

Integrated Management Information System (MIS)

Technical Design Document: Hybrid
Architecture & Disaster Recovery

Version: 1.0

Prepared for: Government Enterprise Client

Role: DevOps / Infrastructure Architect

Status: Draft for Review

Table of Contents

1. Executive Summary & Requirements
2. Infrastructure Design
 - 2.3 Architecture Diagram
3. High Availability & Disaster Recovery
4. Security Architecture
5. CI/CD & Observability
6. Capacity Planning & Cost estimation

1. Executive Summary & Requirements

This Technical Design Document (TDD) outlines the architectural blueprint for a mission-critical Integrated Management Information System (MIS) designed for a government-scale organization. The solution leverages a Hybrid Cloud model, combining On-Premise infrastructure with Amazon Web Services (AWS) to ensure high availability, data sovereignty, and robust disaster recovery.

1.1 Project Objectives

- Serve 1,000+ concurrent users across multiple departments.
- Ensure 99.9% uptime (SLA) through enterprise-grade high availability.
- Maintain strict data protection compliance for citizen data.
- Implement a robust Disaster Recovery (DR) strategy with defined RTO/RPO.
- Enable seamless CI/CD and automated infrastructure management (IaC).

1.2 System Assumptions

Component	Technology Stack
Backend	Containerized Python (FastAPI/Django)
Frontend	React SPA
Database	PostgreSQL (RDS / Self-hosted)
Caching	Redis (ElastiCache / Self-hosted)
Job Engine	Celery with Redis Broker
Cloud Provider	Amazon Web Services (AWS)

Component	Technology Stack
Orchestration	Kubernetes (EKS / On-Prem K8s)

2. Infrastructure Design

2.1 Hybrid Architecture (Overview)

The architecture utilizes a dual-site strategy: an On-Premise Private Cloud and an AWS Public Cloud environment connected via AWS Direct Connect. Primary traffic is balanced via Route 53, enabling global traffic management and failover capabilities.

2.1.1 On-Premise Architecture

- **Network Segmentation**: Three-tier VLAN structure (DMZ, App, Data).
- **DMZ**: Houses hardware WAF and F5/Citrix Load Balancers.
- **Orchestration**: Self-managed Kubernetes (K8s) cluster using high-performance bare-metal or VMware hosts.
- **Data Tier**: High-availability PostgreSQL cluster with synchronous replication.

2.1.2 AWS Cloud Architecture

- **VPC Design**: Multi-AZ VPC spanning at least 3 Availability Zones.
- **Compute**: Amazon EKS (Elastic Kubernetes Service) with managed node groups and Fargate for sensitive workloads.
- **Load Balancing**: Application Load Balancer (ALB) integrated with AWS WAF and Shield for DDoS protection.
- **Storage**: Amazon S3 for document storage with Cross-Region Replication (CRR) enabled.

2.2 Network & Connectivity

A 10Gbps AWS Direct Connect link provides dedicated connectivity between On-Premise and AWS. A redundant Site-to-Site VPN serves as the immediate failover for the Direct Connect link.

2.3 Global Hybrid Architecture Diagram

The following diagram illustrates the integrated flow between On-Premise, AWS Primary, and AWS DR regions.

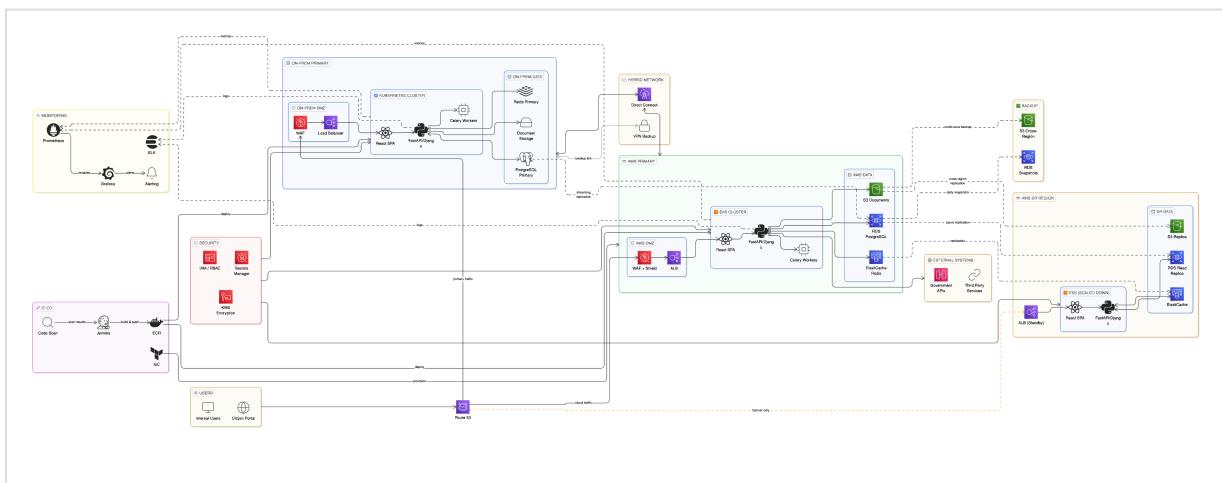


Figure 1: Enterprise Hybrid Architecture Workflow

3. High Availability (HA) & Disaster Recovery (DR)

3.1 Achieving 99.9% Uptime

- **Stateless Application**: FastAPI/Django pods are stateless, managed by ReplicaSets to ensure horizontal scaling.
- **Multi-AZ Strategy**: Workloads are distributed across 3 AZs; loss of an entire AZ does not impact service.
- **Database HA**: AWS RDS Multi-AZ for automatic failover. On-premise uses Patroni/Repmgr for automated PostgreSQL failover.
- **Redis HA**: Redis Sentinel (On-Prem) and Amazon ElastiCache (Cloud) with cluster mode enabled.

3.2 Disaster Recovery Design (Pilot Light/Warm Standby)

Metric	Target Value	Notes
RTO (Recovery Time Objective)	< 2 Hours	Targeting cold/warm start of standby EKS pods.
RPO (Recovery Point Objective)	< 15 Minutes	Based on async DB replication lag.
Strategy	Active-Passive / Warm Standby	AWS Region B acts as the DR site for Region A.
Backup Frequency	Daily + Continuous	Transaction logs (WAL) streamed continuously.

3.3 DR Failover Process

- 1. Trigger Route 53 Health Check failover.
- 2. Promote RDS Read Replica in DR region to Primary.
- 3. Scale EKS standby node groups from minimal to full capacity.
- 4. Update Application configurations to point to local DR resources.

4. Security Architecture

4.1 Zero-Trust Principles

- **Identity & Access**: IAM Roles for Service Accounts (IRSA) in EKS; LDAP/Active Directory integration for internal RBAC.
- **Network Security**: Security Groups (Stateful) and Network ACLs (Stateless) ensure principle of least privilege.
- **Encryption at Rest**: AWS KMS managing keys for RDS, S3, and EBS. AES-256 for On-Prem storage.
- **Encryption in Transit**: Mandatory TLS 1.3 for all internal and external communication.

4.2 Secrets & Compliance

AWS Secrets Manager handles database credentials and API keys with automatic rotation. HashiCorp Vault is utilized for On-Premise secret management. Audit logging is centralized via AWS CloudTrail and ELK Stack for compliance monitoring.

5. CI/CD & Observability

5.1 CI/CD Pipeline

- **Source Control**: GitHub Enterprise (Branching: Gitflow).
- **CI/CD Tool**: Jenkins (as per diagram) or GitHub Actions.
- **Infrastructure as Code**: Terraform for AWS provisioning; Ansible for On-Prem configuration.
- **Deployment**: Rolling updates for standard releases; Blue-Green deployments for major version upgrades.

5.2 Monitoring Stack

Layer	Tooling
Metrics	Prometheus + Grafana
Log Aggregation	ELK Stack (Elasticsearch, Logstash, Kibana)
Tracing	Jaeger / AWS X-Ray
Alerting	Alertmanager (Slack/Email/PagerDuty)

5.3 Capacity Planning (1,000 Concurrent Users)

- **Web Servers**: ~12 pods (2 vCPU, 4GB RAM each) scaled horizontally based on CPU usage.
- **Database**: AWS r6g.2xlarge (8 vCPU, 64GB RAM) to handle concurrent transactional load.
- **Storage**: Start with 5TB S3 / 2TB EBS; projected 20% annual growth.

- **Auto-scaling**: HPA (Horizontal Pod Autoscaler) triggered at 70% CPU threshold.

5.4 Cost Estimation (Cloud Monthly)

Service	Estimated Cost (USD)
Compute (EKS + EC2)	\$2,500
Database (RDS Multi-AZ)	\$1,800
Storage (S3 + Backup)	\$600
Networking (Direct Connect + Bandwidth)	\$1,200
Security (WAF + Shield)	\$3,200
Total Estimated Monthly	**~\$9,300**