

AWS Hands On

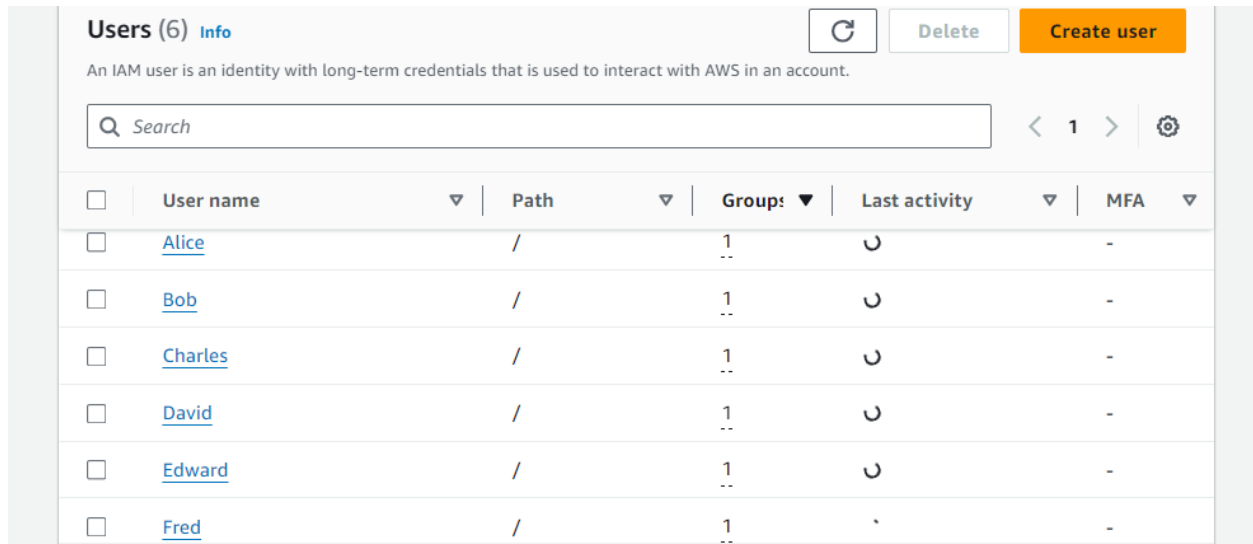
Deadline : 11 January 2024 01:30 pm

in AWS Console

Q1) Create 6 IAM Users:

1. Alice
2. Bob
3. Charles
4. David
5. Edward
6. Fred

SOLUTIONS:-



<input type="checkbox"/>	User name	Path	Group	Last activity	MFA
<input type="checkbox"/>	Alice	/	Users	U	-
<input type="checkbox"/>	Bob	/	Users	U	-
<input type="checkbox"/>	Charles	/	Users	U	-
<input type="checkbox"/>	David	/	Users	U	-
<input type="checkbox"/>	Edward	/	Users	U	-
<input type="checkbox"/>	Fred	/	Users	.	-

Q.2)








Create 3 groups:

1. Developers
2. Operations
3. Audit-Team

Add Alice, Bob, and Charles to the Developers group.

Add David and Edward to the Operations group.

Add Charles and David to the Audit-Team group.

User groups (3) Info							Delete	Create group
A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.								
<input type="text" value="Search"/>						 1  		
<input type="checkbox"/>	Group name	▲	Users	▼	Permissions	▼	Creation time	
<input type="checkbox"/>	Audit-Team		1	..	 Defined		6 minutes ago	
<input type="checkbox"/>	Developers		3	..	 Defined		1 hour ago	
<input type="checkbox"/>	Operations		2	..	 Defined		8 minutes ago	

Q3)

Assign the "IAMReadOnlyAccess" policy to the Developers group.
Assign the "IAMReadOnlyAccess" policy to the Operations group.
Assign the "IAMFullAccess" policy to the Audit-Team group.

Users (2)

Permissions

Access Advisor

Permissions policies (1) Info

Simulate

Remove

Add permissions

You can attach up to 10 managed policies.

Filter by Type

Search

All types

<1>

<input type="checkbox"/>	Policy name	Type	Attached entities
<input type="checkbox"/>	<div><div></div><div>IAMReadOnlyAccess</div></div>	AWS managed	2

Users (3)

Permissions

Access Advisor

Permissions policies (1) [Info](#)

↺

Simulate [↗](#)

Remove

Add permissions ▼

You can attach up to 10 managed policies.

Filter by Type

All types ▼

< 1 > ⚙

<input type="checkbox"/>	Policy name ↗	Type	Attached entities
<input type="checkbox"/>	IAMReadOnlyAccess	AWS managed	2

Users (1)

Permissions

Access Advisor

Permissions policies (1) [Info](#)

↺

Simulate [↗](#)

Remove

Add permissions ▼

You can attach up to 10 managed policies.

Filter by Type

All types ▼

< 1 > ⚙

<input type="checkbox"/>	Policy name ↗	Type	Attached entities
<input type="checkbox"/>	IAMFullAccess	AWS managed	1

Assign an inline policy to Fred.

IAM > Users > Fred > Edit policy

Step 1

Modify permissions in IAM-all-policies-assigned

Step 2

Review and save

Modify permissions in IAM-all-policies-assigned [Info](#)

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

Policy editor

Visual

JSON

Actions ▼

▶ IAM

Allow All actions

=====

Q4)

Log into the AWS account as an IAM user, add MFA, install AWS CLI, configure it in the terminal, and list IAM user actions using CLI command.




1) Added the MFA using google authenticator:-

2) Install AWS CLI, configure it in the terminal.

```
root@DESKTOP-NJS0G33:~# apt install awscli
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
awscli is already the newest version (1.22.34-1).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

simpal [Info](#) [Delete](#)

Summary

ARN  <code>arn:aws:iam::043241213129:user/simpal</code>	Console access  Enabled without MFA	Access key 1 Create access key
Created January 11, 2024, 10:51 (UTC+05:30)	Last console sign-in  Never	

[IAM](#) > [Users](#) > [simpal](#) > Create access key

Step 1

Access key best practices & alternatives

Step 2 - optional

Set description tag

Step 3

Retrieve access keys

Access key best practices & alternatives [Info](#)

Avoid using long-term credentials like access keys to improve your security. Consider the following use cases and alternatives.

Use case

☒ **Command Line Interface (CLI)**
You plan to use this access key to enable the AWS CLI to access your AWS account.

☐ **Local code**
You plan to use this access key to enable application code in a local development environment to access your AWS account.

```
root@DESKTOP-NJSOG33:~# aws configure
AWS Access Key ID [*****mpal]: AKIAQUELARTE20BP5CEJ
AWS Secret Access Key [*****l@01]: qyJyonWGCKG18eNWfGvCw7maikYvxeabJg7qN0EN
Default region name [us-east-1]: ap-south-1
Default output format [json]:
root@DESKTOP-NJSOG33:~#
```

3) IAM user actions using CLI command.

```
root@DESKTOP-NJSOG33:~# aws iam list-users
{
  "Users": [
    {
      "Path": "/",
      "UserName": "Alice",
      "UserId": "AIDAQUELARTE22AVIHUQ6",
      "Arn": "arn:aws:iam::043241213129:user/Alice",
      "CreateDate": "2024-01-10T12:11:03Z"
    },
    {
      "Path": "/",
      "UserName": "Bob",
      "UserId": "AIDAQUELARTERE23HBMUN",
      "Arn": "arn:aws:iam::043241213129:user/Bob",
      "CreateDate": "2024-01-10T12:14:08Z"
    },
    {
      "Path": "/",
      "UserName": "Charles",
      "UserId": "AIDAQUELARTE6Q3MQXPC5",
      "Arn": "arn:aws:iam::043241213129:user/Charles",
      "CreateDate": "2024-01-10T13:58:26Z"
    },
    {
      "Path": "/",
      "UserName": "David",
      "UserId": "AIDAQUELARTEXX5K7GLPI",
      "Arn": "arn:aws:iam::043241213129:user/David",
      "CreateDate": "2024-01-10T14:00:46Z"
    }
  ]
}
```