严翔羽 12210725

Assignment 1

The proposal from an engineer to the CTO:

尊敬的 CTO 您好，以下是所有方案。若时间有限，您可以优先阅读黑体加粗的内容，小字部分为详细介绍。

首先，**鉴于我公司规模较小，且需要存储我司的关键业务数据，直接将这些关键业务数据通过自建 postgreSQL 数据库全部存储在本地机房是相对不安全且成本较高的。**所以，**建议使用云数据库的方式存储我司关键数据。**

一、建议选择使用自治云数据库(对于小规模公司安全性更高且成本较低)

如右图所示，一共有 4 种云数据库管理方式，这里更推荐我司使用自治云数据库。

理由如下：

1.采用自治云数据库安全性更高：自治云数据库作为现在新兴的数据库管理方式，采用了机器学习技术，是可自动执行数据库备份、数据保护、安全、检测和处理、故障切换、打补丁的云技术数据库，可以更加有效保障本司关键业务数据安全。

2.可以有效降低成本：目前我司规模较小，完全自主建立并维护一套数据库需要花费较多研发成本，且自主维护一套数据库需要更多人工成本(需要聘用更多工程师)，并且需要对于物理硬件等进行各种维护。

然后，对于自治云数据库供应商的选择，这里我推荐使用阿里云的 postgreSQL 关系型自治云数据库，理由是**该云数据库提供很多辅助的安全方案**，**阿里云**拥有较强的技术安全实力和较大市场份额。鉴于要存储我司的关键业务数据，选择阿里云的 postgreSQL 关系型自治云数据库安全性和稳定性更有保障。(相比之下，有些小公司虽然价格较低，但是其本身安全性、稳定性等可能不够好，且可能有使用过程中该公司倒闭等各种风险)。

当然，如果确实想要使用我司机房自己搭建数据库也是一种选择，这样做的主要优点是可以将数据完全掌握我司手中，不会受到其他云数据库公司的一些限制，但缺点是对于小规模公司而言成本较高且安全性较低。

二、保护数据库安全的方案以及代价评估 (其中部分方案需要基于阿里云数据库)

(注：若公司选择自建数据库：以下部分的 1、2、3、4 点完全可以自建实现，第 5 点可以自主研发数据库自动监测功能。

Costs(自建数据库相对于云数据库)： **人力财力方面：**短期而言，公司会需要投入更大的研发成本，长期而言，若以后公司规模扩大，公司不依赖于云数据库，可以降低一定成本且更加独立

安全方面：使用自治云数据库会相对于本地自建数据库更加安全**)**

1.定期进行数据备份(增量备份和全量备份相结合)

针对我司情况，鉴于是关键业务数据，建议采用如下的**增量备份和全量备份相结合**的方案：

1)每 1 小时通过逻辑备份**增量备份**一次(根据我司的需求到时候可以进一步调整备份间隙)，24 小时内的快照数据会全部保留。超过 24 小时将仅保留每日 0 点后完成的第一个快照。

2)同时，每天晚上 24:00 保留一个通过逻辑备份方式和物理备份方式各获得一个**全量备份**集，(每周下来保留 14 个备份集)，保留 365 天。

建议**开启跨地域备份**，这样可以避免因为本地机房遭到恶意破坏而出现无法恢复备份的情况。

同时建议**开启告警功能**，即在备份出现任何异常时直接自动电话通知公司技术核心负责团队，以便及时应对处理。

同时注意**对于备份文件做好安全保护**

costs： 1)性能影响：备份时会对数据库性能造成影响

2)存储问题：备份文件存储需要占用大量存储空间，会消耗一定成本，备份文件本身带来的存储安全风险

2.账户分权限管理

我司可以创建两类账号：一类为**高权限账号**：**建议分配给 CTO。**高权限账号可以给用户分配数据库中不同表的查询权限和操作权限，并且可以断开任意账号的连接。。

另一类为**普通账号**：**建议分配给普通工程师。**普通账号在以下方面受到严格限制：

① **只有权限访问有限的表**，若需访问权限外的表需提交表单申请

② (部分普通账号)**只能进行部分操作**，如只可以修改但不能删除等

③ **访问数据库的时间段受到限制**，如只能从早上 9 点至下午 5 点可以访问，其余时间均不可访问。

④ **访问数据库的 IP 地址受到限制**，如只能在公司的机房网络内进行访问数据库，，不能在其他地方访问数据库

costs： 1)工作效率影响：对于拥有普通账号的工程师而言，如果想要使用不在自己权限范围的表进行联合查询，需要提交工单申请查询权限，这个过程会降低一些工作效率。

2)权限管理成本：CTO 需要经常对于普通账号的权限进行各种调整

3.开启 SQL 审计(日志审计和触发器审计(trigger)相结合)

对于数据库里的内容分级开启 SQL 审计：

对于数据库里**所有数据均开启日志审计**，将日志单独存储在另外的安全区域。

对于数据库里**核心数据开启触发器审计**，从而实现实时记录数据变化(因为触发器审计记录数据变化，对于数据库的性能影响较大)，将审计内容单独存储在另外的安全区域。

通过分级 SQL 审计可以提供对数据库操作的全面监控和记录，从而可以**实现对于数据库以下安全保障：**

1)如果发生恶意删除等破坏操作，事后可以通过日志审计查询操作记录，从而可以追究有关人员的责任。

2)在出现潜在风险行为时，通过日志审计及时告警。

3)通过触发器审计，即使核心数据受到破坏，也可以通过触发器审计记录进行数据恢复。

costs： 1）性能影响：日志审计部分，虽然针对所有数据，但因为日志审计仅记录操作日志，所以数据库的性能影响很小，基本可以忽略不计

触发器审计部分，在普通情况下影响较小，但由于需要记录数据变化，在进行高负荷和复杂查询会对数据库的性能会造成较大影响

2）存储问题：会生成大量的审计日志以及数据变化信息，这些日志需要单独存储和管理，将占用存储空间且需要保证这些数据的安全

4. 使用数据库存储过程(procedure)方法预存储各种常见 sql 指令

使用存储过程对于常见 sql 指令进行预存储，可以实现访问控制和权限管理。这样可以**减少对于普通用户直接访问数据库的权限分配，转而让部分用户通过存储过程进行数据操作而非直接操作**，这样可以提高数据库的安全性，同时由于预编译，还可以提高数据库效率。

Costs：基本没有负面成本

5.使用数据库自治服务(Database Autonomy Service) (基于阿里云数据库)

数据库自治服务是由云数据库平台提供的基于机器学习和专家经验实现数据库自感知、自修复、自优化、自运维及自安全的云服务，可以帮助我司消除数据库管理的复杂性及人工操作引发的服务故障，有效保障数据库服务的稳定、安全及高效。数据库自治服务主要可以通过对于异常 SQL 操作进行监控，对数据库性能状态进行监控等并结合机器学习等各种手段进行综合分析与应对，帮助保障数据库安全。

Costs：1）金钱成本：使用特定服务需要额外支出

2)性能影响：基本没有，自治服务还可以帮助优化数据库性能

As the CTO，additional strategies to further mitigate risks：

注：其实以下内容的第 9 点也可以从 engineer 角度提出

1.建立专门维护数据库安全的团队

鉴于我司总规模在 50 人左右，该维护数据库安全团队计划 5 人左右(可以考虑让现有的高级技术人员兼任)，其中设置一名数据库安全总工程师，同时保证每天 24 小时始终有至少一名员工值班。

该团队主要职责：

1)对于数据库日常安全进行维护，并强化我司对于数据库异常行为的监控，包括但不限于：

① 定期进行数据库漏洞评估

② 定期对于 SQL 审计日志进行分析，以尽可能发现潜在威胁或可疑的滥用行为和安全违规

③ 定期使用渗透测试、质量保证措施、入侵检测来主动扫描安全威胁

2) 对于可能的数据库突发异常事件及时有效响应

建立针对数据库突发异常事件的相应机制，如下：

步骤：1.监控识别： 值班人员实时通过自动或手动方式检测数据库潜在异常情况

2.(若发现异常) 评估：值班人员对于异常情况的严重程度情况进行评估

3.协调处理解决：对于可能有较严重后果的异常情况，立刻通知团队数据库安全总工程师，并协调团队对出现的问题及时有效处理

4.总结经验：对于每一次突发事件应对进行经验总结，不断优化应对效率

2.通过法律手段约束员工行为

当公司与程序员签订工作合同时，应当在合同中明确清员工如果出现删库跑路以及其他各项对于数据库的破坏行为应当承担的法律后果以及赔偿责任。

具体如下：1)明确定义各种违约行为(删库跑路、故意破坏数据库、盗取数据、篡改数据、对于公司硬件进行各种破坏等)

2)明确赔偿责任和法律责任：需要向公司赔偿直接或间接造成的损失(数据库受损对公司运营的损失，恢复数据库的费用等)，以及法律后果

3.保证我司服务器机房的物理安全性：

对于我司的服务器机房，为严格限制员工对物理服务器和硬件组件的接触，应该做到以下要求：

① 进行全面的摄像头监控覆盖

② 严格进行生物身份特征识别(面部识别，指纹识别等)认证进入，不让无关人员进入

③ 安排安保人员进行全天巡逻安保，实时监控服务器机房

4.对于所有员工定期进行安全意识教育

1)要求员工主动报告数据库漏洞，并对报告有效漏洞进行奖励

2)要求员工提高安全责任意识(管理好自己的密码等)。

5.严格保护数据库所有账户(尤其特殊身份账户)安全

特殊身份账户是保证数据库安全的重点，一旦特殊账户被盗，后果不堪设想。所以要重点严格保护特殊身份账户安全。

采用**多重身份认证**保护账户安全(密码+动态口令)，其中动态口令为当天在公司内部现场下发。

对于特殊身份账户，进一步结合客户端 IP 地址、程序、用户名和当天时间等多种因素，评估账户安全状态并进行认证，强化认证安全。

同时，对于任何疑似试图非授权攻击进入数据库账户的行为，立刻向 CTO 发送关于可疑数据访问活动的通知预紧。

6. 严格控制员工权限，落实最低权限原则

定期重新评估并更新所有员工的权限：定期(比如每周)根据员工的业务变化重新评估其所需要的数据库权限，并仅批准对执行其作业所必需的数据和操作的访问权限。然后定期使员工以前获得的权限失效，并重新分发给员工新的权限。

7.严控数据库删除权限

一般情况下不授予员工删除数据的权限，**让员工通过给数据打标记的方式实现"删除"，而不是真正从数据库中"删除数据"。若确有删除操作，需要通过审核再执行。**

8.开启全密态数据库服务(基于阿里云数据库)(仅针对小部分核心数据)

全密态数据库是阿里云数据库的一项数据安全功能，开启该功能，便可以对数据库表中的敏感数据列进行加密，这些列中的敏感数据将以密文进行传输、计算和存储。使得数据在用户侧（客户端）加密后，在非受信的服务器端**全程只需要以密文形式存在**，但是**仍然支持所有的数据库事务、查询、分析等操作**。

从而可以避免云平台软件、管理人员、以及其他非授权人员接触到明文数据，做到了数据在数据库内的**可用不可见**，提高数据库安全性。

Costs： 1）性能影响：**基于阿里云官方提供的全密态数据库服务的性能评估报告**进行分析(链接:https://help.aliyun.com/zh/rds/apsaradb-rds-for-postgresql/performance-testing-reports-of-fully-encrypted-databases) 以下简要给出测试结果(**可见右上图**，其他内容详见链接)与结论分析：

由测试场景 1：非密文主键查询场景下，开启全密态数据库扩展后，性能损失较小。

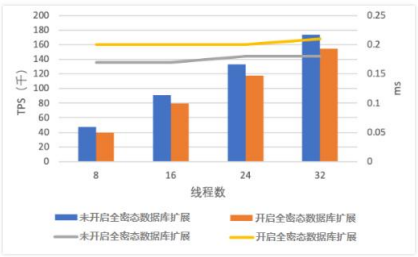
由测试场景 2：加密所有列相比于不加密主键列的查询结果，除了客户端的解密开销外，由于加密列的索引查询总代价更大，性能损失较大。

因此，针对我司的情况，我建议仅对于数据库表中的部分非主键的核心关键业务数据信息开启加密，对于表中的主键以及非关键数据不要开启 加密，否则会对数据库产生过大性能影响。这样的话，开启全密态数据库服务并仅加密小部分核心数据(20%以内)对于数据库性能的影响是较小(10%以内)的。

全密态数据库服务性能评估报告结果(简要摘编自阿里云官方技术文档)

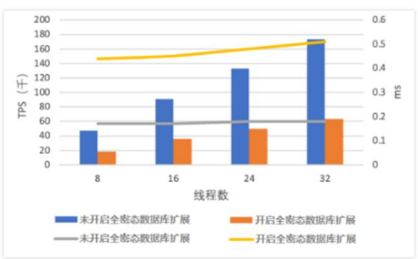
测试场景 1：主键不加密，其他列加密

SQL 模板：SELECT c FROM test1 WHERE id=?;



测试场景 2：加密所有列

SQL 模板：SELECT c FROM test1 WHERE id=?;



注：我司也可以自主设计这样的加密数据库

参考文献：https://help.aliyun.com/zh/rds/apsaradb-rds-for-postgresql，https://www.ibm.com/docs/zh/db2/11.1?topic=strategy-deciding-how-often-back-up，https://help.aliyun.com/zh/dbs/product-overview/backup-modes，https://www.alibabacloud.com/zh/product/das，https://azure.microsoft.com/zh-cn/resources/cloud-computing-dictionary/what-is-database-security，https://www.oracle.com/cn/database/what-is-a-cloud-database/，https://www.oracle.com/cn/autonomous-database/what-is-autonomous-database/，https://help.aliyun.com/zh/rds/apsaradb-rds-for-postgresql/performance-testing-reports-of-fully-encrypted-databases，https://azure.microsoft.com/zh-cn/resources/cloud-computing-dictionary/what-is-database-security，https://www.oracle.com/cn/security/database-security/database-vault