Terna Engineering College
Computer Engineering Department
Program: Sem VIII

Course: Cloud Computing Lab (CSL803)

Faculty: Reshma Koli

Experiment No. 4

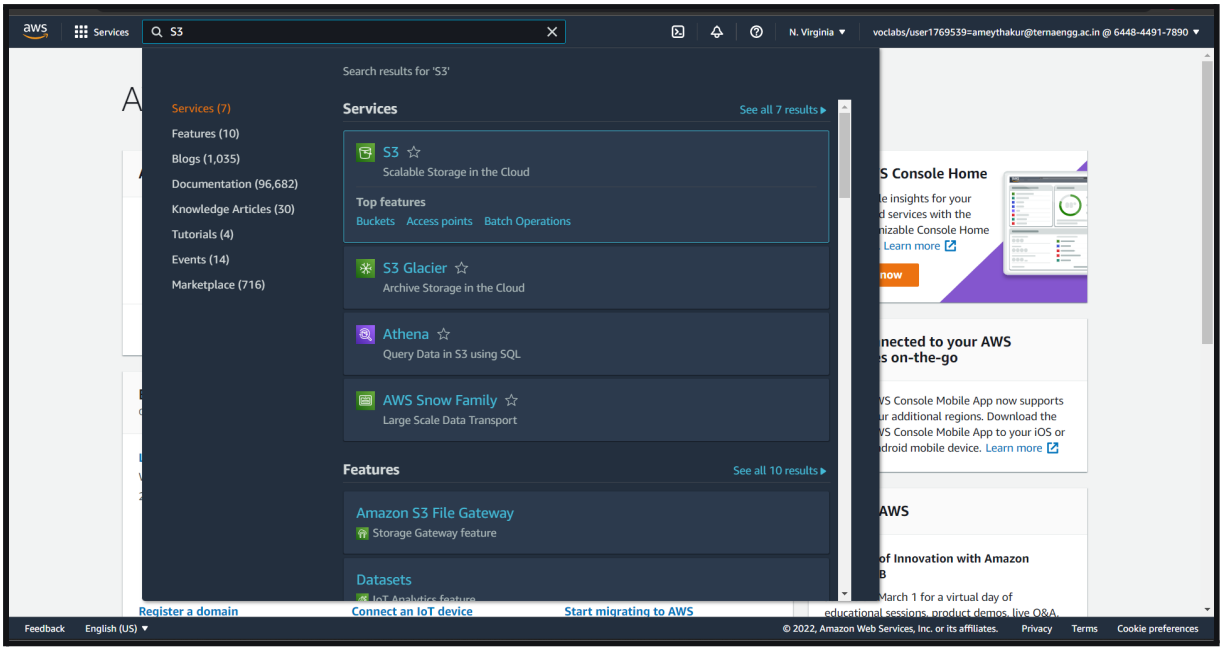
A.1 Aim: To demonstrate and implement Storage as a service using AWS S3 Service.

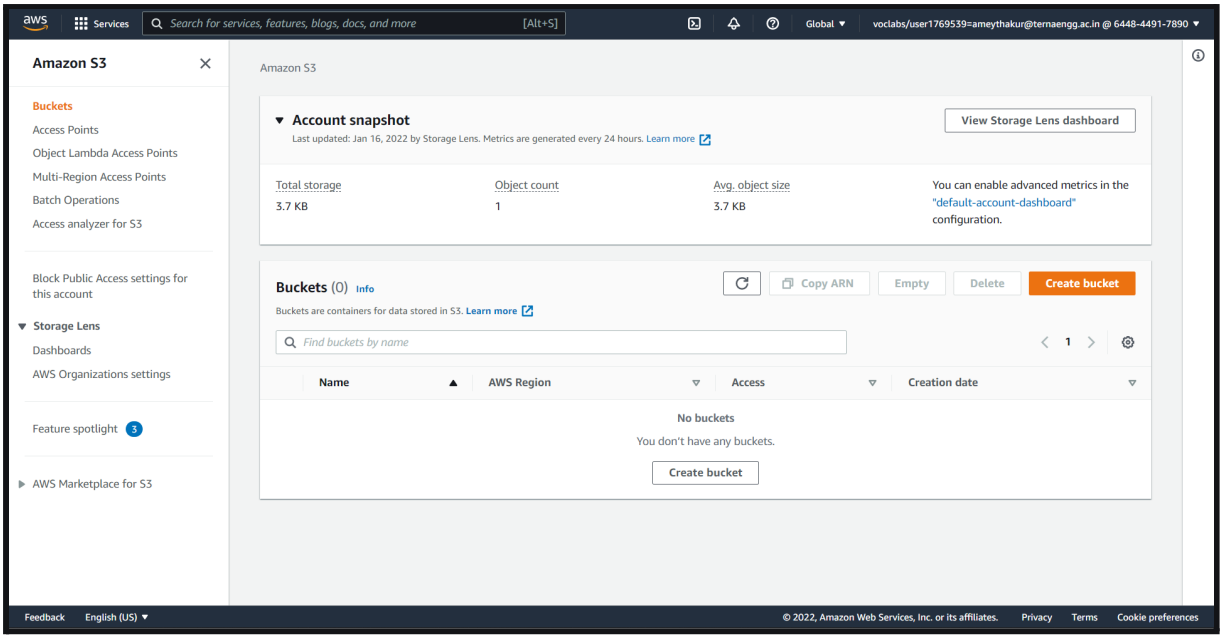
PART B
(PART B: TO BE COMPLETED BY STUDENTS)

Roll No. 50	**Name:** AMEY MAHENDRA THAKUR
Class: BE COMPS B 50	**Batch:** B3
Date of Experiment: 14-02-2022	**Date of Submission:** 14-02-2022
Grade:	

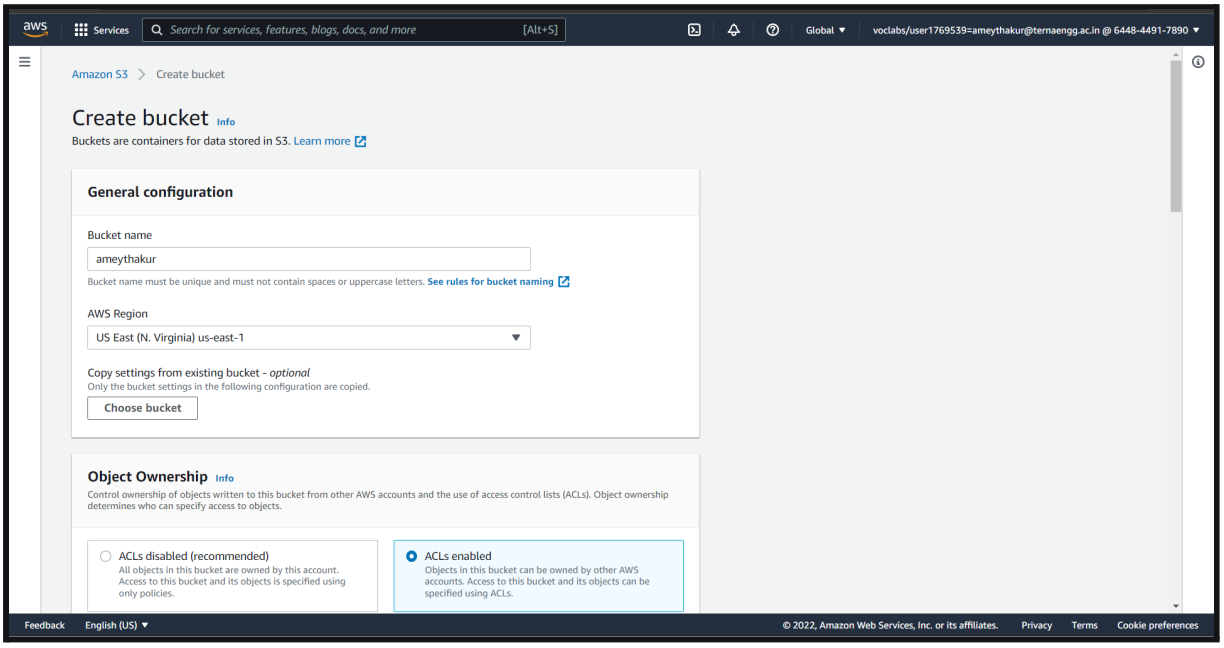
B.1 Question of Curiosity:
Q1: Create Bucket using AWS S3 service (Add stepwise screenshots of the same).
ANS:
Practical Video (AWS S3 Service): https://youtu.be/CnM07Vg7pW8

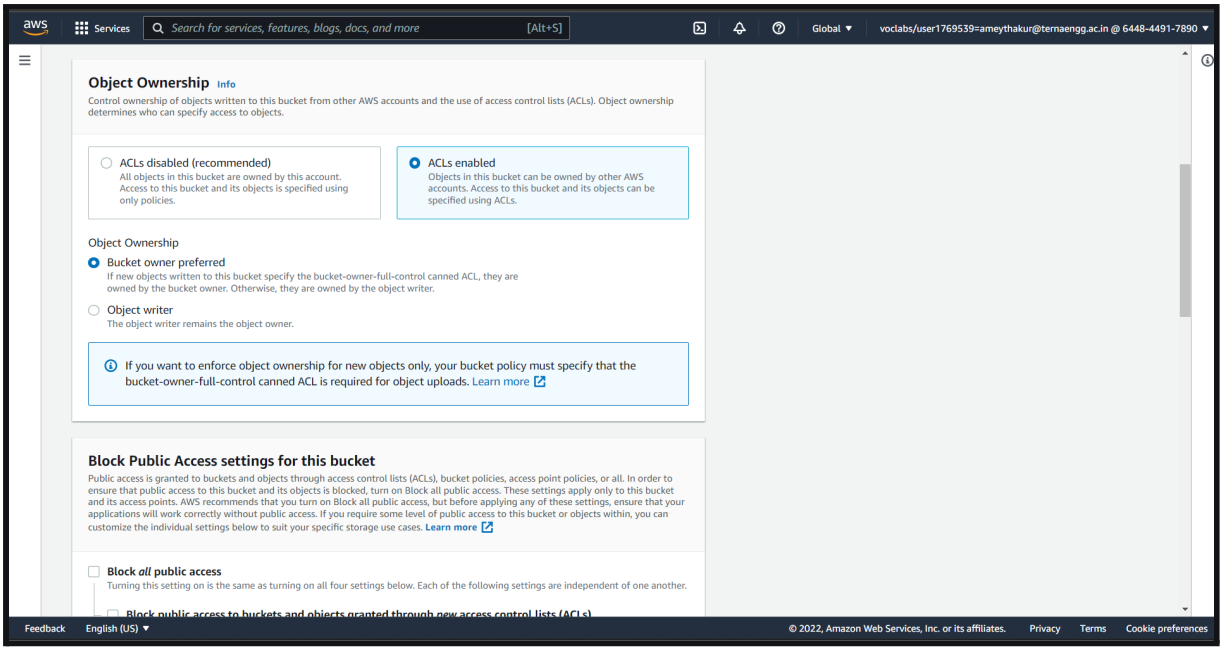
Step 1: Create S3

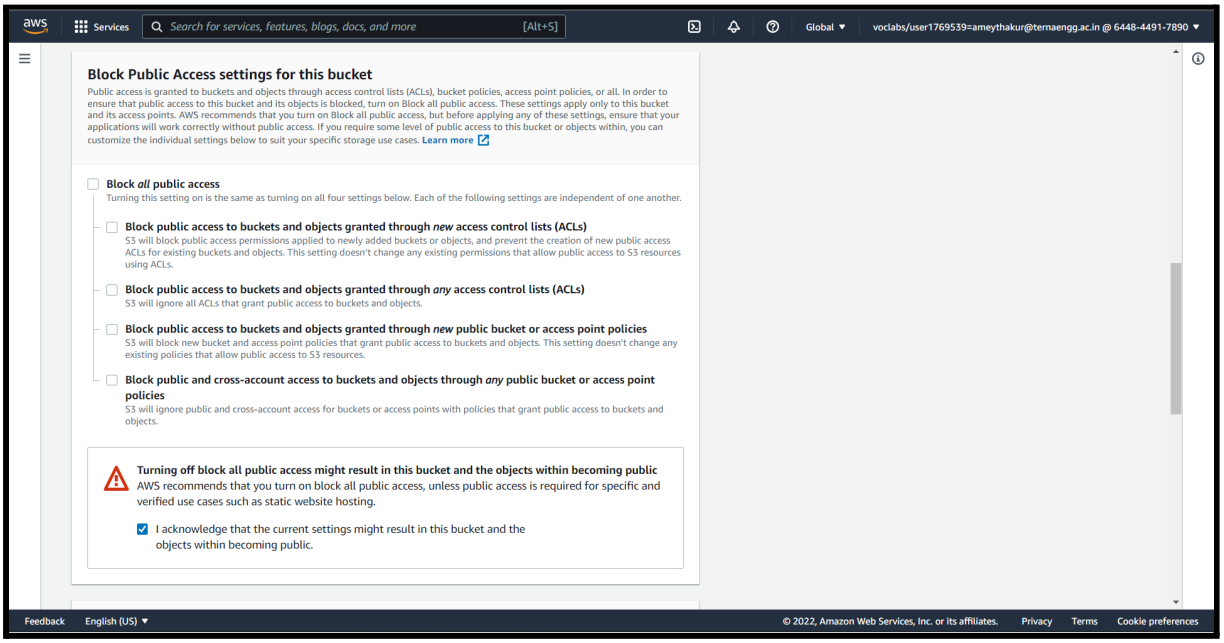


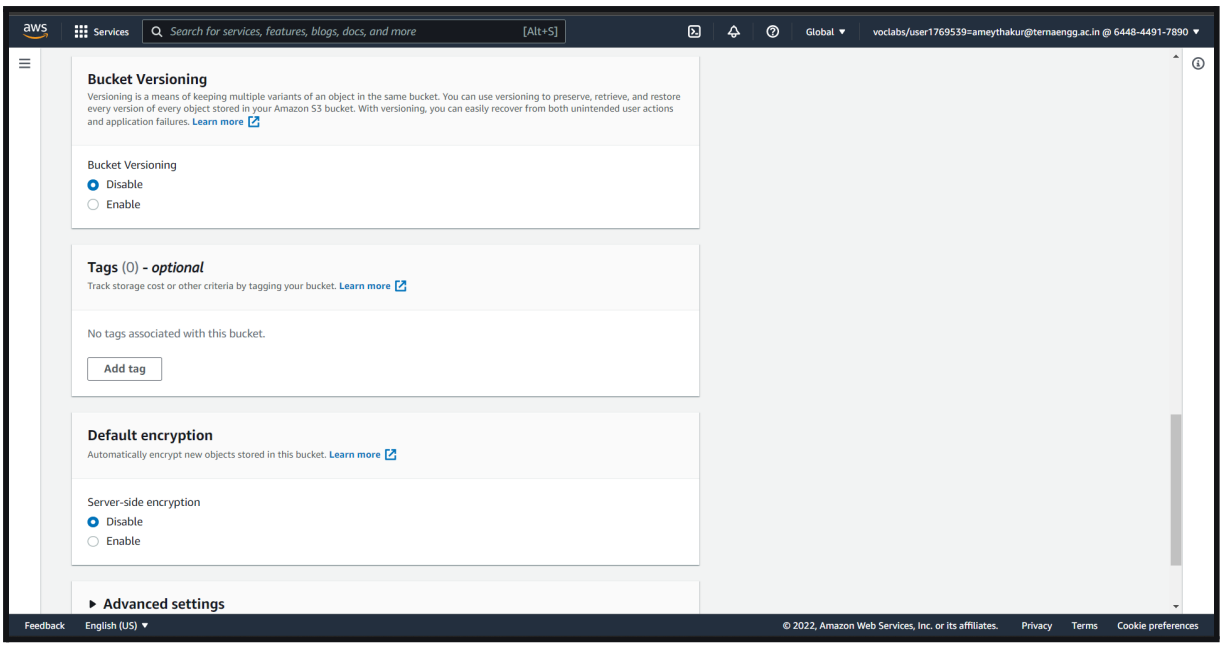


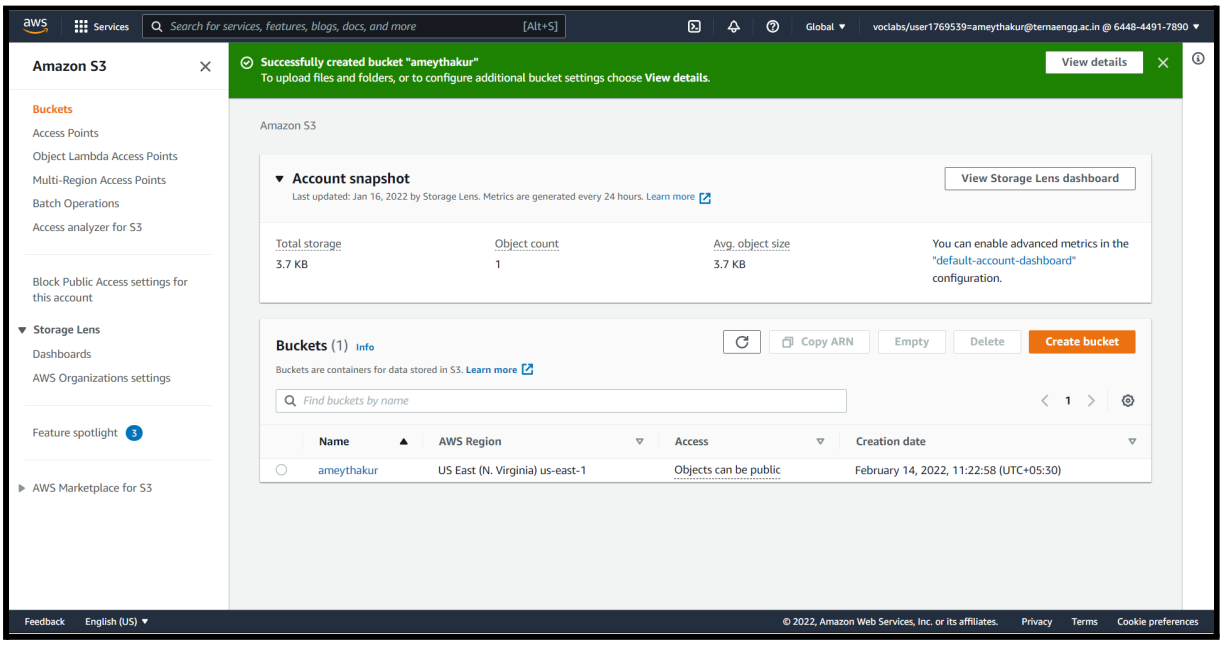
Step 2: Create Bucket

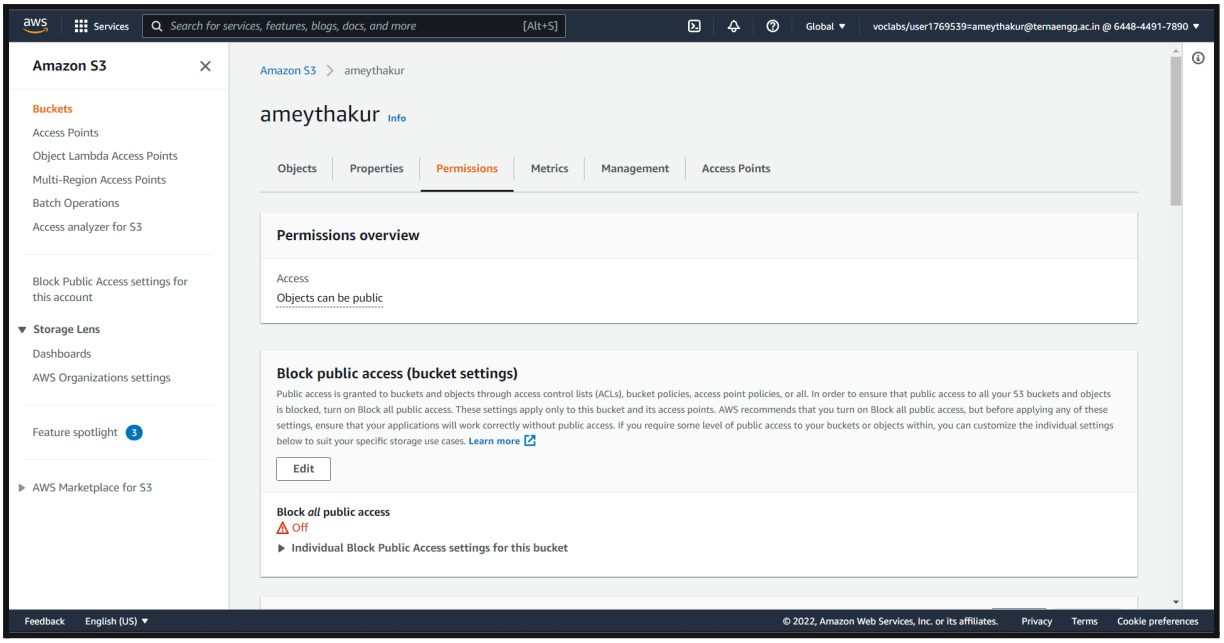


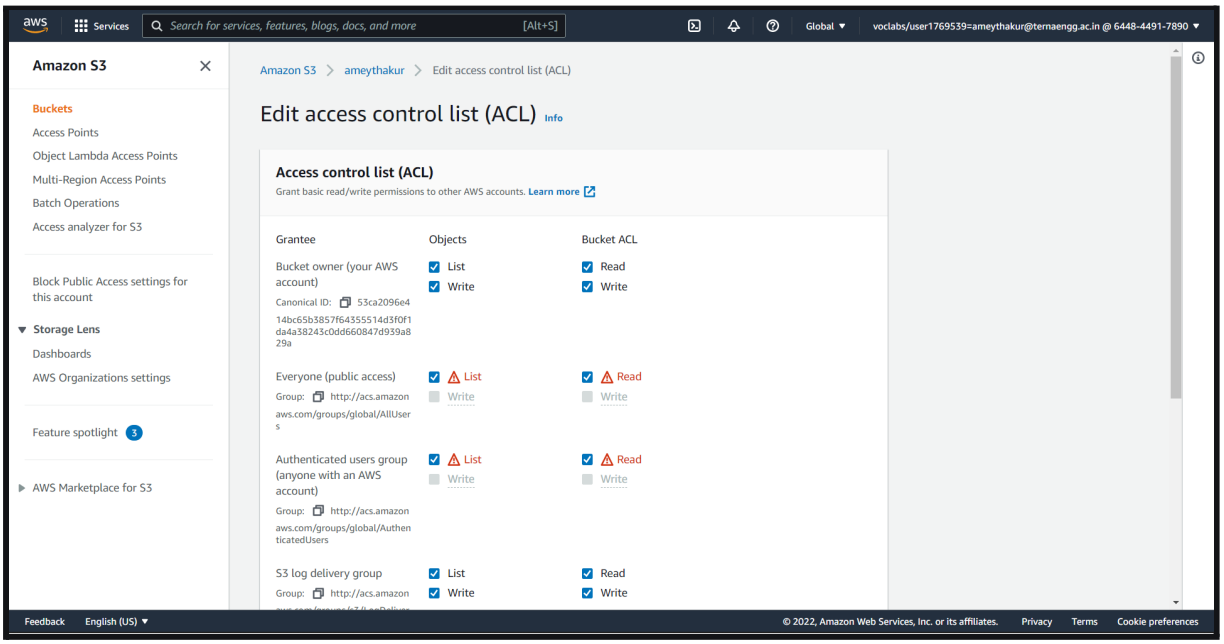

aws
Services
Search for services, features, blogs, docs, and more
[Alt+S]
Global
voclabs/user1769539=ameythakur@ternaengg.ac.in @ 6448-4491-7890
Object Ownership Info
Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.
ACLs disabled (recommended)
All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.
ACLs enabled
Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.
Object Ownership
Bucket owner preferred
If new objects written to this bucket specify the bucket-owner-full-control canned ACL, they are owned by the bucket owner. Otherwise, they are owned by the object writer.
Object writer
The object writer remains the object owner.
If you want to enforce object ownership for new objects only, your bucket policy must specify that the bucket-owner-full-control canned ACL is required for object uploads. Learn more
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.
Feedback
English (US)
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

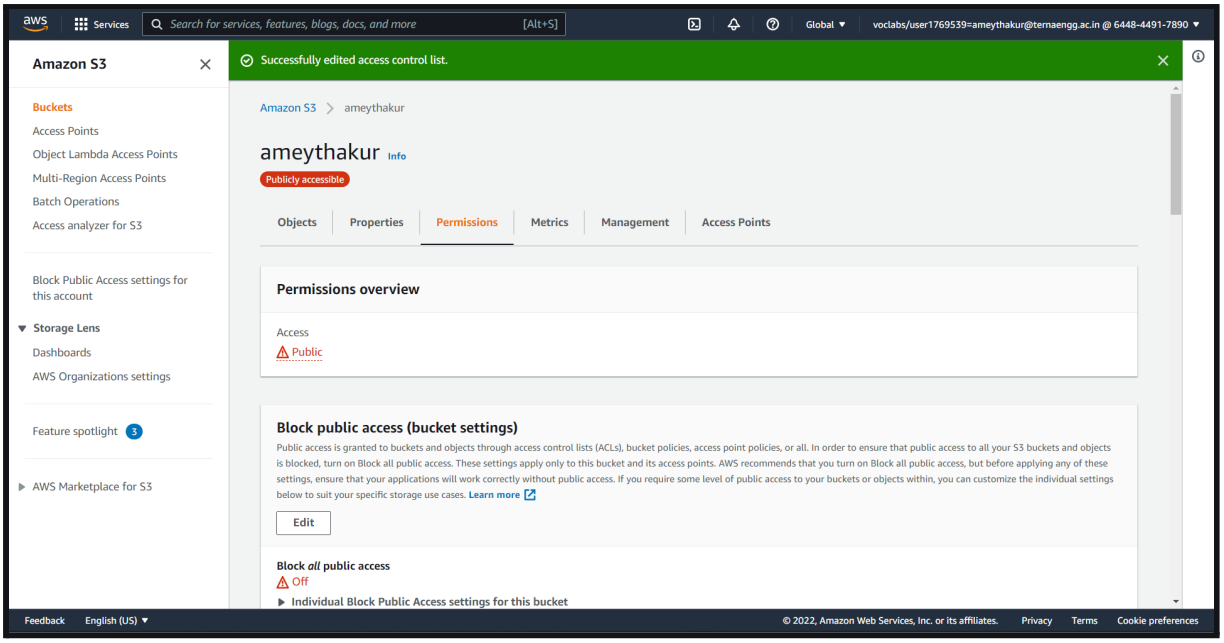

aws
Services
Search for services, features, blogs, docs, and more
[Alt+S]
Global
voclabs/user1769539=ameythakur@ternaengg.ac.in @ 6448-4491-7890
Block Public Access settings for this bucket
Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point 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.
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.
Feedback
English (US)
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

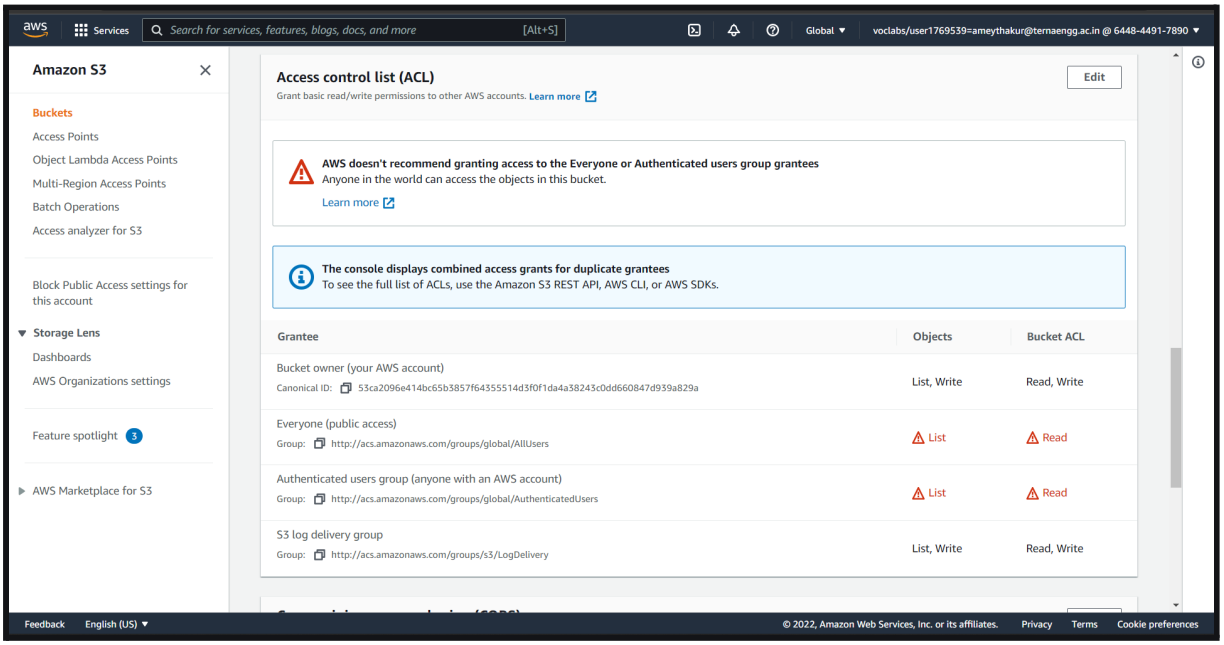

Services
Search for services, features, blogs, docs, and more [Alt+S]
Global
voclabs/user1769539=ameythakur@ternaengg.ac.in @ 6448-4491-7890
Bucket Versioning
Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore 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
Tags (0) - optional
Track storage cost or other criteria by tagging your bucket. Learn more
No tags associated with this bucket.
Add tag
Default encryption
Automatically encrypt new objects stored in this bucket. Learn more
Server-side encryption
Disable
Enable
Advanced settings
Feedback
English (US)
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

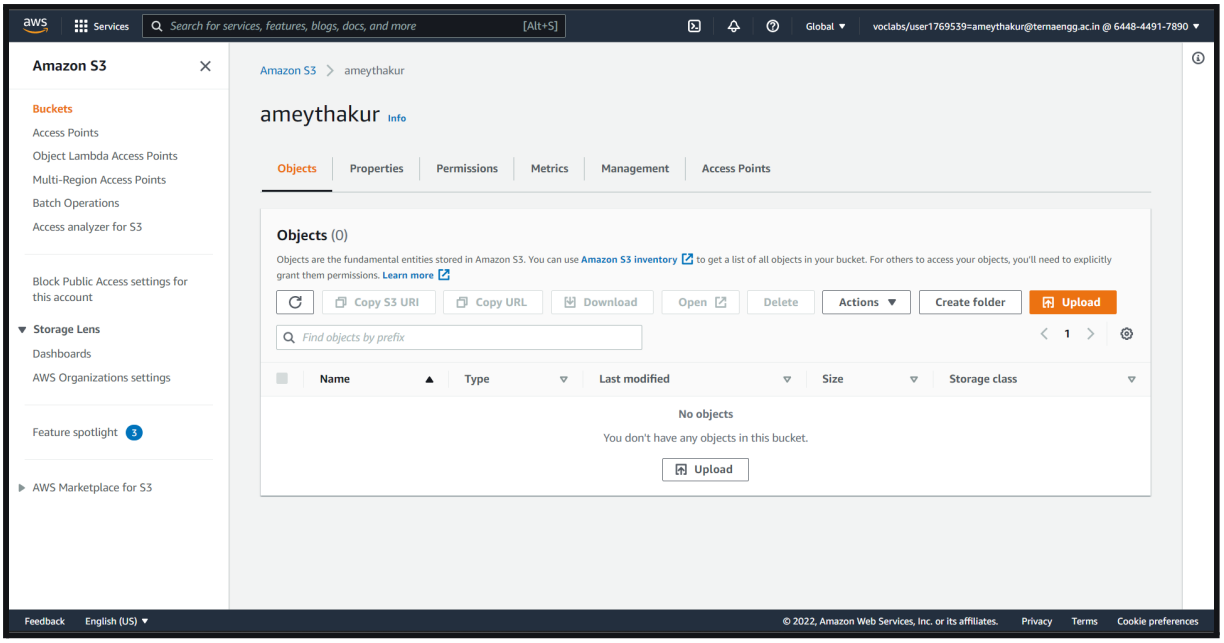

Services
Search for services, features, blogs, docs, and more [Alt+S]
Global
voclabs/user1769539=ameythakur@ternaengg.ac.in @ 6448-4491-7890
Amazon S3
Buckets
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
Access analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
AWS Organizations settings
Feature spotlight 3
AWS Marketplace for S3
Successfully created bucket "ameythakur"
To upload files and folders, or to configure additional bucket settings choose View details.
View details
Amazon S3
Account snapshot
Last updated: Jan 16, 2022 by Storage Lens. Metrics are generated every 24 hours. Learn more
View Storage Lens dashboard
Total storage
3.7 KB
Object count
1
Avg. object size
3.7 KB
You can enable advanced metrics in the "default-account-dashboard" configuration.
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
ameythakur
US East (N. Virginia) us-east-1
Objects can be public
February 14, 2022, 11:22:58 (UTC+05:30)
Feedback
English (US)
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

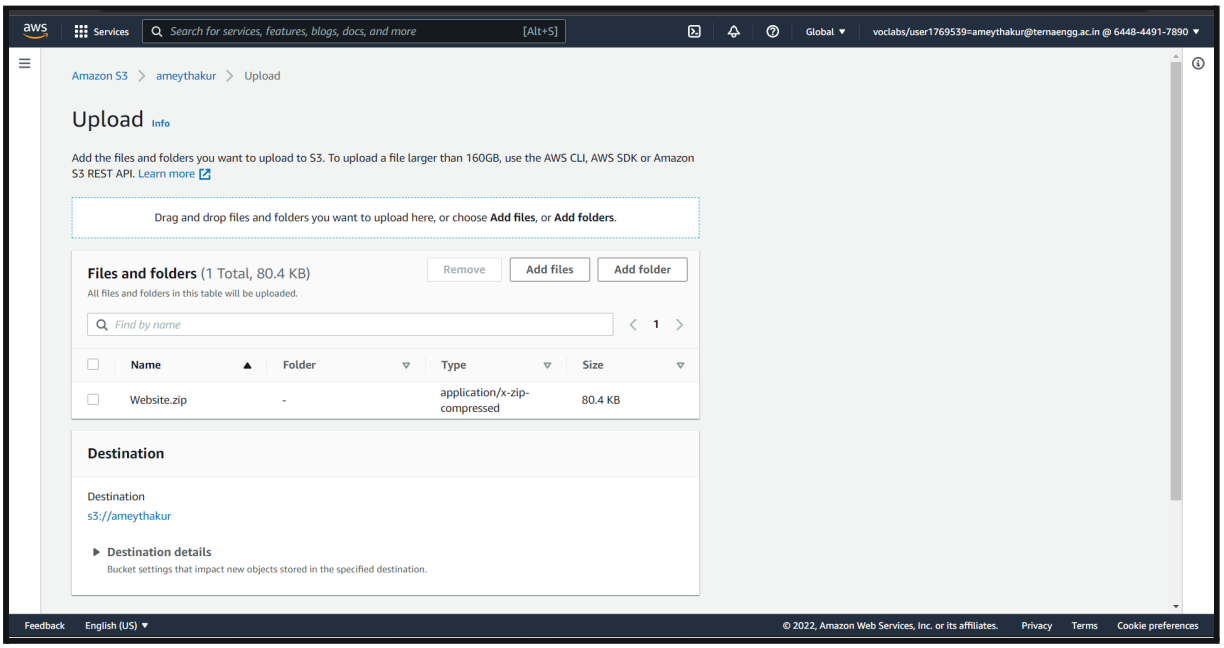

Services
Search for services, features, blogs, docs, and more [Alt+S]
Global
voclabs/user1769539=ameythakur@ternaengg.ac.in @ 6448-4491-7890
Amazon S3
Buckets
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
Access analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
AWS Organizations settings
Feature spotlight 3
AWS Marketplace for S3
Amazon S3 > ameythakur
ameythakur 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
Feedback
English (US)
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

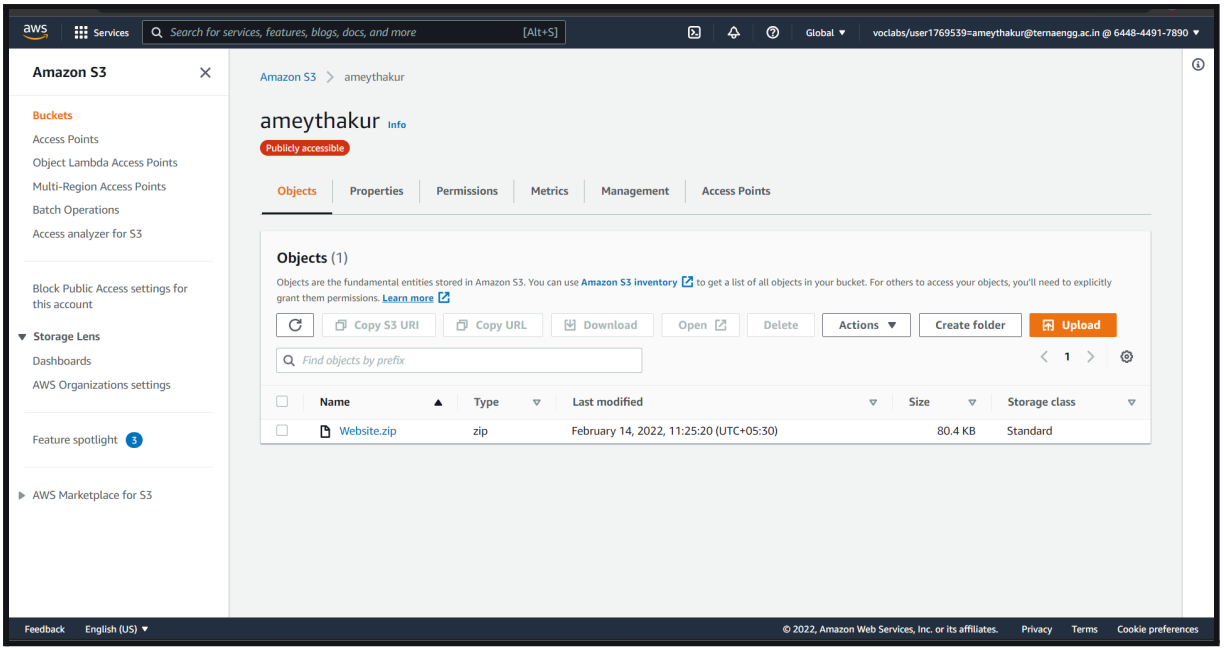

Services
Search for services, features, blogs, docs, and more [Alt+S]
Global
voclabs/user1769539=ameythakur@ternaengg.ac.in @ 6448-4491-7890
Amazon S3
Buckets
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
Access analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
AWS Organizations settings
Feature spotlight 3
AWS Marketplace for S3
Amazon S3 > ameythakur > Edit access control list (ACL)
Edit access control list (ACL) Info
Access control list (ACL)
Grant basic read/write permissions to other AWS accounts. Learn more
Grantee
Objects
Bucket ACL
Bucket owner (your AWS account)
Canonical ID: 53ca2096e4
14bc65b3857f64355514d3f0f1da4a38243c0dd660847d939a829a
List
Write
Read
Write
Everyone (public access)
Group: http://acs.amazonaws.com/groups/global/AllUsers
List
Write
Read
Write
Authenticated users group (anyone with an AWS account)
Group: http://acs.amazonaws.com/groups/global/AuthenticatedUsers
List
Write
Read
Write
S3 log delivery group
Group: http://acs.amazon
List
Write
Read
Write
Feedback
English (US)
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

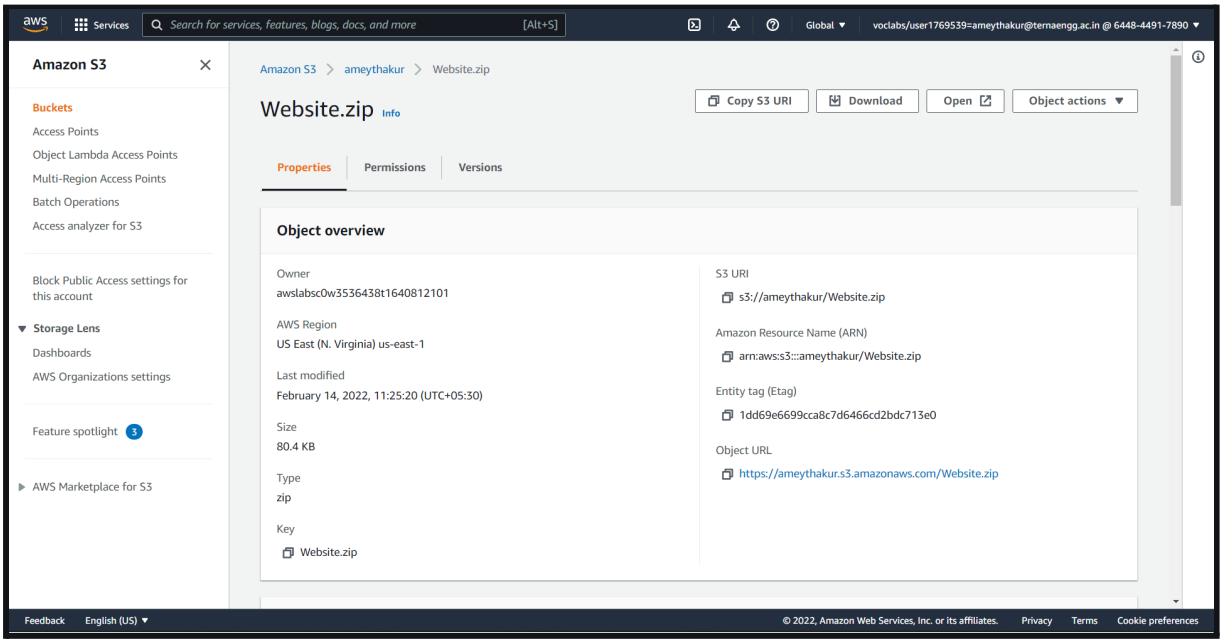

Services
Search for services, features, blogs, docs, and more [Alt+S]
Global
voclabs/user1769539=ameythakur@ternaengg.ac.in @ 6448-4491-7890
Amazon S3
Successfully edited access control list.
Buckets
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
Access analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
AWS Organizations settings
Feature spotlight 3
AWS Marketplace for S3
Amazon S3 > ameythakur
ameythakur Info
Publicly accessible
Objects
Properties
Permissions
Metrics
Management
Access Points
Permissions overview
Access
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
Feedback
English (US)
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

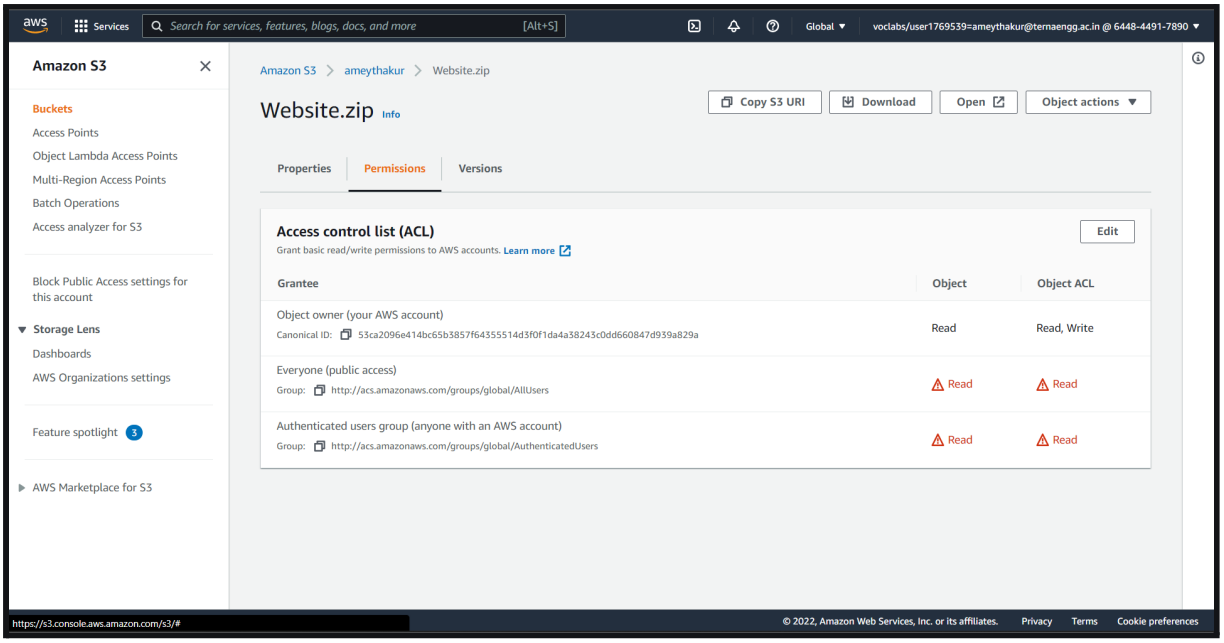

Services
Search for services, features, blogs, docs, and more [Alt+S]
Global
voclabs/user1769539=ameythakur@ternaengg.ac.in @ 6448-4491-7890
Amazon S3
Buckets
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
Access analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
AWS Organizations settings
Feature spotlight 3
AWS Marketplace for S3
Access control list (ACL)
Grant basic read/write permissions to other AWS accounts. Learn more
Edit
AWS doesn't recommend granting access to the Everyone or Authenticated users group grantees
Anyone in the world can access the objects in this bucket.
Learn more
The console displays combined access grants for duplicate grantees
To see the full list of ACLs, use the Amazon S3 REST API, AWS CLI, or AWS SDKs.
Grantee
Objects
Bucket ACL
Bucket owner (your AWS account)
Canonical ID: 53ca2096e414bc65b3857f64355514d3f0f1da4a38243c0dd660847d939a829a
List, Write
Read, Write
Everyone (public access)
Group: http://acs.amazonaws.com/groups/global/AllUsers
List
Read
Authenticated users group (anyone with an AWS account)
Group: http://acs.amazonaws.com/groups/global/AuthenticatedUsers
List
Read
S3 log delivery group
Group: http://acs.amazonaws.com/groups/s3/LogDelivery
List, Write
Read, Write
Feedback
English (US)
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Services
Search for services, features, blogs, docs, and more [Alt+S]
Global
voclabs/user1769539=ameythakur@ternaengg.ac.in @ 6448-4491-7890
Amazon S3
Buckets
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
Access analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
AWS Organizations settings
Feature spotlight 3
AWS Marketplace for S3
Amazon S3 > ameythakur
ameythakur Info
Objects Properties Permissions Metrics Management Access Points
Objects (0)
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
Name Type Last modified Size Storage class
No objects
You don't have any objects in this bucket.
Upload
Feedback English (US)
© 2022, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

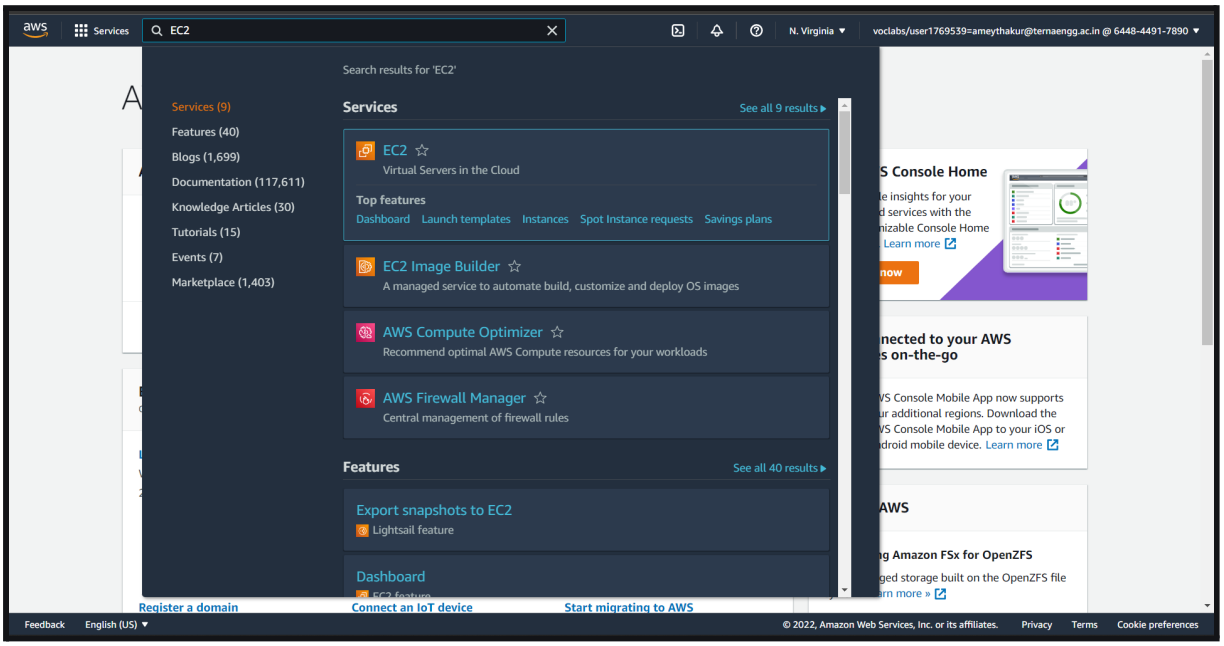

Services
Search for services, features, blogs, docs, and more [Alt+S]
Global
voclabs/user1769539=ameythakur@ternaengg.ac.in @ 6448-4491-7890
Amazon S3 > ameythakur > Upload
Upload Info
Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDK or Amazon S3 REST API. Learn more
Drag and drop files and folders you want to upload here, or choose Add files, or Add folders.
Files and folders (1 Total, 80.4 KB)
All files and folders in this table will be uploaded.
Remove Add files Add folder
Find by name
Name Folder Type Size
Website.zip - application/x-zip-compressed 80.4 KB
Destination
Destination
s3://ameythakur
Destination details
Bucket settings that impact new objects stored in the specified destination.
Feedback English (US)
© 2022, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

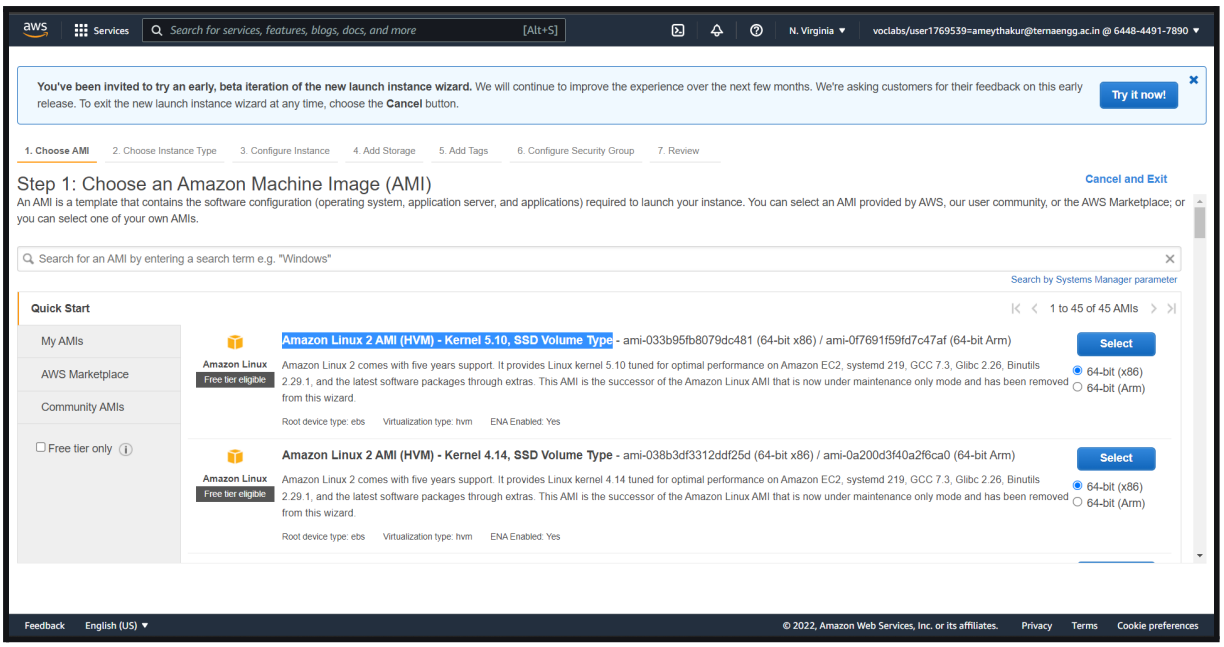

aws
Services
Search for services, features, blogs, docs, and more [Alt+S]
Global
voclabs/user1769539=ameythakur@ternaengg.ac.in @ 6448-4491-7890
Amazon S3
Buckets
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
Access analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
AWS Organizations settings
Feature spotlight 3
AWS Marketplace for S3
Amazon S3 > ameythakur
ameythakur 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
Website.zip
zip
February 14, 2022, 11:25:20 (UTC+05:30)
80.4 KB
Standard
Feedback
English (US)
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

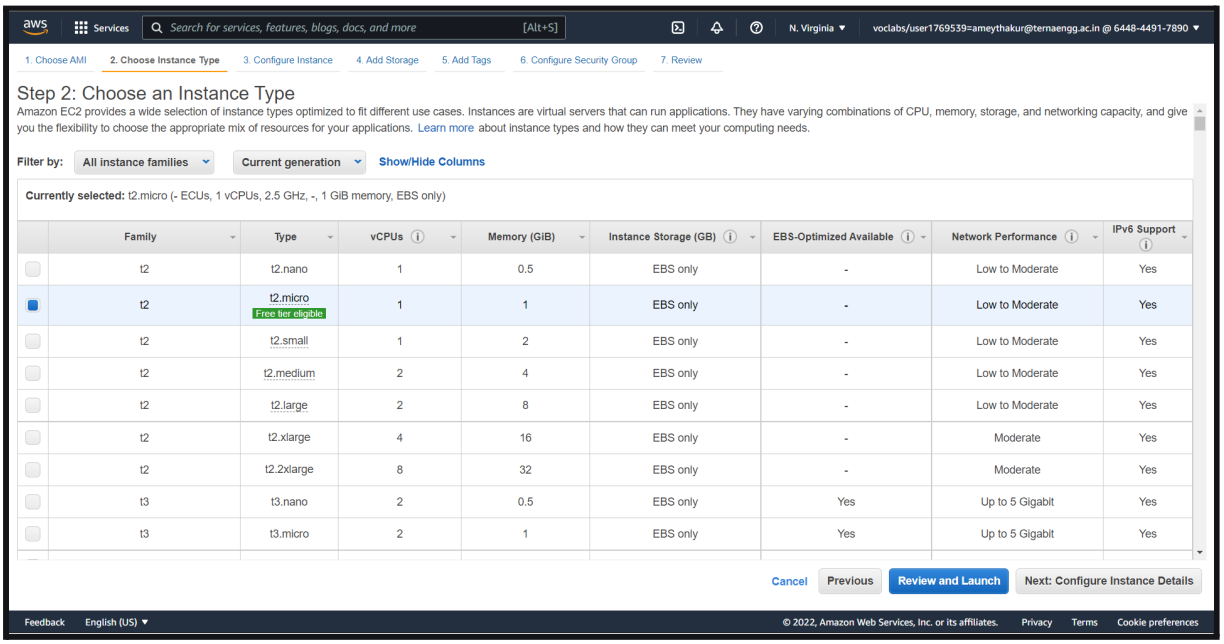

aws
Services
Search for services, features, blogs, docs, and more [Alt+S]
Global
voclabs/user1769539=ameythakur@ternaengg.ac.in @ 6448-4491-7890
Amazon S3
Buckets
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
Access analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
AWS Organizations settings
Feature spotlight 3
AWS Marketplace for S3
Amazon S3 > ameythakur > Website.zip
Website.zip Info
Copy S3 URI
Download
Open
Object actions
Properties
Permissions
Versions
Object overview
Owner
awslabsc0w3536438t1640812101
AWS Region
US East (N. Virginia) us-east-1
Last modified
February 14, 2022, 11:25:20 (UTC+05:30)
Size
80.4 KB
Type
zip
Key
Website.zip
S3 URI
s3://ameythakur/Website.zip
Amazon Resource Name (ARN)
arn:aws:s3:::ameythakur/Website.zip
Entity tag (Etag)
1dd69e6699cca8c7d6466cd2bdc713e0
Object URL
https://ameythakur.s3.amazonaws.com/Website.zip
Feedback
English (US)
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

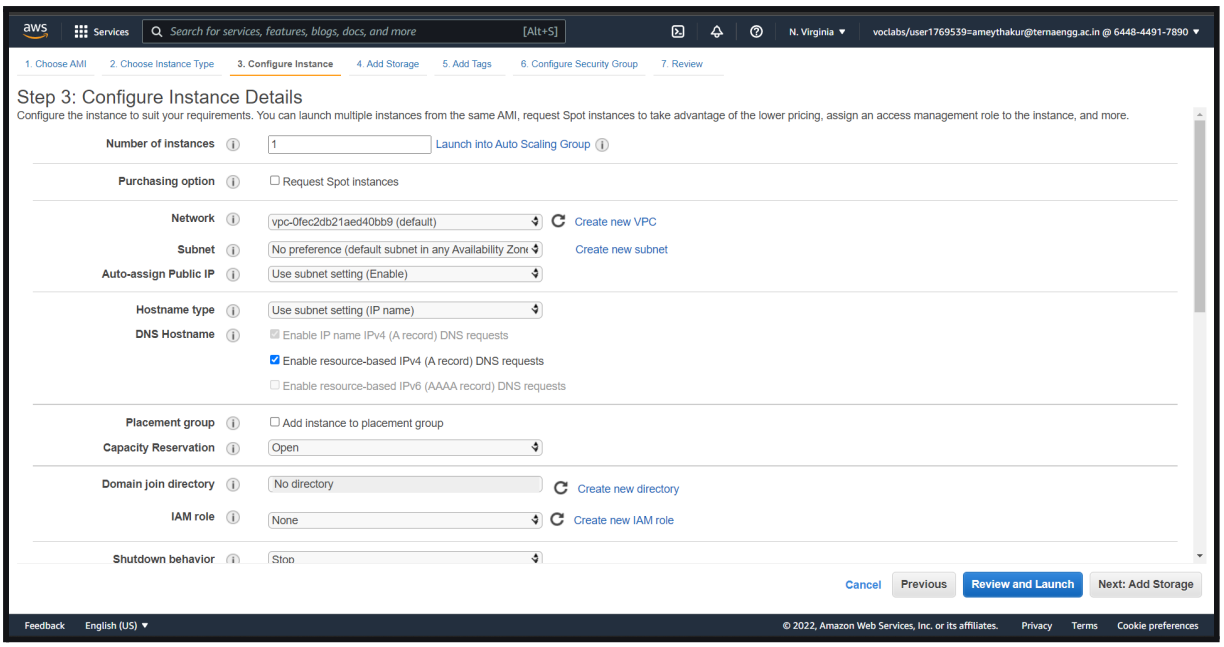


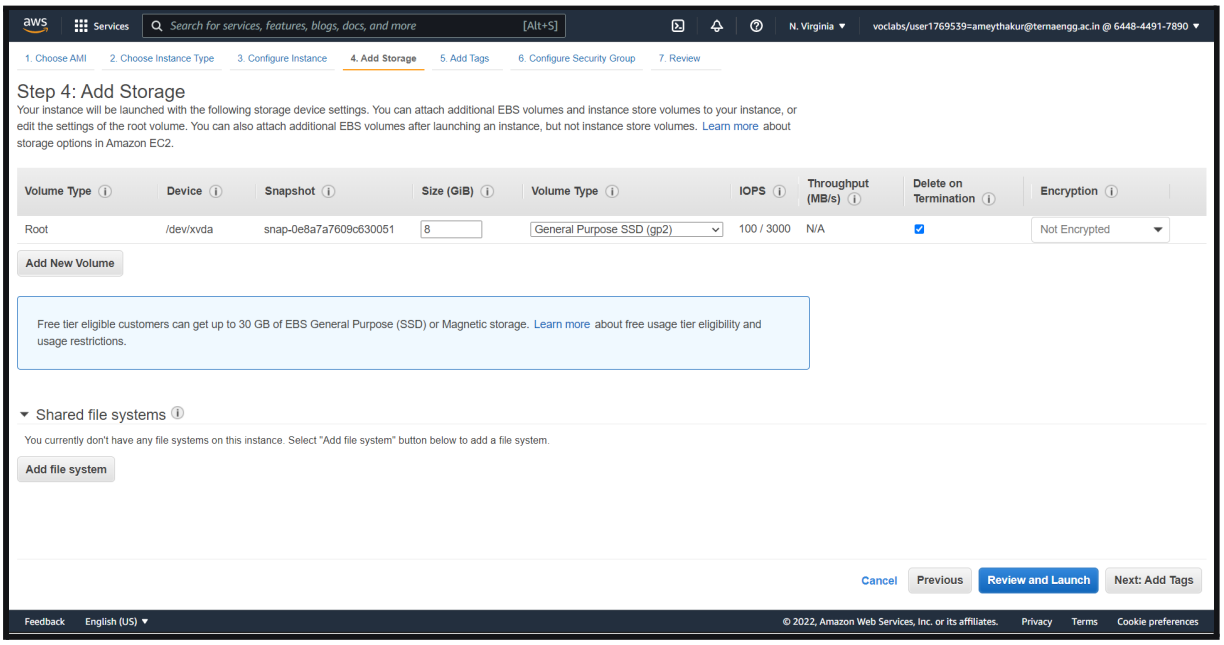
Step 3: Create EC2 Instance

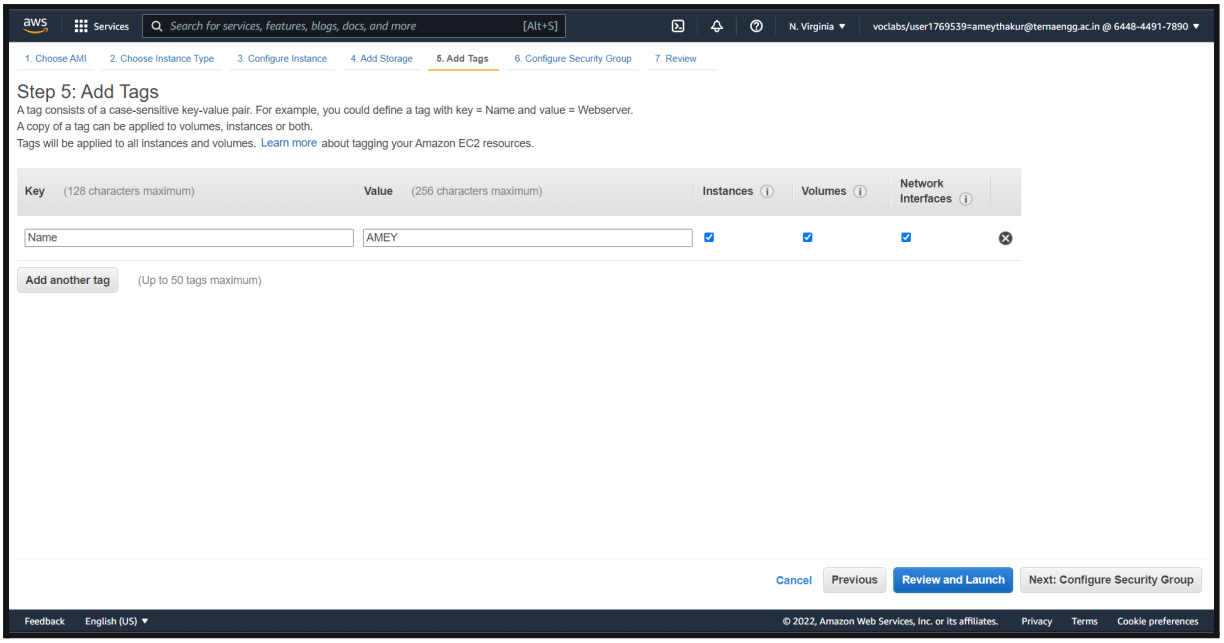


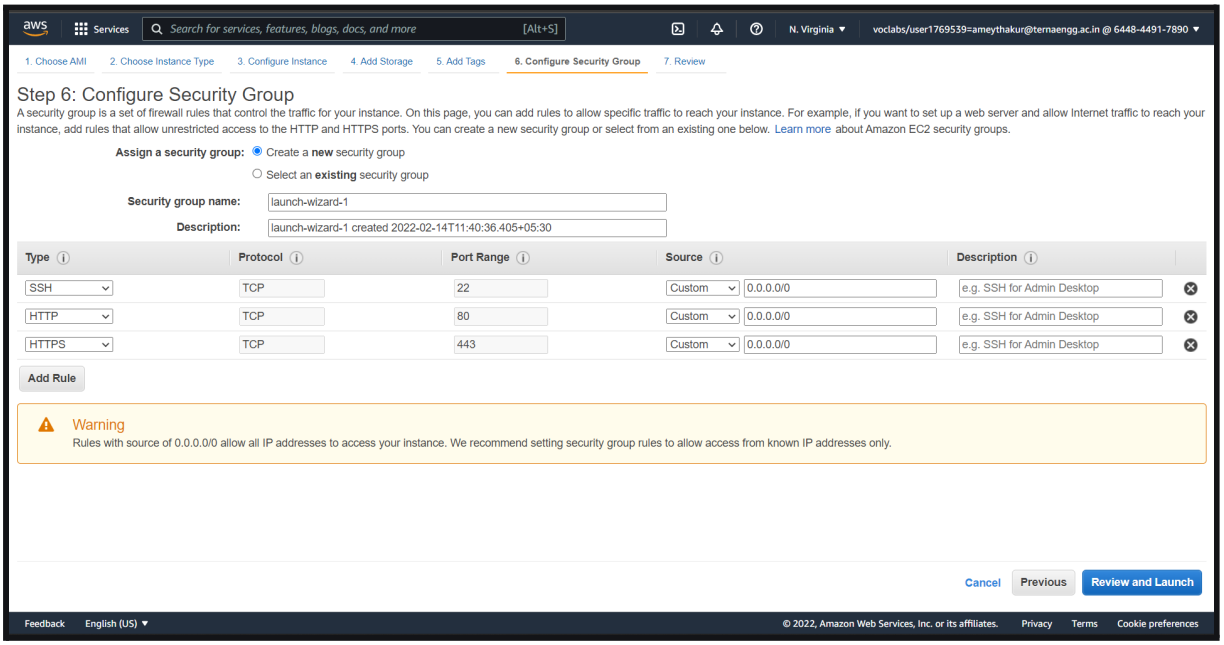

Services
Search for services, features, blogs, docs, and more [Alt+S]
N. Virginia
voclabs/user1769539=ameythakur@ternaengg.ac.in @ 6448-4491-7890
You've been invited to try an early, beta iteration of the new launch instance wizard. We will continue to improve the experience over the next few months. We're asking customers for their feedback on this early release. To exit the new launch instance wizard at any time, choose the Cancel button.
Try it now!
1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Add Tags
6. Configure Security Group
7. Review
Step 1: Choose an Amazon Machine Image (AMI)
Cancel and Exit
An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.
Search for an AMI by entering a search term e.g. "Windows"
Search by Systems Manager parameter
Quick Start
1 to 45 of 45 AMIs
My AMIs
AWS Marketplace
Community AMIs
Free tier only
Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type - ami-033b95fb8079dc481 (64-bit x86) / ami-0f7691f59fd7c47af (64-bit Arm)
Amazon Linux
Free tier eligible
Amazon Linux 2 comes with five years support. It provides Linux kernel 5.10 tuned for optimal performance on Amazon EC2, systemd 219, GCC 7.3, Glibc 2.26, Binutils 2.29.1, and the latest software packages through extras. This AMI is the successor of the Amazon Linux AMI that is now under maintenance only mode and has been removed from this wizard.
Root device type: ebs
Virtualization type: hvm
ENA Enabled: Yes
Select
64-bit (x86)
64-bit (Arm)
Amazon Linux 2 AMI (HVM) - Kernel 4.14, SSD Volume Type - ami-038b3df3312ddf25d (64-bit x86) / ami-0a200d3f40a2f6ca0 (64-bit Arm)
Amazon Linux
Free tier eligible
Amazon Linux 2 comes with five years support. It provides Linux kernel 4.14 tuned for optimal performance on Amazon EC2, systemd 219, GCC 7.3, Glibc 2.26, Binutils 2.29.1, and the latest software packages through extras. This AMI is the successor of the Amazon Linux AMI that is now under maintenance only mode and has been removed from this wizard.
Root device type: ebs
Virtualization type: hvm
ENA Enabled: Yes
Select
64-bit (x86)
64-bit (Arm)
Feedback
English (US)
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

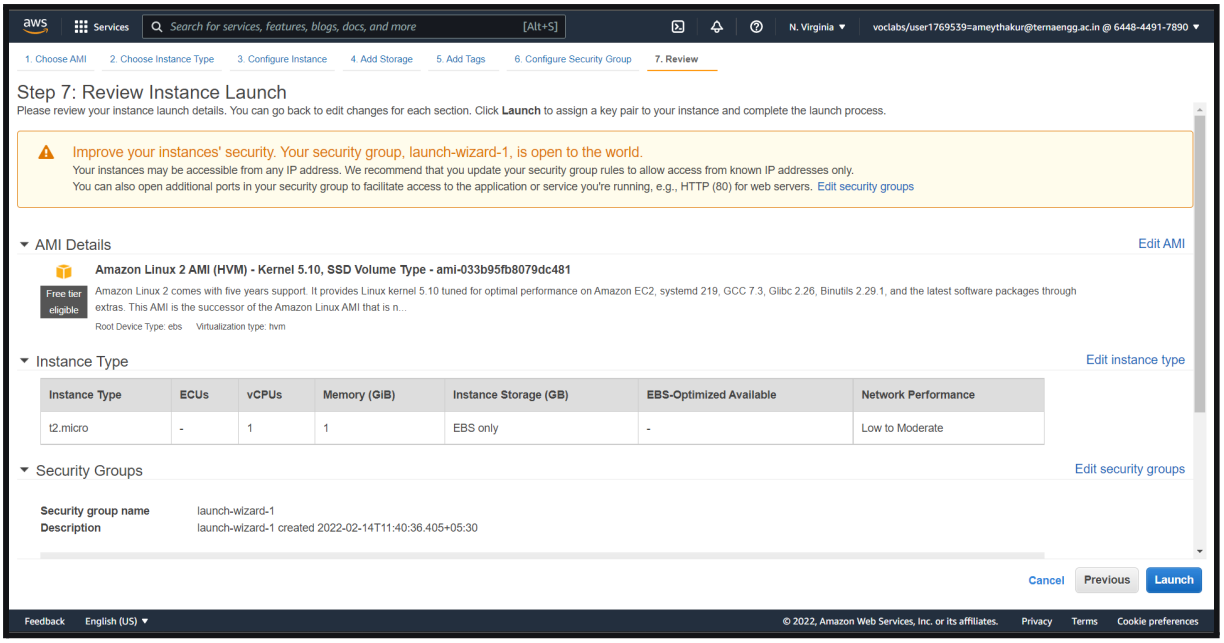

Services
Search for services, features, blogs, docs, and more [Alt+S]
N. Virginia
voclabs/user1769539=ameythakur@ternaengg.ac.in @ 6448-4491-7890
1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Add Tags
6. Configure Security Group
7. Review
Step 2: Choose an Instance Type
Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. Learn more about instance types and how they can meet your computing needs.
Filter by:
All instance families
Current generation
Show/Hide Columns
Currently selected: t2.micro (- ECUs, 1 vCPUs, 2.5 GHz, -, 1 GiB memory, EBS only)
Family
Type
vCPUs
Memory (GiB)
Instance Storage (GB)
EBS-Optimized Available
Network Performance
IPv6 Support
t2 t2.nano 1 0.5 EBS only - Low to Moderate Yes
t2 t2.micro Free tier eligible 1 1 EBS only - Low to Moderate Yes
t2 t2.small 1 2 EBS only - Low to Moderate Yes
t2 t2.medium 2 4 EBS only - Low to Moderate Yes
t2 t2.large 2 8 EBS only - Low to Moderate Yes
t2 t2.xlarge 4 16 EBS only - Moderate Yes
t2 t2.2xlarge 8 32 EBS only - Moderate Yes
t3 t3.nano 2 0.5 EBS only Yes Up to 5 Gigabit Yes
t3 t3.micro 2 1 EBS only Yes Up to 5 Gigabit Yes
Cancel
Previous
Review and Launch
Next: Configure Instance Details
Feedback
English (US)
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

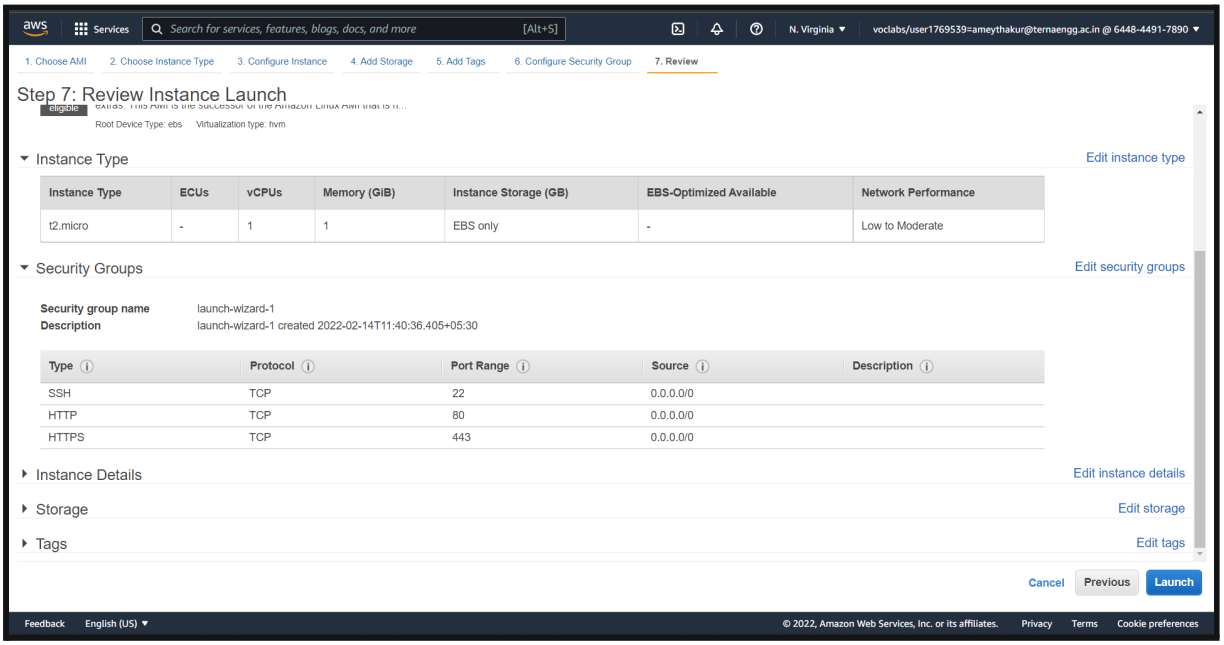

Services
Search for services, features, blogs, docs, and more [Alt+S]
N. Virginia
voclabs/user1769539=ameythakur@ternaengg.ac.in @ 6448-4491-7890
1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Add Tags
6. Configure Security Group
7. Review
Step 3: Configure Instance Details
Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.
Number of instances
1
Launch into Auto Scaling Group
Purchasing option
Request Spot instances
Network
vpc-0fec2db21aed40bb9 (default)
Create new VPC
Subnet
No preference (default subnet in any Availability Zone
Create new subnet
Auto-assign Public IP
Use subnet setting (Enable)
Hostname type
Use subnet setting (IP name)
DNS Hostname
Enable IP name IPv4 (A record) DNS requests
Enable resource-based IPv4 (A record) DNS requests
Enable resource-based IPv6 (AAAA record) DNS requests
Placement group
Add instance to placement group
Capacity Reservation
Open
Domain join directory
No directory
Create new directory
IAM role
None
Create new IAM role
Shutdown behavior
Stop
Cancel
Previous
Review and Launch
Next: Add Storage
Feedback
English (US)
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

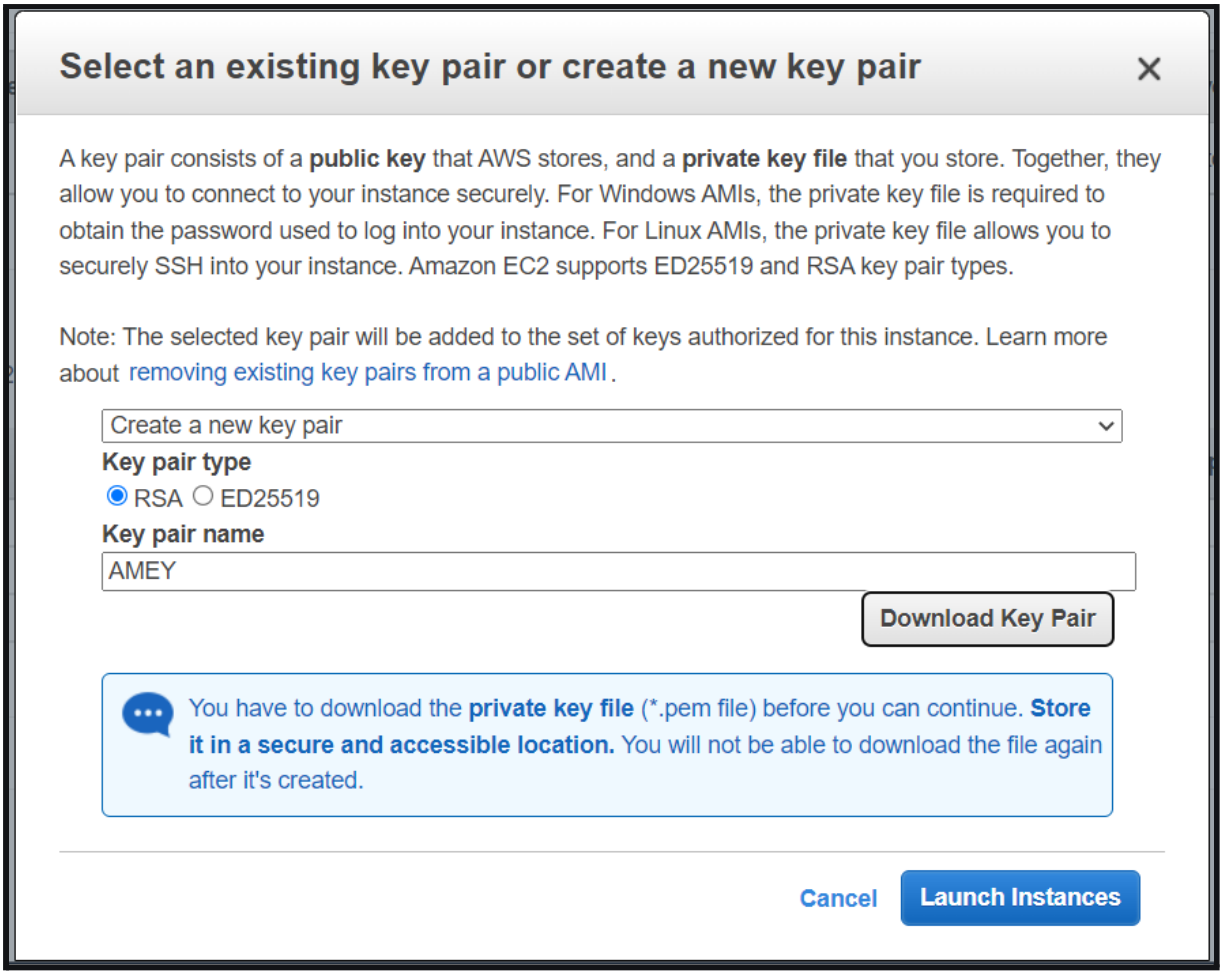

Services
Search for services, features, blogs, docs, and more [Alt+S]
N. Virginia
voclabs/user1769539=ameythakur@ternaengg.ac.in @ 6448-4491-7890
1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Add Tags
6. Configure Security Group
7. Review
Step 4: Add Storage
Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. Learn more about storage options in Amazon EC2.
Volume Type
Device
Snapshot
Size (GiB)
Volume Type
IOPS
Throughput (MB/s)
Delete on Termination
Encryption
Root
/dev/xvda
snap-0e8a7a7609c630051
8
General Purpose SSD (gp2)
100 / 3000
N/A
Not Encrypted
Add New Volume
Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. Learn more about free usage tier eligibility and usage restrictions.
Shared file systems
You currently don't have any file systems on this instance. Select "Add file system" button below to add a file system.
Add file system
Cancel
Previous
Review and Launch
Next: Add Tags
Feedback
English (US)
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

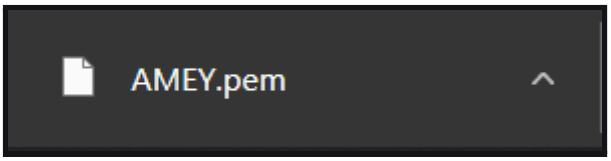

Services
Search for services, features, blogs, docs, and more [Alt+S]
N. Virginia
voclabs/user1769539=ameythakur@ternaengg.ac.in @ 6448-4491-7890
1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Add Tags
6. Configure Security Group
7. Review
Step 5: Add Tags
A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver.
A copy of a tag can be applied to volumes, instances or both.
Tags will be applied to all instances and volumes. Learn more about tagging your Amazon EC2 resources.
Key (128 characters maximum)
Value (256 characters maximum)
Instances
Volumes
Network Interfaces
Name
AMEY
Add another tag
(Up to 50 tags maximum)
Cancel
Previous
Review and Launch
Next: Configure Security Group
Feedback
English (US)
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

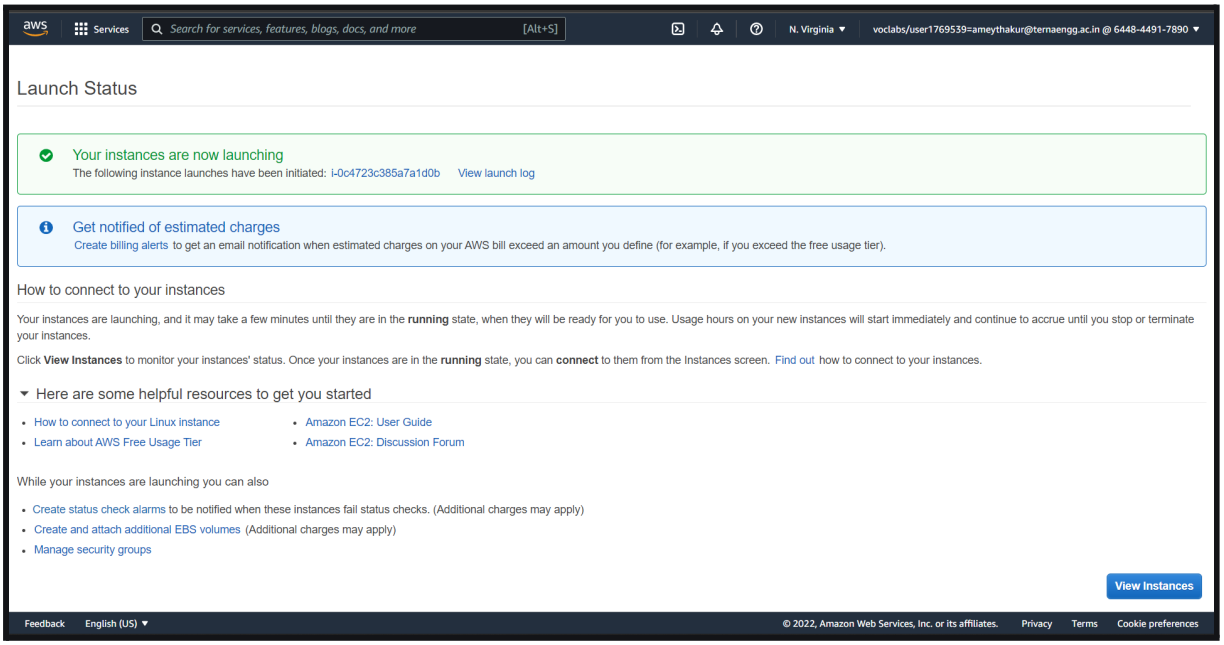

Services
Search for services, features, blogs, docs, and more [Alt+S]
N. Virginia
voclabs/user1769539=ameythakur@ternaengg.ac.in @ 6448-4491-7890
1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Add Tags
6. Configure Security Group
7. Review
Step 6: Configure Security Group
A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. Learn more about Amazon EC2 security groups.
Assign a security group: Create a new security group
Select an existing security group
Security group name: launch-wizard-1
Description: launch-wizard-1 created 2022-02-14T11:40:36.405+05:30
Type
Protocol
Port Range
Source
Description
SSH
TCP
22
Custom
0.0.0.0/0
e.g. SSH for Admin Desktop
HTTP
TCP
80
Custom
0.0.0.0/0
e.g. SSH for Admin Desktop
HTTPS
TCP
443
Custom
0.0.0.0/0
e.g. SSH for Admin Desktop
Add Rule
Warning
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.
Cancel
Previous
Review and Launch
Feedback
English (US)
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

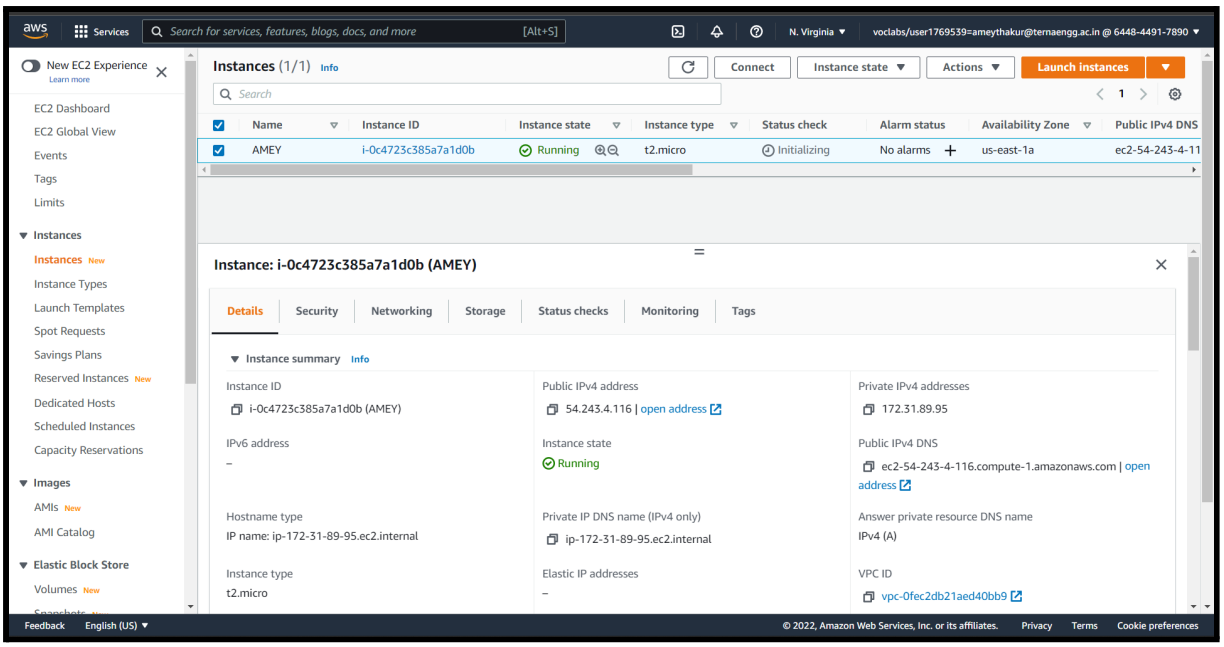

aws
Services
Search for services, features, blogs, docs, and more [Alt+S]
N. Virginia
voclabs/user1769539=ameythakur@ternaengg.ac.in @ 6448-4491-7890
1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Add Tags
6. Configure Security Group
7. Review
Step 7: Review Instance Launch
Please review your instance launch details. You can go back to edit changes for each section. Click Launch to assign a key pair to your instance and complete the launch process.
Improve your instances' security. Your security group, launch-wizard-1, is open to the world.
Your instances may be accessible from any IP address. We recommend that you update your security group rules to allow access from known IP addresses only.
You can also open additional ports in your security group to facilitate access to the application or service you're running, e.g., HTTP (80) for web servers. Edit security groups
AMI Details
Edit AMI
Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type - ami-033b95fb8079dc481
Free tier eligible
Amazon Linux 2 comes with five years support. It provides Linux kernel 5.10 tuned for optimal performance on Amazon EC2, systemd 219, GCC 7.3, Glibc 2.26, Binutils 2.29.1, and the latest software packages through extras. This AMI is the successor of the Amazon Linux AMI that is n...
Root Device Type: ebs Virtualization type: hvm
Instance Type
Edit instance type
Instance Type | ECUs | vCPUs | Memory (GiB) | Instance Storage (GB) | EBS-Optimized Available | Network Performance
t2.micro | - | 1 | 1 | EBS only | - | Low to Moderate
Security Groups
Edit security groups
Security group name launch-wizard-1
Description launch-wizard-1 created 2022-02-14T11:40:36.405+05:30
Cancel
Previous
Launch
Feedback
English (US)
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


aws
Services
Search for services, features, blogs, docs, and more [Alt+S]
N. Virginia
voclabs/user1769539=ameythakur@ternaengg.ac.in @ 6448-4491-7890
1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Add Tags
6. Configure Security Group
7. Review
Step 7: Review Instance Launch
Root Device Type: ebs Virtualization type: hvm
Instance Type
Edit instance type
Instance Type | ECUs | vCPUs | Memory (GiB) | Instance Storage (GB) | EBS-Optimized Available | Network Performance
t2.micro | - | 1 | 1 | EBS only | - | Low to Moderate
Security Groups
Edit security groups
Security group name launch-wizard-1
Description launch-wizard-1 created 2022-02-14T11:40:36.405+05:30
Type | Protocol | Port Range | Source | Description
SSH | TCP | 22 | 0.0.0.0/0
HTTP | TCP | 80 | 0.0.0.0/0
HTTPS | TCP | 443 | 0.0.0.0/0
Instance Details
Edit instance details
Storage
Edit storage
Tags
Edit tags
Cancel
Previous
Launch
Feedback
English (US)
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

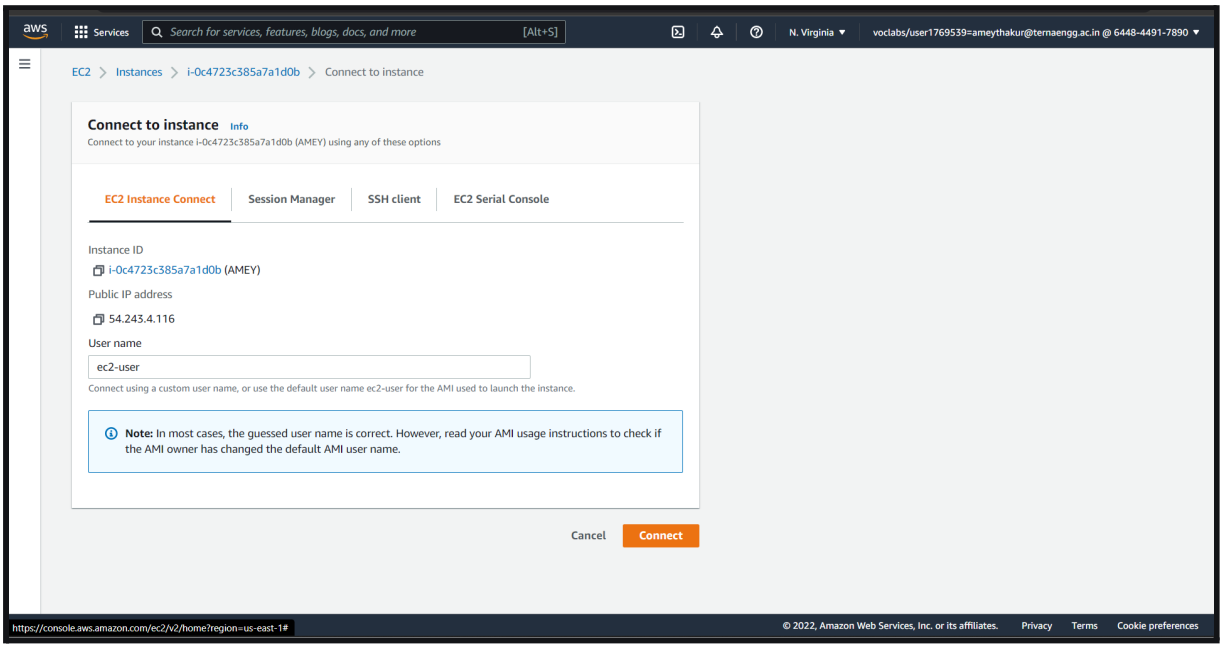

Select an existing key pair or create a new key pair
A key pair consists of a public key that AWS stores, and a private key file that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance. Amazon EC2 supports ED25519 and RSA key pair types.
Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about removing existing key pairs from a public AMI.
Create a new key pair
Key pair type
RSA
ED25519
Key pair name
AMEY
Download Key Pair
You have to download the private key file (*.pem file) before you can continue. Store it in a secure and accessible location. You will not be able to download the file again after it's created.
Cancel
Launch Instances


AMEY.pem

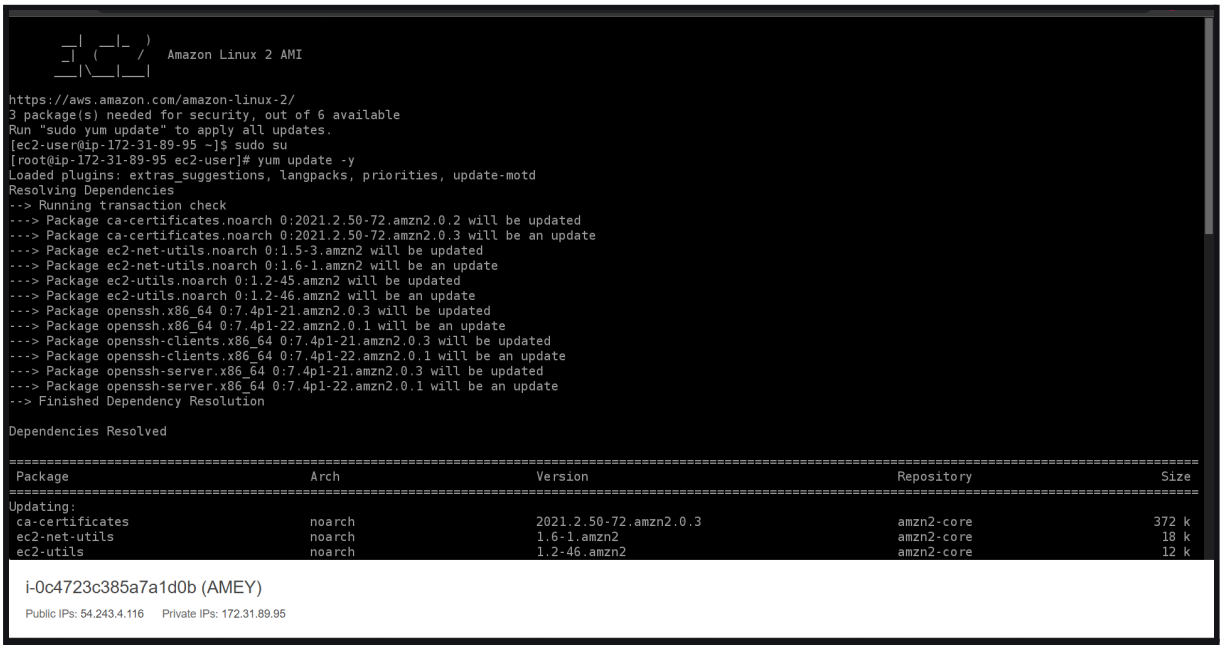

Services
Search for services, features, blogs, docs, and more
[Alt+S]
N. Virginia
voclabs/user1769539=ameythakur@ternaengg.ac.in @ 6448-4491-7890
Launch Status
Your instances are now launching
The following instance launches have been initiated: i-0c4723c385a7a1d0b View launch log
Get notified of estimated charges
Create billing alerts to get an email notification when estimated charges on your AWS bill exceed an amount you define (for example, if you exceed the free usage tier).
How to connect to your instances
Your instances are launching, and it may take a few minutes until they are in the running state, when they will be ready for you to use. Usage hours on your new instances will start immediately and continue to accrue until you stop or terminate your instances.
Click View Instances to monitor your instances' status. Once your instances are in the running state, you can connect to them from the Instances screen. Find out how to connect to your instances.
Here are some helpful resources to get you started
How to connect to your Linux instance
Learn about AWS Free Usage Tier
Amazon EC2: User Guide
Amazon EC2: Discussion Forum
While your instances are launching you can also
Create status check alarms to be notified when these instances fail status checks. (Additional charges may apply)
Create and attach additional EBS volumes (Additional charges may apply)
Manage security groups
View Instances
Feedback
English (US)
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences



Step 4: EC2 Instance Connect



Step 5: Terminal



```
Running transaction
  Updating   : openssh-7.4p1-22.amzn2.0.1.x86_64                                                                 1/12
  Updating   : openssh-server-7.4p1-22.amzn2.0.1.x86_64                                                          2/12
  Updating   : openssh-clients-7.4p1-22.amzn2.0.1.x86_64                                                         3/12
  Updating   : ca-certificates-2021.2.50-72.amzn2.0.3.noarch                                                     4/12
  Updating   : ec2-utils-1.2-46.amzn2.noarch                                                                     5/12
  Updating   : ec2-net-utils-1.6-1.amzn2.noarch                                                                  6/12
  Cleanup    : ca-certificates-2021.2.50-72.amzn2.0.2.noarch                                                     7/12
  Cleanup    : ec2-utils-1.2-45.amzn2.noarch                                                                     8/12
  Cleanup    : ec2-net-utils-1.5-3.amzn2.noarch                                                                  9/12
  Cleanup    : openssh-clients-7.4p1-21.amzn2.0.3.x86_64                                                        10/12
  Cleanup    : openssh-server-7.4p1-21.amzn2.0.3.x86_64                                                         11/12
  Cleanup    : openssh-7.4p1-21.amzn2.0.3.x86_64                                                                12/12
  Verifying  : ec2-net-utils-1.6-1.amzn2.noarch                                                                  1/12
  Verifying  : ec2-utils-1.2-46.amzn2.noarch                                                                     2/12
  Verifying  : ca-certificates-2021.2.50-72.amzn2.0.3.noarch                                                     3/12
  Verifying  : openssh-7.4p1-22.amzn2.0.1.x86_64                                                                 4/12
  Verifying  : openssh-server-7.4p1-22.amzn2.0.1.x86_64                                                          5/12
  Verifying  : openssh-clients-7.4p1-22.amzn2.0.1.x86_64                                                         6/12
  Verifying  : ec2-utils-1.2-45.amzn2.noarch                                                                     7/12
  Verifying  : openssh-7.4p1-21.amzn2.0.3.x86_64                                                                 8/12
  Verifying  : ec2-net-utils-1.5-3.amzn2.noarch                                                                  9/12
  Verifying  : ca-certificates-2021.2.50-72.amzn2.0.2.noarch                                                    10/12
  Verifying  : openssh-server-7.4p1-21.amzn2.0.3.x86_64                                                         11/12
  Verifying  : openssh-clients-7.4p1-21.amzn2.0.3.x86_64                                                        12/12

Updated:
  ca-certificates.noarch 0:2021.2.50-72.amzn2.0.3       ec2-net-utils.noarch 0:1.6-1.amzn2              ec2-utils.noarch 0:1.2-46.amzn2
  openssh.x86_64 0:7.4p1-22.amzn2.0.1                   openssh-clients.x86_64 0:7.4p1-22.amzn2.0.1     openssh-server.x86_64 0:7.4p1-22.amzn2.0.1

Complete!
[root@ip-172-31-89-95 ec2-user]# yum install httpd -y
```

i-0c4723c385a7a1d0b (AMEY)

Public IPs: 54.243.4.116 Private IPs: 172.31.89.95

```
  Installing : apr-1.7.0-9.amzn2.x86_64                                                                          1/9
  Installing : apr-util-bdb-1.6.1-5.amzn2.0.2.x86_64                                                             2/9
  Installing : apr-util-1.6.1-5.amzn2.0.2.x86_64                                                                 3/9
  Installing : httpd-tools-2.4.52-1.amzn2.x86_64                                                                 4/9
  Installing : generic-logos-httpd-18.0.0-4.amzn2.noarch                                                         5/9
  Installing : mailcap-2.1.41-2.amzn2.noarch                                                                     6/9
  Installing : httpd-filesystem-2.4.52-1.amzn2.noarch                                                            7/9
  Installing : mod_http2-1.15.19-1.amzn2.0.1.x86_64                                                              8/9
  Installing : httpd-2.4.52-1.amzn2.x86_64                                                                       9/9
  Verifying  : apr-util-1.6.1-5.amzn2.0.2.x86_64                                                                 1/9
  Verifying  : httpd-tools-2.4.52-1.amzn2.x86_64                                                                 2/9
  Verifying  : apr-util-bdb-1.6.1-5.amzn2.0.2.x86_64                                                             3/9
  Verifying  : httpd-filesystem-2.4.52-1.amzn2.noarch                                                            4/9
  Verifying  : httpd-2.4.52-1.amzn2.x86_64                                                                       5/9
  Verifying  : mailcap-2.1.41-2.amzn2.noarch                                                                     6/9
  Verifying  : generic-logos-httpd-18.0.0-4.amzn2.noarch                                                         7/9
  Verifying  : mod_http2-1.15.19-1.amzn2.0.1.x86_64                                                              8/9
  Verifying  : apr-1.7.0-9.amzn2.x86_64                                                                          9/9

Installed:
  httpd.x86_64 0:2.4.52-1.amzn2

Dependency Installed:
  apr.x86_64 0:1.7.0-9.amzn2                    apr-util.x86_64 0:1.6.1-5.amzn2.0.2           apr-util-bdb.x86_64 0:1.6.1-5.amzn2.0.2
  generic-logos-httpd.noarch 0:18.0.0-4.amzn2   httpd-filesystem.noarch 0:2.4.52-1.amzn2      httpd-tools.x86_64 0:2.4.52-1.amzn2
  mailcap.noarch 0:2.1.41-2.amzn2               mod_http2.x86_64 0:1.15.19-1.amzn2.0.1

Complete!
[root@ip-172-31-89-95 ec2-user]# pwd
/home/ec2-user
[root@ip-172-31-89-95 ec2-user]# cd var/www/html
```

i-0c4723c385a7a1d0b (AMEY)

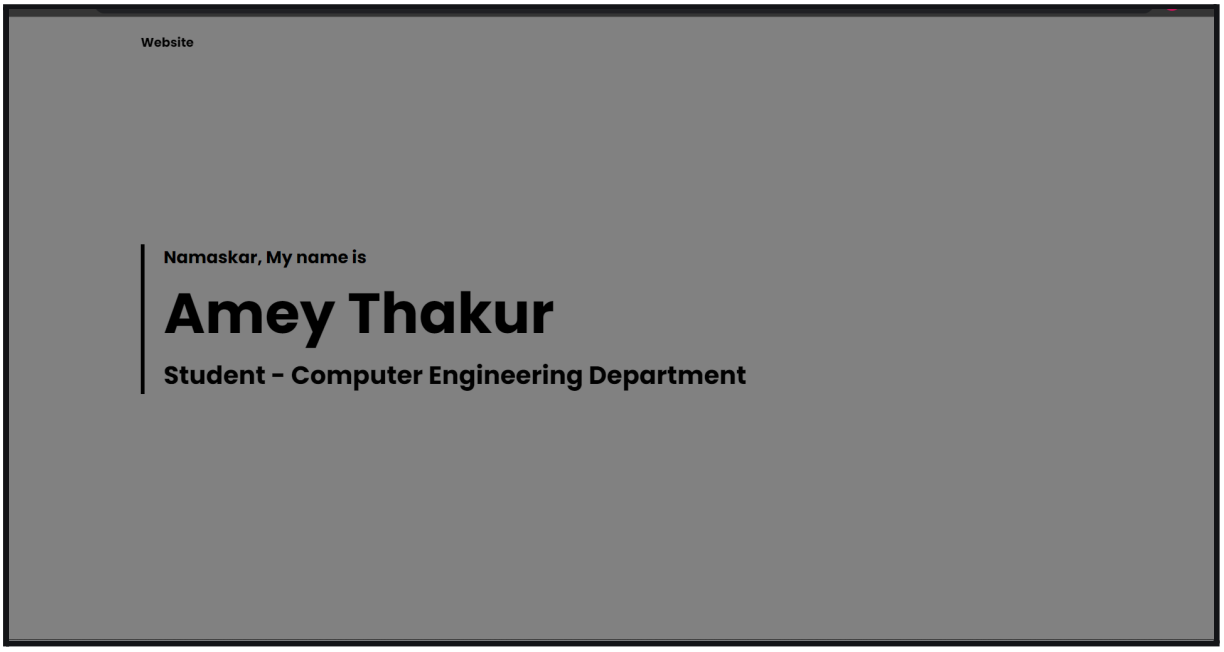
Public IPs: 54.243.4.116 Private IPs: 172.31.89.95

```
[root@ip-172-31-89-95 ec2-user]# pwd
/home/ec2-user
[root@ip-172-31-89-95 ec2-user]# cd /var/www/html
[root@ip-172-31-89-95 html]#
[root@ip-172-31-89-95 html]# wget https://ameythakur.s3.amazonaws.com/Website.zip
--2022-02-14 06:25:15--  https://ameythakur.s3.amazonaws.com/Website.zip
Resolving ameythakur.s3.amazonaws.com (ameythakur.s3.amazonaws.com)... 52.217.227.209
Connecting to ameythakur.s3.amazonaws.com (ameythakur.s3.amazonaws.com)|52.217.227.209|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 82374 (80K) [application/zip]
Saving to: 'Website.zip'

100%[=============================================================================================================>] 82,374      --.-K/s   in 0.001s

2022-02-14 06:25:15 (66.3 MB/s) - 'Website.zip' saved [82374/82374]

[root@ip-172-31-89-95 html]# ls
Website.zip
[root@ip-172-31-89-95 html]# unzip Website.zip
Archive:  Website.zip
   creating: Website/assets/
   creating: Website/assets/css/
  inflating: Website/assets/css/styles.css
   creating: Website/assets/img/
  inflating: Website/assets/img/img.jpg
   creating: Website/assets/js/
  inflating: Website/assets/js/main.js
  inflating: Website/index.html
[root@ip-172-31-89-95 html]# ls
Website  Website.zip
[root@ip-172-31-89-95 html]# mv Website/* .
[root@ip-172-31-89-95 html]# service httpd start
Redirecting to /bin/systemctl start httpd.service
[root@ip-172-31-89-95 html]#
```

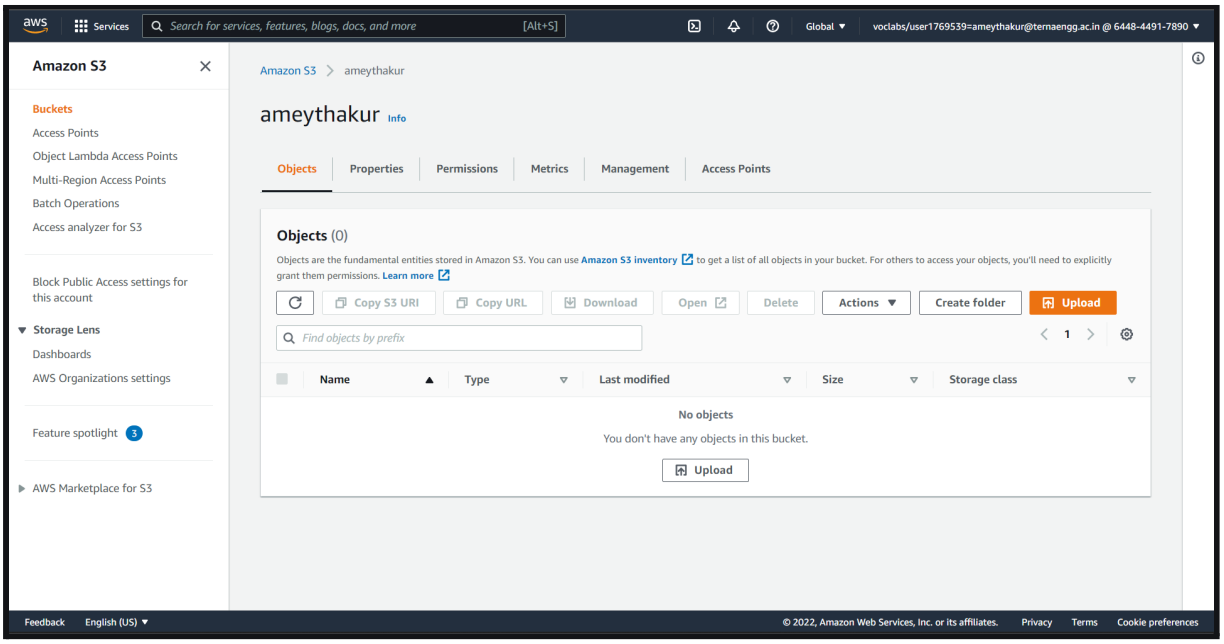
i-0c4723c385a7a1d0b (AMEY)

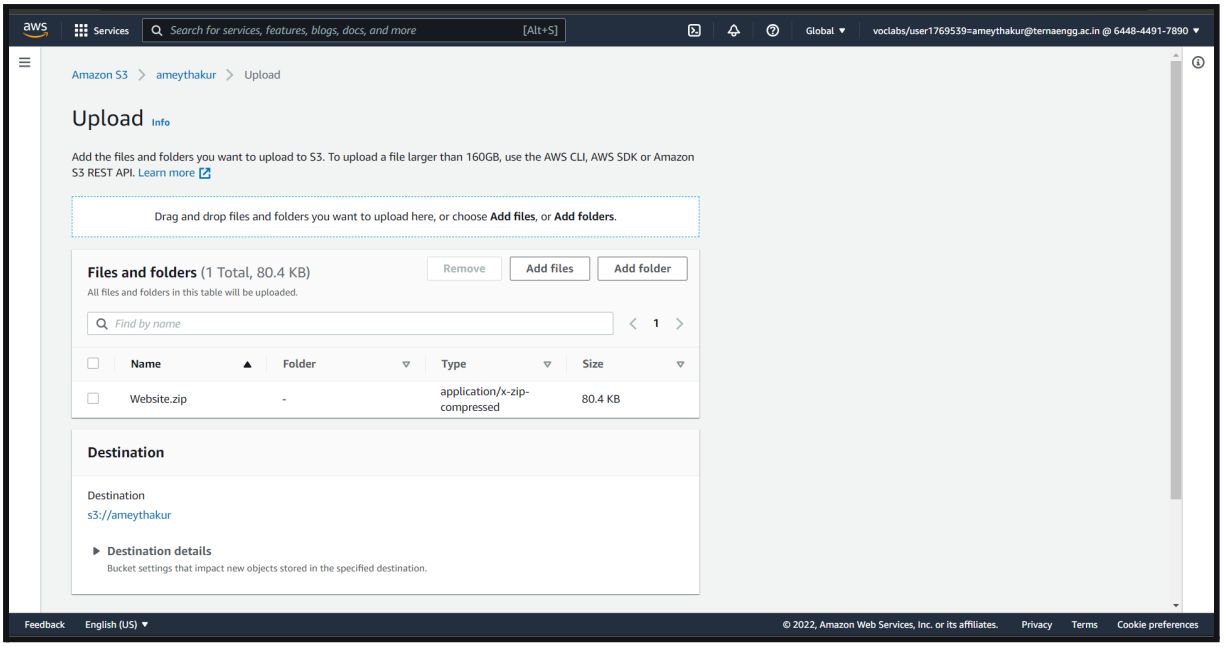
Public IPs: 54.243.4.116 Private IPs: 172.31.89.95

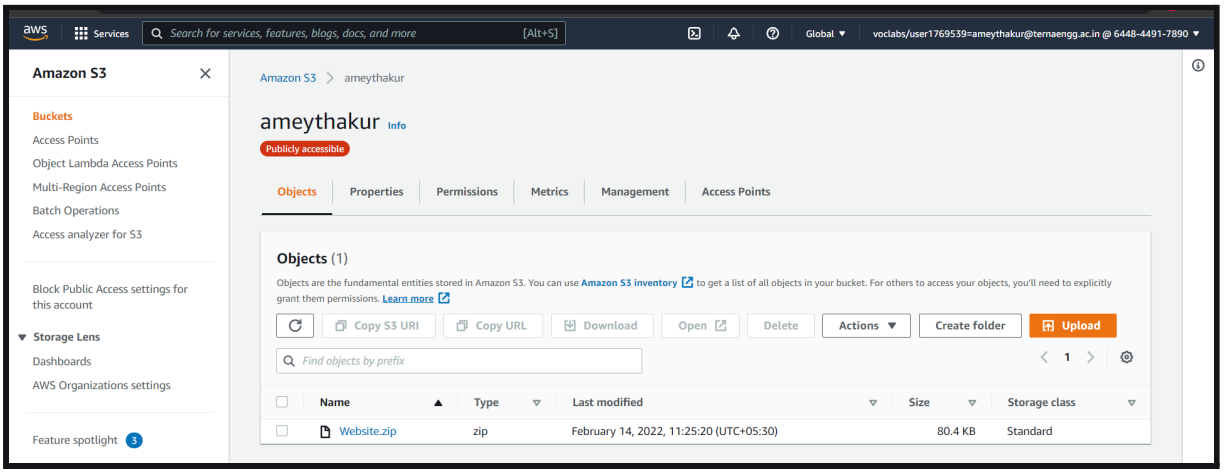
Step 12: RESULT

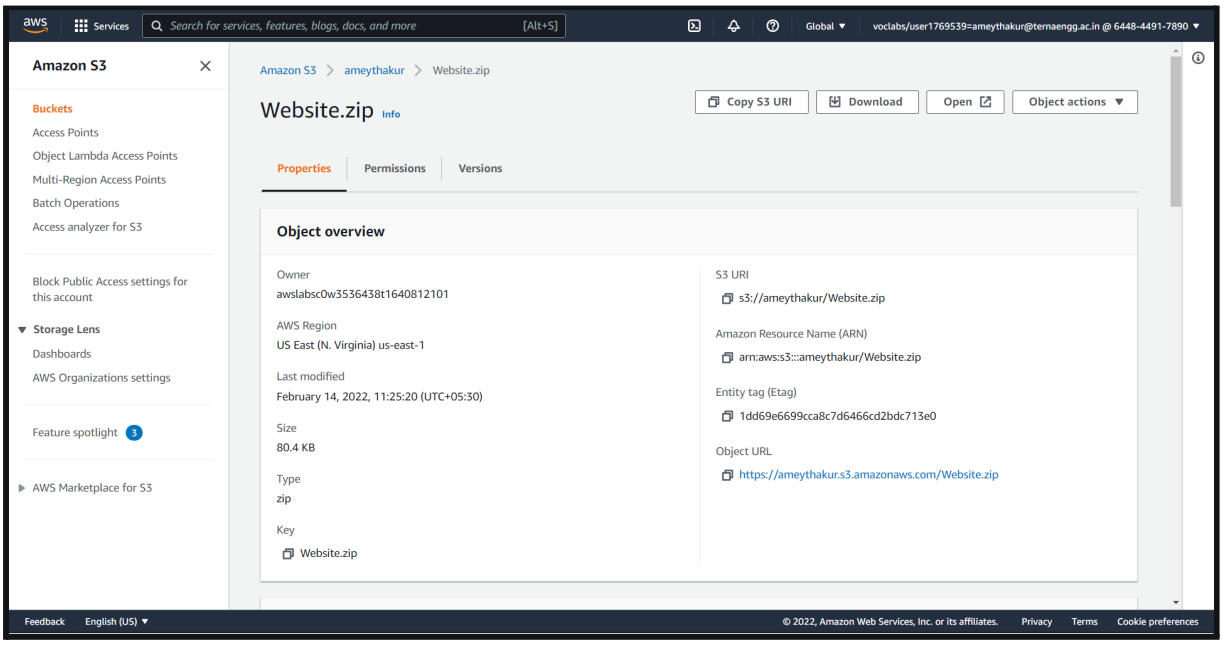


Q2: Add Objects to Bucket created (Add stepwise screenshots of the same).
ANS:




Amazon S3 > ameythakur > 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 folders.
Files and folders (1 Total, 80.4 KB)
All files and folders in this table will be uploaded.
Remove
Add files
Add folder
Find by name
Name
Folder
Type
Size
Website.zip
-
application/x-zip-compressed
80.4 KB
Destination
Destination
s3://ameythakur
Destination details
Bucket settings that impact new objects stored in the specified destination.


Amazon S3
Buckets
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
Access analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
AWS Organizations settings
Feature spotlight
Amazon S3 > ameythakur
ameythakur 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
Name
Type
Last modified
Size
Storage class
Website.zip
zip
February 14, 2022, 11:25:20 (UTC+05:30)
80.4 KB
Standard


Amazon S3
Buckets
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
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 > ameythakur > Website.zip
Website.zip Info
Copy S3 URI
Download
Open
Object actions
Properties
Permissions
Versions
Object overview
Owner
awslabsc0w3536438t1640812101
AWS Region
US East (N. Virginia) us-east-1
Last modified
February 14, 2022, 11:25:20 (UTC+05:30)
Size
80.4 KB
Type
zip
Key
Website.zip
S3 URI
s3://ameythakur/Website.zip
Amazon Resource Name (ARN)
arn:aws:s3:::ameythakur/Website.zip
Entity tag (Etag)
1dd69e6699cca8c7d6466cd2bdc713e0
Object URL
https://ameythakur.s3.amazonaws.com/Website.zip

Q3: Compare Google Drive with AWS S3.
ANS:

GOOGLE DRIVE	AMAZON S3
It is owned by Google LLC.	It is owned by Amazon.
It was launched in 2012.	It was launched in 2006.
It offers 15 GB free storage space.	It does not offer free storage space.
It was developed by Google.	It was developed by Amazon Web Services (AWS).
The number of users using Google Drive is more.	The number of users using Amazon S3 is less.
It provides full security of data.	It also provides full security of data but comparatively less.
It has the maximum storage size of 30 TB.	It has the unlimited maximum storage size for paid users.
It does not support remote uploading.	Remote uploading is not supported here also.
Maximum file size in Google Drive is 5 TB.	Here the maximum file size is 5 GB.
It supports file versioning.	It also supports file versioning.
It does not require credit-card for free services.	It requires credit-card details for a free trial.

B.2 Conclusion:
Using an Amazon AWS Free Tier Account, we learned Storage as a Service and how to use the Amazon S3 Service. On AWS, we were able to successfully host a website by using S3 storage.