Admissions & Support:
support@mockattempt.com
Phone / WhatsApp: +91 98765 43210
Course Code: AWSC • **Updated:** 01 Nov 2026
https://mockattempt.com/courses/aws-training

AWSC • CLOUD COMPUTING & AWS SOLUTIONS ARCHITECTURE | **BEGINNER TO SENIOR AWS CLOUD ARCHITECT**

100% LIVE INDUSTRY EXPERT COHORT + INTERNSHIP LETTER

AWS Training

Master Amazon Web Services from Global Infrastructure, IAM Least-Privilege Policies & STS Roles to S3 Storage Classes, CloudFront OAC, EC2/EBS, ALB, Multi-AZ VPC/NAT, RDS, DynamoDB, Lambda, API Gateway & SQS — with Python Boto3 programs, 10×50 MCQ Mock Tests per topic, and Spoken Voice + Gemini AI Interviews at ₹5,999.

Duration: 15–17 Weeks • Live + Hands-On Projects (210 Hrs) • **Modules:** 16 • **Live Topics:** 42 • **Labs & Tasks:** 84 • **Mocks / AI Vivas:** 244 / 244 • **Projects:** 16 Module + 1 Live Client Prod

Fixed Non-Negotiable Tuition Fee: Base Fee **₹5,999** + 18% GST (₹1,080) = **Total Incl. GST: ₹7,079**

Live Batch Tracks: Weekday Live Online Batch (Mon – Fri) (Monday to Friday (5 Live Interactive Classes / Week) • 1.5 Hours / Day (60 Mins Live Architecture & Coding + 30 Mins Hands-On Lab) • 18–20 Weeks Fast-Track) | Weekend Intensive Live Online Batch (Sat – Sun) (Saturday & Sunday (Designed for Working Professionals & College Students) • 3.0 Hours / Day (2 Hrs Deep-Dive Live Coding + 1 Hr Guided Project Build) • 20–22 Weeks Weekend Track)

Core Technologies & Engineering Stack: AWS IAM, STS & KMS • Amazon S3 & CloudFront CDN • Amazon EC2, EBS & ALB • Amazon VPC, Subnets & NAT Gateway • Amazon RDS Multi-AZ & DynamoDB • AWS Lambda, API Gateway & SQS • Python 3.12 & Boto3 SDK

1. PROGRAM MASTERY OUTCOMES & ELIGIBILITY

End-to-End Engineering Outcomes:

1. Design fault-tolerant Multi-AZ AWS architectures across Regions, Availability Zones, Edge Locations, and isolated VPC public/private subnets
2. Enforce least-privilege security using IAM JSON policies, STS AssumeRole temporary credentials, stateful Security Groups, and stateless NACLs
3. Optimize cloud storage, relational/NoSQL databases, and serverless event-driven pipelines across S3, CloudFront, RDS, DynamoDB, Lambda, API Gateway, and SQS
4. Clear 200 Timed Mock Exams (10,000 AWS MCQs) and 200 Spoken Voice + Gemini AI AWS Solutions Architect Interviews
5. Custom Multi-AZ VPC networking: public/private/isolated subnets, Route Tables, NAT Gateways, NACLs, and Security Groups.
6. Zero-trust IAM governance: IAM Roles, STS temporary credentials, KMS encryption, and AWS Organizations SCPs.
7. Elastic compute & storage: ALB + EC2 Auto Scaling, ECS Fargate, Lambda serverless, S3 lifecycle tiers, and CloudFront.
8. Managed data resilience: RDS Multi-AZ failover, DynamoDB on-demand/DAX, ElastiCache, SQS/SNS decoupling, and Route 53.

Eligibility & Prerequisites: Basic Linux command-line, networking (IP/HTTP), and introductory Python familiarity — teaches AWS cloud architecture from scratch • Any laptop/PC with Python 3.10+, AWS CLI v2 / Boto3, and a Free-Tier AWS account (or LocalStack) • No prior AWS industry experience required — Module 1 starts from environment setup, core mental models, and plain-English fundamentals. • Basic computer & internet familiarity on a Windows, macOS, or Linux laptop (8 GB+ RAM recommended for smooth live coding labs). • Ideal for B.Tech / BCA / MCA / B.Sc IT students, non-CS beginners, career switchers, and working developers upgrading to 2026 production standards. • Commitment to attend live Weekday or Weekend classes, complete daily hands-on lab checklists, and practice topic-wise Mock Tests & AI Interviews.

2. DETAILED MODULE & TOPIC-WISE SYLLABUS (16 MODULES • 42 LIVE TOPICS)

MODULE 1 OF 16 • 11 LIVE + LAB HOURS • 2 TOPICS • 1 CAPSTONE PROJECT (100 MARKS)

Module 1: AWS Cloud Foundations, Shared Responsibility & Global Infrastructure

Understand on-demand cloud economics, the AWS Shared Responsibility Model, AWS Well-Architected pillars, and Multi-AZ / Multi-Region physical topology.

Objectives: ✓ Distinguish AWS security OF the cloud from customer security IN the cloud across IaaS, PaaS, and SaaS services • ✓ Architect workload placement across AWS Regions, isolated Availability Zones (AZs), and CloudFront Points of Presence • ✓ Automate region discovery and service endpoint inspection using the Python Boto3 SDK with explicit timeouts and retries

1.1 AWS Cloud Computing Foundations — Shared Responsibility Model & Well-Architected Pillars [50 mins • Assignment (100M) • Hands-On Lab (50M) • 10 Mock Sets • 10 AI Vivas]

Purpose: To understand and apply AWS Cloud Computing Foundations — Shared Responsibility Model & Well-Architected Pillars in real AWS systems — specifically: How AWS replaces upfr...

1.2 AWS Global Infrastructure — Regions, Availability Zones, Local Zones & Edge Locations [50 mins • Assignment (100M) • Hands-On Lab (50M) • 10 Mock Sets • 10 AI Vivas]

Purpose: To understand and apply AWS Global Infrastructure — Regions, Availability Zones, Local Zones & Edge Locations in real AWS systems — specifically: Deep dive into geographi...

Module 1 Hands-On Capstone Project (100 Marks): Multi-AZ AWS Well-Architected Readiness & Region Latency Evaluator — Build a Python Boto3 architecture utility that audits workload placement across at least 3 Availability Zones in ap-south-1, maps Shared Responsibility controls per service tier, and flags s...

MODULE 2 OF 16 • 12 LIVE + LAB HOURS • 2 TOPICS • 1 CAPSTONE PROJECT (100 MARKS)

Module 2: AWS Identity and Access Management (IAM), Policy Evaluation & STS Roles

Master IAM identities, JSON policy evaluation precedence, Permission Boundaries, MFA conditions, and short-lived STS AssumeRole credentials.

Objectives: ✓ Author strict least-privilege IAM JSON policies scoped by Resource ARNs and Condition keys • ✓ Trace AWS policy evaluation order across Explicit Deny, Organizations SCPs, Resource Policies, and Identity Policies • ✓ Eliminate long-lived static IAM access keys on compute workloads using IAM Instance Profiles and STS AssumeRole

2.1 AWS IAM Architecture — Users, Groups, JSON Policies, Conditions & Explicit Deny Precedence [50 mins • Assignment (100M) • Hands-On Lab (50M) • 10 Mock Sets • 10 AI Vivas]

Purpose: To understand and apply AWS IAM Architecture — Users, Groups, JSON Policies, Conditions & Explicit Deny Precedence in real AWS systems — specifically: How AWS IAM authent...

2.2 AWS IAM Roles & STS — Trust Policies, Instance Profiles, OIDC Federation & AssumeRole [50 mins • Assignment (100M) • Hands-On Lab (50M) • 10 Mock Sets • 10 AI Vivas]

Purpose: To understand and apply AWS IAM Roles & STS — Trust Policies, Instance Profiles, OIDC Federation & AssumeRole in real AWS systems — specifically: Replacing static long-li...

Module 2 Hands-On Capstone Project (100 Marks): Least-Privilege IAM Policy Linter & STS Temporary Session Broker — Create an IAM security auditor and STS credential helper in Python that flags wildcard Action/Resource grants, verifies MFA Condition blocks, and formats short-lived STS session credentials.

MODULE 3 OF 16 • 12 LIVE + LAB HOURS • 2 TOPICS • 1 CAPSTONE PROJECT (100 MARKS)

Module 3: Amazon S3 Object Storage, Strong Consistency & Storage Classes

Architect durable object lakes with Amazon S3, Block Public Access, Pre-Signed URLs, KMS SSE encryption, and tiered S3 Storage Classes.

Objectives: ✓ Secure S3 buckets with Block Public Access, Versioning, SSE-KMS encryption, and time-bounded Pre-Signed URLs • ✓ Leverage S3 strong read-after-write consistency and multipart uploads for multi-gigabyte objects • ✓ Optimize petabyte-scale monthly storage spend across S3 Standard, Intelligent-Tiering, Standard-IA, One Zone-IA, and Glacier tiers

3.1 Amazon S3 Internals — Flat Key-Object Namespace, Strong Consistency, Versioning & Presigned URLs [50 mins • Assignment (100M) • Hands-On Lab (50M) • 10 Mock Sets • 10 AI Vivas]

Purpose: To understand and apply Amazon S3 Internals — Flat Key-Object Namespace, Strong Consistency, Versioning & Presigned URLs in real AWS systems — specifically: How Amazon S3...

3.2 Amazon S3 Storage Classes — Standard, Intelligent-Tiering, Standard-IA, One Zone-IA & Glacier [50 mins • Assignment (100M) • Hands-On Lab (50M) • 10 Mock Sets • 10 AI Vivas]

Purpose: To understand and apply Amazon S3 Storage Classes — Standard, Intelligent-Tiering, Standard-IA, One Zone-IA & Glacier in real AWS systems — specifically: Selecting the op...

Module 3 Hands-On Capstone Project (100 Marks): Secure S3 Presigned Upload Service & Storage Tier Cost Calculator — Implement a Python S3 storage utility that enforces SSE-KMS headers on uploads, computes optimal storage classes based on object access frequency and retention days, and prevents public ACL...

MODULE 4 OF 16 • 11 LIVE + LAB HOURS • 2 TOPICS • 1 CAPSTONE PROJECT (100 MARKS)

Module 4: S3 Lifecycle Automation & Global Edge Delivery with CloudFront CDN

Automate object tier transitions, abort incomplete multipart uploads, and accelerate global static/dynamic delivery securely via CloudFront Origin Access Control (OAC).

Objectives: ✓ Write valid S3 Lifecycle waterfall transitions and AbortIncompleteMultipartUpload cleanup rules • ✓ Lock private S3 origins behind CloudFront Origin Access Control (OAC) with SigV4 edge signing • ✓ Optimize CloudFront Cache Policies, Origin Request Policies, TTLs, and targeted path invalidations

4.1 S3 Lifecycle Management — Waterfall Transitions, Noncurrent Version Expiry & Multipart Cleanup [50 mins • Assignment (100M) • Hands-On Lab (50M) • 10 Mock Sets • 10 AI Vivas]

Purpose: To understand and apply S3 Lifecycle Management — Waterfall Transitions, Noncurrent Version Expiry & Multipart Cleanup in real AWS systems — specifically: Automating zero...

4.2 Amazon CloudFront CDN — Edge Caching, Origin Access Control (OAC), Signed URLs & Origin Shield [50 mins • Assignment (100M) • Hands-On Lab (50M) • 10 Mock Sets • 10 AI Vivas]

Purpose: To understand and apply Amazon CloudFront CDN — Edge Caching, Origin Access Control (OAC), Signed URLs & Origin Shield in real AWS systems — specifically: Accelerating st...

Module 4 Hands-On Capstone Project (100 Marks): Private S3 + CloudFront OAC Global Asset Delivery Blueprint — Generate a compliant S3 Lifecycle configuration (including incomplete multipart cleanup and noncurrent version expiration) paired with a CloudFront OAC bucket policy that blocks direct S3 UR...

MODULE 5 OF 16 • 12 LIVE + LAB HOURS • 2 TOPICS • 1 CAPSTONE PROJECT (100 MARKS)

Module 5: Elastic Compute Cloud (EC2), Purchasing Options & Elastic Block Store (EBS)

Size Nitro-based EC2 instance families, optimize On-Demand/Savings Plans/Spot purchasing, Harden IMDSv2 metadata, and provision gp3/io2 EBS volumes.

Objectives: ✓ Select optimal EC2 instance families (M, C, R, Graviton) and blend Savings Plans with Spot Instances • ✓ Enforce IMDSv2 session-oriented metadata tokens (HttpTokens=required) to block SSRF credential theft • ✓ Provision gp3 and io2 Block Express EBS volumes with KMS encryption, decoupled IOPS, and incremental S3 snapshots

5.1 Amazon EC2 Architecture — Nitro Instances, Purchasing Models, User Data & IMDSv2 Hardening [50 mins • Assignment (100M) • Hands-On Lab (50M) • 10 Mock Sets • 10 AI Vivas]

Purpose: To understand and apply Amazon EC2 Architecture — Nitro Instances, Purchasing Models, User Data & IMDSv2 Hardening in real AWS systems — specifically: Provisioning virtua...

5.2 Amazon EBS Block Storage — gp3 vs io2 Volumes, AZ Affinity, Snapshots & KMS Encryption [50 mins • Assignment (100M) • Hands-On Lab (50M) • 10 Mock Sets • 10 AI Vivas]

Purpose: To understand and apply Amazon EBS Block Storage — gp3 vs io2 Volumes, AZ Affinity, Snapshots & KMS Encryption in real AWS systems — specifically: Persistent network-atta...

Module 5 Hands-On Capstone Project (100 Marks): EC2 Fleet Cost Optimizer & EBS gp3 Migration Planner — Develop a Python capacity planner that splits baseline vs burst compute across Savings Plans and Spot Instances, enforces IMDSv2 launch template settings, and computes savings from migrating...

MODULE 6 OF 16 • 12 LIVE + LAB HOURS • 2 TOPICS • 1 CAPSTONE PROJECT (100 MARKS)

Module 6: Stateful Security Groups & Elastic Load Balancing (ALB / NLB)

Chain tier-to-tier Security Group references without brittle CIDRs and distribute Multi-AZ traffic cleanly via Application and Network Load Balancers.

Objectives: ✓ Chain ALB -> App -> RDS Security Groups using Security Group IDs instead of static instance IPs • ✓ Configure Layer-7 Application Load Balancers with TLS termination, host/path routing, and Target Group health checks • ✓ Contrast Layer-7 ALB with ultra-low-latency Layer-4 Network Load Balancers (NLB) and Connection Draining

6.1 AWS Security Groups — Stateful ENI Firewalls, Implicit Deny & SG-ID Chaining [50 mins • Assignment (100M) • Hands-On Lab (50M) • 10 Mock Sets • 10 AI Vivas]

Purpose: To understand and apply AWS Security Groups — Stateful ENI Firewalls, Implicit Deny & SG-ID Chaining in real AWS systems — specifically: How Security Groups act as statef...

6.2 Elastic Load Balancing — ALB vs NLB, Target Groups, Health Checks & X-Forwarded-For [50 mins • Assignment (100M) • Hands-On Lab (50M) • 10 Mock Sets • 10 AI Vivas]

Purpose: To understand and apply Elastic Load Balancing — ALB vs NLB, Target Groups, Health Checks & X-Forwarded-For in real AWS systems — specifically: Distributing Multi-AZ traf...

Module 6 Hands-On Capstone Project (100 Marks): Zero-Trust 3-Tier Security Group Chain & ALB Target Health Verifier — Build an automated AWS security & load-balancing topology validator that verifies SG-ID chaining across ALB, App, and Database tiers and checks ALB Target Group deregistration delay and heal...

MODULE 7 OF 16 • 12 LIVE + LAB HOURS • 2 TOPICS • 1 CAPSTONE PROJECT (100 MARKS)

Module 7: Amazon VPC Networking, CIDR Subnetting, Gateways & VPC Endpoints

Design non-overlapping Multi-AZ VPC CIDRs, calculate AWS reserved subnet IPs, deploy per-AZ NAT Gateways, and eliminate NAT data charges using Gateway VPC Endpoints.

Objectives: ✓ Carve /16 VPC CIDR blocks into Public, Private App, and Isolated DB subnets while accounting for the 5 AWS-reserved IPs per subnet • ✓ Deploy redundant NAT Gateways in public subnets (1 per AZ) to avoid cross-AZ NAT single points of failure • ✓ Route private S3 and DynamoDB traffic privately at zero hourly/per-GB cost using Gateway VPC Endpoints

7.1 Amazon VPC Internals — CIDR Blocks, 5 Reserved Subnet IPs, Route Tables & Internet Gateways [50 mins • Assignment (100M) • Hands-On Lab (50M) • 10 Mock Sets • 10 AI Vivas]

Purpose: To understand and apply Amazon VPC Internals — CIDR Blocks, 5 Reserved Subnet IPs, Route Tables & Internet Gateways in real AWS systems — specifically: Building logically...

7.2 AWS NAT Gateways & VPC Endpoints — Outbound-Only Private Egress, Multi-AZ HA & S3/DynamoDB Bypass [50 mins • Assignment (100M) • Hands-On Lab (50M) • 10 Mock Sets • 10 AI Vivas]

Purpose: To understand and apply AWS NAT Gateways & VPC Endpoints — Outbound-Only Private Egress, Multi-AZ HA & S3/DynamoDB Bypass in real AWS systems — specifically: Enabling pri...

Module 7 Hands-On Capstone Project (100 Marks): Multi-AZ VPC CIDR Calculator & NAT Cost-Elimination Planner — Write a Python networking tool using ipaddress that partitions a 10.20.0.0/16 VPC into 6 Multi-AZ subnets, computes exact usable host IPs (total minus 5 AWS-reserved addresses), and wires Ga...

MODULE 8 OF 16 • 12 LIVE + LAB HOURS • 2 TOPICS • 1 CAPSTONE PROJECT (100 MARKS)

Module 8: Stateless NACLs vs Security Groups & Managed Relational Databases (Amazon RDS)

Contrast stateless subnet Network ACLs (and ephemeral port ranges) against stateful Security Groups, and architect Multi-AZ Amazon RDS instances with Read Replicas.

Objectives: ✓ Diagnose stateless NACL return-traffic blackholes caused by blocked ephemeral TCP ports (1024–65535) • ✓ Architect Amazon RDS Multi-AZ standby failover (synchronous HA) versus asynchronous Read Replicas (horizontal read scaling) • ✓ Eliminate Lambda-to-RDS connection exhaustion and secure database credentials via RDS Proxy and Secrets Manager

8.1 Network ACL (NACL) vs Security Group — Stateless Subnet Filtering, Rule Ordering & Ephemeral Ports [50 mins • Assignment (100M) • Hands-On Lab (50M) • 10 Mock Sets • 10 AI Vivas]

Purpose: To understand and apply Network ACL (NACL) vs Security Group — Stateless Subnet Filtering, Rule Ordering & Ephemeral Ports in real AWS systems — specifically: Comparing s...

8.2 Amazon RDS Architecture — Multi-AZ Synchronous Failover, Read Replicas, PITR & RDS Proxy [50 mins • Assignment (100M) • Hands-On Lab (50M) • 10 Mock Sets • 10 AI Vivas]

Purpose: To understand and apply Amazon RDS Architecture — Multi-AZ Synchronous Failover, Read Replicas, PITR & RDS Proxy in real AWS systems — specifically: Provisioning managed...

Module 8 Hands-On Capstone Project (100 Marks): Stateless NACL Simulator & Multi-AZ RDS High-Availability Blueprint — Implement a rule evaluator that tests numbered inbound/outbound stateless NACL rules (including ephemeral port return traffic) alongside an RDS Multi-AZ configuration validator.

MODULE 9 OF 16 • 12 LIVE + LAB HOURS • 2 TOPICS • 1 CAPSTONE PROJECT (100 MARKS)

Module 9: Serverless NoSQL & Compute — Amazon DynamoDB & AWS Lambda

Model single-digit-millisecond DynamoDB Partition/Sort keys without hot partitions and engineer fast, idempotent AWS Lambda functions with warm execution reuse.

Objectives: ✓ Design high-cardinality DynamoDB Partition + Sort keys, GSIs, and Query expressions while avoiding full-table Scans • ✓ Calculate DynamoDB RCU/WCU capacity accurately across Eventual, Strongly Consistent, and Transactional operations • ✓ Optimize AWS Lambda cold starts, global SDK connection reuse outside handler(), memory/vCPU sizing, and DLQ resilience

9.1 Amazon DynamoDB — Partition & Sort Keys, Query vs Scan, GSI/LSI, RCU/WCU & Streams [50 mins • Assignment (100M) • Hands-On Lab (50M) • 10 Mock Sets • 10 AI Vivas]

Purpose: To understand and apply Amazon DynamoDB — Partition & Sort Keys, Query vs Scan, GSI/LSI, RCU/WCU & Streams in real AWS systems — specifically: Delivering predictable sing...

9.2 AWS Lambda Internals — Firecracker Execution Lifecycle, Cold Starts, Concurrency & Idempotency [50 mins • Assignment (100M) • Hands-On Lab (50M) • 10 Mock Sets • 10 AI Vivas]

Purpose: To understand and apply AWS Lambda Internals — Firecracker Execution Lifecycle, Cold Starts, Concurrency & Idempotency in real AWS systems — specifically: Event-driven se...

Module 9 Hands-On Capstone Project (100 Marks): Single-Table DynamoDB Capacity Planner & Idempotent AWS Lambda Processor — Build a DynamoDB RCU/WCU estimator paired with an AWS Lambda handler simulator that caches SDK clients at module scope and enforces conditional PutItem idempotency.

MODULE 10 OF 16 • 12 LIVE + LAB HOURS • 2 TOPICS • 1 CAPSTONE PROJECT (100 MARKS)

Module 10: Managed Front-Door APIs & Decoupled Messaging — API Gateway & Amazon SQS

Expose JWT/Cognito-protected serverless endpoints via Amazon API Gateway and buffer traffic spikes reliably with Amazon SQS Standard/FIFO queues, Long Polling, and Dead-Letter Queues.

Objectives: ✓ Choose accurately between API Gateway HTTP APIs, REST APIs, and WebSocket APIs while handling the 29-second synchronous timeout limit • ✓ Configure SQS VisibilityTimeout (>= 6x Lambda timeout), WaitTimeSeconds=20 Long Polling, and RedrivePolicy Dead-Letter Queues • ✓ Implement partial batch failure reporting (batchItemFailures) between SQS Event Source Mappings and AWS Lambda

10.1 Amazon API Gateway — HTTP vs REST vs WebSocket APIs, Authorizers, Throttling & 29s Limit [50 mins • Assignment (100M) • Hands-On Lab (50M) • 10 Mock Sets • 10 AI Vivas]

Purpose: To understand and apply Amazon API Gateway — HTTP vs REST vs WebSocket APIs, Authorizers, Throttling & 29s Limit in real AWS systems — specifically: Securing and throttli...

10.2 Amazon SQS — Standard vs FIFO Queues, Visibility Timeout, Long Polling & Dead-Letter Queues [50 mins • Assignment (100M) • Hands-On Lab (50M) • 10 Mock Sets • 10 AI Vivas]

Purpose: To understand and apply Amazon SQS — Standard vs FIFO Queues, Visibility Timeout, Long Polling & Dead-Letter Queues in real AWS systems — specifically: Decoupling produce...

Module 10 Hands-On Capstone Project (100 Marks): API Gateway Async Ingestion + SQS Partial-Batch Resilient Worker — Architect an async order-processing pipeline that validates API Gateway Lambda Proxy responses, checks SQS VisibilityTimeout >= 6x consumer timeout, and returns batchItemFailures so poison m...

MODULE 11 OF 16 • 16 LIVE + LAB HOURS • 4 TOPICS • 1 CAPSTONE PROJECT (100 MARKS)

Infrastructure as Code on AWS: Terraform / CloudFormation & Multi-Env State

Production-grade AWS Training engineering module covering Infrastructure as Code on AWS: Terraform / CloudFormation & Multi-Env State with hands-on labs and capstone build.

Objectives: ✓ Remote Terraform State in Encrypted S3 + DynamoDB State Locking — Purpose: Prevent two engineers or CI pipelines from corrupting cloud state simultaneously. • ✓ Reusable VPC, ALB & RDS Modules Across Dev/Stage/Prod Workspaces — Purpose: Provision identical, auditable AWS environments in minutes with zero console click-ops. • ✓ IAM OIDC GitHub Actions Federation (Zero Long-Lived AWS Access Keys) — Purpose: Deploy to AWS from CI using short-lived STS tokens instead of leak-prone static keys. • ✓ Drift Detection, Policy-as-Code Guardrails & Tagging Enforcement — Purpose: Block unencrypted buckets or public security groups automatically before apply.

11.1 Remote Terraform State in Encrypted S3 + DynamoDB State Locking [65 mins • Assignment (100M) • Hands-On Lab (50M) • 2 Mock Sets • 2 AI Vivas]

Purpose: To understand and apply Remote Terraform State in Encrypted S3 + DynamoDB State Locking in real AWS systems — specifically: Prevent two engineers or CI pipelines from cor...

11.2 Reusable VPC, ALB & RDS Modules Across Dev/Stage/Prod Workspaces [65 mins • Assignment (100M) • Hands-On Lab (50M) • 2 Mock Sets • 2 AI Vivas]

Purpose: To understand and apply Reusable VPC, ALB & RDS Modules Across Dev/Stage/Prod Workspaces in real AWS systems — specifically: Provision identical, auditable AWS environmen...

11.3 IAM OIDC GitHub Actions Federation (Zero Long-Lived AWS Access Keys) [65 mins • Assignment (100M) • Hands-On Lab (50M) • 2 Mock Sets • 2 AI Vivas]

Purpose: To understand and apply IAM OIDC GitHub Actions Federation (Zero Long-Lived AWS Access Keys) in real AWS systems — specifically: Deploy to AWS from CI using short-lived S...

11.4 Drift Detection, Policy-as-Code Guardrails & Tagging Enforcement [65 mins • Assignment (100M) • Hands-On Lab (50M) • 2 Mock Sets • 2 AI Vivas]

Purpose: To understand and apply Drift Detection, Policy-as-Code Guardrails & Tagging Enforcement in real AWS systems — specifically: Block unencrypted buckets or public security...

Module 11 Hands-On Capstone Project (100 Marks): Modular Terraform AWS VPC + Compute + RDS Blueprint — Design, implement, test, and document 'Modular Terraform AWS VPC + Compute + RDS Blueprint' applying every production concept from Module 11 (Infrastructure as Code on AWS: Terraform / Cloud...

MODULE 12 OF 16 • 16 LIVE + LAB HOURS • 4 TOPICS • 1 CAPSTONE PROJECT (100 MARKS)

AWS Containers & Serverless Event-Driven Architecture (ECS, Lambda, SQS)

Production-grade AWS Training engineering module covering AWS Containers & Serverless Event-Driven Architecture (ECS, Lambda, SQS) with hands-on labs and capstone build.

Objectives: ✓ Amazon ECR Image Scanning & Serverless ECS Fargate Task Definitions — Purpose: Run production containers without patching EC2 hosts, using per-task IAM roles. • ✓ ALB Target Group Health Checks & ECS Service Auto Scaling — Purpose: Scale container tasks seamlessly on CPU/request spikes with zero dropped connections. • ✓ AWS Lambda Cold-Start Tuning, API Gateway & DynamoDB Single-Table Patterns — Purpose: Build pay-per-request serverless APIs with sub-10ms DynamoDB lookups. • ✓ Decoupled Microservices with SQS Dead-Letter Queues, SNS & EventBridge — Purpose: Absorb 10x traffic bursts reliably and isolate failed events for safe replay.

12.1 Amazon ECR Image Scanning & Serverless ECS Fargate Task Definitions [65 mins • Assignment (100M) • Hands-On Lab (50M) • 2 Mock Sets • 2 AI Vivas]

Purpose: To understand and apply Amazon ECR Image Scanning & Serverless ECS Fargate Task Definitions in real AWS systems — specifically: Run production containers without patching...

12.2 ALB Target Group Health Checks & ECS Service Auto Scaling [65 mins • Assignment (100M) • Hands-On Lab (50M) • 2 Mock Sets • 2 AI Vivas]

Purpose: To understand and apply ALB Target Group Health Checks & ECS Service Auto Scaling in real AWS systems — specifically: Scale container tasks seamlessly on CPU/request spik...

12.3 AWS Lambda Cold-Start Tuning, API Gateway & DynamoDB Single-Table Patterns [65 mins • Assignment (100M) • Hands-On Lab (50M) • 2 Mock Sets • 2 AI Vivas]

Purpose: To understand and apply AWS Lambda Cold-Start Tuning, API Gateway & DynamoDB Single-Table Patterns in real AWS systems — specifically: Build pay-per-request serverless AP...

12.4 Decoupled Microservices with SQS Dead-Letter Queues, SNS & EventBridge [65 mins • Assignment (100M) • Hands-On Lab (50M) • 2 Mock Sets • 2 AI Vivas]

Purpose: To understand and apply Decoupled Microservices with SQS Dead-Letter Queues, SNS & EventBridge in real AWS systems — specifically: Absorb 10x traffic bursts reliably and...

Module 12 Hands-On Capstone Project (100 Marks): Event-Driven Order Processing Pipeline on ECS Fargate & SQS — Design, implement, test, and document 'Event-Driven Order Processing Pipeline on ECS Fargate & SQS' applying every production concept from Module 12 (AWS Containers & Serverless Event-Driven...

MODULE 13 OF 16 • 16 LIVE + LAB HOURS • 4 TOPICS • 1 CAPSTONE PROJECT (100 MARKS)

AWS Enterprise Security, KMS Encryption, Secrets Manager & WAF

Production-grade AWS Training engineering module covering AWS Enterprise Security, KMS Encryption, Secrets Manager & WAF with hands-on labs and capstone build.

Objectives: ✓ IAM Permission Boundaries, SCPs & Least-Privilege Policy Analysis — Purpose: Contain blast radius across multi-account AWS Organizations workloads. • ✓ Envelope Encryption with AWS KMS & Automatic Secrets Manager Rotation — Purpose: Rotate RDS credentials and API keys automatically without redeploying application code. • ✓ AWS WAF Managed Rules, Shield DDoS Protection & VPC Endpoints (PrivateLink) — Purpose: Block SQLi/XSS bot traffic at CloudFront edge and keep S3/Dynamo traffic off public internet. • ✓ CloudTrail Audit Trails, GuardDuty Threat Detection & AWS Config Rules — Purpose: Detect anomalous API calls and compliance drift within minutes.

13.1 IAM Permission Boundaries, SCPs & Least-Privilege Policy Analysis [65 mins • Assignment (100M) • Hands-On Lab (50M) • 2 Mock Sets • 2 AI Vivas]

Purpose: To understand and apply IAM Permission Boundaries, SCPs & Least-Privilege Policy Analysis in real AWS systems — specifically: Contain blast radius across multi-account AW...

13.2 Envelope Encryption with AWS KMS & Automatic Secrets Manager Rotation [65 mins • Assignment (100M) • Hands-On Lab (50M) • 2 Mock Sets • 2 AI Vivas]

Purpose: To understand and apply Envelope Encryption with AWS KMS & Automatic Secrets Manager Rotation in real AWS systems — specifically: Rotate RDS credentials and API keys auto...

13.3 AWS WAF Managed Rules, Shield DDoS Protection & VPC Endpoints (PrivateLink) [65 mins • Assignment (100M) • Hands-On Lab (50M) • 2 Mock Sets • 2 AI Vivas]

Purpose: To understand and apply AWS WAF Managed Rules, Shield DDoS Protection & VPC Endpoints (PrivateLink) in real AWS systems — specifically: Block SQLi/XSS bot traffic at Clou...

13.4 CloudTrail Audit Trails, GuardDuty Threat Detection & AWS Config Rules [65 mins • Assignment (100M) • Hands-On Lab (50M) • 2 Mock Sets • 2 AI Vivas]

Purpose: To understand and apply CloudTrail Audit Trails, GuardDuty Threat Detection & AWS Config Rules in real AWS systems — specifically: Detect anomalous API calls and complian...

Module 13 Hands-On Capstone Project (100 Marks): SOC2-Ready Hardened AWS Security & Secrets Architecture — Design, implement, test, and document 'SOC2-Ready Hardened AWS Security & Secrets Architecture' applying every production concept from Module 13 (AWS Enterprise Security, KMS Encryption, Sec...

MODULE 14 OF 16 • 16 LIVE + LAB HOURS • 4 TOPICS • 1 CAPSTONE PROJECT (100 MARKS)

Multi-Region Disaster Recovery, Observability & FinOps Cost Optimization

Production-grade AWS Training engineering module covering Multi-Region Disaster Recovery, Observability & FinOps Cost Optimization with hands-on labs and capstone build.

Objectives: ✓ RTO vs RPO Tiers: Backup/Restore, Pilot Light, Warm Standby & Active-Active — Purpose: Match business continuity SLAs to exact Route 53 failover and RDS cross-region designs. • ✓ CloudWatch Composite Alarms, Logs Insights, X-Ray Tracing & Dashboards — Purpose: Pinpoint cross-service AWS latency bottlenecks and page on-call teams before outages spread. • ✓ S3 Intelligent-Tiering, CloudFront Origin Shield & RDS Read Replicas — Purpose: Slash egress bandwidth bills and database CPU load simultaneously. • ✓ AWS Budgets, Cost Anomaly Alerts, Savings Plans & Right-Sizing Audits — Purpose: Cut monthly AWS cloud spend by 30–50% without sacrificing reliability.

14.1 RTO vs RPO Tiers: Backup/Restore, Pilot Light, Warm Standby & Active-Active [65 mins • Assignment (100M) • Hands-On Lab (50M) • 2 Mock Sets • 2 AI Vivas]

Purpose: To understand and apply RTO vs RPO Tiers: Backup/Restore, Pilot Light, Warm Standby & Active-Active in real AWS systems — specifically: Match business continuity SLAs to...

14.2 CloudWatch Composite Alarms, Logs Insights, X-Ray Tracing & Dashboards [65 mins • Assignment (100M) • Hands-On Lab (50M) • 2 Mock Sets • 2 AI Vivas]

Purpose: To understand and apply CloudWatch Composite Alarms, Logs Insights, X-Ray Tracing & Dashboards in real AWS systems — specifically: Pinpoint cross-service AWS latency bott...

14.3 S3 Intelligent-Tiering, CloudFront Origin Shield & RDS Read Replicas [65 mins • Assignment (100M) • Hands-On Lab (50M) • 2 Mock Sets • 2 AI Vivas]

Purpose: To understand and apply S3 Intelligent-Tiering, CloudFront Origin Shield & RDS Read Replicas in real AWS systems — specifically: Slash egress bandwidth bills and database...

14.4 AWS Budgets, Cost Anomaly Alerts, Savings Plans & Right-Sizing Audits [65 mins • Assignment (100M) • Hands-On Lab (50M) • 2 Mock Sets • 2 AI Vivas]

Purpose: To understand and apply AWS Budgets, Cost Anomaly Alerts, Savings Plans & Right-Sizing Audits in real AWS systems — specifically: Cut monthly AWS cloud spend by 30–50% wi...

Module 14 Hands-On Capstone Project (100 Marks): Multi-AZ/Region Failover & FinOps Cost-Governed Cloud Stack — Design, implement, test, and document 'Multi-AZ/Region Failover & FinOps Cost-Governed Cloud Stack' applying every production concept from Module 14 (Multi-Region Disaster Recovery, Observab...

MODULE 15 OF 16 • 14 LIVE + LAB HOURS • 3 TOPICS • 1 CAPSTONE PROJECT (100 MARKS)

AWS Cloud Security Governance, KMS Encryption & Cost FinOps Architecture

Self-explanatory list-and-bullet production mastery module covering AWS Cloud Security Governance, KMS Encryption & Cost FinOps Architecture in AWS Training, paired with hands-on labs, capstone repository, Topic Mock Tests, and Spoken Gemini AI Viva.

Objectives: ✓ AWS Organizations, Service Control Policies (SCPs), IAM Permission Boundaries & OIDC — Purpose: Enforce multi-account security guardrails and keyless CI/CD deployments without static access keys. • ✓ AWS KMS Customer-Managed Keys, Secrets Manager Rotation & WAF + Shield Protection — Purpose: Encrypt S3, EBS, and RDS data at rest and block SQLi/bot layer-7 attacks at CloudFront/ALB. • ✓ AWS Cost Explorer, Budgets, Savings Plans, S3 Intelligent-Tiering & Right-Sizing — Purpose: Prevent surprise cloud bills with automated anomaly alerts and storage/compute lifecycle rules. • ✓ Build, verify, and document 'Least-Privilege AWS Organization SCP, KMS Envelope Encryption & Budget Guard' with clean Git commits and edge-case protection. • ✓ Clear 100% of Topic Timed Mock Tests and Spoken Voice + Google Gemini AI Technical Interviews.

15.1 AWS Organizations, Service Control Policies (SCPs), IAM Permission Boundaries & OIDC [65 mins • Assignment (100M) • Hands-On Lab (50M) • 2 Mock Sets • 2 AI Vivas]

Purpose: To understand and apply AWS Organizations, Service Control Policies (SCPs), IAM Permission Boundaries & OIDC in real AWS systems — specifically: Enforce multi-account sec...

15.2 AWS KMS Customer-Managed Keys, Secrets Manager Rotation & WAF + Shield Protection [65 mins • Assignment (100M) • Hands-On Lab (50M) • 2 Mock Sets • 2 AI Vivas]

Purpose: To understand and apply AWS KMS Customer-Managed Keys, Secrets Manager Rotation & WAF + Shield Protection in real AWS systems — specifically: Encrypt S3, EBS, and RDS dat...

15.3 AWS Cost Explorer, Budgets, Savings Plans, S3 Intelligent-Tiering & Right-Sizing [65 mins • Assignment (100M) • Hands-On Lab (50M) • 2 Mock Sets • 2 AI Vivas]

Purpose: To understand and apply AWS Cost Explorer, Budgets, Savings Plans, S3 Intelligent-Tiering & Right-Sizing in real AWS systems — specifically: Prevent surprise cloud bills...

Module 15 Hands-On Capstone Project (100 Marks): Least-Privilege AWS Organization SCP, KMS Envelope Encryption & Budget Guard — Architect, implement, test, and document 'Least-Privilege AWS Organization SCP, KMS Envelope Encryption & Budget Guard' applying every bullet-wise engineering concept from Module 15 (AWS Clo...

MODULE 16 OF 16 • 14 LIVE + LAB HOURS • 3 TOPICS • 1 CAPSTONE PROJECT (100 MARKS)

AWS Well-Architected Disaster Recovery, Observability & SAA-C03 Scenarios

Self-explanatory list-and-bullet production mastery module covering AWS Well-Architected Disaster Recovery, Observability & SAA-C03 Scenarios in AWS Training, paired with hands-on labs, capstone repository, Topic Mock Tests, and Spoken Gemini AI Viva.

Objectives: ✓ Disaster Recovery Tiers: Backup & Restore, Pilot Light, Warm Standby & Multi-Site Active-Active — Purpose: Match exact RTO and RPO business targets to cost-effective AWS multi-region architectures. • ✓ Centralized Observability with CloudWatch Embedded Metrics, X-Ray Tracing & CloudTrail — Purpose: Correlate API latency, Lambda cold starts, and IAM audit trails during live incident triage. • ✓ AWS Solutions Architect Scenario Walkthroughs & Production Cutover Checklists — Purpose: Solve real SAA-C03 architecture trade-off questions across networking, storage, and serverless. • ✓ Build, verify, and document 'Multi-Region Failover Architecture Blueprint & CloudWatch Alarm Runbook' with clean Git commits and edge-case protection. • ✓ Clear 100% of Topic Timed Mock Tests and Spoken Voice + Google Gemini AI Technical Interviews.

16.1 Disaster Recovery Tiers: Backup & Restore, Pilot Light, Warm Standby & Multi-Site Active-Active [65 mins • Assignment (100M) • Hands-On Lab (50M) • 2 Mock Sets • 2 AI Vivas]

Purpose: To understand and apply Disaster Recovery Tiers: Backup & Restore, Pilot Light, Warm Standby & Multi-Site Active-Active in real AWS systems — specifically: Match exact RT...

16.2 Centralized Observability with CloudWatch Embedded Metrics, X-Ray Tracing & CloudTrail [65 mins • Assignment (100M) • Hands-On Lab (50M) • 2 Mock Sets • 2 AI Vivas]

Purpose: To understand and apply Centralized Observability with CloudWatch Embedded Metrics, X-Ray Tracing & CloudTrail in real AWS systems — specifically: Correlate API latency,...

16.3 AWS Solutions Architect Scenario Walkthroughs & Production Cutover Checklists [65 mins • Assignment (100M) • Hands-On Lab (50M) • 2 Mock Sets • 2 AI Vivas]

Purpose: To understand and apply AWS Solutions Architect Scenario Walkthroughs & Production Cutover Checklists in real AWS systems — specifically: Solve real SAA-C03 architecture...

Module 16 Hands-On Capstone Project (100 Marks): Multi-Region Failover Architecture Blueprint & CloudWatch Alarm Runbook — Architect, implement, test, and document 'Multi-Region Failover Architecture Blueprint & CloudWatch Alarm Runbook' applying every bullet-wise engineering concept from Module 16 (AWS Well-Arc...

3. LIVE CLIENT PRODUCTION PROJECT, GLOBAL CERTIFICATIONS & CAREER SCOPE

End-of-Course Live Client Production Project + Official Internship Confirmation Letter

Project: CloudShield Multi-AZ Auto-Scaling SaaS Infrastructure & Disaster Recovery Platform • **Confirmed Role:** AWS Cloud & Solutions Architecture Intern

Domain & Production Infra: Cloud-Native FinTech & SaaS Client Infrastructure (AWS VPC + ALB + EC2 Auto Scaling + RDS Multi-AZ + S3 + CloudFront + IAM)

- Designed custom multi-tier AWS VPC architecture across public/private subnets, NAT Gateways, and least-privilege IAM roles.
- Provisioned Application Load Balancers, Auto Scaling EC2/ECS workloads, and encrypted Multi-AZ RDS databases.
- Configured S3 lifecycle policies, CloudFront HTTPS edge distribution, Route 53 DNS failover, and CloudWatch alarms.
- Validated production readiness, cost governance budgets, and live client cutover on AWS cloud infrastructure.

Aligned Global Vendor Certifications: **CLF-C02** (AWS Certified Cloud Practitioner) • **SAA-C03** (AWS Certified Solutions Architect – Associate) • **DVA-C02** (AWS Certified Developer – Associate) • **SOA-C02** (AWS Certified SysOps Administrator – Associate)

Target Job Roles: AWS Cloud Engineer, Associate Solutions Architect, Cloud Operations (CloudOps) Engineer, Junior Site Reliability Engineer (SRE)

Realistic Annual CTC Scope: **Fresher / Entry-Level (0–1 Yr):** ₹5.0 LPA – ₹9.5 LPA **Mid-Level AWS Cloud / DevOps Engineer (1–3 Yrs):** ₹10.5 LPA – ₹21.0 LPA **AWS Solutions Architect / Principal SRE (3–6+ Yrs):** ₹22.0 LPA – ₹44.0+ LPA

MockAttempt Academy Pvt. Ltd. • Email: support@mockattempt.com • Phone/WhatsApp: +91 98765 43210 • Web: https://mockattempt.com/courses/aws-training

Try 2 Free Topic-Wise 50-MCQ Mock Tests & Spoken Gemini AI Interviews daily on every topic above before enrolling.