

BERTRAND MBANWI

Site Reliability and DevSecOps Engineer

Platform and Infrastructure Security

Dallas-Fort Worth, TX | (240) 598-9680 | build@bertrandmbanwi.dev

bertrandmbanwi.dev | github.com/bertrandmbanwi | linkedin.com/in/bombanwi

US Citizen | Active DoD Secret Clearance

PROFESSIONAL SUMMARY

Hands-on engineer with 8+ years across cloud infrastructure, DevSecOps, and platform operations. Own production on-call response, root-cause analysis, observability, and recovery across Azure Government AKS and on-premises Kubernetes. Build secure delivery with Terraform, Helm, ArgoCD, and GitLab CI; validate changes through service, alerting, and restore checks. Earlier roles include AWS and EKS in federal contracting environments. Experienced working with network, storage, security, and database teams in FedRAMP, FISMA, and STIG-constrained environments.

TECHNICAL EXPERTISE

Cloud and platforms Azure Government, Azure, AKS, MKE, Kubernetes, Docker, Linux; AWS and EKS in earlier roles; Terraform, ARM templates, CloudFormation, Atlantis.

Delivery and automation ArgoCD, multi-source Helm applications, GitLab CI, GitHub Actions, Jenkins, Renovate, Bash, Python, Rundeck, Artifactory.

Reliability and security PagerDuty, Prometheus, Alertmanager, Grafana, Blackbox Exporter, Velero, Vault Secrets Operator, Azure Key Vault, Prisma Cloud Compute, RBAC, TLS and PKI.

PROFESSIONAL EXPERIENCE

DevOps Engineer

Kelmavory | Oct 2025 - Present | Remote

Own reliability, GitOps delivery, and platform security across Azure Government AKS and on-premises Mirantis Kubernetes Engine in restricted-egress environments.

Production reliability and incident response

- Carry PagerDuty on-call for production Kubernetes and shared platform services. Investigate workload, identity, networking, and storage failures; coordinate recovery and document root causes, verification steps, and follow-up actions.
- Restored an authentication delivery path by tracing image-pull and registry failures to service-mesh proxy memory exhaustion and stale ingress annotations. Corrected resource limits and configuration, and followed up on alerts that had failed to reach PagerDuty.
- Diagnosed multi-cluster NotReady nodes to an unavailable NFS storage backend after ruling out certificate expiry. Coordinated storage, network, and load-balancer recovery and postponed a cutover until the underlying failure was understood.
- Resolved AKS scheduling and maintenance blockers involving zone-bound Azure Disk storage, autoscaler behavior, and Elasticsearch disruption budgets; checked workload placement and disruption risks before rolling changes.
- Validated Velero backup restoration and GitLab repository recovery through service and repository checks. Identified missing alert coverage for partially failed backups and documented operational gaps and recovery procedures.

PROFESSIONAL EXPERIENCE CONTINUED

DevOps Engineer continued

Kelmavory | Oct 2025 - Present | Remote

Observability and recovery

- Implemented Prometheus and Alertmanager routing to PagerDuty for OOM, restart-loop, and crash-loop conditions. Configured namespace-based routing, resolved a CRD version mismatch, and validated notification delivery and automatic resolution.
- Built Blackbox Exporter synthetic checks for source control, artifact services, collaboration tools, and platform endpoints, including client-certificate authentication. Used probe timings and TLS evidence to distinguish network access failures from certificate mismatches.

GitOps and continuous delivery

- Operate ArgoCD for all Azure Government AKS clusters in a hub-and-spoke topology. Maintain multi-source Helm applications with upstream charts and separate values repositories so chart versions and environment settings are pinned and reviewed in merge requests.
- Keep production auto-sync disabled and review ArgoCD or kubectl diffs before manual sync. Promote development changes before production and document why live patches are not durable under reconciliation. On-premises MKE deployments use manual Helm upgrades.
- Own monthly ArgoCD and platform chart maintenance through Renovate merge requests, local Helm rendering, and test-to-production promotion. Resolved self-heal conflicts and distinguished controller state from workload health when applications remained Progressing.
- Caught silently ignored Helm values that left ArgoCD reporting Synced despite incorrect configuration. Added local chart rendering and key validation to pre-merge checks.
- Migrated GitLab from on-premises Kubernetes to Azure Government AKS with identity integration, backup, and repository validation. Recovered stalled pull mirroring across 114 projects by isolating stale Redis concurrency state from pre-existing repository failures.
- Maintain shared GitLab CI pipelines and migrated runners from shell to AKS Kubernetes executors. Mirror secret-scanning and build images internally, resolve registry permissions, and validate runner and pipeline changes before production use.

Infrastructure security and platform operations

- Upgraded production Prisma Cloud Compute Console and Defenders on MKE using manual Helm changes. Diagnosed a generated connection-address fault, restored all six Defenders on the target version without rollback, and rebuilt the SOP around manifest review, image-pull tests, and connection validation.
- Maintain Terraform-managed AKS infrastructure, custom certificate trust, proxy configuration, and identity/RBAC dependencies. Re-established managed identities and access bindings during AKS recovery after a tenant migration.
- Operate Vault Secrets Operator with namespace-scoped authentication and resolve CA trust between Vault and workloads. Renew PostgreSQL and PgBouncer certificates, validate certificate chains, and confirm application connectivity.
- Centralize external image distribution through Artifactory and troubleshoot restricted-egress paths using TCP, TLS, and proxy checks. Route monitoring traffic through approved proxies and support evidence-based firewall change requests.
- Perform staged Linux maintenance with service and database-team validation; automate patching with Rundeck. Produce recovery runbooks and concise incident summaries for engineering, security, and operational stakeholders.

PROFESSIONAL EXPERIENCE CONTINUED

DevSecOps Engineer

Mechanicode | Nov 2024 - Oct 2025 | Contract | Remote

Introduced container delivery and automated security checks for a CDC government contract.

- Supported Operations and Maintenance through infrastructure automation and ownership of DevSecOps pipelines.
- Containerized applications on Amazon EKS and introduced ArgoCD deployment workflows for Kubernetes delivery.
- Integrated Trivy, SonarQube, Snyk, and OWASP ZAP into Jenkins and GitHub Actions pipelines to incorporate security checks into the delivery process.

CaeliCode Solutions

Dec 2017 - Nov 2024 | Remote

DevOps Engineer Federal Subcontract

Apr 2023 - Nov 2024

Federal application delivery supporting GSA TOTAL-BIMS.

- Integrated Azure Key Vault and Fortify scanning into GitHub Actions, bringing secrets handling and security checks into application delivery.
- Built containerized environments with Docker and AKS. Reviewed Terraform changes through Atlantis to keep infrastructure updates versioned and repeatable.
- Maintained Helm and GitOps delivery practices with separate environment configuration, reviewed changes, and development-before-production validation.
- Automated REST API deployment to Azure API Management using a build-once, deploy-many approach.

DevSecOps Engineer

Jun 2019 - Mar 2023

- Built infrastructure frameworks with Terraform and ARM templates for consistent Azure provisioning.
- Operated AKS clusters with Helm deployments, RBAC, and network segmentation; investigated workload, access, and configuration failures.
- Developed Python and Bash automation for compliance reporting, vulnerability tracking, and infrastructure drift detection.
- Supported platform monitoring, incident troubleshooting, and documented recovery procedures with security and infrastructure teams.

Cloud Security Engineer

Dec 2017 - May 2019

- Designed AWS infrastructure using VPC, EC2, S3, and RDS, with automated provisioning and access controls.
- Automated deployment with CloudFormation and Ansible and implemented IAM and AWS Config controls.
- Built centralized CloudWatch and CloudTrail monitoring, backup strategies, and recovery procedures.

Cloud Infrastructure Engineer Internship

MTN Cameroon | Jun 2017 - Nov 2017 | On-site

- Supported AWS infrastructure operations, monitoring, access controls, and CloudFormation automation.
- Assisted with infrastructure troubleshooting and security patching.

SELECTED INDEPENDENT PROJECTS

Personal engineering projects, separate from employer and client work.

GitOps Supply Chain

- Implemented ArgoCD app-of-apps delivery with Helm, automated reconciliation, pruning, and self-heal in a demonstration environment.
- Implemented Cosign keyless image signing through GitHub Actions and Kyverno signature-verification and baseline runtime policies. Integrated External Secrets Operator with Azure Key Vault through workload identity in the companion platform.

[Project and implementation](#) | [GitHub source](#)

Ephemeral Azure Platform

- Built an AKS lifecycle workflow with ordered Terraform stacks, isolated state, and GitHub OIDC authentication without stored cloud credentials.
- Implemented independent Azure and Kubernetes verification, evidence capture, and teardown. Serialized infrastructure changes and applied destruction in reverse dependency order.

[Project and implementation](#) | [GitHub source](#)

Actions Runner Control Plane

- Built an operational dashboard for self-hosted GitHub Actions runners using webhook ingestion, runner heartbeats, and server-sent updates.
- Implemented repository allowlists, runner-label policy reporting, SQLite evidence exports, and a backup/restore drill. The portfolio edition uses sanitized demonstration organizations and runner data.

[Project and implementation](#) | [GitHub source](#)

JARVIS Personal AI Assistant

- Built a Python and FastAPI execution layer with streamed WebSockets connecting web, browser-extension, and native macOS interfaces.
- Implemented agent and tool routing with cloud models and a local Ollama option, browser automation, voice interaction, permission checks, audit records, and SQLite-backed jobs.

[Project and implementation](#) | [GitHub source](#)

Infraguard

- Built a Python infrastructure review tool for Terraform plan risk scoring, AWS resource-tag checks, and IAM least-privilege policy analysis.
- Produced explainable findings in JSON, Markdown, table, and SARIF formats, with CI-friendly exit codes for pipeline integration.

[Project and implementation](#) | [GitHub source](#)

EDUCATION AND CERTIFICATIONS

Bachelor of Science in Computer Science

AWS Certified DevOps Engineer - Professional

Microsoft Certified: Azure Developer Associate

PROFESSIONAL CASE STUDIES

[Production ArgoCD delivery](#) | [Incident response and recovery](#) | [Prisma Cloud upgrade](#)