IICIS

ITKART Institute of Cyber & Information Security

1-Year Advanced Diploma

Cloud Computing & DevOps

www.iicis.org

48 Weeks (1 Year)

Cloud & DevOps Engineer capable of managing cloud-native environments, automation pipelines, and scalable deployments.

Deep-dive + Labs + Case Studies + Internship

Module	Module Title
1	Cloud Foundations & Virtualization
2	Linux, Networking & Scripting
3	AWS Cloud Deep Dive
4	Azure & GCP Cloud Services
	Revision & Internal Assessment
5	DevOps Fundamentals
6	Advanced DevOps & Automation
7	Cloud Security, Compliance & Governance
8	Capstone Project, Internship & Career Prep
	Final Evaluation

Semester 1 (Month 1–6): Core Cloud Computing

Module 1: Cloud Foundations & Virtualization (Month 1)

Content:

- Evolution of Cloud Computing & Industry Use Cases
- Cloud Service Models (IaaS, PaaS, SaaS, FaaS)
- Cloud Deployment Models (Public, Private, Hybrid, Multi-cloud)
- Virtualization Technologies (VMware, Hyper-V, KVM)
- Containers vs VMs, Serverless Architecture Basics
- Cloud Economics (Pay-as-you-go, CapEx vs OpEx, Cost Optimization)

Labs:

1. Set up a Virtualized Lab using VMware/VirtualBox.
2. Deploy and manage VMs with Hyper-V/KVM.
3. Compare performance of VM vs Container.
4. Create a cost analysis for migrating to cloud.

Module 2: Linux, Networking & Scripting (Month 2)

Content:

- Linux Administration (File Systems, Users, Permissions, Services)
- Process Management, System Monitoring, Crontab & Automation
- Networking Deep Dive (IP addressing, DNS, Routing, Firewalls, VPNs)
- Bash Scripting for Cloud Automation
- Python for Cloud Engineers (APIs, Boto3 for AWS, Azure SDK, GCP SDK)

Labs:

1. Configure Linux servers with user & permission policies.
2. Set up a secure VPN for a cloud lab.
3. Write Bash scripts to automate server setup.
4. Automate AWS resource creation using Python & Boto3.

Module 3: AWS Cloud Deep Dive (Month 3–4)

Content:

- Core AWS Services (EC2, S3, RDS, Lambda, VPC, IAM)
- Networking in AWS (Route 53, Load Balancing, Auto Scaling)
- Infrastructure Automation with AWS CloudFormation & Terraform
- Monitoring & Logging (CloudWatch, CloudTrail, GuardDuty)
- AWS Security & Compliance (IAM Policies, KMS, WAF, Shield)
- Cost Management in AWS

Labs:

1. Launch & configure EC2 instances.
2. Deploy a scalable web app with Load Balancer & Auto Scaling.
3. Create and manage S3 buckets with policies & encryption.
4. Automate AWS infra with CloudFormation & Terraform.
5. Implement AWS Security using GuardDuty, WAF & KMS.

Module 4: Azure & GCP Cloud Services (Month 5–6)

Content:

- Azure Core Services (VMs, Storage, SQL Database, Functions, App Services)
- Azure DevOps Services (Repos, Pipelines, Boards, Artifacts)
- Azure Security Center & Monitoring
- GCP Core Services (Compute Engine, Cloud Storage, BigQuery, Pub/Sub, GKE)
- Identity & Access in Azure & GCP
- Multi-Cloud & Hybrid Cloud Strategy

Labs:

1. Deploy VMs & Storage in Azure.
2. Create CI/CD pipeline with Azure DevOps.
3. Deploy & analyze data with BigQuery on GCP.
4. Build a multi-cloud application using AWS + Azure + GCP.

Semester 2 (Month 7–12): DevOps & Advanced Cloud

Module 5: DevOps Fundamentals (Month 7–8)

Content:

- Introduction to DevOps Culture, Principles & Tools
- Version Control with Git & GitHub/GitLab
- CI/CD Pipelines (Jenkins, GitHub Actions, GitLab CI)
- Containerization with Docker (Images, Volumes, Networking)
- Kubernetes Fundamentals (Pods, Services, Deployments)
- Helm for K8s package management

Labs:

1. Create a GitHub repo & manage workflows.
2. Build a CI/CD pipeline using Jenkins.
3. Containerize a web app with Docker.
4. Deploy containers on Kubernetes.
5. Manage Kubernetes clusters with Helm.

Module 6: Advanced DevOps & Automation (Month 9–10)

Content:

- Infrastructure as Code (Terraform, Ansible)
- Configuration Management & Automation
- Monitoring & Logging (Prometheus, Grafana, ELK Stack)
- Cloud-Native Development & Microservices Architecture
- DevSecOps – Embedding Security in CI/CD pipelines
- Service Mesh (Istio, Linkerd) for K8s

Labs:

1. Automate infrastructure deployment with Terraform.
2. Configure servers with Ansible Playbooks.
3. Monitor cloud infra with Prometheus & Grafana.
4. Log aggregation using ELK Stack.
5. Implement a DevSecOps pipeline with security scans.

Module 7: Cloud Security, Compliance & Governance (Month 11)

Content:

- Cloud Security Operations & SIEM
- Zero Trust Security in Cloud
- Identity & Access Governance (SSO, MFA, PAM)
- Backup, High Availability & Disaster Recovery Planning
- Compliance in Cloud (ISO 27001, GDPR, HIPAA, PCI DSS)
- Cloud Governance & Cost Optimization

Labs:

1. Configure IAM, MFA & role-based access in AWS/Azure.
2. Implement Zero Trust in a multi-cloud environment.
3. Create a backup & recovery plan for cloud workloads.
4. Set up a SIEM dashboard for monitoring cloud logs.

Module 8: Capstone Project, Internship & Career Prep (Month 12)

Content:

- Capstone Project (Choose 1):
    1. Build & Deploy a Multi-Cloud Enterprise Infrastructure
    2. Design & Implement a Secure CI/CD Pipeline
    3. Automate Large-Scale Infrastructure with Terraform & Kubernetes
- Internship / Virtual Labs with Industry Tools
- Resume Building & Interview Training
- Certification Roadmap (AWS Solutions Architect, Azure Admin, GCP Associate Engineer, Docker, Kubernetes, Terraform, Ansible, DevOps Professional)

Labs:

1. Build & deploy a cloud-native application using CI/CD.
2. Automate infra deployment across AWS, Azure & GCP.
3. Secure a Kubernetes cluster with DevSecOps.
4. Disaster recovery simulation for cloud workloads.
5. Resume workshop & mock interview sessions.