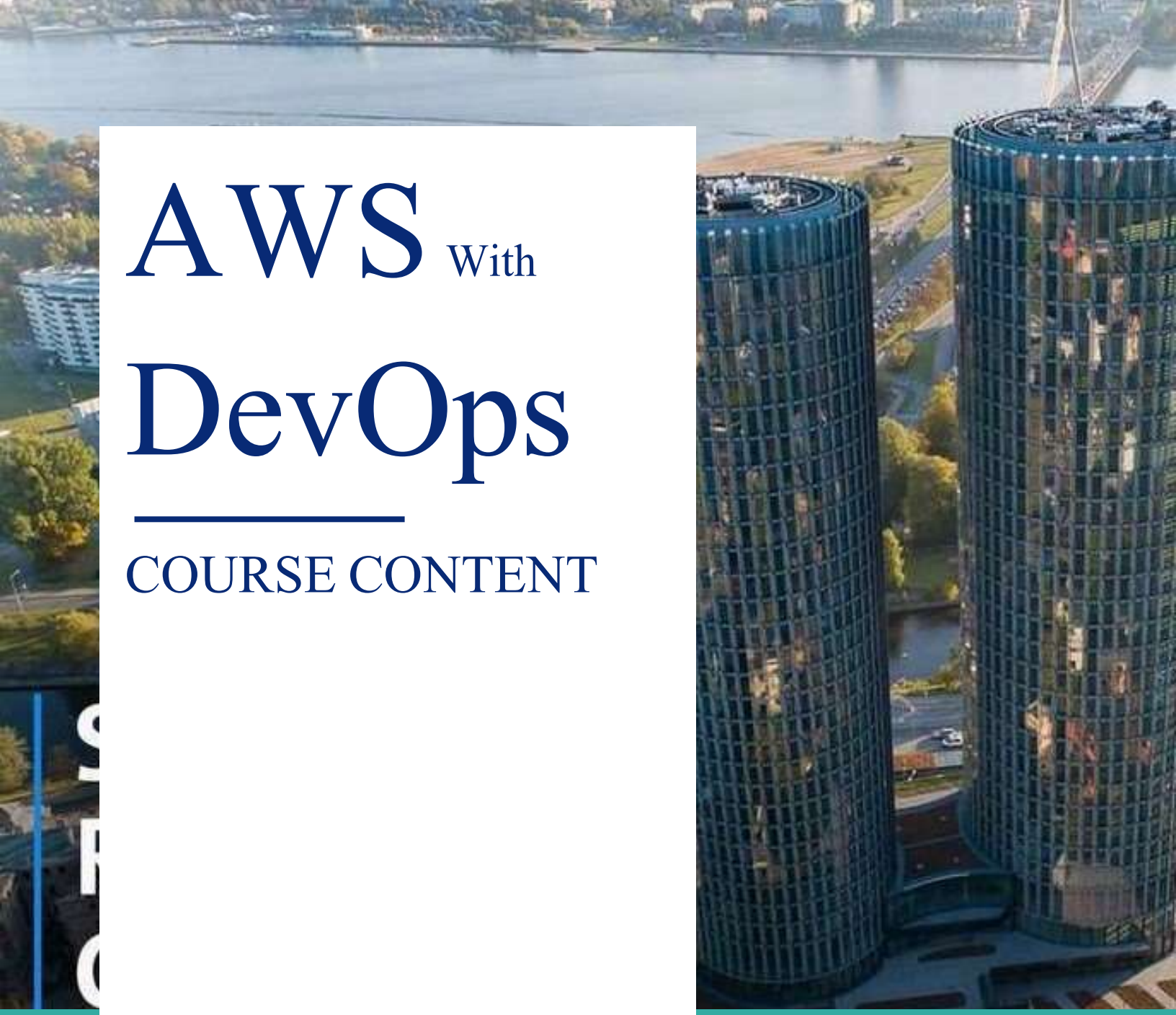

AWS With DevOps

COURSE CONTENT

Lan Edu Center

Address: 506, 5th floor, Manjeera Majestic Commercial, Opp JNTU Road, KPHB Colony, Kukatpally, Hyderabad,
Telangana 500072.

Call: +91-939 254 7028 / +91-963 222 9846

Lan Edu Center

About me,

Anil Kumar,

Dear Candidate,

Thanks for connecting

Having 9+ Years of Experience in IT, Having 6+ Years' Experience into (AWS + GCP + DevOps).

During the entire training program candidates will be allowed to use our communication channels like slack, Microsoft teams etc and will be working as a team member to experience the real time environment.

DevOps is emerging as a revolution in IT industry which has completely changed the process of software development. The benefits that DevOps provides to businesses has forced small to big organizations to move their software development process to DevOps methodology. This new change in industry has increased the demand of DevOps professionals and every company is looking for DevOps professionals with very good salary hike. We observed salary hike going up to 300% for DevOps professionals.

We have designed our DevOps learning program in a way that will not create any problem for candidates working in any time zone. We offer candidates live online as well as self-paced learning modes of training which have the same content and processes to follow. Whether the candidate has opted for live online or self-paced mode he/she must be involved in completing the assignments and work as a team member during the project demo.

DevOps & Cloud Roadmap Syllabus

Module 1: Introduction to DevOps and Version Control

- DevOps Overview
  - What is DevOps? Principles, goals, and benefits
  - DevOps lifecycle and stages
  - Key DevOps practices: Continuous Integration (CI), Continuous Deployment (CD), Infrastructure as Code (IaC), and Monitoring
- Git & GitHub
  - Introduction to version control with Git
  - Git basics: Cloning, committing, branching, merging, and rebasing
  - Collaboration with Git: Pull requests, branching strategies, and resolving conflicts
  - GitHub for collaboration: Repositories, issues, pull requests, and GitHub Actions for CI/CD
  - Hands-on: Create a repository, commit changes, and set up a GitHub repo with multiple collaborators

---

Module 2: Build and Dependency Management

- Maven
  - Introduction to Apache Maven and its role in DevOps
  - Understanding Maven build lifecycle, goals, and phases
  - Configuring and managing project dependencies with pom.xml
  - Building, testing, and packaging Java applications using Maven
  - Hands-on: Setting up Maven in a Java project, running build commands, and creating a WAR/JAR file
- SonarQube
  - Introduction to SonarQube for static code analysis
  - Setting up SonarQube server and integrating with Maven for continuous code quality checks
  - Understanding code quality metrics, issues, and reporting
  - Configuring SonarQube to detect bugs, vulnerabilities, and code smells

- Hands-on: Set up SonarQube with Maven integration and perform static code analysis

- Nexus Repository Manager
  - Overview of Nexus for managing repositories (Artifacts, dependencies, and containers)
  - Setting up a local Maven repository with Nexus
  - Using Nexus to manage Java libraries and Docker images
  - Hands-on: Configure Nexus to store and retrieve artifacts and Docker images

---

Module 3: Continuous Integration and Continuous Delivery

- Jenkins
  - Introduction to Jenkins for automation of build and deployment pipelines
  - Setting up Jenkins master and slave nodes
  - Creating Jenkins pipelines using declarative and scripted syntax
  - Integrating Jenkins with GitHub, Maven, SonarQube, and Docker
  - Continuous Integration and Continuous Deployment concepts
  - Hands-on: Setting up a Jenkins pipeline for building and deploying a Java application
- Tomcat (Web Server)
  - Introduction to Tomcat as an application server for Java web apps
  - Deploying Java web applications (WAR files) to Tomcat using Jenkins
  - Managing Tomcat with Jenkins for continuous deployment
  - Hands-on: Deploy a Maven-built application to Tomcat through Jenkins

---

Module 4: Configuration Management & Automation

- Ansible
  - Introduction to Ansible and its role in configuration management
  - Ansible architecture: Inventory, playbooks, modules, and roles
  - Writing and running Ansible playbooks to automate server setup
  - Using Ansible to install and configure software (e.g., Docker, Tomcat)
  - Hands-on: Write an Ansible playbook to automate the installation of a web server (e.g., Nginx, Tomcat)

Module 5: Containerization and Orchestration

- Docker
  - Introduction to Docker and containerization
  - Building Docker images from Dockerfiles
  - Running and managing containers
  - Docker Compose for multi-container applications
  - Hands-on: Create a Docker image for a simple application and run it as a container
- Kubernetes
  - Introduction to Kubernetes for container orchestration
  - Kubernetes architecture: Pods, nodes, deployments, services, and namespaces
  - Deploying and managing applications with Kubernetes
  - Scaling applications and managing updates in Kubernetes
  - Hands-on: Deploy a Dockerized application on a Kubernetes cluster (using kubectl)

Module 6: Infrastructure as Code (IaC) and Cloud Automation

- Linux Basics for DevOps
  - Understanding Linux commands and file system navigation
  - Managing users, groups, and permissions
  - Networking, process management, and logs
  - Hands-on: Basic Linux commands for server management
- Terraform
  - Introduction to Terraform for Infrastructure as Code (IaC)
  - Writing Terraform configuration files (HCL)
  - Using providers and resources to create cloud infrastructure (AWS, Azure, GCP)
  - Managing and updating infrastructure with Terraform
  - Hands-on: Write a Terraform script to provision an EC2 instance on AWS

Module 7: Monitoring and Logging

- Prometheus
  - Introduction to Prometheus for monitoring applications and infrastructure
  - Setting up Prometheus server and exporters for metrics collection
  - Creating alerts and visualizing data
  - Hands-on: Set up Prometheus to monitor a Docker container and create an alert
- Grafana
  - Introduction to Grafana for data visualization and dashboards
  - Integrating Grafana with Prometheus for metrics visualization
  - Creating interactive dashboards for monitoring application health
  - Hands-on: Set up a Grafana dashboard to visualize metrics collected by Prometheus

---

Module 8: DevOps in Practice

- CI/CD Pipeline Implementation
  - Setting up a complete CI/CD pipeline using Git, Maven, Jenkins, SonarQube, Nexus, Docker, and Tomcat
  - Automating code quality checks, building, testing, and deploying applications
  - Hands-on: Create a Jenkins pipeline that pulls code from GitHub, builds with Maven, checks with SonarQube, stores artifacts in Nexus, and deploys to Tomcat
- Advanced Docker and Kubernetes Deployment
  - Deploying microservices on Kubernetes with Docker
  - Managing deployment strategies: Rolling, Blue-Green, Canary deployments
  - Hands-on: Create and deploy multi-container microservices using Kubernetes and Docker Compose
- Monitoring and Troubleshooting
  - Setting up Prometheus, Grafana, and ELK Stack for full-stack monitoring
  - Troubleshooting Kubernetes and Docker containers
  - Hands-on: Set up monitoring and alerts for a containerized application

---

Module 9: Best Practices and DevOps Culture

- DevOps Best Practices
  - Version control strategies (Git flow, feature branches)
  - Automated testing and deployment best practices
  - Configuration management and automation best practices
  - Scaling and high availability strategies for microservices and applications
- DevOps Culture
  - The role of collaboration, communication, and feedback in DevOps
  - Implementing a continuous feedback loop for improvements
  - The importance of monitoring, feedback, and iteration in the DevOps cycle

---

Capstone Project

- Final Project
  - Implement a full DevOps pipeline with Git, Maven, Jenkins, Docker, Kubernetes, and Terraform
  - Automate deployment to a cloud infrastructure (AWS, GCP, or Azure)
  - Monitor and troubleshoot application performance with Prometheus and Grafana

---

Tools Covered:

- Version Control : Git, GitHub
- Build & Dependency Management : Maven, Nexus
- Continuous Integration : Jenkins
- Code Quality : SonarQube
- Automation : Ansible, Terraform
- Containers & Orchestration : Docker, Kubernetes
- Web Server : Tomcat
- Monitoring & Visualization : Prometheus, Grafana
- Operating System : Linux basics

Module 1: Introduction to AWS and VPC Basics

- Overview of AWS Cloud Infrastructure

- What is AWS? Key services and their roles
- AWS Global Infrastructure: Regions, Availability Zones, Edge Locations

- Amazon VPC (Virtual Private Cloud) Basics
  - Overview of VPC and its components
  - Subnets, route tables, and internet gateway
  - VPC CIDR block and IP addressing
  - Security groups vs NACLs (Network Access Control Lists)
  - Hands-on: Create a VPC with public and private subnets

Module 2: Advanced VPC Networking

- Private vs Public Subnets
  - Configuring public and private subnets in VPC
  - Security considerations and best practices
- Internet Gateway (IGW) and NAT Gateway
  - How to enable internet access for instances in private subnets using NAT Gateway
  - Configuring NAT Gateway for high availability and fault tolerance
  - Hands-on: Configure a VPC with NAT Gateway to provide internet access for instances in private subnets
- VPC Peering
  - What is VPC Peering and how does it work?
  - Configuring VPC peering between two VPCs
  - Limitations of VPC peering (transitive peering, CIDR conflicts)
  - Hands-on: Set up VPC peering and route traffic between peered VPCs

---

Module 3: Transit Gateway and VPC Endpoints

- AWS Transit Gateway
  - Overview of AWS Transit Gateway for centralizing VPC connections
  - Benefits of using Transit Gateway over VPC Peering for large-scale architectures
  - Setting up and configuring Transit Gateway

- Managing route tables and attachments in Transit Gateway
- Hands-on: Set up AWS Transit Gateway to connect multiple VPCs

- VPC Endpoints
  - What are VPC Endpoints and how do they improve security and performance?
  - Types of VPC Endpoints: Interface Endpoints (PrivateLink) and Gateway Endpoints (S3, DynamoDB)
  - Configuring VPC Endpoints for S3 and DynamoDB
  - Best practices for using VPC endpoints to access AWS services securely
  - Hands-on: Create VPC Endpoints for S3 and DynamoDB

Module 4: Amazon S3 (Simple Storage Service)

- Introduction to Amazon S3
  - What is S3? Key features and use cases
  - S3 buckets, objects, and naming conventions
  - S3 storage classes (Standard, Intelligent-Tiering, Glacier, etc.)
  - Hands-on: Create and manage S3 buckets, upload and retrieve objects
- S3 Security and Access Control
  - S3 Bucket Policies and IAM roles
  - S3 Access Control Lists (ACLs)
  - Encryption: SSE (Server-Side Encryption) and client-side encryption
  - Hands-on: Set up S3 bucket policies, configure encryption, and control access using IAM

Module 5: Identity and Access Management (IAM)

- IAM Basics
  - Overview of IAM and its importance in AWS security
  - Creating and managing users, groups, and roles
  - Best practices for IAM policies and permissions
  - Multi-Factor Authentication (MFA) in AWS
  - Hands-on: Create IAM users, groups, roles, and attach policies

- IAM for Resource Access Control
  - Fine-grained access control using IAM policies (JSON policies)
  - Role-based access control (RBAC)
  - Integrating IAM with other AWS services (S3, EC2, Lambda)
  - Hands-on: Configure IAM policies and roles for secure access to resources

---

Module 6: Event-Driven Architectures with EventBridge

- Amazon EventBridge
  - Overview of EventBridge and event-driven architectures
  - Use cases: Real-time data streaming, serverless applications, and microservices
  - EventBridge components: Event buses, rules, and targets
  - Integrating EventBridge with other AWS services (Lambda, Step Functions, SQS)
  - Hands-on: Create an EventBridge event bus and set up a rule to trigger a Lambda function

---

Module 7: Content Delivery and Caching with CloudFront

- Amazon CloudFront
  - What is CloudFront and how does it work?
  - Overview of edge locations, caching, and distribution
  - Setting up CloudFront distributions for static and dynamic content
  - Integration with S3 for content delivery
  - Hands-on: Configure a CloudFront distribution to deliver content from S3
- CloudFront Security
  - SSL/TLS encryption with CloudFront
  - Configuring Geo-blocking and access control
  - Hands-on: Set up HTTPS for a CloudFront distribution and restrict access

---

Module 8: Monitoring and Auditing with CloudTrail and CloudWatch

- Amazon CloudTrail

- Overview of CloudTrail and its importance for auditing and compliance
- Tracking API activity and user actions
- Configuring CloudTrail to capture logs for all regions
- Integrating CloudTrail with CloudWatch Logs for advanced monitoring
- Hands-on: Set up CloudTrail to monitor and audit AWS API calls

- Amazon CloudWatch
  - Introduction to CloudWatch for monitoring AWS resources and applications
  - Metrics, logs, and alarms in CloudWatch
  - Setting up CloudWatch Dashboards and custom metrics
  - CloudWatch Logs for troubleshooting and log aggregation
  - Hands-on: Create CloudWatch alarms to monitor EC2 instances, set up custom metrics and logs

---

Module 9: Network Security with NACLs, Security Groups, and Flow Logs

- Network Access Control Lists (NACLs)
  - Overview of NACLs and their role in VPC security
  - Configuring inbound and outbound rules in NACLs
  - Difference between NACLs and Security Groups
  - Hands-on: Configure NACLs to control traffic to/from VPC subnets
- Security Groups
  - Introduction to Security Groups for instance-level security
  - Stateful vs Stateless security rules
  - Best practices for managing Security Groups in AWS
  - Hands-on: Set up Security Groups to secure EC2 instances and services
- VPC Flow Logs
  - Overview of VPC Flow Logs for capturing network traffic data
  - Using Flow Logs for network troubleshooting and security analysis
  - Storing VPC Flow Logs in CloudWatch Logs or S3
  - Hands-on: Enable and analyze VPC Flow Logs for traffic insights

---

Module 10: Best Practices and Real-World Scenarios

- VPC Design Best Practices
  - Designing VPCs for high availability and fault tolerance
  - Subnet strategies, private and public subnet isolation
  - Peering, Transit Gateway, and VPC Endpoints for optimal performance
- Security Best Practices
  - Securing resources with IAM, VPC security, and encryption
  - Implementing least privilege access with IAM policies
  - Using VPC Flow Logs and CloudTrail for continuous monitoring
- Cost Optimization and Scaling
  - Cost management strategies for networking (e.g., NAT Gateway pricing, data transfer costs)
  - Auto-scaling architectures for optimal resource utilization
  - Hands-on: Architect a secure and cost-effective AWS solution

---

Capstone Project

- Final Project
  - Design and implement a secure, highly available VPC architecture using all the learned services
  - Configure multiple VPCs with Transit Gateway, VPC Peering, and Endpoints
  - Implement IAM roles, CloudTrail, and CloudWatch for monitoring and auditing
  - Secure and optimize S3, CloudFront, and EventBridge for a scalable application
  - Deliverables: A fully functional VPC with monitoring, security, and event-driven components

---

Tools and Services Covered:

- VPC (Virtual Private Cloud)
- NAT Gateway , VPC Peering , Transit Gateway
- VPC Endpoints (S3, DynamoDB)
- S3 (Simple Storage Service)

- IAM (Identity and Access Management)
- EventBridge
- CloudFront (Content Delivery Network)
- CloudTrail (Logging & Auditing)
- CloudWatch (Monitoring & Logging)
- NACL (Network Access Control List)
- VPC Flow Logs (Network Monitoring)

Module 1: Introduction to AWS and VPC Basics

- Overview of AWS Cloud
  - Understanding AWS Global Infrastructure: Regions, Availability Zones, Edge Locations
  - Key AWS Services for Cloud Computing
  - Virtual Private Cloud (VPC) Overview
- Amazon VPC (Virtual Private Cloud)
  - Introduction to VPC: Subnets, Route Tables, and Internet Gateway (IGW)
  - VPC CIDR Block Design: Public and Private IPs
  - Setting up VPC with Public and Private Subnets
  - Hands-on: Creating a VPC, Subnets, and Configuring Route Tables

---

Module 2: Networking Components in AWS

- NAT Gateway and Internet Gateway
  - What is a NAT Gateway and how it works
  - Configuring NAT Gateway to allow internet access for private instances
  - When to use NAT Gateway vs Internet Gateway
  - Hands-on: Setting up NAT Gateway for private subnet internet access
- VPC Peering
  - What is VPC Peering and how does it work?
  - Configuring VPC Peering between two VPCs
  - Route tables and traffic flow between peered VPCs

- Hands-on: Create VPC Peering and route traffic between peered VPCs

- AWS Transit Gateway
  - Overview of Transit Gateway for simplifying VPC interconnection
  - Configuring and managing Transit Gateway
  - Hands-on: Set up Transit Gateway to interconnect multiple VPCs

---

Module 3: VPC Endpoints

- Introduction to VPC Endpoints
  - What are VPC Endpoints and how do they improve security and performance?
  - Types of VPC Endpoints: Interface and Gateway Endpoints
  - Benefits of using VPC Endpoints (Private connectivity to S3, DynamoDB, etc.)
  - Hands-on: Setting up Gateway Endpoints for S3 and DynamoDB

Module 4: Amazon S3 and Storage Services

- Amazon S3 (Simple Storage Service)
  - Overview of S3 and use cases
  - S3 Buckets, Objects, and Versioning
  - S3 Storage Classes (Standard, Glacier, etc.)
  - Hands-on: Create S3 buckets and manage objects (upload, retrieve, delete)
- Elastic Block Store (EBS)
  - Overview of EBS and EBS volumes
  - EBS Volume types (General Purpose SSD, Provisioned IOPS, Magnetic)
  - Attaching and managing EBS volumes to EC2 instances
  - Hands-on: Create and attach EBS volumes to EC2 instances
- Elastic File System (EFS)
  - Overview of EFS for scalable file storage
  - Configuring and mounting EFS to EC2 instances
  - Use cases for EFS vs EBS
  - Hands-on: Set up and mount an EFS file system to EC2 instances

Module 5: Identity and Access Management (IAM)

- IAM Overview
  - What is IAM? Principles of least privilege, and securing AWS resources
  - IAM users, groups, roles, and policies
  - Best practices for IAM: MFA, rotating credentials, least privilege
  - Hands-on: Creating IAM users, groups, and roles
- IAM Policies and Permissions
  - Writing and understanding IAM JSON policies
  - Attach IAM policies to users, groups, and roles
  - Use case: Creating policies for secure S3 bucket access
  - Hands-on: Create and assign IAM policies for secure access

---

Module 6: Elastic Load Balancer and Auto Scaling

- Elastic Load Balancer (ELB)
  - Overview of ELB: Types of Load Balancers (Application, Network, Classic)
  - Configuring and managing Load Balancers in AWS
  - Load Balancer listeners, target groups, and health checks
  - Hands-on: Set up an Application Load Balancer and configure auto-scaling with EC2 instances
- Auto Scaling
  - What is Auto Scaling and why is it important?
  - Configuring Auto Scaling Groups for EC2 instances
  - Scaling policies, metrics, and alarms for Auto Scaling
  - Hands-on: Create Auto Scaling groups with scaling policies and configure EC2 instance health checks

---

Module 7: Event-Driven Architecture with EventBridge

- Amazon EventBridge
  - Overview of EventBridge for building event-driven architectures
  - Event sources and event buses in EventBridge

- Creating event rules to trigger actions like AWS Lambda functions, Step Functions, etc.
- Hands-on: Create EventBridge rules and integrate with AWS Lambda for event processing

---

Module 8: Content Delivery with CloudFront

- Amazon CloudFront
  - Introduction to CloudFront as a content delivery network (CDN)
  - Setting up CloudFront distributions for static and dynamic content
  - Using CloudFront with S3 for faster content delivery
  - Hands-on: Create a CloudFront distribution with S3 origin and enable SSL for secure delivery

---

Module 9: Logging and Monitoring with CloudTrail and CloudWatch

- Amazon CloudTrail
  - Overview of CloudTrail for API call tracking and auditing
  - Setting up CloudTrail in multiple AWS regions
  - Configuring CloudTrail to send logs to CloudWatch or S3
  - Hands-on: Enable CloudTrail for API activity tracking and create CloudWatch logs for security auditing
- Amazon CloudWatch
  - Introduction to CloudWatch for monitoring AWS resources and applications
  - Creating CloudWatch Dashboards, Alarms, and Metrics
  - CloudWatch Logs and integration with Lambda for real-time log processing
  - Hands-on: Create CloudWatch alarms and dashboards for monitoring EC2 instances

---

Module 10: Security and Networking with NACLs and Flow Logs

- Network Access Control Lists (NACLs)
  - What are NACLs and how do they work in VPC?
  - Configuring inbound and outbound rules for NACLs
  - NACLs vs Security Groups: Differences and use cases

- Hands-on: Set up NACLs to control traffic to/from VPC subnets

- VPC Flow Logs
  - Overview of VPC Flow Logs for capturing network traffic information
  - Storing and analyzing VPC Flow Logs in CloudWatch Logs or S3
  - Use cases for troubleshooting, security, and compliance
  - Hands-on: Enable and analyze VPC Flow Logs to monitor network traffic

---

Module 11: Advanced Topics and Best Practices

- VPC Design Best Practices
  - Designing a multi-AZ VPC architecture for high availability
  - Managing CIDR block planning for scalable VPCs
  - Best practices for subnets, routing, and security
- Cost Optimization
  - Optimizing costs for VPC components (NAT Gateway, data transfer, load balancing)
  - Cost-saving strategies for EC2 instances, EBS volumes, and Auto Scaling
  - Hands-on: Implement cost-saving measures for AWS resources
- Security Best Practices
  - Securing data in transit with VPC Peering, VPN, and Direct Connect
  - Encrypting data at rest with S3, EBS, and EFS
  - Implementing IAM best practices for secure access control
  - Hands-on: Review and implement security best practices across AWS services

---

Capstone Project

- Final Project:
  - Design and implement a secure, scalable, and high-availability AWS architecture
  - Configure VPC with public and private subnets, NAT Gateway, and Transit Gateway
  - Set up S3, EBS, and EFS storage with proper access control using IAM

- Implement Auto Scaling and Elastic Load Balancing for fault tolerance
- Use CloudWatch, CloudTrail, and Flow Logs for monitoring and auditing
- Integrate EventBridge for real-time event-driven architectures

---

Tools and Services Covered:

- VPC (Virtual Private Cloud)
- NAT Gateway , VPC Peering , Transit Gateway
- VPC Endpoints (S3, DynamoDB)
- S3 (Simple Storage Service)
- EBS (Elastic Block Store)
- EFS (Elastic File System)
- IAM (Identity and Access Management)
- Elastic Load Balancer (ALB, NLB)
- Auto Scaling (Auto Scaling Groups, Scaling Policies)
- Event Bridge (Event-Driven Architecture)
- CloudFront (Content Delivery Network)
- CloudTrail (API Activity Logging)
- CloudWatch (Monitoring, Alarms, Logs)
- NACL (Network Access Control Lists)
- VPC Flow Logs (Network Traffic Analysis)

ALONG WITH COURSE WE ALSO PROVIDE

- Real Time scenarios example with all concepts.
- Ways of working in Real Time Projects.
- Daily Standup calls.
- Interview Preparations & Mock Interviews.
- Resume Preparation.