Name :- anjali punsi
Class :- D20B
Roll No :- 57
Experiment no :- 8

Aim :- To study and implement Identity and Access Management (IAM) practices on AWS/Azure cloud.

Theory :-

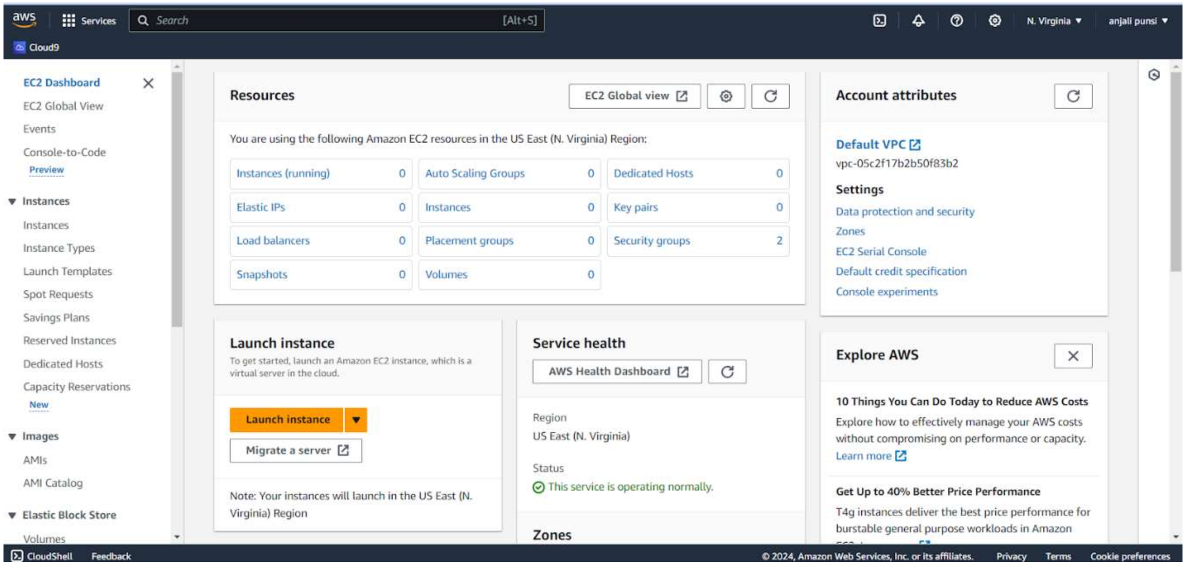
Identity and Access Management (IAM) is a foundational aspect of cloud computing security, enabling organizations to control access to their resources securely. In the context of cloud service providers like Amazon Web Services (AWS) and Microsoft Azure, IAM encompasses a set of practices and technologies designed to manage digital identities and their access to cloud resources. IAM involves the creation, management, and deletion of user accounts, groups, and roles, as well as the assignment of permissions to these entities. Each user is typically assigned a set of credentials, such as a username and password or access keys, which are used to authenticate their identity when accessing cloud services.

Groups are used to organize users based on their roles or permissions, making it easier to manage permissions at scale. Role-based access control (RBAC) is a key component of IAM, allowing organizations to define roles with specific permissions and then assign these roles to users or groups. RBAC helps enforce the principle of least privilege, ensuring that users have only the permissions necessary to perform their jobs.

Multi-factor authentication (MFA) adds an extra layer of security by requiring users to provide two or more verification factors, such as a password and a code sent to their mobile device, to access resources. This helps protect against unauthorized access even if a user's credentials are compromised. Access policies are used to define which actions are allowed or denied for a given user, group, or role. These policies are typically written in a JSON format and can be attached to users, groups, or resources.

Audit logging is another important aspect of IAM, enabling organizations to monitor and audit actions performed by users, groups, and roles. This helps in identifying and mitigating potential security threats, as well as maintaining compliance with regulatory requirements. Implementing IAM practices on AWS or Azure involves creating users, groups, roles, and policies, and assigning permissions based on the principle of least privilege. By following these practices, organizations can maintain a secure and compliant environment in the cloud, ensuring that only authorized entities have access to their resources.

Steps ━
Step 1:- Login to AWS console and Make sure to check all Ec2 dashboard parameters



Resources

You are using the following Amazon EC2 resources in the US East (N. Virginia) Region:

Instances (running)	0	Auto Scaling Groups	0	Dedicated Hosts	0
Elastic IPs	0	Instances	0	Key pairs	0
Load balancers	0	Placement groups	0	Security groups	2
Snapshots	0	Volumes	0		

vpc-05c2f17b2b50f83b2

Launch instance

To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

Note: Your instances will launch in the US East (N. Virginia) Region

Region

US East (N. Virginia)

Status

This service is operating normally.

10 Things You Can Do Today to Reduce AWS Costs

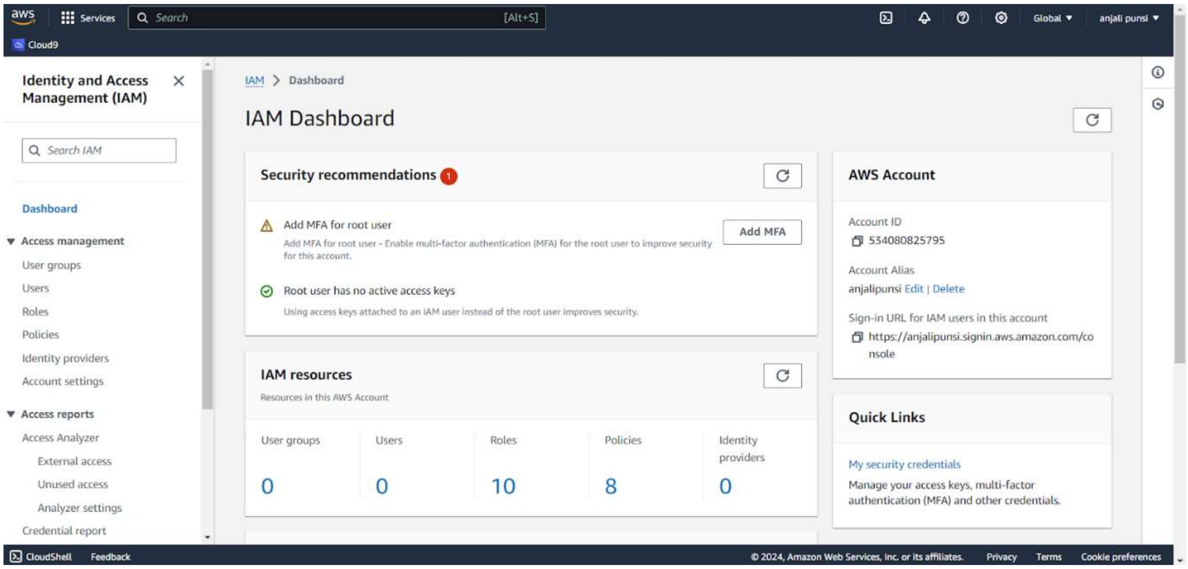
Explore how to effectively manage your AWS costs without compromising on performance or capacity. Learn more

Get Up to 40% Better Price Performance

T4g instances deliver the best price performance for burstable general purpose workloads in Amazon

© 2024, Amazon Web Services, Inc. or its affiliates.

Step 2 :- Go to IAM dashboard



IAM Dashboard

Security recommendations 1

Add MFA for root user

Add MFA for root user - Enable multi-factor authentication (MFA) for the root user to improve security for this account.

Root user has no active access keys

Using access keys attached to an IAM user instead of the root user improves security.

IAM resources

Resources in this AWS Account

User groups	Users	Roles	Policies	Identity providers
0	0	10	8	0

AWS Account

Account ID

534080825795

Account Alias

anjalipunsi Edit | Delete

Sign-in URL for IAM users in this account

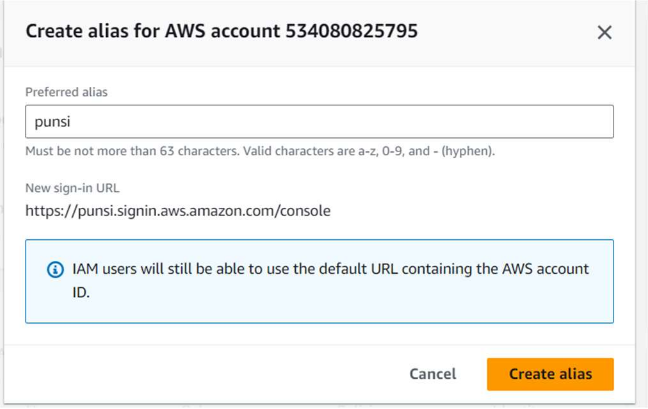
https://anjalipunsi.signin.aws.amazon.com/console

My security credentials

Manage your access keys, multi-factor authentication (MFA) and other credentials.

© 2024, Amazon Web Services, Inc. or its affiliates.

Step 3 :- Click on create option under Account Alias and give a valid name; save changes



Create alias for AWS account 534080825795

Preferred alias

punsi

Must be not more than 63 characters. Valid characters are a-z, 0-9, and - (hyphen).

New sign-in URL

https://punsi.signin.aws.amazon.com/console

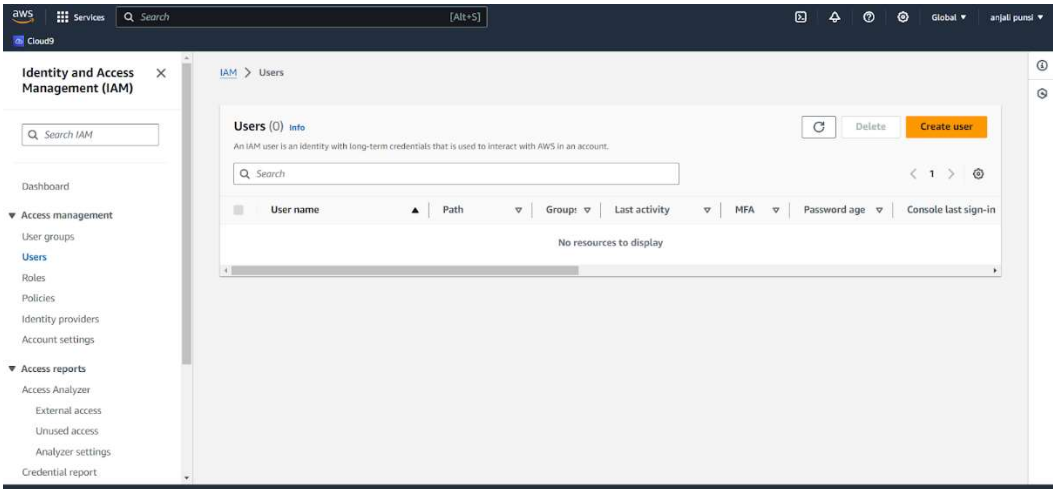
IAM users will still be able to use the default URL containing the AWS account ID.

Alias punsi created for this account.

IAM Dashboard

Step 4 :- (Download Google Authenticator from PlayStore in your Mobile Phone)

Click on “users” in the left column

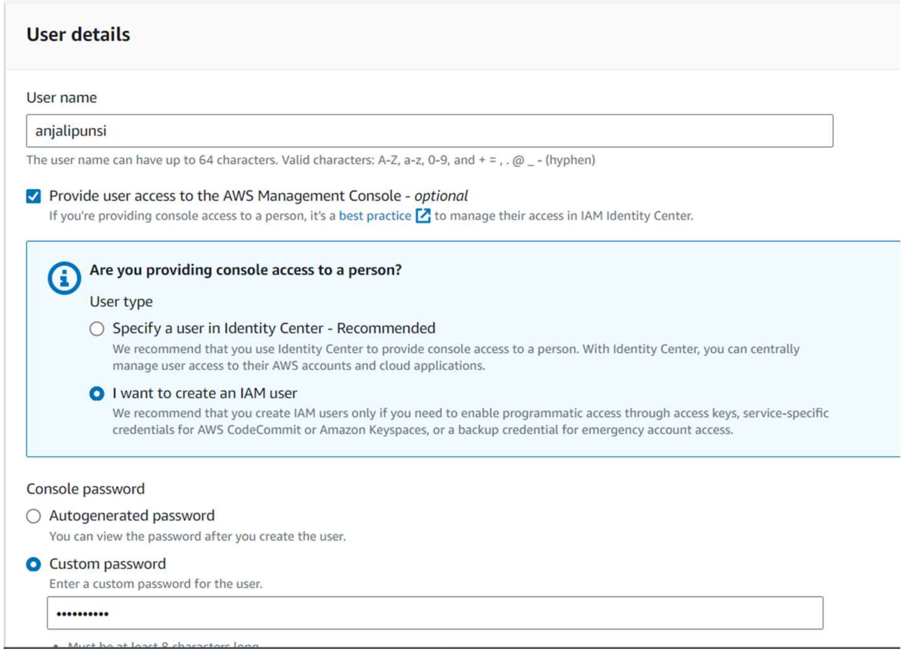


Users (0) Info

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

□	User name ▲	Path	Groups	Last activity	MFA	Password age	Console last sign-in
			No resources to display				

Step 5 :- Click on Add users button



User details

User name

anjalipunsi

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.

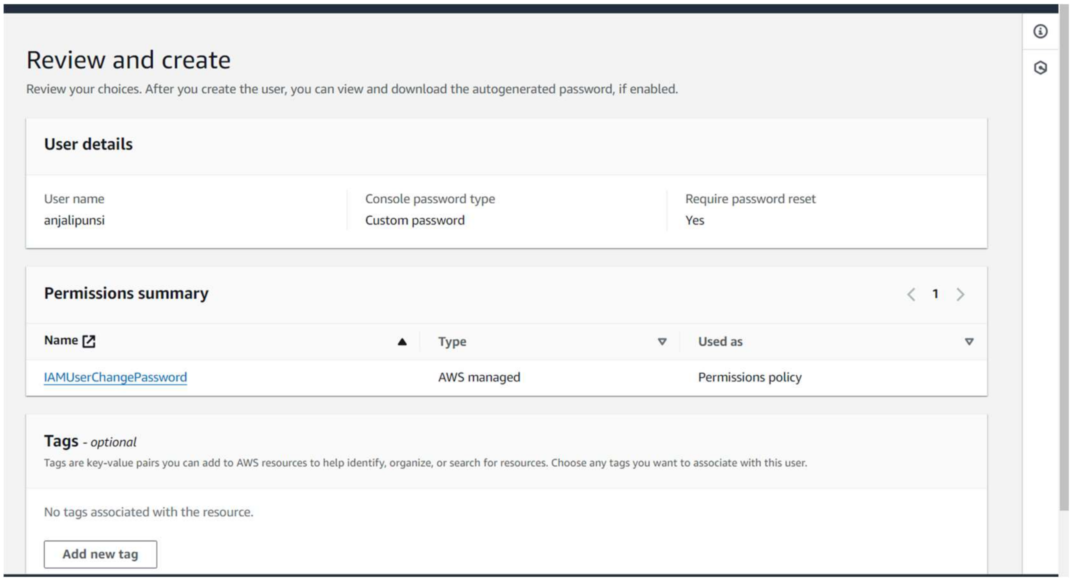
● Custom password

Enter a custom password for the user.

••••••••••

• Must be at least 8 characters long

Step 6 :- Set a custom valid psw (Imc: Qwertyuiop123) and check the Require psw rest box which will make you create a next psw in the next sign in



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	Console password type	Require password reset
anjalipunsi	Custom password	Yes

Permissions summary

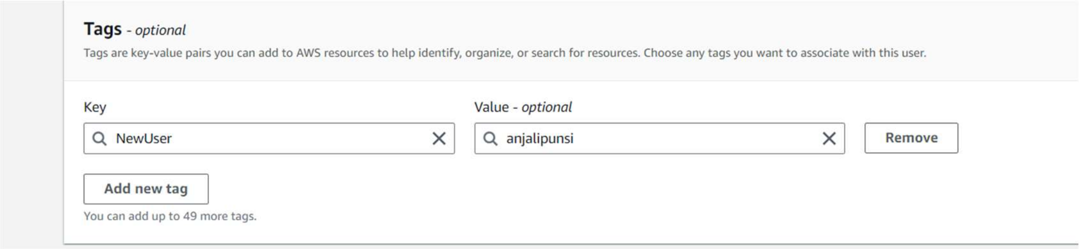
Name	Type	Used as
IAMUserChangePassword	AWS managed	Permissions policy

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.

Step 7 :- Click on Next: Tags Add a tag if you want to just to keep track of your activities; then click on Next: Review



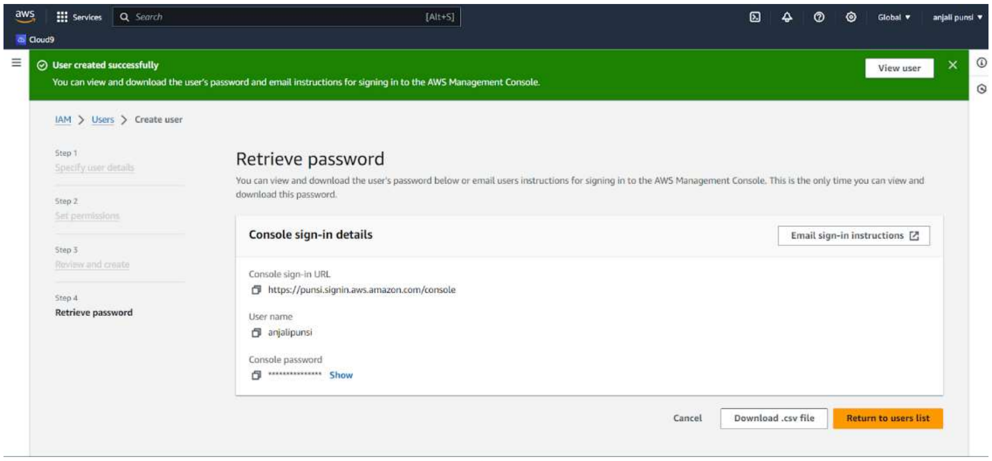
Tags - *optional*

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.

Key	Value - *optional*
NewUser	anjalipunsi

You can add up to 49 more tags.

Step 8 :- Click on Create User Button



User created successfully

You can view and download the user's password and email instructions for signing in to the AWS Management Console.

Retrieve password

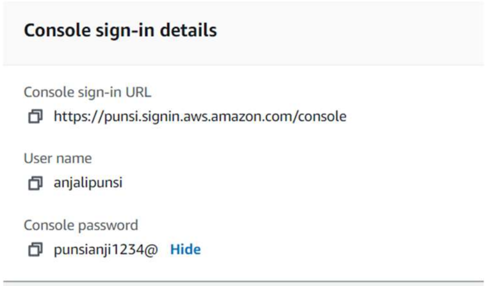
You can view and download the user's password below or email users instructions for signing in to the AWS Management Console. This is the only time you can view and download this password.

Console sign-in details

Console sign-in URL
https://punsi.signin.aws.amazon.com/console

User name
anjalipunsi

Console password
*************** Show



Console sign-in details

Console sign-in URL
https://punsi.signin.aws.amazon.com/console

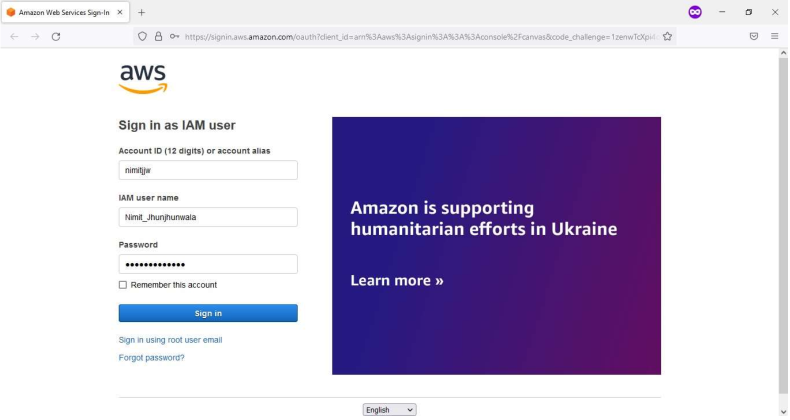
User name
anjalipunsi

Console password
punsianji1234@ Hide

Step 9 :- Open the URL in Incognito Mode (Imc: https://punsi.signin.aws.amazon.com/console)

Note: Save the secret access ID & key in a notepad or download the csv

Now by clicking link add alias which you set then add usename you kept then password of it



https://signin.aws.amazon.com/oauth?client_id=arn%3Aaws%3Asignin%3A%3A%3Aconsole%2Fcanvas&code_challenge=1zenwTcXpi4

Sign in as IAM user

Account ID (12 digits) or account alias: nimitjjw

IAM user name: Nimit_Jhunjhunwala

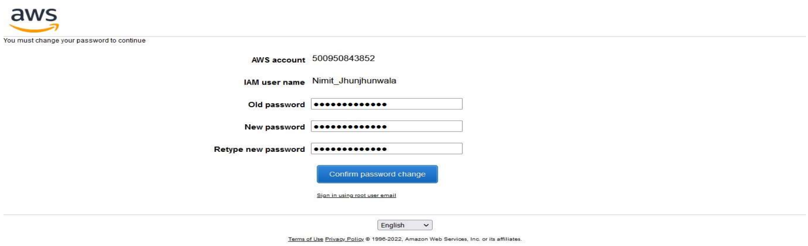
Password: ••••••••••••••

□ Remember this account

Amazon is supporting humanitarian efforts in Ukraine

Learn more »

Step 10 :- Enter a new valid psw



You must change your password to continue

AWS account: 500950843852

IAM user name: Nimit_Jhunjhunwala

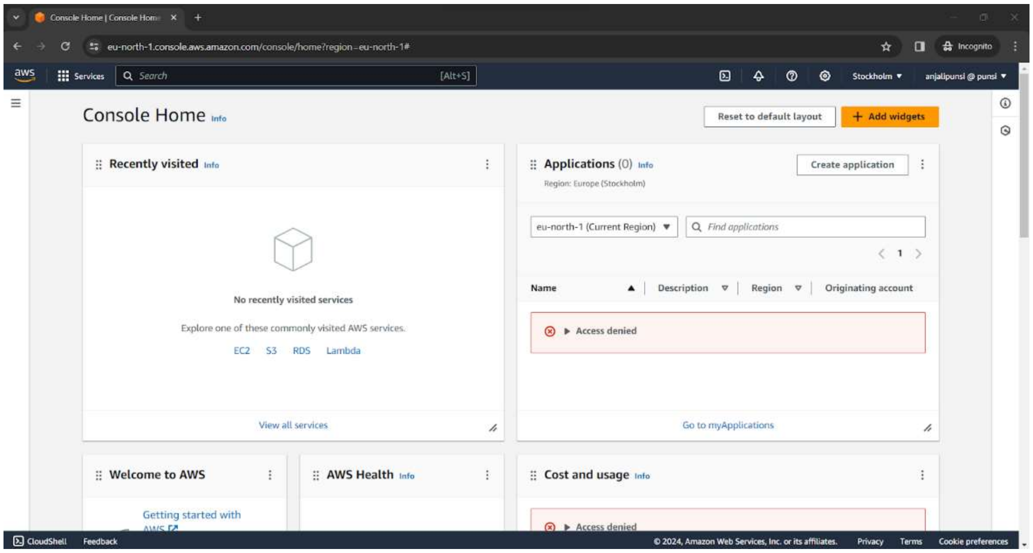
Old password: ••••••••••••••

New password: ••••••••••••••

Retype new password: ••••••••••••••

Terms of Use Privacy Policy © 1996-2022, Amazon Web Services, Inc. or its affiliates.

Step 11 :- After logging in, you will notice that you don't have permission to do anything yet



eu-north-1.console.aws.amazon.com/console/home?region=eu-north-1#

Console Home

Recently visited

No recently visited services

Explore one of these commonly visited AWS services.

Applications (0)

Region: Europe (Stockholm)

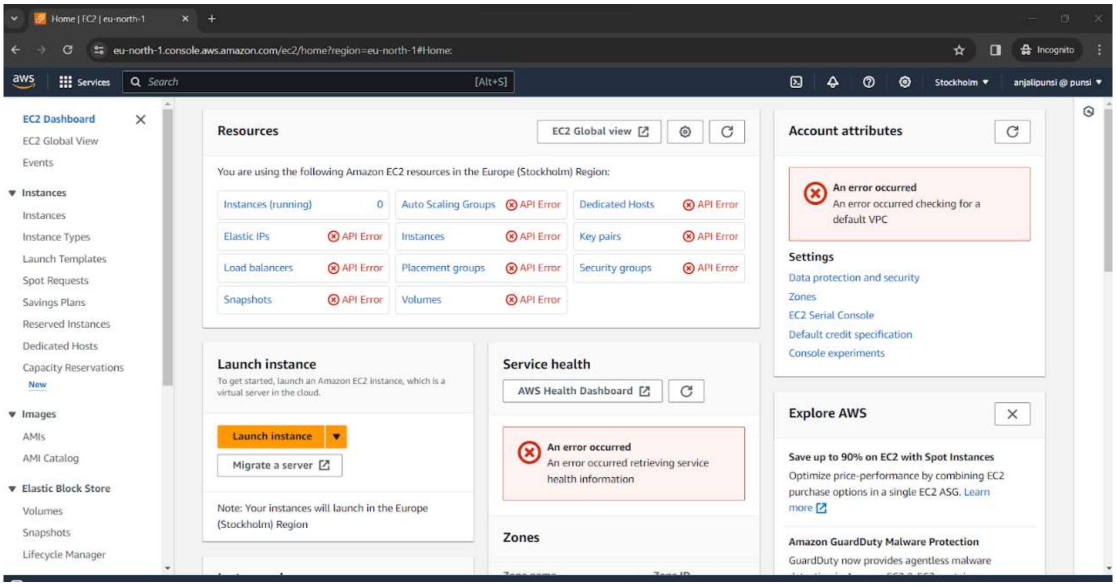
eu-north-1 (Current Region)

Access denied

Cost and usage

Access denied

© 2024, Amazon Web Services, Inc. or its affiliates.



Home | EC2 | eu-north-1

eu-north-1.console.aws.amazon.com/ec2/home?region=eu-north-1#Home:

Incognito

aws Services Search [Alt+S] Stockholm ▾ anjalipunsi @ punsi ▾

EC2 Dashboard
EC2 Global View
Events
▼ Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations New
▼ Images
AMIs
AMI Catalog
▼ Elastic Block Store
Volumes
Snapshots
Lifecycle Manager

Resources EC2 Global view

You are using the following Amazon EC2 resources in the Europe (Stockholm) Region:

Instances (running)	0	Auto Scaling Groups	⊗ API Error	Dedicated Hosts	⊗ API Error
Elastic IPs	⊗ API Error	Instances	⊗ API Error	Key pairs	⊗ API Error
Load balancers	⊗ API Error	Placement groups	⊗ API Error	Security groups	⊗ API Error
Snapshots	⊗ API Error	Volumes	⊗ API Error		

Account attributes

An error occurred
An error occurred checking for a default VPC

Settings
Data protection and security
Zones
EC2 Serial Console
Default credit specification
Console experiments

Launch instance

To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

Launch instance ▾

Migrate a server

Note: Your instances will launch in the Europe (Stockholm) Region

Service health

AWS Health Dashboard

An error occurred
An error occurred retrieving service health information

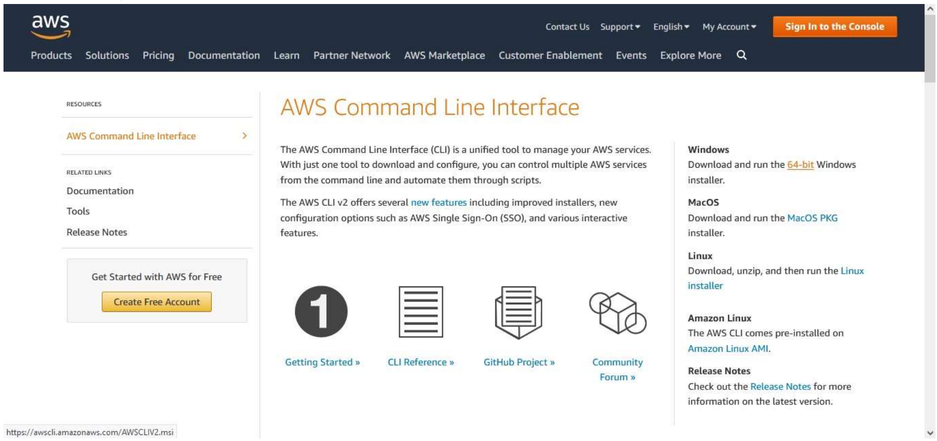
Zones

Explore AWS

Save up to 90% on EC2 with Spot Instances
Optimize price-performance by combining EC2 purchase options in a single EC2 ASG. Learn more

Amazon GuardDuty Malware Protection
GuardDuty now provides agentless malware

Step 12 :- Type "AWS CLI" in a new window of any browser and go to it's the main page of AWS regarding the same Click on 64-bit hyperlink in the RHS column under the Windows section and download, install the AWS CLI



aws

Contact Us Support ▾ English ▾ My Account ▾ Sign In to the Console

Products Solutions Pricing Documentation Learn Partner Network AWS Marketplace Customer Enablement Events Explore More

RESOURCES
AWS Command Line Interface ›

RELATED LINKS
Documentation
Tools
Release Notes

Get Started with AWS for Free
Create Free Account

AWS Command Line Interface

The AWS Command Line Interface (CLI) is a unified tool to manage your AWS services. With just one tool to download and configure, you can control multiple AWS services from the command line and automate them through scripts.

The AWS CLI v2 offers several new features including improved installers, new configuration options such as AWS Single Sign-On (SSO), and various interactive features.

Getting Started » CLI Reference » GitHub Project » Community Forum »

Windows
Download and run the 64-bit Windows installer.

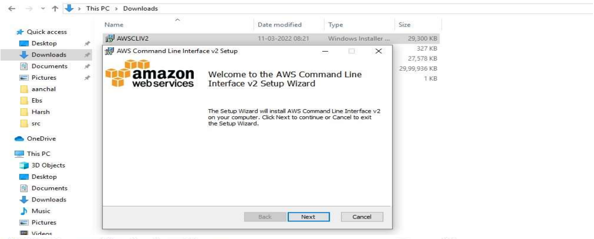
MacOS
Download and run the MacOS PKG installer.

Linux
Download, unzip, and then run the Linux installer

Amazon Linux
The AWS CLI comes pre-installed on Amazon Linux AMI.

Release Notes
Check out the Release Notes for more information on the latest version.

https://awscli.amazonaws.com/AWSCLIV2.msi



This PC › Downloads

Quick access
Desktop
Downloads
Documents
Pictures
aanchal
Ebs
Harsh
src
OneDrive
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos

Name	Date modified	Type	Size
AWSCLIV2	11-03-2022 08:21	Windows Installer ...	29,300 KB
			327 KB
			27,578 KB
			29,99,936 KB
			1 KB

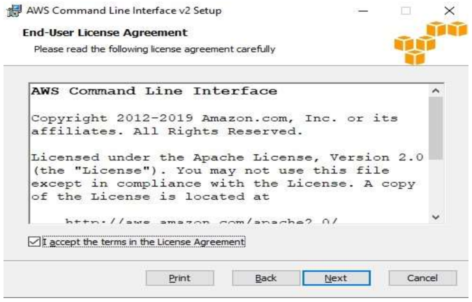
AWS Command Line Interface v2 Setup

amazon web services

Welcome to the AWS Command Line Interface v2 Setup Wizard

The Setup Wizard will install AWS Command Line Interface v2 on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

Back Next Cancel



AWS Command Line Interface v2 Setup

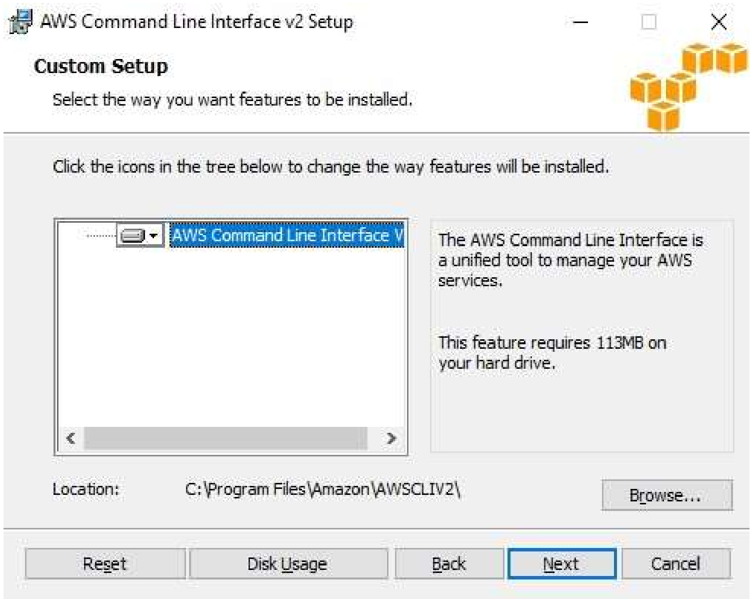
End-User License Agreement

Please read the following license agreement carefully

```
AWS Command Line Interface

Copyright 2012-2019 Amazon.com, Inc. or its
affiliates. All Rights Reserved.

Licensed under the Apache License, Version 2.0
(the "License"). You may not use this file
except in compliance with the License. A copy
of the License is located at

    http://aws.amazon.com/apache2.0/
```

☑ I accept the terms in the License Agreement

Print Back Next Cancel



AWS Command Line Interface v2 Setup

Custom Setup

Select the way you want features to be installed.

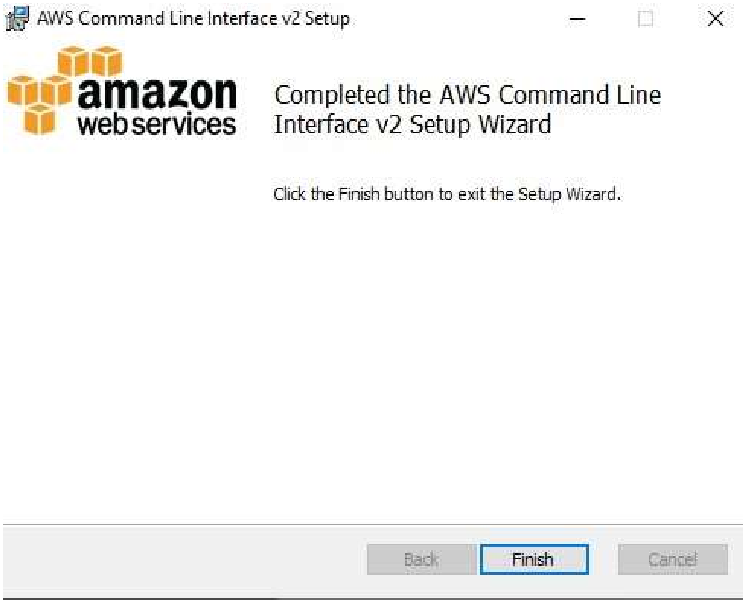
Click the icons in the tree below to change the way features will be installed.

AWS Command Line Interface V

The AWS Command Line Interface is a unified tool to manage your AWS services.

This feature requires 113MB on your hard drive.

Location: C:\Program Files\Amazon\AWSCLIV2\



AWS Command Line Interface v2 Setup

Completed the AWS Command Line Interface v2 Setup Wizard

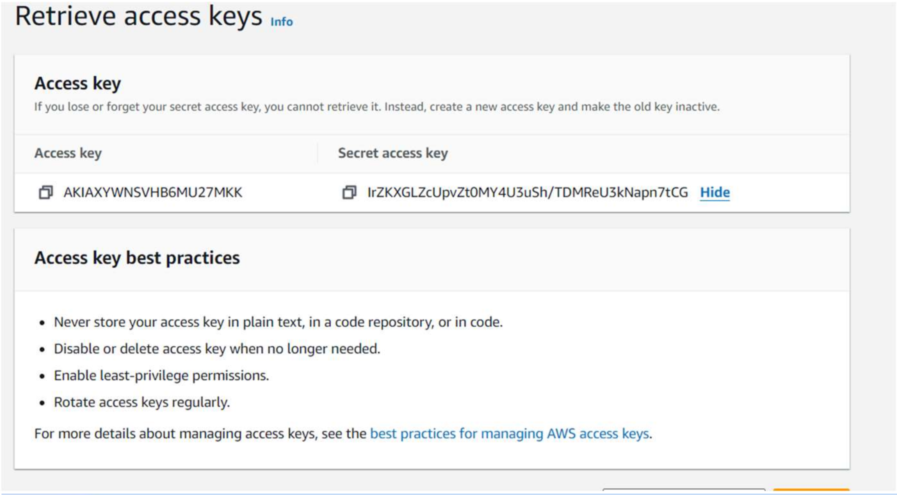
Click the Finish button to exit the Setup Wizard.

Step 13 :- Type “cmd” in the windows search bar and run it as an administrator

Type `aws configure`, it will ask for a few inputs;

AWS Access Key ID and Key are the ones which we saved earlier

Default region name is whichever region AWS you are using; in case of Mumbai, its: `ap-south-1` The output format is `json` in our case



Retrieve access keys Info

Access key

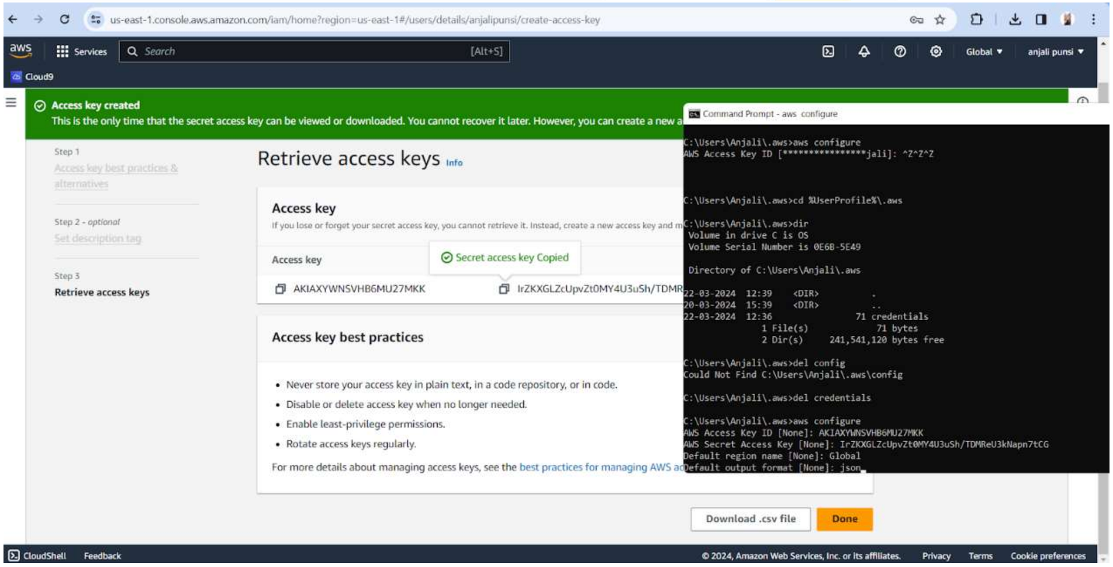
If you lose or forget your secret access key, you cannot retrieve it. Instead, create a new access key and make the old key inactive.

Access key	Secret access key
AKIAXYWNSVHB6MU27MKK	IrZKXGLZcUpvZt0MY4U3uSh/TDMReU3kNapn7tCG Hide

Access key best practices

- Never store your access key in plain text, in a code repository, or in code.
- Disable or delete access key when no longer needed.
- Enable least-privilege permissions.
- Rotate access keys regularly.

For more details about managing access keys, see the best practices for managing AWS access keys.



us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/users/details/anjalipunsi/create-access-key

Access key created

This is the only time that the secret access key can be viewed or downloaded. You cannot recover it later. However, you can create a new a

Step 1 Access key best practices & alternatives

Step 2 - optional Set description tag

Step 3 Retrieve access keys

Retrieve access keys Info

Access key

If you lose or forget your secret access key, you cannot retrieve it. Instead, create a new access key and m

Secret access key Copied

Access key	
AKIAXYWNSVHB6MU27MKK	IrZKXGLZcUpvZt0MY4U3uSh/TDMR

Access key best practices

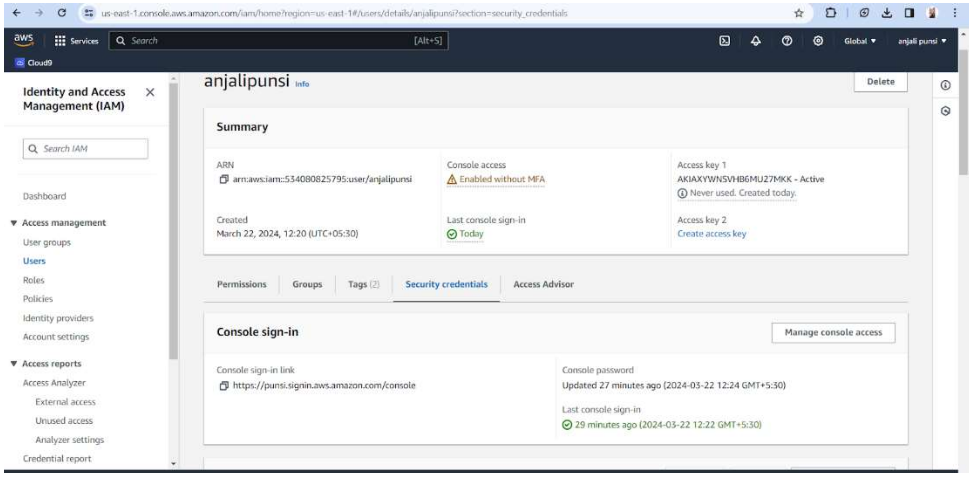
- Never store your access key in plain text, in a code repository, or in code.
- Disable or delete access key when no longer needed.
- Enable least-privilege permissions.
- Rotate access keys regularly.

For more details about managing access keys, see the best practices for managing AWS ac

Command Prompt - aws configure

```
C:\Users\Anjali\.aws>aws configure
AWS Access Key ID [***************jali]: ^Z^Z^Z


C:\Users\Anjali\.aws>cd %UserProfile%\.aws

C:\Users\Anjali\.aws>dir
 Volume in drive C is OS
 Volume Serial Number is 0E6B-5E49

 Directory of C:\Users\Anjali\.aws

22-03-2024  12:39    <DIR>          .
20-03-2024  15:39    <DIR>          ..
22-03-2024  12:36                71 credentials
               1 File(s)             71 bytes
               2 Dir(s)     241,541,120 bytes free

C:\Users\Anjali\.aws>del config
Could Not Find C:\Users\Anjali\.aws\config

C:\Users\Anjali\.aws>del credentials

C:\Users\Anjali\.aws>aws configure
AWS Access Key ID [None]: AKIAXYWNSVHB6MU27MKK
AWS Secret Access Key [None]: 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
Default region name [None]: Global
Default output format [None]: json
```

Step 14 :- Go in the security credentials tab under Users of IAM Dashboard



us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/users/details/anjalipunsi?section=security_credentials

anjalipunsi Info

Summary

ARN: arn:aws:iam::534080825795:user/anjalipunsi

Console access: Enabled without MFA

Access key 1: AKIAXYWNSVHB6MU27MKK - Active
Never used. Created today.

Created: March 22, 2024, 12:20 (UTC+05:30)

Last console sign-in: Today

Access key 2: Create access key

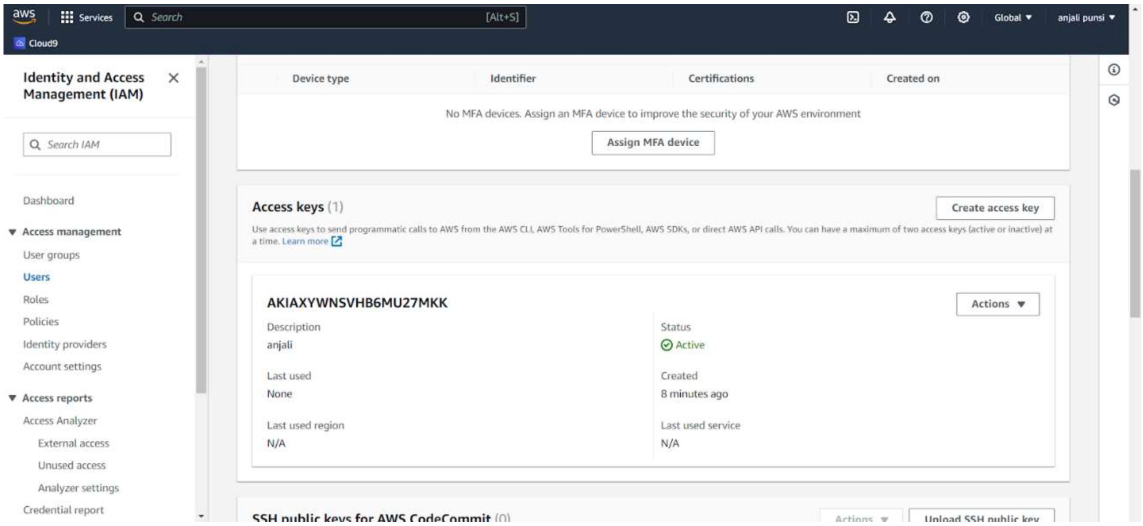
Console sign-in

Console sign-in link: https://punsi.signin.aws.amazon.com/console

Console password: Updated 27 minutes ago (2024-03-22 12:24 GMT+5:30)

Last console sign-in: 29 minutes ago (2024-03-22 12:22 GMT+5:30)

Step 15 :- Click on the “Manage” Hyperlink



Device type	Identifier	Certifications	Created on

No MFA devices. Assign an MFA device to improve the security of your AWS environment

Assign MFA device

Access keys (1)

Create access key

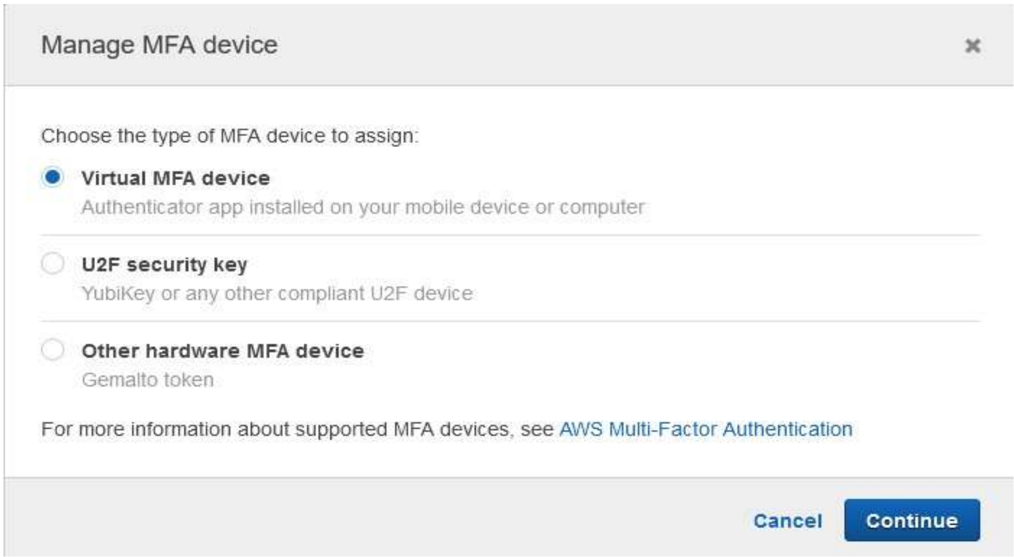
Use access keys to send programmatic calls to AWS from the AWS CLI, AWS Tools for PowerShell, AWS SDKs, or direct AWS API calls. You can have a maximum of two access keys (active or inactive) at a time. Learn more

AKIAXYWNSVHB6MU27MKK

Actions ▼

Description anjali	Status Active
Last used None	Created 8 minutes ago
Last used region N/A	Last used service N/A

SSH public keys for AWS CodeCommit (0)


Manage MFA device

Choose the type of MFA device to assign:

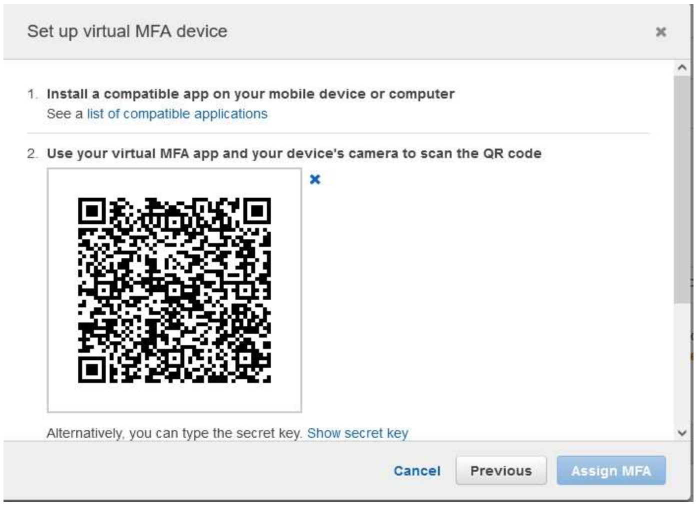
● **Virtual MFA device**
Authenticator app installed on your mobile device or computer

○ **U2F security key**
YubiKey or any other compliant U2F device

○ **Other hardware MFA device**
Gemalto token

For more information about supported MFA devices, see AWS Multi-Factor Authentication

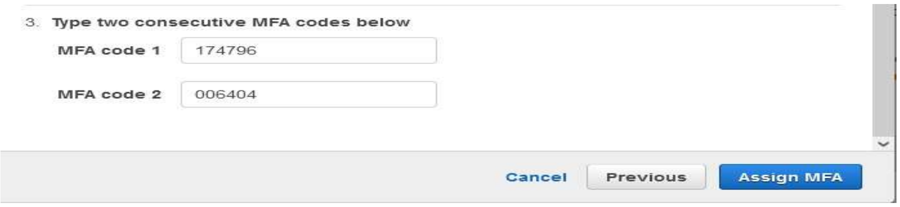
Step 16 :- Use the Google Authenticator app downloaded earlier to scan the QR Code


Set up virtual MFA device

1. **Install a compatible app on your mobile device or computer**
   See a list of compatible applications
2. **Use your virtual MFA app and your device's camera to scan the QR code**

Alternatively, you can type the secret key. Show secret key

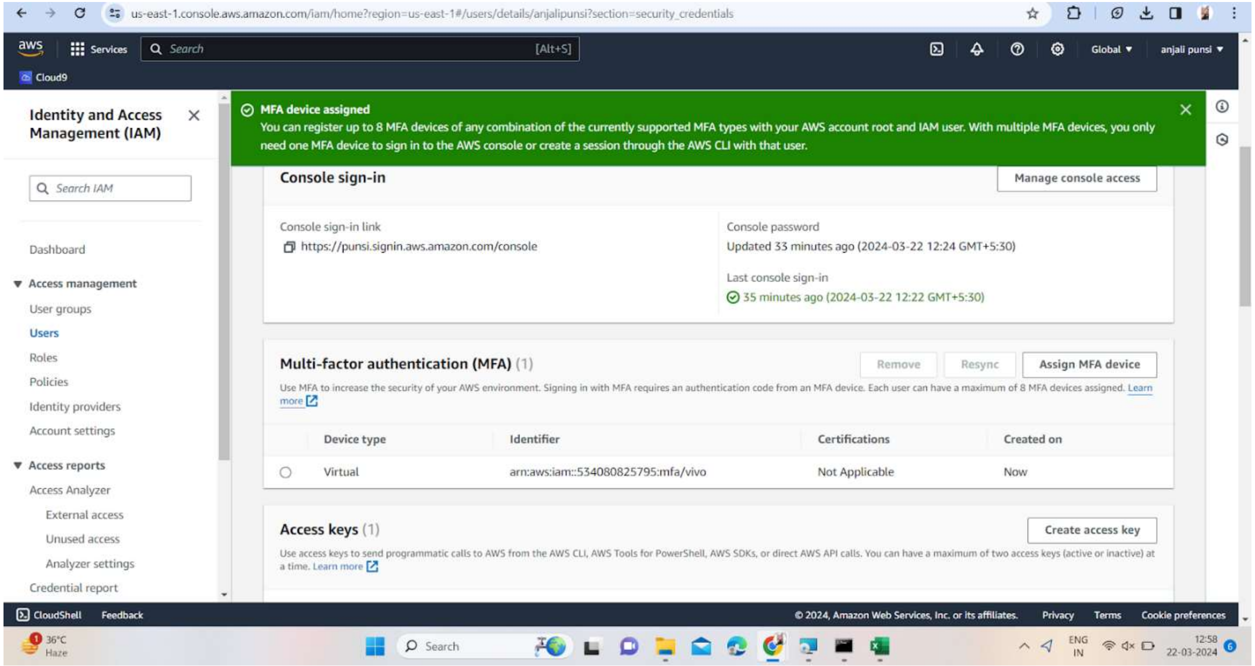
Step 17 :- Enter two of the codes which are shown in the Google Authenticator App over a span of 30 secs each; click on Assign MFA Button



3. Type two consecutive MFA codes below

MFA code 1: 174796

MFA code 2: 006404



us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/users/details/anjalipunsi?section=security_credentials

MFA device assigned

You can register up to 8 MFA devices of any combination of the currently supported MFA types with your AWS account root and IAM user. With multiple MFA devices, you only need one MFA device to sign in to the AWS console or create a session through the AWS CLI with that user.

Console sign-in

Console sign-in link: https://punsi.signin.aws.amazon.com/console

Console password: Updated 33 minutes ago (2024-03-22 12:24 GMT+5:30)

Last console sign-in: 35 minutes ago (2024-03-22 12:22 GMT+5:30)

Multi-factor authentication (MFA) (1)

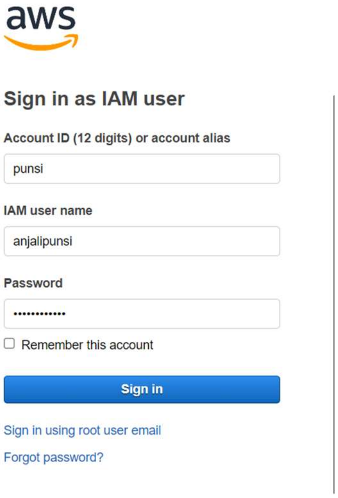
Use MFA to increase the security of your AWS environment. Signing in with MFA requires an authentication code from an MFA device. Each user can have a maximum of 8 MFA devices assigned. Learn more

	Device type	Identifier	Certifications	Created on
○	Virtual	arn:aws:iam::534080825795:mfa/vivo	Not Applicable	Now

Access keys (1)

Use access keys to send programmatic calls to AWS from the AWS CLI, AWS Tools for PowerShell, AWS SDKs, or direct AWS API calls. You can have a maximum of two access keys (active or inactive) at a time. Learn more

Step 18 :- Again try logging in via the new user created earlier; this time it will ask for MFA after you click on Sign In



Sign in as IAM user

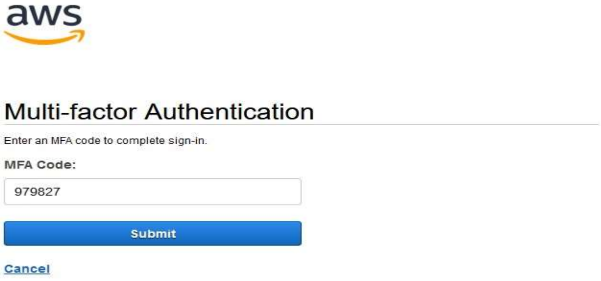
Account ID (12 digits) or account alias: punsi

IAM user name: anjalipunsi

Password: ••••••••••••

□ Remember this account

Step 19 :- Use the code being shown in the Google Authenticator

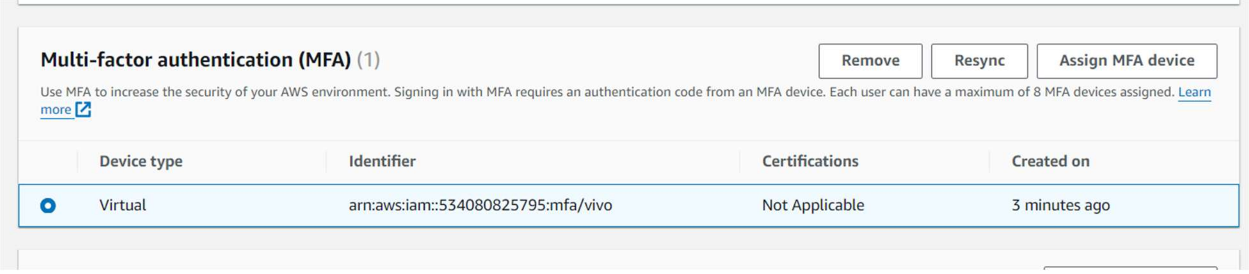


Multi-factor Authentication

Enter an MFA code to complete sign-in.

MFA Code: 979827

Step 20 :- Now, after opening the root user window again After going in the Users section of IAM Dashboard, we can see that MFA has been activated for the new user

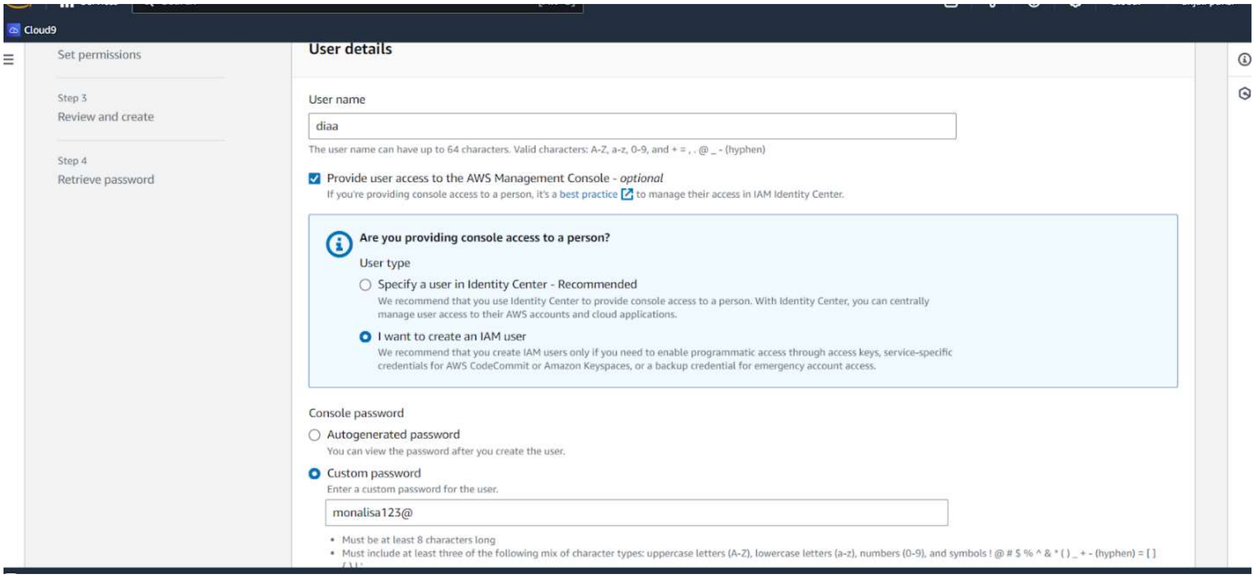


Multi-factor authentication (MFA) (1)

Use MFA to increase the security of your AWS environment. Signing in with MFA requires an authentication code from an MFA device. Each user can have a maximum of 8 MFA devices assigned. Learn more

	Device type	Identifier	Certifications	Created on
●	Virtual	arn:aws:iam::534080825795:mfa/vivo	Not Applicable	3 minutes ago

Step 21 :-Now, Adding 1 More Users



User details

User name: diaa

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.

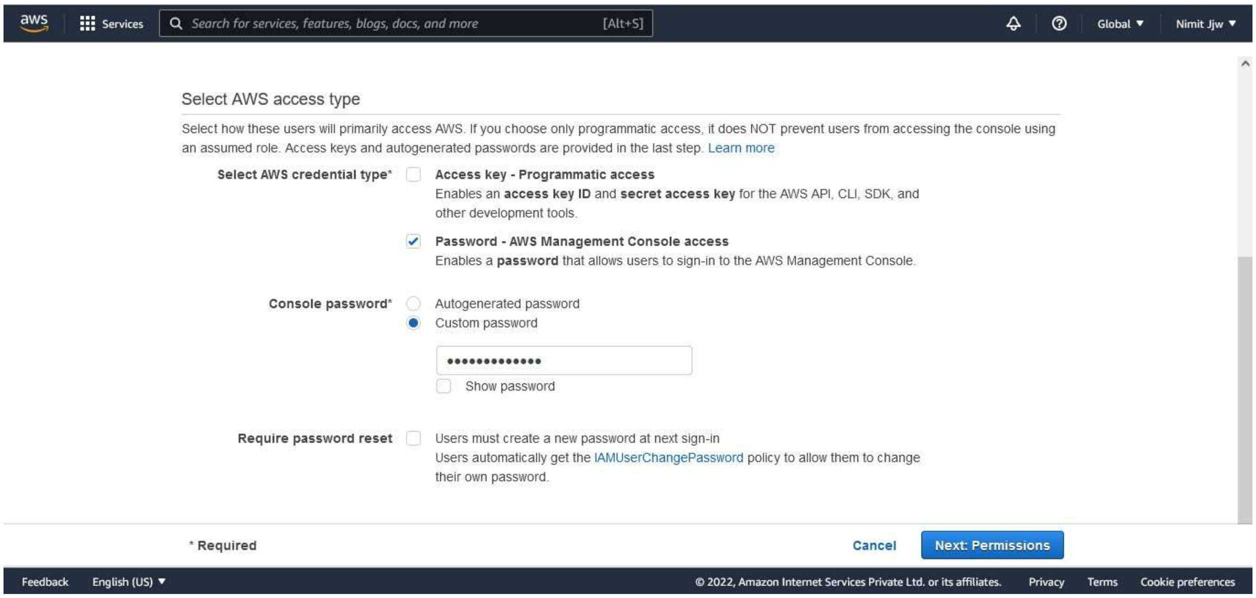
● Custom password

Enter a custom password for the user.

monalisa123@

- 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) = [ ]

Step 22 :-Not giving them an Access key and not checking the Psw Reset Checkbox; Click on the Next: Permissions


aws
Services
Search for services, features, blogs, docs, and more [Alt+S]
Global ▼
Nimit Jjw ▼

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

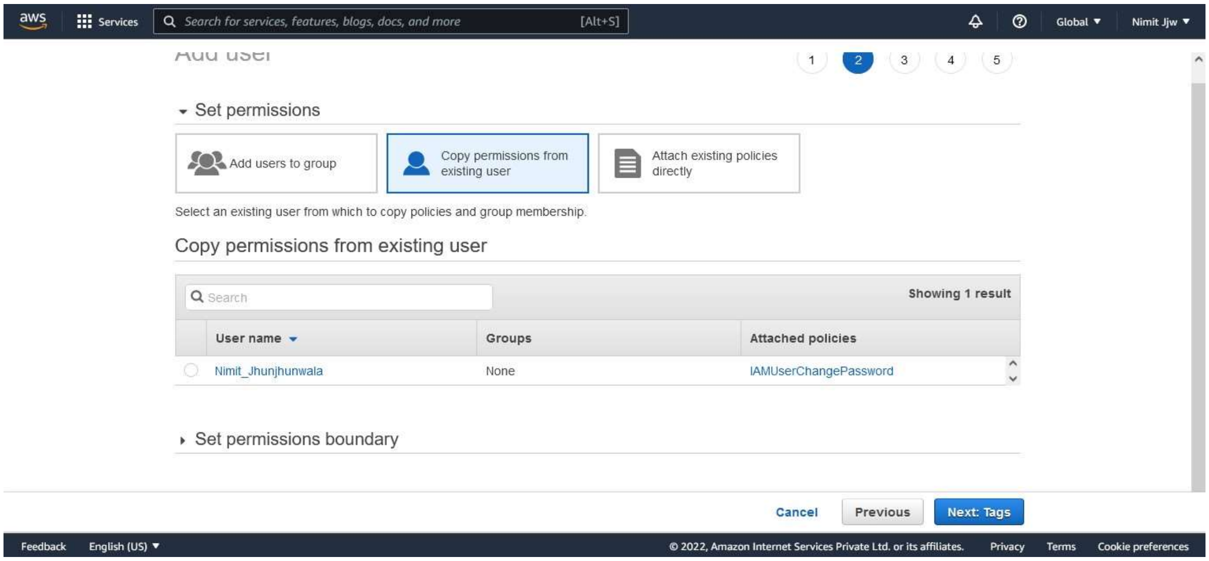
Require password reset □ Users must create a new password at next sign-in
Users automatically get the IAMUserChangePassword policy to allow them to change their own password.

* Required

Step 23 :-We will create a group later

We can see the previous user listed under the copy "permission from existing user" section (just for observation purpose)

Click on the third section: Attach existing policies directly


aws
Services
Search for services, features, blogs, docs, and more [Alt+S]
Global ▼
Nimit Jjw ▼
Add user
1
2
3
4
5

Set permissions

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

Select an existing user from which to copy policies and group membership.

Copy permissions from existing user

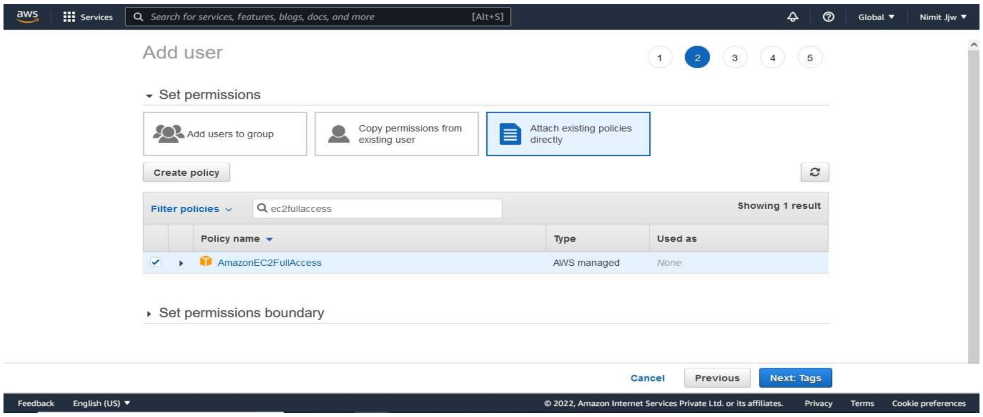
Showing 1 result

	User name	Groups	Attached policies
○	Nimit_Jhunjhunwala	None	IAMUserChangePassword

Set permissions boundary

Cancel
Previous
Next: Tags
Feedback
English (US) ▼
© 2022, Amazon Internet Services Private Ltd. or its affiliates.
Privacy
Terms
Cookie preferences

Step 23 :-Type in `ec2fullaccess` in the search box and click the check box for it; click on Next: Tags


aws
Services
Search for services, features, blogs, docs, and more [Alt+S]
Global
Nimit Jjw
1
2
3
4
5
Cancel
Previous
Next: Tags
Feedback
English (US)
© 2022, Amazon Internet Services Private Ltd. or its affiliates.
Privacy
Terms
Cookie preferences

Add user

Set permissions

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

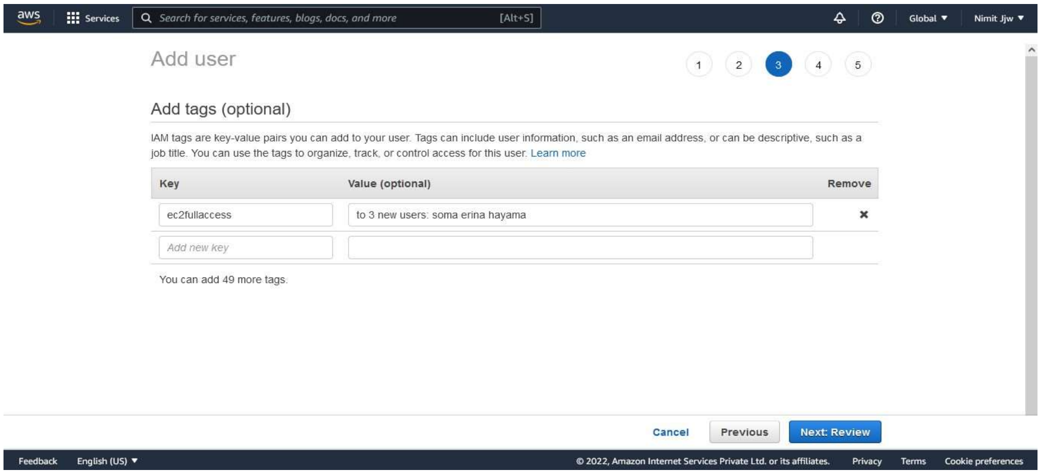
Create policy

Filter policies: ec2fullaccess — Showing 1 result

		Policy name	Type	Used as
✓	▸	AmazonEC2FullAccess	AWS managed	None

Set permissions boundary

Step 24 :-Input the Key and Value for the Tag to keep track of your activities; Click on Next: Review


aws
Services
Search for services, features, blogs, docs, and more [Alt+S]
Global
Nimit Jjw
1
2
3
4
5
Cancel
Previous
Next: Review
Feedback
English (US)
© 2022, Amazon Internet Services Private Ltd. or its affiliates.
Privacy
Terms
Cookie preferences

Add user

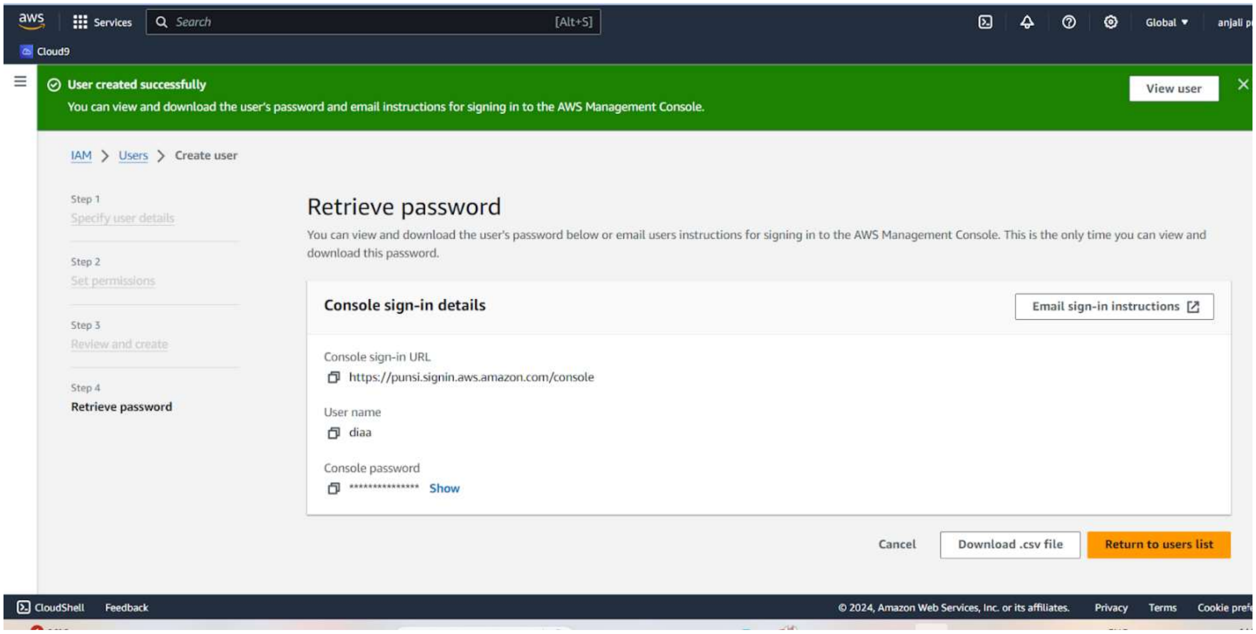
Add tags (optional)

IAM tags are key-value pairs you can add to your user. Tags can include user information, such as an email address, or can be descriptive, such as a job title. You can use the tags to organize, track, or control access for this user. Learn more

Key	Value (optional)	Remove
ec2fullaccess	to 3 new users: soma erina hayama	✖
Add new key		

You can add 49 more tags.

Step 25 :-Click on Create Users Button



User created successfully

You can view and download the user's password and email instructions for signing in to the AWS Management Console.

Retrieve password

You can view and download the user's password below or email users instructions for signing in to the AWS Management Console. This is the only time you can view and download this password.

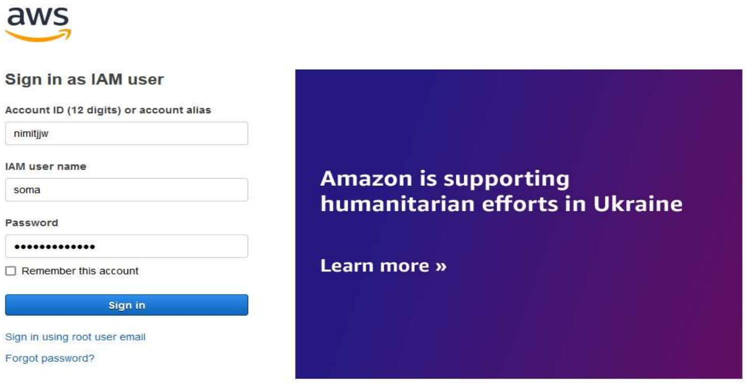
Console sign-in details

Console sign-in URL
https://punsi.signin.aws.amazon.com/console

User name
diaa

Console password
*************** Show

Step 26 :-Try logging in as one of the 3 new users just created



Sign in as IAM user

Account ID (12 digits) or account alias: nimitjjw

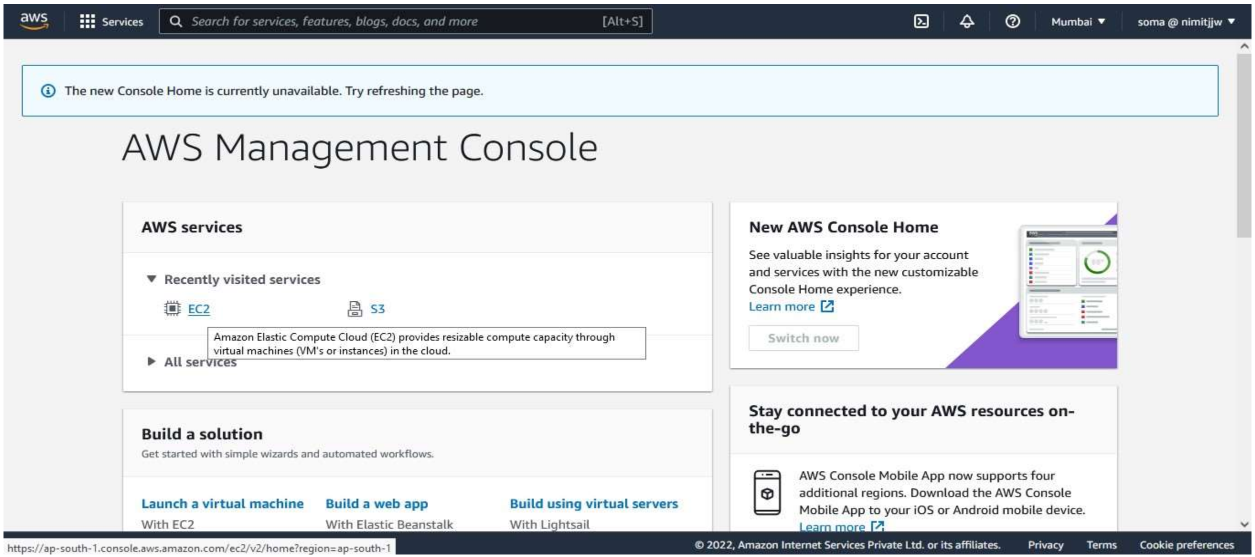
IAM user name: soma

Password: •••••••••••••

□ Remember this account

Sign in
Sign in using root user email
Forgot password?
aws
Amazon is supporting humanitarian efforts in Ukraine
Learn more »

Step 27 :-Try launching an EC2 instance via the new user



The new Console Home is currently unavailable. Try refreshing the page.

AWS Management Console

AWS services

Recently visited services

Amazon Elastic Compute Cloud (EC2) provides resizable compute capacity through virtual machines (VM's or instances) in the cloud.

New AWS Console Home

See valuable insights for your account and services with the new customizable Console Home experience.

Build a solution

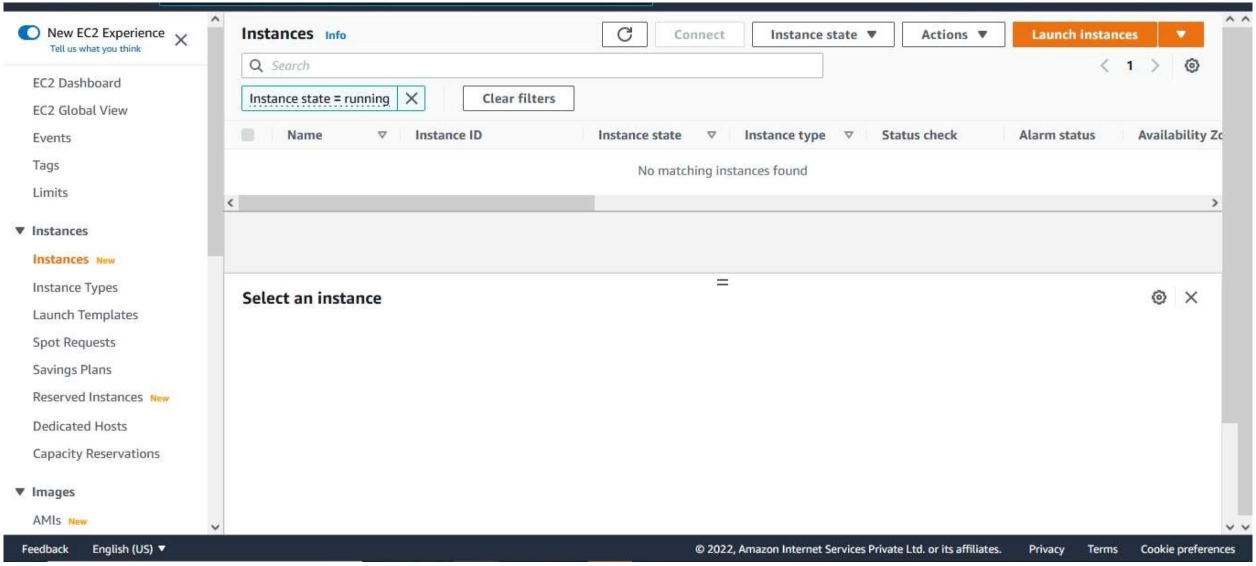
Get started with simple wizards and automated workflows.

Stay connected to your AWS resources on-the-go

AWS Console Mobile App now supports four additional regions. Download the AWS Console Mobile App to your iOS or Android mobile device.

https://ap-south-1.console.aws.amazon.com/ec2/v2/home?region=ap-south-1

© 2022, Amazon Internet Services Private Ltd. or its affiliates.



Instances Info

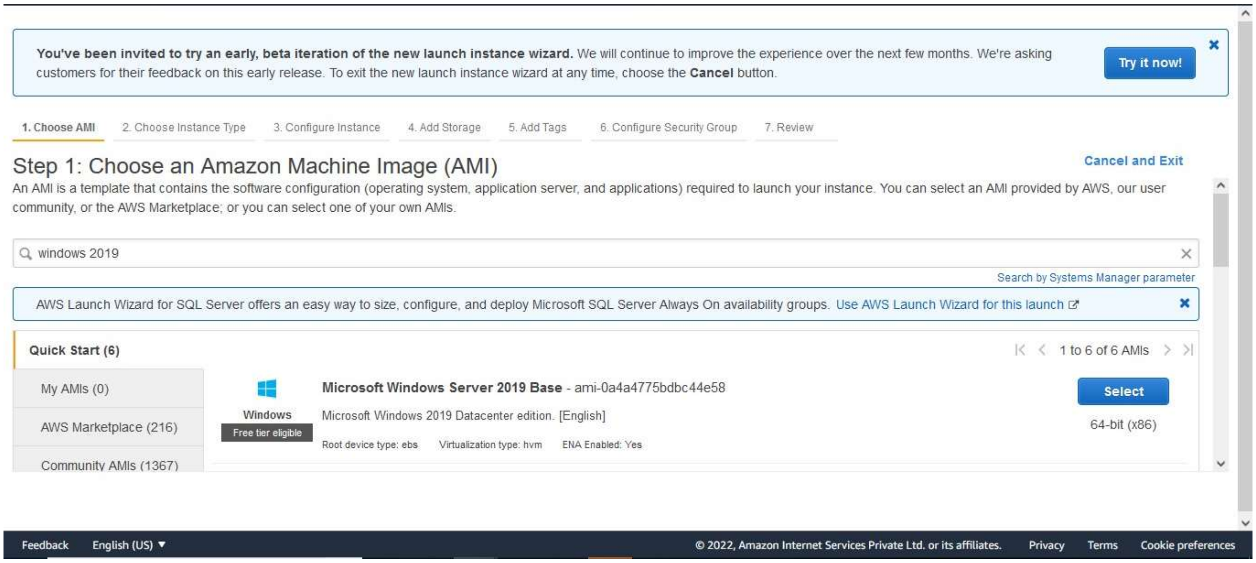
Instance state = running

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zo

No matching instances found

Select an instance

© 2022, Amazon Internet Services Private Ltd. or its affiliates.



You've been invited to try an early, beta iteration of the new launch instance wizard. We will continue to improve the experience over the next few months. We're asking customers for their feedback on this early release. To exit the new launch instance wizard at any time, choose the **Cancel** button.

Step 1: Choose an Amazon Machine Image (AMI)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.

windows 2019

AWS Launch Wizard for SQL Server offers an easy way to size, configure, and deploy Microsoft SQL Server Always On availability groups. Use AWS Launch Wizard for this launch

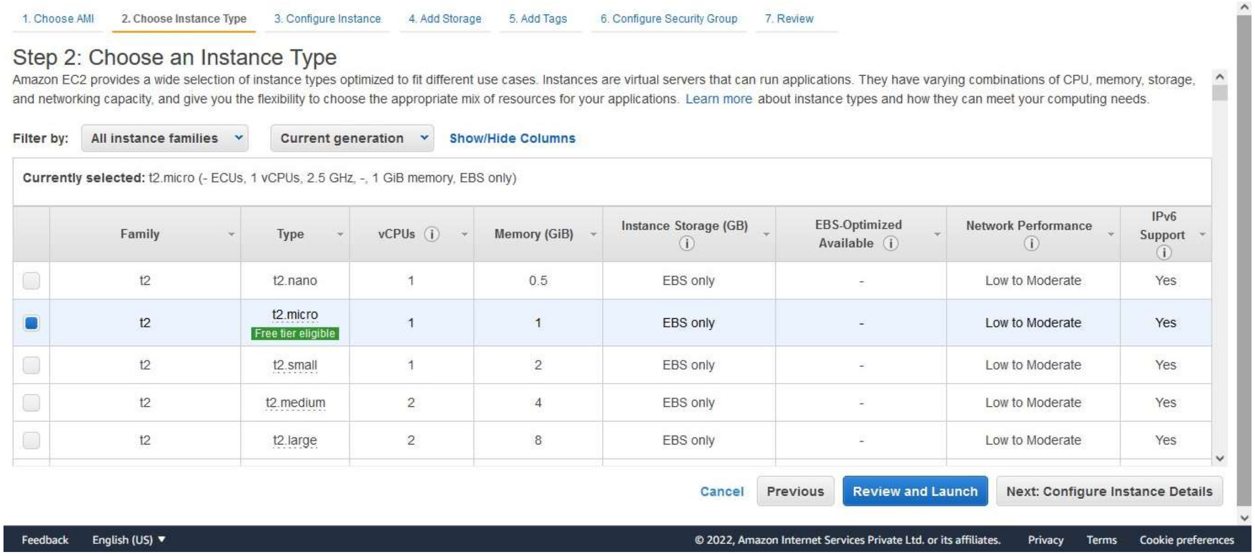
Microsoft Windows Server 2019 Base - ami-0a4a4775bdbc44e58

Microsoft Windows 2019 Datacenter edition. [English]

Root device type: ebs Virtualization type: hvm ENA Enabled: Yes

64-bit (x86)

Feedback
English (US) ▼
© 2022, Amazon Internet Services Private Ltd. or its affiliates.
Privacy
Terms
Cookie preferences



Step 2: Choose an Instance Type

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. Learn more about instance types and how they can meet your computing needs.

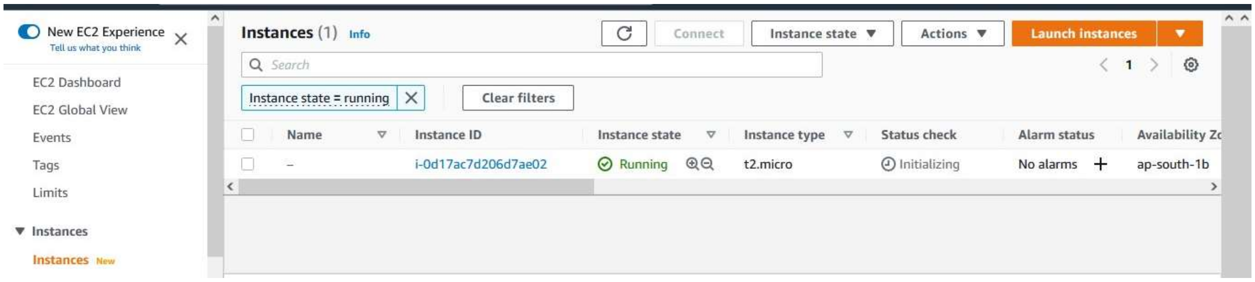
Filter by: All instance families | Current generation | Show/Hide Columns

Currently selected: t2.micro (- ECUs, 1 vCPUs, 2.5 GHz, -, 1 GiB memory, EBS only)

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance	IPv6 Support
☐	t2	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
☑	t2	t2.micro Free tier eligible	1	1	EBS only	-	Low to Moderate	Yes
☐	t2	t2.small	1	2	EBS only	-	Low to Moderate	Yes
☐	t2	t2.medium	2	4	EBS only	-	Low to Moderate	Yes
☐	t2	t2.large	2	8	EBS only	-	Low to Moderate	Yes

Cancel
Previous
Review and Launch
Next: Configure Instance Details
Feedback
English (US) ▼
© 2022, Amazon Internet Services Private Ltd. or its affiliates.
Privacy
Terms
Cookie preferences

Step 28 :-Hence, an instance has been created

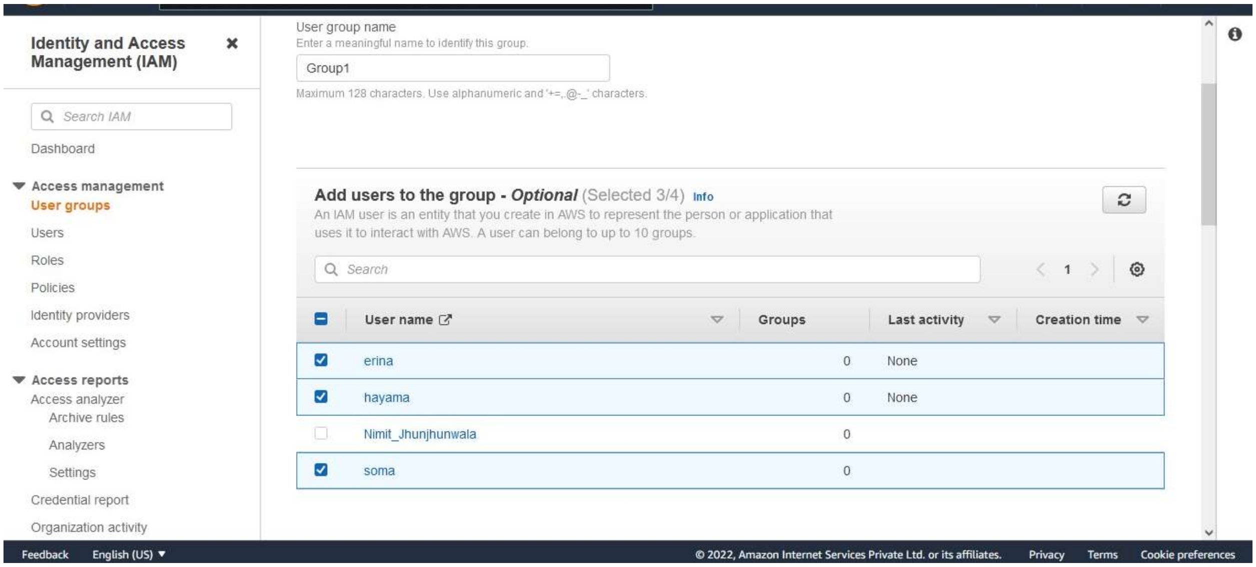


Instance state = running

☐	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zc
☐	–	i-0d17ac7d206d7ae02	Running	t2.micro	Initializing	No alarms +	ap-south-1b

Step 29 :-Delete the bucket when done with your work

Step 30 :-Select the members to be present in the group (max 4 per group)



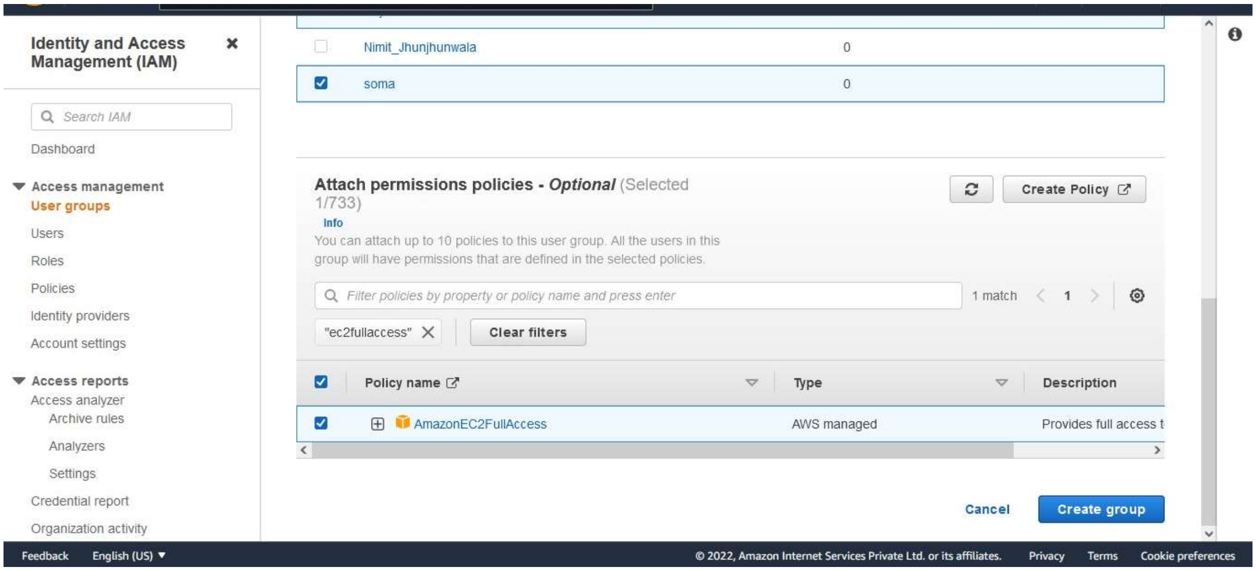
User group name
Enter a meaningful name to identify this group.
Group1
Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.

Add users to the group - *Optional* (Selected 3/4) Info

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS. A user can belong to up to 10 groups.

☐	User name	Groups	Last activity	Creation time
☑	erina	0	None	
☑	hayama	0	None	
☐	Nimit_Jhunjhunwala	0		
☑	soma	0		

Step 31 :-Giving this group `ec2fullaccess` and `s3fullaccess`

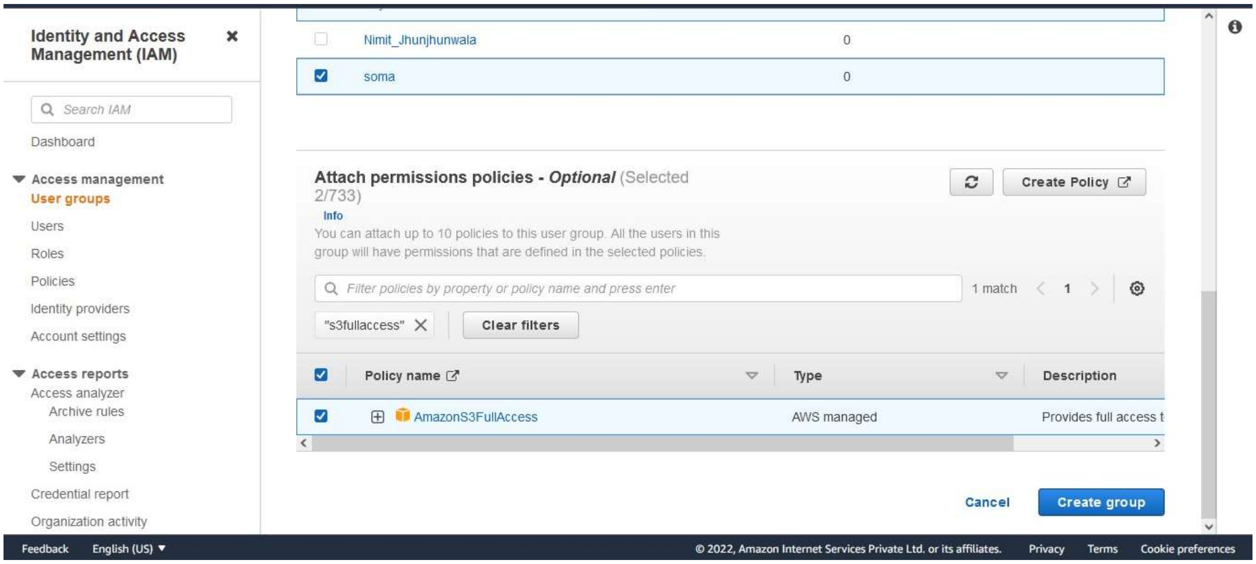


☐	Nimit_Jhunjhunwala	0
☑	soma	0

Attach permissions policies - *Optional* (Selected 1/733)
Info
You can attach up to 10 policies to this user group. All the users in this group will have permissions that are defined in the selected policies.

Filter policies by property or policy name and press enter — 1 match
"ec2fullaccess"

☑	Policy name	Type	Description
☑	AmazonEC2FullAccess	AWS managed	Provides full access t



□	Nimit_Jhunjhunwala	0
☑	soma	0

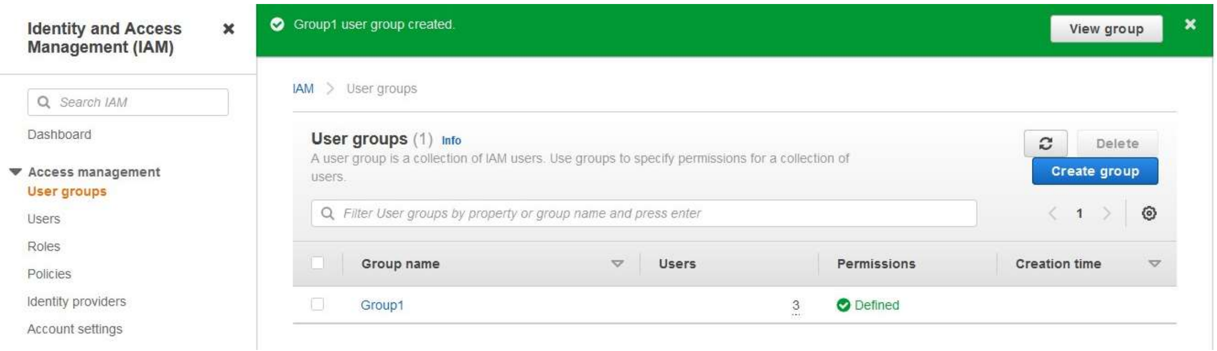
Attach permissions policies - *Optional* (Selected 2/733)
Info

You can attach up to 10 policies to this user group. All the users in this group will have permissions that are defined in the selected policies.

Filter policies by property or policy name and press enter — 1 match — 1

"s3fullaccess"

☑	Policy name	Type	Description
☑	AmazonS3FullAccess	AWS managed	Provides full access t



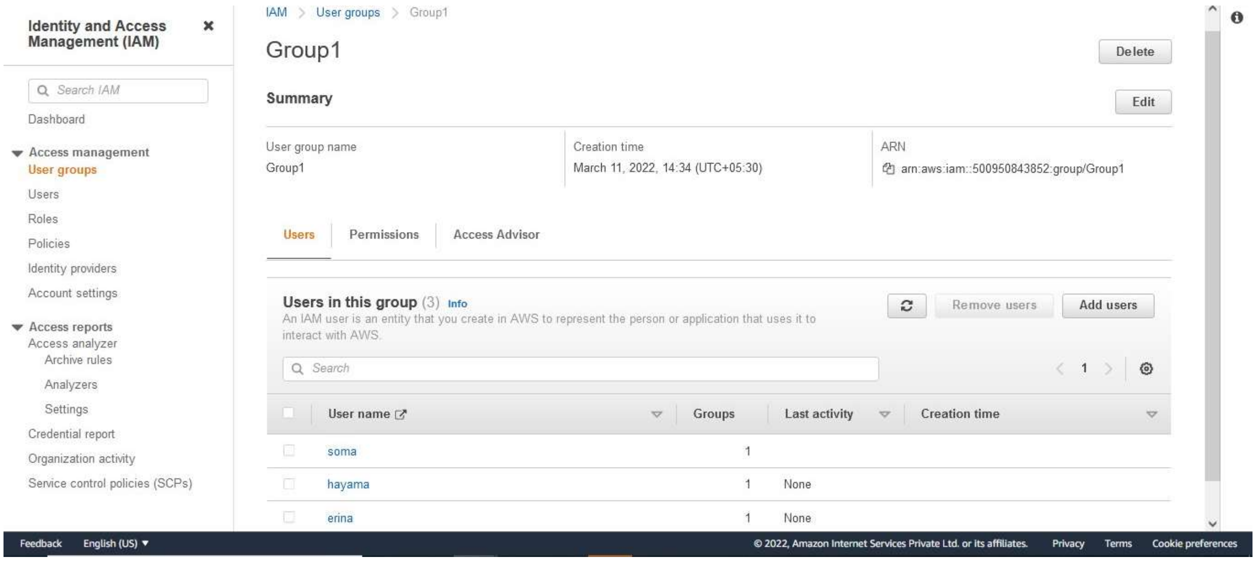
Group1 user group created.

User groups (1) Info

A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

Filter User groups by property or group name and press enter — 1

□	Group name	Users	Permissions	Creation time
□	Group1	3	✓ Defined	



Group1

Summary

User group name: Group1

Creation time: March 11, 2022, 14:34 (UTC+05:30)

ARN: arn:aws:iam::500950843852:group/Group1

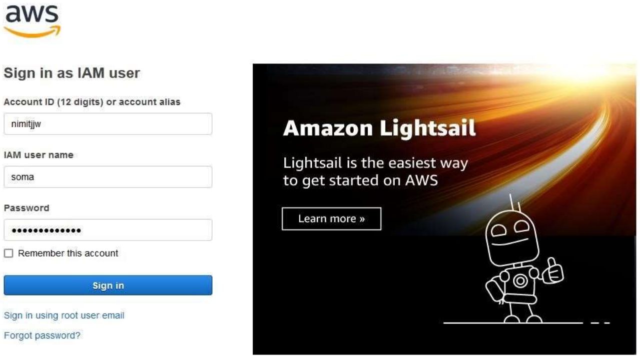
Users in this group (3) Info

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

Search — 1

□	User name	Groups	Last activity	Creation time
□	soma	1		
□	hayama	1	None	
□	erina	1	None	

Step 32 :-Now, login as one of the users from the group and try creating a S3 bucket



Sign in as IAM user

Account ID (12 digits) or account alias: nimitjjw

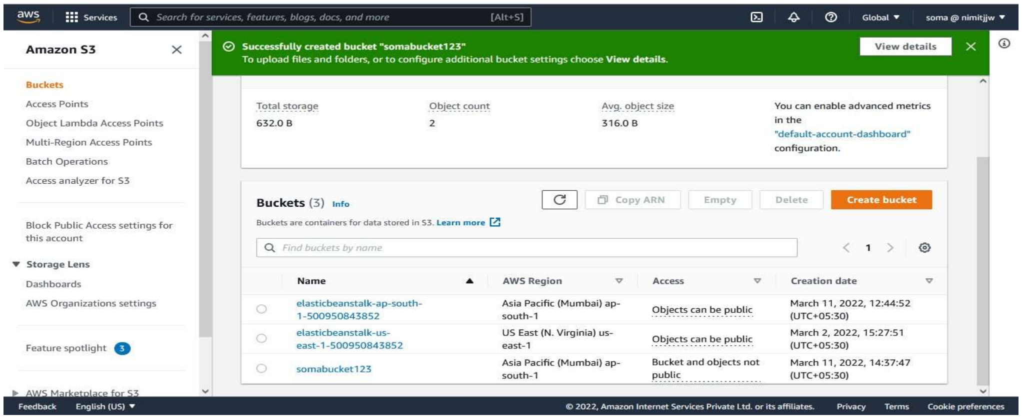
IAM user name: soma

Password: •••••••••••••

□ Remember this account

Sign in
Sign in using root user email
Forgot password?
Amazon Lightsail
Lightsail is the easiest way to get started on AWS
Learn more »

Step 33 :-S3 bucket successfully created



Successfully created bucket "somabucket123"
To upload files and folders, or to configure additional bucket settings choose **View details**.

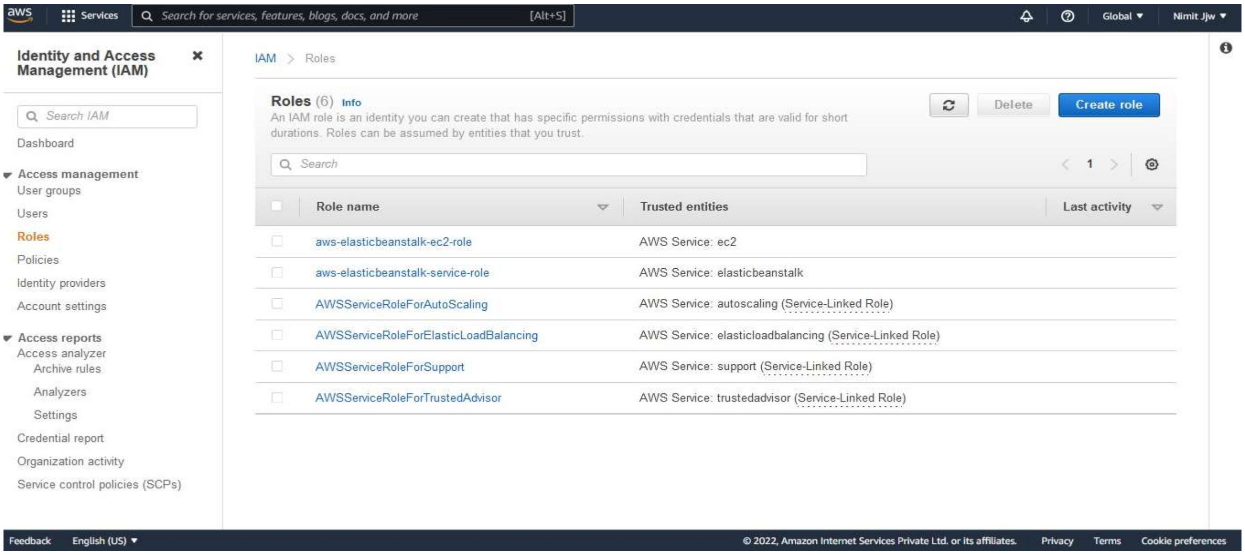
Total storage	Object count	Avg. object size	
632.0 B	2	316.0 B	You can enable advanced metrics in the "default-account-dashboard" configuration.

Buckets (3) Info

Buckets are containers for data stored in S3. Learn more

	Name	AWS Region	Access	Creation date
○	elasticbeanstalk-ap-south-1-500950843852	Asia Pacific (Mumbai) ap-south-1	Objects can be public	March 11, 2022, 12:44:52 (UTC+05:30)
○	elasticbeanstalk-us-east-1-500950843852	US East (N. Virginia) us-east-1	Objects can be public	March 2, 2022, 15:27:51 (UTC+05:30)
○	somabucket123	Asia Pacific (Mumbai) ap-south-1	Bucket and objects not public	March 11, 2022, 14:37:47 (UTC+05:30)

Step 34 :-Delete the bucket when done with your work and Go in the root user window and click on "create role" button in the "Roles" section of IAM Dashboard

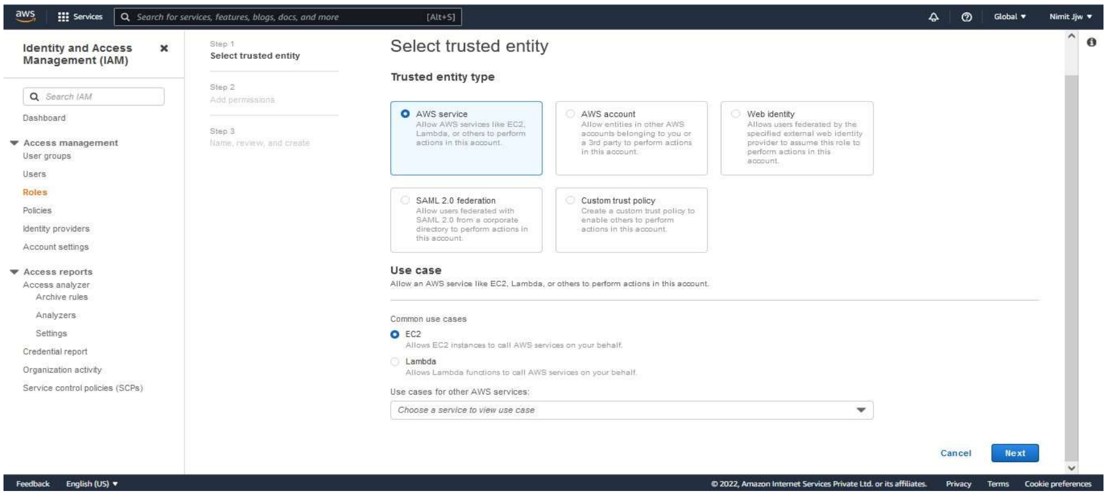


Roles (6) Info

An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

□	Role name	Trusted entities	Last activity
□	aws-elasticbeanstalk-ec2-role	AWS Service: ec2	
□	aws-elasticbeanstalk-service-role	AWS Service: elasticbeanstalk	
□	AWSServiceRoleForAutoScaling	AWS Service: autoscaling (Service-Linked Role)	
□	AWSServiceRoleForElasticLoadBalancing	AWS Service: elasticloadbalancing (Service-Linked Role)	
□	AWSServiceRoleForSupport	AWS Service: support (Service-Linked Role)	
□	AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service-Linked Role)	

Step 34 :-Let it be the default options (you can choose any use case you like) Click
in Next button



Select trusted entity

Trusted entity type

● AWS service
Allow AWS services like EC2, Lambda, or others to perform actions in this account.

○ AWS account
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

○ Web identity
Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.

○ SAML 2.0 federation
Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.

○ Custom trust policy
Create a custom trust policy to enable others to perform actions in this account.

Use case
Allow an AWS service like EC2, Lambda, or others to perform actions in this account.

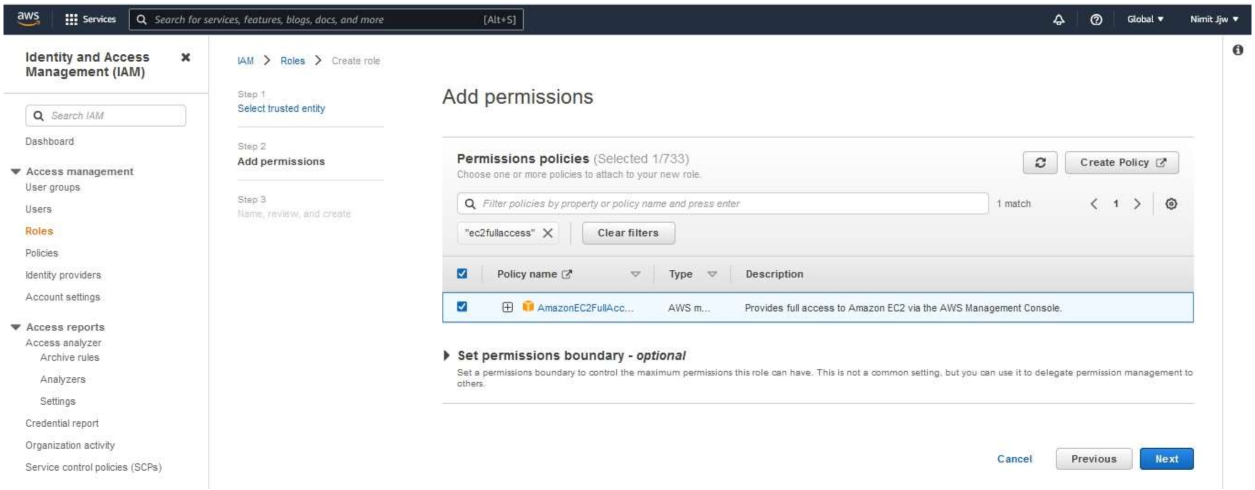
Common use cases

● EC2
Allows EC2 instances to call AWS services on your behalf.

○ Lambda
Allows Lambda functions to call AWS services on your behalf.

Use cases for other AWS services:
Choose a service to view use case

Step 35 :- Give the permission suitable to the use case chosen



Add permissions

Permissions policies (Selected 1/733)
Choose one or more policies to attach to your new role.

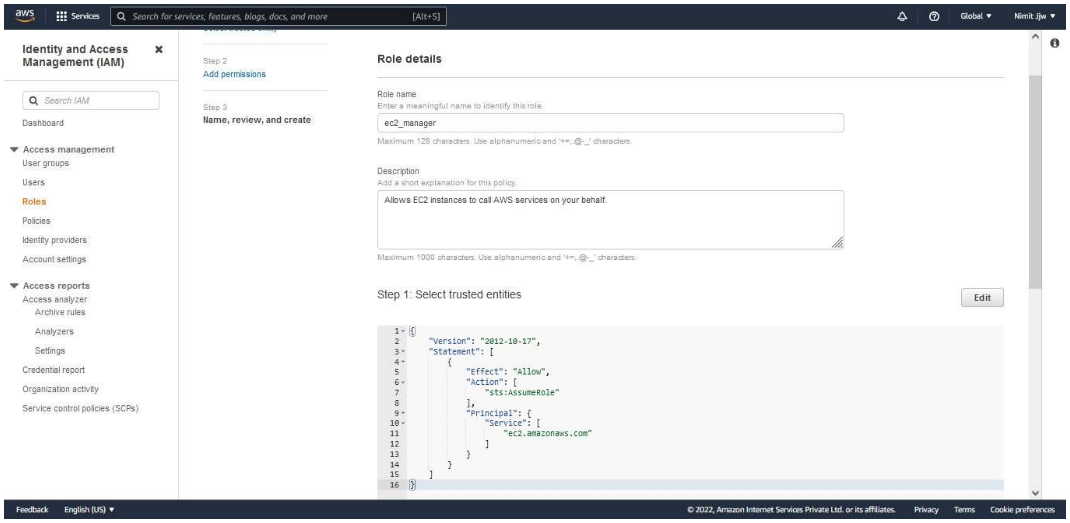
Filter policies by property or policy name and press enter — 1 match — < 1 >

"ec2fullaccess" ✕

☑	Policy name	Type	Description
☑	AmazonEC2FullAcc...	AWS m...	Provides full access to Amazon EC2 via the AWS Management Console.

▸ Set permissions boundary - *optional*
Set a permissions boundary to control the maximum permissions this role can have. This is not a common setting, but you can use it to delegate permission management to others.

Step 36 :-Give suitable Role name and description; rest would remain as default



Role details

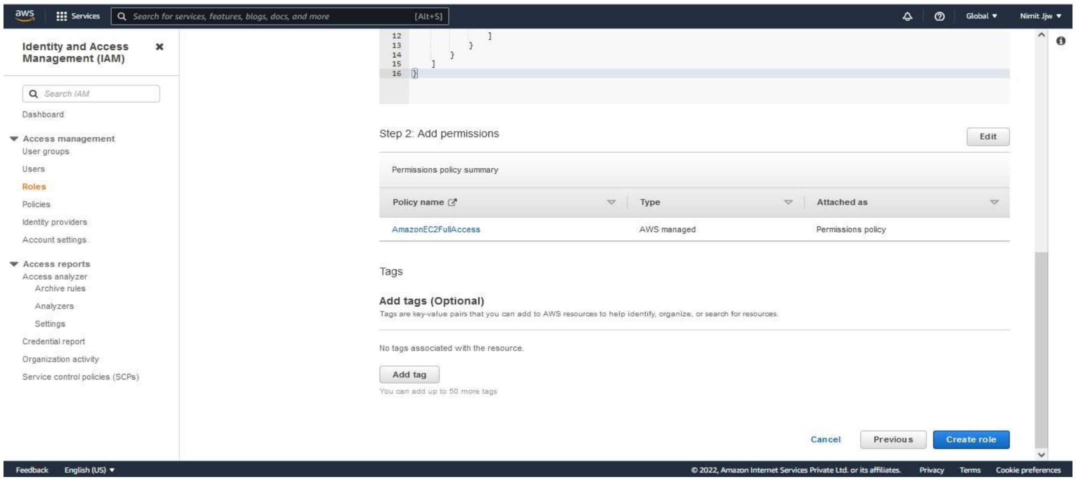
Role name
Enter a meaningful name to identify this role.
ec2_manager
Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.

Description
Add a short explanation for this policy.
Allows EC2 instances to call AWS services on your behalf.
Maximum 1000 characters. Use alphanumeric and '+=,.@-_' characters.

Step 1: Select trusted entities

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sts:AssumeRole"
            ],
            "Principal": {
                "Service": [
                    "ec2.amazonaws.com"
                ]
            }
        }
    ]
}
```

Step 37 :-Add a tag if you want to; click on Create Role button



Step 2: Add permissions

Permissions policy summary

Policy name	Type	Attached as
AmazonEC2FullAccess	AWS managed	Permissions policy

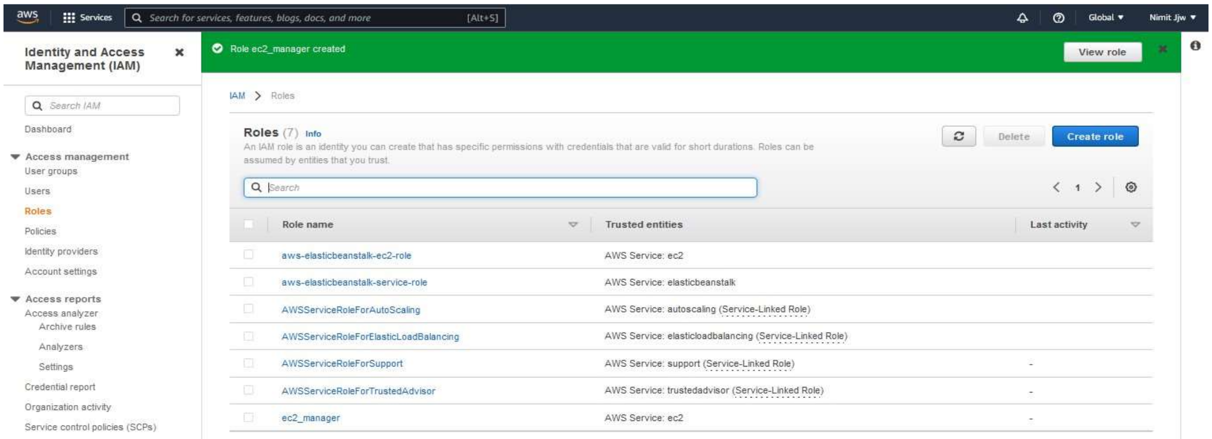
Tags

Add tags (Optional)
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.

You can add up to 50 more tags

Step 38 :-The role has been successfully created

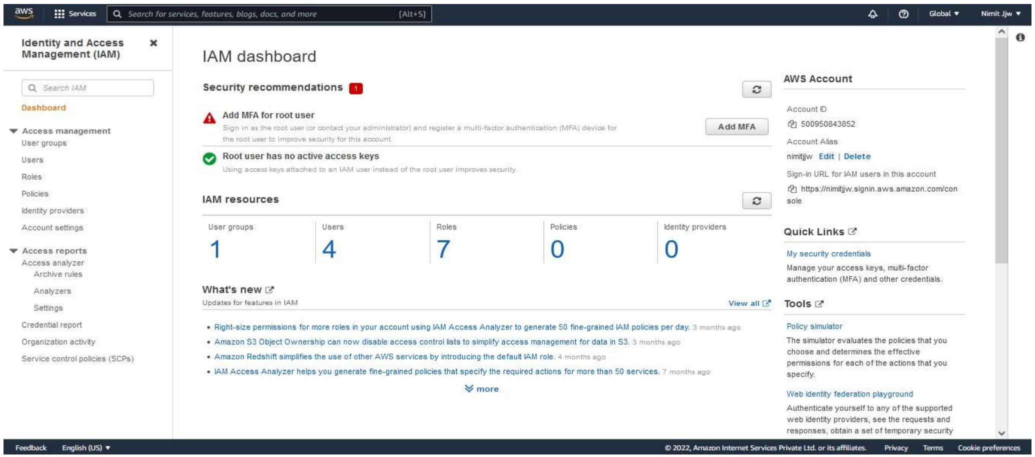


Role ec2_manager created

Roles (7)
An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

Role name	Trusted entities	Last activity
aws-elasticbeanstalk-ec2-role	AWS Service: ec2	
aws-elasticbeanstalk-service-role	AWS Service: elasticbeanstalk	
AWSServiceRoleForAutoScaling	AWS Service: autoscaling (Service-Linked Role)	
AWSServiceRoleForElasticLoadBalancing	AWS Service: elasticloadbalancing (Service-Linked Role)	
AWSServiceRoleForSupport	AWS Service: support (Service-Linked Role)	-
AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service-Linked Role)	-
ec2_manager	AWS Service: ec2	-

Step 39 :-Just to check the overall users, groups and roles, you can check out the IAM Dashboard



IAM dashboard

Security recommendations 1

Add MFA for root user
Sign in as the root user (or contact your administrator) and register a multi-factor authentication (MFA) device for the root user to improve security for this account.

Root user has no active access keys
Using access keys attached to an IAM user instead of the root user improves security.

IAM resources

User groups	Users	Roles	Policies	Identity providers
1	4	7	0	0

What's new
Updates for features in IAM

- Right-size permissions for more roles in your account using IAM Access Analyzer to generate 50 fine-grained IAM policies per day. 3 months ago
- Amazon S3 Object Ownership can now disable access control lists to simplify access management for data in S3. 3 months ago
- Amazon Redshift simplifies the use of other AWS services by introducing the default IAM role. 4 months ago
- IAM Access Analyzer helps you generate fine-grained policies that specify the required actions for more than 50 services. 7 months ago

AWS Account

Account ID
500950843852

Account Alias
nimitjjw Edit | Delete

Sign-in URL for IAM users in this account
https://nimitjjw.signin.aws.amazon.com/console

Quick Links

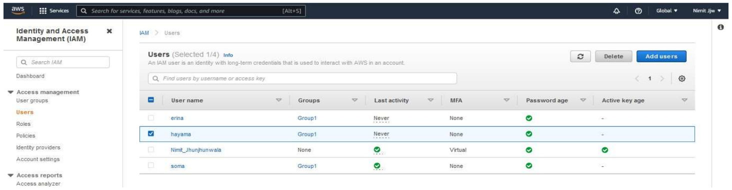
My security credentials
Manage your access keys, multi-factor authentication (MFA) and other credentials.

Tools

Policy simulator
The simulator evaluates the policies that you choose and determines the effective permissions for each of the actions that you specify.

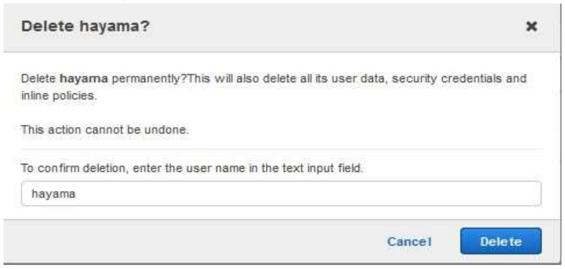
Web identity federation playground
Authenticate yourself to any of the supported web identity providers, see the requests and responses, obtain a set of temporary security

© 2022, Amazon Internet Services Private Ltd. or its affiliates.



Users (Selected 1/4) Info
An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

☐	User name	Groups	Last activity	MFA	Password age	Active key age
☐	erina	Group1	Never	None	✓	-
☑	hayama	Group1	Never	None	✓	-
☐	Nimit_Jhunjhunwala	None	✓	Virtual	✓	✓
☐	soma	Group1	✓	None	✓	-



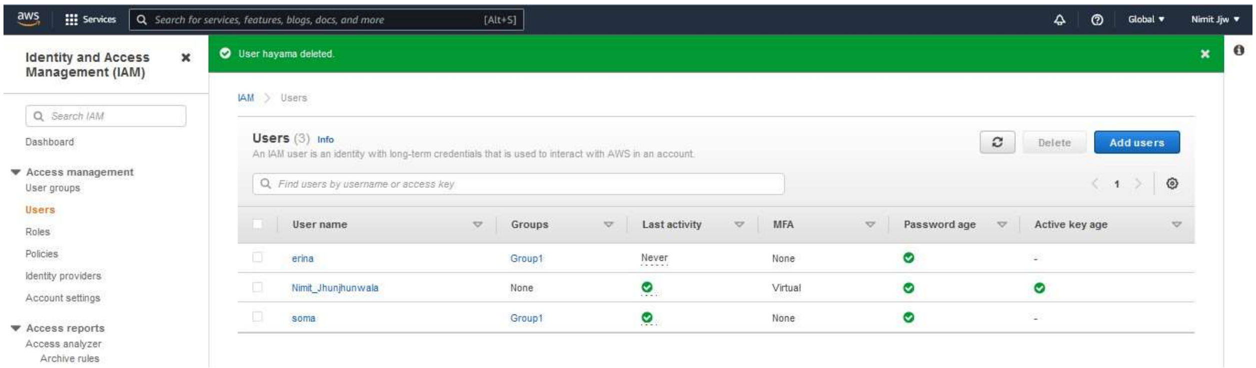
Delete hayama?

Delete **hayama** permanently?This will also delete all its user data, security credentials and inline policies.

This action cannot be undone.

To confirm deletion, enter the user name in the text input field.

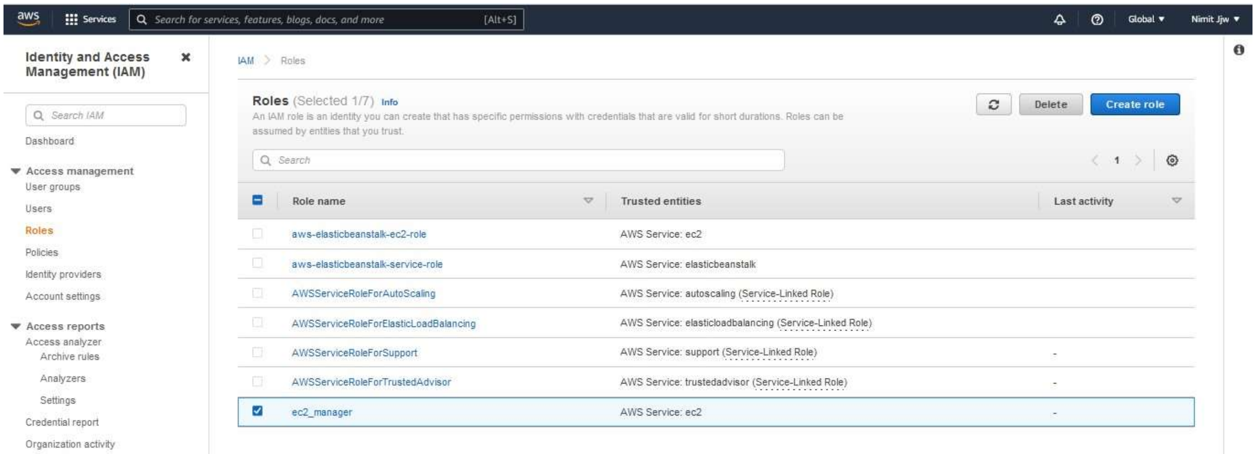
hayama



User hayama deleted.

Users (3) Info
An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

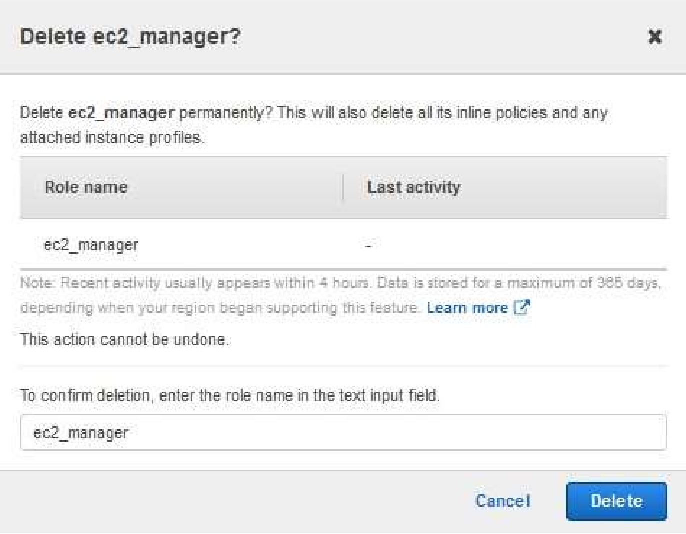
☐	User name	Groups	Last activity	MFA	Password age	Active key age
☐	erina	Group1	Never	None	✓	-
☐	Nimit_Jhunjhunwala	None	✓	Virtual	✓	✓
☐	soma	Group1	✓	None	✓	-



Roles (Selected 1/7) Info

An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

	Role name	Trusted entities	Last activity
□	aws-elasticbeanstalk-ec2-role	AWS Service: ec2	
□	aws-elasticbeanstalk-service-role	AWS Service: elasticbeanstalk	
□	AWSServiceRoleForAutoScaling	AWS Service: autoscaling (Service-Linked Role)	
□	AWSServiceRoleForElasticLoadBalancing	AWS Service: elasticloadbalancing (Service-Linked Role)	
□	AWSServiceRoleForSupport	AWS Service: support (Service-Linked Role)	-
□	AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service-Linked Role)	-
☑	ec2_manager	AWS Service: ec2	-



Delete ec2_manager?

Delete **ec2_manager** permanently? This will also delete all its inline policies and any attached instance profiles.

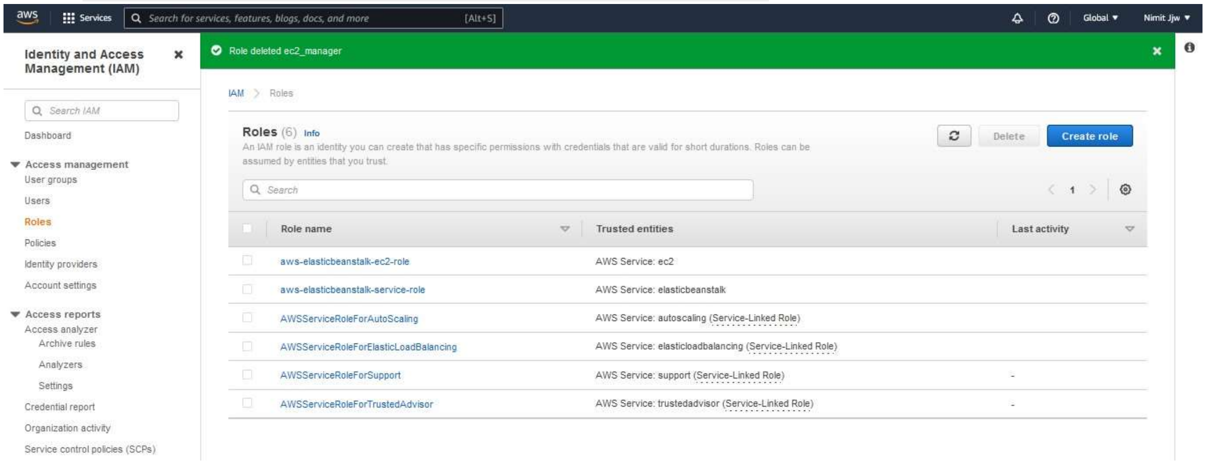
Role name	Last activity
ec2_manager	-

Note: Recent activity usually appears within 4 hours. Data is stored for a maximum of 365 days, depending when your region began supporting this feature. Learn more

This action cannot be undone.

To confirm deletion, enter the role name in the text input field.

ec2_manager

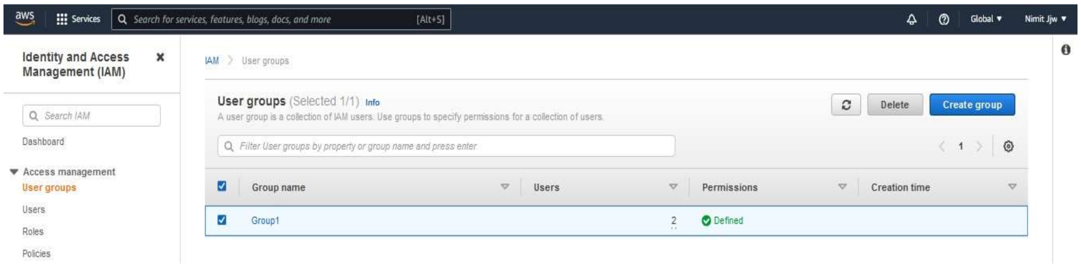


Role deleted ec2_manager

Roles (6) Info

An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

	Role name	Trusted entities	Last activity
□	aws-elasticbeanstalk-ec2-role	AWS Service: ec2	
□	aws-elasticbeanstalk-service-role	AWS Service: elasticbeanstalk	
□	AWSServiceRoleForAutoScaling	AWS Service: autoscaling (Service-Linked Role)	
□	AWSServiceRoleForElasticLoadBalancing	AWS Service: elasticloadbalancing (Service-Linked Role)	
□	AWSServiceRoleForSupport	AWS Service: support (Service-Linked Role)	-
□	AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service-Linked Role)	-

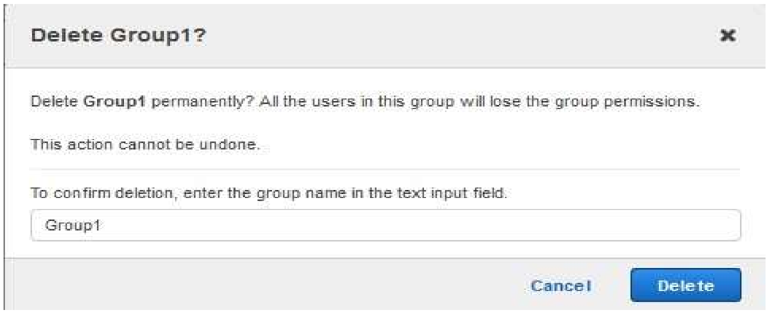


User groups (Selected 1/1) Info

A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

Filter User groups by property or group name and press enter

☑	Group name	Users	Permissions	Creation time
☑	Group1	2	✓ Defined	



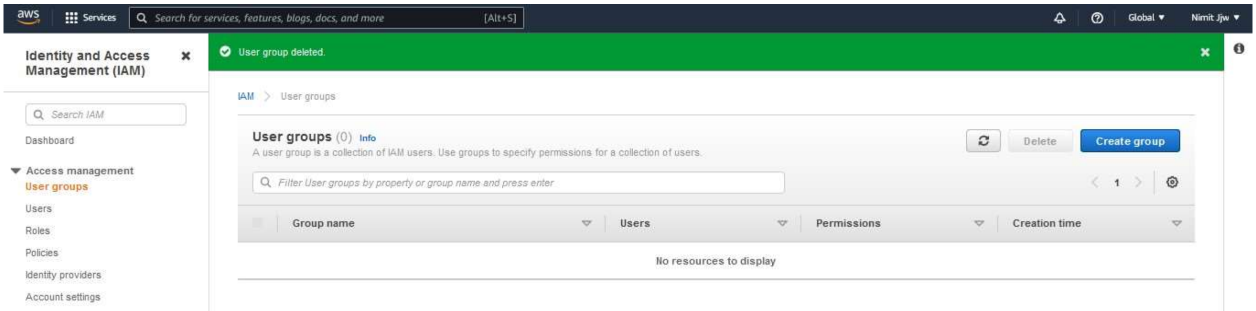
Delete Group1?

Delete Group1 permanently? All the users in this group will lose the group permissions.

This action cannot be undone.

To confirm deletion, enter the group name in the text input field.

Group1



User group deleted.

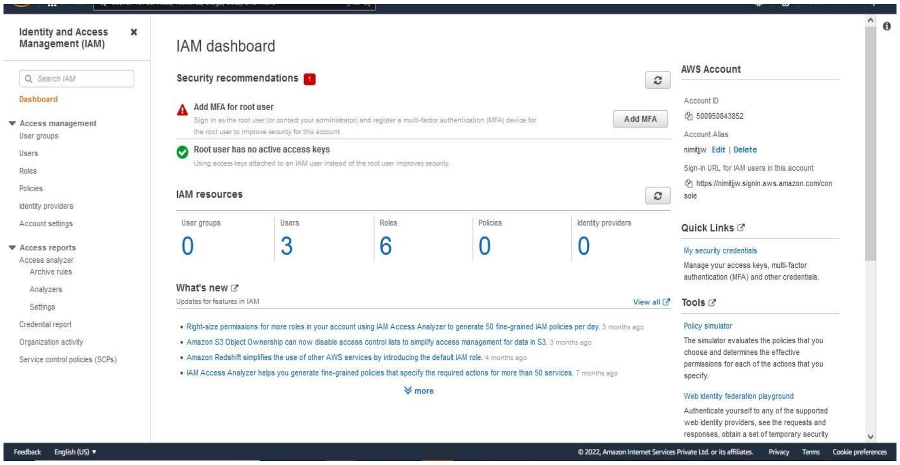
User groups (0) Info

A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

Filter User groups by property or group name and press enter

Group name	Users	Permissions	Creation time
No resources to display			

Step 40 :-Check the IAM dashboard to see the results after deletion activities



IAM dashboard

Security recommendations 1

Add MFA for root user
Sign in as the root user (or contact your administrator) and register a multi-factor authentication (MFA) device for the root user to improve security for this account.

Root user has no active access keys
Using access keys attached to an IAM user instead of the root user improves security.

IAM resources

User groups	Users	Roles	Policies	Identity providers
0	3	6	0	0

What's new
Updates for features in IAM

- Right-size permissions for more roles in your account using IAM Access Analyzer to generate 50 fine-grained IAM policies per day. 3 months ago
- Amazon S3 Object Ownership can now disable access control lists to simplify access management for data in S3. 3 months ago
- Amazon Redshift simplifies the use of other AWS services by introducing the default IAM role. 4 months ago
- IAM Access Analyzer helps you generate fine-grained policies that specify the required actions for more than 50 services. 7 months ago

AWS Account

Account ID
500950843852

Account Alias
nimitjjw Edit | Delete

Sign-in URL for IAM users in this account
https://nimitjjw.signin.aws.amazon.com/console

Quick Links

My security credentials
Manage your access keys, multi-factor authentication (MFA) and other credentials.

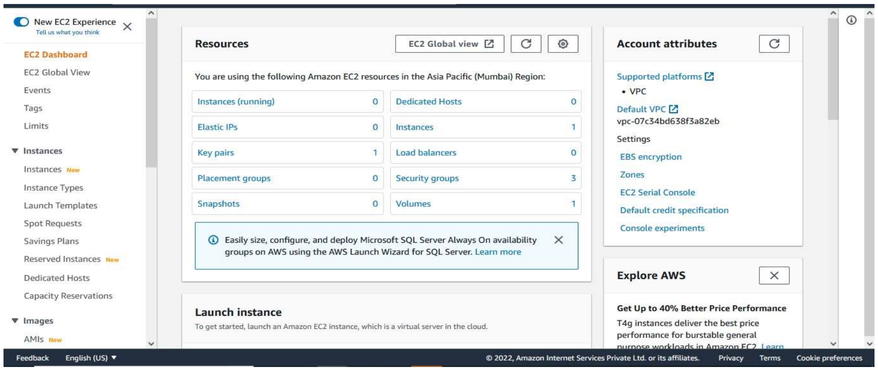
Tools

Policy simulator
The simulator evaluates the policies that you choose and determines the effective permissions for each of the actions that you specify.

Web identity federation playground
Authenticate yourself to any of the supported web identity providers, see the requests and responses, obtain a set of temporary security

© 2022, Amazon Internet Services Private Ltd. or its affiliates.

Step 41 :-Check the ec2 dashboard in case there are any running instances



Resources

You are using the following Amazon EC2 resources in the Asia Pacific (Mumbai) Region:

Instances (running)	0	Dedicated Hosts	0
Elastic IPs	0	Instances	1
Key pairs	1	Load balancers	0
Placement groups	0	Security groups	3
Snapshots	0	Volumes	1

Easily size, configure, and deploy Microsoft SQL Server Always On availability groups on AWS using the AWS Launch Wizard for SQL Server. Learn more

Launch instance

To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

Account attributes

Supported platforms

- VPC

Default VPC
vpc-07c34bd638f3a82eb

Settings

EBS encryption
Zones
EC2 Serial Console
Default credit specification
Console experiments

Explore AWS

Get Up to 40% Better Price Performance

T4g instances deliver the best price performance for burstable general purpose workloads in Amazon EC2. Learn

© 2022, Amazon Internet Services Private Ltd. or its affiliates.

Conclusion :-

In short, Identity and Access Management (IAM) is crucial for securely managing access to cloud resources. It involves creating users, groups, and roles, assigning permissions, and implementing security measures like multi-factor authentication and access policies. IAM helps organizations protect their resources from unauthorized access and maintain compliance with regulations.