MADHUKAR REDDY

@awsandevops · madhukarreddy.com

LIVE TRAINING · COURSE SYLLABUS

Linux + AWS + DevSecOps with AIOps

Become job-ready in DevOps, Cloud & Security. A live, hands-on programme where you build, secure and operate real systems on AWS: from your first Linux command to DevSecOps pipelines and AI-assisted operations.

CURRICULUM **8 modules · 32 topics**	DURATION **3–4 months**	LANGUAGE **English & Telugu**
MODE **Live online classes**	RECORDINGS **Included**	FOCUS **Hands-on projects**

NEXT BATCH

Ask for dates, timings and fee on WhatsApp

New batches start regularly. Seats are limited per batch.

Chat on WhatsApp

Scan to chat on WhatsApp

Trainer: Madhukar Reddy · DevOps & Cloud Engineer · 6 years' experience · YouTube: Madhukar Reddy (@awsandevops)
WhatsApp: +91 93909 52880 · info@madhukarreddy.com · madhukarreddy.com/devsecops-aws-aiops-training/

Why this programme

Most courses teach tools in isolation. Here you learn the way real teams work: build infrastructure, deliver changes, secure every step of the pipeline and keep systems healthy in production. Every module ends with practical work on real AWS infrastructure, so you finish with skills and projects you can show in interviews.

Who it's for

- Freshers and graduates aiming for DevOps or cloud roles
- Developers, testers and support engineers switching careers
- System administrators moving to the cloud
- DevOps engineers adding DevSecOps and AIOps skills
- No prior cloud experience needed. We start from Linux basics

What you'll be able to do

- Run and troubleshoot Linux servers with confidence
- Design secure AWS networks, IAM and highly available workloads
- Automate infrastructure with Terraform, Ansible and Python
- Ship to Amazon EKS with CI/CD, Helm and Argo CD
- Add SAST, secret, dependency, IaC and DAST gates to pipelines
- Monitor systems and use AIOps to investigate incidents faster

Your learning path: 8 modules, 32 topics

01	02	03	04	05	06	07	08
Linux	AWS Foundations	AWS Workloads	AWS Operations	DevOps Automation	DevOps Delivery	DevSecOps	Observability & AIOps

Linux & AWS foundations · AWS workloads & operations · DevOps automation & delivery · DevSecOps · Observability & AIOps

Tools and services you'll use

Linux · Bash · systemd · Nginx · Git · GitHub · AWS IAM · VPC · EC2 · EBS · ALB / NLB · Auto Scaling · S3 · EFS · RDS MySQL · DynamoDB · CloudWatch · CloudTrail · AWS Config · Systems Manager · Route 53 · ACM · CloudFront · AWS WAF · Lambda · API Gateway · SQS / SNS · EventBridge · Python / Boto3 · Terraform · Ansible · Docker · Docker Compose · ECR · GitHub Actions · Jenkins · Kubernetes · Amazon EKS · Helm · Argo CD · SonarQube · Gitleaks · Trivy · Checkov · OWASP ZAP · GuardDuty · Inspector · Prometheus · Grafana · Alertmanager · AIOps

01 Linux fundamentals

MODULE 01 · LINUX

Terminal skills, server administration and practical troubleshooting.

01 Terminal and filesystem

- Linux overview, Ubuntu and Amazon Linux; terminal access and SSH keys.
- Directory structure, paths, file operations, editors and help commands.
- grep, find, pipes, redirection, text processing, archives and backups.

02 Users, permissions and packages

- Users, groups, sudo, file ownership, chmod, chown and umask.
- Package installation, updates, repositories and software removal.
- apt, dnf and yum; environment variables and application permissions.

03 Services, processes and storage

- Process inspection, signals, CPU, memory and load using ps, top and free.
- systemd services, startup configuration, journalctl and application logs.
- Disk usage, filesystems, mount points and persistent mounts with fstab.

04 Networking and shell scripting

- IP addresses, routes, DNS, ports and connectivity with ip, ss, curl and dig.
- SSH, scp, rsync and basic host-firewall troubleshooting.
- Shell variables, arguments, conditions, loops, functions, exit codes and cron.

Hands-on project: Configure an Nginx web server, repair a failed service, investigate disk usage and automate a backup.

02 Cloud identity and networking

MODULE 02 · AWS FOUNDATIONS

Core AWS concepts, account access and secure network configuration.

05 Cloud and AWS foundations

- Cloud service models, on-premises comparisons and shared responsibility.
- AWS Regions, Availability Zones, resource isolation and availability.
- IP addressing, subnetting, pricing concepts, tagging and budget alerts.

06 IAM and account security

- IAM users, groups, roles, policies, MFA and least-privilege permissions.
- AWS CLI access, workload roles, cross-account access and federation.
- Organizations, IAM Identity Center, KMS and secrets-management concepts.

07 VPC architecture

- VPCs, CIDR, public and private subnets, route tables and internet gateways.
- NAT gateways, VPC endpoints and private access to AWS services.
- Security groups, network ACLs and connectivity troubleshooting.

08 Connectivity and network protection

- Same-Region and cross-Region VPC peering; routing and address overlap.
- Transit Gateway, Site-to-Site VPN and Direct Connect overview.
- VPC Flow Logs, AWS Network Firewall and Route 53 Resolver DNS Firewall.

Hands-on project: Design a VPC, apply scoped IAM roles and diagnose a blocked connection between application tiers.

03 MODULE 03 · AWS WORKLOADS
Compute, storage and databases

Application hosting, persistent data and availability on AWS.

09 EC2 and block storage
- Instance types, key pairs, AMIs, user data, IMDSv2 and instance profiles.
- Launch templates; On-Demand, Spot and reservation concepts.
- EBS, instance store, snapshots, AMI recovery and lifecycle management.

10 Load balancing and Auto Scaling
- ALB and NLB, listeners, target groups, health checks and path routing.
- Auto Scaling groups, launch templates, scaling policies and replacement.
- Traffic distribution, capacity testing and unhealthy-target troubleshooting.

11 Object, file and backup services
- S3 permissions, versioning, replication, lifecycle and Glacier storage classes.
- EFS mounts and shared access; FSx and Storage Gateway overview.
- AWS Backup, retention, recovery testing and resource cleanup.

12 Databases on AWS
- SQL and NoSQL concepts; private RDS MySQL deployment and connectivity.
- Multi-AZ availability, snapshots, backups, restores and failover concepts.
- DynamoDB fundamentals; Redshift and ElastiCache use cases.

Hands-on project: Deploy Linux EC2 workloads, connect to private RDS, add load balancing and test application recovery.

04 MODULE 04 · AWS OPERATIONS
Operations and web delivery

Monitoring, managed access, HTTPS and cloud automation.

13 Monitoring, audit and governance
- CloudWatch metrics, logs, dashboards, alarms and Linux agent setup.
- CloudTrail API activity and AWS Config resource history.
- Trusted Advisor, cost visibility, tagging and operational checks.

14 AWS Systems Manager
- Managed-node prerequisites, IAM permissions and VPC endpoints.
- Session Manager access and Run Command for remote configuration.
- Patch Manager, Automation and Parameter Store use cases.

15 DNS, HTTPS and content delivery
- Route 53 hosted zones, DNS records, TTL, routing policies and failover.
- ACM certificates, third-party imports and HTTP-to-HTTPS redirects.
- CloudFront delivery, S3 origins and AWS WAF protection concepts.

16 Serverless integration and migration
- Lambda events, Python/Boto3 and API Gateway integration.
- SNS, SQS, SES, Step Functions and EventBridge use cases.
- Migration overview: AWS Transform MGN, DMS and DataSync.

Hands-on project: Configure managed access, collect application logs, enable DNS and HTTPS and automate a small operational task.

05 MODULE 05 · DEVOPS AUTOMATION
Code and infrastructure automation

Version control, operational scripting and repeatable infrastructure.

17 Git and GitHub collaboration
- Repositories, staging, commits, diffs, branches and pull requests.
- Reviews, merge conflicts, revert, tags, releases and .gitignore.
- Issues, change tracking and collaboration across environments.

18 Python for cloud automation
- Data types, functions, conditions, loops, exceptions, JSON and files.
- Requests, logging, basic tests and Boto3 resource operations.
- Resource inventory, tag-based actions, validation and dry-run workflows.

19 Terraform infrastructure as code
- Providers, resources, variables, outputs, dependencies and plan/apply.
- Modules, remote state, locking, imports, environments and drift.
- Reviewed changes, version constraints, teardown and CloudFormation comparison.

20 Ansible configuration management
- Inventories, SSH connectivity, playbooks, tasks and modules.
- Variables, templates, handlers and idempotent configuration.
- Automate packages, Nginx configuration, services and application setup.

Hands-on project: Deliver a change through Git, provision the environment with Terraform and configure Linux servers with Ansible.

06 MODULE 06 · DEVOPS DELIVERY
Containers, pipelines and Kubernetes

Application packaging, automated releases and GitOps delivery.

21 Docker, Compose and registries
- Images, Dockerfiles, layers, caching, multi-stage builds and non-root users.
- Networks, volumes, health checks, Compose and container troubleshooting.
- Docker Hub and ECR publishing; ECS and Fargate overview.

22 CI/CD with GitHub Actions and Jenkins
- Workflows, triggers, runners, agents, Jenkinsfiles, tests and build artifacts.
- Scoped permissions, credential handling and OIDC access to AWS.
- Staging, approvals, smoke tests, release promotion and rollback.

23 Kubernetes and Amazon EKS
- Cluster architecture, Pods, Deployments, Services, namespaces and selectors.
- ConfigMaps, Secrets, probes, requests, limits, storage and autoscaling.
- EKS access, node groups, workload IAM and load-balancer integration.

24 Helm and Argo CD GitOps
- Helm charts, values, release configuration and environment differences.
- Argo CD applications, desired state, reconciliation and drift detection.
- Reviewed Git changes, image traceability, promotion and recovery.

Hands-on project: Containerize the application, publish a tested image, deploy to EKS and deliver changes through Helm and Argo CD.

07 MODULE 07 · DEVSECOPS
Security across the delivery pipeline

Application, dependency, infrastructure and runtime security checks.

25 Threat modeling and code security
- Application trust boundaries, access control and common web risks.
- SAST, code-quality checks, SonarQube analysis and quality gates.
- Finding triage and remediation; licensed Veracode integration overview.

26 Secrets, dependencies and supply chain
- Gitleaks secret scanning, credential exposure and rotation workflows.
- Trivy dependency and image scanning; vulnerabilities and fix prioritization.
- SBOM generation, image digests and supply-chain integrity concepts.

27 Infrastructure, container and cloud security
- Checkov policies for Terraform; Dockerfile and container hardening.
- RBAC, security contexts, Pod Security Standards and enforced NetworkPolicies.
- Cloud security findings, IAM review, GuardDuty, Inspector and Macie overview.

28 Dynamic application and API security
- OWASP ZAP scans against authorized staging applications and APIs.
- Authentication, scan coverage, reports, false positives and remediation.
- Pipeline security gates, documented exceptions, rescanning and release checks.

Hands-on project: Add security checks to a pipeline, fix seeded application and infrastructure findings and verify the fixes with rescans.

08 MODULE 08 · OBSERVABILITY & AIOPS
Monitoring and AI-assisted operations

Operational evidence, anomaly detection and verified incident investigation.

29 Monitoring, metrics and reliability
- CloudWatch, Prometheus, Node Exporter and Grafana dashboards.
- Traffic, latency, errors, CPU, memory and resource saturation.
- SLIs, SLOs, availability checks and actionable alert rules.

30 Logs, alerts and event correlation
- Structured application logs, request IDs and log-based troubleshooting.
- CloudWatch Logs, Alertmanager, routing, grouping and duplicate reduction.
- Correlate deployment changes, alerts, metrics and incident timelines.

31 AIOps and anomaly detection
- Operational baselines, historical patterns and static alert thresholds.
- Rolling statistical detectors and CloudWatch anomaly-detection examples.
- Seasonality, false positives, alert quality and capacity signals.

32 AI-assisted troubleshooting and recovery
- Log summaries, incident hypotheses, runbook drafting and root cause analysis.
- Read-only diagnostics, prompt construction and sensitive-data redaction.
- Verify suggested fixes, review remediation and confirm service recovery.

Hands-on project: Investigate a failed release using logs and metrics, compare anomaly alerts and validate AI-assisted recovery suggestions.

Real projects for your portfolio

Secure multi-tier app on AWS
Custom VPC, scoped IAM roles, EC2 behind a load balancer, private RDS, Route 53 DNS and HTTPS.

Infrastructure as code
Provision environments with Terraform, configure servers with Ansible, deliver every change through Git.

Containers to Kubernetes
Containerize the app, publish to ECR, deploy to Amazon EKS and ship changes with Helm and Argo CD.

DevSecOps pipeline
SonarQube, Gitleaks, Trivy, Checkov and OWASP ZAP gates. Fix seeded findings, then prove it with rescans.

Observability & AIOps
Prometheus and Grafana dashboards, alerting, anomaly detection and AI-assisted investigation of a failed release.

How the training works

Live, interactive classes
Learn in real time on Google Meet / GoTo Meeting and ask questions as you go.

Every class recorded
Missed a session or want to revise? Recordings are included.

English & Telugu
Concepts explained in both languages, so nothing gets lost.

Hands-on first
Every module is practised on real AWS infrastructure, not just slides.

Frequently asked questions

Q Do I need prior experience?
No. We start from Linux fundamentals. Basic computer skills and willingness to practise every day are enough.

Q What if I miss a class?
Every session is recorded and shared, so you can catch up and revise anytime.

Q What do I need?
A laptop, a stable internet connection and your own AWS account. We show you how to use the free tier and keep costs low.

Q When does the next batch start?
New batches start regularly. Message us on WhatsApp for the next start date, class timings and fee.

Q How do I enrol?
Message us on WhatsApp at +91 93909 52880. We'll share the batch details, fee, payment details and joining link.

LIMITED SEATS IN EVERY BATCH

Reserve your seat in the next batch

WHAT'S INCLUDED

- Live, interactive classes for 3–4 months
- Recordings of every session
- English & Telugu explanations
- 32 topics across 8 modules
- Hands-on projects on real AWS infrastructure
- Portfolio-ready projects for interviews
- Doubt clearing during live sessions

Scan for next batch dates and fee on WhatsApp

Chat on WhatsApp: +91 93909 52880

How to enrol

1 Message us on WhatsApp

Tap the button or scan the QR code.

2 Get batch details

We share the next start date, timings, fee and payment details.

3 Join the live class

Receive your joining link and start learning.

Trainer: Madhukar Reddy · DevOps & Cloud Engineer · 6 years' experience
YouTube: youtube.com/@awsandevops · Email: info@madhukarreddy.com
Course page: madhukarreddy.com/devsecops-aws-aiops-training/