



Sompo International

SOLUTION DOCUMENT

Prepared By: Ayush Ragesh, Solutions Architect

Reviewed By: Manoj Kumar, Principal Cloud Architect

Document Version: 1.0

About Somo International

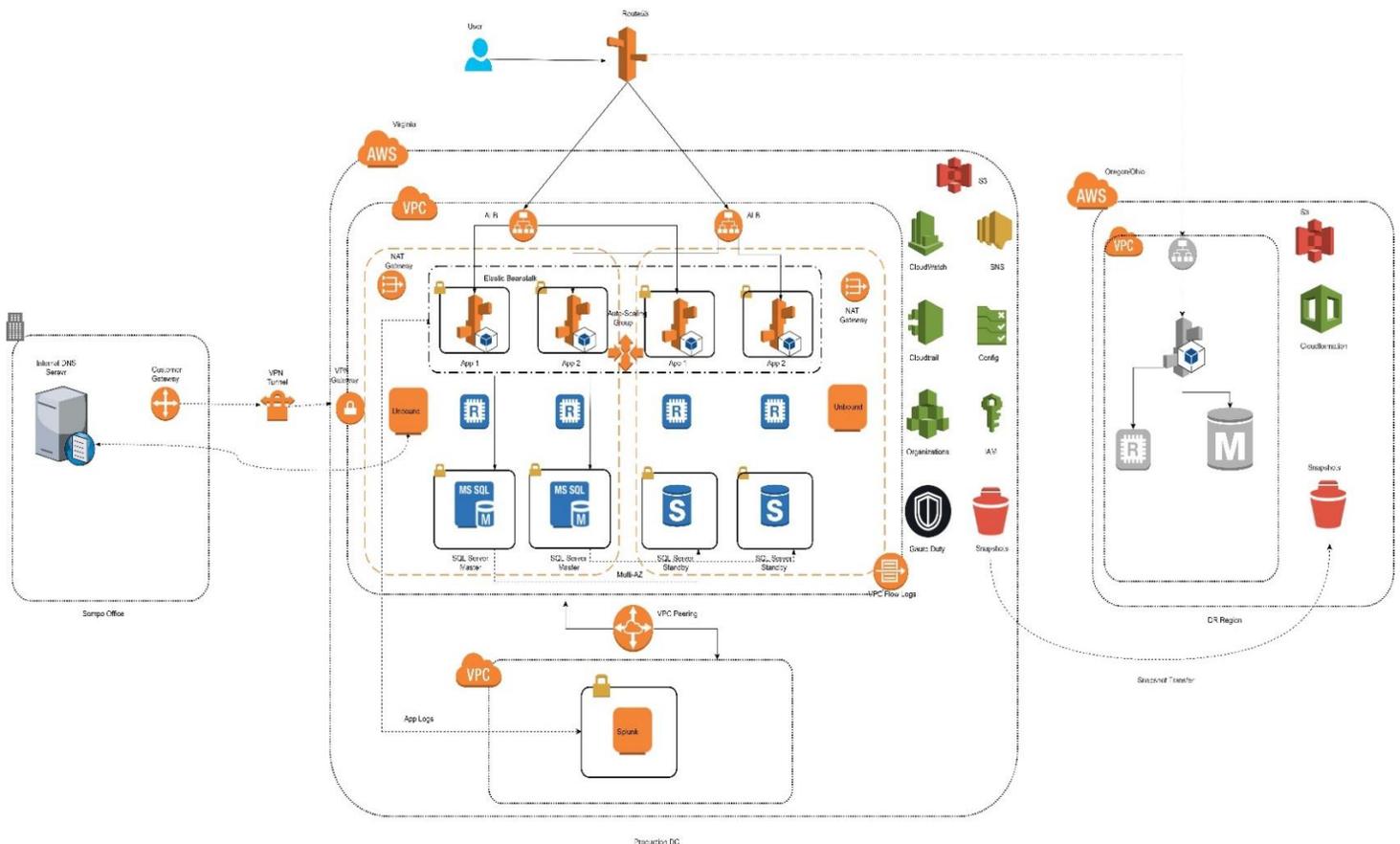
Somo International was established in March 2017 with the acquisition by Somo Holdings, Inc. (Somo) of Endurance Specialty Holdings Ltd. (Endurance) and its wholly owned operating subsidiaries. Somo’s core business encompasses one of the largest property and casualty insurance groups in the Japanese domestic market. Seeking opportunities to grow their business globally, Somo acquired Endurance, a global provider of property and casualty insurance and reinsurance, to effectively become their international operation.

Problem Statement

Somo International wants to migrate 2 of their web services from on-premise to AWS Elastic Beanstalk. Both are .NET based applications and used Microsoft SQL server as the backend. Customer wants to use RDS for the database and AD authentication for SQL server access.

Somo International wants to work with a strong Cloud Consulting Partner like Powerupcloud to help them migrate the applications onto AWS, manage those applications 24*7 and then build Devops capabilities on cloud so that Somo can concentrate on application development.

Solution



Architecture Description

General

1. AWS accounts will be created and managed using AWS Organizations according to customer requirement.
2. Appropriate users, groups and permissions will be created using Identity and Access Management (IAM) service.
3. IAM roles will be created to access different AWS service.
4. Network will be setup using the VPC service. Appropriate CIDR range, subnets, route tables etc. will be created.
5. NAT gateways will be deployed in 2 public subnets in 2 different Availability Zones of AWS.
6. VPN Tunnel will be setup from customer location to AWS data center.
7. 2 Application Load Balancers will be created for the 2 applications being migrated.
8. Route53 service will be used to create the necessary DNS records.
9. An open source DNS forwarding application called Unbound will be deployed across 2 AZs for high availability. Unbound allows resolution of request originating from AWS by forwarding them to on-premise environment and vice-versa.
10. 2 Elastic Beanstalk environments will be created for the 2 applications and the .NET code will be uploaded and then deployed on it.
11. Windows Server 2016 R2 is used to deploy Application & AD.
12. Both the applications will be deployed across 2 Availability Zones and auto-scaling will be enabled for high availability and scalability.
13. MSSQL database will be deployed on RDS service of AWS and multi-AZ feature will be enabled for high availability. Database will be replicated from on-premise to AWS by taking the latest SQL dump and restoring/enabling Always-on replication between the database/using the AWS DMS service. RDS SQL authentication will be used instead of Windows authentication.
14. Elastic Cache Redis cluster will be deployed for storing the user sessions. Multi-AZ feature will be turned on for high availability.
15. All application logs will be sent to Splunk. VPC peering will be enabled between the 2 VPCs.
16. CloudWatch service will be used for monitoring and SNS will be used to notify the users in case of alarms, metrics crossing thresholds etc.
17. All snapshot backups will be regularly taken and automated based on the best practices.
18. All Server Sizing was initially taken based on the current sizing and its utilization shared by the customer. Based on the utilization reports in CloudWatch Servers were scaled up or down.
19. NAT gateway is used for instances in private network to have access to internet.
20. 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.
21. Network Access Control Lists (NACLs) are used to control traffic at the subnet level.
 1. SSL certificates will be deployed on the load balancers to protect data in transit.
 2. CloudTrail will be enabled to capture all the API activities happening in the account.
 3. VPC flow logs will be enabled to capture all network traffic.
 4. ALB access logs will be enabled
 5. All the logs will be sent to AWS Guard Duty for threat detection and identifying malicious activities in the account, account compromise etc.
 6. AWS Config will be enabled, and all the AWS recommended config rules will be created.

Additional Details

AWS Services Used: EC2, EBS, ALB, RDS, Route53, S3, CloudFormation, CloudWatch, CloudTrail, IAM, Config, Guard Duty, Systems Manager, Auto-scaling, Transit Gateway

3rd Party Solutions Used: Unbound, Okta

Windows Stack Used

1. .NET Applications
2. IIS Web Server
3. RDP Gateway
4. SQL Server Enterprise Database
5. Active Directory

Outcomes

- Powerupcloud was able to setup automated landing zone for Somo
- Somo was able to meet the required high availability & scalability
- Somo was able to integrate the migrated applications to the on-premise legacy systems seamlessly

**THANK
YOU!**