Cloud Platform Terraform Components and Blueprints

Overview

AWS resources are deployed to the AWS accounts using components and blueprints hosted on GitLab.

Components create AWS resources using terraform. Blueprints group together a combination of components to create the cloud ecosystem.

Content

Example: S3 components

GitLab Repo: https://gitlab.com/mc-components/terraform-aws-s3-bucket

s3_bucket.tf : creates s3 bucket with versioning enabled, lifecycle rules, server-side encryption, tags

bucket_policy.tf : definies IAM policy for S3 bucket

consumer_policy.tf: creates IAM policy for the consumers of S3 bucket. It can be directly attached to all the consumers which will give them required permissions to access this bucket. *We do not recommend consumers creating s3 bucket access policy on their own*.

folders.tf: Optional, empty folders to be created in the buckets

kms-key.tf : Server side encryption using KMS key

meta.tf : required version of terraform and references aws account and region for reference in the component

variables.tf : defines all input variables for the component

How to use component in a blueprint:

To use the predefined S3 component in a blueprint, you can reference the link to the component’s repository and pass in the necessary input variables.

```
module "config_log_bucket" {
  source = "git::https://<YOUR_VCS_URL>/components/terraform-aws-s3-bucket.git?ref=v2.0.1"

  bucket_name          = var.stack_name}-config-logs
  append_random_suffix = true
  force_s3_destroy     = false

  cross_account_principals = local.all_account_ids

  providers = {
    aws = "aws.logging"
  }
}
```

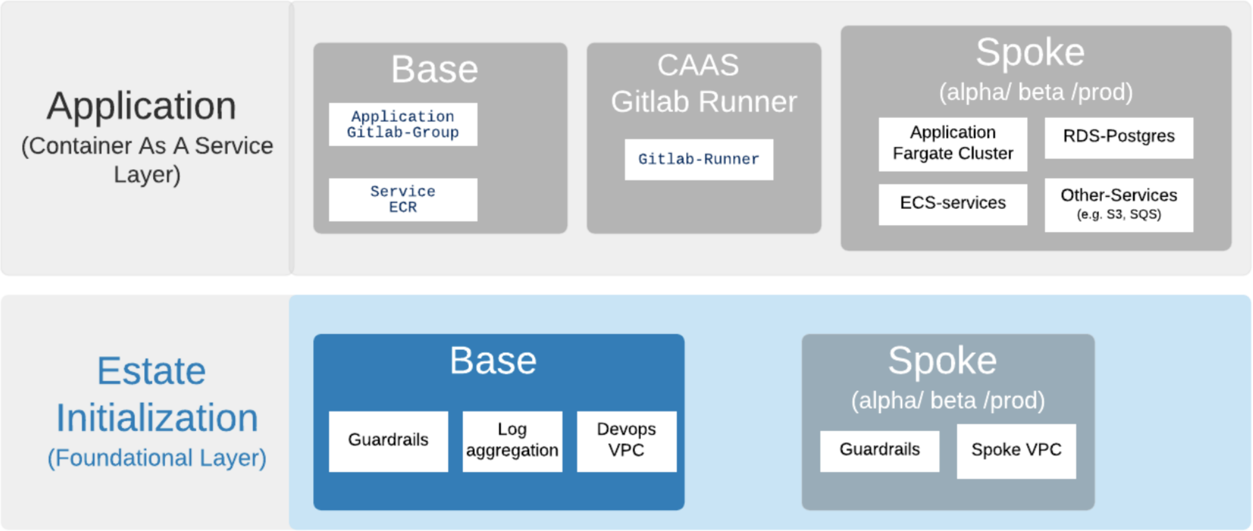
Blueprint to create an estate base for AWS account:

Estate module is the first layer for any cloud estate. It sets up baseline security, centralized logging and VPC for shared tooling. There are two parts of estate setup: estate base and estate spoke. Estate base module setup baseline infra for base AWS accounts (security / logging /devops) and estate-spoke setup baseline infra on individual spoke AWS accounts (alpha/ beta/ prod).

It creates:

- Baseline security enabled in all AWS accounts e.g. Cloud trail, AWS Config, GuardDuty and SecurityHub
- Aggregated security dashboard in Security account
- Centralized logging infra in Logging account (log source examples - VPC flow logs, service logs, RDS logs etc)
- Base networking setup using VPC and subnets in 3 AZs

Architecture



Repo: https://gitlab.com/mc-estate-infra/estate-base

Blueprint to create an estate base for AWS account:

Sets up base infrastructure for spoke accounts. This module must be deployed first on each individual spoke to setup an estate.

Estate module is the first layer for any cloud estate. It sets up baseline security , centralized logging and VPC for shared tooling. There are two parts of estate setup: estate base and estate spoke

Estate base module setup baseline infra for base AWS accounts (security / logging /devops) and estate-spoke setup baseline infra on individual spoke AWS accounts (alpha/ beta/ prod).

Repo: https://gitlab.com/mc-estate-infra/estate-spoke

Relevant materials

GitLab Repo Component for S3: https://gitlab.com/mc-components/terraform-aws-s3-bucket