Final Project

Linda Lichtenstein

Introduction

GoGreen has been experiencing tremendous growth and finds itself procuring added resources repeatedly, only to start the process over again. Each iteration takes both time and money. Therefore, GoGreen wants to move their datacenter to AWS. This project details the all the services required for GoGreen to run production in AWS. AWS recommends that datacenters not migrate to the cloud all at once, but instead in phases according to the AWS Cloud Adoption Framework (CAF) perspectives. These perspectives are:

1. Business – verify business goals and the value to be achieved
2. Platform – which systems and applications are good candidates to migrate
3. Maturity – which systems and applications are ready to migrate and in what order
4. People – plan organizational changes, determine skills to enhance in-house vs. outsource
5. Process – modify and/or automate existing processes to maintain the expected quality bar
6. Operations – manage and maintain AWS services that meet SLAs and provide adequate recoverability and reliability
7. Security – plan and put in place security levels that meet business requirements

AWS recommends Best Practices for architecting datacenters in the cloud. This project has endeavored to include each Best Practice:

1. Design for failure and nothing fails
2. Loose coupling sets you free
3. Implement elasticity
4. Build security into every layer
5. Don’t fear constraints
6. Think parallel
7. Leverage different storage options

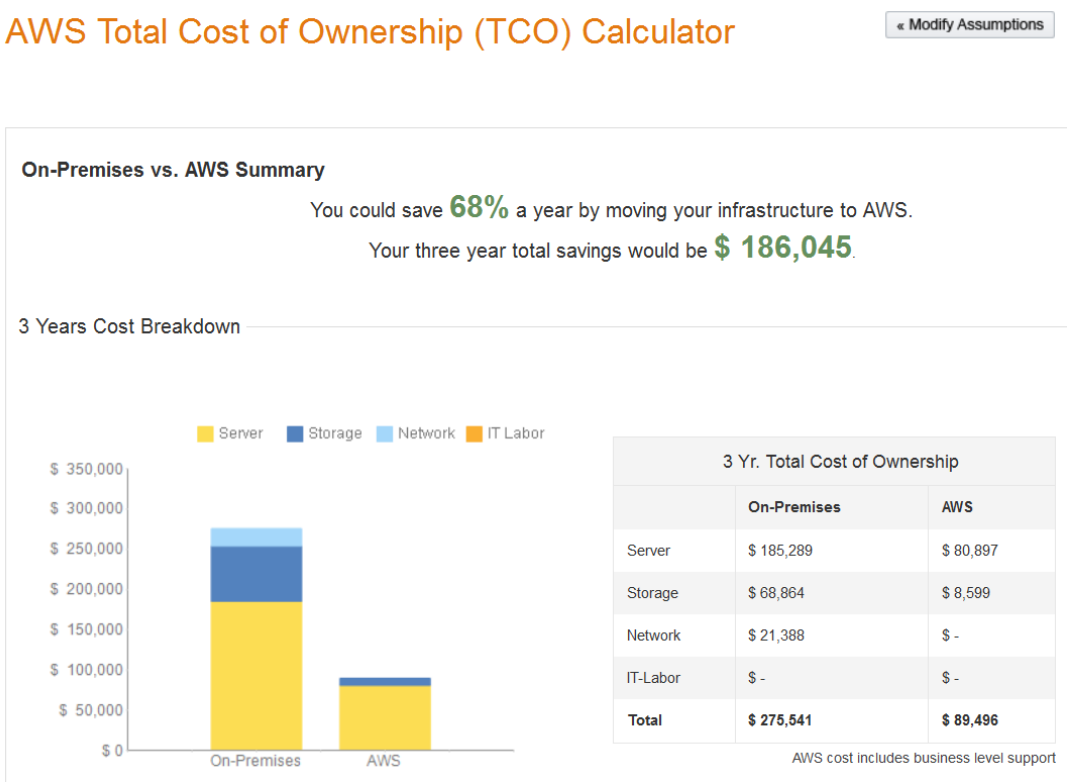
Total Cost of Ownership (TOC)

Region = US West (OR)

GoGreen is based in San Diego, CA. Users include Sales Users at Headquarters, remote users, and mobile users. Most of the users for GoGreen – the Sales Users – are located on the US west coast. AWS recommends that regions be chosen based upon latency, cost, features, and legal compliance. In terms of latency, the region closest to this GoGreen's users is US West (CA) but costs for this region are higher than costs for US West (OR). Since both regions are close to where users are located, and both have the necessary features (legal compliance is not an issue), the region, US West (OR), with the lower costs was chosen. The TCO calculated cost savings for US West (CA) is 68% or $186,045 while the TCO calculated cost savings for US West (OR) is 76% or $208,216.

On occasion, GoGreen's Sales representatives travel to customers in South America and Europe as well. Acceptable performance for access to the application is required when they are in those locations. Because costs to maintain regions in Europe and/or South America are about equivalent to the cost of the main US West region, a second or third region will not be deployed.

Screen shots of the TCO Calculator for GoGreen (based upon current resource levels) for US West (CA) and US West (OR):



Cost savings for US West (CA)

AWS Total Cost of Ownership (TCO) Calculator

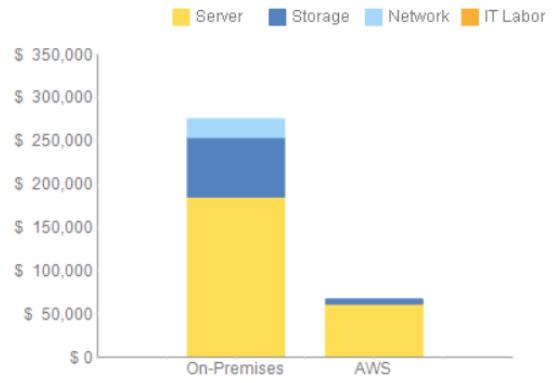
« Modify Assumptions «

On-Premises vs. AWS Summary

You could save **76%** a year by moving your infrastructure to AWS.

Your three year total savings would be **$ 208,216**.

3 Years Cost Breakdown

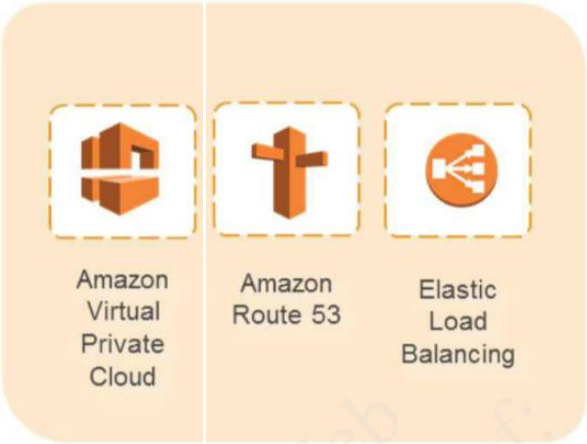


3 Yr. Total Cost of Ownership		
	On-Premises	**AWS**
Server	$ 185,289	$ 61,866
Storage	$ 68,864	$ 5,459
Network	$ 21,388	$ -
IT-Labor	$ -	$ -
Total	**$ 275,541**	**$ 67,325**

AWS cost includes business level support

US West (OR)

Network



Virtual Private Cloud (VPC)

VPCs allow for the definition of the network topology, including definitions for subnets, network access control lists (NACLs), Internet gateways, routing tables, and virtual private gateways. Subnets are created such that webservers that require access to the Internet are placed in Public Subnets while backend systems such as databases or application servers which do not require Internet access are placed in Private Subnets that do not have access to the Internet.

The VPC in the US West (OR) Region has two Availability Zones to ensure High Availability.

Create VPC in US West (OR) with CIDR block 10.0.0.0/16.

Name	VPC ID	State	VPC CIDR	DHCP options set	Route table	Network ACL	Tenancy
GoGreen VPC	vpc-62565907	available	10.0.0.0/16	dopt-5c936739	rtb-d7b6adb2	acl-5807133d	Default

Internet Gateway

The Internet Gateway provides access to the Internet.
Attach the Internet Gateway to the VPC. Destination is 0.0.0.0/0.

Name	ID	State	VPC
GoGreen VPC Gateway	igw-94126cf1	attached	vpc-62565907 (10.0.0.0/16) | GoGreen...

Subnets

Public and Private Subnets as well as an Internet Gateway and NATs provide low-level networking constraints for access to resources.

GoGreen is a three-tier CRM application (web, application, and database); each tier is in a subnet in each Availability Zone. These subnets are private; they do not have access to the Internet.

In addition, in each Availability Zone, there is a public subnet with access to the Internet. Each of these subnets has a Network Address Translation (NAT) server. The NAT servers provide outbound internet access for the EC2 instances in the private web tier. Each NAT is associated with an Elastic Load Balancer and Auto Scaling group.

Create a public subnet in AZ us-west-2a with CIDR block 10.0.10.0/24.

Create three private subnets in AZ us-west-2a.

- Web Subnet with CIDR block 10.0.20.0/24
- App Subnet with CIDR block 10.0.30.0/24
- DB Subnet with CIDR block 10.0.40.0/24

Create a public subnet in AZ us-west-2b with CIDR block 10.0.11.0/24

Create three private subnets in AZ us-west-2b.

- Web Subnet with CIDR block 10.0.21.0/24
- App Subnet with CIDR block 10.0.31.0/24
- DB Subnet with CIDR block 10.0.41.0/24

Name	Subnet ID	State	VPC	CIDR	Available IPs	Availability Zone
GoGreen DB Subnet	subnet-d43527b1	available	vpc-62565907 (10.0.0.0/16) | GoGreen...	10.0.40.0/24	251	us-west-2a
GoGreen Public Subnet	subnet-1a34267f	available	vpc-62565907 (10.0.0.0/16) | GoGreen...	10.0.10.0/24	251	us-west-2a
GoGreen DB Subnet	subnet-1dd8ef6a	available	vpc-62565907 (10.0.0.0/16) | GoGreen...	10.0.41.0/24	251	us-west-2b
GoGreen App Subnet	subnet-3ad8ef4d	available	vpc-62565907 (10.0.0.0/16) | GoGreen...	10.0.31.0/24	251	us-west-2b
GoGreen App Subnet	subnet-883426ed	available	vpc-62565907 (10.0.0.0/16) | GoGreen...	10.0.30.0/24	251	us-west-2a
GoGreen Public Subnet	subnet-69d8ef1e	available	vpc-62565907 (10.0.0.0/16) | GoGreen...	10.0.11.0/24	251	us-west-2b
GoGreen Web Subnet	subnet-de3426bb	available	vpc-62565907 (10.0.0.0/16) | GoGreen...	10.0.20.0/24	251	us-west-2a
GoGreen Web Subnet	subnet-43d8ef34	available	vpc-62565907 (10.0.0.0/16) | GoGreen...	10.0.21.0/24	251	us-west-2b

Routing Tables

Create a route table that allows traffic to flow from and to the Internet and the Public Subnet in AZ 1:

- Set Destination to CIDR Block 0.0.0.0/0 and target to the Internet Gateway (GoGreen VPC Gateway).
- Associate this route table with the Public Subnet in AZ 1 us-west-2a and CIDR range 10.0.10.0/24

Create route tables and associate with subnets in AZ 1 us-west-2a.

- By default, each subnet is associated with the main route table
- Create a route table and associate the Public subnet to the Web subnet
- Create a route table and associate the Web subnet with the App subnet

Create a route table and associate the App subnet with the DB subnet

Name	Route Table ID	Explicitly Associat	Main	VPC
GoGreen Web App	rtb-ffadb69a	1 Subnet	No	vpc-62565907 (10.0.0.0/16) | GoGreen...
GoGreen Public to Web	rtb-25aeb540	1 Subnet	No	vpc-62565907 (10.0.0.0/16) | GoGreen...
GoGreen Public Route	rtb-54a8b331	1 Subnet	No	vpc-62565907 (10.0.0.0/16) | GoGreen...
GoGreen App DB	rtb-67acb702	1 Subnet	No	vpc-62565907 (10.0.0.0/16) | GoGreen...

Create route tables for each subnet in AZ 2 the same as above using subnet 2 CIDR blocks values.

Create a NAT Instance

Choose AMI - Amazon Linux AMI 2015.09.1 (HVM), SSD Volume Type - ami-f0091d91

Choose General Purpose t2.micro Instance type

Place in GoGreen VPC / Public Instance in AZ us-west-2a (CIDR block 10.0.10.0/24)

Can accept traffic from HTTP (port 80), HTTPS (443), or SSH (22)

Instance Type Edit insta

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
t2.micro	Variable	1	1	EBS only	-	Low to Moderate

Security Groups Edit securit

Security group name NAT-SG
Description NAT Security Group

Type	Protocol	Port Range	Source
SSH	TCP	22	0.0.0.0/0
HTTP	TCP	80	0.0.0.0/0
HTTPS	TCP	443	0.0.0.0/0

Create a new Key Pair – GoGreen Key Pair

Point the Private Web Tier subnet to the NAT – Destination is 0.0.0.0/0 and Target is NAT

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No
0.0.0.0/0	eni-2c5ca454 / i-063ac1c1	Black Hole	No

Virtual Private Gateway

A Virtual Private Gateway provides access to a company's data centers.

Create a Virtual Private Gateway to connect GoGreen corporate datacenter to AWS.

Name	ID	State	Type	VPC
GoGreen Virtual Private Gateway	vgw-99d90787	attached	ipsec.1	vpc-d47976b1 (10.0.0.0/16) | GoGreen VPC

Create a connection between AWS and the corporate datacenter. Use IP address associated with GoGreen's datacenter.

Name	ID	State	Type	VPC
GoGreen VPN	vgw-69d60877	attached	ipsec.1	vpc-d2e4ebb7 (10.0.0.0/16) | GoGreen VPC

Create VPN Connection

Select the virtual private gateway and customer gateway that you would like to connect via a VPN connection. You must have entered the virtual private gateway and your customer gateway information already.

Name tag GoGreen VPN Connection

Virtual Private Gateway vgw-99d90787 | GoGreen Virtual Private (

Customer Gateway Existing New

IP Address (e.g. 192.2.1.1)

BGP ASN 65000

Specify the routing for the VPN Connection (Help me choose)

Routing Options Dynamic (requires BGP) Static

VPN connection charges apply once this step is complete. View Rates

VPN NACL Create a Network ACL to allow VPN Gateway traffic from GoGreen datacenter to Subnet 10.0.10.0/24 and from Subnet 10.0.10.0/24 to the GoGreen datacenter.

Route 53

Route 53, a public Internet-facing and Private Intranet-facing Domain Name Service (DNS), is a reliable, cost-effective way to route end users to Internet applications. It routes end users to Internet applications by translating human-readable names into numeric IP addresses that computers use to connect to each other. Since it is global, all GoGreen users (Sales, Remote, and Mobile) may access GoGreen applications from the locations they travel to in Europe and South America. In addition, Route 53 supports multi-region and backup architectures for high availability and scalability.

Create an A Record and CNAME Record where the Hosted Zone (DNS name) is the GoGreen on AWS: gogreenawsdatacenter.com

Elastic Load Balancing (ELB)

Elastic Load Balancing IELB) automatically distributes traffic across multiple EC2 instances. By default, the load balancer routes each request independently to the application instance with the smallest load.

Elastic Load Balancing detects unhealthy instances and automatically reroutes traffic to healthy instances until the unhealthy instances have been restored.

The GoGreen AWS implementation has provisioned load balancers across both Availability Zones for even more consistent application performance. It has two load balancers – one in the public subnet for the NAT servers, and one in the Application tier for the application servers.

Security Groups are defined

Load Balancer for NAT in Public Subnets

Create the Load Balancer for the NAT servers in the Public Subnets. The NAT servers will balance traffic from the Internet (HTTP, HTTPS and TCP) to the Web Tier Private Subnets across both Availability Zones.

Load Balancer name: GoGreen-Public-Load-Balancer

Create LB Inside: vpc-7df0ff18 (10.0.0.0/16) | GoGreen VPC

Create an internal load balancer: ☑ (what's this?)

Enable advanced VPC configuration: ☑

Listener Configuration:

Load Balancer Protocol	Load Balancer Port	Instance Protocol	Instance Port
HTTP	80	HTTP	80

VPC vpc-7df0ff18 (10.0.0.0/16) | GoGreen VPC

Available Subnets

Actions	Availability Zone	Subnet ID	Subnet CIDR	Name
⊕	us-west-2a	subnet-f1564b94	10.0.20.0/24	Private Subnet 1
⊕	us-west-2b	subnet-30221447	10.0.21.0/24	Private Subnet 2

Selected Subnets

Actions	Availability Zone	Subnet ID	Subnet CIDR	Name
⊖	us-west-2a	subnet-51564b34	10.0.10.0/24	Public Subnet 1
⊖	us-west-2b	subnet-862513f1	10.0.11.0/24	Public Subnet 2

sg-f1f41896	ELB SG	Public ELB Security Group

Step 4: Configure Health Check

Your load balancer will automatically perform health checks on
removed from the load balancer. Customize the health check to

Ping Protocol	HTTP
Ping Port	80
Ping Path	/index.html

Advanced Details

Response Timeout	15	seconds
Health Check Interval	30	seconds
Unhealthy Threshold	2	
Healthy Threshold	2	

Security Group Create a security group – ELG SG - for the load balancer in the public subnet. Set inbound rules to the Internet.

Security Group: sg-f1f41896

Description | Inbound | Outbound | Tags

Group name	ELB SG	Group description	Public ELB Security Group
Group ID	sg-f1f41896	VPC ID	vpc-7df0ff18

Type	Protocol	Port Range	Source
HTTP	TCP	80	0.0.0.0/0

Load Balancer for Application in Private Subnets

Create a load balancer similar to that in the Public Subnets in the Private Subnets. The load balancer will balance traffic from the EC2 Instances in the Web Tier to the EC2 Instances in the App Tier across both Availability Zones.

Security Group Create a security group – APP SG – for the load balancer in the private subnet. Set inbound rules to the security group for the load balancer in the Public Subnets

Security Group: sg-2bf5194c

Description | Inbound | Outbound | Tags

Group name	App SG	Group description	Private App Security Group
Group ID	sg-2bf5194c	VPC ID	vpc-7df0ff18

Type	Protocol	Port Range	Source
HTTP	TCP	80	sg-f1f41896 (ELB SG)

Security

Multiple layers of security, including security groups and network access control lists, help control access to EC2 instances in each subnet.

Security Groups are built-in firewalls for virtual servers that sit in front of every network interface providing full control over inbound and outbound traffic. Security Group rules can be defined to control accessibility to instances ranging from completely private to completely public.

Public Subnet – Accepts traffic on ports 80 and 443 from anywhere on the Internet if the source is 0.0.0.0/0.

Web Tier – Accepts traffic from the load balancer in the Public Subnet so that a web serve cannot be overloaded.

App Tier – Can only accept traffic from the Web Tier.

DB Tier – Can only accept traffic from the App Tier.

SSH port 22 – rules to allow remote administration. Restrict remote access by funneling all traffic through the app tier (to a Bastion Host) and allowing access only from a specific IP. After accessing the app tier, can access the web and DB tiers as per their security groups.

Network Access Control Lists (ACLs) NACLs allow or deny traffic entering or exiting the public subnet by enforcing baseline security policies.

Public Subnet NACL: Allow traffic for HTTP and HTTPS to enter and exit the public subnets for AZ 1 and AZ 2.

Create a NACL to access the public subnet 10.0.10.0/24 from the Internet, and to access the Internet from the public subnet, 10.0.10.0/24.

Public NACL	acl-425f4827	2 Subnets	No	vpc-d2e4ebb7 (10.0.0.0/16) | GoGreen VPC

acl-425f4827 | Public NACL

Summary | Inbound Rules | Outbound Rules | Subnet Associations | Tags

Network ACL ID: acl-425f4827 | Public NACL

Default: no

Associated with: 2 Subnets

VPC: vpc-d2e4ebb7 (10.0.0.0/16) | GoGreen VPC

acl-425f4827 | Public NACL

Summary | Inbound Rules | Outbound Rules | Subnet Associations

Allows inbound traffic. Because network ACLs are stateless, you must create inbound and outbound rules.

Edit

Rule #	Type	Protocol	Port Range	Source	Allow / Deny
1	HTTP (80)	TCP (6)	80	0.0.0.0/0	ALLOW
2	HTTPS (443)	TCP (6)	443	0.0.0.0/0	ALLOW
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

acl-425f4827 | Public NACL

Summary | Inbound Rules | **Outbound Rules** | Subnet Associations

Allows outbound traffic. Because network ACLs are stateless, you must create inbound and outbound rules.

Edit

Rule #	Type	Protocol	Port Range	Destination	Allow / Deny
1	ALL Traffic	ALL	ALL	0.0.0.0/0	ALLOW
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

acl-425f4827 | Public NACL

Summary | Inbound Rules | Outbound Rules | **Subnet Associations**

Edit

Subnet	CIDR
subnet-52370125 (10.0.10.0/24) | GoGreen Public Subnet	10.0.10.0/24
subnet-b7aab8d2 (10.0.11.0/24) | GoGreen Public Subnet	10.0.11.0/24

Security Group SSH on port 22 provide rules to allow remote administration. Restrict remote access by funneling all traffic through the app tier (to a Bastion Host) and allowing access only from a specific IP.

GoGreen SG	sg-95876bf2	GoGreen SG	vpc-d2e4ebb7	GoGreen Security Group

sg-95876bf2 | GoGreen SG

Summary | **Inbound Rules** | Outbound Rules | Tags

Cancel | Save

Type	Protocol	Port Range	Source
SSH (22)	TCP (6)	22	sg-95876bf2

Key Management Service

GoGreen data is required to be encrypted - the data is encrypted on S3, the MySQL database, and the Elastic Block Storage Volumes when these resources are created.

Deployment and Management

Identity and Access Management (IAM)

IAM provides secure control access to AWS services and resources for users by creating and managing users, groups, and roles. User accounts can be created to provide each user with his or her own unique security credentials eliminating the need for users to share passwords and allowing the granting of permissions for access to only the AWS services and resources they need to do their jobs.

GoGreen's Sales users access the application while in GoGreen Headquarters, and remotely when they travel to customer locations in Europe and South America. They may also access the applications from their mobile devices.

Users: Two IAM Sales users are created and each given full access to S3, Route53, and Glacier. A group – Sales – is created which includes both Sales users; they are given full access permissions to EC2.

Sales Group – Create a group for Sales employees and grant permissions for EC2 instances so they can access the application.

Admin: Create an admin user and two Admin Groups – Admin Group and Admin User Group. Give the Admin Group full administration permissions.

Dev: Create a developer user and give access to deploy code.

Create users – Create two Headquarters Sales Users, SalesUser1 and SalesUser2, and set passwords.

SalesUser1

Access Key ID: AKIAI7U5BNFPG2WZQPAA
Secret Access Key: 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

SalesUser2

Access Key ID: AKIAJKG2XZG5XQS7HZPA
Secret Access Key: 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

SalesUser1

Password: swQMtFsN5J]T

SalesUser2

Password: kmx)}Wz&q^nz

IAM Policy for Sales Users 1 and 2 – Allow full access to the applications they will use – Route 53, S3, Glacier.

IAM > Users > **SalesUser1**

Summary

User ARN:	arn:aws:iam::588488049979:user/SalesUser1
Has Password:	Yes
Groups (for this user):	0
Path:	/
Creation Time:	2016-01-15 13:09 EST

Groups | Permissions | Security Credentials | Access Advisor

Managed Policies

The following managed policies are attached to this user. You can attach u

Attach Policy

Policy Name	Actions
AmazonS3FullAccess	Show Policy
AmazonGlacierFullAccess	Show Policy
AmazonRoute53FullAccess	Show Policy

IAM > Users > **SalesUser2**

Summary

User ARN:	arn:aws:iam::588488049979:user/SalesUser2
Has Password:	Yes
Groups (for this user):	0
Path:	/
Creation Time:	2016-01-15 13:09 EST

Groups | Permissions | Security Credentials | Access Advisor

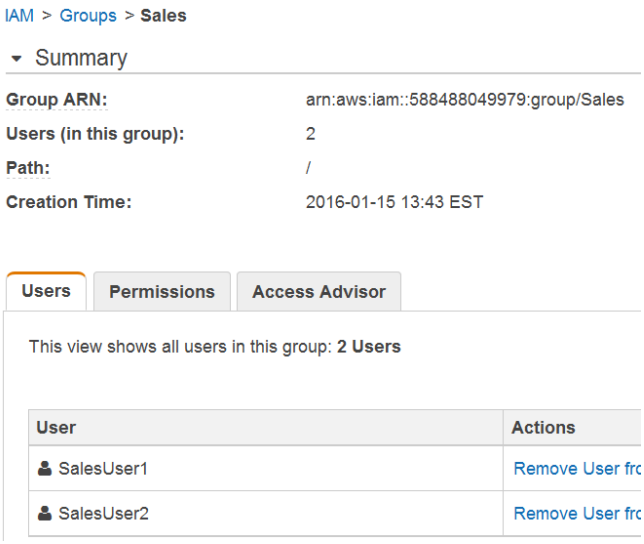
Managed Policies

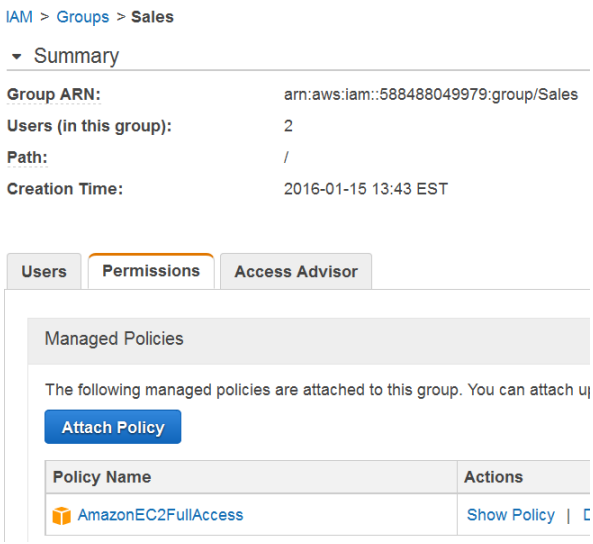
The following managed policies are attached to this user. You can attach u

Attach Policy

Policy Name	Actions
AmazonS3FullAccess	Show Polic
AmazonGlacierFullAccess	Show Polic
AmazonRoute53FullAccess	Show Polic

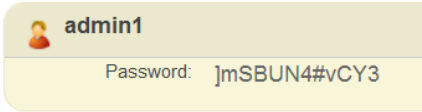
Create Group Sales and add SalesUser1 and SalesUser2.

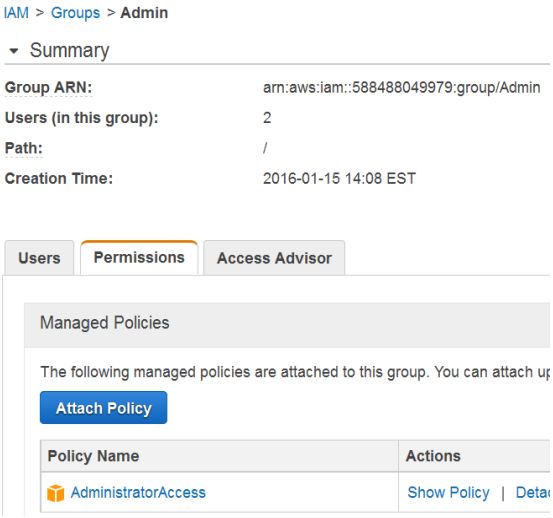




And give full permission to access EC2 functions

Create an Admin User and assign him to the Admin Group. Give the Admin Group all Administration permissions





Create a Development User – Dev1 – and Group – Developers – and grant the group Full access to commit and deploy code

Dev1

Access Key ID: AKIAI2K7POZKWIA23NGA
Secret Access Key: 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

Dev1

Password: u9FuDcB*1Q8D

IAM > Groups > **Developers**

Summary

Group ARN:	arn:aws:iam::588488049979:group/Developers
Users (in this group):	1
Path:	/
Creation Time:	2016-01-15 14:23 EST

Users | **Permissions** | **Access Advisor**

Managed Policies

The following managed policies are attached to this group. You can attach up to 1

Attach Policy

Policy Name	Actions
AWSCodeCommitFullAccess	Show Policy |
AWSCodeDeployFullAccess	Show Policy |

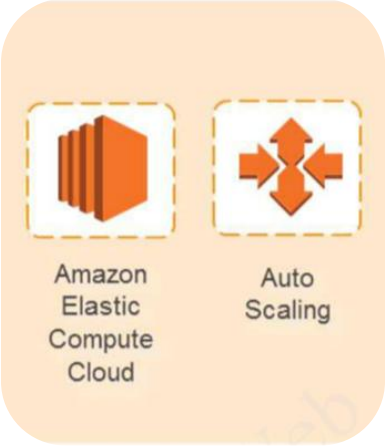
CloudWatch

A centralized metrics repository. Common server and user errors, like 400 HTTP, are returned and an email may be sent to the designated notification list via Simple Notification Service (SNS). An alarm can be set to monitor the GoGreen application and send an email to the administrator if there are more than 100 HTTP 400 errors.

Elastic BeanStalk

Elastic BeanStalk was used to provision the Java platform in the App Tier.

Compute



EC2 instances

EC2 Instances are virtual computing environments comprised of virtual servers that run applications.

EC2 Instances are launched from a pre-configured Amazon Machine Images (AMI), a template which includes the Operating System and Software. AMIs are chosen based on CPU, memory, storage, and network requirements.

It is not necessary to get a larger instance type than the application requires. It is recommended to pick the closest instance size to what the application requires to run smoothly as unexpected spikes in workload can be handled by Auto Scaling.

Instances in the GoGreen AWS implementation are launched in two Availability Zones in one VPC within the US West (OR) region. EC2 Instances can be billed in three ways: On Demand, Reserved, and Spot. Of the three methods, On Demand and Reserved would best satisfy GoGreen's requirements. When first deploying to AWS, AWS recommends using On Demand instances until a history is developed. Once processing requirements are known, a decision can be made as to how many Reserved Instances are required and whether they should be reserved for 1 or 3 years, paid upfront, partially paid upfront, or not paid upfront at all.

General Purpose Instances (M3, M4) were chosen for GoGreen because this family of instances provides a balance of compute, memory, and network resources which is suitable for systems like GoGreen's.

Instances come with locally attached storage – ephemeral storage; This type of storage is terminated when the instance is terminated. Since GoGreen has PHP files in its Web Tier and Java application files in its App Tier, Elastic Block Storage (EBS) volumes which are network attached and provide persistent storage will be provisioned.

A Key Pair is made up of Public and Private keys. EC2 uses public-key cryptography to encrypt and decrypt login information. Public-key cryptography uses a public key to encrypt a piece of data such as a password. The recipient uses the private key to decrypt the data. A key pair must be created to login to the instance. The name

of the key pair is specified when the instance is launched. Linux instances do not have passwords – use a key pair to login using SSH. The Key Pair created is in the file GoGreenKeyPair.pem and is used to login to all GoGreen instances.

NAT in Public Subnet

NAT server in Public subnets are t2.micro instances, ami-f0091d91.

Web Tier

Web Instance - Number of initial instances – 10. GoGreen currently has 6 virtual machines that are at 75% capacity all the time. They need to deploy enough servers so that the machines are running at 50 – 60% capacity.

The ami which matches the current GoGreen system, SUSE Linux Enterprise Server 12 SP1 (HVM), SSD Volume Type - ami-b7b4fedd, was chosen. The General Purpose Instance t2.medium was chosen because it matches GoGreen's current memory and vCPU levels.
Storage – Root volume, General purpose, 10 GB, 30 – 3,000 IOPS

Apache web server with PHP installed.

App Tier

App Instance – Number of initial instances – 8. GoGreen currently has 5 virtual machines that are at 90% capacity all the time. They need to deploy enough servers so that the machines are running at 50 – 60% capacity.

The ami which matches the current GoGreen system, SUSE Linux Enterprise Server 12 SP1 (HVM), SSD Volume Type - ami-b7b4fedd, was chosen. Although its vCPU level is double the current level, the General Purpose Instance m4.2xlarge was chosen because it matches GoGreen's current memory level.

Storage – Root volume, General purpose, 10 GB, 30 – 3,000 IOPS

Java platform installed with Elastic BeanStalk.

Database Tier

Database Instance – The same database currently used at GoGreen - MySQL database engine version 5.6.22 - is provisioned. The ami which matches the current GoGreen system, SUSE Linux Enterprise Server 12 SP1 (HVM), SSD Volume Type - ami-b7b4fedd, was chosen. Db.m4.4xlarge of Database Instance class M3/M4 size was chosen because it is a SSD-based instance storage for fast I/O performance and balanced for compute, memory, and network resources. Although it is larger than what GoGreen currently has, it offers the closest memory requirement (64GB) over the current 48 GB memory. Provisioned IOPS was chosen because the database needs consistent storage performance of 21,000 IOPS (PIOPS provides 1,000 to 30,000 IOPS).

The database instances are provisioned in both AZs.

Specify DB Details

Instance Specifications

DB Engine	mysql
License Model	general-public-license
DB Engine Version	5.6.22

Review the **Known Issues/Limitations** to learn about potential compatibility issues with specific database versions.

DB Instance Class	db.m4.4xlarge — 16 vCPU, 64 GiB RA
Multi-AZ Deployment	Yes
Storage Type	Provisioned IOPS (SSD)
Allocated Storage*	100 GB
Provisioned IOPS	1000

Details:**db.m4.4xlarge**

Type	Standard - Current Generation
vCPU	16 vCPU
Memory	64 GiB
EBS Optimized	2000 Mbps
Network Performance	High
Free Tier Eligible	No

- *Provisioned IOPS (SSD)* storage is suitable for I/O-intensive database workloads. Provides flexibility to provision I/O ranging from 1,000 to 30,000 IOPS.

Settings

DB Instance Identifier*	gogreendbinstance
Master Username*	ggmasteruser
Master Password*	••••••••••
Confirm Password*	••••••••••

Password: ggmasterpw

Make the database multi-AZ and enable encryption.

Database Options

Database Name	GoGreenMasterDB

Note: if no database name is specified then no initial MySQL database will be created on the DB Instance.

Database Port	3306
DB Parameter Group	default.mysql5.6
Option Group	default:mysql-5-6
Copy Tags To Snapshots	☐
Enable Encryption	Yes
Master Key	(default) aws/rds

Auto Scaling

Auto Scaling automatically resizes compute clusters - EC2 Instances - capacity up or down based on demand as determined by a combination of policies and alarms which specify scaling conditions.

Auto Scaling Web Tier – Six servers have a 90% utilization rate. The utilization rate needs to drop to 50% to 60% when move to AWS. Minimum number of instances – 10; Maximum number of instances – 20. Set alarm to Scale-up (add instances) if CPU > 75% for 10 minutes. Set alarm to Scale-down (remove instances) if CPU < 30% for 10 minutes.

Auto Scaling App Tier – Five servers have a 90% utilization rate. The utilization rate needs to drop to 50% to 60% when move to AWS. Minimum number of instances – 8; Maximum number of instances – 16. Set alarm to Scale-up (add instances) if CPU > 75% for 10 minutes. Set alarm to Scale-down (remove instances) if CPU < 30% for 10 minutes.

Auto Scaling DB Tier – Read Replicas added for horizontal scaling of heavy read loads.

Auto Scaling with DynamoDB – Create the table with the desired amount of request capacity. This capacity can be increased or decreased as the application's requirements become better understood. Since the capacity required is unknown, the DynamoDB table was created with the default values.

Storage

Amazon Simple Storage Service (S3)

S3 is a durable, scalable, unlimited object store for images, videos, files, binaries, and snapshots. Data is stored in S3 as objects within buckets. An object is a file and metadata describing the file.

Created a bucket – gogreenlllsalesstorage and three folders.

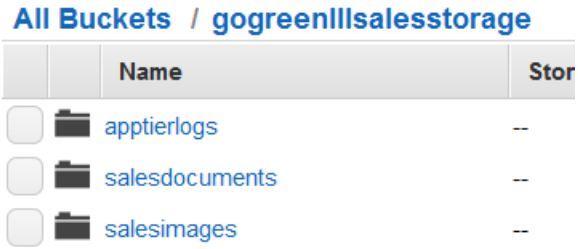
Apptierlogs to hold log files from App Tier

Salesdocuments to store documents such as contracts.

Salesimages to store images

Create folder – SnapShots for storing EBS volume snap shots

Create folder – AMI for storing EC2 Instance AMIs



Since documents and images are rarely accessed after 3 months, set contents in the documents and images folders to be transferred to Glacier after 90 days. Data is encrypted.

Action on Objects

☐ **Transition to the Standard - Infrequent Access Storage Class** Days after the object's creation date

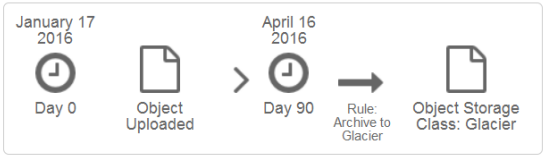
Standard - Infrequent Access has a 30-day minimum retention period and a 128KB minimum object size. Lifecycle policy will not transition objects that are less than 128KB. Refer here to learn more about Standard - Infrequent Access.

☑ **Archive to the Glacier Storage Class** 90 Days after the object's creation date

This rule could reduce your storage costs. Refer here to learn more about Glacier pricing. Note that objects archived to the Glacier Storage Class are not immediately accessible .

☐ **Permanently Delete** Days after the object's creation date

EXAMPLE:



Lifecycle

You can manage the lifecycle of objects by using Lifecycle rules. Lifecy
transition objects to the Standard - Infrequent Access Storage Class,
Storage Class, and/or remove objects after a specified time period. R
share the specified prefix.

Versioning is not currently enabled on this bucket.

You can use Lifecycle rules to manage all versions of your objects. Thi
and Previous versions.

Enabled	Name	Rule Target
☑	Move to Glacier 90 days	salesdocuments
☑	Move to Glacier 90 days i...	salesimages

Bucket: gogreenlllsalesstorage ×

Bucket: gogreenlllsalesstorage
Region: Oregon
Creation Date: Sun Jan 17 19:04:06 GMT-500 2016
Owner: aws03218

Permissions

You can control access to the bucket and its contents using access policies. Learn more.

Grantee: aws03218 ☑ List ☑ Upload/Delete ☑ View Permissions ☑ Edit Permissions x

Grantee: Log Delivery ☐ List ☑ Upload/Delete ☑ View Permissions ☐ Edit Permissions x

Glacier

Glacier is low cost storage for archival and backup. It is designed with the expectation that retrievals are infrequent and unusual, and data will be stored for an extended period of time.

Since the documents and images produced by GoGreen are rarely accessed after three months, they are archived in Glacier. They must be retained for five years; Glacier is set up to delete the images and documents after five years. Data is encrypted in Glacier.

AWS Storage Gateway (ASG)

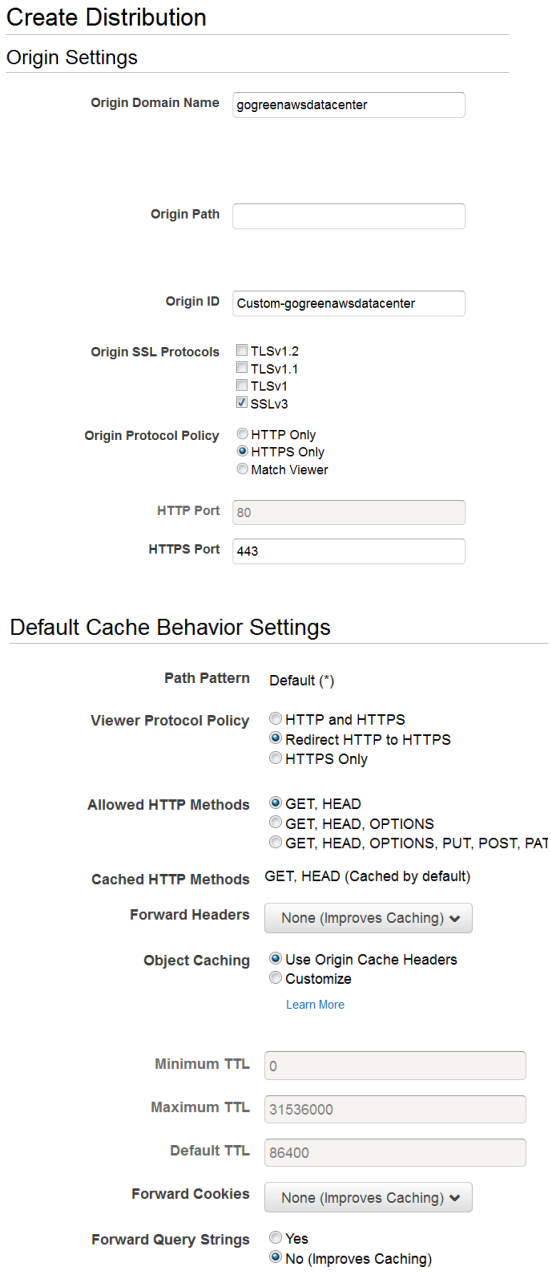
AWS Storage Gateway is a service that connects an on-premises IT with AWS storage.

Provision an AWS Storage Gateway between GoGreen datacenter and AWS to provide for disaster recovery. This service is also needed to migrate GoGreen applications over to AWS and to move new production releases.

CloudFront

CloudFront is a content delivery web service that integrates with other AWS services to give developers and business an easy way to distribute content to end users.

Provision CloudFront: use encryption for submissions: HTTPS and SSL



Smooth Streaming ○ Yes ◉ No

Restrict Viewer Access (Use Signed URLs or Signed Cookies) ○ Yes ◉ No

Compress Objects Automatically ○ Yes ◉ No

Learn More

Distribution Settings

Price Class Use All Edge Locations (Best Performance)

AWS WAF Web ACL None

Alternate Domain Names (CNAMEs)

SSL Certificate ◉ Default CloudFront Certificate (*.cloudfront.net)

Choose this option if you want your users to use HTTPS or HTTP to access your content with the CloudFront domain name (such as https://d111111abcdef8.cloudfront.net/logo.jpg).
Important: If you choose this option, CloudFront requires that browsers or devices support TLSv1 or later to access your content.

○ Custom SSL Certificate (example.com):

Choose this option if you want your users to access your content by using an alternate domain name, such as https://www.example.com/logo.jpg.
You can use SSL certificates previously uploaded to the IAM certificate store.

Default Root Object

Logging ○ On ◉ Off

Bucket for Logs

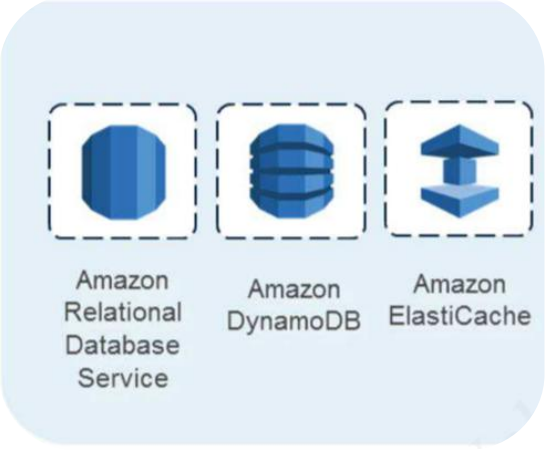
Log Prefix

Cookie Logging ○ On ◉ Off

Comment

Distribution State ◉ Enabled ○ Disabled

Database



Amazon RDS with MySQL

Relational MySQL database. RDS for MySQL provides two distinct but complementary replication features:

Multi-AZ deployments, and

Read replicas

that can be used in conjunction to gain enhanced database availability, protect latest database updates from unplanned outages, and scale beyond the capacity constraints of a single DB instance for read-heavy database workloads.

A MySQL 5.6.22 database cluster is provisioned with Read Replicas. There is a Master database in Availability Zone 1 which writes to the Read Replica in the same AZ. There is also a copy of the Master database – the RDS Standby – in Availability Zone 2. The Master database in AZ 1 reads and writes to that database. In addition, the Master database writes to a second Read Replica in AZ 2.

Data is encrypted via KMS

Read Replica created for AZ 1 Master Database:

Engine	DB Instance	Status	CPU	Current Activity	Maintenance	Class	VPC	Multi-AZ	Replication Role	Encrypted
MySQL	gogreendbinstance	available	0.13%	1 Connections	None	db.m4.4xlarge	vpc-2967694c	Yes	master	No
MySQL	ggdbinstance	available	0.07%	0 Connections	None	db.m4.4xlarge	vpc-2967694c	No	replica	No

RDS Security for the Master Database in AZ 1:

Access Control

Settings

DB Instance Identifier*	gogreendbinstance
Master Username*	ggmasteruser
Master Password*	••••••••••
Confirm Password*	••••••••••

When the first DB instance was first created, a master user account was created. This account is used only within the context of RDS to control access to the DB instances. The master user account is a native database user account that allows the owner to log into the DB instance with all database privileges.

The master user name is “ggmasteruser“ and the password is “ggmasterpw”.

Database Security groups are similar to EC2 security groups, but not interchangeable. They act like a firewall controlling network access to DB instances. Only allow access to the database server port (all others are blocked) 3306.

DynamoDB

DynamoDB is a fast, NoSQL database service that make it simple and cost effective to store and retrieve any amount of data and serve any level of request traffic.

The DynamoDB was created for GoGreen to store session data to ensure mobile users maintain their session while accessing GoGreen applications.

ElastiCache

ElastiCache Improves performance of web applications by retrieving information from a fast, managed, in-memory caching system.

Web Tier – provision ElastiCache in both AZs

Mobile

Simple Notification Service (SNS)

Simple Notification Service (SNS) is a fast, flexible, fully managed push messaging service.

SNS is used by GoGreen to send email messages to the administrator when more than 100 HTTP 400 errors are detected by the Web Tier.

Recovery Time and Recovery Point

Recovery Time Objective and Recovery Point Objective

Recovery Time Objective (RTO) – how quickly must the system recover?

Recovery Point Objective (RPO) – How much data can afford to lose?

The GoGreen Recovery Point Objective of four hours and Recovery Time Objective of 30 minutes is achieved by designing the AWS architecture to be fault tolerant and highly available. Inherently fault tolerant and highly available services include S3, RDS, DynamoDB , Elastic Load Balancing, and Route 53. In addition, the following provides high availability – two Availability Zones, Snapshots of EBS volumes, Elastic Load Balancing and Auto Scaling, Route 53 and EC2 Instances.

Compute Costs

Services | Estimate of your Monthly Bill ($ 1301.23)

Choose region: US-East / US Standard (Virginia)

Inbound Data Transfer is Free and Outbound Data Transfer is 1 GB free per re

Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides resizable compute capacity in the cloud. It is designed to make web-scale computi developers. Amazon Elastic Block Store (EBS) provides persistent storage to Amazon EC2 instances.

Compute: Amazon EC2 Instances:

Description	Instances	Usage	Type	Billing Option	Monthly Cost
NAT Servers	2	24 Hours/Day	Linux on t2.micro	3 Yr All Upfront Res	$ 0.00
Web Servers	20	24 Hours/Day	Linux on t2.medium	3 Yr All Upfront Res	$ 0.00
App Servers	16	24 Hours/Day	Linux on m4.2xlarge	3 Yr All Upfront Res	$ 0.00
Add New Row					

Storage: Amazon EBS Volumes:

Description	Volumes	Volume Type	Storage	IOPS	Snapshot Storage
Web Tier	2	General Purpose (SSD)	5 GB	15	3 GB-month of Storage
App Tier	2	General Purpose (SSD)	40 GB	120	35 GB-month of Storage
Add New Row					

Elastic IP:

Number of Additional Elastic IPs:	0	
Elastic IP Non-attached Time:	0	Hours/Month
Number of Elastic IP Remaps:	0	Per Month

Data Transfer:

Inter-Region Data Transfer Out:	0	GB/Month
Data Transfer Out:	0	GB/Month
Data Transfer In:	50	GB/Month
VPC Peering Data Transfer:	0	GB/Month
Intra-Region Data Transfer:	0	GB/Month
Public IP/Elastic IP Data Transfer:	0	GB/Month

Elastic Load Balancing:

Number of Elastic LBs:	2	
Total Data Processed by all ELBs:	500	GB/Month

Amazon S3 is storage for the Internet. It is designed to make web-scale computing easier for developers. Please check the Amazon S3 Storage Classes page det

Standard Storage:

Storage:	40	GB
PUT/COPY/POST/LIST Requests:	10000	Requests
GET and Other Requests:	1000	Requests

Standard - Infrequent Access Storage:

Storage:	0	GB
PUT/COPY/POST/LIST Requests:	0	Requests
GET and Other Requests:	0	Requests
Lifecycle Transitions:	0	Transitions
Data Retrieval:	0	GB

Reduced Redundancy Storage:

Storage:	0	GB
PUT/COPY/POST/LIST Requests:	0	Requests
GET and Other Requests:	0	Requests

Data Transfer:

Inter-Region Data Transfer Out:	0	GB/Month
Data Transfer Out:	10	GB/Month
Data Transfer In:	100	GB/Month

Amazon Route 53 is a highly available and scalable DNS service designed to give developers and businesses an extremely reliable and cost effective way to Internet applications. Amazon Route 53 charges are based on actual usage of the service in two areas: Hosted Zones and Queries. You pay only for mana through the service and the number of queries that the service answers.

Hosted Zones:

Hosted Zones:	1		
Standard Queries:	3	Per Month	Million Queries
Latency Based Routing Queries:	0	Per Month	Million Queries
Geo DNS Queries:	0	Per Month	Million Queries

DNS Failover Health Checks for endpoints:

Basic Checks Within AWS:	1000	Per Month
Basic Checks Outside of AWS:	500	Per Month
HTTPS Checks Within AWS:	0	Per Month
HTTPS Checks Outside of AWS:	0	Per Month
String Matching Checks Within AWS:	0	Per Month
String Matching Checks Outside of AWS:	0	Per Month
Fast Interval Checks Within AWS:	0	Per Month
Fast Interval Checks Outside of AWS:	0	Per Month

Amazon CloudFront is a web service for content delivery. It delivers your content using a global network of edge locations and works seamlessly with Amaz
durably stores the original, definitive versions of your files.

Data Transfer Out:

Monthly Volume: 80 GB/Month

Requests:

Average Object Size: 30 KB

Type of Requests: HTTP HTTPS

Invalidation Requests: 0 Requests

Edge Location Traffic Distribution:

United States	75	%
Europe	15	%
Hong Kong, Philippines, S. Korea, Singapore & Taiwan	0	%
Japan	0	%
South America	10	%
Australia	0	%
India	0	%

Dedicated IP SSL Certificates:

Number of Certificates: 0

Amazon RDS is a web service that makes it easier to set up, operate, and scale a relational database in the cloud. Cost calculation for Amazon Aurora i
check the pricing page for Amazon Aurora pricing details.

Amazon RDS On-Demand DB Instances:

	Description	DB Instances	Usage	DB Engine and License	Class and Deployment	Storage	PIOPS
	Add New Row						

Additional Backup Storage (Free backup storage up to 100% of provisioned Storage):

	Backup Storage
	100 GB-month of Storage
	Add New Row

Amazon RDS Reserved DB Instances:

	Description	DB Instances	Usage	DB Engine and License	Class and Deployment	Offering and Term	Storage	PIOPS
	MySQL	1	100 % Utilized/Mo	MySQL	db.m4.4xlarge Standard (Single-AZ) (	All Upfront 3 yr term	Provisioned 100 GB	1000
	Add New Row							

Data Transfer:

Inter-Region Data Transfer Out:	0	GB/Month
Data Transfer Out:	0	GB/Month
Data Transfer In:	50	GB/Month
Intra-Region Data Transfer:	0	GB/Month

Amazon DynamoDB is a high performance non-relational database service that is easy to set up, operate, and scale. It is designed to address the core management, performance, scalability, and reliability. It also provides predictable high performance and low latency at scale.

FREE TIER: Each month, Amazon DynamoDB users pay no charges on the first 25GB of storage, the first 2.5 million DynamoDB Streams read request units, as well as 25 writes/second and 25 reads/second of ongoing throughput capacity.

Indexed Data Storage:

Dataset Size: 100 GB

Provisioned Throughput Capacity *:

Item Size (All attributes): 1 KB

Number of items read per second: 10 Reads/Second

Read Consistency: (•) Strongly Consistent ( ) Eventually Consistent (2x cheaper)

Number of items written per second: 10 Writes/Second

DynamoDB Streams:

Read Request Units per month: 100 Units/Month

Data Transfer:

Data Transfer Out: 50 GB/Month

Data Transfer In: 50 GB/Month

Amazon ElastiCache is a web service that makes it easy to deploy, operate, and scale an in-memory cache in the cloud. It is protocol-compliant with Me code, applications, and tools that you use today with your existing Memcached or Redis environments work seamlessly with the service.

Cache Clusters: On-Demand Cache Nodes:

	Cluster Name	Nodes	Usage	Node Type
+	Add New Row			

Cache Clusters: Reserved Cache Nodes:

	Cluster Name	Nodes	Usage	Node Type	Offering and Term
−	Web Tier	2	100 % Utilized/Mo	cache.t2.micro	Heavy Utilization 3 yr term
+	Add New Row				

Amazon Simple Notification Service (Amazon SNS) is a web service that makes it easy to set up, operate, and send notifications from the cloud.

FREE TIER: Each month, Amazon SNS customers receive 1,000,000 Amazon SNS Requests, 100,000 HTTP notifications, 1,000 email notifications and 100 SMS notifications for free.

Requests And Notifications:

Requests: 1000 Requests

Notifications: 1000 HTTP/HTTPS

Data Transfer:

Data Transfer Out: 100 GB/Month

Data Transfer In: 100 GB/Month

Amazon Glacier is an extremely low-cost storage service that provides secure and durable storage for data archiving and backup. It is optimized for dat
accessed and for which retrieval times of several hours are suitable.

Storage

Storage:	100	GB

Requests:

UPLOAD and RETRIEVAL:	1000	Requests		
Data Retrieved:	10000	GB	Retrieval Period:	1 Month

Data Transfer:

Inter-Region Data Transfer Out:	0	GB/Month
Data Transfer Out:	50	GB/Month
Data Transfer In:	500	GB/Month

Amazon Virtual Private Cloud (Amazon VPC) is a secure and seamless bridge between a company's existing IT infrastructure and the AWS cloud.

VPN Connections

	Description	Number of Connections	Usage		Data Transfer Out		Data Transfer In	
	VPN to datacent	1	50	% Utilized/Mo	0	GB/Month	500	GB/Month
	Add New Row							