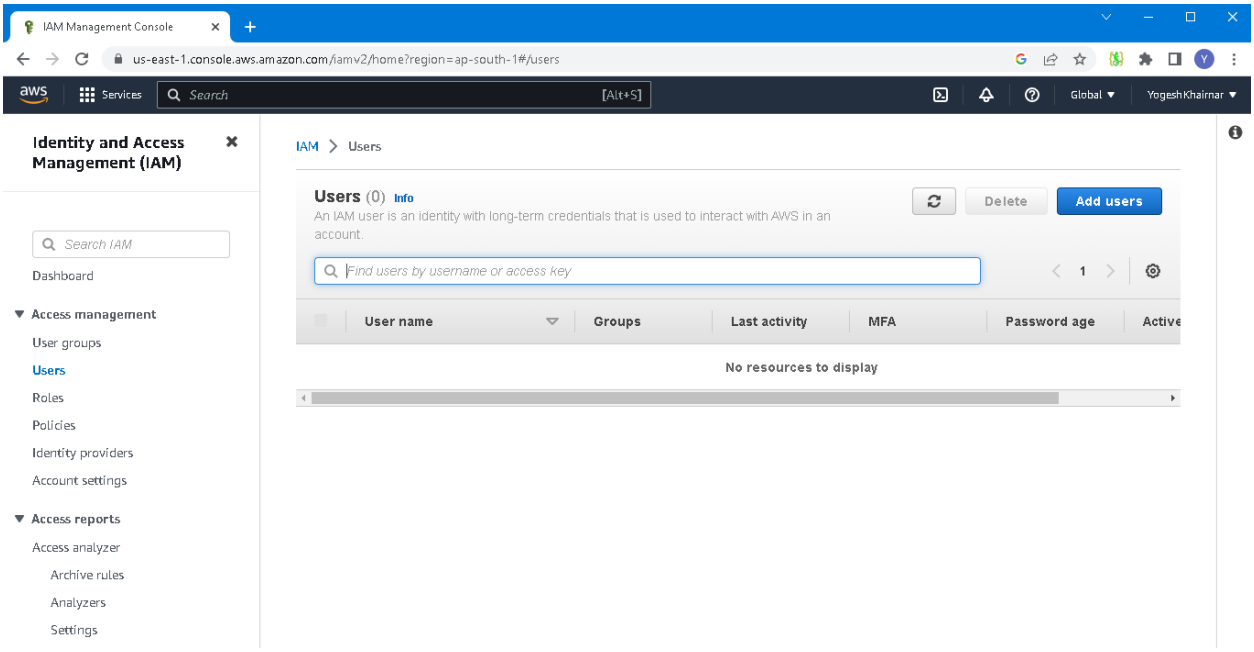
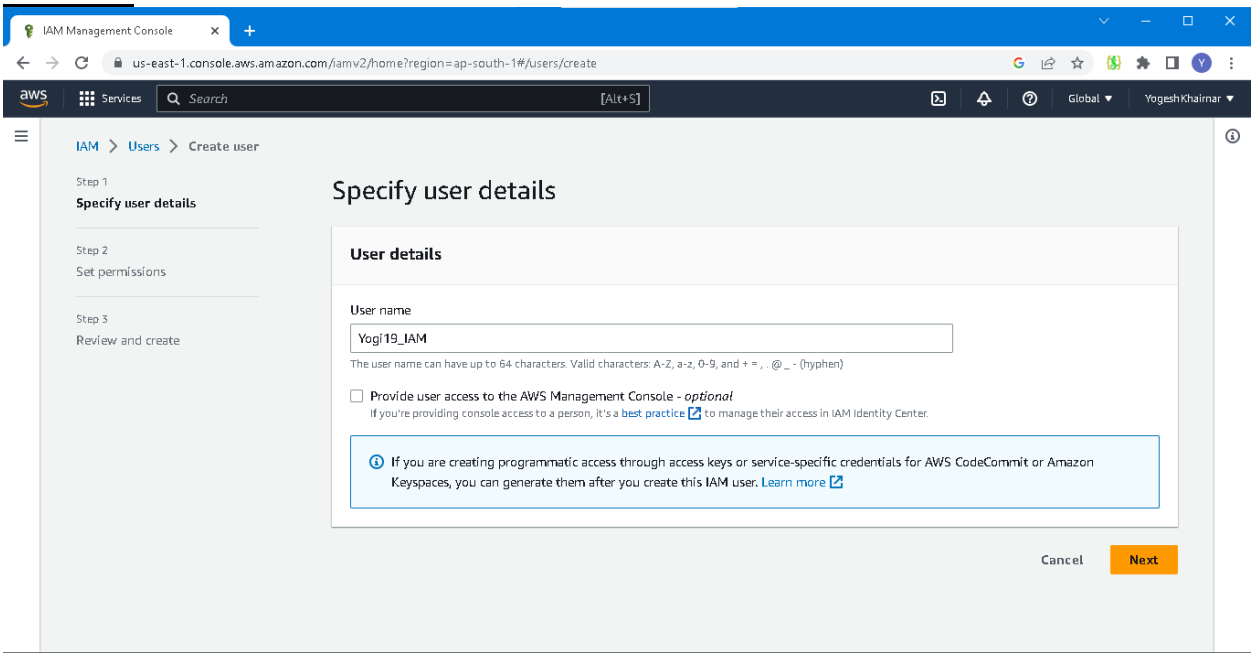
AWS CLI Practical-Launching EC2 Instance and Creating S3 Bucket

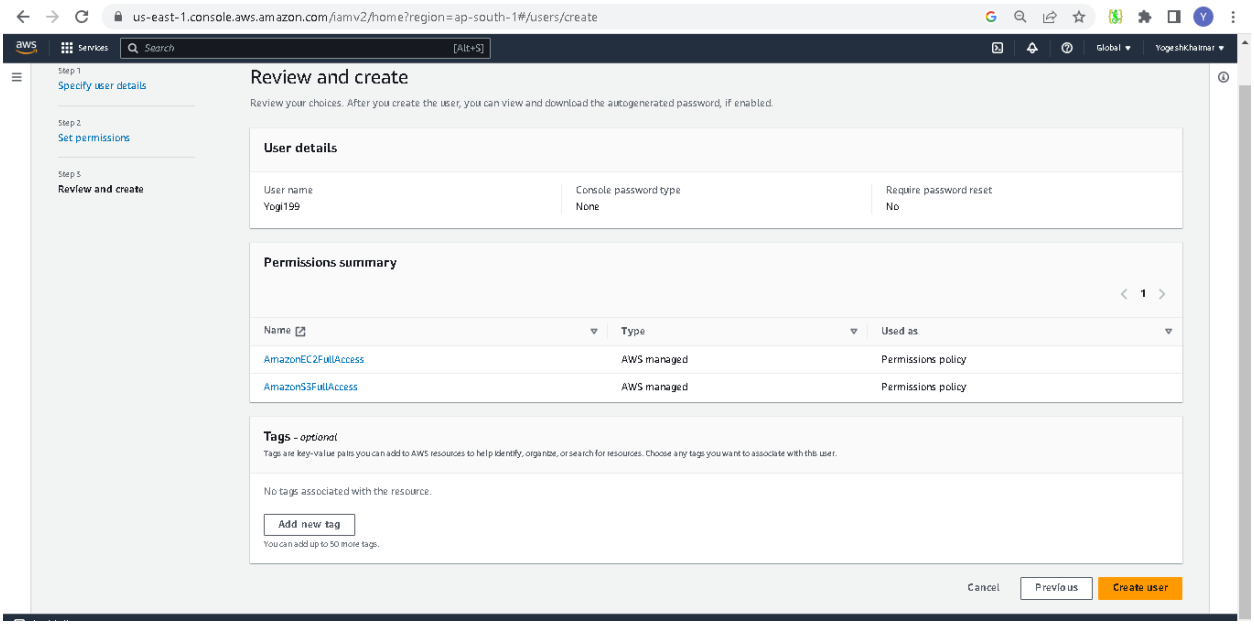
Step 1:- Create a IAM user Account.

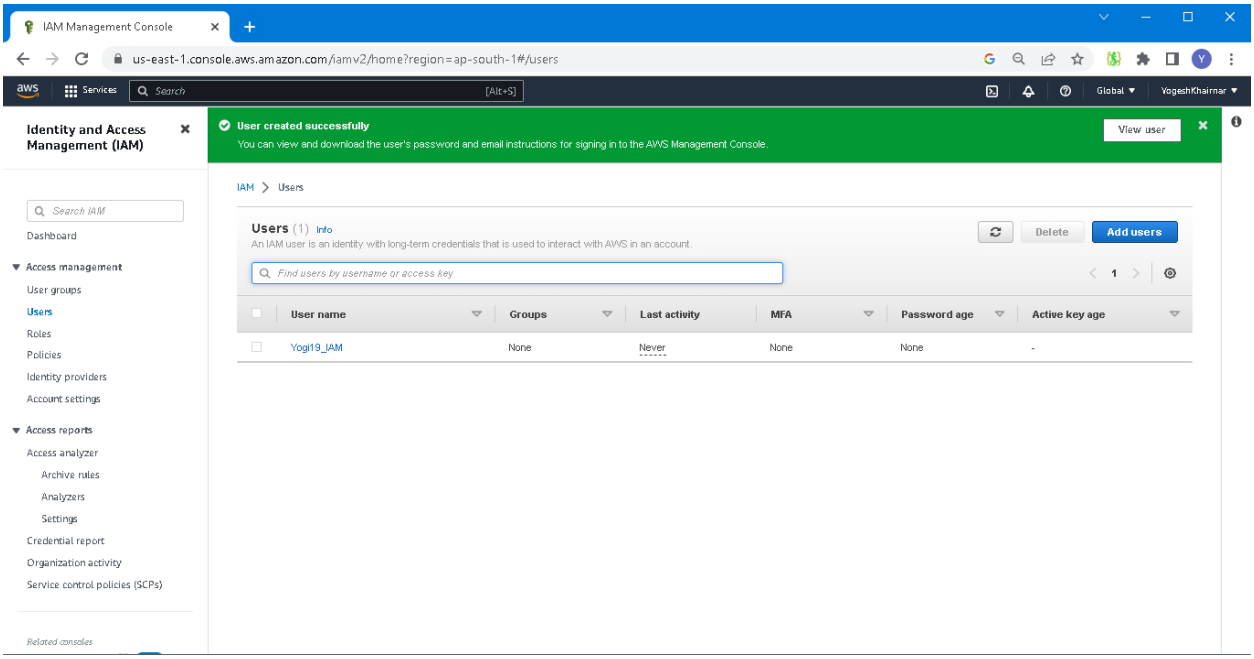
Go to IAM >User > Add User



Step 2:-Specify user details (give username – click on next)>set permission(attach policies- click on next)>Click create user>user will be created.

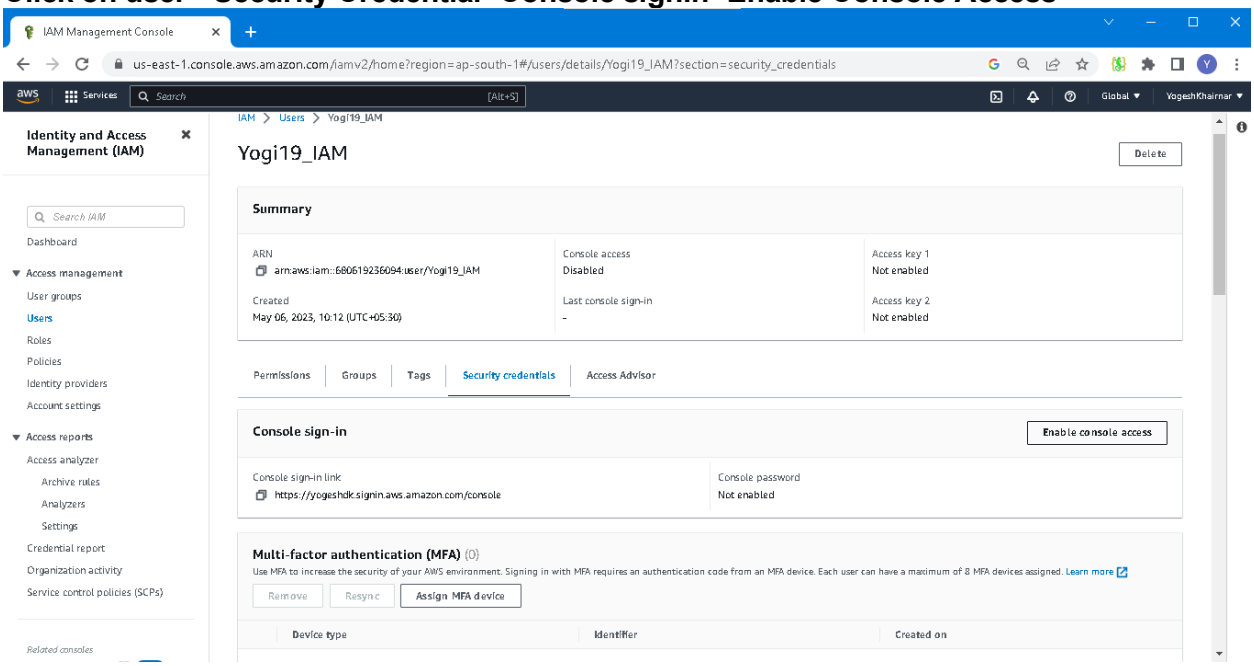



us-east-1.console.aws.amazon.com/iamv2/home?region=ap-south-1#/users/create
Services
Search
[Alt+S]
Global
YogeshKhairnar
Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Review and create
Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.
User details
User name
Yogi199
Console password type
None
Require password reset
No
Permissions summary
Name
Type
Used as
AmazonEC2FullAccess
AWS managed
Permissions policy
AmazonS3FullAccess
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

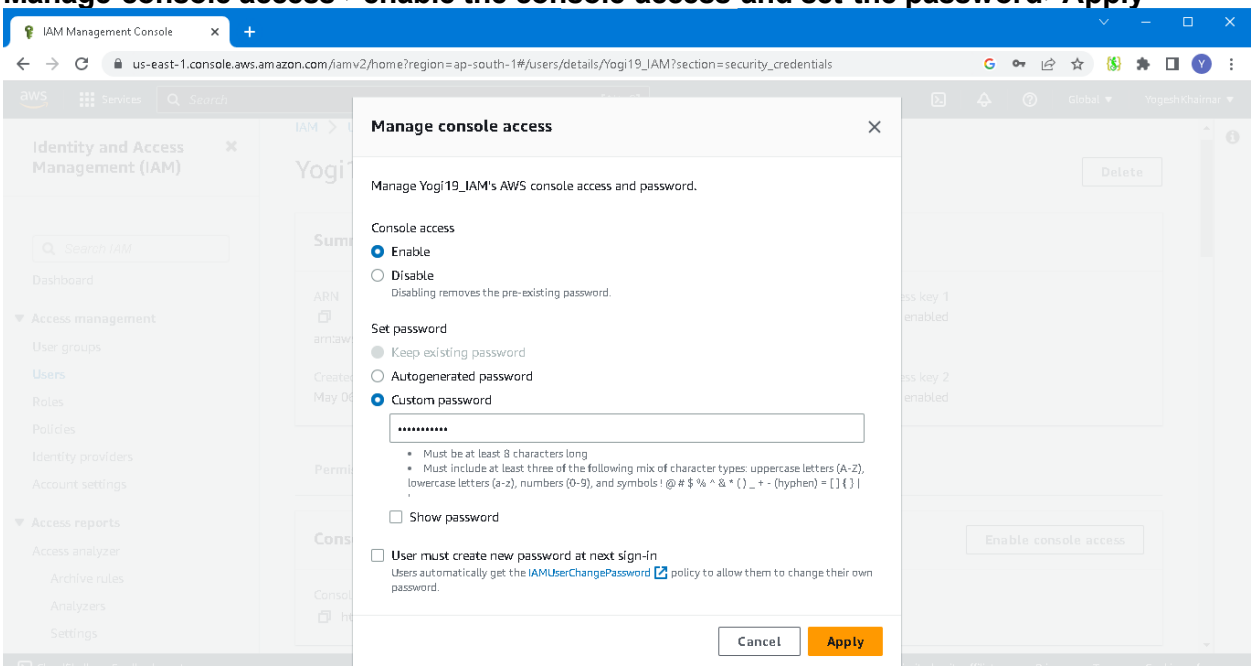

IAM Management Console
us-east-1.console.aws.amazon.com/iamv2/home?region=ap-south-1#/users
Services
Search
[Alt+S]
Global
YogeshKhairnar
Identity and Access Management (IAM)
User created successfully
You can view and download the user's password and email instructions for signing in to the AWS Management Console.
View user
Search 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
Service control policies (SCPs)
Related consoles
IAM
Users
Users (1) Info
An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.
Delete
Add users
Find users by username or access key
User name
Groups
Last activity
MFA
Password age
Active key age
Yogi19_IAM
None
Never
None
None
-

Step 3:- Give user a password.

Click on user >Security Credential>Console signin>Enable Console Access



Manage console access >enable the console access and set the password>Apply



Step 4:-Go to IAM user page>click on user>Security Credential>Click On Create Access Key>Access key best practices & alternative(Select CLI)>Access key will be created>save that Access key & Secret access key.

Step 5:-Launch EC2 Instance(In my case,I have used ubuntu)>Install aws cli by using commands.

sudo apt-get update
sudo apt-get install awscli

```
ubuntu@ip-172-31-40-21:~$ sudo apt-get install awscli
eading package lists... Done
```

Step 6:-Configure aws cli by giving the access key id and secret key(Region you may give of you choice).

```
ubuntu@ip-172-31-40-21:~$ aws configure
AWS Access Key ID [None]: AKIAZ46ARLL7CZLZG6BT
AWS Secret Access Key [None]: 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
Default region name [None]: ap-south-1
Default output format [None]:
```

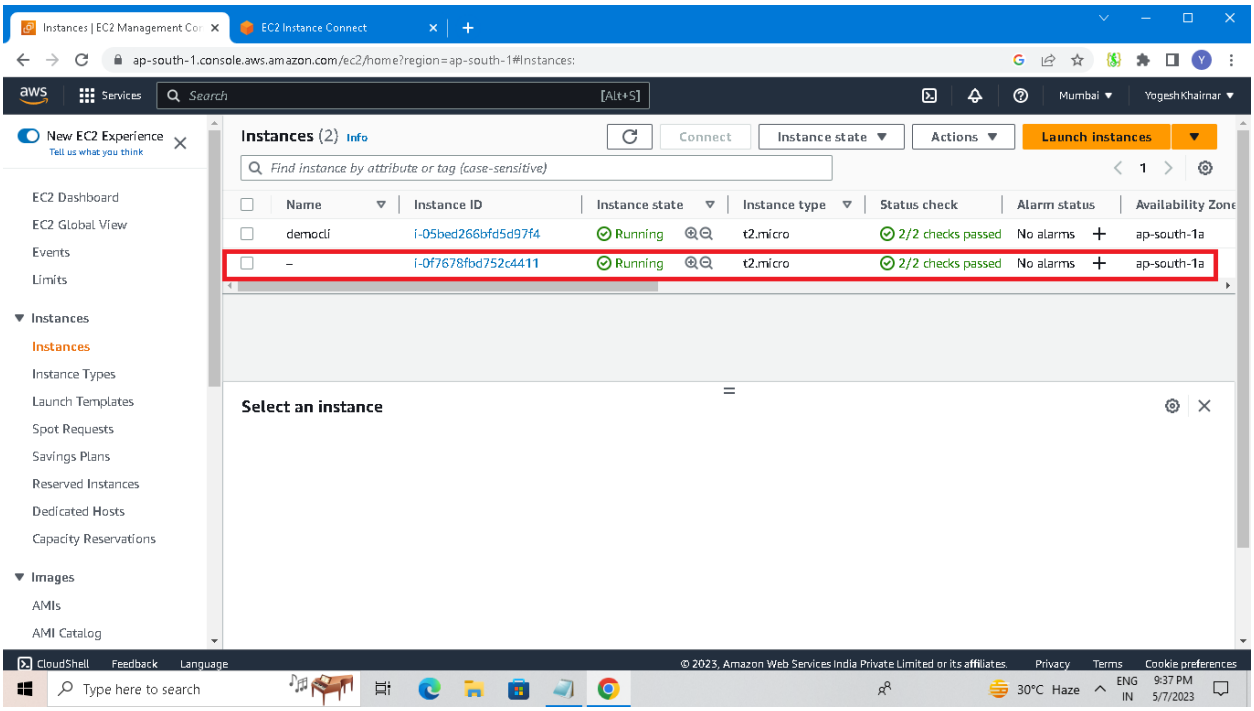
Step 7:-Launch EC2 Instance in awc cli.

For that we have to give these command

aws ec2 run-instances –image-id “copy the ami id from instance page” –count 1 –instance-type t2.micro --key-name “key name which you have created”

```
ubuntu@ip-172-31-40-21:~$ aws ec2 run-instances --image-id ami-02eb7a4783e7e9317 --count 1 --instance-type t2.micro --key-name win_key
{
    "Groups": [],
    "Instances": [
        {
            "AmiLaunchIndex": 0,
```

You can see the instance is created



Step 8:-Create a s3 bucket.

for that use the following command

aws s3api create-bucket --bucket clibucket12 --region us-east-1