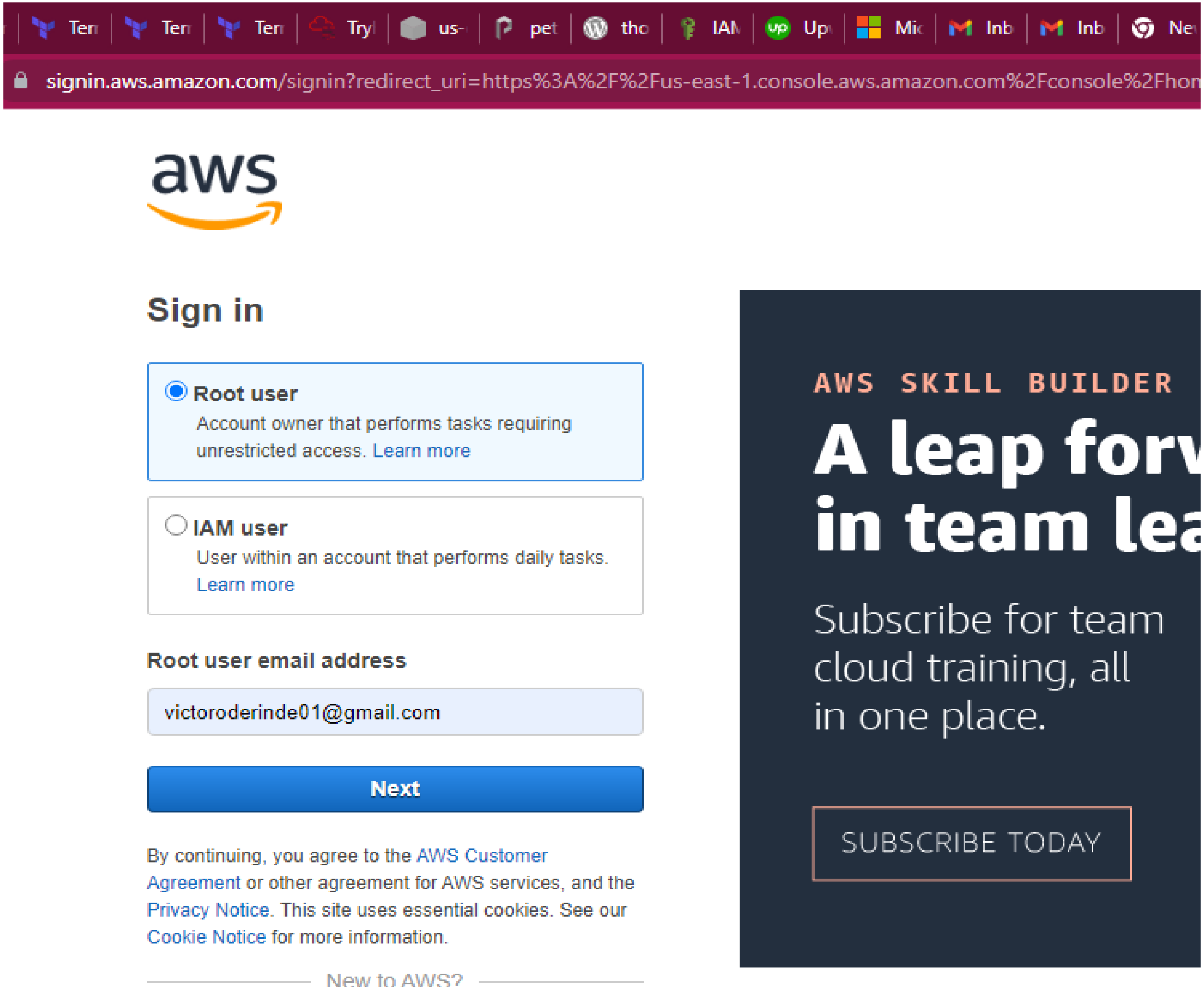
1. **Create your root AWS account and create 2 users, one with programmatic access and the other with username and password**

install the toolings;

AWS Account
VScode
Git
AWS CLI

Create your root AWS account and create user with programmatic access

--Sign in with root aws account into the aws console



signin.aws.amazon.com/signin?redirect_uri=https%3A%2F%2Fus-east-1.console.aws.amazon.com%2Fconsole%2Fhon

Sign in

● Root user
Account owner that performs tasks requiring unrestricted access. Learn more

○ IAM user
User within an account that performs daily tasks. Learn more

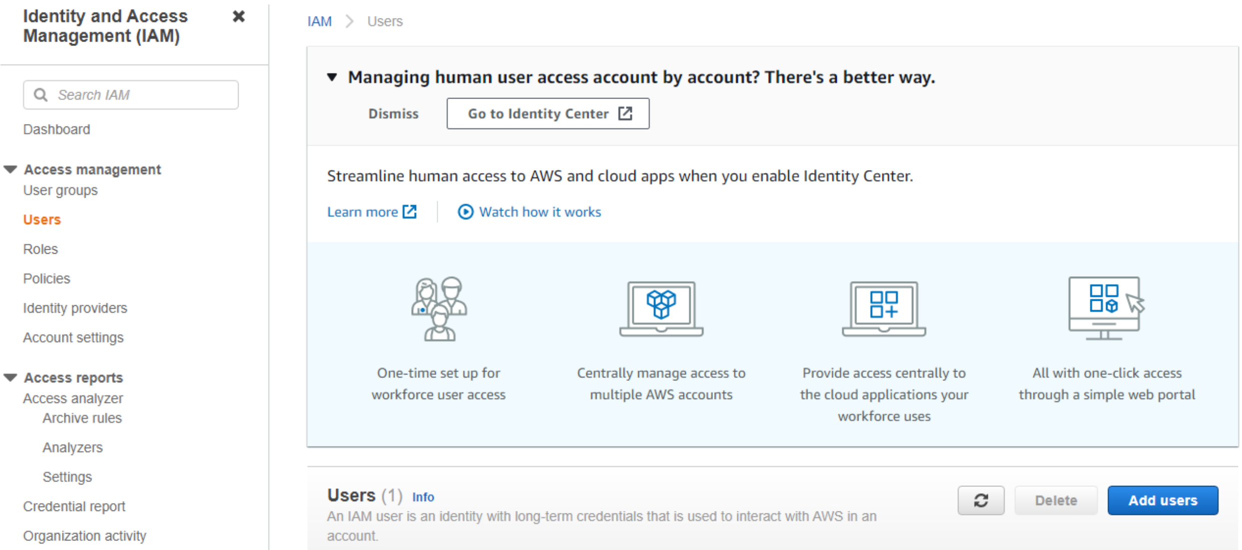
Root user email address
victoroderinde01@gmail.com

By continuing, you agree to the AWS Customer Agreement or other agreement for AWS services, and the Privacy Notice. This site uses essential cookies. See our Cookie Notice for more information.

AWS SKILL BUILDER
A leap forv
in team lea

Subscribe for team cloud training, all in one place.

--Go to IAM(Identity Access Management)



Identity and Access Management (IAM) ✖

Search IAM

Dashboard

▼ Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

▼ Access reports

Access analyzer

Archive rules

Analyzers

Settings

Credential report

Organization activity

IAM > Users

▼ Managing human user access account by account? There's a better way.

Dismiss | Go to Identity Center

Streamline human access to AWS and cloud apps when you enable Identity Center.

Learn more | Watch how it works

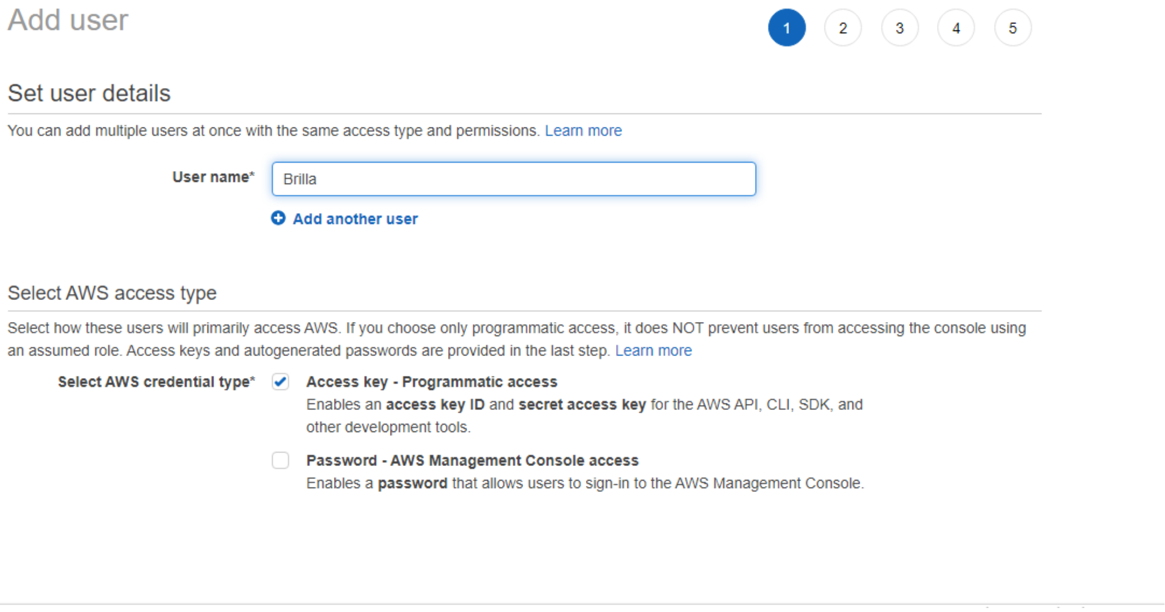
One-time set up for workforce user access
Centrally manage access to multiple AWS accounts
Provide access centrally to the cloud applications your workforce uses
All with one-click access through a simple web portal

Users (1) Info

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

Delete | Add users

--Add user



Add user

Set user details

You can add multiple users at once with the same access type and permissions. Learn more

User name* Brilla

Add another user

Select AWS access type

Select how these users will primarily access AWS. If you choose only programmatic access, it does NOT prevent users from accessing the console using an assumed role. Access keys and autogenerated passwords are provided in the last step. Learn more

Select AWS credential type*

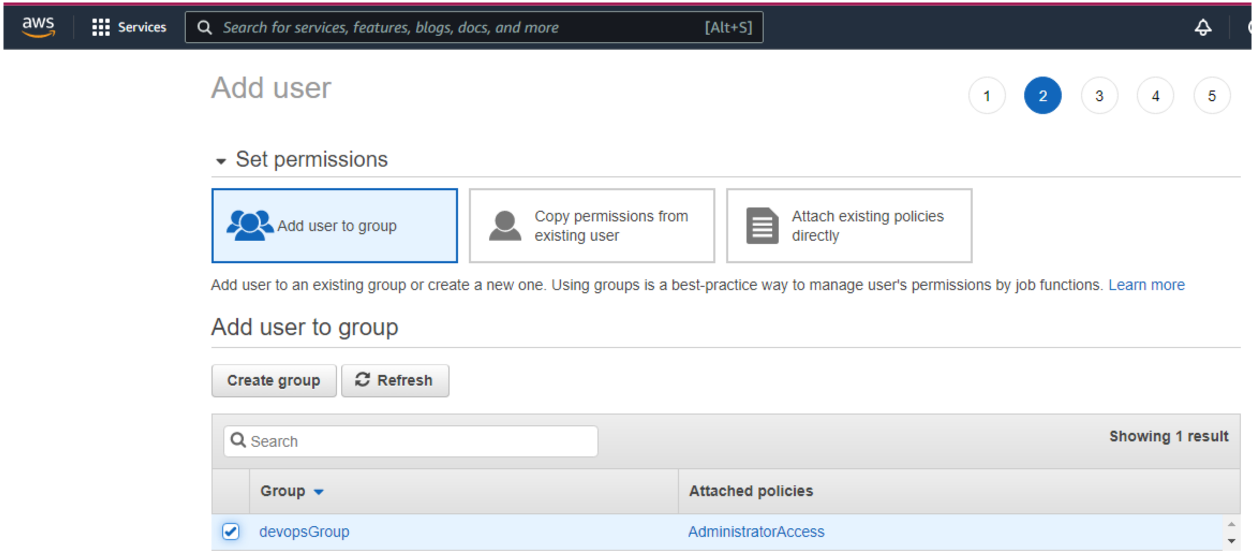
☑ **Access key - Programmatic access**
Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.

☐ **Password - AWS Management Console access**
Enables a **password** that allows users to sign-in to the AWS Management Console.

--Input your desired name and select Access Key- Programmatic access

--Click on next

--create a group and select Administrator access



aws
Services
Search for services, features, blogs, docs, and more [Alt+S]
1
2
3
4
5

Add user

▼ Set permissions

Add user to group | Copy permissions from existing user | Attach existing policies directly

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

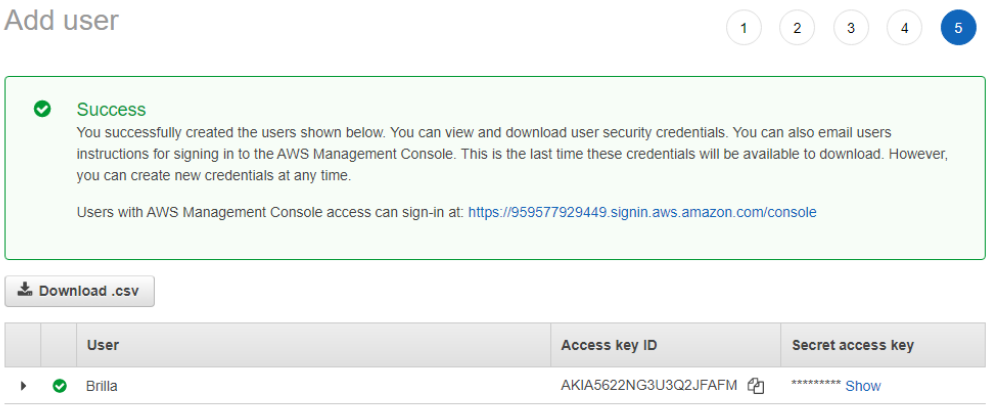
Create group | Refresh

Search | Showing 1 result

	Group	Attached policies
☑	devopsGroup	AdministratorAccess

--select and click next

--create user and download the csv file that contains your credentials



Success

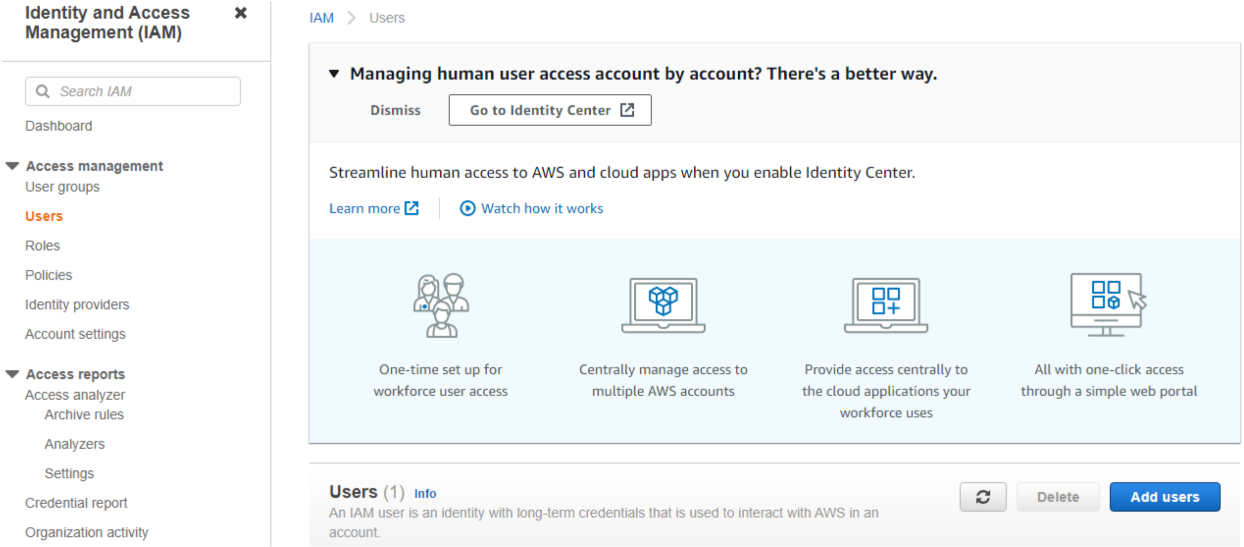
You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time.

Users with AWS Management Console access can sign-in at: https://959577929449.signin.aws.amazon.com/console

User	Access key ID	Secret access key
Brilla	AKIA5622NG3U3Q2JFAFM	********* Show

Create user with username and password

-- Go to IAM(Identity Access Management)



Managing human user access account by account? There's a better way.

Streamline human access to AWS and cloud apps when you enable Identity Center.

One-time set up for workforce user access

Centrally manage access to multiple AWS accounts

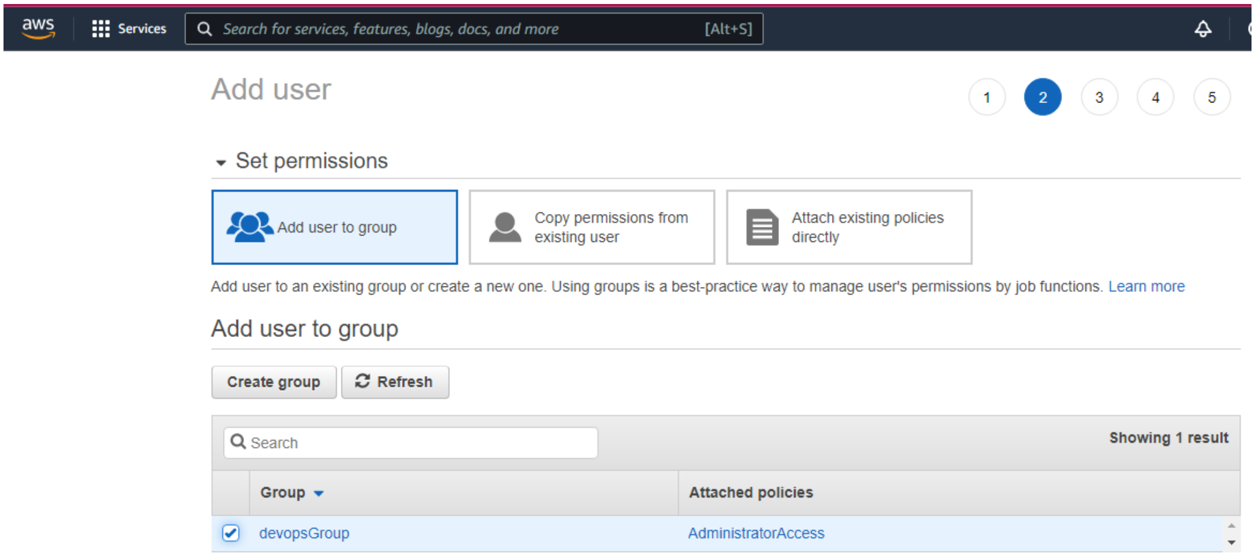
Provide access centrally to the cloud applications your workforce uses

All with one-click access through a simple web portal

Users (1) Info

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

--Add user



Set permissions

● Add user to group | Copy permissions from existing user | Attach existing policies directly

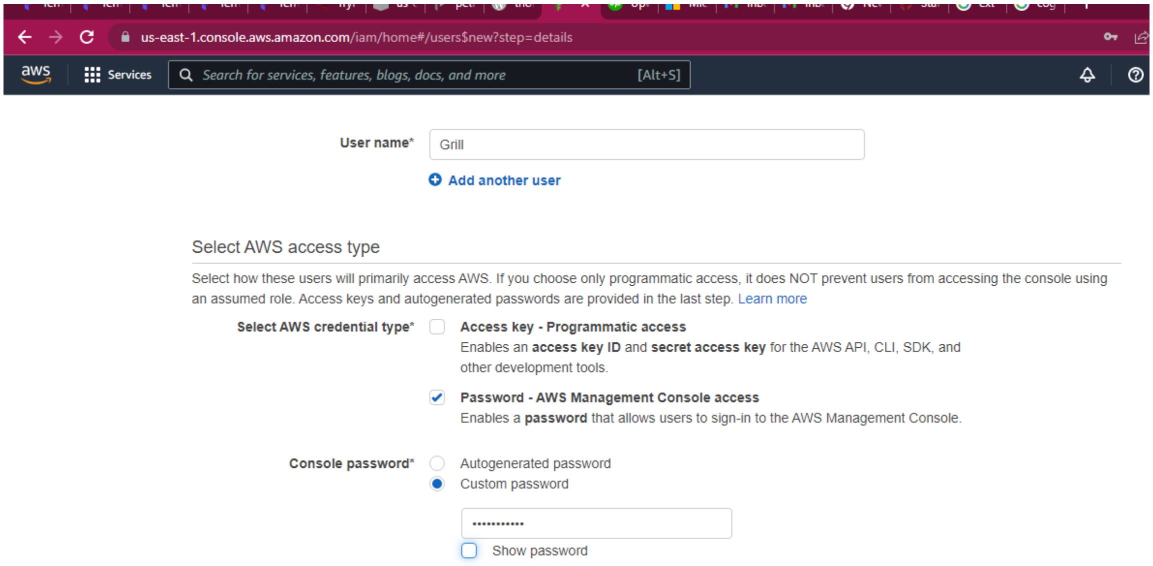
Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. Learn more

Add user to group

	Group	Attached policies
☑	devopsGroup	AdministratorAccess

--input desired name and select Password – AWS Management console access

--select custom password and input desired password


us-east-1.console.aws.amazon.com/iam/home#/users$new?step=details
aws
Services
Search for services, features, blogs, docs, and more
[Alt+S]

User name* Grill

Add another user

Select AWS access type

Select how these users will primarily access AWS. If you choose only programmatic access, it does NOT prevent users from accessing the console using an assumed role. Access keys and autogenerated passwords are provided in the last step. Learn more

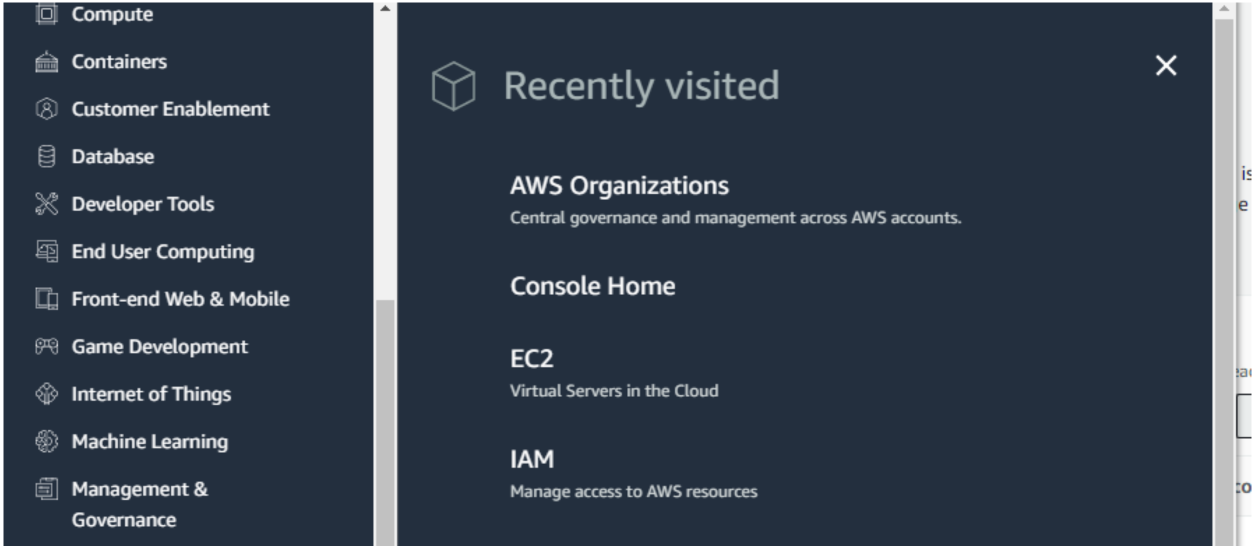
Select AWS credential type*
□ **Access key - Programmatic access**
Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.
☑ **Password - AWS Management Console access**
Enables a **password** that allows users to sign-in to the AWS Management Console.

Console password*
○ Autogenerated password
● Custom password
•••••••••••
□ Show password

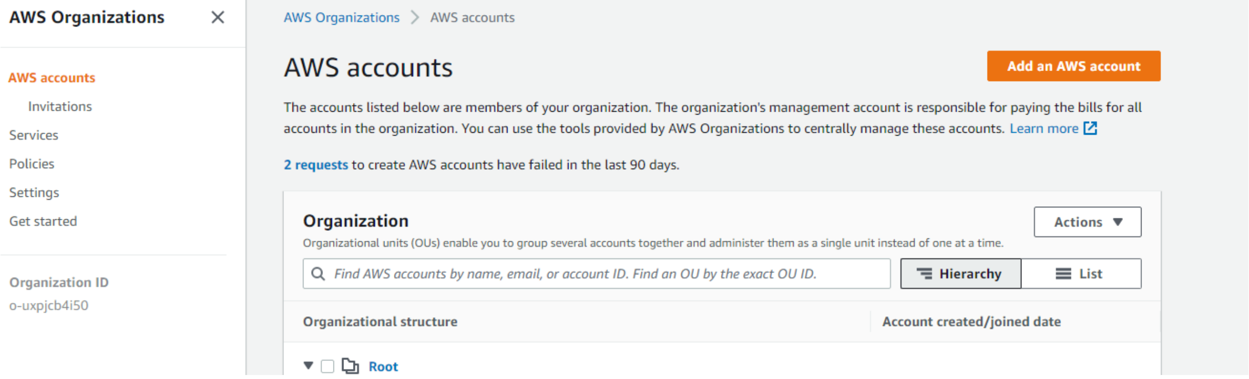
--click next and select the created group
--next and create user

2. Create AWS organisations and create sub-accounts - DTAP (Development, Test, Acceptance and Production)

--Sign in as a root user to your aws console
--Go to management and governance



--Select AWS organization



Organization ID
o-uxpjcb4i50

AWS accounts

The accounts listed below are members of your organization. The organization's management account is responsible for paying the bills for all accounts in the organization. You can use the tools provided by AWS Organizations to centrally manage these accounts. Learn more

2 requests to create AWS accounts have failed in the last 90 days.

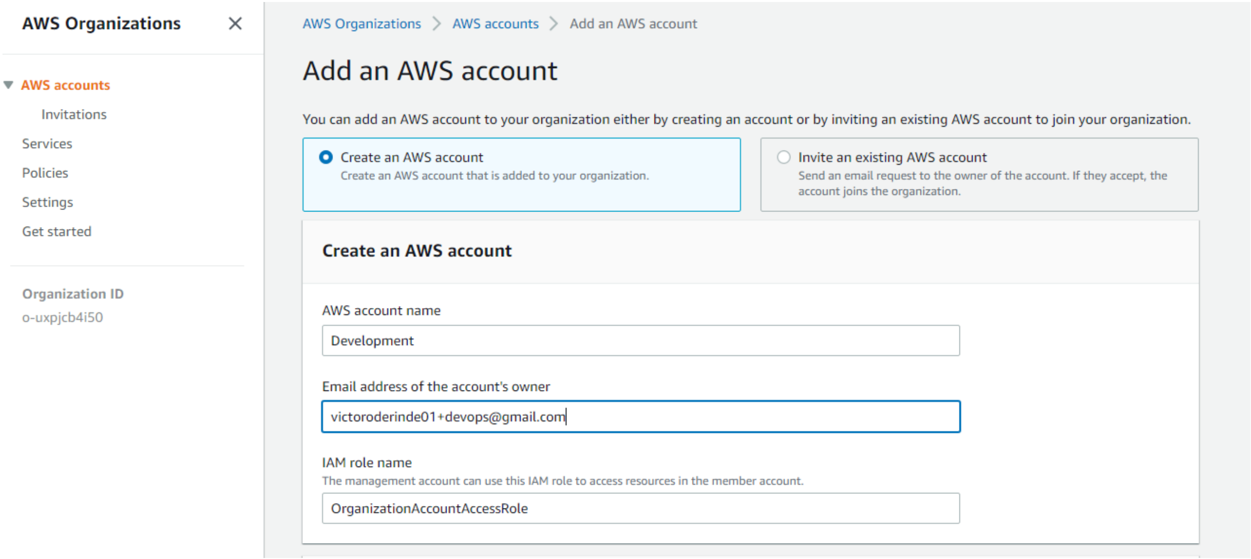
Organization

Organizational units (OUs) enable you to group several accounts together and administer them as a single unit instead of one at a time.

Find AWS accounts by name, email, or account ID. Find an OU by the exact OU ID.

Organizational structure	Account created/joined date
▼ □ Root	

--Select Add an AWS account



Add an AWS account

You can add an AWS account to your organization either by creating an account or by inviting an existing AWS account to join your organization.

● Create an AWS account
Create an AWS account that is added to your organization.

○ Invite an existing AWS account
Send an email request to the owner of the account. If they accept, the account joins the organization.

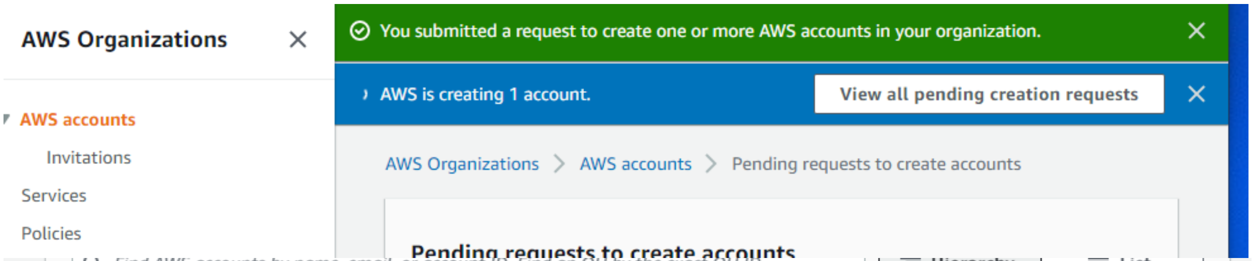
Create an AWS account

AWS account name
Development

Email address of the account's owner
victoroderinde01+devops@gmail.com

IAM role name
The management account can use this IAM role to access resources in the member account.
OrganizationAccountAccessRole

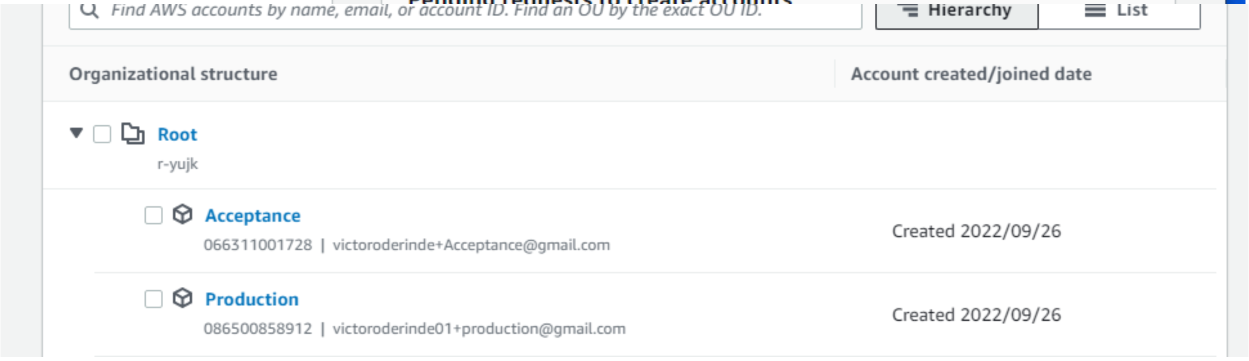
--Select "create an AWS account"
--Give your new account a name "Development"
--Insert your new email or to use your root email use victoroderinde01+devops@gmail.com (in this case victoroderinde01@gmail.com is my root email)
--create AWS account


AWS Organizations
AWS accounts
Invitations
Services
Policies
View all pending creation requests
AWS Organizations > AWS accounts > Pending requests to create accounts

You submitted a request to create one or more AWS accounts in your organization.

AWS is creating 1 account.

Pending requests to create accounts


Find AWS accounts by name, email, or account ID. Find an OU by the exact OU ID.
Hierarchy
List

Organizational structure	Account created/joined date
Root r-yujk	
Acceptance 066311001728 | victoroderinde+Acceptance@gmail.com	Created 2022/09/26
Production 086500858912 | victoroderinde01+production@gmail.com	Created 2022/09/26

3. Show an output of list of users in your organisations via CLI (Gitbash or VSCode)

--open git
--mkdir "Zoe" (make a new directory)
--cd "Zoe" (change directory to the new directory)
--code . (to open the folder using vscode)
--Ctrl + ~ (to open your terminal)
--change terminal to **gitbash** using the drop down beside the powershell and select gitbash
--type "aws configure"
--open the downloaded csv file(while creating users) to select copy your access key

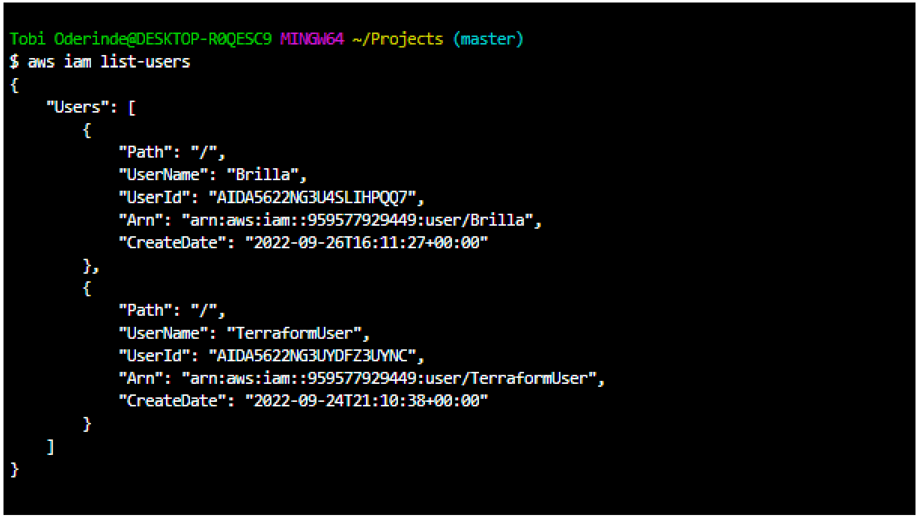
--paste on the terminal

-- copy your secret key and paste on your terminal

--locate your region at the top right corner of your aws console “us-east-1”

--enter the format “json”

--type “aws iam list-users” to display the users created on the aws console



```
Tobi Oderinde@DESKTOP-R0QESC9 MINGW64 ~/Projects (master)
$ aws iam list-users
{
    "Users": [
        {
            "Path": "/",
            "UserName": "Brilla",
            "UserId": "AIDA5622NG3U4SLIHPQQ7",
            "Arn": "arn:aws:iam::959577929449:user/Brilla",
            "CreateDate": "2022-09-26T16:11:27+00:00"
        },
        {
            "Path": "/",
            "UserName": "TerraformUser",
            "UserId": "AIDA5622NG3UYDFZ3UYNC",
            "Arn": "arn:aws:iam::959577929449:user/TerraformUser",
            "CreateDate": "2022-09-24T21:10:38+00:00"
        }
    ]
}
```