

# SML Simplifies Windows Workload with CloudWorkmates



## About Customer: SastaSundar Market Place Ltd(SML)

SastaSundar.Com web portal by SastaSundar Market Place Ltd (SML) is an Innovative Information and Knowledge based web portal that helps people on their path to wellness, focused on providing them information and knowledge about medicines and healthcare products. SastaSundar.Com acts as bridge between users and the Independent Licensed Chemists and enable users to place their enquiry/indent.

SastaSundar.com is supported by a network of Independent Licensed Chemists (sellers). All communications on SastaSundar.com are being forwarded to the said Independent Licensed Chemists. On confirmation of the same, the orders are fulfilled by the said Independent Licensed Chemist and delivered to users by the said Independent Licensed Chemist.

SML is a one of its kind digital platforms excelling in hyperscale transaction management, transformative platforming, technical services built on proven tech expertise in the healthcare industry.

## Customer Challenge

SML was looking for Web based applications on AWS. All the applications need to run the windows workload with MS-SQL and RDS as a Backend DB. Customer focus was on HA for the MS-SQL database and was also having pain with Infra scaling issues causing poor performance during load on server with their existing service provider. Windows Workload. SML wanted to work with a strong Cloud Consulting Partner like Workmates to help them host their windows workload on AWS, manage Infra and applications 24\*7 and then build Cloud capabilities so that SML developer team can concentrate on application development.

## Solution Approach

- The initial Infrastructure would consist of App Server and MSSQL Server running on EC2 on Windows. All Server Sizing was initially taken based on the current sizing and its utilization shared by
- Workmates team will create all the required infra in SML existing AWS a/c. To facilitate secure connectivity, we will provision two separate network segments namely public and private and Network Access Control Lists (NACLs) are used to control traffic at the subnet level. And NAT gateway is used for in stances in private network to have access to internet.
- All the servers be placed in private subnet and ELB (Elastic Load Balancer) will be on internet facing, with ALB you will get the SSL certificate and it will protect and manage the external threat our internal IP's will not be exposed to internet. ALB would be used as per the application team's requirement.
- We will enable the auto recovery feature to ensure the maximum uptime of the infra
- The public facing network (public subnet) will contain one NAT gateway for upgrades patches and occasional system updates to the hosted machine
- The Application and Database server will be hosted on the non-internet network (private subnet) with a network route configured to the NAT gateway and the VPN subnet

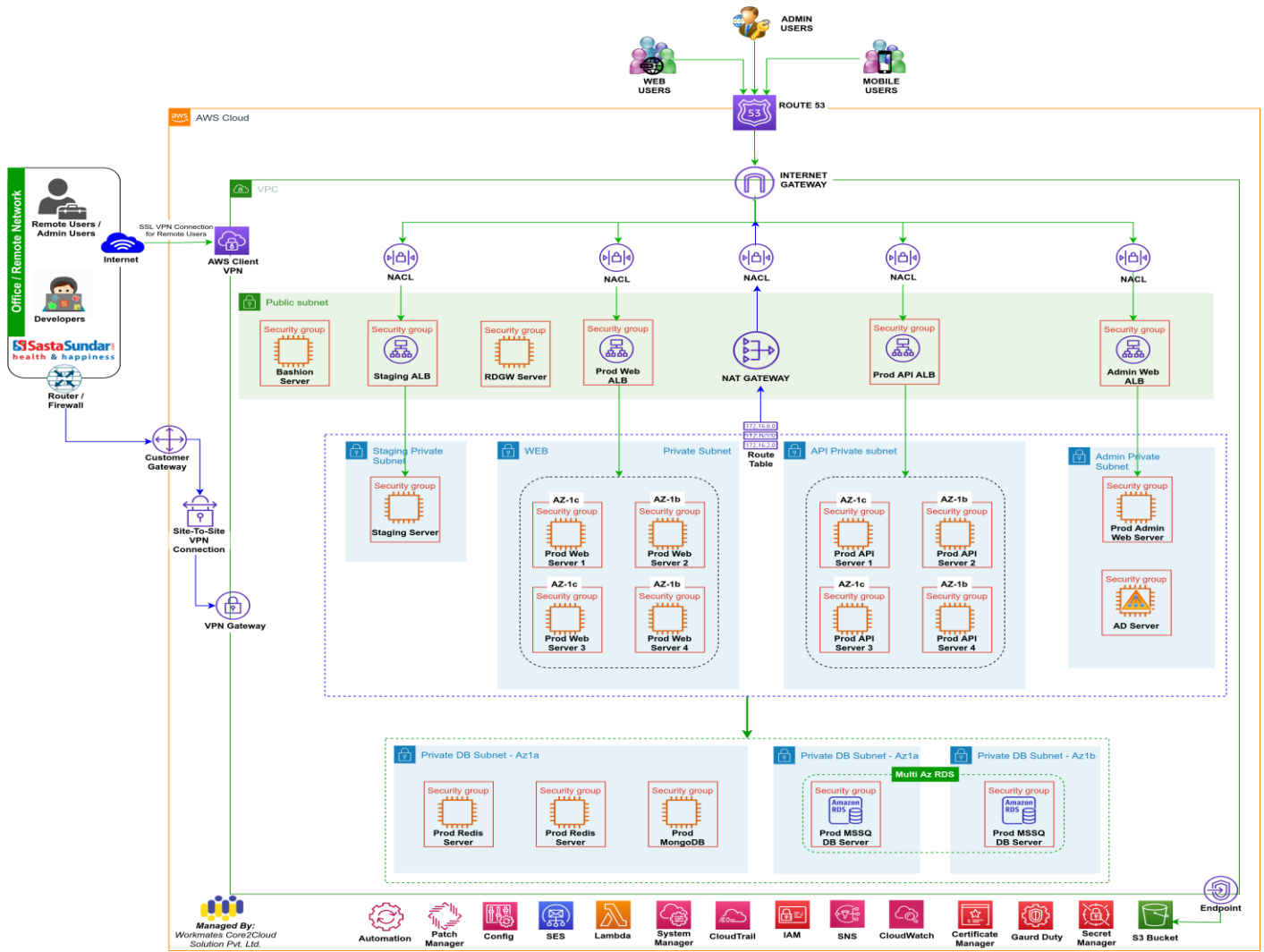
- To protect unwanted access to backups we will also create, and AWS managed KMS encrypted S3 bucket.
- The servers will be configured with the latest update of Windows Server OS with one additional SSD volume
- We shall provision a scheduled task that will take a backup of the primary data store on the RDS/MSSQL DB to S3
- Users will link their client applications to their respective client machines via the local IP of the VM instance via the VPN tunnel
- Our approach towards data backups and AMI snapshots will ensure complete data availability
- The license for Microsoft SQL Server Enterprise has been considered with provisioning RDS.
- All the logs will be sent to AWS Guard Duty for threat detection and identifying malicious activities in the account.
- AWS Config will be enabled, and all the AWS recommended config rules will be created.
- Periodic patching of the servers will do via AWS SSM Patch Manager.

- **Key Services Used**

AWS Services Used	Use Case
AWS EC2	Windows Workload Management
AWS Application Load balancer	Traffic Management across the windows workload
S3	Object Storage for Media related Contents
Amazon EBS GP2/Gp3	Persistent Storage for Stateful apps such as DB
AWS KMS	For EBS and S3 encryption
AWS WAF	For protection of Windows web service from external attack
Amazon CloudFront	Content Delivery Network
AWS CloudFormation	Creation of VPC, ECS cluster and ASG
Amazon CloudWatch Logs	Logging Solution for all microservice applications
AWS Config	Conduct assessment and audit of the AWS resources
AWS Systems Manager	For On demand Patching EC2 Servers.

Third-Party Tools	UseCase
Jenkins	Build, test, and deploy the microservices using Jenkinsfile
Git	Software Version Control - Bitbucket
OpenVpn	Secure access to AWS Infrastructure

## Solution Architecture



## Security Considerations

1. Using IAM we restricted users and group to access specific AWS resources only as per the requirement.
2. AWS Multi-Factor Authentication for privileged accounts, including options for hardware/Software based authenticators is enabled.
3. Quarterly Patch Management and Patch Automations is carried out using AWS SSM. During patch all the security patches, OS critical patches will be applied.
4. Deep visibility into API calls through AWS Cloud Trail, including who, what, and from where calls were made. All user related activity are tracked and logged.
5. For any Administrative task Remote user will use VPN client to connect the servers.
6. All the RDP port will be bind with OpenVPN server, also default ports will be changed to the custom port.

7. DB is accessible only through the Application containers and through the VPN. All servers will be hosted on the private subnet.
8. For Configuration Management and Policy as a Code, AWS Config will be used, which will help us detect any configurations drift within the AWS Account.
9. All the Data on Rest will be encrypted using AWS KMS. EBS volumes of EC2 and RDS to be encrypted, all S3 buckets to be encrypted.
10. Trusted Advisor Checks will be carried out every week ensure the all the security checks are used.
11. AWS Secrets Manager are being used to store the DB credentials encrypted using KMS.
12. AWS WAF has been implemented to help protect web applications and APIs against common web exploits and bots that may affect availability, compromise security, or consume excessive resources.

### Results and Benefits

Cloudworkmates finished the project on-time and under-budget delivering a scalable and highly available infrastructure with no single point of failure. SastaSundar team was happy with the deliverable and the executed timeframe. Should the need arise to extend or modify their infrastructure further, CloudWorkmates is available to continue the relationship.

SML is now able to process more customers data faster than they could by using their in-house solution. Also, on AWS, they can quickly scale their production stack as dynamically as their workloads scale. For example, SML are now easily increase their storage footprint and compute footprint utilizing AWS's highly scalable features. Finally, SML was able to realize the full potential of running Microsoft Workloads on AWS with the required high availability, reliability, performance & Scalability

### About Workmates



Workmates core2cloud Solution Pvt. Ltd is an AWS Advance consulting partner and Leading Cloud Management Company in Eastern India. Workmates Core2cloud is a cloud managed services company focused on AWS services, the fastest growing AWS Advanced Consulting Partner in India. We focus on Managed services, Cloud Migration and Implementation of various value-added services on the cloud including but not limited to Cyber Security and Analytics. Our skills cut across various workloads like Microsoft, SAP, Media Solutions, E-commerce, Analytics, IOT, Machine Learning, VR, AR etc. Our VR services are transforming many businesses.

Workmates has a yellow theme which is the color of youth. Our Vibrant team of 100% certified resources brings the edge to customers for an End to End AWS partner, committed towards quality and supporting their business on a 24X7 basis.