

Aim: Hosting a static website on Amazon Web Services (S3)

1) Open the AWS console home

The screenshot shows the AWS Console Home page. On the left, there's a sidebar with 'Recently visited' (EC2, IAM, Cloud9), 'Welcome to AWS', 'AWS Health', and 'Cost and usage'. The main area has a header for 'Applications (0)' with a 'Create application' button. It shows a message: 'No applications. Get started by creating an application.' Below this is another 'Create application' button and a link to 'Go to myApplications'. At the bottom of the page are links for 'cloudShell', 'Feedback', and copyright information.

2) Navigate to the S3 to host the website

The screenshot shows the AWS navigation sidebar on the left and a 'Recently visited' modal on the right. The sidebar lists various services like Analytics, Application Integration, EC2, IAM, etc. The 'S3' service is highlighted in orange, indicating it is the currently selected service. The 'Recently visited' modal lists 'S3' (Scalable Storage in the Cloud), 'Console Home' (View resource insights, service shortcuts, and feature updates), 'EC2' (Virtual Servers in the Cloud), 'IAM' (Manage access to AWS resources), and 'Cloud9' (A Cloud IDE for Writing, Running, and Debugging Code).

3) On S3, click on create bucket

Create a bucket

Every object in S3 is stored in a bucket. To upload files and folders to S3, you'll need to create a bucket where the objects will be stored.

[Create bucket](#)

- 4) Click on Bucket type as General Purpose and name the bucket.

The screenshot shows the 'Create New Bucket' page in the AWS Management Console. The 'AWS Region' is set to 'US East (N. Virginia) us-east-1'. Under 'Bucket type', the 'General purpose' option is selected, which is described as recommended for most use cases and access patterns. It also notes that general purpose buckets are the original S3 bucket type and allow a mix of storage classes that redundantly store objects across multiple Availability Zones. The 'Directory - New' option is also available but not selected. In the 'Bucket name' section, the name 'brijeshbucket' is entered. A note states that the bucket name must be unique within the global namespace and follows specific naming rules, with a link to 'See rules for bucket naming'. Below this, there's a 'Copy settings from existing bucket - optional' section with a 'Choose bucket' button and a note about copied settings. The 'Format' is shown as 's3://bucket/prefix'.

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](#)

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

- 5) Keep the default settings intact, checking for bucket versioning as disabled and bucket key enabled.

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

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 application 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 case. [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.

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 - optional (0)
You can use bucket tags to track storage costs and organize buckets. [Learn more](#)

No tags associated with this bucket.
[Add tag](#)

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 (DSS-E-KMS)
Secure your objects with two separate layers of encryption. For details on pricing, see SSE-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 DSS-E-KMS. [Learn more](#)

Disable
 Enable

Advanced settings

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

[Cancel](#) [Create bucket](#)

- 6) After successfully creating the bucket, click on bucket name to change the settings to host the website.

The screenshot shows the AWS S3 buckets page. At the top, a green banner indicates: "Successfully created bucket 'brijeshkabucket'". Below the banner, it says "To upload files and folders, or to configure additional bucket settings, choose View details." On the left, the navigation path is "Amazon S3 > Buckets". In the center, there's an "Account snapshot - updated every 24 hours" section with a link to "All AWS Regions". To the right is a "View Storage Lens dashboard" button. Below these are tabs for "General purpose buckets" (selected) and "Directory buckets". Under "General purpose buckets", there's a sub-section titled "General purpose buckets (1) Info All AWS Regions". It shows one bucket named "brijeshkabucket" with the following details: Name (brijeshkabucket), AWS Region (All AWS Regions), IAM Access Analyzer (Off), Creation date (August 7, 2024, 20:38:57 (UTC+05:30)). There are buttons for "Copy ARN", "Empty", "Delete", and "Create bucket". A search bar at the bottom allows finding buckets by name.

- 7) Go on Permissions tab and check for Block public access

The screenshot shows the "static-bucket-first" bucket page. The navigation path is "Amazon S3 > Buckets > static-bucket-first". The main content area displays two objects: "index.html" (html file, 490.0 B, Standard storage class) and "style.css" (css file, 546.0 B, Standard storage class). Above the objects list, there are buttons for "Actions" (including Copy S3 URI, Copy URL, Download, Open, Delete, Create folder, Upload), a search bar, and pagination controls. Below the objects list, there are tabs for "Objects" (selected), "Properties", "Permissions", "Metrics", "Management", and "Access Points".

- 8) Block public access is default on, we need to uncheck it to ensure the hosted website is public.

The screenshot shows the "Block public access (bucket settings)" page. At the top, it says "Block all public access" with a "On" status. Below this, there's a link "Individual Block Public Access settings for this bucket". On the right side, there's an "Edit" button.

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

On

Individual Block Public Access settings for this bucket

- 9) Now the block public access option is unchecked and hence the website can be hosted successfully.

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

⚠ Off

► Individual Block Public Access settings for this bucket

- 10) Now, navigate to the edit bucket policy in Properties tab to provide access to the services.

Amazon S3 > Buckets > brijeshkabucket > 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](#)

Bucket ARN

arn:aws:s3:::brijeshkabucket

Policy

1 |

Edit statement

Select a statement

Select an existing statement in the policy or add a new statement.

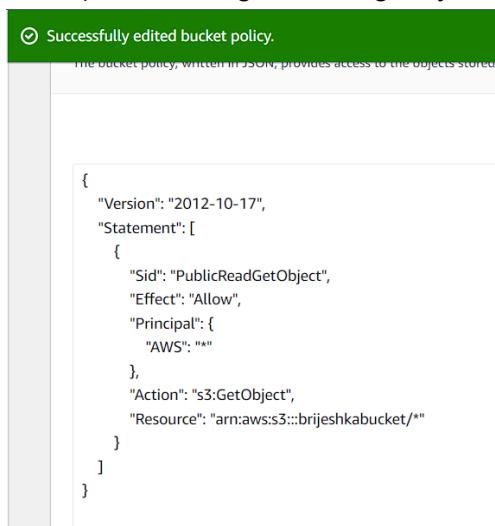
- 11) Fill the following policy in the empty policy space. Ensure that you change the name of the bucket in Resource with the name of your bucket.

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:::brijeshkabucket/*"
12    }
13 }
14 }
```

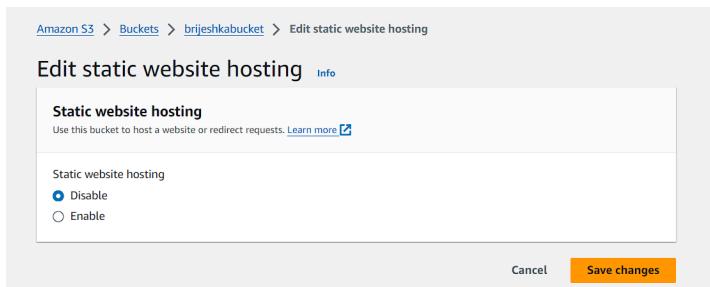
12) After saving the changes, you will see a message.



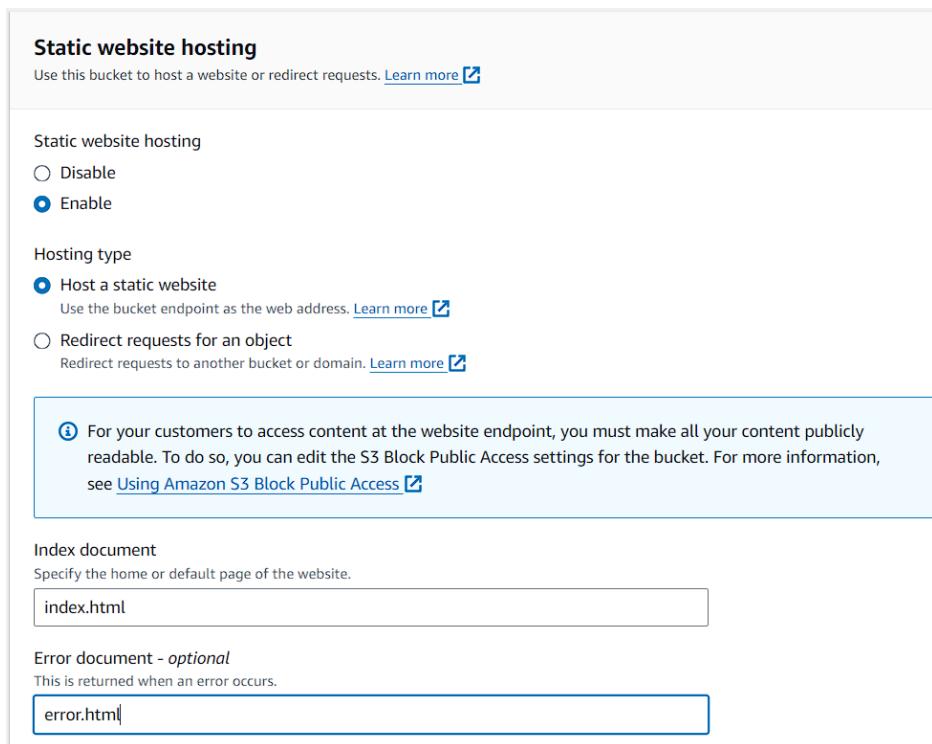
The screenshot shows a green success message box with the text: "Successfully edited bucket policy." Below the message, there is a JSON representation of the bucket policy:

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

13) Go to the edit static website hosting in the properties tab to use bucket to host websites.



14) Check the options as shown below, and add the names of the file.



The screenshot shows the 'Static website hosting' configuration dialog. It includes sections for 'Static website hosting' (radio button for 'Enable' selected), 'Hosting type' (radio button for 'Host a static website' selected), and 'Index document' (input field containing 'index.html'). A note at the bottom explains that content must be publicly readable. There is also an 'Error document - optional' input field containing 'error.html'.

- 15) Navigate to the Upload section and upload the documents with the name as mentioned in the previous section.

The screenshot shows the 'Upload' section of the AWS S3 console. At the top, there's a breadcrumb navigation: Amazon S3 > Buckets > brijeshkabucket > Upload. Below the navigation is a title 'Upload' with a 'Info' link. A sub-instruction says: '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' with a link icon. A large dashed box area is labeled 'Drag and drop files and folders you want to upload here, or choose Add files or Add folder.' Below this is a table titled 'Files and folders (0)' with a 'Remove' button. A note says 'All files and folders in this table will be uploaded.' A search bar 'Find by name' and a page navigation '1' are also present.

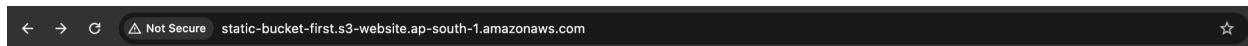
- 16) Uploaded files will be visible after successful upload.

The screenshot shows the 'Files and folders' list in the AWS S3 console. The title is 'Files and folders (2 Total, 906.0 B)'. A note says 'All files and folders in this table will be uploaded.' Below is a search bar 'Find by name' and a table with a 'Remove' button. The table has columns for 'Name', 'Folder', and 'Type'. It lists two files: 'error.html' and 'index.html', both of which are 'text/html' type files.

- 17) Get the link for the hosted website in the properties tab at the bottom.

The screenshot shows the 'Static website hosting' properties tab in the AWS S3 console. It includes sections for 'Static website hosting' (with a note to host a website or redirect requests), 'Hosting type' (Bucket hosting), and 'Bucket website endpoint' (with a note about the AWS Region-specific website endpoint). A link to the endpoint is provided: <http://brijeshkabucket.s3-website-us-east-1.amazonaws.com>.

18) The hosted website using AWS S3.



Welcome to My Basic Webpage by Krushikesh

This is a sample paragraph of content.

© 2024 My Basic Webpage

19) To terminate the S3 bucket, first empty the bucket by selecting the files and clicking on Empty.

The screenshot shows the AWS S3 console interface. At the top, there's a navigation bar with icons for back, forward, and search, followed by a status indicator 'Not Secure' and the URL 'static-bucket-first.s3-website.ap-south-1.amazonaws.com'. Below the navigation is a heading 'Welcome to My Basic Webpage by Krushikesh' and some sample content. Underneath the content, there's a copyright notice. In the center, there's a table listing buckets. One row is selected, showing details: Name 'brijeshkabucket', AWS Region 'US East (N. Virginia) us-east-1', IAM Access Analyzer link, and Creation date 'August 7, 2024, 20:38:57 (UTC+05:30)'. A success message at the bottom of the list says 'Successfully emptied bucket "brijeshkabucket"'. A modal window titled 'Empty bucket: status' is overlaid on the list. It contains a summary section with three boxes: 'Source s3://brijeshkabucket' (with a link icon), 'Successfully deleted 2 objects, 906.0 B' (with a link icon), and 'Failed to delete 0 objects'. Below this is a 'Failed to delete (0)' section with a table header and a message 'No failed object deletions'.

20) Then navigate to the Delete bucket option and enter the name of the bucket and delete the bucket.

Amazon S3 > Buckets > brijeshkabucket > Delete bucket

Delete bucket Info

⚠ • Deleting a bucket cannot be undone.
• Bucket names are unique. If you delete a bucket, another AWS user can use the name.
• If this bucket is used with a Multi-Region Access Point in an external account, initiate failover before deleting the bucket.
• If this bucket is used with an access point in an external account, the requests made through those access points will fail after you delete this bucket.
• This bucket is configured to host a static website. We recommend that you clean up the Route 53 hosted zone settings that are related to the bucket.

[Learn more](#)

Delete bucket "brijeshkabucket"?

To confirm deletion, enter the name of the bucket in the text input field.

[Cancel](#) [Delete bucket](#)

21) After deleting the bucket, a message will appear.

Successfully deleted bucket "brijeshkabucket"

Storage

Amazon S3

Store and retrieve any amount of data from anywhere

Amazon S3 is an object storage service that offers industry-leading scalability, data availability, security, and performance.

Create a bucket

Every object in S3 is stored in a bucket. To upload files and folders to S3, you'll need to create a bucket where the objects will be stored.

[Create bucket](#)

How it works

Introduction to Amazon S3

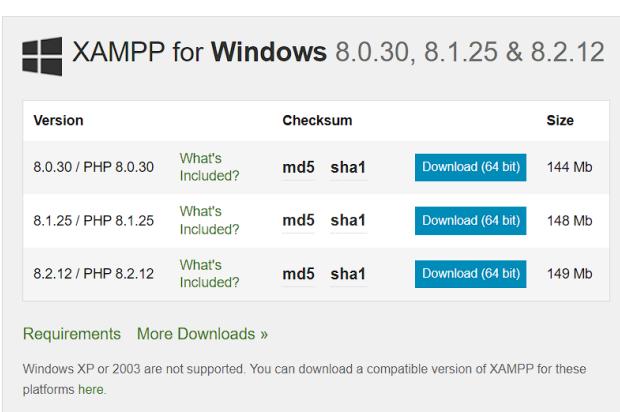
Copy link

Pricing

With S3, there are no minimum fees. You only pay for what you use. Prices are based on the location of your S3 bucket.

Estimate your monthly bill using the [AWS Simple Monthly Calculator](#)

- 1) Search for XAMPP download and navigate to the xampp official website and click on download as per your system.

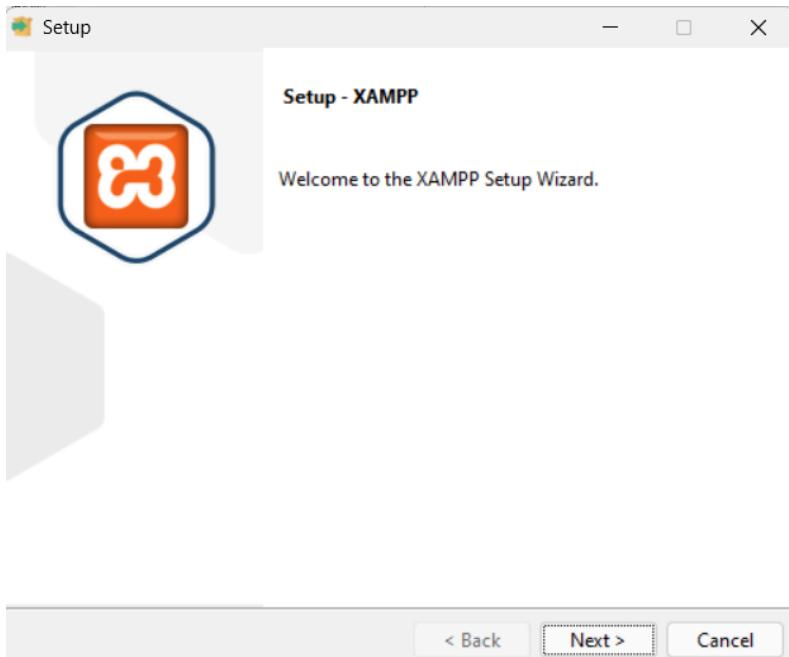


The screenshot shows the XAMPP Download page. At the top, there's a navigation bar with links for Apache Friends, Download, Hosting, Community, and About. There's also a search bar and a language selection for English. The main heading is "Download". Below the heading, a text block says: "XAMPP is an easy to install Apache distribution containing MariaDB, PHP, and Perl. Just download and start the installer. It's that easy. Installers created using InstallBuilder." A table lists three Windows installer versions:

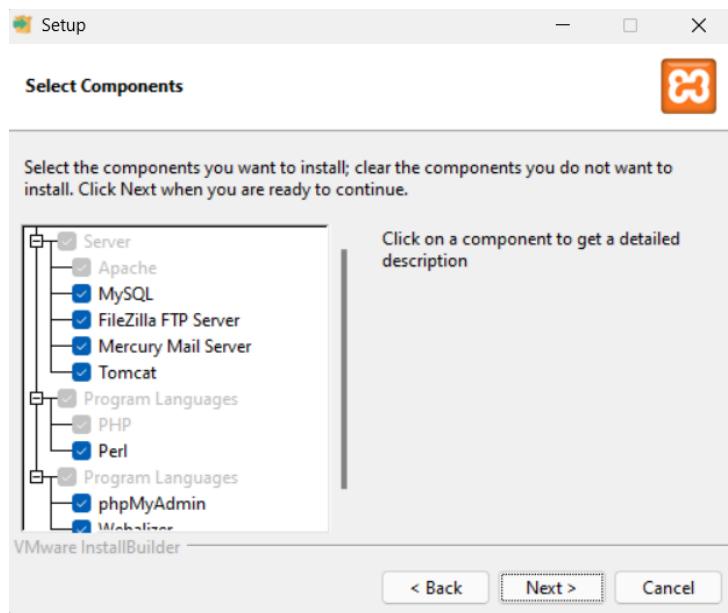
Version	Checksum	Size
8.0.30 / PHP 8.0.30	What's Included? md5 sha1	Download (64 bit) 144 Mb
8.1.25 / PHP 8.1.25	What's Included? md5 sha1	Download (64 bit) 148 Mb
8.2.12 / PHP 8.2.12	What's Included? md5 sha1	Download (64 bit) 149 Mb

Below the table, there are links for "Requirements" and "More Downloads ». A note at the bottom states: "Windows XP or 2003 are not supported. You can download a compatible version of XAMPP for these platforms [here](#)".

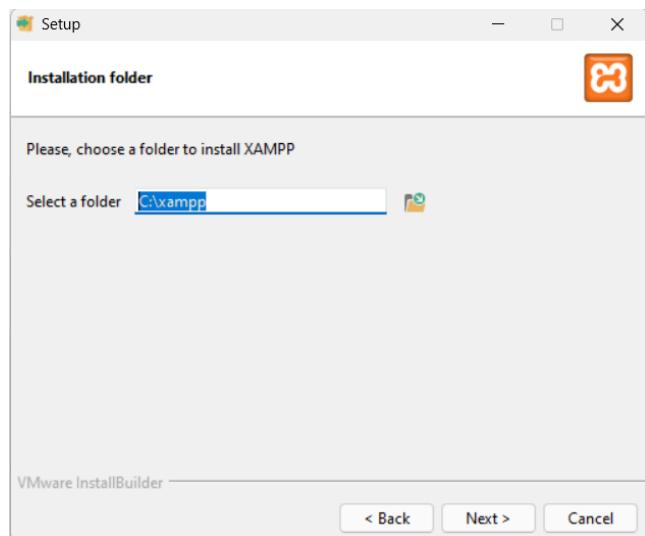
- 2) Xampp installer will be installed in the system.
- 3) Window asking to give permission will appear. Click pn 'Yes'.
- 4) A window will appear for setup. Click on 'Next'.



- 5) Keep the default settings and click on Next.



6) Choose the folder path.



7) Then the XAMPP installation will be done.

8) Locate the folder and then locate the 'htdocs' folder in the xampp folder.

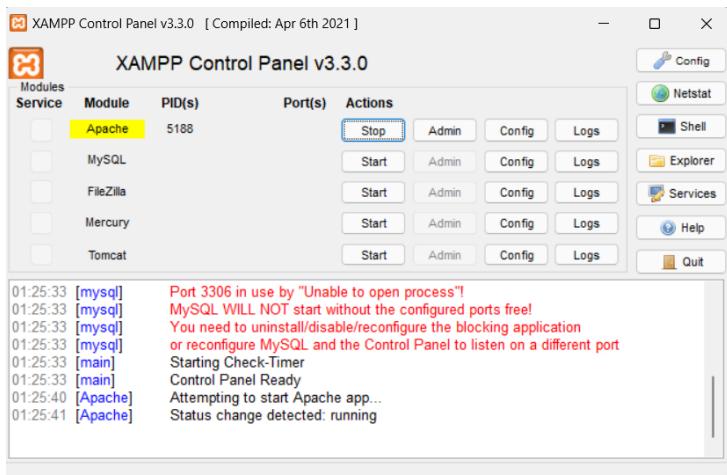
anonymous	01-08-2024 21:37	File folder
apache	01-08-2024 21:38	File folder
cgi-bin	01-08-2024 21:45	File folder
contrib	01-08-2024 21:37	File folder
FileZillaFTP	01-08-2024 21:45	File folder
htdocs	01-08-2024 21:51	File folder
img	01-08-2024 21:37	File folder
install	01-08-2024 21:45	File folder

9) Create a test.php file in the htdocs folder and write php code.

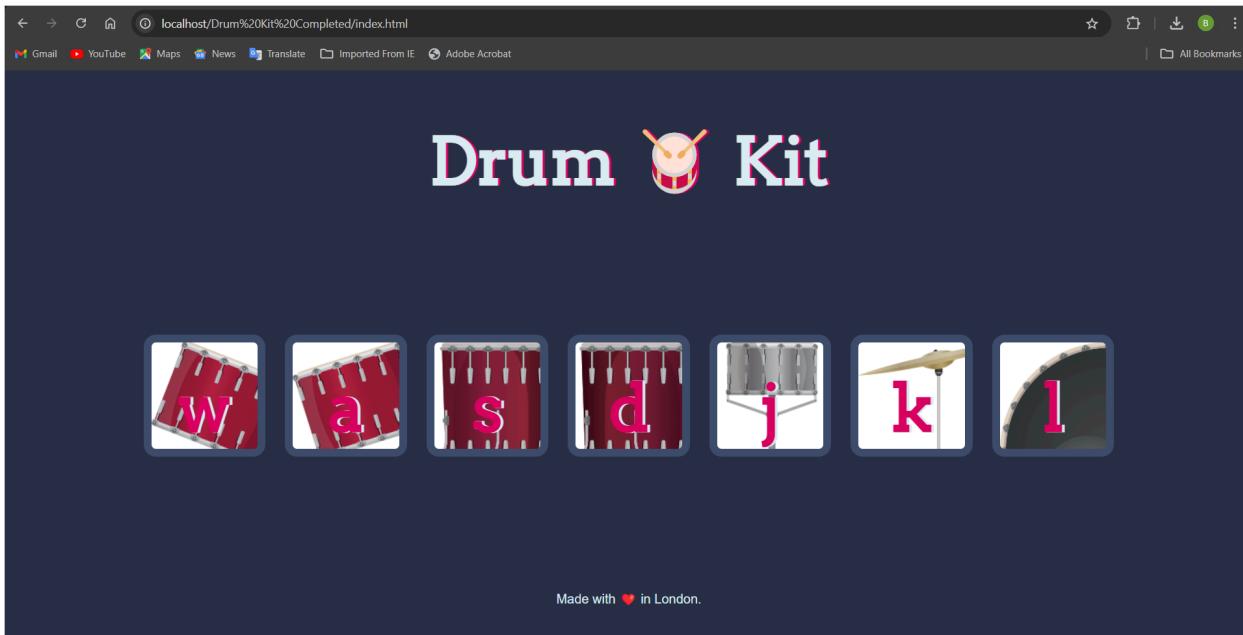
10) Now go to the xampp control panel in the xampp folder.

xampp_start	30-03-2013 17:59	Application	116 KB
xampp_stop	30-03-2013 17:59	Application	116 KB
xampp-control	06-04-2021 17:08	Application	3,290 KB
xampp-control	01-08-2024 21:45	Configuration setti...	1 KB

11) Start the Apache server.

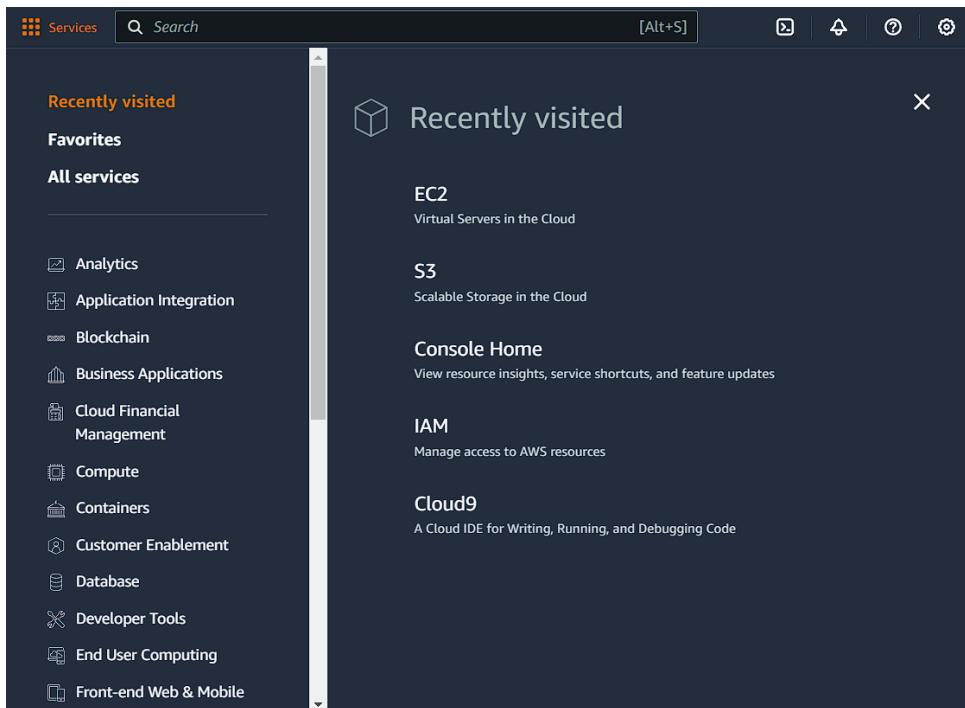


12) After strating the service, got to “localhost/file_name”, then the output window will appear.

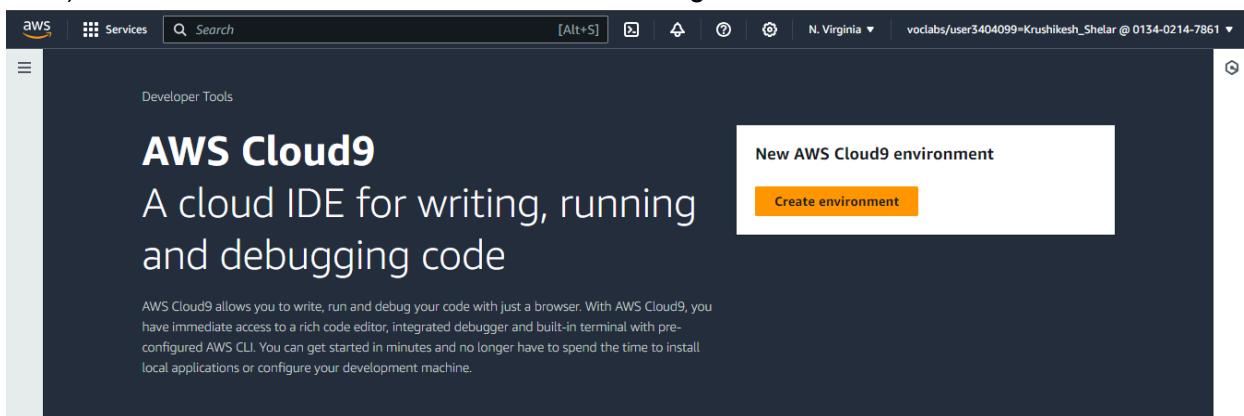


AIM: Setup Cloud 9 - IDE and perform collaboration demonstration.

- 1) Navigate to developer tools -> Cloud9 and start creating Cloud9 environment.



- 2) Click on Create Environment and start creating the environment



3) Name the environment and select new EC2 instance.

Create environment [Info](#)

Details

Name
Limit of 60 characters, alphanumeric and unique per user.

Description – optional
Limit 200 characters.

Environment type [Info](#)
Determines what the Cloud9 IDE will run on.

New EC2 instance
Cloud9 creates an EC2 instance in your account. The configuration of your EC2 instance cannot be changed by Cloud9 after creation.

Existing compute
You have an existing instance or server that you'd like to use.

4) Keep the options default and proceed

New EC2 instance

Instance type [Info](#)
The memory and CPU of the EC2 instance that will be created for Cloud9 to run on.

t2.micro (1 GiB RAM + 1 vCPU)
Free-tier eligible. Ideal for educational users and exploration.

t3.small (2 GiB RAM + 2 vCPU)
Recommended for small web projects.

m5.large (8 GiB RAM + 2 vCPU)
Recommended for production and most general-purpose development.

Additional instance types
Explore additional instances to fit your need.

Platform [Info](#)
This will be installed on your EC2 instance. We recommend Amazon Linux 2023.

Amazon Linux 2023

Timeout
How long Cloud9 can be inactive (no user input) before auto-hibernating. This helps prevent unnecessary charges.
30 minutes

Network settings [Info](#)

Connection
How your environment is accessed.

AWS Systems Manager (SSM)
Accesses environment via SSM without opening inbound ports (no ingress).

Secure Shell (SSH)
Accesses environment directly via SSH, opens inbound ports.

► VPC settings [Info](#)

5) Environment created successfully.

The screenshot shows two windows related to AWS Cloud9. The top window is titled 'AWS Cloud9' and displays the 'Environments' list. It shows one environment named 'D15C48' which is an 'EC2 instance' with 'Secure Shell (SSH)' connection type, owned by the user, and has the ARN 'arn:aws:sts::787881940593:assumed-role/vocabs/user3394024-SHARMA_BRUJESH_RAJARAM'. The bottom window is the 'Cloud9 | us-east-1' interface, showing the 'Welcome' screen of the AWS Cloud9 IDE. It includes sections for 'Getting started' (with options to 'Create File', 'Upload Files...', and 'Clone from GitHub'), a file tree showing 'D15C48 - /home/v', and a terminal window showing the command 'vocabs:~/environment \$'. The system tray at the bottom indicates it's 02-08-2024, 10:15 AM, ENG IN, with a weather icon showing 28°C and 'Mostly cloudy'.

6) Create user using the IAM.

The screenshot shows the AWS IAM 'Users' page. At the top, there is a search bar and a 'Create user' button. Below the search bar, there are filters for 'User name', 'Path', 'Group', 'Last activity', 'MFA', 'Password age', and 'Console last sign-in'. A message 'No resources to display' is centered on the page.

7) Add the username

Specify user details

User details

User name
rushi
The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)

Provide user access to the AWS Management Console - optional
If you're providing console access to a person, it's a [best practice](#) to manage their access in IAM Identity Center.

Info: If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after you create this IAM user. [Learn more](#)

8) Add the remaining user details and provide access to the AWS Management Console

User details

User name
Brij@aws
The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)

Provide user access to the AWS Management Console - optional
If you're providing console access to a person, it's a [best practice](#) to manage their access in IAM Identity Center.

Console password

Autogenerated password
You can view the password after you create the user.

Custom password
Enter a custom password for the user.

• Must be at least 8 characters long
• Must include at least three of the following mix of character types: uppercase letters (A-Z), lowercase letters (a-z), numbers (0-9), and symbols ! @ # \$ % ^ & * () _ + - (hyphen) = [] { } []

Show password

Users must create a new password at next sign-in - Recommended
Users automatically get the [IAMUserChangePassword](#) policy to allow them to change their own password.

Info: If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after you create this IAM user. [Learn more](#)

9) User created successfully and can be added to user groups.

Set permissions

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. [Learn more](#)

Permissions options

Add user to group

Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.

Copy permissions

Copy all group memberships, attached managed policies, and inline policies from an existing user.

Attach policies directly

Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.



Get started with groups

Create a group and select policies to attach to the group. We recommend using groups to manage user permissions by job function, AWS service access, or custom permissions. [Learn more](#)

[Create group](#)

► Set permissions boundary - *optional*

[Cancel](#)

[Previous](#)

[Next](#)

10) User credentials can be downloaded.

Retrieve password

You can view and download the user's password below or email users instructions for signing in to the AWS Management Console. This is the only time you can view and download this password.

Console sign-in details

[Email sign-in instructions](#)

Console sign-in URL

<https://017820672175.signin.aws.amazon.com/console>

User name

Brij@aws

Console password

***** [Show](#)

[Cancel](#)

[Download .csv file](#)

[Return to users list](#)

11) Add user to group if group exists else create a new group.

AWSGroup1 user group created.

[IAM](#) > [Users](#) > [Create user](#)

Step 1

[Specify user details](#)

Step 2

[Set permissions](#)

Step 3

[Review and create](#)

Step 4

[Retrieve password](#)

Set permissions

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. [Learn more](#)

Permissions options

Add user to group

Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.

Copy permissions

Copy all group memberships, attached managed policies, and inline policies from an existing user.

Attach policies directly

Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

12) Write the user group name and proceed.

The screenshot shows the 'User groups' page in the AWS IAM console. It displays one user group named 'AWSGroup1'. The group has 0 users attached and was created on 2024-08-09. Below the table, there is a section titled 'Set permissions boundary - optional' with a 'Next' button at the bottom right.

Group name	Users	Attached policies	Created
AWSGroup1	0	-	2024-08-09 ()

13) Click on *group_name*.

The screenshot shows the 'User groups' page in the AWS IAM console, focusing on the 'AWSGroup1' group. The group has 0 users and no attached policies. It was created 4 minutes ago. The 'Permissions' column shows a warning icon indicating 'Not defined'.

14) Go to Add permissions and click on Add Permissions

The screenshot shows the 'AWSGroup1' permissions page. The 'Permissions' tab is selected. There are 0 managed policies attached. A search bar and filter for 'All types' are present. The table below shows no resources to display.

Policy name	Type	Attached entities
No resources to display		

15) On attach policies, select AWSCloud9EnvironmentMember and click on Attach policies.

The screenshot shows the 'Add permissions' page for the user group 'AWSGroup1'. In the 'Other permission policies' section, the policy 'AWSCloud9EnvironmentMember' is selected. At the bottom right, the 'Attach policies' button is highlighted in orange.

Policy name	Type	Used as	Description
AWSCloud9Administrator	AWS managed	None	Provides administrator access to AWS Clo...
AWSCloud9EnvironmentMember	AWS managed	None	Provides the ability to be invited into AW...
AWSCloud9SSMInstanceProfile	AWS managed	None	This policy will be used to attach a role o...
AWSCloud9User	AWS managed	None	Provides permission to create AWS Cloud...

16) User group is created successfully.

The screenshot shows the 'AWSGroup1' details page. The 'Permissions' tab is selected, showing one attached policy: 'AWSCloud9EnvironmentMember'. The ARN of the group is listed as 'arn:aws:iam::017820672175:group/AWSGroup1'.

Policy name	Type	Attached entities
AWSCloud9EnvironmentMember	AWS managed	1