CLOUD APPLICATION JOURNAL

By Jayesh Dubey

Thakur Educational Trust's (Regd.)
THAKUR COLLEGE OF SCIENCE & COMMERCE
Empowered Autonomous College Permanently Affiliated to University of Mumbai
(NAAC Accredited with Grade "A" (3rd Cycle) & ISO 21001:2018 Certified)
Best College Award by University of Mumbai for the Year 2018-2019

CERTIFICATE

This certifies that **Jayesh Dubey**, Seat Number **4518**, an M.Sc. Part II student in Computer Science, successfully completed all required experiments of the **CC Practicals** as prescribed by the University of Mumbai during the 2025–2026 academic year.

Teacher In-Charge

Head of Department

Date:

Place: Mumbai

Index

Name: Jayesh Dubey
Class: MSc CS - II
Roll no: 4518
Course: CC Practicals

No	Objective	Date	Signature
1	Installing Foss-Cloud in Oracle Vm Virtualbox Manager		
2	Create an IAM User Account in Amazon Web Services (AWS)		
3	Create EC2 Instance and Use it to Host a Website		
4	Store file in S3 Buckets and access it		
5	To Create BACKUP of running amazon Instance by creating an AMIs and launching new instances from the created AMIs		
6	To monitor an EC2 instance using Amazon CloudWatch and create an alarm based on CPU utilization		

PRACTICAL NO. 1

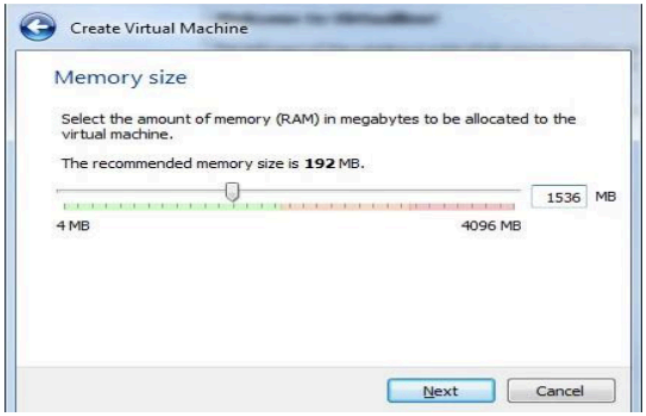
AIM : Installing Foss-Cloud in Oracle Vm Virtualbox Manager

Step 1: Download and Install Foss Cloud
https://sourceforge.net/projects/foss-cloud/

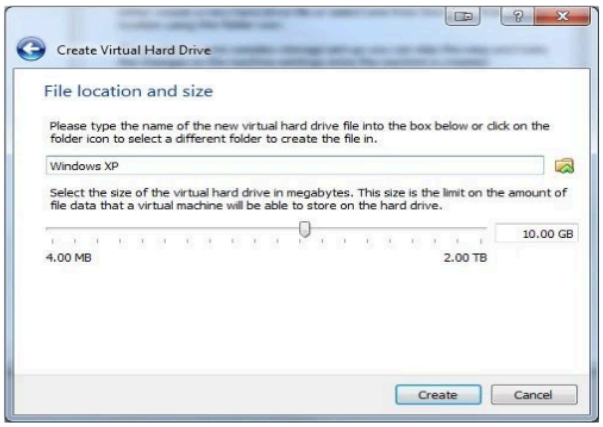
Step 2 : Open Oracle Vm Virtualbox Manager and Create a Virtual Machine

Allocate Memory

Setup the Hard Drive

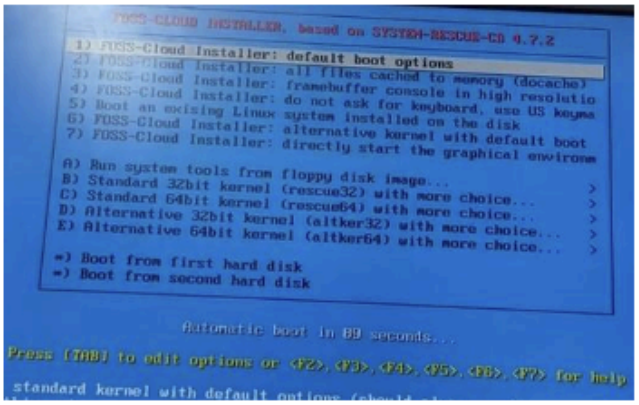


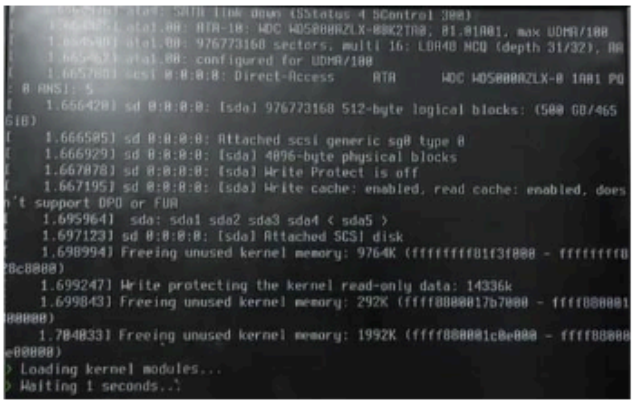
Setup Physical Hard Drive



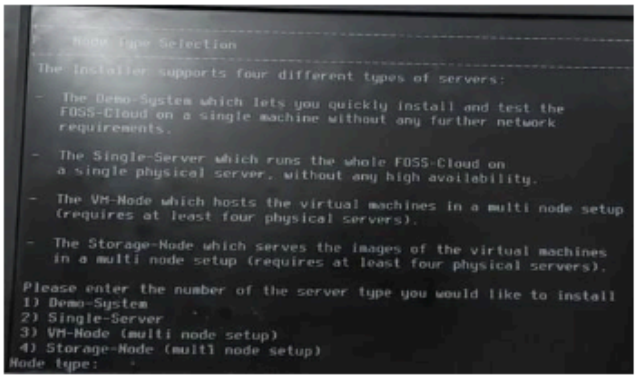
Setup File Location and

Step 3 : Import the Cloud Foss Iso file
Step 4 : Choose a single server installation in the first window.

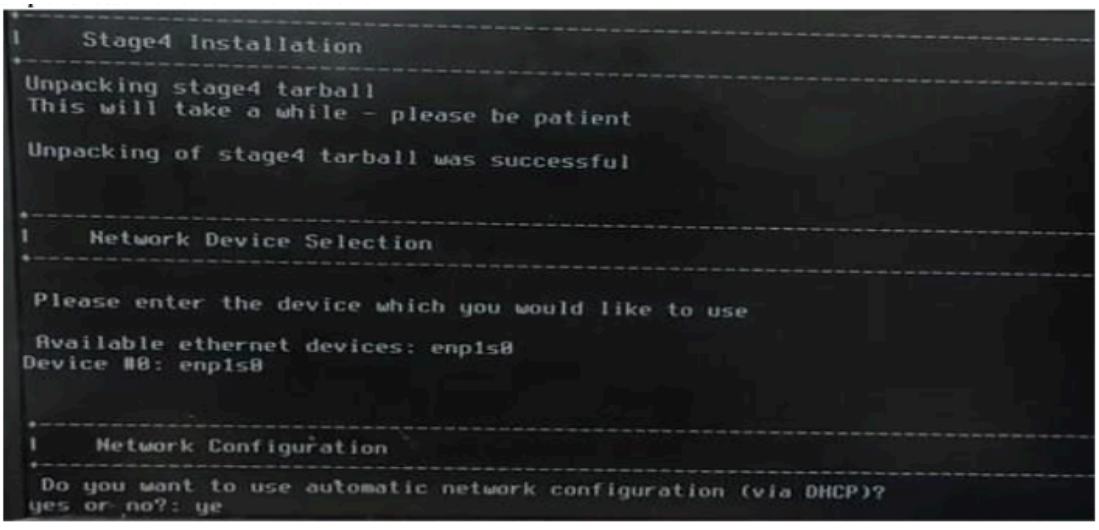




Step 5 : Start the installation By Typing ‘Yes’.

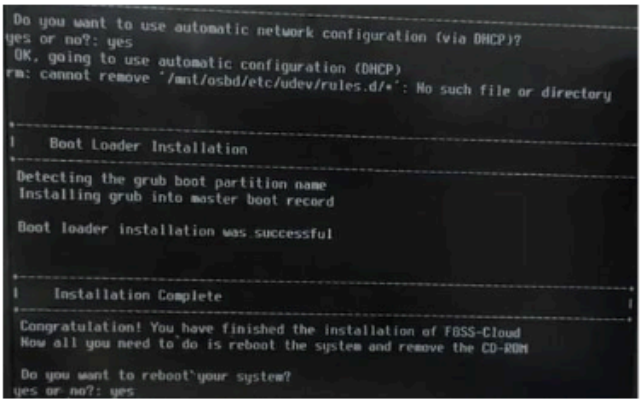


Step 6 : Choose the network interface: eth0

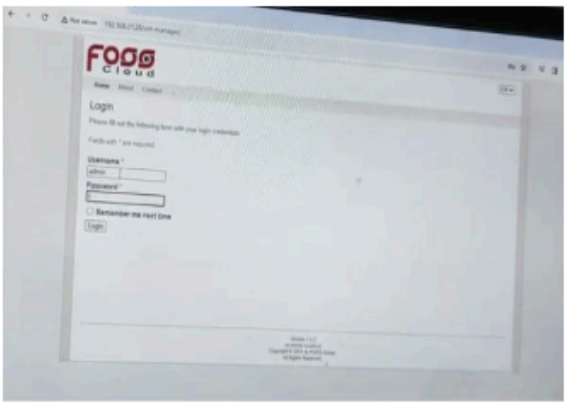


Step 7 : Choose domain name: e.g. foss-cloud.org and a free static IP address in your home network, for instance: 192.168.1.100
Step 8 : Choose the broadcast IP address, gateway and DNS resolver.

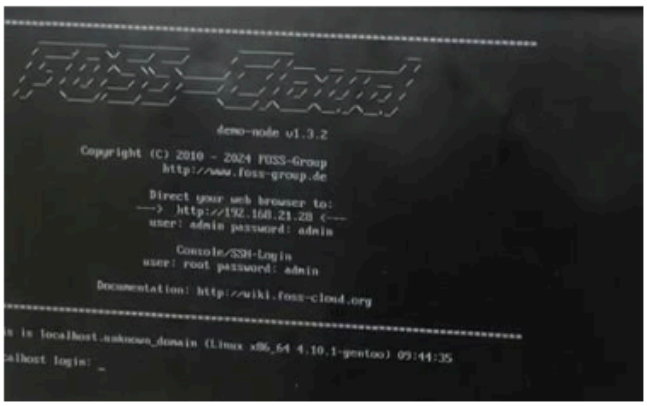
Step 9 : Confirm all entries, and once installed reboot your system.



Step 12 : Open IP Address in Browser and login.



Step 10 : Restart your system.



Step 13 : Welcome Page of Foss Cloud.

Step 11 : Check Up Address using ‘ipconfig’..

CONCLUSION : I have Successfully Completed installation of Foss Cloud in Oracle Vm Virtualbox Manager.

PRACTICAL NO. 2

AIM : Create IAM User Account in Amazon Web Services (AWS).

THEORY : What is IAM?
IAM (Identity and Access Management) is an AWS service that allows you to:

- Create **users**
- Assign **permissions**
- Control **who can access what** in AWS Why NOT use a Root Account?
- Root account has **full access**
- If credentials are leaked → **huge risk**
- Best practice:

Create IAM User (AWS Console)
Step 1: Login to AWS Console

- Go to: **https://aws.amazon.com/**
- Login using **Root Account**

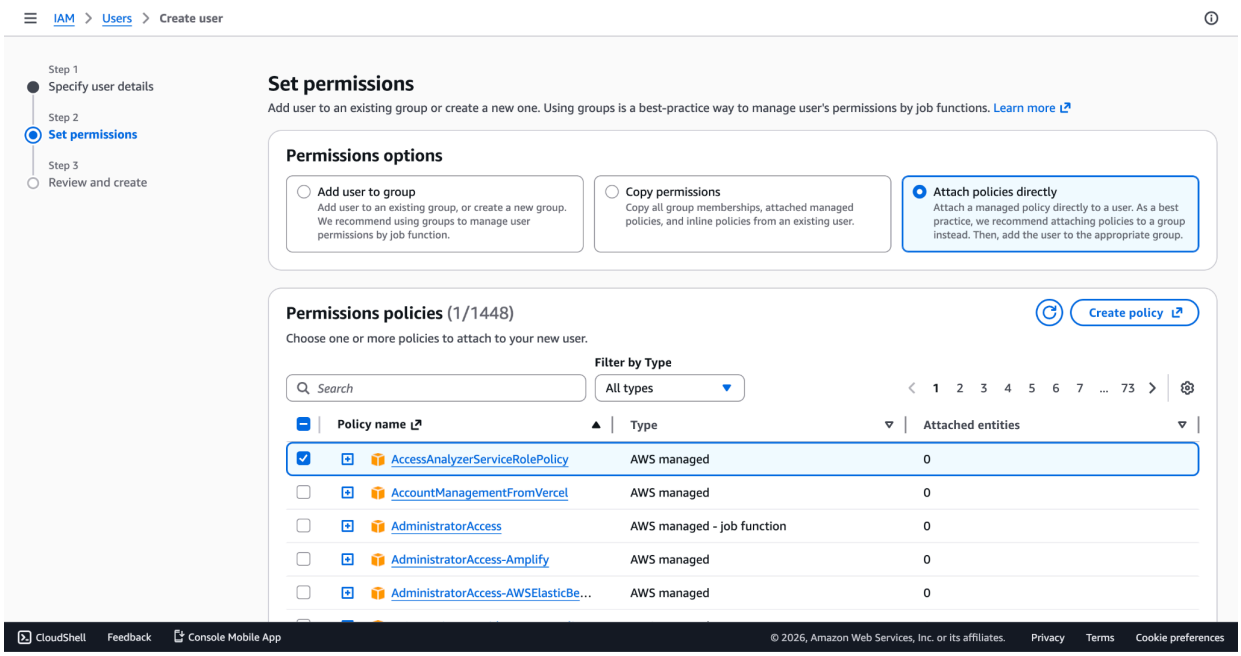
Step 2: Open IAM Service

- Search **IAM**
- Click **IAM → Users → Create user**

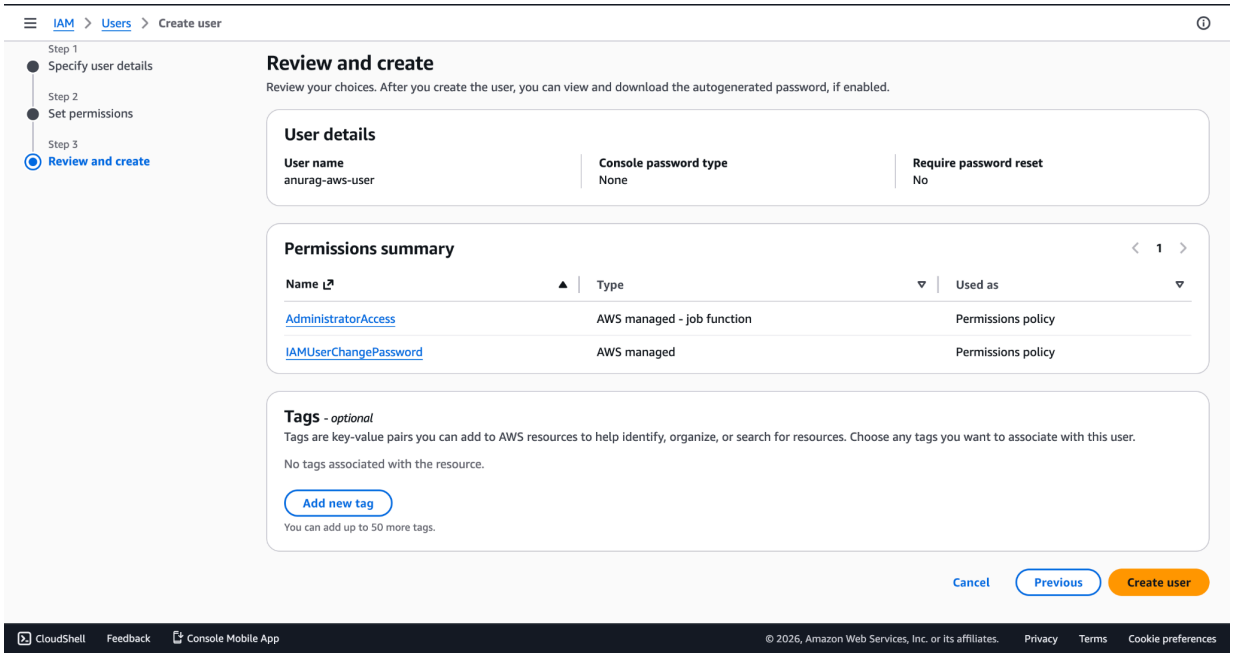
Step 3: User Details

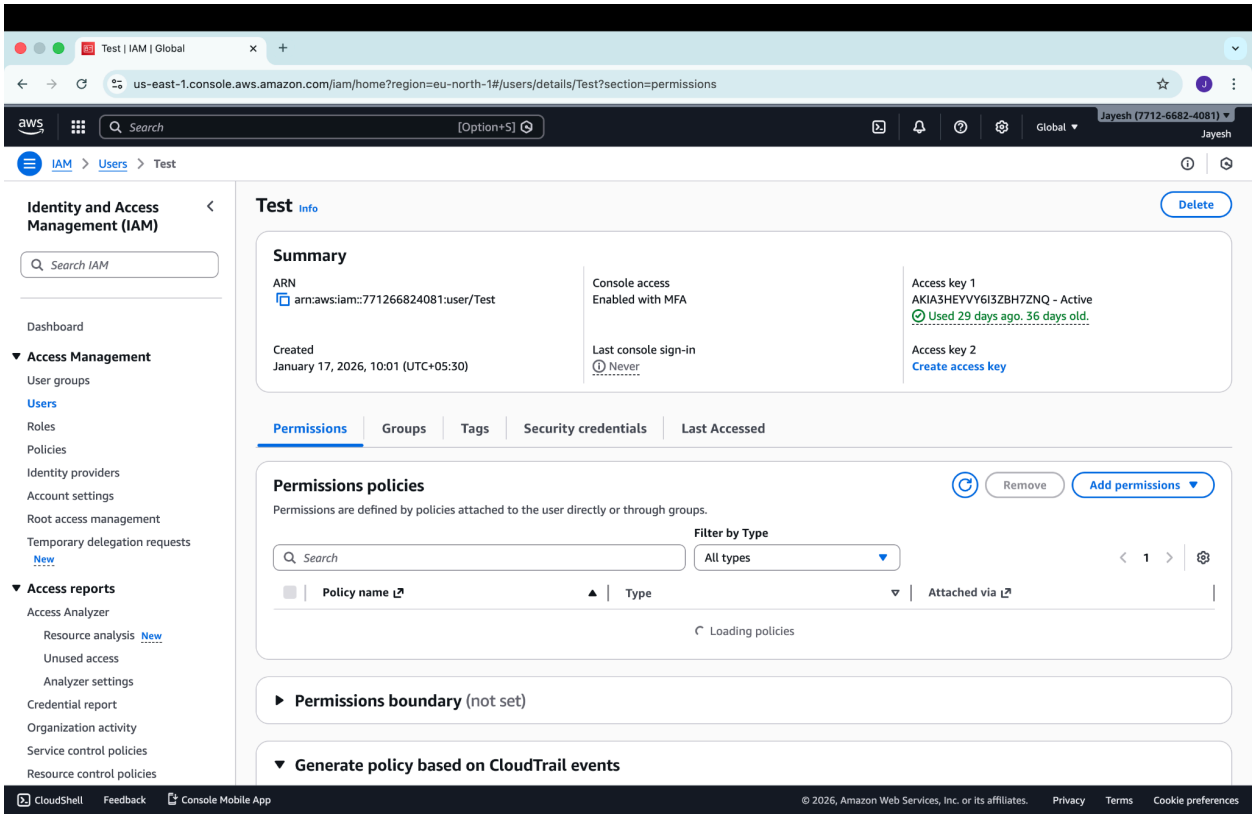
- **User name:** Jayesh-aws-user
- Click **Next**

Step 4: Set Permissions



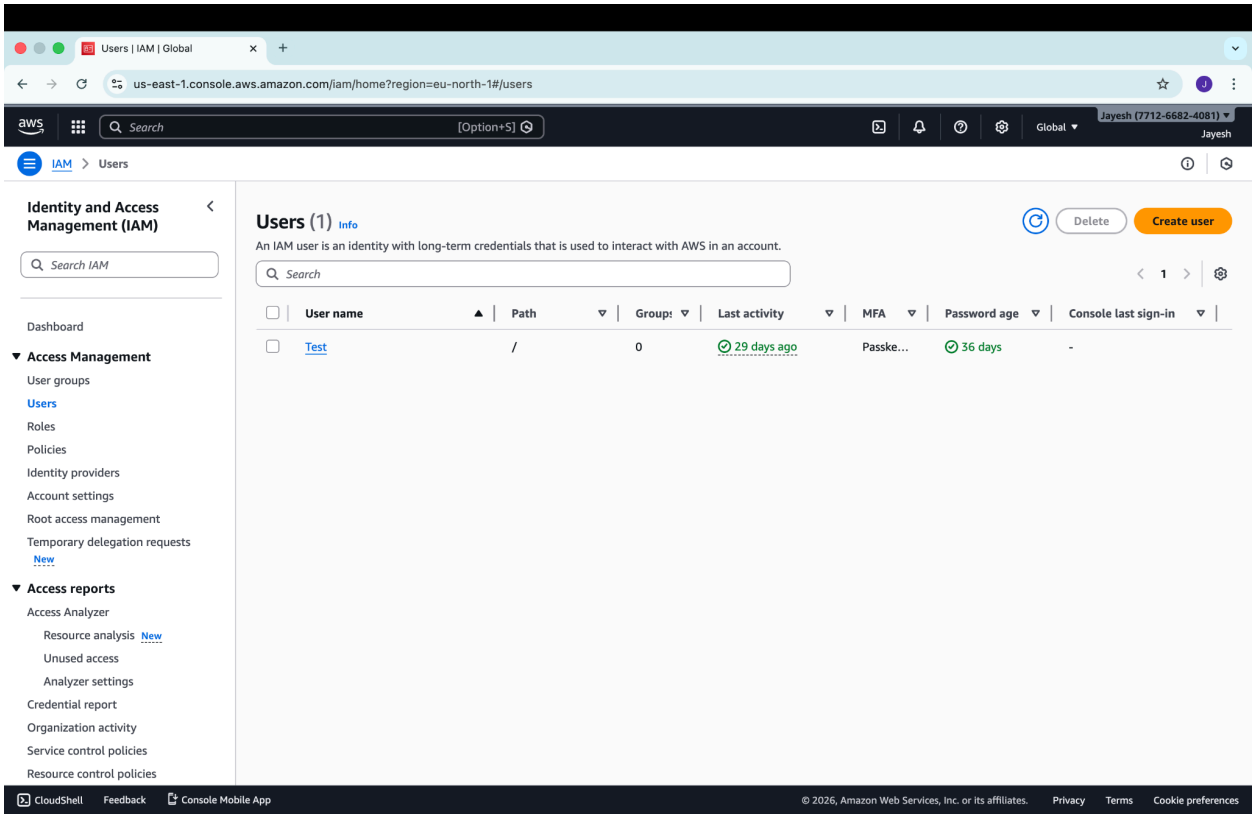
Select **Attach policies directly**
Click **Next → Create user**





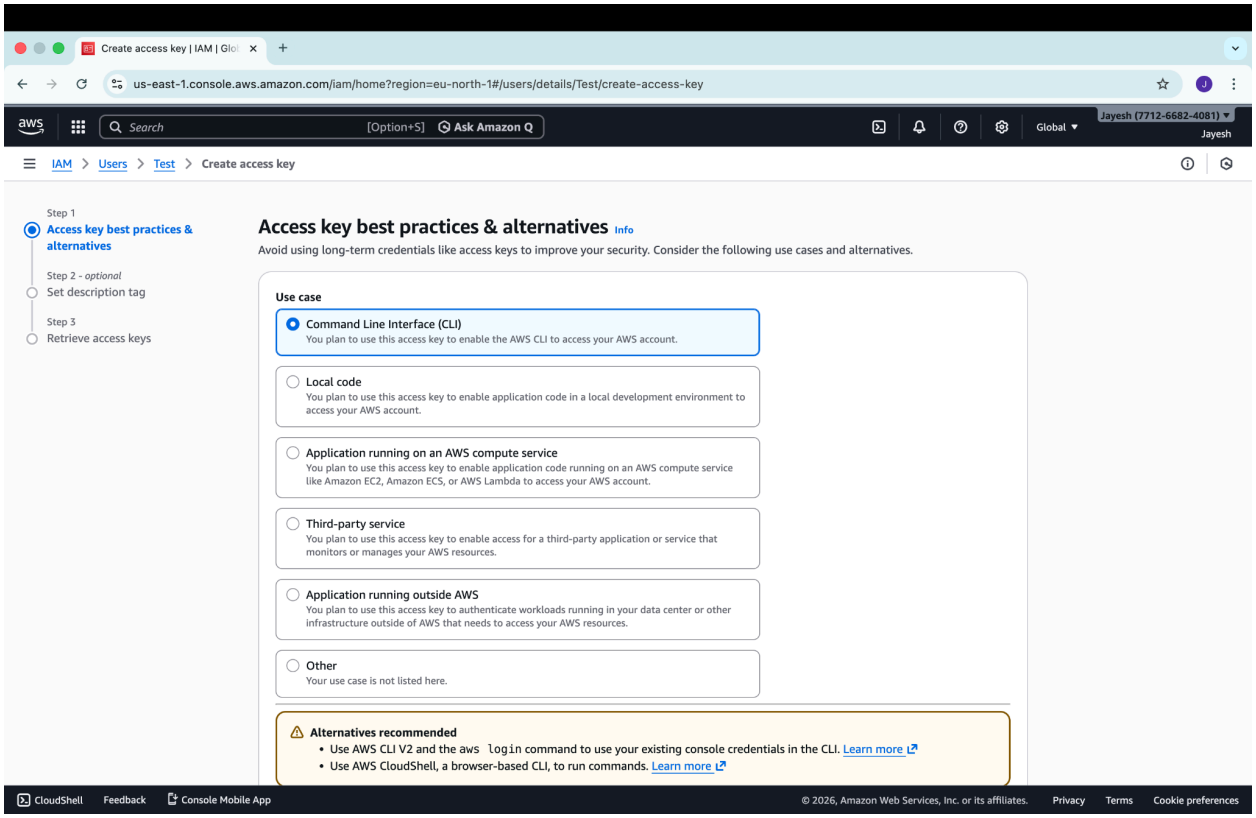
Generate Access Key :

Step 1: Go to **IAM → Users →** Jayesh-aws-user

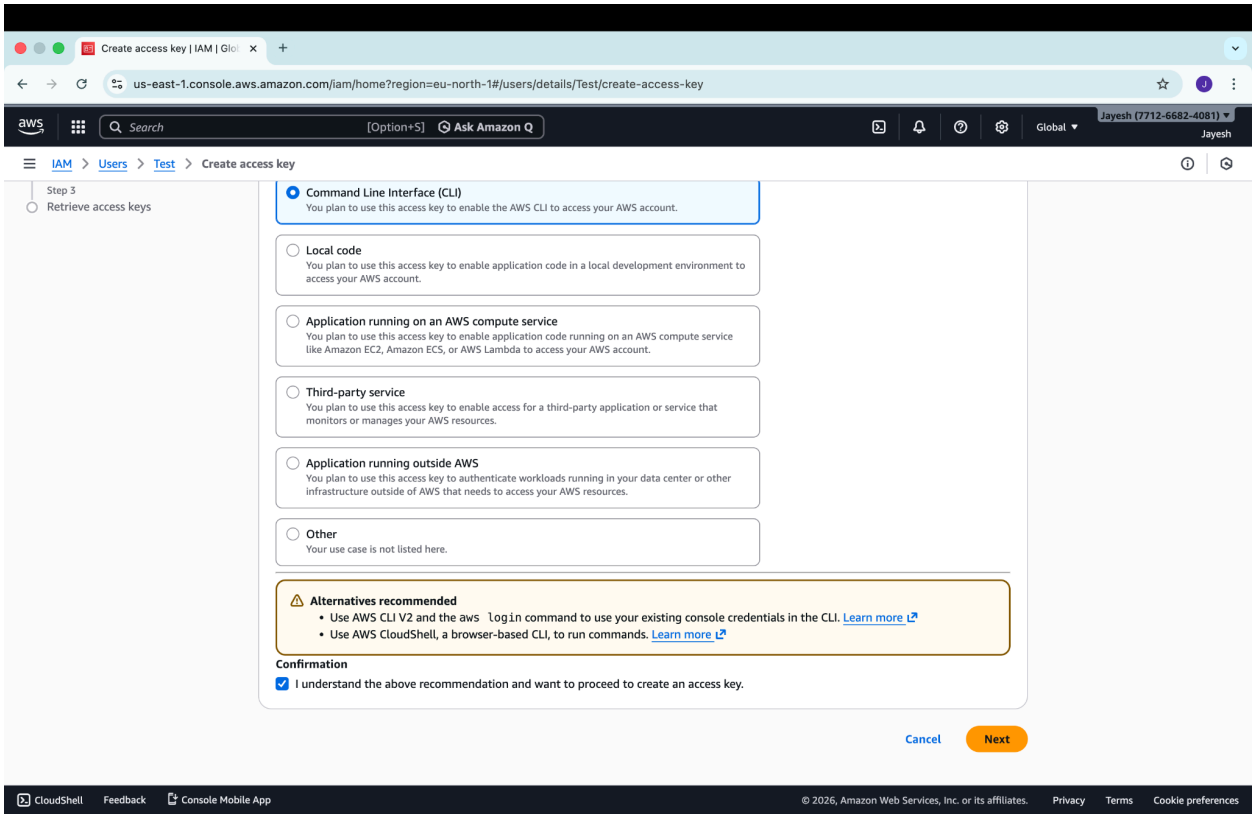


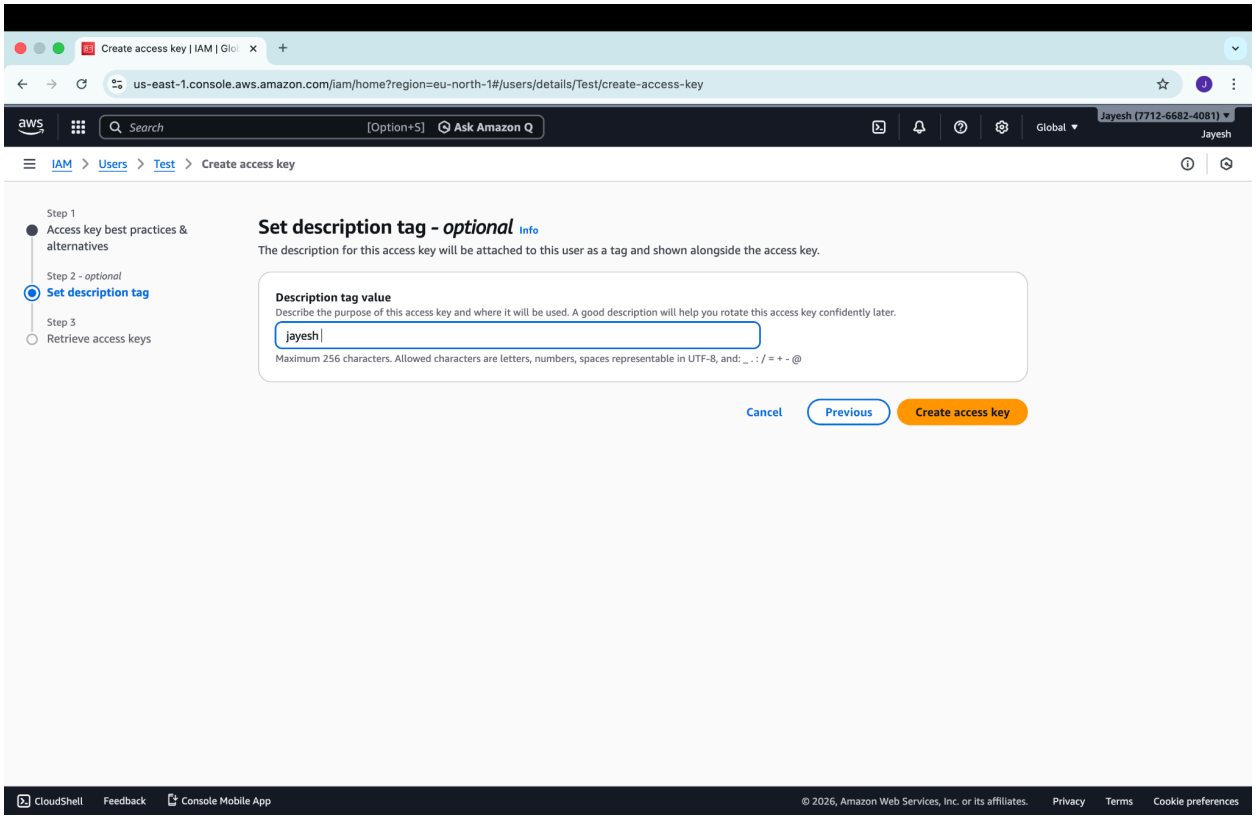
Step 2: Scroll → **Access keys ,** click **Create access key**

Step 3: Choose **Command Line Interface (CLI)**

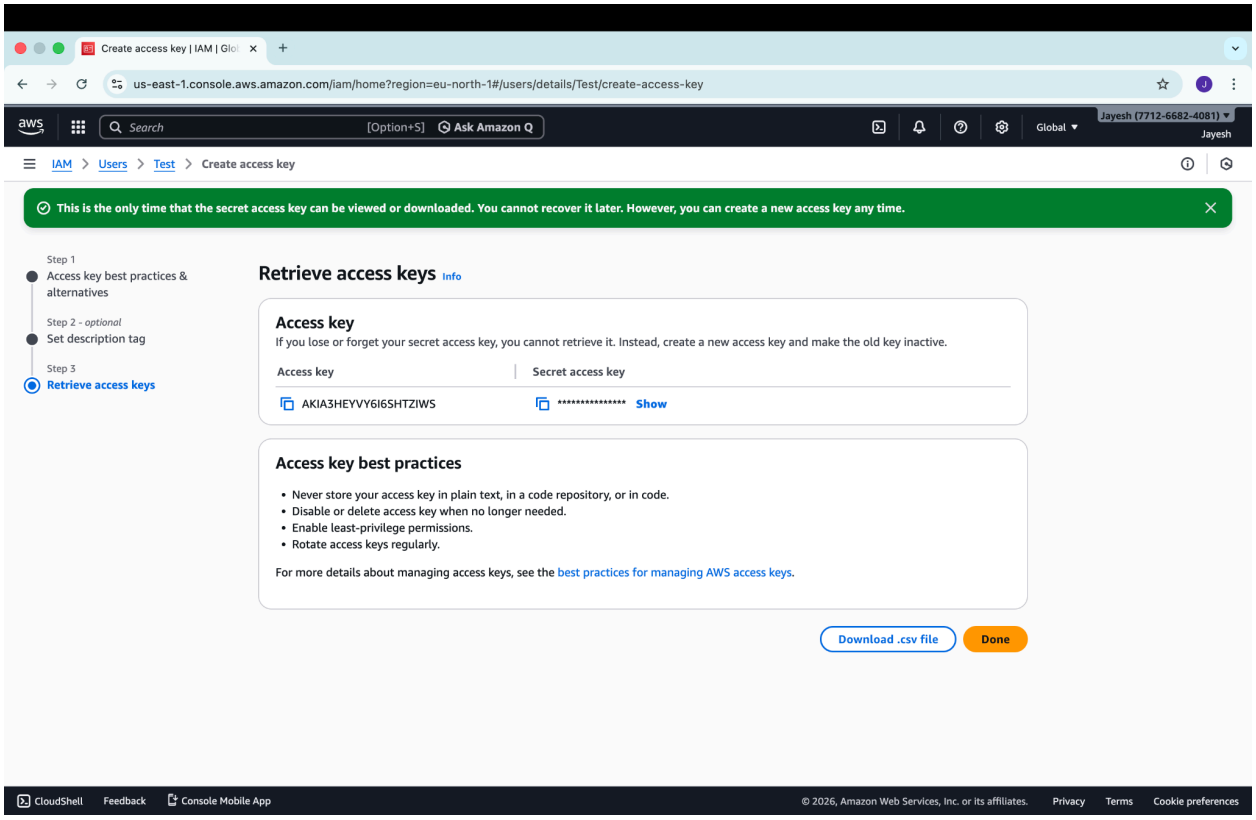


Tick confirmation → **Next**


Create access key | IAM | Glo
us-east-1.console.aws.amazon.com/iam/home?region=eu-north-1#/users/details/Test/create-access-key
Search
[Option+S]
Ask Amazon Q
Global
Jayesh (7712-6682-4081)
Jayesh
IAM > Users > Test > Create access key
Step 3
Retrieve access keys
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.
Application running on an AWS compute service
You plan to use this access key to enable application code running on an AWS compute service like Amazon EC2, Amazon ECS, or AWS Lambda to access your AWS account.
Third-party service
You plan to use this access key to enable access for a third-party application or service that monitors or manages your AWS resources.
Application running outside AWS
You plan to use this access key to authenticate workloads running in your data center or other infrastructure outside of AWS that needs to access your AWS resources.
Other
Your use case is not listed here.
Alternatives recommended
• Use AWS CLI V2 and the aws login command to use your existing console credentials in the CLI. Learn more
• Use AWS CloudShell, a browser-based CLI, to run commands. Learn more
Confirmation
I understand the above recommendation and want to proceed to create an access key.
Cancel
Next
CloudShell
Feedback
Console Mobile App
© 2026, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Create access key | IAM | Glo
us-east-1.console.aws.amazon.com/iam/home?region=eu-north-1#/users/details/Test/create-access-key
Search
[Option+S]
Ask Amazon Q
Global
Jayesh (7712-6682-4081)
Jayesh
IAM > Users > Test > Create access key
Step 1
Access key best practices & alternatives
Step 2 - optional
Set description tag
Step 3
Retrieve access keys
Set description tag - optional
Info
The description for this access key will be attached to this user as a tag and shown alongside the access key.
Description tag value
Describe the purpose of this access key and where it will be used. A good description will help you rotate this access key confidently later.
jayesh
Maximum 256 characters. Allowed characters are letters, numbers, spaces representable in UTF-8, and: _ . : / = + - @
Cancel
Previous
Create access key
CloudShell
Feedback
Console Mobile App
© 2026, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Step 4: Click **Create access key**



Download CSV file

Install AWS CLI:

Download: https://awscli.amazonaws.com/AWSCLIV2.msi, https://awscli.amazonaws.com/AWSCLIV2.pkg ,sudo installer -pkg AWSCLIV2.pkg -target /

Install normally -> Open **Command Prompt - >** Verify: aws –version

```
anurag@MacBook-Air:~$ sudo ./aws/install
You can now run: /usr/local/bin/aws --version
anurag@MacBook-Air:~$ aws --version
aws-cli/2.33.23 Python/3.13.11 Linux/6.8.0-100-generic exe/x86_64.ubuntu.24
anurag@MacBook-Air:~$ aws configure
AWS Access Key ID [None]: AKIAWI4DP6A5ZBBTN6WK
AWS Secret Access Key [None]: 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
Default region name [None]: ap-south-1
Default output format [None]: json
anurag@MacBook-Air:~$ aws sts get-caller-identity
{
    "UserId": "AIDAWI4DP6A52ONZCRZUD",
    "Account": "431383113787",
    "Arn": "arn:aws:iam::431383113787:user/anurag-aws-user"
}
```

Configure AWS CLI (Login)

Enter details:

Test AWS CLI Login:

```
{
    "Users": [
        {
            "Path": "/",
            "UserName": "anurag-aws-user",
            "UserId": "AIDAWI4DP6A52ONZCRZUD",
            "Arn": "arn:aws:iam::431383113787:user/anurag-aws-user",
            "CreateDate": "2026-02-17T19:28:35+00:00"
        }
    ]
}
anurag@MacBook-Air:~$
```

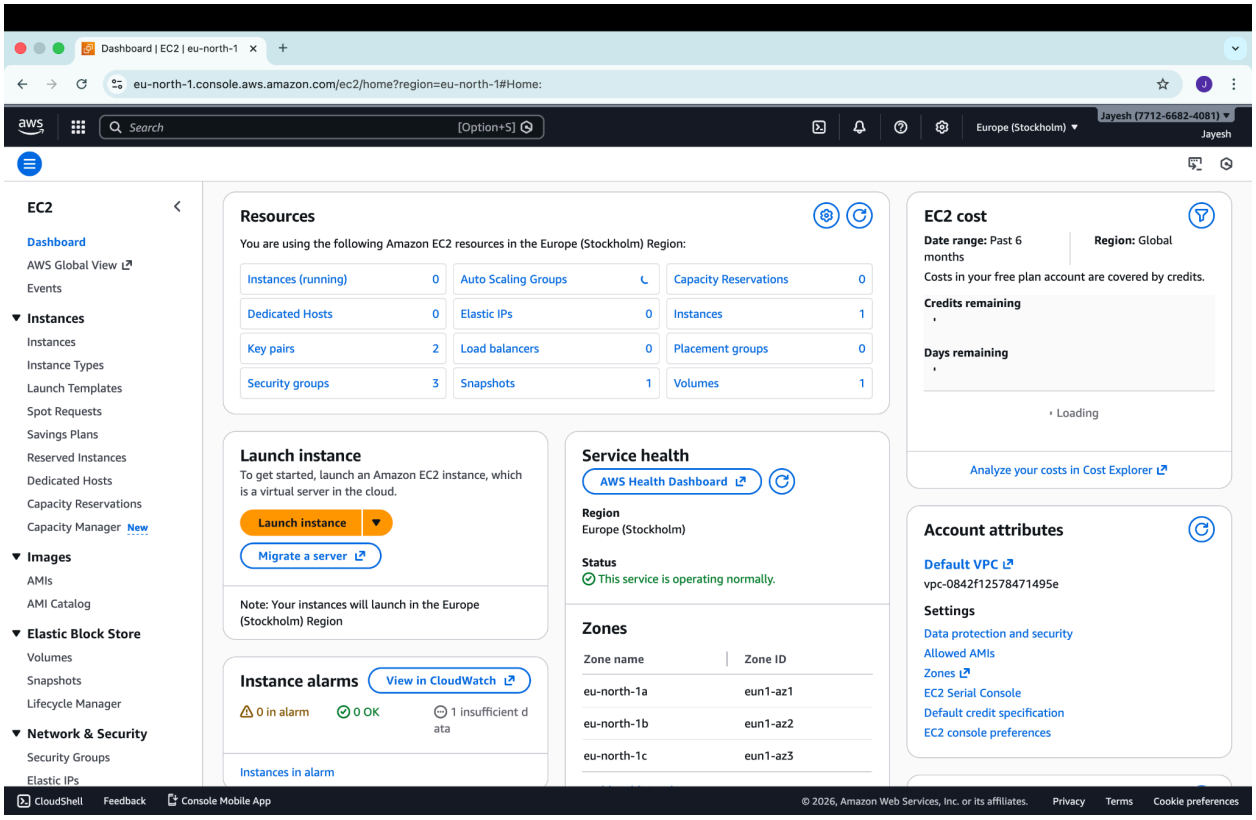
CONCLUSION : I have successfully created the Iam User Account in AWS providing necessary permission and tested it locally .

PRACTICAL NO. 3

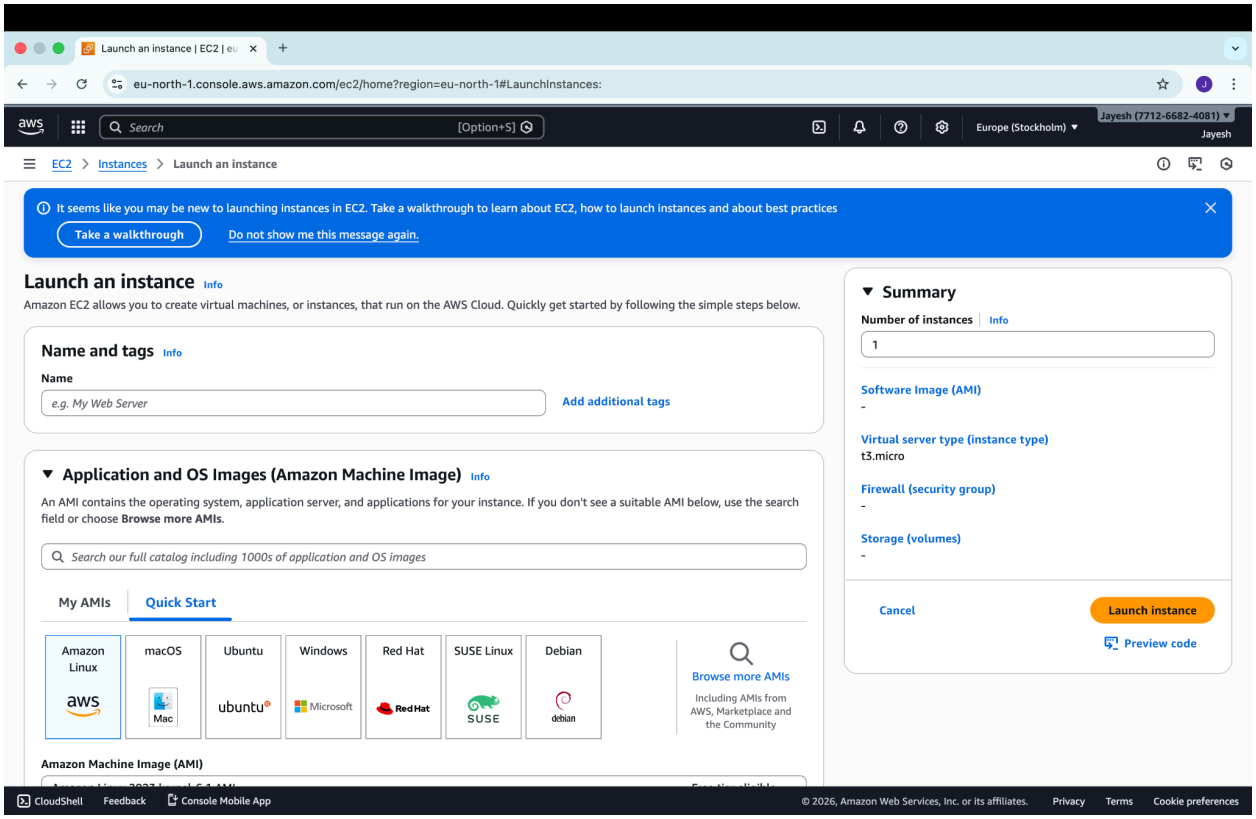
Aim : Create EC2 Instance and Use it to Host a Website.

STEP 1: Create EC2 Linux Instance

1. Login to AWS Console
    - Open 👉 https://aws.amazon.com
    - Sign in → **AWS Management Console**
1. Open EC2
    - Search **EC2**

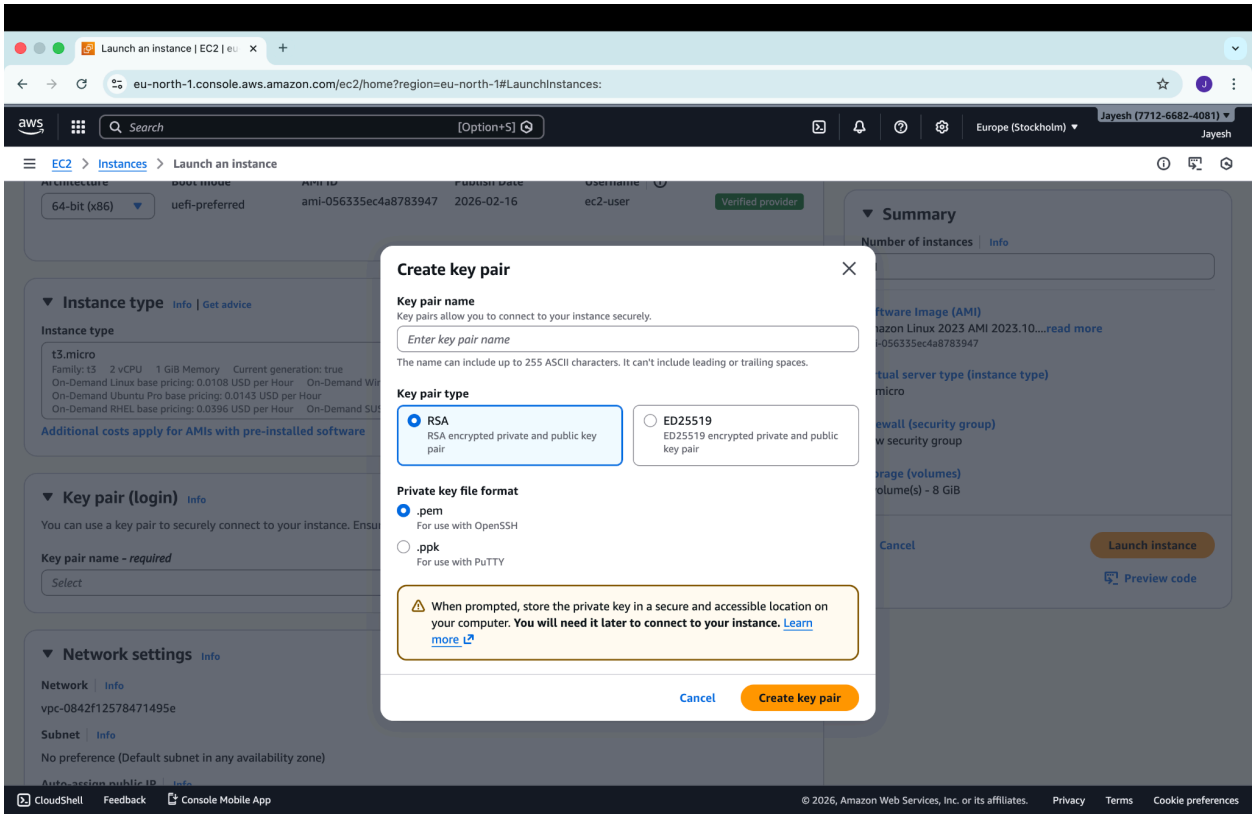


Click **Launch Instance**

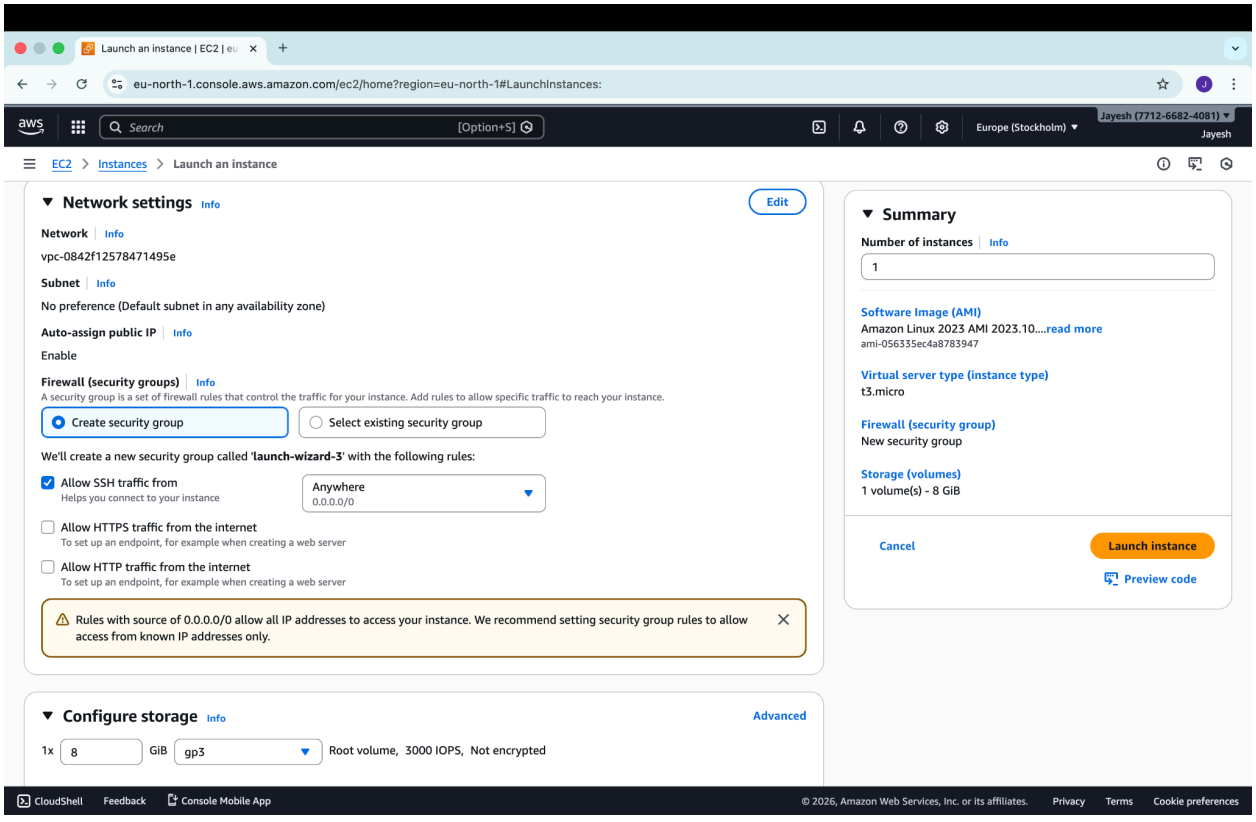


Instance Details:
Name : LinuxWebServer
OS : Amazon Linux 2023
Instance Type: t2.micro (Free Tier)

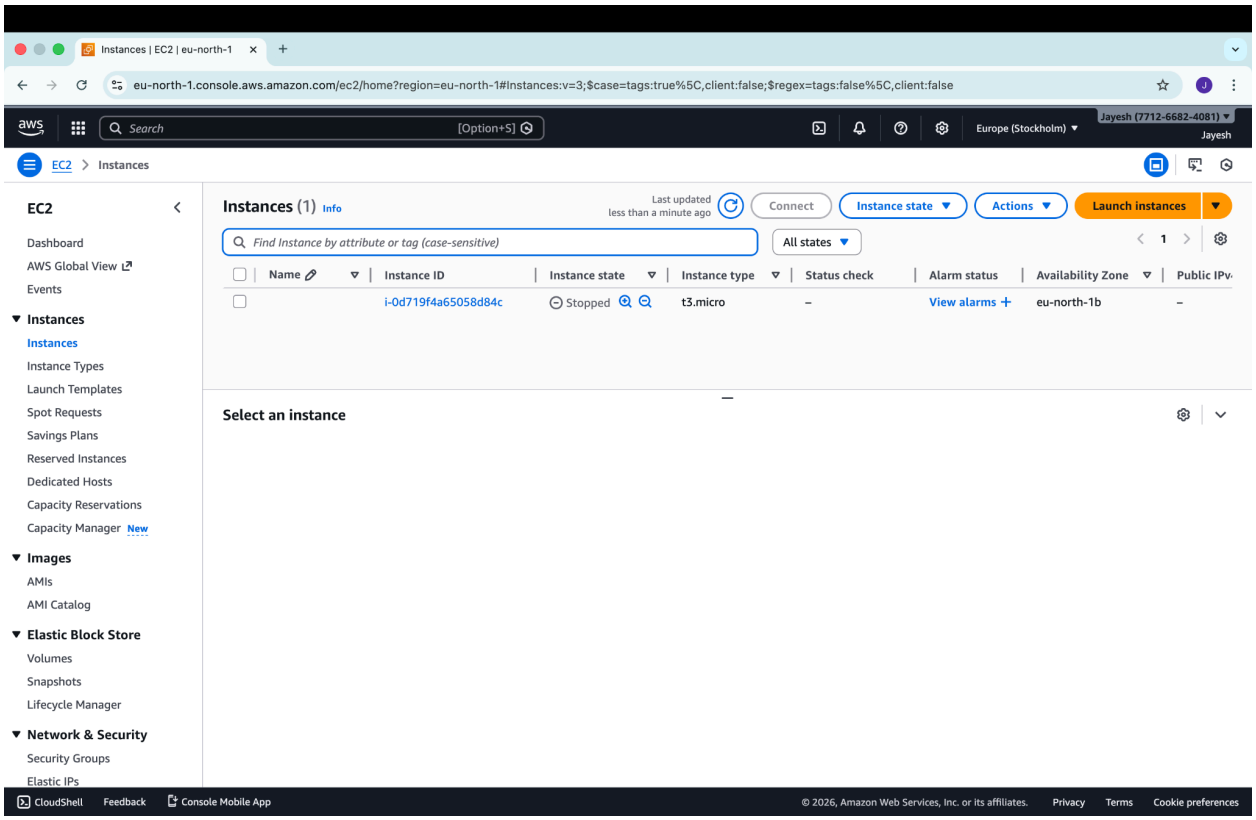
Key Pair:
Click Create New Key Pair
Name: linux-key
Type: RSA
Format: .pem
Download & keep safe (needed even for browser connect)

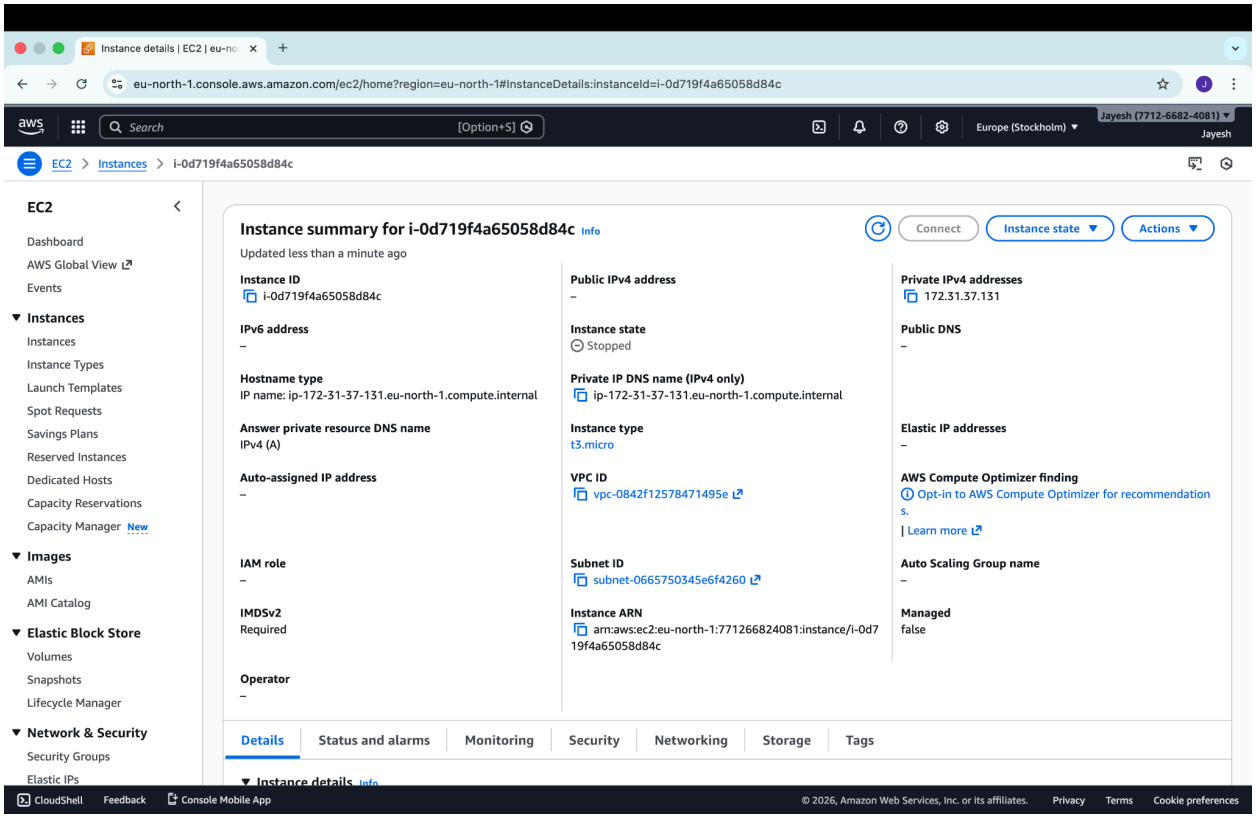


Network Settings:



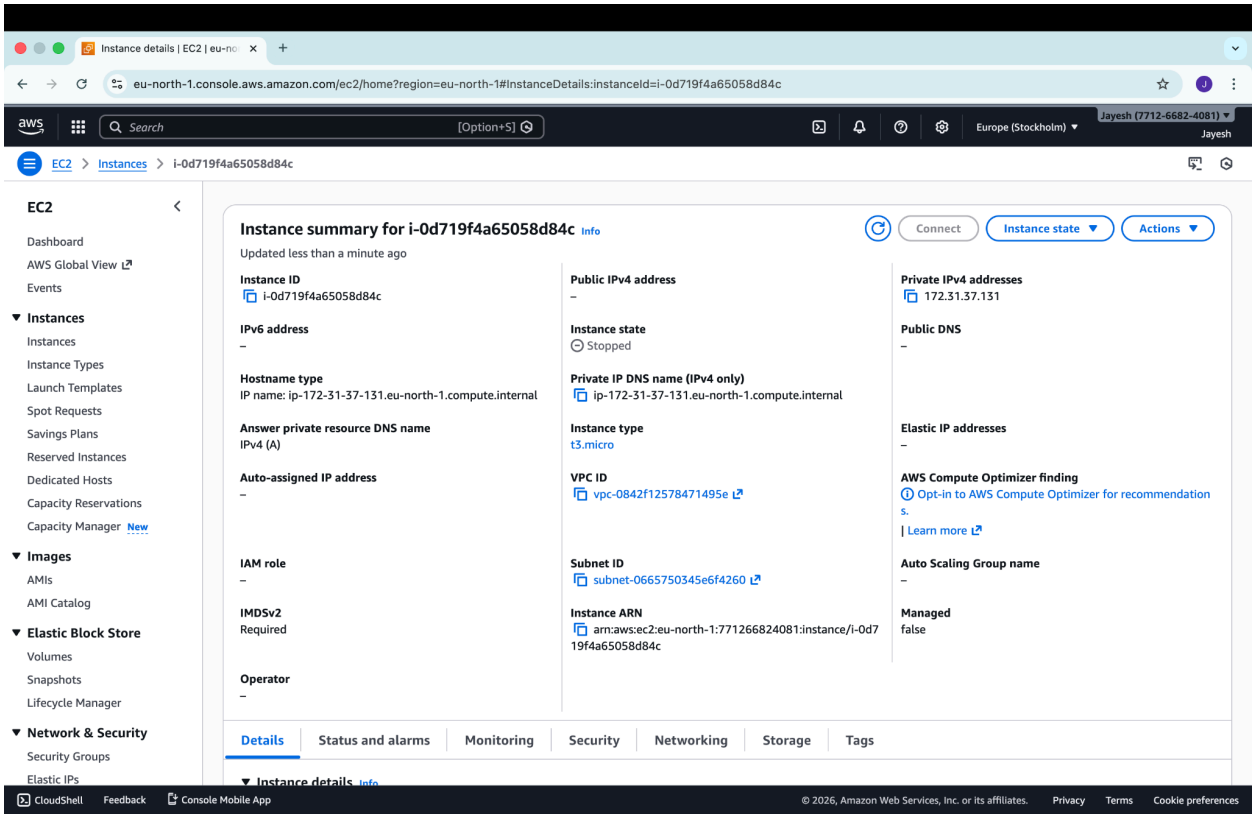
Launch Instance:



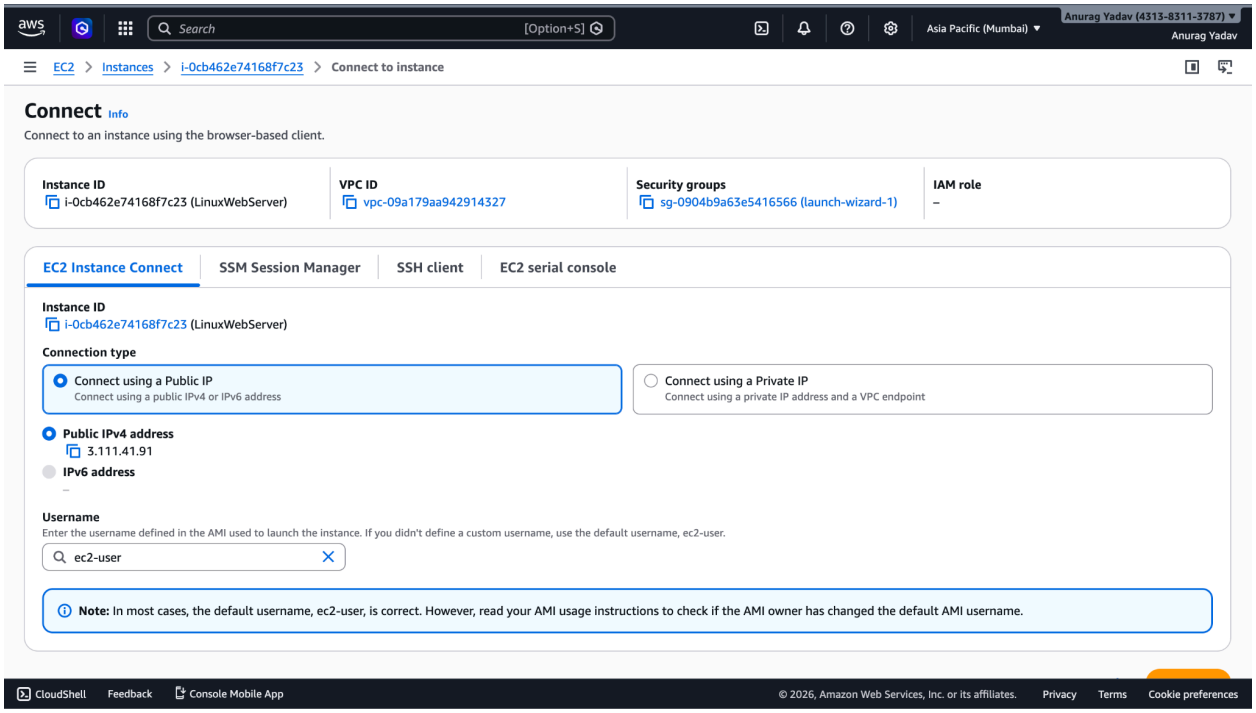


STEP 2: Connect Using EC2 Instance via browser

1) Go to EC2 Dashboard
2) EC2 → Instances
3) Select your instance

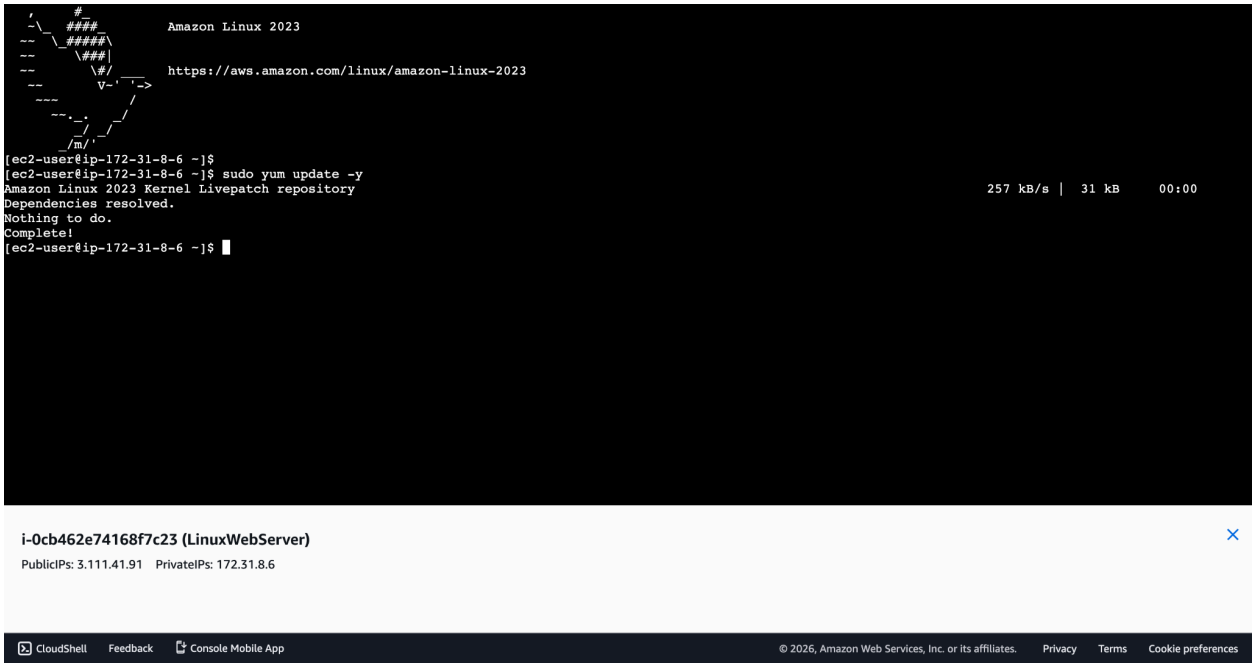


Choose EC2 Instance → Click Connect



STEP 3: Update Linux System

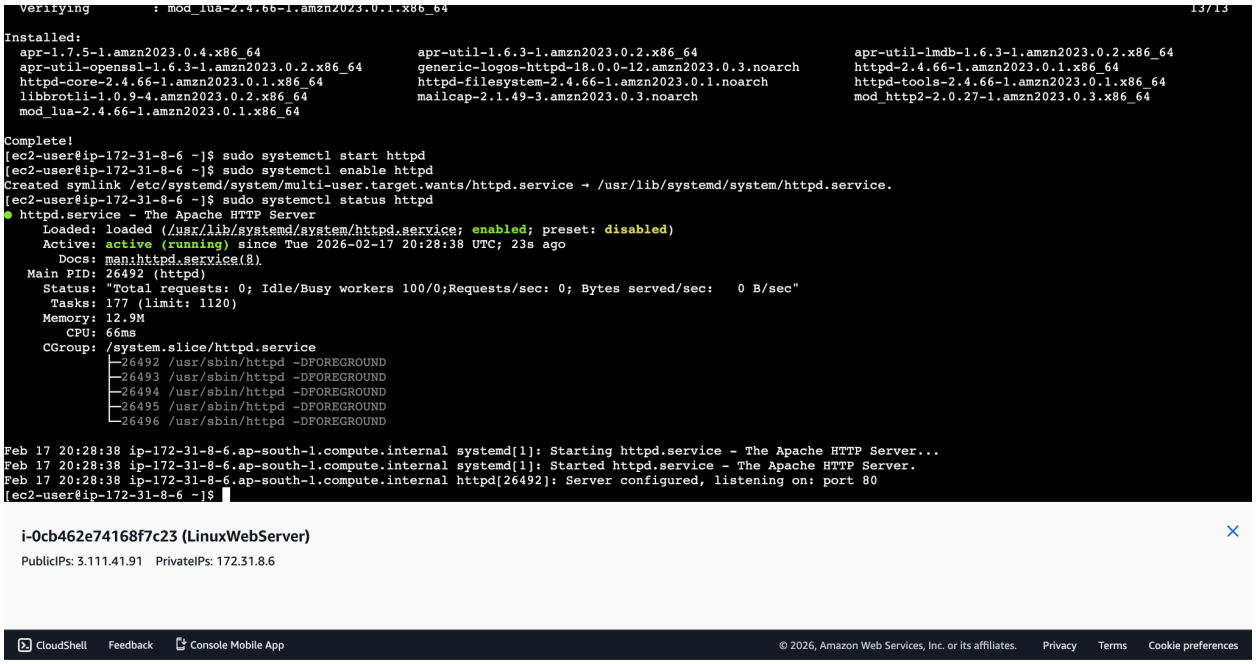
In browser terminal run : sudo yum update -y



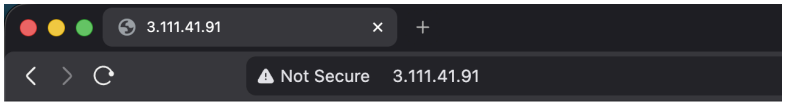
STEP 4: Install Apache WebServer

sudo yum install httpd -y

Start Apache :
sudo systemctl start httpd
sudo systemctl enable httpd

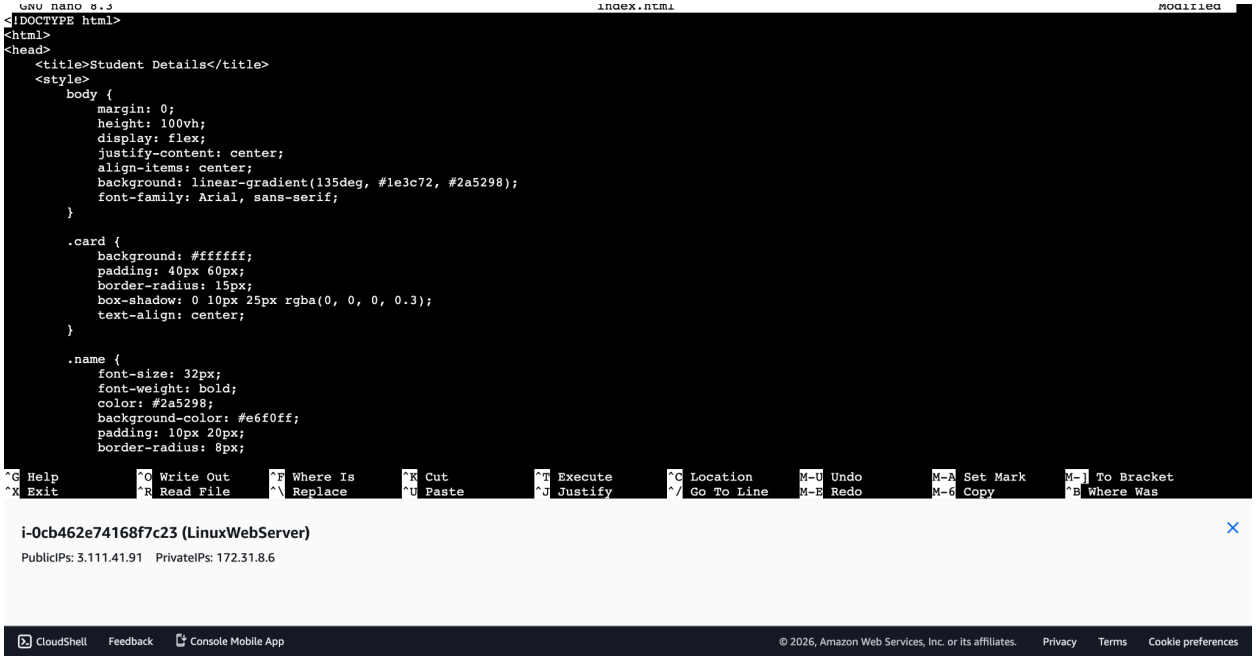


STEP 5: Test Apache WebServer
Copy public Ipv4 Address
EC2 → Instances → Networking → Public Ipv4
Open Browser : http:/public_ip

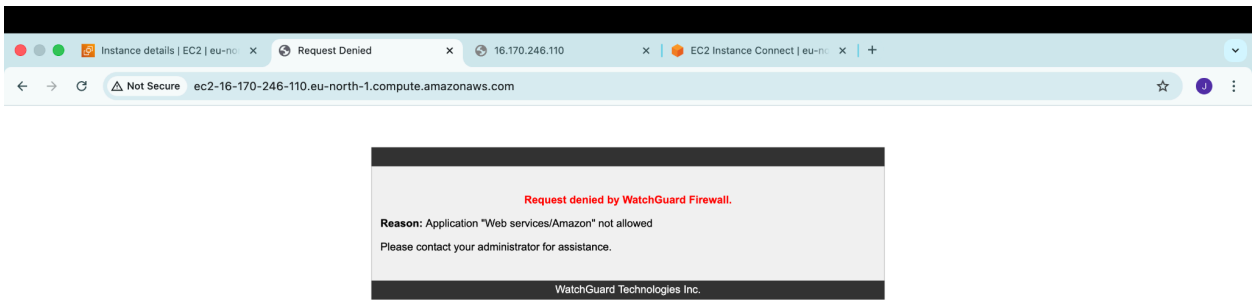


It's Live!

STEP 6: Create Your WebSite
Web folder : /var/www/html
Create Index.html → sudo nano /var/www/html/index.html



STEP 7: Refresh WebSite



Conclusion : I have successfully completed the practical Ec2 Instance creation and hosting website .

PRACTICAL NO. 4

Aim : Store file in S3 Buckets and access it

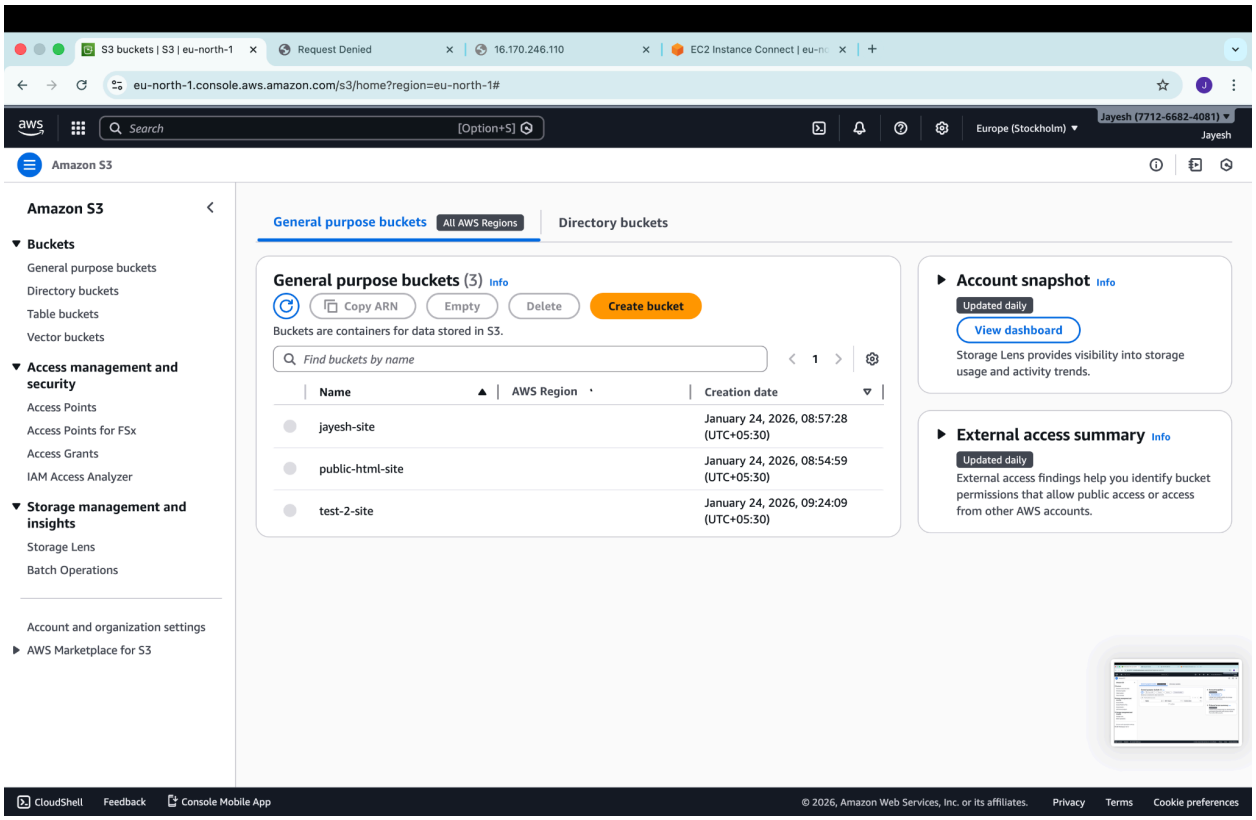
What is S3 ?

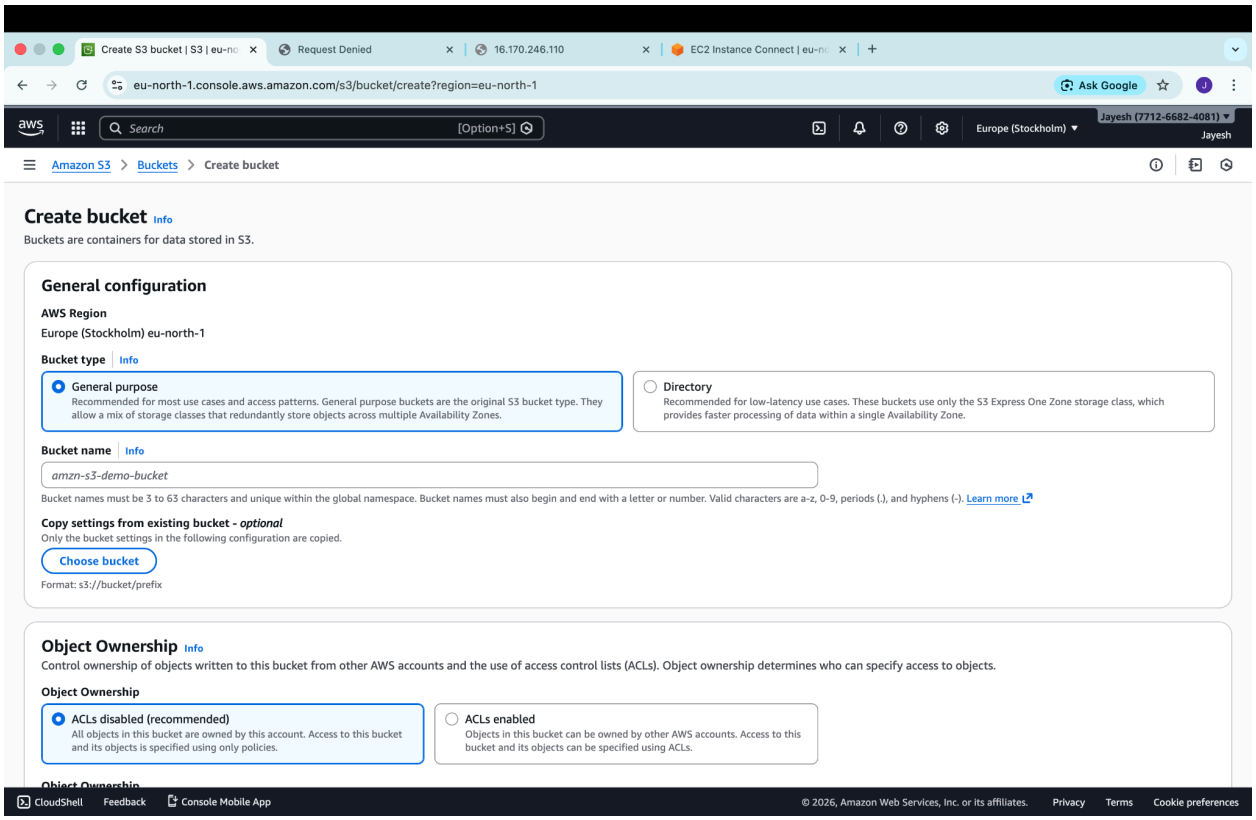
Amazon S3 (Simple Storage Service) is:

- Object storage
- Stores data as objects inside buckets
- Highly durable (99.999999999%) Used for:
- Backups
- Logs
- Media files
- Static websites

PART 1: Create S3 Bucket (AWS Console) Steps:

1. Login to AWS Management Console
2. Go to S3
3. Click Create bucket





Bucket Configuration

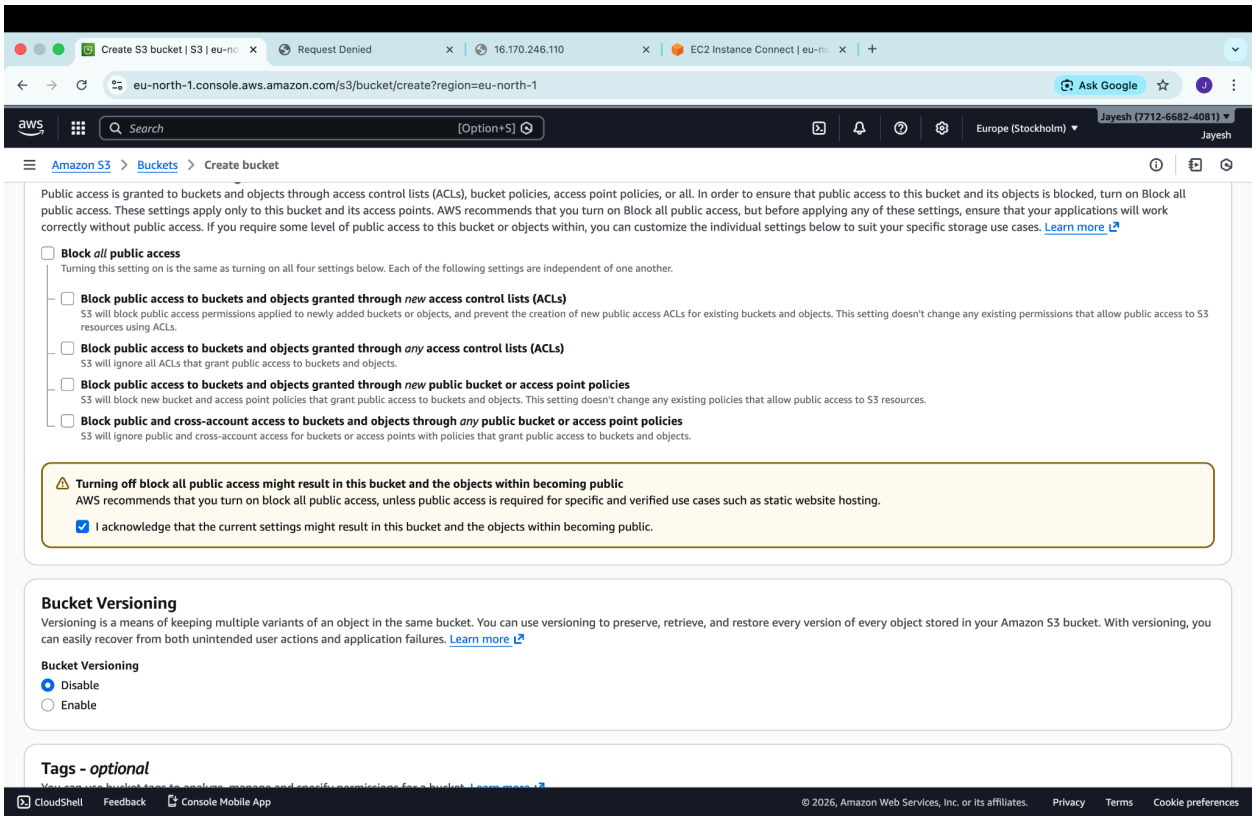
Bucket Name:
Must be globally unique across all AWS users.
Example:
`my-company-backup-2026`

Region:
Choose the nearest region for lower latency.
Example:
`ap-south-1` (Mumbai)

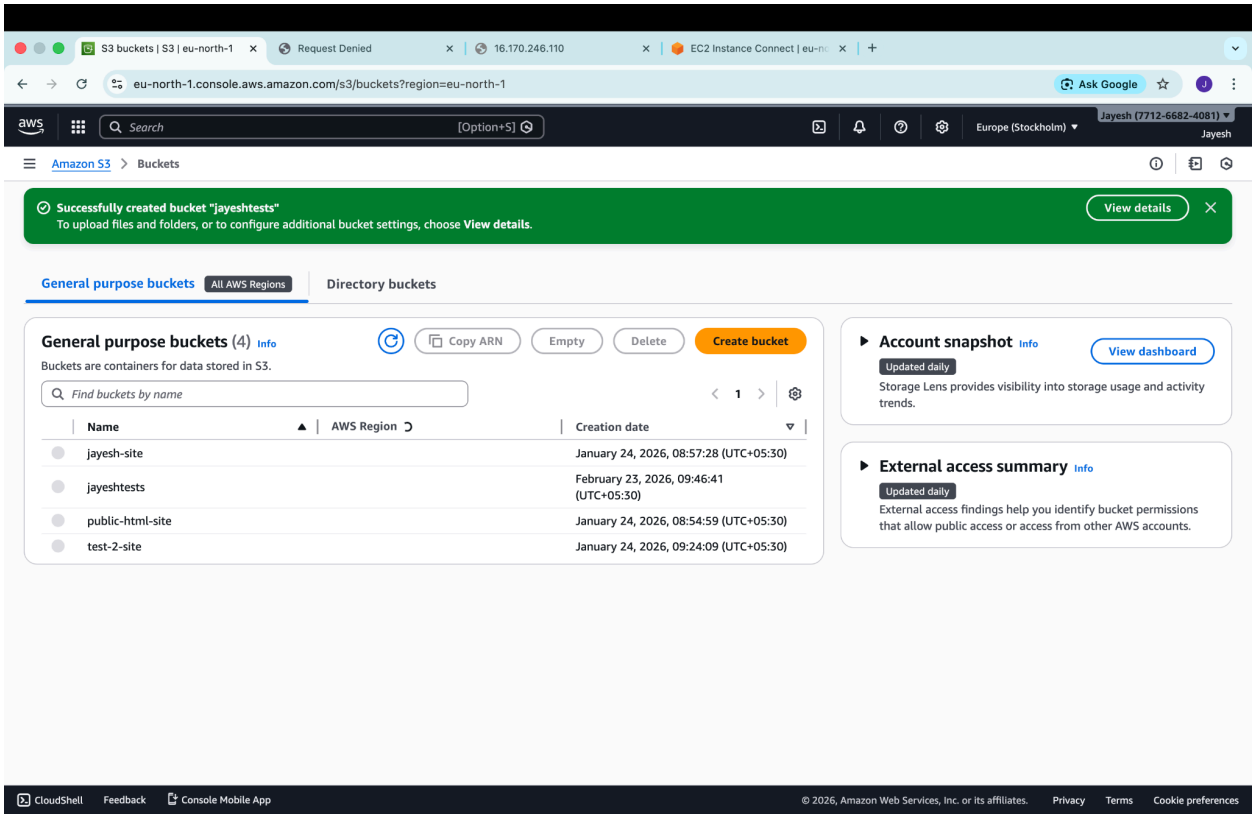
Permissions:
Block all public access: **Disabled**

Other settings: Versioning → optional

Encryption → optional (AES-256 default)



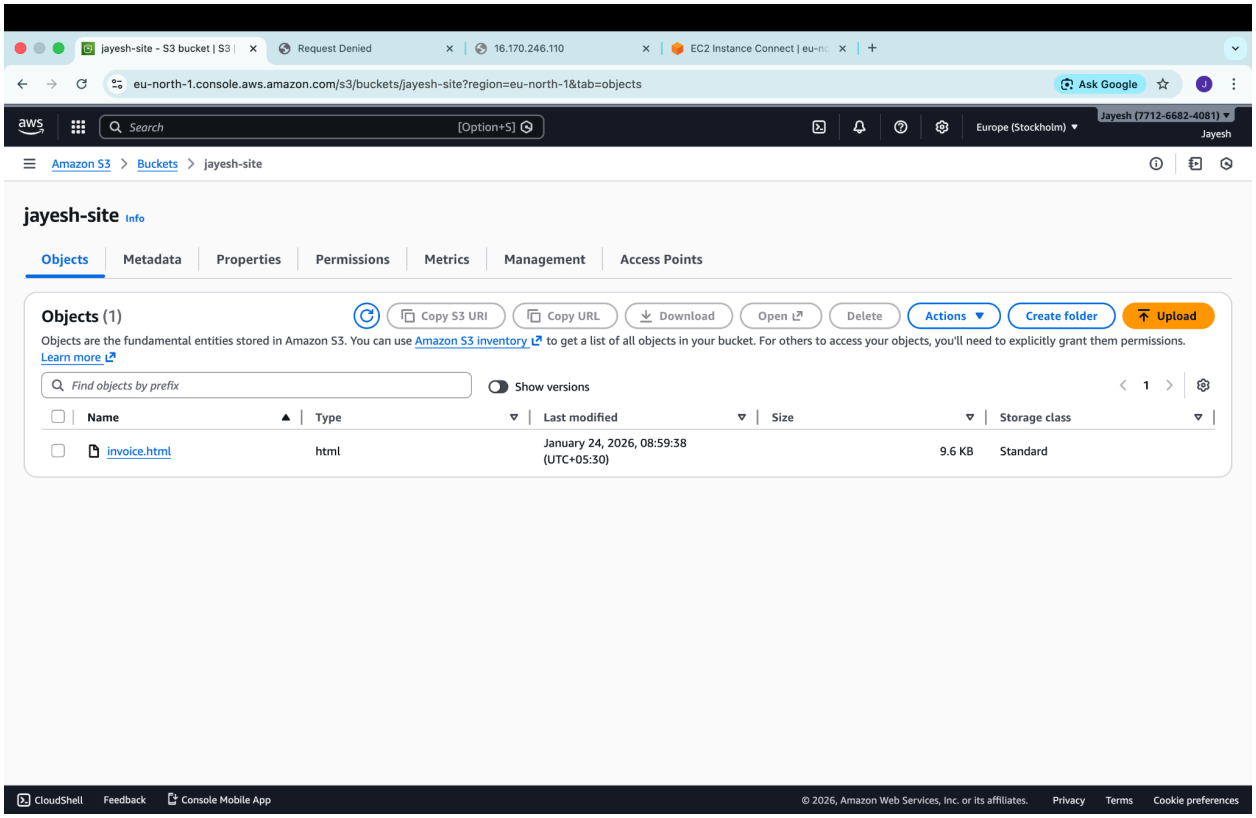
Click Create Bucket:

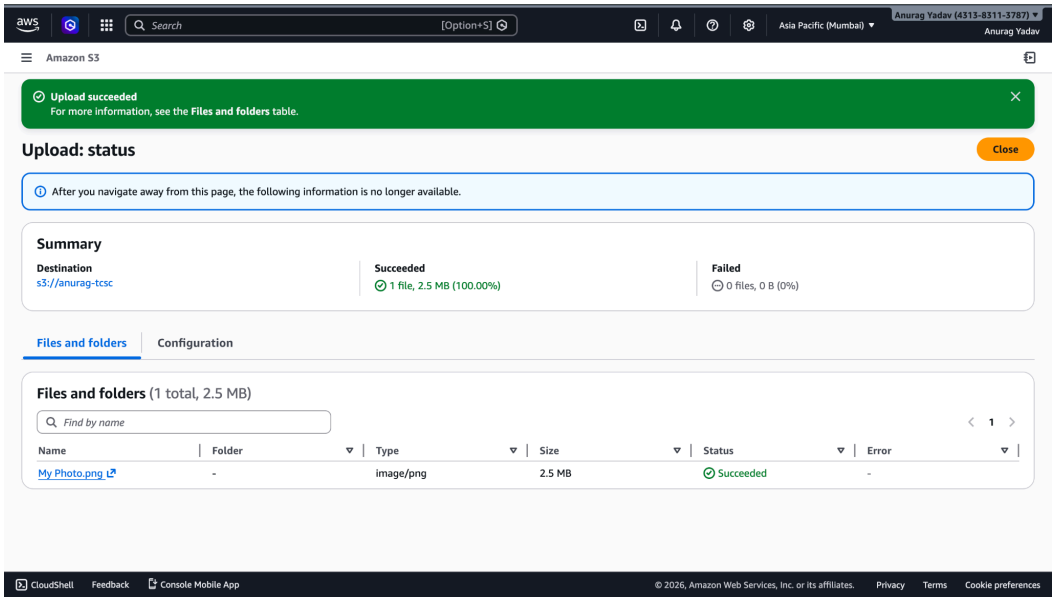


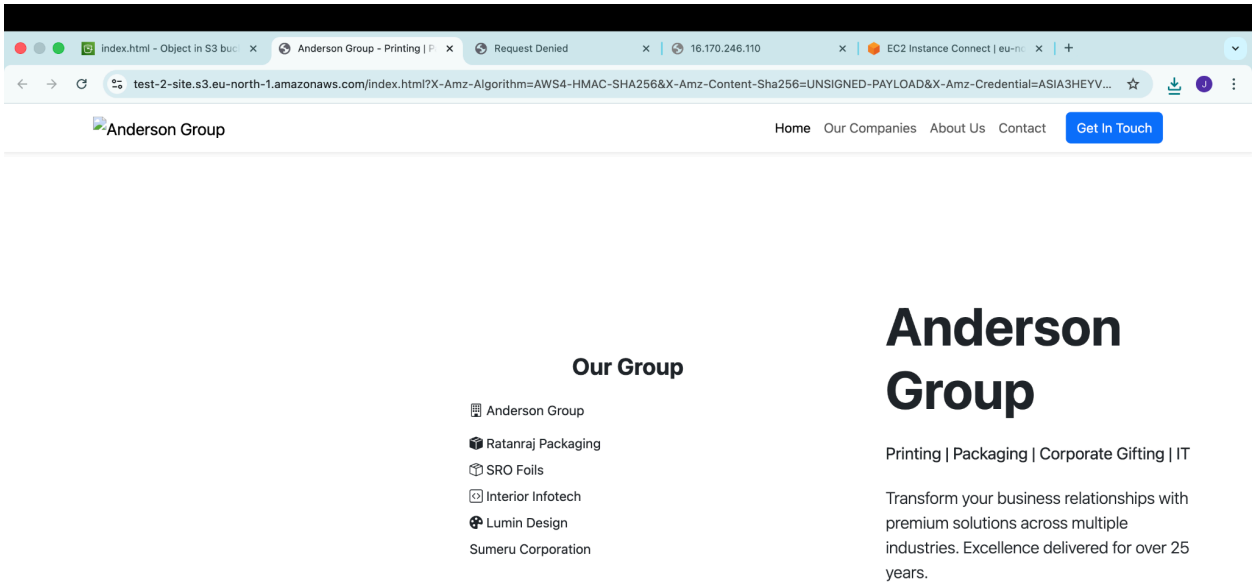
Upload File to S3 from Windows via AWS Console (Easiest)

Steps:

1. Open **S3**
2. Click your **Bucket Name**
3. Click **Upload**
4. Click **Add files** or **Add folder**
5. **Select file from your Windows PC**
6. **Click Upload**


jayesh-site - S3 bucket | S3
Request Denied
16.170.246.110
EC2 Instance Connect | eu-n
eu-north-1.console.aws.amazon.com/s3/buckets/jayesh-site?region=eu-north-1&tab=objects
Ask Google
Search
[Option+S]
Europe (Stockholm)
Jayesh (7712-6682-4081)
Jayesh
Amazon S3 > Buckets > jayesh-site
jayesh-site Info
Objects
Metadata
Properties
Permissions
Metrics
Management
Access Points
Objects (1)
Copy S3 URI
Copy URL
Download
Open
Delete
Actions
Create folder
Upload
Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions.
Learn more
Find objects by prefix
Show versions
1
Name
Type
Last modified
Size
Storage class
invoice.html
html
January 24, 2026, 08:59:38 (UTC+05:30)
9.6 KB
Standard
CloudShell
Feedback
Console Mobile App
© 2026, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Search
[Option+S]
Asia Pacific (Mumbai)
Anurag Yadav (4313-8311-3787)
Anurag Yadav
Amazon S3
Upload succeeded
For more information, see the Files and folders table.
Upload: status
Close
After you navigate away from this page, the following information is no longer available.
Summary
Destination
s3://anurag-tcsc
Succeeded
1 file, 2.5 MB (100.00%)
Failed
0 files, 0 B (0%)
Files and folders
Configuration
Files and folders (1 total, 2.5 MB)
Find by name
1
Name
Folder
Type
Size
Status
Error
My Photo.png
-
image/png
2.5 MB
Succeeded
-
CloudShell
Feedback
Console Mobile App
© 2026, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences



Conclusion : I have Successfully uploaded my file in S3 bucket .

PRACTICAL NO. 5

AIM: To Create BACKUP of running amazon Instance by creating an AMIs and launching new instances from the created AMIs.

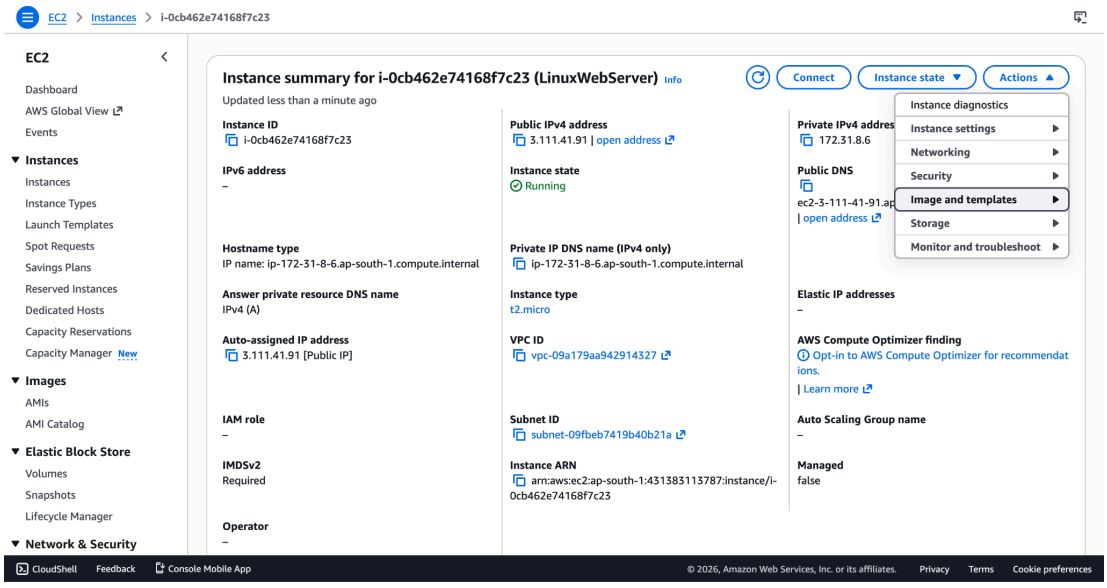
THEORY: An AMI is a template that AWS uses to launch EC2 instances. What does an AMI contain?

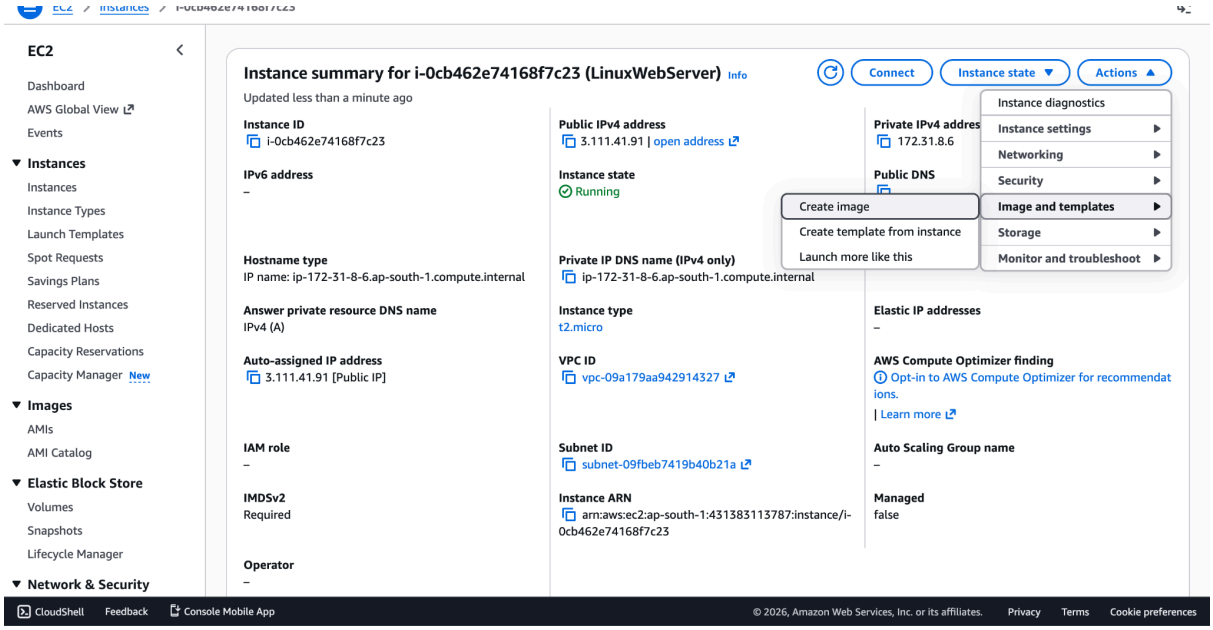
An AMI includes:

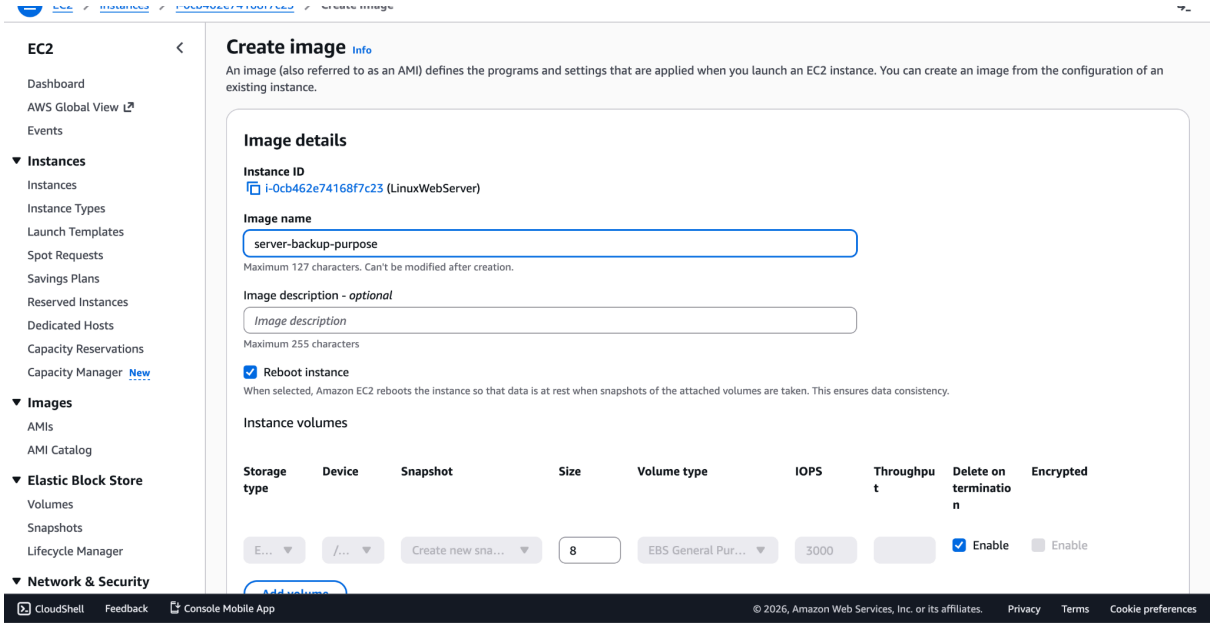
- Root volume snapshot
    - Usually EBS-backed
    - Contains OS (Amazon Linux, Ubuntu, Windows, etc.)
- Additional EBS volume snapshots (if attached)
- Launch permissions
    - Private
    - Shared with specific AWS accounts
    - Public (anyone can use it)
- Block device mapping: Defines volume sizes, types, delete-on-termination

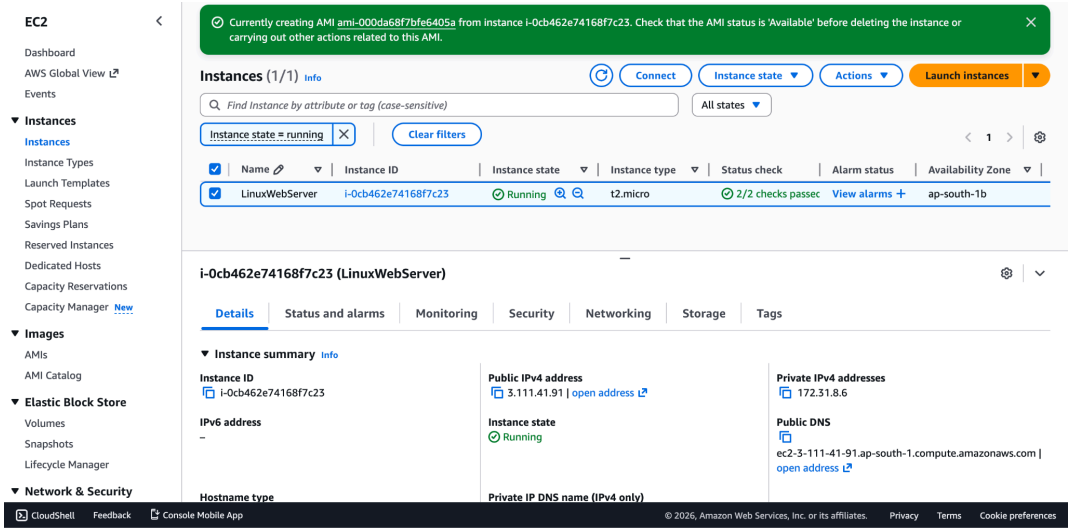
Steps: Create an AMI (backup) from existing EC2

1. Go to EC2 Dashboard
2. Click Instances
3. Select the EC2 instance you want to back up
4. Click Actions → Image and templates → Create image
5. Fill in:
    - Image name:
    - Image description (optional)Click Create image
6. Click Create image



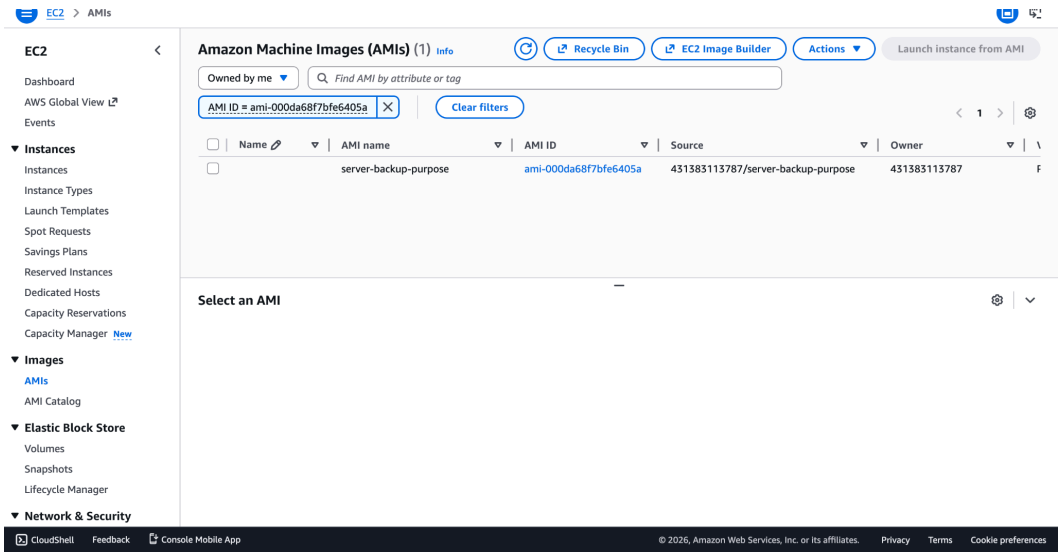

EC2
Dashboard
AWS Global View
Events
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations
Capacity Manager New
Images
AMIs
AMI Catalog
Elastic Block Store
Volumes
Snapshots
Lifecycle Manager
Network & Security
Instance summary for i-0cb462e74168f7c23 (LinuxWebServer) Info
Updated less than a minute ago
Connect
Instance state
Actions
Instance diagnostics
Instance settings
Networking
Security
Image and templates
Storage
Monitor and troubleshoot
Create image
Create template from instance
Launch more like this
Instance ID
i-0cb462e74168f7c23
Public IPv4 address
3.111.41.91 | open address
Private IPv4 addres
172.31.8.6
IPv6 address
–
Instance state
Running
Public DNS
Hostname type
IP name: ip-172-31-8-6.ap-south-1.compute.internal
Private IP DNS name (IPv4 only)
ip-172-31-8-6.ap-south-1.compute.internal
Answer private resource DNS name
IPv4 (A)
Instance type
t2.micro
Elastic IP addresses
–
Auto-assigned IP address
3.111.41.91 [Public IP]
VPC ID
vpc-09a179aa942914327
AWS Compute Optimizer finding
Opt-in to AWS Compute Optimizer for recommendations.
| Learn more
IAM role
–
Subnet ID
subnet-09fbeb7419b40b21a
Auto Scaling Group name
–
IMDSv2
Required
Instance ARN
arn:aws:ec2:ap-south-1:431383113787:instance/i-0cb462e74168f7c23
Managed
false
Operator
–
CloudShell
Feedback
Console Mobile App
© 2026, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

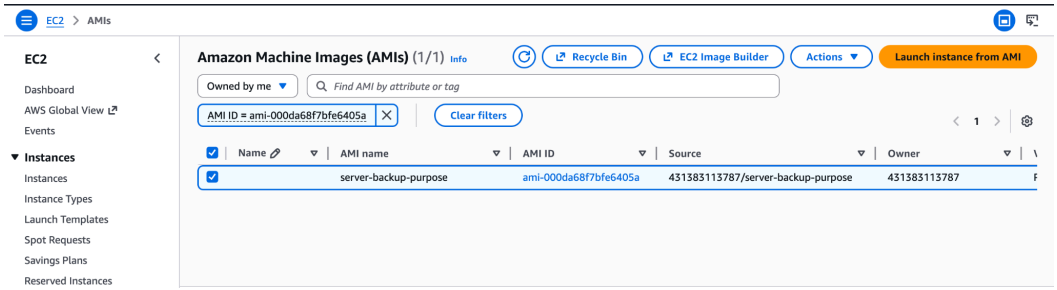

EC2
Dashboard
AWS Global View
Events
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations
Capacity Manager New
Images
AMIs
AMI Catalog
Elastic Block Store
Volumes
Snapshots
Lifecycle Manager
Network & Security
Create image Info
An image (also referred to as an AMI) defines the programs and settings that are applied when you launch an EC2 instance. You can create an image from the configuration of an existing instance.
Image details
Instance ID
i-0cb462e74168f7c23 (LinuxWebServer)
Image name
server-backup-purpose
Maximum 127 characters. Can't be modified after creation.
Image description - optional
Image description
Maximum 255 characters
Reboot instance
When selected, Amazon EC2 reboots the instance so that data is at rest when snapshots of the attached volumes are taken. This ensures data consistency.
Instance volumes
Storage type
Device
Snapshot
Size
Volume type
IOPS
Throughput
Delete on termination
Encrypted
E...
/...
Create new sna...
8
EBS General Pur...
3000
Enable
Enable
CloudShell
Feedback
Console Mobile App
© 2026, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

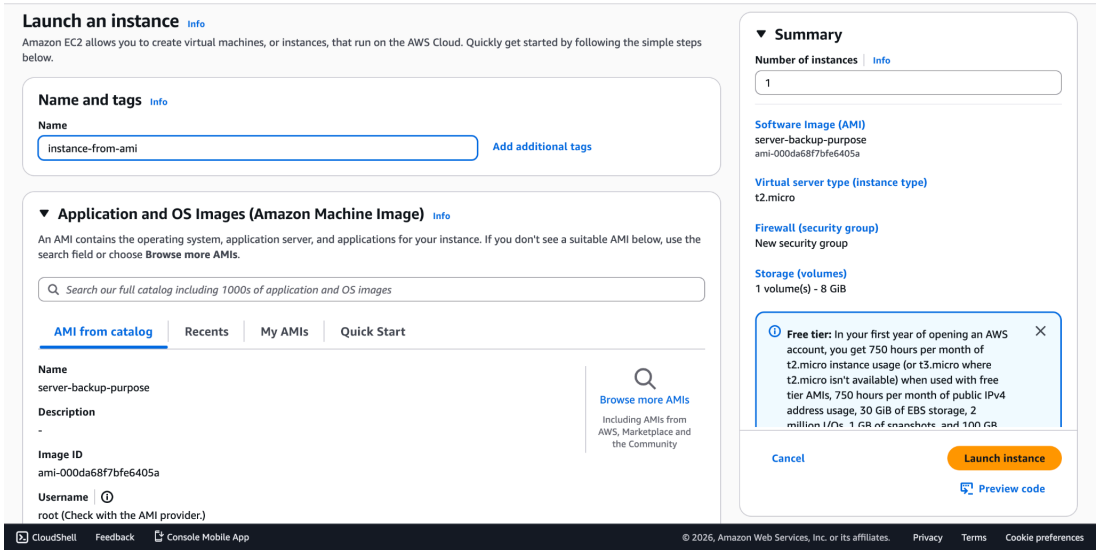


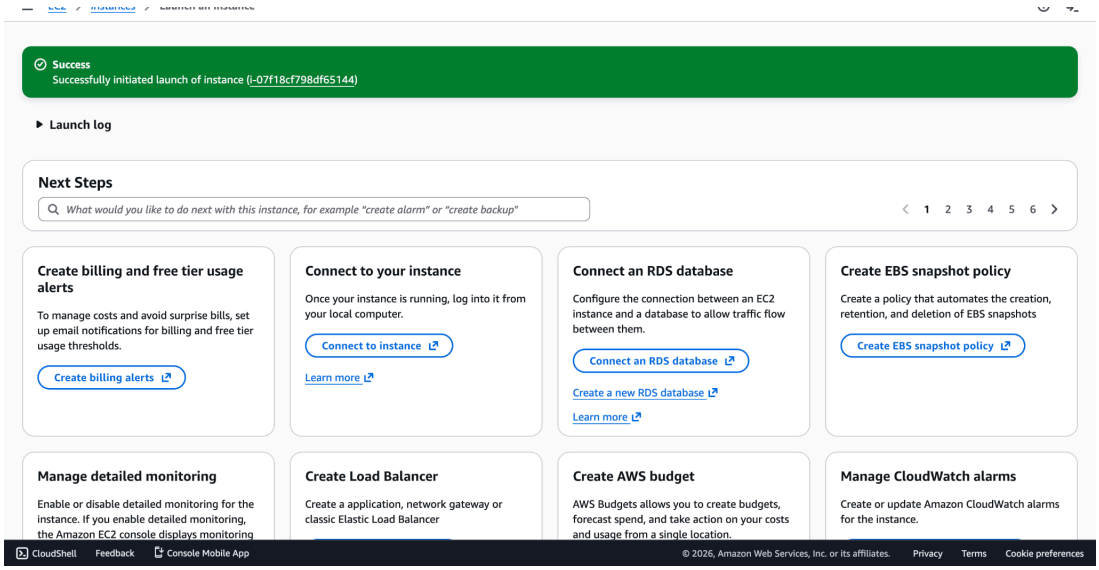
Launch a New EC2 Instance from the Created AMI

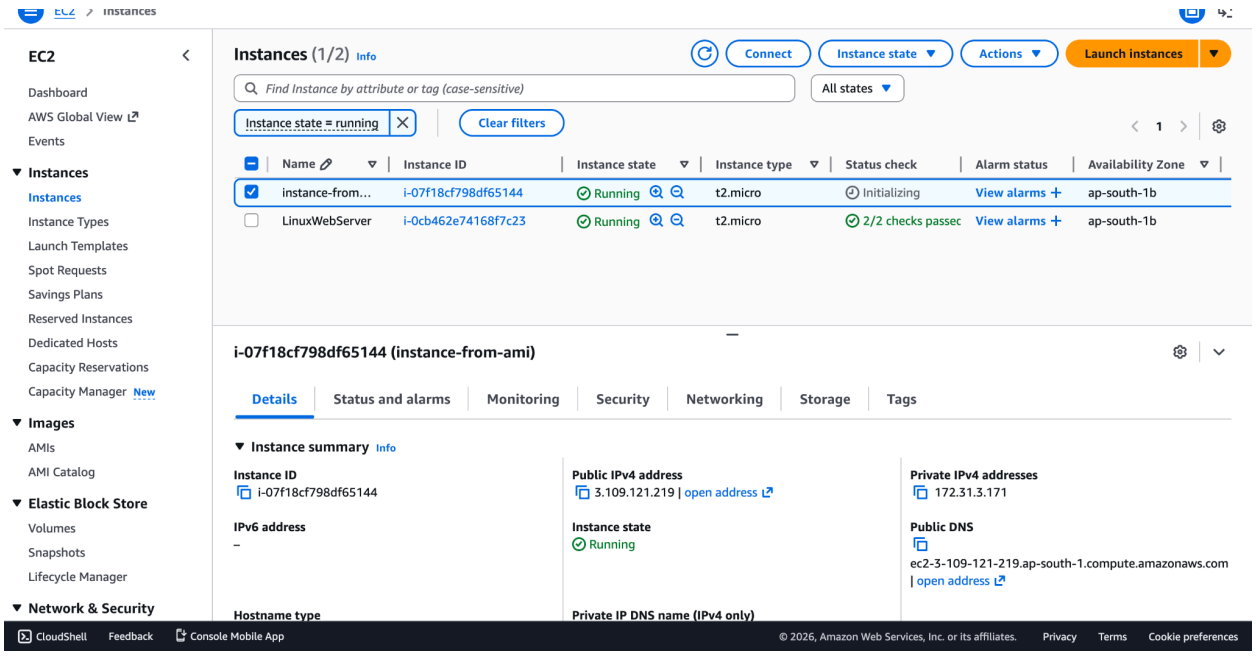
1. Go to **EC2 Dashboard → AMIs**
2. Select your newly created AMI
3. Click **Launch instance from AMI**
4. Configure the following settings:
   Instance type (e.g., t3.micro)
   Key pair
   Security group
   VPC and Subnet
5. Click **Launch instance**

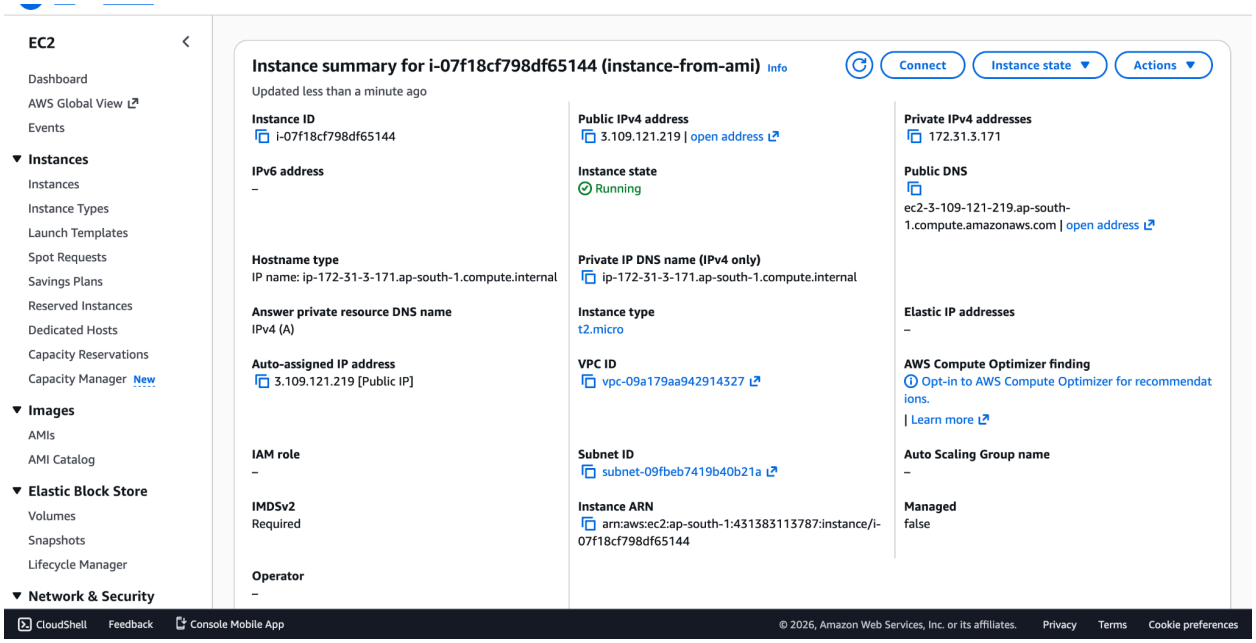


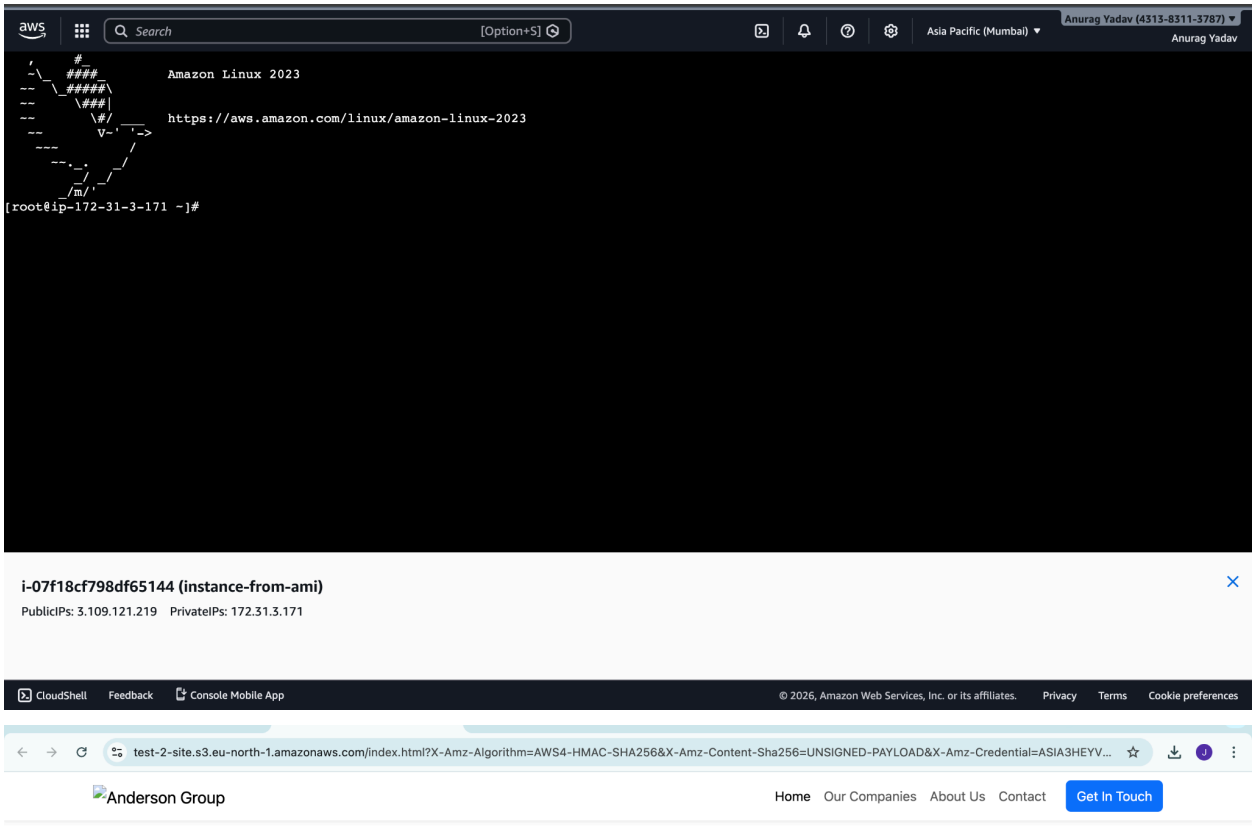

EC2 > AMIs
EC2
Dashboard
AWS Global View
Events
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Amazon Machine Images (AMIs) (1/1) Info
Recycle Bin
EC2 Image Builder
Actions
Launch instance from AMI
Owned by me
Find AMI by attribute or tag
AMI ID = ami-000da68f7bfe6405a
Clear filters
Name
AMI name
AMI ID
Source
Owner
server-backup-purpose
ami-000da68f7bfe6405a
431383113787/server-backup-purpose
431383113787

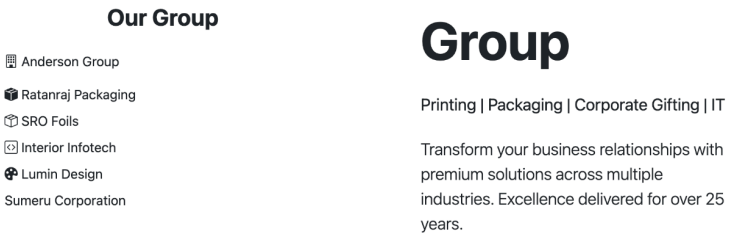

Launch an instance Info
Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.
Name and tags Info
Name
instance-from-ami
Add additional tags
Application and OS Images (Amazon Machine Image) Info
An AMI contains the operating system, application server, and applications for your instance. If you don't see a suitable AMI below, use the search field or choose Browse more AMIs.
Search our full catalog including 1000s of application and OS images
AMI from catalog
Recents
My AMIs
Quick Start
Name
server-backup-purpose
Description
-
Image ID
ami-000da68f7bfe6405a
Username
root (Check with the AMI provider.)
Browse more AMIs
Including AMIs from AWS, Marketplace and the Community
Summary
Number of instances Info
1
Software Image (AMI)
server-backup-purpose
ami-000da68f7bfe6405a
Virtual server type (instance type)
t2.micro
Firewall (security group)
New security group
Storage (volumes)
1 volume(s) - 8 GiB
Free tier: In your first year of opening an AWS account, you get 750 hours per month of t2.micro instance usage (or t3.micro where t2.micro isn't available) when used with free tier AMIs, 750 hours per month of public IPv4 address usage, 30 GiB of EBS storage, 2
Cancel
Launch instance
Preview code
CloudShell
Feedback
Console Mobile App
© 2026, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

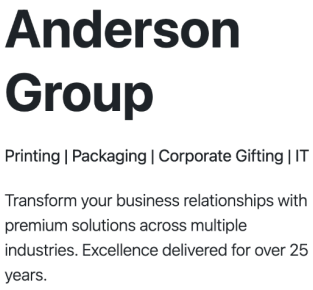

Success
Successfully initiated launch of instance (i-07f18cf798df65144)
Launch log
Next Steps
What would you like to do next with this instance, for example "create alarm" or "create backup"
1 2 3 4 5 6
Create billing and free tier usage alerts
To manage costs and avoid surprise bills, set up email notifications for billing and free tier usage thresholds.
Create billing alerts
Connect to your instance
Once your instance is running, log into it from your local computer.
Connect to instance
Learn more
Connect an RDS database
Configure the connection between an EC2 instance and a database to allow traffic flow between them.
Connect an RDS database
Create a new RDS database
Learn more
Create EBS snapshot policy
Create a policy that automates the creation, retention, and deletion of EBS snapshots
Create EBS snapshot policy
Manage detailed monitoring
Enable or disable detailed monitoring for the instance. If you enable detailed monitoring, the Amazon EC2 console displays monitoring
Create Load Balancer
Create a application, network gateway or classic Elastic Load Balancer
Create AWS budget
AWS Budgets allows you to create budgets, forecast spend, and take action on your costs and usage from a single location.
Manage CloudWatch alarms
Create or update Amazon CloudWatch alarms for the instance.
CloudShell
Feedback
Console Mobile App
© 2026, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


EC2
Instances
Dashboard
AWS Global View
Events
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations
Capacity Manager New
Images
AMIs
AMI Catalog
Elastic Block Store
Volumes
Snapshots
Lifecycle Manager
Network & Security
Instances (1/2) Info
Connect
Instance state
Actions
Launch instances
Find Instance by attribute or tag (case-sensitive)
All states
Instance state = running
Clear filters
Name
Instance ID
Instance state
Instance type
Status check
Alarm status
Availability Zone
instance-from...
i-07f18cf798df65144
Running
t2.micro
Initializing
View alarms
ap-south-1b
LinuxWebServer
i-0cb462e74168f7c23
Running
t2.micro
2/2 checks passec
View alarms
ap-south-1b
i-07f18cf798df65144 (instance-from-ami)
Details
Status and alarms
Monitoring
Security
Networking
Storage
Tags
Instance summary Info
Instance ID
i-07f18cf798df65144
IPv6 address
–
Hostname type
Public IPv4 address
3.109.121.219 | open address
Instance state
Running
Private IP DNS name (IPv4 only)
Private IPv4 addresses
172.31.3.171
Public DNS
ec2-3-109-121-219.ap-south-1.compute.amazonaws.com | open address
CloudShell
Feedback
Console Mobile App
© 2026, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


EC2
Dashboard
AWS Global View
Events
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations
Capacity Manager New
Images
AMIs
AMI Catalog
Elastic Block Store
Volumes
Snapshots
Lifecycle Manager
Network & Security
Instance summary for i-07f18cf798df65144 (instance-from-ami) Info
Updated less than a minute ago
Connect
Instance state
Actions
Instance ID
i-07f18cf798df65144
IPv6 address
–
Hostname type
IP name: ip-172-31-3-171.ap-south-1.compute.internal
Answer private resource DNS name
IPv4 (A)
Auto-assigned IP address
3.109.121.219 [Public IP]
IAM role
–
IMDSv2
Required
Operator
–
Public IPv4 address
3.109.121.219 | open address
Instance state
Running
Private IP DNS name (IPv4 only)
ip-172-31-3-171.ap-south-1.compute.internal
Instance type
t2.micro
VPC ID
vpc-09a179aa942914327
Subnet ID
subnet-09fbeb7419b40b21a
Instance ARN
arn:aws:ec2:ap-south-1:431383113787:instance/i-07f18cf798df65144
Private IPv4 addresses
172.31.3.171
Public DNS
ec2-3-109-121-219.ap-south-1.compute.amazonaws.com | open address
Elastic IP addresses
–
AWS Compute Optimizer finding
Opt-in to AWS Compute Optimizer for recommendations.
| Learn more
Auto Scaling Group name
–
Managed
false
CloudShell
Feedback
Console Mobile App
© 2026, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences







Conclusion : I have Successfully Completed practical to Create Backup of running amazon Instance by creating an AMIs and launching new instances from the created AMIs.

PRACTICAL NO. 6

AIM: To monitor an EC2 instance using Amazon CloudWatch and create an alarm based on CPU utilization.

THEORY:

Amazon CloudWatch is a monitoring and observability service that provides:

- Metrics (CPU, Network, Disk, etc.)
- Logs
- Alarms
- Dashboards
- Events

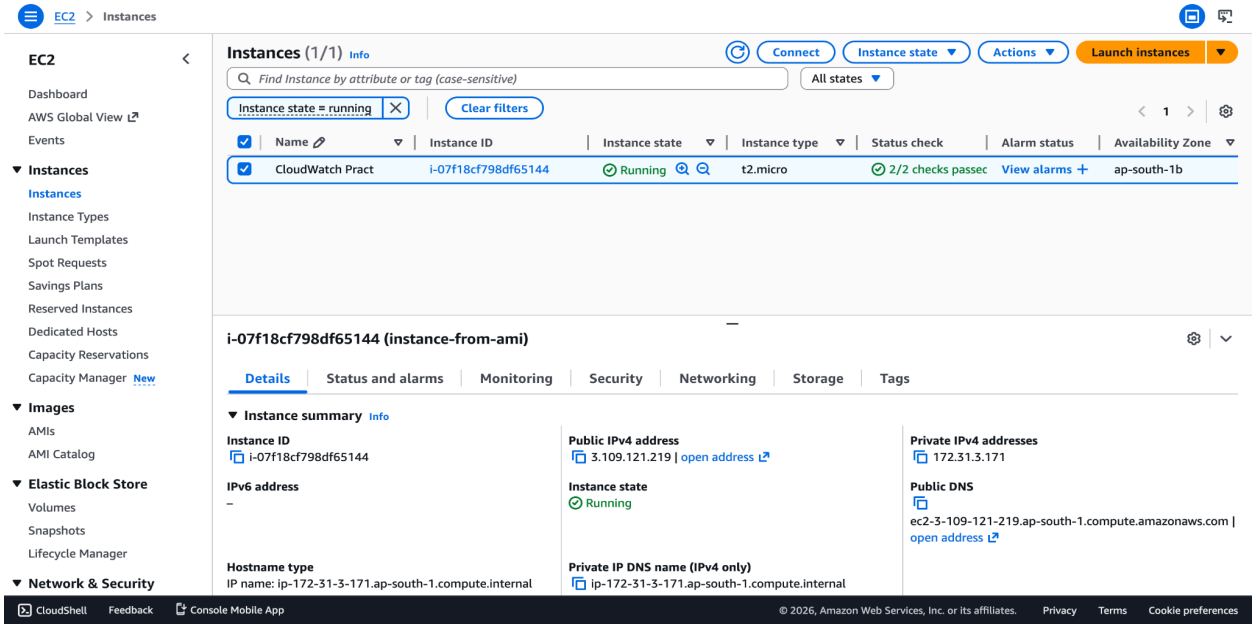
CloudWatch collects default metrics from EC2 automatically. An Alarm monitors a metric and performs an action (like sending notification) when a threshold is breached.

Create CloudWatch Alarm for EC2 → Steps:

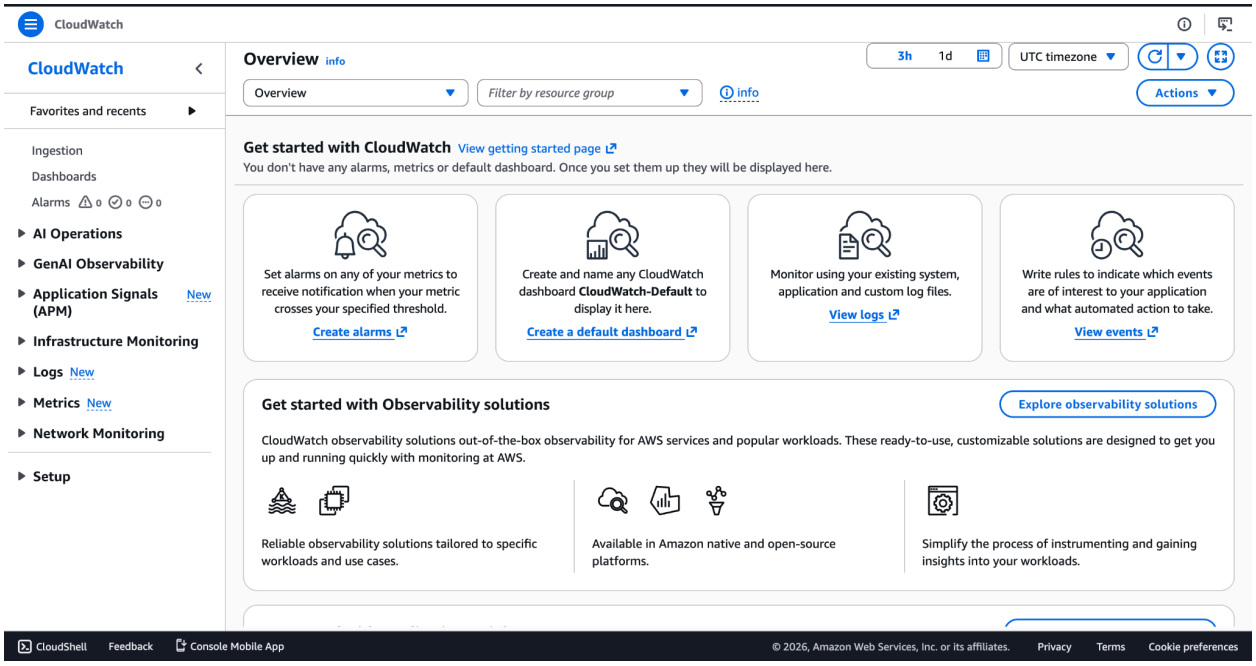
1. Go to AWS Console
2. Open CloudWatch
3. Click Alarms
4. Click Create alarm
5. Click Select metric
6. Choose:
    - EC2
    - Per-Instance Metrics
7. Select CPU Utilization
8. Click Select metric
9. Configure condition:
    - Threshold type → Static
    - Whenever CPUUtilization is:
        - Greater than 70%
10. Click Next
11. Configure notification:
    - Create new SNS topic
    - Enter email address
12. Click Create topic
13. Confirm email subscription
14. Click Next
15. Name the alarm

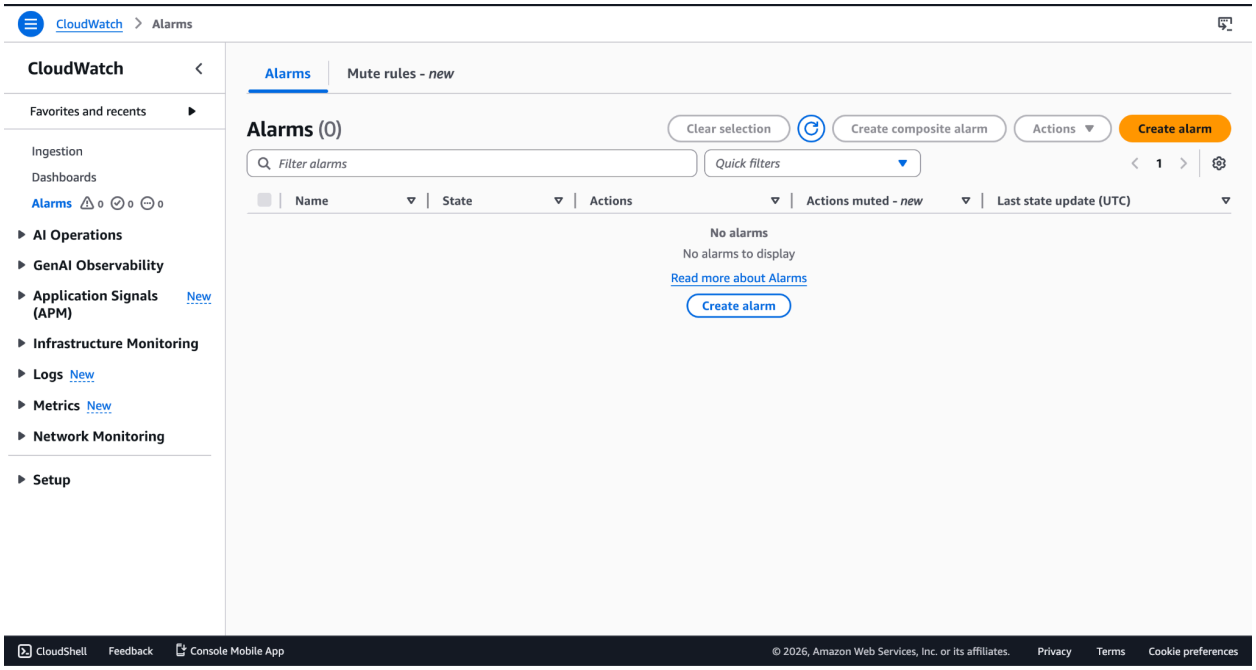
16. Click Create alarm

EC2 instance → Running State

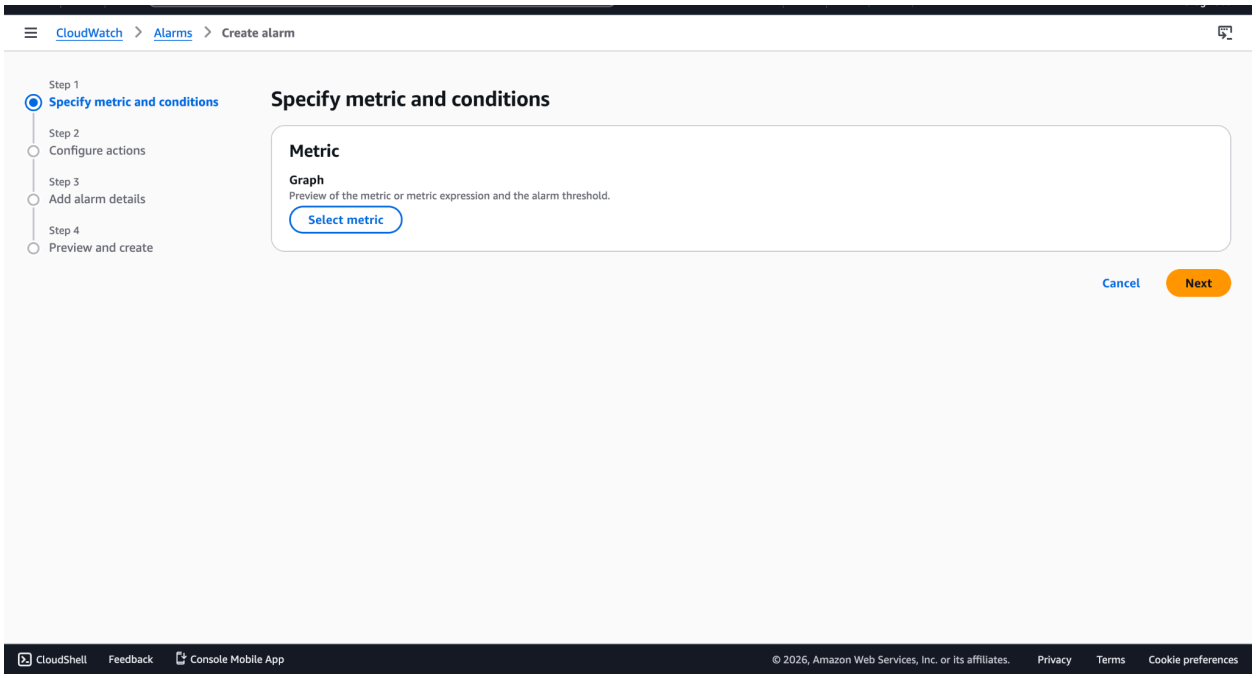


Cloudwatch → Click Create Alarm

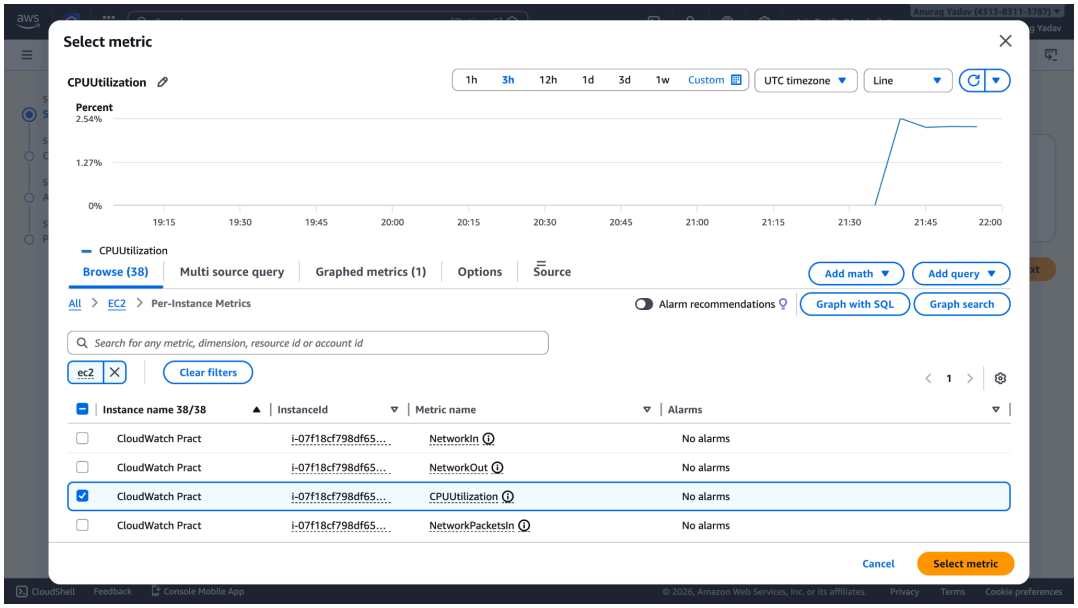




Click on Select Metric



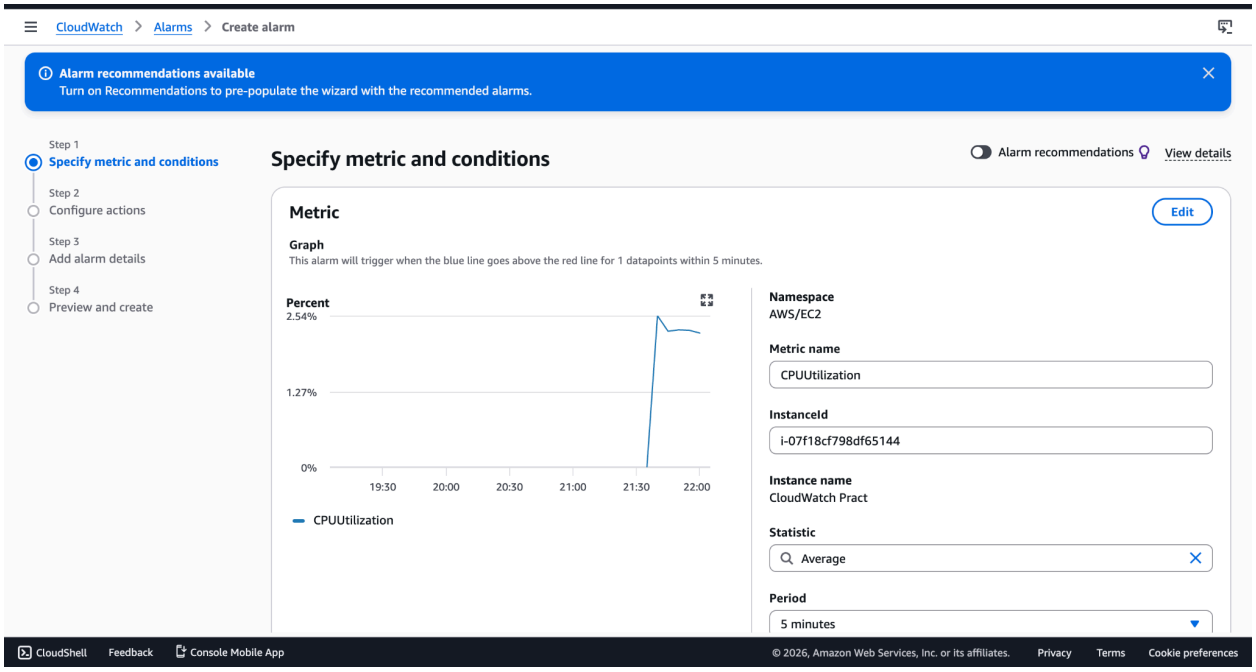
Choose EC2 → Per-Instance Metrics → CPUUtilization → select metric

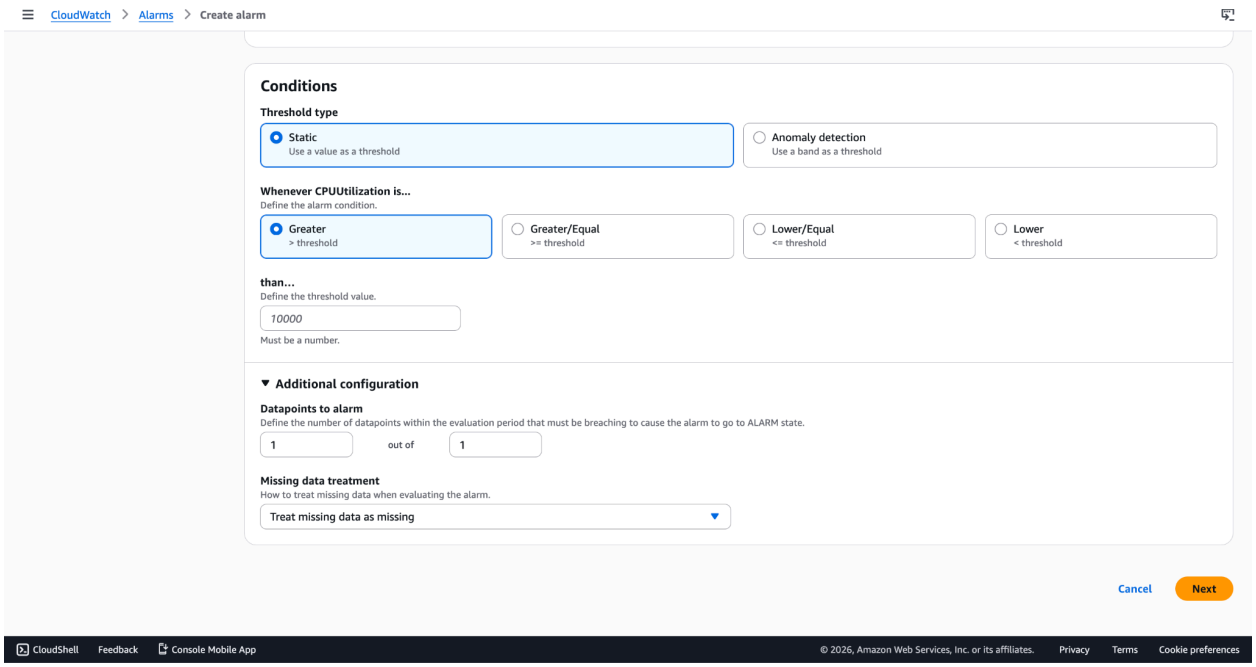


CPU Configuration :

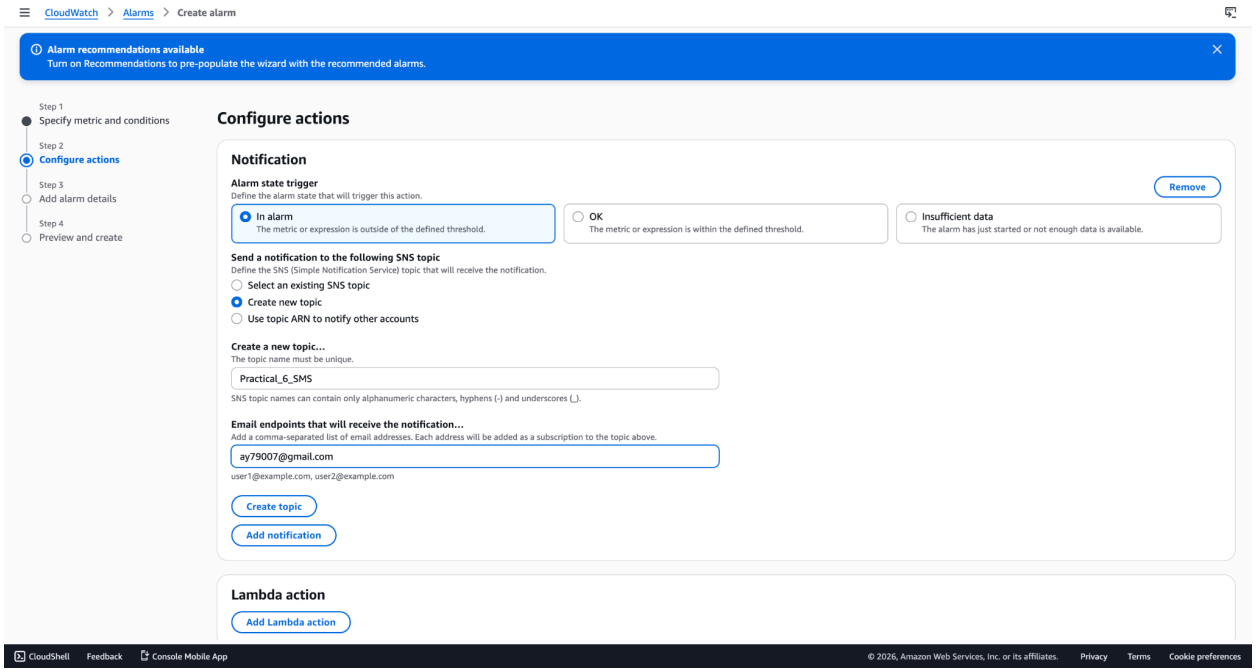
Threshold type → **Static**

CPUUtilization > 70 (e.g here i have choosen value as 2)

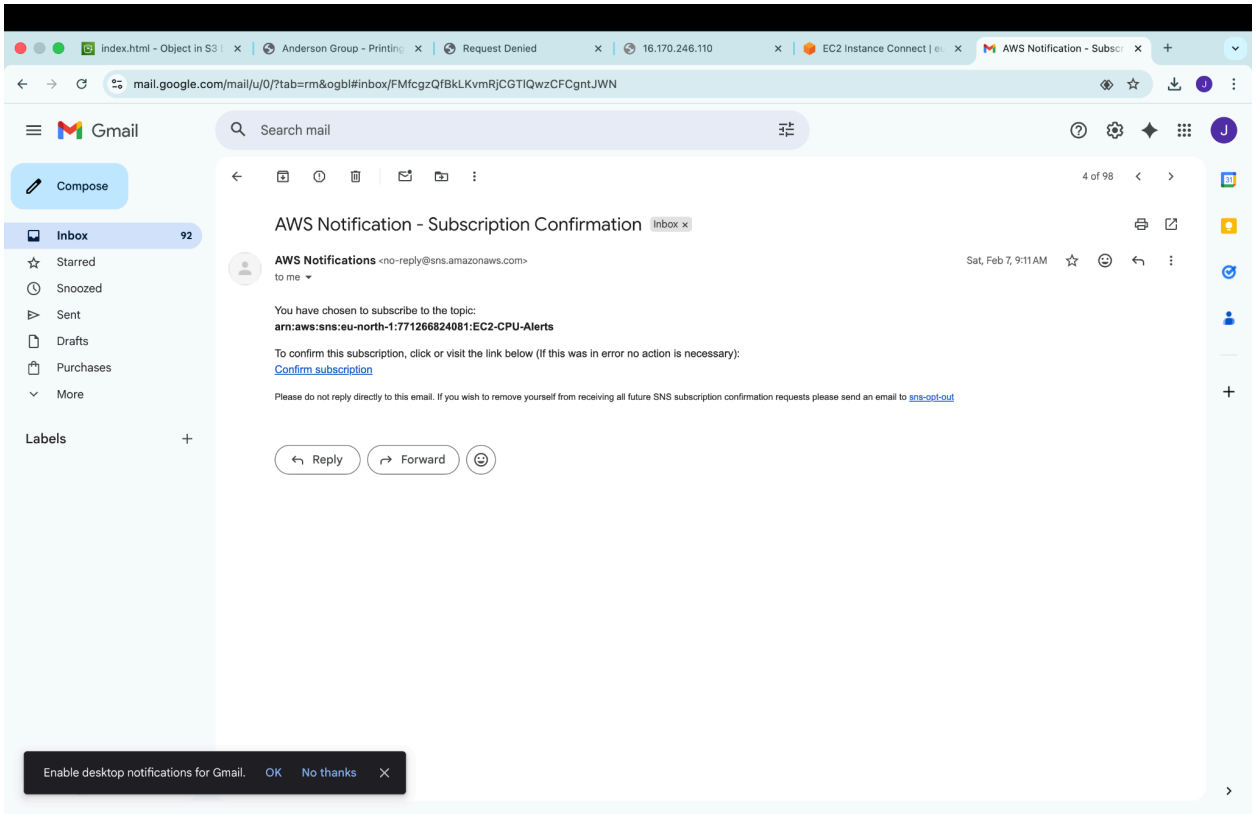


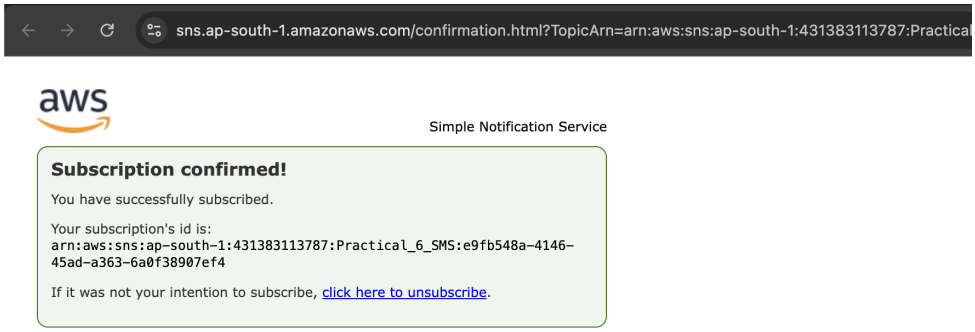


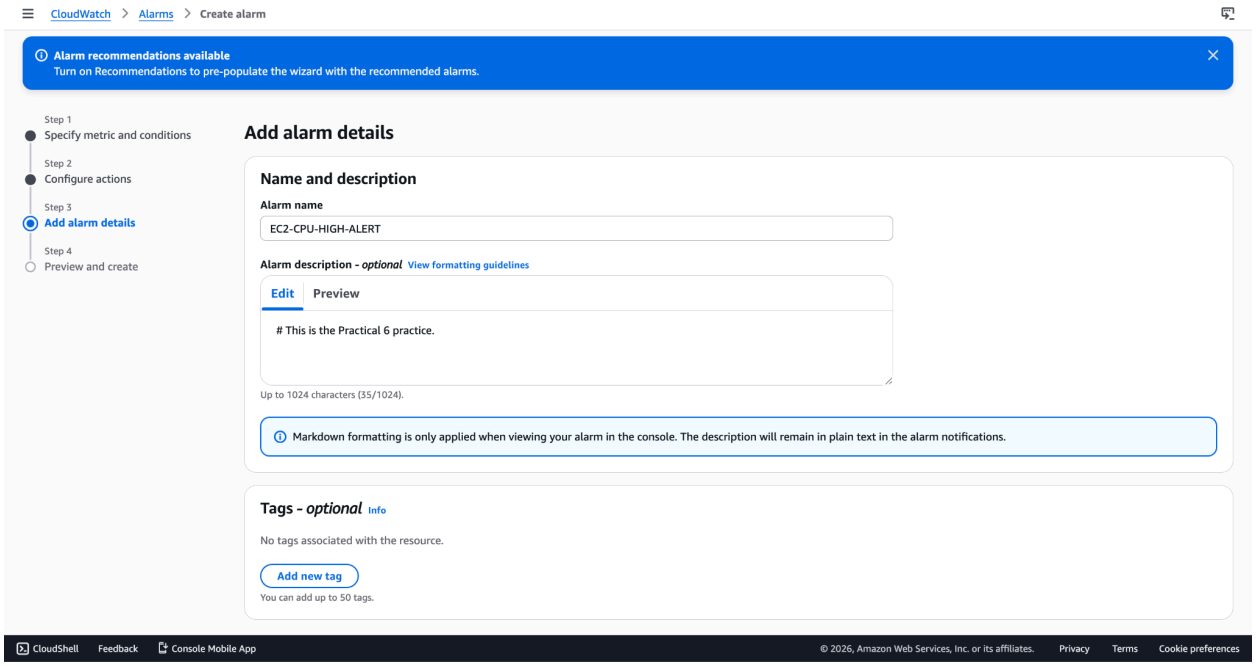
Configure Notification SNS

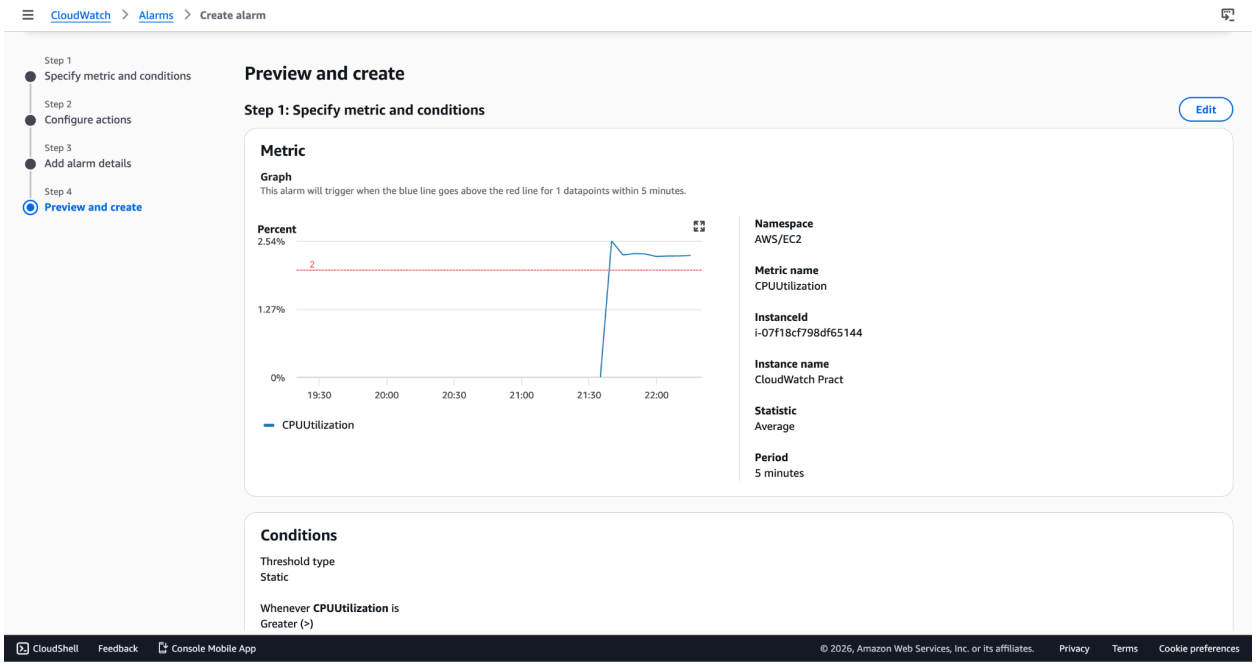


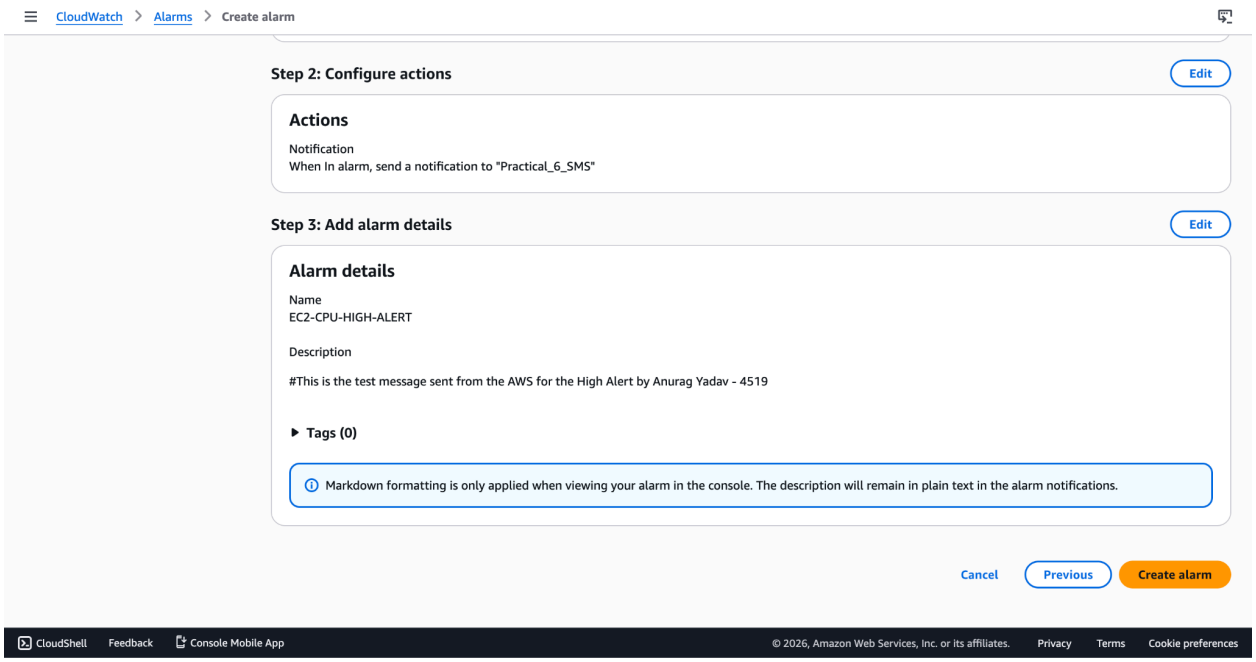
Confirm the subscription from the mail

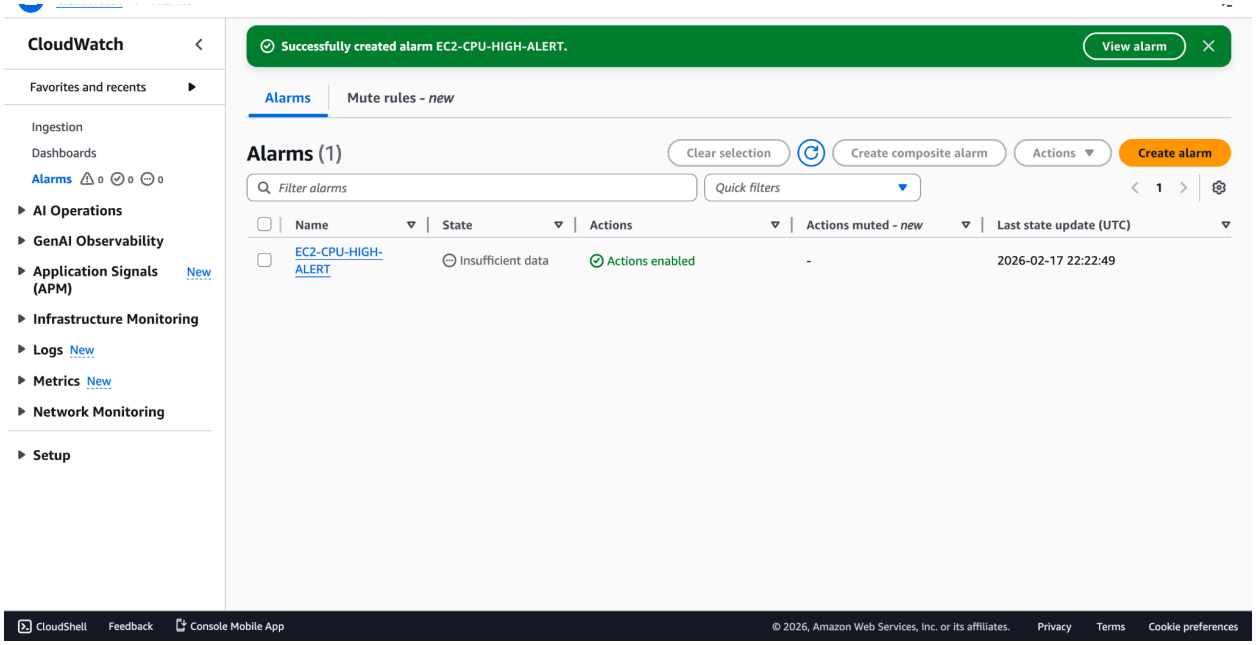

index.html - Object in S3
Anderson Group - Printing
Request Denied
16.170.246.110
EC2 Instance Connect | eu
AWS Notification - Subscr
mail.google.com/mail/u/0/?tab=rm&ogbl#inbox/FMfcgzQfBkLKvmRjCGTlQwzCFCgntJWN
Gmail
Search mail
Compose
Inbox 92
Starred
Snoozed
Sent
Drafts
Purchases
More
Labels
4 of 98
AWS Notification - Subscription Confirmation
Inbox ×
AWS Notifications <no-reply@sns.amazonaws.com>
to me
Sat, Feb 7, 9:11 AM
You have chosen to subscribe to the topic:
arn:aws:sns:eu-north-1:771266824081:EC2-CPU-Alerts
To confirm this subscription, click or visit the link below (If this was in error no action is necessary):
Confirm subscription
Please do not reply directly to this email. If you wish to remove yourself from receiving all future SNS subscription confirmation requests please send an email to sns-opt-out
Reply
Forward
Enable desktop notifications for Gmail.
OK
No thanks

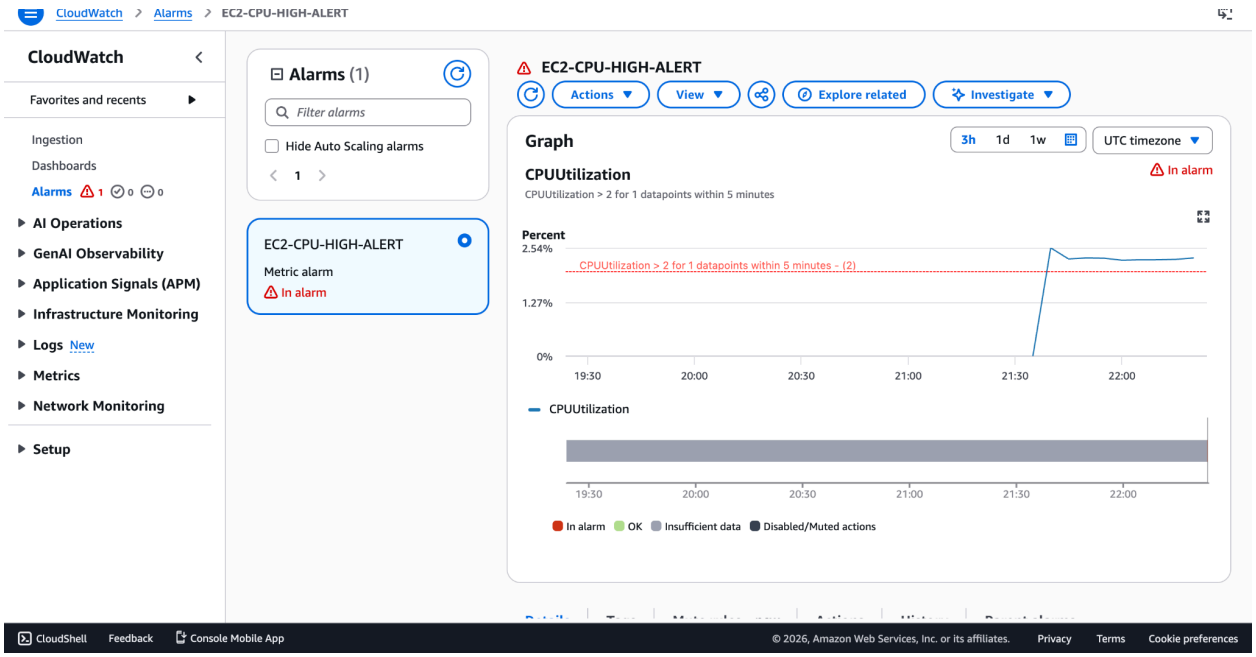

sns.ap-south-1.amazonaws.com/confirmation.html?TopicArn=arn:aws:sns:ap-south-1:431383113787:Practica
aws
Simple Notification Service
Subscription confirmed!
You have successfully subscribed.
Your subscription's id is:
arn:aws:sns:ap-south-1:431383113787:Practical_6_SMS:e9fb548a-4146-45ad-a363-6a0f38907ef4
If it was not your intention to subscribe, click here to unsubscribe.

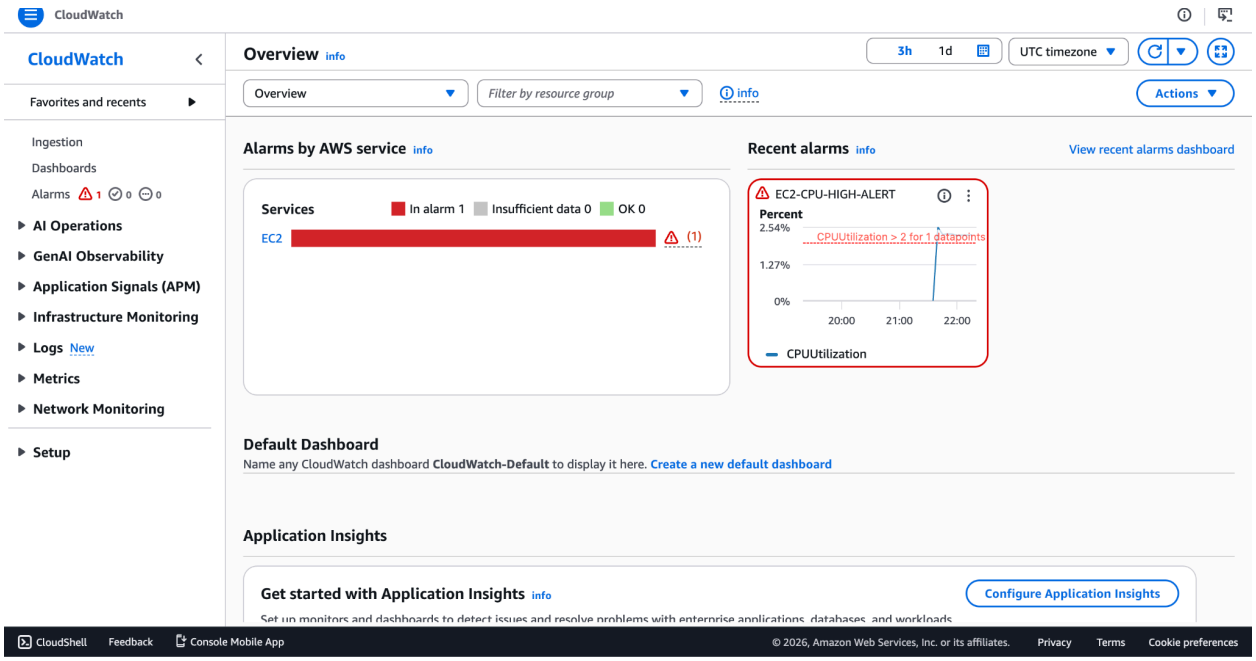

CloudWatch > Alarms > Create alarm
Alarm recommendations available
Turn on Recommendations to pre-populate the wizard with the recommended alarms.
Step 1
Specify metric and conditions
Step 2
Configure actions
Step 3
Add alarm details
Step 4
Preview and create
Add alarm details
Name and description
Alarm name
EC2-CPU-HIGH-ALERT
Alarm description - optional View formatting guidelines
Edit
Preview
This is the Practical 6 practice.
Up to 1024 characters (35/1024).
Markdown formatting is only applied when viewing your alarm in the console. The description will remain in plain text in the alarm notifications.
Tags - optional Info
No tags associated with the resource.
Add new tag
You can add up to 50 tags.
CloudShell
Feedback
Console Mobile App
© 2026, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

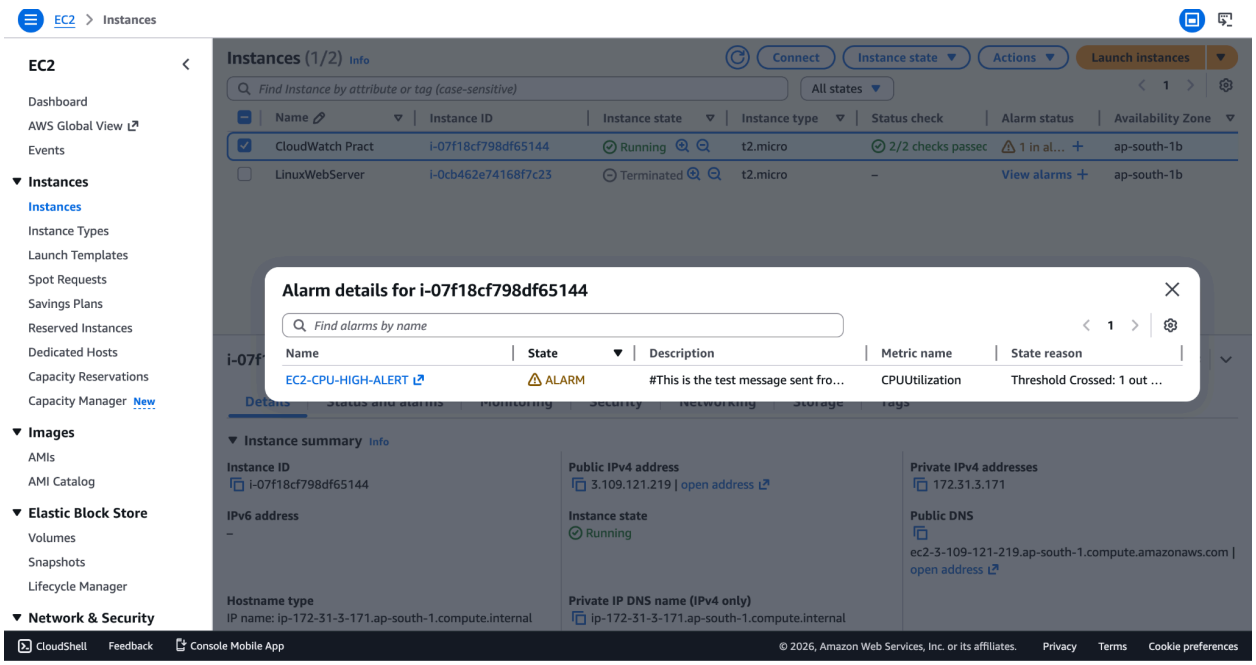

CloudWatch > Alarms > Create alarm
Step 1
Specify metric and conditions
Step 2
Configure actions
Step 3
Add alarm details
Step 4
Preview and create
Preview and create
Step 1: Specify metric and conditions
Edit
Metric
Graph
This alarm will trigger when the blue line goes above the red line for 1 datapoints within 5 minutes.
Percent
2.54%
2
1.27%
0%
19:30
20:00
20:30
21:00
21:30
22:00
CPUUtilization
Namespace
AWS/EC2
Metric name
CPUUtilization
InstanceId
i-07f18cf798df65144
Instance name
CloudWatch Pract
Statistic
Average
Period
5 minutes
Conditions
Threshold type
Static
Whenever CPUUtilization is
Greater (>)
CloudShell
Feedback
Console Mobile App
© 2026, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

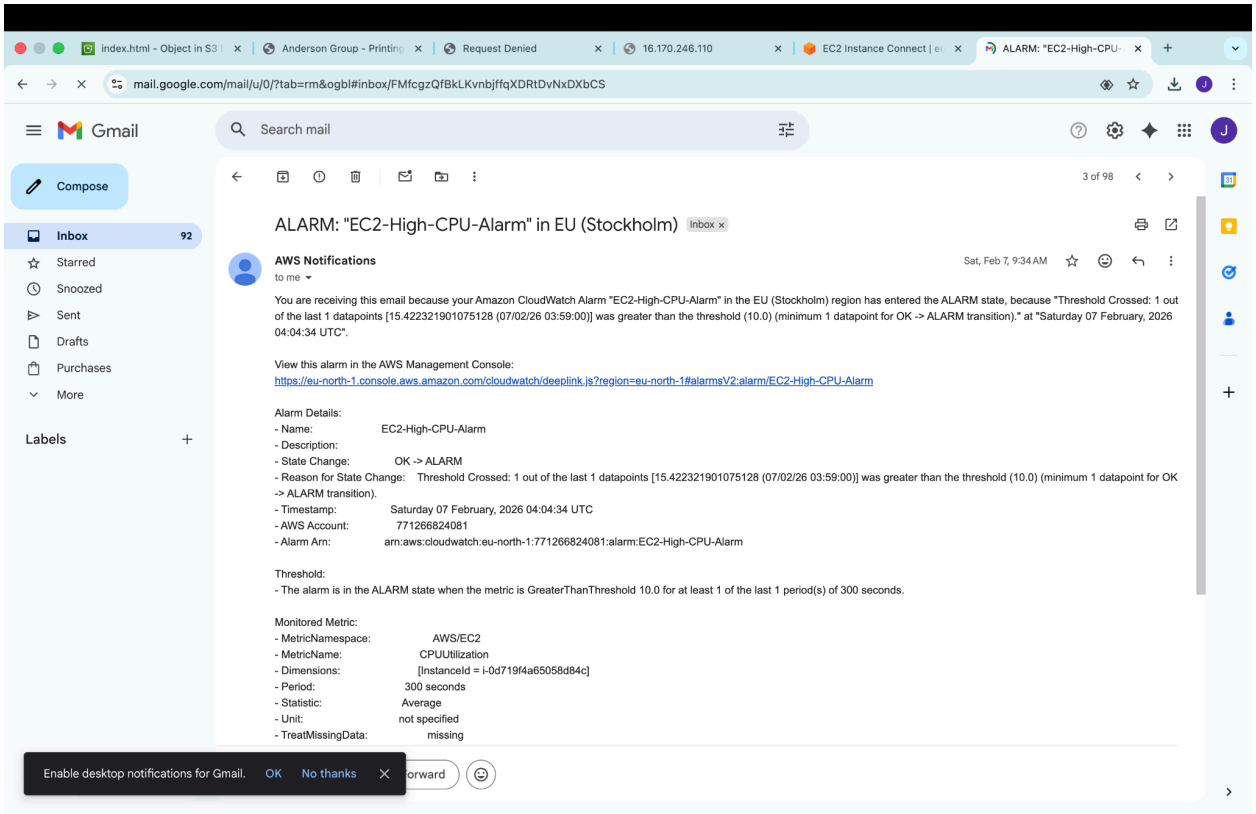

CloudWatch > Alarms > Create alarm
Step 2: Configure actions
Edit
Actions
Notification
When In alarm, send a notification to "Practical_6_SMS"
Step 3: Add alarm details
Edit
Alarm details
Name
EC2-CPU-HIGH-ALERT
Description
#This is the test message sent from the AWS for the High Alert by Anurag Yadav - 4519
Tags (0)
Markdown formatting is only applied when viewing your alarm in the console. The description will remain in plain text in the alarm notifications.
Cancel
Previous
Create alarm
CloudShell
Feedback
Console Mobile App
© 2026, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


CloudWatch
Favorites and recents
Ingestion
Dashboards
Alarms
AI Operations
GenAI Observability
Application Signals (APM) New
Infrastructure Monitoring
Logs New
Metrics New
Network Monitoring
Setup
Successfully created alarm EC2-CPU-HIGH-ALERT.
View alarm
Alarms
Mute rules - new
Alarms (1)
Clear selection
Create composite alarm
Actions
Create alarm
Filter alarms
Quick filters
Name
State
Actions
Actions muted - new
Last state update (UTC)
EC2-CPU-HIGH-ALERT
Insufficient data
Actions enabled
-
2026-02-17 22:22:49
CloudShell
Feedback
Console Mobile App
© 2026, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


CloudWatch > Alarms > EC2-CPU-HIGH-ALERT
CloudWatch
Favorites and recents
Ingestion
Dashboards
Alarms 1 0 0
AI Operations
GenAI Observability
Application Signals (APM)
Infrastructure Monitoring
Logs New
Metrics
Network Monitoring
Setup
Alarms (1)
Filter alarms
Hide Auto Scaling alarms
1
EC2-CPU-HIGH-ALERT
Metric alarm
In alarm
EC2-CPU-HIGH-ALERT
Actions
View
Explore related
Investigate
Graph
3h 1d 1w
UTC timezone
CPUUtilization
In alarm
CPUUtilization > 2 for 1 datapoints within 5 minutes
Percent
2.54%
1.27%
0%
CPUUtilization > 2 for 1 datapoints within 5 minutes - (2)
19:30 20:00 20:30 21:00 21:30 22:00
CPUUtilization
In alarm OK Insufficient data Disabled/Muted actions
CloudShell Feedback Console Mobile App
© 2026, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences


CloudWatch
CloudWatch
Favorites and recents
Ingestion
Dashboards
Alarms 1 0 0
AI Operations
GenAI Observability
Application Signals (APM)
Infrastructure Monitoring
Logs New
Metrics
Network Monitoring
Setup
Overview info
3h 1d
UTC timezone
Overview
Filter by resource group
info
Actions
Alarms by AWS service info
Services
In alarm 1 Insufficient data 0 OK 0
EC2
(1)
Recent alarms info
View recent alarms dashboard
EC2-CPU-HIGH-ALERT
Percent
2.54%
1.27%
0%
CPUUtilization > 2 for 1 datapoints
20:00 21:00 22:00
CPUUtilization
Default Dashboard
Name any CloudWatch dashboard CloudWatch-Default to display it here. Create a new default dashboard
Application Insights
Get started with Application Insights info
Configure Application Insights
Set up monitors and dashboards to detect issues and resolve problems with enterprise applications, databases, and workloads
CloudShell Feedback Console Mobile App
© 2026, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences





Conclusion: The CloudWatch monitoring and alarm configuration practical was performed successfully.