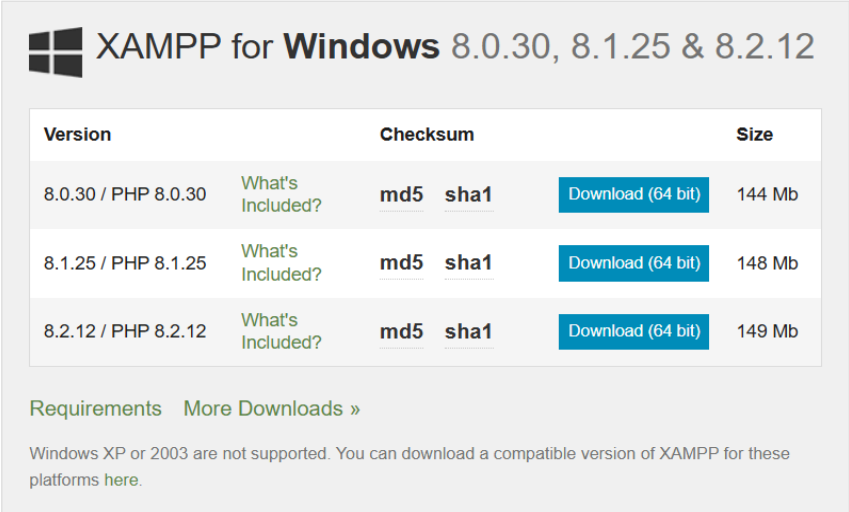


Aim : To develop a website and host it on your local machine on a VM

1. Find a web server that supports PHP and MYSQL

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

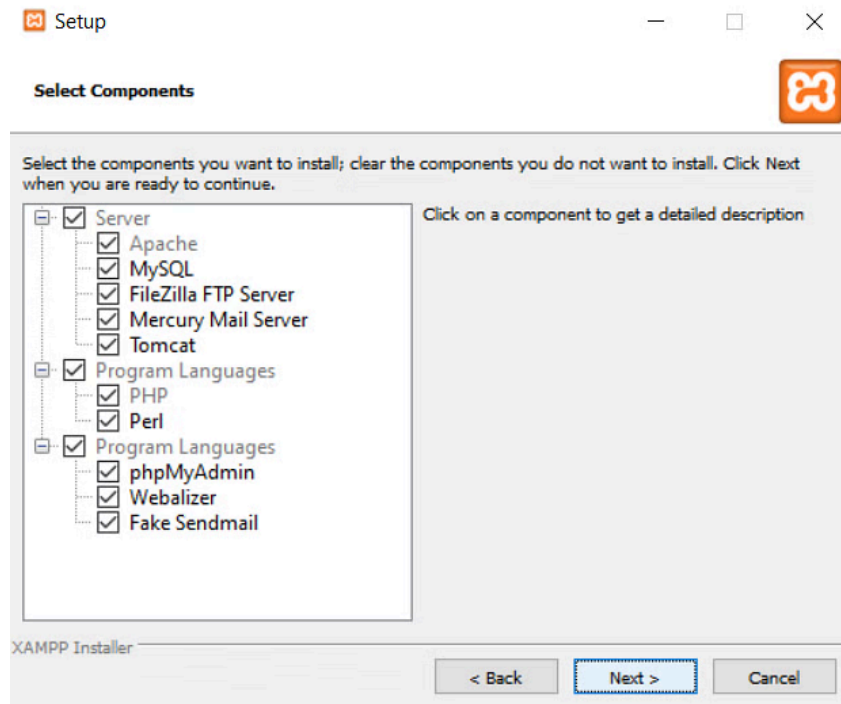
Version	Checksum	Size
8.0.30 / PHP 8.0.30 What's Included?	md5 sha1	Download (64 bit) 144 Mb
8.1.25 / PHP 8.1.25 What's Included?	md5 sha1	Download (64 bit) 148 Mb
8.2.12 / PHP 8.2.12 What's Included?	md5 sha1	Download (64 bit) 149 Mb

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

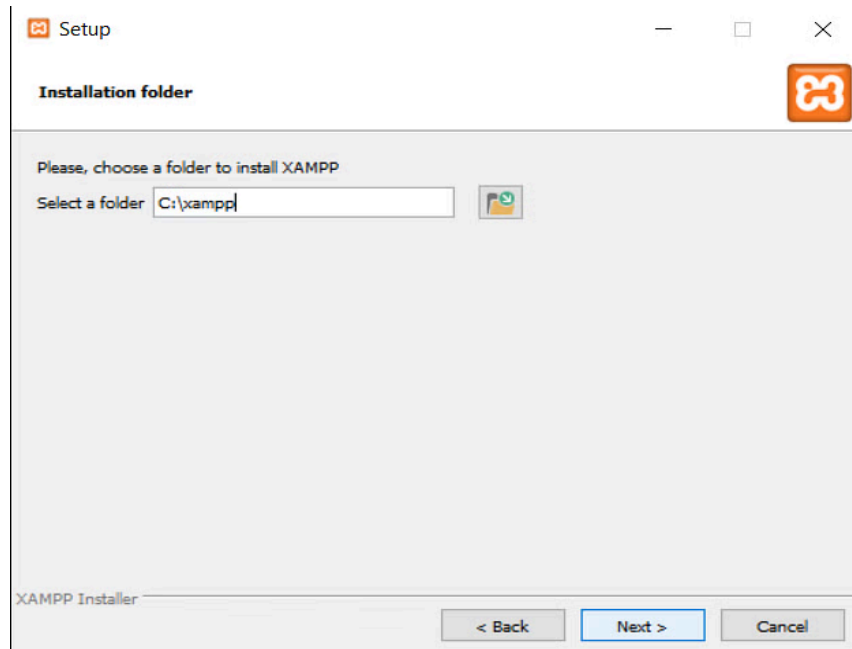
Windows XP or 2003 are not supported. You can download a compatible version of XAMPP for these platforms [here](#).

2. Download the latest version of Xampp and MYSQL DB

3. Once downloaded setup and begin the installation process and, in the “Select Components” section, select all the required components



4. Keep the default directory “C:\xampp” and click on “next” to complete the installation.



5. Go to “C:\xampp\htdocs” and inside it, create a folder called demo (or any name you want)

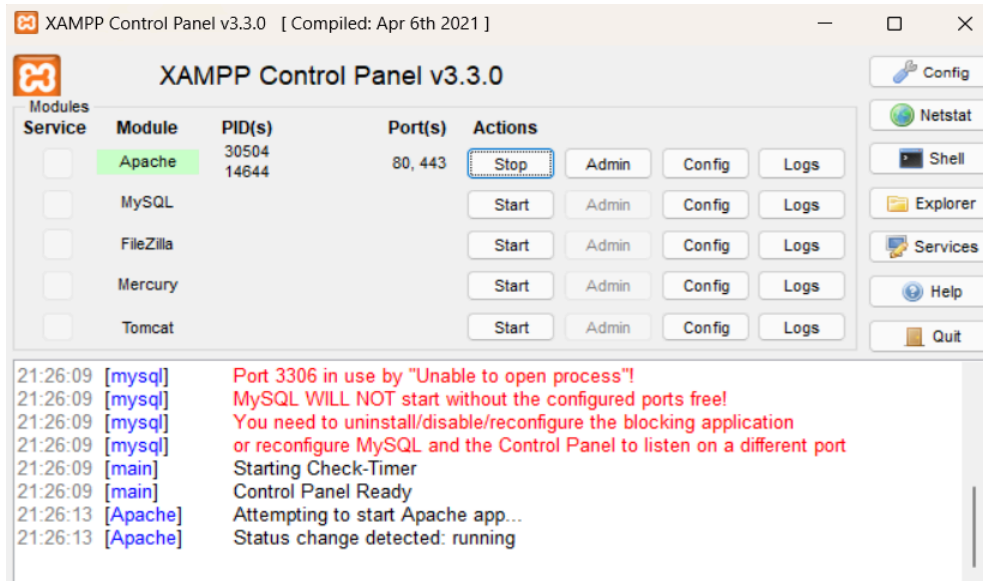
> This PC > OS (C:) > xampp > htdocs >

Name	Date modified	Type	Size
dashboard	09-04-2021 01:26	File folder	
demo	09-04-2021 01:30	File folder	
img	09-04-2021 01:26	File folder	
webalizer	09-04-2021 01:26	File folder	
xampp	09-04-2021 01:26	File folder	
applications.html	27-08-2019 19:32	Microsoft Edge HT...	4 KB
bitnami.css	27-08-2019 19:32	Cascading Style Sh...	1 KB
favicon.ico	16-07-2015 21:02	Icon	31 KB
index.php	16-07-2015 21:02	PHP File	1 KB

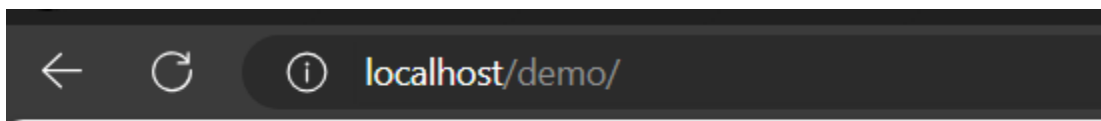
6. Open the folder and create a file name “index.php” and write the required script

```
index.php X
C: > xampp > htdocs > demo > index.php
1  <?php
2
3
4  echo "Dynamic Hosting through apache server for lab of adv devops";
5
6
7
```

7. To see the script output, open the XAMPP control panel and start Apache to host the local web server, where our script will be running.



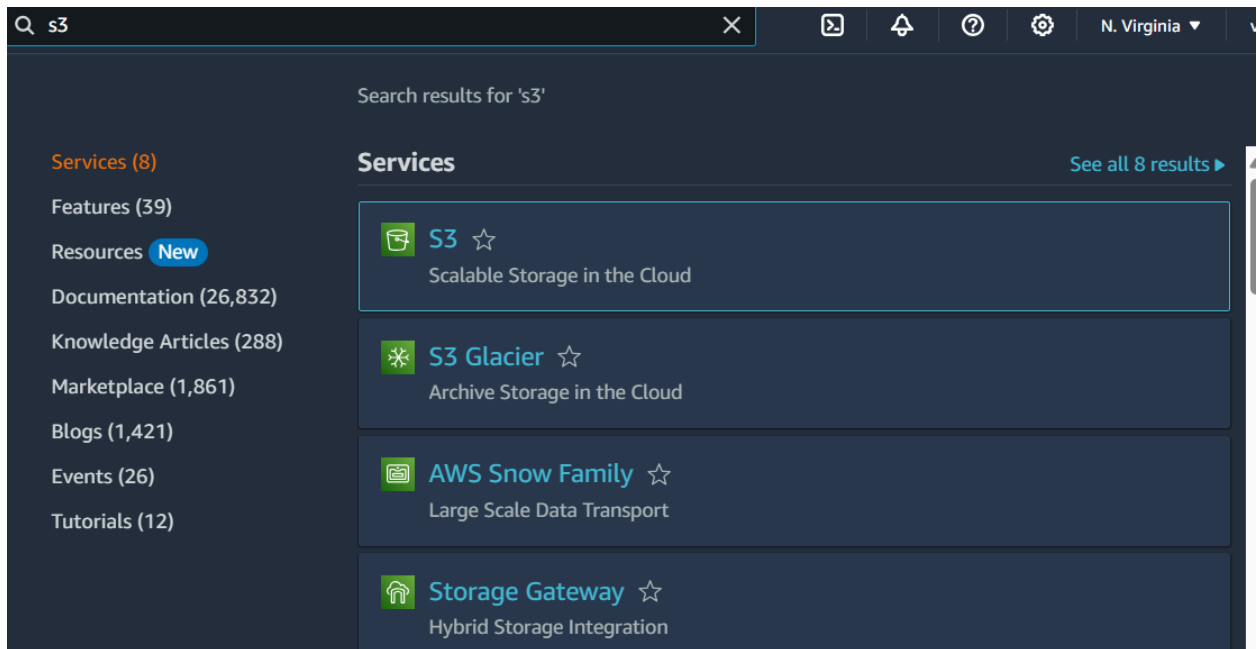
8. Navigate to your browser and type in “localhost/demo/” in the address bar to view the output.



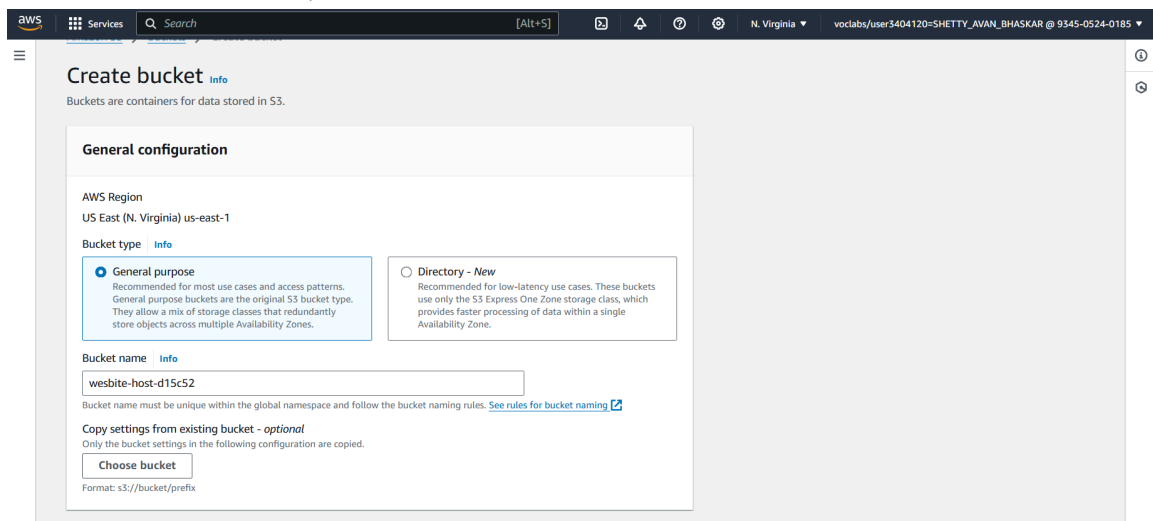
Dynamic Hosting through apache server for lab of adv devops

AWS S3 BUCKET:

1. Open the aws Console and search for S3 bucket



2. Now create a bucket of <-your name-> mine as 'website-host-d15c-52'



3. Scroll down and uncheck the Block of public access (as we are making our static website available for all users in public domain)

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.

⚠ **Turning off block all public access might result in this bucket and the objects within becoming public**

AWS recommends that you turn on block all public access, unless public access is required for specific and verified use cases such as static website hosting.

4. Click on Create bucket option

aws

Services

Search

[Alt+S]

N. Virginia

voclabs/user3404120-SHETTY_AVAN_BHASKAR @ 9345-0524-0185

Default encryption [Info](#)

Server-side encryption is automatically applied to new objects stored in this bucket.

Encryption type [Info](#)

☒ Server-side encryption with Amazon S3 managed keys (SSE-S3)

☐ Server-side encryption with AWS Key Management Service keys (SSE-KMS)

☐ Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)

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

☐ Disable

☒ Enable

► Advanced settings

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

Cancel

Create bucket

5. You go back to your buckets page and see the bucket has been created

General purpose buckets

Directory buckets

General purpose buckets (1) [Info](#) All AWS Regions

↺

Copy ARN

Empty

Delete

Create bucket

Buckets are containers for data stored in S3.

<

1

>

⚙️

	Name	AWS Region	IAM Access Analyzer	Creation date
<input type="radio"/>	website-host-d15c52	US East (N. Virginia) us-east-1	View analyzer for us-east-1	August 7, 2024, 20:36:25 (UTC+05:30)

6. Now upload your static website folder or files, including any images if available. Once uploaded, you will see the message 'Upload successful'

[Amazon S3](#) > [Buckets](#) > [website-host-d15c52](#) > Upload

Upload [Info](#)

Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDK or Amazon S3 REST API. [Learn more](#)

Drag and drop files and folders you want to upload here, or choose **Add files** or **Add folder**.

Files and folders (1 Total, 1.9 KB) [Remove](#) [Add files](#) [Add folder](#)

All files and folders in this table will be uploaded.

< 1 >

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

Upload succeeded
View details below.

Upload: status [Close](#)

The information below will no longer be available after you navigate away from this page.

Summary

Destination s3://website-host-d15c52	Succeeded ✔ 1 file, 1.9 KB (100.00%)	Failed ✖ 0 files, 0 B (0%)
---	---	-------------------------------

7. Go to Properties and when you scroll at the bottom click edit static website hosting
Enable -> host a static website -> input the name of your file uploaded and click save

The screenshot shows the AWS Management Console interface for editing static website hosting on an S3 bucket. The breadcrumb navigation is: Amazon S3 > Buckets > wesbite-host-d15c52 > Edit static website hosting. The main heading is 'Edit static website hosting' with an 'Info' link. Below this is a section titled 'Static website hosting' with a description and a 'Learn more' link. There are two radio button options: 'Disable' and 'Enable', with 'Enable' selected. Under 'Hosting type', there are two radio button options: 'Host a static website' (selected) and 'Redirect requests for an object'. A blue information box states: '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 is the 'Index document' section with a text input field containing 'index.html'. The 'Error document - optional' section is also visible. A green success message at the bottom reads: 'Successfully edited static website hosting.' Below this is a summary page for the bucket 'wesbite-host-d15c52' with tabs for Objects, Properties, Permissions, Metrics, Management, and Access Points. The 'Properties' tab is active, showing a 'Bucket overview' table.

Bucket overview		
AWS Region US East (N. Virginia) us-east-1	Amazon Resource Name (ARN) arn:aws:s3:::wesbite-host-d15c52	Creation date August 7, 2024, 20:36:25 (UTC+05:30)

8. With this your link for the static website through S3 bucket will be generated

Static website hosting

Use this bucket to host a website or redirect requests. [Learn more](#)

Static website hosting
Enabled

Hosting type
Bucket hosting

Bucket website endpoint
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](#)
<http://wesbite-host-d15c52.s3-website-us-east-1.amazonaws.com>

Edit

9. Now go to the Permissions and edit the bucket policy by adding this

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PublicReadGetObject",
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::wesbite-host-d15c52/*"
    }
  ]
}
```

Just change the arn according to your bucket name and click save

Amazon S3 > Buckets > wesbite-host-d15c52 > Edit bucket policy

Edit bucket policy [Info](#)

Bucket policy

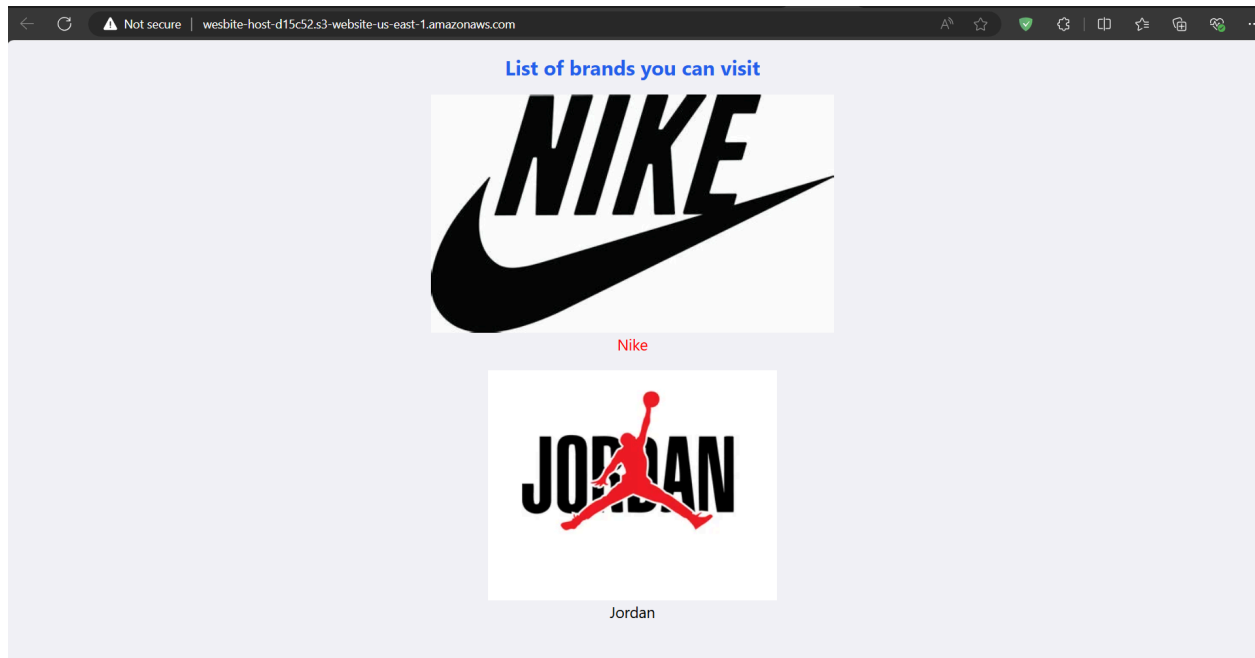
The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. [Learn more](#)

Bucket ARN
[arn:aws:s3:::wesbite-host-d15c52](#)

Policy

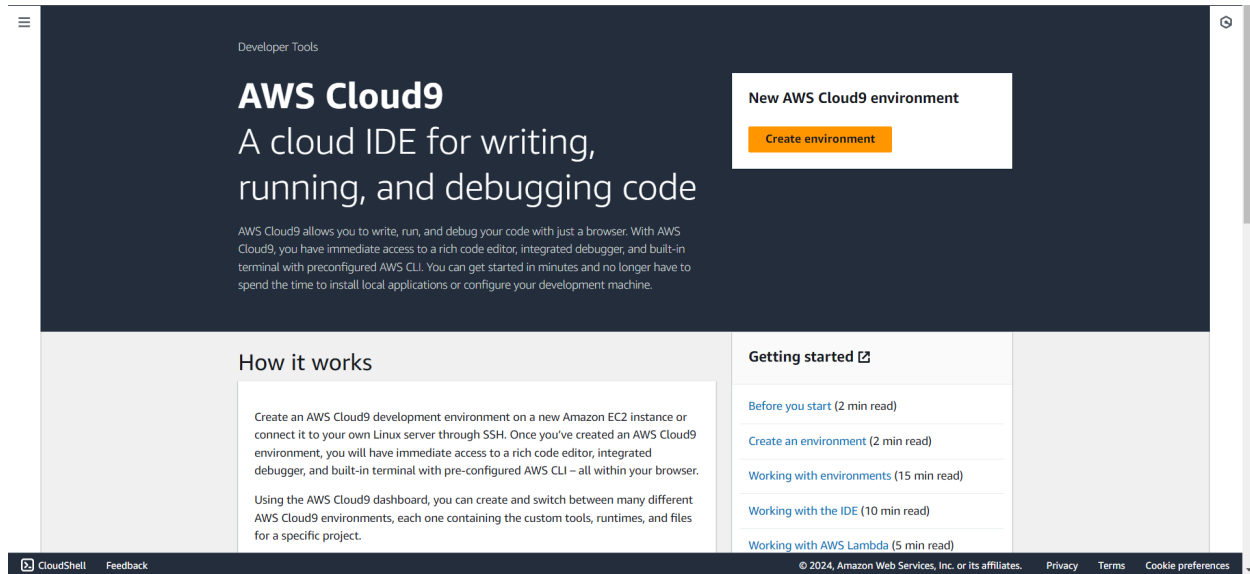
```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Sid": "PublicReadGetObject",
6       "Effect": "Allow",
7       "Principal": {
8         "AWS": "*"
9       },
10      "Action": "s3:GetObject",
11      "Resource": "arn:aws:s3:::wesbite-host-d15c52/*"
12    }
13  ]
14 }
```

10. Once edited the bucket policy click on the link in the generated back in step 8 and your website is hosted through aws S3 bucket

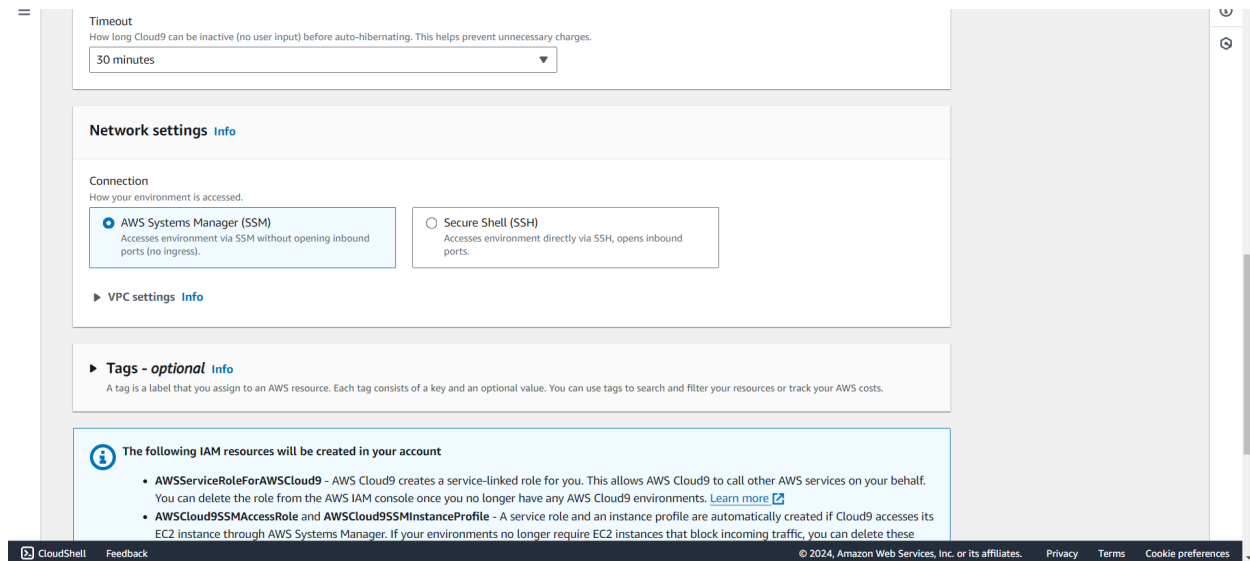


Aim : Exp 1 To understand the benefits of Cloud Infrastructure and Setup AWS Cloud9 IDE, Launch AWS Cloud9 IDE and Perform Collaboration Demonstration.

1. Open the AWS account and search for Cloud9. Click on create environment.



2. Enter the name and other required configuration for creating an environment. In network settings, using the AWS system manager gives an error while creating the environment



VPC settings Info

Tags - optional Info

The following IAM resources will be created in your account

- AWSServiceRoleForAWSCloud9** - AWS Cloud9 creates a service-linked role for you. This allows AWS Cloud9 to call other AWS services on your behalf. You can delete the role from the AWS IAM console once you no longer have any AWS Cloud9 environments. [Learn more](#)
- AWSCloud9SSMAccessRole** and **AWSCloud9SSMInstanceProfile** - A service role and an instance profile are automatically created if Cloud9 accesses its EC2 instance through AWS Systems Manager. If your environments no longer require EC2 instances that block incoming traffic, you can delete these roles using the AWS IAM console. [Learn more](#)

Cancel

Create

There was an error creating the IAM resources needed for SSM connection.

You don't have the permission required to perform this operation. Ask your administrator to give you permissions.

User: arn:aws:sts::354256622778:assumed-role/voclabs/user3404112=SHARMA__RAKSHIT_KUMAR is not authorized to perform: iam:CreateRole on resource: arn:aws:iam::354256622778:role/service-role/AWSCloud9SSMAccessRole because no identity-based policy allows the iam:CreateRole action

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

3. Use the Secure Shell option in Network settings.

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

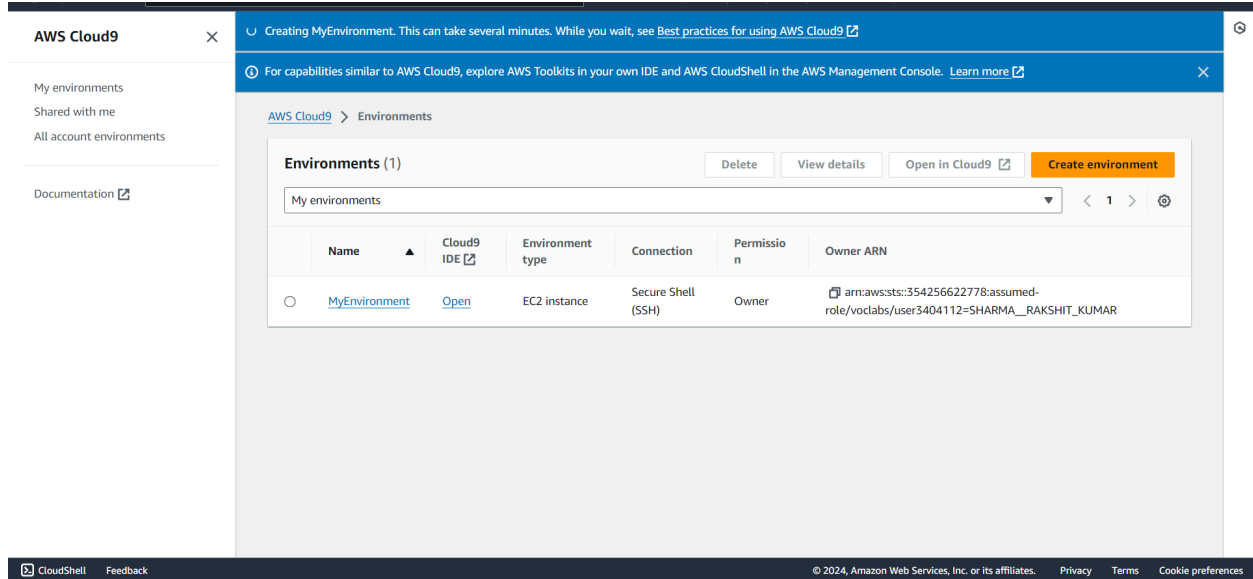
Tags - optional Info

The following IAM resources will be created in your account

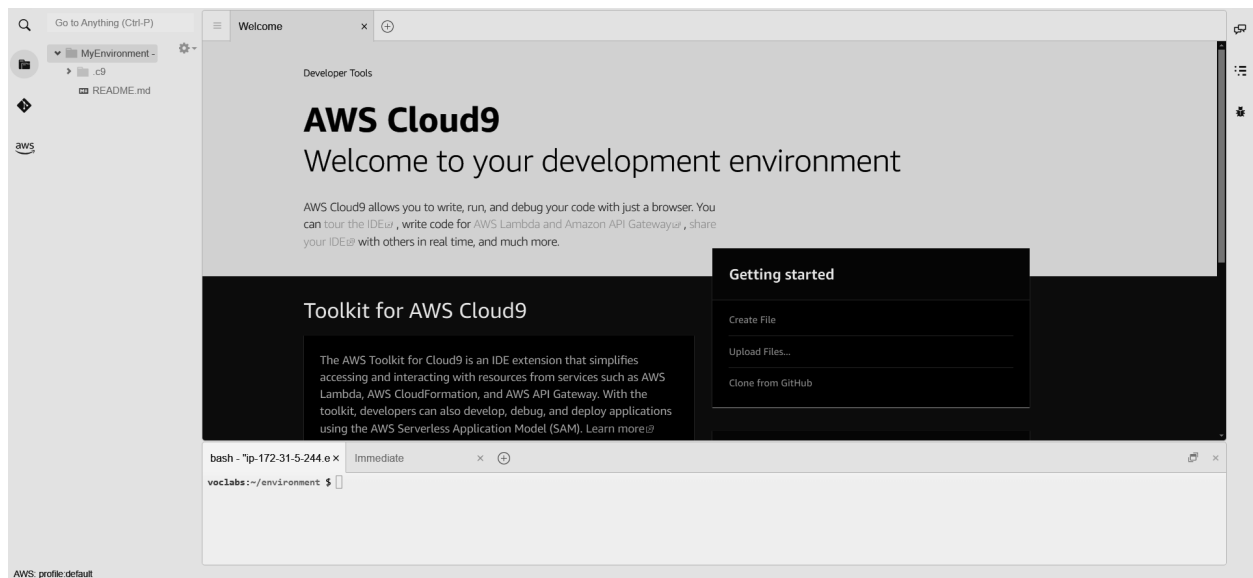
- AWSServiceRoleForAWSCloud9** - AWS Cloud9 creates a service-linked role for you. This allows AWS Cloud9 to call other AWS services on your behalf. You can delete the role from the AWS IAM console once you no longer have any AWS Cloud9 environments. [Learn more](#)

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

4. Once the configuration is complete, click on create environment to create a Cloud9 environment.

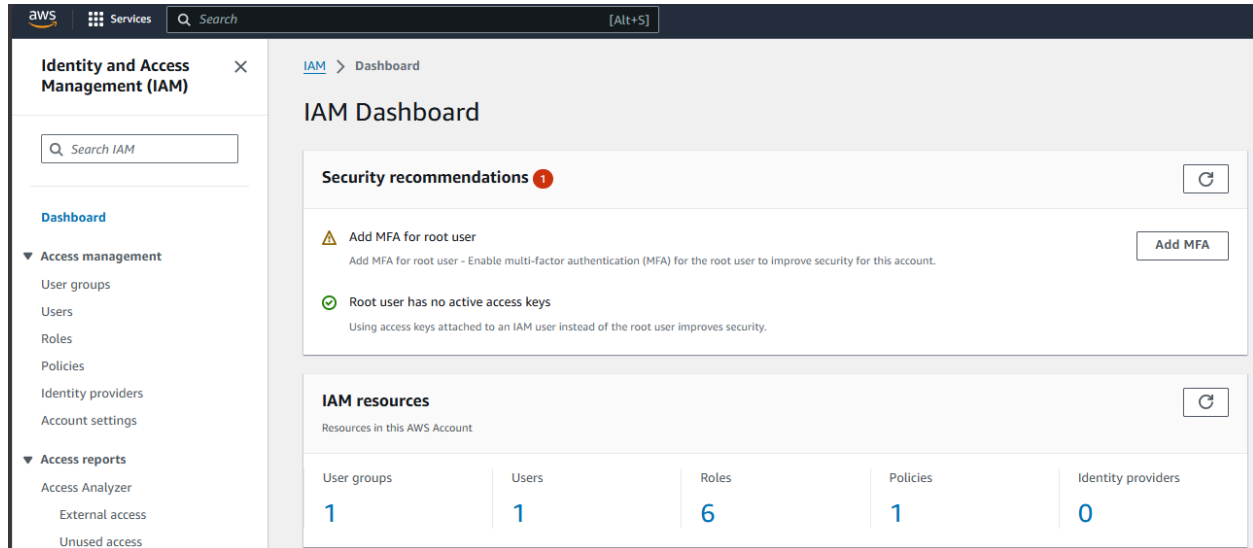


5. Cloud9 Environment is opened when u click on the environment name



IAM user creation steps

1. Open the aws account and search for IAM service.



2. Select the users option from the left panel and click on create user button. Give the user name, select the “provide user access” checkbox. Also select the option “I want to create an IAM user”. Otherwise we will have to enable the Identity center and specify a user there. Add your custom password

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.

Are you providing console access to a person?

User type

☐ **Specify a user in Identity Center - Recommended**
We recommend that you use Identity Center to provide console access to a person. With Identity Center, you can centrally manage user access to their AWS accounts and cloud applications.

☒ **I want to create an IAM user**
We recommend that you create IAM users only if you need to enable programmatic access through access keys, service-specific credentials for AWS CodeCommit or Amazon Keyspaces, or a backup credential for emergency account access.

Console password

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

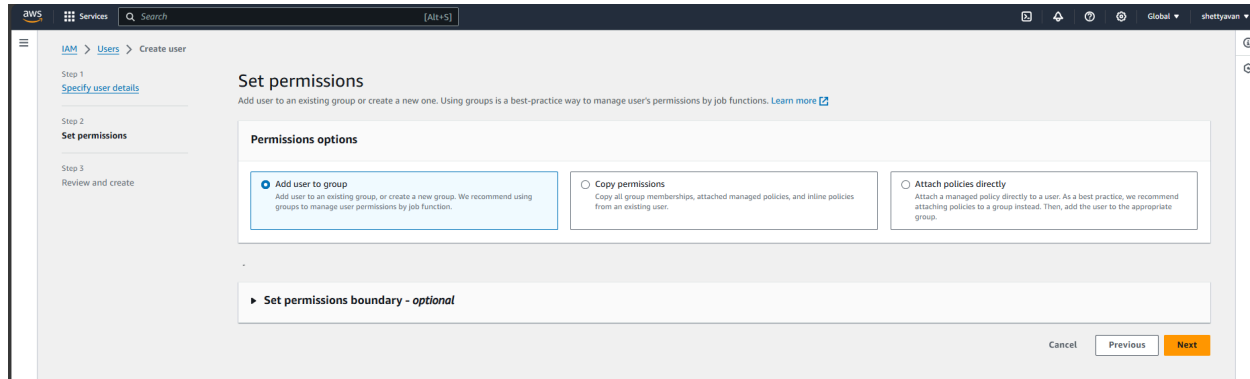
☒ **Custom password**
Enter a custom password for the user.

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

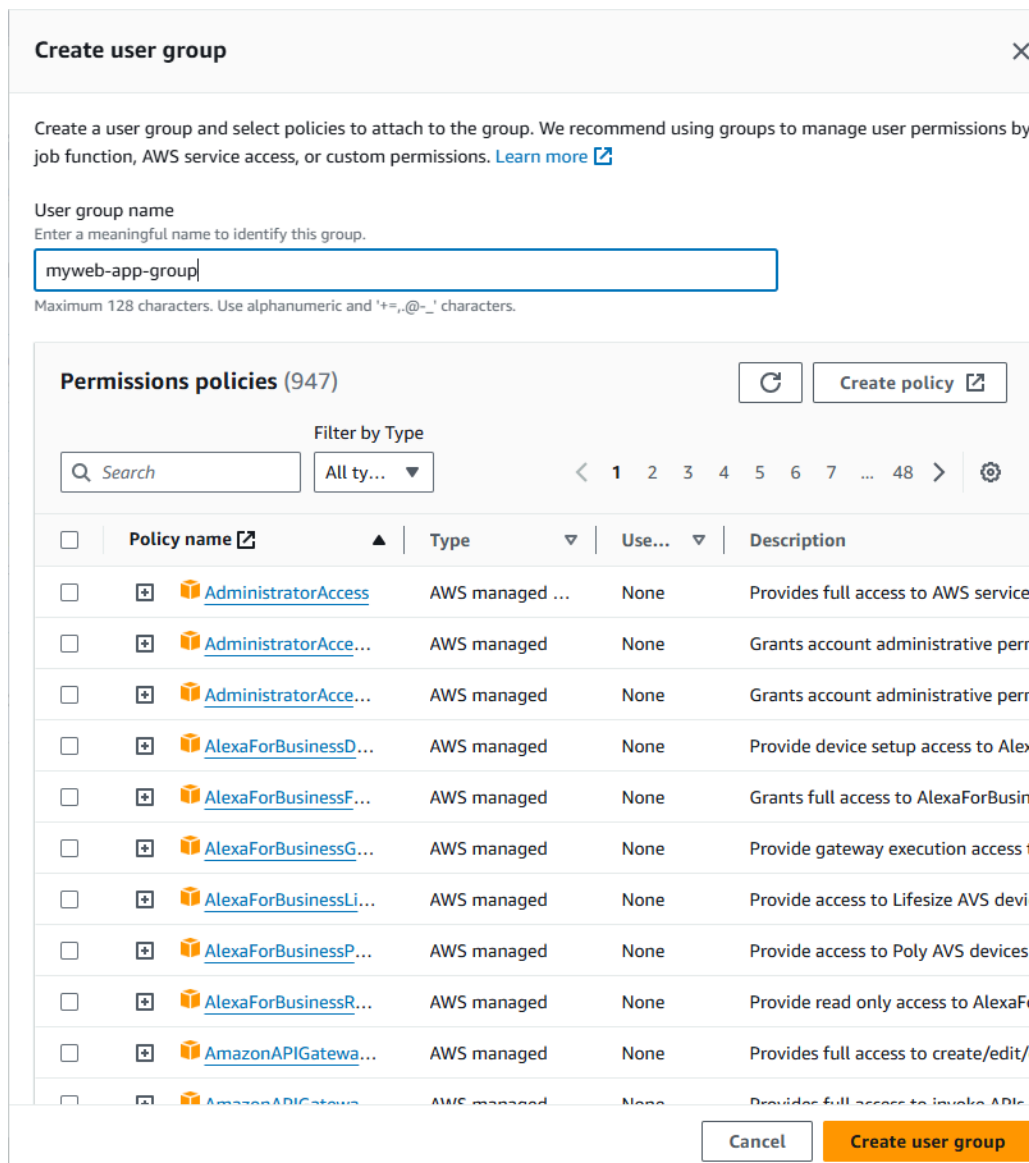
☐ **Show password**

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

3. Click the add user option if you don't have an existing user group



4. Give a name to your user group and check the policies if required any



5. Once the user group is created select the name and click next to create your user

myweb-app-group 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.

User groups (1) Create group

Search

<input type="checkbox"/>	Group name ↗	Users	Attached policies ↗	Created
<input type="checkbox"/>	myweb-app-group	0	-	2024-08-08 (Now)

► **Set permissions boundary - optional**

Cancel Previous **Next**

6. Review the configuration details and check if you have missed any steps and then click on 'Create user' button

Review and create

Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.

User details

User name avan-shetty	Console password type Custom password	Require password reset Yes
--------------------------	--	-------------------------------

Permissions summary < 1 >

Name ↗	Type	Used as
IAMUserChangePassword	AWS managed	Permissions policy

Tags - optional

Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.

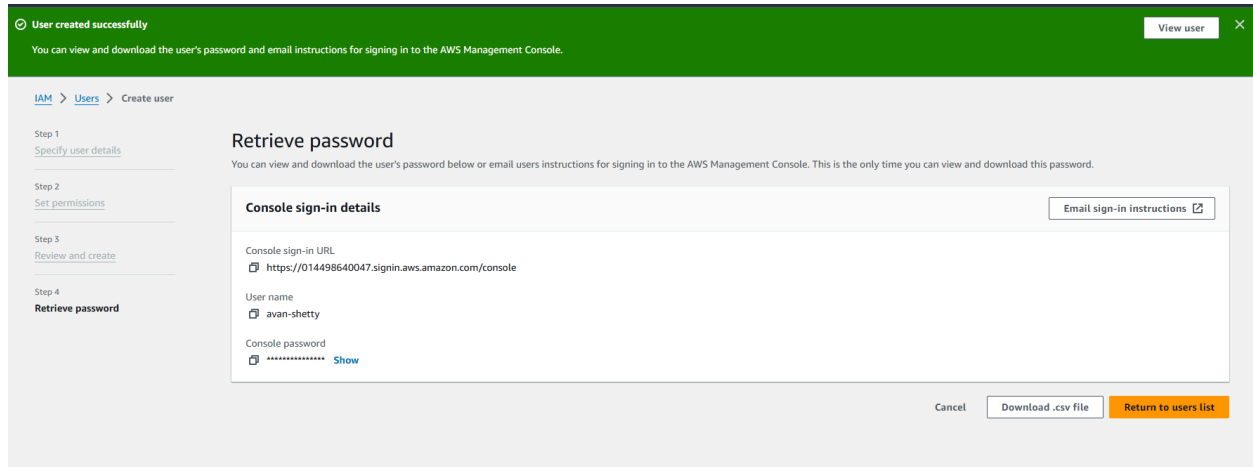
No tags associated with the resource.

Add new tag

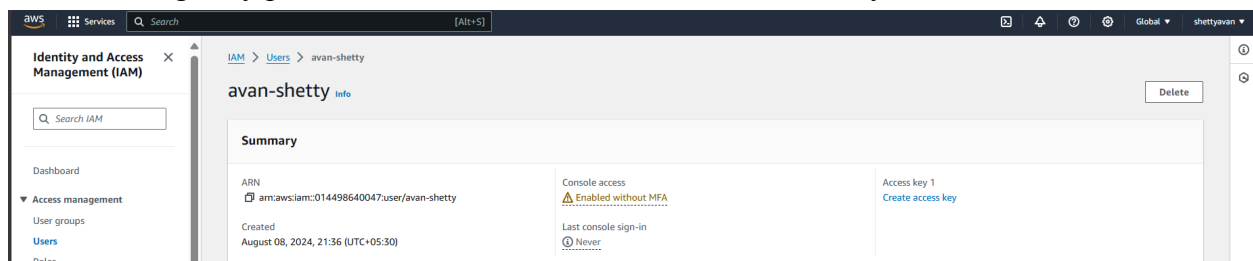
You can add up to 50 more tags.

Cancel Previous **Create user**

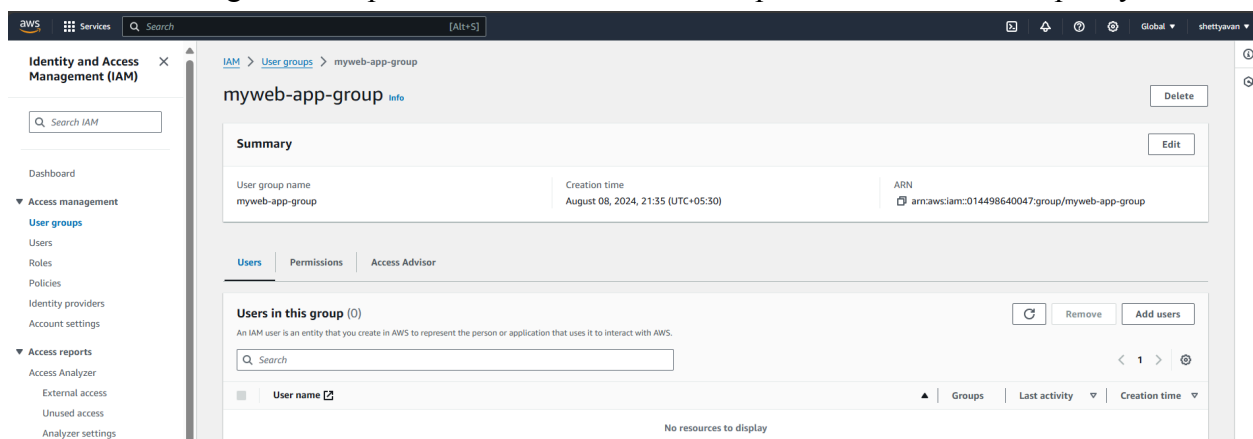
7. You will see the “user created successfully” message and incase you need then store your password by downloading the csv file



8. Click the users tab and you will see the user is created under IAM service. Also this service does not charge any price but this feature is not available in academy lab



9. After creation of the user, go to the user groups tab and select the group in which the user has been added. Navigate to the permissions tab. Click on add permissions and attach policy.



10. Search for the “AWSCloud9EnvironmentMember” policy and attach it.

IAM > User groups > myweb-app-group > Add permissions

Attach permission policies to myweb-app-group

▶ Current permissions policies (0)

Other permission policies (1/945)

You can attach up to 10 managed policies to this user group. All of the users in this group inherit the attached permissions.


Q Awscloud9E

Filter by Type

All types

1 match

< 1 > ⌕

<input checked="" type="checkbox"/>	Policy name	Type	Used as	Description
<input checked="" type="checkbox"/>	 AWSCloud9EnvironmentMember	AWS managed	None	Provides the ability to be invited into AW...

Cancel

Attach policies