云数据库 MySQL

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：2026-03-25 11:52:31

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，管理难度大**：库表、文件、代码、图片等数据分散，缺乏资产目录，权责划分模糊，如公开敏感存储桶或内部数据库公网暴露等，则整体管理效率低下且合规审计压力大。
- **数据访问看不清，溯源成本高**：数据被谁（公网/内网 IP）、通过什么方式（账号/接口）、调用了哪些数据、操作了哪些文件等关键信息缺乏统一视图，管理员需跨多平台人工拼接日志，溯源效率低且易错过处置黄金窗口。
- **数据风险定位难，处置优先级混乱**：传统规则引擎仅通过单点特征匹配，无法识别组合行为风险（如公网访问 + 敏感数据 + 批量下载），企业常陷入“告警疲劳”，难以判断处置优先级，快速收敛影响面。
- **权限滞留难清理，泄露风险高**：员工离职、第三方协作等场景中，临时账号权限若未及时回收，易因账号密码管理疏漏导致敏感数据外泄。

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

云数据库 MySQL 单节点、双节点、三节点和云盘版支持数据安全审计。

支持地域

云数据库 MySQL 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	拓扑访问
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：2026-03-25 11:52:31

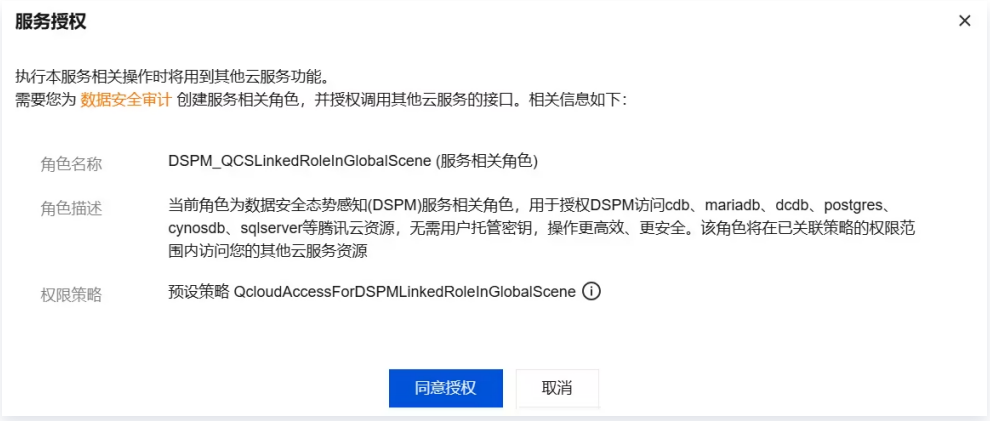
本文为您介绍如何通过控制台购买数据安全审计。

前提条件

已 创建 MySQL 实例 。

操作步骤

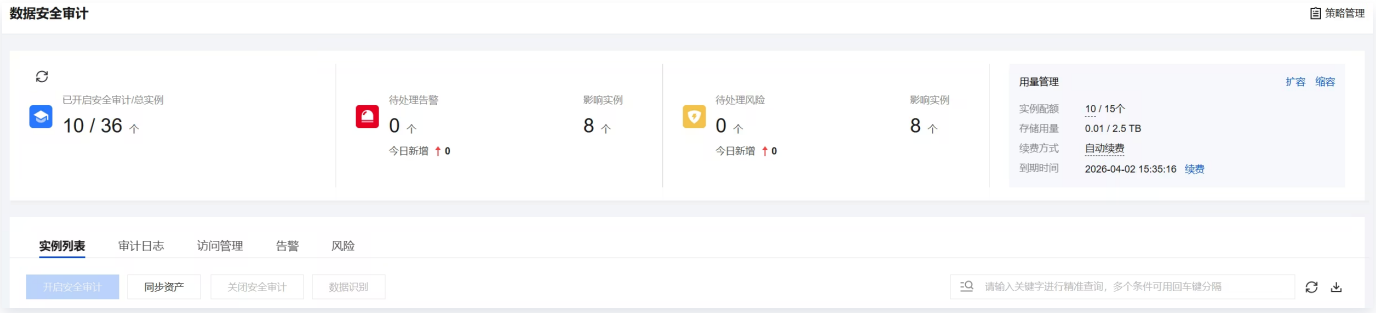
1. 登录 MySQL 控制台 。
2. 在左侧导航栏选择**数据安全审计**。
3. 在数据安全审计页面单击**开启安全审计**。
4. 在弹窗中阅读服务授权信息，单击**同意授权**。



5. 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**。

6. 成功购买后的数据安全审计页面如下。



开启或关闭数据安全审计

最近更新时间：2026-03-25 11:52:31

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 MySQL 实例 。
- 已 购买数据安全审计 。

操作步骤

开启数据安全审计

1. 登录 MySQL 控制台 。
2. 在左侧导航栏选择**数据安全审计**。
3. 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**。

4. 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**。

关闭数据安全审计

1. 登录 MySQL 控制台 。
2. 在左侧导航栏选择**数据安全审计**。
3. 在实例列表下找到目标实例，单击其**安全审计状态**字段下的**关闭**。

4. 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。

数据识别

最近更新时间：2026-03-25 11:52:31

本文为您介绍数据安全审计的数据识别能力相关操作。

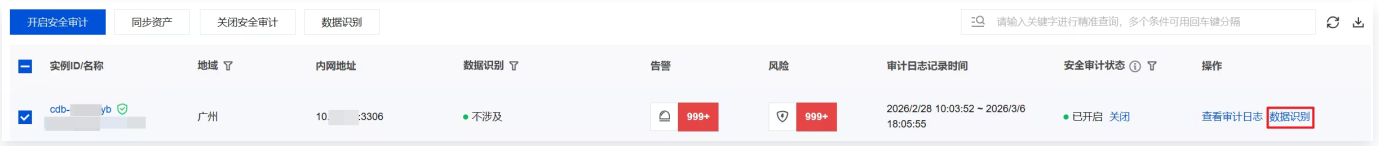
前提条件

- 已 创建 MySQL 实例 。
- 已 购买数据安全审计 。
- 已 开启数据安全审计 。

操作步骤

开启数据识别

1. 登录 MySQL 控制台 。
2. 在左侧导航栏选择**数据安全审计**。
3. 在实例列表下找到目标实例，单击其操作列的**数据识别**。



4. 在弹窗中，完成如下配置，单击**确定**。

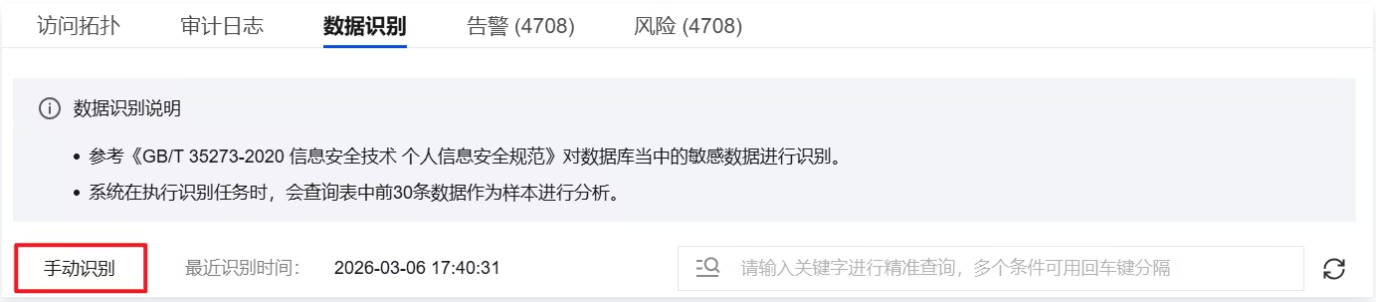
参数	说明
立即识别	打开立即识别按钮，表示单击确定后，将立即对所选实例进行数据识别。当关闭立即识别按钮时，需要打开周期识别按钮并进行设置，否则将无法开启数据识别。

周期识别	若您希望定期对实例进行数据识别，您可以打开周期识别按钮并进行如下设置。 **识别频率及识别周期** • 按天：识别频率选择按天时，识别周期可设置一天中的指定时间（精确到秒）。 • 按周：识别频率选择按周时，识别周期可设置每周一到每周日之间的某一天的指定时间（精确到秒）。 • 按月：识别频率选择按月时，识别周期可设置每月中的某一天的指定时间（精确到秒）。

数据识别配置

1. 登录 MySQL 控制台。
2. 在左侧导航栏选择**数据安全审计**。
3. 在实例列表下找到已开启数据识别的实例，单击其**数据识别**字段下的**详情**。

4. 在弹出的侧边栏中，单击**手动识别**。



5. 在弹窗中，您可以进行数据识别的重新配置。

查看数据识别详情

1. 登录 MySQL 控制台。
2. 在左侧导航栏选择**数据安全审计**。
3. 在实例列表下找到已开启数据识别的实例，单击其**数据识别**字段下的**详情**。
4. 在弹出的侧边栏中，您可以查询被识别的数据类别、数据项等信息。


访问拓扑
审计日志
数据识别
告警 (35213)
风险 (18690)
数据识别说明
参考《GB/T 35273-2020 信息安全技术 个人信息安全规范》对数据库当中的敏感数据进行识别。
系统在执行识别任务时，会查询表中前30条数据作为样本进行分析。
手动识别
最近识别时间：
2026-03-06 17:40:31
请输入关键字进行精准查询，多个条件可用回车键分隔
库名：ds
总表数：1
数据类别：
个人敏感信息
个人信息
数据项：
身份证
银行卡
+9
共 1 条
1
/ 1 页
表名
字段数
数据识别
er
15
数据类别：
个人敏感信息
个人信息
数据项：
卡号
+10
共 1 条
10
条 / 页
1
/ 1 页

拓扑访问

最近更新时间：2026-03-25 11:52:31

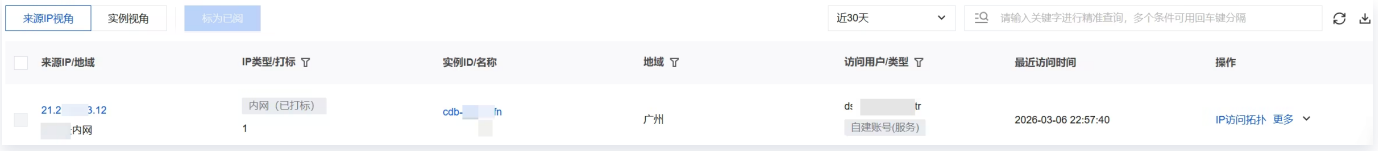
数据库风险监测访问管理模块，通过“来源 IP 视角”与“实例视角”的双维度互补治理，实现对数据库访问行为的精细化管控。支持访问行为的可视化展示（如访问拓扑图）、IP/账号打标操作，实现精细化访问控制。从“来源 IP”和“实例”双维度管控访问行为，解决“谁能访问、从哪访问、访问什么”的核心问题，避免粗放式访问控制导致的安全漏洞。本文为您介绍数据安全审计的访问管理能力。

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 MySQL 控制台 。
2. 在左侧导航栏选择**数据安全审计**。
3. 在数据安全审计页面，选择**访问管理** > **来源 IP 视角**。

4. 在来源 IP 视角标签页面，您可以查看来源 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 视角标签页面下，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

> **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。

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 视角标签页面下，单击目标 IP 对应操作列的**更多 > 来源 IP 打标**。

2. 在弹窗中，编辑**来源 IP 备注**，单击**确定**完成标记。

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 视角标签页面下，单击目标 IP 对应操作列的**更多 > 账号打标**。

2. 在弹窗中，选择**账号类型**，编辑**备注**信息，单击**确定**完成标记。

> **说明：**
> 支持编辑类型为“自建账号”的访问账号类型，若当前访问账号为腾讯云主账号/子账号，则系统将自动识别，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 视角标签页面下，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 MySQL 控制台 。
2. 在左侧导航栏选择**数据安全审计**。
3. 在数据安全审计页面，选择**访问管理** > **实例视角**。

4. 在实例视角标签页面，您可以查看实例 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。

在实例视角标签页面下，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

> **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。

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. 在实例视角标签页面下，单击目标实例对应操作列的**更多** > **来源 IP 打标**。

2. 在弹窗中，编辑**来源 IP 备注**，单击**确定**完成标记。

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. 在实例视角标签页面下，单击目标 IP 对应操作列的**更多** > **账号打标**。

2. 在弹窗中，选择**账号类型**，编辑**备注**信息，单击**确定**完成标记。

> **说明：**
> 支持编辑类型为“自建账号”的访问账号类型，若当前访问账号为腾讯云主账号/子账号，则系统将自动识别，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。
在实例视角标签页面下，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。

审计日志

最近更新时间：2026-03-25 11:52:31

数据库风险监测审计日志模块，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。本文为您介绍数据安全审计的审计日志能力。

查看审计日志

1. 登录 MySQL 控制台 。
2. 在左侧导航栏选择**数据安全审计**。
3. 在数据安全审计页面，单击**审计日志**。
4. 在审计日志页面中，会显示已开启数据安全审计的数据库资产的操作记录。

5. 在审计日志页面中，您可以通过实例、时间范围、数据库账号、客户端 IP、客户端端口和 SQL 语句进行日志检索。

查看归档日志

1. 登录 MySQL 控制台 。
2. 在左侧导航栏选择**数据安全审计**。
3. 在数据安全审计页面，单击**审计日志**。
4. 在审计日志页面，单击**已归档日志**。

5. 在弹出的侧边栏中，会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**（恢复为审计日志）操作。

日志存储设置

说明：

- **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8千万条日志。**
- **日志归档成功后，其对应的审计日志将删除，归档的日志需恢复后才可以查看。**

1. 登录 MySQL 控制台 。
2. 在左侧导航栏选择**数据安全审计**。
3. 在数据安全审计页面，单击**审计日志**。
4. 在审计日志页面，单击**存储设置**。
5. 在存储设置页面，可开启/关闭归档日志存储。开启时支持对**在线日志存储时长、归档日志恢复保留以及日志清除期限**进行设置；关闭时仅支持对**日志清除期限**进行设置。设置完成后单击**保存**。

告警

最近更新时间：2026-03-25 11:52:31

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，实现违规行为精准识别与闭环处理。本文为您介绍数据安全审计的告警能力。

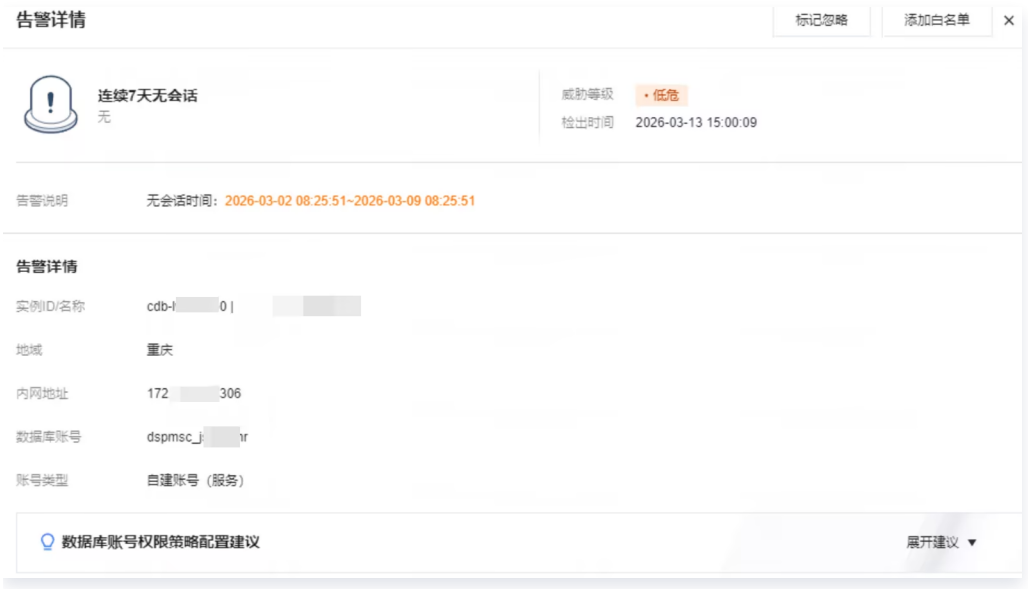
查看告警列表

1. 登录 MySQL 控制台 。
2. 在左侧导航栏选择**数据安全审计**。
3. 在数据安全审计页面，单击**告警**。

4. 在告警标签页面，您可以查看当前数据库资产的相关告警信息，包括告警名称/类型、威胁等级、实例 ID/名称、数据库账号、检出时间、处理状态。

查看告警详情

在告警标签页面下，单击目标告警的告警名称，可以查看告警详情。



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：**

> 若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。
   - 单个处理：单击目标告警操作列的**更多** > **标记忽略**。

   - 批量处理：选择多个目标告警，单击**标记忽略**。

2. 在弹窗中，单击**确定**，即可将告警标记为已忽略。

添加白名单

> **说明：**
> 告警白名单策略生效后，该行为不再触发告警。

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. 在弹窗中，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。

标记已处理

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

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. 在弹窗中核查告警信息，确认无误后，单击**确定**，即可将该告警标记为已处理。

告警策略配置

1. 登录 MySQL 控制台 。
2. 在左侧导航栏选择**数据安全审计**。
3. 在数据安全审计页面，单击右上角的**策略管理**。

4. 在弹窗中，单击**告警策略**。
5. 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、调整威胁等级等操作。

开启或关闭告警策略

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。

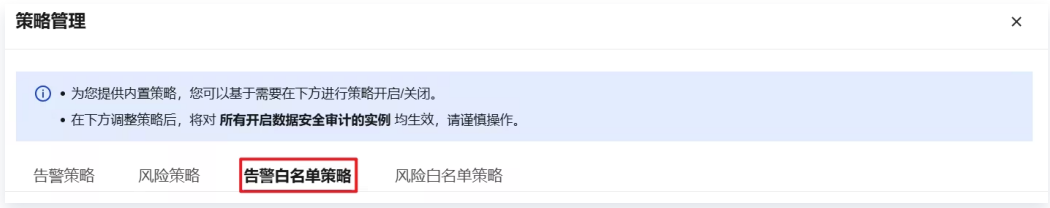
编辑告警策略

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. 在弹窗中，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，您可以定期查看白名单列表，单击**编辑**修改规则，或单击**删除**以过期/无效规则。

风险

最近更新时间：2026-03-25 11:52:31

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。本文为您介绍数据安全审计的风险监测能力。

查看风险列表

1. 登录 MySQL 控制台 。
2. 在左侧导航栏选择**数据安全审计**。
3. 在数据安全审计页面，单击**风险**。

4. 在风险标签页面，您可以查询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、资产实例 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：**
> 若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。
   - 单个处理：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**。

   - 批量处理：选择多个风险名称为**操作权限范围过大**的风险，单击**标记忽略**。

2. 在弹窗中，单击**确定**，即可将风险标记为已忽略。

添加白名单

> **说明：**
> 风险白名单策略规则生效后，该行为不再触发风险。

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. 在弹窗中，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。

标记已处置

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

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. 在弹窗中，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理。

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。

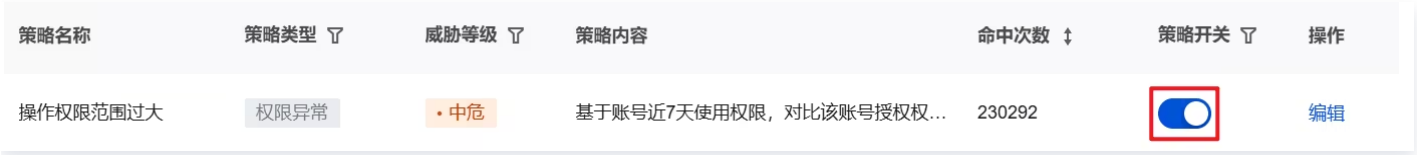
风险策略配置

1. 登录 MySQL 控制台 。
2. 在左侧导航栏选择**数据安全审计**。
3. 在数据安全审计页面，单击**风险**。
4. 在风险标签页面，单击**策略管理**。

5. 在弹出的侧边栏中，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。

开启或关闭风险策略

在风险策略标签页面，找到目标风险策略，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，找到目标风险策略，单击**操作**列中的**编辑**。

2. 在弹窗中，可以对**威胁等级、策略内容（非服务账号）**进行修改。