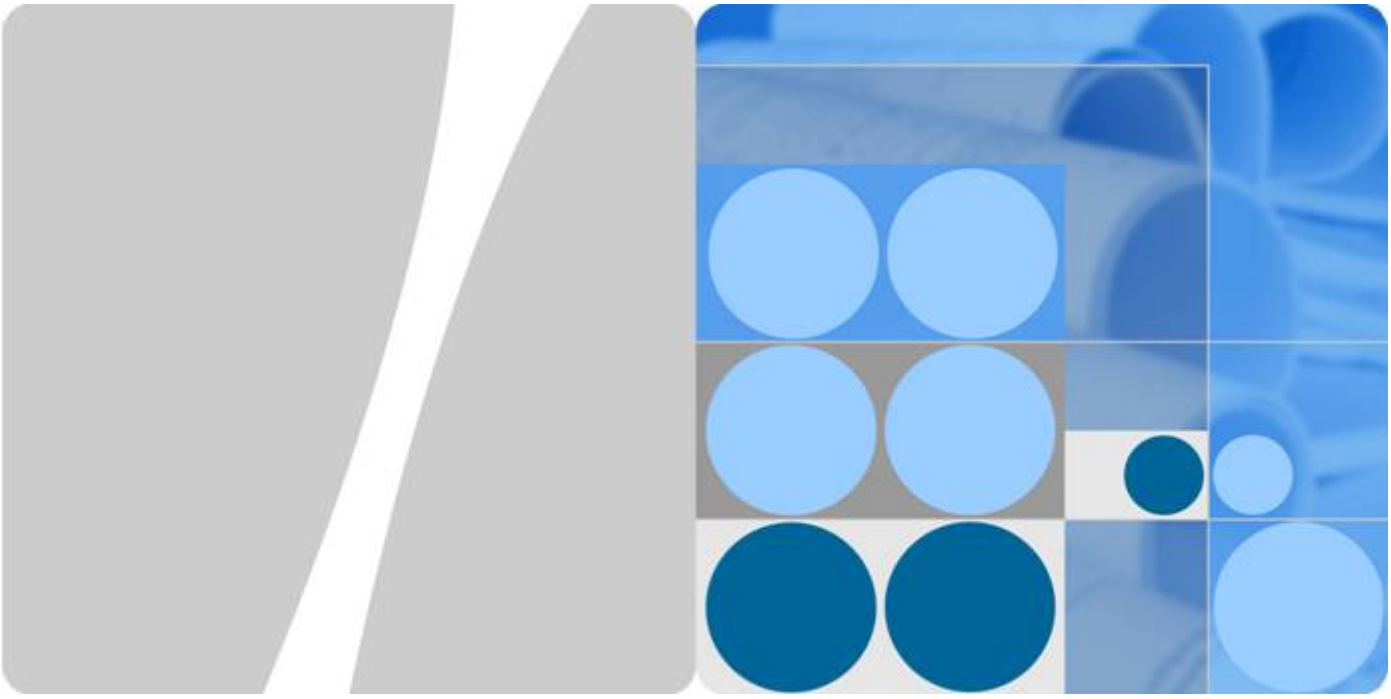


数据库安全服务

产品介绍

文档版本　39

发布日期　2019-10-24

华为技术有限公司

HUAWEI

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默示的声明或保证。

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 什么是数据库安全服务？

数据库安全服务，即DBSS（Database Security Service），包括数据库安全防护和数据库安全审计两大功能模块，提供数据泄露保护、数据库防火墙、数据库审计三大功能，可以全面保障云上数据库安全和资产安全。

数据库安全防护

数据库安全防护基于反向代理及机器学习机制，提供数据脱敏、数据库审计、敏感数据发现、数据库防拖库和防注入攻击等功能，保障云上数据库安全。

- 防攻击

  多种策略防止数据库被攻击，持续保护云上数据库安全。

- 数据脱敏

  敏感数据发现遵从行业合规性，发现用户数据库中的敏感数据，对敏感数据进行动态脱敏。

- 审计

  提供性能、数据、行为异常的监控，审计日志远端存储，满足合规性。

数据库安全防护通过对数据库安全防护实例进行安全防护配置操作，可以为华为云上的以下数据库提供数据库保护和审计功能：

- 关系型数据库（Relational Database Service，RDS）
- 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

说明

数据库安全防护支持DDM（Distributed Database Middleware，分布式数据库中间件），由于DDM机制问题，当前数据库安全防护仅支持DDM部分功能。有关DDM使用限制的详细说明，请参见**HexaTier功能使用限制**。

数据库安全防护支持数据库类型及版本为：

- Microsoft SQL Server 2008 - 2014
- MySQL 5.5 - 5.7
- PostgreSQL 9.4 - 9.5
- DWS 1.2.3

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。

数据库安全审计可以为华为云上的以下数据库提供旁路模式的数据库审计功能：

- 关系型数据库（Relational Database Service，RDS）
- 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

数据库安全审计支持数据库类型及版本为：

- MySQL
  - 5.0、5.1、5.5、5.6、5.7
  - 8.0
- 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
- 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

数据库安全审计可以帮助您解决以下问题：

- 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提前下，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 数据库安全防护和数据库安全审计的功能说明

数据库安全防护基于反向代理及机器学习机制，提供数据脱敏、数据库审计、敏感数据发现、数据库防拖库和防注入攻击等功能，保障云上数据库安全。

- 防攻击

  多种策略防止数据库被攻击，持续保护云上数据库安全。
- 数据脱敏

  敏感数据发现遵从行业合规性，发现用户数据库中的敏感数据，对敏感数据进行动态脱敏。
- 审计

  提供性能、数据、行为异常的监控，审计日志远端存储，满足合规性。

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。

须知

- 如果您需要使用数据库防攻击以及敏感数据脱敏功能，请选择数据库安全防护。
- 如果您需要使用数据库审计功能，建议您选择数据库安全审计。

数据库安全防护提供的审计功能和数据库安全审计的功能差异说明如表2-1所示。

表 2-1 数据库安全防护的审计与数据库安全审计的功能差异说明

性能规格/功能特性	数据库安全防护的审计功能	数据库安全审计
部署模式	直路	旁路（业务零干扰）

性能规格/功能特性	数据库安全防护的审计功能	数据库安全审计
支持的数据库类型和版本	● Microsoft SQL Server 2008 - 2014 ● MySQL 5.5 - 5.7 ● PostgreSQL 9.4 - 9.5 ● DWS 1.2.3	● MySQL – 5.0、5.1、5.5、5.6、5.7 – 8.0 ● 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 ● 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
支持的在线日志上限	3000万	3亿~12亿
支持的数据库实例个数	基础版：2个	基础版：3个
	专业版：4个	专业版：6个
	高级版：8个	高级版：30个
价格	请参见**价格详情**。	

3 相关概念

数据库安全服务实例

一个DBSS实例代表了一个独立运行的数据库安全防护服务或数据库安全审计服务，用户可以在数据库安全防护界面购买并管理数据库安全防护实例，也可以在数据库安全审计界面购买并管理数据库安全审计实例。

HexaTier

HexaTier是数据库安全防护的控制台，用户需要登录HexaTier对开启的数据库安全防护实例进行配置，才能实现对数据库的安全防护。

4 数据库安全防护

4.1 功能特性

在购买数据库安全防护后，用户可以登录HexaTier，为华为云上的数据库提供数据库保护和审计功能。

数据库安全

- 数据库防火墙

  HexaTier支持用户自定义配置防火墙策略、自动学习策略及基于异常检测的IDS/IPS策略，当请求到达数据库防火墙且违反策略时，HexaTier会根据用户需求选择实时告警或阻断。HexaTier还可通过机器学习，建立用户访问行为基线，生成查询模式组并可应用至数据库防火墙策略中。

- 权责分离机制

  HexaTier支持细粒度的帐户管理和权限控制，可以按照角色类型、表、视图对象、列等进行权限控制。

- SQL注入检测和防御

  HexaTier内置了SQL注入特性库、基于上下文的学习模型和评分机制，对SQL注入进行综合诊断，并实时阻断，从而确保用户数据库免受SQL注入攻击。

敏感数据发现

- HexaTier内置PCI、HIPAA、SOX、GDPR等合规知识库，用户也可以自定义敏感数据的规则知识库，并通过配置相应敏感数据发现策略来发现数据库中的敏感数据。
- 一旦识别了敏感数据，用户就可以一键自动生成脱敏规则和审计规则。

数据库防拖库

用户可以设置防拖库规则来对未授权用户、IP地址和应用在数据库特定表中的数据操作进行检测，当操作数据量超过规则设定的阈值后，HexaTier将会向管理员发出告警，并将该事件记录至防拖库日志中，协助用户避免数据泄露。

数据库活动监控

- HexaTier提供数据库的库级、表级和列级的视图监控，可独立监控和分析数据库活动，并对未授权的活动进行监控和告警。
- 数据库活动监控也被称为数据库审计。HexaTier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、成功与否、耗时和返回内容等，协助用户溯源到攻击者。审计记录远程保存，满足用户的审计合规要求。

动态数据脱敏

- 用户可以设置脱敏规则来对指定数据库表/列以及来自特定源IP、用户和应用的查询进行脱敏。
- 通过精确的脱敏引擎，对用户的敏感数据实施实时脱敏，不会对应用产生性能损耗，也不会改变数据在数据库中的存储。

4.2 产品优势

数据库安全防护以反向代理的方式部署在应用服务器与数据库之间，为用户提供数据库防火墙、数据库审计、数据动态脱敏等数据库安全防护功能。

- 功能丰富

  提供数据库审计、数据库防火墙、数据泄露保护三大功能，一站式解决数据库审计效果差、安全防御困难、法律合规要求的问题。
- 超低误报

  整合业界通用的SQL注入特征库，叠加机器学习模型+评分机制，误报率远低于平均水平。
- 防护实时

  采用反向代理部署架构，真正做到实时阻断恶意请求。
- 精细控制权限

  弱耦合机制，不修改用户权限的同时，实现细粒度权限控制。
- 高性能动态脱敏

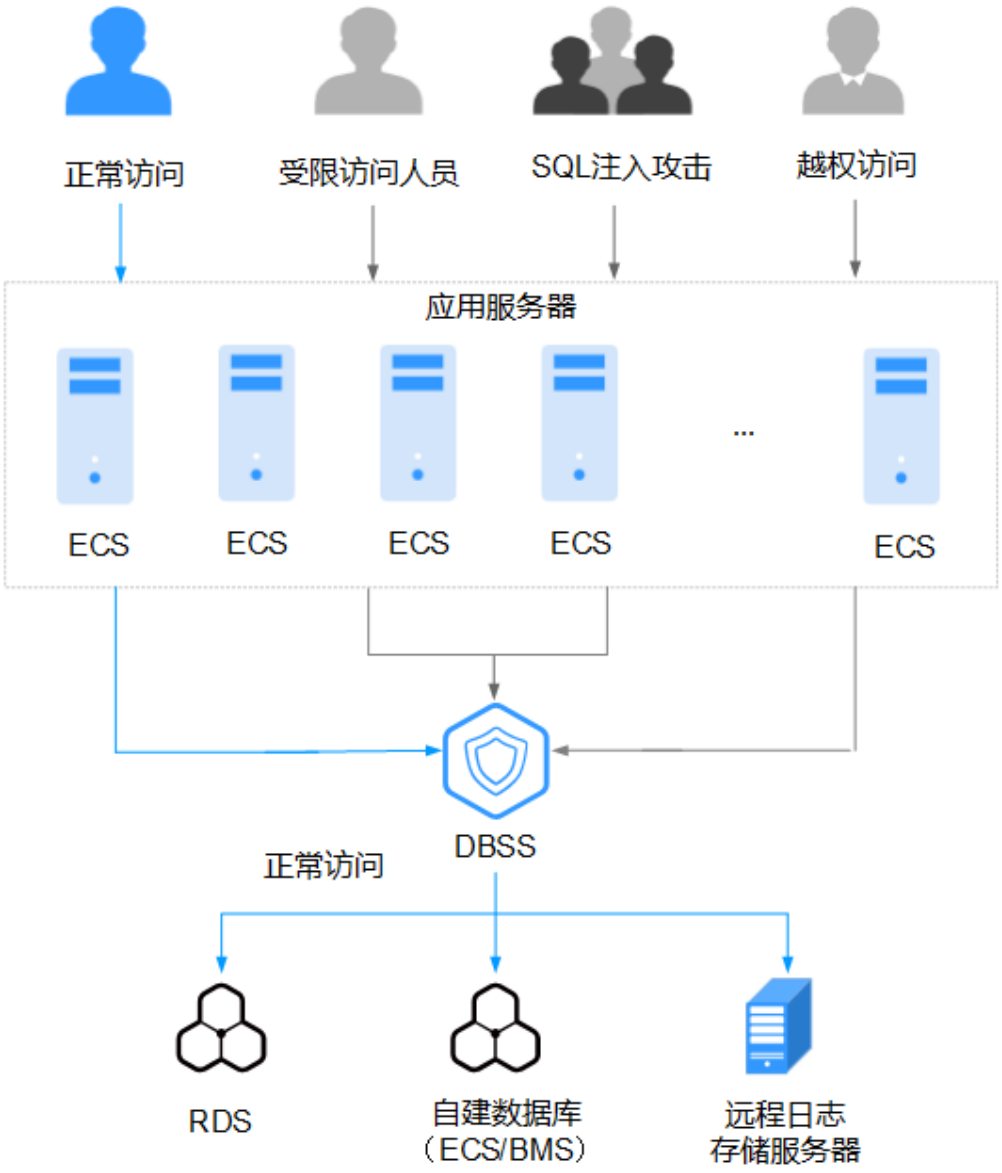
  敏感数据实时保护，不影响数据库和应用。
- 多种合规
  - 整合业界通用的SQL注入特征库，叠加机器学习模型+评分机制，误报率远低于平均水平。
  - 内置合规知识库，满足法律法规遵从。

4.3 部署架构

本章节介绍数据库安全防护的防攻击、数据脱敏和数据库审计的部署架构。

数据库安全防护的部署架构如图4-1所示。

图 4-1 数据库安全防护部署架构

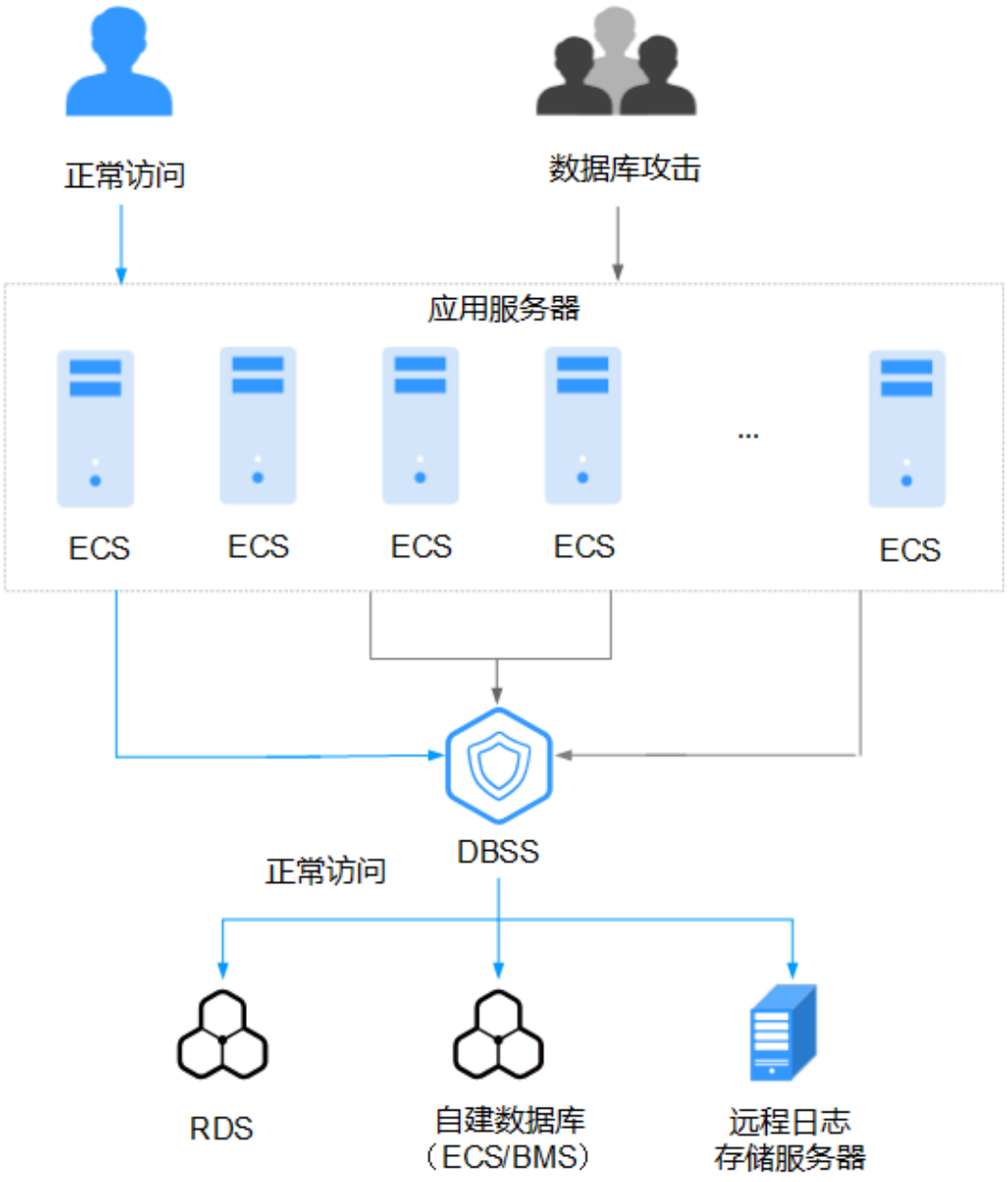


防攻击

数据库安全防护提供多种策略防止数据库被攻击，持续保护云上数据库安全。

防攻击的架构图如图4-2所示。

图 4-2 防攻击架构图

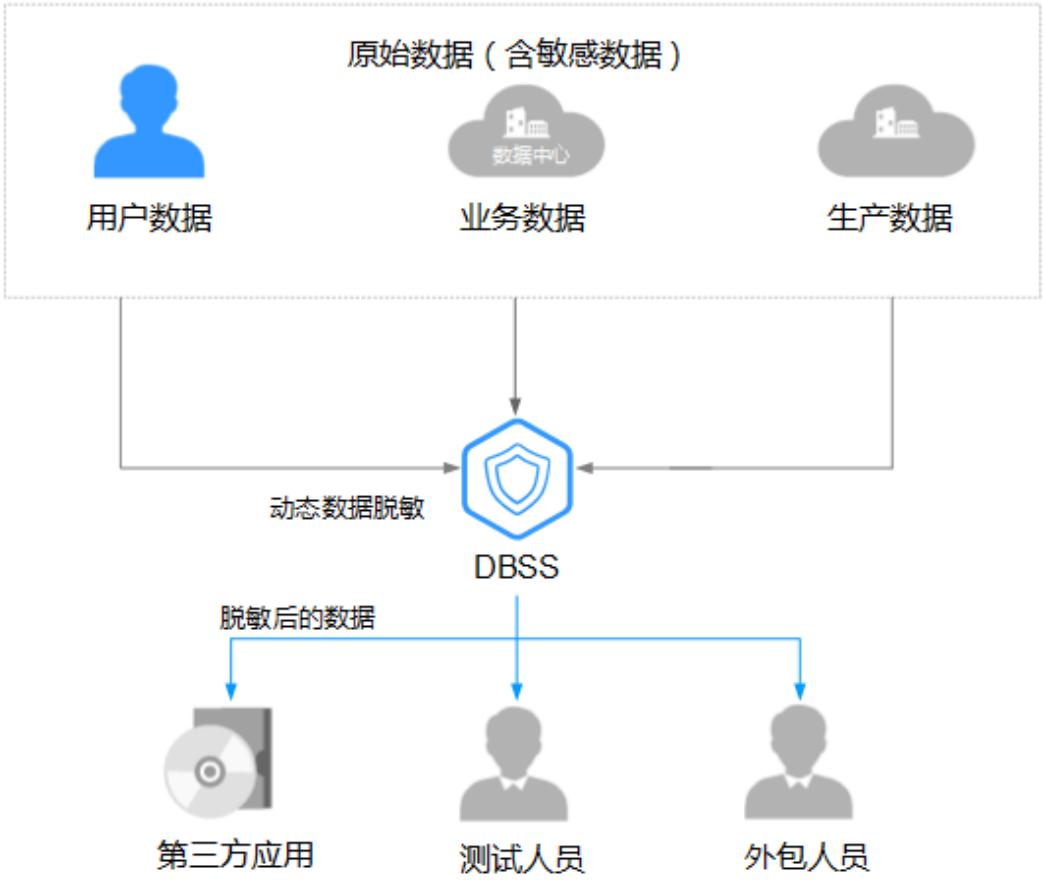


数据脱敏

数据库安全防护可以发现用户数据库中的敏感数据，并对敏感数据进行动态脱敏。

数据脱敏的架构图如图4-3所示。

图 4-3 数据脱敏架构图

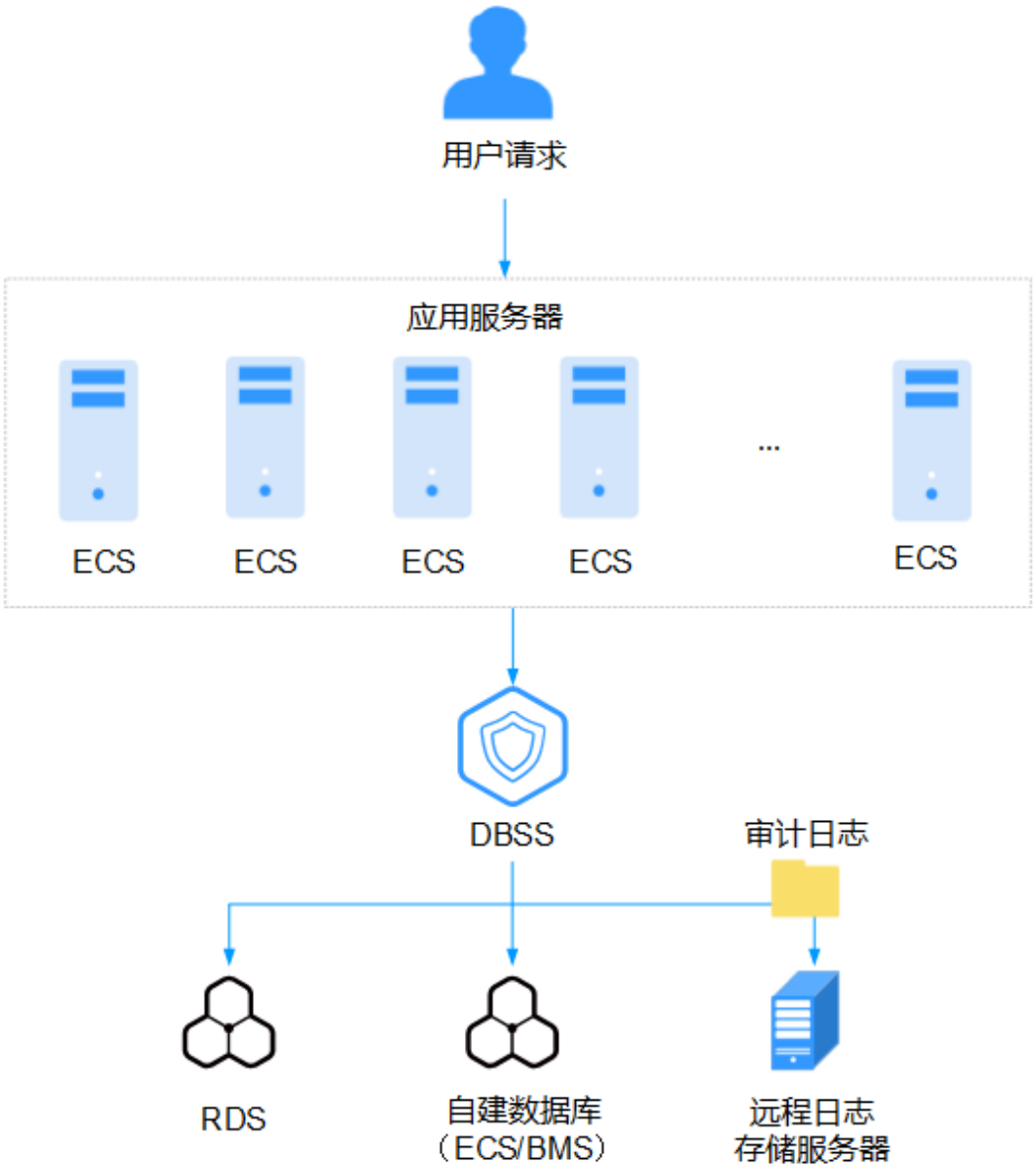


审计

数据库安全防护支持对云上的数据库及自建数据库进行审计，满足数据审计及日志数据留存的要求。

数据库审计架构图如图4-4所示。

图 4-4 数据库审计架构图



5 数据库安全审计

5.1 功能特性

数据库安全审计提供用户行为发现审计、多维度分析、实时告警和报表功能。

用户行为发现审计

- 关联应用层和数据库层的访问操作。
- 实现应用端用户身份行为识别。
- 提供内置或自定义隐私数据保护规则，防止审计日志中的隐私数据（例如，账号密码）在控制台上以明文显示。

多维度线索分析

- 行为线索

  支持审计时长、语句总量、风险总量、风险分布、会话统计、SQL分布等多维度的快速分析。
- 会话线索

  支持根据时间、数据库用户、客户端等多角度进行分析。
- 语句线索

  提供时间、风险等级、数据用户、客户端IP、数据库IP、操作类型、规则等多种语句搜索条件。

风险操作、SQL 注入实时告警

- 风险操作

  支持通过操作类型、操作对象、风险等级等多种元素细粒度定义要求监控的风险操作行为。
- SQL注入

  数据库安全审计提供SQL注入库，可以基于SQL命令特征或风险等级，发现数据库异常行为立即告警。
- 系统资源

  当系统资源（CPU、内存和磁盘）占用率达到设置的告警阈值时立即告警。

针对各种异常行为提供精细化报表

- 会话行为
  提供客户端和数据库用户会话分析报表。
- 风险操作
  提供风险分布情况分析报表。
- 合规报表
  提供满足数据安全标准（例如Sarbanes-Oxley）的合规报告。

5.2 产品优势

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，并对攻击行为进行阻断。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，有效检测并阻断外部入侵，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

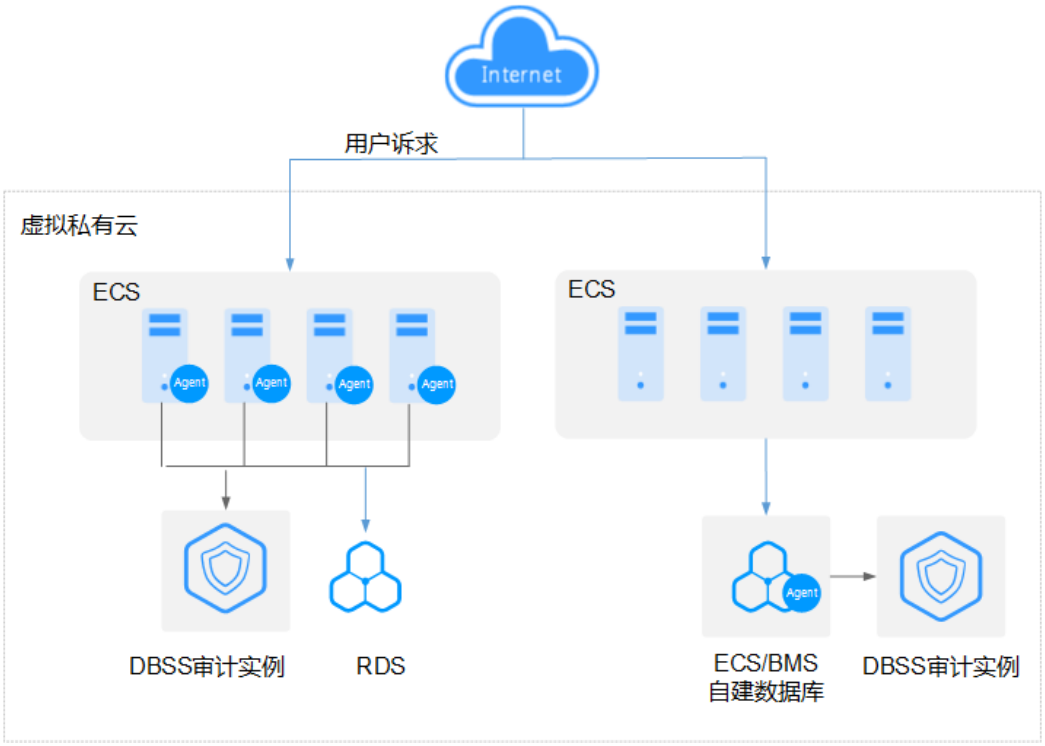
系统管理员，安全管理员，审计管理员权限分离，满足审计安全需求。

5.3 部署架构

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。

数据库安全审计部署架构如图5-1所示。

图 5-1 数据库安全审计部署架构



数据库安全审计的Agent部署说明如下：

- ECS/BMS的自建数据库
  在数据库端、应用端或代理端安装Agent
- RDS关系型数据库
  在应用端或代理端安装Agent

6 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6-1所示。

表 6-1 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：明文存储。

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。

7 权限管理

如果您需要对华为云上购买的DBSS资源，给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。

通过IAM，您可以在华为云账号中给员工创建IAM用户，并使用策略来控制员工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，您希望这些员工拥有DBSS的使用权限，但是不希望其拥有删除ECS等高危操作的权限，那么您可以使用IAM为开发人员创建用户，通过授予仅能使用DBSS，但是不允许删除ECS的权限策略，控制这些员工对华为云资源的使用范围。

如果华为云账号已经能满足您的要求，不需要创建独立的IAM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。关于IAM的详细介绍，请参见**《IAM产品介绍》**。

DBSS 系统策略

策略是以JSON格式描述权限集的语言。默认情况下，新建的IAM用户没有任何权限，您需要将其加入用户组，并给用户组授予策略，才能使得用户组中的用户获得策略定义的权限，这一过程称为授权。授权后，用户就可以基于策略对云服务进行操作。IAM系统预置了各服务的常用权限，例如管理员权限、只读权限，您可以直接使用这些系统策略。

DBSS部署时通过物理区域划分，为项目级服务，需要在各区域（如华北-北京一）对应的项目（cn-north-1）中设置策略，并且该策略仅对此项目生效，如果需要所有区域都生效，则需要在所有项目都设置策略。访问DBSS时，需要先切换至授权区域。

如**表7-1**所示，包括了DBSS的所有系统策略。其中“依赖关系”表示该系统策略对其它策略的依赖。由于华为云各服务之间存在业务交互关系，数据库安全服务的策略依赖其他服务的策略实现功能。因此给用户授予数据库安全服务的权限时，需要同时授予依赖的权限，数据库安全服务的权限才能生效。

表 7-1 DBSS 系统策略

策略名称	描述	依赖关系
DBSS System Administrator	● 数据库安全防护操作权限： – 购买实例。 – 获取实例列表。 – 开启、关闭、重启实例。 – 升级服务实例。 – 绑定、解绑弹性IP。 – 登录数据库安全管理控制台。 ● 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。	购买实例需要同时具有VPC Admin和BSS Administrator策略。 ● VPC Admin：对虚拟私有云的所有执行权限。项目级策略，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。项目级策略，在同项目中勾选。

策略名称	描述	依赖关系
DBSS Audit Administrator	● 数据库安全防护操作权限： – 获取实例列表。 – 登录数据库安全服务管理控制台。 ● 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
DBSS Security Administrator	● 数据库安全防护操作权限： – 获取实例列表。 – 登录数据库安全服务管理控制台。 ● 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7-2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 7-2 常用操作与系统策略的关系

子服务	操作	DBSS System Administrator	DBSS Audit Administrator	DBSS Security Administrator
数据库安全防护	购买实例	√	×	×
	获取实例列表	√	√	√
	开启、关闭、重启实例	√	×	×
	升级服务实例	√	×	×
	绑定、解绑弹性IP	√	×	×
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	√	√	√
	数据库管理	√	×	×
	Agent管理	√	×	×
	邮件设置	√	×	×
	备份与恢复	√	×	×
	获取报表结果	×	√	√

子服务	操作	DBSS System Administrator	DBSS Audit Administrator	DBSS Security Administrator
	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	×	×	√

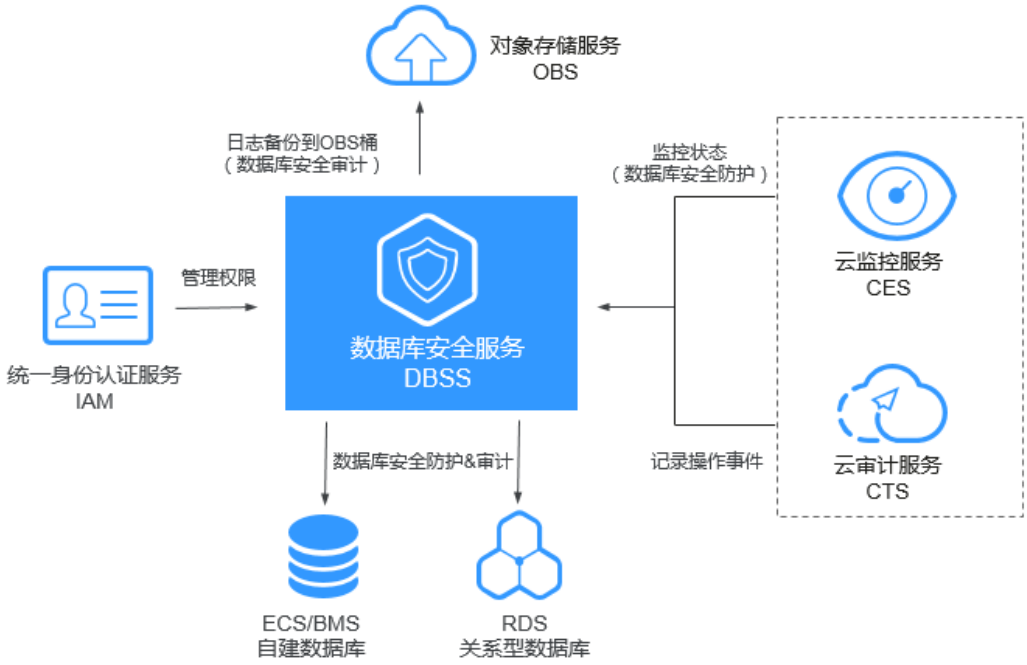
相关链接

- IAM产品介绍
- 创建用户并授权使用DBSS
- 策略语法

8 与其他云服务的关系

数据库安全服务与其他云服务的关系的依赖关系如图8-1所示。

图 8-1 数据库安全服务与其他云服务的关系示意图



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防护和安全审计功能。

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实例提供安全防护和安全审计功能。

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防护和安全审计功能。

与云监控服务的关系

云监控服务可以监控数据库安全防护的相关指标，您可以通过指标及时了解数据库安全防护的防护状况。具体请参见《云监控服务用户指南》。

表 8-1 数据库安全防护的监控指标

指标	指标名称	含义	取值范围	测量对象	监控周期（原始指标）
cpu_util	CPU使用率	该节点的CPU使用率。 单位：百分比	0～100%	server_id	1分钟
mem_util	内存使用率	该节点的内存使用率。 单位：百分比	0～100%	server_id	1分钟
hx_process_status	进程运行状态	该节点的防护进程运行状态，1代表正常，0代表不正常。	0，1	server_id	1分钟
hx_port_status	端口状态	该节点的防护进程使用的端口状态，1代表正常，0代表不正常。	0，1	server_id	1分钟
hx_proxy_num	Proxy数量	该实例配置的Proxy数量，只在主节点显示。	0～8	server_id	1分钟
hx_proxy_status	Proxy状态	该实例配置的Proxy状态，1代表正常，0代表不正常，只在主节点显示。	0，1	server_id	1分钟
hx_qps	QPS	该实例防护的数据库每秒接收的SQL查询语句（含存储过程）请求次数，只在主节点显示。 单位：次数/秒	≥ 0 queries/s	server_id	1分钟
hx_rps	RPS	该实例防护的数据库每秒接收的请求次数，只在主节点显示。 单位：次数/秒	≥ 0 queries/s	server_id	1分钟

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》。

9 数据库安全防护监控指标说明

功能说明

本节定义了数据库安全防护上报云监控服务的监控指标的命名空间，监控指标列表和维度定义，用户可以通过云监控服务提供管理控制台来检索数据库安全防护产生的监控指标。

监控指标

表 9-1 数据库安全防护的监控指标

指标	指标名称	含义	取值范围	测量对象	监控周期（原始指标）
cpu_util	CPU使用率	该节点的CPU使用率。 单位：百分比	0～100%	server_id	1分钟
mem_util	内存使用率	该节点的内存使用率。 单位：百分比	0～100%	server_id	1分钟
hx_process_status	进程运行状态	该节点的防护进程运行状态，1代表正常，0代表不正常。	0，1	server_id	1分钟
hx_port_status	端口状态	该节点的防护进程使用的端口状态，1代表正常，0代表不正常。	0，1	server_id	1分钟
hx_proxy_num	Proxy数量	该实例配置的Proxy数量，只在主节点显示。	0～8	server_id	1分钟

指标	指标名称	含义	取值范围	测量对象	监控周期（原始指标）
hx_proxy_status	Proxy状态	该实例配置的Proxy状态，1代表正常，0代表不正常，只在主节点显示。	0，1	server_id	1分钟
hx_qps	QPS	该实例防护的数据库每秒接收的SQL查询语句（含存储过程）请求次数，只在主节点显示。 单位：次数/秒	≥ 0 queries/s	server_id	1分钟
hx_rps	RPS	该实例防护的数据库每秒接收的请求次数，只在主节点显示。 单位：次数/秒	≥ 0 queries/s	server_id	1分钟