Gold Solar S.r.l.
Via Purgatorio 40, 80147,Napoli, Italia
Tel: 081 016 9472 – Email: info@goldsolarweb.com
Sito: ww.goldenbitweb.com – www.goldsolarweb.com
Partita IVA: 10355251215

Offerta tecnica

Cliente: Piattaforma gestionale multi-tenant per studi dentistici
Proponente: Gold Solar s.r.l
Data: 6 novembre 2025

---

1) Premessa

Approccio **server-like** senza Kubernetes, con riavvio **automatico** di tutti i servizi in caso di reboot. In questa revisione integriamo l'**Identity Provider (IdP)** a scelta tra **Keycloak (self-hosted)** o **Amazon Cognito (cloud)** e l'engine di **autorizzazione fine-grained OpenFGA** per ruoli/permessi/gerarchie. I database applicativi restano su **Amazon RDS for PostgreSQL** (centrale + uno per ciascuno studio su stessa istanza/cluster). Backend e frontend sono container Docker.

Mostriamo due **scenari architetturali compute** (A: doppia istanza; B: istanza unica), entrambe con le varianti **IdP** (Keycloak vs Cognito) e con **OpenFGA**. Analizziamo sicurezza, costi, operatività e scalabilità; includiamo i reverse proxy (**Nginx** e **Traefik**), interfacce web di gestione e raccomandazioni.

---

2) Requisiti chiave (riepilogo)

- Multi-tenant: **DB centrale** + **DB separati per studio** su **RDS PostgreSQL** (isolamento logico).
- **Autenticazione (AuthN)**: **Keycloak** *oppure* **Cognito**.

- **Autorizzazione (AuthZ)**: **OpenFGA** (Zanzibar-style) con schema relazionale dei permessi, ruoli e risorse.

- Container Docker per app (backend/API e frontend), deploy automatizzati **CI/CD**.
- Provisioning nuovo studio ≤ **10 minuti**; **RTO ≤ 40 minuti**.
- Scalabilità **verticale** dell'istanza e **per-tenant** (limiti dei container).
- Backup giornalieri, snapshot periodici, **IaC Terraform**, sicurezza by-design, nessun Kubernetes.

- **Auto-recovery**: a seguito di riavvio server, **tutti i servizi e l'infrastruttura ripartono automaticamente** senza intervento umano.

---

3) Architetture proposte su AWS

3.1 Componenti comuni

- **VPC dedicata**, subnet private, **Security Groups** *deny-by-default*; **Route53** + **ACM** per DNS/TLS.
- **EC2 AppHost** (server-like) con Docker/Compose, **CloudWatch** (log/metriche), **SSM** (bastion-less).
- **Amazon RDS for PostgreSQL**:
  - **DB Centrale** (metadati, licensing, routing) su RDS dedicato.
  - **DB Tenants** su RDS separato con **un database per studio**.
  - **RDS Proxy** per pooling; **Multi-AZ** raccomandato; **PITR** e snapshot automatici.
- **OpenFGA**: container su EC2 con **RDS PostgreSQL dedicato** (database separato dallo schema applicativo).
- **IdP** a scelta:
  - **Keycloak (self-hosted)**: container su EC2 **Admin/Ops** o sull'host unico; DB Keycloak su **RDS PostgreSQL** dedicato.
  - **Amazon Cognito (cloud)**: User Pool + federation SAML/OIDC, nessun server da mantenere.
- **ECR** (immagini), **S3** (backup/logs/assets; lifecycle→Glacier), **IAM**, **Parameter Store/Secrets Manager** (KMS).
- **CI/CD** (GitHub Actions/GitLab CI) con OIDC→IAM per deploy *develop*→preprod e *main*→prod (approvazione manuale).
- **IaC Terraform** per VPC, EC2, SG, RDS/RDS Proxy, ECR, S3, CloudFront opz., Route53, CloudWatch, SSM, IAM, OpenFGA, Keycloak (se scelto).
- **Auto-restart/auto-recovery**: Docker `restart: always`, unit `systemd` per Compose, **ASG size=1** con **Instance Recovery** e **Instance Refresh**, **cloud-init/user-data** idempotenti. In caso di reboot del server, **tutti i container e i servizi ripartono automaticamente**; con Cognito/RDS i piani di HA sono gestiti dal cloud.

Gold Solar S.r.l.
Via Purgatorio 40, 80147,Napoli, Italia
Tel: 081 016 9472 – Email: info@goldsolarweb.com
Sito: ww.goldenbitweb.com – www.goldsolarweb.com
Partita IVA: 10355251215

3.2 Scenario A – Doppia istanza (separazione ruoli)

```
Utenti → (CloudFront opz.) → ALB/Nginx/Traefik → EC2-App/Studios (Docker)
                                                  ├─ Backend/Frontend per-studio
                                                  ├─ Client FGA (SDK) → OpenFGA (EC2) →
RDS Postgres (Permessi)
                                                  └─ RDS Proxy → RDS Postgres TENANTS (
DB per studio)

EC2-Admin/Ops
  ├─ IdP (Keycloak) *oppure* integrazione Cognito (nessun server)
  ├─ Tooling admin (migrazioni, console, batch)
  └─ RDS Postgres CENTRALE (metadati)

S3 (backup/snapshot) — CloudWatch (log/metriche) — IAM/SSM — ECR — Route53/AC
M
```

Note: separazione host tra traffico pubblico applicativo e processi admin/IdP. OpenFGA può stare sull'host App o Admin in base al carico (consigliato App per latenza).

3.3 Scenario B – Istanza unica (all-in-one)

```
Utenti → (CloudFront opz.) → ALB/Nginx/Traefik → EC2-All-in-one (Docker)
  ├─ Backend/Frontend per-studio
  ├─ OpenFGA (EC2) → RDS Postgres (Permessi)
  ├─ IdP Keycloak (opz.) *oppure* Cognito (cloud, senza host)
  └─ RDS Proxy → RDS Postgres (CENTRALE + TENANTS)
S3 — CloudWatch — IAM/SSM — ECR — Route53/ACM
```

Note: costi/gestione minimi; **blast radius** applicativo maggiore. I database restano su **RDS** (gestito).

---

4) Identity & Authorization (dettaglio)

4.1 IdP — due opzioni equivalenti

A) Keycloak (self-hosted) - **AuthN**: OIDC/SAML, social login, MFA. - **Multi-tenant**: un **realm unico** con **gruppi** per studio e **client-roles** (consigliato per limitare sprawl), oppure un realm per studio (solo se richiesto). - **User admin**: console Keycloak; integrazione SSO (OIDC) per le UI interne. - **DB Keycloak**: **RDS PostgreSQL** dedicato (separato da app e da OpenFGA).

B) Amazon Cognito (cloud) - **AuthN**: User Pool (passwordless/MFA/policy), federation SAML/OIDC per B2B, triggers Lambda (post-confirm, pre-token). - **Multi-tenant**: singolo User Pool con attributo `tenant_id` e **Gruppi/Ruoli** mappati nei **claim** JWT; oppure Organizations (pattern logico) lato app. - **Zero-ops**: nessun server; pay-per-MAU.

4.2 OpenFGA — autorizzazione fine-grained

- **Schema** (Zanzibar-style) per **ruoli, gerarchie e risorse** (es. `organization`, `studio`, `patient_record`, `invoice`).
- **Relazioni**: es. `member`, `admin`, `owner`, `can_view`, `can_edit` con **derive** (admin ⇒ edit ⇒ view).
- **Query di decisione**: il backend interroga **OpenFGA** (HTTP/gRPC) per *who can what*; i token JWT del IdP forniscono identità e `tenant_id`.
- **Storage**: **RDS PostgreSQL** dedicato (DB separato).
- **Migrazioni & seed**: pipeline CI per schema OpenFGA e **tuples** iniziali (ruoli base: *Admin Studio*, *Dottore*, *Assistente*, *Front-desk*).
- **UI**: Playground per dev; **UI custom** (nostra) per gestione permessi in produzione.

4.3 Enforcement nel backend/API

- I reverse proxy (Nginx/Traefik) gestiscono TLS/rate-limit/routing.
- L'**enforcement** dei permessi avviene **nell'API**:
    1) valida JWT (IdP), 2) risolve `tenant_id`/attributi, 3) chiama **OpenFGA** per la risorsa/azione, 4) filtra query DB (row-level tenant filter), 5) risponde.

Esempio (pseudocodice)

```
// check permesso: utente può leggere la cartella clinica X?
const sub = jwt.sub; const tenant = jwt.tenant_id;
const decision = fga.check({
  user: `user:${tenant}:${sub}`,
  relation: "can_view",
  object: `patient_record:${tenant}:${recordId}`
});
if (!decision.allowed) throw new Forbidden();
```

Gold Solar S.r.l.
Via Purgatorio 40, 80147,Napoli, Italia
Tel: 081 016 9472 – Email: info@goldsolarweb.com
Sito: ww.goldenbitweb.com – www.goldsolarweb.com
Partita IVA: 10355251215

5) Reverse proxy: Nginx **e** Traefik (entrambi)

Variante Nginx (estratto)

```
upstream api_studio_roma { server 127.0.0.1:18081; }
upstream web_studio_roma { server 127.0.0.1:18082; }
server {
  listen 443 ssl http2;
  server_name studio-roma.example.tld;
  location /api/ { proxy_pass http://api_studio_roma; }
  location / { proxy_pass http://web_studio_roma; }
  proxy_set_header X-Forwarded-Proto https;
}
```

Variante Traefik (labels, estratto)

```
services:
  reverse-proxy:
    image: traefik:v3
    ports: ["80:80", "443:443"]
    command: ["--providers.docker=true", "--entrypoints.websecure.address=:44
3"]
  api-studio-roma:
    image: <account>.dkr.ecr.<region>.amazonaws.com/api:main
    labels:
      - "traefik.http.routers.api-roma.rule=Host(`studio-roma.example.tld`) &
& PathPrefix(`/api`)"
      - "traefik.http.services.api-roma.loadbalancer.server.port=8081"
  web-studio-roma:
    image: <account>.dkr.ecr.<region>.amazonaws.com/web:main
    labels:
      - "traefik.http.routers.web-roma.rule=Host(`studio-roma.example.tld`)"
      - "traefik.http.services.web-roma.loadbalancer.server.port=8082"
```

---

6) Automazione & CI/CD

Pipeline 1. Build/test su `develop` → push immagini su **ECR** `:develop` → **pre-produzione** (EC2 preprod). 2. Promozione `main` → `:main` → **approvazione manuale** → deploy *blue/green* su produzione. 3. **Nuovo studio (≤10 min)**: crea `db_studio_<slug>` su **RDS Tenants** (migrazioni), inserisce segreti su **SSM**, registra **tuples OpenFGA** (ruoli base), genera servizi `api`/`web` con limiti CPU/RAM, emette DNS + certificato ACM, health-check e (opz.) warmup

CloudFront. 4. **Resize per-tenant**: aggiorna `cpus/mem_limit` per lo studio → *rolling restart* dei soli container dello studio. 5. **Resize host**: cambio *instance type* via **Instance Refresh** (ASG) con drain del proxy, downtime minimo. 6. **Policy as Code**: repo dedicato per **schema/tuples OpenFGA** e (se Keycloak) per **realm config**; test autorizzativi in CI.

---

7) Sicurezza

- **IAM** least-privilege; ruoli separati per CI, runtime, backup.
- **Accesso** solo via **SSM Session Manager**; UI admin dietro **SSO OIDC** (IdP scelto) e **IP allowlist**; opzionale tunnel SSM/VPN.
- **Crittografia**: EBS (KMS), S3 (SSE-S3/KMS), **RDS encryption** + **in-transit TLS**; segreti con **Parameter Store/Secrets Manager**.
- **RDS**: **Multi-AZ**, **RDS Proxy**, **PITR**; opzionale **IAM auth**.
- **Supply-chain**: immagini *distroless/alpine*, scansioni (Trivy/Grype), **SBOM** in CI.
- **Auditing**: audit accessi IdP (Keycloak audit log / Cognito CloudTrail), audit decisioni AuthZ (log OpenFGA), CloudWatch centralizzato.

---

8) Backup & Disaster Recovery

- **RDS**: snapshot automatici + **Point-in-Time Recovery**; read-replica opzionale.
- **EC2**: AMI settimanali + snapshot EBS giornalieri.
- **OpenFGA/Keycloak**: backup dello schema/tuples/realm config (repo + esportazioni periodiche); DB su RDS coperto da snapshot/PITR.
- **Runbook RTO ≤ 40 min**:
  - Scenario A: sostituzione host (ASG) 10–20 min + ri-deploy; RDS Multi-AZ auto-failover 2–5 min; verifica/warmup 5–10 min.
  - Scenario B: come sopra su unico host.
- **Test DR** semestrali con report.

---

9) Monitoraggio & allarmi

- **Metriche**: CPU/RAM/disk (CloudWatch Agent), IOPS/latency EBS, connessioni/lag RDS, latenze AuthZ (OpenFGA), code 5xx API.
- **Allarmi**: CPU>75%, mem>80%, spazio EBS, lag replica RDS, error rate, violazioni health, tempi di risposta FGA.
- **Synthetic**: heartbeat `/health` e journey critici (login, apertura cartella, fattura).

Gold Solar S.r.l.
Via Purgatorio 40, 80147,Napoli, Italia
Tel: 081 016 9472 – Email: info@goldsolarweb.com
Sito: ww.goldenbitweb.com – www.goldsolarweb.com
Partita IVA: 10355251215

---

10) Interfacce web (open-source) e **UI personalizzata**

- **Gestione Docker**: **Portainer CE** (solo rete interna/SSM + SSO).
- **IdP**:
  - **Keycloak Admin Console** (se Keycloak) per utenti/gruppi/ruoli;
  - **Cognito Console** (se Cognito) per User Pool/groups/attr.
- **OpenFGA**: Playground per dev; **UI custom** in produzione (nostra) per ruoli/permessi/assign; audit.
- **Database**: **pgAdmin**/**Adminer** (read-only su prod) con **RDS IAM auth** opz.
- **Monitoraggio**: **Netdata** o **Prometheus + Grafana**.
- **Gestione host**: **Cockpit** (facolt.) dietro SSO/IP allowlist.
- **UI personalizzata (nostra)**:
  - **Nuovo studio** (wizard): crea DB RDS, segreti SSM, tuples OpenFGA, servizi `api`/`web`, DNS/ACM, health-check ⇒ **tutto automatico**.
  - **Resize per-studio** (slider CPU/RAM) + *rolling restart*.
  - **Gestione utenti/ruoli** (tenant), feature flags, batch; **audit** azioni.

Tutte le interfacce sono private (SSO + IP allowlist/tunnel SSM), non esposte pubblicamente.

---

11) Pro/Contro e impatti

Scenario A – Doppia istanza

Pro - **Isolamento**: separa piano admin/IdP da piano applicativo; riduce **blast radius**. - **Prestazioni**: dimensionamento autonomo; OpenFGA vicino ai servizi app. - **Sicurezza**: superficie d'attacco più piccola sull'host pubblico. **Contro** - **Costo** più alto (2×EC2 + EBS). - **Operatività** più articolata.

Scenario B – Istanza unica

Pro - **Costo** e **setup** minimi; perfetto per MVP. - **Operatività** più snella. **Contro** - **Blast radius** applicativo maggiore; concorrenza su risorse host. - Crescita limitata: possibile migrazione a A.

Gold Solar S.r.l.
Via Purgatorio 40, 80147,Napoli, Italia
Tel: 081 016 9472 – Email: info@goldsolarweb.com
Sito: ww.goldenbitweb.com – www.goldsolarweb.com
Partita IVA: 10355251215

IdP: Keycloak vs Cognito

- **Keycloak (self-hosted)**: pieno controllo, SSO enterprise ricco; richiede gestione patch/HA/backup (coperti da RDS + auto-restart).
- **Cognito (cloud)**: zero-ops, MFA/SSO pronti; **costi per MAU**; alcune personalizzazioni avanzate richiedono Lambda triggers.

OpenFGA

- Potente su **gerarchie** e **permessi per risorsa**; modello **as-code**; latenza bassa in VPC.
- Richiede **DB dedicato** (RDS Postgres) e governance di schema/tuples (che forniamo).

---

12) Raccomandazione

- **Fase 1 (MVP/early)**: **Scenario B** (istanza unica) + **Cognito** (cloud) + **OpenFGA** (EC2 + RDS Postgres dedicato). Time-to-market rapido, zero-ops su IdP, affidabilità RDS.
- **Fase 2 (growth/enterprise)**: migrazione a **Scenario A** (doppia istanza) mantenendo OpenFGA; se richiesto da **policy/on-prem**, passaggio a **Keycloak** al posto di Cognito (stessa integrazione API).
- Sempre: **RDS Multi-AZ + RDS Proxy + PITR** e **Policy as Code** per OpenFGA.

---

13) Piano di implementazione

Fase 0 – Kick-off (t=?): requisiti, domini, account AWS/CI; scelta IdP; modello permessi. **Fase 1 – Foundation (t=?)**: Terraform (VPC, SG, EC2, RDS + Proxy, ECR, S3, CloudWatch, SSM, Route53/ACM); bootstrap Docker/Compose; deploy OpenFGA (+ RDS dedicato). **Fase 2 – Identity (t=?)**: Cognito *oppure* Keycloak (con RDS dedicato); SSO OIDC; claim/attributi `tenant_id`/ruoli. **Fase 3 – CI/CD & Deploy (t=?)**: pipeline *develop*→preprod, *main*→prod, *blue/green*, healthcheck. **Fase 4 – Automazioni tenant (t=?)**: workflow "Nuovo Studio", UI admin (MVP), integrazione OpenFGA (schema/tuples). **Fase 5 – DR/Hardening (t=?)**: policy RDS (PITR, snapshot), runbook RTO≤40, test restore, audit.

Totale: tempo da determinare (variabile su complessità applicativa e scelta IdP).

Gold Solar S.r.l.
Via Purgatorio 40, 80147,Napoli, Italia
Tel: 081 016 9472 – Email: info@goldsolarweb.com
Sito: ww.goldenbitweb.com – www.goldsolarweb.com
Partita IVA: 10355251215

14) Deliverable

- **Terraform** completo (VPC, EC2, RDS/RDS Proxy, ECR, S3, CloudWatch, SSM, Route53/ACM, IAM, OpenFGA, Keycloak opz.).
- **CI/CD** con approvazioni; **Policy as Code** (repo schema/tuples OpenFGA; realm config Keycloak se usato).
- Template **Docker Compose** + reverse proxy (Nginx **e** Traefik).
- Workflow **“Nuovo Studio”** e altri workflows da determinare (CLI/CI + UI custom) con scrittura automatica di tuples OpenFGA.
- Runbook operativi (deploy, resize host/container, DR, restore PITR, gestione permessi).
- Dashboard/Allarmi CloudWatch + grafici Grafana/Netdata.
- Documentazione tecnica e **manuale UI** amministrativa.
- Documentazione per sviluppatori sull’integrazione dei servizi nel backend

15) Stime costi (IVA esclusa)

Da determinare