

Disaster Recovery & Multi-Cloud

Drei Praxisfälle für belastbare Wiederherstellung, definierte RTO/RPO-Ziele und kontrollierte Cloud-Ausfälle

3 ANONYMISIERTE PRAXISFÄLLE · REFERENZARCHITEKTUREN

AWS · Azure · GCP · Backup · Failover · Recovery Testing

Drei reale Betriebssituationen, drei Recovery-Strategien

Nicht nur Backups: Entscheidend sind Wiederanlauf, Datenverlustgrenze, Verantwortlichkeiten und getestete Abläufe.

01

ONLINE-HANDEL

AWS Primary + Azure Failover

Checkout auch bei Regionalausfall erreichbar

02

PRODUKTION & ERP

Ransomware-sichere Wiederherstellung

Saubere Kopien, isolierter Restore, definierte Reihenfolge

03

B2B-SAAS

Multi-Region Active/Standby

Automatisches Failover mit Recovery Control Center

Gemeinsame Logik: Geschäftsauswirkung verstehen → RTO/RPO festlegen → Architektur umsetzen → Restore und Failover regelmäßig testen.

Projekt 1: E-Commerce ohne langen Stillstand

Online-Handel mit hohem Umsatzrisiko · anonymisierte Referenzarchitektur

PRAXISFALL 1

AUSGANGSLAGE

Ein regionaler Cloud-Ausfall hätte Checkout, Bestellungen und Zahlungsstatus gleichzeitig betroffen. Backups existierten, aber Wiederanlaufzeit und Zuständigkeiten waren nicht belastbar definiert.

UMSETZUNG

AWS blieb Primärumgebung. Azure wurde als schlanke Recovery-Plattform vorbereitet. Datenbank-Replikation, unveränderbare Backups, DNS-Umschaltung und ein zeitlich getestetes Runbook wurden verbunden.

BETRIEBLICHE WIRKUNG

Das Team kann einen Ausfall strukturiert bewerten und den Shop innerhalb eines klaren Zeitfensters kontrolliert in der Recovery-Umgebung wieder bereitstellen.

RECOVERY-ZIELE

15 Min. RTO

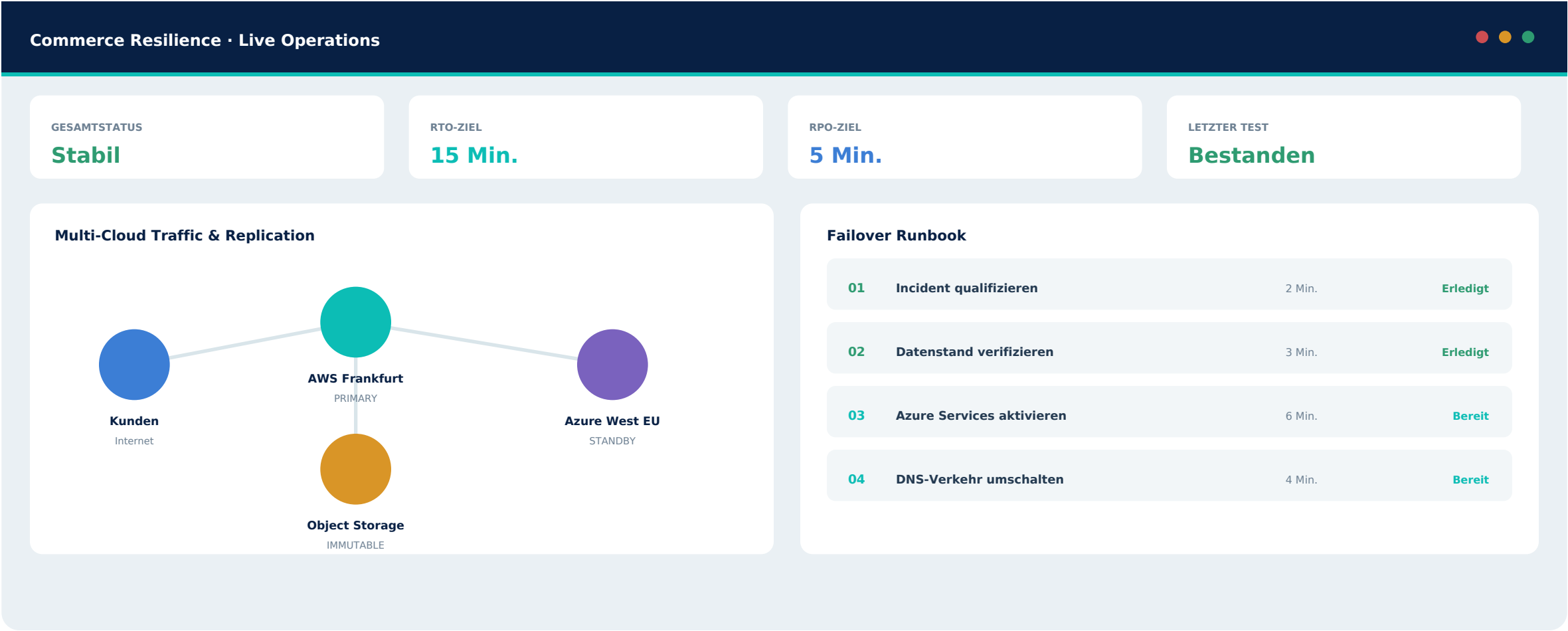
5 Min. RPO

4× jährlich DRIL

getestet STATUS

Projekt 1: E-Commerce Recovery Control Center

AWS als Primärumgebung, Azure als kontrollierte Wiederanlaufplattform.



Projekt 2: ERP-Wiederaufbau nach Cyberangriff

Produktion mit zentralem ERP und mehreren Abhängigkeiten · anonymisierte Referenzarchitektur

PRAXISFALL 2

AUSGANGSLAGE

Ein Verschlüsselungsangriff hätte nicht nur Dateien, sondern auch Identitäten, Datenbank, ERP und Produktionsschnittstellen betroffen. Klassische Backups allein hätten keinen sauberen Wiederaufbau garantiert.

UMSETZUNG

Unveränderbare Kopien, getrennte Zugangsdaten, isolierte Clean-Room-Wiederherstellung, Malware-Prüfung und eine priorisierte Startreihenfolge wurden als gemeinsamer Prozess aufgebaut.

BETRIEBLICHE WIRKUNG

Die Organisation kann saubere Datenstände auswählen, Systeme kontrolliert prüfen und den ERP-Betrieb in nachvollziehbaren Stufen zurückführen.

RECOVERY-ZIELE

4 Std.

RTO ERP

30 Min.

RPO DB

3-2-1-1-0

KOPIEN

halbjährlich

TEST

Projekt 2: Ransomware Recovery Workbench

Isolierte Wiederherstellung, saubere Datenprüfung und kontrollierter ERP-Wiederanlauf.



Projekt 3: SaaS-Plattform über mehrere Regionen absichern

B2B-SaaS mit europäischen Kunden · anonymisierte Referenzarchitektur

PRAXISFALL 3

AUSGANGSLAGE

Die Plattform lief stabil, doch zentrale Abhängigkeiten waren auf eine Region konzentriert. Ein Failover einzelner Dienste hätte ohne Orchestrierung neue Fehlerketten erzeugen können.

UMSETZUNG

Service-Abhängigkeiten, Replikationsstatus, Health Checks und Freigaberegeln wurden in einem Resilience Orchestrator zusammengeführt. Active/Standby blieb bewusst kontrolliert statt blind automatisiert.

BETRIEBLICHE WIRKUNG

Betrieb und Management sehen denselben Recovery-Status. Failover-Entscheidungen basieren auf messbaren Signalen, dokumentierten Regeln und regelmäßig geübten Abläufen.

RECOVERY-ZIELE

30 Min. RTO

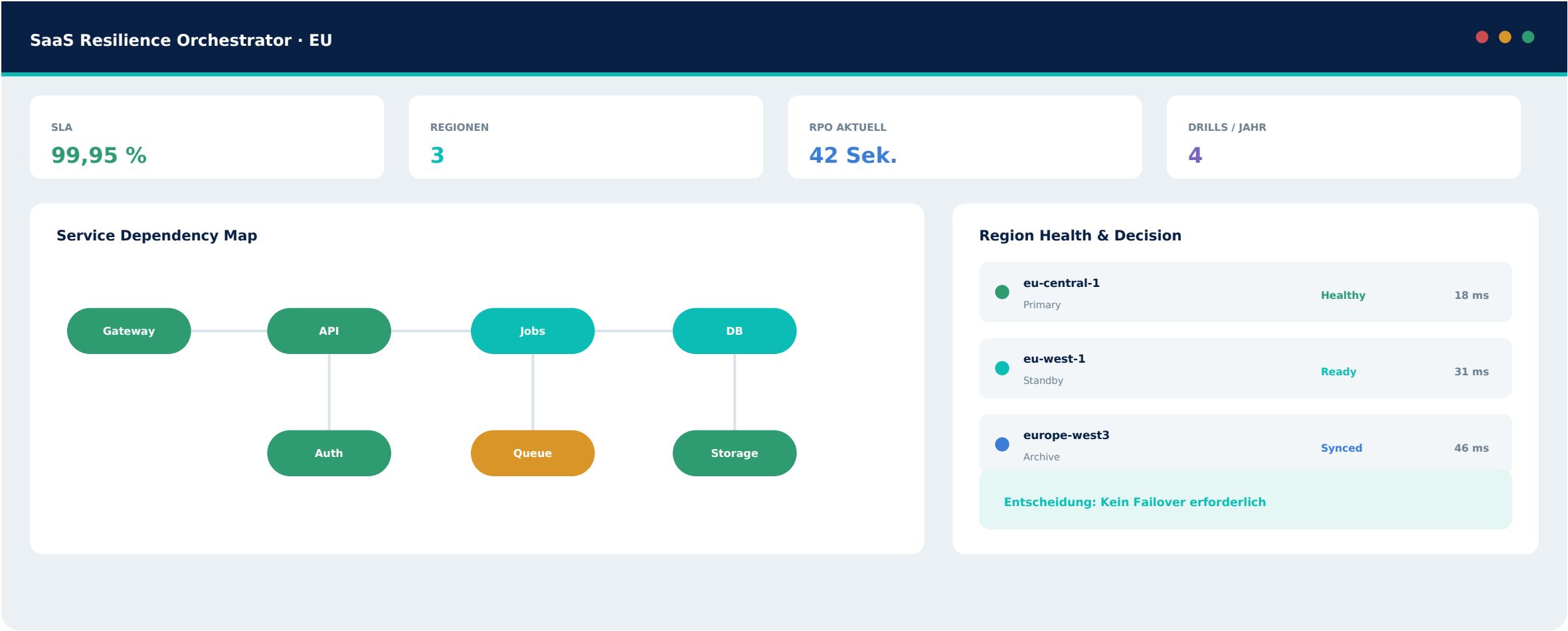
< 1 Min. RPO

3 REGIONEN

99,95 % SLA-ZIEL

Projekt 3: Multi-Region SaaS Resilience

Automatisiertes Failover mit Health-Signalen, Abhängigkeiten und klarer Freigabelogik.



Recovery beginnt vor dem Ausfall.

**Ziele, Architektur und Tests
gemeinsam definieren.**

Wir starten mit den geschäftskritischen
Prozessen, bewerten Abhängigkeiten und
entwickeln daraus eine realistische RTO/RPO- und
Wiederanlaufstrategie.

Anirudh Chawla
Founder & Senior Software Engineer

EaseWerk Digital

anirudh@easewerk.de
+49 162 8893421
easewerk.de

Disaster Recovery · Multi-Cloud · RTO/RPO · Backup · Failover · Recovery
Tests