Setup CI/CD Pipeline for UI App using GitHub Actions

Before proceeding the Pipeline: make sure your application is currently being hosted on S3 bucket using **Cloud-Front**, and your code has been moved to GitHub.

- □ Create a GitHub Action workflow within the folder where your app is located in folder .github/workflows/build-and-deploy.yaml (you can give any name as you like for build-and-deploy.yaml)
- ⇒ In this YAML file, configure all the required configurations as shown below.

.github/workflows/build-and-deploy.yaml

- ⇒ In this YAML file, configure all the required configurations as shown below.
- ⇒ This is for Bootstrap, Html javascript and css

```
name: Build and Deploy UI App to CloudFront
on:
    push:
        branches: [ main ]
    jobs:
    build-and-deploy:
        name: Build and Deploy
        runs-on: ubuntu-latest
        env:
        BUCKET: www.esmelealem.com
        DIST: ./
        REGION: us-east-1
        DIST_ID: E1AE44E6CJ86JT

    steps:
        - name: Checkout code
        uses: actions/checkout@v2
        - name: Configure AWS Credentials
```

```
- name: Configure AWS Credentials
  uses: aws-actions/configure-aws-credentials@v1
 with:
   aws-access-key-id: ${{ secrets.AWS_ACCESS_KEY_ID }}
   aws-secret-access-key: ${{ secrets.AWS_SECRET_ACCESS_KEY }}
   aws-region: ${{ env.REGION }}
# - name: Set up Node.js environment
# uses: actions/setup-node@v2
  with:
    node-version: '14'
# - name: Install Dependencies
  run:
    node --version
     npm install
# - name: Build Static Website
# # run: npm run build
```

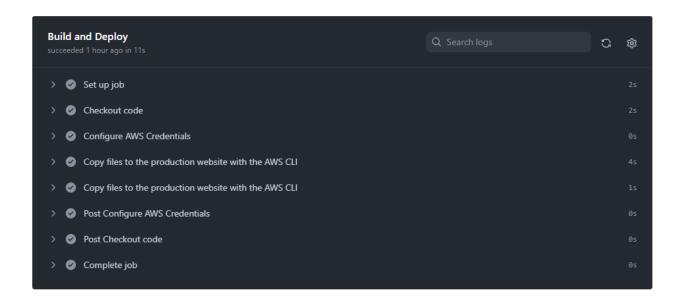
To allow GitHub Actions to upload files to S3and create invalidation in CloudFront, it is necessary to generate a new IAM user and assign the necessary authorizations. We should make a policylike below.

```
{
    "Version": "2012-10-17",
    "Statement":
            "Sid": "ListObjectsInBucket",
            "Effect": "Allow",
            "Action": "s3:ListBucket",
            "Resource": "<your bucket arn>"
        },
{
            "Sid": "AllObjectActions",
            "Effect": "Allow",
            "Action": "s3:*Object",
            "Resource": "<your bucket arn>/*"
        },
            "Sid": "InvalidateCF",
            "Effect": "Allow",
            "Action": "cloudfront:CreateInvalidation",
            "Resource": "*"
        }
```

- Create a new user with the name "github-actions" and attach the policy specified above to it.
- Navigate to the GitHub repository and set up two secrets, namely AWS_ACCESS_KEY_ID and AWS_SECRET_ACCESS_KEY.
- These secrets will be used to authenticate and authorize GitHub actions that require access to your Amazon Web Services (AWS) account.

Repository secrets		
AWS_ACCESS_KEY_ID	Updated 2 hours ago	
AWS_SECRET_ACCESS_KEY	Updated 2 hours ago	/

The Continuous Integration/Continuous
Deployment(CI/CD) pipeline has been successfully
set up and you can verify its functionality by
making changes to the source code. After
committing and pushing the changes, the pipeline
will be triggered, and you can observe the
process in GitHub Actions.



Prepared By: Esmelealem Mihretu - March 2023, MIU







