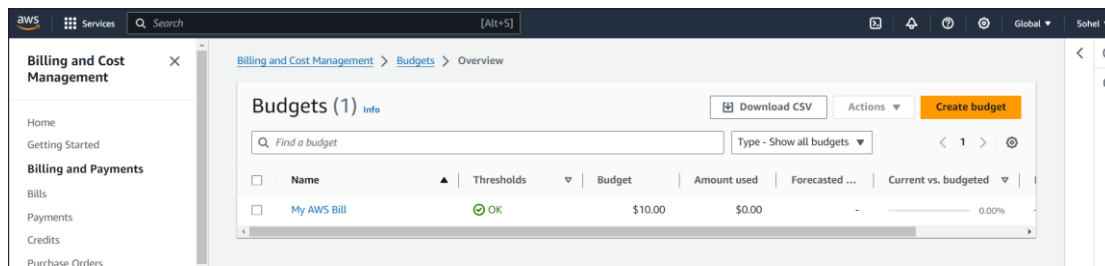


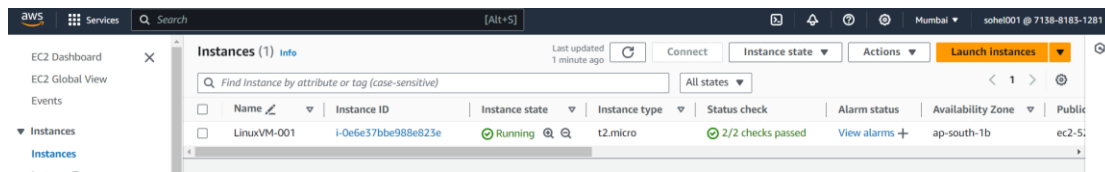
Assignment 1

1. Setup Billing Alarm

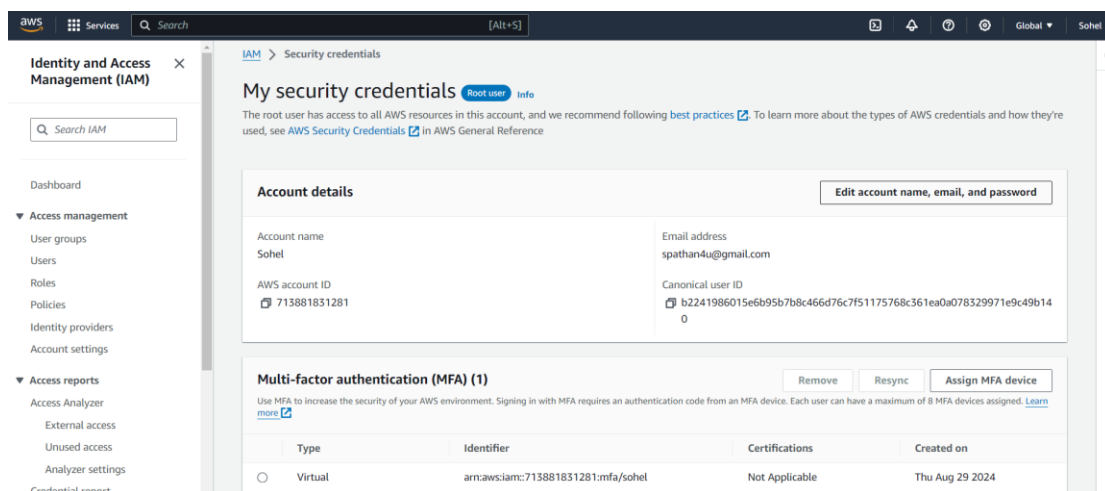
To set up a billing alarm in AWS, you will need to use the AWS Budgets service. This involves creating a budget that tracks your estimated charges, and then setting up an alert that sends you a notification if your charges exceed a defined threshold. For detailed steps, you can refer to the AWS documentation or online resources that explain how to navigate the AWS Billing and Cost Management console. Remember to double-check the steps and settings to ensure everything is configured correctly.



2. Create linux EC2 instance LinuxVM-001

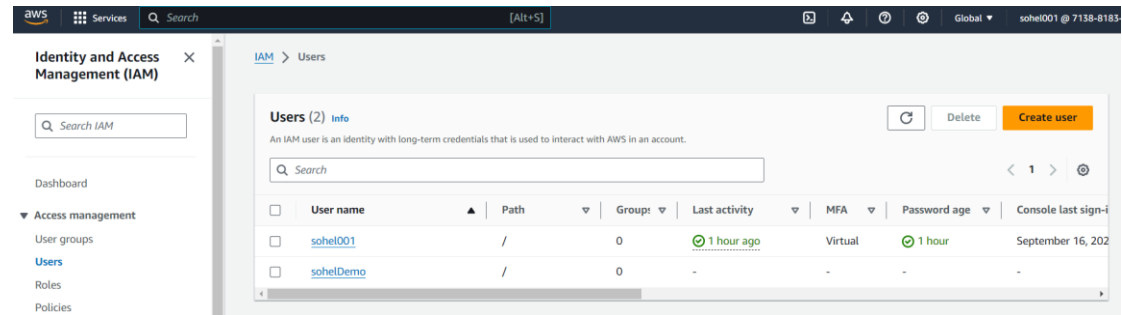


3. Setup MFA for root user



4. Create User, Group Role using GUI

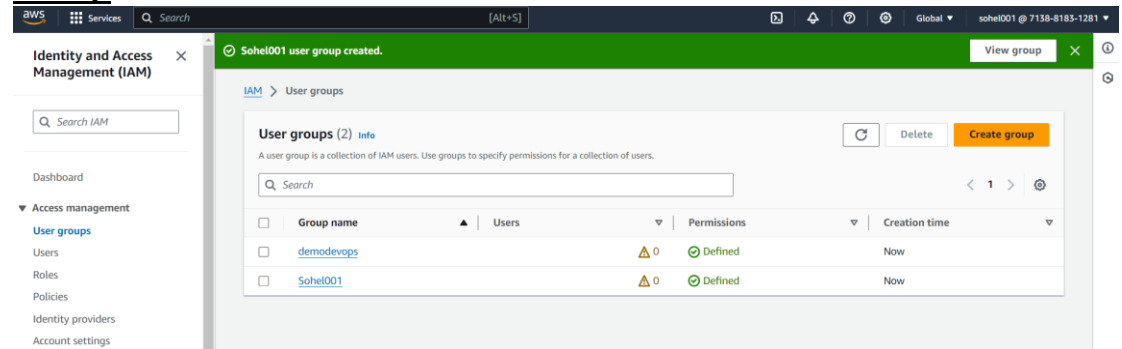
User:



The screenshot shows the AWS IAM console's 'Users' page. The left sidebar contains the 'Identity and Access Management (IAM)' menu with options like Dashboard, Access management, Users, Roles, and Policies. The main content area shows 'Users (2)' with a table listing two users: 'sohel001' and 'sohelDemo'. The 'sohel001' user is active, with a last activity of '1 hour ago' and a console last sign-in of 'September 16, 2024'.

User name	Path	Groups	Last activity	MFA	Password age	Console last sign-in
sohel001	/	0	1 hour ago	Virtual	1 hour	September 16, 2024
sohelDemo	/	0	-	-	-	-

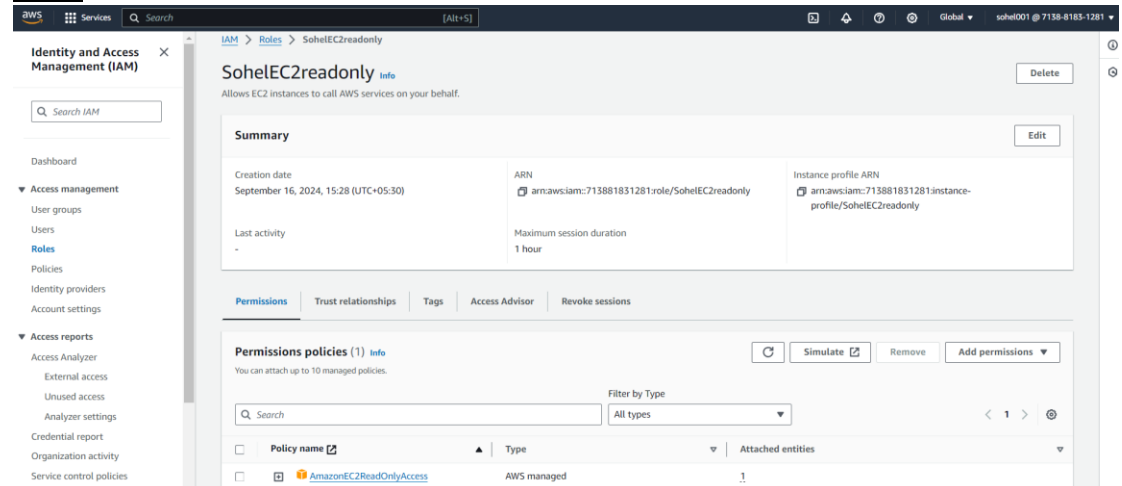
Group



The screenshot shows the AWS IAM console's 'User groups' page. A green banner at the top indicates 'Sohel001 user group created.' The main content area shows 'User groups (2)' with a table listing two groups: 'demodevops' and 'Sohel001'. Both groups are 'Defined' and have a creation time of 'Now'.

Group name	Users	Permissions	Creation time
demodevops	0	Defined	Now
Sohel001	0	Defined	Now

Role



The screenshot shows the AWS IAM console's 'SohelEC2readonly' role details page. The left sidebar shows the 'Roles' menu. The main content area displays the role's summary, including creation date (September 16, 2024, 15:28 UTC+05:30), ARN (arn:aws:iam::713881831281:role/SohelEC2readonly), and instance profile ARN (arn:aws:iam::713881831281:instance-profile/SohelEC2readonly). The 'Permissions' tab is selected, showing 'Permissions policies (1)' with a table listing 'AmazonEC2ReadOnlyAccess' as an AWS managed policy attached to the role.

Policy name	Type	Attached entities
AmazonEC2ReadOnlyAccess	AWS managed	1

5. Create Role Group using CLI

```
C:\WINDOWS\system32\cmd. X + v

Microsoft Windows [Version 10.0.22631.4169]
(c) Microsoft Corporation. All rights reserved.

C:\Users\patha>aws configure
AWS Access Key ID [None]: AKIA2MNVMI5YUFVBCEE7
AWS Secret Access Key [None]: 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
Default region name [None]: ap-south-1
Default output format [None]: json

C:\Users\patha>aws iam create-user --user-name sohel0202
{
  "User": {
    "Path": "/",
    "UserName": "sohel0202",
    "UserId": "AIDA2MNVMI5YW2BUW3W2N",
    "Arn": "arn:aws:iam::713881831281:user/sohel0202",
    "CreateDate": "2024-09-16T10:21:24+00:00"
  }
}
```

Group

```
C:\Users\patha>aws iam create-group --group-name fusion
{
  "Group": {
    "Path": "/",
    "GroupName": "fusion",
    "GroupId": "AGPA2MNVMI5YRYT5L4VBR",
    "Arn": "arn:aws:iam::713881831281:group/fusion",
    "CreateDate": "2024-09-16T10:23:39+00:00"
  }
}
```

GUI:

The screenshot displays the AWS Management Console interface. At the top, a green notification banner indicates that the IAMAdminrole has been successfully attached to instance i-0888bacd7bcfa0cd. The left sidebar shows the navigation menu with 'Instances' selected. The main content area shows the 'Instances' table with two entries: 'demo-vm' (Terminated) and 'demoveops-vm' (Running). The 'demoveops-vm' instance is highlighted, and its details are shown in the right-hand pane. The details include the Instance ID, Public IPv4 address (65.1.111.183), Private IPv4 address (172.31.6.23), and the Instance state (Running).

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public
demo-vm	i-0e892b17dbdd0ad652	Terminated	t2.micro	-	View alarms +	ap-south-1b	-
demoveops-vm	i-0888bacd7bcfa0cd	Running	t2.micro	2/2 checks passed	View alarms +	ap-south-1b	ec2-65-1-111-183.ap-south-1.compute.amazonaws.com

i-0888bacd7bcfa0cd (demoveops-vm)

Instance summary

Instance ID: i-0888bacd7bcfa0cd (demoveops-vm)

Public IPv4 address: 65.1.111.183 | [open address](#)

Private IPv4 address: 172.31.6.23

Instance state: **Running**

Public IPv4 DNS: ec2-65-1-111-183.ap-south-1.compute.amazonaws.com | [open address](#)

Private IP DNS name (IPv4 only): ip-172-31-6-23.ap-south-1.compute.internal

7 . Attach role and secret access key to the instance

Attach role to the instance

```
ec2-user@ip-172-31-6-23:~  
login as: ec2-user  
Authenticating with public key "soheldemo-001"  
Last login: Mon Sep 16 11:01:01 2024 from 152.57.2.140  
#  
~\#### Amazon Linux 2  
~~\#####  
~~\#### AL2 End of Life is 2025-06-30.  
~~\#/   
~~V~' '->  
~~  
~~~ A newer version of Amazon Linux is available!  
~~~  
~~~ Amazon Linux 2023, GA and supported until 2028-03-15.  
~~~ https://aws.amazon.com/linux/amazon-linux-2023/  
ec2-user@ip-172-31-6-23 ~]$ configure list  
bash: configure: command not found  
ec2-user@ip-172-31-6-23 ~]$ aws configure list  
Name Value Type Location  
----  
profile <not set> None None  
access_key *****4YUJ iam-role  
secret_key *****5WtP iam-role  
region <not set> None None  
ec2-user@ip-172-31-6-23 ~]$
```

Attach secret key and access key to the instance

```
[root@ip-172-31-6-23 ~]# aws configure list  
Name Value Type Location  
----  
profile <not set> None None  
access_key *****CEE7 shared-credentials-file  
secret_key *****H7dD shared-credentials-file  
region ap-south-1 config-file ~/.aws/config  
[root@ip-172-31-6-23 ~]#
```