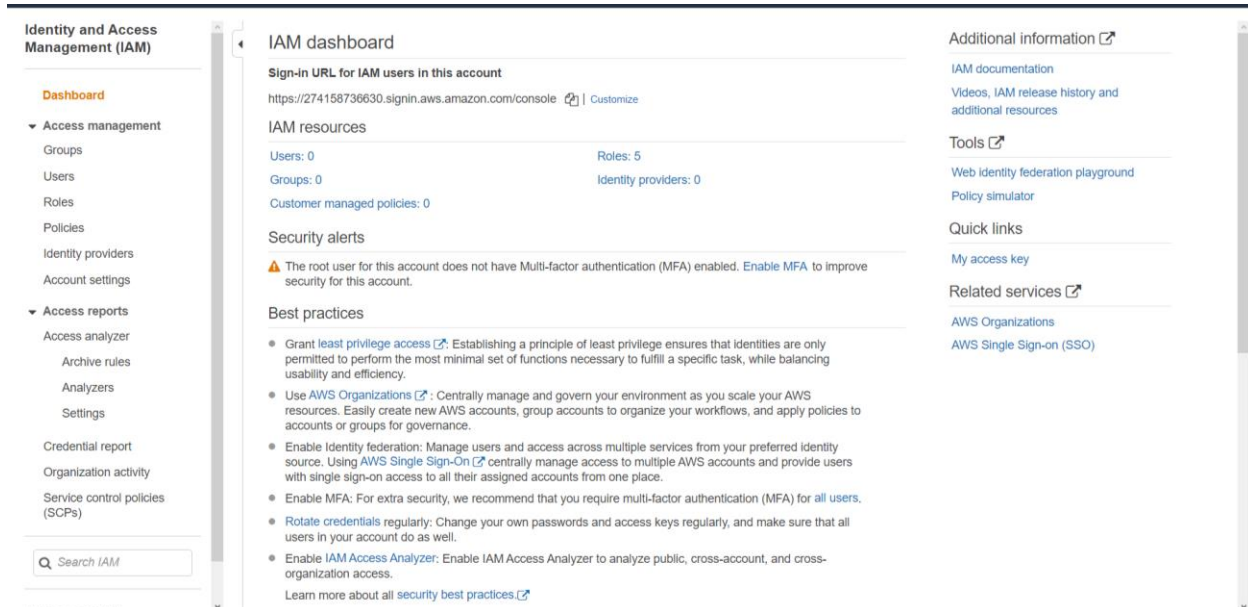


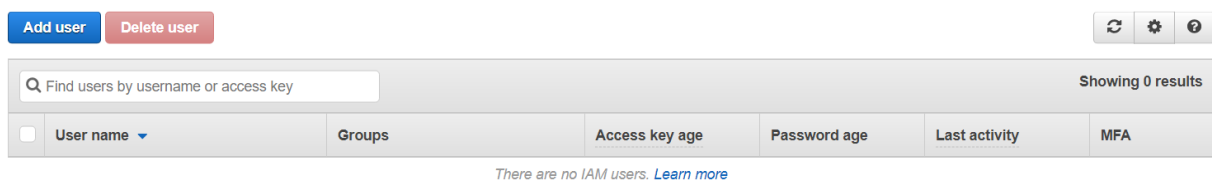
## Lab 4

### Create a new user from root using Identity and access management (IAM)

Step 1: Log in to AWS Console and then choose IAM .Now its Showing Users 0 because there is IAM user is created yet.



Step 2 : Click on add user Button



Step 3: Enter user details

- Enter username
- Access type:( Select the required Access type)
  - Programmatic access
  - AWS Management Console Access

Step 4: Enter the Console Password

- Autogenerated password
- Custom Password

Step 5: Check Required password reset box

## Step 6: Click on Next:Permission Button to go to set permission panel

Set user details

You can add multiple users at once with the same access type and permissions. [Learn more](#)

User name\*

[Add another user](#)

Select AWS access type

Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. [Learn more](#)

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

☒ **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

Require password reset ☒ User must create a new password at next sign-in  
Users automatically get the `IAMUserChangePassword` policy to allow them to change their own password.

\* Required

[Cancel](#) [Next: Permissions](#)

## Step 7: Set Permissions to user

- Add user or group
- Copy permission from existing users
- Attach existing policies directly(Search for the required policy for the user)

### ▼ Set permissions

[Add user to group](#) [Copy permissions from existing user](#) [Attach existing policies directly](#)

[Create policy](#) [Refresh](#)

Filter policies ▼  Showing 637 results

	Policy name ▼	Type	Used as
<input checked="" type="checkbox"/>	AdministratorAccess	Job function	None
<input type="checkbox"/>	AdministratorAccess-Amplify	AWS managed	None
<input type="checkbox"/>	AlexaForBusinessDeviceSetup	AWS managed	None
<input type="checkbox"/>	AlexaForBusinessFullAccess	AWS managed	None
<input type="checkbox"/>	AlexaForBusinessGatewayExecution	AWS managed	None
<input type="checkbox"/>	AlexaForBusinessLifesizeDelegatedAccessPolicy	AWS managed	None
<input type="checkbox"/>	AlexaForBusinessPolyDelegatedAccessPolicy	AWS managed	None
<input type="checkbox"/>	AlexaForBusinessReadOnlyAccess	AWS managed	None

► Set permissions boundary

[Cancel](#) [Previous](#) [Next: Tags](#)

## Step 8 : Review the settings and Click on create user button

## Review

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

### User details

<b>User name</b>	Developer
<b>AWS access type</b>	AWS Management Console access - with a password
<b>Console password type</b>	Custom
<b>Require password reset</b>	Yes
<b>Permissions boundary</b>	Permissions boundary is not set

### Permissions summary

The following policies will be attached to the user shown above.

Type	Name
Managed policy	<a href="#">AdministratorAccess</a>
Managed policy	<a href="#">IAMUserChangePassword</a>

### Tags

No tags were added.

[Cancel](#)[Previous](#)[Create user](#)

## Step 9: Confirmation message for user creation

### ✓ 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://274158736630.signin.aws.amazon.com/console>

[Download .csv](#)

	User	Email login instructions
▶ ✓	Developer	<a href="#">Send email</a> <a href="#">↗</a>

## Step 10: User can Login using generated unique URL

## Step 11: Enter 12 Digit Account ID

## Step 12: Enter IAM Username & password



### Sign in as IAM user

Account ID (12 digits) or account alias

274158736630

IAM user name

Developer

Password

.....

Sign in

[Sign in using root user email](#)

[Forgot password?](#)



English

[Terms of Use](#) [Privacy Policy](#) © 1996-2021, Amazon Web Services, Inc. or its affiliates.

Step 13: For first login IAM user need to change his password

- Users need to enter his old password in order to set the new password



You must change your password to continue

AWS account 274158736630

IAM user name Developer

Old password

New password

Retype new password

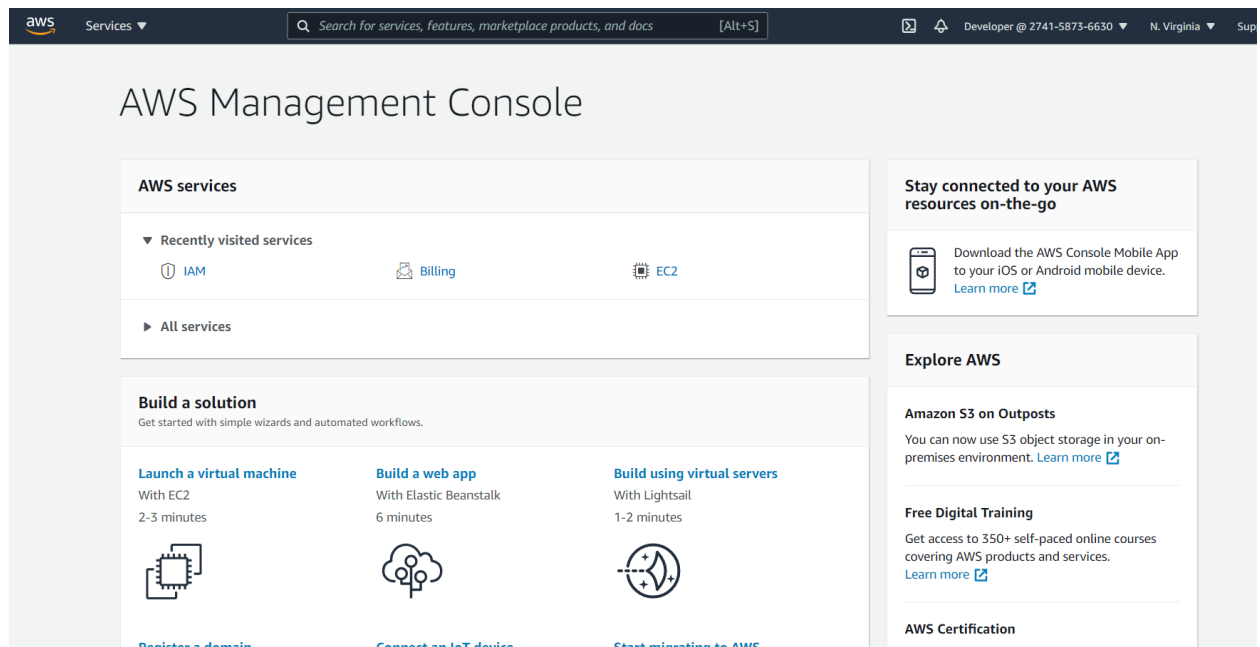
Confirm password change

[Sign in using root user email](#)

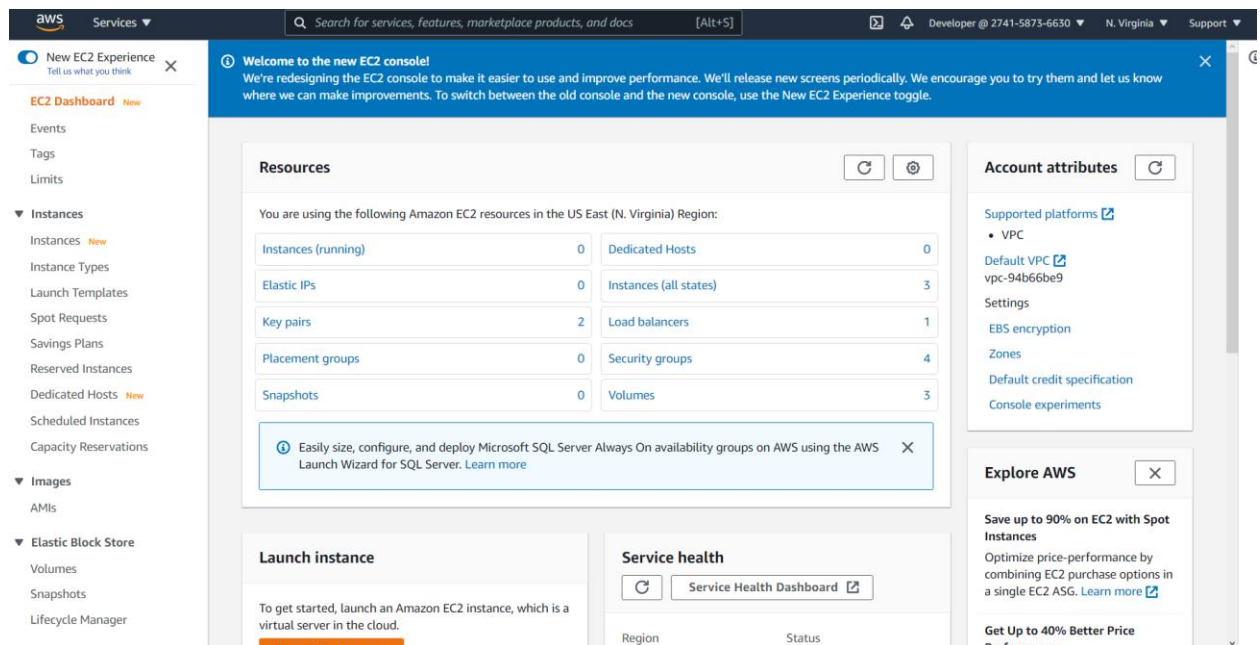
English

[Terms of Use](#) [Privacy Policy](#) © 1996-2021, Amazon Web Services, Inc. or its affiliates.

Step 14: User Login to AWS Account with given privilege



Step 15: IAM user have AdministratorAccess Permission so he has access to the AWS resources according administrator privilege



Step 16 : User account have privilege to create S3 bucket as because root user have given permission to Write.

aws

Services

Search for services, features, marketplace products, and docs

[Alt+S]

Developer @ 2741-5873-6630

Global

Support

Amazon S3

Create bucket

Create bucket

Buckets are containers for data stored in S3. [Learn more](#)

General configuration

Bucket name

myawsbucket

Bucket name must be unique and must not contain spaces or uppercase letters. [See rules for bucket naming](#)

Region

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

Copy settings from existing bucket - optional

Only the bucket settings in the following configuration are copied.

Choose bucket

Bucket settings for Block Public Access

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.

Step 17: Root user can delete the IAM user account by going to IAM Console and clicking Delete user button

Add userDelete user

Find users by username or access key

Showing 1 result

<input checked="" type="checkbox"/>	User name	Groups	Access key age	Password age	Last activity	MFA
<input checked="" type="checkbox"/>	Developer	None	None	Today	Today	Not enabled