

数据安全中心

用户指南

文档版本 24
发布日期 2024-10-30



版权所有 © 华为云计算技术有限公司 2024。保留一切权利。

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

商标声明



HUAWEI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 开通 DSC	1
1.1 购买数据安全中心	1
1.2 升级版本和规格	3
2 云资产委托授权/停止授权	6
3 资产地图	10
4 资产管理	17
4.1 资产中心	17
4.1.1 概述	17
4.1.2 添加 OBS 资产	18
4.1.3 授权数据库资产	20
4.1.4 授权大数据资产	27
4.1.5 添加日志流	30
4.2 资产分组管理	31
4.3 元数据任务	33
4.3.1 创建元数据采集任务	33
4.3.2 运行元数据采集任务	34
4.4 数据探索	36
4.5 资产目录	37
5 敏感数据识别	41
5.1 敏感数据识别概述	41
5.2 敏感数据识别配置	43
5.2.1 新增识别模板	43
5.2.2 管理识别模板	44
5.2.3 新建自定义规则	45
5.2.4 编辑规则	47
5.2.5 查看内置规则	48
5.2.6 新建分级	49
5.2.7 管理级别	49
5.3 敏感数据识别任务	50
5.3.1 新建敏感数据识别任务	50
5.3.2 立即启动识别任务	55
5.3.3 管理识别任务列表	56

5.3.4 识别结果.....	60
6 策略中心.....	65
6.1 策略基线.....	65
6.1.1 概述.....	65
6.1.2 数据采集.....	66
6.1.3 数据传输.....	68
6.1.4 数据存储.....	71
6.1.5 数据使用.....	74
6.1.6 数据共享.....	76
6.1.7 数据销毁.....	79
6.2 策略管理.....	81
6.3 流转日志采集.....	84
7 数据资产保护.....	87
7.1 数据脱敏.....	87
7.1.1 概述.....	87
7.1.2 配置脱敏规则.....	91
7.1.3 数据静态脱敏.....	98
7.1.3.1 创建数据库脱敏任务.....	98
7.1.3.2 创建 Elasticsearch 脱敏任务.....	102
7.1.3.3 创建 MRS 脱敏任务.....	106
7.1.3.4 创建 Hive 脱敏任务.....	109
7.1.3.5 创建 HBase 脱敏任务.....	112
7.1.3.6 创建 DLI 脱敏任务.....	116
7.1.3.7 创建 OBS 脱敏任务.....	119
7.2 数据水印.....	122
7.2.1 概述.....	122
7.2.2 注入水印.....	124
7.2.2.1 数据库水印注入.....	124
7.2.2.2 文档水印注入.....	132
7.2.2.3 图片水印注入.....	136
7.2.3 提取水印.....	142
7.2.3.1 数据库水印提取.....	142
7.2.3.2 文档水印提取.....	144
7.2.3.3 图片水印提取.....	147
7.3 (可选) 配置 DWS 和 MRS Hive.....	150
8 数据安全运营.....	152
8.1 态势大屏.....	152
8.2 数据流转详情.....	160
8.3 事件管理.....	161
8.4 告警管理.....	164
8.5 OBS 使用审计.....	166

8.6 水印溯源.....	170
8.6.1 数据库水印提取.....	170
8.6.2 OBS 桶文件水印提取.....	172
8.6.3 本地文件水印提取.....	174
9 告警通知.....	176
10 多账号管理.....	178
10.1 多账号管理概述.....	178
10.2 开启多账号管理功能.....	178
10.3 查看多账号管理.....	179
11 权限管理.....	181
11.1 创建用户并授权使用 DSC.....	181
11.2 DSC 自定义策略.....	182
11.3 DSC 权限及授权项.....	184
12 审计.....	186
12.1 支持云审计的操作列表.....	186
12.2 查看审计日志.....	188

1 开通 DSC

1.1 购买数据安全中心

数据安全中心服务（DSC）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，具体的操作请参见[创建用户并授权使用DSC](#)。

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1024GB。

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“安全与合规 > 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”。

图 1-1 选择区域和版本规格



说明

如果您需要切换区域, 请在“区域”下拉框里选择区域。同一个区域只支持购买一个DSC版本。

步骤6 选择“数据库扩展包”和“OBS扩展包”的数量。

图 1-2 选择扩展包



- 1个数据库扩展包包含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扩展包包含1T体量，即1024GB。

步骤7 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 1-3 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8 在页面的右下角，单击“立即购买”。

如果您对价格有疑问，可以单击页面左下角的“了解计费详情”，了解产品价格。

步骤9 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 1-4 详情页面

详情					
产品类型	产品规格	计费模式	购买时长	优惠	价格(元)
数据安全中心	标准版 数据库实例数量 2个 OBS体量 100GB	包年/包月	1个月	¥0.00	
<input checked="" type="checkbox"/> 我已阅读并同意《数据安全中心免责声明》					

步骤10 进入“付款”页面，请选择付款方式进行付款。

----结束

1.2 升级版本和规格

购买了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，具体的操作请参见[创建用户并授权使用DSC](#)。
- 已购买任一版本的数据安全中心服务。

约束条件

已到期的服务版本，不支持直接升级，请先完成续费再升级。


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1024GB。

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“安全与合规 > 数据安全中心”。

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 1-5 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 1-6 选择扩展包



- 1个数据库扩展包包含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扩展包包含1T体量，即1024GB。

步骤7 在页面的右下角，单击“立即购买”。

如果您对价格有疑问，可以单击页面左下角的“了解计费详情”，了解产品价格。

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 1-7 详情页面

详情					
产品类型	产品规格	计费模式	购买时长	优惠	价格 (元)
数据安全中心	标准版				
	数据库实例数量 2个 OBS体量 100GB	包年/包月	1个月	¥0.00	

我已阅读并同意《数据安全中心免责声明》

步骤9 进入“付款”页面，请选择付款方式进行付款。

----结束

2 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OBS桶、数据库、大数据、MRS、资产地图以及LTS。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。

📖 说明

- 授权访问OBS桶后，需要获取OBS日志，因此会产生请求费用，具体的请参考[请求费用](#)。
- 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 2-1 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，用于获取OBS服务投递日志等
	EVS ReadOnlyAccess	区域	用于获取云硬盘列表
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
	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
资产地图	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
LTS	LTS ReadOnlyAccess	区域	用于读取LTS日志组/日志流

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“安全与合规 > 数据安全中心”，进入“资产地图”页面。
- 步骤4** 在“资产地图”左上角单击云资产授权“修改”，进入“云资产委托授权”页面。
- 步骤5** 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2-2进行操作。

图 2-1 云资源委托授权



云资产委托授权

1 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，大数据以及其他相应的云上资产。
停止授权前，请确认该资产没有绑定识别任务。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！

1 DSC数据安全总览授权会自动为您的所有OBS桶开启日志记录，生成的OBS访问日志会存储在您的原始桶中，可能涉及部分存储费用。DSC OBS授权会根据您的实际使用情况开通您增加到资产的OBS桶的日志记录，此外针对OBS的敏感数据扫描还会涉及文件请求的费用，计算方式如下：
日志存储费用=实际存储用量*资源单价 
数据请求费用=扫描次数*2*文件总量*请求单价 
更多价格详情请参见：[OBS价格计算器->价格详情](#)

资产模块	开通授权状态	操作
OBS		
数据库		
大数据		
MRS		
资产地图		
LTS		

表 2-2 参数说明

参数名称	参数说明
资产模块	<ul style="list-style-type: none"> • 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)、数据湖探索 (DLI) 的资产、Hive的资产和HBase的资产。 • MRS: 授权访问MapReduce服务 (MapReduce Service, 简称MRS)。 • 资产地图: 授权访问云上资产。 • LTS: 授权访问云日志服务 (Log Tank Service, LTS)。 <p>开通对应资产模块授权后, 获得的授权委托如开通授权后获得的授权委托策略。</p>
开通授权状态	<p>授权状态:</p> <ul style="list-style-type: none"> • 已授权 • 未授权
操作	<p>单击图标开启或者停止授权。</p> <ul style="list-style-type: none"> •  : 未授权 •  : 已授权

----结束

3 资产地图

数据资产地图可以通过可视化的手段，从资产概况、分类分级、权限配置、数据存储、敏感数据以及数据出口分析等多种维度查看资产的安全状况。可协助您快速发现风险资产并进行快速风险处理操作。

约束限制

支持显示1000个资产实例。

前提条件

已完成云资产委托授权，参考[云资产委托授权/停止授权](#)进行操作。

资产地图功能介绍

- **梳理云上数据资产并分区展示：**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。根据云上资源VPC展示各个资产所在区域，和业务区域关联。
- **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。
- **数据出口分析：**基于资产地图构建统一的数据出口和出口风险视图，帮助用户识别云上数据可能的出口，以及这些出口存在的潜在安全风险，方便用户采取相应的数据安全防护措施。
- **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。
 - **安全评分：**资产地图会显示您当前所有资产的总体“安全评分”，单击评分规则后的[?]查看资产安全评分计算规则，如[图3-1](#)所示。

图 3-1 评分规则




- 敏感度等级：按照检测到的敏感度等级将资产进行分类，方便查看和管理，鼠标移动至存在风险的资产类型并单击资产可以查看资产风险详情。

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“安全与合规 > 数据安全中心”。

步骤4 在左侧导航树中选择“资产地图”，进入“资产地图”页面。

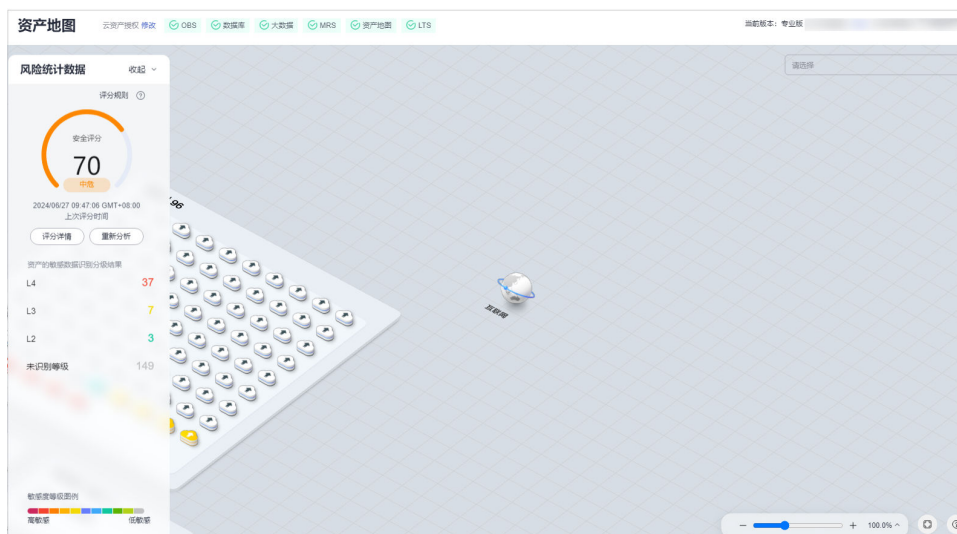
步骤5 单击“添加资产”，进入“资产中心”页面，添加和授权资产。

图 3-2 添加资产



步骤6 资产添加或者授权完成后刷新“资产地图”页面，具体页面中各个模块的功能介绍和使用方法详见下述内容。

图 3-3 资产地图




----结束

风险统计数据

- 如图3-4所示，展示资产的“安全评分”、“上次评分时间”、“评分详情”以及可以手动重新分析评分，具体内容如下：

图 3-4 安全评分



- 展示资产的安全评分，单击评分规则后的  查看资产安全评分计算规则。
- 单击“重新分析”，对云上资产再次进行安全分析扫描。
- 单击“评分详情”，查看各类资产“安全防护策略分析”并根据给出的“配置策略推荐”信息单击操作列的“前去修改”进行处理。

如图3-5所示，“安全防护策略分析”仅展示“风险等级”为“中危”和“高危”的资产，“风险等级”计算方式如表3-1所示，由“配置风险等级”和“分级分类级别”综合得出“风险等级”。

图 3-5 安全防护策略分析

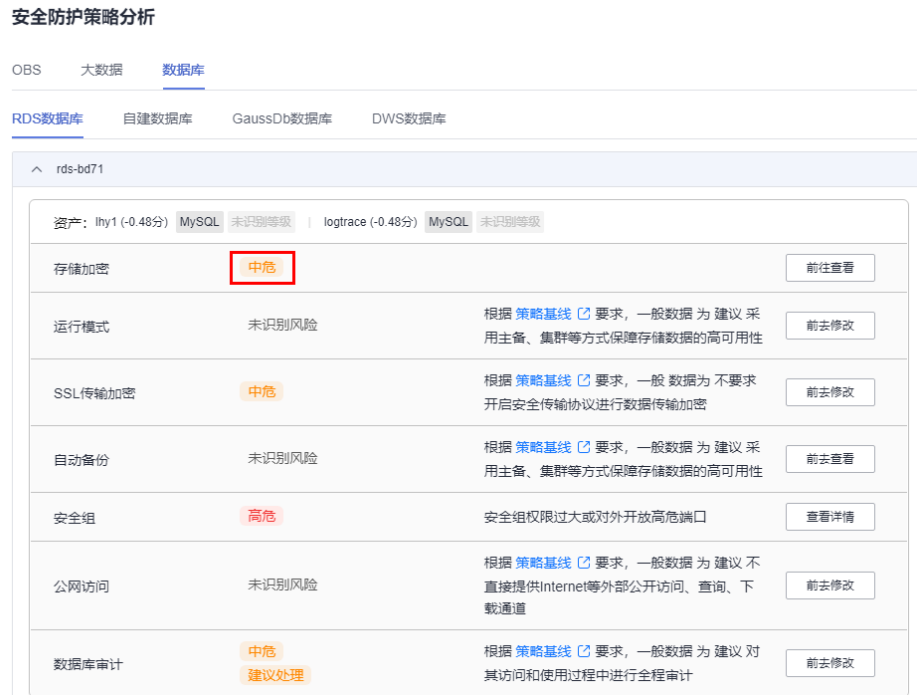


表 3-1 安全防护策略分析展示规则

配置风险等级	分级分类级别	风险等级	是否展示
低危	L0-L3(低危)	低危	不展示
	L4-L7 (中危)	低危	不展示
	L8-L10 (高危)	中危	展示
中危	L0-L3(低危)	低危	不展示
	L4-L7 (中危)	中危	展示
	L8-L10 (高危)	高危	展示
高危	L0-L3(低危)	中危	展示
	L4-L7 (中危)	高危	展示
	L8-L10 (高危)	高危	展示

- 如**图3-6**所示，展示资产的敏感数据识别分级结果，根据分级结果分类展示资产，具体内容如下：

图 3-6 敏感数据识别分级结果

资产的敏感数据识别分级结果	
绝密	1
L4	2
L3	10
L2	1
L1	2
未识别等级	22

- 鼠标移动至敏感等级上，展示该“敏感等级”下的所有资产信息。
- 鼠标移动至对应的资产类型，右侧弹框展示该类型下所有已扫描资产的名称以及扫描时间。
- 单击某个资产，在右侧弹框展示该实例详情，包含资产基础信息、敏感数据识别、安全防护策略分析以及数据出口分析的内容，具体说明请参见[查看实例详情](#)内容。

查看实例详情

- “基础信息”：展示该实例的类型、端口、版本、内网IP以及引擎类型等。
- “敏感数据识别”：展示该实例下已授权的数据库和未授权的数据库。
 - “已授权数据库”但是“未扫描”，单击“创建识别任务”跳转至敏感数据识别功能，创建识别任务识别该资产敏感信息，具体操作请参见[新建敏感数据识别任务](#)章节。
 - “已授权数据库”并且是“已扫描”，单击“展开”查看数据库扫描详情。
 - “未授权数据库”单击“去授权”去给数据库进行授权，授权方式请参见[资产中心](#)授权操作的内容。

图 3-7 敏感数据识别

The screenshot shows a window titled "rds-pgsql-dyf" with a status of "已扫描" (Scanned) and "安全防护中 L3" (Security Protection L3). The instance ID is "60e8b9b2656349daa80724d13938d0b9in03" and it was created on "2023/11/08 07:49:52 GMT+08:00".

基础信息

类型	内网IP
RDS	[Redacted]
端口	引擎类型
5432	PostgreSQL
版本	
11	

Navigation tabs: **敏感数据识别** (Selected), RDS实例安全防护策略分析, 数据出口分析

已授权数据库(2)

- pg_test** (未扫描): 当前数据库未识别密级等级。 [创建识别任务](#)
- zyj_scan** (已扫描): 当前数据库扫描任务完成。 [展开](#)

未授权数据库(0)

说明

如果数据类型为OBS，单击“查看详情”查看敏感数据识别任务的“结果明细”。如果没有识别，请参见[新建敏感数据识别任务](#)章节创建识别任务进行识别后再次查看识别结果。





- “安全防护策略分析”：
 - 检测数据资产的安全策略，展示策略风险，检测项包含是否开启服务端加密、数据库加密、传输加密、安全组以及公网访问等高危权限并给出处理提醒，可单击“查看详情”或者“前去修改”处理。
 - 查看资产的加密、备份、审计等安全配置的现状和策略基线的具体要求，并可跳转策略/任务配置页面进行策略/任务配置。

- “数据出口分析”：识别云上所有的数据出口，包含EIP/NAT/APIGateway/Roma等。将鼠标移动至资产地图数据类型图标或者VPC图标也可查看数据出口网关线路。

图 3-8 数据出口分析



相关操作

- 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。具体操作请参见[云资产委托授权/停止授权](#)章节。
- 资产敏感度等级图例：从L0-L10每种颜色代表一种等级，根据识别到的资产的敏感度等级，资产地图展示的资产图例颜色与之一一对应。
- 拖动进度条滑块调整资产地图显示比例。
- 单击右下角  全屏显示。
- 单击右下角  显示资产地图操作指南。
- 单击右下角  显示数据异常风险事件，方便快速处理。
- 单击右下角  显示资产图例。

4 资产管理

4.1 资产中心

4.1.1 概述

数据安全中心支持自动发现云上资产和添加自建数据资产。

数据库和大数据类型资产需要完成授权之后才能进行敏感数据识别、数据脱敏和数据库水印。

图 4-1 资产中心介绍



4.1.2 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服务进行防护。

前提条件

- 已完成OBS资产委托授权，参考[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”或者该桶为当前账户拥有权限的私有桶。

约束条件


DSC不支持OBS的并行文件系统。

添加自有桶

自有桶是指当前用户自己创建的桶，包含公共桶和私有桶。

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“安全与合规 > 数据安全中心”。

步骤4 在左侧导航树中选择“资产管理 > 资产中心”，进入“资产中心”页面。

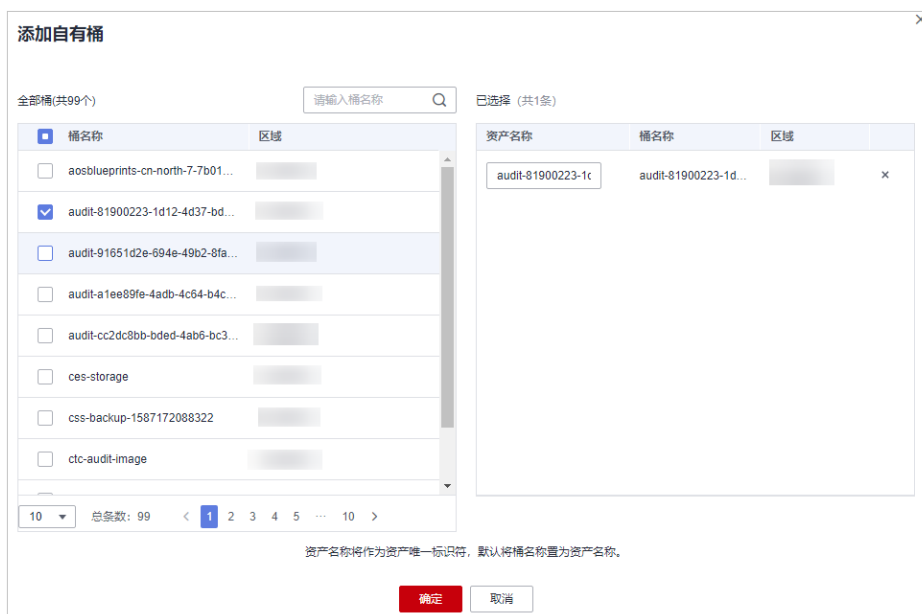
步骤5 单击OBS资产，进入OBS资产列表界面。

步骤6 在OBS资产列表左上角，单击“添加自有桶”。在弹出添加自有桶对话框中，勾选需要添加的OBS桶。

说明

资产名称将作为资产唯一标识符，默认将桶名称置为资产名称。

图 4-2 添加自有桶



步骤7 单击“确定”。


----结束

添加其他桶

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

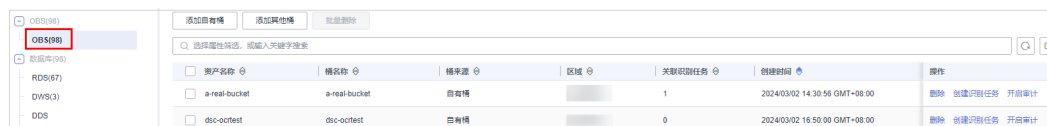
步骤1 登录管理控制台。

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“安全与合规 > 数据安全中心”。

步骤4 在左侧导航树中选择“资产管理 > 资产中心”，进入“资产中心”页面。

图 4-3 资产中心



步骤5 单击“OBS”，进入OBS资产列表界面。

步骤6 在OBS资产列表左上角，单击“添加其他桶”。在弹出“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 4-4 添加其他桶



步骤7 单击“确定”。

----结束

相关操作

- 删除OBS资产**
 勾选多个OBS资产，单击资产列表左上角“批量删除”，删除资产。也可通过单击资产列表“操作”列的“删除”，删除单个资产。
- 创建识别任务**
 单击资产列表“操作”列的“创建识别任务”，为资产创建敏感数据识别任务识别资产，详细操作步骤请参见[新建敏感数据识别任务](#)章节。
- 开启审计**
 单击资产列表“操作”列的“开启审计”，开启OBS资产的审计功能，开启该功能后可在[OBS使用审计](#)章节查看审计记录。

4.1.3 授权数据库资产

如果您的资产是自建数据库类型，请先[添加自建数据库实例](#)或者[添加外部自建数据库实例](#)后再进行[授权数据库](#)。

如果您的资产属于云上数据库类型，请按照[授权数据库](#)直接给数据库授权。

前提条件

- 已完成数据库资产委托授权，参考[云资产委托授权/停止授权](#)进行操作。
- 已申请ECS并且在ECS中安装了数据库。
- 已开通RDS/DWS/DDS/GaussDB服务，且已有资产，且对应子网下含有可用的IP配额。
- 数据库实例的“状态”为“正常”，且安全组的数量为1。

约束限制

自建DB只能添加数据安全中心支持的数据源及版本，DSC支持的数据源及版本如[表4-1](#)所示。

表 4-1 DSC 支持的数据源及版本


数据源类型	版本
MySQL	5.6、5.7、5.8、8.0
SQL Server	<ul style="list-style-type: none">• 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
PostgreSQL	11、10、9.6、9.5、9.4、9.1
TDSQL	10.3.X
Oracle	11、12

授权数据库

这里以RDS数据库类型为例讲解如何授权数据库资产，如果需要授权其他类型的数据库资产，请单击对应的数据库类型按照如下操作步骤进行操作即可。

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“安全与合规 > 数据安全中心”。

步骤4 在左侧导航树中选择“资产管理 > 资产中心”，进入“资产中心”页面。

步骤5 单击“RDS”资产进入RDS“数据库”列表界面。如果需要授权其他类型的数据库，请单击对应的数据库类型即可，这里以RDS数据库类型为例。

图 4-5 RDS 数据库实例



步骤6 单击“数据库实例”，进入“数据库实例”页签。可以通过以下两种途径进行授权：

- 方法一：单击“数据库实例”列表“操作”列的“授权”，输入数据库信息进行授权。
 - 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。

注意

- 创建了RDS只读权限后，DSC服务会在RDS创建一个dsc_readonly账户。
 - dsc_readonly账户的密码在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，建议您不要重置该账户密码。
 - 如果您已在RDS里重置了dsc_readonly账户的密码，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。
- DSC暂不支持对RDS中已开启SSL的MySQL数据库进行扫描和脱敏。

图 4-6 数据库授权



- 方法二：通过单击“实例名称”进入实例详情页面，单击“操作”列的“授权”去给未授权的数据库授权。

图 4-7 实例详情



步骤7 完成授权后，单击“数据库”页签，查看已授权数据库的连通状态。

资产授权完成后，该资产“连通状态”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“连通状态”为“成功”。
- 如果DSC不能正常访问已添加的数据库，该数据库的“连通状态”为“失败”。鼠标移动至“失败”上查看失败原因或者参照[如何排查添加数据库连通性失败?](#)解决。


---结束

添加自建数据库实例

自建DB支持添加和删除数据库实例，DSC支持的数据库类型及版本请参见[表4-1](#)。本节介绍如何添加自建数据库，删除数据库操作请参见[相关操作](#)。

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“安全与合规 > 数据安全中心”。

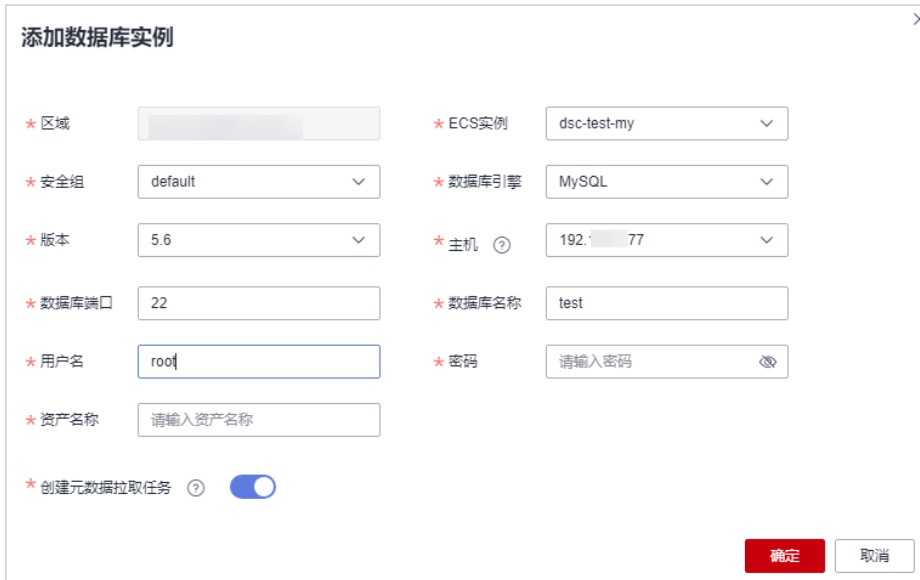
步骤4 在左侧导航树中选择“资产管理 > 资产中心”，进入“资产中心”页面。

步骤5 选择“数据库 > 自建DB”，进入“数据库”页签。

步骤6 单击“数据库实例”，进入“数据库实例”页签。

步骤7 单击左上角的“添加实例”，进入“添加数据库实例”弹框，如[图4-8](#)所示。

图 4-8 添加数据库实例



步骤8 根据[表4-2](#)配置相关参数，单击“确定”完成自建数据库实例的添加。

表 4-2 配置数据库实例信息

参数	说明
ECS实例	单击下拉框选择需要添加的自建数据库实例所属ECS。
安全组	单击下拉框选择所属安全组。
数据库引擎	单击下拉框选择对应的自建数据库的引擎，目前支持如下引擎类型： <ul style="list-style-type: none"> • MySQL • TDSQL • KingBase • DMDBMS • PostgreSQL • SQLServer • Oracle
版本	单击下拉框选择数据库引擎的版本。
主机	单击下拉框选择主机。 集群部署模式下，如需使用脱敏功能需设置为主节点IP。
数据库端口	输入0-65535的整数。
数据库名称	输入数据库名称。
用户名/密码	输入该数据库的用户名和密码。
资产名称	输入长度范围为4-255个字符，仅允许输入中英文、数字、“-”、“_”，并且开头需为中文或者字母。
创建元数据拉取任务	打开开关后，会基于实例的默认数据库自动下发元数据任务，拉取实例的库、表、列信息。

步骤9 实例添加完成后可以授权数据库，具体方法请参见[授权数据库](#)。


----结束

添加外部自建数据库实例

通过[云专线](#)等方法打通云下资产到云上代理VPC的网络就可以将云下数据库添加到数据安全中心。

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“安全与合规 > 数据安全中心”。

步骤4 在左侧导航树中选择“资产管理 > 资产中心”，进入“资产中心”页面。

步骤5 选择“数据库 > 自建DB”，进入“数据库”页签。

步骤6 单击“数据库实例”，进入“数据库实例”页签。

步骤7 单击左上角的“添加外部自建数据库”，进入“添加数据库实例”弹框。

步骤8 根据表4-3配置相关参数，单击“确定”完成外部自建数据库实例的添加。

表 4-3 配置数据库实例信息

参数	说明
区域	实例所在区域。
代理VPC	单击下拉框选择云上代理VPC。
子网	单击下拉框选择所属子网。
安全组	单击下拉框选择所属安全组。
数据库引擎	单击下拉框选择对应的自建数据库的引擎，目前支持如下引擎类型： <ul style="list-style-type: none"> • MySQL • TDSQL • KingBase • DMDBMS • PostgreSQL • SQLServer • Oracle
版本	单击下拉框选择数据库引擎的版本。
主机	输入资产所在主机IP地址。
数据库端口	输入0-65535的整数。
数据库名称	输入数据库名称。
用户名	输入数据库用户名。
密码	输入数据库密码。
资产名称	输入数据库密码输入长度范围为4-255个字符，仅允许输入中英文、数字、“-”、“_”，并且开头需为中文或者字母。

步骤9 打开开关后，会基于实例的默认数据库自动下发元数据任务，拉取实例的库、表、列信息。

步骤10 实例添加完成后可以授权数据库，具体方法请参见[授权数据库](#)。


----结束

批量添加实例与数据库

通过[云专线](#)等方法打通云下资产到云上代理VPC的网络就可以将云下数据库批量添加到数据安全中心。

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“安全与合规 > 数据安全中心”。

步骤4 在左侧导航树中选择“资产管理 > 资产中心”，进入“资产中心”页面。

步骤5 选择“数据库 > 自建DB”，进入“数据库”页签。

步骤6 单击“数据库实例”，进入“数据库实例”页签。

步骤7 单击左上角的“批量添加实例与数据库”，进入“批量添加实例与数据库”弹框。

步骤8 单击“下载模板”，下载Excel模板，根据[表4-4](#)填写相关参数。

表 4-4 数据库实例信息

参数	说明
资产名称	自定义，在填写后在自己数据库列表中显示的资产名称
ECS实例ID	外部自建数据库可以不填，本账号购买ES自建数据库需要填写对应ESC实例的ID。
Oracle服务名	仅Oracle需要填写，其余类型无需填写。
代理VPC	云内数据库无需填写，外部自建数据库必填，对应ECS的代理VPC。
子网	云内数据库可以不填，外部ESC必填，对应ECS的子网ID。
安全组	云内数据库可以不填，外部ESC必填，对应ECS的安全组。
数据库引擎	如果ECS实例已被添加，将会使用已添加引擎。
版本	如果ECS实例已被添加，将会使用已添加版本。
主机IP	如果ECS实例已被添加，将会使用已添加IP。
数据库端口	如果ECS实例已被添加，将会使用已添加端口。
数据库名称	数据库的名称。
用户名	数据库账号。
密码	数据库密码。
是否拉取元数据	TRUE或者FALSE。

步骤9 单击“添加文件”选择填好的模板，单击“确定”。

步骤10 打开开关后，会基于实例的默认数据库自动下发元数据任务，拉取实例的库、表、列信息。

步骤11 实例添加完成后可以授权数据库，具体方法请参见[授权数据库](#)。

----结束

拉取实例下的元数据

- 云数据库实例下的授权数据库大于0时，在实例列表“操作”列，单击“刷新”自动创建元数据任务拉取实例的库、表、列信息。
不支持元数据采集的云数据库除外，如DDS等，详情请参见[创建元数据采集任务](#)章节。
- 添加自建数据库实例时，如果打开“创建元数据拉取任务”的开关，完成实例创建后会自动创建元数据任务拉取实例下的所有元数据。
不支持元数据采集的自建数据库除外，如SQLServer等，详情请参见[创建元数据采集任务](#)章节。
- 参考[创建元数据采集任务](#)章节的内容手动创建元数据任务。

相关操作

- 删除数据库实例
只有自建数据库实例支持删除，且授权数据库为0才可删除。
勾选多个自建数据库实例，单击实例列表左上角“批量删除”，删除实例。也可通过单击实例列表“操作”列的“删除”，删除单个实例。
- 创建识别任务
在数据库页签，单击资产列表“操作”列的“创建识别任务”，为资产创建敏感数据识别任务识别资产，详细操作步骤请参见[新建敏感数据识别任务](#)章节
- 批量测试连通性
可多选批量添加的实例与数据，批量进行连通性测试。

4.1.4 授权大数据资产

- 如果您的资产是自建大数据类型，请先[添加大数据类型实例](#)再进行[授权大数据](#)。
- 如果您的资产属于云上大数据类型，请按照[授权大数据](#)直接给大数据授权。
- 如果您的资产为DLI数据库，请参照[添加DLI数据库](#)进行添加。

前提条件


- 已完成数据库资产委托授权，参考[云资产委托授权/停止授权](#)进行操作。
- 已开通DLI、CSS服务，且DLI、CSS中已有资产，且对应子网下含有可用的IP配额。
- 已获取自建ES、HBase以及Hive数据源的版本、主机、索引等相关信息，且自建ES、HBase以及Hive数据源子网下含有可用的IP配额。

授权大数据

这里以Elasticsearch大数据类型为例讲解如何授权大数据资产，如果需要授权其他类型的大数据资产，请单击对应的大数据类型即可。

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“安全与合规 > 数据安全中心”。

步骤4 在左侧导航树中选择“资产管理 > 资产中心”，进入“资产中心”页面。

步骤5 单击“Elasticsearch”大数据类型，进入“索引”页签。

步骤6 单击“ES实例”，进入“ES实例”页签。

步骤7 单击“ES实例”列表“操作”列的“授权”，输入ES索引信息进行授权。

图 4-9 ES 索引授权

实例名称	状态	类型	内网IP	端口	引擎版本	授权数据库	创建时间	操作
css-628 2b6245fb-c4d7-426a...	成功	CSS	192.168.1.10 undefined	9200	Elasticsearch 6.5.4	已授权2个	2024/05/16 11:49:56...	授权 编辑

步骤8 也可以通过单击“实例名称”进入实例详情页面，查看该实例下所有索引的状态。

单击“操作”列的“授权”去给未授权的索引授权。

说明

单击“设为默认数据”，元数据任务将基于默认数据库创建连接并拉取实例的元数据。

步骤9 单击“索引”页签，查看已授权资产的连通状态。

资产授权完成后，该资产“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资产，该资产的“连通性”为“成功”。
- 如果DSC不能正常访问已添加的资产，该资产的“连通性”为“失败”。鼠标移动至“失败”上查看失败原因或者参照[如何排查添加数据库连通性失败?](#)解决。


---结束

添加大数据类型实例

自建大数据类型的实例需要手动添加，本节以Elasticsearch数据类型为例介绍如何添加自建大数据类型的实例。

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“安全与合规 > 数据安全中心”。

步骤4 在左侧导航树中选择“资产管理 > 资产中心”，进入“资产中心”页面。

步骤5 单击“Elasticsearch”大数据类型，进入“索引”页签。

步骤6 单击“ES实例”，进入“ES实例”页签。

步骤7 单击左上角的“添加实例”，进入“添加实例”弹框。

步骤8 根据[表4-5](#)配置相关参数，单击“确定”。

表 4-5 添加实例参数配置表


参数	说明
ECS实例	单击下拉框选择所属ECS。
大数据类型	与需要添加的数据类型对应，如正在添加的是“Elasticsearch”类型实例时，数据类型就为“Elasticsearch”。
安全组	单击下拉框选择所属安全组。
版本	单击下拉框选择大数据类型的版本。支持的资产类型及版本详情请参见 使用约束 章节。
主机	单击下拉框选择主机。
数据库端口	请输入0-65535的整数。
索引	请输入索引名称，只能由中英文字符、数字、下划线和中划线组成。
用户名/密码	请输入该索引的用户名和密码。
资产名称	请输入自定义的资产名称，长度为4-255个字符。

----结束

添加 DLI 数据库

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“安全与合规 > 数据安全中心”。

步骤4 在左侧导航树中选择“资产管理 > 资产中心”，进入“资产中心”页面。

步骤5 单击“DLI”大数据类型，进入DLI“数据库”页签。

图 4-10 DLI 数据库列表



步骤6 单击数据库列表左上角的“添加数据库”，进入“添加数据库”弹框。

步骤7 根据[表4-6](#)配置相关参数，单击“确定”完成添加。

表 4-6 添加数据库参数配置表

参数	说明
资产名称	请输入自定义的资产名称，长度为4-255个字符。
大数据类型	单击下拉框选择大数据类型，“DLI”。
队列	单击下拉框选择所属队列。
DLI数据库	单击下拉框选择需要添加的DLI数据库。

资产授权完成后，该资产“连通性”为“检查中”，此时，DSC会测试资产的连通性。

- DSC能正常访问已添加的资产，该资产的“连通性”为“成功”。
- 如果DSC不能正常访问已添加的资产，该资产的“连通性”为“失败”。鼠标移动至“失败”上查看失败原因或者参照[如何排查添加数据库连通性失败?](#)解决。

----结束

拉取实例下的元数据

- MRS_Hive实例下数据库授权个数大于0时，在Hive实例列表“操作”列，单击“更多 > 刷新”会自动创建元数据任务拉取实例的库、表、列信息。
- 添加Hive实例时，如果打开自动创建元数据任务的开关，完成实例创建后会自动创建元数据任务拉取实例下的所有元数据。
- 支持元数据采集的大数据类型请参见[创建元数据采集任务](#)章节。
- 参考[创建元数据采集任务](#)章节的内容手动创建元数据任务。

相关操作

- 删除实例
只有自建大数据实例支持删除，且授权数据库为0才可删除。
勾选多个自建大数据实例，单击实例列表左上角“批量删除”，删除实例。也可通过单击实例列表“操作”列的“删除”，删除单个实例。
- 创建识别任务
单击资产列表“操作”列的“创建识别任务”，为资产创建敏感数据识别任务识别资产，详细操作步骤请参见[新建敏感数据识别任务](#)章节

4.1.5 添加日志流

添加云日志资产请参见[添加日志流](#)章节的内容。


前提条件

- 已完成数据库资产委托授权，参考[云资产委托授权/停止授权](#)进行操作。
- 已开通LTS服务，且LTS中已有资产。

添加日志流

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“安全与合规 > 数据安全中心”。

步骤4 在左侧导航树中选择“资产管理 > 资产中心”，进入“资产中心”页面。

步骤5 选择“日志 > LTS”，进入LTS“日志流”页签。

图 4-11 LTS 数据库列表



步骤6 单击数据库列表左上角的“添加日志流”，进入“添加日志流”弹框。

步骤7 根据表4-7配置相关参数，单击“确定”完成添加。

表 4-7 添加数据库参数配置表

参数	说明
资产名称	请输入自定义的资产名称，长度为4-255个字符。
大数据类型	单击下拉框选择大数据类型，“LTS”。
日志组	单击下拉框选择日志组。
日志流	单击下拉框选择需要添加的日志流。

资产授权完成后，该资产“连通性”为“检查中”，此时，DSC会测试资产的连通性。

- DSC能正常访问已添加的资产，该资产的“连通性”为“成功”。
- 如果DSC不能正常访问已添加的资产，该资产的“连通性”为“失败”。鼠标移动至“失败”上查看失败原因或者参照[如何排查添加数据库连通性失败?](#)解决。

---结束

4.2 资产分组管理

对资产中心资产进行分组管理后方便维护和管理，本章介绍如何进行资产分组管理。

前提条件


- 已完成云资产委托授权，具体请参见[云资产委托授权/停止授权](#)进行操作。
- 已对资产进行授权，具体请参见[资产中心](#)章节中资产授权的内容。

新建数据库分组


通过创建子级标签的方式对您的资产进一步分组，方便管理和查看。

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“安全与合规 > 数据安全中心”。

步骤4 在左侧导航树中选择“资产管理 > 资产分组管理”，进入“资产分组管理”页面。

步骤5 将鼠标滑动至全域数据库列表的“全部”或者新创建的标签上，单击添加标签，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”，创建标签成功。


---结束

管理数据库分组


通过移动数据库实例下的数据库对其进行重新分组管理。

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“安全与合规 > 数据安全中心”。

步骤4 在左侧导航树中选择“资产管理 > 资产分组管理”，进入“资产分组管理”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”弹窗中选择目标标签。


步骤7 单击“确定”。

---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“安全与合规 > 数据安全中心”。

步骤4 在左侧导航树中选择“资产管理 > 资产分组管理”，进入“资产分组管理”页面。

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

步骤6 单击“确定”，删除标签。

----结束

4.3 元数据任务

4.3.1 创建元数据采集任务

创建元数据任务，数据任务将基于数据库创建连接并拉取实例的元数据，本章介绍如何创建元数据采集任务。


前提条件

已完成云资产委托授权，具体请参见[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“安全与合规 > 数据安全中心”。









步骤4 在左侧导航树中选择“资产管理 > 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 [数据源配置参数说明](#) 所示。

表 4-8 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”、“TDSQL”、“PostgreSQL”、“达梦”、“人大金仓”、“OpenGuass”、“DWS”、“Hive”、“MRS_HIVE”。
数据库实例	单击下拉框选择数据库实例。
添加配置项	单击  可以增加配置项。



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”，例如包括infomation_schema。
- 选择开启  或关闭  “扫描列约束”，包括主键，是否唯一。
- 选择开启  或关闭  “扫描视图”，扫描元数据中是否包括视图。

- 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 任务信息配置参数说明](#)。

表 4-9 任务信息配置参数说明

参数名称	参数说明
任务信息	<ul style="list-style-type: none"> • 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  “删除连通性失败的元数据”。
执行计划	<ul style="list-style-type: none"> • 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

4.3.2 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

已创建元数据采集任务。

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“安全与合规 > 数据安全中心”。

步骤4 在左侧导航树中选择“资产管理 > 元数据任务”，进入“元数据采集任务”页面

表 4-10 元数据采集任务参数说明

参数名称	参数说明
名称	元数据采集任务名称

参数名称	参数说明
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。

图 4-12 运行元数据采集任务



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 [元数据任务详情参数说明](#)。

表 4-11 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： <ul style="list-style-type: none"> ● 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。

4.4 数据探索

数据探索页面展示通过元数据任务拉取的数据库、数据表以及数据视图等，可以对其添加描述、标签、密级和分类操作，从而实现数据资产分级分类管理。

前提条件

- 已完成数据资产委托授权，具体请参见[云资产委托授权/停止授权](#)进行操作。
- 已进行元数据扫描，具体请参见[元数据任务](#)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“安全与合规 > 数据安全中心”。

步骤4 在左侧导航树中选择“资产管理 > 数据探索”，进入“数据探索”页面。

步骤5 左上角单击下拉框选择展示模式：

- “数据库”
- “数据模式”
- “数据表”
- “数据列”

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。

单击“重新分析”，进行密级自动分析，根据敏感数据识别对数据库列标记的密级等级，分析出库表的密级。

图 4-13 数据库详情



步骤7 查看数据库详细信息。

- 选择“表信息”页签：
 - a. 单击表名称查看表详情。
 - b. 单击数据库名称返回上级页签。
 - c. 选择“表信息”页签，勾选表，单击左上角的“标识”添加表标识。
 - d. 单击给表添加分类、密级、标签和描述等信息。
- 选择“视图信息”：
 - a. 单击视图名称查看视图详情。
 - b. 单击数据库名称返回上级页签。
 - c. 选择“视图信息”页签，勾选视图，单击左上角的“标识”添加视图标识。
 - d. 单击给视图添加分类、密级、标签和描述等信息。
- 选择“schema信息”页签（该页签只有有schema的数据库才会显示）：
 - a. 勾选schema，单击左上角的“标识”添加列标识。
 - b. 单击给列添加分类、密级、标签和描述等信息。

----结束

相关操作

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。

4.5 资产目录

资产目录从不同“业务域”和“数据类型”两种维度统计数据资产的敏感信息，并从库表列三个维度可进行查看。


前提条件

- 已完成云资产委托授权，具体请参见[云资产委托授权/停止授权](#)进行操作。
- 已添加或者授权资产，具体请参见[资产中心](#)中添加和授权资产的操作。

查看资产目录

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“安全与合规 > 数据安全中心”。

步骤4 在左侧导航树中选择“资产管理 > 资产目录”，进入“资产目录”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**表数据目录参数说明**。

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要查看的数据资产。

表 4-12 资产目录参数说明

参数名称	参数说明
统计信息	<p>单击“查看详情”，在“敏感数据统计详情”界面，分别从“敏感数据分类维度”、“密级维度”以及“数据库维度”三个维度展示统计信息。</p> <ul style="list-style-type: none"> 敏感数据库/总库占比：统计敏感数据库在所有数据库中的占比。 敏感数据表/总表占比：统计敏感数据表在所有数据表中的占比。 敏感数据列/总列占比：统计敏感数据列在所有数据列中的占比。 <p>说明 “周同比”表示同比上周数据发生的变化。</p>
数据列密级等级占比	<p>体现不同密级敏感数据列在数据列总量中占比的饼状图。</p> <p>单击“查看详情”，在“敏感数据统计详情”界面，分别从“敏感数据分类维度”、“密级维度”以及“数据库维度”三个维度展示统计信息。</p>
分类结果TOP5	<p>分类结果占比最高的TOP5类型。</p> <p>单击“查看详情”，在“分类结果详情”界面，查看统计信息。</p>
数据量变化	<p>体现数据量随时间变化的曲线图。</p> <p>单击“查看详情”，在“敏感数据统计详情”界面，分别从“敏感数据分类维度”、“密级维度”以及“数据库维度”三个维度展示统计信息。</p>


参数名称	参数说明
库量级表	<p>展示数据库实例下包含敏感数据的库表列数量信息，具体请参见查看实例详情的内容。</p> <ul style="list-style-type: none"> • 数据库实例/ID：数据库实例名称/ID • 主机端口：主机端口号 • 用户：用户名 • 敏感数据库：该实例下有敏感数据的数据库数量。 • 敏感数据表：该实例下有敏感数据的表数量。 • 敏感数据列：该实例下有敏感数据的列数量。

----结束

查看实例详情

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“安全与合规 > 数据安全中心”。

步骤4 在左侧导航树中选择“资产管理 > 资产目录”，进入“资产目录”页面。

步骤5 单击选择“业务域”或者“数据类型”页签。

步骤6 左侧选择分组标签或者数据类型后，在“库量级表”中单击数据库实例名称，进入“实例详情”界面。

查看该实例下所有数据库信息，包含“数据库名称”、“总表数”、“敏感表数”、“敏感等级”、“标签以及最后扫描时间”。

单击数据库名称，进入“数据库详情”界面，包含“基本信息”页签和“库表数”页签。

- “基本信息”页签主要展示数据库类型、版本和名称等信息。单击重新分析，对密级进行分析，根据敏感数据识别对数据库列标记的密级等级，分析出库表的密级。
- “库表数”页签主要展示数据表名、表列数、关联模式名、分类以及密级等。单击可以查看具体详情。

图 4-14 实例详情



数据库名称	总数	引擎总数	引擎等级	标签	最后扫描时间
myod_test 60ac9c8-069a-445e-ba64-58c9205a12a	0	3	def	ddd	2024/09/17 15:31:59 GMT+08:00

----结束

5 敏感数据识别

5.1 敏感数据识别概述

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、DWS等）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。

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

图 5-1 流程图

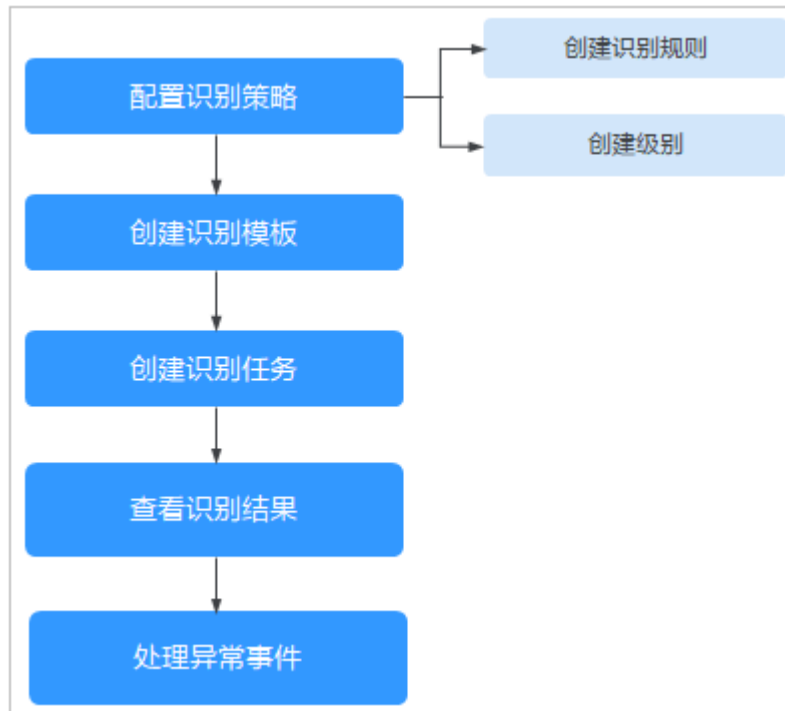


表 5-1 功能介绍

功能	描述	相关操作
识别规则	拥有华为云计算公司数据安全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。	新建自定义规则
级别配置	拥有华为云计算公司数据安全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。	新增分级
识别模板	拥有参考华为云计算公司数据安全分类分级标准和最佳实践内置的模板供使用，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。	新增识别模板
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、MRS或者LTS的指定范围中，自动识别敏感数据并生成识别数据和结果。	新建敏感数据识别任务
查看或下载识别结果	识别任务扫描完成后，可在识别任务列表查看识别结果，也可将识别结果下载到本地查看。	识别结果

5.2 敏感数据识别配置

5.2.1 新增识别模板

DSC默认内置一个识别模板，同时支持通过复制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

一个账号最多可创建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“安全与合规 > 数据安全中心”。

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”，如图5-2所示。

图 5-2 复制模板



复制模板弹框的截图。弹框标题为“复制模板”，右上角有关闭按钮。弹框内包含以下元素：

- 源模板：测试模板
- 必填项：* 新模板名称 (输入框)
- 描述：(输入框)
- 底部按钮：确定 (红色)、取消 (白色)

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。

5.2.2 管理识别模板

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。

模板创建后不支持删除。

编辑识别模板





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“安全与合规 > 数据安全中心”。

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。


- 鼠标移动至“全部”后的创建新的分类名称。
- 鼠标移动至“分类名称”时：
 - 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。
- 右侧分类规则列表左上角单击“添加规则”，具体参见[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“安全与合规 > 数据安全中心”。

- 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，如图5-3所示。

图 5-3 修改分类



- 步骤8** 单击“确定”，提示规则分类修改成功。
- 结束

5.2.3 新建自定义规则

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“安全与合规 > 数据安全中心”。
- 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，如图5-4所示。

图 5-4 识别规则列表




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5-2表配置相关参数。

表 5-2 添加规则参数配置说明

参数	说明
规则名称	<p>您可以自定义敏感数据规则名称。</p> <p>规则名称需要满足以下要求：</p> <ul style="list-style-type: none"> 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。 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	<ul style="list-style-type: none"> 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。 单击删除图标删除模板，至少保留一条模板。
匹配类型	<p>可选择“规则匹配”和“关键字匹配”。</p> <ul style="list-style-type: none"> 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。 <p>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。</p>
匹配逻辑	<p>选择匹配逻辑：</p> <ul style="list-style-type: none"> AND：关键字都需要包含。 OR：仅需要包含其中一个关键字。

参数	说明
规则	<p>“匹配类型”设置为“规则匹配”时，显示该参数，单击下拉框选择规则内容。</p> <ul style="list-style-type: none"> 选择“列名 > 包含”或者“列备注 > 包含”，输入一个关键字，判断列名或列备注中是否包含该关键字。 选择“列名 > 正则”或者“列备注 > 正则”，输入正则表达式，判断正则是否匹配。 选择“内容 > 包含”，输入一个关键字，判断内容中是否包含该关键字。 选择“内容 > 正则”，输入一个正则表达式，判断正则是否匹配。 选择“内容 > 关键字”，输入多个关键字，关键字之间是OR关系，判断内容中有任何一个关键字则为匹配。 <p>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。</p>
规则测试	<ul style="list-style-type: none"> “匹配类型”设置为“规则匹配”时，显示该参数。 输入规则内容单击测试，在测试结果框显示该条规则的测试结果。 单击“添加”，可测试多条规则。 内置规则和自定义规则均支持规则测试，内置规则请在规则列表“操作”列单击“详情”，在“编辑规则”界面，输入规则进行测试。 <p>说明</p> <ul style="list-style-type: none"> 图片类型规则不支持规则测试。 “匹配类型”为“关键字匹配”时不支持规则测试。 仅展示测试内容的第一处匹配结果。
内容	<ul style="list-style-type: none"> “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

5.2.4 编辑规则

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“安全与合规 > 数据安全中心”。

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，如图5-5所示。

图 5-5 识别规则列表



步骤6 在目标规则操作列单击“编辑”查看并修改规则。内置规则支持修改的参数有“添加到模板”。

----结束

5.2.5 查看内置规则

数据安全中心根据行业敏感信息内置了包含图片敏感信息、个人敏感信息、企业敏感信息等七类规则，具体请参见[DSC支持的内置识别规则有哪些？](#)

使用约束


营业执照照片识别目前因为OCR服务只支持部分区域，所以只有部分区域支持识别，支持的区域请参见[ORG支持的区域](#)。

其他图片内置规则使用约束请参见[护照识别约束](#)、。

查看内置规则

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“安全与合规 > 数据安全中心”。

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 在规则列表上方搜索框单击选择属性筛选规则。

----结束

护照识别约束

- 支持中国大陆护照的全字段识别。
- 支持含有完整机读码的中国-港澳台地区及外国护照识别。
- 只支持识别PNG、JPG、JPEG、BMP、TIFF格式的图片。

- 图像各边的像素大小在15到4096px8192px之间。
- 图像中护照首页区域有效占比超过25%，保证护照首页内容及其边缘包含在图像内。
- 支持图像中护照任意角度的水平旋转。
- 支持少量扭曲，扭曲后图像中的护照长宽比与实际护照相差不超过10%。
- 能处理反光、暗光等干扰的图片但影响识别精度。

5.2.6 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。


使用约束

最多只能拥有20个密级。

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“安全与合规 > 数据安全中心”。

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“新建分级”。

步骤6 在“新建分级”弹框中配置相关信息，参数说明如[表5-3](#)。

表 5-3 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”完成新建规则。

----结束

5.2.7 管理级别


如果您需要编辑或者禁用分级，请按照此章节进行操作。

编辑级别

只有自定义级别支持编辑级别内容。

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“安全与合规 > 数据安全中心”。

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

禁用级别

内置级别不支持禁用。

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“安全与合规 > 数据安全中心”。

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

5.3 敏感数据识别任务

5.3.1 新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以及LTS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

- 已完成云资产委托授权，具体请参见[云资产委托授权/停止授权](#)进行操作。
- 已添加OBS资产或者已授权数据库/大数据资产，具体请参见[资产中心](#)中添加和授权资产的操作。

新建敏感数据识别任务

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“安全与合规 > 数据安全中心”。

步骤4 在左侧导航树中，选择“敏感数据识别 > 识别任务”，进入识别任务界面，如图5-6所示。

图 5-6 识别任务列表



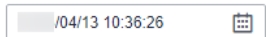
任务名称	识别模板	执行周期	状态	上次识别时间	上次识别结果	通知主题	操作
AllTest	华为云数据安全分类分级模板	单次	识别异常	2023/03/21 10:39:03 GMT+08:00	L4	-	立即识别 识别结果 更多
MRS_HIVE	华为云数据安全分类分级模板	单次	识别完成	2023/03/20 11:51:38 GMT+08:00	L3	-	立即识别 识别结果 更多

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5-4配置相关参数。

表 5-4 新建任务参数说明

参数	说明	取值样例
任务名称	<p>您可以自定义敏感数据识别任务名称。</p> <p>任务名称需要满足以下要求：</p> <ul style="list-style-type: none"> 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	<p>选择识别的数据类型，可多选。</p> <ul style="list-style-type: none"> OBS：授权DSC访问您的华为云OBS资产后，DSC将对华为云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添加OBS资产。 数据库：DSC将对已授权的数据库资产进行敏感数据识别，授权数据库资产的相关操作请参见授权数据库资产。 大数据：DSC将对已授权的大数据资产进行敏感数据识别，授权大数据源资产请参见授权大数据资产。 MRS：DSC将对已授权的MRS资产进行敏感数据识别，授权MRS资产请参见授权大数据资产。 LTS：DSC将对已授权的LTS资产进行敏感数据识别，添加日志流请参见添加日志流。 	数据库

参数	说明	取值样例
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。添加模板请参见 新增识别模板 。	华为云数据安全分类分级模板
识别范围	当“数据类型”选择“LTS”显示该参数，请选择识别日志范围，可选1天、2天和3天。	1天
识别灵敏度	当“数据类型”选择“LTS”显示该参数，请选择识别日志的灵敏度，有高、中、低三种程度供选择，灵敏度越高采样数据越多。	低
识别周期	设置数据识别任务的执行策略： <ul style="list-style-type: none"> • 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： <ul style="list-style-type: none"> • 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。	
通知主题（可选）	<ul style="list-style-type: none"> • 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。 • 如果不配置通知主题，可在识别任务列表查看识别结果，详情请参考识别结果。 	无

步骤7 （可选）如果需要对添加的资产设置扫描范围，详细操作请参见[添加识别范围](#)章节。

步骤8 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

添加识别范围

DSC默认对选择的资产进行全局扫描，您也可以参考本章节的内容添加具体的扫描范围。

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“安全与合规 > 数据安全中心”。

步骤4 在左侧导航树中，选择“敏感数据识别 > 识别任务”，进入识别任务界面，如图5-7所示。

图 5-7 识别任务列表



任务名称	识别模板	执行周期	状态	上次识别时间	上次识别结果	通知主题	操作
AllTest	华为云数据安全分类分级模板	单次	识别异常	2023/03/21 10:39:03 GMT+08:00	L4	-	立即识别 识别结果 更多
MRS_HIVE	华为云数据安全分类分级模板	单次	识别完成	2023/03/20 11:51:38 GMT+08:00	L3	-	立即识别 识别结果 更多

步骤5 单击“新建任务”，进入“新建任务”界面。

步骤6 勾选数据类型并选择具体扫描资产名称，单击“确定”。

步骤7 在新建识别任务界面左下角单击添加识别范围，进行扫描范围配置，可以同时添加多项识别范围，参数配置如表5-5所示。

表 5-5 扫描范围配置参数说明

资产类型	配置参数	说明
OBS	资产	单击下拉框选择需要扫描的桶，支持多选。
	扫描范围配置	<ul style="list-style-type: none"> “文件名前缀”：如：前缀为 <i>dsc_</i> 时就会扫描所有前缀为 <i>dsc_</i> 的文件。 文件名前缀的包含条件最多只能添加1个。 “文件名后缀”：文件名后缀包括"."后面的文件类型，如：<i>dsc_security.txt</i>后缀可以是 <i>security.txt</i> 或者 <i>.txt</i> 等所有条件为组合关系，只扫描满足所有筛选条件的文件。 文件名后缀的包含条件最多只能添加1个。 “目录名”：扫描指定目录名下的所有文件。 目录名包含条件最多只能添加1个。 填写文件名前缀/后缀/目录名称后，单击“添加为包含条件”将其添加为包含条件。 如：选择“文件名前缀”，输入前缀为 <i>dsc_</i> ，单击“添加为包含条件”，添加到包含条件，扫描时只会对文件名前缀为 <i>dsc_</i> 的文件进行扫描。如果单击“添加为不包含条件”，添加到不包含条件，则扫描时只会扫描前缀除了 <i>dsc_</i> 以外的文件。
	扫描深度	<ul style="list-style-type: none"> “全局扫描”：如果选择全局扫描是对全部数据进行扫描。 “指定扫描范围”：也可以选择“指定扫描范围”，输入“扫描深度”，根目录深度为1，依次类推，根目录深度值不能超过10。

资产类型	配置参数	说明
数据库/ 大数据/ MRS	资产	单击下拉框选择实例名称，支持多选。
	扫描范围配置	<ul style="list-style-type: none"> “前缀”：前缀的包含条件最多只能添加1个。如：输入前缀为 <i>dsc</i> 时，单击“添加为包含条件”添加为包含条件后就会只扫描表前缀为 <i>dsc</i> 的表数据。如果单击“添加为不包含条件”添加为不包含条件就只扫描表明前缀除 <i>dsc</i> 以外的表数据。 “后缀”：后缀的包含条件最多只能添加1个。原理如同表明前缀所示。
LTS	资产	单击下拉框选择实例名称，支持多选。
	扫描范围配置	<ul style="list-style-type: none"> “key前缀”：添加为包含条件会扫描包含该key前缀的日志内容。添加为不包含条件会扫描除该key前缀的日志内容。 “key后缀”：原理如同key前缀所示。 <p>说明</p> <ul style="list-style-type: none"> key前缀和key后缀最多可各添加1个包含条件。 key前缀和key后缀总共可以添加10个不包含条件。

图 5-8 OBS 扫描范围配置

+ 添加OBS识别范围

OBS扫描配置1× 取消

资产 请选择

扫描范围 指定扫描范围 ?

文件名前缀

添加为包含条件

添加为不包含条件

包含条件	类型	操作	不包含条件	类型	操作

扫描深度 全局扫描 指定扫描范围 ?

----结束

后续处理

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。

5.3.2 立即启动识别任务

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

- 已完成云资产委托授权，具体请参见[云资产委托授权/停止授权](#)进行操作。
- 已添加或者授权资产，具体请参见[资产中心](#)中添加和授权资产的操作。

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“安全与合规 > 数据安全中心”。

步骤4 在左侧导航树中，选择“敏感数据识别 > 识别任务”，进入识别任务界面，如[图5-9](#)所示。

图 5-9 识别任务列表



任务名称	识别模板	执行周期	状态	上次识别时间	上次识别结果	通知主题	操作
ALLTest	华为云数据安全分级模板	单次	识别异常	2023/03/21 10:39:03 GMT+08:00	L4	--	立即识别 识别结果 更多
MRS_HIVE	华为云数据安全分级模板	单次	识别成功	2023/03/20 11:51:38 GMT+08:00	L3	--	立即识别 识别结果 更多

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

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。

5.3.3 管理识别任务列表

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

- 已完成云资产委托授权，具体请参见[云资产委托授权/停止授权](#)进行操作。
- 已添加或者授权资产，具体请参见[资产中心](#)中添加和授权资产的操作。

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“安全与合规 > 数据安全中心”。

步骤4 在左侧导航树中，单击“敏感数据识别 > 识别任务”，进入识别任务界面查看任务详情，相关参数如[表5-6](#)。

图 5-10 识别任务列表

任务名称	识别模板	执行周期	状态	上次识别时间	上次识别结果	通知主题	操作
ALLTest	华为云数据安全分类分级模板	单次	识别异常	2023/03/21 10:39:03 GMT+08:00	L4	-	立即识别 识别结果 更多
MRS_HIVE	华为云数据安全分类分级模板	单次	识别完成	2023/03/20 11:51:38 GMT+08:00	L3	-	立即识别 识别结果 更多

表 5-6 识别任务参数

参数	说明
任务名称	<p>识别任务名称。</p> <p>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：</p> <ul style="list-style-type: none"> 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	<p>识别任务的具体执行周期。说明如下：</p> <ul style="list-style-type: none"> 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	<p>识别任务的执行状态。</p> <ul style="list-style-type: none"> 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 新建分级 章节。


参数	说明
操作	<p>用户可以在操作栏中，执行以下操作：</p> <ul style="list-style-type: none"> 立即执行识别任务，具体的参见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为您提供详细的结果分析报告，具体的参见识别结果章节。 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。 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“安全与合规 > 数据安全中心”。

步骤4 在左侧导航树中，选择“敏感数据识别 > 识别任务”，进入识别任务界面，如图5-11所示。

图 5-11 识别任务列表



任务名称	识别模板	执行周期	状态	上次识别时间	上次识别结果	通知主题	操作
ALLTest	华为云数据安全分级模板	单次	识别异常	2023/03/21 10:39:03 GMT+08:00	L4	--	立即识别 识别结果 更多
MRS_HIVE	华为云数据安全分级模板	单次	识别完成	2023/03/20 11:51:38 GMT+08:00	L3	--	立即识别 识别结果 更多

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“安全与合规 > 数据安全中心”。

步骤4 在左侧导航树中，选择“敏感数据识别 > 识别任务”，进入识别任务界面，如图5-11所示。

图 5-12 识别任务列表

任务名称	识别模板	执行周期	状态	上次识别时间	上次识别结果	通知主题	操作
ALLTest	华为云数据安全分类分级模板	单次	识别异常	2023/03/21 10:30:03 GMT+08:00	L4	--	立即识别 识别结果 更多
MRS_HIVE	华为云数据安全分类分级模板	单次	识别完成	2023/03/20 11:51:38 GMT+08:00	L3	--	立即识别 识别结果 更多

步骤5 在目标任务“操作”列单击“更多 > 删除”，如图5-13所示。

图 5-13 确认删除



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“安全与合规 > 数据安全中心”。

步骤4 在左侧导航树中，选择“敏感数据识别 > 识别任务”，进入识别任务界面，如图5-11所示。

图 5-14 识别任务列表

任务名称	识别模板	执行周期	状态	上次识别时间	上次识别结果	通知主题	操作
ALLTest	华为云数据安全分类分级模板	单次	识别异常	2023/03/21 10:30:03 GMT+08:00	L4	--	立即识别 识别结果 更多
MRS_HIVE	华为云数据安全分类分级模板	单次	识别完成	2023/03/20 11:51:38 GMT+08:00	L3	--	立即识别 识别结果 更多

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

5.3.4 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”、“Top10命中规则”以及敏感信息分类分级结果并生成结果文件，下载到本地查看。

前提条件

至少执行过一次敏感数据识别任务。

查看识别结果

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“安全与合规 > 数据安全中心”。

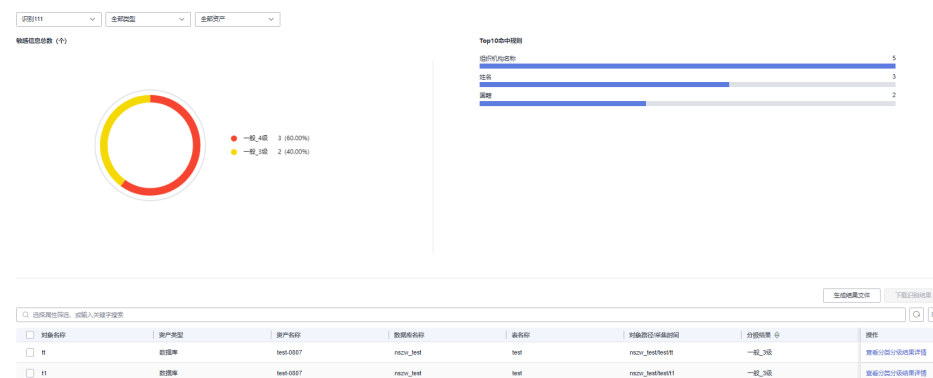
步骤4 在左侧导航树中，选择“敏感数据识别 > 识别任务”，进入识别任务界面，如图5-15所示。

图 5-15 识别任务列表

任务名称	识别模板	执行周期	状态	上次识别时间	上次识别结果	通知主题	操作
ALLTest	华为云数据安全分类分级模板	单次	识别异常	2023/03/21 10:39:03 GMT+08:00	L4	--	立即识别 识别结果 更多
MRS_HIVE	华为云数据安全分类分级模板	单次	识别完成	2023/03/20 11:51:38 GMT+08:00	L3	--	立即识别 识别结果 更多

步骤5 单击目标任务“操作”列的“识别结果”，进入“结果明细”界面。

图 5-16 识别结果明细



步骤6 DSC分别统计了大数据、数据库、OBS、MRS和LTS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，单击列表左上角筛选框，选择筛选项，可通过“对象名称”、“数据库名称”、“表名称”等，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5-7所示。

表 5-7 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	<ul style="list-style-type: none"> ● OBS ● 数据库 ● 大数据 ● MRS ● LTS
资产名称	涉及敏感信息资产名称。
数据库名称	敏感信息所在数据库名称。
表名称	敏感信息所在表名称。
桶名称	资产类型为OBS时显示桶名称。
对象路径/采集时间	敏感信息存储的对象路径/采集时间。
分级结果	敏感信息级别。

步骤7 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，如图5-17所示。

查看结果详情和具体的样例数据。

图 5-17 分类分级结果详情



说明


- “分类分级结果详情”页主要展示“识别对象详情”、“结果详情”和“样例数据”。
- “结果详情”展示识别对象的“匹配规则”、“分级结果”、“分类结果”以及“分类分级模板”。
- 单击“样例数据”页签查看匹配该规则的样例数据信息，目前大数据类型和LTS不支持查看样例数据。

----结束

下载识别结果

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“安全与合规 > 数据安全中心”。

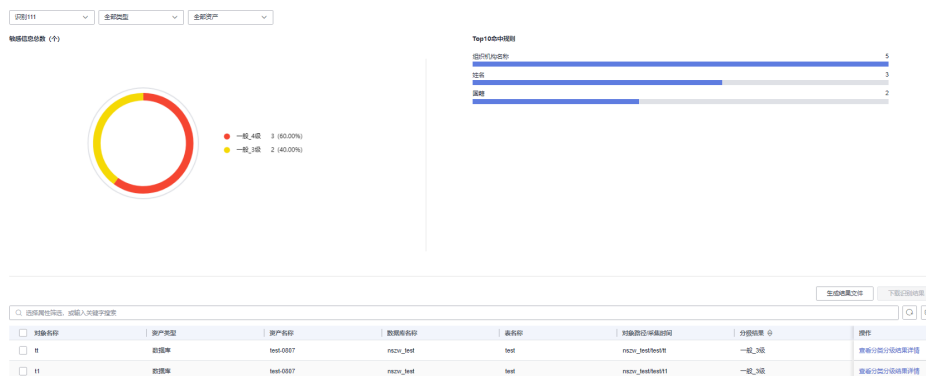
步骤4 在左侧导航树中，选择“敏感数据识别 > 识别任务”，进入“识别任务”界面，如图 5-18 所示。

图 5-18 识别任务列表

任务名称	识别模板	执行周期	状态	上次识别时间	上次识别结果	通知主题	操作
ALLTest	华为云数据安全分类分级模板	单次	识别异常	2023/03/21 10:39:03 GMT+08:00	L4	--	立即识别 识别结果 更多
MRS_HIVE	华为云数据安全分类分级模板	单次	识别完成	2023/03/20 11:51:38 GMT+08:00	L3	--	立即识别 识别结果 更多

步骤5 单击目标任务“操作”列的“识别结果”，进入“结果明细”界面。

图 5-19 识别结果明细



步骤6 单击“生成结果文件”，进入“生成结果文件”弹框。

- “识别任务”：对应的扫描任务名称。
- “扫描对象类型”：选择的扫描对象类型。
- “扫描对象”：选择的扫描对象。
- “导出目标桶”：单击下拉框选择存储识别结果的OBS桶，如果下拉框没有可选择的桶请参照[创建OBS桶](#)创建桶。生成的识别结果将在该桶的根目录创建一个“scan-results”的文件夹存储结果文件。
- “样例数据脱敏”：样例数据脱敏开关只针对支持查看样例数据的资产，如数据库资产，OBS。如果不开启样例数据脱敏，识别结果将会导出明文样例数据，请下载后及时删除。

说明

识别结果列表支持筛选，筛选后生成的结果是筛选后的数据。

使用OBS存储会占用一定的存储空间，可能会产生费用，具体收费请参见[OBS计费说明](#)。

图 5-20 生成结果文件确认框



步骤7 单击“确定”，生成对应资产的敏感数据扫描结果报告，右上角提示“生成识别结果导出文件成功”，“生成结果文件”的状态将变成“排队中”或“运行中”。

- 生成结果文件的状态包含：
 - 运行中：结果报告正在生成中。
 - 排队中：生成任务排队中。
- 如果“下载识别结果”不可单击且提示“暂无有效下载文件，请先生成文件”，请单击“生成结果文件”生成后再下载。

📖 说明

同一个识别任务下不同子任务生成识别结果文件会互相覆盖。

步骤8 单击“下载识别结果”，进入“下载识别结果”弹框，可以查看下载报告包含的“识别任务”、“扫描对象类型”、“扫描对象”、“生成时间”以及“文件路径”。

“文件路径”为**步骤7**生成的识别结果Excel文件存储的OBS路径。

图 5-21 下载识别结果确认框



步骤9 单击“确定”，将识别结果下载到本地，如果需要下载历史的识别结果请参考**OBS下载对象**进行下载。

Excel格式的识别结果报表包含“资产名称（资产类型）”分页签展示识别结果，关键字段有“匹配规则”、“分级结果”、“分类结果”和“分类分级模板”。

图 5-22 识别结果报表样例

A	B	C	D	E	F	G	H	I
资产名称	数据库	数据表	数据列	匹配规则	分级结果	分类结果	分类分级模板	样例数据
scan_db	scan_db	scan.rule_test	zuzhi	组织机构代码	L1	企业标识信息	7	31195515-4
scan_db	scan_db	scan.rule_test	zidingyi	0921自定义	L1	个人一般信息	7	test

----结束

6 策略中心

6.1 策略基线

6.1.1 概述

策略基线是数据安全管理制度、数据分类分级要求、数据出境管理规定、重要数据和核心数据要求等数据安全策略结构化，DSC依据华为云数据安全治理经验预置策略模板，支持策略的增删改查、策略的结构化展示和过滤查询等。

企业通过配置实施统一的数据安全保护策略，实现从敏感数据发现、识别、保护、监督到治理的一体化协同保护措施，满足数据安全与个人信息保护合规要求，简化数据安全治理，让企业的数据更安全、更合规，更高效。

使用场景

初始化阶段，企业管理员进入DSC策略中心界面，定义企业的数据安全保护策略基线。支持对数据全生命周期的策略配置。

相关功能联动


与资产地图联动：

- 进入“资产地图”，选择某个资产，进入安全防护策略分析页面，查看资产的加密、备份、审计等安全配置的现状和策略基线的具体要求，并可跳转策略/任务配置页面进行策略/任务配置。
- 进入“资产地图”，单击“评分详情”，可查看所有资产的加密、备份、审计等安全配置的现状和策略基线的具体要求，并可跳转策略/任务配置页面进行策略/任务配置。

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“安全与合规 > 数据安全中心”。

步骤4 在左侧导航树中，选择“策略中心 > 策略基线”，进入“策略基线”界面，如图6-1所示。

图 6-1 基线策略



----结束

6.1.2 数据采集

配置措施

步骤1 参照**操作步骤**进入“策略基线”界面。

步骤2 单击“配置措施”进入“配置措施”界面。

步骤3 单击取消不需要的措施，取消勾选的措施将不会在策略基线表中显示。

内置措施：DSC针对数据不同周期依据华为云数据安全治理经验内置相应的措施，鼠标移动到措施名称可以查看内置措施的说明。

步骤4 自定义措施：新增的自定义措施将显示在基线策略表中。

- 单击“新增”，进入“新增自定义保护措施”界面。
- 填写“措施名称”和“措施说明”单击“确定”返回“配置措施”界面可查看新增的措施。
- 单击“操作”列的“编辑”可修改该措施，单击“删除”删除不需要的措施。

图 6-2 自定义措施

配置措施

内置措施

分类分级 跟踪记录 数据源安全认证 加密

自定义措施

新增

选择属性筛选，或输入关键字搜索

措施名称	措施说明	操作
解密	--	删除 编辑

步骤5 单击“确定”进入策略基线表查看配置措施。

图 6-3 策略基线列表



----结束

配置数据保护类型

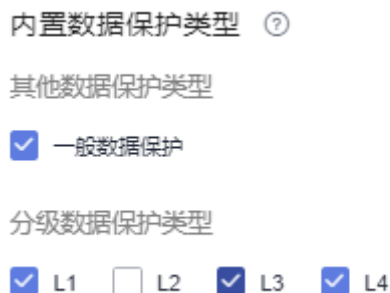
步骤1 参照[操作步骤](#)进入“策略基线”界面。

步骤2 单击“配置数据保护类型”进入“配置数据保护类型”界面。

步骤3 内置数据保护类型：如果取消勾选，在基线策略表格该类型不再显示，且默认配置的各项策略要求将清空，下次启用需自定义该保护类型的策略要求

- 一般数据保护：没有通过敏感数据识别分级分类的数据使用一般数据保护。
- 分级数据保护类型：通过敏感数据识别分级分类的数据可使用分级数据保护，DSC有内置的敏感数据级别L1-L4，去勾选策略基线列表将不展示。

图 6-4 内置数据保护类型



步骤4 自定义数据保护类型：新增的自定义数据保护类型将显示到策略基线表中。

单击下拉框选择自定义级别，如果没有可选择的自定义级别，请参照[新建分级](#)进行新建。

图 6-5 自定义数据保护类型



步骤5 单击“确定”，在策略基线表中查看数据保护类型。

图 6-6 数据资产保护类型

数据保护类型	分类分级	留存记录	加密	审计
一般数据保护	不要求	不要求	不要求	不要求
<input checked="" type="checkbox"/> 分级数据保护				
L1	不要求	建议	不要求	不要求
L3	不要求	强制	建议	不要求
L4	不要求	强制	强制	不要求
一般_1级	不要求	不要求	不要求	不要求

----结束

修改保护要求

步骤1 参照**操作步骤**进入“策略基线”界面。

步骤2 单击“修改保护要求”可对数据保护类型对应措施的保护要求进行修改。

步骤3 如单击“一般数据保护”行的“分类分级”列的下拉框选择：

- 不要求
- 建议
- 强制

图 6-7 修改保护要求

数据保护类型	分类分级	留存记录	加密	审计
一般数据保护	不要求	不要求	不要求	不要求
<input checked="" type="checkbox"/> 分级数据保护				
L1	不要求	建议	不要求	不要求
L3	不要求	强制	建议	不要求
L4	不要求	强制	强制	不要求
一般_1级	不要求	不要求	不要求	不要求

步骤4 修改完成，单击左上角“保存修改”。如果需要取消修改，单击左上角的“取消修改”返回上次保护要求。

----结束

6.1.3 数据传输

配置措施

步骤1 参照**操作步骤**进入“策略基线”界面。

步骤2 选择“传输”页签。

步骤3 单击“配置措施”进入“配置措施”界面。

步骤4 单击取消不需要的措施，取消勾选的措施将不会在策略基线表中显示。

内置措施：DSC针对数据不同周期依据华为云数据安全治理经验内置相应的措施，鼠标移动到措施名称可以查看内置措施的说明。

步骤5 自定义措施：新增的自定义措施将显示在基线策略表中。

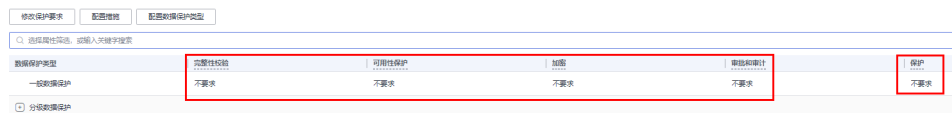
1. 单击“新增”，进入“新增自定义保护措施”界面。
2. 填写“措施名称”和“措施说明”单击“确定”返回“配置措施”界面可查看新增的措施。
3. 单击“操作”列的“编辑”可修改该措施，单击“删除”删除不需要的措施。

图 6-8 自定义措施



步骤6 单击“确定”进入策略基线表查看配置措施。

图 6-9 策略基线列表

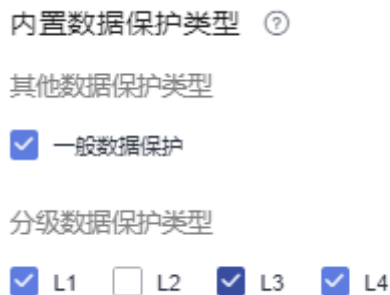


----结束

配置数据保护类型

- 步骤1 参照[操作步骤](#)进入“策略基线”界面。
- 步骤2 选择“传输”页签。
- 步骤3 单击“配置数据保护类型”进入“配置数据保护类型”界面。
- 步骤4 内置数据保护类型：如果取消勾选，在基线策略表格该类型不再显示，且默认配置的各项策略要求将清空，下次启用需自定义该保护类型的策略要求
 - 一般数据保护：没有通过敏感数据识别分级分类的数据使用一般数据保护。
 - 分级数据保护类型：通过敏感数据识别分级分类的数据可使用分级数据保护，DSC有内置的敏感数据级别L1-L4，去勾选策略基线列表将不展示。

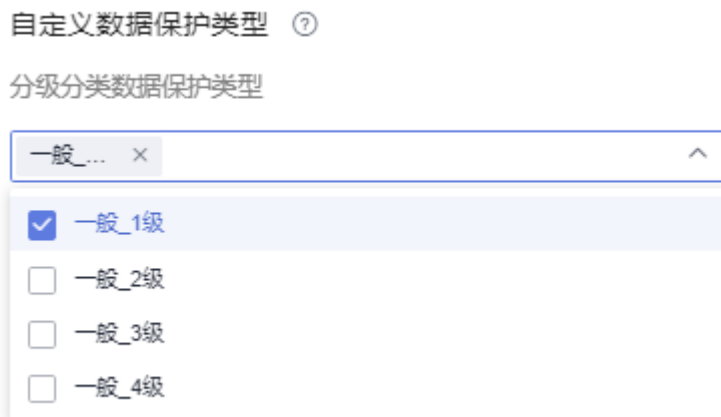
图 6-10 内置数据保护类型



步骤5 自定义数据保护类型：新增的自定义数据保护类型将显示到策略基线表中。

单击下拉框选择自定义级别，如果没有可选择的自定义级别，请参照[新建分级](#)进行新建。

图 6-11 自定义数据保护类型



步骤6 单击“确定”，在策略基线表中查看数据保护类型。

图 6-12 数据资产保护类型

数据保护类型	完整性控制	可用性保护	加密	备份和审计	保护
一般的数据保护	不要求	不要求	不要求	不要求	不要求
<input type="checkbox"/> 分级的数据资产					
L1	● 强制	● 建议	不要求	不要求	不要求
L3	● 强制	● 强制	● 强制	● 强制	不要求
L4	● 强制	● 强制	● 强制	● 强制	不要求
<input type="checkbox"/> 一般_2级	不要求	不要求	不要求	不要求	不要求

----结束

修改保护要求

步骤1 参照[操作步骤](#)进入“策略基线”界面。

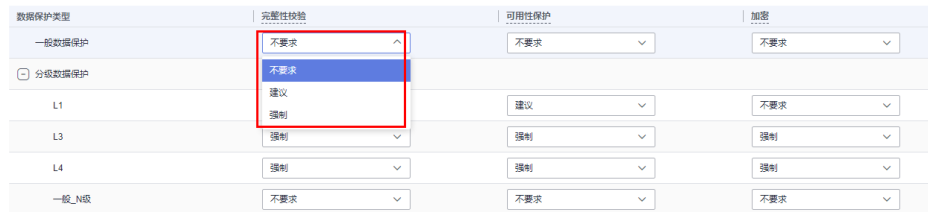
步骤2 选择“传输”页签。

步骤3 单击“修改保护要求”可对数据保护类型对应措施的保护要求进行修改。

步骤4 如单击“一般数据保护”行的“分类分级”列的下拉框选择：

- 不要求
- 建议
- 强制

图 6-13 修改保护要求



步骤5 修改完成，单击左上角“保存修改”。如果需要取消修改，单击左上角的“取消修改”返回上次保护要求。

----结束

6.1.4 数据存储

配置措施

步骤1 参照[操作步骤](#)进入“策略基线”界面。

步骤2 选择“存储”页签。

步骤3 单击“配置措施”进入“配置措施”界面。

步骤4 单击取消不需要的措施，取消勾选的措施将不会在策略基线表中显示。

内置措施：DSC针对数据不同周期依据华为云数据安全治理经验内置相应的措施，鼠标移动到措施名称可以查看内置措施的说明。

步骤5 自定义措施：新增的自定义措施将显示在基线策略表中。

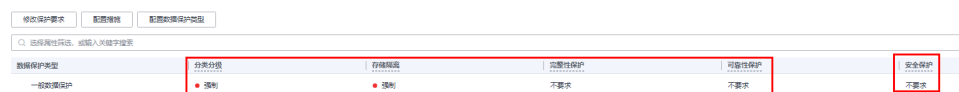
1. 单击“新增”，进入“新增自定义保护措施”界面。
2. 填写“措施名称”和“措施说明”单击“确定”返回“配置措施”界面可查看新增的措施。
3. 单击“操作”列的“编辑”可修改该措施，单击“删除”删除不需要的措施。

图 6-14 自定义措施



步骤6 单击“确定”进入策略基线表查看配置措施。

图 6-15 策略基线列表



----结束

配置数据保护类型

步骤1 参照**操作步骤**进入“策略基线”界面。

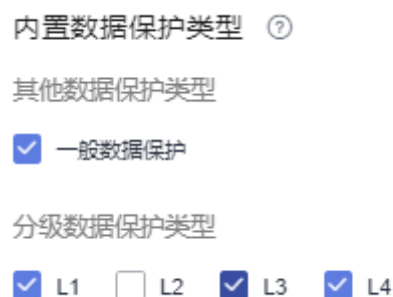
步骤2 选择“存储”页签。

步骤3 单击“配置数据保护类型”进入“配置数据保护类型”界面。

步骤4 内置数据保护类型：如果取消勾选，在基线策略表格该类型不再显示，且默认配置的各项策略要求将清空，下次启用需自定义该保护类型的策略要求

- 一般数据保护：没有通过敏感数据识别分级分类的数据使用一般数据保护。
- 分级数据保护类型：通过敏感数据识别分级分类的数据可使用分级数据保护，DSC有内置的敏感数据级别L1-L4，去勾选策略基线列表将不展示。

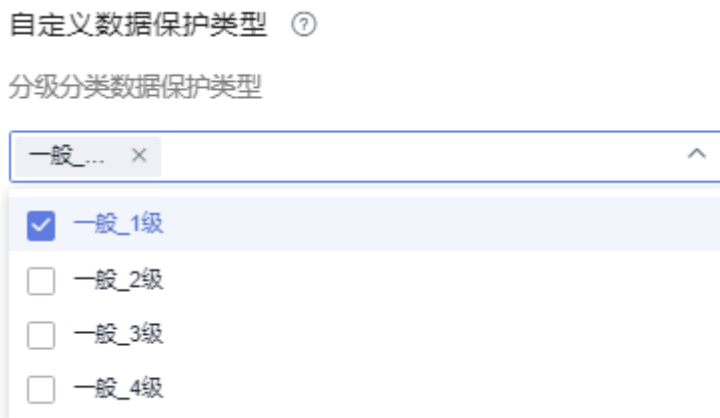
图 6-16 内置数据保护类型



步骤5 自定义数据保护类型：新增的自定义数据保护类型将显示到策略基线表中。

单击下拉框选择自定义级别，如果没有可选择的自定义级别，请参照[新建分级](#)进行新建。

图 6-17 自定义数据保护类型



步骤6 单击“确定”，在策略基线表中查看数据保护类型。

图 6-18 数据资产保护类型

数据保护类型	分类分级	存储隔离	完整性保护	可用性保护	安全保护
一般数据保护	强制	强制	不要求	不要求	不要求
分级数据保护	不要求	不要求	强制	不要求	不要求
L1	不要求	不要求	强制	强制	不要求
L3	不要求	不要求	强制	强制	不要求
L4	不要求	不要求	强制	强制	不要求
一般_1级	不要求	不要求	不要求	不要求	不要求

----结束

修改保护要求

步骤1 参照[操作步骤](#)进入“策略基线”界面。

步骤2 选择“存储”页签。

步骤3 单击“修改保护要求”可对数据保护类型对应措施的保护要求进行修改。

步骤4 如单击“一般数据保护”行的“分类分级”列的下拉框选择：

- 不要求
- 建议
- 强制

图 6-19 修改保护要求

步骤5 修改完成，单击左上角“保存修改”。如果需要取消修改，单击左上角的“取消修改”返回上次保护要求。

----结束

6.1.5 数据使用

配置措施

步骤1 参照**操作步骤**进入“策略基线”界面。

步骤2 选择“使用”页签。

步骤3 单击“配置措施”进入“配置措施”界面。

步骤4 单击取消不需要的措施，取消勾选的措施将不会在策略基线表中显示。

内置措施：DSC针对数据不同周期依据华为云数据安全治理经验内置相应的措施，鼠标移动到措施名称可以查看内置措施的说明。

步骤5 自定义措施：新增的自定义措施将显示在基线策略表中。

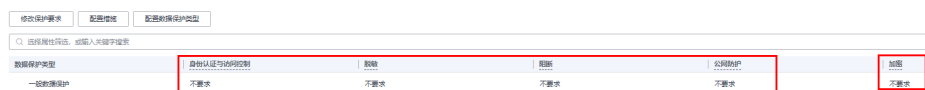
1. 单击“新增”，进入“新增自定义保护措施”界面。
2. 填写“措施名称”和“措施说明”单击“确定”返回“配置措施”界面可查看新增的措施。
3. 单击“操作”列的“编辑”可修改该措施，单击“删除”删除不需要的措施。

图 6-20 自定义措施



步骤6 单击“确定”进入策略基线表查看配置措施。

图 6-21 策略基线列表

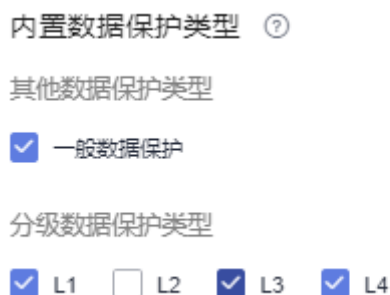


----结束

配置数据保护类型

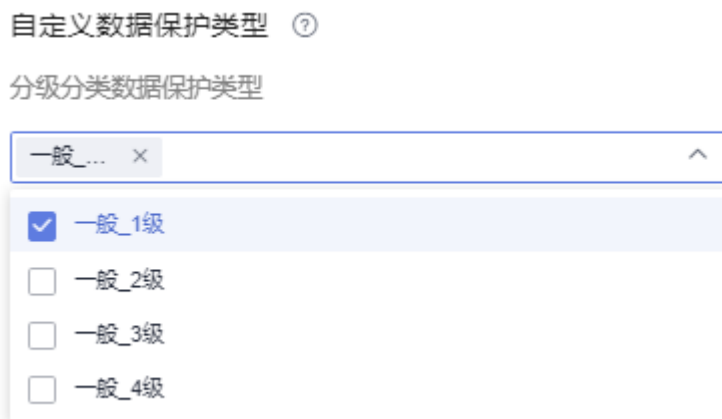
- 步骤1** 参照[操作步骤](#)进入“策略基线”界面。
- 步骤2** 选择“使用”页签。
- 步骤3** 单击“配置数据保护类型”进入“配置数据保护类型”界面。
- 步骤4** 内置数据保护类型：如果取消勾选，在基线策略表格该类型不再显示，且默认配置的各项策略要求将清空，下次启用需自定义该保护类型的策略要求
- 一般数据保护：没有通过敏感数据识别分级分类的数据使用一般数据保护。
 - 分级数据保护类型：通过敏感数据识别分级分类的数据可使用分级数据保护，DSC有内置的敏感数据级别L1-L4，去勾选策略基线列表将不展示。

图 6-22 内置数据保护类型



- 步骤5** 自定义数据保护类型：新增的自定义数据保护类型将显示到策略基线表中。
- 单击下拉框选择自定义级别，如果没有可选择的自定义级别，请参照[新建分级](#)进行新建。

图 6-23 自定义数据保护类型



- 步骤6** 单击“确定”，在策略基线表中查看数据保护类型。

图 6-24 数据资产保护类型

数据保护类型	身份认证与访问控制	脱敏	加密	公钥保护	加密
一般数据保护	不要求	不要求	不要求	不要求	不要求
<input checked="" type="checkbox"/> 分級数据保护					
L1	● 建议	不要求	● 建议	不要求	不要求
L3	● 强制	● 强制	● 强制	● 强制	不要求
L4	● 强制	● 强制	● 强制	● 强制	不要求
一般_1级	不要求	不要求	不要求	不要求	不要求

----结束

修改保护要求

- 步骤1 参照[操作步骤](#)进入“策略基线”界面。
- 步骤2 选择“使用”页签。
- 步骤3 单击“修改保护要求”可对数据保护类型对应措施的保护要求进行修改。
- 步骤4 如单击“一般数据保护”行的“身份认证与访问控制”列的下拉框选择：
 - 不要求
 - 建议
 - 强制

图 6-25 修改保护要求

数据保护类型	身份认证与访问控制	脱敏	加密	公钥保护	加密
一般数据保护	不要求	不要求	不要求	不要求	不要求
<input checked="" type="checkbox"/> 分級数据保护					
L1	● 建议	不要求	● 建议	不要求	不要求
L3	● 强制	● 强制	● 强制	● 强制	不要求
L4	● 强制	● 强制	● 强制	● 强制	不要求
一般_1级	不要求	不要求	不要求	不要求	不要求

- 步骤5 修改完成，单击左上角“保存修改”。如果需要取消修改，单击左上角的“取消修改”返回上次保护要求。

----结束

6.1.6 数据共享

配置措施

- 步骤1 参照[操作步骤](#)进入“策略基线”界面。
- 步骤2 选择“共享”页签。
- 步骤3 单击“配置措施”进入“配置措施”界面。
- 步骤4 单击取消不需要的措施，取消勾选的措施将不会在策略基线表中显示。

内置措施：DSC针对数据不同周期依据华为云数据安全治理经验内置相应的措施，鼠标移动到措施名称可以查看内置措施的说明。
- 步骤5 自定义措施：新增的自定义措施将显示在基线策略表中。

1. 单击“新增”，进入“新增自定义保护措施”界面。
2. 填写“措施名称”和“措施说明”单击“确定”返回“配置措施”界面可查看新增的措施。
3. 单击“操作”列的“编辑”可修改该措施，单击“删除”删除不需要的措施。

图 6-26 自定义措施



步骤6 单击“确定”进入策略基线表查看配置措施。

图 6-27 策略基线列表

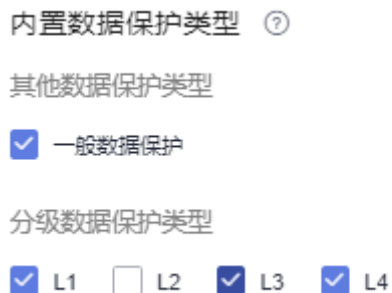


----结束

配置数据保护类型

- 步骤1 参照**操作步骤**进入“策略基线”界面。
- 步骤2 选择“共享”页签。
- 步骤3 单击“配置数据保护类型”进入“配置数据保护类型”界面。
- 步骤4 内置数据保护类型：如果取消勾选，在基线策略表格该类型不再显示，且默认配置的各项策略要求将清空，下次启用需自定义该保护类型的策略要求
 - 一般数据保护：没有通过敏感数据识别分级分类的数据使用一般数据保护。
 - 分级数据保护类型：通过敏感数据识别分级分类的数据可使用分级数据保护，DSC有内置的敏感数据级别L1-L4，去勾选策略基线列表将不展示。

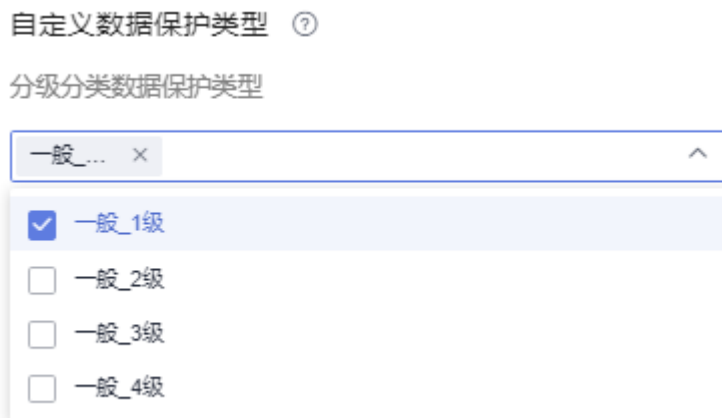
图 6-28 内置数据保护类型



步骤5 自定义数据保护类型：新增的自定义数据保护类型将显示到策略基线表中。

单击下拉框选择自定义级别，如果没有可选择的自定义级别，请参照[新建分级](#)进行新建。

图 6-29 自定义数据保护类型



步骤6 单击“确定”，在策略基线表中查看数据保护类型。

----结束

修改保护要求

步骤1 参照[操作步骤](#)进入“策略基线”界面。

步骤2 选择“共享”页签。

步骤3 单击“修改保护要求”可对数据保护类型对应措施的保护要求进行修改。

步骤4 如单击“一般数据保护”行的“安全审计”列的下拉框选择：

- 不要求
- 建议
- 强制

图 6-30 修改保护要求

数据保护类型	安全审计	删除	脱敏	审核与监督	安全保护
一般数据保护	不要求	不要求	不要求	不要求	不要求
<input type="checkbox"/> 台级数据保护	不要求				
	建议				
	强制				
L1	不要求	不要求	不要求	不要求	不要求
	强制	建议	建议	建议	不要求
L2	强制	强制	强制	强制	不要求
L3	强制	强制	强制	强制	不要求
L4	强制	强制	强制	强制	不要求

步骤5 修改完成，单击左上角“保存修改”。如果需要取消修改，单击左上角的“取消修改”返回上次保护要求。

---结束

6.1.7 数据销毁

配置措施

步骤1 参照[操作步骤](#)进入“策略基线”界面。

步骤2 选择“销毁”页签。

步骤3 单击“配置措施”进入“配置措施”界面。

步骤4 单击取消不需要的措施，取消勾选的措施将不会在策略基线表中显示。

内置措施：DSC针对数据不同周期依据华为云数据安全治理经验内置相应的措施，鼠标移动到措施名称可以查看内置措施的说明。

步骤5 自定义措施：新增的自定义措施将显示在基线策略表中。

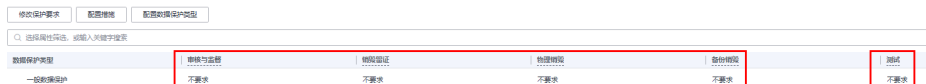
- 单击“新增”，进入“新增自定义保护措施”界面。
- 填写“措施名称”和“措施说明”单击“确定”返回“配置措施”界面可查看新增的措施。
- 单击“操作”列的“编辑”可修改该措施，单击“删除”删除不需要的措施。

图 6-31 自定义措施



步骤6 单击“确定”进入策略基线表查看配置措施。

图 6-32 策略基线列表

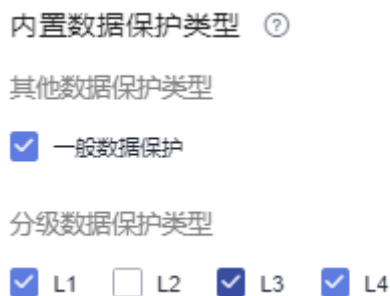


----结束

配置数据保护类型

- 步骤1** 参照[操作步骤](#)进入“策略基线”界面。
- 步骤2** 选择“销毁”页签。
- 步骤3** 单击“配置数据保护类型”进入“配置数据保护类型”界面。
- 步骤4** 内置数据保护类型：如果取消勾选，在基线策略表格该类型不再显示，且默认配置的各项策略要求将清空，下次启用需自定义该保护类型的策略要求
- 一般数据保护：没有通过敏感数据识别分级分类的数据使用一般数据保护。
 - 分级数据保护类型：通过敏感数据识别分级分类的数据可使用分级数据保护，DSC有内置的敏感数据级别L1-L4，去勾选策略基线列表将不展示。

图 6-33 内置数据保护类型



- 步骤5** 自定义数据保护类型：新增的自定义数据保护类型将显示到策略基线表中。
- 单击下拉框选择自定义级别，如果没有可选择的自定义级别，请参照[新建分级](#)进行新建。

图 6-34 自定义数据保护类型



步骤6 单击“确定”，在策略基线表中查看数据保护类型。

图 6-35 数据资产保护类型

数据保护类型	审核与监督	加密保证	物理销毁	软件销毁	测试
一般数据保护	不要求	不要求	不要求	不要求	不要求
<input checked="" type="checkbox"/> 分级数据保护					
L1	不要求	强制	不要求	建议	不要求
L3	强制	强制	强制	强制	不要求
L4	强制	强制	强制	强制	不要求
一般_L1级	不要求	不要求	不要求	不要求	不要求

----结束

修改保护要求

步骤1 参照**操作步骤**进入“策略基线”界面。

步骤2 选择“销毁”页签。

步骤3 单击“修改保护要求”可对数据保护类型对应措施的保护要求进行修改。

步骤4 如单击“一般数据保护”行的“审核与监督”列的下拉框选择：

- 不要求
- 建议
- 强制

图 6-36 修改保护要求

数据保护类型	审核与监督	加密保证	物理销毁	软件销毁	测试
一般数据保护	不要求	不要求	不要求	不要求	不要求
<input checked="" type="checkbox"/> 分级数据保护					
L1	强制	强制	不要求	建议	不要求
L3	强制	强制	强制	强制	不要求
L4	强制	强制	强制	强制	不要求
一般_L1级	不要求	不要求	不要求	不要求	不要求

步骤5 修改完成，单击左上角“保存修改”。如果需要取消修改，单击左上角的“取消修改”返回上次保护要求。

----结束


6.2 策略管理

管理员在策略中心的策略管理页面制定数据库审计、数据库加密、数据库水印、数据库静态脱敏、数据库动态脱敏策略，下发给相应的服务或者实例。

创建策略

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“安全与合规 > 数据安全中心”。
- 步骤4** 选择“策略中心 > 策略管理”，进入策略管理界面。
- 步骤5** 左上角单击“创建策略”，进入“创建策略”界面。
- 步骤6** 选择策略类型并配置策略信息：
- “数据库审计”：监控和记录数据库活动，以确保数据的完整性、安全性和合规性。
参照[配置数据库审计策略](#)进行参数配置。
 - “数据库加密”：对数据进行加密处理，以确保数据的机密性和完整性，防止未经授权的访问和数据泄露。
参照[配置数据库加密策略](#)进行参数配置。
 - “数据库水印”：对数据嵌入难以察觉的标识符，验证数据的真实性、所有权和追踪泄露源头。
参照[数据库水印注入](#)和[数据库水印提取](#)章节的内容进行水印注入和提取。
 - “数据库静态脱敏”：对敏感数据进行脱敏处理，以确保隐私和安全，同时保留数据结构和统计特性。
参照[数据库静态脱敏](#)章节的内容进行水印注入和提取。
 - “数据库动态脱敏”：对敏感数据进行实时脱敏处理，以确保未经授权的数据不可访问。
参照[配置数据库动态脱敏策略](#)进行参数配置。

----结束

配置数据库审计策略

已开启DBSS且已添加实例。

- 步骤1** 单击“开始配置”，进入数据库审计策略类型配置界面。
- 步骤2** 参照[表6-1](#)进行参数配置：

表 6-1 数据库审计策略类型参数配置表

参数	说明
策略名称	输入策略名称，只能由中文字符、英文字母、数字、下划线和中划线组成，长度不超过255个字符。
关联实例	单击下拉框选择数据库审计实例。
目标数据源	单击下拉框选择目标数据源，仅支持免Agent审计的数据库实例。

参数	说明
是否显示结果集	开启记录结果集后，系统将对SQL结果内容进行记录，可在日志中进行查看。如果未开启，日志详情中SQL结果内容为空。 记录结果集存在信息泄露风险，不建议开启。
隐私数据脱敏	通过编写脱敏规则，防止敏感数据泄露，建议开启。

步骤3 单击“保存并下发”，进入策略列表查看新创建的策略。

----结束

配置数据库加密策略

已在DBSS购买数据加密与访问控制。

步骤1 单击“开始配置”，进入数据加密策略类型配置界面。

步骤2 参照表6-2进行参数配置：

表 6-2 数据加密策略类型参数配置表

参数	说明
策略名称	输入策略名称，只能由中文字符、英文字母、数字、下划线和中划线组成。
加密	仅支持加密。
关联实例	数据库加密网关。
目标数据源	单击下拉框选择目标数据源。
代理端口	端口范围14000-14999，不同数据库实例（地址和端口相同）使用不同代理端口，同一数据库实例使用相同代理端口，添加同一数据库实例下的数据源，会自动填充代理端口。
加密算法	单击下拉框选择加密算法，加密算法有AES128和SM4。
被加密表	单击下拉框选择被加密表。 同一目标表不能重复选。
被加密表信息	被加密表的信息，包含“字段名称”、“字段类型”、“数据分级”。

步骤3 单击“保存并下发”，进入策略列表查看新创建的策略。

----结束

配置数据库动态脱敏策略

步骤1 单击“开始配置”，进入数据库动态脱敏策略配置界面。

步骤2 参照表6-3进行参数配置：

表 6-3 数据库动态脱敏策略类型参数配置表

参数	说明
策略名称	输入策略名称，只能由中文字符、英文字母、数字、下划线和中划线组成。
关联实例	数据库加密网关。
目标数据源	单击下拉框选择目标数据源。
脱敏服务端口	端口范围14000-14999，不同数据库实例（地址和端口相同）使用不同代理端口，同一数据库实例使用相同代理端口，添加同一数据库实例下的数据源，会自动填充代理端口。
表	单击下拉框选择表。
表信息	选择“表”后显示该参数。 表的信息，包含“字段名称”、“字段类型”、“数据分级”、“脱敏算法”。

步骤3 单击“保存并下发”，进入策略列表查看新创建的策略。

----结束

相关操作

- 禁用策略：启用（下发成功）的策略可以在“操作”列单击“禁用”，禁用此条策略，单击“禁用”后此条策略的“状态”显示为“禁用（下发中）”，当策略的“状态”变为“禁用（下发成功）”此条策略被禁用。

📖 说明

- 加密策略启用下发成功后不允许禁用和删除，对应加密策略在“操作 > 更多”下单击“解密”进行解密，该加密策略名称添加解密后缀，不会重新创建解密策略。
- 删除策略：下发成功的策略可以在“操作”列单击“删除”，删除此条策略，单击“删除”后界面右上角提示该条策略删除成功。

6.3 流转日志采集

全链路的云上数据流转监测，包括以下几个阶段：通过数据库审计日志分析数据库和源端、目的主机之间流转路径；通过API审计日志分析数据通过API网关对外流转的路径；通过API网关配置分析梳理主机和网关之间的流转路径；最后通过全链路的关联分析实时测绘完整的云上数据流转路径。

DSC对各个应用中的日志数据进行采集，如DBSS服务和API数据安全防护，可动态的采集用户访问行为的路径，可以快速全面支撑溯源或定位，直观了解数据的流转情况，及时发现异常和风险。


前提条件

- 已开通DBSS服务，并安装数据库实例。
- 已创建API数据安全防护实例。

开通流转采集

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“安全与合规 > 数据安全中心”。

步骤4 在左侧导航树中，选择“策略中心 > 流转日志采集”，进入“数据流转”界面。

步骤5 实例列表参数说明如[表6-4](#)所示。

表 6-4 实例列表

参数	说明
实例名称/ID	对接微服务的实例名称，如DBSS和API数据安全防护的实例，如果没有实例请先进行实例购买。
实例类型	实例的类型，“DBSS”和“ADG”。
实例状态	实例的状态： <ul style="list-style-type: none"> • 未开通：没有开通流转日志采集。 • 开通中：流转日志采集开通中。 • 开通失败：开通流转日志采集失败。 • 运行中：开通流转日志采集成功。 • 离线：实例状态异常未接收到心跳信息。 • 关闭失败：流转日志采集关闭失败。 • 关闭中：流转日志采集关闭中。 • 异常：实例上报状态异常。
上次心跳时间	DSC上次与实例建立连接的时间。
数据流转日志采集状态	单击  打开流转日志采集开关，进行日志采集。

步骤6 单击 打开流转日志采集开关，开通日志采集。“实例状态”为“开通中”正在开通采集，“实例状态”为“运行中”证明开启采集成功。


单击左上角“批量开通流转采集”批量开通日志流转采集。

----结束

关闭流转采集

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“安全与合规 > 数据安全中心”。

步骤4 在左侧导航树中, 选择“策略中心 > 流转日志采集”, 进入“数据流转”界面。

步骤5 实例列表参数说明如表6-5所示。

表 6-5 实例列表

参数	说明
实例名称/ID	对接微服务的实例名称, 如DBSS和API数据安全防护的实例, 如果没有实例请先进行实例购买。
实例类型	实例的类型, “DBSS”和“ADG”。
实例状态	实例的状态: <ul style="list-style-type: none"> ● 未开通: 没有开通流转日志采集。 ● 开通中: 流转日志采集开通中。 ● 开通失败: 开通流转日志采集失败。 ● 运行中: 开通流转日志采集成功。 ● 离线: 实例状态异常未接收到心跳信息。 ● 关闭失败: 流转日志采集关闭失败。 ● 关闭中: 流转日志采集关闭中。 ● 异常: 实例上报状态异常。
上次心跳时间	DSC上次与实例建立连接的时间。
数据流转日志采集状态	单击  打开流转日志采集开关, 进行日志采集。

步骤6 单击 关闭流转日志采集开关, 关闭日志采集。

单击左上角“批量关闭流转采集”批量关闭日志流转采集。

----结束

7 数据资产保护

7.1 数据脱敏

7.1.1 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，同时，您也可以使用[数据动态脱敏](#)的API接口实现数据的动态脱敏，全方位确保敏感信息不被泄露，数据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、营销等场景，具体请参考[数据动态脱敏](#)。

数据脱敏操作流程

图 7-1 静态脱敏操作流程

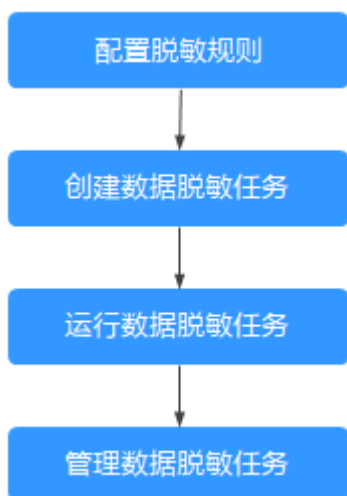
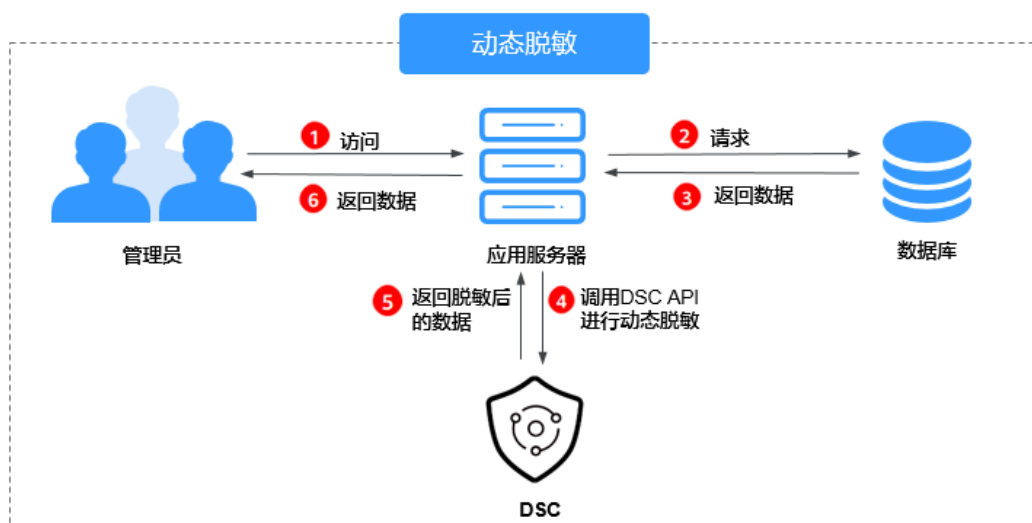


图 7-2 动态脱敏操作流程



脱敏算法

表 7-1 脱敏算法说明

脱敏算法	脱敏方式说明	使用场景
Hash脱敏	<p>使用Hash函数对敏感数据进行脱敏。支持SHA256和SHA512。</p> <ul style="list-style-type: none"> 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。 	<ul style="list-style-type: none"> 敏感类型：密钥类 适用场景：数据存储
加密脱敏	<p>通过加密算法和加密主密钥生成指定的数据密钥，使用数据密钥对敏感数据进行加密达到数据脱敏的效果。 DSC支持AES256和SM4两种加密算法。</p>	<ul style="list-style-type: none"> 敏感类型： <ul style="list-style-type: none"> 个人敏感 企业敏感 适用场景：数据存储
字符掩盖	<p>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：</p> <ul style="list-style-type: none"> 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 <p>说明 敏感数据保护服务中已预置多种字符脱敏模板。</p>	<ul style="list-style-type: none"> 敏感类型：个人敏感 适用场景： <ul style="list-style-type: none"> 数据使用 数据分享

脱敏算法	脱敏方式说明	使用场景
关键字替换	<p>在指定列中查找关键词并替换。</p> <p>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”。</p> <p>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。</p>	<ul style="list-style-type: none"> ● 敏感类型： <ul style="list-style-type: none"> - 个人敏感 - 企业敏感 - 设备敏感 ● 适用场景： <ul style="list-style-type: none"> - 数据存储 - 数据分享
删除脱敏	<p>将指定字段设置为Null或空值进行脱敏。</p> <ul style="list-style-type: none"> ● Null脱敏 <p>将任意类型字段设置为NULL。</p> <p>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”。</p> ● 空值脱敏 <p>将指定字段内容设置为空值。</p> <p>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。</p> 	<ul style="list-style-type: none"> ● 敏感类型： <ul style="list-style-type: none"> - 个人敏感 - 企业敏感 - 设备敏感 ● 适用场景： <ul style="list-style-type: none"> - 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	<p>针对日期或数字特定参数进行取整运算。</p> <ul style="list-style-type: none"> 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。 	<ul style="list-style-type: none"> 敏感类型：通用敏感 适用场景： <ul style="list-style-type: none"> 数据存储 数据使用


7.1.2 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[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“安全与合规 > 数据安全中心”。

步骤4 在左侧导航树中选择“数据资产保护 > 数据静态脱敏”，并选择“脱敏规则”页签，进入脱敏规则页面。

图 7-3 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](#)。
- “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。

图 7-4 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 7-5 Hash 脱敏测试



----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。

- “主密钥算法”：在下拉框选择加密算法，DSC提供了“AES256”和“SM4”加密算法供您选择。
- “KMS加密”可以选择“从KMS密钥中选择”和“输入KMS密钥ID”两种方式：
 - “从KMS密钥中选择”：单击下拉框选择已有的KMS主密钥，如果没有可选择的主密钥，单击“创建KMS主密钥”进行创建，创建方式详情请参见https://support.huaweicloud.com/intl/zh-cn/usermanual-dew/dew_01_0178.html。

说明


默认使用凭据管理为您创建的默认主密钥csm/default作为当前凭证的加密主密钥，您可以前往KMS服务页面创建用户密钥，使用自定义加密密钥。

- “输入KMS密钥ID”：输入位于当前Region的密钥。
- 单击下拉框选择“数据密钥长度”，有128、192和256三种供选择。

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”。

说明

单击  打开轮换策略，轮换周期到期后会更新当前加密配置提升安全性。

----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 7-6 字符掩盖页面

Hash脱敏 加密脱敏 字符掩盖 关键字替换 删除脱敏 取整脱敏				
添加				
名称	规则	掩码字符	效果	操作
组织机构代码	保留前4后2，掩盖文字为*	*	4205****6	编辑/测试

步骤3 单击“添加”，配置字符脱敏规则。

图 7-7 添加字符脱敏

添加字符脱敏

名称

选择规则 保留前n后m

遮盖位置 n m

遮盖方式 固定字符

遮盖字符

测试

原始数据 请输入原始数据 测试

脱敏结果

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

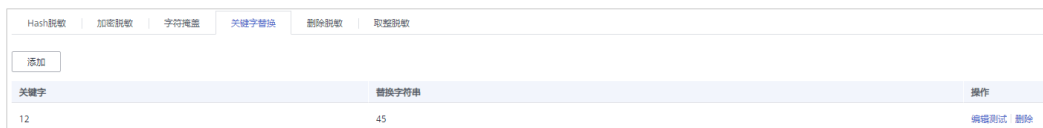
关键字替换

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`abcdefghijklkioij`，“关键字”配置为`bcde`，“替换字符串”配置为`12`，则“脱敏结果”显示为`a12fg12fgkioij`。

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 7-8 关键字替换



关键字	替换字符串	操作
12	45	编辑测试 删除

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 7-9 添加关键字



添加关键字

关键字

替换字符串

测试

原始数据

脱敏结果

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。

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 7-10 删除脱敏

Hash脱敏	加密脱敏	字符掩盖	关键字替换	删除脱敏	取整脱敏
Null脱敏		脱敏字段置为Null			
空值脱敏		将指定字段设置为默认值。具体如下：			
【“数值”类型】		"1024"->"0", "0.123"->"0.0", "0xef"->"0x00"			
【“字符”类型】		"text"->"			
【数据库中“日期时间”类型】		【“字符”类型】			
【数据库中“时间戳”类型】		"1575604312"->"0"			

----结束

取整脱敏

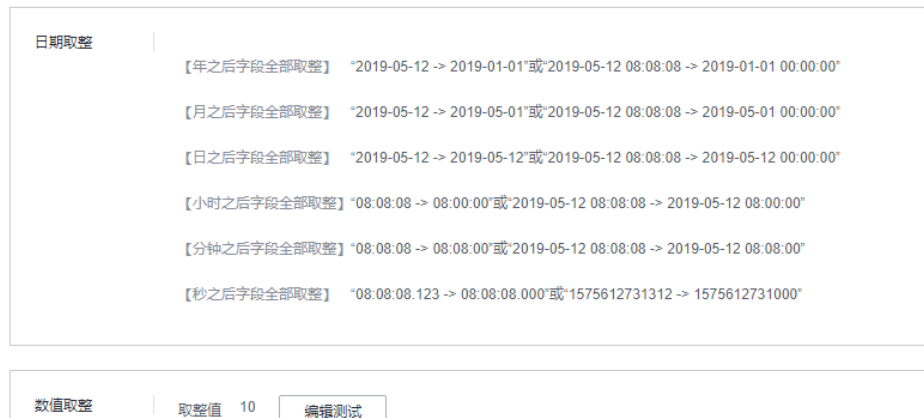
步骤1 参照[操作步骤](#)进入“脱敏规则”页面。

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“数值取整”两种算法。

- “日期取整”算法对应关系型数据库中timestamp, time, data, datetime等与时间相关的字段。
- “数值取整”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 7-11 数值脱敏页面



步骤3 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 7-12 数值取整



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

仿真脱敏

在敏感数据识别到匹配敏感内容后，会使用仿真的数据替换匹配敏感内容，目前仅适用于OBS脱敏任务。

表 7-2 支持的仿真脱敏类型

编号	敏感数据规则名称	仿真脱敏的类型
1	身份证号（中国内地）	身份证号
2	生日	随机日期（指定范围）
3	日期	随机日期（指定范围）
4	手机号码（中国内地）	手机号码
5	邮箱	邮箱
6	邮政编码（中国内地）	邮政编码
7	地址（中国内地）	地址
8	精确地址（中国）	地址
9	唯一设备识别码IMEI	IMEI
10	IPv4地址	ipv4
11	IPv6地址	ipv6
12	银行卡号	银行卡号
13	姓名（简体中文）	人名
14	车牌号（中国内地）	车牌号
15	护照号（中国内地）	护照号

7.1.3 数据静态脱敏

7.1.3.1 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

- 已完成云资产委托授权，具体请参见[云资产委托授权/停止授权](#)进行操作。
- 已添加或者授权资产，具体请参见[资产中心](#)中添加和授权资产的操作。
- 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[新建敏感数据识别任务](#)。


约束条件

支持的数据源有“SQLServer”、“MySQL”、“TDSQL”、“PostgreSQL”、“达梦”、“人大金仓”、“GaussDB”、“Oracle”、“DWS”。



创建并运行数据库脱敏任务

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“安全与合规 > 数据安全中心”。

步骤4 在左侧导航树中选择“数据资产保护 > 数据静态脱敏”，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7-3](#)所示。

图 7-13 数据源配置-数据库脱敏任务



表 7-3 数据源配置参数说明

参数名称	参数说明
任务名称	<p>您可以自定义脱敏任务的名称。</p> <p>任务名称需要满足以下要求：</p> <ul style="list-style-type: none"> • 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。

参数名称	参数说明
数据源选择	选择数据来源。可选择“SQLServer”、“MySQL”、“TDSQL”、“PostgreSQL”、“达梦”、“人大金仓”、“OpenGauss”、“Oracle”、“DWS”。
数据源	数据库实例：选择脱敏数据所在的数据库实例。
说明 如果没有可使用的数据库实例，单击“授权数据库”，授权数据库，具体的操作可参见 授权数据库资产 。	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”、“人大金仓”、“OpenGauss”、“PostgreSQL”和“DWS”时，显示该参数。
	数据表名：选择脱敏数据所在的数据表名称。
脱敏比例	输入数据库的脱敏比例，如数据库存在1000行的数据，此处输入80%时，则对数据库前800行的数据进行脱敏。

步骤7 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[配置脱敏规则](#)。

说明

加密数据选择解密脱敏算法，会对加密的数据进行解密脱敏。

未加密数据选择解密脱敏算法，脱敏后还是原数据不变。

3. 单击“编辑”进入编辑测试界面，测试您选择的脱敏算法结果，测试“关键字替换”脱敏算法，输入“替换字符串”、“原始数据”，单击测试查看“脱敏结果”，具体的脱敏规则请参见[配置脱敏规则](#)。

步骤8 单击“下一步”，进入“脱敏周期配置”页面，配置脱敏周期。

单击“增量脱敏”右边 ，打开增量脱敏开关。

增量键值：单击下拉框选择增量键值，如id。

说明

- 开启“增量脱敏”后，每次脱敏的数据为上次脱敏任务完成后新增的数据，请选择一个源数据中随着时间递增的字段作为增量列，例如创建时间，自增id等。
- 目前增量脱敏支持的数据库字段类型有：int、bigint、integer、date、datetime。

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9 单击“下一步”，进入“数据目标配置”页面。

图 7-14 数据目标配置-数据库脱敏任务

数据库实例	数据库名	模式	数据表名
dyf-ecs-db	test	scan	请输入表名

数据源列名	风险等级	数据目标列名
email	--	email
nul	--	nul
name	--	name

操作按钮：[上一步] [完成] [取消]

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。
- 目标数据表请勿选择原数据表，以免覆盖原始数据。

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。

步骤11 进入“数据库”页签，在目标脱敏任务的“操作”列，单击“立即运行”，如图7-15所示。


图 7-15 立即运行数据库脱敏任务

启用/禁用任务	任务名称	数据源/数据目标	脱敏周期	操作
<input checked="" type="checkbox"/>	sdg_test	sdg_test → sdg_test	手动执行	立即运行 编辑 删除
<input checked="" type="checkbox"/>	sdg_test	sdg_test → sdg_test	手动执行	立即运行 编辑 删除

步骤12 运行后，系统开始按照设置的脱敏周期执行脱敏任务。

----结束

查看数据库脱敏任务的运行状态

- 进入“数据库”页签，单击目标脱敏任务前面的 ，查看脱敏任务运行状态，如图7-16所示。

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。鼠标移动至  查看失败原因。

图 7-16 数据库脱敏任务运行情况

启用/禁用任务	任务名称	数据源/数据目标	脱敏周期	操作										
	test-mysql-1000W	test-tuomin → test-tuomin	手动执行	立即运行 编辑 删除										
<table border="1"> <thead> <tr> <th>开始时间</th> <th>结束时间</th> <th>执行方式</th> <th>执行行数</th> <th>状态</th> </tr> </thead> <tbody> <tr> <td>2023/07/05 18:51:11 GMT+08:00</td> <td>2023/07/05 19:23:18 GMT+08:00</td> <td>手动执行</td> <td>10000000</td> <td>已完成</td> </tr> </tbody> </table>					开始时间	结束时间	执行方式	执行行数	状态	2023/07/05 18:51:11 GMT+08:00	2023/07/05 19:23:18 GMT+08:00	手动执行	10000000	已完成
开始时间	结束时间	执行方式	执行行数	状态										
2023/07/05 18:51:11 GMT+08:00	2023/07/05 19:23:18 GMT+08:00	手动执行	10000000	已完成										

编辑和删除数据库脱敏任务

等待运行或运行中的脱敏任务不支持编辑或删除。

- 在数据库脱敏任务列表中，在目标脱敏任务的“操作”列，单击“编辑”，可重新配置脱敏任务信息，配置脱敏任务信息方法请参见[创建并运行数据库脱敏任务](#)。

图 7-17 编辑数据库脱敏任务

启用/禁用任务	任务名称	数据源/数据目标	脱敏周期	操作
	sdg_test	sdg_test → sdg_test	手动执行	立即运行 编辑 删除
	sdg_test	sdg_test → sdg_test	手动执行	立即运行 编辑 删除

- 在数据库脱敏任务列表中，在目标脱敏任务的“操作”列，单击“删除”，如图7-18所示。

图 7-18 删除数据库脱敏任务

启用/禁用任务	任务名称	数据源/数据目标	脱敏周期	操作
	sdg_test	sdg_test → sdg_test	手动执行	立即运行 编辑 删除
	sdg_test	sdg_test → sdg_test	手动执行	立即运行 编辑 删除

注意

脱敏任务删除后不支持恢复，建议您谨慎操作。

7.1.3.2 创建 Elasticsearch 脱敏任务

创建Elasticsearch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Elasticsearch脱敏任务。

前提条件

- 已完成云资产委托授权，具体请参见[云资产委托授权/停止授权](#)。
- 已授权Elasticsearch索引，具体请参见[授权大数据资产](#)。
- 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[新建敏感数据识别任务](#)。


约束条件

数据源目前仅支持“Elasticsearch”。



创建并运行 Elasticsearch 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“安全与合规 > 数据安全中心”。

步骤4 在左侧导航树中选择“数据资产保护 > 数据静态脱敏”，并选择Elasticsearch页签，进入Elasticsearch脱敏页面。

步骤5 单击，将“Elasticsearch”设置为，开启Elasticsearch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7-4](#)所示。

表 7-4 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： <ul style="list-style-type: none"> • 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Elasticsearch实例，可单击“授权ES源”，授权Elasticsearch索引，具体的操作可参见 授权大数据资产 。	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。

步骤7 单击“下一步”，进入“脱敏算法配置”页面，如[图7-19](#)所示。

图 7-19 脱敏算法配置-Elasticsearch 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“脱敏周期配置”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9 单击“下一步”，进入“数据目标配置”页面，如[图7-20](#)所示。

图 7-20 数据目标配置-Elasticsearch 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”，完成脱敏任务的创建。


步骤11 进入“Elasticsearch”页签，在目标脱敏任务的“操作”列，单击“立即运行”，如图7-21所示。

图 7-21 立即运行 Elasticsearch 脱敏任务

启用/禁用任务	任务名称	数据源/数据目标	脱敏周期	操作
<input checked="" type="checkbox"/>	es_mask	scan_index → mask_index	手动执行	立即运行 编辑 删除


步骤12 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 ，则该任务处于禁用状态，则无法单击“立即运行”，启动任务。

----结束

查看 Elasticsearch 脱敏任务运行状态

- 进入“Elasticsearch”页签，单击目标脱敏任务前面的 ，查看脱敏任务运行状态，如图7-22所示。

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 7-22 Elasticsearch 脱敏任务运行情况

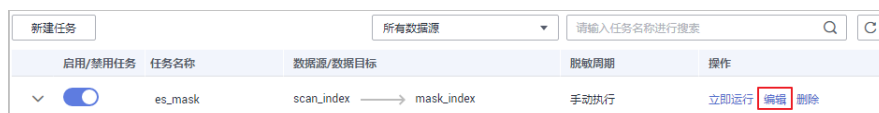
启用/禁用任务	任务名称	数据源/数据目标	脱敏周期	操作																				
<input checked="" type="checkbox"/>	es_mask	scan_index → mask_index	手动执行	立即运行 编辑 删除																				
<table border="1"> <thead> <tr> <th>开始时间</th> <th>结束时间</th> <th>执行方式</th> <th>状态</th> </tr> </thead> <tbody> <tr> <td>2020/04/03 11:35:17 GMT+08:00</td> <td>2020/04/03 11:35:18 GMT+08:00</td> <td>手动执行</td> <td>✅ 已完成</td> </tr> <tr> <td>2020/04/03 11:19:16 GMT+08:00</td> <td>2020/04/03 11:19:16 GMT+08:00</td> <td>手动执行</td> <td>❌ 运行失败</td> </tr> <tr> <td>2020/04/03 11:18:57 GMT+08:00</td> <td>2020/04/03 11:18:58 GMT+08:00</td> <td>手动执行</td> <td>❌ 运行失败</td> </tr> <tr> <td>2020/04/03 11:08:06 GMT+08:00</td> <td>--</td> <td>手动执行</td> <td>⏸ 已终止</td> </tr> </tbody> </table>					开始时间	结束时间	执行方式	状态	2020/04/03 11:35:17 GMT+08:00	2020/04/03 11:35:18 GMT+08:00	手动执行	✅ 已完成	2020/04/03 11:19:16 GMT+08:00	2020/04/03 11:19:16 GMT+08:00	手动执行	❌ 运行失败	2020/04/03 11:18:57 GMT+08:00	2020/04/03 11:18:58 GMT+08:00	手动执行	❌ 运行失败	2020/04/03 11:08:06 GMT+08:00	--	手动执行	⏸ 已终止
开始时间	结束时间	执行方式	状态																					
2020/04/03 11:35:17 GMT+08:00	2020/04/03 11:35:18 GMT+08:00	手动执行	✅ 已完成																					
2020/04/03 11:19:16 GMT+08:00	2020/04/03 11:19:16 GMT+08:00	手动执行	❌ 运行失败																					
2020/04/03 11:18:57 GMT+08:00	2020/04/03 11:18:58 GMT+08:00	手动执行	❌ 运行失败																					
2020/04/03 11:08:06 GMT+08:00	--	手动执行	⏸ 已终止																					

编辑和删除 Elasticsearch 脱敏任务

等待运行或运行中的脱敏任务不支持编辑或删除。

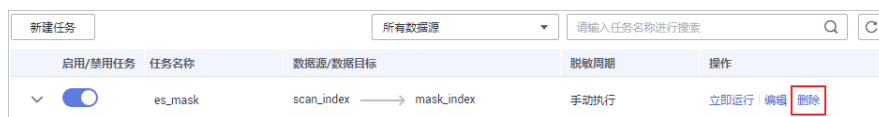
- 在Elasticsearch脱敏任务列表中，在目标脱敏任务的“操作”列，单击“编辑”，可修改脱敏任务配置信息，配置脱敏任务信息请参见[创建并运行Elasticsearch脱敏任务](#)。

图 7-23 编辑 Elasticsearch 脱敏任务



- 在Elasticsearch脱敏任务列表中，在目标脱敏任务的“操作”列，单击“删除”，如[图7-24](#)所示。

图 7-24 删除 Elasticsearch 脱敏任务



注意

脱敏任务删除后不支持恢复，建议您谨慎操作。

7.1.3.3 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

- 已完成云资源委托授权，具体请参见[云资产委托授权/停止授权](#)。
- 已授权Hive数据库，具体请参见[授权大数据资产](#)。
- 已进行MRS_Hive的相关权限配置，[修改Hive用户权限](#)。
- 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[新建敏感数据识别任务](#)。

约束条件

数据源目前仅支持“MRS_HIVE”。

创建并运行 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“安全与合规 > 数据安全中心”。
- 步骤4** 在左侧导航树中选择“数据资产保护 > 数据静态脱敏”，并选择“MRS”页签，进入MRS脱敏页面。
- 步骤5** 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7-5所示。

表 7-5 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： <ul style="list-style-type: none"> 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Hive数据库实例，可单击“授权数据库”，授权数据库资产，具体的操作可参见 授权大数据资产 。	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。
	勾选列名后将该列数据拷贝到目标数据库。

- 步骤7** 单击“下一步”，进入“脱敏算法配置”页面，如图7-25所示。

图 7-25 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“脱敏周期配置”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9 单击“下一步”，进入“数据目标配置”页面，如图7-26所示。

图 7-26 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”，完成脱敏任务的创建。

步骤11 进入“MRS”页签，在目标脱敏任务的“操作”列，单击“立即运行”。

步骤12 运行后，系统开始按照设置的脱敏周期执行脱敏任务。

----结束



查看 MRS 脱敏任务的运行状态

- 进入“MRS”页签，单击目标脱敏任务前面的 ，查看脱敏任务运行状态，如图 7-27 所示。

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 7-27 MRS 脱敏任务运行情况

启用/禁用任务	任务名称	数据源/数据目标	脱敏周期	操作
	test-mrs	lhy → lhy	手动执行	立即运行 编辑 删除
开始时间	结束时间	执行方式	状态	
2023/07/04 11:30:22 GMT+08:00	2023/07/04 11:36:10 GMT+08:00	手动执行	 已完成	
2023/06/28 12:37:39 GMT+08:00	2023/06/28 12:41:22 GMT+08:00	手动执行	 已完成	
2023/06/28 11:42:40 GMT+08:00	--	手动执行	 已停止	
2023/06/28 11:14:34 GMT+08:00	--	手动执行	 已停止	

编辑和删除 MRS 脱敏任务

等待运行或运行中的脱敏任务不支持编辑或删除。

- 在 MRS 脱敏任务列表中，在目标脱敏任务的“操作”列，单击“编辑”，可修改脱敏任务配置信息，配置脱敏任务信息请参见[创建并运行 MRS 脱敏任务](#)。
- 在 MRS 脱敏任务列表中，在目标脱敏任务的“操作”列，单击“删除”。



脱敏任务删除后不支持恢复，建议您谨慎操作。

7.1.3.4 创建 Hive 脱敏任务

创建 Hive 脱敏任务后，可以对 Hive 类型数据的敏感信息进行脱敏。

本章节将介绍如何创建 Hive 脱敏任务。

前提条件

- 已完成云资源委托授权，具体请参见[云资产委托授权/停止授权](#)。
- 已授权 Hive 数据库，具体请参见[授权大数据资产](#)。
- 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[新建敏感数据识别任务](#)。


约束条件

数据源目前仅支持“HIVE”。



创建并运行 Hive 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“安全与合规 > 数据安全中心”。

步骤4 在左侧导航树中选择“数据资产保护 > 数据静态脱敏”，并选择“Hive”页签，进入Hive脱敏页面。

步骤5 单击，将“Hive脱敏”设置为，开启Hive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7-6所示。

表 7-6 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： <ul style="list-style-type: none"> 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“HIVE”。
数据源 说明 如果没有可使用的Hive数据库实例，可单击“授权数据库”，授权数据库，具体的操作可参见 授权大数据资产 。	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。 勾选列后将该列数据拷贝到目标数据库。

步骤7 单击“下一步”，进入“脱敏算法配置”页面，如图7-28所示。

图 7-28 脱敏算法配置-Hive 脱敏任务



该截图展示了“脱敏算法配置”页面的配置项。顶部有四个步骤指示器：1. 数据源配置 (已完成), 2. 脱敏算法配置 (当前步骤), 3. 脱敏周期配置, 4. 数据目标配置。下方显示了数据源信息：Hive_mdtestzyj_192.168.0.120/mdtestzyj/md_table1。配置表如下：

数据列名	数据类型	脱敏算法
<input checked="" type="checkbox"/> gender	string	Hash脱敏 SHA256 编辑
<input checked="" type="checkbox"/> role	string	Hash脱敏 SHA256 编辑

底部有“上一步”、“下一步”和“取消”按钮。

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“脱敏周期配置”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9 单击“下一步”，进入“数据目标配置”页面，如图7-29所示。

图 7-29 数据目标配置-Hive 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”，完成脱敏任务的创建。

步骤11 进入“Hive”页签，在目标脱敏任务的“操作”列，单击“立即运行”。

步骤12 运行后，系统开始按照设置的脱敏周期执行脱敏任务。

----结束

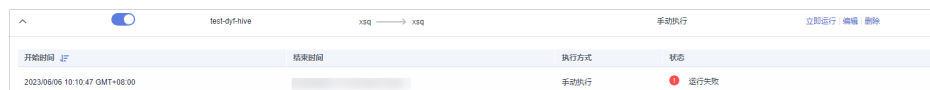
查看 Hive 脱敏任务运行状态

- 进入“Hive”页签，单击目标脱敏任务前面的 ，查看脱敏任务运行状态，如图 6 Elasticsearch脱敏任务运行情况所示。

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 7-30 Hive 脱敏任务运行状态



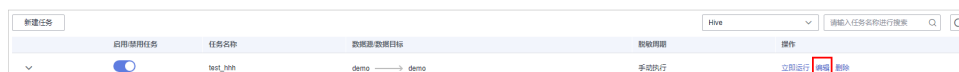
开始时间	结束时间	执行方式	状态
2023/06/06 10:10:47 GMT+08:00		手动执行	运行失败

编辑和删除 Hive 脱敏任务

等待运行或运行中的脱敏任务不支持编辑或删除。

- 在Hive脱敏任务列表中，在目标脱敏任务的“操作”列，单击“编辑”，可修改脱敏任务配置信息，配置脱敏任务信息请参见[创建并运行Hive脱敏任务](#)。

图 7-31 编辑 Hive 脱敏任务



任务名称	数据源/数据目标	脱敏周期	操作
test_100h	demo -> demo	手动执行	立即运行 编辑 删除

- 在Hive脱敏任务列表中，在目标脱敏任务的“操作”列，单击“删除”。

图 7-32 删除 Hive 脱敏任务



任务名称	数据源/数据目标	脱敏周期	操作
test_100h	demo -> demo	手动执行	立即运行 删除 编辑

注意

脱敏任务删除后不支持恢复，建议您谨慎操作。

7.1.3.5 创建 HBase 脱敏任务

创建HBase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HBase脱敏任务。

前提条件

- 已完成云资源委托授权，具体请参见[云资产委托授权/停止授权](#)。
- 已授权HBase命名空间，具体请参见[授权大数据资产](#)。
- 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[新建敏感数据识别任务](#)。


约束条件

数据源目前仅支持“HBase”。



创建并运行 HBase 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“安全与合规 > 数据安全中心”。

步骤4 在左侧导航树中选择“数据资产保护 > 数据静态脱敏”，并选择“HBase”页签，进入HBase脱敏页面。

步骤5 单击，将“HBase脱敏”设置为，开启HBase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7-7](#)所示。

表 7-7 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： <ul style="list-style-type: none"> • 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“HBase”。
数据源 说明 如果没有可使用的数据库实例，可单击“授权数据库”，授权数据库资产，具体的操作可参见 授权大数据资产 。	数据库实例：选择脱敏数据所在的数据库实例。
	命名空间：选择脱敏数据所在的命名空间。
	数据表名：选择脱敏数据所在的数据表名称。
	列族：选择脱敏数据所在的列。
	勾选列后将该列数据拷贝到目标数据库。

步骤7 单击“下一步”，进入“脱敏算法配置”页面，如[图7-33](#)所示。

图 7-33 脱敏算法配置-HBase 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“脱敏周期配置”页面，配置脱敏周期。

选择并设置脱敏任务的执行周期：

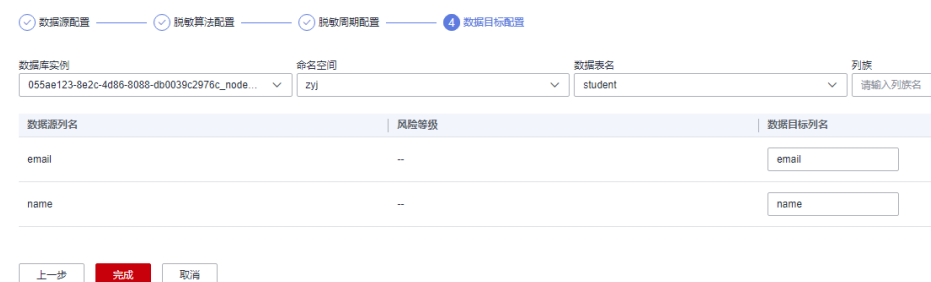
- 手动：由用户自行启动的，且基于脱敏规则执行脱敏任务。
- 每小时：每几个小时执行一次脱敏任务。
示例：如果需要每2小时执行一次脱敏任务，则此处设置为：02:00
- 每天：每天几点几分执行一次脱敏任务。
示例：如果需要每天12:00执行一次脱敏任务，则此处设置为：12:00:00
- 每周：每周几的几点执行一次脱敏任务。
示例：如果需要每周一的12:00执行一次脱敏任务，则此处设置为：每周一 12:00:00
- 每月：每月几日几时执行一次脱敏任务。
示例：如果需要每月12日的12:00执行一次脱敏任务，则此处设置为：每月12日 12:00:00

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9 单击“下一步”，进入“数据目标配置”页面，如[图7-34](#)所示。

图 7-34 数据目标配置-HBase 脱敏任务



1. 选择数据库实例、命名空间、数据表名，并输入列族。

如果输入的列名已存在，系统将刷新目标数据表中的该列的数据。
如果输入的列名不存在，系统将自动在目标数据表中新建该名称的列。

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HBase任务的创建。

步骤11 进入“HBase”页签，在目标脱敏任务的“操作”列，单击“立即运行”。

步骤12 运行后，系统开始按照设置的脱敏周期执行脱敏任务。

----结束

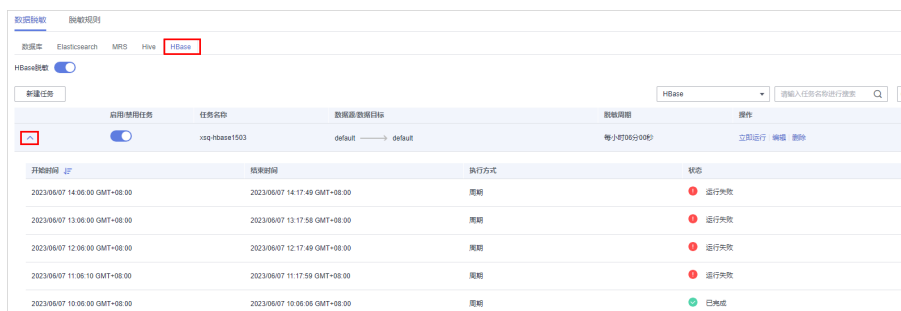
查看 HBase 脱敏任务运行状态

- 进入“HBase”页签，单击目标脱敏任务前面的 ，查看脱敏任务运行状态，如图7-35所示。

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 7-35 HBase 脱敏任务运行状态



任务名称	数据源	数据目标	脱敏周期	操作
task-hbase1503	default	default	每小时3650秒	立即运行 编辑 删除
开始时间	结束时间	执行方式	状态	
2023/06/07 14:06:00 GMT+08:00	2023/06/07 14:17:49 GMT+08:00	周期	运行失败	
2023/06/07 13:06:00 GMT+08:00	2023/06/07 13:17:58 GMT+08:00	周期	运行失败	
2023/06/07 12:06:00 GMT+08:00	2023/06/07 12:17:49 GMT+08:00	周期	运行失败	
2023/06/07 11:06:10 GMT+08:00	2023/06/07 11:17:59 GMT+08:00	周期	运行失败	
2023/06/07 10:06:00 GMT+08:00	2023/06/07 10:06:06 GMT+08:00	周期	已完成	

编辑和删除 HBase 脱敏任务

等待运行或运行中的脱敏任务不支持编辑或删除。

- 在HBase脱敏任务列表中，在目标脱敏任务的“操作”列，单击“编辑”，可修改脱敏任务配置信息，配置脱敏任务信息请参见[创建并运行HBase脱敏任务](#)。
- 在HBase脱敏任务列表中，在目标脱敏任务的“操作”列，单击“删除”。

注意

脱敏任务删除后不支持恢复，建议您谨慎操作。

7.1.3.6 创建 DLI 脱敏任务

创建DLI脱敏任务后，可以对DLI类型数据的敏感信息进行脱敏。

本章节将介绍如何创建DLI脱敏任务。

前提条件

- 已完成云资源委托授权，具体请参见[云资产委托授权/停止授权](#)。
- 已添加DLI数据库，具体请参见[授权大数据资产](#)。
- 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[新建敏感数据识别任务](#)。

约束条件

数据源目前仅支持“DLI”。

创建并运行 DLI 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“安全与合规 > 数据安全中心”。
- 步骤4** 在左侧导航树中选择“数据资产保护 > 数据静态脱敏”，并选择“DLI”页签，进入DLI脱敏页面。
- 步骤5** 单击，将“DLI脱敏”设置为，开启DLI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7-8](#)所示。

表 7-8 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： <ul style="list-style-type: none"> • 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“DLI”。

参数名称	参数说明
数据源 如果没有可使用的数据库实例，可单击“添加云数据库”，添加数据库资产，具体的操作可参见 授权大数据资产 。	数据库实例：选择脱敏数据所在的数据库实例。
	数据库名：选择需要脱敏的数据库。
	数据表名：选择需要脱敏的数据表。 说明 只有具备读写权限的资产才能使用脱敏功能。
	勾选需要脱敏的列数据，支持多选。
AK/SK	请输入访问密钥，请单击创建和查询访问密钥请参见 访问密钥 。创建访问密钥成功后，您可以在访问密钥列表中查看访问密钥ID（AK），在下载.csv文件中查看秘密访问密钥（SK）。

步骤7 单击“下一步”，进入“脱敏算法配置”页面，如[图7-36](#)所示。

图 7-36 脱敏算法配置-DLI 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“脱敏周期配置”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9 单击“下一步”，进入“数据目标配置”页面，如图7-37所示。

图 7-37 数据目标配置-DLI 脱敏任务

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

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DLI任务的创建。

步骤11 进入“DLI”页签，在目标脱敏任务的“操作”列，单击“立即运行”。

步骤12 运行后，系统开始按照设置的脱敏周期执行脱敏任务。

----结束

查看 DLI 脱敏任务运行状态

- 进入“DLI”页签，单击目标脱敏任务前面的 ，查看脱敏任务运行状态，如图7-38所示。

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 7-38 DLI 脱敏任务运行状态



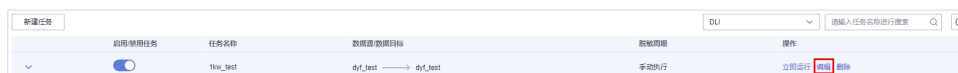
开始时间	结束时间	执行方式	执行行数	状态
2024/05/06 20:16:30 GMT+08:00	2024/05/06 20:20:00 GMT+08:00	手动执行	0	已完成
2024/05/06 19:37:33 GMT+08:00	--	手动执行	0	运行失败

编辑和删除 DLI 脱敏任务

等待运行或运行中的脱敏任务不支持编辑或删除。


- 在DLI脱敏任务列表中，在目标脱敏任务的“操作”列，单击“编辑”，可修改脱敏任务配置信息。

图 7-39 编辑 DLI 脱敏任务



- 在DLI脱敏任务列表中，在目标脱敏任务的“操作”列，单击“删除”。

图 7-40 删除 DLI 脱敏任务



注意

脱敏任务删除后不支持恢复，建议您谨慎操作。

7.1.3.7 创建 OBS 脱敏任务

创建OBS脱敏任务后，可以对OBS类型数据的敏感信息进行脱敏。

本章节将介绍如何创建OBS脱敏任务。

前提条件

- 已完成云资源委托授权，具体请参见[云资产委托授权/停止授权](#)。
- 已添加OBS资产，具体请参见[添加OBS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[新建敏感数据识别任务](#)。


约束条件

- DSC不支持OBS的并行文件系统。
- 支持.txt, .log, .xml, .ini, .sql, .inf, .java, .json等文件或者mime type以text开头的文件。



创建并运行 OBS 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“安全与合规 > 数据安全中心”。

步骤4 在左侧导航树中选择“数据资产保护 > 数据静态脱敏”，并选择“OBS”页签，进入OBS脱敏页面。

步骤5 单击，将“OBS脱敏”设置为，开启OBS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7-9所示。

表 7-9 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： <ul style="list-style-type: none"> 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“OBS”。
数据源	OBS桶名称：单击下拉框选择OBS桶资产名称。
	OBS文件路径：单击下拉框选择OBS桶文件路径。
	文件类型：目前仅支持文本类型。 说明 只有具备读写权限的资产才能使用脱敏功能。

步骤7 单击“下一步”，进入“脱敏算法配置”页面，如图7-41所示。

图 7-41 脱敏算法配置-OBS 脱敏任务



1. 识别模板：单击下拉框选择识别模板。

敏感数据识别模板中该条规则如果未启用，则脱敏页面该条敏感数据不展示。

2. 单击“启用状态”列的开关，关闭该条敏感数据类型不对其进行脱敏。
脱敏页面中的“启用状态”按钮如果关闭，表明虽然启用了该条识别规则，但识别之后不进行脱敏。
3. 脱敏算法：
默认选择选择“仿真脱敏”即脱敏后不损失信息量、不改变数据格式，仿真脱敏支持的敏感数据类型参见[仿真脱敏](#)，同时支持单击下拉框选择如下脱敏算法：
Hash脱敏：详细信息请参见[Hash脱敏](#)。
字符掩盖：详细信息请参见[字符掩盖](#)。
关键字替换：详细信息请参见[关键字替换](#)。
删除脱敏：详细信息请参见[删除脱敏](#)。

步骤8 单击“下一步”，进入“脱敏配置”页面。

- 遍历子目录：打开“遍历子目录”的开关，会对源目录下的子目录进行脱敏。
- 文件重命名：打开“文件重命名”的开关，会对脱敏后的文件进行重命名。
 - 文件前缀/文件后缀：只能由中文字符、英文字母、数字、下划线和中划线组成，长度小于16。
 - 重命名示例：原始文件名称为Test.txt，前缀为DSC_，后缀为1，重命名后的文件为DSC_Test1.txt

步骤9 单击“下一步”，进入“数据目标配置”页面，如[图7-42](#)所示。

图 7-42 数据目标配置-OBS 脱敏任务

1. OBS桶名称：单击下拉框选择脱敏后的存储桶。
2. OBS文件路径：单击在弹框中选择OBS文件路径。

注意

目标OBS桶路径不能选择与源OBS桶路径相同的路径和源OBS桶路径的子目录。


步骤10 单击“完成”，完成OBS脱敏任务的创建。

步骤11 进入“OBS”页签，在目标脱敏任务单击“启用/禁用任务”开关启用任务，在“操作”列单击“立即运行”。

步骤12 运行后，系统开始按照设置执行脱敏任务。

----结束

查看 OBS 脱敏任务运行状态

- 进入“OBS”页签，单击目标脱敏任务前面的 ，查看脱敏任务运行状态，如图 7-43 所示。

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。
- 已终止：用户已手动终止脱敏任务的运行。
- 运行失败：脱敏任务运行失败。

图 7-43 OBS 脱敏任务运行状态



编辑和删除 OBS 脱敏任务

等待运行或运行中的脱敏任务不支持编辑或删除。

- 在 OBS 脱敏任务列表中，在目标脱敏任务的“操作”列，单击“编辑”，可修改脱敏任务配置信息，配置脱敏任务信息请参见 [创建并运行 OBS 脱敏任务](#)。
- 在 OBS 脱敏任务列表中，在目标脱敏任务的“操作”列，单击“删除”。

注意

脱敏任务删除后不支持恢复，建议您谨慎操作。

7.2 数据水印

7.2.1 概述

如果对分发的数据添加水印，当信息泄露时，您可以第一时间从泄露的数据中提取水印标识。通过读取水印标识，可以追溯数据流转过程，精准定位泄露单位及责任人，实现数据溯源追责。对分发的数据添加水印，不会影响分发数据的正常使用。

表 7-10 数据库水印支持的数据库类型

支持嵌入/提取水印的数据库类型	具体支持的数据类型
DWS	smallint, integer, bigint, float4, float8, varchar, text, char
MRS-HIVE	smallint, int, long, float, double, string

表 7-11 文档水印支持的文件类型

支持嵌入/提取水印的文件类型	具体的文件格式
文档	pdf, pptx, docx, xlsx
json数据（调用数据水印接口）	整型、浮点型、字符串型。

表 7-12 图片水印支持的类型

支持嵌入/提取水印的文件类型	具体文件格式
图片（也可通过调用图片水印接口）	*.jpg, *.jpeg, *.jpe, *.png, *.bmp, *.dib, *.rle, *.tiff, *.tif, *.ppm, *.webp, *.tga, *.tpic, *.gif

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**。

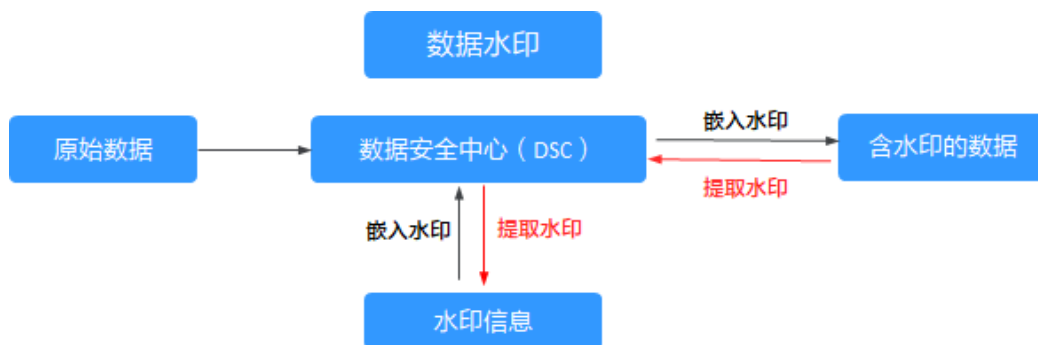
- **数据版权保护**：数字作品被下载或者复制使用，数据库业务（数据挖掘分析）需要提供数据给第三方，发生纠纷时可以通过数字水印明确版权所属。
- **使用过程可追踪溯源**：数据给内部员工或第三方使用时，打上使用者信息水印，可识别使用者身份，提醒使用者要注意安全规范。当发生数据泄露事件时，可追踪泄露源头，挖掘泄露原因。

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。

操作流程

图 7-44 数据水印操作流程



7.2.2 注入水印

7.2.2.1 数据库水印注入

前提条件

- 已完成云资源委托授权，具体请参见[云资产委托授权/停止授权](#)。
- 有已授权的RDS/DWS数据库，具体请参见[授权数据库资产](#)。
- 有已授权的MRS数据库，具体请参见[授权大数据资产](#)。
- 已进行DWS和MRS_Hive权限配置，[（可选）配置DWS和MRS Hive](#)。


约束条件

- DWS数据只支持smallint, integer, bigint, float4, float8, varchar, text, char类型嵌入水印。
- MRS-HIVE数据只支持smallint, int, long, float, double, string类型嵌入水印。
- 嵌入水印单一系列中的内容重复率不高于30%。
- 数据库的内容字符编码格式为UTF-8。
- 数据库注入列为非主键列。
- 数据表中的数据行数建议1500行以上。

新建任务

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“安全与合规 > 数据安全中心”。

步骤4 在左侧导航树中选择“数据资产保护 > 数据库水印”，进入“水印注入”界面。

步骤5 单击“新建任务”，进入“基础信息配置”界面。

图 7-45 基础信息配置

表 7-13 基础信息配置参数说明

参数	说明
任务名称	请输入任务名称。
水印标识	请输入需要注入的水印标识符。
嵌入方案	<p>单击下来框选择嵌入水印的方案，有如下方式：</p> <ul style="list-style-type: none"> 无损-伪列水印：伪造新的属性列，生成与该关系表的其他属性相关的伪列，不容易被攻击者察觉，然后将水印嵌入到伪造的新列中，降低对原数据的损坏。 无损-伪行水印：基于数据各项属性的数据类型、数据格式、取值范围的约束条件生成多个伪造的行，然后将水印嵌入到伪造的新行中，降低对原数据的损坏。 有损-列水印：在列数据直接添加水印，会对数据造成一定的修改或者损坏。 <p>说明 等级越高，水印信息编码位数越长，溯源时误码率越低，需注意高纠错等级需要更大的数据量来保证信息的嵌入完整性，默认为1。</p>

步骤6 单击“下一步”，进入“源目标端配置”界面，请按照参数列表7-14配置相关参数。

- 无损-伪列水印：无损添加水印，创建新的列。

图 7-46 伪列水印

表 7-14 伪列水印源目标端配置参数

参数	说明
数据源类型	<p>单击下拉框选择“数据源类型”。</p> <ul style="list-style-type: none"> 当嵌入方案选择“有损-列水印”时，支持的数据源类型有： <ul style="list-style-type: none"> DWS MRS_HIVE 当嵌入方案选择“无损-伪列水印”和“无损-伪行水印”时，支持的数据类型有： <ul style="list-style-type: none"> DWS PostgreSQL MySQL
数据库实例	单击下拉框选择对应的“数据库实例”。如果没有可用数据库实例，请参考 授权数据库资产 和 授权大数据资产 章节进行授权。
数据库	单击下拉框选择对应的“数据库”。
模式	当“数据库类型”为“DWS”和“PostgreSQL”时显示该参数。单击选择对应的“模式”。
源表名	单击选择对应的“源表名”。
列名称	只能由字母、数字、下划线或中划线组成，且不能超过255个字符长度。
列数据类型	<p>单击选择嵌入伪列的数据类型。</p> <ul style="list-style-type: none"> 数字类型 字符串 日期类型

参数	说明
样例	选择“设置字段规则”后显示嵌入伪列数据样例。
设置字段规则	<ul style="list-style-type: none"> “列数据类型”选择“数字类型”时，该参数为随机数，可以指定随机数的范围和随机数的精度，如果未指定范围和精度将随机生成伪造数据。 “列数据类型”选择“字符串”时，可以单击下拉框选择人名、身份证号、手机号等类型的伪造数据。 “列数据类型”选择“日期类型”时，可以指定日期范围，如果没有指定日期范围，将随机生成伪造数据。
增加伪列	可单击“增加伪列”添加两列伪列数据。
目标表名	请输入目标表名，只能由字母、数字、下划线或中划线组成，且不能超过255个字符长度。

- 无损-伪行水印：无损添加水印，复制新的行数据注入水印。

图 7-47 伪行水印

The screenshot shows a configuration interface with three steps: 1. Basic Information Configuration, 2. Source and Target Configuration (active), and 3. Scheduling Information Configuration. Under 'Source Configuration', there are dropdown menus for 'Data Source Type' (DWS), 'Database Instance' (DWS), 'Database' (gaussdb), and 'Mode' (lhy). There is also a dropdown for 'Source Table Name' (table_name_1) with a help icon. A text input field for 'Pseudo-row Spans' is set to 1. Under 'Target Configuration', there is a text input field for 'Target Table Name' (fd). At the bottom, there are three buttons: 'Previous Step', 'Next Step' (highlighted in red), and 'Cancel'.

表 7-15 伪行水印源目标端配置参数

参数	说明	取值样例
数据源类型	单击下拉框选择“数据源类型”，支持的数据源类型有： - DWS - PostgreSQL - MySQL	DWS
数据库实例	单击下拉框选择对应的“数据库实例”。如果没有可用数据库实例，请参考 授权数据库资产 和 授权大数据资产 章节进行授权。	DWS-dsc-Test
数据库	单击下拉框选择对应的“数据库”。	gaussdb
模式	当“数据库类型”为“DWS”和“PostgreSQL”时显示该参数。单击选择对应的“模式”。	pg_catalog
源表名	单击选择对应的源数据表名。	pg_proc
伪行跨行数	请输入创建伪行数据的行数，输入值为大于1的有效整数。	10
目标表名	请输入嵌入水印后的数据存储表名称，只能由字母、数字、下划线或中划线组成，且不能超过255个字符长度。	Test_Table

- 有损-列水印：在列数据直接添加水印标识。

图 7-48 有损列水印

基础信息配置 — 2 源目标端配置 — 3 调度信息配置

源端配置

- * 数据源类型: DWS
- * 数据库实例: DWS-
- * 数据库: gaussdb
- * 模式: lhy
- * 源表名: test_dws_watermark

水印嵌入列

列名称	源数据类型
<input type="checkbox"/> distance	double precision
<input checked="" type="checkbox"/> age	integer
<input type="checkbox"/> name	character varying
<input type="checkbox"/> address	character varying

目标端配置

- * 目标表名: fd

上一步 下一步 取消

表 7-16 有损列水印源目标端配置参数

参数	说明	取值样例
数据源类型	单击下拉框选择“数据源类型”，支持的数据源类型有： - DWS - MRS-HIVE	DWS
数据库实例	单击下拉框选择对应的“数据库实例”。如果没有可用数据库实例，请参考 授权数据库资产 和 授权大数据资产 章节进行授权。	DWS-dsc-Test
数据库	单击下拉框选择对应的“数据库”。	gaussdb
模式	当“数据库类型”为“DWS”时显示该参数。单击选择对应的“模式”。	pg_catalog
源表名	单击选择对应的“源表名”。	pg_proc

参数	说明	取值样例
水印嵌入列	单击选择水印嵌入的列数据，可多选。 说明 - 源数据库字符集需使用 UTF-8。 - 嵌入水印单一列中的内容重复率不高于30%。	-
目标表名	请输入嵌入水印后的数据存储表名称，只能由字母、数字、下划线或中划线组成，且不能超过255个字符长度。	Test_Table

步骤7 单击“下一步”，进入“调度信息配置”界面。

图 7-49 调度信息配置

- “调度参数”为“单次”时，可以选择“立即执行”，也可以选择“定时启动”在某一时间启动嵌入水印任务。
- “调度参数”为“每日”、“每周”、“每月”时，分别选择在某日某一时间、某周某一时间、每月某一时间启动嵌入水印任务。


步骤8 单击“完成”，水印嵌入任务创建完成。

----结束

运行任务

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“安全与合规 > 数据安全中心”。

步骤4 在左侧导航树中选择“数据资产保护 > 数据库水印”，进入“水印注入”界面。

图 7-50 数据库水印注入

任务名称	源端数据库	源端数据库	源表名	任务状态	水印标识	注入方案	调度信息	最近运行时间	操作
row	PostgreSQL	test	qwer_1111	执行完成		无感-行水印	单次	2023/09/19 15:49:39...	编辑 删除 更多
test	PostgreSQL	test	testlog	执行完成		无感-列水印	单次	2023/09/19 15:29:39...	编辑 删除 更多

步骤5 在目标任务操作列单击“更多 > 运行”，该任务开始运行。


----结束

开启任务

当水印任务为定时任务时显示该参数。

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“安全与合规 > 数据安全中心”。

步骤4 在左侧导航树中选择“数据资产保护 > 数据库水印”，进入“水印注入”界面。

图 7-51 数据库水印注入

任务名称	源端数据库	源端数据库	源表名	任务状态	水印标识	注入方案	调度信息	最近运行时间	操作
row	PostgreSQL	test	qwer_1111	执行完成		无感-行水印	单次	2023/09/19 15:49:39...	编辑 删除 更多
test	PostgreSQL	test	testlog	执行完成		无感-列水印	单次	2023/09/19 15:29:39...	编辑 删除 更多

步骤5 在目标任务操作列单击“更多 > 开启任务”开启该任务。


----结束

关闭任务

当水印任务为定时任务时显示该参数。

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“安全与合规 > 数据安全中心”。

步骤4 在左侧导航树中选择“数据资产保护 > 数据库水印”，进入“水印注入”界面。

图 7-52 数据库水印注入

任务名称	源端数据库	源端数据库	源表名	任务状态	水印标识	注入方案	调度信息	最近运行时间	操作
row	PostgreSQL	test	qwer_1111	执行完成		无感-行水印	单次	2023/09/19 15:49:39...	编辑 删除 更多
test	PostgreSQL	test	testlog	执行完成		无感-列水印	单次	2023/09/19 15:29:39...	编辑 删除 更多

步骤5 在目标任务操作列单击“更多 > 关闭任务”关闭该任务。

----结束

编辑和删除嵌入水印任务

运行中的嵌入水印任务不支持编辑或删除。

- 在目标任务“操作”列单击“编辑”，可对嵌入水印任务配置信息进行修改。

图 7-53 编辑嵌入水印任务



- 在目标任务“操作”列单击“删除”，可删除该嵌入水印任务。也可以选择多条任务，单击列表左上角的批量删除，删除多条任务。

图 7-54 删除嵌入水印任务



说明

删除操作无法恢复，请谨慎操作。

7.2.2.2 文档水印注入

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

- 已完成OBS资产委托授权，参考[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。
- 文档格式为pdf, pptx, docx, xlsx。


约束条件

- PDF文件和word文件最大50M。
- excel文件最大70M。
- ppt文件最大20M。

创建 OBS 桶文件注入水印任务

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“安全与合规 > 数据安全中心”。

步骤4 在左侧导航树中选择“数据资产保护 > 文档水印”，进入“水印注入”页面。

步骤5 单击任务列表左上角的“新建任务”。

图 7-55 新建任务

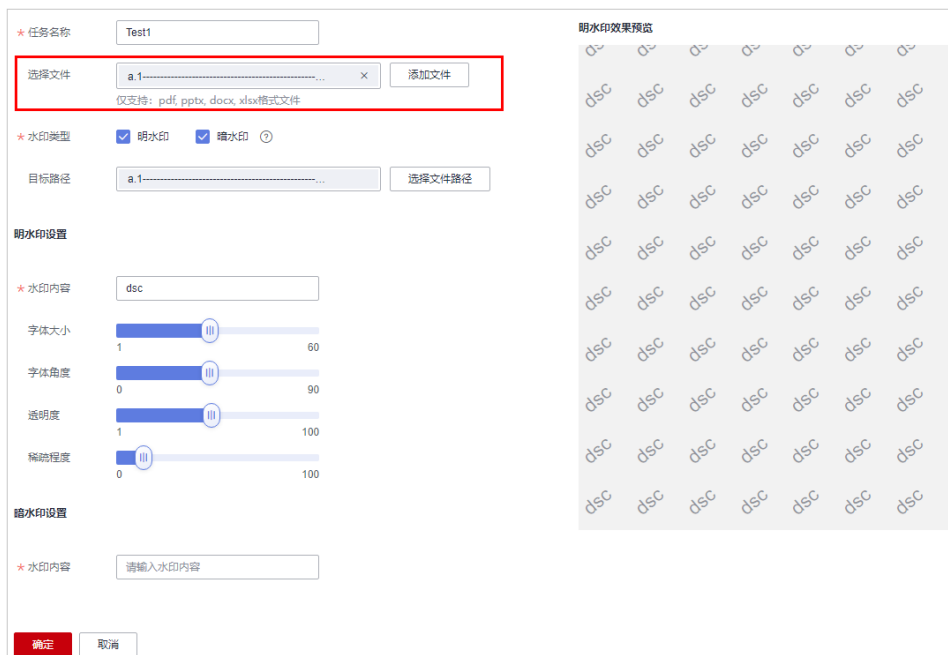


步骤6 按照如表7-17所示配置参数信息。

表 7-17 参数配置

参数	说明
任务名称	请输入水印注入任务名称。
选择文件	单击“添加文件”，在右侧选择需要添加水印的桶名称，左侧选择文件，支持多选。
水印类型	支持“明水印”和“暗水印”，可多选。 <ul style="list-style-type: none"> 明水印，水印内容可以展现在文件内容上，如图7-56中“明水印效果预览”。 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文档水印提取章节。
目标路径	单击“选择文件路径”，选择存储注入水印后的文件。
明水印设置	当“水印类型”选择“明水印”时，拖动滑块设置“水印内容”、“字体大小”、“字体角度”、“透明度”以及水印的“稀疏程度”。
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”。

图 7-56 注入水印



步骤7 单击“确定”，右上角提示任务创建成功，注入水印任务创建完成。

步骤8 在水印任务列表中，单击任务名称前的 查看任务运行状态。

- 如果您注入的是明水印，单击“下载”获取注入水印的文件。
- 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[文档水印提取](#)。

图 7-57 文件水印注入



----结束

本地文件水印注入

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“安全与合规 > 数据安全中心”。

步骤4 在左侧导航树中选择“数据资产保护 > 文档水印”，进入“水印注入”页面。

步骤5 选择“本地文件”页签，进入“水印注入”页面。

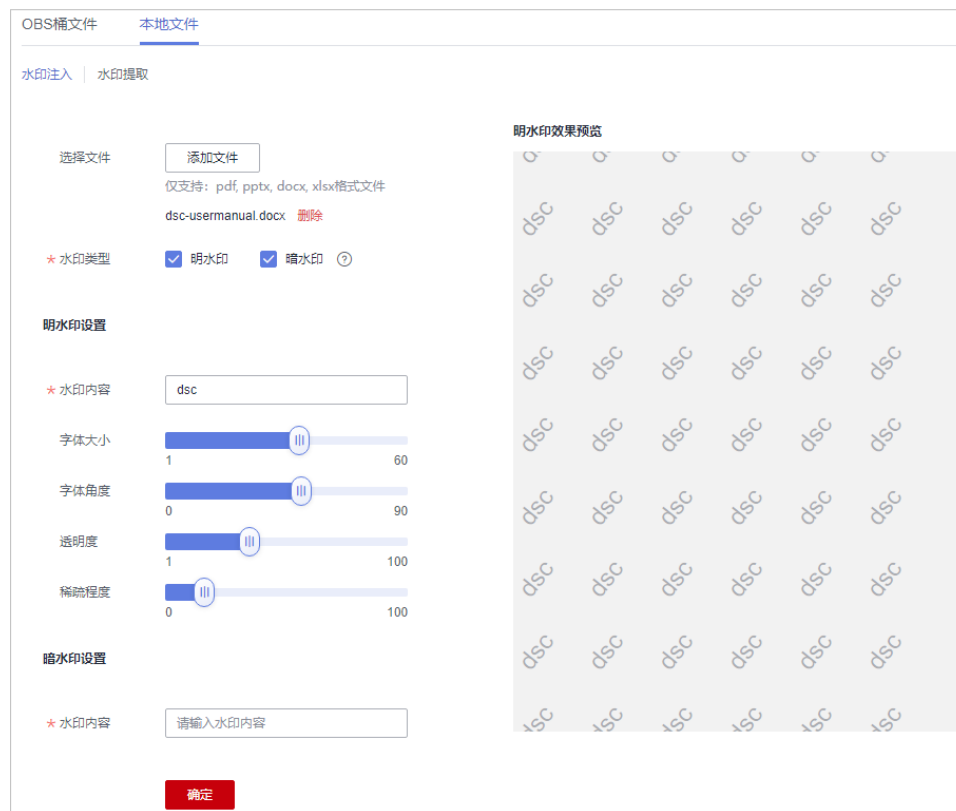
步骤6 单击“添加文件”，选择需要注入水印的文件。

步骤7 文件上传成功后，参照[表7-18](#)配置相关水印参数，如[图7-58](#)所示。

表 7-18 水印设置参数说明

参数名称	参数说明
水印类型	支持“明水印”和“暗水印”，可多选。 <ul style="list-style-type: none"> 明水印，水印内容可以展现在文件内容上，如图7-58中“明水印效果预览”。 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文档水印提取章节。
明水印设置	当“水印类型”选择“明水印”时，拖动滑块设置“水印内容”、“字体大小”、“字体角度”、“透明度”以及水印的“稀疏程度”。
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”。

图 7-58 本地文件水印注入



步骤8 参数配置完后，单击“确定”，注入水印的文件会自动下载到您的本地路径。

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[文档水印提取](#)。

----结束

相关操作

单击目标水印注入任务名称前的[^]，查看、下载OBS桶文件注入水印任务的运行情况和状态。

- 运行中：查看注入水印任务进度。
- 已完成：单击“操作”列的“下载”，下载注入水印后的OBS桶文件。
- 运行失败：注入水印任务执行失败，鼠标移动至[?]查看失败原因。

7.2.2.3 图片水印注入

数据安全中心控制台针对jpg、jpeg等多种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）或者本地图片增加自定义水印内容。

前提条件

- 已完成OBS资产委托授权，参考[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。
- 支持的图片格式为：*.jpg, *.jpeg, *.jpe, *.png, *.bmp, *.dib, *.rle, *.tiff, *.tif, *.ppm, *.webp, *.tga, *.tpic, *.gif。


约束条件

- 图片最大不超过20M。
- 待添加水印的图片文件，添加的图片尺寸需要大于128*128像素。
- 待嵌入的文字水印内容，长度不超过32个字符。

OBS 桶文件注入水印

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“安全与合规 > 数据安全中心”。

步骤4 在左侧导航树中选择“数据资产保护 > 图片水印”，进入“图片水印”页面。

步骤5 在“OBS桶文件”页签，对“文件设置”模块进行路径设置。

图 7-59 文件设置

The screenshot shows a web interface for file settings. At the top, there are tabs for 'OBS桶文件' (OBS Bucket File) and '本地文件' (Local File). Below are options for '水印注入' (Watermark Injection) and '水印提取' (Watermark Extraction). The '文件设置' (File Settings) section contains three input fields: '原始图片路径' (Original Image Path) with the value 'dsc-flight-test-obs/保单/10.jpg' and a red '添加' (Add) button; '存储目标路径' (Storage Target Path) with the value 'a.1-----z/' and a red '添加' (Add) button; and '存储目标文件名' (Storage Target Filename) with the value 'test.jpg'.

1. 单击“原始图片路径”后的“添加”，选择云上原始图片存储路径，选择的图片大小不超过20M。
2. 单击“存储目标路径”后的“添加”，选择云上存储路径。
3. 单击“存储目标文件名”输入框，输入注入水印后的图片保存文件名称。文件名长度不超过32位，且后缀为*.jpg、*.jpeg、*.jpe、*.png、*.bmp、*.dib、*.rle、*.tiff、*.tif、*.ppm、*.webp、*.tga、*.tpic或*.gif。

步骤6 “水印类型”分为“明水印”和“暗水印”两种类型。

- 明水印：水印内容可以展现在图片内容上，如图7-60中“明水印效果预览”。相关参数配置如图7-60所示。

表 7-19 明水印设置

参数	说明
水印内容	单击下拉框选择“水印内容”： - “图片水印” - “文字水印”。
图片路径	“水印内容”选择“图片水印”时，单击“添加”选择云上的图片作为水印。 水印图片需要和原始图片在同一区域，否则会预览失败。
文字内容	“水印内容”选择“文字水印”时，单击输入框输入文字水印内容，长度范围为1-32个字符，当前仅支持数字及英文大小写。
水印位置	在图中选择水印插入的位置。
图片尺寸	“水印内容”选择“图片水印”时显示该参数，待插入图片的绝对大小值，输入值必须在0-100之间。

参数	说明
水印大小	“水印内容”选择“文字水印”时显示该参数，待插入文字水印的大小，输入值必须在1-100之间。
水印透明度	插入水印的透明度，输入值必须在1-100之间。
水平边距	待插入水印相对图片的水平边距，输入值必须在0-100之间。
垂直边距	待插入水印相对图片的垂直边距，输入值必须在0-100之间。
字体颜色	“水印内容”选择“文字水印”时显示该参数，单击颜色条选择需要插入的文字水印的字体颜色。

图 7-60 明水印设置

明水印设置

水印内容
文字水印

文字内容
12QW|
文字水印的长度范围为1-32个字符。当前仅支持数字及英文大小写。

水印位置

↖	↑	↗
←	-	→
↙	↓	↘

水印大小
- 50 +

水印透明度
- 50 +

水平边距
- 0 +

垂直边距
- 0 +

字体颜色
[红色色条]

- 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[图片水印提取](#)章节。

说明

嵌入图片时，嵌入的水印图片像素要大于或等于64*64，提取出的水印结果是嵌入的水印图片缩小到64*64像素后的图片。

表 7-20 暗水印设置

参数	说明
水印内容	单击下拉框选择“水印内容”： - “图片水印” - “文字水印”。
文字内容	“水印内容”选择“文字水印”时，单击输入框输入文字水印内容，长度范围为1-32个字符。
图片路径	“水印内容”选择“图片水印”时单击“添加”选择云上的图片作为水印。

图 7-61 暗水印设置

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[图片水印提取](#)。

步骤8 单击“预览”在右侧“明水印图片预览”区域预览水印效果。暗水印无法预览。


步骤9 单击“确定”，完成水印注入。

----结束

本地文件水印注入

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“安全与合规 > 数据安全中心”。

步骤4 在左侧导航树中选择“数据资产保护 > 图片水印”，进入“图片水印”页面。

步骤5 选择“本地文件”页签，进入“水印注入”页面。

步骤6 对“文件设置”模块进行路径设置。

图 7-62 本地水印注入文件设置



该截图展示了“本地文件”页签下的“水印注入”配置界面。界面顶部有“OBS桶文件”和“本地文件”两个页签，当前选中“本地文件”。下方有“水印注入”和“水印提取”两个子选项卡，当前选中“水印注入”。主要配置区域为“文件设置”，包含三个输入项：1. “原始图片路径”：一个文本输入框，右侧有一个“添加”按钮。下方有提示文字：“图片的对象后缀为jpg、jpeg、jpe、png、bmp、dib、rle、tiff、tif、ppm、webp、tga、tpic或者gif，大小不超过20M”。2. “存储目标路径”：一个文本输入框，右侧有一个“添加”按钮。3. “存储目标文件名”：一个文本输入框，提示文字为“请输入内容”。

1. 单击“原始图片路径”后的“添加”，选择云上原始图片存储路径，选择的图片大小不超过20M。
2. 单击“存储目标路径”后的“添加”，选择云上存储路径。
3. 单击“存储目标文件名”输入框，输入注入水印后的图片保存文件名称。文件名长度不超过32位，且后缀为*.jpg、*.jpeg、*.jpe、*.png、*.bmp、*.dib、*.rle、*.tiff、*.tif、*.ppm、*.webp、*.tga、*.tpic或*.gif。

步骤7 “水印类型”分为“明水印”和“暗水印”两种类型。

- 明水印：水印内容可以展现在图片内容上。
- 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[图片水印提取](#)章节。

步骤8 根据如[表7-21](#)所示参数进行水印相关参数设置。

表 7-21 水印设置

水印类型	参数	说明
明水印	水印内容	单击下拉框选择“水印内容”： <ul style="list-style-type: none"> “图片水印” “文字水印”。
	水印图片	“水印内容”选择“图片水印”时单击“添加”选择图片作为水印。 水印图片需要和原始图片在同一区域，否则会预览失败。
	文字内容	“水印内容”选择“文字水印”时显示该参数，单击输入文字水印内容，文字水印的长度范围为1-32个字符，当前仅支持数字及英文大小写。
	水印位置	在图中选择水印插入的位置。
	图片尺寸	“水印内容”选择“图片水印”时显示该参数，待插入图片的绝对大小值，输入值必须在0-100之间。
	水印大小	“水印内容”选择“文字水印”时显示该参数，待插入文字水印的大小，输入值必须在1-100之间。
	水印透明度	插入水印的透明度，输入值必须在1-100之间。
	水平边距	待插入水印相对图片的水平边距，输入值必须在0-100之间。
	垂直边距	待插入水印相对图片的垂直边距，输入值必须在0-100之间。
	字体颜色	“水印内容”选择“文字水印”时显示该参数，单击颜色条选择需要插入的文字水印的字体颜色。
暗水印	水印内容	单击下拉框选择“水印内容”： <ul style="list-style-type: none"> “图片水印” “文字水印”。
	水印图片	“水印内容”选择“图片水印”时显示该参数，单击“添加文件”选择本地图片作为水印。
	文字内容	“水印内容”选择“文字水印”时显示该参数，单击输入水印文字内容。

步骤9 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[图片水印提取](#)。

----结束

7.2.3 提取水印

7.2.3.1 数据库水印提取

前提条件

- 已完成云资源委托授权，具体请参见[云资产委托授权/停止授权](#)。
- 有已授权的RDS/DWS数据库，具体请参见[授权数据库资产](#)。
- 有已授权的MRS数据库，具体请参见[授权大数据资产](#)。
- 已进行DWS和MRS_Hive权限配置，（可选）配置DWS和MRS Hive。


约束条件

- 源文件格式必须为csv文件且大小不能超过20M。
- 表数据记录预估在1500行以上。
- csv文件内容格式为UTF8编码，请保证数据的完整性以及正确性。

新建任务

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“安全与合规 > 数据安全中心”。

步骤4 在左侧导航树中选择“数据资产保护 > 数据库水印”，进入“水印注入”界面。

步骤5 单击“水印提取”页签，进入“水印提取”界面。

步骤6 单击“新建任务”，进入新建任务弹框，请根据[表7-22](#)配置相关参数。

图 7-63 新建提取任务

新建任务

* 任务名称

描述
0/1,024

源文件

提取方式

分隔符

表 7-22 新建水印提取任务

参数	说明
任务名称	请输入任务名称。
源文件	请选择本地含有水印的源文件，源文件必须为csv文件且大小不能超过20M，表数据记录预估在1500行以上，csv文件内容需为UTF8编码，请保证数据的完整性以及正确性。
提取方式	单击下拉框选择提取水印的方式，有损列嵌入以及无损列嵌入需要使用按列提取，无损行嵌入则需要使用按行提取。
分隔符	文件中的分隔符。例如","。


步骤7 单击“确定”，完成水印提取任务创建。

----结束

查看结果

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“安全与合规 > 数据安全中心”。

步骤4 在左侧导航树中选择“数据资产保护 > 数据库水印”，进入“水印注入”界面。

步骤5 单击“水印提取”页签，进入“水印提取”界面。

步骤6 在目标任务“操作”列单击“查看结果”。


----结束

删除水印提取任务

执行中的提取水印任务不支持删除。

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“安全与合规 > 数据安全中心”。

步骤4 在左侧导航树中选择“数据资产保护 > 数据库水印”，进入“水印注入”界面。

步骤5 单击“水印提取”页签，进入“水印提取”界面。

步骤6 在目标任务“操作”列单击“删除”，可删除该水印提取任务。也可以选择多条任务，单击列表左上角的批量删除，删除多条任务。

说明

删除操作无法恢复，请谨慎操作。

----结束

7.2.3.2 文档水印提取

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

- 已完成OBS资产委托授权，参考[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。
- 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。
- PDF文件和Word文件最大50M。
- Excel文件最大70M。
- PPT文件最大20M。

创建 OBS 桶文件水印提取任务

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。

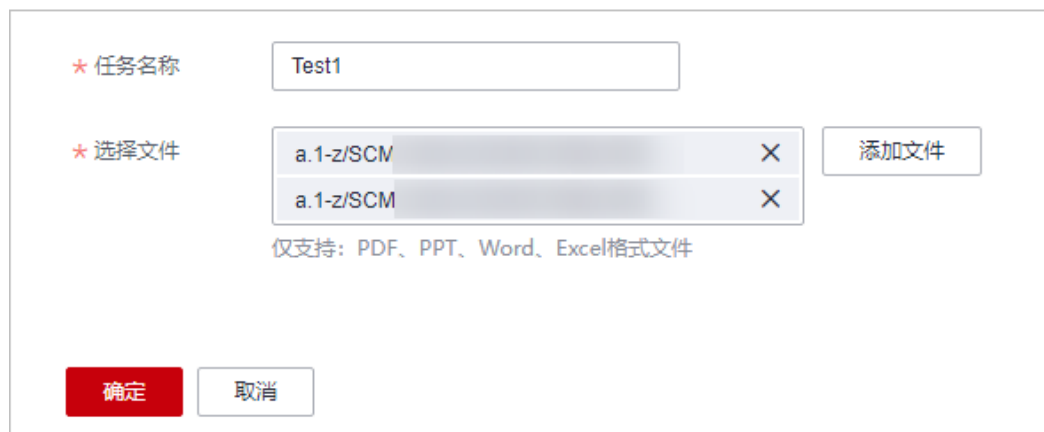
步骤3 在左侧导航树中，单击，选择“安全与合规 > 数据安全中心”。

步骤4 在左侧导航树中选择“数据资产保护 > 文档水印”，进入“OBS桶文件”页签。

步骤5 选择“水印提取”页签，进入“水印提取”页面。

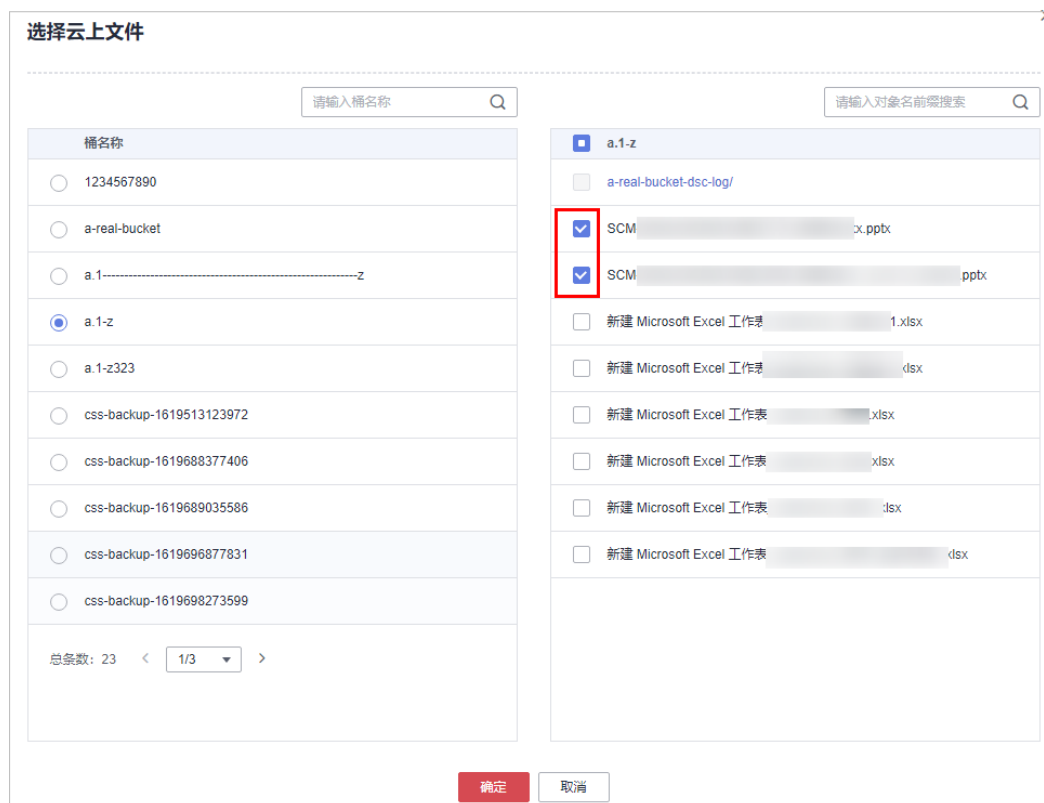
步骤6 单击左上角“新建任务”，进入“新建任务”页面。

图 7-64 新建水印提取任务



步骤7 单击添加文件选择需要进行提取水印的文件，OBS桶文件支持多选。

图 7-65 选择文件



步骤8 单击“确定”，提取水印任务创建完成。

步骤9 单击目标任务名称前的 \surd ，查看水印提取完成的OBS桶文件的暗水印内容。

图 7-66 暗水印


任务名称	状态	源桶路径	操作
新建.xlsx	运行中	--	删除
新建.xlsx	运行中	--	删除
新建.xlsx	已完成	--	删除
dsc_datamap_network_asset_info_收入分为.xlsx	运行中	--	删除
SCM.pptx	运行失败	--	删除

----结束

本地文件水印提取

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“安全与合规 > 数据安全中心”。

步骤4 在左侧导航树中选择“数据资产保护 > 文档水印”，进入“OBS桶文件”页签。

步骤5 选择“本地文件 > 水印提取”，进入水印提取页面。

图 7-67 水印提取页面



步骤6 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。


说明


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

步骤7 文件上传后，单击“确定”，暗水印内容将展示到弹框中。

----结束

相关操作

单击目标水印注入任务名称前的 ，查看OBS通文件水印提取任务的运行情况和状态。

- 运行中：显示提取水印任务进度。
- 已完成：暗水印列显示水印内容，没有暗水印则显示--。
- 运行失败：提取水印任务执行失败，鼠标移动至  查看失败原因。

7.2.3.3 图片水印提取

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图片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

- 已完成OBS资产委托授权，参考[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。
- 支持的图片格式为：*.jpg, *.jpeg, *.jpe, *.png, *.bmp, *.dib, *.rle, *.tiff, *.tif, *.ppm, *.webp, *.tga, *.tpic, *.gif。
- 原始图片像素要大于128*128。


约束条件

- 本章节的方法仅针对提取单个图片文件的暗水印。
- 图片最大不超过20M。
- 暗水印内容，长度不超过32个字节。

OBS 桶文件水印提取

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“安全与合规 > 数据安全中心”。

步骤4 在左侧导航树中选择“数据资产保护 > 文档水印”，进入“OBS桶文件”页签。

步骤5 选择“水印提取”页签，进入“水印提取”页面。

步骤6 选择提取内容：

- “提取内容”为“文字”：单击“添加”选择待提取水印的图片。

图 7-68 提取文字内容



- “提取内容”为“图片”：
 - a. 单击“选择文件”后的“添加”，选择需要提取水印的图片。
 - b. 单击“存储目标路径”后的“添加”，选择存储提取的水印图片的路径。
 - c. 单击“存储目标文件名”输入框输入提取的水印图片的文件名称。

图 7-69 提取图片内容




步骤7 单击“确定”，“提取内容”为“文字”时，暗水印内容将展示到弹框中。“提取内容”为“图片”时，请在存储目标路径下查看。

----结束

本地文件水印提取

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“安全与合规 > 数据安全中心”。

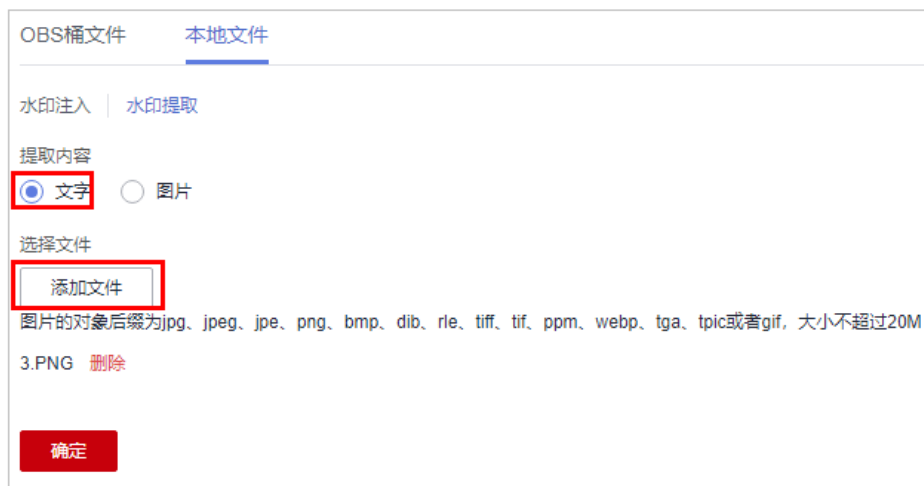
步骤4 在左侧导航树中选择“数据资产保护 > 文档水印”，进入“OBS桶文件”页签。

步骤5 选择“本地文件 > 水印提取”，进入“水印提取”页面。

步骤6 选择“提取内容”：

- “提取内容”为“文字”：单击“添加文件”，将本地需要提取暗水印的图片上传到DSC平台。

图 7-70 提取文字水印



- “提取内容”为“图片”：单击“添加文件”，本地需要提取暗水印的图片上传到DSC平台。

图 7-71 提取图片水印



步骤7 文件上传后，单击“确定”，暗水印内容将展示到弹框中。

---结束

7.3（可选）配置 DWS 和 MRS Hive

使用数据库水印前，您先完成如下操作前提：

1. 修改DWS集群参数。

为能正常对DWS数据进行敏感数据识别和隐私保护管理，需要[提交工单](#)对DWS集群的`javaudf_disable_feature`参数进行修改，否则将导致操作失败。如果您不涉及DWS数据，则可以不用修改。


2. [修改Hive用户权限](#)

为能正常对MRS_Hive数据进行数据水印相关操作，必须通过Ranger管理员为Hive用户进行相关的权限设置。

修改 Hive 用户权限

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“大数据 > MapReduce服务”，进入MapReduce服务“现有集群”界面。

步骤4 在集群列表中单击指定的集群名称，进入集群信息页面。

步骤5 单击“集群管理”页面后的“前往 Manager”，在弹出的窗口中单击“确定”，进入Manager登录页面。

步骤6 输入默认用户名“**admin**”及创建集群时设置的密码，单击“登录”进入Manager页面。

步骤7 选择“集群 > > 服务 > Ranger”，进入Ranger服务概览页面。

步骤8 单击“基本信息”区域中的“RangerAdmin”，进入Ranger WebUI界面。由于**admin**用户在Ranger中的用户类型为“User”，只能查看Access Manager和Security Zone页面。因此您需要切换至**rangeradmin**用户或者其他具有Ranger管理员权限的用户：

1. 在Ranger WebUI界面，单击右上角用户名，选择“Log Out”，退出当前用户。
2. 使用**rangeradmin**用户或者其他具有Ranger管理员权限用户重新登录。

步骤9 在首页中单击“HADOOP SQL”区域的组件插件名称如“Hive”。

步骤10 在“Access”页签单击“Add New Policy”，添加Hive权限控制策略。

步骤11 根据权限要求配置相关参数。关键参数如[表7-23](#)，其他参数无需填写，保持默认即可。

表 7-23 Hive 权限参数

参数名称	描述	取值
Policy Name	策略名称，可自定义，不能与本服务内其他策略名称重复。	示例： dataarts_dsc
database	适用该策略的Hive数据库名称。 此处需将参数“database”修改为“global”，取值为“*”，表示此策略全局生效。	global: *
Allow Conditions	策略允许条件，配置本策略内允许的权限及例外。在“Select Role”、“Select Group”、“Select User”列选择已创建好的需要授予权限的Role、用户组或用户，单击“Add Conditions”，添加策略适用的IP地址范围，然后再单击“Add Permissions”，添加对应权限。 此处需配置“Select Group”、“Select User”和“Add Permissions”列。 <ul style="list-style-type: none"> • Select Group: 选择需要对MRS Hive数据进行数据水印相关操作的用户组。 • Select User: 选择需要对MRS Hive数据进行数据水印相关操作的用户。如果用户已在选择的用户组中，则无需重复选择。 • Add Permissions: All，选择“Select/Deselect All”全选所有权限。 	示例： <ul style="list-style-type: none"> • Select Group: dayu_user • Select User: dgc_test • Add Permissions : All

步骤12 单击“Add”，在策略列表即可查看策略的基本信息。

----结束

8 数据安全运营

8.1 态势大屏

在现场讲解汇报、实时监控等场景下，为了获得更好的演示效果，通常需要将数据安全中心服务的分析结果展示在大型屏幕上。如果只是单纯将控制台界面放大显示，视觉效果并不是很理想。此时可以利用态势大屏，展示专为大型屏幕设计的服务界面，获得更清晰的态势信息和更好的视觉效果。

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


前提条件

- 已完成云资产委托授权，参考[云资产委托授权/停止授权](#)进行操作。
- 已开通DBSS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“安全与合规 > 数据安全中心”。

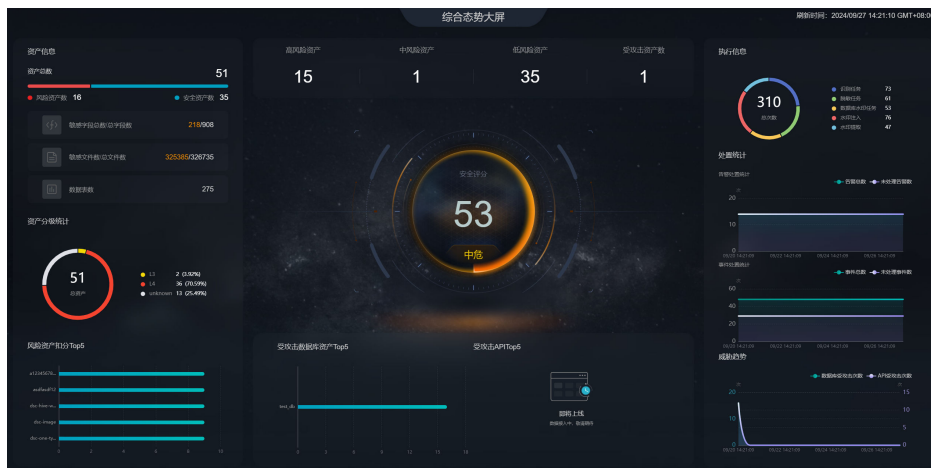
步骤4 在左侧导航树中，选择“数据安全运营 > 态势大屏”，进入“态势大屏”界面。

图 8-1 态势大屏



步骤5 单击“综合态势大屏”图片，进入“综合态势大屏”界面。
页面中各个模块的功能介绍和使用方法详见下述内容。

图 8-2 综合态势大屏



----结束

安全评分

如图8-3所示，展示当前全部资产的安全健康得分。

表 8-1 安全评分

参数名称	来源	说明
安全评分	资产地图评分	具体评分计算规则请在控制台查看，具体参见 查看评分规则 ，最终得分的高、中、低风险的划分标准如下： <ul style="list-style-type: none"> • 100：无风险 • 81-99：低危 • 51-80：中危 • 0-50：高危

图 8-3 安全评分



风险资产统计情况

如[图8-4](#)所示，展示已授权资产的风险统计情况。

风险资产统计情况来源于“资产地图”，如需查看资产详细情况，请前往该页面进行查看。

表 8-2 安全评分

参数名称	来源	说明
高/中/低风险资产	资产地图的“安全防护策略分析”中的“风险等级”。	详细计算规则请参见 风险统计数据 。
受攻击资产数	“数据安全运营 > 告警管理”中的告警。	根据“告警管理”中的告警来分析受攻击的资产数。

图 8-4 风险资产统计情况



资产信息

如图8-5所示，展示资产总数以及高中风险资产总和资产数据识别情况。

表 8-3 资产信息

参数名称	来源	说明
资产总数	高、中、低风险资产总和。	-
风险资产数	高、中风险资产总和。	-
安全资产数	低风险资产数。	-
敏感字段总数/总字段数	敏感数据识别。	统计敏感数据列总数/列的总数。
敏感文件数/总文件数	敏感数据识别。	统计OBS资产中的敏感数据文件总数/总文件数。
数据表数	敏感数据总表数。	统计敏感数据表总数。

图 8-5 资产信息



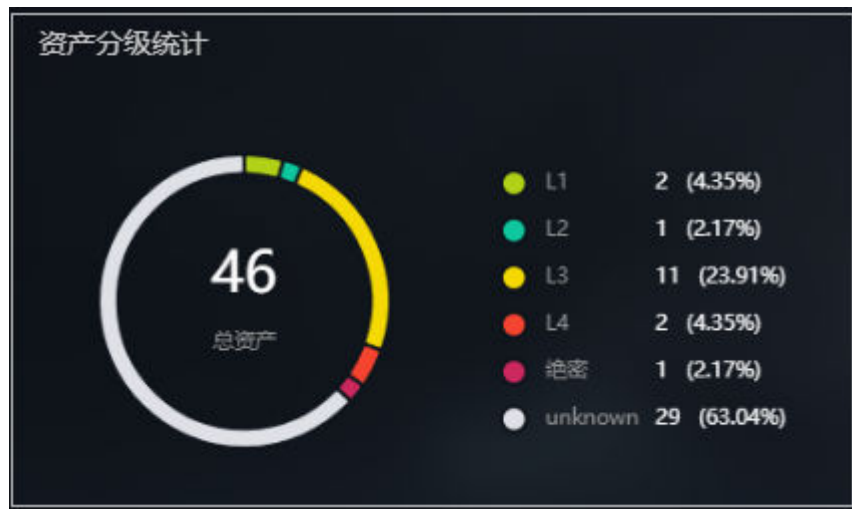
资产分级统计

如图8-6所示，展示经过敏感数据识别进行分类分级的资产总数以及各级别下的资产数量和占比。

表 8-4 资产信息

参数名称	统计周期	说明
总资产	资产地图	通过敏感数据识别功能分级分类的资产总数。
级别	敏感数据识别	各级别的资产数以及相对总资产数的占比。

图 8-6 资产分级统计



风险资产扣分 Top5

如图 8-7 所示，展示风险扣分 Top5 资产，鼠标移动至柱状图显示“资产名称”、“资产类型”、“数据源”以及“风险扣分”。

表 8-5 资产信息

参数名称	来源	说明
风险资产扣分	资产地图	根据资产评分规则中的扣分规则展示单个资产的“资产名称”、“资产类型”、“数据源”以及“风险扣分”。具体扣分规则请在控制台查看，具体参见 查看评分规则 。

图 8-7 风险资产扣分 Top5



执行信息

如图8-8所示，展示敏感数据识别、数据静态脱敏、数据水印执行任务的总和和各功能的执行任务数量。

表 8-6 执行信息

参数名称	来源	说明
总次数	敏感数据识别、数据静态脱敏、数据水印	执行任务的总和统计。

图 8-8 执行信息



处置统计

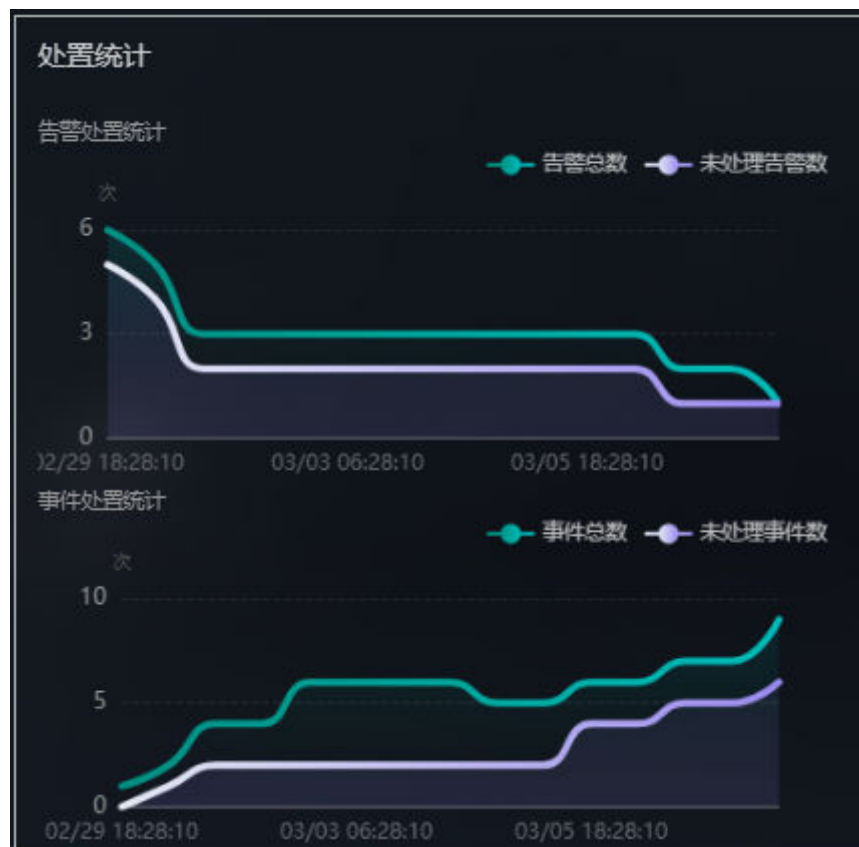
- 告警处置统计
按时间展示来自“告警管理”功能的“告警总数”和“未处理告警数”。
- 事件处置统计

按时间展示来自“事件管理”功能的“事件总数”和“未处理事件数”。

表 8-7 执行信息

参数名称	来源	说明
告警总数	告警管理	统计告警管理列表中的告警总数。
未处理告警数	告警管理	统计告警管理列表中的告警状态为“开启”的告警数量。
事件总数	事件管理	统计事件管理列表中的事件总数。
未处理事件总数	事件管理	统计告警管理列表中的告警状态为“开启”和“阻塞”的事件数量。

图 8-9 处置统计



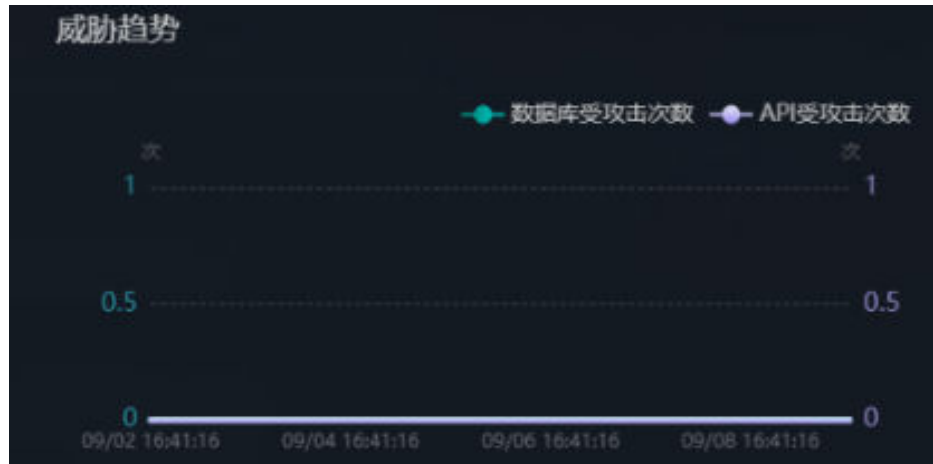
威胁趋势

如图8-10所示，按时间展示数据库受攻击次数。

表 8-8 执行信息

参数名称	来源	说明
数据库受攻击次数	告警管理	根据“告警管理”中的告警来分析数据库受攻击的次数。

图 8-10 威胁趋势



受攻击 Top5

表 8-9 受攻击 Top5

参数名称	来源	说明
受攻击数据库资产 Top5	告警管理	根据“告警管理”中的告警来分析展示受攻击数据库受攻击的 Top5 数据库资产。

受攻击数据库资产 Top5

如图 8-11 所示，展示受攻击的 Top5 数据库资产，鼠标移动至柱状图显示“数据库名称”、“数据库类型”以及“受攻击次数”。

图 8-11 受攻击数据库资产 Top5




8.2 数据流转详情

DSC对采集上报的日志进行数据链路流转分析，并绘制流转图。对采集到的日志数据进行各种指标运算，将运算结果保存起来。

查看数据流转分析

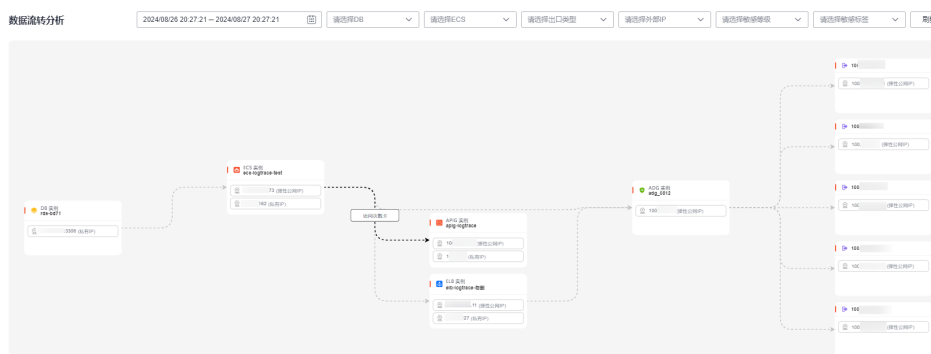
步骤1 [登录管理控制台](#)。

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“安全与合规 > 数据安全中心”。

步骤4 在左侧导航树中选择“数据安全运营 > 数据流转详情”，进入“数据流转分析”界面。

图 8-12 数据流转分析



步骤5 选择时间：单击选择需要查看的时间段。

选择DB：选择需要查看的数据库。

选择ECS：单击下拉框选择访问数据的ECS。

选择出口类型：单击下拉框选择ELB或者APIG。

选择外部IP：单击下拉框选择外部IP。

选择敏感等级：单击下拉框选择敏感等级。

选择敏感标签：单击下拉框选择敏感标签。

----结束

8.3 事件管理

数据安全中心对接数据库审计等安全组件，对各组件事件进行统一管理，会将事件实时推送到DSC，用户可以对事件进行确认和处理。也可以将告警页面的告警转事件。


前提条件

已开通DBSS服务，且DBSS中已有资产。

新建事件

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“安全与合规 > 数据安全中心”。

步骤4 在左侧导航树中选择“数据安全运营 > 事件管理”，进入“事件管理”界面。

步骤5 左上角单击“新建”，进入新建事件界面。

步骤6 根据表8-10配置新建事件相关参数。

表 8-10 新建事件参数

参数	说明
事件名称	输入字符长度只能为4-255个字符，仅允许输入中英文、数字、‘-’、‘_’，并且开头需为中文或者字母。
类型	单击下拉框选择事件类型： <ul style="list-style-type: none"> ● 数据库 <ul style="list-style-type: none"> - SQL注入 - 风险操作 ● 应用API <ul style="list-style-type: none"> - 非法访问 - 登录安全 - 接口安全 - 业务安全 - 数据安全

参数	说明
事件等级	单击下拉框选择事件等级： <ul style="list-style-type: none"> • 提示 • 低危 • 中危 • 高危 • 致命
状态	单击下拉框选择状态： <ul style="list-style-type: none"> • 开启 • 阻塞 • 关闭
来源功能模块	单击下拉框选择来源功能模块： <ul style="list-style-type: none"> • 数据库审计 • 云堡垒机 • 数据库加密网关 • 数据库运维 • API安全网关
来源实例	单击下拉框选择对应的事件来源实例。
责任人	单击下拉框选择对应事件处理责任人。
影响资产（可选）	填写该事件影响资产的信息。
发生时间	事件首次发生时间。
计划关闭事件	事件计划关闭时间。
推荐处理方法（可选）	输入推荐事件处理方法，输入不超过1000个字符。
验证状态	单击下拉框选择事件验证状态： <ul style="list-style-type: none"> • 未知 • 确认 • 误报
描述（可选）	输入事件描述。


步骤7 单击“确定”。

----结束

查看事件管理列表

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“安全与合规 > 数据安全中心”。
- 步骤4** 在左侧导航树中选择“数据安全运营 > 事件管理”，进入“事件管理”界面。
- 步骤5** 查看“未处理事件”和“事件总量”。

环状图展示“已超期”和“未超期”的事件数量。

图 8-13 事件处理情况



- 步骤6** 查看告警列表，参数如表8-11所示。

图 8-14 事件参数列表

事件名称/ID	事件等级	子类/类型	来源	状态	影响资产	验证状态	责任人	创建时间	发生时间	计划关闭时间	操作
213123	高危	风险操作	数据库审计	开启	--	未知	--	2024/03/05 09:26...	2023/12/23 16:30...	--	编辑 关闭 删除
SDP03DF0SD0	高危	登录安全	数据库连接网关	阻塞	--	确认	--	2024/03/02 11:24...	2024/02/29 15:56...	2024/03/06 15:56...	编辑 关闭 删除
2984	高危	应用API	数据库连接网关	阻塞	--	确认	--	2024/03/02 11:24...	2024/02/29 15:56...	2024/03/06 15:56...	编辑 关闭 删除

表 8-11 数据风险事件参数列表

参数名称	参数说明
事件名称/ID	<ul style="list-style-type: none"> 事件名称。事件名称包含对事件的简要描述，单击事件名称右侧弹出详情界面，界面展示事件的基本信息、事件的处置建议和关联告警等。 单击事件名称查看事件详情。
事件等级	事件等级分为五种等级： <ul style="list-style-type: none"> 提示 低危 中危 高危 致命
子类/类型	事件源类型分为： <ul style="list-style-type: none"> 数据库攻击 API攻击
来源	来源于数据库审计、数据库安全网关、API安全网关等组件以及实例名称。
状态	状态说明如下： <ul style="list-style-type: none"> 开启 阻塞 关闭

参数名称	参数说明
影响资产	影响的数据库资产或API。
验证状态	包含如下状态： <ul style="list-style-type: none">● 未知● 确认● 误报
责任人	用户名。
创建时间	事件创建时间。
发生时间	事件首次发生时间。
计划关闭事件	事件计划关闭时间。

----结束

相关操作

- 关闭
 - 单击告警列表“操作”列的“关闭”关闭该告警。
- 编辑
 - 单击告警列表“操作”列的“编辑”编辑该告警。
- 删除
 - 单击告警列表“操作”列的“删除”删除该告警。

8.4 告警管理

DBSS服务出现系统或业务告警时，会将告警实时推送到DSC，用户可以对告警进行确认和处理。


前提条件

已开通DBSS服务，且DBSS中已有资产。

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“安全与合规 > 数据安全中心”。

步骤4 在左侧导航树中选择“数据安全运营 > 告警管理”，进入“告警管理”界面。

步骤5 可查看“未处理告警”、“告警来源”、“告警总量”。

图 8-15 告警环形图



步骤6 查看告警列表，参数如表8-12所示。

表 8-12 数据风险告警参数列表

参数名称	参数说明
告警名称/ID	告警源的名称。告警名称包含对告警的简要描述，单击告警名称右侧弹出详情界面，界面展示告警的基本信息、告警的处置建议和攻击信息等。
告警等级	告警事件等级分为五种等级： <ul style="list-style-type: none"> 提示 低危 中危 高危 致命
子类/类型	告警源类型分为： <ul style="list-style-type: none"> 数据库攻击 API攻击
来源	来源于数据库审计、数据库安全网关、API安全网关等组件以及实例名称
状态	状态说明如下： <ul style="list-style-type: none"> 开启 阻塞 关闭
影响资产	影响的数据库资产或API。
验证状态	包含如下状态： <ul style="list-style-type: none"> 未知 确认 误报
责任人	用户名。
创建时间	告警创建时间。
发生时间	告警首次发生时间。

----结束

相关操作

- 转事件
 - a. 单击告警列表“操作”列的“转事件”进入“转事件”界面。
 - b. 根据如表8-13所示，填写“转事件信息”。

表 8-13 转事件信息参数

参数	说明
事件名称	输入事件名称。
事件类型	单击下拉框选择事件类型。
计划关闭时间	选择事件关闭时间。

- c. 单击“确定”，完成告警转事件，请在事件管理界面查看对应的事件。
- 关闭
单击告警列表“操作”列的“关闭”关闭该告警。
 - 编辑
单击告警列表“操作”列的“更多 > 编辑”编辑该告警。
 - 删除
单击告警列表“操作”列的“更多 > 删除”删除该告警。

8.5 OBS 使用审计

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

前提条件

- 当前异常事件处理页面含有异常事件。
- 在资产中心已开启OBS审计功能。

📖 说明


开启OBS审计后，OBS的日志记录功能进行日志的读写时将产生相应费用，费用的具体说明请参见[请求费用](#)。

- 已对OBS资产进行敏感数据识别。

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“安全与合规 > 数据安全中心”。

步骤4 在左侧导航树中选择“数据安全运营 > OBS使用审计”，进入“OBS使用审计”界面，参数说明请参考表8-14。

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。

图 8-16 数据使用审计列表

用户ID	事件类型	事件名称	告警时间	状态	操作
ca28-...a34c78709b413689	数据访问异常	对象下载	2020/09/03 16:52:23 GMT+08:00	待处理	查看详情 处理
ca28-...0709b413689	数据访问异常	对象下载	2020/09/03 16:52:18 GMT+08:00	待处理	查看详情 处理

表 8-14 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	<p>DSC将异常事件分成了三种类型：</p> <ul style="list-style-type: none"> ● 数据访问异常 <ul style="list-style-type: none"> - 敏感文件的越权操作。 - 敏感文件的下载操作。 ● 数据操作异常 <ul style="list-style-type: none"> - 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 <ul style="list-style-type: none"> - 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	<p>状态说明如下：</p> <ul style="list-style-type: none"> ● “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5 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。

图 8-17 异常事件详情

异常事件详情	
资源所有者	ce28a [redacted] 9a34c78709b413 689
时间	2020/09/03 16:52:23 GMT+08:00
事件类型	数据访问异常
事件名称	对象下载
资产类型	OBS
桶名称	obs-sdg-test-c [redacted]
错误码	--
区域	[redacted]
IP地址	10([redacted]).7
原始日志	ce28abd4fdd44e09a34c78709b413 689 obs-sd [redacted] th-1 [03/S ep/2020 [redacted]] 100.90.1 99.7 ce28abd4fdd44e09a34c78709 b41368 [redacted] ABA3F9019 44EE2A54443F REST.GET.OBJECT OBS2.txt [redacted], [redacted] test-cn-so uth-1/OBS2.txt HTTP/1.1" 200 - 5

步骤6 在异常事件的操作列，单击“处理”，处理该事件，处理方式如下：

- 确认该事件为违规事件
确认违例的事件如未被处理，数据安全中心将会一直对该事件进行异常事件告警。
- 确认事件为正常情况，无需进行处理。
异常事件设为违例排除后，数据安全中心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

8.6 水印溯源

8.6.1 数据库水印提取

前提条件

- 已完成云资源委托授权，具体请参见[云资产委托授权/停止授权](#)。
- 有已授权的RDS/DWS数据库，具体请参见[授权数据库资产](#)。
- 有已授权的MRS数据库，具体请参见[授权大数据资产](#)。
- 已进行DWS和MRS_Hive权限配置，（可选）配置DWS和MRS Hive。


约束条件

- 源文件格式必须为csv文件且大小不能超过20M。
- 表数据记录预估在1500行以上。
- csv文件内容格式为UTF8编码，请保证数据的完整性以及正确性。

新建任务

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“安全与合规 > 数据安全中心”。

步骤4 在左侧导航树中选择“数据安全运营 > 水印溯源”，进入“数据库水印提取”界面。

步骤5 单击“新建任务”，进入新建任务弹框，请根据[表8-15](#)配置相关参数。

图 8-18 新建提取任务

新建任务

* 任务名称

描述
0/1,024

源文件

提取方式

分隔符

表 8-15 新建水印提取任务

参数	说明
任务名称	请输入任务名称。
源文件	请选择本地含有水印的源文件，源文件必须为csv文件且大小不能超过20M，表数据记录预估在1500行以上，csv文件内容需为UTF8编码，请保证数据的完整性以及正确性。
提取方式	单击下拉框选择提取水印的方式，有损列嵌入以及无损列嵌入需要使用按列提取，无损行嵌入则需要使用按行提取。
分隔符	文件中的分隔符。例如","。


步骤6 单击“确定”，完成水印提取任务创建。

----结束

查看结果

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“安全与合规 > 数据安全中心”。

步骤4 在左侧导航树中选择“数据安全运营 > 水印溯源”，进入“数据库水印提取”界面。

步骤5 在目标任务“操作”列单击“查看结果”。


----结束

删除水印提取任务

执行中的提取水印任务不支持删除。

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“安全与合规 > 数据安全中心”。

步骤4 在左侧导航树中选择“数据安全运营 > 水印溯源”，进入“数据库水印提取”界面。

步骤5 在目标任务“操作”列单击“删除”，可删除该水印提取任务。也可以选择多条任务，单击列表左上角的批量删除，删除多条任务。

说明

删除操作无法恢复，请谨慎操作。

----结束

8.6.2 OBS 桶文件水印提取

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）的水印内容。

前提条件

- 已完成OBS资产委托授权，参考[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。
- 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。
- PDF文件和Word文件最大50M。
- Excel文件最大70M。
- PPT文件最大20M。

创建 OBS 桶文件水印提取任务

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。


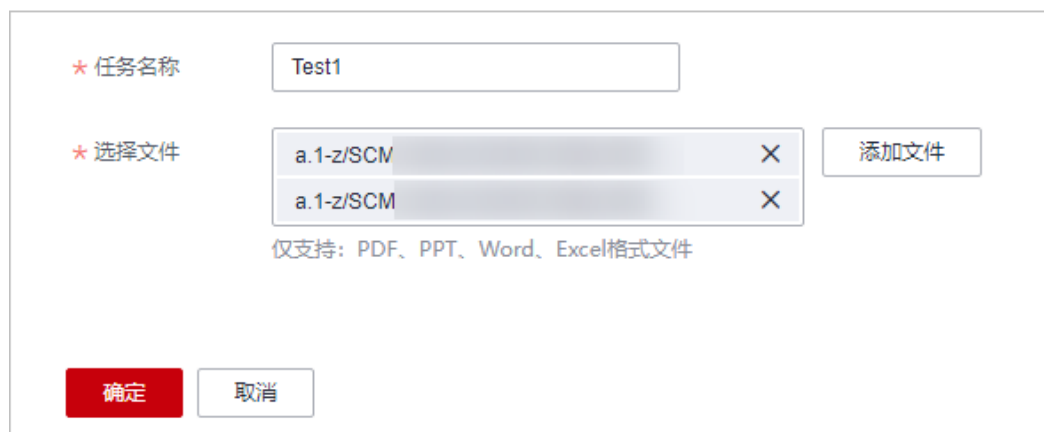
- 步骤3** 在左侧导航树中，单击 ，选择“安全与合规 > 数据安全中心”。
- 步骤4** 在左侧导航树中选择“数据安全运营 > 水印溯源”，进入“数据库水印提取”界面。
- 步骤5** 选择“OBS文件水印提取”页签。
- 步骤6** 单击左上角“新建任务”，进入“新建任务”页面。

图 8-19 新建水印提取任务

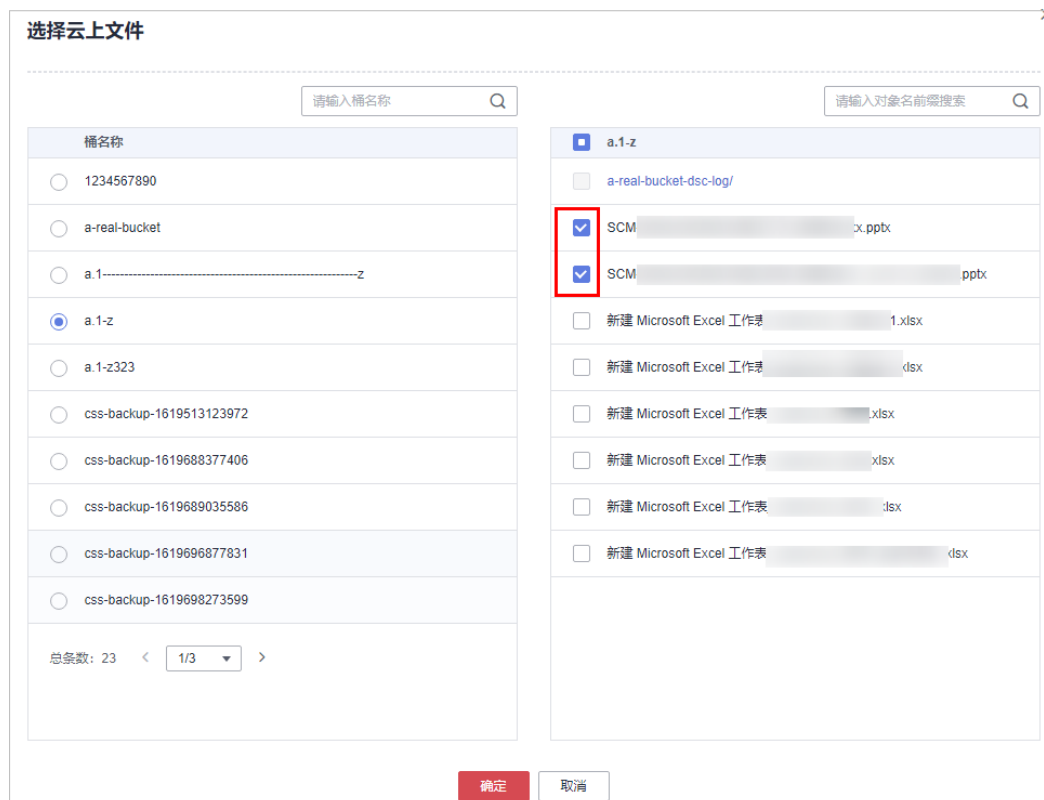


该界面用于创建新的水印提取任务。包含以下元素：

- 任务名称**：输入框中显示为“Test1”。
- 选择文件**：下方列表显示已选择两个文件，均为“a.1-z/SCM”，每个文件右侧有“X”删除按钮。
- 添加文件**：右侧有一个“添加文件”按钮。
- 支持格式**：下方提示“仅支持：PDF、PPT、Word、Excel格式文件”。
- 操作按钮**：底部有红色的“确定”按钮和白色的“取消”按钮。

- 步骤7** 单击添加文件选择需要进行提取水印的文件，OBS桶文件支持多选。

图 8-20 选择文件



该界面用于从云上文件列表中选择合适的文件进行水印提取。包含以下元素：

- 标题**：选择云上文件。
- 搜索框**：顶部左右两侧分别有“请输入桶名称”和“请输入对象名前缀搜索”的搜索框。
- 桶列表**：左侧列表显示了多个桶名称，其中“a.1-z”被选中（带有蓝色圆点）。
- 对象列表**：右侧列表显示了桶“a.1-z”下的对象，其中两个名为“SCM”的.pptx文件被选中（带有蓝色复选框，且被红色方框高亮）。
- 分页**：底部显示“总条数：23”，当前页为“1/3”。
- 操作按钮**：底部有红色的“确定”按钮和白色的“取消”按钮。

- 步骤8** 单击“确定”，提取水印任务创建完成。

步骤9 单击目标任务名称前的 \checkmark ，查看水印提取完成的OBS桶文件的暗水印内容。

图 8-21 暗水印

任务名称	状态	源桶路径	操作
新建.xlsx	运行中	--	删除
新建.xlsx	运行中	--	
新建.xlsx	已完成	--	
disc_datamap_network_asset_info_收入分为.xlsx	运行中	--	
SCM.pptx	运行失败	--	

----结束

相关操作

单击目标水印注入任务名称前的 \wedge ，查看OBS通文件水印提取任务的运行情况和状态。

- 运行中：显示提取水印任务进度。
- 已完成：暗水印列显示水印内容，没有暗水印则显示--。
- 运行失败：提取水印任务执行失败，鼠标移动至 $?$ 查看失败原因。

8.6.3 本地文件水印提取

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本地文件的水印内容。

前提条件

- 已完成OBS资产委托授权，参考[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。
- 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。
- PDF文件和Word文件最大50M。
- Excel文件最大70M。
- PPT文件最大20M。

本地文件水印提取

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“安全与合规 > 数据安全中心”。

步骤4 在左侧导航树中选择“数据安全运营 > 水印溯源”，进入“数据库水印提取”界面。

步骤5 选择“本地文件水印提取”页签。

图 8-22 水印提取页面



步骤6 单击“添加文件”，将本地需要提取暗水印的文件上传到DSC平台。

📖 说明

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

步骤7 文件上传后，单击“确定”，暗水印内容将展示到弹框中。

---结束

相关操作

单击目标水印注入任务名称前的[^]，查看OBS通文件水印提取任务的运行情况和状态。

- 运行中：显示提取水印任务进度。
- 已完成：暗水印列显示水印内容，没有暗水印则显示--。
- 运行失败：提取水印任务执行失败，鼠标移动至[?]查看失败原因。

9 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，消息通知服务为付费服务，价格详情请参见[SMN价格详情](#)。
- 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”，详细操作请参见[创建主题](#)。

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“安全与合规 > 数据安全中心”。

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，如[图9-1](#)所示，相关参数说明如[表9-1](#)所示。

说明

该告警通知为默认通知，如果未添加通知主题，数据使用审计告警将使用默认通知。

图 9-1 设置告警通知

表 9-1 告警通知参数说明

参数名称	说明	取值样例
状态	<p>是否开启通知。</p> <ul style="list-style-type: none"> ：开启状态。 ：关闭状态。 	
通知主题	<p>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。</p> <p>单击“查看通知主题”创建新主题的操作步骤如下：</p> <ol style="list-style-type: none"> 参见创建主题创建一个主题。 配置接收告警通知的手机号码、邮件地址、函数、平台应用的终端、DMS或HTTP(S)终端，即为创建的主题添加一个或多个订阅，具体操作请参见添加订阅。 确认订阅。添加订阅后，完成订阅确认。 <p>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》。</p>	-

步骤6 单击“应用”。

----结束

10 多账号管理

10.1 多账号管理概述

数据安全中心服务具备安全可靠的跨账号数据汇聚和资源访问能力，如果您的账号由组织管理，您可以对组织内所有成员账号进行统一的数据安全防护，而无需逐个登录到成员账号。

通过DSC对组织成员账号进行数据安全防护需要执行以下操作（以A账号管理B账号下的资产为例）：

1. 如果A账号是组织管理员，则跳过此步骤。如果A账号不是组织管理员，则由组织管理员将A账号添加为委托管理员，相关操作请参见[添加委托管理员](#)。

📖 说明

管理员可以添加或者取消成员的委托管理员权限，组织成员架构变动时需要1-2分钟后刷新页面才能生效。

2. 由组织管理员或委托管理员邀请B账号加入组织，相关操作请参见[邀请账号加入组织](#)。
3. B账号加入组织后，登录A账号在DSC服务“多账号管理”页面的列表中可查看B账号资产信息

有关组织的详细说明请参见《[组织用户指南](#)》。

📖 说明

为了请求B账号下的数据资产信息，DSC会自动在B账号中创建服务关联委托：

- 该委托是云服务关联委托，“身份策略”为“DSCServiceLinkedAgencyPolicy”，“服务关联委托名称”为“ServiceLinkedAgencyForDataSecurityCenter”，授权范围为“服务信任委托的创建、删除和查询，服务信任委托的创建和删除仅限于dsc_depend_agency_v5，并将身份策略(DSCServiceAgencyPolicy)绑定到该服务信任委托下”。
- 删除B账号时，DSC会自动删除B账号内的服务关联委托。

10.2 开启多账号管理功能

开启多账号管理功能后，安全管理员在安全运营账号中对所有成员账号进行统一的数据安全防护，而无需逐个登录到成员账号，本章介绍如何开启多账号管理功能。

前提条件

- 开通组织服务，请参见[开通组织服务](#)。
- 授权DSC为可信服务，请参见[授权为可信服务](#)。
- 该账号为管理员或者委托管理员，如果不是请参照[添加委托管理员](#)章节的内容。


使用约束

邀请加入该组织之后，管理员或服务委托管理员可以查看和管理该组织下成员账号的资产，单击“当前账号”下拉框切换账号，管理成员账号下的资产。

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“安全与合规 > 数据安全中心”。

步骤4 单击“多账号管理”，进入“多账号管理”界面。

步骤5 单击“开启多账号管理”，开启多账号管理功能。

---结束

10.3 查看多账号管理


前提条件

- 开通组织服务，请参见[开通组织服务](#)。
- 授权DSC为可信服务，请参见[授权为可信服务](#)。
- 该账号为管理员或者委托管理员，如果不是请参照[添加委托管理员](#)章节的内容。

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“安全与合规 > 数据安全中心”。

步骤4 单击“多账号管理”，进入“多账号管理”界面。

步骤5 进入“账号列表”界面，参数如[表10-1](#)所示。

表 10-1 账号列表

参数	说明
账号名	邀请加入该组织的账号名称，具体请参见 邀请账号加入组织 。

参数	说明
DomainId	当前账号的DomainId。
OBS资产	当前账号下的OBS资产数。
数据库资产	当前账号下的数据库资产数。
大数据资产	当前账号下的大数据资产数。
操作	单击“前往查看”，跳转至“资产中心”界面，查看和管理相关资产。

---结束

11 权限管理

11.1 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，在您的华为云账号中，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、高效的其他华为云账号或者云服务，这些账号或者云服务可以根据权限进行代运维。

如果华为云账号已经能满足您的要求，不需要创建独立的IAM用户，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11-1](#)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11-1](#)所示。

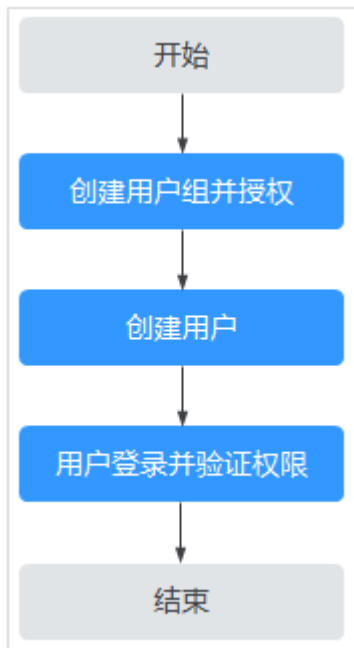
表 11-1 DSC 系统权限

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

角色名称	描述	类别	依赖关系
DSC ReadOnlyAccess	数据安全中心服务只读 权限。	系统策略	无

示例流程

图 11-1 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，如果提示权限不足，表示“DSC FullAccess”已生效。

11.2 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。

目前华为云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。

具体创建步骤请参见：[创建自定义策略](#)。本章为您介绍常用的DSC自定义策略样例。

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"
      ]
    }
  ]
}
```

```
} ]
```

11.3 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），如果华为云账号已经能满足您的要求，不需要创建独立的IAM用户，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

权限	授权项
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
DSC通用资源操作权限	dsc:common:operate
DSC通用资源查询权限	dsc:common:list

12 审计

12.1 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12-1所示。

表 12-1 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


12.2 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”，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 事件列表支持通过高级搜索来查询对应的操作事件，您可以在筛选器组合一个或多个筛选条件：

- 事件名称：输入事件的名称。
- 事件ID：输入事件ID。
- 资源名称：输入资源的名称，当该事件所涉及的云资源无资源名称或对应的API接口操作不涉及资源名称参数时，该字段为空。
- 资源ID：输入资源ID，当该资源类型无资源ID或资源创建失败时，该字段为空。
- 云服务：在下拉框中选择对应的云服务名称。
- 资源类型：在下拉框中选择对应的资源类型。
- 操作用户：在下拉框中选择一个或多个具体的操作用户。
- 事件级别：可选项为“normal”、“warning”、“incident”，只可选择其中一项。
 - normal：表示操作成功。
 - warning：表示操作失败。
 - incident：表示比操作失败更严重的情况，例如引起其他故障等。
- 企业项目ID：输入企业项目ID。
- 访问密钥ID：输入访问密钥ID（包含临时访问凭证和永久访问密钥）。
- 时间范围：可选择查询最近1小时、最近1天、最近1周的操作事件，也可以自定义最近7天内任意时间段的操作事件。

步骤6 在事件列表页面，您还可以导出操作记录文件、刷新列表、设置列表展示信息等。

- 在搜索框中输入任意关键字，按下Enter键，可以在事件列表搜索符合条件的数据。
- 单击“导出”按钮，云审计服务会将查询结果以.xlsx格式的表格文件导出，该.xlsx文件包含了本次查询结果的所有事件，且最多导出5000条信息。
- 单击  按钮，可以获取到事件操作记录的最新信息。
- 单击  按钮，可以自定义事件列表的展示信息。启用表格内容折行开关 ，可让表格内容自动折行，禁用此功能将会截断文本，默认停用此开关。

步骤7 关于事件结构的关键字段详解，请参见[事件结构](#)“云审计服务事件参考 > 事件结构”章节和[事件样例](#)“云审计服务事件参考 > 事件样例”章节。

----结束