Splunk Search App CloudFormation Template

Statement of Confidentiality:s

This document is prepared by Meyi Cloud LLP. All the information contained in this document and any accompanying reference documents or files is confidential and proprietary of ***Splunk Search App CloudFormation Template.*** This information is not to be disclosed, copied, distributed, or made public without prior written approval from Meyi Cloud LLP.

## Introduction:

# **Scope:**

The scope of this project is to create an Infrastructure for Splunk Search App with high Availability Zone using CloudFormation Template that deploys EC2 Instance Specified in the CFT for Splunk App and other related service for the application specified in the requirements documents. This will ensure that the infrastructure is consistent across environments, reducing the risk of errors and downtime.

The goal is to provide a highly available, scalable, reliable, and efficient solution for deploying different AWS services.

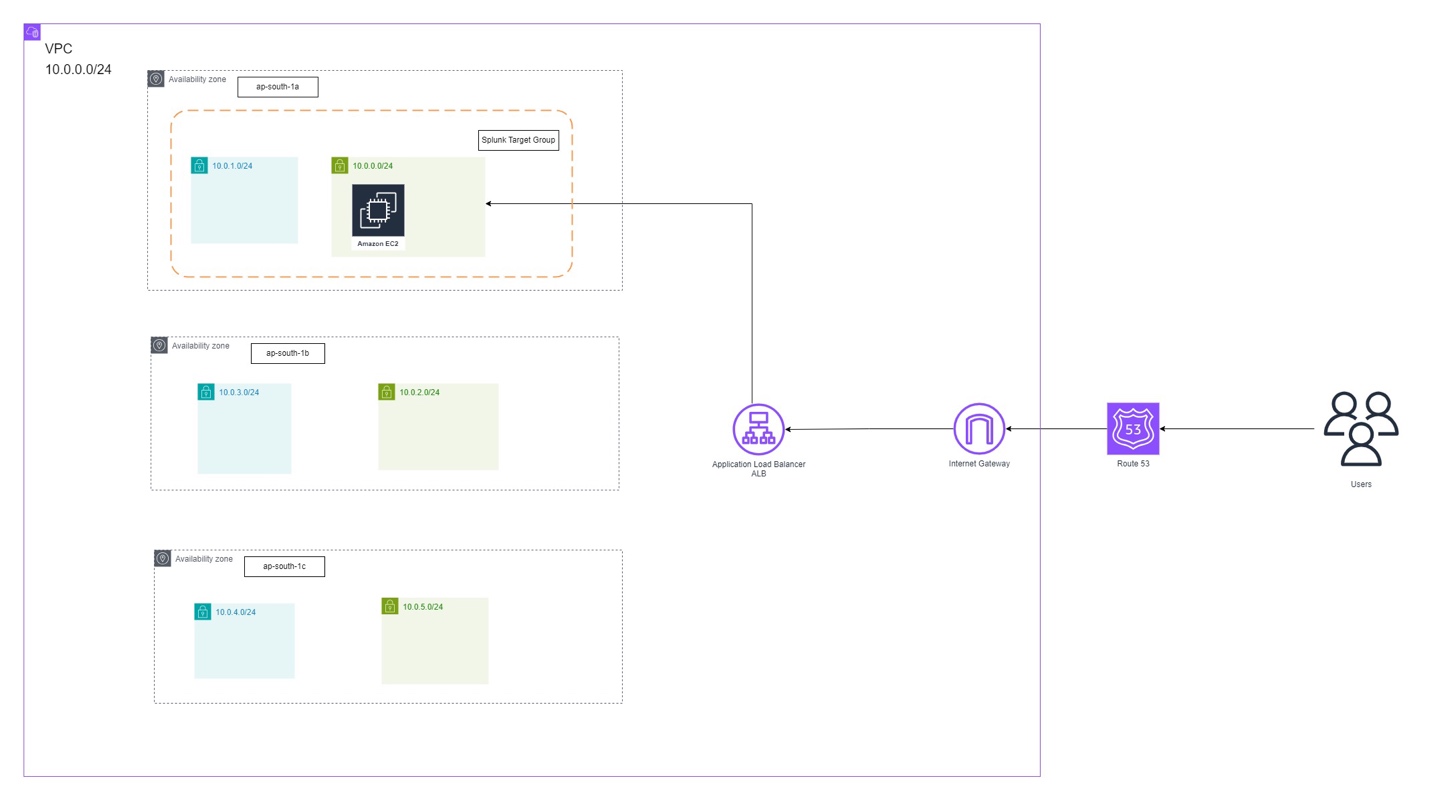
**Automation and Environment Management:**

* Our implementation focuses on automation, enabling seamless environment changes between Development (Dev), Testing (Test), and Production (Prod) stages.
* We utilize CloudFormation for infrastructure automation, with AWS CloudFormation offering significant advantages within the AWS ecosystem.

**AWS CloudFormation Deployment**:

* AWS CloudFormation is a service that allows you to model and provision AWS infrastructure resources in a declarative manner.
* By defining infrastructure as code using CloudFormation templates, we ensure consistency and repeatability across environments.
* These Infrastructures are created via CloudFormation Template are AWS EC2 (Elastic Cloud Computing) and VPC (Virtual Private Cloud), Application Load Balancer (ALB), Security Groups for ALB, VPC, Public and Private Subnets and Splunk EC2 Instance.

**Architecture**

High-Level Architecture for Splunk Infrastructure

**AWS Services**

1. **Virtual Private Cloud (VPC):** Amazon VPC allows you to provision a logically isolated section of the AWS Cloud where you can launch AWS resources in a virtual network that you define. You have complete control over your virtual networking environment, including selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways.

2. **Security Groups:** Security groups act as a virtual firewall for your Amazon EC2 instances to control inbound and outbound traffic. When you launch an instance in a VPC, you can assign it to one or more security groups. Security groups are stateful; this means any changes applied to incoming rules will automatically be applied to outgoing rules.

3. **Target Groups:** Target Groups are used with Application Load Balancers or Network Load Balancers to route requests to registered targets, such as EC2 instances, based on conditions like HTTP headers or paths. They help distribute incoming application traffic across multiple targets in multiple Availability Zones

4. **Route 53:** Amazon Route 53 is a scalable domain name system (DNS) web service designed to route end users to internet applications by translating names for our domain example: example.com to IP addresses like 192.0.2.1. It can also be used for internal DNS.

5. **Private and Public Subnets**: Subnets are segments of a VPC's IP address range that you can allocate to groups of resources. Public subnets are subnets that have a route to the internet gateway, allowing resources within them to access the internet. Private subnets, on the other hand, do not have a route to the internet gateway, making them suitable for resources that should not be directly accessible from the internet.

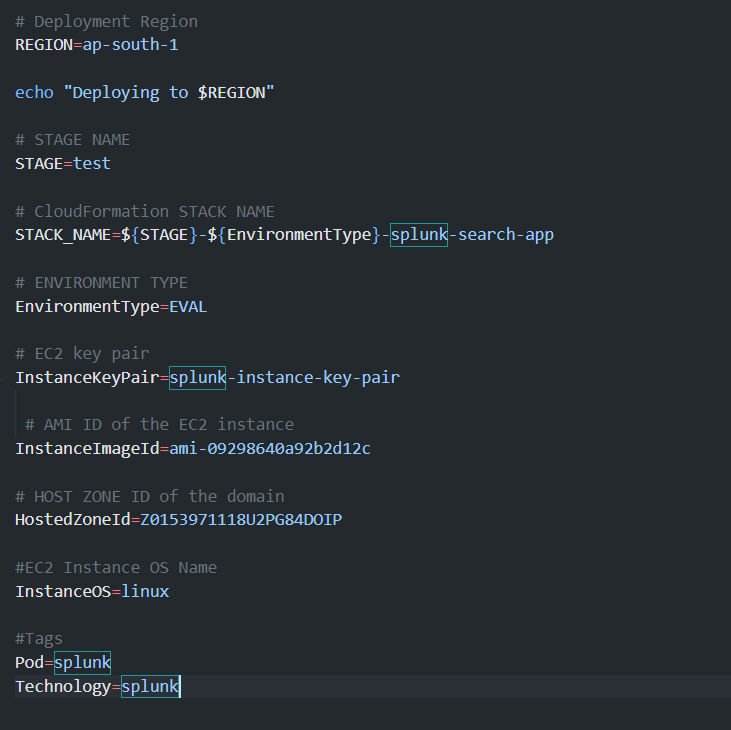
6. **Application Load Balancer:** An Application Load Balancer (ALB) distributes incoming application traffic across multiple targets, such as EC2 instances, in multiple Availability Zones. It operates at the application layer (Layer 7) and supports path-based routing and host-based routing, among other features.

7. **Amazon EC2 (Elastic Compute Cloud):** Amazon EC2 provides scalable computing capacity in the AWS cloud. It allows you to launch virtual servers (instances) on-demand, with a variety of instance types and sizes available to meet different computing needs. EC2 instances can be used for various purposes, including hosting applications, websites, and databases.

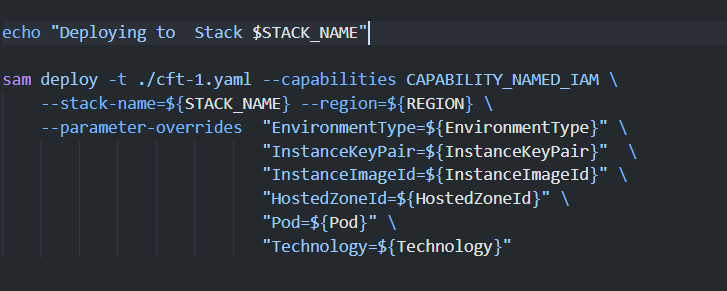
### **Deployment Process:**

* Run the **deploy.sh** file to deploy a SAM (Serverless Application Model) application.
* Deployment utilizes a CloudFormation template (**cf-1.yaml or cft-2.yaml**) to create or update a CloudFormation stack.
* The stack is named **dev-EVAL-splunk-search-app**, with the stage being either 'dev', 'staging', or 'prod'.
* Deployment is targeted to the AWS region **ap-south-1.**
* Here are the below Configuration can be changed for deployment stack.

Content from deploy.sh file.



Deployment Command:



## Result:

Upon execution of the `deploy.sh` script, the CloudFormation Template will automatically deploy the infrastructure for the Splunk Application within a Virtual Private Cloud (VPC). This infrastructure will include an Application Load Balancer (ALB), Internet Gateway (IG), and all necessary Security Groups (SG). Additionally, the deployment process will include the creation of a certificate for the specified domain to ensure secure communication. Moreover, the CloudFormation Template will facilitate seamless updates, enabling easy management and modification of the deployed infrastructure.