Infrastructure Documentation

Table of Contents

- Infrastructure Documentation
  - Overview
  - AWS Account Details
  - Network Architecture
  - Compute
  - Load Balancing
  - Security Groups
  - IAM
  - Storage
  - Secrets Management
  - Logging
  - DNS Configuration
  - Resource IDs
  - Terraform Commands
  - Useful AWS CLI Commands

Infrastructure Documentation

Overview

This document describes the AWS infrastructure for the HIPAA-compliant POC application.

AWS Account Details

Item	Value
Account ID	730543776652
Region	us-east-2 (Ohio)
BAA Status	Signed via AWS Artifact

Network Architecture

VPC Configuration

Resource	CIDR/Value
VPC	10.0.0.0/16
Public Subnet 1	10.0.0.0/24 (us-east-2a)
Public Subnet 2	10.0.1.0/24 (us-east-2b)
Private Subnet 1	10.0.10.0/24 (us-east-2a)
Private Subnet 2	10.0.11.0/24 (us-east-2b)

Internet Connectivity

- **Internet Gateway**: Attached to VPC for public subnet internet access
- **NAT Gateway**: In public subnet, allows private subnet outbound traffic
- **Elastic IP**: Assigned to NAT Gateway

VPC Endpoints (PrivateLink)

Endpoint	Type	Purpose
ssm	Interface	SSM Session Manager
ssmmessages	Interface	SSM Session Manager
ec2messages	Interface	SSM Session Manager
s3	Gateway	S3 access without NAT

Compute

EC2 Instance

Setting	Value
Instance Type	t3.small
AMI	Amazon Linux 2023
Subnet	Private Subnet 1
IAM Role	hipaa-poc-ec2-role

Storage

Volume	Size	Type	Encrypted
Root	20 GB	gp3	Yes
Data	10 GB	gp3	Yes

The data volume is mounted at `/data` and contains the SQLite database.

Load Balancing

Application Load Balancer

Setting	Value
Type	Application (Layer 7)
Scheme	Internet-facing
Subnets	Public Subnet 1 & 2
Security Group	hipaa-poc-alb-sg

Listeners

Protocol	Port	Action
HTTP	80	Redirect to HTTPS
HTTPS	443	Forward to target group

Target Group

Setting	Value
Protocol	HTTP
Port	80
Health Check	GET / (HTTP 200)

SSL/TLS

Setting	Value
Certificate	ACM (DNS validated)
Policy	ELBSecurityPolicy-TLS13-1-2-2021-06
Domain	taxplanner.app

Security Groups

ALB Security Group (hipaa-poc-alb-sg)

Direction	Port	Source	Description
Inbound	443	0.0.0.0/0	HTTPS
Inbound	80	0.0.0.0/0	HTTP (redirect)
Outbound	All	0.0.0.0/0	All traffic

EC2 Security Group (hipaa-poc-ec2-sg)

Direction	Port	Source	Description
Inbound	80	ALB SG	HTTP from ALB
Outbound	All	0.0.0.0/0	All traffic

VPC Endpoints Security Group (hipaa-poc-vpce-sg)

Direction	Port	Source	Description
Inbound	443	VPC CIDR	HTTPS from VPC
Outbound	All	0.0.0.0/0	All traffic

IAM

EC2 Instance Role (hipaa-poc-ec2-role)

Attached Policies:

1. `AmazonSSMManagedInstanceCore` (AWS Managed)
   - Allows SSM Session Manager access
2. `hipaa-poc-s3-backup` (Inline)
   - s3:PutObject, GetObject, ListBucket, DeleteObject
   - Resource: Backup bucket only
3. `hipaa-poc-secrets` (Inline)
   - secretsmanager:GetSecretValue
   - Resource: App secrets only

4. `hipaa-poc-cloudwatch` (Inline)
    - logs:CreateLogGroup, CreateLogStream, PutLogEvents
    - Resource: /hipaa-poc/* log groups

Storage

S3 Backup Bucket

Setting	Value
Name	hipaa-poc-backups-730543776652
Versioning	Enabled
Encryption	SSE-S3 (AES256)
Public Access	Blocked

Lifecycle Rules: - Transition to Glacier after 30 days - Delete after 365 days - Delete old versions after 90 days

Bucket Policy: - Deny unencrypted uploads - Deny insecure transport (HTTP)

Terraform State Bucket

Setting	Value
Name	hipaa-poc-tfstate-730543776652
Versioning	Enabled
Encryption	SSE-S3 (AES256)
DynamoDB Lock Table	hipaa-poc-tfstate-locks

Secrets Management

AWS Secrets Manager

Secret	Content
hipaa-poc/app-secrets	GOOGLE_CLIENT_ID, GOOGLE_CLIENT_SECRET, APP_SECRET, DB_ENCRYPTION_KEY

Secrets are retrieved by EC2 at boot time via IAM role.

Logging

CloudWatch Log Groups

Log Group	Retention	Purpose
/hipaa-poc/application	90 days	Application logs
/hipaa-poc/audit	365 days	Audit trail

DNS Configuration

Required Records

Type	Name	Value
CNAME	_acm-validation	(from ACM)
CNAME	taxplanner.app	hipaa-poc-alb-xxx.us-east-2.elb.amazonaws.com

Resource IDs

Resource	ID
VPC	vpc-0dbc4f0061da966f5
EC2 Instance	i-0500bfb3b4ad44e24
ALB	hipaa-poc-alb
Target Group	hipaa-poc-tg
S3 Bucket (Backups)	hipaa-poc-backups-730543776652
S3 Bucket (TF State)	hipaa-poc-tfstate-730543776652
Secrets Manager	hipaa-poc/app-secrets

Terraform Commands

```
# Initialize (first time or new machine)
cd terraform
terraform init

# Plan changes
terraform plan

# Apply changes
terraform apply

# Destroy (CAREFUL!)
terraform destroy
```

Useful AWS CLI Commands

```
# Connect to EC2 via SSM
aws ssm start-session --target i-0500bfb3b4ad44e24 --region us-east-2

# View CloudWatch logs
aws logs tail /hipaa-poc/application --follow --region us-east-2

# Download backup from S3
aws s3 cp s3://hipaa-poc-backups-730543776652/backups/latest.sqlite.gz . --
        region us-east-2

# Get secret value
aws secretsmanager get-secret-value --secret-id hipaa-poc/app-secrets --region
        us-east-2
```