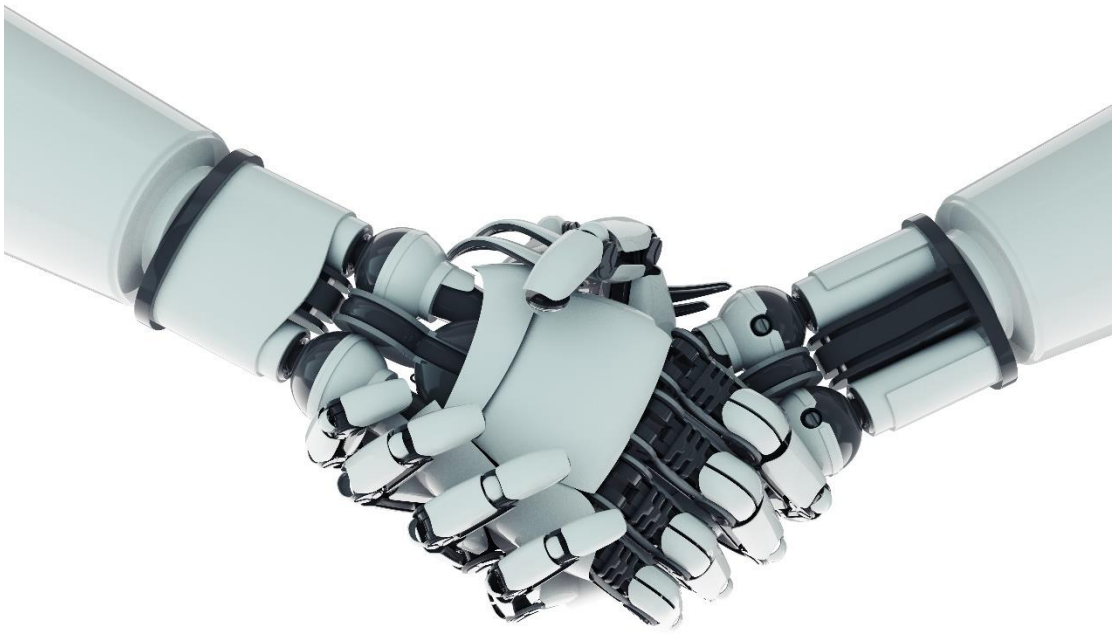

AWS Configuration

Oban Production Environment

Table of Contents

1. Introduction

This document outlines the detailed design specification for the deployment of the production messaging gateway infrastructure into Amazon Web Services (AWS). The focus of this document is the AWS components of the build. This document does not detail any design details of the Oban platform itself.

2. Solution Overview

Figure 1 provides a high-level overview of the deployment of the Oban platform in AWS.

Systems with a low Recovery Time Objective (RTO) are configured with Elastic Load Balancers (ELB) and Autoscaling to provide automated failure detection and recovery.

Systems in the public subnets are accessible from the internet on https protocol.

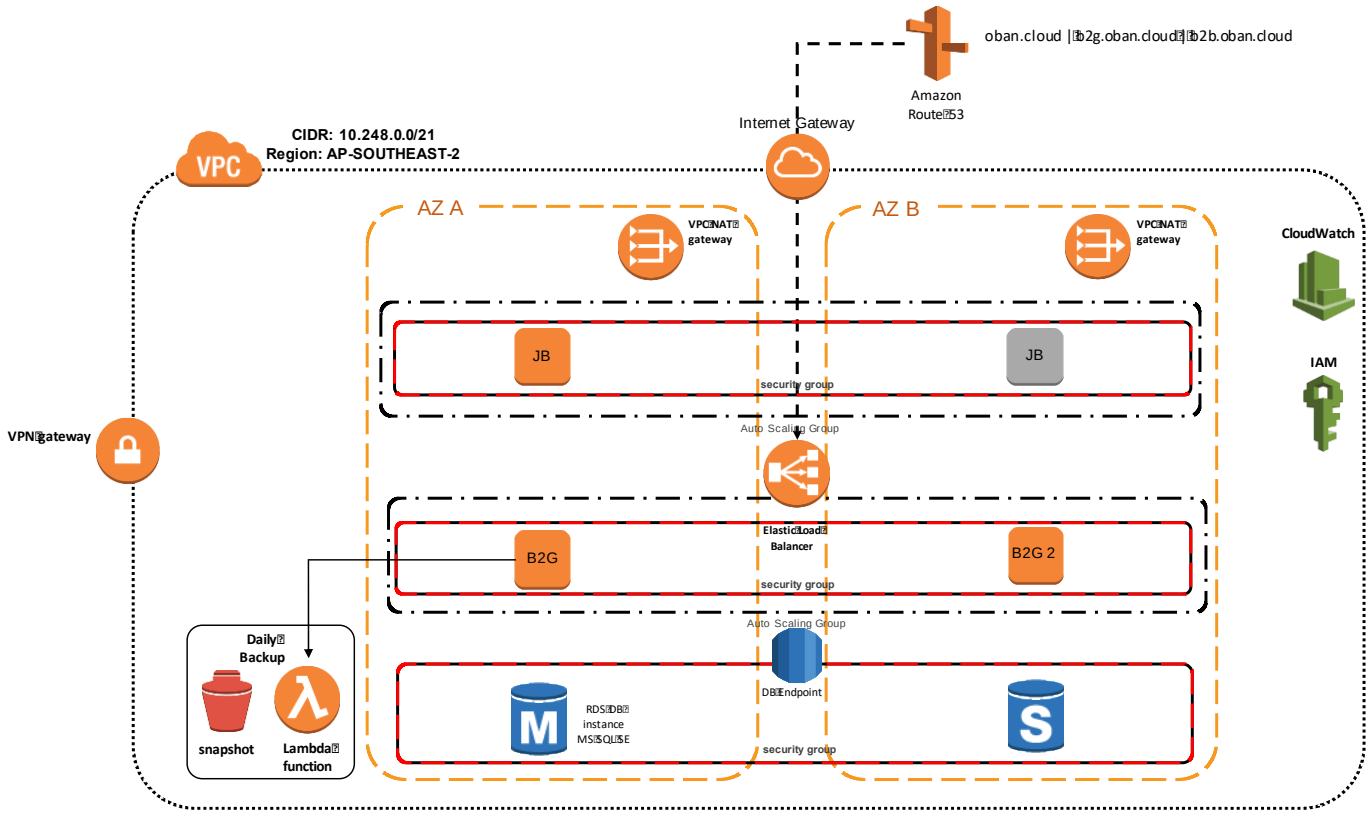

Figure 1 – High Level architecture in AWS

3. AWS Functional Configuration

3.1. Identity and Access Management (IAM)

Identity and Access Management (IAM) is an AWS service enabling the management of users and permissions governing access to AWS resources.

The following IAM groups have been defined:

Group Name	Associated Policies
Admin	Administrator access
Infrastructure Team	Allow all
Development Team	Read only access

3.1.1. Roles

The following IAM Roles have been defined:

Role Name	Associated Policies
Lambda Backups	AutoScalingFullAccess, AmazonEC2FullAccess
EC2_Query	AmazonEC2ReadOnlyAccess
CFNAdmin	CloudFormationFullAccess
SSM	AmazonEC2RoleforSSM

3.1.2. SSL Certificates

AWS has a certificate management service from where SSL certificates can be generated or imported for use with AWS services.

3.2. Networking (VPC)

Amazon Virtual Private Cloud (VPC) is a virtual network defined in AWS. Resources are provisioned into this virtual network. The virtual network contains subnets, NAT Gateways, an Internet Gateway, ACLs and Security Groups to manage traffic, and in the Oban Prod environment, EC2 instances and an RDS database are provisioned within the VPC.

3.3. Compute (EC2)

AWS EC2 provides compute resources and associated services. The associated services include functionality such as Elastic Load Balancing (ELB) and Autoscaling which are configured as part of the environment.

3.3.1. Key Pairs

Key Pairs are SSH keys that enable access to EC2 instances. For Windows instances the sole purpose of the Key Pair is to gain the administrator password for an instance when it is launched.

3.3.2. Instances

There are multiple EC2 instances are running in the Prod VPC.

3.3.3. Elastic Load Balancing (ELB)

Elastic Load Balancing (ELB) is a feature of EC2 where a persistent DNS name is made available to then pass traffic to one or more instances associated with the ELB. The ELB can be linked to an autoscaling group, which manages the instances. Autoscaling and Load Balancing is configured for the B2G server.

3.3.4. Autoscaling

Autoscaling is another feature of EC2 where under specific circumstances EC2 instances can be launched and terminated based on polices assigned to an autoscaling group. The autoscaling group has an associated launch configuration which contains the configuration required for launching new instances.

The typical implementation of autoscaling involves having a number of instances servicing an application, and the number of instances increasing / decreasing based on load.

In the Oban environment, autoscaling is used as a HA feature, catering for the event of a failed EC2 instance in which case it is automatically replaced with a healthy instance. This guarantees there is always two instances maintained of the B2G server.

3.4. Relational Database Service (RDS)

Amazon's Relation Database Service (RDS) is a managed database service provided by AWS. When an RDS instance is provisioned, you only interact with and connect to the database; all the supporting infrastructure and Operating System associated with the database instance is abstracted from you.

Provisioning an RDS instance also removes the need to perform any database setup, and you can switch on automatic backups and replication.

Oban uses *'Microsoft SQL Server Standard Edition on RDS'.*

3.5. Storage

AWS provides a number of storage options, two of which are used by Oban:

Elastic Block Store (EBS) – This is block based volumes that are presented to EC2 instances
Simple Storage Service (S3) – This is object based storage - multiple AWS services can read and write files to.

3.5.1. Elastic Block Storage (EBS)

EBS Volumes

A number of EBS volumes exist in AWS for the Oban platform.

EBS Snapshots and AMI Backups

EBS has a snapshotting capability, where snapshots can be taken as backups of EBS volumes. To be able to boot from one of these volumes, the snapshot needs to be converted into an Amazon Machine Image (AMI). There is an automated function to create AMI images, and expire the images and their associated snapshots. This is performed by Lambda functions and covered in section 3.6 Serverless Execution (Lambda) of this document.

3.5.2. Simple Storage Service (S3)

S3 Buckets

A single S3 bucket is created for storing Cloudtrail Logs.

3.6. Serverless Execution (Lambda)

AWS Lambda is a serverless compute service that runs code without the need for the user interacting with any of the compute resources. You create a function containing the code, and specify a trigger that will trigger the code to run.

The EBS snapshots and AMI creation/expiry are managed by AWS Lambda functions.

3.6.1. Functions

The following Lambda functions are defined:

- Create an AMI daily
- Create an AMI, update launch configuration
- Remove AMIs older than the delete after tag
- Tag all EBS snapshots after AMI creation
- Check status of backups

3.6.2. Triggers

For the Lambda function to be executed, something needs to trigger it. Cloudwatch Events / Rules are configured to trigger the aforementioned Lambda functions.

The triggers occur daily.

3.7. Monitoring and Alerting

3.7.1. Cloudwatch

Cloudwatch will monitor a collected metric, and perform a specified action. The following cloudwatch alarms are defined in the environment:

- Error in the AMI create
- Error in the AMI update launch configuration
- Error in the removal of older AMIs
- Failed EC instance check
- Unhealthy ELB host count
- EC - CPU utilisation
- EC – Memory capacity
- EC – Disk capacity
- RDS – CPU utilisation
- RDS – high read latency
- RDS – high write latency

3.7.2. System Manager Services

EC2 instances come pre-configured with Systems Manager Services Agent (SSM). The agent allows users to leverage the AWS console to perform managements task without logging into the host. The functionality is used to gather the custom monitoring metrics for Memory and Disk.

A new IAM role is created and attached to each EC2 instance to perform this: **Amazon-SSM-Role**

3.7.3. Cloudtrail

Cloudtrail is enabled to track user and API usage.

3.7.4. Simple Notification Service (SNS)

There is a single SNS topic to provide email notifications. Email addresses are subscribed to the topic, and Cloudwatch pushes notifications to the SNS topic which go to Oban's managed services provider (Advent One).