One-Click Kubernetes Deployment - Quickstart Guide

Generated: 2025-08-29 09:56:09

This Quickstart Guide provides a concise overview of the One-Click Kubernetes Deployment system.
It is designed for managers, executives, or stakeholders who want to understand the system's value and workflow without diving into technical detail.

---

1. Purpose

The repository automates provisioning of Kubernetes infrastructure and application deployment using Terraform and GitHub Actions. It reduces manual errors, speeds up delivery, and improves auditability and security.

2. Key Components

- Terraform: Creates cloud resources such as VPCs, clusters, nodes, and load balancers.
- Kubernetes: Runs containerized workloads (Node.js app, NGINX, k8sGPT diagnostic tool).
- GitHub Actions: Orchestrates workflows with security scans, infra provisioning, and app deployment.

3. Deployment Workflow (High-Level)

- Trigger workflow manually in GitHub Actions with parameters (environment, action, provider).
- Optional Security Scan checks infrastructure and images for vulnerabilities.
- Terraform provisions or destroys cloud infrastructure based on inputs.

- Kubernetes deploys apps with manifests; provider choice configures k8sGPT (Google or OpenAI).

- Workflow completes with apps accessible via external load balancers.

4. Safety Features

- Dry run and confirm flags prevent accidental deletions.

- Environment separation ensures dev, test, and prod do not interfere.

- Secrets stored securely in GitHub Secrets.

- Logs and audit trails provide full visibility.

5. Benefits

- Speed: One-click deployment reduces setup time from hours to minutes.

- Reliability: Declarative infrastructure ensures consistency across environments.

- Security: Integrated scans, RBAC, and secret management reduce risks.

- Flexibility: Parameters allow partial or full deployment, destruction, or scanning.

- Cost Savings: Temporary environments can be created and destroyed on demand.

6. Example Use Cases

- Developer spins up a dev cluster with apps in minutes for testing.

- Security team runs scan-only workflow for compliance checks.

- Ops team destroys unused test environments to save costs.

- Manager views audit logs in GitHub for visibility.

Conclusion

This system is a blueprint for modern DevOps: automated, auditable, and secure.

It empowers teams to innovate faster while maintaining compliance and reducing risk.

For technical details, refer to the full HANDBOOK.md or HANDBOOK.html documents.