04 · SCHÜTZEN · BACKUP & DISASTER RECOVERY

Wir messen vorab, in wie vielen Minuten Sie nach einem Katastrophenfall wieder betriebsbereit sind.

Von einer unternehmensspezifischen Backup-Richtlinie über eine Data-Guard-basierte Disaster-Recovery-Architektur bis hin zu regelmäßigen Restore-Tests und einem schrittweisen DR-Runbook sichern wir Ihre Geschäftskontinuität ab.

DAS PROBLEM, DAS WIR LÖSEN

Backups werden erstellt, aber niemand weiß, wann zuletzt eine Wiederherstellung getestet wurde.

Unklar ist, was passiert, wenn Ransomware auch die Backups verschlüsselt.

RTO- und RPO-Ziele sind dokumentiert, wurden aber nie gemessen.

LEISTUNGSUMFANG

Backup-Richtlinie
Entwicklung einer unternehmensspezifischen Backup-Richtlinie und Retention-Planung.

Immutable-Backup-Architekturen
Gegen Ransomware geschützte Kopien mit RMAN, Snapshots und unveränderlichen Backups.

Restore-Tests
Nachweis durch regelmäßige Restore-Tests, dass die Backups tatsächlich funktionieren.

Backup-Integration
Integration mit NetWorker, ZFS und Cloud-Speicher-Infrastrukturen.

DR-Architektur
Disaster Recovery mit Data Guard und plattformunabhängiger Replikation, einschließlich Exadata-to-Exadata.

RTO-/RPO-Design
Auslegung von Wiederherstellungszeit und Datenverlusttoleranz gemäß den Zielen der Geschäftskontinuität.

TECHNOLOGIEN

Oracle Database · Exadata / ExaCC · Microsoft SQL Server · PostgreSQL / EDB · OLVM / KVM · RMAN · Data Guard · NetWorker · ZFS

SCHNELLSTART

Paket	Dauer	Ergebnisse
DR-Übung	1 Woche	Gemessene RTO/RPO und aktuelles Runbook

Kostenloses Erstgespräch

In 45 Minuten lernen wir Ihre Umgebung und Ihre Prioritäten kennen. Kostenlos.

KONTAKT

info@turncloudon.com

0850 346 30 49

www.turncloudon.com.tr/de/uzmanlik/yedekleme-fkm

Istanbul · Ankara · Konya · Prag

VORGEHEN

01

Richtlinie und Inventar

Erfassung kritischer Systeme und des bestehenden Backup-Schemas.

02

Architektur

Auslegung der Backup- und DR-Architektur gemäß den RTO/RPO-Zielen.

03

Implementierung

Inbetriebnahme der Backup-, Replikations- und Monitoring-Infrastruktur.

04

Übungen

Geplante Switchover- und Failover-Übungen mit Messung der Zeiten.

05

Runbooks und Schulung

Schrittweise DR-Runbook-Dokumentation und Teamschulung.

DREI STUFEN AUF BASIS VON RPO UND RTO

Paket	RPO	RTO	Backup-Schema	Geeignete Workloads
Standard	24 Stunden	8 Stunden	Täglich inkrementell, wöchentlich voll; 30 Tage Aufbewahrung, Monatsarchiv 12 Monate	Fileserver, sekundäre Anwendungen, Testumgebungen
Erweitert	4 Stunden	4 Stunden	Täglich voll + untertägig inkrementell, Log-Backups für Datenbanken; 90 Tage Aufbewahrung	Geschäftsanwendungen, Datenbanken mittlerer Kritikalität
Kritisch	15 Minuten	1 Stunde	Kontinuierliche Log-/WAL-Archivierung, Point-in-Time-Recovery, Kopie an einen zweiten Standort	Produktionsdatenbanken, geschäftskritische Anwendungen

Die Werte werden im Anhang zum Servicevertrag je Workload-Klasse verbindlich festgelegt.

DIE 3-2-1-1-0-REGEL

- Drei Kopien, zwei verschiedene Medien, eine extern, eine unveränderlich, null Verifizierungsfehler
- Nicht löschbare Kopie per Object Lock oder WORM
- Das Backup-System wird unabhängig von der produktiven Identitätsinfrastruktur berechtigt
- Verschlüsselung bei Übertragung und Speicherung; das Schlüsselmanagement wird getrennt gehalten
- Integritätsprüfung jedes Backups und regelmäßige Wiederherstellungstests
- Szenariobasierter Disaster-Recovery-Plan und mindestens zwei Übungen pro Jahr

MESSBARE ZUSAGE

Ein Backup ohne Wiederherstellungstest gilt bei uns nicht als erfolgreich. Der Monatsbericht enthält die Anzahl der getesteten Backups, die gemessene Wiederherstellungszeit und deren Vergleich mit dem zugesagten RTO.

LÖSUNGSDETAILS

Hochverfügbarkeit und Replikation	Eine unterbrechungsfreie Datenschicht mit Data Guard, Always On, Patroni und InnoDB Cluster; heterogene Replikation mit GoldenGate.