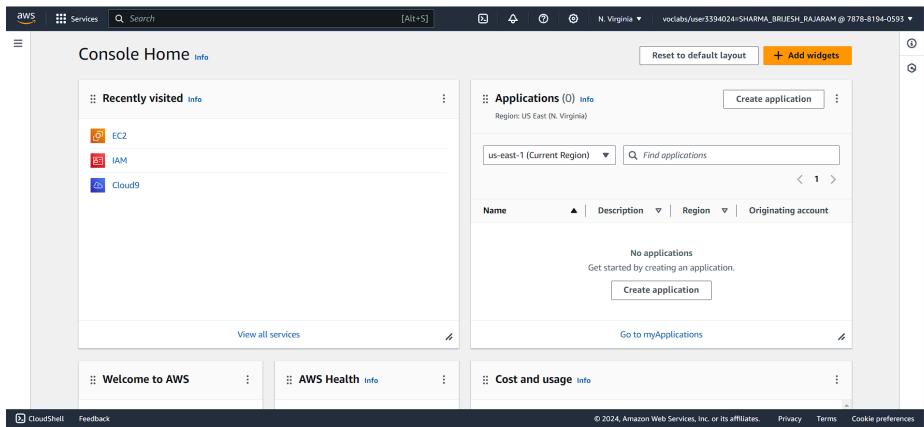


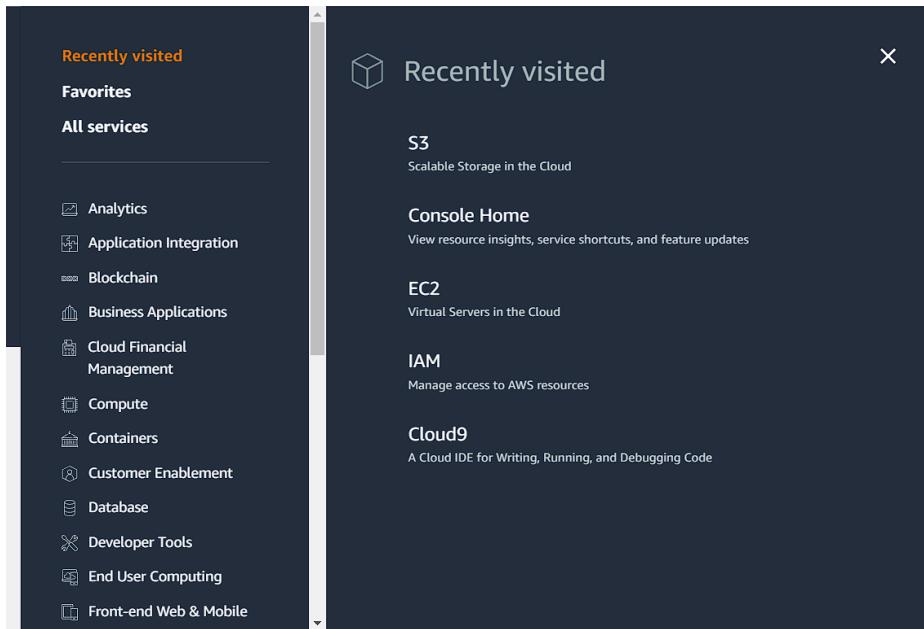
Hosting a static website on Amazon Web Services (S3)

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 'Reset to default layout' button and an 'Add widgets' button. It displays the 'Applications' section with a 'Create application' button. Below it is the 'us-east-1 (Current Region)' dropdown and a search bar. A table lists applications by Name, Description, Region, and Originating account. A note says 'No applications' and 'Get started by creating an application.' with another 'Create application' button. At the bottom, there are links to 'View all services', 'Go to myApplications', and navigation icons.

2) Navigate to the S3 to host the website



The screenshot shows the AWS Console sidebar. Under 'All services', 'S3' is selected and highlighted in orange. Other services listed include Analytics, Application Integration, Blockchain, Business Applications, Cloud Financial Management, Compute, Containers, Customer Enablement, Database, Developer Tools, End User Computing, and Front-end Web & Mobile. The main content area shows a 'Recently visited' section with cards for S3 (Scalable Storage in the Cloud), EC2 (Virtual Servers in the Cloud), IAM (Manage access to AWS resources), and Cloud9 (A Cloud IDE for Writing, Running, and Debugging Code). There is also a 'Console Home' card.

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.

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](#)
piyushbucket

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 disable 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

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 [DSS-E-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

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, there's an "Account snapshot" section with a link to "View details". The main area shows two tabs: "General purpose buckets" (selected) and "Directory buckets". Under "General purpose buckets", there's a table with one row for "brijeshkabucket". The table columns include Name, AWS Region, IAM Access Analyzer, and Creation date. The bucket name "brijeshkabucket" is highlighted in blue. A "Create bucket" button is visible at the top right of the table area.

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

The screenshot shows the "brijeshkabucket" bucket details page. The "Objects" tab is selected. At the top, there's a table header with columns: Name, Type, Last modified, Size, and Storage class. Below the header, a message states "No objects" and "You don't have any objects in this bucket.". There is a prominent "Upload" button at the bottom of the table area.

- 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. It includes a note about public access being granted through ACLs, bucket policies, and access point policies. A "Edit" button is at the top right. Below, there's a section for "Block all public access" with a "On" toggle switch. A link "Individual Block Public Access settings for this bucket" is also present.

- 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.

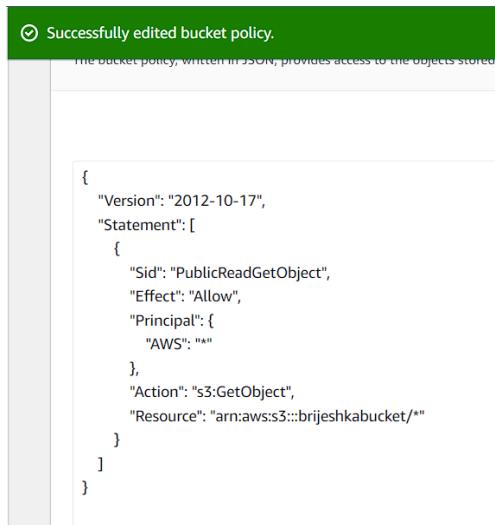
- 11) Fill the following policy in the empty policy space. Ensure that you change the name of the bucket in Resource with the name of your bucket.

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 }
```

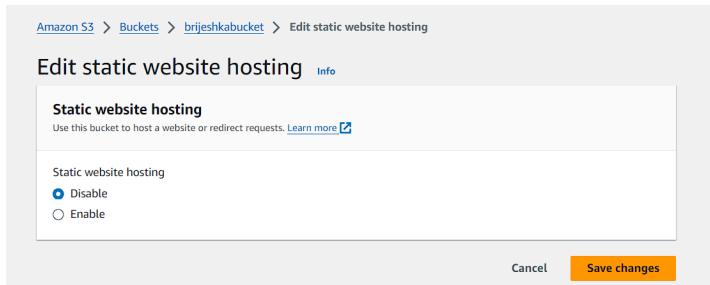
12) After saving the changes, you will see a message.



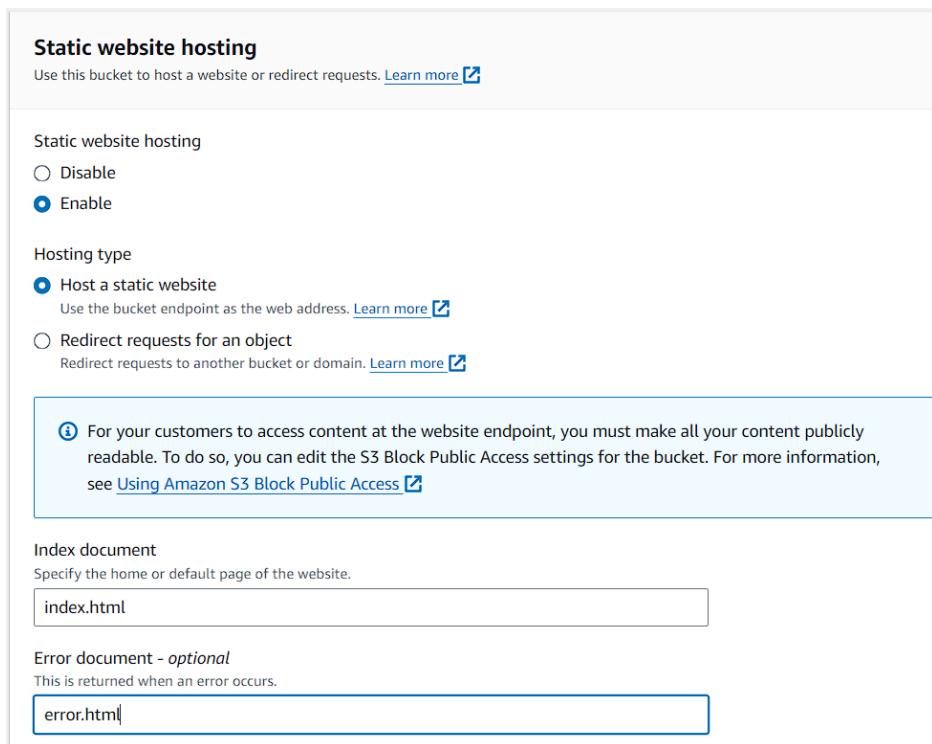
The screenshot shows a green success message at the top: "Successfully edited bucket policy." Below it is a JSON representation of the bucket policy:

```
{ "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" (with "Enable" selected), "Hosting type" (with "Host a static website" selected), and "Index document" (set to "index.html"). A note at the bottom explains that content must be publicly readable. There is also an "Error document - optional" field set to "error.html".

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](#)

Index document
Specify the home or default page of the website.
index.html

Error document - optional
This is returned when an error occurs.
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, the navigation path is: Amazon S3 > Buckets > brijeshkabucket > Upload. Below this, the title 'Upload' has a 'Info' link. A large text area with a dashed border contains the placeholder '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 one row: 'All files and folders in this table will be uploaded.' It includes search and pagination controls ('Find by name', '< 1 >'). The main table body displays a message: 'No files or folders' and 'You have not chosen any files or folders to upload.'

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

The screenshot shows the 'Files and folders' list for the uploaded files. The title is 'Files and folders (2 Total, 906.0 B)'. It includes search and pagination controls ('Find by name', '< 1 >'). The table lists two files: 'error.html' and 'index.html', both of which are 'text/html' type files.

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

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

The screenshot shows the 'Static website hosting' properties tab. It includes sections for 'Static website hosting' (with a note: 'Use this bucket to host a website or redirect requests. Learn more'), 'Edit' button, 'Enabled' status, 'Hosting type' (Bucket hosting), and 'Bucket website endpoint' (with a note: 'When you configure your bucket as a static website, the website is available at the AWS Region-specific website endpoint of the bucket. Learn more') with the URL 'http://brijeshkabucket.s3-website-us-east-1.amazonaws.com'.

18) The hosted website using AWS S3.

VESIT_Batch6_Koma... VESIT-Ganit App Int... Home IoE Theory- D208-V...

Hello

My first AWS Deployment

Made with ❤

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 header with 'General purpose buckets (1)' and buttons for 'Info', 'All AWS Regions', 'Copy ARN', 'Empty', 'Delete', and 'Create bucket'. Below this, a search bar says 'Find buckets by name' with a value of 'brijeshkabucket'. A table lists one bucket: 'brijeshkabucket' in 'US East (N. Virginia)' region, created on 'August 7, 2024, 20:38:57 (UTC+05:30)'. A green notification bar at the bottom states 'Successfully emptied bucket "brijeshkabucket"' with a link to 'View details below'. Below the table, a modal window titled 'Empty bucket: status' shows a summary: 'Source s3://brijeshkabucket' with 'Successfully deleted 2 objects, 906.0 B' and 'Failed to delete 0 objects'. A second section titled 'Failed to delete (0)' shows a table with no data, stating 'No failed object deletions'.

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

The screenshot shows the 'Delete bucket' confirmation dialog. At the top, the breadcrumb navigation is: Amazon S3 > Buckets > brijeshkabucket > Delete bucket. Below this is the title 'Delete bucket' with an 'Info' link. A warning box contains the following text:

⚠ • 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](#)

The main area is titled 'Delete bucket "brijeshkabucket"?' and contains the instruction: 'To confirm deletion, enter the name of the bucket in the text input field.' A text input field contains the value 'brijeshkabucket'. At the bottom right are 'Cancel' and 'Delete bucket' buttons.

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

The screenshot shows the Amazon S3 home page. A green header bar displays the message 'Successfully deleted bucket "brijeshkabucket"'. The main content area features the heading 'Amazon S3' and the subtext 'Store and retrieve any amount of data from anywhere'. It includes a brief description of S3 and a 'Create a bucket' button. On the left, there's a 'How it works' section with a video thumbnail titled 'Introduction to Amazon S3' and a 'Copy link' button. On the right, there's a 'Pricing' section stating that there are no minimum fees and providing a link to the Simple Monthly Calculator. The overall theme is dark with blue and white text.

XAMPP Hosting

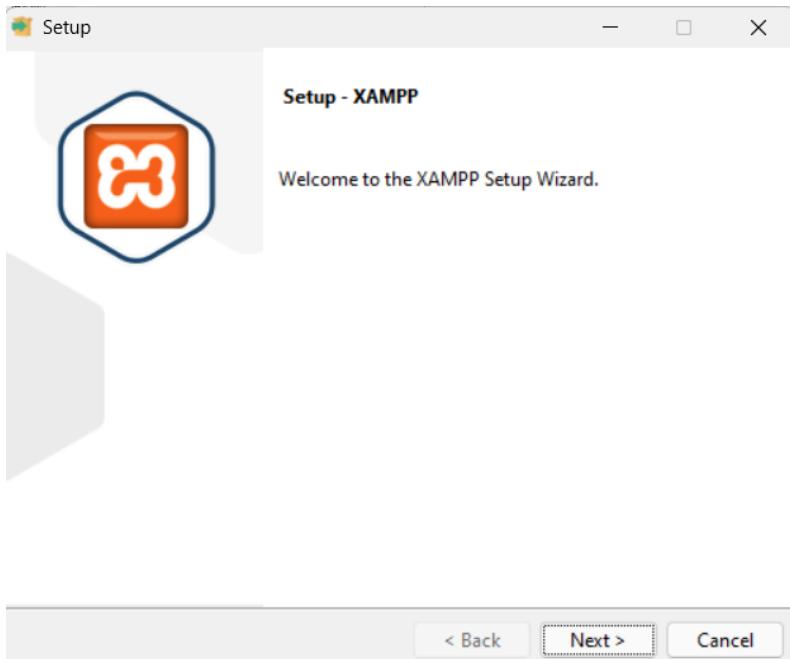
- 1) Search for XAMPP download and navigate to the xampp official website and click on download as per your system.

The screenshot shows the Apache Friends website's download section. At the top, there's a navigation bar with links for Apache Friends, Download, Hosting, Community, and About. A search bar and a language selector (EN) are also present. The main heading is "Download". Below it, a sub-headline reads: "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." To the right, there's a "Documentation/FAQs" sidebar with text about the lack of a manual and links to forums and Stack Overflow. The central part of the page displays a table of XAMPP versions for Windows:

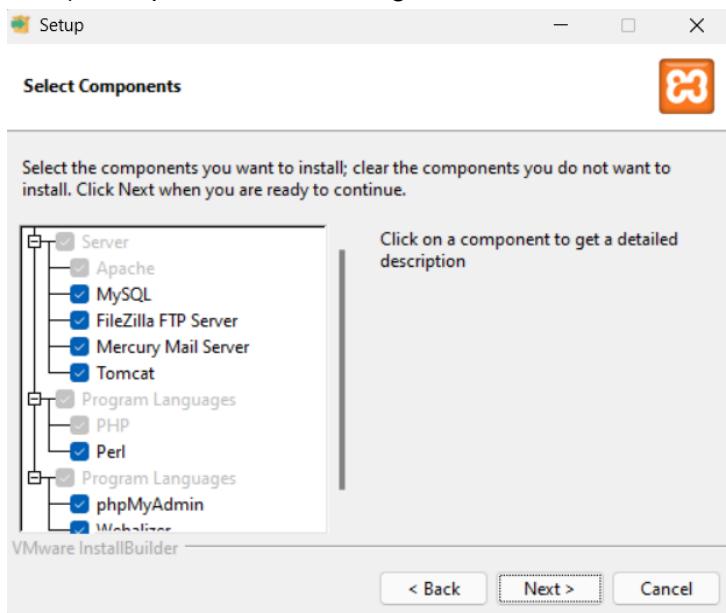
Version	Checksum	Size
8.0.30 / PHP 8.0.30	What's Included? md5 sha1	Download (64 bit) 144 Mb
8.1.25 / PHP 8.1.25	What's Included? md5 sha1	Download (64 bit) 148 Mb
8.2.12 / PHP 8.2.12	What's Included? md5 sha1	Download (64 bit) 149 Mb

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."

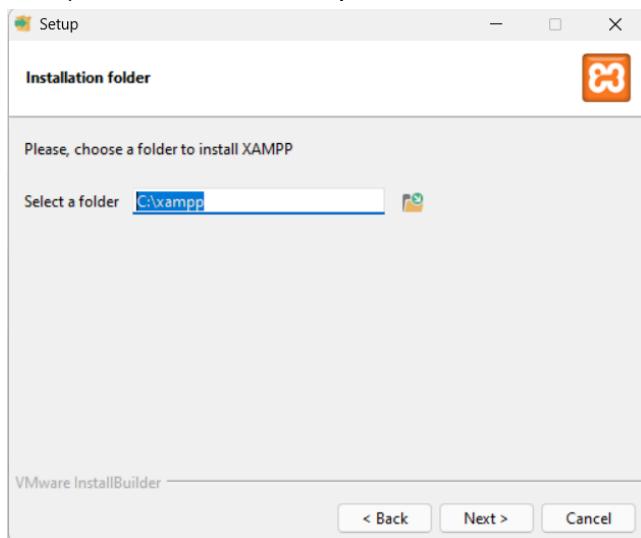
- 2) Xampp installer will be installed in the system.
- 3) Window asking to give permission will appear. Click pn 'Yes'.
- 4) A window will appear for setup. Click on 'Next'.



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.



```
<html>
<head>
    <title>First PHP Program</title>
</head>
<body>
    <center>
        <?php
echo "PHP website hosted using Xampp";
?>

        <font style="font-size:x-large;font-family:'Segoe UI', Tahoma, Geneva, Verdana, sans-serif"><h1>Hello</h1></font>
        <font color="blue" style="font-family:Georgia, 'Times New Roman', Times, serif;"><h2>My first Xampp Deployment</h2></font>
        <h3>Made with <font style="color: red;">&#10084;</font></h3>
    </center>
</center>
</body>
</html>

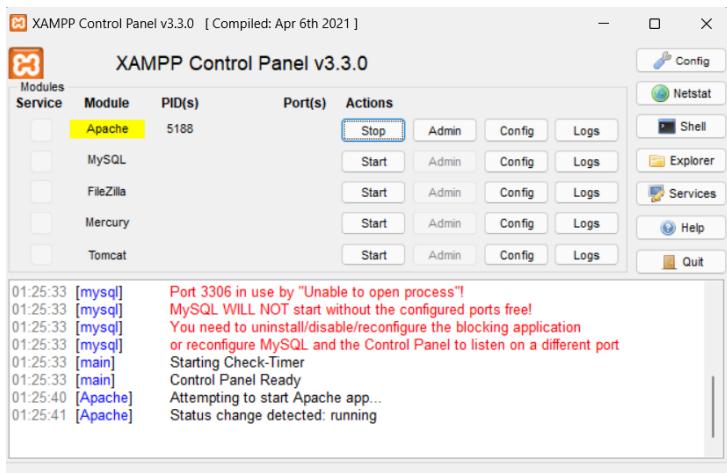
<!-- store in this file whatever to be displayed and then localhost/MicroNG/file_name --&gt;</pre>
```

Ln 1, Col 1 | 575 characters | 100% | Windows (CRL) | UTF-8

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

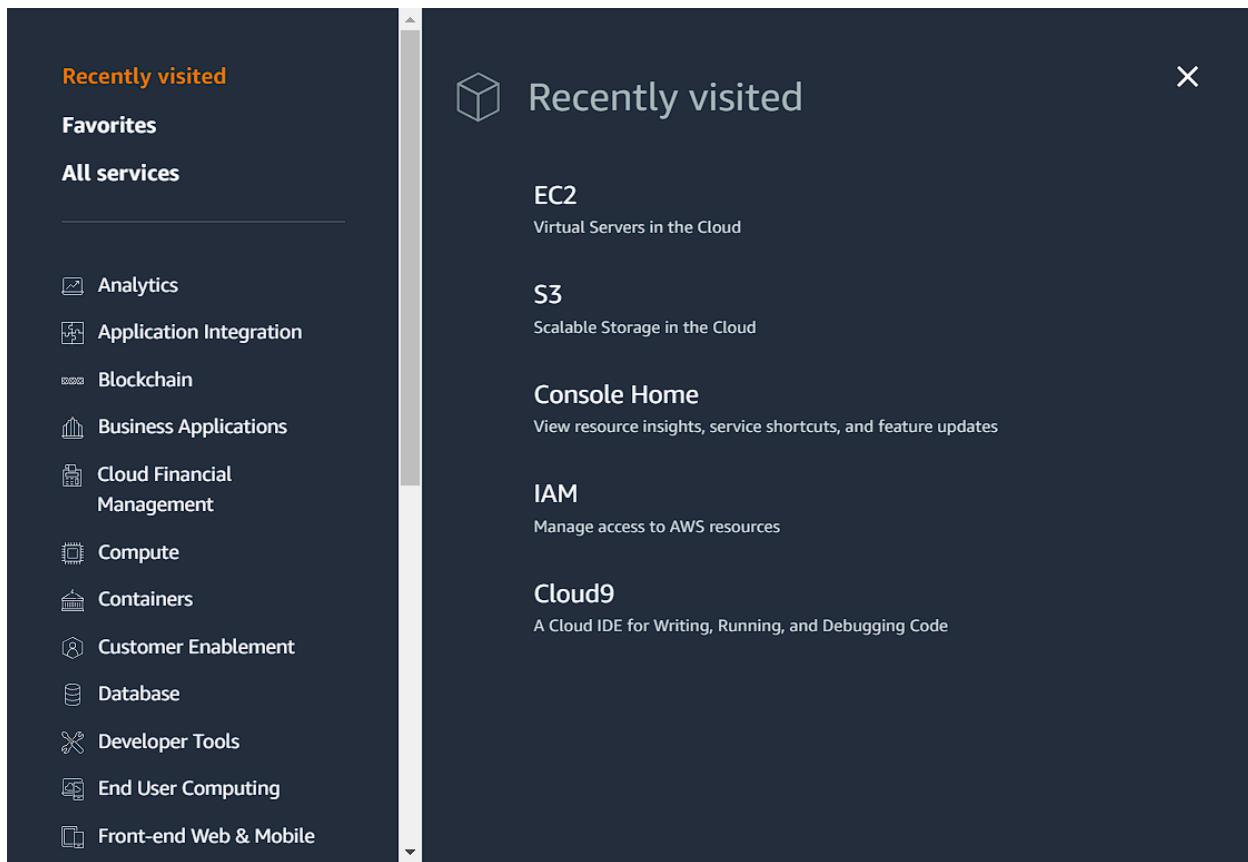
11) Start the Apache server.



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



EC2 Instance



Launch instance

To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

[Launch instance](#)



[Migrate a server](#)

Note: Your instances will launch in the US East (N. Virginia) Region

Launch an instance Info

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags Info

Name

[Add additional tags](#)

▼ Application and OS Images (Amazon Machine Image) Info

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below



Search our full catalog including 1000s of application and OS images

[Recents](#)[Quick Start](#)[Browse more AMIs](#)

Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Ubuntu Server 24.04 LTS (HVM), SSD Volume Type

Free tier eligible

ami-04a81a99f5ec58529 (64-bit (x86)) / ami-0c14ff330901e49ff (64-bit (Arm))

Virtualization: hvm ENA enabled: true Root device type: ebs

Description

Ubuntu Server 24.04 LTS (HVM), EBS General Purpose (SSD) Volume Type. Support available from Canonical (<http://www.ubuntu.com/cloud/services>).

Architecture

64-bit (x86)

AMI ID

ami-04a81a99f5ec58529

Verified provider

▼ Instance type [Info](#) | [Get advice](#)

Instance type

t2.micro

Free tier eligible

Family: t2 1 vCPU 1 GiB Memory Current generation: true
On-Demand Windows base pricing: 0.0162 USD per Hour
On-Demand SUSE base pricing: 0.0116 USD per Hour
On-Demand RHEL base pricing: 0.026 USD per Hour
On-Demand Linux base pricing: 0.0116 USD per Hour

All generations

[Compare instance types](#)

Additional costs apply for AMIs with pre-installed software

▼ Key pair (login) [Info](#)

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - *required*

vockey

 [Create new key pair](#)

▼ Network settings [Info](#)

Edit

Network | [Info](#)

vpc-0531204c9e29f6332

Subnet | [Info](#)

No preference (Default subnet in any availability zone)

Auto-assign public IP | [Info](#)

Enable

[Additional charges apply](#) when outside of [free tier allowance](#)

Firewall (security groups) | [Info](#)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

Create security group

Select existing security group

We'll create a new security group called '**launch-wizard-2**' with the following rules:

Allow SSH traffic from
Helps you connect to your instance

Anywhere
0.0.0.0/0

Allow HTTPS traffic from the internet
To set up an endpoint, for example when creating a web server

Allow HTTP traffic from the internet
To set up an endpoint, for example when creating a web server

⚠ Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

X

▼ Configure storage [Info](#)

[Advanced](#)

1x GiB ▾ Root volume (Not encrypted)

 Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage X

[Add new volume](#)

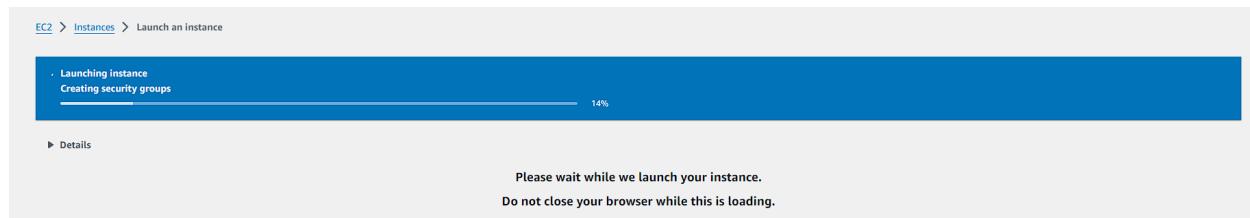
The selected AMI contains more instance store volumes than the instance allows. Only the first 0 instance store volumes from the AMI will be accessible from the instance

 Click refresh to view backup information



The tags that you assign determine whether the instance will be backed up by any Data Lifecycle Manager policies.

0 x File systems

[Edit](#)

Connect to instance Info

Connect to your instance i-033e8bf30d3d5ed91 (AWS Test Server) using any of these options

[EC2 Instance Connect](#)

[Session Manager](#)

[SSH client](#)

[EC2 serial console](#)



Port 22 (SSH) is open to all IPv4 addresses

Port 22 (SSH) is currently open to all IPv4 addresses, indicated by **0.0.0.0/0** in the inbound rule in [your security group](#). For increased security, consider restricting access to only the EC2 Instance Connect service IP addresses for your Region: 18.206.107.24/29. [Learn more](#).

Instance ID

[i-033e8bf30d3d5ed91 \(AWS Test Server\)](#)

Connection Type

[Connect using EC2 Instance Connect](#)

Connect using the EC2 Instance Connect browser-based client, with a public IPv4 address.

[Connect using EC2 Instance Connect Endpoint](#)

Connect using the EC2 Instance Connect browser-based client, with a private IPv4 address and a VPC endpoint.

Public IP address

[35.171.89.89](#)

Username

Enter the username defined in the AMI used to launch the instance. If you didn't define a custom username, use the default username, `ubuntu`.

`ubuntu` X



Note: In most cases, the default username, `ubuntu`, is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI username.



You have insufficient IAM permissions to connect to an instance using EC2 Instance Connect

To connect to an instance via EC2 Instance Connect, you must have an attached IAM policy that grants the following permissions:

- `ec2-instance-connect:SendSSHPublicKey`
- `ec2:DescribeInstances`

Consider restricting access to specific EC2 instances using `ec2:osuser` condition, or specific resource tag. Visit [IAM Console](#) to verify if you have above permissions.

For more information about IAM policy examples, see [Grant IAM permissions for EC2 Instance Connect](#).

[Cancel](#)

[Connect](#)

AWS | Services | Search [Alt+S] | N. Virginia | vclabs/user3394024=SHARMA_BRUJESH_RAJARAM @ 7878-8194-05

```

Usage of /: 22.7% of 6.71GB Users logged in: 0
Memory usage: 20% IPv4 address for enx0: 172.31.38.111
Swap usage: 0%

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-172-31-38-111:~$ i-033e8bf30d3d5ed91 (AWS Test Server)
PublicIPs: 35.171.89.89 PrivateIPs: 172.31.38.111

```

```

ubuntu@ip-172-31-38-111:~$ ping www.google.com
PING www.google.com (142.251.167.106) 56(84) bytes of data.
64 bytes from ww-in-f106.1e100.net (142.251.167.106): icmp_seq=1 ttl=58 time=2.22 ms
64 bytes from ww-in-f106.1e100.net (142.251.167.106): icmp_seq=2 ttl=58 time=2.24 ms
64 bytes from ww-in-f106.1e100.net (142.251.167.106): icmp_seq=3 ttl=58 time=2.26 ms
64 bytes from ww-in-f106.1e100.net (142.251.167.106): icmp_seq=4 ttl=58 time=2.38 ms
64 bytes from ww-in-f106.1e100.net (142.251.167.106): icmp_seq=5 ttl=58 time=2.31 ms
64 bytes from ww-in-f106.1e100.net (142.251.167.106): icmp_seq=6 ttl=58 time=2.26 ms
^C
--- www.google.com ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5007ms
rtt min/avg/max/mdev = 2.220/2.276/2.376/0.052 ms
ubuntu@ip-172-31-38-111:~$ vmstat
procs -----memory----- ---swap-- -----io---- -system-- -----cpu-----
  r   b   swpd   free   buff   cache   si   so   bi   bo   in   cs   us   sy   id   wa   st   gu
  2   0     0 504660 18052 288972     0     0   381   298   141     1   2   1 95   1   2   0
ubuntu@ip-172-31-38-111:~$ df
Filesystem      1K-blocks      Used Available Use% Mounted on
/dev/root        7034376  1609612    5408380  23% /
tmpfs            490212       0    490212   0% /dev/shm
tmpfs            196088      868    195220   1% /run
tmpfs             5120       0      5120   0% /run/lock
/dev/xvda16       901520    76972    761420  10% /boot
/dev/xvda15       106832     6246   100586   6% /boot/efi
tmpfs            98040       12    98028   1% /run/user/1000
ubuntu@ip-172-31-38-111:~$ mkdir test
ubuntu@ip-172-31-38-111:~$ touch e.txt
ubuntu@ip-172-31-38-111:~$ ls
e.txt  test
ubuntu@ip-172-31-38-111:~$ history
  1  ping
  2  ping www.google.com
  3  vmstat
  4  df
  5  mkdir test
  6  touch e.txt
  7  ls
  8  history

```

Instances (1) [Info](#)

Find Instance by attribute or tag (case-sensitive)

All states ▾

Instance ID = i-033e8bf30d3d5ed91 X Clear filters

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IP
AWS Test Server	i-033e8bf30d3d5ed91	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1b	ec2-35-

Instances (1/1) [Info](#)

Find Instance by attribute or tag (case-sensitive)

All states ▾

Instance ID = i-033e8bf30d3d5ed91 X Clear filters

Name	Instance ID	Instance state	Instance type	Status	Alarm	Availability Zone	Public IP
AWS Test Server	i-033e8bf30d3d5ed91	Running	t2.micro	Green	View alarms +	us-east-1b	ec2-35-

Terminate instance?

⚠ On an EBS-backed instance, the default action is for the root EBS volume to be deleted when the instance is terminated. Storage on any local drives will be lost.

Are you sure you want to terminate these instances?

Instance ID	Termination protection
i-033e8bf30d3d5ed91 (AWS Test Server)	Disabled

To confirm that you want to terminate the instances, choose the terminate button below. Instances with termination protection enabled will not be terminated. Terminating the instance cannot be undone.

[Cancel](#)

[Terminate](#)

Instances (1) [Info](#)

Find Instance by attribute or tag (case-sensitive)

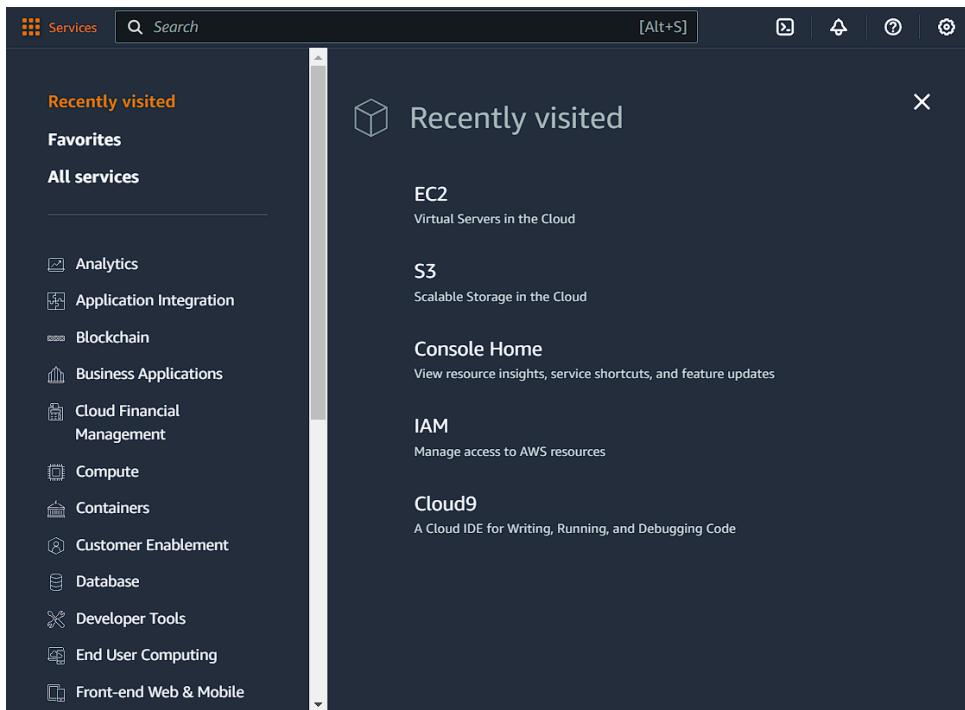
All states ▾

Instance ID = i-033e8bf30d3d5ed91 X Clear filters

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IP
AWS Test Server	i-033e8bf30d3d5ed91	Terminated	t2.micro	-	View alarms +	us-east-1b	-

Cloud 9 - IDE

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



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

A screenshot of the AWS Cloud9 landing page. The page title is 'AWS Cloud9' and the subtitle is 'A cloud IDE for writing, running, and debugging code'. Below the title, there is a brief description of what AWS Cloud9 is and how it works. On the right side, there is a call-to-action box with the heading 'New AWS Cloud9 environment' and a large orange 'Create environment' button. At the bottom of the page, there are two sections: 'How it works' and 'Getting started'. The 'How it works' section contains a brief description of the service. The 'Getting started' section has four links: 'Before you start (2 min read)', 'Create an environment (2 min read)', 'Working with environments (15 min read)', and 'Working with the IDE (10 min read)'. The background shows the AWS navigation bar at the top.

3) Name the environment and select new EC2 instance.

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 a dual-monitor setup. The top monitor displays the AWS Management Console with the Cloud9 service selected. A modal window titled "Creating D15C48. This can take several minutes. While you wait, see Best practices for using AWS Cloud9." is open, indicating the environment is being created. Below it, the "Environments" list shows one entry: "D15C48" (Open), which is an EC2 instance type with Secure Shell (SSH) connection, owned by the user, and associated with the ARN "arn:aws:sts:787881940593:assumed-role/vocabs/user3394024-SHARMA_BRUJESH_RAJARAM". The bottom monitor displays the AWS Cloud9 IDE interface. The left sidebar shows the file structure: ". / D15C48 - /home/vocabs". The main area shows the "Welcome" screen with the title "AWS Cloud9" and the sub-headline "Welcome to your development environment". It includes a "Toolkit for AWS Cloud9" section and a "Getting started" sidebar with options like "Create File", "Upload Files...", and "Clone from GitHub". At the bottom, there's a terminal window showing the command "vocabs:~/environment \$". The taskbar at the bottom of both monitors shows various application icons and system status.

6) Create user using the IAM.

The screenshot shows the AWS IAM 'Users' page. At the top, there is a header with 'Users (0) info'. Below it, a note says 'An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.' A search bar labeled 'Search' is followed by navigation icons: back, forward, and refresh. A large orange button labeled 'Create user' is prominently displayed. Below these, there is a table header with columns: 'User name', 'Path', 'Group', 'Last activity', 'MFA', 'Password age', and 'Console last sign-in'. The main content area below the table header displays the message 'No resources to display'.

7) Add the username

The screenshot shows the 'Specify user details' step of the IAM user creation wizard. The title is 'Specify user details'. Under 'User details', the 'User name' field contains 'Brij@aws'. A note below it states: 'The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = . @ _ - (hyphen)' and includes a link to 'Learn more'. There is an optional checkbox 'Provide user access to the AWS Management Console - optional' with a note: 'If you're providing console access to a person, it's a best practice to manage their access in IAM Identity Center.' A blue callout box contains the note: 'If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keypairs, 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

The screenshot shows the 'Add remaining user details' step of the IAM user creation wizard. The title is 'User details'. The 'User name' field is filled with 'Brij@aws'. An optional checkbox 'Provide user access to the AWS Management Console - optional' is checked, with a note: 'If you're providing console access to a person, it's a best practice to manage their access in IAM Identity Center.' Under 'Console password', there are three options: 'Autogenerated password' (unchecked), 'Custom password' (checked), and 'Show password' (unchecked). The 'Custom password' field contains '*****'. A note below it specifies: '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) = [] { } ; , . / ? '.

A checked checkbox 'Users must create a new password at next sign-in - Recommended' has a note: 'Users automatically get the IAMUserChangePassword policy to allow them to change their own password.'

A blue callout box contains the note: 'If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keypairs, 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.

X

[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 (1)' page in the AWS IAM console. At the top right are 'Create group' and 'Cancel' buttons. Below is a search bar and a table with columns: Group name, Users, Attached policies, and Created. A single row is shown for 'AWSGroup1'. At the bottom is a note about setting a permissions boundary and navigation buttons 'Previous' and 'Next'.

13) Click on *group_name*.

The screenshot shows the 'User groups (1) Info' page. It displays a table with columns: Group name, Users, Permissions, and Creation time. The 'AWSGroup1' row shows 0 users, 'Not defined' permissions, and was created 4 minutes ago. Buttons for 'Delete' and 'Create group' are at the top right.

14) Go to Add permissions and click on Add Permissions

The screenshot shows the 'AWSGroup1 Info' page with the 'Permissions' tab selected. It includes sections for Summary (with Edit button), User group name (AWSGroup1), Creation time (August 09, 2024, 00:07 (UTC+05:30)), and ARN (arn:aws:iam::017820672175:group/AWSGroup1). Below is a table for Permissions policies (0) with columns: Policy name, Type, and Attached entities. A note says 'No resources to display'.

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

The screenshot shows the 'Attach permission policies' dialog for the user group 'AWSGroup1'. At the top, it says 'Attach permission policies to AWSGroup1'. Below that is a section titled 'Current permissions policies (0)'. Underneath is a heading 'Other permission policies (1/945)' with a note: 'You can attach up to 10 managed policies to this user group. All of the users in this group inherit the attached permissions.' A search bar and filter dropdown are present. A table lists four policies:

Policy name	Type	Used as	Description
AWSCloud9Administrator	AWS managed	None	Provides administrator access to AWS Clo...
<input checked="" type="checkbox"/> 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...

At the bottom right are 'Cancel' and 'Attach policies' buttons, with 'Attach policies' being highlighted.

16) User group is created successfully.

The screenshot shows the 'AWSGroup1' details page. At the top, a green bar indicates 'Policies attached to this user group.' Below is the 'Summary' section with fields: 'User group name' (AWSGroup1), 'Creation time' (August 09, 2024, 00:07 (UTC+05:30)), and 'ARN' (arn:aws:iam::017820672175:group/AWSGroup1). Below the summary is a navigation bar with 'Users', 'Permissions' (which is selected), and 'Access Advisor'. The 'Permissions' section shows 'Permissions policies (1)' attached, with a note: 'You can attach up to 10 managed policies.' A table lists the attached policy:

Policy name	Type	Attached entities
<input type="checkbox"/> AWSCloud9EnvironmentMember	AWS managed	1