

CAMUNDA AUF STACKIT

CLOUD-SOUVERÄNITÄT IN DER PRAXIS

HEJ, ICH BIN STEFAN

- CONSULTANT BEI **CONSID**
- PROCESS AUTOMATION
- CLOUD ARCHITECTURE
- **CAMUNDA** CHAMPION



EIN BRIEF AUS WASHINGTON D.C.

- › IM JUNI ANWEISUNG AN ANTHROPIC
- › NEUSTES KI-MODELL GESPERRT
- › KEINE VORWARNUNG ODER FRIST
- › EUROPÄISCHE NUTZER AUSGESPERRT
- › TRUMP HAT NOCH 2.5 JAHRE IM AMT



BLEIBT DAS EIN
EINZELFALL?



WAS WÄRE, WENN DAS CLOUD-ANBIETER TRIFFT?

- > DATEN: WEG
- > ANWENDUNGEN: OFFLINE
- > BUSINESS: STILLSTAND
- > NUR EINEN REGIERUNGSENTSCHEID
AUS WASHINGTON ENTFERNT



DIE **HYPERSCALER**-LANDSCHAFT

- **AMAZON WEB SERVICES** → SEATTLE, USA
- **MICROSOFT AZURE** → REDMOND, USA
- **GOOGLE CLOUD** → MOUNTAIN VIEW, USA

"ABER WIR NUTZEN DOCH
DIE EU-REGION..."

DREI EBENEN DER SOUVERÄNITÄT

EBENE	BEDEUTET	HYPERSCALER
DATENRESIDENZ	WO LIEGEN DIE DATEN?	 EU
OPERATIVE AUTONOMIE	WER BETREIBT DIE INFRASTRUKTUR?	 EU
RECHTL. SOUVERÄNITÄT	WELCHES RECHT GREIFT?	 CLOUD ACT



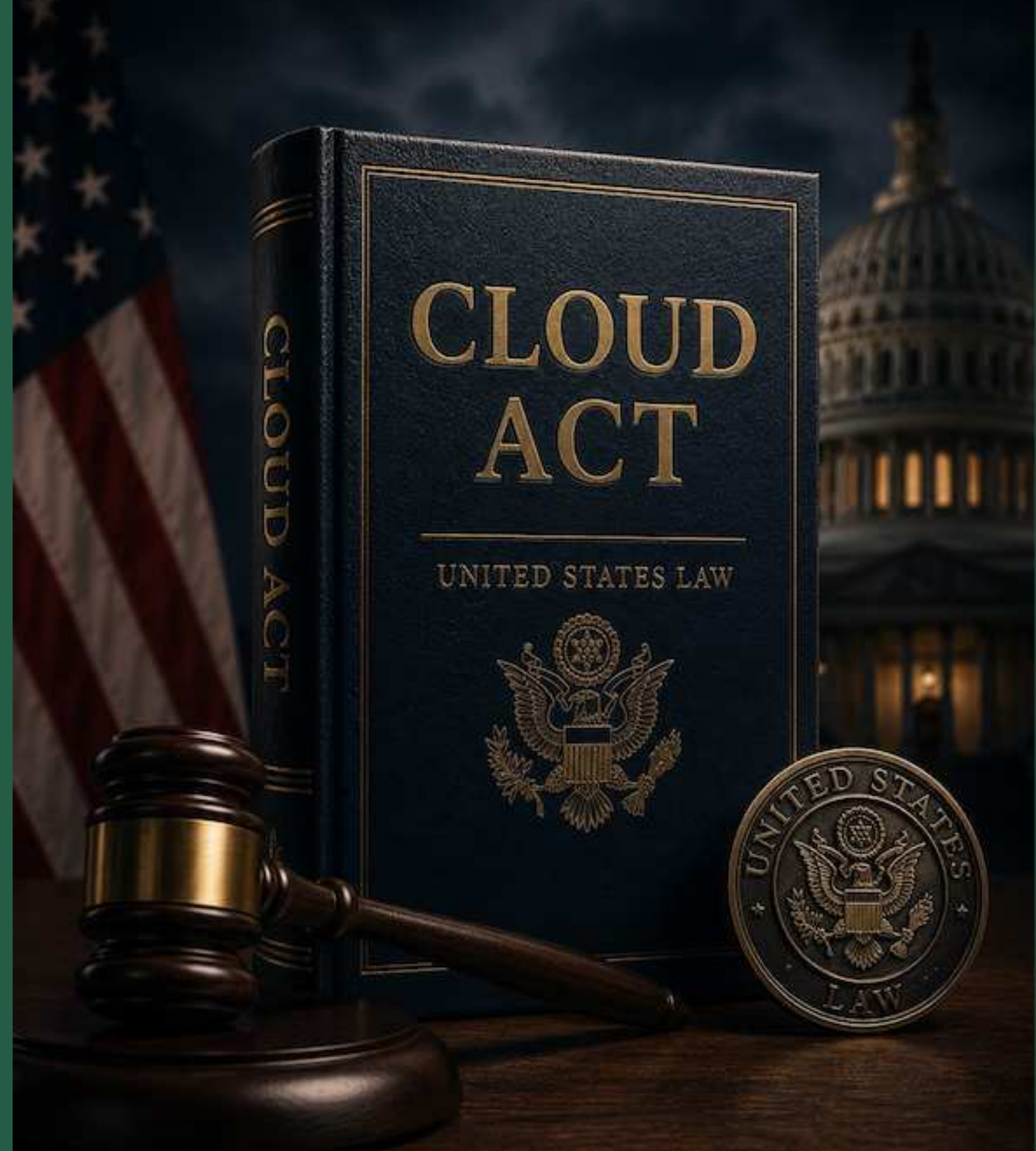
EUROPÄISCHE TOCHTERGESELLSCHAFTEN

- AWS EUROPEAN SOVEREIGN CLOUD
- MICROSOFT IRELAND
- GOOGLE CLOUD EMEA

→ UNTERLIEGEN TEILS EU RECHT
→ SCHLIEßT US-RECHT **NICHT** AUS

DER CLOUD ACT

- › US-BEHÖRDEN DÜRFEN DATEN ANFORDERN
- › **EGAL** WO DIE DATEN GESPEICHERT SIND
- › DAS UNTERNEHMEN MUSS **KOOPERIEREN**
- › KEIN EU-GERICHT KANN DAS STOPPEN



WAS IST CLOUD-SOUVERÄNITÄT?

- > RECHTSPERSON UNTER EU-RECHT
- > KEINE MUTTERGESELLSCHAFT UNTER FREMDEM RECHT
- > INFRASTRUKTUR IN EUROPÄISCHEM EIGENTUM
- > KEINE VERSTECKTEN US-ABHÄNGIGKEITEN

WER KONTROLLIERT
DEN AUS-SCHALTER?

STACKIT

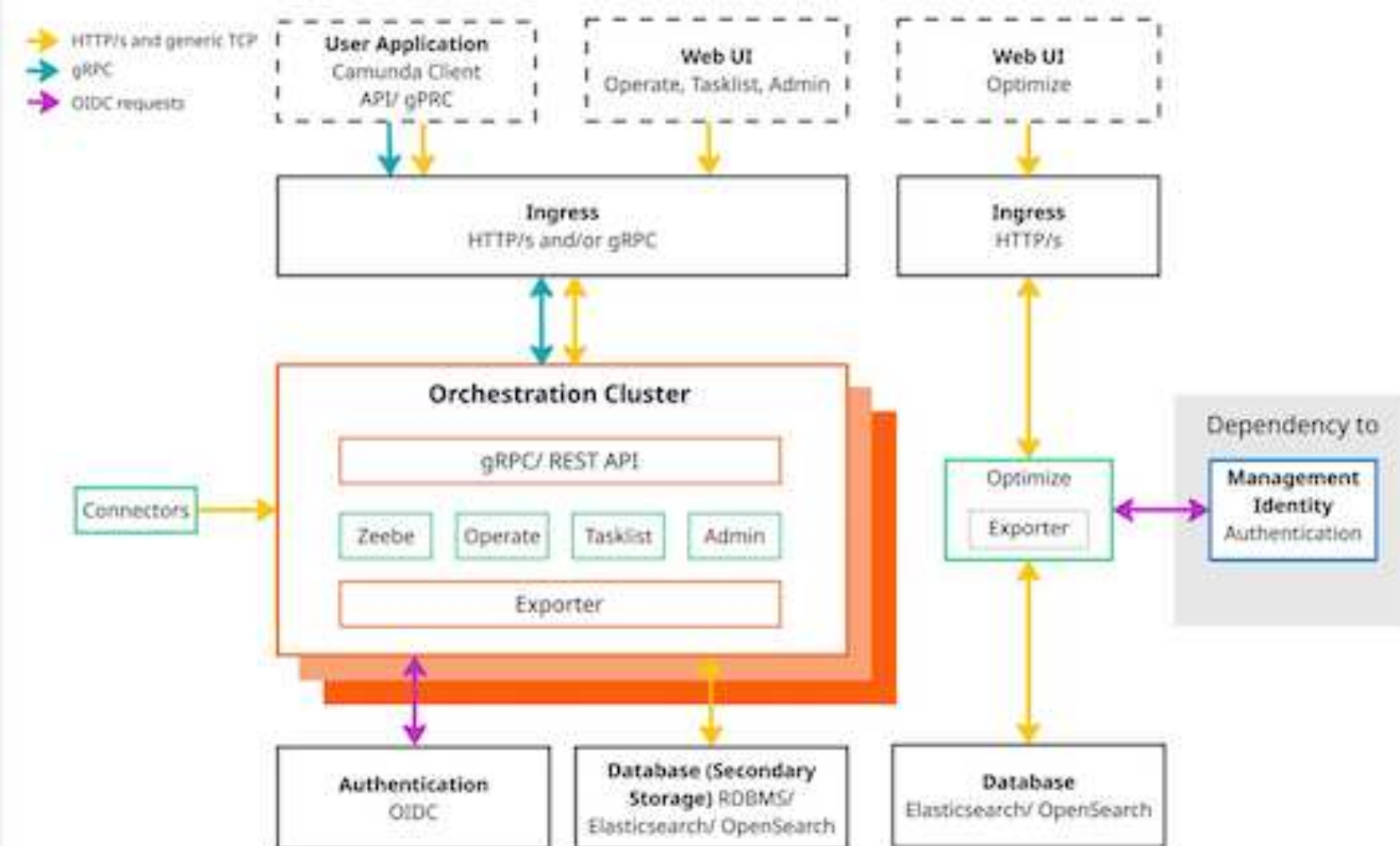
- › CLOUD-PLATTFORM DER **SCHWARZ GRUPPE**
- › 100% **EUROPÄISCHES** EIGENTUM
- › AUSSCHLIEßLICH **EU-RECHT** / DSGVO
- › **KEIN** CLOUD ACT



STACKIT VS. **HYPERSCALER**

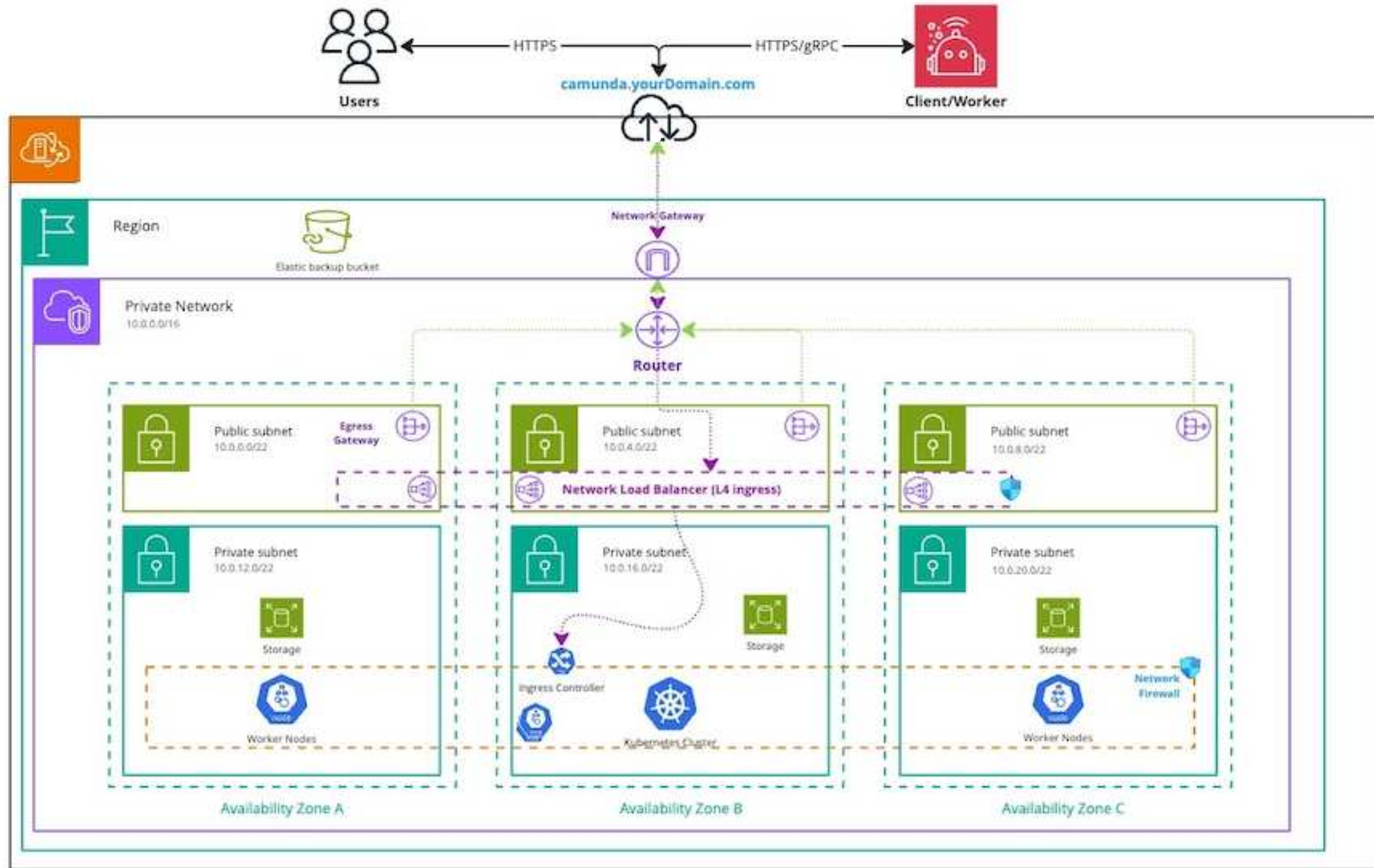
	STACKIT	AWS / AZURE / GCP
EU-EIGENTUM	✓	✗ / ✓ / ✓
REINES EU-RECHT	✓	✗ / ✗ / ✗
KUBERNETES	✓	✓
MANAGED STORAGE	✓	✓
MANAGED SERVICES	✓	✓
MONITORING	✓	✓

CAMUNDA AUF STACKIT



- > **CAMUNDA 8 (SELF-MANAGED) DEPLOYEN**
- > **KUBERNETES VIA STACKIT SKE**
- > **BACKUP VIA OBJECT STORAGE (S3-KOMPATIBEL)**
- > **PERSISTENZ VIA MANAGED DBS & VOLUME CLAIMS**
- > **ZIEL: REPRODUZIERBAR UND DOKUMENTIERT**

REFERENCE ARCHITECTURE (AWS)



REFERENCE ARCHITECTURE (AWS)

- > KUBERNETES, CAMUNDA, ETC. VIA TERRAFORM
- > EIN TERRAFORM STATE PRO UMGEBUNG
- > KEIN GITOPS, KEIN SELF-HEALING
- > KEIN PLATFORM ENGINEERING

ABWEICHUNGEN ZU **AWS**

- > KEIN PRIVATE NETWORK: **ACLS FÜR MANAGED SERVICES**
- > KEIN NATIVE SECRET INJECTION: **ESO + SECRET MANAGER**
 - > KEIN MANAGED TLS: **CERTMANAGER + LET'S ENCRYPT**
- > KEIN DEFAULT KUBERNETES INGRESS: **EIGENER NGINX DELOYED**

WIE WIR **ANGEFANGEN** HABEN

- > EIN TERRAFORM STATE FÜR ALLES
- > INFRASTRUKTUR & CAMUNDA. ALLES ZUSAMMEN
- > DEPLOYMENT: TERRAFORM UND HELM GEMISCHT
- > SECRETS: TERRAFORM OUTPUTS → HELM VALUES

EIN CAMUNDA CONFIG-CHANGE
BETRAFF IMMER DEN GANZEN STACK.

PLATFORM-ENGINEERING

INFRA MIT TERRAFORM

- KUBERNETES CLUSTER
- POSTGRES / OPENSEARCH
 - OBJECT STORAGE
 - SECRETS MANAGER
- ESO + ARGOCD BOOTSTRAP

PLATFORM MIT GITOPS

- CERT-MANAGER + INGRESS
 - MONITORING STACK
 - NETWORK POLICIES
 - VOLUMES CLAIMS
 - CAMUNDA

TEST UND PROD

- > **TEST**: MINIMAL – KEIN OPENSEARCH, KEIN MONITORING, SINGLE AZ
- > **PROD**: 3-AZ, HA POSTGRESQL, OPENSEARCH, PROMETHEUS + GRAFANA

WARUM DIESER WECHSEL?

1. **BLAST RADIUS:** CAMUNDA-ÄNDERUNG RE-PLANTE SKE + DATENBANKEN
2. **GITOPS:** KEIN SELF-HEALING, KEIN DRIFT-SCHUTZ OHNE ARGOCD
3. **SECRETS:** TERRAFORM-OUTPUTS ALS HELM-VALUES KOPPELN INFRA UND APP

VORTEILE UNSERES ANSATZES

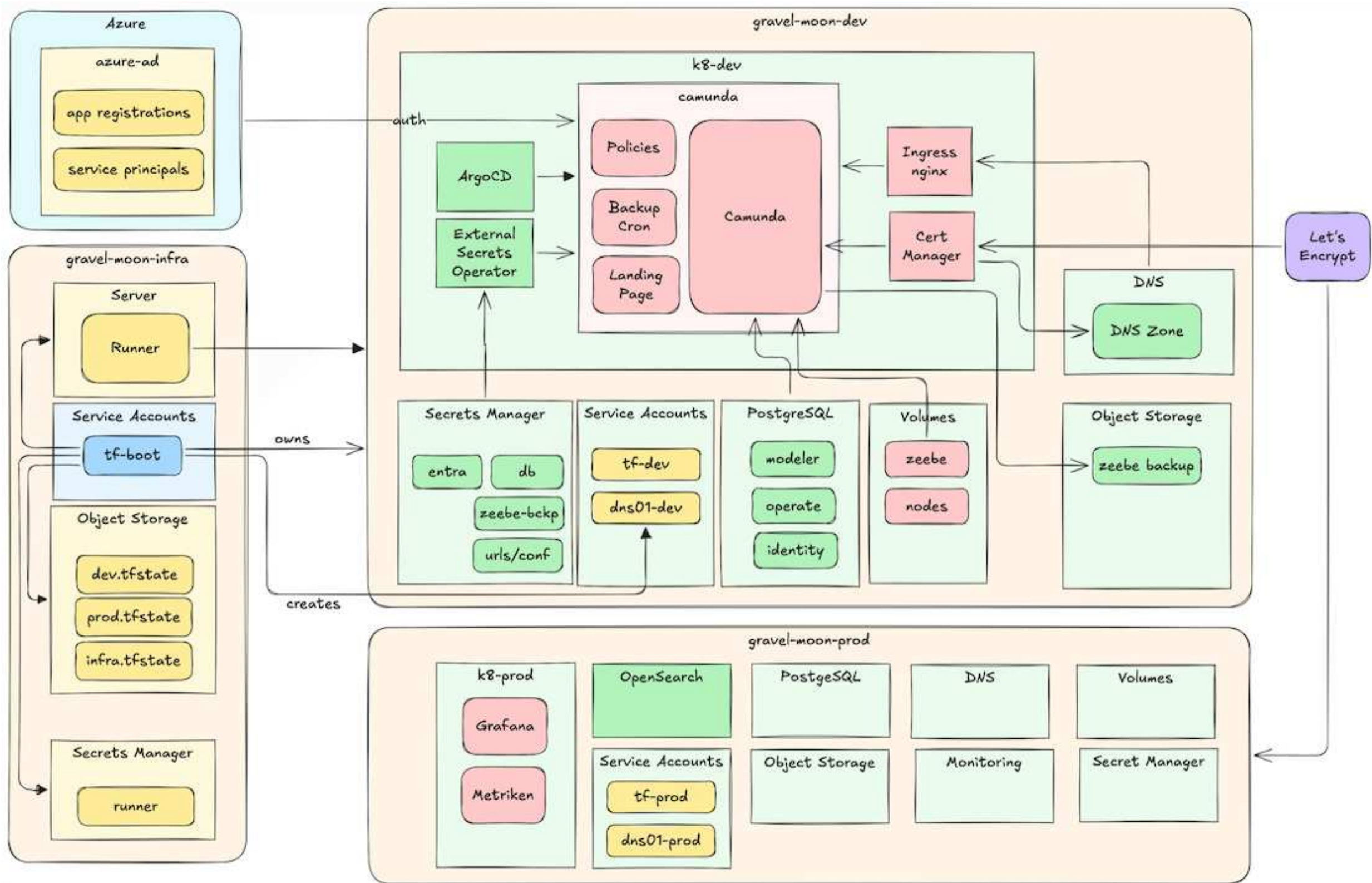
- > **BLAST RADIUS:** CAMUNDA-ÄNDERUNG $\neq$ INFRA-RE-PLAN
- > **SELF-HEALING:** ARGOCD ERKENNT UND KORRIGIERT DRIFT
- > **CREDENTIAL-TRENNUNG:** RUNNER $\neq$ ARGOCD $\neq$ APP
- > **PROMOTION VIA PR:** AUDITIERBAR, REVIEWBAR, KEINE MANUELLE APPLY

NACHTEILE UNSERES ANSATZES

- > **BOOTSTRAPPING KOMPLEX:** INFRA HÄNDISCH AUFBAUEN
- > **2 REPOS:** NEUE DATENBANK = 2 PRS IN 2 REPOS
- > **TOOLING-OVERHEAD:** ARGOCD + ESO + TERRAFORM = 3 SYSTEME ZU LERNEN
- > OVERKILL FÜR **KLEINE TEAMS** OHNE PLATFORM-ERFAHRUNG

WAS PLATFORM ENGINEERING SCHWER MACHT

- > **BOOTSTRAPPING-PARADOX:** PLATFORM MUSS SICH SELBST DEPLOYEN: JEMAND MUSS 1. SCHRITT TUN
- > **DYNAMISCHE ABHÄNGIGKEITEN:** RESSOURCEN ENTSTEHEN ZUR LAUFZEIT, Z.B. POSTGRESQL HOSTNAME
- > **LAYER-KOORDINATION:** FEATURE BERÜHRT MEHRERE LAYER.
NEUE DB = TF + ESO + HELM + GITOPS
- > **TIMING:** LAYER N SETZT LAYER N-1 VORAUS



KUBERNETES AUF STACKIT (SKE)

- > STANDARD-KONFORMES **MANAGED KUBERNETES**
- > **HELM CHARTS** LAUFEN MIT KLEINEN ANPASSUNGEN
- > INGRESS, LOAD BALANCER, PERSISTENT VOLUMES: ALLES DA
- > **KEIN VENDOR-LOCK-IN** AUF K8S-EBENE

HERAUSFORDERUNGEN

- > **WENIG VORBILDER:** KEINE TUTORIALS FÜR STACKIT + CAMUNDA
- > **ANDERE DEFAULTS:** UNTERSCHIEDE BEI PROVIDERN
- > **GRENZEN VON MANAGED SERVICES:** NICHT ALLE VERSIONEN + FEATURES VERFÜGBAR

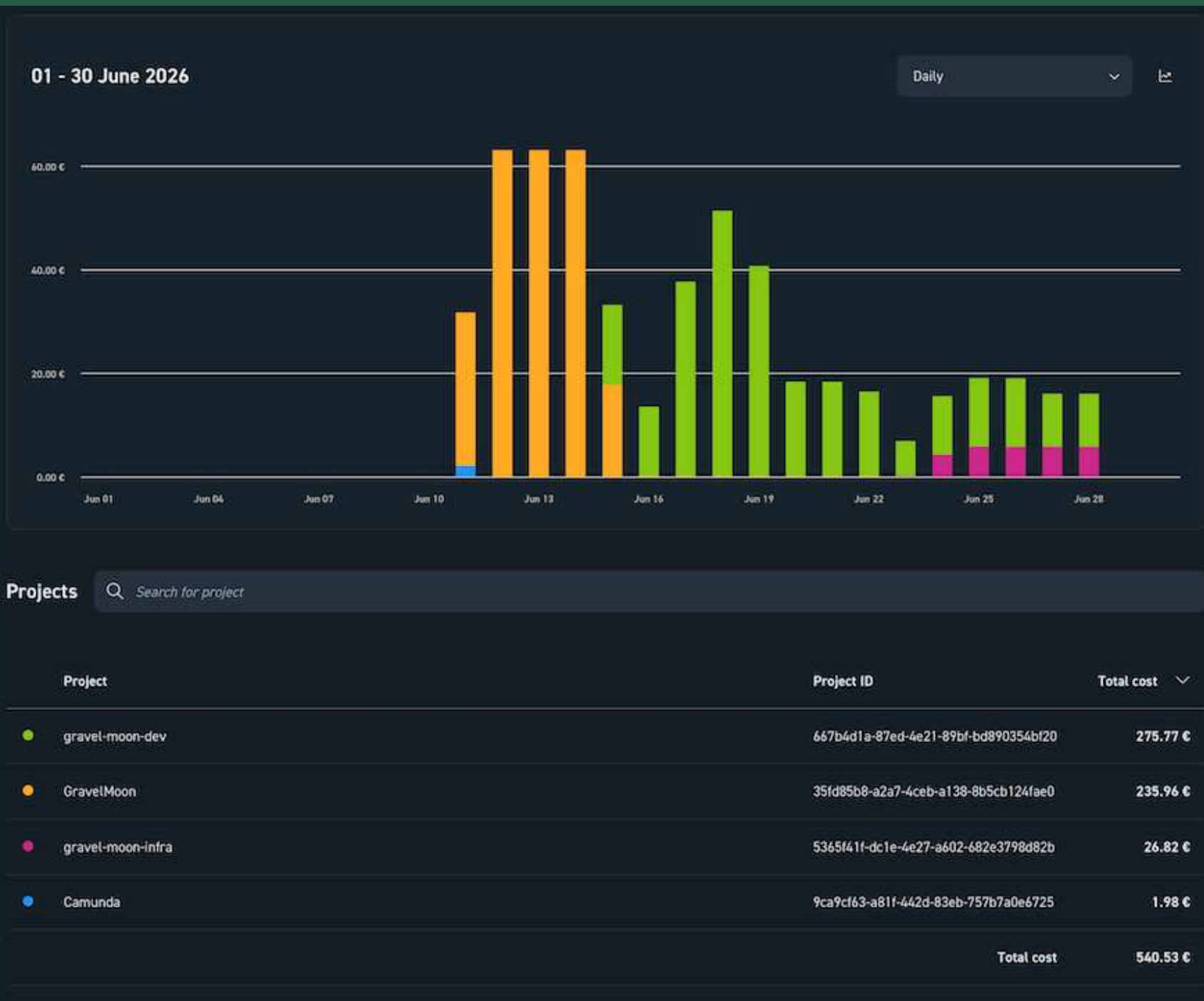
WAS **GUT** FUNKTIONIERT HAT

- > **TEMPO**: ERSTER CLUSTER IN UNTER EINEM TAG
- > **KEIN VENDOR LOCK-IN**: STANDARDWERKZEUGE FUNKTIONIEREN
- > **STACKIT SUPPORT**: VIELE TERRAFORM PROVIDER
- > **KOSTENTRASPARENZ**: KEINE ÜBERRASCHUNGEN

INFRASTRUKTURKOSTEN

- > INFRA CA. 90€/MONAT (GITHUB RUNNER)
- > TEST CA. 600€/MONAT (MIT HIBERNATION)
- > PROD CA. 1.200€/MONAT

ZUM VERGLEICH: CAMUNDA SAAS (PROD)
KOSTET CA. 8000€/JAHR



DIE SOUVERÄNE CLOUD

- > IST BEREITS **PRODUKTIONSREIF**
- > KOSTET VERHÄLTNISMÄßIG MEHR
- > KANN MIT US-HYPERSCALERN MITHALTEN
- > IST EINE **ECHTE** ALTERNATIVE

CLOUD-SOUVERÄNITÄT IST RISIKOMANAGEMENT

FAZIT

- > DER AI-VORFALL WAR EIN WECKRUF
- > CAMUNDA AUF STACKIT FUNKTIONIERT
- > SOUVERÄNITÄT HAT IHRE KOSTEN
- > DIE FRAGE IST NICHT OB, SONDERN WANN