# Automated HIPAA compliant Infrastructure Deployment on AWS

Table of Contents

Automated HIPAA compliant Infrastructure Deployment on AWS 1

Prerequisites 2

Architecture 2

Architecture Flow 2

CloudFormation Template Input Parameters 3

## Prerequisites

* Two SSH Key Pairs for server login.
* AWS Config recorder.
* AWS ACM – ARN of the certificate.
* S3 bucket with SSL certificate files. (.cert, .bundle)

## Architecture

The architecture includes the following components and features:

* Basic AWS Identity and Access Management (IAM) configuration with custom (IAM) policies, with associated groups, roles, and instance profiles.
* Standard, external-facing Amazon Virtual Private Cloud (Amazon VPC) Multi-AZ architecture with separate subnets for different application tiers and private (back-end) subnets for application and database.
* Amazon Simple Storage Service (Amazon S3) buckets for encrypted web content, logging, and backup data.
* Standard Amazon VPC security groups for Amazon Elastic Compute Cloud (Amazon EC2) instances and load balancers used in the sample application stack.
* Three-tier Linux web application using Amazon EC2 Auto Scaling and Elastic Load Balancing, which can be modified and/or bootstrapped with customer application.
* A secured bastion login host to facilitate command-line Secure Shell (SSH) access to Amazon EC2 instances for troubleshooting and systems administration activities
* Encrypted, Multi-AZ Amazon Relational Database Service (Amazon RDS) MySQL database.
* Logging, monitoring, and alerts using AWS CloudTrail, Amazon CloudWatch, and AWS Config rules.
* Encrypted secondary EBS volumes on all EC2 instances.

### Architecture Flow

1. Master template will trigger nested template to create different components.
2. IAM template will be triggered to create IAM resources.
3. Logging template will be triggered to create CloudTrail, S3 buckets for CloudTrail and CloudWatch alarms, SNS.
4. Production Vpc template will be triggered to create network environment that provides a standard public facing application, separates private-public subnets and enforce traffic with NACL rules.
5. Management Vpc template will be triggered to create network environment for a standard management Vpc and a nested template will be triggered to create a bastion server.

**NOTE**: Management template will be triggered on successful execution of Step 4.

1. Application template will be triggered to deploy a web application with reverse proxy, Application Load Balancers, Auto Scaling., etc.

**NOTE**: This template will be triggered on successful execution of step 2, 3, 4 and 5.

1. Config Rule template will be triggered to set up AWS Config Rules.

**NOTE**: This template is optional.

## CloudFormation Template Input Parameters

1. **CF-Template Stack** **Name** - Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-).
2. **Database Password –** Mixed alphanumeric and must be between 8 and 28 characters and contain at least one capital letter.
3. **Notification Email Address** -Notification email address for security events.
4. **Existing SSH Key for the Bastion Instance** - The SSH key pair in your account to use for the bastion host login.
5. **Existing SSH Key for Other Instances** - The SSH key pair in your account to use for all other EC2 instance logins.
6. **Support Config** - Is AWS Config Rules already configured for this region?
7. **First Availability Zone** - Availability Zone 1
8. **Second Availability zone** - Availability Zone 2
9. **Operating System of the Instances** - Specify Operating system you want to use.
10. **Database Engine of RDS Instance** - Specify the Database Engine.
11. **AWS ACM ARN** - SSL Certificate for application load balancer.
12. **Tag Parameter** - Specify Tag for the Stack.
13. **EnvType** – Environment Type.

Following parameters have static value.

1. Quick Start S3 Bucket Name
2. Quick Start S3 bucket region
3. Quick Start S3 Key Prefix
4. pVPCTenancy

Following parameters and values are hardcoded, but can be made dynamic in further development phases.

1. ***InstanceType***
2. ***EBS Volume type***

**NOTE**: As of now, the CloudFormation template are created considering **Amazon Linux 2** OS and **Maria DB** Database engine.