数据库安全服务

产品介绍

文档版本 25

发布日期 2025-12-15

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 什么是数据库安全服务?

数据库安全服务（Database Security Service，DBSS）提供数据库安全审计、数据库加密与访问控制功能，数据库审计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。数据库加密与访问控制将系统作为代理加密网关，部署在数据库和客户端应用程序之间，任何访问都需要经过该网关，从而实现数据加密和访问控制功能。

数据库安全审计

数据库安全审计采用数据库旁路部署方式，支持对华为云上的RDS、ECS/BMS自建的数据库进行审计。

图 1-1 数据库安全审计部署架构

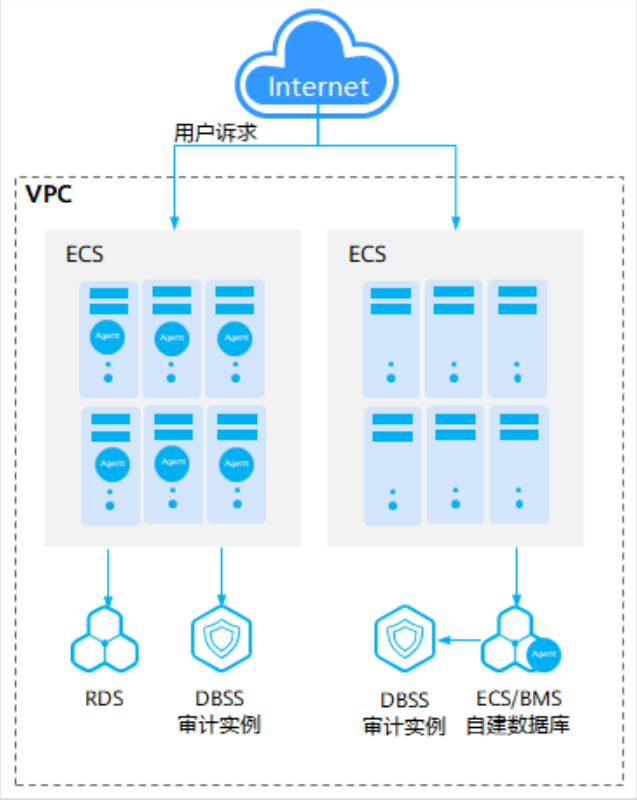


图 1-2 组网方式

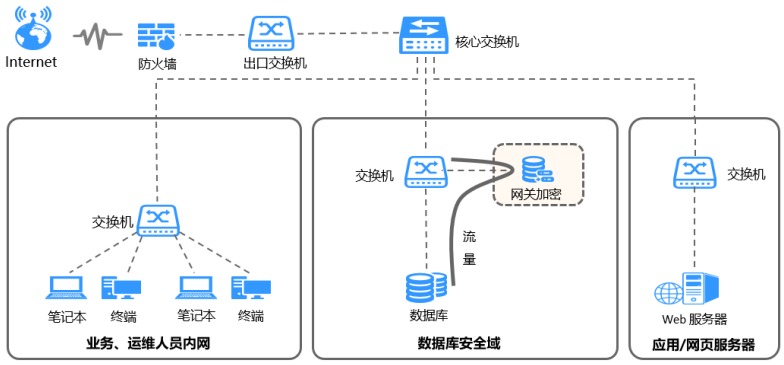


图 1-3 实现流程

数据库安全审计的Agent部署说明如下：

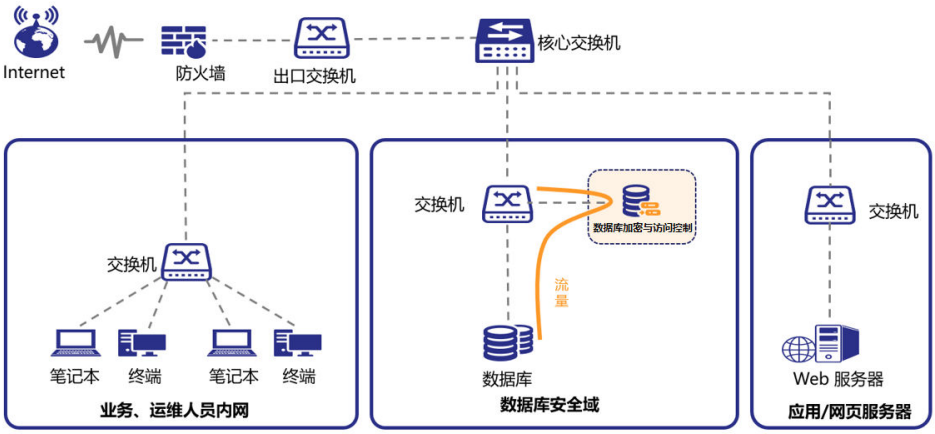
- ECS/BMS自建数据库：在数据库端部署Agent
- RDS关系型数据库：在应用端或代理端部署Agent

数据库安全加密

数据库加密与访问控制是一款基于网关代理加密技术，实现敏感数据加密存储的数据库安全防护产品。

系统作为代理加密网关，部署在数据库和客户端应用程序之间，任何访问都需要经过该网关，从而实现数据加密和访问控制功能。

图 1-4 组网方式



服务特点

- 助力企业满足等保合规要求
  - 满足等保测评数据库审计需求
  - 满足国内外安全法案合规需求，提供满足数据安全标准（例如Sarbanes-Oxley）的合规报告
- 支持备份和恢复数据库审计日志，满足审计数据保存期限要求
- 支持风险分布、会话统计、会话分布、SQL分布的实时监控能力
- 提供风险行为和攻击行为实时告警能力，及时响应数据库攻击
- 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

数据库安全审计采用数据库旁路部署方式，在不影响用户业务的前提下，可以对数据库进行灵活的审计。

- 基于数据库风险操作，监视数据库登录、操作类型（数据定义、数据操作和数据控制）和操作对象，有效对数据库进行审计。
- 从风险、会话、SQL注入等多个维度进行分析，帮助您及时了解数据库状况。
- 提供审计报表模板库，可以生成日报、周报或月报审计报表（可设置报表生成频率）。同时，支持发送报表生成的实时告警通知，帮助您及时获取审计报表。

2 产品优势

数据库安全审计

数据库安全审计提供的旁路模式数据库审计功能，可以对风险行为进行实时告警。同时，通过生成满足数据安全标准的合规报告，可以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。

- 部署简单
  采用数据库旁路部署方式，操作简单，快速上手。
- 全量审计
  支持对华为云上的RDS、ECS/BMS自建的数据库进行审计。
- 快速识别
  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。
- 多种合规
  - 满足等保三级数据库审计需求。
  - 满足网安法，SOX等国内外法案。
- 三权分立
  系统管理员，安全管理员，审计管理员权限分离，满足审计安全需求。

数据库安全加密

- 采用网关加密技术
  免插件、免改造方案，适合新旧应用零改造上线。
- 支持密文模糊查询
  加密后的模糊查询可以正常执行，无需业务适配，提升业务兼容性。
- 精细化授权
  基于数据库的权控加设二级访问授权，防止高危操作。
- 密文索引加速
  通过密文索引加速技术，1000万量级数据表的密文列随机查询时间由21.7s提速达到6ms。

- 高可靠性保证
  支持双机热备，实现快速切换。

3 产品功能

配置数据库

数据库安全审计支持对华为云上的RDS关系型数据库、ECS/BMS自建数据库进行审计。购买数据库安全审计实例后，您需要将待审计的数据库添加至数据库安全审计实例中。成功添加数据库后，您可以查看数据库信息、关闭、删除数据库。

配置 Agent

将待审计数据库添加至数据库安全审计实例后，您需要根据您在云上实际部署的数据库选择添加Agent的方式以及在应用端或数据库端安装Agent。Agent程序会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，帮助您实现对数据库的安全审计。安装Agent后，您才能开启数据库安全审计。支持在Linux操作系统和Windows操作系统安装Agent。数据库添加了Agent，您还可以查看Agent信息、关闭或删除Agent。

配置安全组规则

Agent添加完成后，您需要为数据库安全审计实例所在的安全组添加入方向规则TCP协议（8000端口）和UDP协议（7000-7100端口），使Agent与审计实例之间的网络连通，数据库安全审计才能对添加的数据库进行审计。

配置审计范围

数据库安全审计默认提供一条“全审计规则”的审计范围，可以对成功连接数据库安全审计的所有数据库进行安全审计。您也可以通过添加审计范围，设置需要审计的数据库范围。添加审计范围后，您可以查看审计范围信息，启用、编辑、禁用或删除审计范围。

SQL 注入

数据库安全审计的SQL注入检测默认开启，您可以禁用或启用SQL注入的检测规则。一条审计数据只能命中SQL注入检测中的一个规则。

隐私数据保护

当需要对输入的SQL语句的敏感信息进行脱敏时，您可以通过开启隐私数据脱敏功能，以及配置隐私数据脱敏规则，防止数据库用户敏感信息泄露。

告警通知

通过设置告警通知，当数据库发生设置的告警事件时，您可以收到DBSS发送的告警通知，及时了解数据库的安全风险。否则，无论是否有危险，您都只能登录管理控制台自行查看，无法收到告警信息。告警通知信息可能会被误拦截，若您未收到相关告警信息，请在信息拦截中查看。系统每5分钟进行一次告警统计，并触发告警通知。

审计日志

数据库安全审计支持将数据库的审计日志备份到OBS桶，实现高可用容灾。您可以根据需要备份或恢复数据库审计日志。备份审计日志后，您可以查看备份的审计日志信息，或删除备份的审计日志。

实例管理

成功购买数据库安全审计实例后，您可以查看实例信息，开启、重启或关闭实例。

风险操作管理

成功添加风险操作后，您可以查看风险操作信息，启用、编辑、禁用、删除风险操作，或设置风险操作优先级。

报表管理

数据库安全审计默认提供一条“全审计规则”的审计范围，可以对成功连接数据库安全审计的所有数据库进行审计。添加的数据库连接到数据库安全审计实例后，您可以查看报表模板信息和报表结果。

数据库安全加密

- 数据加密

  系统支持对数据进行加密和完整性校验，满足等保、分保等评测要求，同时也满足商用密码系统应用与安全性评估的存储数据完整性和机密性保障的评测要求。

  - 加密算法：支持AES算法和SM4国密算法。
  - 完整性校验算法：支持AES-GCM算法和SM3-HMAC算法。

- 访问控制

  系统具有独立于数据库的访问授权机制，拥有合法访问权限可以访问加密数据，非授权用户无法访问加密数据，从而有效防止管理员越权访问及黑客拖库。

  系统支持系统管理员，安全管理员，审计管理员的三权分立管理，增强数据库使用的安全合规性

4 服务版本差异

数据库安全审计提供了专业版和高级版两种服务版本。您可以根据业务需求选择相应的服务版本。

各版本的性能规格说明如表4-1所示。

表 4-1 数据库安全服务版本规格说明

版本	支持的数据库实例	性能参数
专业版	最多支持6个数据库实例	• 吞吐量峰值：6,000条/秒 • 入库速率：720万条/小时 • 在线SQL语句存储：6亿条
高级版	最多支持30个数据库实例	• 吞吐量峰值：30,000条/秒 • 入库速率：1,080万条/小时 • 在线SQL语句存储：15亿条

说明

- 数据库实例通过**数据库IP+数据库端口**计量。

  如果同一数据库IP具有多个数据库端口，数据库实例数为数据库端口数。1个数据库IP只有1个数据库端口，即为一个数据库实例；1个数据库IP具有N个数据库端口，即为N个数据库实例。

  例如：用户有2个数据库资产分别为IP_1和IP_2，IP_1有一个数据库端口，则为1个数据库实例；IP_2有3个数据库端口，则为3个数据库实例。IP_1和IP_2合计为4个数据库实例，选择服务版本规格时需要大于或等于4个数据库实例，即选用专业版（最多支持审计6个数据库实例）。
- 不支持修改规格。若要修改，请退订后重购。
- 本表中的系统资源要求，是指购买数据库安全审计实例时会消耗的系统资源。购买时，用户的系统需要满足审计版本对应的配置。
- 本表中在线SQL语句的条数，是按照每条SQL语句的容量为1KB来计算的。

数据库安全服务提供多种类型，多种版本的规格，您可以根据业务需求选择相应的服务版本。

表 4-2 数据库安全服务版本性能规格说明

版本规格	性能规格	支持的数据库实例	系统资源要求	性能参数
入门版	数据库审计入门版	最多支持1个数据库实例	-	• 吞吐量峰值：1,000条/秒 • 入库速率：120万条/小时 • 在线SQL语句存储：1亿条
基础版	数据库审计基础版	最多支持3个数据库实例	-	• 吞吐量峰值：3,000条/秒 • 入库速率：360万条/小时 • 在线SQL语句存储：4亿条
专业版	数据库审计专业版	最多支持6个数据库实例	-	• 吞吐量峰值：6,000条/秒 • 入库速率：720万条/小时 • 在线SQL语句存储：6亿条
	数据库审计运维增强版	最多支持10个数据库实例	• CPU：8U • 内存：16GB	• 性能：35000QPS • 最大并发连接数：5000
高级版	数据库审计高级版	最多支持30个数据库实例	-	• 吞吐量峰值：30,000条/秒 • 入库速率：1,080万条/小时 • 在线SQL语句存储：15亿条
	数据库审计加密增强版	最多支持10个数据库实例	• CPU：16U • 内存：32GB	• 加解密性能：40000QPS • 最大并发连接数：3000

5 个人数据保护机制

为了确保网站访问者的个人数据（例如用户名、密码、手机号码等）不被未经过认证、授权的实体或者个人获取，DBSS通过控制个人数据访问权限以及记录操作日志等方法防止个人数据泄露，保证您的个人数据安全。

收集范围

DBSS收集及产生的个人数据如表5-1所示。

表 5-1 个人数据范围列表

类型	收集方式	是否可以修改	是否必须
用户名	在登录管理台时，由用户在登录界面输入。	否	是 用户名是用户的身份标识信息
邮箱	在数据库安全审计设置邮件通知时，由用户在界面输入。	是	否

存储方式

- 用户名：不属于敏感数据，明文存储。
- 邮箱：加密存储。

访问权限控制

拥有“DBSS System Administrator”权限的用户才可以设置邮箱通知，且用户只能查看自己业务的邮箱信息。

日志记录

用户个人数据的所有非查询类操作，包括创建、删除实例等，DBSS都会记录审计日志并上传至云审计服务（CTS），用户仅可以查看自己的审计日志。

6 安全

6.1 资产识别与管理

DBSS服务实例创建在用户的弹性云服务器上，用户通过该实例，为RDS、ECS/BMS自建的数据库提供安全审计功能。

DBSS对接了RMS（资源管理服务）、TMS（标签管理服务），用户可通过登录这些服务页面查看DBSS实例信息。

6.2 身份认证与访问控制

- 身份认证

  用户访问DBSS的方式有多种，包括DBSS控制台、API、SDK，无论访问方式封装成何种形式，其本质都是通过DBSS提供的REST风格的API接口进行请求。

  DBSS的接口需要经过认证请求后才可以访问成功。DBSS支持如下认证方式：

  - Token认证：通过Token认证调用请求，访问DBSS控制台默认使用Token认证机制。
  - AK/SK认证：通过AK（Access Key ID）/SK（Secret Access Key）加密调用请求。推荐使用AK/SK认证，其安全性比Token认证要高。

- 访问控制

  DBSS支持通过权限控制（IAM权限）进行访问控制。

表 6-1 DBSS 访问控制

访问控制方式		简要说明	详细介绍
权限控制	IAM权限	IAM权限是作用于云资源的，IAM权限定义了允许和拒绝的访问操作，以此实现云资源权限访问控制。管理员创建IAM用户后，需要将其加入用户组，并给用户组授予策略或角色，才能使得用户组中的用户获得对应的权限。	**IAM权限介绍** **DBSS权限管理** **DBSS权限管理（细粒度）**

6.3 数据保护技术

DBSS通过多种数据保护手段和特性，保证审计、存储在DBSS中的数据安全可靠。

表 6-2 DBSS 的数据保护手段和特性

数据保护手段	简要说明	详细介绍
传输加密（HTTPS）	DBSS支持HTTP和HTTPS两种传输协议，为保证数据传输的安全性，推荐您使用更加安全的HTTPS协议。	构造请求
个人数据保护	DBSS通过控制个人数据访问权限以及记录操作日志等方法防止个人数据泄露，保证您的个人数据安全。	个人数据保护机制
隐私数据保护	DBSS会对存储的用户审计数据进行敏感数据脱敏。	管理隐私数据保护规则
数据备份	DBSS支持用户手动、自动备份审计日志。备份日志后，审计日志将备份到OBS中。	备份和恢复数据库审计日志
数据销毁	DBSS在用户主动删除实例，或用户销户的情况下，会删除对应用户的审计实例。	-

6.4 审计与日志

- 审计

DBSS向用户提供数据库审计功能，可以对普通用户、管理员账户的所有活动情况进行审计，并生成合规性报告。DBSS通过记录流量、入侵、异常监控、数据脱敏、远程工作等日志，锁定异常操作到人，对特定事件实时告警，对TOP活动进行可视化呈现，满足ISO27001、信息安全等级保护测评等合规场景下对数据库审计的要求。

表 6-3 DBSS 审计功能

功能特性	功能详情
系统行为审计	系统操作行为全纪录，针对您设置的高、中、低风险行为、发送告警通知。 • **SQL注入检测**：DBSS提供“添加SQL注入规则”，您可根据需要自定义添加对应的SQL规则，添加后可以对成功连接数据库安全审计的所有数据进行安全审计。 • **风险操作检测**：DBSS内置了“数据库拖库检测”、“数据库慢SQL检测”、“批量数据篡改检测”和“批量数据删除检测”四条检测规则，帮助您及时发现数据库安全风险。同时，您也可以通过添加风险操作，自定义数据库需要审计的风险操作规则。 • **告警通知**：通过配置系统告警，针对系统操作和系统环境制定不同告警方式和告警级别，以邮件方式和系统消息方式推送告警通知，以便及时发现系统异常和用户异常操作。

同时DBSS已经接入云审计服务（Cloud Trace Service，CTS），是华为云安全解决方案中专业的日志审计服务，提供对各种云资源操作记录的收集、存储和查询功能，可用于支撑安全分析、合规审计、资源跟踪和问题定位等常见应用场景。

用户开通云审计服务并创建和配置追踪器后，CTS可记录DBSS的管理事件用于审计。

CTS的详细介绍和开通配置方法，请参见**CTS快速入门**。

CTS支持追踪的DBSS操作列表，请参见**云审计服务支持的DBSS操作列表**。

- 日志

出于分析或审计等目的，用户开启了云审计服务后，系统开始记录DBSS资源的操作。云审计服务管理控制台保存最近7天的操作记录。

关于DBSS云审计日志的查看，请参见**如何查看云审计日志**。

6.5 服务韧性

DBSS提供四层可靠性架构，通过检测、承受、恢复和适应四个方面保障系统在收到攻击后可以手动、自动恢复服务能力，保障服务和数据的持久性和可靠性。

表 6-4 DBSS 可信架构分类

可信架构分类	可信架构能力项	目标	分类
检测	入侵检测	支持主机异常检测，部署主机安全服务，检测率准确率98%以上。检测时长1分钟	安全
	监控	针对微服务的异常日志出对应的告警	系统

可信架构分类	可信架构能力项	目标	分类
承受	数据备份	支持关键数据100%备份，即使数据库遭到完全损坏，也可以根据以前备份数据恢复业务。 用户业务日志备份到OBS	系统
	快速响应	AZ级或Region级服务故障时，快速检测和恢复。DBSS本身属于旁路业务，不会影响业务系统。	系统
	服务解耦	微服务化，微服务独立部署和启停	系统
恢复	虚机级恢复	虚机级恢复：单虚拟机故障，支持自动重建和手工重建	系统
	系统级恢复	系统级的恢复：自动恢复和系统手工恢复能力。	系统
适应	密钥自动轮转	SCC密钥动态轮转	安全
	证书自动轮转	内部微服务通信证书动态轮转	安全
	账号口令自动轮转	服务账号口令动态轮转	安全

6.6 监控安全风险

DBSS提供基于云监控服务CES的资源和操作监控能力，帮助用户查看DBSS的相关指标，及时了解数据库安全状况。

用户可以实时掌握DBSS实例的CPU使用率、内存使用率和磁盘使用率等信息。

关于DBSS支持的监控指标，如何设置监控告警规则以及查看监控指标等内容，请参见**监控**章节。

6.7 认证证书

合规证书

华为云服务及平台通过了多项国内外权威机构（ISO/SOC/PCI等）的安全合规认证，用户可自行**申请下载**合规资质证书。

图 6-1 合规证书下载

资源中心

华为云还提供以下资源来帮助用户满足合规性要求，具体请查看**资源中心**。

图 6-2 资源中心

7 约束与限制

7.1 数据库安全审计

数据库安全审计支持云上数据库及云下或其他云数据库（需数据库与审计实例网络连接正常），对于云上的数据库支持以下类型：

- 云数据库
- 弹性云服务器（Elastic Cloud Server ，ECS）的自建数据库
- 裸金属服务器（Bare Metal Server，BMS）的自建数据库

支持免安装 Agent 数据库类型及版本

部分数据库类型及版本支持免安装Agent方式，如表7-1所示。

表 7-1 支持免 Agent 安装的关系型数据库

数据库类型	支持的版本
TaurusDB	默认都支持
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

数据库类型	支持的版本
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 MariaDB	默认都支持

支持安装 Agent 数据库类型及版本

数据库安全审计支持的数据库类型及版本如表7-2所示。

表 7-2 数据库安全审计支持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 • 8.0.33 • 8.0.35 • 8.1.0 • 8.2.0
Oracle	• 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

数据库类型	版本
SQL Server	• 2008 • 2012 • 2014 • 2016 • 2017
TaurusDB	8.0
DWS	• 1.5 • 8.1
DAMENG	DM8
KINGBASE	V8
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	• 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

数据库类型	版本
TiDB	• V4 • V5 • V6 • V7 • V8

Agent 支持的操作系统

使用数据库安全审计功能，必须在数据库节点或应用节点安装Agent。数据库安全审计的Agent可运行在Linux64位和Windows64位操作系统上。

- 数据库安全审计的Agent支持的Linux系统版本如表7-3所示。

表 7-3 Agent 支持的 Linux 系统版本说明

系统名称	系统版本
CentOS	• CentOS 7.0 (64bit) • CentOS 7.1 (64bit) • CentOS 7.2 (64bit) • CentOS 7.3 (64bit) • CentOS 7.4 (64bit) • CentOS 7.5 (64bit) • CentOS 7.6 (64bit) • CentOS 7.8 (64bit) • CentOS 7.9 (64bit) • CentOS 8.0 (64bit) • CentOS 8.1 (64bit) • CentOS 8.2 (64bit)
Debian	• Debian 7.5.0 (64bit) • Debian 8.2.0 (64bit) • Debian 8.8.0 (64bit) • Debian 9.0.0 (64bit) • Debian 10.0.0 (64bit)
Fedora	• Fedora 24 (64bit) • Fedora 25 (64bit) • Fedora 29 (64bit) • Fedora 30 (64bit)

系统名称	系统版本
OpenSUSE	• SUSE 13 (64bit) • SUSE 15 (64bit) • SUSE 42 (64bit)
SUSE	• SUSE 11 SP4 (64bit) • SUSE 12 SP1 (64bit) • SUSE 12 SP2 (64bit)
Ubuntu	• Ubuntu 14.04 (64bit) • Ubuntu 16.04 (64bit) • Ubuntu 18.04 (64bit) • Ubuntu 20.04 (64bit)
EulerOS	• Euler 2.2 (64bit) • Euler 2.3 (64bit) • Euler 2.5 (64bit)
OpenEuler	• OpenEuler 20.03 (64bit)
Oracle Linux	• Oracle Linux 6.9 (64bit) • Oracle Linux 7.4 (64bit)
Red Hat	• Red Hat Enterprise Linux 7.4 (64bit) • Red Hat Enterprise Linux 7.6 (64bit)
NeoKylin	• NeoKylin 7.0 (64bit)
Kylin	• Kylin Linux Advanced Server release V10 (64bit)
Uniontech OS	• Uniontech OS Server 20 Enterprise (64bit)
Huawei Cloud Euler	• Huawei Cloud Euler 2.0 (64bit)
KylinSec	• KylinSec 3.4（64bit）
Anolis OS	• 7.9（64bit） • 8.4（64bit） • 8.6（64bit）

- 数据库安全审计的Agent支持的Windows系统版本如下所示：
  - Windows Server 2008 R2(64bit)
  - Windows Server 2012 R2(64bit)
  - Windows Server 2016(64bit)
  - Windows Server 2019(64bit)
  - Windows 7(64bit)

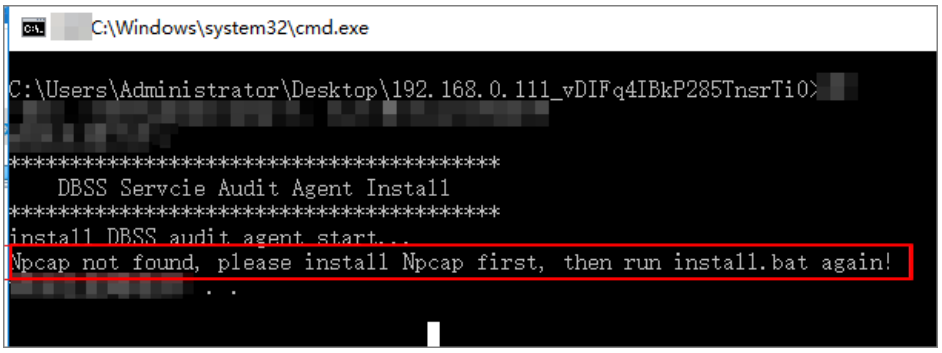
- Windows 10(64bit)

说明

DBSS Agent的运行依赖Npcap，如果安装过程中提示"Npcap not found，please install Npcap first"，请安装Npcap后，再安装DBSS Agent。

安装前先**下载Npcap**。

图 7-1 Npcap not found



其他约束条件

- 数据库安全审计不支持跨区域（Region）使用。待审计的数据库必须和购买申请的数据库安全审计实例在同一区域。
- Windows操作系统的Agent不支持审计IPv6数据库。
- 数据库开启SSL时，将不能使用数据库安全审计功能。如果您需要使用数据库安全审计功能，请关闭数据库的SSL。关闭数据库SSL的详细操作，请参见**如何关闭数据库SSL?** 。
- 购买数据库安全审计配置VPC时，需与Agent安装节点（应用端或数据库端）所在的VPC保持一致。否则，将导致Agent与审计实例之间的网络不通，无法使用数据库安全审计。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?**
- 部分SQL Server中的复杂declare语句、select函数和包含系统无法识别的符号语句可能无法解析。
- 免安装Agent的所有数据库都不支持记录SQL请求结果，安装Agent仅SQL Server、PostgreSQL、MySQL数据库支持记录SQL请求结果（需开启存储结果集开关，默认关闭，详情请参见**配置隐私数据保护规则**）。
- 在对免Agent的GaussDB和RDS for MariaDB数据库进行审计时，由于部分字段和部分场景下数据库的日志不会进行记录，因此DBSS侧无法进行审计。
- 在对免Agent的PostgreSQL、RDS for SQLServer、RDS for MySQL、GaussDB for mysql(TaurusDB)和RDS for MySQL数据库进行审计时，不支持审计登录登出语句。

7.2 数据库安全加密

数据库加密支持纳管的数据库及版本

在系统中添加数据资产（即数据库）后，您可以对数据库进行敏感数据识别，对敏感信息进行加解密、脱敏等操作。

数据库安全加密支持的数据库类型及版本如表7-4所示。

表 7-4 数据库安全加密支持的数据库类型和版本

数据库类型	版本
MySQL	• 5.5、5.6、5.7 • 8.0
Oracle	• 11g • 12c
PostgreSQL	• 9.4 • 11.5
SQL Server	2012
DAMENG	• DM6 • DM7.6 • DM8.1
KINGBASE	• V8R3 • V8R6
TBASE	V2.15
HOTDB	2.5.6
GaussDB	A
TDSQL	10.3

8 权限管理

如果您需要对华为云上购买的数据库安全服务（DBSS）资源，为企业中的员工设置不同的访问权限，以达到不同员工之间的权限隔离，您可以使用统一身份认证服务（Identity and Access Management，简称IAM）进行精细的权限管理。该服务提供用户身份认证、权限分配、访问控制等功能，可以帮助您安全的控制华为云资源的访问。如果华为账号已经能满足您的要求，不需要通过IAM对用户进行权限管理，您可以跳过本章节，不影响您使用DBSS服务的其它功能。

IAM是华为云提供权限管理的基础服务，无需付费即可使用，您只需要为您账号中的资源进行付费。

通过IAM，您可以通过授权控制他们对华为云资源的访问范围。例如您的员工中有负责软件开发的人员，您希望他们拥有DBSS的使用权限，但是不希望他们拥有删除DBSS等高危操作的权限，那么您可以使用IAM进行权限分配，通过授予用户仅能使用DBSS，但是不允许删除DBSS的权限，控制他们对DBSS资源的使用范围。

目前IAM支持两类授权，一类是角色与策略授权，另一类为身份策略授权。

两者有如下的区别和关系：

表 8-1 两类授权的区别

名称	核心关系	涉及的权限	授权方式	适用场景
角色与策略授权	用户-权限-授权范围	• 系统角色 • 系统策略 • 自定义策略	为主体授予角色或策略	核心关系为“用户-权限-授权范围”，每个用户根据所需权限和所需授权范围进行授权，无法直接给用户授权，需要维护更多的用户组，且支持的条件键较少，难以满足细粒度精确权限控制需求，更适用于对细粒度权限管控要求较低的中小企业用户。

名称	核心关系	涉及的权限	授权方式	适用场景
身份策略授权	用户-策略	• 系统身份策略 • 自定义身份策略	• 为主体授予身份策略 • 身份策略附加至主体	核心关系为“用户-策略”，管理员可根据业务需求定制不同的访问控制策略，能够做到更细粒度更灵活的权限控制，新增资源时，对比角色与策略授权，基于身份策略的授权模型可以更快速地直接给用户授权，灵活性更强，更方便，但相对应的，整体权限管控模型构建更加复杂，对相关人员专业能力要求更高，因此更适用于中大型企业。

例如：如果需要对IAM用户授予可以创建华北-北京四区域的ECS和华南-广州区域的OBS的权限，基于角色与策略授权的场景中，管理员需要创建两个自定义策略，并且为IAM用户同时授予这两个自定义策略才可以实现权限控制。在基于身份策略授权的场景中，管理员仅需要创建一个自定义身份策略，在身份策略中通过条件键“g:RequestedRegion”的配置即可达到身份策略对于授权区域的控制。将身份策略附加主体或为主体授予该身份策略即可获得相应权限，权限配置方式更细粒度更灵活。

两种授权场景下的策略/身份策略、授权项等并不互通，推荐使用身份策略进行授权。

关于IAM的详细介绍，请参见**IAM产品介绍**。

角色与策略权限管理

DBSS服务支持角色与策略授权。默认情况下，管理员创建的IAM用户没有任何权限，需要将其加入用户组，并给用户组授予策略或角色，才能使得用户组中的用户获得对应的权限，这一过程称为授权。授权后，用户就可以基于被授予的权限对云服务进行操作。

DBSS部署时通过物理区域划分，为项目级服务。授权时，“授权范围”需要选择“指定区域项目资源”，然后在指定区域（如亚太-曼谷）对应的项目（ap-southeast-2）中设置相关权限，并且该权限仅对此项目生效；如果“授权范围”选择“所有资源”，则该权限在所有区域项目中都生效。访问DBSS时，需要先切换至授权区域。

如**表8-2**所示，包括了DBSS的所有系统权限。角色与策略授权场景的系统策略和身份策略授权场景的并不互通。

表 8-2 DBSS 系统权限与角色

系统角色/策略名称	描述	依赖关系
DBSS System Administrator （数据库安全服务系统管理员，拥有操作数据库安全服务系统资源的权限）	● 数据库安全审计操作权限： – 购买实例。 – 开启、关闭、重启实例。 – 获取实例列表。 – 获取基本信息。 – 获取审计概况。 – 获取监控信息。 – 获取操作日志。 – 数据库管理。 – Agent管理。 – 邮件设置。 – 备份与恢复。	进行付费操作（例如，购买DBSS实例、续费）时需要同时具有BSS Administrator角色、VPC Administrator角色和ECS Administrator角色。 ● VPC Administrator：对虚拟私有云的所有执行权限。项目级角色，在同项目中勾选。 ● BSS Administrator：对账号中心、费用中心、资源中心中的所有菜单项执行任意操作。项目级角色，在同项目中勾选。 ● ECS Administrator：对弹性云服务器的所有执行权限。项目级角色，在同项目中勾选。
DBSS Audit Administrator （数据库安全服务审计管理员，拥有审核数据库安全服务日志信息的权限）	● 数据库安全审计操作权限： – 获取实例列表。 – 获取基本信息。 – 获取审计概况。 – 获取报表结果。 – 获取规则信息。 – 获取语句信息。 – 获取会话信息。 – 获取监控信息。 – 获取操作日志。 – 获取数据库列表。 – 报表管理。	无

系统角色/策略名称	描述	依赖关系
DBSS Security Administrator （数据库安全服务安全管理员，拥有设置数据库安全服务安全策略的权限）	• 数据库安全审计操作权限： – 获取实例列表。 – 获取基本信息。 – 获取审计概况。 – 获取报表结果。 – 获取规则信息。 – 获取语句信息。 – 获取会话信息。 – 获取监控信息。 – 获取操作日志。 – 获取数据库列表。 – 审计规则设置。 – 告警通知设置。 – 报表管理。	无

表8-3列出了DBSS常用操作与系统权限的授权关系，您可以参照该表选择合适的系统权限。

表 8-3 常用操作与系统权限的关系

子服务	操作	DBSS System Administrator	DBSS Audit Administrator	DBSS Security Administrator
数据库安全审计	购买实例	√	×	×
	开启、关闭、重启实例	√	×	×
	获取实例列表	√	√	√
	获取基本信息	√	√	√
	获取审计概况	√	√	√
	获取监控信息	√	√	√
	获取操作日志	√	√	√

子服务	操作	DBSS System Administrator	DBSS Audit Administrator	DBSS Security Administrator
	数据库管理	√	×	×
	Agent管理	√	×	×
	邮件设置	√	×	×
	备份与恢复	√	×	×
	获取报表结果	√	√	√
	获取规则信息	√	√	√
	获取语句信息	√	√	√
	获取会话信息	√	√	√
	获取数据库列表	√	√	√
	报表管理	×	√	×
	审计规则设置	×	×	√
	告警通知设置	×	×	√

相关链接

- IAM产品介绍。

9 基于 IAM 进行访问控制

如果您需要对华为云上购买的数据库安全服务（DBSS）资源，为企业中的员工设置不同的访问权限，以达到不同员工之间的权限隔离，您可以使用统一身份认证服务（Identity and Access Management，简称IAM）进行精细的权限管理。该服务提供用户身份认证、权限分配、访问控制等功能，可以帮助您安全地控制华为云资源的访问。如果华为账号已经能满足您的要求，不需要通过IAM对用户进行权限管理，您可以跳过本章节，不影响您使用DBSS服务的其它功能。

IAM是华为云提供权限管理的基础服务，无需付费即可使用，您只需要为您账号中的资源进行付费。

通过IAM，您可以通过授权控制他们对华为云资源的访问范围。例如您的员工中有负责软件开发的人员，您希望他们拥有数据库安全服务（DBSS）的使用权限，但是不希望他们拥有删除DBSS等高危操作的权限，那么您可以使用IAM进行权限分配，通过授予用户仅能使用DBSS，但是不允许删除DBSS的权限，控制他们对DBSS资源的使用范围。

权限根据授权精细程度分为角色和策略。

- 角色：IAM最初提供的一种根据用户的工作职能定义权限的粗粒度授权机制。该机制以服务为粒度，提供有限的服务相关角色用于授权。由于华为云各服务之间存在业务依赖关系，因此给用户授予角色时，可能需要一并授予依赖的其他角色，才能正确完成业务。角色并不能满足用户对精细化授权的要求，无法完全达到企业对权限最小化的安全管控要求。
- 策略：IAM最新提供的一种细粒度授权的能力，可以精确到具体服务的操作、资源以及请求条件等。这是一种更加灵活的授权方式，能够满足企业对权限最小化的安全管控要求。例如：针对ECS服务，管理员能够控制IAM用户仅能对某一类云服务器资源进行指定的管理操作。多数细粒度策略以API接口为粒度进行权限拆分，权限的最小粒度为API授权项（action），数据库安全服务（DBSS）支持的API授权项请参见权限及授权项说明。

目前IAM支持两类授权模型，一类是经典授权（RBAC）模型，称为角色授权。

默认情况下，新建的主体没有任何权限，需要为主体授予系统角色、系统策略或自定义策略，并选择授权范围，才能使主体获得相应的权限。

另一类是基于ABAC的新模型，称为策略授权。管理员可根据业务需求定制不同的访问控制策略，将策略附加主体或为主体授予该策略即可获得相应权限，能够做到更细粒度更灵活的权限控制。授权后，主体就可以基于已有权限对云服务进行操作。

两者有如下的区别和关系：

表 9-1 角色授权与策略授权的区别

名称	核心关系	涉及的权限	授权方式	适用场景
角色授权	用户-角色-权限	• 系统角色 • 系统策略 • 自定义策略	为主体授予角色或策略	每个用户可以根据被分配的角色相对快速地被授予相关权限，但灵活性较差，难以满足细粒度精确权限控制需求，更适用于对维护角色和授权关系工作量较小的中小企业用户。
策略授权	用户-策略	• 系统策略 • 自定义策略	• 为主体授予策略 • 策略附加至主体	新增资源时，对比角色授权需要维护所有相关角色，基于策略的授权模型仅需要维护较少的资源，可扩展性更强，更方便。但相对应的，整体模型构建更加复杂，对相关人员专业能力要求更高，因此更适用于中大型企业。

例如：如果需要对IAM用户授予可以创建华北-北京四区域的ECS和华南-广州区域的OBS的权限，基于角色授权的场景中，管理员需要创建两个自定义策略，并且为IAM用户同时授予这两个自定义策略才可以实现权限控制。在基于策略授权的场景中，管理员仅需要创建一个自定义策略，在策略中通过条件键“g:RequestedRegion”的配置即可达到策略对于授权区域的控制。将策略附加主体或为主体授予该策略即可获得相应权限，权限配置方式更细粒度更灵活。

两种授权模型场景下的策略、授权项等并不互通，推荐使用基于策略授权的模型进行授权。**角色授权系统权限**和**策略授权系统权限**分别介绍两种模型的系统权限。

数据库安全服务（DBSS）目前仅支持角色授权模型，该场景下支持的系统权限请参考**角色授权系统权限**。

关于IAM的详细介绍，请参见**IAM产品介绍**。

角色授权系统权限

DBSS服务支持基于角色授权的授权模型。默认情况下，管理员创建的IAM用户没有任何权限，需要将其加入用户组，并给用户组授予策略或角色，才能使得用户组中的用户获得对应的权限，这一过程称为授权。授权后，用户就可以基于被授予的权限对云服务进行操作。

DBSS部署时通过物理区域划分，为项目级服务。授权时，“授权范围”需要选择“指定区域项目资源”，然后在指定区域（如亚太-曼谷）对应的项目（ap-southeast-2）中设置相关权限，并且该权限仅对此项目生效；如果“授权范围”选择“所有资源”，则该权限在所有区域项目中都生效。访问DBSS时，需要先切换至授权区域。

如**表9-2**所示，包括了DBSS的所有系统权限。基于角色授权场景的系统策略与基于策略授权场景的并不互通。

表 9-2 DBSS 系统权限

系统角色/策略名称	描述	类别	依赖关系
DBSS System Administrator（数据库安全服务系统管理员，拥有操作数据库安全服务系统资源的权限）	● 数据库安全审计操作权限： – 购买实例。 – 开启、关闭、重启实例。 – 获取实例列表。 – 获取基本信息。 – 获取审计概况。 – 获取监控信息。 – 获取操作日志。 – 数据库管理。 – Agent管理。 – 邮件设置。 – 备份与恢复。	系统角色	进行付费操作（例如，购买DBSS实例、续费）时需要同时具有BSS Administrator角色、VPC Administrator角色和ECS Administrator角色。 ● VPC Administrator：对虚拟私有云的所有执行权限。项目级角色，在同项目中勾选。 ● BSS Administrator：对账号中心、费用中心、资源中心中的所有菜单项执行任意操作。项目级角色，在同项目中勾选。 ● ECS Administrator：对弹性云服务器的所有执行权限。项目级角色，在同项目中勾选。

系统角色/策略名称	描述	类别	依赖关系
DBSS Audit Administrator（数据库安全服务审计管理员，拥有审核数据库安全服务日志信息的权限）	• 数据库安全审计操作权限： – 获取实例列表。 – 获取基本信息。 – 获取审计概况。 – 获取报表结果。 – 获取规则信息。 – 获取语句信息。 – 获取会话信息。 – 获取监控信息。 – 获取操作日志。 – 获取数据库列表。 – 报表管理。	系统角色	无
DBSS Security Administrator（数据库安全服务安全管理员，拥有设置数据库安全服务安全策略的权限）	• 数据库安全审计操作权限： – 获取实例列表。 – 获取基本信息。 – 获取审计概况。 – 获取报表结果。 – 获取规则信息。 – 获取语句信息。 – 获取会话信息。 – 获取监控信息。 – 获取操作日志。 – 获取数据库列表。 – 审计规则设置。 – 告警通知设置。 – 报表管理。	系统角色	无

表9-3列出了DBSS常用操作与系统权限的授权关系，您可以参照该表选择合适的系统权限。

表 9-3 常用操作与系统权限的关系

操作	DBSS System Administrator	DBSS Audit Administrator	DBSS Security Administrator
购买实例	√	×	×
开启、关闭、重启实例	√	×	×

操作	DBSS System Administrator	DBSS Audit Administrator	DBSS Security Administrator
获取实例列表	√	√	√
获取基本信息	√	√	√
获取审计概况	√	√	√
获取监控信息	√	√	√
获取操作日志	√	√	√
数据库管理	√	×	×
Agent管理	√	×	×
邮件设置	√	×	×
备份与恢复	√	×	×
获取报表结果	×	√	√
获取规则信息	×	√	√
获取语句信息	×	√	√
获取会话信息	×	√	√
获取数据库列表	√	√	√
报表管理	×	√	√
审计规则设置	×	×	√
告警通知设置	×	×	√

策略授权系统权限

DBSS服务支持基于策略授权的授权模型。如表9-4所示，包括了DBSS基于策略授权中的所有系统策略。策略授权的系统策略与角色授权的系统策略并不互通。

表 9-4 DBSS 系统策略

系统策略名称	描述	策略类别
DBSS FullAccess	数据库安全服务所有权限。	系统策略
DBSS ReadOnlyAccess	数据库安全服务只读。	系统策略

表9-5列出了DBSS常用操作与系统策略的授权关系，您可以参照该表选择合适的系统策略。

表 9-5 常用操作与系统策略的关系

操作	DBSS FullAccess	DBSS ReadOnlyAccess
购买实例	√	×
开启、关闭、重启实例	√	×
获取实例列表	√	√
获取基本信息	√	√
获取审计概况	√	√
获取监控信息	√	√
获取操作日志	√	√
数据库管理	√	×
Agent管理	√	×
邮件设置	√	×
备份与恢复	√	×
获取报表结果	√	√
获取规则信息	√	√
获取语句信息	√	√
获取会话信息	√	√
获取数据库列表	√	√
报表管理	√	×
审计规则设置	√	×
告警通知设置	√	×

相关链接

- **IAM产品介绍**
- 通过角色/策略管理资源访问权限

10 与其他云服务的关系

与弹性云服务器的关系

数据库安全服务实例创建在弹性云服务器上，用户可以通过该实例，为弹性云服务器上的自建数据库提供安全审计功能。

与关系型数据库的关系

数据库安全服务可以为关系型数据库服务中的RDS实例提供安全审计功能。

与裸金属服务器的关系

数据库安全服务可以为裸金属服务器上的自建数据库提供安全审计功能。

与云审计服务的关系

云审计服务（Cloud Trace Service，CTS）记录数据库安全服务相关的操作事件，方便用户日后的查询、审计和回溯，具体请参见《云审计服务用户指南》。

表 10-1 云审计服务支持的数据库安全服务操作列表

操作名称	资源类型	事件名称
创建实例	dbss	createInstance
删除实例	dbss	deleteInstance
开启实例	dbss	startInstance
关闭实例	dbss	stopInstance
重启实例	dbss	rebootInstance
实例状态变化	dbss	cloudServiceInstanceStatus
创建包周期实例	dbss	cloudServiceInstanceCreate
实例元数据变化	dbss	updateMetaData
更新实例	dbss	upgradeInstance

操作名称	资源类型	事件名称
CBC调用云服务接口更新实例状态	dbss	cloudServiceInstanceStatus
CBC通知云服务订单发生变化	dbss	updateMetaData
包周期购买实例	dbss	cloudServiceInstanceCreate
添加标签	dbss	createTag
删除标签	dbss	deleteTag

与对象存储服务的关系

对象存储服务（Object Storage Service，简称OBS）是一个基于对象的海量存储服务，为客户提供海量、安全、高可靠、低成本的数据存储能力。数据库安全审计支持将数据库的审计日志备份到OBS桶，实现高可用容灾。

与消息通知服务的关系

消息通知服务（Simple Message Notification，简称SMN），是一个可拓展的高性能消息处理服务。

- 开启消息通知前，您需先配置“消息通知服务”。
- 开启消息通知服务后，当数据库设置的告警事件发生或生成报表时，您可以收到告警或报表生成的消息通知。
- 在“告警通知”界面，您可以根据运维计划开启告警消息通知或关闭告警消息通知。
- 在“报表管理”界面，您可以根据运维计划开启报表生成消息通知或关闭报表生成消息通知。

关于SMN的详细内容，请参见《消息通知服务用户指南》。

与云监控服务的关系

云监控服务（Cloud Eye）为用户提供一个针对弹性云服务器、带宽等资源的立体化监控平台。使您全面了解云上的资源使用情况、业务的运行状况，并及时收到异常报警做出反应，保证业务顺畅运行。详情请参见《云监控服务用户指南》

表 10-2 云监控服务支持的 DBSS 监控指标

指标名称	指标含义	取值范围	单位	进制	测量对象	监控周期
SQL注入告警个数	该指标用于统计测量对象的SQL注入告警个数	≥0 count	Count	不涉及	弹性云服务器	4分钟

指标名称	指标含义	取值范围	单位	进制	测量对象	监控周期
XSS跨站脚本漏洞告警个数	该指标用于统计测量对象的XSS跨站脚本漏洞告警个数	≥0 count	Count	不涉及	弹性云服务器	4分钟
Webshell上传告警个数	该指标用于统计测量对象的Webshell上传告警个数	≥0 count	Count	不涉及	弹性云服务器	4分钟
盗链告警个数	该指标用于统计测量对象的盗链告警个数	≥0 count	Count	不涉及	弹性云服务器	4分钟
IP黑名单告警个数	该指标用于统计测量对象的IP黑名单告警个数	≥0 count	Count	不涉及	弹性云服务器	4分钟
IP白名单告警个数	该指标用于统计测量对象的IP白名单告警个数	≥0 count	Count	不涉及	弹性云服务器	4分钟

与统一身份认证服务的关系

统一身份认证服务（Identity and Access Management，简称IAM）为数据库安全服务提供了权限管理的功能。

需要拥有DBSS System Administrator权限的用户才能使用DBSS。

如需开通该权限，请联系拥有Security Administrator权限的用户，详细内容请参考《统一身份认证服务用户指南》。

11 基本概念

双向审计

双向审计是DBSS对数据库的请求和响应都进行审计。

旁路模式

旁路模式（Bypass Mode）是一种系统运行模式，主要用于在设备或系统出现异常时绕过常规检核机制，确保核心功能继续运行。

DBSS在审计数据库时就采用的旁路模式，只对数据库进行审计，不影响业务，不与本地审计工具冲突。

云上云下/云内云外

云上/云内：华为云，常见描述如资源部署在云上/云内，指的就是资源部署在华为云。

云下/云外：非华为云，常见描述如资源部署在云下/云外，指的就是资源部署在非华为云的环境，如部署在其他的厂商云或线下的场景。

磁盘容量/使用率

磁盘在DBSS控制台的系统监控页面中为数据中心分区。

磁盘容量即DBSS数据中心分区的总可用内存大小。

磁盘使用即DBSS数据中心分区已使用的占比。