Amazon VPC Use Case

Amazon VPC Client Project: Deploying a Secure Multi-Tier Application

GENERAL CHARACTERISTICS

Intent	To implement a secure multi-tier application architecture leveraging Amazon Virtual Private Cloud (VPC) to isolate resources, control traffic, and enhance security for a healthcare client.
Scope	Deployment of a three-tier application with web, application, and database layers using Amazon VPC, subnets, and network access control mechanisms.
Level	Network-level.
Client	Confidential (Healthcare Company).
Last Update	[Today's Date]
Status	Finalized.
Stage	Implementation and Monitoring.

ACTORS

Primary Actor	Network Engineer.
Secondary Actors	Application Developer, Security Architect, Client's IT Operations Team.

PREREQUISITES

Static Preconditions	- An AWS account with appropriate permissions. - Enabled services: Amazon VPC, Elastic Load Balancing (ELB), Amazon EC2, Amazon Relational Database Service (RDS), and AWS Identity and Access Management (IAM). - VPC and subnets configured for public and private layers.
Dynamic Preconditions	- Application code is containerized or ready for deployment. - Security Groups and Network ACLs defined to restrict traffic between layers. - Database backups stored securely using Amazon S3 or Amazon RDS snapshots.
Assumptions	- Client's application is compatible with AWS infrastructure. - Compliance with healthcare regulations such as HIPAA.

Amazon VPC Use Case

TRIGGERS

Trigger Event	The client requires a scalable and secure architecture to host a multi-tier healthcare application while meeting compliance standards.

EXPECTED OUTCOME

Success Postcondition	The application is deployed securely, with each layer isolated and protected against unauthorized access.
Failed Postcondition	Data breaches or non-compliance with healthcare regulations.

OPERATIONS AND CONCEPTS

Operations	1. Created a custom VPC with public and private subnets. 2. Configured security groups and Network ACLs to control inbound and outbound traffic. 3. Deployed a load balancer in the public subnet for distributing traffic to the web layer. 4. Launched EC2 instances for the application layer in private subnets. 5. Set up Amazon RDS in a private subnet for database operations. 6. Implemented AWS CloudTrail and AWS Config for compliance monitoring.
Concepts	- Amazon VPC: Provides isolated networking for AWS resources. - Subnets: Used to segregate public-facing resources from private ones. - Security Groups/Network ACLs: Fine-grained control of network traffic. - Elastic Load Balancer (ELB): Distributes traffic to ensure high availability. - Amazon RDS: Managed database service for secure and scalable database hosting.

MAIN SUCCESS SCENARIO

Step 1	Analyzed the client's application requirements and compliance needs.
Step 2	Designed and provisioned a custom VPC

Amazon VPC Use Case

	with appropriate subnets.environments.
Step 3	Configured security groups and network ACLs for traffic control.
Step 4	Deployed a load balancer to distribute user requests to the web tier.
Step 5	Launched EC2 instances for the application and web layers.
Step 6	Set up Amazon RDS with multi-AZ deployment for database resilience.
Step 7	Implemented AWS CloudTrail for audit logging and compliance monitoring.
Step 8	Conducted performance tests to ensure scalability and reliability.