ALIBABA CLOUD

阿里云

数据库审计
产品简介

文档版本：20201029

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

1.什么是数据库审计

数据库审计服务是一款专业、主动、实时监控数据库安全的审计产品，可用于审计阿里云平台中的RDS云数据库、ECS自建数据库和NoSQL数据库。

数据库审计服务将数据库监控、审计技术与公共云环境相结合，针对数据库SQL注入、风险操作等数据库风险行为进行记录与告警，形成对核心数据的安全防护，为您的云端数据库提供完善的安全诊断、维护、管理功能。

数据库审计服务符合等级保护三级标准，帮助您满足合规性要求，包括但不限于：

- 中国银监会、工业和信息化部、公安部、国家互联网信息办公室制定的《网络借贷信息中介机构业务活动管理暂行办法》中第十八条指出需要进行信息安全检查和审计。
- 网络安全法
  - 第二十一条 （三）采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月。
  - 第三十八条 关键信息基础设施的运营者应当自行或者委托网络安全服务机构对其网络的安全性和可能存在的风险每年至少进行一次检测评估，并将检测评估情况和改进措施报送相关负责关键信息基础设施安全保护工作的部门。

适用范围

数据库审计服务可以帮助您解决以下问题：

- 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。
- 支持审计数据增量备份，满足等保规范对审计数据保存期限要求。
- 具备风险状况、运行状况、性能状况、语句分布的实时监控能力。
- 帮助您记录、分析、追查数据库安全事件。
- 通过数据库性能诊断，追踪危险事件和不安全操作。
- 有效发现程序后门，降低数据泄密风险。
- 提供数据库实时风险告警能力，及时响应数据库攻击。

工作原理

数据库审计服务通过旁路监听模式，支持完全独立于数据库的部署。在不影响数据库日常运行效能的前提下，实现灵活的审计与监控。

- 基于数据库操作语句进行审计，监视数据库登录、访问行为，有效地实施审计策略。数据库审计服务还具备强大的数据库活动审计分析能力，从多个角度灵活呈现数据库的活动状态，帮助您有效执行安全策略。
- 采用全新的人机交互操作模式，基于人性化、专业化和可用性三个层面设计产品界面。在审计日志统计分析方面，数据库审计服务采用独创的综合性统计分析报表，基于日报、周报、月报等基础型业务报表（可设置自动定时发送），并结合专项性的模式分析类报表，开启数据库审计产品报表展现形式的新纪元。
- 审计查询方式支持单库（单个数据库）级和全库（所有数据库）级两个层面进行审计查询。采用多重页面钻取功能，逐层递进地引导用户完成审计日志的查询分析。同时，为方便您定制审计规则，采用优先级由上而下的规则命中机制，从多个层面定义数据库审计规则。

产品定价

数据库审计按照包年包月方式计费，更多详情请参见计费方式。

如何使用

- 数据库审计（C100），请参见C100快速入门。
- 数据库审计（A100），请参见A100快速入门。

2.功能特性

数据库审计提供用户行为发现审计、多维度分析、实时报警和报表功能。

用户行为发现审计

- 关联应用层和数据库层的访问操作。
- 支持溯源到应用者的身份和行为。

多维度线索分析

- 风险和危害线索

  支持对高中低的风险等级、SQL注入、黑名单语句、违反授权策略等SQL行为进行分析。

- 会话线索

  支持根据时间、用户、IP、应用程序、客户端等多角度进行分析。

- 详细语句线索

  提供用户、IP、客户端工具、访问时间、操作对象、SQL操作类型、操作成功与否、访问时长、影响行数等多种检索条件。

多维度告警机制

- 异常操作风险

  支持通过IP、用户、数据库客户端工具、时间、敏感对象、返回行数、系统对象、高危操作等多种元素细粒度定义要求监控的风险访问行为。

- SQL注入

  提供系统性的SQL注入库，以及基于正则表达式或语法抽象的SQL注入描述，发现数据库异常行为立即告警。

- 黑白名单

  通过准确而抽象的方式，对系统中的特定访问SQL语句进行描述，在这些SQL语句出现时能够迅速告警。

精细化报表

- 会话行为

  提供登录失败报表、会话分析报表。

- SQL行为

  提供新型SQL报表、SQL语句执行历史报表、失败SQL报表。

- 风险行为

  提供告警报表、通知报表、SQL注入报表、批量数据访问行为报表。

- 政策性报表

  提供SOX报告。

说明 *SOX法案*是美国政府出台的一部涉及会计职业监管、公司治理、证券市场监管等方面的重要法律。根据 *SOX法案* 的审计要求，相关企业必须对信息系统的日志信息以及操作明细进行有效的保存，为外部审计人员对企业的合规性审计提供依据。云盾数据库审计系统的SOX报告是关于数据库安全审计方面的符合性报告。

3.产品优势

数据库审计服务具有旁路部署、合规达成、全量审计、快速识别、高效分析等优势。

旁路部署

通过旁路检测方式，不影响数据库运行效率，实现灵活的审计与监控。

合规达成

满足外部审计对审计数据内容增量备份和存储时长的要求，满足网络安全法对日志数据存储的要求。

全量审计

支持对RDS云数据库、ECS自建数据库的审计，最大程度的满足云上用户数据库审计需求。

快速识别

可实现99%+的应用关联审计、完整的SQL解析、精确的协议分析。

高效分析

每秒万次入库、海量存储、亿级数据秒级响应。

4.应用场景

数据库审计服务支持对云数据库及自建数据库进行适配审计，满足您对数据审计及日志数据留存的要求。

RDS数据库审计

通过在访问数据库的应用系统服务器上部署数据库审计Agent，获取访问日志数据用于日志审计，实现对RDS云数据库的审计。

说明

- 数据库审计系统（C100）如何部署Agent请参见部署Agent程序。
- 数据库审计系统（A100）如何部署Agent请参见部署Agent程序。

ECS自建数据库审计

通过在ECS中安装数据库审计Agent，获取数据库操作日志，实现对ECS自建数据库的审计。支持目前流行的各类数据库，保证数据审计兼容、有效。

说明

- 数据库审计系统（C100）如何部署Agent请参见部署Agent程序。
- 数据库审计系统（A100）如何部署Agent请参见部署Agent程序。