

# Syllabus

## Advance Kubernetes (12 hours)

### Topics:

- Kubernetes architecture and components
- Advanced workload management (Jobs, CronJobs, StatefulSets, and DaemonSets)
- Networking deep dive (Ingress, Services, NetworkPolicies, CNI)
- Kubernetes storage (Persistent Volumes, CSI drivers)
- Monitoring and logging (Prometheus, Grafana, Fluentd)

### Labs:

- Deploying advanced workloads (multi-container pods, Jobs, StatefulSets)
- Configuring Ingress with TLS
- Setting up Prometheus and Grafana for Kubernetes
- Creating and managing Persistent Volume



# Syllabus

## Advanced CI/CD (10 hours)

### Topics:

- Advanced pipeline designs (multi-branch, event-driven pipelines)
- GitOps principles and tools (ArgoCD, Flux)
- Securing CI/CD pipelines with DevSecOps
- Advanced testing strategies in pipelines (dynamic, static analysis)

### Labs:

- Building a CI/CD pipeline with Jenkins or GitHub Actions
- Implementing GitOps with ArgoCD
- Integrating static and dynamic code analysis in CI/CD
- Automating blue-green or canary deployments



# Syllabus

## In-depth AWS (12 hours)

### Topics:

- AWS compute deep dive (EC2, Lambda, Fargate)
- Advanced networking (VPC peering, Transit Gateway, VPNs)
- Storage strategies (S3, EFS, FSx)
- Monitoring with CloudWatch, X-Ray, and OpenSearch
- Multi-account and multi-region architecture (AWS Organizations, Control Tower)

### Labs:

- Deploying and scaling containerized applications on ECS/EKS
- Automating infrastructure with Terraform or CloudFormation
- Setting up monitoring for a distributed application
- Configuring AWS IAM policies and roles for DevOps pipelines



# Syllabus

## Architecture (10 hours)

### Topics:

- Modern cloud architecture patterns (microservices, event-driven)
- High availability and disaster recovery strategies
- Infrastructure scalability (horizontal, vertical)
- Architecting for performance and cost optimization
- Governance and compliance in cloud-native environments

### Labs:

- Architecting a multi-tier application
- Setting up highly available infrastructure with load balancers and Auto Scaling
- Deploying a secure and compliant workload
- Simulating disaster recovery with backups and failover



# Syllabus

## DevSecOps (8 hours)

### Topics:

- Integrating security into DevOps workflows
- Vulnerability management (SAST, DAST, SCA)
- Securing containers (image scanning, runtime security)
- Secrets management (AWS Secrets Manager, Vault)

### Labs:

- Implementing image scanning with Trivy or Aqua Security Configuring AWS Secrets Manager for secure credentials
- Automating security testing in CI/CD pipelines
- Setting up runtime security for Kubernetes



# Syllabus

## Projects

### Capstone Project:

- **Objective:** Build an end-to-end DevOps workflow for a cloud-native application.
- **Tasks:**
  - Develop a CI/CD pipeline integrating GitOps and security
  - Deploy a Kubernetes application with advanced configurations
  - Implement monitoring, logging, and distributed tracing
  - Use AWS for infrastructure, serverless components, and observability
  - Present the architecture and justify design decisions

