Celebrating 20 Years

Statement of Work

AWS Infrastructure for PAM Application deployment

Presented To:

Sompo International

A Larsen & Toubro Group Company

Contents

1 Executive Summary

Larsen & Toubro Infotech Limited (LTI) is pleased to respond to Sompo International's PAM application deployment on AWS requirement. Currently about 5 subscriptions on AWS part of the Sompo landscape, which are managed by LTI. The current statement of work contains scope for the PAM application deployment on AWS.

This statement of work describes the scope of work for the engagement and commercial terms and conditions.

With our expertise of Public cloud management & scaling gives us a head start and right partner advantage.

Based on our understanding, we have put together this response document that articulates our understanding of scope and our methodologies. We trust with our commitment, experience and partnership with Sompo will realize best of results.

2 Scope of Work

The purpose of this SOW is to deploy the PAM application within the existing AWS Accounts of Sompo. The application is a microservices (5) based application, built on the following tech stack:

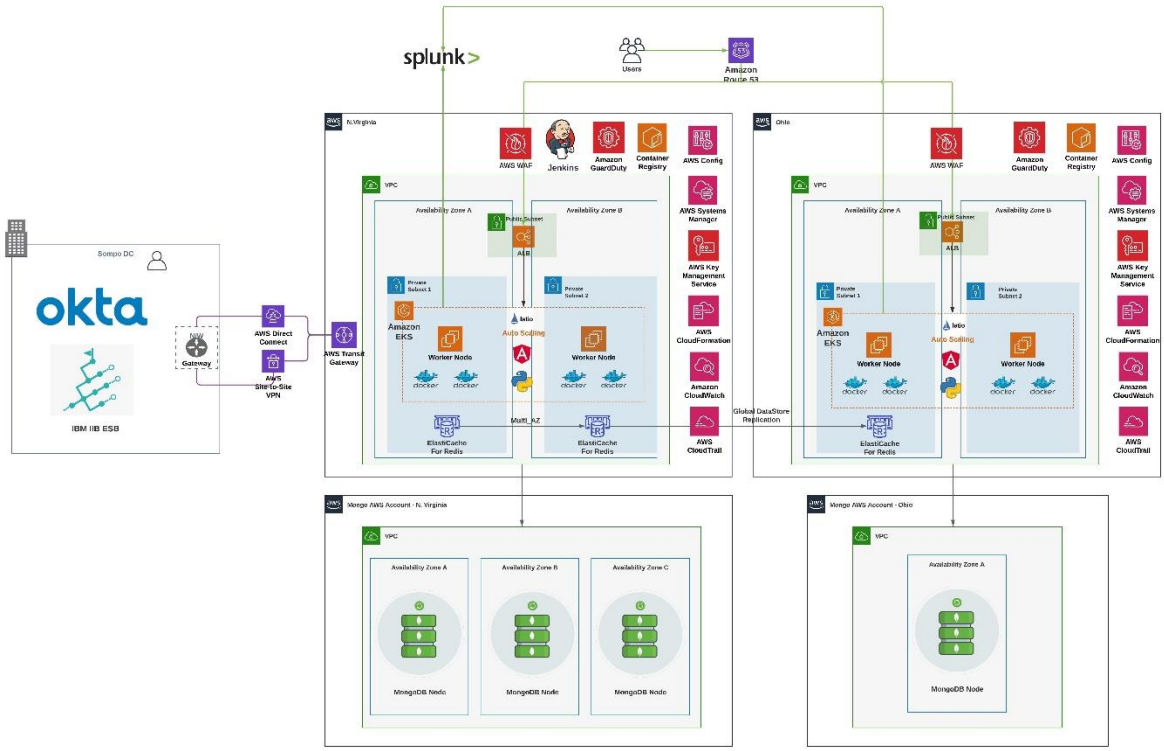
- Angular – Front End
- Python – Backend APIs
- Redis
- Mongo

The Application will have 2 environments to begin with – Production and Non-Production. A separate DR will to be setup as per compliance in the Ohio region while N. Virginia will be used as the primary AWS region.

Sompo also needs a well-defined CI/CD setup to be in place and existing Jenkins tool will be leveraged for the same. Sompo being in a financial services nature of business, application security is of utmost importance for Sompo and LTI will design the solution on AWS to meet the security and compliance requirements.

3 Detailed solution description

3.1 Proposed architecture diagram



Architecture description

1. 3 environments will be created – Production, DR & Non-Production
2. IAM roles will be created to access different AWS service
3. Network will be setup using the VPC service. Appropriate CIDR range, subnets, route tables etc. will be created
4. Required transit gateway attachments will be made to the existing TGW
5. Existing VPN/Direct connect setup will be used to connect to the integrations – Okta, IBM ESB
6. GitlabCI runner will be deployed in the shared services account
7. EKS cluster will be setup and the worker nodes will be deployed across multiple AZs for high availability
8. VM level autoscaling will be configured for the EKS worker Nodes
9. Application Microservices will be Dockerized and deployed on the Worker Nodes
10. Pod level scaling will be configured for application microservices using horizontal pod autoscaler
11. Istio will be configured as the service mesh for service level routing
12. Application Load Balancer will be deployed as the ingress controller to distribute the traffic between the Worker Nodes
13. Redis cache will be deployed on AWS Elasticache service and multi-AZ will be enabled for high availability

14. MongoDB Atlas solution is chosen to deploy the MongoDB database within the AWS Account managed by Mongo
15. With Mongo Atlas high availability, patching and backups are managed by MongoDB
16. Mongo Atlas deploys a minimum of 3 replica sets across 2 AZs of AWS where available for high availability
17. Mongo Atlas also supports autoscaling at 2 levels – Storage and Compute
18. An Active Active DR is proposed. Similar EKS cluster setup will be running in the Ohio Region and the microservices will be deployed
19. MongoDB Atlas supports deploying databases across 2 regions which will be a read only copy and can be manually promoted as the primary in the unlikely event of the primary region going down
20. Redis cache will be replicated to the DR region using Global Data Store feature
21. Route53 failover routing with health checks will be used to redirect the traffic to the DR region in case the primary region becomes unavailable
22. Similar scaled down Application environment will be setup for Non-Production
23. All backups will be centrally managed using AWS Backup Manager

Monitoring

1. CloudWatch tool will be used for infrastructure monitoring and SNS will be used for notifications
2. Sensu will be used for additional monitoring of infrastructure
3. Influx DB will be used as the database to store all data and Grafana will be used to visualize and create the dashboards
4. Pingdom will be used for URL monitoring
5. Prometheus monitoring tool will be used for container service level monitoring
6. CloudTrail will be enabled to capture all the API activities happening in the account
7. VPC flow logs will be enabled to capture all network traffic
8. ALB access logs will be enabled
9. Config rules will be created according to AWS best practices for Change Management

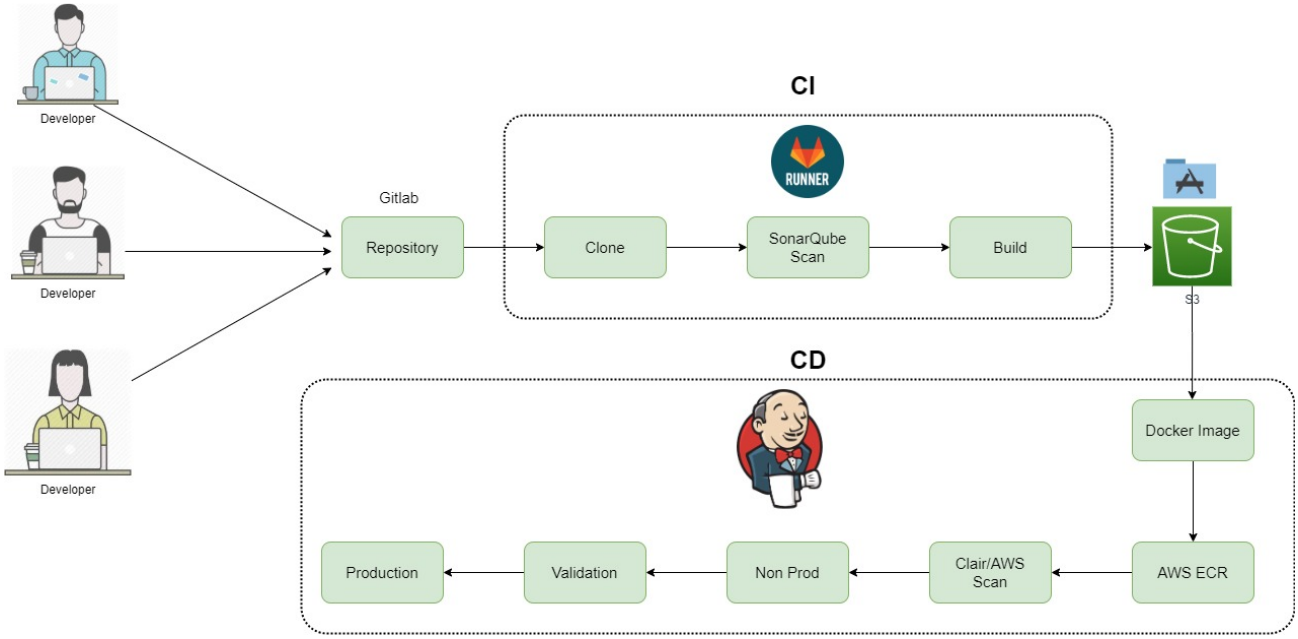
Security

1. Application, Databases & Redis clusters will be deployed in private subnet. This ensures that there is no direct internet access to critical servers like database, app servers etc.
2. AWS WAF will be configured with the required ACL rules for layer 7 protection
3. Security groups are used to control traffic at the VM level. Only the required ports will be opened, and access allowed from required IP addresses. IP whitelisting for various 3rd party providers can be done at the security group level
4. Network Access Control Lists (NACLs) are used to control traffic at the subnet level. Rules will be defined to allow/deny the required traffic from the required IP addresses
5. SSL certificates will be deployed on the load balancers to protect data in transit. Customers can either bring in their own SSL certificates or use public SSL certificates from AWS for free
6. KMS will be used to encrypt all data at rest. The Master Key can either be brought in by the customer or use AWS provided Master key. Customer Managed Master keys are fully controlled

& managed by the customer and can change their permissions, define key rotation policies etc. Data keys will be created to encrypt the data and data keys will be encrypted using Master keys

7. MongoDB database and backups can be encrypted using the KMS service
8. SonarQube will be used for static code analysis
9. ECR Scan will be used for container image vulnerability scanning
10. All the logs will be sent to AWS Guard Duty for threat detection and identifying malicious activities in the account, account compromise etc
11. All logs from AWS like CloudTrail logs, ALB access logs, VPC flow logs, CloudWatch logs, Application logs etc. can be pushed to Splunk
12. All AWS API endpoints are SSL enabled
13. VPN Tunnels/ Direct Connect will be enabled between AWS, Customer Locations & Customer Data Centers

CI/CD



1. Gitlab CI will be used for all the CI part of the pipeline
2. Jenkins will be used for CD part of the pipeline
3. Developers will commit the code to GitLab
4. GitLab CI will clone the code and build the application package and push it to the S3 bucket
5. Unit test case that are written will be executed during the build process
6. Once the unit testing is done SonarQube will perform static code analysis of the application code to find bugs
7. Jenkins will be used to build the Docker image using docker commands and store the Docker image to AWS ECR

8. ECR Scan will be used to do container image level vulnerability scanning
9. Jenkins will be used to deploy the Docker image on EKS Worker Node
10. Required testing can be automated using Jenkins
11. After proper validating we will push the image from Non-Prod to Production environment

4 Prerequisites

In order to execute this scope, Sompo will have to fulfil below prerequisites

- AWS Account access with the necessary permissions for the implementation team
- Application to be stateless
- Availability of the required SMEs from the application team during the implementation phase
- Working with the MongoDB to finalize the sizing and costing for running Mongo Atlas on AWS

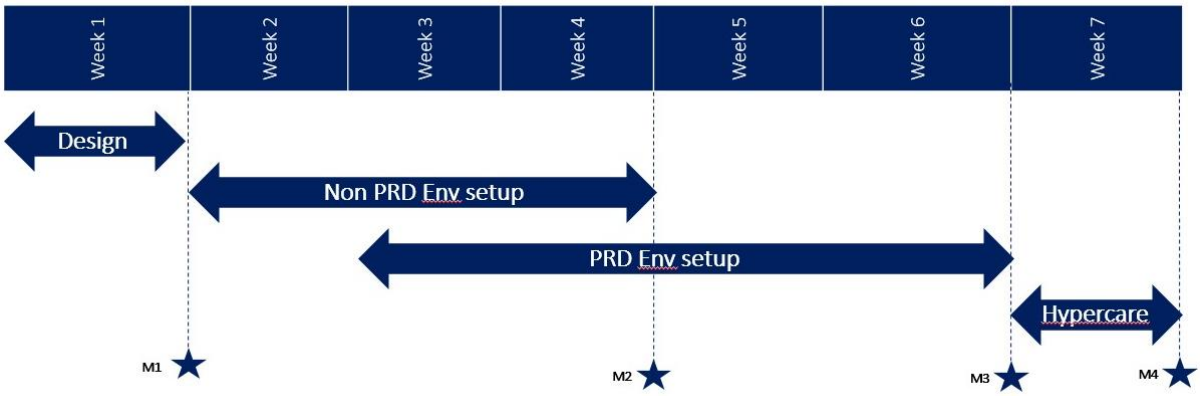
5 Assumptions

- English is assumed to be the primary language of communication
- Customer will work with the Mongo team to finalize the Atlas pricing and create the necessary pre-requisites like Account creation. LTI might
- Application will have access to internet to download the necessary packages/updates
- The application will be deployed into the existing production and non-production accounts of Sompo leveraging the existing LZ setup
- It is assumed that any third-party hardware, licenses & software required during the implementation will be provided by Sompo
- LTI consultants will follow LTI's standard holidays and leave policies, which will be provided in advance to Sompo before execution of the Services
- Sompo will nominate a project coordinator/ manager empowered to facilitate LTI in resolving any project roadblocks or logistical issues related to the engagement
- Sompo will ensure timely availability of application SMEs from respective technical & functional areas for requirement gathering/design validation, as and when required for any discussions/clarifications
- Sompo and LTI together will develop communication guidelines
- Sompo will ensure proactive communication of changes in the plan/execution roadmap from Customer side, if any
- Any delays attributed to the project timeline from Sompo's side might result in re assessment of the effort & plan

6 Out of Scope

- Implementation of any other environment than Production, DR & Non-Production
- Implementation of multiple environments within non-production
- MongoDB Atlas account creation and pricing estimates/contracts
- On-premise VPN Setup
- Any application level changes/configuration required as part of the implementation
- Purchase of any 3rd party licenses
- Any new AWS Account creation and guardrails setup

7 Proposed Project timelines



7.1 Project milestones

Milestone	Description	Milestone	Description
M1	Design & project plan sign off	M3	Production Go live
M2	Non Production Go live	M4	Completion of Hypercare & handover

7.2 LTI Work Execution Locations

The delivery of services will be undertaken through following locations:

Airoli: Mind Space SEZ (Serene Properties), Bldg. No. 1 (2nd Floor), Thane Belapur Road, Airoli, Navi Mumbai 400 708, India

Pune: 5th floor, IT-6 Building, m/s. Neopro Technologies Pvt. Ltd – SEZ, Rajiv Gandhi Infotech Park, phase -1, Hinjewadi, Pune 411057, India

Bangalore: Sirish Foundation, 3rd Floor, 1084, 14th Main Road, Sector 3, HSR Layout, Bangalore 560102

8 Project Tasks

Detailed RACI is show as below

S.No.	Task	LTI	Sompo/App Team/Mongo Team
	Design Phase		
1	Meeting Customer and understanding the requirements	RA	CI
2	Understanding the current application architecture, tech stack and integrations - discovery	RA	CI
3	Liaising with the Mongo team for pricing and pre-requisites	CI	RA
4	Designing the solution document	RA	CI
5	Solution Validation and customer sign-off	CI	RA
6	Preparing detailed Project Plan for Implementation	RA	CI
	Pre-requisites		
7	Provide access to existing AWS account to the consulting team	CI	RA
8	Provide the expected CIDR range, required Port details	CI	RA
9	Creating the Mongo Account	CI	RA
10	Create required IAM users, groups, roles and policies as per requirement and validate with Viacom team	RA	CI
	Non Production - Network Setup		
11	Create the VPC & Subnets & Route Tables for EKS, Elasticache, Gitlab CI & enable VPC flow logs	RA	CI
12	Creating the Security groups for ALB, EC2, & Elasticache & Gitlab CI	RA	CI
13	Creating VPC peering and TGW attachments	RA	CI
	Non-Production- Infra Setup		
14	Provision and configure the EKS cluster	RA	CI
15	Provision MongoDB Atlas	RA	CI
16	Provision the Elasticache Redis engine	RA	CI
17	Provision Gitlab CI in the shared services account	RA	CI
	Non-Production- Application + DB Setup & Migration		
18	Containerize the application and deploy the Docker image on EKS	RA	CI
19	Configure MongoDB Atlas and verify connectivity	RA	CI
20	Configure Elasticache	RA	CI
21	Deploy & Configure Istio	RA	CI
22	SSL + Encryption Setup	RA	CI
23	Route53 Setup	RA	CI
24	Make necessary application level changes	CI	RA
	Non-Production - End to End Validation		
25	End to End Application Validation	CI	RA
26	Database Validation	CI	RA
	Non-Production - DevOps		
27	Configure GitLab runner for CI	RA	CI
28	Creation of Jenkins jobs using Jenkins file	RA	CI

29	Configure the CI/CD Pipeline - Clone --> Build --> Deploy --> Validate	RA	CI
30	Configure the Roll back job	RA	CI
31	Validate the deployment lifecycle	CI	RA
32	Validation of the Roll back process	CI	RA
	Non-Production - Operations Setup		
33	Monitoring Setup - CloudWatch, Prometheus, Grafana	RA	CI
34	Backup Setup	RA	CI
	Production - Network Setup		
35	Create the VPC & Subnets & Route Tables for EKS, Elasticache, Gitlab CI & enable VPC flow logs	RA	CI
36	Creating the Security groups for ALB, EC2, & Elasticache	RA	CI
37	Creating VPC peering and TGW attachments	RA	CI
	Production- Infra Setup		
38	Provision and configure the EKS cluster	RA	CI
39	Provision MongoDB Atlas	RA	CI
40	Provision the Elasticache Redis engine	RA	CI
	Production- Application + DB Setup & Migration		
41	Containerize the application and deploy the Docker image on EKS	RA	CI
42	Configure MongoDB Atlas and verify connectivity	RA	CI
43	Configure Elasticache	RA	CI
44	Deploy & Configure Istio	RA	CI
45	Autoscaling Setup - VM & Pod Level	RA	CI
46	AWS WAF Setup	RA	CI
47	SSL + Encryption Setup	RA	CI
48	Route53 Setup	RA	CI
49	Make any application level changes	CI	RA
50	DR Setup - EKS Mongo, Elasticache, WAF	RA	CI
	Production - End to End Validation + Go Live		
51	End to End Application Validation	CI	RA
52	Database Validation	CI	RA
53	Update the DNS to point to AWS and Go-Live	RA	CI
54	DR Testing and verification of RTO & RPO	RA	CI
	Production - DevOps		
55	Configure GitLab runner for CI	RA	CI
56	Creation of Jenkins jobs using Jenkins file	RA	CI
57	Configure the CI/CD Pipeline - Clone --> Build --> Deploy --> Validate	RA	CI
58	Configure the Roll back job	RA	CI
59	Validate the deployment lifecycle	CI	RA
60	Validation of the Roll back process	CI	RA
	Production - Operations Setup		
61	Monitoring Setup - CloudWatch, Prometheus, Grafana	RA	CI
62	Backup Setup	RA	CI
	Documentation, KT & Handover		
63	Documentation, KT & Handover to Customer/ MS Team	RA	CI

9 Deliverables

Following are the deliverables from this SOW:

1. Non-Production Setup of the PAM application
2. Production Setup of the PAM application
3. DR Setup and Testing
4. CI/CD Setup

10 Commercials

10.1 Implementation costs

S. No.	Task	Duration (Weeks)	Costs (USD)
1	Infrastructure setup on AWS for PAM application deployment DevOps setup on AWS	7	34,920

*Current costs are only for the scope highlighted in this SOW. Any changes in the scope will require a change request to be raised, post discussion & approval from the Sompo team

10.2 Projected AWS hosting costs

With Mongo Atlas

S No	Component	Pricing per month (On Demand)	Pricing per month (1 Yr RI)
1	AWS Calculator Link - EKS Worker Nodes, ALB, Elasticache, EBS etc.	$ 742.42	$ 531.52
2	EKS Control Plane	$ 219.00	$ 219.00
3	AWS WAF	$ 60.60	$ 60.60
4	ECR	$ 10.00	$ 10.00
5	MongoDB Atlas	To be updated	To be updated
Total (Per month)		$ 1,032.02	$ 821.12

Prod – $ 741.3
Non Prod - $ 290.72

With Document DB

S No	Component	Pricing per month (On Demand)	Pricing per month (1 Yr RI)
1	AWS Calculator Link - EKS Worker Nodes, ALB, Elasticache, EBS etc.	$ 742.42	$ 531.52
2	EKS Control Plane	$ 219.00	$ 219.00
3	AWS WAF	$ 60.60	$ 60.60
4	ECR	$ 10.00	$ 10.00
5	DocumentDB	$ 483.56	$ 483.56
Total Pricing		$ 1,515.58	$ 1,304.68

Prod - $ 1157.72
Non-Prod - $ 357.86
DocumentDB Prod - $ 416.42
DocumentDB Non-Prod - $ 67.14

AWS calculator link:
https://calculator.s3.amazonaws.com/index.html#key=files/calc-daa613905a85aadb544a538cdc468c0e3bd19f5d&v=ver20201112bC

10.3 Payment milestones

Milestone	% Payable
Project kick off	15%
Non - Production go live	35%
Production go live	45%
Hypercare completion	5%

10.4 Commercial Assumptions

- All relevant payments to be released within 30 days from the receipt of invoice. Overdue payments subject to an additional service charge of 1% per month
- Any additional activity beyond the scope of work defined in this proposal shall be taken up as a separate activity and would trigger a Change Request
- Rates are exclusive of any taxes / duties
- Invoicing will be delivered to Sompo no later than Seven (7) days following the end of the milestone
- The SOW will remain valid for acceptance for a period of 15 days from the date of the submission of the SOW
- If Sompo requires any additional services to be provided under this SOW, the same can be added to scope by an approved Change Service Request

11 Approval

Customer Approval	LTI's Approval
Signature: _____	Signature: _____
Name: _____	Name: _____
Title: _____	Title: _____
Date: _____	Date: _____