ALIBABA CLOUD

阿里云

数据安全中心

用户指南

文档版本：20220421

阿里云

法律声明

阿里云提醒您在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 `cd /d C:/window` 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	`bae log list --instanceid` *Instance_ID*
[] 或者 [a|b]	表示可选项，至多选择一个。	`ipconfig [-all|-t]`
{} 或者 {a|b}	表示必选项，至多选择一个。	`switch {active|stand}`

目录

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

权限说明和代码段隐藏，后续备用。

权限说明：

```
{
    "Version": "1",
    "Statement": [
        {
            "Action": [
                "oss:PutBucket",
                "oss:ListBuckets",
                "oss:GetObject",
                "oss:ListObjects",
                "oss:GetBucketInfo",
                "oss:GetObjectToFile",
                "oss:GetObjectAcl",
                "oss:PutObjectAcl",
                "oss:GetBucketStat",
                "oss:DoesObjectExist",
                "oss:PutObject",
                "oss:AppendObject",
                "oss:CompleteMultipartUpload",
                "oss:GetSimplifiedObjectMeta",
                "oss:InitiateMultipartUpload",
```

```
                "oss:UploadPart",
                "oss:GetBucketPolicy"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "oss:PutObject",
                "oss:DeleteObject"
            ],
            "Resource": [
                "acs:oss:*:*:yundun-dsc-*"
            ],
            "Effect": "Allow"
        },
        {
            "Action": [
                "ram:ListUsers",
                "ram:ListGroups",
                "ram:ListUsersForGroup",
                "ram:ListRoles",
                "ram:ListPolicyVersions",
                "ram:ListPoliciesForUser",
                "ram:ListGroupsForUser",
                "ram:ListPoliciesForGroup"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": "ram:DeleteServiceLinkedRole",
            "Resource": "*",
            "Effect": "Allow",
            "Condition": {
                "StringEquals": {
                    "ram:ServiceName": "dsc.aliyuncs.com"
                }
            }
        },
        {
            "Action": [
                "rds:DescribeDBInstances",
                "rds:DescribeDatabases",
                "rds:DescribeAccounts",
                "rds:DescribeDBInstanceNetInfo",
                "rds:ModifySecurityIps",
                "rds:DescribeDBInstanceIPArrayList",
                "rds:DescribeSQLLogRecords",
                "rds:StartSqlLogTrail",
                "rds:ModifySQLCollectorPolicy",
                "rds:DescribeSQLCollectorPolicy",
                "rds:DescribeSQLCollectorVersion",
                "rds:ModifySQLCollectorRetention",
```

```
                "rds:DescribeSQLCollectorRetention"
            ],
            "Resource": [
                "*"
            ],
            "Effect": "Allow"
        },
        {
            "Action": [
                "ecs:DescribeInstances",
                "ecs:AuthorizeSecurityGroup",
                "ecs:RevokeSecurityGroup",
                "ecs:DescribeSecurityGroups",
                "ecs:DescribeSecurityGroupAttribute"
            ],
            "Resource": [
                "*"
            ],
            "Effect": "Allow"
        },
        {
            "Action": [
                "log:CreateConsumerGroup",
                "log:UpdateConsumerGroup",
                "log:ConsumerGroupHeartBeat",
                "log:GetConsumerGroupCheckPoint",
                "log:GetCursorOrData",
                "log:ConsumerGroupUpdateCheckPoint",
                "log:GetApp",
                "log:GetProject",
                "log:GetLogStore"
            ],
            "Resource": [
                "*"
            ],
            "Effect": "Allow"
        },
        {
            "Action": [
                "drds:DescribeDrdsInstances",
                "drds:DescribeDrdsInstance",
                "drds:DescribeDrdsDBs",
                "drds:DescribeDrdsDB",
                "drds:DescribeTables",
                "drds:DescribeTable",
                "drds:ModifyDrdsIpWhiteList",
                "drds:DescribeDrdsDBIpWhiteList",
                "drds:DescribeInstanceAccounts",
                "drds:DescribeDrdsSqlAuditStatus",
                "drds:DescribeDrdsSlowSqls",
                "drds:DescribeInstDbLogInfo",
                "drds:EnableSqlAudit",
                "drds:DescribeInstDbSlsInfo",
                "drds:DisableSqlAudit"
```

```
            ],
            "Resource": [
                "*"
            ],
            "Effect": "Allow"
        },
        {
            "Action": [
                "polardb:DescribeDBClusters",
                "polardb:DescribeDBClusterAttribute",
                "polardb:DescribeDBClusterParameters",
                "polardb:DescribeDBClusterEndpoints",
                "polardb:DescribeDatabases",
                "polardb:DescribeAccounts",
                "polardb:DescribeDBClusterAccessWhitelist",
                "polardb:ModifyDBClusterAccessWhitelist",
                "polardb:DescribeSQLExplorerPolicy",
                "polardb:DescribeSQLExplorerRetention",
                "polardb:ModifySQLExplorerPolicy",
                "polardb:ModifySQLExplorerRetention",
                "polardb:StartSQLLogTrail",
                "polardb:DescribeSQLLogRecords"
            ],
            "Resource": [
                "*"
            ],
            "Effect": "Allow"
        },
        {
            "Action": [
                "ots:ListInstance",
                "ots:GetInstance",
                "ots:ListTable",
                "ots:ComputeSplitPointsBySize",
                "ots:GetRange"
            ],
            "Resource": [
                "*"
            ],
            "Effect": "Allow"
        }
    ]
}
```

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。

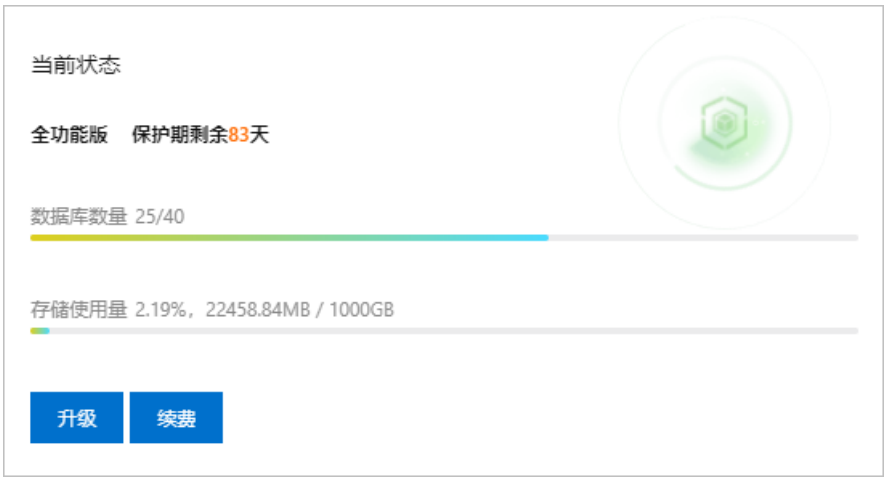
查看数据保护授权状态

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。

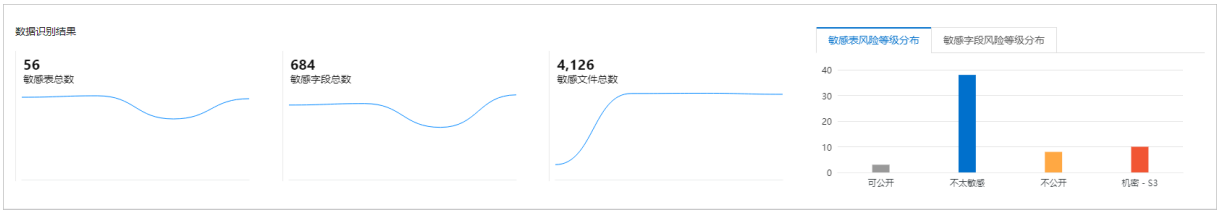
查看DSC服务当前状态

在**当前状态**区域查看DSC的版本信息、保护期剩余天数、数据库数量和存储使用量。如果您需要进行升级或续费操作，您可以单击**升级**或**续费**。



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。

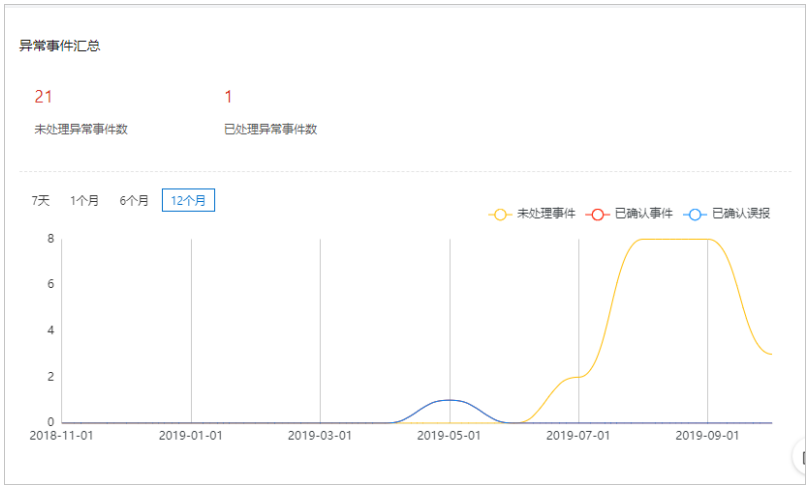
查看静态脱敏数据统计

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和风险趋势

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。更多信息，请参见异常事件告警。

- **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，请参见购买数据安全中心和授权DSC访问云资源。

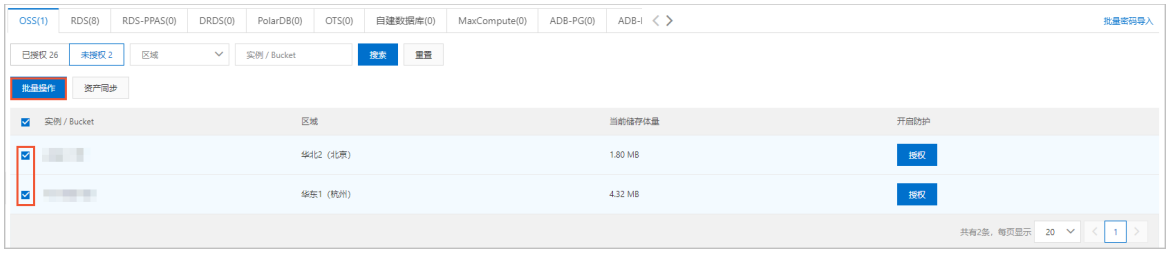
背景信息

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。

> **注意** 已开启授权的OSS Bucket会消耗您购买的OSS存储容量，已开启授权的数据库或项目会消耗您购买的数据库和项目数。只有在OSS存储容量、数据库和项目数量充足时，您才可以成功进行相应授权操作。您可以在**云上托管**页面查看剩余的OSS存储容量、数据库和项目数。

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。更多有关DSC内置的安全审计规则信息，请参见内置的安全审计规则。

     DSC安全审计功能使用的更多信息，请参见创建审计规则。

     > **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，0.008元/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。
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	

6. 在授权页面，设置识别、审计、脱敏等权限。
7. 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

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**DRDS**页签。
4. 在**DRDS**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

- 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）	○ 100.104.238.64/26 ○ 100.104.198.192/26
华北 2（北京）	○ 100.104.250.0/26 ○ 100.104.51.192/26
华东 1（杭州）	○ 100.104.207.192/26 ○ 100.104.232.64/26

地域	IP段
华南 1（深圳）	○ 100.104.247.0/26 ○ 100.104.150.64/26
华北 3（张家口）	○ 100.104.37.128/26 ○ 100.104.191.64/26
华北 5（呼和浩特）	○ 100.104.234.192/26 ○ 100.104.26.128/26
中国香港	○ 100.104.153.64/26 ○ 100.104.65.192/26
亚太东南 1（新加坡）	○ 100.104.158.192/26 ○ 100.104.218.128/26
马来西亚（吉隆坡）	○ 100.104.240.128/26 ○ 100.104.127.0/26
印度尼西亚（雅加达）	○ 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。

参数	说明
库名称	输入您需要授权DSC访问的ECS自建数据库名称。 **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。
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**。

   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 odps.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。

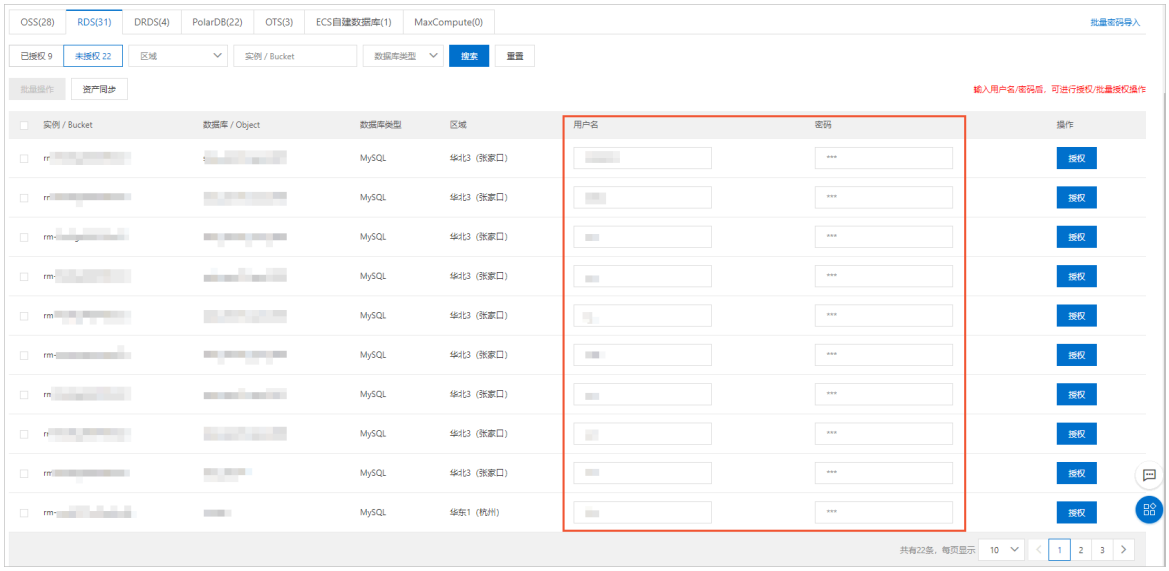
批量密码导入

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.全域数据审计

5.1. 审计报表

审计报表页面从资产管理和安全保障、异常和审计事件、安全性变化角度向您展示了您资产中存在的敏感信息的统计数据。本文介绍了审计报表页面展示的不同数据内容，帮助您更好地了解资产中存在的敏感数据。

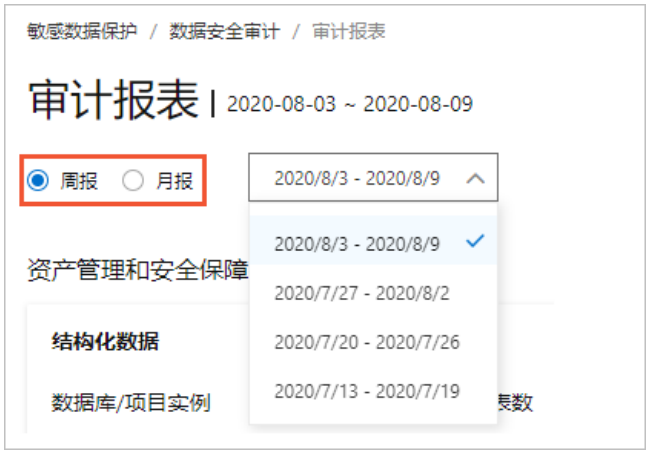
背景信息

智能审计每日自动更新审计报表，并为您展示上一周的报表统计数据。

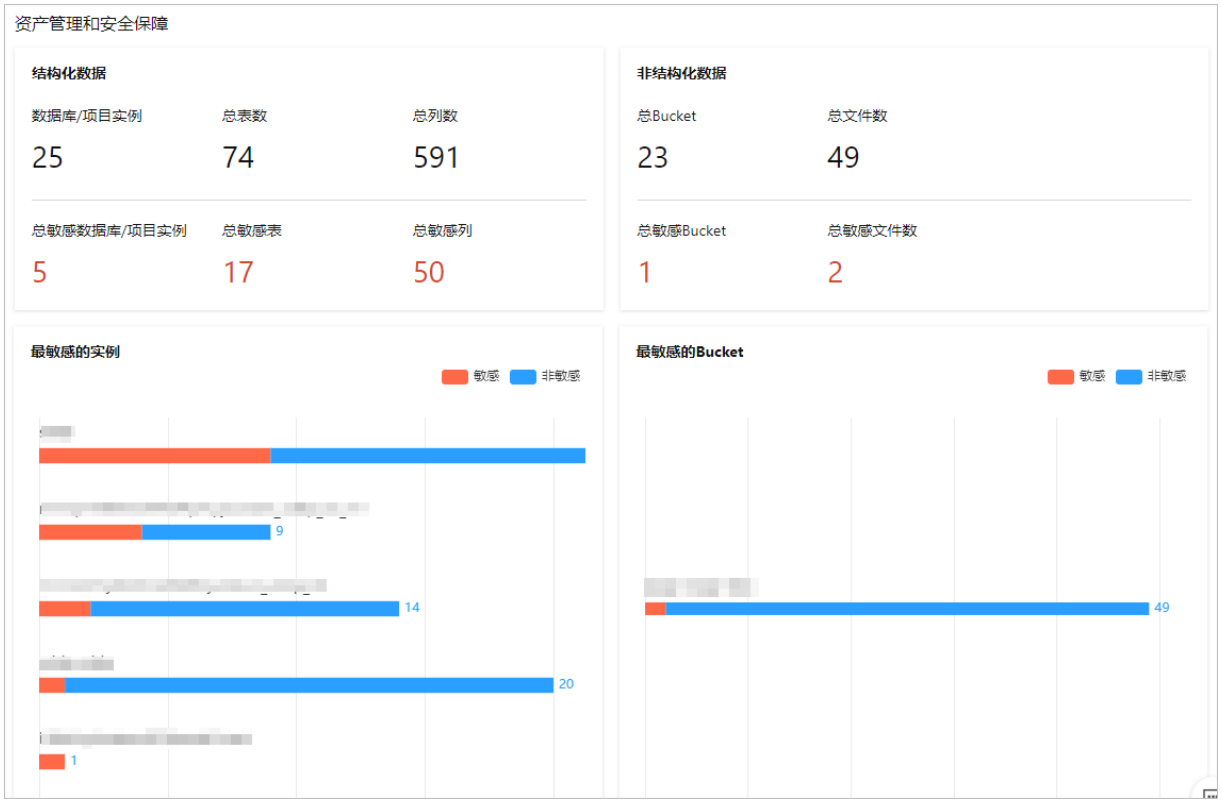
访问审计报表页面

1. 登录数据安全中心控制台。
2. 在左侧导航栏，选择**全域数据审计 > 审计报表**。
3. 在**审计报表**页面您可以查看以下模块的内容。
   - 资产管理和安全保障
   - 异常和审计事件
   - 安全性变化

     审计报表左上角展示了审计报表统计的时间范围。您可以选择**周报**或**月报**查看一周或一月的审计报表。



资产管理和安全保障



资产管理和安全保障展示您当前账号下资产的总数及包含敏感数据的资产数量，具体包含以下内容。

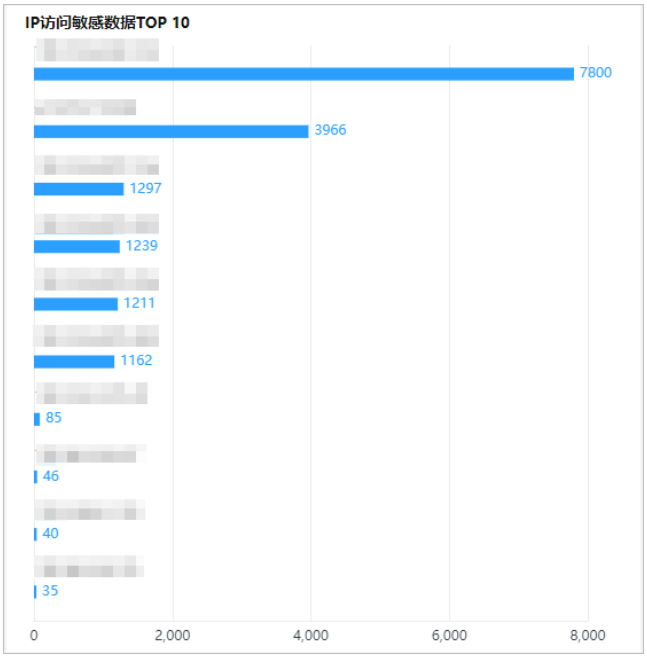
- **结构化数据**：展示您RDS、DRDS、PolarDB、OTS（表格存储）、ECS自建数据库和MaxCompute数据的总量和敏感数据的数量，包括**数据库/项目实例**总数、**总表数**、**总列数**、**总敏感数据库/项目实例**、**总敏感表**和**总敏感列**。
- **非结构化数据**：展示您OSS数据的总量及敏感数据的数量，包括总Bucket数、总文件数、总敏感Bucket数和总敏感文件数。
- **最敏感的实例**：展示您RDS、DRDS、PolarDB、OTS（表格存储）、ECS自建数据库和MaxCompute数据源中存在的敏感数据的实例或项目名称及每个敏感实例中敏感表和非敏感表的数量。
- **最敏感的Bucket**：展示您OSS数据中出现敏感数据的Bucket名称及每个敏感Bucket的敏感文件和非敏感文件数量。

异常和审计事件

异常和审计事件展示您当前账号下检测出的异常事件和审计风险的统计数据图表，具体包含以下内容。

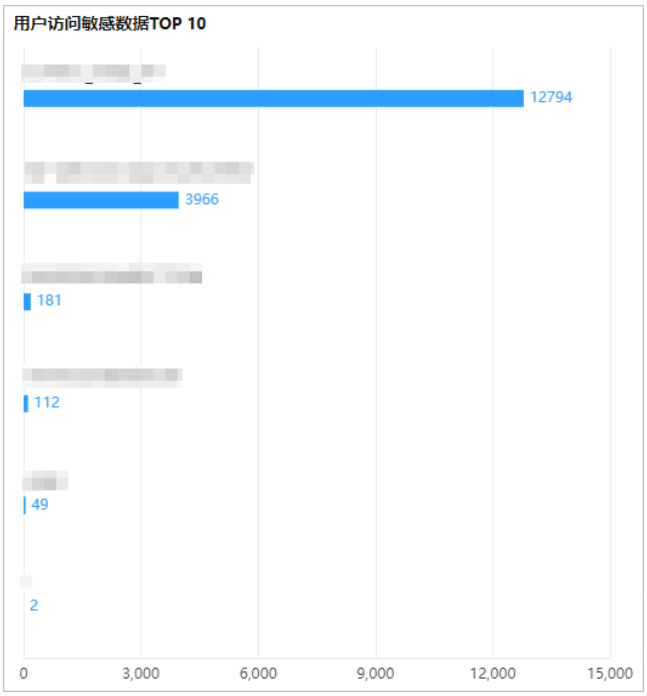
- **异常和审计事件分布**：展示您RDS、MaxCompute和OSS存储空间（Bucket）中异常事件和审计事件占统计数据的比例。

- **异常事件分类占比**：展示不同类型的异常事件在总异常事件中占比分布。已检测出的不同类型异常事件的详细信息请参见异常事件告警。
- **审计风险分布情况**：展示高、中、低类型的审计风险的分布情况。
- **IP访问敏感数据TOP 10**：展示访问敏感数据排名前10的IP地址及访问次数。



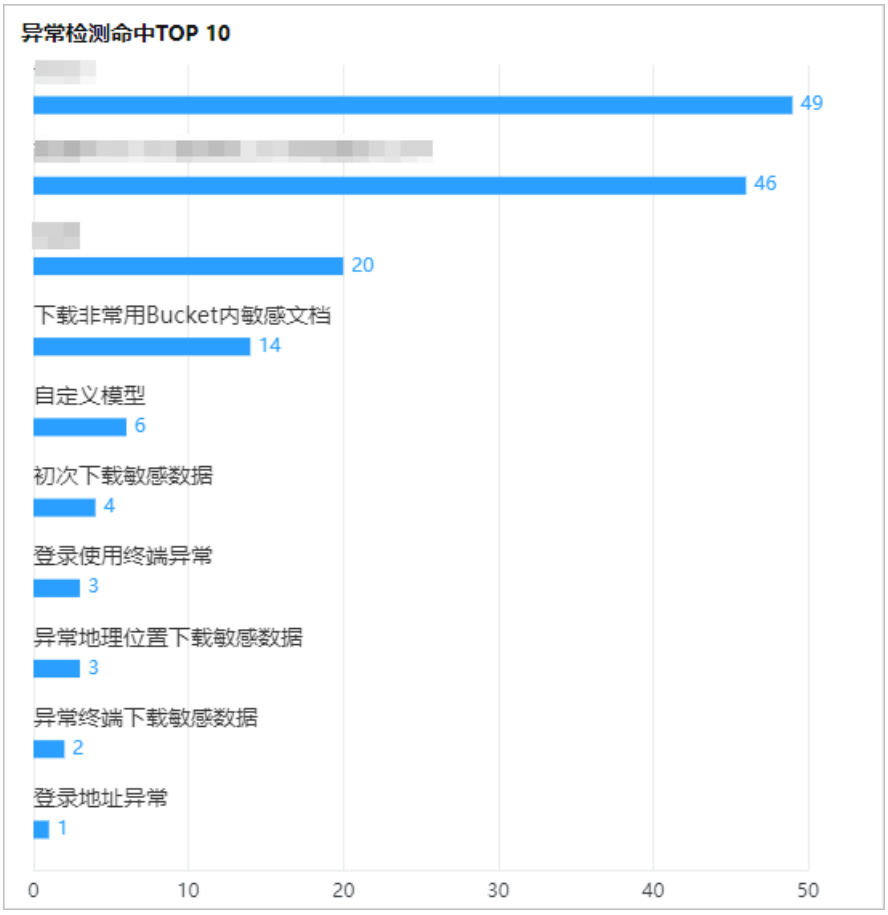
> **说明** 同一IP地址多次访问敏感数据，可能会造成敏感数据泄露，建议您重点关注及时排除数据泄露隐患。

- **用户访问敏感数据TOP 10**：展示访问敏感数据排名前10的用户名称及访问次数。

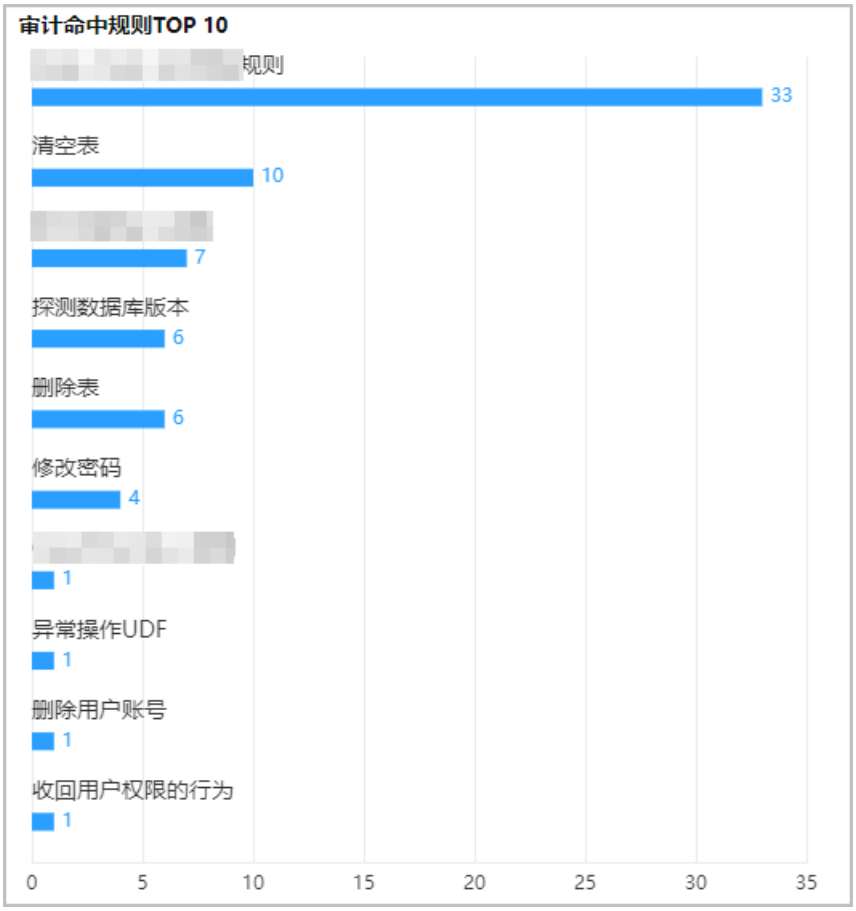


> **说明** 同一用户多次访问敏感数据，可能会造成敏感数据泄露，建议您及时排查访问授权配置是否正确。

- **异常检测命中TOP 10**：展示检测出命中次数排名前10的异常事件子类型名称及命中次数。处理异常事件的操作步骤，请参见处理异常事件。



- **审计命中规则TOP 10**：展示命中次数排名前10的审计规则名称及命中次数。审计规则的更多信息请参见创建审计规则。



安全性变化

安全性变化展示异常检测和审计规则检测出的新增异常事件的统计信息。具体包含以下内容。

- **安全异常**：展示异常检测检测出的新增异常事件、事件的风险类型和事件类型的统计数据。
- **安全审计**：展示审计规则检测出的异常事件、用户异常事件、IP异常事件和事件风险类型的统计数据。
- **安全性变化趋势图**：展示一周内每天新增的审计事件、异常事件和处理异常事件数量变化的曲线图，可

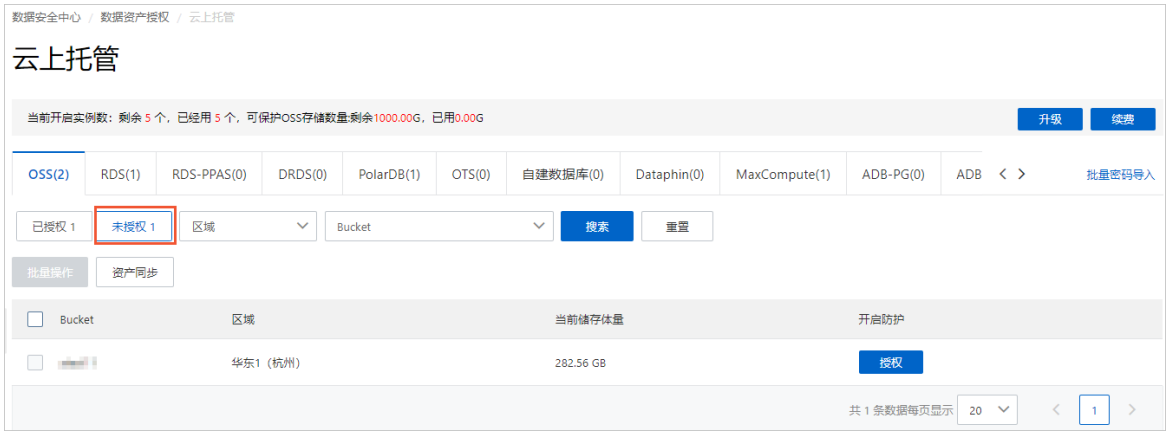
帮助您快速定位到新增异常事件和审计事件较多的日期，及时排查系统中存在的数据泄露风险。

5.2. 授权日志审计

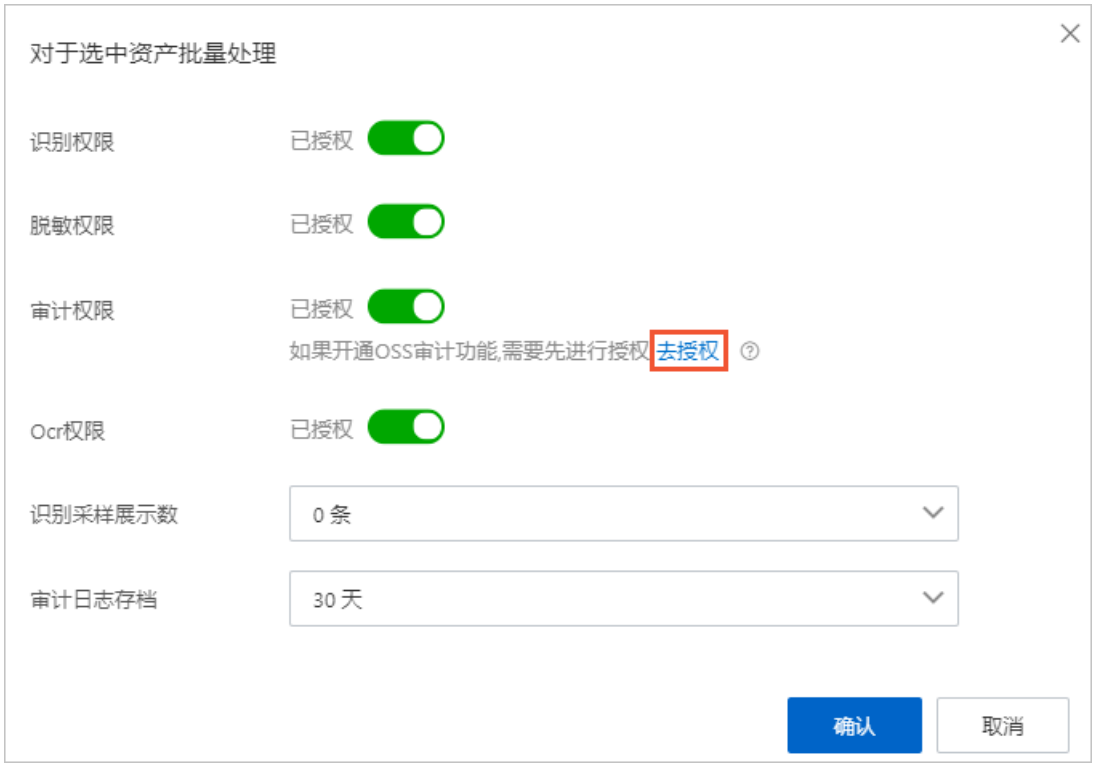
当数据资产类型为OSS时，为确保OSS审计日志功能正常开启，需先开通并授权OSS日志服务。本文介绍如何开通及授权OSS日志服务。

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**数据资产授权 > 数据资产授权**。
3. 在**云上托管**页面的OSS页签中，单击**未授权**。



4. 在资产列表中，定位到需要授权日志审计的资产，单击**开启防护**列的**授权**。
5. 在**对于选中资产批量处理**对话框中，单击**审计权限**下方的**去授权**。



执行此步骤后，控制台会跳转到**对象存储**服务的**实时查询**页面。

6. 在**对象存储**服务的**日志管理 > 实时查询**页签，单击**立即开通**。

系统将开通日志服务，页面将显示OSS操作审计界面。

5.3. 原始日志

原始日志页面展示了资产的实例、库、账号、源IP地址、返回行数、时间等日志信息，您可通过搜索功能查看原始日志及其详细信息。

背景信息

可以获取已完成扫描授权的资产相关的原始日志数据。

目前，DSC可获取OSS、RDS、OTS、自建数据库、DRDS、PolarDB、OceanBase、MaxCompute和MaxCompute-Audit产品相关操作的原始日志。支持的云产品操作类型的更多信息，请参见原始日志支持的操作类型说明。

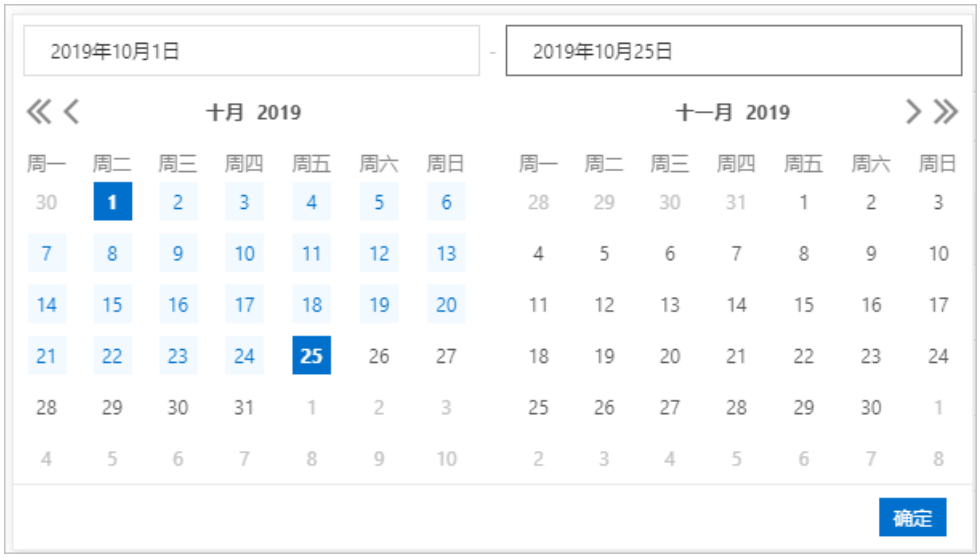
> **说明** MaxCompute页签展示了MaxCompute产品的数据下载日志，MaxCompute-Audit页签展示了MaxCompute产品的SQL操作日志。

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**全域数据审计 > 原始日志**。
3. 在**原始日志**页面，根据需要执行以下操作查看日志信息。

> 说明 原始日志页面默认显示最近1天的原始日志信息。

- **根据搜索功能定位查看相关审计日志**：可根据以下筛选条件查看相关日志。
  - **时间**：在日志列表上方，单击时间搜索框右侧的 图标，依次选择**开始时间**和**结束时间**，并单击**确定**。



  - **设置搜索条件**：在日志列表上方，输入实例、库、账号、项目等条件或选择操作类型，单击**搜索**。

> 说明
> - 不同的云产品支持的搜索条件不同，请您根据控制台实际显示的搜索条件进行搜索。
> - 搜索条件支持模糊查询。
> - 不同产品对应的操作类型说明的更多信息，请参见原始日志支持的操作类型说明。

- **查看日志详情**：在日志列表中，定位到目标资产的数据项，单击其**操作**栏的**详情**，查看日志详情，包括客户端信息、服务端信息和行为信息。

原始日志支持的操作类型说明

OSS

操作类型	说明
AbortMultiPartUpload	终止MultipartUpload事件。
AppendObject	以追加写的方式上传文件（Object）。
CompleteUploadPart	完成断点上传。
CopyObject	复制文件（Object）。
DeleteBucket	删除存储空间（Bucket）。
DeleteBucketEncryption	删除存储空间（Bucket）加密规则。
DeleteMultipleObjects	删除同一个存储空间（Bucket）中的多个文件（Object）。
DeleteObject	删除单个文件（Object）。
DeleteObjects	删除多个文件（Object）。
GetBucket	列举存储空间（Bucket）。

操作类型	说明
GetBucketAcl	获取存储空间（Bucket）权限。
GetBucketCors	查看存储空间（Bucket）的跨域资源共享（CORS）配置。
GetBucketEncryption	获取存储空间（Bucket）的加密规则。
GetBucketInfo	查看存储空间（Bucket）信息。
GetBucketLifecycle	查看存储空间（Bucket）的生命周期（Lifecycle）配置。
GetBucketLocation	查看存储空间（Bucket）地域。
GetBucketLog	查看存储空间（Bucket）访问日志配置。
GetBucketReferer	查看存储空间（Bucket）的防盗链（Referer）相关配置。
GetBucketReplication	查看跨地域复制。
GetBucketReplicationLocation	查看跨地域复制可同步的目标地域。
GetBucketReplicationProgress	查看跨地域复制进度。
GetBucketStat	获取存储空间（Bucket）的相关信息。
GetBucketWebSite	查看存储空间（Bucket）的静态网站托管状态。
get_image_info	获取图片的长宽等信息。
get_image_infoexif	获取图片的长宽以及exif信息。
GetObject	读取文件（Object）。
GetObjectAcl	获取文件（Object）访问权限。
GetObjectInfo	获取文件（Object）信息。
GetObjectMeta	查看文件（Object）元数据信息。
GetPartData	获取断点文件块数据。
GetPartInfo	获取断点文件块信息。
GetService	获取存储空间（Bucket）列表信息
HeadBucket	查看存储空间（Bucket）信息。
HeadObject	查看文件（Object）信息。
InitiateMultipartUpload	初始化断点上传文件。
ListCname	列举规范名称。

操作类型	说明
ListMultiPartUploads	列举断点事件。
ListParts	列举断点块状态。
list_style	列举存储空间（Bucket）的样式。
ListUserRegions	列举用户区域。
PostObject	使用HTML表单上传Object到指定存储空间（Bucket）。
ProcessImage	处理图片。
PutBucket	创建存储空间（Bucket）。
PutBucketAcl	设置或修改存储空间（Bucket）的访问权限（ACL）。
PutBucketEncryption	配置存储空间（Bucket）的加密规则。
PutObject	上传文件（Object）。
PutObjectAcl	修改文件访问权限。
PutObjectSymlink	创建Symlink文件。
RedirectBucket	Bucket Endpoint重定向。
UploadPart	断点上传文件。
UploadPartCopy	复制文件块。

RDS和DRDS

操作类型	说明
Alter	修改数据库。
Create	创建数据表。
CreateIndex	创建索引。
Delete	删除数据。
Drop	删除数据库。
DropIndex	删除索引。
Insert	插入数据。
Merge	合并数据。
Select	查看数据。

操作类型	说明
Update	修改数据。

OTS

操作类型	说明
ComputeSplitPointsBySize	将全表的数据在逻辑上划分成接近指定大小的若干分片。
GetRange	读取指定主键范围内的数据。
GetRow	根据指定的主键读取单行数据。
ListTable	获取当前实例下已创建的所有表的表名。
PutRow	插入数据到指定的行。

PolarDB

操作类型	说明
Alter	修改数据库。
Begin	开启事务（数据库Sesssion）。
Call	调用存储过程。
Commit	提交事务（数据库Sesssion）。
Create	创建数据表。
CreateIndex	创建索引。
Delete	删除数据。
Desc	在查询表信息时对查询结果进行降序排序。
Describe	查看特定表的详细设计信息。
Drop	删除数据库。
DropIndex	删除索引。
Flush	刷新操作。
Insert	插入数据。
Login	登录数据库。
Logout	登出数据库。
Merge	合并数据。

操作类型	说明
Replace	插入或替换数据。
Rollback	回滚事务（数据库Sesssion）。
Select	查看数据。
Set	设置变量。
Show	查看数据库相关信息。
Start	启动数据库。
Update	修改数据。

MaxCompute和MaxCompute-Audit

操作类型	说明
DOWNLOAD	下载操作。
UPLOAD	上传操作。
Alter	修改数据库。
Create	创建数据表。
Delete	删除数据。
Drop	删除数据库。
Insert	插入数据。
Select	查看数据。

5.4. 会话信息

会话信息页面展示登录您RDS和PolarDB数据库的会话信息。本文介绍如何查看登录RDS和PolarDB的会话。

背景信息

如果您发现RDS和PolarDB数据库被异常登录或修改，您可以在**数据安全审计 > 会话信息**页面查看数据库登录会话的详细记录。

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**全域数据审计 > 会话信息**。
3. 在**RDS**或**PolarDB**页面设置搜索条件并单击**搜索**。

支持设置以下搜索条件：

- **时间**：设置需要搜索的会话的开始时间和结束时间。
- **账号**：输入登录数据库的账号名称。支持模糊搜索。
- **IP**：输入登录会话使用的IP地址。请输入完整IP地址，不支持模糊搜索。
- **实例**：输入实例名称。支持模糊搜索。

4. 定位到目标会话，单击操作列下的**详情**。
5. 在**详情**页面，查看当前会话的详细信息。

   您可以查看登录源IP地址、登录时间、登出时间、会话时长等详细信息。

5.5. 异常告警

异常告警页面展示了资产命中审计规则结果、命中规则的操作类型和操作账号等事件信息，您可通过搜索功能查看告警事件及其详细信息。

背景信息

可根据系统内置的默认审计规则或自定义的审计规则抓取对应的异常告警事件数据。 更多信息，请参见创建审计规则。

> **说明** 目前，DSC支持查看来自OSS、RDS、OTS（表格存储）、MaxCompute、DRDS、PolarDB、ADB-PG（分析型数据库PostgreSQL版）、OceanBase数据源的异常告警事件。

操作步骤

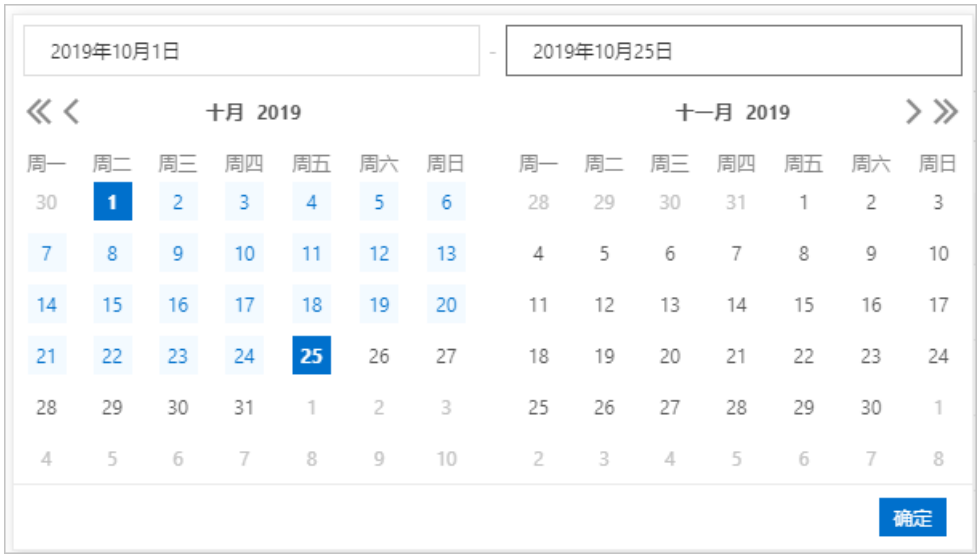
1. 登录数据安全中心控制台。
2. 在左侧导航栏，选择**全域数据审计 > 异常审计告警**。
3. 在**异常审计告警**页面，单击指定数据源的页签。
4. 在指定数据源页签中，根据需要执行以下操作查看异常告警信息。

   > **说明** 异常审计告警页面默认展示最近1天的异常告警信息。

   - **根据搜索功能定位查看相关异常告警**

     可根据以下筛选条件查看相关异常告警：

- **时间**：在告警事件列表上方，单击时间搜索框右侧的 图标，依次选择**开始时间**和**结束时间**，并单击**确定**。

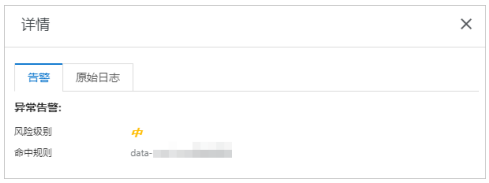


- **搜索事件**：在事件列表上方，输入**账号**、**实例/桶**或选择**风险级别**（高、中、低），单击**搜索**。

> **说明** 账号和实例/桶支持模糊搜索。

- **查看事件详情**：在事件列表中，定位到目标事件项，单击其**操作**栏的**详情**，查看异常告警详情和原始日志信息。
  - **告警**

    在**告警**页签可以查看敏感数据风险级别和命中规则的信息。



- **原始日志**

  单击**原始日志**页签，可以查看客户端信息、服务端信息和行为信息的详情。

5.6. 创建审计规则

您可以在数据安全中心DSC（Data Security Center）中基于自己的需求创建审计规则，来获取对应的审计日志数据。本文介绍了如何创建审计规则。

背景信息

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。更多有关DSC内置的安全审计规则信息，请参见内置的安全审计规则。

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**云原生数据审计 > 审计规则**。
3. 在**审计规则**页面单击**自定义规则**页签，然后单击**新增规则**。
4. 在**新增规则**面板配置审计规则参数，如下图所示。

您可以参考以下表格中的参数说明配置审计规则参数。

参数	说明
规则名称	自定义审计规则的名称，建议输入有实际意义的名称以便有效识别审计规则。
规则类型	从下拉列表中选择审计规则类型，支持选择以下类型： ○ **SQL注入尝试利用** ○ **SQL注入尝试绕过** ○ **存储过程滥用** ○ **缓冲区溢出** ○ **基于报错的SQL注入** ○ **基于布尔值的SQL注入** ○ **基于时间的SQL注入** ○ **拒绝服务漏洞** ○ **数据库探测** ○ **配置操作** ○ **其他**
风险级别	从下拉列表中选择审计规则的风险等级，支持选择以下风险级别： ○ **高** ○ **中** ○ **低**

参数	说明
资产类型	从下拉列表中选择审计规则生效的资产类型，支持选择以下资产类型： ○ OSS ○ RDS ○ OTS ○ MaxCompute ○ DRDS ○ PolarDB ○ ADB-PG ○ ADB-MYSQL ○ MongoDB ○ OceanBase ○ Redis ○ Dataphin
行为信息	输入审计规则的说明信息。
规则描述	您可以根据实际需要配置规则条件，DSC将在规则条件限定范围内采集审计数据。
添加	点击**添加**，完成规则配置。支持添加多条规则。

5. 单击**提交**。
   审计规则列表页面出现创建的审计规则，审计规则的状态默认为开启。

后续步骤

创建并开启审计规则后，DSC将在5分钟内同步审计结果。您可以执行以下操作。

- 在**审计规则**列表中查看审计规则的开启状态、命中次数和详情信息，或修改审计规则。您可以手动开启或关闭审计规则。关闭审计规则后，DSC不会再执行审计规则项抓取审计日志数据。
- 在**异常审计告警**页面查看相关告警数据。更多信息，请参见异常告警。

5.7. 异常事件告警

可检测敏感数据相关的异常操作并提供告警信息。

背景信息

异常事件告警分为4大类：

- **权限使用异常**：不规范的权限使用情况，例如：登录地址异常、使用其他人的AccessKey进行登录等。
- **数据流转异常**：数据在流转过程中出现的异常情况，例如：下载非常用敏感数据文件、异常时间下载敏感数据文件等。
- **数据操作异常**：非正常的数据操作，例如：敏感数据字段变更等。
- **自定义异常**：根据您自定义的异常事件规则检测并告警对应的异常事件。更多信息，请参见自定义异常事件规则。

DSC内置的异常检测规则详情，请参见内置的异常检测规则。

步骤一：查看异常事件告警

1. 登录数据安全中心控制台。
2. 在左侧导航栏，选择**全域数据审计 > 异常事件告警**。
3. 在**异常事件告警**页面查看异常事件告警的统计结果和列表信息。

   您可以单击**权限使用异常**、**数据流转异常**、**数据操作异常**或**自定义异常**切换到对应异常事件告警类型页面，查看以下信息：

   - 在页面上方查看不同异常事件告警类型的统计数据，包括异常事件告警类型及未处理、已处理和确认误报的异常事件告警数量。
   - 在**异常事件告警**页面下方查看已检测出的异常事件告警列表信息。您可根据**事件类型**、事件的**所处状态（待处理、已处理、确认误报）**和**告警时间**筛选定位到您需要查看的异常事件告警。

     > **说明** **告警时间**范围的设置无限制。

步骤二：处理异常事件告警

您可在**异常事件告警**页面下方的异常事件告警列表中，查看异常事件告警详情和处理DSC检测到的异常事件告警。

您可以进行以下操作：

- 查看异常事件告警详情：单击异常告警事件操作列的**查看详情**展开异常事件告警详情页面。您可在该页面查看异常事件告警的基本信息、所属的云产品信息、异常操作描述和异常处理建议方案等。

- 导出异常事件告警：选择**事件类型**、**所处状态**、**起始日期**和**结束日期**后，单击**导出**可以导出满足搜索条件的异常告警列表。
- 处理异常事件告警：单击异常事件告警操作列的**处理**展开**异常事件告警**面板，对异常事件告警进行处理。

  异常事件告警通常是非法用户在未经授权的情况下对敏感数据进行了访问、下载，或合法用户在非正常时间对敏感数据进行了访问、下载，以及访问敏感数据的用户登录终端异常等情况。DSC检测到敏感数据相关的异常情况后，会将检测结果展示在**异常事件告警**页面中。

您可在**异常事件告警**页面处理异常事件告警。您需要设置以下参数：

- **事件核查结果**
  - **确认异常并已处理**：如果您确认该检测结果确实为异常事件，选择该选项，并需要您根据**异常事情详情**页面提示的信息，定位到该异常事件的位置，并根据**事件处置建议方案**在对应的云产品中进行手动处理。确认违例的事件如未被处理，DSC将会一直对该事件进行异常事件告警。
  - **误报**：如果您确认该检测结果属于正常操作、无需进行处理，选择该选项。异常事件设为误报后，DSC将不再对该事件进行告警提示，即该事件将不会展示在异常事件告警列表中。
- **处理方式**：开启对异常事件告警的处理方式，例如开启账号禁用、移除白名单开关。
- **添加事件处理记录**：填写您对该异常事件告警的备注信息，方便后续回溯。
- **异常事件检测强化**：您确认该检测结果属于正常操作时事件核查结果选择**误报**，并选择**异常事件检测强化**后，DSC会将该异常事件输入到误报样本库中用于优化异常事件告警命中准确率。

5.8. 自定义异常事件规则

支持自定义异常事件检测规则并提供告警。SDDP会根据您自定义的异常事件规则抓取对应的异常事件日志数据。本文介绍了如何创建异常事件自定义规则。

背景信息

DSC支持根据系统内置的规则（更多信息，请参见内置的异常检测规则）和用户自定义规则检测异常事件并提供告警。

> **说明** 目前，仅OSS、MaxCompute和RDS支持自定义异常事件检测规则，其余云产品仅支持使用系统内置的规则检测异常事件。

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**全域数据审计 > 自定义异常事件规则**。
3. 单击**新增规则**。
4. 在**新增规则**面板配置自定义规则相关参数。

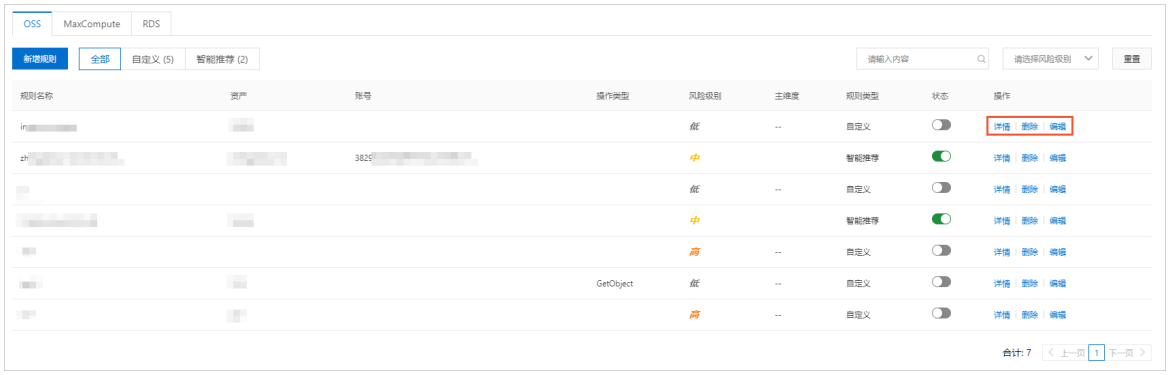
您可以参考以下表格配置自定义规则的参数。

参数	说明
规则名称	自定义异常事件检测规则的名称，建议输入有实际意义的名称以便有效识别该规则。
风险级别	从下拉列表中选择该异常事件规则的风险等级，可选以下3种风险等级： ○ **高** ○ **中** ○ **低**

参数	说明
资产类型	异常事件规则检测的资产类型，可选以下3种资产： ○ **OSS** ○ **MaxCompute** ○ **RDS**
过滤条件	根据实际需要配置过滤条件，指定需要检测的异常事件。每个过滤条件之间是和（AND）关系。例如：过滤出OSS产品中**识别结果**为**身份证（中国内地）**的日志。
添加	单击**添加**，完成过滤条件的配置。支持添加多条过滤条件。
告警条件	设置告警检测的时间单位和告警产生的条件。DSC基于上一步中过滤的数据进行异常检测，在自定义时间段内满足告警条件，将触发异常事件告警。 **说明** 告警条件中的**任何UA**是指任何浏览器的UserAgent。UserAgent的信息包括硬件平台、系统软件、应用软件和用户个人偏好，通过UA可以分析出浏览器名称、浏览器版本号、渲染引擎、操作系统。告警条件选择了**任何UA**，可以抓取UserAgent中的相应异常事件。

5. 单击**确定**，完成异常事件规则的创建。

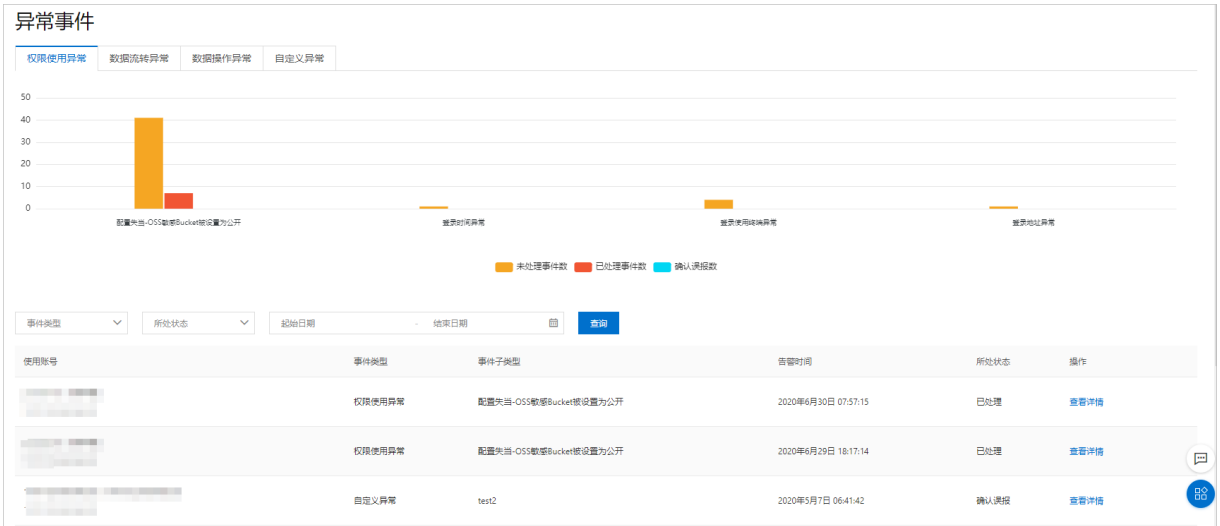
   异常事件规则创建完成后，您可以在规则列表中查看该异常事件检测规则的开启状态、命中结果和详情信息，或编辑该检测规则。



说明 已创建异常事件规则的**状态**默认为**开启**。您也可在**自定义规则**列表中手动关闭该规则。关闭该规则后，DSC将不会再用该规则项进行检测。

后续步骤

创建并开启异常事件规则后，DSC将在1小时左右同步检测结果，您可在**异常事件处理**页面查看相关数据。更多信息，请参见异常事件告警。



5.9. 内置检测模型

根据内置和自定义的检测规则对文件或表中的敏感数据进行识别和告警。您可以在内置检测模型页面，配置异常告警通用规则并启用异常告警配置。本文介绍如何进行异常告警配置。

异常告警通用配置

1. 登录数据安全中心控制台。
2. 在左侧导航栏，选择**全域数据审计 > 内置异常事件规则**。
3. 在**内置检测模型**页面，定位到**异常告警通用配置**区域，单击异常告警通用配置项右侧的**修改**。
4. 设置触发告警的异常事件的阈值。

   支持设置以下事件的阈值：

   - **非授权资源多次访问尝试**：设置阈值后，如果非授权资源访问敏感数据的尝试次数超过了阈值定义的次数，并且您已在**异常告警启用配置**区域启用了该配置项，DSC将会为您提供该异常事件告警。您可以在**异常事件**页面查看具体的告警信息。更多信息，请参见异常事件告警。
   - **权限闲置期间超过阈值**：设置阈值后，如果权限闲置的时长超过了阈值定义的时长，并且您已在**异常告警启用配置**区域启用了该配置项，DSC将会为您提供该异常事件告警。您可以在**异常事件**页面查看具体的告警信息。
   - **日志未有效输出**：设置阈值后，如果日志的输出量低于阈值定义的百分比，并且您已在**异常告警启用配置**区域启用了该配置项，DSC将会为您提供该异常事件告警。您可以在**异常事件**页面查看具体的告警信息。
5. 单击**提交**。

异常告警启用配置

1. 登录数据安全中心控制台。
2. 在左侧导航栏，选择**全域数据审计 > 内置异常事件规则**。
3. 在**内置检测模型**页面，定位到**异常告警启用配置**区域，选中需要DSC识别的异常事件类型。

   被选中的事件类型如果触发了告警条件，对应的告警信息将展示在**异常事件**页面的列表中。更多信息，请参见异常事件告警。

6.敏感数据发现

6.1. 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**

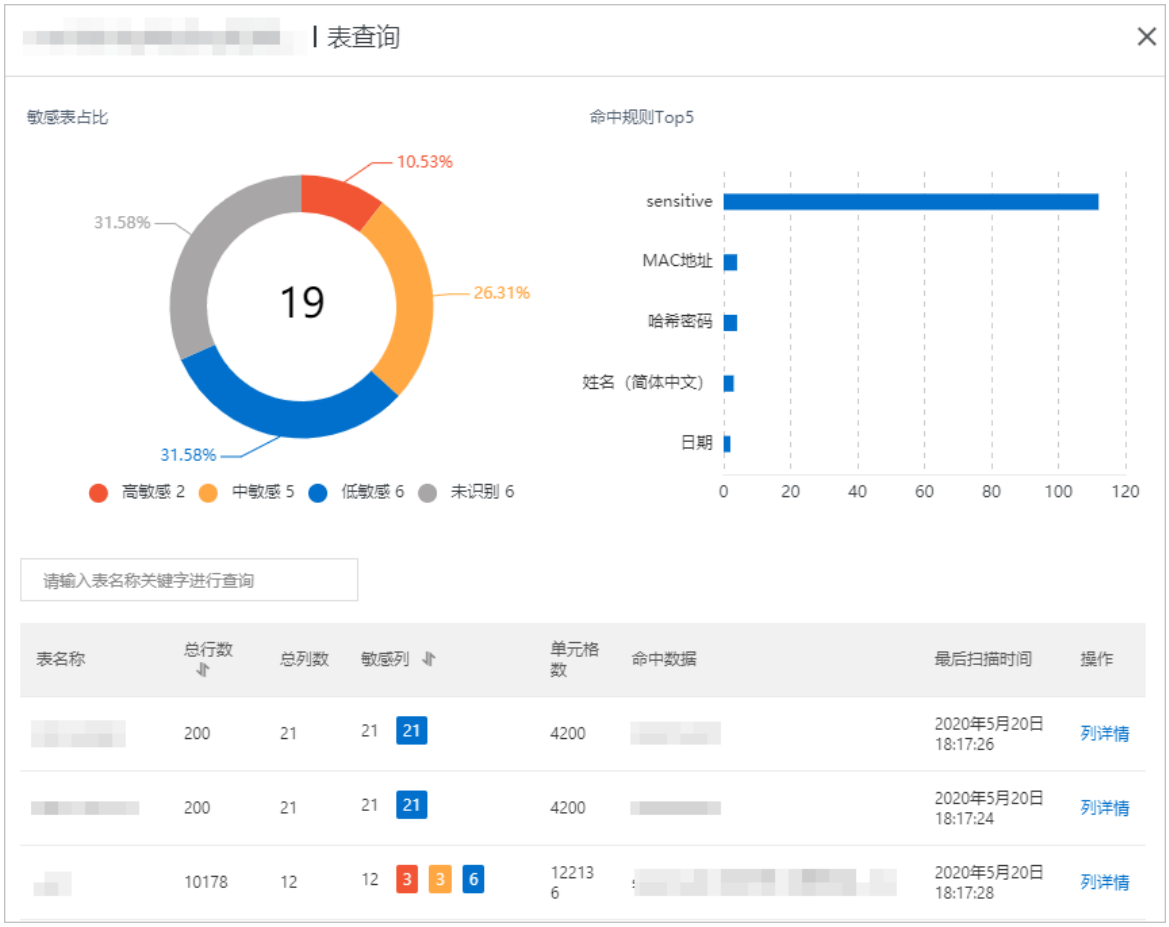
  在**命中规则Top 5**区域，您可以查看命中敏感数据次数排名前5的规则名称及命中次数。

- **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**

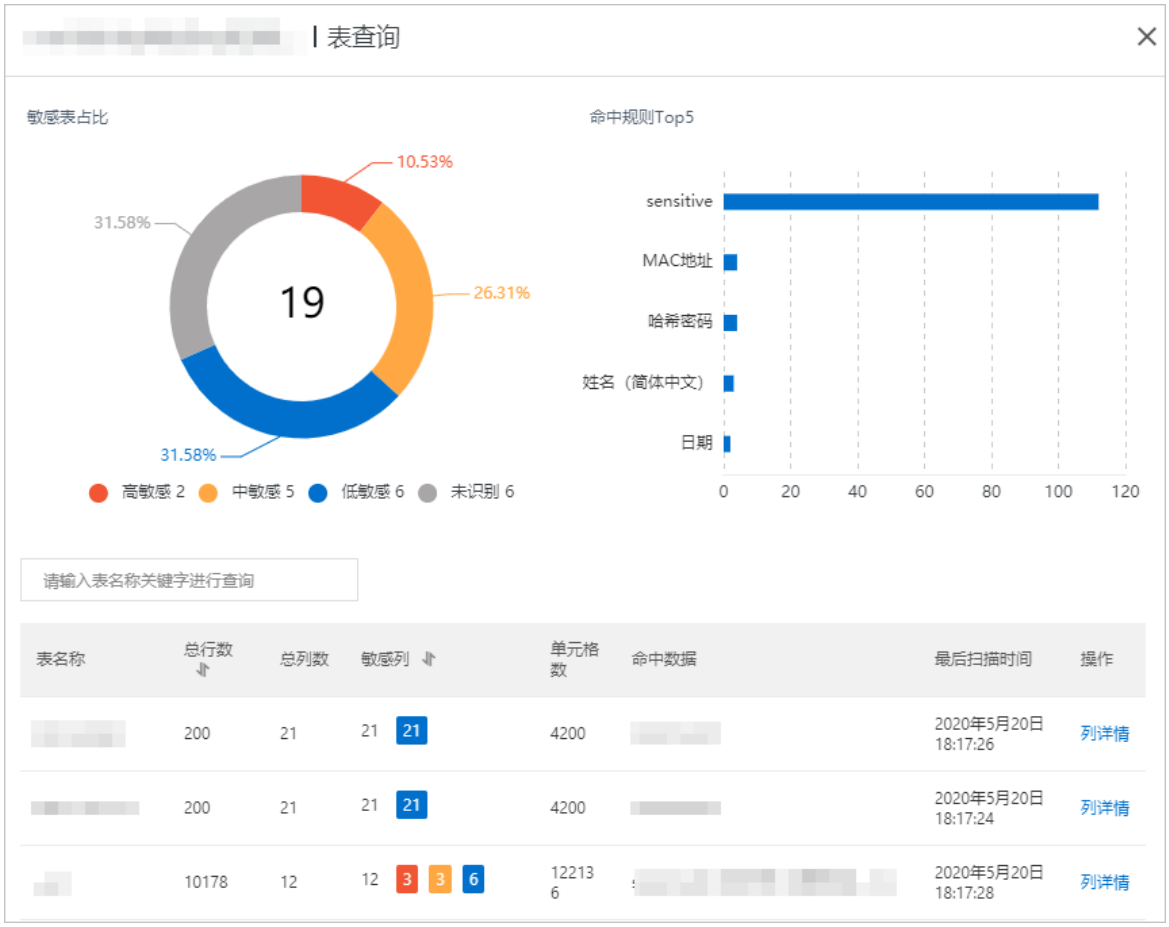
  在**命中规则Top 5**区域，您可以查看命中敏感数据次数排名前5的规则名称及命中次数。

- **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**

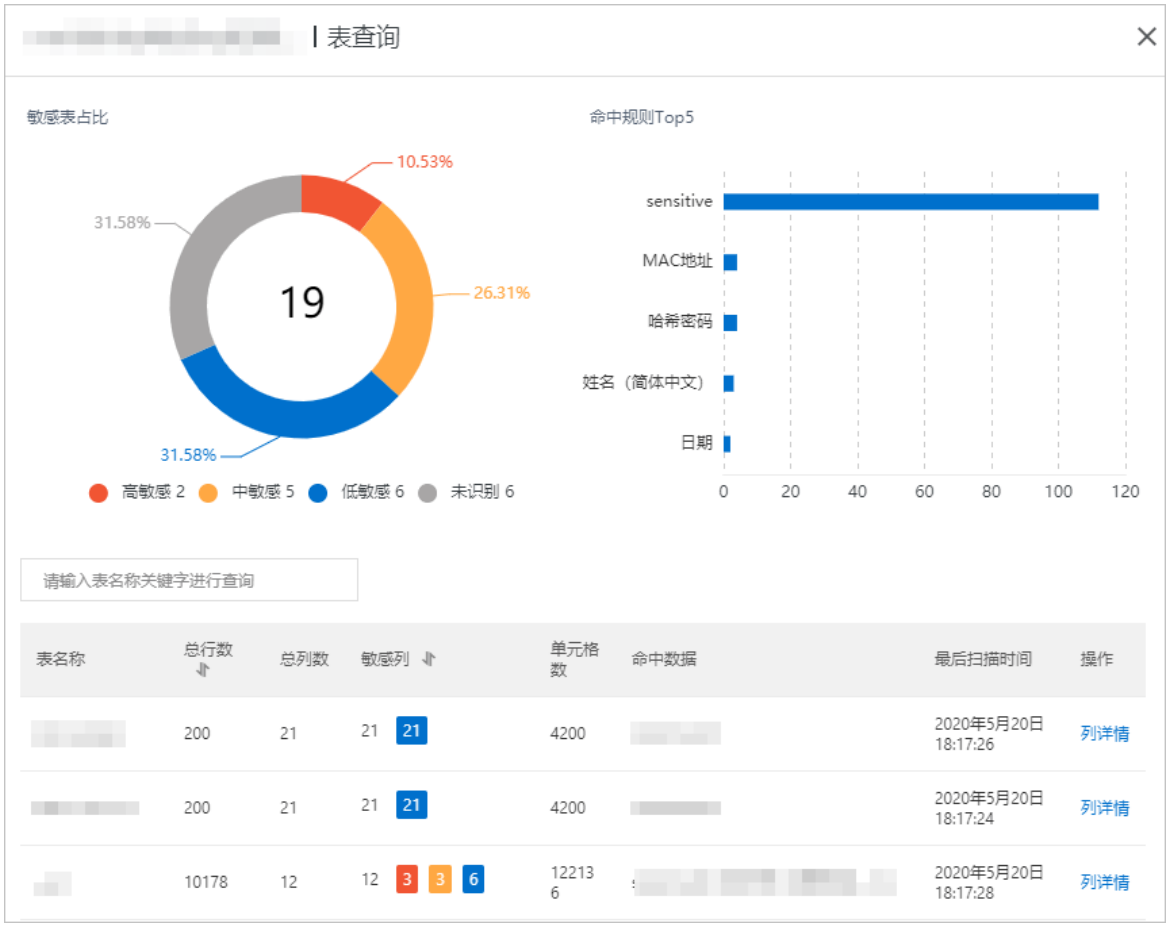
  在**命中规则Top 5**区域，您可以查看命中敏感数据次数排名前5的规则名称及命中次数。

- **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**

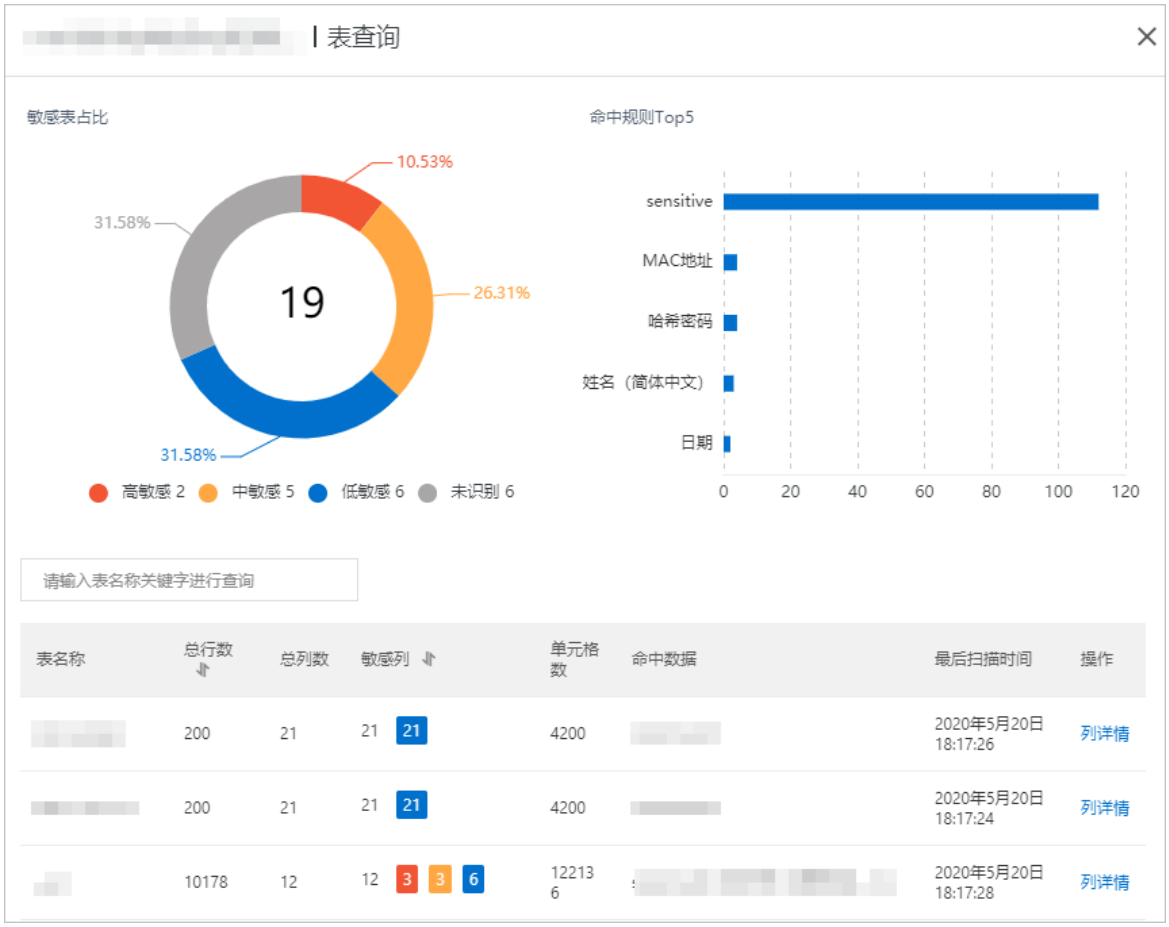
  在**命中规则Top 5**区域，您可以查看命中敏感数据次数排名前5的规则名称及命中次数。

- **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**

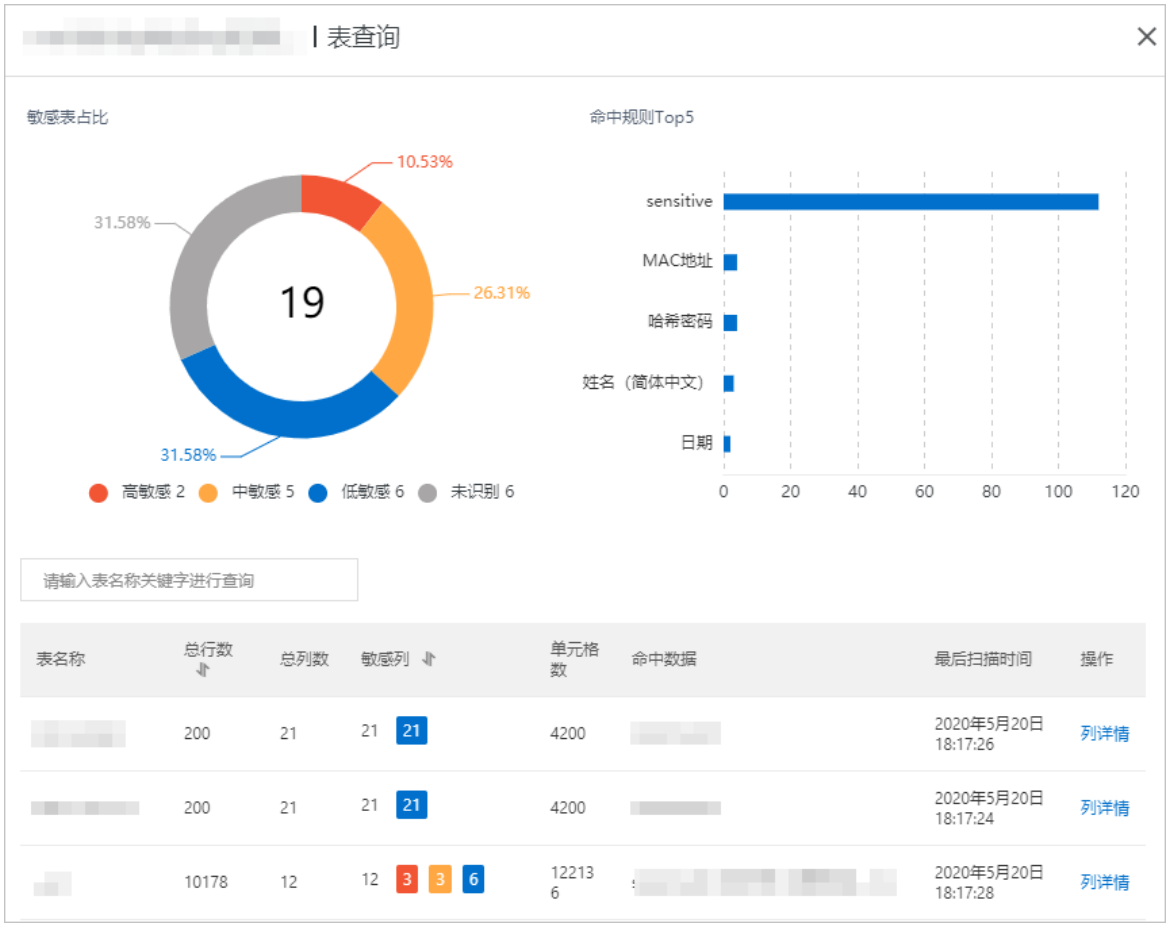
  在**命中规则Top 5**区域，您可以查看命中敏感数据次数排名前5的规则名称及命中次数。

- **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。

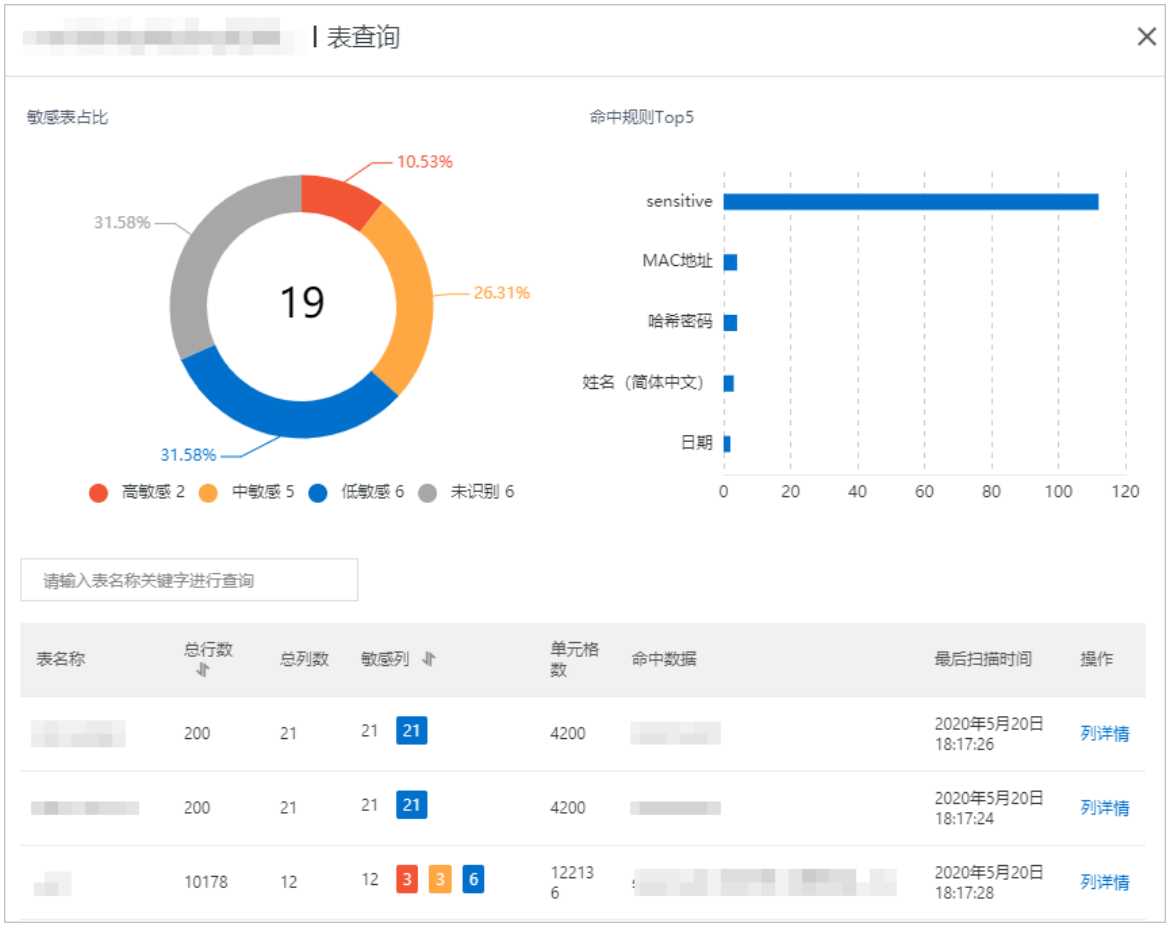
- **查看存在敏感数据的表**

  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

6.2. 导出敏感数据资产

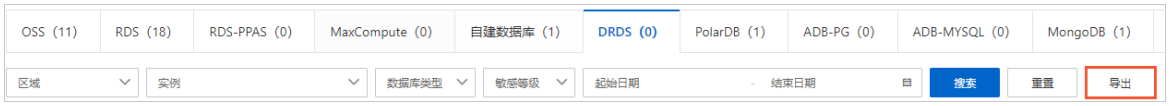
当借助数据安全中心DSC（Data Security Center）检测出数据源的敏感数据资产后，您可以将敏感数据资产以CSV格式导出，从Bucket、表、集合的维度查看导出的敏感数据资产。

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）*。

6.3. 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。

6.4. 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。

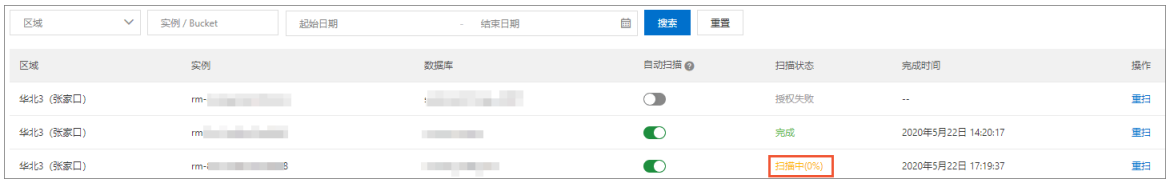
> **说明** DSC支持包年包月（预付费）的计费方式，进行重扫不会产生额外的费用。计费更多信息，请参见包年包月计费。

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**。



6.5. 管理识别模型

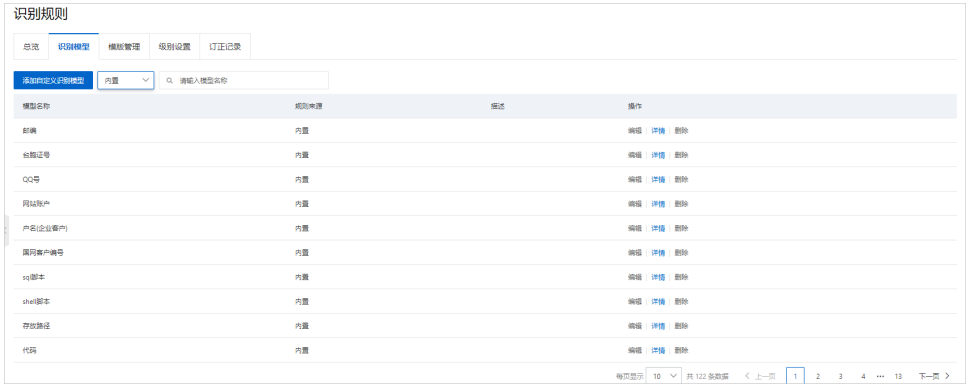
识别模型定义了识别您资产中敏感数据的具体规则。提供了识别典型敏感数据的内置识别模型，并支持自定义识别模型，您可以通过使用内置和自定义的识别模型构建专属的敏感数据识别能力。本文介绍如何查看内置识别模型、添加、编辑和删除自定义识别模型。

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。

6. 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。

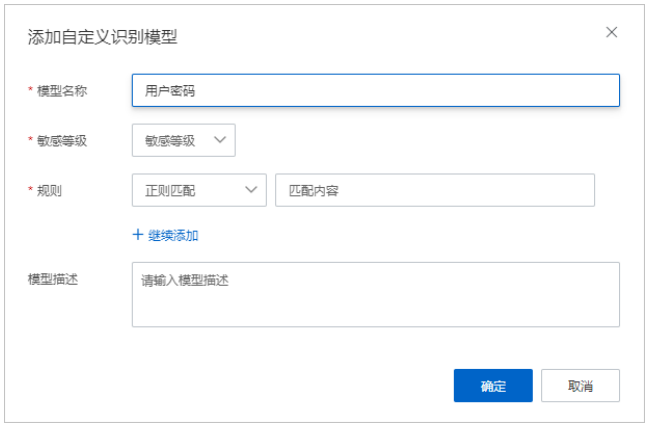
7. 在 **查看内置识别模型**对话框，查看该内置识别模型的详细信息。

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。待确认为什么不支持查看规则的详细信息。

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。

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. 在**识别模型**页签下，单击**添加自定义识别模型**。
5. 在**添加自定义识别模型**对话框，配置以下参数。



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	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： ○ **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 **说明** S1至S5的敏感等级依次升高，S5为最高敏感等级。待确认自定义模板是否可以添加敏感等级，待级别设置文档更新后，增加到级别设置文档的链接。
规则	设置敏感数据的识别规则。可选： ○ **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： ■ *Exampleoo+a*：表示Exampleooa、Exampleoooa、Exampleooooooa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。 ■ *Exampleoo*a*：表示Exampleoa、Exampleooa、Exampleooooooa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，也可以出现一次或多次。 ■ *Exampleo?a*：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。 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。 **注意** ○ 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。

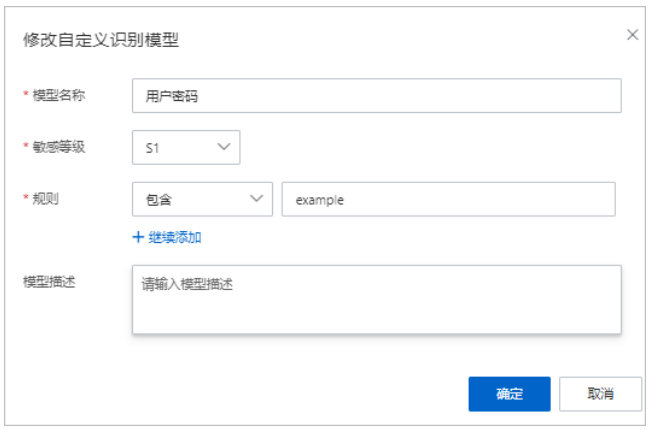
1. 登录数据安全中心控制台。
2. 在左侧导航栏，选择**敏感数据发现 > 识别规则**。
3. 在**识别规则**页面，单击**识别模型**页签。
4. 将搜索条件**规则来源**设置为**自定义**。
5. 定位到待操作的识别模型，执行以下操作。
   - **查看自定义识别模型详情**

     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。

7.数据脱敏

7.1. 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。

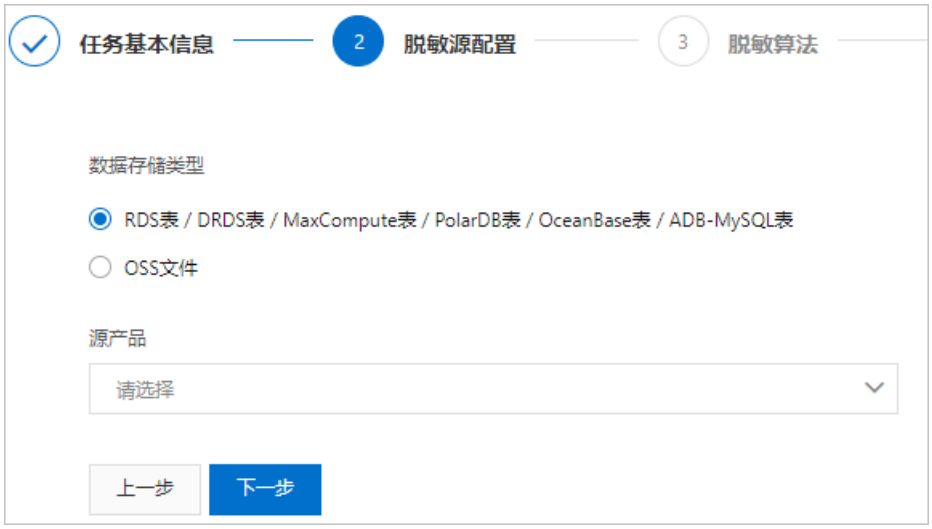
> **说明** 目前，DSC支持对OSS文件、RDS表、MaxCompute表、PolarDB表、OceanBase表等进行静态脱敏，具体请参见支持的数据库类型。

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。



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	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。 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。 说明 ■ **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。
抽样SQL	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。 说明 **源产品**选择MaxCompute和PolarDB时，无需配置**抽样SQL**。

- **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**。 **说明** 本地上传仅支持结构化TXT、CSV、XLSX和XLS格式文件。
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。 **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*test*.xls*。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。
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： - **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。

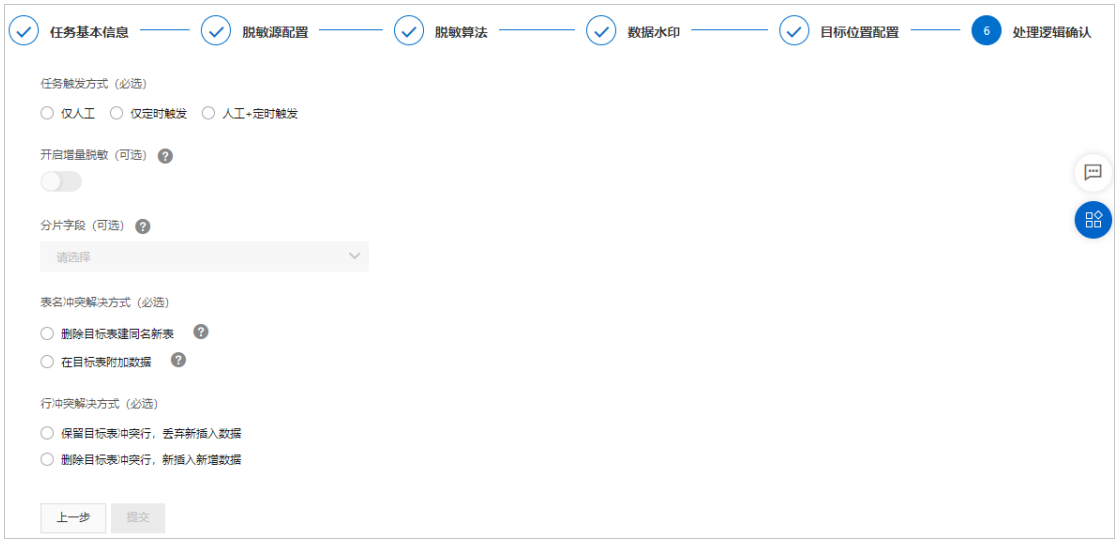
对进行分发的数据添加水印后，可以实现泄露数据溯源。水印添加成功后，自定义的水印信息将嵌入到数据库的数据中。

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填加到数据里。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	触发方式表示执行脱敏任务的方式。可选项： ■ **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	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。 **说明** 当前仅有RDS数据支持增量脱敏。
分片字段	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。 **说明** ■ 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	表名称存在冲突的情况下处理的方式。可选项： ■ *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	表中的行内容存在冲突的情况下处理的方式。可选项： ■ *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。

> **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。

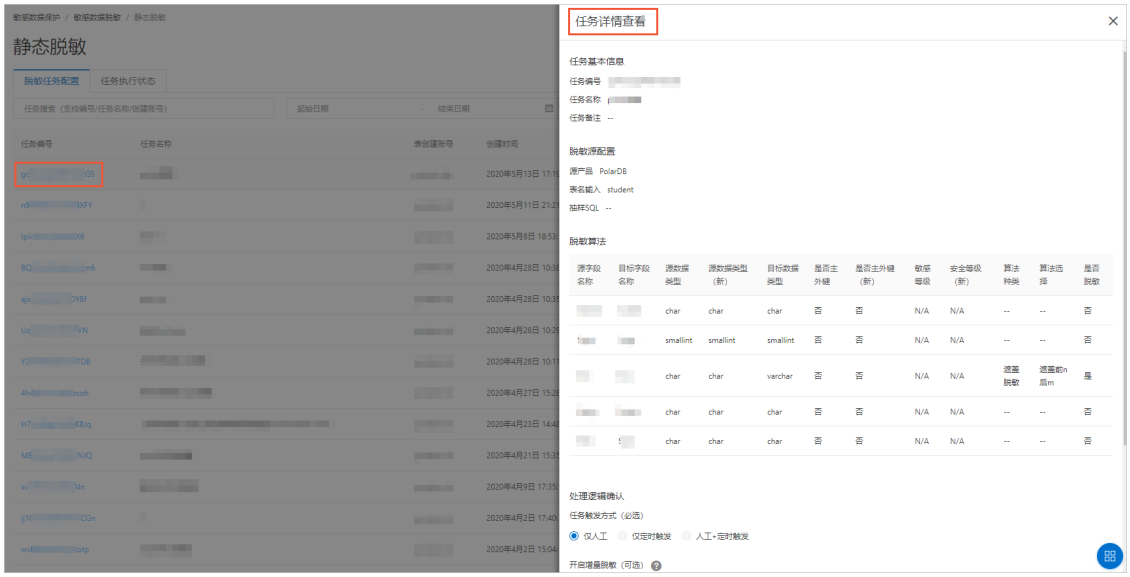
分区写法参考

分区类型	分区写法	分区示例
后N周	自定义分区字段名称=$[yyyymmdd+7*N]	time=$[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=$[yyyymmdd-7*N]	time=$[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=$[yyyymmdd+N]	time=$[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=$[yyyymmdd-N]	time=$[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。

7.2. 动态脱敏

您可以通过调用ExecDatamask接口对数据进行动态脱敏。

背景信息

您可以通过调用ExecDatamask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ExecDatamask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ExecDatamask接口的详细操作记录。

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**。

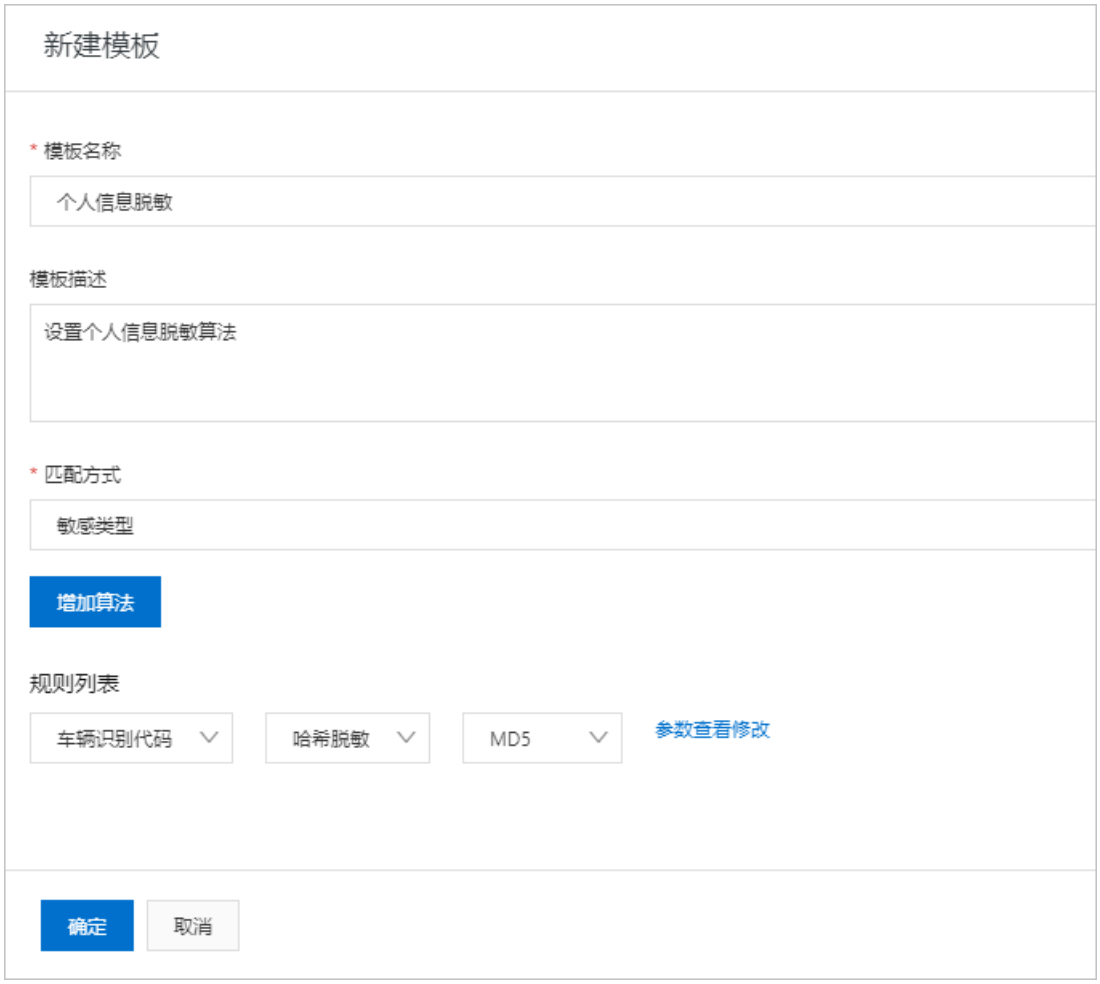
7.3. 脱敏模板

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。

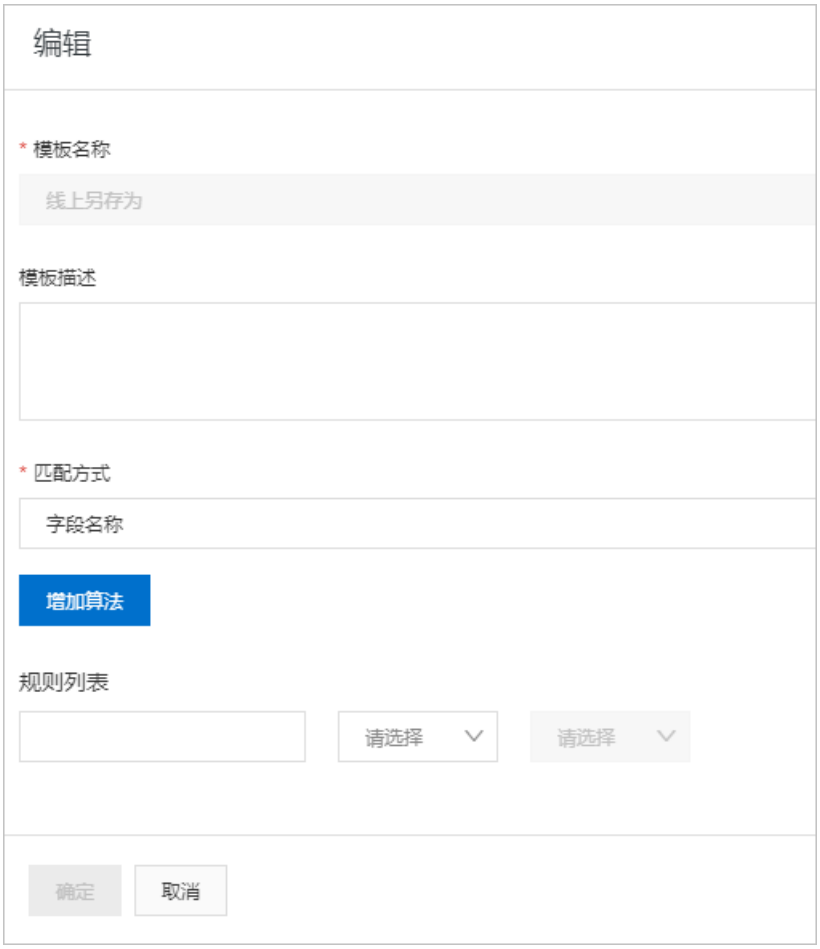


参数	说明
模板名称	脱敏模板的名称。
模板描述	脱敏模板的相关信息。您可以在此输入脱敏模板的使用范围等关键信息。
匹配方式	选择一种敏感数据的匹配方式，可以选择以下方式： ○ **敏感类型**：选择DSC支持的敏感数据类型并设置相应的脱敏算法，例如车辆识别代码、统一社会信用代码等。 ○ **字段名称**：指定需要脱敏的字段名称并设置相应的脱敏算法。
规则列表	在规则列表中选择敏感类型或输入需要进行脱敏的字段，设置您需要使用的脱敏算法。DSC支持以下脱敏算法： ○ 哈希脱敏 ○ 遮盖脱敏 ○ 替换脱敏 ○ 变换脱敏 ○ 加密脱敏 ○ 洗牌脱敏 ○ 数据解密 更多信息，请参见支持的数据脱敏算法。 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。

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。



- **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。

7.4. 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。

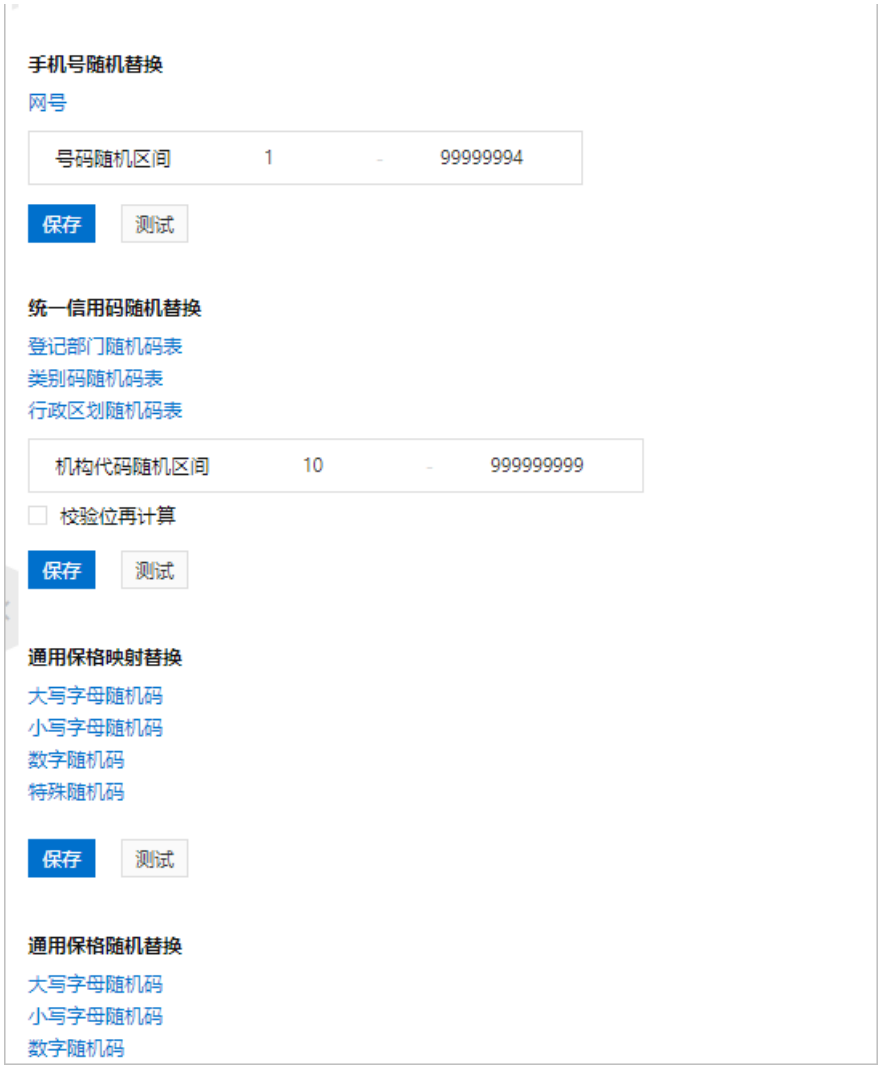
     

   - **遮盖脱敏**：设置遮盖脱敏算法的参数。

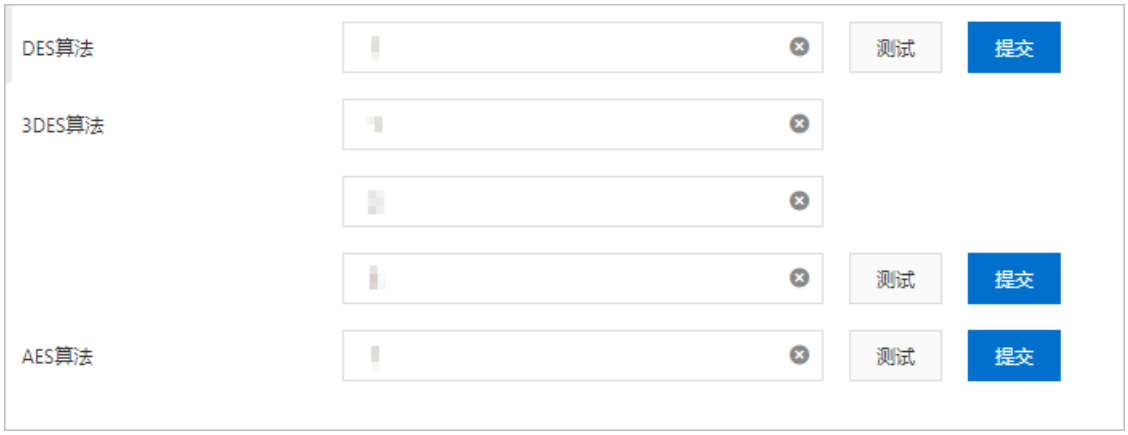
   - **替换脱敏**：设置替换脱敏算法的参数。


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
军官证码随机区间
66
97
保存
测试
护照随机替换
用途字段随机码
第子编号随机区间
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

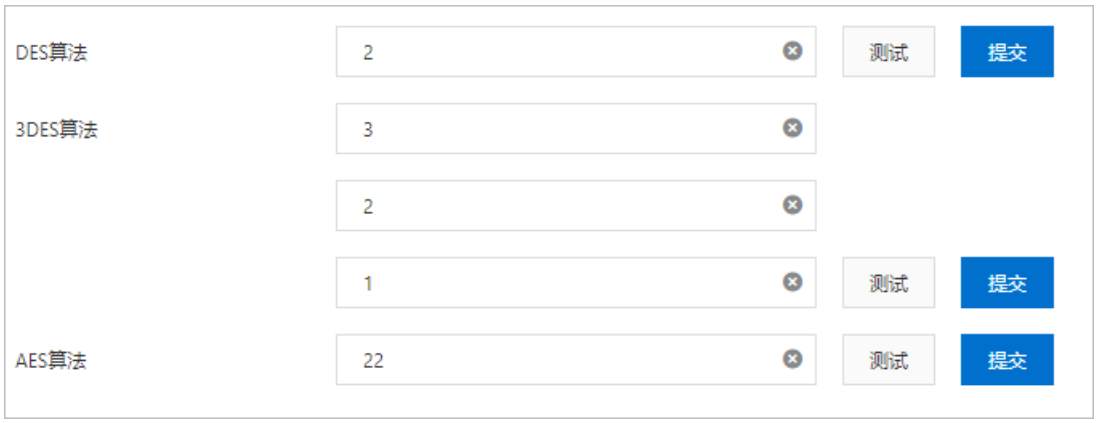


- **变换脱敏**：设置变换脱敏算法的参数。

- **加密脱敏**：设置加密脱敏算法的密钥。



- **数据解密**：设置解密算法的密钥。

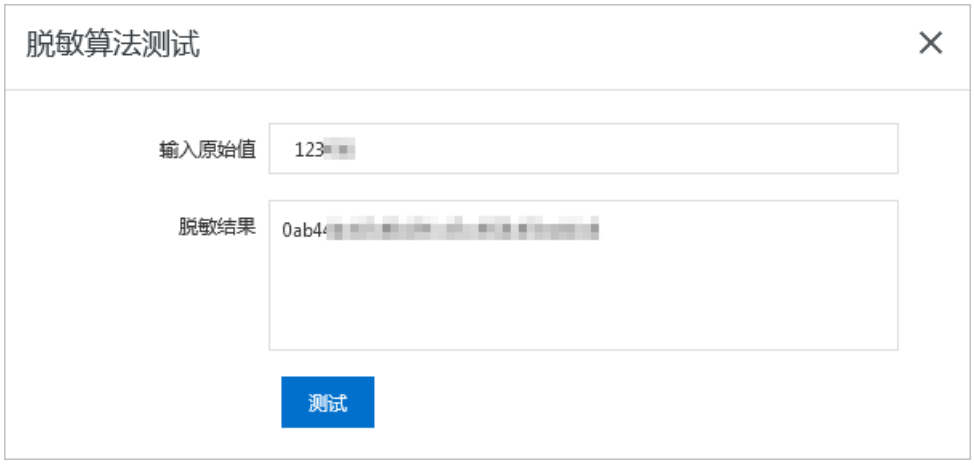


- **洗牌脱敏**：选择洗牌脱敏算法的洗牌方式。

> **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。



   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。

7.5. 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。

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。

8.数据安全实验室

8.1. 数据资产地图

数据资产地图展示最近7天您的所有资产数据和敏感数据统计图表。本文介绍如何使用数据资产地图查看您资产的详细信息。

前提条件

已授权保护您的云资产。更多信息，请参见数据资产授权。

查看资产的统计图表

1. 登录数据安全中心控制台。
2. 在左侧导航栏，选择**数据安全实验室 > 数据资产地图**。
3. 单击需要查看的云产品页签。您可以单击**OSS**、**RDS**、**MaxCompute**、**ECS自建数据库**、**DRDS**、**PolarDB**或**OTS**。
4. 查看您关注的云产品的统计数据或图表信息。

   您可以查看以下统计数据或图表信息。

   > **说明** 本步骤以OSS页签下的数据为例描述图表信息，其余云产品的图表详情以控制台页面为准。

   - **Bucket数**：为您展示受DSC保护的OSS Bucket的总数和存在敏感数据的OSS Bucket数量。
   - **文件数**：为您展示受DSC保护的OSS文件的总数和存在敏感数据的文件总数。
   - **命中规则TOP 10**：为您展示检测出敏感数据数量排名前10的命中规则。
   - **敏感文件占比**：为您展示可公开、不太敏感、不公开和机密文件在OSS文件中占比的饼状图。
   - **数据量变化**：为您展示受DSC保护的OSS产品文件总数和敏感文件数的变化曲线图。

查看资产的详细列表信息

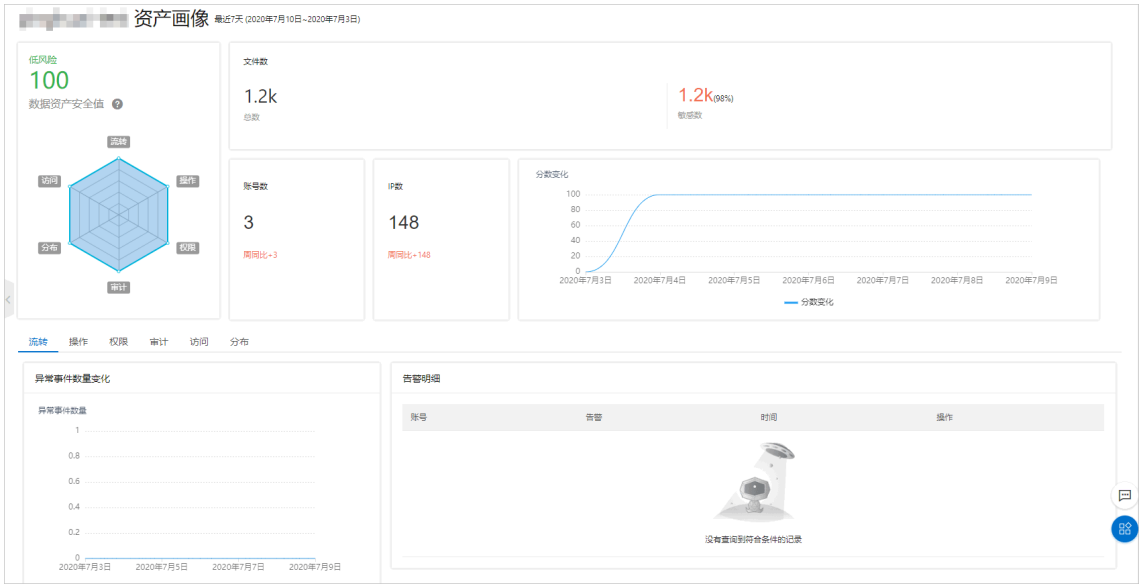
1. 登录数据安全中心控制台。
2. 在左侧导航栏，选择**数据安全实验室 > 数据资产地图**。
3. 单击需要查看的云产品页签。您可以单击**OSS**、**RDS**、**MaxCompute**、**ECS自建数据库**、**DRDS**、**PolarDB**或**OTS**。
4. 查看您关注的云产品资产的详细列表信息。

   您可以执行以下操作。

   > **说明** 本步骤以OSS页签下的数据为例描述文件列表信息，其余云产品的文件列表详情以控制台页面为准。

- 查看Bucket列表：在Bucket列表处，您可以按照敏感等级（高敏感、中敏感、低敏感、未识别）查看对应等级Bucket的信息，包括Bucket所在区域、Bucket名称、总文件数、数据安全分、敏感等级、敏感文件数、最新扫描时间等信息。
- 查看文件详情：在指定Bucket操作列单击**文件详情**，可查看该Bucket中的敏感文件占比、命中规则TOP 5和文件详情列表。在文件详情列表中，单击指定文件操作列的**命中详情**可查看敏感数据命中的相关信息。

- 查看Bucket资产画像：在指定Bucket操作列单击**资产画像**，可查看该Bucket的资产安全情况画像，包括数据资产安全值、文件数、账号数、IP数、安全值分数变化曲线图、异常事件、告警明细等详细信息。



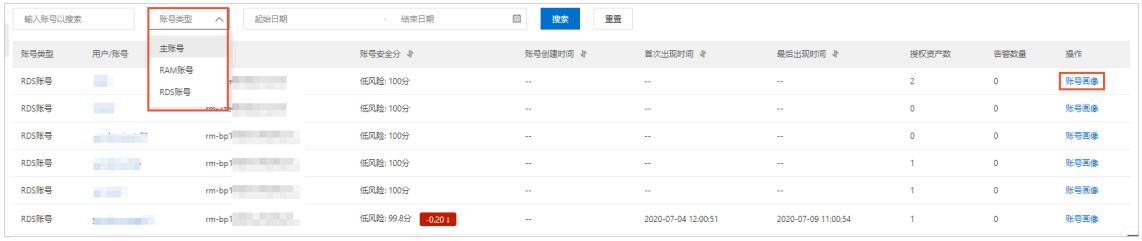
8.2. 用户账号分析

用户账户分析功能提供您资产中所有账号最近7天的统计数据和安全分值，帮助您更好地了解您所有账号的概况和安全状态。本文介绍如何使用用户账号分析功能。

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**数据安全实验室 > 用户账号分析（公测）**。
3. 在**用户账号分析**页面，您可以进行以下操作。
   - 查看账号统计数据：在统计图表模块，您可以查看**总用户数**、**休眠用户数**、**活跃用户数**和**高风险用户数**的统计数据，以及**账号量变化**折线图。

   - 查看账号详细信息列表：在账号列表信息处，您可以分类查看主账号、RAM账号或RDS账号的信息，包括账号对应的实例、账号安全分、账号创建时间、授权资产数、告警数量等信息。您可以在指定账号操作列单击**账号画像**，查看该账号画像的详细信息，包括该账号的安全值、用户信息、安全分值变化图、异常事件变化数量和告警明细等。



> **注意** 如果某个账号的安全值较低，该账号可能存在访问或下载敏感数据等违规操作。建议您及时在该账号的**账号画像**页面查看导致安全值较低的原因，并处理相应告警和异常事件。

9.实时告警通知

9.1. 自定义钉钉机器人告警通知

数据安全中心支持通过钉钉机器人在钉钉群实时发送异常审计告警和泄漏风险告警通知，以便于您及时处理异常问题，保障您业务的正常运行。本文指导您如何设置钉钉群接收告警通知。

前提条件

已安装钉钉并建立了接收告警通知的钉钉群。

背景信息

您需要依次在钉钉群中添加钉钉机器人，在数据安全中心控制台配置告警通知，才能开启钉钉机器人告警通知。

您一次只能为一个钉钉群添加告警通知。如果您需要为多个钉钉群添加告警通知，您需要分别在每个钉钉群中添加钉钉机器人，然后在数据安全中心控制台为每一个钉钉群配置一条告警通知。

步骤一：在钉钉群中添加自定义机器人

> **注意** 本部分介绍的操作需在钉钉客户端中完成，仅供您参考，具体操作请以钉钉客户端显示为准。

1. 打开钉钉客户端。
2. 打开需要添加机器人的钉钉群，在钉钉群的右上角选择**群设置 > 智能群助手 > 添加机器人**。
3. 在**群机器人**对话框中，单击**添加机器人**右侧的 图标。
4. 选择**自定义**机器人。
5. 在**机器人详情**对话框中，单击**添加**。
6. 在**机器人管理**对话框中，参考以下说明完成相关配置。

参数	说明
机器人名称	设置钉钉机器人的名称。
添加到群组	展示钉钉机器人添加到的群组。
安全设置	配置机器人的安全设置方式，配置说明： ○ **自定义关键词**：必填项，支持配置多个自定义关键词，但必须包含关键词：DSC实时告警通知。 ○ **加签**：选填项，如果选中了该项，请保存好该密钥。您需要在数据安全中心控制台配置钉钉机器人（即执行）时，填写此处产生的密钥。 ○ **IP地址（段）**：选填项，告警通知是由数据安全中心服务器发出。设置该项后，只有来自已设置的IP地址范围内的请求才会发送消息通知，因此设置的IP地址范围必须包含数据安全中心的服务器，否则，您将无法收到告警通知。不建议设置该项。

7. 选中**我已阅读并同意《自定义机器人服务及免责条款》**并单击**完成**。
8. 在**机器人管理**对话框中，单击**Webhook**地址右侧的**复制**并保存Webhook地址。

   如果在自定义钉钉机器人设置完成后未复制Webhook地址，您可以选择机器人所在钉钉群，然后在钉钉群右上角依次选择**群设置 > 智能群助手 > 本群的机器人**，并单击要查看的机器人，即可获取对应的Webhook地址。Webhook地址的格式如下：

   ```
   https://oapi.dingtalk.com/robot/send?access_token=XXXXXX
   ```

步骤二：在控制台配置告警通知

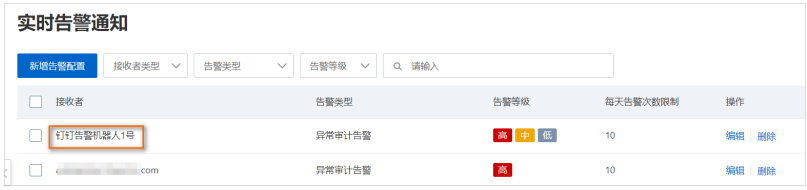
您需要在数据安全中心控制台完成告警通知配置，才能开启钉钉机器人告警通知。

1. 登录数据安全中心控制台。
2. 左侧导航栏，选择**设置 > 实时告警通知**。
3. 在**实时告警通知**页面，单击**新增告警配置**。
4. 在**新增告警通知配置**面板，参考以下说明完成相关配置。

参数	说明
告警方式	选择配置告警的方式。 支持选择**邮箱**或**钉钉机器人**。此处您需要选择**钉钉机器人**。
机器人名称	设置告警通知配置的名称。 如果您未设置该参数，数据安全中心将为您自动生成一个名称。该名称将作为接收者名称展示在**实时告警通知**页面。
Webhook地址	输入您在中复制的Webhook地址。
安全配置	如果您在中配置钉钉机器人时，**安全设置**选中了**加签**，您必须在此处填写对应的签名密钥。否则，您无需配置此参数。
告警类型	选择发送通知的告警类型。可选项： ○ **异常审计告警** ○ **泄露风险告警**

参数	说明
告警等级	选择发送通知的告警等级，支持同时选择多个告警等级。可选项： ○ **高** ○ **中** ○ **低**
告警次数限制	设置24小时内同一规则触发的通知的次数上限。 可设置范围：0~100，默认为10。每日零点清零告警次数的统计值。如果您不需要接收告警，可将该项设置为0。

5. 单击**确定**。
   告警通知配置完成后，您可以在**实时告警通知**页面查看已配置的告警通知。



步骤三：验证告警通知是否配置成功

根据您配置的告警类型，在数据安全中心控制台**异常审计告警**或**泄漏风险告警**页面查看到告警的同时，在相应钉钉群中收到钉钉机器人发送的通知，说明钉钉机器人已配置成功。

如果您在**异常审计告警**或**泄漏风险告警**页面查看到相应告警，钉钉群内未收到通知，请检查Webhook地址的配置是否正确。如果问题仍未解决，请提交工单咨询。提交工单时，在产品分类中未找到数据安全中心，暂不提供工单链接

相关操作

- 修改钉钉机器人告警配置

  如果需要修改发送通知的告警等级、告警类型、或钉钉群的Webhook地址，您可以在**实时告警通知**页面定位到对应的钉钉机器人通知，单击**操作**列的**修改**，修改相应配置。

- 删除钉钉机器人告警配置

  如果您不再需要在指定钉钉群中接收告警通知，您可以在**实时告警通知**页面定位到对应的钉钉机器人通知，单击**操作**列的**删除**，删除该条配置。