Building Resilient Multi-Region Service Mesh with Istio and Vault

Whoami

Vishnu Nair
Director, Codewise Analytics
DevSecOps Consultant - TopTal / Braintrust

Agenda

1. Introduction to Zero Trust
2. Challenges in Multi-Cluster Kubernetes
3. Istio Multi-Primary
4. Integrating HashiCorp Vault as a Central CA
5. Demo
6. Q&A

Introduction to Zero Trust in Kubernetes

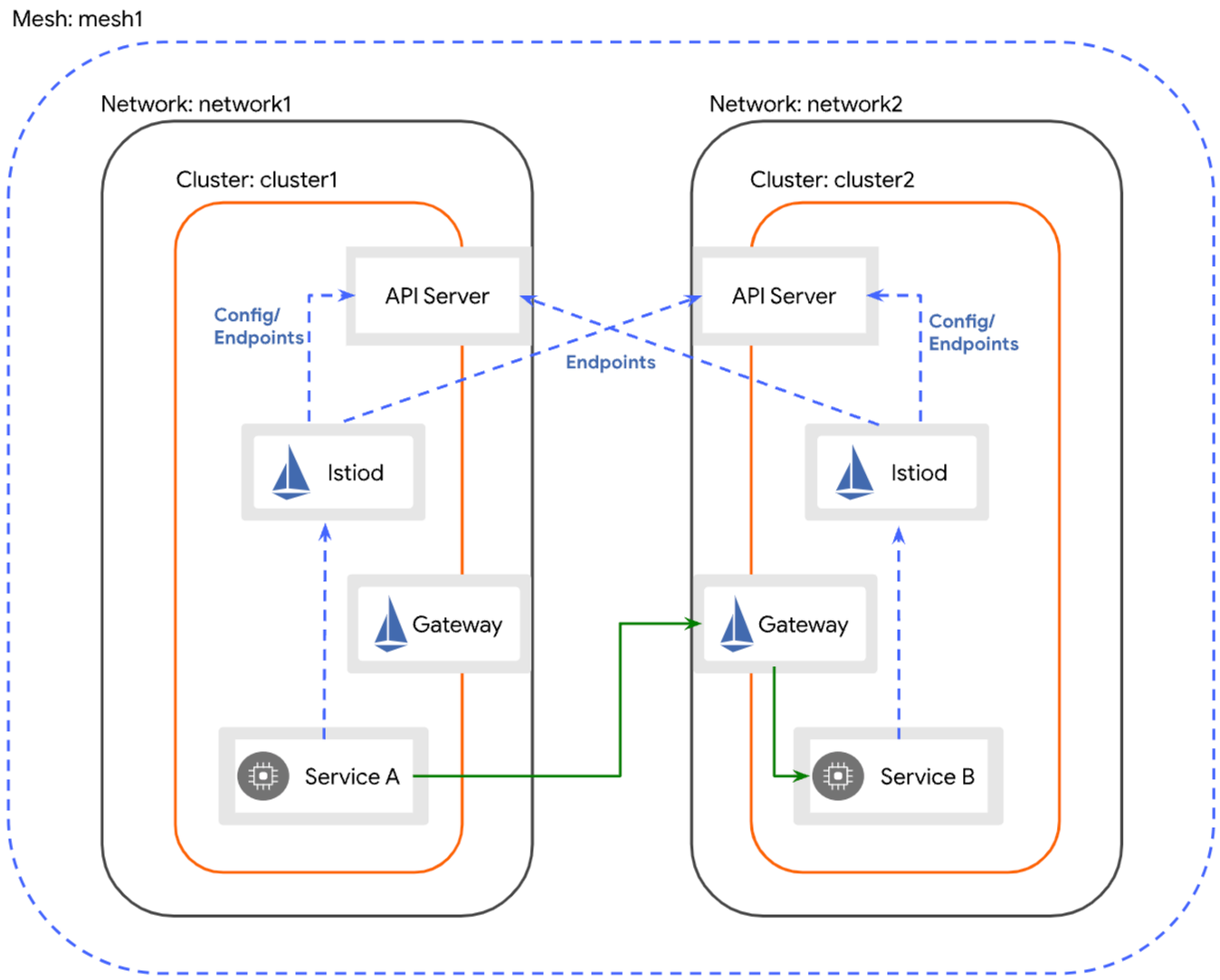
- Traditional perimeter-based security fails in dynamic cloud environments.
- Zero Trust ensures:
  1. Identity verification for every request.
  2. Secure inter-service communication.
  3. Continuous policy enforcement.

Challenges in Multi-Cluster Kubernetes

- Service discovery across clusters.
- Securing communication without manual configurations.
- Enforcing consistent policies across clusters.
- Managing sensitive data and secrets securely.

Istio Multi-Primary

1) Use Case: Geographical Distribution
2) Independent Control Planes
3) Scalability Across Multi-Cloud and Hybrid Cloud
4) Fault Isolation
5) Simplified Multi-Network Communication
6) Secure Inter-Cluster Communication with mTLS
7) Autonomy in Disaster Recovery

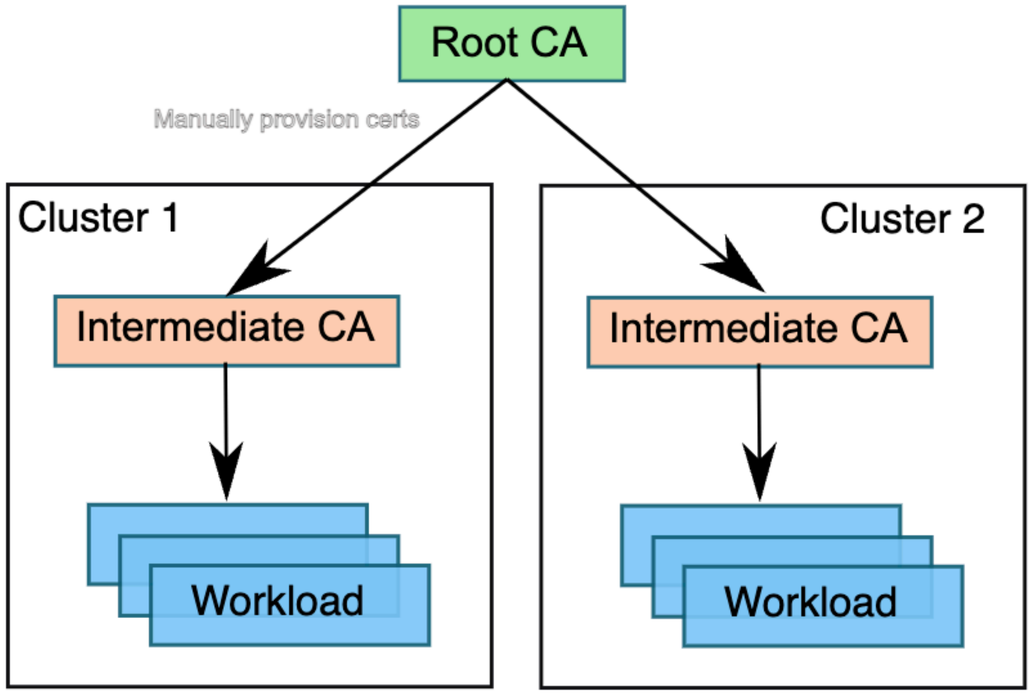


Multiple primary clusters on separate networks

https://istio.io/latest/docs/setup/install/multicluster/multi-primary_multi-network/

Integrating HashiCorp Vault as a Central CA

- Deploy Vault in the Kubernetes cluster.
- Use Vault to create and manage the Root CA.
- Generate Intermediate CAs for each cluster.
- Integrate Istio with Vault-managed certificates.



CA Hierarchy

https://istio.io/latest/docs/tasks/security/cert-management/

Demo

Q&A