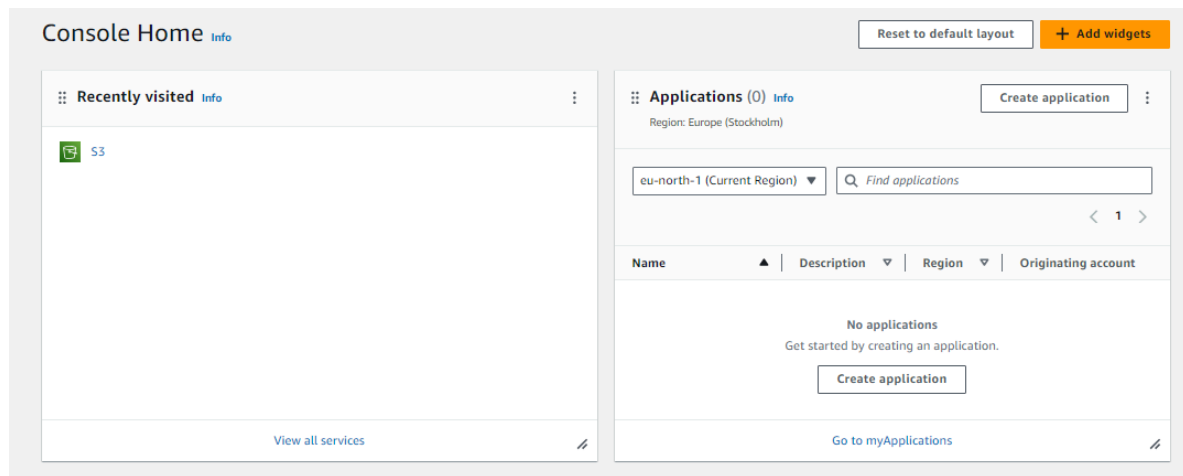
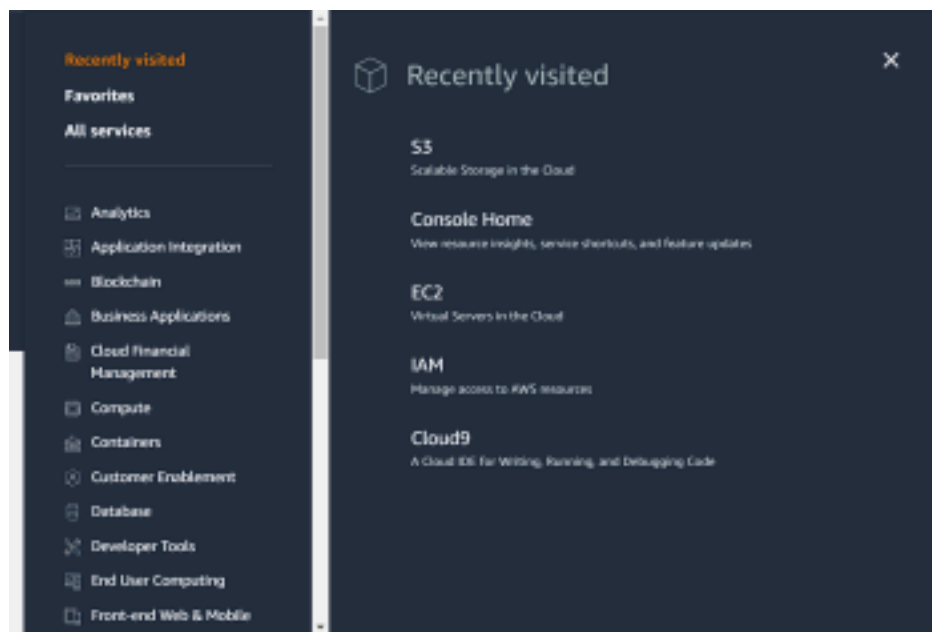


## Hosting a static website on Amazon Web Services (S3)

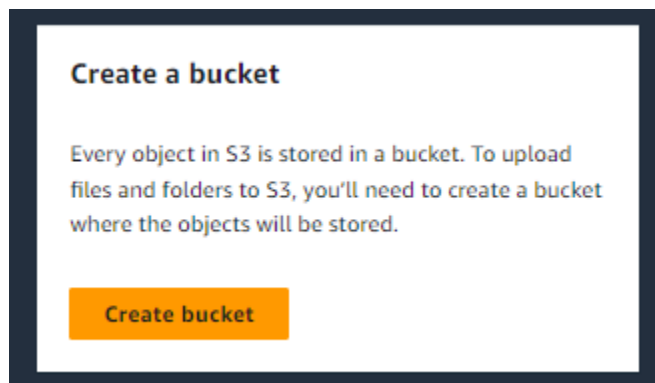
1) Open the AWS console home



2) Navigate to the S3 to host the website



3) On S3, click on create bucket



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

## General configuration

AWS Region  
Europe (Stockholm) eu-north-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.

Format: s3://bucket/prefix

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

### Object Ownership

Enables ownership of objects within the bucket from either the account administrator or another IAM role with the `s3:PutObject` permission.

☒ **ACLs disabled (recommended)**  
 An object's permissions are determined by the bucket's ACL. This is the default and is simpler to manage.

☐ **ACLs enabled**  
 A separate ACL is used to control access to the bucket and its objects. This is more complex to manage.

Object Ownership  
Bucket owner enforced

---

### Make Public Access settings for this bucket

Public access is granted to buckets and objects through several mechanisms. To ensure that your bucket and its objects are secure, you should disable public access. These settings apply only to the bucket and its objects. They do not affect the permissions of the bucket's owner. To learn more about public access, see [Public Access Settings](#).

☒ **Block all public access**  
 Enabling this setting on the bucket will block all public access to the bucket and its objects. This setting is the most restrictive and is recommended for all buckets.

- ☒ **Block public access to buckets and objects granted through new access control lists (ACLs)**  
 To prevent public access to buckets and objects granted through new access control lists (ACLs), you must disable public access to buckets and objects granted through new access control lists (ACLs).
- ☒ **Block public access to buckets and objects granted through new access control lists (ACLs)**  
 To prevent public access to buckets and objects granted through new access control lists (ACLs), you must disable public access to buckets and objects granted through new access control lists (ACLs).
- ☒ **Block public access to buckets and objects granted through new public bucket or access point policies**  
 To prevent public access to buckets and objects granted through new public bucket or access point policies, you must disable public access to buckets and objects granted through new public bucket or access point policies.
- ☒ **Block public and cross-account access to buckets and objects granted through public bucket or access point policies**  
 To prevent public and cross-account access to buckets and objects granted through public bucket or access point policies, you must disable public and cross-account access to buckets and objects granted through public bucket or access point policies.

---

### Bucket Versioning

Versioning is a feature that allows you to store multiple versions of an object in the same bucket. This can be useful for protecting against accidental deletion of objects and for recovering from accidental deletion of objects. For more information, see [Bucket Versioning](#).

Bucket Versioning  
☒ **Disable**  
☐ **Enable**

---

### Tags - optional

You can use bucket tags to track objects and manage buckets. [Learn more](#)

No tags associated with this bucket.

---

### Default encryption

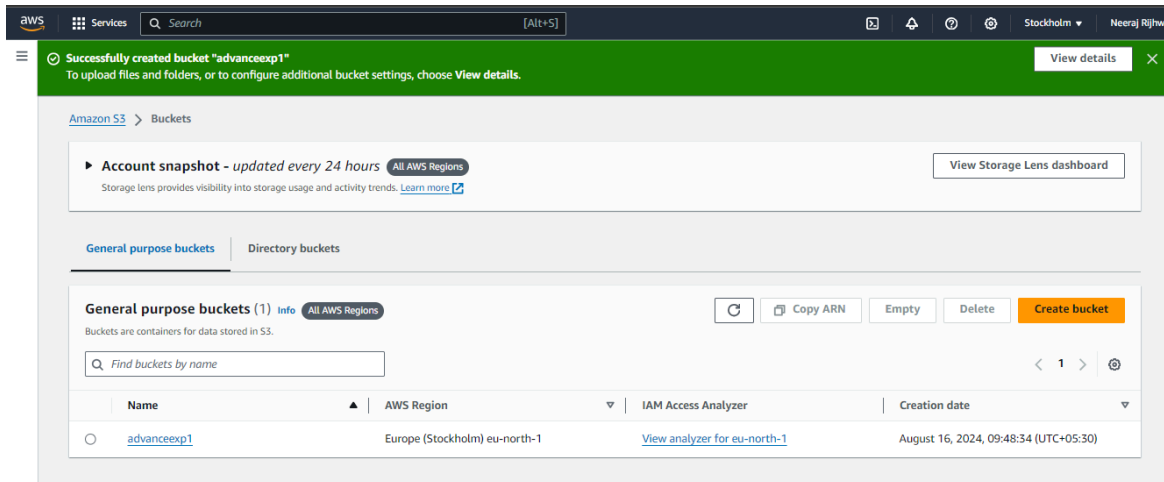
Amazon S3 automatically encrypts objects in the bucket at rest. You can choose the encryption method and key management service (KMS) to use.

Encryption type  
☒ **Server-side encryption with Amazon S3 managed keys (SSE-S3)**  
☐ **Server-side encryption with AWS Key Management Service keys (SSE-KMS)**  
☐ **Client-side encryption with AWS Key Management Service keys (CSE-KMS)**

Bucket Key  
 Enabling this setting on the bucket will enable bucket key for the bucket. This setting is not supported for buckets with `public_access` set to `off`.  
☐ **Disable**  
☒ **Enable**

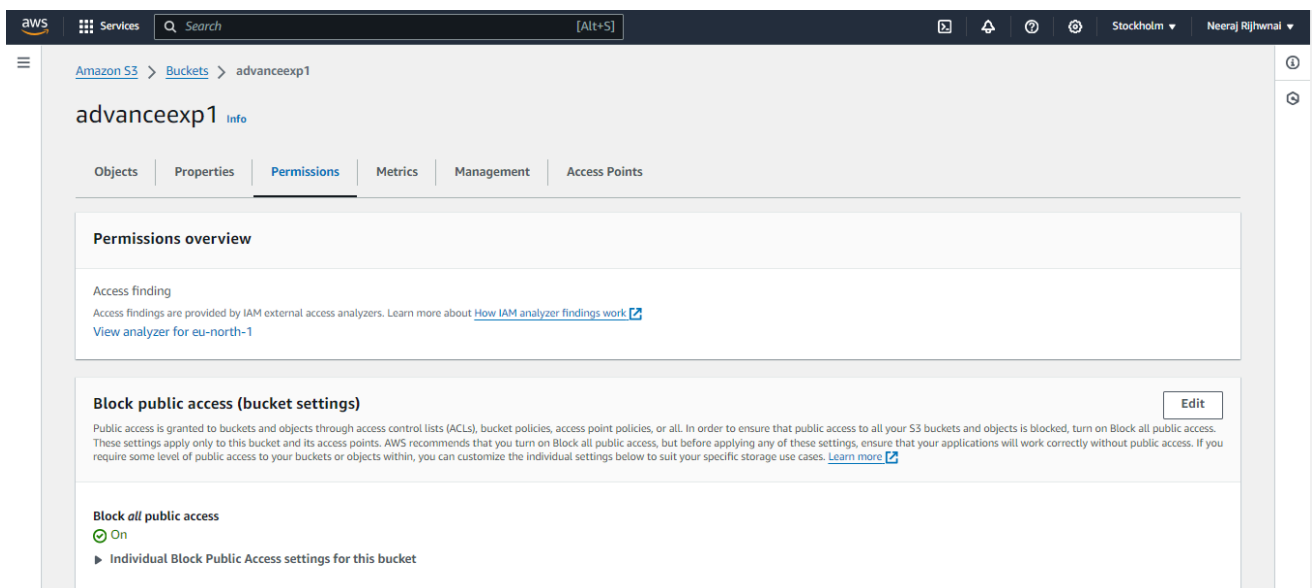
[Advanced settings](#)

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



7)

Go on Permissions tab and check for Block public access



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

### 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.

Cancel

Save changes

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

successfully.



✓ Successfully edited Block Public Access settings for this bucket.

10) Now, navigate to the edit bucket policy in permission 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.

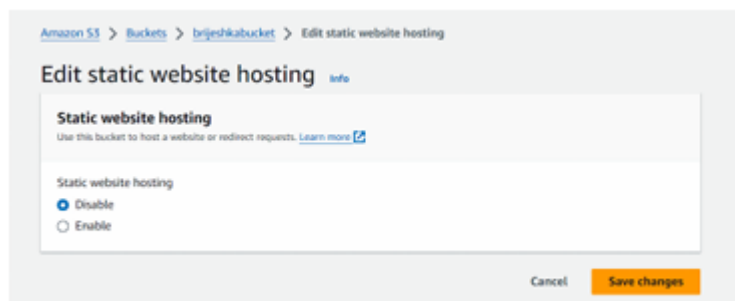
11) Fill the following policy in the empty policy space. Ensure that you change the name of the bucket in Resource with the name of your bucket.

### 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.

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

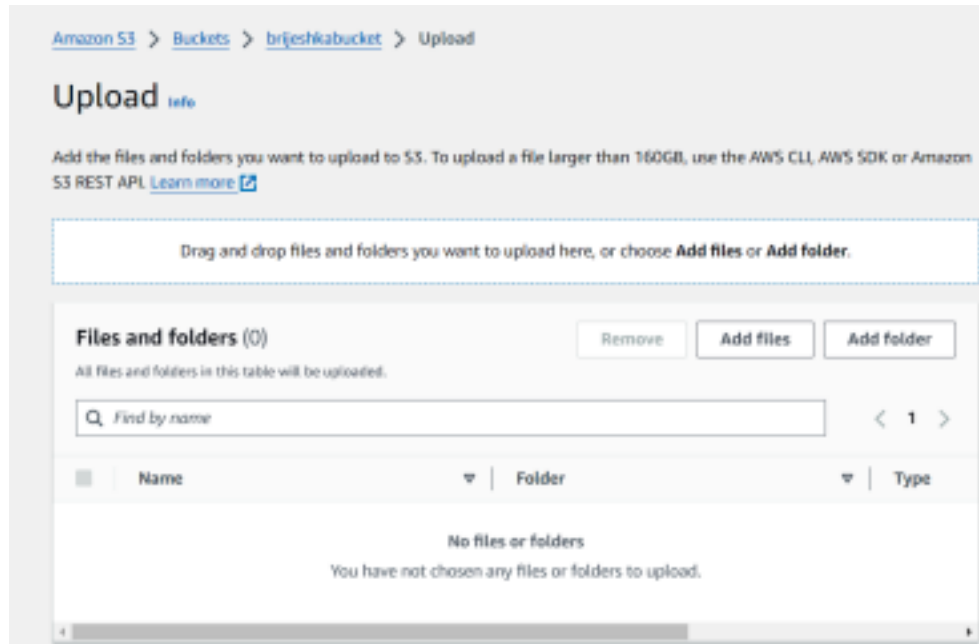


websites.  
shown below, and add the names of the file.

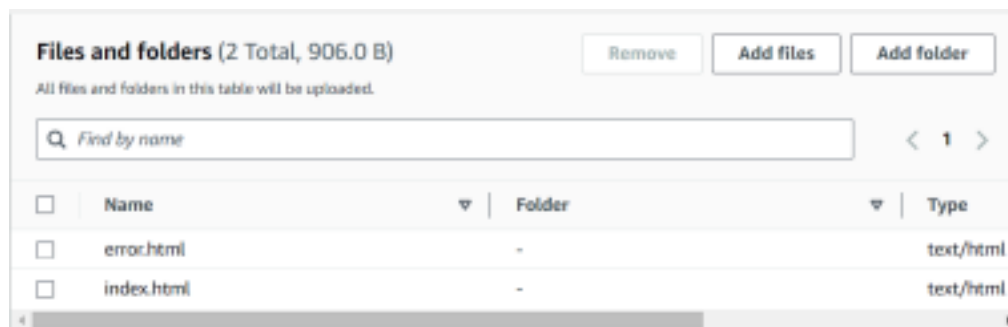
14) Check the options as

A screenshot of the 'Static website hosting' configuration page in the Amazon S3 console. The page title is 'Static website hosting' with a subtext: 'Use this bucket to host a website or redirect requests. [Learn more](#)'. Under the 'Static website hosting' section, the 'Enable' radio button is selected. Under the 'Hosting type' section, 'Host a static website' is selected, with a subtext: 'Use the bucket endpoint as the web address. [Learn more](#)'. The 'Redirect requests for an object' option is also visible. A blue information box contains the text: '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](#)'. Below this, the 'Index document' field is set to 'index.html' and the 'Error document' field is set to 'error.html'.

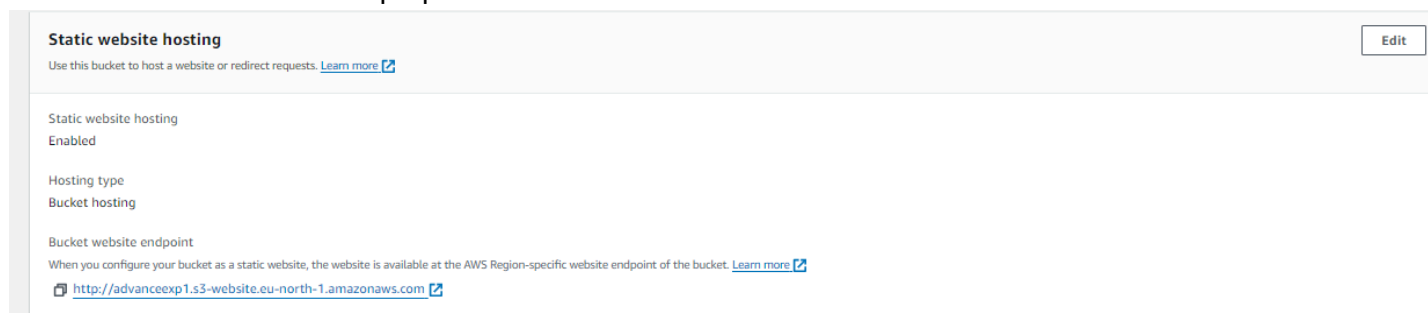
15) Navigate to the Upload section and upload the documents with the name as mentioned in the previous section.



16) Uploaded files will be visible after successful upload.



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



18) The hosted website using AWS S3.

## 403 Forbidden

- Code: AccessDenied
- Message: Access Denied
- RequestId: KS0XA8XZTXSSDHKH
- HostId: +8Eaptgn+uiLPwYcZ3+eEjPEFHTouzxrKdHrxhNTYiDO7E9mwLQv5bqaDJMhSc8KaBc2IHZjH9I=

### An Error Occurred While Attempting to Retrieve a Custom Error Document

- Code: AccessDenied
- Message: Access Denied

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

Objects (2) [Info](#)

Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

Find objects by prefix

<input checked="" type="checkbox"/>	Name	Type	Last modified	Size	Storage class
<input checked="" type="checkbox"/>	<a href="#">error.html</a>	html	August 16, 2024, 10:27:52 (UTC+05:30)	220.0 B	Standard
<input checked="" type="checkbox"/>	<a href="#">index.html</a>	html	August 16, 2024, 10:27:53 (UTC+05:30)	247.0 B	Standard

Successfully emptied bucket "brijeshkibucket"

View details below. If you want to delete this bucket, use the [delete bucket configuration](#).

### Empty bucket: status

The details below are no longer available after you navigate away from this page.

#### Summary

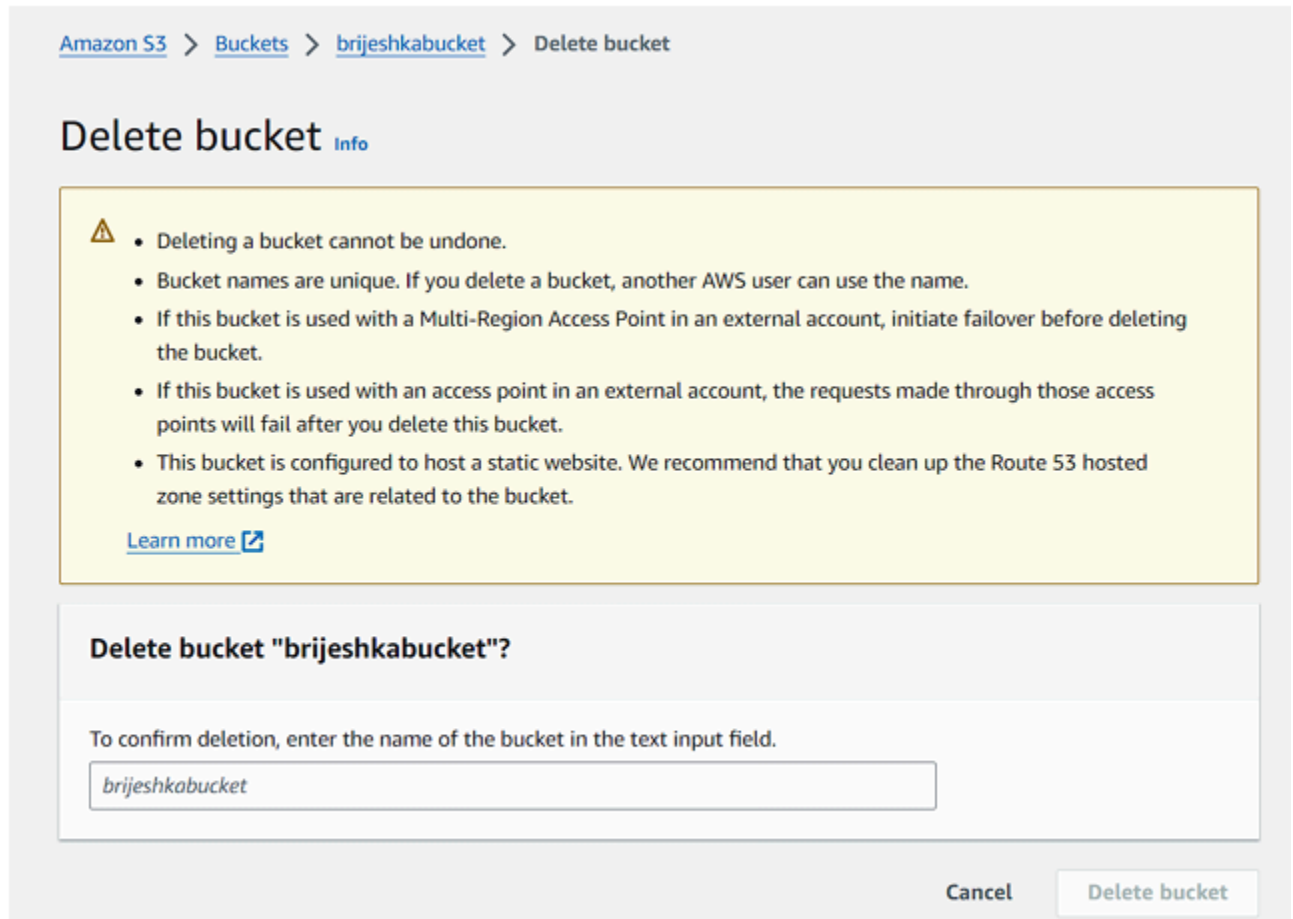
Source <a href="#">s3://brijeshkibucket</a>	Successfully deleted ✔ 2 objects, 906.0 B	Failed to delete 0 objects
--	--	-------------------------------

#### Failed to delete (0)

Find objects by name

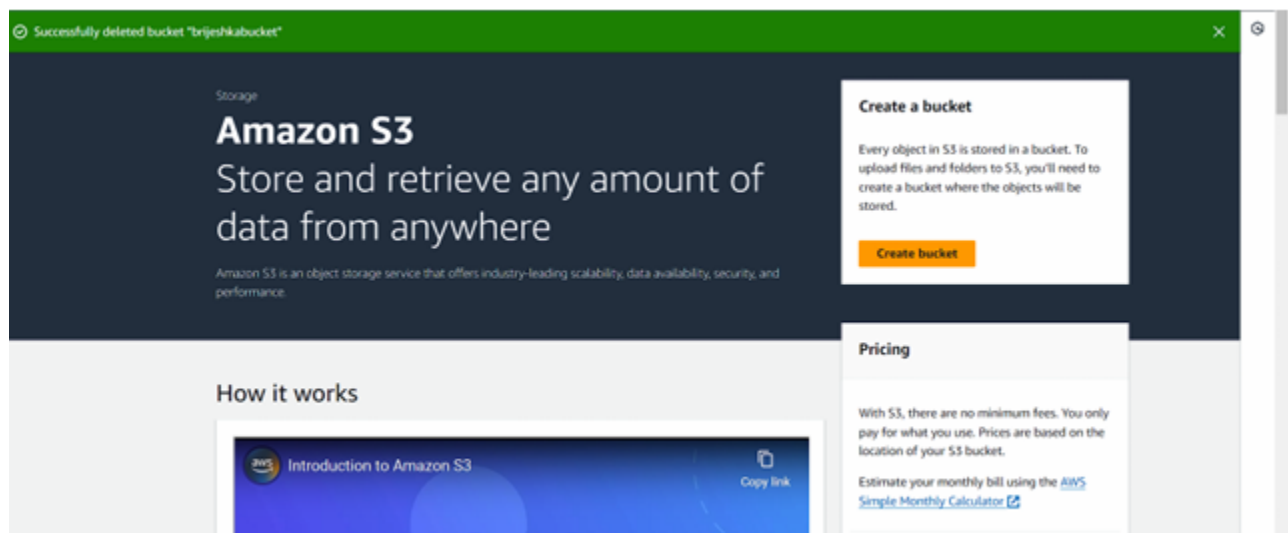
Name	Prefix	Version ID	Type	Last modified	Size	Error
No failed object deletions						

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



21) After deleting the bucket, a message will appear

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



## XAMPP Hosting

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



[Apache Friends](#)
[Download](#)
[Hosting](#)
[Community](#)
[About](#)

EN

# Download

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](#).

## XAMPP for Windows 8.0.30, 8.1.25 & 8.2.12

Version	Checksum	Size
8.0.30 / PHP 8.0.30	<a href="#">What's Included?</a> md5 sha1	<a href="#">Download (64 bit)</a> 144 Mb
8.1.25 / PHP 8.1.25	<a href="#">What's Included?</a> md5 sha1	<a href="#">Download (64 bit)</a> 148 Mb
8.2.12 / PHP 8.2.12	<a href="#">What's Included?</a> md5 sha1	<a href="#">Download (64 bit)</a> 148 Mb

[Requirements](#)
[More Downloads »](#)

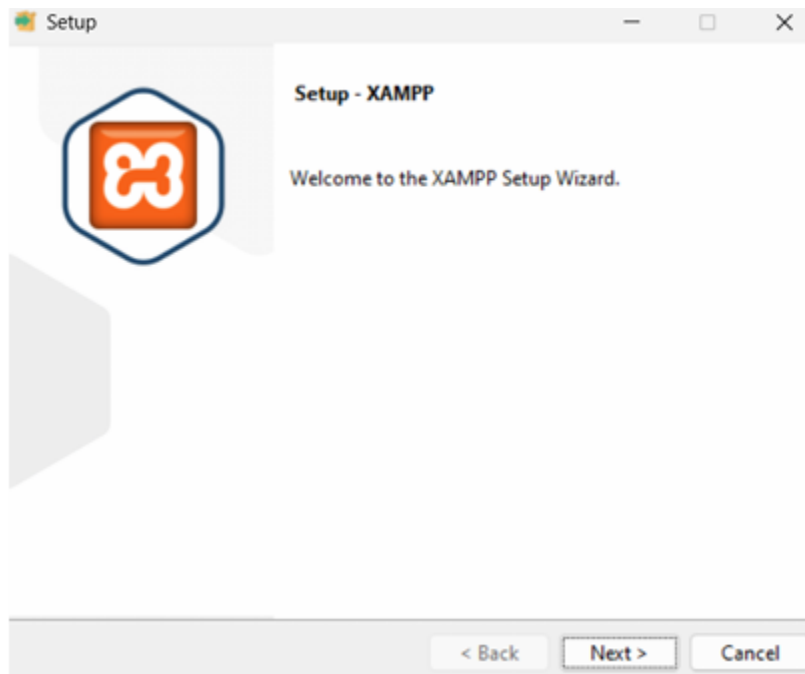
Windows XP or 2003 are not supported. You can download a compatible version of XAMPP for these platforms [here](#).

### Documentation/FAQs

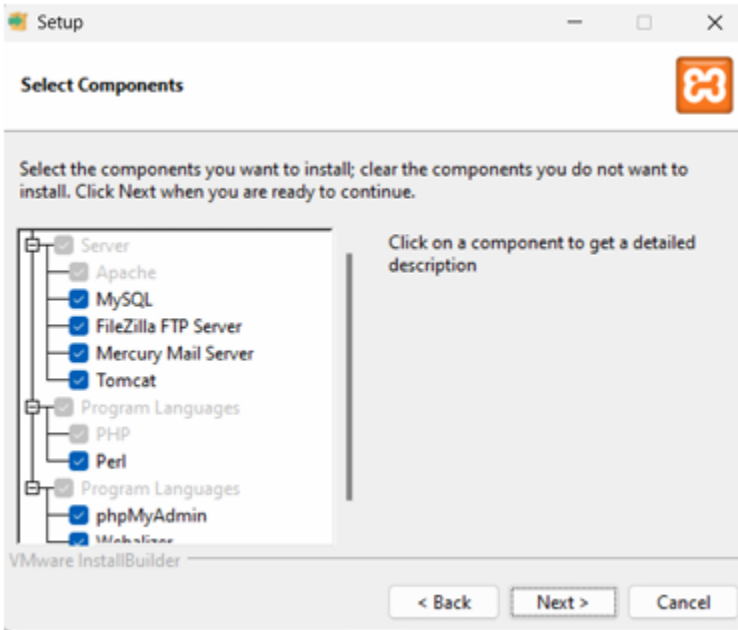
There is no real manual or handbook for XAMPP. We wrote the documentation in the form of FAQs. Have a burning question that's not answered here? Try the [Forums](#) or [Stack Overflow](#).

- Linux FAQs
- Windows FAQs
- OS X FAQs

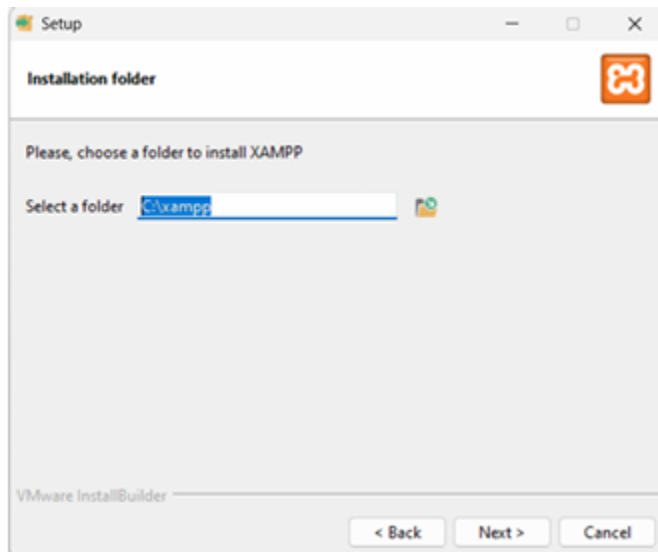
- 2) Xampp installer will be installed in the system.
- 3) Window asking to give permission will appear. Click on 'Yes'.
- 4) A window will appear for setup. Click on 'Next'.



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

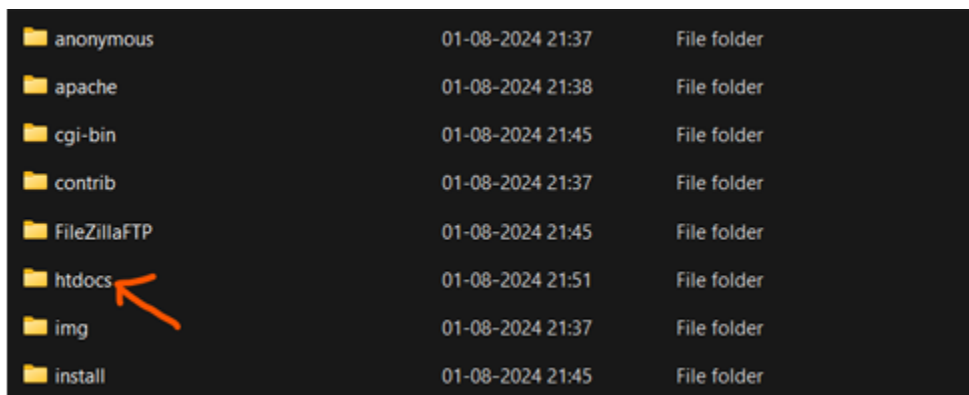


6) Choose the folder path.



7) Then the XAMPP installation will be done.

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



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

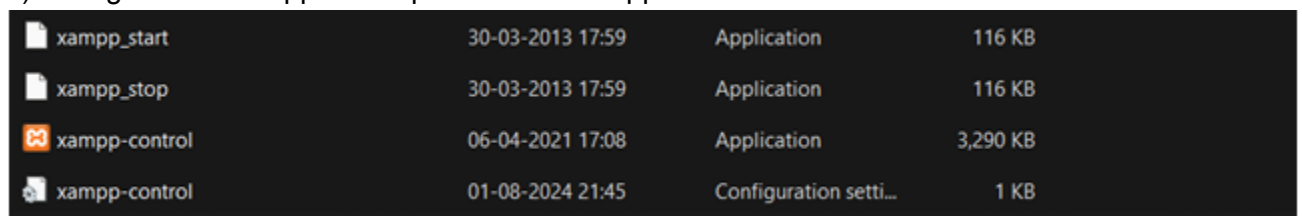


```
<html>
<head>
  <title>First PHP Program</title>
</head>
<body>
  <center>
    <?php
    echo "PHP website hosted using Xampp";
    ?>

    <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>

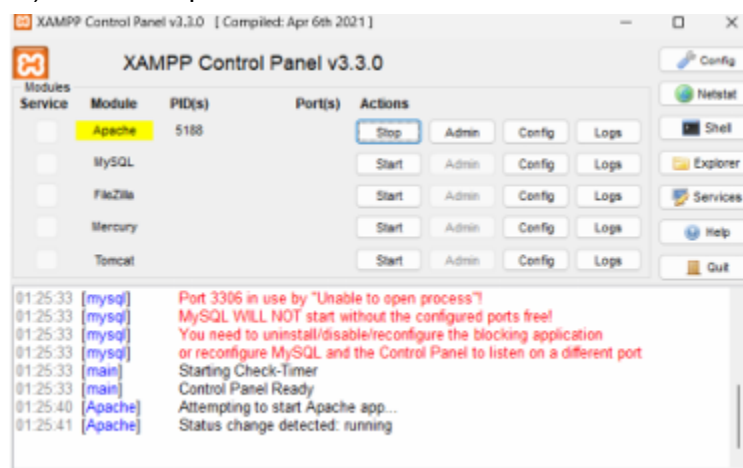
<!-- store in this file whatever to be displayed and
then localhost/MicroNG/file_name -->
```

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.

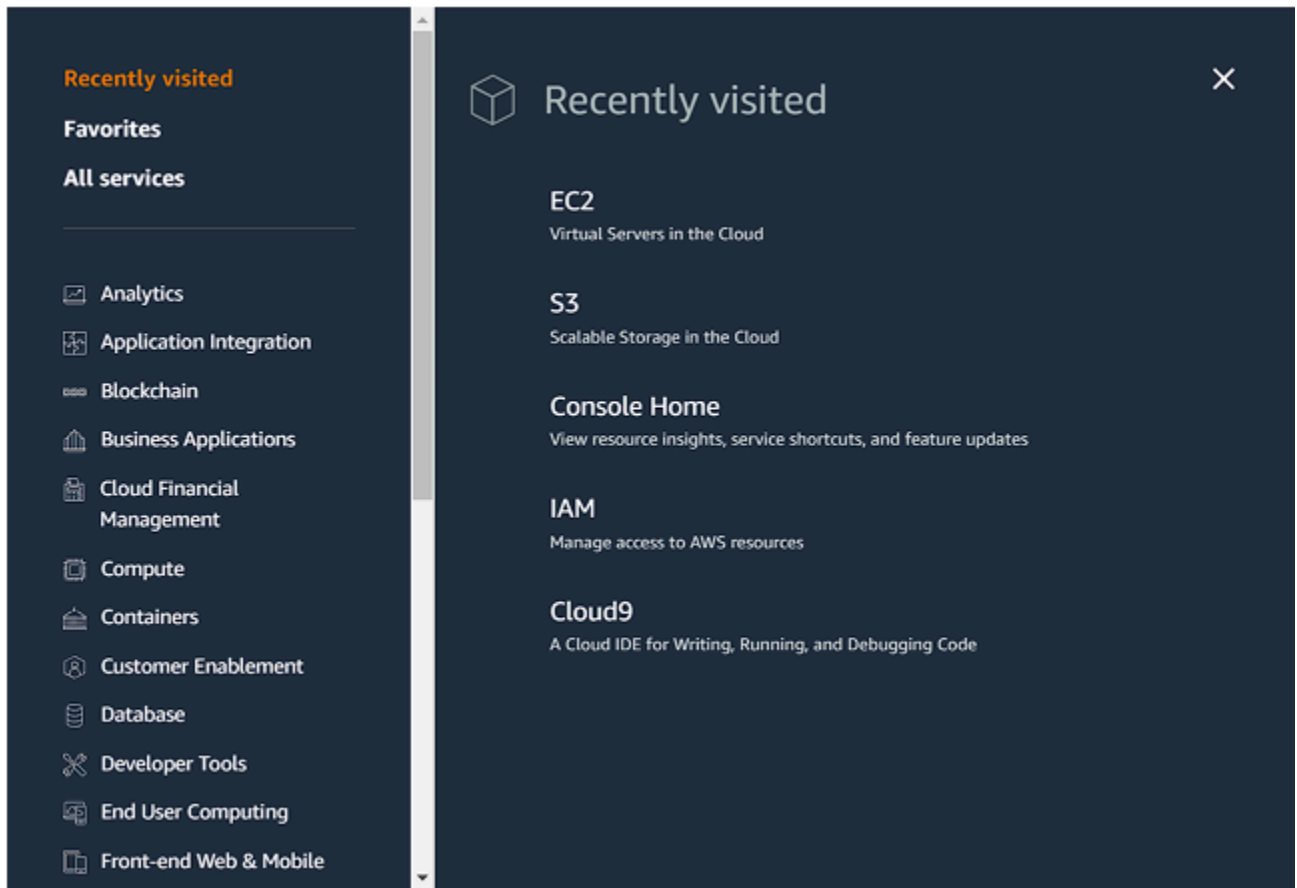
## 403 Forbidden

- Code: AccessDenied
- Message: Access Denied
- RequestId: KS0XA8XZTXSSDHHK
- HostId: +8Eaptgn+uiLPwYcZ3+eEjPEFHtouzxrKdHrxhNTYiDO7E9mwLQv5bqaDJMhSc8KaBc2IHZjH9I=

### An Error Occurred While Attempting to Retrieve a Custom Error Document

- Code: AccessDenied
- Message: Access Denied

## EC2 Instance



## 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.

[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  
ami-04a81a995ec58529 (64-bit (x86)) / ami-0c14f330901e49ff (64-bit (Arm))  
Virtualization: hvm    ENA enabled: true    Root device type: ebs

Free tier eligible

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-04a81a995ec58529

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.

✕

## ▼ Configure storage [Info](#)

[Advanced](#)

1x  GiB  Root volume (Not encrypted)

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

✕

[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](#)

EC2 > Instances > Launch an instance

Availability options  
Creating security groups

➤ Next

Please wait while we launch your instance.  
Do not close your browser while this is loading.

[illegible]

Instances (1) [Info](#) Refresh Connect Instance state ▼ Actions ▼ Launch instances ▼

All states ▼

Clear filters

<input type="checkbox"/>	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IP
<input type="checkbox"/>	AWS Test Server	i-033e8bf30d3d5ed91	Running	t2.micro	2/2 checks passed	<a href="#">View alarms</a>	us-east-1b	ec2-35-

Instances (1/1) [Info](#) Refresh Connect Instance state ▲ Actions ▼ Launch instances ▼

All states ▼

Clear filters

<input checked="" type="checkbox"/>	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IP
<input checked="" type="checkbox"/>	AWS Test Server	i-033e8bf30d3d5ed91	Running	t2.micro	2/2 checks passed	<a href="#">View alarms</a>	us-east-1b	ec2-35-

Stop instance  
Start instance  
Reboot instance  
Hibernate instance  
Terminate instance

### 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)	<span>✔ Disabled</span>

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](#) Refresh Connect Instance state ▼ Actions ▼ Launch instances ▼

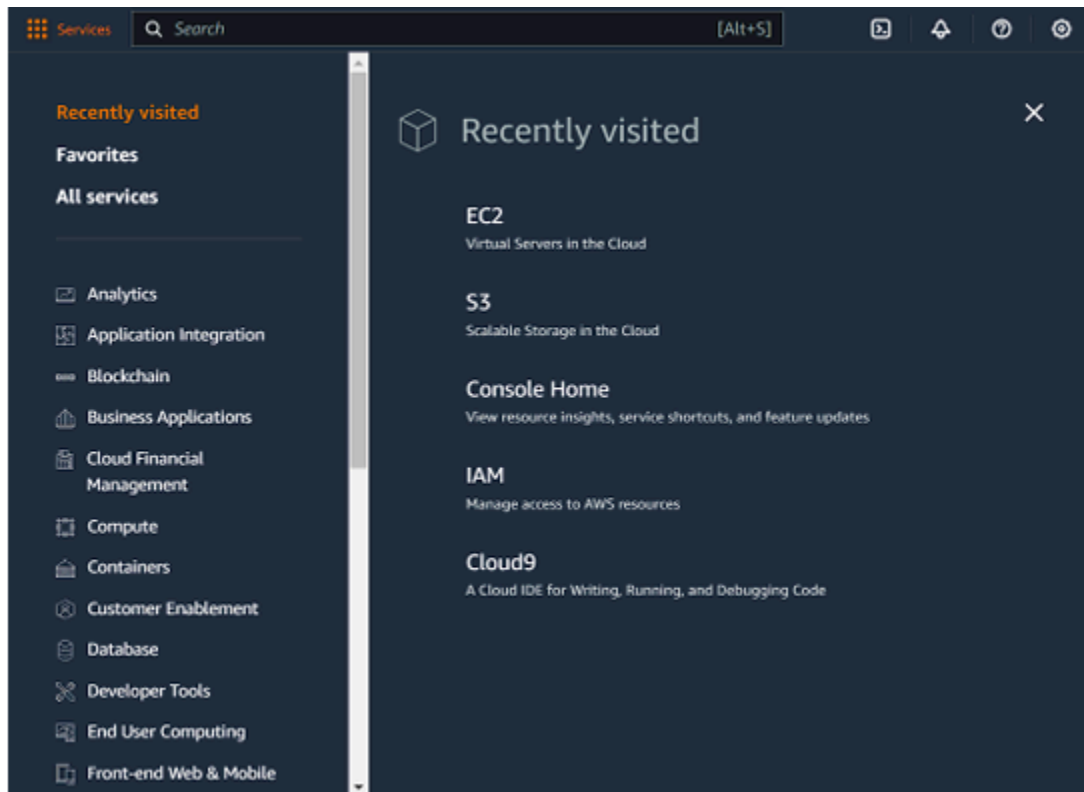
All states ▼

<input type="checkbox"/>	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IP
<input type="checkbox"/>	AWS Test Server	i-033e8bf30d3d5ed91	Terminated	t2.micro	-	<a href="#">View alarms</a>	us-east-1b	-

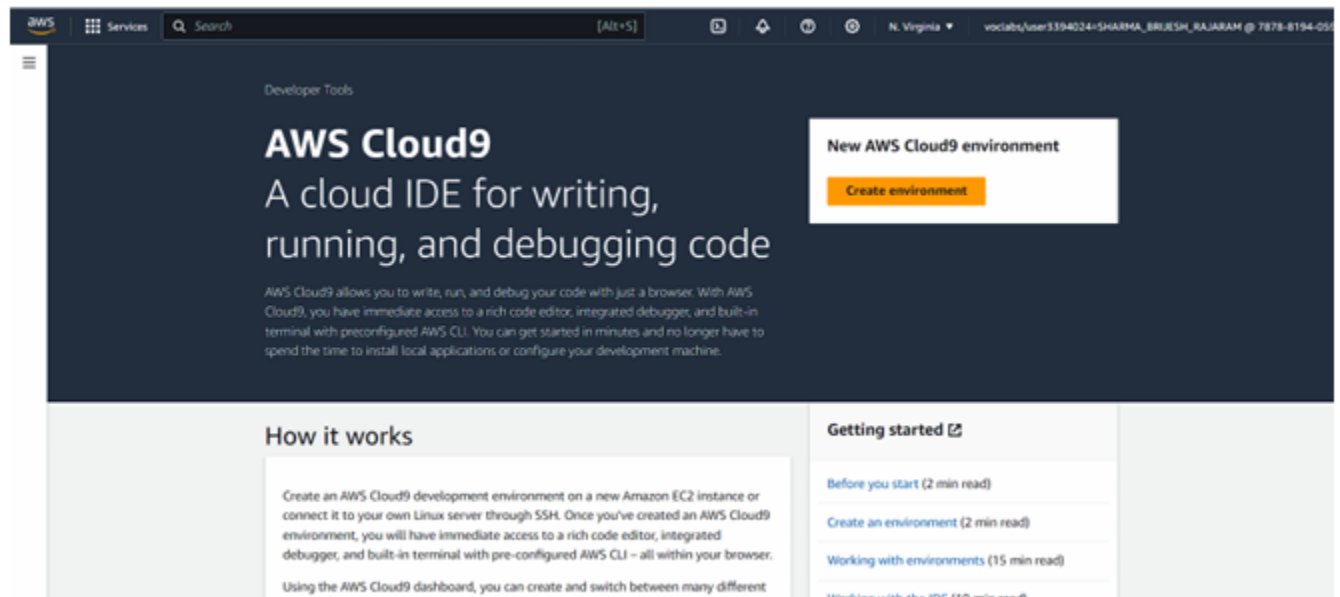
## Cloud 9 - IDE

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





2) Click on Create Environment and start creating the environment



3) Name the environment and select new EC2 instance.

## Details

Name

AWS Cloud9

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)

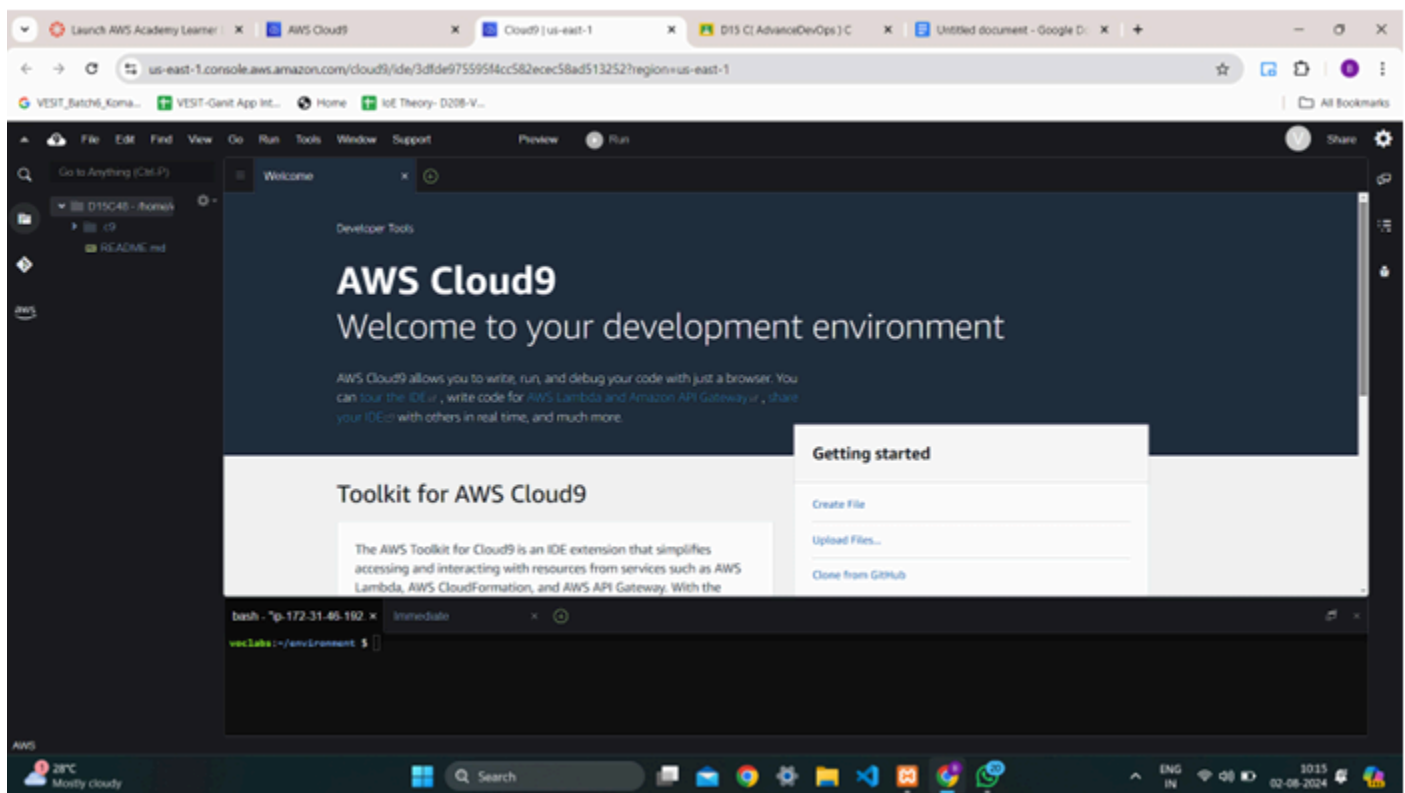
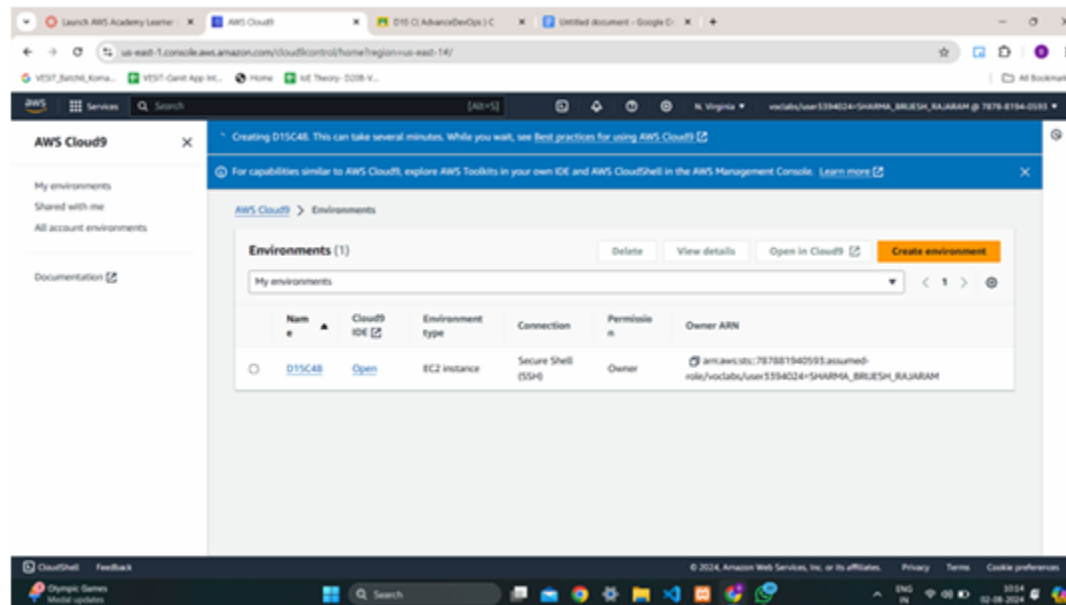
Accesses environment via SSM without opening inbound ports (no ingress).

☐ Secure Shell (SSH)

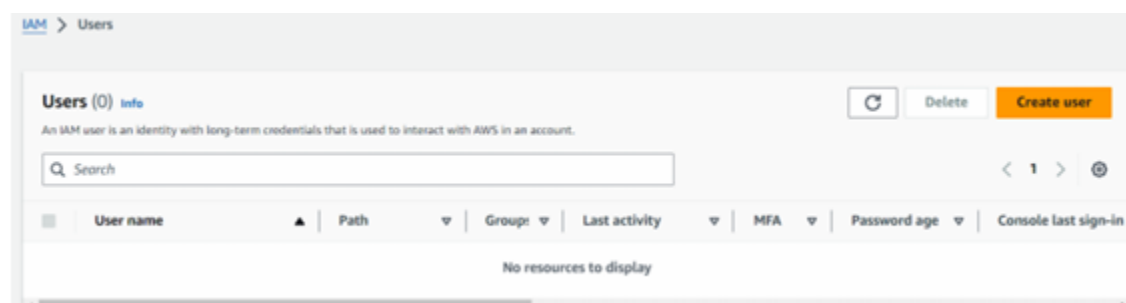
Accesses environment directly via SSH, opens inbound ports.

► VPC settings [Info](#)

5) Environment created successfully.



6) Create user using the IAM.



7) Add the username

## Specify user details

### User details

User name

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.

**i** 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](#)

Cancel Next

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

### User details

User name

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 ! @ # \$ % ^ & \* ( ) \_ + - { } | ' " =

☐ 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.

**i** 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.

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](#)

- Add user to group

- Copy permissions

☐ Attach policies directly



Create group

**Next**

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.

[Email sign-in instructions](#) 

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

 Brij@ews

[Return to users list](#)

👉 AWSGroup1 user group created.

IAM &gt; Users &gt; Create user

### Step 1

#### Specify user details

### Step 2

#### Set permissions

Step 3  
Review and create

Step 4  
Retrieve password

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](#)

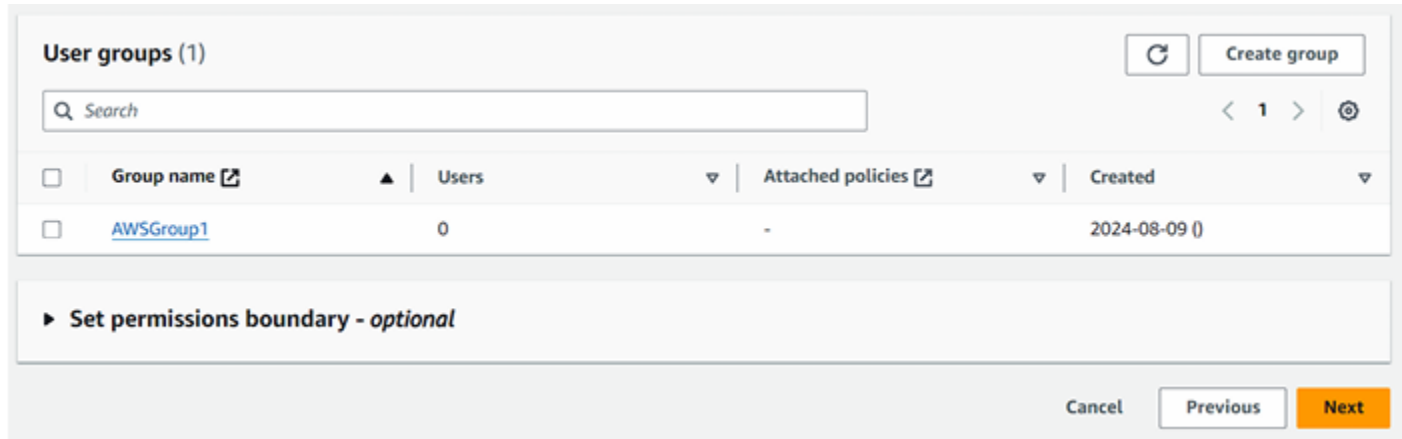
- Add user to group

☐ Copy permissions

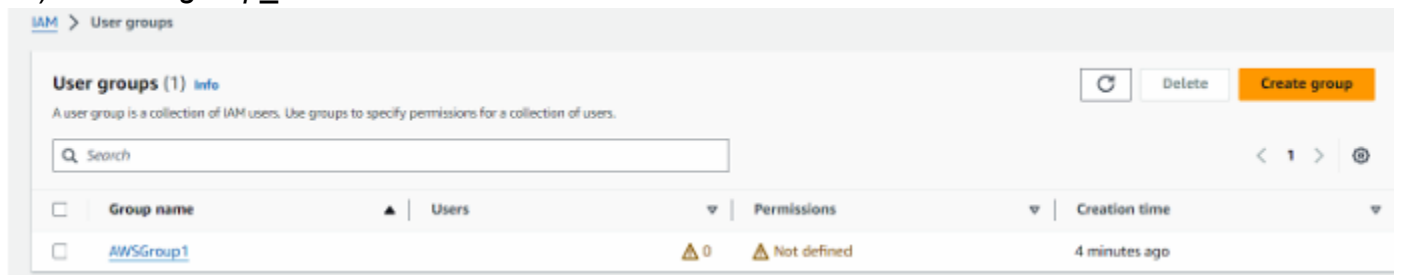
☐ Attach policies directly

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.

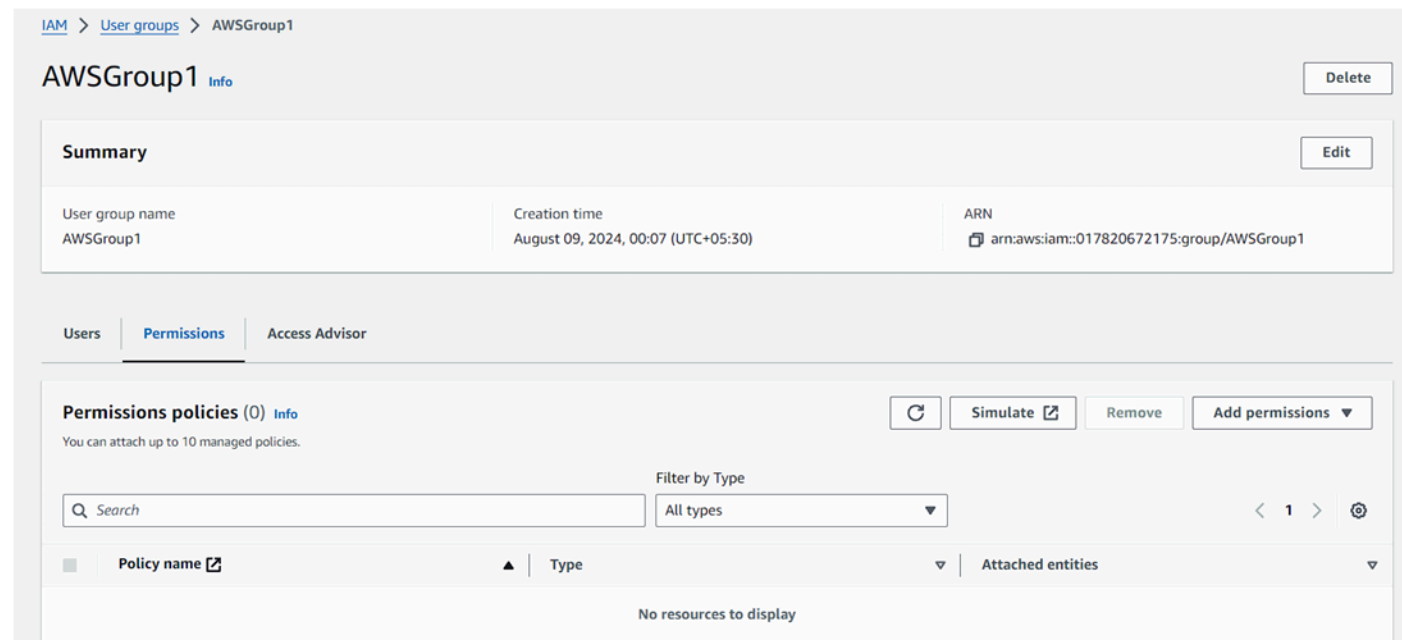
12) Write the user group name and proceed.



13) Click on *group\_name*.



14) Go to Add permissions and click on Add Permissions



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

[IAM](#) > [User groups](#) > AWSGroup1

## AWSGroup1

Info

Delete

Summary

Edit

User group name	Creation time	ARN
AWSGroup1	August 09, 2024, 00:07 (UTC+05:30)	arn:aws:iam::017820672175:group/AWSGroup1

Users

Permissions

Access Advisor

Permissions policies (0)

Info

You can attach up to 10 managed policies.

Search

Filter by Type

All types

< 1 >

☐

Policy name

▲

Type

▼

Attached entities

▼

No resources to display

16) User group is created successfully.

Policies attached to this user group.

[IAM](#) > [User groups](#) > AWSGroup1

## AWSGroup1

Info

Delete

Summary

Edit

User group name	Creation time	ARN
AWSGroup1	August 09, 2024, 00:07 (UTC+05:30)	arn:aws:iam::017820672175:group/AWSGroup1

Users

Permissions

Access Advisor

Permissions policies (1)

Info

You can attach up to 10 managed policies.

Search

Filter by Type

All types

< 1 >

☐

Policy name

▲

Type

▼

Attached entities

▼

☐

[AWSCloud9EnvironmentMember](#)

AWS managed

1