数据库安全服务(DBSS)

快速入门

文档版本 01

发布日期 2024-10-30

华为云计算技术有限公司

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云计算技术有限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，华为云计算技术有限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。

华为云计算技术有限公司

地址： 贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

网址： https://www.huaweicloud.com/

目 录

1 购买并开启数据库安全审计

数据库安全服务（Database Security Service，DBSS）是一个智能的数据库安全服务，基于大数据分析技术，提供数据库审计，SQL注入攻击检测，风险操作识别等功能，保障云上数据库的安全。

本文介绍购买入门版管理1个数据库为例，开启数据库安全服务。您可以根据默认的审计规则，通过多维度分析、实时告警和报表功能发现异常行为。

操作流程

操作步骤	说明
准备工作	您需要注册华为账号，并为账户充值。
步骤一 购买入门版数据库安全服务	设置DBSS的子网、安全组、购买时长等配置信息，购买入门版数据库安全服务。
步骤二 添加数据库	添加数据库，同时您可以根据不同数据库类别，选择免Agent或安装Agent。
步骤三 开启数据库安全审计	开启数据库安全审计，并验证审计结果。
相关操作	自定义配置审计规则，并查看审计结果和监控信息。

准备工作

- 在购买Web应用防火墙之前，请先注册华为账号并开通华为云。具体操作详见**注册华为账号并开通华为云**、**实名认证**。

  如果您已开通华为云并进行实名认证，请忽略此步骤。
- 请保证账户有足够的资金，以免购买Web应用防火墙失败。

步骤一 购买入门版数据库安全服务

步骤1 登录管理控制台。

步骤2 单击页面左上方的 ☰，选择“安全与合规 > 数据库安全服务”，进入数据库安全审计“总览”界面。

步骤3 在界面右上角，单击“购买数据库安全服务”。

步骤4 在**购买数据库安全服务**页面完成以下配置。

表 1-1 数据库安全审计实例参数说明

参数	示例	说明
虚拟私有云	**default_vpc**	您可以选择使用区域中已有的虚拟私有云（Virtual Private Cloud，VPC）网络，或者单击“查看虚拟私有云”，跳转到VPC管理控制台创建新的虚拟私有云。 **说明** • 请选择Agent安装节点（应用端或数据库端）所在的VPC。数据库安全审计的Agent安装节点，请参见：**如何选择数据库安全审计的Agent安装节点?** • 不支持修改VPC。若要修改，请退订后重购。 更多有关虚拟私有云的信息，请参见《虚拟私有云用户指南》。
安全组	**default**	您可以选择区域中已有的安全组，或者在VPC管理控制台创建新的安全组。选择实例的安全组后，该实例将受到该安全组访问规则的保护。 更多有关安全组的信息，请参见《虚拟私有云用户指南》。
子网	**default_subnet**	您可以选择VPC中已配置的子网，或者在VPC管理控制台为VPC创建新的子网。
实例名称	**DBSS-test**	您可以自定义实例的名称。
备注	-	您可以添加实例备注信息。
企业项目	**default**	该参数针对企业用户使用。 企业项目是一种云资源管理方式，企业项目管理服务提供统一的云资源按项目管理，以及项目内的资源管理、成员管理，默认项目为default。 请在下拉框中选择所在的企业项目。更多关于企业项目的信息，请参见**《企业管理用户指南》**。
购买时长	**1**	选择数据库安全服务的有效时长。 勾选“自动续费”后，当购买的数据库安全审计实例到期时，如果账号余额充足，DBSS将自动为该实例续费，您可以继续使用该实例。

步骤5 确认当前配置无误后，单击“立即购买”。

如果您对价格有疑问，可以单击“了解计费详情”，了解产品价格。

步骤6 在“详情”页面，阅读《数据库安全审计安全免责声明》后，勾选“我已阅读并同意《数据库安全审计安全免责声明》”，单击“提交”。

步骤7 在购买页面，请选择付款方式进行付款。

步骤8 成功付款后，在数据库安全审计实例列表界面，可以查看数据库安全审计实例的创建情况。

----结束

步骤二 添加数据库

数据库安全服务审计的数据库支持免安装Agent和安装Agent。支持免安装Agent的数据库类型和版本如表1-2所示，支持安装Agent的数据库类型和版本如表1-3。您可以根据不同的数据库类型和版本，选择免安装Agent或安装Agent，开启数据库安全审计。

添加数据库免安装 Agent

表 1-2 免安装 Agent 的数据库类型和版本

数据库类型	支持的版本
GaussDB for MySQL	默认都支持
PostgreSQL **须知** 当SQL语句大小超过4KB审计时会被截断，会导致审计到的SQL语句不完整。	• 14（14.4及以上版本） • 13（13.6及以上版本） • 12（12.10及上版本） • 11（11.15及以上版本） • 9.6（9.6.24及以上版本） • 9.5（9.5.25及以上版本）
RDS for SQLServer	默认都支持
RDS for MySQL	• 5.6（5.6.51.1及以上版本） • 5.7（5.7.29.2及以上版本） • 8.0（8.0.20.3及以上版本）
GaussDB(DWS)	• 8.2.0.100及以上版本
RDS for MariaDB	默认都支持

步骤1 在左侧导航树中，选择“数据库列表”，进入数据库列表界面。

步骤2 在“选择实例”下拉列表框中，选择需要添加数据库的实例。

步骤3 在数据库列表框左上方，单击“添加数据库”。

步骤4 在弹出的对话框中，配置数据库的信息。

步骤5 单击“确定”，数据库列表中将新增一条“审计状态”为“已关闭”的数据库。

----结束

添加数据库安装 Agent

表 1-3 需安装 Agent 的数据库类型和版本

数据库类型	版本
MySQL	• 5.0、5.1、5.5、5.6、5.7 • 8.0（8.0.11及以前的子版本） • 8.0.30 • 8.0.35 • 8.1.0 • 8.2.0
Oracle (因Oracle为闭源协议，适配版本复杂，如您需审计Oracle数据库，请先联系客服人员)	• 11g 11.1.0.6.0 、11.2.0.1.0 、11.2.0.2.0、11.2.0.3.0、11.2.0.4.0 • 12c 12.1.0.2.0 、12.2.0.1.0 • 19c
PostgreSQL	• 7.4 • 8.0、8.1、8.2、8.3、8.4 • 9.0、9.1、9.2、9.3、9.4、9.5、9.6 • 10.0、10.1、10.2、10.3、10.4、10.5 • 11 • 12 • 13 • 14
SQLServer	• 2008 • 2012 • 2014 • 2016 • 2017
GaussDB(for MySQL)	MySQL 8.0
DWS	• 1.5 • 8.1
DAMENG	DM8
KINGBASE	V8

数据库类型	版本
SHENTONG	V7.0
GBase 8a	V8.5
GBase 8s	V8.8
Gbase XDM Cluster	V8.0
Greenplum	V6.0
HighGo	V6.0
GaussDB	• 1.3企业版 • 1.4企业版 • 2.8企业版 • 3.223企业版
MongoDB	V5.0
DDS	4.0
Hbase （华为云审计实例：23.02.27.182148 及其之后的版本支持）	• 1.3.1 • 2.2.3
Hive （华为云审计实例：23.02.27.182148 及其之后的版本支持）	• 1.2.2 • 2.3.9 • 3.1.2 • 3.1.3
MariaDB	10.6
TDSQL	10.3.17.3.0
Vastbase	G100 V2.2
TiDB	• V4 • V5 • V6 • V7 • V8

步骤1 添加数据库。

1. 在左侧导航树中，选择“数据库列表”，进入数据库列表界面。
2. 在“选择实例”下拉列表框中，选择需要添加数据库的实例。
3. 在数据库列表框左上方，单击“添加数据库”。
4. 在弹出的对话框中，配置数据库的信息。

5. 单击“确定”，数据库列表中将新增一条“审计状态”为“已关闭”的数据库。

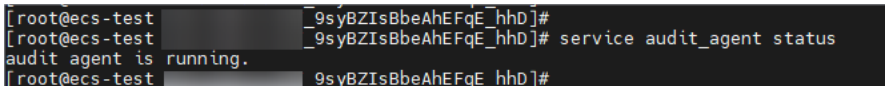
步骤2 添加Agent。

1. 在左侧导航树中，选择“数据库列表”，进入数据库列表界面。
2. 在“选择实例”下拉列表框中，选择需要添加Agent的数据库所属的实例。
3. 在添加的数据库所在行的“Agent”列，单击“添加Agent”。
4. 在弹出的“添加Agent”对话框中，选择添加方式。
5. 单击“确定”，Agent添加成功。

步骤3 下载并安装Agent。

1. 在左侧导航树中，选择“数据库列表”，进入数据库列表界面。
2. 在“选择实例”下拉列表框中，选择需要下载Agent的数据库所属的实例。
3. 单击“数据库列表”列表页面下方的 ^ 展开Agent的详细信息，在Agent所在行的“操作”列，单击“下载agent”。将Agent安装包下载到本地。
4. 安装Agent。
   a. 将下载的Agent安装包“xxx.tar.gz”上传到待安装Agent的节点（例如使用WinSCP工具）。
   b. 使用跨平台远程访问工具（例如PuTTY）以**root**用户通过SSH方式，登录该节点。
   c. 执行以下命令，进入Agent安装包“xxx.tar.gz”所在目录。
      cd *Agent安装包所在目录*
   d. 执行以下命令，解压缩“xxx.tar.gz”安装包。
      tar -xvf xxx.tar.gz
   e. 执行以下命令，进入解压后的目录。
      cd *解压后的目录*
   f. 执行以下命令，安装Agent。
      sh install.sh
   g. 执行以下命令，查看Agent程序的运行状态。
      service audit_agent status

      如果界面回显以下信息，说明Agent程序运行正常。

      audit agent is running.

----结束

步骤三 开启数据库安全审计

步骤1 开启数据库安全审计。

1. 在左侧导航树中，选择“数据库列表”，进入数据库列表界面。
2. 在选择实例下拉框中，选择需要开启审计的数据库安全审计实例。
3. 在待开启审计所在行的“操作”列，单击“开启”，开启审计功能。
   审计功能开启后，该数据库的“审计状态”为“已开启”，不需要重启数据库。

步骤2 验证审计结果。

1. 开启审计后，在数据库上执行一条SQL语句（例如“show databases”）。

2. 在左侧导航栏选择“数据报表”，进入“数据报表”页面。
3. 在“选择实例”下拉列表框中，选择需要验证的数据库所属的实例。
4. 选择“语句”页签。
5. 在“时间”所在行右侧，单击 ，选择开始时间和结束时间，单击“提交”，SQL语句列表将显示**图1-1**中输入的SQL语句。

图 1-1 查看 SQL 语句

----结束

相关操作

为了有效的审计数据库，您还可以自定义配置审计规则，并查看审计结果和监控信息，帮助您对内部违规和不正当操作进行定位追责，保障数据资产安全。相关操作请参考**配置审计规则**、**查看审计结果**和**查看监控信息**。

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） **审计RDS关系型数据库（免安装Agent）**	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）数量多），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、源SQL语句、操作等，协助您溯源到攻击者。