Implementation and Configuration Guide

Document Version

- Version: v1.0
- Date: 18 june 2025
- Author: Ricky Raj

Table of Contents

1. Introduction

- Purpose: Briefly describe the purpose of this guide and what it will cover.
- Scope: Define the scope of the implementation and what the guide will focus on.
- References: List any reference documents or external resources.

2. Prerequisites

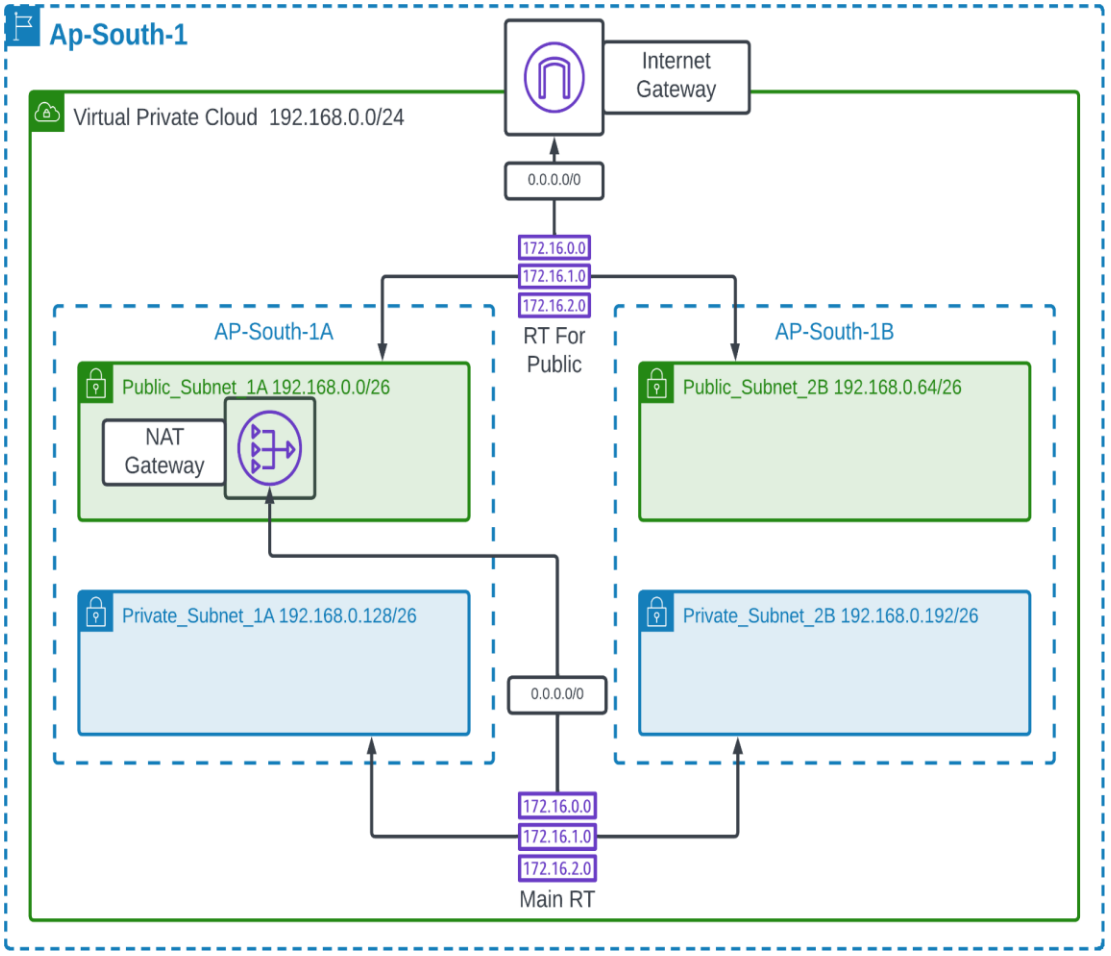
- AWS Account: Ensure you have an active AWS account.
- IAM Roles: Define the IAM roles required for the implementation.
- Knowledge Base: Specify any required knowledge or skills.

3. Architecture Overview

- Architecture Diagram: Include a diagram of the architecture.
- Description: Describe the high-level architecture and how different components interact.

4. AWS Services Configuration

4.1 Virtual Private Cloud (VPC)



Cloud Capstone Project-1

Step 1: Create the VPC

Go to the VPC Dashboard in the AWS Management Console.
Click on "Create VPC".
In the "Name tag" field, input a name for your VPC (e.g., "Ap-South-1"). For the IPv4 CIDR block, enter `192.168.0.0/24`.
Skip the IPv6 CIDR block unless you need it.
Select "No" for Tenancy (unless you require a Dedicated Instance). Click "Create".

Step 2: Create Subnets

In the VPC Dashboard, click on "Subnets".
Click on "Create subnet".
Select the VPC you created from the dropdown list.
For the first subnet:

- Name tag: "Public_Subnet_1A".
- Availability Zone: Select "ap-south-1a".
- IPv4 CIDR block: `192.168.0.0/26`.

Click "Create" to create the first subnet.
Repeat the steps for the additional subnets with the following details:

- For the second subnet:
  - Name tag: "Private_Subnet_1A".
  - Availability Zone: "ap-south-1a".
  - IPv4 CIDR block: `192.168.0.128/26`.
- For the third subnet:
  - Name tag: "Public_Subnet_2B".
  - Availability Zone: "ap-south-1b".
  - IPv4 CIDR block: `192.168.0.64/26`.
- For the fourth subnet:
  - Name tag: "Private_Subnet_2B".
  - Availability Zone: "ap-south-1b".
  - IPv4 CIDR block: `192.168.0.192/26`.

Step 3: Set Up Internet Gateway

In the VPC Dashboard, click on "Internet Gateways".
Click "Create internet gateway".
Provide a name tag (e.g., "IGW-Ap-South-1"). Click "Create".
Select the newly created internet gateway and click on "Actions".
Click "Attach to VPC" and select the VPC you have created
Click "Attach".

Step 4: Create Route Tables

In the VPC Dashboard, go to "Route Tables".
Click "Create route table".
Enter a name for the route table (e.g., "Main RT").
Select your VPC from the dropdown list.
Click "Create".
After creation, select the new route table and click on "Routes".
Click "Edit routes" and add the following route to allow internet access:

- Destination: `0.0.0.0/0`.
- Target: Select the Internet Gateway you created.

Click "Save routes".

Step 5: Associate Route Tables with Subnets

Select the route table, click on "Subnet Associations". Click "Edit subnet associations".
Select the public subnets ("Public_Subnet_1A" and "Public_Subnet_2B").
Click "Save".

Step 6: Create NAT Gateway (for Private Subnets)

Go to "NAT Gateways" in the VPC Dashboard.
Click "Create NAT gateway".
Select one of the public subnets (e.g., "Public_Subnet_1A").
Allocate an Elastic IP by clicking "Allocate Elastic IP".
Click "Create a NAT Gateway".
Once created, go back to "Route Tables", and create a new route table for your private subnets.
Follow a similar process as before to add a route pointing to the NAT Gateway for internet access from the private subnets.

4.2 Elastic Compute Cloud (EC2)

- Instance Setup: Instructions for setting up EC2 instances.
- Auto Scaling: Configuration steps for auto-scaling groups.

4.3 Elastic File System (EFS)

- Creation and Configuration: Steps to create and configure EFS.

4.4 Application Load Balancer (ALB)

- Setup: Define the steps to create and configure the ALB.

4.5 Route 53

- DNS Configuration: Guide through setting up DNS with Route 53.

5. Application Deployment

- Code Deployment: Steps to deploy the application code to the EC2 instances.
- Configuration Management: Best practices for managing application configuration.

6. Security Configuration

- Security Groups: Define security groups and rules.
- IAM Policies: Best practices for creating and assigning IAM policies.

7. Monitoring and Logging

- CloudWatch: Instructions for setting up monitoring with CloudWatch.
- Logging: Define how to set up and manage logs.

8. Backup and Disaster Recovery

- Data Backup: Steps to back up application data.
- Recovery Plan: Outline the disaster recovery plan.

9. Troubleshooting

- Common Issues: List common issues and their solutions.
- Support: Information on how to get help or support.

10. Additional Resources

- Documentation: Links to AWS documentation and other helpful resources.

Appendices

- Appendix A: Detailed configuration settings.
- Appendix B: Scripts and commands used.

Revision History

- [Date]: [Changes made], [Author]