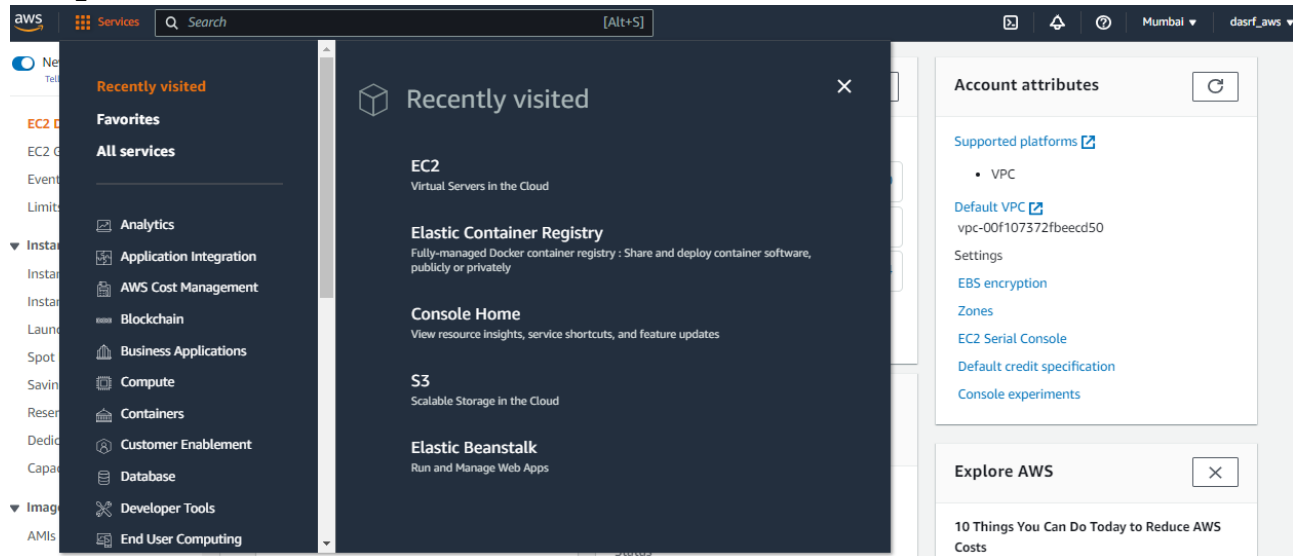
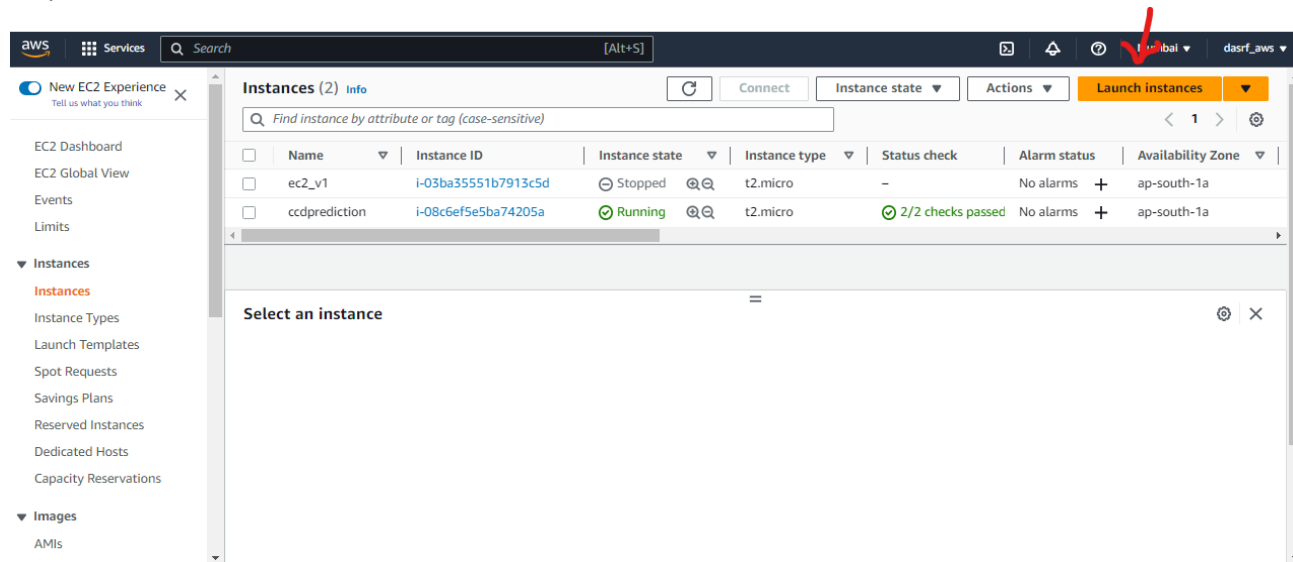


Launch EC2 Instance in free tier in AWS with free tier:

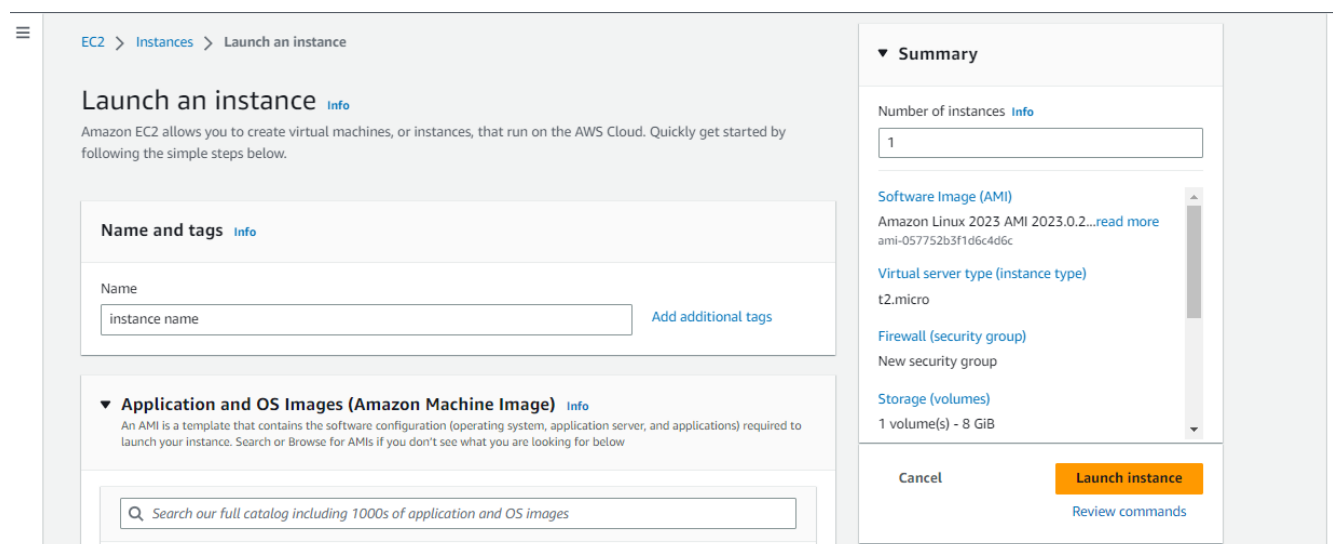
Step1: Search for EC2



Step2: Click on Launch Instances



Step3: Provide an instance name



Step4: Select a platform on which your instance will run. For free tire select Ubuntu and choose free tire eligible machine and configuration. Otherwise, services will be charged

Recents

Quick Start

Amazon Linux

aws

macOS

Mac

Ubuntu

ubuntu

Windows

Microsoft

Red Hat

Red Hat

Browse more AMIs

Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Ubuntu Server 22.04 LTS (HVM), SSD Volume Type

Free tier eligible

ami-0f5ee92e2d63afc18 (64-bit (x86)) / ami-077053fb4029de92f (64-bit (Arm))

Virtualization: hvm ENA enabled: true Root device type: ebs

Description

Canonical, Ubuntu, 22.04 LTS, amd64 jammy image build on 2023-05-16

Architecture

AMI ID

64-bit (x86)

ami-0f5ee92e2d63afc18

Verified provider

▼ Summary

Number of instances [Info](#)

1

Software Image (AMI)

Canonical, Ubuntu, 22.04 LTS, ...[read more](#)

ami-0f5ee92e2d63afc18

Virtual server type (instance type)

t2.micro

Firewall (security group)

New security group

Storage (volumes)

1 volume(s) - 8 GiB

Cancel

Launch instance

[Review commands](#)

Step5: Create a key-pair and download the .perm file in your local desktop and Launch instances

▼ Instance type [Info](#)

Instance type

t2.micro

Free tier eligible

Family: t2 1 vCPU 1 GiB Memory Current generation: true

On-Demand Linux pricing: 0.0124 USD per Hour

On-Demand Windows pricing: 0.017 USD per Hour

On-Demand RHEL pricing: 0.0724 USD per Hour

On-Demand SUSE pricing: 0.0124 USD per Hour

All generations

[Compare instance types](#)

▼ Key pair (login) [Info](#)

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - required

Select

Create new key pair

▼ Network settings [Info](#)

Edit

Network [Info](#)

▼ Summary

Number of instances [Info](#)

1

Software Image (AMI)

Canonical, Ubuntu, 22.04 LTS, ...[read more](#)

ami-0f5ee92e2d63afc18

Virtual server type (instance type)

t2.micro

Firewall (security group)

New security group

Storage (volumes)

1 volume(s) - 8 GiB

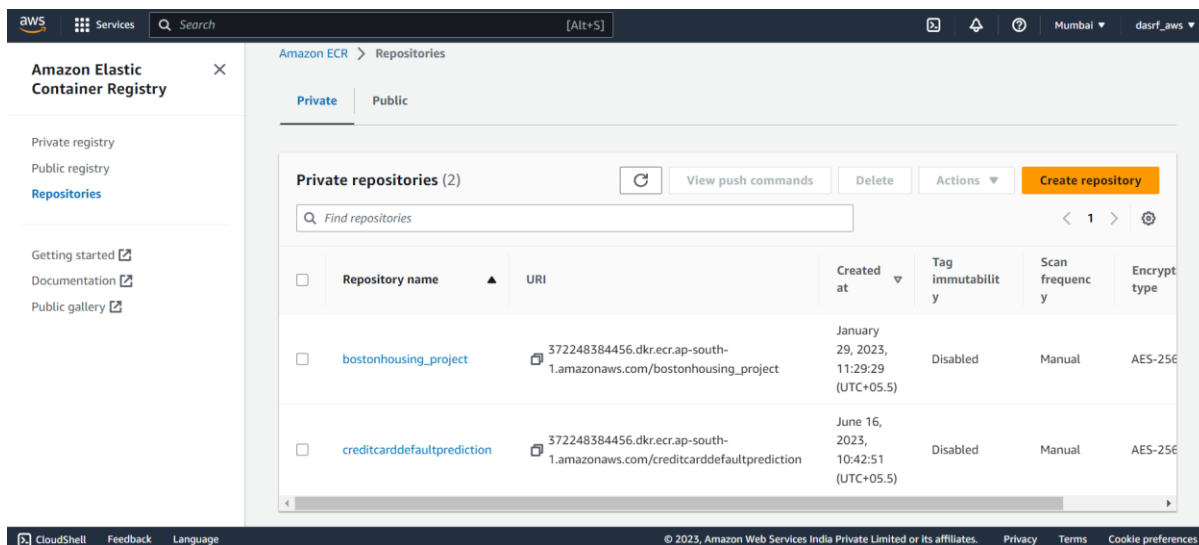
Cancel

Launch instance

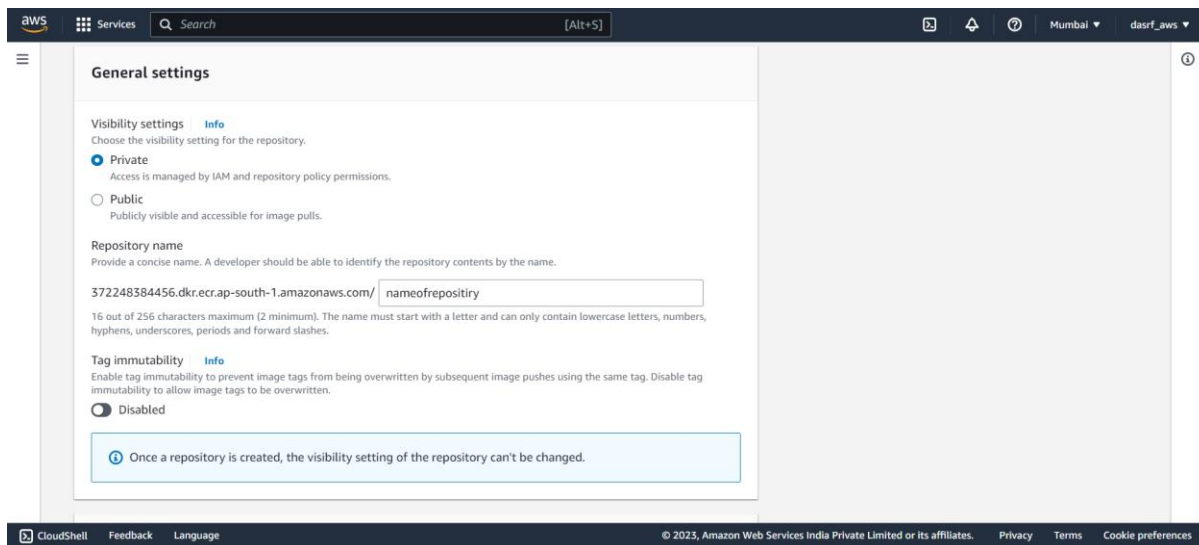
[Review commands](#)

Launch ECR in AWS

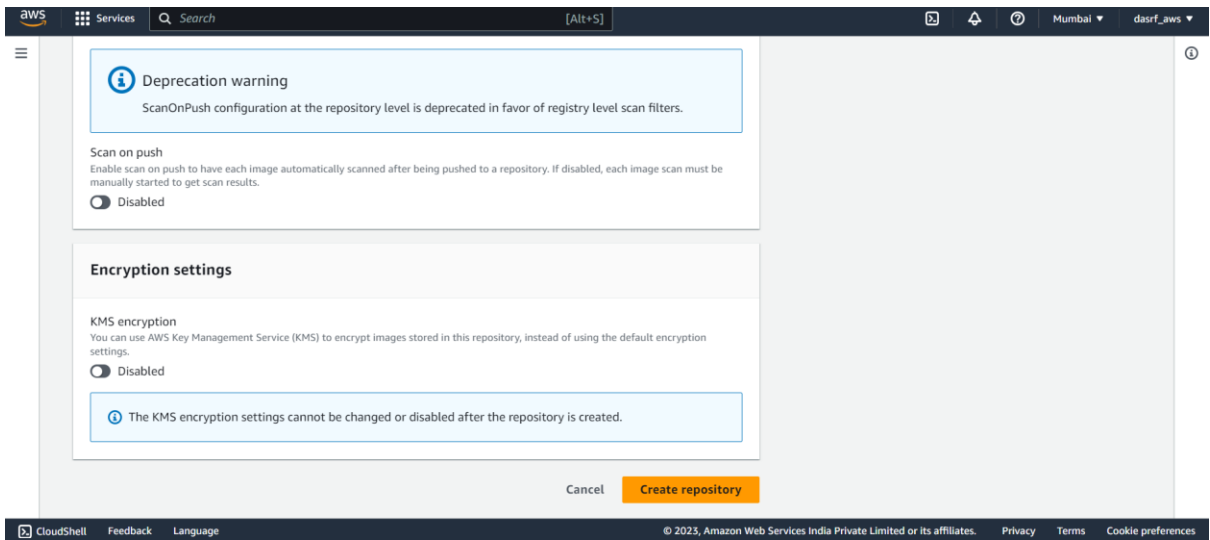
Step1: Create an ECR registry



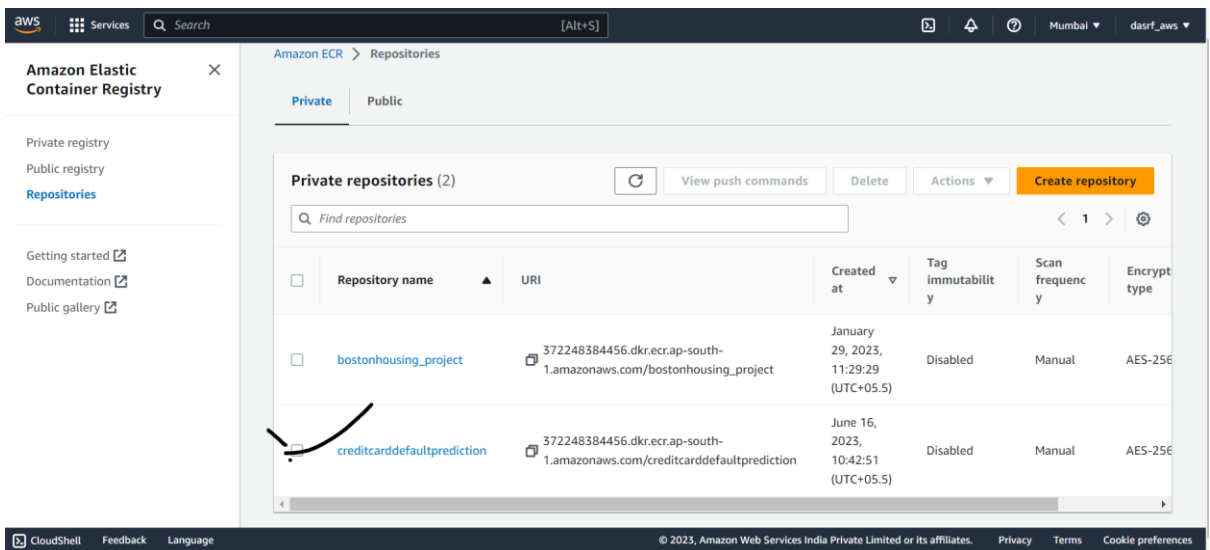
Step2: name of repo



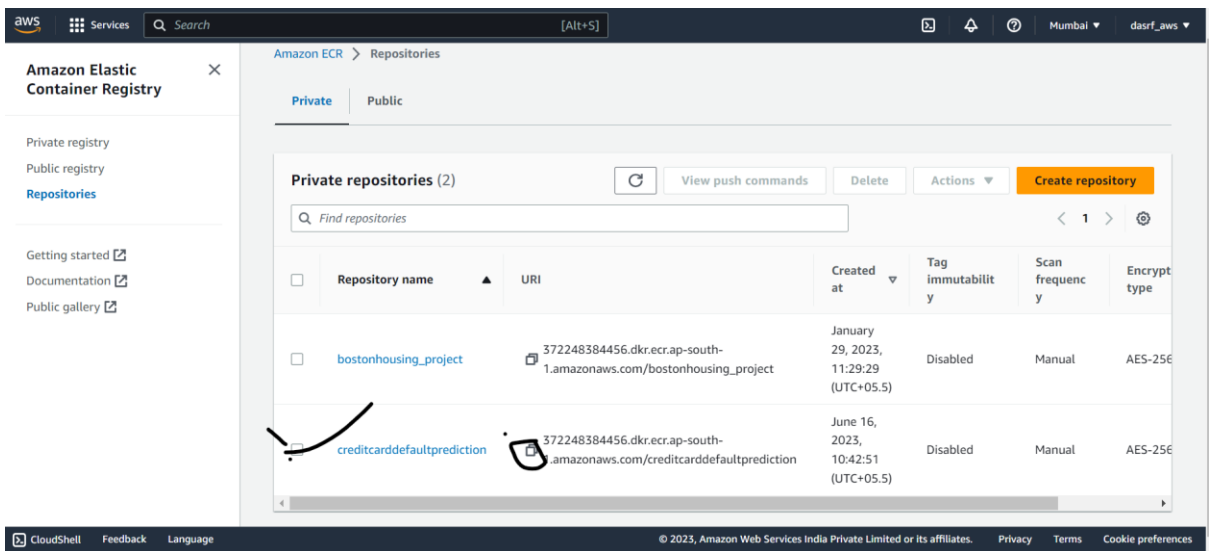
Step 3: create repo



Step4: Your repository created:

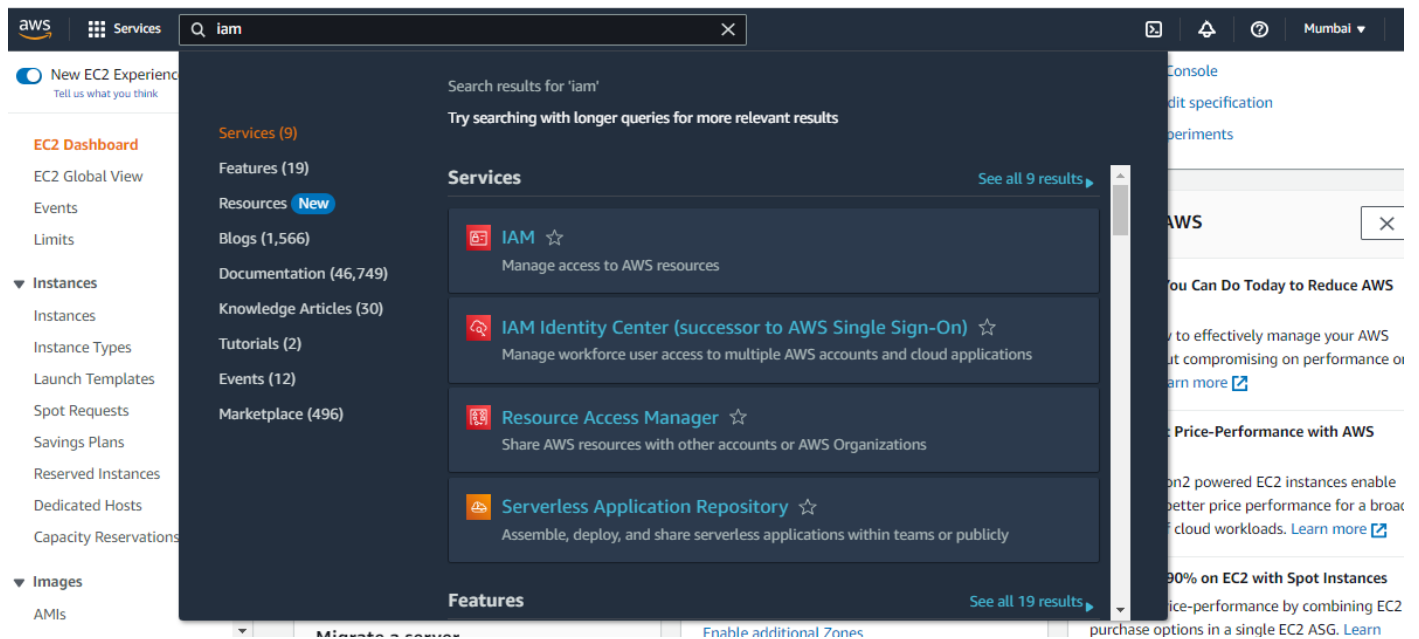


Step5: Copy URL

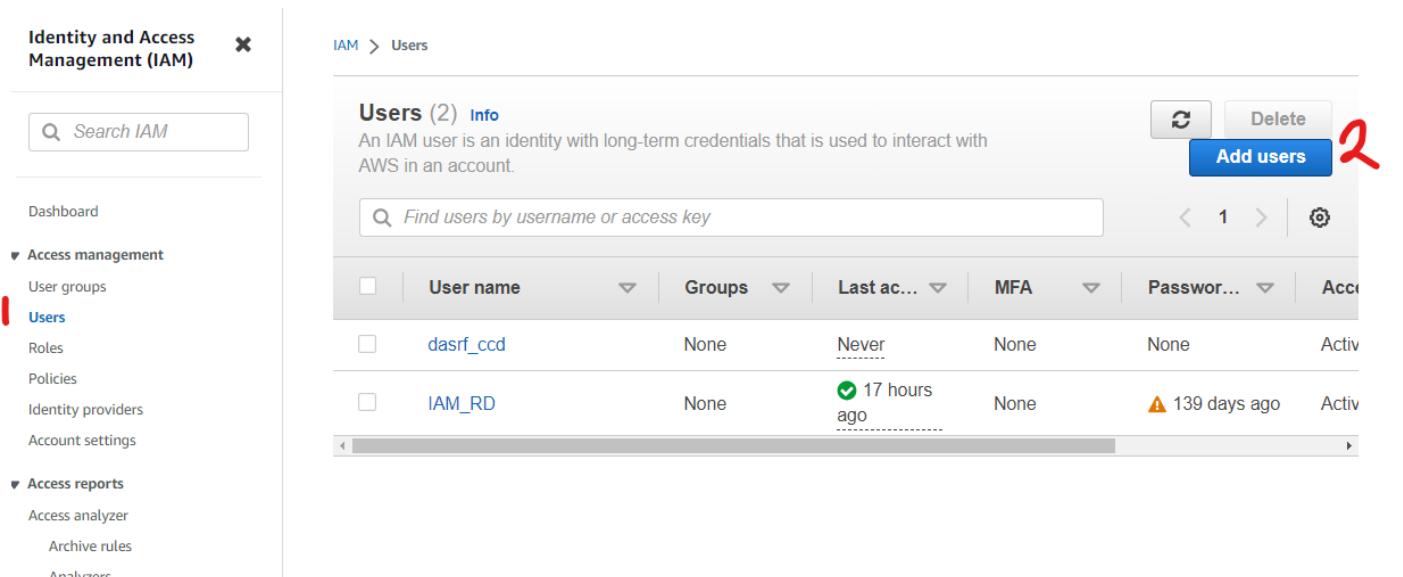


Create IAM role:

Step1: Search for IAM role



Step2: go to Users and Add users



IAM > Users > Create user

Step 1
Specify user details

Step 2
Set permissions

Step 3
Review and create

Specify user details

User details

User name

name of user

The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)

☐ Provide user access to the AWS Management Console - optional
If you're providing console access to a person, it's a [best practice](#) to manage their access in IAM Identity Center.

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

IAM > Users > Create user

Step 1
Specify user details

Step 2
Set permissions

Step 3
Review and create

Set permissions

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. [Learn more](#)

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.

Permissions policies (1102)

Choose one or more policies to attach to your new user.

Create policy

Step3: Attach policy to use ECR container registry and click next

manage user permissions by job function.

an existing user.

attaching policies to a group instead. Then, add the user to the appropriate group.

Permissions policies (Selected 2/1102)

Choose one or more policies to attach to your new user.

Q Search

All types

< 1 2 3 4 5 6 7 ... 56 >

	Policy name	Type	Atta...
<input checked="" type="checkbox"/>	AmazonEC2FullAccess	AWS managed	2
<input checked="" type="checkbox"/>	AmazonEC2ContainerRegistryFullAccess	AWS managed	2
<input type="checkbox"/>	AWSTrustedAdvisorServiceRolePolicy	AWS managed	1
<input type="checkbox"/>	AWSsupportServiceRolePolicy	AWS managed	1
<input type="checkbox"/>	AdministratorAccess	AWS managed - job function	0
<input type="checkbox"/>	PowerUserAccess	AWS managed - job function	0
<input type="checkbox"/>	ReadOnlyAccess	AWS managed - job function	0

Permissions summary

< 1 >

Name	Type	Used as
AmazonEC2ContainerRegistryFullAccess	AWS managed	Permissions policy
AmazonEC2FullAccess	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

Connect EC2 instance :

New EC2 Experience

EC2 Dashboard

EC2 Global View

Events

Limits

Instances

Instances

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts

Capacity Reservations

Images

AMIs

Instances (2) Info

Find instance by attribute or tag (case-sensitive)

	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
<input type="checkbox"/>	ec2_v1	i-03ba35551b7913c5d	Stopped	t2.micro	-	No alarms	ap-south-1a
<input checked="" type="checkbox"/>	creditcarddefa...	i-094b9d9bc7bd70b6e	Running	t2.micro	2/2 checks passed	No alarms	ap-south-1a

Select an instance

CloudShell

Feedback

Language

© 2023, Amazon Web Services India Private Limited or its affiliates.

Privacy

Terms

Cookie preferences

Connect to instance

Info

Connect to your instance i-094b9d9bc7bd70b6e (creditcarddefaultprediction_neuron) using any of these options

EC2 Instance Connect

Session Manager

SSH client

EC2 serial console

Instance ID

i-094b9d9bc7bd70b6e (creditcarddefaultprediction_neuron)

Connection Type

☒ Connect using EC2 Instance Connect

Connect using the EC2 Instance Connect browser-based client, with a public IPv4 address.

☐ Connect using EC2 Instance Connect Endpoint

Connect using the EC2 Instance Connect browser-based client, with a private IPv4 address and a VPC endpoint.

Public IP address

13.233.215.189

User name

Enter the user name defined in the AMI used to launch the instance. If you didn't define a custom user name, use the default user name, ubuntu.

ubuntu

Note:

In most cases, the default user name, ubuntu, is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI user name.

Step1: Docker Setup In EC2 commands to be Executed

#optinal

```
sudo apt-get update -y
```

```
sudo apt-get upgrade
```

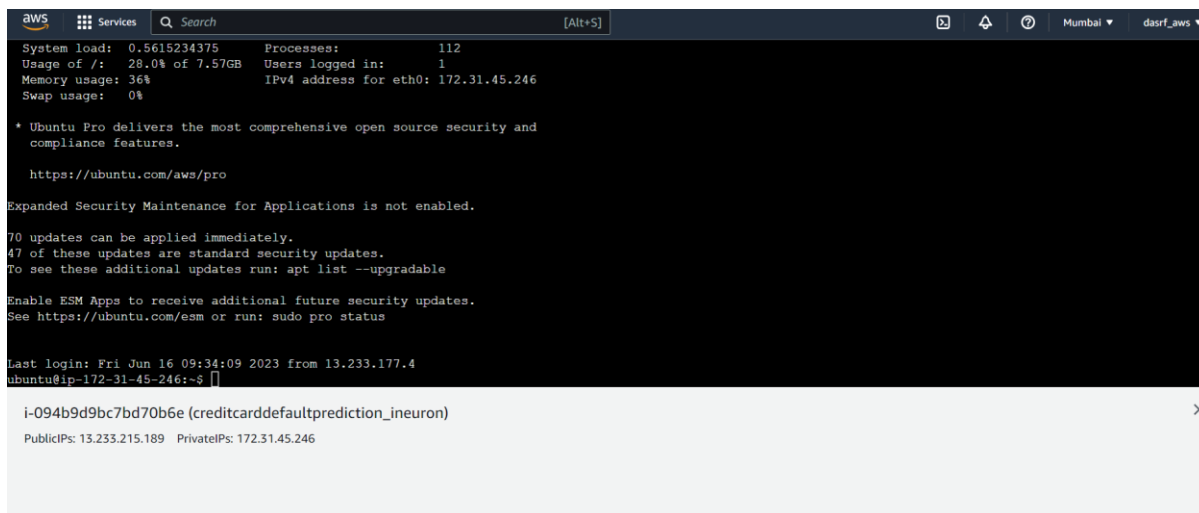
#required

```
curl -fsSL https://get.docker.com -o get-docker.sh
```

```
sudo sh get-docker.sh
```

```
sudo usermod -aG docker ubuntu
```

```
newgrp docker
```



The screenshot shows an AWS EC2 terminal window with the following content:

```
aws Services Search [Alt+S] Mumbai dasrf_aws
System load: 0.5615234375 Processes: 112
Usage of /: 28.0% of 7.57GB Users logged in: 1
Memory usage: 36% IPv4 address for eth0: 172.31.45.246
Swap usage: 0%

* Ubuntu Pro delivers the most comprehensive open source security and
  compliance features.
  https://ubuntu.com/aws/pro

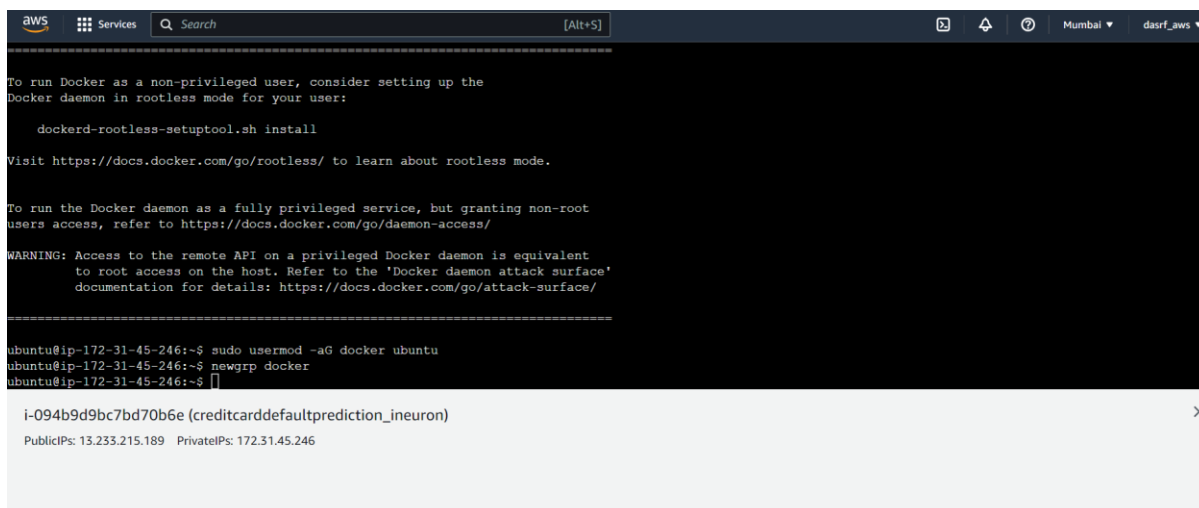
Expanded Security Maintenance for Applications is not enabled.

70 updates can be applied immediately.
47 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Last login: Fri Jun 16 09:34:09 2023 from 13.233.177.4
ubuntu@ip-172-31-45-246:~$
```

Below the terminal window, a metadata box displays the instance ID: i-094b9d9bc7bd70b6e (creditcarddefaultprediction_ineuron) and IP addresses: PublicIPs: 13.233.215.189 PrivateIPs: 172.31.45.246.



The screenshot shows an AWS EC2 terminal window with the following content:

```
aws Services Search [Alt+S] Mumbai dasrf_aws

=====
To run Docker as a non-privileged user, consider setting up the
Docker daemon in rootless mode for your user:

  dockerd-rootless-setuptool.sh install

Visit https://docs.docker.com/go/rootless/ to learn about rootless mode.

To run the Docker daemon as a fully privileged service, but granting non-root
users access, refer to https://docs.docker.com/go/daemon-access/

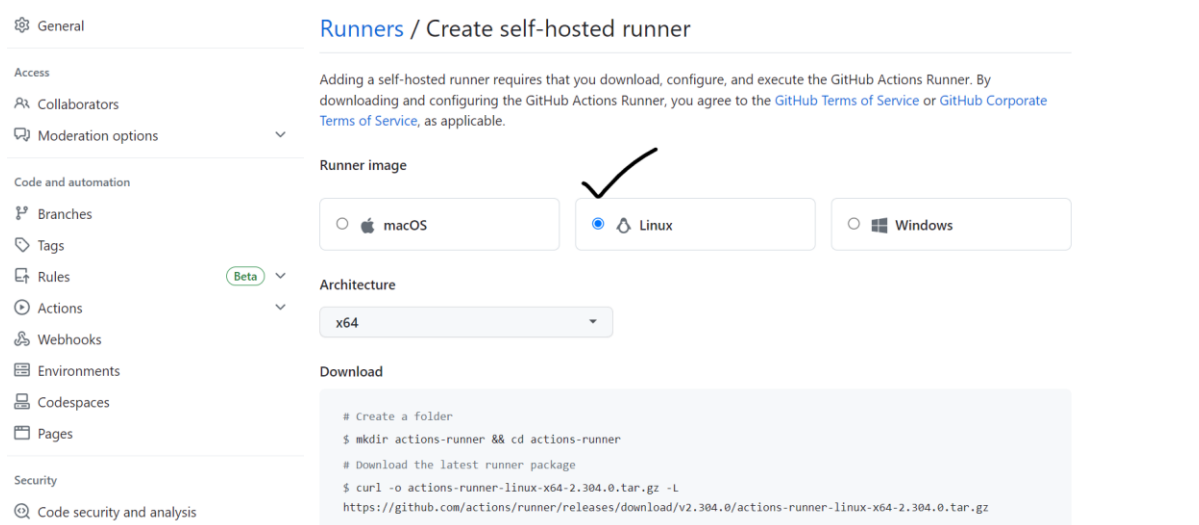
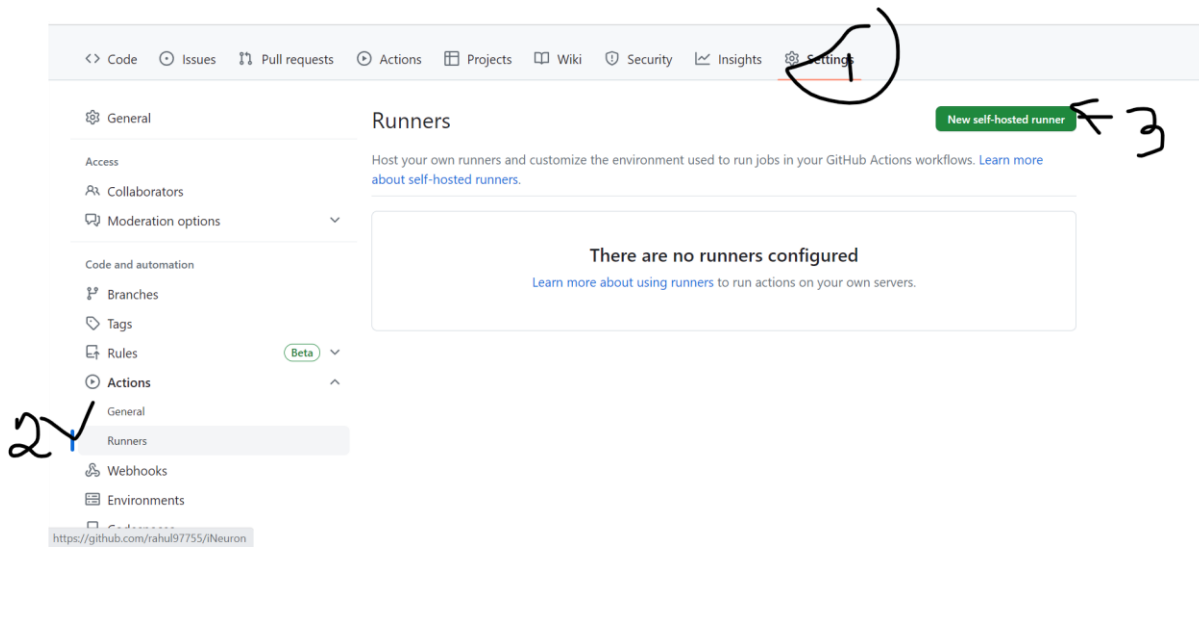
WARNING: Access to the remote API on a privileged Docker daemon is equivalent
to root access on the host. Refer to the 'Docker daemon attack surface'
documentation for details: https://docs.docker.com/go/attack-surface/

=====

ubuntu@ip-172-31-45-246:~$ sudo usermod -aG docker ubuntu
ubuntu@ip-172-31-45-246:~$ newgrp docker
ubuntu@ip-172-31-45-246:~$
```

Below the terminal window, a metadata box displays the instance ID: i-094b9d9bc7bd70b6e (creditcarddefaultprediction_ineuron) and IP addresses: PublicIPs: 13.233.215.189 PrivateIPs: 172.31.45.246.

Step2: Setup github action runner to listing the docker command and



Run all commands just right after the docker setup commands

Note: Do not skip any commands otherwise flow will be interrupted



```
aws Services Search [Alt+S]
Enter any additional labels (ex. label-1,label-2): [press Enter to skip]
✓ Runner successfully added
✓ Runner connection is good
# Runner settings
Enter name of work folder: [press Enter for _work] ./run.sh
✓ Settings Saved.
ubuntu@ip-172-31-45-246:~/actions-runner$ runs-on: self-hosted
runs-on:: command not found
ubuntu@ip-172-31-45-246:~/actions-runner$ runs-on: self-hosted
runs-on:: command not found
ubuntu@ip-172-31-45-246:~/actions-runner$ ./run.sh
✓ Connected to GitHub
Current runner version: '2.304.0'
2023-06-16 10:09:13Z: Listening for Jobs

i-094b9d9bc7bd70b6e (creditcarddefaultprediction_in neuron)
PublicIPs: 13.233.215.189 PrivateIPs: 172.31.45.246
```

Go to runner under

The image shows two screenshots from a GitHub interface. The top screenshot displays the 'General' settings for a repository named 'iNeuron'. In the left sidebar, under 'Code and automation', the 'Runners' link is highlighted with a handwritten 'Click' and an arrow. The main content area shows settings for repository name, template repository, and default branch. The bottom screenshot shows the 'Runners' page for the same repository. It features a 'New self-hosted runner' button and a table with one runner listed as 'self-hosted' with a status of 'Idle'. A handwritten checkmark is placed next to the 'Idle' status.

← workflow

✅ **yaml file changed #2**

Re-run all jobs



Summary

Jobs

- ✅ Continuous Integration
- ✅ Continuous Delivery
- ✅ Continuous-Deployment

Run details

- Usage
- Workflow file

Triggered via push 4 minutes ago
Status: **Success** Total duration: **4m 1s** Artifacts: —
👤 rahul97755 pushed → d144f6 **main**

main.yml
on: push



Annotations

- Codespaces
- Pages
- Security
 - Code security and analysis
 - Deploy keys
 - Secrets and variables**
- Actions**
- Codespaces
- Dependabot
- Integrations
 - GitHub Apps
 - Email notifications



Repository secrets

There are no secrets for this repository.

Runners

- Webhooks
- Environments
- Codespaces
- Pages

Security

- Code security and analysis
- Deploy keys
- Secrets and variables**
- Actions**
- Codespaces
- Dependabot

Integrations

- GitHub Apps
- Email notifications

Code and automation










workflows that are triggered by a pull request from a fork.

Secrets Variables [New repository secret](#)

Environment secrets [Manage environments](#)

There are no secrets for this repository's environments.

Repository secrets

 AWS_ACCESS_KEY_ID	Updated 20 hours ago	 
 AWS_ECR_LOGIN_URI	Updated 20 hours ago	 
 AWS_REGION	Updated 20 hours ago	 

Setup github secrets:

AWS_ACCESS_KEY_ID=

AWS_SECRET_ACCESS_KEY=

AWS_REGION = us-east-1

AWS_ECR_LOGIN_URI = demo>> 53434343545.dkr.ecr.ap-south-1.amazonaws.com

ECR_REPOSITORY_NAME = simple-app