数据安全中心

产品介绍

文档版本 27

发布日期 2024-04-15

华为云计算技术有限公司

版权所有 © 华为云计算技术有限公司 2024。 保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

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

 版权所有 © 华为云计算技术有限公司

1 什么是数据安全中心

数据安全中心服务（Data Security Center，DSC）是新一代的云化数据安全平台，提供数据分级分类、数据安全风险识别、数据水印溯源和数据静态脱敏等基础数据安全能力，通过资产地图整合数据安全生命周期各阶段状态，对外整体呈现云上数据安全态势。

云上全场景覆盖

整合云上各类数据源，提供一站式数据保护和防御机制。支持结构化和非结构化类型数据，支持云原生和ECS自建场景。

全栈敏感数据防护

根据敏感数据发现策略来精确识别数据库中的敏感数据，基于多种预置脱敏算法+用户自定义脱敏算法，实现全栈敏感数据防护。

须知

DSC仅对数据进行敏感数据检测，不会对您的数据文件进行保存。

版权所有 © 华为云计算技术有限公司

2 规格版本差异

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。

表 2-1 服务版本差异

规格版本	支持添加的数据库数量	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 • 敏感数据识别 • 数据风险检测
专业版	2个	100GB	100W次	• 资产地图 • 敏感数据识别 • 数据风险检测 • 数据脱敏 • 数据水印注入/提取 • API接口的调用

版权所有 © 华为云计算技术有限公司

3 功能特性

数据安全中心为您提供的功能如表3-1。

表 3-1 功能概览

功能特性	说明	参考文档
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。 ● 资产可视化 – 数据服务资产：涵盖了云上所有数据资产，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：识别云上关键数据出口，包含EIP/NAT/APIGateway/Roma等。 – 出口关联资产：云上出口和数据关联，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。	资产地图

版权所有 © 华为云计算技术有限公司

功能特性	说明	参考文档
资产管理	• **资产中心：**DSC支持管理OBS、数据库、大数据和MRS数据资产。 • **资产目录：**查看不同业务域或不同类型数据的统计信息。 • **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。 • **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。 • **资产分组管理：**对现有数据进行分组管理。	**资产管理**
敏感数据识别	• **数据自动分级分类：精确**识别敏感数据和文件，覆盖结构化（RDS、DWS等）和非结构化（OBS）两种数据类型，实现云上全场景覆盖。 – 文件类型：支持近200种非结构化文件。 – 数据类型：支持数十种个人隐私数据类型，包含中英文。 – 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。 – 合规模板：多种内置合规知识库，如GDPR，PCI DSS，HIPAA等。 • **自动识别敏感数据** – 自动识别敏感数据及个人隐私数据。 – 支持自定义规则，场景适配不同行业。 – 提供可视化识别结果。 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**。	**新建敏感数据识别任务**

版权所有 © 华为云计算技术有限公司

功能特性	说明	参考文档
数据脱敏	DSC的数据脱敏支持静态脱敏和动态脱敏。 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**脱敏算法**。 • **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提供了数据动态脱敏的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和HBase数据进行脱敏，具体的脱敏时长请参见**DSC脱敏时长**。	**配置脱敏规则**
数据水印	针对数据库、文档提供了添加和提取水印的功能。 • **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**。	**水印注入**
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。	**OBS使用审计**
设备管理	设备管理的作用是纳管第三方设备，包含应用数据审计设备、应用数据安全网关设备、数据库防火墙设备、数据库加密设备，进行状态监控和告警展示，将风险和告警呈现给客户。 用户可单击DSC设备列表“操作”列“登录”，跳转到第三方设备管理页面。	**设备管理**
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。	**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。	**告警通知**

版权所有 © 华为云计算技术有限公司

4 产品优势

数据安全全生命周期可视

整合数据安全全生命周期各阶段状态，对外整体呈现云上数据安全态势。

云上全场景覆盖

整合云上各类数据源，提供一站式数据保护和防御机制。支持结构化和非结构化类型数据，支持云原生和ECS自建场景。

高效识别

在专家知识库和NLP的双重加权下，识别能力更强，高效锁定敏感数据源。

全栈敏感数据防护

根据敏感数据发现策略来精确识别数据库中的敏感数据，基于多种预置脱敏算法+用户自定义脱敏算法，实现全栈敏感数据防护。

版权所有 © 华为云计算技术有限公司

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。

版权所有 © 华为云计算技术有限公司

- 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。

保留期的时长由客户等级而定，详细信息请参见“**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**。

版权所有 © 华为云计算技术有限公司

6 应用场景

敏感数据自动识别分类

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（RDS）和非结构化数据（OBS）进行扫描、分类、分级，解决数据“盲点”，以此做进一步安全防护。

用户异常行为分析

通过深度行为识别引擎，建立用户行为基线，实现基线外异常操作实时告警，行为操作实时查询，行为轨迹可视化，风险事件关联识别，针对风险事件关联用户操作，完善溯源审计链条。及时发现数据使用是否存在安全违规并及时预警，预防数据泄露。

数据脱敏保护

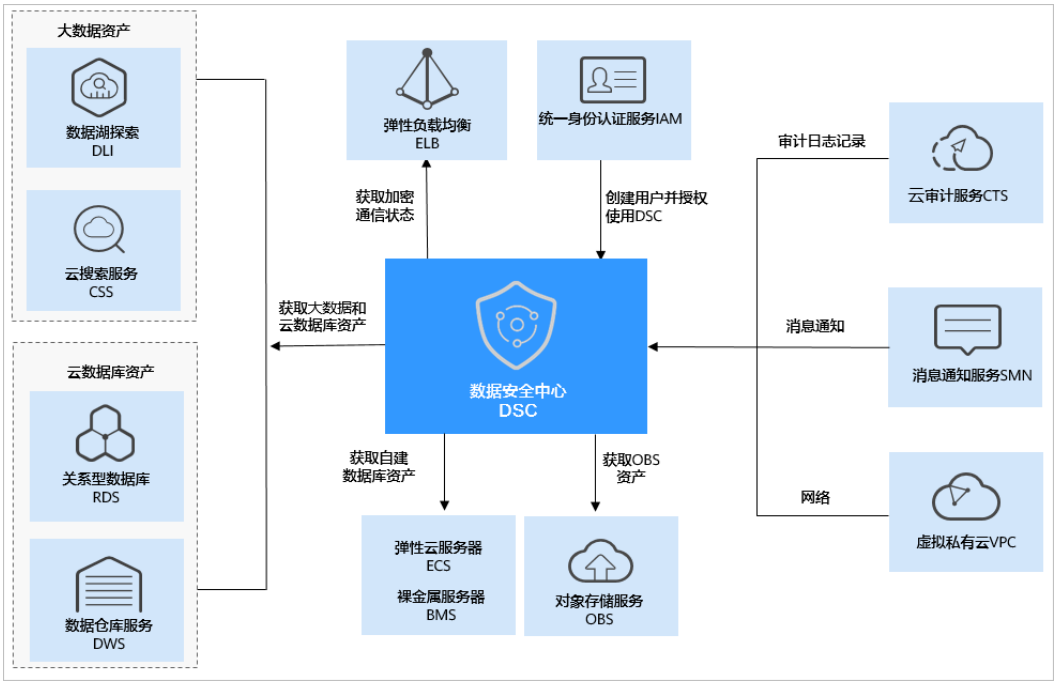
通过多种预置脱敏算法+用户自定义脱敏算法，搭建数据保护引擎，实现非结构化数据脱敏储存，结构化数据静态脱敏，防止敏感数据泄露。

版权所有 © 华为云计算技术有限公司

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。

版权所有 © 华为云计算技术有限公司

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。

与文档数据库服务的关系

文档数据库服务（Document Database Service，简称DDS）完全兼容MongoDB协议，提供安全、高可用、高可靠、弹性伸缩和易用的数据库服务，同时提供一键部署、弹性扩容、容灾、备份、恢复、监控和告警等功能。经用户授权后，数据安全中心可以为文档数据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。

版权所有 © 华为云计算技术有限公司

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

版权所有 © 华为云计算技术有限公司

操作名称	资源类型	事件名称
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
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

版权所有 © 华为云计算技术有限公司

操作名称	资源类型	事件名称
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
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。

版权所有 © 华为云计算技术有限公司

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。

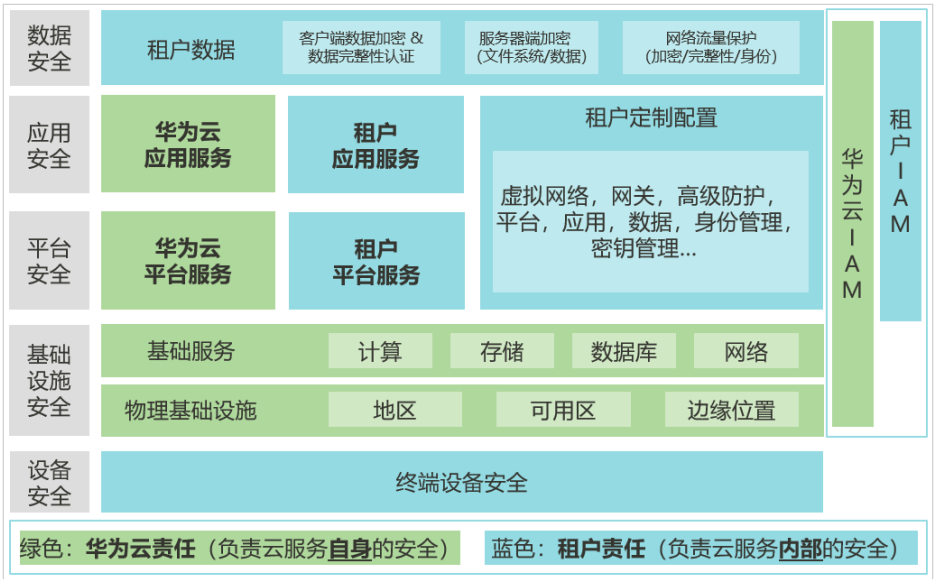
安全性是华为云与您的共同责任，如图8-1所示。

- **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。

版权所有 © 华为云计算技术有限公司

图 8-1 华为云安全责任共担模型



8.2 资产识别与管理

DSC是新一代的云化数据安全平台，支持管理用户的OBS、数据库、大数据和MRS数字资产，帮助用户的云上资产进行风险识别，呈现云上数据安全态势。

表 8-1 DSC 的资产管理

资产管理方式	简要说明	详细介绍
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、敏感数据以及数据出口分析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进行快速风险处理操作。	资产地图
资产管理	DSC提供资产管理的功能，对云上资产进行数据探索、分组管理等。	资产管理
敏感数据识别	敏感数据自动识别分类，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（RDS）和非结构化数据（OBS）进行扫描、分类、分级，解决数据“盲点”，以此做进一步安全防护。	新建敏感数据识别任务
数据脱敏	DSC的数据脱敏支持静态脱敏和动态脱敏。您可以对指定数据配置脱敏规则实现敏感数据静态脱敏，同时，您也可以使用数据动态脱敏的API接口实现数据的动态脱敏，全方位确保敏感信息不被泄露。	数据脱敏

版权所有 © 华为云计算技术有限公司

8.3 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 8-2 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）**

8.4 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 8-3 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**

版权所有 © 华为云计算技术有限公司

数据保护手段	简要说明	详细介绍
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。	水印注入

8.5 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**。

8.6 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。

版权所有 © 华为云计算技术有限公司

8.7 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。

8.8 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 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**。

版权所有 © 华为云计算技术有限公司

图 8-3 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 8-4 销售许可证&软件著作权证书

版权所有 © 华为云计算技术有限公司

9 使用约束

DSC目前仅支持管理华为云上数据资产，暂不支持管理其他云厂商的数据资产。

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）
- 文档数据库服务（Document Database Service，DDS）
- 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）
- 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

DSC 支持的数据源类型及版本

数据安全中心支持的资产类型及版本如表1所示。

表 9-1 DSC 支持的数据源类型及版本

数据源类型	版本
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

版权所有 © 华为云计算技术有限公司

数据源类型	版本
KingBase	V8
DMDBMS	7、8
GaussDB for openGauss	1.4
PostgreSQL	11、10、9.6、9.5、9.4、9.1
TDSQL	10.3.X
Oracle	11、12
DDS	4.2、4.0、3.4
DWS	4.2、4.0、3.4
ElasticSearch	5.x、6.x、7.x
DLI	1.0
Hive	1.0
HBase	1.0
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	OBS
数据库	RDS、DWS、DDS、GaussDB、自建DB（MySQL、TDSQL、KingBase、DMDBMS、PostgreSQL、SQLServer、Oracle）
大数据	Elasticsearch、DLI、Hive、HBase

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	资产类型	支持的数据源类型
数据库脱敏	数据库	SQLServer、MySQL、TDSQL、PostgreSQL、DMDBMS、KingBase、OpenGauss、Oracle、DWS

版权所有 © 华为云计算技术有限公司

脱敏类型	资产类型	支持的数据源类型
Elasticsearch脱敏	大数据	Elasticsearch
Hive脱敏		Hive
HBase脱敏		HBase
MRS脱敏	MRS	MRS_HIVE

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	资产类型	水印类型	支持的数据源类型
数据库水印	数据库	有损-列水印	DWS、MRS_HIVE
		无损-伪列/伪行水印	DWS、PostgreSQL、MySQL
文档水印	OBS	-	OBS

版权所有 © 华为云计算技术有限公司

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。

版权所有 © 华为云计算技术有限公司

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。

版权所有 © 华为云计算技术有限公司

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。

版权所有 © 华为云计算技术有限公司

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

版权所有 © 华为云计算技术有限公司

A 修订记录

发布日期	修改说明
2024-04-15	第二十八次正式发布。 修改**功能特性**章节。
2024-01-15	第二十八次正式发布。 修改**使用约束**章节。
2023-11-30	第二十七次正式发布。 修改**功能特性**章节。
2023-09-30	第二十六次正式发布。 修改**功能特性**章节。
2023-06-30	第二十五次正式发布。 修改功能特性章节。
2023-03-30	第二十四次正式发布。 修改**功能特性**章节。
2023-01-31	第二十三次正式发布。 修改**个人数据保护机制**章节。
2023-01-16	第二十二次正式发布。 修改**功能特性**章节。
2022-11-09	第二十一次正式发布。 增加**安全**章节。
2022-09-30	第二十次正式发布。 修改**功能特性**章节。
2022-03-11	第十九次正式发布。 修改**功能特性**章节，优化相关描述。

版权所有 © 华为云计算技术有限公司

发布日期	修改说明
2022-01-26	第十八次正式发布。 增加“图解数据安全中心”章节。
2021-12-28	第十七次正式发布。 修改如下章节： **规格版本差异**
2021-09-22	第十六次正式发布。 修改计费说明章节。
2021-09-14	第十五次正式发布。 ● 修改**功能特性**章节。 ● 修改计费说明章节。
2021-06-18	第十四次正式发布。 ● 修改**与其他云服务的关系**章节，增加与裸金属服务器的关系。 ● 修改**使用约束**章节，支持的数据库类别增加裸金属服务器。
2021-05-18	第十三次正式发布。 修改**使用约束**章节，增加厂商的相关描述。
2021-04-30	第十二次正式发布。 ● 修改**功能特性**章节，敏感数据识别增加图片类型。 ● 修改**使用约束**章节，feedback问题修改。
2021-03-11	第十一次正式发布。 修改**功能特性**章节。
2021-02-27	第十次正式发布。 ● 修改计费说明章节，DSC正式商用。 ● 增加**规格版本差异**章节。
2021-02-19	第九次正式发布。 修改**使用约束**章节，增加了RDS数据库的使用限制。
2021-02-03	第八次正式发布。 修改**使用约束**章节，MySQL数据库支持8.0版本。
2021-01-13	第七次正式发布。 修改**功能特性**章节，增加了数据脱敏和水印的功能。

版权所有 © 华为云计算技术有限公司

发布日期	修改说明
2021-01-04	第六次正式发布。 修改1.13-DSC权限管理章节，增加了DSC的系统策略。
2020-12-18	第五次正式发布。 增加**使用约束**章节。
2020-12-14	第四次正式发布。 增加**个人数据保护机制**章节。
2020-11-26	第三次正式发布。 优化**与其他云服务的关系**，增加了与数据湖服务的关系。
2020-11-16	第二次正式发布。 优化**功能特性**章节。
2020-09-30	第一次正式发布。

版权所有 © 华为云计算技术有限公司