平凯数据库安全白皮书

平凯星辰

20230713

目录

1 平凯数据库安全白皮书（企业版）

1.1 法律声明

平凯星辰提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过平凯星辰网站其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为平凯星辰的保密信息，您应当严格遵守保密义务；未经平凯星辰事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。
2. 未经平凯星辰事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。
3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。平凯星辰保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在平凯星辰授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过平凯星辰网站或平凯星辰授权渠道下载、获取最新版的用户文档。
4. 本文档仅作为用户使用平凯星辰产品及服务的参考性指引，平凯星辰以产品及服务的“现状”、“有缺陷”和“当前功能”的状态提供本文档。平凯星辰在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但平凯星辰在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证，本文档所引用的性能数据和程序示例仅用于说明目的，实际的性能结果可能因特定配置和操作条件而异。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，平凯星辰不承担任何法律责任。在任何情况下，平凯星辰均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使平凯星辰已被告知该等损失的可能性）。
5. 本文档中及平凯星辰网站上所有内容，包括但不限于作品、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计等，均由平凯星辰和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经平凯星辰和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表平凯星辰网站、产品程序或包括本文档在内的内容。此外，未经平凯星辰事先书面同意，任何人不得以任何目的使用平凯星辰商标（包括但不限于单独为或以组合形式包含“平凯星辰”等平凯星辰和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别平凯星辰和/或其关联公司）。
6. 平凯星辰可能拥有涵盖本文档中描述的主题的专利或者专利申请，未经平凯星辰事先书面许可，本文档并不授予您关于这些专利或专利申请的任何许可。
7. 本文档中如有关于平凯星辰未来方向或意图的声明，仅表示目标或者目的，如有更改或撤销，恕不另行通知。
8. 如若发现本文档存在任何错误，请与平凯星辰取得直接联系。平凯星辰可能会以它认为合适的任何方式使用或分发您提供的任何信息，而无需对您承担任何义务。

1.2 平凯数据库安全性简介

本手册介绍了平凯数据库产品的安全功能。

平凯数据库是一款定位于在线事务处理与在线分析处理（HTAP）的融合型分布式数据库产品，因此安全功能是平凯数据库产品的关键能力和核心价值。本手册从数据库安全风险分析到平凯数据库安全功能设计，再到平凯数据库的软件升级和漏洞管理，详细地描述了平凯数据库的安全功能。

本手册的读者包括并不局限于以下人员：

- 数据库管理员
- 运维工程师

1.3 数据库安全风险分析

在数字化、信息化时代，数据作为个人或公司的重要资产，数据的安全性变得越来越重要。因此对于数据库而言，其安全能力也是产品的核心价值所在。

通过分析数据库所面临的安全风险，可以更深入理解数据库的安全能力，数据库安全能力面临的主要安全风险：

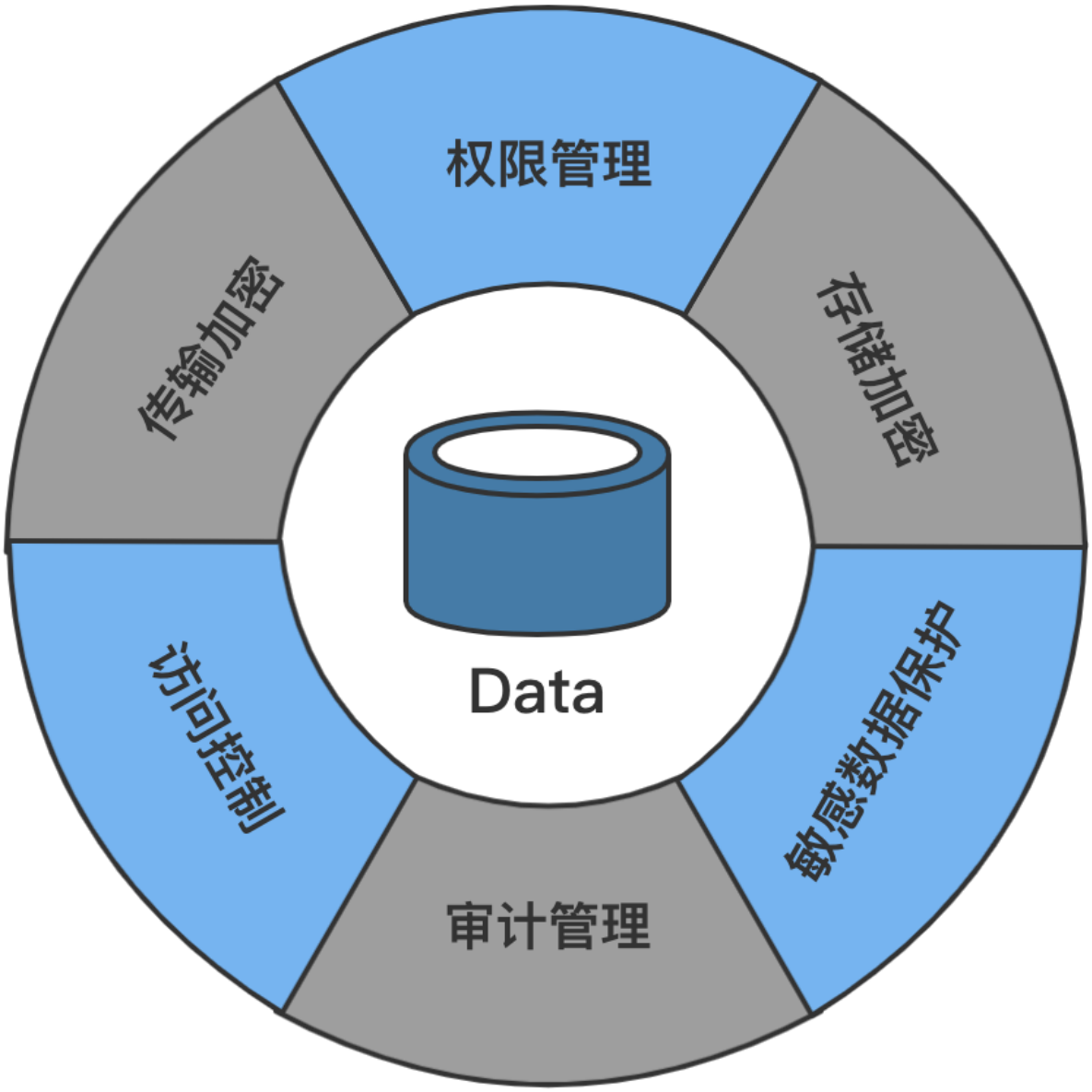

图 1: Data Risks

- 访问控制机制：数据库不支持对账户访问的合理控制，如：不能支持 IP 白名单控制，不能支持账户密码的管理。
- 传输加密机制：数据库不支持对认证证书和传输加密的合理管理。如：不支持证书过期告警，不支持数据库客户端与服务端的传输进行加密。
- 权限管理机制：数据库不支持对账户进行合理的权限管理，如：不能满足账户权限最小化原则。
- 存储加密机制：数据库不支持对静态数据进行加密，如：不支持对存储数据进行加密，不支持对备份数据进行加密。
- 敏感数据保护机制：数据库不支持对敏感数据进行合理保护，如：不支持对各类日志中对敏感数据进行脱敏处理。

- 审计管理机制：数据库缺乏完善的审计机制，如：存在审计遗漏场景和审计可被绕过场景。

1.4 平凯数据库安全功能介绍

基于数据库面临的各类安全风险，平凯数据库通过多层立体的安全功能设计保证了产品的安全性和可靠性，平凯数据库的安全功能主要包括：访问控制、传输加密、权限管理、存储加密、脱敏数据保护、审计管理等。

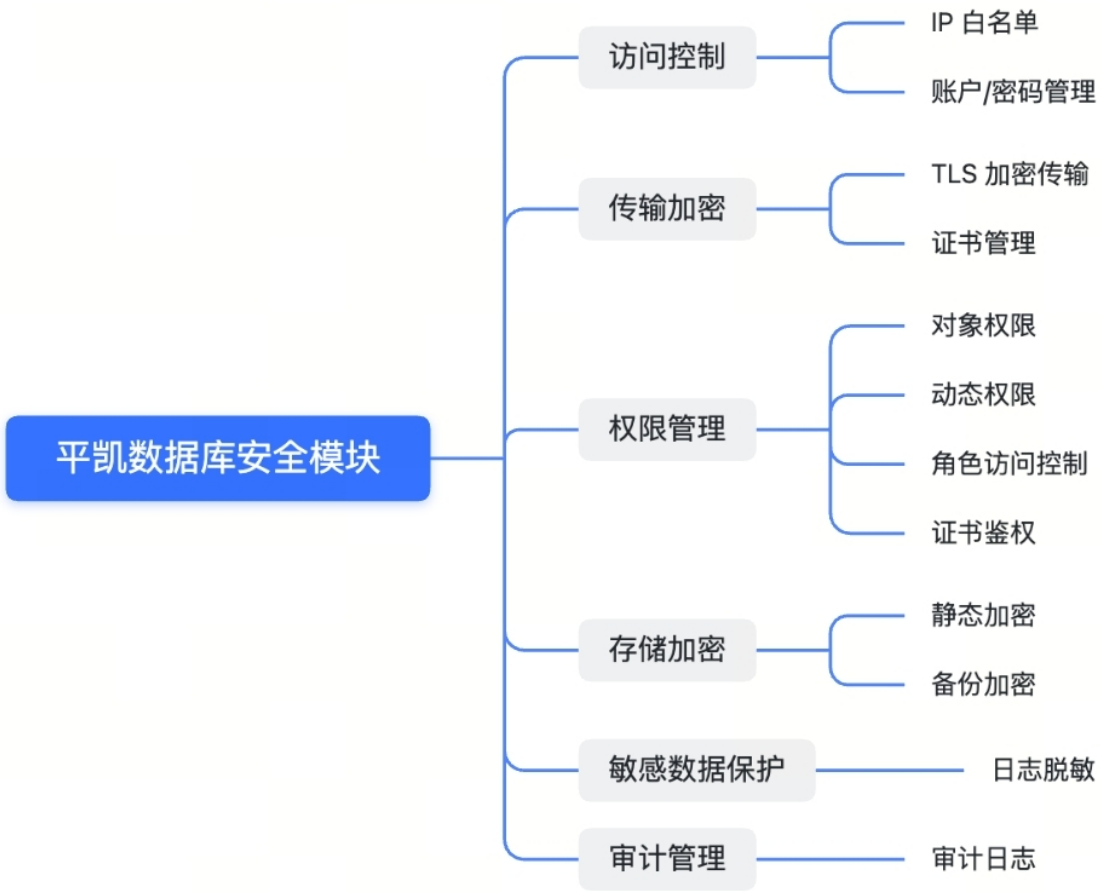

图 2: 平凯数据库 Security

1.4.1 访问控制

- 平凯数据库支持 IP 白名单控制

  创建用户时，指定该用户可以从哪些 IP 登录到平凯数据库的计算模块 TiDB 节点，如下：

- create user ‘user1’@‘%’;–允许所有 IP 的客户端登录；
- create user ‘user1’@‘localhost’;–仅允许本地客户端登录；
- create user ‘user1’@‘172.16.40.%’;–允许指定网段的客户端登录。
- 平凯数据库支持账户/密码管理

- 用户密码支持加密存储在 mysql.user 中；
- 支持用户通过校验“用户名 + 密码”登录到平凯数据库；
- 支持用户通过校验证书登录到平凯数据库（此时必须开启加密传输）。

1.4.2 传输加密

- TLS 加密传输
- 平凯数据库计算模块（TiDB 节点）服务端支持启用基于 TLS 协议的加密连接，通过客户端与服务端加密传输，可以保证信息传输的保密性、完整性，同时基于证书的单向认证/双向认证可以保证通信双方身份的真实性；
- 兼容 MySQL 客户端，现有 MySQL 客户端可直接与 TiDB 节点进行加密连接。平凯数据库支持 TLS 1.2、TLS 1.3 版本协议，同时兼容 TLS 1.0、TLS 1.1（因为 TLS 1.0、TLS 1.1 已经不安全，不建议使用）；
- 平凯数据库集群内部组件之间支持加密传输，各组件间的加密传输支持校验调用方身份，以防止拥有有效证书的非法访问者进行访问（例如：TiKV 只能被 TiDB 节点访问，则需要阻止拥有合法证书但非 TiDB 节点的其他访问者访问到 TiKV）。
- 证书管理

  对于证书替换场景，支持重载证书、密钥，无需重启 TiDB 实例。

1.4.3 权限管理

- 对象权限

  平凯数据库的权限管理系统是按照 MySQL 的权限管理的原理，自研实现了一套平凯数据库的权限管理系统，平凯数据库兼容大部分的 MySQL 的语法和权限类型。通过 GRANT/REVOKE 进行权限的授予/收回操作，例如：

  授予 xxx 用户对数据库 test 的读权限：

  GRANT SELECT ON test.* TO ‘xxx’@‘%’;

  收回 xxx 用户对数据库 test 的读权限：

  REVOKE SELECT ON test.* FROM ‘xxx’@‘%’;

- 动态权限

  平凯数据库兼容 MySQL 8.0 中的动态权限特性。动态权限用于限制 SUPER 权限，实现对某些操作更细粒度的访问。例如，系统管理员可以使用动态权限来创建一个只能执行 BACKUP 和 RESTORE 操作的用户账户。

- 角色访问控制

  平凯数据库使用基于角色的访问控制（Role-Based Access Control），其实现与 MySQL 8.0 的 RBAC 系统相类似。RBAC 可以实现批量授权，可以灵活维护用户的权限，使得其可以精细化地保障数据访问安全，实现账号、操作、表级别的精细化授权控制。

  平凯数据库兼容大部分 MySQL RBAC 系统的语法。用户可以创建角色、删除角色、将权限赋予角色；也可以将角色授予给其他用户，被授予的用户在启用角色后，可以得到角色所包含的权限。

为角色授予权限和为用户授予权限操作相同，可参考平凯数据库权限管理，例如：为 app_read 角色授予数据库 app_db 的读权限：

GRANT SELECT ON app_db.* TO ‘app_read’@‘%’;

- 证书鉴权

  平凯数据库支持基于证书鉴权的登录方式。采用这种方式，平凯数据库对不同用户签发证书，使用加密连接来传输数据，并在用户登录时验证证书。相比 MySQL 用户常用的用户名密码验证方式，与 MySQL 相兼容的证书鉴权方式更安全。

1.4.4 存储加密

- 静态加密

  静态加密 (Encryption at Rest) 即在存储数据时进行数据加密。对于数据库，静态加密功能也叫透明数据加密 (TDE)。静态加密功能是在存储数据前就对数据进行加密处理，用户必须通过数据库的身份和权限验证才能访问静态加密后的数据。即使有攻击者获得物理机的访问权限，也无法通过复制磁盘上的文件来访问这些数据。

  静态加密功能主要包括 TiKV 静态加密和 TiFlash 静态加密，同时对于 TiDB 节点落盘的临时文件也支持对其进行加密存储。

- TiKV 静态加密

  TiKV 支持静态加密，即在 CTR 模式下使用 AES 对数据文件进行透明加密。要启用静态加密，用户须提供一个加密密钥，即主密钥。可以通过 AWS Key Management Service (KMS) 提供主密钥 (Master Key)，也可以指定将密钥以明文形式存储在文件中，推荐使用 KMS 提供主密钥。

  TiKV 支持自动轮换 (Rotate) 用于加密实际数据文件的密钥，主密钥则可以由用户手动轮换。请注意，静态加密仅加密静态数据（即磁盘上的数据），而不加密网络传输中的数据。

- TiFlash 静态加密

  TiFlash 支持静态加密。数据密钥由 TiFlash 生成。TiFlash（包括 TiFlash Proxy）写入的所有文件，包括数据文件、Schema 文件、临时文件等，均由当前数据密钥加密。TiFlash 支持的加密算法、加密配置方法和监控项含义等均与 TiKV 一致。

- TiDB 节点落盘临时文件加密

  当配置项 oom-use-tmp-storage 为 true 时，如果单条 SQL 语句的内存使用超出 mem-quota-query 的限制，某些算子可以将执行时的中间结果作为临时文件落盘保存，直到查询执行完成之后将它们删除。对于这类落盘的临时文件，支持用户开启加密功能，以防止攻击者通过读取临时文件来访问数据。

- 备份加密

  Backup & Restore (BR) 支持对备份到 S3 的数据进行 S3 服务端加密 (SSE)。BR S3 服务端加密也支持使用用户自行创建的 AWS KMS 密钥进行加密。

1.4.5 日志脱敏数据保护

平凯数据库在提供详细的日志信息时，可能会把数据库敏感的数据（例如用户数据）打印出来，造成数据安全方面的风险。因此 TiDB 、TiKV、TiFlash、PD 等组件各提供了一个配置项开关，开关打开后，会隐藏日志中包含的用户数据值。

1.4.6 审计管理

平凯数据库提供 SQL 审计功能，满足合规审计的要求，也便于安全、运维人员查看 SQL 明细功能，及时发现问题。

平凯数据库支持的审计事件类型有:

事件类型	描述	父类型
CONNECTION	记录所有与连接相关的操作，包括握手、建立连接、断开连接、重设连接、变更用户等	-
CONNECT	记录连接过程中的握手操作	CONNECTION
DISCONNECT	记录断开连接的操作	CONNECTION
CHANGE_USER	记录变更用户的操作	CONNECTION
QUERY	记录所有执行 SQL 语句的操作，包括所有对数据的查询和修改的报错	-
TRANSACTION	记录所有与事务相关的语句，比如 BEGIN，COMMIT，ROLLBACK 等	QUERY
EXECUTE	记录所有执行 EXECUTE 语句的操作	QUERY
QUERY_DML	记录所有 DML 语句的操作，包括 INSERT、 REPLACE、 UPDATE、 DELETE 和 LOAD DATA	QUERY
INSERT	记录所有 INSERT 语句的操作	QUERY_DML
REPLACE	记录所有 REPLACE 语句的操作	QUERY_DML
UPDATE	记录所有 UPDATE 语句的操作	QUERY_DML
DELETE	记录所有 DELETE 语句的操作	QUERY_DML
LOAD DATA	记录所有 LOAD DATA 语句的操作	QUERY_DML
SELECT	记录所有 SELECT 语句的操作	QUERY
QUERY_DDL	记录所有 DDL 语句的操作	QUERY
AUDIT	记录所有平凯数据库审计日志相关设置语句的操作，包括系统变量和函数调用	-
AUDIT_SET_SYS_VAR	记录所有设置平凯数据库审计日志相关系统变量语句的操作	AUDIT
AUDIT_FUNC_CALL	记录所有调用平凯数据库审计日志相关函数的操作	AUDIT
AUDIT_ENABLE	记录所有开启平凯数据库审计日志的操作	AUDIT_SET_SYS_VA
AUDIT_DISABLE	记录所有关闭平凯数据库审计日志的操作	AUDIT_SET_SYS_VA

1.5 软件升级及漏洞管理

1.5.1 软件升级

- 平凯数据库将定期提供产品的新版本软件；
- 版本升级采用自愿原则，由客户自行决定是否升级；
- 若某个版本存在重大的安全风险，平凯数据库将会发布预警提示，并通知用户尽快升级至安全可靠版本。

1.5.2 漏洞管理

根据相关法规要求，平凯数据库提供了漏洞披露渠道，及时向用户披露产品的漏洞信息。

欢迎反馈平凯数据库相关的威胁情报和安全建议，提交平凯数据库产品的未知漏洞，请发邮件到 security@pingcap.com 。详情请参考官网公布的漏洞响应机制。

如果你对平凯数据库产品有任何安全相关的疑问或建议，欢迎反馈，平凯数据库团队期待与你有更频繁的直接交流。
