School of Computer Science, Engineering and Applications(SCSEA)
B.Tech TY (CCSA)
Subject : Fundamentals of Cloud Computing (P)

Name of the Student:	**Kshitij Khanka**	**PRN**	**20230802236**
Title of Practical :	**Implementing Fine-Grained Control on EC2 Start/Stop/Terminate Actions**		
Faculty Name:	**Dr. Swapnil Waghmare**	**Sign:**	

Introduction

In this lab, we explore the concept of fine-grained access control in AWS Identity and Access Management (IAM). By implementing selective permissions on Amazon EC2, we ensure that users have only the necessary privileges required for their tasks, reducing the risk of accidental or unauthorized actions.

Objectives

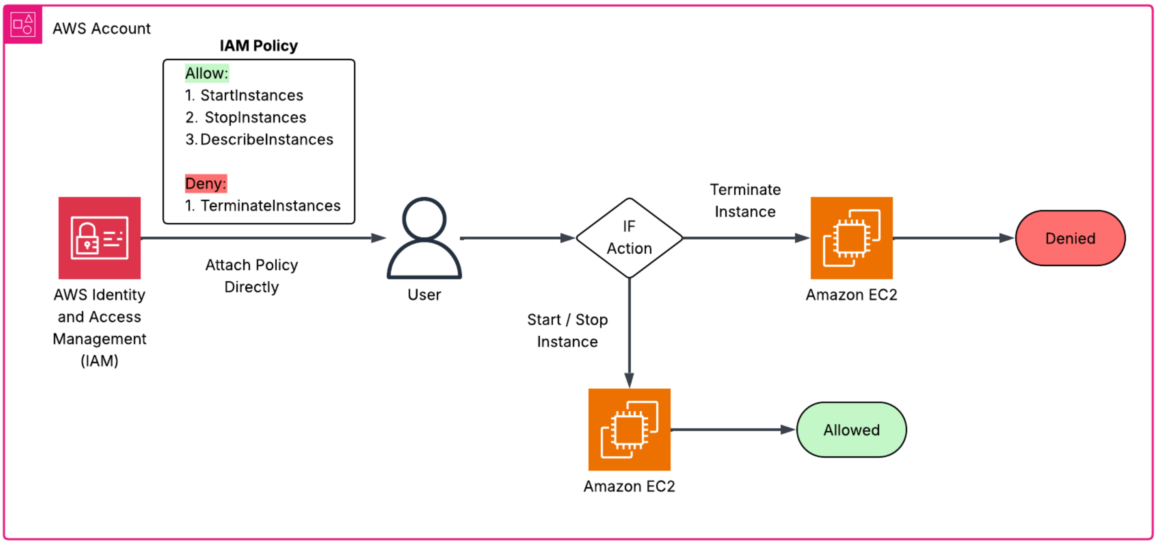
1. Create a user **ec2_operator** with restricted permissions.
2. Attach a custom policy that allows starting and stopping EC2 instances but explicitly denies terminating them.
3. Verify access by logging in as **ec2_operator** and testing the allowed and denied actions.
4. Understand how fine-grained permissions enhance resource protection in AWS.

D Y PATIL INTERNATIONAL UNIVERSITY
AKURDI PUNE

School of Computer Science, Engineering and Applications(SCSEA)
B.Tech TY (CCSA)
Subject : Fundamentals of Cloud Computing (P)

Name of the Student:	**Kshitij Khanka**	**PRN**	**20230802236**
Title of Practical :	**Implementing Fine-Grained Control on EC2 Start/Stop/Terminate Actions**		
Faculty Name:	**Dr. Swapnil Waghmare**	**Sign:**	

Architecture Diagram



D Y PATIL
INTERNATIONAL
UNIVERSITY
AKURDI PUNE

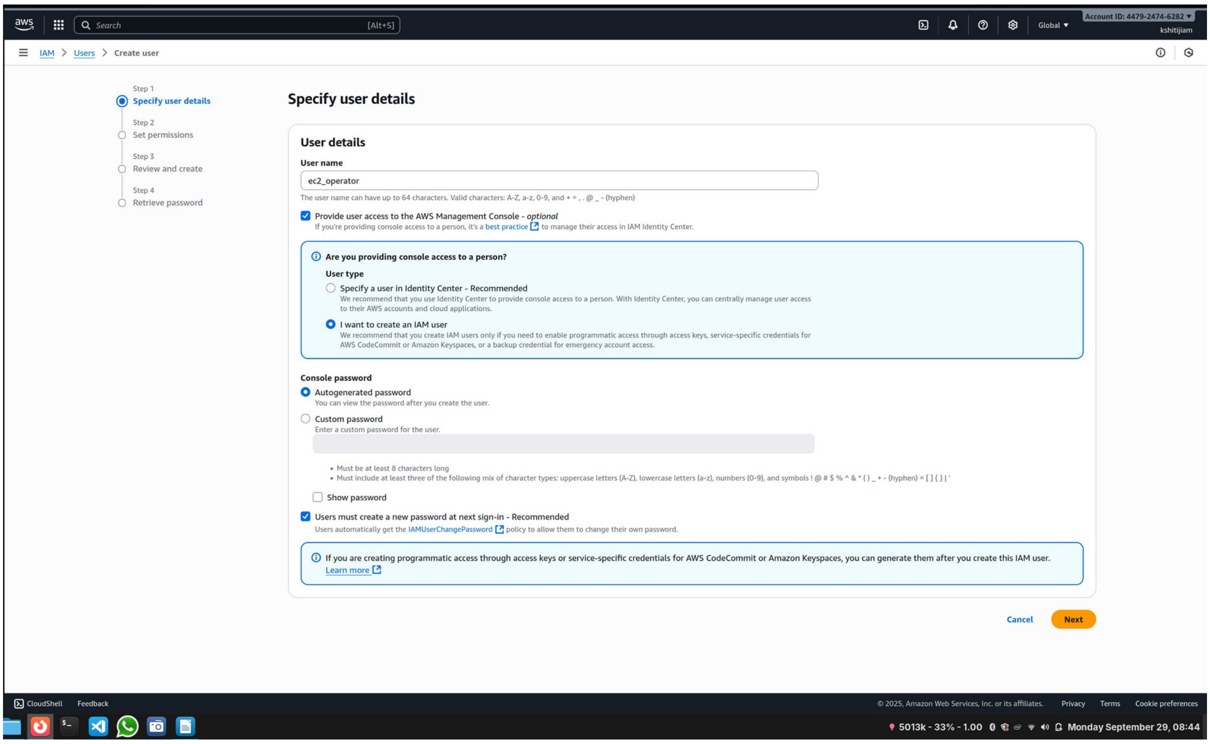
School of Computer Science, Engineering and Applications(SCSEA)
B.Tech TY (CCSA)
Subject : Fundamentals of Cloud Computing (P)

Name of the Student:	**Kshitij Khanka**	**PRN**	**20230802236**
Title of Practical :	**Implementing Fine-Grained Control on EC2 Start/Stop/Terminate Actions**		
Faculty Name:	**Dr. Swapnil Waghmare**	**Sign:**	

Procedure:

1. Creating User

- Go to IAM Dashboard > Users > Create User.
- User name: ec2_operator, Check “Provide access to AWS Management Console”, User Type: IAM user, Check “User must create a new password at next sign-in”



Specify user details

User details

User name

ec2_operator

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.

Are you providing console access to a person?

User type

○ Specify a user in Identity Center - Recommended
We recommend that you use Identity Center to provide console access to a person. With Identity Center, you can centrally manage user access to their AWS accounts and cloud applications.

● I want to create an IAM user
We recommend that you create IAM users only if you need to enable programmatic access through access keys, service-specific credentials for AWS CodeCommit or Amazon Keyspaces, or a backup credential for emergency account access.

Console password

● Autogenerated password
You can view the password after you create the user.

○ Custom password
Enter a custom password for the user.

- Must be at least 8 characters long
- Must include at least three of the following mix of character types: uppercase letters (A-Z), lowercase letters (a-z), numbers (0-9), and symbols ! @ # $ % ^ & * ( ) _ + - (hyphen) = [ ] { } | '

□ Show password

☑ Users must create a new password at next sign-in - Recommended
Users automatically get the IAMUserChangePassword policy to allow them to change their own password.

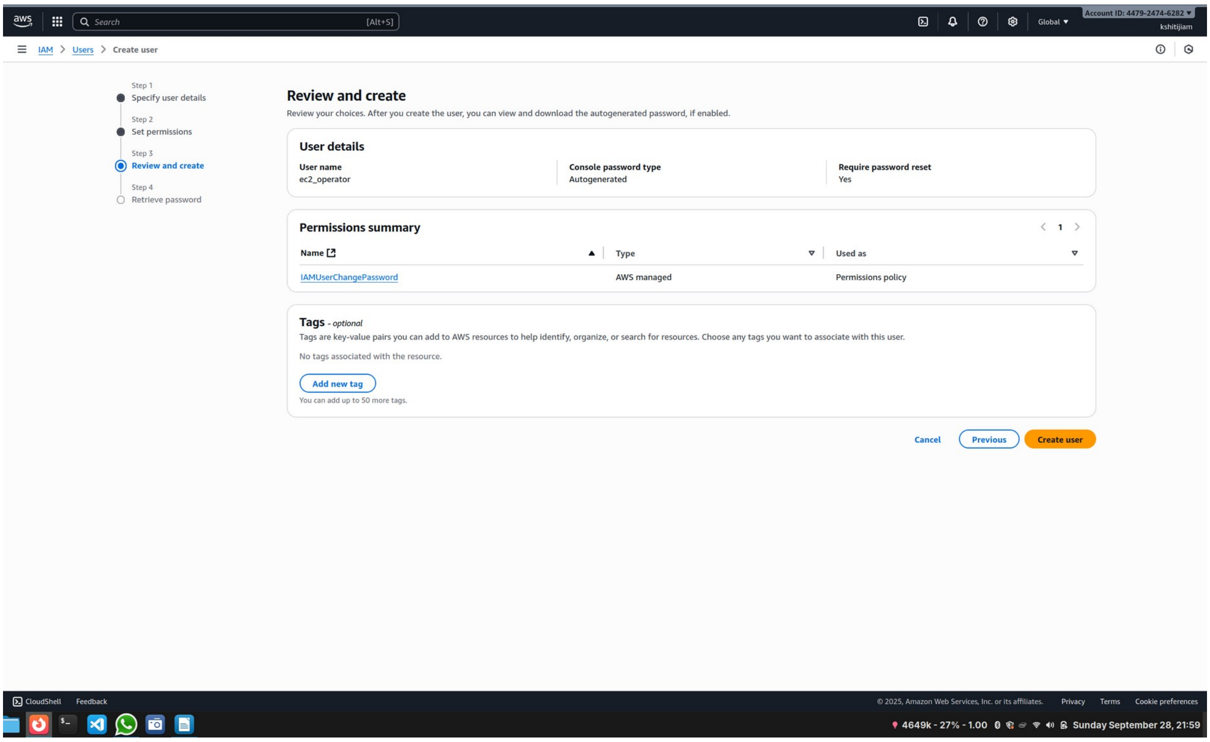
If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after you create this IAM user. Learn more

D Y PATIL
INTERNATIONAL
UNIVERSITY
AKURDI PUNE

School of Computer Science, Engineering and Applications(SCSEA)
B.Tech TY (CCSA)
Subject : Fundamentals of Cloud Computing (P)

Name of the Student:	**Kshitij Khanka**	**PRN**	**20230802236**
Title of Practical :	**Implementing Fine-Grained Control on EC2 Start/Stop/Terminate Actions**		
Faculty Name:	**Dr. Swapnil Waghmare**	**Sign:**	

- Set Permissions: We will attach later, Review and Create User.



Step 1
● Specify user details
Step 2
● Set permissions
Step 3
◉ Review and create
Step 4
○ Retrieve password

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	Console password type	Require password reset
ec2_operator	Autogenerated	Yes

Permissions summary

Name	Type	Used as
IAMUserChangePassword	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.

D Y PATIL INTERNATIONAL UNIVERSITY
AKURDI PUNE

School of Computer Science, Engineering and Applications(SCSEA)
B.Tech TY (CCSA)
Subject : Fundamentals of Cloud Computing (P)

Name of the Student:	**Kshitij Khanka**	**PRN**	**20230802236**
Title of Practical :	**Implementing Fine-Grained Control on EC2 Start/Stop/Terminate Actions**		
Faculty Name:	**Dr. Swapnil Waghmare**	**Sign:**	

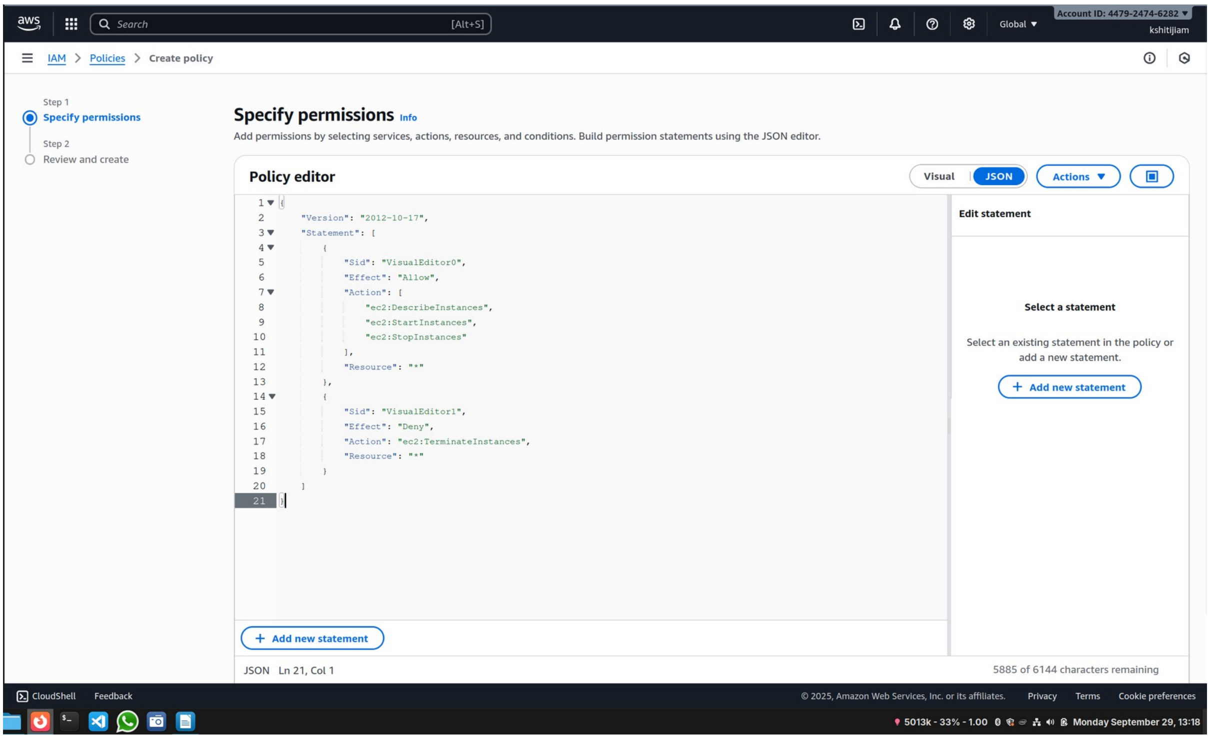
2. Create a custom Policy

- Go to IAM Dashboard > Policies > Create Policy
- We create a policy that gives granular access to user, here user should be able to Start and Stop EC2 instance but not Terminate it.
- In policy editor, Under Visual mode, Select Service: EC2, Effect: Allow. Actions Allowed: Under Write Actions > **StartInstances**, **StopInstances**, **DescribeInstances** . Resources: All Resources.
- AWS has created granular permissions spread across List, Read, Write, Permission Management and Tagging. It also allows us to select resources on which this policy is applicable.
- After selecting permissions, we can choose whether to allow or deny it.
- So in the first half, we allowed 2 actions, here we want to deny an action. Click on Add More Permissions, Select Service: EC2, Effect: Deny. Actions Denied: **TerminateInstances**, Resources: All Resources.

School of Computer Science, Engineering and Applications(SCSEA)
B.Tech TY (CCSA)
Subject : Fundamentals of Cloud Computing (P)

Name of the Student:	**Kshitij Khanka**	**PRN**	**20230802236**
Title of Practical :	**Implementing Fine-Grained Control on EC2 Start/Stop/Terminate Actions**		
Faculty Name:	**Dr. Swapnil Waghmare**	**Sign:**	

- JSON view of our Policy:



Specify permissions Info

Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.

Policy editor

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:StartInstances",
                "ec2:StopInstances"
            ],
            "Resource": "*"
        },
        {
            "Sid": "VisualEditor1",
            "Effect": "Deny",
            "Action": "ec2:TerminateInstances",
            "Resource": "*"
        }
    ]
}
```

Edit statement

Select a statement

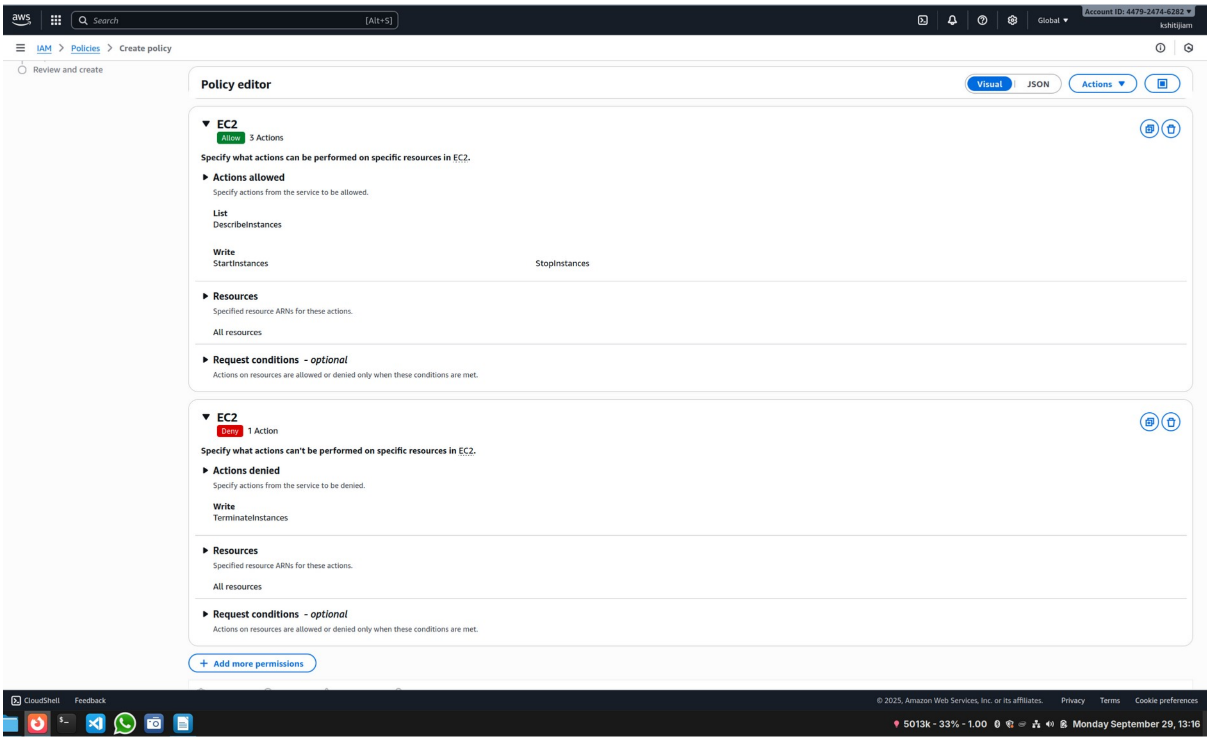
Select an existing statement in the policy or add a new statement.

JSON Ln 21, Col 1

5885 of 6144 characters remaining

CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
5013k - 33% - 1.00
Monday September 29, 13:18

- Visual Editor view of our Policy:



Policy editor

▼ EC2
Allow 3 Actions

Specify what actions can be performed on specific resources in EC2.

▶ Actions allowed
Specify actions from the service to be allowed.

List
DescribeInstances

Write
StartInstances StopInstances

▶ Resources
Specified resource ARNs for these actions.

All resources

▶ Request conditions *- optional*
Actions on resources are allowed or denied only when these conditions are met.

▼ EC2
Deny 1 Action

Specify what actions can't be performed on specific resources in EC2.

▶ Actions denied
Specify actions from the service to be denied.

Write
TerminateInstances

▶ Resources
Specified resource ARNs for these actions.

All resources

▶ Request conditions *- optional*
Actions on resources are allowed or denied only when these conditions are met.

+ Add more permissions

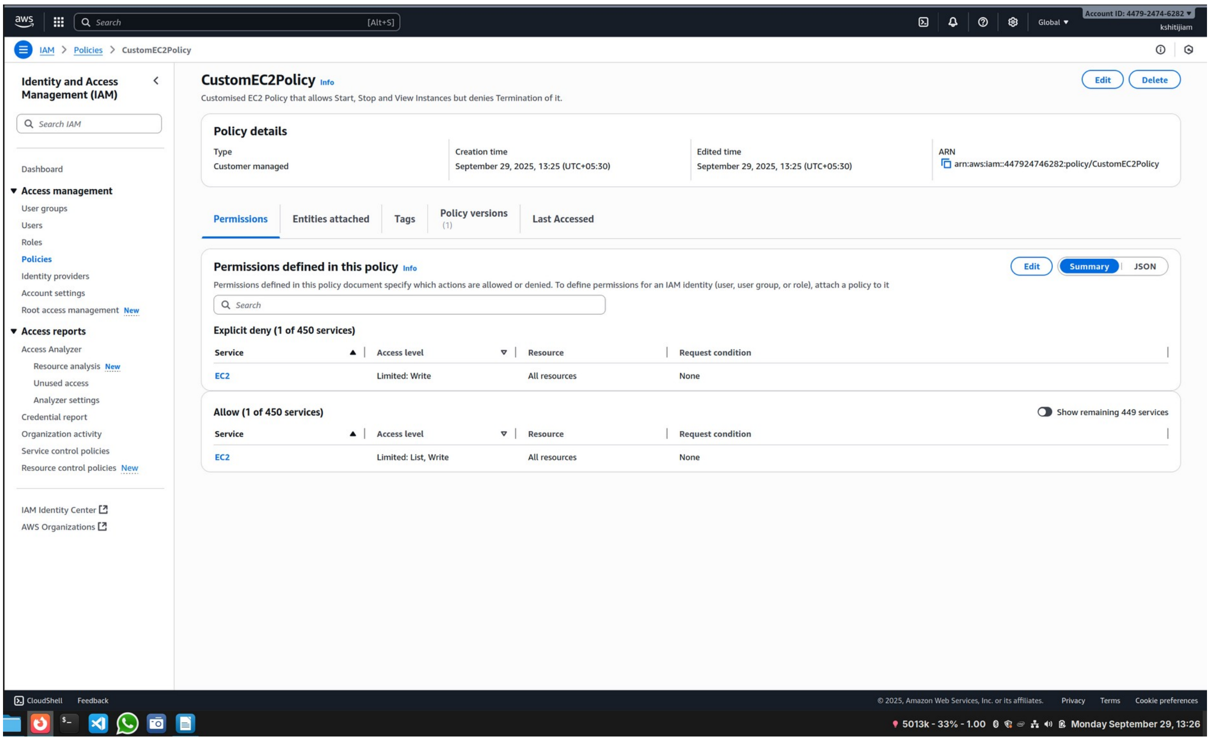
- Go to Review & Create, Assign a Policy name and description.

D Y PATIL INTERNATIONAL UNIVERSITY
AKURDI PUNE

School of Computer Science, Engineering and Applications(SCSEA)
B.Tech TY (CCSA)
Subject : Fundamentals of Cloud Computing (P)

Name of the Student:	**Kshitij Khanka**	**PRN**	**20230802236**
Title of Practical :	**Implementing Fine-Grained Control on EC2 Start/Stop/Terminate Actions**		
Faculty Name:	**Dr. Swapnil Waghmare**	**Sign:**	

- Create Policy.



CustomEC2Policy Info

Customised EC2 Policy that allows Start, Stop and View Instances but denies Termination of it.

Policy details

Type	Creation time	Edited time	ARN
Customer managed	September 29, 2025, 13:25 (UTC+05:30)	September 29, 2025, 13:25 (UTC+05:30)	arn:aws:iam::447924746282:policy/CustomEC2Policy

Permissions defined in this policy Info

Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it

Explicit deny (1 of 450 services)

Service	Access level	Resource	Request condition
EC2	Limited: Write	All resources	None

Allow (1 of 450 services)

Service	Access level	Resource	Request condition
EC2	Limited: List, Write	All resources	None

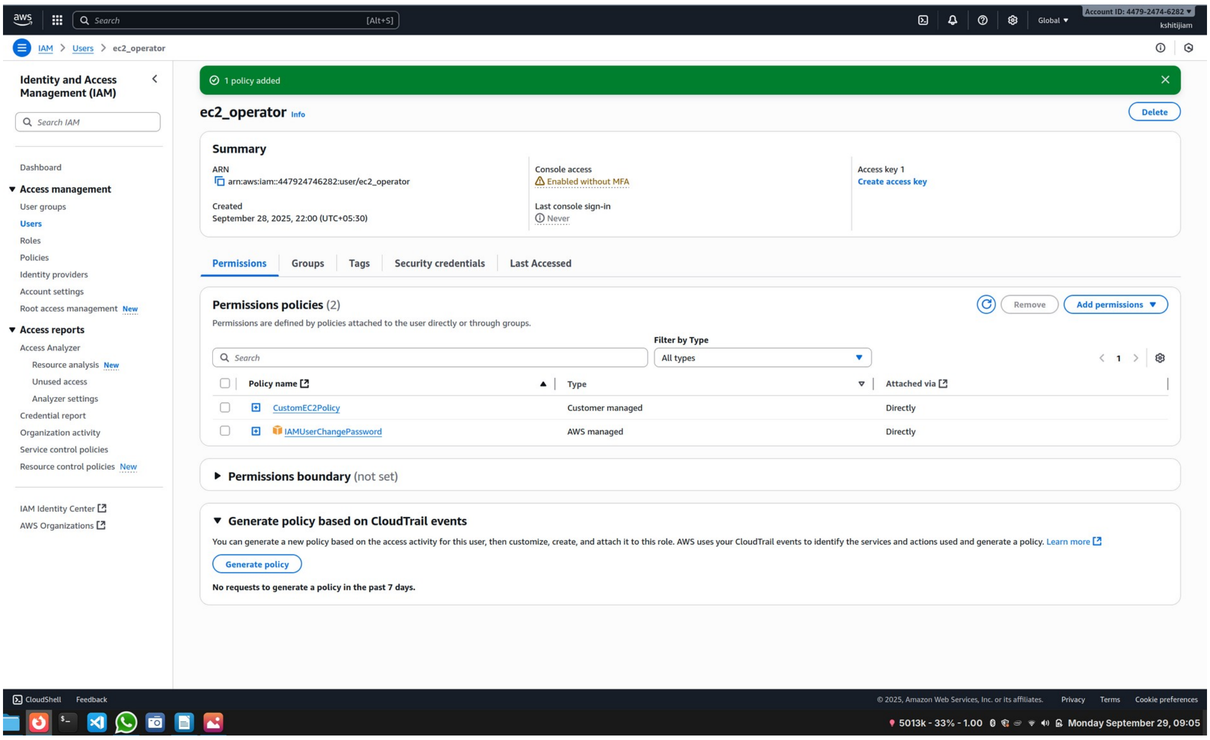
3. Attaching Custom Policy to User

- Go to IAM Dashboard > User > Click on ec2_operator > Add Permission > Attach Policies Directly

School of Computer Science, Engineering and Applications(SCSEA)
B.Tech TY (CCSA)
Subject : Fundamentals of Cloud Computing (P)

Name of the Student:	**Kshitij Khanka**	**PRN**	**20230802236**
Title of Practical :	**Implementing Fine-Grained Control on EC2 Start/Stop/Terminate Actions**		
Faculty Name:	**Dr. Swapnil Waghmare**	**Sign:**	

- On Filter Type: Customer Managed > Select our Custom Policy: CustomEC2Policy > Next > Add Permissions.
- Finally, the ec2_operator should look like this.



1 policy added

ec2_operator Info

Summary

ARN
arn:aws:iam::447924746282:user/ec2_operator

Created
September 28, 2025, 22:00 (UTC+05:30)

Console access
Enabled without MFA

Last console sign-in
Never

Access key 1
Create access key

Permissions policies (2)

Permissions are defined by policies attached to the user directly or through groups.

Filter by Type: All types

Policy name	Type	Attached via
CustomEC2Policy	Customer managed	Directly
IAMUserChangePassword	AWS managed	Directly

Permissions boundary (not set)

Generate policy based on CloudTrail events

You can generate a new policy based on the access activity for this user, then customize, create, and attach it to this role. AWS uses your CloudTrail events to identify the services and actions used and generate a policy. Learn more

No requests to generate a policy in the past 7 days.

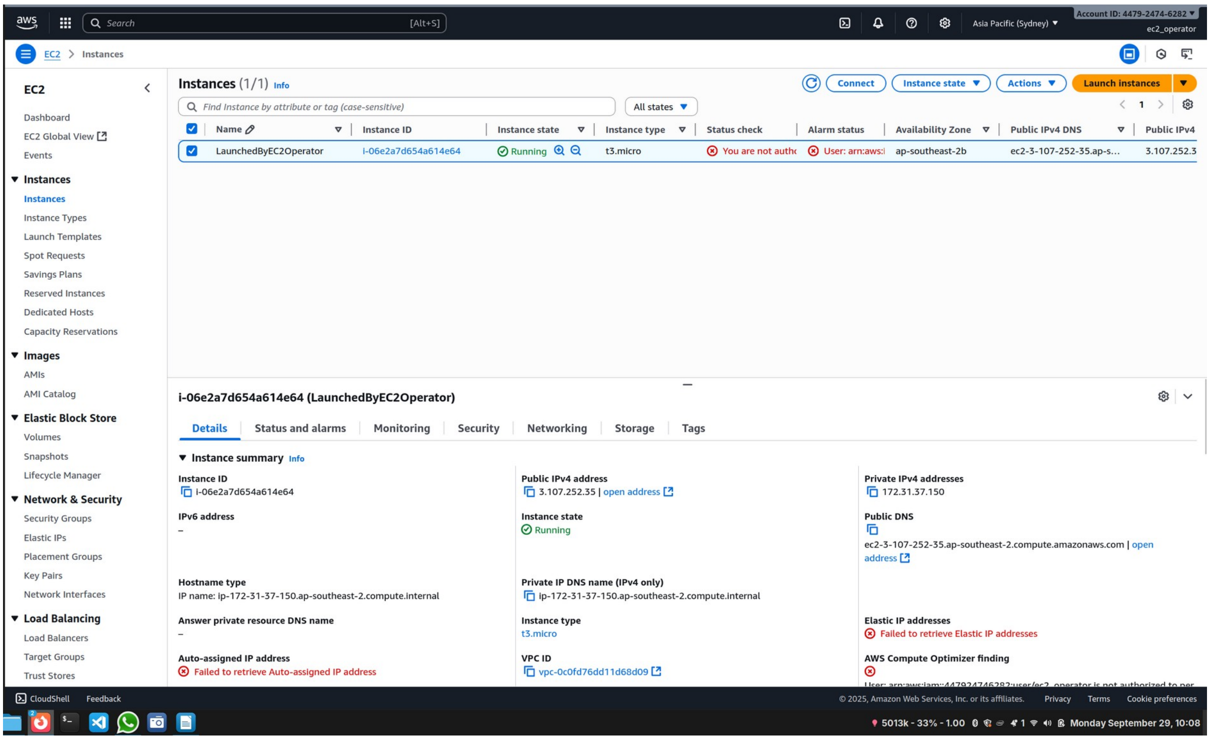
D Y PATIL INTERNATIONAL UNIVERSITY
AKURDI PUNE

School of Computer Science, Engineering and Applications(SCSEA)
B.Tech TY (CCSA)
Subject : Fundamentals of Cloud Computing (P)

Name of the Student:	**Kshitij Khanka**	**PRN**	**20230802236**
Title of Practical :	**Implementing Fine-Grained Control on EC2 Start/Stop/Terminate Actions**		
Faculty Name:	**Dr. Swapnil Waghmare**	**Sign:**	

4. Testing our granular policy

- Log in as ec2_operator > Go To EC2 Dashboard > Launch Instance with default settings.
- Launch EC2 with default settings.



Instances (1/1) Info

Find Instance by attribute or tag (case-sensitive)

☑	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4
☑	LaunchedByEC2Operator	i-06e2a7d654a614e64	Running	t3.micro	⊗ You are not authc	⊗ User: arn:aws:i	ap-southeast-2b	ec2-3-107-252-35.ap-s...	3.107.252.3

i-06e2a7d654a614e64 (LaunchedByEC2Operator)

Instance summary Info

Instance ID
i-06e2a7d654a614e64

IPv6 address
–

Hostname type
IP name: ip-172-31-37-150.ap-southeast-2.compute.internal

Answer private resource DNS name
–

Auto-assigned IP address
⊗ Failed to retrieve Auto-assigned IP address

Public IPv4 address
3.107.252.35 | open address

Instance state
Running

Private IP DNS name (IPv4 only)
ip-172-31-37-150.ap-southeast-2.compute.internal

Instance type
t3.micro

VPC ID
vpc-0c0fd76dd11d68d09

Private IPv4 addresses
172.31.37.150

Public DNS
ec2-3-107-252-35.ap-southeast-2.compute.amazonaws.com | open address

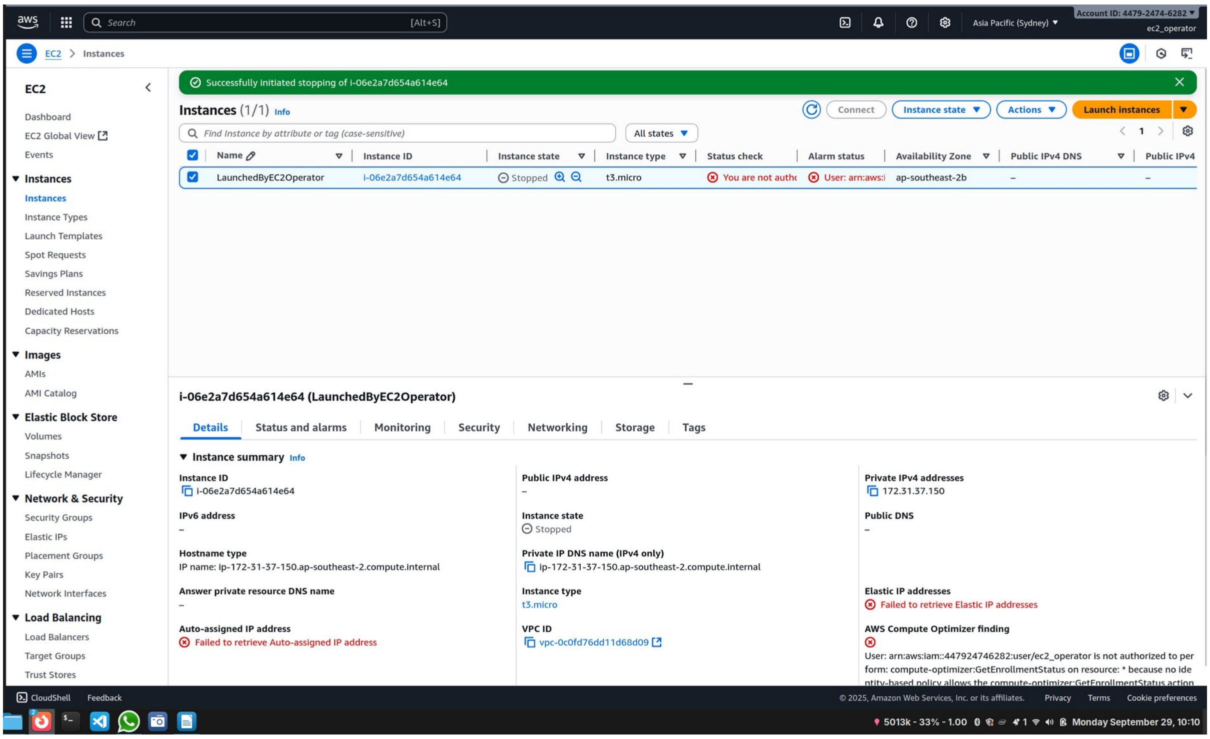
Elastic IP addresses
⊗ Failed to retrieve Elastic IP addresses

AWS Compute Optimizer finding
⊗
User: arn:aws:iam::447924746282:user/ec2_operator is not authorized to per

School of Computer Science, Engineering and Applications(SCSEA)
B.Tech TY (CCSA)
Subject : Fundamentals of Cloud Computing (P)

Name of the Student:	**Kshitij Khanka**	**PRN**	**20230802236**
Title of Practical :	**Implementing Fine-Grained Control on EC2 Start/Stop/Terminate Actions**		
Faculty Name:	**Dr. Swapnil Waghmare**	**Sign:**	

- Now, Test whether user can Stop running instance. Select instance > Instance State > Stop Instance



Successfully initiated stopping of i-06e2a7d654a614e64

Instances (1/1)

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4
LaunchedByEC2Operator	i-06e2a7d654a614e64	Stopped	t3.micro	You are not authc	User: arn:aws:i	ap-southeast-2b	–	–

i-06e2a7d654a614e64 (LaunchedByEC2Operator)

Instance summary

Instance ID: i-06e2a7d654a614e64

IPv6 address: –

Hostname type: IP name: ip-172-31-37-150.ap-southeast-2.compute.internal

Answer private resource DNS name: –

Auto-assigned IP address: Failed to retrieve Auto-assigned IP address

Public IPv4 address: –

Instance state: Stopped

Private IP DNS name (IPv4 only): ip-172-31-37-150.ap-southeast-2.compute.internal

Instance type: t3.micro

VPC ID: vpc-0c0fd76dd11d68d09

Private IPv4 addresses: 172.31.37.150

Public DNS: –

Elastic IP addresses: Failed to retrieve Elastic IP addresses

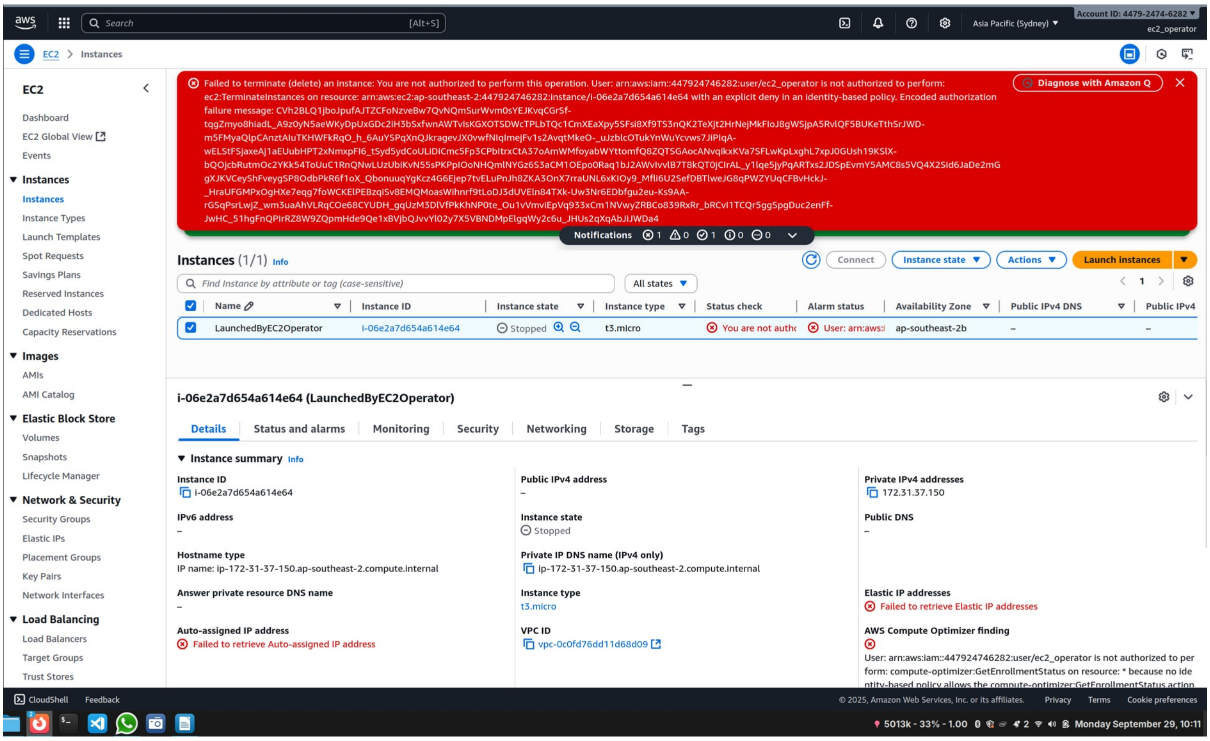
AWS Compute Optimizer finding: User: arn:aws:iam::447924746282:user/ec2_operator is not authorized to perform: compute-optimizer:GetEnrollmentStatus on resource: * because no identity-based policy allows the compute-optimizer:GetEnrollmentStatus action

- Now, Test whether user can Terminate an instance. Select instance > Instance State > Terminate Instance

D Y PATIL INTERNATIONAL UNIVERSITY
AKURDI PUNE

School of Computer Science, Engineering and Applications(SCSEA)
B.Tech TY (CCSA)
Subject : Fundamentals of Cloud Computing (P)

Name of the Student:	**Kshitij Khanka**	**PRN**	**20230802236**
Title of Practical :	**Implementing Fine-Grained Control on EC2 Start/Stop/Terminate Actions**		
Faculty Name:	**Dr. Swapnil Waghmare**	**Sign:**	



⊗ Failed to terminate (delete) an instance: You are not authorized to perform this operation. User: arn:aws:iam::447924746282:user/ec2_operator is not authorized to perform: ec2:TerminateInstances on resource: arn:aws:ec2:ap-southeast-2:447924746282:instance/i-06e2a7d654a614e64 with an explicit deny in an identity-based policy. Encoded authorization failure message: CVh2BLQ1jboJpufAJTZCFoNzveBw7QvNQmSurWvm0sYEJKvqCGrSf-tqgZmyo8hiadL_A9z0yN5aeWKyDpUxGDc2iH3bSxfwnAWTvIsKGXOTSDWcTPLbTQc1CmXEaXpy5SFsi8Xf9TS3nQK2TeXjt2HrNejMkFIoJ8gWSjpA5RvlQF5BUKeTthSrJWD-m5FMyaQlpCAnztAIuTKHWFkRqO_h_6AuYSPqXnQJkragevJX0vwfNIqImejFv1s2AvqtMkeO-_uJzblcOTukYnWuYcvws7JiPIqA-wELStFSjaxeAj1aEUubHPT2xNmxpFI6_tSyd5ydCoULiDiCmc5Fp3CPbItrxCtA37oAmWMfoyabWYttomfQ8ZQTSGAocANvqikxKVa7SFLwKpLxghL7xpJ0GUsh19KSlX-bQOjcbRutmOc2YKk54ToUuC1RnQNwLUzUbiKvN55sPKPpIOoNHQmlNYGz6S3aCM1OEpo0Raq1bJ2AWvIvvlB7T8kQT0jCIrAL_y1lqe5jyPqARTxs2JDSpEvmY5AMC8s5VQ4X2SId6JaDe2mGgXJKVCeyShFveygSP8OdbPkR6f1oX_QbonuuqYgKcz4G6Ejep7tvELuPnJh8ZKA3OnX7rraUNL6xKIOy9_Mfli6U2SefDBTlweJG8qPWZYUqCFBvHckJ-_HraUFGMPxOgHXe7eqg7foWCKElPEBzqiSv8EMQMoasWihnrf9tLoDJ3dUVEln84TXk-Uw3Nr6EDbfgu2eu-Ks9AA-rGSqPsrLwjZ_wm3uaAhVLRqCOe68CYUDH_gqUzM3DlVfPkKhNP0te_Ou1vVmviEpVq933xCm1NVwyZRBCo839RxRr_bRCvI1TCQr5ggSpgDuc2enFf-JwHC_51hgFnQPIrRZ8W9ZQpmHde9Qe1xBVjbQJvvYl02y7X5VBNDMpElgqWy2c6u_JHUs2qXqAbJiJWDa4

Instances (1/1) Info

Find Instance by attribute or tag (case-sensitive)

☑	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4
☑	LaunchedByEC2Operator	i-06e2a7d654a614e64	⊖ Stopped	t3.micro	⊗ You are not authc	⊗ User: arn:aws:i	ap-southeast-2b	–	–

i-06e2a7d654a614e64 (LaunchedByEC2Operator)

▼ Instance summary Info

Instance ID
i-06e2a7d654a614e64

IPv6 address
–

Hostname type
IP name: ip-172-31-37-150.ap-southeast-2.compute.internal

Answer private resource DNS name
–

Auto-assigned IP address
⊗ Failed to retrieve Auto-assigned IP address

Public IPv4 address
–

Instance state
⊖ Stopped

Private IP DNS name (IPv4 only)
ip-172-31-37-150.ap-southeast-2.compute.internal

Instance type
t3.micro

VPC ID
vpc-0c0fd76dd11d68d09

Private IPv4 addresses
172.31.37.150

Public DNS
–

Elastic IP addresses
⊗ Failed to retrieve Elastic IP addresses

AWS Compute Optimizer finding
⊗
User: arn:aws:iam::447924746282:user/ec2_operator is not authorized to perform: compute-optimizer:GetEnrollmentStatus on resource: * because no identity-based policy allows the compute-optimizer:GetEnrollmentStatus action

- Since, we are not allowed to Terminate Instance, AWS throws us an error when terminating it.

School of Computer Science, Engineering and Applications(SCSEA)
B.Tech TY (CCSA)
Subject : Fundamentals of Cloud Computing (P)

Name of the Student:	**Kshitij Khanka**	**PRN**	**20230802236**
Title of Practical :	**Implementing Fine-Grained Control on EC2 Start/Stop/Terminate Actions**		
Faculty Name:	**Dr. Swapnil Waghmare**	**Sign:**	

Conclusion

This lab demonstrated how fine-grained IAM policies can precisely control user actions on EC2 instances. By granting start and stop permissions while denying termination, we successfully prevented accidental deletion of critical resources. This exercise highlights the importance of implementing least-privilege access to maintain both security and operational reliability in cloud environments.