TDSQL-C MySQL 版

数据安全审计

腾讯云

【联系我们】

我们致力于为您提供个性化的售前购买咨询服务，及相应的技术售后服务，任何问题请联系 4009100100或95716。

文档目录

数据安全审计
数据安全审计简介

最近更新时间：2026-08-21 18:00:31

数据安全态势管理 DSPM 和数据库构建了云数据安全统一运营视图，您可以全面掌握云数据资产与敏感数据的分布及访问情况。结合云原生行为日志与动态风险监测引擎，系统能够对外网与内网入口实施从资产梳理、访问权限控制到风险识别的全链路监测，实现数据资产的可视化、可控化与精准防护，确保数据在云上安全合规，真正做到“看得见、管得住、防得准”。

数据安全主要问题

- **数据资产有盲区，敏感数据分布不明：**数据库实例分散于不同地域、VPC 和业务部门，缺乏统一的资产台账；库表字段数量庞大，敏感数据分布位置不明，安全团队难以精准定位保护对象。
- **数据访问行为不可见，溯源困难：**数据库的每一次查询、导出、修改操作缺乏统一审计视图，公网 IP 访问、异常时段操作、批量下载等高危行为难以被及时发现；一旦发生数据泄露事件，管理员需手动跨平台拼接日志，溯源周期长、证据链不完整，极易错过处置黄金窗口。
- **异常操作难识别，风险响应滞后：**传统规则引擎仅通过单点特征匹配（如登录失败次数）进行告警，无法识别组合行为风险（如“公网访问 + 敏感数据 + 批量导出”），导致告警数量庞大但有效信息稀少，安全团队陷入“告警疲劳”，难以判断处置优先级，快速收敛影响面。
- **合规审计压力大，敏感数据处理缺乏依据：**面对合规要求，企业需要对数据进行分类分级管理，并具备全量操作审计能力。然而手动梳理资产、逐表逐字段识别敏感数据、人工审计操作日志的工作量巨大，合规成本高且难以持续。

应用场景

- **核心数据资产保护：**对云数据库中的敏感数据（如个人信息、交易记录）进行全量访问审计，为数据泄露、越权访问等事件提供溯源依据。
- **等保合规与法规遵从：**满足法律法规对日志留存和审计能力的要求，以及金融、运营商等行业对等保标准的合规审计需求。
- **数据库攻击与风险监测：**实时监测并告警针对数据库的恶意行为，实现事中阻断与事后追责。
- **运维与开发安全审计：**对运维人员通过控制台等工具执行的高危操作（如 DROP / ALTER、批量导出）进行审计。同时，识别开发、测试环境中因敏感数据暴露或违规导出引发的风险。

优势

- **访问关系一目了然：**访问关系可视化，清晰展示。
- **全量操作可追溯：**记录每一次数据库操作，支持事后还原。
- **风险实时监控：**异常访问、敏感操作实时监测，及时发现潜在风险。
- **敏感数据自动发现：**主动识别敏感数据分布，为权限收敛提供依据。

计费说明

数据安全审计采用包年包月的预付费模式，按照套餐形式售卖，您可根据实际需求选择合适的套餐数量，计费项及计费标准如下表，详细计费说明请参见 数据安全审计计费说明 。

> **说明：**
> 以下套餐中，每一套里包含：一个数据库实例、1000条 SQL/秒吞吐量、2000万条在线 SQL 语句存储、100GB存储空间。

计费项	规格	单价
企业版	1 - 3套	1950元/套/月
	4 - 20套	1800元/套/月
	21 - 50套	1700元/套/月
	51 - 100套	1600元/套/月
	101 - 200套	1500元/套/月
	201 - 300套	1400元/套/月
	301 - 400套	1300元/套/月
	401 - 500套	1200元/套/月
	500套以上（不包含500）	1000元/套/月
日志存储扩展包	1TB	1000元/月

支持版本

数据库类型	版本		安全审计	数据识别
TDSQL-C MySQL 版	预置资源	事务集群 - MySQL 5.7	✓	✓
		事务集群 - MySQL 8.0	✓	✓
		只读实例	✓	✓
	Serverless	Serverless - MySQL 5.7	✓	✓
		Serverless - MySQL 8.0	✓	✓

支持地域

TDSQL-C MySQL 版支持数据安全审计的地域为：广州、上海、北京、南京、成都、重庆、上海金融、北京金融、深圳金融。

相关文档

相关功能	说明	文档指引
购买数据安全审计	介绍如何通过控制台购买数据安全审计	购买数据安全审计
开启或关闭数据安全审计	介绍如何通过控制台开启 / 关闭数据安全审计	开启或关闭数据安全审计
数据识别	介绍数据安全审计的数据识别能力相关操作	数据识别
拓扑访问	介绍数据安全审计的访问管理能力	访问拓扑
审计日志	介绍数据安全审计的审计日志能力	审计日志
告警	介绍数据安全审计的告警能力	告警
风险	介绍数据安全审计的风险监测能力	风险

购买数据安全审计

最近更新时间：2026-08-21 18:00:31

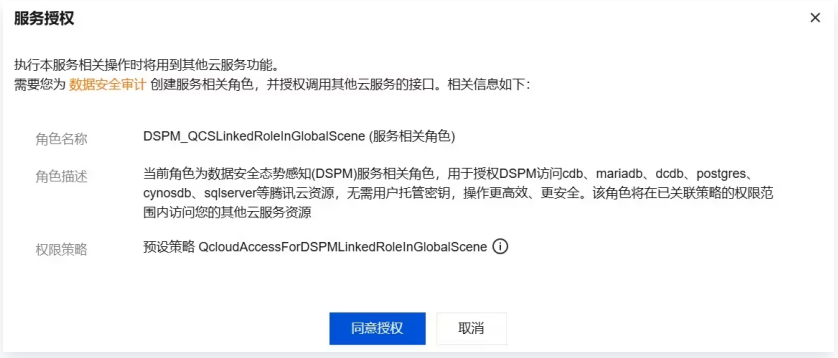
本文为您介绍如何通过控制台购买数据安全审计。

前提条件

已 创建集群 。

操作步骤

1. 登录 TDSQL-C MySQL 版控制台 ，在左侧导航栏单击**数据安全审计**。
2. 在数据安全审计页面单击**开启安全审计**。
3. 在弹窗中阅读服务授权信息，单击**同意授权**。



4. 在弹窗中选择需要购买的配置，单击**确定**，完成付费后即可成功购买数据安全审计。

参数	说明
审计实例	选择审计实例的配额数量，默认为1个，设置范围：1 - 9999，推荐设置为大于等于5个。设置后支持修改。
日志存储	设置日志存储量，所有数据库实例共用此空间，设置范围：0 - 9999TB。设置后支持扩容或缩容。
自动续费	选择是否开启自动续费，若未开启自动续费，在设置完成后也支持手动开启。 **说明：** 若未开启自动续费，在设置完成后，也可在**数据安全审计**页面 > **用量管理** > **续费方式**后单击**开启自动续费**。

开启或关闭数据安全审计

最近更新时间：2026-08-21 18:00:31

本文为您介绍如何通过控制台开启/关闭数据安全审计。

前提条件

已 创建集群 。
已 购买数据安全审计 。

开启数据安全审计

对目标数据库资产开启安全审计，开启后系统将实时监测该资产的安全状态，包括访问行为、违规操作等，并生成告警与风险信息。

1. 登录 TDSQL-C MySQL 版控制台 ，在左侧导航栏单击**数据安全审计**。
2. 在实例列表下找到目标实例，单击其操作列的**开启安全审计**。

3. 在弹窗中，确认需要开启的实例 ID / 名称、地域、内网地址，以及消耗配额、可用配额，然后单击**确定**。

> **说明：**
> - 开启安全审计将消耗 License 授权资产数，请确认剩余授权额度充足。
> - 开启安全审计后，系统需要短暂时间初始化监测策略，期间可能存在少量延迟。
> - 开启安全审计是查看告警信息和风险信息的前提条件，未开启时无法产生监测数据。

关闭数据安全审计

对已开启安全审计的数据库资产关闭安全监测，关闭后系统将不再审计该资产，也无法查看该资产的新增审计日志。

1. 登录 TDSQL-C MySQL 版控制台 ，在左侧导航栏单击**数据安全审计**。
2. 在实例列表下找到目标实例，鼠标移动到目标实例行，单击其安全审计状态字段下的**关闭**。

3. 在弹窗中，确认需要关闭的实例 ID / 名称、地域、内网地址，然后单击**确定**。

> **说明：**
> 单击确认后，将关闭所选实例的安全防护，停止对实例进行安全审计，且历史审计日志将被清空。

访问拓扑

最近更新时间：2026-08-21 18:00:31

数据安全审计访问管理模块，通过“来源 IP 视角”与“实例视角”的双维度互补治理，实现对数据库访问行为的精细化管控。支持访问行为的可视化展示（如访问拓扑图）、IP / 账号打标操作，实现精细化访问控制。从“来源 IP”和“实例”双维度管控访问行为，解决“谁能访问、从哪访问、访问什么”的核心问题，避免粗放式访问控制导致的安全漏洞。

管控视角	描述	适用场景
来源 IP 视角	以访问发起端的来源 IP 为核心管控维度，整合该 IP 对数据库实例的访问数据，提供访问拓扑可视化、IP / 账号精准打标及安全组策略快速调整能力，实现对访问发起端的集中精细化管控。	排查单一 IP 的跨实例访问风险、批量标记某类访问端。
实例视角	以访问目标端的数据库实例为核心资源维度，整合来源 IP 对该实例的访问数据，提供资产访问拓扑可视化、IP / 账号精准打标及安全组策略快速调整能力，实现对访问目标端的集中精细化管控。	梳理单一实例的全量访问来源、针对核心实例做专项管控。

来源 IP 视角

1. 登录 TDSQL-C MySQL 版控制台，在左侧导航栏单击**数据安全审计**。
2. 在数据安全审计页面，选择**访问管理 > 来源 IP 视角**。

3. 在来源 IP 视角标签页面，可以查看**来源 IP / 地域、IP 类型 / 打标、实例 ID / 名称、地域、访问用户 / 类型、最近访问时间**等信息。

IP 访问拓扑

以可视化图谱的形式，直观展示单个来源 IP 与所有关联账号、数据库实例之间的访问关系、访问频率及安全状态。在来源 IP 视角列表，单击目标 IP 对应操作列的 **IP 访问拓扑**，可查看该 IP 与关联数据库实例的访问关系图谱。

IP 打标

为目标来源 IP 添加预设或自定义标签，实现对 IP 的分类管控，便于后续风险监测时进行差异化判定。

1. 在来源 IP 视角列表，单击目标 IP 对应操作列的**更多 > 来源 IP 打标**。

2. 在来源 IP 打标窗口，编辑来源 IP 备注，单击**确定**完成标记。

> **说明：**
> 来源 IP 视角和实例视角的打标操作是相互联动的，在来源 IP 视角为某 IP 打标后，在实例视角查看该 IP 时，打标状态会同步更新；反之亦然。

账号打标

为目标来源 IP 访问数据库时使用的账号添加预设或自定义标签，实现对访问账号的分类管控，便于后续审计和风险排查。

1. 在来源 IP 视角列表，单击目标 IP 对应操作列的**更多 > 账号打标**。

2. 在账号打标窗口，选择账号类型，编辑账号备注信息，单击**确定**完成标记。

> **说明：**
> 可以编辑类型为“自建账号”的访问账号类型，若当前访问账号为云主账号 / 子账号，系统将自动识别，无需手动编辑。

修改安全组策略

快速跳转至目标 IP 关联的数据库实例资产页面，直接修改安全组策略，实现对该 IP 访问权限的快速管控（允许 / 拒绝访问）。

在来源 IP 视角列表，单击目标 IP 对应操作列的**更多 > 修改安全组策略**，可前往数据库实例资产页面修改安全组策略。

实例视角

1. 登录 TDSQL-C MySQL 版控制台，在左侧导航栏单击**数据安全审计**。
2. 在数据安全审计页面，选择**访问管理 > 实例视角**。

3. 在实例视角页面，可查看**实例 ID / 名称、地域、访问用户 / 类型、来源 IP / 类型、最近访问时间**等信息。

资产访问拓扑

以可视化图谱的形式，直观展示单个数据库实例的所有访问来源 IP、关联访问账号之间的访问关系、访问频率及风险状态。

在实例视角列表，单击目标实例对应操作列的**资产访问拓扑**，可查看该实例的所有访问来源 IP、关联账号的拓扑关系。

IP 打标

为访问目标实例的指定来源 IP 添加预设或自定义标签，实现对该实例访问 IP 的精准分类管控，便于后续风险监测和审计。

1. 在实例视角列表，单击目标实例对应操作列的**更多 > 来源 IP 打标**。

2. 在来源 IP 打标窗口，编辑来源 IP 备注，单击**确定**完成标记。

> **说明：**

> 来源 IP 视角和实例视角的打标操作是相互联动的，在来源 IP 视角为某 IP 打标后，在实例视角查看该 IP 时，打标状态会同步更新；反之亦然。

账号打标

为访问目标实例的指定账号添加预设或自定义标签，实现对该实例访问账号的精准分类管控，便于后续风险排查和权限审计。

1. 在实例视角列表，单击目标实例对应操作列的**更多 > 账号打标**。

2. 在账号打标窗口，选择账号类型，编辑账号备注信息，单击**确定**完成标记。

> **说明：**
> 可以编辑类型为“自建账号”的访问账号类型，若当前访问账号为云主账号 / 子账号，系统将自动识别，无需手动编辑。

修改安全组策略

快速跳转至目标数据库实例的资产页面，直接修改安全组策略，实现对该实例所有访问来源 IP 的管控。
在实例视角列表，单击目标实例对应操作列的**更多 > 修改安全组策略**，可前往数据库实例资产页面修改安全组策略。

数据识别

最近更新时间：2026-08-21 18:00:32

数据分类分级为数据安全态势管理核心治理模块，为数据资产合规盘点、敏感数据管控、重要数据专项防护等业务场景提供能力支撑。

相关操作

操作项		适用场景
开启数据识别		对目标数据库资产启用数据识别功能，系统将基于分类分级模板自动扫描敏感数据。
查看数据识别结果		查看数据识别扫描后的分类分级分布、敏感数据详情及统计信息。
分类分级管理	新建分类分级模板	当系统内置模板无法满足业务需求时，可自定义创建数据分类和分级体系。
	切换分类分级模板	在不同业务场景下更换当前使用的分类分级模板。
	复制分类分级模板	基于已有模板快速创建新模板，复用其分类和分级配置。
	新建数据项	定义在分类分级识别中具体的敏感数据类型（如身份证号、手机号等）。

开启数据识别

1. 登录 TDSQL-C MySQL 版控制台，在左侧导航栏单击**数据安全审计**。
2. 在实例列表标签页中，选择目标数据库资产，单击操作列中的**数据识别**。

3. 在数据识别配置窗口中，选择**立即识别**或**周期识别**（选择周期识别时需配置识别频率，如按天、按周、按月，以及配置识别周期），配置完成后，单击**确定**。
4. 识别成功后将自动刷新数据库资产库表详情，同时新增数据资产内容标签。

查看分类分级结果

1. 在实例列表标签页面，找到目标数据库资产，单击其**实例 ID**。

2. 在实例详情页面，单击**数据识别**标签。
3. 在数据识别标签页面，将会显示当前分类分级模板下的分类分级详情，单击**数据名**、**表名**，可查看具体的数据库、表、字段的分类分级识别情况。

新建分类分级模板

分类分级模板是通过配置分类、分级、数据项的关联关系而生成的标准化数据分类分级标准。作为数据分类分级识别统一标准。

1. 登录 TDSQL-C MySQL 版控制台，在左侧导航栏单击**数据安全审计**。
2. 在数据安全审计页面，单击**分类分级管理**，打开分类分级管理面板。

3. 在分类分级标签页中，单击**新建模板**。
4. 在弹出的新建模板窗口中，配置模板基本信息：

配置项	说明
模板名称	自定义模板名称，不超过64个字符。
描述	分类分级模板描述，不超过200个字符。
分级方案	用于模板配置时向数据项关联相对应的分级，仅支持从已有分级方案中选择。若当前没有符合需求的分级方案，可单击**新建分级方案**，快速创建分级方案。

5. 单击**确定**，即可成功创建分类分级模板。
6. 创建完成后，在分类分级标签页中，选择创建好的模板，单击**配置**，对分类分级模板进行配置。

> **说明：**
> 系统内置模板由系统默认配置；自定义模板支持手动配置。

7. 在模板配置页面，单击按钮“+”，添加需要的分类。
8. 分类添加成功后，选择目标分类，单击**添加数据项**。
9. 在弹出的添加数据项窗口中，选择需要关联分类的数据项并为每条数据项配置分级。
10. 根据需要重复上述步骤，为模板添加多个分类及数据项。即可完成创建一个分类分级模板。

切换分类分级模板

应用中的模板是全局适用的，您可以通过切换模板来选择符合需求的分类分级模板。

1. 在分类分级标签页中，选择需要应用的模板，单击右上角的**切换应用此模板**。

2. 在确认窗口中，单击**确定**，即可切换成功。

> **说明：**
> 切换后立即生效，仅影响新的数据识别结果，历史扫描数据记录保留。

复制分类分级模板

支持通过复制模板，快速创建并基于复制的模板进行修改调整。

1. 在分类分级标签页中，选择需要应用的模板，单击**复制**。

2. 在复制模板窗口中，输入模板名称、描述，单击**确定**，即可复制成功。

> **说明：**
> 系统内置模板不支持编辑和删除。如需基于内置模板进行调整，请使用复制功能创建副本后修改。

新建数据项

数据项是用于识别敏感数据的最小规则单元，通过关键字、正则表达式等匹配逻辑判定字段敏感属性，是自动化扫描识别敏感数据的核心规则依据。系统内置了**797条**数据项，同时也支持自定义新建。

1. 登录 TDSQL-C MySQL 版控制台，在左侧导航栏单击**数据安全审计**。
2. 在数据安全审计页面，单击**分类分级管理**，打开分类分级管理面板。
3. 在分类分级管理窗口中，单击**数据项**标签页。

4. 在数据项页签中，单击**新建数据项**。

5. 在新建数据项页面，配置相应的数据项配置项，单击**确定**即可新建成功。

参数		说明
基本信息	数据项名称	数据项名称是分类-数据项的标识符，用于在系统中唯一地识别每个数据项。
	描述	数据项描述是对识别数据项的详细说明，可以帮助使用者更好地理解数据项的目的、作用和预期效果。
	启用状态	表示该数据项在分类分级任务执行时是否生效。
规则配置	匹配逻辑	且：所有条件都必须满足，才能识别成功。 或：只要满足其中一个条件，就可以识别成功。
	识别对象	识别对象指进行数据识别的对象，支持同时配置多个识别对象的特征，如字段名、内容等。
	识别方式	可自由选择所需要的识别方式（匹配 / 不匹配）。
	识别逻辑	**关键字：**关键字匹配是通过在数据中搜索特定的关键字来识别数据的匹配模式。一旦发现数据中包含这些关键词，将会对其进行标记，并进行分类分级。 **正则：**正则匹配使用正则表达式来定义复杂的匹配模式。通过正则表达式进行匹配，可提高匹配的准确性和灵活性。
	忽略大小写	若开启“忽略大小写”，则在进行匹配时不区分字母的大小写。
	全文匹配	全文匹配指的是将待识别的数据与识别内容进行完全一致的对比。如果数据与识别内容完全相同，将会对其进行标记，并进行分类分级。

6. 配置完成后，可单击**测试**，对已配置的识别规则进行测试验证。

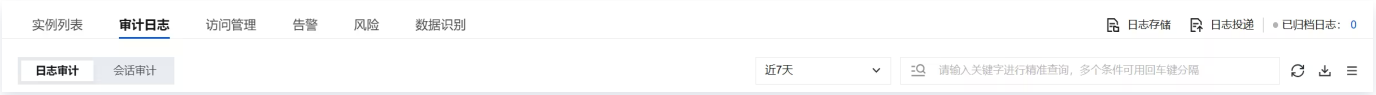
审计日志

最近更新时间：2026-08-21 18:00:32

数据安全审计审计日志模块，全面记录数据库操作全量行为，包含 SQL 语句、操作人员、来源 IP、时间戳等关键溯源信息，支持多维度精准检索与详情查看，为数据库操作行为提供全程可追溯能力。

日志审计

1. 登录 TDSQL-C MySQL 版控制台，在左侧导航栏单击**数据安全审计**。
2. 在数据安全审计页面，单击**审计日志 > 日志审计**。



3. 在审计日志页面中，显示已同步数据库资产的操作记录。
4. 在审计日志页面中，可通过实例、数据库账号、客户端 IP、客户端端口、数据库名、表名、SQL 语句、SessionID 进行日志检索。

SQL 语句详情

1. 在审计日志标签页面中，鼠标移动至目标日志行，单击目标日志 SQL 语句列的**详情**。

2. 在 SQL 语句详情页，您可查看完整 SQL 语句信息。

会话审计

会话审计从数据库连接会话的维度，帮您进行安全分析。

1. 登录 TDSQL-C MySQL 版控制台，在左侧导航栏单击**数据安全审计**。
2. 在数据安全审计页面，单击**审计日志 > 会话审计**。
3. 在审计日志页面中，显示已同步数据库会话连接记录。

存储设置

> **说明：**
> - 当日志量或日志存储时长达到对应量级时，将自动以文件形式归档较早的日志；

- 归档时，将优先归档最早的日志单元，1个日志单元最大包含45GB或八千万条日志。
- 日志归档成功后，其对应的在线日志将删除，归档的日志需恢复后才能查看。

1. 在审计日志标签页面中，单击**日志存储**。

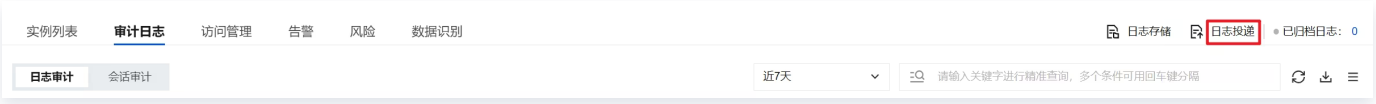
2. 在日志存储设置窗口，可开启 / 关闭归档日志存储，以及对在线日志存储时间、恢复日志保留时间、日志生命周期进行调整。

日志投递

说明：

- 购买 Ckafka 实例：前往消息队列控制台购买 Ckafka 实例，推荐使用专业版。
- 开通网络接入：根据消息队列 CKafka 文档指引，开通支撑网络接入或公网域名接入。

1. 登录 TDSQL-C MySQL 版控制台，在左侧导航栏单击**数据安全审计**。
2. 在数据安全审计页面，单击**审计日志**。
3. 在审计日志页面中，单击**日志投递**。



4. 在日志投递窗口，配置日志投递信息。

参数名称	参数说明
网络接入方式	选择消息队列的接入方式。 • 支撑环境接入。 • 公网域名接入。
消息队列实例	选择日志投递的消息队列实例。
网络	选择需使用的网络，支持 PLAINTEXT 类型。
用户名	设置用户名。仅公网域名接入方式需要填写。
密码	设置密码。仅公网域名接入方式需要填写。
Topic ID/名称	选择投递的 Topic。

归档日志管理

> **说明：**
> - 最多支持恢复500GB日志。
> - 同一时间只能进行一个恢复任务。
> - 在线日志和归档日志会占用存储空间，恢复日志不占用存储空间。

1. 登录 TDSQL-C MySQL 版控制台，在左侧导航栏单击**数据安全审计**。
2. 在数据安全审计页面，单击**审计日志**。
3. 在审计日志页面中，单击**已归档日志**。
4. 在已归档日志窗口，将显示所有已归档的审计日志，您可以对已归档的日志进行删除或恢复（恢复为在线日志）操作。

告警

最近更新时间：2026-08-21 18:00:32

数据库风险监测告警模块，通过对数据库资产的安全事件实时监测与响应体系，实现违规行为精准识别与闭环处理。

告警列表

1. 登录 TDSQL-C MySQL 版控制台，在左侧导航栏单击**数据安全审计**。
2. 在数据安全审计页面，单击**告警**。

3. 在告警标签页面，您可查看当前数据库资产的相关告警信息。告警列表将展示告警名称 / 类型、威胁等级、实例 ID / 名称、数据库账号、检出时间、处理状态等。

> **说明：**
> 告警导出会自动将告警列表中的检出时间换算为 UTC+08:00（东八区 / 北京时间），两组时间对应同一事件发生时刻，仅统计展示时区不同，原始数据保持一致。

查看告警详情

在告警标签页面，单击目标**告警名称**，查看告警触发原因、违规操作详情（SQL 语句、来源 IP）、关联资产等信息。

告警处理操作

标记忽略

对误报或无需处理的告警进行状态标记，排除风险统计干扰。

> **说明：**
> 告警处理状态标记为已忽略，则该风险将不会纳入风险统计中。

1. 在告警标签页面，支持单个或者批量处理目标告警：
   - **单个处置**：单击目标告警操作列的**标记忽略**。

- **批量处置**：选择多个目标告警，在列表上方单击**标记忽略**。

2. 在二次确认中，单击**确定**，即可将告警标记为已忽略。

添加白名单

对于需要长期放行的行为，可以将该告警所触发的策略添加至规则白名单中。

1. 在告警标签页面，单击目标告警操作列的**添加白名单**。

2. 在添加白名单窗口中，查看白名单策略内容，确认无误后单击**确定**，即可将该告警所触发的策略信息添加至白名单。

> **说明：**
> 告警白名单策略规则生效后，该行为不再触发告警。

标记已处置

对已完成应急响应的告警进行状态更新，实现处置闭环。

1. 在告警标签页面，选择单个或多个目标告警，单击**标记处置**。

2. 在确认窗口中，核查告警信息，确认无误后，单击**确定**，即可将该告警标记为已处置。

> **说明：**
> 告警处理状态标记已处置后，该告警将不会纳入风险统计中。

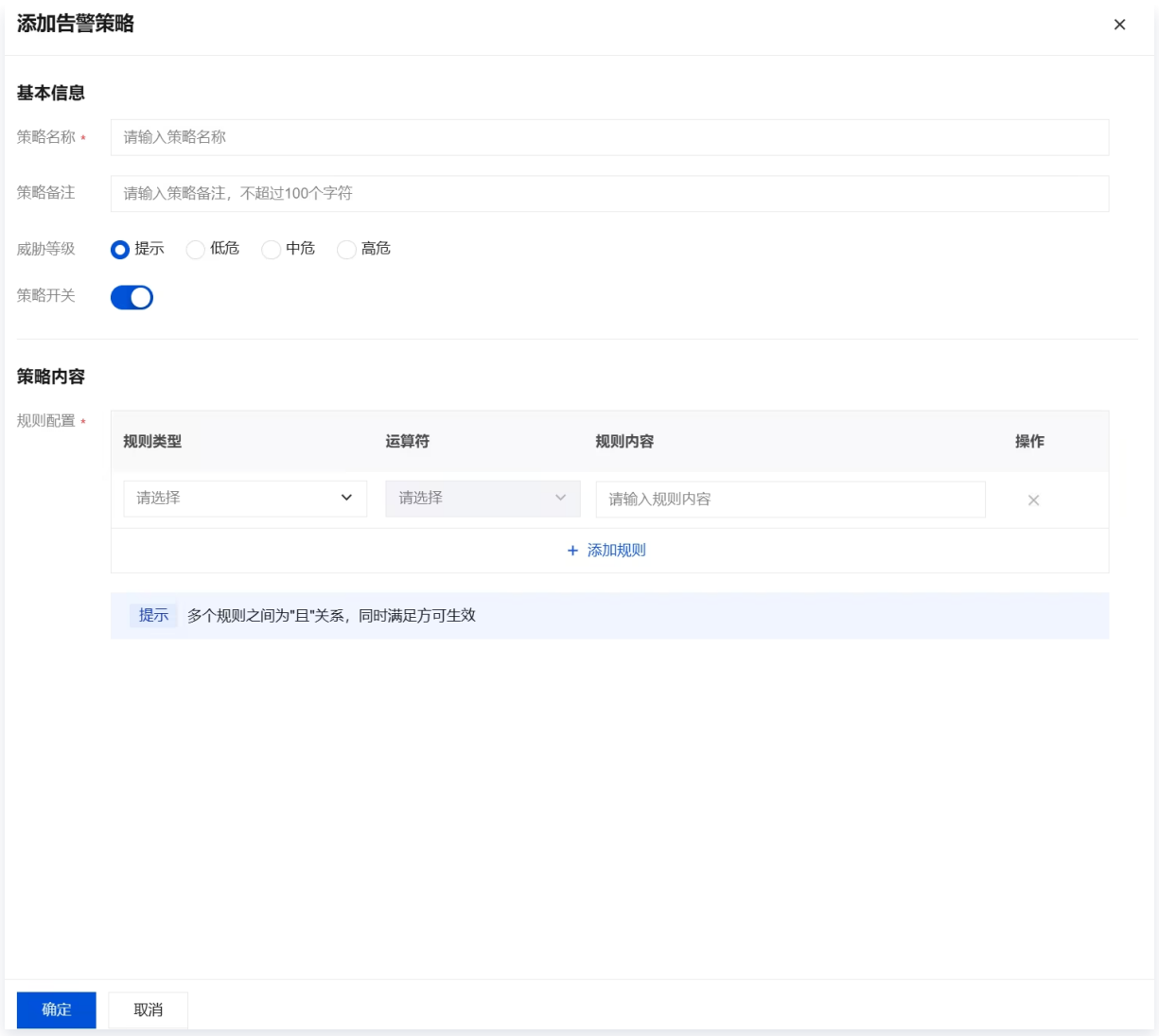
告警策略配置

1. 登录 TDSQL-C MySQL 版控制台，在左侧导航栏单击**数据安全审计**。
2. 在数据安全审计页面，单击右上角的**策略管理**。

3. 在策略管理窗口中，单击**告警策略**。
4. 在告警策略标签页面中，将显示所有内置的预设告警策略。您可以在该标签页面中对告警策略进行开启 / 关闭、调整威胁等级、修改策略内容等操作。

添加告警策略

1. 在告警策略标签页面，单击**添加策略**。
2. 在弹窗中，设置策略名称、策略备注、威胁等级、策略开关、策略内容后，单击**确定**。



开启 / 关闭告警策略

在告警策略标签页面，选择目标告警策略，单击策略开关列的**开关**，开启或关闭告警策略。

编辑告警策略

1. 在告警策略标签页面，选择目标告警策略，单击操作列的**编辑**。
2. 在编辑策略窗口，可以对威胁等级、策略内容（非服务账号）进行修改。

告警白名单管理

1. 在策略管理窗口中，单击**告警白名单策略**。

2. 在告警白名单策略标签页面，将显示所有已添加的告警白名单策略。
3. 在告警白名单策略标签页面，可定期查看白名单列表，单击“编辑”可以修改规则，单击“删除”可使规则过期/无效。

风险

最近更新时间：2026-08-21 18:00:31

数据库风险监测模块，聚焦未触发风险但存在长期安全隐患的行为。覆盖权限合规整改、暴露面安全加固、账号安全优化等核心场景，降低安全事件发生概率。

策略名称	策略内容	处置操作建议
操作权限范围过大	基于账号近7天使用权限计算权限使用率（使用权限 / 授权权限），当其小于配置的比例时，触发风险	• 风险忽略 • 风险加白 • 一键处置
暴露公网访问入口	数据库实例启用公网地址时，触发风险	一键处置

风险列表

1. 登录 TDSQL-C MySQL 版控制台，在左侧导航栏单击**数据安全审计**。
2. 在数据安全审计页面，单击**风险**标签。

3. 在风险页面，将展示已触发风险策略的数据安全风险，包括风险名称 / 类型、威胁等级、实例 ID / 名称、数据库账号、检出时间、处理状态等信息。

风险详情

在风险标签页面，找到目标风险，单击风险名称，可以查看风险详情。

风险处置

标记忽略

对**操作权限范围过大的风险项**进行状态标记，排除风险统计干扰。

> **说明：**
> 风险处理状态标记为已忽略，则该风险将不会纳入风险统计中。

1. 在风险标签页面，支持单个或者批量处理目标风险：
   - **单个处置**：单击风险名称为**操作权限范围过大**的风险操作列中的**标记忽略**。
   - **批量处置**：在风险页面，选择风险名称为**操作权限范围过大**的风险，在列表上方单击**标记忽略**。

2. 在二次确认中，单击**确定**，即可将该风险标记为已忽略。

添加白名单

1. 在风险标签页面，单击风险名称为**操作权限范围过大**的风险操作列中的**添加白名单**。

2. 在添加白名单窗口中，查看白名单策略内容，确认无误后单击**确定**，即可将该风险所触发的策略信息添加至白名单。

> **说明：**
> 风险白名单策略规则生效后，该行为不再触发风险。

标记已处置

对已完成应急响应的风险进行状态更新，实现处置闭环。

1. 在风险标签页面，选择单个或多个目标风险，单击**标记处置**。
2. 在确认窗口中，核查风险信息，确认无误后，单击**确定**，即可将该风险标记为已处置。

> **说明：**
> 风险处理状态标记已处置后，该风险将不会纳入风险统计中。

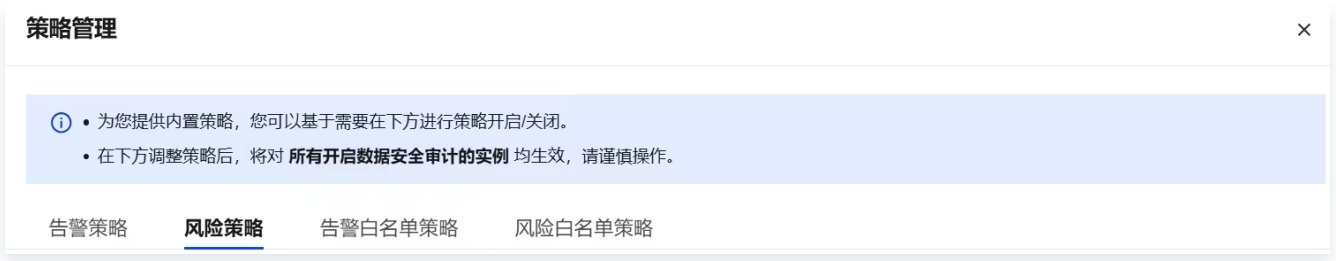
一键处置

针对不同的风险项，可以通过一键处置进行风险的处置操作。
在风险标签页面，选择目标风险，单击操作列中的**一键处置**。可通过系统预设的处置操作进行风险处置。

风险策略配置

1. 登录 TDSQL-C MySQL 版控制台，在左侧导航栏单击**数据安全审计**。
2. 在数据库风险监测页面，单击右上角**策略管理**。

3. 在策略管理窗口中，单击**风险策略**标签。



4. 在风险策略标签页面中，将显示所有内置的预设风险策略。您可以在该标签页面中对风险策略进行开启 / 关闭、调整威胁等级、修改策略内容等操作。

开启/关闭风险策略

在风险策略标签页面，选择目标风险策略，单击策略开关列中的**开关**，开启或关闭风险策略。

编辑风险策略

1. 在风险策略标签页面，选择目标风险策略，单击操作列中的**编辑**。
2. 在编辑策略窗口，可以对威胁等级、策略内容（非服务账号）进行修改。