Case Study: GoGreen Insurance Company Cloud adoption

Name: Lee Kean Lim

ID: TP065778

Date: 26-July-2022

Network

VPC	Region	Purpose	Subnets	AZs	CIDR Range
1	us-west-1 (US West, N. California)	Production	6	2	10.0.0.0/24
2	us-west-1 (US West, N. California)	Testing + Backup	6	2	10.0.1.0/24

Subnet Name	VPC	Subnet Type	AZ	Subnet Address	
				VPC 1	VPC 2
web-public1	1, 2	Public	A	10.0.0.0/27	10.0.1.0/27
web-public2	1, 2	Public	B	10.0.0.32/27	10.0.1.32/27
app-private1	1, 2	Private	A	10.0.0.64/27	10.0.1.64/27
app-private2	1, 2	Private	B	10.0.0.96/27	10.0.1.96/27
database-private1	1, 2	Private	A	10.0.0.128/28	10.0.1.128/28
database-private2	1, 2	Private	B	10.0.0.144/28	10.0.1.144/28

VPC Architecture Diagram

Security

Security Group (SG)	SG Name	Rule (Allowed Port)	Source
ELB Load Balancer	ELB_SG	443	0.0.0.0/0
Web Tier	WEB_SG	8080	ELB
App Tier	APP_SG	8080	Web Tier
Database Tier	DB_SG	3306	App Tier

Other Security Option	Justification
AWS Web Application Firewall (WAF)	Protects web application and the data from web attacks
Network access control list (ACL)	Allows or denies specific inbound or outbound traffic at the subnet level
Amazon Multi-Factor Authentication (MFA)	Additional authentication layer which strengthens username and password credentials

Encryption

Requirement	Solution
Encryption option for **data at rest**	- Implement secure key management from AWS KMS to create and manage encryption keys for the encrypted data - Enable default encryption in Amazon S3 (FOC) - Implement Amazon RDS for database encryption
Encryption option for **data in transit**	- Implement SSL/TLS to encrypt connection to DB

Instance Details

Tier	AMI	Tag	Type	Size	Justification	# of instances
Web	Linux	Key: Name Value: app-tier	t2	large	**Current**: 6VM @ 4GB mem each **Required**: 36GB Mem **Instance**: each VM (2 vCPU, 8GB Mem)	6 (Providing total 48GB memory)
App	Linux	Key: Name Value: web-tier	r4	2xlarge	**Current**: 5VM @ 4vCPU, 16GB mem each **Required**: 216GB Mem **Instance**: each VM (8 vCPU, 61 GB mem)	5 (Providing total 40 vCPU and 305 GB Mem)
DB	Linux	N/A	db.r5	2xlarge	**Current**: 2VM @ 8vCPU, 32GB Mem **Required**: 21,000 IOPS **Instance**: each VM (8 vCPU, 64GB Mem, 12,000 IOPS)	2 (Providing 24,000 IOPS)

Recovery Point Objective

Requirement to achieve Recovery Point Objective (RPO) of four hours
Implement backup & restore disaster recovery strategy. - Easiest and least expensive strategy - Use Amazon RDS configuration to provide snapshot of DB instance every 4 hour.

Document Storage

Storage/Archive Option	Detail
Amazon Simple Storage Service (S3)	- Amazon S3 is the only cloud storage service with query-in-place functionality, allowing you to run analytics directly on your data at rest. - Files will initially be stored in S3 for the first 3 months. - After 3 months, move to Amazon Glacier. - Delete from S3 to free up space.
Amazon S3 Glacier	- Amazon S3 Glacier is a secure, durable, and low-cost storage class of S3 for data archiving and long-term backup. - Files will be stored here after transferring from S3 for long-term of 5 years. - Delete from Glacier to free up space after 5 year.

Web Tier

Requirement	Solution
Architecture must be flexible and handle any peak in traffic or performance.	- Implement AWS Auto Scaling to monitor applications and automatically adjusts capacity to maintain steady, predictable performance at the lowest possible cost.
The overall acceptable incoming network bandwidth is between 300 Mbps and 750 Mbps.	- Implement Amazon CloudWatch to monitor resources and applications usage. - Set automated actions for Amazon Auto Scaling to scale up or down web servers when capacity is nearing thresholds.
Application administrators want to be notified by email if there are more than 100 “400 HTTP errors” per minute in the application.	- Implement Amazon CloudWatch to monitor logs from web servers. - Set trigger alarm for the specified errors and conditions and send email to admin.

Application Tier

Requirement	Solution
Architecture must be flexible and handle any peak in traffic or performance.	- Implement AWS Auto Scaling to monitor applications and automatically adjusts capacity to maintain steady, predictable performance at the lowest possible cost.
Overall memory and CPU utilization should not go above 80% and 75% respectively or below 30% for either.	- Implement Amazon CloudWatch to monitor resources and applications usage. - Set automated actions for Amazon Auto Scaling to scale up or down instances when capacity is nearing thresholds.
Internet access is required for patching and updates without exposing the servers.	- Set up Network Address Translation (NAT) gateway to allow private subnet to connect internet without exposing those resources to incoming internet connections.

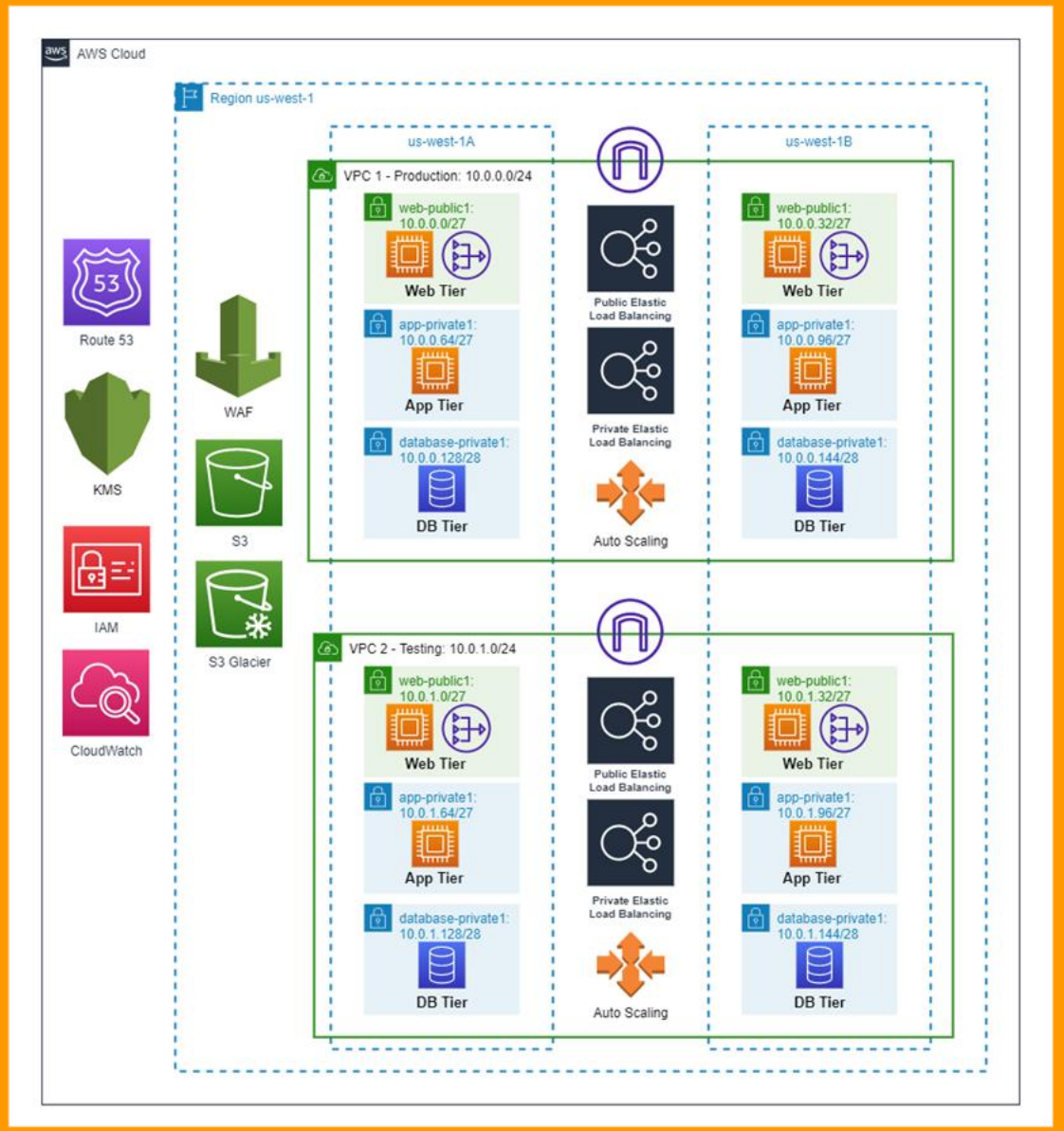
Database Tier

Requirement	Solution
Database needs consistent storage performance at 21,000 IOPS	- The proposed DB instances support EBS optimization which provides a combined baseline IOPS of 24,000.
High availability is a requirement.	- Adopt Multi-AZ deployment for the DB instance. - Amazon RDS maintains a redundant and consistent standby copy of your data using synchronous storage replication.
No change to the database schema can be made at this time.	- Adopt MySQL 5.7.22 engine for the RDS. - This version is currently used by the company which can facilitate seamless transitioning.

Additional Services

Additional Service	Justification
AWS Identity and Access Management (IAM)	- This service provides control and visibility on users accessing to resources which improves security. - To specify who can access which services and resources, and under which conditions. - Free service from AWS.
Amazon Route 53	- Domain Name System (DNS) service. - To manage public DNS names.

Proposed Architecture Diagram



Cost considerations

Cost Monitoring	Justification
Amazon CloudWatch	- Collects monitoring and operational data and provides unified view on operational health and resources in real time - Based on the metrics, performance optimization and resource utilization - Detect anomalous behavior - Set alarms based on certain triggers - Automate actions based on predefined thresholds, automatic scaling of EC2 instances to reduce billing