**Requirement Document**

|  |  |
| --- | --- |
| **Work Effort Name** | Requirement Document |
| **Prepared By** | KAVYA S |
| **Document Issued Date** | 28.02.2024 |
| **Document Version** | 5 |
| **Reviewed By** | MAHAVISHNU |
| **SA Certificate Number** |  |

| **Version No.** | **Date** | **Revised by** | **Description of Changes** |
| --- | --- | --- | --- |
| 1. | 28.02.24 | KAVYA S | Architecture diagram, Repository details, Guardrails and Scp’s,Resouce specifications, Flow diagram, Table of contents, Specifications table |
| 2. | 01.03.24 | KAVYA S | Table of contents, Font changes, Architect diagram, Terraform details. |
| 3. | 04.03.24 | KAVYA S | Abbreviations, Flow diagram , Font changes, Alignments. |
| 4. | 04.03.24 | KAVYA S | AFT explanation,Prerequirement of control tower ,Architect diagram |
| 5. | 05.03.24 | KAVYA S | Architect diagram. |

Table of Contents

[1. PROJECT TITLE AND OBJECTIVE 4](#_Toc1209586672)

[2. INTRODUCTION 4](#_Toc1554769867)

[3. PURPOSE 4](#_Toc1096342163)

[4. INFRA-AUTOMATION RESOURCES 5](#_Toc505024090)

[5.RESOURCE SPECIFICATIONS 5](#_Toc1682533356)

[6. SUBNET SPECIFICATIONS 5](#_Toc363675462)

[7.TOOLS REQUIRED 6](#_Toc1320738159)

[8.ORGANIZATIONAL UNITS 6](#_Toc1403373938)

[9.ACCOUNTS UNDER ORGANIZATIONAL UNITS(OU) 6](#_Toc1246773326)

[10.OTHER REQUIREMENTS 6](#_Toc1813327229)

[11. PRE REQUISITES FOR CONTROL TOWER 6](#_Toc678652681)

[12. SCP’S AND GUARD RAILS UNDER OU’S 7](#_Toc2043950499)

[13. COMPONENTS UNDER ACCOUNT FACTORY FOR TERRAFORM(AFT) 7](#_Toc681102076)

[14. REPOSITORY DETAILS 7](#_Toc907546595)

[15.ARCHITECT DIAGRAM 8](#_Toc799326725)

[16.WORKING PROCEDURE: 9](#_Toc594418280)

[17. AWS CONTROL TOWER ACCOUNT FACTORY FOR TERRAFORM - ACCOUNT PROVISIONING WORKFLOW 10](#_Toc1131441941)

**AWS LANDING ZONE DEPLOYMENT USING TERRAFORM**

# 1. PROJECT TITLE AND OBJECTIVE

Title: AWS landing zone deployment using Terraform

Objective: Deploy a standardized AWS landing zone infrastructure using terraform, incorporating best practices for security, networking, and account management.

## 2. INTRODUCTION

The deployment of a standardized AWS Landing Zone using Terraform represents a comprehensive approach to establishing a robust, secure, and well-organized cloud infrastructure. This project aims to seamlessly orchestrate the provisioning of AWS resources by incorporating industry best practices for security, networking, and account management. Leveraging tools such as AWS CLI/API and Terraform, we will create a modularized and scalable architecture, encompassing critical aspects like IAM policies, VPC architecture design, automated account provisioning, auditing, and compliance. The organizational structure will be defined with dedicated units for Logging, Security, Prod, and Non-Prod environments, and Service Control Policies will be employed to enforce policies across the AWS accounts. This endeavor will be accompanied by detailed documentation, including Terraform configuration files, network diagrams, IAM policies, and deployment logs, offering a comprehensive guide to both the deployment process and the ongoing management of the AWS Landing Zone.

## 3. PURPOSE

The purpose of this project is to deploy a standardized AWS Landing Zone infrastructure using Terraform, emphasizing best practices for security, networking, and account management. Leveraging tools such as AWS CLI/API and Terraform, the project encompasses the creation of an organized VPC architecture with secure network measures, automated account provisioning, and compliance monitoring. Detailed documentation will be produced, including Terraform configuration files, network diagrams, IAM policies, and deployment logs, showcasing successful infrastructure provisioning. The project places a strong emphasis on security, implementing IAM role and permission management, Service Control Policies (SCPs), and network security measures. Organizational units, such as Log, Security, Prod, and Non-Prod, will be established to streamline account management. Tagging policies enforcement and secret management strategies will enhance resource organization and security. Compliance monitoring through AWS Config Rules, centralized logging, and auditing mechanisms will ensure adherence to security standards. The project aims to provide a robust, well-documented, and continually improving AWS Landing Zone infrastructure aligned with best practices and organizational requirements.

## 4. INFRA-AUTOMATION RESOURCES

Resources to be created

* VPC and its components (subnets, nat gateway, route table, security group, Access Control List(ACL),Internet Gateway( IGW))
* AFT- Account factory for terraform (For automation)
* AWS control tower
* AWS config
* IAM – Identity access management
* Cloud trail
* Security Hub
* S3
* Transit gateway
* AWS resource access manager.
* AWS Root account.
* AWS cloud formation Stacksets

## 5.RESOURCE SPECIFICATIONS

|  |  |  |
| --- | --- | --- |
| **RESOURCE** | **SPECIFICATIONS** | **REGION** |
| VPC - aws\_vpc | CIDR -192.32.0.0/16 | N VIRGINA |

## 6. SUBNET SPECIFICATIONS

|  |  |  |  |
| --- | --- | --- | --- |
| **SUBNET** | **NAME** | **RANGE** | **AVAILABILITY ZONE** |
| PRIVATE SUBNET - 1 | private\_subnet\_1 | 192.32.1.0/24 | Us-east-1a |
| PRIVATE SUBNET - 2 | private\_subnet\_2 | 192.32.2.0/24 | Us-east-1b |
| PUBLIC SUBNET - 1 | public\_subnet\_1 | 192.32.3.0/24 | Us-east-1a |
| PUBLIC SUBNET - 2 | public\_subnet\_2 | 192.32.4.0/24 | Us-east-1b |

## 7.TOOLS REQUIRED

* Terraform
* AWS CLI.

## 8.ORGANIZATIONAL UNITS

* Production
* Non production
* Log
* Security.

## 9.ACCOUNTS UNDER ORGANIZATIONAL UNITS(OU)

* Prod account 1 for production OU.
* Non prod account 1 for non production OU.
* Log archive account under security OU.
* Audit account under security OU.
* Log account 1 under Log OU.

## 10.OTHER REQUIREMENTS

* AWS SSO (Single Sign On)
* Service control policies (SCP’S)
* Guard Rails.
* Cross account audit
* Service catalog
* SNS (Simple Notification Service)

## 11. PRE REQUISITES FOR CONTROL TOWER

* Integrated services limits include - AWS cloud formation
* AWS Cloud trail
* Amazon cloudwatch
* AWS config
* AWS IAM
* AWS Lambda
* AWS Organization
* AWS Simple Notification Service
* AWS Single Sign On
* AWS Step functions
* AWS S3.

## SCP’S AND GUARD RAILS UNDER OU’S

**LOG OU**

* **CloudTrail Logging**
* **Restrict Key Management Service (KMS) Access**

**SECURITY OU**

* **IAM User/Group Restriction**
* **VPC Security Controls**

**PRODUCTION OU**

* **Data Classification Controls**
* **Change Management Guardrail.**

**NON PRODUCTION OU**

* **Resource Cleanup Guardrail.**
* **Testing Policies**

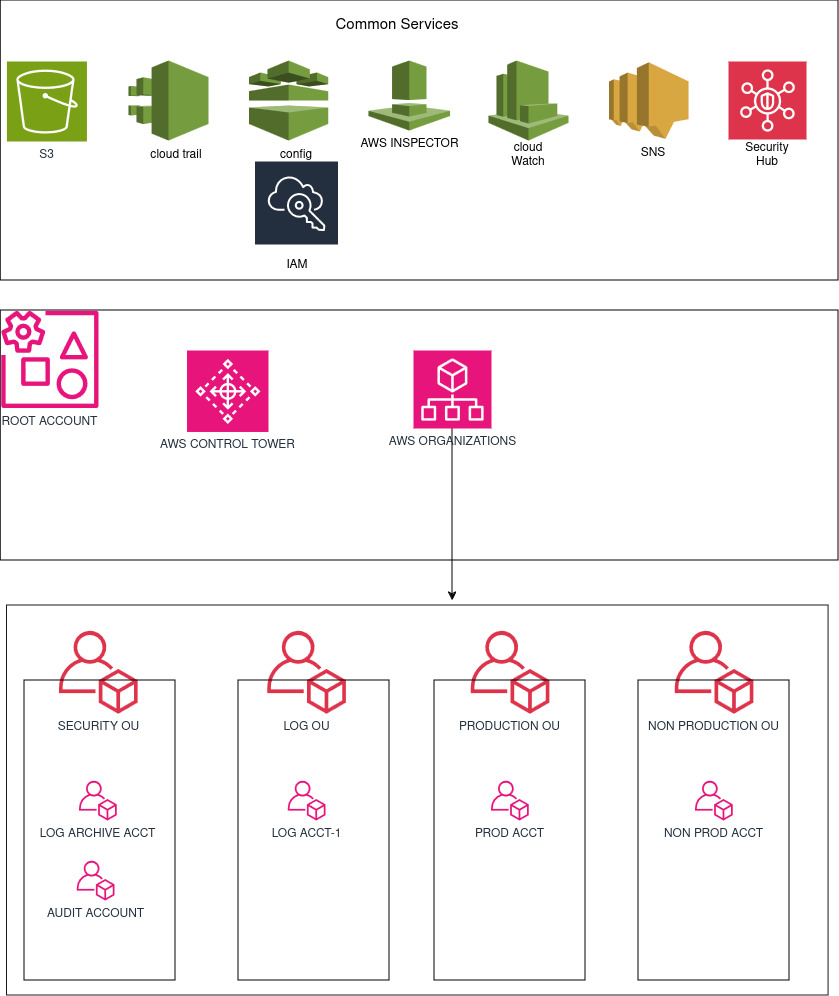
## COMPONENTS UNDER ACCOUNT FACTORY FOR TERRAFORM(AFT)

* **Terraform Configs**
* **AWS Code pipline**
* **AWS Code build**
* **Artifact repository**
* **Source code repository (VCS) (Github)**
* **IAM roles and policies**
* **Logging and monitoring.**

## 14. REPOSITORY DETAILS

|  |  |
| --- | --- |
| **Repository Name** | **Purpose** |
| Landing\_zone | To host the code |

## 15.ARCHITECT DIAGRAM

****

1. Under AWS organization 4 Organizational Units are created.
2. Under security OU default two accounts will be created - log archive account and audit account.
3. A production account under production OU and a non production account under Non production OU is created.
4. A log account under Log OU is created to store the log.
5. AWS control tower is enabled to provision all the accounts.

6.Common services include S3,IAM,Cloud trail,Cloud watch,security hub and inspector are mentioned.

## 16.WORKING PROCEDURE:

STEP -1 **Prepare AWS Environment -** Set up an AWS account and ensure necessary permissions for AWS Control Tower.

STEP - 2 **Install AWS CLI and Terraform.**

**STEP - 3 Set Up AWS Control Tower.**

**STEP - 4 Organize Organizational Units (OUs) in AWS Control Tower -** Define OUs like "Log," "Security," "Prod," and "Non-Prod" in AWS Control Tower.

STEP - 5 **Create Terraform Code Repository -** Set up a version-controlled repository(GITHUB) to store Terraform code.

**STEP - 6 Design VPC Architecture -** Develop Terraform modules for VPC architecture in the root account considering security and scalability.

STEP - 7 **Define IAM Policies -**  Write Terraform configurations for IAM roles and policies following the principle of least privilege.

**STEP - 8 Implement Service Control Policies (SCPs) -** Configure Terraform modules to enforce Service Control Policies in AWS Control Tower.

**STEP - 9 Set Up Tagging Policies -** Define Terraform configurations to enforce tagging policies for consistent resource tagging.

STEP - 10 **Automate Account Provisioning -** Use Terraform to create modules for the Account Factory within AWS Control Tower for automated AWS account provisioning.

**STEP - 11 Implement Network Security Measures -** Configure Terraform modules for network security measures, including NACLs and Security Groups.

**STEP - 12 Enable Auditing and Compliance -** Set up AWS CloudTrail and AWS Config for auditing and compliance monitoring. Use Terraform to configure logging and centralize logs in Amazon S3.

**STEP - 13 Secret Management Strategies -** Implement Terraform configurations for secret management using AWS Secrets Manager or other strategies.

STEP - 14 **Deploy the Landing Zone -** Execute Terraform commands to deploy the landing zone infrastructure, including VPCs, IAM roles, and network configurations.

## AWS CONTROL TOWER ACCOUNT FACTORY FOR TERRAFORM - ACCOUNT PROVISIONING WORKFLOW

STEP - 1 New account request

STEP - 2 AFT account request repository.

STEP - 3 Account request pipeline

STEP - 4 The request will be sent to request table and the request trigger function will invoke.

STEP - 5 If there is control tower update it will be sent to account request queue and there will be account request processor and sent to the AWS service catalog under control tower management account.

STEP - 6 If there is no control tower update it will go to the Account provisioning invoker.

STEP - 7 Then it will be sent to the account provisioning state machine and the pipeline creation will be sent to the codebuild stage.

STEP - 8 When new customizations request is invoked it will be sent to customization invocation statemachine and sent to the invocation pipeline.

STEP - 9 If customizations are specified in the initial account provisioning requests,the customizations run only on targeted accounts,If there is an already provisioned account,furthur customizations need to be initiated and manually in the accounts pipeline.

STEP - 10 The entire AFT operations are done in the AFT management account.