

Experiment No. 7

Steps of Implementation:

Login to AWS console

Make sure to check all Ec2 dashboard parameters

The screenshot shows the AWS EC2 Dashboard. On the left, there's a sidebar with options like EC2 Global View, Events, Tags, Limits, Instances, Images, and AMIs. The main area displays EC2 resources: Instances (running) 0, Dedicated Hosts 0, Elastic IPs 0, Instances 1, Key pairs 1, Load balancers 0, Placement groups 0, Security groups 2, Snapshots 0, and Volumes 0. A callout box suggests using the AWS Launch Wizard for Microsoft SQL Server Always On availability groups. To the right, the Account attributes section lists supported platforms (VPC), default VPC (vpc-07c34bd638f3a82eb), settings for EBS encryption, zones, EC2 Serial Console, default credit specification, and console experiments. At the bottom, there's an 'Explore AWS' section with tips to reduce AWS costs.

----- Configuring IAM Dashboard -----

Go to IAM dashboard

The screenshot shows the AWS IAM Dashboard. The left sidebar includes Identity and Access Management (IAM), Access management (User groups, Roles, Policies, Identity providers, Account settings), Access reports (Access analyzer, Analyzers, Settings, Credential report, Organization activity), and a Feedback link. The main area features a 'Security recommendations' section with a red warning icon for 'Add MFA for root user' and a green checkmark for 'Root user has no active access keys'. Below is an 'IAM resources' summary table with counts: User groups 0, Users 0, Roles 6, Policies 0, and Identity providers 0. A 'What's new' section indicates updates for features in IAM. On the right, the 'AWS Account' section shows the account ID (500950843852), account alias (500950843852), and sign-in URL (https://500950843852.signin.aws.amazon.com/console). There are also 'Quick Links' for My security credentials and Tools.

Click on create option under Account Alias and give a valid name; save changes

Create alias for AWS account 500950843852

X

Preferred alias

nimitjw

Must be no more than 63 characters. Valid characters are a-z, 0-9, and - (hyphen).

New sign-in URL

<https://nimitjw.signin.aws.amazon.com/console>

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

The screenshot shows the AWS IAM Dashboard. At the top, there is a green banner with the message "Alias nimitjw created for this account". Below the banner, the "IAM dashboard" section is visible, featuring "Security recommendations" (with one item) and "IAM resources" (showing 0 User groups, 0 Users, 6 Roles, 0 Policies, and 0 Identity providers). On the left, a sidebar lists "Identity and Access Management (IAM)" and various management sections like "Access management", "Access reports", and "Quick Links". On the right, the "AWS Account" sidebar displays the Account ID (500950843852), Account Alias (nimitjw), and the Sign-in URL (https://nimitjw.signin.aws.amazon.com/console). At the bottom, there are links for "Feedback", "English (US)", and copyright information from 2022.

----- Creating a new User -----

Click on “users” in the left column

The screenshot shows the AWS IAM service interface. On the left, a sidebar menu for 'Identity and Access Management (IAM)' is open, with 'Users' selected. The main content area is titled 'Users (0) Info' and displays a message: 'An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.' Below this is a search bar labeled 'Find users by username or access key'. A table header row includes columns for 'User name', 'Groups', 'Last activity', 'MFA', 'Password age', and 'Active'. A message 'No resources to display' is centered below the table. At the top right, there are buttons for 'Delete' and 'Add users'. The bottom of the screen shows standard AWS navigation links like Feedback, English (US), and copyright information.

Click on Add users button

The screenshot shows the 'Add user' wizard at step 1: 'Set user details'. The title is 'Set user details'. It says 'You can add multiple users at once with the same access type and permissions. [Learn more](#)'. A 'User name' input field contains 'Nimit_Jhunjhunwala'. Below it is a link '[Add another user](#)'. Step 1 is highlighted in blue. Step 2 through 5 are shown as numbered circles at the top right.

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

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
 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](#)

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

Click on Next: Tags

Set permissions

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

Get started with groups
 You haven't created any groups yet. Using groups is a best-practice way to manage users' permissions by job functions, AWS service access, or your custom permissions. Get started by creating a group. [Learn more](#)

[Create group](#)

Set permissions boundary

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

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

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

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
NewUser	Nimit_Jhunjhunwala	
Add new key		

You can add 49 more tags.

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

[Feedback](#) [English \(US\) ▾](#) © 2022, Amazon Internet Services Private Ltd. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

Click on Create User Button

Add user

Review

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

User details

User name	Nimit_Jhunjhunwala
AWS access type	Programmatic access and AWS Management Console access
Console password type	Custom
Require password reset	Yes
Permissions boundary	Permissions boundary is not set

Permissions summary

The user shown above will be added to the following groups.

Type	Name
Managed policy	IAMUserChangePassword

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

[Feedback](#) [English \(US\) ▾](#) © 2022, Amazon Internet Services Private Ltd. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

Open the URL in Incognito Mode
(Imc: <https://nimitjjw.signin.aws.amazon.com/console>)

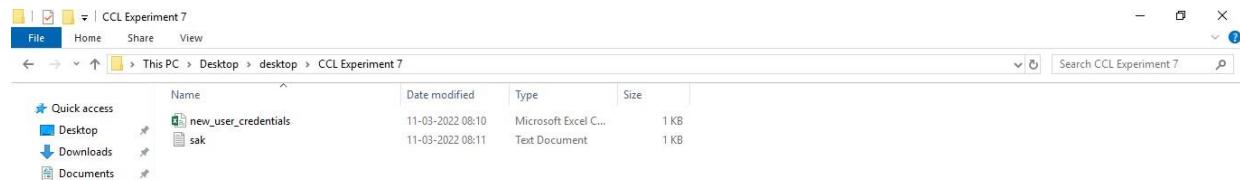
Note: Save the secret access ID & key in a notepad or download the csv

The screenshot shows the AWS Management Console interface. At the top, there's a navigation bar with the AWS logo, a search bar, and account information for "Nimit Jjw". Below the navigation bar, a success message box is displayed, stating: "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." It also provides a link to sign-in: "Users with AWS Management Console access can sign-in at: https://nimitjjw.signin.aws.amazon.com/console".

Below the message box is a table showing the newly created user details:

	User	Access key ID	Secret access key	Email login instructions
▶	Nimit_Jhunjhunwala	AKIAJX7IHGJVS54367	***** Show	Send email

At the bottom of the page, there are links for "Feedback", "English (US)", and copyright information: "© 2022, Amazon Internet Services Private Ltd. or its affiliates.", "Privacy", "Terms", and "Cookie preferences". A "Close" button is located in the bottom right corner of the message box.



----- Logging in as the new User & Checking their permissions -----

Enter the new user's name and psw saved earlier

Amazon Web Services Sign-In

Sign in as IAM user

Account ID (12 digits) or account alias
nimitjw

IAM user name
Nimit_Jhunjhunwala

Password

Remember this account

Sign in

Sign in using root user email
Forgot password?

Amazon is supporting humanitarian efforts in Ukraine
[Learn more »](#)

English

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 *****

Confirm password change

[Sign in using root user email](#)

English

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

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

AWS Services Search for services, features, blogs, docs, and more [Alt+S] Mumbai Nimit_Jhunjhunwala @ nimitjw

New EC2 Experience Tell us what you think

EC2 Dashboard

- EC2 Global View
- Events
- Tags
- Limits

Instances

- Instances **New**
- Instance Types
- Launch Templates
- Spot Requests
- Savings Plans
- Reserved Instances **New**
- Dedicated Hosts
- Capacity Reservations

Images

- AMIs **New**

Feedback English (US) ▾

Resources EC2 Global view

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

Instances (running)	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

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.

© 2022, Amazon Internet Services Private Ltd. or its affiliates. Privacy Terms Cookie preferences

New EC2 Experience Tell us what you think

Instances Info Connect Instance state Actions **Launch instances**

Search Instance state = running Clear filters

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
You are not authorized to perform this operation.						

Feedback English (US) ▾

Amazon S3

Buckets

- Access Points
- Object Lambda Access Points
- Multi-Region Access Points
- Batch Operations
- Access analyzer for S3

Block Public Access settings for this account

Storage Lens

- Dashboards
- AWS Organizations settings

Feature spotlight 3

Amazon S3

Account snapshot Storage lens provides visibility into storage usage and activity trends. [Learn more](#) View Storage Lens dashboard

Buckets (0) Info Copy ARN Empty Delete Create bucket

Find buckets by name

Name	AWS Region	Access	Creation date
You don't have permissions to list buckets After you or your AWS administrator have updated your permissions to allow the s3>ListAllMyBuckets action, refresh this page. Learn more about Identity and access management in Amazon S3			

Feedback English (US) ▾

AWS Marketplace for S3

AWS Billing Dashboard

You Need Permissions
You don't have permission to access billing information for this account. Contact your AWS administrator if you need help. If you are an AWS administrator, you can provide permissions for your users or groups by making sure that (1) [this account allows IAM and federated users to access billing information](#) and (2) [you have the required IAM permissions](#).

Feedback English (US) ▾

----- Adding MFA for the user via Root User -----

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

The screenshot shows the AWS CLI landing page. At the top, there's a navigation bar with links for various AWS services and a 'Sign In to the Console' button. Below the navigation is a sidebar with links for 'AWS Command Line Interface' (which is currently selected), 'Documentation', 'Tools', and 'Release Notes'. There's also a 'Get Started with AWS for Free' button with a 'Create Free Account' link. The main content area is titled 'AWS Command Line Interface' and describes the tool as a unified way to manage AWS services. It highlights the v2 version with new features like improved installers and AWS Single Sign-On. Below this text are four large icons: a '1' for 'Getting Started', a document icon for 'CLI Reference', a GitHub icon for 'GitHub Project', and a cube icon for 'Community Forum'. To the right of the main content are sections for 'Windows' (with a 64-bit Windows installer link), 'MacOS' (with a MacOS PKG installer link), 'Linux' (with a Linux installer link), and 'Amazon Linux' (noting it's pre-installed on Amazon Linux AMI). A 'Release Notes' section links to more information.

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

This PC > Downloads

Name	Date modified	Type	Size
AWSCLIV2	11-03-2022 08:21	Windows Installer ...	29,300 KB
AWS Command Line Interface v2 Setup	-	X	327 KB
			27,578 KB
			29,99,936 KB
			1 KB

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

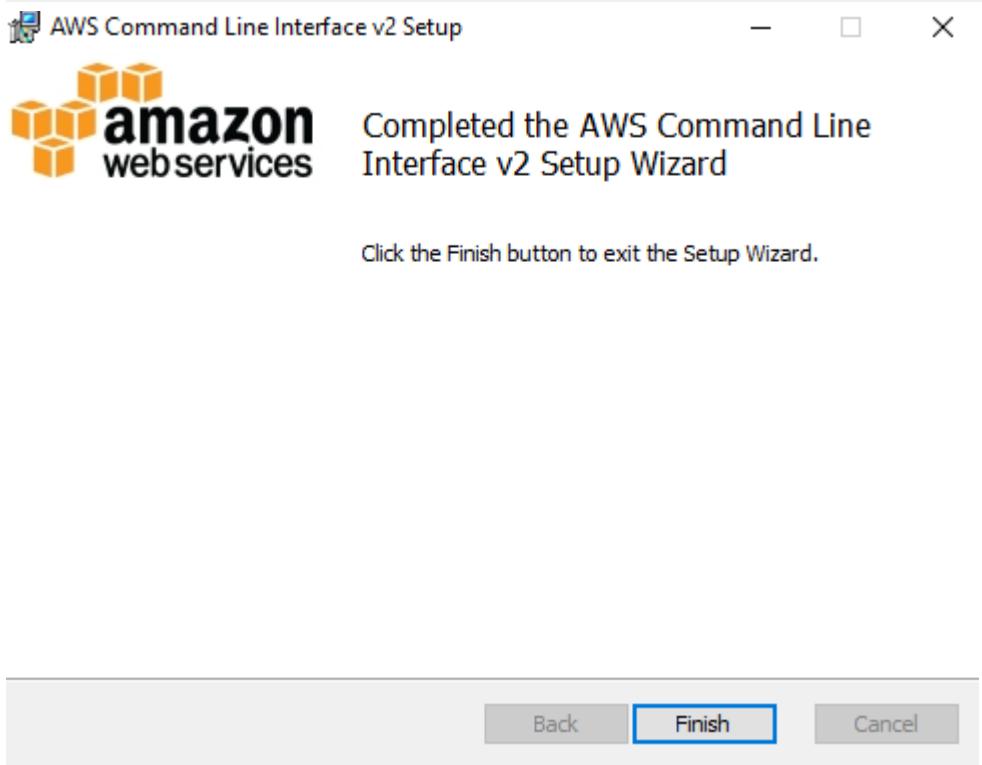
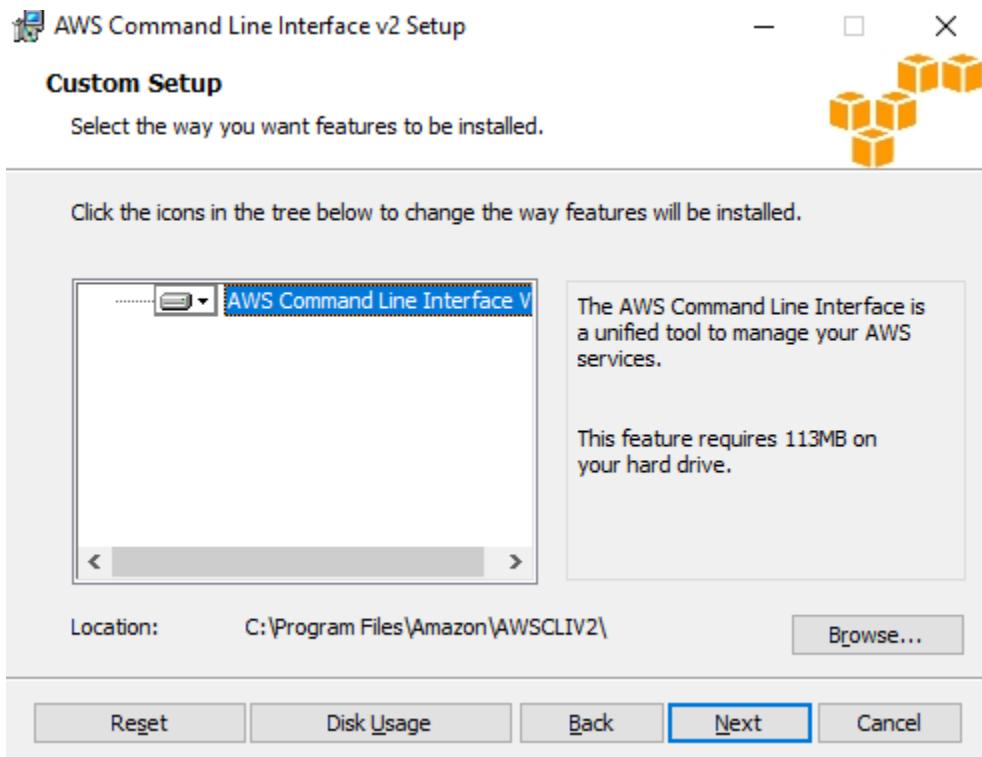
Copyright 2012-2019 Amazon.com, Inc. or its affiliates. All Rights Reserved.

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

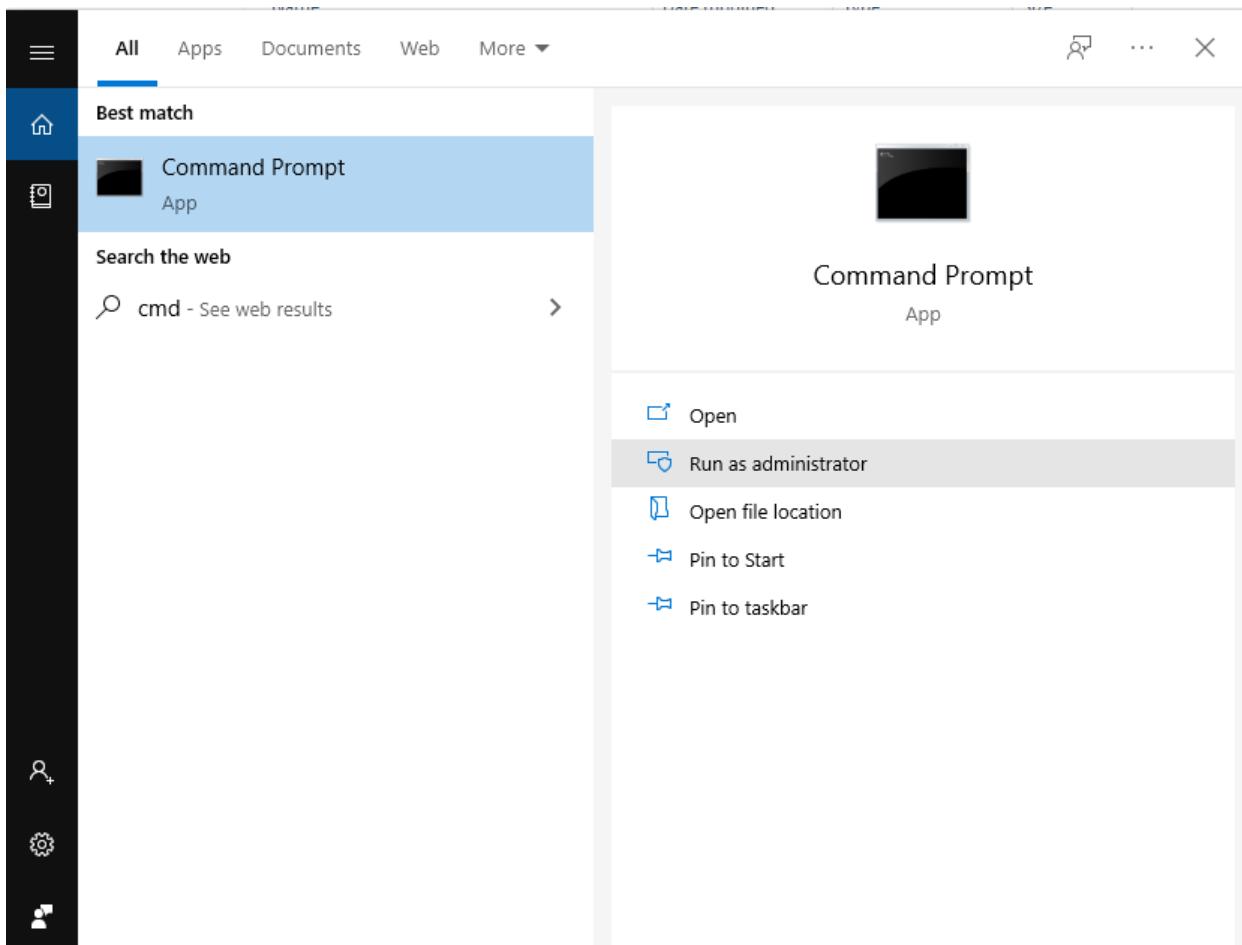
<http://aws.amazon.com/apache2.0/>

I accept the terms in the License Agreement

Print Back Next Cancel



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

A screenshot of a Command Prompt window titled "Administrator: Command Prompt - aws configure". The window shows the following text:

```
C:\Administrator: Command Prompt - aws configure
Microsoft Windows [Version 10.0.17763.437]
(c) 2018 Microsoft Corporation. All rights reserved.

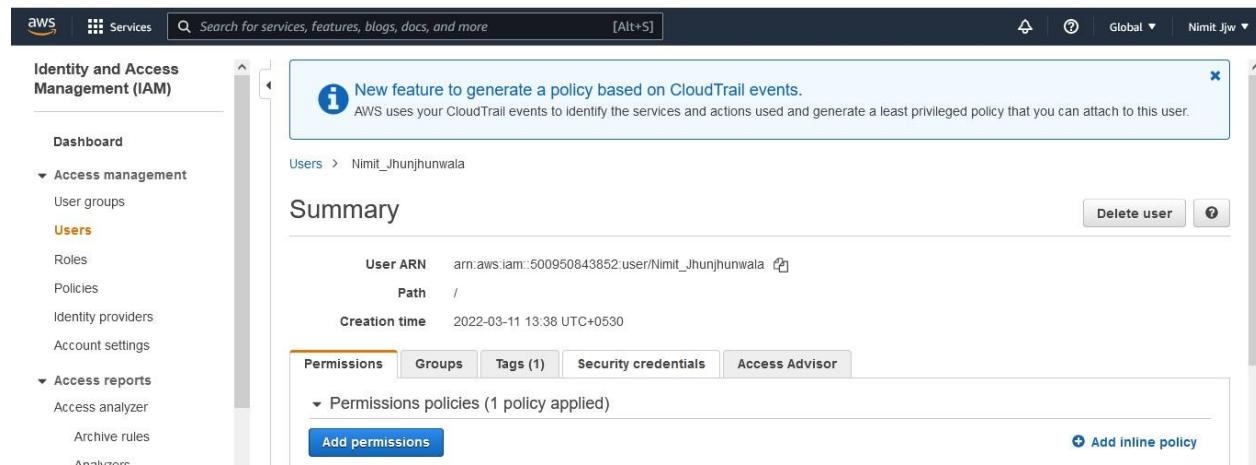
C:\Windows\system32>aws configure
AWS Access Key ID [None]: AKIAJIX7IHGJVS54367
AWS Secret Access Key [None]: ROB/NAJIkXI3HqzcxavveWYkRpE1gHLJwWg2qoc
Default region name [None]: ap-south-1
Default output format [None]: json
```

The next two steps are OPTIONAL:

```
aws --version  
aws s3 ls
```

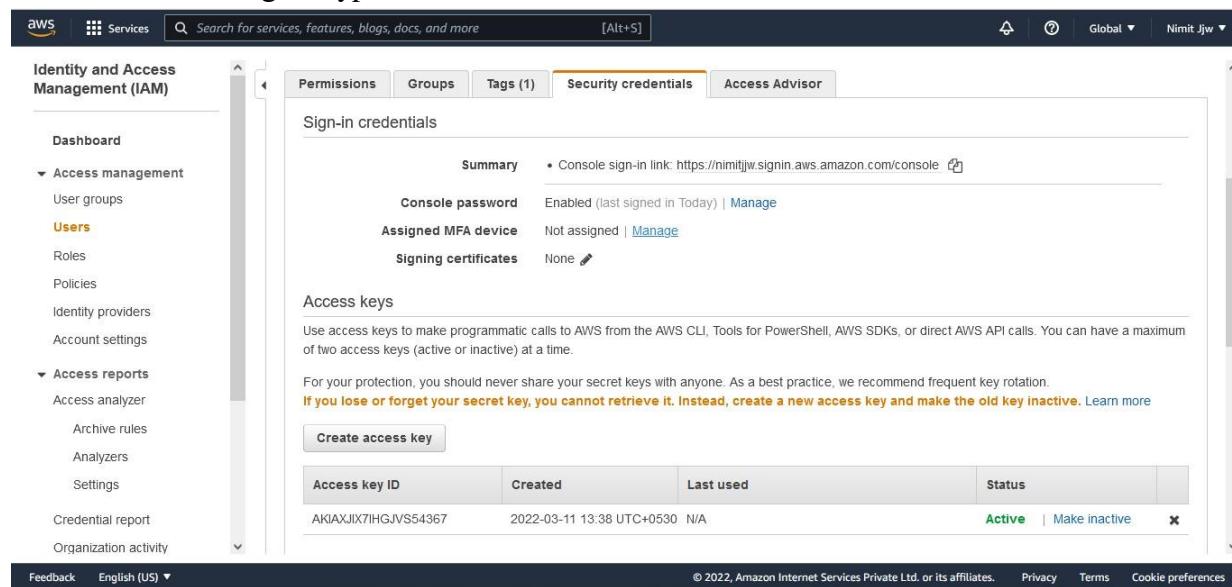
```
C:\Windows\system32>aws --version  
aws-cli/2.4.25 Python/3.8.8 Windows/10 exe/AMD64 prompt/off  
  
C:\Windows\system32>aws s3 ls  
  
An error occurred (RequestTimeTooSkewed) when calling the ListBuckets operation: The difference between the request time and the current time is too large.
```

Go in the security credentials tab under Users of IAM Dashboard



This screenshot shows the AWS IAM User Summary page for a user named 'Nimit_Jhunjhunwala'. The left sidebar navigation bar is visible, with 'Users' selected. The main content area displays the user's ARN, creation date, and a summary of their permissions. At the top of the main content area, there is a message about generating policies based on CloudTrail events. Below this, the 'Security credentials' tab is active, showing sign-in credentials like a console sign-in link and an assigned MFA device, along with access keys.

Click on the “Manage” Hyperlink



This screenshot shows the 'Security credentials' tab for the same user. It displays sign-in credentials and access keys. Under the 'Access keys' section, it says 'Use access keys to make programmatic calls to AWS from the AWS CLI, 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.' A note below states 'For your protection, you should never share your secret keys with anyone. As a best practice, we recommend frequent key rotation. If you lose or forget your secret key, you cannot retrieve it. Instead, create a new access key and make the old key inactive.' A 'Create access key' button is present. Below this, a table lists an existing access key with details like ID, creation date, last used, and status (Active). A 'Manage' link is located in the status column.

Manage MFA device

X

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](#)

[Cancel](#)

[Continue](#)

Use the Google Authenticator app downloaded earlier to scan the QR Code

Set up virtual MFA device

X

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](#)

[Cancel](#)

[Previous](#)

[Assign MFA](#)

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

Cancel

Previous

Assign MFA

Set up virtual MFA device



✓ You have successfully assigned virtual MFA

This virtual MFA will be required during sign-in.

Close

----- Logging in as the new user after MFA -----

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

nimitjw

IAM user name

Nimit_Jhunjhunwala

Password

Remember this account

Sign in

Sign in using root user email

Forgot password?



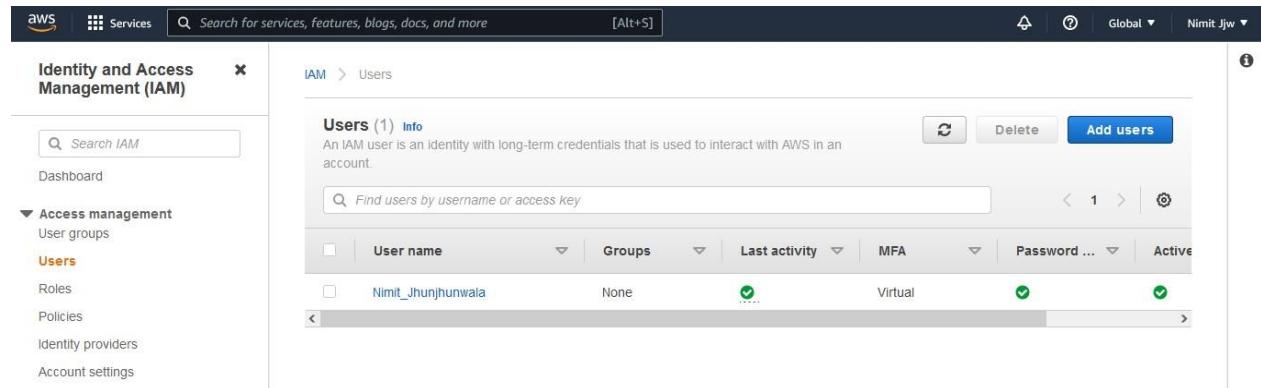
Use the code being shown in the Google Authenticator



The screenshot shows the AWS Multi-factor Authentication (MFA) sign-in page. At the top is the AWS logo. Below it, the title "Multi-factor Authentication" is displayed. A sub-instruction "Enter an MFA code to complete sign-in." is present. A text input field labeled "MFA Code:" contains the value "979827". Below the input field is a blue "Submit" button. At the bottom left is a "Cancel" link.

Now, after opening the root user window again

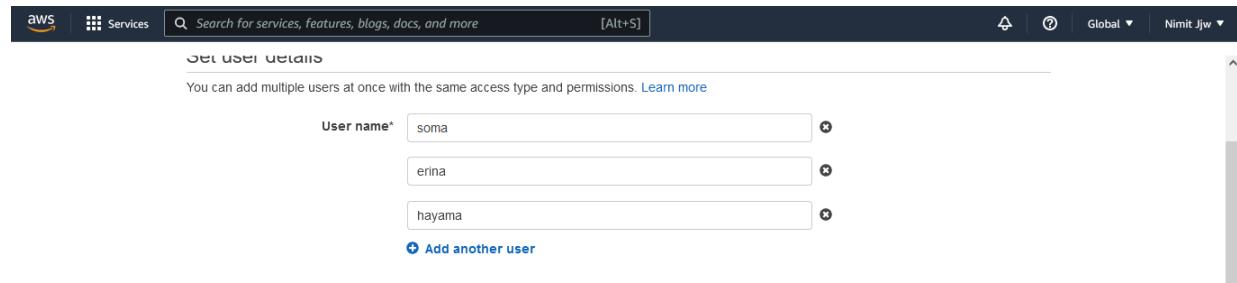
After going in the Users section of IAM Dashboard, we can see that MFA has been activated for the new user



The screenshot shows the AWS IAM Users page. The left sidebar is titled "Identity and Access Management (IAM)" and includes sections for "Dashboard", "Access management" (with "User groups", "Users" selected, "Roles", "Policies", "Identity providers", and "Account settings"), and a search bar. The main content area shows a table titled "Users (1) Info". The table has columns for "User name", "Groups", "Last activity", "MFA", "Password last changed", and "Active". There is one row for "Nimit_Jhunjhunwala" which is marked as "Virtual" and has "MFA Enabled" checked. Buttons for "Delete" and "Add users" are visible at the top right of the table.

----- Adding 3 More Users and giving them permissions -----

Now, Adding 3 More Users



The screenshot shows the "Set user details" page for adding multiple users. The left sidebar is identical to the previous screenshot. The main content area has a heading "Set user details" and a note "You can add multiple users at once with the same access type and permissions. [Learn more](#)". Below this are three input fields for "User name": "soma", "erina", and "hayama". At the bottom is a blue "Add another user" button.

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

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

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

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

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

User name	Groups	Attached policies
Nimit_Jhunjhunwala	None	IAMUserChangePassword

Set permissions boundary

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

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

Add user

Set permissions

Attach existing policies directly

Filter policies ▾ ec2fullaccess Showing 1 result

Policy name	Type	Used as
AmazonEC2FullAccess	AWS managed	None

Set permissions boundary

Cancel Previous Next: Tags

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

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	x
Add new key		

You can add 49 more tags.

Cancel Previous Next: Review

Click on Create Users Button

The screenshot shows the 'Review' step of the 'Add user' wizard. At the top, there's a navigation bar with the AWS logo, a search bar, and a 'Global' dropdown set to 'Nimit Jjw'. Below the navigation is a breadcrumb trail: 'Add user' → 'Review' → '1' (highlighted), '2', '3', '4' (highlighted), '5'. The main content area has a heading 'Review' and a sub-section 'User details' containing five configuration items:

User names	soma, erina, and hayama
AWS access type	AWS Management Console access - with a password
Console password type	Custom
Require password reset	No
Permissions boundary	Permissions boundary is not set

Below this is a 'Permissions summary' section with a note: 'The following policies will be attached to the users shown above.' A table shows one policy:

Type	Name
Managed policy	AmazonEC2FullAccess

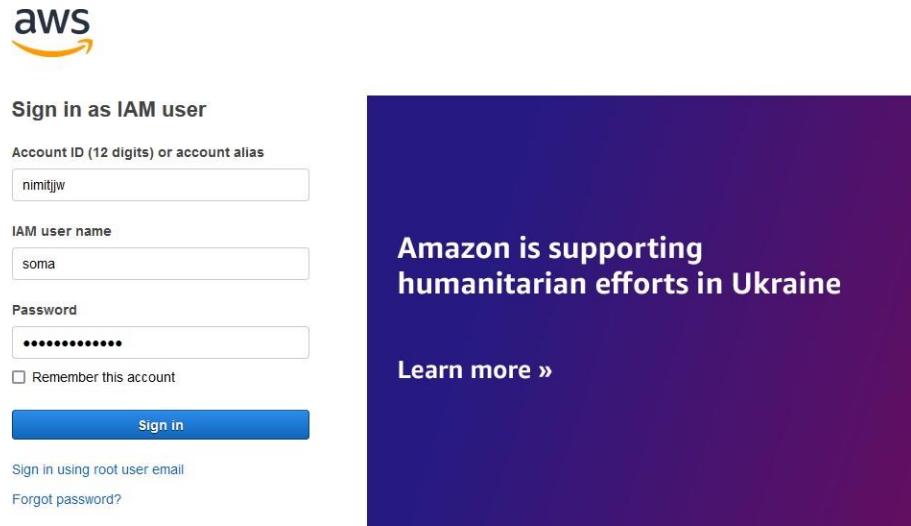
At the bottom are three buttons: 'Cancel', 'Previous', and a blue 'Create users' button.

The screenshot shows the 'Success' step of the 'Add user' wizard. At the top, it displays the same navigation bar and breadcrumb trail as the previous screenshot. The main content area features a green success message box with a checkmark icon and the word 'Success'. It states: '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.' Below this message is a link: 'Users with AWS Management Console access can sign-in at: <https://nimitjjw.signin.aws.amazon.com/console>'.

Below the message is a 'Download .csv' button. The main table lists three users: 'soma', 'erina', and 'hayama', each with a 'Send email' link next to it. At the bottom right is a 'Close' button.

----- Logging in as one of the 3 new Users and checking their permissions -----

Try logging in as one of the 3 new users just created



Try launching an EC2 instance via the new user

The image shows the AWS Management Console homepage. At the top, there's a navigation bar with the AWS logo, a search bar, and a 'Services' dropdown. The main content area has a message: 'The new Console Home is currently unavailable. Try refreshing the page.' Below this, the title 'AWS Management Console' is displayed. On the left, there's a sidebar titled 'AWS services' with a 'Recently visited services' section showing 'EC2' and 'S3'. Under 'Build a solution', there are three options: 'Launch a virtual machine With EC2', 'Build a web app With Elastic Beanstalk', and 'Build using virtual servers With Lightsail'. On the right, there are two promotional boxes: 'New AWS Console Home' and 'Stay connected to your AWS resources on-the-go'. The 'New AWS Console Home' box features a screenshot of the updated console interface. The 'Stay connected' box features a smartphone icon and information about the AWS Console Mobile App. The bottom of the page includes a URL (https://ap-south-1.console.aws.amazon.com/ec2/v2/home?region=ap-south-1), copyright information (© 2022, Amazon Internet Services Private Ltd. or its affiliates.), and links for 'Privacy', 'Terms', and 'Cookie preferences'.

Screenshot of the AWS EC2 Instances page in the New EC2 Experience.

The sidebar shows:

- New EC2 Experience (Tell us what you think)
- EC2 Dashboard
- EC2 Global View
- Events
- Tags
- Limits
- Instances (New)
 - Instance Types
 - Launch Templates
 - Spot Requests
 - Savings Plans
 - Reserved Instances (New)
 - Dedicated Hosts
 - Capacity Reservations
- Images (AMIs (New))

The main content area shows the "Instances" tab selected. A search bar contains "Instance state = running". The table header includes columns for Name, Instance ID, Instance state, Instance type, Status check, Alarm status, and Availability Z.

No matching instances found.

Select an instance

© 2022, Amazon Internet Services Private Ltd. or its affiliates. Privacy Terms Cookie preferences

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.

Try it now!

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review Cancel and Exit

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.

Search for services, blogs, docs, and more [Alt+S]

windows 2019

Search by Systems Manager parameter

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

Quick Start (6)

Category	AMI Name	Description	Type	Status	Action
My AMIs (0)					
AWS Marketplace (216)	Microsoft Windows Server 2019 Base - ami-0a4a4775bdb44e58	Microsoft Windows 2019 Datacenter edition. [English]	Windows	Free tier eligible	Select
Community AMIs (1367)					

© 2022, Amazon Internet Services Private Ltd. or its affiliates. Privacy Terms Cookie preferences

Screenshot of the AWS EC2 Instance Creation Wizard - Step 2: Choose an Instance Type.

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
<input type="checkbox"/>	t2	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
<input checked="" type="checkbox"/>	t2	t2.micro <small>Free tier eligible</small>	1	1	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	t2	t2.small	1	2	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	t2	t2.medium	2	4	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	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

Hence, an instance has been created

Screenshot of the AWS EC2 Instances page.

New EC2 Experience Tell us what you think

Instances (1) Info

Instance state = running

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

Delete the bucket when done with your work

----- Creating a new Group and giving it permissions -----

Select the members to be present in the group (max 4 per group)

The screenshot shows the AWS Identity and Access Management (IAM) Groups page. On the left, a sidebar lists navigation options under 'Access management' and 'Access reports'. The main area is titled 'User group name' with a placeholder 'Enter a meaningful name to identify this group.' A search bar at the top right says 'Search for services, features, blogs, docs, and more [Alt+S]'. Below the search bar, there's a 'Global' dropdown and a user profile 'Nimit Jiw'. The 'User groups' section shows three users: erina, hayama, and soma, each with a checkbox. The checkbox for soma is checked, indicating it is selected for the new group.

Giving this group ec2fullaccess and s3fullaccess

The screenshot shows the 'Attach permissions policies' step for the new group. It displays a table with one row selected: 'AmazonEC2FullAccess' (Type: AWS managed, Description: Provides full access to Amazon EC2). A 'Create Policy' button is visible at the top right of this section. At the bottom right of the main content area, there are 'Cancel' and 'Create group' buttons.

Screenshot of the AWS IAM User Groups page showing the creation of a new user group.

Identity and Access Management (IAM)

User groups

Attach permissions policies - Optional (Selected 2/733)

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

Clear filters

Policy name

AmazonS3FullAccess

AWS managed | Provides full access to S3

Create group

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

Screenshot of the AWS IAM User Groups page showing the creation of a new user group named "Group1".

Identity and Access Management (IAM)

User groups

Group1 user group created.

View group

IAM > User groups

User groups (1)

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

Create group

Filter User groups by property or group name and press enter

Group name

Group1

Defined

Screenshot of the AWS IAM User Groups page showing the details of the newly created "Group1".

Identity and Access Management (IAM)

User groups

Group1

Summary

User group name: Group1 | Creation time: March 11, 2022, 14:34 (UTC+05:30) | ARN: arn:aws:iam::500950843852:group/Group1

Edit | **Delete**

Users | **Permissions** | **Access Advisor**

Users in this group (3)

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

Add users | **Remove users**

Search

User name

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

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

----- Logging in as a member of the Group & checking their permissions -----

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
nimitjw

IAM user name
soma

Password

Remember this account

Sign in

Sign in using root user email
Forgot password?



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	You can enable advanced metrics in the "default-account-dashboard" configuration.
632.0 B	2	316.0 B	

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)

Delete the bucket when done with your work

----- Creating a new Role -----

Go in the root user window and click on “create role” button in the “Roles” section of IAM Dashboard

The screenshot shows the AWS IAM Roles page. On the left, there's a navigation sidebar with options like 'Identity and Access Management (IAM)', 'Dashboard', 'Access management', 'Access reports', and 'Service control policies (SCPs)'. The main area is titled 'Roles (6) Info' and contains a table with columns 'Role name' and 'Trusted entities'. The roles listed are: '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)), and 'AWSServiceRoleForTrustedAdvisor' (AWS Service: trustedadvisor (Service-Linked Role)). There are buttons for 'Create role' and 'Delete' at the top right.

Let it be the default options (you can choose any use case you like)

Click in Next button

The screenshot shows the 'Select trusted entity' step in the IAM Role creation wizard. It has three steps: Step 1 (Select trusted entity), Step 2 (Add permissions), and Step 3 (Name, review, and create). Under 'Trusted entity type', the 'AWS service' option is selected. Other options include 'AWS account', 'SAML 2.0 federation', and 'Custom trust policy'. Under 'Use case', 'EC2' is selected. There are sections for 'Common use cases' (EC2, Lambda) and 'Use cases for other AWS services' (with a dropdown menu labeled 'Choose a service to view use case'). At the bottom right are 'Cancel' and 'Next' buttons.

Give the permission suitable to the use case chosen

The screenshot shows the 'Add permissions' step of creating a new IAM role. In the 'Permissions policies' section, the 'AmazonEC2FullAccess' policy is selected. A note below states: 'Provides full access to Amazon EC2 via the AWS Management Console.' Navigation buttons 'Cancel', 'Previous', and 'Next' are visible at the bottom.

Give suitable Role name and description; rest would remain as default

The screenshot shows the 'Role details' step of creating a new IAM role. The 'Role name' is set to 'ec2_manager'. The 'Description' field contains the text: 'Allows EC2 instances to call AWS services on your behalf.' Below the role details, the 'Step 1: Select trusted entities' section displays the following JSON-based policy document:

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

Navigation buttons 'Edit' and 'Next Step' are visible at the bottom.

Add a tag if you want to; click on Create Role button

The screenshot shows the 'Step 2: Add permissions' page of the IAM role creation wizard. On the left, the navigation menu includes 'Identity and Access Management (IAM)', 'Dashboard', 'Access management' (with 'User groups', 'Users', and 'Roles' expanded), 'Access reports' (with 'Access analyzer', 'Archive rules', 'Analyzers', and 'Settings'), 'Credential report', 'Organization activity', and 'Service control policies (SCPs)'. The main area displays a JSON policy document with lines 12 through 16 visible. Below the policy is a table titled 'Permissions policy summary' showing a single entry: 'AmazonEC2FullAccess' (Type: AWS managed, Attached as: Permissions policy). A 'Tags' section follows, with a note about optional tags and a 'Add tag' button. At the bottom are 'Cancel', 'Previous', and 'Create role' buttons.

The role has been successfully created

The screenshot shows the 'Roles (7)' page in the IAM console. The left sidebar is identical to the previous screenshot. The main content area shows a table of roles with columns for 'Role name' and 'Trusted entities'. The roles listed are: '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)), and 'ec2_manager' (AWS Service: ec2). There are buttons for 'View role' and 'Create role' at the top right of the table area.

Just to check the overall users, groups and roles, you can check out the IAM Dashboard

The screenshot shows the AWS IAM Dashboard. On the left, a sidebar navigation includes 'Identity and Access Management (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', and 'Service control policies (SCPs)'. The main area displays 'IAM dashboard' with 'Security recommendations' (Add MFA for root user, Root user has no active access keys). It also shows 'IAM resources' with counts: User groups (1), Users (4), Roles (7), Policies (0), and Identity providers (0). A 'What's new' section lists recent changes like right-size permissions for roles and Amazon Redshift simplifying access management. On the right, there are sections for 'AWS Account' (Account ID: 500950843852, Account Alias: nimtjiv, Sign-in URL: https://nimtjivsignin.aws.amazon.com/console), 'Quick Links' (My security credentials, Tools), 'Tools' (Policy simulator, Web identity federation playground), and footer links (Feedback, English (US), © 2022, Privacy, Terms, Cookie preferences).

----- Deleting a User -----

The screenshot shows the 'Users' page in the IAM service. The sidebar navigation is identical to the previous dashboard. The main table lists users: erina, hayama (selected), Nimit_Junjunwala, and soma. The 'hayama' row is highlighted with a blue border. A modal dialog box titled 'Delete hayama?' contains the message: 'Delete hayama permanently? This will also delete all its user data, security credentials and inline policies.' Below this, it says 'This action cannot be undone.' and 'To confirm deletion, enter the user name in the text input field.' with a text input box containing 'hayama'. At the bottom of the dialog are 'Cancel' and 'Delete' buttons.

The screenshot shows the AWS Identity and Access Management (IAM) service. In the left sidebar, under 'Access management', the 'Users' section is selected. The main content area displays a table of users with columns for User name, Groups, Last activity, MFA, Password age, and Active key age. The users listed are erina, Nimit_Jhunjhunwala, and soma.

----- Deleting a Role -----

The screenshot shows the AWS IAM service. In the left sidebar, under 'Access management', the 'Roles' section is selected. The main content area displays a table of roles with columns for Role name, Trusted entities, and Last activity. One role, 'ec2_manager', is selected and highlighted.

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

Cancel

Delete

The screenshot shows the AWS IAM Roles page. At the top, a green header bar indicates that the role 'Role deleted ec2_manager' has been deleted. The main content area shows a table of roles with the following data:

Role name	Trusted entities
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)

----- Deleting a Group -----

The screenshot shows the AWS IAM User Groups page. A single user group, 'Group1', is selected. The table displays the following information for 'Group1':

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.

Cancel **Delete**

The screenshot shows the AWS Identity and Access Management (IAM) service. In the left sidebar, under 'Access management', 'User groups' is selected. The main content area displays a green success message: 'User group deleted.' Below it, the 'User groups (0)' section is shown with a table header: 'Group name', 'Users', 'Permissions', and 'Creation time'. A note states: 'A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.' A search bar at the top says 'Filter User groups by property or group name and press enter'. At the bottom, it says 'No resources to display'.

Check the IAM dashboard to see the results after deletion activities

The screenshot shows the AWS IAM dashboard. The left sidebar includes sections for 'Dashboard', 'Access management' (with 'User groups' selected), 'Identity providers', and 'Access reports'. The main content area has a heading 'IAM dashboard' and a 'Security recommendations' section with two items: 'Add MFA for root user' (with a link to 'Edit | Delete') and 'Root user has no active access keys' (with a link to 'Edit | Delete'). Below this is a 'IM resources' summary table:

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

Under 'What's new', there are several recent updates listed. On the right side, there are sections for 'AWS Account' (Account ID: S00950843852, Account Alias: nimtiwv, Sign-in URL: https://nimtiwv.signin.aws.amazon.com/console), 'Quick Links' (My security credentials, Tools), and 'Tools' (Policy simulator, Web identity federation playground). The bottom of the screen shows standard AWS footer links: Feedback, English (US) ▾, © 2022, Amazon Internet Services Private Ltd. or its affiliates., Privacy, Terms, Cookie preferences.

Check the ec2 dashboard in case there are any running instances

The screenshot shows the AWS EC2 Dashboard. The left sidebar includes sections for 'EC2 Global View', 'Events', 'Tags', 'Limits', 'Instances' (with 'Instances New' selected), 'Launch Templates', 'Spot Requests', 'Savings Plans', 'Reserved Instances New', 'Dedicated Hosts', and 'Capacity Reservations'. The main content area has a 'Resources' section with a table:

Instances (running)	Dedicated Hosts
0	0

Below this is a callout box: 'Easily size, configure, and deploy Microsoft SQL Server Always On availability groups on AWS using the AWS Launch Wizard for SQL Server. Learn more'.

On the right side, there are sections for 'Account attributes' (Supported platforms: VPC, Default VPC: vpc-07c34bd638f3a82eb, Settings, EBS encryption, Zones, EC2 Serial Console, Default credit specification, Console experiments) and 'Explore AWS' (Get Up to 40% Better Price Performance, T4g instances deliver the best price performance for burstable general purpose workloads in Amazon EC2). The bottom of the screen shows standard AWS footer links: Feedback, English (US) ▾, © 2022, Amazon Internet Services Private Ltd. or its affiliates., Privacy, Terms, Cookie preferences.