**ACA Project 2:**

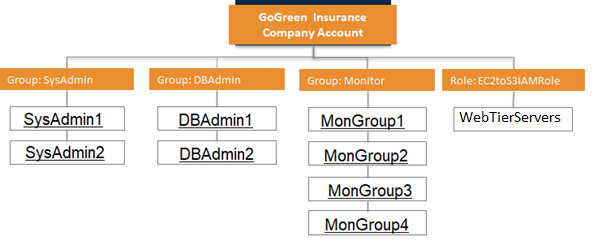
**Designing a Cloud Solution for a GoGreen Insurance Company**

This project is for a GoGreen Insurance Company who are wishing to move onto AWS.

|  |
| --- |
| **Group - Mariah Carey Remastered** |
| *Sean Daly - K00228585* |
| *Christie Molloy - K00227958* |
| *Alexander Ryan - K00209829* |

Use this chart to document users, groups, and roles that need to be created.



Use this chart to document the groups and their associated permissions.

|  |  |  |
| --- | --- | --- |
| **Group/Role #** | **Group/Role Name** | **Permissions** |
| Group | System Administrator | aws:policy/AdministratorAccess |
| Group | Database Administrator | aws:policy/DatabaseAccess |
| Group | Monitoring Group | Monitors 4 users |
| Role | EC2toS3IAMRole | Elevated Permissions0 |

Use this chart to identify solutions for each requirement.

|  |  |
| --- | --- |
| Requirement | Solution |
| Should be at least 8 characters and have 1 uppercase, 1 lowercase, 1 special character, and a number. | Set password policy on AWS for IAM users. |
| Change Passwords every 90 days and ensure that the previous three passwords can’t be re-used. | Require IAM users to change their password after a specified period of time (enable password expiration). Prevent IAM users from reusing previous passwords. |
| All administrators require programmatic access | Add permission policy for admin user group for programmatic access. |
| Administrator sign-in to the AWS Management Console requires the use of Virtual MFA. | Choose the Security credentials tab. Next to Assigned MFA device, choose Manage.    In the Manage MFA Device wizard, choose Virtual MFA device, and then choose Continue. |

Web Tier Requirements

|  |  |
| --- | --- |
| Requirement | Solution |
| Architecture must be flexible and handle any peak in traffic or performance. | Auto Scaling |
| The overall acceptable incoming network bandwidth is between 300 Mbps and 750 Mbps. | Use the proper type to allow the required bandwidth to perform |
| Application administrators want to be notified by email if there are more than 100 “400 HTTP errors” per minute in the application. | Set a cloud watch alarm to send an email to the admin if there are more than 100 “400 HTTP errors” per minute in the application. |
| Web Tier instances should be tagged as “Key=Name” and “Value=web-tier | Set the tags in AWS management console. |

App Tier Requirements

|  |  |
| --- | --- |
| Requirement | Solution |
| Architecture must be flexible and handle any peak in traffic or performance. | Auto scaling |
| Server capacity should be between 50% and 60%. | Load Balancing |
| Overall memory and CPU utilization should not go above 80% and 75% respectively or below 30% for either. | Picking the right instances for the load. |
| Internet access is required for patching and updates without exposing the servers. | Nat Gateway |
| Application Tier instances should be tagged as “Key=Name” and “Value=app-tier”. | Set the tags in AWS management console. |

Database Tier Requirements

|  |  |
| --- | --- |
| Requirement | Solution |
| Database needs consistent storage performance at 21,000 IOPS. | Create RDS DB with provisioned iops of 25000 |
| High availability is a requirement. | Multi AZ deployment with one primary DB and a secondary backup in a separate AZ |
| No change to the database schema can be made at this time. | Use MySQL database engine |

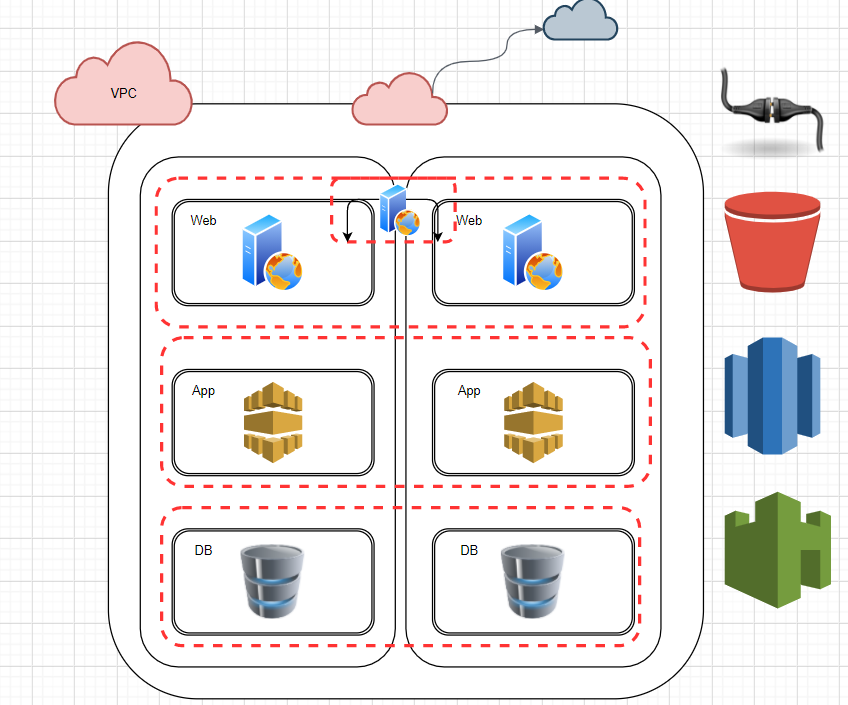
VPC Details

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| VPC | Region | Purpose | Subnets | AZs | CIDR Range |
| 1 | EUwest-1 | Production | 6 | 2 | 10.0.0.0/16 |
| 2 | EUwest-1 | Test Dev | 6 | 2 | 10.0.0.0/16 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Subnet Name | VPC | Subnet Type | AZ | Subnet Address |
| Web-PublicSubnet1 | 1+2 | Public | A | 10.0.0.0/27 |
| Web-PublicSubnet2 | 1+2 | Public | B | 10.0.1.0/27 |
| App-PrivateSubnet1 | 1+2 | Private | A | 10.0.10.0/24 |
| App-PrivateSubnet2 | 1+2 | Private | B | 10.0.11.0/24 |
| DB-PrivateSubnet1 | 1+2 | Private | A | 10.0.20.0/24 |
| DB-PrivateSubnet2 | 1+2 | Private | B | 10.0.21.0/24 |

**Production Subnet Details**

**Diagram:**



Security Details

|  |  |  |  |
| --- | --- | --- | --- |
| Security Group | SG Name | Rule | Source |
| ELB load balancer | Web-elb-sg | Https | 0.0.0.0/0 |
| Web Tier | Web-tier-sg | Http | ELB |
| App Tier | App-tier-sg | Http | WebTier |
| Database Tier | Db-tier=sg | MYSQL/Auror | AppTier |

|  |  |
| --- | --- |
| Other Security Options | Justification |
| VPC Route Tables | Ensure that traffic is routed to the correct locations |
| Network Access Control Lists | Provides traffic protection at the subnet level |
| Host Based Firewalls | Adds another layer of security locally at the OS level |

Encryption Options

|  |  |
| --- | --- |
| Requirement | Solution |
| Encryption option for data at rest | Enable RDS Encryption  Enable S3 server-side encryption |
| Encryption option for data in transit | Enable certificates for all endpoints |

Instance Details

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Tier | Tag | AMI | Type | Size | Justification | # of instance |
| Web | Key = Name  Value = web-tier | Red Hat Enterprise Linux 8 | C5 | Large | They meet the requirements of the current architecture | 6 |
| App | Key = Name  Value = app-tier | Red Hat Enterprise Linux 8 | C5 | 4xLarge | They meet the requirements of the current architecture | 5 |
| DB | n/a | Red Hat Enterprise Linux 8 | Db.r3 | 2xlarge | They meet the requirements of the current architecture | 2 |

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

1. Run game days frequently and practice bringing the system to a working state.

Document Storage

|  |  |
| --- | --- |
| Storage/Archive Option | Detail |
| S3 | S3 life policy for 3 months |
| Glacier | Life policy for 4 years and 9 months then deleted |