Create 6 Users and grant them permissions like EC2, S3, RDS, ECS and Lambda individually

Create groups Developers, Admins and AWS Architect and add above users to Group. Add permissions to Group.

Create Custom policy via Policy generator and attach it to the user.

Add MFA for user or Root Account

Generate AK and SK for a user and delete it

Generate Credentials Report and share screenshots of Access Advisor.

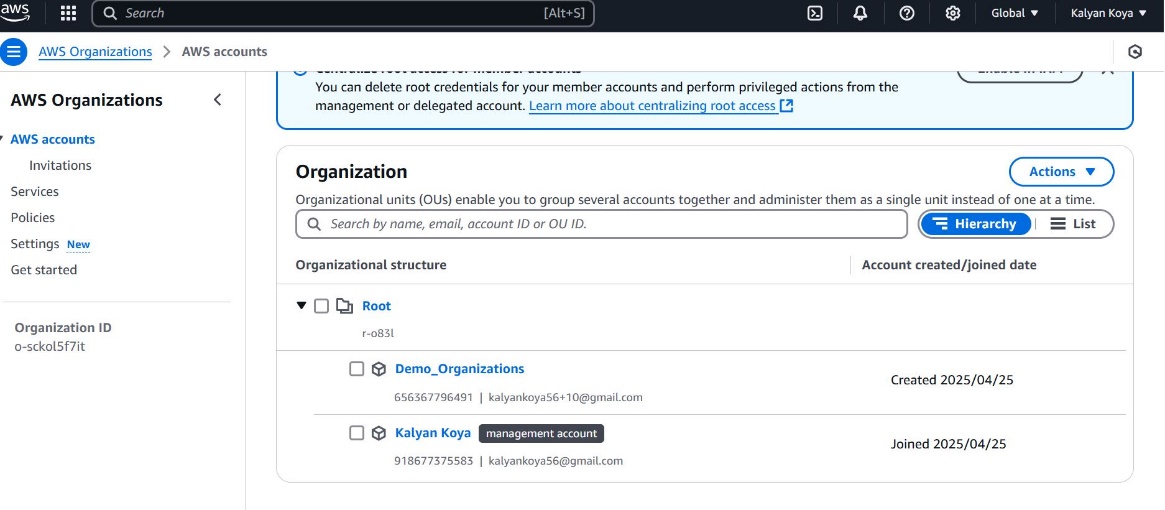
Access Cloudshell, run some commands and share snippet of the same

Implement same demo of User Assuming an IAM role in another AWS Account ()

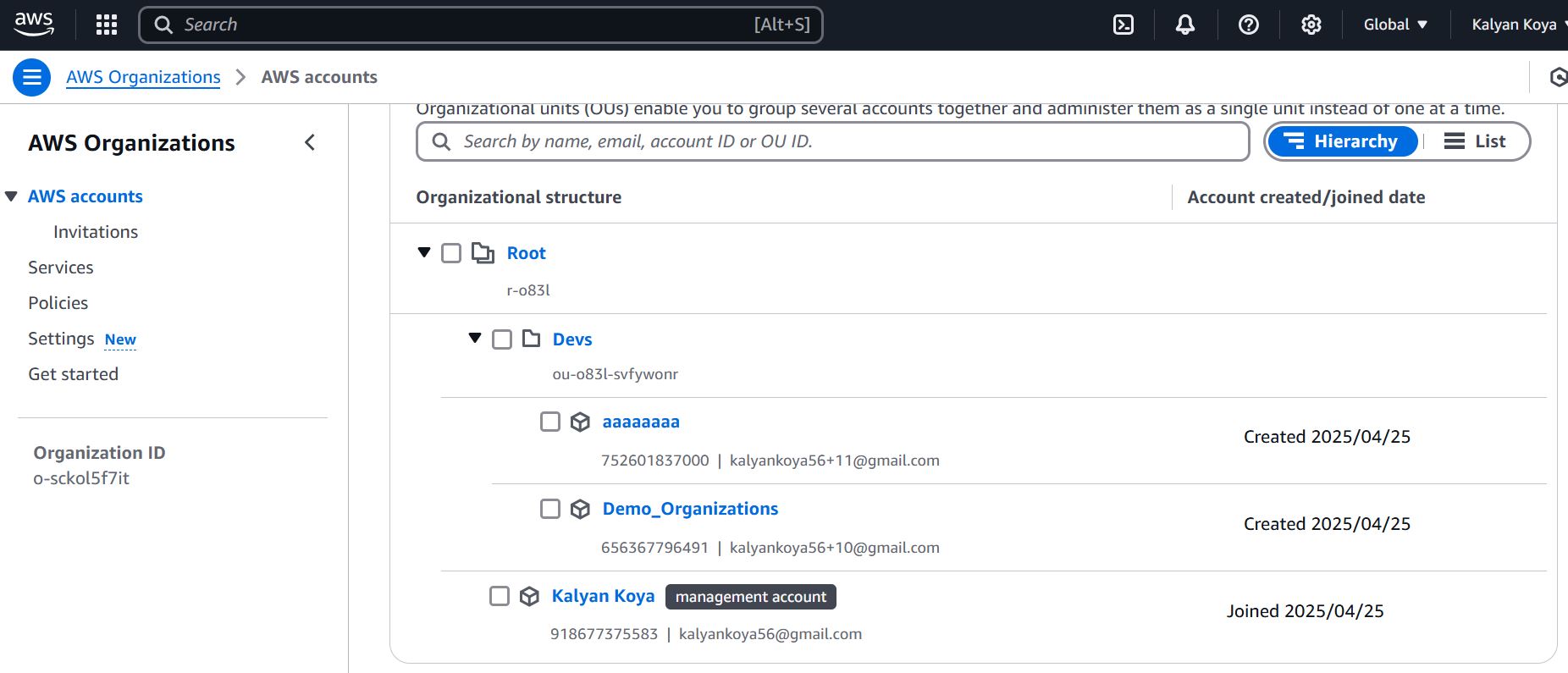
Difference between root user and IAM User.

* **Root User**:
* This is the account that was created when signing up for AWS.
* Has **full access** to all AWS services and resources.
* Cannot be restricted by IAM policies.
* It is recommended **NOT** to use the root user for everyday tasks.
* Best practice: **Secure it with MFA (Multi-Factor Authentication)** and use IAM users instead.
* **IAM User**:
* Created within an AWS account by the administrator.
* Can have **specific permissions** granted via IAM policies.
* Can be **restricted** in access based on assigned roles.
* Used to follow the principle of **least privilege** (only give necessary access).
* Best practice: Assign IAM users different roles to improve security.

Create AWS Organization



Add AWS Accounts to AWS Organization



Create SCP and attach it to OU or Aws Account and test it.

Attach Inline Policy to a User

Create any IAM based policy with a Condition element included in the same.s