

ALIBABA CLOUD

Alibaba Cloud

数据安全中心
用户指南

文档版本：20220118

 阿里云

法律声明

阿里云提醒您阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。
2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。
3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。
4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的“现状”、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。
5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含“阿里云”、“Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。
6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
 危险	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	 危险 重置操作将丢失用户配置数据。
 警告	该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。	 警告 重启操作将导致业务中断，恢复业务时间约十分钟。
 注意	用于警示信息、补充说明等，是用户必须了解的内容。	 注意 权重设置为0，该服务器不会再接受新请求。
 说明	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	 说明 您也可以通过按Ctrl+A选中全部文件。
>	多级菜单递进。	单击设置>网络>设置网络类型。
粗体	表示按键、菜单、页面名称等UI元素。	在结果确认页面，单击确定。
Courier字体	命令或代码。	执行 <code>cd /d C:/window</code> 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	<code>bae log list --instanceid</code> <i>Instance_ID</i>
[] 或者 [a b]	表示可选项，至多选择一个。	<code>ipconfig [-all -t]</code>
{ } 或者 {a b}	表示必选项，至多选择一个。	<code>switch {active stand}</code>

目录

1.授权DSC访问云资源	05
2.控制台概览	06
3.数据资产支持的授权方式	10
4.数据资产授权	11
5.敏感数据发现	27
5.1. 查看敏感数据资产	27
5.2. 导出敏感数据资产	33
5.3. 搜索敏感数据	34
5.4. 识别任务监控	35
5.5. 管理识别模型	36
6.数据脱敏	41
6.1. 静态脱敏	41
6.2. 动态脱敏	48
6.3. 脱敏模板	49
6.4. 脱敏算法	51
6.5. 提取水印	56

1. 授权DSC访问云资源

使用数据安全中心DSC（Data Security Center）服务前，您需要先完成允许DSC访问云资源的授权。本文档介绍如何进行云资源授权。

前提条件

您已购买DSC实例。

背景信息

您购买DSC实例后，首次登录DSC控制台时，概览页面会提示您执行云资源授权的流程。完成授权后，您的DSC实例才能访问OSS、RDS、MaxCompute等云服务的资源，并对这些云资源进行敏感数据扫描和分析等操作。

操作步骤

1. 登录[数据安全中心控制台](#)。
2. 在Welcome页面，单击立即授权。

当您单击立即授权后，阿里云将自动为您创建DSC服务关联角色AliyunServiceRoleForSDDP。您可以在[RAM控制台](#)的角色页面查看系统为您自动创建的服务关联角色。您也可以使用API、CLI调用ListRoles，在返回结果中查看DSC服务的关联角色。更多信息，请参见[服务关联角色](#)。

完成授权DSC访问云资源操作后，您需要进行资产保护授权才能进行敏感数据扫描和分析等操作。具体操作，请参见[数据资产授权](#)。

DSC服务关联角色介绍

角色名称：AliyunServiceRoleForSDDP

角色权限策略：AliyunServiceRolePolicyForSDDP

删除服务关联角色

当您不再需要使用DSC服务时，可以删除DSC的服务关联角色。您可以登录[RAM控制台](#)删除AliyunServiceRoleForSDDP角色，具体操作，请参见[服务关联角色](#)。

相关说明

首次使用DSC需要进行的云资源授权，与DSC提供的资产保护授权功能，是两个不同的操作。云资源授权是允许DSC访问其他提供数据服务的云产品，资产保护授权功能是允许DSC访问具体的云产品中存有数据的部分空间或项目。完成授权DSC访问云资源操作后，您需要进行资产保护授权才能进行敏感数据扫描和分析等操作。具体操作，请参见[数据资产授权](#)。

2.控制台概览

开通并设置敏感级别和识别规则后，您可在概览页面查看资产的数据保护授权状态、数据识别结果、静态脱敏结果和异常事件汇总信息。

目前DSC支持检测MaxCompute、RDS、OSS、表格存储、自建ECS数据库、DRDS、PolarDB中的敏感数据。

说明 为保护您的隐私，DSC仅对数据执行必要的敏感数据处理（例如：打标、静态脱敏），不会保存您的数据文件。

查看数据保护授权状态

在数据保护授权区域查看数据资产的授权状态，包括已接入DSC的数据资产占比、数据资产的库总量、未接入和已接入DSC的数据资产数量、DSC扫描数据资产的总次数、DSC已完成扫描授权的数据资产总表数。

单击各产品区域的去授权进入云上托管页面，添加资产授权项目，并查看、编辑、删除已授权资产项目。更多信息，请参见[数据资产授权](#)。



查看按量计费使用情况

在按量计费使用情况区域，查看今天、本周、本月或本年内DSC对结构化数据、非结构化数据的扫描量，及脱敏数据量。

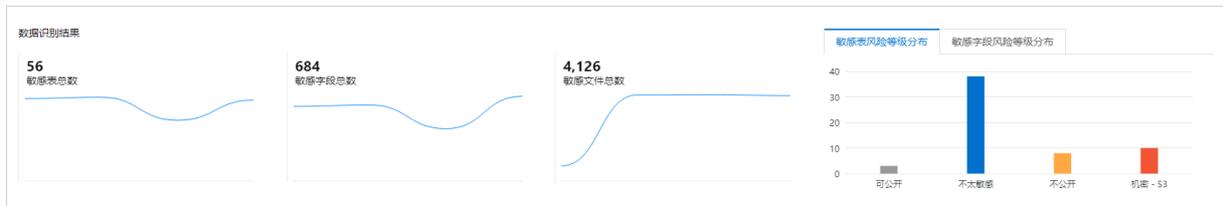
- 说明**
- 结构化数据来源于MaxCompute、RDS、OSS、表格存储、自建ECS数据库、DRDS、PolarDB，非结构化数据主要包含OSS。
 - 脱敏数据量计费单位是单元格。
 - 此处统计信息可能存在延迟，仅供参考，最终计费以实际账单为准。



单击账单详情可跳转到阿里云用户中心的费用账单页面查看具体的账单信息。

查看敏感数据识别统计

在数据识别结果区域查看已完成扫描的数据资产中敏感表、字段、文件的统计数据。



DSC根据已配置的敏感数据识别规则识别需要关注的敏感文件和敏感数据。敏感数据规则分为系统默认规则和用户自定义规则两种，DSC会根据敏感数据规则对敏感数据表、字段、文件进行识别和敏感等级分类。更多信息，请参见[管理识别模型](#)。

数据识别结果包括以下信息：

- **敏感表总数**：数据资产中敏感级别的数据表的总数量。数据资产是指MaxCompute、RDS、表格存储、自建ECS数据库、DRDS、PolarDB。
- **敏感字段总数**：数据资产中敏感级别的数据字段的总数量。数据字段来源于MaxCompute、RDS、表格存储、自建ECS数据库、DRDS、PolarDB的数据表。
- **敏感文件总数**：OSS数据中敏感文件的总数量。
- **敏感表及或敏感字段风险等级分布**：您可在数据识别结果区域查看数据资产中不同风险等级的敏感表及其敏感字段的分布情况，包括每类风险等级对应的敏感表和敏感字段数量。

DSC基于敏感字段在识别规则中的设置，将敏感字段划分为3个风险等级（S1、S2、S3）。S1~S3风险等级对应的危害程度依次递增，具体如下：

- S1：低风险等级。
- S2：中风险等级。
- S3：高风险等级。

查看静态脱敏数据统计

在静态脱敏结果区域查看根据脱敏算法进行脱敏的敏感表总数、脱敏表总数和脱敏字段总数，及配置静态脱敏的表占有所有敏感表的比例。

DSC支持创建静态脱敏任务对您项目中的敏感数据进行脱敏和保护。更多信息，请参见[静态脱敏](#)。



查看异常事件统计数据 and 风险趋势

在异常事件汇总区域查看最近7天、1个月、6个月或12个月内的异常事件风险趋势。



异常事件统计信息如下：

- **未处理异常事件数：**未处理的数据异常事件的数量。
DSC可识别出敏感数据读取和使用上的异常事件，包括权限使用异常、数据流转异常和数据操作异常。DSC会根据异常告警配置的规则对异常事件进行识别和告警。
- **已处理异常事件数：**已处理的数据异常事件的数量。
DSC可对异常事件处理结果进行核查，包括确认该异常事件已处理或标记为误报。

数据资产搜索

单击概览页面右上角的数据资产搜索，搜索和查看DSC检测出的数据资产的敏感数据项及其敏感数据风险等级情况。

数据资产搜索支持以下筛选条件：

- **搜索覆盖风险等级：**可选择单个或多个风险等级进行搜索。不选择任何风险等级表示查看所有风险等级的资产。

 说明 N/A表示未知风险等级。

- **搜索覆盖资产范围：**可选择单个或多个数据资产进行搜索，包括MaxCompute项目、MaxCompute表等数据源。
- **含敏感数据：**从下拉列表中选择需要搜索的包含指定敏感数据信息的资产。

 说明 此处展示的敏感数据信息是从敏感数据识别 > 识别规则中的规则名称同步而来，包含了系统内置的敏感数据规则和您自定义的敏感数据规则。

- **资产名称：**输入资产的文件、表、包、项目、实例或库名称进行搜索。

3.数据资产支持的授权方式

本文介绍数据安全中心支持的授权类型。

数据资产支持的授权方式有一键授权、账号密码授权两种方式。

- 一键授权是指您无需输入账号、密码，可通过控制台按钮一键进行数据资产授权的方式。授权过程中数据安全中心会自动针对资产生成只读账号，该账号无脱敏权限。
- 账号密码授权是指您可输入账号、密码，进行数据资产授权。资产授权后，可对资产进行敏感数据识别、脱敏和审计。识别出资产敏感数据后，可选择敏感数据进行脱敏。

数据类型	一键授权（无需输入密码）	数据库账号与密码授权
RDS-SQL Server	支持	支持
RDS-PostgreSQL	支持	支持
RDS-PPAS	支持	支持
RDS-MariaDB	支持	支持
DRDS	支持	支持
分析型数据库MySQL版	不支持	支持
分析型数据库PostgreSQL版	不支持	支持
MaxCompute	不支持	支持
OSS	支持	支持
PolarDB-X（原DRDS）	不支持	支持
PolarDB MySQL	不支持	支持
PolarDB PostgreSQL版	不支持	支持
ECS自建数据库 MySQL	不支持	支持
OceanBase MySQL	不支持	支持
OceanBase Oracle	不支持	支持
云数据库MongoDB版	不支持	支持

4.数据资产授权

数据安全中心DSC（Data Security Center）在检测数据源（OSS、RDS、RDS-PPAS、DRDS、PolarDB、表格存储OTS、ECS自建数据库、MaxCompute、ADB-PG、ADB-MYSQL、MongoDB、OceanBase、Redis）中存储的敏感数据之前，需要首先获取允许访问这几类云产品中指定数据的授权。本文介绍数据资产授权的操作步骤。

前提条件

已购买DSC服务并完成DSC访问云服务的授权。更多信息，请参见[授权DSC访问云资源](#)。

背景信息

资产保护授权功能允许DSC访问具体的云产品中存有数据的部分空间或项目。如果不授权，DSC将无法对云产品中的敏感数据进行识别和脱敏。

OSS文件桶访问授权

1. 登录[数据安全中心控制台](#)。
2. 在左侧导航栏，选择[数据保护授权](#) > [数据资产授权](#)。
3. 在OSS页签下，单击[未授权](#)。
4. 选中需要授权的OSS文件桶（Bucket）并单击[批量操作](#)。



您也可以单击某个OSS文件桶（Bucket）开启防护列下的授权，为该Bucket开启授权。

5. 在对于选中资产批量处理对话框，设置识别权限、审计权限、脱敏权限等参数。



设置说明如下：

- **识别权限**：开启或关闭DSC识别选中资产敏感数据的权限。

- **审计权限**：开启或关闭DSC对选中资产进行数据审计的权限。
- **脱敏权限**：开启或关闭DSC对选中资产进行敏感数据脱敏的权限。
- **敏感数据采样**：设置DSC对选中资产进行敏感数据采样的条数。敏感数据采样是指DSC自动识别到敏感数据后，保留的敏感数据样本。您可以通过保留的敏感数据样本，人工对敏感数据进行更深入的判断。可选取值：
 - 0条
 - 5条
 - 10条
- **审计日志存档**：设置选中资产的审计日志保存时间。可选取值：
 - 30天
 - 90天
 - 180天

 **说明** 设置审计日志存档时间无需您额外开通日志服务。

6. 单击**确认**。

完成资产授权后，DSC将会对开启授权的OSS存储空间中的文件执行敏感数据检测。如果该存储空间是首次开启授权，DSC将会自动触发全量扫描并收取全量数据扫描的费用。更多信息，请参见[数据源授权完成后需要多长时间完成扫描](#)。

已授权资产中的数据可进行编辑或取消授权。取消授权后，DSC不会检测该文件桶中的数据。

 **说明** DSC仅对已授权的Bucket进行数据扫描和风险分析。

RDS库访问授权

1. 登录[数据安全中心控制台](#)。
2. 在左侧导航栏，选择[数据保护授权](#) > [数据资产授权](#)。
3. 在云上托管页面，单击RDS页签。
4. 在RDS页签下，单击**未授权**。
5. 定位到需要授权的实例，在**用户名和密码**文本框输入连接数据库的用户名和密码。

您可以使用DSC提供的**批量密码导入**功能，批量导入数据库的用户名和密码。更多信息，请参见[批量密码导入](#)。

 **注意** 用户名和密码错误将会导致授权失败，请您输入正确的用户名和密码。

6. 选中需要授权的资产并单击**批量操作**。
您也可以单击某个实例**操作**列下的**授权**为该实例授权。
7. 在授权页面，设置识别权限、审计权限、脱敏权限等参数。

设置说明如下：

- **识别权限**：开启或关闭DSC识别选中资产敏感数据的权限。
- **审计权限**：开启或关闭DSC对选中资产中进行数据审计的权限。

审计日志数据包括审计规则命中结果、审计规则检测的资产类型、命中规则的操作类型和操作账号等信息，覆盖资产数据产生、更新和使用等全链路的日志数据。

 **说明** 开通RDS审计日志会自动开启RDS SQL洞察功能，开启该功能将额外产生SQL洞察费用。非试用版按小时扣费，USD 0.0018/GB/小时。该费用将体现在您的RDS账单中，查看该费用的具体方法，请参见[查看消费明细](#)。SQL洞察更多信息，请参见[SQL洞察](#)。

- **脱敏权限**：开启或关闭DSC对选中资产进行敏感数据脱敏的权限。
- **敏感数据采样**：设置DSC对选中资产进行敏感数据采样的条数。敏感数据采样是指DSC自动识别到敏感数据后，保留的敏感数据样本。您可以通过保留的敏感数据样本，人工对敏感数据进行更深入的判断。可选取值：
 - 0条
 - 5条
 - 10条
- **审计日志存档**：设置选中资产的审计日志保存时间。可选取值：
 - 30天
 - 90天
 - 180天

 **说明** 设置审计日志存档时间无需您额外开通日志服务。

8. 单击**确定**。

 **说明** 若授权未通过，请检查输入的用户名和密码是否正确。

授权完成后，DSC会检测该资产中的数据。

已授权的资产可编辑或取消授权。仅支持编辑该RDS数据库合法用户的用户名和密码。取消授权后，DSC不会检测该数据库中的数据。

RDS-PPAS访问授权

1. 登录[数据安全中心控制台](#)。
2. 在左侧导航栏，选择[数据保护授权](#) > [数据资产授权](#)。
3. 在云上托管页面，单击[RDS-PPAS](#)页签。
4. 在[RDS-PPAS](#)页签下，单击[添加数据资产](#)。
5. 在[添加数据资产](#)对话框中，配置相应参数并单击**下一步**。

您可以参考以下表格中的参数说明配置相应参数。

参数	说明
所在区域	选择您需要授权DSC访问的RDS-PPAS库的所在地域。
实例名称	选择您需要授权DSC访问的RDS-PPAS库所在的ECS实例名称。
数据库名称	输入您需要授权DSC访问的RDS-PPAS库名称。

参数	说明
用户名	输入可以访问RDS-PPAS库合法用户的用户名和密码。
密码	

- 在授权页面，设置识别、审计、脱敏等权限。
- 单击**确定**。
授权完成后，DSC会检测该资产中的敏感数据。

DRDS访问授权

- 登录[数据安全中心控制台](#)。
- 在左侧导航栏，选择[数据保护授权](#) > [数据资产授权](#)。
- 在云上托管页面，单击[DRDS](#)页签。
- 在[DRDS](#)页签下，单击[未授权](#)。
- 定位到需要授权的实例，在[用户名和密码](#)文本框输入连接数据库的用户名和密码。

您可以使用DSC提供的[批量密码导入](#)功能，批量导入数据库的用户名和密码。更多信息，请参见[批量密码导入](#)。

 **注意** 用户名和密码错误将会导致授权失败，请您输入正确的用户名和密码。

- 选中需要授权的资产并单击**批量操作**。
您也可以单击某个实例**操作**列下的**授权**为该实例授权。
- 在授权页面，设置识别、审计、脱敏等权限。
设置说明如下：
 - 识别权限：开启或关闭DSC识别选中资产敏感数据的权限。
 - 审计权限：开启或关闭DSC对选中资产进行数据审计的权限。
 - 脱敏权限：开启或关闭DSC对选中资产进行敏感数据脱敏的权限。
 - 敏感数据采样：设置DSC对选中资产进行敏感数据采样的条数。敏感数据采样是指DSC自动识别到敏感数据后，保留的敏感数据样本。您可以通过保留的敏感数据样本，人工对敏感数据进行更深入的判断。可选取值：
 - 0条
 - 5条
 - 10条
 - 审计日志存档：设置选中资产的审计日志保存时间。可选取值：
 - 30天
 - 90天
 - 180天

 **说明** 设置审计日志存档时间无需您额外开通日志服务。

- 单击**确定**。

 **说明** 若授权未通过，请检查输入的用户名和密码是否正确。

授权完成后，DSC会检测该资产中的数据。

已授权的资产可编辑或取消授权。仅支持编辑该DRDS数据库合法用户的用户名和密码。取消授权后，DSC不会检测该数据库中的数据。

PolarDB访问授权

1. 登录[数据安全中心控制台](#)。
2. 在左侧导航栏，选择[数据保护授权](#) > [数据资产授权](#)。
3. 在云上托管页面，单击PolarDB页签。
4. 在PolarDB页签下，单击未授权。
5. 定位到需要授权的实例，在用户名和密码文本框输入连接数据库的用户名和密码。

您可以使用DSC提供的[批量密码导入](#)功能，批量导入数据库的用户名和密码。更多信息，请参见[批量密码导入](#)。

 **注意** 用户名和密码错误将会导致授权失败，请您输入正确的用户名和密码。

6. 选中需要授权的资产并单击**批量操作**。
您也可以单击某个实例操作列下的**授权**为该实例授权。
7. 在授权页面，设置识别、审计、脱敏等权限。
设置说明如下：
 - **识别权限**：开启或关闭DSC识别选中资产敏感数据的权限。
 - **审计权限**：开启或关闭DSC对选中资产进行数据审计的权限。
 - **脱敏权限**：开启或关闭DSC对选中资产进行敏感数据脱敏的权限。
 - **敏感数据采样**：设置DSC对选中资产进行敏感数据采样的条数。敏感数据采样是指DSC自动识别到敏感数据后，保留的敏感数据样本。您可以通过保留的敏感数据样本，人工对敏感数据进行更深入的判断。可取值：
 - 0条
 - 5条
 - 10条
 - **审计日志存档**：设置选中资产的审计日志保存时间。可取值：
 - 30天
 - 90天
 - 180天

 **说明** 设置审计日志存档时间无需您额外开通日志服务。

8. 单击**确定**。

 **说明** 若授权未通过，请检查输入的用户名和密码是否正确。

授权完成后，DSC会检测该资产中的数据。

已授权的资产可编辑或取消授权。仅支持编辑该PolarDB数据库合法用户的用户名和密码。取消授权后，DSC不会检测该数据库中的数据。

OTS访问授权

OTS即表格存储服务。

1. 登录[数据安全中心控制台](#)。
2. 在左侧导航栏，选择[数据保护授权](#) > [数据资产授权](#)。
3. 在云上托管页面，单击OTS页签。
4. 在OTS页签下，单击未授权。
5. 选中需要授权的资产并单击**批量操作**。

您也可以单击某个实例操作列下的**授权**为该实例授权。

6. 在授权页面，设置识别、审计、脱敏等权限。

设置说明如下：

- **识别权限**：开启或关闭DSC识别选中资产敏感数据的权限。
- **审计权限**：开启或关闭DSC对选中资产进行数据审计的权限。
- **脱敏权限**：开启或关闭DSC对选中资产进行敏感数据脱敏的权限。
- **敏感数据采样**：设置DSC对选中资产进行敏感数据采样的条数。敏感数据采样是指DSC自动识别到敏感数据后，保留的敏感数据样本。您可以通过保留的敏感数据样本，人工对敏感数据进行更深入的判断。可选取值：
 - 0条
 - 5条
 - 10条
- **审计日志存档**：设置选中资产的审计日志保存时间。可选取值：
 - 30天
 - 90天
 - 180天

 **说明** 设置审计日志存档时间无需您额外开通日志服务。

7. 单击**确定**。
授权完成后，DSC会检测该资产中的敏感数据。

ECS自建数据库访问授权

DSC支持检测的ECS自建数据库有以下限制：

- 仅VPC网络中的ECS自建数据库支持使用DSC服务。
- 目前仅支持MySQL、SQL Server、PostgreSQL和Oracle类型的ECS自建数据库。
- ECS自建数据库资产在数据安全中心进行授权之前，需要在自建数据库内，授予待授权用户指定IP段的远程访问权限。

1. 登录数据库，授予待授权用户指定IP段的远程访问权限。

以下以MySQL类型的ECS自建数据库命令为例，进行操作说明。其他类型ECS自建数据库，请执行对应的授权命令。

```
GRANT ALL PRIVILEGES ON *.* TO '用户'@'IP段' IDENTIFIED BY '密码'
```

命令中参数说明如下所示：

- 用户：待授权的ECS自建数据库用户名。
- IP段：待授权的ECS自建数据库IP段。

授权命令中IP段与地域、用户资产所使用的网络有关。用户需要根据资产所在地域和所选择的网络类型，授权对应的IP段。

IP段的具体说明，请参见[IP段说明](#)。授权命令中至少要设置地域对应的两个IP段，IP范围也可大于地域对应的两个IP段。

- 密码：待授权用户的密码。

IP段说明

地域	IP段
华东 2（上海）	<ul style="list-style-type: none"> ○ 100.104.238.64/26 ○ 100.104.198.192/26
华北 2（北京）	<ul style="list-style-type: none"> ○ 100.104.250.0/26 ○ 100.104.51.192/26
华东 1（杭州）	<ul style="list-style-type: none"> ○ 100.104.207.192/26 ○ 100.104.232.64/26
华南 1（深圳）	<ul style="list-style-type: none"> ○ 100.104.247.0/26 ○ 100.104.150.64/26
华北 3（张家口）	<ul style="list-style-type: none"> ○ 100.104.37.128/26 ○ 100.104.191.64/26
华北 5（呼和浩特）	<ul style="list-style-type: none"> ○ 100.104.234.192/26 ○ 100.104.26.128/26
中国香港	<ul style="list-style-type: none"> ○ 100.104.153.64/26 ○ 100.104.65.192/26
亚太东南 1（新加坡）	<ul style="list-style-type: none"> ○ 100.104.158.192/26 ○ 100.104.218.128/26

地域	IP段
马来西亚（吉隆坡）	<ul style="list-style-type: none"> ◦ 100.104.240.128/26 ◦ 100.104.127.0/26
印度尼西亚（雅加达）	<ul style="list-style-type: none"> ◦ 100.104.127.0/26 ◦ 100.104.182.128/26

2. 登录[数据安全中心控制台](#)。
3. 在左侧导航栏，选择[数据保护授权](#) > [数据资产授权](#)。
4. 在云上托管页面，单击ECS自建数据库页签。
5. 在ECS自建数据库页签，单击[添加数据资产](#)。
6. 在资产授权对话框，配置相应参数并单击下一步。

您可以参考以下表格中的参数说明配置相应参数。

参数	说明
区域	选择您需要授权DSC访问的ECS自建数据库的所在地域。
ECS实例ID	选择您需要授权DSC访问的ECS自建数据库所在的ECS实例ID。
数据库类型	选择您需要授权DSC访问的ECS自建数据库的类型。目前DSC仅支持MySQL和SQL Server两种类型的ECS自建数据库。
库名称	输入您需要授权DSC访问的ECS自建数据库名称。 <div style="border: 1px solid #ccc; background-color: #e6f2ff; padding: 5px; margin-top: 10px;"> ? 说明 如果当前ECS实例下还有其他ECS自建数据库需要授权DSC访问，您可以单击添加数据库，填写其他ECS自建数据库的信息。 </div>
端口	填写访问ECS自建数据库使用的端口号。
用户名	输入可以访问ECS自建数据库合法用户的用户名和密码。
密码	

7. 在授权页面，设置识别、审计、脱敏等权限。

设置说明如下：

- **识别权限**：开启或关闭DSC识别选中资产敏感数据的权限。
- **审计权限**：开启或关闭DSC对选中资产进行数据审计的权限。
- **脱敏权限**：开启或关闭DSC对选中资产进行敏感数据脱敏的权限。
- **敏感数据采样**：设置DSC对选中资产进行敏感数据采样的条数。敏感数据采样是指DSC自动识别到敏感数据后，保留的敏感数据样本。您可以通过保留的敏感数据样本，人工对敏感数据进行更深入的判断。可取值：
 - 0条

- 5条
- 10条
- 审计日志存档：设置选中资产的审计日志保存时间。可选取值：
 - 30天
 - 90天
 - 180天

 **说明** 设置审计日志存档时间无需您额外开通日志服务。

8. 单击**确定**。
授权完成后，DSC会检测该资产中的敏感数据。

MaxCompute项目访问授权

1. 登录[数据安全中心控制台](#)。
2. 在左侧导航栏，选择[数据保护授权](#) > [数据资产授权](#)。
3. 在云上托管页面，单击MaxCompute页签。
4. 在MaxCompute页签下，单击添加数据资产。
5. 在添加数据资产页面，设置授权参数（详见下表）。

参数	说明
区域	选择您需要授权DSC访问的MaxCompute项目的所在地域。
项目名称	输入MaxCompute项目名称。  说明 项目名称不支持模糊查询，请输入准确的名称。

6. 在MaxCompute客户端执行以下命令，将DSC数据访问子账号yundun_sddp添加到该MaxCompute项目中。

```
add user aliyun$yundun_sddp;
grant admin to aliyun$yundun_sddp;
```

您可以根据以下说明判断接下来执行的步骤。

- 如果此步骤执行后无报错提示，请直接跳转至[步骤8](#)。
 - 如果此步骤执行后提示添加失败，请执行[步骤7](#)。
7. （可选）执行以下命令将DSC服务IP地址添加到MaxCompute IP白名单中。

```
setproject odps.security.ip.whitelist=11.193.236.0/24,11.193.64.0/24,11.193.58.0/24 odp
s.security.vpc.whitelist=<VPC网段ID>;
//11.193.236.0/24,11.193.64.0/24,11.193.58.0/24是DSC服务使用的经典网络IP段，必须配置；
//VPC网段ID需要替换为您的MaxCompute项目所在地域的VPC网段ID。地域和VPC网段ID的对应关系详见以下表格。
```

如果您已开启了MaxCompute IP白名单限制，为了避免资产授权失败，您需要执行本步骤将DSC服务IP地址添加到MaxCompute IP白名单中。您可以执行 `setproject;` 命令，查询是否已开启MaxCompute IP白名单。如果 `odps.security.vpc.whitelist=` 等号后面的内容为空，表示未开启白名单，则您可以跳过本步骤。

地域	地域ID	VPC网段ID
华北 3 (张家口)	cn-zhangjiakou	cn-zhangjiakou_399229
华北 2 (北京)	cn-beijing	cn-beijing_691047
华南 1 (深圳)	cn-shenzhen	cn-shenzhen_515895
华东 2 (上海)	cn-shanghai	cn-shanghai_28803
华东 1 (杭州)	cn-hangzhou	cn-hangzhou_551733

 **说明** 设置IP白名单后，您需要等待5分钟再进行授权。

8. 单击**确认**。

 **说明** 若授权未通过，请检查授权参数是否有误或DSC访问子账号是否添加成功。

授权完成后，DSC会对该项目列表中的所有数据进行检测。

资产完成授权后可取消授权。取消授权后，DSC不会检测该资产中的数据。

ADB-PG库访问授权

1. 登录[数据安全中心控制台](#)。
2. 在左侧导航栏，选择**数据保护授权 > 数据资产授权**。
3. 在云上托管页面，单击**ADB-PG**页签。
4. 在**ADB-PG**页签下，单击**添加数据资产**。
5. 在**添加数据资产**对话框中，配置相应参数并单击**下一步**。

您可以参考以下表格中的参数说明配置相应参数。

参数	说明
所在区域	选择您需要授权DSC访问的ADB-PG库的所在地域。
实例名称	选择您需要授权DSC访问的ADB-PG库所在的ECS实例名称。
数据库名称	输入您需要授权DSC访问的ADB-PG库名称。
用户名	输入可以访问ADB-PG库合法用户的用户名和密码。
密码	

6. 在授权页面，设置**识别、审计、脱敏**等权限。

设置说明如下：

- **识别权限**：开启或关闭DSC识别选中资产敏感数据的权限。
- **审计权限**：开启或关闭DSC对选中资产进行数据审计的权限。
- **脱敏权限**：开启或关闭DSC对选中资产进行敏感数据脱敏的权限。
- **敏感数据采样**：设置DSC对选中资产进行敏感数据采样的条数。敏感数据采样是指DSC自动识别到敏感数据后，保留的敏感数据样本。您可以通过保留的敏感数据样本，人工对敏感数据进行更深入的判断。可选取值：
 - 0条
 - 5条
 - 10条
- **审计日志存档**：设置选中资产的审计日志保存时间。可选取值：
 - 30天
 - 90天
 - 180天

 **说明** 设置审计日志存档时间无需您额外开通日志服务。

7. 单击**确定**。
授权完成后，DSC会检测该资产中的敏感数据。

ADB-MYSQL访问授权

1. 登录[数据安全中心控制台](#)。
2. 在左侧导航栏，选择**数据保护授权 > 数据资产授权**。
3. 在云上托管页面，单击**ADB-MYSQL**页签。
4. 在**ADB-MYSQL**页签下，单击**未授权**。
5. 定位到需要授权的实例，在**用户名和密码**文本框输入连接数据库的用户名和密码。

您可以使用DSC提供的**批量密码导入**功能，批量导入数据库的用户名和密码。更多信息，请参见[批量密码导入](#)。

 **注意** 用户名和密码错误将会导致授权失败，请您输入正确的用户名和密码。

6. 选中需要授权的资产并单击**批量操作**。
您也可以单击某个实例**操作**列下的**授权**为该实例授权。
7. 在授权页面，设置识别、审计、脱敏等权限。
设置说明如下：
 - **识别权限**：开启或关闭DSC识别选中资产敏感数据的权限。
 - **审计权限**：开启或关闭DSC对选中资产进行数据审计的权限。
 - **脱敏权限**：开启或关闭DSC对选中资产进行敏感数据脱敏的权限。
 - **敏感数据采样**：设置DSC对选中资产进行敏感数据采样的条数。敏感数据采样是指DSC自动识别到敏感数据后，保留的敏感数据样本。您可以通过保留的敏感数据样本，人工对敏感数据进行更深入的判断。可选取值：
 - 0条

- 5条
- 10条
- 审计日志存档：设置选中资产的审计日志保存时间。可选取值：
 - 30天
 - 90天
 - 180天

 **说明** 设置审计日志存档时间无需您额外开通日志服务。

8. 单击**确定**。

 **说明** 若授权未通过，请检查输入的用户名和密码是否正确。

授权完成后，DSC会检测该资产中的数据。

已授权的资产可编辑或取消授权。仅支持编辑该ADB-MYSQL数据库合法用户的用户名和密码。取消授权后，DSC不会检测该数据库中的数据。

MongoDB访问授权

1. 登录[数据安全中心控制台](#)。
2. 在左侧导航栏，选择**数据保护授权 > 数据资产授权**。
3. 在云上托管页面，单击**MongoDB**页签。
4. 在**MongoDB**页签下，单击**添加数据资产**。
5. 在**添加数据资产**对话框中，配置相应参数并单击**下一步**。

您可以参考以下表格中的参数说明配置相应参数。

参数	说明
所在区域	选择您需要授权DSC访问的MongoDB的所在地域。
实例名称	选择您需要授权DSC访问的MongoDB所在的ECS实例名称。
数据库名称	输入您需要授权DSC访问的MongoDB名称。
用户名	输入可以访问MongoDB合法用户的用户名和密码。
密码	

6. 在授权页面，设置识别、审计、脱敏等权限。

设置说明如下：

- **识别权限**：开启或关闭DSC识别选中资产敏感数据的权限。
- **审计权限**：开启或关闭DSC对选中资产进行数据审计的权限。
- **脱敏权限**：开启或关闭DSC对选中资产进行敏感数据脱敏的权限。
- **敏感数据采样**：设置DSC对选中资产进行敏感数据采样的条数。敏感数据采样是指DSC自动识别到敏感数据后，保留的敏感数据样本。您可以通过保留的敏感数据样本，人工对敏感数据进行更深入的判

断。可选取值：

- 0条
- 5条
- 10条

○ 审计日志存档：设置选中资产的审计日志保存时间。可选取值：

- 30天
- 90天
- 180天

 说明 设置审计日志存档时间无需您额外开通日志服务。

7. 单击**确定**。

授权完成后，DSC会检测该资产中的敏感数据。

OceanBase访问授权

1. 登录[数据安全中心控制台](#)。

2. 在左侧导航栏，选择[数据保护授权](#) > [数据资产授权](#)。

3. 在云上托管页面，单击OceanBase页签。

4. 在OceanBase页签下，单击**未授权**。

5. 定位到需要授权的实例，在**用户名和密码**文本框输入连接数据库的用户名和密码。

您可以使用DSC提供的**批量密码导入**功能，批量导入数据库的用户名和密码。更多信息，请参见[批量密码导入](#)。

 注意 用户名和密码错误将会导致授权失败，请您输入正确的用户名和密码。

6. 选中需要授权的资产并单击**批量操作**。

您也可以单击某个实例**操作**列下的**授权**为该实例授权。

7. 在授权页面，设置识别、审计、脱敏等权限。

设置说明如下：

- **识别权限**：开启或关闭DSC识别选中资产敏感数据的权限。
- **审计权限**：开启或关闭DSC对选中资产进行数据审计的权限。
- **脱敏权限**：开启或关闭DSC对选中资产进行敏感数据脱敏的权限。
- **敏感数据采样**：设置DSC对选中资产进行敏感数据采样的条数。敏感数据采样是指DSC自动识别到敏感数据后，保留的敏感数据样本。您可以通过保留的敏感数据样本，人工对敏感数据进行更深入的判断。可选取值：
 - 0条
 - 5条
 - 10条
- **审计日志存档**：设置选中资产的审计日志保存时间。可选取值：
 - 30天

- 90天
- 180天

 **说明** 设置审计日志存档时间无需您额外开通日志服务。

8. 单击**确定**。

 **说明** 若授权未通过，请检查输入的用户名和密码是否正确。

授权完成后，DSC会检测该资产中的数据。

已授权的资产可编辑或取消授权。仅支持编辑该OceanBase数据库合法用户的用户名和密码。取消授权后，DSC不会检测该数据库中的数据。

Redis访问授权

Redis

1. 登录[数据安全中心控制台](#)。
2. 在左侧导航栏，选择[数据保护授权](#) > [数据资产授权](#)。
3. 在云上托管页面，单击Redis页签。
4. 在Redis页签下，单击**未授权**。
5. 定位到需要授权的实例，在**用户名和密码**文本框输入连接数据库的用户名和密码。

您可以使用DSC提供的**批量密码导入**功能，批量导入数据库的用户名和密码。更多信息，请参见[批量密码导入](#)。

 **注意** 用户名和密码错误将会导致授权失败，请您输入正确的用户名和密码。

6. 选中需要授权的资产并单击**批量操作**。

您也可以单击某个实例**操作**列下的**授权**为该实例授权。

7. 在授权页面，设置识别、审计、脱敏等权限。

设置说明如下：

- **识别权限**：开启或关闭DSC识别选中资产敏感数据的权限。
- **审计权限**：开启或关闭DSC对选中资产进行数据审计的权限。
- **脱敏权限**：开启或关闭DSC对选中资产进行敏感数据脱敏的权限。
- **敏感数据采样**：设置DSC对选中资产进行敏感数据采样的条数。敏感数据采样是指DSC自动识别到敏感数据后，保留的敏感数据样本。您可以通过保留的敏感数据样本，人工对敏感数据进行更深入的判断。可选取值：
 - 0条
 - 5条
 - 10条
- **审计日志存档**：设置选中资产的审计日志保存时间。可选取值：
 - 30天
 - 90天

- 180天

说明 设置审计日志存档时间无需您额外开通日志服务。

8. 单击**确定**。

说明 若授权未通过，请检查输入的用户名和密码是否正确。

授权完成后，DSC会检测该资产中的数据。

已授权的资产可编辑或取消授权。仅支持编辑该Redis数据库合法用户的用户名和密码。取消授权后，DSC不会检测该数据库中的数据。

批量密码导入

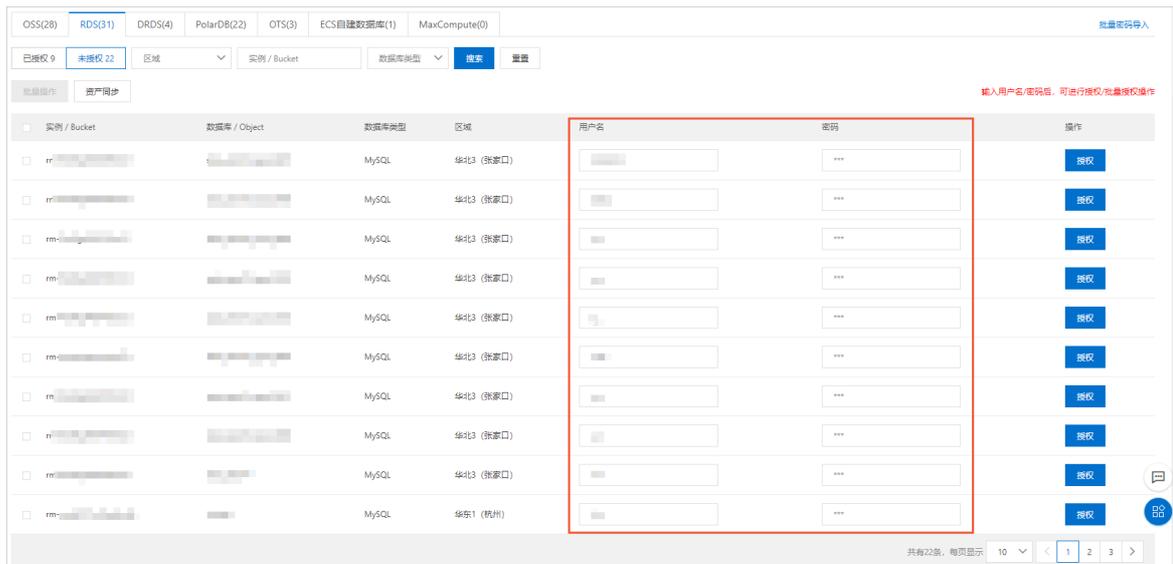
DSC支持通过Excel模板批量导入RDS、DRDS和PolarDB未授权数据库的用户名和密码，方便您批量授权DSC访问多个数据库项目。以下介绍批量导入数据库密码的详细步骤。

1. 登录**数据安全中心控制台**。
2. 在左侧导航栏，选择**数据保护授权 > 数据资产授权**。
3. 在云上托管页面右上角单击**批量密码导入**。
4. 在**批量密码导入**对话框中单击**DSC授权文件模板.xlsx**。
5. 打开下载到本地的模板文件，编辑数据库产品中的**用户名和密码**列并保存模板文件。

如果您修改了模板文件中已有的用户名和密码，批量导入密码操作完成后，已有的用户名和密码将被更新为您修改后的用户名和密码。

6. 在**批量密码导入**对话框中单击**文件上传**，完成修改后模板的上传。
7. 单击**确定**。

EXCEL文件成功上传后，DSC会自动为您在RDS、DRDS和PolarDB页签下的**用户名和密码**列导入该Excel文件中的数据库用户名和密码（如下图所示）。您无需手动填写数据库的用户名和密码，即可在云上托管页面执行批量授权操作，对多个数据库进行批量DSC访问授权。



排查资产授权失败原因

添加资产授权时可能会出现授权失败的情况。授权失败时请排查是否存在以下问题：

- **RDS连接授权失败的可能原因**

- RDS数据库账号或密码输入错误。
- 您自行删除了RDS访问白名单中DSC自动添加的服务器地址。
- 部署在经典网络中的阿里云数据产品外网地址未放行流量的访问控制，导致网络不通。

- **MaxCompute连接授权失败的可能原因**

- MaxCompute项目名称输入错误。
- MaxCompute项目中添加DSC账号失败。

5.敏感数据发现

5.1. 查看敏感数据资产

本文介绍如何查看在OSS、RDS、MaxCompute等云产品中检测出的敏感数据。

查看OSS敏感数据

1. 登录[数据安全中心控制台](#)。
2. 在左侧导航栏，选择敏感数据发现 > 敏感数据资产。
3. 在OSS页签下，定位到需要查看详情的Bucket，单击其操作列下的文件详情。
4. 在敏感数据详情页面，您可以查看敏感文件占比、命中规则TOP 5和存在敏感数据的文件列表。



查看敏感文件占比

在敏感文件占比区域，您可以查看高敏感、中敏感、低敏感和未识别敏感程度的文件的数量和占比饼状图。

查看命中规则Top 5

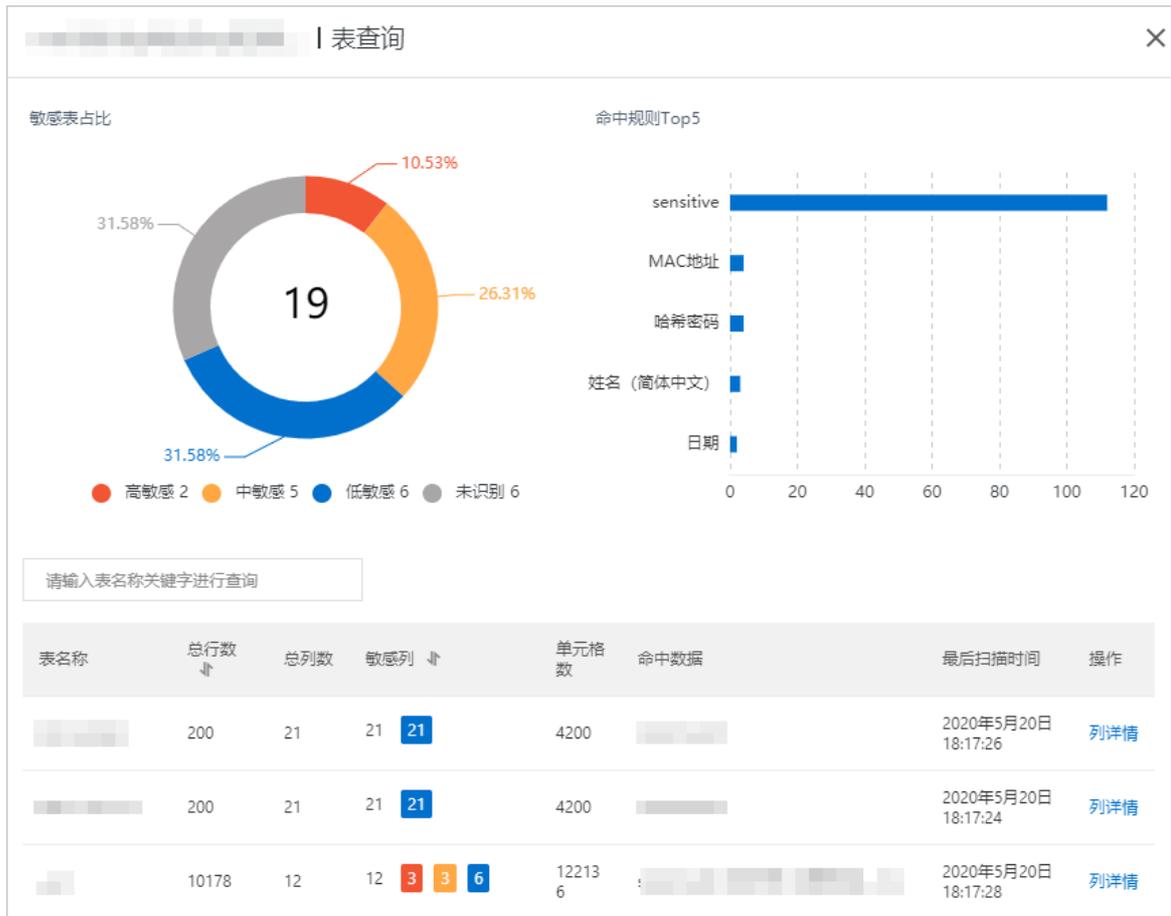
在命中规则Top 5区域，您可以查看命中敏感数据次数排名前5的规则名称及命中次数。

查看存在敏感数据的文件列表

在文件列表区域，您可以查看存在敏感数据的文件的名称、大小、类型和敏感字段数等信息。您也可以单击操作列下的命中详情查看当前文件命中的敏感数据检测规则的详细信息。

查看RDS敏感数据

1. 登录[数据安全中心控制台](#)。
2. 在左侧导航栏，选择敏感数据发现 > 敏感数据资产。
3. 在敏感数据资产页面单击RDS页签。
4. 在RDS页签下，定位到需要查看详情的RDS实例，单击其操作列下的表详情。
5. 在敏感数据详情页面，您可以查看敏感表占比、命中规则TOP 5和存在敏感数据的表的列表。



查看敏感表占比

在敏感表占比区域，您可以查看高敏感、中敏感、低敏感和未识别敏感程度的表的数量和占比饼状图。

查看命中规则Top 5

在命中规则Top 5区域，您可以查看命中敏感数据次数排名前5的规则名称及命中次数。

查看存在敏感数据的表

在列表区域，您可以查看存在敏感数据的表的名称、总行数、总列数、敏感列和命中数据等信息。您也可以单击操作列下的列详情查看命中敏感数据规则的列、敏感等级等详细信息。

查看MaxCompute敏感数据

1. 登录数据安全中心控制台。
2. 在左侧导航栏，选择敏感数据发现 > 敏感数据资产。
3. 在敏感数据资产页面单击MaxCompute页签。
4. 在MaxCompute页签下，定位到需要查看详情的MaxCompute实例，单击其操作列下的表详情。
5. 在敏感数据详情页面，您可以查看敏感表占比、命中规则TOP 5和存在敏感数据的表的列表。



查看敏感表占比

在敏感表占比区域，您可以查看高敏感、中敏感、低敏感和未识别敏感程度的表的数量和占比饼状图。

查看命中规则Top 5

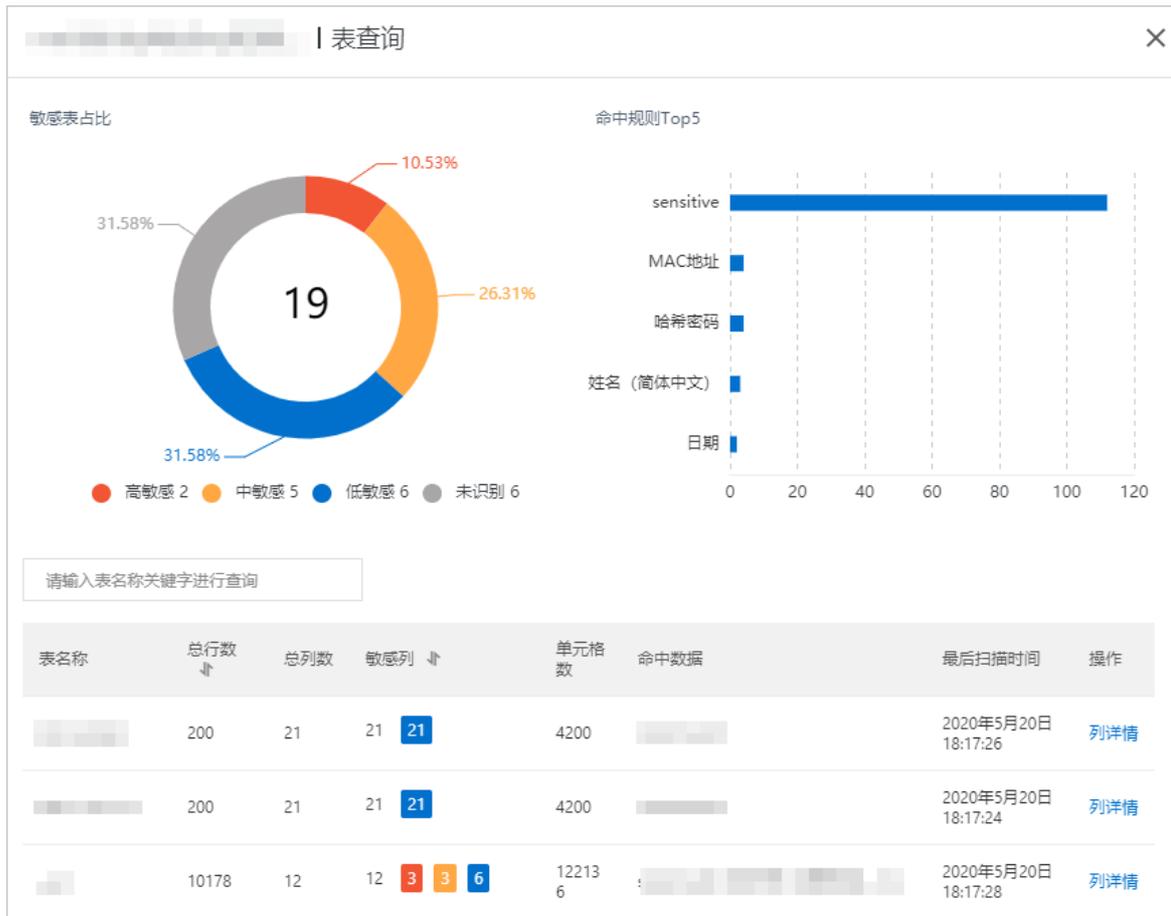
在命中规则Top 5区域，您可以查看命中敏感数据次数排名前5的规则名称及命中次数。

查看存在敏感数据的表

在列表区域，您可以查看存在敏感数据的表的名称、总行数、总列数、敏感列和命中数据等信息。您也可以单击操作列下的列详情查看命中敏感数据规则的列、敏感等级等详细信息。

查看ECS自建数据库敏感数据

1. 登录数据安全中心控制台。
2. 在左侧导航栏，选择敏感数据发现 > 敏感数据资产。
3. 在敏感数据资产页面单击ECS自建数据库页签。
4. 在ECS自建数据库页签下，定位到需要查看详情的数据实例，单击其操作列下的表详情。
5. 在敏感数据详情页面，您可以查看敏感表占比、命中规则TOP 5和存在敏感数据的表的列表。



查看敏感表占比

在敏感表占比区域，您可以查看高敏感、中敏感、低敏感和未识别敏感程度的表的数量和占比饼状图。

查看命中规则Top 5

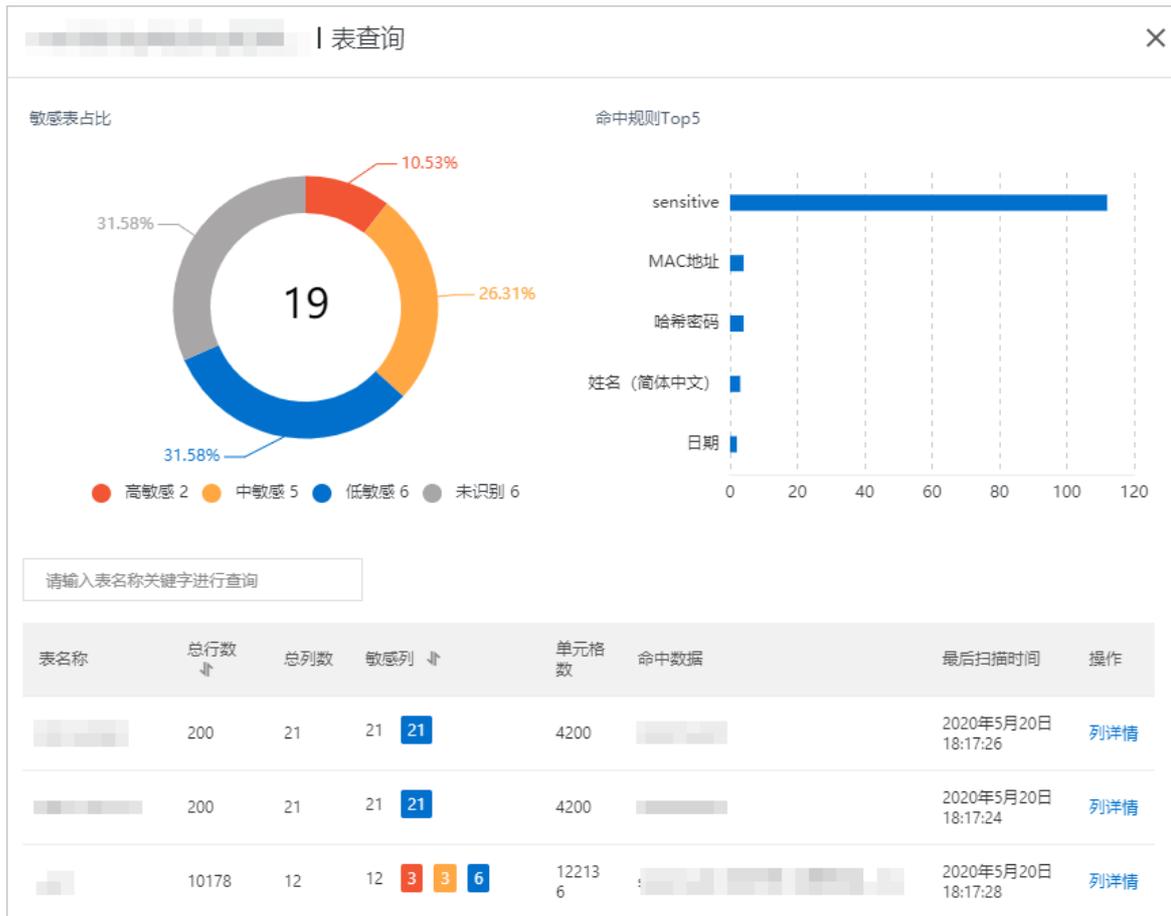
在命中规则Top 5区域，您可以查看命中敏感数据次数排名前5的规则名称及命中次数。

查看存在敏感数据的表

在列表区域，您可以查看存在敏感数据的表的名称、总行数、总列数、敏感列和命中数据等信息。您也可以单击操作列下的列详情查看命中敏感数据规则的列、敏感等级等详细信息。

查看DRDS敏感数据

1. 登录数据安全中心控制台。
2. 在左侧导航栏，选择敏感数据发现 > 敏感数据资产。
3. 在敏感数据资产页面单击DRDS页签。
4. 在DRDS页签下，定位到需要查看详情的数据库实例，单击其操作列下的表详情。
5. 在敏感数据详情页面，您可以查看敏感表占比、命中规则TOP 5和存在敏感数据的表的列表。



查看敏感表占比

在敏感表占比区域，您可以查看高敏感、中敏感、低敏感和未识别敏感程度的表的数量和占比饼状图。

查看命中规则Top 5

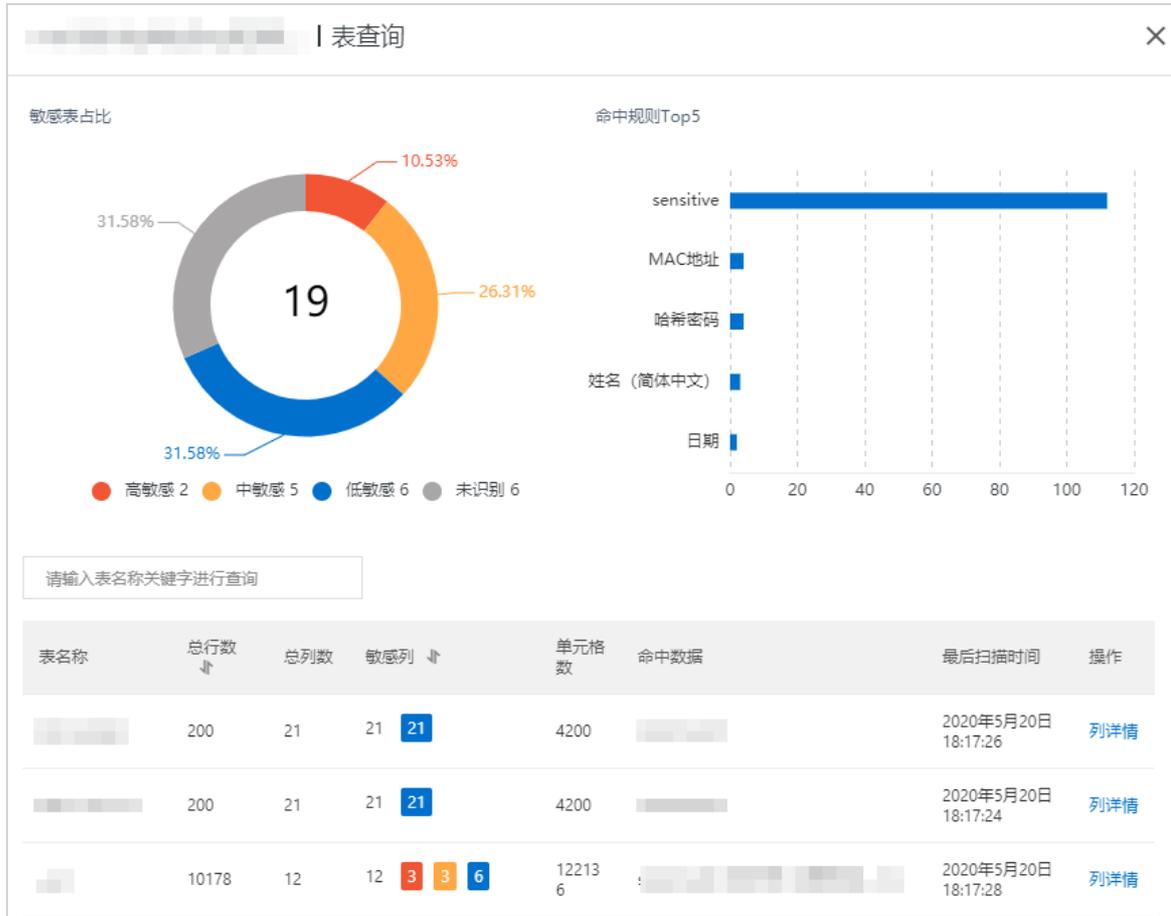
在命中规则Top 5区域，您可以查看命中敏感数据次数排名前5的规则名称及命中次数。

查看存在敏感数据的表

在列表区域，您可以查看存在敏感数据的表的名称、总行数、总列数、敏感列和命中数据等信息。您也可以单击操作列下的列详情查看命中敏感数据规则的列、敏感等级等详细信息。

查看PolarDB敏感数据

1. 登录数据安全中心控制台。
2. 在左侧导航栏，选择敏感数据发现 > 敏感数据资产。
3. 在敏感数据资产页面单击PolarDB页签。
4. 在PolarDB页签下，定位到需要查看详情的数据库实例，单击其操作列下的表详情。
5. 在敏感数据详情页面，您可以查看敏感表占比、命中规则TOP 5和存在敏感数据的表的列表。



查看敏感表占比

在敏感表占比区域，您可以查看高敏感、中敏感、低敏感和未识别敏感程度的表的数量和占比饼状图。

查看命中规则Top 5

在命中规则Top 5区域，您可以查看命中敏感数据次数排名前5的规则名称及命中次数。

查看存在敏感数据的表

在列表区域，您可以查看存在敏感数据的表的名称、总行数、总列数、敏感列和命中数据等信息。您也可以单击操作列下的列详情查看命中敏感数据规则的列、敏感等级等详细信息。

查看OTS敏感数据

OTS即表格存储服务。

1. 登录数据安全中心控制台。
2. 在左侧导航栏，选择敏感数据发现 > 敏感数据资产。
3. 在敏感数据资产页面单击OTS页签。
4. 在OTS页签下，定位到需要查看详情的实例，单击其操作列下的表详情。
5. 在敏感数据详情页面，您可以查看敏感表占比、命中规则TOP 5和存在敏感数据的表的列表。



查看敏感表占比

在敏感表占比区域，您可以查看高敏感、中敏感、低敏感和未识别敏感程度的表的数量和占比饼状图。

查看命中规则Top 5

在命中规则Top 5区域，您可以查看命中敏感数据次数排名前5的规则名称及命中次数。

查看存在敏感数据的表

在列表区域，您可以查看存在敏感数据的表的名称、总行数、总列数、敏感列和命中数据等信息。您也可以单击操作列下的列详情查看命中敏感数据规则的列、敏感等级等详细信息。

相关链接

- 数据扫描和识别
- DAP支持识别的敏感数据
- 支持识别的OSS文件类型

5.2. 导出敏感数据资产

当借助数据安全中心DSC (Data Security Center) 检测出数据源的敏感数据资产后，您可以将敏感数据资产以CSV格式导出，从Bucket、表、集合的维度查看导出的敏感数据资产。

操作步骤

1. 登录数据安全中心控制台。

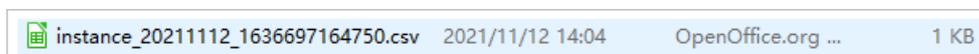
2. 在左侧导航栏，选择敏感数据发现 > 敏感数据资产。
3. 根据需要，单击要导出敏感数据资产的数据源的页签。
4. 设置导出敏感数据的过滤条件。

不同数据源支持的敏感数据过滤条件有差异。本步骤以设置DRDS的过滤条件为例。DRDS支持的过滤条件包括：区域、实例、数据库类型、敏感等级（包括：N/A、S1、S2、S3、S4）、起始日期和结束日期。

5. 单击导出。



导出成功后，文件被存储在默认存储路径中，例如，Windows系统默认存储路径为此电脑>下载。文件的默认命名方式为instance_导出该文件的日期（格式：YYYYMMDD）_导出该文件的时间（单位：毫秒，格式：时间戳）。



5.3. 搜索敏感数据

敏感数据搜索页面为您展示了资产中的所有敏感数据，您可以输入敏感数据或敏感数据的组合作为搜索条件，快速定位所关注的敏感数据在所有资产中的分布情况。

操作步骤

1. 登录数据安全中心控制台。
2. 在左侧导航栏，选择敏感数据发现 > 敏感数据搜索。
3. 在敏感数据搜索页面，设置搜索条件。

您可以设置以下搜索条件：

- 命中数据：选择需要查看的敏感数据类型，支持同时选择多个类型。例如：同时选择手机号和邮箱。
- 输入文件名称或输入表名称：输入需要查看敏感数据的文件名称或表名称。文件名称和表名称都支持模糊搜索。
- 区域：选择需要查看的云产品实例所在地域。
- Bucket、实例或项目：选择需要搜索的Bucket、实例或项目名称。
- 设置日期：设置需要搜索的起始日期和结束日期。

说明 如果您同时设置了多个搜索条件，将为您展示同时满足这些搜索条件的敏感数据列表。

4. 单击搜索。

相关操作

- 按敏感等级搜索

在OSS-文件下的搜索结果中，设置敏感等级（S1、S2、S3），查看指定敏感等级的敏感数据列表。

- 按总行数或敏感列数量升序或降序排敏感数据

在RDS-表等产品的敏感数据搜索结果下，单击总行数或敏感列右侧的  图标，按照表总行数或敏感列数量升序或降序排列当前列表中的敏感数据。单击第一次为降序排列，第二次切换到升序排列。

● 查看敏感数据详情

定位到具体的敏感数据列并单击详情或列详情，可跳转到指定Bucket的命中查询或指定数据表的列详情页面。该页面展示当前文件或表中检测出的所有敏感数据的详细信息，包括以下内容：

- 列名称：命中敏感数据的列名称。

 说明 RDS、MaxCompute、ECS自建数据库、DRDS、PolarDB和OTS的列详情页面会展示该参数。OSS文件的命中查询页面不会展示该参数。

- 命中规则：命中敏感数据的规则分类和规则名称。
- 敏感等级：敏感数据的等级。
- 命中数量：当前规则在该文件中命中敏感数据的次数。

 说明 只有OSS文件的命中查询页面会展示该参数。

- 数据采样：展示DSC识别的敏感数据字段。您可以在资产保护授权页面设置敏感数据采样的数量，可以设置为0条、5条或10条。此处将根据您的设置，最多展示0条、5条或10条采样数据。

5.4. 识别任务监控

自动为识别权限授权成功的资产创建敏感数据扫描任务。您可以在识别任务监控页面查看敏感数据扫描任务的详细信息并执行重新扫描操作。

背景信息

DSC支持监控OSS、RDS、DRDS、PolarDB、OTS（即表格存储）、ECS自建数据库和MaxCompute的敏感数据扫描任务。

云产品授权成功后，DSC自动为该产品的相应资产创建扫描任务并立即执行敏感数据检测。DSC创建扫描任务后会默认开启自动扫描。开启自动扫描服务后，自动进行首次扫描，之后每隔4个小时重新扫描资产中新增或修改的数据。新增或修改识别规则都会触发扫描任务。

查看扫描任务详细信息

您可以在识别任务监控页面查看敏感数据检测任务相关的资产、扫描状态和完成时间等信息。以下步骤介绍如何查看扫描任务的详细信息。

1. 登录[数据安全中心控制台](#)。
2. 在左侧导航栏，选择敏感数据发现 > 识别任务监控。
3. 选择需要查看的云产品，并单击其页签。
4. （可选）在搜索栏，您可以输入实例或Bucket名称，选择区域、起始日期和结束日志，并单击搜索查看指定任务。
5. 在任务列表，您可以查看扫描任务相关的资产、Bucket名称、扫描时间、扫描状态和完成时间等信息。

重新扫描资产

以下是重新扫描资产的应用场景说明：

- 未开启自动扫描的任务，需要您执行重扫操作才会进行敏感数据扫描。
- 已开启自动扫描的任务，默认每4个小时扫描资产中新增或修改的数据。如果您修改了服务器数据需要立即扫描资产中是否存在敏感数据，您可以进行重扫操作。

以下步骤介绍如何重新扫描资产中的敏感数据。

1. 登录[数据安全中心控制台](#)。
2. 在左侧导航栏，选择敏感数据发现 > 识别任务监控。
3. 选择需要重新扫描资产的云产品，并单击其页签。
4. 定位到需要重新扫描的实例，并单击其操作列下的重扫。
5. 在确定重新扫描对话框中单击确定。

一般情况下，重新扫描可以在10分钟以内完成，请您耐心等待。

重新扫描后，扫描状态将变为扫描中或等待。您可以在扫描状态处查看扫描进度。扫描完成后扫描状态将变为完成。

区域	实例 / Bucket	起始日期	结束日期	搜索	重置	
区域	实例	数据库	自动扫描	扫描状态	完成时间	操作
华北3 (张家口)	rm-...	...	<input type="checkbox"/>	授权失败	--	重扫
华北3 (张家口)	rm-...	...	<input checked="" type="checkbox"/>	完成	2020年5月22日 14:20:17	重扫
华北3 (张家口)	rm-...	...	<input checked="" type="checkbox"/>	扫描中(0%)	2020年5月22日 17:19:37	重扫

5.5. 管理识别模型

识别模型定义了识别您资产中敏感数据的具体规则。提供了识别典型敏感数据的内置识别模型，并支持自定义识别模型，您可以通过使用内置和自定义的识别模型构建专属的敏感数据识别能力。本文介绍如何查看内置识别模型、添加、编辑和删除自定义识别模型。

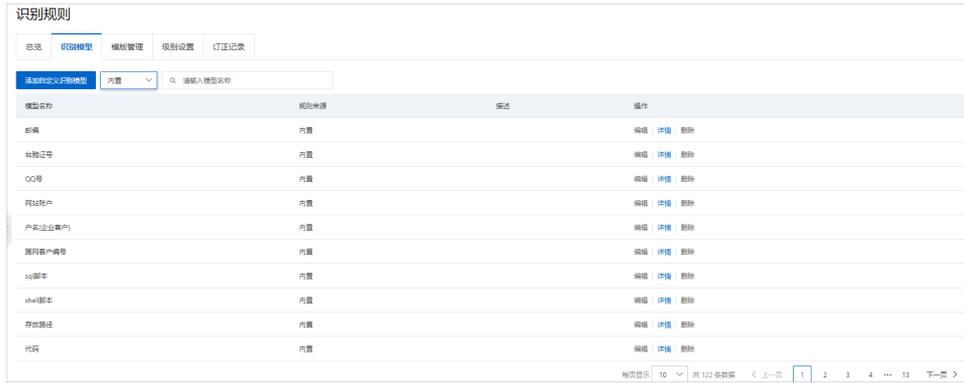
查看内置识别模型

DSC提供的内置识别模型已覆盖手机号码、身份证号等常见敏感信息。您可以查看DSC内置识别模型的名称、敏感等级和规则信息。以下步骤介绍如何查看DSC内置的识别模型。

1. 登录[数据安全中心控制台](#)。
2. 在左侧导航栏，选择敏感数据发现 > 识别规则。
3. 在识别规则页面，单击识别模型页签。
4. 将搜索条件规则来源设置为内置。



5. 查看内置识别模型列表。



您可以查看内置识别模型的名称等信息。

- 定位到需要查看详情的内置规则，单击其操作列下的详情。

说明 内置识别模型不支持修改和删除。

- 在查看内置识别模型对话框，查看该内置识别模型的详细信息。

您可以查看该内置识别模型的模型名称、敏感等级和规则信息。

添加自定义识别模型

DSC通过识别模型中定义的敏感数据识别规则，对文件或表中的敏感数据进行识别和告警。如果内置识别模型无法满足您的业务需求，您可参考以下步骤添加自定义识别模型。

- 登录数据安全中心控制台。
- 在左侧导航栏，选择敏感数据发现 > 识别规则。
- 在识别规则页面，单击识别模型页签。
- 在识别模型页签下，单击添加自定义识别模型。
- 在添加自定义识别模型对话框，配置以下参数。

添加自定义识别模型

* 模型名称

* 敏感等级

* 规则

[+ 继续添加](#)

模型描述

参数	说明
模型名称	输入识别模型的名称。

参数	说明
敏感等级	<p>选择识别模型识别出的敏感数据对应的风险等级。风险等级包括：</p> <ul style="list-style-type: none"> ○ S1：一级敏感数据 ○ S2：二级敏感数据 ○ S3：三级敏感数据 ○ S4：四级敏感数据 ○ S5：五级敏感数据 <p> 说明 S1至S5的敏感等级依次升高，S5为最高敏感等级。</p>
规则	<p>设置敏感数据的识别规则。可选：</p> <ul style="list-style-type: none"> ○ 正则匹配：使用正则表达式来定义敏感数据识别规则。可参考以下示例配置该参数： <ul style="list-style-type: none"> ■ <i>Exampleoo+a</i>：表示Exampleooa、Exampleoooa、Exampleooooooooa等都会被识别为敏感数据。+表示该符号前面的字符必须至少出现一次。 ■ <i>Exampleoo*a</i>：表示Exampleoa、Exampleooa、Exampleooooooooa等都会被识别为敏感数据。*表示该符号前面的字符可以不出现在，也可以出现一次或多次。 ■ <i>Exampleo?a</i>：表示只有Examplea、Exampleoa会被识别为敏感数据。?表示该符号前面的字符可以不出现在或最多出现一次。 ○ 不包含：使用不包含某个关键字来定义敏感数据识别规则。 ○ 包含：使用包含某个关键字来定义敏感数据识别规则。 <p>一个规则模型中可以添加多条规则。需要设置多条规则时，您可以单击继续添加在当前识别模型下再添加一条识别规则。</p> <p> 注意</p> <ul style="list-style-type: none"> ○ 如果自定义识别模型中有多条规则，同时满足该识别模型中所有规则才能命中敏感数据。 ○ 不包含的规则可以作为排除误报的条件，建议和其他规则一起使用。 ○ DSC提供的内置规则已覆盖手机号码、身份证号。建议您在新建具体的识别规则之前先查看DSC已提供的内置规则。更多信息，请参见查看内置识别模型。
模型描述	输入识别模型的描述信息。

6. 单击**确定**。

创建完成后，您可以在识别模型列表中查看新创建的识别模型。



查看、编辑、删除自定义识别模型

DSC支持查看、编辑和删除自定义识别模型。以下步骤介绍如何查看、编辑和删除自定义识别模型。

1. 登录[数据安全中心控制台](#)。
2. 在左侧导航栏，选择敏感数据发现 > 识别规则。
3. 在识别规则页面，单击识别模型页签。
4. 将搜索条件规则来源设置为自定义。
5. 定位到待操作的识别模型，执行以下操作。

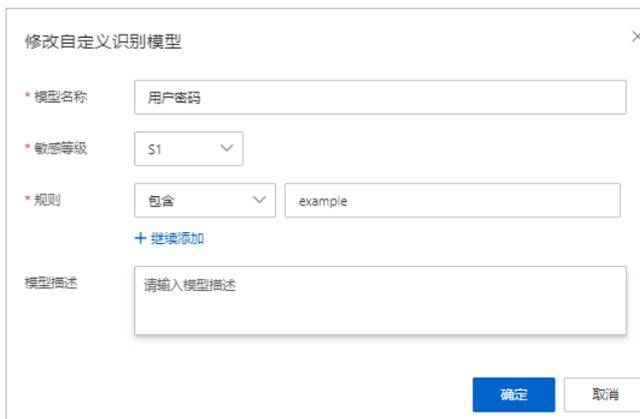
○ 查看自定义识别模型详情

需要查看某个自定义识别模型的详情时，单击该识别模型操作列下的详情，在查看自定义识别模型对话框中查看该识别模型的详情。



○ 编辑自定义识别模型

需要修改某个自定义识别模型的敏感数据识别规则时，单击该识别模型操作列下的编辑，在修改自定义识别模型对话框中，修改该识别模型的参数，并单击确定。识别模型参数配置的更多信息，请参见[识别模型参数说明](#)。



 **注意** 如果正在使用的敏感数据识别模板开启了该识别模型，DSC在执行下一次敏感数据扫描时，修改后的识别模型会生效。之前使用原识别模型扫描出的敏感数据结果不受影响。

○ 删除自定义识别模型

不再需要使用某个自定义识别模型时，单击该识别模型操作列下的**删除**，在确认对话框单击**确定**。

 **注意**

- 删除自定义识别模型后，DSC将无法使用该识别模型检测敏感数据，请谨慎进行删除操作。
- 删除自定义识别模型后，之前使用该模型扫描出的敏感数据结果不受影响。

6. 数据脱敏

6.1. 静态脱敏

数据安全中心支持对敏感数据进行脱敏，对您项目中的敏感数据进行保护。本文介绍如何新增脱敏任务、检索脱敏任务。

前提条件

在对敏感数据进行脱敏前，需确认已完成了DSC对数据所在项目、库或文件桶的访问授权。访问授权具体操作，请参见[数据资产授权](#)。

背景信息

DSC支持静态脱敏和动态脱敏。

- 动态脱敏相对于静态脱敏更加灵活，可以直接对指定数据进行脱敏。但每次可进行动态脱敏的数据有大小限制（必须小于2 MB）。动态脱敏更多信息，请参见[动态脱敏](#)。
- 静态脱敏功能使用脱敏算法对敏感数据进行遮盖、加密或替换，并将脱敏后的数据保存到您选择的目标位置。更多信息，请参见[支持的数据脱敏算法](#)。

 **说明** 目前，DSC支持对OSS文件、RDS表、MaxCompute表、PolarDB表、OceanBase表等进行静态脱敏，具体请参见[支持的数据库类型](#)。

新增脱敏任务

1. 登录[数据安全中心控制台](#)。
2. 在左侧导航栏，选择[数据脱敏](#) > [静态脱敏](#)。
3. 在[静态脱敏](#)页面单击[新增脱敏任务](#)。
4. 完成以下步骤创建自定义脱敏任务。

- i. 填写任务基本信息，并单击下一步。

 **说明** 任务名称输入不受限制。

- ii. 配置脱敏数据的来源文件信息（见下表），并单击下一步。
 - [RDS表/DRDS表/MaxCompute表/PolarDB表/OceanBase表/ADB-MySQL表](#)脱敏源参数配置。

1 任务基本信息
2 脱敏源配置
3 脱敏算法

数据存储类型

RDS表 / DRDS表 / MaxCompute表 / PolarDB表 / OceanBase表 / ADB-MySQL表

OSS文件

源产品

请选择
▼

上一步
下一步

脱敏源配置项	配置描述
数据存储类型	选择脱敏文件的数据存储类型。此处选择RDS表/DRDS表/MaxCompute表/PolarDB表/OceanBase表/ADB-MySQL表。
源产品	选择包含脱敏数据的文件来源的产品名称。可选RDS、DRDS、OceanBase、MaxCompute、ADB-MySQL或PolarDB。
源数据库/项目名	必填项。选择包含脱敏数据的表所在的项目名称。
源表名	必填项。选择脱敏数据所在的数据表名称。
源分区	<p>选填项。手动输入需要脱敏的数据在数据表中的分区名称，分区写法更多信息，请参见分区写法参考。</p> <p>分区是指在创建MaxCompute数据表时指定的分区空间，用于限定不同区域，方便快速和高效地对指定内容进行查询。更多信息，请参见分区。</p> <div style="background-color: #e6f2ff; padding: 10px; border: 1px solid #d9e1f2;"> <p>? 说明</p> <ul style="list-style-type: none"> ■ 源产品选择RDS和PolarDB时，无需配置源分区。 ■ 源分区为选填项，不填写则代表会对整个表中的敏感数据进行脱敏。 </div>
抽样SQL	<p>选填项。手动输入SQL语句可选择脱敏数据范围。不填写则进行全表脱敏。</p> <div style="background-color: #e6f2ff; padding: 10px; border: 1px solid #d9e1f2;"> <p>? 说明 源产品选择MaxCompute和PolarDB时，无需配置抽样SQL。</p> </div>

■ OSS文件脱敏源参数配置。

脱敏源配置项	配置描述
数据存储类型	选择脱敏文件的数据存储类型。此处选择OSS文件。
文件源	选择OSS文件的来源，可选本地上传或OSS Bucket。 <div style="border: 1px solid #ccc; background-color: #e6f2ff; padding: 5px; margin-top: 10px;"> <p>? 说明 本地上传仅支持结构化TXT、CSV、XLSX和XLS格式文件。</p> </div>
源文件所在OSS Bucket	在下拉列表中选择源文件所在的OSS Bucket。您也可输入关键字进行搜索并选择源文件所在的OSS Bucket。
源文件名称	输入源文件的名称。源文件名称需要包含后缀，仅支持结构化TXT、CSV、XLSX和XLS格式。 如果需要对多个同类型的源文件进行批量脱敏，您可以单击右侧 开启通配 按钮。 <div style="border: 1px solid #ccc; background-color: #e6f2ff; padding: 5px; margin-top: 10px;"> <p>? 说明 开启通配后，您可以使用*方式指定一批源文件进行批量脱敏，目前仅支持对文件名前缀进行匹配，例如 <i>test*.xls</i>。设置批量脱敏后，系统会采用相同的规则进行脱敏，请务必保证这批文件有相同的列结构。</p> </div>
源文件描述	输入对OSS源文件的描述。 文件源 选择OSS Bucket时无需配置该参数。
分隔符选择	选填项。对于.csv和.txt类型的文件，需要指定列分隔符，请根据源文件类型进行选择。支持选择以下类型分隔符： <ul style="list-style-type: none"> ■ 分号 “;”（macOS、Linux默认） ■ 逗号 “,”（Windows默认）
表格包含标题行	选填项。根据需要选择待脱敏表格是否包含标题行。

iii. 配置脱敏算法，并单击下一步。

在脱敏算法配置列表中，定位到需要进行脱敏的源字段，打开**脱敏开关**，并选择需要的脱敏算法。更多信息，请参见[脱敏算法](#)。

? 说明

- 单击已选择算法后的**参数查看修改**，可查看或修改已选择算法的规则内容。
- 脱敏开关未开启，将无法对数据进行脱敏。

iv. 开启数据水印开关。

对进行分发的数据添加水印后，可以实现泄露数据溯源。水印添加成功后，自定义的水印信息将嵌入到数据库的数据中。

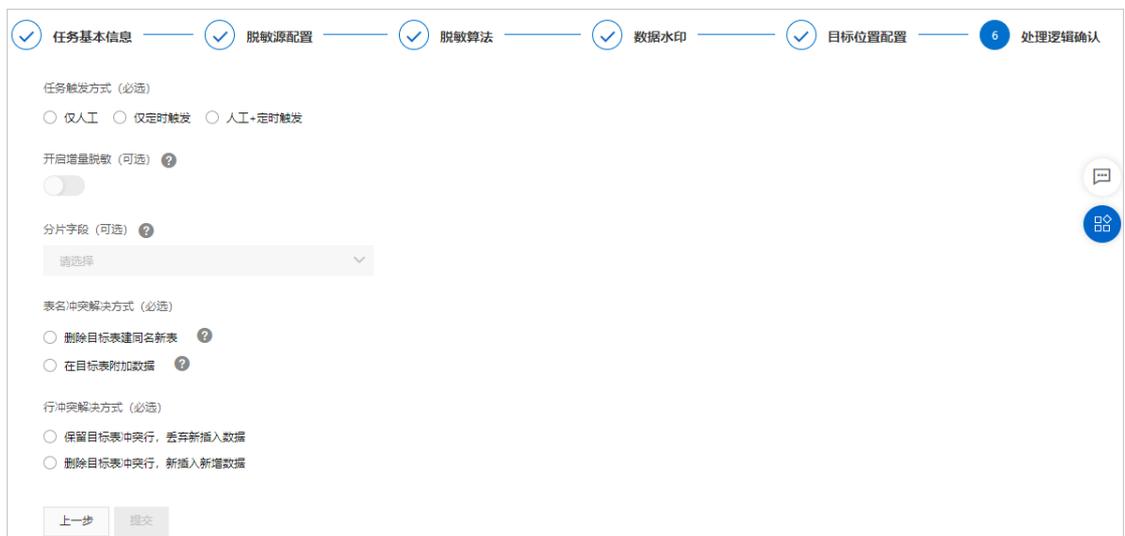
自定义的水印信息可以是数据分发的信息，例如：员工A需要导出一份订单数据，管理员将“某年某月某日导出XX数据给员工A”的水印信息在导出时添加到数据里。当数据出现泄露时，管理员可以在获取到泄露的数据后、通过提取水印，将数据中的备注信息提取出来，就可以定位到泄漏数据的是员工A。



水印使用限制，请参见[水印使用限制](#)。

v. 设置敏感数据要移动的目标位置，测试写入权限，并单击下一步。

vi. 确认处理逻辑。



目标位置配置项	配置项描述
---------	-------

目标位置配置项	配置项描述
触发方式选择	<p>触发方式表示执行脱敏任务的方式。可选项：</p> <ul style="list-style-type: none"> ■ 仅人工：需要在静态脱敏配置页面，通过手动的方式启动脱敏任务。 ■ 仅定时触发：通过设置的时间点定时自动执行脱敏任务，可选每小时、每天、每月固定时间点自动触发任务。 ■ 人工+定时触发：选择该方式，支持您手动单击启动来执行脱敏任务，和系统根据配置的定时时间自动执行脱敏任务（可选每小时、每天、每月、每周固定时间点自动触发任务）。
开启增量脱敏	<p>选填项。您可根据需要选择是否开启增量脱敏。增量脱敏是指每次脱敏数据为上次脱敏任务完成后新增的数据的脱敏方式。您需要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（数据库自带的自增列）等。</p> <p> 说明 当前仅有RDS数据支持增量脱敏。</p>
分片字段	<p>选填项。DSC执行静态脱敏时会对源数据进行字段分片，通过并发处理的方式提高脱敏效率。您可根据需要选择分片字段，支持选择多个分片字段。</p> <p> 说明</p> <ul style="list-style-type: none"> ■ 当前仅有RDS数据支持增量脱敏，建议使用主键或者唯一索引作为分片字段。 ■ 分片字段选择框内如果未选取任何字段，DSC将会默认使用主键作为分片字段，对源数据进行脱敏处理。如果您的源数据中没有主键，您必须选择分片字段，否则会导致脱敏任务失败。 ■ 过多的分片字段会影响查询性能以及数据准确性，请谨慎选择。
表名冲突解决方式	<p>表名称存在冲突的情况下处理的方式。可选项：</p> <ul style="list-style-type: none"> ■ 删除目标表建新同名表。 ■ 在目标表增加新数据：建议选择该选项。
行冲突解决方式	<p>表中的行内容存在冲突的情况下处理的方式。可选项：</p> <ul style="list-style-type: none"> ■ 保留目标表冲突行，丢弃新插入数据。建议选择该选项。 ■ 删除目标表冲突行，新插入新增数据。

vii. 单击提交，完成脱敏任务的创建。

在静态脱敏页面的脱敏任务配置页签中可查看到已创建的脱敏任务。

5. 执行脱敏任务。

脱敏任务创建完成后，在脱敏任务列表中操作列下单击  图标开启任务，并单击启动，开始执行脱敏任务。

任务编号	执行时间	第N次执行该任务	执行方式	源产品类型	目标产品类型	执行进度	新增脱敏行	冲突行数	状态	操作
	2020年5月26日 11:01:01	2023	定时	RDS	RDS	<div style="width: 100%;"><div style="width: 100%;"></div></div> 100%	1000	0	执行成功	终止任务
	2020年5月26日 10:01:01	2022	定时	RDS	RDS	<div style="width: 100%;"><div style="width: 100%;"></div></div> 100%	1000	0	执行成功	终止任务
	2020年5月26日 09:01:01	2021	定时	RDS	RDS	<div style="width: 100%;"><div style="width: 100%;"></div></div> 100%	1000	0	执行成功	终止任务

 **说明** DSC支持修改和删除已创建的脱敏任务，不支持修改和删除在执行中的脱敏任务。

6. 查看脱敏任务的执行进度和状态。

脱敏任务启动后，单击任务执行状态页签，在任务执行状态列表上方单击任务执行检索，更新最新任务执行情况。

 **说明** 未单击任务执行检索的情况下，在任务执行状态列表当前页中您可能无法看到该任务执行记录。

任务执行状态列表中的状态列会展示该脱敏任务执行成功或失败。执行失败原因的更多信息，请参见[脱敏任务执行失败排查](#)。

任务编号	执行时间	第N次执行该任务	执行方式	源产品类型	目标产品类型	执行进度	新增脱敏行	冲突行数	状态	操作
	2020年5月26日 11:01:01	2023	定时	RDS	RDS	<div style="width: 100%;"><div style="width: 100%;"></div></div> 100%	1000	0	执行成功	终止任务
	2020年5月26日 10:01:01	2022	定时	RDS	RDS	<div style="width: 100%;"><div style="width: 100%;"></div></div> 100%	1000	0	执行成功	终止任务
	2020年5月26日 09:01:01	2021	定时	RDS	RDS	<div style="width: 100%;"><div style="width: 100%;"></div></div> 100%	1000	0	执行成功	终止任务

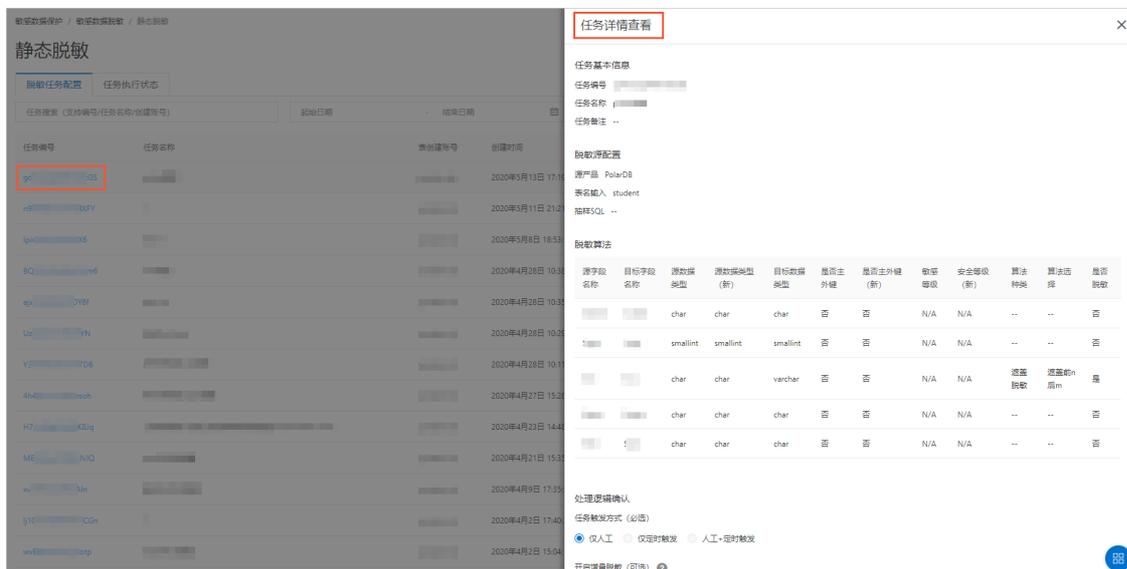
分区写法参考

分区类型	分区写法	分区示例
后N周	自定义分区字段名称 = \${yyyyymmdd+7*N}	time=\${20190710+7*1}，表示对2019年7月10日后一周的数据进行脱敏。
前N周	自定义分区字段名称=\${yyyyymmdd-7*N}	time=\${20190710-7*3}，表示对2019年7月10日前的3周时间内的数据进行脱敏。
后N天	自定义分区字段名称 = \${yyyyymmdd+N}	time=\${20190710+2}，表示对2019年7月10日后的2天内的数据进行脱敏。
前N天	自定义分区字段名称=\${yyyyymmdd-N}	time=\${20190710-5}，表示对2019年7月10日前的5天内的数据进行脱敏。
后N小时	自定义分区字段名称 = \${hh24mi:ss+N/24}	time=\${0924mi:ss+N/24}，表示对9点以后的2小时的数据进行脱敏。

分区类型	分区写法	分区示例
前N小时	自定义分区字段名称=\${hh24mi:ss-N/24]	time=\${0924mi:ss-1/24]，表示对9点前的1个小时内的数据进行脱敏。
后N分钟	自定义分区字段名称=\${hh24mi:ss+N/24/60]	time=\${0924mi:ss+2/24/60]，表示对9点过后的2分钟内的数据进行脱敏。
前N分钟	自定义分区字段名称=\${hh24mi:ss-N/24/60]	time=\${0924mi:ss-2/24/60]，表示对9点的前2分钟内的数据进行脱敏。

脱敏任务检索

您可在静态脱敏页面，对已创建的脱敏任务进行查询。在任务列表中单击任务编号，可展开任务详情页面信息。



如需对某个已创建的任务进行修改，您可将该任务的任务编号复制到任务配置列表搜索栏中，并单击脱敏任务检索，筛选出该脱敏任务进行修改。



脱敏任务执行失败排查

执行失败错误提示	错误原因
找不到脱敏任务，有可能是因为任务已经被删除或者关闭	脱敏任务可能被删除或被关闭（脱敏任务列表中操作栏关闭按钮未开启）。
定时任务的调度周期设置有误	每日具体任务执行时间输入有误。

执行失败错误提示	错误原因
找不到脱敏源实例	脱敏源表实例不存在。
找不到脱敏目标实例	可能的原因有实例授权取消或目标实例删除等。
找不到脱敏源表	可能的原因有实例授权取消、源表删除等。
脱敏算法参数设置有误	算法参数填写错误。
源表列为空	源分区字段的列没有数据。
写入目标表失败	目标位置配置时写入目标表失败。
从源表查询失败	源表中未查询到该数据。
创建目标表失败	目标位置中可能不存在该表格。
找不到主键	RDS源表缺少主键。有关主键的更多信息，请参见 RDS MySQL查看表的主键字段的方法 。
任务配置的MaxCompute分区字段有误	创建脱敏任务时，在脱敏源配置项中填写的源分区或者目标位置配置项填写的目标分区有误。

6.2. 动态脱敏

您可以通过调用ExecDat amask接口对数据进行动态脱敏。

背景信息

您可以通过调用ExecDat amask接口，对数据进行动态脱敏。调用该接口时需要提供脱敏模板ID。动态脱敏和静态脱敏可以共用已创建的脱敏模板。您可以在[数据安全中心控制台脱敏模板](#)页面获取脱敏模板ID，也可以新建脱敏模板。



限制条件

您调用ExecDat amask接口对指定数据进行动态脱敏时，请求参数 `Data` 必须小于2 MB。

查看调用动态脱敏接口记录

1. 登录[数据安全中心控制台](#)。
2. 在左侧导航栏，选择数据脱敏 > 动态脱敏。
3. 在动态脱敏页面，查看调用ExecDat amask接口的详细操作记录。

动态脱敏

您可以通过调用SDP提供的动态脱敏 Open API ExecDatamask(详情), 实现对数据进行脱敏, 动态脱敏可与静态脱敏共用设置好的脱敏模板及脱敏算法

[调用API](#)

动态脱敏 Open API	UID	IP地址	首次调用时间	最后一次调用时间	累计调用次数
ExecDatamask	19-...-29	-	2020年7月3日 18:03:23	2020年7月3日 18:03:23	1

共有1条, 每页显示 10 < 上一页 1 下一页 >

说明 如果您在调用接口时使用了相同的账号和IP地址, 即使多次调用接口, 操作记录只会保留一条, 并记录累计调用次数。

6.3. 脱敏模板

支持自定义脱敏模板。您可以将使用频率较高且应用场景相同的脱敏算法配置在同一个脱敏模板中, 避免重复地配置脱敏算法, 提高处理敏感数据的效率。本文介绍如何新增和管理脱敏模板。

新增脱敏模板

您可以创建的脱敏模板数量没有限制。

1. 登录[数据安全中心控制台](#)。
2. 在左侧导航栏, 选择[数据脱敏 > 脱敏模板](#)。
3. 在[脱敏模板](#)页面, 单击[新建模板](#)。
4. 在[新建模板](#)页面, 参考以下表格配置模板参数。

新建模板

* 模板名称

个人信息脱敏

模板描述

设置个人信息脱敏算法

* 匹配方式

敏感类型

[增加算法](#)

规则列表

车辆识别代码 哈希脱敏 MD5 [参数查看修改](#)

[确定](#) [取消](#)

参数	说明
模板名称	脱敏模板的名称。
模板描述	脱敏模板的相关信息。您可以在这里输入脱敏模板的使用范围等关键信息。
匹配方式	<p>选择一种敏感数据的匹配方式，可以选择以下方式：</p> <ul style="list-style-type: none"> 敏感类型：选择DSC支持的敏感数据类型并设置相应的脱敏算法，例如车辆识别代码、统一社会信用代码等。 字段名称：指定需要脱敏的字段名称并设置相应的脱敏算法。
规则列表	<p>在规则列表中选择敏感类型或输入需要进行脱敏的字段，设置您需要使用的脱敏算法。DSC支持以下脱敏算法：</p> <ul style="list-style-type: none"> 哈希脱敏 遮盖脱敏 替换脱敏 变换脱敏 加密脱敏 洗牌脱敏 数据解密 <p>更多信息，请参见支持的数据脱敏算法。</p> <p>您可以在一个模板中添加多个规则，单击增加算法可新增一条脱敏算法规则。</p>

管理模板

- 编辑模板

如果需要更新指定脱敏模板的描述或规则，您可以在脱敏模板页面定位到该模板，并单击其操作列的编辑，在编辑页面修改模板的描述或相关规则。

编辑

* 模板名称

线上另存为

模板描述

* 匹配方式

字段名称

增加算法

规则列表

请选择

请选择

确定 取消

• 删除模板

如果某个模板不再适用于当前的业务场景，您可以在脱敏模板页面定位到该模板，并单击其操作列的删除，删除该模板。

 说明 模板删除后无法恢复，请谨慎操作。

6.4. 脱敏算法

本文介绍了脱敏算法的配置方法和相关示例。

背景信息

支持哈希脱敏、遮盖脱敏、替换脱敏、变换脱敏、加密脱敏、数据解密和洗牌脱敏。更多信息，请参见[支持的数据脱敏算法](#)。

操作步骤

1. 登录[数据安全中心控制台](#)。
2. 在左侧导航栏，选择[数据脱敏 > 脱敏算法](#)。
3. 选择静态脱敏要应用的脱敏算法，并单击相应页签。

4. 配置脱敏算法。

您可以配置以下脱敏算法：

- **哈希脱敏**：设置各加密算法的盐值。

说明

在密码学中，通过在密码任意固定位置插入特定的字符串，让散列后的结果和使用原始密码的散列结果不相符，这种过程称之为加盐。盐值即插入的特定字符串。

MD5	<input type="text" value="015a"/>	<input type="button" value="测试"/>	<input type="button" value="提交"/>
SHA1	<input type="text" value="请输入“盐值”"/>	<input type="button" value="测试"/>	<input type="button" value="提交"/>
SHA256	<input type="text" value="请输入“盐值”"/>	<input type="button" value="测试"/>	<input type="button" value="提交"/>
HMAC	<input type="text" value="请输入“盐值”"/>	<input type="button" value="测试"/>	<input type="button" value="提交"/>

- **遮盖脱敏**：设置遮盖脱敏算法的参数。

源类型选择 *

* #

保留前n后m

n m

保留自x至y

x y

遮盖前n后m

n m

遮盖自x至y

x y

特殊字符前遮盖 (针对首次出现该字符)

@ & .

特殊字符后遮盖 (针对首次出现该字符)

@ & .

- **替换脱敏**：设置替换脱敏算法的参数。

新增替换脱敏算法

身份证映射替换
行政区划随机码表

校验位再计算

保存 **测试**

身份证随机替换
行政区划随机码表

1920年1月1日 - 2200年1月1日 

校验位再计算

保存 **测试**

军官证随机替换
行政区划随机码表

军官证随机区间 66 - 97

保存 **测试**

护照随机替换
用途字段随机码

簿子编号随机区间 1 - 99999999

保存 **测试**

港澳通行证随机替换
用途字段随机码

通行证编号随机区间 100 - 99999999

保存 **测试**

银行卡随机替换
Bin码随机码表

卡编码随机区间 1 - 999999999999

校验位再计算

保存 **测试**

座机号码随机替换
行政区划随机码表

号码随机区间 10000000 - 99999999

保存 **测试**

手机号随机替换
网号

号码随机区间 1 - 99999994

统一信用码随机替换
登记部门随机码表
类别码随机码表
行政区划随机码表

机构代码随机区间 10 - 99999999

校验位再计算

通用保格映射替换
大写字母随机码
小写字母随机码
数字随机码
特殊随机码

通用保格随机替换
大写字母随机码
小写字母随机码
数字随机码

- **变换脱敏**：设置变换脱敏算法的参数。

数字取整	保留小数点前第N位	<input type="text" value="33"/>	<input type="button" value="测试"/>	<input type="button" value="提交"/>
日期取整	日期取整保留到	年 <input type="button" value="v"/>	<input type="button" value="测试"/>	<input type="button" value="提交"/>
字符位移	整体循环位移Bit数	<input type="text" value="22"/>	<input checked="" type="radio"/> 向左 <input type="radio"/> 向右	<input type="button" value="测试"/> <input type="button" value="提交"/>

- **加密脱敏**：设置加密脱敏算法的密钥。

DES算法	<input type="text"/>	<input type="button" value="测试"/>	<input type="button" value="提交"/>
3DES算法	<input type="text"/>		
	<input type="text"/>		
	<input type="text"/>	<input type="button" value="测试"/>	<input type="button" value="提交"/>
AES算法	<input type="text"/>	<input type="button" value="测试"/>	<input type="button" value="提交"/>

- **数据解密**：设置解密算法的密钥。

DES算法	<input type="text" value="2"/>	<input type="button" value="测试"/>	<input type="button" value="提交"/>
3DES算法	<input type="text" value="3"/>		
	<input type="text" value="2"/>		
	<input type="text" value="1"/>	<input type="button" value="测试"/>	<input type="button" value="提交"/>
AES算法	<input type="text" value="22"/>	<input type="button" value="测试"/>	<input type="button" value="提交"/>

- **洗牌脱敏**：选择洗牌脱敏算法的洗牌方式。

随机洗牌	洗牌方式	<input checked="" type="radio"/> 打散重排 <input type="radio"/> 随机选择	<input type="button" value="提交"/>
------	------	--	-----------------------------------

 **说明** 洗牌脱敏算法的设置无需测试，即无需执行后续步骤，直接单击提交。

- 5. 单击已设置参数的**测试**。

在**脱敏算法测试**页面，测试数据是否脱敏。

脱敏算法测试

输入原始值

脱敏结果

测试完成后，关闭**脱敏算法测试**页面。

- 6. 单击已测试参数的**提交**。

后续步骤

完成脱敏算法配置后，可前往[静态脱敏](#)页面，创建或修改静态脱敏任务中的脱敏算法配置。更多信息，请参见[静态脱敏](#)。

6.5. 提取水印

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。本文介绍如何提取水印的操作指导。

背景信息

数据库水印具有以下特点：

- **安全性**：数据水印不会因为数据改动而导致水印信息丢失，保障数据水印被准确鉴别。
- **透明性**：在原始数据中嵌入水印标记信息且不易被察觉，不影响原数据使用。
- **可检测性**：可以从数据片段中提取水印信息，进行数据溯源，溯源成功率高。
- **鲁棒性**：受到恶意攻击后，仍然可以完整地提取水印信息。
- **低错误率**：精确设计的水印提取规则，可以最大限度地降低数据溯源的错误概率。

使用限制

当前仅支持从RDS中提取水印。

操作步骤

1. 登录[数据安全中心控制台](#)。
2. 在左侧导航栏，选择[数据脱敏](#) > [提取水印](#)。
3. 在[提取水印](#)页面，填写数据源信息。

数据安全中心 / 数据脱敏 / 提取水印

提取水印

源产品

请选择 ▼

源数据库/项目名

请选择 ▼

源表名

请输入

提取水印

复制结果

配置项	配置描述
源产品	选择包含脱敏数据的文件来源的产品名称，当前仅能选择RDS。

配置项	配置描述
源数据库/项目名	必填项。选择包含水印信息的表所在的项目名称。
源表名	必填项。选择水印信息所在的数据表名称。

4. 单击提取水印。

在提取水印页面下方的文本框中可以查看提取出来的水印信息。该信息是新增静态脱敏任务时，设置的水印信息。

单击复制结果可以复制文本框中提取的水印信息。