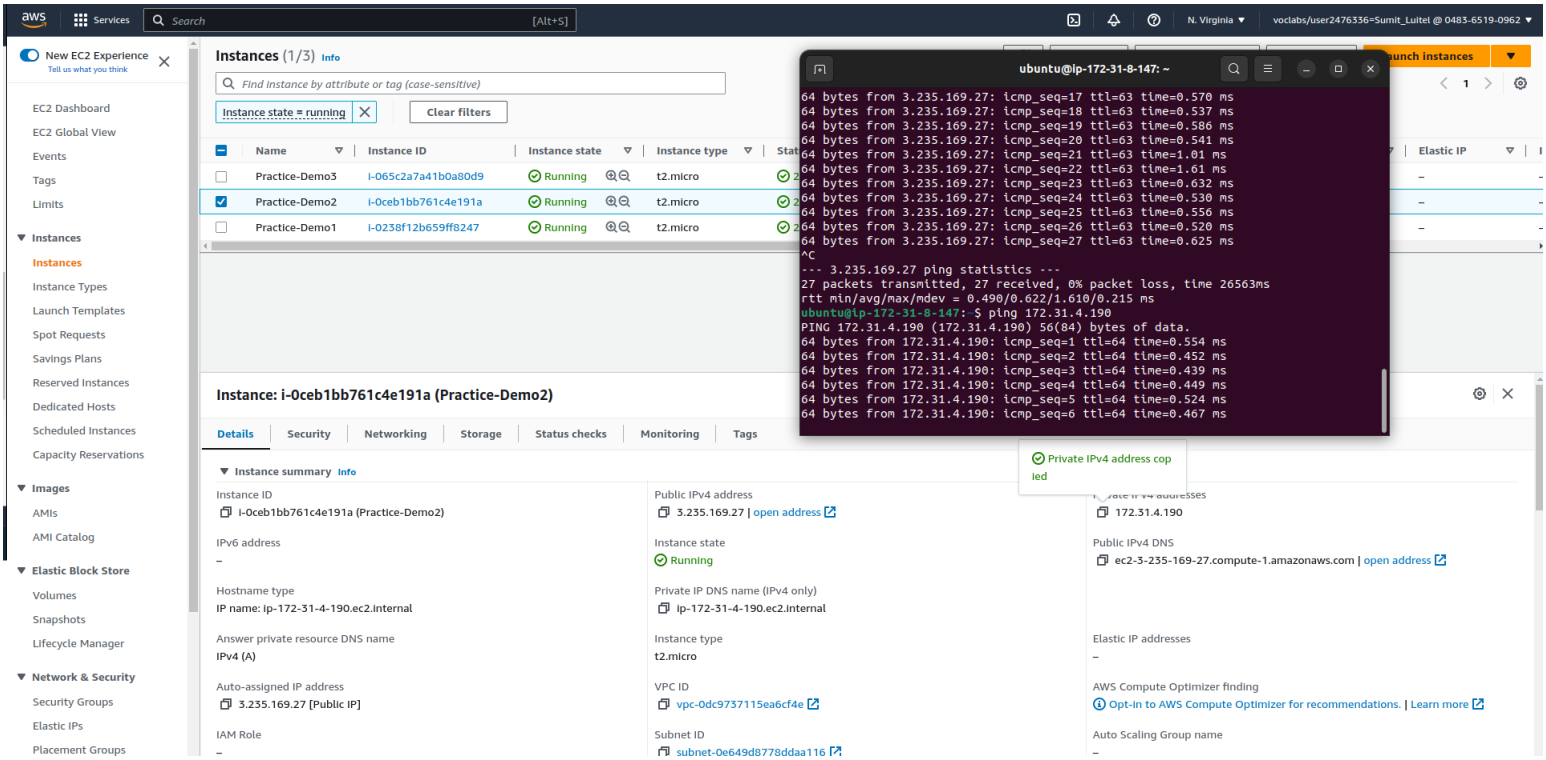
- Add ICMP Protocol in **Practice-Demo2**



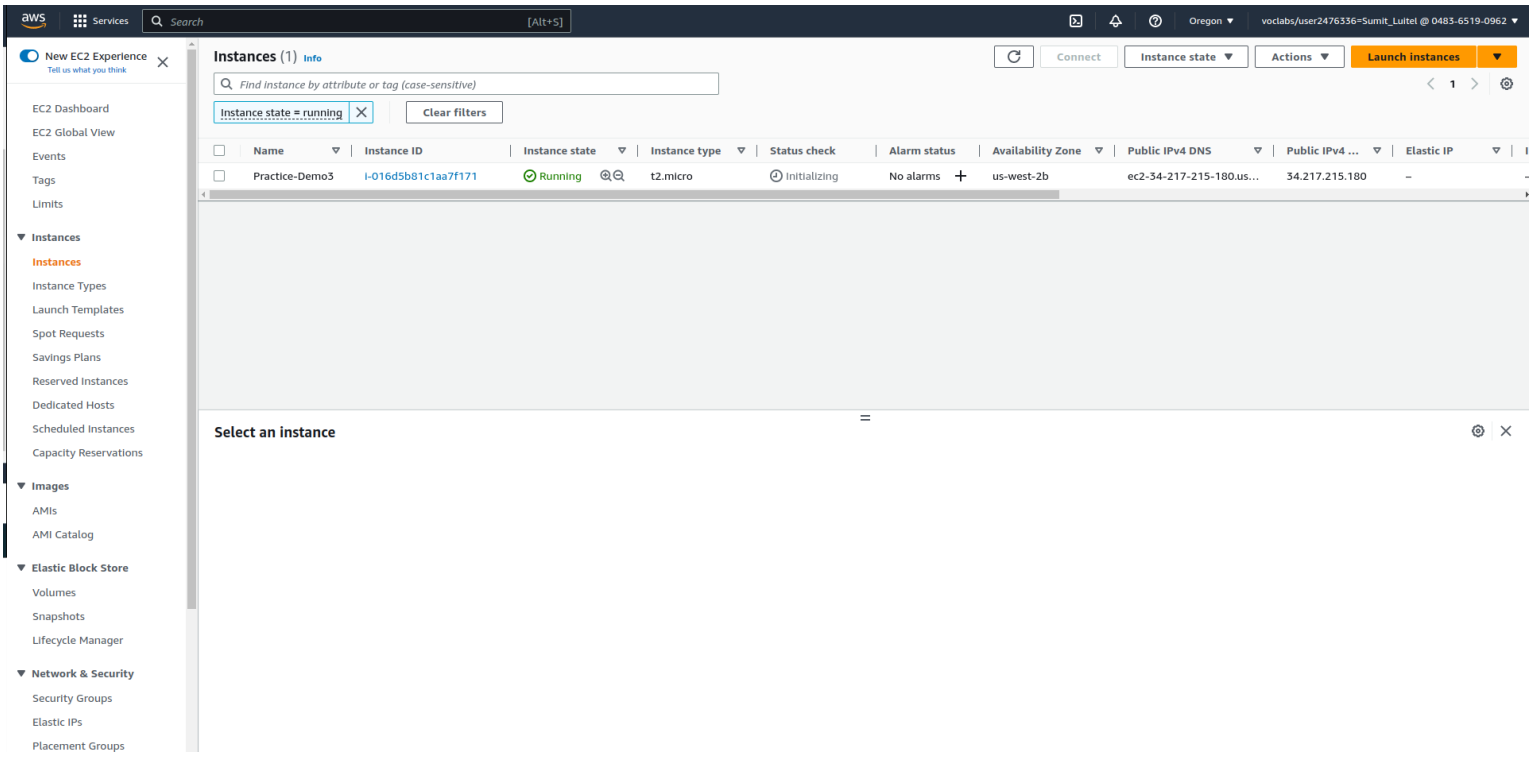
- Ping the public IP

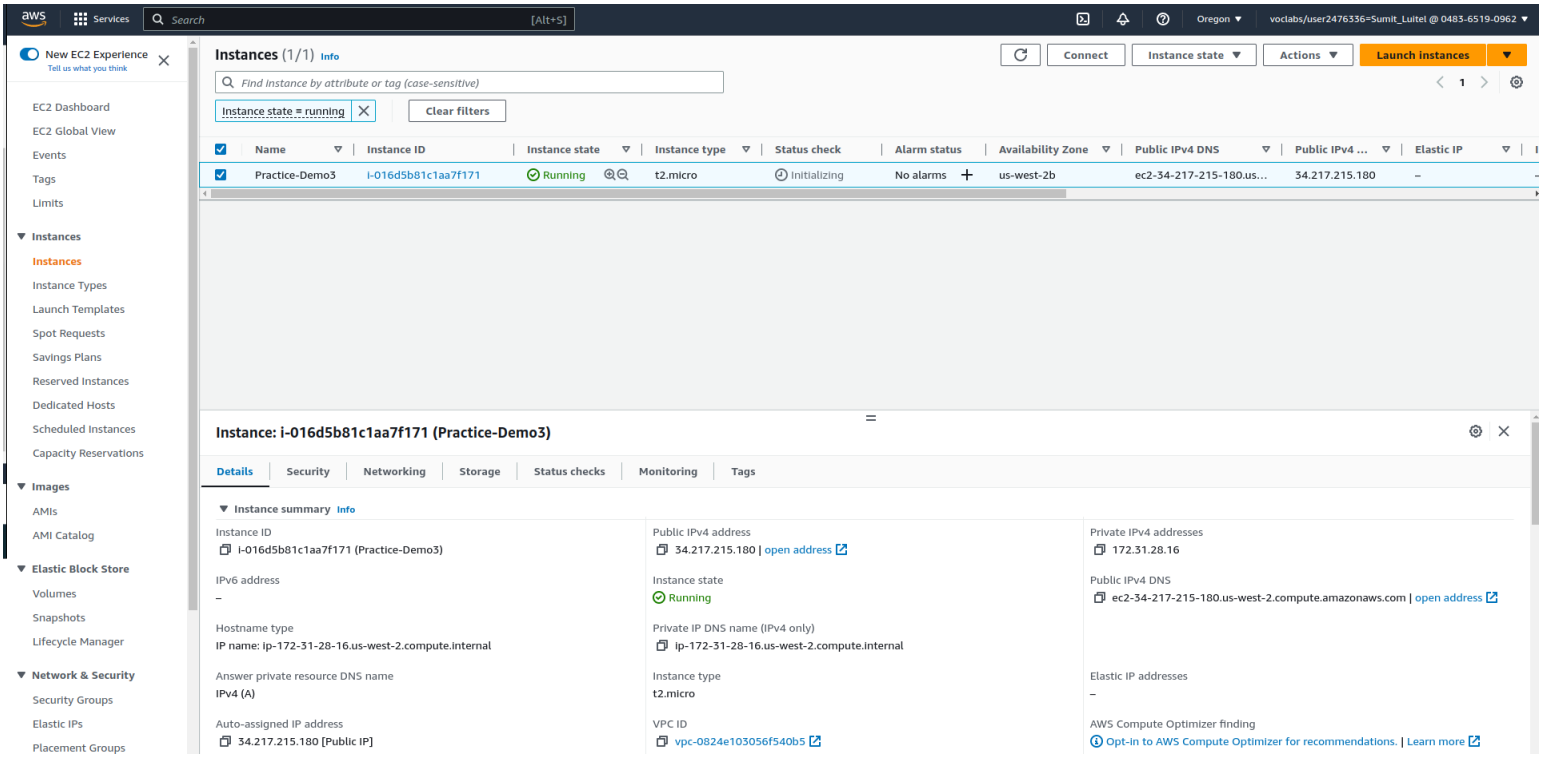


- Ping the private IP

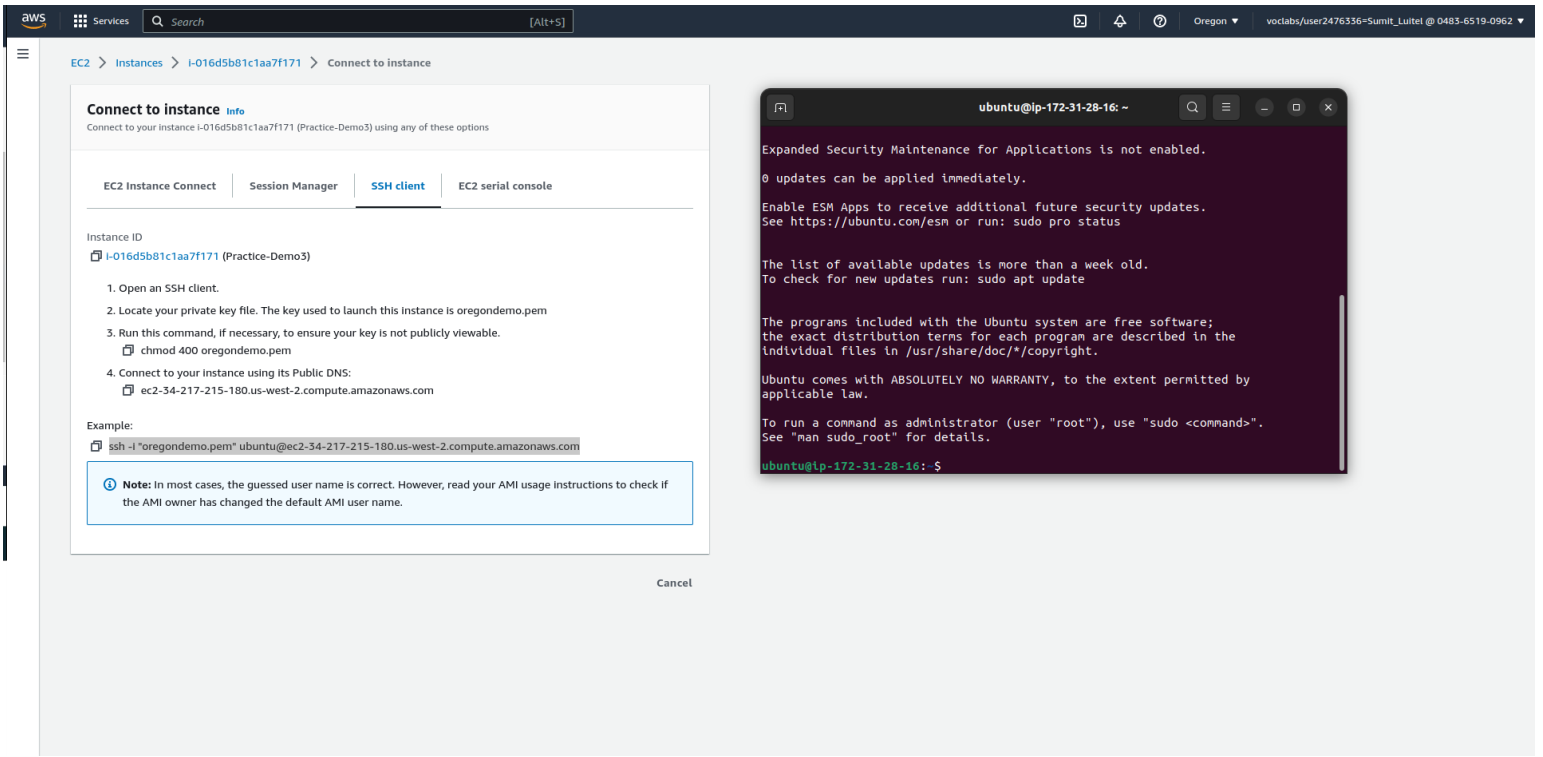


Create **new instance** in **new region** (**Oregon** in example)

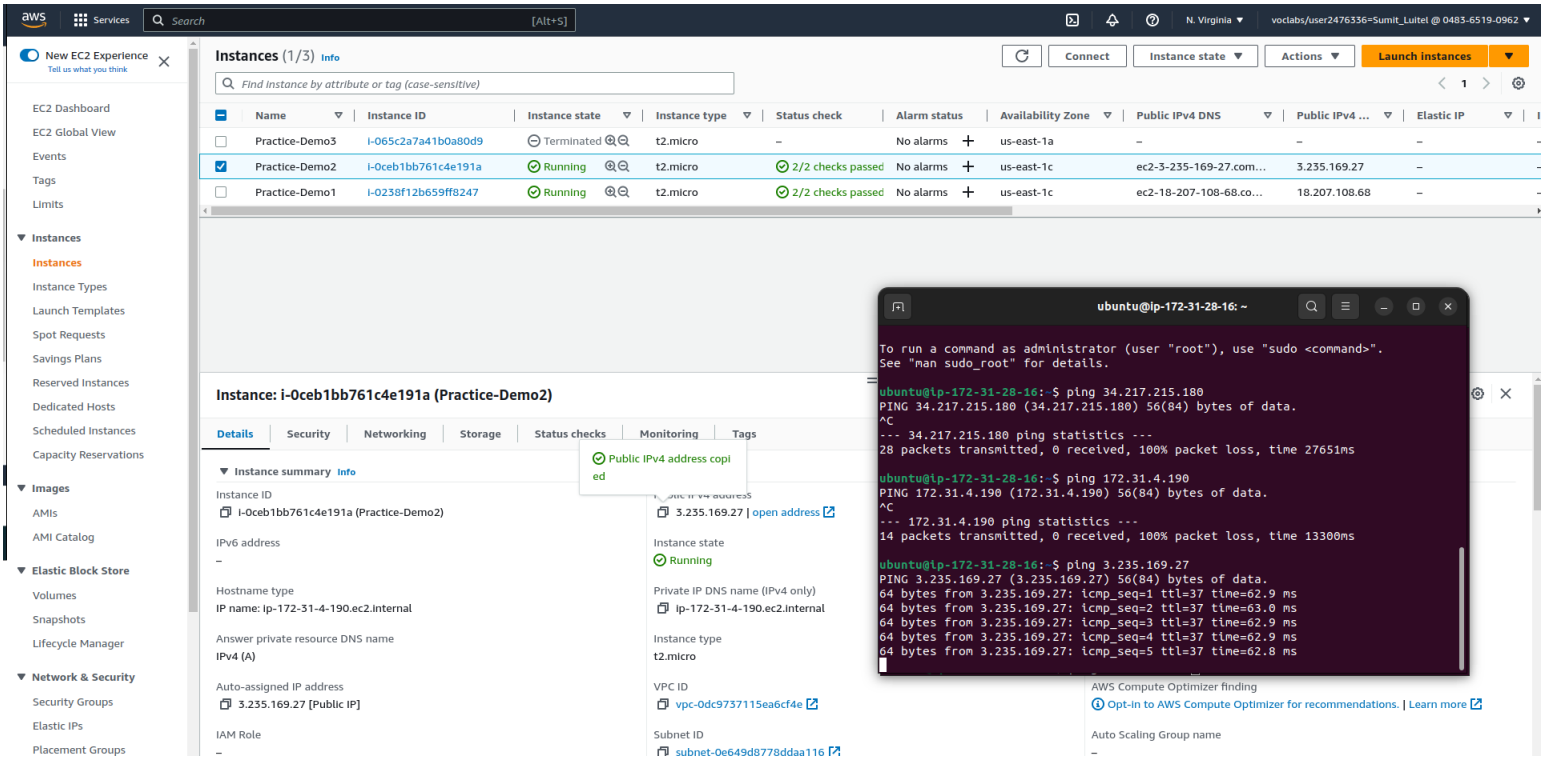




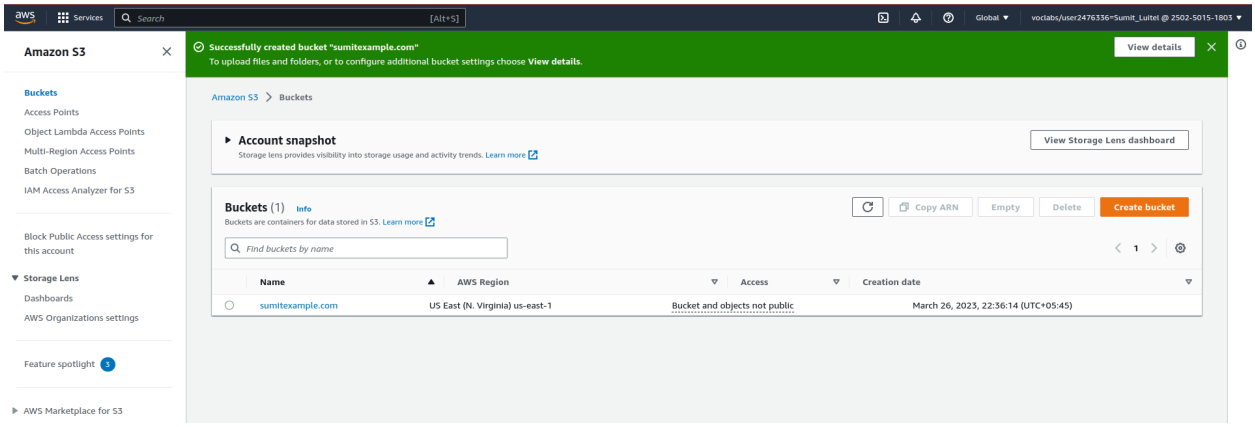
- Connection via SSH

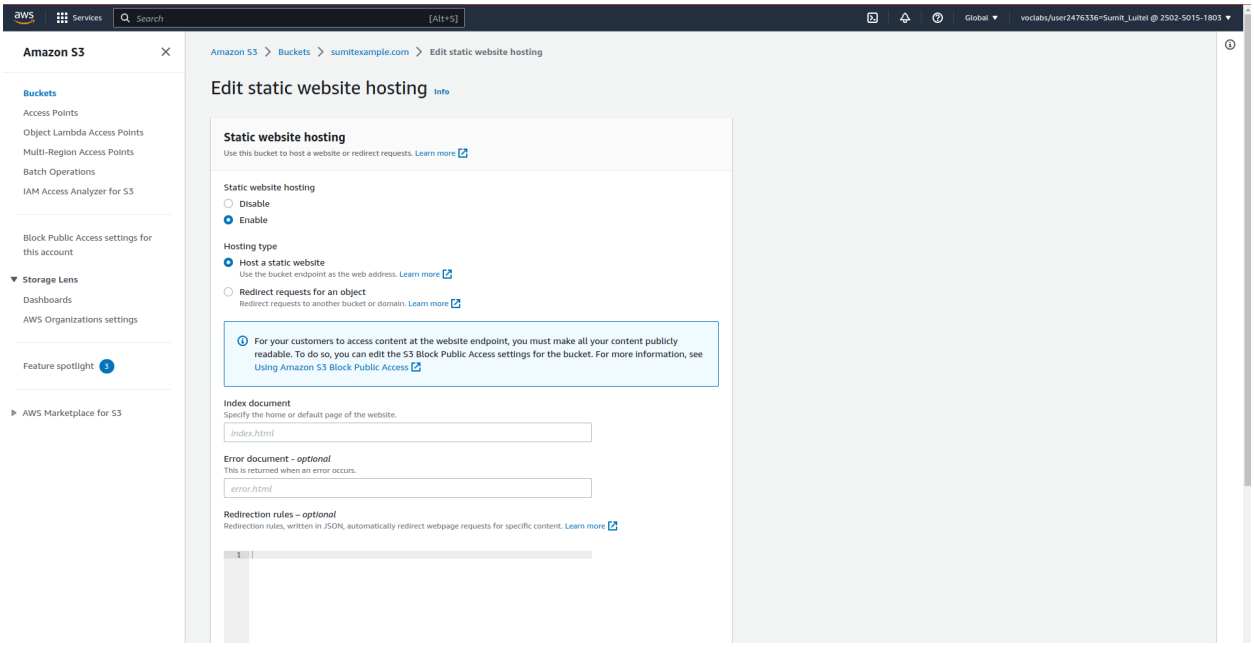


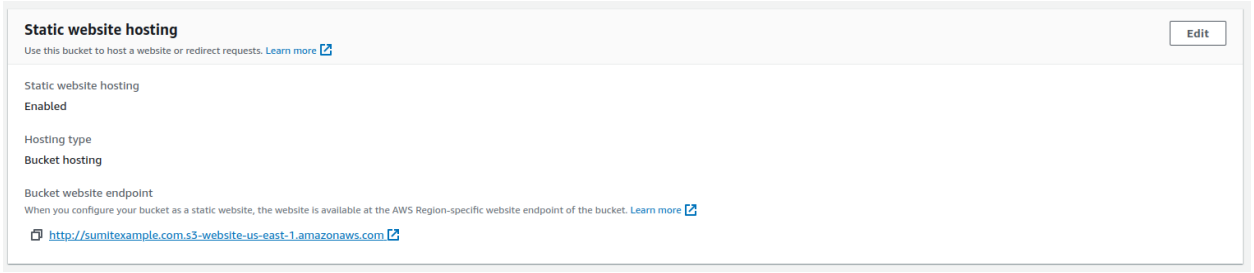
- Can be connected to Public IP
- Cannot be connected to Private IP



3. Configuring a static website on Amazon S3





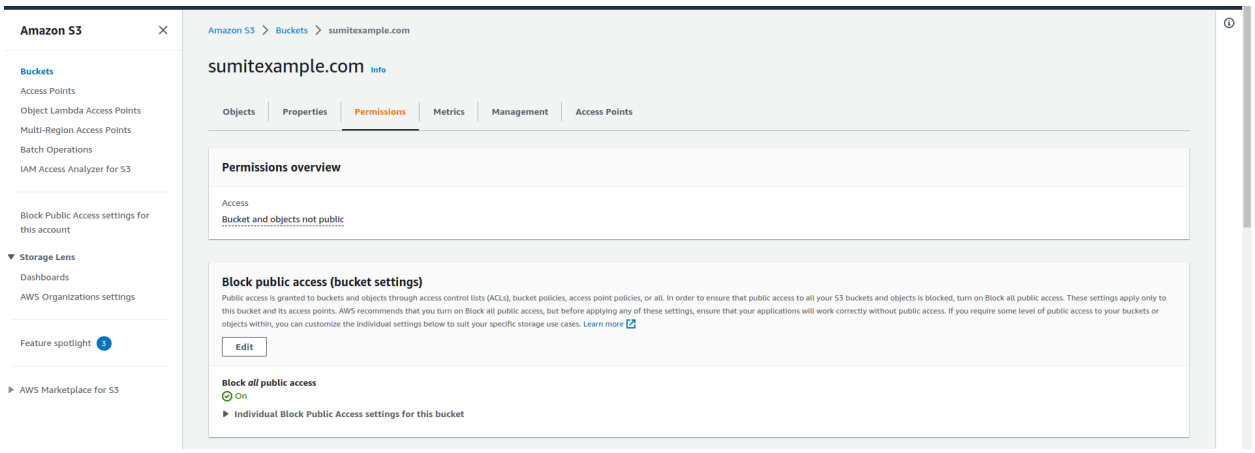


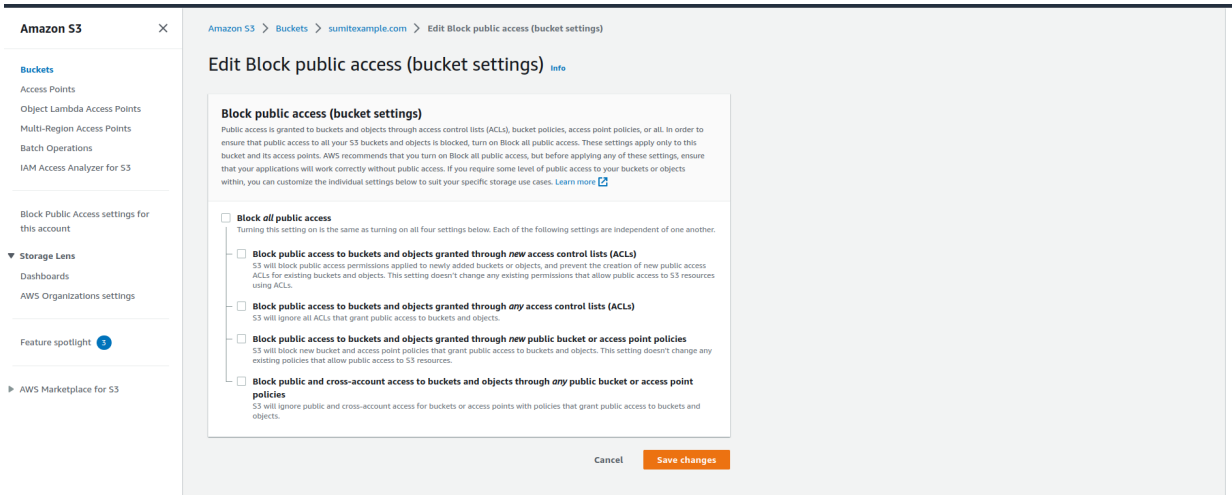
403 Forbidden

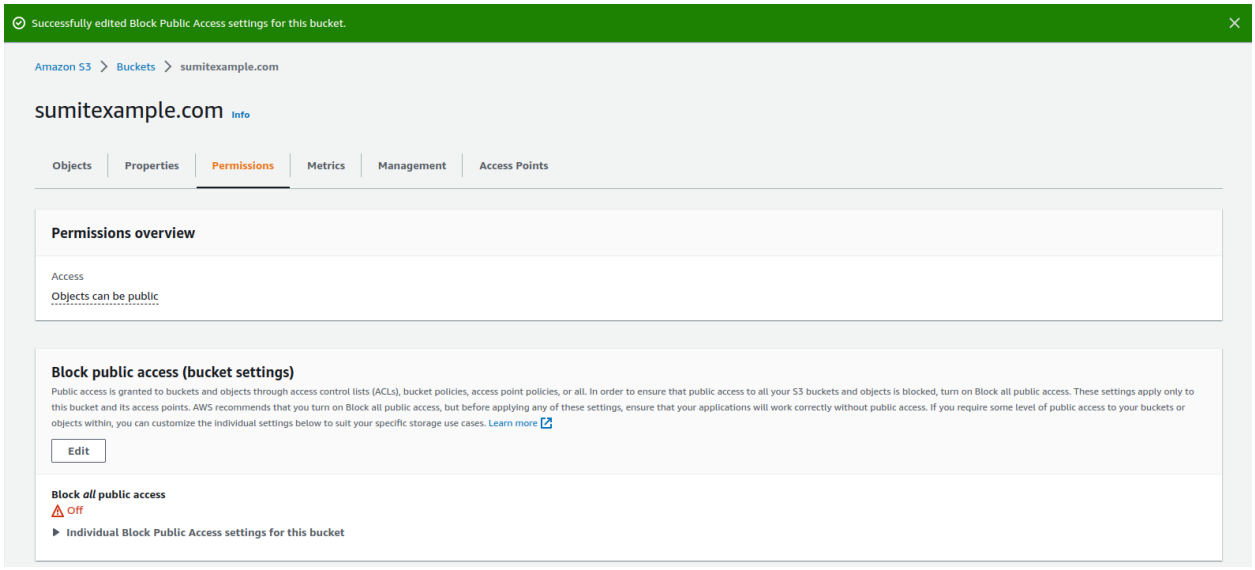
- Code: AccessDenied
- Message: Access Denied
- RequestId: 13Z395XPP79AYMRK
- HostId: gXYvBSZXwnDlEAjYQ9gFfwsReo3oJWg+z1WrbedIDt/SqRisgRkDFVDdYAwVuxCk/HjcVR8lQsc=

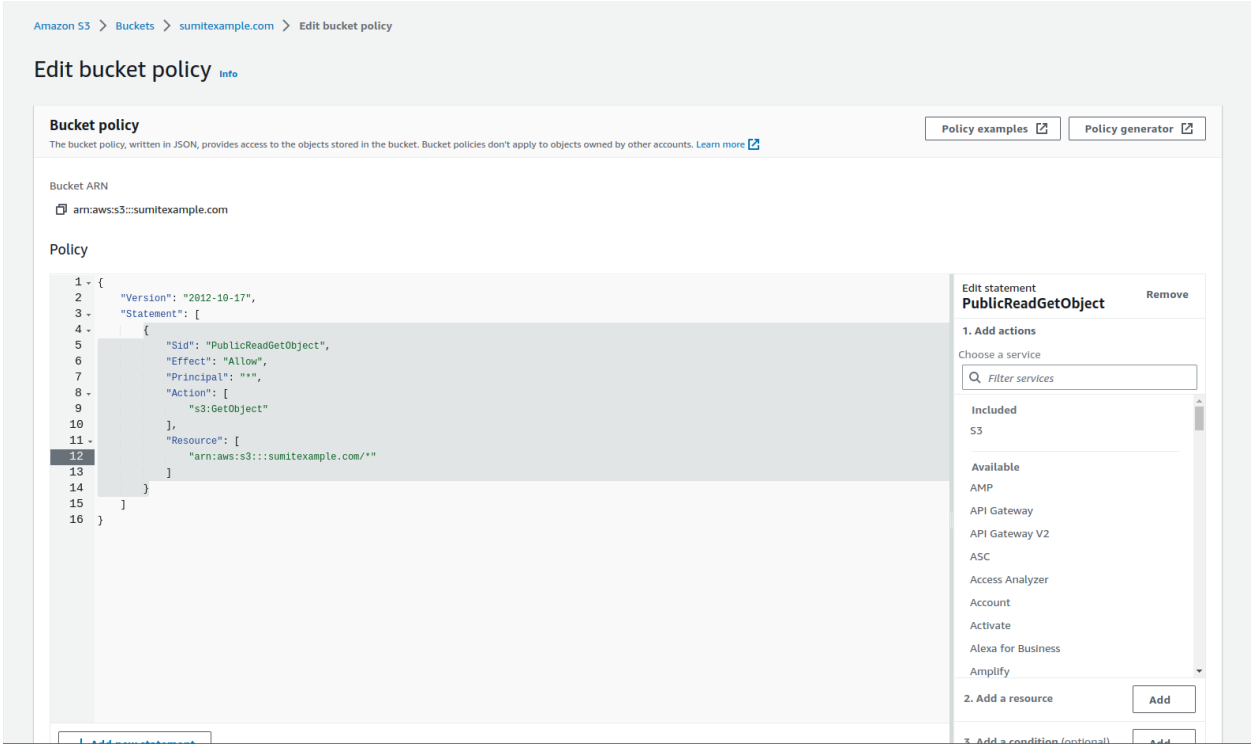
An Error Occurred While Attempting to Retrieve a Custom Error Document

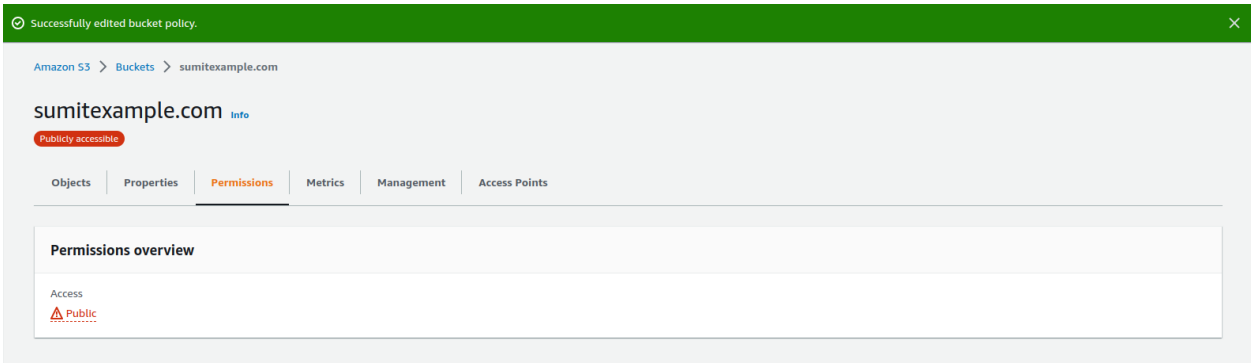
- Code: AccessDenied
- Message: Access Denied

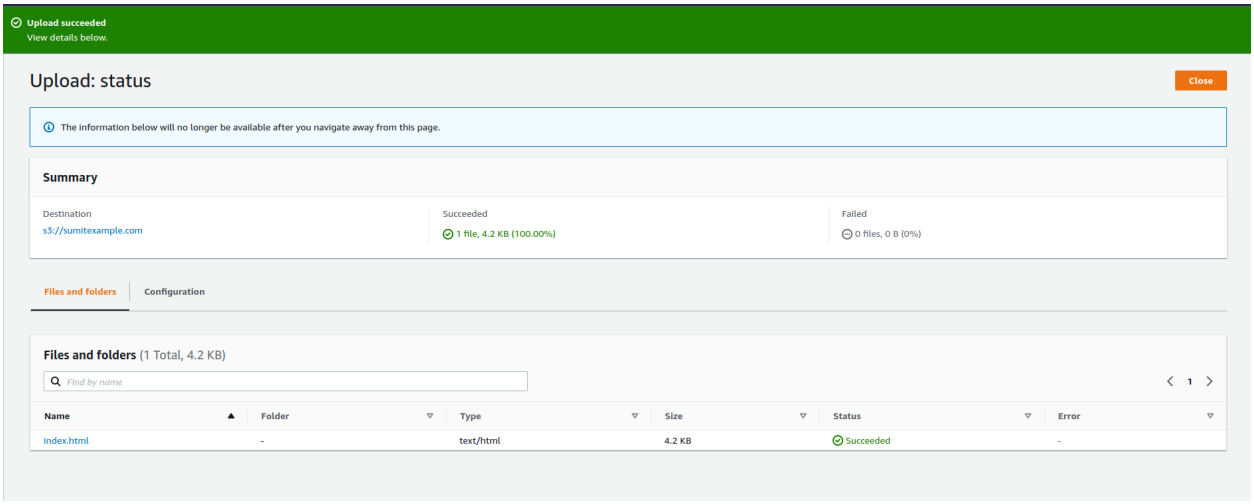

Amazon S3
Buckets
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
AWS Organizations settings
Feature spotlight
AWS Marketplace for S3
Amazon S3 > Buckets > sumitexample.com
sumitexample.com Info
Objects
Properties
Permissions
Metrics
Management
Access Points
Permissions overview
Access
Bucket and objects not public
Block public access (bucket settings)
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. Learn more
Edit
Block all public access
On
Individual Block Public Access settings for this bucket

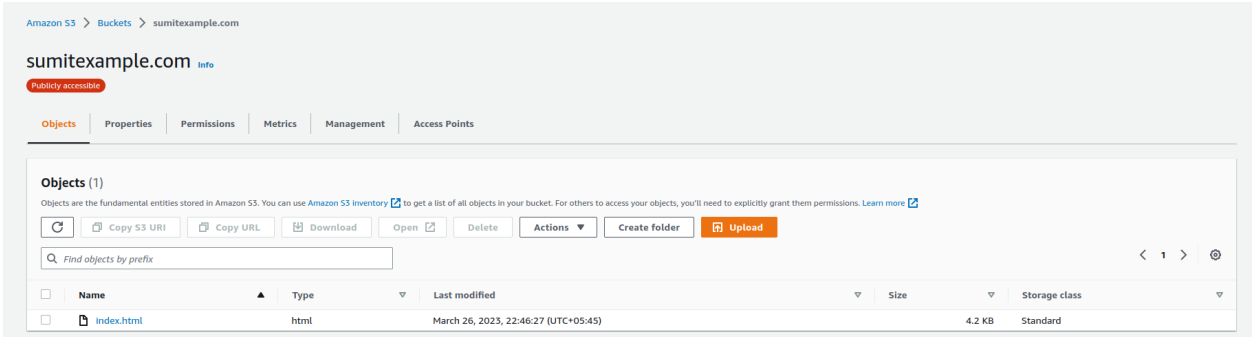

Amazon S3
Buckets
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
AWS Organizations settings
Feature spotlight
AWS Marketplace for S3
Amazon S3 > Buckets > sumitexample.com > Edit Block public access (bucket settings)
Edit Block public access (bucket settings) Info
Block public access (bucket settings)
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. 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.
Cancel
Save changes

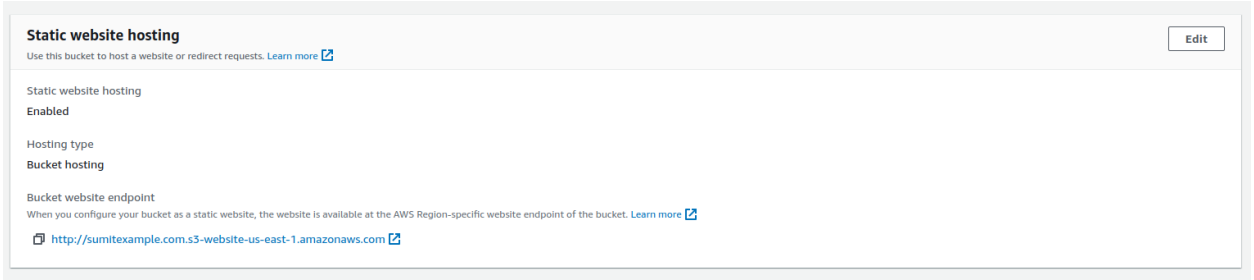

Successfully edited Block Public Access settings for this bucket.
Amazon S3 > Buckets > sumitexample.com
sumitexample.com Info
Objects
Properties
Permissions
Metrics
Management
Access Points
Permissions overview
Access
Objects can be public
Block public access (bucket settings)
Public access is granted 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. Learn more
Edit
Block all public access
Off
Individual Block Public Access settings for this bucket

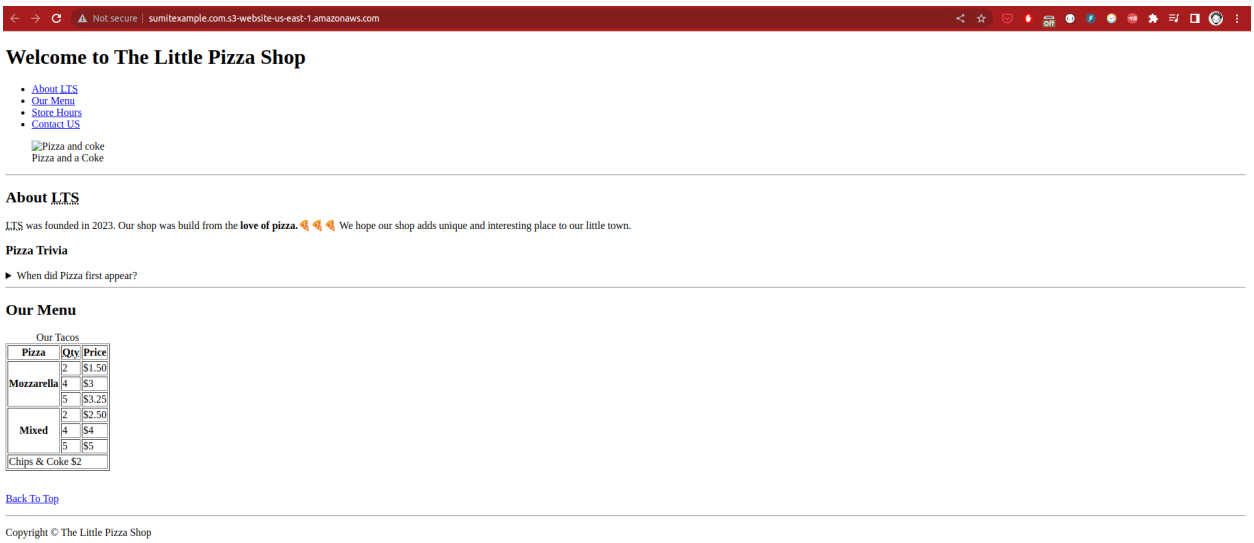

Amazon S3 > Buckets > sumitexample.com > Edit bucket policy
Edit bucket policy Info
Bucket policy
The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. Learn more
Policy examples
Policy generator
Bucket ARN
arn:aws:s3:::sumitexample.com
Policy
{
"Version": "2012-10-17",
"Statement": [
{
"Sid": "PublicReadGetObject",
"Effect": "Allow",
"Principal": "*",
"Action": [
"s3:GetObject"
],
"Resource": [
"arn:aws:s3:::sumitexample.com/*"
]
}
]
}
Edit statement
PublicReadGetObject
Remove
1. Add actions
Choose a service
Filter services
Included
S3
Available
AMP
API Gateway
API Gateway V2
ASC
Access Analyzer
Account
Activate
Alexa for Business
Amplify
2. Add a resource
Add


Successfully edited bucket policy.
Amazon S3 > Buckets > sumitexample.com
sumitexample.com Info
Publicly accessible
Objects
Properties
Permissions
Metrics
Management
Access Points
Permissions overview
Access
Public

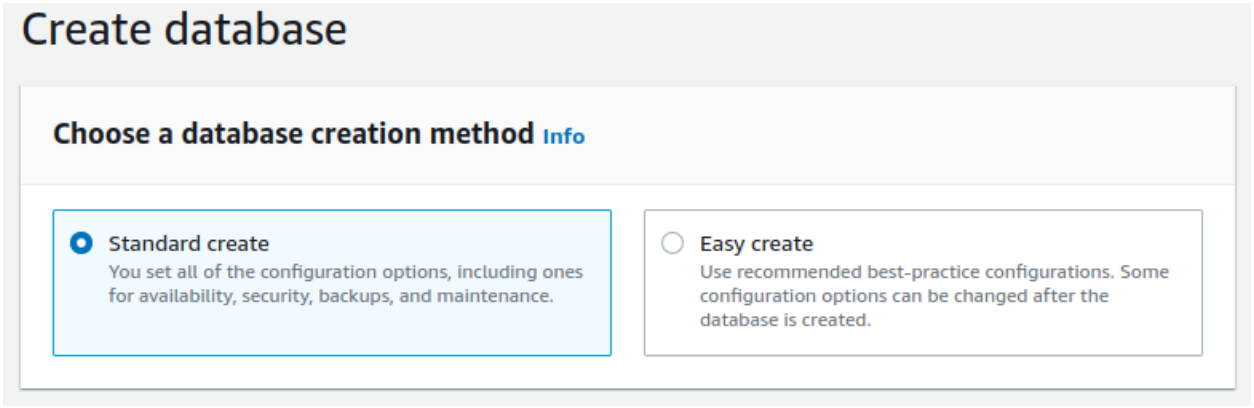

Upload succeeded
View details below.
Upload: status
Close
The information below will no longer be available after you navigate away from this page.
Summary
Destination
s3://sumitexample.com
Succeeded
1 file, 4.2 KB (100.00%)
Failed
0 files, 0 B (0%)
Files and folders
Configuration
Files and folders (1 Total, 4.2 KB)
Find by name
1
Name
Folder
Type
Size
Status
Error
index.html
-
text/html
4.2 KB
Succeeded
-


Amazon S3
Buckets
sumitexample.com
sumitexample.com
Info
Publicly accessible
Objects
Properties
Permissions
Metrics
Management
Access Points
Objects (1)
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
Copy S3 URI
Copy URL
Download
Open
Delete
Actions
Create folder
Upload
Find objects by prefix
1
Name
Type
Last modified
Size
Storage class
index.html
html
March 26, 2023, 22:46:27 (UTC+05:45)
4.2 KB
Standard


Static website hosting
Use this bucket to host a website or redirect requests. Learn more
Edit
Static website hosting
Enabled
Hosting type
Bucket hosting
Bucket website endpoint
When you configure your bucket as a static website, the website is available at the AWS Region-specific website endpoint of the bucket. Learn more
http://sumitexample.com.s3-website-us-east-1.amazonaws.com



4. Create and Connect to a MySQL Database with Amazon RDS



Engine options

Engine type Info

- ○ Aurora (MySQL Compatible)
- ○ Aurora (PostgreSQL Compatible)
- ◉ MySQL
- ○ MariaDB
- ○ PostgreSQL
- ○ Oracle
- ○ Microsoft SQL Server

Templates

Choose a sample template to meet your use case.

- ○ **Production**
  Use defaults for high availability and fast, consistent performance.
- ◉ **Dev/Test**
  This instance is intended for development use outside of a production environment.
- ○ **Free tier**
  Use RDS Free Tier to develop new applications, test existing applications, or gain hands-on experience with Amazon RDS.
  Info

Availability and durability

Deployment options Info

The deployment options below are limited to those supported by the engine you selected above.

- Multi-AZ DB Cluster - *new*
  Creates a DB cluster with a primary DB instance and two readable standby DB instances, with each DB instance in a different Availability Zone (AZ). Provides high availability, data redundancy and increases capacity to serve read workloads.
- Multi-AZ DB instance
  Creates a primary DB instance and a standby DB instance in a different AZ. Provides high availability and data redundancy, but the standby DB instance doesn't support connections for read workloads.
- (•) Single DB instance
  Creates a single DB instance with no standby DB instances.

Settings

DB instance identifier Info

Type a name for your DB instance. The name must be unique across all DB instances owned by your AWS account in the current AWS Region.

inventory-db

The DB instance identifier is case-insensitive, but is stored as all lowercase (as in "mydbinstance"). Constraints: 1 to 60 alphanumeric characters or hyphens. First character must be a letter. Can't contain two consecutive hyphens. Can't end with a hyphen.

▼ Credentials Settings

Master username Info

Type a login ID for the master user of your DB instance.

admin

1 to 16 alphanumeric characters. First character must be a letter.

☐ Manage master credentials in AWS Secrets Manager
Manage master user credentials in Secrets Manager. RDS can generate a password for you and manage it throughout its lifecycle.

ⓘ If you manage the master user credentials in Secrets Manager, some RDS features aren't supported.
Learn more

Instance configuration

The DB instance configuration options below are limited to those supported by the engine that you selected above.

DB instance class Info

- ○ Standard classes (includes m classes)
- ○ Memory optimized classes (includes r and x classes)
- ◉ Burstable classes (includes t classes)

db.t3.micro
2 vCPUs 1 GiB RAM Network: 2,085 Mbps

Include previous generation classes

Storage

Storage type Info

General Purpose SSD (gp2)
Baseline performance determined by volume size

Allocated storage Info

20 GiB

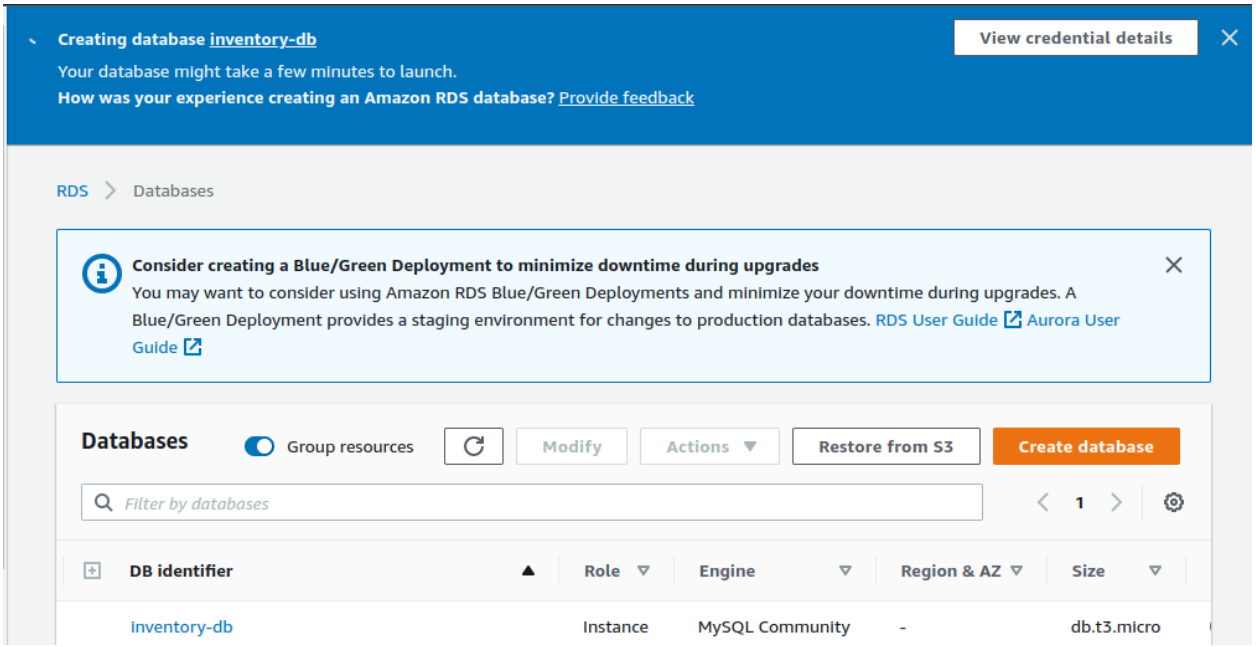
The minimum value is 20 GiB and the maximum value is 6,144 GiB

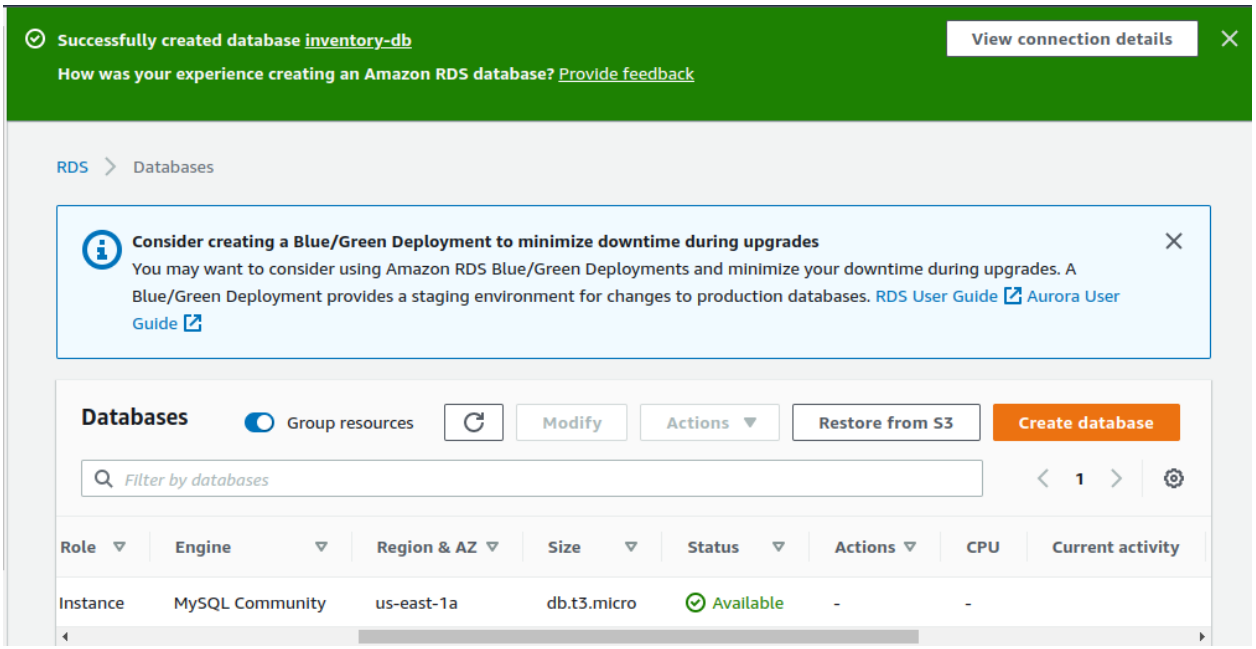
Provisioning less than 100 GiB of General Purpose (SSD) storage for high throughput workloads could result in higher latencies upon exhaustion of the initial General Purpose (SSD) IO credit balance. Learn more

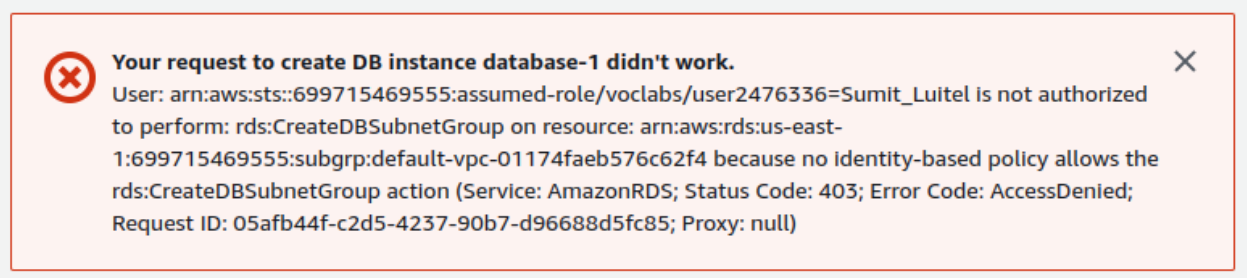
Storage autoscaling Info

Provides dynamic scaling support for your database's storage based on your application's needs.

☑ Enable storage autoscaling
Enabling this feature will allow the storage to increase after the specified threshold is exceeded.





Cannot connect to the server via VSCode.

Error when following class session. Cannot Create a database.