Proposal for the Migration Of Workloads On

the AWS Platform

Noventiq

AWS Premier Consulting Partner - Noventiq

For

ZYKRR

Author: Pulkit Kumar
Version: V1.2
Document date: 08th March 2025

Revision History

Revision No.	Revision Date	Description of Change	Author	Approved By
1.0	07th MARCH 2025	Initial Document	Pulkit K	Vineet P
1.1	08th MARCH 2025	Removed High-Availability and DR	Pulkit K	Vineet P
1.2	08th MARCH 2025	Landing Zone deployment shifted in Phase 2	Pulkit K	Vineet P

1 Executive Summary

1.1 Confidentiality Notice

The information contained in this document has been prepared to be used in the context of this project. It should not be used as a model or precedent in any situation outside of this project. This document must not be copied or reproduced by any means without the authorization of the parties involved.

A great deal of effort has gone into the preparation of this document to ensure that the information presented is correct at the time of printing. The parties involved in this project assume no responsibility for any errors that may arise in the application of this information in a context other than the project for which it was prepared.

1.2 Introduction to Noventiq

Noventiq (Legal Entity Softline Holdings PLC) is a leading global solutions and services provider in digital transformation and cybersecurity, headquartered and soon to be listed on Nasdaq. The company enables, facilitates, and accelerates digital transformation for its customers' businesses, connecting 80,000+ organizations across all sectors with a vast selection of best-in-class IT vendors, alongside its own services and solutions. In May 2023, Noventiq announced its intent to list on Nasdaq through a proposed business combination with Corner Growth Acquisition Corp.

As a digital transformation catalyst and leader in Cybersecurity solutions, Noventiq has of 6,400+ employees working in ~60 countries throughout India, Asia, Latin America, Europe, the Middle East, and Africa – markets with significant growth potential.

Noventiq has over a decade of experience as a pioneering AWS Cloud Partner. We have a proven track record of guiding businesses through cloud migration and modernization. Our team holds the highest credentials with 6 major AWS competencies, 12 service validations, and over 250 certified AWS specialists, including solution architects holding 200 active AWS certifications. An AWS Global SCA Partner and a Premier Tier Services Partner, we demonstrate excellence across a range of specialities such as AWS Managed Services, Data & Analytics, Migration, and DevOps. We were also recognized as the AWS Data & Analytics Partner of the Year, APJ in 2022.

1.3 About Customer

Zykrr, founded in 2016 and headquartered in Gurugram, India, is an innovative AI-powered customer experience management platform. The company specializes in capturing and analyzing customer feedback across various channels to help businesses enhance their customer experience. Zykrr offers a comprehensive suite of tools, including a survey builder, real-time feedback collection, and AI-driven insights. The platform is designed to serve a wide range of industries, such as financial services, healthcare, retail, and travel. With a focus on data security, seamless integration, and actionable insights, Zykrr empowers businesses to create personalized and memorable customer experiences. The company has raised $121K in funding and is valued at $26.1M.

2 Project Objectives

Following is the high-level objectives of this project

- Phase 1- Migrate the existing AZURE (Central India) workloads to AWS Mumbai & AZURE (USA East 1) to AWS (N. Virginia region)
- Set up an AWS environment to host the application and database servers in the existing AWS organization.
- Phase 2- Implementation of foundational landing zone

3 Understanding of current infrastructure

- Zykrr' s current infrastructure is hosted on Microsoft Azure. (India & USA)
- Current infrastructure is configured with Single AZ.
- Application architecture is Microservice and hosted on Azure AKS.
- There are 6 Microservices running:
    - Diy
    - Insight
    - Survey
    - Zapi
    - Auth
    - Authentication
- Application tech-stack is React JS, NodeJS and JavaScript.
- There are Azure VMs for GitLab, Runner, FTP, Jump Server and test (Nginx, PM2).
- Zykrr are using Azure CDN for static content.
- Database – Postgres (Same is getting used in all the three regions)
- Azure ElastiCache for storing Content.
- Azure Network Firewall is configured in the India region.

3.1 Summary of existing Infrastructure

AZURE Managed Database

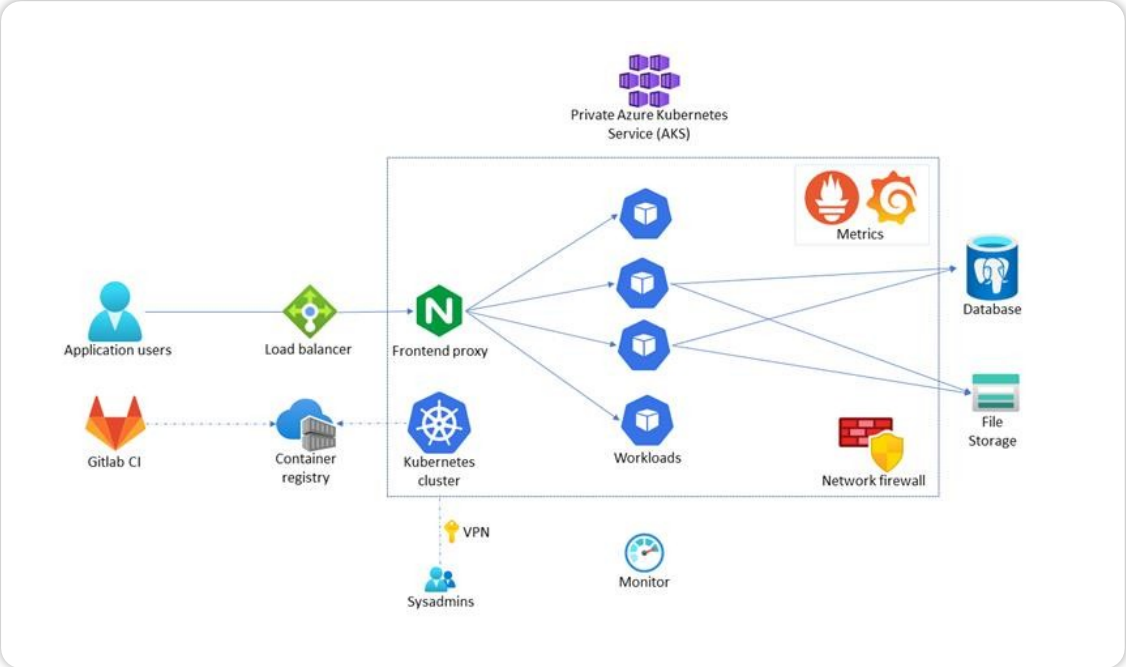
NAME	TYPE	LOCATION	CORE	STORAGE
d-prod-db-zykrr	Azure Database for PostgreSQL flexible server	Central India	48	1TB
test-zykrr-31-jul-new	Azure Database for PostgreSQL flexible server	Central India	16	100GB
us-zykrr-db-new	Azure Database for PostgreSQL flexible server	East US	32	128GB

AZURE VM Infrastructure

NAME	LOCATION	OS	STORAGE	CORE	RAM
zykrr-admin-zyva	Central India	Linux	30	4	32
us-sftp-machine	East US	Linux	30	2	8
text-analysis-1	Central India	Linux	30	2	16
test-zykrr	Central India	Linux	30	8	32
prod-ftp	Central India	Linux	60	2	4
prod-bastion	Central India	Linux	30	2	8
gitlab-Runner	Central India	Linux	30	4	16
bajaj-server-new	East US	Linux	30	8	32

- Azure Blob: 50 GB
- Azure Elastic Cache (Redis): 50 GB

3.2 Exiting Architecture Diagram



4 Scope of Work

Below is the high-level scope of engagement

- Phase 1 Migration of AZURE workload to AWS
  - AZURE Central India to AWS Mumbai
  - AZURE East US to AWS N. Virginia
- Phase 2 Implementation of foundational Landing zone

5 Proposed Solution

5.1 Phase 1 Migration of AZURE workload to AWS

5.1.1 Migration of Azure VM to AWS EC2

Cloud Infra Deployment

- Implementation Of Production setup in following regions – Mumbai and N.Virginia.

Network Implementation

- VPC, Sub Net, Route Table, Internet Gateway, Transit Gateway, Route 53
- Implementation Of ALB

DevOps Implementation

- Migrate AKS to EKS using KMF tool

Compute Implementation

- EC2 Instance Implementation
- EBS & S3 storage Implementation

Database Implementation

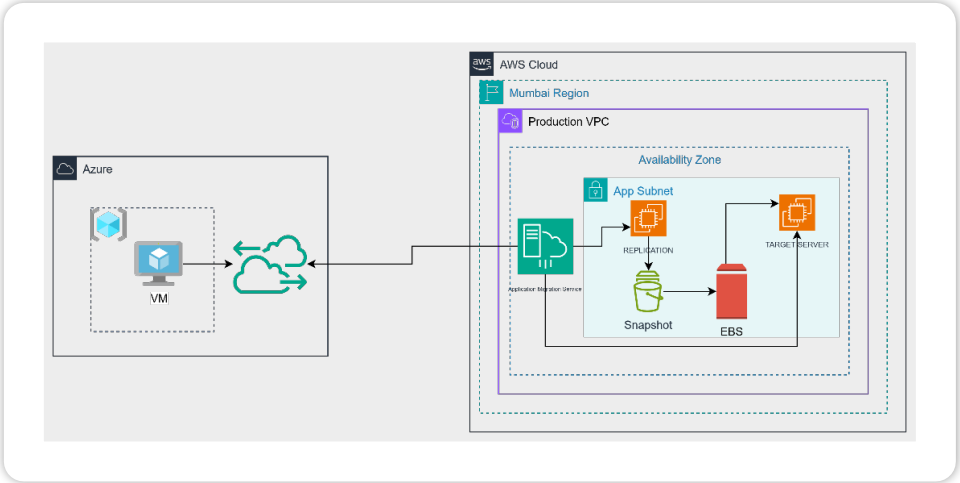
- Configuration of Postgres on RDS
- Migrate the existing Data of Postgres from AZURE to AWS

Other Services Implementation

- SKS,SNS, CloudWatch, Guard Duty, IAM
- Configuration of Amazon MQ.
- Configuration of AWS ElastiCache.

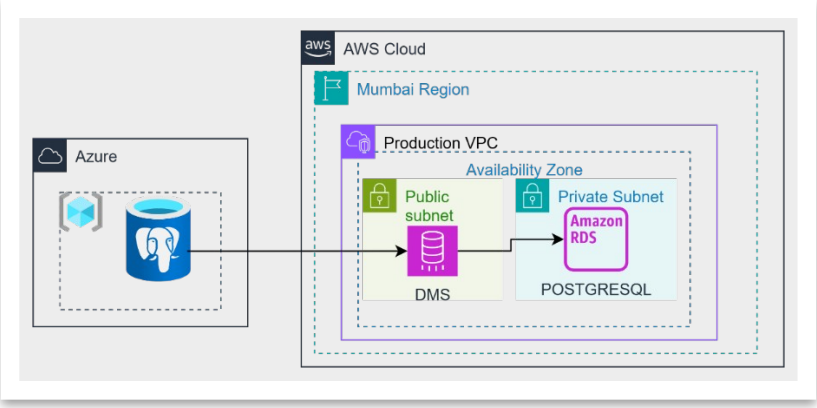
Security Implementation

- VPN Implementation
- WAF – AWS Native



- Set up a replication server in Azure to facilitate data transfer.
- Use AWS Application Migration Service (MGN) to automate and manage the migration process.
- Replicate Azure VMs to AWS using AWS Application Migration Service.
- Perform smoke tests to ensure VMs are running correctly on AWS.
- Conduct load testing to verify performance and scalability.
- Validate data integrity and consistency post-migration.
- Perform a final data sync to ensure all changes are captured.
- Switch production traffic to the AWS environment.
- Monitor the environment closely during the initial go-live period.

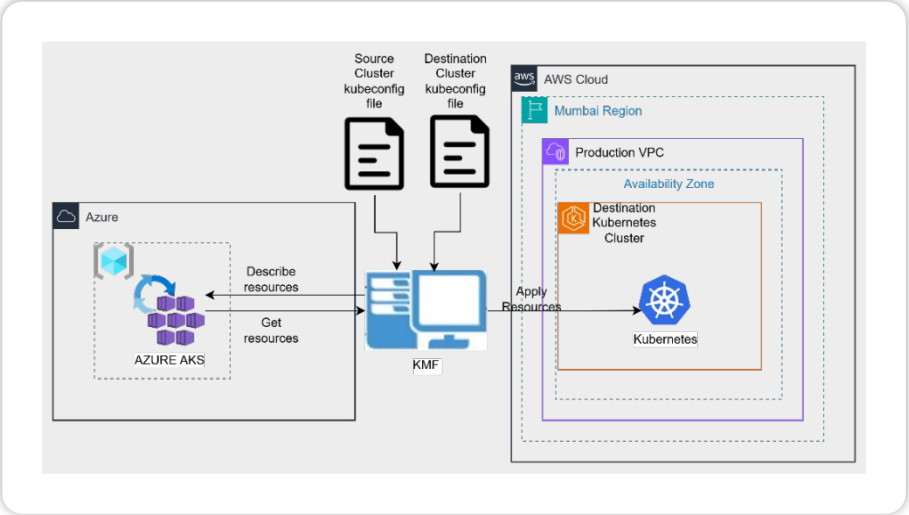
5.1.2 Migration of Azure Database for PostgreSQL to RDS for PostgreSQL



- The Noventiq team will ensure proper routing and the establishment of security group rules to allow traffic between the Azure Database for PostgreSQL and the RDS for PostgreSQL.
- The AWS DMS service will be configured on an EC2 instance launched in the same private subnet as the RDS for PostgreSQL.
- The Noventiq team will configure the necessary IAM roles and permissions needed for DMS to access both the source and destination endpoints.
- The source and destination endpoints will be registered with the AWS DMS service.
- Once the basic DMS setup is complete, a replication task will be created in AWS DMS to initiate database replication from the source to the destination.
- After replication is complete, the customer team must verify data consistency in RDS for PostgreSQL. This can be done by running checksums, comparing record counts, or executing sample queries.
- Once replication is finished, the tasks in DMS will be deleted, and the EC2 instance will be terminated.
- The customer's application team must integrate the application with the Amazon RDS for PostgreSQL instance and make any necessary changes to the application.

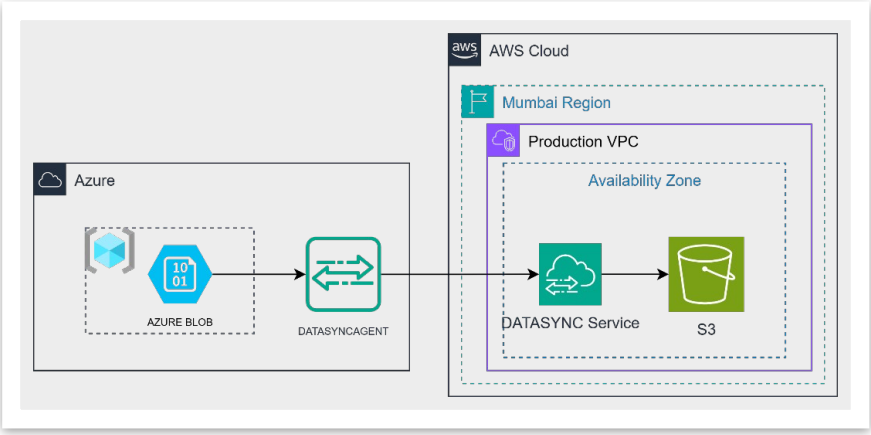
5.1.3 Migration of Azure AKS to AWS EKS

KMF is an open-source tool (Apache 2.0) that can migrate Kubernetes resources from a cluster running on Azure AKS to a cluster running on Amazon EKS. It is designed to coordinate and automate many of the manual processes, eliminating human error and speeding migration phases down to minutes from weeks of planning and data collection.



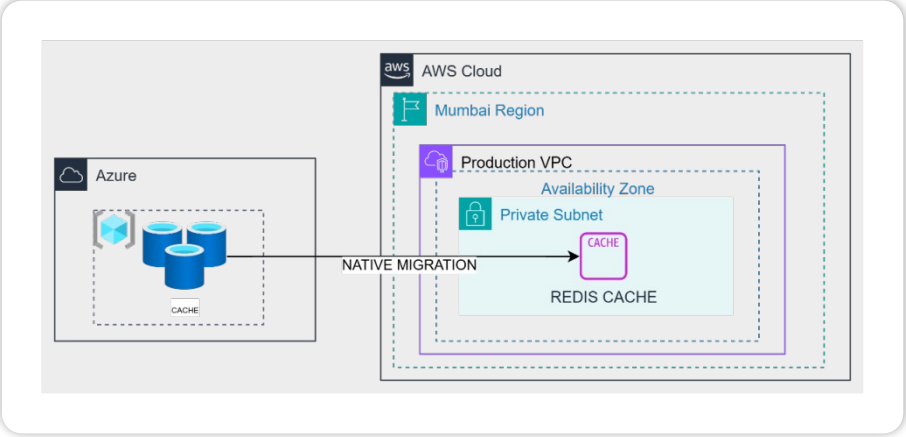
- Noventiq will connect the Zykrr team to list all the resources in the AKS cluster, including deployments, services, persistent volumes, and configurations.
- Perform initial compatibility checks to identify any Kubernetes features configurations that may not have direct equivalents in EKS or AWS services.
- Migration of data stored in Persistent Volumes, ConfigMaps, and Secrets.
- Configure the EKS cluster in AWS, ensuring it has the necessary capacity and configuration to match the AKS cluster running at the Zykrr' s Azure account.
- Export all Kubernetes manifests from the AKS cluster to be migrated to the AWS along with the Zykrr team.
- Install & configure KMF in the Azure account and will register the both source and target cluster with KMF.
- Noventiq team will migrate all application from Azure AKS to AWS EKS.
- Noventiq team will do the data migration and setting up services and ingress to match the configuration in AKS.
- Zykrr will do the functional and load testing of migrated application to AWS EKS.

5.1.4 Migration of data from Azure Blob to AWS S3



- Deploy the DataSync agent in the Azure.
- Configure the source and destination location in DataSync.
- Create a DataSync task to transfer data from the Blob Storage to the AWS S3.
- Start the DataSync task to begin the data transfer.
- Monitor the task progress and ensure data is being transferred correctly.
- Zykrr will validate the data in the AWS S3 bucket.

5.1.5 Migration of Azure ElastiCache (Redis) to AWS ElastiCache (Redis)



- Configure AWS ElastiCache (Redis)
- Make the connectivity in between Azure ElastiCache and AWS ElastiCache.
- Noventiq will use native migration method for migrating the cache (Redis).
- Zykrr will validate the migrated cache.

5.2 Phase 2 Implementation of Landing Zone

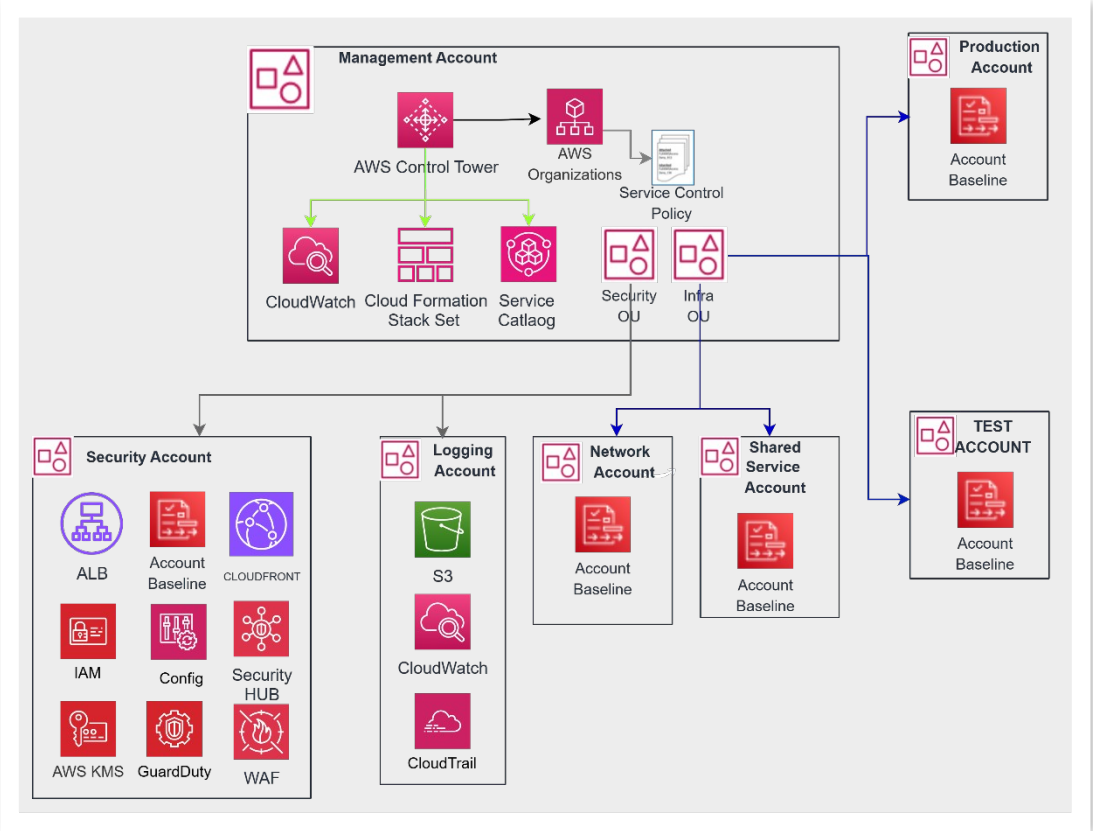
5.2.1 Configuration of Control Tower Setup

Steps for configuration of control tower setup are mostly automated with few interventions of manual configuration. Herby mentions the set of activities as:

- Enable Control Tower from AWS Console because the control tower does not have any API or programmatic access
- Register OU to Control Tower using the console
- Creation of a new Account in the Organization using Automation
- Configuration of service control policies using control tower customization automation

5.2.2 AWS Landing Zone Architecture

AWS Landing Zone saves time by automating the set-up of an environment for running secure and scalable workloads and implementing an initial security baseline through the creation of core accounts and resources. It also provides a baseline environment to get started with a multi-account architecture, identity, and access management (IAM), governance, data security, network design, and logging.



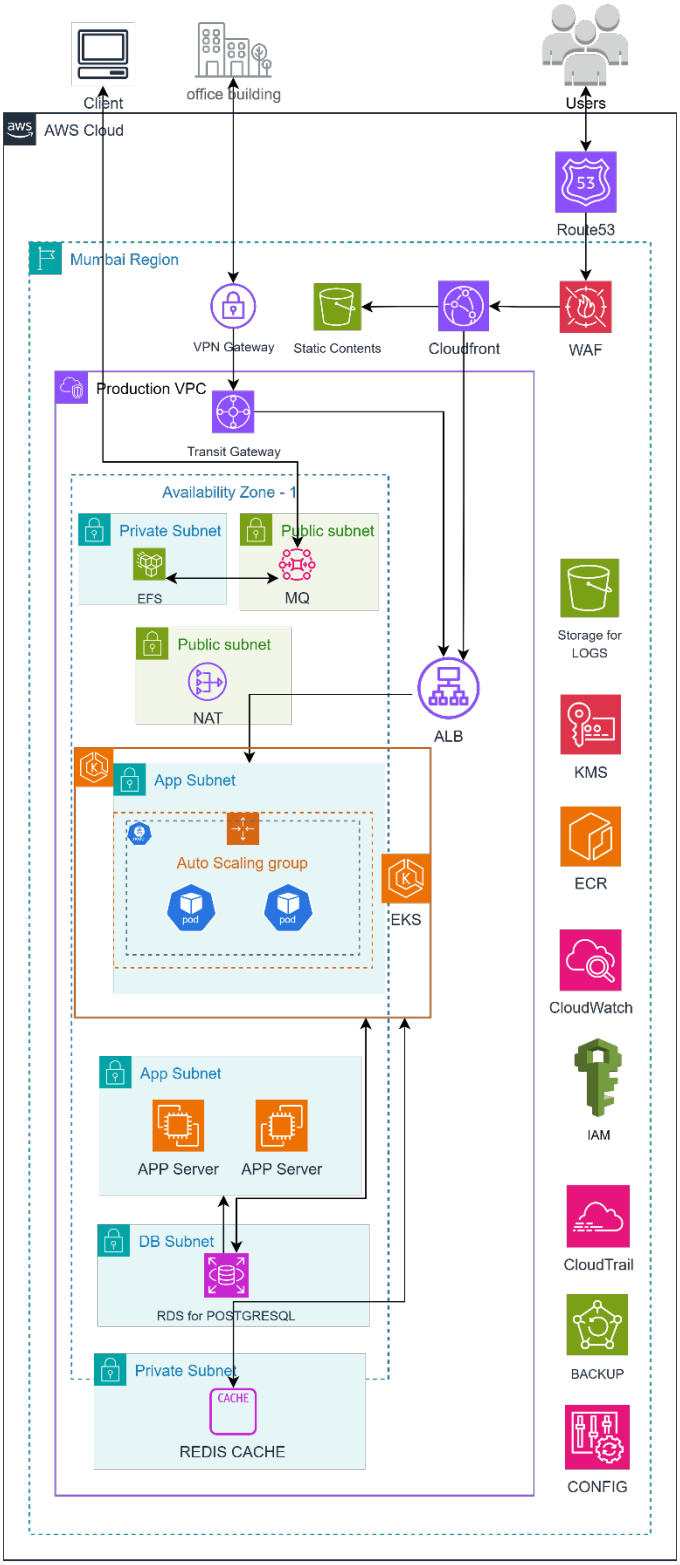
- This architecture is for the Landing Zone implementation of ZYKRR.
- Centralized logging and immutable archive for all Cloud infrastructure and application logs e.g., AWS CloudTrail, AWS Config, VPC Flow logs, and application logs.
- Workload OU and Accounts to be defined for separate Business Units, applications, or environments.
- Isolation of resources using separate accounts for similar groups of workloads
- Automation for compliance management and security posture management
- Automation for Organization policies like SCP, backup, and Tagging policies
- Automatic Tagging of resources for Billing segmentation for CloudFinOps.
- Enabling Security Hub/GuardDuty and setup notifications in Security Hub.

5.2.3 Adding account to Landing Zone

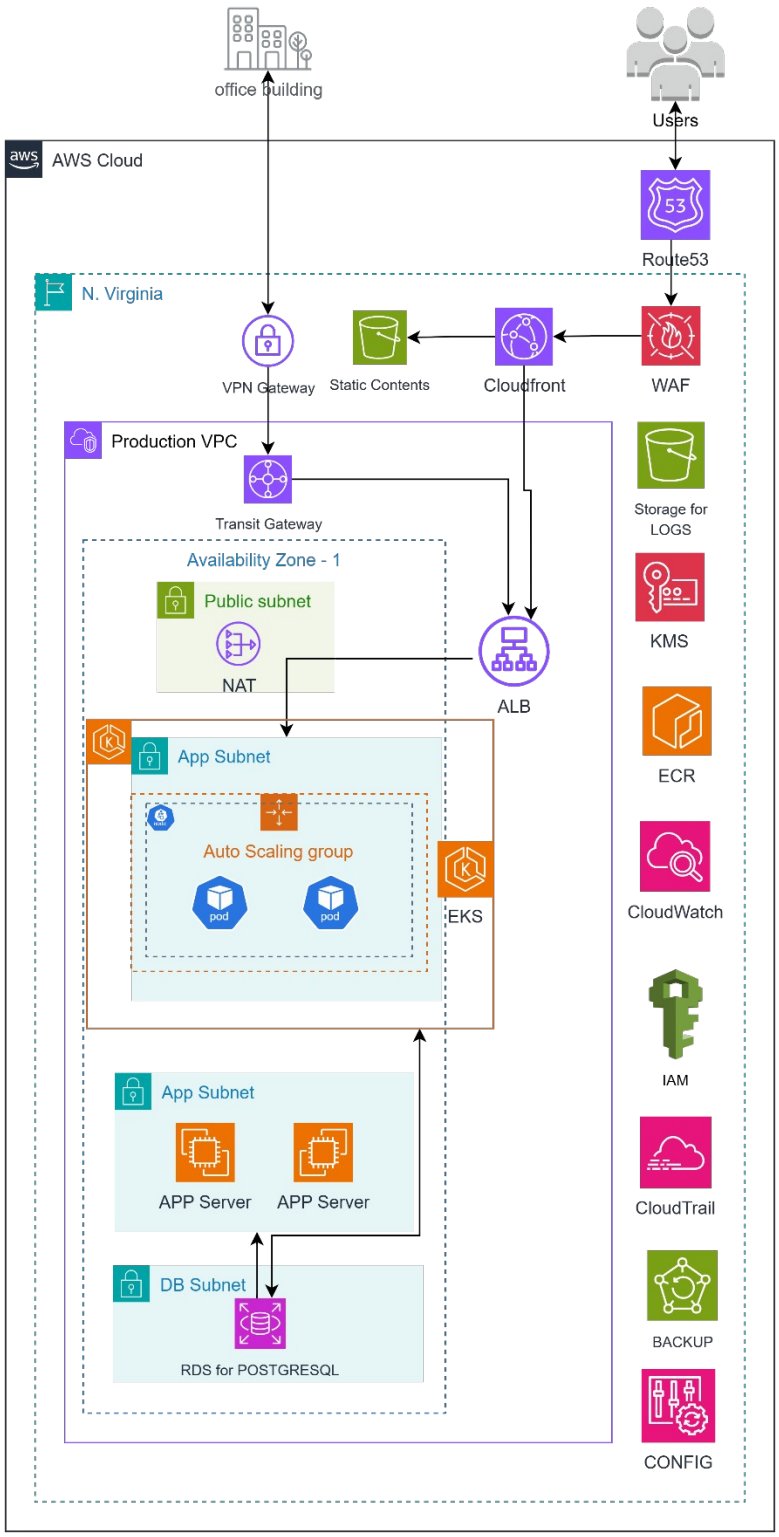
- Send an invite to the individual production account
- Accept the invite from the production account so that the account can be moved to the new control tower setup

5.3 Proposed AWS Architecture

5.3.1 India:


Client
office building
Users
AWS Cloud
Route53
Mumbai Region
VPN Gateway
Static Contents
Cloudfront
WAF
Production VPC
Transit Gateway
Availability Zone - 1
Private Subnet
Public subnet
EFS
MQ
Public subnet
NAT
ALB
Storage for LOGS
KMS
App Subnet
Auto Scaling group
pod
pod
EKS
ECR
CloudWatch
IAM
App Subnet
APP Server
APP Server
DB Subnet
RDS for POSTGRESQL
CloudTrail
BACKUP
Private Subnet
CACHE
REDIS CACHE
CONFIG

5.3.2 USA:


office building
Users
AWS Cloud
Route53
N. Virginia
VPN Gateway
Static Contents
Cloudfront
WAF
Production VPC
Transit Gateway
Storage for LOGS
Availability Zone - 1
Public subnet
NAT
ALB
KMS
App Subnet
ECR
Auto Scaling group
pod
pod
EKS
CloudWatch
IAM
App Subnet
APP Server
APP Server
CloudTrail
DB Subnet
BACKUP
RDS for POSTGRESQL
CONFIG

5.4 AWS TCO & Assumptions

Environment	MRR	ARR
DC (Single Zone)	$6,306.75	$75,681.00

TCO LINK:

DC (Single Zone):

https://calculator.aws/#/estimate?id=d9cc8938739022480fe7424ec76c6024e0382472

Assumptions In TCO
Region
AWS Mumbai and AWS N.Virgina region has been considered for all prod workloads.
Compute
Compute sizing for the instances has been taken according to the specification provided
Amazon Linux has been considered for the all workloads
All AWS EC2 has been considered with 3yr Savings Plan for the EC2 instances.
AWS EKS with 1 cluster for Prod has been considered. 1 AWS MQ and EFS has been considered in AWS Mumbai region. 1 Elastic for Cache (Redis) has been considered. 3 RDS for PostgreSQL has been considered; 2 in India and 1 in USA. AWS ECR has been considered for Prod.
Storage
Storage is considered with GP3 EBS volumes for all proposed EC2 instances.
Snapshots has been considered for AWS EC2.
S3 has been considered for Logs and Static contents storage.
Network, Security & Other Services
NAT Gateway and Data Transfer costs have been considered as part of the VPC cost
Transit Gateway and VPN has been considered.
Application Load Balancers has been considered.
Other security services like WAF and GuardDuty
Other standard services like KMS, AWS Config, CloudWatch and CloudTrail have also been considered
Licenses
No additional license costs have been considered

6 Noventiq Deliverables.

Below are the Noventiq deliverables for the project.

- Phase 1
    - Migration of workload from Azure to AWS.
    - Implementation of production environment in AWS Mumbai and N. Virginia region.
    - Migration of Azure AKS to AWS EKS (Central India to Mumbai & East USA to N. Virginia)
    - Deployment of EC2 for PROD.
    - Azure Database for PostgreSQL Migration to RDS for PostgreSQL.
    - Backup configuration of Application server and RDS for PostgreSQL.
    - S3 configuration for storing Logs and static content for CloudFront.
    - Implementation of security services for protecting the Application and Database from any-type of attack.
        - Route 53
        - Guard Duty
        - WAF
    - Implementation of network services
        - Site-to-Site tunnels
        - CloudFront
    - Implementation of other operational services
        - AWS Config
        - AWS CloudWatch
        - AWS CloudTrail
        - AWS IAM
    - Final cutover to the newly created AWS accounts.
- Phase 2
    - Implementation of foundational Landing Zone.

7 Customer Dependencies

- Providing CIDR ranges for the new VPCs to be created
- Zykrr team will provide the complete know-how of the all the necessary ports, IPs, DNS details, backup requirements, tag details and any other application dependencies and pre-requisites as required by the Noventiq team
- Any changes in the application code for supporting a load balancer and auto-scaling architecture will be done by the ZYKRR team within the defined timeline
- If there are any static IPs hardcoded in the applications or the applications have dependency on static IPs for Database connectivity, those code changes will have to be handled by the ZYKRR team within the defined timeline
- All the DNS related changes during cutover will be done by the ZYKRR team
- All application deployment on AWS EKS cluster will be performed by ZYKRR team.
- Providing a suitable downtime for cutover activity

8 Prerequisites:

- Zykrr team will provide the following access:
    - Existing AKS infra.

- AWS account
- Existing Docker registry.
- Admin access of existing Azure Database for PostgreSQL
- Admin access of Azure VM
- Admin access of Azure ElastiCache

9 Assumptions

- Applications have no hard-coded IP addresses or static IP address requirements.
- Applications are communicating with the DB servers based on host name and ports.
- No additional service apart from Application load Balancer is going to be provisioned.
- Any DNS changes will be done by the ZYKRR team.
- All the application code changes will be done by the ZYKRR team.
- Application functional and load testing will be done by the ZYKRR team.
- Connectivity with the existing firewall within the landing zone is not required.
- Any additional licenses, if required will be procured by the ZYKRR team.

10 Exclusions

The following activities are out of scope for this engagement

- Security configurations and settings outside of the AWS environment will not be part of the scope.
- Security configuration in the corporate network environment.
- Any change in OS, application, or third-party tool/service configuration.
- Changes in application code or configuration in the application.
- 3rd party App Integrations is not included in this scope.
- Any activities related to modernization will be done after the migration phase.
- Any new cloud solution build and deployment requirement including but not limited to application modernization and innovation will be a separate engagement and scope of work, efforts & cost will be shared with client separately as and when required.
- Any change in the ZYKRR current AWS environment.
- Establishing any connectivity with on-prem locations
- Any other service apart from the ones mentioned in the scope document
- Establishing cross account communication with any other AWS account
- Existing Firewall configuration and connectivity with the applications for traffic flow
- Writing any test scripts for functional and load testing
- Pipeline configuration.

11 Risk Analysis

S. No.	Risk	Proposed Mitigation
1	As the project involves migration to the cloud along with changes in the application configuration and architecture might be required	This would require higher involvement of the application and infrastructure team of Zykrr.
2	Network bandwidth constraint in uploading data/server replication	The client team will ensure enough bandwidth for migration activity.
3	Availability of resources and teams	Stand-by team will be employed for the project activities.
4	Coordination among multiple teams	Zykrr team will assign a SPOC from each team for the project activity to coordinate with Noventiq team during the migration.
5	Non-availability of information	Zykrr team will provide all the necessary access as mention in section 8.
6	Delay in approvals and sign-off	Regular reviews will be done to check the status of the project tasks and follow-up will be done for approvals and signoffs.

12 Project Plan

Responsibility	
Joint Responsibilities	
Noventiq	
Customer	

12.1 Migration of AZURE workload to AWS

	Azure Workload Migration

S.No	Activities / Milestones	Week 1	Week 2	Week 3
1	Contract Sign Off			
	Project Initiation / Requirement Gathering			
2	Finalization of ownership of activities between Noventiq and Zykrr			
3	Prepare and share Detailed Project Plan			
4	Coordination with application team to Knowledge Transfer and provide all the pre-requisite information			
5	Sign off on Documentation by ZYKRR			
	Phase 1 - Migration of Azure workload to AWS			
6	Create accounts (Domestic (Mumbai), Test (Mumbai) and USA (N. Virginia) for ZYKRR.			
7	Create the required VPCs and subnets for all 3 environments.			
8	Deployment of Transit and NAT Gateway in all 3 environments.			
9	Configure of site-to-site VPN from AWS to On-Premise.			
10	Migration of Azure VM to AWS EC2 through AWS Application Migration service (Domestic, Test and USA account).			
11	Migration of Azure AKS to AWS EKS using AWS KMF (each in Domestic and USA accounts).			
12	Deployment of RDS for POSTGRESQL (Domestic, Test and USA).			
13	Migration of Azure Database for PostgreSQL to RDS for PostgreSQL.			
14	Configure Backup of AWS EC2 and RDS for PostgreSQL.			
15	Configuration of Amazon MQ.			
16	Configuration of AWS ElastiCache (Redis).			
17	Migration of Cache from Azure ElastiCache (50GB) to AWS ElastiCache (Redis).			
18	Create S3 for storing logs and static contents			
19	Create S3 for static contents.			
20	Migrate data from Azure Blob storage to AWS S3 through AWS DataSync.			
21	Configuration of Route 53.			
22	Configuration of CloudFront.			
23	Configure CloudTrail, CloudWatch, AWS IAM, ALB, AWS Guard Duty and AWS Config.			
24	Configure WAF and its rules with CloudFront.			
25	Ensure data integrity for all the application and RDS for PostgreSQL.			
26	Conduct initial functional and load testing			
27	DNS changes to be performed pre and during the cutover activity			
28	Setup monitoring and autoscaling			
29	Configure Security services and compliance.			
	Implementation & Review of AWS Best Security Practices			
30	Configuration of Password policy in IAM in AWS account			
31	Configure WAF for the ELBs and Guard Duty			
32	Enable CloudTrail to keep a track of account level activities			
33	Configure CloudWatch dashboards along with alerts if required			
	Testing, Validation and Support			

34	Final testing and Cutover			
35	Handover of Document and SOP post implementation of setup			
36	Testing of and troubleshooting of applications in Mumbai location			
37	Validation & Sign-Off by ZYKRR			

12.2 Implementation of Landing-Zone:

	Azure Workload Migration		
S.No	Activities / Milestones	Week 1	Week 2
1	Contract Sign Off		
	Phase 2 - Implementation of foundational Landing Zone		
2	Create AWS Control Tower and Landing zone (Master, Security and Log Accounts)		
3	Create OU for Network and Shared services account.		
4	Setting up the control tower and preparation of Cloud Formation template		
5	Configure Service Control Policies as per the requirements		
6	Enable CloudTrail to keep a track of account level activities		
7	Enrolling existing accounts in Landing Zone.		
8	Handover of Document and SOP post implementation of setup		
9	Validation & Sign-Off by ZYKRR		