Job Ref. No: JLIL 378

Position: Cloud Engineer

Jubilee Insurance was established in August 1937, as the first locally incorporated Insurance Company based in Mombasa. Jubilee Insurance has spread its sphere of influence throughout the region to become the largest Composite insurer in East Africa, handling Life, Pensions, Asset Management and Medical Insurance. Today, Jubilee is the number one insurer in East Africa with over 1.9 million clients. Jubilee Insurance has a network of offices in Kenya, Uganda, Tanzania, Burundi. It is the only ISO certified insurance group listed on the three East Africa stock exchanges – The Nairobi Securities Exchange (NSE), Dar es Salaam Stock Exchange and Uganda Securities Exchange. Its regional offices are highly rated on leadership, quality and risk management and have been awarded an AA- in Kenya and Uganda, and an A+ in Tanzania. For more information, visit www.JubileeInsurance.com.

We currently have an exciting career opportunity for a **Cloud Engineer** within **Jubilee Life Insurance Limited.** The position holder will report to the **Manager – Cloud Services** and will be based at our Head Office in Nairobi.

Role Purpose

The Cloud Engineer will design, build, operate, secure, and optimise scalable cloud infrastructure across public cloud platforms, ensuring high availability, security, resilience, and cost efficiency. The role holder will work closely with DevOps, Security, and Application teams to support production workloads, automate infrastructure deployment, and maintain reliable cloud environments aligned to business and regulatory requirements.

Key Responsibilities
Strategy

1. Design and maintain secure, scalable, and highly available cloud infrastructure aligned to business and technology strategy.
2. Develop and implement cloud architecture standards, security baselines, and operational best practices.
3. Drive infrastructure automation initiatives to improve deployment speed, consistency, and reliability.
4. Optimise cloud spend through effective resource planning, cost governance, and FinOps practices.
5. Provide input into cloud adoption roadmaps, migration strategies, and technology refresh initiatives.
6. Stay current with evolving cloud technologies and recommend improvements to enhance performance, resilience, and security.

Operational

1. Design, deploy, and manage cloud infrastructure across AWS, Azure, OCI, and/or GCP environments.
2. Build and maintain IaaS and PaaS services including compute, storage, networking, and databases.

3. Implement high availability, backup, and disaster recovery (DR) strategies aligned to defined RTO/RPO requirements.
4. Automate infrastructure provisioning and configuration using Infrastructure as Code (IaC) tools such as Terraform, ARM, CloudFormation, or Bicep.
5. Administer Linux and Windows servers in cloud environments, including patching, performance tuning, and hardening.
6. Implement monitoring, logging, and alerting solutions using cloud-native tools (e.g., CloudWatch, Azure Monitor, OCI Monitoring).
7. Enforce cloud security best practices including IAM, RBAC, encryption, vulnerability management, and network segmentation.
8. Troubleshoot cloud infrastructure incidents, conduct root cause analysis, and implement preventive measures.
9. Support cloud migrations from on-premises or other environments to target cloud platforms.
10. Collaborate with DevOps teams on CI/CD pipelines and container orchestration platforms such as Docker and Kubernetes.
11. Develop and maintain architecture documentation, standard operating procedures (SOPs), and operational runbooks.

Corporate Governance
1. Ensure adherence to corporate IT policies, standards, and security frameworks.
2. Ensure compliance with data protection, privacy, and regulatory requirements across cloud environments.
3. Implement and maintain governance controls for identity, access, resource provisioning, and cost management.
4. Support audit processes by providing accurate documentation, logs, and compliance evidence.
5. Proactively identify and mitigate cloud-related operational and security risks.

People and Culture
1. Collaborate effectively with DevOps, Security, Application, and Project teams to deliver reliable cloud services.
2. Promote a culture of automation, documentation, and continuous improvement within the infrastructure function.
3. Share knowledge on cloud technologies and operational best practices with internal teams.
4. Demonstrate accountability, responsiveness, and ownership in supporting business-critical systems.

Key Competencies
1. Strategic thinking and planning.
2. Strong analytical and problem-solving capability.
3. Technical depth in cloud architecture and operations.
4. Effective communication and stakeholder engagement.
5. Collaboration and teamwork.
6. Adaptability in fast-evolving technology environments.
7. Results orientation and accountability.

Functional Skills
1. Hands-on cloud platform administration across AWS, Azure, OCI, or GCP.
2. Infrastructure as Code (IaC) and automation using Terraform, ARM, CloudFormation, or Bicep.
3. Windows and Linux server administration in cloud environments.

4. Cloud networking design including VPC/VNet, VPNs, load balancers, DNS, firewalls, and hybrid connectivity.
5. Implementation of cloud security controls including IAM, RBAC, encryption, and vulnerability management.
6. Backup, disaster recovery, and high availability architecture design.
7. Monitoring, logging, and incident management using cloud-native tools.
8. Cloud cost optimisation and resource governance practices.

Key Deliverables for the Role
1. Secure, scalable, and highly available cloud infrastructure environments.
2. Improved cloud performance, uptime, and service reliability metrics.
3. Reduced incident recurrence through effective root cause analysis and preventive controls.
4. Automated infrastructure deployment pipelines with improved consistency and speed.
5. Optimised cloud costs and improved resource utilisation.
6. Up-to-date cloud documentation, architecture diagrams, and operational procedures.
7. Timely resolution of cloud infrastructure and platform-related incidents.

Academic Qualifications
1. Bachelor's degree in Computer Science, Information Technology, or a related field.
2. Professional cloud certifications (e.g., Azure Administrator, AWS CloudOps Engineer Associate, Google Associate Cloud Engineer) are highly desirable.

Relevant Experience
1. Minimum of 3 years' hands-on experience managing cloud platforms (AWS, Azure, OCI, or GCP).
2. Demonstrated experience implementing cloud infrastructure, automation, and security controls in production environments.
3. Experience supporting high-availability systems and responding to critical incidents.

**If you are qualified and seeking an exciting new challenge, please apply via Recruitment@jubileekenya.com quoting the Job Reference Number and Position by 25th February 2026
Only shortlisted candidates will be contacted.**