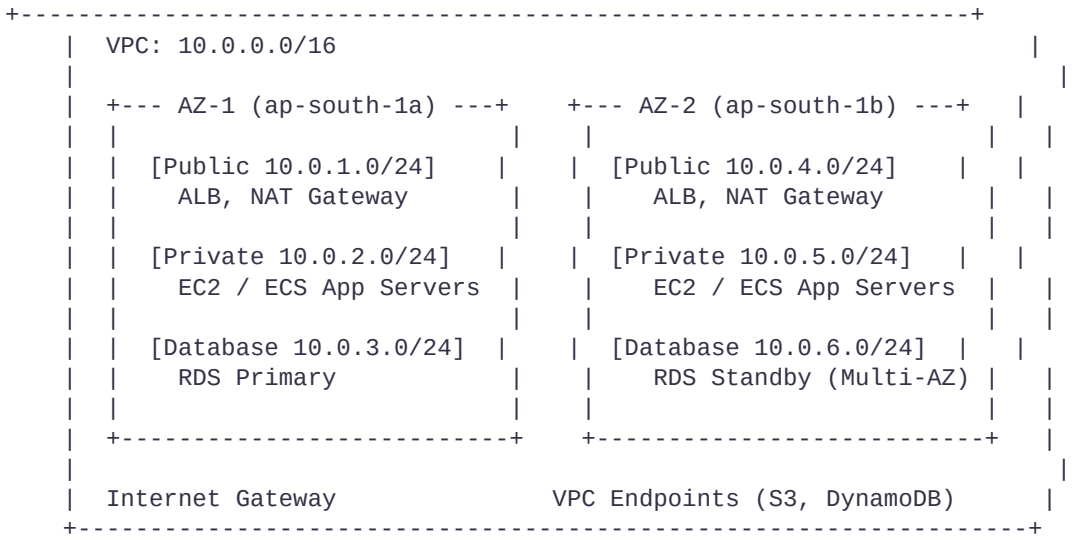
Production VPC Architecture

Multi-AZ design for AWS production workloads

Architecture Overview

Three-tier VPC across 2 Availability Zones: public subnets (ALB, NAT), private subnets (app servers), database subnets (RDS). This is the architecture I use for multi-tenant SaaS serving 1000+ customers.



Security Group Rules

- ALB SG: Inbound 80/443 from 0.0.0.0/0. Outbound to App SG.

- App SG: Inbound from ALB SG only. Outbound to DB SG + NAT.
- DB SG: Inbound 3306/5432 from App SG only. No internet access.
- Bastion SG (optional): Inbound 22 from your IP only.

Route Tables

- Public RT: 0.0.0.0/0 -> Internet Gateway (direct internet access)
- Private RT: 0.0.0.0/0 -> NAT Gateway (outbound only)
- Database RT: No internet route (completely isolated)
- S3 endpoint route added to Private + Database RTs (free, avoids NAT)