Dr. J.C. Martinez Class 3367

Team 14- 4/4/2022

AWS Solution Analysis and Recommendation for GOGREEN Insurance

Team 14

D. Doan

V.Lopez

S.Rajan

C.Williams

Dr. J.C. Martinez Class 3367
Team 14- 4/4/2022

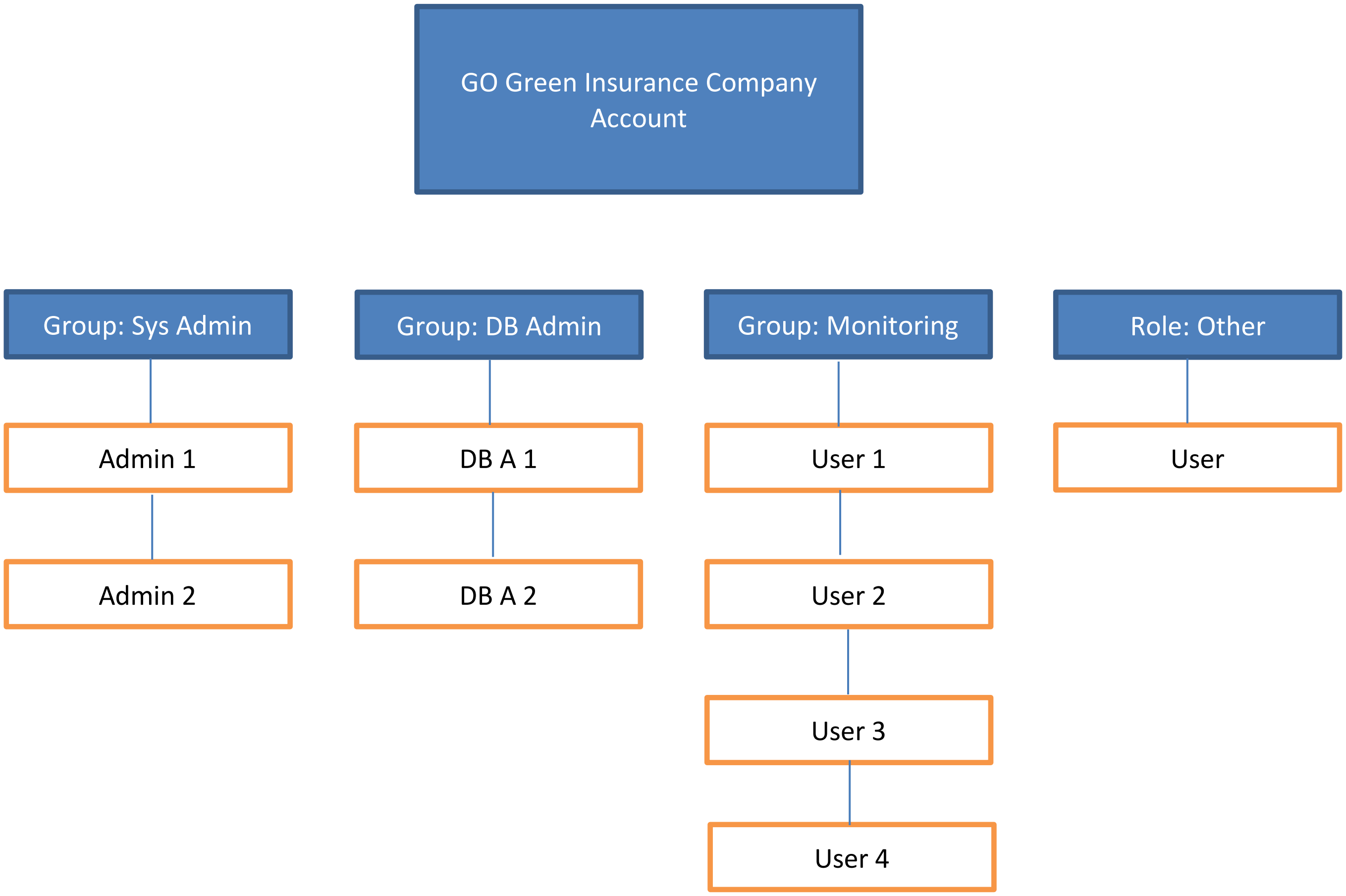
Contents

Solution – Identify AWS Services

Potential services and the purpose of each service that will be used to move GO Green’s current environment to AWS.

- Amazon CloudFront
- Amazon CloudFormation
- S3 Simple Storage
- AWS DB Migration Service
- IAM
- Amazon CloudWatch
- Autoscaling feature
- Load Balancer
- Amazon DynamoDB
- Network Access control list
- AWS Management Console
- MFA Token
- EC2
- VPC
- SNS

Solution – User Authentication



Group/Role #	Group/Role Name	Permissions
Group	Sys Admin	AWS SDKs, IAM HTTPS API, AWS Management Console
Group	DB Admin	AWS SDKs, IAM HTTPS API, AWS Management Console
Group	Monitoring	EC2, S3, RDS
Group	Other	AWS Management Console

Following the User authentication requirement, users are put into groups which would limit their user access depending on which groups they are in, this is identity-based policies to limit user access to resources. Permissions are assigned as GoGreen Also, generated a random code for any Admin by MFA.

Requirement	Solution
Should be at least 8 characters and have 1 uppercase, 1 lowercase, 1 special character, and a number.	Create IAM password policy/rules to require 8 characters, 1 uppercase, 1 lowercase, 1 special character, and a number.
Change passwords every 90 days and ensure that the previous three passwords can't be reused.	Create IAM password policy/rule to require password change every 90 days and require to not be the past 3 passwords.
All administrators require programmatic access.	Allow Admin groups to have access to Access Management Console, AWS SDKs, IAM HTTPS API.
Administrator sign-in to the AWS Management Console requires the use of Virtual MFA.	Enable and require the use of AWS Multi Factor Authenticator to login.

By using different services, we should allow the specific groups only to access specific things on AWS. Also, using Amazon Identity and Access Management policies will allow us to set up rules for the user account to follow.

Design: Web Tier

Requirement	Solution
Architecture must be flexible and handle any peak in traffic or performance.	Use Load balancer and AutoScaling to scale up during high traffic hours
The overall acceptable incoming network bandwidth is between 300 Mbps and 750 Mbps.	Use Cloudwatch to watch over acceptable bandwidth.
Application administrators want to be notified by email if there are more than 100 “400 HTTP errors” per minute in the application.	Use Cloudwatch alarm to setup SNS notification
Web Tier instances should be tagged as “Key=Name” and “Value=web-tier	Use autoscaling group tags Key=Name and Value = web-tier

Using Load balancer and autoscaling will help with being flexible and be able to handle high traffic amount. Also using CloudWatch will enable the company to watch over acceptable bandwidth amount. CloudWatch can also be setup for HTTP Error and send SNS notification when a limit is met. Also during the autoscaling, there is parameter where the minimum and maximum can be set.

Design: Application Tier

Requirement	Solution
Architecture must be flexible and handle any peak in traffic or performance.	Use Autoscaling and Load balancer
Server capacity should be between 50% and 60%.	Create a metric for cloudwatch to oversee then use auto scaling policy to setup when limit is reach
Overall memory and CPU utilization should not go above 80% and 75% respectively or below 30% for either.	Autoscaling policy to more than 75% add one, then if less than 30%, minus one
Internet access is required for patching and updates without exposing the servers.	Security Group SSH with VPN Gateway
Application Tier instances should be tagged as “Key=Name” and “Value=app-tier”.	Autoscaling tag Key=Name Value=app-tier

Again, the use of autoscaling and the load balancer will help with being flexible and allow the application to be used during high traffic hours. Server capacity can be met using CloudWatch to check CPU usage and keep it between a certain amount by utilizing an autoscaling policy. For updating servers without exposing it, the company can set up a security group SSH using a VPN Gateway.

Design: Database Tier

Requirement	Solution
Database needs consistent storage performance at 21,000 IOPS.	Use AWS RDS with MySQL 5.7.22
High availability is a requirement.	Use DB with a standby DB on different availability zone
No change to the database schema can be made at this time.	AWS database migration service – schema conversion tool

Go Green can setup their DB using the same DB that they have been using. They should utilize AWS Database Migration Service to move their database over without touching any schema related.

Design – Network

VPC	Region	Purpose	Subnets	AZs	CIDR Range
1	US West	HQ	Hq-public, hq-private	Us-west-1	172.31.0.0/16
2	EU	Production	Eu-public, eu-private	Eu-west-1	172.32.0.0/16
3	South America	Production	Sa-public, sa-private	Sa-east-1	172.33.0.0/16

Three VPC will be needed since they are in 3 different zones in the world. They should each have different subnet for each and availability zone also.

Subnet Name	VPC	Subnet Type (Public/private)	AZ	Subnet Address
Hq-public	#1	Public	Us-west-1	172.31.0.0/20
Hq-private	#1	Private	Us-west1	172.31.64.0/20
Eu-public	#2	Public	Eu-west-1	172.32.0.0/20
Eu-private	#2	Private	Eu-west-1	172.32.64.0/20
Sa-public	#3	Public	Sa-east-1	172.33.0.0/20
Sa-private	#3	Private	Sa-east-1	172.33.64.0/20

Each VPC will have at least two subnet, one private and one public.

Design – Security

Security Group (SG)	SG Name	Rule	Source
ELB Load Balancer	Elb-sg	None?	
Web Tier	Web-sg	Can receive request on 80 and 443	Anywhere
App Tier	App-sg	Can receive request on 443 and SSH	Webserver
Database Tier	Db-sg	Can receive request on 443	App server

Security group should be made with the company usage in mind. Following direction, only

HTTPs should be used as data going in and out would be encrypted.

Other Security Options	Justification
S3 bucket encryption	Data Leaks

Using encryption on the S3 Bucket would allow the prevention of compromise data leaks.

Design – Encryption

Requirement	Solution
Encryption option for data at rest	RDS > enable encryption
Encryption option for data in transit	HTTPs traffic only

Using RDS and encrypting its data will take care of data at rest while only utilizing HTTPs will allow for encryption of data in transit.

Design – Instance Details

Tier	AMI	Tag	Type	Size	Justification	# of instances
Web	Red Hat Enterprise Linux 7.0 (HVM)	Key: Name Value: app-tier	M4	xlarge	High network performance	6
App	Red Hat Enterprise Linux 7.0 (HVM)	Key: Name Value: web-tier	T2	Xlarge	Meet client requirement	5
DB	Red Hat Enterprise Linux 7.0 (HVM)	N/A	M5	2xLarge	Meet client requirement	2

Size and type should be put into consideration since Go Green only need a certain amount of storage and size of all the application which should be using EC2, the number of instances should be the same as the one they are currently having. AMI should fit the same system they are using which is Red Hat Linux 7.5 .

Design: Recovery Point Objective

Q. How would you achieve a Recovery Point Objective (RPO) of four hours?

A. Use AWS Backup

Usage of AWS Backup will allow for the achievement of RPO of 4 hours if correct setup is made.

Design: Document Storage

Storage/Archive Option	Detail
AWS S3	For frequently accessed data
AWS S3 – Infrequent access	For infrequently accessed data

Use S3 Bucket for document both infrequent and frequently accessed as it's the one that offer the cheapest and easiest to use.

Additional AWS Services

Route 53 – it’s the DNS and it routes to different services and the using the of CloudFront

RDS is just the services used for our database.

RDS for storage and route 53 for large DNS service.

Transit Gateway is used to connect between the three region allows the communication in between the regions, specifically for the database data.