Final Project –AWS Cloud Architecting

1. Introduction
2. Executive Summary
3. Requirements & Assumptions
4. Architecture
5. Network & Security
6. Scalability, HA and Business Continuity
7. Monitoring and Auditing
8. Conclusion

Presented by - Team 8

Shreya Karakata
Richa Umesh Rambhia
Keith Medas

Introduction

Problem Statement:

A start-up software-as-a-service (SaaS) medical company has started an online medical social networking and diagnosis assistance application for its users mainly residing in the United States, Europe, and the APAC region. The company wants to use the cloud services for its new application once it is launched as the current environment is using a traditional server approach which proves time-consuming and costly.

Solution:

The project highlights the use of different AWS services to help the company control the anticipated growth after launching their new application and host the development, test, and production environments through AWS cloud infrastructure. Additionally covered are the features and solutions of topics including User Authentication, Network Security, Web & Application layers, Business Continuity, & Auditing.

Executive Summary

- The medical company currently uses an outdated method of leveraging physical resources such as servers and a hosting company to aid infrastructure development and testing of the production and development environments.
- The current architecture is divided into three tiers: the web layer, the application tier, and the database tier. If the resources demand an infrastructure upgrade, this strategy can become costly, time-consuming to manage, and challenging to perform modifications and upgrades to essential applications.
- The team will employ Amazon Web Services (AWS) to transition from the on-premise model to the cloud environment to meet customer needs.
- The requirements:
  1. High Availability
  2. Scalability
  3. Security
  4. Utilization of Load Balancers
  5. Supporting multiple locations

Requirements

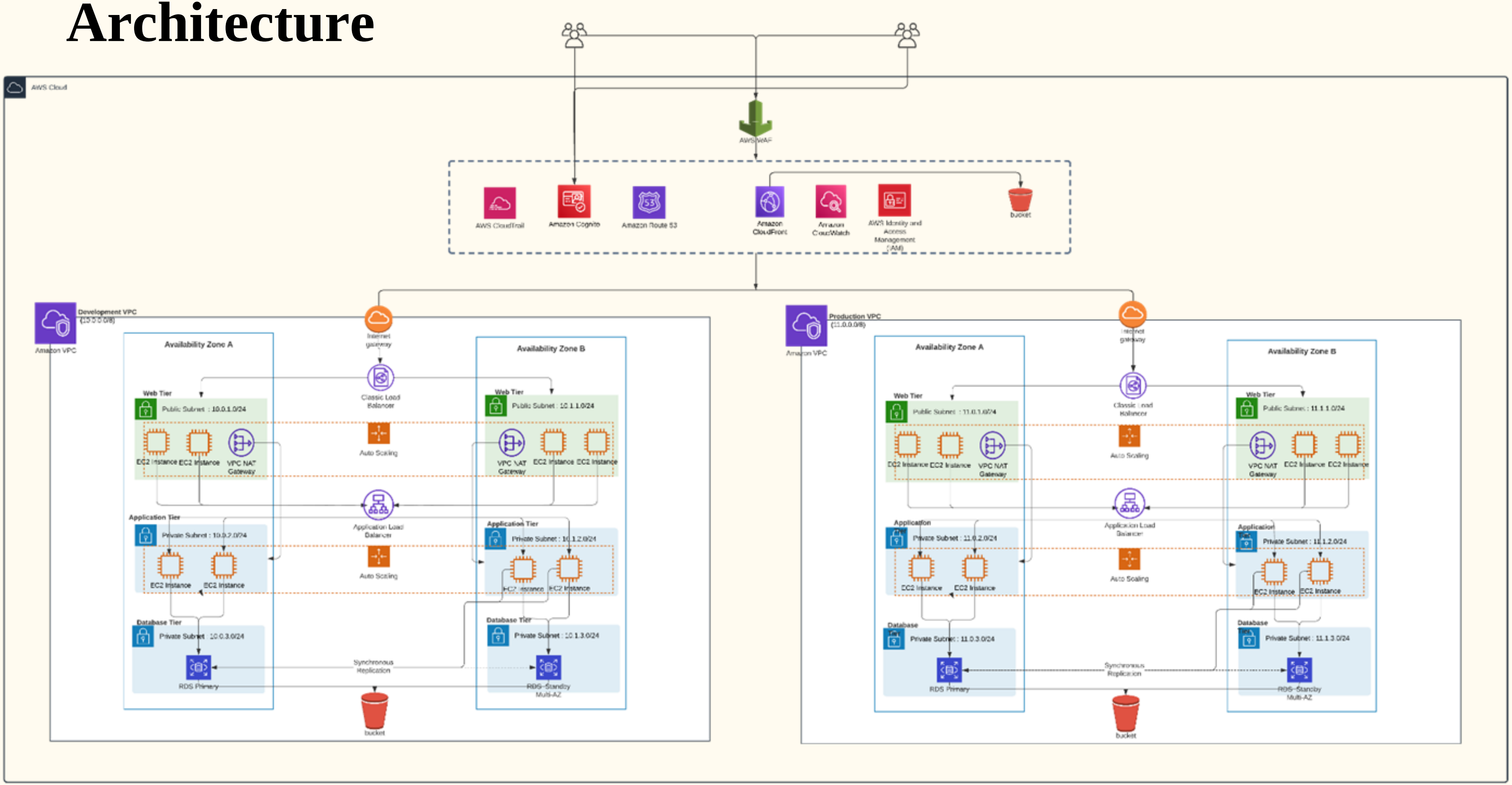
The overview of requirements:

1. High Availability
2. Scalability
3. Security
4. Utilization of Load Balancers
5. Supporting multiple locations

The detailed customer requirements are as follows:

1. Configuring access permissions to conform with AWS best practices.
2. Building networks that conform to AWS best practices while providing all the necessary network services to the application in their different environments.
3. Building an architecture that matches the current server hosting company's existing architecture can handle double the number of servers.
4. Securing all medical information, as medical information usually contains highly sensitive personally identifiable information (PII).
5. Utilizing load balancers for the web and application tiers that must support HTTP, HTTPS, and TCP protocols plans to move their application into AWS.

Architecture

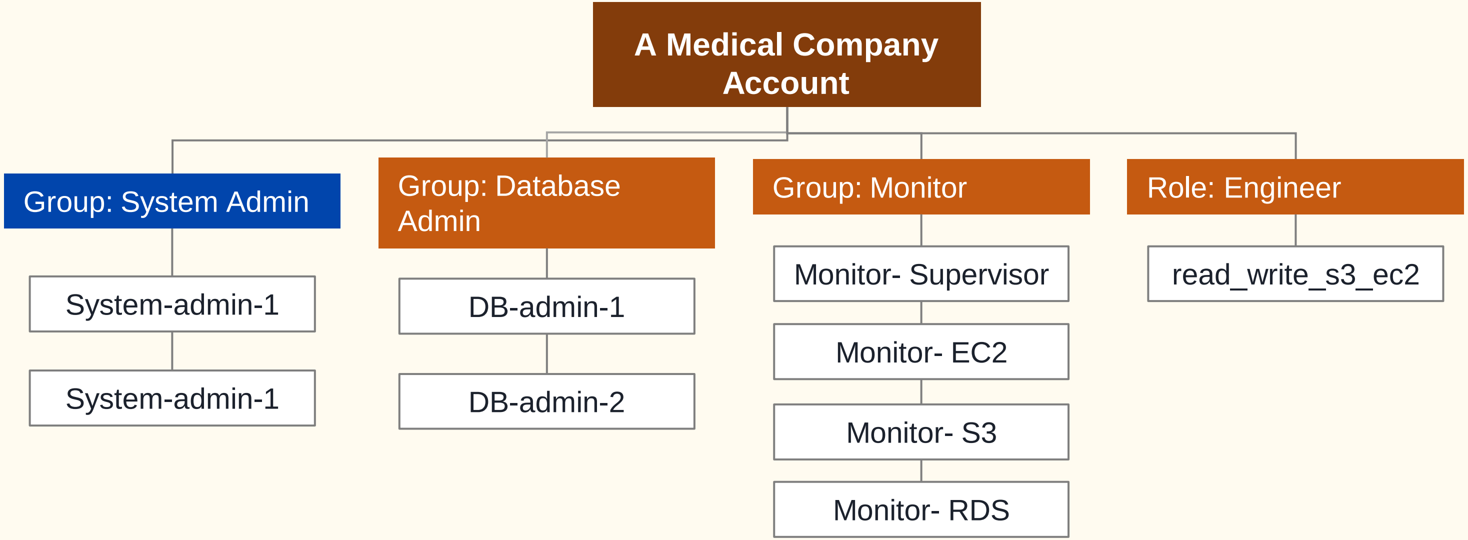


AWS Services

- AWS WAF (Web Application Firewall)
- AWS CloudTrail
- AWS Cognito
- AWS Route 53
- AWS CloudFront
- AWS CloudWatch
- AWS IAM (Identity and Access Management)
- AWS S3 (Simple Storage Service)
- AWS Classic Load Balancer
- AWS VPC (Virtual Private Cloud)
- AWS EC2 (Elastic Compute Cloud)
- AWS NAT Gateway
- AWS Auto Scaling Group
- AWS Application Load Balancer
- AWS RDS (Relational Database System)
- AWS Availability Zones

Users and Groups

The following are the groups and users created:



User Authentication

The groups and their associated roles are as follows:

Group/Role #	Group/Role Name	Permissions
Group	System Administrator	AWS Console Management Access Programmatic Access
Group	Database Administrator	AWS Console Management Access Programmatic Access
Group	Monitor	AWS Console Management Access
Role	read_write_s3_ec2	AWS Console Management Access

User Authentication

The following are the solutions for user authentication requirements:

Requirement	Solution
Should be at least 8 characters and have 1 uppercase, 1 lowercase, 1 special character, and a number.	Checking the following in IAM Password Policy: ➔ Enforce password minimum length : 8 characters ➔ Require at least one uppercase letter ➔ Require at least one lowercase letter ➔ Require at least one number ➔ Require at least one non-alphanumeric character
Change passwords every 90 days and ensure that the previous three passwords can't be re-used.	Checking the following in IAM Password Policy: ➔ Enable password expiration : 90 days ➔ Prevent password reuse : 3
All administrators require programmatic access	Give administrator groups programmatic access through IAM groups
Administrator sign-in to the AWS Management Console requires the use of Virtual MFA.	Enable virtual MFA for administrator groups

Network and Security

The VPC and Subnet details for each VPC are as follows:

VPC	Region	Purpose	Subnets (Each AZs)	AZs	CIDR Range
1	us-east-1	Development	1 public (web tier) 2 private(app and db tier)	use1-az1 use1-az2	10.0.0.0/8
2	us-east-1	Production	1 public (web tier) 2 private(app and db tier)	use1-az1 use1-az2	11.0.0.0./8

Development VPC

Subnet Name	VPC	Subnet Type (Public/private)	AZ	Subnet Address
dev_web_pub_1	#1	Public	1	10.0.1.0/24
dev_web_pub_2	#1	Public	2	10.1.1.0/24
dev_app_priv_1	#1	Private	1	10.0.2.0/24
dev_app_priv_2	#1	Private	2	10.1.2.0/24
dev_db_priv_1	#1	Private	1	10.0.3.0/24
dev_db_priv_2	#1	Private	2	10.1.3.0/24

Network and Security

Production VPC

Subnet Name	VPC	Subnet Type (Public/private)	AZ	Subnet Address
prod_web_pub_1	#2	Public	1	11.0.1.0/24
prod_web_pub_2	#2	Public	2	11.1.1.0/24
prod_app_priv_1	#2	Private	1	11.0.2.0/24
prod_app_priv_2	#2	Private	2	11.1.2.0/24
prod_db_priv_1	#2	Private	1	11.0.3.0/24
prod_db_priv_2	#2	Private	2	11.1.3.0/24

Web, Application and Database Tier

The following are the type and size of instances in each tier

Tier	Tag*	OS	Type	Size	Justification	# of instances	User Data?
Web	Key = Name Value = web-tier	MS Windows 2016	t3 medium	4 GB Memory	For the size and it is required for a high network performance	2	Yes
App	Key = Name Value = app-tier	MS Windows 2016	t3 large	16 GB Memory	For the size and it is required for a high network performance and less interference	2	Yes
DB	Key = Name Value = db-tier	MS Windows with SQL server SE	db.t3 3x large	32 GB Memory, 5TB Storage	For the size and to support all on-demand services	1	No

Web, Application and Database Tier

The following gives information about the load balancer and security groups

Load Balancer	Name*	External/ Internal	Subnets	SG Name*	Rule	Source
For Web Tier	web-elb	External	prod_web_pub_1 prod_web_pub_2	web-elb-sg	Inbound port 80 and 443	80 (Internet)
For App Tier	app-elb	Internal	prod_app_priv_1 prod_app_priv_2	app-elb-sg	Inbound port 8080	8080 (Web Tier)

Instance Tier	SG Name*	Rule	Source
Web Tier	web-tier-sg	Inbound port 80 Receives requests from web tier load balancer	web-elb
App Tier	app-tier-sg	Inbound port 80 Receives requests from application tier load balancer	app-elb
Database Tier	db-tier-sg	Inbound port 1433 Receives requests from application tier	App Tier

Business Continuity

The following are the autoscaling details:

Tier	OS	Type	Size	Configuration Name*	Role	Security Group
Web	Microsoft Windows	(t3) medium	4 CPU , 8 GB	WebTier	read_write_s3_ec2	System admin
App	Microsoft Windows	(t3) xlarge	6 CPU , 32 GB	AppTier	read_write_s3_ec2	System admin

Tier	Launch Configuration*	Group Name*	Group Size	VPC	Subnets	ELB	Tags
Web	WebTier	WebTier	Min : 2 Max 4	Production	prod_web_pub_1 prod_web_pub_2	web-elb	Key =Name Value =web-tier
App	AppTier	AppTier	Min : 2 Max 4	Production	prod_app_priv_1 prod_app_priv_2	app-elb	Key =Name Value =app-tier

Auditing & Next Steps

When Auditing AWS it is recommended to do the following:

- Secure IAM : IAM is frequently over-privileged, therefore we want to ensure that we have a sound plan for dealing with it. (Shadow IT)
- AWS Cloud Trail: Audit logs are critical for spotting unusual occurrences and understanding what happened after an event. CloudTrail is essentially an auto-log of every action that occurs in AWS.
- AWS Cognito: Amazon Cognito helps to quickly and easily add user sign-up, user sign-in, and access control to your online and mobile apps.
- VPC Logs: Data regarding network traffic in VPC is captured and logged using VPC Flow logging.
- AWS Config: AWS Config offers an inventory of AWS resources, a history of configurations, and alerts of configuration changes to facilitate security and control.
- Next steps:
  - Add more security controls.
    - Guard Duty- Amazon Guard Duty helps with analyzing your entire AWS environment for potential threats.
    - Inspector-Amazon Inspector provides you with security assessments of your applications settings and configurations on your EC2 instances

Conclusion

- This design is built considering the best practices for the AWS architecture.
- The cloud solution architecture is designed to help the Startup shift from on-premises architecture to AWS cloud infrastructure and to meet client requirements such as high availability, scalability, security, load balancing, and support for many locations.
- We have also implemented other necessary requirements including:
  - the usage of virtual MFA
  - 16 character password policy.
  - The usage of multiple zone server deployment also ensures that the application is fault-tolerant and resilient.
  - Private subnetting to maintains the confidentiality of sensitive information.
- AWS-related operations made on the infrastructure will also be tracked and audited by the administrators.

Thank You