Harold Akioye

Address: 14837 Strawberry Lane Burtonsville, MD 20866

Home (240)-291-4789 Cell: (240)-291-4789 Email: harold.akioye@gmail.com

**Professional Summary**

AWS Cloud Solutions Architect, with more than five (5) years of experience working as a Cloud Solutions Architect for several customers. Adept at developing solutions, procedures & service standards for project transformation and business excellence. Proficient in designing effective solutions for cloud deployment, transitioning multiple projects & ensuring seamless delivery of services. Exceptional hands-on experience in managing server infrastructures, database migration and data center operations. Implementing upgradable, scalable, hyper-converged infrastructure and micro-services with AWS Cloud.

**Skills**

|  |  |
| --- | --- |
| Python, Firewalls & Log Analysis, SIEM, etc. Docker Containers, Jenkins, Puppet, Chef, Terraform, Ansible. AWS Inspector, AWS Shield, Macie, Guard Duty, AWS Secret Manager, (IDS/IPS) SIEM (Splunk), Cloud Applications - Splunk, Oracle Databases, SQL, Open SSH, OpsWorks, Barracuda. | Kubernetes, Elastic Beanstalk – Amazon Web Services (EC2, EBS,  S3, IAM, AMI, VPC, VPC Peering, NACL, Security Groups, Route53, Auto Scaling, ELB, SNS, Cloud Watch, Cloud Formation, Terraform, , AWS Cloud Computing Services. |

**Certifications**

* **AWS Certified Cloud Practitioner - (Certified)**
* **AWS Certified Solutions Architect - Associate (Certified)**
* **AWS Developer Associate (Certified)**
* **AWS Certified SysOps Administrator - Associate (In-View)**

**Work History**

|  |  |
| --- | --- |
| 09/2018 to 10/2020 | Consultant; Cloud Solutions Architect  Chase Bank – Reston, Virginia   * Designed and contributed to security architecture processes that enable the enterprise to develop and implement secure solutions and capabilities that are clearly aligned with the business, technology, and threat drivers. * Design, implement and maintain all AWS infrastructure and services within a managed service environment. * Design, Deploy and maintain enterprise class security, network and systems management applications within an AWS environment. * Implement process and quality improvements through task automation. Institute infrastructure as code, security automation and automation or routine maintenance tasks. * Deep understanding of Cloud Services for Amazon Web Services (AWS), Azure, Google, etc. Including, but not limited to, Infrastructure as a Service (VPC/VNET, EC2/Virtual Machines, Security Groups, Network ACL, ELB/ALB/NLB, etc), Platform as a Service (EBS/S3/Blob, Database, Route53, CDN, etc), Serverless Services (Lambda/Functions, etc), Micro Services (Docker,ECS, etc), Security Services (GuardDuty, WAF, HSM, KMS, etc). * AWS Cloud Services experience; solution delivery expertise, migration of applications to the cloud, automation through various tools both AWS native and third-party. * Experience working in a hybrid IT configuration with customer workloads in multiple locations or cloud service providers. * Knowledge of Identity and Access Management. * Participated in architectural discussions with customers when building new and migrating existing applications on a multi cloud platform including both Azure and AWS cloud platform. * Provisioned cloud networking architectures in a DevTest environment, utilizing Virtual Networks, VPN, Express Route/Direct Connect, Vnet/subnets, Network Security Groups, Load Balancers. * Experienced with "on-premise to cloud" migrations and IT transformations with the aid of Azure solutions, promoting the use of industry best practices, security frameworks, automation and standardization. * Configured and provisioned micro-services and instances on both Azure and AWS Cloud Platform using Azure Container Instance and AWS ECS. * Proactively monitored resources and applications using AWS CloudWatch including creating alarms to monitor metrics for services like EBS, EC2, ELB, RDS, S3. * Experience in setting up Life-cycle policies to back data from AWS S3 to AWS Glacier for archiving. * Built VPCs from scratch, creating private and public subnets, security groups and network access lists, configuring Internet gateways, and NAT gateway. * Created business continuity/disaster recovery, fail-over and runbook documentation, identifying the top cloud architecture solutions to successfully meet the strategic needs of the company. * Responsible for deploying web/application servers and database traditional servers in Azure Virtual Network and AWS VPC. * Scripted manually built services in DevTest environment into Azure Template and CloudFormation, and maintained the templates and stacks leveraging Azure Blob Storage and AWS S3. |

|  |  |
| --- | --- |
| 08/2017 to 09/2018  07/2016 to 08/2017 | Consultant; Cloud Engineer  Citigroup – Remote/Onsite, VA   * Work with distributed teams to design and develop frameworks, solution accelerators, proofs of concept, and external customer facing products. * Configured multi-account architecture, identity and access management, governance, data security, network design, and logging within provisioned AWS Landing Zones using AWS Cloud Formation. * Automated snapshot backup, stopping and starting EC2 servers using Ansible playbook I wrote. * Manually built over 300 VPCs, creating both private and public subnets, security groups, network access lists and configuring internet gateways to drive traffic to VPC. * Reviewed/Monitored entire environment and execute initiatives to reduce failures, defects, and improve overall performance. * Provided incident management support on escalated trouble tickets when necessary. * Deployed hundreds of Amazon Workspaces and App Stream 2.0 for end users. * Conducted education/training sessions for Azure cloud services and offering guidance in infrastructure movement techniques including bulk application transfers into the Azure cloud platform. * Hands-on experience writing Production-ready automation code to implement solutions with Puppet, Ansible, CloudFormation, Terraform. * Designed production, staging, QA and development Cloud Infrastructures. * Experience with building, delivering, and managing hybrid Cloud IaaS environments in Azure cloud platform. * Creating solutions using PaaS with cloud platforms such as Azure. * Experienced in Azure and AWS cloud migration. * Managed AWS-provided portal account access credentials and privileges. * Rotated IAM access keys regularly and standardize on a selected number of days for password expiration to ensure that data cannot be accessed with a potential lost or stolen key. * Consistently built VPCs from scratch, creating private and public sub-nets, creating security groups and network access lists, configuring internet gateways, OpenVPN, creating AMI, understanding of user access management/role based access/multi- factor authentication and API access, configuration of auto scaling and elastic load balancer for scaling services, configuration of SNS to send notifications and Cloud Watch to collect logs and metrics. * Worked with engineers and development teams to ensure that architecture solutions are compliant with security frameworks, such as NIST, FedRAMP, ISO 27001/27002, PCI, etc. * Designed and contributed to security architecture processes that enable the enterprise to develop and implement secure solutions and capabilities that are clearly aligned with the business, technology, and threat drivers. * Participated in application and infrastructure projects and other business initiatives to provide security-planning guidance with the following drivers: reduce risk, protect business applications while ensuring the highest level of data and infrastructure (endpoints, servers, networks, data center, cloud) security. * Reviewed and evaluated current access routes, sites, vendor integration points, and security platform v integrations; recommended improvements and develop corrective strategies to improve security prior to implementation. * Involved with the design and security oversight of next-generation firewalls, intrusion prevention systems, DDoS solutions, SSL-terminating load balancers, WAF, security groups and NACL. * Turned on Redshift audit logging in order to support auditing and post-incident forensic investigations for a given database. * Encrypted data stored in EBS as an added layer of security. * Encrypted Amazon RDS as an added layer of security. * Restricted access to RDS instances to decrease the risk of malicious activities such as brute force attacks, SQL injections, or DoS attacks. * Encrypted highly sensitive data such as Protected Health Information (PHI) or Personally Identifiable Information (PII) using customer-controlled keys. * Granted the fewest privileges possible for application users. * Involved IT security teams throughout the application development life-cycle. * Inventoried and categorized all existing custom applications deployed in AWS.   Consultant; Cloud Engineer  CVS Pharmacy – Remote Reston, VA   * Assisted with designed and security oversight of next-generation firewalls, intrusion prevention systems, DDoS solutions, SSL-terminating load balancers, WAF, security groups and NACL. * Strong understanding of information processing principles and practices. * In-depth technical knowledge of networks, storage systems and computing platforms including Amazon AWS, .NET, Windows, and CI/CD pipelines. * As a last line of defense against a compromised account, I ensured all IAM users have multi-factor authentication activated for their individual accounts and limited the number of IAM users with administrative privileges. * Rotated IAM access keys regularly and standardize on a selected number of days for password expiration to ensure that data cannot be accessed with a potential lost or stolen key. * Turned on Redshift audit logging in order to support auditing and post-incident forensic investigations for a given database. * Encrypted data stored in EBS as an added layer of security. * Encrypted Amazon RDS as an added layer of security. * Recommended and managed transmission protection requirements for all environments (systems, applications, containers, etc.) such as VPC peering best practices, SSL certificate management, key pairs, etc * Created and executed a strategy to build mindshare and broad use of AWS within a wide range of customers and partners. * Work with onboarding internal clients. * Solution design for client opportunities in one or more AWS Competencies or general cloud managed services. * Create a lift and shift process model clearly defining the individual steps of the lift and shift process. * Designed and implemented monitoring and protection capabilities to help identify and protect against DoS attacks, MITM, EC2 instance compromise, secret compromise, etc. * Developed tactical response procedures for security incidents. * Performed security monitoring, security event triage, and incident response; coordinate with other team members and management to document and report incidents. * Operational experience with network security appliances with a clear understanding of the architecture behind secure networks, DMZ's, NAT's, rule placement, VPN setup, and system maintenance. * Led root cause analysis, debugging, support, and postmortem analysis for security incidents and service interruptions. * Enabled Cloud Trail across all geographic regions and AWS services to prevent activity monitoring gaps. * Enabled Cloud Trail log file validation so that any changes made to the log file itself after it has been delivered to the S3 bucket is trackable to ensure log file integrity. * Enabled access logging for Cloud Trail S3 bucket so that you can track access requests and identify potentially unauthorized or unwarranted access attempts. |

**Education**

Expected in 07/2021 Bachelor of Science: Cloud System Administration

Western Governors University – Online

06/2016 Bachelor of Science: Civil Engineering Covenant University - Ota, Nigeria