DevOps Kitchen Workshop

S3 Bucket - Conditional Access Policy

#day_four - Manage user's access with conditions

duration: 1 day

ForgTech company wanna test your ability to type down a clean code by Deploying the structure of resources. This will help you to build a good reputation.

FrogTech intends to use S3 Bucket as centralized storage between internal and external users utilizing IAM policies and Roles. you're requested to Deploy an S3 beside Three users for Ahmed as an internal user with IAM policy of S3 Administrator access AWS-managed-Policy, Mahmoud as an external user with IAM policy allows to get objects of S3 Bucket with IP conditional restriction of his company public IP only, and Mostafa as an internal user and his team delegated to fetching files, with IAM Role holds the get-objects policy.

Use IaC Terraform to build all resources and consider the below requirements specifications. and ensuring that you can destroy the S3 *(i.e. using terraform destroy command)* even if the bucket is not empty.

1. Resources must be created at the us-east-1 region.
2. Resources must have tags as below:
   a. Key: "Environment", Value: "terraformChamps"
   b. Key: "Owner", Value: <"Your_first_name">
3. Preferd to use variables
4. Create & Share a document that Explains what you learn.

Code Sample:

- Day four sample/Blog
- Day four sample/Code i.e. iam creation, IP restriction, etc
- Day four sample/Attache AWS Managed policy to IAM Role