天翼云·数据安全中心

用户使用指南

天翼云科技有限公司

目 录

1 产品介绍

1.1 产品定义

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

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
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/存储安全和数据交换/删除安全，实时呈现了用户资产的具体情况。
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进行快速风险处理操作。
资产目录	• 资产列表：DSC 支持管理 OBS、数据库、大数据和 MRS 数据资产。 • 数据目录：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：采集原数据。 • 数据管理：对现有数据进行分组管理。
敏感数据识别	• **数据自动分级分类：**在 AI 和专家知识库的双重加权下，精确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。 – 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。

功能特性	说明
数据风险检测	用户异常行为分析：基于深度行为识别技术，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。 通常情况下，以下行为均被视为异常事件： • 非法用户在未经授权的情况下对敏感数据进行了访问、下载。 • 合法用户对敏感数据进行了访问、下载、修改、权限更改、权限删除。 • 合法用户对敏感数据的桶进行权限更改、权限删除。 • 访问敏感数据的用户登录终端异常等情况。
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。
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。 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。
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。

1.4 术语解释

本文为您介绍数据安全中心的相关名词的主要含义。

API

API（Application Programming Interface，应用程序编程接口）是一些预先定义的函数，应用将自身的服务能力封装成 API，并通过 API 网关开放给用户调用。API 包括基本信息、前后端的请求路径和参数以及请求相关协议。

安全风险

安全风险是对资产安全状况的综合评估，反映了一段时间内资产遭受的安全风险。安全风险通常体现为一个量化的数值，便于用户理解目前资产的安全状况，数值大小并不代表资产的绝对安全或危险，仅作为资产遭受攻击严重程度的参考。

数据脱敏

指对某些敏感信息通过脱敏规则进行数据的变形，实现敏感隐私数据的可靠保护。

数据源

是指业务上首次正式发布某项数据的应用系统，经过数据管理专业组织认证，作为唯一数据源头被周边系统调用。

数据库数据库实例（DWS）

一个数据库实例是一个进程以及它控制的数据库文件。在集群的一个物理节点上安装多个数据库实例，集群各节点上所安装的 GTM、CM、CN、DN 统称为实例。一个数据库实例也被称为一个逻辑节点。

数据库实例（RDS）

数据库实例是在云中运行的独立数据库环境。它是 RDS 的基本构建模块。一个数据库实例可以包含多个由数据库用户创建的数据库，并且可以使用与独立数据库实例相同的客户端工具和应用程序进行访问。

索引

数据库索引，是数据库管理系统中一个排序的数据结构，以协助快速查询、更新数据库表中数据。

元数据

用来定义数据的数据。主要是描述数据自身信息，包含源、大小、格式或其它数据特征。数据库字段中，元数据用于理解以及诠释数据仓库的内容。

元数据采集

元数据采集是指获取数据源的元数据，然后将元数据写入到元数据系统中的过程。

云数据库

云数据库是指云服务提供商提供的各种服务化的关系型数据库（RDS）、文档数据库服务（DDS）等。

1.5 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。

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，精确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。

与云审计的关系

云审计（Cloud Trace Service，CTS）记录了 Web 应用防火墙相关的操作事件，方便用户日后的查询、审计和回溯。

表 1-3 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

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

操作名称	资源类型	事件名称
启用/停用 ES 脱敏	dscBigDataMaskSwitch	switchBigDataMaskStatus
获取 ElasticSearch field 信息	dscBigDataMetaData	getESField
添加 ES 脱敏模板	dscBigDataMaskTemplate	addBigDataTemplate
编辑 ES 脱敏模板	dscBigDataMaskTemplate	editBigDataTemplate
删除 ES 脱敏模板	dscBigDataMaskTemplate	deleteBigDataTemplate
查询 ES 脱敏模板列表	dscBigDataMaskTemplate	showBigDataTemplates
启动/停止 ES 脱敏模板	dscBigDataMaskTemplate	operateBigDataTemplate
切换 ES 脱敏模板状态	dscBigDataMaskTemplate	switchBigDataTemplate
启用/停用数据库脱敏	dscDBMaskSwitch	switchDBMaskStatus
获取数据库字段信息	dscDBMetaData	getColumn
添加数据库脱敏模板	dscDBMaskTemplate	addDBTemplate
修改数据库脱敏模板	dscDBMaskTemplate	editDBTemplate
删除数据库脱敏模板	dscDBMaskTemplate	deleteDBTemplate
查询数据库脱敏模板列表	dscDBMaskTemplate	showDBTemplates
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

操作名称	资源类型	事件名称
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）
- 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 1-4 所示。

表 1-4 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

数据库类型	版本
	• 2016_SE、2016_EE、2016_WEB • 2014_SE、2014_EE • 2012_SE、2012_EE、2012_WEB • 2008_R2_EE、2008_R2_WEB
KingBase	V8
DMDBMS	7、8
GaussDB for openGauss	1.4
PostgreSQL	11、10、9.6、9.5、9.4、9.1
Oracle	10、12
DDS	4.2、4.0、3.4
DWS	4.2、4.0、3.4
ElasticSearch	5.x、6.x、7.x
OBS	V3

1.9 用户权限

系统默认提供两种权限策略：系统策略和自定义策略。系统策略是 IAM 预置的策略，用户只能使用不能修改。若系统策略不满足授权要求，用户可以创建自定义策略，自由搭配需要授予的权限集。

用户组配置权限策略后，将用户加入用户组中，可以使该用户获得权限策略中定义的操作权限。

2 开通 DSC

2.1 购买 DSC 服务

DSC 提供两个服务版本：标准版和专业版，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购买数据安全中心服务。

前提条件

已通过 IAM 对用户绑定“DSC FullAccess”权限的用户组。

约束条件

- DSC 不支持降低购买版本的规格。如果您需要降低购买的 DSC 规格，您可以先退订当前的 DSC，再重新购买较低版本的 DSC。
- 数据库扩展包和 OBS 扩展包与 DSC 版本绑定，不能单独续费或退订。

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、DLI、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”。

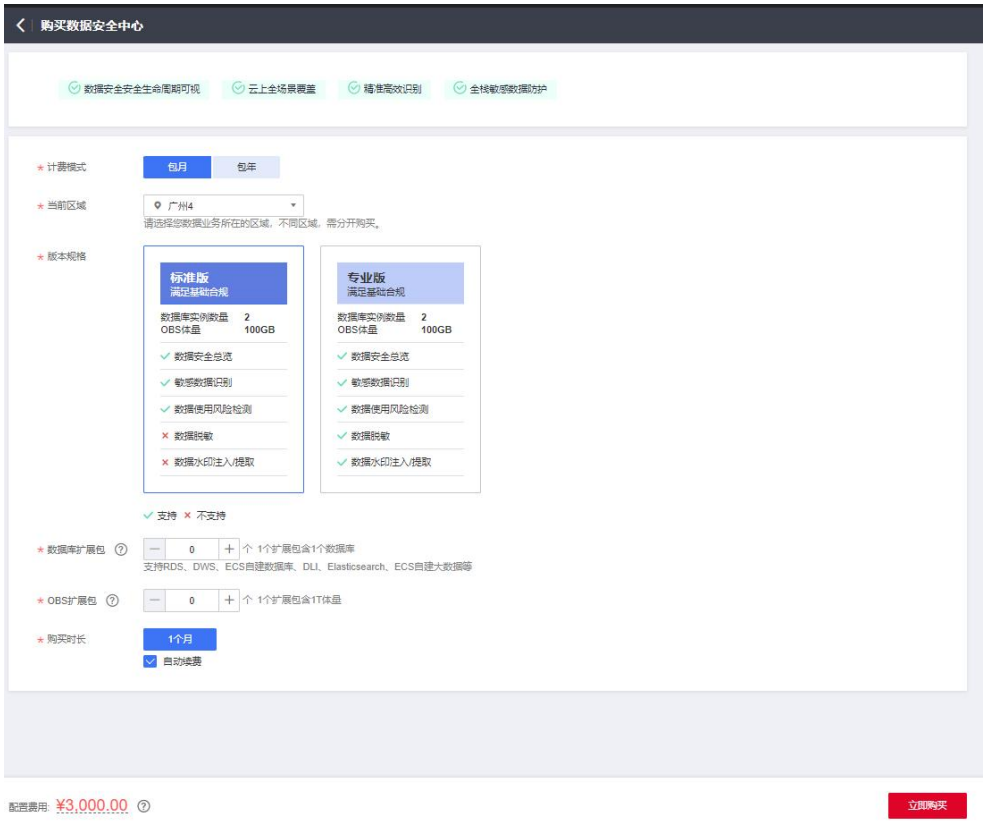
步骤 5 选择“数据库扩展包”和“OBS 扩展包”的数量。

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

步骤 6 选择“购买时长”。单击时间轴的点，选择购买时长 ，可以选择 1 个月～3 年的时长。

图 2-2 购买时长



说明

勾选“自动续费”后，当服务期满时，系统会自动按照购买周期进行续费。

步骤 7 在页面的右下角，单击“立即购买”。

步骤 8 确认订单无误后，阅读并勾选“我已阅读并同意《数据安全中心免责声明》”，单击“去支付”。

图 2-3 详情页面

步骤 9 进入“付款”页面，请选择付款方式进行付款。

----结束

2.2 升级规格

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、DLI、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 选择“数据库扩展包”和“OBS 扩展包”的数量。

图 2-4 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、DLI、Elasticsearch、ECS 自建大数据等）资产。
- 1 个 OBS 扩展包含 1T 体量，即 1024G。

步骤 6 在页面的右下角，单击“立即购买”。

----结束

3 数据安全概览

总览页面分为云服务全景图、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。

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。

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。

步骤 6 查看数据安全中心服务的总览—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，为了避免您的资产存在不必要的存储安全风险，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。

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。

步骤 8 查看数据安全中心服务的总览—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 8.1.3.1 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

4 资产可视化图

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进行快速风险处理操作。

此功能处于公测阶段，公测阶段可免费使用。

前提条件

- 已完成资产访问的授权，参考 5.1.1 云资产委托授权/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“资产地图”进入“资产地图”页面。

步骤 5 查看资产地图。

资产地图可以实现：

- **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。

  说明

  资产地图最多支持显示 1000 个资产。

- **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。

- **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。

  资产地图会显示您当前所有资产的总体安全评分，评分规则请参见资产地图评分规则

步骤 6 单击“风险等级”上面显示的数字，可进入资产风险概览页面，并查看各风险等级下所有的数据库及数据表。

步骤 7 单击资产风险概览下方输入框，可输入数据库或数据表关键词搜索您想要展示的数据库或数据表。

步骤 8 单击想要查看的数据表名称，会在页面右侧弹框展示数据表的详细信息。

说明

- 将鼠标移动到数据资产图标处，也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“敏感数据识别”、或者“ES集群安全防护策略分析”等信息。
- 如您需要对您的云资产授权进行更改，可单击右上角“修改”进行更改。（如需停止授权，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。）

表 4-1 DSC 资产地图参数说明

参数名称	参数说明
风险等级	您的资产存在的风险等级。
数据表总数	数据类型为数据库时显示该参数，数据库的表总数量，可单击“查看详情”进行查看。
扫描文件总数	数据类型为 OBS 时显示该参数，OBS 的文件总数，可单击“查看详情”进行查看。
文档总数	数据类型为 ES 时显示该参数，ES 的文档总数量，可单击“查看详情”进行查看。
敏感文档数	包含敏感信息的文档总数量，可单击“查看详情”进行查看。
最新扫描时间	上次对您的资产进行安全扫描的时间。
分类分级模板	选择内置模板或者自定义模板，DSC 将根据您选择的模板对数据进行分级分类展示。添加模板请参见 6.2.1 新增识别模板。 可单击“查看详情”进行查看。

----结束

资产地图评分规则

一个资产的风险分数=资产的敏感等级*资产的风险等级*系数分

- 资产的敏感等级计算方法：
  - OBS 桶敏感等级为该桶下所有文件敏感等级最大值，数据库/大数据敏感等级为其所有表的敏感等级最大值。
  - 高、中、低等级与旧版分数的对应规则如下：高，8-10；中，4-7；低，1-3。
- 资产的风险等级=MAX（资产静态配置风险等级分，资产动态威胁风险等级分）
  - 资产静态配置风险等级分为资产的安全防护策略分析的安全等级的最大值。
  - 资产动态威胁风险等级分为资产的威胁分析的安全等级的最大值。
  - 风险等级分：
    - 低风险：1 分
    - 中风险：2 分
    - 高风险：3 分
- 系数分与该用户的总资产数相关，具体计算规则如下：
  - 假设用户有 X 个资产，全部是高敏感、高风险的，该用户的资产得分应该是 0，即 X*3*3*Y=100，所以 Y = 100/9X -> Y 即为系数分。
  - 如果 X 个资产全部是低敏感、低风险的，风险分应该为 X*1*1*100/9X=11.1，最终得分为 88.9。
  - 如果 X 个资产全部是中敏感、中风险的，风险分应该为 X*2*2*100/9X = 44.4，最终得分为 55.6。
- 按照上述计算规则，最终得分的高、中、低风险的划分标准如下：
  - 100：无风险
  - 81-99：低风险
  - 51-80：中风险
  - 0-50：高风险

5 资产目录

5.1 资产列表

5.1.1 云资产委托授权/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。

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 5-1 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 Administrator	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 Administrator	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
	GaussDB ReadOnlyAccess	区域	用于获取 GaussDB 列表
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
MRS	MRS CommonOperations	区域	用于集群查询、任务创建等
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 Administrator	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 Administrator	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“资产目录 > 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”。

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 5-2 进行操作。

表 5-2 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：授权访问数据库内的资产。 • 大数据：授权访问云搜索服务（CSS）、数据湖探索（DLI）的资产和 Hive 的资产。 • 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

5.1.2 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 5.1.1 云资产委托授权/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 5-3 所示。

表 5-3 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
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
KingBase	V8
DMDBMS	7、8
GaussDB for openGauss	1.4
PostgreSQL	11、10、9.6、9.5、9.4、9.1
Oracle	10、12
DDS	4.2、4.0、3.4
DWS	4.2、4.0、3.4
ElasticSearch	5.x、6.x、7.x
OBS	V3

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“资产目录 > 资产列表”，进入 OBS 资产列表页面。

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。

步骤 7 单击“确定”，批量添加数据库完成。

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

5.1.3 对象存储 OBS 资产列表

5.1.3.1 添加对象存储 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 5.1.1 云资产委托授权/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“资产目录 > 资产列表”，进入 OBS 资产列表页面。

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。
  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。

c. 单击“确定”。

----结束

相关操作

- OBS 资产授权/停止授权，请参见 5.1.1 云资产委托授权/停止授权章节。
- 删除 OBS 资产，请参见 5.1.3.2 删除 OBS 资产章节。

5.1.3.2 删除对象存储 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 5.1.1 云资产委托授权/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。

⚠ 注意

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“资产目录 > 资产列表”，进入 OBS 资产列表页面。

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

5.1.4 数据库资产清单

5.1.4.1 新增 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 5.1.1 云资产委托授权/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”，且安全组的数量为 1。

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“资产目录 > 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。

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 5-4 配置数据库参数。

表 5-4 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

参数名称	参数说明
	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。

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 5.1.1 云资产委托授权/停止授权章节。
- 删除数据库资产，请参见 5.1.4.4 编辑数据库信息章节。
- 编辑数据库资产，请参见 5.1.4.5 删除数据库资产章节。

5.1.4.2 新增云数据库

如果您已经开通了数据仓库服务（DWS）、文档数据库服务（DDS）或 GaussDB 服务，并已在 DWS、DDS 或 GaussDB 里创建了数据库，可参考本章节直接将 DWS、DDS 和 GaussDB 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 5.1.1 云资产委托授权/停止授权进行操作。
- 已开通 DWS、DDS 或者 GaussDB 服务，且 DWS、DDS 或者 GaussDB 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“资产目录 > 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。

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 5-5 配置数据库参数。

表 5-5 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
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”、“DDS 实例”和“GaussDB 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。	--
GaussDB 实例	在下拉框中选择本帐号下已在 GaussDB 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	--

参数名称	参数说明	举例
	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。

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 5.1.1 云资产委托授权/停止授权章节。
- 删除数据库资产，请参见 5.1.4.4 编辑数据库信息章节。
- 编辑数据库资产，请参见 5.1.4.5 删除数据库资产章节。

5.1.4.3 新增自建数据库

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 5.1.1 云资产委托授权/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 5-6 所示。

表 5-6 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

数据库类型	版本
KingBase	V8
DMDBMS	7、8
GaussDB for openGauss	1.4
PostgreSQL	11、10、9.6、9.5、9.4、9.1
Oracle	11、12
DDS	4.2、4.0、3.4
DWS	4.2、4.0、3.4
ElasticSearch	5.x、6.x、7.x
OBS	V3

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“资产目录 > 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。

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 5-7 配置数据库参数。

表 5-7 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	MySQL

参数名称	参数说明	取值样例
	“Oracle”。	
版本	选择数据库引擎对应的版本。	5.6
模式名	输入数据库模式名。	-
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。	-
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，并展示在已授权的数据库列表中。

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 5.1.1 云资产委托授权/停止授权章节。
- 删除数据库资产，请参见 5.1.4.4 编辑数据库信息章节。
- 编辑数据库资产，请参见 5.1.4.5 删除数据库资产章节。

5.1.4.4 配置数据库信息

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 5.1.1 云资产委托授权/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“资产目录 > 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。

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

5.1.4.5 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 5.1.1 云资产委托授权/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“资产目录 > 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。

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

5.1.5 大数据资产清单

5.1.5.1 新增大数据源资产

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 5.1.1 云资产委托授权/停止授权进行操作。
- 已开通 CSS 和 DLI 服务，且已有 CSS、DLI 和 Hive 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“资产目录 > 资产列表”，并选择“大数据”页签，进入大数据资产列表页面。

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 5-8 配置大数据源参数。

表 5-8 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 5-9。 • “DLI”，选择此类型时，其	Elasticsearch

参数名称	参数说明	取值样例
	他参数说明请参见表 5-10。 • “Hive”，选择此类型时，其他参数说明请参见表 5-11。	

表 5-9“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 5-10“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 5-11“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

参数名称	参数说明	取值样例
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

5.1.5.2 新增自建大数据源

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 5.1.1 云资产委托授权/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“资产目录 > 资产列表”，并选择“大数据”页签，进入大数据资产列表页面。

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 5-12 配置大数据源参数。

表 5-12 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。	--

参数名称	参数说明	取值样例
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。	9200
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。	--

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

5.1.5.3 配置大数据源资产

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 5.1.1 云资产委托授权/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“资产目录 > 资产列表”，并选择“大数据”页签，进入大数据资产列表页面。

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

5.1.5.4 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 5.1.1 云资产委托授权/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。

⚠ 注意

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“资产目录 > 资产列表”，并选择“大数据”页签，进入大数据资产列表页面。

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

5.1.6 MRS 资产清单

5.1.6.1 新增 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 5.1.1 云资产委托授权/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“资产目录 > 资产列表”，并选择“MRS > 待授权”，进入待授权 MRS 资产列表页面。

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 5-13 配置数据库参数。

表 5-13 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。

参数名称	参数说明
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

5.1.6.2 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 5.1.1 云资产委托授权/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。

⚠ 注意

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“资产目录 > 资产列表”，并选择“MRS > 待授权”，进入待授权 MRS 资产列表页面。

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”。

步骤 6 在弹出的删除资产提示框中，单击“确定”。

----结束

5.2 数据目录

如您需要在数据目录页面查看不同业务域或不同类型数据的统计信息，可参考本章节。

此功能处于公测阶段，公测阶段可免费使用。

前提条件

- 已完成数据库资产委托授权，参考 5.1.1 云资产委托授权/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“资产目录 > 数据目录”，进入“数据目录”页面。

步骤 5 在“业务域”或“数据类型”页签查看已经添加的数据资产信息，相关参数说明如表 5-14。

您可以在业务域页签左侧导航栏，选择分组展示您想要查看的数据资产，或在数据类型页签左侧导航栏选择数据类型展示您想要查看的数据资产。

表 5-14 数据目录参数说明

参数名称	参数说明
统计信息	• 敏感数据库占比：统计敏感数据库在所有数据库中的占比 • 敏感数据表占比：统计敏感数据表在所有数据表中的占比 • 敏感数据列占比：统计敏感数据列在所有数据列中的占比 说明 周同比表示同比上周数据发生的变化。
敏感列占比	体现不同密级敏感数据列在数据列总量中占比的饼状图

参数名称	参数说明
分类结果 TOP5	分类结果占比最高的 TOP5 类型
数据量变化	体现数据量随时间变化的曲线图
库量级表	• 数据库实例：数据库实例名称 • 实例 ID：实例 ID • 主机端口：主机端口号 • 用户：用户名

----结束

5.3 数据探索

您可在数据探索页面查看您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。

此功能处于公测阶段，公测阶段可免费使用。

前提条件

- 已完成数据库资产委托授权，参考 5.1.1 云资产委托授权/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“资产目录 > 数据探索”，进入“数据探索”页面。

步骤 5 在搜索框输入数据库名、数据库表名、数据表列名或模式名来搜索您想要查看的数据库信息。

您还可以在搜索框底部选择模板、模板分类和密级等筛选您想要查看的某类数据库信息。

步骤 6 单击数据库名称，进入数据库详情页面，您可以对数据库、数据表以及数据视图等添加描述、标签、密级和分类等。

----结束

5.4 元数据任务

5.4.1 新建元数据采集任务

本章介绍如何创建元数据采集任务。此功能处于公测阶段，公测阶段可免费使用。

前提条件

已完成数据库资产委托授权，参考 5.1.1 云资产委托授权/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“资产目录 > 元数据任务”，进入“元数据采集任务”页面。

步骤 5 在“元数据采集任务”页面，单击“新建”，进入“新建采集任务 > 数据源配置”页面，具体参数说明如表 5-15 所示。

表 5-15 数据源配置参数说明

参数名	参数说明
选择数据源	选择数据来源。可选择“MySQL”、“PostgreSQL”、“DMDBMS”、“KingBase”、“OpenGuass”。
数据库实例	选择支持的数据库实例。

步骤 6 单击“下一步”，进入“子任务配置”页面：

- 选择开启或关闭“扫描用户表”。
- 选择开启或关闭“扫描系统表”。
- 选择开启或关闭“扫描列约束”。
- 选择开启或关闭“扫描视图”。
- 选择开启或关闭“扫描列注释”。
- 选择开启或关闭“扫描权限”

步骤 7 单击“下一步”，进入“任务信息配置”页面，配置任务信息，参数说明请参见表 5-16。

表 5-16 任务信息配置参数说明

参数名称	参数说明
任务信息	• 任务名称：必填项， 您可以自定义采集任务的名称。 • 任务描述：非必填项，对您的采集任务进行描述。
任务配置	选择开启  或关闭  “删除联通性失败的元数据”。
执行计划	• 识别周期：您可以选择“单次”、“每日”、“每周”或“每月”。 • 执行计划：您可以选择“立即执行”或“定时启动”。

步骤 8 单击“下一步”，进入“配置确认”页面，确认您已经配置好的参数。

步骤 9 确认无误后单击“完成”，即可成功创建一个新的元数据采集任务。

----结束

5.4.2 运行元数据采集任务

对于已创建成功的元数据采集任务，您可以在任务列表进行查看并运行。

前提条件

- 已完成数据库资产委托授权，参考 5.1.1 云资产委托授权/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“资产目录 > 元数据任务”，进入“元数据采集任务”页面。

表 5-17 元数据采集任务参数说明

参数名称	参数说明

参数名称	参数说明
名称	元数据采集任务名称
启用/禁用任务	启用或禁用当前任务
子任务	子任务名称
调度策略	可选择“单次”、“每日”、“每周”或“每月”
创建人	任务的创建人 ID
最后运行时间	任务的最后运行时间

步骤 5 单击操作栏“运行”，开始运行当前创建的元数据采集任务。

步骤 6 单击元数据采集任务左侧 ，可查看任务的运行详情，参数说明请参见表 5-18。

表 5-18 元数据任务详情参数说明

参数名称	参数说明
开始时间	任务开始运行的时间
结束时间	任务运行结束的时间
执行方式	“单次”、“每日”、“每周”或“每月”
状态	当前任务运行的状态，任务状态分为： • 已完成：已完成元数据采集任务。 • 运行中：正在运行元数据采集任务。 • 运行失败：元数据采集任务运行失败。 • 调度中：元数据采集任务已添加成功，待运行。 • 部分完成：已完成部分元数据采集任务。
运行时长	任务开始运行到结束运行用的时间

----结束

相关操作

您还可以在任务的操作栏对当前元数据采集任务进行“编辑”或“删除”操作。

5.5 数据管理

本章节介绍如何对现有数据进行分组管理操作。

此功能处于公测阶段，公测阶段可免费使用。

前提条件

- 已完成数据库资产委托授权，参考 5.1.1 云资产委托授权/停止授权进行操作。
- 已添加数据库资产。

新建数据库分组

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“资产目录 > 数据管理”，进入“数据管理”页面。

步骤 5 将鼠标滑动至全域数据库列表的分组名称处，单击创建子级分组，系统弹出“添加标签”弹窗。

步骤 6 自定义标签名称（即分组名称），单击“确定”，创建分组成功。

----结束

管理数据库分组

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“资产目录 > 数据管理”，进入“数据管理”页面。

步骤 5 在全域数据列表选择需要管理的分组，并在右侧页面单击展开数据库实例详情。

步骤 6 勾选待移动数据库，单击待移动数据库所在行操作列“移动到”，在“移动到”弹窗中选择目标分组。

步骤 7 单击“确定”，为数据库重新分组成功。

----结束

删除数据库分组

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“资产目录 > 数据管理”，进入“数据管理”页面。

步骤 5 将鼠标滑动至全域数据库列表的分组名称处，单击删除分组，系统弹出“确认要删除标签”弹窗。

步骤 6 单击“确定”，删除数据库分组。

----结束

6 敏感数据识别（新）

6.1 敏感数据识别简介

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。

新版敏感数据识别是采用分级分类模板对扫描后的数据进行分类分级，方便查看和处理同类异常事件。可以在新的敏感数据识别任务页面左上角单击“进入旧版敏感数据识别页面”进行新旧版敏感数据识别切换。此功能处于公测阶段，公测阶段可免费使用。

使用约束

对于 MRS 中的 HIVE 数据，在敏感数据识别时，当前仅支持“匹配类型”为“规则匹配”、“规则”为“内容 > 包含”的方式。

使用流程

表 6-1 功能介绍

功能	描述	相关操作
识别规则	拥有内置的规则可供使用，同时可以自定义新的规则，将零散的数据按照识别规则进行分类，是创建识别模板必须的配置项。	6.2.3 新建自定义规则
级别配置	拥有内置的级别可供使用，同时可以自定义新的级别，将每条规则进行分级。	6.2.5 新增分级
识别模板	拥有内置的模板供使用，同时可以自定义新的分类分级模板，将多个零散的规则进行统一分级分类管理，是创建识别任务必须的配置项。	6.2.1 新增识别模板

功能	描述	相关操作
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。	6.3.1 新建敏感数据识别任务
查看识别结果	识别任务扫描完成后，可在识别任务列表查看识别结果，根据识别结果处理异常事件。	6.3.4 查看识别结果

6.2 敏感数据识别配置

6.2.1 新建识别模板

DSC 默认内置一个识别模板，同时支持通过复制模板来自定义新的识别模板。如果您需要新增分类分级模板请参考此章节操作。

约束限制

- 识别模板创建后不支持删除。
- 一个帐号最多可创建 20 个识别模板。

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 > 识别配置”，进入识别模板页签。

步骤 5 在目标模板单击“复制”，在复制模板弹框中填写“新模板名称”和“描述”。

步骤 6 单击“确定”。

----结束

相关操作

- 单击“设为默认”，可将该模板设置为默认模板。
- 单击模板“概览”查看模板分类分级详情。

6.2.2 配置识别模板

自定义模板支持修改模板内容，如果您需要修改模板内容，请按照编辑分类分级模板操作。

模板的规则分类支持修改，如果您需要修改规则分类，请按照修改模板规则分类操作。

约束限制

内置模板不支持编辑修改。

编辑识别模板

步骤 1 登录管理控制台。

步骤 2 使用浏览器，以 VDC 管理员或 VDC 业务员帐号登录 ManageOne。

步骤 3 单击左上角的，选择区域或项目。

步骤 4 在左侧导航树中，单击，选择选择“安全 > 数据安全中心”，进入数据安全中心总览界面。

步骤 5 在左侧导航树中选择“敏感数据识别 > 识别配置”，进入识别模板页签。

步骤 6 单击目标模板的“详情”进入模板详情界面。

- 鼠标移动至“分类名称”时：
  - 单击创建新的分类名称。
  - 单击编辑分类名称。
  - 单击删除分类名称。
- 单击左侧“分类名称”，在右侧查看相关分类规则，支持多选。
- 右侧分类规则列表左上角单击“添加规则”，具体参见 6.2.3 新建自定义规则章节。
- 单击“批量删除”，删除右侧勾选的规则。
- 单击“状态”列可以选择打开或者关闭此条规则。
- 单击“操作”列“查看详情”，可以编辑规则内容。
- 单击“操作”列“删除”，删除规则。

----结束

修改模板规则分类

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 > 识别配置”，进入识别模板页签。

步骤 5 单击目标模板的“详情”进入模板详情界面。

步骤 6 单击列表选择规则，支持多选。

步骤 7 在规则列表左上角单击“修改分类”，在修改分类的弹框中选择目标分类。

步骤 8 单击“确定”，提示规则分类修改成功。

----结束

6.2.3 新增自定义规则

敏感数据识别规则有系统内置的规则，同时支持用户自定义规则。可在新增和编辑识别模板时选择内置或者自定义的识别规则。

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 > 识别配置”，进入识别模板页签。

步骤 5 选择“识别规则”页签，进入识别规则界面。

步骤 6 单击界面左上角“新建自定义规则”，弹出“添加规则”弹框。

步骤 7 请参照表 6-2 表配置相关参数。

表 6-2 添加规则参数配置说明

参数	说明
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、中划线和括号组成。

参数	说明
	• 规则名称不能与已有的规则名称重复。
描述（可选）	请输入规则描述。
添加到模板	• 在下拉框中依次选择“模板名称”、“模板规则分类”、“级别”将规则添加到规则模板中进行分类管理。 • 单击 添加 可添加到多个模板。 • 单击删除模板，至少保留一条模板。
匹配类型	可选择“规则匹配”和“关键字匹配”。 • 关键字匹配：通过关键字来执行该条敏感规则。 • 规则匹配：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。 **说明** 对于 MRS 中的 HIVE 数据，在敏感数据识别时，当前仅支持“匹配类型”为“规则匹配”、“规则”为“内容 > 包含”的方式。
匹配逻辑	选择匹配逻辑： • AND：关键字都需要包含。 • OR：仅需要包含其中一个关键字。
规则	• “匹配类型”设置为“规则匹配”时，显示该参数。 • 单击 十添加 添加多条规则。 • 单击删除规则，至少保留一条规则。 **说明** 对于 MRS 中的 HIVE 数据，在敏感数据识别时，当前仅支持“匹配类型”为“规则匹配”、“规则”为“内容 > 包含”的方式。
内容	• “匹配类型”设置为“关键字匹配”时，显示该参数。 • 通过回车换行分隔多个关键字。
识别阈值配置	适用于非结构化数据，可单击 选择低、中、高三种阈值，阈值越高要求命中的次数越多。
命中率	适用于结构化数据，可拖动滑块设置。

步骤 8 单击“确认”完成新建规则。

----结束

6.2.4 配置规则

约束限制

内置规则不支持编辑。

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 > 识别配置”，进入识别模板页签。

步骤 5 选择“识别规则”页签，进入识别规则界面。

步骤 6 在目标规则操作列单击“详情”查看并修改规则。支持修改的参数有“规则基础信息”、“添加到模板”、“匹配条件”和“识别阈值配置”。

----结束

相关操作

如果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目标规则操作列单击“删除”，删除该规则。

- 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。

6.2.5 新建分级

DSC 内置有 L1-L4 四种敏感数据级别，如果内置级别无法满足您的需要，可以根据此章节进行自定义级别。

约束限制

级别创建后不支持删除。

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 > 识别配置”，进入识别模板页签。

步骤 5 选择“级别配置”页签，在级别配置列表左上角单击“新增分级”。

步骤 6 在“新增分级”弹框中配置相关信息，参数说明如表 6-3。

表 6-3 新增级别参数说明

参数	说明
级别名称	输入自定义的级别名称。
级别颜色	可根据敏感等级选择级别颜色，级别颜色数值越高敏感度越高。 如姓名、性别等为低敏感数据；身份证号、加密密钥等为高敏感数据。

步骤 7 单击“确定”完成新增规则。

----结束

6.2.6 配置分级内容

如果您需要修改级别信息，请按照此章节进行操作。

前提条件

级别来源为自定义。

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 > 识别配置”，进入识别模板页签。

步骤 5 选择“级别配置”页签查看级别配置列表。

步骤 6 在目标级别操作列，单击“编辑”修改级别内容。

步骤 7 单击“确定”保存修改内容。

----结束

6.2.7 禁用分级

如果您需要禁用级别，请按照此章节进行操作。

约束限制

内置级别不支持禁用。

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 > 识别配置”，进入识别模板页签。

步骤 5 选择“级别配置”页签查看级别配置列表。

步骤 6 在目标级别操作列，单击“禁用”。

说明

- 禁用的级别在新增或者编辑模板时不会显示。
- 如果需要解除禁用，请在对应级别操作列单击“启用”。

----结束

6.3 敏感数据识别任务

6.3.1 新增敏感数据识别任务

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。

前提条件

已添加 OBS、数据库、大数据源资产或 MRS，具体操作请参见 5.1 资产列表。

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（新） > 识别任务”，进入识别任务界面。

步骤 5 在任务列表左上角，单击“新建任务”。

步骤 6 在弹出的“新建任务”的对话框中，参照表 6-4 配置相关参数。

表 6-4 新建任务参数说明

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： • 4~255 个字符。 • 字符可由中文、英文字母、数字、下划线或中划线组成。 • 开头需为中文或者字母。 • 任务名称不能与已有的任务名称重复。	Test 任务_01
数据类型	选择识别的数据类型，可多选。 • OBS：授权 DSC 访问您的 OBS 资产后，DSC 将对 OBS 里的资产进行敏感数据识别，添加 OBS 资产的相关操作请参见 5.1.3 OBS 资产列表。 • 数据库：授权 DSC 访问您的数据库，DSC 将对数据库资产进行敏感数据识别，添加数据库资产的相关操作请参见 5.1.4 数据库资产列表。 • 大数据：授权 DSC 访问您的大数据源资产后，DSC 将支持对相关资产进行敏感数据识别，添加大数据源资产请参见 5.1.5 大数据资产列表。 • MRS：授权 DSC 访问您的 Hive 资产后，DSC 将支持对相关资产进行敏感数据识别，相关操作请参见 5.1.6 MRS 资产列表。	数据库
识别模板	选择内置模板或者自定义模板，DSC 将根据您选择的模板对数据进行分级分类展示。添	数据安全分类分级模板

参数	说明	取值样例
	加模板请参见 6.2.1 新增识别模板。	
识别周期	设置数据识别任务的执行策略： • 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，即在每天的固定时间执行该识别任务。 • 每周：选择该选项，即在设定的每周这一时间点执行该识别任务。 • 每月：选择该选项，即在设定的每月这一时间点执行该识别任务。	单次
执行计划	“识别周期”为“单次”时，显示该选项： • 立即执行：选择该选项，单击“确定”，系统立即执行数据识别任务。 • 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	“识别周期”为“每天”、“每周”、“每月”时显示该选项： 选择识别任务执行时间。选择时间后，该任务在每天、每周、每月或者当前时间点执行此识别任务。	/04/13 10:36:26

步骤 7 单击“确定”，界面右上角提示创建任务成功，即识别任务创建成功。

----结束

后续处理

6.3.4 查看识别结果：敏感数据识别任务扫描完成后，可在识别任务列表目标任务操作列单击“识别结果”，查看数据资产的敏感信息总数、风险等级以及敏感信息分类分级结果。

6.3.2 启动识别任务

DSC 可重复执行识别任务，如果您需要对数据进行再一次的扫描，可参考本章节启动识别任务。

前提条件

已添加 OBS、数据库、大数据源资产或 MRS，具体操作请参见 5.1 资产列表。

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（新） > 识别任务”，进入识别任务界面。

步骤 5 在待启动任务行的“操作”列单击“立即识别”，右上角弹框提示扫描任务开始扫描，即执行成功。

说明

如果您需要停止正在执行的任务，请在目标任务“操作”列，单击“停止”。

----结束

后续处理

6.3.4 查看识别结果：敏感数据识别任务扫描完成后，可在识别任务列表目标任务操作列单击“识别结果”，查看数据资产的敏感信息总数、风险等级以及敏感信息分类分级结果。

6.3.3 识别任务列表

在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

已添加 OBS、数据库、大数据源资产或 MRS，具体操作请参见 5.1 资产列表。

查看识别任务列表

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，单击“敏感数据识别（新） > 识别任务”，进入识别任务界面查看任务详情，相关参数如表 6-5。

表 6-5 识别任务参数

参数	说明

参数	说明
任务名称	识别任务名称。 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扫描结果。 • 单击“删除”，删除该任务下具体对象。
识别模板	识别模板名称。
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：每周固定时间执行一次识别任务。 • 每月：每月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：识别任务在队列中，等待识别。 • 识别中：正在执行的识别任务。 • 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，包含内置级别和自定义级别，详情参见 6.2.5 新增分级章节。
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，具体的参见 6.3.2 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“ 结果明细”页面，DSC 为您提供了详细的结果分析报告，具体的参见 6.3.4 查看识别结果章节。 • 开启任务，当该任务处于关闭状态时，单击“更多 > 开启任务”，具体请参见 6.3.2 立即启动识别任务章节。 • 关闭任务，当该任务处于开启状态时，单击“更多 > 关闭任务”，具体请参见关闭识别任务。 • 编辑扫描任务，单击“更多 > 编辑”，具体请参见编辑识别任务。

参数	说明
	• 删除扫描任务，单击“更多 > 删除”，具体请参见删除识别任务。

----结束

编辑识别任务

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（新） > 识别任务”，进入识别任务界面。

步骤 5 在目标任务“操作”列单击“更多 > 编辑”进入“编辑任务”弹框。

步骤 6 在弹框中编辑和修改任务内容，单击“确定”保存。

----结束

删除识别任务

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（新） > 识别任务”，进入识别任务界面。

步骤 5 在目标任务“操作”列单击“更多 > 删除”。

步骤 6 在确认删除的弹框中单击“确定”，删除此任务。

⚠ 注意

- 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。

----结束

关闭识别任务

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（新） > 识别任务”，进入识别任务界面。

步骤 5 在目标任务的“操作”列，单击“更多 > 关闭任务”。

说明

- 状态在“识别中”的任务无法关闭任务。
- 关闭的任务名称显示灰色，显示任务已关闭。
- 如需开启该任务，请在目标任务“操作”列单击“更多 > 开启任务”。

----结束

6.3.4 查看识别结果

敏感数据识别任务扫描完成后，可在识别任务列表目标任务操作列单击“识别结果”，查看数据资产的敏感信息总数、风险等级以及敏感信息分类分级结果。

前提条件

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。

步骤 5 单击目标任务“操作”列的“识别结果”查看识别结果。

DSC 分别统计了大数据、数据库、OBS、MRS 四个服务风险等级的数量及分布图。

同时 DSC 针对扫描对象提供了详细的识别结果列表，在页面左上角，可通过识别任务名称、资产类型、资产名称，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 6-6 所示。

表 6-6 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。
资产类型	• OBS • 数据库 • 大数据 • MRS
资产名称	涉及敏感信息资产名称。
对象路径	敏感信息对象路径。
分级结果	敏感信息级别。

步骤 6 在目标扫描对象所在行的“操作”列，单击“查看分类分级结果详情”，进入“分类分级结果详情”弹框。

说明

- “分类分级结果详情”页主要展示“识别对象详情”和“结果详情”。
- 结果详情主要展示匹配规则、分级结果、分类结果以及分类分级模板。

----结束

7 敏感数据识别（旧）

7.1 敏感数据规则

7.1.1 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（旧） > 识别规则”，进入敏感数据规则列表。

图 7-1 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 7-1 所示。

表 7-1 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
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

7.1.2 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 单击左上角的，选择区域或项目。

步骤 2 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 3 在左侧导航树中，选择“敏感数据识别（旧） > 识别规则”，进入敏感数据规则列表，参数说明如表 7-2 所示。

图 7-2 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 7-2 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。

参数名称	参数说明
规则描述	该规则的备注信息。

----结束

7.1.3 配置敏感数据规则

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 单击左上角的，选择区域或项目。

步骤 2 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 3 在左侧导航树中，选择“敏感数据识别（旧） > 识别规则”，进入敏感数据规则列表。

图 7-3 规则列表

步骤 4 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 5 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 7-3 所示

表 7-3 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。	-

参数	参数说明	取值样例
	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 6 单击“确定”，完成敏感数据规则的编辑。

----结束

7.1.4 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 7.2.3 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 单击左上角的，选择区域或项目。

步骤 2 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 3 在左侧导航树中，选择“敏感数据识别（旧） > 识别规则”，进入敏感数据规则列表。

图 7-4 规则列表

步骤 4 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 5 在弹出的删除规则的提示框中，单击“确定”。

----结束

7.1.5 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 单击左上角的，选择区域或项目。

步骤 2 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 3 在左侧导航树中，选择“敏感数据识别（旧） > 识别规则”，进入敏感数据规则列表。

图 7-5 规则列表

步骤 4 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 5 在“添加到组”的对话框中，选择敏感数据规则组。

步骤 6 单击“确定”。

----结束

7.2 敏感数据规则组

7.2.1 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 单击左上角的，选择区域或项目。

步骤 2 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 3 在左侧导航树中，选择“敏感数据识别（旧） > 识别规则”，并选择“规则组”页签，进入规则组列表。

步骤 4 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 5 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 7-4 所示。

表 7-4 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。
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 6 单击“确定”，完成敏感数据规则组的创建。

----结束

7.2.2 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 单击左上角的，选择区域或项目。

步骤 2 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 3 在左侧导航树中，选择“敏感数据识别（旧） > 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 7-5 所示。

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 7-5 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。
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 7.2.3 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 7.2.4 删除敏感数据规则组。

----结束

7.2.3 配置敏感数据规则组

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 单击左上角的，选择区域或项目。

步骤 2 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 3 在左侧导航树中，选择“敏感数据识别（旧） > 识别规则”，并选择“规则组”页签，进入规则组列表。

步骤 4 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 5 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 7-6 所示

表 7-6 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 6 单击“确定”，完成规则组的编辑。

----结束

7.2.4 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 单击左上角的，选择区域或项目。

步骤 2 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 3 在左侧导航树中，选择“敏感数据识别（旧） > 识别规则”，并选择“规则组”页签，进入规则组列表。

步骤 4 在目标敏感规则组所在行的“操作”列，单击“删除”。

步骤 5 在弹出的提示框中，单击“确定”。

----结束

7.3 敏感数据识别任务

7.3.1 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 5.1 资产列表。
- 已创建敏感数据规则组，具体操作请参见 7.2.1 新增敏感数据规则组。

操作步骤

步骤 1 单击左上角的，选择区域或项目。

步骤 2 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 3 在左侧导航树中，选择“敏感数据识别（旧） > 识别任务”，进入“识别任务”页面。

步骤 4 在敏感数据任务列表的左上角，单击“新建任务”。

步骤 5 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 7-7 所示。

表 7-7 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 5.1.3.1 添加 OBS 资产章节。 • 数据库，添加云数据库资产，参考 5.1.4.2 添加云数据库章节。 • 大数据，添加大数据源资产，参考 5.1.5.1 添加大数据源资产章节。 • MRS，添加 Hive 资产，参考 5.1.6.1 添加 MRS 资产。	数据库
识别规则组	单击输入框在弹框中选择识别任务需要使用的规则组，可多选，如图 7-6 所示。可参考 7.2.1 新增敏感数据规则组章节创建规则组。 **图 7-6 规则组弹框** 	GDPR
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，	快速扫描

参数	参数说明	取值样例
	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。	
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
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。	-

步骤 6 单击“确定”，完成敏感数据识别任务的创建。

----结束

7.3.2 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 单击左上角的，选择区域或项目。

步骤 2 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 3 在左侧导航树中，选择“敏感数据识别（旧） > 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 7-8 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 7-8 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

参数名称	参数说明
	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。
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 7.3.3 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 7.4 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 7.3.4 编辑识别任务章节。 • 删除扫描任务，具体的参考 7.3.5 删除识别任务章节。

----结束

7.3.3 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（旧） > 识别任务”，进入“识别任务”页面。

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

7.3.4 配置识别任务

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 单击左上角的，选择区域或项目。

步骤 2 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 3 在左侧导航树中，选择“敏感数据识别（旧） > 识别任务”，进入“识别任务”页面。

步骤 4 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 5 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 7-9 所示。

表 7-9 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。	-

参数	参数说明	取值样例
	• 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 5.1.3.1 添加 OBS 资产章节。 • 数据库，添加云数据库资产，参考 5.1.4.2 添加云数据库章节。 • 大数据，添加大数据源资产，参考 5.1.5.1 添加大数据源资产章节。 • MRS，添加 Hive 资产，参考 5.1.6.1 添加 MRS 资产。	数据库
识别规则组	单击输入框在弹框中选择识别任务需要使用的规则组，可多选，如图 7-7 所示。可参考 7.2.1 新增敏感数据规则组章节创建规则组。 **图 7-7 规则组弹框** 	GDPR
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。	-

步骤 6 单击“确定”。

----结束

7.3.5 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 单击左上角的，选择区域或项目。

步骤 2 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 3 在左侧导航树中，选择“敏感数据识别（旧） > 识别任务”，进入“识别任务”页面。

步骤 4 在待删除识别任务所在行的“操作”列，单击“更多 > 删除”。

步骤 5 在弹出删除任务提示框中，单击“确定”。

----结束

7.3.6 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。

下载识别任务报告

步骤 1 单击左上角的，选择区域或项目。

步骤 2 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 3 在左侧导航树中，选择“敏感数据识别（旧） > 识别任务”，进入“识别任务”页面。

步骤 4 单击任务名称，选择“报表下载”页签，进入报告下载页面。

步骤 5 在目标报告所在行的“操作”列，单击“下载”，PDF 格式的检测报告会保存在您的本地。

说明

如果不在需要某报告，可在目标报告所在行的“操作”列，单击“删除”，在弹出的提示框中，单击“确定”，删除该报告。

----结束

下载识别结果报表

步骤 1 单击左上角的，选择区域或项目。

步骤 2 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 3 在左侧导航树中，选择“敏感数据识别（旧） > 识别任务”，进入“识别任务”页面。

步骤 4 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

7.4 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 单击左上角的，选择区域或项目。

步骤 2 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 3 在左侧导航树中选择“敏感数据识别（旧） > 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 7-10 所示。

表 7-10 识别结果参数说明

参数名称	参数说明
资产名称	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。
上次识别时间	最近扫描该对象的时间。

参数名称	参数说明
操作	单击“查看详情”，查看该对象的识别结果明细。

步骤 4 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。

- 血缘图

  可查看资产中敏感数据的具体名称、路径、风险等级。

----结束

8 数据隐私保护

8.1 数据脱敏

8.1.1 数据脱敏概述

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。

脱敏算法

表 8-1 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	• 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
	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。	
加密脱敏	通过加密算法和加密主密钥生成一种加密配置，达到数据脱敏的效果。加密脱敏的结果中，初始向量 IV 为加密字符串的前 16 个字节，剩余部分是加密的密文。 DSC 支持 AES128、AES192 和 AES256 三种加密算法。	• 敏感类型： – 个人敏感 – 企业敏感 • 适用场景：数据存储
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）方式掩盖部分内容。 支持以下六种脱敏方式： • 保留前 n 后 m • 保留自 x 至 y • 掩盖前 n 后 m • 掩盖自 x 至 y • 特殊字符前掩盖 • 特殊字符后掩盖 **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
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。	• 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
	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。	
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“1575612731312 -> 1575612731000” • 数字取整 针对指定数字进行取整运算。	• 敏感类型：通用敏感 • 适用场景： – 数据存储 – 数据使用

相关操作

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

8.1.2 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 8.1.1 概述。

操作步骤

步骤 1 单击左上角的，选择区域或项目。

步骤 2 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 3 在左侧导航树中选择“数据隐私保护 > 数据脱敏”，并选择“脱敏规则”页签，进入脱敏规则页面。

步骤 4 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。
- “加密脱敏”的配置方法请参考加密脱敏。
- “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。

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。

----结束

加密脱敏

通过加密算法和加密主密钥生成一种加密配置，达到数据脱敏的效果。加密脱敏的结果中，初始向量 IV 为加密字符串的前 16 个字节，剩余部分是加密的密文。

步骤 1 参照操作步骤进入“脱敏规则”页面。

步骤 2 选择“加密脱敏”页签，进入“加密脱敏”页面。

- “加密算法”：在下拉框中选择加密算法，DSC 提供了 AES128、AES192 和 AES256 三种加密算法供您选择。
- “加密主密钥”：如果您已在其他云服务里创建了主密钥，可在下拉框里直接选择已创建的主密钥。如果您还未创建主密钥，可单击“创建 KMS 主密钥”，跳转到数据加密服务里创建主密钥。

步骤 3 配置完成后，单击“生成加密配置”。

如果您需要删除已配置的加密脱敏规则，可在目标规则所在列的“操作”列，单击“删除”。

----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。

步骤 3 单击“添加”，配置字符脱敏规则。

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。

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。

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。

----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。

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。

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

8.1.3 静态脱敏

8.1.3.1 创建数据脱敏任务

8.1.3.1.1 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 6.3.1 新建敏感数据识别任务。

操作步骤

步骤 1 单击左上角的，选择区域或项目。

步骤 2 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 3 在左侧导航树中选择“数据隐私保护 > 数据脱敏”，进入“数据库脱敏”页面。

步骤 4 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 5 单击“新建任务”，进入“数据源配置”页面，具体参数说明如表 8-2 所示。

表 8-2 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”、“DMDBMS”、“KingBase”、“OpenGauss”。

参数名称	参数说明
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 5.1.4.2 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”、“KingBase”、“OpenGauss”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 6 单击“下一步”，进入“脱敏算法配置”页面。

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 8.1.2 配置脱敏规则。

步骤 7 单击“下一步”，进入“脱敏周期”页面，配置脱敏周期。

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 8 单击“下一步”，进入“数据目标配置”页面。

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 9 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 8.1.3.2.1 运行数据库脱敏任务。

8.1.3.1.2 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 5.1.5 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 6.3.1 新建敏感数据识别任务。

操作步骤

步骤 1 单击左上角的，选择区域或项目。

步骤 2 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 3 在左侧导航树中选择“数据隐私保护 > 数据脱敏”，并选择“ES 脱敏”页签，进入 ES 脱敏页面。

步骤 4 单击，将“ES 脱敏”设置为，开启 ES 脱敏。

步骤 5 单击“新建任务”，进入“数据源配置”页面，具体参数说明如表 8-3 所示。

表 8-3 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。

参数名称	参数说明
	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 5.1.5.1 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 6 单击“下一步”，进入“脱敏算法配置”页面。

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 8.1.2 配置脱敏规则。

步骤 7 单击“下一步”，进入“脱敏周期”页面，配置脱敏周期。

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 8 单击“下一步”，进入“数据目标配置”页面。

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 9 单击“完成”，完成脱敏任务的创建。

----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 8.1.3.2.2 运行 ES 脱敏任务。

8.1.3.1.3 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。
- 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 6.3.1 新建敏感数据识别任务。

操作步骤

步骤 1 单击左上角的，选择区域或项目。

步骤 2 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 3 在左侧导航树中选择“数据隐私保护 > 数据脱敏”，并选择“MRS 脱敏”页签，进入“MRS 脱敏”页面。

步骤 4 在“MRS 脱敏”页签中，单击，将“MRS 脱敏”设置为，开启 MRS 脱敏。

步骤 5 单击“新建任务”，进入“数据源配置”页面，具体参数说明如表 8-4 所示。

表 8-4 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 5.1.6.1 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 6 单击“下一步”，进入“脱敏算法配置”页面。

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 8.1.2 配置脱敏规则。

步骤 7 单击“下一步”，进入“脱敏周期”页面，配置脱敏周期。

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 8 单击“下一步”，进入“数据目标配置”页面。

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 9 单击“完成”，完成脱敏任务的创建。

----结束

8.1.3.2 运行数据脱敏任务

8.1.3.2.1 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 单击左上角的，选择区域或项目。

步骤 2 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 3 在左侧导航树中选择“数据隐私保护 > 数据脱敏”，进入“数据库脱敏”页面。

步骤 4 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”。

运行后，系统开始按照设置的脱敏周期执行脱敏任务。

步骤 5 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。

----结束

8.1.3.2.2 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 单击左上角的，选择区域或项目。

步骤 2 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 3 在左侧导航树中选择“数据隐私保护 > 数据脱敏”，并选择“ES 脱敏”页签，进入 ES 脱敏页面。

步骤 4 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”。

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 5 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。

----结束

8.1.3.2.3 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 脱敏任务。

操作步骤

步骤 1 单击左上角的，选择区域或项目。

步骤 2 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 3 在左侧导航树中选择“数据隐私保护 > 数据脱敏”，并选择“MRS 脱敏”页签，进入“MRS 脱敏”页面。

步骤 4 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 5 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。

----结束

8.1.3.3 管理数据脱敏任务

8.1.3.3.1 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 单击左上角的，选择区域或项目。

步骤 2 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 3 在左侧导航树中选择“数据隐私保护 > 数据脱敏”，进入“数据库脱敏”页面。

步骤 4 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 8-5 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 8-5 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 单击左上角的，选择区域或项目。

步骤 2 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 3 在左侧导航树中选择“数据隐私保护 > 数据脱敏”，进入“数据库脱敏”页面。

步骤 4 在数据库脱敏任务列表中，在待编辑脱敏任务所在行的“操作”列，单击“编辑”，进入“数据源配置”页面。

步骤 5 配置数据源，具体参数说明如表 8-6 所示。

表 8-6 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”、“DMDBMS”、“KingBase”、“OpenGauss”。
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 5.1.4.2 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”、“KingBase”、“OpenGauss”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 6 单击“下一步”，进入“脱敏算法配置”页面。

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 8.1.2 配置脱敏规则。

步骤 7 单击“下一步”，进入“脱敏周期”页面，配置脱敏周期。

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 8 单击“下一步”，进入“数据目标配置”页面。

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 9 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 8.1.3.2.1 运行数据库脱敏任务。

----结束

删除数据库脱敏任务

步骤 1 单击左上角的，选择区域或项目。

步骤 2 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 3 在左侧导航树中选择“数据隐私保护 > 数据脱敏”，进入“数据库脱敏”页面。

步骤 4 在数据库脱敏任务列表中，在待删除脱敏任务所在行的“操作”列，单击“删除”。

步骤 5 在弹出删除任务对话框，单击“确定”。

----结束

8.1.3.3.2 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 单击左上角的，选择区域或项目。

步骤 2 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 3 在左侧导航树中选择“数据隐私保护 > 数据脱敏”，并选择“ES 脱敏”页签，进入 ES 脱敏页面。

步骤 4 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 8-7 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 8-7 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。

参数名称	参数说明
	• 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 单击左上角的，选择区域或项目。

步骤 2 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 3 在左侧导航树中选择“数据隐私保护 > 数据脱敏”，并选择“ES 脱敏”页签，进入 ES 脱敏页面。

步骤 4 在 ES 脱敏任务列表中，在待编辑脱敏任务所在行的“操作”列，单击“编辑”，进入“数据源配置”页面。

步骤 5 配置数据源，具体参数说明如表 8-8 所示。

表 8-8 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	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
的操作可参见 5.1.5.1 添加大数据源资产。	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 6 单击“下一步”，进入“脱敏算法配置”页面。

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 8.1.2 配置脱敏规则。

步骤 7 单击“下一步”，进入“脱敏周期”页面，配置脱敏周期。

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 8 单击“下一步”，进入“数据目标配置”页面。

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 9 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 8.1.3.2.2 运行 ES 脱敏任务。

----结束

删除 ES 脱敏任务

步骤 1 单击左上角的，选择区域或项目。

步骤 2 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 3 在左侧导航树中选择“数据隐私保护 > 数据脱敏”，并选择“ES 脱敏”页签，进入 ES 脱敏页面。

步骤 4 在 ES 脱敏任务列表中，在待删除脱敏任务所在行的“操作”列，单击“删除”。

步骤 5 在弹出删除任务对话框，单击“确定”。

----结束

8.1.3.3.3 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 脱敏任务。

查看 MRS 脱敏任务

步骤 1 单击左上角的，选择区域或项目。

步骤 2 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 3 在左侧导航树中选择“数据隐私保护 > 数据脱敏”，并选择“MRS 脱敏”页签，进入“MRS 脱敏”页面。

步骤 4 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 8-9 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 8-9 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 单击左上角的  ，选择区域或项目。

步骤 2 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 3 在左侧导航树中选择“数据隐私保护 > 数据脱敏”，并选择“MRS 脱敏”页签，进入“MRS 脱敏”页面。

步骤 4 在 MRS 脱敏任务列表中，在待编辑脱敏任务所在行的“操作”列，单击“编辑”，进入“数据源配置”页面。

步骤 5 配置数据源，具体参数说明如表 8-10 所示。

表 8-10 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 5.1.6.1 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 6 单击“下一步”，进入“脱敏算法配置”页面。

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 8.1.2 配置脱敏规则。

步骤 7 单击“下一步”，进入“脱敏周期”页面，配置脱敏周期。

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 8 单击“下一步”，进入“数据目标配置”页面。

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 9 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 单击左上角的，选择区域或项目。

步骤 2 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 3 在左侧导航树中选择“数据隐私保护 > 数据脱敏”，并选择“MRS 脱敏”页签，进入“MRS 脱敏”页面。

步骤 4 在 MRS 脱敏任务列表中，在待删除脱敏任务所在行的“操作”列，单击“删除”。

步骤 5 在弹出删除任务对话框，单击“确定”。

----结束

8.2 数据水印

8.2.1 水印概述

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 8-11 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

支持嵌入/提取水印的文件类型	具体的文件格式
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

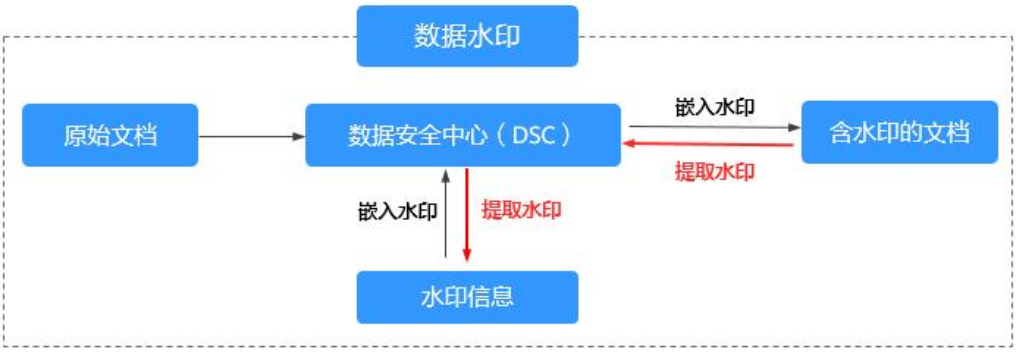
- 支持**明暗双重水印**：可根据需要对数据打上视觉上看得见的明水印或看不见的暗水印，都不影响使用效果，有效应对图像处理工具或者拍照截图等绕过方式窃取数据。
- **可检测性强，不易被篡改**：数据打上水印能够被检测且不会因为数据的改动而导致丢失、伪造或篡改。
- **高鲁棒性**：水印在传输或使用过程中不易被磨灭掉，数据载体即使经过被改动或受到攻击损坏后，依然有很大概率提取出水印。

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 8-2 数据水印操作流程



8.2.2 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 8.2.3 水印提取。

操作步骤

步骤 1 单击左上角的，选择区域或项目。

步骤 2 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 3 在左侧导航树中选择“数据隐私保护 > 数据水印”，进入“水印注入”页面。

步骤 4 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”。

- 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 5 文件上传成功后，参照表 8-12 配置相关水印参数。

表 8-12 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 8.2.3 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”。	• 水印内容：ZhangSan • 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 6 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 8.2.3 水印提取。

----结束

8.2.3 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 单击左上角的，选择区域或项目。

步骤 2 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 3 在左侧导航树中选择“数据隐私保护 > 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。

步骤 4 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”。
- 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 5 文件上传后，单击“确定”，暗水印内容将展示到弹框中。

----结束

9 数据风险检测

9.1 数据使用审计

9.1.1 查看异常行为检测事件

DSC 针对云上数据使用异常行为实时告警与审计。可查看“近 30 分钟”、“近 3 小时”、“近 24 小时”、“近 7 天”、“近 30 天”的异常行为数据。DSC 对于异常事件数据将保留 180 天。

数据安全中心服务可检测敏感数据相关的访问、操作、管理等异常，并提供告警提示信息，用户可以对异常事件进行确认和处理。

通常情况下，以下行为均被视为异常事件：

- 非法用户在未经授权的情况下对敏感数据进行了访问、下载。
- 合法用户对敏感数据进行了访问、下载、修改、权限更改、权限删除。
- 合法用户对敏感数据的桶进行权限更改、权限删除。
- 访问敏感数据的用户登录终端异常等情况。

前提条件

当前异常事件处理页面含有异常事件。

步骤 1 单击左上角的，选择区域或项目。

步骤 2 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 3 在左侧导航树中选择“数据风险检测 > 数据使用审计”，进入“数据使用审计”页面，参数说明请参考表 9-1。

在列表的右上角，可选择“近 30 分钟”、“近 3 小时”、“近 24 小时”、“近 7 天”、“近 30 天”的时间周期，事件类型以及事件状态来展示您想要的异常行为事件信息。

表 9-1 风险行为检测参数列表

参数名称	参数说明
用户 ID	资源所有者对应的 ID。
事件类型	DSC 将异常事件分成了三种类型： • 数据访问异常 – 敏感文件的越权操作。 – 敏感文件的下载操作。 • 数据操作异常 – 敏感文件的更新操作。 – 敏感文件的文件内容追加操作。 – 敏感文件的删除操作。 – 敏感文件的复制操作。 • 数据管理异常 – 添加桶时，检测到桶为公共读或公共读写桶。 – 添加桶时，检测到私有桶对匿名用户或注册用户组开通了访问/ACL 访问权限。 – 含有敏感文件的桶出现桶策略更改、删除操作。 – 含有敏感文件的桶出现桶 ACL 更改、删除操作。 – 含有敏感文件的桶出现跨区域复制配置的更改、删除操作。 – 敏感文件的对象出现 ACL 更改、删除操作。
事件名称	导致异常事件发生的具体事件。
告警时间	异常事件发生的具体时间。
状态	状态说明如下： • “待处理”：异常事件未进行处理。 • “违例确认”：已处理异常事件为违例确认。 • “违例排除”：已处理异常事件为违例排除。

步骤 4 在异常事件的操作列，单击“查看详情”，查看该事件的详细信息。

您可以根据异常事件的详细信息判断该事件是否为违例事件，从而确定如何来处理该事件，具体的处理方法请参见 9.1.2 处理异常行为检测事件。

----结束

9.1.2 处理异常行为检测事件

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。

前提条件

当前异常事件处理页面含有异常事件。

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“数据风险检测 > 数据使用审计”。

步骤 5 在异常事件列表中，在需要处理的异常事件所在行的“操作”列，单击“处理”。

步骤 6 在弹出的对话框中，选择处理方式，并单击“确定”。

处理方式包括以下 2 种：

- “确认该事件为违例事件”：如果您确认该事件的识别结果确实为异常事件，则勾选该选项。

  异常事件设为违例确认后，DSC 将继续对该事件进行告警提示，即该事件仍会展示在异常事件列表中。
- “确认该事件为正常情况，无需进行处理”：如果您确认该事件的识别结果为正常操作，无需进行处理，则勾选该选项。

  异常事件设为违例排除后，DSC 将不再对该事件进行告警提示，即该事件将不会展示在异常事件列表中。

----结束

9.2 查看并处理 Access Key 泄露检测事件

针对 git 代码库中包含访问密钥 ID（AK）和秘密访问密钥（SK）的访问密钥进行泄露检测，并将检测结果展示在列表中，您可以根据需要对异常事件进行处理。

前提条件

已获取管理控制台的登录帐号与密码。

操作步骤

步骤 1 单击左上角的，选择区域或项目。

步骤 2 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 3 在左侧导航树中选择“数据风险检测 >Access Key 泄漏检测”，进入“Access Key 泄露检测”页面。

表 9-2 Access Key 泄露检测参数列表

参数名称	参数说明
Access Key ID	访问密钥 ID。 可单击“去 Access Key 管理”，管理（创建、编辑、启用/停用、删除）访问密钥。
情报来源	该 Access Key 泄露检测事件的来源。如 github。
受影响账户	该 Access Key 泄露检测事件可能会影响到的帐户。
泄露类型	Accesskey
首次发现时间	首次爬取到该泄露事件的时间。
处理状态	根据事件详情对事件进行判断和处理后，有以下状态： • 待处理：还未处理。 • 已处理（已手动删除）：已登录 GitHub 手动删除/隐藏已泄露的 Access Key 及相关内容。 • 已处理（已手动禁用）：已进入 Access Key 控制台，禁用并重置 Access Key（或直接删除）。 • 已处理（加入白名单）：该事件加入白名单后，该 Access Key 在相同源链接中再次出现时，将不再进行告警，请慎重选择。

步骤 4 在目标事件的“操作”列，单击“查看”，可查看“Access Key 泄露详情”、“代码片段”、“相关推荐”。

步骤 5 可根据事件的推荐策略，对事件进行处理。并在目标事件的“操作”列，单击“处理”。

步骤 6 在弹出的对话框，选择“处理方式”，并单击“确定”。

处理方式包括以下 3 种：

- 已手动删除：已登录 GitHub 手动删除/隐藏已泄露的 Access Key 及相关内容。

- 已手动禁用：已进入 Access Key 控制台，禁用并重置 Access Key（或直接删除）。
- 加入白名单：该事件不存在风险，不进行处理，加入白名单后，该 Access Key 在相同源链接中再次出现时，将不再进行告警。

----结束

10 常见问题

10.1 产品咨询类

10.1.1 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。

10.1.2 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。

10.1.3 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 10-1、表 10-2 和表 10-3。

表 10-1 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

序号	文件类型	序号	文件类型
6	Bcpl 源代码	79	Plist 文件
7	Bib 文件	80	Postgres 数据库文件
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

序号	文件类型	序号	文件类型
35	Html 文件	108	Tnef 文件
36	Htm 文件	109	Tomcat Application 配置文件
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

序号	文件类型	序号	文件类型
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
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 10-2 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

序号	类型说明	序号	类型说明
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
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 10-3 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

10.2 资产添加类

10.2.1 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 10-4 所示。

表 10-4 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

资产模块	服务策略	作用范围	备注
OBS	OBS Administrator	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 Administrator	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
	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
	GaussDB ReadOnlyAccess	区域	用于获取 GaussDB 列表
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 Administrator	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 Administrator	全局	用于 OBS 服务投递日志

10.2.2 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

10.3 数据识别和数据脱敏

10.3.1 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 10-5 所示。

表 10-5 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）	--	--

数据源	具体的数据类型	扫描限制
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	--

10.3.2 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 10-6 中提供的扫描时长仅作参考。

表 10-6 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 进行脱敏，一般情况下，脱敏时长如表 10-7 所示。

表 10-7 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

10.3.3 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 10-8 所示。

表 10-8 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
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

敏感数据分类	数据类型
	• 城市 • GPS 位置 • 地址
通用敏感信息	日期

10.3.4 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。

10.3.5 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：10.3.1 DSC 能够识别哪些数据源对象？。

DSC 支持识别的敏感数据类型：10.3.3 DSC 支持识别的敏感数据类型？。

10.3.6 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。

10.4 数据水印类

10.4.1 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。

10.4.2 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。

10.4.3 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。

10.5 数据审计

10.5.1 DSC 可以检测哪些类型的异常事件？

数据安全中心服务当前仅支持对 OBS 桶数据进行异常检测。

DSC 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。DSC 支持检测的异常类型和异常内容如表 10-9 所示。

表 10-9 DSC 异常检测

异常类型	异常内容
数据访问异常	• 敏感文件的越权操作。 • 敏感文件的下载操作。
数据操作异常	• 敏感文件的更新操作。 • 敏感文件的文件内容追加操作。 • 敏感文件的删除操作。 • 敏感文件的复制操作。
数据管理异常	• 添加桶时，检测到桶为公共读或公共读写桶。 • 添加桶时，检测到私有桶对匿名用户或注册用户组开

异常类型	异常内容
	通了访问/ACL 访问权限。 • 含有敏感文件的桶出现桶策略更改、删除操作。 • 含有敏感文件的桶出现桶 ACL 更改、删除操作。 • 含有敏感文件的桶出现跨区域复制配置的更改、删除操作。 • 敏感文件的对象出现 ACL 更改、删除操作。

10.5.2 如何对 DSC 的操作记录进行审计？

DSC 的所有操作都会通过 API 形式记录在云审计服务（Cloud Trace Service，CTS）中。

开通云审计服务后，您可以在云审计服务中查看有关 DSC 的所有操作记录，供安全审查使用。

10.6 计费、到期续费与退订重购

10.6.1 数据安全中心如何收费？

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。同时，DSC 提供两个服务版本：标准版和专业版，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选择相应的服务版本和搭配扩展包，服务将根据您选择的计费项目进行收费。

计费项

表 10-10 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。
	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。

10.6.2 如何为数据安全中心服务续费？

该任务指导用户如何在购买的数据安全中心服务即将过期时进行续费。续费后，用户可以继续使用数据安全中心服务。

服务到期前，系统会以短信或邮件的形式提醒您服务即将到期，并提醒您续费。

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。

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 在“续费管理”界面，根据页面提示完成续费。

----结束

10.6.3 如何退订数据安全中心服务？

该任务指导用户退订购买的数据安全中心服务。DSC 不支持单独退订扩展包，如果您要退订扩展包，只能将购买的服务版本和扩展包一起退订。

操作步骤

步骤 1 登录管理控制台。

步骤 2 在界面右上方，单击“费用与成本”，进入“费用中心”界面。

步骤 3 在左侧导航树上选择“订单管理 > 退订与退换货”。

步骤 4 根据页面提示完成退订。

----结束