数据安全中心

产品介绍

文档版本 24

发布日期 2025-10-29

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 什么是数据安全中心

数据安全中心服务（Data Security Center，DSC）是新一代的云原生数据安全管理平台，提供数据分级分类、数据脱敏、数据水印等基础数据安全能力，通过资产地图整体呈现云上数据安全态势，并实现一站式数据安全运营能力。

介绍视频

为什么选择数据安全中心

- 一站式数据安全中心

  一款产品提供传输加密、个人数据保护、隐私数据保护、数据备份、数据销毁、数据脱敏和数据水印7种数据安全保护能力，企业无需重复安装。
- 云上场景全覆盖
  - 全数据服务资产：涵盖云上所有数据资产，包含OBS/RDS/CSS/Hive/Hbase等。
  - 数据风险：数据关联分级分类结果，一览展示各个数据风险级别。
- 无缝对接的云原生能力
  - 基于AI的敏感数据识别，识别准确率>95%。
  - 无缝对接云原生数据环境，提供数据安全地图，数据、出口、风险全可视。
  - 从底层提供数据加密、分级分类、脱敏水印等能力。
- 一体化防护
  - 防护能力一体化：数据安全中心统一集成数据安全能力。
  - 安全策略一体化：一条策略可编排不同安全原子服务。

更多数据安全中心产品优势请参见**产品优势**。

2 规格版本差异

本章节介绍数据安全中心服务的版本规格差异。

数据安全中心服务提供了“标准版”和“专业版”两个服务版本供您选择，其差异如**表2-1**所示。

说明

- 当前版本的数据库数量和OBS体量不能满足业务需求时，可以通过**升级版本和规格**增加数据库扩展包和OBS扩展包的数量。
- OBS体量即OBS桶的“存储用量”，进入OBS服务控制台，左侧菜单选择“桶列表”查看桶“存储用量”，请根据OBS桶的“存储用量”选择大于或者相等的OBS体量。

表 2-1 服务版本差异

规格版本	支持添加的数据库数量	支持添加的OBS体量	API调用额度	支持的功能
标准版	2个	100GB	不支持	• 资产地图 • 资产管理 • 敏感数据识别 • 数据安全运营
专业版	2个	100GB	100W次	• 资产地图 • 资产管理 • 敏感数据识别 • 数据脱敏 • 文档/图片/数据库水印 • 数据安全运营 • 动脱/水印API调用

3 功能特性

数据安全中心提供数据分级分类、数据脱敏、数据水印等基础数据安全能力，通过资产地图整体呈现云上数据安全态势，并实现一站式数据安全运营能力。

同时，为满足不同用户需求，数据安全中心在通用数据安全防护场景下提供“标准版”和“专业版”两个版本供您选择。

- “标准版”：支持在资产中心添加数据资产并查看资产地图、态势大屏等，同时支持使用敏感数据识别功能进行数据资产分类分级。
- “专业版”：支持对分类分级后的数据资产进行静态脱敏（控制台）和调用API接口进行脱敏以及添加和提取数据水印。

资产地图

数据资产地图可以通过可视化的手段，从资产概况、分类分级、权限配置、数据存储、敏感数据等多种维度查看资产的安全状况。可协助您快速发现风险资产并快速进行风险处理操作。有关更多信息详情请参见**资产地图**。

- 资产可视化
  - 数据服务资产：涵盖了云上和云下所有数据资产，包含OBS、RDS、CSS、Hive以及Hbase等。
  - 数据风险：数据关联分级分类结果，一览展示各个数据风险级别。
  - 分区展示：根据云上和云下资源VPC展示各个资产所在区域，和业务区域关联。
- 出口可视
  - 数据出口：识别云上和云下关键数据出口，包含EIP/NAT/APIGateway/Roma等。
  - 出口关联资产：云上和云下出口和数据关联，结合分级分类结果，一览数据出口风险。
  - 级联关联：数据出口包含直接出口和级联间接出口，不同展示方式。
- 策略可视
  - 数据安全策略：云原生能力检测数据资产的安全策略，一览策略风险。
  - 策略推荐：根据数据资产等级推荐不同的安全策略配置。

资产管理

- **资产中心：**DSC支持管理OBS、数据库、大数据、MRS数据资产以及云日志类型资产。有关更多信息请参阅**资产中心**。
- **资产目录：**查看不同业务域或不同数据类型（结构化和非结构化数据）的统计信息。有关更多信息请参阅**管理资产目录**
- **数据探索：**查看当前已添加的所有数据资产详细信息，并对数据库、数据表以及数据视图等添加描述、标签、密级和分类操作，从而实现数据资产分级分类管理。有关更多信息请参阅**通过数据探索实现资产分级分类**。
- **元数据任务**：用户可以创建元数据任务扫描数据资产，数据资产信息会以元数据的形式被采集、收纳到DSC中，后续用户可以对数据资产进行分级分类管理。有关更多信息请参阅**通过数据探索实现资产分级分类**。
- **资产分组管理：**对现有数据进行分组管理。有关更多信息请参阅**管理资产分组**。

敏感数据识别

- 敏感数据识别基于数据识别引擎，对其储存结构化数据（RDS、DWS等）和非结构化数据（OBS）进行扫描、分类、分级。
- 文件类型：支持近200种非结构化文件，详情请参见**DSC支持识别的非结构化文件类型**。
- 数据类型：支持数十种个人隐私数据类型，包含中英文，支持的个人隐私数据类型详情请参见**查看内置规则**。
- 图片类型：支持识别（png、jpeg、x-portable-pixmap、tiff、bmp、gif、jpx、jp2总共8种类型）图片中的敏感文字，包含中英文。
- **自动识别敏感数据**
  - 自动识别敏感数据及个人隐私数据。
  - 提供可视化识别结果，同时，可供用户下载到本地查看。有关更多信息请参阅**新建敏感数据识别任务**

DSC服务敏感数据的识别时长将由您所扫描数据源的数据量、扫描规则数、扫描模式决定，具体请参见**DSC扫描时长**。

数据脱敏

DSC的数据脱敏支持静态脱敏和调用API接口进行脱敏。有关更多信息请参阅**创建数据静态脱敏任务**。

DSC的数据脱敏特点：

- **不影响用户数据**：从原始数据库读取数据，通过精确的脱敏引擎，对用户的敏感数据实施静态脱敏，脱敏结果另行存放，不会影响原始的用户数据。
- **支持云上各类场景**：支持RDS，ECS自建数据库，大数据合规。
- **满足多种脱敏需求**：用户可以通过20+种预置脱敏规则，或自定义脱敏规则来对指定数据库表进行脱敏，DSC支持的脱敏算法详见**配置脱敏规则**。
- **实现一键合规**：基于扫描结果自动提供脱敏合规建议，一键配置脱敏规则。

同时，DSC提供API接口供您使用，具体请参考**数据动态脱敏**。

DSC通过内置和自定义脱敏算法，实现对RDS、Elasticsearch、MRS、Hive、HBase、DLI以及OBS数据进行脱敏，具体的脱敏时长请参见**DSC脱敏时长**。

数据水印

针对数据库、文档以及图片提供了注入和提取水印的功能。有关更多信息请参阅**数据水印**。

- **版权证明：**嵌入数据拥有者的信息，保证资产唯一归属，实现版权保护。
- **追踪溯源：**嵌入数据使用者的信息，在发生数据泄露事件时，追踪其泄露源头。

同时，DSC提供了数据动态添加水印和提取数据水印的API接口供您使用，具体请参考**Api接口参考**。

策略中心

- **策略基线**：策略基线是数据安全管理规定、数据分类分级要求、数据出境管理规定、重要数据和核心数据要求等数据安全策略结构化，DSC依据华为云数据安全治理经验预置策略模板，支持策略的增删改查、策略的结构化展示和过滤查询等。有关更多信息请参阅**策略基线**。
- **流转日志采集**：DSC对各个应用中的日志数据进行采集，如DBSS服务和API数据安全防护，可动态地采集用户访问行为的路径，可以快速全面支撑溯源或定位，直观了解数据的流转情况，及时发现异常和风险。有关更多信息请参阅**流转日志采集**。
- **策略管理**：管理员在策略中心的策略管理页面制定数据库审计、数据库水印、数据库静态脱敏，下发给相应的服务或者实例。有关更多信息请参阅**策略管理**。

API 数据安全防护

API数据安全防护是一款为企业提供综合的API安全防护系统。

对应用API接口进行自动梳理，实现应用接口细粒度访问控制、API异常风险发现、API敏感数据检测、脱敏和水印等能力。API数据安全防护实例需要单独购买才能使用，有关更多信息请参阅**API数据安全防护**。

态势大屏

数据安全中心默认提供一个综合态势感知大屏，对云上风险资产、识别任务、脱敏任务、水印任务、事件、告警等信息进行综合展示和分析，实现一屏全面感知，帮助用户快速识别资产综合态势，对风险资产和紧急告警快速做出响应。有关更多信息请参阅**查看态势大屏**。

告警管理

当DBSS有系统或者业务方面的风险告警事件时，会将告警事件推送到DSC，用户可以在DSC控制台确认相关的告警事件。有关更多信息请参阅**告警管理**。

事件管理

数据安全中心对接数据库审计、云堡垒机等安全组件，对各组件事件进行统一管理，会将事件实时推送到DSC，用户可以对事件进行确认和处理。也可以将告警页面的告警转事件。有关更多信息请参阅**事件管理**。

OBS 使用审计

数据安全中心服务根据敏感数据规则对OBS桶进行识别，根据识别的敏感数据进行监控，监控到敏感数据的异常事件相关操作后，会将监控结果展示在异常事件处理页面中，用户可根据需要对异常事件进行处理。有关更多信息请查阅**OBS使用审计**。

查看数据流转详情

- **调用链数据采集**，对各个应用中的日志数据进行采集。
- **调用链数据存储及查询**，对采集到的数据进行存储，由于日志数据量一般都很大，不仅要能对其存储，还需要能提供快速查询。
- **调用链数据生成**，DSC负责对采集上报的日志进行数据链路流转分析，并绘制流转图
- **指标运算、存储及查询**，对采集到的日志数据进行各种指标运算，将运算结果保存起来。更多相关信息请查阅**查看数据流转详情**

多账号管理

开启多账号管理功能后，安全管理员在安全运营账号中对所有成员账号进行统一的数据安全防护，而无需逐个登录到成员账号。更多相关信息请查阅**多账号管理**。

告警通知

通过设置告警通知，当敏感数据检测完成后或异常事件处理监测到异常事件时，DSC会将其检测结果通过用户设置的接收通知方式发送给用户。更多相关信息请查阅**告警通知**。

4 产品优势

数据安全态势可视

通过资产地图可视化的手段，从资产分布概况、分类分级结果、权限配置风险、数据出口风险等多种维度查看资产的安全状况，整体呈现您的数据安全态势。

云上全场景覆盖

整合云上各类数据源，包括大数据、数据库、对象存储、日志等，并提供一站式数据保护和防御机制。

准确识别

在正则引擎和机器学习模型的双重加权下，识别能力更强，高效锁定敏感数据源。

5 计费说明

数据安全中心服务版本支持包年/包月（预付费）的计费方式，API接口（数据脱敏和水印API调用）支持按需计费（后付费）的计费方式。

计费项

表 5-1 计费项信息

计费模式	计费项目	计费说明
包周期（包年/包月）	服务版本（必须）	按购买的版本规格（标准版、专业版）计费。 各服务版本支持的业务规格和功能，请参见**规格版本差异**。
	数据库扩展包（可选）	按购买个数计费。
	OBS扩展包（可选）	按购买个数计费。
	购买时长	提供包月和包年的购买模式。
按需计费	API接口（数据脱敏和水印API调用）	仅专业版支持，且默认支持每月100W次的调用额度，不累计，月末清零。超出部分按照调用次数收费，详情请参见**产品价格详情**。

计费模式

- 包周期（包年/包月）：服务版本计费模式，使用越久越便宜。包周期计费按照订单的购买周期来进行结算。
- 按需计费：API接口计费模式，这种购买方式比较灵活，可以即开即停。

详细的服务资费费率标准请参见**产品价格详情**。

变更配置

- 购买数据安全中心服务后，您可以通过升级规格操作，将DSC从较低版本升级到更高版本，也可以根据业务需求增加数据库扩展包和OBS扩展包的数量。

- 退订：以包年/包月方式购买DSC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DSC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。

保留期的时长请参见“**保留期**”。

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DSC服务。

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

  如果购买的服务版本到期后，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

  如果购买的服务版本已欠费，可以查看欠费详情。为了更好的使用服务，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**DSC常见问题**。

6 应用场景

数据资产盘点

无缝对接云原生数据环境，自动发现云上数据资产，从资产概况、分类分级、权限配置以及数据出口分析等多种维度查看资产的安全状况。

数据分级分类

从海量数据中自动发现并分析敏感数据使用情况，基于数据识别引擎，对其储存结构化数据（数据库、大数据）和非结构化数据（OBS、日志）进行扫描、分类、分级，解决数据“盲点”，以此做进一步安全防护。

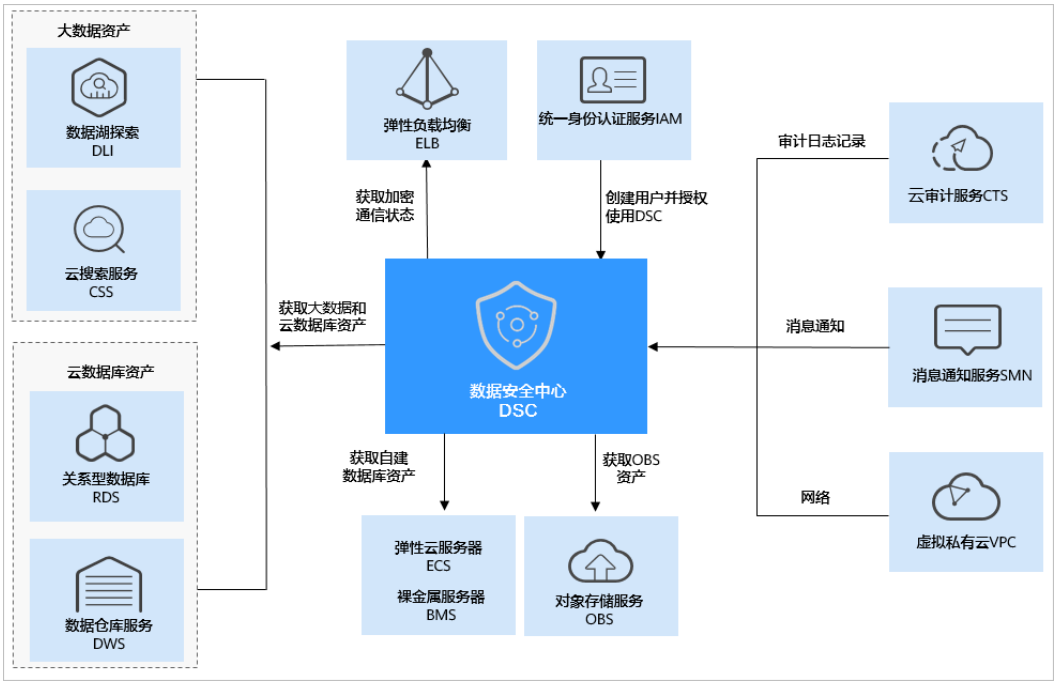
数据脱敏保护

通过多种预置脱敏算法+用户自定义脱敏算法，搭建数据保护引擎，实现大批量数据静态脱敏存储和API数据实时脱敏返回，防止敏感数据泄露。

7 与其他云服务的关系

数据安全中心与周边服务的依赖关系如图7-1所示。

图 7-1 与其他云服务的关系



与对象存储服务的关系

对象存储服务（Object Storage Service，简称OBS）是一款稳定、安全、高效、易用的云存储服务，具备标准Restful API接口，可存储任意数量和形式的非结构化数据。经用户授权后，数据安全中心可以为OBS提供敏感数据自动识别分类、用户异常行为分析、数据保护三大服务。

与关系型数据库的关系

关系型数据库（Relational Database Service，简称RDS）是一种基于云计算平台的即开即用、稳定可靠、弹性伸缩、便捷管理的在线关系型数据库服务。经用户授权后，数据安全中心可以为关系型数据库服务中的RDS实例提供敏感数据自动识别分类和数据保护服务。

与数据仓库服务的关系

数据仓库服务（Data Warehouse Service，简称DWS）是一种基于公有云基础架构和平台的在线数据处理数据库，提供即开即用、可扩展且完全托管的分析型数据库服务。经用户授权后，数据安全中心可以为数据仓库服务提供敏感数据自动识别分类和数据保护服务。

与弹性云服务器的关系

弹性云服务器（Elastic Cloud Server，简称ECS）是一种可随时自助获取、可弹性伸缩的云服务器。经用户授权后，数据安全中心可以为弹性云服务器上的自建数据库提供敏感数据自动识别分类和数据保护服务。

与裸金属服务器的关系

裸金属服务器（Bare Metal Server，简称BMS）是一款兼具虚拟机弹性和物理机性能的计算类服务。经用户授权后，数据安全中心可以为裸金属服务器上的自建数据库提供敏感数据自动识别分类和数据保护服务。

与云搜索服务的关系

云搜索服务（Cloud Search Service，简称CSS），为您提供托管的分布式搜索引擎服务，完全兼容开源Elasticsearch搜索引擎，支持结构化、非结构化文本的多条件检索、统计、报表。云搜索服务的使用流程和数据库类似。经用户授权后，数据安全中心可以为云搜索服务上的大数据资产提供敏感数据自动识别分类和数据保护服务。

与数据湖探索服务的关系

数据湖探索（Data Lake Insight，简称DLI），是完全兼容Apache Spark、Apache Flink、openLooKeng（基于Apache Presto）生态，提供一站式的流处理、批处理、交互式分析的Serverless融合处理分析服务。经用户授权后，数据安全中心可以为数据湖探索服务上的大数据资产提供敏感数据自动识别分类和数据保护服务。

与 MapReduce 服务的关系

MapReduce服务（MapReduce Service，简称MRS），提供租户完全可控的企业级大数据集群云服务，轻松运行Hadoop、Spark、HBase、Kafka、Storm等大数据组件。经用户授权后，数据安全中心可以为MapReduce服务上的Hive资产提供敏感数据自动识别分类和数据保护服务。

与弹性负载均衡的关系

数据安全中心与**弹性负载均衡**（Elastic Load Balance，以下简称ELB）绑定，DSC通过ELB获取加密通信状态。

与消息通知服务的关系

消息通知服务（Simple Message Notification，简称SMN）提供消息通知功能。DSC开启通知设置后，当敏感数据检测完成后或异常事件处理监测到异常事件时，告警信息会通过用户设置的邮箱发送给用户。

与云审计服务的关系

云审计服务（Cloud Trace Service，CTS）记录了数据安全中心相关的操作事件，方便用户日后的查询、审计和回溯。

表 7-1 云审计服务支持的 DSC 操作列表

操作名称	资源类型	事件名称
授权或者取消对DSC的授权	dscGrant	grantOrRevokeTodsc
添加OBS桶资产	dscObsAsset	addBuckets
删除OBS桶资产	dscObsAsset	deleteBucket
添加数据库资产	dscDatabaseAsset	addDatabase
修改数据库资产	dscDatabaseAsset	updateDatabase
删除数据库资产	dscDatabaseAsset	deleteDatabase
添加大数据资产	dscBigdataAsset	addBigdata
修改大数据资产	dscBigdataAsset	updateBigdata
删除大数据资产	dscBigdataAsset	deleteBigdata
更新对象名称	dscAsset	updateAssetName
下载批量添加模板	dscBatchImportTemplate	downloadBatchImportTemplate
批量添加数据库	dscAsset	batchAddDatabase
批量添加资产	dscAsset	batchAddAssets
展示异常事件	dscExceptionEvent	listExceptionEventInfo
获取异常事件详细信息	dscExceptionEvent	getExceptionEventDetail
添加告警配置	dscAlarmConfig	addAlarmConfig
修改告警配置	dscAlarmConfig	updateAlarmConfig
下载报表	dscReport	downloadReport
删除报表	dscReport	deleteReport
添加扫描规则	dscRule	addRule
修改扫描规则	dscRule	editRule
删除扫描规则	dscRule	deleteRule
添加扫描规则组	dscRuleGroup	addRuleGroup
修改扫描规则组	dscRuleGroup	editRuleGroup
删除扫描规则组	dscRuleGroup	deleteRuleGroup

操作名称	资源类型	事件名称
添加扫描任务	dscScanTask	addScanJob
修改扫描任务	dscScanTask	updateScanJob
删除扫描子任务	dscScanTask	deleteScanTask
删除扫描任务	dscScanTask	deleteScanJob
启动扫描任务	dscScanTask	startJob
停止扫描任务	dscScanTask	stopJob
启动扫描子任务	dscScanTask	startTask
停止扫描子任务	dscScanTask	stopTask
启用/停用ES脱敏	dscBigDataMaskSwitch	switchBigDataMaskStatus
获取ElasticSearch field信息	dscBigDataMetaData	getESField
添加ES脱敏模板	dscBigDataMaskTemplate	addBigDataTemplate
编辑ES脱敏模板	dscBigDataMaskTemplate	editBigDataTemplate
删除ES脱敏模板	dscBigDataMaskTemplate	deleteBigDataTemplate
查询ES脱敏模板列表	dscBigDataMaskTemplate	showBigDataTemplates
启动/停止ES脱敏模板	dscBigDataMaskTemplate	operateBigDataTemplate
切换ES脱敏模板状态	dscBigDataMaskTemplate	switchBigDataTemplate
启用/停用数据库脱敏	dscDBMaskSwitch	switchDBMaskStatus
获取数据库字段信息	dscDBMetaData	getColumn
添加数据库脱敏模板	dscDBMaskTemplate	addDBTemplate
修改数据库脱敏模板	dscDBMaskTemplate	editDBTemplate
删除数据库脱敏模板	dscDBMaskTemplate	deleteDBTemplate
查询数据库脱敏模板列表	dscDBMaskTemplate	showDBTemplates

操作名称	资源类型	事件名称
启动/停止数据库脱敏模板	dscDBMaskTemplate	operateDBTemplate
切换数据库脱敏模板状态	dscDBMaskTemplate	switchDBTemplate
添加脱敏算法	dscMaskAlgorithm	addMaskAlgorithm
编辑脱敏算法	dscMaskAlgorithm	editMaskAlgorithm
删除脱敏算法	dscMaskAlgorithm	deleteMaskAlgorithm
测试脱敏算法	dscMaskAlgorithm	testMaskAlgorithm
获取字段与脱敏算法的映射关系	dscMaskAlgorithm	getFieldAlgorithms
添加加密算法配置	dscEncryptMaskConfig	addEncryptConfig
修改加密算法配置	dscEncryptMaskConfig	editEncryptConfig
删除加密算法配置	dscEncryptMaskConfig	deleteEncryptConfig

与虚拟私有云的关系

虚拟私有云（Virtual Private Cloud，以下简称VPC），为云服务器、云容器、云数据库等资源构建隔离的、用户自主配置和管理的虚拟网络环境，提升用户云上资源的安全性，简化用户的网络部署。

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）为数据安全中心服务提供了权限管理的功能。需要拥有Tenant Administrator权限的用户才能拥有DSC服务的操作权限（包括云资源授权，资产管理以及执行资产检测任务等）。如需开通该权限，请联系拥有Security Administrator权限的用户。

8 安全

8.1 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。

与传统的本地数据中心相比，云计算的运营方和使用方分离，提供了更好的灵活性和控制力，有效降低了客户的运营负担。正因如此，云的安全性无法由一方完全承担，云安全工作需要华为云与您共同努力，如图8-1所示。

- **华为云**：无论在任何云服务类别下，华为云都会承担基础设施的安全责任，包括安全性、合规性。该基础设施由华为云提供的物理数据中心（计算、存储、网络等）、虚拟化平台及云服务组成。在PaaS、SaaS场景下，华为云也会基于控制原则承担所提供服务或组件的安全配置、漏洞修复、安全防护和入侵检测等职责。
- **客户**：无论在任何云服务类别下，客户数据资产的所有权和控制权都不会转移。在未经授权的情况，华为云承诺不触碰客户数据，客户的内容数据、身份和权限都需要客户自身看护，这包括确保云上内容的合法合规，使用安全的凭证（如强口令、多因子认证）并妥善管理，同时监控内容安全事件和账号异常行为并及时响应。

图 8-1 华为云安全责任共担模型

云安全责任基于控制权，以可见、可用作为前提。在客户上云的过程中，资产（例如设备、硬件、软件、介质、虚拟机、操作系统、数据等）由客户完全控制向客户与华为云共同控制转变，这也就意味着客户需要承担的责任取决于客户所选取的云服务。如图8-1所示，客户可以基于自身的业务需求选择不同的云服务类别（例如IaaS、PaaS、SaaS服务）。不同的云服务类别中，每个组件的控制权不同，这也导致了华为云与客户的责任关系不同。

- 在On-prem场景下，由于客户享有对硬件、软件和数据等资产的全部控制权，因此客户应当对所有组件的安全性负责。
- 在IaaS场景下，客户控制着除基础设施外的所有组件，因此客户需要做好除基础设施外的所有组件的安全工作，例如应用自身的合法合规性、开发设计安全，以及相关组件（如中间件、数据库和操作系统）的漏洞修复、配置安全、安全防护方案等。
- 在PaaS场景下，客户除了对自身部署的应用负责，也要做好自身控制的中间件、数据库、网络控制的安全配置和策略工作。
- 在SaaS场景下，客户对客户内容、账号和权限具有控制权，客户需要做好自身内容的保护以及合法合规、账号和权限的配置和保护等。

8.2 身份认证和访问控制

- 身份认证

  用户访问DSC的方式有多种，包括DSC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DSC提供的REST风格的API接口进行请求。

  DSC的接口需要经过认证请求后才可以访问成功。DSC支持两种认证方式：

  - Token认证：通过Token认证调用请求，访问DSC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

  DSC支持通过权限控制（IAM权限）进行访问控制。

  表 8-1 DSC 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产品介绍** **DSC权限管理** **DSC权限管理（细粒度）**

8.3 数据保护技术

DSC通过多种数据保护手段和特性，保证通过DSC的数据安全可靠。

表 8-2 DSC 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）	DSC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	DSC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	• 涉及到用户的数据库账号信息需要存储时，DSC提供敏感数据加密存储，支持加密密钥轮换更新。 • 涉及到用户数据检测时，数据不落盘，只在内存中处理，处理后原始数据及时删除。	-
数据备份	DSC支持用户数据备份。	-
数据销毁	用户主动删除业务数据或销户的情况下，DSC会物理删除对应的业务数据和用户数据。	-
数据脱敏	DSC支持在不影响原始用户数据的情况下对敏感数据进行脱敏，包括静态脱敏和动态脱敏。	**配置脱敏规则**

数据保护手段	简要说明	详细介绍
数据水印	DSC提供数据水印能力，针对用户的PDF、PPT、Word、Excel格式文件提供添加和提取水印的功能，帮助用户文件烙上专属水印，保证资产唯一归属。	文档水印注入或提取

8.4 审计与日志

- 审计

  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DSC的管理事件和数据事件用于审计。

  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DSC操作列表，请参见**支持云审计的操作列表**。

- 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DSC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DSC云审计日志的查看，请参见**查看审计日志**。

8.5 故障恢复

- 数据安全中心故障恢复：
  - DSC提供多个在物理上独立且隔离的可用区，这些可用区通过延迟低、吞吐量高且冗余性高的网络连接在一起。
  - 利用可用区，DSC可以在可用区之间无中断地自动实现故障应用程序和数据库的转移。
  - 与传统的单个或多个数据中心基础设施相比，可用区具有更高的可用性、容错性和可扩展性。
- API数据安全防护故障恢复：
  - 支持双机热备高可用，当主机设备故障时，自动触发主备切换，原主机变备机，提高系统稳定性。
  - Watchdog实时监控服务状态，当服务异常时及时拉起进程。
  - 支持Bypass紧急逃生机制，透传流量，保证业务可用性。
  - 支持OBS配置备份恢复，故障后可快速还原配置信息。

8.6 更新管理

DSC支持定期更新或修补OS、特征库、证书、漏洞和系统配置。

DSC对接CCMS服务管理服务凭证，保证明文的有效凭据不落盘，并保持定期轮转。

8.7 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 8-2 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 8-3 资源中心

9 约束与限制

DSC 支持的华为云数据源

- 关系型数据库（Relational Database Service，RDS）
- 对象存储服务（Object Storage Service，OBS）

  说明

  OBS只支持桶列表，不支持并行文件系统。
- 数据仓库服务（Data Warehouse Service，DWS）
- MapReduce服务（MapReduce Service，MRS）
- 云搜索服务（Cloud Search Service，CSS）
- 数据湖探索服务（Data Lake Insight，DLI）
- 云数据库服务（GaussDB）
- 弹性云服务器（Elastic Cloud Server ，ECS）的自建数据库，支持的自建数据库版本如表9-1所示。
- 裸金属服务器（Bare Metal Server，BMS）的自建数据库
- 云日志服务（Log Tank Service，LTS）

DSC 支持的数据源类型及版本

表 9-1 DSC 支持的数据源类型及版本

数据类型	数据源类型	版本
数据库	MySQL	5.6、5.7、5.8、8.0
	SQL Server	2017_SE、2017_EE、2017_WEB
		2016_SE、2016_EE、2016_WEB
		2014_SE、2014_EE
		2012_SE、2012_EE、2012_WEB
		2008_R2_EE、2008_R2_WEB

数据类型	数据源类型	版本
	PostgreSQL	15、14、13、12、11、10、9.6、9.5、9.4、9.1、1.0
	TDSQL	10.3.X
	Oracle	11、12
	KingBase	V8
	GaussDB	1.3、1.4、2.7
	DMDBMS	7、8
	DWS	8.1.X
大数据	ElasticSearch	5.x、6.x、7.x
	DLI	1.0
	Hive	1.0
	MRS-Hive	3.x
	Hbase	1.0
OBS	OBS	V3

敏感数据识别功能支持的数据源类型

表 9-2 敏感数据功能支持的数据源

资产类型	支持的数据源类型
OBS（传统识别、大语言模型识别）	OBS桶
数据库（传统识别）	RDS、DWS、GaussDB、自建DB（MySQL、TDSQL、KingBase(人大金仓)、DMDBMS(达梦)、PostgreSQL、SQLServer、Oracle）
大数据（传统识别）	Elasticsearch、DLI、Hive、HBase
日志（传统识别）	LTS

数据脱敏功能支持的数据源类型

表 9-3 数据脱敏功能支持的数据源

脱敏类型	支持的数据源类型
数据库脱敏	SQLServer、MySQL、TDSQL、PostgreSQL、KingBase(人大金仓)、DMDBMS(达梦)、GaussDB、Oracle、DWS
Elasticsearch脱敏	Elasticsearch
Hive脱敏	Hive
HBase脱敏	HBase
DLI脱敏	DLI
MRS脱敏	MRS_HIVE
OBS脱敏	OBS桶文件（文本、图片（人脸和车牌））

数据水印功能支持的数据源类型

表 9-4 数据水印功能支持的数据源类型

水印类型	水印类型	支持的数据源类型
数据库水印	有损-列水印	DWS、MRS_HIVE数据库
	无损-伪列/伪行水印	DWS、PostgreSQL、MySQL数据库
文档水印	-	OBS桶、本地文件
图片水印	-	OBS桶、本地文件

10 个人数据保护机制

为了确保您的个人数据（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，DSC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

DSC收集及产生的个人数据如表10-1所示：

表 10-1 个人数据范围列表

类型	收集方式	是否可以修改	是否必须
租户ID	• 在控制台进行任何操作时Token中的租户ID • 在调用API接口时Token中的租户ID	否	是，租户ID是用户的身份标识信息。
数据库密码	租户在控制台自行填入	是	是，对数据库数据进行扫描、脱敏和注入水印时，DSC需使用数据库密码联通数据库，获取数据。

存储方式

- 租户ID不属于敏感数据，明文存储。
- 数据库密码：加密存储。

访问权限控制

用户只能查看自己业务的相关日志。

日志记录

用户个人数据的所有操作，包括修改、查询和删除等，DSC都会记录审计日志并上传至云审计服务（CTS），用户可以并且仅可以查看自己的审计日志。

11 DSC 权限管理

如果您需要对华为云上购买的数据安全中心（DSC）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安全中心（DSC）的使用权限，但是不希望他们拥有删除DSC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DSC，但是不允许删除DSC的权限策略，控制他们对华为云DSC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DSC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》**。

DSC 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。

DSC部署时通过物理区域划分，为项目级服务。授权时，“作用范围”需要选择“区域级项目”，然后在指定区域对应的项目中设置相关权限，并且该权限仅对此项目生效；如果在“所有项目”中设置权限，则该权限在所有区域项目中都生效。访问DSC时，需要先切换至授权区域。

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DSC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。

如表11-1所示，包括了DSC下所有的系统角色。

表 11-1 DSC 系统权限

角色名称	描述	类别	依赖关系
DSC DashboardReadOnlyAccess	数据安全中心服务大屏服务只读权限。	系统策略	无
DSC FullAccess	数据安全中心服务所有权限。	系统策略	购买RDS包周期实例需要配置授权项： bss:order:update bss:order:pay
DSC ReadOnlyAccess	数据安全中心服务只读权限。	系统策略	无

须知

用户在执行**云资源委托授权/停止授权**时必须拥有IAM的管理员权限（“Security Administrator”权限）。

相关链接

- **IAM产品介绍**
- **创建用户组、用户并授权DSC权限**

12 基本概念

自有桶

自有桶是指当前用户自己创建的桶，包含公共桶和私有桶。

公共桶

创建OBS桶时，“桶策略”选择为“公共读”或者“公共写”的桶为公共桶，任何用户都可以对桶内对象进行读/写/删除操作。

私有桶

创建OBS桶时，“桶策略”选择为“私有”的桶为私有桶，仅当前用户自己能访问该桶。

其他桶

其他桶是指其他用户创建的桶且桶权限设置为“公共”的桶，或者为当前账户拥有权限的私有桶。

数据库扩展包

1个数据库扩展包含1个可添加数据库（支持RDS、DWS、ECS自建数据库、DLI、Elasticsearch、ECS自建大数据等）资产。

OBS 扩展包

1个OBS扩展包含1T体量，即1024GB。

伪行

在数据库中插入按照原始数据格式生成的虚假行数据，相关功能请参见**数据库水印**。

伪列

在数据库中插入按照用户所填列信息生成的虚假列数据，相关功能请参见**数据库水印**。