GUIA DE BOAS PRÁTICAS PARA API DO KUBERNETES

1 INTRODUÇÃO

Apresenta a motivação e o contexto do guia, com foco na proteção da API do Kubernetes em ambientes críticos, como cidades inteligentes. Testado e validado com Minikube.

2 AUTENTICAÇÃO E AUTORIZAÇÃO

Implemente autenticação forte com ServiceAccounts e TLS 1.3. Use RBAC baseado no princípio do menor privilégio para restringir o que cada identidade pode acessar.

3 PROTEÇÃO DO SECRETS

Armazene dados sensíveis com cuidado. Use criptografia no etcd, monte secrets como volumes, restrinja leitura com RBAC e evite exposição em logs ou imagens.

4 PROTEÇÃO DO TLS E HTTPS

Exija TLS 1.3 para todas as conexões com a API. Use certificados válidos (Let's Encrypt ou autoassinados) e monitore sua validade com cert-manager.

5 CONTROLE DE ACESSO DA API

Nunca exponha diretamente o kube-apiserver. Utilize firewalls, VPNs, bastion hosts e Ingress com TLS para controlar e proteger o acesso.

6 FERRAMENTAS E AUDITORIA

Use Falco para detectar comportamentos anômalos, Kubeaudit para revisar configurações inseguras, cert-manager para gerenciar TLS, e Postman para testes com token.

7 PONTOS DE ATENÇÃO

Não negligencie MFA, controle de IP e rate limiting. Esses fatores são cruciais para proteger contra ataques de força bruta e acessos indevidos.

8 CONCLUSÃO

Segurança é um processo contínuo. Revise configurações regularmente, atualize práticas com base em novas ameaças e mantenha o cluster resiliente.

2025