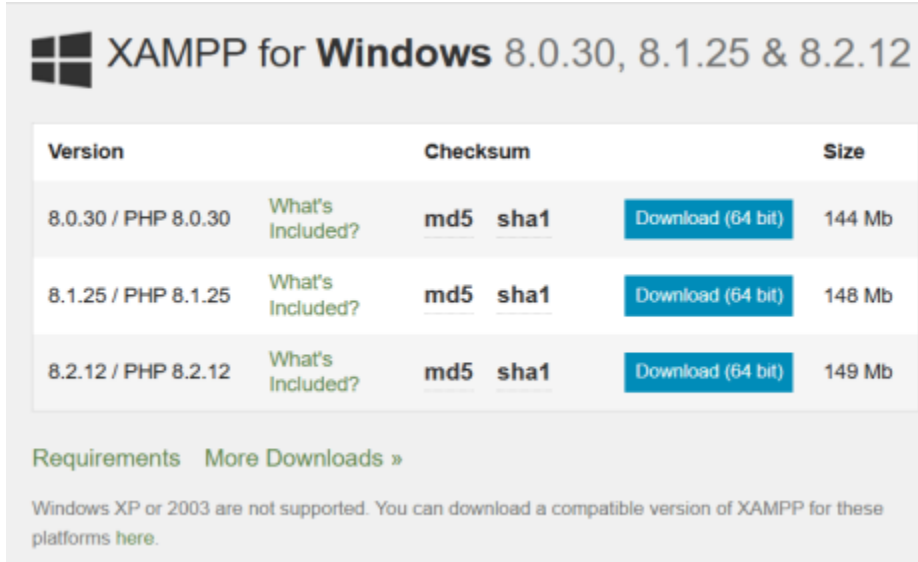


## Experiment 1

**Part 1 : a) To develop a website and host it on your local machine on a VM**

Download xampp from this website <https://www.apachefriends.org/download.html>



**XAMPP for Windows 8.0.30, 8.1.25 & 8.2.12**

| Version             | Checksum | Size   |
|---------------------|----------|--------|
| 8.0.30 / PHP 8.0.30 | md5 sha1 | 144 Mb |
| 8.1.25 / PHP 8.1.25 | md5 sha1 | 148 Mb |
| 8.2.12 / PHP 8.2.12 | md5 sha1 | 149 Mb |

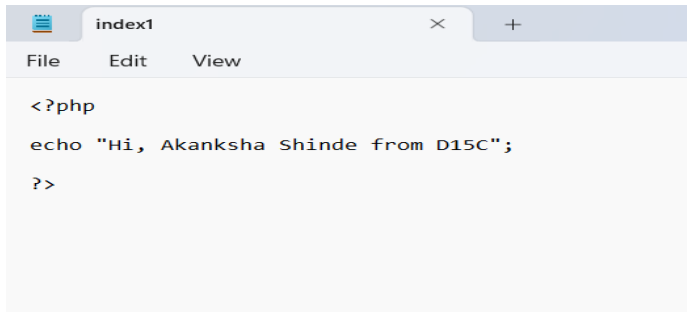
[What's Included?](#) [Download \(64 bit\)](#)

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

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

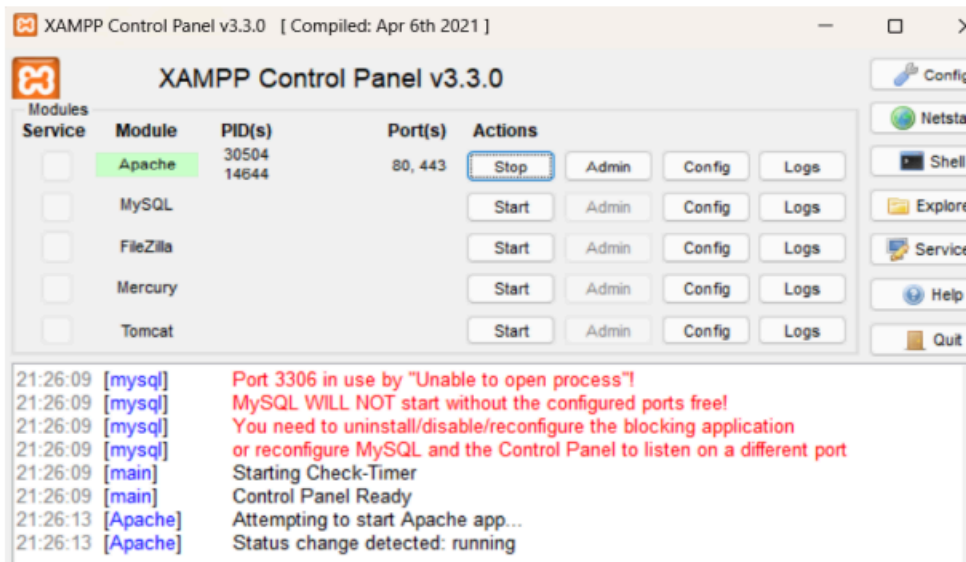
**After downloading just select Apache and MySQL you can skip other options as it is not required.**

**Now go in the xampp folder and inside the htdocs file create a php file just like this**



```
<?php
echo "Hi, Akanksha Shinde from D15C";
?>
```

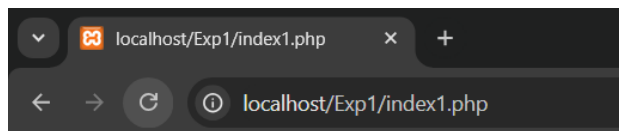
**Save it and go to the xampp control panel and start the Apache and MySQL**



Go in the browser and type localhost and hit enter you will get to see the file you created like in this case index1.php



Click on the index1.php and the website is hosted locally.



Hi, Akanksha Shinde from D15C

## Hosting a static website on Amazon S3

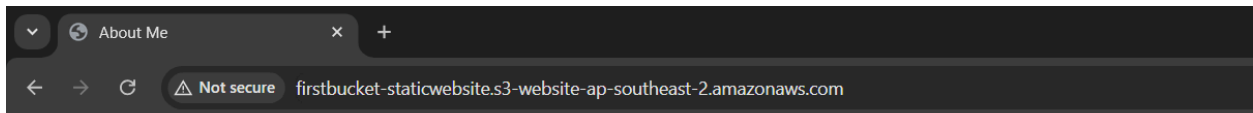
After creating the bucket on AWS add the file in it that is to be hosted and configure the visibility as public and add /\* at the end of the resource key.

### Bucket policy

The bucket policy, written in JSON, provides access to the objects stored in the bucket.

```
{
  "Version": "2012-10-17",
  "Id": "Policy1722527682607",
  "Statement": [
    {
      "Sid": "Stmt1722527493263",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::firstbucket-staticwebsite/*"
    }
  ]
}
```

Copy the url from the Bucket ARN and paste it in the browser and the static website is hosted.



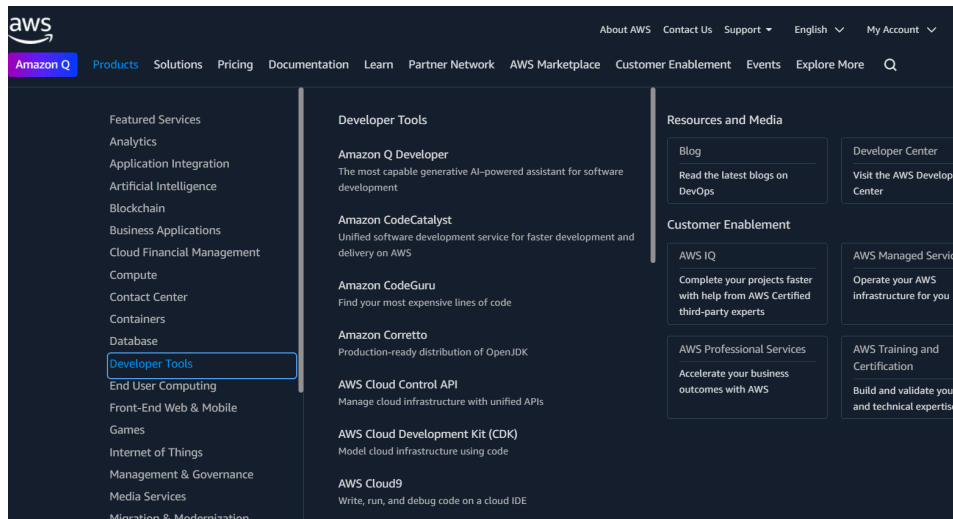
**Hi, I am Akanksha Shinde.**

A Third-year engineering student.

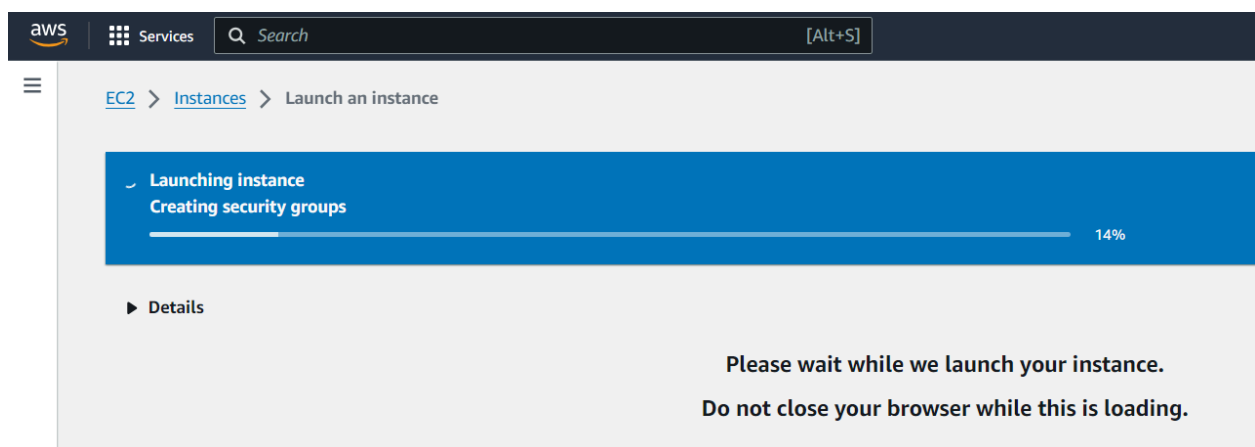
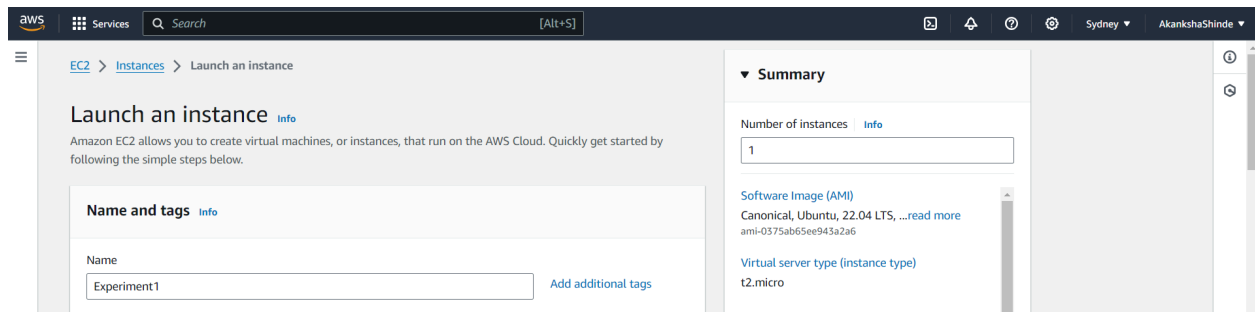
I'm pursuing IT engineering at VESIT.

## To Create EC2 instance

### Go to AWS services and search for developer tools



### Search for EC2 instance and launch an instance



## Connect to instance [Info](#)

Connect to your instance i-0dbff2d1864aed490 (Experiment1) 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: 13.239.158.0/29. [Learn more](#).

Instance ID

i-0dbff2d1864aed490 (Experiment1)

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

3.24.123.186

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.

Cancel

Connect

```
System load: 0.03          Processes:           107
Usage of / : 6.5% of 24.05GB Users logged in:       0
Memory usage: 21%          IPv4 address for eth0: 172.31.15.82
Swap usage:  0%
```

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

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

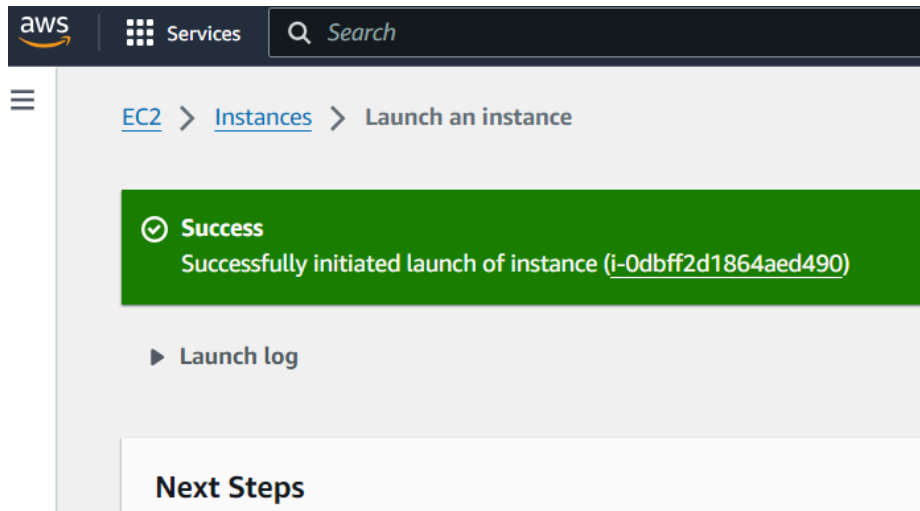
The list of available updates is more than a week old.  
To check for new updates run: `sudo apt update`

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

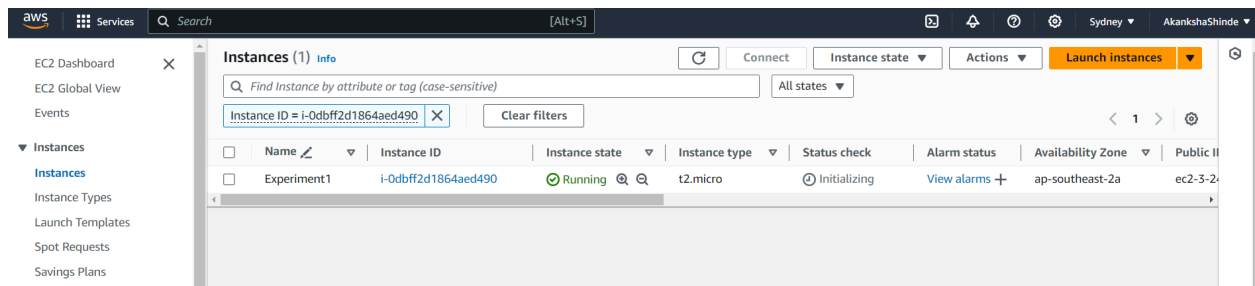
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.

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

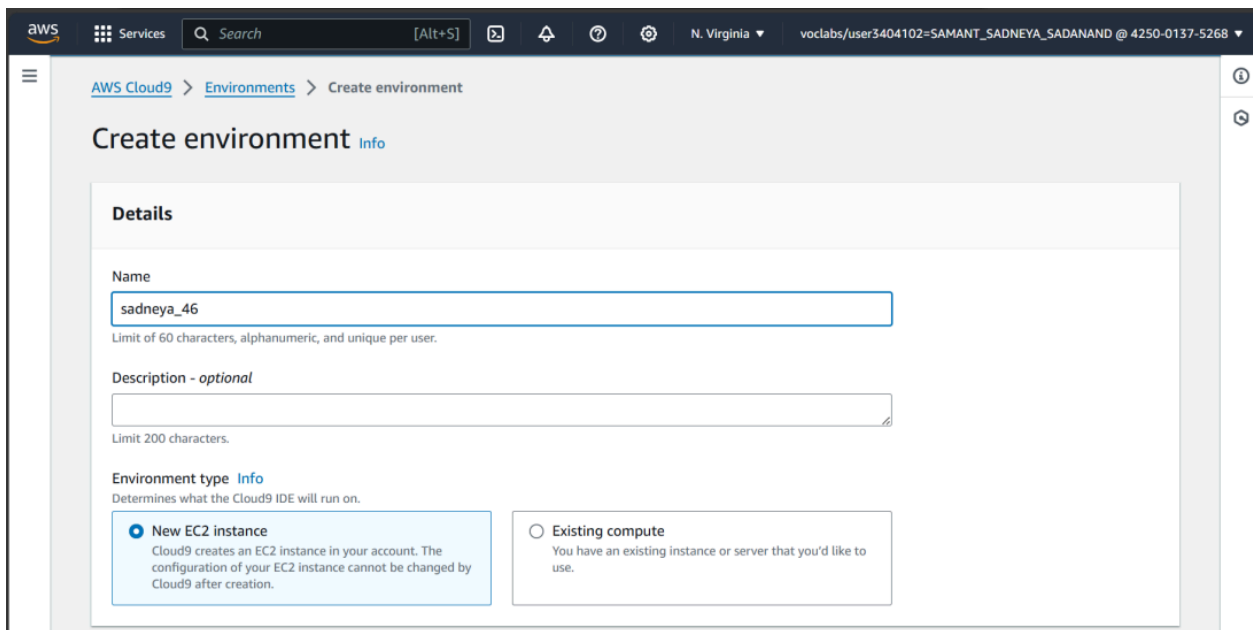
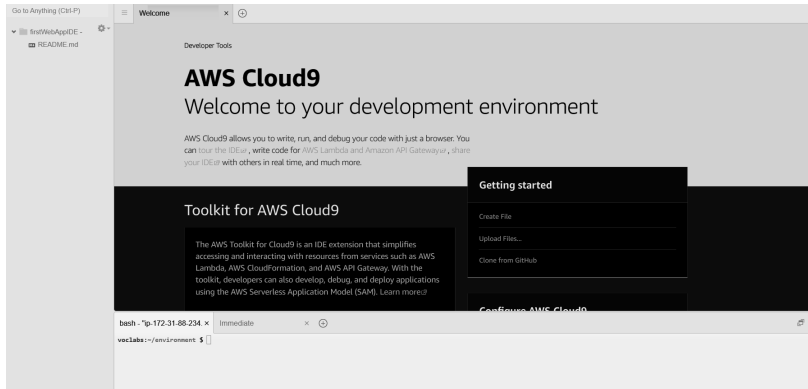
ubuntu@ip-172-31-15-82:~\$



An instance would be recorded with the name you created.



# Experiment 1 B



## 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](#)

### ▼ **Tags - optional** [Info](#)

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

No tags associated with the resource.

Add new tag

You can add up to 50 more tags.



## 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](#)

#### Amazon Virtual Private Cloud (VPC)

The VPC that your environment will access. To allow the AWS Cloud9 environment to connect to its EC2 instance, attach an internet gateway (IGW) to your VPC. [Create new VPC](#)

vpc-051bba342b3626898

Name -

#### Subnet

Used to setup your VPC configuration. To use a private subnet, select AWS Systems Manager (SSM) as the connection type. [Create new subnet](#)

No preference

Uses default subnet in any Availability Zone

## AWS Cloud9

My environments

Shared with me

All account environments

[Documentation](#)

Creating sadneya\_46. This can take several minutes. While you wait, see [Best practices for using AWS Cloud9](#)

For capabilities similar to AWS Cloud9, explore AWS Toolkits in your own IDE and AWS CloudShell in the AWS Management Console.

[Learn more](#)

[AWS Cloud9](#) > Environments

### Environments (1)

Delete

View details

Open in Cloud9

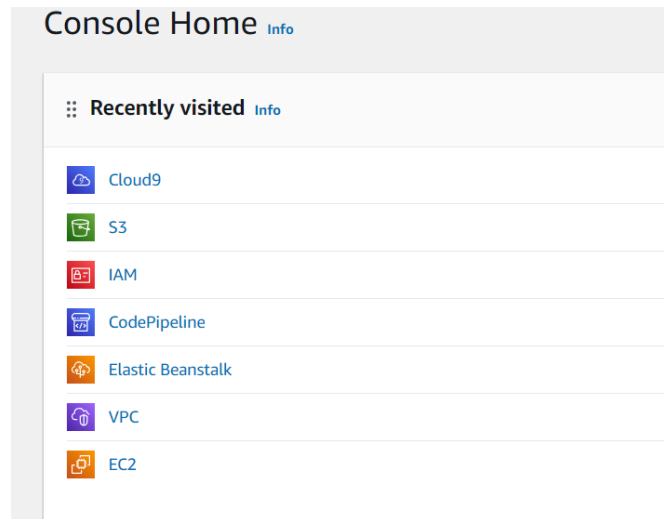
Create environment

My environments

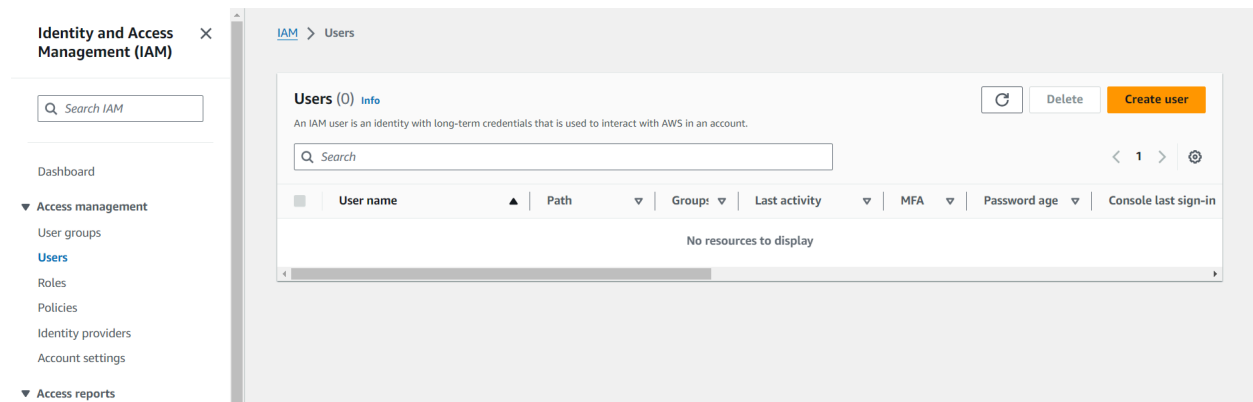
|                       | Name ▲                     | Cloud9 IDE           | Environment type | Connection         | Permission | Owner ARN   |
|-----------------------|----------------------------|----------------------|------------------|--------------------|------------|---|
| <input type="radio"/> | <a href="#">sadneya_46</a> | <a href="#">Open</a> | EC2 instance     | Secure Shell (SSH) | Owner      | arn:aws:sts::42500137526role/voclabs/user3404102=5/ |

# IAM

## Go to IAM services



## Click on create user



# Give username and set password

User details

User name

akanksha

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 ! @ # \$ % ^ & \* ( ) \_ + - (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.

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

# Set permissions as below

Set permissions

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. [Learn more](#)

Permissions options

☒ Add user to group

Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.

☐ Copy permissions

Copy all group memberships, attached managed policies, and inline policies from an existing user.

☐ Attach policies directly

Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

Get started with groups

Create a group and select policies to attach to the group. We recommend using groups to manage user permissions by job function, AWS service access, or custom permissions. [Learn more](#)

Create group

► Set permissions boundary - *optional*

Cancel

Previous

Next

# Create user group

Create user group

Create a user group and select policies to attach to the group. We recommend using groups to manage user permissions by job function, AWS service access, or custom permissions. [Learn more](#)

User group name  
Enter a meaningful name to identify this group.  

myGroup

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

Permissions policies (951)

Filter by Type

Search

All ty...

< 1 2 3 4 5 6 7 ... 48 >

| <input type="checkbox"/> | Policy name          | Type            | Use...    | Description                            |
|--------------------------|----------------------|-----------------|-----------|--|
| <input type="checkbox"/> | AdministratorAccess  | AWS managed ... | Permis... | Provides full access to AWS service... |
| <input type="checkbox"/> | AdministratorAcce... | AWS managed     | None      | Grants account administrative perm...  |
| <input type="checkbox"/> | AdministratorAcce... | AWS managed     | None      | Grants account administrative perm...  |
| <input type="checkbox"/> | AlexaForBusinessD... | AWS managed     | None      | Provide device setup access to Alex... |

# You must see the below screen

myGroup user group created.

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)

Search

< 1 >

| <input type="checkbox"/> | Group name | Users | Attached policies | Created          |
|--------------------------|------------|-------|-------------------|------------------|
| <input type="checkbox"/> | myGroup    | 0     | -                 | 2024-08-08 (Now) |

► Set permissions boundary - optional

Cancel

Previous

Next