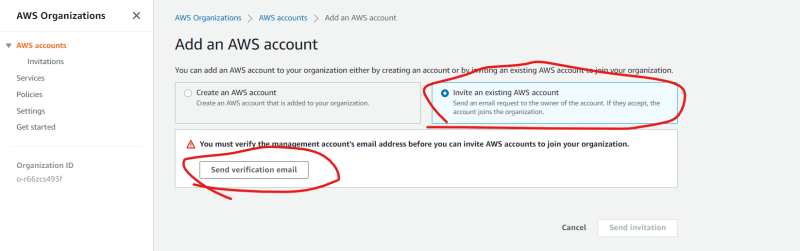
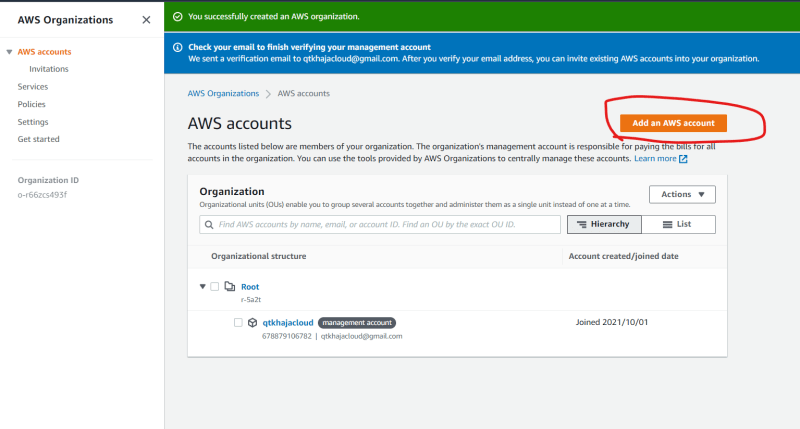
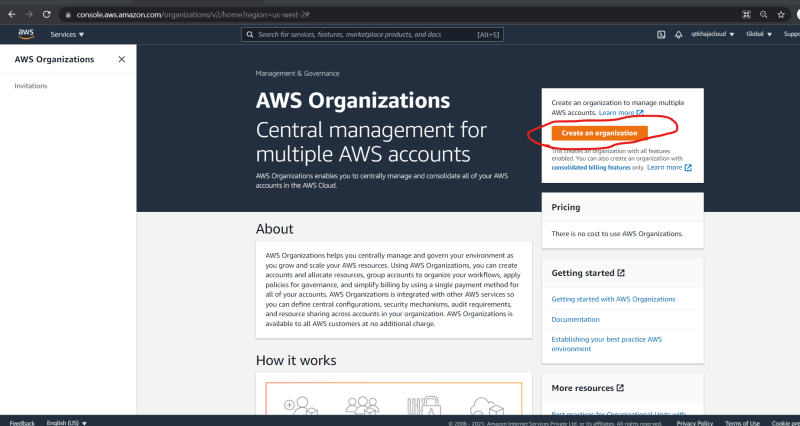
**AWS Organizations**

This is an account management service that enables us to consolidate multiple AWS accounts into an organization <https://console.aws.amazon.com/organizations/v2/home?region=us-west-2> 

Once you add accounts, we can enforce some policies common to multiple accounts

**Activities**

Scenario-1: Your Developer has written a AWS lambda code which starts stops ec2 instances, how can we give access to AWS lambda to start or stop ec2 instances

We need to create a role with start instances & stop instances actions to lambda

Create a policy with actions start and stop instances

{

"Version": "2012-10-17",

"Statement": [

{

"Sid": "VisualEditor0",

"Effect": "Allow",

"Action": [

"ec2:StartInstances",

"ec2:StopInstances"

],

"Resource": "\*"

}

]

}

Now attach this is iam role for AWS Lambda

Scenario-2: Your Testing team is working on AWS and there are 10 testers, they are using the application deployed on AWS Ec2 and RDS instances, Sometimes they might need to restart the ec2 instances and rds instances while they are testing. How can we give an access.

Create a policy with ec2 readonly, rds only & restart actions for ec2 & rds

Assign this policy to a group

Add all 10 users to this group.

Scenario-3: Your application which your organization is developing allows users to upload the images. Your application internally creates the bucket for every user. Now how can give an access to an application to create and upload images to bucket.

Create a user with programmatic access and use access keys and secret key in the code

Attach the policy to allow s3 access to perform creating buckets & objects

Scenario-4: You are asked to develop a shell script which takes a backup of s3 bucket contents into the on-premise. What would be your steps?