ALIBABA CLOUD

阿里云

数据库自治服务
安全审计

文档版本：20200929

阿里云

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。

2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。

3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。

4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的“现状”、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。

5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含“阿里云”、“Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。

6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
危险	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	危险 重置操作将丢失用户配置数据。
警告	该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。	警告 重启操作将导致业务中断，恢复业务时间约十分钟。
注意	用于警示信息、补充说明等，是用户必须了解的内容。	注意 权重设置为0，该服务器不会再接受新请求。
说明	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	说明 您也可以通过按Ctrl+A选中全部文件。
>	多级菜单递进。	单击**设置**> **网络**> **设置网络类型**。
粗体	表示按键、菜单、页面名称等UI元素。	在**结果确认**页面，单击**确定**。
`Courier字体`	命令或代码。	执行 `cd /d C:/window` 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	`bae log list --instanceid` *Instance_ID*
[] 或者 [a|b]	表示可选项，至多选择一个。	`ipconfig [-all|-t]`
{} 或者 {a|b}	表示必选项，至多选择一个。	`switch {active|stand}`

目录

1.安全审计

本文档主要介绍DAS安全审计的功能和使用方法。

前提条件

在DAS中接入对应的数据库实例，并且接入状态显示为**连接正常**，目前该功能仅支持用户自建的MySQL数据库。

> **说明** 接入数据库实例的操作详情可参见**接入其他自建数据库实例**。

背景信息

数据库是企业最重要的资产之一，其可能面临来自外部的攻击、内部的危险操作、数据泄漏等风险。DAS安全审计功能，采用旁路的技术，采集并分析对数据库服务器的各类操作行为，实时地、智能地解析对数据库服务器的各种操作，自动识别高位SQL、SQL注入、新增访问来源等风险。

SQL

高危SQL

DAS会根据预设的规则库，自动识别三种类型的高危SQL。

- DDL（新建表、修改表结构、修改索引、重命名表等操作）。
- 全表更新（例如全表Update、全表Delete等操作）。
- 大请求，默认规则是满足下面三个条件中的任意一个。
  - 扫描行数 >= 100万
  - 返回行数 >= 10万
  - 更新行数 >= 10万

SQL注入

SQL注入就是通过把SQL命令插入到Web表单、域名或页面请求中，最终达到欺骗服务器执行恶意的SQL命令，严重危害数据库的健康。DAS会持续不断地监控和识别数据库中是否存在SQL注入的情况，并且发现访问来源。

新增访问来源

DAS会与历史的访问来源纪录进行对比，自动识别新增的访问来源，帮助用户确认是否存在未知的机器在访问或者读取数据库。

> **说明** 默认规则是过去七天没有出现过的访问来源，即为新增访问来源。

操作步骤

1. 登录**DAS控制台**。
2. 在左侧导航栏，单击**实例监控**。
3. 单击目标实例，进入实例详情页面。
4. 在左侧导航栏，单击**安全审计**。
5. 单击**开启**，在弹出框中单击**确定**即可；单击右上角的**关闭安全审计**，即可以关闭该功能，并且同时关闭**全量SQL**功能。


性能趋势
实例告警
实例会话
请求分析
慢SQL
全量SQL
安全审计
安全风险趋势 (实例: :3306)
关闭安全审计
点击趋势图可查看特定时段的风险详情
近1天 近3天 近1周 近1月
2018-10-09 17:12:01 - 2018-10-16 17:12:01
查看
2018-10-11 11:00
2
1.5
1
0.5
0
00:00 00:00 00:00 00:00 00:00 00:00 00:00
高风险请求 SQL注入 新增访问来源 全部
安全风险详情 (时间范围: 2018-10-11 11:00 - 2018-10-11 12:00)
0
高风险请求
2
SQL注入
0
新增访问来源
SQL模板 数据库 检测结果 执行次数 平均执行耗时(毫秒) 操作
* Where 子句中有部分条件总为真
2
0.00
样本