GOGREEN MIGRATION WORKSHEET – AWS SPECS BUILT FROM REQUIREMENTS

## VPC Details

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| VPC | Region | Purpose | Subnets | AZs |
| 1 | US-West-1 | Production | 6 | 2 |
| 2 | US-West-1 | Test | 6 | 2 |

|  |  |  |  |
| --- | --- | --- | --- |
| Subnet Name | VPC | Subnet Type (Public/Private) | AZ |
| Web-Private1 | 1 & 2 | Private | A |
| Web-Private2 | 1 & 2 | Private | B |
| App-Private1 | 1 & 2 | Private | A |
| App-Private2 | 1 & 2 | Private | B |
| DB-Private1 | 1 & 2 | Private | A |
| DB-Pivate2 | 1 & 2 | Private | B |

## Security Details

|  |  |  |  |
| --- | --- | --- | --- |
| Security Group | SG Name | Rule | Source |
| ELB Load Balancer | web-elb-sg | Allow 443 | 0.0.0.0/0 |
| Web Tier | web-tier-sg | Allow 8080 | ELB |
| App Tier | app-tier-sg | Allow 8080 | Web Tier |
| Database Tier | db-tier-sg | Allow 3306 | App Tier |

|  |  |
| --- | --- |
| 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 firewall protection at the OS level |
| AWS Marketplace | Offers several advanced security appliances |

## Encryption Options

Based on the requirements, list your encryption options:

|  |  |
| --- | --- |
| Requirement | Solution |
| Encryption option for data at rest | * Enable RDS Encryption * Enable S3 server-side encryption * Use KMS to manage keys |
| Encryption option for data in transit | * Enable SSL certificates for all endpoints |

## Instance Details

Describe the type, size, and justification for the instances you will use for each tier.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Tier | AMI | Tag | Type | Size | Justification | # of instances |
| Web | Amazon Linux | Key: Name  Value: web-tier | T2 | Large | Servers currently at 75% of memory capacity all the time. This number has to decrease to between 50 and 60%. | 6 |
| App | Amazon Linux | Key: Name  Value: app-tier | R3 | 2xlarge | Servers currently at 90% of memory and CPU capacity all the time. This number has to decrease to 50 to 60%. | 6 |
| DB | N/A | N/A | DB.R3 | 2xlarge | RDS instance to match physical resources. Can resize later. | N/A |

## RPO Options

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

Because servers are stateless, snapshots should only be configured on the RDS DB (every 4 hours). Anything extra would not be cost-conscious.

## Document Storage

How would you design document storage based on the requirements?

|  |  |
| --- | --- |
| Storage/Archive Option | Detail |
| S3 | Documents and pictures will be stored in S3 for the first three months. A lifecycle policy will be used to move the data into Glacier at the three-month mark, and then delete it from S3. |
| Glacier | Data will be kept in Glacier for four years and nine months. A lifecycle policy will be used to delete the documents and pictures from Glacier when the time expires. |

## Web Tier Requirements

|  |  |
| --- | --- |
| Requirement | Solution |
| Architecture must be flexible and handle any peak in traffic or performance. | Web server design must allow for the service to scale in parallel. |
| The overall acceptable incoming network bandwidth is between 300 Mbps and 750 Mbps. | Auto Scaling and CloudWatch must start new web servers when incoming network utilization is greater than 750Mbps for at least five minutes. To save money, we will start terminating web servers when incoming network utilization falls below 300Mbps for 10 minutes to avoid autoscaling thrashing. |
| Application administrators want to be notified by email if there are more than 100 “400 HTTP errors” per minute in the application. | Stream the web logs for your web servers to CloudWatch logs and set up an alarm when 400 errors are greater than 100; send an email to the application administrators. |

## App Tier Requirements

|  |  |
| --- | --- |
| Requirement | Solution |
| Architecture must be flexible and handle any peak in traffic or  performance. | Application server design must allow for the service to scale in parallel. |
| Overall memory and CPU utilization should not go above  80% and 75% respectively or below 30% for either. | Auto Scaling and CloudWatch must start new application servers when memory utilization reaches 80% and CPU utilization reaches 75% for at least five minutes. To save money, we will start terminating application servers when both memory and CPU utilization fall below 30% for 10 minutes.  Note: Memory utilization is not a default metric |
| Internet access is required for patching and updates without  exposing the servers. | Ensure that the VPC is set up with a NAT gateway and the route table for the application server’s subnet routes non-local traffic to the gateway. |

## Database Tier Requirements

|  |  |
| --- | --- |
| Requirement | Solution |
| Database needs consistent storage performance at 21,000 IOPS. | Create the RDS database using provisioned IOPS (SSD) EBS volumes. The volume allows for up to 30,000 IOPS. |
| High availability is a requirement. | Configure RDS for Multi-AZ deployment. The primary database will be in one Availability Zone, and a synchronously replicated secondary will be in another Availability Zone. |
| No change to the database schema can be made at this time. | Choose MySQL engine 5.6.22 when creating the RDS database. It will offer a seamless migration option to GoGreen. |

## Additional Services

List any additional AWS services that you would use for your solution and why?

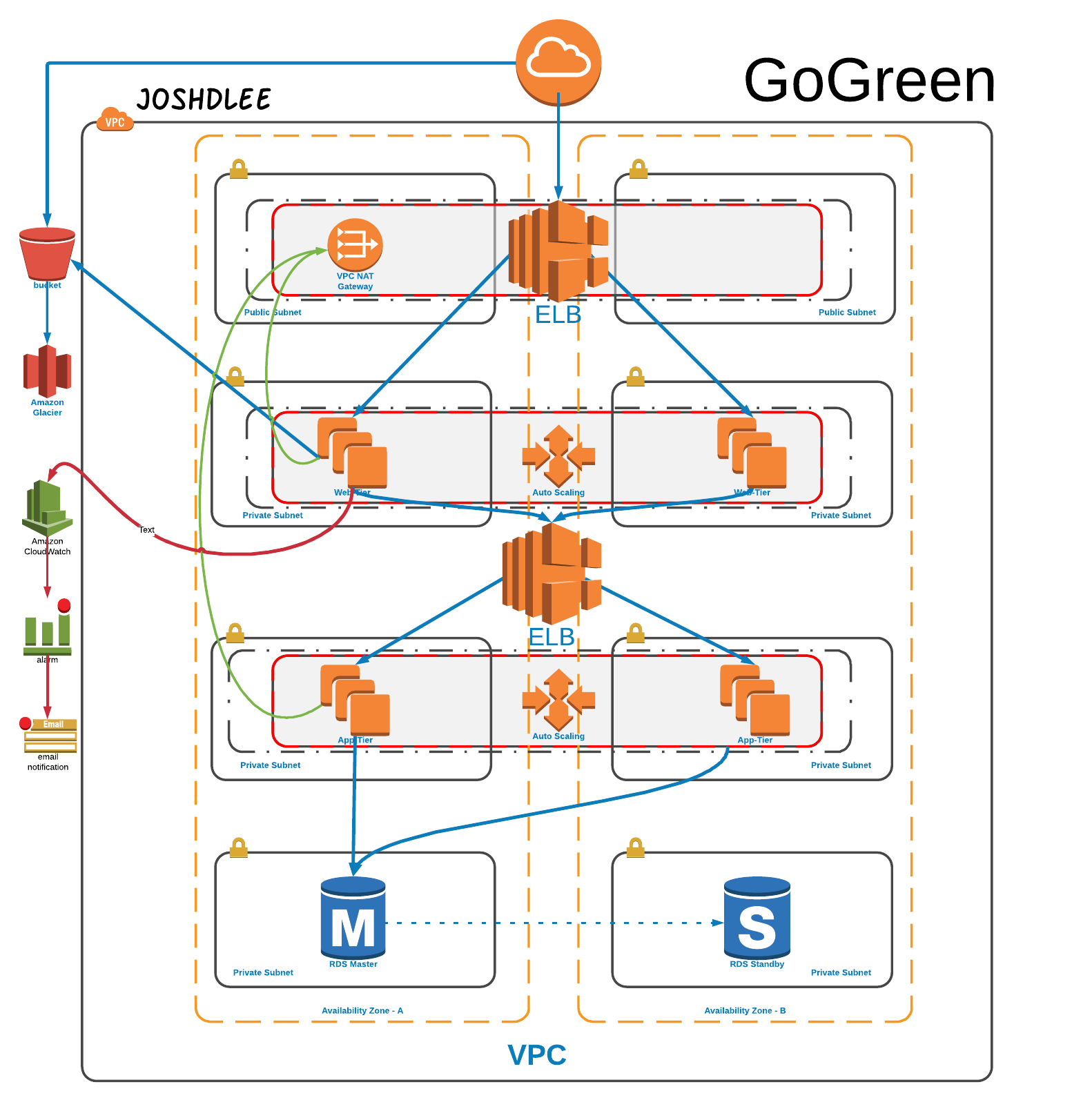
Cloudfront

* CF distribution to get app closer to users in Europe and South America

IAM

* Users/Groups: Only Cloud Team should have access to AWS Services
* Roles: Instances accessing S3 bucket (document and image uploads)

Proposed Architecture Diagram



Joshua Lee [x@joshdlee.com](mailto:x@joshdlee.com) AWS Certified Solutions Architect Professional