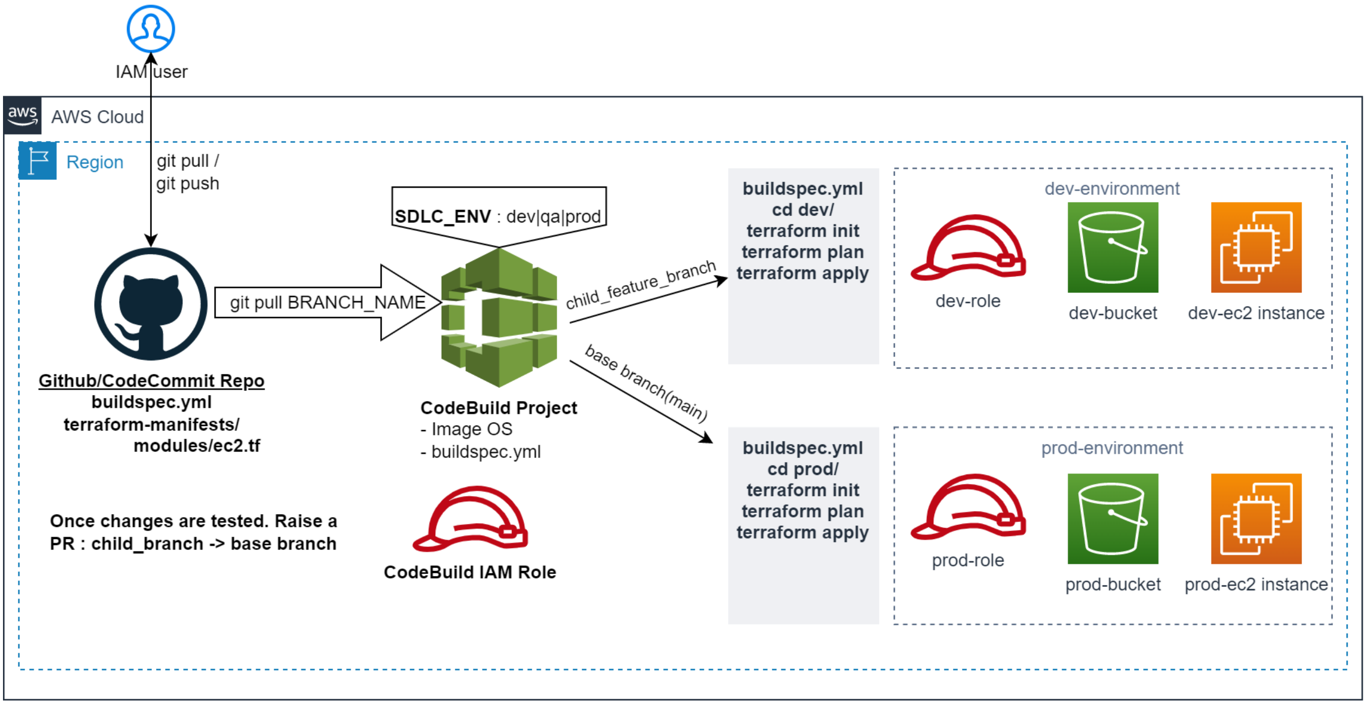
Table of Contents

Create Terraform Infrastructure Using Github and CodeBuild



--

Pre-requisites

- Create a Github repository and upload the files using git bash and other git commands like **git add, git commit and git push** in a child branch.
  - This Repo will contain Terraform Files that will be deployed using CodeBuild Service.
  - Update the **terraform-manifests/dev/backends.tf** , **terraform-manifests/qa/backends.tf** and **terraform-manifests/prod/backends.tf** file to update the **bucket** value as per your AWS Account.
- 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:7.0**.

  - Create environment variables as below to pass the value while executing the Codebuild job. During the CodeBuild Project Creation, keep below values as blank.
    - **SDLC_ENV** : Pass the value as **dev/qa/prod** as per environment folders available in the Git Repo
    - **TF_COMMAND** : Pass the value as **apply/destroy** , based on the terraform command that you want to run
- The CodeBuild IAM Role should have Permissions to create IAM, EC2, S3 buckets etc.
  - These same permissions are going to be used by Terraform to authenticate to your AWS Account.

--

Repository structure

```
|-- buildspec.yml
`-- terraform-manifests
    |-- dev
    |   |-- backends.tf
    |   `-- main.tf
    |-- modules
    |   |-- buildspec.yaml
    |   |-- infra_services
    |   |   |-- assumerolepolicy.json
    |   |   |-- compute.tf
    |   |   |-- iam.tf
    |   |   |-- networking.tf
    |   |   |-- outputs.tf
    |   |   |-- storage.tf
    |   |   `-- variables.tf
    |-- prod
        |-- backends.tf
        `-- main.tf
    `-- qa
        |-- backends.tf
        `-- main.tf
```

- **buildspec.yml** - contains commands to install terraform and execute **terraform init,plan,apply** commands file that will be used by CodeBuild Project from the environment specific directory.
- **terraform-manifests** - contains all source code for Terraform Code Files.

--

Infrastruction Creation Execution

- Execute CodeBuild Project for **non-prod** environment creation from a specific child branch.
  - Provide **SDLC_ENV : dev** and **TF_COMMAND : apply** as CodeBuild Environment Variable.
  - Validate the CodeBuild Execution and Infrastructure creation in **dev** environment.
  - Validate the S3 Backend State File for dev 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.
    - Provide **SDLC_ENV : prod** and **TF_COMMAND : apply** as CodeBuild Environment Variable.
    - Validate the CodeBuild Execution and Infrastructure creation in **prod** environment.
    - Validate the S3 Backend State File for **prod** environment.

--

Infrastruction Update Execution

- To modify any specific AWS Resource changes in an environment like updating IAM Policy, Changing Security Group Configuration, these changes should be done in TF code in a child branch.
- Any Change made in TF code has to be executed again against that specific environment to take effect from that specific branch.
- So CodeBuild Job will have to be re-run again by passing same values of the Environment Variables.
- Once Terraform Resources are updated, validate the changes done using AWS Console.
- Once changes are validated in child branch, PR has to be raised to get this changes in master/base branch.
- Use the master/base branch to deploy changes to higher environment.

--

Infrastruction Deletion Execution

- Execute CodeBuild Project for **non-prod** environment creation from a specific child branch.
    - Provide **SDLC_ENV : dev** and **TF_COMMAND : destroy** as CodeBuild Environment Variable.
    - Validate the CodeBuild Execution and Infrastructure deletion in **dev** environment.
    - Validate the S3 Backend State File for dev environment.
- Execute CodeBuild Project for **prod** environment creation from **master/main** stable branch.
    - Provide **SDLC_ENV : prod** and **TF_COMMAND : destroy** as CodeBuild Environment Variable.
    - Validate the CodeBuild Execution and Infrastructure deletion in **prod** environment.

> NOTE: Make sure all unused AWS Resources are destroyed to avoid AWS Cost in Billing.

--

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.

IAC using CI Assignment

- Create two CodeBuild Projects as below:

    - **AWS-Create-Infrastructure**
        - User should be able to provide environment variable for which infra creation should be working.
        - This CodeBuild Project should run Terraform **Apply** Command.
    - **AWS-Delete-Infrastructure**

        - User should be able to provide environment variable for which infra creation should be working.
        - This CodeBuild Project should run Terraform **Destroy** Command.

- **Below AWS Resources should be created with above CodeBuild Projects**

    - Provision a VPC Network Resources having 2 public subnets and 2 private subnets, IGW attached to VPC, VPC Gateway Endpoint for S3 Service.
    - Create an S3 Bucket with sdlc name as prefix.
    - Provision RDS Instance in VPC private subnet launched in the previous step (network resources)
    - Create IAM Role, Policy and Provision a EC2 instances having this IAM Role attached, that contains IAM Permissions to read and write data to S3 buckets.
    - Validate the data copy from ec2 instance to/from S3 bucket.
    - Validate network to connect with RDS instance.
    - Validate the connection to RDS Instance from EC2 instance by executing mysql commands
    - Document all steps with AWS Service Screenshots

--

> Code structure should be re-usable for multiple environment setup. Ensure that dev environment EC2 Instance should have access to only Dev Environment Resources i.e S3, RDS etc. Similarly for other environments.