Northeastern University

ITC6480 - AWS Cloud Architecting
Winter 2023 CPS

Final Project Report
By
Group – 8

Venkata Sasank Jonnalagadda

Phanindra Raja Varma Gadiraju

Sai Sruthi Kalidindi

Instructor - Carmen Taglienti

Introduction

For startups, using traditional servers to host the medical application can be expensive, time-consuming, and inflexible. Traditional servers have high upfront costs for hardware and maintenance, which can be prohibitively expensive for a startup. Furthermore, scaling traditional servers to meet increased user demand can be difficult because it necessitates the purchase of additional hardware and upgrades. Cloud services, on the other hand, provide a pay-as-you-go model, allowing the company to only pay for what they require, making it both cost-effective and scalable.

Secondly, the medical application requires a high level of performance and reliability to ensure patient data security and accurate diagnoses. Traditional servers are prone to outages and other performance issues, which can result in downtime and data loss. By leveraging the cloud provider's high-performance infrastructure, the company can ensure that the application is always available and running efficiently.

Finally, as the company grows and its user base expands, it will need to be able to efficiently store and process large amounts of data. Large amounts of data on traditional servers can quickly overwhelm them, resulting in slow performance and other issues. Cloud services enable the storage and processing of large amounts of data, ensuring that the medical application can continue to provide high-quality service to its users as it grows.

In conclusion, migrating to cloud services is a wise decision for the medical software as a service company. It will enable the company to cut costs, improve performance and reliability, and scale the application as necessary.

Solution

The project's primary goal is to create an AWS architecture for the medical company that meets its future needs. Because the application handles sensitive documents and financial transactions, security is an important consideration when designing the architecture. In addition, multiple environments, such as Test/Dev and Production, must be deployed in the AWS environment. To meet these requirements, AWS provides a variety of services that can be used to improve application performance while ensuring data security.

AWS offers a variety of security services, such as identity and access management, encryption, and threat detection, that can be used to safeguard sensitive data. Using AWS CloudFormation, which can help automate deployment and configuration management, you can also use multiple environments. Furthermore, the company can achieve high availability, scalability, and reliability for its application by utilizing services such as Amazon RDS and Amazon S3.

Overall, AWS can provide a secure, scalable, and cost-effective solution for the medical company's application needs. The company can ensure that its application performs optimally and that patient data is secure by leveraging the many AWS services available.

Executive Summary

The medical company is currently utilizing physical resources such as servers and a hosting company to aid infrastructure development and testing of the production and development environments, which is an outdated method. There are three tiers in the architecture: the web layer, the application tier, and the database tier. However, expanding these to meet future needs would not be cost-effective and would necessitate significant resources.

To address these issues, the team decided to transition from traditional on-premise servers to AWS cloud services. As a result, the company will be able to scale the infrastructure to meet future demands while also providing an excellent customer experience. The migration will also help the company save money by removing the need for physical hardware and associated maintenance costs. AWS cloud services offer a variety of scalable and secure infrastructure services, including Amazon EC2, Amazon RDS, and Amazon S3, that can be used to meet the company's needs.

Migrating to AWS cloud services will provide the medical company with the infrastructure it needs to meet future needs, reduce costs, and improve customer experience. It will also assist the company in remaining competitive in the industry by keeping up with the latest technological trends.

Overall Requirements and Assumptions

The architecture for the medical company's production and development VPCs will be consistent across all regions, with consistent services and components. However, specific implementation details may differ depending on the unique requirements and constraints of each region. This allows the medical company to ensure that its application is performant, secure, and scalable across all regions.

While the architecture of both the production and development VPCs may be similar, the resources allocated to each environment in the real-world scenario may differ slightly. These distinctions may be required to meet the unique requirements of each environment, such as scaling requirements or performance optimization.

Below are the few major requirements by the company

- High Availability
- Scalability
- Security
- Utilization of Load Balancers
- Supporting multiple locations

Solution – Identifying AWS Services

A number of AWS services were used in the architecture designed for the medical company to meet the company's specific requirements. AWS WAF for web application firewall, AWS CloudFront for content delivery, AWS CloudWatch for monitoring, AWS IAM for identity and access management, AWS S3 for storage, AWS Classic Load Balancer for load balancing, AWS CloudTrail for logging and auditing, AWS Route 53 for DNS management, AWS Availability Zones for high availability, AWS Application Load Balancer for application load balancing

The architecture can provide high availability, scalability, security, and load balancing across multiple locations by leveraging AWS services, while also supporting the needs of the medical company's users and ensuring the application remains performant and reliable. Each of these services has been carefully chosen and configured to meet the medical company's specific needs, ensuring that the architecture remains cost-effective and efficient while also meeting the high security and compliance standards required for handling sensitive medical data.

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

Solution – User Authentication

As part of the IAM policies, we have created 4 different groups and each of these groups have different permissions.

Below are the list of 4 groups:

- System Admin
- Database Admin
- Monitoring
- Engineer

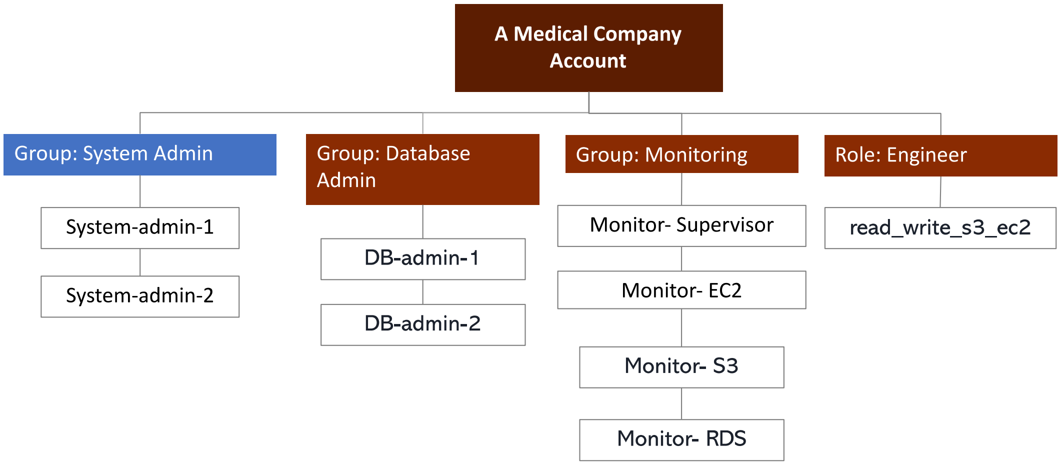
Now let us look into the significance of these groups and how many users are assigned in respective groups.

System Admin: This group is like a superior group, as the members of this groups will be given access to both AWS management console and programmatic access. In our project we are assigning 2 people to this group (System-admin-1 and System-admin-2)

Database Admin: This group majorly concentrates on the operations of the RDS databases, from loading the data to storing and monitoring the data. In our project we are assigning 2 people in to this group (DB-admin-1 and DB-admin-2)

Monitoring: As stated above, we have used wide range of services in our architecture and its our responsibility to monitor those services and understand how the application is performing. It not only helps to understand how it is performing, but also helps us to take necessary actions on the services when required. In our project, we have assigned 4 different users for monitoring 4 different areas i.e Monitor-Supervisor, Monitor-EC2, Monitor-S3 and Monitor-RDS

Engineer: This group of users will have read and write access to the RDS and S3. In our project, we have allocated one such engineer who have the access to read and write in both S3 and RDS.



The groups and their associated permissions

Group/Role #	Group/Role Name	Permissions
Group	System Administrator	AWS Console Management Access Programmatic Access
Group	Database Administrator	Manages and monitors RDS databases
Group	Monitor	Monitors the functioning of various AWS services such as EC2, RDS, and S3
Role	Engineer	Read/Write permissions to S3 and RDS

The following are the solutions for user authentication requirements

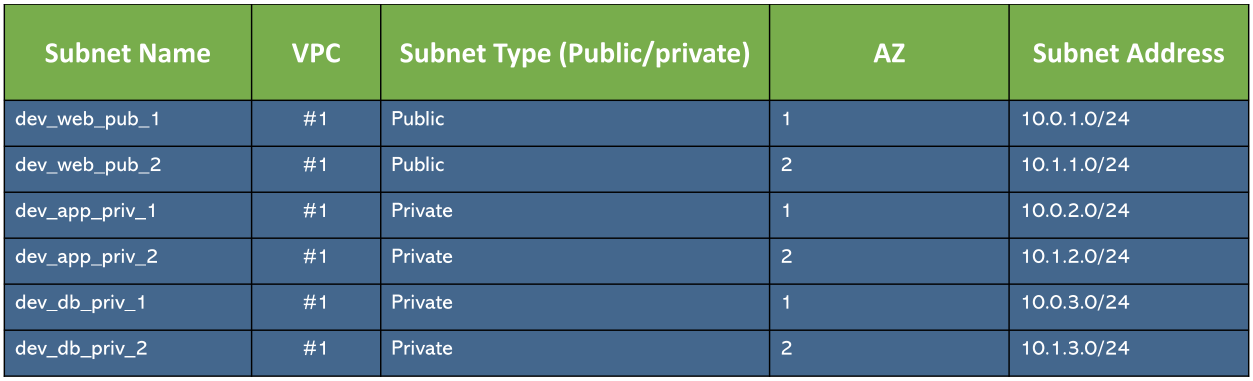
Requirement	Solution
Should be at least 8 characters and have 1 uppercase, 1 lowercase, 1 special character, and a number.	Checking the following in IAM Password Policy: ➔ Enforce password minimum length : 8 characters ➔ Require at least one uppercase letter ➔ Require at least one lowercase letter ➔ 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

Solution – Network and Security

The VPC and Subnet details for each VPC are as follows

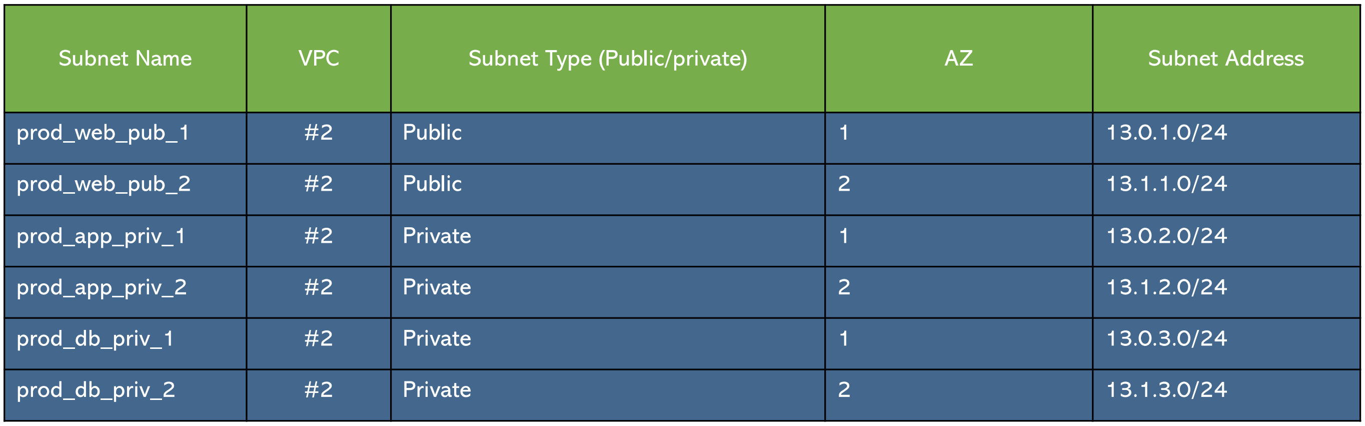
VPC	Region	Purpose	Subnets	AZs	CIDR Range
1	us-east-1	Development	1 public (web tier) 2 private(app and db tier)	use1-az1 use1-az2	10.0.0.0/16
2	us-east-1	Production	1 public (web tier) 2 private(app and db tier)	use1-az1 use1-az2	13.0.0.0./16

Development VPC



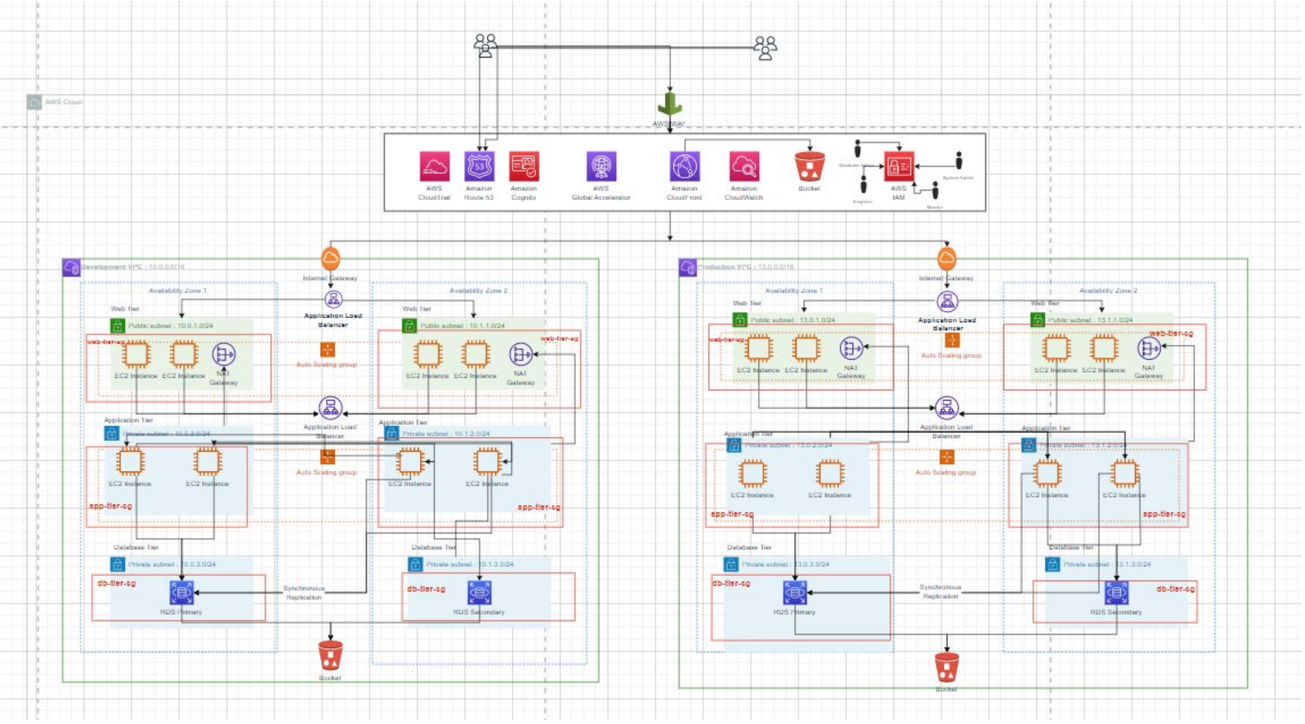
Subnet Name	VPC	Subnet Type (Public/private)	AZ	Subnet Address
dev_web_pub_1	#1	Public	1	10.0.1.0/24
dev_web_pub_2	#1	Public	2	10.1.1.0/24
dev_app_priv_1	#1	Private	1	10.0.2.0/24
dev_app_priv_2	#1	Private	2	10.1.2.0/24
dev_db_priv_1	#1	Private	1	10.0.3.0/24
dev_db_priv_2	#1	Private	2	10.1.3.0/24

Production VPC



Subnet Name	VPC	Subnet Type (Public/private)	AZ	Subnet Address
prod_web_pub_1	#2	Public	1	13.0.1.0/24
prod_web_pub_2	#2	Public	2	13.1.1.0/24
prod_app_priv_1	#2	Private	1	13.0.2.0/24
prod_app_priv_2	#2	Private	2	13.1.2.0/24
prod_db_priv_1	#2	Private	1	13.0.3.0/24
prod_db_priv_2	#2	Private	2	13.1.3.0/24

Architecture Diagram


AWS Cloud
AWS WAF
AWS CloudTrail
Amazon Route 53
Amazon Cognito
AWS Global Accelerator
Amazon CloudFront
Amazon CloudWatch
Bucket
Database Admin
Engineer
AWS IAM
System Admin
Monitor
Development VPC : 10.0.0.0/16
Internet Gateway
Availability Zone 1
Availability Zone 2
Application Load Balancer
Web Tier
Public subnet : 10.0.1.0/24
Public subnet : 10.1.1.0/24
web-tier-sg
EC2 Instance
NAT Gateway
Auto Scaling group
Application Tier
Private subnet : 10.0.2.0/24
Private subnet : 10.1.2.0/24
app-tier-sg
Database Tier
Private subnet : 10.0.3.0/24
Private subnet : 10.1.3.0/24
db-tier-sg
RDS Primary
RDS Secondary
Synchronous Replication
Bucket
Production VPC : 13.0.0.0/16
Public subnet : 13.0.1.0/24
Public subnet : 13.1.1.0/24
Private subnet : 13.0.2.0/24
Private subnet : 13.1.2.0/24
Private subnet : 13.0.3.0/24
Private subnet : 13.1.3.0/24

Solution – Web and Application 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	medium	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	x large	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	2x large	For the size and to support all on-demand services	1	No

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	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	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

Solution – 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	Engineer	System admin
App	Microsoft Windows	(t3) xlarge	6 CPU , 32 GB	AppTier	Engineer	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 and Next Steps

Below are the list of services that are utilized in the our architecture for auditing purpose

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.

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.

Secure IAM: IAM is frequently over-privileged, therefore we want to make sure that we have a sound plan for dealing with it.

AWS Config: AWS Config offers an inventory of AWS resources, a history of configurations, and alerts of configuration changes to facilitate security and control.

Besides from the previously mentioned AWS services, the architecture designed for the medical company also makes use of AWS Trusted Advisor, Amazon SNS, and Guard Duty.

AWS Trusted Advisor is a service that provides recommendations to optimize your AWS environment's performance, security, and cost. It can identify areas for improvement in the architecture by analyzing it on a regular basis, such as lowering costs, increasing availability, and improving security. This enables the medical firm to continuously improve its architecture and ensure that it remains optimized over time.

SNS (Simple Notification Service) by Amazon is a messaging service that allows businesses to send direct customer notifications via email, mobile push notifications, and SMS text messaging. This enables the medical company to quickly and easily send notifications to its users, keeping them informed of important updates or changes to their account or the application.

Guard Duty is an AWS service that assists in the detection of potential threats throughout the AWS environment. It continuously monitors and processes logs and network traffic, detecting suspicious activity with machine learning and threat intelligence. This aids in the detection of potential security threats and their prevention of damage or data breaches. The medical company can use Guard Duty to ensure that its architecture is secure and protected from cyber threats.

Conclusion:

The AWS architecture created for the medical firm follows best practices to ensure high availability, scalability, security, load balancing, and support for multiple locations. This architecture is intended to assist the company in transitioning from on-premises to AWS cloud infrastructure while meeting customer requirements.

We have implemented virtual MFA and a 16-character password policy to ensure security. We also used multiple zone server deployment to create a fault-tolerant and resilient architecture. Private subnetting is used to protect sensitive information from prying eyes. Administrators will also track and audit AWS-related operations performed on the infrastructure to ensure that the system is secure and compliant with regulatory requirements.

Overall, the architecture has been designed to meet the specific needs of the medical company, including high availability, scalability, security, and load balancing. With this architecture, the company can benefit from the advantages of cloud infrastructure while also ensuring the security and compliance of its applications and data.