IKENNA OKWARA

Philadelphia, PA | (267) 394-3341 | jjustinbrowno@gmail.com
www.linkedin.com/in/ikenna-okwara-01560130a | https://github.com/okwarajustin/

PROFESSIONAL SUMMARY

Results-driven AWS Solutions Architect and DevOps Engineer with 8+ years of expertise in designing, automating, and securing cloud infrastructures. Skilled in architecting scalable, high-availability solutions on AWS, Microsoft Azure, and implementing CI/CD pipelines to enhance delivery and reduce operational costs. Specializes in Infrastructure-as-Code (IaC), cloud security, and container orchestration, with a strong track record of optimizing performance and ensuring compliance with industry standards. Proven leader in driving cloud transformation initiatives and fostering collaboration across development and operations teams.

TECHNICAL SKILLS AND TOOLS

- **Data Protection:** AWS Certificate Manager, AWS KMS, Snapshot Lifecycle Manager, AWS CloudHSM.
- **DevOps Tools:** Jenkins, GitLab CI, Docker, Kubernetes, Ansible, Terraform, Prometheus, Grafana, Packer, Chef, Puppet.
- **Cloud Platforms:** AWS (EC2, S3, RDS, Lambda, ECS, EKS, CloudFormation, VPC, CloudFront, Elastic Beanstalk, IAM, Route 53, Redshift, Glue), Azure (VMs, Azure DevOps, Blob Storage, Functions). GCP Google Compute Engine.
- **Databases:** DynamoDB, Amazon RDS, MySQL, PostgreSQL, Oracle, MongoDB, Redis.
- **Programming Languages:** Python, Bash, YAML, PowerShell, JSON, Java, Go, Ruby, Shell Scripting.
- **Version Control:** Git, GitLab, GitHub, Bitbucket.
- **CI/CD & Automation:** Jenkins, CircleCI, TravisCI, Bamboo, AWS CodePipeline, GitLab CI/CD.
- **Infrastructure as Code (IaC):** Terraform, AWS CloudFormation, Packer, Ansible.
- **Containerization & Orchestration:** Docker, Kubernetes, AWS EKS, OpenShift, Mesos, Nomad.
- **Application Delivery and DevOps**: Jira, Confluence, Jenkins, AWS CodePipeline, AWS CodeCommit, AWS CodeBuild, AWS CodeDeploy.
- **Networking:** AWS VPC, AWS Transit Gateway (TGW), Internet Gateway (IGW), NAT Gateway (NGW).
- **AWS Migration Tools:** CART, AWS Application Discovery Service (ADS), AWS Migration Hub, CloudEndure, AWS Database Migration Service (DMS), AWS Schema Conversion Tool (SCT).
- **Access Management & AWS Security:** AWS Organizations, AWS IAM, AWS Secrets Manager, AWS Security Hub, AWS GuardDuty, AWS Shield, AWS Firewall Manager, AWS Inspector.
- **Monitoring & Event Management:** AWS CloudWatch (Events & Logs), AWS SNS, AWS CloudTrail, AWS Event Bridge.
- **Governance & Compliance:** AWS Config Rules, AWS Organizations, AWS Control Tower, AWS Trusted Advisor, AWS Well-Architected Tool, AWS Budgets, AWS License Manager, CodeCommit, AWS CodeBuild, AWS CodeDeploy.
- **Other Tools:** Jira, Confluence, Snyk, SonarQube, Artifactory, Nexus, Splunk, Vault, Consul, Helm, Istio, ArgoCD.

WORK HISTORY

DEVOPS ENGINEER | AWS SOLUTIONS ARCHITECT – 10/2021 to Present
Volvo CE, Shippensburg, PA

- Build and maintain CI/CD pipelines using Jenkins, GitLab CI, and AWS CodePipeline to streamline the development, automating security testing (SAST, DAST) to identify vulnerabilities early in the development cycle, testing, and deployment process.
- Implement autoscaling, load balancing, and monitoring using AWS Auto Scaling Groups, Elastic Load Balancers (ELB), and Cloud Watch to optimize performance and uptime.
- Collaborate with DevSecOps teams to integrate AWS Security services such as AWS GuardDuty, AWS Config, and Security Hub into the DevOps pipeline for continuous security monitoring.
- Developed API-driven solutions to facilitate secure data exchange between internal and external applications, enhancing cross-functional connectivity and data accuracy.
- Deploy and manage containerized applications using Docker, Kubernetes, and AWS EKS, ensuring efficient orchestration and scaling.
- Architect and manage highly scalable, secure AWS environments using services like EC2, S3, RDS, Lambda, VPC, and CloudFront.
- Automated IaaS infrastructure deployment and implement Infrastructure-as-Code (IaC) solutions using Terraform and AWS CloudFormation to automate cloud infrastructure provisioning.
- Designed automated Transcribe workflows for real-time audio-to-text conversion, enhancing data accessibility and enabling robust search and analysis capabilities across large datasets.
- Lead cloud migration initiatives, performing lift-and-shift. Designed and deployed comprehensive integration solutions within Azure, leveraging API Management, Logic Apps, and Service Bus to connect disparate systems seamlessly.
- Design disaster recovery and backup strategies for critical applications using AWS Backup, AWS Lambda, and Cross-Region Replication.
- Develop and implement security policies using Azure and AWS IAM, enabling role-based access control (RBAC) and multi-factor authentication (MFA) for cloud resources.
- Implement monitoring and logging solutions using AWS CloudWatch, ELK Stack, and Prometheus to provide real-time visibility into infrastructure performance and security.
- Automate routine operational tasks using AWS Lambda, Python, and Boto3 to reduce manual intervention and improve efficiency.
- Leveraged AWS Bedrock to develop and deploy generative AI models, enabling applications to integrate natural language processing and advanced ML capabilities seamlessly.
- Conduct regular reviews of Azure and AWS Well-Architected Framework, implementing recommendations to ensure best practices for security, reliability, performance, and cost efficiency. Configured SSO and multi-factor authentication (MFA) with SaaS tools (e.g., Okta, Azure AD) to centralize identity management and enhance security.
- Integrate third-party tools like HashiCorp Vault for secure credential management in AWS.
- Manage the deployment of serverless architectures using AWS Lambda, API Gateway, and DynamoDB for efficient, scalable microservices
- Perform ongoing cloud cost management by auditing Azure and AWS services usage and implementing Reserved Instances and Spot Instances for cost savings.
- Conduct threat modeling, vulnerability assessments, and automated security testing within the CI/CD pipeline to ensure a secure AWS and Azure environment.
- Architected SAP integration frameworks, improving data flow and synchronization across multiple business units, reducing operational lag by over 20%.
- Mentor junior DevOps engineers and cloud architects in best practices for AWS and cloud-native applications.

AWS CLOUD ENGINEER | DEVOPS ENGINEER – 06/2018 to 09/2021

COFCO, **Philadelphia, PA.**

- Created and managed CI/CD pipelines using Jenkins, GitLab CI, and AWS CodeBuild for automated application deployment and testing.
- Implemented "Security as Code" by embedding policies in Infrastructure as Code (IaC) tools (e.g., Terraform, AWS CloudFormation) to ensure secure and compliant resource provisioning.
- Implemented real-time monitoring and alerting solutions using AWS CloudWatch, Prometheus, and ELK Stack to ensure continuous application performance visibility.
- Designed and implemented highly available, fault-tolerant architectures using AWS Auto Scaling, Elastic Load Balancers (ELB), and Route 53.
- Created automated compliance checks for frameworks like CIS, GDPR, and NIST within DevOps workflows, reducing manual checks and enhancing audit readiness.
- Architected and deployed secure and scalable solutions on AWS, utilizing services such as EC2, RDS, S3, Lambda, and CloudFormation.
- Automated cloud infrastructure deployment using Terraform, reducing provisioning time by 70%.
- Utilized AWS Bedrock to streamline model deployment and management, minimizing the time-to-market for AI solutions and enabling rapid iterations to meet evolving business needs.
- Managed the migration of legacy on-premises applications to AWS cloud, ensuring minimal downtime and post-migration optimization.
- Integrated Azure and AWS Identity and Access Management (IAM) policies for securing applications, enabling least privilege access to cloud resources.
- Developed security controls using Azure or AWS Security Hub, GuardDuty, and AWS Config for continuous security monitoring and compliance.
- Configured AWS Elastic File System (EFS) and S3 lifecycle policies for optimized data storage and cost management.
- Automated security patching and updates using AWS Systems Manager to ensure compliance with security standards. Secured sensitive data by integrating secrets management solutions (e.g., HashiCorp Vault, AWS Secrets Manager), minimizing risks of credential exposure in DevOps workflows.
- Used AWS Cost Explorer and AWS Trusted Advisor to optimize cloud resource usage and reduce costs by 30%.
- Integrated third-party monitoring tools such as Datadog and New Relic for enhanced visibility into cloud resources.
- Conducted regular vulnerability assessments and security audits to ensure cloud infrastructure met compliance and security standards.
- Configured AWS VPC, Security Groups, and Network ACLs for secure and efficient network architecture.
- Implemented Microsoft Azure and AWS backup strategies and disaster recovery plans, ensuring business continuity for mission-critical applications.
- Participated in cross-team collaboration to improve application performance, reduce deployment times, and streamline processes.
- Automated daily backups of critical data using AWS S3, reducing the risk of data loss in case of system failures.
- Continuously updated knowledge of industry trends, emerging technologies, and best practices in the AWS ecosystem, enabling informed decision-making and effective problem-solving.
- Established strong relationships with key stakeholders to ensure that cloud initiatives were aligned with broader organizational goals and priorities.

- Collaborated with cross-functional teams to identify integration requirements, analyze system dependencies, and deliver tailored solutions that align with business objectives and IT architecture best practices.

DEVOPS ENGINEER – 03/2016 to 05/2018
Covance, Princeton, NJ

- Set up and maintained scalable virtual machines (VMs) on AWS EC2, Azure VMs, Google Compute Engine, optimizing for performance and cost efficiency.
- Collaborated with security teams to implement AWS security best practices, including encryption for data-at-rest and in-transit using KMS and SSL.
- Developed and deployed AWS Lambda functions for automating serverless tasks and cloud operations.
- Implemented disaster recovery and failover strategies using AWS Elastic Load Balancers, Route 53, and S3 Cross-Region Replication.
- Led the migration of monolithic applications to microservices architectures, leveraging Docker, Kubernetes, and AWS EKS.
- Worked closely with developers to implement automated testing and continuous integration pipelines, reducing release times by 50%.
- Configured logging and monitoring solutions using ELK Stack (Elasticsearch, Logstash, and Kibana) to improve troubleshooting and incident response.
- Automated security patch management using AWS Systems Manager, ensuring compliance with industry security standards.
- Implemented Infrastructure-as-Code (IaC) using Terraform and AWS CloudFormation for automating the provisioning and management of AWS resources.
- Designed, built, and maintained CI/CD pipelines using Jenkins, Git, and Ansible to streamline application deployment processes.
- Integrated Docker for containerization and Kubernetes for orchestration to achieve scalable and consistent application deployments.
- Monitored and maintained cloud environments using AWS CloudWatch, Prometheus, and Grafana to ensure optimal performance and uptime.
- Integrated third-party tools, such as HashiCorp Vault, for secure secrets management in CI/CD pipelines.
- Configured AWS IAM roles and policies to enforce the principle of least privilege for securing access to cloud resources.
- Configured network security using AWS VPC, subnets, and security groups, ensuring secure and isolated cloud infrastructure.
- Performed regular performance tuning of cloud infrastructure, identifying and addressing bottlenecks to improve system scalability.
- Maintained version control systems like Git or SVN for seamless collaboration among developers and engineers during project lifecycles.
- Automated manual tasks through scripting languages such as Python or Shell, boosting team productivity levels.
- Contributed to the creation of a DevOps culture within the organization, leading to increased agility and cross-functional collaboration.
- Monitored automated build and continuous software integration process to drive build/release failure resolution.
- Optimized build processes using tools such as Jenkins or Bamboo for fast feedback loops in development cycles.
- Monitored and remediated cloud configurations and policies using tools like AWS Security Hub and Azure Security Center to maintain strong security posture.

- Provided 24/7 on-call support for critical systems, ensuring high availability and rapid issue resolution.

EDUCATION

- Associate in arts, Health Care Studies, 2021, Community College of Philadelphia, PA.
- Bachelor of Science Industrial Physics 2010, Anambra State University Uli, Anambra State, Nigeria.

CERTIFICATIONS

- AWS Certified Solutions Architect – Associate.
- CompTIA Security+ in process