Member-only story

Postgres Security 101: Special Configuration Considerations (8/8)

Oz · Following
3 min read · Oct 4, 2024

Listen Share More

In this final installment of the Postgres Security 101 series, we'll focus on crucial configuration considerations to enhance your PostgreSQL database's security. These configurations ensure that your database is fortified against potential threats while maintaining performance and integrity. This article serves as a wrap-up, combining practical tips and manual review recommendations for a secure PostgreSQL setup.

8.1 Ensure PostgreSQL Subdirectory Locations Are Outside the Data Cluster

- Place subdirectories outside the main data directory to enhance security and manageability. Please do not forget logical volume is not enough. You must use

Open in app ↗

Medium Search

```
/pg_data
/pg_temp
/pg_log
/pg_wal
```

8.2 Ensure the Backup and Restore Tool, 'pgBackRest', Is Installed and Configured

- Use `pgBackRest` for reliable backup and restore operations. Also, you can read Taking Backups Using pgBackRest on a Replication Server for more detail.

8.3 Ensure Miscellaneous Configuration Settings Are Correct (Manual)

- Manually review and configure any additional settings to ensure comprehensive security.

1. Review Security Policies and Procedures

- Ensure all organizational security policies are up to date.
- Confirm that security policies are consistently enforced across all systems.

2. Check for Default Settings

- Change any default settings, especially those related to security.
- Disable or remove unnecessary default accounts or services.

3. Audit and Logging

- Enable logging for all critical systems and review logs regularly.
- Implement log rotation and retention policies to avoid storage issues and maintain efficient auditing.

4. Review User Accounts and Permissions

- Perform regular audits of user accounts and permissions, adhering to the principle of least privilege.
- Promptly remove inactive or unnecessary accounts.

5. Network Configuration

- Review firewall rules and ACLs to ensure they are up to date.
- Close any open ports and disable unnecessary services to minimize attack vectors.

6. Update and Patch Management

- Ensure all systems and applications are patched regularly and up to date.
- Implement a routine patch management process.

7. Application Security

- Review application configurations to ensure they follow secure coding standards.
- Make sure secure protocols like HTTPS are enforced where applicable.

8. Data Protection

- Encrypt sensitive data both at rest and in transit.

- Regularly test your data backup process and store backups securely.

9. Incident Response

- Regularly update your incident response plan and conduct drills to keep your team prepared for potential security breaches.

10. Physical Security

- Restrict physical access to critical systems and monitor entry points.
- Consider implementing biometric scanners or surveillance to monitor access.

11. Mobile Device Management

- Secure mobile devices accessing company data using device encryption and remote wipe capabilities.
- Ensure regular updates and enforce policies on mobile device usage.

12. Review Cloud Security Settings

- Regularly verify that cloud storage, network, and computing configurations are secure and compliant with your policies.

13. Third-Party and Vendor Management

- Ensure third-party vendors adhere to your security standards.
- Conduct periodic security reviews of their systems and practices.

Conclusion

This concludes the Postgres Security 101 series. By implementing the configurations discussed, such as isolating subdirectories, using `pgBackRest`, and regularly reviewing security policies and settings, you are taking significant steps toward safeguarding your PostgreSQL environment. Maintaining security is an ongoing process, but these best practices provide a solid foundation to keep your system safe from evolving threats. For more detailed and technical articles like this, keep following our blog on Medium. If you have any questions or need further assistance, feel free to reach out in the comments below and directly.

Database Security Postgres Security Security Cybersecurity Technology

Following

Written by Oz

149 Followers · 13 Following

Database Administrator 🐘

No responses yet

Gvadakte

What are your thoughts?

More from Oz

Queries

time	Service	username	Query	Execution_time
2024-09-26 13:15:00	pmm-server-postgresql	pmm-ma...	SELECT /* agent='pgstatstatements' */ "pg_stat_statements"."userid", "pg_stat_statements"."dbid", "pg_stat_statements"."queryi...	0.0242
2024-09-26 13:19:00	pmm-server-postgresql	pmm-ma...	SELECT current_database() datname, schemaname, relname, heap_blks_read, heap_blks_hit, idx_blks_read, idx_blks_hit, toast_b...	0.0165
2024-09-26 13:10:48	pmm-server-postgresql	pmm-ma...	SELECT * FROM pg_stat_database_conflicts	0.0159
2024-09-26 13:18:00	pmm-server-postgresql	pmm-ma...	SELECT /* agent='pgstatstatements' */ "pg_stat_statements"."userid", "pg_stat_statements"."dbid", "pg_stat_statements"."queryi...	0.0131
2024-09-26 13:19:00	pmm-server-postgresql	pmm-ma...	SELECT /* agent='pgstatstatements' */ "pg_stat_statements"."userid", "pg_stat_statements"."dbid", "pg_stat_statements"."queryi...	0.0131
2024-09-26 13:12:00	pmm-server-postgresql	pmm-ma...	SELECT /* agent='pgstatstatements' */ "pg_stat_statements"."userid", "pg_stat_statements"."dbid", "pg_stat_statements"."queryi...	0.0126
2024-09-26 13:15:00	pmm-server-postgresql	pmm-ma...	SELECT current_database() datname, schemaname, relname, heap_blks_read, heap_blks_hit, idx_blks_read, idx_blks_hit, toast_b...	0.0113

1 2 3 4 5 6 7 ... 77

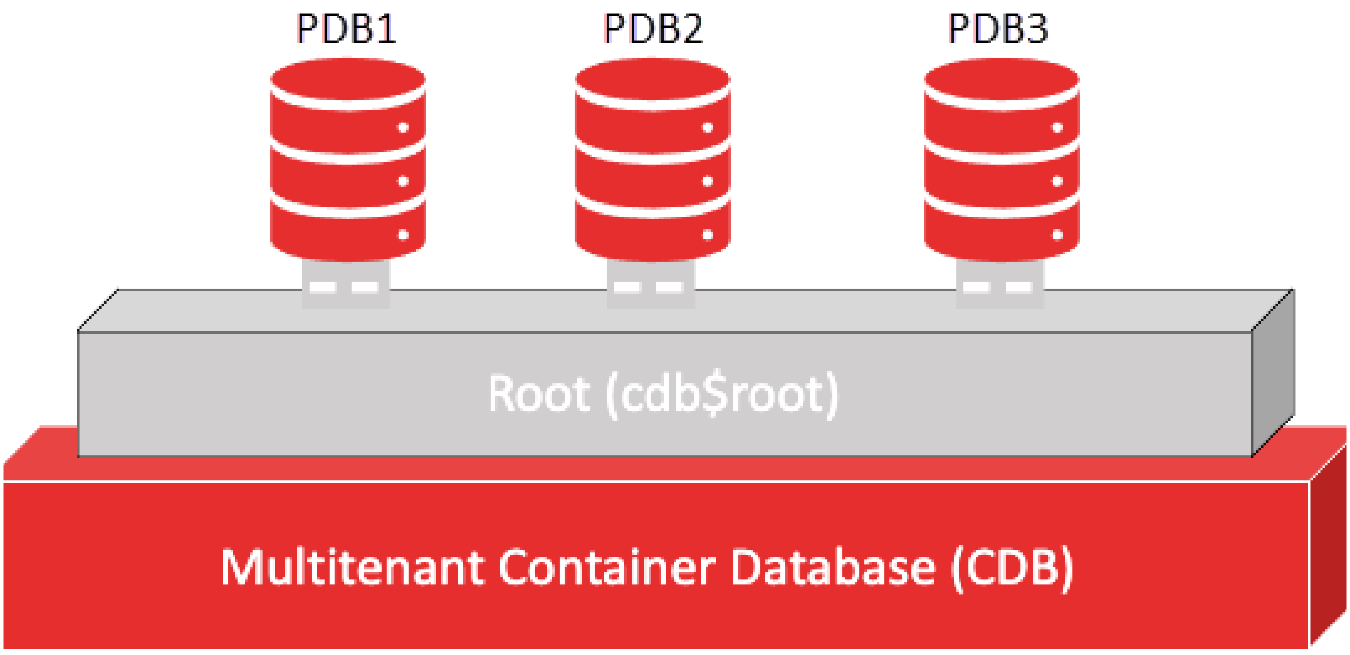
1 - 7 of 538 rows

Oz

Installing Percona Monitoring & Management (PMM) with Postgres

Introduction:

Sep 26, 2024 54 1

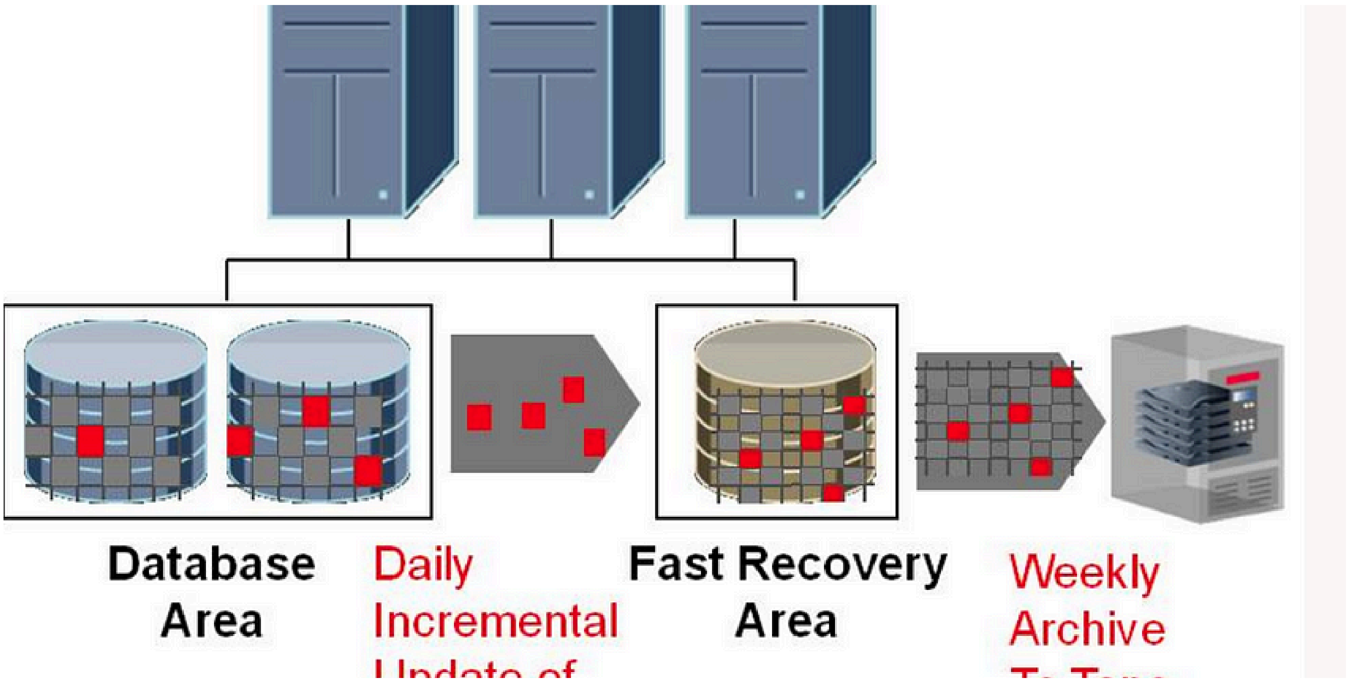


Oz

Pluggable Database Command

—————————— -————————————— - create pluggable database pdb1 admin user root identified by test123; alter pluggable database...

May 12, 2023



Oz

RMAN Backup Basic Commands

rman target / rman target sys/password@YDKTST; backup database; backup database format '/backup/path/%d_%t_%s.rman'; backup tablespace...

May 11, 2023 1

Oz

delete jobs

May 8, 2023

See all from Oz

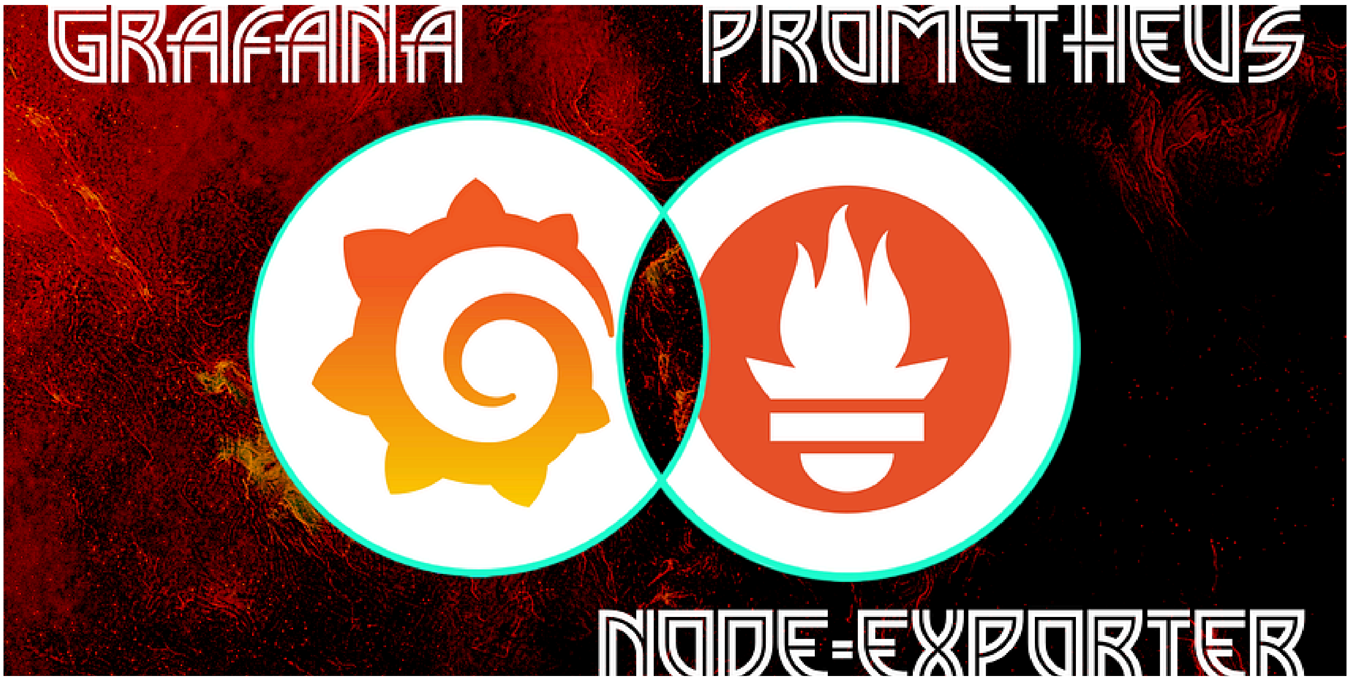
Recommended from Medium

Tihomir Manushev

Vector Search with pgvector in PostgreSQL

Simple AI-powered similarity search

Mar 9

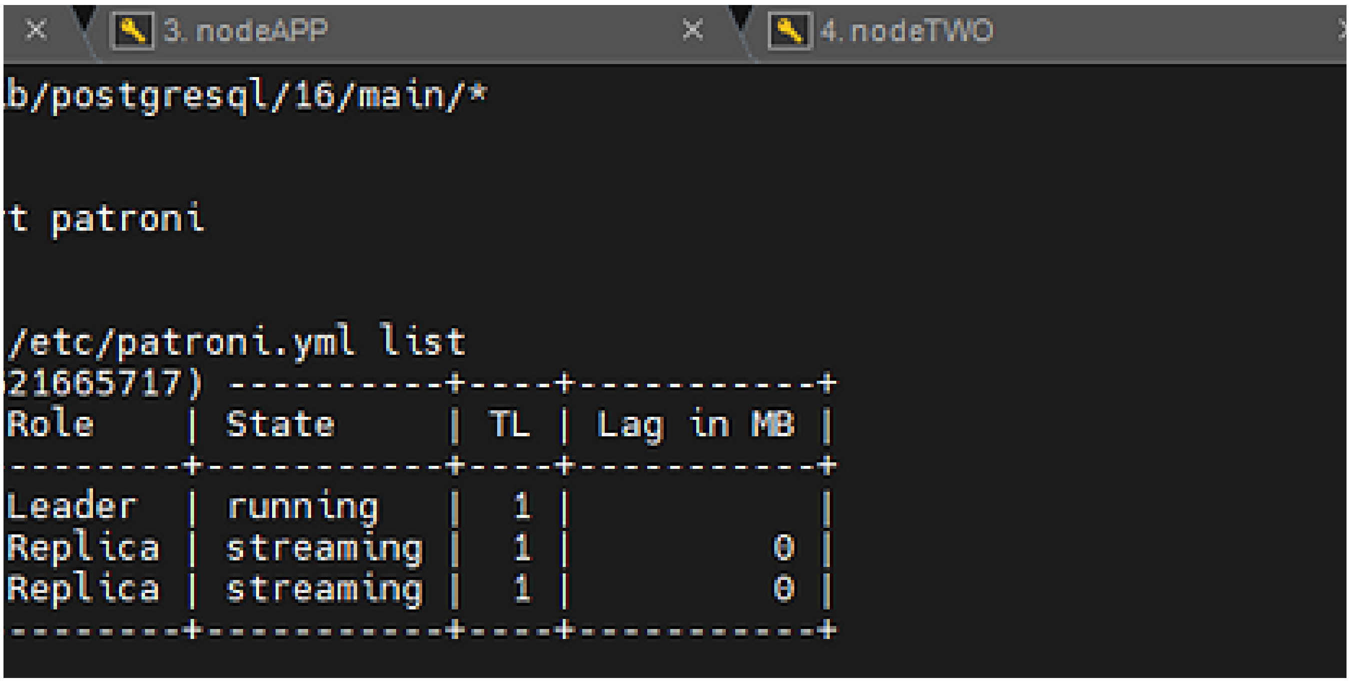


crptcpchk

Grafana, Prometheus & Node-Exporter | Setup Guide

Grafana open source software enables you to query, visualize, alert on, and explore your metrics, logs, and traces wherever they are stored…

Oct 30, 2024 8 1



```
b/postgresql/16/main/*


t patroni


/etc/patroni.yml list
21665717) ----------+----+-----------+
Role     | State     | TL | Lag in MB |
--------+-----------+----+-----------+
Leader  | running   |  1 |           |
Replica | streaming |  1 |         0 |
Replica | streaming |  1 |         0 |
--------+-----------+----+-----------+
```

Dickson Gathima

Building a Highly Available PostgreSQL Cluster with Patroni, etcd, and HAProxy

Achieving high availability in PostgreSQL requires the right combination of tools and architecture.

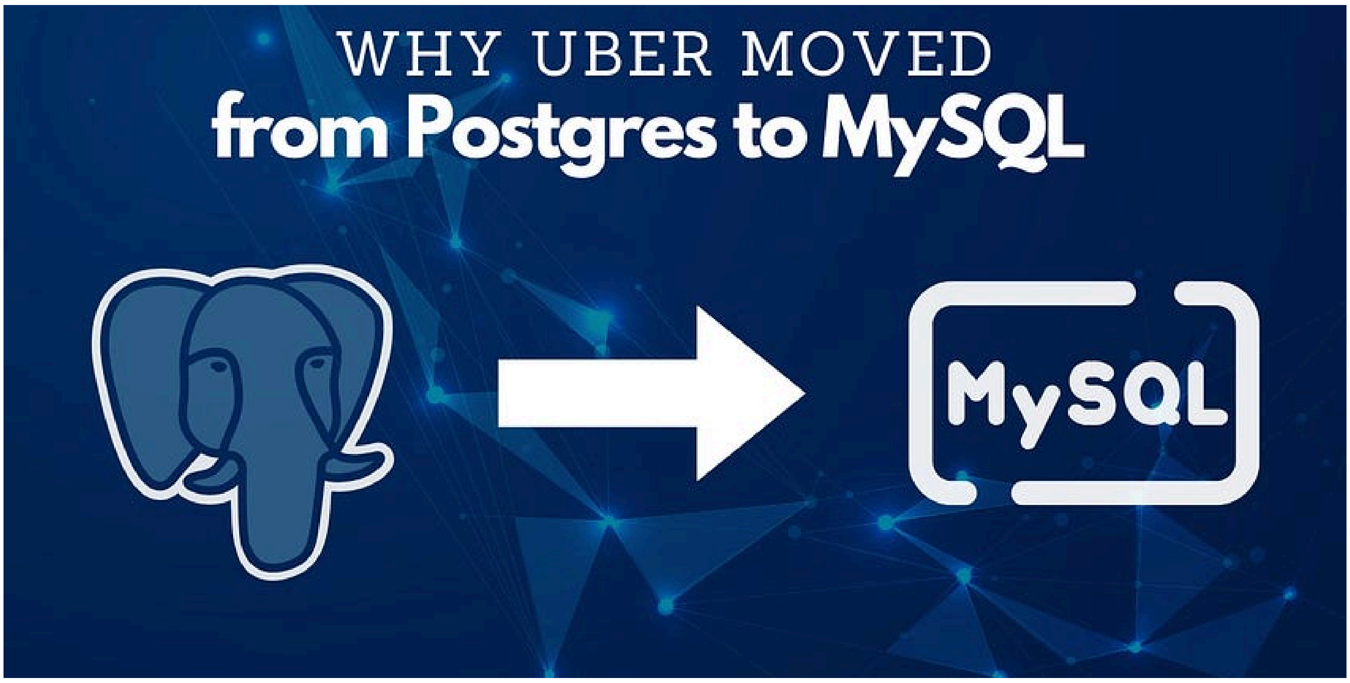
Mar 14 4

In Towards Dev by Nakul Mitra

PostgreSQL Performance Optimization — Cleaning Dead Tuples & Reindexing

Performance optimization is crucial in PostgreSQL to ensure efficient query execution and minimal resource consumption.

Mar 28 1

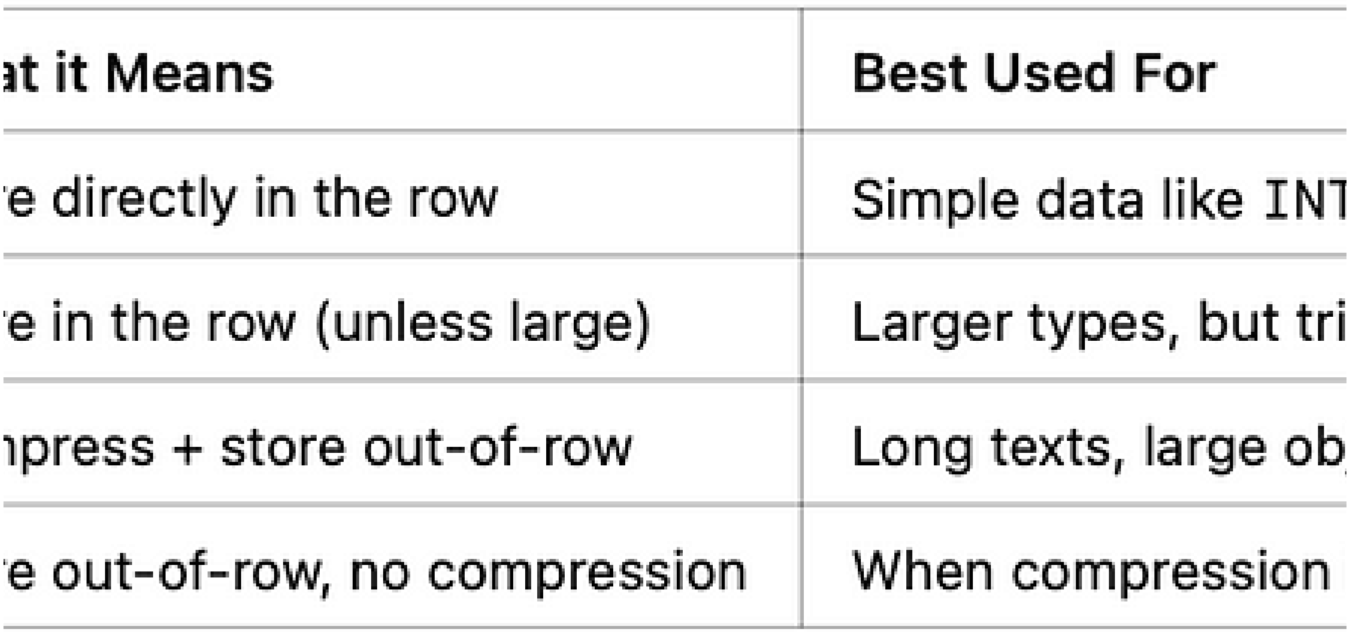


In Databases by Sergey Egorenkov

Why Uber Moved from Postgres to MySQL

How PostgreSQL's architecture clashed with Uber's scale — and why MySQL offered a better path forward

Mar 29 228 7



ıt it Means	Best Used For
·e directly in the row	Simple data like INT
·e in the row (unless large)	Larger types, but tri
ıpress + store out-of-row	Long texts, large ob
·e out-of-row, no compression	When compression

Udbhav Singh

Storages in PostgreSQL

What Are Storage Types in PostgreSQL — And Why Should You Care?

6d ago 18

See more recommendations