AWS Lab 05: Implementing Checks and Validations

Contents

Overview

In this lab, you will:

- Apply input validation rules in Terraform configurations.

- Implement precondition and postcondition checks to enforce constraints.

- Introduce AWS IAM policies and tag-based constraints on resources.

- Implement post-deployment validation checks to ensure compliance.

Before You Begin

Ensure you have completed Lab 0 before attempting this lab.

In your terminal, enter:

cd /aws-tf-int/labs/05

Ensure all Terraform commands are executed in this directory.

Reference Documentation

[Terraform Input Validation](#)

[Terraform Preconditions and Postconditions](#)

[AWS IAM Policies](#)

[AWS Tag Policies](#)

Scenario

You are a Cloud Engineer responsible for enforcing naming and policy constraints in Terraform deployments. Your tasks involve:

- Applying preconditions (e.g., S3 bucket names must follow a naming convention).
- Using postconditions (e.g., checking the assigned IAM role post-deployment).
- Enforcing AWS IAM Policies (e.g., only approved EC2 instance types can be used).
- Performing post-deployment Terraform data checks.

Step 1: Review Terraform Files

The lab consists of the following Terraform files:

- main.tf - The Terraform configuration
- variables.tf - Input variables with constraints

- terraform.tfvars - Default values for variables

Step 2: Check AWS IAM Policies & Resource Compliance

Before deploying resources, check for AWS IAM policies restricting actions.

List IAM Policies Attached to Your User/Role:

aws iam list-attached-user-policies --user-name YOUR_USER

aws iam list-attached-role-policies --role-name YOUR_ROLE

Step 3: Deploy the Configuration

Run the following Terraform commands:

terraform init

terraform plan

terraform apply

terraform output

Step 4: Test Validation Failures

Test 1: Invalid S3 Bucket Name

Modify terraform.tfvars:

s3_bucket_name = "Invalid_Bucket_Name!"

Run **terraform apply**

Expected error: S3 bucket names must be lowercase, globally unique, and follow naming conventions.

Step 5: Try Yourself - Implementing Allowed EC2 Regions

Enhance the Terraform configuration to enforce allowed AWS regions for EC2 instances.

Step 6: Lab Clean-Up

Remove all deployed resources:

terraform destroy