数据库安全服务

快速入门

文档版本 1

发布日期 2023-07-14

华为技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

目 录

1 快速使用数据库安全审计

- 数据库安全审计是数据库安全服务提供的旁路模式数据库审计功能，通过实时记录用户访问数据库行为，形成细粒度的审计报告，对风险行为和攻击行为进行实时告警。同时，数据库安全审计可以生成满足数据安全标准（例如Sarbanes-Oxley）的合规报告，对数据库的内部违规和不正当操作进行定位追责，保障数据资产安全。
- 数据库安全审计在不影响用户业务的前提下，支持对华为云上的关系型数据库（RDS）、弹性云服务器（ECS）/裸金属服务器（BMS）的自建数据库进行灵活的审计。
- 本指南以审计ECS的自建数据库为例，指导您快速上手数据库安全审计。
- 示例请参见：**快速使用数据库安全审计**。

2 入门实践

当您配置完数据库安全服务（DBSS）后，可以根据自身业务的业务场景使用DBSS提供的一系列常用实践。

表 2-1 常用最佳实践

实践		描述
审计数据库	**审计ECS数据库**	数据库安全审计采用旁路部署模式，通过在数据库或应用系统服务器上部署数据库安全审计Agent，获取访问数据库流量、将流量数据上传到审计系统、接收审计系统配置命令和上报数据库状态监控数据，实现对ECS/BMS自建数据库的安全审计。
	审计RDS关系型数据库（安装Agent方式） **审计RDS关系型数据库（免Agent方式）**	数据库安全服务支持对关系型数据库（应用部署于ECS）进行安全审计。对于部分关系型数据库，DBSS服务支持免安装Agent模式，无需安装Agent，即可开启数据库安全审计。
	容器化部署数据库安全审计Agent	数据库安全审计支持批量部署流量采集Agent，针对大规模业务场景（容器化部署应用、数据库（RDS关系型数据库）数量大），能够显著提升产品配置的效率，降低配置的复杂度，减少运维人员的日常维护压力。
数据库检测	**数据库拖库检测**	数据库安全审计默认提供一条“数据库拖库检测”的风险操作，用于检测原始审计日志疑似拖库的SQL语句，及时发现数据安全风险。 通过数据库拖库检测，您可获知执行耗时长、影响行数、执行该SQL语句的数据库信息。
	数据库慢SQL检测	数据库安全审计默认提供一条“数据库慢SQL检测”的风险操作，用于检测原始审计日志的响应时间大于1秒的SQL语句。 通过数据库慢SQL检测，您可获知执行耗时长、影响行数、执行该SQL语句的数据库信息并根据实际需求对慢SQL进行优化。

实践		描述
	数据库脏表检测	数据库安全审计规则可增加一条“数据库脏表检测”的高风险操作。用户预设无用的库、表或列作为“脏表”，无风险程序不会访问用户自建的“脏表”，用于检测访问“脏表”的可能的恶意程序。 通过数据库脏表检测，可以帮助您监控识别访问“脏表”的SQL语句，及时发现数据安全风险。
等保合规	数据库等保合规相关项	为客户提供一站式的安全解决方案，帮助客户快速、低成本完成安全整改，轻松满足等保合规要求。
数据库审计配置	Oracle RAC集群审计配置	在使用Oracle RAC集群的DBSS时，RAC集群中的每一个节点都是作为一个独立的数据库，在配置时需要为集群中的每一个节点安装Agent，以实现网络流量的转发。
	数据库审计实例规则配置	数据库安全服务提供多维度的数据库审计线索，包括源IP、用户身份、应用程序、访问时间、请求的数据库、原SQL语句、操作等，协助您溯源到攻击者。

A 修订记录

发布日期	修改说明
2023-07-18	第一次正式发布。