CodeBuild - Create CF stack using Templates in CodeCommit

This Repo will create CloudFormation Template using CodeBuild Service.

Pre-requisites

- Create a codecommit repository and upload the files using git bash and other git commands like *git add, git commit and git push*.
- Create a child branch and add code in child branch to remote.
- Create a Codebuild Project from AWS Console with below information:
    - For Operating system, choose Ubuntu.
    - For Runtime, choose Standard.
    - For Image, choose aws/codebuild/standard:5.0.
    - Create environment variables `ENVIRONMENT_NAME` , `VPC_ID`, `SUBNET_ID` to pass the values while executing the build job.
    - Under Build Specification, enter the path of the buildspec.yml file present in the repo. i.e `config/buildspec.yml`
- Add Permissions to create `IAM`, `EC2`, `CloudFormation` to the CodeBuild Role.
- As we are using SSM Parameter to get LatestAmiId, SSM Read Only Access to codebuild role.

Repository structure

- `config` - contains `buildspec.yml` file that will be used by CodeBuild Project.
- `templates` - contains CF templates to create stack.
- `scripts` - contains scripts that runs aws cli commands to create CF stack

Execution information

- Create a child branch and check-in this code to AWS CodeCommit Remote Repo.
- Execute CodeBuild Project by providing Runtime Values for CodeBuild Environment Variables, use child branch for non-prod environment build execution.
    - Navigate to the CodeBuild Execution Logs to validate the Commands executions.
    - Validate the Environment Variables that are set during the CodeBuild Execution.
- Validate the CodeBuild Execution and CF stack creation in non-prod environment.
- Raise a PR from child branch to master/main i.e stable git branch.
- Review and once approved, merge changes from child branch into master/main stable branch.
- Execute CodeBuild Project for prod environment creation from master/main stable branch.
- `Resolved source version` => Commit id of the repo , which helps you to navigate back to git repo to re-evalutate incase u have to know what code was executed by the build.

Best Practices:

- Run your Build Projects with develop or any feature branch with dev/qa as environment values only.
- Production environment build should always happen from `master/main` branch.

IAM user

AWS Cloud

Region git pull /
        git push

SDLC_ENV : dev|qa|prod

CloudFormation

CodeCommit Repo
config/buildspec.yml
templates/ec2.yml
scripts/ec2_create.sh

git pull BRANCH_NAME

CodeBuild Project
- Image OS
- IAM Role
- config/buildspec.yml

child_feature_branch

dev-ec2-stack

base branch(main)

prod-ec2-stack

Once changes are
tested. Raise a PR :
child_branch -> base
branch