**Low Level Solution Design**

**HNAS to AWS migration (Prod Environment)**

* SUBMITTED TO: Iberia
* SUBMITTED BY: Coforge Inc.
* SUBMISSION DATE: 19th Nov 24

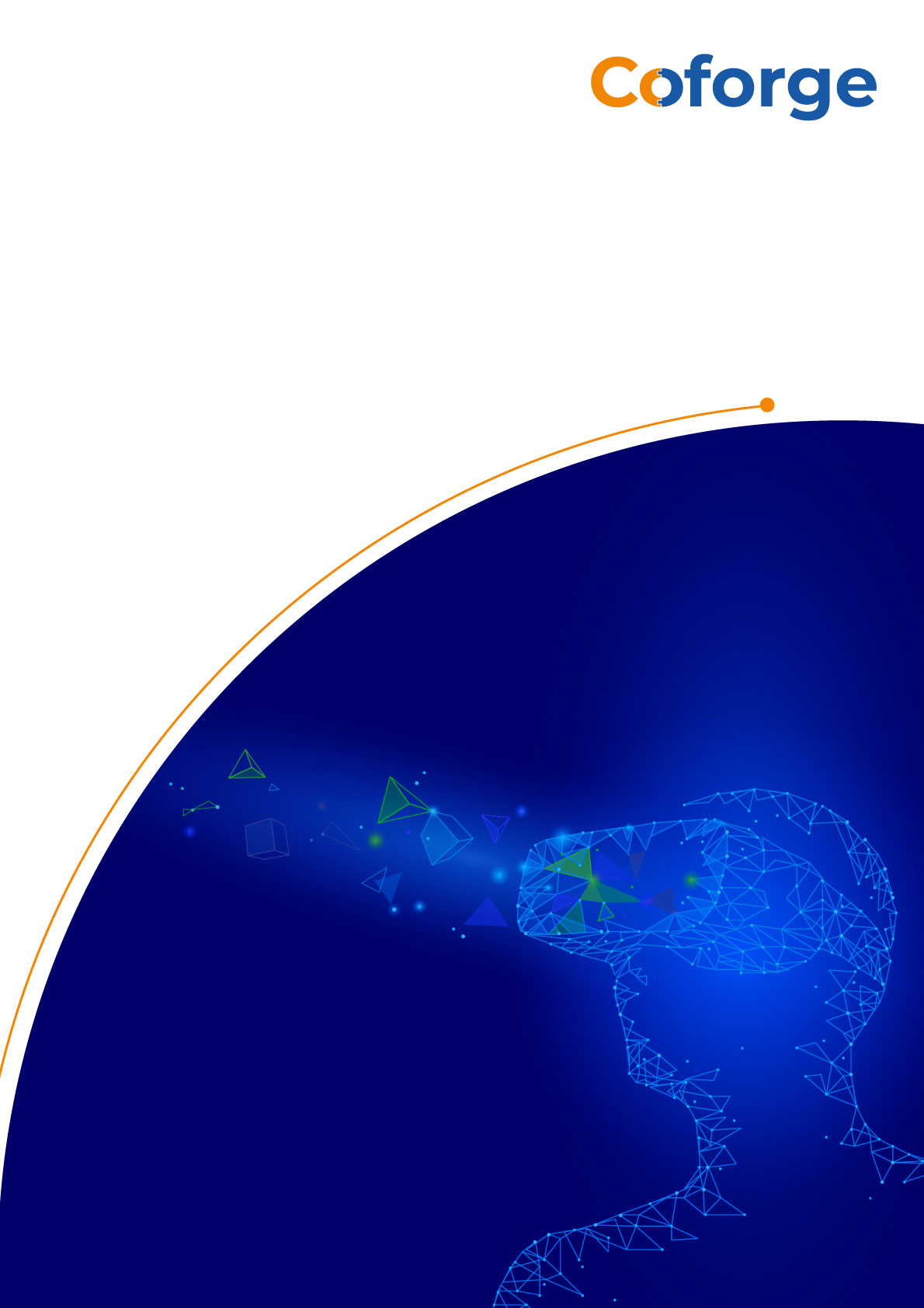


Table of Contents

[**1** **Abstract** 3](#_Toc182912798)

[**2** **Scope Definition** 3](#_Toc182912799)

[**3.** **Current State of Infrastructure** 4](#_Toc182912800)

[**4** **Architecture Considerations** 5](#_Toc182912801)

[4.1 Current Reference Architecture Model - Iberia 5](#_Toc182912802)

[4.2 Architecture Model – OSB - Production Environment 5](#_Toc182912803)

[4.2.1 Architecture Standards 6](#_Toc182912804)

[4.2.1.1 AWS Account Standard 6](#_Toc182912805)

[4.2.1.2 Network Standards 7](#_Toc182912806)

[4.2.1.3 Applications Standards 7](#_Toc182912807)

[4.2.1.4 Security Standards 8](#_Toc182912808)

[4.2.1.5 Tagging 8](#_Toc182912809)

[4.2.1.6 Deployment via Terraform 9](#_Toc182912810)

[4.2.1.7 Monitoring 9](#_Toc182912811)

|  |  |  |
| --- | --- | --- |
| **Author** | **Position / Responsibility** | **Date** |
| Vonteddu Krishna Bhaskar | Solution Architect / AWS | 19th Nov 2024 |
| Sachin Choudhary | Project Manager | 19th Nov 2024 |

|  |  |  |
| --- | --- | --- |
| **Document Approval** | | |
| Name | Position / Responsibility | Date |
| Alberto (iBeria) | Cloud Lead (IB Operations) | 2024 |
|  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Document Index** | | | |
| Version No | Date | Modified/Created By | Nature of Amendment |
| 0.1 | 19th Nov 2024 | Vonteddu Krishna Bhaskar | Initial Draft |
| 0.2 | 26th Nov 2024 | Vonteddu Krishna Bhaskar | Final version |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# **1 Abstract**

This document serves as the solution architecture for executing the project of migrating the OSB servers to AWS.

It includes AWS-centric high level architectural considerations, and sizing recommendations to support Cloud Solution Sets. The approach defined in this architecture takes existing functionality into consideration reckoning the security of running workloads and hinges on the re-usable architecture patterns that could be extended to incorporate fault tolerance and autoscaling into to the design.

# **2 Scope Definition**

Iberia has engaged Coforge to migrate the below listed OSB servers to AWS cloud.

1. Coforge will be performing migration from OSB servers On-Prem to AWS.

2. Coforge will be Creating a similar environment like OSB On Prem and application team will be configuring their application accordingly.

3. Coforge will be working on any issues reported during the time of the migration project.

4. Post migration and hyper care, Coforge will hand over the service to Iberia’s cloud support supplier.

The in-scope services are –

* AWS EC2 instances.
* ALB configuring.
* EFS File system and sharing the same between both the OSB servers.

The out-of-scope services are –

* Any changes On-Premises like network changes, firewall changes etc.

In the event of a requirement to perform migration these will be performed by involved 3rd parties (Iberia team or other suppliers).

* AWS Cloud Disaster Recovery

Coforge will enable backup/DR during project phase. Rest of the DR activities will be taken care by Iberia’s cloud support supplier team during the incident of disaster.

* Software licenses (on-premises, AWS, OneDrive)

Any licensed software will be provided by Iberia

* Provisioning of network and bandwidth between source and target

Network connectivity will be provided by Iberia

* Non-Functional Testing e.g., Performance and Security testing of application, infra & network

This will be part of the scope for application migration threads.

# **3. Current State of Infrastructure**

Current Architecture

Landscape of existing OSB architecture is shown in below figure:

<https://github.com/Iberia-Ent/service-delivery--cloud-support--osb-design/blob/main/docs/Existing-OSB-architecture.jpg>

# **4 Architecture Considerations**

## 4.1 Current Reference Architecture Model - Iberia

Iberia utilizes a separate AWS account for each SDLC phase (also referred to as “environment”) of each application suite. These accounts are sub-accounts of the Wellful master account (AWS Organization), therefore enforcing common set of rules and policies to all accounts. Access is granted within the accounts via SSO integration, using AZ-SSO, mapped to IAM Roles in the account

Iberia has an automated continuous integration/continuous delivery (CI/CD) pipeline which uses GitHub as its code repository and GITHUB Actions for deployment to CI, DI using Terraform as Infrastructure Software tool.

## 4.2 Architecture Model – OSB - Production Environment

Reference Architecture model:

<https://github.com/Iberia-Ent/service-delivery--cloud-support--osb-design/blob/main/docs/Iberia%20OSB%20Architectural%20Diagram.pdf>

### 4.2.1 Architecture Standards

The AWS services which were considered for the OSB migration are: AWS EC2, ALB, AWS VPC, AWS EFS and s3 Gateway end point.

Amazon VPC Transit Gateways is a network transit hub used to interconnect virtual private clouds (VPCs) and on-premises networks. Hence any application which is in Iberia network can connect to the OSB servers. So, the application users who are trying to access the WebLogic service should be in Iberia network.

### 4.2.1.1 AWS Account Standard

* AWS accounts are divided into 2 accounts based on the Environment (OSB Pre and OSB Prod).
* The account names are as follows:

**workloads-prod-common**

**workloads-sdlc-pre-common**

AWS Account numbers are depicted in the below screenshot:

<https://github.com/Iberia-Ent/service-delivery--cloud-support--osb-design/blob/main/docs/AWS-accounts-details.png>

* Separate Environments are provisioned for Stage and Production environments.
* Above figureshows the high-level view of the AWS landing zone for the Production environment.
* The Disaster Recovery strategy for the Production environment will be Pilot Light Approach.

AWS Backup service is enabled on the EC2 instances and if any failure happens both the EC2 instances are built quickly using the Image (or snapshot) created by the Backup service. EFS file system will be mounted after the Instances are built and as EFS file system is AWS managed service, hence there won’t be any data loss.

### 4.2.1.2 Network Standards

* Production environment is created in be created in eu-west-1.
* Disaster Recovery setup for production environments will be in the same region. All network resources (e.g. VPC’s, subnets, route tables, NAT Gateways, Internet Gateways and Transit Gateways) for Prod environment is created in a separate infrastructure account and then shared to the respective Application Accounts for better management of network resources.
* CIDR ranges for Production environment will be (10.96.54.0/24).
* Production environment will have 2 subnets as below
* The details of the subnets created for Production environment are mentioned below.

|  |  |  |  |
| --- | --- | --- | --- |
| **Subnet Name** | **CIDR** | **IP's** | **AZ** |
| OCPAME2IDVN00014-private-eu-west-1b | 10.96.54.64/26 | 64 | eu-west-1 |
| OCPAME2IDVN00014-private-eu-west-1a | 10.96.54.0/26 | 64 | eu-west-1 |

* NAT Gateways will be configured in each Availability Zone for High Availability
* Separate route tables will be maintained for each private subnet.
* NACLs will be used and configured to control overall traffic flowing to each subnet tiers of the network
* Security groups will be used to restrict the application specific access for EC2 Instances and ALB..
* VPC flow logs will be enabled at the VPC level to monitor the incoming and outgoing traffic. The data from flow logs will be published to CloudWatch
* Below s3-Endpoint gateway is used for uploading any files from on-prem to AWS. ‘vpce-01a395aac1c1acdc3’ is the end-point ID.

### 4.2.1.3 Applications Standards

* GITOPS actions will be used as DevOps and CI/CD tool for automation. M5xLarge class instance is launched to build the OSB servers:

|  |  |  |
| --- | --- | --- |
| Server Name | Instance Name | IP Address |
| Osbprod5 | i-0c777cc064acc5324 | 10.96.54.40 |
| Osbprod4 | i-0c4ef0a69c263d10a | 10.96.54.25 |

* Application Load Balance details are as below:

Name: alb-prodosb-web

URL: internal-alb-prodosb-web-911517006.eu-west-1.elb.amazonaws.com

Ports: 6001 and 7001

### 4.2.1.4 Security Standards

* Application Layer and Database layer (if any) are hosted in Private Subnets, making sure the access is restricted from Internet.
* AWS security group acts as a virtual firewall for AWS FSx file system to control incoming and outgoing traffic. Both inbound and outbound rules control the flow of traffic to and traffic from the compute.
* Need to connect to Iberia VPN (Ivanti Secure Access) to connect to the AWS Windows Instance using Remote desktop (or) can connect from AWS console Terminal to connect to the EC2 instance.
* IAM policies will be created for the individuals and the access is restricted as per the requirements of the privileges. An IAM policy is created to assume the role for the GITHUB to run the Terraform Script.

### 4.2.1.5 Tagging

* All AWS Resources Production environment will be tagged using the Standard Tagging Conventions, described below

<https://github.com/Iberia-Ent/service-delivery--cloud-support--osb-design/blob/main/docs/tags.md>

### 4.2.1.6 Deployment via Terraform

* The deployment of all the environments will be done using Terraform.
* Terraform scripts are stored in Github repository – “https://github.com/Iberia-Ent/software-engineering--cloud--cloud-support--osb--infra”
* Github automated Actions and runners are setup up for CI/CD.
* Branching strategies are used to organize repositories and prevent merge conflicts.
* All changes are added to Feature branches first. Once all the testing is done and results are validated under terraform plan stage, Code is merged to main branch.
* CD is appliable only on main branch, after raising pull request from feature branch and other developer approves the request.
* Any change in the parameters of the AWS services will be managed from Terraform scripts for all the environments.

### 4.2.1.7 Monitoring

* CloudWatch alarms need to configured according to the situation and the mail notifications will be sent to relevant teams.
* CloudWatch Dashboards can be created to monitor the EC2 instances and the ALB.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*