MUSTERMANN
IT-SERVICES

AWS Architektur-Dokumentation

ARCHITECTURE DOCUMENTATION · DOC-2025-003

Projekt:	AWS Cloud Migration
Kunde:	MedTech Solutions AG
Version:	1.0
Status:	FINAL
Erstellt:	2025-01-22
Autoren:	Dr. Michael Hoffmann, TechVision Consulting

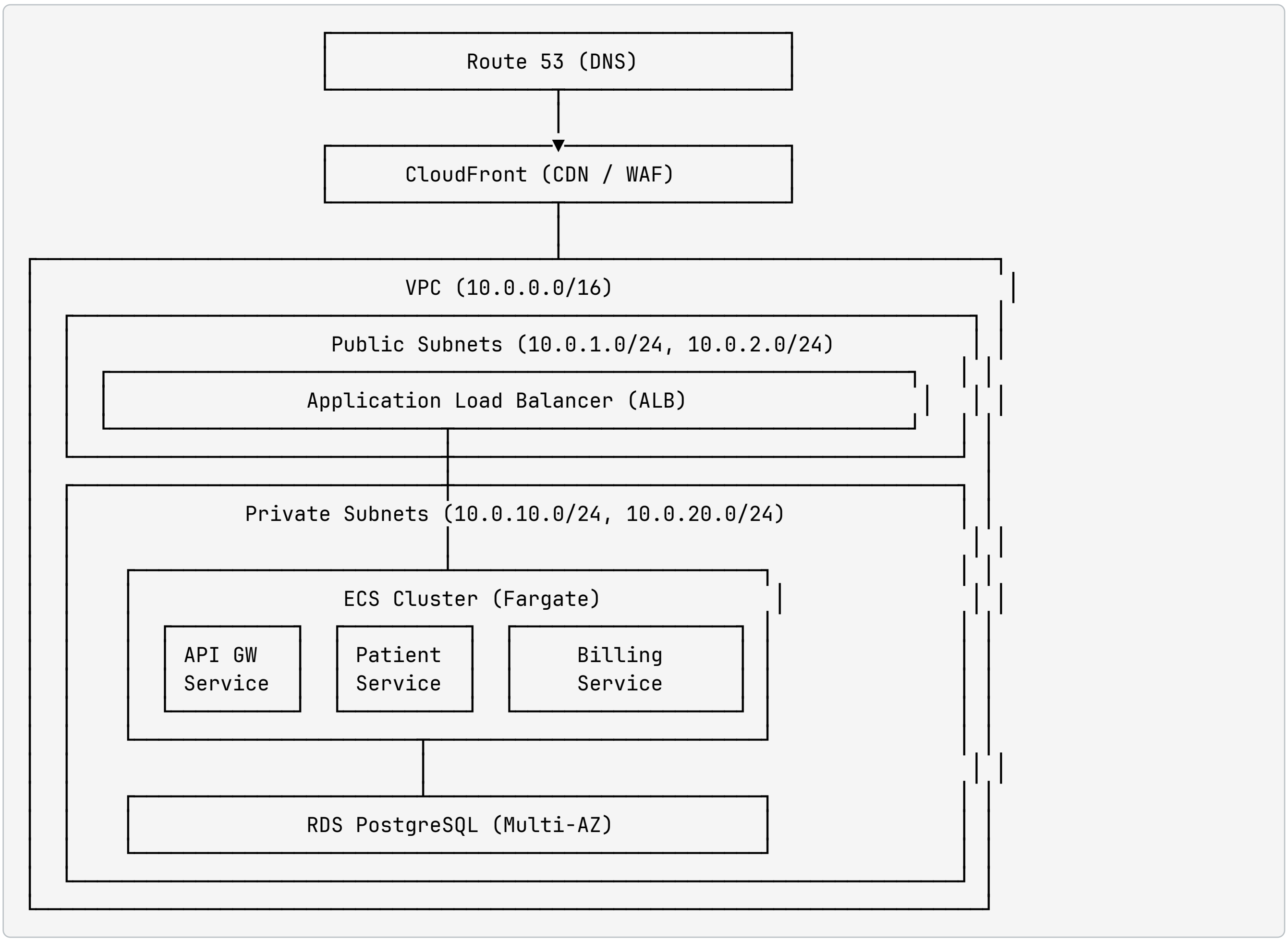
AWS Architecture Cloud Infrastructure

Inhaltsverzeichnis

1 Überblick

Diese Dokumentation beschreibt die AWS-Cloud-Architektur der MedTech Solutions AG nach Abschluss der Migration. Sie dient als Referenz für das DevOps-Team und externe Auditoren.

1.1 Architektur-Diagramm


Route 53 (DNS)
CloudFront (CDN / WAF)
VPC (10.0.0.0/16)
Public Subnets (10.0.1.0/24, 10.0.2.0/24)
Application Load Balancer (ALB)
Private Subnets (10.0.10.0/24, 10.0.20.0/24)
ECS Cluster (Fargate)
API GW Service
Patient Service
Billing Service
RDS PostgreSQL (Multi-AZ)

2 Netzwerk

2.1 VPC Konfiguration

Parameter	Wert
VPC CIDR	10.0.0.0/16
Region	eu-central-1 (Frankfurt)

Availability Zones	eu-central-1a, eu-central-1b
DNS Hostnames	Aktiviert
DNS Resolution	Aktiviert

2.2 Subnets

Name	CIDR	AZ	Typ
public-1a	10.0.1.0/24	eu-central-1a	Public
public-1b	10.0.2.0/24	eu-central-1b	Public
private-1a	10.0.10.0/24	eu-central-1a	Private
private-1b	10.0.20.0/24	eu-central-1b	Private
db-1a	10.0.100.0/24	eu-central-1a	Isolated
db-1b	10.0.200.0/24	eu-central-1b	Isolated

2.3 Security Groups

2.3.1 ALB Security Group

Typ	Port	Quelle	Beschreibung
Inbound	443	0.0.0.0/0	HTTPS von Internet
Inbound	80	0.0.0.0/0	HTTP Redirect
Outbound	8080	ECS SG	Zu ECS Services

2.3.2 ECS Security Group

Typ	Port	Quelle	Beschreibung
Inbound	8080	ALB SG	Von Load Balancer
Outbound	5432	RDS SG	Zu Datenbank
Outbound	443	0.0.0.0/0	AWS APIs, ECR

3 Compute (ECS)

3.1 Cluster Konfiguration

- **Cluster Name:** medtech-prod-cluster
- **Capacity Provider:** FARGATE, FARGATE_SPOT
- **Container Insights:** Aktiviert

3.2 Services

Service	CPU	Memory	Replicas
api-gateway	512	1024 MB	2
patient-service	1024	2048 MB	3
billing-service	512	1024 MB	2

3.3 Auto Scaling

- **Metrik:** CPU Utilization
- **Target:** 70%
- **Min Capacity:** 2
- **Max Capacity:** 10
- **Scale-out Cooldown:** 60s
- **Scale-in Cooldown:** 300s

4 Datenbank (RDS)

4.1 Konfiguration

Parameter	Wert
Engine	PostgreSQL 15.4
Instance Class	db.r6g.large
Multi-AZ	Ja
Storage	500 GB gp3
IOPS	3000
Encryption	AES-256 (AWS KMS)
Backup Retention	35 Tage
Maintenance Window	Sun 03:00-04:00 UTC

4.2 Connection Pooling

PgBouncer läuft als Sidecar in jedem ECS Task:

- **Pool Mode:** Transaction
- **Max Connections:** 100
- **Default Pool Size:** 20

5 Secrets Management

Alle sensiblen Daten werden in AWS Secrets Manager gespeichert:

Secret Name	Inhalt
prod/rds/admin	Datenbank Admin Credentials
prod/rds/app	Application User Credentials
prod/api/jwt-secret	JWT Signing Key
prod/external/stripe	Stripe API Keys

Rotation: Automatische Rotation alle 30 Tage für DB-Credentials.

6 CI/CD Pipeline

6.1 Übersicht

```
GitHub Push → GitHub Actions → Build & Test → ECR Push → CodePipeline → ECS Deploy
```

6.2 Stages

1. **Source:** GitHub Repository (main branch)
2. **Build:** Docker Image bauen, Unit Tests
3. **Push:** Image zu ECR pushen
4. **Deploy Staging:** Automatisches Deployment
5. **Integration Tests:** Automatisierte API Tests
6. **Approve:** Manuelle Freigabe
7. **Deploy Production:** Blue/Green Deployment

6.3 Blue/Green Deployment

- **Deployment Controller:** CodeDeploy
- **Traffic Shift:** Linear10PercentEvery1Minute
- **Rollback:** Automatisch bei CloudWatch Alarms

7 Monitoring & Alerting

7.1 CloudWatch Dashboards

- **Production Overview:** CPU, Memory, Request Count

- **API Metrics:** Latency, Error Rate, 4xx/5xx
- **RDS Health:** Connections, CPU, Storage

7.2 Alarms

Alarm	Threshold	Action
API Error Rate > 1%	5 min	PagerDuty P2
API Latency p99 > 500ms	5 min	PagerDuty P3
RDS CPU > 80%	15 min	PagerDuty P3
RDS Connections > 80%	5 min	PagerDuty P2
ECS Task Failed	1 min	PagerDuty P1

8 Disaster Recovery

8.1 RPO / RTO

- **RPO (Recovery Point Objective):** 1 Stunde
- **RTO (Recovery Time Objective):** 4 Stunden

8.2 Backup-Strategie

- **RDS:** Automatische Snapshots (täglich), Transaction Logs (5 min)
- **S3:** Cross-Region Replication nach eu-west-1
- **Secrets:** Replikation nach eu-west-1

8.3 Failover-Prozedur

1. Route 53 Health Check schlägt fehl
2. Automatischer Failover zu Standby (Multi-AZ)
3. PagerDuty Alarm an On-Call Engineer
4. Manuelle Prüfung und Bestätigung

9 Kosten

9.1 Monatliche Kosten (geschätzt)

Service	Kosten/Monat

ECS Fargate	850 EUR
RDS PostgreSQL (Multi-AZ)	650 EUR
Application Load Balancer	50 EUR
CloudFront	100 EUR
S3 + Backups	80 EUR
Secrets Manager	15 EUR
CloudWatch	120 EUR
Data Transfer	200 EUR
Gesamt	**2.065 EUR**

10 Kontakt

TechVision Consulting
Dr. Michael Hoffmann
info@techvision-consulting.de
+49 30 12345678