Thiraviya kumar. A

Cloud DevOps Engineer

✉ buzzmethiravi@gmail.com

📞 +91 9094392226

📍 Chennai

💼 Experience

TATA Consultancy Services,
Devops Engineer
Dec 2019 – Sep 2025
Chennai

ACCENTURE,
Senior Process Associate
Oct 2016 – Oct 2019
Chennai

🧠 Skills

- AWS
- Jenkins
- Git/GitHub
- ACDC/Octopus
- Terraform
- Ansible
- CloudFormation
- Docker
- Apache/Tomcat
- Kubernetes
- IAM/Identity Manager
- Linux/Ubuntu
- AppD and Splunk

🪪 ABOUT ME

Holding overall 7.5 years into technical and 5+ years of experience into Cloud DevOps architecting and automating scalable AWS cloud solutions. Expert in designing and managing CI/CD pipelines, containerized workloads, and IaC using Terraform and CloudFormation. Skilled in AWS, Kubernetes, Jenkins, Docker, and cloud-native monitoring tools.

📂 Project Summary

TATA Consultancy Services
Client: Commonwealth Bank of Australia
Apr 2022 – Sep 2025

- Designed and optimized CI/CD pipelines in Jenkins, integrating SonarQube, Maven, and Docker for secure, high-quality builds.
- Developed reusable Terraform modules to provision AWS infrastructure (VPC, EC2, RDS, S3, Security Groups) with version-controlled IaC.
- Implemented blue-green and canary deployments in Kubernetes and AWS ECS, reducing release risk and downtime by 30%.
- Led offshore deployments of new application versions, achieving 100% error-free production rollouts.
- Automated EC2 provisioning & configuration with Ansible playbooks, ensuring consistent environments and post-deployment validation.
- Resolved P1 and P2 production incidents under tight SLAs, minimizing downtime and ensuring business continuity.
- Reduced compute costs by automating EC2 off-hour shutdowns with AWS Lambda and EventBridge.
- Managed IAM roles/policies, security groups & AWS KMS encryption to enforce least-privilege and compliance.
- Configured Prometheus, Grafana & CloudWatch for monitoring and log centralization, improving incident detection time.
- Managed application secrets with AWS Secrets Manager and designed DR strategies with AMI backups, EBS snapshots, and cross-region S3 replication.
- Developed correlation searches using Splunk's transaction and stats commands to trace customer journeys—such as login → navigate → payment—and surface latency bottlenecks or anomalous transaction paths .
- Integrated Splunk alerts with CI/CD pipelines,using configuration management tools and CI/CD workflows to deploy firewall and monitoring updates seamlessly to dev,test and prod. environments
- Automated forwarder deployment and monitoring via Ansible/Shell scripts, ensuring consistent Splunk data ingestion from web servers, APIs, and AWS services, while maintaining compliance with SRE and ITIL change management protocols
- Designed and implemented centralized log aggregation using Splunk for distributed systems across cloud (AWS) improving observability across 75+services.
- Developed and maintained dashboards and custom alerts for monitoring critical application metrics, reducing incident response time by over 40%.
- Created correlation searches and detection rules in Splunk Enterprise Security (ES) to identify security anomalies, improving threat detection accuracy by 30%.
- Built automation scripts using Shell & Splunk REST API to schedule searches, export reports & manage data ingestion pipelines.
- Created role-based access control (RBAC) and data model configurations to meet SOX and HIPAA compliance standards.

🎓 Education

MBA, Jeppiaar Maamallan Institute of Technology
Aug 2012 – Apr 2014
Sriperumbudur,
Tamil Nadu

- Partnered with DevOps and Security teams to integrate Splunk into CI/CD pipelines for log-based testing and security monitoring.
- Led the development of custom alert workflows integrated with Jira and ServiceNow, streamlining incident creation and improving SLA compliance.
- Analyzed prod. inc. via Splunk logs & built root cause dashboards, reducing mean time to resolution (MTTR) by 50%.
- Provided 24/7 on-call support, proactively troubleshooting alerts & maintaining high availability of production systems.

Client: Refinitiv-London Stock Exchange Group
Dec 2019 – Apr 2022
- Provisioned and managed AWS EC2 instances for dev, staging & prod. environments, applied OS hardening, and configured security groups with least-privilege inbound/outbound rules.
- Created and updated IAC templates using Terraform and AWS CloudFormation to provision EC2, S3, and VPC resources.
- Managed application deployments on Apache Tomcat servers hosted on AWS instance, ensuring zero-downtime rollouts.
- Built and managed Docker images for applications, stored them in Amazon ECR, and deployed to ECS.
- Configured IAM users, roles, and policies to implement least-privilege access and enhance cloud security.
- Automated EC2 provisioning, server configuration, and package installation using Ansible playbooks, ensuring consistent environment setup and performing post-deployment validation across all stages.
- Implemented S3 bucket policies and lifecycle rules for secure and cost-effective storage management.
- Participated in Agile/Scrum ceremonies and collaborated with developers to streamline build and deployment processes.
- Built fully automated CI/CD pipelines using Jenkins, reducing deployment times and manual intervention.
- Managed backups, patching, and scaling of EC2 instances, including AMI/snapshot lifecycle.
- Enhanced application performance with Amazon CloudFront CDN integration.
- Assisted in troubleshooting deployment failures by analyzing Jenkins logs, application logs, and AWS CloudWatch metrics.

ACCENTURE INDIA PRIVATE LIMITED
Client: Schlumberger
Oct 2016 – Oct 2019
- Granted role-based access using Identity Manager, ensuring the principle of least privilege.
- Built CI/CD pipelines for staging and production with Octopus and ACDC, improving deployment frequency.
- Managed privileged access credentials with Cyber-Ark Password Vault, automating rotation for compliance.
- Configured and optimized F5 BIG-IP LTM for SSL offloading, health monitoring, and high-availability traffic routing.
- Managed SSL/TLS certificates with TLS Protect and ACDC, ensuring uninterrupted service compliance.
- Executed timely patch updates to address critical vulnerabilities, maintaining system stability, and security compliance.
- Implemented system monitoring via Prometheus, Grafana, and SCOM alert reducing MTTR.
- Configured SOCKS proxy via PuTTY, and managed environment variables for multi-environment deployments.