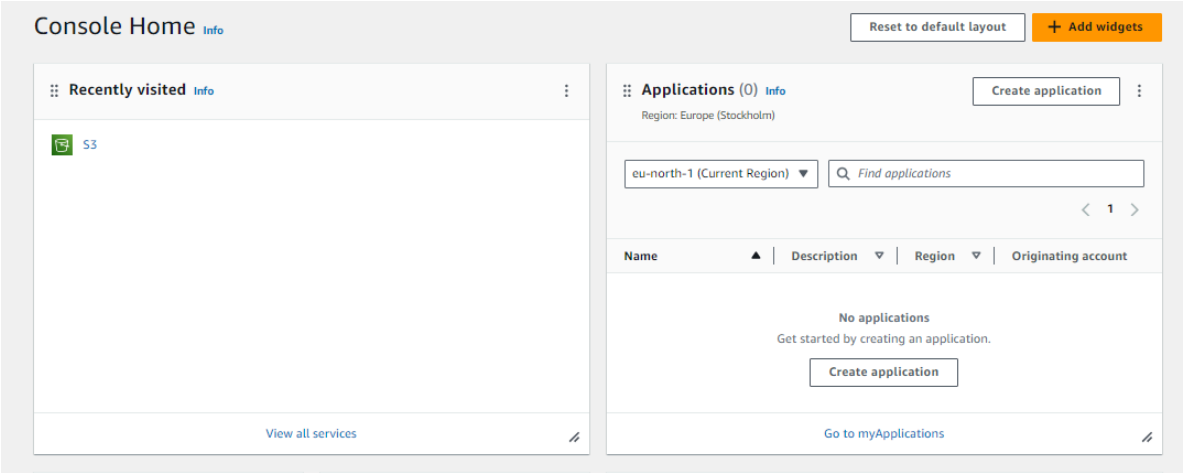
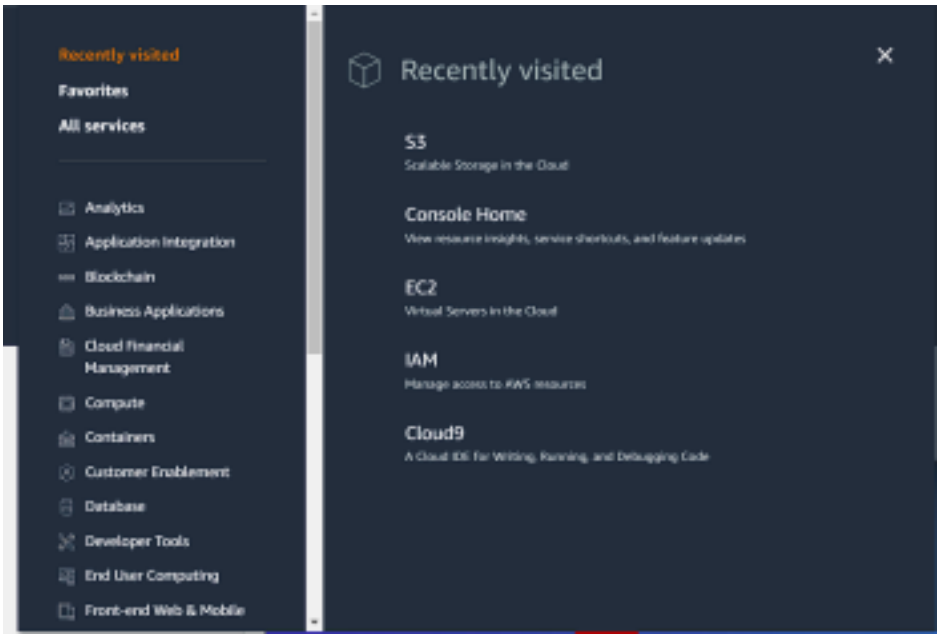
Hosting a static website on Amazon Web Services (S3)

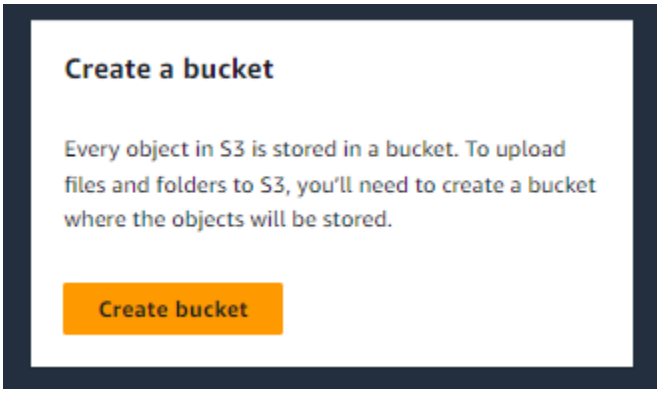
1) Open the AWS console home



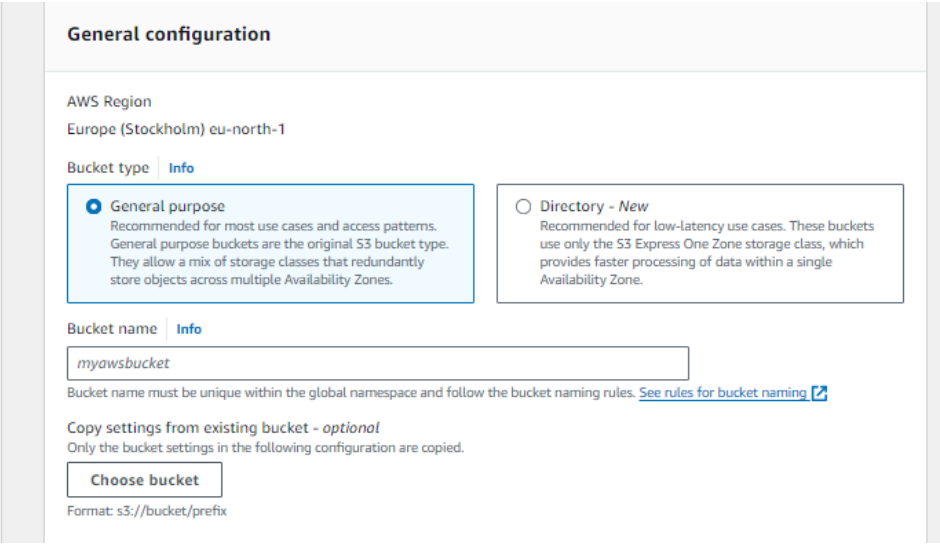
2) Navigate to the S3 to host the website



3) On S3, click on create bucket

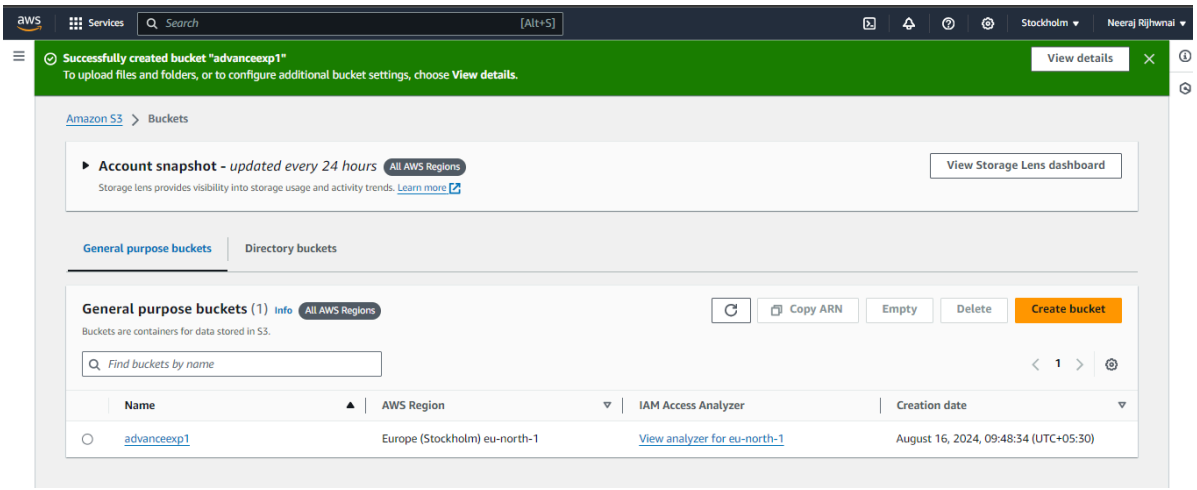


4) Click on Bucket type as General Purpose and name the bucket.



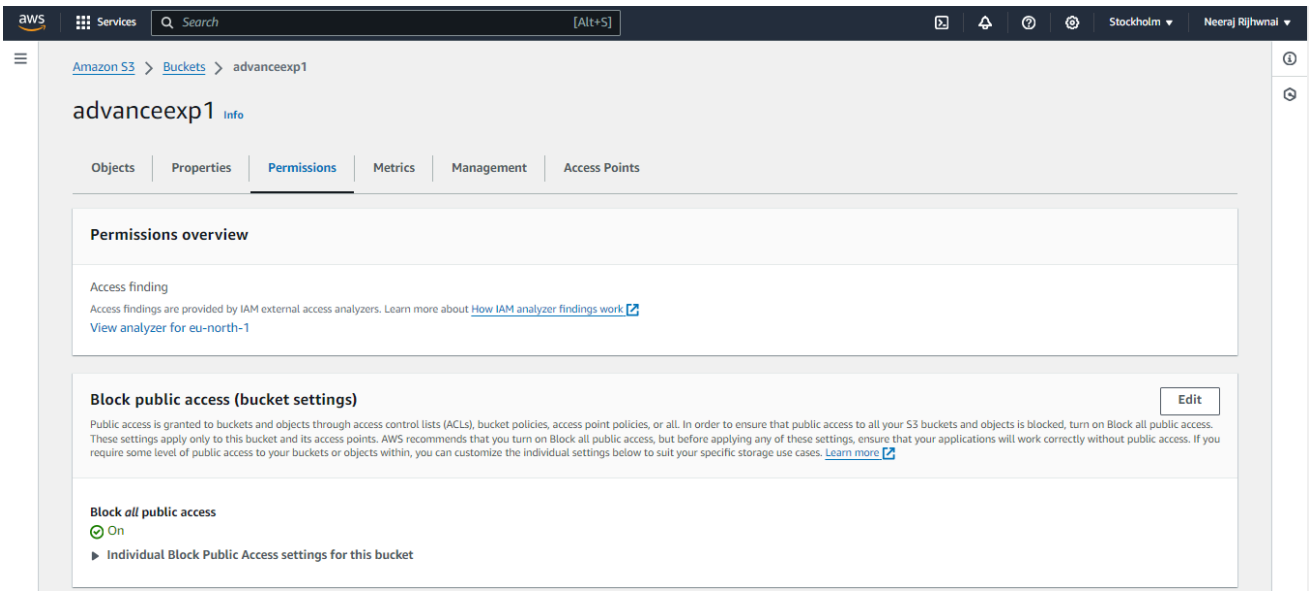
5) Keep the default settings intact, checking for bucket versioning is disabled and bucket key enabled.

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

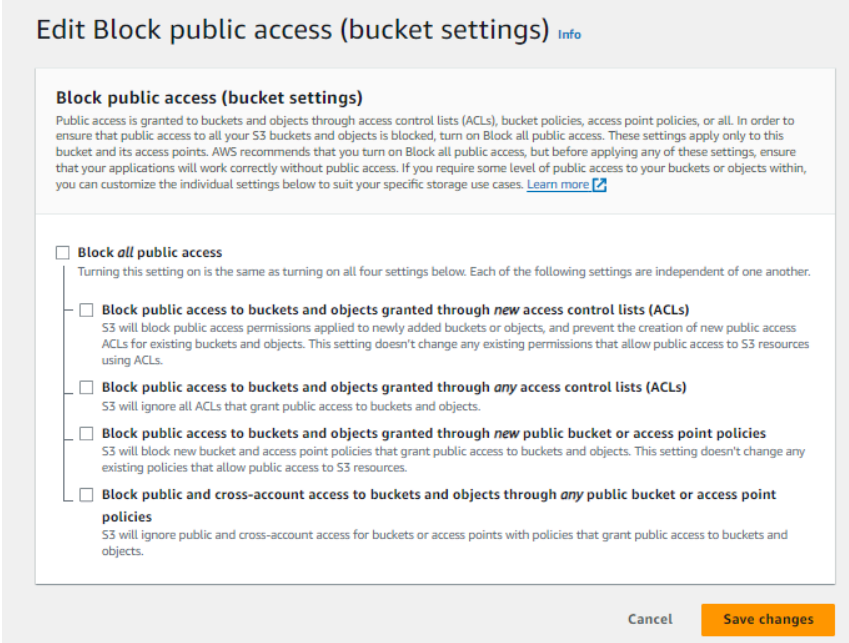


7)

Go on Permissions tab and check for Block public access

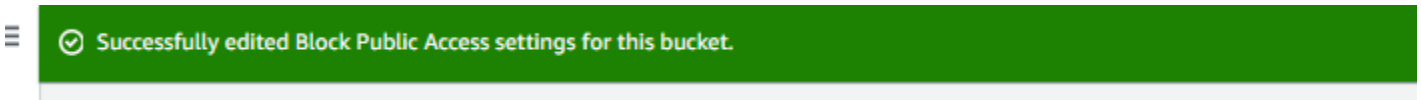


8) Block public access is default on, we need to uncheck it to ensure the hosted website is public.

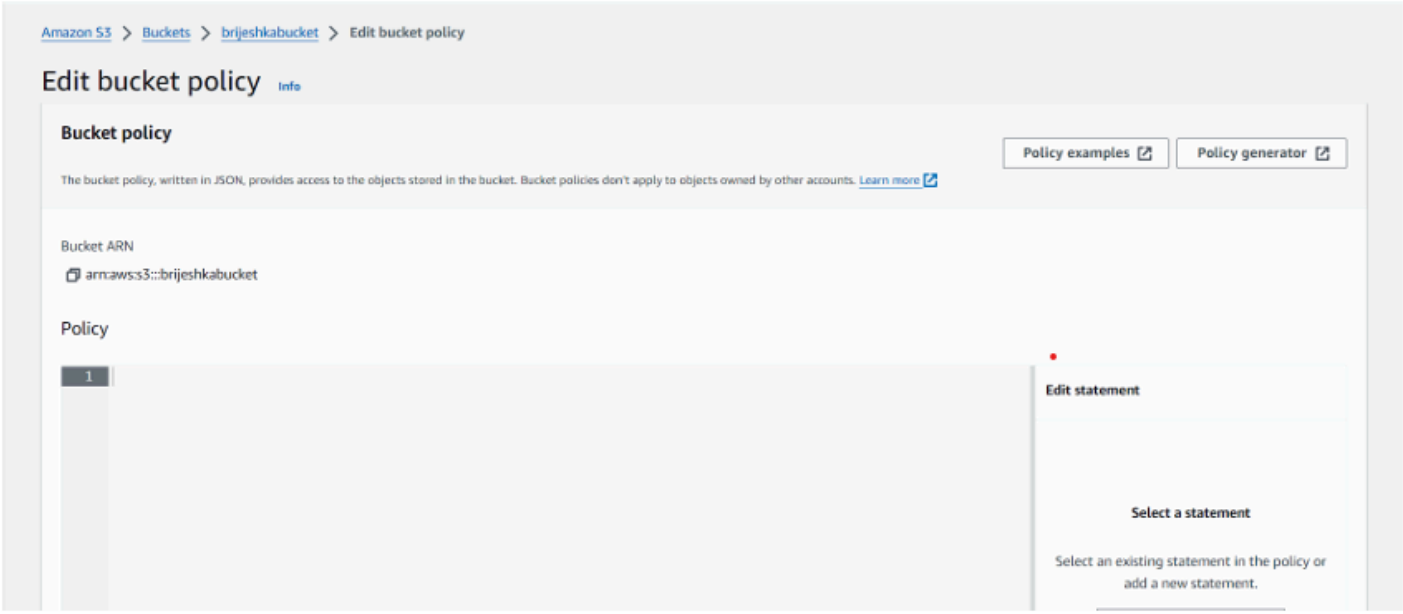


9) Now the block public access option is unchecked and hence the website can be hosted

successfully.



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



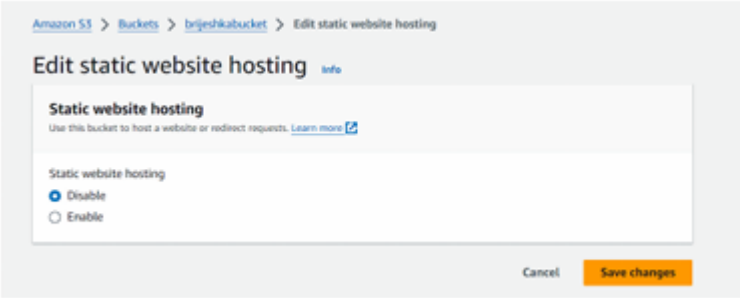
11) Fill the following policy in the empty policy space. Ensure that you change the name of the bucket in Resource with the name of your bucket.

Policy

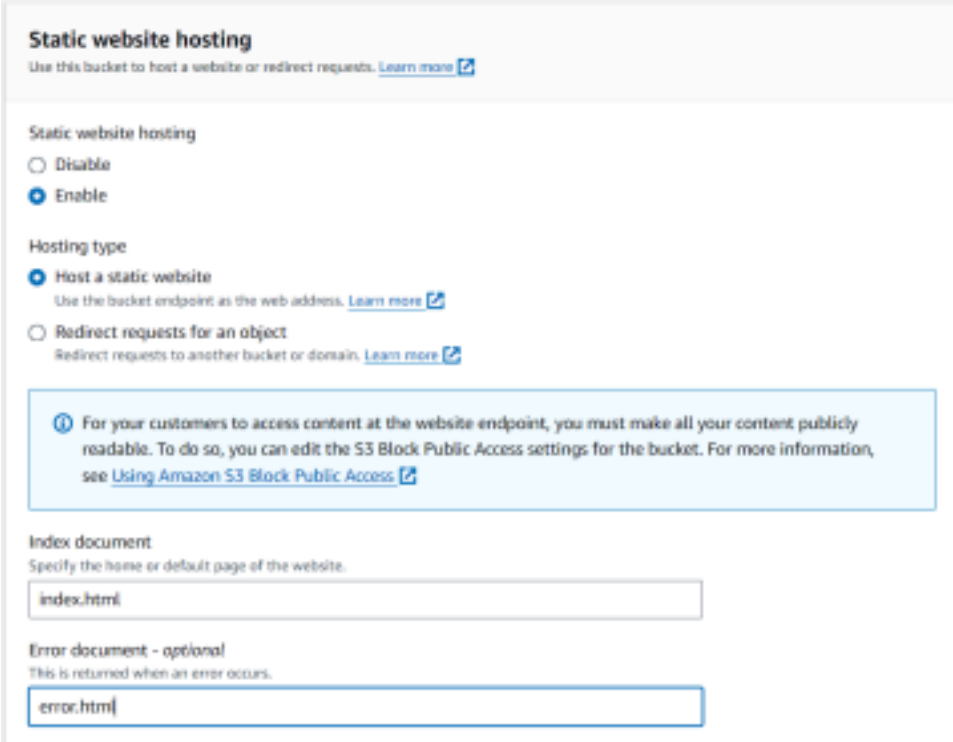
```
1  {
2      "Version": "2012-10-17",
3      "Statement": [
4          {
5              "Sid": "PublicReadGetObject",
6              "Effect": "Allow",
7              "Principal": {
8                  "AWS": "*"
9              },
10             "Action": "s3:GetObject",
11             "Resource":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

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

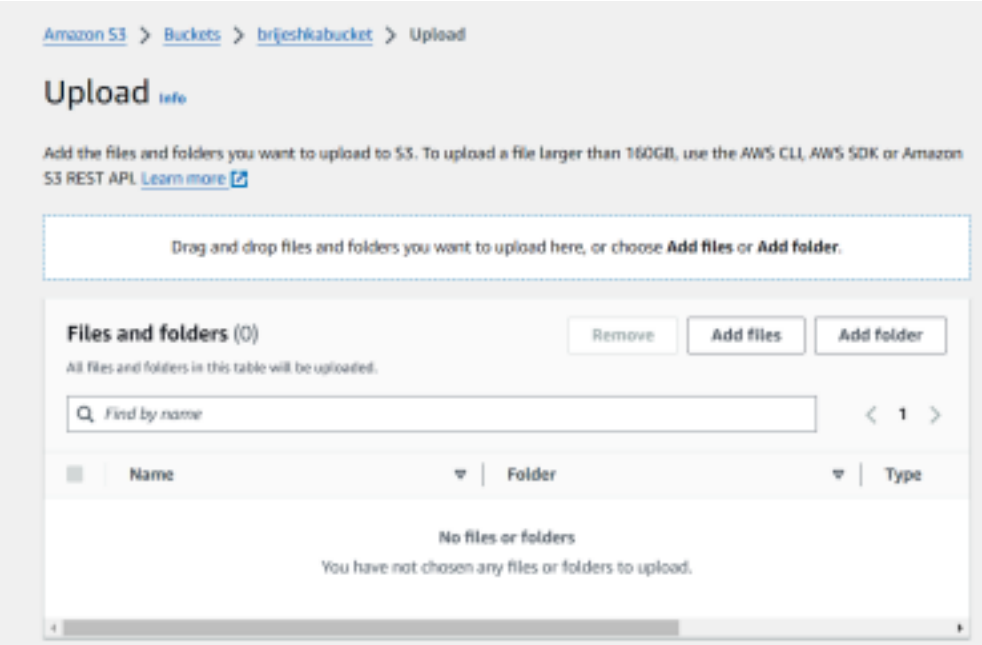
13) Go to the edit static website hosting in the properties tab to use bucket to host



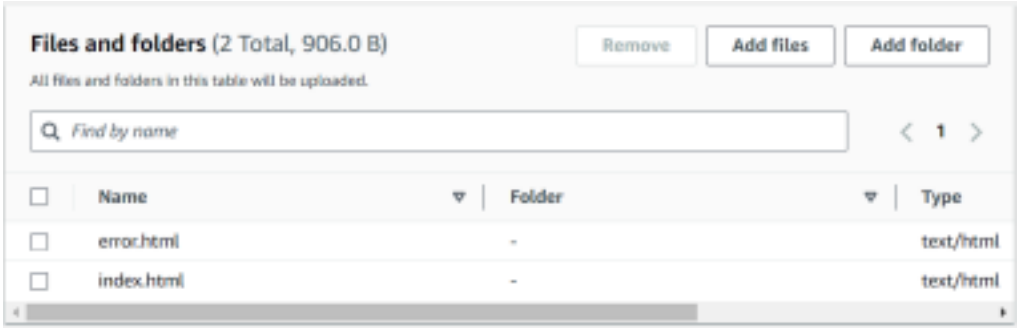
websites. 14) Check the options as shown below, and add the names of the file.



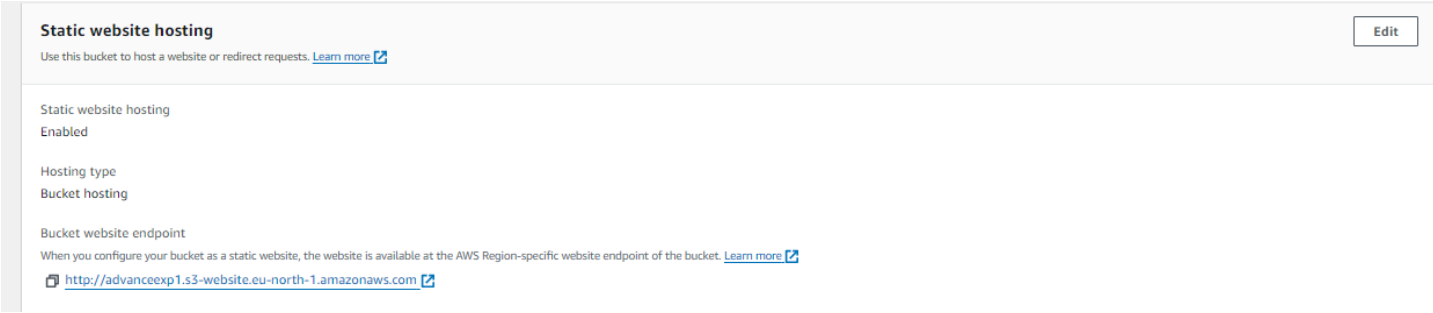
15) Navigate to the Upload section and upload the documents with the name as mentioned in the previous section.



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.

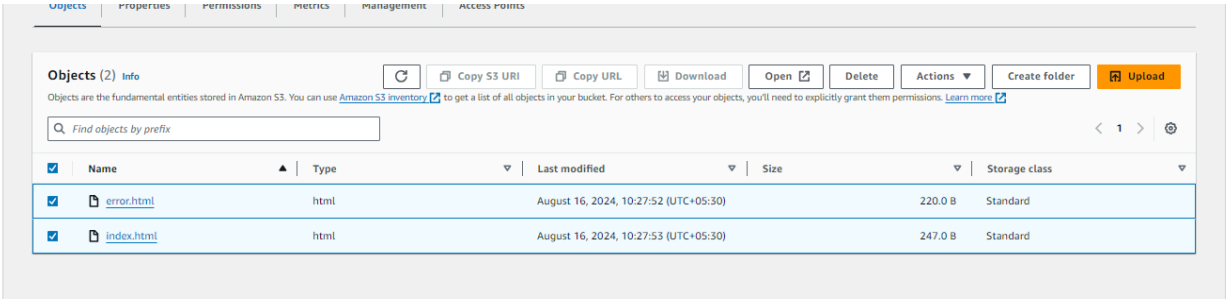
403 Forbidden

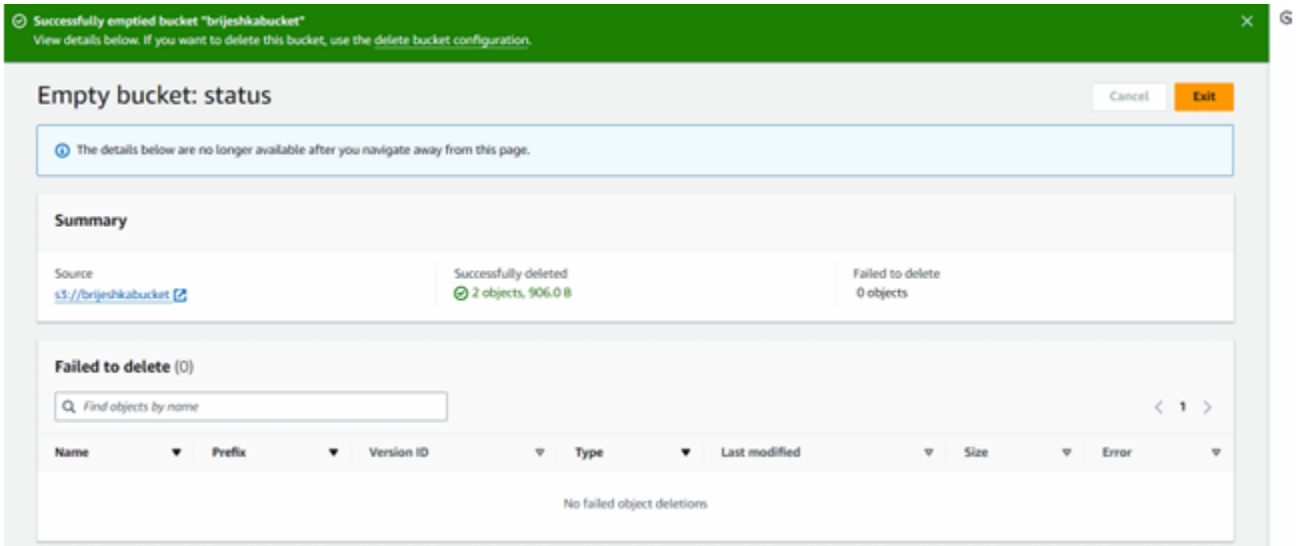
- Code: AccessDenied
- Message: Access Denied
- RequestId: KS0XA8XZTXSSDHKH
- HostId: +8Eaptgn+uiLPwYcZ3+eEjPEFHtouzxrKdHrxhNTYiDO7E9mwLQv5bqaDJMhSc8KaBc2IHzjH9I=

An Error Occurred While Attempting to Retrieve a Custom Error Document

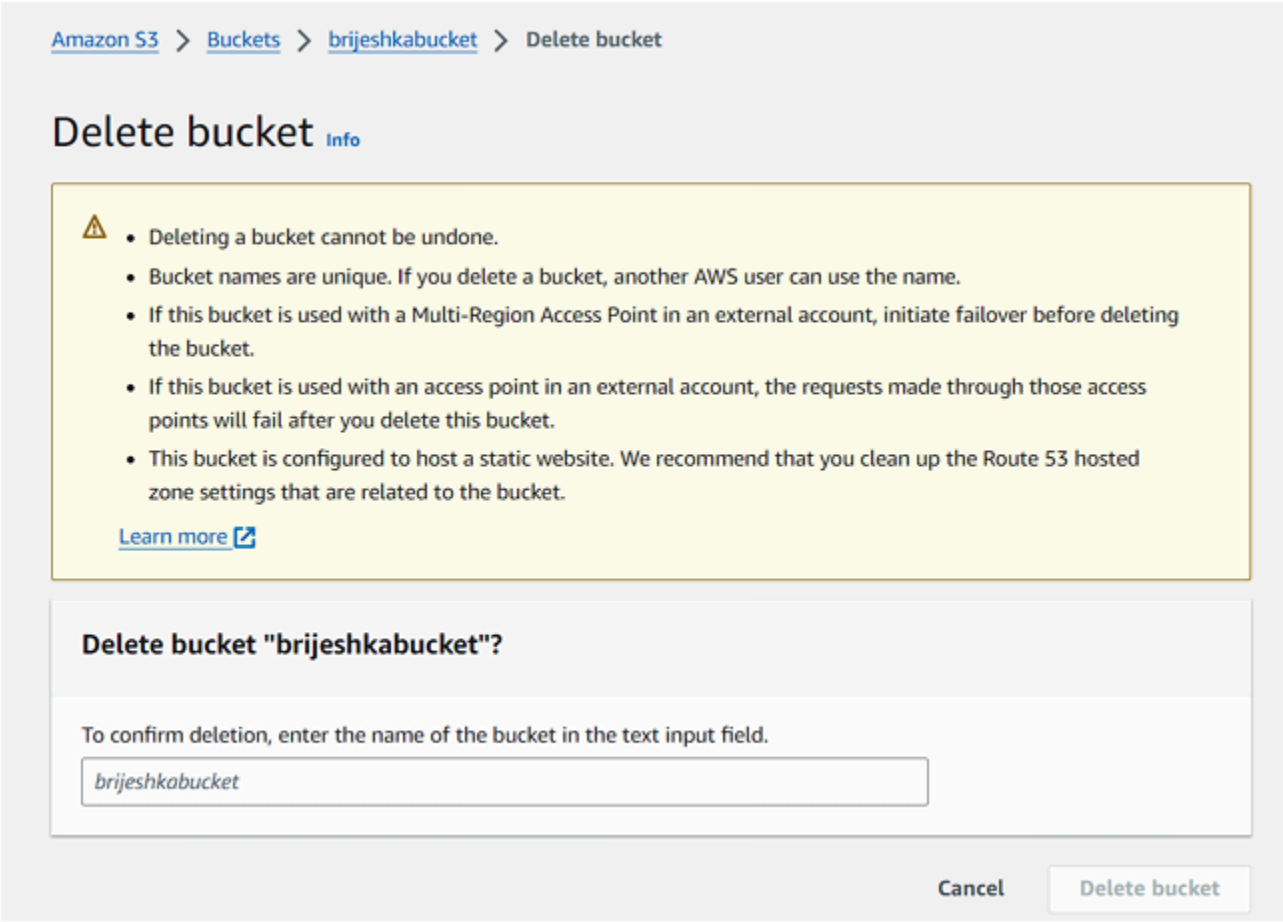
- Code: AccessDenied
- Message: Access Denied

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

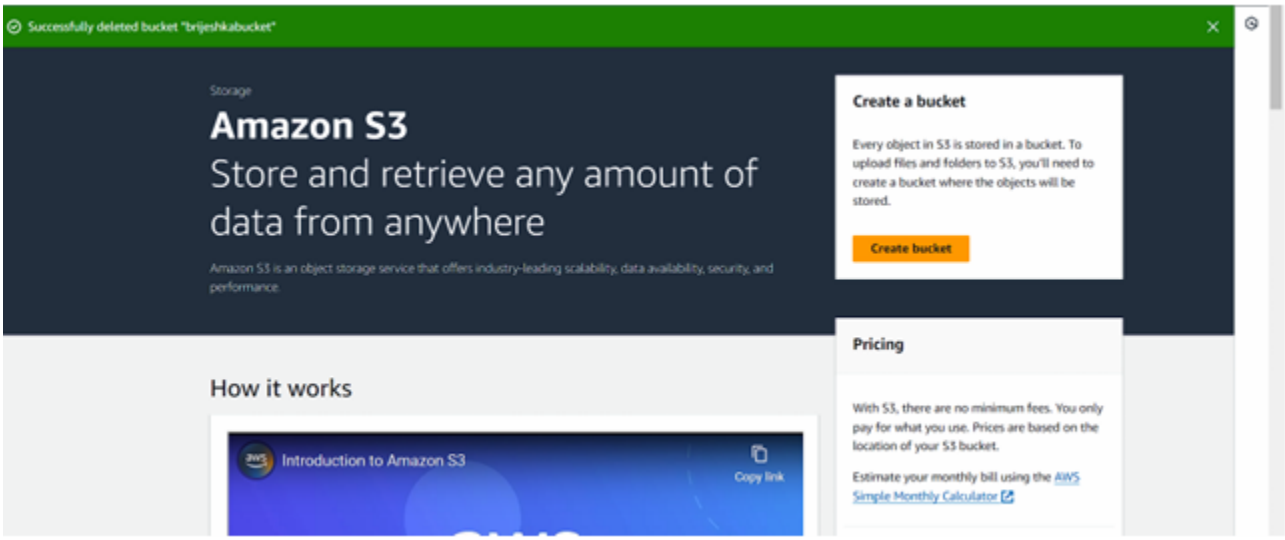




20) Then navigate to the Delete bucket option and enter the name of the bucket and delete the bucket.

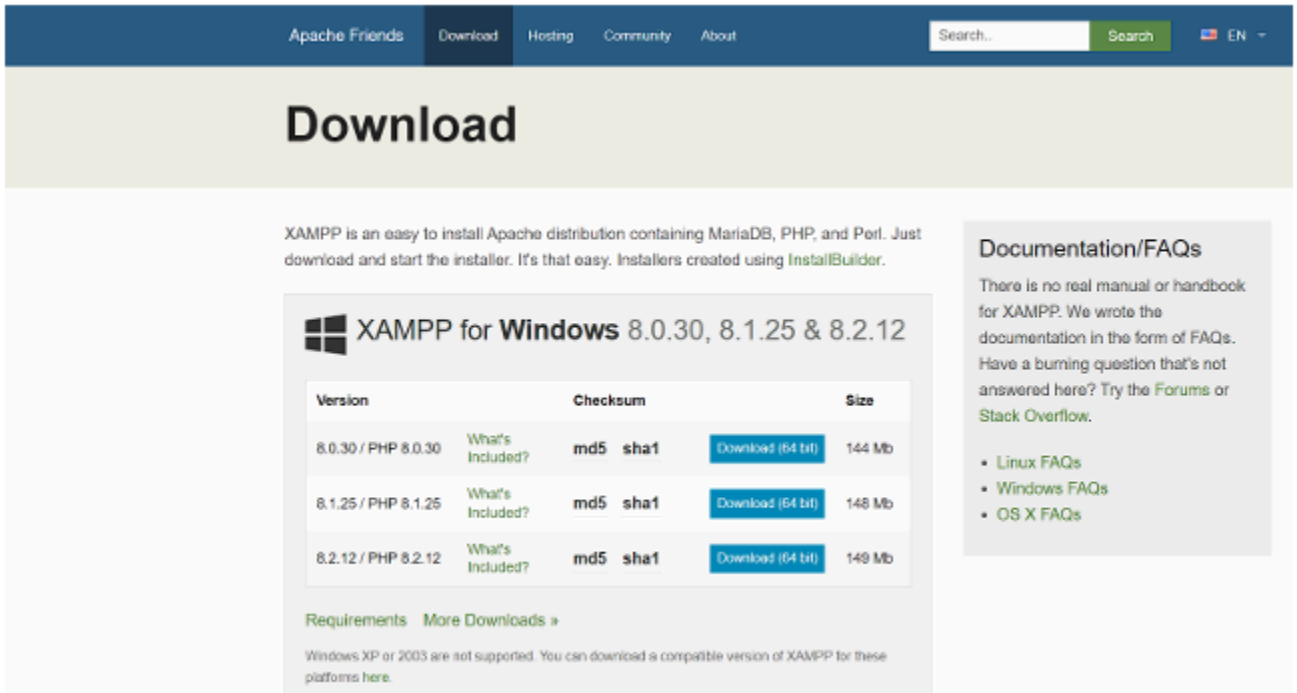


21) After deleting the bucket, a message will appear.



XAMPP Hosting

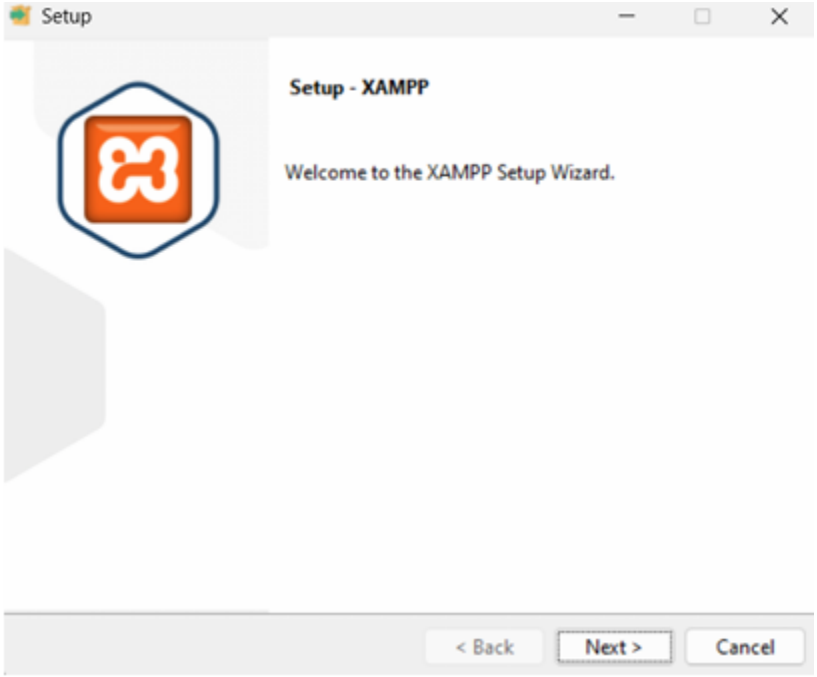
1) Search for XAMPP download and navigate to the xampp official website and click on download as per your system.



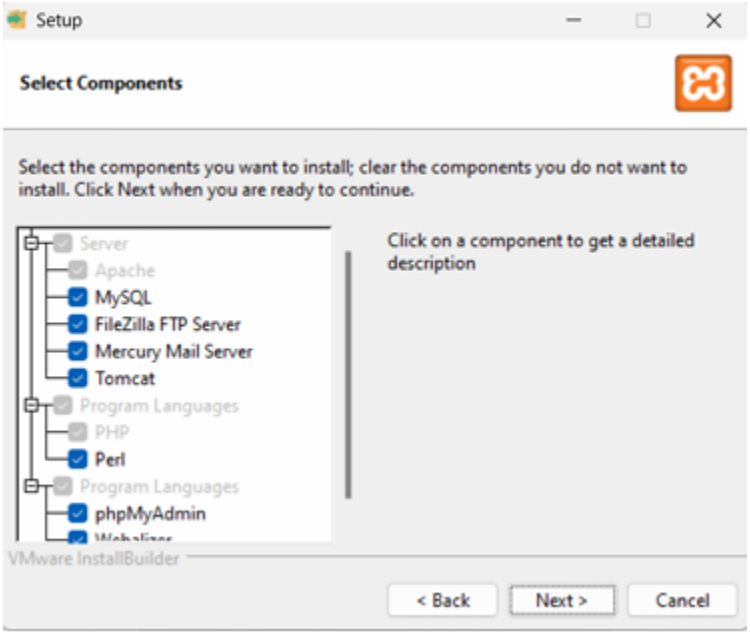
2) Xampp installer will be installed in the system.

3) Window asking to give permission will appear. Click on ‘Yes’.

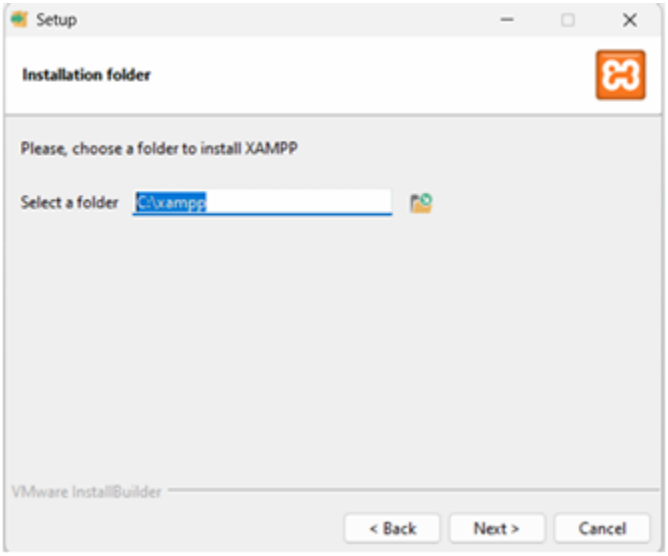
4) A window will appear for setup. Click on ‘Next’.



5) Keep the default settings and click on Next.

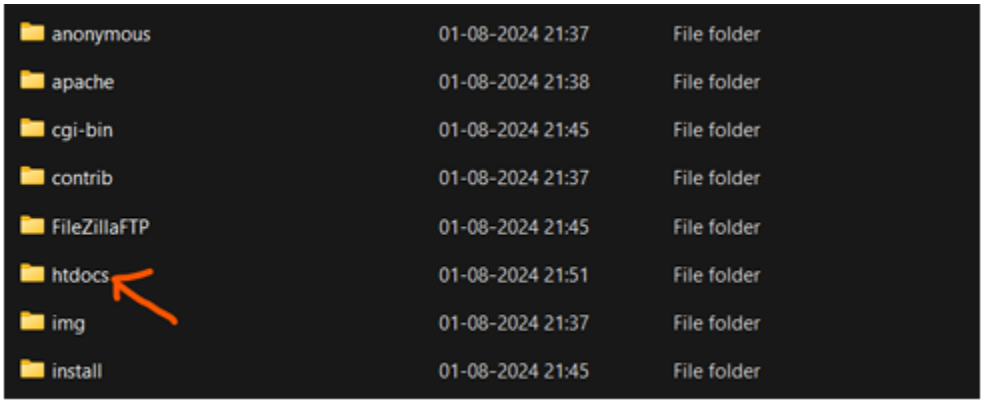


6) Choose the folder path.



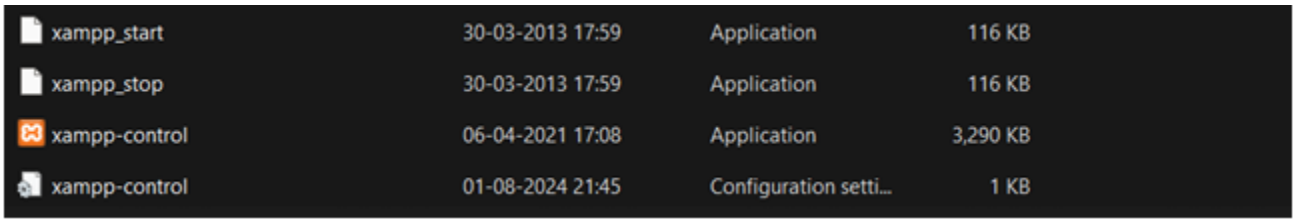
7) Then the XAMPP installation will be done.

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



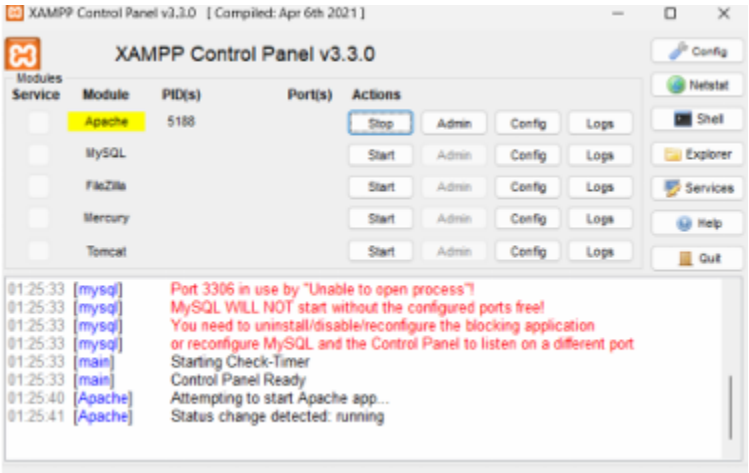
9) Create a test.php file in the htdocs folder and write php code.

10) Now go to the xampp contol 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.

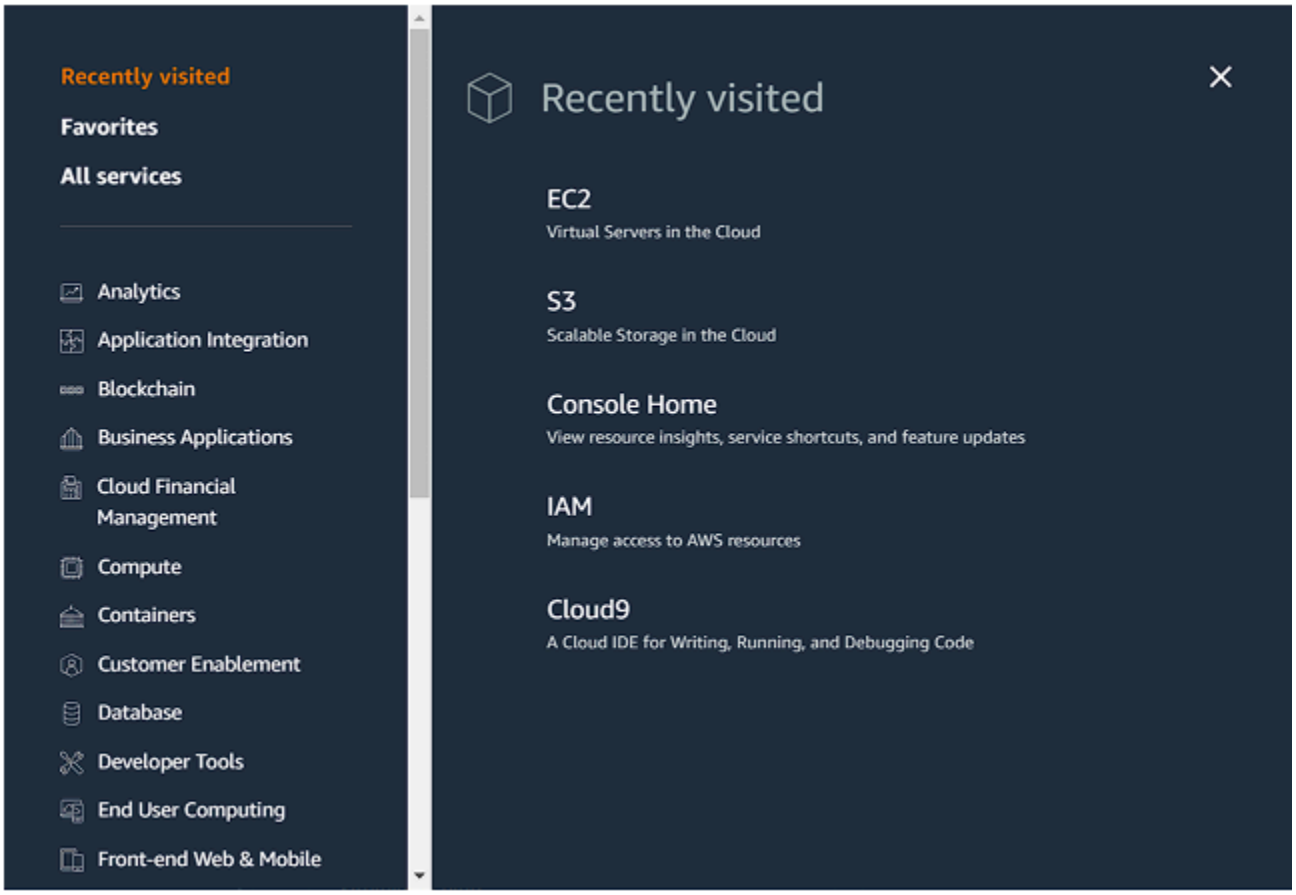
403 Forbidden

- Code: AccessDenied
- Message: Access Denied
- RequestId: KS0XA8XZTXSSDHKH
- 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

AWS Test Server

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

Amazon Linux | macOS | Ubuntu | Windows | Red Hat | SUSE Li

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-0c14f530901e49ff (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:

- [x] Allow SSH traffic from — Anywhere 0.0.0.0/0
  Helps you connect to your instance
- [ ] 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 | 8 | GiB | gp3 | Root volume (Not encrypted)

ⓘ Free tier eligible customers can get up to 30 GB 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 > i-033e8bf30d3d5ed91 > Connect to instance

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

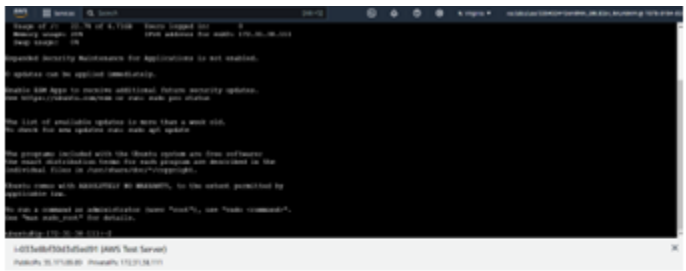
Note: In most cases, the default username, ubuntu, is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI username.

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:

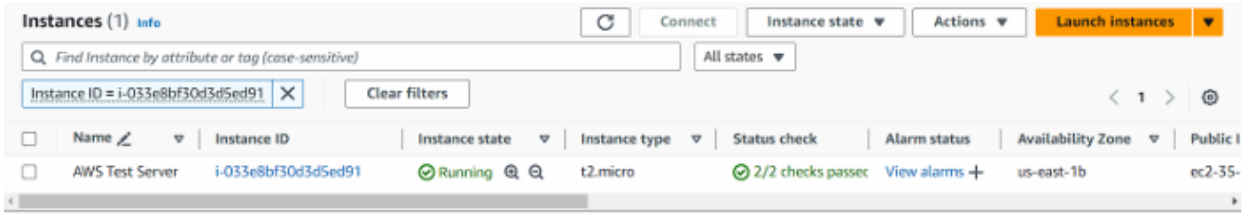
- ec2-instance-connect:SendSshPublicKey
- ec2:DescribeInstances

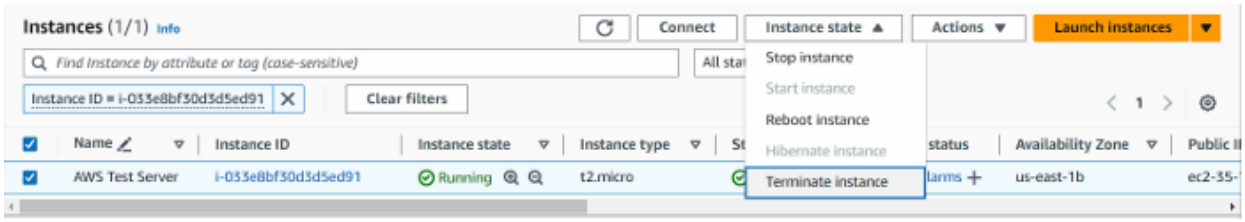
Consider restricting access to specific EC2 instances using ec2:osuser condition, or specific resource tag.
Visit IAM Console to verify if you have above permissions.
For more information about IAM policy examples, see Grant IAM permissions for EC2 Instance Connect.

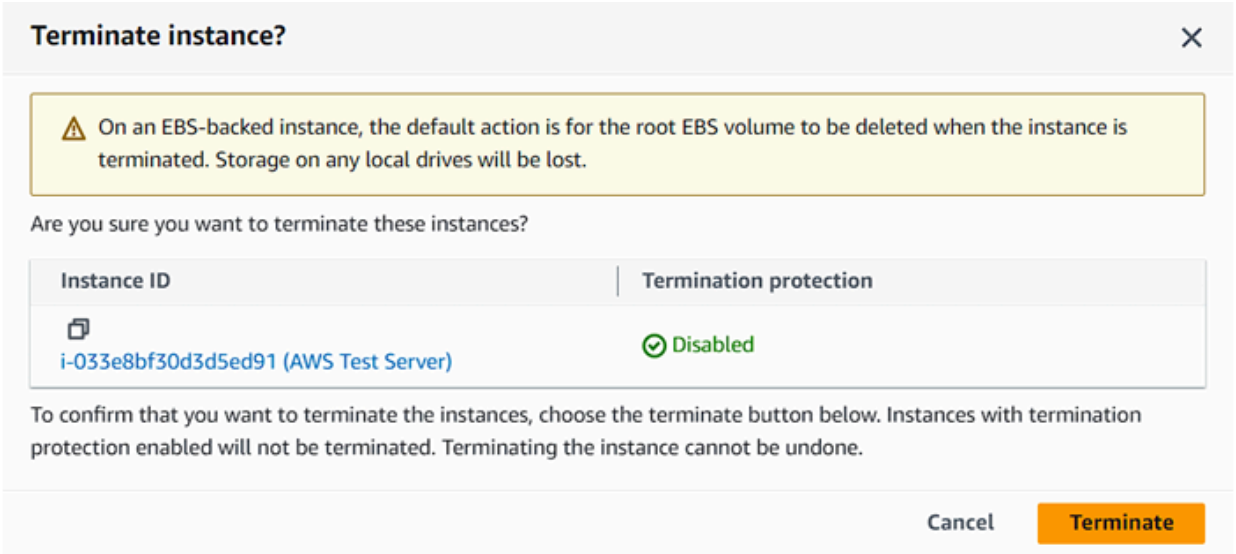
Cancel | Connect

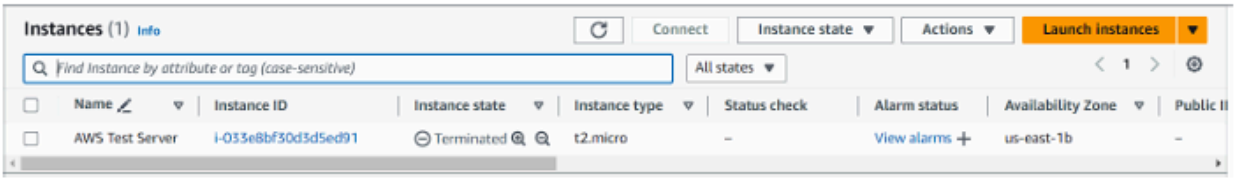



```
ubuntu@ip-172-31-38-111:~$ ping www.google.com
PING www.google.com (142.251.167.106) 56(84) bytes of data.
64 bytes from ww-in-f106.1e100.net (142.251.167.106): icmp_seq=1 ttl=58 time=2.22 ms
64 bytes from ww-in-f106.1e100.net (142.251.167.106): icmp_seq=2 ttl=58 time=2.24 ms
64 bytes from ww-in-f106.1e100.net (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 1603612   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       104832    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
```



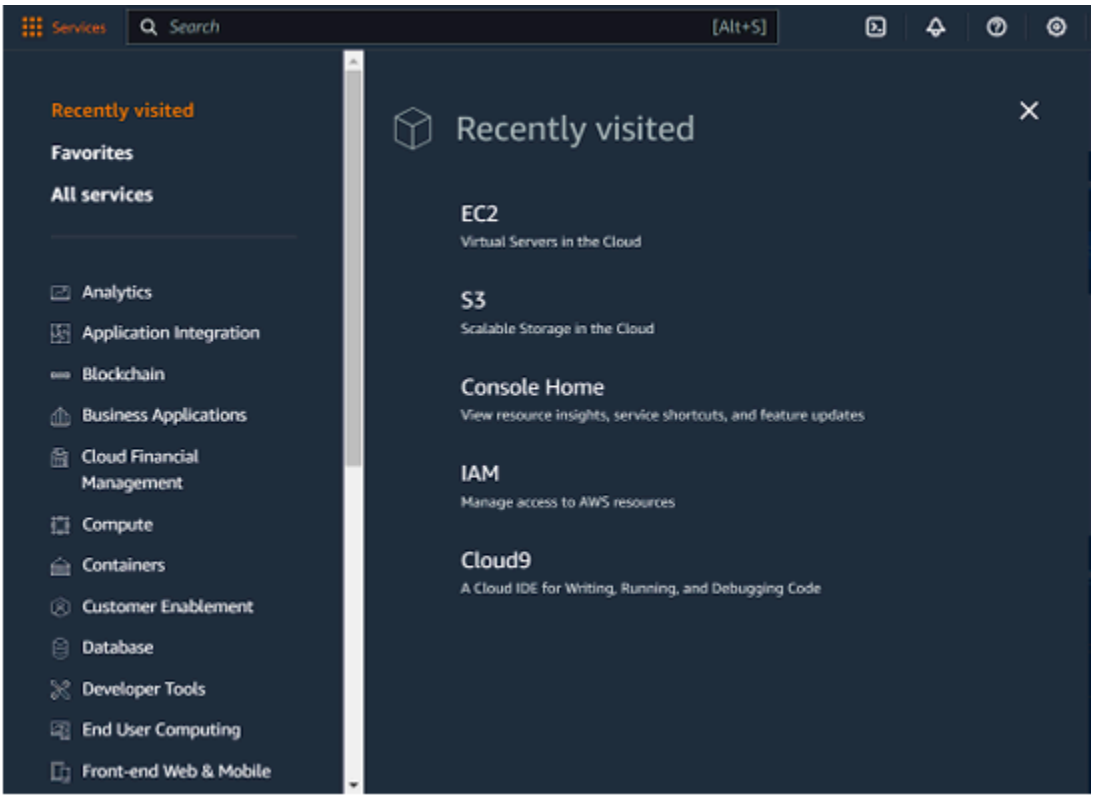






Cloud 9 - IDE

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



2) Click on Create Enviornment 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

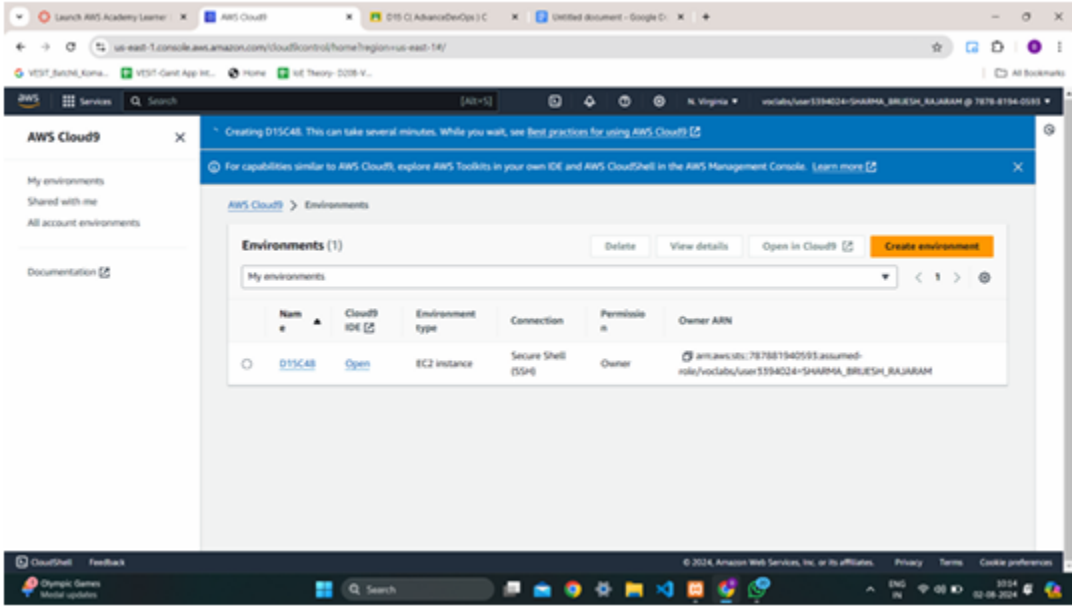
Connection

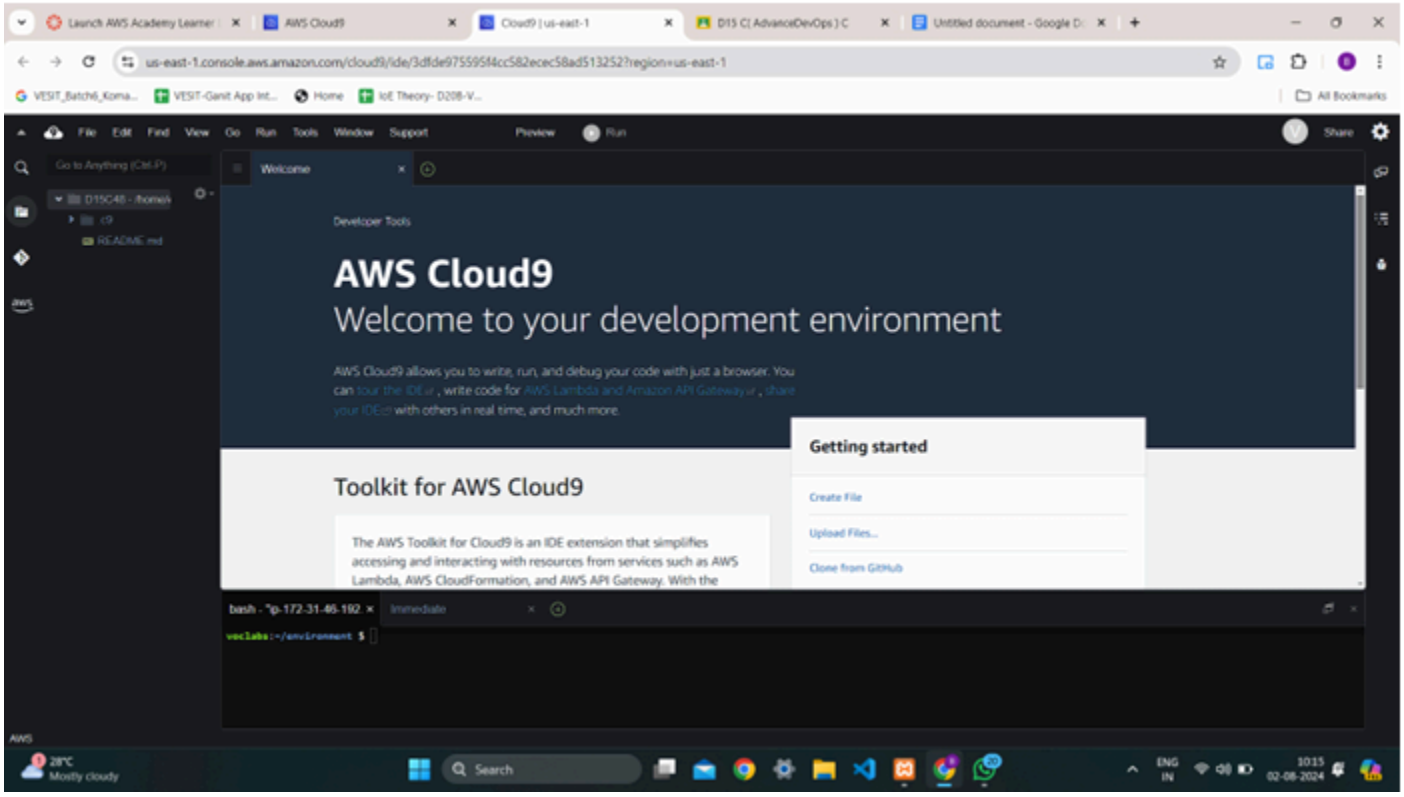
How your environment is accessed.

- (●) **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.

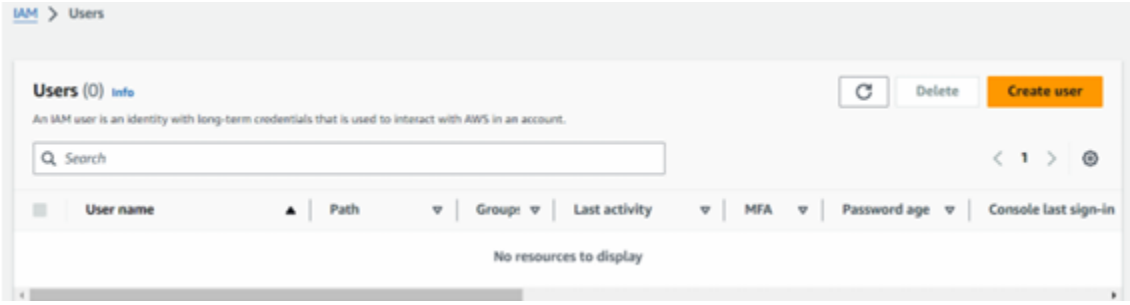
▶ **VPC settings** Info

5) Environment created successfully.

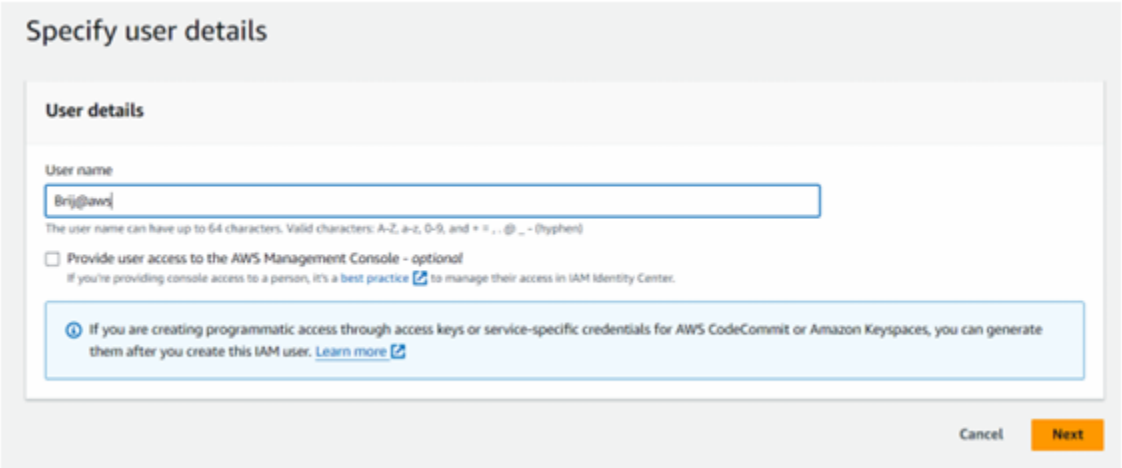




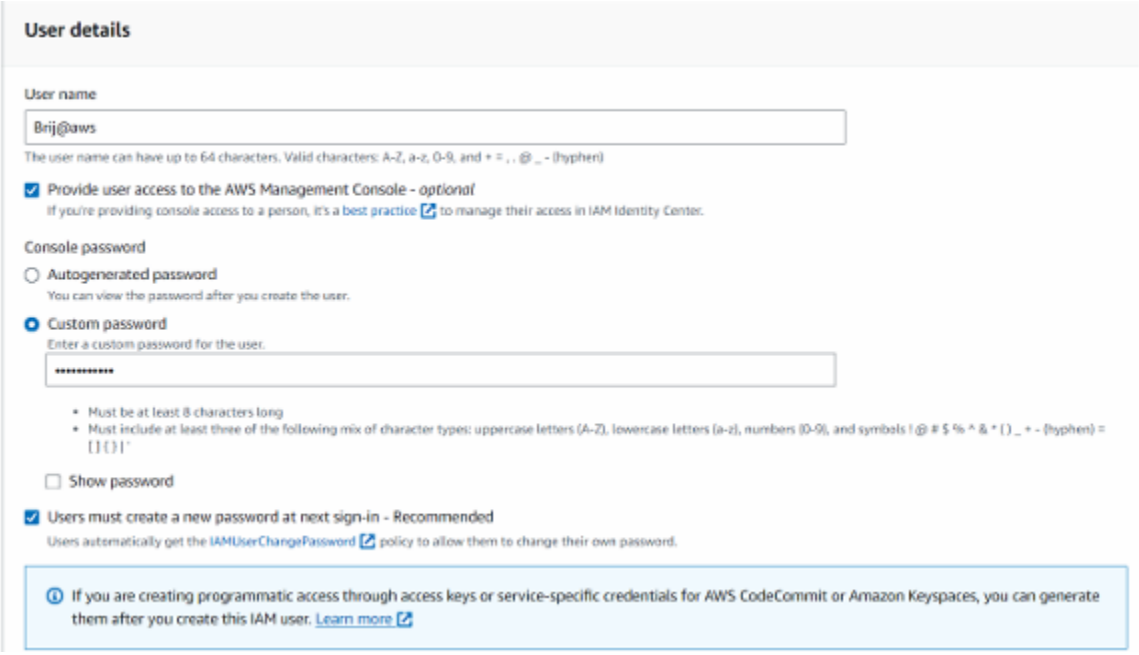
6) Create user using the IAM.



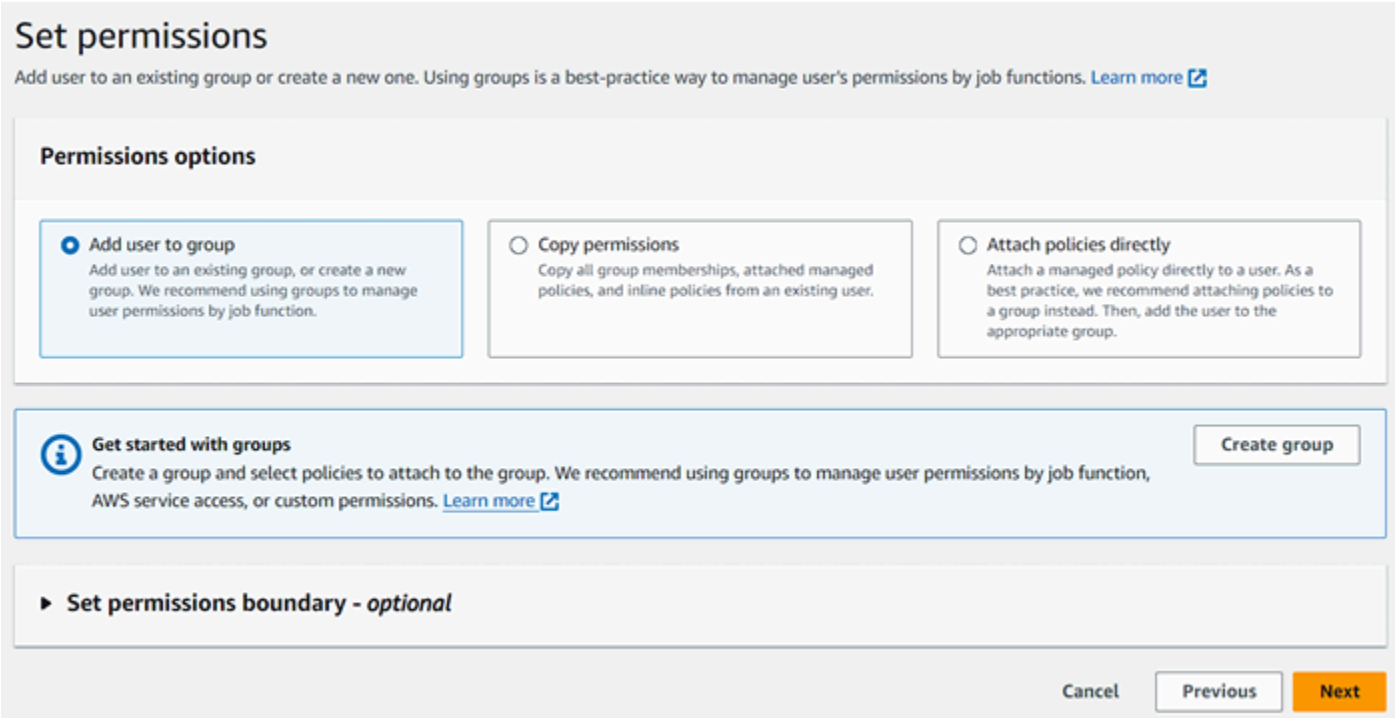
7) Add the username



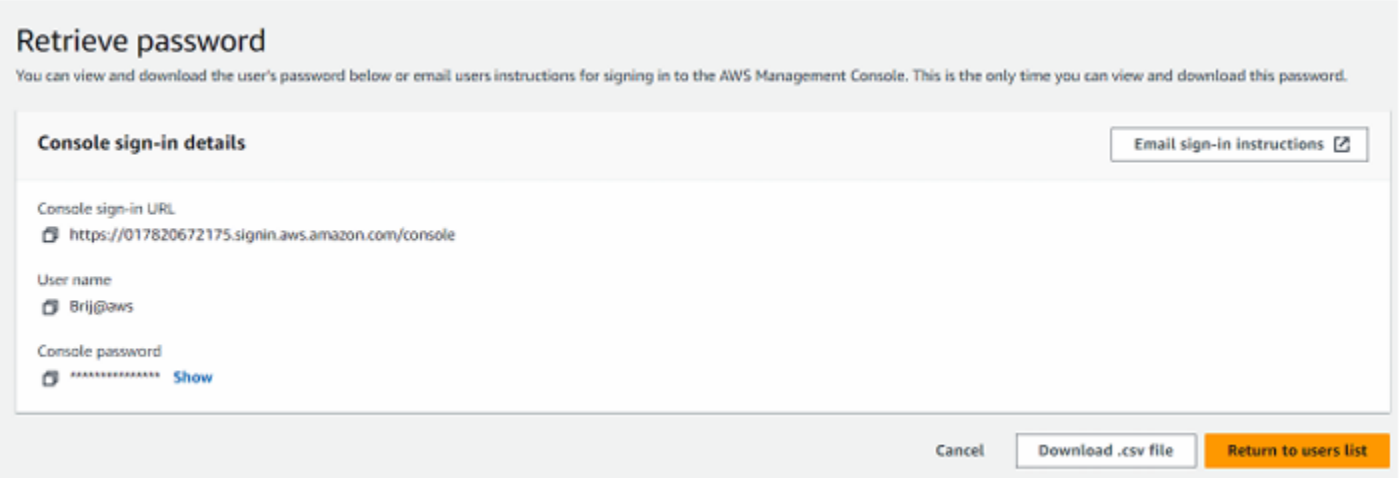
8) Add the remaining user details and provide access to the AWS Management Console



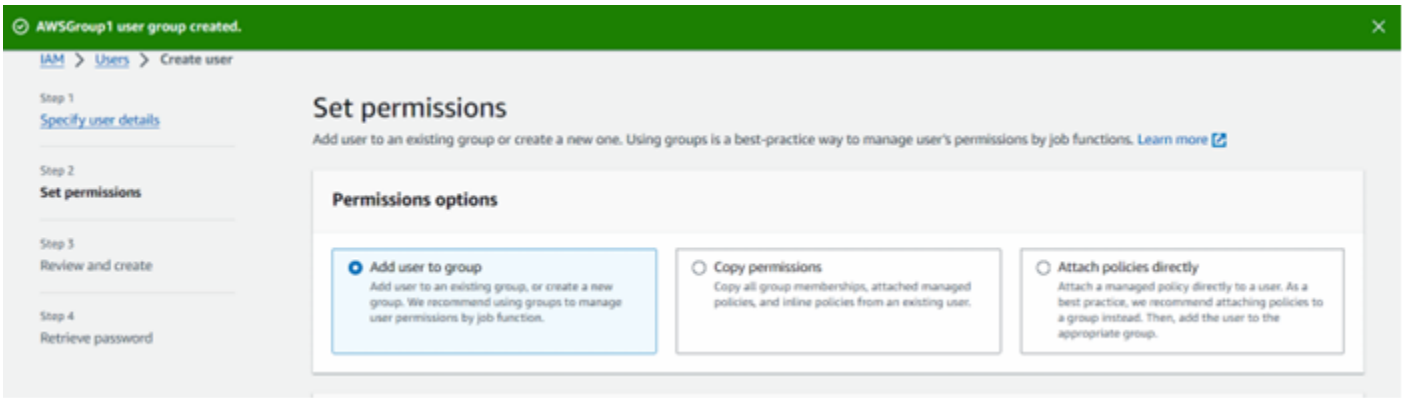
9) User created successfully and can be added to user groups.



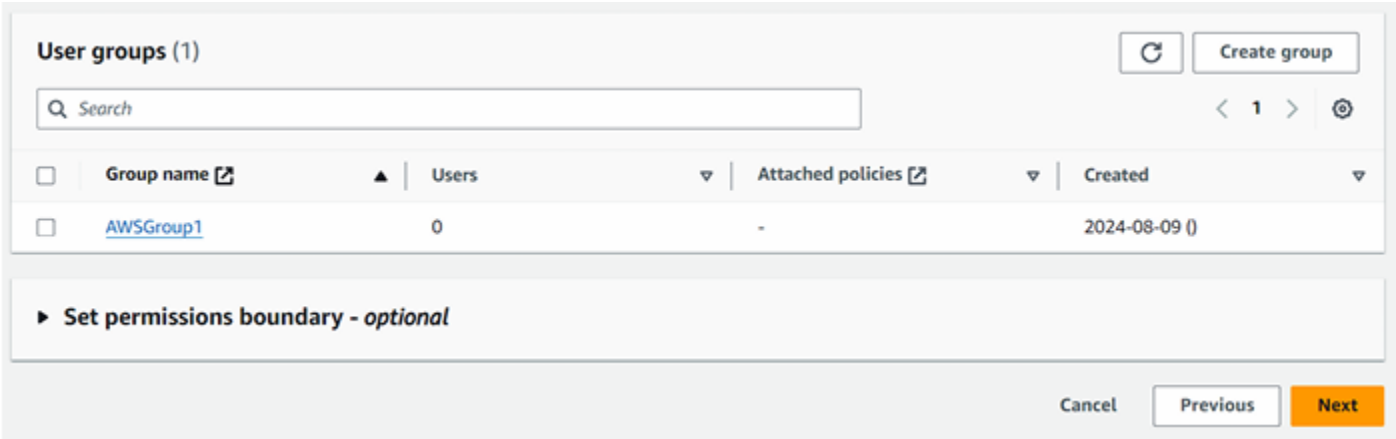
10) User credentials can be downloaded.



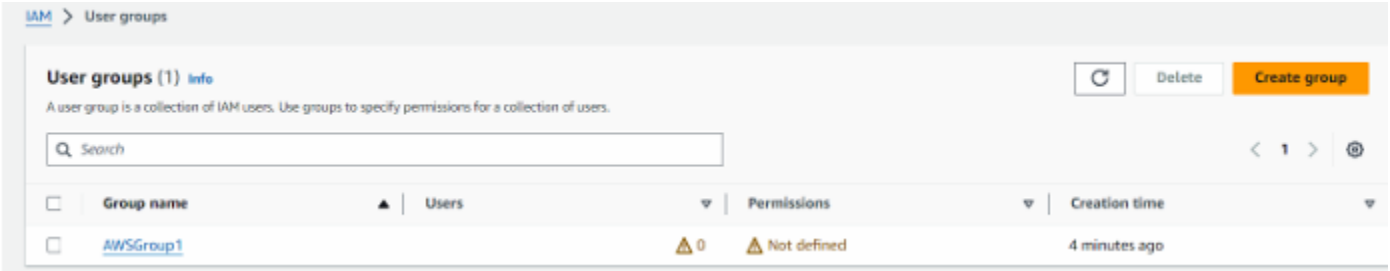
11) Add user to group if group exists else create a new group.



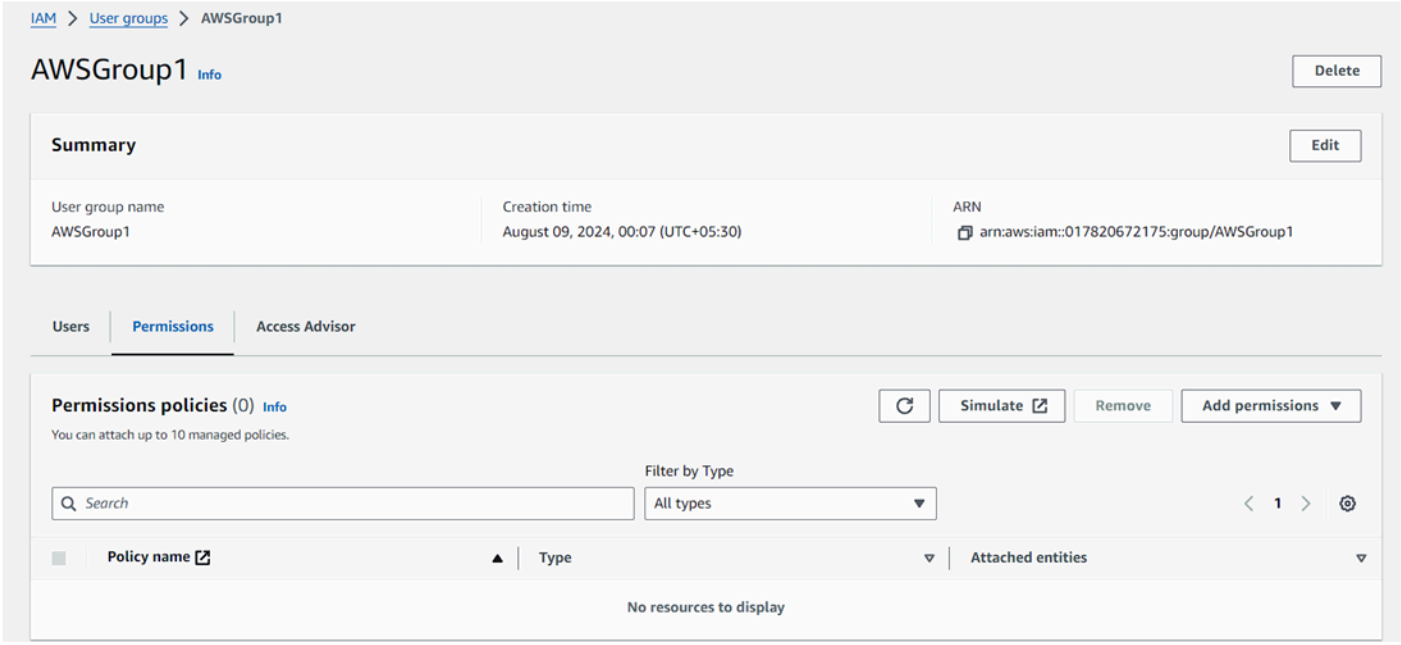
12) Write the user group name and proceed.



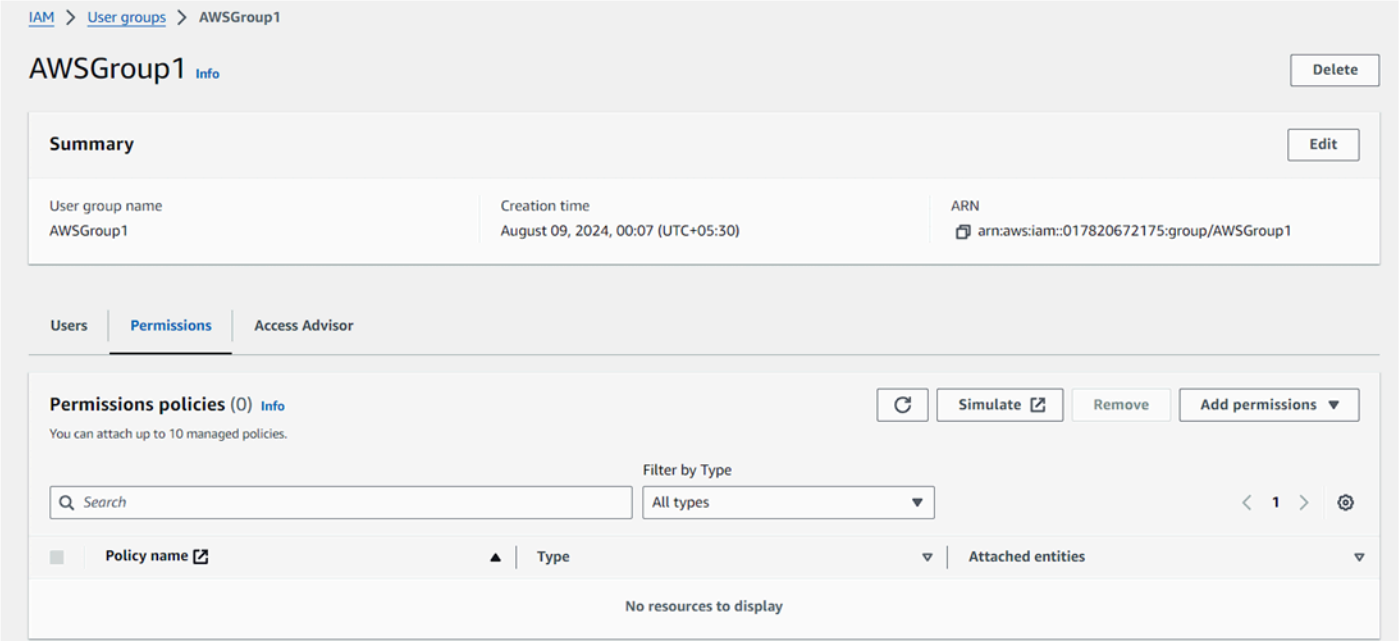
13) Click on *group_name.*



14) Go to Add permissions and click on Add Permissions



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



16) User group is created successfully.