🗄️ Self-Managed High-Availability PostgreSQL with Patroni

To meet the requirement for a resilient, self-managed database, this project proposes a Patroni-managed PostgreSQL cluster.

Architecture Overview

The cluster consists of three nodes spread across different Availability Zones (AZs) within the private subnets.

- **Patroni:** Acts as a cluster manager, handling automatic failover and leader election.
- **etcd/Consul:** Used as the Distributed Configuration Store (DCS) for consensus.
- **HAProxy/Keepalived:** Provides a single virtual IP or endpoint to the application, routing traffic to the current Primary node.

Security Constraints

- **Network Isolation:** Database nodes are located in the `isolated` subnets with no NAT or IGW access.
- **Encryption:** Data at rest is encrypted using **AWS KMS**, and all transit traffic is forced over **TLS/SSL**.
- **Principle of Least Privilege:** The application connects via a restricted IAM-mapped user role rather than a superuser account.