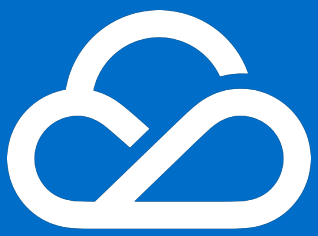
腾讯云数据库PostgreSQL

安全管理

产品文档



腾讯云

【版权声明】

【商标声明】

【服务声明】

本文档意在向客户介绍腾讯云全部或部分产品、服务的当时的整体概况，部分产品、服务的内容可能有所调整。您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定，除非双方另有约定，否则，腾讯云对本文档内容不做任何明示或模式的承诺或保证。

文档目录

信息安全说明

特对本文做如下声明

1. 本文档意在向客户介绍腾讯云对于PostgreSQL产品、服务的安全概况，部分产品、服务的内容可能有所调整。如您对此有强制要求，建议您与腾讯云以书面商业合同（SLA）进行约定。否则，腾讯云对本文档内容不做任何明示或模式的承诺或保证；
2. 安全特性范围较广，本文仅涉及“部分”技术安全要点；
3. 本文档不作为国家或行业信息安全相关标准、要求参考文档；
4. 本文经过可阅读性加工，加之笔者能力有限，若存在描述不准确的地方请参考第1点。
5. 文档解释权归腾讯云所有。

1、概述

腾讯云PostgreSQL通过下列认证并符合下列认证的安全要求

- ISO22301认证
- ISO27001认证
- ISO20000认证
- ISO9001认证
- 可信云服务认证
- 信息安全等级保护（三级）
- STAR认证

PostgreSQL部分功能设计也参考：

- GBT 20273-2006 信息安全技术 数据库管理系统安全技术要求（二级以上）
- JRT 0072-2012 金融行业信息系统信息安全等级保护测评指南（四级）

2、腾讯云PostgreSQL服务安全保障（运维安全说明）

2.1 综述

PostgreSQL的管理安全与技术安全要求符合国家信息安全等级保护（三级），部分要求达到金融行业信息安全（四级）标准。

2.2 内部人员、系统身份鉴别

为提高数据库主机系统安全性，保障各种运维的安全性，腾讯云进行一系列的加固措施，包括但不限于：

- 对登录操作系统和数据库系统的用户进行身份标识和鉴别，且保证用户名的唯一性；
- 根据基本要求配置用户名/口令；口令必须具备采用3种以上字符、长度不少于8位并定期更换；
- 启用登陆失败处理功能，登陆失败后采取结束会话、限制非法登录次数和自动退出等措施。
- 远程管理时通过腾讯企业IT监控下的访问方式，提供内部风控审计，敏感操作均进行加密。
- 对数据库主机管理员登录运维系统进行双因素认证方式，即采用动态令牌+密码进行身份鉴别

2.3 内部人员、系统访问控制

腾讯云云数据库管理系统和管理人员提供自主访问控制方案，包括但不限于：

- 内部运维人员和系统全部基于腾讯云安全策略进行控制（满足审核要求）；
- 主体的粒度为用户级，客体的粒度精确到数据库表级；
- 提供严格的代码管理和访问控制。
- 高危系统仅腾讯内网（开发网）可访问；与互联网严格物理隔离。

2.4 内部安全审计

提供全面的安全审计和风控机制：审计功能包括但不限于数据库操作审计、管理系统操作审计、文件操作审计、外挂设备操作审计、非法外联审计、IP地址更改审计、服务与进程审计等。审计范围覆盖到服务器上的每个操作系统用户和数据库用户；例如包括：腾讯云管理员行为、系统资源的异常使用和重要系统命令的使用等系统内重要的安全相关事件；审计记录包括事件的日期、时间、类型、主体标识、客体标识和结果等；审计记录保存1年以上，且存储在安全等级更高的位置，避免受到未预期的删除、修改或覆盖等。

- 数据库安全审计：对数据库主机和数据库所有操作，均经过数据库安全审计系统。[暂未提供，敬请期待]
- 管理系统操作审计：腾讯云对内外管理系统的操作均记录详细操作日志，以便于风险追溯。
- 定期风险评估：腾讯云安全团队定期对数据库运维管理进行安全评估。

2.5 内部入侵防范

针对数据库主机的入侵防范，腾讯云已经从多个角度进行处理：

- 入侵检测系统可以起到防范针对数据库主机的入侵行为；
- 部署漏洞扫描并定期进行系统安全性检测；
- 部署终端安全管理系统，开启补丁分发功能模块及时进行系统补丁升级；
- 操作系统的安装遵循最小安装的原则，仅安装需要的组件和应用程序，关闭多余服务等；
- 另外根据系统类型进行其它安全配置的加固处理。

2.6 备份与恢复

腾讯云数据库默认提供数据的备份与恢复功能。

2.7 客体安全重用

若客户退还设备或故障更换设备，腾讯云将及时清除剩余信息，从而保证用户的鉴别信息、文件、目录、数据库记录等敏感信息所在的存储空间（内存、硬盘）被及时释放或再分配给其他用户前得到完全清除。

2.8 抗抵赖

腾讯云内部运维人员登录系统，均通过双因素认证和抗抵赖方案，相关人员均签订了保密协议。

2.9 更多安全

更多详细描述，敬请期待笔者更新。