PostgreSQL Security Best Practices

—

Whitepaper

2ndQuadrant®
PostgreSQL

© 2019 2ndQuadrant

PostgreSQL Security Best Practices

Introduction

The following practices are well proven in the field. We present them as an introduction into the minimum concepts that are needed for any system. This is not an exhaustive list. It is provided as a compilation of field experience related to security, and avoids the most common pitfalls of security configuration.

- Keep your system updated to the latest minor version. The PGDG provides interim security patches as part of the minor release cycle.
- Do not expose PostgreSQL directly to the general internet on a public port.
- Disallow superuser login from ipv4 connections.
- Confine access to the configuration files for PostgreSQL to the system root user. (most distributions do this anyway, so don't circumvent it.)
- SCRAM
- Certificates

Contents

Copyright © 2019, 2ndQuadrant Limited. Copyright in these materials belongs to 2ndQuadrant Limited and no permissions or licences in relation to these materials are granted. No part of these materials may be reproduced in any form, stored in a retrieval system or transmitted in any way or by any means without the written permission of 2ndQuadrant Limited.

Connecting Securely

libPQ is a library that is provided by the PostgreSQL Global Development Group (PGDG). This library provides secure authentication methods and implements the communications protocol for PostgreSQL. Many different application development platforms provide wrappers around this library to provide secure communications to PostgreSQL.

Language	Library
Python	psycopg2

Stay on the top of PostgreSQL database security best practices and **download the free whitepaper**