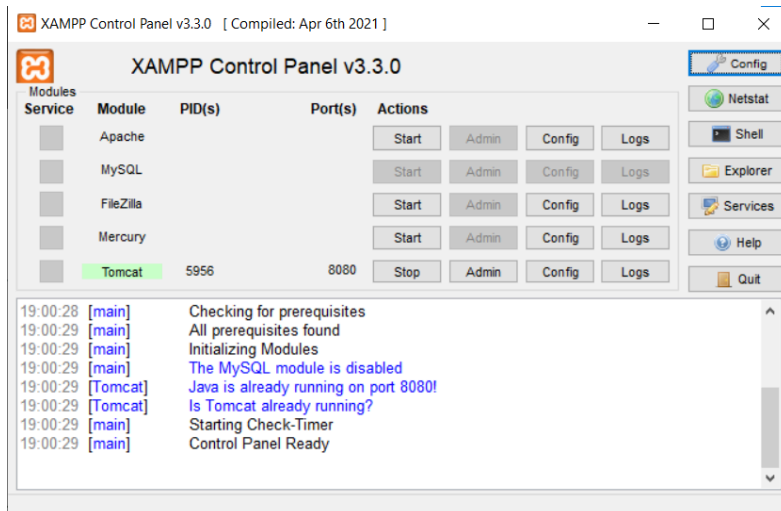


Experiment 1A

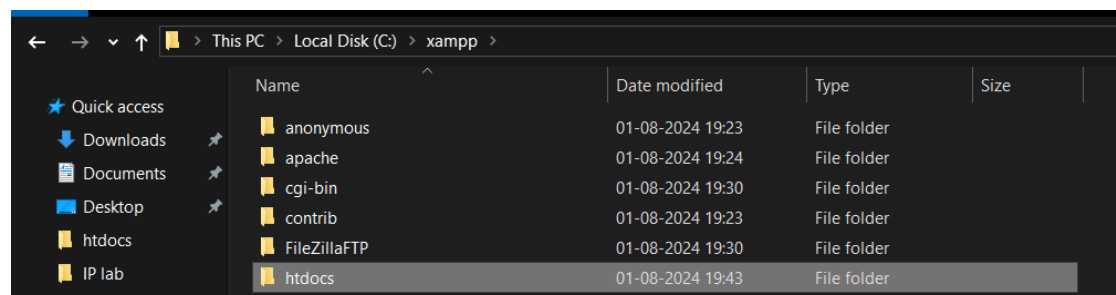
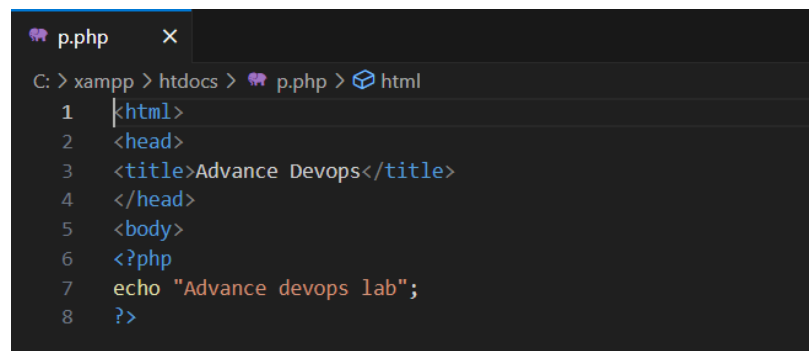
Part 1: To develop a website and host it on Xampp:

Step 1: Go to the official website of Xampp. <https://www.apachefriends.org/download.html>.
Select the suitable version and complete the installation.

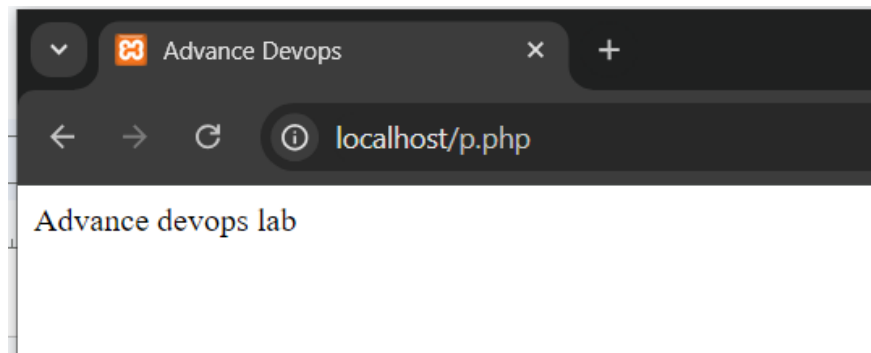
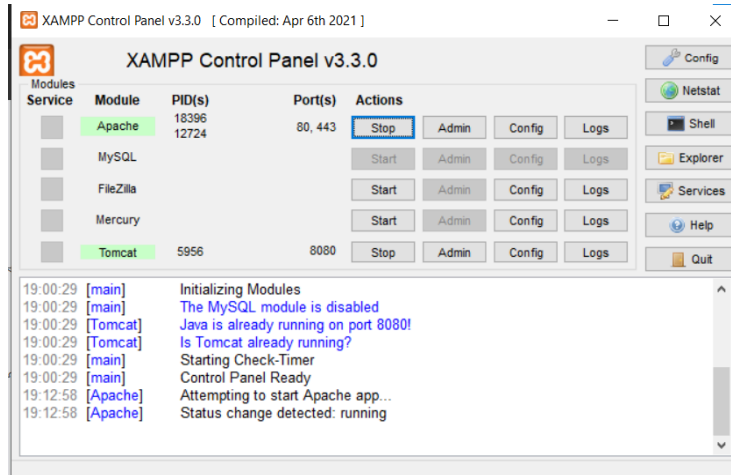
Step 2: After installation open the Xampp control panel, we need to start the Apache server to host the website.



Step 3: Setup a php project, create a php project and save it as .php file. The file should be saved in 'htdocs' folder present in the 'Xampp' folder created after installation.



Step 4: Start the Xampp server and go to localhost in browser. Edit the URL such that it is localhost/filename.php or localhost/folder_name .

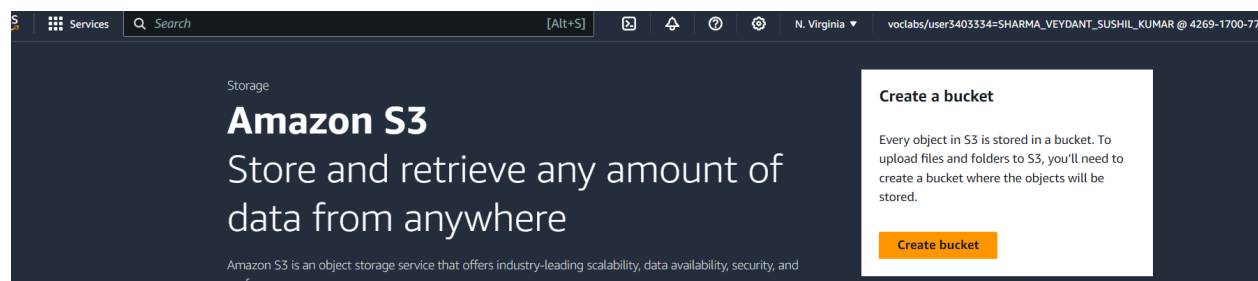
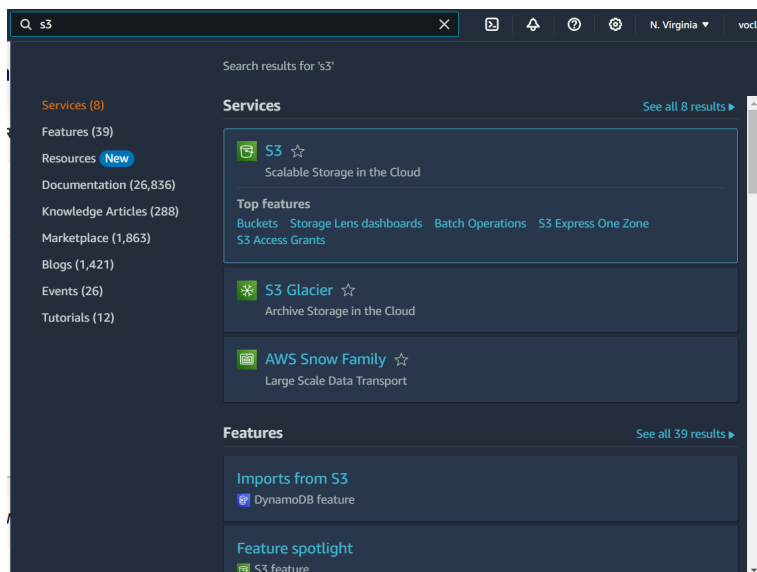


Our website has now been hosted using xampp

Part 2: Hosting a static website on AWS S3.

Step1: Login to AWS Academy and launch learner's lab.

Step 2: Search for the S3 service and Create a bucket.



Step 3: Fill in the details and name your bucket. Use default settings. Uncheck the “Block all public access” box to prevent error.

General configuration

AWS Region

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

Bucket type

☒ 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

veydant-bucket

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

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 applications 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 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.

Once completed, Click 'Create Bucket'.

Successfully created bucket "veydant-bucket"

To upload files and folders, or to configure additional bucket settings, choose [View details](#).

Amazon S3 > Buckets

Account snapshot - updated every 24 hours

[View Storage Lens dashboard](#)

General purpose buckets

Directory buckets

General purpose buckets (1)

[Info](#)

All AWS Regions

Buckets are containers for data stored in S3.

Find buckets by name

< 1 > ⚙

Name	AWS Region	IAM Access Analyzer	Creation date
veydant-bucket	US East (N. Virginia) us-east-1	View analyzer for us-east-1	August 8, 2024, 19:27:53 (UTC+05:30)

Step 4: Open the bucket and click on upload in the objects tab.

Objects

Properties

Permissions

Metrics

Management

Access Points

Objects (0)

[Info](#)

Copy S3 URI

Copy URL

Download

Open

Delete

Actions

Create folder

Upload

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

< 1 > ⚙

Name	Type	Last modified	Size	Storage class
No objects				
You don't have any objects in this bucket.				
<div>Upload</div>				

Drag and drop files and folders you want to upload here, or choose [Add files](#) or [Add folder](#).

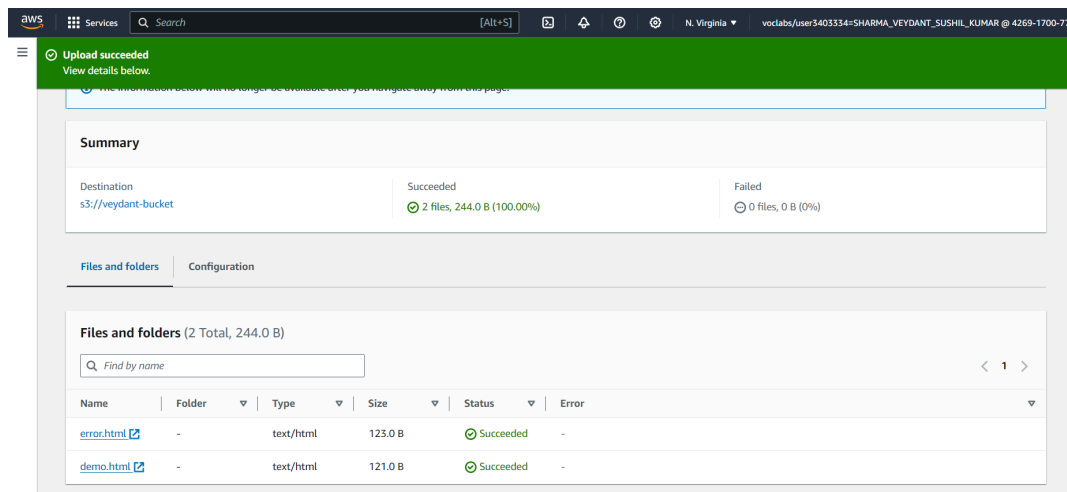
Files and folders (2 Total, 244.0 B)

All files and folders in this table will be uploaded.

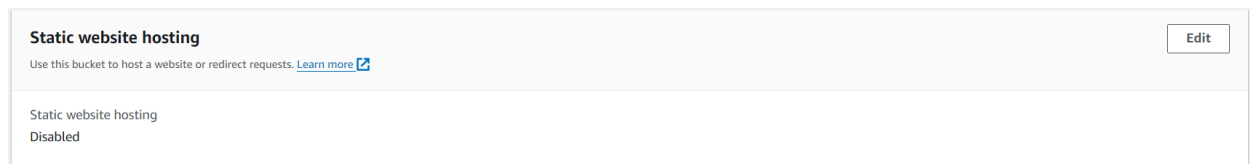
Find by name

< 1 >

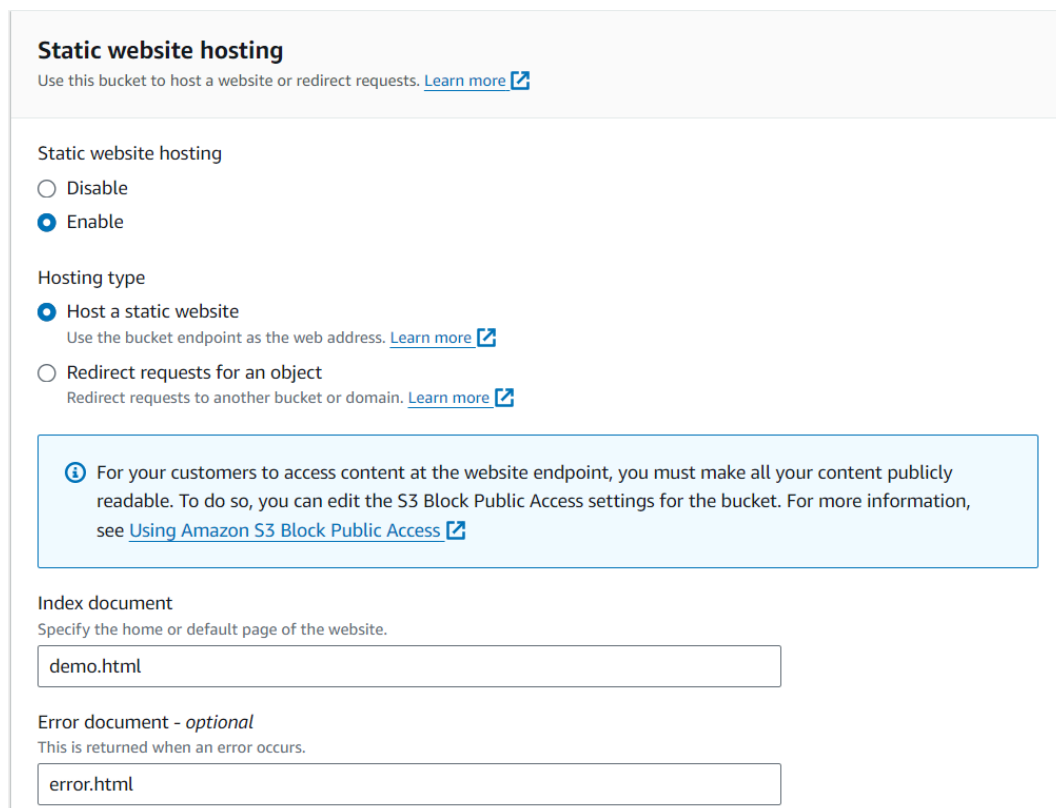
After adding the files click on upload files.



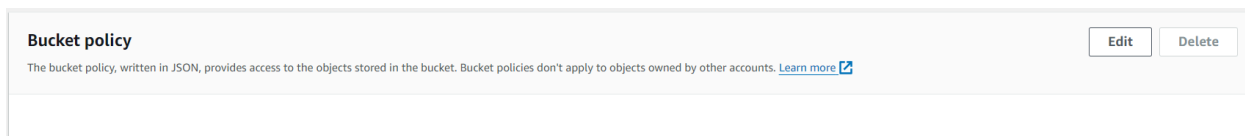
Step 5: Go to the properties tab and navigate to the “Static website hosting” section and click on edit , then click on enable.



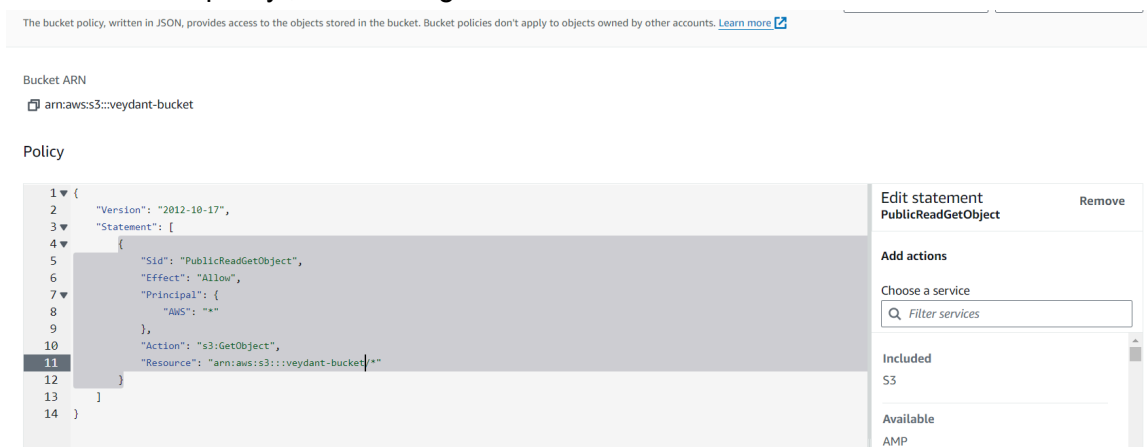
Specify the document/filenames and click on save changes.



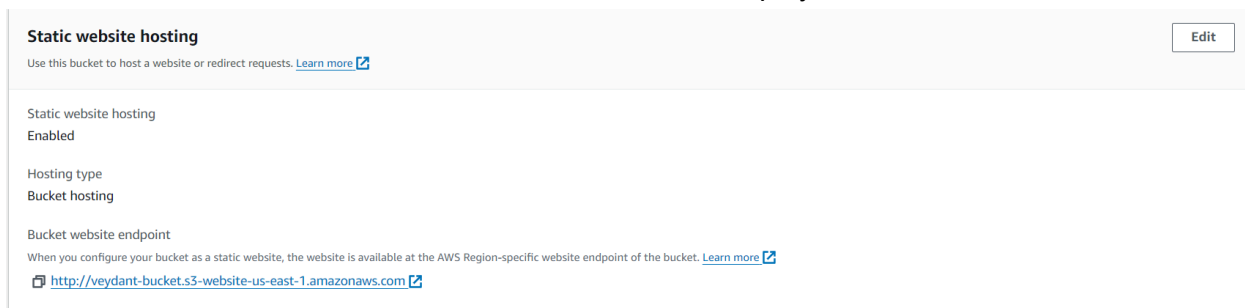
Step 6: Head to the Permissions tab and navigate to the “Bucket Policy” section and click on edit.



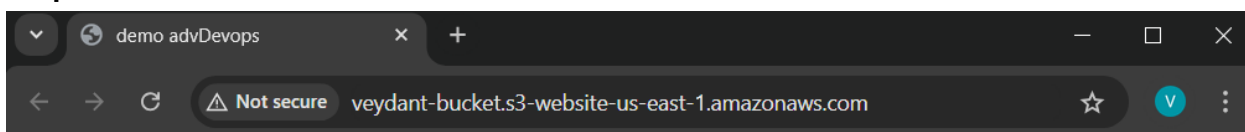
Add the bucket policy , save changes and exit.



Step 7: Once the Bucket policy has been updated , navigate back to “Static website hosting”, a link will be available, click on the link to view the hosted/deployed website.



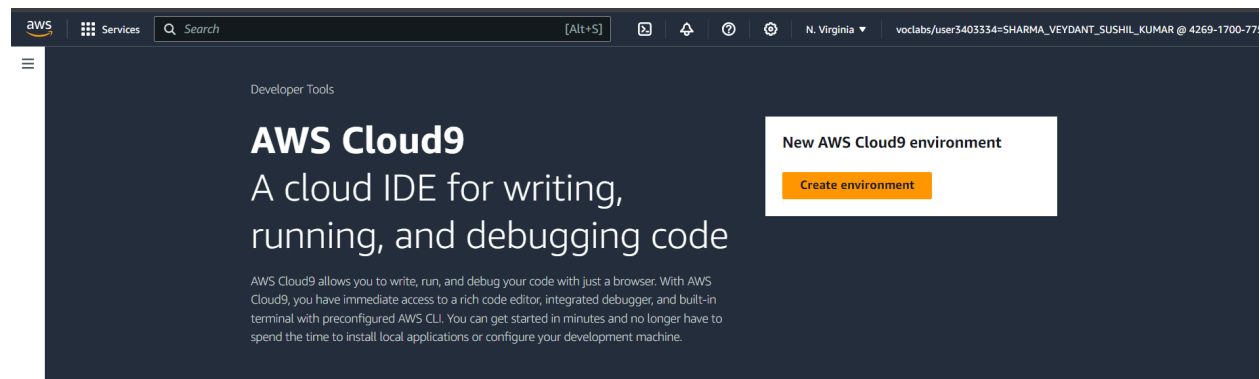
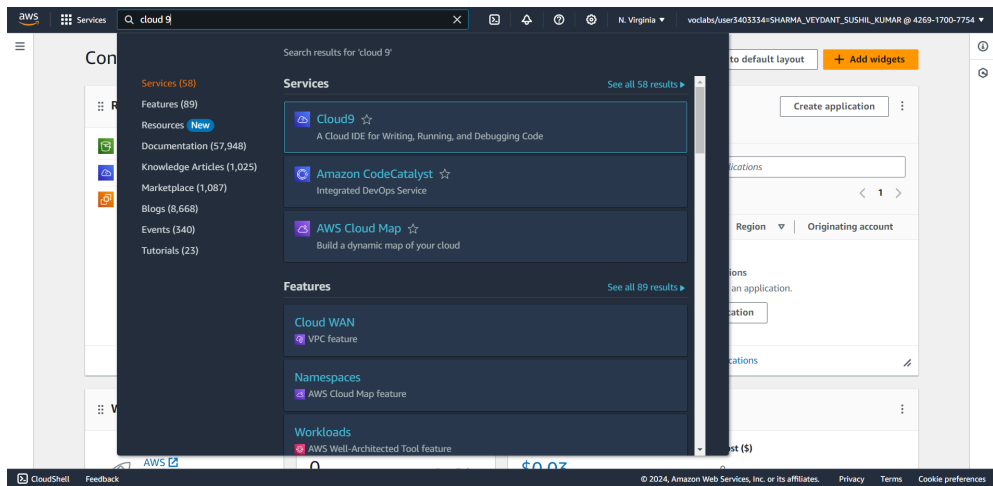
Output:



Experiment 1B

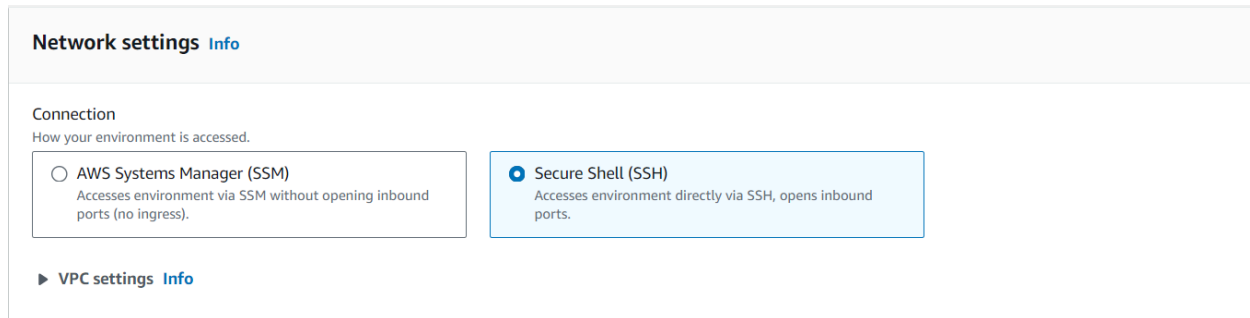
Aim: To understand the benefits of Cloud Infrastructure and Setup AWS Cloud9 IDE, Launch AWS Cloud9 IDE and Perform Collaboration Demonstration.

Step 1: Navigate to Cloud 9 service



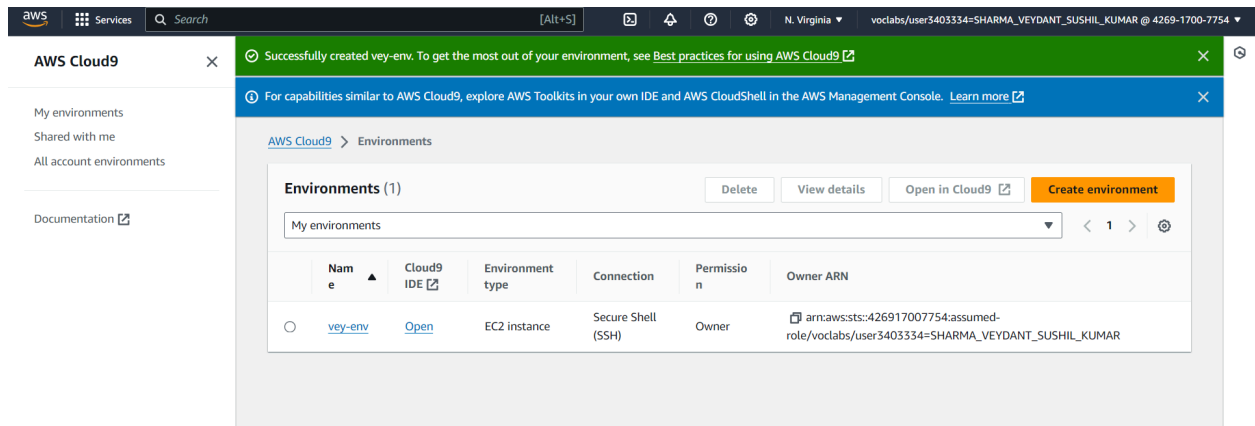
Step 2: Create Environment

A screenshot of the AWS Cloud9 'Create environment' form. The breadcrumb navigation at the top shows 'AWS Cloud9 > Environments > Create environment'. The main heading is 'Create environment' with a link to 'Info'. The form is divided into two main sections: 'Details' and 'Environment type'. In the 'Details' section, there is a 'Name' field with the value 'vey-env' and a note 'Limit of 60 characters, alphanumeric, and unique per user.' Below this is a 'Description - optional' field with a note 'Limit 200 characters.' In the 'Environment type' section, there are two radio buttons: 'New EC2 instance' (selected) and 'Existing compute'. The 'New EC2 instance' option has a note: 'Cloud9 creates an EC2 instance in your account. The configuration of your EC2 instance cannot be changed by Cloud9 after creation.' The 'Existing compute' option has a note: 'You have an existing instance or server that you'd like to use.'

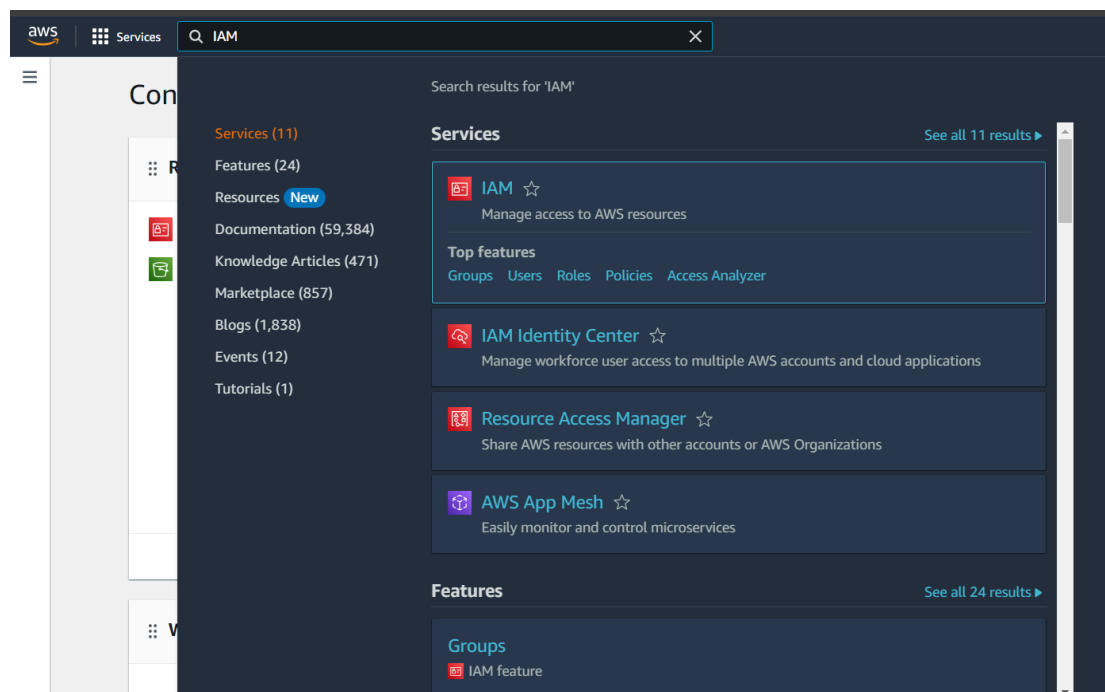


Click on “Create”

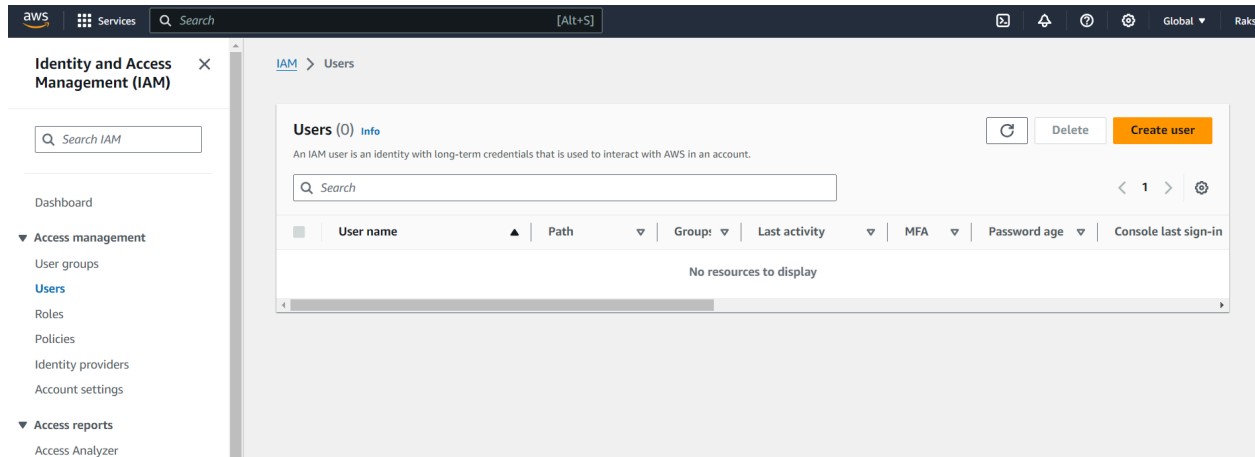
Step 3: Environment Will be created.



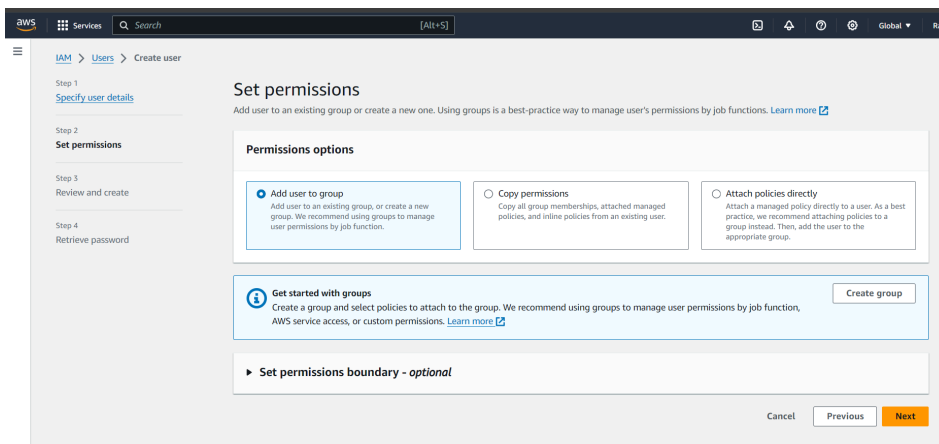
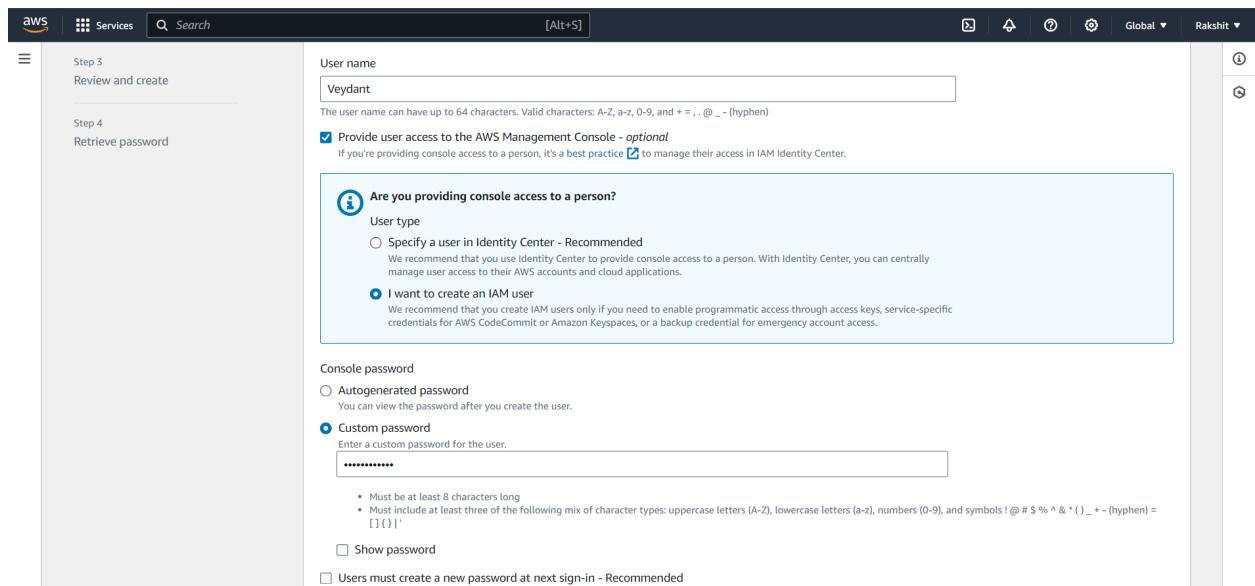
Step 4: Navigate to IAM service in AWS.



Step 5: Navigate to users tab and Create new User.



Add name, custom password. Keep the “Users create new password at next sign in” button checked



Select default settings for the rest.

User created successfully

View user

You can view and download the user's password and email instructions for signing in to the AWS Management Console.

IAM > Users > Create user

Step 1
Specify user details

Step 2
Set permissions

Step 3
Review and create

Step 4
Retrieve password

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://975050293750.signin.aws.amazon.com/console

User name
Veydant

Console password
***** Show

Cancel

Download .csv file

Return to users list

Step 6: Navigate to User groups tab.

aws

Services

Search

[Alt+S]

Global

Rakshit

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Access reports

Access Analyzer

External access

Unused access

Analyzer settings

Credential report

Organization activity

IAM > User groups

User groups (0) Info

A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

Search

< 1 >

Group name

Users

Permissions

Creation time

No resources to display

Create group

aws

Services

Search

[Alt+S]

Global

Rakshit

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Access reports

User group name

Enter a meaningful name to identify this group.

D15C_50

Maximum 128 characters. Use alphanumeric and '+', '@', '_' characters.

Add users to the group - Optional (1) Info

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

Search

< 1 >

☐

User name

Groups

Last activity

Creation time

☐

Veydant

0

None

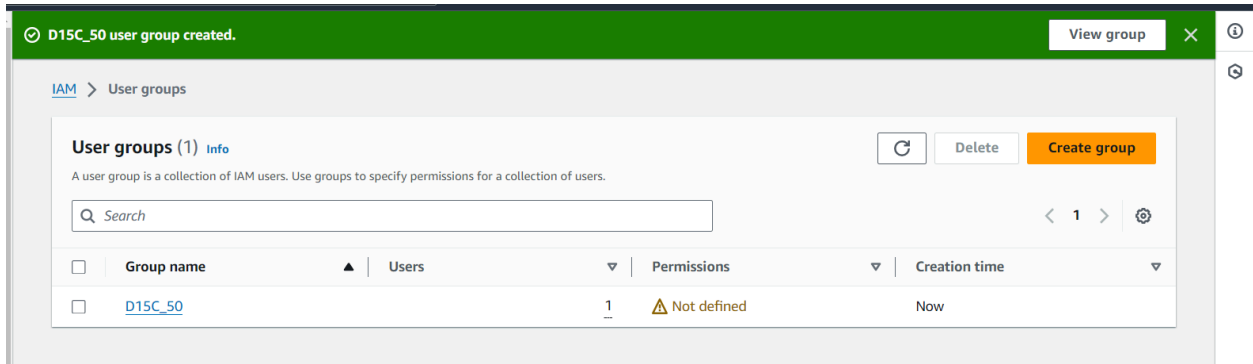
1 minute ago

Attach permissions policies - Optional (945) Info

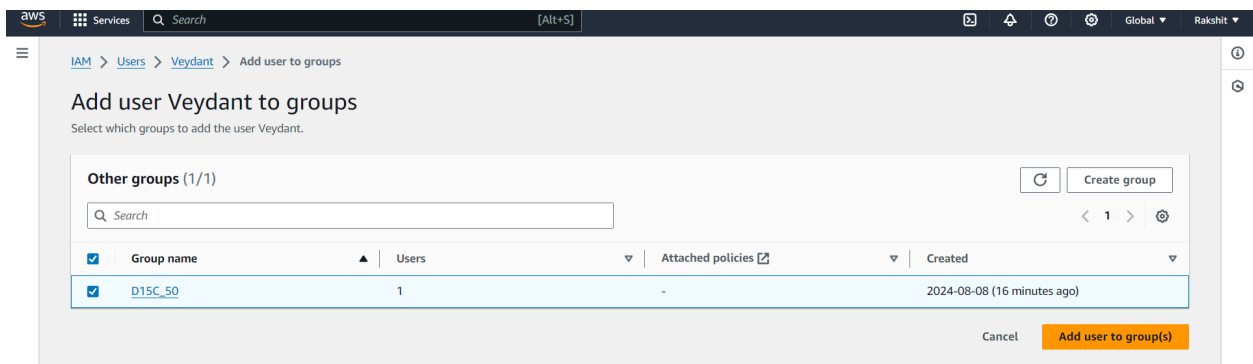
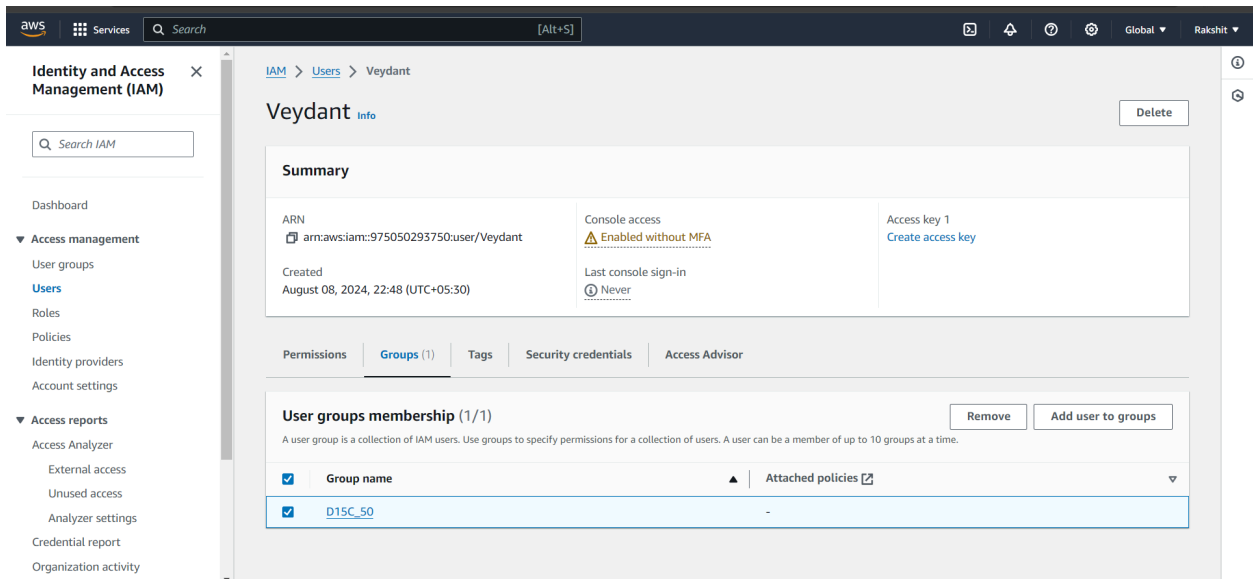
You can attach up to 10 policies to this user group. All the users in this group will have permissions that are defined in the selected policies.

Filter by Type

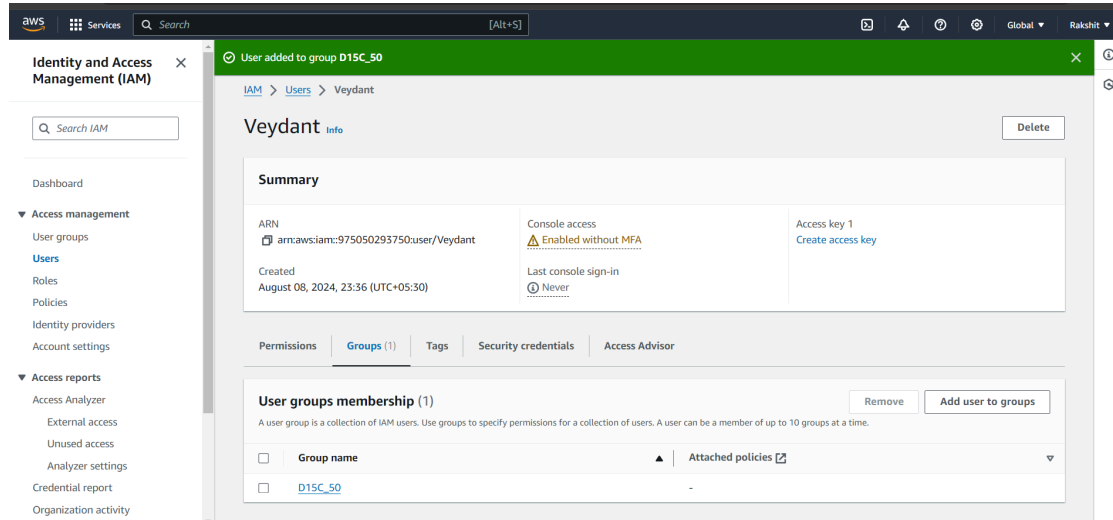
Create a new user group.



Step 7: Navigate to Users tab , go to Groups tab and add User to the group.



Veydant Sharma D15C 50 Adv DevOps



The user has been added to the the user group.

Step 8 : Navigate to the permissions tab in User group, select “AWSCloud9EnvironmentMember” and add the permissions.

