CLOUD COMPUTING AND INFRASTRUCTURE SECURITY USING AWS

4 WEEKS | 60 HOURS | ONLINE MODE | HANDS-ON | PROJECT BASED

Course Start:- 10 November 2026 | Fee 1,800/-

Duration 4 Weeks / 60 Hours Mode Online

Focus Linux • Networking • AWS • Cloud Security Format Practical labs and final project

Course Overview

This course introduces cloud computing and AWS infrastructure, with a practical focus on deploying, configuring, monitoring and securing cloud resources. Participants work with core AWS services and learn security-oriented practices for identity, networking, storage, compute, monitoring and project deployment.

Course Objectives

- Understand cloud computing concepts, service models and AWS global infrastructure.
- Build and configure virtual networks using Amazon VPC, subnets, route tables and gateways.
- Launch and manage EC2 instances, S3 storage, RDS databases and load balancers.
- Apply IAM controls, MFA, least-privilege access, security groups, encryption and secure configuration practices.
- Monitor AWS resources and activity using CloudWatch and CloudTrail, while keeping cost awareness in view.
- Deploy and secure a small AWS infrastructure project using the concepts covered in the course.

Who Should Join? — Eligibility

B.E.*/B.Tech.* (in Any Stream), MCA*/BCA*/B.Sc.* (IT/CS)/M.Sc.* (IT/CS), Diploma* (CS/IT), NIELIT A Level and NIELIT O Level (*pursuing candidate may also apply) OR Professional/Official with Graduation (in Any Stream) and working in relevant domain, having knowledge of Computer Networking and Operating System.

Prerequisites

- A computer or laptop with at least 4 GB RAM.
- A valid credit or debit card, email ID and mobile number may be required for AWS account registration and verification.
- A reliable internet connection (preferably 2 Mbps or higher).
- Participants are responsible for monitoring AWS usage and any charges beyond applicable Free Tier limits.

Important AWS Free Tier Note

AWS Free Tier has usage limits. Students must monitor their usage and any charges incurred beyond Free Tier limits. NIELIT WILL NOT PAY OR REIMBURSE ANY AWS CHARGES INCURRED BY STUDENTS. How to Apply

Step 1: Read the course details, eligibility and prerequisites carefully.

Step 2: Visit the course registration page and select the course.

Step 3: Create or log in to your registration account, complete the form and review details before submission.

Step 4: Complete required verification, upload requested documents and follow the portal instructions for payment.

DETAILED DAY-WISE CURRICULUM — DAYS 1–10

Each day includes key topics, a guided practical activity and a tangible learning output. Practical activities depend on lab access and should use controlled AWS resources.

DAY 01 — Computer Fundamentals and Virtualization

Topics covered: Cloud computing prerequisites; hardware, CPU, memory, storage and operating-system basics; client/server model; purpose of virtualization; virtual machines and hypervisors; types of virtualization (server, network, storage and OS); overview of VMware/Hyper-V and virtualized environments.

Hands-on / guided activity: Identify the components of a computer and draw a simple client/server model. Explore VM settings such as CPU, RAM, disk and network adapter in an available virtualization tool.

Expected output: A labelled infrastructure diagram and a short comparison of physical machines and virtual machines.

DAY 02 — Linux Fundamentals I — Environment and Commands

Topics covered: Linux distributions and common use cases; terminal and shell; filesystem hierarchy; absolute and relative paths; navigation commands (pwd, ls, cd); file and directory operations (touch, mkdir, cp, mv, rm); viewing files (cat, less, head, tail); help pages; basic text editing; command chaining and redirection.

Hands-on / guided activity: Navigate a Linux filesystem, create a practice directory structure, create/copy/move files, inspect command output and save selected output to a text file.

Expected output: A command log showing directory navigation, file operations and basic shell usage.

DAY 03 — Linux Fundamentals II — Users, Permissions and Administration

Topics covered: User and group concepts; account and group management; passwd and password practices; ownership with chown; permissions with chmod; read/write/execute permissions; sudo; process and disk inspection basics; package managers and repositories; basic interface and DNS configuration; overview of ACLs.

Hands-on / guided activity: Create sample files and directories, inspect permissions, change file ownership/permissions in a lab, review running processes and practise safe administrative commands.

Expected output: A checklist demonstrating user/group concepts, file permissions and common administrative commands.

DAY 04 — Networking Fundamentals I — Models and Addressing

Topics covered: Network types and topologies; network devices (switch, router, hub, repeater); client/server and peer-to-peer models; Ethernet and MAC addresses; OSI reference model; TCP/IP model; TCP vs UDP; ports and common protocols; IPv4 structure; public and private IP addresses; basic subnet masks.

Hands-on / guided activity: Map common protocols to layers and ports, inspect the local IP configuration and identify the default gateway and DNS server.

Expected output: A network reference sheet containing OSI/TCP-IP layers, protocol examples and IP configuration.

DAY 05 — Networking Fundamentals II — Subnetting and Troubleshooting

Topics covered: Subnet masks and CIDR notation; subnetting concepts; network, host and broadcast addresses; DNS and name resolution; DHCP; routing and default gateways; NAT; VPN concepts; firewalls; troubleshooting with ping, traceroute/tracert, ipconfig/ip, arp, netstat and nslookup.

Hands-on / guided activity: Calculate basic subnet ranges, test connectivity to a gateway, trace a route and use DNS lookup tools to diagnose sample connectivity issues.

Expected output: A small subnetting worksheet and documented results from basic network troubleshooting.

DAY 06 — Cloud Computing and AWS Fundamentals

Topics covered: Cloud computing definition, benefits and limitations; IaaS, PaaS and SaaS; public, private and hybrid cloud concepts; cloud-provider overview; introduction to AWS services and terminology; AWS global infrastructure (Regions, Availability Zones and edge locations); AWS Management Console; Shared Responsibility Model; Free Tier usage limits and account safety.

Hands-on / guided activity: Navigate the AWS Management Console or instructor demonstration; identify Regions and Availability Zones; classify sample services by purpose and service model.

Expected output: A cloud service-model comparison and an AWS service/infrastructure map.

DAY 07 — AWS Account Security, IAM and Cost Awareness

Topics covered: Root user risks and protection; IAM users, groups, roles and policies; identity-based permissions; least privilege; MFA; secure credentials; access-key safety; AWS Organizations overview; billing dashboard; budgets, Cost Explorer and billing alerts; account hygiene and resource cleanup.

Hands-on / guided activity: Review IAM examples and permissions; create or inspect a lab user/role when permitted; demonstrate MFA and locate billing/cost tools without creating unnecessary paid resources.

Expected output: An IAM access-control worksheet and a cost-monitoring checklist.

DAY 08 — Amazon VPC I — Network Design

Topics covered: Virtual Private Cloud purpose and components; IPv4 CIDR planning; public and private subnets; route tables and routes; Internet Gateway; NAT Gateway concept and cost awareness; availability-zone placement; network diagrams and traffic flow.

Hands-on / guided activity: Design a simple VPC addressing plan and, in a controlled lab if available, create or inspect a VPC, subnets and route tables.

Expected output: A labelled VPC diagram showing CIDR, subnets, gateways and route paths.

DAY 09 — Amazon VPC II — Network Security and Connectivity

Topics covered: Security groups as stateful controls; network ACLs; inbound/outbound rules; principle of least exposure; VPC endpoints; VPC peering; VPN overview; VPC Flow Logs; secure administration access; common misconfiguration risks.

Hands-on / guided activity: Review sample security-group and network ACL rules, restrict a sample workload to required traffic and inspect VPC Flow Logs in a demonstration.

Expected output: A secure network-rule set with brief justifications for permitted ports and sources.

DAY 10 — Amazon EC2 I — Instance Launch and Access

Topics covered: EC2 use cases and instance families; Amazon Machine Images; instance sizing; key pairs; launch settings; public/private addressing; instance states; security groups; Linux and Windows access concepts; metadata and basic monitoring.

Hands-on / guided activity: Walk through launching or planning an EC2 instance using an approved lab account; choose an AMI and size, configure storage and networking, and review access settings before launch.

Expected output: An EC2 deployment checklist with AMI, instance type, network, key-pair and security-group selections.

DETAILED DAY-WISE CURRICULUM — DAYS 11–20

Each day includes key topics, a guided practical activity and a tangible learning output. Practical activities depend on lab access and should use controlled AWS resources.

DAY 11 — Amazon EC2 II — Storage and Web Server Basics

Topics covered: Elastic IP concepts; user data and bootstrap scripts; EBS volumes and snapshots; volume attachment; instance recovery and termination protection; basic Linux/Windows administration; web server concepts; patching and safe shutdown/termination.

Hands-on / guided activity: In a controlled lab, connect to a test instance, inspect attached storage, demonstrate a simple web server or review its deployment, then stop or clean up resources.

Expected output: A short EC2 operations record including access, storage and cleanup steps.

DAY 12 — AWS Storage Services — S3, EBS and EFS

Topics covered: Object, block and file storage; S3 buckets and objects; bucket access settings and public-access blocking; versioning; lifecycle rules and storage classes; encryption options; EBS block volumes; EFS shared file storage; archive/backup use cases; AWS CLI overview.

Hands-on / guided activity: Create or inspect a practice S3 bucket, upload a non-sensitive sample file, review permissions and versioning, and compare when S3, EBS or EFS is appropriate.

Expected output: A storage comparison table and an S3 configuration checklist.

DAY 13 — AWS Database Services — RDS and NoSQL Overview

Topics covered: Relational database concepts; Amazon RDS use cases; DB instance configuration and network placement; database credentials and access controls; security groups; backups and restore; Multi-AZ and read replicas; overview of Aurora, DynamoDB, Redshift and ElastiCache.

Hands-on / guided activity: Design a secure database placement inside a VPC; identify which application components require database access and review backup and availability settings.

Expected output: A database architecture sketch with access boundaries and backup/availability notes.

DAY 14 — Load Balancing and Auto Scaling

Topics covered: Elastic Load Balancing purpose and types; Application Load Balancer concepts; listeners and target groups; health checks; TLS/SSL certificate use; Auto Scaling groups and policies; high availability; capacity planning and cost awareness.

Hands-on / guided activity: Draw traffic flow from users to a load balancer and EC2 targets; review health-check behaviour and identify how Auto Scaling responds to demand.

Expected output: A high-level scalable application diagram and a load-balancer configuration checklist.

DAY 15 — Route 53 and Application Services

Topics covered: DNS and hosted zones; common record types; Route 53 routing policy concepts (simple, weighted, latency, failover and geolocation); domain registration overview; Amazon SNS, SQS, SES, Lambda and API Gateway use cases; event-driven and serverless basics.

Hands-on / guided activity: Map a sample domain to a service using a conceptual Route 53 setup and choose appropriate notification, queue or serverless services for example scenarios.

Expected output: A DNS/routing worksheet and a service-selection exercise.

DAY 16 — Monitoring, Logging and Audit

Topics covered: Amazon CloudWatch metrics, logs, dashboards and alarms; monitoring EC2 and other resources; CloudTrail event history and audit logs; difference between operational metrics and API activity records; alerting basics; log review and troubleshooting workflow.

Hands-on / guided activity: Identify useful metrics for an EC2 workload, draft an alarm threshold, review example CloudTrail events and trace an example configuration change.

Expected output: A basic monitoring plan listing metrics, alarms, audit events and response steps.

DAY 17 — Infrastructure Security Practices

Topics covered: AWS Shared Responsibility Model review; identity security and least privilege; MFA and credential protection; secure network design; security groups and NACLs; data classification; encryption in transit and at rest; secure S3 configuration; logging, monitoring and security-service overview; configuration review.

Hands-on / guided activity: Conduct a guided security review of a sample AWS design and record exposed ports, overly broad permissions, storage risks and missing monitoring.

Expected output: A prioritized security checklist with recommended remediations.

DAY 18 — Backup, Recovery and Cost Control

Topics covered: Backup principles and recovery objectives; EBS snapshots; S3 versioning and lifecycle rules; database backups; restore considerations; off-site and cross-Region concepts; cost drivers; budgets and Cost Explorer; tags; stopping/terminating unused lab resources.

Hands-on / guided activity: Create a backup and recovery plan for a sample workload, identify cost-risk resources and prepare a resource-cleanup checklist.

Expected output: A backup matrix and a basic AWS cost-control checklist.

DAY 19 — Final Project — Deploy the Infrastructure

Topics covered: Project planning and requirements; choose a simple use case; architecture and network diagram; VPC and subnet design; IAM roles and permissions; EC2 deployment; S3 storage; optional RDS or load balancer based on scope; documentation and testing plan.

Hands-on / guided activity: Build or simulate the agreed project using only approved lab resources. Validate connectivity and confirm that resources follow the intended architecture.

Expected output: A working or demonstrable AWS architecture with initial deployment notes.

DAY 20 — Final Project — Secure, Monitor and Present

Topics covered: Review least-privilege access; network exposure; storage access and encryption; monitoring with CloudWatch; audit visibility with CloudTrail; backup and recovery notes; cost review; architecture documentation; test evidence and project presentation.

Hands-on / guided activity: Run a final configuration review, demonstrate the deployed design, show monitoring/audit evidence, explain key security decisions and clean up resources when finished.

Expected output: A final project presentation/report with architecture diagram, security checklist, monitoring evidence and cleanup confirmation.

DETAILED COURSE CONTENT — PART I

The detailed syllabus expands the main topics covered in the day-wise plan.

1. Computer Fundamentals and Virtualization

Computer fundamentals relevant to cloud use; virtualization concepts and benefits; hardware, network, operating-system and storage virtualization; virtual machines; hypervisors; overview of VMware/Hyper-V and virtualized infrastructure.

2. Linux Fundamentals

Linux file system and shell; command-line utilities; working with files and directories; text editing; user and group administration; password management; permissions and ownership; ACL concepts; sudo; network interface and DNS configuration; package management.

3. Networking Fundamentals

Network types and components; client/server model; switches, routers, hubs and repeaters; LAN and internetworking basics; Ethernet; OSI and TCP/IP models; ports; TCP/UDP; MAC and IP addressing; public/private addresses; subnet masks; CIDR and subnetting; DNS, DHCP, routing, NAT, VPN concepts and troubleshooting utilities such as ping, traceroute, netstat and nslookup.

4. Cloud Computing and AWS

Cloud computing concepts, advantages and service models (IaaS, PaaS and SaaS); cloud provider overview; AWS services and terminology; AWS global infrastructure; Regions, Availability Zones and edge locations; AWS Management Console; AWS Shared Responsibility Model; AWS account setup and Free Tier awareness; launching introductory Linux and Windows EC2 instances.

5. Identity and Access Management (IAM)

AWS root account security; IAM users, groups, roles and policies; permissions and least privilege; multi-factor authentication (MFA); credential and account settings; role assignment; account security practices; billing dashboard, budgets, Cost Explorer and cost alerts.

6. Amazon Virtual Private Cloud (VPC)

VPC concepts and use cases; CIDR notation; public and private subnets; route tables; Internet Gateway and NAT Gateway; security groups and network ACLs; VPC endpoints; VPC peering; VPN overview; VPC Flow Logs and network isolation principles.

Hands-on Activities

- Use Linux commands to manage files, users, groups and permissions.
- Practise IP addressing, subnetting and basic network troubleshooting.
- Review IAM users, roles and policies; enable MFA where available.
- Create a VPC with subnets and routing components in a controlled lab environment.

DETAILED COURSE CONTENT — PART II

7. Amazon EC2 — Compute

EC2 instance categories and types; Amazon Machine Images (AMIs); instance launch and lifecycle; key pairs and secure access; public and Elastic IP addresses; instance metadata and user data; security groups; EBS volumes and snapshots; instance termination protection; basic Linux/Windows access; deploying a simple web server.

8. AWS Storage Services

Amazon S3 buckets and objects; bucket configuration and access control; static website hosting overview; object versioning; lifecycle rules and storage classes; cross-Region replication overview; EBS block storage; EFS shared file storage; archive and backup use cases; AWS CLI overview for storage tasks.

9. AWS Database Services

Amazon RDS concepts and use cases; database instance configuration; database access security; storage and instance classes; backups and restore; Multi-AZ deployment and read replicas; overview of Aurora, DynamoDB, Redshift and ElastiCache.

10. Load Balancing, Auto Scaling and Route 53

Elastic Load Balancing and target groups; health checks; Application Load Balancer concepts; SSL/TLS certificates; Auto Scaling fundamentals; Route 53 hosted zones and DNS records; simple, weighted, latency, failover and geolocation routing concepts.

11. Application and Notification Services

Overview and use cases of Amazon SNS, SQS, SES, Lambda and API Gateway; event-driven and serverless application concepts; identifying appropriate services for simple workloads.

12. Monitoring, Logging and Audit

Amazon CloudWatch metrics, logs, dashboards and alarms; AWS CloudTrail event history and audit trails; monitoring compute and network resources; using logs to support troubleshooting and security review.

13. Infrastructure Security and Best Practices

AWS Shared Responsibility Model; identity and access controls; MFA and least privilege; security groups and network ACLs; secure storage permissions; data protection and encryption concepts; logging and monitoring; backup and recovery; security services overview; cost and resource hygiene.

14. Final Project — Deploy and Secure AWS Infrastructure

Design and deploy a small AWS environment using suitable services such as VPC, EC2, IAM, S3, RDS and Load Balancer. Apply secure access and network settings, configure monitoring with CloudWatch and audit visibility with CloudTrail, review resource costs, document the architecture and demonstrate the deployment.

Certificate Criteria

You will receive the digital certificate only after completing the course.

The previous course form specified a certificate based on minimum 75% attendance and at least 50% marks in an end-of-course online test conducted by NIELIT Gorakhpur. Confirm the final assessment and certificate criteria with the course team before publishing. Course Details and Application

Apply Now: https://regn.nielitvte.edu.in/m/m-courseinfo.php?ci=283
Course Coordinator: Sh. Abhinav Mishra, Scientist D, NIELIT Gorakhpur
Course Instructor: Sh. Satyam Singh, Project Associate, NIELIT Gorakhpur | 7706816329
Course Start: 10 November 2026 | Mode: Online | Fee: 1,800/-

Course highlights: Linux and networking included • Security-oriented AWS training • Practical sessions • Real-time cloud labs • Live project • AWS best practices • Certificate of completion subject to the announced criteria.