Oracle-Datenbanken: Verantwortlichkeiten und Sicherheit im Vergleich

Diese Übersicht vergleicht drei Betriebsmodelle für Oracle-Datenbanken: den klassischen Eigenbetrieb, den Eigenbetrieb mit Oracle Exadata Cloud@Customer (ExaCC) sowie die Managed Oracle Database Cloud von T-Systems. Sie zeigt, welche Verantwortlichkeiten in den einzelnen Modellen beim Kunden, bei Oracle oder bei T-Systems liegen, und unterstützt Infrastrukturverantwortliche dabei, die Optionen intern zu beurteilen und mit weiteren Entscheidungsträgern zu besprechen.

Detail-Vergleich: Eigenbetrieb klassisch, Eigenbetrieb mit ExaCC und Managed Oracle Database Cloud

Die entscheidende Frage lautet nicht nur, wo die Datenbank läuft, sondern welche Aufgaben im eigenen Team bleiben. Die folgende Tabelle zeigt die Verantwortlichkeiten Ebene für Ebene.

Ebene / Aufgabe	Eigenbetrieb klassisch	Eigenbetrieb mit ExaCC	Managed Oracle Database Cloud (T-Systems)
Infrastruktur			
Besitz Hardware	Kunde	Oracle	Oracle
Rechenzentrum (Fläche, Strom, Kühlung, Netz)	Kunde	Kunde	T-Systems (Zollikofen und Bern)
Infrastruktur-Patching, Sicherheitsscans und -updates	Kunde, allenfalls mit Wartungsvertrag	Oracle	Oracle; Cluster-Patching durch T-Systems, rolling, unterbruchsfrei
Hardware-Überwachung und Wartung	Kunde oder Hersteller	Oracle	Oracle
Zugriff auf die Infrastruktur	Kunde	Oracle, Kunde ohne Zugriff	Oracle; Zugang auditierbar und von T-Systems kontrolliert, mit Notfall-Trennung
Zweiter Standort für Disaster Recovery	Kunde	Kunde (zweites System, zweiter Standort)	T-Systems: zwei Rechenzentren mit Data Guard, 99.9% Disaster Recovery Verfügbarkeit ab SLA-Stufe Advanced
Datenbanken			
Bereitstellung und Verwaltung von VMs und Datenbanken	Kunde	Kunde, mit Oracle-Cloud-Automatisierung	T-Systems; Bestellung durch den Kunden per Portal oder API

Monitoring und Event-Management	Kunde	Kunde	T-Systems, Events klassifiziert und Incidents an Ihr Service Desk; Kunde mit lesendem Zugriff über Oracle Enterprise Manager
Kapazitäts- und Verfügbarkeitsmanagement	Kunde	Kunde	T-Systems, inklusive Trends, Analysen und Verbesserungsvorschlägen
Lizenzen	Kunde: Lizenz plus jährlicher Support an Oracle	Kunde: Abo inklusive Lizenz oder eigene Lizenzen	T-Systems: License Included mit allen Enterprise-Funktionen; für grosse Umgebungen mit eigenen BYOL Lizenzen möglich
Migration	Kunde oder Dienstleister	Kunde oder Dienstleister	Kunde und T-Systems gemeinsam
Bereitschaftsdienst	Kunde	Kunde	T-Systems, 7x24 ab SLA-Stufe Basic
Datenbank-Patching	Kunde	Kunde	T-Systems stellt bereit, Kunde bestimmt den Zeitpunkt
Backup und Recovery	Kunde	Kunde, Recovery Appliance optional und separat	T-Systems mit ZDLRA: unveränderbar, validiert, Wiederherstellung auf Zeitpunkte, redundant in beiden Rechenzentren
Automatisierung	Kunde, eigene Skripte	Oracle-Cloud-Automatisierung, bedient durch den Kunden	T-Systems-Automatisierung, für den Kunden über API und Portal nutzbar, CI/CD-Integration
Zugriff auf das Betriebssystem der Datenbankserver	Kunde	Kunde	T-Systems, kein OS-Zugriff für Kunden
Anwendungen und Daten			
Daten, Schemas, Schlüssel	Kunde	Kunde	Kunde
Anwendungen und Anwendungsbetrieb	Kunde	Kunde	Kunde

Sicherheit und Wiederherstellbarkeit: Schutz in fünf Schichten

Sicherheit entsteht nicht durch eine einzelne Massnahme, sondern durch mehrere Schichten, die sich ergänzen. Die Übersicht zeigt, welche Aufgaben in jedem Betriebsmodell selbst umgesetzt werden müssen und welche Verantwortlichkeiten beim jeweiligen Anbieter liegen.

Schicht	Eigenbetrieb klassisch	Eigenbetrieb mit ExaCC	Managed Oracle Database Cloud (T-Systems)
1. Trennung	Segmentierung, Härtung und Rechtekonzept selbst umsetzen und pflegen	Oracle trennt die Infrastruktur; Segmentierung der VMs und Netze, Härtung und Rechtekonzept beim Kunden	Eigene VM-Cluster pro Kunde und Umgebung, Produktion getrennt von Test und Entwicklung; Netzwerk-Segregation; kein direkter OS-Zugriff und damit kleinere Angriffsfläche
2. Verschlüsselung	Transparent Data Encryption (TDE) je nach Lizenz; Schlüsselverwaltung selbst organisieren	TDE standardmässig aktiv; Betrieb der Schlüsselverwaltung beim Kunden	TDE durchgängig, im License-Included-Modell enthalten; die Schlüssel bleiben beim Kunden
3. Kontrollierter Herstellerzugriff	Zugriffe von Herstellern und Dienstleistern selbst regeln, protokollieren und prüfen	Oracle betreut Hardware und Hypervisor im Kunden-Rechenzentrum; Regelung und Kontrolle der Zugänge beim Kunden	Oracle betreut nur Hardware und Hypervisor, ohne Zugriff auf Kunden-VMs; der Oracle-Zugang ist auditierbar, von T-Systems kontrolliert und im Notfall trennbar
4. Backup, das im Ernstfall funktioniert	Eigene Backup-Infrastruktur beschaffen, Unveränderbarkeit sicherstellen, Restore-Tests durchführen	Backup-Lösung wählen und betreiben, Recovery Appliance optional und separat; Unveränderbarkeit und Tests selbst sicherstellen	Zero Data Loss Recovery Appliance (ZDLRA): unveränderbare Backups, geschützt vor Manipulation und Löschung; Validierung bei Empfang und Erstellung; Wiederherstellung auf definierte Zeitpunkte
5. Zwei Standorte	Zweiten Standort betreiben, Replikation einrichten, Umschaltung üben	Zweites ExaCC am zweiten Standort, Data Guard einrichten und betreiben, Umschaltung üben	ZDLRA redundant und synchronisiert in Zollikofen und Bern, Datenbanken mit Data Guard gespiegelt; Disaster Recovery ab SLA-Stufe Advanced

Wann welcher Weg passt

Weg	Passt, wenn …
Eigenbetrieb klassisch	die Hardware frisch erneuert ist, ein grosses und stabiles Datenbankteam vorhanden ist und der Betrieb bewusst als Kernkompetenz verstanden wird
Eigenbetrieb mit ExaCC	moderne Exadata-Technik gewünscht ist, die Umgebung gross ist und die Organisation Rechenzentrum und Datenbankbetrieb bewusst selbst tragen will
Managed Oracle Database Cloud (T-Systems)	ein Refresh ansteht, Personal knapp oder an wenige Köpfe gebunden ist, grosse Einmalinvestitionen vermieden werden sollen, hohe Anforderungen an Sicherheit und Verfügbarkeit ohne eigenen zweiten Standort bestehen oder eine gewachsene Landschaft konsolidiert werden soll

Die Übersicht dient der grundsätzlichen Einordnung der drei Betriebsmodelle. Der konkrete Leistungsumfang, die Zuständigkeiten sowie die zugesicherten Service Levels sind im Einzelfall anhand der vereinbarten Leistungen, Vertragsunterlagen und SLA zu prüfen.

November 2026