

Terna Engineering College
Computer Engineering Department
Program: Sem VIII

Course: Cloud Computing Lab (CSL803)

Faculty: Reshma Koli

Experiment No. 5

A.1 Aim: Demonstrate and implement PaaS that is Deploy static Website 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: 21-02-2022	Date of Submission: 21-02-2022
Grade:	

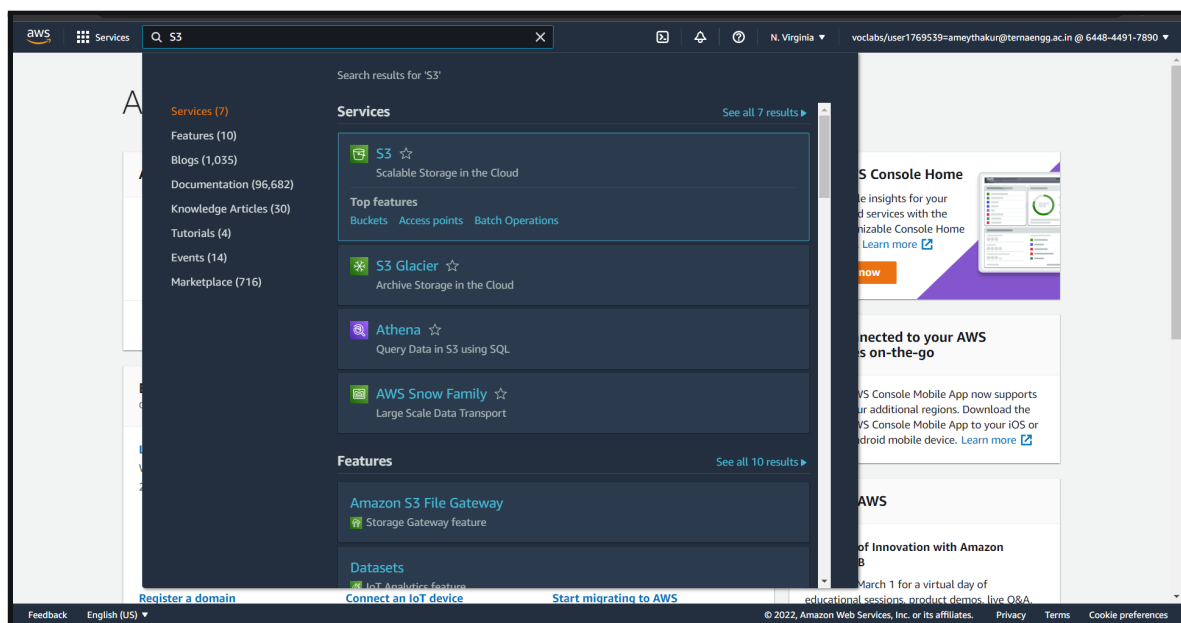
B.1 Question of Curiosity:

Q1: Deploy static website using AWS S3 (Add stepwise screenshots of the same)

ANS:

Practical Video (AWS S3 Service): <https://youtu.be/CnM07Vg7pW8>

Step 1:



Step 2:

The screenshot shows the Amazon S3 console interface. On the left, there is a navigation pane with options like Buckets, Access Points, Object Lambda Access Points, Multi-Region Access Points, Batch Operations, Access analyzer for S3, Storage Lens, Dashboards, AWS Organizations settings, Feature spotlight, and AWS Marketplace for S3. The main content area displays the 'Account snapshot' section, which includes a 'View Storage Lens dashboard' button and a table with the following data:

Total storage	Object count	Avg. object size
3.7 KB	1	3.7 KB

Below the account snapshot, there is a 'Buckets (0)' section with a 'Create bucket' button. A message states: 'No buckets. You don't have any buckets.' with another 'Create bucket' button.

Step 3:

The screenshot shows the 'Create bucket' wizard in the Amazon S3 console. The 'General configuration' section includes a 'Bucket name' field with the value 'ameythakur', an 'AWS Region' dropdown set to 'US East (N. Virginia) us-east-1', and a 'Copy settings from existing bucket - optional' section with a 'Choose bucket' button. The 'Object Ownership' section has two radio buttons: 'ACLs disabled (recommended)' and 'ACLs enabled'. The 'ACLs enabled' option is selected, with a note: 'Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.'

Step 4:

The screenshot shows the AWS console interface for configuring a bucket's Object Ownership. The top navigation bar includes the AWS logo, a search bar, and user information. The main content area is titled "Object Ownership" and includes an "Info" link. It explains that object ownership determines who can specify access to objects. There are two radio button options: "ACLs disabled (recommended)" and "ACLs enabled". The "ACLs enabled" option is selected. Below this, the "Object Ownership" section has two radio button options: "Bucket owner preferred" (selected) and "Object writer". A blue callout box states: "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". At the bottom, the "Block Public Access settings for this bucket" section is partially visible, showing the "Block all public access" checkbox.

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.

☐ **Block public access to buckets and objects granted through new access control lists (ACLs)**

Step 5:

The screenshot shows the AWS console interface for configuring a bucket's Block Public Access settings. The top navigation bar is the same as in Step 4. The main content area is titled "Block Public Access settings for this bucket" and includes an "Info" link. It explains that public access is granted through ACLs, bucket policies, access point policies, or all. There are five checkboxes for individual settings: "Block all public access", "Block public access to buckets and objects granted through new access control lists (ACLs)", "Block public access to buckets and objects granted through any access control lists (ACLs)", "Block public access to buckets and objects granted through new public bucket or access point policies", and "Block public and cross-account access to buckets and objects through any public bucket or access point policies". The "Block all public access" checkbox is selected. A warning box at the bottom states: "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." Below the warning box is a checkbox labeled "I acknowledge that the current settings might result in this bucket and the objects within becoming public." which is checked.

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.

Step 6:

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**

Step 7:

Amazon S3

Successfully created bucket "ameythakur"
To upload files and folders, or to configure additional bucket settings choose [View details](#).

Account snapshot
Last updated: Jan 16, 2022 by Storage Lens. Metrics are generated every 24 hours. [Learn more](#)

Total storage	Object count	Avg. object size	You can enable advanced metrics in the "default-account-dashboard" configuration.
3.7 KB	1	3.7 KB	

Buckets (1) Info
Buckets are containers for data stored in S3. [Learn more](#)

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)

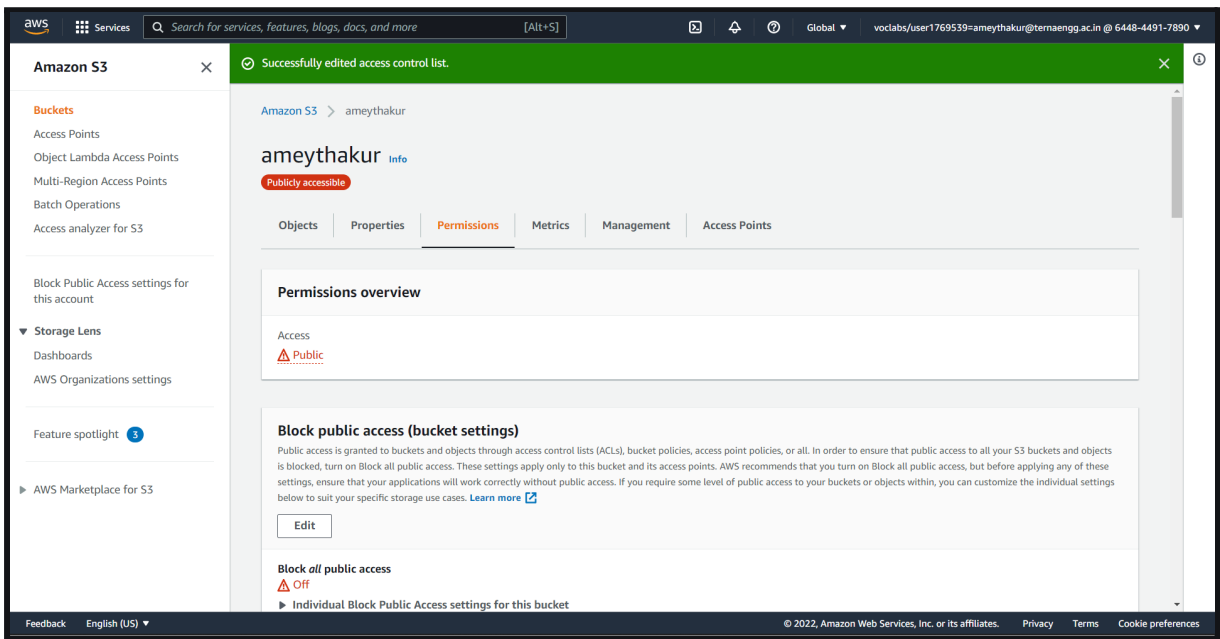
Step 8:

The screenshot shows the Amazon S3 console interface. On the left is a navigation pane with 'Amazon S3' selected. The main content area is titled 'ameythakur' and has tabs for 'Objects', 'Properties', 'Permissions' (which is active), 'Metrics', 'Management', and 'Access Points'. Under the 'Permissions' tab, there is a 'Permissions overview' section. It includes an 'Access' section stating 'Objects can be public'. Below that is a 'Block public access (bucket settings)' section with a paragraph explaining the settings and an 'Edit' button. At the bottom of this section, it says 'Block all public access' is 'Off' and provides a link to 'Individual Block Public Access settings for this bucket'.

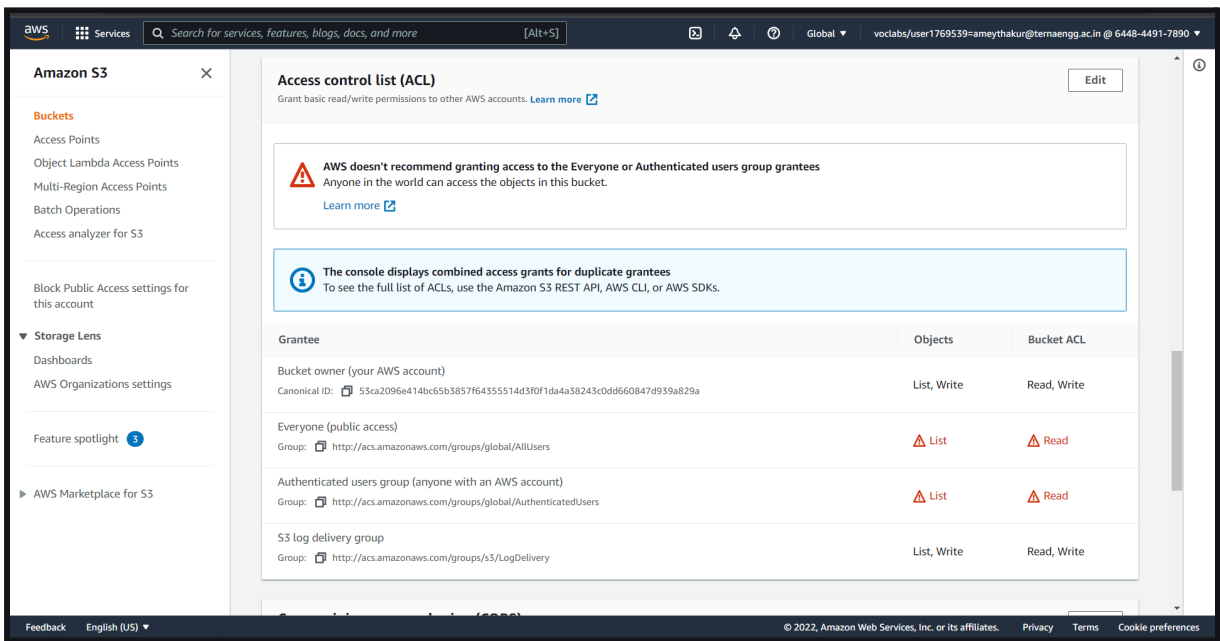
Step 9:

The screenshot shows the 'Edit access control list (ACL)' page in the Amazon S3 console. The navigation pane on the left is the same. The main content area is titled 'Edit access control list (ACL)'. Below the title is a section 'Access control list (ACL)' with a description and a 'Learn more' link. The main part of the page is a table with three columns: 'Grantee', 'Objects', and 'Bucket ACL'. The table lists four grantees: 'Bucket owner (your AWS account)', 'Canonical ID: 53ca2096e414bc65b3857f64355514d3f0f1da4a38243c0dd660847d939a825a', 'Everyone (public access)', and 'Authenticated users group (anyone with an AWS account)'. For each grantee, the 'Objects' column shows 'List' and 'Write' permissions, and the 'Bucket ACL' column shows 'Read' and 'Write' permissions. The 'Everyone (public access)' and 'Authenticated users group' rows have a red triangle icon next to the 'List' permission in the 'Objects' column and the 'Read' permission in the 'Bucket ACL' column. At the bottom of the table, there is a row for 'S3 log delivery group' with 'List' and 'Write' permissions in the 'Objects' column and 'Read' and 'Write' permissions in the 'Bucket ACL' column.

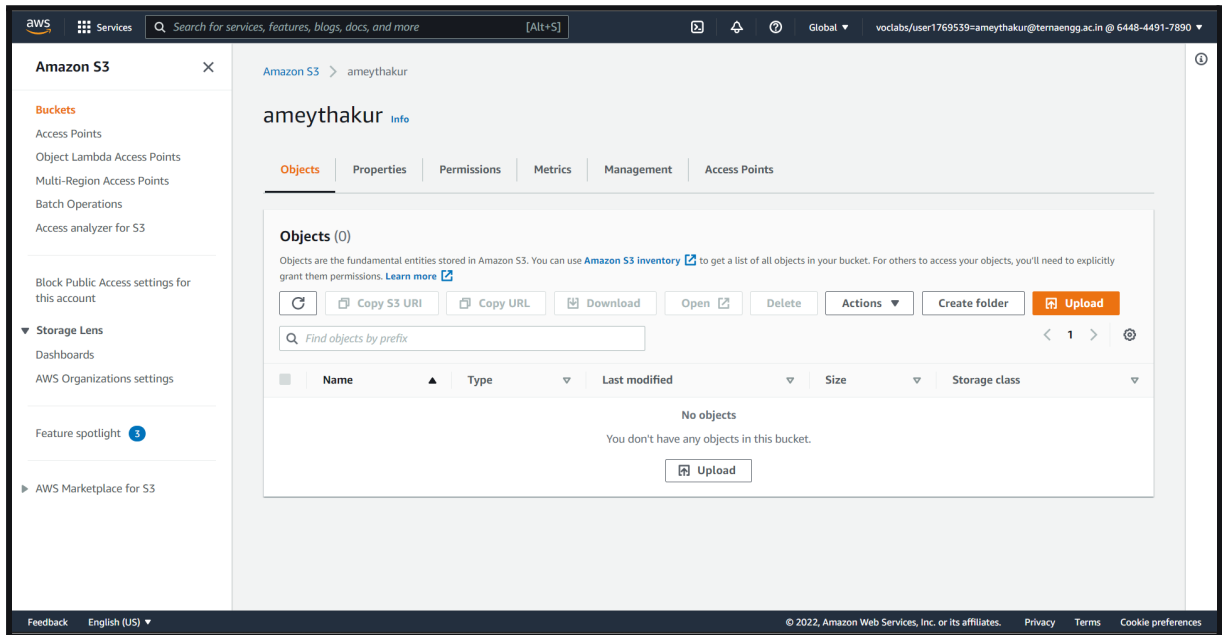
Step 10:



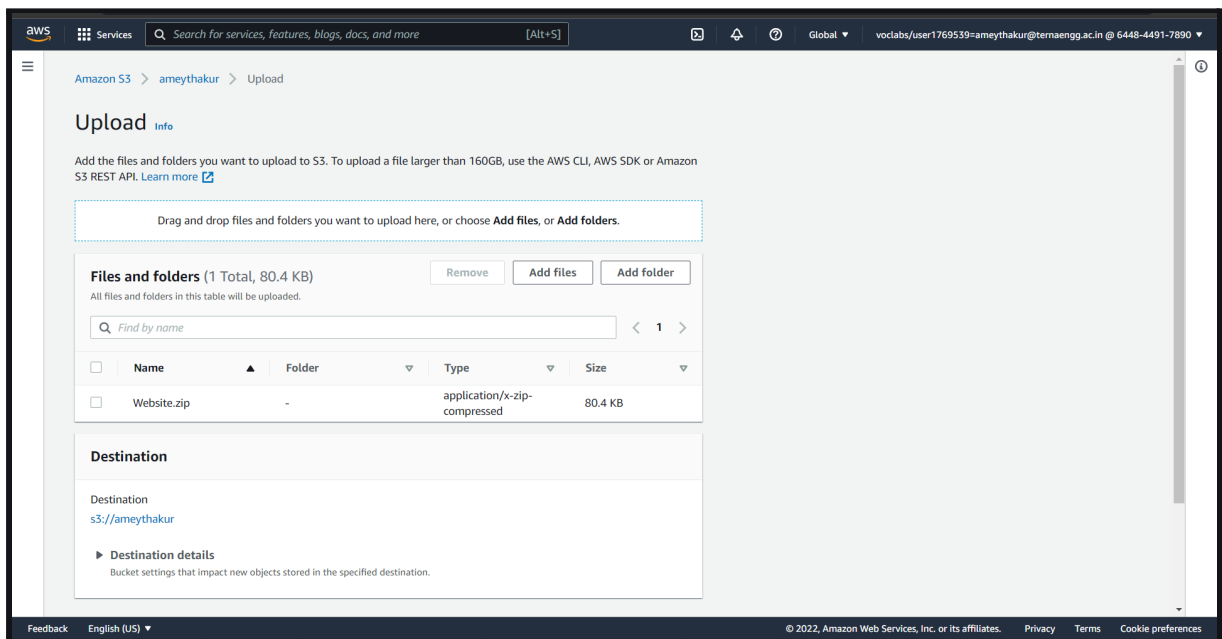
Step 11:



Step 12:



Step 13:



Step 14:

The screenshot shows the Amazon S3 console interface. On the left, the 'Amazon S3' sidebar is visible with options like Buckets, Access Points, and Storage Lens. The main content area displays the 'ameythakur' bucket, which is 'Publicly accessible'. Below the bucket name, there are tabs for Objects, Properties, Permissions, Metrics, Management, and Access Points. The 'Objects' tab is active, showing a list of objects. There is one object, 'Website.zip', which is a zip file, 80.4 KB in size, and stored in the Standard storage class. The object was last modified on February 14, 2022, at 11:25:20 (UTC+05:30). Above the object list, there are buttons for 'Copy S3 URI', 'Copy URL', 'Download', 'Open', 'Delete', 'Actions', 'Create folder', and 'Upload'. A search bar for finding objects by prefix is also present.

Step 15:

The screenshot shows the Amazon S3 console interface, specifically the details for the 'Website.zip' object. The breadcrumb navigation shows 'Amazon S3 > ameythakur > Website.zip'. The object name 'Website.zip' is displayed with an 'Info' link. Above the object name, there are buttons for 'Copy S3 URI', 'Download', 'Open', and 'Object actions'. Below the object name, there are tabs for Properties, Permissions, and Versions. The 'Properties' tab is active, showing an 'Object overview' section. This section contains two columns of metadata. The left column includes Owner (aws:labs0w3536438t1640812101), 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), and Key (Website.zip). The right column includes S3 URI (s3://ameythakur/Website.zip), Amazon Resource Name (ARN) (arn:aws:s3::ameythakur/Website.zip), Entity tag (Etag) (1dd69e6699cca8c7d6466cd2bdc713e0), and Object URL (https://ameythakur.s3.amazonaws.com/Website.zip).

Step 16:

The screenshot shows the AWS Management Console interface. On the left, the 'Amazon S3' sidebar is visible with options like Buckets, Access Points, and Storage Lens. The main content area displays the 'Website.zip' object details. The 'Permissions' tab is selected, showing the 'Access control list (ACL)'. The ACL table lists three entries:

Grantee	Object	Object ACL
Object owner (your AWS account) Canonical ID: 53ca2096e414bc65b3857f64355514d3f0f1da4a38243cdd660847d939a829a	Read	Read, Write
Everyone (public access) Group: http://acs.amazonaws.com/groups/global/AllUsers	Read	Read
Authenticated users group (anyone with an AWS account) Group: http://acs.amazonaws.com/groups/global/AuthenticatedUsers	Read	Read

Buttons for 'Copy S3 URI', 'Download', 'Open', and 'Object actions' are at the top right. The footer shows the URL 'https://s3.console.aws.amazon.com/s3/#' and copyright information for 2022.

Step 17:

The screenshot shows the AWS Management Console search results for 'EC2'. The search bar at the top contains 'EC2'. The results are displayed in a list of services and features. The 'Services' section includes:

- EC2** (Virtual Servers in the Cloud) - Top features: Dashboard, Launch templates, Instances, Spot Instance requests, Savings plans.
- EC2 Image Builder** (A managed service to automate build, customize and deploy OS images)
- AWS Compute Optimizer** (Recommend optimal AWS Compute resources for your workloads)
- AWS Firewall Manager** (Central management of firewall rules)

The 'Features' section includes:

- Export snapshots to EC2** (Lightsail feature)
- Dashboard** (EC2 features)

The sidebar on the left shows search results for 'EC2' across various categories like Services (9), Features (40), Blogs (1,699), Documentation (117,611), Knowledge Articles (30), Tutorials (15), Events (7), and Marketplace (1,403). The footer shows the URL 'https://console.aws.amazon.com/ec2/#' and copyright information for 2022.

Step 18:

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

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) [Select](#)

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

Amazon Linux 2 AMI (HVM) - Kernel 4.14, SSD Volume Type - ami-038b3df3312ddf25d (64-bit x86) / ami-0a200d3f40a2f6ca0 (64-bit Arm) [Select](#)

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

Feedback English (US) © 2022, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Step 19:

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 ⓘ
<input type="checkbox"/>	t2	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
<input checked="" type="checkbox"/>	t2	t2.micro Free tier eligible	1	1	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	t2	t2.small	1	2	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	t2	t2.medium	2	4	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	t2	t2.large	2	8	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	t2	t2.xlarge	4	16	EBS only	-	Moderate	Yes
<input type="checkbox"/>	t2	t2.2xlarge	8	32	EBS only	-	Moderate	Yes
<input type="checkbox"/>	t3	t3.nano	2	0.5	EBS only	Yes	Up to 5 Gigabit	Yes
<input type="checkbox"/>	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

Step 20:

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](#)

Step 21:

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	<input checked="" type="checkbox"/>	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](#)

Step 22:

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	Value	Instances	Volumes	Network Interfaces
Name	AMEY	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[Add another tag](#) (Up to 50 tags maximum)

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Configure Security Group](#)

Step 23:

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](#)

Step 24:

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, system 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](#)

Step 25:

Step 7: Review Instance Launch
Free tier eligible
CAUTION: THIS AMI IS THE SUCCESSOR OF THE PREVIOUS LINUX AMI THAT IS EL...
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](#)

Step 26:

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

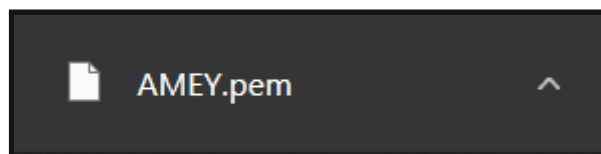
AMEY

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

Step 27:



Step 28:

The screenshot shows the 'Launch Status' page in the AWS Management Console. At the top, a green banner states 'Your instances are now launching' with a link to 'View launch log'. Below this, a blue banner provides information about estimated charges and a link to 'Create billing alerts'. The main content area is titled 'How to connect to your instances' and explains that instances will be in the 'running' state. It includes a section 'Here are some helpful resources to get you started' with links to 'How to connect to your Linux Instance', 'Learn about AWS Free Usage Tier', 'Amazon EC2: User Guide', and 'Amazon EC2: Discussion Forum'. A 'View Instances' button is located at the bottom right.

Launch Status

✓ **Your instances are now launching**
The following instance launches have been initiated: [i-0c4723c385a7a1d0b](#) [View launch log](#)

ℹ **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](#)

Step 29:

The screenshot shows the 'Instances' page in the AWS Management Console. A table lists the instance 'AMEY' with ID 'i-0c4723c385a7a1d0b', state 'Running', type 't2.micro', and status 'Initializing'. Below the table, the 'Details' tab is selected, showing the 'Instance summary' for 'i-0c4723c385a7a1d0b (AMEY)'. The summary includes the instance ID, public and private IP addresses, DNS names, and VPC ID.

Instances (1/1) Info

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
AMEY	i-0c4723c385a7a1d0b	Running	t2.micro	Initializing	No alarms	us-east-1a	ec2-54-243-4-11

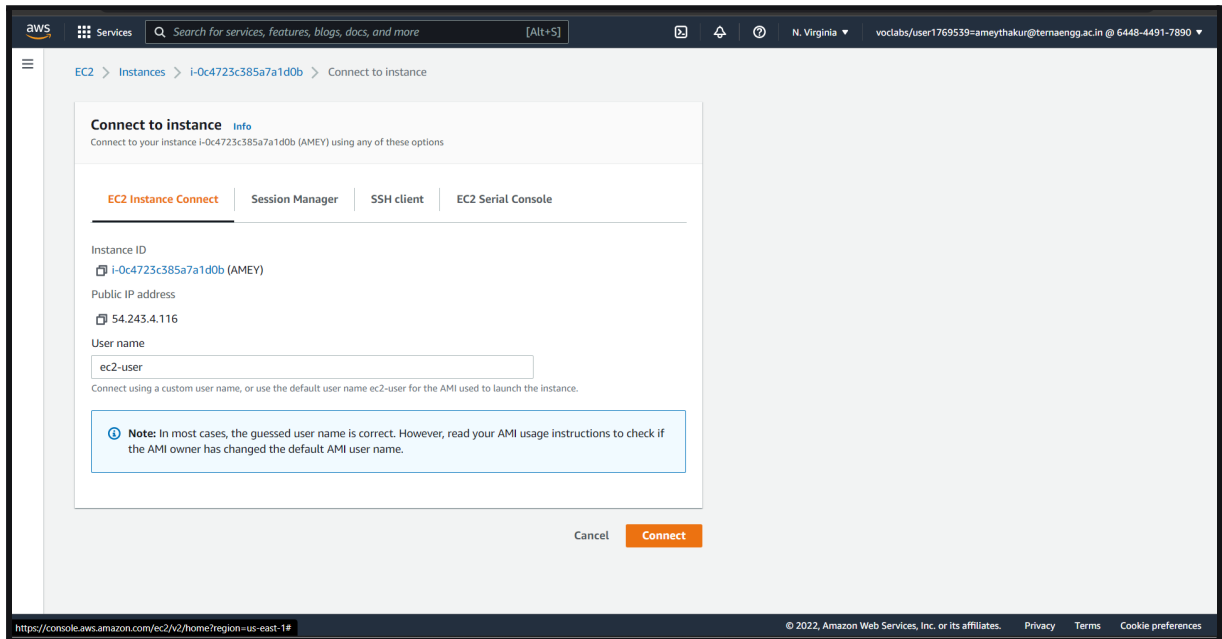
Instance: i-0c4723c385a7a1d0b (AMEY)

Details | Security | Networking | Storage | Status checks | Monitoring | Tags

▼ **Instance summary** Info

Instance ID i-0c4723c385a7a1d0b (AMEY)	Public IPv4 address 54.243.4.116 open address	Private IPv4 addresses 172.31.89.95
IPv6 address -	Instance state Running	Public IPv4 DNS ec2-54-243-4-116.compute-1.amazonaws.com open address
Hostname type IP name: ip-172-31-89-95.ec2.internal	Private IP DNS name (IPv4 only) ip-172-31-89-95.ec2.internal	Answer private resource DNS name IPv4 (A)
Instance type t2.micro	Elastic IP addresses -	VPC ID vpc-0fec2db21aed40bb9

Step 30:



Step 31:



Step 32:

```

  ____  _
 / ___|| | | |
| |___| | | |
 \___|| | | |
      |_|_|_|

Amazon Linux 2 AMI

https://aws.amazon.com/amazon-linux-2/
3 package(s) needed for security, out of 6 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-172-31-89-95 ~]$ sudo su
[root@ip-172-31-89-95 ec2-user]# yum update -y
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
Resolving Dependencies
--> Running transaction check
--> Package ca-certificates.noarch 0:2021.2.50-72.amzn2.0.2 will be updated
--> Package ca-certificates.noarch 0:2021.2.50-72.amzn2.0.3 will be an update
--> Package ec2-net-utils.noarch 0:1.5-3.amzn2 will be updated
--> Package ec2-net-utils.noarch 0:1.6-1.amzn2 will be an update
--> Package ec2-utils.noarch 0:1.2-45.amzn2 will be updated
--> Package ec2-utils.noarch 0:1.2-46.amzn2 will be an update
--> Package openssh.x86_64 0:7.4p1-21.amzn2.0.3 will be updated
--> Package openssh.x86_64 0:7.4p1-22.amzn2.0.1 will be an update
--> Package openssh-clients.x86_64 0:7.4p1-21.amzn2.0.3 will be updated
--> Package openssh-clients.x86_64 0:7.4p1-22.amzn2.0.1 will be an update
--> Package openssh-server.x86_64 0:7.4p1-21.amzn2.0.3 will be updated
--> Package openssh-server.x86_64 0:7.4p1-22.amzn2.0.1 will be an update
--> Finished Dependency Resolution

Dependencies Resolved

=====
Package Arch Version Repository Size
=====
Updating:
ca-certificates noarch 2021.2.50-72.amzn2.0.3 amzn2-core 372 k
ec2-net-utils noarch 1.6-1.amzn2 amzn2-core 18 k
ec2-utils noarch 1.2-46.amzn2 amzn2-core 12 k
=====

i-0c4723c385a7a1d0b (AMEY)
Public IPs: 54.243.4.116 Private IPs: 172.31.89.95
```

Step 33:

```

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
```

Step 34:

```
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
```

Step 35:

```
[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 36:



Q2: Compare static and dynamic websites.

ANS:

Static Web Page	Dynamic Web Page
In static web pages, Pages will remain the same until someone changes them manually.	In dynamic web pages, the Content of pages is different for different visitors.
Static Web Pages are simple in terms of complexity.	Dynamic web pages are complicated.
In static web pages, Information is changed rarely.	In a dynamic web page, Information is changed frequently.
Static Web Page takes less time for loading than a dynamic web page.	Dynamic web page takes more time for loading.
In Static Web Pages, the database is not used.	In dynamic web pages, the database is used.

Static web pages are written in languages such as HTML, JavaScript, CSS, etc.	Dynamic web pages are written in languages such as CGI, AJAX, ASP, ASP.NET, etc.
Static web pages do not contain any application program.	Dynamic web pages contain application programs for different services.
Static web pages require less work and cost in designing them.	Dynamic web pages require comparatively more work and cost in designing them.

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.