

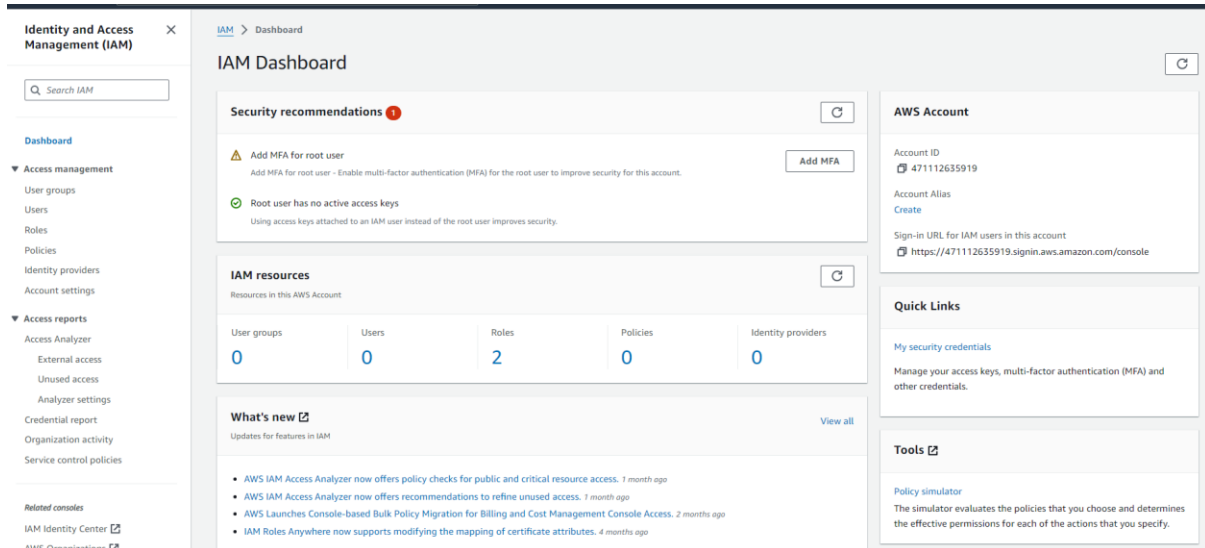
NAME: Suraj Giramkar

SAP ID: 86062300052

Roll No.: A014

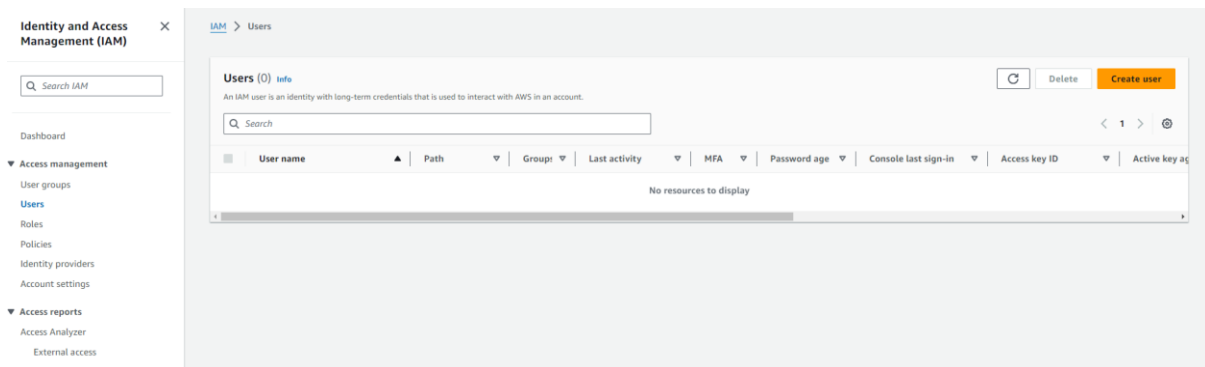
### Practical 3: Identity and Access Management

Search IAM after logging into your AWS account.



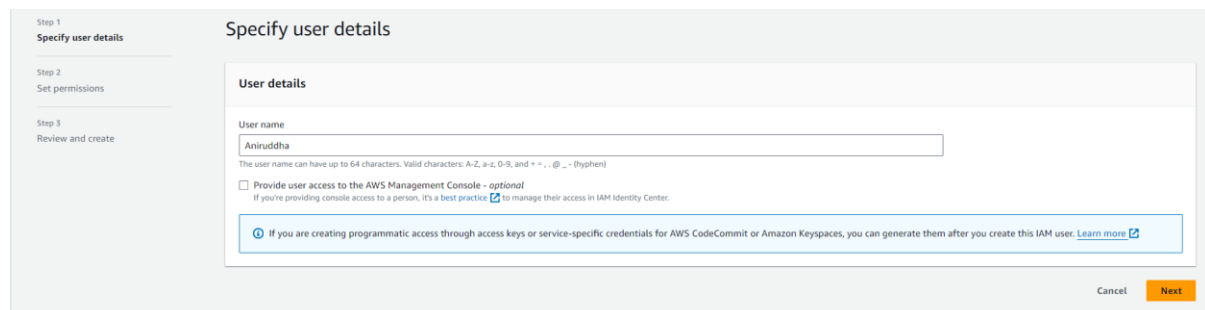
The screenshot shows the AWS IAM Dashboard. On the left is a navigation sidebar with sections: 'Dashboard', 'Access management' (containing User groups, Users, Roles, Policies, Identity providers, Account settings), 'Access reports' (containing Access Analyzer, External access, Unused access, Analyzer settings, Credential report, Organization activity, Service control policies), and 'Related consoles' (containing IAM Identity Center and AWS Organizations). The main content area is titled 'IAM Dashboard' and includes: 'Security recommendations' with a warning to 'Add MFA for root user' and a note that the 'Root user has no active access keys'; 'IAM resources' showing counts for User groups (0), Users (0), Roles (2), Policies (0), and Identity providers (0); 'What's new' with updates for IAM Access Analyzer and IAM Roles Anywhere; 'AWS Account' information including Account ID, Alias, and Sign-in URL; 'Quick Links' for security credentials; and 'Tools' including a policy simulator.

Select Users from left tab and create user



The screenshot shows the 'Users' page in the AWS IAM console. The left sidebar is the same as the dashboard. The main content area is titled 'Users (0)' and includes a search bar, a table with columns for User name, Path, Group, Last activity, MFA, Password age, Console last sign-in, Access key ID, and Active key age. Below the table, it states 'No resources to display'. At the top right of the main content area are buttons for 'Delete' and 'Create user'.

Enter user name



The screenshot shows the 'Specify user details' step in the AWS IAM console. The left sidebar shows a progress bar with three steps: 'Step 1: Specify user details' (active), 'Step 2: Set permissions', and 'Step 3: Review and create'. The main content area is titled 'Specify user details' and includes a 'User details' section with a 'User name' field containing 'Aniruddha'. Below the field, it states 'The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and +, -, @, \_ (hyphen)'. There is a checkbox for 'Provide user access to the AWS Management Console - optional' with a note that it's a best practice to manage access in IAM Identity Center. At the bottom right are 'Cancel' and 'Next' buttons.

## Update policies to attach policies directly

### 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.

#### Permissions policies (1223)

Choose one or more policies to attach to your new user.

Filter by TypeAll types

<input type="checkbox"/>	Policy name	Type	Attached entities
<input type="checkbox"/>	<a href="#">AccessAnalyzerServiceRolePolicy</a>	AWS managed	0
<input type="checkbox"/>	<a href="#">AdministratorAccess</a>	AWS managed - job function	0
<input type="checkbox"/>	<a href="#">AdministratorAccess-Amplify</a>	AWS managed	0
<input type="checkbox"/>	<a href="#">AdministratorAccess-AWSElasticBeanstalk</a>	AWS managed	0
<input type="checkbox"/>	<a href="#">AlexaForBusinessDeviceSetup</a>	AWS managed	0
<input type="checkbox"/>	<a href="#">AlexaForBusinessFullAccess</a>	AWS managed	0
<input type="checkbox"/>	<a href="#">AlexaForBusinessGatewayExecution</a>	AWS managed	0

## Enable console access by selecting security credential and select autogenerated password

uddha

Disabled

Create access key

### Enable console access

Enable console access for Aniruddha.

Console password

☒ Autogenerated password

☐ Custom password

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

Cancel

Enable console access

A) (0)

Remove

Resync

Copy the url for I AM user login: <https://471112635919.signin.aws.amazon.com/console>

Password: 8lY5] '[@



## Sign in as IAM user

Account ID (12 digits) or account alias

471112635919

IAM user name

Aniruddha


Password

.....|

☐ Remember this account

Sign in



Sign in as IAM user by opening incognito tab and check if you have the access

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



### Failed to create bucket

To create a bucket, the `s3:CreateBucket` permission is required.

View your permissions in the [IAM console](#) . [Identity and Access Management in Amazon S3](#) 

▶ API response

Cancel

Create bucket

Attach policies to the IAM user

Select policy from the left tab and search for S3 services.

Specify permissions [Info](#)

Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.

Policy editor

VisualJSONActions

S3

Allow All actions

Specify what actions can be performed on specific resources in S3.

▼ Actions allowed

Specify actions from the service to be allowed.

Filter Actions

Manual actions | [Add actions](#)

☒ All S3 actions (s3:\*)

Access level

▶ List (Selected 15/15)

▶ Read (Selected 60/60)

▶ Write (Selected 57/57)

▶ Permissions management (Selected 15/15)

▶ Tagging (Selected 12/12)

Expand all | Collapse all

Effect

☒ Allow ☐ Deny

Dependent permissions not selected

Specify permissions [Info](#)

Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.

Policy editor

VisualJSONActions

1 {

2   "Version": "2012-10-17",

3   "Statement": [

4     {

5       "Sid": "Aniruddha",

6       "Effect": "Allow",

7       "Action": "s3:\*",

8       "Resource": "\*"

9     }

10   ]

11 }

Edit statement

Aniruddha

Remove

Add actions

Choose a service

Filter services

Included

S3

Available

AMP

# Review and create [info](#)

Review the permissions, specify details, and tags.

## Policy details

### Policy name

Enter a meaningful name to identify this policy.

aniruddha

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

### Description - optional

Add a short explanation for this policy.

Maximum 1,000 characters. Use alphanumeric and '+-.,@\_-' characters.

## Permissions defined in this policy [info](#)

Edit

Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it

Allow (1 of 420 services)

☐ Show remaining 419 services

Service	Access level	Resource	Request condition
<a href="#">S3</a>	Full access	All resources	None

## Permissions defined in this policy [info](#)

Edit

Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it

Allow (1 of 420 services)

☐ Show remaining 419 services

Service	Access level	Resource	Request condition
<a href="#">S3</a>	Full access	All resources	None

## Add tags - optional [info](#)

Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.

No tags associated with the resource.

Add new tag

You can add up to 50 more tags.

Cancel

Previous

Create policy

# Attach as a permissions policy

To define permissions for an IAM identity (user, user group, or role), attach a policy to it.

## IAM Entities (1/1)

Entities are IAM users, user groups and roles.

Filter by Entity type

All types

< 1 > ⌂

<input checked="" type="checkbox"/>	Entity name	Entity type
<input checked="" type="checkbox"/>	Aniruddha	IAM Users

Cancel

Attach policy

## Specify permissions [Info](#)

Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.

**Policy editor**

VisualJSONActions

▼ EC2

AllowAll actions

Specify what actions can be performed on specific resources in EC2.

▼ Actions allowed

Specify actions from the service to be allowed.

Manual actions | Add actions

☒ All EC2 actions (ec2:\*)

Access level

▶ List (Selected 175/175)

▶ Read (Selected 36/36)

▶ Write (Selected 420/420)

▶ Permissions management (Selected 5/5)

▶ Tagging (Selected 2/2)

Effect

☒ Allow ☐ Deny

Expand all | Collapse all

▼ Resources

Specify resource ARNs for these actions.

☒ All ☐ Specific

⚠ The all wildcard "\*" may be overly permissive for the selected actions. Allowing specific ARNs for these service resources can improve security.

▶ Request conditions - optional

Actions on resources are allowed or denied only when these conditions are met.

+ Add more permissions

Security: 0Errors: 0Warnings: 0Suggestions: 0

CancelNext

## Review and create [Info](#)

Review the permissions, specify details, and tags.

**Policy details**

Policy name

Enter a meaningful name to identify this policy.

Maximum 128 characters. Use alphanumeric and "+", "@", "-" characters.

Description - optional

Add a short explanation for this policy.

Maximum 1,000 characters. Use alphanumeric and "+", "@", "-" characters.

**Permissions defined in this policy** [Info](#)

Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM Identity (user, user group, or role), attach a policy to it

Allow (1 of 420 services) ☐ Show remaining 419 services

Service	Access level	Resource	Request condition
<a href="#">EC2</a>	Full access	All resources	None

**Add tags - optional** [Info](#)

aws

Services

[Alt+S]

Stockholm

Aniruddha @ 4711-1265-5919

EC2 > Instances > Launch an instance

Success

Successfully initiated launch of instance (i-0978cb2e46146c29c)