**Project Documentation: Web Application Infrastructure with Deletion Policies**

**Project Overview**

This CloudFormation template is designed to automate the deployment of a scalable, secure, and highly available web application infrastructure. The stack includes the following resources:

* A Virtual Private Cloud (VPC) with public subnets.
* An Internet Gateway for public access.
* An Auto Scaling Group of EC2 instances behind an Application Load Balancer (ALB).
* Security Groups to regulate network traffic.
* A Launch Template to define EC2 instance configurations.
* Deletion policies (Retain) for critical resources to prevent accidental deletions.

**Purpose and Goals**

1. **Purpose**: To deploy a robust web application infrastructure that supports auto-scaling and ensures high availability while providing a secure environment.
2. **Goals**:
   * Automate infrastructure provisioning to reduce deployment time and errors.
   * Ensure scalability by automatically adjusting EC2 instances based on demand.
   * Provide public access via an ALB with secure traffic routing.
   * Retain critical resources to safeguard data and configurations.

**Deployment Instructions**

**Prerequisites**

1. **AWS Account**: Ensure you have an active AWS account with sufficient permissions to create CloudFormation stacks and associated resources.
2. **Key Pair**: Create or have an existing EC2 KeyPair for SSH access.
3. **Region**: Select an AWS Region with at least two Availability Zones.

**Steps to Deploy the Stack**

1. **Log in to the AWS Management Console**.
2. **Navigate to CloudFormation**:
   * Go to **Services > CloudFormation**.
3. **Create Stack**:
   * Click **Create stack** and select **Upload a template file**.
   * Upload the YAML file containing this template.
4. **Specify Stack Details**:
   * Enter a stack name (e.g., WebApp).
   * Fill in the parameters:
     + EnvironmentName: A unique name prefix for resources.
     + VpcCIDR: Adjust if necessary; default is 10.0.0.0/16.
     + InstanceType: Choose t3.micro or t3.small.
     + KeyName: Provide the name of your existing EC2 KeyPair.
     + AmiId: Confirm or update the default AMI ID.
5. **Configure Stack Options**:
   * Add tags for better resource organization (optional).
6. **Review and Create**:
   * Review the configurations and acknowledge that CloudFormation will create resources.
   * Click **Create stack**.
7. **Monitor Deployment**:
   * Monitor the progress in the **Events** tab. Wait until the stack status is **CREATE\_COMPLETE**.

**Security Considerations and Best Practices**

**Network Security**

1. **Ingress Rules**:
   * Allow only HTTP (port 80) and SSH (port 22) traffic in the Security Group.
   * Restrict SSH access to trusted IPs by updating the CidrIp parameter in WebServerSecurityGroup.
2. **Private Access**:
   * Use private subnets for backend services in a production environment (not included in this stack).

**Resource Protection**

1. **Deletion Policies**:
   * Critical resources like VPC, subnets, and security groups are configured with Retain to prevent accidental deletions.
   * Periodically review and delete unused resources manually to avoid unnecessary costs.

**Instance Security**

1. **SSH Keys**:
   * Ensure the private key corresponding to the KeyName is securely stored.
2. **Update EC2 Instances**:
   * Use the provided User Data script to update and secure instances upon initialization.

**Data Security**

1. **SSL**:
   * Integrate SSL certificates with the ALB for secure communication.
2. **IAM Roles**:
   * Apply least privilege principles to IAM roles and policies.

**Testing and Validation Procedures**

**Infrastructure Validation**

1. **Check Resource Creation**:
   * Go to the **Resources** tab in CloudFormation and verify all resources are created successfully.
   * Navigate to **EC2 > Auto Scaling Groups** and confirm EC2 instances are running.
2. **Network Validation**:
   * Verify that the ALB is accessible via its DNS name (found in the **Outputs** section of the stack).
   * Test HTTP traffic to ensure proper routing to EC2 instances.
3. **Subnet Configuration**:
   * Confirm public subnets have auto-assigned public IPs enabled.

**Application Testing**

1. **Access the Web Application**:
   * Open a browser and navigate to the ALB DNS name.
   * Confirm the default index.html page (<h1>${EnvironmentName} Web Application</h1>) is displayed.
2. **Test Auto Scaling**:
   * Simulate load using a tool like Apache Benchmark or JMeter to ensure the Auto Scaling Group launches additional instances as needed.

**Security Testing**

1. **Port Scans**:
   * Use a network scanner (e.g., Nmap) to confirm only ports 80 and 22 are open.
2. **Restricted Access**:
   * Verify SSH access is limited to authorized IPs.