**AWS Cloud Infrastructure Solution for MedCo**

Brandon Luff and Benjamin Gaudlip

Robert Morris University

INFS 4460: Cloud Computing and AWS

Professor Al-Jaroodi

November 6, 2023



Table of Contents

Introduction ……………................................................................................................. 3

1. Architectural Design .................................................................................................... 4

1.1 Overview of the Proposed Architecture ................................................................ 4

1.2 Resilience and High Availability ........................................................................... 4

1.3 Scalability .............................................................................................................. 4

1.4 Network Services and Infrastructure Design ......................................................... 4

1.5 Instance Configuration ........................................................................................... 5

1.6 Resource Tagging and Management Strategy ........................................................ 5

1.7 Scalable Architecture ............................................................................................. 6

2. Security and Compliance ............................................................................................. 7

2.1 Security Groups and Network ACLs ..................................................................... 7

2.2 Identity and Access Management (IAM) ............................................................... 7

2.3 AWS WAF and Firewall Manager .......................................................................... 7

2.4 Data Encryption with AWS KMS .......................................................................... 7

3. Monitoring and Auditing .............................................................................................. 7

3.1 AWS CloudTrail ..................................................................................................... 7

3.2 AWS Config ............................................................................................................ 7

3.3 Amazon CloudWatch .............................................................................................. 8

4. Cost Management ......................................................................................................... 8

4.1 Cost Breakdown ...................................................................................................... 8

4.2 Cost Optimization Measures ................................................................................... 8

4.3 Sustainability .......................................................................................................... 8

4.4 Integration for Comprehensive Oversight ……………………………………….. 8

5. Conclusion and Lessons Learned .................................................................................. 8

5.1 Summary of Proposed Solution's Benefits .............................................................. 9

5.2 Discussion on the Adoption of the Solution ............................................................ 9

5.3 Reflection on the Lessons Learned .......................................................................... 9

Appendix A ....................................................................................................................... 10

Appendix B ....................................................................................................................... 11

Figures .............................................................................................................................. 12

References ........................................................................................................................ 13

**Introduction**

In the rapidly advancing field of healthcare technology, MedCo has initiated a pivotal shift to capitalize on the benefits of cloud computing. This strategic move is anchored in deploying a cloud infrastructure that aligns with the medical industry's cutting-edge requirements and reflects MedCo's dedication to robust and flexible operations. This report captures the essence of our strategy, which entails leveraging Amazon Web Services (AWS), a platform that stands out for its ease of use, flexibility, and unwavering reliability—qualities imperative in the healthcare domain.

AWS's design is inherently accommodating, allowing MedCo to host their existing applications and develop new SaaS solutions swiftly and securely. This agility in hosting services is crucial for MedCo, as it provides the freedom to tailor the software and services environment according to specific application needs. This flexibility is further demonstrated by AWS's ability to streamline the migration process for MedCo's existing applications, ensuring business continuity while offering the versatility to innovate.

Regarding financial strategy, AWS's cost-effective model is particularly appealing. By incurring costs only for the computing power, storage, and resources used and without the burden of long-term contracts or upfront investments, MedCo can maintain financial agility. This pay-as-you-go approach aligns with MedCo's cost optimization and operational scalability commitment.

Reliability is paramount in healthcare, where system downtime can have critical implications. AWS's reputable and secure global computing infrastructure, which forms the backbone of Amazon's vast online enterprise, provides MedCo with a proven platform refined over a decade. The robustness of AWS infrastructure assures that MedCo's services are always on and always available, a non-negotiable requirement in the medical field.

Further enhancing this infrastructure's capabilities are AWS's scalability and high-performance computing tools, such as Auto Scaling and Elastic Load Balancing. These tools ensure that MedCo's applications remain responsive to the fluctuating demands of healthcare delivery, scaling effortlessly and maintaining performance standards that healthcare professionals and patients expect.

Lastly, protecting sensitive health data is a top concern for MedCo. AWS's comprehensive security measures, encompassing physical, operational, and software facets, ensure an end-to-end fortified architecture. This level of security is critical for protecting patient information and underpins the essential trust between MedCo and its stakeholders.

As we explore MedCo's cloud architecture in subsequent sections, these attributes of AWS form the foundation of our design and decision-making processes. This introduction sets the stage for a detailed discussion of how MedCo's cloud solution, powered by AWS, not only achieves the operational, financial, and ethical benchmarks but is also designed with the future in mind—adaptable, cost-effective, and uncompromisingly secure.

**Proposal Outline**

1. **Architectural Design**

1.1 Overview of the Proposed Architecture

Our team has architected a multi-tier cloud solution for MedCo that is robust, secure, and scalable. The web tier, running on Amazon EC2 instances and orchestrated by an Elastic Load Balancer (ELB), efficiently manages client interactions, and maintains high availability. The application tier, also on EC2, handles business logic and interfaces with the RDS-hosted database tier, leveraging RDS's high durability and Multi-AZ failover capabilities.

1.2 Resilience and High Availability

To assure resilience and high availability, we have implemented Multi-AZ deployments for critical systems such as the RDS database tier, thus avoiding single points of failure. ELBs are essential in our load-balancing strategy, optimizing resource utilization and providing fault tolerance.

1.3 Scalability

We have enabled Auto Scaling for EC2 instances, which allows MedCo's infrastructure to scale resource allocation automatically in response to fluctuating demand, ensuring cost optimization and consistent performance.

Configuring Access Permissions and Policies:

A robust identity and access management (IAM) system establishes secure MedCo's AWS resources, creating specific user groups and roles for varying operational needs:

* Group 1: System Admin - Provides full administrative access for comprehensive AWS management.
* Group 2: DB Admin - Grants full access to manage Amazon RDS databases.
* Group 3: Monitoring - Offers read-only access for monitoring purposes, ensuring integrity while enabling oversight.
* Role 1: EC2 Application - Allows read/write access to a designated S3 bucket for data handling.

Our security approach includes a stringent password policy, requiring complexity and regular changes, with multi-factor authentication (MFA) safeguarding administrator console access.

1.4 Network Services and Infrastructure Design

Availability and Continuity:

We have architected MedCo's AWS infrastructure to span two Availability Zones, reinforcing business continuity and resilience. This strategic layout allows for uninterrupted operations, as traffic can be rerouted automatically to a secondary zone should the primary encounter any issues, thereby ensuring MedCo's operations are robust against disruptions.

Public and Private Subnets:

The EC2 instances within the public subnets use the Elastic Load Balancers (ELBs) to manage, which proficiently distribute incoming web traffic and provide defense against unexpected traffic surges. In tandem with Auto-Scaling, the infrastructure can dynamically adjust, scaling resources per the fluctuating load and optimizing both performance and cost.

The application layer, housed within private subnets, benefits from enhanced security due to its isolation from direct internet access. However, it remains up-to-date and functional through NAT gateways, which facilitate necessary external communication. Auto-scaling also applies here, ensuring the application layer is resilient and responsive to demand.

Database Management:

Amazon RDS is also nestled within these private subnets, taking advantage of Multi-AZ deployment for database high availability. Data replication to Amazon Simple Storage Service (S3) is configured to provide robust and reliable data backup solutions, safeguarding MedCo's critical data assets.

Monitoring and Management:

The entire operation is under the vigilant eye of Amazon CloudWatch, which offers detailed monitoring capabilities. This allows for a proactive stance in operational management, enabling quick responses to any changes or anomalies in system performance.

Adherence to AWS Well-Architected Framework:

Our infrastructure design follows the principles of the AWS Well-Architected Framework, ensuring that MedCo benefits from a secure, high-performing, and cost-efficient cloud environment. By leveraging AWS best practices, we provide a solution that meets today's needs and is scalable for future growth.

1.5 Instance Configuration

Web Tier: MedCo's proposed web tier has two T3a.medium EC2 instances, each equipped with two vCPUs and four GiB RAM. This setup can handle moderate web traffic efficiently, with the provision to scale out using auto-scaling if the demand increases.

Application Tier: The application tier can handle more intensive computing and memory requirements with two M4.XLarge EC2 instances. Each instance provides four vCPUs and sixteen GiB RAM, offering a balanced set of resources to support the application servers requiring more CPU and memory than the web servers.

Database Tier: The database tier consists of a single i3en.2XLarge EC2 instance that includes eight vCPUs, sixty-four GiB RAM, and five TB of SSD storage. This choice is due to the i3en. 2XLarge's optimization for low latency, high random I/O performance, and high sequential disk throughput makes it an ideal solution for database workloads that demand the fastest access to storage with the most cost-effective pricing per GB on Amazon EC2.

These instance configurations are fundamental to ensuring that each tier of MedCo's architecture is optimized for its specific workload, providing a scalable and robust infrastructure to support the company's services.

1.6 Resource Tagging and Management Strategy

In constructing MedCo's AWS architecture, we have implemented a systematic approach to resource tagging using clear and consistent key-value pairings. This method streamlines resource management and enhances the efficiency of monitoring and automation workflows.

Windows Server OS Unification: All levels of our infrastructure—the Web, Application, and Database tiers—operate on the Windows Server OS platform. This uniformity across tiers promotes operational coherence and provides a stable and familiar environment for MedCo's application ecosystem.

Web Tier Tagging: We have designated the Web Tier with two key-value pairs: 'WebTier1' and 'WebTier2', each tied to the 'web-tier' value. This tagging schema is essential for categorizing instances that manage the user-facing components and front-end operations of MedCo's applications, facilitating targeted scaling and maintenance activities.

Application Tier Tagging: We employ keys' AppTier1' and 'AppTier2' for the Application Tier, tagged with 'app-tier'. This allows us to pinpoint the instances dedicated to processing business logic, differentiating them for operational management, such as scaling policies and system updates.

Database Tier Tagging: The Database Tier is labeled with the key 'DBTier1', associated with the 'db-tier' value. This tag is particularly critical for identifying the instances that handle data storage and retrieval functions—the linchpin of MedCo's service reliability and performance.

Operational Benefits: Our key-value pairing strategy provides a robust framework for an organized AWS environment. It ensures that resources are easily identifiable and manageable, vital for maintaining MedCo's complex cloud infrastructure. Moreover, it allows for precise control and quick identification in automated scripts and policies, significantly reducing the overhead of managing a large-scale cloud presence.

Our resource tagging approach aligns with AWS best practices, offering MedCo a scalable, manageable, and transparent infrastructure setup that supports its operational demands and growth trajectory.

1.7 Scalable Architecture

MedCo's AWS deployment is engineered with scalability as a focal point, accommodating the company's dynamic growth and fluctuating traffic patterns.

Auto Scaling Groups (ASGs): ASGs are pivotal in our design, applied to both the web and application layers. These groups enable MedCo's infrastructure to dynamically scale the EC2 instances up or down, aligning with the demand. This elasticity preserves performance under varying load conditions and enhances cost efficiency by matching resource utilization with actual needs.

Amazon RDS with Multi-AZ and Read Replicas: We have opted for Amazon RDS to handle our database needs, employing a Multi-AZ setup for maximum availability and automatic failover. Additionally, using read replicas offloads the read operations from the primary database, thereby speeding up data retrieval and effectively handling high-volume user queries.

Elastic Load Balancing (ELB): Our load balancing strategy involves ELB, which includes an Application Load Balancer (ALB) for managing HTTP/HTTPS traffic. The ALB ensures the smooth operation of web transactions by distributing incoming traffic across multiple targets, improving the web tier's scalability and security. We employ the Network Load Balancer (NLB) for TCP traffic, which is renowned for its high throughput and ability to handle volatile traffic patterns.

Amazon S3 for Data Storage and Management: Amazon S3 provides a comprehensive and secure data storage solution for MedCo. Beyond mere data storage, S3 offers advanced features like lifecycle policies and versioning, which safeguard data integrity and optimize storage costs. These features enable intelligent data management, allowing for automated archiving or deleting of outdated objects, thereby maintaining data relevance, and reducing expenditure.

With this combination of scalable services, MedCo's infrastructure is positioned to meet current operational demands while maintaining the agility to expand effortlessly in line with the company's trajectory. Our approach ensures that MedCo can continue to deliver its services reliably and efficiently, regardless of scale.

1. **Security and Compliance**

A paramount aspect of MedCo's cloud deployment is its security posture and adherence to compliance standards. The architecture incorporates multiple security measures to protect data, manage access, and secure applications.

2.1 Security Groups and Network ACLs: Within the VPC, we configure security groups as virtual firewalls for EC2 instances, defining which traffic is permitted to and from the servers. Each tier—web, application, and database—has its dedicated security group with rules tailored to the minimum necessary access, ensuring that instances are not exposed to unnecessary risks.

Network Access Control Lists (ACLs) act as an added layer of security at the subnet level, providing stateless filtering of incoming and outgoing traffic. We strategically configure ACLs to block unwanted traffic, mitigating risks from potential network-based attacks.

2.2 Identity and Access Management (IAM): IAM is pivotal in managing user access within MedCo's AWS environment. We have established comprehensive policies and roles that govern users' and systems' actions, minimizing the risk of unauthorized access. By adhering to the principle of least privilege, we ensure that users only have access to the resources essential for their role.

2.3 AWS WAF and Firewall Manager: AWS Web Application Firewall (WAF) protects MedCo's web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources. AWS Firewall Manager simplifies the administration of firewall rules across the organization, ensuring consistent enforcement of security policies.

* 1. Data Encryption with AWS KMS: AWS Key Management Service (KMS) manages cryptographic

keys for data encryption, providing MedCo with control over encryption across the AWS services. All sensitive data, at rest or in transit, is encrypted using keys managed by KMS, which integrates with other AWS services to facilitate seamless encryption while maintaining high security and compliance standards.

1. **Resilient Architecture**

The architecture at the core of MedCo's cloud infrastructure is engineered for resilience to ensure uninterrupted, robust, and efficient service delivery.

3.1 Multi-AZ Deployments: MedCo's AWS deployment leverages Multi-AZ Deployments for essential services such as Amazon RDS databases and critical EC2 instances. We ensure high availability by maintaining active replicas of these services in separate regional locations. In the event of a zone failure, the system is architected to facilitate automatic failover to a standby zone, thereby minimizing service interruption and maintaining operational continuity.

3.2 Content Delivery with Amazon CloudFront: MedCo's web content is delivered with enhanced efficiency and reduced latency through Amazon CloudFront. This global content delivery network (CDN) strategically caches content at edge locations nearest to users, significantly improving load times and user experience. CloudFront's expansive network is optimized for high-speed data transfer and immediate content delivery, providing a swift and seamless user experience regardless of geographic location.

3.3 DNS Management with Amazon Route 53: An essential component of our resilient architecture is practical DNS management, accomplished using Amazon Route 53. This scalable and highly available DNS service routes user requests to MedCo's internet applications with reliability and precision. Route 53, designed to provide businesses and developers with a dependable method to connect user requests to infrastructure running in AWS, can be adjusted in response to real-time conditions.

Through the strategic implementation of these AWS services, MedCo's infrastructure is safeguarded against outages and primed for optimal performance. The result is a robust architecture that ensures MedCo's users enjoy consistent access to services, underpinned by a commitment to resilience and efficiency.

1. **Cost Management and Optimization**

MedCo's AWS deployment strategy balances a robust, scalable infrastructure and economic efficiency. We have conducted a detailed cost analysis using the AWS Pricing Calculator to estimate and manage monthly expenses effectively.

**4.1 Detailed Cost Analysis:**

The projected monthly cost for MedCo's AWS services is approximately $5,000. This includes:

* **EC2 Instances:** $136 for T3a instances to handle web traffic and $934 for M4 instances to balance the compute and memory needs.
* **Database Infrastructure:** $1,768 for i3en instances chosen for high I/O performance and storage, with $1,994 allocated for RDS providing 3 TB of storage and Multi-AZ failover capabilities.
* **Storage and Security:** $70 for the S3 bucket for durable object storage and $12 for AWS WAF to protect web applications.

**4.2 Cost Optimization Strategies:**

To optimize costs, we are implementing several measures:

* **Auto Scaling:** Dynamically adjusting compute resources to match demand, preventing overprovisioning.
* **Reserved Instances:** Leveraging lower prices for long-term commitments where feasible.
* **Right-Sizing:** Continuously evaluating and adjusting resource allocation to fit current workloads.
* **CloudWatch Monitoring:** Identifying and downsizing underused resources to cut unnecessary costs.
* **S3 Lifecycle Policies:** Transitioning older data to cheaper storage classes to manage storage costs efficiently.

**4.3 Environmental Impact Considerations:**

Sustainability is a crucial factor in our design. We utilize carbon-neutral cloud regions and optimize resource use to minimize environmental impact. Serverless and containerized services are employed to maximize server utilization and operational efficiency.

By addressing cloud infrastructure's financial and environmental aspects, MedCo can ensure its AWS investment is cost-effective and sustainable.

1. **Conclusion and Lessons Learned**

As we reach the culmination of our proposal for MedCo's cloud infrastructure, it is essential to encapsulate our journey and the insights gleaned. Our proposed solution, architected on AWS, promises a transformative impact on MedCo’s operations, infusing agility, reliability, and innovation into their healthcare services.

5.1 Summary of Proposed Solution's Benefits: The solution we have architected for MedCo harnesses the full spectrum of AWS capabilities to deliver:

* Resilience: Through Multi-AZ deployments and robust disaster recovery strategies, ensuring high availability and business continuity.
* Scalability: With Auto Scaling and elastic load balancing, MedCo's infrastructure can dynamically adapt to changing demand patterns.
* Security: By employing IAM, WAF, and AWS Shield, we have ensured that MedCo's data and services are protected against the latest security threats.
* Cost Efficiency: Through detailed cost breakdown and optimization measures, we have laid a foundation for operational expenditure that scales sensibly with the company's growth.
* Sustainability: Our design considers the environmental impact, aiming for a deployment that is as green as it is powerful.

5.2 Discussion on the Adoption of the Solution: Adopting this AWS-based cloud architecture positions MedCo at the forefront of healthcare innovation. It is a decisive step towards a future where scalability meets cost efficiency, and security protocols are embedded within the fabric of the company's digital infrastructure. The transition to this cloud solution will be a phased process marked by meticulous planning, execution, and continual adaptation.

5.3 Reflection on Lessons Learned: Throughout this project, our team has absorbed invaluable lessons:

* The importance of planning: Every aspect of the cloud architecture was preceded by thorough planning, which helped avoid costly missteps and ensure a seamless deployment.
* Adaptability is key: The ability to pivot and adjust our strategies in response to evolving project requirements and external feedback has been instrumental.
* Collaboration drives success: Working closely with stakeholders and maintaining open communication channels have been pivotal in aligning the infrastructure with MedCo's business goals.
* Continuous learning: The rapidly changing landscape of cloud technologies necessitates ongoing education and adaptability to harness innovative solutions effectively.

In conclusion, the proposed AWS architecture for MedCo is not just a blueprint for a state-of-the-art digital infrastructure but also a testament to strategic planning, collaborative effort, and our commitment to continuous improvement. As MedCo looks to the future, this cloud solution is a resilient, secure, and scalable foundation that will support and foster the company's aspirations to revolutionize healthcare delivery.

**Appendixes**

**Appendix A: Role Play Activity**

Ben represented our team and worked with another presentation team as Group #1, and we engaged in a productive dialogue with the MedCo representatives during the role-play activity. The following is a detailed account of the questions, the responses, and the key discussion points that emerged from the conversation.

Question 1: What is high availability? How is it different from high dependability?

Response: High availability refers to a system's ability to remain accessible and functional for long, minimizing potential downtime and service interruptions. High availability is achieved through redundancies and failover mechanisms that ensure service continuity during component failures. While high availability focuses on system uptime and accessibility, high dependability encompasses a broader spectrum that includes availability, reliability, maintainability, and the overall trustworthiness of the system. Dependability ensures the system is up and running and operates correctly, securely, and efficiently over time.

Question 2: Why do I need to worry about high availability? I already have a disaster recovery plan.

Response: High availability and disaster recovery serve different purposes. A disaster recovery plan is a reactive measure for restoring systems after a catastrophic event, while high availability is a proactive approach designed to prevent downtime before it occurs. Relying solely on disaster recovery could lead to significant service disruptions, which high availability seeks to avoid.

Question 3: Our customers have asked us if our application is highly available. So, if we operate from NY and all of our resources are in the cloud in one Availability Zone in the US West (Oregon) region, can we tell our customers that we are highly available?

Response: Operating from a single Availability Zone does not constitute high availability. High availability requires a multi-AZ approach where resources are distributed across multiple geographically dispersed data centers. This ensures that if one zone is compromised, others can take over without affecting the end-user experience.

Discussion Points:

* The importance of distinguishing between high availability and disaster recovery in customer communications.
* There is a need to implement a multi-AZ strategy to achieve actual high availability.
* Clarification on the misconception that having resources in the cloud automatically equates to high availability.
* The critical role of geographical diversity in protecting against regional outages and ensuring continuous service.

The dialogue with the MedCo representatives highlighted the necessity of a well-architected cloud solution that aligns with their business continuity goals and addresses their customers' concerns regarding uptime and reliability.

**Appendix B: Statement of Contributions**

Member 2: Brandon Luff:

Discussion Contribution: Our group convened outside of regular class hours for project discussions, maintaining communication through text and email. This collaborative effort allowed us to align our ideas and approaches effectively.

Presentation Contribution: After concluding our discussions and pulling together the information required to piece together a presentation, I created and organized all slides as seen in the presentation as well as created the architecture graphic displayed in the presentation as well as in this paper. Additionally, I prepared and presented slides 1 through 9 thoroughly depicting a handful of the decisions we made on MedCo’s behalf as well as detailing why the AWS cloud is a strong and viable option to host a cloud-based software as a service.

Paper Contribution: Overall, contributed to the architecture graphic as well as the reference page and reviewed the final paper to ensure and correct any spelling, grammar, or formatting issues.

**Member 1: Benjamin Gaudlip**

Role Play Contribution: As the sole representative for our group during the role play phase, I collaborated closely with Marcella Dias and Thi Xinh Vu to address the questions assigned to Group #1. I took the lead in developing our comprehensive response to the first question on high availability and dependability.

Discussion Contribution: Our group convened outside of regular class hours for project discussions, maintaining communication through text and email. This collaborative effort allowed us to align our ideas and approaches effectively.

Presentation Contribution: I was responsible for presenting slides 10 through 16 and provided detailed speaker notes for the slides I contributed to or presented. During the Q&A session, I addressed a question regarding our choice of US-East (N. Virginia) and US-East (Ohio) regions for the deployment, explaining that our strategy anticipates rapid growth for MedCo, necessitating a system designed for immediate and scalable availability.

Report Contribution: I compiled our collective research and notes into the final report, overseeing the document's formatting to ensure adherence to the statement of work provided and APA formatting best practices.

**Figures**

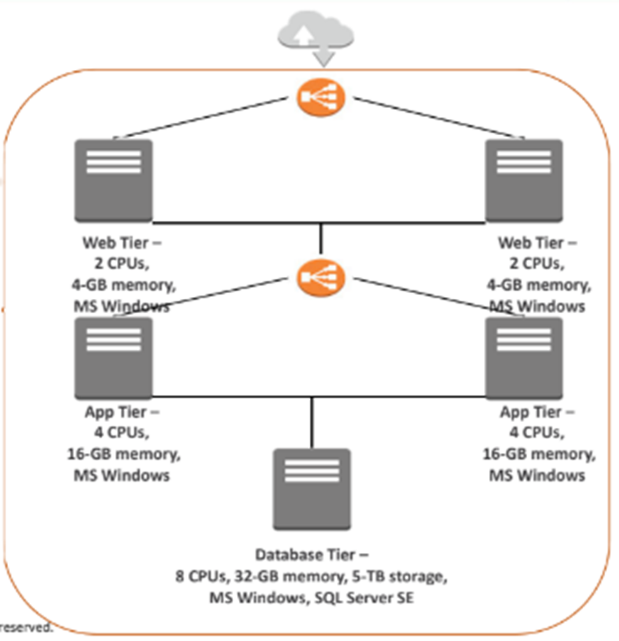


Figure 1. Overview of MedCo's AWS Multi-Tier Architecture

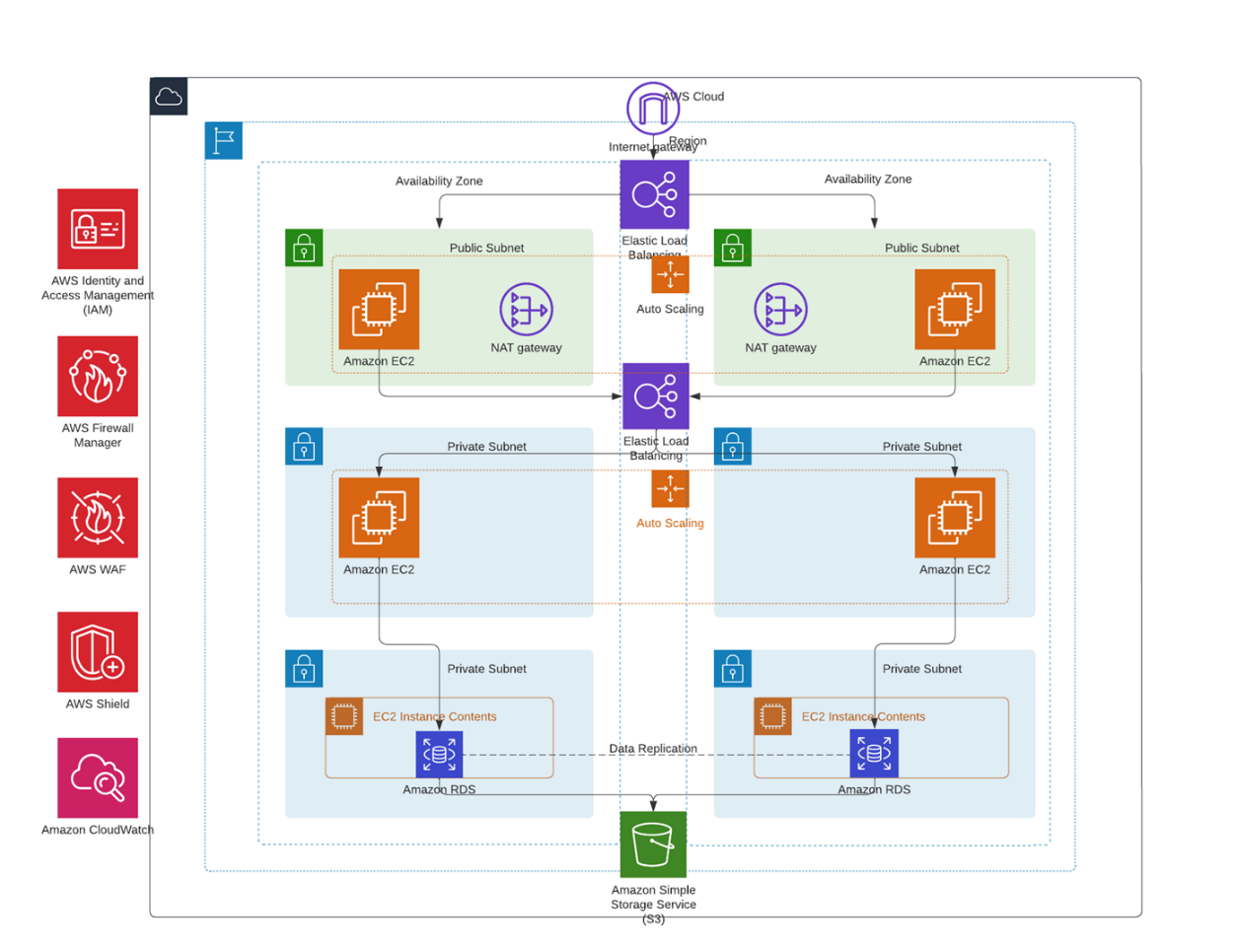


Figure 2. Schematic of Availability Zones and Subnet Configuration in MedCo's AWS Infrastructure

**References**

FARRAR, STRAUS & GIROUX. (2024). *Amazon Web Services*. Amazon. https://aws.amazon.com/console/