

EXPERIMENT 1A

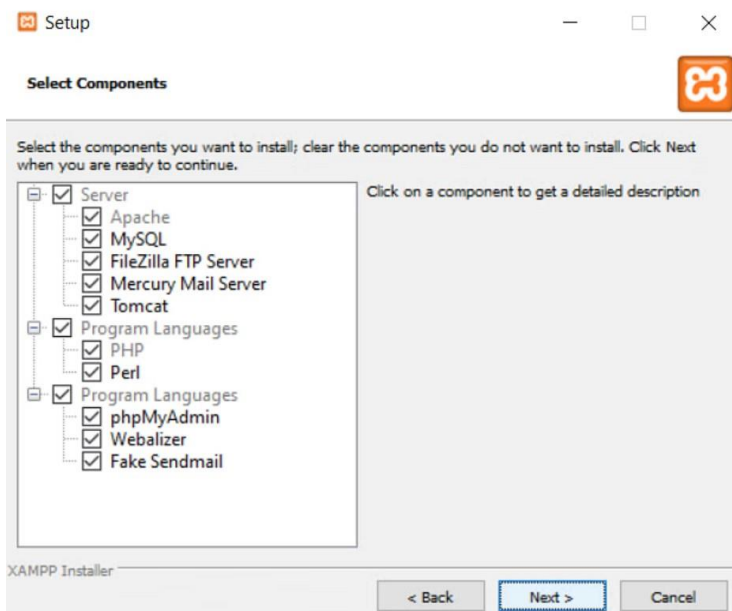
Aim: To develop a website and host it on i) local machine or virtual machine
ii) Amazon S3 Bucket

Static Hosting:

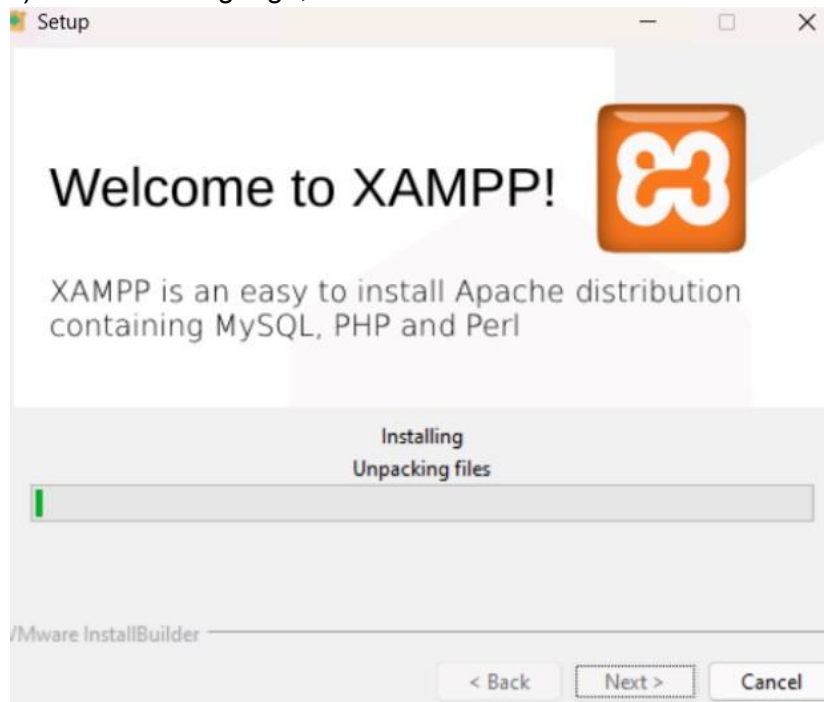
1) On local server (XAMPP)

Step 1: Install XAMPP from <https://www.apachefriends.org/> .

1) Select your OS. It will automatically start downloading.



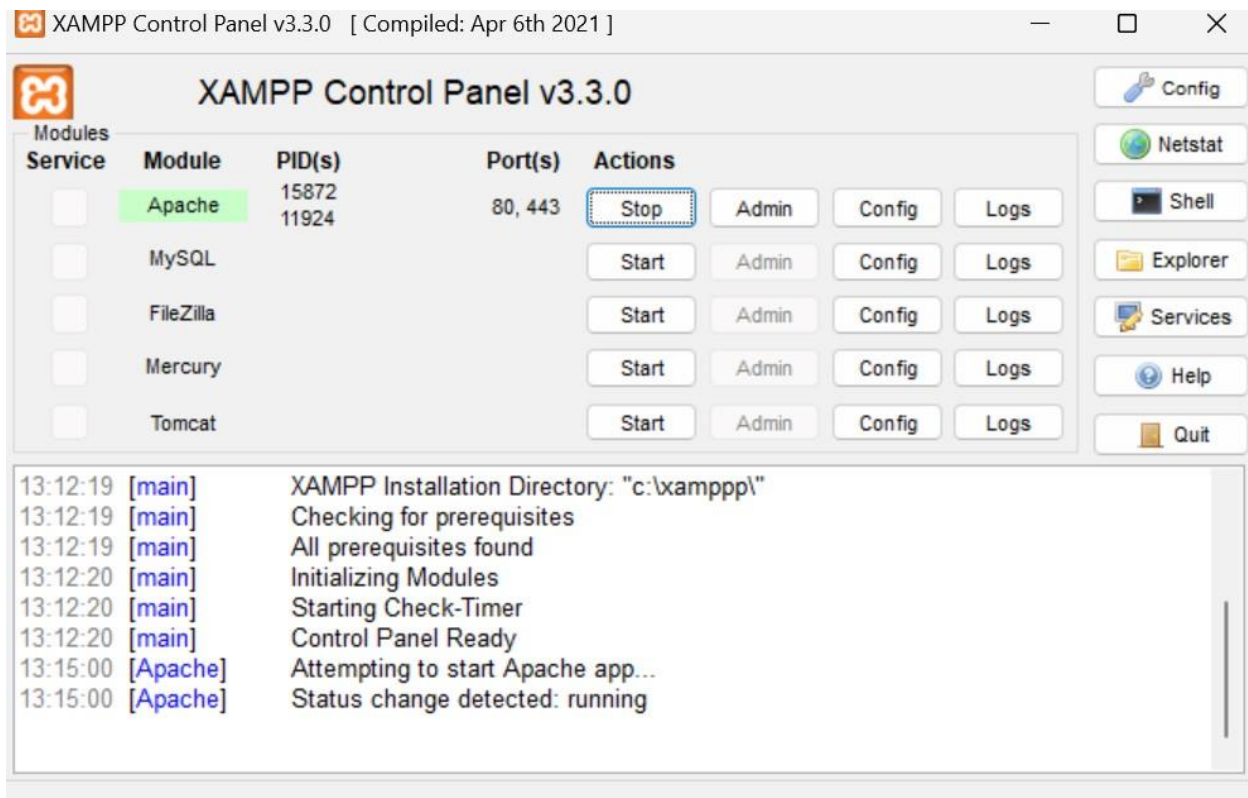
- 2) Open the setup file. Select all the required components and click next.
- 3) Select the language, click next. XAMPP starts to install.



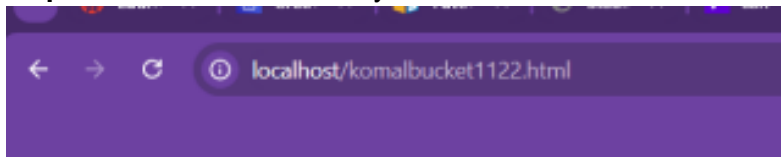
- 4) The installation is complete. Click Finish.



Step 2: Open XAMPP Control Panel, start the Apache service (Required) and mySQL service (if needed)



Step 3: Write an html file for your website and host it



My Information

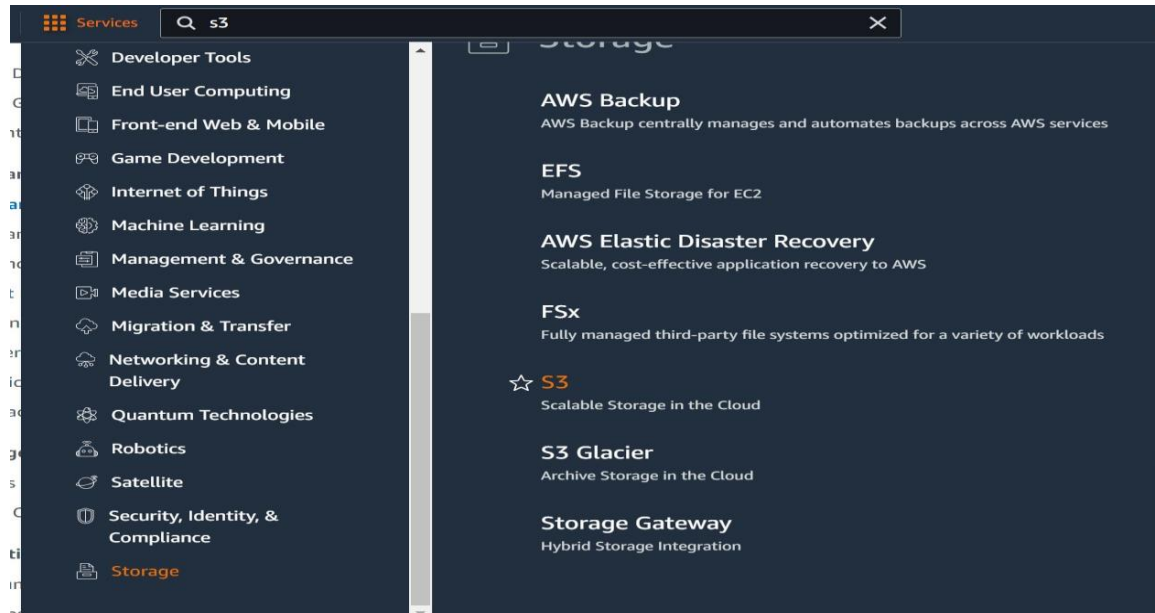
Name:Komal Sabale

Class:D15C

Roll No:45

2) AWS S3

Step 1: Login to your AWS account. Go to services and open S3.



Step 2: Click on Create Bucket. Give a name to your bucket, keeping other options default, scroll down and click on Create Bucket.

Create bucket [Info](#)

Buckets are containers for data stored in S3.

General configuration

AWS Region

US East (N. Virginia) us-east-1

Bucket type [Info](#)

☒ **General purpose**

Recommended for most use cases and access patterns. General purpose buckets are the original S3 bucket type. They allow a mix of storage classes that redundantly store objects across multiple Availability Zones.

☐ **Directory - New**

Recommended for low-latency use cases. These buckets use only the S3 Express One Zone storage class, which provides faster processing of data within a single Availability Zone.

Bucket name [Info](#)

komalbucket1122

Bucket name must be unique within the global namespace and follow the bucket naming rules. [See rules for bucket naming](#)

Copy settings from existing bucket - *optional*

Only the bucket settings in the following configuration are copied.

[Choose bucket](#)

Format: s3://bucket/prefix

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 enforced

Default encryption [Info](#)

Server-side encryption is automatically applied to new objects stored in this bucket.

Encryption type [Info](#)

☒ **Server-side encryption with Amazon S3 managed keys (SSE-S3)**

☐ **Server-side encryption with AWS Key Management Service keys (SSE-KMS)**

☐ **Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)**

Secure your objects with two separate layers of encryption. For details on pricing, see [DSSE-KMS pricing](#) on the [Storage](#) tab of the [Amazon S3 pricing page](#).

Bucket Key

Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. [Learn more](#)

☐ **Disable**

☒ **Enable**

► Advanced settings

i After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.

Cancel

Create bucket

Step 3: Go to the Objects tab and click on upload file.

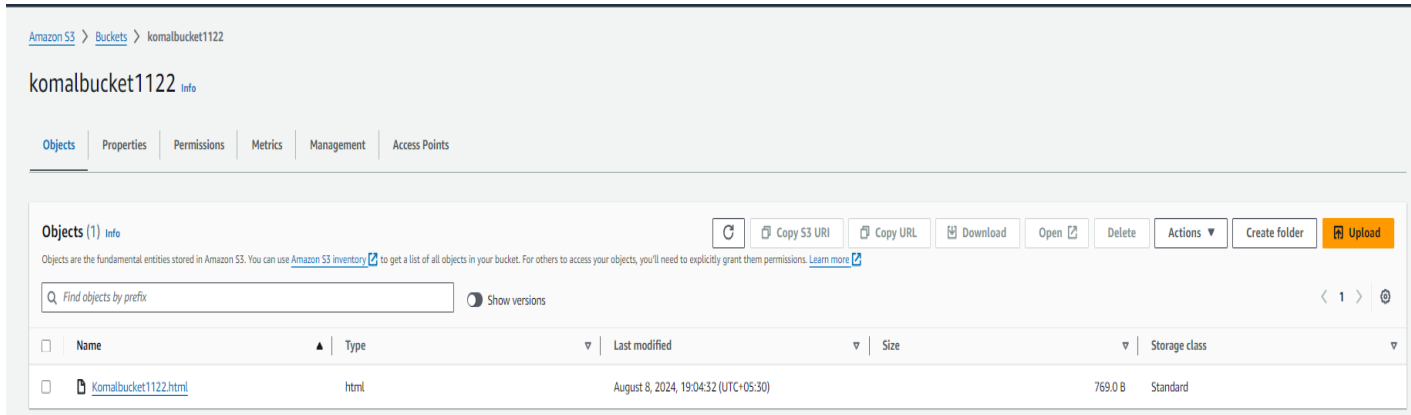
The screenshot shows the AWS Management Console interface for the 'Upload' page of the bucket 'komalbucket1122'. The breadcrumb navigation at the top reads 'Amazon S3 > Buckets > komalbucket1122 > Upload'. The main heading is 'Upload' with an 'Info' link. Below this, a message states: 'Add the files 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](#)'. A dashed box contains the instruction: 'Drag and drop files and folders you want to upload here, or choose **Add files** or **Add folder**.' Below this is a section titled 'Files and folders (1 Total, 769.0 B)' with 'Remove', 'Add files', and 'Add folder' buttons. A note says 'All files and folders in this table will be uploaded.' There is a search bar with the placeholder 'Find by name' and pagination controls showing '< 1 >'. A table lists the upload items:

<input type="checkbox"/>	Name	Folder	Type
<input type="checkbox"/>	Komalbucket1122.html	-	text/html

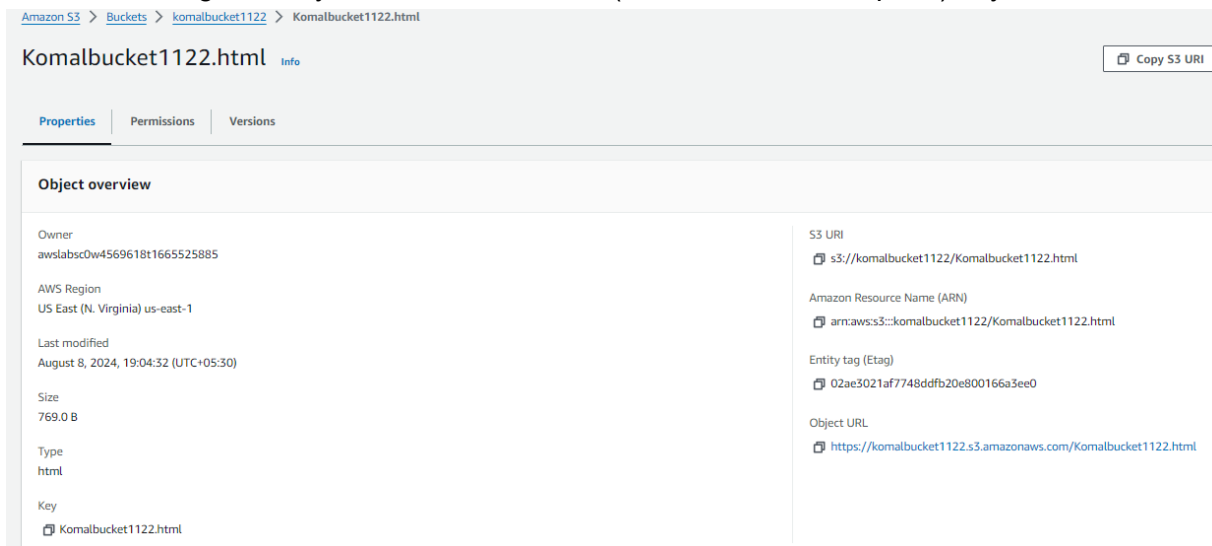
Below the table is a 'Destination' section with an 'Info' link. It shows the destination as 's3://komalbucket1122' and includes a 'Destination details' link.

Komal Sabale
D15C-45

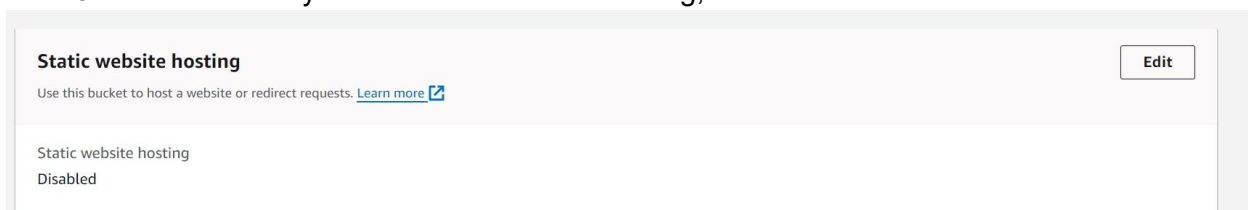
4: Click on Add files. Add all the files you want to upload. Then scroll down and click on Upload.



Step 5: This will take you to the Objects screen. Switch to Properties and scroll down to Static Website Hosting. There you would find the link (Bucket website endpoint) to your website.



6: Scroll down till you find Static website hosting, click on edit.



Komal Sabale
D15C-45

Step 7: Enable static website hosting, in Index document, write the name of your document.
Save your changes.

Edit static website hosting [Info](#)

Static website hosting

Use this bucket to host a website or redirect requests. [Learn more](#)

Static website hosting

☐ Disable

☒ Enable

Hosting type

☒ Host a static website
Use the bucket endpoint as the web address. [Learn more](#)

☐ Redirect requests for an object
Redirect requests to another bucket or domain. [Learn more](#)

i For your customers to access content at the website endpoint, you must make all your content publicly readable. To do so, you can edit the S3 Block Public Access settings for the bucket. For more information, see [Using Amazon S3 Block Public Access](#)

Index document

Specify the home or default page of the website.

static.html

Step 8: Uncheck the Block all public access checkbox and click on save changes.
9: Scroll down to bucket policy and click edit.

Edit Block public access (bucket settings) [Info](#)

Block public access (bucket settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

☐ **Block all public access**
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

- ☐ **Block public access to buckets and objects granted through new access control lists (ACLs)**
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
- ☐ **Block public access to buckets and objects granted through any access control lists (ACLs)**
S3 will ignore all ACLs that grant public access to buckets and objects.
- ☐ **Block public access to buckets and objects granted through new public bucket or access point policies**
S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.
- ☐ **Block public and cross-account access to buckets and objects through any public bucket or access point policies**
S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

Komal Sabale

D15C-45

Amazon S3 > Buckets > statichosting27 > Edit bucket policy

Edit bucket policy

Info

Bucket policy

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. [Learn more](#)

Policy examples

Policy generator

Bucket ARN

arn:aws:s3:::statichosting27

Policy

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Sid": "PublicReadGetObject",
6       "Effect": "Allow",
7       "Principal": {
8         "AWS": "*"
9       },
10      "Action": "s3:GetObject",
11      "Resource": "arn:aws:s3:::statichosting27/*"
12    }
13  ]
14 }
```

Edit statement

PublicReadGetObject

Remove

Add actions

Choose a service

Filter services

Included

S3

Available

AMP

API Gateway

API Gateway V2

CloudShell

Feedback

© 2024, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preference](#)

Successfully edited bucket policy.

Bucket policy

Edit

Delete

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. [Learn more](#)

```
{
  "Version": "2012-10-17",
  "id": "Policy1723131852074",
  "Statement": [
    {
      "Sid": "Stmt1723131850535",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::komalbucket1122/*"
    }
  ]
}
```

Copy

Komal Sabale
D15C-45

Step 10: You can access your website now.

