# POC AWS Infrastructure – Challenge Documentation

## Overview

This document describes the Terraform-based solution developed to meet the proof-of-concept (POC) challenge. The infrastructure was implemented using a combination of Coalfire’s open-source Terraform modules and native AWS resources, following infrastructure-as-code (IaC) best practices.

### Architecture Summary

1. Networking: Dedicated VPC (10.1.0.0/16), 4 subnets across 2 AZs, Internet Gateway, route tables, and CloudWatch flow logs.
2. Compute: One standalone EC2 in Sub2 (public) with Red Hat Linux (t2.micro, 20 GB EBS), plus an Auto Scaling Group (ASG) across Sub3/Sub4 (private) with 2–6 Red Hat instances (t2.micro, 20GB EBS, Apache installed via user data).
3. Load Balancing: Application Load Balancer (ALB) in public subnets, listening on HTTP/80, forwarding to ASG on HTTPS/443.
4. Security: Security groups using Coalfire module. IAM roles for ASG (read from Images bucket) and EC2s (write to Logs bucket).
5. Storage: Images S3 bucket (with Glacier lifecycle for Memes folder) and Logs S3 bucket (Active folder ® Glacier, Inactive folder ® delete after 90 days).

### Deployment Instructions

1. Clone the GitHub repository

$ git clone https://github.com//cf-challenge-infra.git

1. Initialize Terraform:

$ terraform init

1. Review the plan

$ terraform plan

1. Apply the infrastructure

$ terraform apply

1. Retrieve the EC2 instance’s public IP

$ terraform output ec2\_public\_ip

1. SSH into the instance:

$ ssh -i .pem ec2-user@

### Diagram

