**Case Study: Infrastructure, Networks and Ops**

**Pre-Conditions**

1. Candidates must give an evidence folder with screenshots and approach for the case study along with implementation. This folder will be part of training team one drive.
2. IaC Scripts should be committed to Git Folder

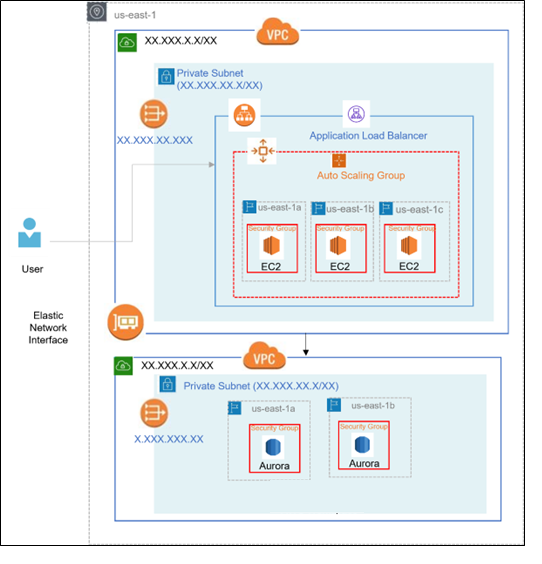
**Context**

Our client is a # 1 healthcare payor in US who wants to migrate their on-prem applications to cloud. But want to have a robust infra, network, security, and Ops to manage these applications effectively and efficiently to improve the business performance while reducing the cost and improving the business effectiveness. Mainly by meeting the healthcare compliance and data security. Most of the critical applications are leveraging cloud native application architecture, standpoints, and best practices. They are concerned about the following:

* Application scaling to meet the demand (concern around the open enrollment period or unseen disturbing events) while focusing on the application scalability, performance, availability, and cost.
* Ability to configure the entire application for high performance and throughput
* A self-healing infrastructure that recovers from failed service instances
* Security of data at rest and in transit as per the healthcare compliance
* Securing access to the environment as the delivery team expands
* Ability to easily manage and replicate multiple environments based on their blueprint architecture
* Disaster Recovery planning and execution for the business-critical apps yearly once

**OBJECTIVE**

Implement a manageable, secure, scalable, high performance, efficient, elastic, highly available, fault tolerant and recoverable infrastructure architecture / network that allows this healthcare payor enterprise to improve their efficiencies and effectiveness both from infra and operation standpoint. Consider the following archiecture as the baseline and optimize it based on the above points( In case of Azure/GCP, replace the AWS services in the diagram with equiavalent Azure/GCP servies)



**DELIVERABLES**

1. Diagram of the updated infrastructure architecture and network design
2. Clearly convey your thoughts – why you are proposing this optimized infrastructure, architecture and design
3. Implentation using Infrastructure as Code and working demo

❌ Missing / To Add:

* Bastion host
* S3 + CloudWatch for logs/backup
* Secret management (avoid plaintext passwords)
* WAF / Shield for ALB
* DR / replication setup
* IAM role granularity & KMS encryption for DB

| **Missing Component** | **Purpose** | **Cost Impact** | **Notes** |
| --- | --- | --- | --- |
| **AWS Systems Manager Parameter Store (for secrets)** | Securely store DB/app credentials instead of plaintext | 🟢 **Free / Very Low** | Standard parameters are free; advanced (for encryption) ~$0.05 per parameter/month |
| **AWS CloudWatch (basic monitoring/logs)** | Collects metrics, EC2/ALB/DB logs | 🟡 **Low** | Basic metrics free; custom metrics ~$0.30/metric/month, logs ~$0.50/GB ingested |
| **AWS S3 (for backups, logs)** | Store DB/app backups, access logs | 🟡 **Low** | ~$0.023/GB/month in standard; can use infrequent access or glacier for cheaper storage |
| **AWS WAF** | Protects ALB against web attacks | 🔴 **Moderate** | ~$5 per web ACL + ~$1 per rule + $0.60/million requests |
| **Bastion Host (t2.micro)** | Secure SSH entry to private subnet | 🟡 **Low** | ~$8–10/month if always on |
| **AWS Secrets Manager** | Store and rotate credentials | 🔴 **Moderate** | ~$0.40 per secret/month + $0.05 per 10K API calls |
| **Multi-AZ NAT Gateways** | High availability outbound access | 🔴 **High** | ~$0.045/hour per NAT + data processing ($0.045/GB) |
| **AWS Shield (Basic)** | DDoS protection | 🟢 **Free** | Automatically included with all AWS accounts |
| **Disaster Recovery (cross-region)** | Backup infra replication | 🔴 **High** | Duplicates infra + data transfer + storage |