EKANGAKI NJANG

DevOps Engineer

Email: njangekangaki@gmail.com | **Phone:** +1 (240) 643 1098 | **Location:** BOWIE, MD | **LinkedIn**

PROFESSIONAL SUMMARY:

With over 9 years of extensive experience in Networking, Firewall Management, DevOps and Cloud Engineering. I specialize in optimizing infrastructure, automating workflows, and deploying scalable solutions in diverse tech environments. Proficient in CI/CD pipelines, container orchestration using Docker and Kubernetes, and skilled in AWS and Azure, I drive efficiency and innovation through strategic implementation of cutting-edge technologies to ensure seamless operations and deliver top-notch performance. My strong background in scripting with Python and Bash allows me to create robust automation frameworks, while my commitment to collaboration and continuous improvement enables cross-functional teams to achieve exceptional results and exceed project goals.

AREA OF EXPERTISE:

- **CI/CD Pipeline Orchestration:** Expertise in designing, implementing, and managing end-to-end Continuous Integration and Continuous Deployment pipelines using tools like Jenkins, GitLab CI/CD.
- **Infrastructure as Code (IaC):** Proficient in leveraging IaC tools such as Terraform or CloudFormation to automate the provisioning and management of cloud resources, ensuring consistency and scalability.
- **Containerization and Orchestration:** Skilled in container technologies like Docker and container orchestration platforms like Kubernetes for efficient deployment, scaling, and management of microservices.
- **Cloud Platforms:** Experience working with major cloud providers (AWS, Azure) to design, deploy, and optimize cloud-native solutions, utilizing services like EC2, S3, Azure DevOps, and Google Cloud Build.
- **Configuration Management**: Familiarity with configuration management tools such as Ansible to automate server configuration and application deployments.
- **Monitoring and Logging:** Proficiency in setting up monitoring and logging solutions like Prometheus, Grafana, ELK stack (Elasticsearch, Logstash, Kibana) for real-time system analysis and troubleshooting.
- **Version Control**: Strong command of version control systems like Git, including branching strategies, pull requests, and code review workflows to ensure collaborative development.
- **Security Best Practices:** Knowledge of security protocols and best practices for securing CI/CD pipelines, containers, cloud environments, and ensuring compliance with industry standards.
- **Collaborative Communication:** Effective communication and teamwork abilities to collaborate with cross-functional teams, bridge the gap between development and operations, and drive DevOps culture within the organization.

TECHNICAL SKILLS:

Cloud Platforms:	Amazon Web Services (AWS), Microsoft Azure
DevOps Tools:	Jenkins, Azure DevOps
Operating Systems:	Linux (Ubuntu, CentOS), Windows Server
Containerization:	Docker, Kubernetes, AWS EKS
Artifact Repositories	DockerHub, Nexus and AWS Elastic Container Registry (ECR)
Infrastructure as Code (IaC):	Terraform, AWS CloudFormation, Ansible
Source Control:	Git, GitHub, Bitbucket, GitHub Actions

Storage Services:	Amazon S3 (Simple Storage Service), Amazon EBS (Elastic Block Store), Amazon Glacier, AWS Storage Gateway
Scripting Languages:	PowerShell, Bash, YAML, Groovy DSL
Monitoring and Logging:	Prometheus, Grafana, ELK Stack
Serverless:	AWS Lambda (Serverless Computing), Amazon API Gateway (Build, Deploy, and Manage APIs)
Networking:	Load Balancing, Virtual Networks, Site to Site VPN, Remote Access VPN, DNS, Firewalls, IDS/IPS, secure tunnelling, Network segmentation
NGFW	Palo Alto Next Generation Firewall, Panorama, Cisco MX 84 Routers
Security:	Identity and Access Management (IAM), SSL/TLS, Security Groups, OWASP, 2FA, MFA
Infrastructure:	Virtual Machines (VMs), VM Scale Sets (VMSS)
Monitoring and Logging:	Amazon CloudWatch (Monitoring), AWS CloudTrail (Audit API Calls)
Cloud Technology:	AWS
RDBMS:	AWS Aurora, MS SQL Server, MySQL
Operating Systems:	Windows, Linux, Unix
Compute Services:	Amazon EC2 (Elastic Compute Cloud), AWS Lambda, AWS Elastic Beanstalk, AWS Auto Scaling

PROFESSIONAL EXPERIENCE:

HEALTHCARE FOR THE HOMELESS

JUNE 2018 - PRESENT

ROLE: DEVOPS ENGINEER

- Led incident response efforts during critical incidents, identified root causes through thorough analysis, and collaborated with cross-functional teams to implement preventive measures, reducing incident recurrence by 40%.
- Created comprehensive technical documentation and conducted knowledge-sharing sessions on Git workflows, CI/CD best practices, and infrastructure management for onboarding new team members.
- Actively pursued skill enhancement by attending workshops and staying up to date with industry trends, introducing Argo CD for GitOps-based deployments, leading to a 25% increase in deployment accuracy.
- Enhanced observability using Prometheus and Grafana to implement monitoring and alerting systems.
- Worked in tandem with development teams to enhance the performance of applications in Kubernetes settings.
- Performed Kubernetes cluster troubleshooting and performance tuning.
- Knowledge of CI/CD principles and technologies
- Expertise and in-depth understanding of Terraform
- Create and maintain AWS Network entities, AWS servers and applications, and control costs.
- Working knowledge of Azure networking and security principles, practices, and technologies in real-world Azure settings. Solid familiarity with Azure's container-based technology
- Create Infrastructure as code (IAC) by utilizing cloud-native technology to guarantee platform deployments that are automated and reliable.
- Knowledge and familiarity with cloud security protocols such as Azure AD, IAM, Web Application Firewalls, and Data Protection.
- Strong analytical and organizational abilities; practical networking knowledge and skills; advanced troubleshooting and tuning of cloud and OS performance; implementation of security best practices for Kubernetes clusters, guaranteeing adherence to industry standards.
- Successfully managed and administered Palo Alto Panorama to oversee and control PA460 firewalls across the main office and six branch offices.
- Centralized firewall policy management, ensuring consistent security policies and configurations across all sites.
- Designed and implemented site-to-site VPN configurations connecting the main office with six branch offices, ensuring secure and reliable communication.

- Monitored and maintained VPN connections to ensure high availability and performance.
- Configured high availability (HA) for firewalls to ensure continuous network protection and minimize downtime.
- Developed and tested disaster recovery plans for Panorama and PA460 firewalls.
- Enable continuous monitoring and track security-related defects and the status of their resolutions.

HEALTHCARE FOR THE HOMELESS

ROLE: CLOUD INFRASTRUCTURE ENGINEER

JUNE 2017 – MAY 2018

- **Cloud Platform Management**:
  - Managed and maintained cloud infrastructure on AWS and Azure, ensuring high availability, scalability, and security of services.
  - Utilized AWS services such as EC2, S3, RDS, Lambda, and CloudFormation to architect and deploy reliable, cost-effective solutions.
  - Implemented Azure services including Virtual Machines, Blob Storage, SQL Database, and Azure DevOps for CI/CD pipelines.
- **Automation and Scripting**:
  - Developed Infrastructure as Code (IaC) using Terraform and AWS CloudFormation to automate the provisioning and management of cloud resources.
  - Automated deployment processes with Ansible and Jenkins, reducing manual intervention and deployment times by 50%.
- **Containerization and Orchestration**:
  - Deployed and managed containerized applications using Docker and Kubernetes, enhancing application portability and resource utilization.
  - Set up Kubernetes clusters on AWS EKS and Azure AKS, implementing Helm charts for efficient application deployment and management.
- **Security and Compliance**:
  - Ensured cloud infrastructure security by implementing best practices for IAM, security groups, and network ACLs.
  - Conducted regular security audits and vulnerability assessments using tools like Trivy and OWASP Dependency-Check.
  - Implemented Multi-Factor Authentication (MFA) and Single Sign-On (SSO) with Okta for secure access control.
- **Monitoring and Optimization**:
  - Implemented monitoring and logging solutions using AWS CloudWatch, Azure Monitor, and ELK Stack (Elasticsearch, Logstash, Kibana) to ensure system health and performance.
  - Conducted performance analysis and optimization of cloud resources, achieving a 30% cost reduction through rightsizing and reserved instances.
- **Backup and Disaster Recovery**:
  - Designed and implemented backup strategies using AWS S3 and Azure Backup, ensuring data integrity and availability.
  - Developed disaster recovery plans and performed regular DR drills to validate recovery processes and minimize downtime.
- **Collaboration and Communication**:
  - Collaborated with cross-functional teams to align cloud infrastructure initiatives with organizational goals and financial strategies.
  - Documented infrastructure designs, procedures, and best practices, facilitating knowledge sharing and onboarding processes.

Key Projects

- **Network and Security Upgrade**:
  - Led projects to upgrade network performance and security by implementing advanced networking devices and firewalls.
  - Achieved a more stable network and improved visibility, enhancing the overall IT capabilities to support healthcare services.
- **CI/CD Pipeline Implementation**:
  - Designed and implemented a complete CI/CD pipeline using Jenkins, Git, Maven, SonarQube, Nexus, Docker, and Kubernetes.
  - Improved deployment frequency and code quality, reducing time-to-market for new features and bug fixes.

HEALTHCARE FOR THE HOMELESS

ROLE: NETWORK/DEVOPS ENGINEER

NOV 2016 – JUNE 2017

- Managed and optimized the CI/CD pipeline using Jenkins, reducing deployment cycle time by 25% and increasing code quality by implementing automated tests at different stages.
- Utilized Ansible for automating server provisioning and configuration management, leading to a 40% reduction in manual setup time and improving consistency across environments.
- Implemented Docker to containerize applications, enabling seamless deployment and scaling of microservices on AWS ECS, resulting in improved application availability during traffic spikes.
- Designed and implemented auto-scaling groups and load balancers on AWS, ensuring 99.99% uptime for critical applications and minimizing downtime during maintenance.
- Managed Git repositories, enforced branching strategies, and conducted training sessions for the team, enhancing collaboration.
- Implemented robust security measures in the end-to-end pipeline, incorporating threat modelling and security best practices to safeguard applications against potential vulnerabilities and cyber threats.
- Conducted regular security audits and assessments using industry-standard tools, ensuring the EKS server farm and Kubernetes cluster management to adhere to security compliance standards.
- Enhanced the security posture of the deployment pipeline by implementing AWS key management service (KMS) to securely store and retrieve sensitive credentials, reducing the risk of unauthorized access during pipeline runs.
- Applied security controls and compliance checks using Terraform scripts to ensure that the DEV, STAGE, and PROD environments in AWS meet industry-specific security standards.
- Implemented Jenkins pipeline security practices incorporating code analysis tools and static code analysis to identify and mitigate potential security vulnerabilities in Java code.
- Conducted security consultations and provided guidance on best practices for securing applications and infrastructure on AWS and Azure, contributing to the overall cybersecurity posture of the USA-based company.
- Applied container security best practices in Docker-based deployments on AWS, ensuring that both stateful and stateless applications meet security benchmarks and minimizing the risk of container-related vulnerabilities.
- Administered Cloud Infrastructure, creating VPCs, defining IP ranges, and ensuring security.
- Migrated object storage to S3 Buckets and implemented IAM roles for EC2s.
- Configured Auto Scaling Groups, Launch Templates, and launched web servers in public subnets.
- Managed private subnets, launched DB servers, and set up NAT servers for secure internet access.
- Configured security groups and NACLs for enhanced security.
- Installed and configured Jenkins, Java, and integrated tools like Git, Maven, JUnit, Tomcat. Developed and administered Kubernetes clusters, deployed Docker containers, and created service YAML files.
- Automated infrastructure activities using Ansible playbooks, integrated Ansible with Jenkins.
- Managed AWS infrastructure with CLI and API, automated activities using Terraform.
- Implemented ELB and Auto-Scaling policies for scalability and high availability.
- Written Docker files developed Docker images, and managed Docker containers.
- Worked with monitoring tools like ELK & EFK, AWS CloudWatch, Prometheus, and Grafana.
- Managed AWS resources, including EC2, RDS, ELB, Auto-Scaling Group, S3, and more.

TELIA COPENHAGEN DENMARK Network Technician

June 2014 – August 2016

- Provided solutions for network, hardware, and operating systems issues.
- Installed and maintained network equipment, troubleshooting network connectivity issues.
- Administered LAN infrastructure with Windows 2003 Active Directory.

EDUCATION:

- Bachelor's in computer science
  University of Yaoundé, Cameroon – Africa (2014)
- Masters in Forced Migration and Minor in Computer Science,
  Aalborg University Copenhagen (2016)

CERTIFICATIONS:

- AWS Cloud Practitioner
- AWS Certified Solutions Architect – Associate
- Cisco Certified Network Associate (CCNA)
- Palo Alto Network Certified Network Security Engineer (PCNSE)