数据安全中心

用户指南

文档版本 02

发布日期 2023-03-30

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 产品介绍

1.1 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，通过数据安全总览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。

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。

1.2 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1-1**所示。

表 1-1 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	• 数据安全总览 • 敏感数据识别
专业版	2个	100GB	100W次	• 数据安全总览 • 敏感数据识别 • 数据脱敏 • 数据水印注入/提取 • API接口的调用

1.3 功能特性

数据安全中心为您提供的功能如**表1-2**。

表 1-2 功能概览

功能特性	说明	参考文档
数据安全总览	展示数据安全全生命周期各个阶段的状态，包括云服务全景图（资产地图）、数据采集安全、数据传输/存储安全、数据使用安全和数据交换/删除安全，实时呈现了用户资产的具体情况。	**数据安全概览**
资产列表	DSC支持管理OBS、数据库、大数据和MRS数据资产。 可添加资产的约束条件详见**使用约束**。	**批量添加资产**

功能特性	说明	参考文档
敏感数据识别	• **数据自动分级分类：**精准识别敏感数据和文件，覆盖结构化（RDS）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。 – 血缘图梳理敏感文件框架，清晰定位。 – 提供合规报表下载，数据透明可视。	创建敏感数据识别任务

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。 • **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。 DSC通过内置和自定义脱敏算法，实现对RDS、Elasticsearch数据进行脱敏。	配置脱敏规则
数据水印	针对PDF、PPT、Word、Excel格式的文件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。	水印注入

功能特性	说明	参考文档
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

1.4 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。

精准高效识别

在专家知识库和NLP的双重加权下，识别能力更强，精准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准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。

1.5 计费说明

数据安全中心服务支持按需计费（后付费）计费方式。

计费项

表 1-3 计费项信息

计费模式	计费项目	计费说明
按需计费	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。

计费模式	计费项目	计费说明
	OBS扩展包（可选）	按购买个数计费。
	API接口（数据脱敏和水印API调用）	仅专业版支持，按调用次数收费。

计费模式

按需计费：购买方式比较灵活，可以即开即停。

从开通并使用DSC开始计费到关闭按需计费时结束计费，按申请的服务版本、数据库扩展包和OBS扩展包个数以及使用的API接口请求数计费。

1.6 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。

满足信息合规要求

DSC拥有数十种合规模板，包含GDPR，PCI DSS，HIPAA等，多种合规规则一键匹配识别，生成报表供针对性整改，精准区分和保护个人数据，避免产生合规问题。

1.7 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

数据湖探索服务（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 1-4 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

操作名称	资源类型	事件名称
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
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

操作名称	资源类型	事件名称
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
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。

1.8 使用约束

支持的数据源

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

支持的数据库类型及版本

数据安全中心支持的数据库类型及版本如**表1**所示。

表 1-5 DSC 支持的数据库类型及版本

数据库类型	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
PostgreSQL	11、10、9.6、9.5、9.4、9.1
Oracle	10、12

1.9 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1-6**所示：

表 1-6 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。

1.10 DSC 权限管理

如果您需要对云上的数据安全中心（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云上资源的访问。

通过IAM，您可以在帐号中给员工创建IAM用户，并使用策略来控制他们对云资源的访问范围。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DSC资源的使用范围。

如果帐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。

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1-7所示，包括了DSC下所有的系统角色。

表 1-7 DSC 系统角色

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	无
DSC ReadOnlyAccess	数据安全中心服务只读权限。	系统策略	无

2 开通 DSC

2.1 购买数据安全中心

数据安全中心支持按需计费的计费方式。同时，DSC提供两种扩展包：数据库扩展包和OBS扩展包。您可以根据业务需求申请数据安全中心服务。

前提条件

已通过IAM对用户绑定“DSC FullAccess”权限的用户组。

规格限制

- 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、Elasticsearch、ECS自建大数据等）资产。
- 1个OBS扩展包含1T体量，即1024G。

操作步骤

步骤1 登录管理控制台。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全 > 数据安全中心”。

步骤4 首次购买DSC，在界面左侧，单击“立即购买”。

步骤5 在“购买数据安全中心”页面，选择“当前区域”和“版本规格”。

步骤6 选择“数据库扩展包”和“OBS扩展包”的数量。

图 2-1 选择扩展包

- 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、Elasticsearch、ECS自建大数据等）资产。
- 1个OBS扩展包含1T体量，即1024G。

步骤7 在页面的右下角，单击“申请使用”。

----结束

2.2 升级规格

申请数据安全中心服务后，您可以从较低版本（标准版）的DSC升级到更高版本（专业版），也可以根据需求增加数据库扩展包和OBS扩展包的数量。

前提条件

- 已通过IAM对用户绑定“DSC FullAccess”权限的用户组。
- 已购买任一版本的数据安全中心服务。

规格限制

- 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、Elasticsearch、ECS自建大数据等）资产。
- 1个OBS扩展包含1T体量，即1024G。

操作步骤

步骤1 登录管理控制台。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全 > 数据安全中心”，进入数据安全中心总览界面。

步骤4 在页面的右上角单击“升级规格”。

步骤5 在DSC的购买页面，“版本规格”默认为当前服务版本，您可以选择比当前服务规格更高的服务版本。

“版本规格”从左到右，服务版本的规格越高。

图 2-2 升级版本规格

步骤6 选择“数据库扩展包”和“OBS扩展包”的数量。

图 2-3 选择扩展包

- 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、Elasticsearch、ECS自建大数据等）资产。
- 1个OBS扩展包含1T体量，即1024G。

步骤7 在页面的右下角，单击“申请使用”。

----结束

2.3 退订数据安全中心

申请数据安全中心后，可参考本章节退订已申请的订单。

前提条件

已申请数据安全中心服务。

操作步骤

步骤1 登录管理控制台。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全 > 数据安全中心”，进入数据安全中心总览界面。

步骤4 在页面的右上角单击“退订”。

步骤5 在弹出的对话框中，单击“确定”。

----结束

3 资产列表

3.1 云资源委托授权/停止授权

本章节将介绍如何授权或者停止授权访问私有OBS桶、数据库、大数据、MRS以及数据安全总览。系统将为您创建可供DSC使用的委托关系。

前提条件

已通过IAM对用户绑定“DSC FullAccess”权限的用户组，具体的操作请参见**创建用户并授权使用DSC**。

约束条件

- 同意授权后，DSC将根据您的选择，设置委托权限以此来访问您的OBS，数据库，大数据实例以及其他相应的云上资产。
- 停止授权，需要您的资产没有绑定任务。停止授权后，DSC会删除您的委托和资产信息，对应的所有数据将被清除，请谨慎操作。

开通授权后获得的授权委托策略

表 3-1 对应授权项服务创建的委托

资产模块	服务策略	作用范围	备注
OBS	OBS Adminstrator	全局	用于配置OBS日志，获取OBS对象列表，下载OBS对象等
	EVS ReadOnlyAccess	区域	用于获取云硬盘列表
	OBS Adminstrator	全局	用于获取OBS服务投递日志

资产模块	服务策略	作用范围	备注
数据库	ECS ReadOnlyAccess	区域	用于获取自建数据库ECS列表
	RDS ReadOnlyAccess	区域	用于获取RDS数据库列表及数据库列表相关信息
	DWS ReadOnlyAccess	区域	用于获取DWS列表
	VPC FullAccess	区域	用于打通网络，VPC的端口创建，安全组规则创建等
	KMS CMKFullAccess	区域	用于使用KMS加密脱敏的场景
大数据	ECS ReadOnlyAccess	区域	用于获取自建大数据ECS列表
	CSS ReadOnlyAccess	区域	用于获取CSS数据集群列表及数据索引等相关信息
	DLI Service User	区域	用于获取DLI队列及数据库
	VPC FullAccess	区域	用于打通网络，VPC的端口创建，安全组规则创建等
	KMS CMKFullAccess	区域	用于使用KMS加密脱敏的场景
数据安全总览	Tenant Guest	区域	用于获取用户涉及数据存储处理等相关云服务的列表等
	OBS Adminstrator	全局	用于配置OBS日志，获取OBS对象列表，下载OBS对象等
	EVS ReadOnlyAccess	区域	用于云硬盘列表获取
	OBS Adminstrator	全局	用于OBS服务投递日志

操作步骤

步骤1 登录管理控制台。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击 ，选择“安全 > 数据安全中心”，进入数据安全中心总览界面。

步骤4 在左侧导航树中选择“资产列表”，进入OBS资产列表页面。

步骤5 单击页面右上角的“云资产委托授权”。

图 3-1 资产列表

步骤6 在“云资源委托授权”页面，开启/停止授权访问对应的云资源，根据**表3-2**进行操作。

图 3-2 云资源委托授权

表 3-2 参数说明

参数名称	参数说明
资产模块	DSC提供了四种资产模块： • OBS：对象存储服务。 • 数据库：DSC支持的数据库类型及版本请参见**使用约束**。 • 大数据：授权访问云搜索服务（CSS）和数据湖探索（DLI）的资产。 • MRS：MapReduce服务（MapReduce Service，简称MRS） • 数据安全总览：授权访问云上数据存储，传输，使用，交换以及删除等信息的采集权限。
开通授权状态	两种状态： • 已授权 • 未授权
操作	单击图标开启或者停止授权。 •  ：未授权 •  ：已授权

----结束

3.2 批量添加资产

如果您需要批量添加OBS、数据库、大数据或者MRS资产，可参考本章节进行操作。

前提条件

- 已完成数据库资产委托授权，参考**云资源委托授权/停止授权**进行操作。
- 已获取自建数据库的引擎、版本、主机等相关信息，且自建数据库子网下含有可用的IP配额。

约束条件

只能添加数据安全中心支持的数据库类型及版本，DSC支持的数据库类型及版本如**表3-3**所示。

表 3-3 DSC 支持的数据库类型及版本

数据库类型	版本
MySQL	5.6、5.7、5.8、8.0

数据库类型	版本
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
PostGreSQL	11、10、9.6、9.5、9.4、9.1
Oracle	10、12

操作步骤

步骤1 登录管理控制台。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全 > 数据安全中心”，进入数据安全中心总览界面。

步骤4 在左侧导航树中选择“资产列表”，进入OBS资产列表页面。

图 3-3 OBS 资产列表

步骤5 在OBS资产列表右上角，单击“批量添加”。

步骤6 在弹出的“批量添加”对话框中，单击“添加文件”，将已整理好的资产文件导入到系统中。

单击“下载模板”，将资产信息按模板整理好。

图 3-4 批量添加自建数据库

步骤7 单击“确定”，批量添加数据库完成。

图 3-5 连通性测试

数据库添加完成后，该数据库的“连通性”为“检查中”，此时，DSC会测试数据库的连通性。

- DSC能正常访问已添加的数据库，该数据库的“连通性”状态为“成功”。
- 若DSC不能正常访问已添加的数据库，该数据库的“连通性”状态为“失败”。单击“原因”查看失败的原因。

----结束

3.3 OBS 资产列表

3.3.1 添加 OBS 资产

授权DSC服务访问OBS资产后，可将OBS资产添加到DSC服务里进行防护。

前提条件

- 已完成OBS资产委托授权，参考**云资源委托授权/停止授权**进行操作。
- 如果需要添加自有OBS桶，则需要已开通且已使用过OBS服务。
- 如果需要添加其他桶，则需设置该桶的权限为“公共”。

操作步骤

步骤1 登录管理控制台。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全 > 数据安全中心”，进入数据安全中心总览界面。

步骤4 在左侧导航树中选择“资产列表”，进入OBS资产列表页面。

图 3-6 OBS 资产列表

步骤5 添加OBS资产。

- 添加自有桶

a. 在OBS资产列表左上角，单击“添加自有桶”。
b. 在弹出添加自有桶对话框中，勾选需要添加的OBS桶。

图 3-7 添加自有桶

c. 单击“确定”。

- 添加其他桶

a. 在OBS资产列表左上角，单击“添加其他桶”。
b. 在弹出的添加其他桶对话框中，输入待添加桶的名称。

如需添加多个桶，则可单击 添加 ，继续进行添加。

图 3-8 添加其他桶

c. 单击“确定”。

----结束

相关操作

- OBS资产授权/停止授权，请参见**云资源委托授权/停止授权**章节。
- 删除OBS资产，请参见**删除OBS资产**章节。

3.3.2 删除 OBS 资产

本章节介绍如何删除已添加到DSC防护的OBS桶。删除后，该资产在DSC服务里建立的相关任务模板以及扫描任务结果报告都将被删除，且无法恢复。

前提条件

- 已完成OBS资产委托授权，参考**云资源委托授权/停止授权**进行操作。
- 待删除的OBS资产未被应用在敏感数据识别任务中。

约束条件

- 如果需要删除的OBS资产已被应用在敏感数据检测任务中，请先解绑资产或者删除任务，再参照本章节删除资产。
- 资产删除后无法恢复，资产相关的任务模板，任务结果，报表都将删除，请谨慎操作。

操作步骤

步骤1 登录管理控制台。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全 > 数据安全中心”，进入数据安全中心总览界面。

步骤4 在左侧导航树中选择“资产列表”，进入OBS资产列表页面。

图 3-9 OBS 资产列表

步骤5 在OBS资产列表中，在需要删除的OBS资产所在行的“操作”列，单击“删除”。

步骤6 在弹出窗口中，单击“确定”。

----结束

3.4 数据库资产列表

3.4.1 添加 RDS 数据库

如果您已经完成数据库资产委托授权，并开通了关系型数据库（RDS），且已在RDS里创建了数据库，可参考本章节对RDS创建的云数据库进行相关操作的授权。具体如下：

- 授权“只读权限”：只能使用敏感数据识别功能。

- 授权“读写权限”：可使用敏感数据识别和数据脱敏功能。

说明

DSC暂不支持对RDS中已开启SSL的MySQL数据库进行扫描和脱敏。

前提条件

- 已完成数据库资产委托授权，参考**云资源委托授权/停止授权**进行操作。
- 已开通RDS服务，且RDS中已有资产，且对应子网下含有可用的IP配额。
- RDS实例的“状态”为“正常”。

操作步骤

步骤1 登录管理控制台。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全 > 数据安全中心”，进入数据安全中心总览界面。

步骤4 在左侧导航树中选择“资产列表”，并选择“数据库 > 未授权”，进入未授权数据库资产列表页面。

图 3-10 未授权数据库资产列表

步骤5 在需要授权的数据库资产所在行的“操作”列，单击“授权”。

说明

如果只需要授权数据库实例下的某个数据库，单击数据库实例前的，展开实例列表，单击数据库所在行的操作列的“授权”即可。

步骤6 在弹出的“数据库批量授权”对话框中，参考**表3-4**配置数据库参数。

图 3-11 数据库批量授权

表 3-4 参数说明

参数名称	参数说明
权限设置	• 只读权限：只能用于敏感数据识别。 **注意** 创建了RDS只读权限后，DSC服务会在RDS创建一个dsc_readonly帐户。 – dsc_readonly帐户的密码在RDS重置后，将不会自动同步到DSC服务，会导致敏感数据识别任务失败，因此，建议您不要重置该帐户密码。 – 如果您已在RDS里重置了dsc_readonly帐户的密码，建议您在DSC服务里先删除已授权的rds实例，再重新对该实例进行权限设置。 • 读写权限：可使用敏感数据识别和数据脱敏功能。
资产列表	• “权限设置”选择“只读权限”时，可修改需要授权的“资产名称”。 • “权限设置”选择“读写权限”时，可修改需要授权的“资产名称”，必需配置访问该数据库的“用户名”和“密码”。

步骤7 单击“确定”，数据库添加完成，并展示在已授权的数据库列表中。

图 3-12 连通性测试

数据库添加完成后，该数据库的“连通性”为“检查中”，此时，DSC会测试数据库的连通性。

- DSC能正常访问已添加的数据库，该数据库的“连通性”状态为“成功”。
- 若DSC不能正常访问已添加的数据库，该数据库的“连通性”状态为“失败”。单击“原因”查看失败的原因。

----结束

相关操作

- 数据库资产授权/停止授权，请参见**云资源委托授权/停止授权**章节。
- 编辑数据库资产，请参见**编辑数据库信息**章节。
- 删除数据库资产，请参见**删除数据库资产**章节。

3.4.2 添加云数据库

如果您已经开通了数据仓库服务（DWS）或文档数据库服务（DDS），并已在DWS或者DDS里创建了数据库，可参考本章节直接将DWS和DDS创建的云数据库数据添加到DSC里。

前提条件

- 已完成数据库资产委托授权，参考**云资源委托授权/停止授权**进行操作。
- 已开通DWS或者DDS服务，且DWS或者DDS中已有资产，且对应子网下含有可用的IP配额。

操作步骤

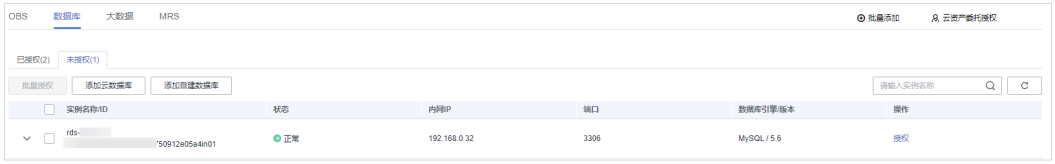
步骤1 登录管理控制台。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全 > 数据安全中心”，进入数据安全中心总览界面。

步骤4 在左侧导航树中选择“资产列表”，并选择“数据库 > 未授权”，进入未授权数据库资产列表页面。

图 3-13 未授权数据库资产列表



步骤5 在数据库资产列表左上角，单击“添加云数据库”。

步骤6 在弹出的“添加云数据库”对话框中，参考**表3-5**配置数据库参数。

图 3-14 添加云数据库

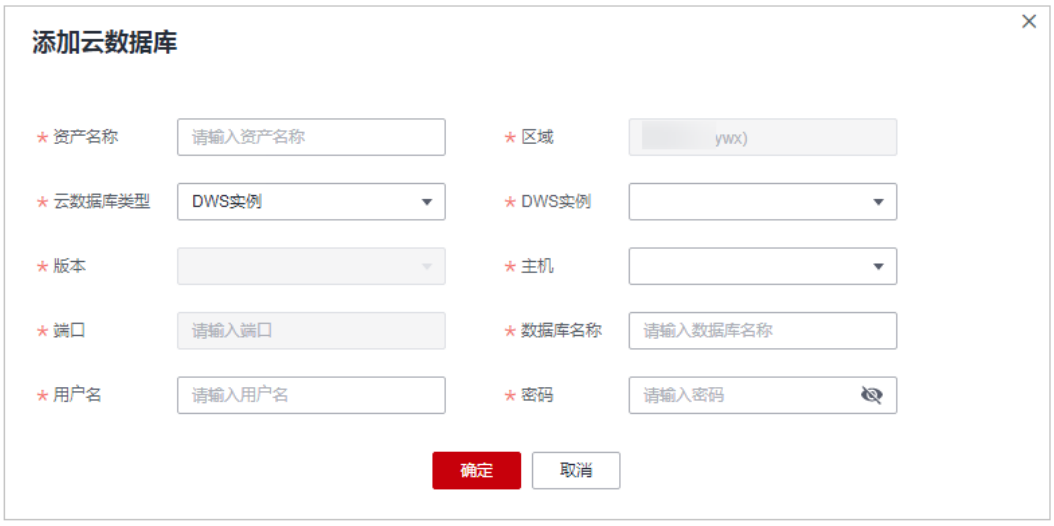


表 3-5 云数据库参数列表

参数名称	参数说明	举例
资产名称	自定义参数。	dsc_test

参数名称	参数说明	举例
区域	默认为当前帐号登录的区域。	--
云数据库类型	可选择“DWS实例”和“DDS实例”。	DWS实例
DWS实例	“云数据库类型”选择“DWS实例”时，配置此参数。 在下拉框中选择本帐号下已在DWS里创建的数据库实例。	--
DDS实例	“云数据库类型”选择“DDS实例”时，配置此参数。 在下拉框中选择本帐号下已在DDS里创建的数据库实例。	--
版本	已选数据库实例对应的版本号，默认参数，不支持修改。	5.7
主机	在下拉框中选择数据库服务器IP地址。	192.168.0.233
端口	数据库服务器的端口号，默认参数，不支持修改。	3306
数据库名称	在DWS里创建的数据库，支持下拉框选择和手动输入。	--
用户名	输入访问数据库服务器的用户名，与DWS里创建的保持一致。	--
密码	输入访问数据库服务器的密码，与DWS里创建的保持一致。	--

步骤7 单击“确定”，数据库添加完成，并展示在已授权的数据库列表中。

图 3-15 连通性测试

数据库添加完成后，该数据库的“连通性”为“检查中”，此时，DSC会测试数据库的连通性。

- DSC能正常访问已添加的数据库，该数据库的“连通性”状态为“成功”。
- 若DSC不能正常访问已添加的数据库，该数据库的“连通性”状态为“失败”。单击“原因”查看失败的原因。

----结束

相关操作

- 数据库资产授权/停止授权，请参见**云资源委托授权/停止授权**章节。
- 编辑数据库资产，请参见**编辑数据库信息**章节。
- 删除数据库资产，请参见**删除数据库资产**章节。

3.4.3 添加自建数据库

如果您需要添加RDS和云数据库以外的自建数据库资产，可参考本章节进行操作，添加自建数据库资产前，需要获取自建数据库的引擎、版本、主机等相关信息。

前提条件

- 已完成数据库资产委托授权，参考**云资源委托授权/停止授权**进行操作。
- 已获取自建数据库的引擎、版本、主机等相关信息，且自建数据库子网下含有可用的IP配额。

约束条件

只能添加数据安全中心支持的数据库类型及版本，DSC支持的数据库类型及版本如**表3-6**所示。

表 3-6 DSC 支持的数据库类型及版本

数据库类型	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
PostGreSQL	11、10、9.6、9.5、9.4、9.1
Oracle	10、12

操作步骤

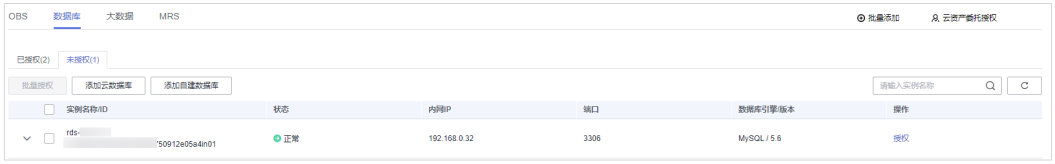
步骤1 登录管理控制台。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全 > 数据安全中心”，进入数据安全中心总览界面。

步骤4 在左侧导航树中选择“资产列表”，并选择“数据库 > 未授权”，进入未授权数据库资产列表页面。

图 3-16 未授权数据库资产列表



步骤5 在未授权数据库资产列表左上角，单击“添加自建数据库”。

步骤6 在弹出的“添加自建数据库”对话框中，参考**表3-7**配置数据库参数。

图 3-17 添加自建数据库

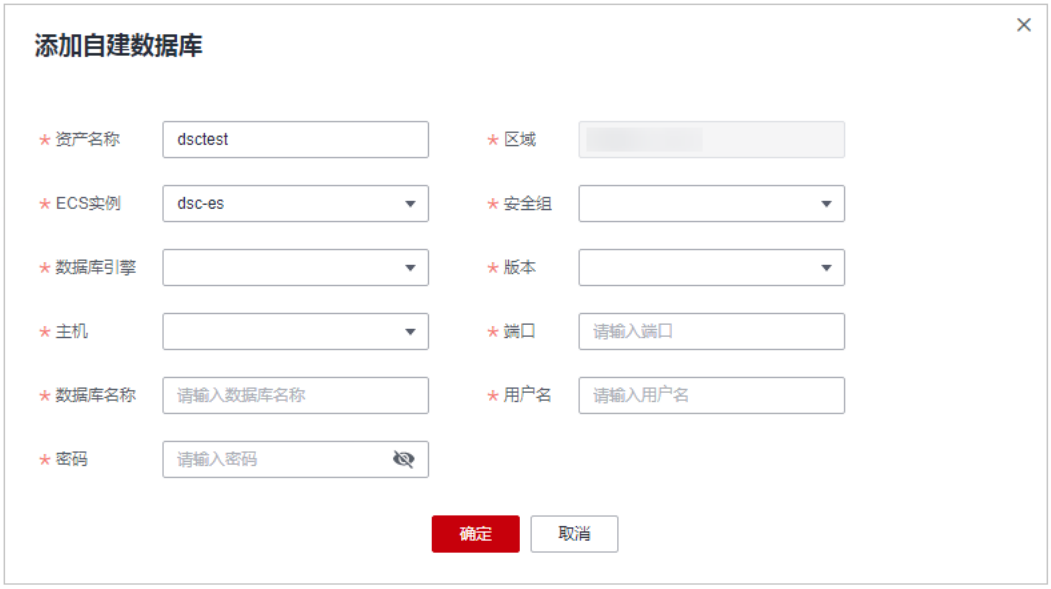


表 3-7 添加自建数据库参数说明

参数名称	参数说明	取值样例
资产名称	输入数据库对象名称。	-
区域	默认为当前帐号登录的区域。	-
ECS实例	在下拉框中选择已在ECS服务里创建的数据库实例。	--
安全组	选择对应的ECS实例所在的安全组名称。	default
数据库引擎	选择数据库引擎。可选择“MySQL”、“PostgreSQL”、“SQLServer”和“Oracle”。	MySQL
版本	选择数据库引擎对应的版本。	5.6
主机	输入数据库服务器IP地址。	-
端口	输入数据库服务器的端口号。	-

参数名称	参数说明	取值样例
数据库名称	输入自建数据库名称。	-
用户名	输入访问数据库服务器的用户名。	-
密码	输入访问数据库服务器的密码。	-

步骤7 单击“确定”，数据库添加完成。

图 3-18 连通性测试

数据库添加完成后，该数据库的“连通性”为“检查中”，此时，DSC会测试数据库的连通性。

- DSC能正常访问已添加的数据库，该数据库的“连通性”状态为“成功”。
- 若DSC不能正常访问已添加的数据库，该数据库的“连通性”状态为“失败”。单击“原因”查看失败的原因。

----结束

相关操作

- 数据库资产授权/停止授权，请参见**云资源委托授权/停止授权**章节。
- 编辑数据库资产，请参见**编辑数据库信息**章节。
- 删除数据库资产，请参见**删除数据库资产**章节。

3.4.4 编辑数据库信息

如果已添加的数据库服务器的用户名和密码已修改或者访问数据库的用户名和密码配置有误，您可以参考本章节进行重新配置。

前提条件

- 已完成数据库资产委托授权，参考**云资源委托授权/停止授权**进行操作。
- 已添加数据库资产。

操作步骤

步骤1 登录管理控制台。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全 > 数据安全中心”，进入数据安全中心总览界面。

步骤4 在左侧导航树中选择“资产列表”，并选择“数据库 > 已授权”，进入已授权数据库资产列表页面。

图 3-19 已授权数据库资产列表

步骤5 在需要编辑的数据库资产所在行的“操作”列，单击“编辑”。

步骤6 在系统弹出编辑数据库对话框中，修改数据库服务器的用户名或密码。

步骤7 修改后，单击“确定”。

修改完成后，该数据库的“连通性”为“检查中”，此时，DSC会测试数据库的连通性，即测试DSC是否能够通过您配置的用户名和密码正常访问添加的数据库。

- DSC能正常访问已添加的数据库，该数据库的“连通性”状态为“成功”。
- 若DSC不能正常访问已添加的数据库，该数据库的“连通性”状态为“失败”。单击“原因”查看失败的原因。

----结束

3.4.5 删除数据库资产

本章节介绍如何对已添加的数据库资产进行删除。删除后，该资产在DSC服务里建立的相关任务模板以及扫描任务结果报告都将被删除，且无法恢复。

前提条件

- 已完成数据库资产委托授权，参考**云资源委托授权/停止授权**进行操作。
- 待删除的数据库资产未被应用在敏感数据检测任务中。

约束条件

- 如果需要删除的数据库资产已被应用在敏感数据检测任务中，请先解绑资产或者删除任务，再参照本章节删除资产。
- 删除操作无法恢复，删除后，资产相关的任务模板、任务结果、报表都将被删除，请谨慎操作。

操作步骤

步骤1 登录管理控制台。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全 > 数据安全中心”，进入数据安全中心总览界面。

步骤4 在左侧导航树中选择“资产列表”，并选择“数据库 > 已授权”，进入已授权数据库资产列表页面。

图 3-20 已授权数据库资产列表

步骤5 在数据库资产列表中，在需要删除的数据库资产所在行的“操作”列，单击“删除”。

步骤6 在弹出删除资产提示框中，单击“确定”。

----结束

3.5 大数据资产列表

3.5.1 添加大数据源资产

如果您需要添加云搜索服务（CSS）、数据湖探索（DLI）和Hive的资产，可参考本章节进行操作。

前提条件

- 已完成大数据资产委托授权，参考**云资源委托授权/停止授权**进行操作。
- 已开通CSS和DLI服务，且CSS和DLI中已有资产，且对应子网下含有可用的IP配额。

操作步骤

步骤1 登录管理控制台。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全 > 数据安全中心”，进入数据安全中心总览界面。

步骤4 在左侧导航树中选择“资产列表”，并选择“大数据”页签，进入大数据资产列表页面。

图 3-21 进入大数据资产列表入口

步骤5 在大数据资产列表左上角，单击“添加大数据源”。

步骤6 在弹出的“添加大数据源”对话框中，参考**表3-8**配置大数据源参数。

图 3-22 添加大数据源

表 3-8 添加大数据源参数说明

参数名称	参数说明	取值样例
资产名称	自定义参数。	--
区域	默认为当前帐号登录的区域。	-
大数据类型	选择大数据类型。 • “Elasticsearch”，选择此类型时，其他参数说明请参见**表3-9**。 • “DLI”，选择此类型时，其他参数说明请参见**表3-10**。 • “Hive”，选择此类型时，其他参数说明请参见**表3-11**。	Elasticsearch

表 3-9 “Elasticsearch”参数说明

参数名称	参数说明	取值样例
ES实例	在下拉框中选择ES实例。	--
版本	选择大数据类型对应的版本。	5.x
主机	大数据源服务器IP地址。	192.168.0.233
端口	大数据源服务器的端口号。	3306
索引	输入大数据源对应的index。	--
用户名	输入访问大数据服务器的用户名。	--
密码	输入访问大数据服务器的密码。	--

表 3-10 “DLI”参数说明

参数名称	参数说明	取值样例
队列	在下拉框中选择DLI中数据源的队列名称。	default
DLI数据库	选择DLI中目标队列下的数据库名称。	5.x

表 3-11 “Hive”参数说明

参数名称	参数说明	取值样例
虚拟私有云	在下拉框中选择虚拟私有云。	--
子网	选择虚拟私有云对应的子网名称。	--
安全组	在下拉框中选择可用的安全组。	--
主机	大数据源服务器IP地址。	192.168.0.233
端口	大数据源服务器的端口号。	3306
数据库名称	输入数据库名称。	--

步骤7 单击“确定”，大数据源资产添加完成。

大数据资产添加完成后，该大数据源的“连通性”为“检查中”，此时，DSC会测试数据源的连通性，即测试DSC是否能够通过您配置的用户名和密码正常访问添加的大数据源。

- DSC能正常访问已添加的大数据源，该大数据源的“连通性”状态为“成功”。
- 若DSC不能正常访问已添加的大数据源，该大数据源的“连通性”状态为“失败”。单击“原因”查看失败的原因并重新正确填写访问目标大数据源的用户名和密码。

----结束

3.5.2 添加自建大数据源

本章节将介绍如何添加自建大数据源资产。

前提条件

- 已完成大数据资产委托授权，参考**云资源委托授权/停止授权**进行操作。
- 已获取其他自建大数据源的类型、版本、主机、索引等相关信息，且自建大数据源子网下含有可用的IP配额。

操作步骤

步骤1 登录管理控制台。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全 > 数据安全中心”，进入数据安全中心总览界面。

步骤4 在左侧导航树中选择“资产列表”，并选择“大数据”页签，进入大数据资产列表页面。

图 3-23 进入大数据资产列表入口

步骤5 在大数据资产列表左上角，单击“添加自建大数据源”。

步骤6 在弹出“添加自建大数据源”对话框中，参照表3-12配置大数据源参数。

图 3-24 添加自建大数据源

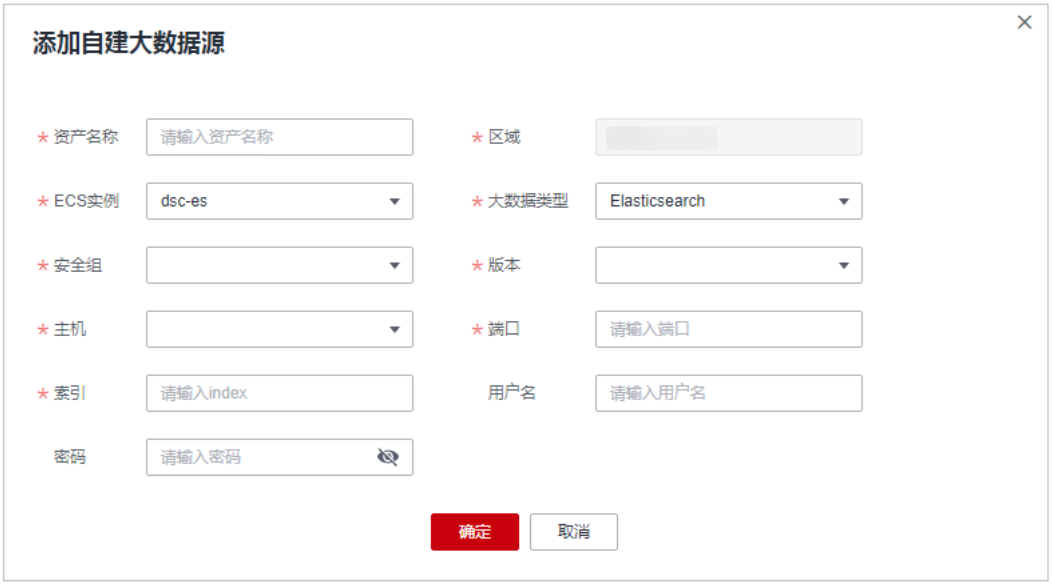


表 3-12 添加自建大数据源参数说明

参数名称	参数说明	取值样例
资产名称	自定义参数。	--
区域	默认为当前帐号登录的区域。	-
ECS实例	选择ECS里的“Elasticsearch”类型的实例。	--
大数据类型	选择大数据类型。目前仅支持“Elasticsearch”。	Elasticsearch
安全组	在下拉框中选择已有的安全组。	default
版本	选择大数据库类型对应的版本。	5.x
主机	输入大数据源服务器IP地址。	192.168.0.233
端口	输入大数据源服务器的端口号。	3306
索引	输入大数据源对应的index。	--
用户名	输入访问大数据服务器的用户名。	--

参数名称	参数说明	取值样例
密码	输入访问大数据服务器的密码。	--

步骤7 单击“确定”，大数据源资产添加完成。

大数据资产添加完成后，该大数据源的“连通性”为“检查中”，此时，DSC会测试数据源的连通性，即测试DSC是否能够通过您配置的用户名和密码正常访问添加的大数据源。

- DSC能正常访问已添加的大数据源，该大数据源的“连通性”状态为“成功”。
- 若DSC不能正常访问已添加的大数据源，该大数据源的“连通性”状态为“失败”。单击“原因”查看失败的原因并重新正确填写访问目标大数据源的用户名和密码。

----结束

3.5.3 编辑大数据源资产

如果已添加的大数据源服务器的用户名和密码已修改或者访问数据源的用户名和密码配置有误，您可以参考本章节进行重新配置。

前提条件

- 已完成大数据资产委托授权，参考**云资源委托授权/停止授权**进行操作。
- 已添加大数据源资产。

操作步骤

步骤1 登录管理控制台。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全 > 数据安全中心”，进入数据安全中心总览界面。

步骤4 在左侧导航树中选择“资产列表”，并选择“大数据”页签，进入大数据资产列表页面。

图 3-25 进入大数据资产列表入口

步骤5 在需要编辑的大数据资产所在行的“操作”列，单击“编辑”。

步骤6 在系统弹出编辑数据库对话框中，修改访问大数据源的用户名或密码。

步骤7 修改后，单击“确定”。

修改完成后，该大数据源的“连通性”为“检查中”，此时，DSC会测试数据源的连通性，即测试DSC是否能够通过您配置的用户名和密码正常访问添加的大数据源。

- DSC能正常访问已添加的大数据源，该大数据源的“连通性”状态为“成功”。
- 若DSC不能正常访问已添加的大数据源，该大数据源的“连通性”状态为“失败”。单击“原因”查看失败的原因并重新正确填写访问目标大数据源的用户名和密码。

----结束

3.5.4 删除大数据源资产

本章节介绍如何对已添加的大数据源资产进行删除的操作。删除后，该资产在DSC服务里建立的相关任务模板以及扫描任务结果报告都将被删除，且无法恢复。

前提条件

- 已完成大数据资产委托授权，参考**云资源委托授权/停止授权**进行操作。
- 待删除的大数据源资产未被应用在敏感数据检测任务中。

约束条件

- 如果需要删除的大数据源资产已被应用在敏感数据检测任务中，请先解绑资产或者删除任务，再参照本章节删除资产。
- 删除操作无法恢复，删除后，资产相关的任务模板、任务结果、报表都将被删除，请谨慎操作。

操作步骤

步骤1 登录管理控制台。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全 > 数据安全中心”，进入数据安全中心总览界面。

步骤4 在左侧导航树中选择“资产列表”，并选择“大数据”页签，进入大数据资产列表页面。

图 3-26 进入大数据资产列表入口

步骤5 在需要编辑的大数据资产所在行的“操作”列，单击“删除”。

步骤6 在弹出的删除资产提示框中，单击“确定”。

----结束

3.6 MRS 资产列表

3.6.1 添加 MRS 资产

如果您已经完成MRS资产委托授权，可参考本章节对MRS创建的Hive数据进行相关操作的授权。

前提条件

- 已完成MRS资产委托授权，参考**云资源委托授权/停止授权**进行操作。

操作步骤

步骤1 登录管理控制台。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全 > 数据安全中心”，进入数据安全中心总览界面。

步骤4 在左侧导航树中选择“资产列表”，并选择“MRS > 待授权”，进入待授权MRS资产列表页面。

图 3-27 待授权 MRS 资产列表

步骤5 在需要授权的MRS资产所在行的“操作”列，单击“授权”。

步骤6 在弹出的“MRS授权”对话框中，参考**表3-13**配置数据库参数。

图 3-28 MRS 授权

表 3-13 参数说明

参数名称	参数说明
资产名称	用户自定义的MRS实例的名称。
数据库名称	和MRS实例中的数据库名称保持一致。
用户名	输入访问数据库服务器的用户名，与MRS里创建的保持一致。
密码	输入访问数据库服务器的密码，与MRS里创建的保持一致。

步骤7 单击“确定”，数据库添加完成，并展示在已授权的MRS资产列表中。

----结束

3.6.2 删除 MRS 资产

本章节介绍如何对已添加的MRS资产进行删除的操作。删除后，该资产在DSC服务里建立的相关任务模板以及扫描任务结果报告都将被删除，且无法恢复。

前提条件

- 已完成MRS资产委托授权，参考**云资源委托授权/停止授权**进行操作。
- 待删除的数据资产未被应用在敏感数据检测任务中。

约束条件

- 如果需要删除的数据资产已被应用在敏感数据检测任务中，请先解绑资产或者删除任务，再参照本章节删除资产。
- 删除操作无法恢复，删除后，资产相关的任务模板、任务结果、报表都将被删除，请谨慎操作。

操作步骤

步骤1 登录管理控制台。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全 > 数据安全中心”，进入数据安全中心总览界面。

步骤4 在左侧导航树中选择“资产列表”，并选择“MRS > 待授权”，进入待授权MRS资产列表页面。

图 3-29 待授权 MRS 资产列表

步骤5 在MRS资产列表中，在需要删除的MRS资产所在行的“操作”列，单击“删除”。

图 3-30 删除资产

步骤6 在弹出的删除资产提示框中，单击“确定”。

----结束

4 数据安全概览

总览页面分为云服务全景图（资产地图）、数据采集安全、数据传输/存储安全、数据使用安全和数据交换/删除安全共五大板块，实时呈现了用户资产的具体情况。

前提条件

- 已完成资产访问的授权。
- 已添加资产。

操作步骤

步骤1 登录管理控制台。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击 ，选择“安全 > 数据安全中心”，进入数据安全中心总览界面。

步骤4 查看数据安全中心服务的总览—云服务全景图。

提供数据资产地图，帮助客户建立数据资产的全景视图，可视化呈现数据资产分布、数据敏感程度、当前的风险级别。

- **梳理云上数据资产**：自动扫描并梳理云上数据资产，地图化展示资产分布，帮助用户解决数据在哪里的问题。
- **敏感数据展示**：基于DSC的三层数据识别引擎、预置合规规则、自然语义识别技术、文件相似度检测技术，对数据资产进行分类分级。
  - 对数据资产按照“风险VPC数”、“风险安全组数”、“风险主机数”、“风险RDS数”、“风险OBS数”进行分类展示。
  - 每类资产按照“高危”、“中危”、“低危”、“未识别风险”对敏感数据进行分级定位。
- **风险监控和预警**：基于风险识别引擎，对数据资产进行风险监控，展示每类资产的风险分布，并预警。

图 4-1 云服务全景图

说明

- 将鼠标移动到数据资产图标处，可查看资产相关信息。
- 单击数据资产图标，在界面的右侧弹框中可详细查看该资产的“基本信息”、“风险信息”或者“风险安全组规则”等信息。

步骤5 查看数据安全中心服务的总览—数据采集安全，如图4-2所示。

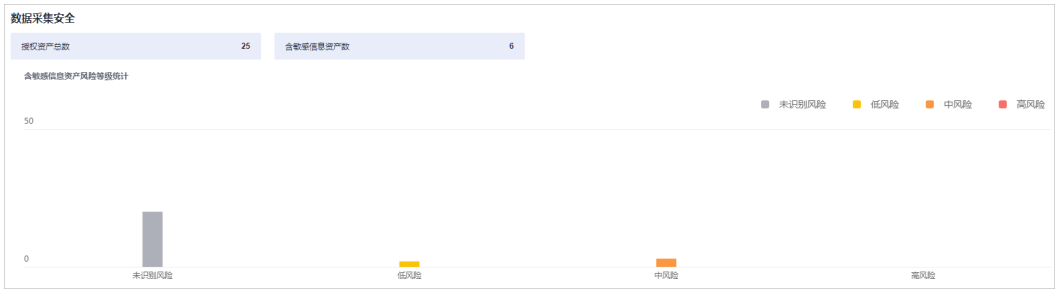
DSC根据敏感数据规则对敏感数据进行识别和敏感等级分类，您可以在总览页面查看您资产中不同风险等级的数据的分布情况。

基于敏感字段在文件中出现的累计次数和敏感字段关联组来判断文件的敏感性，并根据文件的敏感程度将其划分为四个等级：“未识别风险”、“低风险”、“中风险”和“高风险”。风险等级依次递增。具体风险等级情况说明：

- 未识别风险：0级
- 低风险：1~3级
- 中风险：4~7级
- 高风险：8~10级

在柱状图中，不同高度代表该风险等级的资产数量。将鼠标箭头放置在柱状图上，可查看该风险等级的资产数量。

图 4-2 数据采集安全



步骤6 查看数据安全中心服务的总览—数据传输/存储安全，如图4-3所示。

图 4-3 数据传输/存储安全

- 数据传输安全：DSC统计了以下可能存在传输安全的项，您可以直接单击具体项的名称，查看详细情况。
  - VPN连接数：您的资产中存在已创建的虚拟专用网络，具体的请参考《VPN服务用户指南》。
  - 云专线连接数：您的资产中存在已创建的云专线物理连接，具体的请参考《云专线用户指南》。
  - ELB未采用加密通信的监听器：添加监听器时，未使用加密通信HTTPS协议的监听器数量的统计，建议您采用HTTS协议进行加密通信。
  - SSL证书订阅：您的资产中存在已购买或者已上传的证书数量，了解SSL证书请参考《SSL证书管理用户指南》。
  - WAF未采用加密通信的域名：WAF中添加域名时，未使用加密传输HTTPS协议的域名数量的统计，建议您采用HTTPS协议进行加密通信。
- 数据存储安全：该模块为您罗列了存在未加密的对象桶，为了防止您的资产存在不必要的存储安全，建议您单击对象桶名称，前往OBS界面，对未加密的对象桶进行加密。

步骤7 查看数据安全中心服务的总览—数据使用安全，如图4-4所示。

该模块统计了“近30分钟”、“近3小时”、“近24小时”、“近7天”、“近30天”内的数据使用安全信息。

- 未处理异常事件：按“数据访问异常”、“数据操作异常”、“数据管理异常”所占比例进行展示。同时，展示了异常事件总数、违例确认总数和违例排除总数。
  - 单击“未处理异常事件”中的其中一个颜色区域，可查看指定数据异常占比。
  - 当不需要展示某种类型的异常事件时，单击事件分布图右侧攻击类型对应的颜色方块，取消在事件分布圆环中的展示。
- Top5访问源IP：前5的访问源IP的统计。
- Top5被访问高风险对象：被访问的对象中，排在前5的高风险对象。
- Top5访问帐号：前5的访问帐号的统计。

图 4-4 数据使用安全

步骤8 查看数据安全中心服务的总览—数据交换/删除安全，如图4-5所示。

图 4-5 数据交换/删除安全

- 数据交换安全：展示了已创建的“静态脱敏任务数”以及“水印API调用次数”，如何创建数据脱敏任务请参考**创建数据脱敏任务**。
- 数据删除安全：DSC为您统计了数据库、ECS、OBS资产的当日删除数和总删除数。

----结束

5 敏感数据识别

5.1 敏感数据规则

5.1.1 新增敏感数据规则

定义敏感数据识别规则组操作将多个零散的规则组合成为一个有业务逻辑的规则组，该操作是用户后续进行敏感数据发现任务操作的前提 。

约束条件

敏感数据规则分为自定义的规则和内置的规则，内置的规则不可新增、编辑和删除。

操作步骤

步骤1 登录管理控制台。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击 ，选择“安全 > 数据安全中心”，进入数据安全中心总览界面。

步骤4 在左侧导航树中，选择“敏感数据识别 > 识别规则”，进入敏感数据规则列表。

图 5-1 规则列表

步骤5 在规则列表的左上角，单击“新增规则”，进入“新增规则”页面。

步骤6 在“新增规则”对话框中配置规则基本信息，相关参数说明如表5-1所示。

图 5-2 新增敏感数据规则

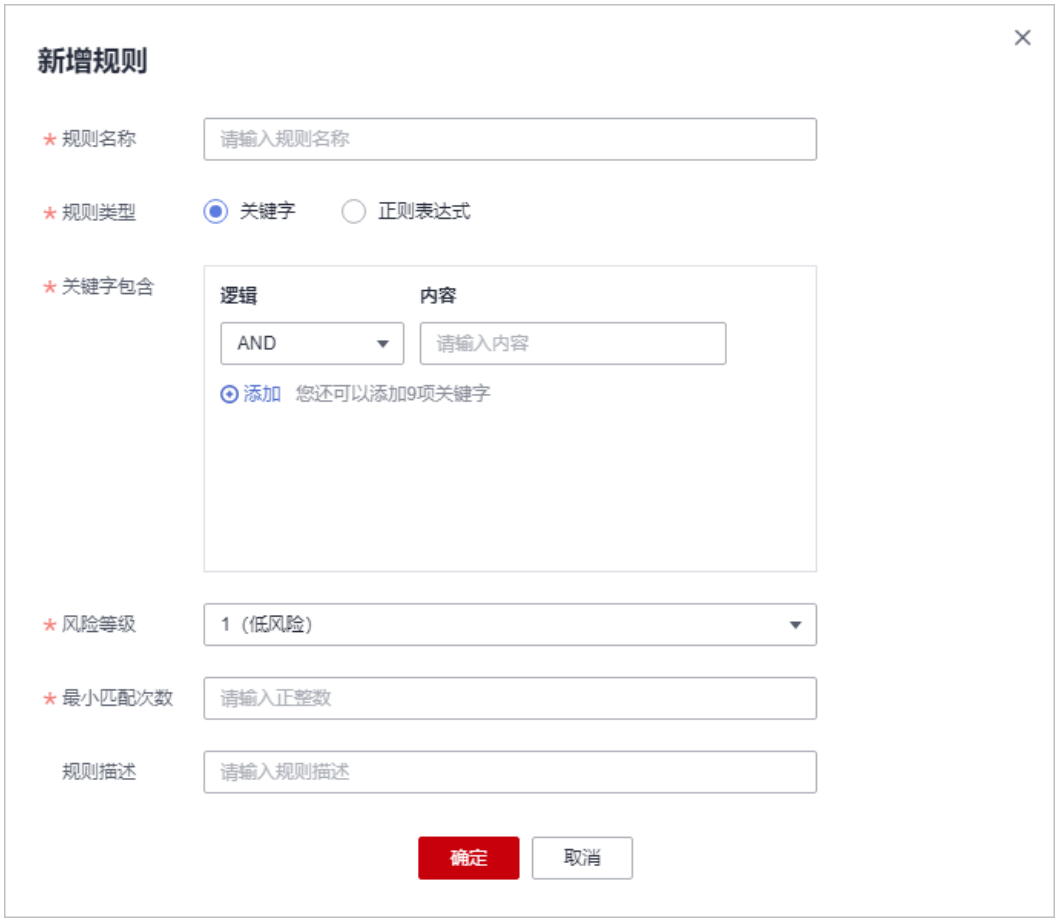


表 5-1 敏感规则参数说明

参数	参数说明	取值样例
规则名称	您可以自定义敏感数据规则名称。 规则名称需要满足以下要求： ● 1~255个字符。 ● 字符可由中文、英文字母、数字、下划线或中划线组成。 ● 规则名称不能与已有的规则名称重复。	-
规则类型	可选择“关键字”和“正则表达式”。 ● 关键字：通过关键字来执行该条敏感规则。 ● 正则表达式：用于指定和识别文本字符串（如特定字符，单词或字符模式）的一种简洁而灵活的方式。	关键字

参数	参数说明	取值样例
关键字包含	“规则类型”设置为“关键字”时，显示该参数。 ● 逻辑：需要选择关键字的逻辑： – AND：关键字都需要包含。 – OR：仅需要包含其中一个关键字。 ● 内容：输入关键字。单击 添加 可添加关键字，最多可添加10项关键字。	and，张三
正则表达式	“规则类型”设置为“正则表达式”时，显示该参数。	-
风险等级	选择该条规则的风险等级。 风险等级分为1~10级。1~3级属于低风险，4~7级属于中风险，8~10级属于高风险。	5（中风险）
最小匹配次数	规则命中次数。同一个规则达到命中次数，则被标记为敏感信息。	2
规则描述	可选参数。该规则的备注信息，用于区别其他规则。	-

步骤7 单击“确定”，完成敏感数据规则的创建。

----结束

5.1.2 查看敏感数据规则列表

本章节介绍如何查看敏感数据规则。

前提条件

已添加敏感数据规则。

操作步骤

步骤1 登录管理控制台。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全 > 数据安全中心”，进入数据安全中心总览界面。

步骤4 在左侧导航树中，选择“敏感数据识别 > 识别规则”，进入敏感数据规则列表，参数说明如表5-2所示。

图 5-3 规则列表

说明

- 在“全部规则类型”、“全部风险等级”搜索栏选择敏感规则的类型、等级，敏感数据规则列表界面将只显示对应状态的规则。
- 输入规则名称或规则名称的关键字，单击 或按“Enter”，可以搜索指定的敏感数据规则。

表 5-2 规则参数说明

参数名称	参数说明
规则名称	敏感数据规则的名称。
规则类型	规则类型说明如下： ● 关键字：通过关键字来执行敏感规则。 ● 正则表达式：通过正则表达式来执行敏感规则。
风险等级	敏感数据规则的风险等级。 风险等级分为1~10级。1~3级属于低风险，4~7级属于中风险，8~10级属于高风险。
规则描述	该规则的备注信息。

----结束

5.1.3 编辑敏感数据规则

敏感数据规则创建完成后，可根据需要编辑规则，对规则组的名称、类型、描述等进行修改。

前提条件

已添加敏感数据规则。

约束条件

DSC内置的敏感数据规则不可编辑。

操作步骤

步骤1 登录管理控制台。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击 ☰，选择“安全 > 数据安全中心”，进入数据安全中心总览界面。

步骤4 在左侧导航树中，选择“敏感数据识别 > 识别规则”，进入敏感数据规则列表。

图 5-4 规则列表

步骤5 在敏感数据规则列表中，在需要编辑的规则所在行的“操作”列，单击“编辑”，系统弹出“编辑规则”的对话框。

步骤6 在“编辑规则”对话框中，根据您的需求，编辑规则参数，相关参数说明如表5-3所示

图 5-5 编辑敏感数据规则

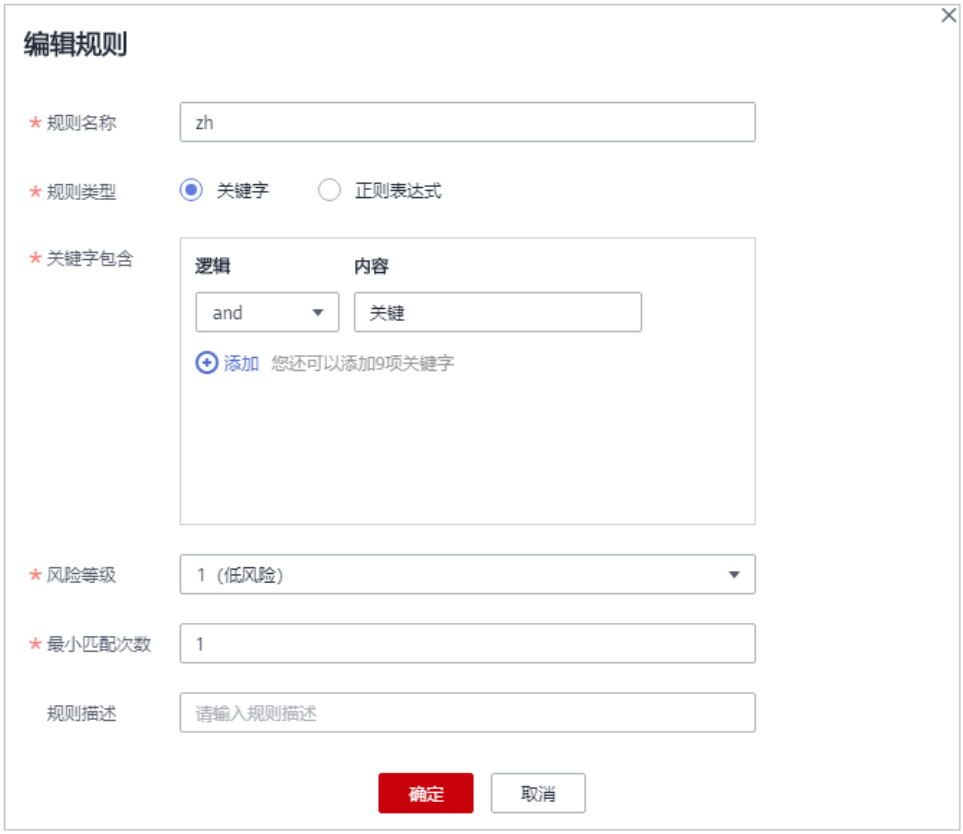


表 5-3 敏感规则参数说明

参数	参数说明	取值样例
规则名称	您可以自定义敏感数据规则名称。 规则名称需要满足以下要求： ● 1~255个字符。 ● 字符可由中文、英文字母、数字、下划线或中划线组成。 ● 规则名称不能与已有的规则名称重复。	-
规则类型	可选择“关键字”和“正则表达式”。 ● 关键字：通过关键字来执行该条敏感规则。 ● 正则表达式：用于指定和识别文本字符串（如特定字符，单词或字符模式）的一种简洁而灵活的方式。	关键字
关键字包含	“规则类型”设置为“关键字”时，显示该参数。 ● 逻辑：需要选择关键字的逻辑： – AND：关键字都需要包含。 – OR：仅需要包含其中一个关键字。 ● 内容：输入关键字。单击 添加 可添加关键字，最多可添加10项关键字。	and，张三
正则表达式	“规则类型”设置为“正则表达式”时，显示该参数。	-
风险等级	选择该条规则的风险等级。 风险等级分为1~10级。1~3级属于低风险，4~7级属于中风险，8~10级属于高风险。	5（中风险）
最小匹配次数	规则命中次数。同一个规则达到命中次数，则被标记为敏感信息。	2
规则描述	可选参数。该规则的备注信息，用于区别其他规则。	-

步骤7 单击“确定”，完成敏感数据规则的编辑。

----结束

5.1.4 删除敏感数据规则

不再使用的自定义敏感数据规则，可在DSC的敏感数据规则列表中删除。

- 已添加到敏感数据规则组中的规则，不可删除。
- DSC内置规则不可删除。

前提条件

- 已添加敏感数据规则。
- 待删除的规则未添加到规则组。

约束条件

- DSC内置的规则不可删除。
- 如果待删除的规则已在敏感数据规则组中使用，您需要先参考**编辑敏感数据规则组**章节将待删除的规则移出规则组，然后参考本章节删除该规则。
- 规则删除后将无法恢复，请谨慎操作。

操作步骤

步骤1 登录管理控制台。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全 > 数据安全中心”，进入数据安全中心总览界面。

步骤4 在左侧导航树中，选择“敏感数据识别 > 识别规则”，进入敏感数据规则列表。

图 5-6 规则列表

步骤5 在敏感数据规则列表中，在需要删除的规则所在行的“操作”列，单击“删除”。

步骤6 在弹出的删除规则的提示框中，单击“确定”。

----结束

5.1.5 添加敏感数据规则到组

本章节介绍如何将规则添加到敏感数据规则组。创建敏感数据识别任务时，可根据用户场景选择规则组。

前提条件

- 已添加敏感数据规则。
- 已有敏感数据规则组。

操作步骤

步骤1 登录管理控制台。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全 > 数据安全中心”，进入数据安全中心总览界面。

步骤4 在左侧导航树中，选择“敏感数据识别 > 识别规则”，进入敏感数据规则列表。

图 5-7 规则列表

步骤5 在目标规则所在行的“操作”列，单击“添加到组”，进入“添加到组”页面。

步骤6 在“添加到组”的对话框中，选择敏感数据规则组。

图 5-8 添加到组

步骤7 单击“确定”。

----结束

5.2 敏感数据规则组

5.2.1 新增敏感数据规则组

如果DSC内置的规则组不能满足您的敏感数据识别场景，可参考本章节自定义敏感数据规则组，自由组合规则，实现敏感数据的多场景识别。

约束条件

敏感数据规则组分为自定义的规则组和内置的规则组，内置的规则组不可新增、编辑和删除。

操作步骤

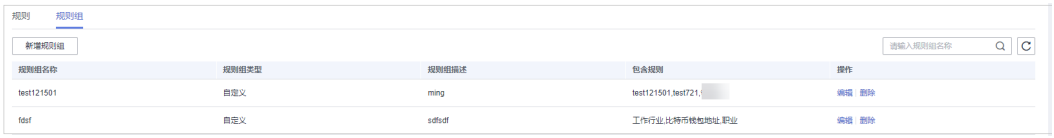
步骤1 登录管理控制台。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全 > 数据安全中心”，进入数据安全中心总览界面。

步骤4 在左侧导航树中，选择“敏感数据识别 > 识别规则”，并选择“规则组”页签，进入规则组列表。

图 5-9 敏感数据规则组



步骤5 在规则组列表的左上角，单击“新增规则组”，弹出新增规则组对话框。

步骤6 在“新增规则组”对话框中配置规则组基本信息，相关参数说明如表5-4所示。

图 5-10 新增规则组

表 5-4 敏感数据规则组参数说明

参数	参数说明
规则组名称	您可以自定义敏感数据规则组名称。 规则组名称需要满足以下要求： ● 1~255个字符。 ● 字符可由中文、英文字母、数字、下划线或中划线组成。 ● 规则组名称不能与已有的规则组名称重复。
规则组描述	该规则组的备注信息，用于区别其他规则组。

参数	参数说明
规则添加	可选参数。勾选需要添加的敏感数据规则。 如果您想移除已选的规则，可在右边已选择的规则框中，找到目标规则，并在其所在行的“操作”列，单击 ×移除。

步骤7 单击“确定”，完成敏感数据规则组的创建。

----结束

5.2.2 查看敏感数据规则组列表

本章节介绍如何查看敏感数据规则组的详细信息。

前提条件

已添加敏感数据规则组。

操作步骤

步骤1 登录管理控制台。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全 > 数据安全中心”，进入数据安全中心总览界面。

步骤4 在左侧导航树中，选择“敏感数据识别 > 识别规则”，并选择“规则组”页签，进入规则组列表规则组参数说明如表5-5所示。

图 5-11 敏感数据规则组

说明

输入规则组名称或规则名称的关键字，单击或按“Enter”，可以搜索指定的敏感数据规则组。

表 5-5 规则组参数说明

参数名称	参数说明
规则组名称	敏感数据规则组的名称。

参数名称	参数说明
规则组类型	规则组类型说明如下： ● 自定义：用户自行创建的规则组。 ● 默认：DSC内置的规则组。
规则组描述	该规则组的备注信息。
包含规则	规则组所包含的规则。
操作	用户可以在操作栏中，执行以下操作： ● 单击“编辑”，修改敏感数据规则组的相关信息，具体操作请参见**编辑敏感数据规则组**。 ● 单击“删除”，删除自定义的敏感数据规则组，具体操作请参见**删除敏感数据规则组**。

----结束

5.2.3 编辑敏感数据规则组

本章节介绍如何编辑敏感数据规则组，可执行以下操作：

- 修改“则组名称”以及“规则组描述”。
- 添加敏感数据规则。
- 移除敏感数据规则。

前提条件

- 已添加敏感数据规则组。
- 敏感数据规则组的“规则组类型”为“自定义”。

约束条件

DSC内置的敏感数据规则组不可编辑。

操作步骤

步骤1 登录管理控制台。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全 > 数据安全中心”，进入数据安全中心总览界面。

步骤4 在左侧导航树中，选择“敏感数据识别 > 识别规则”，并选择“规则组”页签，进入规则组列表。

图 5-12 敏感数据规则组

步骤5 在目标敏感规则组所在行的“操作”列，单击“编辑”，系统弹出编辑规则组的对话框。

步骤6 在“编辑规则组”对话框中编辑规则组参数，相关参数说明如表5-6所示

图 5-13 编辑敏感数据规则组

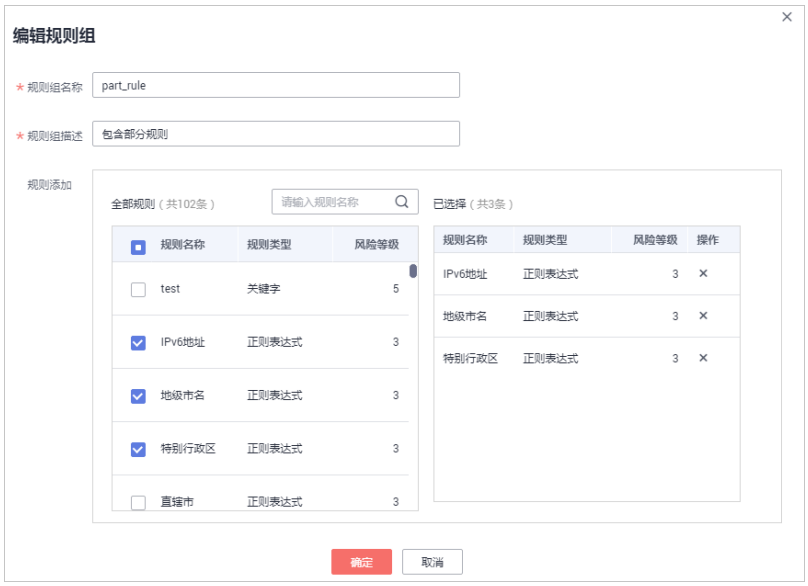


表 5-6 敏感数据规则组参数说明

参数	参数说明
规则组名称	您可以自定义敏感数据规则组名称。 规则组名称需要满足以下要求： ● 1~255个字符。 ● 字符可由中文、英文字母、数字、下划线或中划线组成。 ● 规则组名称不能与已有的规则组名称重复。
规则组描述	该规则组的备注信息，用于区别其他规则组。
规则添加	可选参数。勾选需要添加的敏感数据规则。 如果您想移除已选的规则，可在右边已选择的规则框中，找到目标规则，并在其所在行的“操作”列，单击✕移除。

步骤7 单击“确定”，完成规则组的编辑。

----结束

5.2.4 删除敏感数据规则组

不再使用的自定义敏感数据规则组，可在DSC敏感数据规则组列表中进行删除。

- 不可删除已在识别任务中使用的规则组。

- DSC内置的规则组不可删除。

前提条件

已添加敏感数据规则组。

约束条件

- DSC内置的规则组不可删除。
- 如果待删除的规则组已在识别任务中使用，您需要先删除包含该规则组的敏感数据任务，再参照本章节删除该规则组。
- 规则组删除后将无法恢复，请谨慎操作。

操作步骤

步骤1 登录管理控制台。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全 > 数据安全中心”，进入数据安全中心总览界面。

步骤4 在左侧导航树中，选择“敏感数据识别 > 识别规则”，并选择“规则组”页签，进入规则组列表。

图 5-14 敏感数据规则组

步骤5 在目标敏感规则组所在行的“操作”列，单击“删除”。

步骤6 在弹出的提示框中，单击“确定”。

----结束

5.3 敏感数据识别任务

5.3.1 创建敏感数据识别任务

数据安全中心会根据创建的识别任务，在选定的OBS桶、数据库、大数据或者MRS的指定范围中，自动识别敏感数据并生成识别数据和结果。本章节介绍如何创建敏感数据识别任务。

创建任务时，选择多个场景的规则组，实现为同一资产配置多场景的扫描任务。

前提条件

- 已添加OBS、数据库或大数据源资产，具体操作请参见**资产列表**。

- 已创建敏感数据规则组，具体操作请参见**新增敏感数据规则组**。

操作步骤

步骤1 登录管理控制台。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全 > 数据安全中心”，进入数据安全中心总览界面。

步骤4 在左侧导航树中，选择“敏感数据识别 > 识别任务”，进入“识别任务”页面。

图 5-15 识别任务

步骤5 在敏感数据任务列表的左上角，单击“新建任务”。

步骤6 在弹出的“新建任务”对话框中，配置任务基本信息，相关参数说明如**表5-7**所示。

图 5-16 新建敏感数据识别任务

表 5-7 敏感数据识别任务参数说明

参数	参数说明	取值样例
开启任务	是否开启敏感数据识别任务，系统默认开启任务。 ●  ：开启状态。 ●  ：关闭状态。	
任务名称	您可以自定义敏感数据识别任务名称。 任务名称需要满足以下要求： ● 1~255个字符。 ● 字符可由中文、英文字母、数字、下划线或中划线组成。 ● 任务名称不能与已有的任务名称重复。	-
数据类型	选择识别的数据类型。可多选。 ● OBS，添加OBS资产，参考**添加OBS资产**章节。 ● 数据库，添加云数据库资产，参考**添加云数据库**章节。 ● 大数据，添加大数据源资产，参考**添加大数据源资产**章节。 ● MRS，添加Hive资产，参考**添加MRS资产**。	数据库
识别规则组	选择识别任务需要使用的规则组，可多选。可参考**新增敏感数据规则组**章节创建规则组。	-
识别模式	选择检测任务的扫描模式： ● 快速识别：根据规则组进行扫描，实现数据分布快速识别。 ● 全量识别：在规则组的基础上加入自然语义处理NLP能力，扫描速度相对较慢，识别率更高。	快速扫描
识别周期	选择任务的识别周期： ● 单次：根据设置的执行计划，在设定的时间执行一次该识别任务。 ● 每天：选择该选项，需要设置“启动时间”，即在每天的固定时间执行该识别任务。 ● 每周：选择该选项，需要设置“启动时间”，即在设定的时间以及每周这一时间点执行该识别任务。 ● 每月：选择该选项，需要设置“启动时间”，即在设定的时间以及每月这一时间点执行该识别任务。	单次

参数	参数说明	取值样例
执行计划	“扫描周期”选择“单次”时，显示该参数。 • 立即执行：选择该选项，保存后，可以在当前立即执行一次该识别任务。 • 定时启动：在指定时间执行一次该识别任务。	立即执行
启动时间	“扫描周期”选择“每天”、“每周”、“每月”时，显示该参数。 设置识别任务的具体启动时间。设置后，会在指定时间以及每天或者每周或者每月的该时间点执行一次识别任务。	-
通知主题	单击下拉列表选择已创建消息通知主题或者单击“查看通知主题”创建新的主题，用于配置接收告警通知的终端。 告警通知的具体操作请参见**告警通知**。	--

步骤7 单击“确定”，完成敏感数据识别任务的创建。

----结束

5.3.2 查看敏感数据任务列表

在敏感数据任务列表中，可查看敏感数据识别任务的详细信息。

前提条件

已完成识别任务的创建。

操作步骤

步骤1 登录管理控制台。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全 > 数据安全中心”，进入数据安全中心总览界面。

步骤4 在左侧导航树中，选择“敏感数据识别 > 识别任务”，进入“识别任务”页面，查看识别任务的详细信息，检测任务参数说明如**表5-8**所示。

说明

- 输入任务名称或任务名称的关键字，单击或按“Enter”，可以搜索指定的敏感数据识别任务。
- 单击任务名称，可以查看检测任务报告。
- 在目标任务的“操作”列，单击“更多 > 下载风险结果”，下载风险结果报表，DSC为您提供了Excel格式的风险结果报表。

表 5-8 检测任务参数说明

参数名称	参数说明
任务名称	识别任务的名称。 ● 单击任务名称前方的，查看任务下各个对象执行扫描的具体时间以及识别状态，并在具体对象所在行的“操作”列，可执行以下操作： – 单击“停止”，停止对该任务下具体对象的扫描。 – 单击“立即识别”，立即执行对该任务下具体对象的扫描。 – 单击“识别结果”，查看该任务下具体对象的识别情况。 – 单击“删除”，删除该任务下具体对象。 ● 单击任务名称，可以查看检测任务报告。
识别规则组	识别任务使用的规则组。
执行周期	识别任务的具体执行周期。说明如下： ● 单次：识别任务仅执行一次。 ● 每天：每天固定时间执行一次识别任务。 ● 每周：每月固定时间执行一次识别任务。 ● 每月：每周固定时间执行一次识别任务。
状态	识别任务的执行状态。 ● 待识别：识别任务在对列中，等待识别。 ● 识别中：正在执行识别任务。 ● 识别完成：目标任务下的所有识别对象都已成功完成了扫描。 ● 识别异常：目标任务下至少存在一个识别对象执行识别任务失败。 ● 识别终止：正在识别中的任务，被强行停止。
上次识别时间	上一次执行该任务的具体时间。
上次识别结果	上一次该任务扫描的结果，未识别风险、低风险、中风险、高风险。
通知主题	选择的消息通知主题。

参数名称	参数说明
操作	用户可以在操作栏中，执行以下操作： • 立即执行识别任务，具体的参考**立即启动识别任务**章节。 • 查看识别结果，单击“识别结果”，跳转到“识别结果”页面，DSC为您提供了详细的结果分析报告，具体的参考**识别结果**。 • 下载风险结果，单击“更多 > 下载风险结果”，获得详细的风险结果报表。 • 编辑扫描任务，具体的参考**编辑识别任务**章节。 • 删除扫描任务，具体的参考**删除识别任务**章节。

----结束

5.3.3 立即启动识别任务

如果您需要立即执行识别任务，可参考本章节进行操作。

前提条件

已完成识别任务的创建。

操作步骤

步骤1 登录管理控制台。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全 > 数据安全中心”，进入数据安全中心总览界面。

步骤4 在左侧导航树中，选择“敏感数据识别 > 识别任务”，进入“识别任务”页面。

图 5-17 识别任务

步骤5 在待开启敏感数据检测任务所在行的“操作”列，单击“立即识别”。

说明

如果您想停止正在执行的扫描任务，在目标检测任务的操作列，单击“停止”。

----结束

5.3.4 编辑识别任务

本章节指导您如何编辑识别任务。

前提条件

已完成识别任务的创建。

操作步骤

步骤1 登录管理控制台。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全 > 数据安全中心”，进入数据安全中心总览界面。

步骤4 在左侧导航树中，选择“敏感数据识别 > 识别任务”，进入“识别任务”页面。

图 5-18 识别任务

步骤5 在待编辑敏感数据识别任务所在行的“操作”列，单击“更多 > 编辑”。

步骤6 在“编辑任务”对话框中，编辑检测任务的具体参数，相关参数说明如表5-9所示。

图 5-19 编辑任务

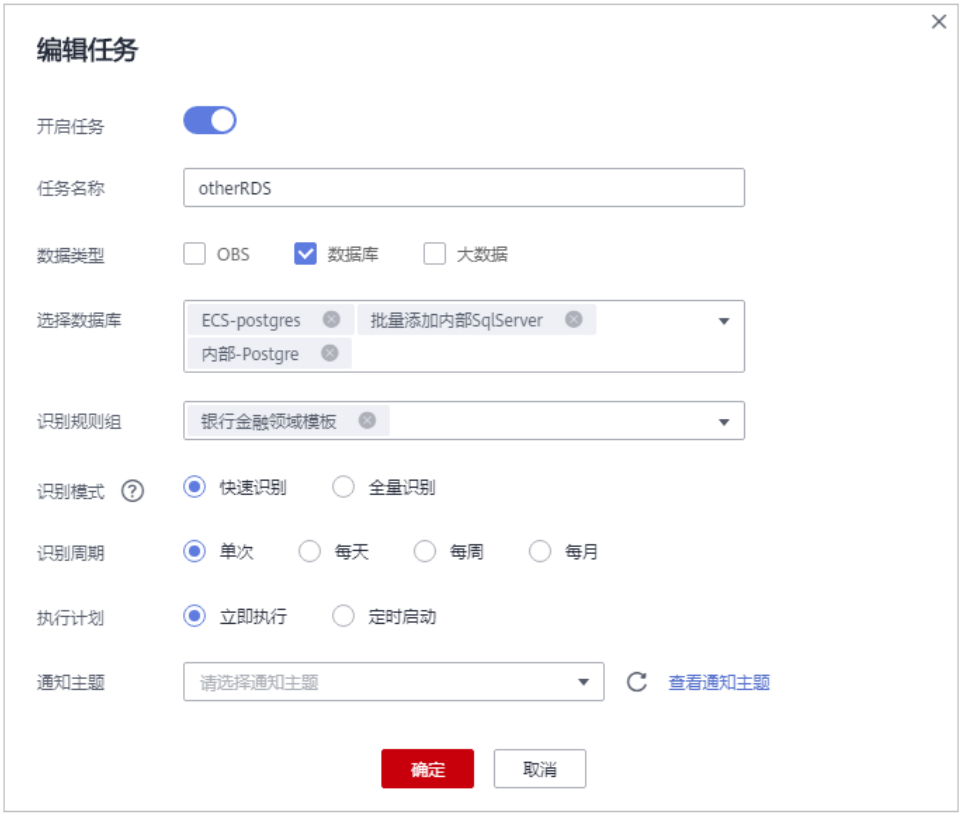


表 5-9 敏感数据识别任务参数说明

参数	参数说明	取值样例
开启任务	是否开启敏感数据识别任务，系统默认开启任务。 ●  ：开启状态。 ●  ：关闭状态。	
任务名称	您可以自定义敏感数据识别任务名称。 任务名称需要满足以下要求： ● 1~255个字符。 ● 字符可由中文、英文字母、数字、下划线或中划线组成。 ● 任务名称不能与已有的任务名称重复。	-
数据类型	选择识别的数据类型。可多选。 ● OBS，添加OBS资产，参考**添加OBS资产**章节。 ● 数据库，添加云数据库资产，参考**添加云数据库**章节。 ● 大数据，添加大数据源资产，参考**添加大数据源资产**章节。 ● MRS，添加Hive资产，参考**添加MRS资产**。	数据库
识别规则组	选择识别任务需要使用的规则组，可多选。可参考**新增敏感数据规则组**章节创建规则组。	-
识别模式	选择检测任务的扫描模式： ● 快速识别：根据规则组进行扫描，实现数据分布快速识别。 ● 全量识别：在规则组的基础上加入自然语义处理NLP能力，扫描速度相对较慢，识别率更高。	快速扫描
识别周期	选择任务的识别周期： ● 单次：根据设置的执行计划，在设定的时间执行一次该识别任务。 ● 每天：选择该选项，需要设置“启动时间”，即在每天的固定时间执行该识别任务。 ● 每周：选择该选项，需要设置“启动时间”，即在设定的时间以及每周这一时间点执行该识别任务。 ● 每月：选择该选项，需要设置“启动时间”，即在设定的时间以及每月这一时间点执行该识别任务。	单次

参数	参数说明	取值样例
执行计划	“扫描周期”选择“单次”时，显示该参数。 • 立即执行：选择该选项，保存后，可以在当前立即执行一次该识别任务。 • 定时启动：在指定时间执行一次该识别任务。	立即执行
启动时间	“扫描周期”选择“每天”、“每周”、“每月”时，显示该参数。 设置识别任务的具体启动时间。设置后，会在指定时间以及每天或者每周或者每月的该时间点执行一次识别任务。	-
通知主题	单击下拉列表选择已创建消息通知主题或者单击“查看通知主题”创建新的主题，用于配置接收告警通知的终端。 告警通知的具体操作请参见**告警通知**。	--

步骤7 单击“确定”。

----结束

5.3.5 删除识别任务

本章节指导您如何删除识别任务。

前提条件

已完成识别任务的创建。

约束条件

- 如果识别任务正在运行，需先停止任务或者待任务识别完成后再执行删除操作。
- 删除操作无法恢复，请谨慎操作。

操作步骤

步骤1 登录管理控制台。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全 > 数据安全中心”，进入数据安全中心总览界面。

步骤4 在左侧导航树中，选择“敏感数据识别 > 识别任务”，进入“识别任务”页面。

图 5-20 识别任务

步骤5 在待删除识别任务所在行的“操作”列，单击“更多 > 删除”。

步骤6 在弹出删除任务提示框中，单击“确定”。

----结束

5.3.6 下载报告

本章节介绍如何下载识别任务报告和识别结果报表。DSC为您提供了PDF格式的识别任务报告和Excel格式的识别结果报表。

前提条件

- 已完成识别任务的创建。
- 已完成扫描。

下载识别结果报表

步骤1 登录管理控制台。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全 > 数据安全中心”，进入数据安全中心总览界面。

步骤4 在左侧导航树中，选择“敏感数据识别 > 识别任务”，进入“识别任务”页面。

图 5-21 识别任务

步骤5 在识别任务所在行的“操作”列，单击“更多 > 下载识别结果”，Excel格式的识别结果报表会保存在您的本地。

----结束

5.4 识别结果

敏感数据识别任务扫描完成后，可通过DSC服务的“识别结果”页面，查看数据资产的风险分布、风险等级以及敏感数据存在的位置。

前提条件

已至少执行过一次敏感数据识别任务。

操作步骤

步骤1 登录管理控制台。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击 ☰，选择“安全 > 数据安全中心”，进入数据安全中心总览界面。

步骤4 在左侧导航树中选择“敏感数据识别 > 识别结果”，进入识别结果页面。

DSC分别统计了大数据、数据库、OBS三个服务中高风险、中风险和低风险对象的数量及分布图。

同时DSC针对扫描对象提供了详细的识别结果列表，同时，在检测结果列表右上角，可通过风险等级、任务名称、数据类型或者对象名称，筛选您想要查看的敏感数据识别结果，识别结果列表参数说明如**表5-10**所示。

图 5-22 识别结果

表 5-10 识别结果参数说明

参数名称	参数说明
对象名称	敏感数据识别的对象名称。
数据类型	• OBS • 数据库 • 大数据 • MRS
所属任务	任务名称，检测结果对象隶属的敏感数据检测任务名称。
未知风险信息	根据您设置的识别规则，经检测，未发现风险的资产数量。
低风险敏感信息	根据您设置的识别规则，经检测，统计的低风险（风险等级：1~3级）的资产数量。
中风险敏感信息	根据您设置的识别规则，经检测，统计的中风险（风险等级：4~7级）的资产数量。
高风险敏感信息	根据您设置的识别规则，经检测，统计的高风险（风险等级：8~10级）的资产数量。
上次扫描时间	最近扫描该对象的时间。
操作	单击“查看详情”，查看该对象的识别结果明细。

步骤5 在扫描对象所在行的“操作”列，单击“查看详情”，进入“结果明细”页面。

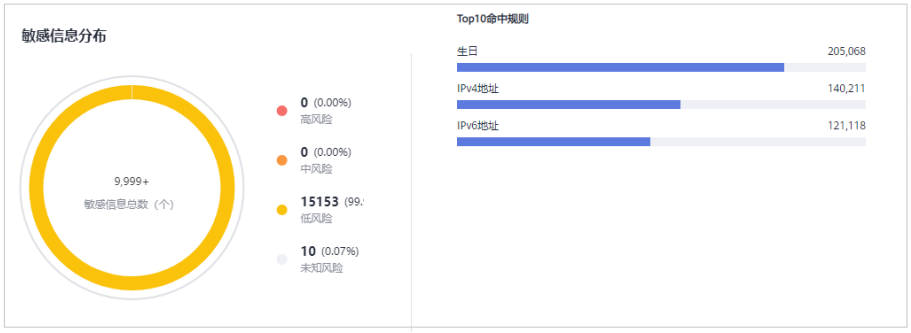
在页面的左上角，在下拉框中可以选择任务名称、数据类型或者对象名称来查看具体扫描对象的识别结果明细。

在页面的右上角，可单击“下载识别结果”，下载风险结果报表。

- 敏感信息分布

  可查看敏感信息的风险分布情况、对应风险等级资产的数量及其占比、Top10命中规则。

  图 5-23 敏感信息分布图

- 血缘图

  可查看资产中敏感数据的具体名称、路径、风险等级。

  图 5-24 血缘图

----结束

6 数据脱敏

6.1 概述

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，数据安全中心支持的脱敏算法如**脱敏算法**所示。

静态脱敏：可以按照脱敏规则一次性完成大批量数据的变形转换处理，静态脱敏通常用在将生产环境中的敏感数据交付至开发、测试或者外发环境的情况使用，适用于开发测试、数据分享、数据研究等场景。您可以通过DSC控制台创建脱敏任务，快速实现对数据库和大数据的脱敏。

动态脱敏：DSC提供动态脱敏API，支持用户对外部申请访问的数据实时脱敏。动态脱敏通常会在数据对外提供查询服务的场景中使用，适用于生产应用、数据交换、运维应用、精准营销等场景。

数据脱敏操作流程

图 6-1 静态脱敏操作流程

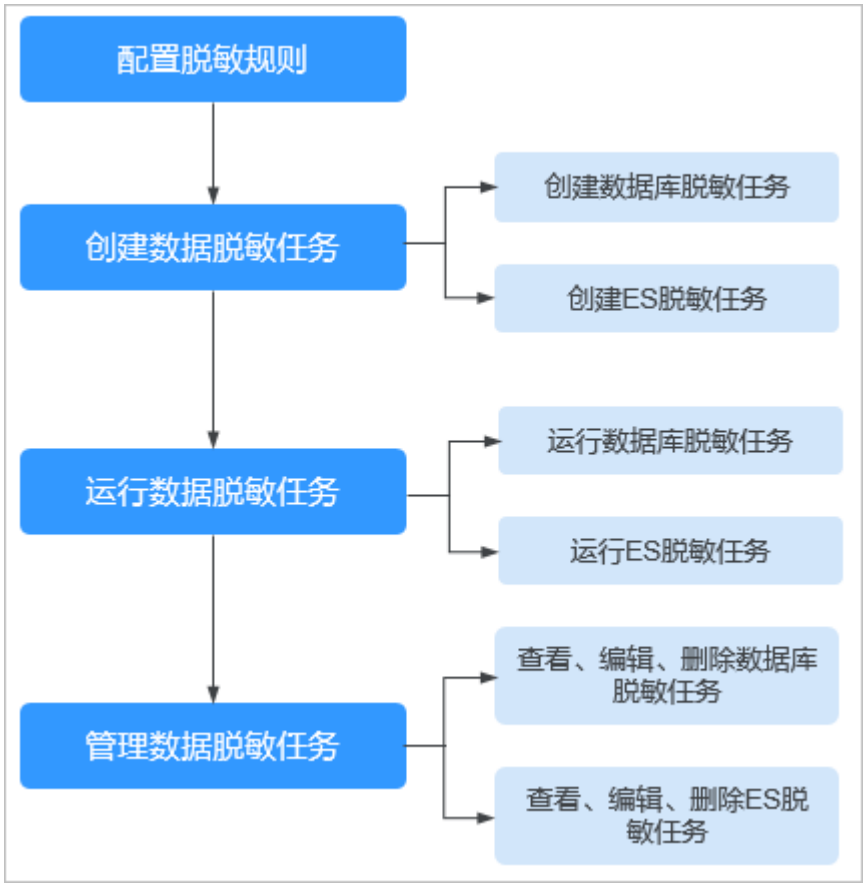
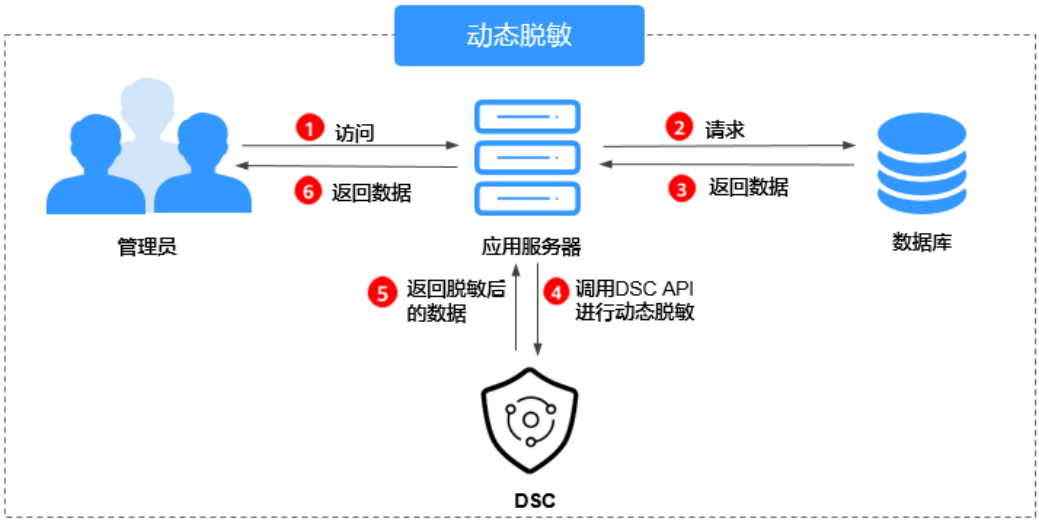


图 6-2 动态脱敏操作流程



脱敏算法

表 6-1 脱敏算法说明

脱敏算法	脱敏方式说明	使用场景
Hash脱敏	使用Hash函数对敏感数据进行脱敏。支持SHA256和SHA512。 ● SHA256 将数据库表中字符串类型字段的内容用其SHA256的摘要值代替。 该算法执行完后，结果的长度可能超过原表中列允许的最大长度。该算法按照SHA256输出长度调整列的长度。 ● SHA512 将数据库表中字符串类型字段的内容用其SHA512的摘要值代替。 该算法执行完后，结果的长度可能超过原表中列允许的最大长度。该算法按照SHA512输出长度调整列的长度。	● 敏感类型：密钥类 ● 适用场景：数据存储

脱敏算法	脱敏方式说明	使用场景
字符掩盖	使用指定字符*或随机字符（随机字符包含随机数字、随机字母、随机数字字母三种类型）方式遮盖部分内容。 支持以下六种脱敏方式： ● 保留前n后m ● 保留自x至y ● 遮盖前n后m ● 遮盖自x至y ● 特殊字符前遮盖 ● 特殊字符后遮盖 **说明** 敏感数据保护服务中已预置多种字符脱敏模板。	● 敏感类型：个人敏感 ● 适用场景： – 数据使用 – 数据分享
关键字替换	在指定列中查找关键词并替换。 例如，目标字符串为“张三在家吃饭”，算法执行完后映射为“张先生在家吃饭”，其中指定将“张三”替换为“张先生”。 该算法执行完后，结果的长度可能超过数据库允许的最大长度。该算法将超出部分截断后插入数据库。	● 敏感类型： – 个人敏感 – 企业敏感 – 设备敏感 ● 适用场景： – 数据存储 – 数据分享

脱敏算法	脱敏方式说明	使用场景
删除脱敏	将指定字段设置为Null或空值进行脱敏。 ● Null脱敏 将任意类型字段设置为NULL。 对于列属性设置为“NOT NULL”的字段，该算法在拷贝时将该列属性修改为“NULL”。 ● 空值脱敏 将指定字段内容设置为空值。 具体来说，将字符型的字段设置为空串，数值类的字段设置为0，日期类的字段设置为1970，时间类的字段设置为零点。	● 敏感类型： – 个人敏感 – 企业敏感 – 设备敏感 ● 适用场景： – 数据存储 – 数据分享

脱敏算法	脱敏方式说明	使用场景
取整脱敏	针对日期或数字特定参数进行取整运算。 ● 日期取整 年之后字段全部取整。示例：“2019-05-12 -> 2019-01-01”或“2019-05-12 08:08:08 -> 2019-01-01 00:00:00” 月之后字段全部取整。示例：“2019-05-12 -> 2019-05-01”或“2019-05-12 08:08:08 -> 2019-05-01 00:00:00” 日之后字段全部取整。示例：“2019-05-12 -> 2019-05-12”或“2019-05-12 08:08:08 -> 2019-05-12 00:00:00” 小时之后字段全部取整。示例：“08:08:08 -> 08:00:00”或“2019-05-12 08:08:08 -> 2019-05-12 08:00:00” 分钟之后字段全部取整。示例：“08:08:08 -> 08:08:00”或“2019-05-12 08:08:08 -> 2019-05-12 08:08:00” 秒之后字段全部取整。示例：“08:08:08.123 -> 08:08:08.000”或	● 敏感类型：通用敏感 ● 适用场景： – 数据存储 – 数据使用

脱敏算法	脱敏方式说明	使用场景
	“1575612731312 -> 1575612731000” • 数字取整 针对指定数字进行取整运算。	

相关操作

- 配置脱敏规则
- 创建数据脱敏任务
- 运行数据脱敏任务
- 管理数据脱敏任务

6.2 配置脱敏规则

本章节介绍如何配置脱敏规则。更多关于脱敏算法说明请参见概述。

操作步骤

步骤1 登录管理控制台。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全 > 数据安全中心”，进入数据安全中心总览界面。

步骤4 在左侧导航树中选择“数据脱敏”，并选择“脱敏规则”页签，进入脱敏规则页面。

步骤5 在“脱敏规则”页签中，选择合适的脱敏方式，配置脱敏规则。

- “Hash脱敏”的配置方法请参考Hash脱敏。
- “字符掩盖”的配置方法请参考字符掩盖。
- “关键字替换”的配置方法请参考关键字替换。
- “删除脱敏”的配置方法请参考删除脱敏。
- “取整脱敏”的配置方法请参考取整脱敏。

----结束

Hash 脱敏

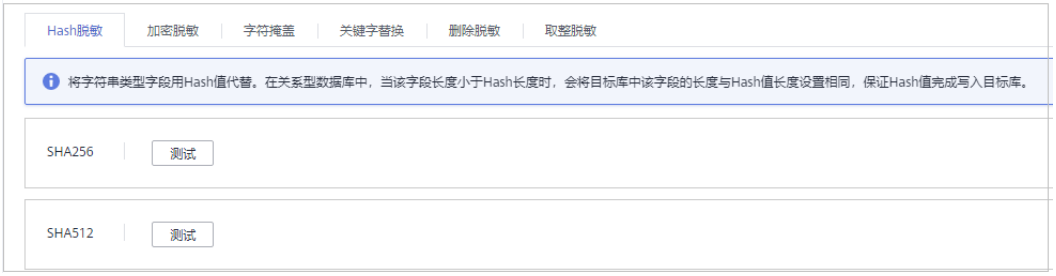
将字符串类型字段用Hash值代替。在关系型数据库中，当该字段长度小于Hash长度时，会将目标库中该字段的长度与Hash值长度设置相同，保证Hash值完整写入目标库。DSC默认配置了SHA256和SHA512两种Hash脱敏的算法。

Hash脱敏为DSC内置的脱敏规则，不需要配置，如果您需要测试脱敏效果，可参考以下方法查看脱敏结果。

步骤1 参照**操作步骤**进入“脱敏规则”页面。

步骤2 选择“Hash脱敏”，进入Hash脱敏的页面。

图 6-3 Hash 脱敏



步骤3 在选择的SHA256或SHA512算法所在列，单击“测试”。

步骤4 在弹出的页面中输入“原始数据”，并单击“测试”，在“脱敏结果”文本框中展示已完成脱敏的数据。

图 6-4 Hash 脱敏测试

----结束

字符掩盖

使用指定字符“*”或随机字符，按照指定方式遮盖部分内容。

支持“保留前n后m”、“保留自x至y”、“遮盖前n后m”、“遮盖自x至y”、“特殊字符前遮盖”和“特殊字符后遮盖”六种字符掩盖的方式。

步骤1 参照**操作步骤**进入“脱敏规则”页面。

步骤2 选择“字符掩盖”页签，进入“字符掩盖”页面。

图 6-5 字符掩盖页面

步骤3 单击“添加”，配置字符脱敏规则。

图 6-6 添加字符脱敏

步骤4 输入“原始数据”，单击“测试”，在“脱敏结果”文本框中展示已完成脱敏的数据。

步骤5 测试确认无误后，单击“保存”。

说明

- 数据安全中心服务中已预置多种字符脱敏规则。内置的脱敏规则不支持删除，自定义的规则可以在规则列表的“操作”列，单击“删除”，删除规则。
- 所有的规则都支持编辑，在规则列表的“操作”列，单击“编辑测试”，修改规则。

----结束

关键字替换

利用自定义的字符串替换数据中匹配到的关键字，达到脱敏的效果。例如：原始数据为a**bcde**fg**bcde**fgkjkoij，“关键字”配置为“bcde”，“替换字符串”配置为12，则“脱敏结果”显示为a**12**fg**12**fgkjkoij。

步骤1 参照**操作步骤**进入“脱敏规则”页面。

步骤2 选择“关键字替换”页签，进入“关键字替换”页面。

图 6-7 关键字替换

步骤3 设置需要替换的“关键字”，以及“替换字符串”。

配置后，“原始数据”中匹配到的“关键字”将被设置的“替换字符串”替换，以完成数据脱敏。

图 6-8 添加关键字

步骤4 输入“原始数据”，单击“测试”，在“脱敏结果”文本框中展示已完成脱敏的数据。

步骤5 测试确认无误后，单击“保存”。

- 如果您想修改已配置的脱敏规则，可以在关键字替换规则列表的操作列，单击“编辑测试”进行修改。
- 如果您想删除已配置的脱敏规则，可以在关键字替换规则列表的操作列，单击“删除”。

----结束

删除脱敏

系统内置“Null脱敏”和“空值脱敏”两种算法。

- Null脱敏：将任意类型字段设置为NULL。对于属性设置为“NOT NULL”的字段，该算法在拷贝时将该属性修改为“NULL”。
- 空置脱敏：将指定字段内容设置为空值。具体来说，将字符型的字段设置为空串，数值类的字段设置为0，日期类的字段设置为1970，时间类的字段设置为零点。

删除脱敏为DSC内置的脱敏规则，不需要配置，可参考以下方法查看脱敏规则。

步骤1 参照**操作步骤**进入“脱敏规则”页面。

步骤2 选择“删除脱敏”页签，进入“删除脱敏”的规则展示页面。

图 6-9 删除脱敏

----结束

取整脱敏

步骤1 参照**操作步骤**进入“脱敏规则”页面。

步骤2 选择“取整脱敏”，进入“取整脱敏”的页面。

系统设置了“日期取整”和“数字取整”两种算法。

- “日期取整”算法对应关系型数据库中timestamp，time，data，datatime等与时间相关的字段。
- “数字取整”算法对应double，float，int，long等数值类型，脱敏成功后，保持原字段类型不变。

图 6-10 取整脱敏页面

步骤3 在“数字取整”所在列，单击“编辑测试”，配置“取整值”。

脱敏原理：结果值取靠近“取整值”倍数的向下值。例如：“取整值”设置为5，“原始数据”为14，5的倍数向下靠近14的数为10，则原始数据14按此规则脱敏后为10，即“脱敏结果”为10。

图 6-11 数字取整

步骤4 输入“原始数据”，单击“测试”，在“脱敏结果”文本框中展示已完成脱敏的数据。

步骤5 测试确认无误后，单击“保存”。

----结束

6.3 静态脱敏

6.3.1 创建数据脱敏任务

6.3.1.1 创建数据库脱敏任务

创建数据库脱敏任务后，可以对指定数据库的敏感信息脱敏。

本章节将介绍如何创建数据库脱敏任务。

前提条件

- 已在“资产列表”中完成了云资源委托授权。
- 已添加数据库资产。
- 已在“敏感数据识别”中完成了敏感数据识别，具体操作请参见**创建敏感数据识别任务**。

创建数据库脱敏

步骤1 登录管理控制台。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全 > 数据安全中心”，进入数据安全中心总览界面。

步骤4 在左侧导航树中选择“数据脱敏”，进入“数据库脱敏”页面。

步骤5 在“数据库脱敏”页签中，单击，将“数据库脱敏”设置为，开启数据库脱敏。

步骤6 单击“新建任务”，进入“数据源配置”页面，具体参数说明如**表6-2**所示。

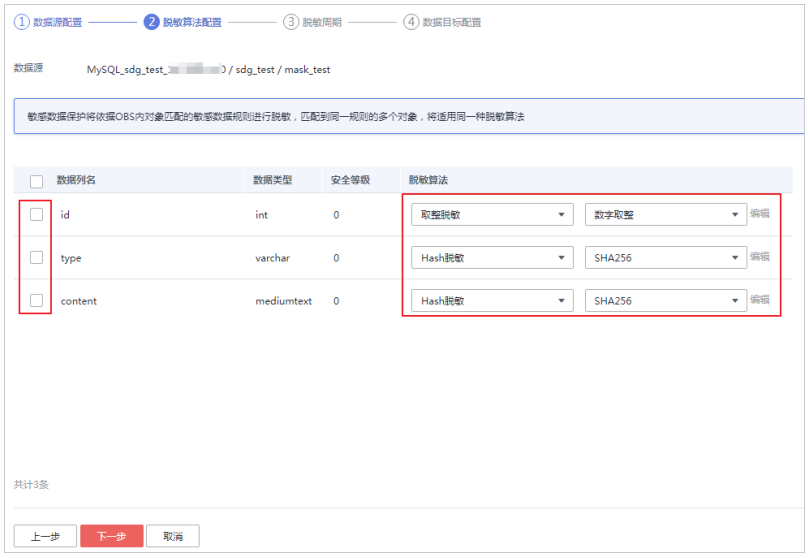
图 6-12 数据源配置-数据库脱敏任务

表 6-2 数据源配置参数说明

参数名称	参数说明
任务名称	您可以自定义脱敏任务的名称。 任务名称需要满足以下要求： • 1~255个字符。 • 字符可由中文、英文字母、数字、下划线或中划线组成。
数据源选择	选择数据来源。可选择“SQLServer”、“MySQL”、“PostgreSQL”。
数据源 **说明** 如果没有可使用的云数据库，可单击“添加云数据库”，添加云数据库资产，具体的操作可参见**添加云数据库**。	数据库实例：选择脱敏数据所在的数据库实例。
	数据库名：选择脱敏数据所在的数据库名称。
	模式：当“数据源选择”选择“SQLServer”和“PostgreSQL”时，显示该参数。
	数据表名：选择脱敏数据所在的数据表名称。
	数据类型：勾选后将该列数据拷贝到目标数据库。 此处还显示数据列的“目标数据类型”，“风险等级”。

步骤7 单击“下一步”，进入“脱敏算法配置”页面。

图 6-13 脱敏算法配置-数据库脱敏任务



1. 勾选需要脱敏的数据列。
2. 选择脱敏算法。脱敏算法详细信息请参见**配置脱敏规则**。

步骤8 单击“下一步”，进入“脱敏周期”页面，配置脱敏周期。

图 6-14 脱敏周期

选择并设置脱敏任务的执行周期：

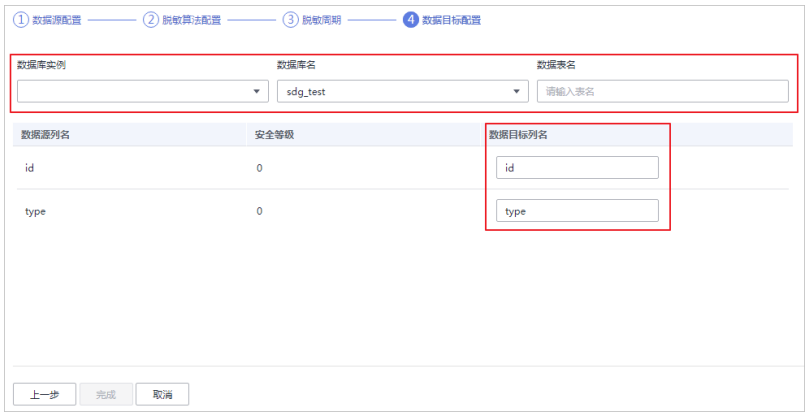
- 手动：由用户自行启动的，且基于脱敏规则执行脱敏任务。
- 每小时：每几个小时执行一次脱敏任务。
  示例：如果需要每2小时执行一次脱敏任务，则此处设置为：02:00
- 每天：每天几点几分执行一次脱敏任务。
  示例：如果需要每天12:00执行一次脱敏任务，则此处设置为：12:00:00
- 每周：每周几的几点几分执行一次脱敏任务。
  示例：如果需要每周一的12:00执行一次脱敏任务，则此处设置为：每周一 12:00:00
- 每月：每月几日几时执行一次脱敏任务。
  示例：如果需要每月12日的12:00执行一次脱敏任务，则此处设置为：每月12日 12:00:00

  说明

  如果设置每月31日执行一次脱敏任务，在当月日期少于31日的情况下，系统自动在当月最后一日执行任务。

步骤9 单击“下一步”，进入“数据目标配置”页面。

图 6-15 数据目标配置-数据库脱敏任务



1. 选择数据库实例、数据库名，并输入数据表名。

   如果输入的数据表名已存在，系统将刷新目标数据库中该数据表中的数据。

   如果输入的数据表名不存在，系统将自动在目标数据库中新建该名称的数据表。

   注意

   如果需要填写已有的数据表，请勿选择业务数据表，以免影响业务。

2. 设置数据目标列名。

   系统默认将生产与数据源列相同的名称，您可以保持默认名称，也可以根据需要进行修改。

步骤10 单击“完成”，完成数据库脱敏任务的创建。

----结束

后续处理

数据库脱敏任务创建成功后，需运行脱敏任务，系统才会按照设置的脱敏周期执行脱敏任务，运行数据库脱敏任务具体操作请参见**运行数据库脱敏任务**。

6.3.1.2 创建 ES 脱敏任务

创建ES脱敏任务后，可以对指定Elasticsearch数据源中的表/列进行敏感信息脱敏。

本章节将介绍如何创建ES脱敏任务。

前提条件

- 已在“资产列表”中完成了云资源委托授权。
- 已添加了ES资产，具体请参见**大数据资产列表**。
- 已在“敏感数据识别”中完成了敏感数据识别，具体操作请参见**创建敏感数据识别任务**。

操作步骤

步骤1 登录管理控制台。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全 > 数据安全中心”，进入数据安全中心总览界面。

步骤4 在左侧导航树中选择“数据脱敏”，并选择“ES脱敏”页签，进入ES脱敏页面。

步骤5 单击，将“ES脱敏”设置为，开启ES脱敏。

步骤6 单击“新建任务”，进入“数据源配置”页面，具体参数说明如表6-3所示。

图 6-16 数据源配置-ES 脱敏任务

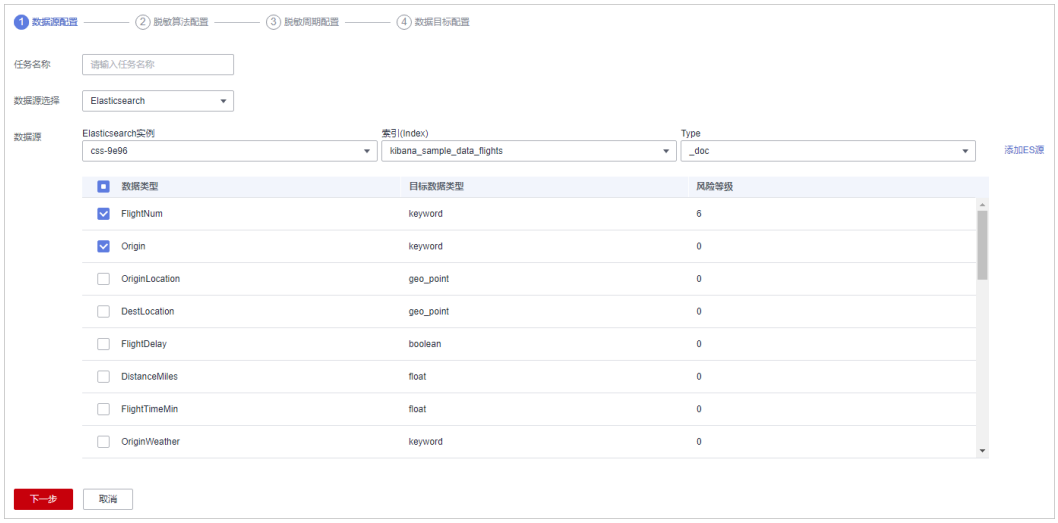


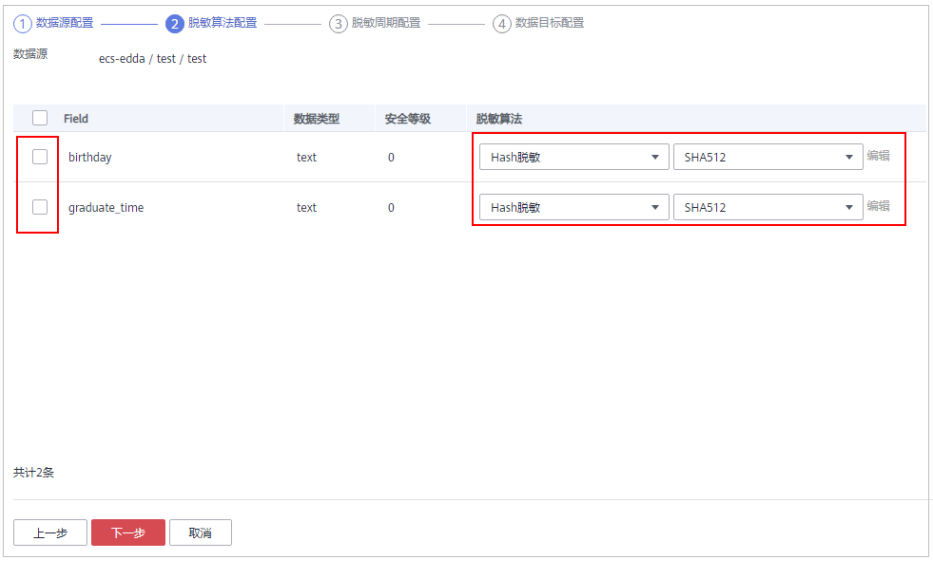
表 6-3 数据源配置参数说明

参数名称	参数说明
任务名称	您可以自定义脱敏任务的名称。 任务名称需要满足以下要求： • 1~255个字符。 • 字符可由中文、英文字母、数字、下划线或中划线组成。
数据源选择	选择数据来源。目前仅支持“Elasticsearch”。
数据源 **说明** 如果没有可使用的ES资产，可单击“添加ES源”，添加ES资产，具体的操作可参见**添加大数据源资产**。	Elasticsearch实例：选择脱敏数据所在的Elasticsearch实例。
	索引(Index)：选择脱敏数据所在的索引。
	Type：选择脱敏数据所在的Type。

参数名称	参数说明
	Field：勾选后将该列数据拷贝到目标数据库。 此处还显示数据列的“目标数据类型”，“风险等级”。

步骤7 单击“下一步”，进入“脱敏算法配置”页面。

图 6-17 脱敏算法配置-ES 脱敏任务



1. 勾选需要脱敏的Field。
2. 选择脱敏算法。脱敏算法更多详细信息请参见**配置脱敏规则**。

步骤8 单击“下一步”，进入“脱敏周期”页面，配置脱敏周期。

图 6-18 脱敏周期

选择并设置脱敏任务的执行周期：

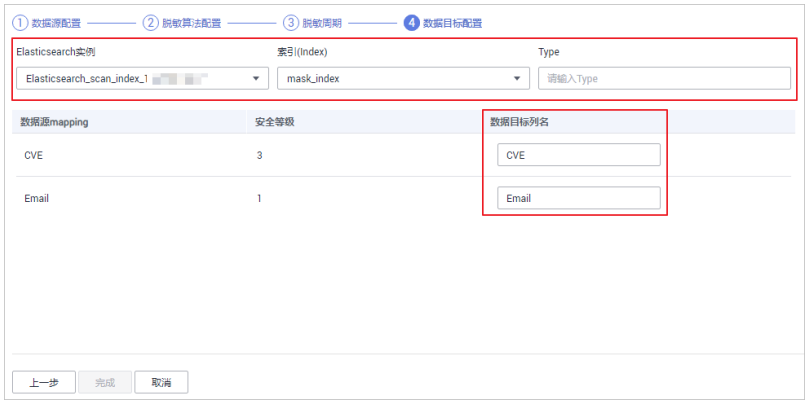
- 手动：由用户自行启动的，且基于脱敏规则执行脱敏任务。
- 每小时：每几个小时执行一次脱敏任务。
  示例：如果需要每2小时执行一次脱敏任务，则此处设置为：02:00
- 每天：每天几点几分执行一次脱敏任务。
  示例：如果需要每天12:00执行一次脱敏任务，则此处设置为：12:00:00
- 每周：每周几的几点几分执行一次脱敏任务。
  示例：如果需要每周一的12:00执行一次脱敏任务，则此处设置为：每周一 12:00:00
- 每月：每月几日几时执行一次脱敏任务。
  示例：如果需要每月12日的12:00执行一次脱敏任务，则此处设置为：每月12日 12:00:00

  说明

  如果设置每月31日执行一次脱敏任务，在当月日期少于31日的情况下，系统自动在当月最后一日执行任务。

步骤9 单击“下一步”，进入“数据目标配置”页面。

图 6-19 数据目标配置-ES 脱敏任务



1. 选择“Elasticsearch实例”、“索引(Index)”，并输入“Type”。
   如果输入的Type已存在，系统将刷新目标数据源中该Type中的数据。
   如果输入的Type不存在，系统将自动在目标数据源中新建该名称的Type。

   注意

   如果需要填写已有的Type，请勿选择业务Type，以免影响业务。

2. 设置数据目标列名。
   系统默认将生成与数据源列相同的名称，您可以保持默认名称，也可以根据需要进行修改。

步骤10 单击“完成”，完成脱敏规则的创建。

----结束

后续处理

ES脱敏任务创建成功后，需运行脱敏任务，系统才会按照设置的脱敏周期执行脱敏任务，运行ES脱敏任务具体操作请参见**运行ES脱敏任务**。

6.3.1.3 创建 MRS 脱敏任务

创建MRS脱敏任务后，可以对指定数据的敏感信息脱敏。

本章节将介绍如何创建MRS脱敏任务。

前提条件

- 已在“资产列表”中完成了云资源委托授权。
- 已添加MRS资产，具体请参见**添加MRS资产**。
- 已在“敏感数据识别”中完成了敏感数据识别，具体操作请参见**创建敏感数据识别任务**。

创建数据库脱敏

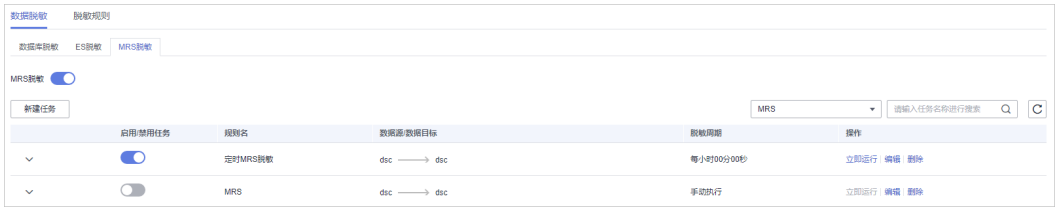
步骤1 登录管理控制台。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全 > 数据安全中心”，进入数据安全中心总览界面。

步骤4 在左侧导航树中选择“数据脱敏”，并选择“MRS脱敏”页签，进入“MRS脱敏”页面。

图 6-20 进入 MRS 脱敏



步骤5 在“MRS脱敏”页签中，单击，将“MRS脱敏”设置为，开启MRS脱敏。

步骤6 单击“新建任务”，进入“数据源配置”页面，具体参数说明如**表6-4**所示。

图 6-21 数据源配置-MRS 脱敏任务

表 6-4 数据源配置参数说明

参数名称	参数说明
任务名称	您可以自定义脱敏任务的名称。 任务名称需要满足以下要求： • 1~255个字符。 • 字符可由中文、英文字母、数字、下划线或中划线组成。
数据源选择	选择数据来源。仅支持“MRS_HIVE”。
数据源 **说明** 如果没有可使用的云数据，可单击“添加云数据库”，添加云数据库资产，具体的操作可参见**添加MRS资产**。	数据库实例：选择脱敏数据所在的数据库实例。
	数据库名：选择脱敏数据所在的数据库名称。
	数据表名：选择脱敏数据所在的数据表名称。
	数据类型：勾选后将该列数据拷贝到目标数据库。 此处还显示数据列的“目标数据类型”，“风险等级”。

步骤7 单击“下一步”，进入“脱敏算法配置”页面。

图 6-22 脱敏算法配置-MRS 脱敏任务

1. 勾选需要脱敏的数据列。
2. 选择脱敏算法。脱敏算法更多详细信息请参见**配置脱敏规则**。

步骤8 单击“下一步”，进入“脱敏周期”页面，配置脱敏周期。

图 6-23 脱敏周期

选择并设置脱敏任务的执行周期：

- 手动：由用户自行启动的，且基于脱敏规则执行脱敏任务。
- 每小时：每几个小时执行一次脱敏任务。
  示例：如果需要每2小时执行一次脱敏任务，则此处设置为：02:00
- 每天：每天几点几分执行一次脱敏任务。
  示例：如果需要每天12:00执行一次脱敏任务，则此处设置为：12:00:00
- 每周：每周几的几点几分执行一次脱敏任务。
  示例：如果需要每周一的12:00执行一次脱敏任务，则此处设置为：每周一 12:00:00
- 每月：每月几日几时执行一次脱敏任务。
  示例：如果需要每月12日的12:00执行一次脱敏任务，则此处设置为：每月12日 12:00:00

说明

如果设置每月31日执行一次脱敏任务，在当月日期少于31日的情况下，系统自动在当月最后一日执行任务。

步骤9 单击“下一步”，进入“数据目标配置”页面。

图 6-24 数据目标配置-MRS 脱敏任务

1. 选择数据库实例、数据库名，并输入数据表名。
   如果输入的数据表名已存在，系统将刷新目标数据库中该数据表中的数据。
   如果输入的数据表名不存在，系统将自动在目标数据库中新建该名称的数据表。

   注意

   如果需要填写已有的数据表，请勿选择业务数据表，以免影响业务。

2. 设置数据目标列名。
   系统默认将生产与数据源列相同的名称，您可以保持默认名称，也可以根据需要进行修改。

步骤10 单击“完成”。

----结束

6.3.2 运行数据脱敏任务

6.3.2.1 运行数据库脱敏任务

创建数据库脱敏任务后，可以对指定数据库中的表/列进行敏感信息脱敏。

本章节将介绍如何运行数据库脱敏任务。

前提条件

已创建数据库脱敏任务。

操作步骤

步骤1 登录管理控制台。

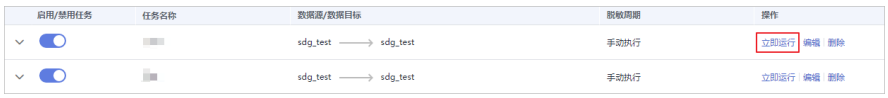
步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全 > 数据安全中心”，进入数据安全中心总览界面。

步骤4 在左侧导航树中选择“数据脱敏”，进入“数据库脱敏”页面。

步骤5 在“数据库脱敏”页签中，在需要执行的任务所在行的“操作”列，单击“立即运行”。

图 6-25 立即运行数据库脱敏任务



运行后，系统开始按照设置的脱敏周期执行脱敏任务。

步骤6 可单击脱敏任务所在行前面的，查看脱敏任务运行状态。

运行“状态”说明如下：

- 已完成：脱敏任务已完成运行，且运行成功。
- 运行中：脱敏任务正在执行中。
- 待运行：脱敏任务未运行。
- 已停止：用户已手动停止脱敏任务的运行。
- 运行失败：脱敏任务运行失败。

图 6-26 数据库脱敏任务运行情况

----结束

6.3.2.2 运行 ES 脱敏任务

创建ES脱敏任务后，可以对指定ES中的表/列进行敏感信息脱敏。

本章节将介绍如何运行ES脱敏任务。

前提条件

已创建ES脱敏任务。

操作步骤

步骤1 登录管理控制台。

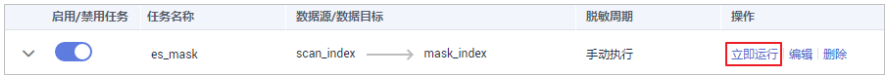
步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全 > 数据安全中心”，进入数据安全中心总览界面。

步骤4 在左侧导航树中选择“数据脱敏”，并选择“ES脱敏”页签，进入ES脱敏页面。

步骤5 在“ES脱敏”页签中，在需要执行的任务所在行的“操作”列，单击“立即运行”。

图 6-27 立即运行 ES 脱敏任务



运行后，系统开始按照设置的脱敏周期执行脱敏任务。

说明

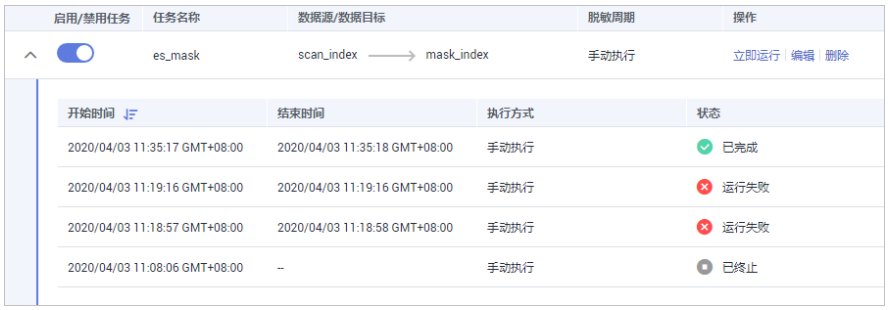
如果“启用/禁用任务”的状态为，即该任务处于禁用状态，则无法单击“立即运行”，启动任务。

步骤6 可单击脱敏任务所在行前面的 ，查看脱敏任务运行状态。

运行“状态”说明如下：

- 已完成：脱敏任务已完成运行，且运行成功。
- 运行中：脱敏任务正在执行中。
- 待运行：脱敏任务未运行。
- 已停止：用户已手动停止脱敏任务的运行。
- 运行失败：脱敏任务运行失败。

图 6-28 ES 脱敏任务运行情况



----结束

6.3.2.3 运行 MRS 脱敏任务

创建MRS脱敏任务后，可以对指定MRS中的表/列进行敏感信息脱敏。

本章节将介绍如何运行MRS脱敏任务。

前提条件

已创MRS库脱敏任务。

操作步骤

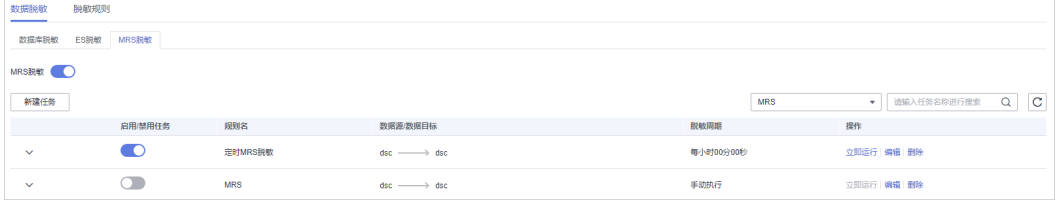
步骤1 登录管理控制台。

步骤2 单击左上角的 ，选择区域或项目。

步骤3 在左侧导航树中，单击 ，选择“安全 > 数据安全中心”，进入数据安全中心总览界面。

步骤4 在左侧导航树中选择“数据脱敏”，并选择“MRS脱敏”页签，进入“MRS脱敏”页面。

图 6-29 进入 MRS 脱敏



步骤5 在“MRS脱敏”页签中，在需要执行的任务所在行的“操作”列，单击“立即运行”。

运行后，系统开始按照设置的脱敏周期执行脱敏任务。

步骤6 可单击脱敏任务所在行前面的，查看脱敏任务运行状态。

运行“状态”说明如下：

- 已完成：脱敏任务已完成运行，且运行成功。
- 运行中：脱敏任务正在执行中。
- 待运行：脱敏任务未运行。
- 已停止：用户已手动停止脱敏任务的运行。
- 运行失败：脱敏任务运行失败。

图 6-30 MRS 脱敏任务运行情况

----结束

6.3.3 管理数据脱敏任务

6.3.3.1 管理数据库脱敏任务

本章节介绍如何查看、编辑、删除数据库脱敏任务。

前提条件

已创建数据库脱敏任务。

查看数据库脱敏任务

步骤1 登录管理控制台。

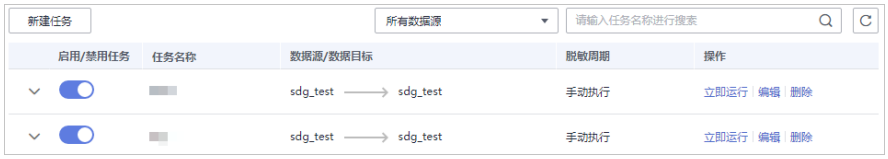
步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全 > 数据安全中心”，进入数据安全中心总览界面。

步骤4 在左侧导航树中选择“数据脱敏”，进入“数据库脱敏”页面。

步骤5 在数据库脱敏任务列表中，查看脱敏任务的详细信息，脱敏任务参数说明如表6-5所示。

图 6-31 查看数据库脱敏任务



说明

输入任务名称或任务名称的关键字，单击 或按“Enter”，可以搜索指定的脱敏任务。

表 6-5 脱敏任务参数说明

参数名称	参数说明
启用/禁用任务	启用或禁用脱敏任务。 • ：启用 • ：禁用
任务名称	脱敏任务的名称。
数据源/数据目标	脱敏任务的数据源和数据目标。
脱敏周期	脱敏规则的具体执行周期，说明如下： • 手动执行：由用户自行启动的，且基于脱敏规则执行脱敏任务。 • 每小时：每几小时按照脱敏规则执行一次脱敏任务。 • 每天：每天固定时间按照脱敏规则执行一次脱敏任务。 • 每周：每周固定时间按照脱敏规则执行一次脱敏任务。 • 每月：每月固定时间按照脱敏规则执行一次脱敏任务。
操作	用户可以在操作栏中，执行立即运行、编辑、删除等操作。

----结束

编辑数据库脱敏任务

步骤1 登录管理控制台。

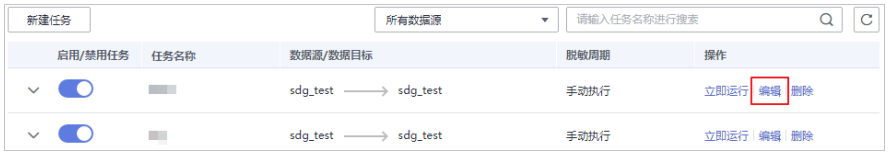
步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击 ，选择“安全 > 数据安全中心”，进入数据安全中心总览界面。

步骤4 在左侧导航树中选择“数据脱敏”，进入“数据库脱敏”页面。

步骤5 在数据库脱敏任务列表中，在待编辑脱敏规则所在行的“操作”列，单击“编辑”，进入“数据源配置”页面。

图 6-32 编辑数据库脱敏任务



步骤6 配置数据源，具体参数说明如**表6-6**所示。

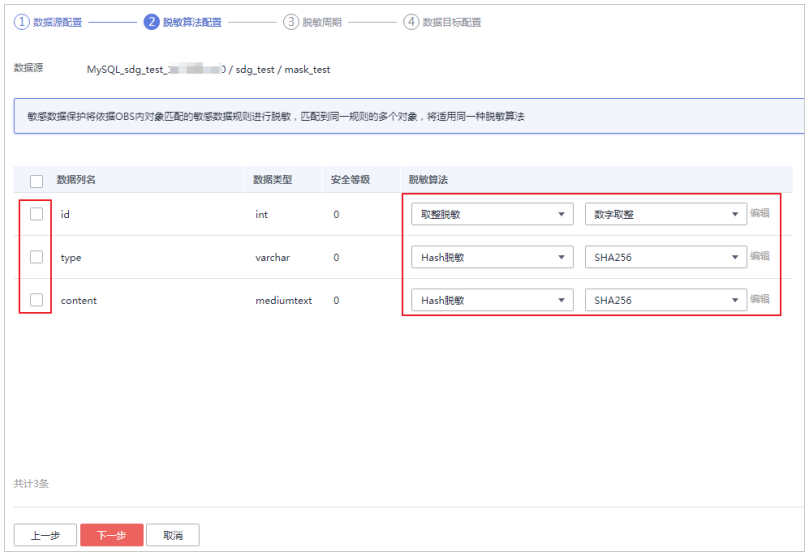
图 6-33 数据源配置-数据库脱敏任务

表 6-6 数据源配置参数说明

参数名称	参数说明
任务名称	您可以自定义脱敏任务的名称。 任务名称需要满足以下要求： ● 1~255个字符。 ● 字符可由中文、英文字母、数字、下划线或中划线组成。
数据源选择	选择数据来源。可选择“SQLServer”、“MySQL”、“PostgreSQL”。
数据源 **说明** 如果没有可使用的云数据库，可单击“添加云数据库”，添加云数据库资产，具体的操作可参见**添加云数据库**。	数据库实例：选择脱敏数据所在的数据库实例。
	数据库名：选择脱敏数据所在的数据库名称。
	模式：当“数据源选择”选择“SQLServer”和“PostgreSQL”时，显示该参数。
	数据表名：选择脱敏数据所在的数据表名称。
	数据类型：勾选后将该列数据拷贝到目标数据库。 此处还显示数据列的“目标数据类型”，“风险等级”。

步骤7 单击“下一步”，进入“脱敏算法配置”页面。

图 6-34 脱敏算法配置-数据库脱敏任务



1. 勾选需要脱敏的数据列。
2. 选择脱敏算法。脱敏算法详细信息请参见**配置脱敏规则**。

步骤8 单击“下一步”，进入“脱敏周期”页面，配置脱敏周期。

图 6-35 脱敏周期

选择并设置脱敏任务的执行周期：

- 手动：由用户自行启动的，且基于脱敏规则执行脱敏任务。
- 每小时：每几个小时执行一次脱敏任务。
  示例：如果需要每2小时执行一次脱敏任务，则此处设置为：02:00
- 每天：每天几点几分执行一次脱敏任务。
  示例：如果需要每天12:00执行一次脱敏任务，则此处设置为：12:00:00

- 每周：每周几的几点几分执行一次脱敏任务。

  示例：如果需要每周一的12:00执行一次脱敏任务，则此处设置为：每周一 12:00:00

- 每月：每月几日几时执行一次脱敏任务。

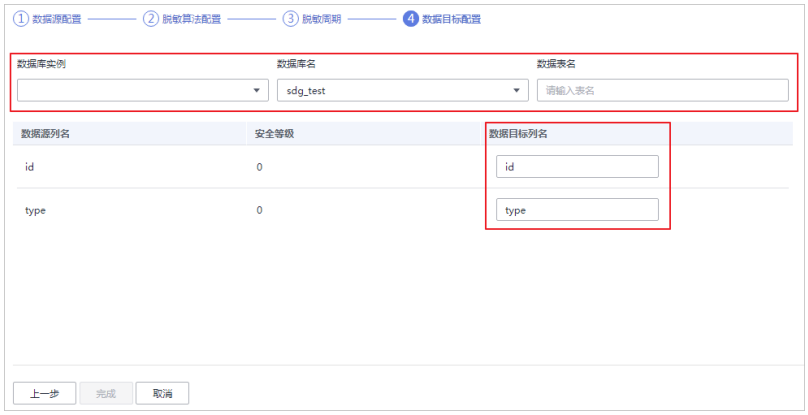
  示例：如果需要每月12日的12:00执行一次脱敏任务，则此处设置为：每月12日 12:00:00

  说明

  如果设置每月31日执行一次脱敏任务，在当月日期少于31日的情况下，系统自动在当月最后一日执行任务。

步骤9 单击“下一步”，进入“数据目标配置”页面。

图 6-36 数据目标配置-数据库脱敏任务



1. 选择数据库实例、数据库名，并输入数据表名。

   如果输入的数据表名已存在，系统将刷新目标数据库中该数据表中的数据。

   如果输入的数据表名不存在，系统将自动在目标数据库中新建该名称的数据表。

   注意

   如果需要填写已有的数据表，请勿选择业务数据表，以免影响业务。

2. 设置数据目标列名。

   系统默认将生产与数据源列相同的名称，您可以保持默认名称，也可以根据需要进行修改。

步骤10 单击“完成”，完成脱敏规则的编辑。

数据库脱敏任务创建成功后，需运行脱敏任务，系统才会按照设置的脱敏周期执行脱敏任务，运行数据库脱敏任务具体操作请参见**运行数据库脱敏任务**。

----结束

删除数据库脱敏任务

步骤1 登录管理控制台。

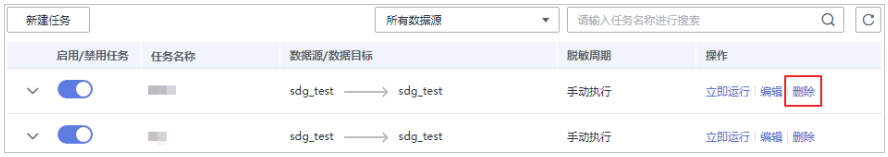
步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全 > 数据安全中心”，进入数据安全中心总览界面。

步骤4 在左侧导航树中选择“数据脱敏”，进入“数据库脱敏”页面。

步骤5 在数据库脱敏任务列表中，在待删除脱敏规则所在行的“操作”列，单击“删除”。

图 6-37 删除数据库脱敏任务



步骤6 在弹出删除任务对话框，单击“确定”。

----结束

6.3.3.2 管理 ES 脱敏任务

操作场景

本章节介绍如何查看、编辑、删除ES源脱敏任务。

前提条件

已创建ES脱敏任务。

查看 ES 脱敏任务

步骤1 登录管理控制台。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全 > 数据安全中心”，进入数据安全中心总览界面。

步骤4 在左侧导航树中选择“数据脱敏”，并选择“ES脱敏”页签，进入ES脱敏页面。

步骤5 在脱敏任务列表中，查看脱敏任务的详细信息，脱敏任务参数说明如表6-7所示。

图 6-38 查看 ES 脱敏任务

说明

输入任务名称或任务名称的关键字，单击或按“Enter”，可以搜索指定的脱敏任务。

表 6-7 脱敏任务参数说明

参数名称	参数说明
启用/禁用任务	启用或禁用脱敏任务。 •  ：启用 •  ：禁用
任务名称	脱敏任务的名称。
数据源/数据目标	脱敏任务的数据源和数据目标。
脱敏周期	脱敏规则的具体执行周期，说明如下： • 手动执行：由用户自行启动的，且基于脱敏规则执行脱敏任务。 • 每小时：每几小时按照脱敏规则执行一次脱敏任务。 • 每天：每天固定时间按照脱敏规则执行一次脱敏任务。 • 每周：每周固定时间按照脱敏规则执行一次脱敏任务。 • 每月：每月固定时间按照脱敏规则执行一次脱敏任务。
操作	用户可以在操作栏中，执行立即运行、编辑、删除等操作。

----结束

编辑 ES 脱敏任务

步骤1 登录管理控制台。

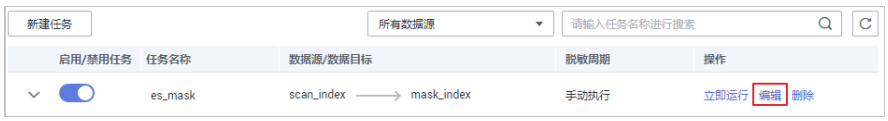
步骤2 单击左上角的  ，选择区域或项目。

步骤3 在左侧导航树中，单击  ，选择“安全 > 数据安全中心”，进入数据安全中心总览界面。

步骤4 在左侧导航树中选择“数据脱敏”，并选择“ES脱敏”页签，进入ES脱敏页面。

步骤5 在ES脱敏任务列表中，在待编辑脱敏规则所在行的“操作”列，单击“编辑”，进入“数据源配置”页面。

图 6-39 编辑 ES 脱敏任务



步骤6 配置数据源，具体参数说明如**表6-8**所示。

图 6-40 数据源配置-ES 脱敏任务

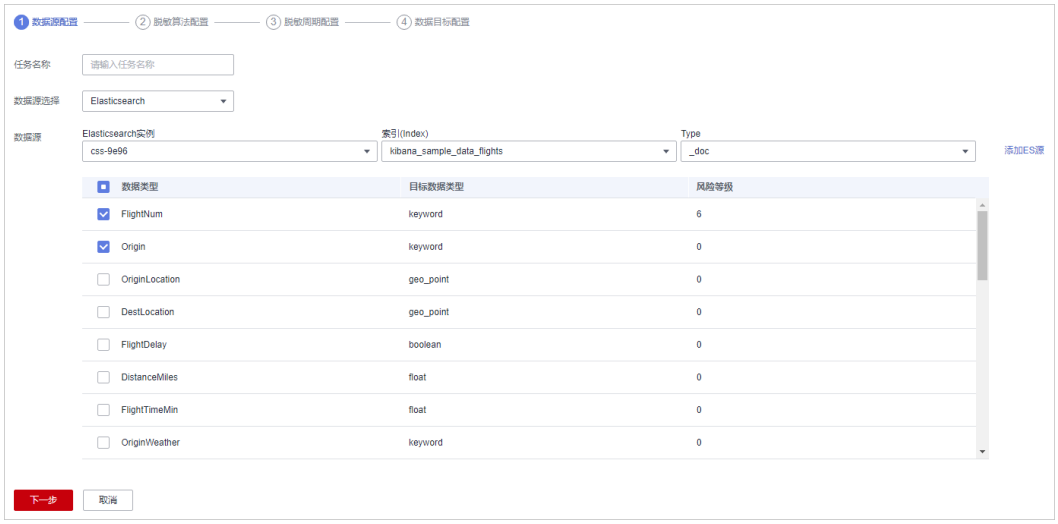


表 6-8 数据源配置参数说明

参数名称	参数说明
任务名称	您可以自定义脱敏任务的名称。 任务名称需要满足以下要求： ● 1~255个字符。 ● 字符可由中文、英文字母、数字、下划线或中划线组成。
数据源选择	选择数据来源。目前仅支持“Elasticsearch”。
数据源 **说明** 如果没有可使用的ES资产，可单击“添加ES源”，添加ES资产，具体的操作可参见**添加大数据源资产**。	Elasticsearch实例：选择脱敏数据所在的Elasticsearch实例。
	索引(Index)：选择脱敏数据所在的索引。
	Type：选择脱敏数据所在的Type。
	Field：勾选后将该列数据拷贝到目标数据库。 此处还显示数据列的“目标数据类型”，“风险等级”。

步骤7 单击“下一步”，进入“脱敏算法配置”页面。

图 6-41 脱敏算法配置-ES 脱敏任务

1. 勾选需要脱敏的Field。
2. 选择脱敏算法。脱敏算法更多详细信息请参见**配置脱敏规则**。

步骤8 单击“下一步”，进入“脱敏周期”页面，配置脱敏周期。

图 6-42 脱敏周期

选择并设置脱敏任务的执行周期：

- 手动：由用户自行启动的，且基于脱敏规则执行脱敏任务。
- 每小时：每几个小时执行一次脱敏任务。
  示例：如果需要每2小时执行一次脱敏任务，则此处设置为：02:00
- 每天：每天几点几分执行一次脱敏任务。
  示例：如果需要每天12:00执行一次脱敏任务，则此处设置为：12:00:00

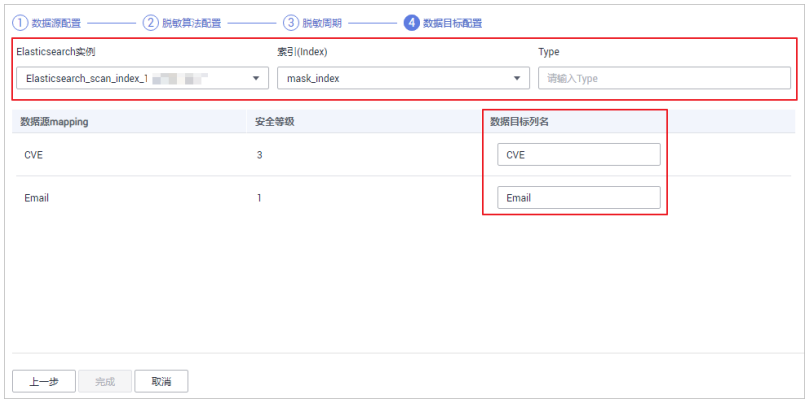
- 每周：每周几的几点几分执行一次脱敏任务。
  示例：如果需要每周一的12:00执行一次脱敏任务，则此处设置为：每周一 12:00:00
- 每月：每月几日几时执行一次脱敏任务。
  示例：如果需要每月12日的12:00执行一次脱敏任务，则此处设置为：每月12日 12:00:00

  说明

  如果设置每月31日执行一次脱敏任务，在当月日期少于31日的情况下，系统自动在当月最后一日执行任务。

步骤9 单击“下一步”，进入“数据目标配置”页面。

图 6-43 数据目标配置-ES 脱敏任务



1. 选择“Elasticsearch实例”、“索引(Index)”，并输入“Type”。
   如果输入的Type已存在，系统将刷新目标数据源中该Type中的数据。
   如果输入的Type不存在，系统将自动在目标数据源中新建该名称的Type。

   注意

   如果需要填写已有的Type，请勿选择业务Type，以免影响业务。

2. 设置数据目标列名。
   系统默认将生成与数据源列相同的名称，您可以保持默认名称，也可以根据需要进行修改。

步骤10 单击“完成”，完成脱敏规则的编辑。

ES脱敏任务创建成功后，需运行脱敏任务，系统才会按照设置的脱敏周期执行脱敏任务，运行ES脱敏任务具体操作请参见**运行ES脱敏任务**。

----结束

删除 ES 脱敏任务

步骤1 登录管理控制台。

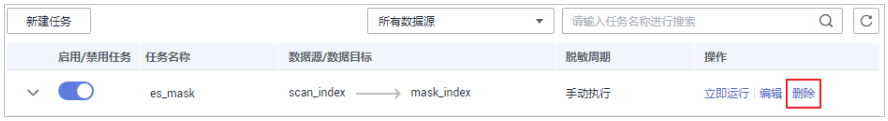
步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全 > 数据安全中心”，进入数据安全中心总览界面。

步骤4 在左侧导航树中选择“数据脱敏”，并选择“ES脱敏”页签，进入ES脱敏页面。

步骤5 在ES脱敏任务列表中，在待删除脱敏规则所在行的“操作”列，单击“删除”。

图 6-44 删除 ES 脱敏任务



步骤6 在弹出删除任务对话框，单击“确定”。

----结束

6.3.3.3 管理 MRS 脱敏任务

本章节介绍如何查看、编辑、删除MRS脱敏任务。

前提条件

已创MRS库脱敏任务。

查看 MRS 脱敏任务

步骤1 登录管理控制台。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全 > 数据安全中心”，进入数据安全中心总览界面。

步骤4 在左侧导航树中选择“数据脱敏”，并选择“MRS脱敏”页签，进入“MRS脱敏”页面。

图 6-45 进入 MRS 脱敏

步骤5 在脱敏任务列表中，查看脱敏任务的详细信息，脱敏任务参数说明如表6-9所示。

说明

输入任务名称或任务名称的关键字，单击或按“Enter”，可以搜索指定的脱敏任务。

表 6-9 脱敏任务参数说明

参数名称	参数说明
启用/禁用任务	启用或禁用脱敏任务。 •  ：启用 •  ：禁用
规则名	脱敏任务的名称。
数据源/数据目标	脱敏任务的数据源和数据目标。
脱敏周期	脱敏规则的具体执行周期，说明如下： • 手动执行：由用户自行启动的，且基于脱敏规则执行脱敏任务。 • 每小时：每几小时按照脱敏规则执行一次脱敏任务。 • 每天：每天固定时间按照脱敏规则执行一次脱敏任务。 • 每周：每周固定时间按照脱敏规则执行一次脱敏任务。 • 每月：每月固定时间按照脱敏规则执行一次脱敏任务。
操作	用户可以在操作栏中，执行立即运行、编辑、删除等操作。

----结束

编辑 MRS 脱敏任务

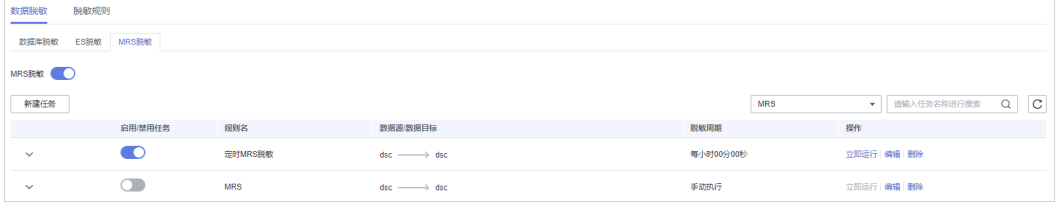
步骤1 登录管理控制台。

步骤2 单击左上角的  ，选择区域或项目。

步骤3 在左侧导航树中，单击  ，选择“安全 > 数据安全中心”，进入数据安全中心总览界面。

步骤4 在左侧导航树中选择“数据脱敏”，并选择“MRS脱敏”页签，进入“MRS脱敏”页面。

图 6-46 进入 MRS 脱敏



步骤5 在MRS脱敏任务列表中，在待编辑脱敏规则所在行的“操作”列，单击“编辑”，进入“数据源配置”页面。

步骤6 配置数据源，具体参数说明如**表6-10**所示。

图 6-47 数据源配置-MRS 脱敏任务

表 6-10 数据源配置参数说明

参数名称	参数说明
任务名称	您可以自定义脱敏任务的名称。 任务名称需要满足以下要求： ● 1~255个字符。 ● 字符可由中文、英文字母、数字、下划线或中划线组成。
数据源选择	选择数据来源。仅支持“MRS_HIVE”。
数据源 **说明** 如果没有可使用的云数据，可单击“添加云数据库”，添加云数据库资产，具体的操作可参见**添加MRS资产**。	数据库实例：选择脱敏数据所在的数据库实例。
	数据库名：选择脱敏数据所在的数据库名称。
	数据表名：选择脱敏数据所在的数据表名称。
	数据类型：勾选后将该列数据拷贝到目标数据库。 此处还显示数据列的“目标数据类型”，“风险等级”。

步骤7 单击“下一步”，进入“脱敏算法配置”页面。

图 6-48 脱敏算法配置-MRS 脱敏任务

1. 勾选需要脱敏的数据列。
2. 选择脱敏算法。脱敏算法更多详细信息请参见**配置脱敏规则**。

步骤8 单击“下一步”，进入“脱敏周期”页面，配置脱敏周期。

图 6-49 脱敏周期

选择并设置脱敏任务的执行周期：

- 手动：由用户自行启动的，且基于脱敏规则执行脱敏任务。
- 每小时：每几个小时执行一次脱敏任务。
  示例：如果需要每2小时执行一次脱敏任务，则此处设置为：02:00
- 每天：每天几点几分执行一次脱敏任务。
  示例：如果需要每天12:00执行一次脱敏任务，则此处设置为：12:00:00
- 每周：每周几的几点几分执行一次脱敏任务。
  示例：如果需要每周一的12:00执行一次脱敏任务，则此处设置为：每周一 12:00:00
- 每月：每月几日几时执行一次脱敏任务。

示例：如果需要每月12日的12:00执行一次脱敏任务，则此处设置为：每月12日12:00:00

说明

如果设置每月31日执行一次脱敏任务，在当月日期少于31日的情况下，系统自动在当月最后一日执行任务。

步骤9 单击“下一步”，进入“数据目标配置”页面。

图 6-50 数据目标配置-MRS 脱敏任务

1. 选择数据库实例、数据库名，并输入数据表名。

   如果输入的数据表名已存在，系统将刷新目标数据库中该数据表中的数据。

   如果输入的数据表名不存在，系统将自动在目标数据库中新建该名称的数据表。

   注意

   如果需要填写已有的数据表，请勿选择业务数据表，以免影响业务。

2. 设置数据目标列名。

   系统默认将生产与数据源列相同的名称，您可以保持默认名称，也可以根据需要进行修改。

步骤10 单击“完成”，完成脱敏规则的编辑。

----结束

删除 MRS 脱敏任务

步骤1 登录管理控制台。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全 > 数据安全中心”，进入数据安全中心总览界面。

步骤4 在左侧导航树中选择“数据脱敏”，并选择“MRS脱敏”页签，进入“MRS脱敏”页面。

图 6-51 进入 MRS 脱敏

步骤5 在MRS脱敏任务列表中，在待删除脱敏规则所在行的“操作”列，单击“删除”。

步骤6 在弹出删除任务对话框，单击“确定”。

----结束

7 数据水印

7.1 概述

数据安全中心提供数据水印能力，帮您把50M以内大小的文件烙上您的专属水印，保证资产唯一归属。

表 7-1 支持的文件类型

支持嵌入/提取水印的文件类型	具体的文件格式
文档	PDF、PPT、Word、Excel
图片	*.jpg、 *.jpeg、 *.jpe、*.png、*.bmp、*.dib、 *.rle、*.tiff、*.tif、*.ppm、*.webp、*.tga、*.tpic、*.gif
json数据	整型、浮点型、字符串型。

使用场景

数字水印广泛适用于政府部门、医疗、金融、科研等单位机构。一般用于**版权保护**、**追踪溯源**。

- **数据版权保护**：数字作品被下载或者复制使用，数据库业务（数据挖掘分析）需要提供数据给第三方，发生纠纷时可以通过数字水印明确版权所属。
- **使用过程可追踪溯源**：数据给内部员工或第三方使用时，打上使用者信息水印，可识别使用者身份，提醒使用者要注意安全规范。当发生数据泄露事件时，可追踪泄露源头，挖掘泄露原因。

优势特点

- 支持**明暗双重水印**：可根据需要对数据打上视觉上看得见的明水印或看不见的暗水印，都不影响使用效果，有效应对图像处理工具或者拍照截图等绕过方式窃取数据。
- **可检测性强**，**不易被篡改**：数据打上水印能够被检测且不会因为数据的改动而导致丢失、伪造或篡改。

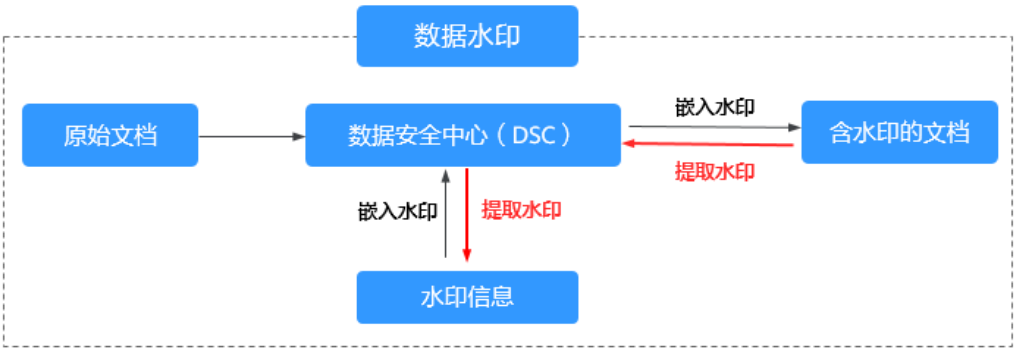
- **高鲁棒性**：水印在传输或使用过程中不易被磨灭掉，数据载体即使经过被改动或受到攻击损坏后，依然有很大概率提取出水印。

使用约束

DSC控制台仅支持对PDF、PPT、Word、Excel格式的文档嵌入和提取水印。

操作流程

图 7-1 数据水印操作流程



7.2 水印注入

数据安全中心控制台针对PDF、PPT、Word、Excel格式文件提供了注入水印的功能，您可以参考本章节对云上文件（文件存储在OBS桶）或者本地文件增加自定义水印内容。

前提条件

文件格式为PDF、PPT、Word、Excel。

约束条件

- 本章节的操作方法仅针对PDF、PPT、Word、Excel格式文件的单个文件注入水印。
- 如果您注入的是暗水印，水印内容不可见，需要用水印工具提取，详细操作请参见**水印提取**。

操作步骤

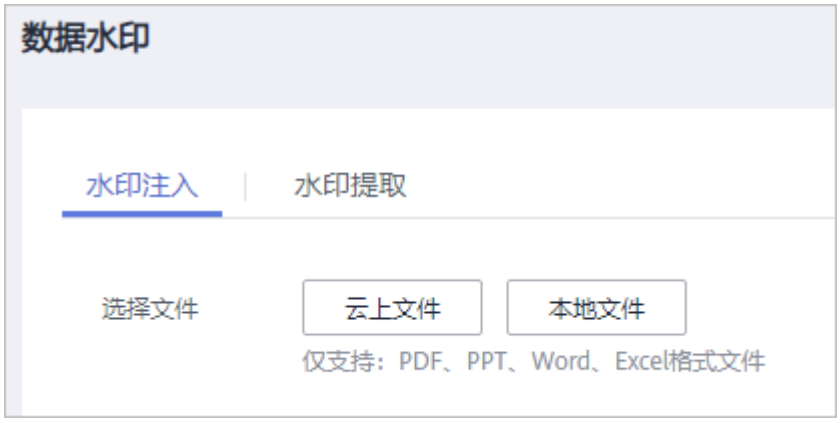
步骤1 登录管理控制台。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全 > 数据安全中心”，进入数据安全中心总览界面。

步骤4 在左侧导航树中选择“数据水印”，进入“水印注入”页面。

图 7-2 水印注入页面



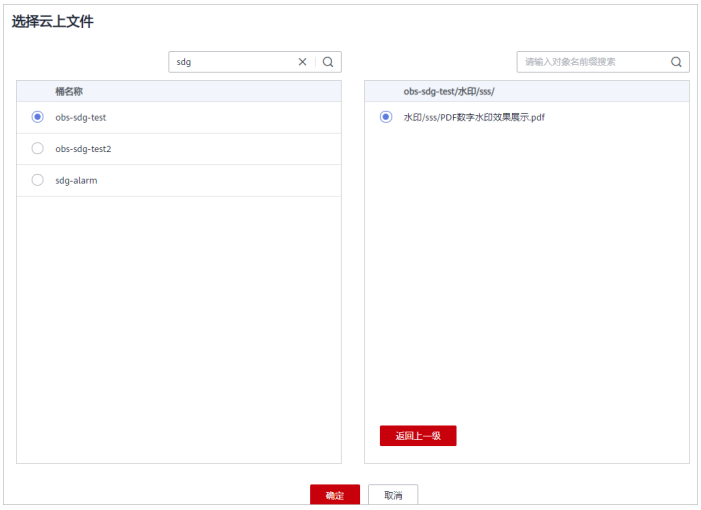
步骤5 选择文件，即上传需要注入水印的文件。

说明

当前DSC服务的控制台仅支持对PDF、PPT、Word、Excel格式文件注入水印。

- 若需要嵌入的文件保存在OBS桶，请单击“云上文件”，选择桶名称和需要增加水印的文件名称，单击“确定”。

图 7-3 选择云上文件



- 若需要嵌入的文件保存在本地，请单击“本地文件”，将本地需要注入水印的文件上传到DSC平台。

步骤6 文件上传成功后，参照**表7-2**配置相关水印参数。

表 7-2 水印设置参数说明

参数名称	参数说明	样例
水印类型	支持“明水印”和“暗水印”，可多选。 • 明水印，水印内容可以展现在文件内容上。 • 暗水印，水印内容不可见，需要水印工具提取，提取暗水印的详细操作请参见**水印提取**章节。	明水印
明水印设置	当“水印类型”选择“明水印”时，需要配置此参数。 根据自己的需要，设置“水印内容”、“字体大小”、“字体角度”、“透明度”。	• 字体大小：45 • 字体角度：46 • 透明度：30
暗水印设置	当“水印类型”选择“暗水印”时，需要配置此参数。 根据自己的需要，设置“水印内容”。	水印内容：ZhangSan

步骤7 参数配置完后，单击“确定”，注入水印的文件会自动下载到您指定的本地路径下。

须知

- 如果您注入的是明水印，可在本地打开水印文件查看效果。
- 如果您注入的是暗水印，水印内容不可见，需要用水印工具提取，详细操作请参见**水印提取**。

----结束

7.3 水印提取

暗水印的水印内容不可见，需要用水印工具提取，数据安全中心控制台针对PDF、PPT、Word、Excel格式文件提供了提取水印的功能，本章节教您如何提取云上文件（文件存储在OBS桶）或者本地文件的水印内容。

前提条件

文件格式为PDF、PPT、Word、Excel。

约束条件

本章节的方法仅针对提取PDF、PPT、Word、Excel格式文件的单个文件的暗水印。

操作步骤

步骤1 登录管理控制台。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全 > 数据安全中心”，进入数据安全中心总览界面。

步骤4 在左侧导航树中选择“数据水印”，在界面左上方，选择“水印提取”页签，进入“水印提取”页面。

图 7-4 水印提取页面

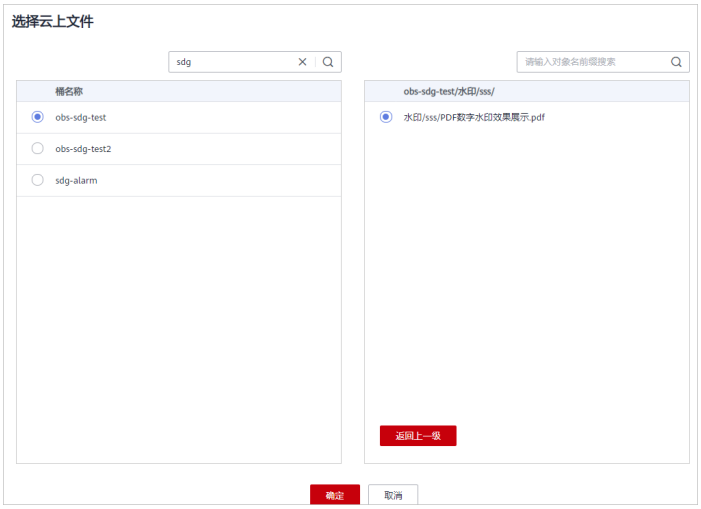
步骤5 选择文件，即上传需要提取暗水印的文件。

说明

当前DSC服务仅支持对PDF、PPT、Word、Excel格式文件提取水印。

- 若需要提取水印的文件保存在OBS桶，请单击“云上文件”，选择桶名称和需要提取暗水印的文件名称，单击“确定”。

图 7-5 选择云上文件



- 若需要提取水印的文件保存在本地，请单击“本地文件”，将本地需要提取暗水印的文件上传到DSC平台。

步骤6 文件上传后，单击“确定”，暗水印内容将展示到弹框中。

图 7-6 水印提取完成

----结束

8 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，数据安全中心将敏感数据检测结果以及异常事件通过用户设置的接收通知方式发送给用户。

前提条件

已开通消息通知服务。

约束条件

- 在使用告警通知前，确认已开通消息通知服务。
- 在设置告警通知前，建议您先以管理员身份在“消息通知服务”中创建“消息主题”。

操作步骤

步骤1 登录管理控制台。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全 > 数据安全中心”，进入数据安全中心总览界面。

步骤4 在左侧导航树中选择“告警通知”，进入告警通知页面。

步骤5 配置告警通知，相关参数说明如表8-1所示。

图 8-1 设置告警通知

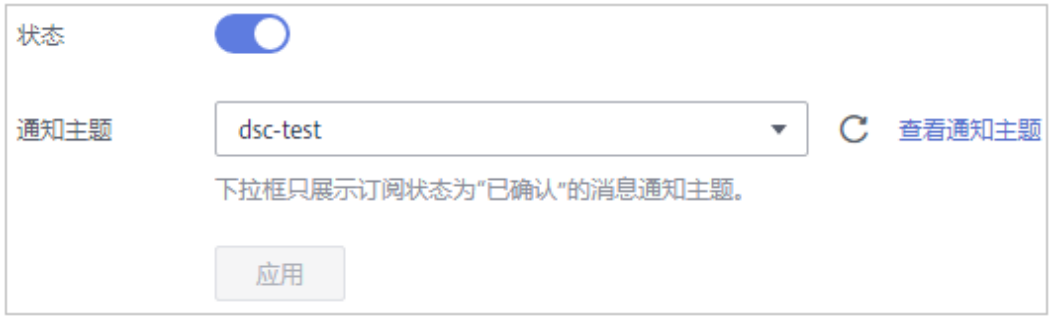


表 8-1 告警通知参数说明

参数名称	说明	取值样例
状态	是否开启通知。 ●  ：开启状态。 ●  ：关闭状态。	
通知主题	单击下拉列表选择已创建消息通知主题或者单击“查看通知主题”创建新的主题，用于配置接收告警通知的终端。 更多关于主题和订阅的信息，请参见《消息通知服务用户指南》。	-

步骤6 单击“应用”。

----结束

9 权限管理

9.1 创建用户并授权使用 DSC

如果您需要对您所拥有的DSC进行精细的权限管理，您可以使用统一身份认证服务（Identity and Access Management，简称IAM），通过IAM，您可以：

- 根据企业的业务组织，在您的帐号中，给企业中不同职能部门的员工创建IAM用户，让员工拥有唯一安全凭证，并使用DSC资源。
- 根据企业用户的职能，设置不同的访问权限，以达到用户之间的权限隔离。
- 将DSC资源委托给更专业、高效的其他帐号或者云服务，这些帐号或者云服务可以根据权限进行代运维。

如果帐号已经能满足您的要求，不需要创建独立的IAM用户，您可以跳过本章节，不影响您使用DSC服务的其它功能。

本章节为您介绍对用户授权的方法，操作流程如图9-1所示。

前提条件

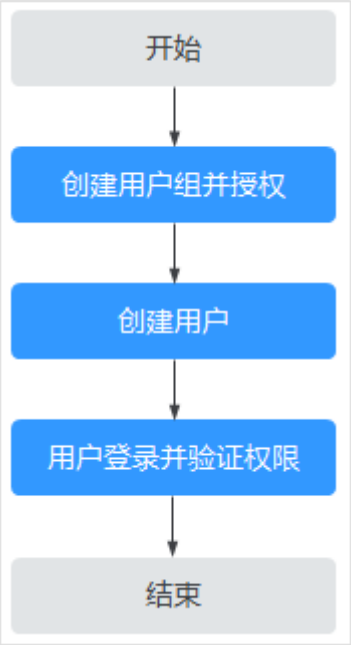
给用户组授权之前，请您了解用户组可以添加的DSC权限，并结合实际需求进行选择，DSC支持的系统权限如表9-1所示。

表 9-1 DSC 系统角色

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	无
DSC ReadOnlyAccess	数据安全中心服务只读权限。	系统策略	无

示例流程

图 9-1 给用户授权服务权限流程



1. 创建用户组并授权
   在IAM控制台创建用户组，并授予数据安全中心权限“DSC FullAccess”。
2. 创建用户并加入用户组
   在IAM控制台创建用户，并将其加入1中创建的用户组。
3. 用户登录并验证权限
   新创建的用户登录控制台，切换至授权区域，验证权限：
   在“服务列表”中选择除数据安全中心外（假设当前策略仅包含“DSC FullAccess”）的任一服务，若提示权限不足，表示“DSC FullAccess”已生效。

9.2 DSC 自定义策略

如果系统预置的DSC权限，不满足您的授权要求，可以创建自定义策略。

目前支持以下两种方式创建自定义策略：

- 可视化视图创建自定义策略：无需了解策略语法，按可视化视图导航栏选择云服务、操作、资源、条件等策略内容，可自动生成策略。
- JSON视图创建自定义策略：可以在选择策略模板后，根据具体需求编辑策略内容；也可以直接在编辑框内编写JSON格式的策略内容。

DSC 自定义策略样例

- 示例1：授权用户查询大数据资产列表

```
{
    "Version": "1.1",
    "Statement": [
        {
```

```
                "Effect": "Allow",
                "Action": [
                    "dsc:bigdataAsset:list"
                                ]
            }
        ]
}
```

- 示例2：拒绝查询OBS资产列表

  拒绝策略需要同时配合其他策略使用，否则没有实际作用。用户被授予的策略中，一个授权项的作用如果同时存在Allow和Deny，则遵循Deny优先。

  如果您给用户授予“DSC FullAccess”的系统策略，但不希望用户拥有“DSC FullAccess”中定义的查询OBS资产列表的权限（dsc:obsAsset:list），您可以创建一条相同Action的自定义策略，并将自定义策略的Effect设置为“Deny”，然后同时将“DSC FullAccess”和拒绝策略授予用户，根据Deny优先原则用户可以对DSC执行除了查询OBS资产列表的所有操作。以下策略样例表示：拒绝用户查询OBS资产列表。

  ```
  {
      "Version": "1.1",
      "Statement": [
          {
              "Effect": "Deny",
              "Action": [
                  "dsc:obsAsset:list"
              ]
          },
      ]
  }
  ```

- 多个授权项策略

  一个自定义策略中可以包含多个授权项，且除了可以包含本服务的授权项外，还可以包含其他服务的授权项，可以包含的其他服务必须跟本服务同属性，即都是项目级服务。多个授权语句策略描述如下：

  ```
  {
      "Version": "1.1",
      "Statement": [
          {
              "Effect": "Allow",
              "Action": [
                  "dsc:obsAsset:list",
                  "dsc:scanRule:list"
              ]
          },
          {
              "Effect": "Allow",
              "Action": [
                  "hss:hosts:switchVersion",
                  "hss:hosts:manualDetect",
                  "hss:manualDetectStatus:get"
              ]
          }
      ]
  }
  ```

9.3 DSC 权限及授权项

如果您需要对您所拥有的DSC进行精细的权限管理，您可以使用统一身份认证服务（Identity and Access Management，IAM），如果登录帐号已经能满足您的要求，不需要创建独立的IAM用户，您可以跳过本章节，不影响您使用DSC服务的其它功能。

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或角色，才能使用户组中的用户获得相应的权限，这一过程称为授权。授权后，用户就可以基于已有权限对云服务进行操作。

权限根据授权的精细程度，分为角色和策略。角色以服务为粒度，是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。策略授权更加精细，可以精确到某个操作、资源和条件，能够满足企业对权限最小化的安全管控要求。

支持的授权项

策略包含系统策略和自定义策略，如果系统策略不满足授权要求，管理员可以创建自定义策略，并通过给用户组授予自定义策略来进行精细的访问控制。

- 权限：允许或拒绝某项操作。
- 授权项：自定义策略中支持的Action，在自定义策略中的Action中写入授权项，可以实现授权项对应的权限功能。

权限	授权项
查询OBS资产列表	dsc:obsAsset:list
更新DSC扫描任务规则	scanRule:update
添加大数据资产	dsc:bigdataAsset:create
查询DSC扫描任务规则列表	dsc:scanRule:list
添加OBS资产	dsc:obsAsset:create
查询rds列表	dsc:rds:list
删除数据库资产	dsc:databaseAsset:delete
创建DSC扫描任务规则	dsc:scanRule:create
删除DSC扫描任务	dsc:scanTask:delete
查询DSC服务授权信息	dsc:authorization:get
查询RDS数据库列表	dsc:rdsDatabase:list
更新DSC扫描任务	dsc:scanTask:update
查询CSS列表	dsc:css:list
创建DSC扫描任务	dsc:scanTask:create
授予DSC服务用户操作权限	dsc:authorization:grant
查询大数据资产列表	dsc:bigdataAsset:list
查询DSC扫描任务列表	dsc:scanTask:list
添加数据库资产	dsc:databaseAsset:create
删除DSC扫描任务规则	dsc:scanRule:delete
查询DSC数据安全总览	dsc:overview:list

权限	授权项
查询数据库资产列表	dsc:databaseAsset:list
删除OBS资产	dsc:obsAsset:delete
删除大数据资产	dsc:bigdataAsset:delete

10 审计

10.1 支持云审计的操作列表

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，具体请参见《云审计服务用户指南》。

云审计服务支持的DSC操作列表如**表10-1**所示。

表 10-1 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

操作名称	资源类型	事件名称
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
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

操作名称	资源类型	事件名称
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
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

10.2 查看审计日志

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。

查看 DSC 的云审计日志

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 单击页面左上方的，在右方的弹框中选择“管理与监管 > 云审计服务 CTS”，进入云审计服务信息页面。

步骤4 单击左侧导航树的“事件列表”，进入事件列表信息页面。

步骤5 事件列表支持通过筛选来查询对应的操作事件。当前事件列表支持四个维度的组合查询，详细信息如下：

- “事件类型”、“事件来源”、“资源类型”和“筛选类型”。
  - “事件类型”选择“管理事件”。
  - “事件来源”选择“DSC”。
  - “筛选类型”选择“按资源ID”时，还需手动输入某个具体的资源ID。
- “操作用户”：在下拉框中选择某一具体的操作用户，此操作用户指用户级别，而非租户级别。
- “事件级别”：可选项为“所有事件级别”、“normal”、“warning”、“incident”，只可选择其中一项。
- “时间范围”：可在页面右上角选择查询最近1小时、最近1天、最近1周及自定义时间段的操作事件。

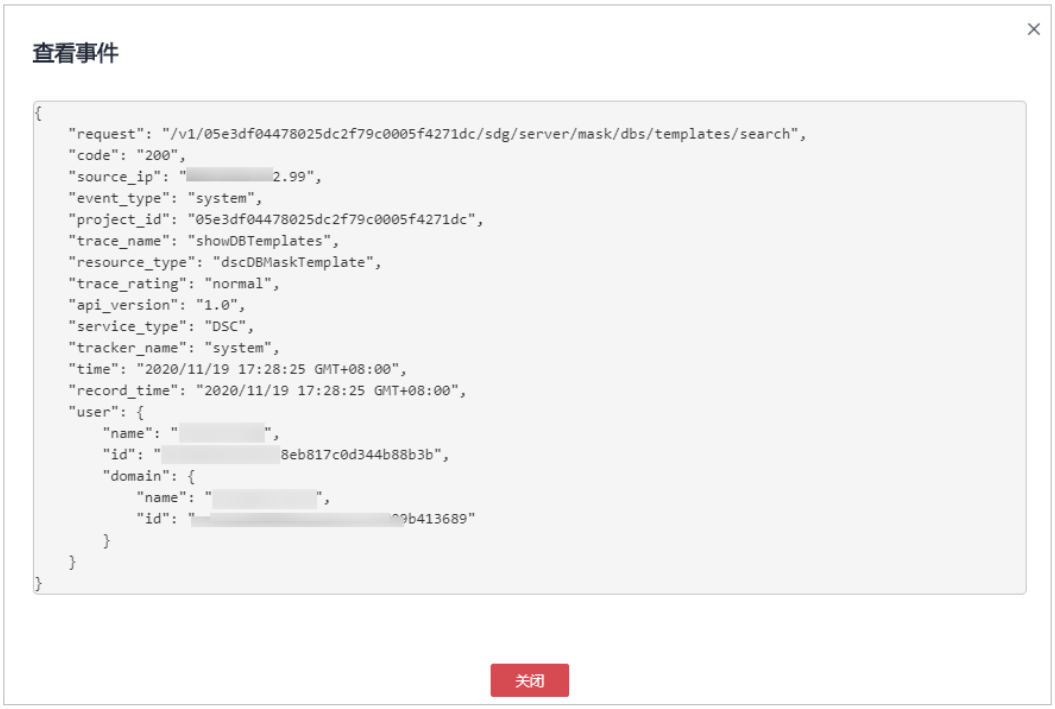
步骤6 单击“查询”，查看对应的操作事件。

步骤7 在需要查看的记录左侧，单击展开该记录的详细信息，展开记录如图10-1所示。

图 10-1 展开记录

步骤8 在需要查看的记录右侧，单击“查看事件”，弹出一个窗口，如图10-2所示，显示了该操作事件结构的详细信息。

图 10-2 查看事件



----结束

11 常见问题

11.1 产品咨询类

11.1.1 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，通过数据安全总览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。

11.1.2 数据安全中心是否会保存您的数据和文件?

数据安全中心（DSC）不会保存您的数据和文件，在您授权访问数据源后，DSC会对数据进行识别、脱敏、或添加水印等操作。

数据识别的结果将展示在DSC的控制台。

11.1.3 DSC 支持解析的非结构化文件类型?

数据安全中心（DSC）支持解析的非结构化文件类型如**表11-1**、**表11-2**和**表11-3**。

表 11-1 文本文档代码类

序号	文件类型	序号	文件类型
1	Access数据库文件	74	Pdf文档
2	Arff文件	75	Perl源代码
3	Asp文件	76	Pgp文件
4	Atom文件	77	Php源代码
5	Bat文件	78	Pkcs7数字证书文件
6	Bcpl源代码	79	Plist文件
7	Bib文件	80	Postgres数据库文件

序号	文件类型	序号	文件类型
8	C#源代码	81	Postscript文档
9	C/C+源代码	82	Powerpoint文档
10	Cad Sldworks文件	83	Properties文件
11	Cad文档	84	Publisher文件
12	Cbor文件	85	Python源代码
13	Cfg文件	86	Quattro-Pro电子表格
14	Chm文件	87	Redis数据库文件
15	Com可执行文件	88	Rss文件
16	Css文件	89	Rtf文档
17	Datax配置文件	90	Ruby源代码
18	Dbf文件	91	R源代码
19	Dif文件	92	Sas7Bdat文件
20	Dita文件	93	Sas文件
21	Djvu文档	94	Scala源代码
22	Dos可执行文件	95	Shell脚本
23	D源代码	96	Sqlite3数据库文件
24	Elf可执行文件	97	Sqlserver数据库文件
25	Epub电子书	98	Sql源代码
26	Excel文档	99	Ssh公钥
27	Fdf文档	100	Ssh配置文件
28	Fictionbook Xml文件	101	Ssh私钥
29	Ftp会话文件	102	Staroffice文档
30	Gnuccash财务xml文件	103	Swift源代码
31	Go源代码	104	Tab文件
32	Groovy源代码	105	Tcl源代码
33	Hdr文件	106	Text文件
34	Hocon文件	107	Tff文件
35	Html文件	108	Tnef文件
36	Htm文件	109	Tomcat Application配置文件

序号	文件类型	序号	文件类型
37	Hwp文件	110	Tomcat Users配置文件
38	Ibooks文件	111	Tomcat配置文件
39	Iis配置文件	112	Toml文件
40	Ini 文件	113	Tsd文件
41	Isa-Tab文件	114	Tsv文件
42	Iwork文档	115	Vcs文件
43	Java Jce Keystore文件	116	Visio文档
44	Java Keystore文件	117	Visualbasic源代码
45	Javascript源代码	118	Vrml虚拟现实建模语言代码
46	Java源代码	119	Webarchive文件
47	Json文件	120	Weblogic配置文件
48	Jsp源代码	121	Webvtt文件
49	Latex源代码	122	Windowsinf文件
50	Log日志文件	123	Windows帮助全文搜索引
51	Lua源代码	124	Windows预编译文件
52	Mariadb数据库文件	125	Wordperfect文档
53	Markdown文档	126	Word文档
54	Matlab源代码	127	Wpd文档
55	Mbox文件	128	Wps文档
56	Mhtml文件	129	Xdp文件
57	Microsoft Reader文档	130	Xfdf文件
58	Mongodb数据库文件	131	Xhtml文件
59	Mrs配置文件	132	Xlf文件
60	Msworks文档	133	Xliff文件
61	Mysql数据库文件	134	Xlr文件
62	Netcdf文件	135	Xlz文件
63	Objective-C源代码	136	Xml Sitemap文件
64	Obs配置文件	137	Xml文件
65	Office文档	138	Xmp文件

序号	文件类型	序号	文件类型
66	Onenote文件	139	Xps文档
67	Opendocument文件	140	Xpt文件
68	Openvpn配置文件	141	Yaml文件
69	Oracle数据库文件	142	常见数字证书文件
70	Outlook文件	143	空文件
71	Pascal源代码	144	配置文件windows Initialization
72	Pbm文件	145	其他普通未加密文本文件
73	Pcx文件	146	邮件文档

表 11-2 压缩和二进制类

序号	类型说明	序号	类型说明
1	7Zip文件	26	Lha压缩文件
2	Apk安卓程序	27	Lz4压缩文件
3	Arj文件	28	Lzma压缩文件
4	Ar文件	29	Mat文件
5	Bgp文件	30	Netcdf文件
6	Brotli压缩文件	31	Object文件
7	Bzip2压缩文件	32	Pack200压缩文件
8	Bzip压缩文件	33	Rar压缩文件
9	Cabinet压缩文件	34	Sharelib文件
10	Coredump文件	35	Snappy压缩文件
11	Cpio压缩文件	36	Tar压缩文件
12	Deflate64压缩文件	37	Tcpdump捕获文件
13	Dmg文件	38	Tika-Unix-Dump文件
14	Elf可执行文件	39	Unix压缩文件
15	Gdal文件	40	Xcompress压缩文件
16	Grb文件	41	Xlz压缩文件
17	Grib2文件	42	Xpi Firefox插件安装包
18	Grib文件	43	Xz压缩文件

序号	类型说明	序号	类型说明
19	Gzip文件	44	Zip压缩文件
20	Hdf文件	45	Zlib压缩文件
21	He5文件	46	Zstd压缩文件
22	Iso-19139地理信息文件	47	Zstd字典文件
23	Iso压缩文件	48	Z压缩文件
24	Jar文件	49	可执行文件
25	Java Class文件	50	普通压缩文件

表 11-3 图片类

序号	类型说明	序号	类型说明
1	BMP文件	4	JFIF文件
2	PNM文件	5	JPEG文件
3	PNG文件	6	TIFF文件

11.2 资产添加类

11.2.1 开通云资源授权后，获得了授权资产服务的哪些权限?

开通云资源授权后，可以访问私有OBS桶、数据库、大数据以及数据安全总览，获得了授权资产服务的权限如表11-4所示。

表 11-4 对应授权项服务创建的委托

资产模块	服务策略	作用范围	备注
OBS	OBS Adminstrator	全局	用于配置OBS日志，获取OBS对象列表，下载OBS对象等
	EVS ReadOnlyAccess	区域	用于获取云硬盘列表
	OBS Adminstrator	全局	用于获取OBS服务投递日志
数据库	ECS ReadOnlyAccess	区域	用于获取自建数据库ECS列表

资产模块	服务策略	作用范围	备注
	RDS ReadOnlyAccess	区域	用于获取RDS数据库列表及数据库列表相关信息
	DWS ReadOnlyAccess	区域	用于获取DWS列表
	VPC FullAccess	区域	用于打通网络，VPC的端口创建，安全组规则创建等
	KMS CMKFullAccess	区域	用于使用KMS加密脱敏的场景
大数据	ECS ReadOnlyAccess	区域	用于获取自建大数据ECS列表
	CSS ReadOnlyAccess	区域	用于获取CSS数据集群列表及数据索引等相关信息
	DLI Service User	区域	用于获取DLI队列及数据库
	VPC FullAccess	区域	用于打通网络，VPC的端口创建，安全组规则创建等
	KMS CMKFullAccess	区域	用于使用KMS加密脱敏的场景
数据安全总览	Tenant Guest	区域	用于获取用户涉及数据存储处理等相关云服务的列表等
	OBS Adminstrator	全局	用于配置OBS日志，获取OBS对象列表，下载OBS对象等
	EVS ReadOnlyAccess	区域	用于云硬盘列表获取
	OBS Adminstrator	全局	用于OBS服务投递日志

11.2.2 如何排查数据库资产连通性失败?

数据库添加完成后，该数据库的“连通性”为“检查中”，此时，DSC会测试数据库的连通性，如果数据库的“连通性”为“失败”，请按照以下步骤进行排查：

步骤1 检查添加资产的IP、帐号、密码、数据库名是否正确。

- 不正确，修改添加资产的IP、帐号、密码、数据库名。
- 正确，执行2。

步骤2 检查您资产安全组的出方向是否全部放开。

- 没有全部放开，需要添加出方向规则，安全组的出方向全部放开后再编辑数据库重新添加，如果仍失败，执行3。
- 已全部放开，执行3。

步骤3 检查数据库对应IP子网的可用IP数是否为0。

由于DSC服务需要对数据库进行网络打通，至少需要一个可用IP数。如果数据库对应IP子网的可用IP数为0，则需要在对应数据库服务中添加可用IP。

----结束

11.3 数据识别和数据脱敏

11.3.1 DSC 能够识别哪些数据源对象?

DSC能通过内置规则和自定义规则从OBS、RDS、Elasticsearch、DWS、DLI的海量数据中分析并识别出敏感对象。

DSC支持的数据源如表11-5所示。

表 11-5 支持的数据源

数据源	具体的数据类型	扫描限制
RDS（关系型数据库）	MySQL、SqlServer、PostgreSQL类型。	采样扫描前500行数据。扫描指标QPS为300次/秒。
CSS（云搜索服务）	大数据资产	--
OBS（对象存储服务）	支持200+文件类型。	大于200MB以上的文件不会对其进行扫描；同时如果OBS桶的文件进行了加密，则无法对其扫描。
DWS（数据仓库服务）	--	--
ECS（弹性云服务器）	搭建的Mysql、SqlServer、PostgreSQL、Oracle数据库及ElasticSearch实例。	--
DLI（数据湖探索）	大数据资产	--

11.3.2 DSC 的扫描时长和脱敏时长?

扫描时长

DSC服务扫描的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，表11-6中提供的扫描时长仅作参考。

表 11-6 扫描时长

数据源	数据量	扫描模式	扫描时长
RDS（关系型数据库）	1000张表	快速扫描	5分钟
CSS（云搜索服务）	1000Wdoc	快速扫描	15分钟
OBS（对象存储服务）	100M	快速扫描	1分钟
OBS（对象存储服务）	100M	全量扫描	15分钟

脱敏时长

DSC通过内置和自定义脱敏算法，实现对RDS、ES和MRS数据进行脱敏，一般情况下，脱敏时长如表11-7所示。

表 11-7 脱敏时长

数据源	数据量	脱敏时长
RDS（关系型数据库）	1000W行	40分钟
Elasticsearch实例	1000Wdoc	40分钟
MRS_HIVE	1000W行	40分钟

11.3.3 DSC 支持识别的敏感数据类型?

数据安全中心服务可识别的敏感数据包括敏感图片信息、个人敏感信息、企业敏感信息等七类，具体可识别的敏感数据类型如表11-8所示。

表 11-8 可识别的数据类型

敏感数据分类	数据类型
敏感图片信息	• 身份证图片 • 护照图片

敏感数据分类	数据类型
个人敏感信息	• 身份证 • 银行卡 • 姓名 • 手机号 • 邮箱 • 护照号 • 港澳通行证 • 车牌号 • 电话号码 • 军官司证 • 性别 • 车辆识别代码
企业敏感信息	• 营业执照号码 • 税务登记证号码 • 组织机构代码 • 统一社会信用代码
密钥敏感信息	• PEM证书 • KEY私钥 • AccessKeyId • AccessKeySecret • 哈希密码
设备敏感信息	• IP地址 • MAC地址 • JDBC连接串 • IPv6地址 • IMEI • MEID
位置敏感信息	• 省份 • 城市 • GPS位置 • 地址
通用敏感信息	日期

11.3.4 数据脱敏是否对原始数据有影响?

没有影响。数据脱敏功能只会对数据进行读取，脱敏后保存到您选择的目标位置，不会对源数据进行改动。

11.3.5 DSC 对可识别和脱敏的数据的字符集是否有要求?

DSC对可识别和脱敏的数据字符集没有任何要求。

DSC可以识别的数据源对象：**DSC能够识别哪些数据源对象?** 。

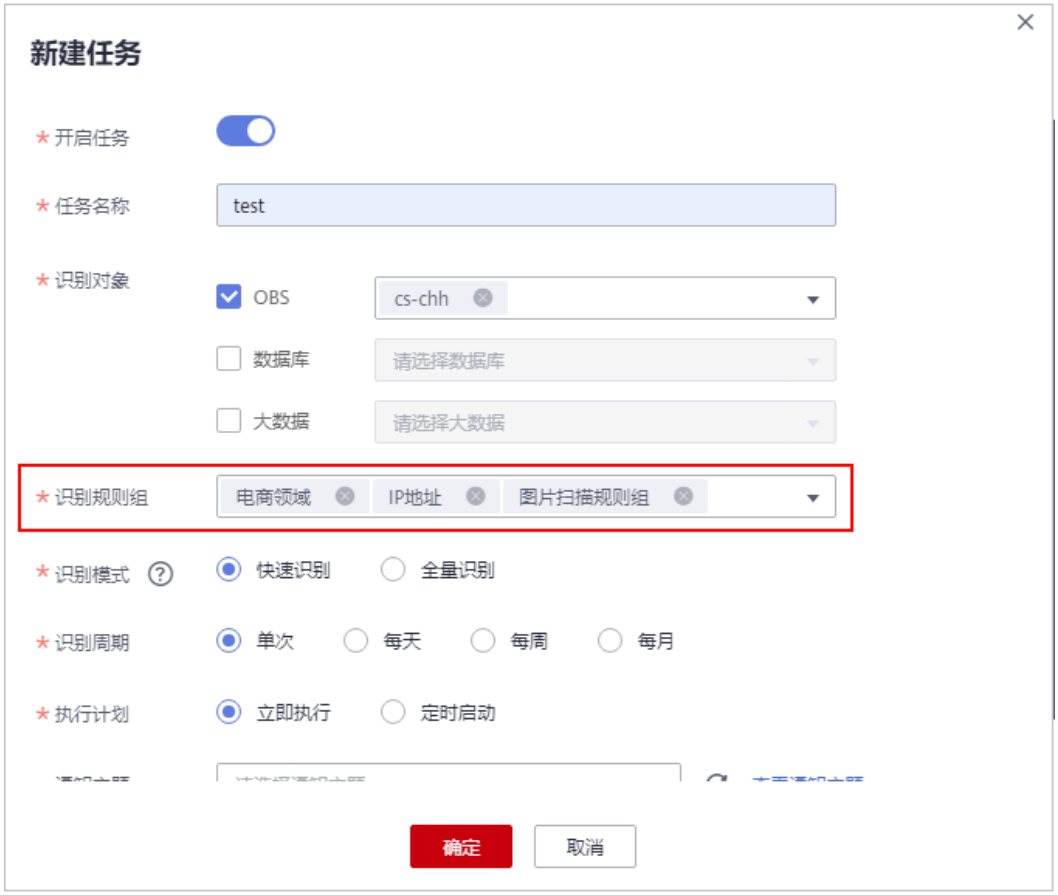
DSC支持识别的敏感数据类型：**DSC支持识别的敏感数据类型?** 。

11.3.6 如何同时启动多个敏感数据识别规则组?

DSC根据不同的场景预置了100+条敏感数据识别和脱敏规则，可对个人敏感信息（身份证、银行卡、姓名、手机号、邮箱等）、企业敏感信息（营业执照号码、税务登录证号码等）、密钥敏感信息（PEM证书、HEY私钥等）、设备敏感信息（IP地址、MAC地址、IPV6地址等）、位置敏感信息（省份、城市、GPS位置、地址等）和通用敏感信息（日期）等敏感信息进行识别和脱敏。

在为同一个资产创建扫描任务时，可添加多个“识别规则组”，同时启动多个敏感数据识别规则，实现为同一资产配置多场景的扫描任务，如图11-1所示。

图 11-1 新建任务



11.4 数据水印类

11.4.1 数据水印功能会不会修改源数据?

数据安全中心服务的数据水印功能不会修改源数据。

使用数据水印功能时，DSC通过调用OBS桶数据或者本地文件，将水印信息嵌入到文件后生成新的文档，该文档会下载到您指定的本地路径，所以对源数据不会有任何影响。

11.4.2 文档损坏后，是否可以提取出水印?

DSC提供的数字水印能力具有高鲁棒性，即水印在传输或使用过程中不易被磨灭掉，数据载体即使经过被改动或受到攻击损坏后，依然有很大概率提取出水印。

- 添加水印后的文档被删除了几页后，仍然可以提取出水印。
- 添加水印后的图片被旋转、剪裁、缩放、修图等形变后，根据形变大小决定，形变较小则可以提取。

11.4.3 对待注入水印的源数据有什么要求?

由于注入水印的原理是将水印原子信息嵌入到不同特征的数据中去，因此源数据特征越多，越能嵌入完整的水印信息、提高提取成功率，并且即使缺失部分数据也不影响水印提取。所以对需要注入水印的数据有如下要求：

- 待注入水印的源数据需要大于等于1000行。

  小于1000行的源数据有可能因为特征不够导致提取水印失败。
- 尽量选取数据取值比较多样的列注入水印，如果该列的值是可枚举穷尽的，则有可能因为特征不够导致提取失败。

  常见的适合嵌入水印的列如地址、姓名、UUID、金额、总数等。

A 修订记录

发布日期	修改说明
2023-03-30	第二次正式发布。 文档补齐常见问题和约束条件。
2022-12-20	第一次正式发布。