HEBERT NTSE

(240) 838 4768 | hebertntse@gmail.com | www.linkedin.com/in/hebert-ntse-9b7259197

A self-motivated Cloud Security engineer offering over 12 years of experience in Cloud/Linux/ environment with expertise in cloud security, identity and access management, monitoring and event management, governance and compliance and data protection.

Passionate about designing and implementing automated security solutions to enhance system efficiency and ensure robust protection

Technical Skills:

AWS Security	WIZ, AWS Security Hub, AWS Guard Duty, AWS Shield, AWS Firewall Manager, AWS Inspector.
Monitoring	Cloud Watch, Datadog
Web Server	Nginx, Apache Tomcat, Apache Httpd
Scripting	Bash, Groovy, Python
CI/CD	Jenkins, Azure DevOps
Configuration Management	Ansible, AWS Systems Manager
Containers & Orchestration	Docker, ECS, EKS
Operating Systems	Linux, Windows
Version Control	Git, Bitbucket
IaC	Terraform, CloudFormation
Network	VPC, TGW, IGW, NGW
AWS Services	S3, EC2, VPC, SNS, SQS, Lambda, ELB, RDS, SES, Route53, CloudFront, Auto Scaling, CloudWatch
Azure Services	Azure Policies, Azure DevOps
Governance & Compliance	AWS Config, AWS Organizations, SCP, Trusted Advisor, AWS Well Architected Tool
Identity & Access Management	AWS IAM, AWS Organization, Active Directory, AWS Single Sign On, AWS AD Connector, Roles Anywhere

Professional Experience:

Sr. Cloud Security Engineer
CISCO ***present***

- Implemented and managed Wiz to seamlessly integrate with multi-cloud environments including AWS and Azure, enabling centralized security visibility and compliance monitoring across multi cloud platforms.
- Developed and implemented custom Wiz controls, cloud configuration rules, and event rules to enforce rigorous security standards and ensure compliance.
- Used AWS IAM Roles Anywhere service to extend AWS IAM roles to workloads such as Jenkins servers outside of AWS by use of Private Certificate Authority.
- Built and maintained an Elasticbeanstalk environment on AWS using terraform and deployed a CICD pipeline using Jenkins to deploy new application versions to the environment.
- Configured AWS session manager using terraform to manage Amazon elasticbeanstalk servers through an interactive one-click browser-based shell and then blocked the use of SSH access.
- Deployed a static website on Amazon s3 for internal users by leveraging private link service and an application loadbalancer.
- Deployed and managed Kubernetes clusters on AWS EKS for production environments.
- Built an EC2 Image pipeline for automating custom AMI builds for EKS managed Node groups using Parameter Store, EventBridge, Lambda Function, EC2 Image Builder and EKS
- Configured Kubernetes networking components such as service discovery, load balancing, and Ingress.
- Monitored and troubleshooted Kubernetes applications using tools such as CloudWatch Logs, Prometheus, Grafana, and Fluentd.
- Installed Prometheus on EKS clusters using Helm charts. Configured Prometheus to scrape metrics from various systems and applications.
- Installed Grafana on Kubernetes clusters using Helm Charts. Configured Grafana to connect to Prometheus as data source. Created dashboards and alerts based on data from Prometheus.
- Maintained and updated Kubernetes clusters with security patches and updates.
- Developed and maintained automation scripts using Python and AWS Lambda functions and boto3.
- Created AWS Config rules using AWS Lambda and boto3 library to monitor resource compliance.
- Used Migrate for Compute Engine (M4CE) to migrate VMs from AWS Cloud to GCP.

- Studied existing application infrastructures running on AWS and developed Terraform code for these applications to be migrated to GCP.
- Automated Terraform deployment with GitHub Actions.
- Developed Technology Architecture Proposals (TAP) for migrating On-prem applications to AWS Cloud
- Designed and deployed highly available and fault tolerant applications on AWS Elastic Kubernetes Service (EKS)
- Designed complex Solution Design Documentation (SDD) for complex environments on AWS
- Designed and implemented for elasticity, availability and scalability using ElastiCache, RDS – Edge locations, RDS
- Managed provisioning of AWS infrastructures using CloudFormation and Terraform
- Developed and documented security guardrails for AWS Cloud environments
- Developed Terraform scripts to build complex environments on AWS with services like Amazon Cognito user pool as an authorizer for API Gateway REST API.
- Configured and used AWS Backup to backup all resources that have a production tag.
- Configured Multi Region S3 buckets to use a single Multi-Region Access Point to improve latency and disaster recovery.
- Configured and integrated NewRelic monitoring tool to monitor CloudWatch metrics from all AWS Services.

DevOps Engineer/Cloud Engineer,

MERCK ***02/2017* – 10/2021**

- Configured and managed various AWS services such as EC2, ELB, Application Load Balancer, VPC, Subnets, Security groups, S3 Buckets, Cloud Watch, Cloud Trail, Elastic Container Service (ECS), NAT gateway, and IAM Roles.
- Developed Technology Architecture Proposals (TAP) for migrating On-prem applications to AWS Cloud
- Managed provisioning of AWS infrastructures using CloudFormation and Terraform
- Created Terraform modules for two tier Architecture which includes AWS resources VPC, Subnets, Security groups, Load Balancers, Auto scaling group, Cloud watch Alarms, ECS clusters, S3 buckets for logs.
- Successfully built and configured CI/CD pipelines using AWS CodePipline and AWS CodeBuild for application development.
- Built Jenkins jobs to create AWS infrastructure from GitHub repos containing Terraform code to deploy different Applications infrastructure for Dev, QA and Pre-prod based on the requirement from different teams as Infrastructure as a Code.
- Created Restful API's with Lambda Proxy Integrations using API Gateway to map the client request to backend Lambda function.
- Leveraged Docker to build, test and deploy applications in different environments.
- Involved in Development and Implementation of CI/CD pipeline using Jenkins, Ansible, Terraform, ECS and Docker containers to complete the automation from commit to deployment.
- Integrated SonarQube with Jenkins to analyze code quality and obtain combined code coverage reports after performing static code analysis.
- Created Ansible playbooks to automatically install packages from a repository, to change the configuration of remotely configured machines and to deploy new builds.
- Leveraged AWS Elastic Kubernetes Service (EKS), Jenkins and GitHub, to deploy Microservices applications into AWS Cloud.
- Supported AWS Cloud environment with multiple AWS servers and configured Elastic IP & Elastic Storage, Load balancing, Security groups and Network ACLs, S3 buckets for logs.
- Built and deployed Docker containers to break up monolithic app into microservices, improving developer workflow, increasing scalability, and optimizing speed.
- Used Ansible to provision and configure clusters in Kubernetes.
- Configured Git with Jenkins and schedule jobs using POLL SCM option.

AWS Solutions Architect

PENFED CREDIT UNION ***04/2014* – 01/2017**

- Implemented Machine Image Pipeline and integrated Patch Management
- Migrated legacy applications to AWS cloud environment
- Configure Palo Alto Firewalls and CSRs
- Leveraged Docker to build, test and deploy applications in different environments.
- Developed LLDs for migrating various applications including network sizing, Instance types, names, tags etc.
- Developed required and optional tagging reference document for automation, compliance and consolidated billing
- Developed baseline VPC and Network design including leveraging VPN connectivity and Direct Connect
- Developed baseline AWS account security, implemented/integrated end-point protection, vulnerability scanning and intelligent threat detection
- Built severless architecture with Lambda integrated with SNS, Cloudwatch logs and other AWS services.
- Leveraged automated DevOps tools deployment and Blue-green deployment patterns and strategies

- Configured CI/CD Pipelines using Jenkins connected to Github and build environments (Dev, stage & Prod)
- Implemented IAM best practices and role-based access control
- Deployed tenable.io for integration with AWS for vulnerability, configuration and compliance assessment and leveraged pre-authorized Nessus scanner to secure AWS environments and EC2 instances
- Implemented AWS Organization to centrally manage multiple AWS accounts including consolidated billing and policy-based restrictions
- Implemented Control Tower Preventive and Detective guardrails and leveraged Account Factory, integrated with Lambda for new AWS account creation and setup.
- Setup Ansible control and slave nodes and developed playbooks to automation configuration of servers across environments.
- Design for high availability and business continuity using self-healing-based architectures, fail-over routing policies, multi-AZ deployment of EC2 instances, ELB health checks, Auto Scaling and other disaster recovery models.
- Created patch management using Systems Manager automation for multi-region and multi account execution
- Implemented preventive guardrails using Service Control Policies (SCPs)
- Implemented detective guardrails using Cloud Custodian policies and AWS config
- Designed and implemented for elasticity and scalability using ElastiCache, CloudFront – Edge locations, RDS (read replicas, instance sizes) etc.
- Implemented security best practices in AWS including multi factor authentication, access key rotation, encryption using KMS, firewalls- security groups and NACLs, S3 bucket policies and ACLs, mitigating DDOS attacks etc
- Implemented Jenkins, GitHub and Git for version control, code build, testing and release and CI/CD.
- Monitored end-to-end infrastructure using CloudWatch and SNS for notification
- Used AWS system manager to automate operational tasks across AWS resources
- Project Management -AWS Infra design & application migration
- Used System Manager to automate operational tasks across WK AWS infrastructure.
- Setup AWS Single Sign On (SSO) for on premise Active Director (AD)
- Built kinesis dashboards and applications that react to incoming data using AWS provided SDKs; and exported data from kinesis to other AWS services including EMR for analytics, S3 for storage, Redshift for big data and Lambda for event driven actions
- Built custom images though docker server, docker compose with multiple local containers and created production grade workflows and a continuous application workflow for multiple images
- Implemented multiple container deployments to AWS and maintained sets of containers with deployments
- Setup, Configured, and used Ad Hoc ansible Commands

Linux Systems Administrator
KPMG ***03/2011- 03/2014***

- Maintained server integrity by applying updates and patches per our maintenance policies
- Configured and Managed NFS and Samba for File Sharing
- Configured and Managed Firewalld
- Configured and Managed Apache Web Service
- Controlled access to files and directories using ACL permissions
- Performed package management, system updates using yum and rpm
- Created partitions, including raid, logical volumes and swap, formatted with ext3 and ext4, zfx, resized and created logical partitions
- Managed and Configured Postfix for Relay SMTP
- Hardened Linux servers based on recommendations provided by our security team and best practice.
- Prepare Standard Operating Procedures (SOPs), work instructions, and related supporting documents based on Quality Systems Unit guidelines.

EDUCATION: ***GPA: 3.21***

Bachelor of Science, Electrical and Computer Engineering, University of Buea, Cameroon.

CERTIFICATIONS:

- ***AWS Certified Solutions Architect - Associate***
- ***AWS Certified Security Specialty***
- ***HashiCorp Certified Terraform Associate***