ENPM665: CLOUD SECURITY

FINAL PROJECT

Securing a Cloud-based Healthcare Application

GROUP 15

Members:

Rishabh Nama

Manarth Bhavsar

Srinivasan Anandan

Under the Guidance of:

Prof. Kevin Shivers

Prof. Thomas Dineen

Overview

The healthcare AWS structure is crafted meticulously to serve patients, health providers, and administration, fostering a secure environment. In this report, AWS Shield and WAF fortify patient data security while caregivers securely access information using ELB and CloudTrail. IT administrators manage the system through VPN access and IAM policies.

Thorough security assessments cover vulnerabilities, data protection, and network security, utilizing solutions like Multi-Factor Authentication, encryption, and IAM policies for mitigation. Network enhancements incorporate multi-region architecture and AWS WAF.

Disaster recovery strategies prioritize centralized logging and multi-region approaches. AWS features such as AWS Shield, WAF, ELB, CloudTrail, IAM, and multi-region architecture bolster security and establish robust disaster recovery measures within this healthcare AWS framework, ensuring a resilient and safeguarded ecosystem.

Summary of vulnerabilities and its Mitigation: -

1.1 Vulnerability Assessment Report: -

1> EC2 Instance - EC2 API Termination Protection: -

The EC2 instances on the cloud lack termination protection. It increases the risk of accidental terminations.which can lead to unexpected disruptions. To overcome this problem, we enable the DisableApiTermination attribute with a value of "true". By doing this we will safeguard instances from unintended shutdowns/terminations, ensuring system stability and preventing accidental data loss.

2> Public Subnet - Automatic Public IP Assignment: -

On cloud, Instances launched in the public subnet automatically receive public IP assignments which potentially expose them to unauthorized access via the internet. To address this security issue, we set the Properties.MapPublicIpOnLaunch attribute to false. This adjustment will restrict public accessibility, reducing the risk of unauthorized access of the instances. Thus, hardening network security.

3> S3 Bucket - Versioning and Access Logs: -

The S3 bucket is lacking versioning, making changes or object deletions irreversible. To prevent this issue, we activate versioning by setting the Properties.VersioningConfiguration.Status attribute to ‘Enabled’. Moreover, access logs for S3 are not being collected, which poses a challenge in tracking and auditing access to S3 objects. We enable logging by configuring the Properties.LoggingConfiguration attribute to ensure comprehensive auditing and monitoring of S3 access.

4> RDS (Relational Database Service) - Backup and Authentication: -

Automatic backup for the AWS Relational Database is disabled, leaving the system vulnerable in any unwanted or unexpected events of a disaster. To overcome this risk, we set the Properties.BackupRetentionPeriod attribute to 1 or more, ensuring regular backups for data recovery and system availability. Moreover, RDS IAM authentication is disabled, increasing security risks associated with using passwords over tokens. We enable IAM database authentication by setting the Properties.EnableIAMDatabaseAuthentication attribute to true which will enhance security measures and user access control.

5> Security Group - Ingress Access: -

AWS Component: - Security Group

The security group allows open ingress, permitting inbound traffic from any source. This unrestricted access increases the risk of unauthorized entry by allowing everyone to access system resources. To resolve this vulnerability, we will configure the Properties.SecurityGroupIngress.CidrIp attribute with a more restrictive IP range which will eventually limit the access to authorized entities only.

6> RDS Encryption: -

The RDS instance is non-encrypted at rest which poses a risk of data leak in the case of unauthorized access. We will enable encryption by setting the Properties.StorageEncrypted attribute to ‘true’, securing data stored within the RDS instance. Similarly, the EC2 instance's root block device lacks encryption, making data vulnerable to unauthorized access. To overcome this, set the BlockDeviceMappings.Encrypted attribute of the root device to ‘true’, ensuring data security in case of unauthorized access to the EC2 instance.

Logging & Monitoring: -

The fundamental pillars of AWS security are logging and monitoring. They offer quick insight into system operations, facilitating prompt threat identification, incident handling, and adherence to regulations. In the event of an issue with security, comprehensive logs provide a trail of user activity, facilitating forensic investigation and responsibility. By actively monitoring, anomalies can be found and remedial action against such dangers can be taken. In the end, efficient monitoring and logging strengthen AWS security by guaranteeing resource optimizations', regulatory compliance, and system integrity.

1> CloudTrail: - We will enable the Cloudtrail feature on the system because AWS API calls made on your account are tracked by CloudTrail, which offers a history of events for security analysis, compliance audits, and troubleshooting. Here, every action made with your AWS resources is fully recorded by turning on CloudTrail.

2> VPC Flow Logs: - We will enable VPC Flow Logs. Within our Virtual Private Cloud (VPC), VPC Flow Logs record network traffic details, including source and destination IP addresses, ports, and protocols utilized. Understanding network traffic patterns and identifying connectivity problems are made easier by analyzing these records.

3> S3 Access logs: - We also need to enable the S3 Access Logs because requests made to your Amazon S3 (Simple Storage Service) buckets are tracked by S3 Access Logs. These logs help with security auditing, compliance, and access monitoring by offering insightful information on who accessed the data, when, and from where.

4> WAP Logs: - We will enable the WAP Logs storing because the web traffic that AWS WAF inspects and any actions performed in accordance with established rules are detailed in WAF Logs. Understanding possible dangers, evaluating the efficacy of security regulations, and strengthening defences against web-based attacks are all aided by the analysis of these logs.

A centralized log repository is established to store all AWS environment logs. CloudTrail is set up to capture API calls, feeding its events into a CloudWatch log group, which, in turn, forwards data to the centralized bucket. Security tools like GuardDuty, Inspector, Macie, and Detective direct their logs to Security Hub, which consolidates them into the same CloudWatch log group. VPC flow logs and S3 server access logs from all buckets are funneled into this log group as well. The S3 bucket additionally sends logs to a Simple Queue Service (SQS), acting as a bridge to a Security Information and Event Management (SIEM) tool. In this instance, Splunk serves as the SIEM tool, allowing log querying for identifying misconfigurations during security incidents or outages. Custom dashboards in Splunk provide visualization for easy monitoring and assessment of potential misconfigurations.

1.2 Access Control Results: -

1> EC2 - Non-Encrypted Root Block Device

Here, the Root block device is not encrypted which makes data readable in case of unauthorized access. To overcome this, we will enable encryption with the help of AWS Key Management System. For our EC2 instances, we use Amazon EBS encryption as a simple encryption option for EBS resources. You don't need to create, administer, and safeguard your own key management infrastructure while using Amazon EBS encryption. AWS KMS keys are used by Amazon EBS encryption to create encrypted volumes and snapshots.

2> RDS - Non-Encrypted RDS Instance at Rest: -

This is a medium severity issue where there is a non-encrypted RDS instance which exposes data risks in case of unauthorized access. To overcome this, Amazon RDS DB instances can be encrypted by Amazon RDS. The underlying storage for database instances, as well as its automated backups, read replicas, and snapshots, are all encrypted at rest. The server hosting Amazon RDS encrypted DB instances encrypts the data using the industry-standard AES-256 encryption method. Following the encryption of the data, Amazon RDS transparently manages access authentication and data decryption with little to no performance impact.

3> RDS - Hard Coded Credentials in Plain Text: -

This is a high severity issue where hardcoded credentials are there in the yml files in plain text pose a very high security risk. To overcome this situation, We can use AWS Secrets Manager to securely store, rotate, and retrieve keys and passwords, ensuring a higher level of security for sensitive credentials.

4> RDS - Poor Password Policy: -

This is a low severity where password policy is very weak which is susceptible to brute force attacks. To overcome this, we enforce strong password policies requiring where at least 12 characters comprising alphanumeric characters and symbols are applied. This security measure will enhance password security reducing brute forcing and enumeration attempts.

5> S3 - Improper Access Control: -

This is a medium severity issue where there is Improper access control in S3. To overcome this, we implement S3 Bucket Policy least privilege with the principle of least privilege. This approach ensures that access permissions are associated to specific roles, minimizing the risk of unauthorized access.

1.3 Virtual Machine Security Results: -

1> Missing Software Security Updates: -

This is a medium severity issue where The EC2 instances lack necessary software security updates which imposes the risk of exploiting critical vulnerabilities as well as risk of zero-day vulnerability. To overcome this, we enable AWS Patch Manager that will automate the patching process, ensuring regular updates and securing against potential vulnerabilities. These security measures will ensure system integrity and security by keeping software up to date.

2> Instance Placement in a Public Subnet: -

This is a high severity issue where an EC2 instance is placed within a public subnet, which is accessing to the public which exposes it to potential security threats and unauthorized access. To overcome this, we transfer the instance to a private subnet or place it within a Virtual Private Cloud (VPC) and establish VPC Peering which will restrict external access. Thus, ensuring security by isolating the instance from public exposure.

3> Unencrypted Root Block Device: -

This is a medium severity issue where the root block device of the EC2 instance has no encryption which risks data exposure in the event of unauthorized access. To overcome this issue, KMS EBS Encryption must be used. Data security is greatly increased when EBS (Elastic Block Store) encryption is used with KMS (Key Management Service). First, we encrypt the root disc using a customer-managed key that you produce in KMS or with the default AWS-managed key. Next, affix this encryption key to the root EBS storage of the EC2 instance. To strengthen security against unauthorized access and possible data exposure, make sure that only authorized entities have access to the encryption keys. This preventive precaution makes sure that the data stays encrypted even in the event of unauthorized access, reducing the danger of exposure and upholding security standards.

1.4 Network Security Scans: -

1> EC2 - Unencrypted Communication (Web Communication through port 80) Issue: -

This is a medium severity issue where web communication occurs over an unencrypted channel via port 80 (HTTP), which is a clear text protocol that risks data integrity. To overcome this we use HTTPS (HTTP over SSL/TLS) instead of HTTP that enhances data security. This encryption ensures secure, encrypted communication that ensures data integrity and confidentiality.

2> WAF (Web Application Firewall) - Absence of Web Application Firewall: -

This is a high severity issue. The absence of a WAF leaves the web application vulnerable to various attacks like DDoS, Command Injection, etc. To overcome this, a Web Application Firewall is required to protect the web application from malicious requests and attacks. A WAF filters incoming traffic and blocks potential threats, enhancing the security posture of the web application.

3> VPC (Virtual Private Cloud) - Improper Access Control: -

This is a high severity issue. This public security group allows unrestricted access to ports 80 and 22, posing a significant security risk. To overcome this, we restrict access by configuring **security groups** to only allow access only from trusted sources.we implement tighter security controls by limiting access to necessary ports and applying the principle of least privilege.

4> Amazon Shield - Absence of DDoS Protection: -

This is a high severity issue. DDoS protection provided by Amazon Shield is not enabled, which threatens the servers to potential DDoS attacks. To overcome this, we enable Amazon Shield, a service designed to safeguard servers against potential DDoS attacks. By Activating this service, it strengthens the infrastructure resilience against large-scale and sophisticated DDoS attacks, ensuring the availability pillar of CIA Triad.

1.5 Disaster recovery Assessment: -

1> No Disaster Recovery Playbook

This is a medium impact vulnerability. Here due to lack of playbook for disaster recovery, the organization lacks guidelines and procedures for handling disasters, leading to potential chaos and prolonged downtime. To mitigate this risk, we develop a comprehensive disaster recovery playbook outlining procedures and protocols for different disaster scenarios.

(Make a Playbook)

2> Not Multi AZ

This is a low impact risk. Here the lack of multi-AZ setup can result in a single point of failure which can potentially risk the whole infrastructure to collapse if a geographical region is affected. To prevent this kind of situation, we implement multi-AZ configuration across EC2, RDS, and S3 to enhance availability and resilience against regional outages.

EC2: No Data Backups: -

This is a medium impact vulnerability. In absense of backups or snapshots, recovering data or instance states in case of any disaster or attack is impossible which imposes a very high risk on availability. To overcome this we set up regular data backups and snapshots for EC2 instances with the help of AWS Backup which is a service which ensures data recovery and instance state restoration. By automating backup scheduling, it makes point-in-time recovery possible for EC2 volumes and RDS databases with personalized lifecycle management and retention policies. Data protection is streamlined by this one solution, which also provides policy-based backup plans and effective disaster recovery. To ensure data resiliency across AWS resources, users may benefit from centralized control, automated backups, and simplified recovery choices with AWS Backup.

EC2: No autoscaling: -

Managing varying needs effectively is the main problem when running EC2 instances without autoscaling. It becomes imperative to adopt manual scaling techniques in order to handle this. Start by keeping a close eye on workload trends in order to make precise resource predictions. Next, manually modify the capacity of EC2 instances in light of these findings. Although this approach does not have the automatic response to scaling as autoscaling groups have, it does permit scaling changes in response to expected needs. Consider establishing scaling policies with AWS CloudWatch alarms to initiate notifications or scripts for timely scaling adjustments in order to maximize the effectiveness of this strategy. But take note that compared to autoscaling, manual scaling may result in slower responses. To efficiently handle fluctuating demands, careful observation and timely manual interventions are needed.

EC2: Load Balancer: -

Using EC2 instances without load balancers makes it difficult to effectively handle different traffic volumes. Manual load balancing techniques must be used to get around this. To start, keep a close eye on incoming traffic patterns to gauge resource requirements. Next, manually split up incoming traffic among EC2 instances according to trends you've noticed. Although this manual method does not have the automated load distribution of a load balancer, it does allow for manual modifications to take changing traffic patterns into account. Establish monitoring using AWS CloudWatch metrics to cause manual load modifications based on observed thresholds or patterns in order to optimise this procedure. Nevertheless, keep in mind that human load balancing could be less agile than automatic load balancers, requiring constant observation and prompt manual interventions to efficiently balance traffic among instances.

S3: No Archived Glacier Storage

This is a medium impact vulnerability. The lack of archived Glacier storage complicates disaster restoration in multiple locations, hindering efficient recovery strategies. To overcome this, we implement archived Glacier storage for better disaster recovery and restoration options across multiple locations.

S3: No S3 Backup: -

In scenarios where S3 data lacks backup, Cross-Region Replication (CRR) serves as a vital strategy for enhancing data durability and availability. Redundancy and disaster recovery capabilities are ensured through the automatic replication of S3 objects across several AWS regions, made possible by CRR. Data saved in a source bucket on S3 is replicated asynchronously to a destination bucket in a different region by enabling CRR. Any changes, removals, or new uploads to the source bucket are immediately duplicated to the destination bucket almost instantly thanks to this automatic replication process. By keeping identical copies of S3 items in distinct regions, CRR enables enterprises to improve their data resilience and lowers the risk of data loss from failures or outages that are exclusive to a given region. In addition to enhancing data durability, this functionality makes it possible to comply with data residency regulations and promotes high availability for applications that need low-latency access to S3 objects across several regions.

RDS: No Encryption at Rest

This is a medium impact vulnerability. Here, Absence of encryption at rest and disabled automatic backups pose confidentiality, integrity, and availability risks in case of theft or disaster. To overcome this, we enable encryption at rest for RDS instances and ensure automatic backups are present to overcome any unwanted situations.

Incident Response & Logging: -

Operations will inevitably involve security issues, which highlights the need for thorough logging to enable effective incident response. Quick evaluation and correction are essential in these circumstances. For these situations, an incident response plan acts as a thorough road map. This plan entails inventorying vital resources, outlining the duties and responsibilities of the incident response team, and creating frameworks for categorizing occurrences according to their nature and severity. Monitoring important security metrics and setting up alert automation are further made easier by connection with Splunk, which facilitates log gathering and visualization via personalized dashboards. Quick replies are ensured via automatic incident generation and workflow management made possible by integration with ServiceNow. In addition, communication protocols, regular training exercises, incident response processes, documentation, and post-mortem studies are essential elements that guarantee ongoing enhancement and flexibility in response to changing security environments.

Data Flow Patient Point of View: -

Here, we create a picture where a patient john uses his laptop to access the web application portal of the healthcare company.

1. **DNS Resolution:** Imagine the patient, John, sitting with his laptop. When he types the healthcare company's website into his browser, it's like asking for directions. Now, his device requests to translate the website name into a specific address.
2. **Route 53 Directs Traffic:** Amazon Route 53 is like a traffic manager for the internet. It guides John's request to the best AWS region based on his location and the company's setup. It uses DNSSEC (Domain Name System Security Extensions). DNSSEC is a security shield which authenticates responses to domain name lookups.
3. **Protection Against DDoS:** John's request now passes through AWS Shield. It is like a fortress protecting the infrastructure. If someone tries to flood the website with too much traffic, AWS Shield stops it, keeping the site running smoothly.
4. **Authentication Security:** Imagine John using not just a password but also a fingerprint or face scan to access the healthcare portal. This is Multi-factor authentication that strengthens the authentication mechanism with an extra layer.
5. **Data Encryption:** Now AWS Certificate Manager's TLS/SSL certificates come in very handy, ensuring the integrity of the message. When John sends information to the healthcare portal, it's like putting it in a locked box. AWS Certificate Manager's TLS/SSL certificates are the locks, ensuring that only the intended recipient can access or read the data.
6. **IAM Access Control:** Now IAM comes into the picture. It ensures that the patient has access to his own resources.
7. **Security Filtering with AWS WAF:** This traffic will pass through a WAF. It checks everyone entering (web traffic) and blocks troublemakers (like hackers trying to inject harmful code) from causing issues.
8. **Enhanced Performance via ALB:** Elastic Load Balancer (ELB) is like a traffic director at a busy intersection. It spreads the incoming requests evenly among servers, making sure no server gets overwhelmed, similar to how traffic lights manage the flow of cars.

9. **Traffic Security Policies:** NACLs and Security Groups ensure that only authorized traffic can pass through, especially on essential paths. This acts like security gates at specific entry points. (like controlling who can enter particular doors in a building).
10. **Enhanced Network Segmentation:** AWS Transit Gateway is like dividing a big office building into smaller sections, each with its security system. This way, if there's a problem in one area, it doesn't affect the others.

Patient's IAM Policy: -

- **AmazonS3ReadOnlyAccess:** Provides restricted read-only access to S3 buckets, specifically for accessing assets within the portal.

- **AmazonRDSDataReadOnly:** Allows read-only access to RDS data, facilitating the viewing of test results and accessing patient data within the system.

- **Custom Policy: ScheduleAppointments**: Grants permissions exclusively for scheduling appointments within the portal's functionalities.

- **Custom Policy: AccessGeneralInquiries:** Offers permissions tailored for accessing the general inquiries section of the portal, ensuring limited, specific access.

- **Custom Policy: TelemedicineConsultation:** Provides access permissions specifically for participation in telemedicine consultations through the platform.

- **Custom Policy: ViewOwnData:** Enables users to access and view their personal health records and related information exclusively.

Data Flow for Care Provider's Point of View:

1. **Care Provider's Device:** The care provider uses their authorized work device or mobile gadget to access the healthcare company's web application portal, Here we employed robust security measures such as antivirus software, strong passwords, enabling multi-factor authentication (MFA), and connecting through secure networks such as VPNs for enhanced security.

2. **Amazon Route 53:** The care provider's browser initiates a DNS request, resolved by Route 53 to direct them to the correct AWS region. This safeguards against potential malicious sites and ensures secure connections.

3. **AWS Shield:** Care provider requests pass through AWS Shield, shielding the web server from DDoS attacks. This ensures uninterrupted portal access even during high traffic periods.

4. **ELB (Elastic Load Balancing):** Requests, directed by Shield, are managed by ELB, distributing traffic across multiple web servers for optimized performance and availability even during server issues.

5. **Web Servers:** Serving static content, these servers interact with application servers for dynamic content, maintaining security via updated software and secure coding practices.

6. **Application Servers:** Managing various care-related actions, including accessing patient data, scheduling appointments, message exchange, and file uploads/downloads. These servers interact securely with databases and employ measures like access controls and encryption.

7. **Database Servers:** Securely store patient data with encryption, restricted access, and a secure environment.

8. **Care Provider Portal:** Presents processed data, ensuring ease of use, security, and compliance with healthcare regulations.

9. **AWS CloudTrail:** Logs all AWS API calls, enabling tracking of care provider activities, ensuring access to authorized data, and investigating security incidents.

10. **Amazon CloudWatch:** Monitors metrics and logs from various AWS resources, aiding in issue identification before impacting care providers and assessing portal performance.

Additional Considerations:
- Secure Communication: Encourage care providers to use encrypted communication channels for patient interactions.
- Data Encryption & Access Controls: Ensure patient data encryption at rest and in transit while strictly controlling access based on user roles and needs.

Care-Provider's IAM Policy: -

- **AmazonRDSFullAccess:** Provides complete access to RDS instances, allowing comprehensive management of all patients' data within the system.

- **AmazonS3FullAccess:** Grants unrestricted access to S3 buckets, facilitating the seamless uploading and retrieval of pertinent documents and data.

- **AmazonSNSFullAccess:** Offers complete access to Amazon SNS, enabling the sending and receiving of messages from third-party entities.

- **Custom Policy: AccessAllPatientData:** Tailored permissions exclusively for accessing and managing all patients' data within the system.

- **Custom Policy: SendReceiveThirdPartyMsgs:** Specifies permissions exclusively for sending and receiving messages from third-party sources, ensuring designated communication capabilities.

Data Flow Admin Point of View: -

1. **IT Support Device:**
   a. The IT support utilizes their work devices for accessing the healthcare company's management console or administrative tools, employing Multi-Factor Authentication (MFA) and Single Sign-On (SSO) for secure authentication.
2. **VPN Access:**
   a. Access to the Virtual Private Cloud (VPC) is available to IT support, including DBAs and system administrators, via a Client VPN, ensuring a secure tunnel for end-user support.
3. **Route 53:**
   a. IT support requests are directed through Route 53 to locate the internal IP address of the VPC endpoint, ensuring accurate and secure connections.
4. **ELB:**
   a. ELB effectively distributes IT support requests across multiple secure web servers within the private subnet, ensuring improved performance and scalability.
5. **SSH Access to EC2 Instances:**
   a. IT support can securely manage EC2 instances using SSH over port 22, allowing for effective management purposes.
6. **Web Servers:**
   a. Serving static content and interfacing with application servers, ensuring dynamic request processing and secure interactions.
7. **Application Servers:**
   a. Handling various IT support tasks like user management, resource allocation, monitoring, security configurations, backup management, and software updates.
8. **Database Servers (RDS or Aurora):**
   a. Provisioning, configuration, performance monitoring, troubleshooting, and recovery tasks are managed by IT support based on the chosen database solution.
9. **Management Console/Admin Tools:**

   a. IT support interacts with these tools to manage infrastructure effectively, accessing detailed resource information, logs, and alerts based on their roles and permissions.

10. **CloudTrail:**
    a. Logs all API calls and actions for IT support, ensuring a comprehensive audit trail for security and compliance.
11. **CloudWatch:**
    a. Collects and monitors metrics and logs from various AWS resources, aiding IT support in identifying issues, monitoring resource utilization, and optimizing performance.

Common Security Measures:

- Security Monitoring: Utilizing various services like CloudWatch, CloudTrail, GuardDuty, Security Hub, and Inspector to monitor logs and identify suspicious activities.
- Encryption and Security Configurations: Implementing encryption protocols and IAM policies to enforce access controls for sensitive data.
- S3 Versioning and Deletion Security: Utilizing S3 Versioning and MFA deletion for enhanced data security.
- NAT Gateway for Security: Implementation of NAT Gateway for secure communication from private subnet to external services.
- AWS Management Console Access: Access via MFA and SSO, configuring various services for secure usage.
- Incident Response and Patch Management: Employing incident response plans and automated patching for swift issue resolution.

Admin’s IAM Policy: -

End-User Support: -

AWSHealthFullAccess: It Provides complete access to AWS Health for comprehensive monitoring of service health.

IAMUserSSHKeys: Permissions designated for the management of SSH keys specifically intended for system administrators.

AWSLambdaReadOnlyAccess: Offers read-only access to AWS Lambda, allowing basic troubleshooting tasks to be performed.

IAMReadOnlyAccess: Grants read-only access to IAM, enabling the viewing of user information and permissions.

Custom Policy: EndUserSupport: Tailored permissions to facilitate end-user support tasks like password resets and troubleshooting efforts.

Database Administrators (DBAs): -

AmazonRDSFullAccess: Provides complete access to RDS instances for comprehensive database administration tasks.

AmazonRDSDataFullAccess: Grants full access to RDS data, facilitating efficient management and optimization of databases.

AmazonRDSDBInstanceIdentifier: Specific permissions enabling the management of RDS database instances.

Custom Policy: DBA_Tasks: Tailored permissions dedicated to Database Administrators for the management and optimization of RDS databases.

System Administration: -

1. **AmazonEC2FullAccess: -** Grants comprehensive access to EC2 instances, intended for system administrators to perform various tasks.

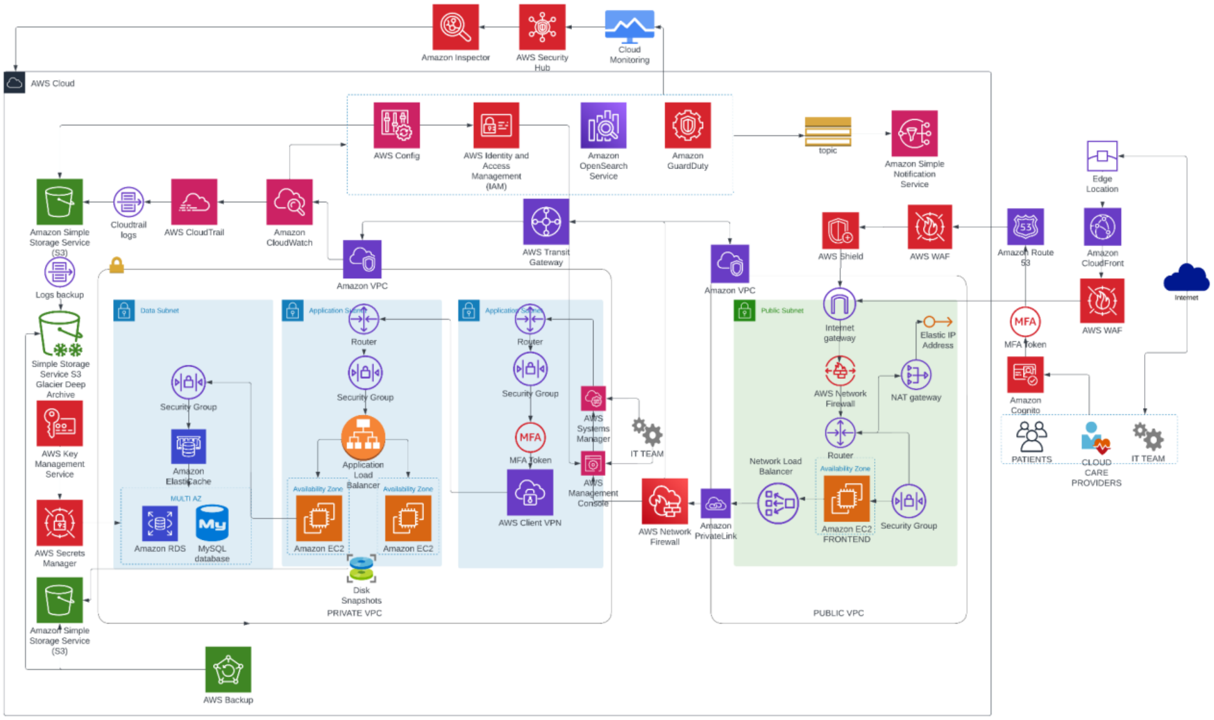
2. **AmazonEC2ReadOnlyAccess: -** Offers read-only access to EC2 instances, allowing monitoring and observation without modification abilities.

3. **AmazonS3FullAccess: -** Provides complete access to S3 buckets, facilitating the management of system-related data.

4. **AmazonS3ReadOnlyAccess: -** Allows read-only access to S3 buckets, enabling the retrieval of pertinent documents without the ability to modify data.

5. **AWSLambdaFullAccess: -** Grants full access to AWS Lambda, allowing the implementation of automation scripts and comprehensive utilization of Lambda services.

6. **Custom Policy: IAMUserSSHKeys: -** Permissions specifically dedicated to managing SSH keys designed for system administrators.


Amazon Inspector
AWS Security Hub
Cloud Monitoring
AWS Cloud
AWS Config
AWS Identity and Access Management (IAM)
Amazon OpenSearch Service
Amazon GuardDuty
topic
Amazon Simple Notification Service
Amazon Simple Storage Service (S3)
Cloudtrail logs
AWS CloudTrail
Amazon CloudWatch
AWS Transit Gateway
Amazon VPC
Logs backup
Simple Storage Service S3 Glacier Deep Archive
AWS Key Management Service
AWS Secrets Manager
Amazon Simple Storage Service (S3)
AWS Backup
Data Subnet
Security Group
Amazon ElastiCache
MULTI AZ
Amazon RDS
MySQL database
Application Subnet
Router
Security Group
Application Load Balancer
Availability Zone
Amazon EC2
Availability Zone
Amazon EC2
Disk Snapshots
PRIVATE VPC
Application Subnet
Router
Security Group
MFA
MFA Token
AWS Client VPN
AWS Systems Manager
AWS Management Console
IT TEAM
AWS Network Firewall
Amazon PrivateLink
Amazon VPC
Public Subnet
Internet gateway
AWS Network Firewall
Elastic IP Address
NAT gateway
Router
Network Load Balancer
Availability Zone
Amazon EC2 FRONTEND
Security Group
PUBLIC VPC
AWS Shield
AWS WAF
Amazon Route 53
Edge Location
Amazon CloudFront
AWS WAF
Internet
MFA
MFA Token
Amazon Cognito
PATIENTS
CLOUD CARE PROVIDERS
IT TEAM