

## Lesson 07 Lesson-End Project

### Creating and Configuring Groups and Users Using Policies

**Project agenda:** To create and configure groups and users with different policies and permissions using AWS IAM

**Description:** The corporation's admin wants to create three groups of IAM users, each with two users and two policies assigned to them. The policies will define the permissions and roles for the users to perform their tasks in their respective groups.

**Tools required:** AWS

**Prerequisites:** None

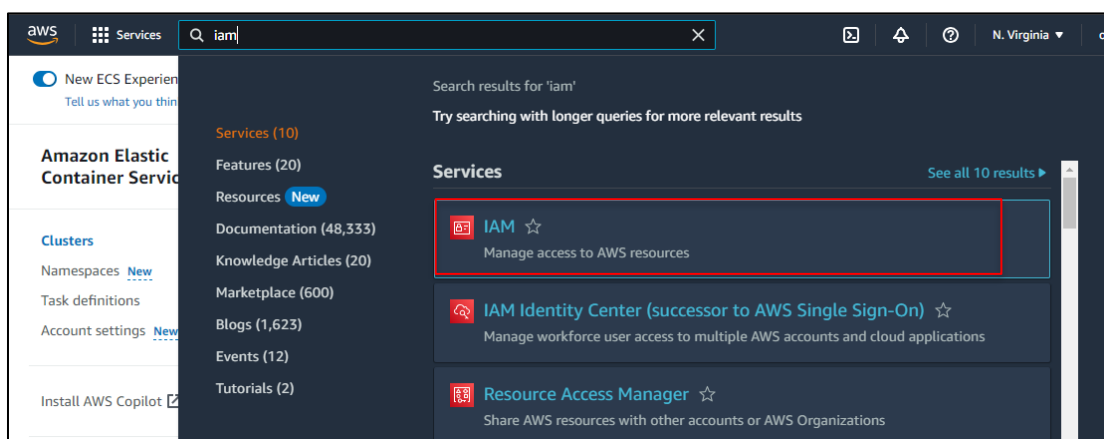
**Expected deliverables:** One of the three groups must be able to operate using CLI commands without accessing the AWS console

Steps to be followed:

1. Create a group
2. Configure the user for CLI operation

#### Step 1: Create a group

1.1 Navigate to the AWS Management Console, search for and select **IAM**



## 1.2 Select **User groups**, and then click on **Create group**

The screenshot shows the AWS IAM console interface. On the left sidebar, under 'Access management', the 'User groups' link is highlighted with a red box. In the main content area, the 'User groups (2)' page is displayed. At the top right of this page, the 'Create group' button is highlighted with a red box. Below the button, there is a table listing existing user groups.

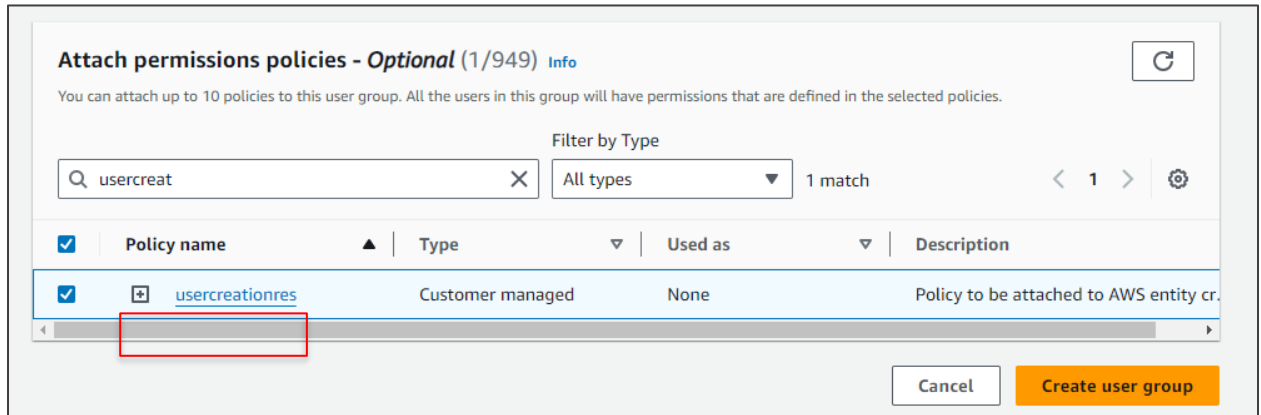
<input type="checkbox"/>	Group name	Users	Permissions	Creation time
<input type="checkbox"/>	<a href="#">Admins</a>	0	Not defined	2 years ago
<input type="checkbox"/>	<a href="#">Attendees</a>	1	Defined	11 minutes ago

## 1.3 Enter the user group name as **Groups1**

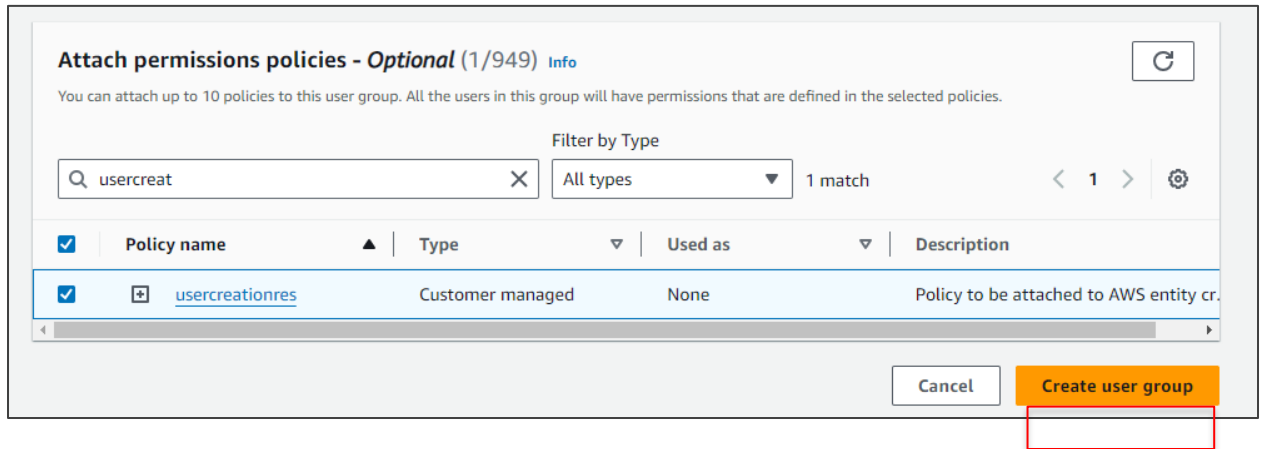
The screenshot shows the 'Create user group' page in the AWS IAM console. The 'Name the group' section contains a text input field for the 'User group name'. The text 'Group1' is entered into this field, and the input field is highlighted with a red box. Below the input field, a note states: 'Maximum 128 characters. Use alphanumeric and '+@\_.' characters.'

The 'Add users to the group - Optional (2)' section is also visible below the naming section.

1.4 Scroll down to **Attach permissions policies** section, search for and select the policy named **usercreationres**:



1.5 Click on the **Create group** button



The group **Groups1** is created successfully.

## 1.6 Follow the same procedure to create **Groups2** and **Groups3**

**User groups (5)** Info

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

Search

<input type="checkbox"/>	Group name	Users	Permissions	Creation time
<input type="checkbox"/>	<a href="#">Admins</a>	0	Not defined	2 years ago
<input type="checkbox"/>	<a href="#">Attendees</a>	1	Defined	25 minutes ago
<input type="checkbox"/>	<a href="#">Group1</a>	0	Defined	3 minutes ago
<input type="checkbox"/>	<a href="#">Group2</a>	0	Defined	Now
<input type="checkbox"/>	<a href="#">Group3</a>	0	Defined	Now

## 1.7 In the IAM dashboard, click on **Users**, and then click on **Create user**

**Identity and Access Management (IAM)**

Search IAM

Dashboard

Access management

- User groups
- Users**
- Roles
- Policies
- Identity providers
- Account settings

**Users (2)** Info

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

Search

<input type="checkbox"/>	User name	Path	Group	Last activity	MFA	Password age
<input type="checkbox"/>	<a href="#">dev-admin</a>	/	Access denied	Access denied	Access denied	Access denied
<input type="checkbox"/>	<a href="#">odl_user_1424101</a>	/	1	24 minutes ago	-	28 minutes

1.8 Enter the user name as **user1\_Groups1**, and select the **Provide user access to the AWS Management Console** checkbox. Then click **Next**.

The screenshot shows the AWS IAM console 'Specify user details' page. The breadcrumb navigation is IAM > Users > Create user. The left sidebar shows the steps: Step 1: Specify user details (active), Step 2: Set permissions, Step 3: Review and create, and Step 4: Retrieve password. The main content area is titled 'Specify user details' and contains a 'User details' section. In this section, the 'User name' field is populated with 'user1\_Groups1'. Below this field, a note states: 'The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , @ \_ - (hyphen)'. A checkbox labeled 'Provide user access to the AWS Management Console - optional' is checked. Below this checkbox, a note states: 'If you're providing console access to a person, it's a [best practice](#) to manage their access in IAM Identity Center.' There is also a blue information box with the title 'Do you want to provide console access to a person?' and the text: '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. To do so, you must be signed in to the Identity Center console using the credentials of the management account in AWS Organizations. If you aren't the management account owner, contact the owner to perform this task.' Below the 'User details' section, there is a 'Show password' checkbox which is unchecked. A checked checkbox states: 'Users must create a new password at next sign-in - Recommended'. Below this, a note states: 'Users automatically get the [IAMUserChangePassword](#) policy to allow them to change their own password.' There is also a blue information box with the title 'If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after you create this IAM user. [Learn more](#)'. At the bottom right of the page, there are 'Cancel' and 'Next' buttons. The 'Next' button is highlighted in orange.

## 1.9 In the **Add user to group** section, select **Groups1** and click **Next**

**Permissions options**

- ☒ **Add user to group**  
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.
- ☐ **Copy permissions**  
Copy all group memberships, attached managed policies, and inline policies from an existing user.
- ☐ **Attach policies directly**  
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

**User groups (1/8)**

Search

<input type="checkbox"/>	Group name	Users	Attached policies	Created
<input type="checkbox"/>	Admin	0	-	2023-07-17 (1 month ago)
<input type="checkbox"/>	Admins	0	-	2022-01-19 (1 year ago)
<input type="checkbox"/>	Attendees	1	AWS11554-1057974-Pg...	2023-09-05 (10 hours ago)
<input type="checkbox"/>	group1	0	-	2023-09-05 (39 minutes ago)
<input type="checkbox"/>	group1.	1	-	2023-09-05 (38 minutes ago)
<input checked="" type="checkbox"/>	<b>Groups1</b>	0	UserCreationRestriction	2023-09-05 (30 minutes ago)

**Info:** If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after you create this IAM user. [Learn more](#)

Cancel **Next**

## 1.10 Click on the **Create user** button

**User details**

User name user1_Groups1	Console password type Autogenerated	Require password reset Yes
----------------------------	--	-------------------------------

**Permissions summary**

Name	Type	Used as
Groups1	Group	Permissions group
IAMUserChangePassword	AWS managed	Permissions policy

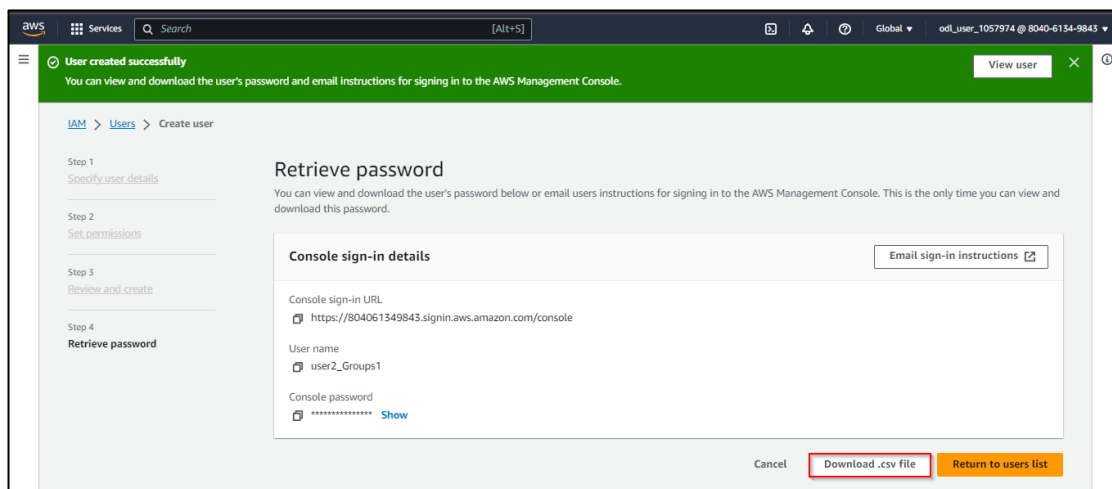
**Tags - optional**  
Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.

No tags associated with the resource.

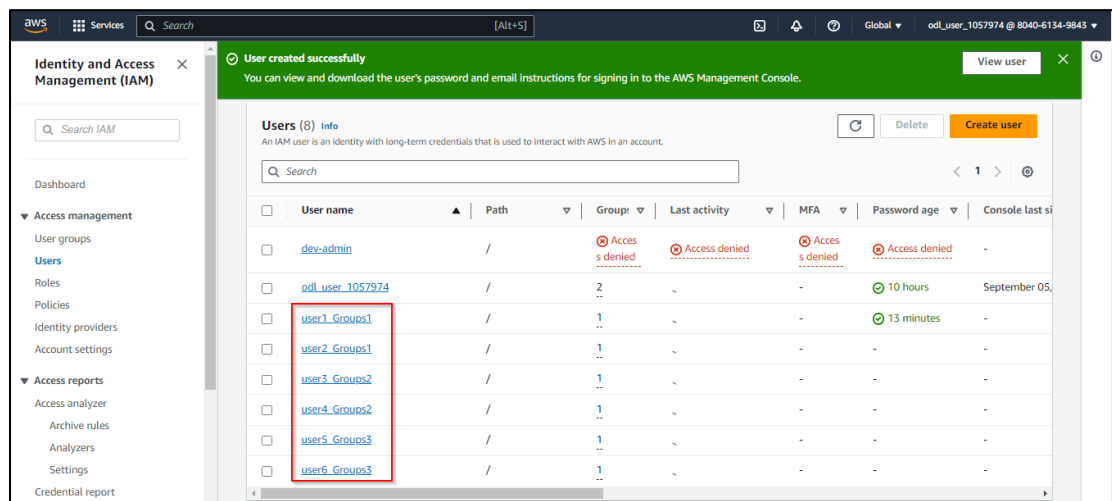
[Add new tag](#)  
You can add up to 50 more tags.

Cancel Previous **Create user**

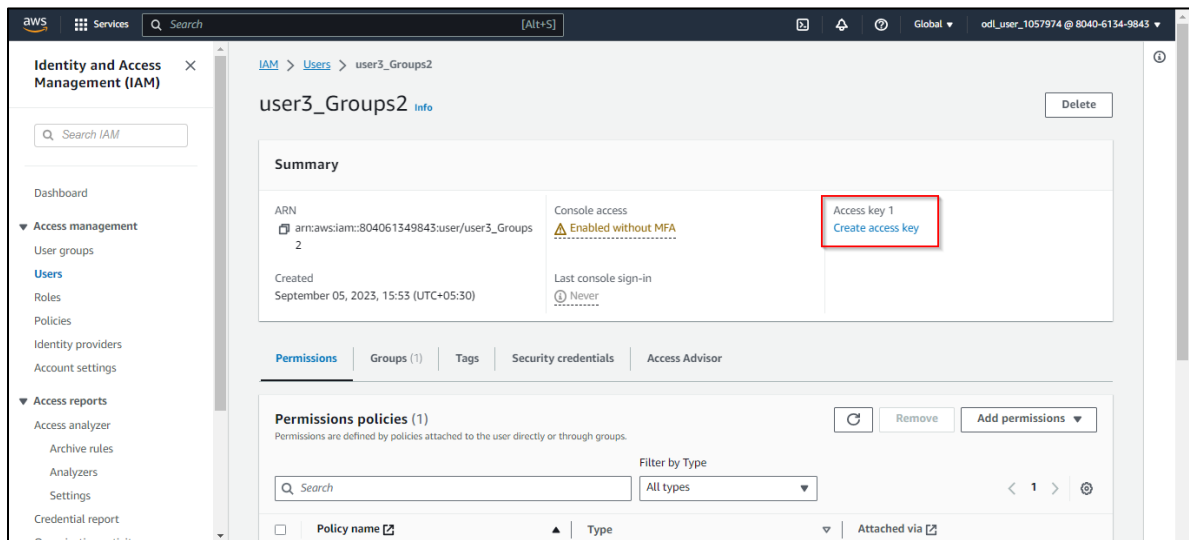
### 1.11 Select **Download the .csv file**, and then click on **Close**



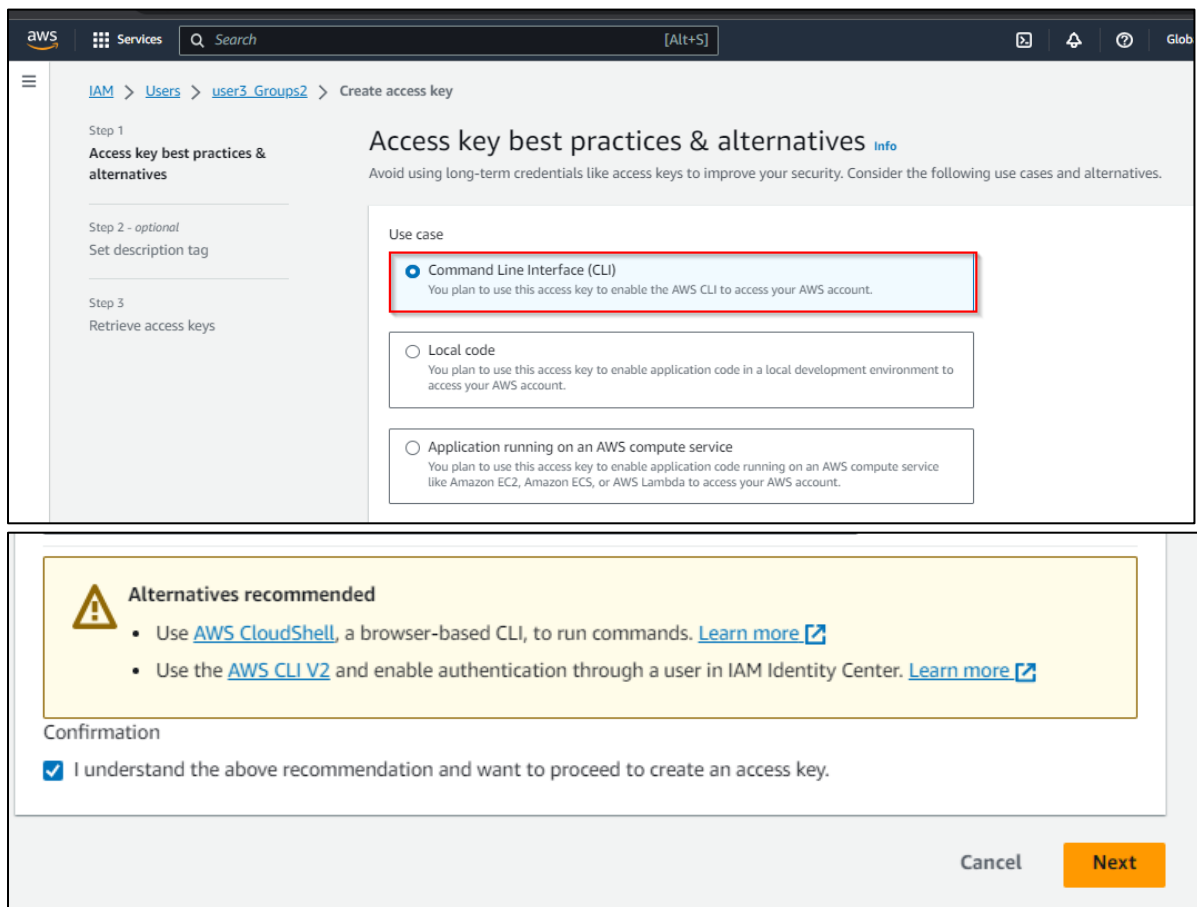
### 1.12 Create five more users, and assign them to their respective groups following the above procedure



### 1.13 Select any user and click on **Create access key**



### 1.14 Click on **Command Line Interface (CLI)**, and then click **Next**





## 1.15 Enter any description tag value, and click on **Create access key**

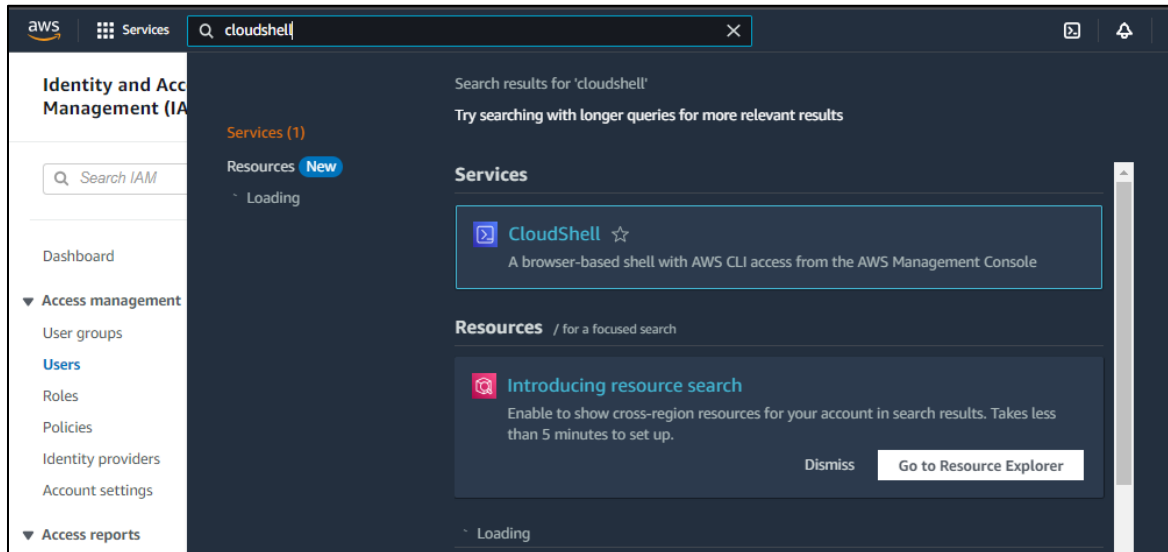
The screenshot shows the AWS IAM console interface. The breadcrumb trail is IAM > Users > user3\_Groups2 > Create access key. The left sidebar shows the progress: Step 1 (Access key best practices & alternatives), Step 2 - optional (Set description tag), and Step 3 (Retrieve access keys). The main content area is titled 'Set description tag - optional' with an info icon. Below the title, it says 'The description for this access key will be attached to this user as a tag and shown alongside the access key.' There is a text input field labeled 'Description tag value' with the text 'Users' entered. Below the field, it says 'Maximum 256 characters. Allowed characters are letters, numbers, spaces representable in UTF-8, and: \_ . : / = + \* @'. At the bottom right, there are three buttons: 'Cancel', 'Previous', and 'Create access key'.

The screenshot shows the AWS IAM console interface after the access key has been created. A green banner at the top states: '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 access key any time.' The breadcrumb trail is IAM > Users > user2\_Groups1 > Create access key. The left sidebar shows the progress: Step 1 (Access key best practices & alternatives), Step 2 - optional (Set description tag), and Step 3 (Retrieve access keys). The main content area is titled 'Retrieve access keys' with an info icon. Below the title, it says '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.' There is a table with two columns: 'Access key' and 'Secret access key'. The first row shows the access key 'AKIA3WNOKQ7JVAR2FH44' and the secret access key 'NDLyBVKNnA27ghPMkmou1EsdoituNvx1z7TqGVk'. A 'Hide' link is next to the secret access key. Below the table, there is a section titled 'Access key best practices' with a list of bullet points: '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.', and 'Rotate access keys regularly.' At the bottom, it says 'For more details about managing access keys, see the [best practices for managing AWS access keys](#)'.

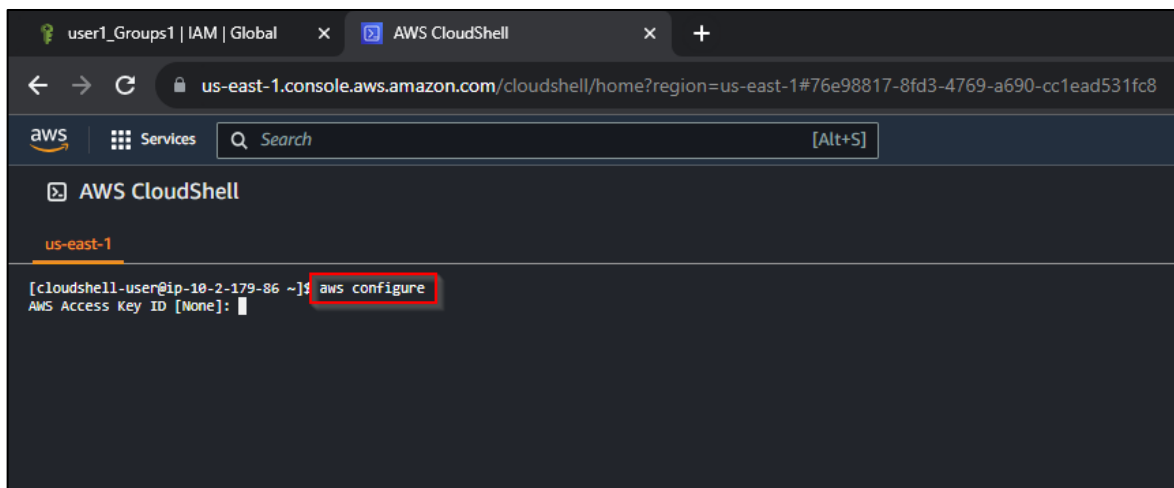
The Access key is created successfully.

## Step 2: Configure the user for CLI operation

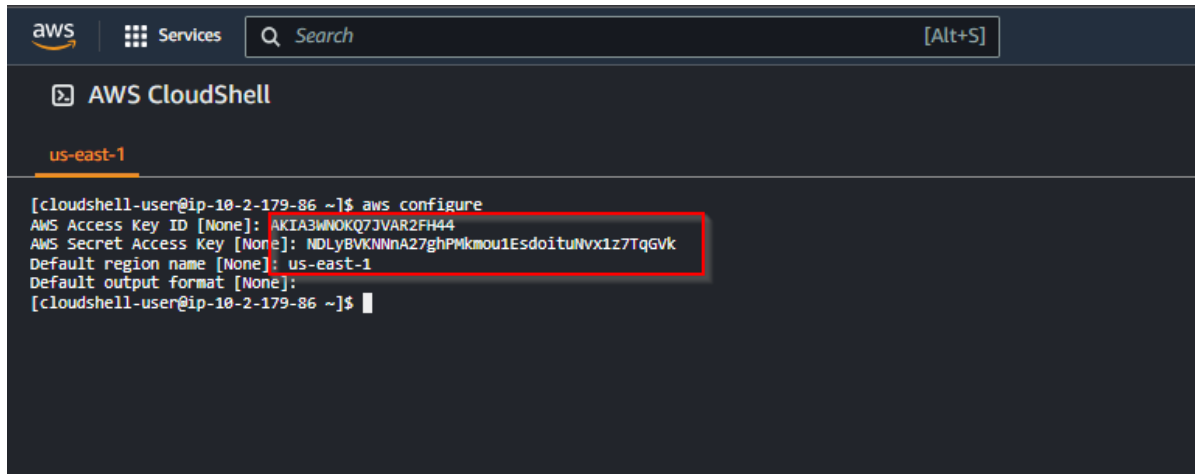
2.1 In the AWS dashboard, search for and select **CloudShell**



2.2 In CloudShell, enter the following command:  
**aws configure**



2.3 Open the downloaded .csv file, and copy-paste the Access Key ID and Secret Access Key into the terminal



The screenshot shows the AWS CloudShell interface. At the top, there's a navigation bar with the AWS logo, a 'Services' menu, a search bar, and an '[Alt+S]' button. Below this, the 'AWS CloudShell' header is visible, followed by the region 'us-east-1'. The terminal window shows the command `aws configure` being executed. The output displays the configuration details: 'AWS Access Key ID [None]: AKIA3WNNOKQ7JVAR2FH44', 'AWS Secret Access Key [None]: NDLYBVKNNnA27ghPMkmou1EsdoituNvx1z7TqGVk', 'Default region name [None]: us-east-1', and 'Default output format [None]:'. A red rectangular box highlights the Access Key ID and Secret Access Key values. The prompt `[cloudshell-user@ip-10-2-179-86 ~]$` is shown at the bottom.

```
[cloudshell-user@ip-10-2-179-86 ~]$ aws configure
AWS Access Key ID [None]: AKIA3WNNOKQ7JVAR2FH44
AWS Secret Access Key [None]: NDLYBVKNNnA27ghPMkmou1EsdoituNvx1z7TqGVk
Default region name [None]: us-east-1
Default output format [None]:
[cloudshell-user@ip-10-2-179-86 ~]$
```

The user is configured successfully for CLI operation.

By following these steps, you have successfully created and configured groups and users with different policies and permissions using AWS IAM.