



Geschäftsdokument

Vg-26-002 PostgreSQL Datenbankservices: Leistungsbeschreibung

Version 1.0

Stand: 26.05.2026

Klassifizierung

Geheimchutz: ☐ VS-NfD

Verteiler: ☐ BDBOS ☐ AS

Inhaltsverzeichnis

1	Ziel und Gegenstand der Ausschreibung.....	4
2	Ausgangssituation und Systemanforderungen	4
2.1	IT-Umgebungen	4
2.2	CPU-Architecture	4
2.3	Betriebssysteme.....	4
2.4	Integration ins Monitoring-System	5
2.5	Containerisierung.....	5
3	Leistungsumfang	5
3.1	Software Delivery.....	5
3.2	PostgreSQL-Datenbanksystem.....	5
3.2.1	Timescale-DB.....	6
3.2.2	Tools für Administration der Datenbank	6
3.2.3	Tool für Performance, Diagnose und Queries	6
3.2.4	Tool für Hochverfügbarkeit.....	6
3.2.5	Tools für Backup, Wiederherstellung und Disaster Recovery	6
3.2.6	Weitere Tools.....	7
3.3	Supportleistungen.....	7
3.3.1	Incident-Management	7
3.3.2	Service Level Agreements (SLA).....	8
3.4	Unterstützungsleistungen.....	10
3.5	Personalverfügbarkeit und Qualifikation.....	10
3.5.1	Verfügbarkeit von Contributor-Kompetenz im PostgreSQL-Umfeld	10
3.5.2	Verfügbarkeit von Support-Personal	10
3.5.3	Verfügbarkeit von Dienstleistungs- und Beratungspersonal	10
3.5.4	Organisatorische Sicherstellung.....	10
3.5.5	Nachweisführung (§ 46 VgV)	10
4	Rahmenbedingungen	10
4.1	Kommunikationssprache	10
4.2	Vertraulichkeit	11
4.3	Eingangstore / Kommunikationswege	11
5	Bereitstellung	11
5.1	Release-Management / Aktualität.....	11
5.1.1	Standard-Releases.....	11
5.1.2	Sicherheitspatches	11
5.1.3	Release-Notes, Release-Dokumentation	12
5.2	BSI IT Grundschutz	12
5.3	Geografische Speicherung	12
5.4	Sichere Speicherung / Verarbeitung der Daten.....	12
5.5	Schwachstellenanalyse	13
5.6	Regression-Tests	13

5.7	Repository	13
-----	------------------	----

1 Ziel und Gegenstand der Ausschreibung

Die ALDB GmbH (im Weiteren ALDB genannt) beabsichtigt, einen zuverlässigen, sicheren, skalierbaren und wartbaren PostgreSQL-Stack aufzubauen und diesen zu betreiben. Dieser umfasst das relationale Datenbankmanagementsystem (RDBMS) einschließlich Erweiterungen und Tools, welche für erweiterte Hochverfügbarkeitsanforderung und die Administration notwendig sind.

Ziel und Gegenstand dieser Ausschreibung ist der Abschluss eines Vertrages mit einem Unternehmen, zur Bereitstellung eines PostgreSQL Stacks (Open Source) inkl. Erweiterungen/Tools, sowie zur Erbringung eines ganzheitlichen Datenbank Supports (1st–3rd Level) inkl. 24/7 Rufbereitschaft. Der Leistungsumfang umfasst u. a. Software Delivery inkl. Updates/Sicherheitspatches, Unterstützung beim Aufbau und Betrieb einer (geo-)hochverfügbaren Umgebung, Monitoring Integration sowie definierte Prozesse für Incident Management und SLAs. Die Lösung muss für RHEL, sowie den Betrieb auf x86_64 geeignet sein und Sicherheits- und Qualitätsanforderungen nach BSI IT Grundschutz (u. a. Schwachstellenmanagement, Regressionstests, sichere Repository Bereitstellung) erfüllen.

2 Ausgangsituation und Systemanforderungen

2.1 IT-Umgebungen

Der Auftraggeber betreibt eine nicht-produktive Umgebung, welche aus einer Testumgebung und einer Referenz-Umgebung besteht und eine produktive Umgebung, welche eine vollständige Geo-Redundanz besitzt.

Das DBMS wird auf allen 3 Systemen installiert werden. Vor einem Rollout auf die Produktiv-Umgebung wird die Funktionalität in der Test- und Referenz-Umgebung durch den Auftraggeber geprüft.

2.2 CPU-Architecture

Die Postgres-Datenbank und die im Kapitel 3.2.2, 3.2.3, 3.2.4, 3.2.5 und 3.2.6 beschriebenen Tools sollen auf einer IT-Plattform mit X86 (64bit) und IBM Power (momentan Power 9, aktuell in Migration auf Power 11) betrieben werden.

2.3 Betriebssysteme

Als Betriebssystem wird Red Hat Enterprise Linux (RHEL) eingesetzt (momentan Migration von Rel. 8 auf 9, Rel 10 in Planung).

Die zu liefernden Installationspakete müssen deshalb für diese Plattform ausgelegt sein.

2.4 Integration ins Monitoring-System

Der Auftraggeber nutzt Icinga und Zabbix als zentrale Anwendung zur System- und Netzwerküberwachung. Sämtliche installierte Tools und Prozesse sollen in dieses System integriert werden.

Vom Auftragnehmer sind deshalb diverse Konnektoren und APIs zu berücksichtigen bzw. bereitzustellen, um die nachfolgend beschriebenen Tools und Prozesse in dieses System zu integrieren.

2.5 Containerisierung

Es ist seitens des Auftraggebers mittelfristig geplant, eine containerisierte Umgebung zu etablieren. Deshalb soll es auch möglich sein, die entsprechende Software auf die im Enterprise-Umfeld verbreiteten Containerisierungs-Lösungen einzusetzen.

3 Leistungsumfang

3.1 Software Delivery

Der Auftragnehmer stellt dem Auftraggeber die Softwarekomponenten für PostgreSQL-RDBMS bereit, einschließlich der in diesem Kapitel beschriebenen Erweiterungen und Tools, die für den Aufbau, Betrieb, Sicherheit und Verfügbarkeit einer georedundanten Hochverfügbarkeitslösung notwendig sind.

Die Software-Delivery beinhaltet auch die Software-Aktualisierungen (Patch- und Release-Management, siehe auch Kapitel 5).

Vor jeder Software-Auslieferung ist vom Auftragnehmer eine Schwachstellenanalyse vorzunehmen (siehe Kapitel 5.5) sowie Regression-Tests durchzuführen (siehe Kapitel 4.9).

Der Auftraggeber folgt der allgemeinen Empfehlung der „Digitalen Souveränität“ und hat deshalb das Ziel, nach Möglichkeit Open-Source-Software einzusetzen.

Die nachfolgend beschriebenen Erweiterungen / Tools müssen vom Auftragnehmer geliefert werden und müssen mindestens folgende Funktionsbereiche abdecken.

3.2 PostgreSQL-Datenbanksystem

Es sollen Postgres-DBS als Primary und auch als Replikas in einer produktiven Umgebung und nicht produktiven Umgebungen errichtet werden.

3.2.1 Timescale-DB

Da der Auftraggeber auch zeitreihenbasierte Daten speichern und verarbeiten möchte, muss TimeScale-DB / Tiger Data mitgeliefert werden.

3.2.2 Tools für Administration der Datenbank

Nachfolgende Tools sollen für die Verwaltung der Datenbank genutzt werden, wie z.B.

- Datenbanken / Tabellen / Views verwalten
- SQL schreiben und ausführen
- Benutzer & Rechte managen
- Monitoring / Alarming (Sessions, Locks, basic Performance)
 - relevanter Metriken
 - geeigneter Dashboards/Views Alarmierungslogik (Schwellwerte/Eskalationen werden im Betriebskonzept konkretisiert)

- grafische Bedienoberfläche

Beispielsweise „pgAdmin“ oder gleichwertig.

3.2.3 Tool für Performance, Diagnose und Queries

- Erweiterungen und Tools zur Analyse von Workloads und Queries sowie zur Unterstützung von Tuning-Maßnahmen
- Bevorzugtes Tool: pg_qualstats (oder funktional gleichwertig)

3.2.4 Tool für Hochverfügbarkeit

- Komponenten und Tools für:
- lokale Redundanz (z. B. innerhalb eines RZ)
- geografische Redundanz (z. B. zweites RZ)
- Replikation, Clusterbetrieb, Failover
- inkl. Unterstützung eines Failover-Betriebskonzepts (technische Umsetzbarkeit durch die gelieferten Komponenten)

Beispielsweise „Patroni“ oder gleichwertig

3.2.5 Tools für Backup, Wiederherstellung und Disaster Recovery

- Werkzeuge und Komponenten zur Sicherung und Wiederherstellung inkl.:
 - definierbarer Retention
 - inkrementeller Backups

- WAL-Archivierung
- Point-in-Time-Recovery
- dokumentierter Wiederherstellungsprozeduren
- Unterstützung von Disaster Recovery-Szenarien (z. B. Wiederanlauf in Ausweichumgebung)

Beispielsweise: pgBackRest oder gleichwertig

3.2.6 Weitere Tools

Der Auftragnehmer soll auch weitere Tools und Erweiterungen entsprechend des in den folgenden Kapiteln beschriebenen Lieferweges bereitzustellen.

- Load Balancer/ connection pooling, z.B. HA-Proxy Pg Bouncer
- Post-GIS
- AI-Extensions

Des Weiteren kann der Auftragnehmer Empfehlungen für weitere Erweiterungen und Umsysteme abgeben, die er für einen sicheren und zuverlässigen Betrieb für sinnvoll erachtet.

3.3 Supportleistungen

Der Auftragnehmer erbringt im Rahmen einer jährlichen Pauschale Leistungen im Rahmen des Incident Managements gemäß ITIL, insbesondere die strukturierte Analyse, Qualifizierung, Priorisierung und Behebung von Incidents zur schnellstmöglichen Wiederherstellung innerhalb des vereinbarten Servicelevels. Der Auftragnehmer erbringt Support für alle unter Kapitel 3.2 bereitgestellten Komponenten.

3.3.1 Incident-Management

Der Auftragnehmer verfügt für die in diesem Dokument beschriebenen Lieferleistungen über ein umfassendes Incident-Management, sowohl auf technischer als auch auf organisatorisch/prozessualer Ebene.

Das Incident-Management-System sollte sich an den ITIL V4 beschriebenen Practices orientieren

Dieses System muss folgendes abdecken können:

- Fehleranalyse und Fehlerbehebung inkl. strukturierter Root-Cause-Analyse entsprechend in den folgenden Kapiteln beschriebenen SLAs und Rahmenbedingungen
- Unterstützung bei Disaster-Recovery-Ereignissen (Restore, Wiederanlauf, Datenkonsistenz)
- Zeitnahe Bereitstellung von Patches bei betriebskritischen Fehlern z.B. Hotfix/Workaround/Backport, abhängig vom Schweregrad, siehe Kapitel 5.1.2.

3.3.2 Service Level Agreements (SLA)

3.3.2.1 Supportverfügbarkeit

Der Auftragnehmer muss eine durchgängige Support-Verfügbarkeit von 24 Stunden pro Tag, an 7 Tagen pro Woche (24/7) mit entsprechendem qualifiziertem Personal sicherstellen.

3.3.2.2 Reaktionszeiten / Lösungszeiten

Definition:

*Reaktionszeit (Time to Response)

Die Reaktionszeit ist die Zeitspanne zwischen dem Eingang des Incidents beim Auftragnehmer und einer qualifizierten Rückmeldung durch den Auftragnehmer beim Auftraggeber. Innerhalb dieser Zeit wird aktiv mit der Entstörung durch die Fachexperten des Auftragnehmers begonnen wird und sich durch einen Fachexperte des Auftragnehmers mit dem Auftraggeber Verbindung setzt.

*Lösungszeit (Time to Resolution)

Die Lösungszeit ist die Zeit zwischen dem Eingang des Incidents beim Auftragnehmer und einem qualifizierten Lösungsvorschlag durch den Auftragnehmer beim Auftraggeber.

Innerhalb dieser Zeit müssen vom Auftragnehmer bereitgestellte Indizien (Logs, Konfigs, ...) ausgewertet werden sowie ein Lösungsvorschlag zur Behebung der Störung unterbreitet werden.

Definition der Prioritäten

Mit welcher Priorität ein Incident eingestuft wird, hängt von der Dringlichkeit und den Auswirkungen ab und ist der folgenden Tabelle zu entnehmen:

INCIDENT PRIORITY MATRIX		IMPACT			
		EXTENSIV Betrifft die gesamte Organisation oder kritische Geschäftsprozesse	SIGNIFICANT Betrifft eine Abteilung oder wichtige Services	MODERATE Betrifft wenige Nutzer oder nicht essenzielle Funktionen	LOW Betrifft einen einzelnen Nutzer
URGENCY	CRITICAL Verlust kritischer Daten kritische Systeme betroffen	P1	P1	P2	P2
	HIGH Verlust wichtiger Daten Kernsystem betroffen	P1	P2	P2	P3
	MEDIUM kein Datenverlust Ausfall wird durch Redundanz kompensiert	P2	P3	P3	P3
	LOW kein Datenverlust Einschränkungen im Bedienungskomfort, Bzw. zumutbarer Workaround vorhanden	P3	P4	P4	P4

- je Severity

Priorität	Reaktionszeit*	Lösungszeit*
<i>P1 – kritisch</i>	30 Minuten	2 Stunden
<i>P2 – hoch</i>	2 Stunden	4 Stunden
<i>P3 – mittel</i>	2 Werktage	4 Werktage
<i>P4 – niedrig</i>	3 Werktage	7 Werktage

3.3.2.3 Onsite-Support

Der Auftragnehmer soll auch einen On-Site-Support anbieten. Sollte es erforderlich sein, so muss ein qualifizierter Mitarbeiter innerhalb von 36 Stunden bzw. -abhängig von der Priorität der Störung- am Standort des Auftraggebers in Berlin eintreffen.

3.3.2.4 Eskalationsprozess (technisch/managementseitig)

Der Auftragnehmer verfügt während des Vertragszeitraums über einen Eskalationsprozess.

Der Auftragnehmer stellt bei Angebotsabgabe seinen Eskalationsprozess dar und benennt entsprechend der Eskalationsstufen im Dokument Anforderungskatalog-PostgreSQL.xls, Blatt Eskalationsprozess einen Ansprechpartner.

Die Eskalationsstufen werden wie folgt eingeleitet:

Eskalationsstufe	Auslöser / Trigger
Stufe 1 (Operativ)	Eingang eines Incidents / SLA-Abweichung
Stufe 2 (Erweitert)	Keine Lösung innerhalb SLA / wiederkehrende Störung
Stufe 3 (Management)	Eskalation bei SLA-Verletzung / kritische Betriebsbeeinträchtigung
Stufe 4 (Leitungsebene)	Anhaltender schwerer Verstoß / geschäftskritischer Ausfall

3.4 Unterstützungsleistungen

Der Auftragnehmer unterstützt (Leistung und Vergütung nur bei Abruf) den Auftraggeber bei migrationsbezogenen Maßnahmen, der laufenden Pflege und Wartung der eingesetzten Systeme sowie bei der kontinuierlichen Weiterentwicklung der Betriebsumgebung. Dies schließt Maßnahmen zur Performance Analyse und Optimierung ein, mit dem Ziel, die Stabilität, Verfügbarkeit und Leistungsfähigkeit der Services dauerhaft sicherzustellen.

Der Auftragnehmer unterstützt den Auftraggeber bei der Weiterentwicklung und Optimierung des DBMS, z.B. bei:

- Performance-Analyse und -Tuning (Query- und System-Ebene)
- Regelmäßige Health-Checks inkl. Empfehlungen und Priorisierung
- Migrations-Support, u. a. bei Migrationen von kommerziellen RDBMS (z. B. Oracle nach PostgreSQL)
- Unterstützung bei der Integration weiterer Funktionalitäten (z.B. PostGIS, Artificial Intelligence-Extensions, ...)

3.5 Personalverfügbarkeit und Qualifikation

Der Auftragnehmer erbringt die Leistungen mit dem Personal, das mindestens über die Qualifikationsanforderungen verfügt, die zum Nachweis der Eignung zu „Techniker oder technische Stellen“ im Rahmen der Prüfung der technischen und beruflichen Leistungsfähigkeit angegeben wurden..

Die personelle Leistungsfähigkeit muss insbesondere die folgenden Leistungsbereiche abdecken:

- tiefgehende technische Expertise (Contributor-Leistungen),
- Supportleistungen,
- Dienstleistungen und Beratungsleistungen.

Der Auftragnehmer hat dem Auftraggeber spätestens zwei Wochen vor Beginn der tatsächlichen Leistungserbringung die Namen und die konkreten Qualifikationsnachweisen der tatsächlich eingesetzten Personen vorzulegen. Der Auftraggeber kann den Einsatz von Personen ablehnen, wenn diese das erklärte Qualifikationsniveau unterschreiten. Ein Austausch des Personals erfolgt mit Zustimmung des Auftraggebers.

4 Rahmenbedingungen

4.1 Kommunikationssprache

Die Kommunikation muss generell in deutscher Sprache mind. Sprach Level B erfolgen (remote sowie on Site).

4.2 Vertraulichkeit

Die vom Auftraggeber dem Auftragnehmer zur Fehlernanalyse übergebenen Informationen (Konfigs, Logs, Performance-Daten, ...) sind vertraulich. Der Auftragnehmer muss sicherstellen, dass sowohl seine IT-Umgebung -sowohl in technischer als auch in organisatorischer Hinsicht- sensible Daten verarbeiten kann.

4.3 Eingangstore / Kommunikationswege

Der Auftragnehmer muss für die Übergabe von Tickets bzw. Incidents folgende Eingangstore bereitstellen:

- Telefonische Hotline (24/7)
- E-Mail mit einer Größe des Anhangs von mind. 30 MB

Es ist auch eine Ticketkopplung wünschenswert. Beim Auftraggeber wird momentan das TTS-„Remedy“ eingesetzt. Eine entsprechende Schnittstellenbeschreibung kann vom Auftraggeber zugesendet werden. Details können im Rahmen des Projektes abgesprochen werden.

5 Bereitstellung

5.1 Release-Management / Aktualität

5.1.1 Standard-Releases

Die vom Auftragnehmer zur Verfügung gestellten Versionen der Software-Komponenten sollten möglichst den aktuellen Versionen der Community-Editions entsprechen, mindestens jedoch das Kriterium n-1 erfüllen, wobei n für die neuste Version der Community-Edition steht.

5.1.2 Sicherheitspatches

Der Auftragnehmer muss

1. proaktiv nach bekanntwerdenden Schwachstellen und Sicherheitslücken suchen. (z.B. Sicherheitsmitteilungen vom BSI / Cert-bund.de, durch Medien und IT-Fachportale, Community-Mitteilungen)
2. diese unverzüglich, spätestens innerhalb von 24 Stunden an den Auftraggeber melden
3. gemeinsam mit dem Auftraggeber eine Bewertung dieser Schwachstelle vornehmen
4. abhängig von dem Schadensrisiko sofort entsprechende Gegenmaßnahmen einleiten, (i.d.R. durch Bereitstellung von Security-Patches)

5.1.3 Release-Notes, Release-Dokumentation

Zusätzlich soll je Release bereitgestellt werden:

- Release Notes / Change Log
- CVE-Bezug inkl. kurzer Einordnung (sofern zutreffend)
- Upgrade-Hinweise und Upgrade-Pfade

5.2 BSI IT Grundschutz

Der Auftragnehmer nutzt Tools und Erweiterungen zur Erfüllung von Anforderungen aus BSI IT-Grundschutz, u.a.:

- Auditing / Nachvollziehbarkeit
- Verschlüsselung (Transport und/oder ruhende Daten, gemäß Zielarchitektur der Auftraggeberin)
- Unterstützung bei Härtingsmaßnahmen (z. B. sichere Default-Konfigurationen, Rollen-/Rechtekonzepte)

Vor der Übergabe der Software-Pakete sind alle dafür relevanten Grundschutz-Bausteine anzuwenden, bzw. -sofern notwendig- in Absprache mit dem Auftraggeber daran mitzuwirken vor allem

- OPS.1.1.3 Patch- und Änderungsmanagement
- OPS.1.1.4 Schutz vor Schadprogrammen
- OPS.1.1.5 Protokollierung
- OPS.1.1.6 Software-Tests und -Freigaben
- APP.4.3 Relationale Datenbanksysteme

Ein Audit bzw. Zertifizierung durch das BSI wird hier nicht verlangt.

5.3 Geografische Speicherung

Es muss gewährleistet sein, dass von der Auftraggeberin zum Zwecke einer Fehler-Analyse zur Verfügung gestellte Daten gemäß BSI-Grundschutz in Deutschland oder mindestens nicht außerhalb des Wirtschaftsraumes der Europäischen Union in sogenannten Drittländern gespeichert werden.

5.4 Sichere Speicherung / Verarbeitung der Daten

Die IT-Plattform des Auftragnehmers muss vertrauliche Inhalte verarbeiten und speichern können.

Der Auftragnehmer stellt die Datensicherheit sicher und fügt den Prozess, z. Bsp. mittels technische und organisatorische Maßnahmen diese als Anlage zum Angebot bei.

5.5 Schwachstellenanalyse

Vor der Bereitstellung der Software müssen sämtliche Software-Komponenten vom Auftragnehmer einer Schwachstellenanalyse unterzogen worden sein.

Diese Schwachstellen-Analyse sollte vor allem folgendes beinhalten

1. Identifizierung:

Scannen auf Schad-Software und bekannte Sicherheitslücken im Sinne der geltenden BSI-Grundschutzanforderungen

2. Bewertung & Klassifizierung:

Die gefundenen Schwachstellen werden vom Auftragnehmer analysiert, nach Risiko bewertet (z. B. kritisch, hoch, mittel, niedrig) und deren Auswirkungen auf das Unternehmen eingeschätzt.

3. Maßnahmenplanung

Der Auftragnehmer gibt auf Grundlage der Risiko-Analyse eine Handlungsempfehlung ab, und unterstützt bei der Maßnahmenumsetzung und deren Priorisierung. (Risikomanagement).

5.6 Regression-Tests

Vor der Bereitstellung neuer Software muss sichergestellt werden, dass bestehende Funktionalitäten weiterhin einwandfrei funktionieren und keine neuen Fehler entstanden sind. Dies schließt ebenfalls die Kompatibilität der Software zu den im Kapitel 4.1 dargestellten Tools ein.

Die Funktionalität / Kompatibilität ist durch entsprechende Regression-Tests nachzuweisen und zu dokumentieren sowie dem Auftraggeber zu übergeben.

5.7 Repository

Der Auftragnehmer muss die Software-Komponenten über ein vom Auftragnehmer betriebenes Repository bereitstellen, auf das die Auftraggeberin zum Zwecke des Software-Downloads zugreifen kann.

Ebenso soll es dem Auftraggeber ermöglicht werden, Daten (z.B. Logs, oder Konfigs) für den AB zur Analyse abzulegen. Das Repository ist Bestandteil der IT-Infrastruktur des Auftragnehmers und unterliegt deshalb auch den allgemeinen Anforderungen an die IT-Infrastruktur des Auftragnehmers (siehe Kapitel 5.2)

Anforderungen:

- Zugriff der Auftraggeberin über sichere Verbindung.

Eine Verbindung wird dann vom Auftraggeber als sicher eingestuft, wenn die dafür einschlägigen Empfehlungen des BSI (TR-02102, TR-02116, IT-Grundschutz, ...) umgesetzt werden

- Authentifizierung/Autorisierung für den Repository-Zugriff

Die Authentifizierung muss auch den aktuell gültigen Richtlinien des BSI entsprechen. Eine 2FA wird gefordert.

- Integritätsnachweise für Software-Pakete

Dies können z. B. Signaturen und/oder Checksummen sein