TDSQL-C MySQL 版

数据库审计

产品文档

腾讯云

版权所有：腾讯云计算（北京）有限责任公司

【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

- 数据库审计
  - 简介
  - 查看审计实例列表
  - 开通审计服务
  - 查看审计日志
  - 配置事后告警
  - 修改审计规则
  - 修改审计服务
  - 关闭审计服务
  - 审计规则模板
    - 查看规则模板列表
    - 新建规则模板
    - 修改规则模板
    - 删除规则模板
  - 查看审计任务
  - 授权子用户使用数据库审计

版权所有：腾讯云计算（北京）有限责任公司

数据库审计
简介

最近更新时间：2023-12-12 10:25:22

数据库审计是腾讯云自主研发的一款专业、高效、全面、实时监控数据库安全的审计产品，数据库审计能够实时记录腾讯云数据库活动，对数据库操作进行细粒度审计的合规性管理，对数据库遭受到的风险行为进行告警。
TDSQL-C MySQL 版提供数据库审计能力，记录对数据库的访问及 SQL 语句执行情况，帮助企业进行风险控制，提高数据安全等级，同时支持自定义高低频存储，可大幅降低数据库审计的使用成本。
数据库审计功能支持事后告警，支持配置高、中、低三个风险等级的事件告警策略，命中策略的审计日志可发送告警通知给绑定的用户，同时也可在腾讯云可观测平台中，查看告警历史、进行告警策略管理（告警开关）及告警屏蔽，帮助企业及时获取相关告警通知，准确定位触发问题的审计日志。

应用场景

助力企业顺利通过等保合规审计，提供等保三级及其他行业合规审计依据。
帮助企业记录、分析、追查技术人员误操作等数据库安全相关事件。
基于数据库审计数据，提升性能优化、故障定位等场景的效率和精准度。

产品计费

按照审计日志的存储量进行按量计费。每小时为一个计费周期，不足一小时的按一小时计费。
具体产品定价请参见 数据库审计计费说明。

支持版本

TDSQL-C MySQL 版数据库审计目前支持的兼容版本为 MySQL 5.7、8.0。

优势

TDSQL-C MySQL 版数据库审计提供全审计、规则审计、高低频存储、长期保存审计日志等功能特性，具备以下几点优势：
数据采集完整性
TDSQL-C MySQL 版数据库审计基于 MySQL 的内核插件实现，每一条 SQL 语句的执行都会经过连接、解析、分

析、重写、优化、执行、返回、审计、释放的完整过程。开通数据库审计，连接到 TDSQL-C MySQL 服务器后，每条 SQL 语句在执行过程中都会被审计，若审计未成功，则代表 SQL 语句没有执行成功，若 SQL 语句执行成功，则一定会被审计。审计完成后，SQL 的请求连接才能被释放，确保了审计采集数据的完整性。

采集数据可靠性

TDSQL-C MySQL 版数据库审计是基于 MySQL 自身执行层同步抓取数据，而不是通过旁路异步抓取数据，因此审计的 SQL 会与 TDSQL-C MySQL 版执行的 SQL 实时同步且一致，保障数据不会抓取错误，确保了审计采集数据的可靠性。

数据防篡改

审计管控系统具备行为监测机制，当有人利用漏洞进行攻击时，漏洞扫描可以实时捕获到相关会话信息并发送告警，实时监控入侵行为；当有人对审计数据进行操作时，访问日志会被全量记录，可以确定哪些用户何时从哪个源 IP 地址进行了数据访问，及时发现高风险访问操作记录；对于操作人员，具有权限管控功能，通过账号及角色鉴权，可实现不同角色的人员，对数据具备不同的读写权限，进而规避账号共享问题，当有人进行高危操作时，会触发实时篡改告警，及时发现高风险操作并进行分析追踪和阻止。

数据传输完整性

审计数据采集后，在传输链路层的处理过程中，审计数据会通过 CRC（循环冗余校验码）循环冗余校验、全局唯一消息 ID、链路 MQ 冗余、Flink 流处理等步骤，多维度多角度来进行校验，以确保在传输过程中数据的完整性。

数据存储完整性

在数据存储端，数据库审计系统对审计日志文件进行了加密存储，以确保审计数据安全性，只有具备加密证书访问权的用户才能查看审计日志，能够有效防止明文存储引起的数据内部泄密、高权限用户的数据窃取，从根源上防止审计数据泄漏，保证数据存储的完整性。

版权所有：腾讯云计算（北京）有限责任公司

查看审计实例列表

最近更新时间：2024-06-07 14:42:32

本文为您介绍如何查看数据库审计实例列表，以及在数据库审计实例列表页您可查看到的字段信息和可执行的相关操作。

数据库审计实例列表页展示

查看数据库审计实例列表

1. 登录 TDSQL-C MySQL 版控制台。
2. 在左侧导航栏单击**数据库审计**。
3. 跳转页面默认为**数据库审计** > **审计实例**。
4. 在审计实例页面可以：查看工具列表（快速筛选集群/实例、刷新审计实例页面、下载审计实例列表信息）、查看相关功能操作、查看实例列表字段信息。

工具列表

工具	说明
筛选	可在审计实例列表上方搜索框内，选择资源属性（实例 ID、实例名称、集群 ID、集群名称、标签键、标签）进行过滤筛选，多个关键字用竖线分隔，多个过滤标签用回车键分隔。
刷新	单击 ，可刷新审计实例列表数据。
下载	单击 ，可下载过滤筛选后的审计实例列表信息到本地，文件格式为“.csv”，文件列表字段包括：实例 ID、实例名称、审计状态、审计类型、审计规则、总存储时长、高频存储时长、低频存储时长、总存储量、高

	频存储量、低频存储量、所属项目、标签、备注。

相关功能操作

审计状态	功能	说明
已开启审计服务	关闭审计服务	可进行关闭审计服务操作，支持批量关闭，详见 关闭审计服务。
	修改审计规则	可进行审计规则修改，支持批量修改，详见 修改审计规则。
	修改审计服务	可进行审计服务内容修改（审计保存时长、高低频存储时长），支持批量修改，详见 修改审计服务。
	查看审计日志	可查询历史审计日志记录，详见 查看审计日志。
未开启审计服务	开通审计服务	可进行开通审计服务操作，支持批量开通，详见 开通审计服务。

审计实例列表字段信息

字段	说明
集群 ID / 名称	展示某个地域下的所有集群的集群 ID / 名称信息。
实例 ID / 名称	展示对应集群下读写实例的实例 ID / 名称信息。
审计状态	展示已开启或未开启审计服务的状态，支持筛选展示对应状态的集群/实例。
审计类型	展示已开启审计服务时，对应实例当前配置的审计规则：全审计或规则审计，支持下拉筛选进行单一规则展示。
日志保存时长	展示已开启审计服务时，对应集群或实例的总存储时长（天）、高频存储时长（天）、低频存储时长（天）。
日志存储量	展示已开启审计服务时，对应集群或实例的总存储量（MB）、高频存储量（MB）、低频存储量（MB）。
审计规则	展示实例所绑定的审计规则模板数量，鼠标指向对应实例的审计规则字段时您可看到每个规则模板的 ID 和名称，点击具体规则模板，可查看该规则模板的具体规则详情，包括基本信息、参数设置、修改历史。
所属项目	展示对应集群/实例的所属项目，便于轻松对资源进行分类和管理，支持下拉筛选所需项目下的集群/实例。
标签（key：	展示集群/实例的标签信息。

value）	
开通时间	展示对应集群/实例开启审计服务的时间，精确到秒。
操作	已开启审计服务的操作项： 查看审计日志 更多（修改审计规则、修改审计服务、关闭） 未开启审计服务的操作项： 开通审计服务

开通审计服务

最近更新时间：2024-06-18 09:37:27

腾讯云 TDSQL-C MySQL 版提供数据库审计能力，记录对数据库的访问及 SQL 语句执行情况，帮助企业进行风险控制，提高数据安全等级。
本文为您介绍通过控制台开通审计服务相关操作。

前提条件

已 创建集群。
如需使用规则审计功能，请 提交工单。
事件告警功能当前仅支持北京、上海、广州、成都、新加坡地域，如需使用，请 提交工单。
审计类型为全审计的实例，如需为审计日志设置风险等级和告警策略，请 提交工单。

操作步骤

1. 登录 TDSQL-C MySQL 版控制台。
2. 在左侧导航栏选择**数据库审计**。
3. 在上方选择地域后，在**审计实例**页，单击**审计状态**选择**未开启**选项过滤未开启审计的实例。

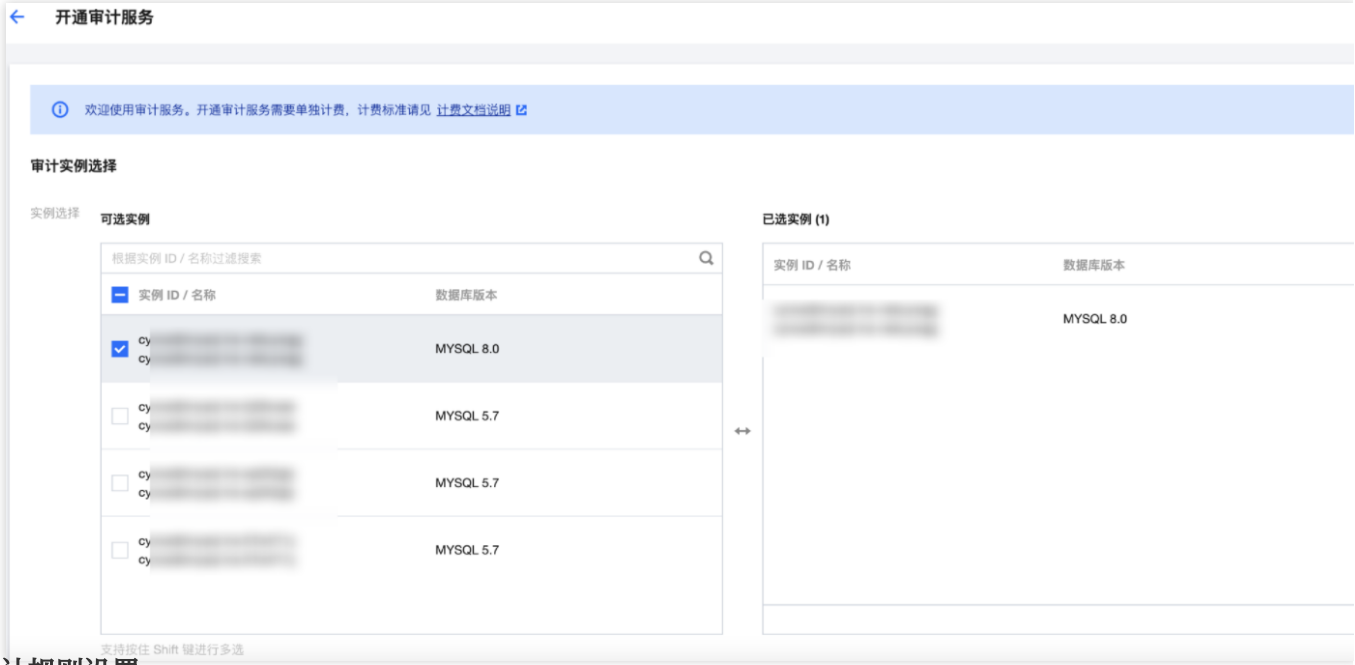
4. 在审计实例列表里找到目标实例（也可在搜索框通过资源属性筛选快速查找），在其**操作**列单击**开通审计服务**。

说明：
支持批量开通审计服务。在审计实例列表页勾选多个目标实例，单击上方**开通审计服务**即可进入设置界面。

5. 在开通审计服务界面，依次完成审计实例选择、审计规则设置、审计服务设置，阅读并勾选腾讯云服务协议，单击**确定**。

5.1 **审计实例选择**

在审计实例选择项下面，系统默认勾选**步骤4**中所选择的实例，同时支持在此窗口下修改目标实例（选择其他实例、多选实例），也可在搜索框根据**实例 ID / 名称**快速查找目标实例，完成实例选择后进入审计规则设置。



5.2 **审计规则设置**

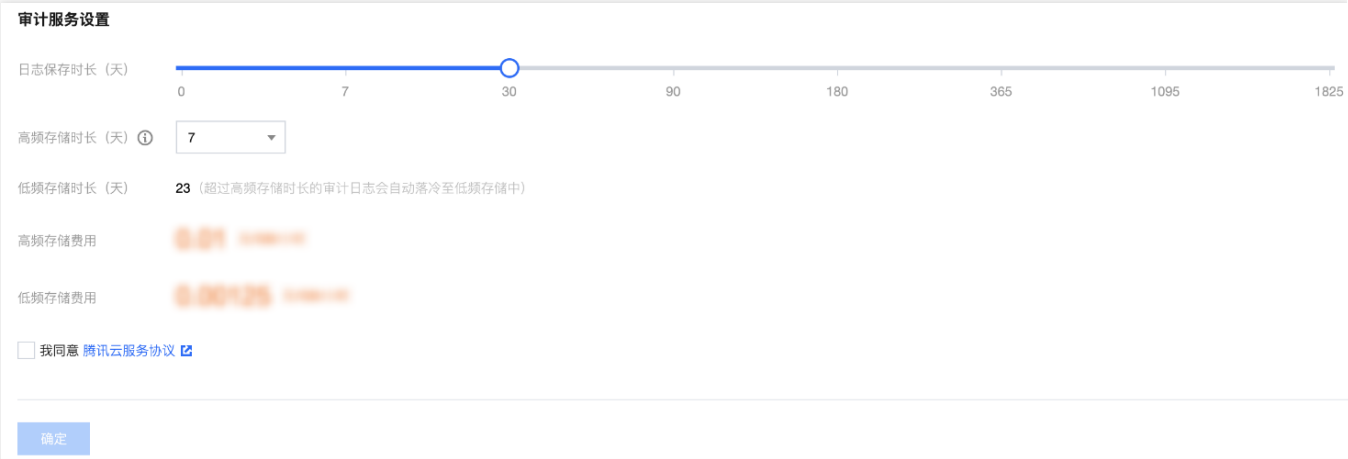
在审计类型设置项，您需要选择类型为**全审计**或者**规则审计**，两者详细对比说明见下表。

参数	说明

全审计	全面记录对数据库的所有访问及 SQL 语句执行情况。
规则审计	规则审计将根据自定义的审计规则记录对数据库的访问及 SQL 语句执行情况。

审计类型设置为全审计时
，控制台实际操作分如下两种场景，您可对应参考操作。
场景一：未申请使用全审计的风险等级和告警策略能力
场景二：已申请使用全审计的风险等级和告警策略能力
选择审计类型为全审计后，您可直接进入 审计服务设置 步骤。
5.2.1 从规则模板中选择已有模板或选择新建规则模板，关于新建模板的详细操作可参考 新建规则模板。
5.2.2 规则模板设置完成后，进入 审计服务设置 步骤。
说明：
您最多可应用5个规则模板，不同规则模板之间为“或”的关系。
规则模板针对审计类型为“全审计”实例，仅用于对命中模板中规则内容的审计日志设置风险等级及告警策略，未命中规则内容的审计日志依然保留。
审计类型设置为规则审计时，您可从规则模板中选择已有规则模板或选择新建规则模板，若从规则模板中选择了一个已有的规则模板，则可直接进入审计服务设置，若规则模板中没有合适的规则，您可以新建规则模板后刷新，即可选择新建的规则模板，详细操作可参考 新建规则模板。
说明：
您最多可应用5个规则模板，不同规则模板之间为“或”的关系。
规则模板针对审计类型为“规则审计”的实例，用于对命中模板规则内容的审计日志进行日志保留、设置风险等级及告警策略，未命中规则内容的审计日志不再保留。
5.3
审计服务设置

在审计服务设置项下面，您需要设置审计日志保存时长及高低频存储时长，阅读并勾选腾讯云服务协议，然后单击**确定**开通审计服务。



参数	说明
日志保存时长	设置审计日志的保存时长，单位：天，支持选择7、30、90、180、365、1095、1825天。
高频存储时长	高频存储代表超高性能存储介质，拥有很好的查询性能；单位：天，设定存储时长后，指定时长范围内审计数据会存储在高频存储中，超过高频存储时长部分数据会自动落冷至低频存储中。不同存储支持的审计能力完全相同，仅性能差异。例如：日志保存时长设置为30天，高频存储时长设置为7天，则低频存储时长默认为23天。

查看审计日志

最近更新时间：2024-07-31 11:17:37

本文为您介绍如何查看数据库审计日志及相关审计日志列表的字段。

说明：

2023年07月12日发布了新版审计日志页面，审计日志搜索字段“扫描行数”为新增字段，在此日期之前的存量审计日志，此字段数据会显示为“-”，对应下载的文件和 API 展示为“-1”。

审计日志字段“执行时间”、“CPU 时间”在控制台和下载的审计日志文件里的单位统一调整为微秒。

搜索审计日志时，对多个搜索项进行分隔的字符由**逗号**更换为**换行符**。

开通数据库审计后，天津、台北、深圳地域的实例审计日志文件存储的地域有所不同，对应存储地域请参见下表。

实例地域	审计日志存储地域
天津	北京
台北	中国香港
深圳	广州

前提条件

已 开通审计服务。

查看审计日志

说明：

审计日志展示时间扩展到毫秒，便于对 SQL 进行更精确的排序和问题分析。

1. 登录 TDSQL-C MySQL 版控制台。
2. 在左侧导航选择**数据库审计**。
3. 在上方选择**地域**后，在**审计实例**页，单击**审计状态**选择**已开启**选项过滤已开启审计的实例。
4. 在审计实例列表里找到目标实例（也可在搜索框通过资源属性筛选快速查找），在其操作列单击**查看审计日志**，跳转至审计日志页，即可查看对应实例的审计日志。

工具列表

在**审计实例筛选框**，可选择切换已开启审计服务的其他审计实例。

在**时间框**，默认选择近1小时，可快捷选择其他时间（近3小时、近24小时、近7天），也支持自定义时间段，可查看所选时间段内相关审计日志。

说明：

搜索时间段支持选取存在数据的任意时间段进行搜索，最多展示符合条件的前60000条记录。

在**搜索框**，选择搜索项（SQL 命令详情、客户端 IP、用户账号、数据库名、错误码、SQL 类型、风险等级、执行时间（微秒）、锁等待时间（微秒）、IO 等待时间（微秒）、事务持续时间（微秒）、CPU 时间（微秒）、审计规则、线程 ID、事务 ID、扫描行数、影响行数、返回行数等）进行搜索，可查看相关审计结果，多个关键词使用换行符分隔。

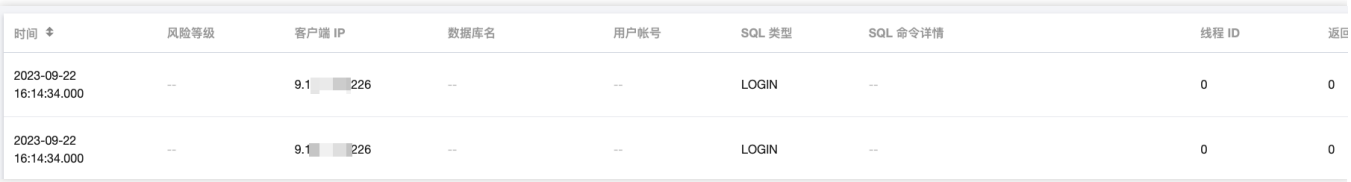
搜索项	匹配项	说明
SQL 命令详情	包含-或-分词 包含-且-分词 不包含-且-分词 包含-或-通配 包含-且-通配 不包含-且-通配	**规则说明** 输入 SQL 命令详情，多个关键字使用换行符进行分隔。 SQL 命令详情搜索框的匹配项分为三层，一层设置正反向的匹配模式（包含、不包含）；二层设置关键词之间的逻辑关系（或、且）；三层设置每个关键词的匹配模式（分词、通配）。 **注意：** SQL 命令详情搜索不区分大小写。 支持“包含”、“不包含”两种正反向匹配模式。 关键词之间支持“或”、“且”两种逻辑匹配，“或”表示不同关键词之间取“并集”关系，“且”表示不同关键词之间取“交集”关系。 每个关键词支持“分词”、“通配”两种匹配模式，“分词”表示 SQL 命令详情中的每个关键词需要精确匹配，“通配”表示 SQL 命令详情中的每个关键词可以模糊匹配。 **示例说明** 假设 SQL 命令详情为：SELECT * FROM test_db1 join test_db2 LIMIT 1; 在“包含（分词）”搜索模式下，可以通过“SELECT”、“select * from”、“*”、“SELECT * FROM test_db1 join test_db2 LIMIT 1;”、“from

		Test_DB1”等分词关键词进行搜索，无法通过 “SEL”、“sel”、“test” 等通配关键词进行搜索。 在“包含（通配）”搜索模式下，可以通过“SEL”、“sel”、“test”、“DB”等通配关键词进行搜索。 在“包含（且）” 搜索模式下，多个关键词之间是“且”的关系，即输入“SELECT”、“test_db” 等关键词，可以查询到所有包含“SELECT”和“test_db”的 SQL 命令。 在“包含（或）” 搜索模式下，多个关键词之间是“或”的关系，即输入“test_db1”、“test_db2” ，可查询到所有包含“test_db1”或者包含“test_db2”的 SQL 命令。
客户端 IP	包含 不包含 等于 不等于	输入客户端 IP，多个关键字使用换行符进行分隔；IP 地址支持使用 * 作为条件进行筛选。如搜索客户端 IP: 9.223.23.2*，则匹配以9.223.23.2 开头的 IP 地址。
用户账号	包含 不包含 等于 不等于	输入用户账号，多个关键字使用换行符进行分隔。
数据库名	包含 不包含 等于 不等于	输入数据库名，多个关键字使用换行符进行分隔。 **说明：** 数据库名的搜索不区分大小写。
错误码	等于 不等于	输入错误码，多个关键字使用换行符进行分隔。
SQL 类型	等于 不等于	下拉选择 SQL 类型（ALTER、CHANGEUSER、CREATE、DELETE、DROP、EXECUTE、INSERT、LOGOUT、OTHER、REPLACE、SELECT、SET、UPDATE），支持多选。
风险等级	包含 不包含	选择低风险、中风险或高风险，过滤命中规则模板风险等级设置的审计日志。 也支持输入为空，表示过滤历史存量没有风险等级标签的审计日志。
执行时间（微秒）	区间格式	输入执行时间，格式为 M-N，如10-100或20-200。
锁等待时间（微秒）	区间格式	输入锁等待时间，格式为 M-N，如10-100或20-200。
IO 等待时间（微秒）	区间格式	输入 IO 等待时间，格式为 M-N，如10-100或20-200。
事务持续时间	区间格式	输入事务持续时间，格式为 M-N，如10-100或20-200。

（微秒）		
CPU 时间（微秒）	区间格式	输入 CPU 时间，格式为 M-N，如10-100或20-200。
审计规则	包含 不包含	展示所有某地域的规则模板的模板 ID 和模板名称，您可以根据规则模板过滤出命中该规则模板的审计日志。 支持输入为空，表示过滤历史存量没有审计规则标签的审计日志和没有命中规则的全审计日志。 支持按照规则模板 ID 和规则模板名称对审计规则进行搜索。 支持同时选中多个规则模板。
线程 ID	等于 不等于	输入线程 ID，多个关键字使用换行符进行分隔。
事务 ID	等于 不等于	输入事务 ID，多个关键字使用换行符进行分隔。 **说明：** 仅 TDSQL-C MySQL 版 5.7 的内核小版本2.1.11及以上支持“事务 ID”字段，TDSQL-C MySQL 版 8.0 暂不支持。
扫描行数	区间格式	输入扫描行数，格式为 M-N，如10-100或20-200。
影响行数	区间格式	输入影响行数，格式为 M-N，如10-100或20-200。
返回行数	区间格式	输入返回行数，格式为 M-N，如10-100或20-200。

日志列表

返回行数字段代表执行 SQL 返回的具体行数，主要用于对 SELECT 类型 SQL 影响的判断。



时间	风险等级	客户端 IP	数据库名	用户帐号	SQL 类型	SQL 命令详情	线程 ID	返回
2023-09-22 16:14:34.000	--	9.1 226	--	--	LOGIN	--	0	0
2023-09-22 16:14:34.000	--	9.1 226	--	--	LOGIN	--	0	0

审计字段

TDSQL-C MySQL 版的审计日志中支持如下字段。您可以在**审计日志**页面单击**下载图标**，下载完成后单击**文件列表图标**，在跳转页面复制下载地址进行下载，即可获取完整的 SQL 审计日志。

注意：

目前日志文件下载仅提供腾讯云内网地址，请通过同一地域的腾讯云服务器进行下载（例如：北京区的数据库实例审计日志请通过北京区的 CVM 下载）。
日志文件有效期为 24 小时，请及时下载。
每一个数据库实例的日志文件不得超过 30 个，请下载后及时删除清理。
若状态显示失败，可能是由于日志过多导致，请缩短时间窗口分批下载。

序号	字段名	备注
1	时间	-
2	风险等级	分为低风险、中风险、高风险，对于全审计，没有命中审计规则的日志，风险等级会显示为“-”
3	客户端 IP	-
4	数据库名	-
5	用户账号	-
6	SQL 类型	-
7	SQL 命令详情	-
8	错误码	0表示成功
9	线程 ID	-
10	事务 ID	-
11	扫描行数	-
12	返回行数	-
13	影响行数	-
14	执行时间（微秒）	-
15	CPU 时间（微秒）	-
16	锁等待时间（微秒）	-
17	IO 等待时间（微秒）	-
18	事务持续时间（微秒）	-
19	策略名称	-
20	审计规则	展示该条审计日志所命中的是哪个规则模板，单击对应规则模板后，可展示该规则模板的具体规则详情，包括基本信

		息、参数设置、修改历史。 历史存量的审计日志，审计规则的值展示为“-”。 没有命中规则的全审计日志，审计规则的值展示为“-”。

SQL 语句类型与 SQL 语句映射对象关系

序号	SQL 语句类型	SQL 语句映射对象
0	OTHER	除下述 SQL 语句类型外的所有 SQL 语句类型。
1	SELECT	SQLCOM_SELECT
2	INSERT	SQLCOM_INSERT，SQLCOM_INSERT_SELECT
3	UPDATE	SQLCOM_UPDATE，SQLCOM_UPDATE_MULTI
4	DELETE	SQLCOM_DELETE，SQLCOM_DELETE_MULTI，SQLCOM_TRUNCATE
5	CREATE	SQLCOM_CREATE_TABLE，SQLCOM_CREATE_INDEX，SQLCOM_CREATE_DB，SQLCOM_CREATE_FUNCTION，SQLCOM_CREATE_USER，SQLCOM_CREATE_PROCEDURE，SQLCOM_CREATE_SPFUNCTION，SQLCOM_CREATE_VIEW，SQLCOM_CREATE_TRIGGER，SQLCOM_CREATE_SERVER，SQLCOM_CREATE_EVENT，SQLCOM_CREATE_ROLE，SQLCOM_CREATE_RESOURCE_GROUP，SQLCOM_CREATE_SRS
6	DROP	SQLCOM_DROP_TABLE，SQLCOM_DROP_INDEX，SQLCOM_DROP_DB，SQLCOM_DROP_FUNCTION，SQLCOM_DROP_USER，SQLCOM_DROP_PROCEDURE，SQLCOM_DROP_VIEW，SQLCOM_DROP_TRIGGER，SQLCOM_DROP_SERVER，SQLCOM_DROP_EVENT，SQLCOM_DROP_ROLE，SQLCOM_DROP_RESOURCE_GROUP，SQLCOM_DROP_SRS
7	ALTER	SQLCOM_ALTER_TABLE，SQLCOM_ALTER_DB，SQLCOM_ALTER_PROCEDURE，SQLCOM_ALTER_FUNCTION，SQLCOM_ALTER_TABLESPACE，SQLCOM_ALTER_SERVER，SQLCOM_ALTER_EVENT，SQLCOM_ALTER_USER，SQLCOM_ALTER_INSTANCE，SQLCOM_ALTER_USER_DEFAULT_ROLE，SQLCOM_ALTER_RESOURCE_GROUP
8	REPLACE	SQLCOM_REPLACE，SQLCOM_REPLACE_SELECT

9	SET	SQLCOM_SET_OPTION，SQLCOM_RESET，SQLCOM_SET_PASSWORD，SQLCOM_SET_ROLE，SQLCOM_SET_RESOURCE_GROUP
10	EXECUTE	SQLCOM_EXECUTE
11	LOGIN	登入数据库行为，不受审计规则约束。
12	LOGOUT	登出数据库行为，不受审计规则约束。
13	CHANGEUSER	更改用户行为，不受审计规则约束。

版权所有：腾讯云计算（北京）有限责任公司

配置事后告警

最近更新时间：2023-12-12 14:40:14

数据库审计功能相关的事件告警已接入腾讯云可观测平台和事件总线，若您在规则模板中设置了风险等级告警，并且选择发送告警，则命中该规则模板的审计日志会触发告警通知给绑定的用户，同时在腾讯云可观测平台，用户也可以查看告警历史、进行告警策略管理（告警开关）及告警屏蔽。为数据库审计配置事件告警，可帮助用户及时获取风险告警，快速定位问题审计日志。
本文介绍如何从腾讯云可观测平台以及事件总线，为已开通数据库审计的实例配置事件告警。

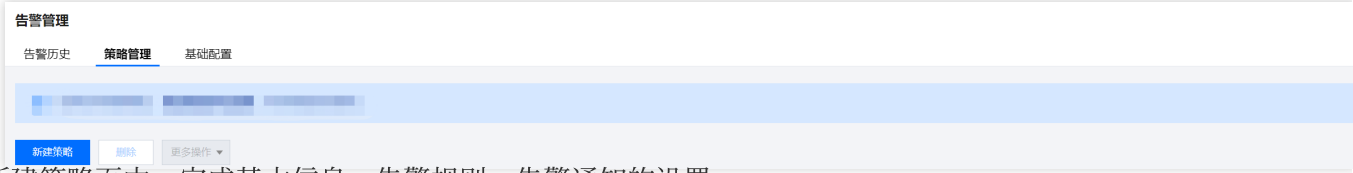
前提条件

已 开通审计服务。
已 提交工单 申请使用事件告警功能（此功能的申请仅支持部署在北京、上海、广州、成都、新加坡地域的实例）。
已 提交工单 申请使用规则审计功能。

通过腾讯云可观测平台配置事件告警

创建告警策略

1. 登录 腾讯云可观测平台控制台，在左侧导航选择**告警管理** > **策略管理**页。
2. 在告警策略列表页，单击**新建策略**。



3. 在新建策略页中，完成基本信息、告警规则、告警通知的设置。

策略类型：选择**云数据库** > **TDSQL-C** > **MySQL**。
告警对象：可通过选择对象所在的地域或搜索对象的实例 ID 找到需要关联的对象实例。
触发条件：找到事件告警，单击**添加事件**，根据实际需要告警的风险等级添加**数据库审计低风险**、**数据库审计中风险**或**数据库审计高风险**的告警事件。
配置告警通知：支持选择系统预设通知模板和用户自定义通知模板，每个告警策略最多只能绑定三个通知模板，自定义通知模板请参见 新建通知模板。
选择系统预设模板

选择通知模板
已选择1个通知模板，还可以选择2个
搜索通知模板
通知模板名称
包含操作
系统预设通知模板
接收人：1个
CPU_CALL
接收人：1个
共 2 条
10 条 / 页
1
/ 1 页
确定
取消

新建模板

4. 确认无误后，单击**完成**。

关联告警对象

创建完告警策略后，您也可以为其关联其他告警对象（需要和此告警策略一致的实例），当命中规则模板中的规则内容，同时风险等级为所添加的等级且规则模板的告警策略设置为**发送告警**的实例，其生成的审计日志将会发送告警通知。

1. 在 告警策略列表页，单击**告警策略名称**，进入管理告警策略页。
2. 在管理告警策略页的**告警对象**栏，单击**新增对象**。
3. 在弹出的对话框，选择您需要关联的告警对象，单击**确定**，即可关联告警对象。

查看告警历史、进行告警策略管理（告警开关）及告警屏蔽

您可通过 腾讯云可观测平台，查看相关事件告警历史，或进行告警策略管理及创建告警屏蔽，相关操作可参考如下指引：

查看告警历史

告警启停

告警屏蔽

通过事件总线配置事件告警

步骤1：开通事件总线

腾讯云事件总线通过访问管理（Cloud Access Management，CAM）来实现权限管理。CAM 是腾讯云提供的权限及访问管理服务，主要用于帮助客户安全管理腾讯云账户下的资源的访问权限。用户可以通过 CAM 创建、管理和销毁用户（组），并使用身份管理和策略管理控制其他用户使用腾讯云资源的权限。使用事件总线 EventBridge 前，您需在产品页开通该服务。主账号开通方法及为子账号授权使用此服务，请参见 开通事件总线。

步骤2：配置 TDSQL-C MySQL 版数据库审计相关事件告警

开通事件总线服务后，需要选择事件源接入方式，目前已支持通过 TDSQL-C MySQL 版数据库审计产生的监控事件作为事件源接入事件总线。

注意：

对于 TDSQL-C MySQL 版产生的告警、审计等运维事件，将全部投递至**云服务事件集**，该投递为默认投递，不支持更改或编辑。

开启腾讯云事件总线服务后，将为您自动在**广州地域**创建默认云服务事件集，TDSQL-C MySQL 版所产生的告警事件（监控事件及审计事件）将自动投递至此。

1. 登录 事件总线控制台。
2. 在上方选择地域为**广州**。
3. 单击云服务事件集下的 **default** 事件集。

4. 在 default 事件集详情页单击**管理事件规则**。

5. 在跳转页面单击**新建**。

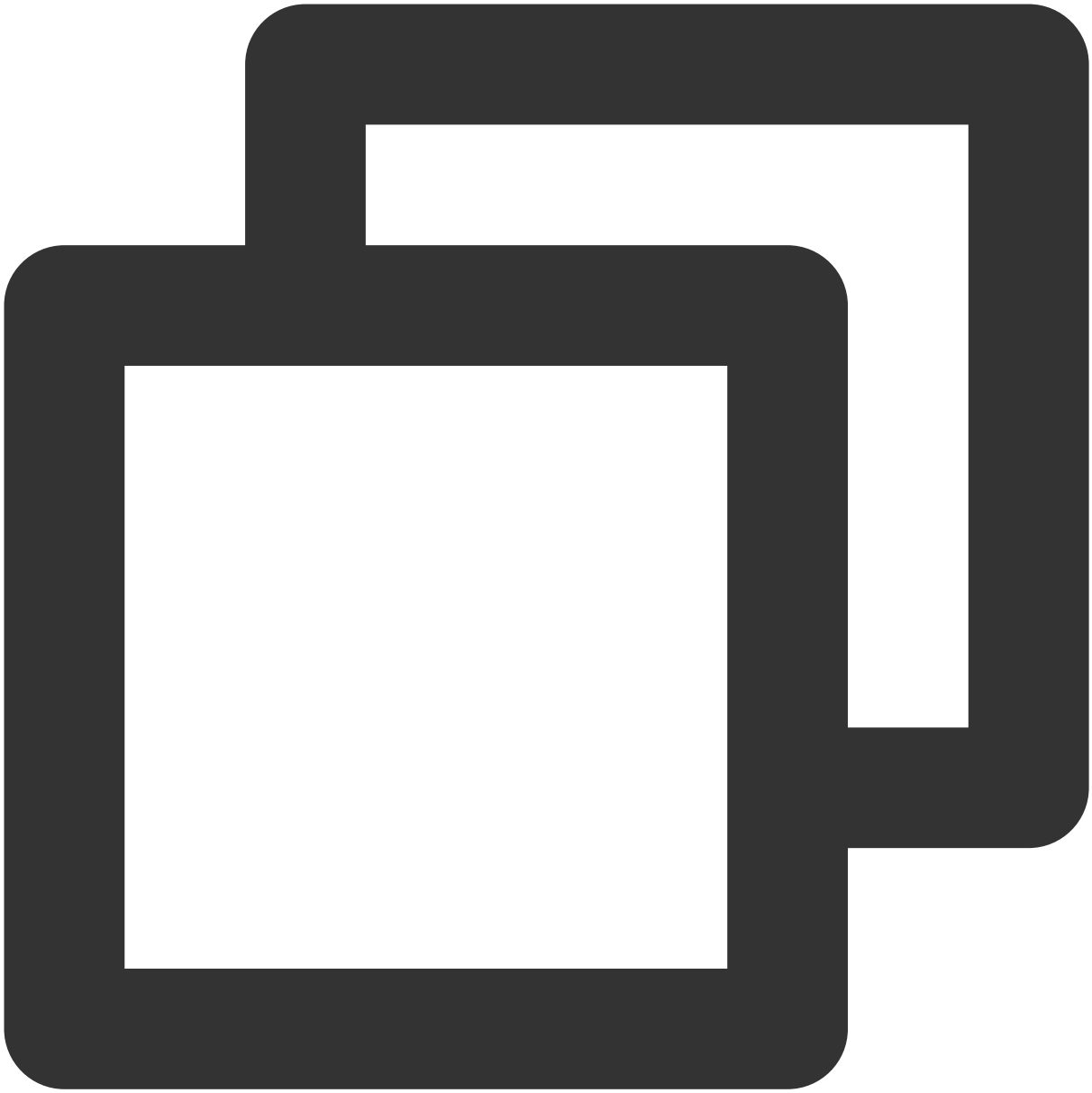
6. 在新建事件规则页面完成如下配置后单击**下一步**。

参数	说明
规则名称	填写规则名称，只能包含字母、数字、下划线、连字符，以字母开头，以数字或字母结尾，2个 - 60个字符
规则描述	填写规则描述，只能包含数字、中英文及常用标点符号，不超过200个字符
标签	自定义是否启用标签，启用后可以对该事件规则添加标签
数据转换	事件数据转换可以帮助您轻松的对事件内容进行简单的处理。例如，您可以对事件中的字段进行提取解析和映射重组后，再投递到事件目标
事件示例	提供了事件结构示例，为配置事件匹配规则做参考，您可以在事件示例选择下找到目标模板以作参考
事件模式	支持表单模式和自定义事件，这里建议使用表单模式更为便捷

云服务类型	选择 TDSQL-C MySQL 版
事件类型	选择需要的，数据库审计相关告警的事件类型（数据库审计低风险、数据库审计中风险、数据库审计高风险）
测试匹配规则	选择事件示例中选择的事件类型模板，然后单击测试匹配规则，测试通过可执行下一步

说明：

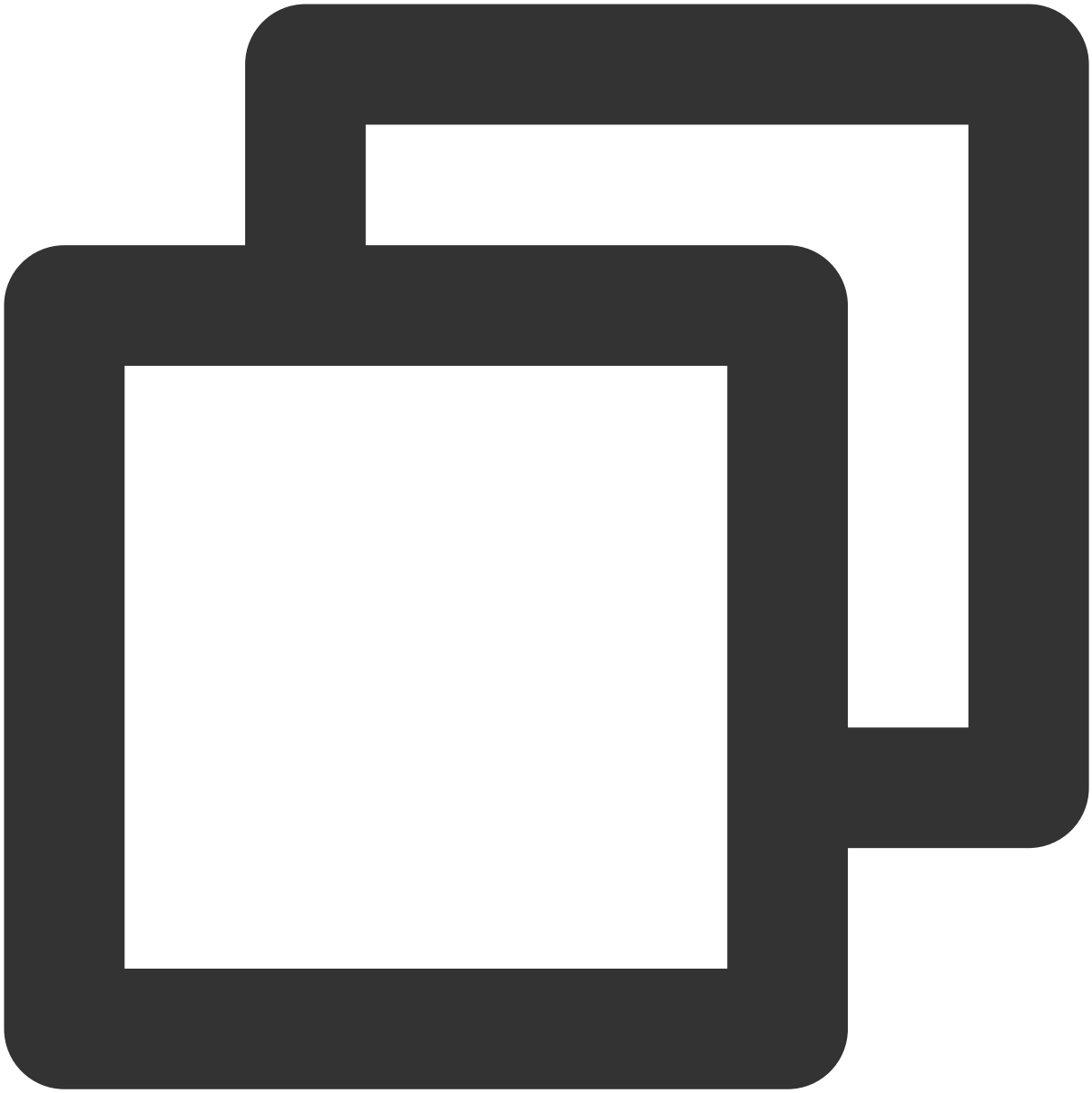
如需接收来自指定实例的事件告警，规则配置为：



```
{
  "source":"cynosdb_mysql.cloud.tencent",
  "subject":"ins-xxxxxx"
}
```

表示所有来自 TDSQL-C MySQL 版并且实例 id 为 ins-xxx 的事件才可以通过规则匹配进行推送，其它事件将被丢弃，无法触达用户。

也可以使用数组模式匹配多个资源：



```
{
  "source":"cynosdb_mysql.cloud.tencent",
  "subject":["ins-xxxxxx","ins-xxxxxx"]
}
```

7. 在事件目标页签完成如下配置，勾选**立即启用事件规则**，单击**完成**。

参数	说明
触发方式	选择消息推送
消息模板	支持选择监控告警模板或通用通知模板
告警内容	支持选择中文或者英文
通知方式	支持选择接口回调、渠道推送或全部方式，此处以选择渠道推送方式为例进行后续设置
接收对象	选择接收用户或用户组
通知时段	自定义通知时间段

接收渠道	勾选接收渠道，短信限500字，电话限350字，过长的事件（可能由过长的实例名称等原因导致）将不会推送。建议同时配置多个渠道

说明：

如需配置多个事件目标，可单击**添加**进行设置。

8. 创建完成后即可在事件规则列表查询和管理该事件规则。

修改审计规则

最近更新时间：2024-06-07 15:44:12

本文为您介绍通过控制台修改审计规则相关操作。

前提条件

已 开通审计服务。

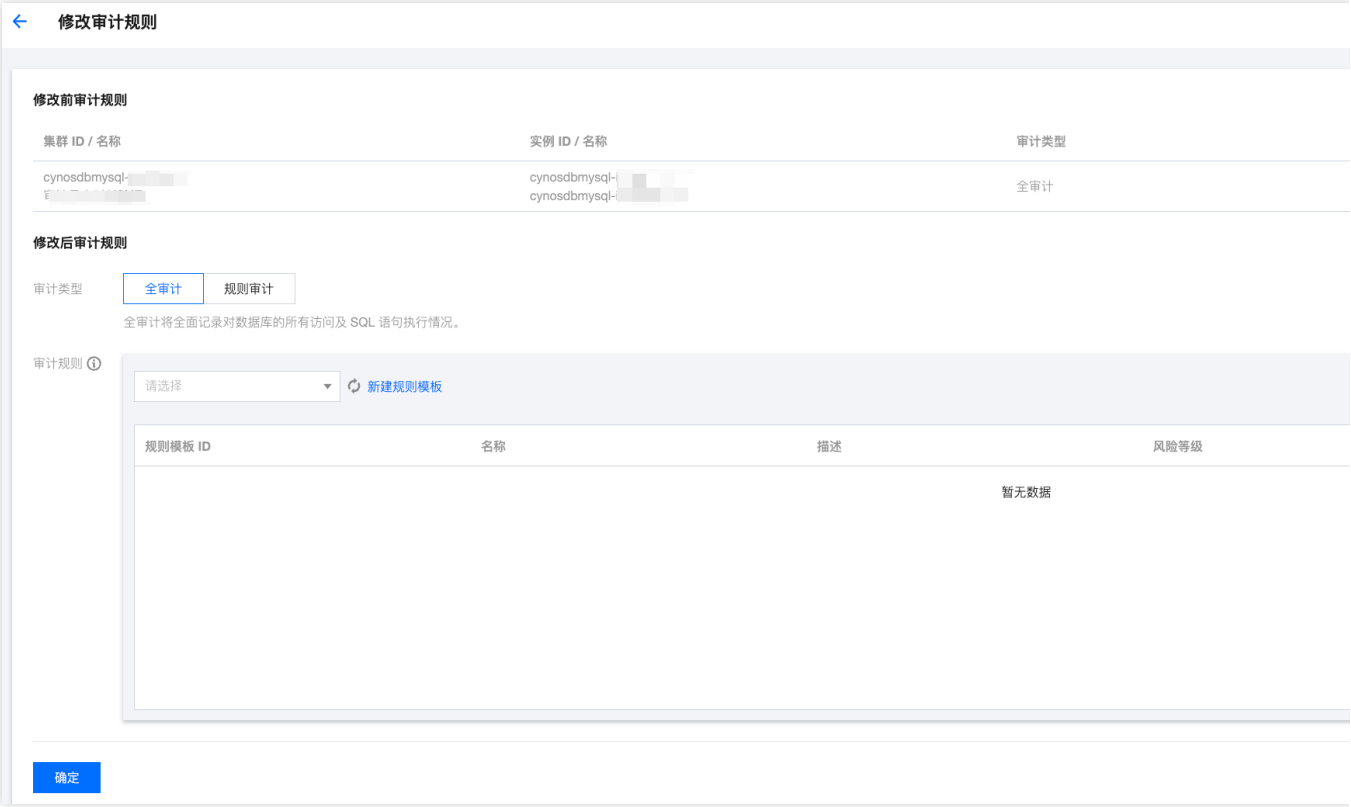
功能说明

审计规则支持从全审计变为规则审计，也支持从规则审计变为全审计。
审计规则修改后，所选实例将会按照修改后的审计规则进行审计规则调整。
审计规则修改包括审计类型、规则模板的修改。

单实例修改审计规则

1. 登录 TDSQL-C MySQL 版控制台。
2. 在左侧导航选择**数据库审计**。
3. 在上方选择**地域**后，在**审计实例**页，单击**审计状态**选择**已开启**选项过滤已开启审计的实例。
4. 在审计实例列表里找到目标集群/实例（也可在搜索框通过资源属性筛选快速查找），在其**操作**列选择**更多** > **修改审计规则**。

5. 在修改审计规则窗口下，完成所需修改（审计类型或审计规则），单击**确定**。



批量修改审计规则

说明：

审计规则支持从全审计变为规则审计，也支持从规则审计变为全审计。

批量修改审计规则后，所选实例将会统一按照修改后的审计规则进行审计规则调整。

审计规则修改包括审计类型、规则模板的修改。

1. 登录 TDSQL-C MySQL 版控制台。
2. 在左侧导航选择**数据库审计**。
3. 在上方选择**地域**后，在**审计实例**页，单击**审计状态**选择**已开启**选项过滤已开启审计的实例。
4. 在审计实例列表里找到目标集群/实例（也可在搜索框通过资源属性筛选快速查找），在审计实例列表页勾选多个目标实例，单击上方**修改审计规则**。

5. 在修改审计规则窗口下，完成所需修改（审计类型或审计规则），单击**确定**。

修改审计服务

最近更新时间：2024-06-18 09:39:17

本文为您介绍通过控制台修改审计服务相关操作。

说明

若选择延长日志保存时长，将会立即生效，若选择缩短日志保存时长，历史超过存储期限的日志将会被立即清除。若设置最近 n 天的数据存储在高频存储中，则超过最近 n 天的数据会自动落冷至低频存储中，延长高频存储时长后，符合保存时长的审计数据会自动从低频存储迁移至高频存储中。

前提条件

已 开通审计服务。

单实例修改审计服务

1. 登录 TDSQL-C MySQL 版控制台。
2. 在左侧导航选择**数据库审计**。
3. 在上方选择**地域**后，在**审计实例**页，单击**审计状态**选择**已开启**选项过滤已开启审计的实例。
4. 在审计实例列表里找到目标实例（也可在搜索框通过资源属性筛选快速查找），在其**操作**列选择**更多** > **修改审计服务**。

5. 在审计服务修改窗口下，修改**日志保存时长**或**高频存储时长**后，单击**确认**。

批量修改审计服务

1. 登录 TDSQL-C MySQL 版控制台。
2. 在左侧导航选择**数据库审计**。
3. 在上方选择**地域**后，在**审计实例**页，单击**审计状态**选择**已开启**选项过滤已开启审计的实例。
4. 在审计实例列表里找到目标实例（也可在搜索框通过资源属性筛选快速查找），在审计实例列表页勾选多个目标实例，单击上方**修改审计服务**。

5. 在审计服务修改窗口下，修改**日志保存时长**或**高频存储时长**后，单击**确认**。

注意

为方便对比，批量修改审计服务窗口会展示修改前后的日志保存时长，修改后，所选实例会统一开始按新的日志保存时长进行调整，请确认无误后再进行修改。

关闭审计服务

最近更新时间：2024-06-18 09:41:04

本文为您介绍通过控制台关闭审计服务相关操作。

注意：

审计服务关闭后，将会停止对实例进行审计且历史审计日志将被清空。

前提条件

已 开通审计服务。

操作步骤

1. 登录 TDSQL-C MySQL 版控制台。
2. 在左侧导航栏选择**数据库审计**。
3. 在上方选择**地域**后，在**审计实例**页，单击**审计状态**选择**已开启**选项过滤已开启审计的实例。
4. 在审计实例列表里找到目标实例（也可在搜索框通过资源属性筛选快速查找），在其**操作**列选择**更多** > **关闭**。

说明：

支持批量关闭审计服务。在审计实例列表页勾选多个目标实例，单击上方**关闭审计服务**。

5. 在关闭审计服务窗口下，检查无误后单击**确定**。

6. 确定后结果提示列会显示关闭结果，单击**查看任务**可跳转至任务列表查询详情。

审计规则模板
查看规则模板列表

最近更新时间：2023-12-12 14:25:17

本文为您介绍通过控制台查看规则模板列表。

查看规则模板列表及查看模板详情

1. 登录 TDSQL-C MySQL 版控制台。
2. 在左侧导航栏选择**数据库审计**。
3. 选择**地域**后，单击**规则模板**。

4. 在**规则模板**列表里找到目标规则模板（也可在搜索框通过资源属性筛选快速查找），在其**操作**列单击**详情**。
5. 在弹窗下，可切换查看该规则模板的**基本信息**、**参数设置**、**关联实例**及**修改历史**情况。

工具列表

工具	说明
搜索框	单击 进行过滤，支持按照资源属性（规则模板 ID、名称）进行过滤，多个关键字用竖线分隔，多个过滤标签用回车键分隔。
修改历史	单击 可跳转至修改历史页面，可全局查看某地域下的规则模板修改历史记录。
刷新	单击 可刷新列表。

模板列表字段

字段	说明
规则模板 ID	展示已创建的规则模板 ID。
名称	展示已创建的规则模板名称。
风险等级	展示对应规则模板的风险等级（低风险、中风险、高风险），支持筛选。
告警策略	展示对应规则模板的告警策略（不发送告警、发送告警），支持筛选。
关联实例	展示对应规则模板绑定的实例个数，点击实例个数可显示关联实例的明细，包括实例 ID、审计类型等。
描述	展示已创建的规则模板的描述备注。
创建时间	展示对应规则模板的创建时间，统计格式为 年-月-日 时：分：秒。
更新时间	展示对应规则模板的最新更新时间。
操作	详情，可查看规则模板详情**基本信息**、**参数设置**、**关联实例**、**修改历史**。 编辑，可修改规则模板内容。 删除，删除规则模板。

相关操作

新建规则模板
修改规则模板
删除规则模板

新建规则模板

最近更新时间：2024-06-07 16:05:49

本文为您介绍通过控制台新建规则模板。

说明：

2023年09月25日起，规则模板与审计实例的关系由**初始化**调整为**强关联**，修改规则模板的内容**会同步影响**已绑定该规则模板的实例所应用的审计规则。

规则内容的同一个参数字段中最多可配置5个特征串，多个特征串之间使用英文竖线“|”分隔。

操作步骤

1. 登录 TDSQL-C MySQL 版控制台。
2. 在左侧导航栏选择**数据库审计**。
3. 选择地域后，单击**规则模板**。
4. 在模板列表，单击**新建规则模板**。

5. 在新建规则模板窗口下完成如下配置后，单击**确定**。

参数	说明
规则模板名称	仅支持数字、英文大小写字母、中文以及特殊字符 -_./()[]（）+=：:@，不能以数字开头，最多30个字符。
规则内容	设置规则内容（参数字段、匹配类型、特征串），详细设置说明请参见以下 规则内容详情及示例 介绍。 **说明：** 在规则内容下可单击添加增加参数字段。 在规则内容下的操作列可单击删除去掉不需要的参数字段及条件，但至少需保留一个参数字段及条件。
风险等级	为新建的规则模板选择风险等级，支持选项为低风险、中风险、高风险。
告警策略	为新建的规则模板选择告警策略，支持选项为不发送告警、发送告警。 **说明：** 请前往 腾讯云可观测平台->告警管理 中配置告警规则及告警通知，详情请参考 配置事后告警。
规则模板备注	仅支持数字、英文大小写字母、中文以及特殊字符-_./()[]（）+=：:@，不能以数字开头，最多200个字符。

规则内容详情及示例

说明：

可以配置单个或多个规则。

不同规则之间，是与的关系，表示需同时满足。

一个规则内不同特征串之间是或的关系，表示多者间只需满足其中一个。

同一个规则只可加一条，例如同是数据库名，在一个模板中要么仅支持包含，要么仅支持不包含。

参数字段	匹配类型	特征串
客户端 IP	包含、不包含、等于、不等于、正则	最多可配置5个客户端 IP，使用英文竖线分隔。
用户账号	包含、不包含、等于、不等于、正则	最多可配置5个用户名，使用英文竖线分隔。
数据库名	包含、不包含、等于、不等于、正则	最多可配置5个数据库名，使用英文竖线分隔。
SQL 命令详情	包含、不包含	最多可配置5句 SQL 命令，使用英文竖线分隔。
SQL 类型	等于、不等于	可选类型：Alter、Changeuser、Create、delete、drop、execute、insert、login、logout、other、replace、select、set、update，最多可选择5个 SQL 类型。
影响行数	大于、小于	选择影响行数。
返回行数	大于、小于	选择返回行数。
扫描行数	大于、小于	选择扫描行数。
执行时间	大于、小于	选择执行时间，单位微秒。

示例

若用户设置的规则内容为：数据库名，包含 a、b、c，客户端 IP 包含 IP1、IP2、IP3，则该规则过滤出的审计日志为：数据库名包含 a 或 b 或 c 且客户端 IP 包含 IP1 或 IP2 或 IP3 的审计日志。

版权所有：腾讯云计算（北京）有限责任公司

修改规则模板

最近更新时间：2024-06-07 16:09:24

本文为您介绍通过控制台修改数据库审计规则模板。

说明：

2023年09月25日起，规则模板与审计实例的关系由**初始化**调整为**强关联**，修改规则模板的内容**会同步影响**已绑定该规则模板的实例所应用的审计规则。

规则内容的同一个参数字段中最多可配置5个特征串，多个特征串之间使用英文竖线“|”分隔。

操作步骤

1. 登录 TDSQL-C MySQL 版控制台。
2. 在左侧导航栏选择**数据库审计**。
3. 选择地域后，单击**规则模板**。

4. 在规则模板列表里找到目标规则模板（也可在搜索框通过资源属性筛选快速查找），在其**操作**列单击**编辑**。
5. 在编辑规则模板窗口下，修改相关配置后，单击**确定**。

参数	说明
规则模板名称	仅支持数字、英文大小写字母、中文以及特殊字符 -_./()[]（）+=：:@，不能以数字开头，最多30个字符。
规则内容	设置规则内容（参数字段、匹配类型、特征串），详细设置说明请参见以下 规则内容详情及示例 介绍。 **说明：** 在规则内容下可单击添加增加参数字段。 在规则内容下的操作列可单击删除去掉不需要的参数字段及条件，但至少需保留一个参数字段及条件。
风险等级	为该规则模板选择风险等级，支持选项为低风险、中风险、高风险。
告警策略	为该规则模板选择告警策略，支持选项为不发送告警、发送告警。 **说明：** 请前往 腾讯云可观测平台->告警管理 中配置告警规则及告警通知，详情请参考 配置事后告警。
规则模板备注	仅支持数字、英文大小写字母、中文以及特殊字符-_./()[]（）+=：:@，不能以数字开头，最多200个字符。

规则内容详情及示例

说明：

可以配置单个或多个规则。

不同规则之间，是与的关系，表示需同时满足。

一个规则内不同特征串之间是或的关系，表示多者间只需满足其中一个。

同一个规则只可加一条，例如同是数据库名，在一个模板中要么仅支持包含，要么仅支持不包含。

参数字段	匹配类型	特征串
客户端 IP	包含、不包含、等于、不等于、正则	最多可配置5个客户端 IP，使用英文竖线分隔。
用户账号	包含、不包含、等于、不等于、正则	最多可配置5个用户名，使用英文竖线分隔。
数据库名	包含、不包含、等于、不等于、正则	最多可配置5个数据库名，使用英文竖线分隔。
SQL 命令详情	包含、不包含	最多可配置5句 SQL 命令，使用英文竖线分隔。
SQL 类型	等于、不等于	可选类型：Alter、Changeuser、Create、delete、drop、execute、insert、login、logout、other、replace、select、set、update，最多可选择5个 SQL 类型。
影响行数	大于、小于	选择影响行数。
返回行数	大于、小于	选择返回行数。
扫描行数	大于、小于	选择扫描行数。
执行时间	大于、小于	选择执行时间，单位微秒。

示例

若用户设置的规则内容为：数据库名，包含 a、b、c，客户端 IP 包含 IP1、IP2、IP3，则该规则过滤出的审计日志为：数据库名包含 a 或 b 或 c 且客户端 IP 包含 IP1 或 IP2 或 IP3 的审计日志。

版权所有：腾讯云计算（北京）有限责任公司

删除规则模板

最近更新时间：2023-12-12 15:03:05

本文为您介绍通过控制台删除数据库审计规则模板。

说明：

若规则模板有关联实例，则不支持删除，仅规则模板没有绑定实例时，才支持被删除，规则模板删除后，将不能应用于实例。

操作步骤

1. 登录 TDSQL-C MySQL 版控制台。
2. 在左侧导航栏选择**数据库审计**。
3. 选择地域后，单击**规则模板**。
4. 在规则模板列表里找到目标规则模板（也可在搜索框通过资源属性筛选快速查找），在其**操作**列单击**删除**。

5. 在弹窗中单击**确定**。

查看审计任务

最近更新时间：2023-02-23 11:06:12

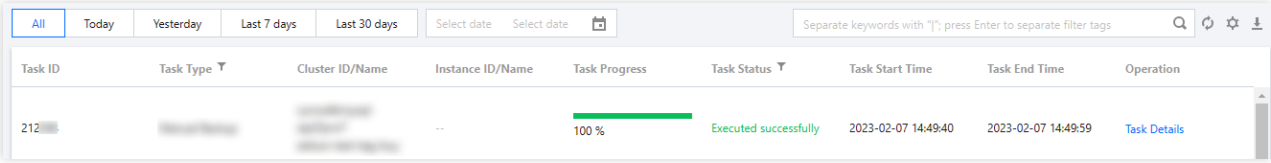
您可以通过控制台查看审计任务详情，方便您了解对实例进行开启、关闭审计服务、修改审计服务、修改审计规则等的任务进度。本文为您介绍如何通过控制台查看审计任务。

任务类型

通过任务列表，您可查看的审计任务类型包括：开通审计服务、关闭审计服务、修改审计服务、修改审计规则、修改审计规则模板、删除审计规则模板等。

查看审计任务

1. 登录 TDSQL-C MySQL 版控制台。
2. 在左侧导航栏单击**任务列表**进入任务列表界面。
3. 在上方选择对应地域。
4. 您可以在任务列表直接查找或检索关键字查询对应审计任务并了解任务详情。



检索关键字

在任务列表，您可以通过搜索框检索关键字快速查找到目标任务，搜索框内支持按照任务 ID、集群 ID、实例 ID、集群名称、实例名称的资源属性来进行搜索，多个关键字用“|”分隔，多个过滤标签用回车键分隔。

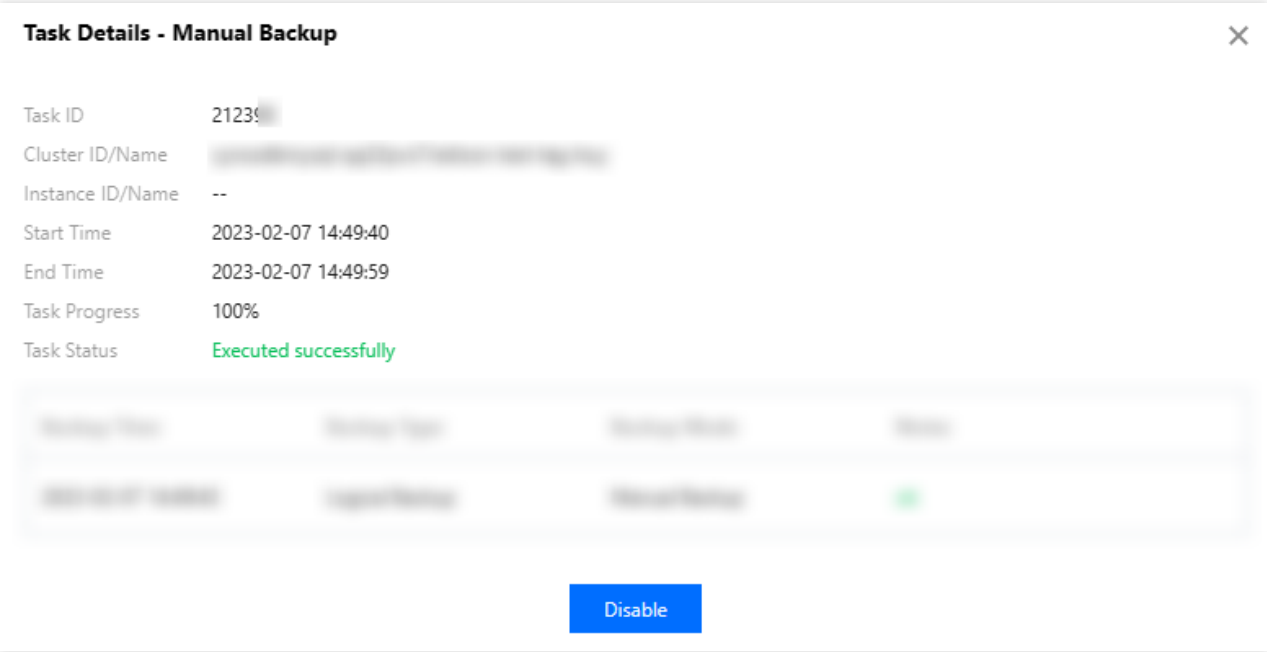
下载任务数据

单击检索框后的下载按钮

，可下载当前页的数据或者当前查询条件下的数据。

查看任务详情

在任务列表找到需要查询审计任务详情的任务项，在其**操作**列单击**任务详情**。



授权子用户使用数据库审计

最近更新时间：2023-07-27 15:37:38

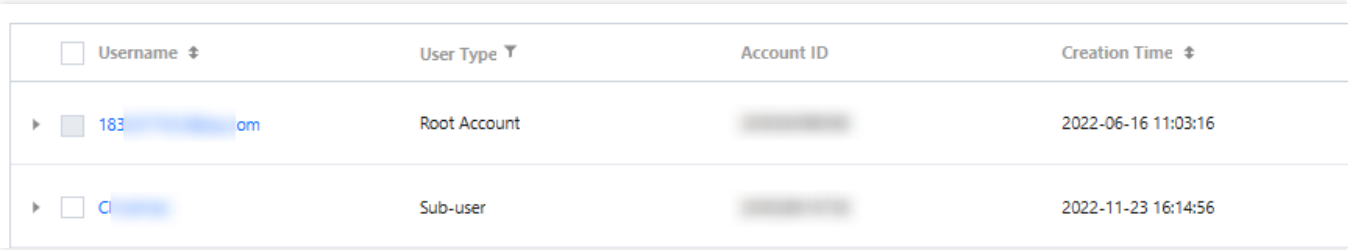
默认情况下，子用户没有使用 TDSQL-C MySQL 版数据库审计的权利。因此用户需要创建策略来允许子用户使用数据库审计。若您不需要对子用户进行 TDSQL-C MySQL 版数据库审计相关资源的访问管理，可以忽略此文档。

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号下资源的访问权限。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。

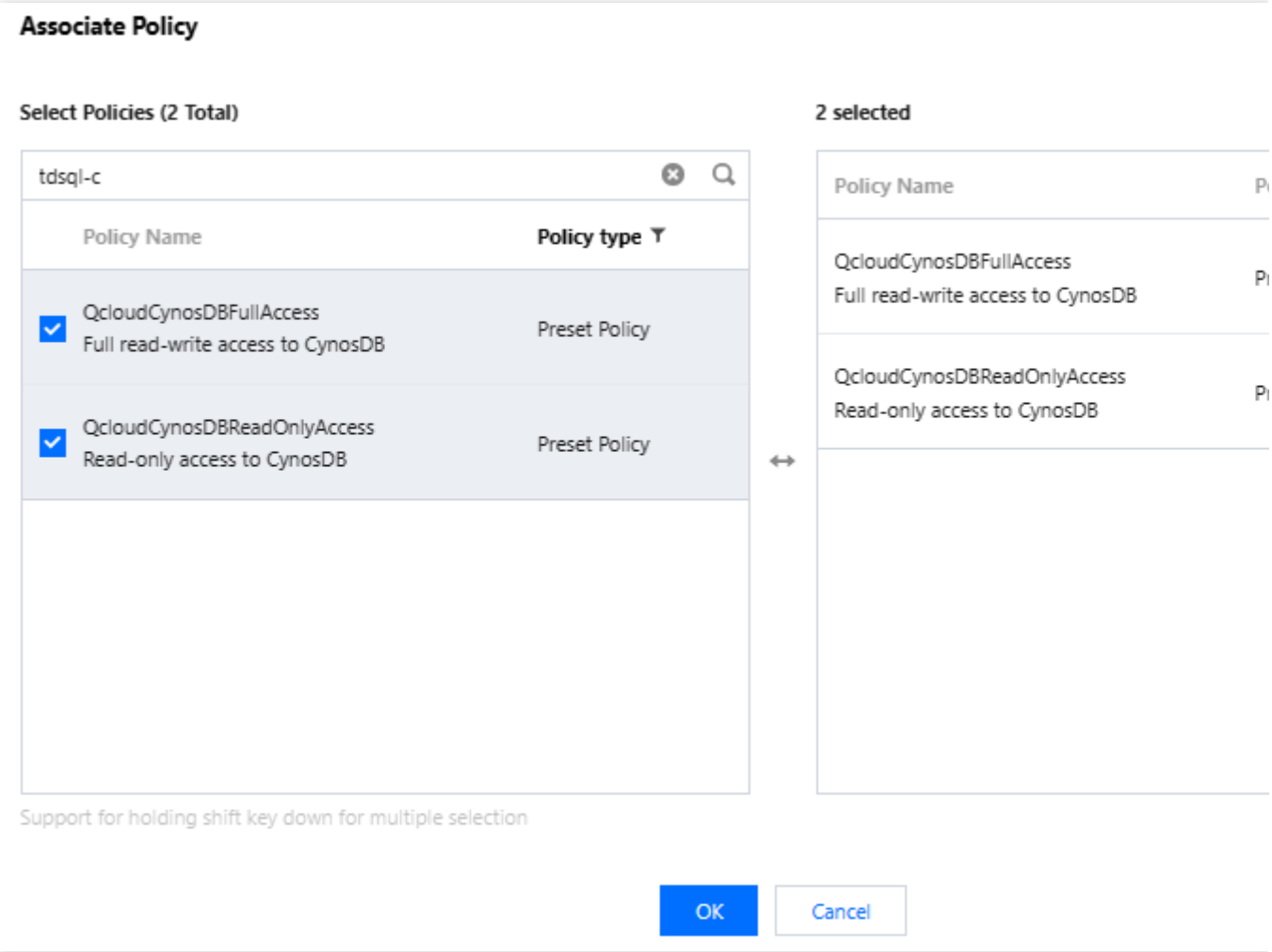
当您使用 CAM 的时候，可以将策略与一个用户或一组用户关联起来，策略能够授权或者拒绝用户使用指定资源完成指定任务。有关 CAM 策略的更多基本信息，请参见 策略语法。

操作步骤

1. 以主账号身份登录 访问管理控制台，在用户列表选择对应子用户，单击**授权**。



2. 在弹出的对话框，选择 **QcloudCynosDBFullAccess 云数据库 TDSQL-C(CynosDB)全读写访问权限**或 **QcloudCynosDBReadOnlyAccess 云原生数据库 TDSQL-C(CynosDB)只读访问权限**预设策略，单击**确定**，即可完成子用户授权。


Associate Policy
Select Policies (2 Total)
2 selected
tdsql-c
Policy Name
Policy type
QcloudCynosDBFullAccess
Full read-write access to CynosDB
Preset Policy
QcloudCynosDBReadOnlyAccess
Read-only access to CynosDB
Preset Policy
Policy Name
QcloudCynosDBFullAccess
Full read-write access to CynosDB
QcloudCynosDBReadOnlyAccess
Read-only access to CynosDB
Support for holding shift key down for multiple selection
OK
Cancel