

# TASK IAM

## 1-Create one IAM user and assign ec2,s3 full access role

The screenshot shows the AWS IAM console for user 'Farsaan97'. The left sidebar contains the 'Identity and Access Management (IAM)' menu. The main content area shows the user's details, including the ARN, console access status, and a list of permissions policies. The 'Permissions policies' section is expanded, showing three policies: 'AmazonEC2FullAccess', 'AmazonS3FullAccess', and 'IAMUserChangePassword'. Red arrows point to the 'Info' link and the 'AmazonEC2FullAccess' and 'AmazonS3FullAccess' policies.

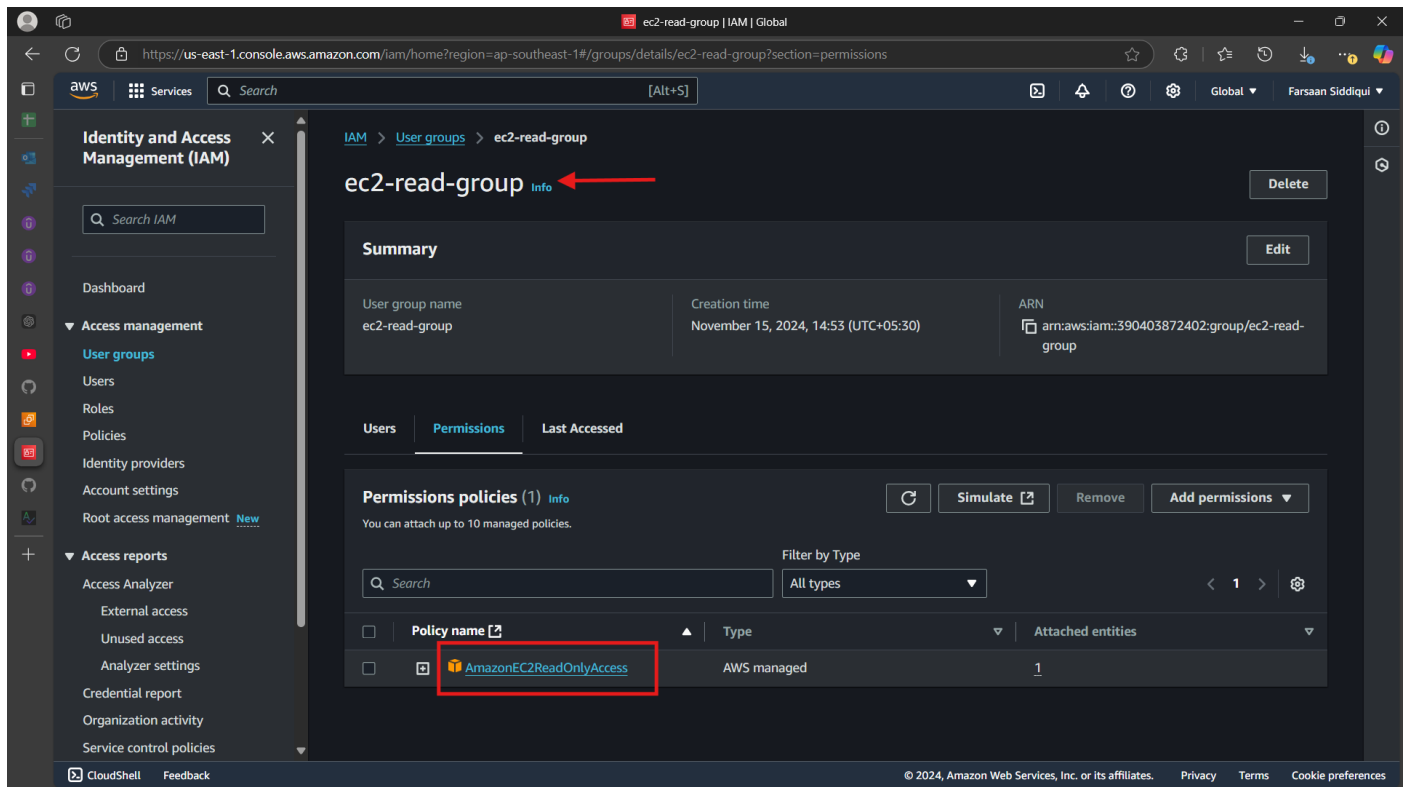
Policy name	Type	Attached via
AmazonEC2FullAccess	AWS managed	Directly
AmazonS3FullAccess	AWS managed	Directly
IAMUserChangePassword	AWS managed	Directly

\*Checking by login in with <Farsaan97>

The screenshot shows the AWS Management Console for the 'Resources' section. The 'Launch instance' button is highlighted. A red box highlights the 'Launch instance' button and the 'Migrate a server' button.

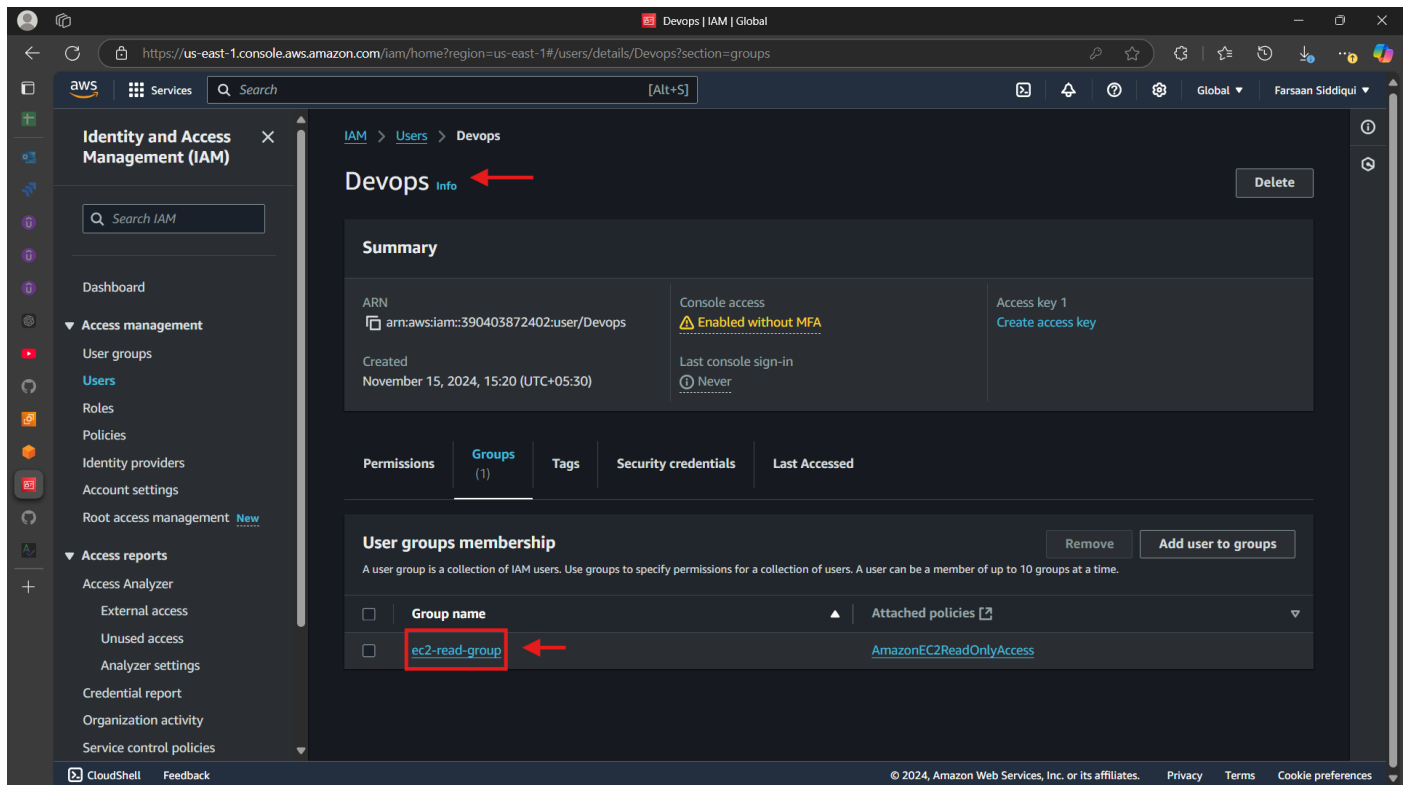
The screenshot shows the AWS Management Console for the 'Amazon S3' page. The 'Create a bucket' button is highlighted. A red box highlights the 'Create a bucket' button and the 'Pricing' section.

## 2.Create one Group in IAM and Assign Read access for ec2



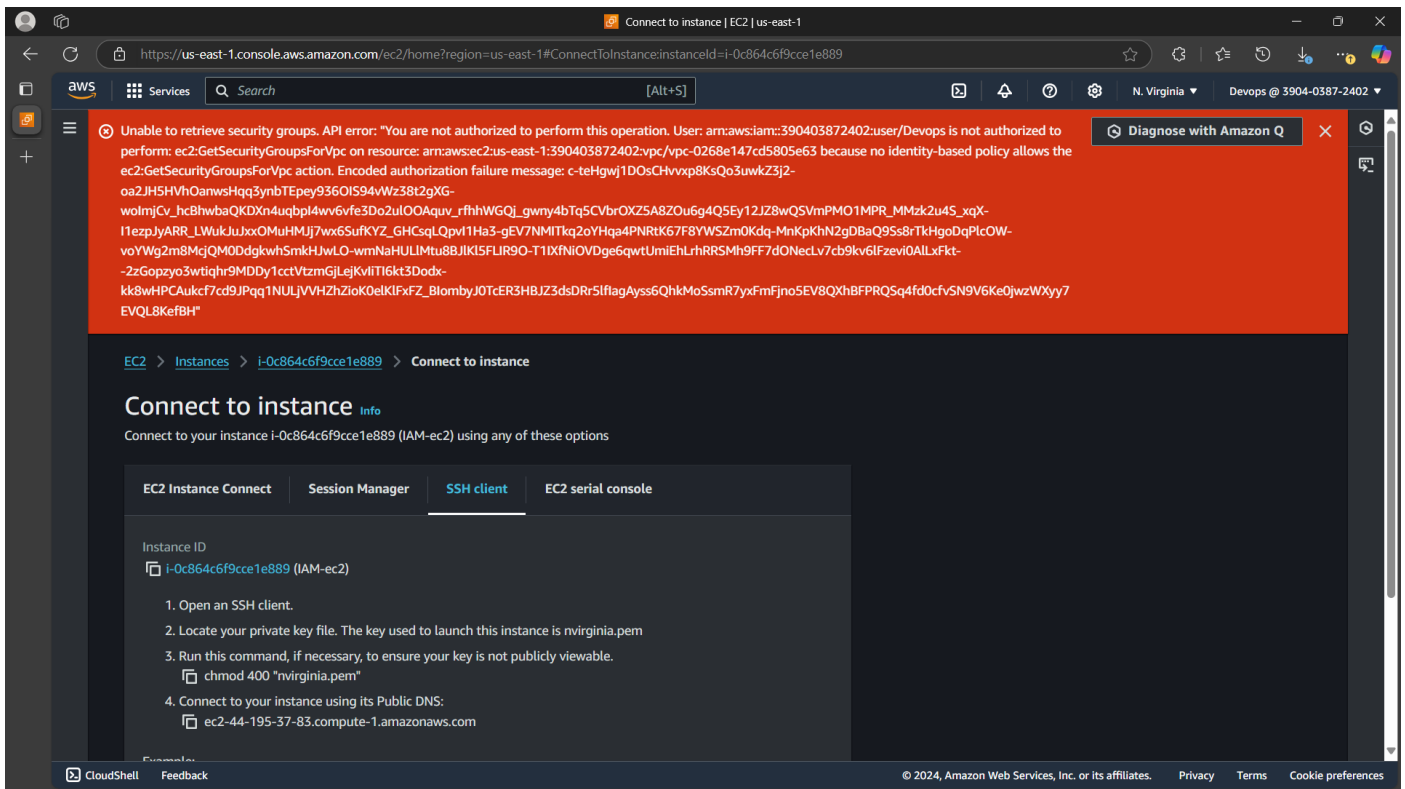
The screenshot shows the AWS IAM console interface. The left sidebar contains the 'Identity and Access Management (IAM)' menu with options like Dashboard, Access management, Users, Roles, Policies, Identity providers, Account settings, Root access management, Access reports, Access Analyzer, External access, Unused access, Analyzer settings, Credential report, Organization activity, and Service control policies. The main content area displays the details for the 'ec2-read-group' user group. The 'Summary' section shows the user group name 'ec2-read-group', creation time 'November 15, 2024, 14:53 (UTC+05:30)', and ARN 'arn:aws:iam::390403872402:group/ec2-read-group'. The 'Permissions' tab is active, showing a table of attached policies. The table has columns for 'Policy name', 'Type', and 'Attached entities'. One policy is listed: 'AmazonEC2ReadOnlyAccess' (AWS managed) with 1 attached entity. A red arrow points to the 'ec2-read-group' group name, and another red box highlights the 'AmazonEC2ReadOnlyAccess' policy.

## 3.Create a new user with name Devops and add to the group created in task2



The screenshot shows the AWS IAM console interface for the 'Devops' user. The left sidebar is the same as in the previous screenshot. The main content area displays the details for the 'Devops' user. The 'Summary' section shows the user's ARN 'arn:aws:iam::390403872402:user/Devops', console access status 'Enabled without MFA', and last console sign-in 'Never'. The 'Groups' tab is active, showing a table of group memberships. The table has columns for 'Group name' and 'Attached policies'. One group is listed: 'ec2-read-group' with the 'AmazonEC2ReadOnlyAccess' policy attached. A red arrow points to the 'Devops' user name, and another red box highlights the 'ec2-read-group' group name.

\*Checking by logging in as Devops if we have only read access or we can connect to ec2



## 4. Write a bash script to create a IAM user with VPC full access

```
#!/bin/bash
```

```
USER_NAME="vpc_iam_ujser"
```

```
POLICY_NAME="VPCFullAccessPolicy"
```

```
# Create IAM user
```

```
aws iam create-user --user-name $USER_NAME
```

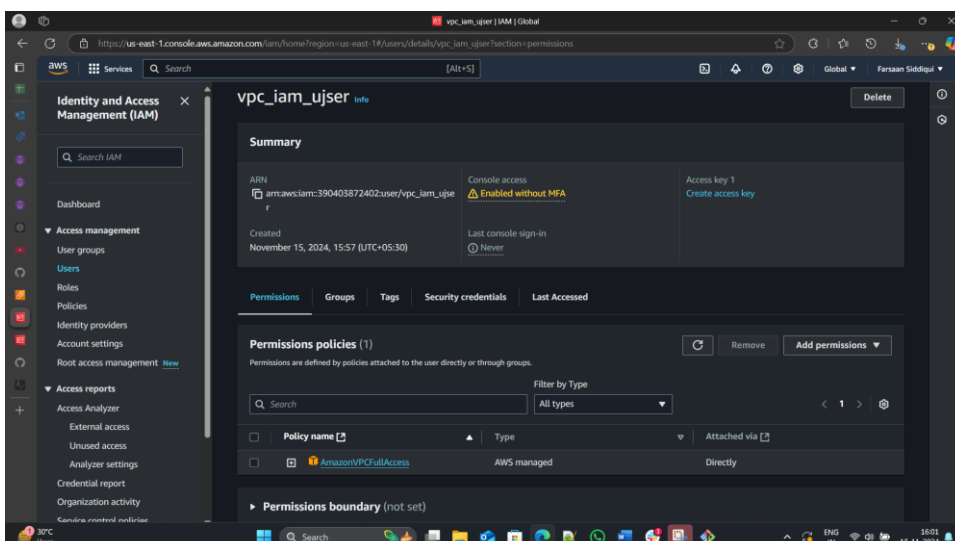
```
# Attach policy to the user
```

```
aws iam attach-user-policy --user-name $USER_NAME --policy-arn arn:aws:iam::aws:policy/AmazonVPCFullAccess
```

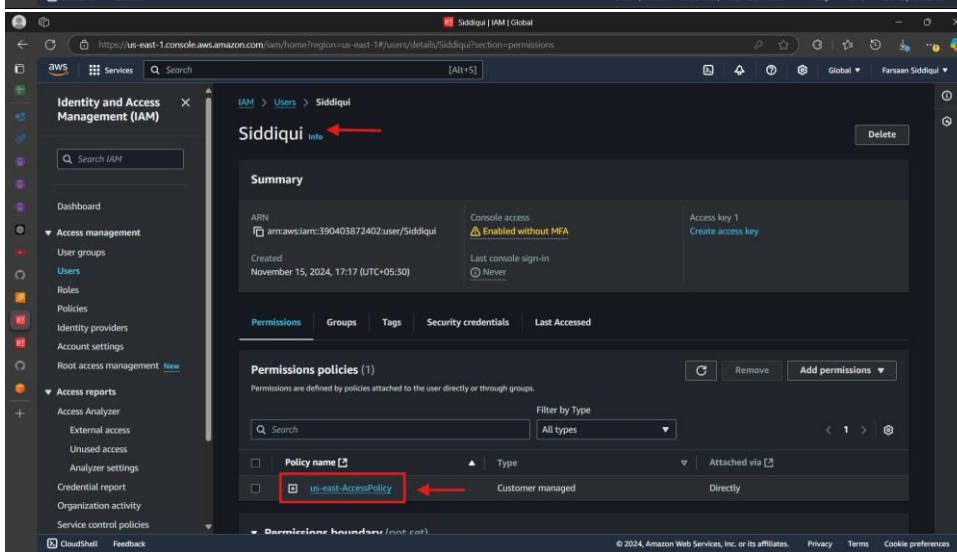
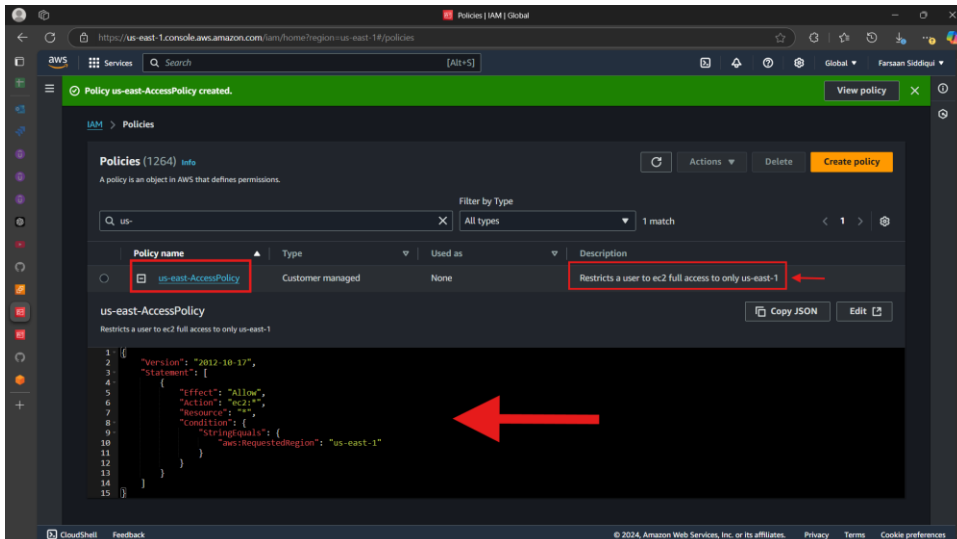
```
# Create login profile for console access
```

```
aws iam create-login-profile --user-name $USER_NAME --password "Devops@123" --password-reset-required
```

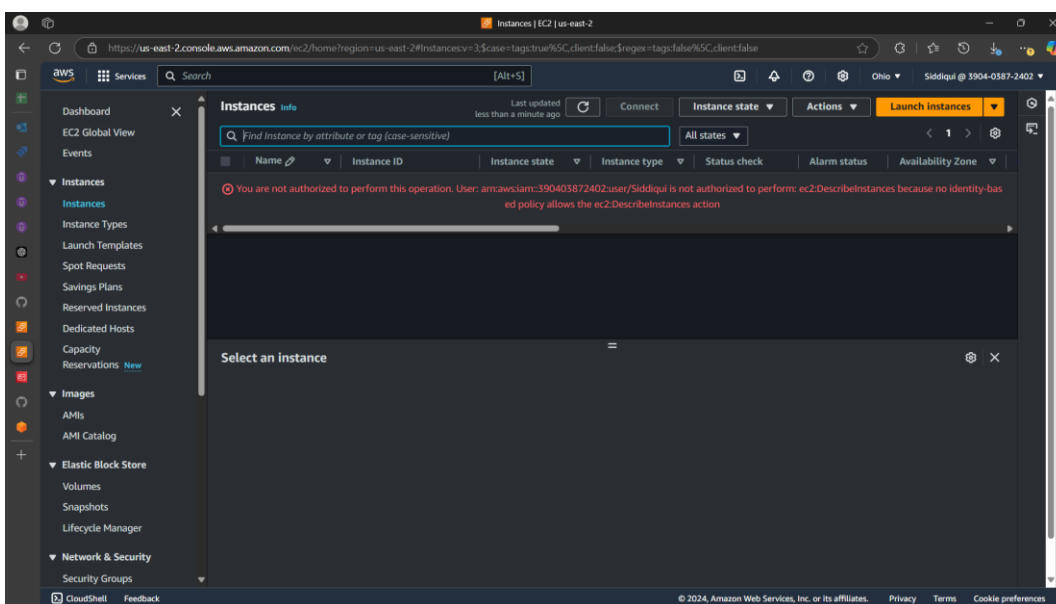
```
echo "IAM user $USER_NAME created with VPC full access and console access."
```



## 5. Create a IAM policy to access ec2 for a specific user in specific regions only



\*Logging in as Siddiqui as trying to change region and access ec2 service



<We have two accounts Account A and Account B, Account A user should access s3 bucket in Account B.>