数据库安全服务

产品介绍

文档版本 01

发布日期 2024-10-14

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、数据库运维服务功能，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。数据库运维安全管理通过统一登录、权限管控、多因素认证、操作审批等技术，可实现对于运维人员的最小化权限控制、危险操作阻断以及行为审计。

支持的数据库

数据库安全审计仅支持对华为云上的以下数据库提供旁路模式的数据库审计功能：

- 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

部分数据库类型及版本支持免安装Agent方式，如表1-1所示。

表 1-1 支持免 Agent 安装的关系型数据库

数据库类型	支持的版本
GaussDB for MySQL	默认都支持
RDS for SQLServer （华为云审计实例：23.02.27.182148 及其之后的版本支持）	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 （华为云审计实例：23.04.17.123301 及其之后的版本支持） **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

数据库安全审计支持数据库类型及版本如表1-2所示。

表 1-2 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 • 8.0.35 • 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

数据库类型	版本
SQL Server	• 2008 • 2012 • 2014 • 2016 • 2017
GaussDB(for MySQL)	MySQL 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 （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

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 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。
  - 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。

- 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

- 数据库运维

  数据库运维安全管理系统具有支持丰富的数据库类型、细粒度的运维权限管控、丰富的内置威胁特征库、支持集群化等优势。

3 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。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。
- 细粒度和运维权限管控
  数据库运维安全管理系统访问控制基于主体、客体和行为三元组进行设置，每个类别之下再细分多种维度。策略组合种类多达数百种，能够精准实现各种数据级的访问控制。
  - 主体颗粒度可细化至用户、IP、主机、程序、时间、频次等。
  - 客体颗粒度可达针对表、列、行数等。
  - 行为颗粒度可达操作、特权操作、SQL语句、异常、存储过程等。
- 强大的内置威胁特征库
  数据库运维安全管理系统内置丰富的数据库漏洞信息、SQL注入攻击、以及其它高危风险操作特征模板（其中数据库漏洞数超过600个，高危操作、SQL注入攻击特征超过200个，数据库风险配置策略超过200个），能够精准检测数据库风险操作，并定位至具体用户、实时阻断，保障客户数据资产安全。
- 灵活的保护对象及策略
  数据库运维安全管理系统支持针对数据资产进行分级管控。通过策略配置，使得用户可以灵活定义被保护的对象，包括库、表、字段、记录、关键字、条件等。

可以针对上述被保护的对象设置严格管控策略，非经审批不可改、不可删甚至不可见。

4 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。

图 4-1 数据库安全审计部署架构

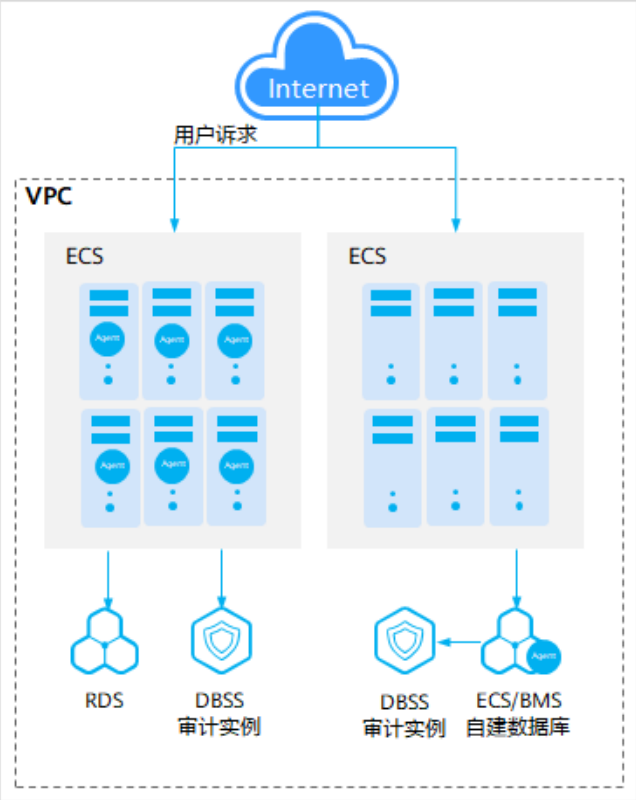


图 4-2 组网方式

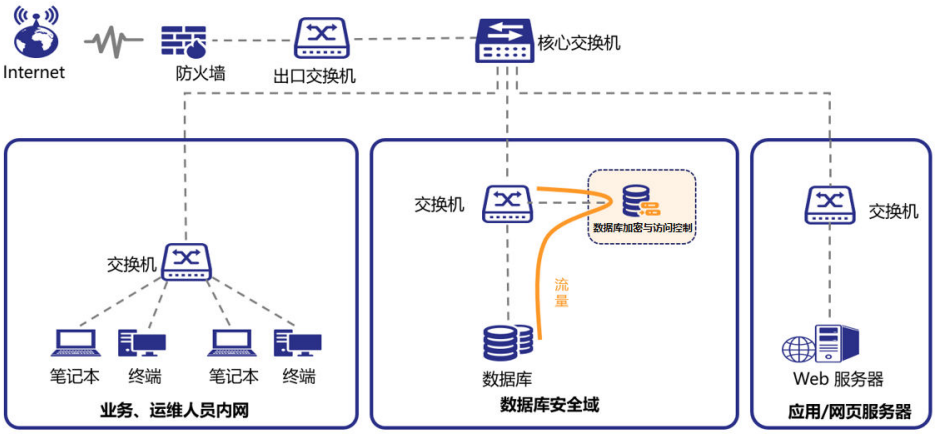
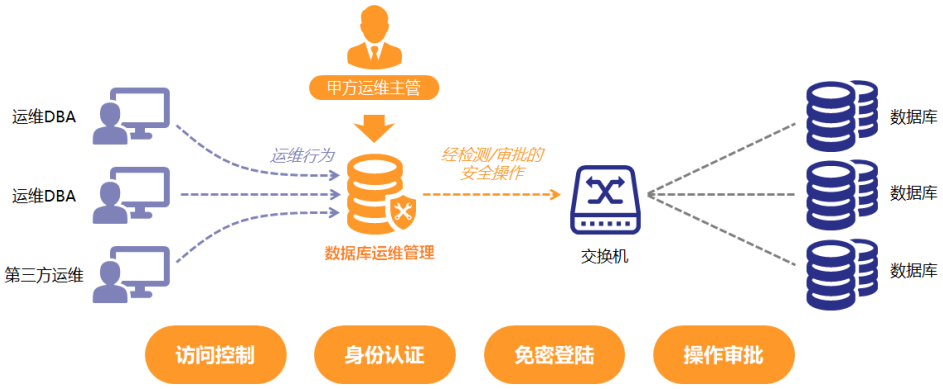


图 4-3 实现流程



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

5 服务版本规格

数据库安全审计提供了入门版、基础版、专业版和高级版三种服务版本。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5-1所示。

表 5-1 数据库安全审计版本性能规格说明

版本	支持的数据库实例	性能参数
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 • 1亿条在线SQL语句存储
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 • 4亿条在线SQL语句存储
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 • 6亿条在线SQL语句存储
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 • 15亿条在线SQL语句存储

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。
- 云原生版仅支持在RDS控制台购买。
- 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。

6 使用约束

在使用数据库安全审计前，您需要了解数据库安全审计的使用限制。

支持的数据库类别

数据库安全审计支持对华为云上的以下数据库提供旁路模式的审计功能：

- 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6-1所示。

表 6-1 支持免 Agent 安装的关系型数据库

数据库类型	支持的版本
MySQL	默认都支持
PostgreSQL （华为云审计实例：23.04.17.123301 及其之后的版本支持） **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。	默认都支持
SQLServer	• 2008 • 2012 • 2014 • 2016 • 2017
GaussDB(for MySQL)	Mysql8.0
DWS	• 8.2.0.100及以上版本

数据库类型	支持的版本
MariaDB	10.2

支持安装 Agent 数据库类型及版本

支持的数据库类型及版本如表6-2所示。

表 6-2 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 • 8.0.35 • 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
SQL Server	• 2008 • 2012 • 2014 • 2016 • 2017
GaussDB(for MySQL)	MySQL 8.0
DWS	• 1.5 • 8.1

数据库类型	版本
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 （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

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6-3所示。

表 6-3 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)
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)（华为云审计实例：23.02.27.182148 及其之后的版本支持）

系统名称	系统版本
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）

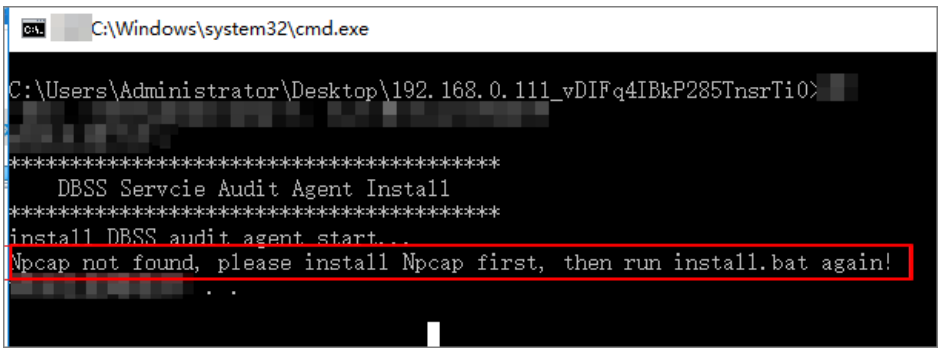
- 数据库安全审计的Agent支持的Windows系统版本如下所示：
  - Windows Server 2008 R2(64bit)
  - Windows Server 2012 R2(64bit)
  - Windows Server 2016(64bit)
  - Windows Server 2019(64bit)
  - Windows 7(64bit)
  - Windows 10(64bit)

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。

Npcap下载链接：**https://npcap.com/#download**

图 6-1 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。
- 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SQLserver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。

7 安全

7.1 责任共担

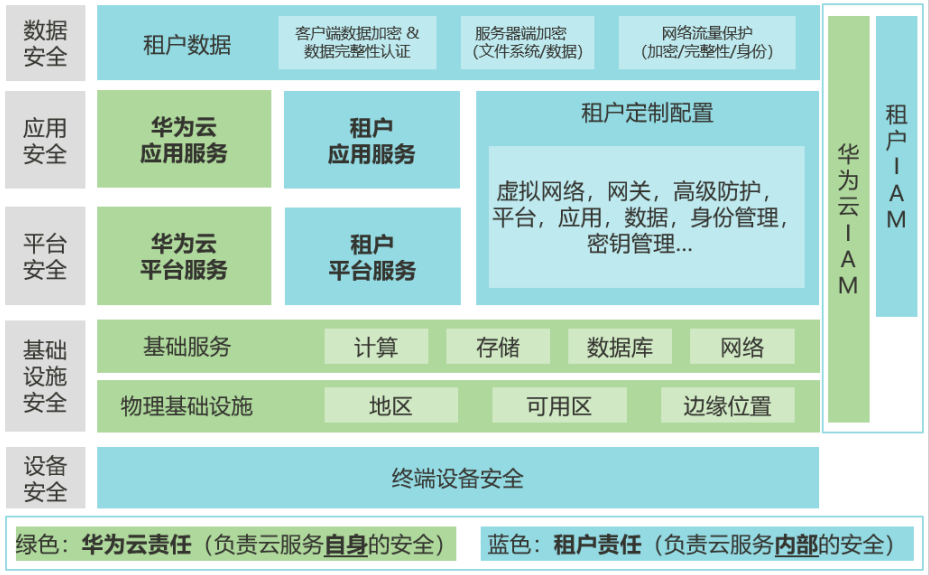
华为云秉承“将公司对网络和业务安全性保障的责任置于公司的商业利益之上”。针对层出不穷的云安全挑战和无孔不入的云安全威胁与攻击，华为云在遵从法律法规业界标准的基础上，以安全生态圈为护城河，依托华为独有的软硬件优势，构建面向不同区域和行业的完善云服务安全保障体系。

安全性是华为云与您的共同责任，如图7-1所示。

- **华为云**：负责云服务**自身**的安全，提供安全的云。华为云的安全责任在于保障其所提供的IaaS、PaaS和SaaS类云服务自身的安全，涵盖华为云数据中心的物理环境设施和运行其上的基础服务、平台服务、应用服务等。这不仅包括华为云基础设施和各项云服务技术的安全功能和性能本身，也包括运维运营安全，以及更广义的安全合规遵从。
- **租户**：负责云服务**内部**的安全，安全地使用云。华为云租户的安全责任在于对使用的IaaS、PaaS和SaaS类云服务内部的安全以及对租户定制配置进行安全有效的管理，包括但不限于虚拟网络、虚拟主机和访客虚拟机的操作系统，虚拟防火墙、API网关和高级安全服务，各项云服务，租户数据，以及身份账号和密钥管理等方面的安全配置。

《华为云安全白皮书》详细介绍华为云安全性的构建思路与措施，包括云安全战略、责任共担模型、合规与隐私、安全组织与人员、基础设施安全、租户服务与租户安全、工程安全、运维运营安全、生态安全。

图 7-1 华为云安全责任共担模型



7.2 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。

7.3 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。

    关于认证鉴权的详细介绍及获取方式，请参见**认证鉴权**。

- 访问控制

  DBSS支持通过权限控制（IAM权限）进行访问控制。

表 7-1 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）

7.4 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 7-2 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。	-

7.5 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 7-3 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”和“数据库慢SQL检测”两条检测规则，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**。

7.6 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 7-4 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

可信架构分类	可信架构能力项	目标	分类
	监控	针对微服务的异常日志出对应的告警	系统
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

7.7 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。

7.8 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 7-2 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 7-3 资源中心

销售许可证&软件著作权证书

另外，华为云还提供了以下销售许可证及软件著作权证书，供用户下载和参考。具体请查看**合规资质证书**。

图 7-4 销售许可证&软件著作权证书

8 计费说明

本章节主要介绍数据库安全服务的计费说明，包括计费项、计费模式和续费等。

计费项

数据库安全服务根据您选择的性能规格和购买时长计费，用户选择实例规格与购买时长后，会自动获取费用值。

表 8-1 计费项说明

计费项	计费说明
性能规格	根据您选择的性能规格（基础版、专业版、高级版）计费。
购买时长	提供包年和包月的购买模式。

计费模式

数据库安全服务提供包年/包月的计费模式，暂不支持按需计费。详细的服务资费和费率标准，请参见**产品价格详情**。

变更配置

- 如果您需要变更DBSS实例规格，可以先退订当前DBSS实例后，再重新购买DBSS。
- 退订：购买数据库安全服务后，如需停止使用，请到费用中心执行**退订**操作。

续费

包年/包月方式购买的DBSS实例到期后，如果没有按时续费，公有云平台会提供一定的保留期。

保留期的时长由客户等级而定，具体请参见**保留期**。

当您购买的DBSS实例到期后，DBSS将停止服务。为了防止造成不必要的损失，请您及时续费。如果未续费，您将不能使用DBSS，不影响您的业务。

如需续费，请在管理控制台**续费管理**页面进行续费操作。详细操作请参考**续费管理**。

到期与欠费

- **服务到期**

  若您购买的实例到期后，如果没有按时续费，公有云平台会提供一定的保留期，请参考**保留期**。

- **欠费**

  若您购买的实例已欠费，可以查看欠费详情。为了数据库安全和资产安全，建议您及时进行充值，详细操作请参考**欠费还款**。

FAQ

更多计费相关FAQ，请参见**DBSS常见问题**。

9 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9-1所示。

表 9-1 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。

10 DBSS 权限管理

如果您需要对华为云上购买的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。

通过IAM，您可以在账号中给员工创建IAM用户，并授权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，您希望员工拥有DBSS的使用权限，但是不希望员工拥有删除DBSS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DBSS的权限，控制员工对DBSS资源的使用范围。

如果华为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是华为云云服务平台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 权限

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（如华北-北京1）对应的项目（cn-north-1）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。

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。基于策略的授权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），DBSS支持的API授权项请参见策略支持的授权项。

如表10-1所示，包括了DBSS的所有系统角色。

表 10-1 DBSS 系统角色

角色名称	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

角色名称	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10-2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 10-2 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	×	×	√

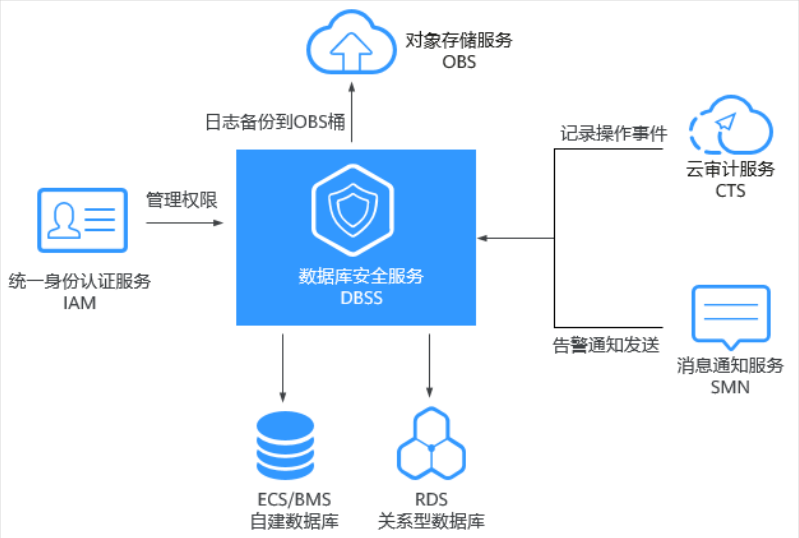
相关链接

- IAM产品介绍
- 创建用户组、用户并授予DBSS权限

11 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11-1所示。

图 11-1 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 11-1 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
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 11-2 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	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	弹性云服务器	4分钟
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	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	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	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	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	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》。