**Day 32**



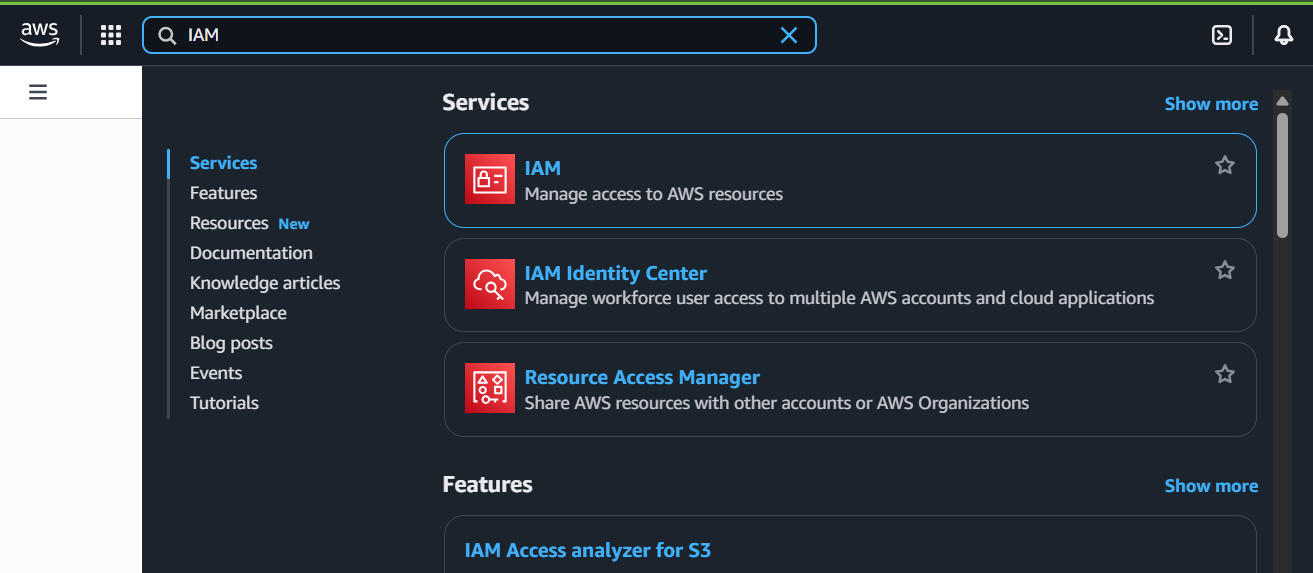


**“CLOUD SECURITY”**

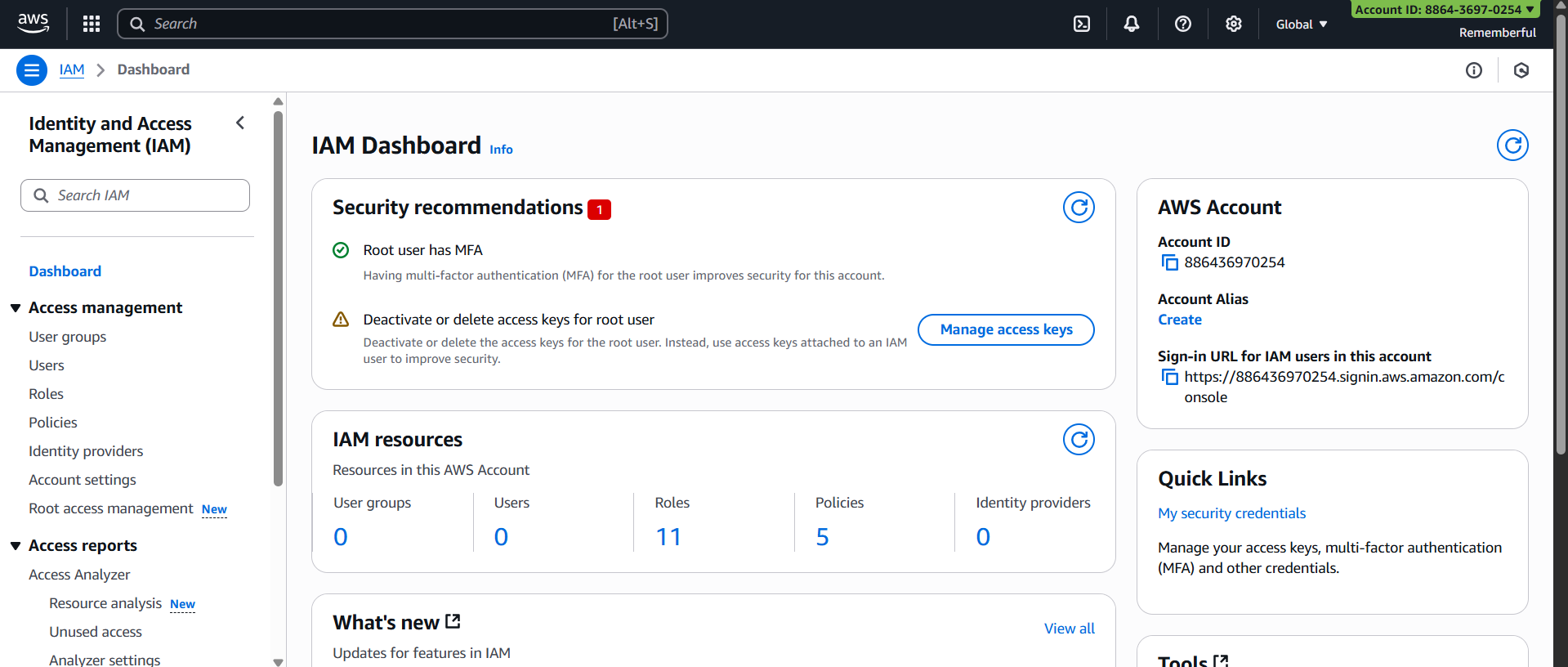
**AWS IAM: Remove Unnecessary Credentials**:

Steps:

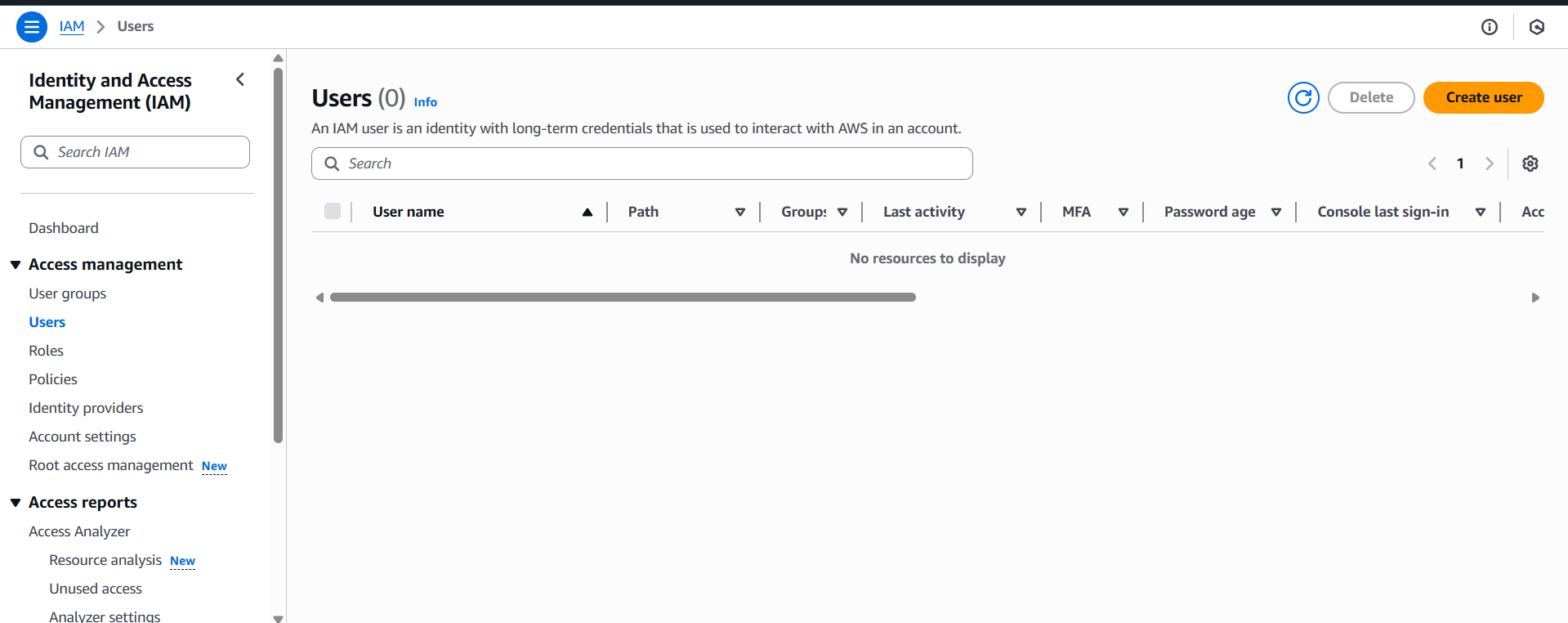
Open the IAM console:



Following window will open:



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



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--