**Emmanuel C. Nnodim**

2238 Brightseat Road, Hyattsville, MD 20785  20721, 9809 Glenkirk Street, MD
Home: (240)-556-3645- Cell: (240)-556-3645- e.nnodim@yahoo.com

**Professional Summary**

AWS Solutions Architect with Six (6) + years of experience and a Breadth of expertise in private and public Cloud Computing (i.e. AWS platform), technologies, and architectural best practices. Vast experience across the Enterprise IT in each of the following fields: Infrastructure architecture; Information Science, Database architecture; Advanced Networking; IT Security; Enterprise DevOps; and Analytics.

**Certifications**

**• AWS Certified Cloud Practitioner - Certified
• AWS Solutions Architect Associate – Certified**

**• AWS Certified Security Specialty – (In-View)
• AWS SysOps Administrator Associate – Certified**

**• AWS Developer Associate – Certified**

**Skills**

|  |  |
| --- | --- |
| Firewalls & Log Analysis, SIEM, etc.Orchestration Services ECS, Docker Containers, Jenkins, Puppet, Chef, Terraform, Ansible. AWS Inspector, AWS Shield, Macie, Guard Duty, AWS Secret Manager, (IDS/IPS) SIEM (Splunk/Qradar) Palo. Cloud Applications - Splunk, Nagios, DNS, OpenVPN, Open SSH, VPG, OpsWorks. | Database Querying Languages; PostgreSQL, MySQL, SQL Server, NoSQL/DynamoDB. Elastic Beanstalk – Amazon Web Services (EC2, EBS, S3, IAM, AMI, VPC, VPC Peering, NACL, Route53, Auto Scaling, ELB, SNS, Cloud Watch, and Cloud Formation). Dome9, Barracuda Guardian Security, F5.  |

**Work History**

|  |  |
| --- | --- |
| 02/2019 to 08/2020 | Consultant: AWS Solutions Architect/Security EngineerRite Aid – Rockville, MD* Configured Docker container for branching purposes.
* Provisioned AWS Landing Zones to create a customized baseline of AWS accounts, networks, and security policies.
* Configured multi-account architecture, identity and access management, governance, data security, network design, and logging within provisioned AWS Landing Zones.
* AWS – 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, 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 security solutions and capabilities that are aligned with the business, technology, and threat drivers.
* Hands-on AWS Technical Architect with 5 Years in developing and Architecting enterprise-level large scale multi-tier solutions that require complex Architectural decisions.
* Result-oriented approach with Exceptional leadership skills.
* Extensive experience defining IT Roadmap, cloud strategy, Enterprise/solution architecture, Architecture assessment.
* Hands-on experience on implementing Cloud Solutions using various AWS services including EC2, VPC, S3, Glacier, EFS, AWS Kinesis, Lambda, Directory Services, Cloud Formation, Ops Works, Code Pipeline, Code Build, Code Deploy, Elastic Beanstalk, RDS, Data Pipeline, DynamoDB, Redshift, etc.
* Hands-on experience on Architecting and securing the Infrastructure on AWS using IAM, KMS, SSO, MFA, Cognito, API Gateway, Cloud Trail, Cloud Watch, Config, Trusted Advisor, Security Groups, NACL, etc.
* Worked closely with Project Managers to understand a code/configuration release scope and how to confirm a release was successful.
* Wrote Puppet models for installing and managing java versions using the Eclipse
* Ensure compliance to defined privileged user access controls.
* Experience in deploying and monitoring applications on various platforms using Elastic Beanstalk, setting up the life cycle policies to back the data from AWS S3 to AWS Glacier.
* Provisioned AWS Landing Zones to create a customized baseline of AWS accounts, networks, and security policies.
* Configured multi-account architecture, identity and access management, governance, data security, network design, and logging within provisioned AWS Landing Zones.
* AWS – 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, configuration of SNS to send notifications, and Cloud Watch to collect logs and metrics.* Practiced understanding of AWS Organizations and account modeling strategies to segment billing, network, identity, management, etc.
* 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.
* ELB/ALB, Route53 Public and Private Zones and Resolvers.
* Identify opportunities for infrastructure optimization and cost reduction
* Practiced understanding of AWS Organizations and account modeling strategies to segment billing, network, identity, management, etc.
* 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.
 |
| 10/2016 to 02/201908/2014 to 10/2016 | Consultant: AWS Solutions Arch/Cloud Security Engineer Bank of America – Chicago, IL* Assisted with designed and security oversight of next-generation firewalls, intrusion prevention systems, DDoS solutions, SSL-terminating load balancers, WAF, security groups, and NACL.
* Designing and implementation of public and private facing websites on AWS Cloud.
* Migrating from On-Premise Infrastructure to AWS Cloud.
* Focusing on high-availability, fault tolerance, and auto-scaling using AWS Cloud Formation. Configured and managed various AWS Services including EC2, RDS, VPC, S3, Glacier, Cloud Watch, Cloud Front, and Route 53, etc.
* Configured various performance metrics using AWS Cloud watch & Cloud Trial
* 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.
* 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.
* Designed and implemented system security and data assurance Extensive experience interacting with AWS infrastructure via AWS Command Line Interface (CLI).
* Experience with deployment orchestration, automation, and security configuration management (Jenkins, Terraform, Ansible) preferred.
* Implemented DevOps practices such as infrastructure as code, continuous integration, and automated deployment.
* Good understanding of enterprise architecture and operational procedures such as availability, recovery, archiving, etc.
* 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.
* 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.
* Created and managed user accounts, groups and service permission using IAM. Granted the least privileged access, Enabled Identity federation for multiple accounts by leveraging AWS SSO, Utilized MFA and enabled IAM Access Analyzer to review access policies on S3.
* 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.
* Enabled required SSL parameter in all Redshift clusters to minimize the risk of the man-in-the-middle attack.
* 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.
* Provisioned load balancer, auto-scaling group, and launch configuration for microservices using Ansible.
* Installation of search technologies such as Apache Solr on AWS EC2.
* Creation of dynamic inventory on Ansible for the management of resources on AWS.
* Installation of Apache Tomcat on EC2 instances and the utilization of STS to request for temporary credentials for IAM users.

Consultant: Cloud Security Engineer Wells Fargo – Beaverton, OR* Developed tactical response procedures for security incidentsPerformed 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.
* Own all aspects of cloud security product definition including vendor integration, platform integration, and monitoring for cloud platforms including but not limited to AWS, Azure, and Google Cloud.

 Serve as the subject matter expert for the products and features and acts as a product evangelist to build internal awareness across the organization.* Performed security monitoring, security event triage, and incident response coordinate with other team members and management to document and report incidents.
* 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 environments and executed initiatives to reduce failures, defects, and improve overall performance.
* Provided incident management support on escalated trouble tickets when necessary.
* Deployed Palo Alto VM1 & VM2 Series Firewall in AWS, configured High Availability (HA) pair in AWS.
* Deployed and configured Palo Alto Panorama Product to manage several firewalls, creating a one-click deployment solution to firewalls on the network.
* Recognize, adopt, utilize, and teach best practices in cloud security engineering
* Participate in efforts to promote security throughout the project and build good working relationships within the team and with others in the organization
* Participate in efforts that tailor the company’s security policies and standards for use in cloud environments.
* Defined, assessed, and communicated security risk to product owners. Deployed hundreds of Amazon Workspaces and App Stream 2.0 for end-users working from home.
* Enabled access logging for Cloud Trail S3 bucket so that you can track access requests and identify potentially unauthorized or unwarranted access attempts.
* Assisted in the build, deploy, and tune process of scalable systems that automate security event detection, response, and repeatable tasks.
* Kept up to date on emerging vulnerability, response, mitigation, threat landscape trends, and use this knowledge to drive proactive threat monitoring.
* Participated in creating innovative ways to use a wide range of security event data to advance detection methods.
* Introduced, provided, and reviewed architectural work in local projects in a joint approach with local companies based on secured architecture development methods.
* Made recommendations, gained approval, and developed implementation strategies for new technologies based on necessity.
* Conducted large scale projects and research through all stages: concept formulation, the definition of metrics, determination of appropriate methodology, research evaluation, and final research report.
 |

**Education**

|  |  |
| --- | --- |
| 05/2020 | **Bachelor of Science, Information Science** **University of Maryland, College Park, MD** |

|  |  |
| --- | --- |
| Expected 06/2022 | Bachelor of Science: Cloud System Administration Western Governors University - Online |