Name: Amar Kishor Kalbande

Internship: Cloud Computing

Virtual Internship (CODTECH)

TASK 4: IMPLEMENTATION OF IDENTITY AND ACCESS MANAGEMENT

INTERN ID: CT04DR2400

Cloud Plarform: Amazon Web Services (AWS)

Duration: 1 MONTH

Objective

The objective of this task is to implement AWS Identity and Access Management (IAM) policies to ensure secure access control by defining users, groups, permissions, and following AWS security best practices.

Introduction

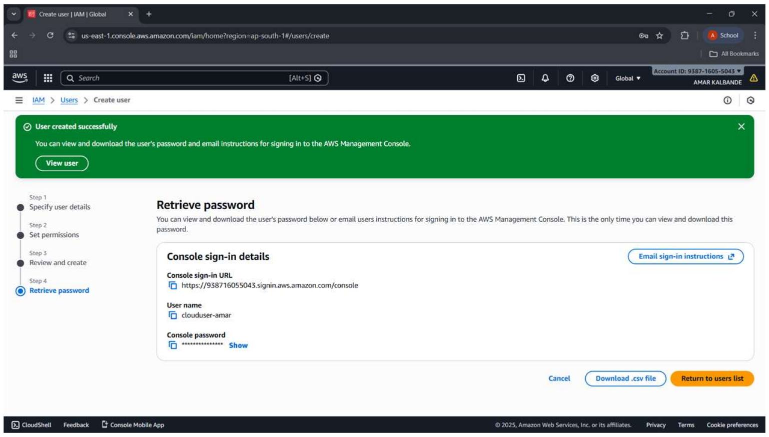
AWS Identity and Access Management (IAM) is a service that helps manage access to AWS resources securely. IAM allows creating users, groups, and permissions to control who can access AWS services and what actions they can perform.

Why Root Account Should Not Be Used

The root account has full administrative privileges and unrestricted access to all AWS services. Using the root account for daily tasks increases security risks. AWS recommends using the root account only for critical account-level operations and using IAM users for regular work

Steps Performed

1. Logged in using AWS Root Account.
2. Created an IAM user named clouduser-amar.



Create user | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/create
School
All Bookmarks
aws
Search
[Alt+S]
Global ▼
Account ID: 9387-1605-5043 ▼
AMAR KALBANDE
IAM > Users > Create user

User created successfully

You can view and download the user's password and email instructions for signing in to the AWS Management Console.

Retrieve password

You can view and download the user's password below or email users instructions for signing in to the AWS Management Console. This is the only time you can view and download this password.

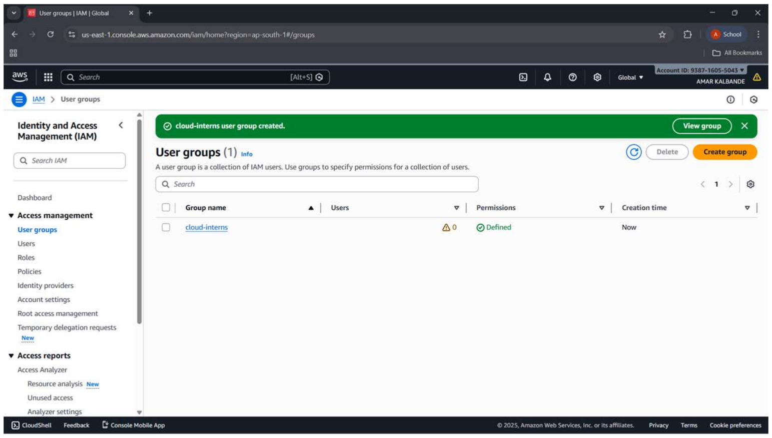
Console sign-in details

Console sign-in URL
https://938716055043.signin.aws.amazon.com/console

User name
clouduser-amar

Console password
****

3. Created an IAM group named cloud-interns.



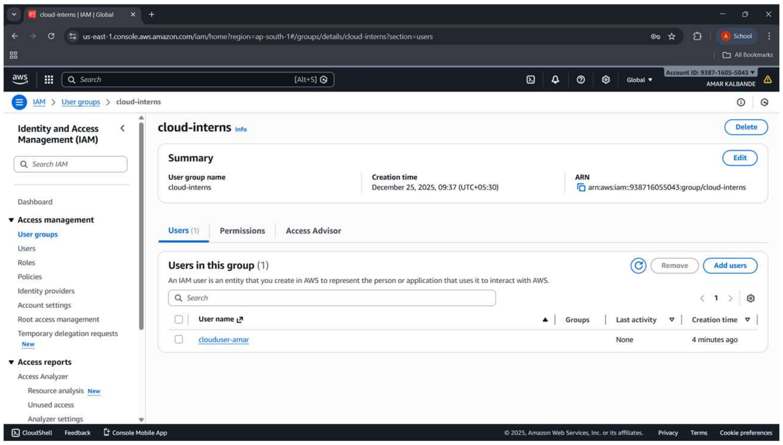
cloud-interns user group created.

User groups (1)

A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

□	Group name	Users	Permissions	Creation time
□	cloud-interns	⚠ 0	✓ Defined	Now

4. Added the IAM user to the group.



cloud-interns

Summary

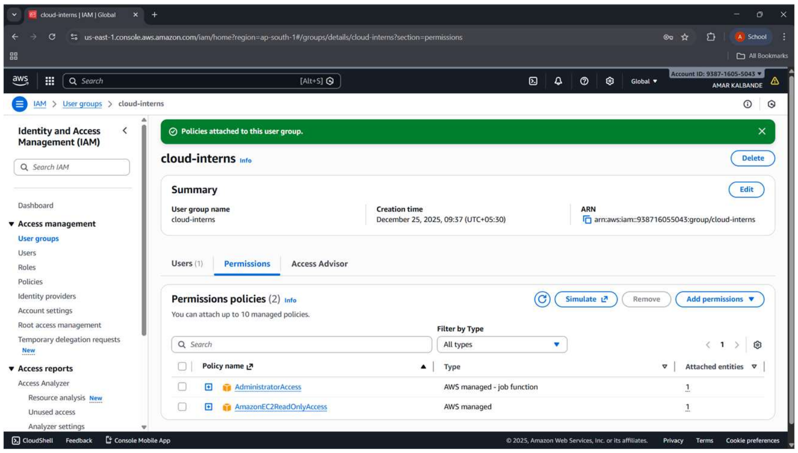
User group name: cloud-interns
Creation time: December 25, 2025, 09:37 (UTC+05:30)
ARN: arn:aws:iam::938716055043:group/cloud-interns

Users in this group (1)

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

□	User name	Groups	Last activity	Creation time
□	clouduser-amar		None	4 minutes ago

5. Attached appropriate IAM policies to the group.



Policies attached to this user group.

cloud-interns

Summary

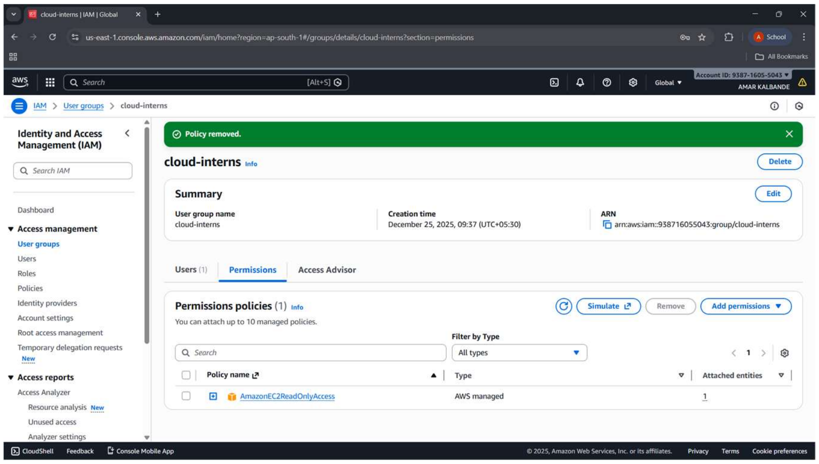
User group name: cloud-interns
Creation time: December 25, 2025, 09:37 (UTC+05:30)
ARN: arn:aws:iam::938716055043:group/cloud-interns

Permissions policies (2)

You can attach up to 10 managed policies.

Filter by Type: All types

□	Policy name	Type	Attached entities
□	AdministratorAccess	AWS managed - job function	1
□	AmazonEC2ReadOnlyAccess	AWS managed	1


cloud-interns | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/groups/details/cloud-interns?section=permissions
Account ID: 9387-1605-5043
AMAR KALBANDE
IAM > User groups > cloud-interns
Identity and Access Management (IAM)
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management
Temporary delegation requests
Access reports
Access Analyzer
Resource analysis
Unused access
Analyzer settings
Delete
Edit
Simulate
Remove
Add permissions

Policy removed.

cloud-interns

Summary

User group name: cloud-interns
Creation time: December 25, 2025, 09:37 (UTC+05:30)
ARN: arn:aws:iam::938716055043:group/cloud-interns

Users (1) | Permissions | Access Advisor

Permissions policies (1)

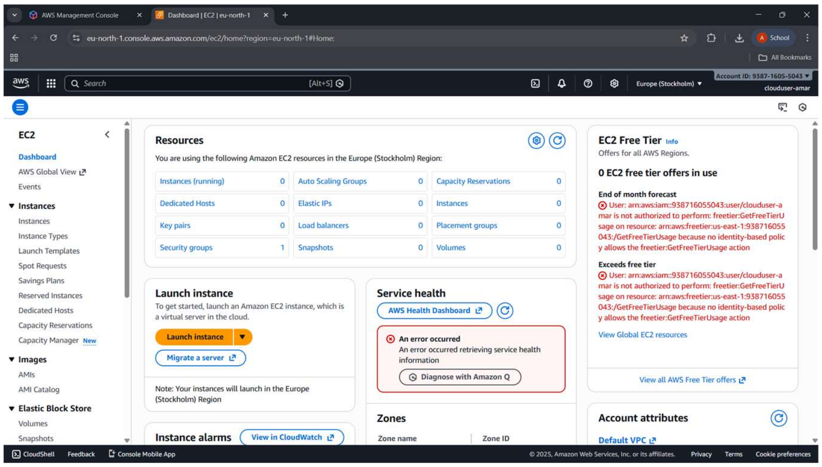
You can attach up to 10 managed policies.

Filter by Type: All types

Policy name	Type	Attached entities
AmazonEC2ReadOnlyAccess	AWS managed	1

6. Logged out from root account.

7. Logged in using IAM user credentials.



Resources

You are using the following Amazon EC2 resources in the Europe (Stockholm) Region:

Instances (running)	0	Auto Scaling Groups	0	Capacity Reservations	0
Dedicated Hosts	0	Elastic IPs	0	Instances	0
Key pairs	0	Load balancers	0	Placement groups	0
Security groups	1	Snapshots	0	Volumes	0

Launch instance

To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

Note: Your instances will launch in the Europe (Stockholm) Region

Service health

An error occurred
An error occurred retrieving service health information

EC2 Free Tier

Offers for all AWS Regions.

0 EC2 free tier offers in use

End of month forecast
User: arn:aws:iam::938716055043:user/clouduser-amar is not authorized to perform: freetier:GetFreeTierUsage on resource: arn:aws:freetier:us-east-1:938716055043:/GetFreeTierUsage because no identity-based policy allows the freetier:GetFreeTierUsage action

Exceeds free tier
User: arn:aws:iam::938716055043:user/clouduser-amar is not authorized to perform: freetier:GetFreeTierUsage on resource: arn:aws:freetier:us-east-1:938716055043:/GetFreeTierUsage because no identity-based policy allows the freetier:GetFreeTierUsage action

Instance alarms

Zones

Zone name | Zone ID

Account attributes

8. Verified access permissions and observed restricted access where permissions were not granted.

Security Best Practices Followed

- Root account not used for daily work
- IAM user created with controlled permissions
- Permissions assigned using groups
- Principle of least privilege followed
- Access verified through IAM login

Result

Secure access control was successfully implemented using AWS IAM. The IAM user was able to log in and access only permitted services, while restricted actions were denied, proving correct permission enforcement.

Conclusion

AWS IAM provides a robust mechanism for managing access securely. By using IAM users, groups, and policies, organizations can protect their cloud resources and follow security best practices effectively.