

云数据库 MariaDB

安全白皮书

产品文档



腾讯云

【版权声明】

©2013-2024 腾讯云版权所有

本文档著作权归腾讯云单独所有，未经腾讯云事先书面许可，任何主体不得以任何形式复制、修改、抄袭、传播全部或部分本文档内容。

【商标声明】

及其它腾讯云服务相关的商标均为腾讯云计算（北京）有限责任公司及其关联公司所有。本文档涉及的第三方主体的商标，依法由权利人所有。

【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默示的承诺或保证。

文档目录

安全白皮书

平台侧安全设计

租户侧安全功能

安全白皮书

平台侧安全设计

最近更新时间：2024-01-11 11:14:10

本文为您介绍平台侧安全隔离、鉴权认证、传输加密的安全设计。

安全隔离

不同地域之间网络完全隔离，不同地域之间的云产品默认不能通过内网通信。此外，采用安全组和私有网络 VPC 措施进行网络隔离。

安全组：是一种有状态的包过滤功能虚拟防火墙，用于设置单台或多台云服务的网络访问控制，是腾讯云提供的重要的网络安全隔离手段。

用户可以使用如下方法来控制 MariaDB 实例的访问权限：

创建多个安全组，并给每个安全组指定不同的规则。

每个 MariaDB 实例分配一个或多个安全组，将按照这些规则确定：哪些流量可访问 MariaDB 实例、MariaDB 实例可以访问哪些资源。

配置安全组，以便只有特定的 IP 地址可以访问 MariaDB 实例。

私有网络 VPC：是一块用户在腾讯云上自定义的逻辑隔离网络空间。即使在相同地域下，不同的私有网络之间默认无法内网通信。

鉴权认证

访问管理（Cloud Access Management，CAM）是腾讯云提供的一套 Web 服务，主要用于帮助用户安全管理腾讯云账户下资源的访问权限。通过 CAM，您可以创建、管理和销毁用户（组），并通过身份管理和策略管理控制指定用户可以使用的腾讯云资源。

当用户使用 CAM 的时候，可以将策略与一个用户或一组用户关联起来，策略能够授权或者拒绝用户使用指定资源完成指定任务。

如果用户在中使用到了云服务器、私有网络、数据库等服务，这些服务由不同的人管理，但都共享用户的云账号密钥，将存在以下问题：

用户的密钥由多人共享，泄密风险高。

用户无法限制其它人的访问权限，易产生误操作造成安全风险。

您可以通过子账号实现不同的人管理不同的服务来规避以上的问题。默认情况下，子账号没有使用云服务的权利或者相关资源的权限。因此，我们就需要创建策略来允许子账号使用他们所需要的资源或权限。

传输加密

MariaDB 控制台支持 HTTPS 传输协议，通过支持网络访问的标准协议，保障用户的访问安全，满足用户敏感数据加密传输的需求。

租户侧安全功能

最近更新时间：2024-01-11 11:14:10

本文为您介绍租户侧强同步复制、自动故障转移、数据安全加密等安全功能。

强同步复制（MAR）

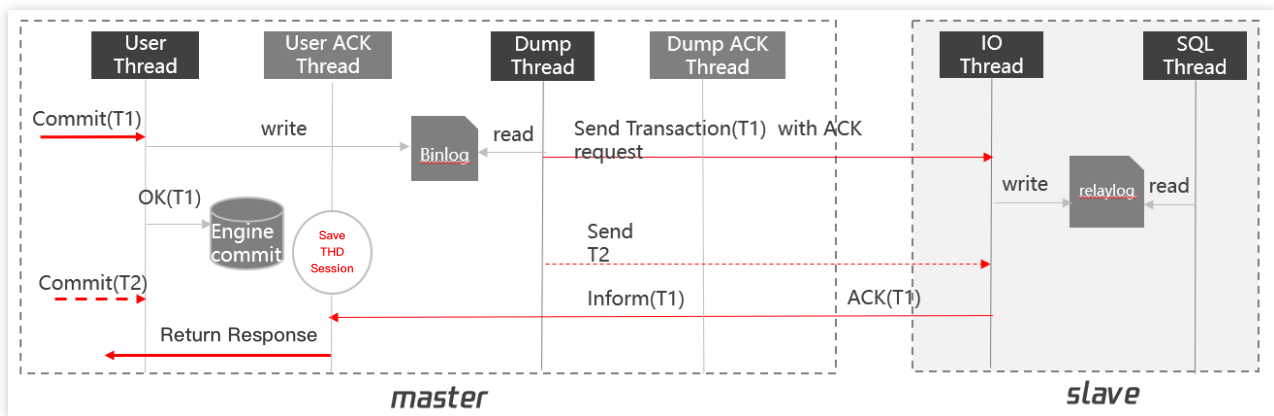
背景

数据库中记录了数据，若要在多台数据库中切换，数据必须是同步的，所以数据同步技术是数据库高可用方案的基础。

目前，开源 MySQL 数据库数据复制包括异步复制、半同步复制两种类型。这两种复制技术的主要问题是，当出现节点故障时，将可能导致数据丢失或错乱，且这类复制技术以串行复制为主，性能相对比较低。

解决方案

腾讯云基于 MySQL 协议自主研发的并行多线程强同步复制方案（Multi-thread Asynchronous Replication，MAR），在应用层发起请求时，只有当从节点（Slave）返回信息成功后，主节点（Master）才向应用层应答请求成功，以确保主从节点数据完全一致。

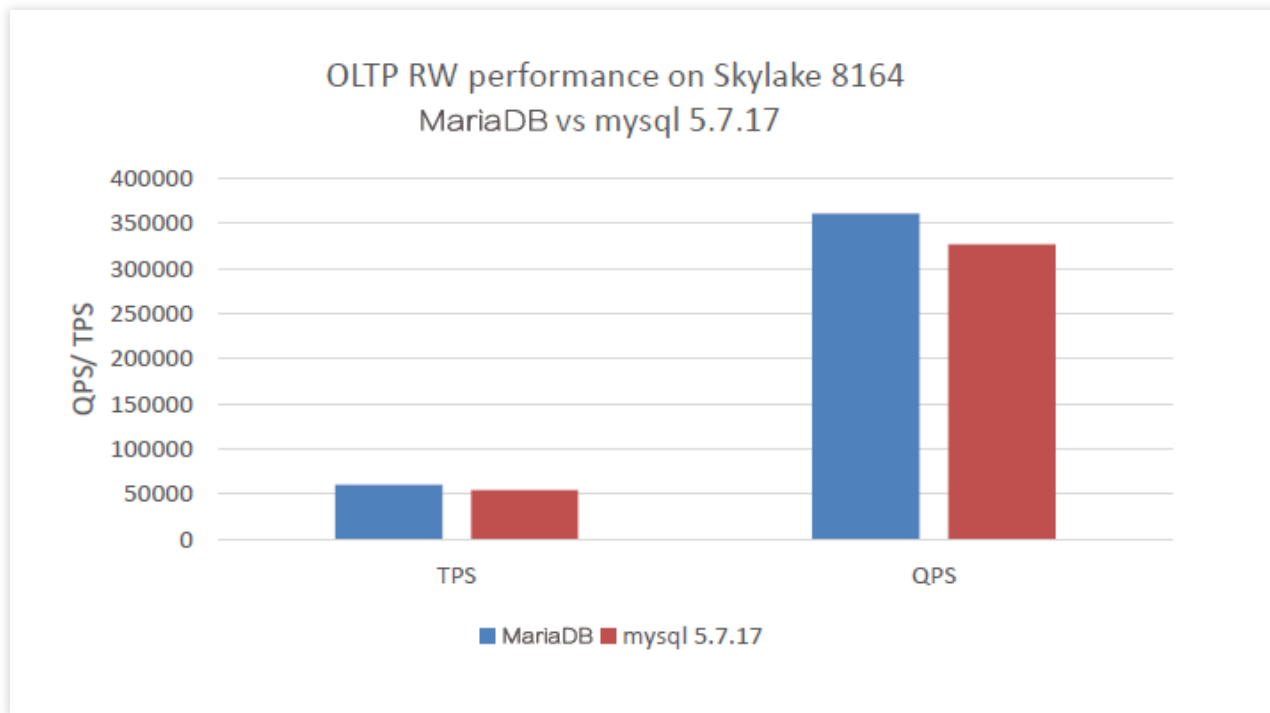


使用强同步复制时，如果主库与备库自建的网络中断或备库出现问题，主库也会被锁住（Hang），此时如果只有一个主库或一个备库，将无法做高可用方案，因为单一服务器服务时，如果出现故障，将直接导致部分数据完全丢失，不符合金融级数据安全要求。

因此，MariaDB 在强同步技术的基础上，提供强同步可退化的方案，方案原理类似于半同步，但实现方案与 Google 的半同步技术不同。

另外，MariaDB 强同步将串行同步线程并行化，引入工作线程能力，大幅度提高性能；对比在跨可用区（IDC 机房，延迟约 10ms - 20ms）同样的测试方案下，MAR 技术性能优于 MySQL 5.6 的半同步约 5 倍，优于 MariaDB

Galera Cluster 性能1.5倍；在 OLTP RW（读写混合，主从架构）下，MAR 技术性能是 MySQL 5.7 异步的1.2倍，具体由英特尔®技术团队测试的性能对比如下图所示：



自动故障转移与恢复

在生产系统中，通常都需要用高可用方案来保证系统不间断运行，数据库作为系统数据存储和服务的核心，其可用要求高于计算服务资源。

MariaDB 高可用方案原理是让多个数据库服务协同工作，当一台数据库故障，其余机器立即顶替工作，以使服务不中断或只中断很短时间，该方案简称主从高可用，也可称主备高可用。

在普通的主从高可用基础上，MariaDB 还支持如下功能：

支持故障自动转移，集群成员自动控制，故障节点自动从集群中移除；如果是实例级的主从切换，换后 VIP（虚拟 IP）不变；基于强同步复制策略下，主从切换将保证主从数据完全一致，可满足金融级数据一致性要求。

支持故障自动恢复，承载分片的物理节点故障，调度系统自动尝试恢复节点，如果原节点无法恢复，将在30分钟内自动申请新资源，并通过备份重建（Rebuild）节点，并将节点自动加入集群，以确保实例长期来保持完整的高可用架构。

每个节点都包含完整的数据副本，可以根据数据库管理页需求切换。

支持免切设置，即可以设置在某一特殊时期，不处理故障转移。

可支持配置为 x86 的计算机设备，且无需共享存储设备。

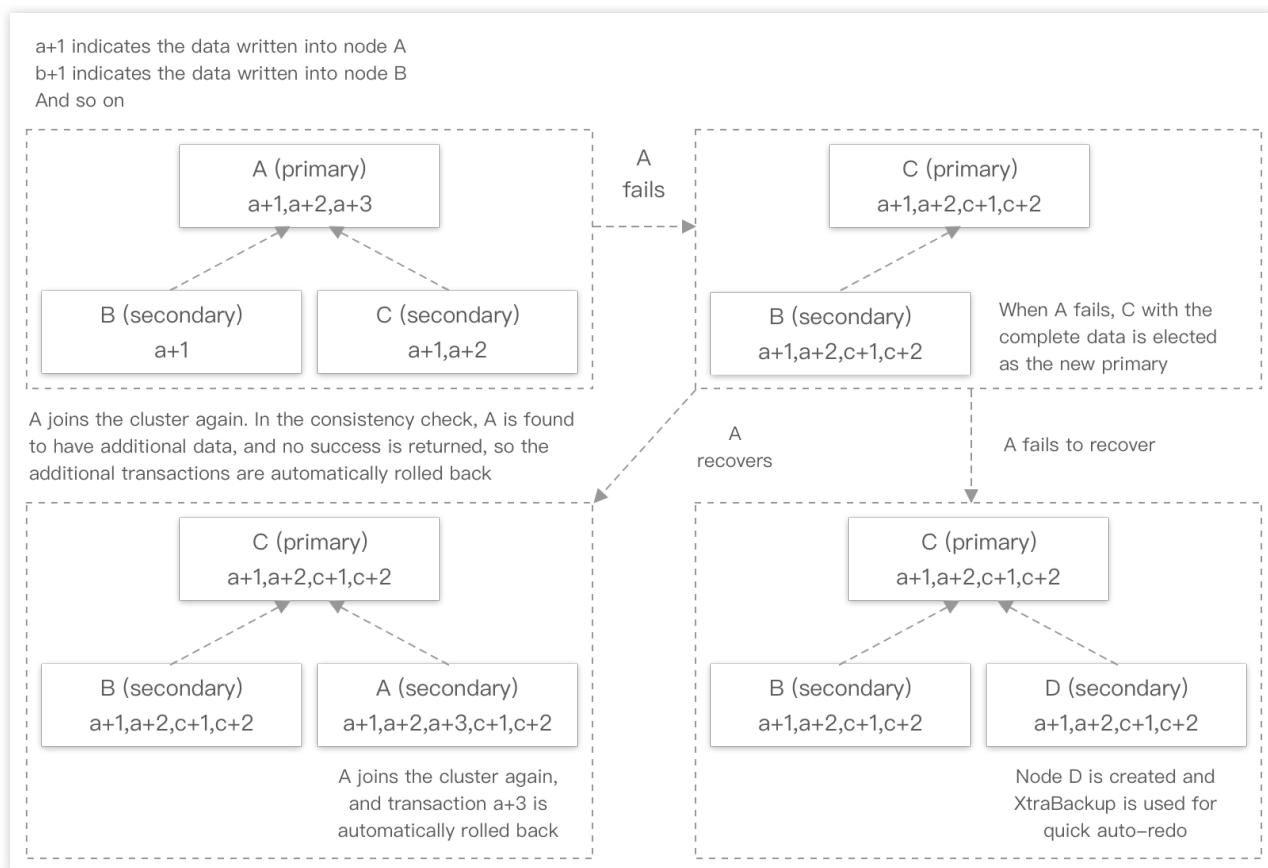
支持跨可用区部署，实例的主机和从机可分处于不同机房（无论是否同城），数据之间通过专线网络进行实时数据复制。若本地为主机，远程为从机，首先将访问本地节点，若本地实例发生故障或访问不可达，则访问远程从机。

若配合腾讯 VPC 网络环境，可支持同城双活架构，即业务系统可以直接在两个中心读写数据库。

跨可用区部署特性为 MariaDB 提供了多可用区容灾的能力，以避免单 IDC（Internet Data Center）部署的运营风险。

MariaDB 的每一个分片都支持基于强同步的高可用方案，如果主数据库故障时，系统将立即自动选举出最优备机顶替工作，切换过程对用户透明，不改变访问 IP，并且对数据库和底层物理设备提供 7 x 24 小时持续监控。

如果发生故障，系统将自动重启数据库及相关进程；如果节点崩溃无法恢复，将通过备份文件自动重建节点，具体流程如下所示：



多项国家或国际认证

MariaDB 符合国家相关信息安全标准，并代表腾讯云数据库通过多项国家和国际认证。

MariaDB 白金会员

ACMUG 和中国开源数据库专业委员会的主席团成员

ISO27001

ISO27001 : 2013

ISO20000

ISO20000-1 : 2011

ISO22301

ISO9001

ISO27018

PCI DSS 1级服务提供商

SOC 审计

ITSS 云服务增强级认证

中国公有云三级备案和测评

中国金融云四级备案和测评

中国信通院可信云云数据库服务认证

中国信通院可信云云用户数据安全保护能力测评

中国信通院可信云金牌运维专项评估

ITSS 认证

金牌等级通过 CSA STAR 认证，同时获得 CNAS 和 UKAS 国内外双认可信息安全管理体认证

数据安全加密

MariaDB 支持连接加密（SSL 连接加密），SSL 确保了来往于数据库和服务器之间的流量安全。

SQL 防火墙

SQL 防火墙是对用户发送的 SQL 语句进行语法解析，具有过滤非法 SQL 语句的安全能力，其与 SQL Engine 配合，可以对用户预先定义的非法 SQL 语句进行判断，从而进行过滤和阻断，可以有效地预防 SQL 注入恶意非法攻击。

说明：

SQL 防火墙可以配合 WAF（Web Application Firewall）等一起使用，因考虑到业务情况和 SQL 复杂性，目前 MariaDB 的 SQL 防火墙暂未预存规则。

全维度的安全审计

安全审计是一项最重要的事后追溯手段，例如，国家等级保护（三级）明确要求信息系统应支持审计能力。MariaDB 提供如下三个层面的审计能力，为用户提供完善的安全保护：

运维系统的安全审计，由赤兔运营系统的操作日志提供安全能力。

数据库系统的安全审计，由腾讯云自研的数据库审计系统完成。

服务器操作系统的安全审计，由腾讯云自研的铁将军系统提供。

说明：

公有云默认全部配置安全审计功能。

专有云默认配置系统操作日志（赤兔系统），选配数据库 SQL 审计、服务器操作审计功能。

内核级安全策略

MariaDB 在数据库内核层面提供了多种安全方案并开源，部分功能也已获得社区认可。部分内核安全手段列举如下：

慢速删除

当用户执行 `drop table` 或 `alter table ... drop partition` 指令时，数据库没有立即删除表空间文件，而是将其重命名，并在后台逐步缩小并最终删除。该功能可避免因单次删除过大表空间文件，使服务器的文件系统 IO 负载突增，从而导致系统出现波动的情况。

防止误删元数据

只允许已授权用户登录系统，删除存储元数据的库表，防止用户误操作导致业务不可用。

禁止非授权用户安装插件

数据库虽然提供了标准的接口，允许用户实现自定义的功能，但黑客经常利用该漏洞以实现攻击。因此，只允许规定的管理员用户挂载插件。

禁止非授权用户访问物理服务器文件系统

我们禁止非授权用户访问物理服务器的目录结构和文件系统，从而防止黑客通过选择文件、注入文件、路径探测等方式绕开安全系统。

数据销毁

腾讯云用户在销毁 MariaDB 实例时，存储在 MariaDB 数据库的所有数据（包括所有备份数据）都会被销毁，腾讯云不会保留数据，更不会主动恢复用户的数据库实例。

单中心容灾部署建议

单中心容灾时，数据库集群需要预防如下故障：

机房内交换机、负载转发或网卡等单点故障。

机架电源、风扇、冷却等相关的单点故障。

数据库服务器硬件的单点故障。

因此，建议单中心容灾部署至少采用如下要求：

交换机、负载转发等网络设备至少双活容灾。

数据库服务器、管理调度建议采用一主二从模式部署。

同模块不同设备需跨机架部署。

需部署数据备份模块。

两地三中心部署建议

两地三中心即在同城双中心的基础上，增加一个灾备中心。两个灾备实例之间，通过 DCN（Data Communication Network）同步方式进行同步，以确保数据一致。

