


VIT

Vellore Institute of Technology
(Chartered to be a University under section 3 of the UGC Act, 1956)

Final Assessment Test – November 2025

Course: BCSE355L - Cloud Architecture Design
 Class NBR(s): 1828/1872/1879/1886/1892/1912/1917/
 1922/1926/1935/1949/1967/2435/2439/2440/4899/
 4900

Slot: G2+TG2

Time: Three Hours

Max. Marks: 100

- KEEPING MOBILE PHONE/ANY ELECTRONIC GADGETS, EVEN IN 'OFF' POSITION IS TREATED AS EXAM MALPRACTICE
- DON'T WRITE ANYTHING ON THE QUESTION PAPER

COs	CO Statements
CO1	Demonstrate an in-depth understanding of AWS Cloud architecture, services, and design patterns.
CO2	Apply security and compliance measures effectively in AWS architectures using encryption, access controls, and monitoring
CO3	Optimize cost and performance by selecting appropriate AWS services and utilizing cost-effective resource management strategies.
CO4	Configure and manage advanced AWS networking features, storage solutions, database technologies, and compute resources.

BL – Blooms Taxonomy Level (1 – Remember, 2 – Understand, 3 – Apply, 4 – Analyse, 5 – Evaluate, 6 – Create)

Answer ALL Questions

(10 X 10 = 100 Marks)

1. Explain cloud computing in line with the NIST definition, enumerate and briefly explain its five essential characteristics, describe three service models and four deployment models with appropriate examples, and state similarities between AWS and traditional on-premises IT infrastructure with a suitable diagram. CO1 BL1
2. Describe the essential elements of any IAM policy and write down a policy for the following scenario: CO1 BL6
 A single IAM policy that allows all actions on all the tables in dynamoDB except table named as "Table1" and allows all actions on all the objects in s3 except an object named as, "Object1.txt".
3. A small e-commerce site needs its web tier reachable from the internet, the database kept private, and automatic web-server failover across Availability Zones (AZs). With a neat diagram, explain how the auto scaling feature of AWS is used to handle the overload or failover of its web tier by a step-by-step procedure. CO4 BL4
4. Explain in detail the nine-step process for launching an Amazon EC2 instance, describing the required options and decision choices at each step. CO4 BL3

- 5.a) ShopGlobal is migrating their e-commerce platform to AWS. Due to compliance requirements, they must separate customer-facing web servers from backend payment processing systems into two different VPCs. The technical design specification given by the company is as follows:

CO4 BL3

VPC A: "Web-VPC" (10.0.0.0/16), Public Subnet: 10.0.1.0/24 (Web Servers ONLY);
VPC B: "Payment-VPC" (10.3.0.0/16), Private Subnet: 10.3.1.0/24 (Payment Processors ONLY). With a neat diagram, design and explain these VPC architectures with appropriate network elements, subnets, and route tables that should satisfy the following traffic requirements: Internet users can access Web Servers (HTTP/HTTPS) and Web Servers can initiate connections to Payment Processors; Payment Processors can respond to Web Server requests but cannot initiate connections to Web Servers. Further, Payment Processors cannot receive any inbound connections from the internet, which means Internet users cannot directly access Payment Processors.

OR

- 5.b) A manufacturing company is migrating their legacy inventory management system to AWS while maintaining connectivity to their on-premises corporate datacentre (192.168.10.0/24). Their AWS architecture includes a VPC (10.0.0.0/16) with both public and private subnets. The public subnet hosts a web application accessible to internet users, while the private subnet contains application servers that need to communicate with on-premises SQL databases in the corporate datacentre. The company demands a low cost and faster set-up that would support encryption over the internet during the data transfer. With a neat diagram, design and explain the chosen network connectivity architecture with appropriate network elements, subnets, and route tables that would connect the on-premise datacentre with the AWS datacentre.

CO4 BL3

6. You are the lead cloud architect for "GlobalStream," a fast-growing video streaming platform. The application has a PostgreSQL database running on AWS RDS as its primary data store. You are facing two major issues:

CO4 BL2

Performance During Peak Hours: Every evening, your database experiences a massive spike in read traffic from users browsing the catalog, loading profiles, and reading reviews.

Recovery Time Objective (RTO): During a recent scheduled maintenance in a single Availability Zone (AZ), the entire application was unavailable for 5 minutes. What specific AWS RDS feature or combination of features would you implement to cost-effectively solve both the read performance issue and the high-availability requirement simultaneously?

7. A regulated fintech company runs 250 Linux EC2 instances across dev and prod in two AWS accounts and two Regions. All instances are in private subnets (no SSH/RDP allowed). Leadership requires: (1) define and track system configurations along with the capability to explore operational health insights and analysis (2) automated remediation for critical issues (e.g., failed patch, high CPU, failed agent) with human approval when changes are risky; (3) formal change control with approvals and auditable records; and (4) a 24x7 incident response workflow with paging, runbook execution, and post-incident tracking. Explain the steps to integrate AWS Systems Manager to achieve the above-mentioned leadership requirements with a neat diagram. CO3 BL4
- 8.a) A healthcare application is deployed on AWS behind an Application Load Balancer. The application allows patients to schedule appointments, access medical records, and communicate with healthcare providers. During a security audit, the team discovers frequent SQL injection attempts and cross-site scripting (XSS) attacks targeting the patient portal. The application needs to block these attacks while maintaining trusted traffic from patients and healthcare providers. Design a WAF based solution should be able to distinguish between malicious attack patterns and legitimate complex medical queries that may contain similar character patterns to SQL commands, DDoS attacks and filters out the traffic from black listed IPs using appropriate sample WAF rules. CO2 BL4
- OR
- 8.b) Compare and contrast the following with suitable diagrams. CO2 BL4
- Client-Side Encryption – Client
 - Client-Side Encryption – S3
 - Server-Side Encryption – Client
 - Service-Side Encryption – S3
9. Compare and contrast AWS Simple Workflow Service and AWS Step Functions. CO1 BL5
10. You are tasked with migrating a 500 GB on-premises MySQL database, which supports a critical 24/7 customer-facing application, to an Amazon RDS for PostgreSQL instance to reduce operational overhead. The business has mandated a maximum downtime window of 15 minutes. The database schema has several incompatible data types and stored procedures that require transformation. How would you design the database migration strategy to ensure data consistency, handle the schema conversion, and achieve the minimal downtime objective? CO2 BL3

⇔⇔⇔ D/L/TY ⇔⇔⇔