**JOSEPH OMIJIE**

5335 TANEY AVE, ALEXANDRIA, VA 22304
Cell: 5712746423, Email: omijiejosep@gmail.com

**Professional Summary**

A multi-skilled solutions architect/Cloud engineer experienced in cloud services/architecture in addition to information security, Risk Management and possess a special set of skills, managing server infrastructures and data center operations. Implementing upgradable, scalable, Hyper-converged infrastructure and micro-services across multiple platforms (Unix, Linux, Amazon Linux). Helping Client meets and exceeds business expectations...

**Certifications**

* **AWS Certified Cloud Practitioner - Certified.**
* **AWS Certified Solutions Architect (Associate) Certified.**
* **AWS Certified Security Specialty-Certified**
* **AWS Certified Developer Associates**
* **Splunk Core User - Certified**
* **Splunk Power User - Certified**
* **CompTIA SECURITY+ Certified**

**Skills**

|  |  |
| --- | --- |
| • Amazon Web Services (EC2, EBS, S3, IAM, AMI, VPC, VPC Peering, NACL, Lambda, SG, Route53, ASG, ELB, SNS, CloudWatch, Elastic Beanstalk, Cloud Formation), Terraform, API Gateway, CodeCommit, AWS CodeBuild, AWS CodeDeploy, AWS CodePipeline, Cloud Passage, F5, Barracuda Guardian Angel, Jira, Aviatrix, F5 .• Information Protection and Analysis. | • Governance, Risk & Compliance (GRC)• AWS, Azure, Google Cloud, Salesforce, BCP & DRP, PKI, Scripting.• Gradle, Git, bitbucket, Docker, Ansible, Kubernetes, Bamboo, Slack, Nagios, Jenkins.• Database Querying Languages; MySQL, NOSQL/DynamoDB, Python,• Team Motivation/ Self-motivation• Strong verbal communication. |

**Work History**

|  |  |
| --- | --- |
| 01/2020 to Current | Consultant; Cloud Security Engineer Capital One – Richmond, VA* Worked with customers engineering teams to understand infrastructure requirements, provide insight and direction to achieve a balance between strategic design and tactical needs.
* Experience in documenting security controls for DevOps and Cloud environments using industry standard guidelines such as Center for Internet Security (CIS), Cloud Security Alliance (CSA) in conjunction with business requirements.
* Strong practiced and demonstrated knowledge of AWS Networking including VPCs (sharing and peering), NACLs, Security Groups, Routing, Subnets, NAT Gateways, ELB/ALB, Route53 Public and Private Zones and Resolvers.
* Strong experience with various source code management tools such as GitHub, GitLab, Bitbucket etc.
* Experience with many of AWS services 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, Database, Route53, CDN, etc), Serverless Services (Lambda/Functions, etc), Micro Services (Docker, ECS, etc), Security Services (GuardDuty, WAF, Cloud HSM, KMS, etc).
* Deployed resources, made infrastructural change through the Jenkins CI/CD pipeline to production.
* Experience building distributed, failure-resistant architecture, including disaster recovery, backups, failover, etc.
* Experience with CI/CD tools like Jenkins, Maven, AWS Code Commit, AWS CodeDeploy, Docker etc.
* Used Kubernetes to orchestrate the deployment, scaling and management of Docker Containers.
* Utilized Kubernetes for the runtime environment of the CI/CD system to build, test deploy.
* Utilization of SQL and SPL to query logs and other forms of data.
* Monitor and test system performance for potential bottlenecks, identify possible solutions, and work with other team members to implement those fixes.
 |
| 03/2017 to 12/2019 | Consultant; AWS Solutions Architect Boeing – Arlington, VA* Developed technical plans and roadmaps.
* Designed and implement AWS cloud infrastructure tools.
* Designed and implement proactive monitoring solutions to ensure service SLA's and other metrics are met.
* Assisted in migration and maintenance of development, staging, and production environments in AWS using Terraform configurations (infrastructure as code).
* Built VPCs from scratch, creating private and public subnets, 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 if a configured threshold has been exceeded, configuration of SNS to send notifications and Cloud Watch to collect logs and metrics.
* Participate in deep architectural discussions to build confidence and ensure customer success when building new and migrating existing applications, software and services on the AWS platform.
* Proactively monitor resources and applications using AWS CloudWatch including creating alarms to monitor metrics such as EBS, EC2, ELB, RDS, S3, SNS and configured notifications for the alarms generated based on events defined.
* Third Party Vendor engagement and coordination to customer site for Demo and POC.
* Created implementation diagrams and data flow mappings for all projects with current customer.
* Involved in development of test environment on Docker containers and configuration of Docker containers using Kubernetes.
* Experience with container-based deployments using Docker, working with Docker images, Docker Hub and Docker-registries and Kubernetes.
* Presentation skills with a high degree of comfort speaking with executives, IT Management, and developers; strong communication skills with an ability to right level conversations.
* Created life cycle policies to back the data from AWS S3 to AWS Glacier in line with business compliance and need.
* Configured NACL and security groups, thus limiting malicious attacks from blacklisted range IP addresses.
* Designed and managed public/private cloud infrastructures, using Amazon Web Services which include EC2, S3, Cloud Front, Elastic File System, RDS, VPC, Direct Connect Route53, Cloud Watch, Cloud Trail, Cloud Formation, and IAM roles for several customers (WAG Departments).
* Knowledge of AWS and common open source VPN technologies, such as OpenVPN server for SSL VPN.
* Implemented security and compliance in the cloud using various tools like Guard duty, WAF, Inspector, Security Hub, Amazon Macie, Config rules, SSM, Baracuda guardian angel, Dome9 etc.
* Proficient in Linux OS (CentOS, Ubuntu) and bash/shell scripting.
* Strong experience with JIRA and Confluence administration and Agile principles.
* Analyzed, develop, and execute a plan to migrate eligible applications from on-prem to the cloud.
 |

|  |  |
| --- | --- |
| 01/2014 to 02/2017 | AWS Cloud EngineerHilton Headquarters – McLean, VA* Experienced in designing the overall Virtual VPC environment including server instance, storage instances, subnets, network access controls, security groups, peers, availability zones etc.
* Provisioning and setting up of Integrated AWS Solutions such as EC2, S3, RDS, EMR etc.
* Knowledge of cloud virtualization technologies, such as VMware, Hyper-V etc
* Design and implement proactive monitoring solutions to ensure service SLA's and other metrics are met.
* Supported and advise in project that involves planning, analysis, design, development, testing, quality assurance, configuration, installation, implementation, integration, maintenance, and management of cloud IT assets and infrastructure.
* Managed services such as RDS, SQS, SNS, Kinesis, ElastiCache, Elastic Beanstalk, IAM, Cognito and others.
* Proficient in managing customer’s Security, Identity, directory, authentication/authorization, single-sign-on, access management, API hardening, encryption, data privacy, backup, and disaster recovery.
* Strong experience with Cloud Formation and Terraform Automation.
* Helped educate enterprise customers on AWS and participated in deep architectural discussions to ensure solutions are designed for successful deployment in the cloud.
* Migrated from On-Premise Infrastructure to AWS Cloud using third party software like cloud endure.
* Ability to work within an agile project management methodology.
* Excellent verbal/written communication skills, including communicating technical issues to non-technical audiences.
 |

|  |  |
| --- | --- |
| 03/2012 to 12/2013 | Consultant; Information Security AnalystGDIT– Towson, MD* Participated in Risk Assessment and documentation of controls.Reviewed audit logs and identified any unusual or suspicious event/behavior notifying the end client concerning suspicious traffic.
* Utilizing the Cyber Security Assessments and Management (CSAM) tool to record, manage, assess and remediate failed security controls.
* I used Nessus Vulnerability Scanner to detect potential risks on a single or multiple asset across the company Network.
* Documented, Reviewed and updated security policies and procedures like Incident response plans (IR), contingency plans (CP), contingency plan tests (CPT), privacy impact assessments (PIA), and risk assessment (RA) documents.
* Defined, implement and maintain corporate security policies.Proficient in explaining technical information, resolutions, documentations, and presentations to clients and non-technical personnel at all levels of the organization.
* Strong experience in computer networking concepts and protocols, and network security methodologies.
* Strong experience in network access, identity, and access management (e.g., public key infrastructure, Oauth, OpenID, SAML).
* Experience provisioning solution for network security (e.g., encryption, firewalls, authentication, honey pots, perimeter protection).
* Directly involved in cyber-attack stages (e.g., reconnaissance, scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks).
 |

**Education**

|  |  |
| --- | --- |
| 12/2010 | Bachelor of Engineering: Mechanical Engineering Technology Ambrose Alli University - Overseas  |

|  |  |
| --- | --- |
| 05/2018 | Master of Science: Computer Information Systems California University of Management and Sciences - Arlington, VA |

|  |  |
| --- | --- |
| 04/2018 | Certificate of Completion: Cloud Security Architecture and Operations SANS INSTITUTE - Orlando, FL  |