— Audit Report —

PostgreSQL Database n8ndb

Weekly Digest Corp. – July 15, 2026

Global Score: 4.4 / 10

Security	Performance	Integrity
5.0 / 10	4.2 / 10	7.3 / 10

Executive Summary

This audit covers a PostgreSQL 18.1 instance hosting the **n8ndb** database. The overall audit score of **4.4/10** reflects a database that is functionally stable in terms of storage and query load, but carries **significant security and structural integrity gaps** that require prompt remediation.

The most critical finding is that **SSL/TLS encryption is not enforced** (`ssl_enforced = 0`), meaning client-server traffic may travel unencrypted. Combined with the presence of a **superuser role** (`superuser_roles = 1`) and an inability to verify password hygiene on roles (`roles_without_password` returned insufficient privileges on `pg_authid`), the security posture of this instance cannot currently be considered adequate.

On the integrity side, **two tables lack a primary key** (`articles_categories_en` , `ontology`) and **five foreign keys are missing supporting indexes**, which exposes the database to both data consistency risks and cascading performance degradation on delete/update operations. Additionally, **autovacuum is disabled** (`autovacuum_enabled = 0`), a configuration state that, if confirmed at the instance level, will lead to progressive table and index bloat over time even though no bloat is currently detected.

Performance indicators are largely reassuring: no bloated tables, no duplicate indexes, no duplicate primary keys, no long-running transactions, and a healthy connection ratio (**0.17**). One full table scan and one table with a missing index were detected, both currently low in probability/severity but worth monitoring. Query-level visibility remains limited since `slow_queries_count` is unavailable.

In summary, the instance is not at immediate risk of outage, but it is **exposed on security and data-integrity dimensions** that should be addressed before this environment scales further or handles sensitive data.

Top 3 Recommendations

1. Enforce SSL/TLS on all client connections
- Priority: Critical
- Business impact: Prevents interception or tampering of data in transit, protecting sensitive application and user data from network-level exposure.
- Technical rationale: `ssl_enforced = 0` combined with a Probability=4/5, Severity=5/5 (Score: 20) risk rating indicates unencrypted connections are currently permitted. Enable and enforce SSL at the server configuration level, require valid certificates, and reject non-SSL connection attempts for all roles, especially those with elevated privileges.

2. Review and restrict superuser privileges
- Priority: High
- Business impact: Reduces the blast radius of a compromised credential or misconfigured application role, limiting the potential for unauthorized schema or data manipulation.
- Technical rationale: One superuser role was identified (`superuser_roles = 1`), corresponding to a Probability=3/5, Severity=4/5 (Score: 12) risk. Audit the purpose of this role, replace superuser usage with scoped, least-privilege roles wherever possible, and reserve superuser access strictly for administrative maintenance windows.

3. Add primary keys to unprotected tables
- Priority: High
- Business impact: Ensures row-level uniqueness and referential reliability, which is foundational for downstream joins, replication, and application-level data consistency.
- Technical rationale: `articles_categories_en` and `ontology` currently have no primary key, matching a Probability=3/5, Severity=3/5 (Score: 9) risk. Define a suitable primary key (natural or surrogate) for each table, validating existing data for duplicates beforehand to avoid constraint violations during creation.

Risk Matrix

RISK	PROBABILITY	SEVERITY	SCORE
SSL/TLS not enabled (unencrypted connections)	4/5	5/5	20
Excessive privileges (superuser/global)	3/5	4/5	12
Tables without primary key	3/5	3/5	9
Foreign keys without index (cascade performance issue)	3/5	2/5	6
Missing index on hot tables	1/5	3/5	3
Large full-table scans	1/5	3/5	3

Score = Facilité d'exploitation × Gravité (échelle 1 – 25)

Overall Assessment

The **4.4/10** score reflects a database that performs adequately under current load — no bloat, no duplicate objects, a comfortable connection ratio, and no long-running transactions — but that is undermined by **unresolved security exposure and data-integrity gaps**. The absence of enforced SSL/TLS is the single largest contributor to risk exposure, and the confirmed presence of a superuser role compounds this by increasing the potential impact of any credential compromise.

Structural weaknesses — two tables without primary keys and five foreign keys lacking supporting indexes — are secondary but material concerns. These do not yet manifest as active incidents (no bloat, no broken queries reported), but they represent latent risk that will surface as data volume grows or as delete/update cascades increase in frequency.

The **disabled autovacuum setting** deserves attention even though no bloat is currently observed: this metric describes a configuration state, not yet a consequence, and should be corrected proactively rather than after bloat appears. Similarly, visibility gaps — `slow_queries_count` unavailable and `roles_without_password` unverifiable due to privilege restrictions — should be closed by granting the audit role sufficient read access to `pg_authid` and enabling query statistics collection, so that future audits can validate these dimensions with confidence rather than reporting them as unknown.

Overall, remediation should prioritize security controls first (encryption, privilege scope), followed by integrity fixes (primary keys, foreign key indexing), and conclude with configuration hardening (autovacuum, observability).

Metrics Test Summary

METRIC	STATUS	VALUE
autovacuum_enabled	Critical	0
bloated_tables	OK	0
connection_count_ratio	OK	0.17
duplicate_indexes	OK	0
duplicate_primary_keys	OK	0
full_table_scans	Warning	1
large_tables_count	OK	0
long_running_transactions	OK	0
roles_without_password		insufficient privileges on pg_authid
slow_queries_count		Unavailable
ssl_enforced	Critical	0
superuser_roles	Warning	1
tables_missing_indexes	Warning	1
tables_without_pk	Warning	2
unindexed_foreign_keys	Critical	5
unused_indexes	OK	0

Tables without primary key:

- `articles_categories_en`
- `ontology`

Unindexed foreign keys:

- `articles_categories_category_id_fkey`
- `curated_feed_feed_id_fkey`
- `domains_category_id_fkey`
- `kl_segments_article_id_fkey`
- `kl_style_ref_article_id_fkey`

Pascal Cescato — Database and Security Consultant

contact@dbgrade.tech

dbgrade.tech