

MICLEN JEH

LOUISVILLE, KY 40258
+1(202) 677-1912 jehmiclen@gmail.com

PROFESSIONAL SUMMARY

Highly skilled and results-driven DevOps Engineer with about 8 years of experience in designing and implementing robust CI/CD pipelines, automating infrastructure deployment, and optimizing application performance. Leveraging a deep understanding of industry best practices and cutting-edge technologies, I have successfully streamlined development workflows, reduced time-to-market, and improved overall software quality. Proficient in a wide range of DevOps tools and cloud platforms, I excel in orchestrating scalable and secure infrastructure using infrastructure as code (IaC) principles. With a strong focus on collaboration and continuous improvement, I have effectively bridged the gap between development and operations teams, fostering a culture of agility and innovation. Committed to delivering exceptional results, I thrive in dynamic and challenging environments, driving successful project outcomes while ensuring seamless application delivery and high availability.

TECHNICAL SKILLS

AWS Cloud Services / Azure	Ec2, EFS, VPC, RDS, S3, Glacier, IAM, Kinesis, Cloud Front, Cloud Watch, Cloud Trail, Cloud Formation, Meme cached, Lambda, Route53, SNS, SQS, API Gateway, Elastic Cache, Redshift, Bastion Host, load balancing, cloud formation, WAF, Shield, AWS config, ASG, Ec2 instance launch types, placement groups, instance state, User data,
Networking Services	CIDR Block range, VPC Subnets, switches, Routers, transit gateway, VPC Endpoints, Egress and Ingress VPC, VPC peering, Site to Site VPN, Direct Connect, VPC, NACLs, Bastion Host, Subnetting, Security Groups, Gateway and Interface Endpoints, Transit Gateway
Disaster Recovery	The Business continuity plan (BCP), Disaster Recovery Strategies (Backup and restore, Pilot light, Warm standby, Active / Active (Multi-site) Recovery Time objective, Recovery Point objective
Monitoring Tools	Cloud Trail, Cloud watch (Cloud watch Events, Cloud watch logs, Cloud watch Matrice, cloud watch Alarms, AWS Inspector, Datadog
Encryption Tools	AWS KMS, HSM, TLS
Storage Services	Object Storage, Block Storage and File Storage
Source Code Management	Git Hub, Git.
Databases	AWS RDS (MYSQL, MSSQL, Post Gress, Maria DB,) Dynamo DB, Document DB, Redshift, Aurora
Platforms	Windows, Linux, Unix, Ubuntu, Centos
Ticketing tools	Jira, Confluence, Service Now (agile/scrum methodology)
Operating Systems	Windows, Linux, Ubuntu, Red hat, Centos
Programming Languages	Python, YAML, JSON, BASH Scripting

Migration tools	AWS Application Discovery service, AWS Application Migration service, AWS Migration Hub Database Migration Service, Data syn, Edge
Kubernetes	Docker, Kubernetes, EKS ECS, AKS ACR Deployments, Statefulsets, Ingress Controllers, Kubectl, Helm charts, Role base access control, Kubeconfig, Nodes, Node groups, Advance Scheduling, HPA, PVC, PV, Grafana, Prometheus, cluster maintenance and upgrade, Network, Security and Troubleshooting.
DevOps / CICD Tools	GitHub, Code Commit, Code Pipeline, Code Build, Code Deploy, ECR, EKS, ECS, SSM (systems manager), Terraform, GitHub Actions, Git, Bitbucket, Maven, Ansible,
Infrastructure As Code	Terraform, Ansible

WORK HISTORY

DEVOPS ENGINEER / KUBERNETES ENGINEER | 01/2019 to Current

Wipro - San Francisco, CA

Native Infrastructure and Kubernetes Management:

Designed and deployed Kubernetes clusters on AWS, managing resources with kubectl, Helm, and Terraform.

Implemented Kubernetes networking with Services, Ingress, and Network Policies to ensure secure and reliable communication.

Architected and deployed Kubernetes clusters for multiple projects, achieving resilience, scalability, high availability, and fault tolerance.

Automated deployment workflows using Kubernetes and Helm, reducing deployment time by 40% and minimizing human errors.

Designed and configured persistent storage solutions for Kubernetes clusters, enabling data persistence and seamless application scaling.

Utilized StatefulSets to ensure stable and unique network identities for stateful applications, enabling reliable data storage.

Collaborated with development teams to optimize application performance in Kubernetes environments.

Collaborated with cross-functional teams to optimize application performance and resource utilization.

Containerization and Microservices:

Containerized applications with Docker, optimizing runtime environments and facilitating consistent deployments

Redesigned monolithic applications into microservices architecture, enhancing scalability and maintainability.

Implemented Kubernetes deployment strategies, Rolling Updates, including Canary and Blue-Green releases, to minimize user impact during updates.

Monitoring and Observability:

Orchestrated monitoring and observability using Prometheus and Grafana, providing real-time insights into cluster performance and health.

Developed custom Prometheus exporters and Grafana dashboards to visualize application-specific metrics and trends.

Infrastructure as Code (IaC) and Automation:

Applied Infrastructure as Code (IaC) practices using Terraform, automating the provisioning and management of Kubernetes resources.

Defined and maintained declarative Kubernetes manifests and Helm charts for consistent application deployments.

Security and Compliance:

- Regularly updated the Kubernetes version to benefit from security patches and improvements.
- Configured authorization plugins like ABAC (Attribute-Based Access Control) or RBAC to ensure only authorized users can access the API server.

Designed network policies to restrict communication between microservices, enhancing application security.

Conducted security audits and vulnerability assessments, addressing findings and ensuring compliance with industry standards.

Regularly back up critical data and ensure a disaster recovery plan is put in place.

Ensured that communication within the cluster and with the API server is encrypted using TLS.

Used strong authentication mechanisms, such as client certificates, bearer tokens, or integration with OAuth providers like OIDC.

Used trusted sources for container images and scan them for vulnerabilities before deploying.

Stored sensitive information, like passwords or API tokens, in Kubernetes Secrets rather than hardcoding them in configurations.

Encrypting Confidential Data at Rest in a Kubernetes cluster

Technical Documentation and Knowledge Sharing:

Documented Kubernetes architecture, deployment procedures, and best practices for internal knowledge sharing.

Provided technical guidance and mentorship to junior team members, fostering skill development and growth.

Incident Response and Troubleshooting:

Led incident response efforts during critical production incidents, quickly identifying root causes and implementing corrective actions.

Conducted post-incident reviews to analyze incident handling, identify areas for improvement, and implement preventive measures.

Devops and cloud implementations:

- Designed, implemented, and managed AWS infrastructure components like Virtual Private Cloud (VPC), Subnets, Route Tables, Security Groups, Network Access Control Lists (NACLs), etc.
- Configured networking services such as Amazon EC2, Amazon RDS, Elastic Load Balancing (ELB), and Amazon Route 53.
- Proficient in working with Amazon EC2 instances, including instance types, auto-scaling, and Elastic Beanstalk for deploying and managing applications.
- Leveraged AWS Lambda for serverless computing and event-driven applications.
- Implemented security best practices, including identity and access management (IAM), roles, and policies.
- Managed encryption for data at rest and in transit.
- Utilized Git and GitHub for version control, branching, merging, and collaborating with development teams on code repositories.
- Integrated SonarQube for static code analysis, enforcing code quality standards and ensuring adherence to best practices.
- Orchestrated containerized deployments using Kubernetes for application deployment, scaling, and management in a microservices architecture.
- Implemented CI/CD pipelines using Jenkins, Maven, and GitHub Actions, enabling automated build, test, and deployment processes for multiple applications and services.
- Configured and maintained Prometheus for monitoring and alerting, collecting and analyzing metrics for application and infrastructure health.
- Developed automation scripts and workflows using YAML, JSON, Bash, and Python to streamline and optimize deployment, configuration, and maintenance tasks.

DEVOPS ENGINEER | 10/2015 to 12/2018

CloudBees - Denver, CO

- Utilized containerization technologies, including Docker and Kubernetes, to facilitate efficient application deployment, scalability, and management.
- Implemented and managed configuration management tools like Puppet and Chef, ensuring consistent configuration across servers and environments.

- Collaborated with development teams to optimize application performance and reliability by conducting thorough performance testing using tools like JMeter and Gatling.
- Monitored and maintained application and infrastructure health using monitoring tools such as Prometheus, Grafana, and ELK stack (Elasticsearch, Logstash, Kibana).
- Developed infrastructure as code using tools like Terraform and Ansible, resulting in scalable and consistent infrastructure deployments across multiple environments.
- Implemented CI/CD pipelines using tools such as Jenkins, GitLab CI/CD, and Travis CI, enabling automated builds, tests, and deployments for multiple projects.
- Implemented security measures and best practices, including user access controls, encryption, and vulnerability scanning tools like Nessus and OpenVAS.
- Collaborated with cross-functional teams to improve release management processes, resulting in faster and more reliable deployments.
- Conducted regular infrastructure and code reviews to identify areas for optimization, cost reduction, and process improvement.
- Assisted in capacity planning and scaling infrastructure resources to meet growing application demands.
- Provided support and troubleshooting expertise during incidents and outages, facilitating prompt resolution and minimizing downtime.
- Documented and maintained standard operating procedures (SOPs) and infrastructure diagrams for reference and knowledge sharing purposes.

Professional Certification and Training

- Certified Kubernetes Administrator (CKA)

- Certificate ID: LF-qcccbelnw4

EDUCATION

Presbyterian University of Cameroon | Bachelor of Science

Computer Science, 12/2014