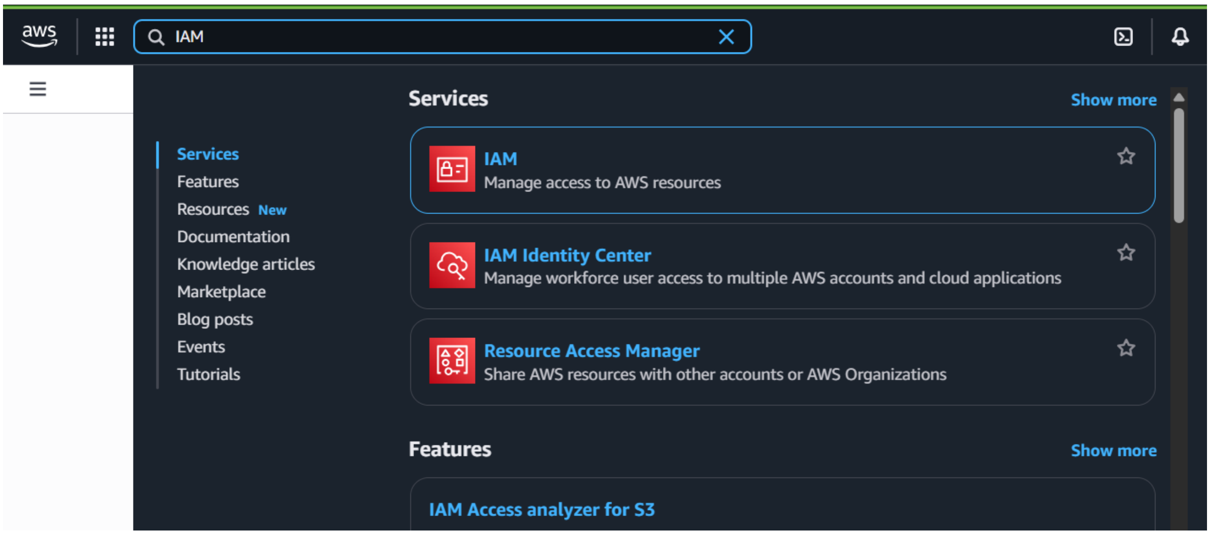
Day 32

“CLOUD SECURITY”

AWS IAM: Remove Unnecessary Credentials:

Steps:

Open the IAM console:

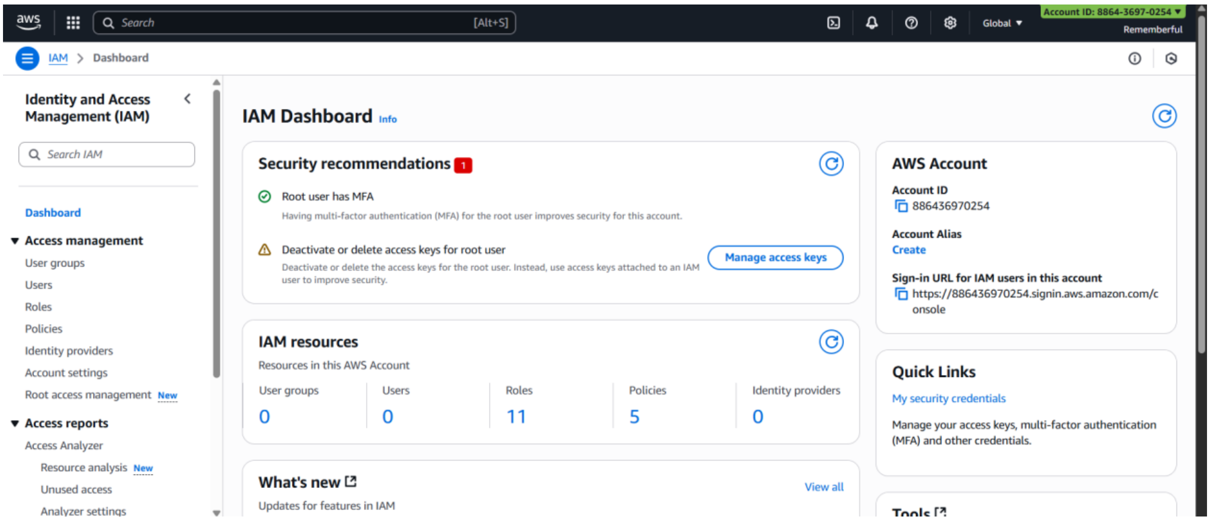


IAM — Manage access to AWS resources

IAM Identity Center — Manage workforce user access to multiple AWS accounts and cloud applications

Resource Access Manager — Share AWS resources with other accounts or AWS Organizations

Following window will open:



Security recommendations 1

Root user has MFA
Having multi-factor authentication (MFA) for the root user improves security for this account.

Deactivate or delete access keys for root user
Deactivate or delete the access keys for the root user. Instead, use access keys attached to an IAM user to improve security.

IAM resources
Resources in this AWS Account

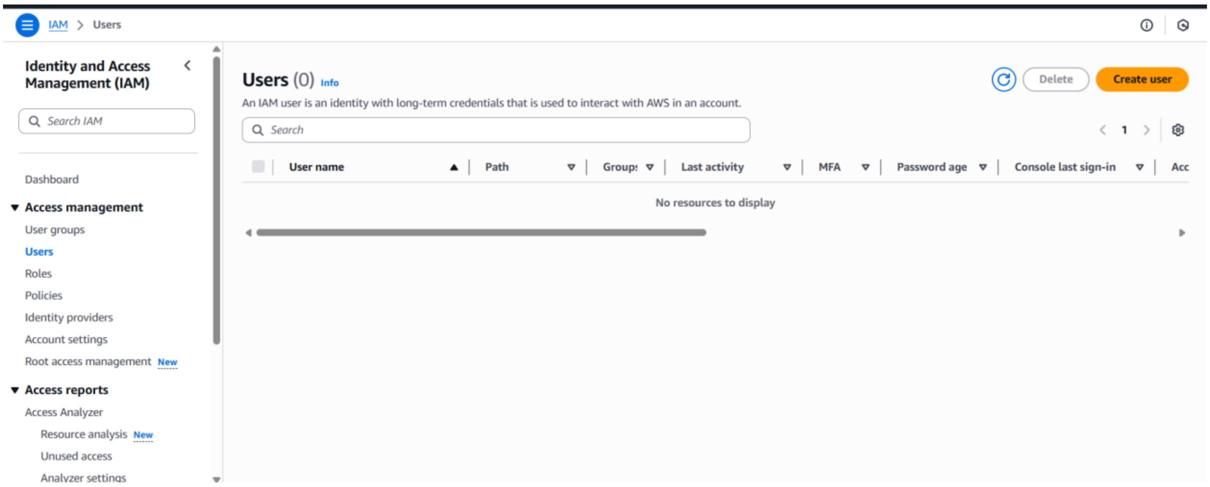
User groups	Users	Roles	Policies	Identity providers
0	0	11	5	0

What's new
Updates for features in IAM

AWS Account
Account ID: 886436970254
Account Alias: Create
Sign-in URL for IAM users in this account: https://886436970254.signin.aws.amazon.com/console

Quick Links
My security credentials
Manage your access keys, multi-factor authentication (MFA) and other credentials.

Click on the “Users” option from left pane: following window appear.



Users (0) Info

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

User name	Path	Group:	Last activity	MFA	Password age	Console last sign-in	Acc
No resources to display							

Clearly, no user exists in our system, so nothing is shown to us.

Best Practices for Securing AWS Credentials

1. Use IAM Roles instead of root credentials – never use or share the root account.
2. Enable Multi-Factor Authentication (MFA) for root and all IAM users.
3. Follow the principle of least privilege – grant only required permissions.
4. Rotate access keys & passwords regularly to reduce risk of compromise.
5. Use AWS Secrets Manager or Parameter Store to store API keys, DB passwords, and tokens securely.
6. Apply strong password policies – enforce length, complexity, and rotation.
7. Monitor with AWS CloudTrail & Config – detect suspicious credential use.
8. Avoid hardcoding credentials in apps/code – use IAM roles or environment variables.

--The End--