

数据安全中心

用户指南

文档版本 40
发布日期 2025-01-17



版权所有 © 华为云计算技术有限公司 2025。保留一切权利。

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

商标声明



HUAWEI和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为云计算技术有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为云计算技术有限公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为云计算技术有限公司

地址：贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

网址：<https://www.huaweicloud.com/>

目录

1 开通 DSC	1
1.1 购买数据安全中心	1
1.2 升级版本和规格	3
2 购买 API 数据安全防护实例并绑定弹性公网 IP	5
3 云资产委托授权/停止授权	9
4 资产地图	13
5 资产管理	22
5.1 资产中心	22
5.1.1 资产中心介绍	22
5.1.2 添加 OBS 资产	23
5.1.3 添加自建数据库实例	25
5.1.4 授权数据库资产	32
5.1.5 添加大数据资产	34
5.1.6 授权大数据资产	36
5.1.7 添加日志流	38
5.2 资产分组管理	39
5.3 元数据任务	40
5.3.1 创建元数据采集任务	40
5.3.2 运行元数据采集任务	42
5.4 数据探索	43
5.5 资产目录	45
6 敏感数据识别	48
6.1 敏感数据识别概述	48
6.2 敏感数据识别配置	50
6.2.1 新增识别模板	50
6.2.2 管理识别模板	50
6.2.3 新建自定义规则	52
6.2.4 编辑规则	54
6.2.5 查看内置规则	54
6.2.6 新建分级	59
6.2.7 管理级别	59

6.3 敏感数据识别任务.....	61
6.3.1 新建敏感数据识别任务.....	61
6.3.2 立即启动识别任务.....	66
6.3.3 管理识别任务列表.....	67
6.3.4 识别结果.....	70
7 策略中心.....	74
7.1 策略基线.....	74
7.1.1 策略基线概述.....	74
7.1.2 数据采集.....	77
7.1.3 数据传输.....	79
7.1.4 数据存储.....	80
7.1.5 数据使用.....	81
7.1.6 数据共享.....	83
7.1.7 数据销毁.....	84
7.2 策略管理.....	86
7.3 流转日志采集.....	90
8 数据资产保护.....	93
8.1 数据脱敏.....	93
8.1.1 数据脱敏概述.....	93
8.1.2 配置和查看脱敏规则.....	94
8.1.3 数据静态脱敏.....	105
8.1.3.1 创建数据静态脱敏任务.....	105
8.1.3.2 查看数据静态脱敏运行状态.....	122
8.1.3.3 编辑和删除数据静态脱敏任务.....	123
8.2 数据水印.....	123
8.2.1 数据水印概述.....	123
8.2.2 注入水印.....	125
8.2.2.1 数据库水印注入.....	125
8.2.2.2 文档水印注入.....	132
8.2.2.3 图片水印注入.....	136
8.2.3 提取水印.....	143
8.2.3.1 数据库水印提取.....	143
8.2.3.2 文档水印提取.....	145
8.2.3.3 图片水印提取.....	146
8.3 数据库安全审计.....	148
8.4 数据库安全加密.....	149
8.5 云堡垒机.....	151
8.6 (可选) 配置 DWS 和 MRS Hive.....	153
9 API 数据安全防护.....	155
9.1 登录实例 Web 控制台.....	155
9.2 实例管理.....	157

9.2.1 查看实例详情.....	157
9.2.2 开启.....	158
9.2.3 关闭.....	159
9.2.4 重启实例.....	159
9.2.5 重启服务.....	160
9.2.6 解绑弹性公网 IP.....	160
9.2.7 重置密码.....	161
9.2.8 版本升级.....	161
9.3 系统管理员操作指南.....	162
9.3.1 首页概览.....	162
9.3.2 资产中心.....	163
9.3.2.1 资产中心概览.....	164
9.3.2.2 应用服务.....	164
9.3.2.3 接口资产.....	167
9.3.2.4 账号资产.....	168
9.3.2.4.1 配置账号解析规则.....	168
9.3.2.4.2 配置账号分组.....	170
9.3.2.5 敏感数据资产.....	171
9.3.3 安全策略管理.....	172
9.3.3.1 创建白名单.....	172
9.3.3.2 访问控制.....	174
9.3.3.2.1 添加基础访问控制规则.....	174
9.3.3.2.2 添加黑名单.....	176
9.3.3.2.3 添加流量控制规则.....	178
9.3.3.3 启用内置规则.....	179
9.3.3.4 添加自定义规则.....	180
9.3.3.5 添加内容替换规则.....	182
9.3.4 脱敏管理.....	184
9.3.4.1 概述.....	184
9.3.4.2 新增自定义脱敏算法.....	185
9.3.4.3 配置脱敏模板.....	187
9.3.4.4 添加脱敏规则.....	188
9.3.4.5 查看脱敏结果.....	190
9.3.5 水印管理.....	191
9.3.5.1 概述.....	191
9.3.5.2 配置水印模板.....	191
9.3.5.3 添加水印规则.....	195
9.3.5.4 查看水印结果.....	197
9.3.5.5 执行水印溯源.....	198
9.3.6 日志中心.....	200
9.3.6.1 告警.....	200
9.3.6.1.1 查看告警信息.....	200

9.3.6.1.2 审阅告警日志.....	201
9.3.6.1.3 告警页面配置策略.....	202
9.3.6.2 检索.....	203
9.3.6.2.1 查看审计日志信息.....	203
9.3.6.2.2 检索页面配置策略.....	204
9.3.7 业务配置.....	204
9.3.7.1 添加敏感数据标签.....	204
9.3.7.2 配置客户端 IP 解析参数.....	207
9.3.7.3 证书管理.....	208
9.3.7.4 添加分类标签.....	209
9.3.7.5 添加分级标签.....	209
9.3.8 系统管理.....	210
9.3.8.1 新建账号.....	210
9.3.8.2 语言切换.....	213
9.3.8.3 修改告警设置.....	213
9.3.8.4 查看设备状态.....	213
9.3.8.5 重启服务或设备.....	214
9.3.8.5.1 重启服务.....	214
9.3.8.5.2 重启设备.....	215
9.3.8.5.3 关闭设备.....	215
9.3.8.6 系统实时诊断.....	216
9.3.8.7 升级系统.....	217
9.3.8.8 网络管理.....	218
9.3.8.8.1 启用 bypass.....	218
9.3.8.8.2 配置网卡与路由信息.....	218
9.3.8.9 查看高可用信息.....	220
9.3.8.10 备份恢复.....	220
9.3.8.10.1 备份审计日志和配置数据.....	220
9.3.8.10.2 恢复审计日志和配置数据.....	221
9.3.8.11 消息通知.....	224
9.3.8.12 数据清理.....	224
9.3.8.12.1 自动清理业务数据.....	224
9.3.8.12.2 手动清理业务数据.....	225
9.3.8.12.3 清理系统运行日志.....	225
9.3.8.12.4 查看清理记录.....	226
9.4 安全管理员操作指南.....	227
9.4.1 系统管理.....	227
9.4.2 用户管理.....	227
9.4.2.1 审核账号.....	227
9.4.2.1.1 手动审核账号.....	227
9.4.2.1.2 启用自动审核.....	227
9.4.2.2 查看角色.....	228

9.4.3 系统运维.....	228
9.4.3.1 启用安全配置.....	228
9.4.3.1.1 设置平台登录安全.....	228
9.4.3.1.2 设置账号密码安全.....	229
9.4.3.1.3 设置网络访问安全.....	230
9.4.3.2 消息通知.....	231
9.5 审计管理员操作指南.....	231
9.5.1 查看操作日志.....	231
9.5.2 消息通知.....	232
10 数据安全运营.....	233
10.1 态势大屏.....	233
10.2 数据流转详情.....	241
10.3 事件管理.....	242
10.4 告警管理.....	246
10.5 OBS 使用审计.....	248
10.6 水印溯源.....	250
10.6.1 数据库水印提取.....	250
10.6.2 OBS 桶文件水印提取.....	251
10.6.3 本地文件水印提取.....	252
11 告警通知.....	254
12 设备管理.....	256
12.1 设备管理概述.....	256
12.2 设备列表.....	256
12.2.1 添加设备.....	257
12.2.2 设备上线.....	258
12.2.3 设备下线.....	258
12.2.4 查看设备列表.....	259
12.3 设备监控.....	260
12.4 设备告警.....	261
12.4.1 处理设备告警.....	261
12.4.2 查看设备告警列表.....	262
12.5 策略管理.....	263
13 共享 VPC.....	268
14 多账号管理.....	270
14.1 多账号管理概述.....	270
14.2 开启多账号管理功能.....	270
14.3 查看多账号管理.....	271
15 权限管理.....	273
15.1 创建用户并授权使用 DSC.....	273
15.2 DSC 自定义策略.....	274

15.3 DSC 权限及授权项.....	276
16 审计.....	278
16.1 支持云审计的操作列表.....	278
16.2 在 CTS 事件列表查看云审计事件.....	280

1 开通 DSC

1.1 购买数据安全中心

数据安全中心服务（DSC）版本支持包年/包月（预付费）的计费方式，API接口（数据脱敏和水印API调用）支持按需计费（后付费）的计费方式。同时，DSC提供两个服务版本：标准版和专业版，两种扩展包：数据库扩展包和OBS扩展包。您可以根据业务需求购买数据安全中心服务。

前提条件

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

约束条件

- 同一账号在同一个大区域（例如华东区域）只能选择一个服务版本。

说明

数据安全中心不支持跨区域使用，即在本Region下购买的DSC版本，只能在该Region下使用。

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

规格限制

- 1个数据库扩展包含1个可添加数据库（支持RDS、DWS、ECS自建数据库、DLI、Elasticsearch、ECS自建大数据等）资产。
- 1个OBS扩展包含1T体量，即1024GB。

操作步骤

步骤1 [登录管理控制台](#)。

步骤2 单击左上角的，选择区域或项目。


- 步骤3** 在左侧导航树中，单击 ，选择“安全与合规 > 数据安全中心”。
- 步骤4** 首次购买DSC，在界面左侧，单击“立即购买”。
- 步骤5** 在“购买数据安全中心”页面，选择“当前区域”。

图 1-1 选择区域和版本规格



说明

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

- 步骤6** 选择“数据库扩展包”和“OBS扩展包”的数量。

图 1-2 选择扩展包



- 1个数据库扩展包包含1个可添加数据库（支持RDS、DWS、ECS自建数据库、DLI、Elasticsearch、ECS自建大数据等）资产。
- 1个OBS扩展包包含1T体量，即1024GB。

- 步骤7** 选择“购买时长”。单击时间轴的点，选择购买时长，可以选择1个月~3年的时长。

说明

勾选“自动续费”后，当服务期满时，系统会自动按照购买周期进行续费。

- 步骤8** 在页面的右下角，单击“立即购买”。

如果您对价格有疑问，可以单击页面左下角的“了解计费详情”，了解产品价格。

- 步骤9** 确认订单无误后，阅读并勾选“我已阅读并同意《数据安全中心免责声明》”，单击“去支付”。

步骤10 进入“付款”页面，请选择付款方式进行付款。

----结束

相关操作

- [升级版本和规格](#)
购买了数据安全中心服务后，您可以从较低版本（标准版）的DSC升级到更高版本（专业版），也可以根据需求增加数据库扩展包和OBS扩展包的数量。
- [如何为数据安全中心服务进行续费？](#)
- [如何退订数据安全中心服务？](#)

1.2 升级版本和规格

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

前提条件

- 已通过IAM对用户绑定“DSC FullAccess”权限的用户组，具体的操作请参见[创建用户并授权使用DSC](#)。
- 已购买任一版本的数据安全中心服务。

约束条件

已到期的服务版本，不支持直接升级，请先完成续费再升级。


规格限制

- 1个数据库扩展包含1个可添加数据库（支持RDS、DWS、ECS自建数据库、DLI、Elasticsearch、ECS自建大数据等）资产。
- 1个OBS扩展包含1T体量，即1024GB。

操作步骤

步骤1 [登录管理控制台](#)。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全与合规 > 数据安全中心”。

步骤4 在页面的右上角单击“升级规格”。

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

“版本规格”从左到右，服务版本的规格越高。

图 1-3 升级版本规格



步骤6 选择“数据库扩展包”和“OBS扩展包”的数量。

图 1-4 选择扩展包



- 1个数据库扩展包包含1个可添加数据库（支持RDS、DWS、ECS自建数据库、DLI、Elasticsearch、ECS自建大数据等）资产。
- 1个OBS扩展包包含1T体量，即1024GB。

步骤7 在页面的右下角，单击“立即购买”。

如果您对价格有疑问，可以单击页面左下角的“了解计费详情”，了解产品价格。

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

步骤9 进入“付款”页面，请选择付款方式进行付款。

----结束

相关操作

- [如何为数据安全中心服务进行续费？](#)
- [如何退订数据安全中心服务？](#)

2 购买 API 数据安全防护实例并绑定弹性公网 IP

一个API数据安全防护实例对应一个独立运行的系统。使用Web浏览器登录API数据安全防护实例必须绑定弹性公网IP。

如果购买的是云外的API数据安全防护实例，请[提交工单](#)获取实例镜像并安装。


前提条件

购买API数据安全防护实例的账号必须是主账号或者是具有创建委托并给委托授权权限的子账号，创建委托请参见[委托其他云服务管理资源](#)。

操作步骤

步骤1 [登录管理控制台](#)。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全与合规 > 数据安全中心”。

步骤4 选择“数据资产保护 > API数据安全防护”，进入“API数据安全防护”界面。

步骤5 在界面左上角单击“购买实例”，进入“购买API数据安全防护”界面。

步骤6 参照[表2-1](#)填写基础配置信息：

表 2-1 基础配置

参数	说明
计费模式	支持包年/包月的计费模式。
当前区域	单击下拉框选择要购买的区域。
当前项目	单击下拉框选择所属项目。
实例类型	支持主备的实例类型。
实例布局	实例属于云上或者云外。

参数	说明
实例名称	单击输入实例名称。
主可用区	“实例布局”为“云上”时需要配置该参数： 单击选择主可用区，如何选择区域和可用区请参见 如何选择区域和可用区？ 。
备可用区	“实例布局”为“云上”时需要配置该参数： 主备选择不同可用区，可以具备跨可用区故障容灾的能力。

步骤7 选择实例规格，包含基础版和专业版，请按照如表2-2所示规格选择。

表 2-2 实例规格

业务规格	基础版	专业版
-	满足基础防护需求	适用于中量级防护需求
支持应用数量	10个（最大）	20个（最大）
支持HTTP流量	1,000 Mbps	2,000 Mbps
支持HTTPS流量	500 Mbps	1,000 Mbps

图 2-1 实例规格



步骤8 设置“网络”：

表 2-3 配置网络

参数	说明
虚拟私有云	<ul style="list-style-type: none"> 单击下拉框选择已创建的虚拟私有云，如果没有可选的VPC请在虚拟私有云控制台申请，申请步骤请参见创建虚拟私有云。 实例创建成功后，VPC不可更换，如选错，只能退订实例后重新购买。 单击“查看虚拟私有云”进入虚拟私有云界面查看和管理您的VPC。
子网	<ul style="list-style-type: none"> 单击下拉框选择已创建的子网，如果没有可选的子网，请单击“创建子网”前往网络控制台申请，详情请参见创建子网。 消耗子网中的1个IP，请确认IP资源配置额充足。 <p>说明 不支持双栈IPv6。</p>
安全组	<p>“实例布局”为“云上”时需要配置该参数：</p> <ul style="list-style-type: none"> 单击下拉框选择已创建的安全组，如果没有可选的安全组，请单击“管理安全组”前往网络控制台申请，详情请参见创建安全组。 为正常使用数据库加密与访问控制，请手动添加安全组规则：TCP协议8441入方向。
弹性IP	<p>“实例布局”为“云上”时需要配置该参数：</p> <p>单击下拉框选择已申请的弹性IP，如果没有可选的弹性IP，请单击“购买弹性IP”前往网络控制台申请，详情请参见绑定弹性公网IP。</p>
主节点IP	<p>“实例布局”为“云下”时需要配置该参数。</p> <p>输入主节点IP地址。</p>
备节点IP	<p>“实例布局”为“云下”时需要配置该参数。</p> <p>输入备节点IP地址。</p>
浮动IP	<p>“实例布局”为“云下”时需要配置该参数。</p> <p>输入浮动节点IP地址。</p>

步骤9 填写“登录信息”：

自定义sysadmin用户密码信息。

- 密码设置要求
 - 长度范围：8~32个字符，不能低于8个字符，且不能超过32个字符。
 - 规则要求：可设置英文大写字母（A~Z）、英文小写字母（a~z）、数字（0~9）和特殊字符（!@\$%^&~_+={[}]:./?~#*），且需同时至少包含其中三种。

- 不能包含用户名或倒序的用户名。
- 系统无法获取系统管理员admin用户密码，请务必保存好登录账号信息。

步骤10 选择“购买时长”，单击“下一步”进入支付确认界面。

步骤11 单击“立即购买”，进入支付界面，完成支付。

步骤12 完成支付后返回“API数据安全防护”界面，可在实例列表查看实例状态为“创建中”，创建实例一般需要10-20分钟。

步骤13 购买“实例布局”为“云上”时需要绑定弹性公网IP：

1. 实例状态为“运行中”时，在需要绑定弹性IP的实例所在行，单击“操作”列的“更多 > 绑定弹性公网IP”。
2. 在弹出的绑定弹性IP对话框中，选择已有“未绑定”状态的弹性IP，单击“确定”。

如果没有可选择的弹性IP，请参考[弹性公网IP](#)，创建新的弹性IP。

步骤14 “实例布局”为“云外”时，单击操作列的“获取对接信息”获取实例的相关对接信息，“云上代理域名”、“云上代理节点IP”、“云上代理节点端口”、“云外主节点ID”以及“云外备节点ID”。

----结束

3 云资产委托授权/停止授权

本章节将介绍如何授权或者停止授权访问OBS桶、数据库、大数据、MRS、资产地图以及LTS。系统将为您创建可供DSC使用的委托关系。

前提条件

已通过IAM对用户绑定“Tenant Administrator”权限的用户组，具体的操作请参见[创建用户组并授权](#)。

约束条件

- 同意授权后，DSC将根据您的选择，设置委托权限以此来访问您的OBS，数据库，大数据实例以及其他相应的云上资产。

说明

- 授权访问OBS桶后，需要获取OBS日志，因此会产生请求费用，具体的请参考[请求费用](#)。
- 停止授权，需要您的资产没有绑定任务。停止授权后，DSC会删除您的委托和资产信息，对应的所有数据将被清除，请谨慎操作。

开通授权后获得的授权委托策略

表 3-1 对应授权项服务创建的委托


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

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

操作步骤

步骤1 [登录管理控制台](#)。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全与合规 > 数据安全中心”，进入“资产地图”页面。

步骤4 在“资产地图”左上角单击云资产授权“修改”，进入“云资产委托授权”页面。

步骤5 在“云资源委托授权”页面，开启/停止授权访问对应的云资源，根据[表3-2](#)进行操作。

图 3-1 云资源委托授权

云资产委托授权 ×

1 同意授权后，DSC将根据您的选择，设置委托权限以此来访问您的OBS，数据库，大数据以及其他相应的云上资产。
停止授权前，请确认该资产没有绑定识别任务。停止授权后，DSC会删除您的委托和资产信息，对应的所有数据将被清除，请谨慎操作！

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

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

表 3-2 参数说明

参数名称	参数说明
资产模块	<ul style="list-style-type: none"> • OBS: 授权访问对象存储服务。 • 数据库: 授权访问数据库, DSC支持的数据库类型及版本请参见使用约束。 • 大数据: 授权访问云搜索服务 (CSS)、数据湖探索 (DLI) 的资产、Hive的资产和HBase的资产。 • MRS: 授权访问MapReduce服务 (MapReduce Service, 简称MRS)。 • 资产地图: 授权访问云上数据资产。 • LTS: 授权访问云日志服务 (Log Tank Service, LTS)。 <p>开通对应资产模块授权后, 获得的授权委托如开通授权后获得的授权委托策略。</p>
开通授权状态	<p>授权状态:</p> <ul style="list-style-type: none"> • 已授权 • 未授权
操作	<p>单击图标开启或者停止授权。</p> <ul style="list-style-type: none"> •  : 未授权 •  : 已授权

----结束

4 资产地图

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

约束限制

- 支持显示1000个资产实例。
- 支持的数据源如所示。

表 4-1 DSC 支持的数据源类型及版本

数据类型	数据源类型	版本
数据库	MySQL	5.6、5.7、5.8、8.0
	SQL Server	2017_SE、2017_EE、2017_WEB
		2016_SE、2016_EE、2016_WEB
		2014_SE、2014_EE
		2012_SE、2012_EE、2012_WEB
		2008_R2_EE、2008_R2_WEB
	PostgreSQL	11、10、9.6、9.5、9.4、9.1、1.0
	TDSQL	10.3.X
	Oracle	11、12
	DDS	4.2、4.0、3.4
	GaussDB	1.3、1.4、2.7
	KingBase	V8
DMDBMS	7、8	

数据类型	数据源类型	版本
	DWS	8.1.X
大数据	ElasticSearch	5.x、6.x、7.x
	DLI	1.0
	Hive	1.0
	Hbase	1.0
OBS	OBS	V3
MRS	MRS-Hive	3.x

前提条件

已完成云资产委托授权，参考[云资产委托授权/停止授权](#)进行操作。

资产地图功能介绍

- 梳理云上数据资产并分区展示：**自动扫描并梳理云上数据资产，地图化展示资产分布，帮助用户解决数据在哪里的问题。根据云上资源VPC展示各个资产所在区域，和业务区域关联。

图 4-1 资产地图



- 敏感数据展示：**基于DSC的三层数据识别引擎、预置合规规则、自然语义识别技术、文件相似度检测技术，对数据资产进行分类分级。
- 数据出口分析：**基于资产地图构建统一的数据出口和出口风险视图，帮助用户识别云上数据可能的出口，以及这些出口存在的潜在安全风险，方便用户采取相应的数据安全防护措施。

图 4-2 数据出口分析



- **风险监控和预警：**基于风险识别引擎，对数据资产进行风险监控，展示每类资产的风险分布，并预警。
 - **安全评分：**资产地图会显示您当前所有资产的总体“安全评分”，单击评分规则后的[?]查看资产安全评分计算规则，如图4-3所示。

图 4-3 评分规则



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


图 4-4 敏感度等级分类



操作步骤

步骤1 [登录管理控制台](#)。

步骤2 单击左上角的 ，选择区域或项目。

步骤3 在左侧导航树中，单击 ，选择“安全与合规 > 数据安全中心”。

步骤4 在左侧导航树中选择“资产地图”，进入“资产地图”页面。

步骤5 [资产添加](#)或者[授权](#)完成后刷新“资产地图”页面，具体页面中各个模块的功能介绍和使用方法详见下述内容。

----结束

风险统计数据

- 如[图4-5](#)所示，展示资产的“安全评分”、“上次评分时间”、“评分详情”以及可以手动重新分析评分，具体内容如下：

图 4-5 安全评分



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

如图4-6所示，“安全防护策略分析”仅展示“风险等级”为“中危”和“高危”的资产。“风险等级”计算方式如表4-2所示，由“配置风险等级”和“分级分类级别”综合得出“风险等级”。

图 4-6 安全防护策略分析

安全防护策略分析

OBS 大数据 数据库

RDS数据库 自建数据库 GaussDb数据库 DWS数据库

^ rds-jingtuo

资产: test (-0.96分) MySQL L3		
存储加密	中危	前往查看
运行模式	未识别风险	根据 策略基线 要求, L3数据为 不要求 采用主备、集群等方式保障存储数据的高可用性 前去修改
SSL传输加密	中危 急需处理	根据 策略基线 要求, L3数据为 强制 开启 安全传输协议进行数据传输加密 前去修改
自动备份	未识别风险	根据 策略基线 要求, L3数据为 强制 采用 主备、集群等方式保障存储数据的高可用性 前去查看
安全组	高危	安全组权限过大或对外开放高危端口 查看详情
公网访问	中危 急需处理	根据 策略基线 要求, L3数据为 强制 不直接提供Internet等外部公开访问、查询、下载 通道 前去修改
数据库审计	中危 急需处理	根据 策略基线 要求, L3数据为 强制 对其访问和使用过程中进行全程审计 前去修改

表 4-2 安全防护策略分析展示规则

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

- 如图4-7所示，展示资产的敏感数据识别分级结果，根据分级结果分类展示资产，具体内容如下：

图 4-7 敏感数据识别分级结果

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

- 鼠标移动至敏感等级上，展示该“敏感等级”下的所有资产信息。
- 鼠标移动至对应的资产类型，右侧弹框展示该类型下所有已扫描资产的名称以及扫描时间。

- 单击某个资产，在右侧弹框展示该实例详情，包含资产基础信息、敏感数据识别、安全防护策略分析以及数据出口分析的内容，具体说明请参见[查看实例详情](#)内容。

查看实例详情

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

图 4-8 敏感数据识别

 rds-zzr-test 已扫描 安全防护中 L4 ×
实例ID: 5345d7d7e3e044beae85662eef3a1b52in01
创建时间: 2024/10/23 01:47:16 GMT+08:00

基础信息

类型	内网IP
RDS	192.168.0.60
端口	引擎类型
3306	MySQL
版本	
5.7	

敏感数据识别 安全防护策略分析 数据出口分析

已授权数据库(1)

 dsc_test 已扫描 收起 ^
当前数据库扫描任务完成。

密级等级	L4
扫描表总数	33 查看详情
敏感表总数	24 查看详情
最新扫描时间	2024/11/13 10:48:19
分类分级模板	华为云数据安全分类分级模板 查看详情

未授权数据库(0)

说明

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





- “安全防护策略分析”：
 - 检测数据资产的安全策略，展示策略风险，检测项包含是否开启服务端加密、数据库加密、传输加密、安全组以及公网访问等高危权限并给出处理提醒，可单击“查看详情”或者“前去修改”处理。

- 查看资产的加密、备份、审计等安全配置的现状和策略基线的具体要求，并可跳转策略/任务配置页面进行策略/任务配置。
- “数据出口分析”：识别云上所有的数据出口，包含EIP/NAT/APIGateway/Roma等。将鼠标移动至资产地图数据类型图标或者VPC图标也可查看数据出口网关线路。

图 4-9 数据出口分析



相关操作

- 如您需要对您的云资产授权进行更改，可单击右上角“修改”进行更改。如需停止授权，需要您的资产没有绑定任务。停止授权后，DSC会删除您的委托和资产信息，对应的所有数据将被清除，请谨慎操作。具体操作请参见[云资产委托授权/停止授权](#)章节。
- 资产敏感度等级图例：从L0-L10每种颜色代表一种等级，根据识别到的资产的敏感度等级，资产地图展示的资产图例颜色与之一一对应。
- 拖动进度条滑块调整资产地图显示比例。
- 单击右下角  全屏显示。
- 单击右下角  显示资产地图操作指南。
- 单击右下角  显示数据异常风险事件，方便快速处理。
- 单击右下角  显示资产图例。

5 资产管理

5.1 资产中心

5.1.1 资产中心介绍

数据安全中心支持自动发现云上数据资产，同时也支持手动添加云上云下自建数据库资产。进行[云资产委托授权](#)后系统将为您创建可供DSC使用的委托关系，此时您可以在资产中心查看和添加您的数据资产，具体支持的资产类型及数据源类型如[表5-1](#)所示。

- OBS桶添加后可以直接对其进行[敏感数据扫描](#)、[OBS脱敏](#)和[数据水印](#)。
- 数据库和大数据类型资产需要完成授权后才能进行[敏感数据识别](#)、[数据脱敏](#)和[数据库水印](#)。

表 5-1 资产中心支持的资产类型及数据源类型

资产类型	数据源类型	添加后操作
OBS	OBS	添加OBS资产： 添加OBS资产
数据库	RDS	授权云上数据库： 授权数据库
	DWS	
	DDS	
	GaussDB	
	自建DB	<ul style="list-style-type: none"> • 添加数据库实例：添加自建数据库实例 • 授权数据库实例：授权数据库。
大数据	Elasticsearch	<ul style="list-style-type: none"> • 添加自建大数据实例：添加大数据资产。 • 授权大数据：授权大数据资产。
	Hive	
	HBase	
	DLI	添加DLI数据库： 添加DLI数据库 。

资产类型	数据源类型	添加后操作
日志	LTS	添加日志流： 添加日志流
说明 当前DSC仅部分Region支持纳管已启用IPv6 VPC的数据库资产，具体支持的Region请见 功能总览 。		

5.1.2 添加 OBS 资产

对OBS资产进行云资产委托授权后，参考此章节将您的OBS资产添加到DSC服务，进行数据资产管理，包含敏感数据识别、数据脱敏以及注入\提取数据水印等。

前提条件

- 已完成OBS资产委托授权，参考[云资产委托授权/停止授权](#)进行操作。
- 添加自有OBS桶/其他桶，需要开通且已使用过OBS服务，开通OBS服务请参见[开通并使用OBS](#)。
- 如果添加其他桶，则需设置该桶的权限为“公共”或者该桶为当前账户拥有权限的私有桶，如何查看桶策略请参见[查看桶策略](#)。

约束条件


DSC不支持OBS的并行文件系统。

添加自有桶

自有桶是指当前用户自己创建的桶，包含公共桶和私有桶。

步骤1 [登录管理控制台](#)。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全与合规 > 数据安全中心”。

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

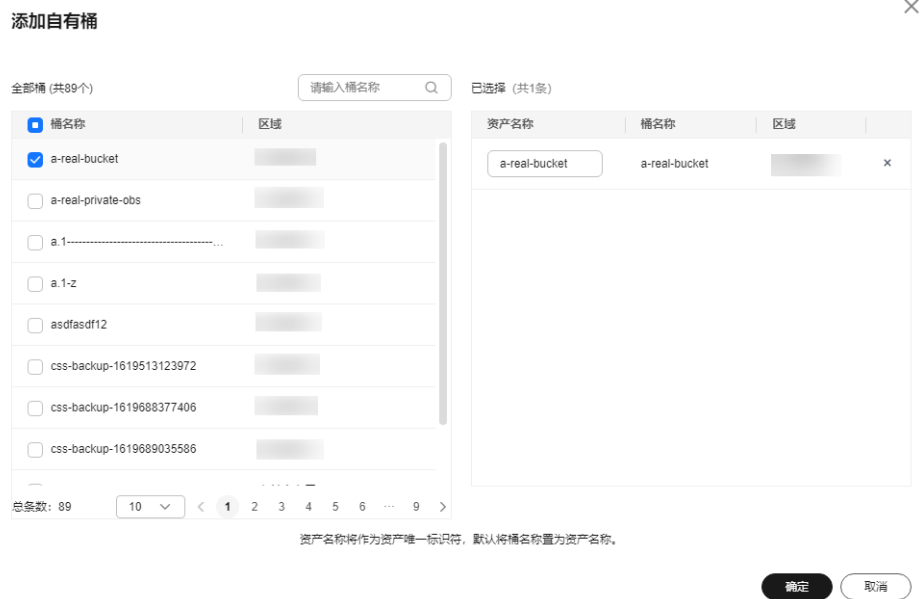
步骤5 单击OBS资产，进入OBS资产列表界面。

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

说明

资产名称将作为资产唯一标识符，默认将桶名称置为资产名称。

图 5-1 添加自有桶



步骤7 单击“确定”。


----结束

添加其他桶

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

步骤1 [登录管理控制台](#)。

步骤2 单击左上角的, 选择区域或项目。

步骤3 在左侧导航树中, 单击, 选择“安全与合规 > 数据安全中心”。

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

步骤5 单击“OBS”, 进入OBS资产列表界面。

步骤6 在OBS资产列表左上角, 单击“添加其他桶”。在弹出“添加其他桶”对话框中, 输入待添加桶的名称。

如需添加多个桶, 则可单击“添加”, 继续进行添加。

图 5-2 添加其他桶

添加其他桶

区域

* 桶名称 添加

资产名称	桶名称	操作
<input type="text" value="dsc-obs"/>	<input type="text" value="dsc-obs"/>	删除
<input type="text" value="请输入资产名称"/>	<input type="text" value="请输入桶名称"/>	删除

确定 取消

步骤7 单击“确定”。

----结束

相关操作

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

5.1.3 添加自建数据库实例

如果您的资产是自建数据库类型，请参照此章节将数据库实例添加到DSC服务。

前提条件

- 已完成数据库资产委托授权，参考[云资产委托授权/停止授权](#)进行操作。
- 已申请ECS并且在ECS中安装了数据库，请参见[快速购买和使用Windows ECS](#)。

约束限制

自建DB只能添加数据安全中心支持的数据源及版本，DSC支持的数据源及版本如[表5-2](#)所示。

表 5-2 DSC 支持的数据源及版本


数据源类型	版本
MySQL	5.6、5.7、5.8、8.0
SQL Server	<ul style="list-style-type: none"> • 2017_SE、2017_EE、2017_WEB • 2016_SE、2016_EE、2016_WEB • 2014_SE、2014_EE • 2012_SE、2012_EE、2012_WEB • 2008_R2_EE、2008_R2_WEB
KingBase	V8
DMDBMS	7、8
PostgreSQL	15、14、13、12、11、10、9.6、9.5、9.4、9.1
TDSQL	10.3.X
Oracle	11、12

添加云上自建数据库实例

自建DB支持添加和删除数据库实例，DSC支持的数据库类型及版本请参见表5-2。本节介绍如何添加云上自建数据库。

步骤1 登录管理控制台。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全与合规 > 数据安全中心”。

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

步骤5 选择“数据库 > 自建DB”，进入“数据库”页签。

步骤6 单击“数据库实例”，进入“数据库实例”页签。

步骤7 单击左上角的“添加实例”，进入“添加数据库实例”弹框。

图 5-3 添加数据库实例

步骤8 根据表5-3配置相关参数，单击“确定”完成自建数据库实例的添加。

表 5-3 配置数据库实例信息

参数	说明
ECS实例	单击下拉框选择需要添加的自建数据库实例所属ECS。
安全组	单击下拉框选择所属安全组。
数据库引擎	单击下拉框选择对应的自建数据库的引擎，目前支持如下引擎类型： <ul style="list-style-type: none"> • MySQL • TDSQL • KingBase • Dmdbms • PostgreSQL • SQLServer • Oracle
版本	单击下拉框选择数据库引擎的版本。
连接方式	“数据库引擎”选择“Oracle”时显示该参数，单击下拉框选择连接方式： <ul style="list-style-type: none"> • 服务名：请输入服务名称。 • SID：请输入服务名称。
主机	单击下拉框选择主机。 集群部署模式下，如需使用脱敏功能需设置为主节点IP。

参数	说明
数据库端口	输入0-65535的整数。
数据库名称	输入数据库名称。
用户名/密码	输入该数据库的用户名和密码。
资产名称	输入长度范围为4-255个字符，仅允许输入中英文、数字、“-”、“_”，并且开头需为中文或者字母。
创建元数据拉取任务	打开开关后，会基于实例的默认数据库自动下发元数据任务，拉取实例的库、表、列信息。

步骤9 实例添加完成后如果需要对该实例下的数据库进行敏感数据识别和脱敏，请先对该实例下的数据库进行授权，具体操作请参见[授权数据库](#)。


----结束

添加外部自建数据库实例

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

步骤1 [登录管理控制台](#)。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全与合规 > 数据安全中心”。

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

步骤5 选择“数据库 > 自建DB”，进入“数据库”页签。

步骤6 单击“数据库实例”，进入“数据库实例”页签。

步骤7 单击左上角的“添加外部自建数据库实例”，进入“添加数据库实例”弹框。

图 5-4 添加外部自建数据库实例

✕

添加外部数据库实例

<p>* 区域 <input type="text"/></p> <p>* 子网 <input type="text" value="subnet-5555"/></p> <p>* 数据库引擎 <input type="text" value="MySQL"/></p> <p>* 主机 <input type="text" value="请输入IP地址"/></p> <p>* 数据库名称 <input type="text" value="请输入数据库名称"/></p> <p>* 密码 <input type="password" value="请输入密码"/></p>	<p>* 代理VPC <input type="text" value="vpc-default"/></p> <p>* 安全组 <input type="text" value="mrs_mrs_dyf_dTths"/></p> <p>* 版本 <input type="text" value="11"/></p> <p>* 数据库端口 <input type="text" value="请输入端口"/></p> <p>* 用户名 <input type="text" value="请输入用户名"/></p> <p>* 资产名称 <input type="text" value="请输入资产名称"/></p>
--	---

* 创建元数据拉取任务

确定
取消

步骤8 根据表5-4配置相关参数，单击“确定”完成外部自建数据库实例的添加。

表 5-4 配置数据库实例信息

参数	说明
区域	实例所在区域。
代理VPC	单击下拉框选择云上代理VPC。
子网	单击下拉框选择所属子网。
安全组	单击下拉框选择所属安全组。
数据库引擎	单击下拉框选择对应的自建数据库的引擎，目前支持如下引擎类型： <ul style="list-style-type: none"> ● MySQL ● TDSQL ● KingBase ● Dmdbms ● PostgreSQL ● SQLServer ● Oracle
版本	单击下拉框选择数据库引擎的版本。
连接方式	“数据库引擎”选择“Oracle”时显示该参数，单击下拉框选择连接方式： <ul style="list-style-type: none"> ● 服务名：请输入服务名称。 ● SID：请输入服务名称。
主机	输入资产所在主机IP地址。

参数	说明
数据库端口	输入0-65535的整数。
数据库名称	输入数据库名称。
用户名	输入数据库用户名。
密码	输入数据库密码。
资产名称	输入数据库密码输入长度范围为4-255个字符，仅允许输入中英文、数字、“-”、“_”，并且开头需为中文或者字母。

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

步骤10 实例添加完成后如果需要对该实例下的数据库进行敏感数据识别和脱敏，请先对该实例下的数据库进行授权，具体操作请参见[授权数据库](#)。


---结束

批量添加实例与数据库

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

步骤1 [登录管理控制台](#)。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全与合规 > 数据安全中心”。

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

步骤5 选择“数据库 > 自建DB”，进入“数据库”页签。

步骤6 单击“数据库实例”，进入“数据库实例”页签。

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

步骤8 单击“下载模板”，下载Excel模板，根据[表5-5](#)填写相关参数。

表 5-5 数据库实例信息

参数	说明
资产名称	自定义，在填写后在自己数据库列表中显示的资产名称
ECS实例ID	外部自建数据库可以不填，本账号购买ECS自建数据库需要填写对应ESC实例的ID。
Oracle连接方式（默认服务名）	仅Oracle需要填写，其余类型无需填写。
Oracle服务名/SID	填写服务名称。

参数	说明
代理VPC	云内数据库无需填写，外部自建数据库必填，对应ECS的代理VPC。
子网	云内数据库可以不填，外部ESC必填，对应ECS的子网ID。
安全组	云内数据库可以不填，外部ESC必填，对应ECS的安全组。
数据库引擎	如果ECS实例已被添加，将会使用已添加引擎。
版本	如果ECS实例已被添加，将会使用已添加版本。
主机IP	如果ECS实例已被添加，将会使用已添加IP。
数据库端口	如果ECS实例已被添加，将会使用已添加端口。
数据库名称	数据库的名称。
用户名	数据库账号。
密码	数据库密码。
是否拉取元数据	TRUE或者FALSE。

步骤9 单击“添加文件”选择填好的模板，单击“确定”。

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

步骤11 实例添加完成后如果需要对实例下的数据库进行敏感数据识别和脱敏，请先对该实例下的数据库进行授权，具体操作请参见[授权数据库](#)。

----结束

相关操作

- 删除数据库实例

只有自建数据库实例支持删除，删除时实例下的授权数据库为0且元数据已被清空才可删除。

勾选多个自建数据库实例，单击实例列表左上角“批量删除”，删除实例。也可通过单击实例列表“操作”列的“删除”，删除单个实例。
- 拉取实例下的元数据
 - 数据库实例下的授权数据库大于0时，在实例列表“操作”列，单击“刷新”自动创建元数据任务拉取实例的库、表、列信息。
不支持元数据采集的云数据库除外，如DDS等，详情请参见[创建元数据采集任务](#)章节。
 - 添加自建数据库实例时，如果打开“创建元数据拉取任务”的开关，完成实例创建后会自动创建元数据任务拉取实例下的所有元数据。
不支持元数据采集的自建数据库除外，如SQLServer等，详情请参见[创建元数据采集任务](#)章节。
 - 参考[创建元数据采集任务](#)章节的内容手动创建元数据任务。
- 创建识别任务

在数据库页签，单击资产列表“操作”列的“创建识别任务”，为资产创建敏感数据识别任务识别资产，详细操作步骤请参见[新建敏感数据识别任务](#)章节

- 批量测试连通性
可多选批量添加的实例与数据，批量进行连通性测试。

5.1.4 授权数据库资产

对数据库资产进行敏感数据识别、数据脱敏或者添加/提取水印则需要对实例下的数据库进行授权，该章节介绍如何对数据库进行授权操作。

前提条件


- 已开通RDS/DWS/DDS/GaussDB服务，且已有资产，且对应子网下含有可用的IP配额。
- 数据库实例的“状态”为“正常”，且安全组的数量为1。

授权数据库

这里以“RDS”数据库类型为例讲解如何对实例下的数据库资产进行授权。如果需要对其他类型的数据库进行授权，请单击对应的数据库类型如“DWS”或者“自建DB”按照如下操作步骤进行操作即可。

步骤1 登录管理控制台。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全与合规 > 数据安全中心”。

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

步骤5 单击“RDS”进入RDS“数据库”列表界面。

图 5-5 RDS 数据库实例



实例名称	状态	类型	内网IP	端口	引擎版本	授权数据库	创建时间	操作
rds-2dr-1eef	正常	云数据库	192.168.40	3306	MySQL / 5.7	已授权1个	2024/10/23 01:47:1...	授权 刷新 清空元数据
4d9sewz019	创建失败	云数据库	192.168.77	1433	SQL Server / 2019...	已授权0个	2024/05/07 02:53:4...	授权

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

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

图 5-6 数据库授权



- 授权“只读权限”：只能使用敏感数据识别功能。
- 授权“读写权限”：可使用敏感数据识别和数据脱敏功能。

注意

- 创建了RDS只读权限后，DSC服务会在RDS创建一个dsc_readonly账户。
 - dsc_readonly账户的密码在RDS重置后，将不会自动同步到DSC服务，会导致敏感数据识别任务失败，因此，建议您不要重置该账户密码。
 - 如果您已在RDS里重置了dsc_readonly账户的密码，建议您在DSC服务里先删除已授权的rds实例，再重新对该实例进行权限设置。
 - DSC暂不支持对RDS中已开启SSL的MySQL数据库进行扫描和脱敏。
- 方法二：通过单击“实例名称”进入实例详情页面，单击“操作”列的“授权”。

图 5-7 实例详情



步骤7 完成授权后，单击“数据库”页签，查看已授权数据库的连通状态。

资产授权完成后，该资产“连通状态”为“检查中”，此时，DSC会测试数据库的连通性。

- DSC能正常访问已添加的数据库，该数据库的“连通状态”为“成功”。

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

----结束

相关操作

- 删除数据库实例
只有自建数据库实例支持删除，删除时实例下的授权数据库为0且元数据已被清空才可删除。
勾选多个自建数据库实例，单击实例列表左上角“批量删除”，删除实例。也可通过单击实例列表“操作”列的“删除”，删除单个实例。
- 拉取实例下的元数据
 - 数据库实例下的授权数据库大于0时，在实例列表“操作”列，单击“刷新”自动创建元数据任务拉取实例的库、表、列信息。
不支持元数据采集的云数据库除外，如DDS等，详情请参见[创建元数据采集任务](#)章节。
 - 添加自建数据库实例时，如果打开“创建元数据拉取任务”的开关，完成实例创建后会自动创建元数据任务拉取实例下的所有元数据。
不支持元数据采集的自建数据库除外，如SQLServer等，详情请参见[创建元数据采集任务](#)章节。
 - 参考[创建元数据采集任务](#)章节的内容手动创建元数据任务。
- 创建识别任务
在数据库页签，单击资产列表“操作”列的“创建识别任务”，为资产创建敏感数据识别任务识别资产，详细操作步骤请参见[新建敏感数据识别任务](#)章节
- 批量测试连通性
可多选批量添加的实例与数据，批量进行连通性测试。

5.1.5 添加大数据资产

如果您的资产是自建大数据类型，请参照此章节将大数据实例添加到DSC服务。

如果您的资产为DLI数据库，请参照[添加DLI数据库](#)进行添加。

前提条件

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

添加大数据类型实例

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

步骤1 [登录管理控制台](#)。

步骤2 单击左上角的，选择区域或项目。


- 步骤3** 在左侧导航树中，单击 ，选择“安全与合规 > 数据安全中心”。
- 步骤4** 在左侧导航树中选择“资产管理 > 资产中心”，进入“资产中心”页面。
- 步骤5** 单击“Elasticsearch”大数据类型，进入“索引”页签。
- 步骤6** 单击“ES实例”，进入“ES实例”页签。
- 步骤7** 单击左上角的“添加实例”，进入“添加实例”弹框。
- 步骤8** 根据表5-6配置相关参数，单击“确定”。

表 5-6 添加实例参数配置表

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

----结束

添加 DLI 数据库



- 步骤1** [登录管理控制台](#)。
- 步骤2** 单击左上角的 ，选择区域或项目。
- 步骤3** 在左侧导航树中，单击 ，选择“安全与合规 > 数据安全中心”。
- 步骤4** 在左侧导航树中选择“资产管理 > 资产中心”，进入“资产中心”页面。
- 步骤5** 单击“DLI”大数据类型，进入DLI“数据库”页签。

图 5-8 DLI 数据库列表



步骤6 单击数据库列表左上角的“添加数据库”，进入“添加数据库”弹框。

步骤7 根据表5-7配置相关参数，单击“确定”完成添加。

表 5-7 添加数据库参数配置表

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

步骤8 资产授权完成后，该资产“连通性”为“检查中”，此时，DSC会测试资产的连通性。

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

----结束

相关操作

- 删除实例
只有自建大数据实例支持删除，且授权数据库为0才可删除。
勾选多个自建大数据实例，单击实例列表左上角“批量删除”，删除实例。也可通过单击实例列表“操作”列的“删除”，删除单个实例。
- 拉取实例下的元数据
 - MRS_Hive实例下数据库授权个数大于0时，在Hive实例列表“操作”列，单击“更多 > 刷新”会自动创建元数据任务拉取实例的库、表、列信息。
 - 添加Hive实例时，如果打开自动创建元数据任务的开关，完成实例创建后会创建元数据任务拉取实例下的所有元数据。
 - 支持元数据采集的大数据类型请参见[创建元数据采集任务](#)章节。
 - 参考[创建元数据采集任务](#)章节的内容手动创建元数据任务。
- 创建识别任务
单击资产列表“操作”列的“创建识别任务”，为资产创建敏感数据识别任务识别资产，详细操作步骤请参见[新建敏感数据识别任务](#)章节

5.1.6 授权大数据资产

对大数据资产进行敏感数据识别或数据脱敏则需要对实例下的数据库进行授权，该章节介绍如何对数据库进行授权操作。

前提条件


已开通DLI、CSS服务，且DLI、CSS中已有资产，且对应子网下含有可用的IP配额。

授权大数据

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

步骤1 [登录管理控制台](#)。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全与合规 > 数据安全中心”。

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

步骤5 单击“Elasticsearch”大数据类型，进入“索引”页签。

步骤6 单击“ES实例”，进入“ES实例”页签。可以通过以下两种途径完成授权：

- 方法一：单击“ES实例”列表“操作”列的“授权”，输入ES索引信息进行授权。
- 方法二：单击“实例名称”进入实例详情页面，查看该实例下所有索引的状态。单击“操作”列的“授权”去给未授权的索引授权。

说明

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

步骤7 单击“索引”页签，查看已授权资产的连通状态。

资产授权完成后，该资产“连通性”为“检查中”，此时，DSC会测试数据库的连通性。

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

---结束

相关操作

- 删除实例
只有自建大数据实例支持删除，且授权数据库为0才可删除。
勾选多个自建大数据实例，单击实例列表左上角“批量删除”，删除实例。也可通过单击实例列表“操作”列的“删除”，删除单个实例。
- 拉取实例下的元数据
 - MRS_Hive实例下数据库授权个数大于0时，在Hive实例列表“操作”列，单击“更多 > 刷新”会自动创建元数据任务拉取实例的库、表、列信息。
 - 添加Hive实例时，如果打开自动创建元数据任务的开关，完成实例创建后会自动创建元数据任务拉取实例下的所有元数据。
 - 支持元数据采集的大数据类型请参见[创建元数据采集任务](#)章节。
 - 参考[创建元数据采集任务](#)章节的内容手动创建元数据任务。
- 创建识别任务
单击资产列表“操作”列的“创建识别任务”，为资产创建敏感数据识别任务识别资产，详细操作步骤请参见[新建敏感数据识别任务](#)章节

5.1.7 添加日志流

该章节介绍如何将云日志资产添加到DSC。


前提条件

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

添加日志流

步骤1 [登录管理控制台](#)。

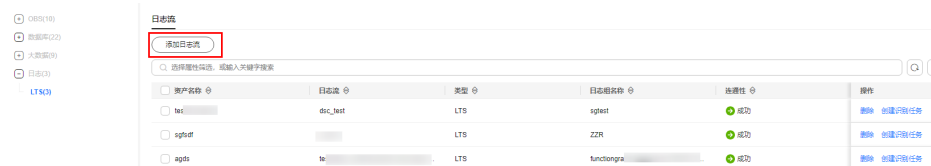
步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全与合规 > 数据安全中心”。

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

步骤5 选择“日志 > LTS”，进入LTS“日志流”页签。

图 5-9 LTS 数据库列表



步骤6 单击数据库列表左上角的“添加日志流”，进入“添加日志流”弹框。

步骤7 根据[表5-8](#)配置相关参数，单击“确定”完成添加。

表 5-8 添加数据库参数配置表

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

步骤8 资产授权完成后，该资产“连通性”为“检查中”，此时，DSC会测试资产的连通性。

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

----结束

5.2 资产分组管理

对资产中心数据库和大数据资产进行分组后方便维护和管理，本章介绍如何进行资产分组管理。

前提条件


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

新建数据库分组

通过创建子级标签的方式对您的资产进一步分组，方便管理和查看。

步骤1 [登录管理控制台](#)。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全与合规 > 数据安全中心”。

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


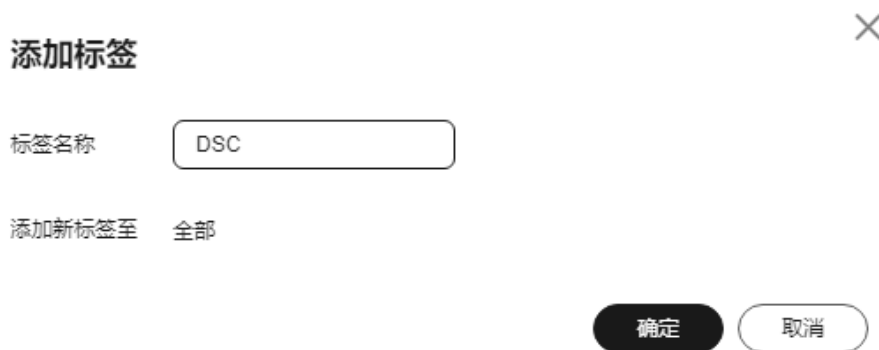
步骤5 将鼠标滑动至全域数据库列表的“全部”或者新创建的标签上，单击添加标签，系统弹出“添加标签”弹窗。

图 5-10 添加标签



步骤6 自定义标签名称（即分组名称），单击“确定”，创建标签成功。



----结束

管理数据库分组

通过移动数据库实例下的数据库对其进行重新分组管理。




步骤1 [登录管理控制台](#)。

步骤2 单击左上角的，选择区域或项目。

- 步骤3** 在左侧导航树中，单击 ，选择“安全与合规 > 数据安全中心”。
- 步骤4** 在左侧导航树中选择“资产管理 > 资产分组管理”，进入“资产分组管理”页面。
- 步骤5** 在“全域数据列表”选择需要管理的分组，并在右侧页面单击  展开数据库实例详情。
- 步骤6** 勾选待移动数据库，单击待移动数据库所在行“操作”列“移动到”，在“移动到”弹窗中选择目标标签。
- 步骤7** 单击“确定”。
- 结束

删除数据库分组

系统自带的未分组不支持删除。

- 步骤1** [登录管理控制台](#)。
- 步骤2** 单击左上角的 ，选择区域或项目。
- 步骤3** 在左侧导航树中，单击 ，选择“安全与合规 > 数据安全中心”。
- 步骤4** 在左侧导航树中选择“资产管理 > 资产分组管理”，进入“资产分组管理”页面。
- 步骤5** 将鼠标滑动至全域数据库列表的标签名称处，单击  删除标签，系统弹出“确认要删除标签”弹窗。
- 步骤6** 单击“确定”，删除标签。
- 删除标签后，该标签下的资产将移动到未分组下。
- 结束

5.3 元数据任务

5.3.1 创建元数据采集任务

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

前提条件

已完成云资产委托授权，具体请参见[云资产委托授权/停止授权](#)进行操作。

操作步骤

- 步骤1** [登录管理控制台](#)。
- 步骤2** 单击左上角的 ，选择区域或项目。














- 步骤3** 在左侧导航树中，单击 ，选择“安全与合规 > 数据安全中心”。
- 步骤4** 在左侧导航树中选择“资产管理 > 元数据任务”，进入“元数据采集任务”页面。
- 步骤5** 在“元数据采集任务”页面，单击“新建”，进入“新建采集任务 > 数据源配置”页面，具体参数说明如表 [数据源配置参数说明](#) 所示。

表 5-9 数据源配置参数说明



参数名	参数说明
选择数据源	选择数据来源。可选择“MySQL”、“TDSQL”、“PostgreSQL”、“达梦”、“人大金仓”、“OpenGuass”、“DWS”、“Hive”、“MRS_HIVE”。
数据库实例	单击下拉框选择数据库实例。
添加配置项	单击“添加配置项”可以增加配置项。

步骤6 单击“下一步”，进入“子任务配置”页面：

- 选择开启  或关闭  “扫描用户表”。
- 选择开启  或关闭  “扫描系统表”，例如包括information_schema。
- 选择开启  或关闭  “扫描列约束”，包括主键，是否唯一。
- 选择开启  或关闭  “扫描视图”，扫描元数据中是否包括视图。
- 选择开启  或关闭  “扫描列注释”。
- 选择开启  或关闭  “扫描权限”。

步骤7 单击“下一步”，进入“任务信息配置”页面，配置任务信息，参数说明请参见表 [任务信息配置参数说明](#)。

表 5-10 任务信息配置参数说明

参数名称	参数说明
任务信息	<ul style="list-style-type: none"> • 任务名称：必填项，您可以自定义采集任务的名称。 • 任务描述：非必填项，对您的采集任务进行描述。
任务配置	选择开启  或关闭  “删除连通性失败的元数据”。
执行计划	<ul style="list-style-type: none"> • 识别周期：您可以选择“单次”、“每日”、“每周”或“每月”。 • 执行计划：您可以选择“立即执行”或“定时启动”。

步骤8 单击“下一步”，进入“配置确认”页面，确认您已经配置好的参数。

步骤9 确认无误后单击“完成”，即可成功创建一个新的元数据采集任务。

---结束

5.3.2 运行元数据采集任务

对于已创建成功的元数据采集任务，您可以在任务列表进行查看并运行。


前提条件

已创建元数据采集任务，具体请参见[创建元数据采集任务](#)。

操作步骤

步骤1 [登录管理控制台](#)。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全与合规 > 数据安全中心”。

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

表 5-11 元数据采集任务参数说明

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

步骤5 单击操作栏“运行”，开始运行当前创建的元数据采集任务。


步骤6 单击元数据采集任务左侧，可查看任务的运行详情，参数说明请参见[表 元数据任务详情参数说明](#)。

表 5-12 元数据任务详情参数说明

参数名称	参数说明
开始时间	任务开始运行的时间
结束时间	任务运行结束的时间

参数名称	参数说明
执行方式	“单次”、“每日”、“每周”或“每月”
状态	当前任务运行的状态，任务状态分为： <ul style="list-style-type: none"> ● 已完成：已完成元数据采集任务。 ● 运行中：正在运行元数据采集任务。 ● 运行失败：元数据采集任务运行失败。 ● 调度中：元数据采集任务已添加成功，待运行。 ● 部分完成：已完成部分元数据采集任务。
运行时长	任务开始运行到结束运行用的时间

----结束

相关操作

您还可以在任务的操作栏对当前元数据采集任务进行“编辑”或“删除”操作。

5.4 数据探索

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


前提条件

- 已完成数据资产委托授权，具体请参见[云资产委托授权/停止授权](#)进行操作。
- 已进行元数据扫描，具体请参见[元数据任务](#)进行操作。

操作步骤

步骤1 [登录管理控制台](#)。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全与合规 > 数据安全中心”。

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

步骤5 左上角单击下拉框选择展示模式：

- “数据库”
- “数据模式”
- “数据表”

- “数据列”

步骤6 单击数据库名称，进入数据库详情页面。

您可以对数据库、数据表以及数据视图等添加描述、标签、密级和分类等。

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

图 5-11 数据库详情



步骤7 查看数据库详细信息。

- 在数据详情页面选择“表信息”页签：
 - 单击表名称查看表详情。
 - 勾选表，单击左上角的“标识”添加表标识，标识可以选择标签或者密级。
 - 标签：单击“选择标签”输入框选择已添加标签或者输入文字并回车可临时添加标签，单击“确认”。
 - 密级：单击“选择密级”下拉框选择密级，该密级包含内置级别和自定义级别，如果需要新建密级请参见[新建分级](#)。选择密级后单击“确认”提交。
 - 也可通过单击编辑按钮给单个表分别添加分类、密级、标签和描述等信息。
- 在数据详情页面选择“视图信息”页签：
 - 单击视图名称查看视图详情。
 - 选择“视图信息”页签，勾选视图，单击左上角的“标识”添加视图标识。标识可以选择标签或者密级。
 - 标签：单击“选择标签”输入框选择已添加标签或者输入文字并回车可临时添加标签，单击“确认”。
 - 密级：单击“选择密级”下拉框选择密级，该密级包含内置级别和自定义级别，如果需要新建密级请参见[新建分级](#)。选择密级后单击“确认”提交。
 - 也可通过单击编辑按钮给视图添加分类、密级、标签和描述等信息。
- 在数据详情页面选择“schema信息”页签（该页签只有有schema的数据库才会显示）：

- 勾选schema，单击左上角的“标识”添加列标识。标识可以选择标签或者密级。
 - 标签：单击“选择标签”输入框选择已添加标签或者输入文字并回车可临时添加标签，单击“确认”。
 - 密级：单击“选择密级”下拉框选择密级，该密级包含内置级别和自定义级别，如果需要新建密级请参见[新建分级](#)。选择密级后单击“确认”提交。
- 也可通过单击编辑按钮给schema添加分类、密级、标签和描述等信息。

---结束

相关操作

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

5.5 资产目录

资产目录从“业务域”和“数据类型”两种维度统计数据资产的敏感信息，并从数据库、表、列三个维度进行展示。

- “业务域”的分类标签是按照资产分组管理中创建的标签来分类的，如果需要修改该分类标签请在[资产分组管理](#)中进行修改。
- “数据类型”：
结构化数据：支持元数据任务的数据类型，包含DWS、“PostgreSQL”、“DMDBMS（达梦）”、“MySQL”、“OpenGauss”、“KingBase（人大金仓）”、“TDSQL”、“SQLServer”、“Hive”、“MRS_HIVE”。


前提条件

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

查看资产目录

步骤1 [登录管理控制台](#)。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全与合规 > 数据安全中心”。

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

步骤5 在“业务域”或“数据类型”页签查看已经添加的数据资产信息，相关参数说明如[表数据目录参数说明](#)。

在“业务域”页签左侧导航栏，选择分组展示您想要查看的数据资产，或在“数据类型”页签左侧导航栏选择数据类型展示您要查看的数据资产。

表 5-13 资产目录参数说明


参数名称	参数说明
统计信息	<p>单击“查看详情”，在“敏感数据统计详情”界面，分别从“敏感数据分类维度”、“密级维度”以及“数据库维度”三个维度展示统计信息。</p> <ul style="list-style-type: none"> 敏感数据库/总库占比：统计敏感数据库在所有数据库中的占比。 敏感数据表/总表占比：统计敏感数据表在所有数据表中的占比。 敏感数据列/总列占比：统计敏感数据列在所有数据列中的占比。 <p>说明 “周同比”表示同比上周数据发生的变化。</p>
数据列密级等级占比	<p>体现不同密级敏感数据列在数据列总量中占比的饼状图。</p> <p>单击“查看详情”，在“敏感数据统计详情”界面，分别从“敏感数据分类维度”、“密级维度”以及“数据库维度”三个维度展示统计信息。</p>
分类结果TOP5	<p>分类结果占比最高的TOP5类型。</p> <p>单击“查看详情”，在“分类结果详情”界面，查看统计信息。</p>
数据量变化	<p>体现数据量随时间变化的曲线图。</p> <p>单击“查看详情”，在“敏感数据统计详情”界面，分别从“敏感数据分类维度”、“密级维度”以及“数据库维度”三个维度展示统计信息。</p>
库量级表	<p>展示数据库实例下包含敏感数据的库表列数量信息，具体请参见查看实例详情的内容。</p> <ul style="list-style-type: none"> 数据库实例/ID：数据库实例名称/ID 主机端口：主机端口号 用户：用户名 敏感数据库：该实例下有敏感数据的数据库数量。 敏感数据表：该实例下有敏感数据的表数量。 敏感数据列：该实例下有敏感数据的列数量。

----结束

查看实例详情

步骤1 登录管理控制台。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全与合规 > 数据安全中心”。

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

步骤5 单击选择“业务域”或者“数据类型”页签。

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

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

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

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

图 5-12 实例详情



数据库名称	总表数	敏感表数	敏感等级	标签	最后扫描时间
PL_NEW c309a9f5-3a54-4d55-67e1-930a7ba02b42	0	5	L4		2024/09/24 16:41:14 GMT+08:00
SHI f775646-c8b2-4a8c-aba5-150a22985222	0	0	NA		2024/09/24 21:48:12 GMT+08:00

----结束

6 敏感数据识别

6.1 敏感数据识别概述

敏感数据自动识别分类，从海量数据中自动发现并分析敏感数据使用情况，基于数据识别引擎，对其储存结构化数据（RDS、DWS等）和非结构化数据（OBS）进行扫描、分类、分级，解决数据“盲点”，以此做进一步安全防护。

使用约束

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

使用流程

图 6-1 流程图

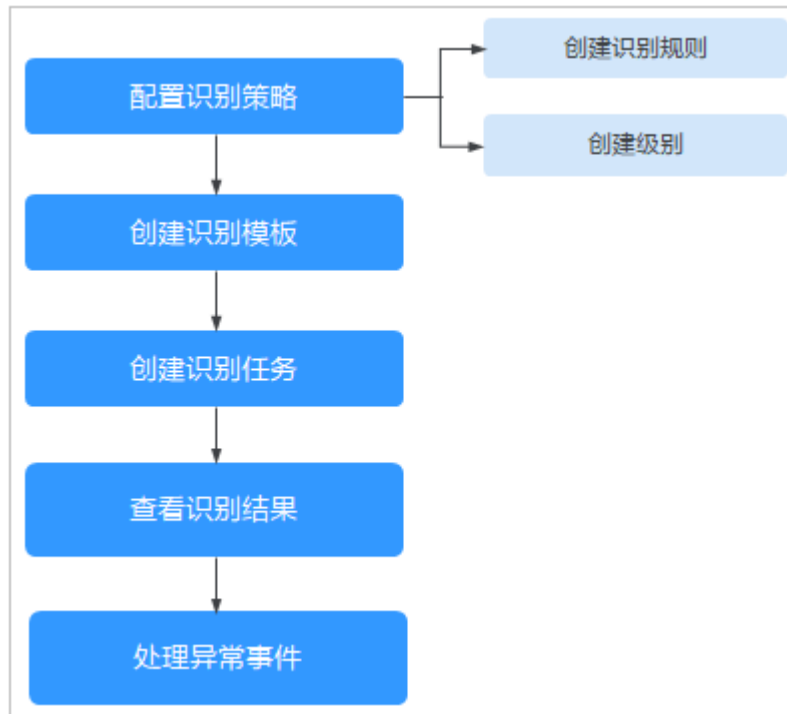


表 6-1 功能介绍

功能	描述	相关操作
识别规则	拥有华为云计算公司数据安全内置的规则可供使用，同时可以自定义新的规则，将零散的数据按照识别规则进行分类，是创建识别模板必须的配置项。	新建自定义规则
级别配置	拥有华为云计算公司数据安全内置的级别可供使用，同时可以自定义新的级别，将每条规则进行分级。	新增分级
识别模板	拥有参考华为云计算公司数据安全分类分级标准和最佳实践内置的模板供使用，同时可以自定义新的分类分级模板，将多个零散的规则进行统一分级分类管理，是创建识别任务必须的配置项。	新增识别模板
识别任务	数据安全中心会根据创建的识别任务，在选定的OBS桶、数据库、大数据、MRS或者LTS的指定范围中，自动识别敏感数据并生成识别数据和结果。	新建敏感数据识别任务
查看或下载识别结果	识别任务扫描完成后，可在识别任务列表查看识别结果，也可将识别结果下载到本地查看。	识别结果

6.2 敏感数据识别配置

6.2.1 新增识别模板

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


约束限制

一个账号最多可创建20个识别模板。

复制识别模板

步骤1 [登录管理控制台](#)。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全与合规 > 数据安全中心”。

步骤4 在左侧导航树中选择“敏感数据识别 > 识别配置”，进入“识别模板”页签。

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


步骤6 单击“确定”。

----结束

新建识别模板

步骤1 [登录管理控制台](#)。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全与合规 > 数据安全中心”。

步骤4 在左侧导航树中选择“敏感数据识别 > 识别配置”，进入识别模板页签。

步骤5 单击界面左上角“新建模板”，在“新建模板”弹框中输入“模板名称”和“描述”。

步骤6 单击“确定”，即可在识别模板列表看到新增的识别模板。

----结束

相关操作

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

6.2.2 管理识别模板

自定义模板支持修改模板内容，[编辑分类分级模板](#)介绍如何修改模板内容。

模板的规则分类支持修改，[修改模板规则分类](#)介绍如何修改规则分类。


约束限制

内置模板和设置为默认的认识模板不支持删除。

编辑识别模板


步骤1 [登录管理控制台](#)。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全与合规 > 数据安全中心”。

步骤4 在左侧导航树中选择“敏感数据识别 > 识别配置”，进入“识别模板”页签。

步骤5 单击目标模板的“详情”进入模板详情界面。


- 鼠标移动至“全部”后，单击加号创建新的分类名称。
- 鼠标移动至“分类名称”时：
 - 单击编辑按钮编辑分类名称。
 - 单击删除按钮删除分类名称。
- 单击左侧“分类名称”，在右侧查看相关分类规则。
- 右侧分类规则列表左上角单击“添加规则”，具体参见[新建自定义规则](#)章节。
- 单击“批量删除”，删除右侧勾选的规则。
- 单击“状态”列可以打开或者关闭此条规则，关闭此条规则使用该模板进行识别时此条规则不会再生效。
- 单击“操作”列“查看详情”，可以编辑规则内容。
- 单击“操作”列“删除”，删除规则。

----结束

修改模板规则分类

步骤1 [登录管理控制台](#)。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全与合规 > 数据安全中心”。

步骤4 在左侧导航树中选择“敏感数据识别 > 识别配置”，进入“识别模板”页签。

步骤5 单击目标模板的“详情”进入模板详情界面。

步骤6 单击列表选择规则，支持多选。

步骤7 在规则列表左上角单击“修改分类”，在修改分类的弹框中选择目标分类。


步骤8 单击“确定”，提示规则分类修改成功。

----结束

删除识别模板

步骤1 [登录管理控制台](#)。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全与合规 > 数据安全中心”。

步骤4 在左侧导航树中选择“敏感数据识别 > 识别配置”，进入“识别模板”页签。

步骤5 单击对应分类分级模板的“删除”。

步骤6 单击“确定”删除该模板。使用中的分类分级模板无法删除，请先删除对应的识别任务再删除分类分级模板。

----结束


6.2.3 新建自定义规则

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

操作步骤

步骤1 [登录管理控制台](#)。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全与合规 > 数据安全中心”。

步骤4 在左侧导航树中选择“敏感数据识别 > 识别配置”，进入“识别模板”页签。

步骤5 选择“识别规则”页签，进入识别规则界面。

步骤6 单击界面左上角“新建自定义规则”，弹出“添加规则”弹框。

步骤7 请参照[表6-2](#)表配置相关参数。

表 6-2 添加规则参数配置说明

参数	说明
规则名称	您可以自定义敏感数据规则名称。 规则名称需要满足以下要求： <ul style="list-style-type: none"> 1~255个字符。 字符可由中文、英文字母、数字、下划线、中划线和括号组成。 规则名称不能与已有的规则名称重复。
描述（可选）	请输入规则描述。

参数	说明
添加到模板	<ul style="list-style-type: none"> 在下拉框中依次选择“模板名称”、“模板规则分类”、“级别”将规则添加到规则模板中进行分类管理。 单击“添加”可添加到多个模板。 单击删除图标删除模板，至少保留一条模板。
匹配类型	<p>可选择“规则匹配”和“关键字匹配”。</p> <ul style="list-style-type: none"> 关键字匹配：通过关键字来执行该条敏感规则。 规则匹配：用于指定和识别文本字符串（如特定字符，单词或字符模式）的一种简洁而灵活的方式。 <p>说明 对于MRS中的HIVE数据，在敏感数据识别时，当前仅支持“匹配类型”为“规则匹配”、“规则”为“内容 > 包含”的方式。</p>
匹配逻辑	<p>选择匹配逻辑：</p> <ul style="list-style-type: none"> AND：关键字都需要包含。 OR：仅需要包含其中一个关键字。
规则	<p>“匹配类型”设置为“规则匹配”时，显示该参数，单击下拉框选择规则内容。</p> <ul style="list-style-type: none"> 选择“列名 > 包含”或者“列备注 > 包含”，输入一个关键字，判断列名或列备注中是否包含该关键字。 选择“列名 > 正则”或者“列备注 > 正则”，输入正则表达式，判断正则是否匹配。 选择“内容 > 包含”，输入一个关键字，判断内容中是否包含该关键字。 选择“内容 > 正则”，输入一个正则表达式，判断正则是否匹配。 选择“内容 > 关键字”，输入多个关键字，关键字之间是OR关系，判断内容中有任何一个关键字则为匹配。 <p>说明 对于MRS中的HIVE数据，在敏感数据识别时，当前仅支持“匹配类型”为“规则匹配”、“规则”为“内容 > 包含”的方式。</p>
规则测试	<ul style="list-style-type: none"> “匹配类型”设置为“规则匹配”时，显示该参数。 输入规则内容单击测试，在测试结果框显示该条规则的测试结果。 单击“添加”，可测试多条规则。 内置规则和自定义规则均支持规则测试，内置规则请在规则列表“操作”列单击“详情”，在“编辑规则”界面，输入规则进行测试。 <p>说明</p> <ul style="list-style-type: none"> 图片类型规则不支持规则测试。 “匹配类型”为“关键字匹配”时不支持规则测试。 仅展示测试内容的第一处匹配结果。

参数	说明
内容	<ul style="list-style-type: none">“匹配类型”设置为“关键字匹配”时，显示该参数。通过回车换行分隔多个关键字。
识别阈值配置	适用于非结构化数据，可选择低、中、高三种阈值，阈值越高要求命中的次数越多。
命中率	适用于结构化数据，可拖动滑块设置，数值越大命中率越高。

步骤8 单击“确认”完成新建规则。


----结束

6.2.4 编辑规则

操作步骤

步骤1 [登录管理控制台](#)。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全与合规 > 数据安全中心”。

步骤4 在左侧导航树中选择“敏感数据识别 > 识别配置”，进入“识别模板”页签。

步骤5 选择“识别规则”页签，进入识别规则界面。

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

----结束

6.2.5 查看内置规则

数据安全中心根据行业敏感信息内置了包含图片敏感信息、个人敏感信息、企业敏感信息等七类规则，此章节介绍如何查看DSC服务有哪些内置规则。

使用约束

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

其他图片内置规则使用约束如下所示：

驾驶证识别约束

- 只支持中国大陆驾驶证纸质版本及交管12123提供的电子驾驶证版本识别。
- 只支持识别PNG、JPG、JPEG、BMP、TIFF格式的图片。
- 图像各边的像素大小在100到8000px之间。
- 图像中驾驶证区域有效占比超过50%，保证整张驾驶证内容及其边缘包含在图像内。

- 支持图像中驾驶证任意角度的水平旋转。
- 支持少量扭曲，扭曲后图像中的驾驶证长宽比与实际驾驶证相差不超过10%。
- 能处理反光、暗光、防伪标识等干扰的图片但影响识别精度。

银行卡识别约束

- 只支持识别JPG、JPEG、PNG、BMP、TIFF格式的图片。
- 图像各边的像素大小在15到8192px之间。
- 只支持识别银行卡正面，不支持识别背面。
- 只支持识别85.60×53.98 mm常规大小的银行卡，不支持迷你卡和形状不规则的异形卡。
- 支持图像中银行卡任意角度的水平旋转。

身份证识别约束

- 支持中华人民共和国居民身份证的识别。
- 只支持识别PNG、JPG、JPEG、BMP、TIFF格式的图片。
- 图像各边的像素大小在15到8000px之间。
- 图像中身份证区域有效占比超过25%，保证整张身份证内容及其边缘包含在图像内。
- 支持图像中身份证任意角度的水平旋转。
- 支持少量扭曲，扭曲后图像中的身份证长宽比与实际身份证相差不超过10%。
- 能处理反光、暗光等干扰的图片但影响识别精度。
- 目前支持识别单张身份证的正面或者反面。
- 支持居民身份证的正反面同时识别，不支持存在两张及以上同面身份证的图片识别。

护照识别约束

- 支持中国大陆护照的全字段识别。
- 支持含有完整机读码的中国-港澳台地区及外国护照识别。
- 只支持识别PNG、JPG、JPEG、BMP、TIFF格式的图片。
- 图像各边的像素大小在15到4096px8192px之间。
- 图像中护照首页区域有效占比超过25%，保证护照首页内容及其边缘包含在图像内。
- 支持图像中护照任意角度的水平旋转。
- 支持少量扭曲，扭曲后图像中的护照长宽比与实际护照相差不超过10%。
- 能处理反光、暗光等干扰的图片但影响识别精度。

机动车行驶证识别约束

- 只支持中国大陆行驶证的识别。
- 只支持识别PNG、JPG、JPEG、BMP、TIFF格式的图片。
- 图像各边的像素大小在100到8000px之间。

- 图像中行驶证区域有效占比超过5%，保证整张行驶证内容及其边缘包含在图像内。
- 支持图像中行驶证任意角度的水平旋转。
- 支持少量扭曲，扭曲后图像中的行驶证长宽比与实际行驶证相差不超过10%。
- 能处理反光、暗光、防伪标识等干扰的图片但影响识别精度。
- 目前只支持识别2008年版的行驶证。


营业执照识别约束

- 只支持识别PNG、JPG、JPEG、BMP、TIFF格式的图片及PDF。
- 图像各边的像素在15到8192px之间。
- 图像中营业执照区域有效占比超过70%，保证整张营业执照及其边缘包含在图像内。
- 支持图像中营业执照旋转、支持少量扭曲。
- 能处理暗光等干扰的图片但影响识别精度。

查看内置规则

步骤1 [登录管理控制台](#)。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全与合规 > 数据安全中心”。

步骤4 在左侧导航树中选择“敏感数据识别 > 识别配置”，进入“识别模板”页签。

步骤5 选择“识别规则”页签，进入识别规则界面，内置规则如表6-3所示。

在规则列表上方搜索框单击选择属性筛选规则。

表 6-3 内置规则

敏感数据分类	类型
个人敏感图片信息	<ul style="list-style-type: none"> ● 驾照图片（中国内地） ● 银行卡图片（中国内地） ● 身份证图片（中国内地） ● 机动车登记证书图片（中国内地） ● 护照图片（中国内地） ● 车险保单图片（中国内地） ● 机动车行驶证图片（中国内地）

敏感数据分类	类型
个人敏感信息	<ul style="list-style-type: none"> ● 身份证号（中国内地） ● 护照号（中国内地） ● 驾照号（中国内地） ● 港澳通行证 ● 车牌号（中国内地） ● 军官证号 ● 美国社会保险号码SSN ● ITIN ● 社保相关信息 ● 车辆识别代码 ● 姓名（简体中文） ● 姓名（英文） ● 国籍 ● 性别 ● 民族 ● 生日 ● 出生地 ● 教育程度 ● 工作单位 ● 工作行业 ● 电话号码（中国内地） ● 手机号码（中国内地） ● 邮箱 ● 婚姻状况 ● 家庭成员关系 ● 宗教信仰 ● 银行卡号 ● 信用卡号 ● 万事达信用卡 ● VISA信用卡 ● 信用卡安全码
企业敏感图片信息	营业执照图片

敏感数据分类	类型
企业敏感信息	<ul style="list-style-type: none"> • 工商注册号 • 统一社会信用代码 • 纳税人识别号（税号） • 组织机构代码 • 企业类型 • 经营状态 • 企业交付信息 • 企业需求信息
设备敏感信息	<ul style="list-style-type: none"> • 唯一设备识别码IMEI • 移动设备识别码MEID • MAC地址 • SIM卡IMSI信息 • IPv4地址 • IPv6地址 • Linux-Passwd文件 • Linux-Shadow文件
密钥凭证敏感信息	<ul style="list-style-type: none"> • SSL Certificate • Access_Key_Id • Secret_Access_Key • AWS_ACCESS_KEY • AWS_SECRET_KEY • Facebook_SECRET • IAM账号密码 • GitHub_KEY • DSA私钥 • EC私钥 • 加密私钥 • RSA私钥
位置敏感信息	<ul style="list-style-type: none"> • GPS信息 • 精确地址（中国） • 省份（中国内地） • 邮政编码（中国内地） • 城市（中国内地） • 直辖市（中国） • 地址（中国内地）

敏感数据分类	类型
系统网络信息	<ul style="list-style-type: none"> • URL链接 • LDAP • OS类型
时间信息	<ul style="list-style-type: none"> • 日期 • 时间

----结束

6.2.6 新建分级

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


使用约束

最多只能拥有20个密级。

操作步骤

步骤1 [登录管理控制台](#)。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全与合规 > 数据安全中心”。

步骤4 在左侧导航树中选择“敏感数据识别 > 识别配置”，进入“识别模板”页签。

步骤5 选择“级别配置”页签，在级别配置列表左上角单击“新建分级”。

步骤6 在“新建分级”弹框中配置相关信息，参数说明如[表6-4](#)。

表 6-4 新增级别参数说明

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

步骤7 单击“确定”完成新建规则。

----结束

6.2.7 管理级别


如果您需要编辑、删除或者禁用分级，请按照此章节进行操作。

编辑级别

内置级别不支持编辑。

步骤1 [登录管理控制台](#)。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全与合规 > 数据安全中心”。

步骤4 在左侧导航树中选择“敏感数据识别 > 识别配置”，进入“识别模板”页签。

步骤5 选择“级别配置”页签查看级别配置列表。

步骤6 在目标级别操作列，单击“编辑”修改级别内容。

步骤7 单击“确定”保存修改内容。


----结束

删除级别

只有未被引用的自定义级别才能删除。

步骤1 [登录管理控制台](#)。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全与合规 > 数据安全中心”。

步骤4 在左侧导航树中选择“敏感数据识别 > 识别配置”，进入“识别模板”页签。

步骤5 选择“级别配置”页签查看级别配置列表。

步骤6 在目标级别“操作”列，单击“删除”，删除级别内容。

步骤7 单击“确定”删除。


----结束

禁用级别

内置级别不支持禁用。

步骤1 [登录管理控制台](#)。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全与合规 > 数据安全中心”。

步骤4 在左侧导航树中选择“敏感数据识别 > 识别配置”，进入“识别模板”页签。

步骤5 选择“级别配置”页签查看级别配置列表。

步骤6 在目标级别“操作”列，单击“禁用”。

说明

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

----结束

6.3 敏感数据识别任务

6.3.1 新建敏感数据识别任务

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


前提条件

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

新建敏感数据识别任务

步骤1 [登录管理控制台](#)。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全与合规 > 数据安全中心”。

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

步骤5 在任务列表左上角，单击“新建任务”。

步骤6 在弹出的“新建任务”的对话框中，参照[表6-5](#)配置相关参数。

图 6-2 新建任务

新建任务

* 任务名称

* 数据类型

- OBS
- 数据库
- 大数据
- MRS
- LTS

* 识别模板

* 识别范围 1天 2天 3天

* 识别灵敏度 低 中 高

* 识别周期 单次 每天 每周 每月

* 执行计划 立即执行 定时启动

通知主题 [查看通知主题](#)

下拉框只展示订阅状态为“已确认”的消息通知主题。

表 6-5 新建任务参数说明

参数	说明
任务名称	<p>您可以自定义敏感数据识别任务名称。</p> <p>任务名称需要满足以下要求：</p> <ul style="list-style-type: none"> ● 4~255个字符。 ● 字符可由中文、英文字母、数字、下划线或中划线组成。 ● 开头需为中文或者字母。 ● 任务名称不能与已有的任务名称重复。

参数	说明
数据类型	<p>选择识别的数据类型，可多选。</p> <ul style="list-style-type: none"> ● OBS：授权DSC访问您的华为云OBS资产后，DSC将对华为云OBS里的数据进行敏感数据识别，添加OBS资产的相关操作请参见添加OBS资产。 ● 数据库：DSC将对已授权的数据库资产进行敏感数据识别，授权数据库资产的相关操作请参见授权数据库资产。 ● 大数据：DSC将对已授权的大数据资产进行敏感数据识别，授权大数据源资产请参见授权大数据资产。 ● MRS：DSC将对已授权的MRS资产进行敏感数据识别，授权MRS资产请参见授权大数据资产。 ● LTS：DSC将对已授权的LTS资产进行敏感数据识别，添加日志流请参见添加日志流。
识别模板	<p>选择内置模板或者自定义模板，DSC将根据您选择的模板对数据进行分级分类展示。添加模板请参见新增识别模板。</p>
识别范围	<p>当“数据类型”选择“LTS”显示该参数，请选择识别日志范围，可选1天、2天和3天。</p>
识别灵敏度	<p>当“数据类型”选择“LTS”显示该参数，请选择识别日志的灵敏度，有高、中、低三种程度供选择，灵敏度越高采样数据越多。</p>
识别周期	<p>设置数据识别任务的执行策略：</p> <ul style="list-style-type: none"> ● 单次：根据设置的执行计划，在设定的时间执行一次该识别任务。 ● 每天：选择该选项，即在每天的固定时间执行该识别任务。 ● 每周：选择该选项，即在设定的每周这一时间点执行该识别任务。 ● 每月：选择该选项，即在设定的每月这一时间点执行该识别任务。
执行计划	<p>“识别周期”为“单次”时，显示该选项：</p> <ul style="list-style-type: none"> ● 立即执行：选择该选项，单击“确定”，系统立即执行数据识别任务。 ● 定时启动：在指定时间执行一次该识别任务。
启动时间	<p>“识别周期”为“每天”、“每周”、“每月”时显示该选项：</p> <p>选择识别任务执行时间。选择时间后，该任务在每天、每周、每月或者当前时间点执行此识别任务。</p>
通知主题（可选）	<ul style="list-style-type: none"> ● 单击下拉列表选择已创建消息通知主题或者单击“查看通知主题”创建新的主题，用于配置接收告警通知的终端。 ● 如果不配置通知主题，可在识别任务列表查看识别结果，详情请参考识别结果。

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

步骤8 单击“确定”，界面右上角提示创建任务成功，即识别任务创建成功。


----结束

添加识别范围

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

步骤1 [登录管理控制台](#)。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全与合规 > 数据安全中心”。

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

步骤5 单击“新建任务”，进入“新建任务”界面。

步骤6 选择“数据类型”并选择具体扫描资产名称，单击“确定”。

步骤7 在新建识别任务界面左下角单击添加识别范围，进行扫描范围配置，可以同时添加多项识别范围，参数配置如[表6-6](#)所示。

表 6-6 扫描范围配置参数说明

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

资产类型	配置参数	说明
	扫描深度	<ul style="list-style-type: none"> “全局扫描”：如果选择全局扫描是对全部数据进行扫描。 “指定扫描范围”：选择“指定扫描范围”，输入扫描深度值，根目录深度为1，依次类推，根目录深度值不能超过10。
数据库/ 大数据/MRS	资产	单击下拉框选择实例名称，支持多选。
	扫描范围配置	<ul style="list-style-type: none"> “前缀”：前缀的包含条件最多只能添加1个。如：输入前缀为 <i>dsc</i> 时，单击“添加为包含条件”添加为包含条件后就会只扫描表名前缀为 <i>dsc</i> 的表数据。如果单击“添加为不包含条件”添加为不包含条件就只扫描表名前缀除 <i>dsc</i> 以外的表数据。 “后缀”：后缀的包含条件最多只能添加1个。原理如同表名前缀所示。
LTS	资产	单击下拉框选择实例名称，支持多选。
	扫描范围配置	<ul style="list-style-type: none"> “key前缀”：添加为包含条件会扫描包含该key前缀的日志内容。添加为不包含条件会扫描除该key前缀的日志内容。 “key后缀”：原理如同key前缀所示。 <p>说明</p> <ul style="list-style-type: none"> key前缀和key后缀最多可各添加1个包含条件。 key前缀和key后缀总共可以添加10个不包含条件。

图 6-3 扫描范围配置

----结束

后续处理

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



6.3.2 立即启动识别任务

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

前提条件

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

操作步骤

- 步骤1** [登录管理控制台](#)。
- 步骤2** 单击左上角的，选择区域或项目。
- 步骤3** 在左侧导航树中，单击，选择“安全与合规 > 数据安全中心”。
- 步骤4** 在左侧导航树中，选择“敏感数据识别 > 识别任务”，进入“识别任务”界面。
- 步骤5** 在待启动任务行的“操作”列单击“立即识别”，右上角弹框提示扫描任务开始扫描，即执行成功。

说明

如果您需要停止正在执行的任务，请在目标任务“操作”列，单击“停止”。
如果需要关闭定时任务，请在目标任务“操作”列，选择“更多 > 关闭任务”。

----结束

后续处理

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

6.3.3 管理识别任务列表

该章节介绍在任务列表中查看、编辑和删除敏感数据识别任务。

前提条件

已创建并执行识别任务。

查看识别任务列表




- 步骤1** [登录管理控制台](#)。
- 步骤2** 单击左上角的，选择区域或项目。
- 步骤3** 在左侧导航树中，单击，选择“安全与合规 > 数据安全中心”。
- 步骤4** 在左侧导航树中，单击“敏感数据识别 > 识别任务”，进入识别任务界面查看任务详情，相关参数如[表6-7](#)。

表 6-7 识别任务参数

参数	说明
任务名称	<p>识别任务名称。</p> <p>单击任务名称前方的 ，查看任务下各个对象上次执行扫描的具体时间以及识别状态，并在具体对象所在行的“操作”列，可执行以下操作：</p> <ul style="list-style-type: none"> • 单击“停止”，停止对该对象的扫描。 • 单击“立即识别”，立即执行该对象的扫描任务。 • 单击“识别结果”，查看该对象的扫描结果。 • 单击“删除”，删除该对象的扫描任务。
识别模板	该任务使用的识别模板名称。
执行周期	<p>识别任务的具体执行周期。说明如下：</p> <ul style="list-style-type: none"> • 单次：识别任务仅执行一次。 • 每天：每天固定时间执行一次识别任务。 • 每周：每周固定时间执行一次识别任务。 • 每月：每月固定时间执行一次识别任务。
状态	<p>识别任务的执行状态。</p> <ul style="list-style-type: none"> • 待识别：识别任务在队列中，等待识别。 • 识别中：正在执行的识别任务。 • 识别完成：目标任务下的所有识别对象都已成功完成了扫描。 • 识别异常：目标任务下至少存在一个识别对象执行识别任务失败。 • 识别终止：正在识别中的任务，被强行停止。
上次识别时间	上一次执行该任务的具体时间。
上次识别结果	上一次该任务扫描的等级结果。


参数	说明
操作	<p>用户可以在操作栏中，执行以下操作：</p> <ul style="list-style-type: none"> • 立即识别：立即执行识别任务，具体的参见立即启动识别任务章节。 • 识别结果：查看和下载识别结果，单击“识别结果”，跳转到“结果明细”页面，DSC为您提供详细的结果分析报告，具体的参见识别结果章节。 • 开启任务，当该任务处于关闭状态时，单击“更多 > 开启任务”，具体请参见立即启动识别任务章节。 • 关闭任务，当该任务处于开启状态时，单击“更多 > 关闭任务”，具体请参见关闭识别任务。 • 编辑扫描任务，单击“更多 > 编辑”，具体请参见编辑识别任务。 • 删除扫描任务，单击“更多 > 删除”，具体请参见删除识别任务。

----结束

编辑识别任务

步骤1 [登录管理控制台](#)。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全与合规 > 数据安全中心”。

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

步骤5 在目标任务“操作”列单击“更多 > 编辑”进入“编辑任务”弹框。


步骤6 在弹框中编辑和修改任务内容，单击“确定”保存。

----结束

删除识别任务

步骤1 [登录管理控制台](#)。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全与合规 > 数据安全中心”。

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

步骤5 在目标任务“操作”列单击“更多 > 删除”。

步骤6 在确认删除的弹框中单击“确定”，删除此任务。

 **注意**


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

----结束

关闭识别任务

步骤1 [登录管理控制台](#)。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全与合规 > 数据安全中心”。

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

步骤5 在目标任务的“操作”列，单击“更多 > 关闭任务”。

 **说明**

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

----结束

6.3.4 识别结果

敏感数据识别任务扫描完成后，可在结果明细界面查看识别结果详情，同时支持将生成的识别结果下载到本地查看，本章节介绍如何查看识别结果以及下载识别结果。


前提条件

至少执行过一次敏感数据识别任务，新建敏感数据识别任务请参见[新建敏感数据识别任务](#)。

查看识别结果

步骤1 [登录管理控制台](#)。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全与合规 > 数据安全中心”。

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

步骤5 单击目标任务“操作”列的“识别结果”，进入“结果明细”界面。

步骤6 DSC统计了扫描对象存在的敏感信息总数及风险等级的数量分布图和Top10命中规则。

同时DSC针对扫描对象提供了详细的识别结果列表，单击列表左上角筛选框，选择筛选选项，可通过“列名称”或“对象名称”、“数据库名称”、“表名称”等，筛选敏感数据识别结果，识别结果列表参数说明如表6-8所示。

表 6-8 识别结果参数说明

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

步骤7 在目标扫描对象所在行的“操作”列，单击“查看分类分级结果详情”，进入“分类分级结果详情”弹框。查看结果详情和具体的样例数据。

- 单击结果详情列表左上角“添加规则”进入“添加规则”弹框中，单击“新规则”下拉框选择新规则，单击“确定”提示“替换规则成功”完成规则添加。
- 单击“操作”列“替换”进入“替换”弹框中，单击“新规则”下拉框选择新规则替换识别结果中的规则，单击“确定”提示“替换规则成功”完成规则替换。
- 单击“操作”列的“移除”，删除不需要的规则。

📖 说明


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

---结束

下载识别结果

步骤1 [登录管理控制台](#)。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全与合规 > 数据安全中心”。

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

步骤5 单击目标任务“操作”列的“识别结果”，进入“结果明细”界面。

步骤6 单击“生成结果文件”，进入“生成结果文件”弹框。

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

说明

识别结果列表支持筛选，筛选后生成的结果是筛选后的数据。

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

图 6-4 生成结果文件确认框



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

- 生成结果文件的状态包含：
 - 运行中：结果报告正在生成中。
 - 排队中：生成任务排队中。

- 如果“前往OBS桶下载结果文件”不可单击且提示“暂无有效下载文件，请先生成文件”，请单击“生成结果文件”生成后再下载。

 说明

同一个识别任务下不同子任务生成识别结果文件会互相覆盖。

步骤8 单击“前往OBS桶下载结果文件”，进入“前往OBS桶下载结果文件”弹框，查看“文件路径”等信息，单击“确定”进入对象存储服务 OBS的“桶列表”界面，按照“文件路径”中的桶名称找到对应的桶，单击桶名称进入桶，勾选识别结果文件，单击“操作”列的“下载”，下载对应的识别结果文件到本地。

步骤9 Excel格式的识别结果报表根据资产名称（资产类型）分页展示识别结果，关键字段有“匹配规则”、“分级结果”、“分类结果”和“分类分级模板”。

图 6-5 识别结果报表样例

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

----结束

7 策略中心

7.1 策略基线

7.1.1 策略基线概述

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

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

使用场景

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

- 进入“资产地图”，选择某个资产，进入“安全防护策略分析”页面，查看资产的加密、备份、审计等安全配置的现状和策略基线的具体要求，可单击“前往查看”或者“策略基线”前往对应数据源的管理控制台根据策略要求配置相关权限。

图 7-1 安全防护策略分析

The screenshot shows the 'Security Protection Strategy Analysis' page for an RDS instance named 'rds-zyj-pg15'. The instance is marked as 'Scanned' (已扫描) and 'Security Protection in Progress' (安全防护中) with an L4 risk level. The instance ID is 866d4dcfc0f84bc1a9ac932fcd34ed27in03 and it was created on 2024/12/19 02:05:57 GMT+08:00. The 'Basic Information' (基础信息) section lists: Type (类型) as 'Intranet IP' (内网IP), RDS, Port (端口) as 5432, Engine Type (引擎类型) as PostgreSQL, and Version (版本) as 15. Below this, there are three tabs: 'Sensitive Data Identification' (敏感数据识别), 'Security Protection Strategy Analysis' (安全防护策略分析), and 'Data Export Analysis' (数据出口分析). The 'Storage Encryption' (存储加密) section shows it is 'Not Enabled' (未开启) with a 'Go to View' (前往查看) link. The text below explains that according to the 'Strategy Baseline' (策略基线) requirements, L4 data does not require encryption to ensure confidentiality. The 'Run Mode' (运行模式) section shows it is 'Not Identified Risk' (未识别风险) with a 'Go to Modify' (前去修改) link. The text below explains that according to the 'Strategy Baseline' requirements, L4 data should be forced to use primary/standby or clustering to ensure high availability.

- 进入“资产地图”，单击“评分详情”，可查看所有资产的加密、备份、审计等安全配置的现状和策略基线的具体要求，可单击“前往查看/前往开启”或者“策略基线”前往对应数据源的管理控制台根据策略要求配置相关权限。

图 7-2 安全策略分析

The screenshot shows the 'Security Strategy Analysis' page for an asset named 'dsc-hive'. The asset is marked as 'OBS' and 'Not Identified Risk' (未识别风险). The 'Service Encryption' (服务端加密) section shows it is 'Not Identified Risk'. The 'Bucket Policy' (桶策略) section shows it is 'Not Identified Risk' with a 'Recommend Handling' (建议处理) label. The text below explains that according to the 'Strategy Baseline' requirements, general data is recommended not to be directly provided to external public access, query, or download channels. The 'OBS Audit' (OBS审计) section shows it is 'Not Identified Risk' with a 'Go to Enable' (前往开启) link.

内置措施

DSC在数据全生命周期各阶段内置了措施供您选择，各生命周期内置措施介绍如下。

采集阶段

- 分类分级：对采集的数据进行分类分级标识，并对不同级别的数据实施相应的安全管理策略和保障措施。
- 跟踪记录：跟踪和记录数据的采集过程，包括来源、时间、类型、数量等信息。
- 数据源安全认证：应结合口令密码、证书、设备物理位置、网络接入方式等多种因素对数据采集设备或系统的安全性进行增强验证。
- 加密：对采集的数据进行加密。

传输阶段

- 完整性校验：对数据传输过程实施数据完整性校验。
- 可用性保护：采用设备冗余、线路冗余等措施，确保数据传输的可用性。
- 身份鉴别和认证：应对通信双方进行身份鉴别和认证，确保数据传输双方可信任。
- 加密：应采取数据加密、安全传输通道或安全传输协议进行数据传输加密。
- 审批和审计：应事先经过审批授权，并留存数据传输日志用于审计。

存储阶段

- 分类分级：对静态存储数据进行分类分级标识，并对不同级别的数据实施相应的安全管理策略和保障措施。
- 存储隔离：将不同级别的数据分开存储，并采取物理或逻辑隔离机制，对不同区域之间的数据流动进行安全管控。
- 完整性保护：应采用密码技术、完整性监控等措施保证数据完整性。
- 可靠性保护：采取主备、集群等方式保障存储数据的高可用性。
- 安全管控：对数据存储设备和系统进行必要的安全管控，包括操作终端的鉴权机制、系统的访问控制、系统配置的安全基线等。
- 备份与恢复：建立数据容灾备份和恢复机制，做好数据容灾应急预案，一旦发生数据丢失或破坏，可及时检测和恢复数据。
- 加密：应采取数据加密、磁盘加密等方式保证数据存储保密性。

使用阶段

- 身份认证与访问控制：对访问者进行身份认证，将数据访问权限与实际访问者的身份或角色进行关联，防止数据的非授权访问。
- 审计：遵循可审计原则，数据访问和使用过程应留存相关操作日志，支撑实时或事后审计。
- 审核与二次授权：建立访问权限申请和审核批准机制，并对实际操作和申请操作进行验证；建立多因素认证或二次授权机制。
- 脱敏：数据访问、展示、加工、开发测试等过程中应采取脱敏、匿名化等技术措施防止敏感信息泄露。
- 阻断：采取数据库防火墙等技术措施实时监测和拦截针对数据库的SQL注入、漏洞利用等恶意攻击行为。

- 公网防护：不允许直接提供Internet等外部查询、下载通道。

共享阶段

- 安全审计：数据共享过程留存日志记录，对共享的数据进行安全审计。
- 阻断：建立应急响应机制或技术手段，必要时及时切断数据共享。
- 脱敏：对含敏感字段的数据进行脱敏。
- 加密：因业务需要无法对数据进行脱敏的，应对数据进行加密、选用安全可靠的传输协议或在安全可控的环境中进行共享。
- 水印：对共享数据添加水印并建立水印溯源机制，以达到泄露时溯源定责的目的。
- 审核与监督：建立数据共享审批机制，采取一次一审批策略，必须获得数据Owner或其授权人审批，并对共享出去的数据进行例行的安全监督和审查。


销毁阶段

- 审核与监督：建立销毁的审批和监督流程，采取一次一审批的机制，必须获得数据Owner或其授权人员审批，并对实施过程进行监督。
- 销毁留证：记录数据销毁操作详情，从而便于管理员等角色针对数据销毁操作进行查看、追踪、确认、取证等活动。
- 物理销毁：应采用物理销毁的方式对存储介质进行处理，如消磁或磁介质、粉碎、融化等。
- 备份销毁：对保存数据副本的存储介质进行数据销毁处理，确保数据不可还原。

操作步骤

步骤1 [登录管理控制台](#)。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全与合规 > 数据安全中心”。

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

----结束

7.1.2 数据采集

配置措施

步骤1 按照[操作步骤](#)进入“策略基线”界面。

步骤2 选择“采集”页签。

步骤3 单击“配置措施”进入“配置措施”界面。

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

步骤4 取消勾选不需要的内置措施，取消勾选的措施将不会在策略基线表中显示。

步骤5 单击“新增”，进入“新增自定义保护措施”界面。

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

步骤6 单击“确定”进入策略基线表查看配置措施。

----结束

配置数据保护类型

步骤1 参照[操作步骤](#)进入“策略基线”界面。

步骤2 单击“配置数据保护类型”进入“配置数据保护类型”界面。

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

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

步骤4 自定义数据保护类型：新增的自定义数据保护类型将显示到策略基线表中。

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

步骤5 单击“确定”，在策略基线表中查看数据保护类型。

----结束

修改保护要求

步骤1 参照[操作步骤](#)进入“策略基线”界面。

步骤2 单击“修改保护要求”可对数据保护类型对应措施的保护要求进行修改。

步骤3 如单击“一般数据保护”行的“分类分级”列的下拉框选择：

- 不要求
- 建议
- 强制

图 7-3 修改保护要求

数据保护类型	分类分级	脱敏记录	加密	脱敏
一般数据保护	不要求	不要求	不要求	不要求
<input type="checkbox"/> 分级数据保护	不要求 建议 强制	不要求	不要求	不要求
L1	不要求	建议	不要求	不要求
L4	不要求	强制	不要求	不要求
L3	不要求	不要求	不要求	不要求
S1	不要求	不要求	不要求	不要求

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

----结束

7.1.3 数据传输

配置措施

步骤1 参照[操作步骤](#)进入“策略基线”界面。

步骤2 选择“传输”页签。

步骤3 单击“配置措施”进入“配置措施”界面。

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

步骤4 单击取消勾选不需要的措施，取消勾选的措施将不会在策略基线表中显示。

步骤5 单击“新增”，进入“新增自定义保护措施”界面。

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

步骤6 单击“确定”进入策略基线表查看配置措施。

----结束

配置数据保护类型

步骤1 参照[操作步骤](#)进入“策略基线”界面。

步骤2 选择“传输”页签。

步骤3 单击“配置数据保护类型”进入“配置数据保护类型”界面。

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

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

步骤5 自定义数据保护类型：新增的自定义数据保护类型将显示到策略基线表中。

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

步骤6 单击“确定”，在策略基线表中查看数据保护类型。

----结束

修改保护要求

步骤1 参照[操作步骤](#)进入“策略基线”界面。

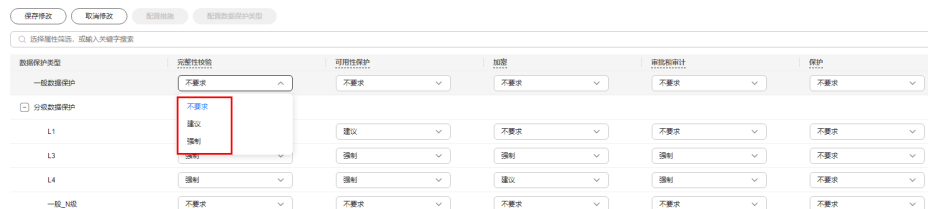
步骤2 选择“传输”页签。

步骤3 单击“修改保护要求”可对数据保护类型对应措施的保护要求进行修改。

步骤4 如单击“一般数据保护”行的“分类分级”列的下拉框选择：

- 不要求
- 建议
- 强制

图 7-4 修改保护要求



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

----结束

7.1.4 数据存储

配置措施

步骤1 参照[操作步骤](#)进入“策略基线”界面。

步骤2 选择“存储”页签。

步骤3 单击“配置措施”进入“配置措施”界面。

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

步骤4 单击取消不需要的措施，取消勾选的措施将不会在策略基线表中显示。

步骤5 单击“新增”，进入“新增自定义保护措施”界面。

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

步骤6 单击“确定”进入策略基线表查看配置措施。

----结束

配置数据保护类型

步骤1 参照[操作步骤](#)进入“策略基线”界面。

步骤2 选择“存储”页签。

步骤3 单击“配置数据保护类型”进入“配置数据保护类型”界面。

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

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

步骤5 自定义数据保护类型：新增的自定义数据保护类型将显示到策略基线表中。

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

步骤6 单击“确定”，在策略基线表中查看数据保护类型。

----结束

修改保护要求

步骤1 参照[操作步骤](#)进入“策略基线”界面。

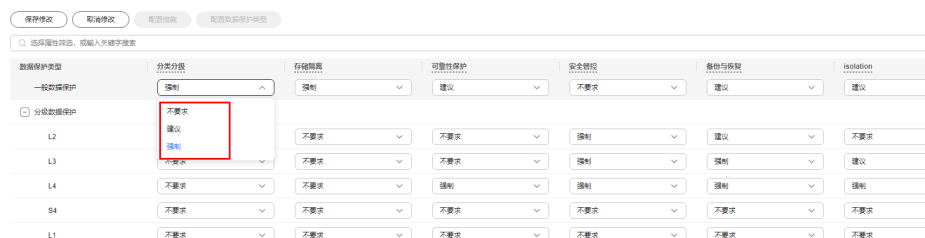
步骤2 选择“存储”页签。

步骤3 单击“修改保护要求”可对数据保护类型对应措施的保护要求进行修改。

步骤4 如单击“一般数据保护”行的“分类分级”列的下拉框选择：

- 不要求
- 建议
- 强制

图 7-5 修改保护要求



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

----结束

7.1.5 数据使用

配置措施

步骤1 参照[操作步骤](#)进入“策略基线”界面。

步骤2 选择“使用”页签。

步骤3 单击“配置措施”进入“配置措施”界面。

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

步骤4 单击取消不需要的措施，取消勾选的措施将不会在策略基线表中显示。

步骤5 单击“新增”，进入“新增自定义保护措施”界面。

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

步骤6 单击“确定”进入策略基线表查看配置措施。

----结束

配置数据保护类型

步骤1 参照[操作步骤](#)进入“策略基线”界面。

步骤2 选择“使用”页签。

步骤3 单击“配置数据保护类型”进入“配置数据保护类型”界面。

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

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

步骤5 自定义数据保护类型：新增的自定义数据保护类型将显示到策略基线表中。

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

步骤6 单击“确定”，在策略基线表中查看数据保护类型。

----结束

修改保护要求

步骤1 参照[操作步骤](#)进入“策略基线”界面。

步骤2 选择“使用”页签。

步骤3 单击“修改保护要求”可对数据保护类型对应措施的保护要求进行修改。

步骤4 如单击“一般数据保护”行的“身份认证与访问控制”列的下拉框选择：

- 不要求
- 建议
- 强制

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

----结束

7.1.6 数据共享

配置措施

步骤1 参照[操作步骤](#)进入“策略基线”界面。

步骤2 选择“共享”页签。

步骤3 单击“配置措施”进入“配置措施”界面。

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

步骤4 单击取消不需要的措施，取消勾选的措施将不会在策略基线表中显示。

步骤5 单击“新增”，进入“新增自定义保护措施”界面。

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

步骤6 单击“确定”进入策略基线表查看配置措施。

----结束

配置数据保护类型

步骤1 参照[操作步骤](#)进入“策略基线”界面。

步骤2 选择“共享”页签。

步骤3 单击“配置数据保护类型”进入“配置数据保护类型”界面。

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

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

步骤5 自定义数据保护类型：新增的自定义数据保护类型将显示到策略基线表中。

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

步骤6 单击“确定”，在策略基线表中查看数据保护类型。

----结束

修改保护要求

步骤1 参照[操作步骤](#)进入“策略基线”界面。

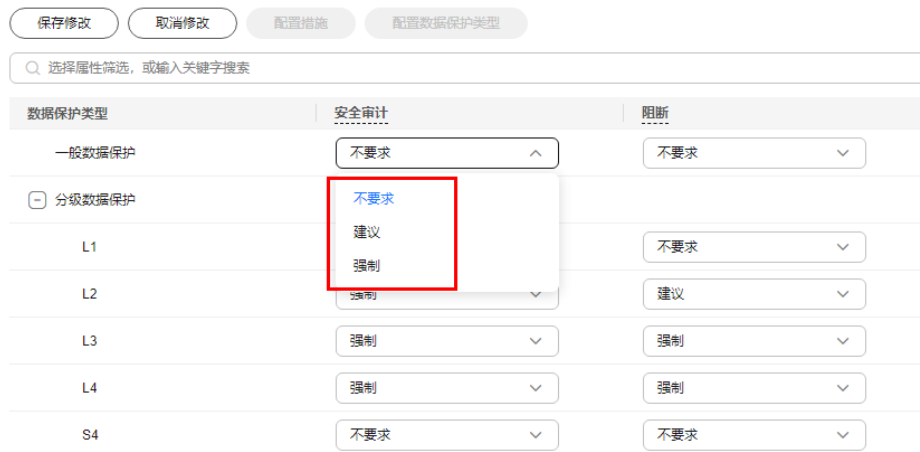
步骤2 选择“共享”页签。

步骤3 单击“修改保护要求”可对数据保护类型对应措施的保护要求进行修改。

步骤4 如单击“一般数据保护”行的“安全审计”列的下拉框选择：

- 不要求
- 建议
- 强制

图 7-6 修改保护要求



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

----结束

7.1.7 数据销毁

配置措施

步骤1 参照[操作步骤](#)进入“策略基线”界面。

步骤2 选择“销毁”页签。

步骤3 单击“配置措施”进入“配置措施”界面。

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

步骤4 单击取消不需要的措施，取消勾选的措施将不会在策略基线表中显示。

步骤5 单击“新增”，进入“新增自定义保护措施”界面。

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

步骤6 单击“确定”进入策略基线表查看配置措施。

----结束

配置数据保护类型

步骤1 参照[操作步骤](#)进入“策略基线”界面。

步骤2 选择“销毁”页签。

步骤3 单击“配置数据保护类型”进入“配置数据保护类型”界面。

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

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

步骤5 自定义数据保护类型：新增的自定义数据保护类型将显示到策略基线表中。

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

步骤6 单击“确定”，在策略基线表中查看数据保护类型。

----结束

修改保护要求

步骤1 参照[操作步骤](#)进入“策略基线”界面。

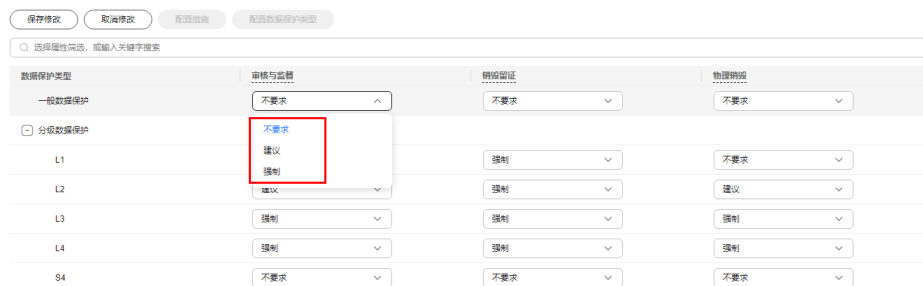
步骤2 选择“销毁”页签。

步骤3 单击“修改保护要求”可对数据保护类型对应措施的保护要求进行修改。

步骤4 如单击“一般数据保护”行的“审核与监督”列的下拉框选择：

- 不要求
- 建议
- 强制

图 7-7 修改保护要求



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

----结束

7.2 策略管理

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

数据库加密支持的数据库类型及版本

数据源类型	版本
MySQL	5.6、5.7、5.8、8.0
SQL Server	<ul style="list-style-type: none"> • 2019_SE、2019_EE、2019_WEB • 2017_SE、2017_EE、2017_WEB • 2016_SE、2016_EE、2016_WEB • 2014_SE、2014_EE • 2012_SE、2012_EE、2012_WEB • 2008_R2_EE、2008_R2_WEB
Oracle	11、12
PostgreSQL	13、12、11、10、9.6、9.5、9.4
KingBase(人大金仓)	V8
DMDBMS(达梦)	7、8
TDSQL	10.3.X
DWS	8.1.X

策略类型介绍

- “数据库审计”：监控和记录数据库活动，以确保数据的完整性、安全性和合规性。
- “数据库加密”：对数据进行加密处理，以确保数据的机密性和完整性，防止未经授权的访问和数据泄露。
- “数据库水印”：对数据嵌入难以察觉的标识符，验证数据的真实性、所有权和追踪泄露源头。
- “数据库静态脱敏”：对敏感数据进行脱敏处理，以确保隐私和安全，同时保留数据结构和统计特性。
- “数据库动态脱敏”：对敏感数据进行实时脱敏处理，以确保未经授权的数据不可访问。

创建策略

本章节介绍如何创建策略。

创建数据库审计策略


对接DBSS服务，对免Agent审计的数据库实例进行监控和记录数据库，以确保数据的完整性、安全性和合规性。

前提条件

已开启DBSS且已添加实例。

步骤1 [登录管理控制台](#)。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全与合规 > 数据安全中心”。

步骤4 选择“策略中心 > 策略管理”，进入策略管理界面。

步骤5 左上角单击“创建策略”，进入“创建策略”界面。

步骤6 选择“数据库数据库审计”策略类型。

步骤7 单击“开始配置”，进入数据库审计策略类型配置界面。

步骤8 参照[表7-1](#)进行参数配置：

表 7-1 数据库审计策略类型参数配置表

参数	说明
策略名称	输入策略名称，只能由中文字符、英文字母、数字、下划线和中划线组成，长度不超过255个字符。
关联实例	单击下拉框选择数据库审计实例。
目标数据源	单击下拉框选择目标数据源，仅支持免Agent审计的数据库实例。
是否显示结果集	开启记录结果集后，系统将对SQL结果内容进行记录，可在日志中进行查看。如果未开启，日志详情中SQL结果内容为空。 记录结果集存在信息泄露风险，不建议开启。
隐私数据脱敏	通过编写脱敏规则，防止敏感数据泄露，建议开启。

步骤9 单击“保存并下发”，进入策略列表查看新创建的策略。

----结束

创建数据库加密策略

对数据进行加密处理，以确保数据的机密性和完整性，防止未经授权的访问和数据泄露。


前提条件

已在DBSS购买数据加密与访问控制。

已对待加密的数据源进行敏感数据识别。

步骤1 [登录管理控制台](#)。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全与合规 > 数据安全中心”。

步骤4 选择“策略中心 > 策略管理”，进入策略管理界面。

步骤5 左上角单击“创建策略”，进入“创建策略”界面。

步骤6 选择“数据库加密”策略类型。

步骤7 单击“开始配置”，进入数据加密策略类型配置界面。

步骤8 参照[表7-2](#)进行参数配置：

表 7-2 数据加密策略类型参数配置表

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

步骤9 单击“保存并下发”，进入策略列表查看新创建的策略。


----结束

创建数据库水印策略

对数据嵌入难以察觉的标识符，验证数据的真实性、所有权和追踪泄露源头。

步骤1 [登录管理控制台](#)。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全与合规 > 数据安全中心”。

步骤4 选择“策略中心 > 策略管理”，进入策略管理界面。

步骤5 左上角单击“创建策略”，进入“创建策略”界面。

步骤6 选择“数据库水印”策略类型。

步骤7 单击“开始配置”，进入数据库水印界面，创建水印注入或者水印提取任务，详细操作请参见[数据库水印注入](#)和[数据库水印提取](#)。


----结束

创建数据库静态脱敏

对敏感数据进行脱敏处理，以确保隐私和安全，同时保留数据结构和统计特性。

步骤1 [登录管理控制台](#)。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全与合规 > 数据安全中心”。

步骤4 选择“策略中心 > 策略管理”，进入策略管理界面。

步骤5 左上角单击“创建策略”，进入“创建策略”界面。

步骤6 选择“数据库静态脱敏”策略类型。

步骤7 单击“开始配置”，进入数据脱敏界面，创建数据脱敏任务，详细操作请参见[数据静态脱敏](#)。


----结束

创建数据库动态脱敏策略

对敏感数据进行实时脱敏处理，以确保未经授权的数据不可访问。

步骤1 [登录管理控制台](#)。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全与合规 > 数据安全中心”。

步骤4 选择“策略中心 > 策略管理”，进入策略管理界面。

步骤5 左上角单击“创建策略”，进入“创建策略”界面。

步骤6 选择“数据库动态脱敏”策略类型。

步骤7 单击“开始配置”，进入数据库动态脱敏策略配置界面。

步骤8 参照表7-3进行参数配置：

表 7-3 数据库动态脱敏策略类型参数配置表

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

步骤9 单击“保存并下发”，进入策略列表查看新创建的策略。

----结束

相关操作

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

📖 说明

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

7.3 流转日志采集

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


前提条件

- 已开通DBSS服务，并安装数据库实例，开通DBSS服务请参见[购买数据库安全审计](#)。
- 已创建API数据安全防护实例，具体请参见[购买API数据安全防护实例并绑定弹性公网IP](#)。

开通流转采集

步骤1 [登录管理控制台](#)。


步骤2 单击左上角的，选择区域或项目。


步骤3 在左侧导航树中，单击，选择“安全与合规 > 数据安全中心”。

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

步骤5 实例列表参数说明如[表7-4](#)所示。

表 7-4 实例列表

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

步骤6 单击 打开流转日志采集开关，开通日志采集。


步骤7 单击左上角“批量开通流转采集”批量开通日志流转采集。

----结束

关闭流转采集

步骤1 [登录管理控制台](#)。


步骤2 单击左上角的，选择区域或项目。


步骤3 在左侧导航树中，单击，选择“安全与合规 > 数据安全中心”。

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

步骤5 实例列表参数说明如[表7-5](#)所示。

表 7-5 实例列表

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

步骤6 单击 关闭流转日志采集开关，关闭日志采集。

单击左上角“批量关闭流转采集”批量关闭日志流转采集。

----结束

8 数据资产保护

8.1 数据脱敏

8.1.1 数据脱敏概述

DSC的数据脱敏支持静态脱敏和动态脱敏。您可以对指定数据类型配置脱敏规则实现敏感数据静态脱敏，同时，您也可以使用[数据动态脱敏API接口](#)实现数据的动态脱敏，全方位确保敏感信息不被泄露，数据安全中心支持的脱敏算法如[脱敏算法和对应的使用场景](#)所示。

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

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

操作流程

图 8-1 静态脱敏操作流程

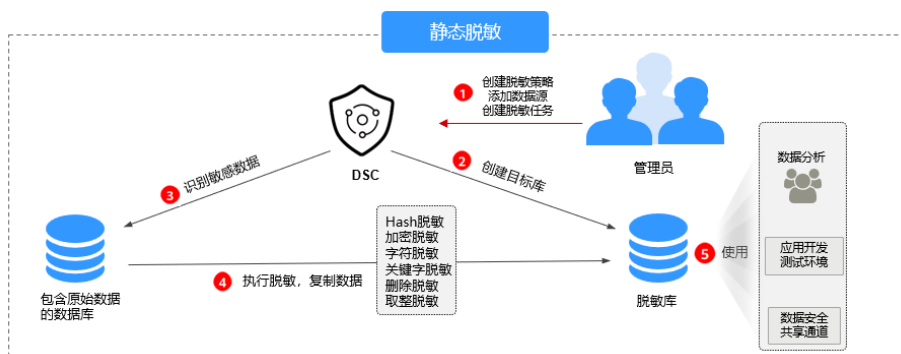
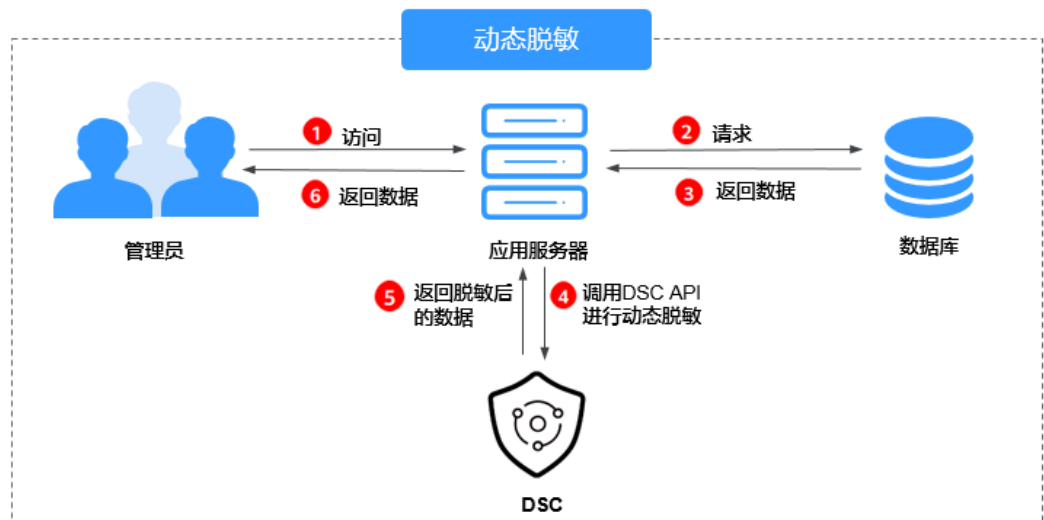


图 8-2 动态脱敏操作流程



8.1.2 配置和查看脱敏规则

脱敏算法和对应的使用场景

表 8-1 脱敏算法说明

脱敏算法	脱敏方式说明	使用场景
Hash脱敏	<p>使用Hash函数对敏感数据进行脱敏。支持SHA256和SHA512。</p> <ul style="list-style-type: none"> SHA256 将数据库表中字符串类型字段的内容用其SHA256的摘要值代替。 该算法执行完后，结果的长度可能超过原表中列允许的最大长度。该算法按照SHA256输出长度调整列的长度。 SHA512 将数据库表中字符串类型字段的内容用其SHA512的摘要值代替。 该算法执行完后，结果的长度可能超过原表中列允许的最大长度。该算法按照SHA512输出长度调整列的长度。 	<ul style="list-style-type: none"> 敏感类型： <ul style="list-style-type: none"> 密钥类 适用场景： <ul style="list-style-type: none"> 数据存储
加密脱敏	<p>通过加密算法和加密主密钥生成指定的数据密钥，使用数据密钥对敏感数据进行加密达到数据脱敏的效果。</p> <p>DSC支持AES256和SM4两种加密算法。</p>	<ul style="list-style-type: none"> 敏感类型： <ul style="list-style-type: none"> 个人敏感 企业敏感 适用场景： <ul style="list-style-type: none"> 数据存储

脱敏算法	脱敏方式说明	使用场景
字符掩盖	<p>使用指定字符*或随机字符（随机字符包含随机数字、随机字母、随机数字字母三种类型）方式掩盖部分内容。支持以下六种脱敏方式：</p> <ul style="list-style-type: none"> 保留前n后m 保留自x至y 掩盖前n后m 掩盖自x至y 特殊字符前掩盖 特殊字符后掩盖 <p>说明 敏感数据保护服务中已预置多种字符脱敏模板。</p>	<ul style="list-style-type: none"> 敏感类型： <ul style="list-style-type: none"> 个人敏感 适用场景： <ul style="list-style-type: none"> 数据使用 数据分享
关键字替换	<p>在指定列中查找关键词并替换。</p> <p>例如，目标字符串为“张三在家吃饭”，算法执行完后映射为“张先生在家吃饭”，其中指定将“张三”替换为“张先生”。</p> <p>该算法执行完后，结果的长度可能超过数据库允许的最大长度。该算法将超出部分截断后插入数据库。</p>	<ul style="list-style-type: none"> 敏感类型： <ul style="list-style-type: none"> 个人敏感 企业敏感 设备敏感 适用场景： <ul style="list-style-type: none"> 数据存储 数据分享
删除脱敏	<p>将指定字段设置为Null或空值进行脱敏。</p> <ul style="list-style-type: none"> Null脱敏 将任意类型字段设置为NULL。 对于列属性设置为“NOT NULL”的字段，该算法在拷贝时将该列属性修改为“NULL”。 空值脱敏 将指定字段内容设置为空值。 具体来说，将字符型的字段设置为空串，数值类的字段设置为0，日期类的字段设置为1970，时间类的字段设置为零点。 	<ul style="list-style-type: none"> 敏感类型： <ul style="list-style-type: none"> 个人敏感 企业敏感 设备敏感 适用场景： <ul style="list-style-type: none"> 数据存储 数据分享

脱敏算法	脱敏方式说明	使用场景
取整脱敏	<p>针对日期或数字特定参数进行取整运算。</p> <ul style="list-style-type: none"> 日期取整 年之后字段全部取整。示例： “2019-05-12 -> 2019-01-01” 或 “2019-05-12 08:08:08 -> 2019-01-01 00:00:00” 月之后字段全部取整。示例： “2019-05-12 -> 2019-05-01” 或 “2019-05-12 08:08:08 -> 2019-05-01 00:00:00” 日之后字段全部取整。示例： “2019-05-12 -> 2019-05-12” 或 “2019-05-12 08:08:08 -> 2019-05-12 00:00:00” 小时之后字段全部取整。示例： “08:08:08 -> 08:00:00” 或 “2019-05-12 08:08:08 -> 2019-05-12 08:00:00” 分钟之后字段全部取整。示例： “08:08:08 -> 08:08:00” 或 “2019-05-12 08:08:08 -> 2019-05-12 08:08:00” 秒之后字段全部取整。示例： “08:08:08.123 -> 08:08:08.000” 或 “1575612731312 -> 1575612731000” 数字取整 针对指定数字进行取整运算。 	<ul style="list-style-type: none"> 敏感类型： 通用敏感 适用场景： <ul style="list-style-type: none"> - 数据存储 - 数据使用

配置和查看脱敏规则

您可以对指定数据类型配置脱敏规则实现敏感数据静态脱敏，本章节介绍脱敏算法支持的数据类型及如何添加和测试脱敏算法。

Hash 脱敏

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

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

步骤1 [登录管理控制台](#)。

步骤2 单击左上角的，选择区域或项目。


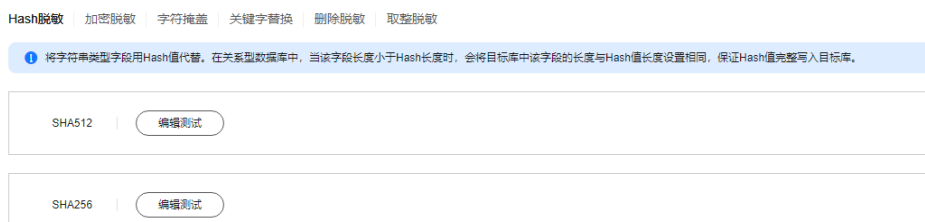
- 步骤3** 在左侧导航树中，单击 ，选择“安全与合规 > 数据安全中心”。
- 步骤4** 在左侧导航树中选择“数据资产保护 > 数据静态脱敏”，并选择“脱敏规则”页签，进入Hash脱敏的页面。

图 8-3 Hash 脱敏



- 步骤5** 在选择的SHA256或SHA512算法所在列，单击“编辑测试”。
- 步骤6** 在“编辑测试”页面中，“脱敏算法”选择“Hash脱敏”，输入“原始数据”，单击“测试”，“脱敏结果”文本框中展示已完成脱敏的数据。


图 8-4 Hash 脱敏测试



---结束

加密脱敏

通过加密算法和加密主密钥生成一种加密配置，达到数据脱敏的效果。

- 步骤1** [登录管理控制台](#)。
- 步骤2** 单击左上角的 ，选择区域或项目。


- 步骤3** 在左侧导航树中，单击 ，选择“安全与合规 > 数据安全中心”。
- 步骤4** 在左侧导航树中选择“数据资产保护 > 数据静态脱敏”，并选择“脱敏规则”页签，进入Hash脱敏的页面。

图 8-5 Hash 脱敏



- 步骤5** 选择“加密脱敏”页签，进入“加密脱敏”页面。
- “主密钥算法”：在下拉框选择加密算法，DSC提供了“AES256”和“SM4”加密算法供您选择。

表 8-2 主密钥算法介绍

密钥类型	算法类型	密钥规格	说明	用途
对称密钥	AES	AES_256	AES对称密钥	少量数据的加解密或用于加解密数据密钥。
对称密钥	SM4	SM4	国密SM4对称密钥	少量数据的加解密或用于加解密数据密钥。

- “KMS加密”可以选择“从KMS密钥中选择”和“输入KMS密钥ID”两种方式：
 - “从KMS密钥中选择”：单击下拉框选择已有的KMS主密钥，如果没有可选择的主密钥，单击“创建KMS主密钥”进行创建，创建方式详情请参见[创建KMS主密钥](#)。


 说明

- 默认使用凭据管理为您创建的默认主密钥csm/default作为当前凭证的加密主密钥，您可以前往KMS服务页面创建用户密钥，使用自定义加密密钥。
- “输入KMS密钥ID”：输入位于当前Region的密钥。
- 单击下拉框选择“数据密钥长度”，有128、192和256三种供选择。

步骤6 配置完成后，单击“生成加密配置”。

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

说明

单击  打开轮换策略，轮换周期到期后会更新当前加密配置提升安全性。

----结束


字符掩盖

使用指定字符“*”或随机字符，按照指定方式遮盖部分内容。

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

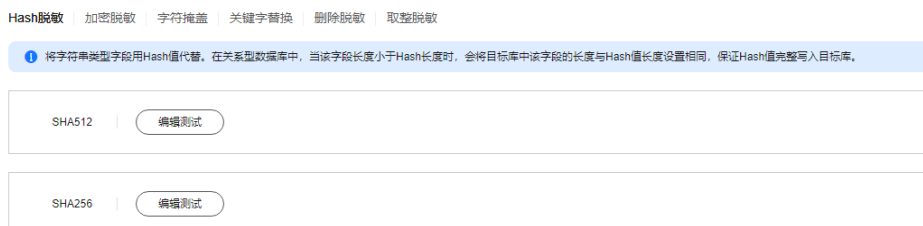
步骤1 登录管理控制台。

步骤2 单击左上角的 ，选择区域或项目。

步骤3 在左侧导航树中，单击 ，选择“安全与合规 > 数据安全中心”。

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

图 8-6 Hash 脱敏



步骤5 选择“字符掩盖”页签，进入“字符掩盖”页面。

步骤6 单击“添加”，配置字符脱敏规则。

图 8-7 添加字符脱敏

添加字符脱敏

* 名称

* 选择规则

* 掩盖位置 n m

* 掩盖方式

* 掩盖字符

测试

原始数据

脱敏结果

we3*****ff

步骤7 按照如表8-3所示配置相关参数，输入“原始数据”，单击“测试”，在“脱敏结果”文本框中展示已完成脱敏的数据。

表 8-3 字符脱敏参数配置

参数	说明
名称	输入字符脱敏名称，只能由中文、英文字母、数字、下划线或中划线组成，且不能超过255个长度。

参数	说明
选择规则	有如下规则供选择： <ul style="list-style-type: none"> “保留前n后m” “保留自x至y” “遮盖前n后m” “遮盖自x至y” “特殊字符前遮盖” “特殊字符后遮盖”
遮盖位置	输入选择的对应规则的数值，如选择“保留自x至y”，x输入3，y输入6，则保留第3位到第6位的字符。
遮盖方式	遮盖方式包含： <ul style="list-style-type: none"> 固定字符：用固定字符替换指定位置字符。 随机字符：用随机字符替换指定位置字符。
遮盖字符	“遮盖方式”选择“固定字符”时显示该参数，输入指定字符。
随机方式	随机方式包含： <ul style="list-style-type: none"> 随机字母 随机数字 随机数字字母组合

步骤8 测试确认无误后，单击“保存”。

说明

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


----结束

关键字替换

利用自定义的字符串替换数据中匹配到的关键字，达到脱敏的效果。例如：原始数据为abcde**fg**bcde**fg**kjkoij，“关键字”配置为“bcde”，“替换字符串”配置为12，则“脱敏结果”显示为a12**fg**12**fg**kjkoij。

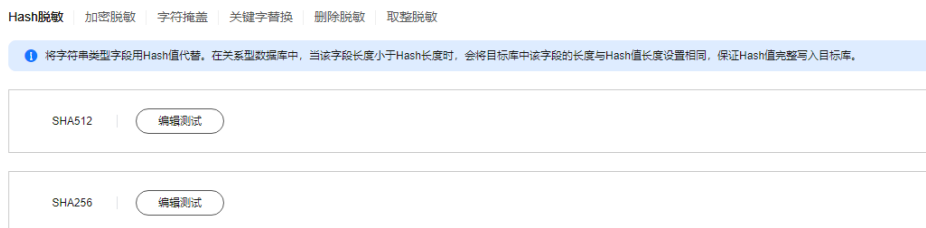
步骤1 [登录管理控制台](#)。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全与合规 > 数据安全中心”。

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

图 8-8 Hash 脱敏



步骤5 选择“关键字替换”页签，进入“关键字替换”页面。

步骤6 单击左上角“添加”，进入“添加关键字”界面。

步骤7 设置需要替换的“关键字”，以及“替换字符串”。

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

图 8-9 添加关键字

添加关键字

★ 关键字

★ 替换字符串

测试

原始数据

脱敏结果

1ac45ac67ac89

步骤8 输入“原始数据”，单击“测试”，在“脱敏结果”文本框中展示已完成脱敏的数据。

步骤9 测试确认无误后，单击“保存”。

- 在关键字替换规则列表的“操作”列，单击“编辑测试”修改脱敏规则。
- 在关键字替换规则列表的“操作”列，单击“删除”删除脱敏规则。

---结束

删除脱敏


系统内置“Null脱敏”和“空值脱敏”两种算法。

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

删除脱敏为DSC内置的脱敏规则，不需要配置，可参考以下方法查看脱敏规则。

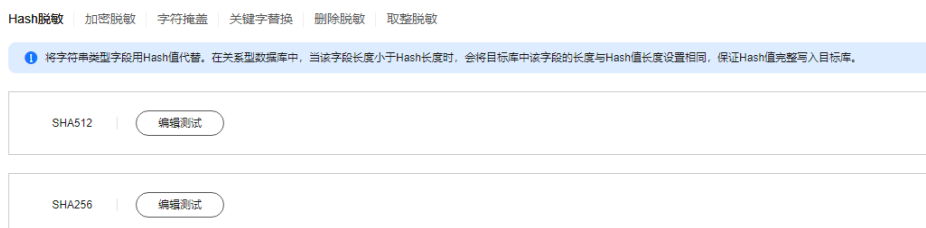
步骤1 [登录管理控制台](#)。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全与合规 > 数据安全中心”。

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

图 8-10 Hash 脱敏




步骤5 选择“删除脱敏”页签，进入“删除脱敏”的规则展示页面。

----结束

取整脱敏

步骤1 [登录管理控制台](#)。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全与合规 > 数据安全中心”。

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

图 8-11 Hash 脱敏



步骤5 选择“取整脱敏”，进入“取整脱敏”的页面。

系统设置了“日期取整”和“数值取整”两种算法。

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

步骤6 单击“编辑测试”，进入“编辑测试”界面，选择“取整脱敏”脱敏算法，配置“取整值”。

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

图 8-12 数值取整

编辑测试

The screenshot shows a web interface for configuring and testing a numerical rounding algorithm. At the top, under the heading "编辑测试", there is a configuration bar. On the left, it says "脱敏算法" (Desensitization Algorithm). To its right are two dropdown menus: the first is set to "取整脱敏" (Rounding Desensitization) and the second is set to "数值取整" (Numerical Rounding). Below this bar, there is a field labeled "取整值" (Rounding Value) with a red asterisk, containing the number "5".

Below the configuration section is a "测试" (Test) section. It has a label "原始数据" (Original Data) next to a text input field containing "14". To the right of this field is a "测试" (Test) button. Below the input field is a larger text area labeled "脱敏结果" (Desensitized Result) which displays the number "10".

步骤7 输入“原始数据”，单击“测试”，在“脱敏结果”文本框中展示已完成脱敏的数据。

步骤8 测试确认无误后，单击“保存”。

----结束

仿真脱敏

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

表 8-4 支持的仿真脱敏类型

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

8.1.3 数据静态脱敏

8.1.3.1 创建数据静态脱敏任务

DSC服务支持对数据库、大数据以及OBS类型数据进行脱敏，支持的数据类型请参见[约束限制](#)，本章节介绍如何创建各类型脱敏任务。

前提条件

- 已完成云资产委托授权，具体请参见[云资产委托授权/停止授权](#)进行操作。
- 已添加OBS桶或者授权数据库/大数据资产，具体请参见[资产中心](#)中添加和授权资产的操作。
- 已在“敏感数据识别”中完成了敏感数据识别，具体操作请参见[新建敏感数据识别任务](#)。
- MRS脱敏需要配置MRS_Hive的相关权限，具体操作请参见[修改Hive用户权限](#)。

约束限制

- 数据库脱敏：

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

- 大数据脱敏：
支持“Elasticsearch”、“MRS_HIVE”、“Hive”、“HBase”、“DLI”。
- OBS桶：
 - DSC不支持OBS的并行文件系统。
 - 支持.txt, .log, .xml, .ini, .sql, .inf, .java, .json等文件或者mime type以text开头的文件。


创建数据静态脱敏任务

DSC支持在控制台创建数据静态脱敏任务，根据选择的脱敏规则对数据源进行脱敏，查看和测试脱敏规则请参见[配置和查看脱敏规则](#)。



创建并运行数据库脱敏任务

步骤1 [登录管理控制台](#)。

步骤2 单击左上角的，选择区域或项目。

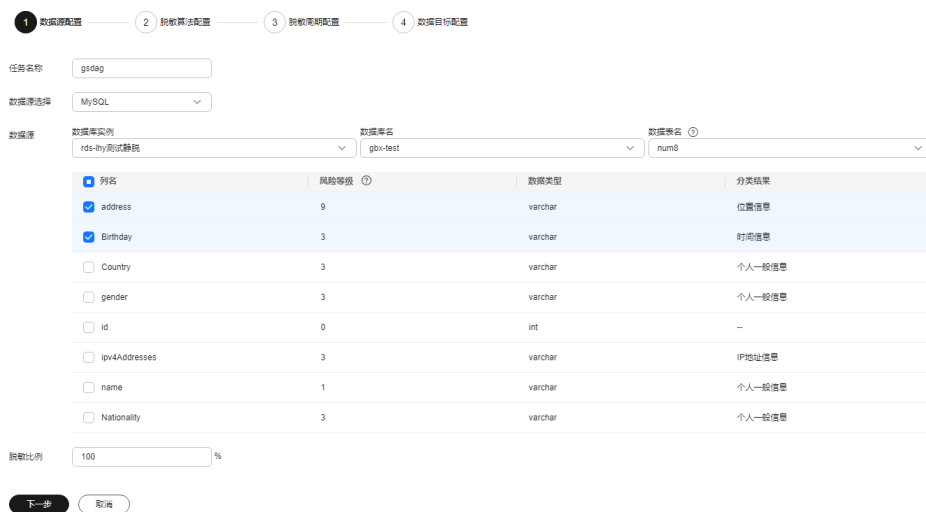
步骤3 在左侧导航树中，单击，选择“安全与合规 > 数据安全中心”。

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

步骤5 在“数据库”页签中，单击，将“数据库脱敏”设置为，开启数据库脱敏。

步骤6 单击“新建任务”，进入“数据源配置”页面，具体参数说明如[表8-5](#)所示。

图 8-13 数据源配置-数据库脱敏任务



该截图展示了“数据源配置-数据库脱敏任务”的界面。顶部有四个步骤指示器：1. 数据源配置 (当前选中), 2. 脱敏算法配置, 3. 脱敏策略配置, 4. 数据项目配置。

配置项包括：

- 任务名称: gsdag
- 数据源选择: MySQL
- 数据库实例: rds-hby测试脱敏
- 数据库名: gbx-test
- 数据表名: num8

列名	风险等级	数据类型	分类结果
<input checked="" type="checkbox"/> address	9	varchar	位置信息
<input checked="" type="checkbox"/> Birthday	3	varchar	时间信息
<input type="checkbox"/> Country	3	varchar	个人一般信息
<input type="checkbox"/> gender	3	varchar	个人一般信息
<input type="checkbox"/> id	0	int	--
<input type="checkbox"/> ipv4Addresses	3	varchar	IP地址信息
<input type="checkbox"/> name	1	varchar	个人一般信息
<input type="checkbox"/> Nationality	3	varchar	个人一般信息

脱敏比例: 100 %

底部按钮: 下一步, 取消

表 8-5 数据源配置参数说明

参数名称	参数说明
任务名称	您可以自定义脱敏任务的名称。 任务名称需要满足以下要求： <ul style="list-style-type: none"> • 1~255个字符。 • 字符可由中文、英文字母、数字、下划线或中划线组成。
数据源选择	选择数据来源。支持选择“SQLServer”、“MySQL”、“TDSQL”、“PostgreSQL”、“达梦”、“人大金仓”、“OpenGauss”、“Oracle”、“DWS”。
数据源 说明 如果没有可使用的数据库实例，单击“添加云数据库”，添加或者授权数据库，具体的操作可参见 添加自建数据库实例 和 授权数据库资产 。	数据库实例：选择需要脱敏的数据库实例。
	数据库名：选择需要脱敏的数据库名称。
	模式：当“数据源选择”选择“SQLServer”、“人大金仓”、“OpenGauss”、“PostgreSQL”和“DWS”时，显示该参数。
	数据表名：选择脱敏数据所在的数据表名称。
列信息	列信息展示“列名称”、“风险等级”、“数据类型”以及“分类结果”。
脱敏比例	输入数据库的脱敏比例，如数据库存在1000行的数据，此处输入80%时，则对数据库前800行的数据进行脱敏。

步骤7 单击“下一步”，进入“脱敏算法配置”页面。

图 8-14 脱敏算法配置



1. 勾选需要脱敏的数据列。
2. 根据不同的“数据类型”选择合适的脱敏算法。脱敏算法详细信息请参见[配置和查看脱敏规则](#)。

📖 说明

加密数据选择解密脱敏算法，会对加密的数据进行解密脱敏。

未加密数据选择解密脱敏算法，脱敏后还是原数据不变。

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

步骤8 单击“下一步”，进入“脱敏周期配置”页面，配置脱敏周期。

单击“增量脱敏”右边 ，打开增量脱敏开关。

增量键值：单击下拉框选择增量键值，如id。

📖 说明

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

选择并设置脱敏任务的执行周期：

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

📖 说明

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

步骤9 单击“下一步”，进入“数据目标配置”页面。

图 8-15 数据目标配置-数据库脱敏任务



数据库源列名	风险等级	数据目标列名
address	9	address
Birthday	3	Birthday
PhoneNumbers	6	PhoneNumbers

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

注意

- 如果需要填写已有的数据表，请勿选择业务数据表，以免影响业务。
- 目标数据表请勿选择原数据表，以免覆盖原始数据。

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

步骤10 单击“完成”，完成数据库脱敏任务的创建。

步骤11 进入“数据库”页签，单击“启用/禁用任务”开关，启动任务，在目标脱敏任务的“操作”列，单击“立即运行”。


运行后，系统开始按照设置的脱敏周期执行脱敏任务。

----结束



创建并运行 Elasticsearch 脱敏任务

步骤1 [登录管理控制台](#)。

步骤2 单击左上角的 ，选择区域或项目。

步骤3 在左侧导航树中，单击 ，选择“安全与合规 > 数据安全中心”。

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

步骤5 单击 ，将“Elasticsearch”设置为 ，开启Elasticsearch脱敏。

步骤6 单击“新建任务”，进入“数据源配置”页面，具体参数说明如[表8-6](#)所示。

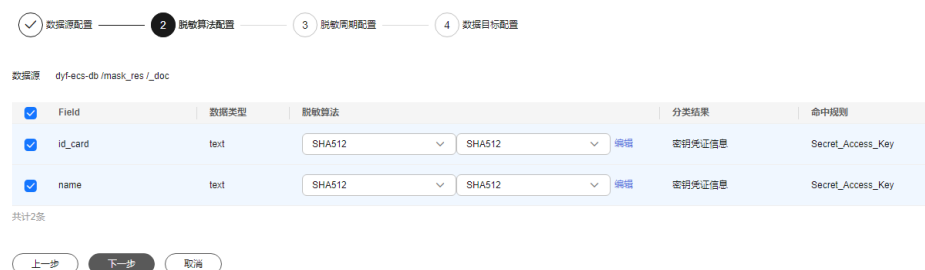
表 8-6 数据源配置参数说明

参数名称	参数说明
任务名称	您可以自定义脱敏任务的名称。 任务名称需要满足以下要求： <ul style="list-style-type: none"> • 1~255个字符。 • 字符可由中文、英文字母、数字、下划线或中划线组成。
数据源选择	选择数据来源。目前仅支持“Elasticsearch”。

参数名称	参数说明
数据源 说明 如果没有可使用的Elasticsearch实例，可单击“添加ES源”，添加Elasticsearch索引，具体的操作可参见 添加大数据资产 。	Elasticsearch实例：选择脱敏数据所在的Elasticsearch实例。
	索引(Index)：选择脱敏数据所在的索引。
	Type：选择脱敏数据所在的Type。
字段信息	字段信息展示“字段名”、“风险等级”、“数据类型”以及“分类结果”。

步骤7 单击“下一步”，进入“脱敏算法配置”页面。

图 8-16 脱敏算法配置-Elasticsearch 脱敏任务



1. 勾选需要脱敏的数据列。
2. 选择脱敏算法。脱敏算法更多详细信息请参见[配置和查看脱敏规则](#)。

步骤8 单击“下一步”，进入“脱敏周期配置”页面，配置脱敏周期。

选择并设置脱敏任务的执行周期：

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

📖 说明

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

步骤9 单击“下一步”，进入“数据目标配置”页面。

图 8-17 数据目标配置-Elasticsearch 脱敏任务



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

注意

如果需要填写已有的Type，请勿选择业务Type，以免影响业务。


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

步骤10 单击“完成”，完成脱敏任务的创建。

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

步骤12 运行后，系统开始按照设置的脱敏周期执行脱敏任务。

说明


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

----结束



创建并运行 MRS 脱敏任务

步骤1 [登录管理控制台](#)。

步骤2 单击左上角的 ，选择区域或项目。

步骤3 在左侧导航树中，单击 ，选择“安全与合规 > 数据安全中心”。

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

步骤5 单击 ，将“MRS脱敏”设置为 ，开启MRS脱敏。

步骤6 单击“新建任务”，进入“数据源配置”页面，具体参数说明如表8-7所示。

表 8-7 数据源配置参数说明

参数名称	参数说明
任务名称	您可以自定义脱敏任务的名称。 任务名称需要满足以下要求： <ul style="list-style-type: none"> • 1~255个字符。 • 字符可由中文、英文字母、数字、下划线或中划线组成。
数据源选择	选择数据来源。仅支持“MRS_HIVE”。
数据源 说明 如果没有可使用的Hive数据库实例，可单击“授权数据库”，添加大数据实例资产，具体的操作可参见 添加大数据资产 。	数据库实例：选择脱敏数据所在的数据库实例。
	数据库名：选择脱敏数据所在的数据库名称。
	数据表名：选择脱敏数据所在的数据表名称。
	勾选列名后将该列数据拷贝到目标数据库。
列信息	列信息展示“列名称”、“风险等级”、“数据类型”以及“分类结果”。

步骤7 单击“下一步”，进入“脱敏算法配置”页面。

图 8-18 脱敏算法配置-MRS 脱敏任务



1. 勾选需要脱敏的数据列。
2. 选择脱敏算法。脱敏算法更多详细信息请参见[配置和查看脱敏规则](#)。

步骤8 单击“下一步”，进入“脱敏周期配置”页面，配置脱敏周期。

选择并设置脱敏任务的执行周期：

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

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

- 每月：每月几日几时执行一次脱敏任务。

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

📖 说明

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

步骤9 单击“下一步”，进入“数据目标配置”页面。

图 8-19 数据目标配置-MRS 脱敏任务

1. 选择数据库实例、数据库名，并输入数据表名。

如果输入的数据表名已存在，系统将刷新目标数据库中该数据表中的数据。

如果输入的数据表名不存在，系统将自动在目标数据库中新建该名称的数据表。

⚠️ 注意

如果需要填写已有的数据表，请勿选择业务数据表，以免影响业务。

2. 设置数据目标列名。

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

步骤10 单击“完成”，完成脱敏任务的创建。

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


步骤12 运行后，系统开始按照设置的脱敏周期执行脱敏任务。

----结束



创建并运行 Hive 脱敏任务

步骤1 [登录管理控制台](#)。

步骤2 单击左上角的 ，选择区域或项目。

步骤3 在左侧导航树中，单击 ，选择“安全与合规 > 数据安全中心”。

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

步骤5 单击 ，将“Hive脱敏”设置为 ，开启Hive脱敏。

步骤6 单击“新建任务”，进入“数据源配置”页面，具体参数说明如表8-8所示。

表 8-8 数据源配置参数说明

参数名称	参数说明
任务名称	您可以自定义脱敏任务的名称。 任务名称需要满足以下要求： <ul style="list-style-type: none"> • 1~255个字符。 • 字符可由中文、英文字母、数字、下划线或中划线组成。
数据源选择	选择数据来源。仅支持“HIVE”。
数据源 说明	数据库实例：选择脱敏数据所在的数据库实例。 数据库名：选择脱敏数据所在的数据库名称。 数据表名：选择脱敏数据所在的数据表名称。 勾选列后将该列数据拷贝到目标数据库。
如果没有可使用的Hive数据库实例，可单击“授权数据库”，添加大数据资产，具体的操作可参见 添加大数据资产 。	
列信息	列信息展示“列名称”、“风险等级”、“数据类型”以及“分类结果”。

步骤7 单击“下一步”，进入“脱敏算法配置”页面。

图 8-20 脱敏算法配置-Hive 脱敏任务



1. 勾选需要脱敏的数据列。
2. 选择脱敏算法。脱敏算法更多详细信息请参见[配置和查看脱敏规则](#)。

步骤8 单击“下一步”，进入“脱敏周期配置”页面，配置脱敏周期。

选择并设置脱敏任务的执行周期：

- 手动：由用户自行启动的，且基于脱敏规则执行脱敏任务。

- 每小时：每几个小时执行一次脱敏任务。
示例：如果需要每2小时执行一次脱敏任务，则此处设置为：02:00
- 每天：每天几点几分执行一次脱敏任务。
示例：如果需要每天12:00执行一次脱敏任务，则此处设置为：12:00:00
- 每周：每周几的几点执行一次脱敏任务。
示例：如果需要每周一的12:00执行一次脱敏任务，则此处设置为：每周一12:00:00
- 每月：每月几日几时执行一次脱敏任务。
示例：如果需要每月12日的12:00执行一次脱敏任务，则此处设置为：每月12日12:00:00

📖 说明

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

步骤9 单击“下一步”，进入“数据目标配置”页面。

图 8-21 数据目标配置-Hive 脱敏任务

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

⚠️ 注意

如果需要填写已有的数据表，请勿选择业务数据表，以免影响业务。

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

步骤10 单击“完成”，完成脱敏任务的创建。

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


步骤12 运行后，系统开始按照设置的脱敏周期执行脱敏任务。

----结束



创建并运行 HBase 脱敏任务

步骤1 [登录管理控制台](#)。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全与合规 > 数据安全中心”。

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

步骤5 单击，将“HBase脱敏”设置为，开启HBase脱敏。

步骤6 单击“新建任务”，进入“数据源配置”页面，具体参数说明如[表8-9](#)所示。

表 8-9 数据源配置参数说明

参数名称	参数说明
任务名称	您可以自定义脱敏任务的名称。 任务名称需要满足以下要求： <ul style="list-style-type: none"> • 1~255个字符。 • 字符可由中文、英文字母、数字、下划线或中划线组成。
数据源选择	选择数据来源。仅支持“HBase”。
数据源	数据库实例：选择脱敏数据所在的数据库实例。
说明 如果没有可使用的数据库实例，可单击“授权数据库”，添加大数据资产，具体的操作可参见 添加大数据资产 。	命名空间：选择脱敏数据所在的命名空间。
	数据表名：选择脱敏数据所在的数据表名称。
	列族：选择脱敏数据所在的列。
	勾选列后将该列数据拷贝到目标数据库。
列信息	列信息展示“列名称”、“风险等级”、“数据类型”以及“分类结果”。

步骤7 单击“下一步”，进入“脱敏算法配置”页面。

图 8-22 脱敏算法配置-HBase 脱敏任务



1. 勾选需要脱敏的数据列。
2. 选择脱敏算法。脱敏算法更多详细信息请参见[配置和查看脱敏规则](#)。

步骤8 单击“下一步”，进入“脱敏周期配置”页面，配置脱敏周期。

选择并设置脱敏任务的执行周期：

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

📖 说明

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

步骤9 单击“下一步”，进入“数据目标配置”页面。

图 8-23 数据目标配置-HBase 脱敏任务

1. 选择数据库实例、命名空间、数据表名，并输入列族。
如果输入的列名已存在，系统将刷新目标数据表中的该列的数据。
如果输入的列名不存在，系统将自动在目标数据表中新建该名称的列。

⚠️ 注意

如果需要填写已有的数据表，请勿选择业务数据表，以免影响业务。

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

步骤10 单击“完成”，完成HBase任务的创建。

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


步骤12 运行后，系统开始按照设置的脱敏周期执行脱敏任务。

----结束



创建并运行 DLI 脱敏任务

步骤1 [登录管理控制台](#)。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全与合规 > 数据安全中心”。

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

步骤5 单击，将“DLI脱敏”设置为，开启DLI脱敏。

步骤6 单击“新建任务”，进入“数据源配置”页面，具体参数说明如[表8-10](#)所示。

表 8-10 数据源配置参数说明

参数名称	参数说明
任务名称	您可以自定义脱敏任务的名称。 任务名称需要满足以下要求： <ul style="list-style-type: none"> • 1~255个字符。 • 字符可由中文、英文字母、数字、下划线或中划线组成。
数据源选择	选择数据来源。仅支持“DLI”。
数据源	数据库实例：选择脱敏数据所在的数据库实例。
如果没有可使用的数据库实例，可单击“添加云数据库”，添加数据库资产，具体的操作可参见 添加大数据资产 。	数据库名：选择需要脱敏的数据库。
	数据表名：选择需要脱敏的数据表。
	说明 只有具备读写权限的资产才能使用脱敏功能。
	勾选需要脱敏的列数据，支持多选。
AK/SK	请输入访问密钥，请单击创建和查询访问密钥请参见 访问密钥 。创建访问密钥成功后，您可以在访问密钥列表中查看访问密钥ID（AK），在下载.csv文件中查看秘密访问密钥（SK）。
列信息	列信息展示“列名称”、“风险等级”、“数据类型”以及“分类结果”。

步骤7 单击“下一步”，进入“脱敏算法配置”页面。

图 8-24 脱敏算法配置-DLI 脱敏任务



1. 勾选需要脱敏的数据列。
2. 选择脱敏算法。脱敏算法更多详细信息请参见[配置和查看脱敏规则](#)。

步骤8 单击“下一步”，进入“脱敏周期配置”页面，配置脱敏周期。

选择并设置脱敏任务的执行周期：

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

说明

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

步骤9 单击“下一步”，进入“数据目标配置”页面。

图 8-25 数据目标配置-DLI 脱敏任务



1. 选择数据库实例、数据库名，并输入数据表名称。
如果输入的表名已存在，系统将刷新目标数据表中的数据。

如果输入的表名不存在，系统将自动在目标数据库中新建该名称的表。

注意

如果需要填写已有的数据表，请勿选择业务数据表，以免影响业务。

2. 设置数据目标列名。

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

步骤10 单击“完成”，完成DLI任务的创建。

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


步骤12 运行后，系统开始按照设置的脱敏周期执行脱敏任务。

----结束



创建并运行 OBS 脱敏任务

步骤1 [登录管理控制台](#)。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全与合规 > 数据安全中心”。

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

步骤5 单击，将“OBS脱敏”设置为，开启OBS脱敏。

步骤6 单击“新建任务”，进入“数据源配置”页面，具体参数说明如[表8-11](#)所示。

表 8-11 数据源配置参数说明

参数名称	参数说明
任务名称	您可以自定义脱敏任务的名称。 任务名称需要满足以下要求： <ul style="list-style-type: none"> 1~255个字符。 字符可由中文、英文字母、数字、下划线或中划线组成。
数据源选择	选择数据来源。仅支持“OBS”。
数据源	OBS桶名称：单击下拉框选择OBS桶资产名称。
	OBS文件路径：单击下拉框选择OBS桶文件路径。
	文件类型：目前仅支持文本类型。 说明 只有具备读写权限的资产才能使用脱敏功能。

步骤7 单击“下一步”，进入“脱敏算法配置”页面。

图 8-26 脱敏算法配置-OBS 脱敏任务



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

步骤8 单击“下一步”，进入“脱敏配置”页面。

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

步骤9 单击“下一步”，进入“数据目标配置”页面。

图 8-27 数据目标配置-OBS 脱敏任务



1. OBS桶名称：单击下拉框选择脱敏后的存储桶。

2. OBS文件路径：单击在弹框中选择OBS文件路径。

 **注意**

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

步骤10 单击“完成”，完成OBS脱敏任务的创建。

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

步骤12 运行后，系统开始按照设置执行脱敏任务。

----结束

8.1.3.2 查看数据静态脱敏运行状态


前提条件

已创建数据静态脱敏任务，参考[创建数据静态脱敏任务](#)章节。


查看数据静态脱敏任务的运行状态

步骤1 [登录管理控制台](#)。


步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全与合规 > 数据安全中心”。

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

步骤5 选择“脱敏任务”页签，并选择需要查看的脱敏任务类型，数据库、Elasticsearch或者MRS等，单击目标脱敏任务前面的，查看脱敏任务运行状态。

运行“状态”说明如下：

- 排队中：脱敏任务在队列中排队。
- 已完成：脱敏任务已完成运行，且运行成功。
- 运行中：脱敏任务正在执行中。
- 待运行：脱敏任务未运行。
- 已停止：用户已手动停止脱敏任务的运行。
- 运行失败：脱敏任务运行失败。鼠标移动至查看失败原因。

----结束


8.1.3.3 编辑和删除数据静态脱敏任务

编辑和删除数据静态脱敏任务

运行完成的脱敏任务可在控制台进行编辑和删除，运行中的任务可先终止脱敏再进行编辑和删除。

步骤1 [登录管理控制台](#)。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全与合规 > 数据安全中心”。

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

步骤5 选择“脱敏任务”页签，并选择脱敏任务类型，数据库、Elasticsearch或者MRS等，在对应的脱敏任务列表中，单击目标脱敏任务“操作”列的“编辑”，可重新配置脱敏任务信息，配置脱敏任务信息方法请参见[创建并运行数据库脱敏任务](#)。

步骤6 单击目标脱敏任务“操作”列的“删除”，删除脱敏任务。

注意

脱敏任务删除后不支持恢复，建议您谨慎操作。

---结束

8.2 数据水印

8.2.1 数据水印概述

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

表 8-12 数据库水印支持的数据库类型

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

表 8-13 文档水印支持的文件类型

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

表 8-14 图片水印支持的类型

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

使用场景

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

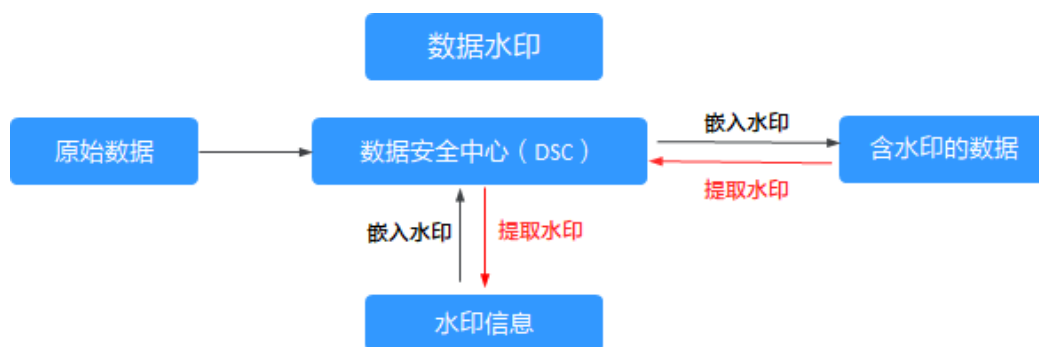
- **数据版权保护**：数字作品被下载或者复制使用，数据库业务（数据挖掘分析）需要提供数据给第三方，发生纠纷时可以通过数字水印明确版权所属。
- **使用过程可追踪溯源**：数据给内部员工或第三方使用时，打上使用者信息水印，可识别使用者身份，提醒使用者要注意安全规范。当发生数据泄露事件时，可追踪泄露源头，挖掘泄露原因。

优势特点

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

操作流程

图 8-28 数据水印操作流程



8.2.2 注入水印

8.2.2.1 数据库水印注入

前提条件

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


约束条件

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

新建任务

步骤1 [登录管理控制台](#)。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全与合规 > 数据安全中心”。

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

步骤5 单击“新建任务”，进入“基础信息配置”界面。

图 8-29 基础信息配置

1 基础信息配置 ———— 2 源目标端配置 ———— 3 调度信息配置

* 任务名称

* 水印标识

* 嵌入方案

描述

0/1,024

下一步 取消

表 8-15 基础信息配置参数说明

参数	说明
任务名称	请输入任务名称。 只能由中文、英文字母、数字、下划线或中划线组成，且不能超过255个长度。
水印标识	请输入需要注入的水印标识符。
嵌入方案	单击下来框选择嵌入水印的方案，有如下方式： <ul style="list-style-type: none"> 无损-伪列水印：伪造新的属性列，生成与该关系表的其他属性相关的伪列，不容易被攻击者察觉，然后将水印嵌入到伪造的新列中，降低对原数据的损坏。 无损-伪行水印：基于数据各项属性的数据类型、数据格式、取值范围的约束条件生成多个伪造的行，然后将水印嵌入到伪造的新行中，降低对原数据的损坏。 有损-列水印：在列数据直接添加水印，会对数据造成一定的修改或者损坏。 <p>说明 等级越高，水印信息编码位数越长，溯源时误码率越低，需注意高纠错等级需要更大的数据量来保证信息的嵌入完整性，默认为1。</p>

步骤6 单击“下一步”，进入“源目标端配置”界面，请按照参数列表8-16配置相关参数。

- 无损-伪列水印：无损添加水印，创建新的列。

图 8-30 伪列水印

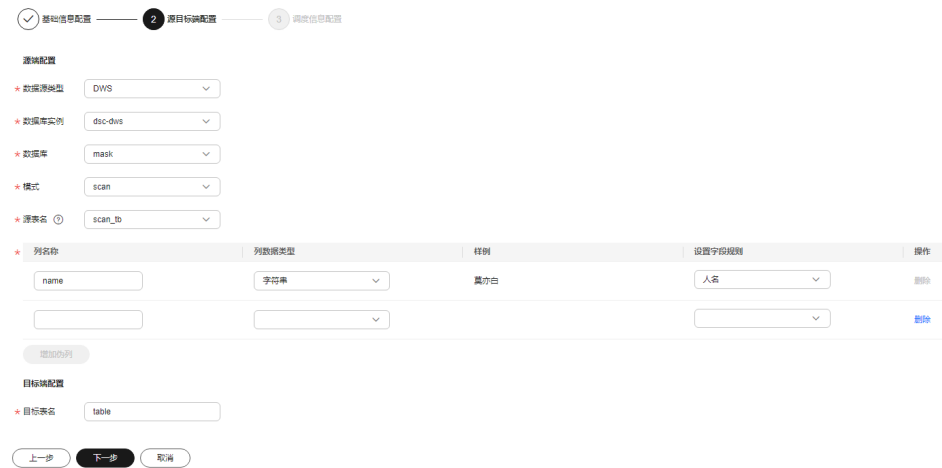


表 8-16 伪列水印源目标端配置参数

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

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

- 无损-伪行水印：无损添加水印，复制新的行数据注入水印。

图 8-31 伪行水印

基础信息配置 — 2 源目标端配置 — 3 调度信息配置

源端配置

* 数据源类型

* 数据库实例

* 数据库

* 模式

* 源表名

* 伪行跨行数

目标端配置

* 目标表名

表 8-17 伪行水印源目标端配置参数

参数	说明
数据源类型	单击下拉框选择“数据源类型”，支持的数据源类型有： - DWS - PostgreSQL - MySQL
数据库实例	单击下拉框选择对应的“数据库实例”。如果没有可用数据库实例，请参考 添加自建数据库实例 和 添加大数据资产 章节进行授权。
数据库	单击下拉框选择对应的“数据库”。
模式	当“数据库类型”为“DWS”和“PostgreSQL”时显示该参数。单击选择对应的“模式”。

参数	说明
源表名	单击选择对应的源数据表名。
伪行跨行数	请输入伪行在原始数据中插入的跨行数，输入值为大于1的有效整数。
目标表名	请输入嵌入水印后的数据存储表名称，只能由字母、数字、下划线或中划线组成，且不能超过255个字符长度。

- 有损-列水印：在列数据直接添加水印标识。

图 8-32 有损列水印

表 8-18 有损列水印源目标端配置参数

参数	说明
数据源类型	单击下拉框选择“数据源类型”，支持的数据源类型有： - DWS - MRS-HIVE
数据库实例	单击下拉框选择对应的“数据库实例”。如果没有可用数据库实例，请参考 添加自建数据库实例 和 添加大数据资产 章节进行授权。

参数	说明
数据库	单击下拉框选择对应的“数据库”。
模式	当“数据库类型”为“DWS”时显示该参数。单击选择对应的“模式”。
源表名	单击选择对应的“源表名”。
水印嵌入列	单击选择水印嵌入的列数据，可多选。 说明 - 源数据库字符集需使用UTF-8。 - 嵌入水印单一系列中的内容重复率不高于30%。
目标表名	请输入嵌入水印后的数据存储表名称，只能由字母、数字、下划线或中划线组成，且不能超过255个字符长度。

步骤7 单击“下一步”，进入“调度信息配置”界面。

图 8-33 调度信息配置



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


步骤8 单击“完成”，水印嵌入任务创建完成。

----结束

运行任务

步骤1 [登录管理控制台](#)。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全与合规 > 数据安全中心”。

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

步骤5 在目标任务操作列单击“更多 > 运行”，该任务开始运行。


----结束

开启任务

当水印任务为定时任务时显示该参数。

步骤1 [登录管理控制台](#)。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全与合规 > 数据安全中心”。

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

步骤5 在目标任务操作列单击“更多 > 开启任务”开启该任务。


----结束

关闭任务

当水印任务为定时任务时显示该参数。

步骤1 [登录管理控制台](#)。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全与合规 > 数据安全中心”。

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

步骤5 在目标任务操作列单击“更多 > 关闭任务”关闭该任务。

----结束

编辑和删除嵌入水印任务

运行中的嵌入水印任务不支持编辑或删除。

- 在目标任务“操作”列单击“编辑”，可对嵌入水印任务配置信息进行修改。
- 在目标任务“操作”列单击“删除”，可删除该嵌入水印任务。也可以选择多条任务，单击列表左上角的批量删除，删除多条任务。

说明

删除操作无法恢复，请谨慎操作。

8.2.2.2 文档水印注入

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

前提条件

- 已完成OBS资产委托授权，参考[云资产委托授权/停止授权](#)进行操作。
- 已开通且已使用过OBS服务，开通OBS服务请参见[开通并使用OBS](#)。
- 文档格式为pdf, pptx, docx, xlsx。


约束条件

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

创建 OBS 桶文件注入水印任务

步骤1 [登录管理控制台](#)。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全与合规 > 数据安全中心”。

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

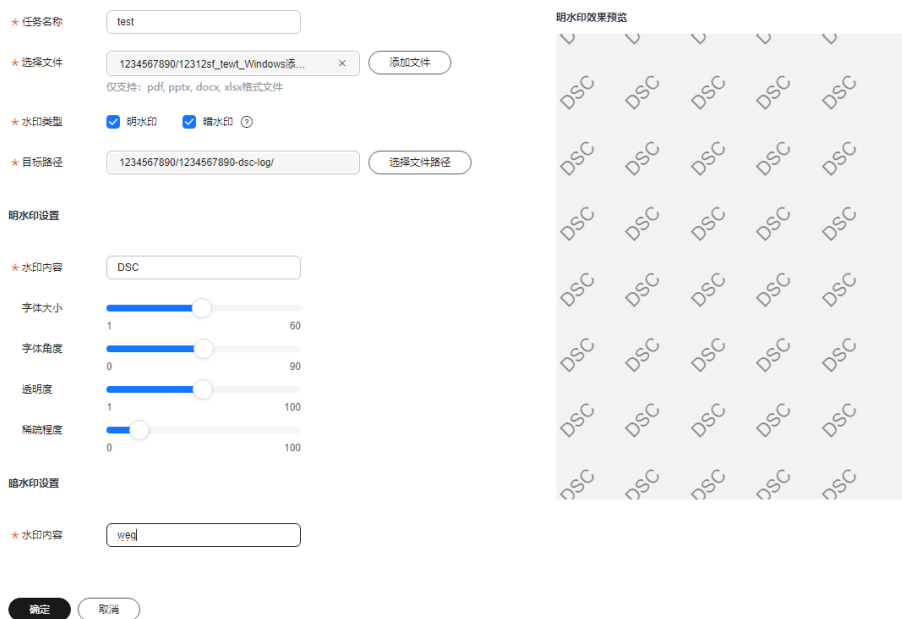
步骤5 单击任务列表左上角的“新建任务”。

步骤6 按照如[表8-19](#)所示配置参数信息。

表 8-19 参数配置


参数	说明
任务名称	请输入水印注入任务名称。只能由中文、英文字母、数字、下划线或中划线组成，且不能超过255个长度。
选择文件	单击“添加文件”，在右侧选择需要添加水印的桶名称，左侧选择文件，支持多选。
水印类型	支持“明水印”和“暗水印”，可多选。 <ul style="list-style-type: none"> • 明水印，水印内容可以展现在文件内容上。 • 暗水印，水印内容不可见，需要水印工具提取，提取暗水印的详细操作请参见文档水印提取章节。
目标路径	单击“选择文件路径”，选择存储注入水印后的文件。
明水印设置	当“水印类型”选择“明水印”时，输入水印内容，拖动滑块设置“字体大小”、“字体角度”、“透明度”以及水印的“稀疏程度”。
暗水印设置	当“水印类型”选择“暗水印”时，需要配置此参数。根据自己的需要，设置“水印内容”。

图 8-34 注入水印



步骤7 单击“确定”，右上角提示任务创建成功，注入水印任务创建完成。

步骤8 在水印任务列表中，单击任务名称在弹框中查看任务运行状态。

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

步骤9 如果您注入的是明水印，单击“下载”获取注入水印的文件。


如果您注入的是暗水印，水印内容不可见，需要用水印工具提取，详细操作请参见[文档水印提取](#)。

----结束

本地文件水印注入

步骤1 [登录管理控制台](#)。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全与合规 > 数据安全中心”。

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

步骤5 选择“本地文件”页签，进入“水印注入”页面。

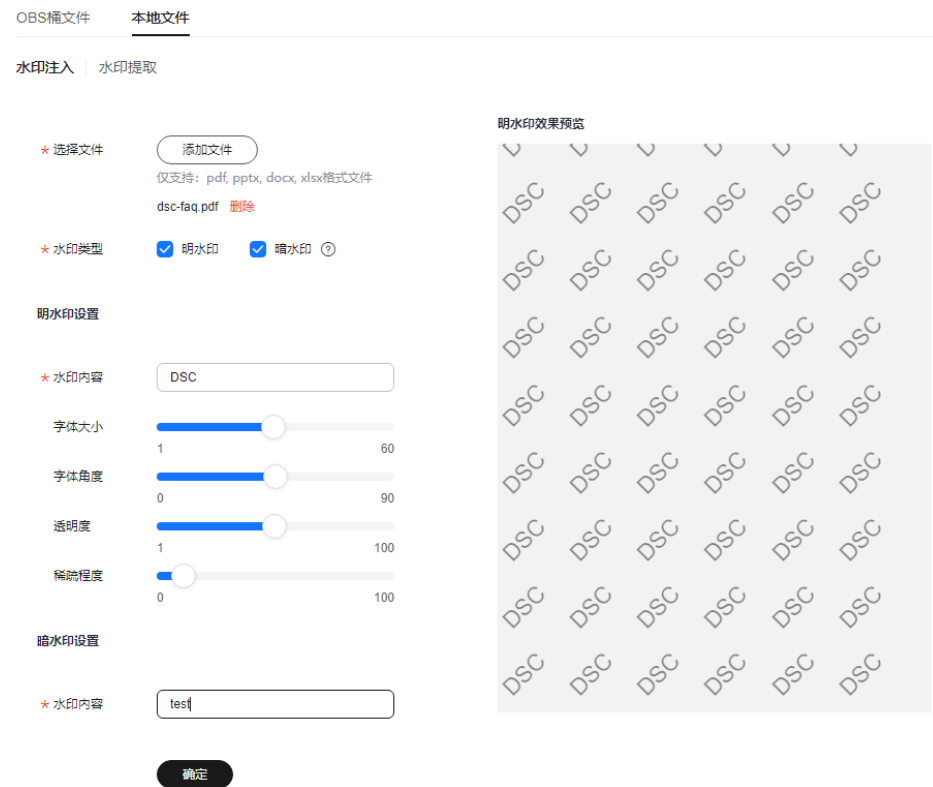
步骤6 单击“添加文件”，选择需要注入水印的文件。

步骤7 文件上传成功后，参照[表8-20](#)配置相关水印参数。

表 8-20 水印设置参数说明

参数名称	参数说明
水印类型	支持“明水印”和“暗水印”，可多选。 <ul style="list-style-type: none">明水印，水印内容可以展现在文件内容上。暗水印，水印内容不可见，需要水印工具提取，提取暗水印的详细操作请参见文档水印提取章节。
明水印设置	当“水印类型”选择“明水印”时，输入水印内容，拖动滑块设置“字体大小”、“字体角度”、“透明度”以及水印的“稀疏程度”。
暗水印设置	当“水印类型”选择“暗水印”时，需要配置此参数。根据自己的需要，设置“水印内容”。

图 8-35 本地文件水印注入



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

须知

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

----结束

8.2.2.3 图片水印注入

数据安全中心控制台针对jpg、jpeg等多种格式文件提供了注入水印的功能，您可以参考本章节对云上文件（文件存储在OBS桶）或者本地图片增加自定义水印内容。

前提条件

- 已完成OBS资产委托授权，参考[云资产委托授权/停止授权](#)进行操作。
- 已开通且已使用过OBS服务，开通OBS服务请参见[开通并使用OBS](#)。
- 支持的图片格式为：*.jpg, *.jpeg, *.jpe, *.png, *.bmp, *.dib, *.rle, *.tiff, *.tif, *.ppm, *.webp, *.tga, *.tpic, *.gif。


约束条件

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

OBS 桶文件注入水印

步骤1 [登录管理控制台](#)。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全与合规 > 数据安全中心”。

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

步骤5 在“OBS桶文件”页签，对“文件设置”模块进行路径设置。

图 8-36 文件设置

OBS桶文件 本地文件

水印注入 | 水印提取

文件设置

原始图片路径

dsc-ocrtest/bjwl20221107.jpeg × 添加

图片的对象后缀为jpg、jpeg、jpe、png、bmp、dib、rle、tiff、tif、ppm、webp、tga、tpic或者gif，大小不超过20M

存储目标路径

dsc-zzr/security-info/ × 添加

存储目标文件名

12.jpeg

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

步骤6 “水印类型”分为“明水印”和“暗水印”两种类型。

- 明水印：水印内容可以展现在图片内容上，相关参数配置如表8-21所示。

表 8-21 明水印设置

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

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

图 8-37 明水印设置

明水印设置

水印内容
文字水印

文字内容
文字水印的长度范围为1-32个字符。当前仅支持数字及英文大小写。

水印位置

水印大小
50

水印透明度
50

水平边距
1

垂直边距
1

字体颜色

- 暗水印，水印内容不可见，需要水印工具提取，提取暗水印的详细操作请参见[图片水印提取](#)章节。

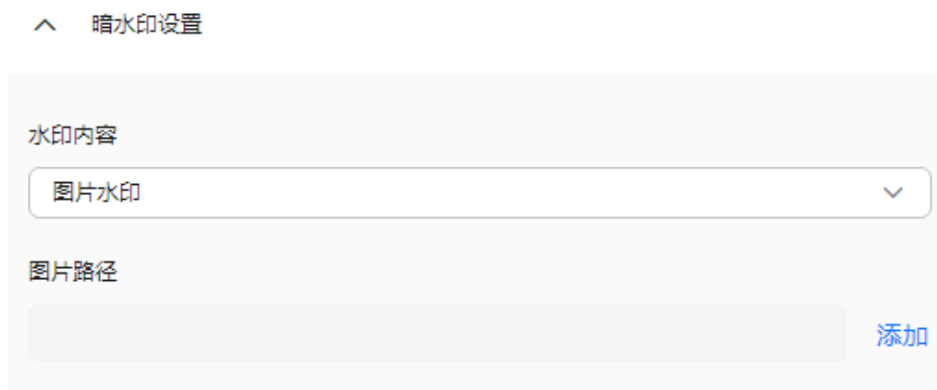
 说明

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

表 8-22 暗水印设置

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

图 8-38 暗水印设置



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

须知

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

步骤8 在页面左下角单击“预览”，在右侧“明水印图片预览”区域预览水印效果。暗水印无法预览。


步骤9 单击“确定”，完成水印注入。

----结束

本地文件水印注入

步骤1 [登录管理控制台](#)。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全与合规 > 数据安全中心”。

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

步骤5 选择“本地文件”页签，进入“水印注入”页面。

步骤6 单击“添加文件”，添加需要添加水印的本地图片文件。

步骤7 “水印类型”分为“明水印”和“暗水印”两种类型。

- 明水印：水印内容可以展现在图片内容上。
- 暗水印，水印内容不可见，需要水印工具提取，提取暗水印的详细操作请参见[图片水印提取](#)章节。

步骤8 根据如[表8-23](#)所示参数进行水印相关参数设置。

表 8-23 水印设置

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

水印类型	参数	说明
	垂直边距	待插入水印相对图片的垂直边距，输入值必须在0-100之间。
	字体颜色	“水印内容”选择“文字水印”时显示该参数，单击颜色条选择需要插入的文字水印的字体颜色。
暗水印	水印内容	单击下拉框选择“水印内容”： <ul style="list-style-type: none"> • “图片水印” • “文字水印”。
	水印图片	“水印内容”选择“图片水印”时显示该参数，单击“添加文件”选择本地图片作为水印。
	文字内容	“水印内容”选择“文字水印”时显示该参数，单击输入水印文字内容。

图 8-39 水印设置

The image shows two panels for watermark settings. The top panel is titled '明水印设置' (Visible Watermark Settings). It includes a dropdown menu for '水印内容' (Watermark Content) set to '图片水印' (Image Watermark), a '添加文件' (Add File) button, a '水印位置' (Watermark Position) grid with directional arrows, and four sliders: '图片尺寸(%)' (Image Size) at 50, '水印透明度' (Watermark Transparency) at 50, '水平边距' (Horizontal Margin) at 0, and '垂直边距' (Vertical Margin) at 0. The bottom panel is titled '暗水印设置' (Invisible Watermark Settings) and shows the same '水印内容' dropdown and '添加文件' button, but lacks the position grid and sliders.

步骤9 参数配置完后，单击“确定”，注入水印的文件会自动下载到您指定的本地路径下。

须知

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

----结束

8.2.3 提取水印

8.2.3.1 数据库水印提取

前提条件

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


约束条件

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

新建任务

步骤1 [登录管理控制台](#)。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全与合规 > 数据安全中心”。

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

步骤5 单击“水印提取”页签，进入“水印提取”界面。

步骤6 单击“新建任务”，进入新建任务弹框，请根据[表8-24](#)配置相关参数。

图 8-40 新建提取任务

新建任务

* 任务名称

描述

* 源文件

* 提取方式

* 分隔符

表 8-24 新建水印提取任务

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


步骤7 单击“确定”，完成水印提取任务创建。

----结束

查看结果

步骤1 [登录管理控制台](#)。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全与合规 > 数据安全中心”。

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

步骤5 单击“水印提取”页签，进入“水印提取”界面。

步骤6 在目标任务“操作”列单击“查看结果”。


----结束

删除水印提取任务

执行中的提取水印任务不支持删除。

步骤1 [登录管理控制台](#)。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全与合规 > 数据安全中心”。

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

步骤5 单击“水印提取”页签，进入“水印提取”界面。

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

说明

删除操作无法恢复，请谨慎操作。

----结束

8.2.3.2 文档水印提取

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

前提条件




- 已完成OBS资产委托授权，参考[云资产委托授权/停止授权](#)进行操作。
- 已开通且已使用过OBS服务，开通OBS服务请参见[开通并使用OBS](#)。
- 文件格式为PDF、PPT、Word、Excel。

约束条件




- 本章节的方法仅针对提取PDF、PPT、Word、Excel格式文件的单个文件的暗水印。
- PDF文件和Word文件最大50M。
- Excel文件最大70M。
- PPT文件最大20M。

创建 OBS 桶文件水印提取任务

步骤1 [登录管理控制台](#)。

- 步骤2** 单击左上角的，选择区域或项目。
- 步骤3** 在左侧导航树中，单击，选择“安全与合规 > 数据安全中心”。
- 步骤4** 在左侧导航树中选择“数据资产保护 > 文档水印”，进入“OBS桶文件”页签。
- 步骤5** 选择“水印提取”页签，进入“水印提取”页面。
- 步骤6** 单击左上角“新建任务”，进入“新建任务”页面。
- 步骤7** 单击添加文件选择需要进行提取水印的文件，OBS桶文件支持多选。
- 步骤8** 单击“确定”，提取水印任务创建完成。
- 步骤9** 单击目标任务名称，在弹框中查看水印提取任务状态以及OBS桶文件的暗水印内容。
- 运行中：显示提取水印任务进度。
 - 已完成：暗水印列显示水印内容，没有暗水印则显示--。
 - 运行失败：提取水印任务执行失败，鼠标移动至查看失败原因。
- 结束

本地文件水印提取

- 步骤1** [登录管理控制台](#)。
- 步骤2** 单击左上角的，选择区域或项目。
- 步骤3** 在左侧导航树中，单击，选择“安全与合规 > 数据安全中心”。
- 步骤4** 在左侧导航树中选择“数据资产保护 > 文档水印”，进入“OBS桶文件”页签。
- 步骤5** 选择“本地文件 > 水印提取”，进入水印提取页面。
- 步骤6** 单击“本地文件”，将本地需要提取暗水印的文件上传到DSC平台。
-  **说明**
- 当前DSC服务仅支持对PDF、PPT、Word、Excel格式文件提取水印。
- 步骤7** 文件上传后，单击“确定”，暗水印内容将展示到弹框中。
- 结束

8.2.3.3 图片水印提取

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

前提条件

- 已完成OBS资产委托授权，参考[云资产委托授权/停止授权](#)进行操作。
- 已开通且已使用过OBS服务，开通OBS服务请参见[开通并使用OBS](#)。
- 支持的图片格式为：*.jpg, *.jpeg, *.jpe, *.png, *.bmp, *.dib, *.rle, *.tiff, *.tif, *.ppm, *.webp, *.tga, *.tpic, *.gif。

- 原始图片像素要大于128*128。


约束条件

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

OBS 桶文件水印提取

步骤1 [登录管理控制台](#)。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全与合规 > 数据安全中心”。

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

步骤5 选择“水印提取”页签，进入“水印提取”页面。

步骤6 选择提取内容：

- “提取内容”为“文字”：单击“添加”选择待提取水印的图片。

图 8-41 提取文字内容



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

图 8-42 提取图片内容

The screenshot shows the 'Watermark Extraction' interface for 'Local Files'. It includes the following elements:

- Watermark Injection | Watermark Extraction**
- Extract Content:** Radio buttons for 'Text' and 'Image'. The 'Image' option is selected and highlighted with a red box and a '1' marker.
- Select File:** A text input field containing '1234567890/11.jpg' and a 'Add' button. The 'Add' button is highlighted with a red box and a '2' marker.
- Storage Path:** A text input field containing '1234567890/1234567890-dsc-log/' and a 'Add' button. The 'Add' button is highlighted with a red box and a '3' marker.
- Storage Filename:** A text input field containing '1.jpg' and a '4' marker.
- Confirm:** A black button labeled '确定'.


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

----结束

本地文件水印提取

步骤1 [登录管理控制台](#)。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全与合规 > 数据安全中心”。

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

步骤5 选择“本地文件 > 水印提取”，进入“水印提取”页面。

步骤6 选择“提取内容”：

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

步骤7 文件上传后，单击“确定”，暗水印内容将展示到弹框中。

----结束

8.3 数据库安全审计

数据库安全审计基于大数据分析技术，提供数据库审计，SQL注入攻击检测，风险操作识别等功能，保障云上数据库的安全。功能特性描述如表8-25所示。

详细功能介绍及使用请参见[DBSS功能特性](#)和[DBSS用户指南](#)。

表 8-25 功能特性介绍

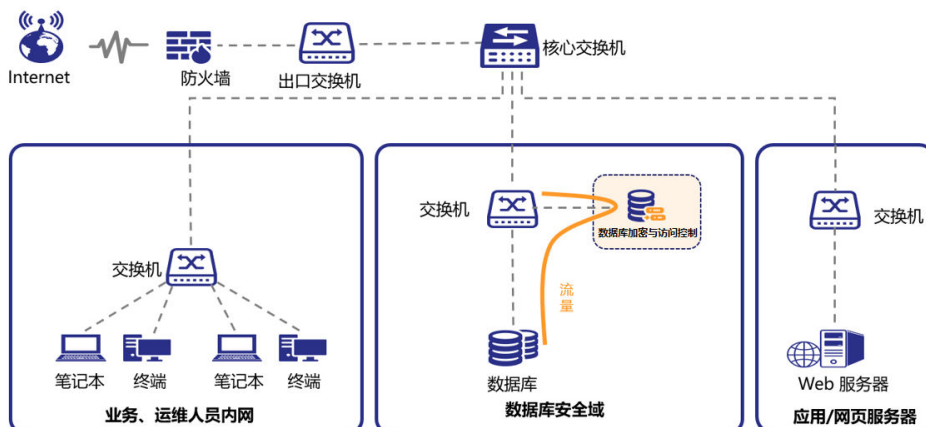
功能	描述
用户行为发现审计	<ul style="list-style-type: none"> 关联应用层和数据库层的访问操作。 提供内置或自定义隐私数据保护规则，防止审计日志中的隐私数据（例如，账号密码）在控制台上以明文显示。
多维度线索分析	<ul style="list-style-type: none"> 行为线索 支持审计时长、语句总量、风险总量、今日语句、今日风险和今日会话量等多维度的快速分析。 会话线索 支持根据时间、数据库用户、客户端等多角度进行分析。 语句线索 提供时间、风险等级、数据用户、客户端IP、数据库IP、操作类型、规则等多种语句搜索条件。
风险操作、SQL注入实时告警	<ul style="list-style-type: none"> 风险操作 支持通过操作类型、操作对象、风险等级等多种元素细粒度定义要求监控的风险操作行为。 SQL注入 数据库安全审计提供SQL注入库，可以基于SQL命令特征或风险等级，发现数据库异常行为立即告警。 系统资源 当系统资源（CPU、内存和磁盘）占用率达到设置的告警阈值时立即告警。
针对各种异常行为提供精细化报表	<ul style="list-style-type: none"> 会话行为 提供客户端和数据库用户会话分析报表。 风险操作 提供风险分布情况分析报表。 合规报表 提供满足数据安全标准（例如Sarbanes-Oxley）的合规报告。

8.4 数据库安全加密

数据库加密与访问控制是一款基于网关代理加密技术，实现敏感数据加密存储的数据库安全防护产品。

系统作为代理加密网关，部署在数据库和客户端应用程序之间，任何访问都需要经过该网关，从而实现数据加密和访问控制功能。系统组网场景如下[图8-43](#)所示。

图 8-43 组网方式



数据加密

系统支持对数据进行加密和完整性校验，满足等保、分保等评测要求，同时也满足商用密码系统应用与安全性评估的存储数据完整性和机密性保障的评测要求。

- 加密算法：支持AES算法和SM4国密算法。
- 完整性校验算法：支持AES-GCM算法和SM3-HMAC算法。

访问控制

系统具有独立于数据库的访问授权机制，拥有合法访问权限可以访问加密数据，非授权用户无法访问加密数据，从而有效防止管理员越权访问及黑客拖库。

系统支持系统管理员，安全管理员，审计管理员的三权分立管理，增强数据库使用的安全合规性。

使用场景

数据库加密与访问控制可以满足合规要求，同时可以满足数据库敏感数据防护需求。

满足国家评测的合规要求

应用系统本身会根据用户的权限对数据进行处理，对于遗留系统（旧系统无法再做升级改造）以及开发时未考虑《网络安全法》中要求的个人隐私保护问题，如果重新更改代码过于复杂，需要依赖于外部技术实现数据的隐私保护。

通过数据库加密与访问控制能够实现数据库的加密，满足各项法律法规。

满足数据库敏感数据防护需求

数据库加密与访问控制可以有效解决因数据库管理员DBA等高权限账号密码泄漏所导致的数据泄漏问题，同时也可防止因外部APT攻击或内部管理失当导致的数据库文件被下载、复制等数据泄漏风险，满足数据库的敏感数据防护需求。

功能介绍

本节介绍数据库加密与访问控制的主要功能及相关章节。

表 8-26 功能介绍

功能名称	功能描述
资产管理	支持数据库资产的增删改查以及数据源连通性测试，并支持数据库读写分离配置、加密模式配置、返回值配置、账号权限检测。
敏感数据发现	支持敏感数据扫描、敏感数据类型管理、敏感数据行业模板管理。
业务测试	支持业务仿真测试，模拟是否可以正常加解密；支持在加密前接入网络进行业务SQL流量分析，定位出加密后可能执行异常的SQL，并生产分析报表。
数据加密	在数据加密模块对加密与解密队列管理，支持对客户端和数据库用户授权限制用户访问，查看并下载加密日志、回滚表结构、管理加密表、下载bypass插件。
动态脱敏	支持对敏感数据配置脱敏算法，对明文数据进行动态脱敏展示。
密钥管理	支持三级密钥算法、密钥来源配置、密钥(DSK)周期轮转更新，支持配置KMS对接，密钥记录查看与密钥检索。
平台管理	在平台管理模块对系统进行基础网卡与路由配置、系统升级、配置数据的备份与恢复、查看应用访问记录、安全口令配置等管理操作。
系统管理	<ul style="list-style-type: none"> 系统管理模块支持对平台使用用户进行维护，包括账号的管理、组织架构管理、角色的管理、账号的审核等，同时支持对系统各类消息进行查看与管理。 展示设备状态，管理设备，对系统内核、CPU、硬盘等使用情况进行诊断、进行系统升级、系统安全配置等。
日志管理	支持查看与检索系统所有操作行为的日志信息。

8.5 云堡垒机

云堡垒机（Cloud Bastion Host, CBH）是华为云的一款4A统一安全管控平台，为企业提供集中的账号（Account）、授权（Authorization）、认证（Authentication）和审计（Audit）管理服务。

云堡垒机提供云计算安全管控的系统 and 组件，包含部门、用户、资源、策略、运维、审计等功能模块，集单点登录、统一资产管理、多终端访问协议、文件传输、会话协同等功能于一体。通过统一运维登录入口，基于协议正向代理技术和远程访问隔离技术，实现对服务器、云主机、数据库、应用系统等云上资源的集中管理和运维审计。

功能特性请参见如下内容，详细功能介绍及使用请参见[CBH功能特性](#)和[CBH用户指南](#)。

身份认证

采用多因子认证和远程认证技术，加强用户身份认证管理。

- 引用多因子认证技术，包括手机短信、手机令牌、USBKey、动态令牌等方式，安全认证登录用户身份，降低用户账号密码风险。
- 对接第三方认证服务或平台，包括AD域、RADIUS、LDAP、Azure AD远程认证，支持远程认证用户身份，防止身份泄露。并支持一键同步AD域服务器用户，复用原有用户部署结构。

账户管理

集中管理系统用户和资源账号信息，对账号全生命周期建立可视、可控、可管运维体系。

- 用户账号管理：系统用户账号全生命周期管理，用户使用唯一账号登录系统，解决共享账号、临时账号、滥用权限等问题。
- 资源账户管理：集中资源账户管理，资源账户全生命周期管理，实现单点登录资源，管理或运维无缝切换。

权限控制

集中管控用户访问系统和资源的权限，对系统和资源的访问权限进行细粒度设置，保障了系统管理安全和资源运维安全。

- 系统访问权限：从单个用户账号属性出发，控制用户登录和访问系统权限。
- 资源访问权限：按照用户、用户组与资源账户、账户组之间的关联关系，建立用户对资源的控制权限。

操作审计

基于用户身份系统唯一标识，从用户登录系统开始，全程记录用户在系统的操作行为，监控和审计用户对目标资源的所有操作，实现对安全事件的实时发现与预警。

- 系统行为审计：系统操作行为全纪录，针对操作失误、恶意操作、越权操作等行为告警通知。
- 资源运维审计：全程记录用户的运维操作，支持多种运维审计技术和审计形式，可随时审计用户操作行为，识别运维风险，为安全事件追溯和分析提供依据。

高效运维

通过多种架构运维、多种运维资源、多种运维工具、多种运维形式的接入，全面提升运维效率。

- Web浏览器运维：HTML5远程登录资源，无需安装客户端，一键登录运维资源，实现操作实时监控、文件上传下载等运维管理。
- 第三方客户端运维：在不改变用户使用原来客户端习惯的前提下，支持一键接入多种运维工具，提升运维效率。
- 自动化运维：线上多步骤复杂操作自动化执行，告别枯燥的重复工作，提高工作效率。

工单申请

系统运维用户在运维过程中，遇到需运维资源而无权限情况，可提交系统工单申请资源控制权限，寻求管理人员授权审批。

- 系统运维人员
 - 通过手动或自动触发工单系统，提交访问授权工单、命令授权工单、数据库授权工单申请权限。
 - 支持提交工单、查询工单、撤销工单、删除工单等功能。
- 系统管理人员
 - 通过自定义审批流程，支持多级审批。
 - 支持批准单个工单、批量批准工单、驳回工单、撤销工单、查询工单、删除工单等功能。

8.6（可选）配置 DWS 和 MRS Hive


使用数据库水印前，您先完成如下操作前提：

1. 修改DWS集群参数。
为能正常对DWS数据进行敏感数据识别和隐私保护管理，需要[提交工单](#)对DWS集群的`javaudf_disable_feature`参数进行修改，否则将导致操作失败。如果您不涉及DWS数据，则可以不用修改。
2. [修改Hive用户权限](#)
为能正常对MRS_Hive数据进行数据水印相关操作，必须通过Ranger管理员为Hive用户进行相关的权限设置。

修改 Hive 用户权限

步骤1 [登录管理控制台](#)。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“大数据 > MapReduce服务”，进入MapReduce服务“现有集群”界面。

步骤4 在集群列表中单击指定的集群名称，进入集群信息页面。

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

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

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

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

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

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

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

步骤11 根据权限要求配置相关参数。关键参数如表8-27，其他参数无需填写，保持默认即可。

表 8-27 Hive 权限参数

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

步骤12 单击“Add”，在策略列表即可查看策略的基本信息。

----结束

9 API 数据安全防护

9.1 登录实例 Web 控制台

系统管理员登录Web控制台后，可以管理和维护API数据安全防护。

前提条件

- 您已经从技术支持人员处获取登录用户名和密码。
- 出厂默认用户名如下，具体实际用户名密码请从技术支持工程师处获取。

表 9-1 系统默认账号信息

出厂默认账号		说明
系统管理员	sysadmin	主要负责系统的日常运行维护。 默认密码为 购买API数据安全防护实例并绑定弹性公网IP 章节设置的密码，首次登录进行重置密码。
安全管理员	secadmin	主要负责系统的日常安全保密管理工作，包括系统用户权限的授予与撤销，平台登录、账号密码和网络访问的安全配置等。 默认密码和 购买API数据安全防护实例并绑定弹性公网IP 章节设置的sysadmin用户密码相同，首次登录进行重置密码。
审计管理员	audadmin	主要负责对系统管理员和安全管理员的操作行为进行审计跟踪、分析和监督检查。 默认密码和 购买API数据安全防护实例并绑定弹性公网IP 章节设置的sysadmin用户密码相同，首次登录进行重置密码。

操作步骤

步骤1 登录实例。

- 方式一：登录服务管理控制台，进入数据库运维页面，在目标实例“操作”列单击“远程登录”或“本地登录”。
- 方式二：通过方式一进入的API数据安全防护页面获取“弹性IP”，在浏览器地址栏中输入访问地址，按回车键，进入登录界面。访问地址：`https://服务器弹性IP地址:端口`，例如`https://172.xx.xx.44:8441`。

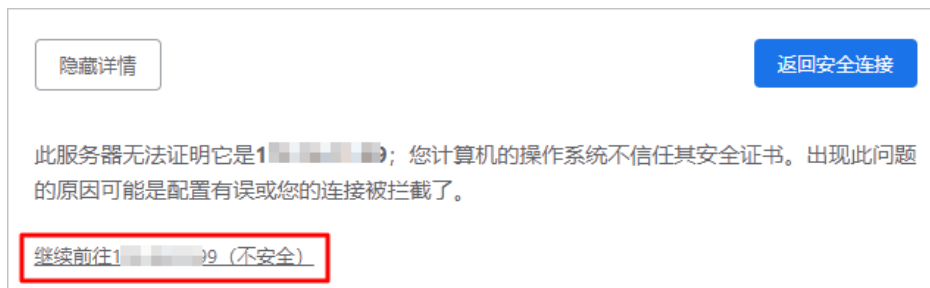
步骤2 （可选）在安全告警页面，单击“高级”。

图 9-1 安全告警



步骤3 （可选）在详情说明区域单击“继续前往xx.xx.xx.xx（不安全）”。

图 9-2 进入登录页面



步骤4 在登录页面，输入用户名和密码，单击“登录”。

步骤5 登录成功后，您可以进入Web控制台，查看和配置API数据安全防护。

步骤6 首次登录后，您需要修改默认密码。在后续使用过程中，建议您定期修改密码，确保登录安全，请参见[修改登录密码](#)。

----结束

修改登录密码

- 步骤1** 登录Web控制台，单击右上角用户名。
- 步骤2** 在下拉框中单击“修改密码”。
- 步骤3** 在弹出的对话框中，输入“原密码”、“新密码”和“确认密码”，单击“确定”，完成密码修改。

表 9-2 参数说明

参数	说明
原密码	输入原来的登录密码。
新密码	输入修改后的新密码。 说明 为了登录安全，建议您将密码设置成复杂密码，例如包含以下多种字符组合： <ul style="list-style-type: none"> • 大写字母（从A到Z） • 小写字母（从a到z） • 数字（0~9） • 特殊符号（例如：!@#\$）
确认密码	重新输入修改后的新密码。

----结束



9.2 实例管理

9.2.1 查看实例详情

一个API数据安全防护实例对应一个独立运行的系统。

用户可以在获取有操作权限的账号和密码后，对实例进行管理操作。

操作步骤

- 步骤1** [登录管理控制台](#)。
- 步骤2** 单击左上角的，选择区域或项目。
- 步骤3** 在左侧导航树中，单击，选择“安全与合规 > 数据安全中心”。
- 步骤4** 选择“数据资产保护 > API数据安全防护”，进入“API数据安全防护”界面。
- 步骤5** 单击实例名称，进入实例详情界面，包含监控分析和实例详情两块内容，详情参见如下内容。

----结束

监控分析

- 负载
包含“CPU使用率”和“内存使用率”。
- 资源使用
包含“系统盘”和“数据盘”百分比。

图 9-3 监测分析



实例详情

实例详情模块展示“实例名称”、“实例ID”、“实例类型”、“节点ID”以及实例“创建时间”等。

- 单击实例名称后的编辑按钮可修改实例名称。
- 单击实例ID或者服务器ID后的复制按钮拷贝相关信息。

图 9-4 实例详情

基础信息		网络信息	
实例名称	测试升级-节点	创建时间	2024/11/23 14:52:52 GMT-08:00
实例ID	8a2c222493...4e019357cb79300008	实例网络	CPU 8核 内存 16G 硬盘 500G
实例类型	主备	弹性公网IP	--
节点ID	主机: 8a2c2224...55ecde019357cb82d90009 备机: 8a2c2224...ecde019357cb82d7000a	私有IP	虚拟私有云 vpc-ny2 子网 subnet-ny1
		实例版本	1.0
		服务器ID	主机: 760adf4b-dc...33-91be-2b-495a350d58 备机: 9f0d1900-3...400-ab86-075b57c49a98
		安全组	default

9.2.2 开启


使用场景

- 当实例的“运行状态”为“关闭”时，如果需要登录使用API数据安全防护实例，则需执行开启实例操作。
- 当实例的“运行状态”为“异常”时，如果需要登录使用API数据安全防护实例，可尝试执行开启实例操作。

操作步骤

步骤1 [登录管理控制台](#)。

步骤2 单击左上角的，选择区域或项目。



- 步骤3** 在左侧导航树中，单击 ，选择“安全与合规 > 数据安全中心”。
- 步骤4** 选择“数据资产保护 > API数据安全防护”，进入“API数据安全防护”界面。
- 步骤5** 在需要开启的实例所在行，单击“操作”列的“更多 > 开启”。

----结束

9.2.3 关闭

当实例的“运行状态”为“运行中”时，可以关闭实例。关闭实例后，将不能登录API数据安全防护实例。

操作步骤

- 步骤1** [登录管理控制台](#)。
- 步骤2** 单击左上角的 ，选择区域或项目。
- 步骤3** 在左侧导航树中，单击 ，选择“安全与合规 > 数据安全中心”。
- 步骤4** 选择“数据资产保护 > API数据安全防护”，进入“API数据安全防护”界面。
- 步骤5** 在需要关闭的实例所在行，单击“操作”列的“更多 > 关闭”。
- 步骤6** 在弹出的关闭实例对话框中，单击“确定”。实例成功关闭后，实例的“运行状态”变为“关闭”。

说明

在关闭实例对话框，可选择“强制关机”，强制关闭实例可能会造成数据丢失，请确保数据文件已全部保存。



----结束

9.2.4 重启实例

出于维护目的，当系统的运行异常，用户可以尝试重启实例即虚拟机，恢复到可用状态。

- 当实例的“运行状态”为“运行中”时，可执行重启操作。
- 重启API数据安全防护实例将导致系统业务中断约5分钟，在此期间实例“运行状态”将显示为“重启中”。
- 重启过程中，API数据安全防护实例将不可用。

操作步骤

- 步骤1** [登录管理控制台](#)。
- 步骤2** 单击左上角的 ，选择区域或项目。
- 步骤3** 在左侧导航树中，单击 ，选择“安全与合规 > 数据安全中心”。
- 步骤4** 选择“数据资产保护 > API数据安全防护”，进入“API数据安全防护”界面。

步骤5 在需要重启的实例所在行，单击“操作”列的“更多 > 重启实例”。

步骤6 在弹出的是否要重启实例的对话框中，单击“确定”。

步骤7 重启过程一般需要5-10分钟左右，且实例状态会变成“重启中”。

实例状态变为“运行中”，即重启完成，可以正常使用系统。

说明

在重启实例对话框，可选择“强制重启”，强制重启实例可能会造成数据丢失，请确保数据文件已全部保存，且系统无操作。

----结束

9.2.5 重启服务


出于维护目的，当系统的运行异常，用户可以尝试重启服务即相关进程，恢复到可用状态。

- 当实例的“运行状态”为“运行中”时，可执行重启操作。
- 重启API数据安全防护实例将导致系统业务中断约5分钟，在此期间实例“运行状态”将显示为“重启中”。
- 重启过程中，API数据安全防护实例将不可用。

操作步骤

步骤1 [登录管理控制台](#)。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全与合规 > 数据安全中心”。

步骤4 选择“数据资产保护 > API数据安全防护”，进入“API数据安全防护”界面。

步骤5 在需要重启服务的实例所在行，单击“操作”列的“更多 > 重启服务”。

步骤6 在弹出的是否要重启服务的对话框中，单击“确定”。

步骤7 重启过程一般需要5-10分钟左右，且实例状态会变成“重启中”。

实例状态变为“运行中”，即重启完成，可以正常使用系统。

----结束


9.2.6 解绑弹性公网 IP

当实例需要重新绑定EIP或者释放EIP时，需要为该实例解绑EIP。当实例成功解绑EIP后，则无法再通过该EIP登录API数据安全防护实例。

解绑弹性公网 IP

步骤1 [登录管理控制台](#)。

步骤2 单击左上角的，选择区域或项目。

- 步骤3** 在左侧导航树中，单击 ，选择“安全与合规 > 数据安全中心”。
- 步骤4** 选择“数据资产保护 > API数据安全防护”，进入“API数据安全防护”界面。
- 步骤5** 在需要解绑弹性IP的实例所在行，单击“操作”列的“更多 > 解绑弹性公网IP”。
- 步骤6** 在弹出的解绑EIP对话框中确认解绑IP信息后，单击“确定”。
- 解绑成功后，“弹性IP”列无IP信息，且“本地登录”变为不可操作。

----结束



9.2.7 重置密码

实例包含三个默认账户，系统管理员账号（sysadmin）、安全管理员账号（secadmin）和审计管理员账号（audadmin），支持重置这3个账号中任何一个账号的密码，重置密码在2~3min内生效。

前提条件

“实例状态”为“运行中”。

重置密码

- 步骤1** [登录管理控制台](#)。
- 步骤2** 单击左上角的 ，选择区域或项目。
- 步骤3** 在左侧导航树中，单击 ，选择“安全与合规 > 数据安全中心”。
- 步骤4** 选择“数据资产保护 > API数据安全防护”，进入“API数据安全防护”界面。
- 步骤5** 在需要重置密码的实例所在行，单击“操作”列的“更多 > 重置密码”。
- 步骤6** 在“重置密码”对话框中，单击下拉框选择需要重置密码的“用户名”，输入“登录密码”和“确认密码”。
- 步骤7** 单击“确定”，重置密码在2~3min内生效。

----结束

9.2.8 版本升级

主备类型的API数据安全防护实例支持在管理界面进行自动化升级。

前提条件

“实例状态”为“运行中”。

版本升级

- 步骤1** [登录管理控制台](#)。
- 步骤2** 单击左上角的 ，选择区域或项目。


- 步骤3** 在左侧导航树中，单击 ，选择“安全与合规 > 数据安全中心”。
- 步骤4** 选择“数据资产保护 > API数据安全防护”，进入“API数据安全防护”界面。
- 步骤5** 在需要进行升级的实例所在行，单击“操作”列的“更多 > 版本升级”。
- 步骤6** 在“版本升级”对话框中，显示“上次升级任务状态”、“当前可升级的版本”。升级方式：
- 立即升级：输入确认升级信息，单击“确定”后立即开始升级，升级预计需要30分钟，升级过程中不可操作实例。
 - 预约升级：选择升级开始时间，输入确认升级信息，单击“确定”提示升级命令下发成功即任务下发成功，在升级开始时间执行升级任务。

图 9-5 版本升级



----结束

9.3 系统管理员操作指南

9.3.1 首页概览

系统管理员登录成功后，将自动进入“概览”页面。您可通过查看概览页面，了解API数据安全保护的资产与风险情况，可在界面右上角选择“近7天”或者“近30天”的概览信息。

查看访问概览信息

首页概览页面以可视化面板的形式展示系统的统计信息。

- 步骤1** 使用系统管理员sysadmin账号[登录API数据安全防护系统web控制台](#)。
- 步骤2** 在左侧导航栏，选择“首页概览 > 访问概览”。

步骤3 在“访问概览”页面，查看资产的概览统计信息。

图 9-6 访问概览

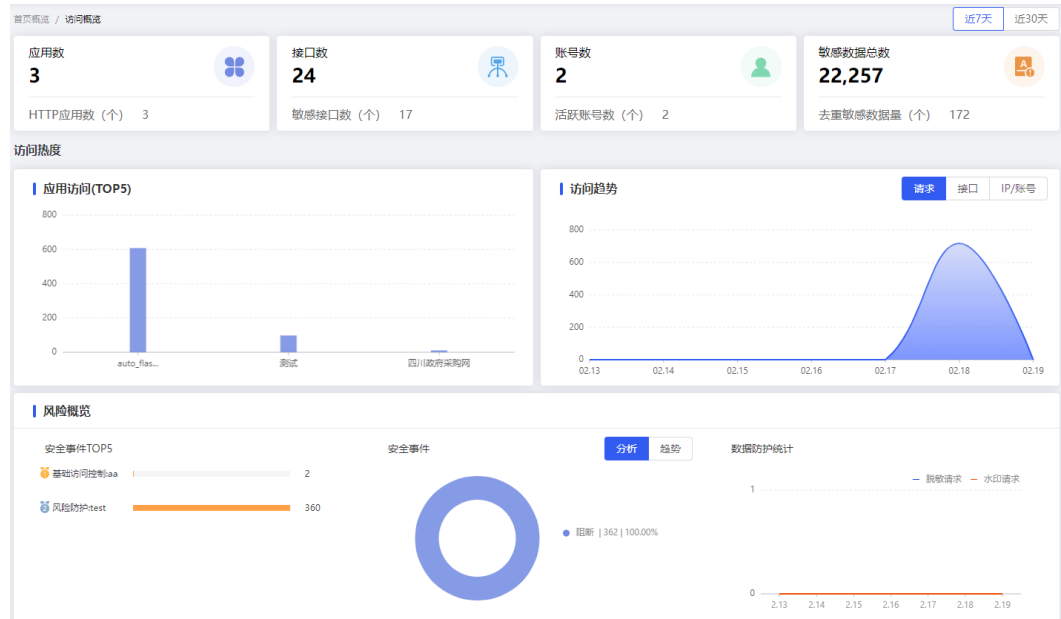


表 9-3 访问概览信息看板

区域	说明
资产概览	<p>显示数据资产概览统计信息。</p> <ul style="list-style-type: none"> 应用数：审计应用资产的总个数。 接口数：审计所有应用的接口个数总和。 敏感数据总数：所有应用的敏感数据数量统计。 账号数：审计所有应用的登录账号个数总和。
访问热度	<p>统计所选时间段内应用资产的访问热度。</p> <ul style="list-style-type: none"> 应用访问（TOP5）：展示被访问次数最多的应用TOP5。 访问趋势：展示所选时间段内访问应用次数的热度趋势。
风险概览	<p>统计所选时间段内应用资产的风险事件。</p> <ul style="list-style-type: none"> 安全事件TOP5：展示被触发次数最多的风险规则TOP5。 安全事件分析/趋势：展示所选时间段内安全事件的响应类型以及时间趋势。 数据防护统计：展示所选时间段内脱敏与水印服务的请求趋势。

----结束

9.3.2 资产中心

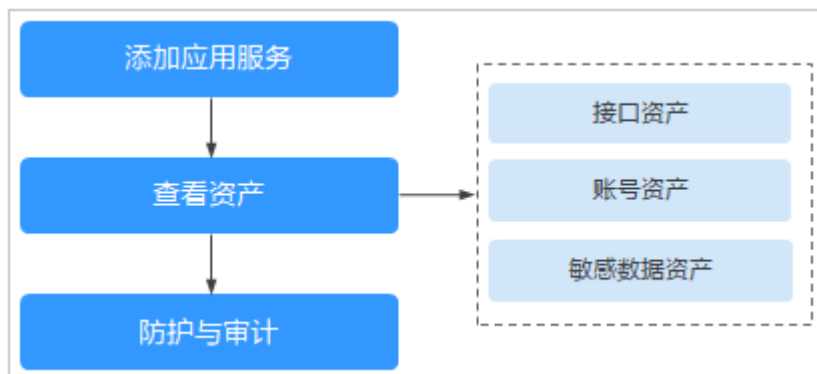
9.3.2.1 资产中心概览

资产中心模块包括应用资产、接口资产、账号资产以及敏感数据资产。

您需要将目标应用手动添加至应用资产页面，代理访问应用成功后，系统将识别接口、账号与敏感数据资产。

使用流程

图 9-7 使用流程



9.3.2.2 应用服务

添加应用服务是API数据安全防护实现应用防护的第一步。添加完成并代理访问应用后，系统将自动梳理应用中的接口、账号以及敏感数据，并对资产进行防护与审计。

将需要审计与防护的应用资产手动添加至“应用服务”页面，实现代理访问应用资产。

例如，您需要添加一个应用，应用名为demo，应用资产的域名为example.com，应用原地址为172.xx.xx.53:8182，应用协议为https模式；API数据安全防护服务器地址为172.xx.xx.44:8441。

本章节介绍如何将该应用添加至应用资产，实现代理访问。

添加代理应用

步骤1 使用系统管理员sysadmin账号[登录API数据安全防护系统web控制台](#)。

步骤2 在左侧导航栏，选择“资产中心 > 应用服务”。

步骤3 单击“添加”。

步骤4 在“添加应用资产”对话框中，设置资产信息。

图 9-8 添加应用资产

添加应用资产

智能填写: 172.16.43.51:8182 识别

* 应用名称: demo

* 服务:

访问地址: 172.16.43.51:46586

协议: http

WebSocket:

服务名: http://172.16.43.51:46586

* 访问路径: /
访问路径需以"/"开始和结尾, 例: "/api/"

* 源站协议: http https

* 源站地址: IP 域名

172.16.43.51:8182

IPv4地址示例: 172.16.43.51:8080
IPv6地址示例: [fe80::fb0a:24d9:d772:1cca]:8080

源站路径: 请输入
源站路径需以"/"开始和结尾, 例: "/api/"

* 负载均衡策略: 轮询 IP Hash 随机 最小连接

取消 确定

表 9-4 添加应用资产

参数	说明
智能填写	将应用服务器原始URL复制到此处, 单击“识别”, 可智能识别并填写各项参数。
应用名称	自定义设置应用服务的名称。

参数	说明
服务-访问地址	<p>填写客户端用户最终访问的地址，与应用协议绑定。</p> <ul style="list-style-type: none"> ● 如果填写域名（例如example.com），无需填写端口。配置后访客通过该域名代理访问应用资产。 ● 如果填写域名，需要修改域名和IP的映射关系，使该域名解析到API数据安全防护的IP。正常情况下修改DNS中域名与IP的映射关系；没有DNS时或者测试时，可以通过修改客户端的hosts文件，使域名解析到API数据安全防护的IP。 ● 如果填写IP，则填写API数据安全防护的IP与代理端口，端口可配置为1~65535范围内的空闲端口。配置后，访客通过该IP + 端口号即可代理访问应用资产。
服务-协议	<ul style="list-style-type: none"> ● 选择API数据安全防护服务器的代理协议。 ● 如果选择https，需要在证书选择下拉框中选择证书。
证书选择	<p>如果“应用协议”选择“https”，需要在“应用证书”下拉框中选择证书。在此之前，需要在证书管理页面上传或制作证书。具体操作请参见证书管理。</p>
访问路径	代理路径，客户端访问地址url的前缀。
源站协议	选择源站协议，即应用原地址所用协议。
源站地址	<p>选择源站地址的类型，包括ip与域名。</p> <ul style="list-style-type: none"> ● 如果源站地址为ip，则输入应用服务器原始IP地址，即服务端原本的地址（例如图中的172.16.35.53+端口号）。 ● 如果源站地址为域名，则输入应用服务器原始域名。
DNS服务器	如果源站地址选择域名，则需要输入代理服务器DNS地址。
服务端IP	如果源站地址选择域名，不输入DNS地址也可以输入服务端IP。
源站路径	源站url的前缀。
负载均衡策略	选择代理访问的负载均衡策略，当源站地址有多个时将采用配置的负载均衡策略进行访问。
启用状态	选择是否启用该应用代理服务。

步骤5 单击“确定”。

步骤6 添加完成后，访客通过配置的应用域名/IP（例如example.com）可对应用进行代理访问。

图 9-9 应用资产列表



----结束

相关操作

在“应用服务”页面中支持进行以下应用管理操作：

- 编辑应用资产：单击目标应用右侧的“编辑”，修改应用资产配置。
- 删除应用资产：单击目标应用右侧的“删除”，删除不再需要的应用资产。
- 批量删除应用资产：勾选多个应用，单击右上角的“删除”。
- 查看接口信息：单击目标应用右侧的 \dots ，在下拉框中选择接口配置，查看应用资产的接口信息。

9.3.2.3 接口资产

API数据安全防护添加应用资产后，将自动梳理接口资产，并根据所配置的敏感数据标签，将接口划分为敏感接口与非敏感接口。

您可以对系统中的接口资产进行管理，包括查询、配置、删除等操作。

📖 说明

在添加应用并配置代理后，如果有流量第一次访问该应用的某个接口，则会自动发现该接口并添加至接口列表。如果接口中识别到敏感数据标签，将定义为敏感接口。

前提条件

已添加代理应用，操作步骤请参见[添加代理应用](#)。

禁用接口

步骤1 使用系统管理员sysadmin账号[登录API数据安全防护系统web控制台](#)。

步骤2 在左侧导航栏，选择“资产中心 > 接口资产”。

图 9-10 接口资产页面

接口名称	接口URL	应用名称	接口类型	流量	访问数	敏感属性	启用状态	发现时间	操作
<input type="checkbox"/>	/faker/sensitive/ldogin	/faker/sensitive/ldogin	demo	普通接口	3.55KB	2	敏感	2024-08-21 14:56:42	接口配置 删除
<input type="checkbox"/>	/faker/sensitive/test	/faker/sensitive/test	demo	普通接口	3.29KB	2	敏感	2024-08-21 14:56:24	接口配置 删除
<input type="checkbox"/>	/faker/sensitive/app	/faker/sensitive/app	demo	普通接口	20.24KB	12	敏感	2024-08-21 14:53:01	接口配置 删除
<input type="checkbox"/>	/test/sensitive	/test/sensitive	demo	普通接口	3.12KB	2	敏感	2024-08-21 14:52:01	接口配置 删除

步骤3 关闭目标接口的启用状态。

📖 说明

禁用后，所有配置的规则对该接口不生效。识别到的接口默认为启用状态。

----结束

修改接口操作步骤

步骤1 使用系统管理员sysadmin账号[登录API数据安全防护系统web控制台](#)。

步骤2 在左侧导航栏，选择“资产中心 > 接口资产”。

图 9-11 接口资产页面

接口名称	接口URL	应用名称	接口类型	流量	访问量	接口属性	应用状态	发现时间	操作
/faker/sensitive/dologin	/faker/sensitive/dologin	demo	普通接口	3.55KB	2	敏感	开启	2024-08-21 14:56:42	接口配置 删除
/faker/sensitive/test	/faker/sensitive/test	demo	普通接口	3.29KB	2	敏感	开启	2024-08-21 14:56:24	接口配置 删除
/faker/sensitive/app	/faker/sensitive/app	demo	普通接口	20.24KB	12	敏感	开启	2024-08-21 14:53:01	接口配置 删除
/test/sensitive	/test/sensitive	demo	普通接口	3.12KB	2	敏感	开启	2024-08-21 14:52:01	接口配置 删除

步骤3 如果需要修改接口信息，则在接口资产列表区域，单击目标接口右侧的“接口配置”，修改接口资产的相关信息。

----结束

相关操作

- 删除接口：单击接口资产列表“操作”列的“删除”，删除接口资产。
- 其他批量操作：勾选多个目标接口，单击右上角的“批量操作”，在下拉框中选择相应操作。

9.3.2.4 账号资产

9.3.2.4.1 配置账号解析规则

API数据安全防护系统添加应用资产后，将自动梳理接口资产。配置账号解析规则后，系统将识别账号资产，并对账号资产进行审计。

您需要配置应用的账号解析参数，配置完成后，如果有用户通过代理登录应用，系统将根据所配置的账号解析参数识别账号资产，梳理至账号资产页面，访问相应接口的日志详情中将标记账号信息。

前提条件

确保您已经添加代理应用，具体请参见[添加代理应用](#)。

操作步骤

- 步骤1** 使用系统管理员sysadmin账号[登录API数据安全防护系统web控制台](#)。
- 步骤2** 在左侧导航栏，选择“资产中心 > 账号资产”。
- 步骤3** 单击“账号解析”。
- 步骤4** 在“账号解析”页面，单击“添加”。
- 步骤5** 在添加账号解析规则对话框中配置账号解析参数，完成后单击“确定”。

图 9-12 添加账号解析规则

添加账号解析规则
✕

* 规则名称:

* 应用名称: 全部 自选

demo ✕

* 接口关键字:

* token关键字:

* 账号关键字:

是否开启:

^ 扩展发现

表 9-5 账号解析规则参数说明

参数	说明
规则名称	填写规则名称。
应用名称	选择规则适用的应用，可选全部或自选。 <ul style="list-style-type: none"> 全部：规则适用于所有应用。 自选：从下拉框中选择规则适用的应用。
接口关键字	填写接口关键字。可在代理访问的应用页面使用F12查看接口信息。
token关键字	填写token关键字。可在代理访问的应用页面使用F12查看token信息。
账号关键字	填写账号关键字。可在代理访问的应用页面使用F12查看账号的键名信息。
是否开启	开启和关闭规则。 <ul style="list-style-type: none"> 开启状态：添加规则后直接生效。 关闭状态：配置完成后不生效，需要手动开启。

参数	说明
拓展发现	是否开启扩展发现：选择是否启用账号拓展发现。 启用后，配置账号来源及具体参数，可从缓存或页面发现账号。

----结束

操作结果

配置完成并启用账号解析规则后，如果有用户登录应用，系统将识别到账号资产，梳理至“账号列表”页面。

图 9-13 识别到账号资产

账号ID	用户名	登录方式	常用登录IP	风险等级	最后登录IP	风险等级	操作
vrf052	echo	账号密码	119.101.111.227	0	172.16.1.36	0	删除
duwind02	echo	账号密码	129.10.10.224	0	73.111.111.235	0	删除
test	echo	账号密码	111.10.111.205	0	12.111.111.231	0	删除
admin1	echo	账号密码	172.16.1.36	0	172.16.1.36	0	删除
admin	echo	账号密码	172.16.1.36	0	172.16.1.36	0	删除
sysadmin	账号密码	账号密码	172.16.1.36	0	172.16.1.36	0	删除

9.3.2.4.2 配置账号分组

您可对应用的账号进行分组，后续在配置安全策略时可通过账号分组作为匹配条件。

操作步骤

- 步骤1** 使用系统管理员sysadmin账号登录API数据安全防护系统web控制台。
- 步骤2** 在左侧导航栏，选择“资产中心 > 账号资产”。
- 步骤3** 单击“分组管理”页签。
- 步骤4** 配置账号分组信息。
 - 在“账号组”区域，单击“添加”，添加账号组。
 - 单击账号组名称，进入步骤4.1添加的账号组。
 - 在账号列表区域，单击“添加”，添加账号标识并选择该账号所属的账号组，完成后保存。

图 9-14 添加账号

账号组名称	账号组	备注	添加时间	操作
账号组测试	-	-	2024-08-27 16:26:47	编辑 删除
125	账号组测试	125	2024-08-27 16:26:41	编辑 删除

说明

添加的账号标识须选择已识别到的账号。

----结束

9.3.2.5 敏感数据资产

API数据安全防护添加应用后，将根据启用的敏感数据标签来识别接口中的敏感数据资产，梳理至“敏感数据资产”页面。

您可在敏感数据资产页面查看各应用中包含的敏感数据，形成敏感数据的统计概览。

系统将根据启用的敏感数据标签对识别到的敏感数据资产进行梳理，您可在敏感数据资产页面查看系统识别到的敏感数据资产。

前提条件

- 确保您已经添加代理应用，具体请参见[添加代理应用](#)。
- 确保您已配置并开启敏感数据标签，具体操作，请参见[添加敏感数据标签](#)。

操作步骤

步骤1 使用系统管理员sysadmin账号[登录API数据安全防护系统web控制台](#)。

步骤2 在左侧导航栏，选择“资产中心 > 敏感数据”。

步骤3 在“敏感数据资产”页面，查看敏感数据审计信息。

图 9-15 敏感数据资产

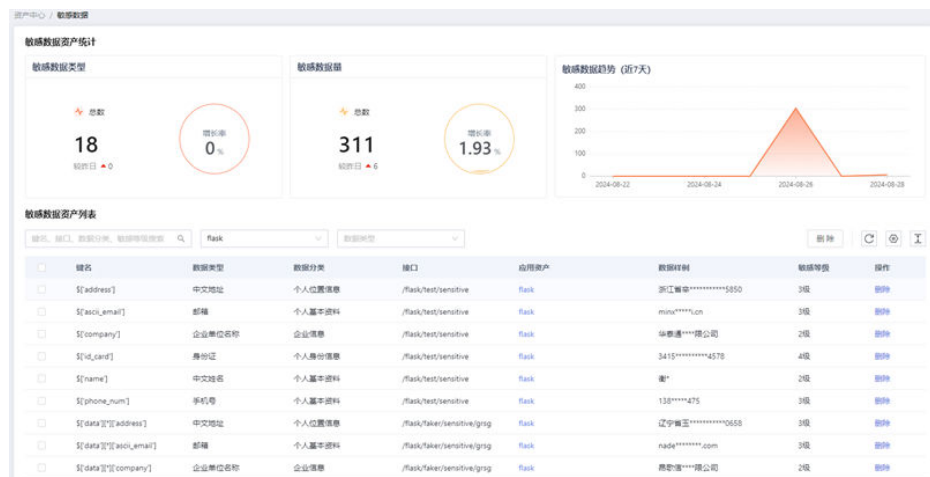


表 9-6 敏感数据资产

区域	说明
敏感数据资产统计	<ul style="list-style-type: none"> 敏感数据类型数据：统计所选应用敏感数据类型的总量与敏感数据类型的当日新增量。 敏感数据量：统计所选应用敏感数据的总量与当日新增量。 敏感数据量图：展示所选应用近7天内敏感数据每日新增量的变化趋势。
检索条件	通过检索条件搜索对应的敏感数据。
敏感数据列表	展示敏感数据的具体信息。 说明 数据分类与敏感等级根据配置进行匹配，具体操作，参见 添加分类标签 和 添加分级标签 。

----结束

相关操作

除了以上操作，您还可以进行以下管理操作：

- 删除敏感数据资产：找到目标敏感数据资产，单击右侧的“删除”。
- 批量删除敏感数据资产：勾选多个敏感数据资产，单击右上角的“删除”。

9.3.3 安全策略管理

9.3.3.1 创建白名单

对于受信任的访问者，您可配置白名单。系统支持从应用、账号、客户端IP等维度配置白名单。

配置白名单策略后，针对命中白名单策略的访问会放行。

例如，对于应用demo，来自客户端IP172.xx.xx.28为受信任的IP，来自客户端IP172.xx.xx.28的访问均可放行。如下步骤说明如何将客户端IP172.xx.xx.28配置为应用demo的白名单。

操作步骤

- 步骤1** 使用系统管理员sysadmin账号[登录API数据安全防护系统web控制台](#)。
- 步骤2** 在左侧导航栏，选择“安全策略 > 白名单”。
- 步骤3** 单击“添加”，配置白名单规则参数。

图 9-16 配置白名单规则

表 9-7 白名单参数说明

参数	说明
规则名称	自定义白名单规则的名称。
规则描述	添加规则的描述信息。
应用名称	选择白名单适用的应用资产。
规则条件	配置白名单的规则条件，可配置项包括客户端IP、区域、账号、账号组等。
生效范围	配置白名单的生效范围，勾选后，如果访问命中勾选的规则项，则白名单优先生效。 例如此处勾选水印，如果访问同时命中白名单，则白名单生效，水印不生效。
是否开启	开启和关闭白名单。 <ul style="list-style-type: none"> 开启状态：添加白名单后直接生效。 关闭状态：配置完成后不生效，需要手动开启。

步骤4 单击“确定”。

步骤5 添加完成后，以客户端IP172.xx.xx.28访问应用demo，访问将放行。

----结束

相关操作

在“白名单”列表页面，您还可以进行以下管理操作：

- 修改白名单：找到目标白名单，单击右侧的“编辑”。
- 删除白名单：找到目标白名单，单击右侧的“删除”。
- 批量删除白名单：勾选多个目标白名单，单击右上角的“删除”。
- 批量启用白名单：勾选多个目标白名单，单击右上角的“启用”。
- 批量禁用白名单：勾选多个目标白名单，单击右上角的“禁用”。

9.3.3.2 访问控制

9.3.3.2.1 添加基础访问控制规则

操作场景

系统支持从应用、接口、Host、用户、客户端IP等维度配置基础访问控制规则，对命中规则的请求实行放行或阻断动作。

例如，应用Demo拥有文件下载接口，您可以添加基础访问控制规则阻断访问应用Demo的文件下载接口的请求。

本章节介绍如何创建基础访问控制规则。

操作步骤

步骤1 使用系统管理员sysadmin账号[登录API数据安全防护系统web控制台](#)。

步骤2 在左侧导航栏，选择“安全策略 > 访问控制”。

步骤3 选择“基础访问控制”页签，单击“添加”，配置基础访问控制规则参数。相关参数说明请参见[表 基础访问控制规则参数说明](#)。

图 9-17 配置基础访问控制规则

添加基础访问控制规则

* 规则名称: test1

规则描述: 请输入

* 应用名称: 全部 自选

demo x

规则条件: 账号 等于 admin

+ 添加

* 执行动作: 放行 阻断

* 优先级: 100

* 生效时间: 永久生效 自定义

是否开启:

取消 确定

表 9-8 添加基础访问控制规则参数说明

参数	说明
规则名称	自定义规则的名称。
规则描述	添加规则的描述信息。
应用名称	选择该规则适用的应用。
规则条件	配置该规则的规则条件，可配置项包括请求方法、URL、请求体、接口类型、客户端IP、区域、账号、账号组等。
执行动作	配置命中该规则后的执行动作。
优先级	当请求命中多个基础访问控制规则时，优先级更高的规则生效。
生效时间	配置规则的生效时间。 <ul style="list-style-type: none"> 永久生效：该规则开启状态下永久生效。 自定义：配置在每周或每天的固定时间段生效。
是否开启	开启和关闭基础访问控制规则。 <ul style="list-style-type: none"> 开启状态：添加规则后直接生效。 关闭状态：配置完成后不生效，需要手动开启。

步骤4 单击“确定”，添加基础访问控制规则。

----结束

操作结果

添加完成后，访问控制规则生效；访问应用的请求将根据规则放行和阻断。

相关操作

在“基础访问控制规则”列表页面，您还可以进行以下管理操作：

- 修改基础访问控制规则：找到目标规则，单击右侧的“编辑”。
- 删除基础访问控制规则：找到目标规则，单击右侧的“删除”。
- 批量删除基础访问控制规则：勾选多个目标规则，单击右上角的“删除”。
- 批量启用基础访问控制规则：勾选多个目标规则，单击右上角的“启用”。
- 批量禁用基础访问控制规则：勾选多个目标规则，单击右上角的“禁用”。

9.3.3.2.2 添加黑名单

操作场景

对于不受信任的访问者，您可配置黑名单。系统支持从应用、账号、客户端IP等维度配置黑名单。配置黑名单后，命中黑名单的访问会被直接阻断，且命中黑名单的审计日志风险等级会标记为“非法”。

例如，对于应用demo，客户端IP172.xx.xx.28为不受信任的IP，您可以添加黑名单阻断来自这个IP的所有访问。

本章节介绍如何创建黑名单。

操作步骤



步骤1 使用系统管理员sysadmin账号[登录API数据安全防护系统web控制台](#)。

步骤2 在左侧导航栏，选择“安全策略 > 访问控制”。

步骤3 选择“黑名单”页签，单击“添加”，配置黑名单规则参数。相关参数说明请参见[表添加黑名单规则参数说明](#)。

图 9-18 添加黑名单规则

表 9-9 添加黑名单规则参数说明

参数	说明
规则名称	自定义规则的名称。
规则描述	添加规则的描述信息。
应用名称	选择该规则适用的应用。
规则条件	配置该规则的规则条件，可配置项包括URL、客户端IP、区域、账号、账号组等。
是否开启	开启和关闭黑名单。 <ul style="list-style-type: none">  开启状态：添加黑名单后直接生效。  关闭状态：配置完成后不生效，需要手动开启。

步骤4 单击“确定”，添加黑名单规则。

----结束

操作结果

添加完成后，命中黑名单规则的访问会被阻断；日志中心中该访问的风险等级被标记为“非法”，表示黑名单配置生效。

相关操作

在“黑名单”列表页面，您还可以进行以下管理操作：

- 修改黑名单：找到目标黑名单，单击右侧的“编辑”。
- 删除黑名单：找到目标黑名单，单击右侧的“删除”。
- 批量删除黑名单：勾选多个目标黑名单，单击右上角的“删除”。
- 批量启用黑名单：勾选多个目标黑名单，单击右上角的“启用”。
- 批量禁用黑名单：勾选多个目标黑名单，单击右上角的“禁用”。

9.3.3.2.3 添加流量控制规则

操作背景

在需要对应用进行限流时，可对应用添加流量控制规则。

例如，如果您需要对应用demo进行限流，可以添加流量控制规则使其访问应用中所有接口的阈值上限为每秒钟1000次。

本章节介绍如何创建流量控制规则。

操作步骤

- 步骤1** 使用系统管理员sysadmin账号[登录API数据安全防护系统web控制台](#)。
- 步骤2** 在左侧导航栏，选择“安全策略 > 访问控制”。
- 步骤3** 选择“流量控制”页签。
- 步骤4** 单击“添加”，配置流量控制规则参数。相关参数说明请参见[表 流量控制规则参数说明](#)。



图 9-19 添加流量控制规则

The screenshot shows a dialog box titled "添加流量控制规则" (Add Traffic Control Rule) with a close button (X) in the top right corner. The form contains the following fields and controls:

- * 规则名称:** A text input field containing "demo流控1000/s".
- 规则描述:** A text area containing "对测试demo应用进行1000次/秒的流控".
- * 应用名称:** A dropdown menu showing "demo".
- * 应用流量阈值:** A control consisting of a unit dropdown set to "秒", a text input field containing "1000", and a unit label "次 (次: 10-10w)".
- 是否开启:** A toggle switch that is currently turned on (blue).

At the bottom right of the dialog, there are two buttons: "取消" (Cancel) and "确定" (Confirm).

表 9-10 添加流量控制规则参数说明

参数	说明
规则名称	自定义流控规则的名称。
规则描述	填写规则的描述信息。
应用名称	在下拉框中选择规则适用的应用。
应用流量阈值	配置流量阈值，时间单位可选秒或分钟。
是否开启	开启和关闭规则。 <ul style="list-style-type: none">  开启状态：添加规则后直接生效。  关闭状态：配置完成后不生效，需要手动开启。

步骤5 单击“确定”，添加流量控制规则。

----结束

操作结果

添加完成并启用后，高频访问应用时，获取接口数据的速率会被限制。

相关操作

在“流量控制”页面，您还可以进行以下管理操作：

- 修改规则：找到目标规则，单击右侧的“编辑”。
- 删除规则：找到目标规则，单击右侧的“删除”。
- 批量删除规则：勾选多个目标规则，单击右上角的“删除”。
- 批量启用规则：勾选多个目标规则，单击右上角的“启用”。
- 批量禁用规则：勾选多个目标规则，单击右上角的“禁用”。

9.3.3.3 启用内置规则


操作场景

系统拥有内置风险规则，您可启用系统内置风险规则，对应用数据资产进行防护。

操作步骤

步骤1 使用系统管理员sysadmin账号[登录API数据安全防护系统web控制台](#)。

步骤2 在左侧导航栏，选择“安全策略 > 风险防护”，并单击“内置规则”页签。


步骤3 在列表区域找到目标规则，单击其右侧的  图标，启用规则。

如果需要批量启用多个规则，则在列表区域勾选多个目标内置规则，单击右上角的“批量操作 > 启用”。

----结束

相关操作

后续您可以根据需要，在“内置规则列表”页签进行以下管理操作：

- 编辑内置规则：单击目标规则右侧的“编辑”，编辑规则适用的应用范围、风险等级、攻击规则、响应动作等。
- 禁用单个内置规则：找到已启用的目标内置规则，单击其右侧的  图标，禁用规则。
- 批量禁用内置规则：勾选多个目标内置规则，单击右上角的“禁用”。

9.3.3.4 添加自定义规则

操作背景

自定义的风险防护规则包括IP访问异常、账号访问异常与其他异常三类，当出现异常情况时，可进行告警或阻断访问。

例如，您认为同一客户端IP在1分钟内访问demo应用超过1000次是一种风险行为，希望出现这种情况时将其阻断5分钟，可以创建自定义规则进行阻断。

本章节介绍如何创建自定义规则。

操作步骤

- 步骤1** 使用系统管理员sysadmin账号[登录API数据安全防护系统web控制台](#)。
- 步骤2** 在左侧导航栏，选择“安全策略 > 风险防护”，并单击“自定义规则”页签。
- 步骤3** 在“自定义规则”页面，单击“添加”。
- 步骤4** 在添加自定义规则对话框中，配置规则具体参数。相关参数说明请参见[表9-11](#)。

图 9-20 添加自定义规则



The screenshot shows a configuration window titled '添加自定义规则' (Add Custom Rule). The fields are as follows:

- 规则名称:** 自定义IP访问异常
- 规则类型:** IP访问异常
- 应用名称:** 全部 (radio), 自选 (radio selected)
- 应用名称输入框:** demo x
- 风险等级:** 高风险
- 规则条件:**
 - 客户端IP 等于 172.16.194.1~172.16.194.255
 - 接口类型 等于 文件上传接口 x 文件下载接口 x
 - + 添加
- 触发频率:** 10 秒 访问次数 超过 10000 次
- 响应动作:** 告警 (radio), 阻断 (radio selected)
- 阻断时间:** 5 分
- 是否开启:** 开启 (toggle)

Buttons: 取消 (Cancel), 确定 (Confirm)

表 9-11 添加自定义规则参数说明

参数	说明
规则名称	自定义填写规则名称。
规则类型	选择规则类型，可选IP访问异常、账号访问异常或其他异常。
应用名称	在下拉框中选择规则适用的应用。
风险等级	选择命中该规则的请求的风险等级。
规则条件	配置该规则的规则条件，可配置项包括请求方法、URL、请求参数、请求体、数据标签、客户端IP等
触发频率	配置该规则的触发条件。其中时间单位可选秒、分、时： <ul style="list-style-type: none"> 选择秒时，时间可填10 ~ 86400间任意整数； 选择分时，时间可填1 ~ 1440间任意整数； 选择时时，时间可填1 ~ 24间任意整数； 访问次数可填1 ~ 100000间任意整数。

参数	说明
响应动作	选择规则的响应动作。 <ul style="list-style-type: none"> 告警：访问匹配该规则时，产生告警日志。 阻断：访问匹配该规则时，对访问进行阻断，并产生告警日志。 选择阻断时，需配置阻断时间。
阻断时间	配置阻断时间。时间单位可选秒、分、时，时间设置的阈值为10秒 ~ 10000时。
是否启动	开启和关闭规则。 <ul style="list-style-type: none">  开启状态：添加规则后直接生效。  关闭状态：配置完成后不生效，需要手动开启。

步骤5 规则配置完成后，单击“确定”。

----结束

操作结果

添加完成并启用后，以同一客户端IP高频访问应用触发该规则，将被告警或阻断。

相关操作

在“风险防护”页面，您还可以进行以下管理操作：

- 放行被阻断的IP：单击目标规则右侧的“放行”，可放行触发风险防护规则而被拒绝访问的IP。
后续如果IP再次触发该规则，仍会被阻断。放行按钮对于响应动作为告警的规则无实质效果。
- 修改风险防护规则：找到目标规则，单击右侧的“编辑”。
- 删除风险防护规则：找到目标规则，单击右侧的“删除”。
- 批量删除风险防护规则：勾选多个目标规则，单击右上角的“批量操作 > 删除”。
- 批量启用风险防护规则：勾选多个目标规则，单击右上角的“批量操作 > 启用”。
- 批量禁用风险防护规则：勾选多个目标规则，单击右上角的“批量操作 > 禁用”。

9.3.3.5 添加内容替换规则

操作场景

内容替换规则支持根据Key名进行接口内容替换。

例如，您希望应用demo接口中的内容“杨xx”替换为“张三”，可使用内容替换规则。

本章节介绍如何配置创建内容替换规则。

操作步骤

- 步骤1** 使用系统管理员sysadmin账号[登录API数据安全防护系统web控制台](#)。
- 步骤2** 在左侧导航栏，选择“安全策略 > 内容替换”。
- 步骤3** 在“内容替换”页面，单击“添加”，配置内容替换规则参数。相关参数说明请参见[表 添加内容替换规则参数说明](#)。

图 9-21 配置内容替换规则

表 9-12 添加内容替换规则参数说明

参数	说明
规则名称	自定义内容替换规则的名称。
规则描述	填写规则描述信息。
应用名称	在下拉框中选择规则适用的应用。
接口URL	选择并配置接口匹配条件。输入多条接口时以换行分隔，命中其中一条即触发规则。

参数	说明
替换规则	配置替换规则的具体参数。 <ul style="list-style-type: none"> • 位置：选择替换内容的位置。 • Key：填写替换内容的键名。 • 替换方式：选择替换的匹配方式，包括关键字或正则。 • 源：填写需要替换的原始内容。 • 目标：填写替换后的内容。
文件类型	选择规则适用的文件类型，包括json、html、js 与 xml。

步骤4 参数配置完成后，单击“确定”。

----结束

操作结果

添加完成并启用后，使用代理访问应用，可查看到相关替换内容。

相关操作

在“内容替换”页面，您还可以进行以下管理操作：

- 修改规则：找到目标规则，单击右侧的“编辑”。
- 删除规则：找到目标规则，单击右侧的“删除”。
- 批量删除规则：勾选多个目标规则，单击右上角的“删除”。

9.3.4 脱敏管理

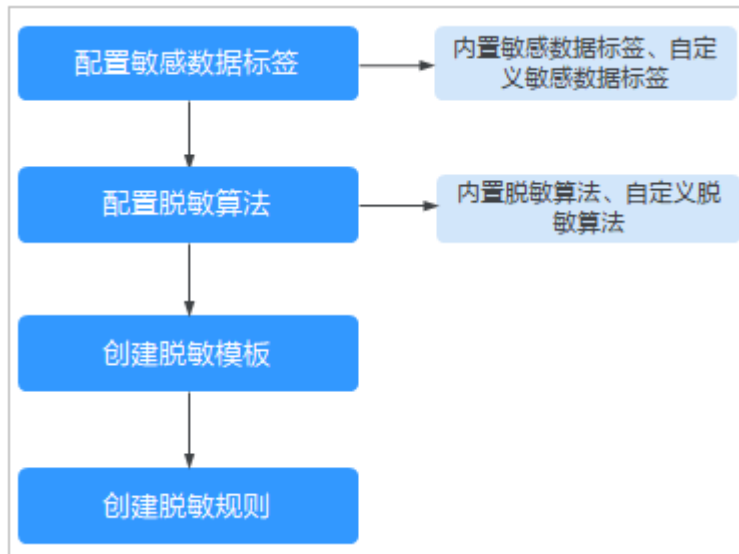
9.3.4.1 概述

API数据安全防护内置常用[添加敏感数据标签](#)，启用标签后系统将自动识别应用接口中的敏感数据，同时您可添加自定义的敏感数据标签。

系统也内置针对这些内置敏感数据标签的常用的脱敏算法，同时支持自定义脱敏算法。您可以配置脱敏算法，形成一套行业脱敏模板。

在配置脱敏规则时，可引用脱敏算法或脱敏模板对接口中的敏感数据进行脱敏。

图 9-22 使用流程介绍



9.3.4.2 新增自定义脱敏算法

操作场景

对于系统内置的敏感数据标签，系统内置了相应的脱敏算法，您可以更新系统内置的脱敏算法，也可新增自定义的脱敏算法。配置并启用脱敏规则后，系统将根据配置的脱敏算法对接口中的敏感数据进行脱敏。脱敏算法可在配置脱敏行业模板时进行引用，具体操作，请参见[配置脱敏模板](#)。

如果内置脱敏算法不能满足业务需求，您可以根据业务特点新增自定义脱敏算法。本章节介绍如何新增自定义脱敏算法。

操作步骤

- 步骤1** 使用系统管理员sysadmin账号[登录API数据安全防护系统web控制台](#)。
- 步骤2** 在左侧导航栏，选择“安全策略 > 脱敏管理”。
- 步骤3** 选择“脱敏算法”页签，单击右上角的“添加自定义算法”。
- 步骤4** 在“添加自定义算法”对话框中，配置自定义算法。相关参数说明请参见[表 添加自定义脱敏算法参数说明](#)。

图 9-23 添加自定义算法

添加自定义算法
✕

* 算法名称:

* 数据标签:

* 脱敏类型: 遮蔽类型 置空类型

遮蔽规则: 保留前 字符

保留后 字符

* 遮蔽符号:

算法说明:

表 9-13 添加自定义脱敏算法参数说明

参数	说明
算法名称	设置自定义算法的名称。
数据标签	在下拉栏中选择关联的敏感数据标签。关于数据标签的说明，请参见 添加敏感数据标签 。
脱敏类型	选择脱敏的算法类型。 <ul style="list-style-type: none"> ● 遮蔽类型：脱敏后数据将被遮蔽。需设置遮蔽规则和遮蔽符号。 <ul style="list-style-type: none"> - 遮蔽规则：设置数据前后保留的字符数，保留的字符脱敏后不被遮蔽。 - 遮蔽符号：在下拉栏中选择用以遮蔽的符号，可选符号包括* # ?。 ● 置空类型：脱敏后数据将置空。
算法说明	描述自定义算法的说明信息。

步骤5 单击“确定”，新增自定义脱敏算法。

----结束

操作结果

新增完成后，您可以在“脱敏算法”列表页面查看新增的自定义算法。后续在创建脱敏模板时，可使用新增的自定义脱敏算法，具体操作，请参见[新增自定义脱敏算法](#)。

相关操作

后续您可以根据情况，在“脱敏算法”列表页面进行以下管理操作。

- 编辑自定义的脱敏算法：单击“编辑”，修改自定义脱敏算法。
- 删除自定义的脱敏算法：单击“删除”，删除不再使用的自定义脱敏算法。

9.3.4.3 配置脱敏模板

操作场景

您可以基于行业信息，创建一套适合行业的脱敏模板，快速关联敏感数据和脱敏算法。脱敏行业模板在创建脱敏规则时可直接使用。

例如，您的企业关注个人财产信息类的隐私，想要创建一套脱敏行业模板，模板中将银行卡号、订单号这两类敏感数据进行部分遮蔽，而对其他类型的敏感数据选择不脱敏。

本章节介绍如何配置脱敏模板。

操作步骤

步骤1 使用系统管理员sysadmin账号[登录API数据安全防护系统web控制台](#)。

步骤2 在左侧导航栏，选择“安全策略 > 脱敏管理”。

步骤3 选择“脱敏模板”页签，单击右上角的“添加模板”。

步骤4 在“添加模板”对话框中，配置模板信息。相关参数说明请参见[表 添加模板参数说明](#)。

图 9-24 添加模板

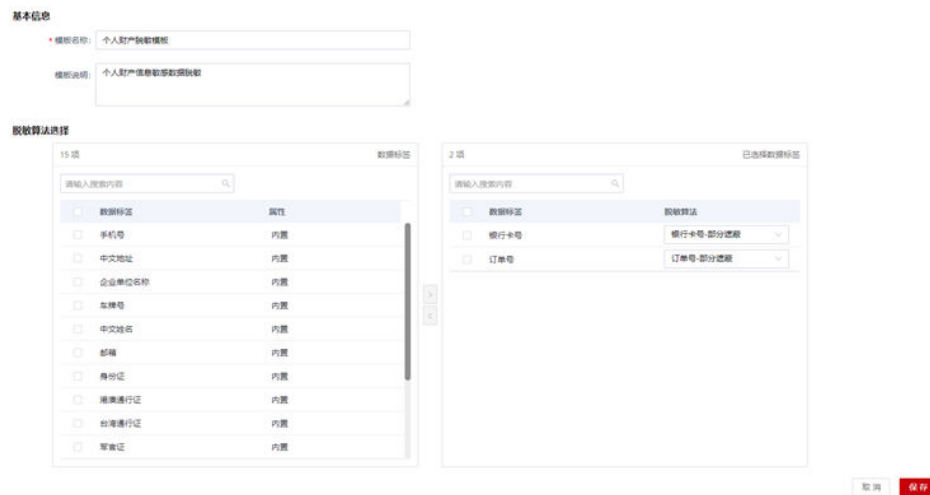


表 9-14 添加模板参数说明

参数	说明
基本信息	填写行业模板的基本信息。 <ul style="list-style-type: none">模板名称：设置行业模板的名称。备注说明：描述行业模板的信息。
脱敏算法选择	选择加入模板的敏感数据类型以及对应的脱敏算法。 <ul style="list-style-type: none">数据类型：勾选加入模板的敏感数据类型。脱敏算法：在下拉栏中选择数据类型对应的脱敏算法。

步骤5 单击“保存”，新增脱敏行业模板。

----结束

操作结果

添加完成后，您可以在“脱敏模板”列表页面查看新增加的行业模板。后续在配置脱敏规则时，可直接引用配置的脱敏行业模板。具体操作，请参见[添加脱敏规则](#)。

相关操作

后续您可以根据情况，在“脱敏模板”列表页面进行以下管理操作。

- 复制脱敏行业模板：单击“复制”，复制一套脱敏行业模板，在此基础上进行修改，可快速创建一个相似的脱敏模板。
- 编辑脱敏行业模板：单击“编辑”，修改自定义行业模板。
- 删除脱敏行业模板：单击“删除”，删除不再使用的自定义行业模板。

9.3.4.4 添加脱敏规则

操作场景

系统支持从应用、URL、客户端IP、账号、账号组等维度配置脱敏规则，对访问行为进行精准鉴权与脱敏防护，您可在脱敏管理模块配置脱敏规则。

例如，您想要对应用demo配置一条脱敏规则，使访问demo应用时，银行卡号类的敏感数据脱敏展示。

本章节介绍如何添加脱敏规则。

说明

脱敏规则仅对代理访问应用服务生效，“检索日志”页面以及“敏感数据”页面的脱敏效果是系统内置的，不会根据脱敏规则的创建而改变。

前提条件

- 确保您已添加应用，具体请参见[应用服务](#)。
- 已配置脱敏模板，具体请参见[配置脱敏模板](#)。

操作步骤

- 步骤1 使用系统管理员sysadmin账号[登录API数据安全防护系统web控制台](#)。
- 步骤2 在左侧导航栏，选择“安全策略 > 脱敏管理”。
- 步骤3 选择“脱敏规则”页签。
- 步骤4 单击“添加”，配置脱敏规则。相关参数说明请参见[表 添加脱敏规则参数说明](#)。

图 9-25 添加脱敏规则

表 9-15 添加脱敏规则参数说明

参数	说明
规则名称	填写自定义的脱敏规则名称。
应用名称	选择使用该规则的应用。
优先级	当请求命中多个脱敏规则时，优先级更高的规则生效。
数据类型	选择脱敏的数据类型。
脱敏算法	配置脱敏算法，可根据脱敏模板、数据标签以及数据字段来匹配敏感数据并脱敏。
规则条件	配置该规则的规则条件，可配置项包括URL、客户端IP、账号、账号组等。

参数	说明
开启交互可见	开启交互可见后，脱敏数据上将展示眼睛图标，单击可查看原始数据。
开启分词	开启后对于段落进行分词。
是否开启	开启和关闭脱敏规则。 <ul style="list-style-type: none"> 开启状态：添加脱敏规则后直接生效。 关闭状态：配置完成后不生效，需要手动开启。

步骤5 单击“确定”，添加脱敏规则。

----结束

操作结果

添加完成后，您可以在列表区域查看新添加的脱敏规则。代理访问应用资产时，将根据脱敏规则进行脱敏，具体操作，请参见[查看脱敏结果](#)。

相关操作

后续您可以根据情况，在“脱敏规则”页面进行以下管理操作。

- 编辑脱敏规则：单击目标规则右侧的“编辑”，修改规则的相关信息。
- 删除脱敏模板：单击目标规则右侧的“删除”，删除脱敏规则。
- 批量删除脱敏规则：勾选目标规则，单击右上方的“删除”，批量删除脱敏规则。

9.3.4.5 查看脱敏结果

操作场景

配置脱敏规则后，使用代理访问应用，可查看脱敏结果。

本章节介绍如何查看并验证所配置脱敏规则的效果。

操作步骤

步骤1 在浏览器中输入代理访问地址，即[应用服务](#)时所配置的应用域名/IP（例如 example.com），回车进行访问。

步骤2 在网页上查看脱敏效果。

如[图 查看脱敏效果](#)所示，信用卡号与订单号根据脱敏规则进行了脱敏展示。

图 9-26 查看脱敏效果



---结束

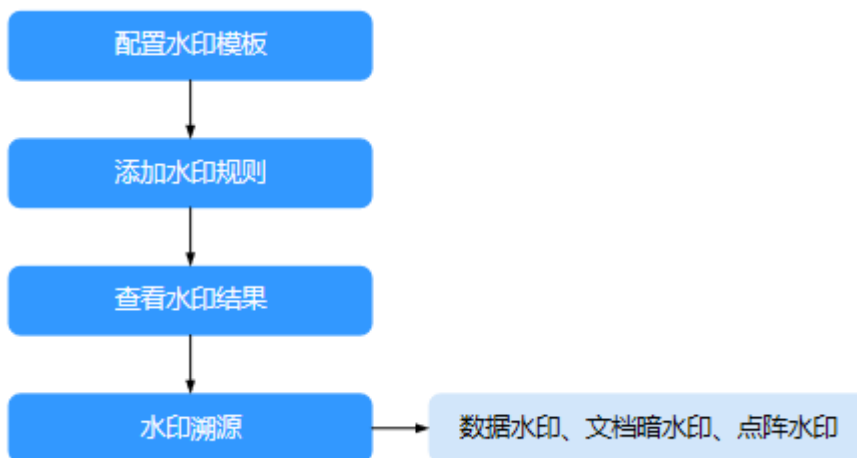
9.3.5 水印管理

9.3.5.1 概述

API数据安全防护支持网页水印、数据水印、文档水印、文档暗水印以及点阵水印。

您可在水印管理模块配置水印模板，并在水印规则中引用配置的水印模板，为应用资产打上水印。对于数据水印、文档暗水印和点阵水印，API数据安全防护支持水印溯源功能，通过水印追溯访问信息，精准定位到相关责任人。

图 9-27 水印使用流程



9.3.5.2 配置水印模板

配置水印模板是使用水印功能的第一步。您需要在系统中手动配置并启用水印模板。

背景信息

系统支持配置网页水印、数据水印、文档水印、文档暗水印以及点阵水印。五种水印形式的说明如下：

- **网页水印:** 直接以文字作为水印，在网页页面上显示，用户访问页面时，可直观地看到水印内容。

图 9-30 启用伪列的数据水印效果



- **文档水印:** 在应用的文档中直观显示。代理访问应用资产时，若客户端有下载文档的动作，将在所下载的文档中打上所配置的文件水印。当前文档类型仅支持 PDF。

图 9-31 文档中的文档水印效果



- **文档暗水印:** 在应用的文档中不可见。代理访问应用资产时，若客户端有下载文档的动作，将在所下载的文档中打上不可见水印。后续可对该文档进行水印溯源。当前文档类型支持PDF、EXCEL、WORD、PPT。
- **点阵水印:** 以点阵图案的形式在网页页面上显示，用户访问页面时，可直观地看到水印内容。

操作步骤

- 步骤1** 使用系统管理员sysadmin账号[登录API数据安全防护系统web控制台](#)。
- 步骤2** 在左侧导航栏，选择“安全策略 > 水印管理”，单击“水印模板”页签。
- 步骤3** 单击“添加”，配置自定义的水印模板。如[图 配置水印](#)所示，详细参数说明如[表 配置水印参数说明](#)。

图 9-32 配置水印

* 名称:

描述:

* 水印类型: 网页水印 数据水印 文档水印 文档暗水印 点阵水印

水印内容: 时间 IP 用户名 应用名称 自定义内容

自定义内容 5/20

字体大小: 14 (12-32)

显示方式: 平铺 固定

间距:

倾斜角度:

字体颜色:

不透明度: 20%

表 9-16 配置水印参数说明

参数	说明
名称	设置自定义的水印模板名称。
描述	对自定义的水印模板添加描述。
水印类型	选择启用的水印类型，可选类型包括： <ul style="list-style-type: none"> ● 网页水印 ● 数据水印 ● 文档水印 ● 文档暗水印 ● 点阵水印

参数	说明
网页水印	配置网页水印的具体参数。 <ul style="list-style-type: none"> • 水印内容：选择网页水印显示的具体内容，支持多选。 • 字体大小：选择网页水印的字体大小。 • 显示方式：选择网页水印的显示方式。 • 间距：选择网页水印的间距类型。 • 倾斜角度：选择网页水印的倾斜角度。 • 字体颜色：选择网页水印的字体颜色。 • 不透明度：选择网页水印的不透明度。
数据水印	配置数据水印的具体参数。 <ul style="list-style-type: none"> • 水印算法：选择数据水印算法。如果选择无痕，则需配置水印位置。 • 水印位置：选择无痕水印添加到数据中的位置。
点阵水印	配置点阵水印的具体参数。 <ul style="list-style-type: none"> • 间距：选择点阵水印的间距类型。 • 颜色：选择点阵的颜色。 • 不透明度：选择点阵水印的不透明度。

步骤4 单击“保存”完成水印模板配置。

步骤5 配置完成后，您可以在水印列表区域查看新增加的水印模板。在配置水印规则时，可引用已配置的水印模板。具体操作请参见[添加水印规则](#)。

----结束

相关操作

您可以根据情况，在水印配置页面进行以下管理操作。

- 复制水印模板：单击“复制”，复制一套水印模板，在此基础上进行修改，可快速创建一个相似的水印模板。
- 编辑水印模板：找到对应目标模板，单击其右侧的“编辑”，修改水印模板的相关信息。
- 删除水印模板：找到对应目标模板，单击其右侧的“删除”，删除水印模板。
- 批量删除水印模板：勾选目标水印模板，单击右上方的“删除”，批量删除水印模板。

9.3.5.3 添加水印规则

系统支持从应用、URL、客户端IP、账号、账号组等维度配置水印规则，对访问行为进行精准鉴权与水印防护。您可在水印管理模块配置水印规则。

前提条件

- 确保您已添加应用，具体请参见[应用服务](#)。

- 已配置水印模板，具体请参见[配置水印模板](#)。

背景信息

如您想要对应用资产demo配置一条水印规则，代理访问demo应用时页面上出现网页水印，可参考以下步骤配置该水印规则。

操作步骤

- 步骤1** 使用系统管理员sysadmin账号[登录API数据安全防护系统web控制台](#)。
- 步骤2** 在左侧导航栏，选择“安全策略 > 水印管理”，单击“水印规则”页签。
- 步骤3** 单击“添加”，配置水印规则。如[图 添加水印规则](#)，参数说明请参考[表 添加水印规则](#)。

图 9-33 添加水印规则

The screenshot shows a web form titled '添加水印规则' (Add Watermark Rule). The form contains the following fields and controls:

- 规则名称:** A text input field containing the value '1'.
- 应用名称:** A dropdown menu with 'demo' selected.
- 优先级:** A text input field containing the value '100'.
- 水印模板:** A dropdown menu with '默认网页水印模板' (Default Web Watermark Template) selected.
- 规则条件:** A section with a '+ 添加' (Add) button.
- 启用状态:** A toggle switch that is currently turned on.
- Buttons:** '取消' (Cancel) and '确定' (Confirm) buttons at the bottom right.

表 9-17 添加水印规则

参数	说明
规则名称	填写自定义的水印规则名称。
应用名称	选择该规则适用的应用。
水印模板	选择水印模板。如何配置水印模板，请参见 配置水印模板 。
规则条件	配置该规则的规则条件，可配置项包括URL、客户端IP、账号、账号组等。
启用状态	开启和关闭水印规则。 <ul style="list-style-type: none"> • 开启状态：添加水印规则后直接生效。 • 关闭状态：配置完成后不生效，需要手动开启。

步骤4 单击“确定”完成水印规则配置。

步骤5 新增完成后，您可以在水印规则列表区域查看新添加的水印规则。代理访问应用资产 demo 时，将出现配置的网页水印。具体操作，请参见[查看水印结果](#)。

----结束

相关操作

后续您可以根据情况，在水印规则页面进行以下管理操作。

- 编辑水印规则：单击目标规则右侧的“编辑”，修改规则的相关信息。
- 删除水印模板：单击目标规则右侧的“删除”，删除水印规则。
- 批量删除水印规则：勾选目标规则，单击右上方的“批量操作 > 批量删除”，批量删除水印规则。

9.3.5.4 查看水印结果

配置水印规则后，代理访问应用，可查看水印结果。

背景信息

以所添加的应用 demo 为例，以下步骤说明如何验证所配置水印规则的效果。

操作步骤

步骤1 在浏览器中输入代理访问地址，即添加应用资产时所配置的应用域名/IP（例如 example.com），回车进行访问。

步骤2 在网页上直接查看网页水印效果。

不同类型水印效果不同，具体请参见[3.4.5.2 配置水印模板](#)中的说明。

图 9-34 文字水印效果



步骤3 如果配置了数据水印，以F12键打开浏览器开发者工具，选择网络（Network）模块，查看数据水印效果。

将添加数据水印的数据复制到水印溯源页面，可进行溯源定位，具体操作，请参见[执行水印溯源](#)。

图 9-35 启用无痕的数据水印效果



图 9-36 启用伪列的数据水印效果



---结束

9.3.5.5 执行水印溯源

当开启数据水印或点阵水印的数据资产未经授权而外泄时，可通过水印溯源功能，追溯外泄数据涉及的人员信息。

前提条件

在进行水印溯源之前，确保您已获取添加数据水印的外泄数据、添加文档暗水印的文档或点阵水印图形。如何对数据资产开启水印防护，请参见[添加水印规则](#)。

操作步骤

- 步骤1** 使用系统管理员sysadmin账号[登录API数据安全防护系统web控制台](#)。
- 步骤2** 在左侧导航栏，选择“安全策略 > 水印管理”，单击“溯源管理”页签。
- 步骤3** 如果溯源“数据水印”，请参考以下步骤：
 1. 在“溯源管理”页面选择“数据水印”。

2. 如果直接输入外泄数据进行水印溯源，将溯源内容复制到水印溯源页面对话框中，单击“溯源”。

图 9-37 复制溯源内容




图 9-38 粘贴到溯源对话框



说明

数据水印具有高透明性与高隐蔽性。如果您配置的水印为数据水印，则复制到对话框的溯源内容中将带有水印溯源ID，但水印溯源ID在对话框中不可见。

步骤4 如果溯源“文档暗水印”，请参考以下步骤：

1. 在溯源管理页面选择文档暗水印。
2. 单击  图标。
3. 在导入页面，单击“点击或将文件拖拽到这里上传”，从本地PC上传带有文档暗水印的文件，完成后单击“溯源”。

步骤5 如果溯源“点阵水印”，请参考以下步骤：

1. 在“溯源管理”页面选择“点阵水印”。
2. 根据所获取的点阵水印形状，从左至右、从上至下地按顺序单击矢量编码对照表中的点阵。

说明

点阵水印的9个点阵中，第一个是开始符，后面8个点阵对应不同的信息。矢量编码对照表单击完毕后，输入框中将产生8个字符的字符串。

3. 完成后，单击“溯源”。

步骤6 在“溯源结果”页面，查看溯源信息。

图 9-39 溯源结果

[返回](#)

溯源内容	请求时间	客户端IP/源客户端IP	账号/源账号	服务端IP/源应用IP	操作
1DCDFA9C	2024-02-21 11:06:31	172.16.194.36/172.16.194.36	-/-	172.16.194.36	详情

总共 1 条 < 1 > 15 条/页

步骤7 (可选) 在溯源结果页面, 单击“详情”, 查看溯源结果的详细信息。

----结束

9.3.6 日志中心

9.3.6.1 告警

对于识别到的风险访问行为, 将会梳理在告警页面, 您可查看与审阅告警日志, 并在告警页面配置策略。

9.3.6.1.1 查看告警信息

应用数据资产开启资产保护状态后, 对于风险访问会形成告警日志信息, 您可以通过查看告警日志及时发现应用数据资产的风险问题。

操作步骤

步骤1 使用系统管理员sysadmin账号[登录API数据安全防护系统web控制台](#)。

步骤2 在左侧导航栏, 选择“日志中心 > 告警”。

步骤3 在“告警”页面, 查看告警统计信息。如图[告警统计信息](#)。参数说明请参考表[告警统计信息](#)。

图 9-40 告警统计信息

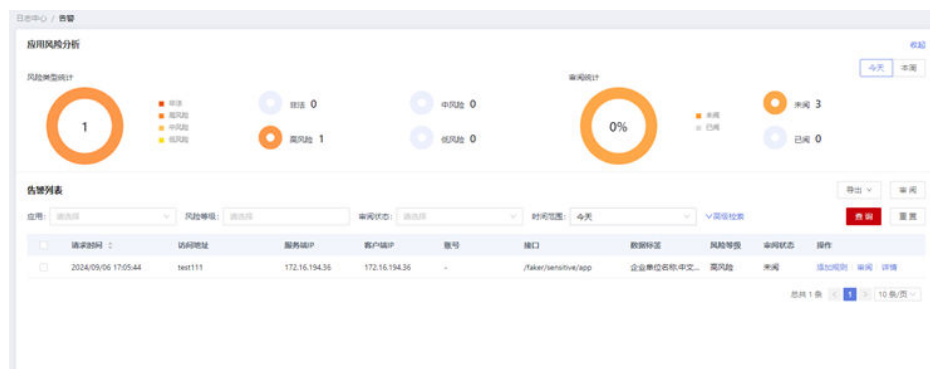


表 9-18 告警统计信息

区域	说明
风险类型统计	以环形图展示非法、高危、中危、低危四种风险等级的告警统计数值。

区域	说明
审阅统计	以环形图展示所已审阅和未审阅两种情况下的告警统计数。
检索条件	通过检索条件搜索对应的告警信息，支持默认检索条件和高级检索。
告警列表	告警日志的具体信息。

步骤4 （可选）在告警列表中，单击“详情”查看此条告警日志的详细信息。

步骤5 （可选）如果需要将告警日志信息下载到本地，单击“导出”，可以导出告警日志。

----结束

相关操作

您可以审阅确认告警信息，具体操作，请参见[审阅告警日志](#)。

如果存在告警信息不符合要求，您可以根据此告警配置审计与防护策略。具体操作，请参见[告警页面配置策略](#)。

9.3.6.1.2 审阅告警日志

管理员可在告警页面审阅系统产生的告警日志，识别数据资产的风险问题，以审阅的方式对告警日志进行标记。

背景信息

系统支持审阅单个告警日志和批量审阅多个告警日志。

操作步骤

步骤1 使用系统管理员sysadmin账号[登录API数据安全防护系统web控制台](#)。

步骤2 在左侧导航栏，选择“日志中心 > 告警”。

步骤3 如果需要审阅单个告警日志，请参考此步骤操作。

1. 在告警列表中，找到目标告警日志，单击“审阅”。
2. 在审阅对话框的审阅意见区域，填写审阅意见信息。

图 9-41 审阅告警日志

3. 在审阅规则区域，设置审阅规则。

📖 说明

设置审阅规则后，系统根据此规则同时审阅尚未完成审阅的同类事件日志。如果您选择多个审阅规则，则需要同时满足这些条件的日志才能被审阅。

4. 单击“提交”，完成审阅告警日志。

步骤4 如果需要“批量审阅”多个告警日志，请参考以下步骤操作。

1. 在告警列表中，选中多个告警日志。
2. 单击右上角的“审阅”。
3. 为多个告警日志同时填写审阅意见。
4. 单击“提交”，完成审阅告警日志。

----结束

9.3.6.1.3 告警页面配置策略

您可以针对告警信息，直接在告警页面配置审计与防护策略。如后续访问行为匹配此策略，则自动生效。

操作步骤

- 步骤1** 使用系统管理员sysadmin账号[登录API数据安全防护系统web控制台](#)。
- 步骤2** 在左侧导航栏，选择“日志中心 > 告警”。
- 步骤3** 找到目标告警，单击“添加规则”，在下拉栏中，选择策略类型，可选审计策略包括：“添加黑名单”、“添加白名单”。
- 步骤4** 在相应的策略类型页面，设置审计与防护策略。

- 白名单参数说明，请参见表 [白名单参数说明](#)。
- 黑名单参数说明，请参见表 [黑名单参数说明](#)。

---结束

操作结果

配置完成后，您可以在以下页面查看配置成功的策略：

- 如果配置的是白名单，请在左侧导航栏选择“安全策略 > 白名单”，在白名单页签中查看。
- 如果配置的是黑名单，请在左侧导航栏选择“安全策略 > 访问控制”，在黑名单页签中查看。

9.3.6.2 检索

检索页面记录了访问行为的审计日志，并按请求时间进行梳理。您可在检索页面检索并查看各类访问行为的审计日志，并配置相应的防护与审计策略。

9.3.6.2.1 查看审计日志信息

应用数据资产开启资产保护状态后，系统会对每个应用资产操作进行审计，您可以通过查看审计日志信息了解具体信息，方便应用数据资产管理和事后回溯。

操作步骤

步骤1 使用系统管理员sysadmin账号[登录API数据安全防护系统web控制台](#)。

步骤2 在左侧导航栏，选择“日志中心 > 检索”。

步骤3 在检索页面，查看审计日志列表。

图 9-42 审计日志统计信息

检索时间	日志类型	访问地址	服务器IP	客户端IP	账号	接口URL	风险等级	状态码	执行动作	操作
2024-09-06 17:33:29	登录访问	172.16.43.57:65000	172.16.43.41	172.16.194.35	-	/base/info1	无风险	200	放行	添加规则 详情
2024-09-06 17:33:29	业务访问	172.16.43.57:65000	172.16.43.41	172.16.194.35	-	/	无风险	302	放行	添加规则 详情
2024-09-06 17:33:29	业务访问	172.16.43.57:65000	172.16.43.41	172.16.194.35	-	/echo_page	无风险	200	放行	添加规则 详情
2024-09-06 17:33:29	业务访问	172.16.43.57:65000	172.16.43.41	172.16.194.35	-	/encode	无风险	200	放行	添加规则 详情
2024-09-06 17:33:28	业务访问	172.16.43.57:65000	172.16.43.41	172.16.194.35	-	/	无风险	302	放行	添加规则 详情
2024-09-06 17:33:28	登录访问	172.16.43.57:65000	172.16.43.41	172.16.194.35	-	/base/info1	无风险	200	放行	添加规则 详情
2024-09-06 17:33:28	业务访问	172.16.43.57:65000	172.16.43.41	172.16.194.35	-	/	无风险	302	放行	添加规则 详情
2024-09-06 17:33:27	业务访问	172.16.43.57:65000	172.16.43.41	172.16.194.35	-	/	无风险	302	放行	添加规则 详情

步骤4 （可选）在审计日志列表中，单击“详情”查看此条日志的详细信息。

步骤5 （可选）如果需要将审计日志信息下载到本地，单击“导出”，可以导出审计日志。

---结束

相关操作

如果存在不符合要求的审计日志，您可以根据此审计日志配置审计策略。具体操作，请参见[检索页面配置策略](#)。

9.3.6.2.2 检索页面配置策略

您可以针对审计日志信息，直接配置审计与防护策略。如果后续访问行为匹配此策略，则自动生效。

操作步骤

- 步骤1** 使用系统管理员sysadmin账号[登录API数据安全防护系统web控制台](#)。
- 步骤2** 在左侧导航栏，选择“日志中心 > 检索”。
- 步骤3** 找到目标告警，单击“添加规则”，在下拉栏中，选择策略类型，可选审计策略包括：“添加黑名单”、“添加白名单”。
- 步骤4** 在相应的策略类型页面，设置审计与防护策略。
 - 白名单参数说明，请参见[表 白名单参数说明](#)。
 - 黑名单参数说明，请参见[表 黑名单参数说明](#)。

---结束

操作结果

配置完成后，您可以在以下页面查看配置完成的策略：

- 如果配置的是白名单，请在左侧导航栏选择“安全策略 > 白名单”，在白名单页面中查看。
- 如果配置的是黑名单，请在左侧导航栏选择“安全策略 > 访问控制”，在黑名单页签中查看。

9.3.7 业务配置

9.3.7.1 添加敏感数据标签

操作场景

系统基于敏感数据标签来识别应用接口中的敏感数据，启用敏感数据标签后，如果系统识别到接口中包含敏感数据标签，将会将接口定义为敏感接口，并开启全文记录。

系统内置了数十种敏感数据标签，如果默认敏感数据标签类型不能满足业务需求，您可以通过正则表达式或关键字的方式添加自定义敏感数据标签类型。

本章节介绍如何添加敏感数据标签。

背景信息

正则表达式（Regular Expression）是一种字符串匹配的模式，可以用来检查一个串是否含有某种子串、将匹配的子串做替换或者从某个串中取出符合某个条件的子串等。

例如，您的应用接口中有一项数据为订单号，该订单号的表示形式通常为“DD+12位数字”（例如DD123456789123）。

操作步骤

- 步骤1** 使用系统管理员sysadmin账号[登录API数据安全防护系统web控制台](#)。
- 步骤2** 在左侧导航栏，选择“业务配置 > 敏感标签”。
- 步骤3** 在“敏感标签”列表页面，单击右上角的“添加”。
- 步骤4** 在“添加数据标签”对话框中，配置自定义的敏感数据标签。相关参数说明请参见[表 9-19](#)。

图 9-43 添加敏感数据标签

添加敏感标签 ✕

* 标签名称:

描述:

* 数据分类:

* 敏感等级:

* 识别位置:

* 规则类型:

* 指定KEY:

例外VALUE:

指定VALUE:

启用状态:

表 9-19 添加敏感数据标签参数说明

参数	说明
标签名称	设置自定义的敏感数据标签名称，方便后续管理。
标签描述	对自定义的敏感标签添加描述。
数据分类	选择敏感数据所属的类型。数据分类可手动配置，具体操作请参见 添加分类标签 。
敏感等级	选择敏感数据等级。数据分级可手动配置，具体操作请参见 添加分级标签 。
识别位置	选择敏感数据的识别位置。
规则类型	敏感数据识别的方式，可选正则、精确关键字、模糊关键字。
指定KEY	如果识别位置为KEY，在此处指定KEY关键字。
规则内容	<ul style="list-style-type: none"> 如果识别位置为“VALUE”，设置匹配自定义敏感数据的内容。 如果规则类型选择“正则”，则在此输入对应的正则表达式。 如果规则类型选择“精确关键字”或“模糊关键字”，则在此输入敏感数据的关键字。
例外VALUE	配置例外VALUE关键字，识别到例外VALUE时，不匹配该敏感标签。
指定VALUE	配置指定VALUE关键字，识别到指定VALUE时，匹配该敏感标签。
启用状态	选择是否启用敏感数据标签，  表示启用。

步骤5 单击“确定”，完成添加。

----结束

操作结果

新增完成后，您可以在敏感标签列表页面查看新增加的自定义敏感数据标签。新增的自定义敏感数据标签启用后，系统还不能自动识别到新添加的敏感数据标签，需要在接口中进行配置。

图 9-44 成功添加敏感数据标签



说明

添加自定义敏感数据标签后，若要在某一接口中识别到该敏感数据标签，必须将接口删除，重新识别接口后方可识别到该敏感数据。

相关操作

后续您可以根据情况，在“敏感数据标签库”列表页面进行以下管理操作。

- 编辑自定义的数据标签：单击“编辑”，修改自定义敏感数据标签的相关信息。

📖 说明

自定义敏感数据标签的识别机制为1000次之后重新识别，即敏感数据标签在首次识别后，如果修改标签内容，1000次内仍将识别为原标签内容。

- 删除自定义的数据标签：单击“删除”，删除不再使用的自定义敏感数据标签。

9.3.7.2 配置客户端 IP 解析参数

通过配置客户端IP解析规则，将对应识别位置的识别内容，解析成客户端IP。

操作步骤

步骤1 使用系统管理员sysadmin账号[登录API数据安全防护系统web控制台](#)。

步骤2 在左侧导航栏，选择“业务配置 > 配置解析”，单击“客户端IP解析”页签。

步骤3 单击右上角的“添加”，新增客户端IP解析规则。如[图 新增客户端IP解析规则](#)。详细参数说明请参考[表 新增客户端IP解析规则](#)。

图 9-45 新增客户端 IP 解析规则

表 9-20 新增客户端 IP 解析规则

参数	说明
应用名称	选择解析规则适用的应用资产。

参数	说明
识别内容	<ul style="list-style-type: none">输入识别的内容，在识别位置匹配到识别内容时，将会解析为客户端IP进行存储。支持输入多个，以英文逗号,隔开。
业务是否使用	<ul style="list-style-type: none">开启状态：IP识别到并在业务中使用。关闭状态：IP识别到后，规则校验仍用五元组里的IP。
是否开启	<ul style="list-style-type: none">开启状态：开启客户端IP解析规则。关闭状态：关闭客户端IP解析规则。

步骤4 单击“确定”完成配置。

----结束

操作结果

添加完成后，您可在列表中查看已配置的客户端IP解析规则。后续根据客户端IP解析规则解析IP。

相关操作

后续您可以根据情况，在客户端IP解析页面，对客户端IP解析规则进行删除、启用、禁用等管理操作。

9.3.7.3 证书管理

添加应用资产时，如果使用https协议，需要选择代理证书。代理证书需要在证书管理页面上上传。

如果本地已有证书，可直接在证书管理页面上上传API数据安全防护的证书。

背景信息

在添加代理应用时，如果应用协议选择为https模式，需选择已上传的证书。如何添加代理应用，请参见[添加代理应用](#)。

操作步骤

步骤1 使用系统管理员sysadmin账号[登录API数据安全防护系统web控制台](#)。

步骤2 在左侧导航栏，选择“业务配置 > 配置解析”，单击“证书管理”页签。

步骤3 在证书管理页面，单击“上传证书”。

步骤4 在“上传证书”对话框中，填写证书信息并从本地上传证书。

表 9-21 上传证书

参数	说明
证书名称	自定义证书名称。
证书描述	自定义证书的描述信息。
key文件上传	上传key格式证书。 单击确定上传后将根据MD5值进行重复性校验，如果上传相同证书（key文件和crt文件均相同）则会提示证书已存在且不进行保存。
crt文件上传	上传crt格式证书。 单击确定上传后将根据MD5值进行重复性校验，如果上传相同证书（key文件和crt文件均相同）则会提示证书已存在且不进行保存。

步骤5 填写完成后，单击“确定上传”。

----结束

操作结果

上传完成后，证书列表将展示已上传证书的证书名、有效期、上传时间、证书描述等信息。

相关操作

对于已上传的证书，您可进行下载、删除等管理操作。

9.3.7.4 添加分类标签

系统内置常见数据分类，如果需要自定义添加分类标签，可在“业务配置 > 分类分级”页面新增分类标签。

背景信息

新增的分类标签，可在配置敏感数据标签时引用。具体操作，请参见[添加敏感数据标签](#)。

操作步骤

步骤1 使用系统管理员sysadmin账号[登录API数据安全防护系统web控制台](#)。

步骤2 在左侧导航栏，选择“业务配置 > 分类分级”，单击“分类标签”页签。

步骤3 单击“添加”，在对话框中填写分类标签名称与描述信息。

步骤4 完成后，单击“确定”。

----结束

9.3.7.5 添加分级标签

系统内置常见数据分级，如果需要自定义添加分级标签，可在“业务配置 > 分类分级”页面新增分级标签。

背景信息

新增的分级标签，可在配置敏感数据标签时引用。具体操作，请参见[添加敏感数据标签](#)。

操作步骤

步骤1 使用系统管理员sysadmin账号[登录API数据安全防护系统web控制台](#)。

步骤2 在左侧导航栏，选择“业务配置 > 分类分级”，单击“分级标签”页签。

步骤3 单击添加，在对话框中填写分级标签名称、级别与描述信息。

步骤4 完成后，单击“确定”。

----结束

9.3.8 系统管理

9.3.8.1 新建账号

系统默认已经创建“系统管理员（sysadmin）”、“审计管理员（audadmin）”、“安全管理员（secadmin）”账号。如果有多个员工需要使用系统，建议您为每个员工单独创建账号，便于管理。

背景信息

账号的权限由角色决定，系统默认创建系统管理员、审计管理员和安全管理员角色，各角色权限说明，请参见[表 2 系统默认账号信息](#)。

例如，您需要为张三新建一个系统管理员的账号。以下步骤说明如何进行新建账号操作。

创建单个账号

步骤1 使用系统管理员sysadmin账号[登录API数据安全防护系统web控制台](#)。

步骤2 在左侧导航栏，选择“系统管理 > 账号管理”。

步骤3 如果需要创建单个账号（例如为张三创建账号zhangsan），请参见以下操作。

1. 单击右上角的“新建账号”。
2. 配置账号参数。

图 9-46 新建账号

新建账号
✕

* 账号:

* 密码:

* 确认密码:

使用人:

* 关联角色:

电话:

邮箱:

使用期限: 永久 定义期限

备注说明:

0 / 200

表 9-22 参数说明

参数	说明
账号	填写自定义账号名称。
密码/密码确认	填写账号登录密码。
使用人	填写该账号的使用人员。
角色	在下拉栏中选择角色。
电话	填写使用人员的联系电话。
邮箱	填写使用人员的联系邮箱。
使用期限	配置账号的有效期限。支持以下选项： <ul style="list-style-type: none"> - 永久：账号不会过期停用。 - 定义期限：选中后，设置时间期限，到期将停用账号。
备注说明	填写账号的描述信息。

3. 单击“提交审核”。

步骤4 如果需要批量创建多个账号，请参见以下操作。

1. 单击“导入”。
2. 在“导入账号信息”对话框中，单击“下载文件模板”，下载导入的模板文件。

图 9-47 导入账号



3. 在本地PC，根据模板文件示例填写账号信息。账号参数说明请参见[表9-22](#)。
4. 填写完成后，从本地PC选择文件上传。
5. 单击“导入测试”，校验格式是否正确。
6. 测试完成后，单击“确认导入”。

步骤5 在审核账号页面，审核账号。

创建完成后，账号处于未审核状态，还需要通过管理员审核账号。关于审核账号的更多信息，请参见[审核账号](#)。

----结束

操作结果

创建并审核完账号后，您可以使用新账号登录系统。

相关操作

- 修改账号信息：单击“编辑”，修改账号信息。
- 删除单个账号：单击“删除”，删除账号。
- 批量删除多个账号：选中账号后，单击“删除账号”，删除多个账号。

📖 说明

对于系统默认账号，仅支持编辑邮箱与电话。

9.3.8.2 语言切换

您可以在“系统管理 > 系统设置”页面系统支持切换语言设置。

操作步骤

- 步骤1 使用系统管理员sysadmin账号[登录API数据安全防护系统web控制台](#)。
- 步骤2 在左侧导航栏，选择“系统管理 > 系统设置”。
- 步骤3 单击“通用设置”页签的默认语言下拉框选择语言（可选中文或English）。

图 9-48 语言切换



----结束

9.3.8.3 修改告警设置

您可以通过告警设置，配置发送到消息通知告警的触发阈值、等级和频率。

操作步骤

- 步骤1 使用系统管理员sysadmin账号[登录API数据安全防护系统web控制台](#)。
- 步骤2 在左侧导航栏，选择“系统管理 > 系统设置”。
- 步骤3 单击“告警设置”页签。
- 步骤4 单击要修改告警的“编辑”，在对话框修改告警的阈值、等级和频率。
- 步骤5 单击“保存”。

----结束

9.3.8.4 查看设备状态

您可以通过查看设备状态，查看系统的资源使用情况，方便排查问题。

操作步骤

- 步骤1 使用系统管理员sysadmin账号[登录API数据安全防护系统web控制台](#)。

步骤2 在左侧导航栏，选择“系统管理 > 系统运维”。

步骤3 单击“系统监控”页签。

步骤4 查看CPU使用率、内存使用率和硬盘使用情况等设备实时状态信息。

图 9-49 设备状态



表 9-23 参数说明

参数	说明
系统概况	展示系统实时的CPU使用率与内存使用率。
CPU使用率	展示最近15分钟系统CPU使用率的变化情况。
内存使用率	展示最近15分钟系统内存使用率的变化情况。
吞吐量	展示最近15分钟系统网卡的吞吐量变化情况。
磁盘使用情况	展示各文件系统与挂载点的使用情况。

----结束

9.3.8.5 重启服务或设备

9.3.8.5.1 重启服务

注意

重启服务影响API数据安全防护各业务功能的运行，重启期间API数据安全防护各业务功能不可用，建议在业务运行低谷时执行此操作。

操作步骤

步骤1 使用系统管理员sysadmin账号[登录API数据安全防护系统web控制台](#)。

步骤2 在左侧导航栏，选择“系统管理 > 系统运维”。

步骤3 单击“系统监控”页签。

步骤4 在设备管理页面，单击右上角的“重启服务”。

步骤5 在确认提示框中，单击“确认”。

----结束

9.3.8.5.2 重启设备

注意

重启设备影响API数据安全防护各业务功能的运行，重启期间API数据安全防护各业务功能不可用，建议在业务运行低谷时执行此操作。

操作步骤

步骤1 使用系统管理员sysadmin账号[登录API数据安全防护系统web控制台](#)。

步骤2 在左侧导航栏，选择“系统管理 > 系统运维”。

步骤3 单击“系统监控”页签。

步骤4 在设备管理页面，单击右上角的“重启设备”。

步骤5 在确认提示框中，单击“确认”。

操作完成后，将重启设备，重启过程中业务功能将中断。

----结束

9.3.8.5.3 关闭设备

注意

关闭设备后，API数据安全防护各业务功能将不可用，建议只在必要情况下执行此操作。

操作步骤

步骤1 使用系统管理员sysadmin账号[登录API数据安全防护系统web控制台](#)。

步骤2 在左侧导航栏，选择“系统管理 > 系统运维”。

步骤3 单击“系统监控”页签。

步骤4 在设备管理页面，单击右上角的“关闭设备”。

步骤5 在确认提示框中，单击“确认”。

----结束

9.3.8.6 系统实时诊断

安全管理员可在系统诊断页面实时诊断系统的内核、CPU与内存、磁盘、网卡和端口等信息，用于辅助排查系统问题。

操作步骤

步骤1 使用系统管理员sysadmin账号[登录API数据安全防护系统web控制台](#)。

步骤2 在左侧导航栏，选择“系统管理 > 系统运维”。

步骤3 单击“系统诊断”页签。

步骤4 在“实时诊断”下拉框中，选择诊断项目，单击“执行”。

图 9-50 实时诊断

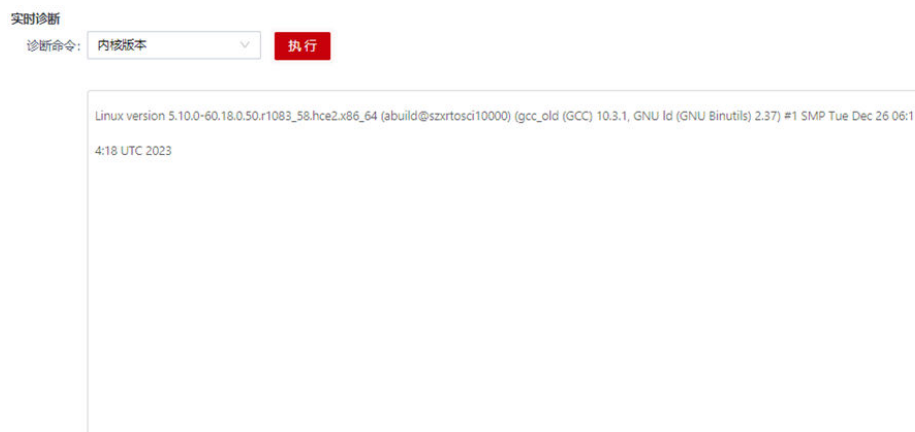


表 9-24 参数说明

诊断项目	说明
内核	查询服务器内核信息。
CPU & MEM	查询服务器CPU和内存资源使用情况，以及进程信息。
磁盘	查询服务器硬盘使用情况。
网卡	查询服务器网卡信息。
磁盘IO	查询服务器硬盘IO情况。
PING	查询服务器连通情况，需要输入服务器IP地址。
NETSTAT	查询显示网络连接、路由表和网络接口信息。

----结束

相关操作

进行实施诊断后，您可以单击调试日志下载，下载调试日志。

9.3.8.7 升级系统

系统管理员可在系统升级页面，通过上传升级包，将系统版本更新到指定版本。

双机高可用场景下升级时，需先进入“系统管理 > 高可用管理”页面关闭数据同步按钮，然后停止备机B的高可用（若为双主模式则关闭一台主机的高可用），先对设备B进行升级，升级成功后，开启设备B的高可用，停止设备A的高可用，对设备A进行升级，升级完成后，开启设备A的高可用，再开启数据同步，此步骤可保障双机 HA 升级时业务影响最低。

⚠ 注意

升级系统会影响业务运行，请选择业务低谷时间升级系统软件。

前提条件

已经从技术支持工程师处获取系统升级包。

操作步骤

- 步骤1** 使用系统管理员sysadmin账号[登录API数据安全防护系统web控制台](#)。
- 步骤2** 在左侧导航栏，选择“系统管理 > 系统运维”。
- 步骤3** 单击“系统升级”页签。
- 步骤4** 单击“上传升级脚本”。
- 步骤5** 在“版本变更”对话框中，将升级包拖拽到升级区域。

图 9-51 上传升级包



- 步骤6** 上传完毕后，单击“升级”。

步骤7 在确认提示框中，单击“确定”，开始升级。

完成后，您可以在版本变更历史区域，查看软件的升级结果等信息。

----结束

9.3.8.8 网络管理

9.3.8.8.1 启用 bypass

当API数据安全防护出现组件错误时，可启用一键bypass功能，在不影响业务的前提下排查系统问题。进入bypass状态后，仅保留API数据安全防护基本的代理功能和流量控制功能。

操作步骤

步骤1 使用系统管理员sysadmin账号[登录API数据安全防护系统web控制台](#)。

步骤2 在左侧导航栏，选择“系统管理 > 网络管理”。

步骤3 在“应急逃生”区域，按需启用bypass开关

bypass状态：启动后，系统主动进入bypass状态，保留代理访问功能，而所有策略将自动失效，直至手动关闭。

图 9-52 直接启用



----结束

相关操作

如果系统进入bypass状态，可远程连接服务器，进入`/usr/setup/appgateway/merry/core_files`路径，查看`core_dump`文件，排查系统问题。

9.3.8.8.2 配置网卡与路由信息

您可在系统管理模块配置网卡、路由与DNS信息，或是一键启用bypss状态，便于排查系统问题。

通过配置网络地址，修改API数据安全防护的设备IP、DNS与路由等信息。

📖 说明

若要修改网卡IP，必须通过该页面配置，不能直接在后台通过修改网卡配置文件的方式修改，否则会导致ssh服务（22端口）的IP绑定错误。

前提条件

已经获取设备需要配置的IP地址、DNS与路由等信息。

操作步骤

步骤1 使用系统管理员sysadmin账号[登录API数据安全防护系统web控制台](#)。

步骤2 在左侧导航栏，选择“系统管理 > 网络管理”。

步骤3 在网卡列表页面，找到对应网口，单击“编辑”。

图 9-53 配置网络地址



步骤4 在“编辑”对话框中，设置网卡信息，完成后单击“确定”。

表 9-25 配置网络地址参数

参数	说明
网口名称	<ul style="list-style-type: none"> 显示网卡名称。 默认网卡名，无法修改。
网口类型	在下拉栏中，选择网卡用途。可选类型包括业务口和管理口。
网口描述	添加网口的描述信息。
地址类型	在下拉栏中，选择地址类型。可选类型包括不配置地址、IPv4、IPv6、IPv4&IPv6 <ul style="list-style-type: none"> IPv4：需要配置IPv4地址、子网掩码、网关和DNS IPv6：需要配置IPv6地址、子网掩码、网关和DNS IPv4&IPv6：需要配置IPv4和IPv6的IP地址、子网掩码、网关和DNS

步骤5 单击“设置DNS”，设置主域名系统与备用域名系统信息，完成后单击“确定”。

说明

如果存在配置域名的资产，必须设置DNS服务器地址。

步骤6 如果需要修改路由信息，在路由列表页面，单击“添加路由”，配置路由信息，完成后单击“确定”。

表 9-26 路由参数说明

参数	说明
目标地址	设置目标地址。
子网掩码	设置子网掩码。根据网络规划决定。
下一跳地址	设置路由器的下一跳地址。
接口	选择路由器接口。 选择接口：从下拉框中手动选择可用接口。

----结束

9.3.8.9 查看高可用信息

若系统采用高可用部署，您可以在“系统管理 > 高可用管理”页面查看高可用信息，包括主备机IP与VIP、主备机的运行时间以及各项指标的状态。

📖 说明

双机高可用场景下升级时，需先进入“系统管理 > 高可用管理”页面关闭数据同步按钮，然后停止备机B的高可用（若为双主模式则关闭一台主机的高可用），先对设备B进行升级，升级成功后，开启设备B的高可用，停止设备A的高可用，对设备A进行升级，升级完成后，开启设备A的高可用，再开启数据同步，此步骤可保障双机 HA 升级时业务影响最低。

9.3.8.10 备份恢复

9.3.8.10.1 备份审计日志和配置数据

系统支持备份审计日志与配置文件（包括资产配置、策略配置、用户配置等），在遇到问题或误操作时，可以恢复审计日志或配置信息。

操作步骤

步骤1 使用系统管理员sysadmin账号[登录API数据安全防护系统web控制台](#)。

步骤2 在左侧导航栏，选择“系统管理 > 备份恢复”。

步骤3 单击“数据备份”页签。

步骤4 如果进行单次备份，请参照以下步骤：

1. 在手动备份区域，单击“手动备份”。
2. 在“手动备份”对话框中，配置“备份类型”（可选审计日志或配置文件）、“备份位置”与“备份范围”。

图 9-54 手动备份

手动备份

* 备份类型: 审计日志

* 备份位置: 本地

备份范围: 2024-08-01 00:00:00 ~ 2024-08-28 00:00:00


取消 确认

表 9-27 备份位置说明


备份位置	说明
本地	将备份信息直接保存在服务器，在备份列表中单击下载可直接下载到本地。

3. 单击“确认”。

步骤5 如果进行“自动备份审计日志”，请参照以下步骤：

1. 单击审计日志自动备份区域的“设置”，设置备份位置与备份周期。单击“确认”。
2. 开启审计日志自动备份后的  按钮，启用审计日志自动备份。

步骤6 如果进行“自动备份配置数据”，请参照以下步骤：

1. 单击配置数据自动备份区域的“设置”，设置备份位置与备份周期。单击“确认”。
2. 开启配置数据自动备份后的  按钮，启用配置数据自动备份。

---结束

操作结果

每次备份完成后，在审计日志备份列表中将能查看到已备份日志的信息，可单击“下载”将备份文件下载到本地。

相关操作

如果您需要删除备份文件，单击备份文件右侧的“删除”。

9.3.8.10.2 恢复审计日志和配置数据

您可以在“系统管理 > 备份恢复”页面上传备份文件，恢复系统的审计日志和配置数据。

恢复审计日志

- 步骤1** 使用系统管理员sysadmin账号[登录API数据安全防护系统web控制台](#)。
- 步骤2** 在左侧导航栏，选择“系统管理 > 备份恢复”。
- 步骤3** 单击“备份恢复”页签。
- 步骤4** 单击右上角的“文件导入”。
- 步骤5** 在文件导入对话框中，设置导入的备份文件类型和文件位置信息。

图 9-55 日志备份恢复



表 9-28 文件位置说明

备份位置	说明
本地	从本地上传备份文件进行恢复。

步骤6 单击“确认”。

上传的备份文件出现在“备份恢复列表”中。

步骤7 单击右侧的“恢复”。

----结束

恢复配置数据

步骤1 使用系统管理员sysadmin账号[登录API数据安全防护系统web控制台](#)。

步骤2 在左侧导航栏，选择“系统管理 > 备份恢复”。

步骤3 单击“备份恢复”页签。

步骤4 单击右上角的“文件导入”。

步骤5 在文件导入对话框中，设置导入的备份文件类型和文件位置信息。

图 9-56 配置备份本地恢复

The screenshot shows a '文件导入' (File Import) dialog box with a close button (X) in the top right corner. It contains the following elements:

- A dropdown menu for '备份类型' (Backup Type) set to '配置数据' (Configuration Data).
- Radio buttons for '导入方式' (Import Method): '文件上传' (File Upload) is selected, and 'OBS下载' (OBS Download) is unselected.
- A '文件上传' (File Upload) section with a cloud upload icon and the text: '点击或将文件拖拽到这里上传' (Click or drag files here to upload) and '仅支持.tar.gz/.zip文件格式' (Only supports .tar.gz/.zip file formats).
- Buttons for '取消' (Cancel) and '确认' (Confirm) at the bottom right.

图 9-57 配置备份 OBS 恢复

The screenshot shows a '文件导入' (File Import) dialog box with a close button (X) in the top right corner. It contains the following elements:

- A dropdown menu for '备份类型' (Backup Type) set to '配置数据' (Configuration Data).
- Radio buttons for '导入方式' (Import Method): 'OBS下载' (OBS Download) is selected, and '文件上传' (File Upload) is unselected.
- Input fields for 'OBS服务地址' (OBS Service Address) containing 'obs-...com', 'OBS桶名' (OBS Bucket Name) containing 'obs-...', and '文件路径' (File Path) containing 'adg/...tar.gz'.
- Buttons for '取消' (Cancel) and '确认' (Confirm) at the bottom right.

表 9-29 文件位置说明

备份位置	说明
本地	从本地上传备份文件进行恢复。
OBS下载	输入OBS服务地址、OBS桶和备份文件路径，远程下载备份文件（实例中已配置ak和sk），dsc下发OBS备份配置和aksk配置。

步骤6 单击“确认”。

上传的配置备份文件出现在“备份恢复列表”中。

步骤7 单击右侧的“恢复”。

----结束

9.3.8.11 消息通知

在消息通知，您可以查看系统的通知公告等消息，配置推送的消息类型、消息模板和接收角色等。

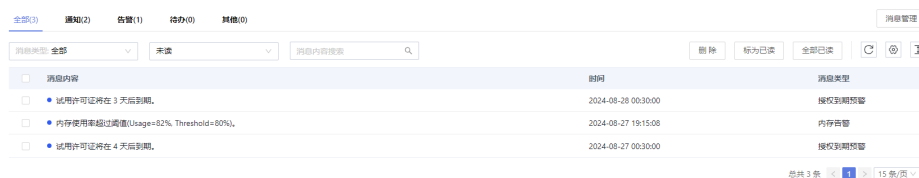
操作步骤

步骤1 使用系统管理员sysadmin账号[登录API数据安全防护系统web控制台](#)。

步骤2 在左侧导航栏，选择“系统管理 > 消息通知”。

步骤3 在全部、通知、告警、待办和其他等页签，查看最近的通知告警等信息。

图 9-58 消息通知



----结束

9.3.8.12 数据清理

9.3.8.12.1 自动清理业务数据

操作步骤

步骤1 使用系统管理员sysadmin账号[登录API数据安全防护系统web控制台](#)。

步骤2 在左侧导航栏，选择“系统管理 > 数据清理”。

步骤3 在业务数据清理区域，单击自动清理后的“设置”，设置业务数据自动清理参数。

图 9-59 设置参数



表 9-30 参数说明

参数	说明
业务数据超时时间	设置自动清理超时的业务数据。
数据磁盘空间最大阈值	设置数据磁盘空间的最大阈值。业务数据所在挂载点的磁盘空间使用率超过阈值时，开始告警并自动清理数据。
数据磁盘空间最小阈值	设置数据磁盘空间的最小阈值。业务数据所在挂载点的磁盘空间使用率小于阈值时，停止清理数据。

说明

超时时间清理和根据存储阈值清理为并列关系，任意符合一个都可以进行自动清理数据。

步骤4 单击“确定”。

步骤5 单击 ，开启自动清理开关。

----结束

9.3.8.12.2 手动清理业务数据

操作步骤

步骤1 使用系统管理员sysadmin账号[登录API数据安全防护系统web控制台](#)。

步骤2 在左侧导航栏，选择“系统管理 > 数据清理”。

步骤3 在业务数据清理区域，单击“手动清理”，设置清理策略。

图 9-60 设置参数



步骤4 单击“立即清理”。

----结束

9.3.8.12.3 清理系统运行日志

您可以配置日志文件清理，自动清理过期的系统运行日志。

操作步骤

- 步骤1** 使用系统管理员sysadmin账号[登录API数据安全防护系统web控制台](#)。
- 步骤2** 在左侧导航栏，选择“系统管理 > 数据清理”。
- 步骤3** 在日志文件清理区域，单击自动清理后的“设置”，设置系统运行日志自动清理参数。

图 9-61 设置参数



表 9-31 参数说明

参数	说明
数据磁盘空间最大存储量	设置数据磁盘空间的最大存储量。系统日志所在挂载点的磁盘空间存储量超过阈值时，开始告警并自动清理数据。

- 步骤4** 单击“确定”。
- 步骤5** 单击 ，开启自动清理开关。

----结束

9.3.8.12.4 查看清理记录

系统将记录数据清理信息，您可根据需要查看清理记录。

操作步骤

- 步骤1** 使用系统管理员sysadmin账号[登录API数据安全防护系统web控制台](#)。
- 步骤2** 在左侧导航栏，选择“系统管理 > 数据清理”。
- 步骤3** 单击“清理记录”页签。
- 步骤4** 在列表中查看具体的清理记录，包括每次清理的结束时间、清理内容、清理范围以及清理方式信息。

图 9-62 清理记录



时间	清理内容	清理范围	清理方式
2024-08-28 16:15:46	审计日志	基于2024-08-22的数据	手动清理

----结束

9.4 安全管理员操作指南

9.4.1 系统管理

9.4.2 用户管理

9.4.2.1 审核账号

创建账号后，需要安全管理员审核通过后，才能够正常使用。系统支持手动审核和自动审核两种方式。

9.4.2.1.1 手动审核账号

前提条件

在此之前，确保您已经创建新的用户账号，具体操作请参见[新建账号](#)。

操作步骤


- 步骤1** 使用安全管理员secadmin账号[登录API数据安全防护系统web控制台](#)。
- 步骤2** 在左侧导航栏，选择“系统管理 > 账号审核”。
- 步骤3** 单击“待审核”页签。
- 步骤4** 勾选需要审核的账号，单击“通过”。
- 步骤5** 在确认提示框中，单击“确定”。

----结束

9.4.2.1.2 启用自动审核

开启自动审核后，创建新账号无需再进行手动审核，账号直接生效。

操作步骤

- 步骤1** 使用安全管理员secadmin账号[登录API数据安全防护系统web控制台](#)。
- 步骤2** 在左侧导航栏，选择“系统管理 > 账号审核”。
- 步骤3** 开启右上角自动审核的  图标。

步骤4 在确认提示框中，单击“确定”。

您可单击已审核页签，查看已审核的账号信息与审核状态。

----结束

9.4.2.2 查看角色

系统默认创建系统管理员、审计管理员和安全管理员等角色，各角色拥有系统的不同权限。

操作步骤

步骤1 使用安全管理员secadmin账号[登录API数据安全防护系统web控制台](#)。

步骤2 在左侧导航栏，选择“系统管理 > 角色管理”。

步骤3 查看系统默认创建的角色信息。

表 9-32 系统默认账号

出厂默认账号	账号类型	说明
sysadmin	系统管理员	主要负责系统的日常运行维护。
secadmin	安全管理员	主要负责系统的日常安全保密管理工作，包括系统用户权限的授予与撤销，平台登录、账号密码和网络访问的安全配置等。
audadmin	审计管理员	主要负责对系统管理员和安全管理员的操作行为进行审计跟踪、分析和监督检查。

----结束

9.4.3 系统运维

9.4.3.1 启用安全配置

9.4.3.1.1 设置平台登录安全

操作步骤

步骤1 使用安全管理员secadmin账号[登录API数据安全防护系统web控制台](#)。

步骤2 在左侧导航栏，选择“系统管理 > 系统设置”，并单击“安全设置”页签。

步骤3 在平台登录安全设置区域，设置平台登录的安全性。

图 9-63 平台登录安全设置



表 9-33 参数说明

参数	说明
动态验证码	选择登录时是否启用动态验证码。 启用后，系统登录时，输入正确的动态验证码是必要条件之一，可以防暴力破解密码。
空闲超时登出	设置账号超时自动退出时间。
多端登录	选择同一账号是否可以在多个合法IP同时登录。如果不允许多端登录，账号在新IP登录时，原IP会被登出。
登录安全策略	选择是否启用登录安全策略，防止账号被暴力破解。

----结束

9.4.3.1.2 设置账号密码安全

操作步骤

- 步骤1 使用安全管理员secadmin账号[登录API数据安全防护系统web控制台](#)。
- 步骤2 在左侧导航栏，选择“系统管理 > 系统设置”，并单击“安全设置”页签。
- 步骤3 在账号密码安全设置区域，设置密码安全要求。

图 9-64 账号密码安全设置



表 9-34 参数说明

参数	说明
初次登录强制更改密码	设置是否开启初次登录强制更改密码功能。默认开启，增加账号安全性。
密码长度要求	设置密码最少长度。
密码复杂度要求	配置密码必须包含哪些字符。
密码有效期	设置密码有效时间。

----结束

9.4.3.1.3 设置网络访问安全

操作步骤

- 步骤1** 使用安全管理员secadmin账号[登录API数据安全防护系统web控制台](#)。
- 步骤2** 在左侧导航栏，选择“系统管理 > 系统设置”，并单击“安全设置”页签。
- 步骤3** 在网络访问安全设置区域，设置访问安全要求。

图 9-65 网络访问安全设置

网络访问安全设置

登录IP限制: 接受所有IP 限制IP

网络权限配置: 禁止ICMP探测 禁止SSH登录

表 9-35 参数说明

参数	说明
登录IP限制	<p>可选项包括接受所有IP与限制IP。</p> <ul style="list-style-type: none"> 接受所有IP：所有IP均可登录系统。 限制IP：需要设置允许登录IP地址，允许登录IP 地址内的可以登录系统，其他IP不可以登录。
网络权限配置	<p>设置是否禁止ICMP探测和禁止SSH登录。</p> <ul style="list-style-type: none"> 启用禁止ICMP探测：关闭ICMP功能，则其他设备无法ping系统。 启用禁止SSH登录：禁止使用SSH命令登录服务器。

----结束

9.4.3.2 消息通知

在消息通知，您可以查看系统的通知公告等消息。

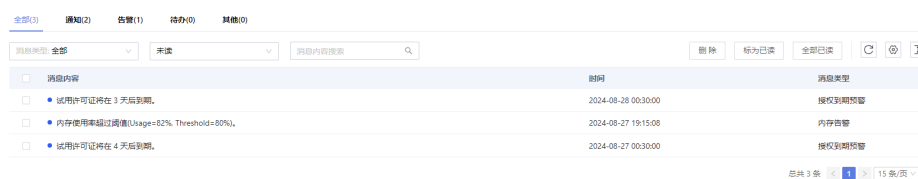
操作步骤

步骤1 使用安全管理员secadmin账号[登录API数据安全防护系统web控制台](#)。

步骤2 在左侧导航栏，选择“系统管理 > 消息通知”。

步骤3 在全部、通知、告警、待办和其他等页签，查看最近的通知告警等信息。

图 9-66 消息通知



----结束

9.5 审计管理员操作指南

9.5.1 查看操作日志

系统会保存所有的操作记录，审计管理员可以定期检查操作审计日志，保障系统自身安全。

操作步骤

步骤1 使用审计管理员audadmin账号[登录API数据安全防护系统web控制台](#)。

步骤2 在左侧导航栏，选择“日志管理 > 操作日志”。

步骤3 设置过滤条件，单击🔍图标，查询对应的操作日志。

图 9-67 过滤条件



表 9-36 参数说明

查询条件	说明
时间范围	设置查询的开始时间和结束时间。
操作账号/IP/内容等	输入操作账号/访问来源IP/内容等关键字，支持模糊匹配。

----结束

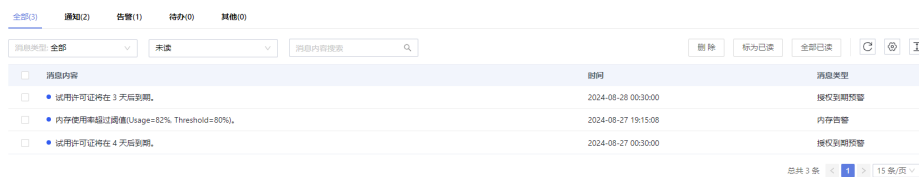
9.5.2 消息通知

在消息通知，您可以查看系统的通知公告等消息。

操作步骤

- 步骤1** 使用审计管理员audadmin账号[登录API数据安全防护系统web控制台](#)。
- 步骤2** 在左侧导航栏，选择“系统管理 > 消息通知”。
- 步骤3** 在全部、通知、告警、待办和其他等页签，查看最近的通知告警等信息。

图 9-68 消息通知



----结束

10 数据安全运营

10.1 态势大屏

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

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


前提条件

- 已完成云资产委托授权，参考[云资产委托授权/停止授权](#)进行操作。
- 已开通DBSS服务，详情请参见[购买数据库安全审计](#)。

操作步骤

步骤1 [登录管理控制台](#)。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全与合规 > 数据安全中心”。

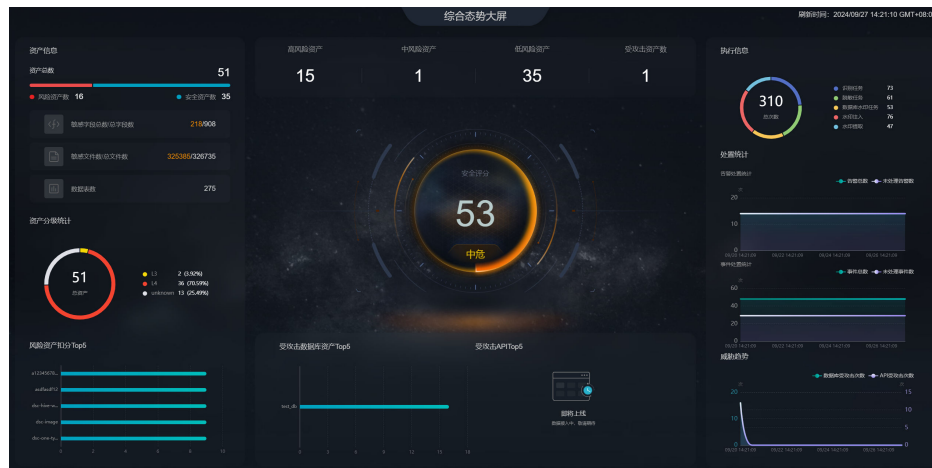
步骤4 在左侧导航树中，选择“数据安全运营 > 态势大屏”，进入“态势大屏”界面。

图 10-1 态势大屏



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

图 10-2 综合态势大屏



----结束

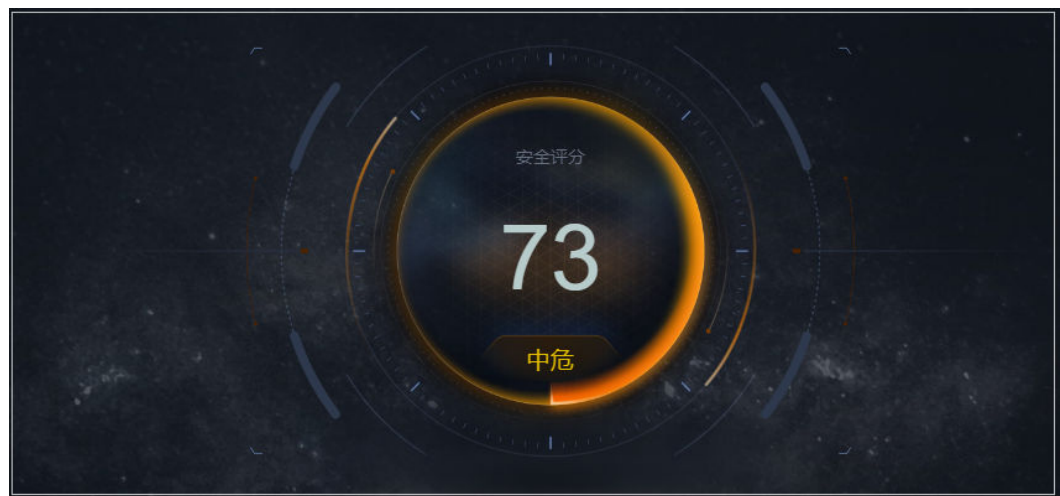
安全评分

如图10-3所示，展示当前全部资产的安全健康得分。

表 10-1 安全评分

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

图 10-3 安全评分



风险资产统计情况

如[图10-4](#)所示，展示已授权资产的风险统计情况。

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

表 10-2 安全评分

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

图 10-4 风险资产统计情况



资产信息

如图10-5所示，展示资产总数以及高中风险资产总和资产数据识别情况。

表 10-3 资产信息

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

图 10-5 资产信息



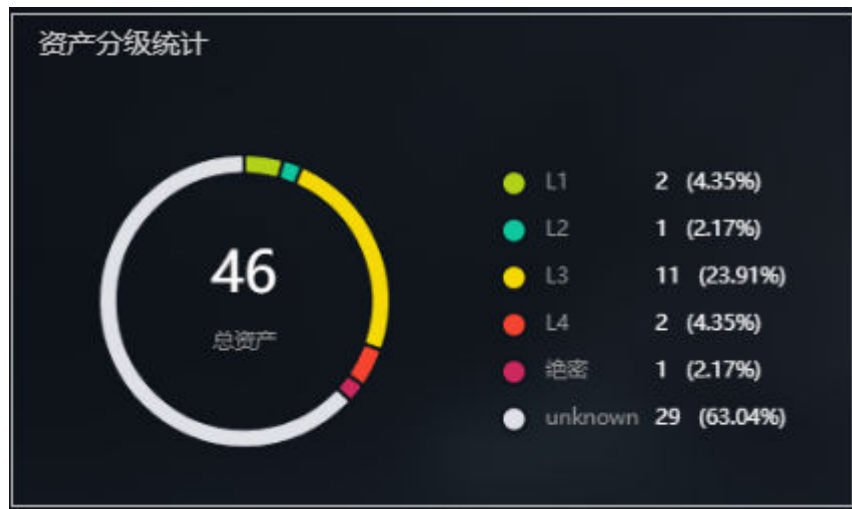
资产分级统计

如图10-6所示，展示经过敏感数据识别进行分类分级的资产总数以及各级别下的资产数量和占比。

表 10-4 资产信息

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

图 10-6 资产分级统计



风险资产扣分 Top5

如图10-7所示，展示风险扣分Top5资产，鼠标移动至柱状图显示“资产名称”、“资产类型”、“数据源”以及“风险扣分”。

表 10-5 资产信息

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

图 10-7 风险资产扣分 Top5



执行信息

如图10-8所示，展示敏感数据识别、数据静态脱敏、数据水印执行任务的总和及各功能的执行任务数量。

表 10-6 执行信息

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

图 10-8 执行信息



处置统计

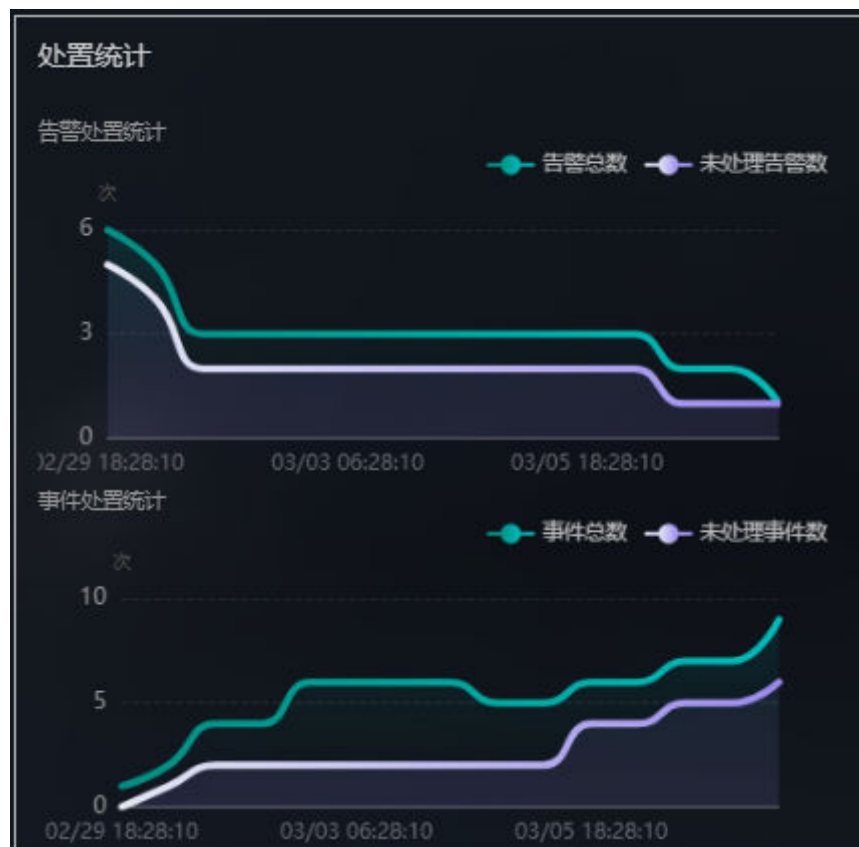
- 告警处置统计
按时间展示来自“告警管理”功能的“告警总数”和“未处理告警数”。
- 事件处置统计

按时间展示来自“事件管理”功能的“事件总数”和“未处理事件数”。

表 10-7 执行信息

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

图 10-9 处置统计



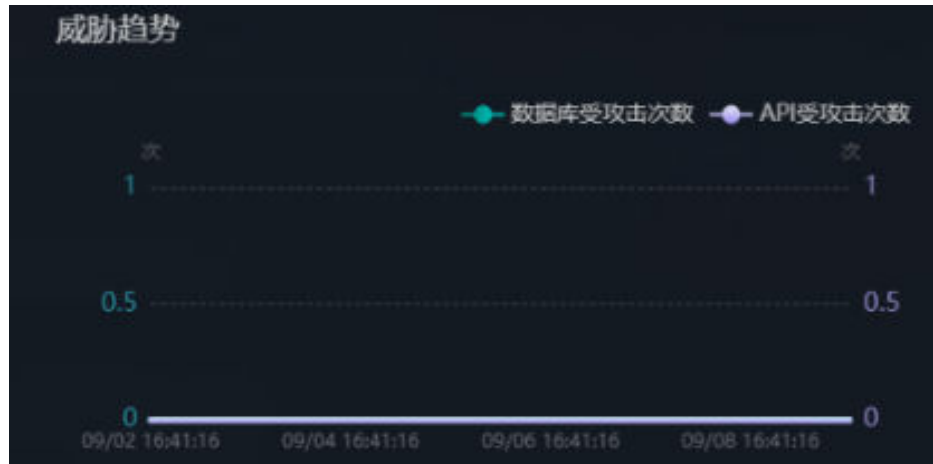
威胁趋势

如图10-10所示，按时间展示数据库受攻击次数。

表 10-8 执行信息

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

图 10-10 威胁趋势



受攻击 Top5

表 10-9 受攻击 Top5

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

受攻击数据库资产 Top5

如图 10-11 所示，展示受攻击的 Top5 数据库资产，鼠标移动至柱状图显示“数据库名称”、“数据库类型”以及“受攻击次数”。

图 10-11 受攻击数据库资产 Top5



10.2 数据流转详情

全链路的云上数据流转监测，包括以下几个阶段：


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

在[流转日志采集](#)开启对实例的数据流转日志采集，DSC会对采集上报的日志进行数据链路流转分析，并绘制流转图。对采集到的日志数据进行各种指标运算，将运算结果保存起来。

查看数据流转分析

步骤1 [登录管理控制台](#)。

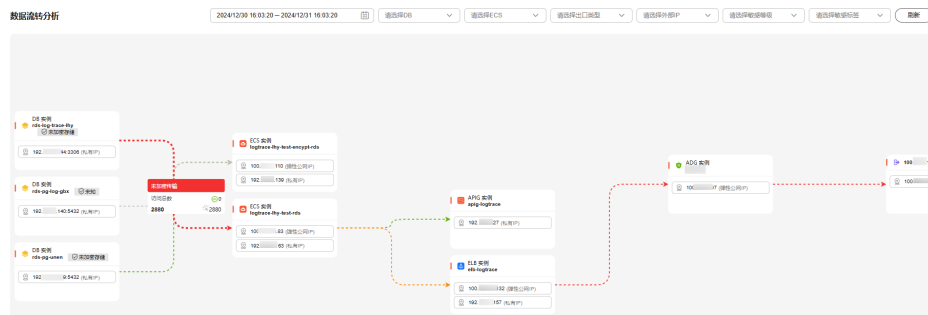
步骤2 单击左上角的 ，选择区域或项目。

步骤3 在左侧导航树中，单击 ，选择“安全与合规 > 数据安全中心”。

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

鼠标移动至流转通道上显示数据是否加密传输以及访问总数等，红色箭头代表未加密传输，绿色箭头表示全部加密传输，黄色箭头表示部分加密传输，连线加密状态均代表当前的加密状态。

图 10-12 数据流转分析



步骤5 选择时间：单击选择需要查看的时间段。

选择DB：选择需要查看的数据库。

选择ECS：单击下拉框选择访问数据的ECS。

选择出口类型：单击下拉框选择ELB或者APIG。

选择外部IP：单击下拉框选择外部IP。

选择敏感等级：单击下拉框选择敏感等级。

选择敏感标签：单击下拉框选择敏感标签。

----结束

10.3 事件管理

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

前提条件

已开通DBSS服务，且DBSS中已有资产，详情请参见[购买数据库安全审计](#)。

新建事件

步骤1 [登录管理控制台](#)。

步骤2 单击左上角的📍，选择区域或项目。

步骤3 在左侧导航树中，单击☰，选择“安全与合规 > 数据安全中心”。

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

步骤5 左上角单击“新建”，进入新建事件界面。

步骤6 根据[表10-10](#)配置新建事件相关参数。

表 10-10 新建事件参数

参数	说明
事件名称	输入字符长度只能为4-255个字符，仅允许输入中英文、数字、‘-’、‘_’，并且开头需为中文或者字母。
类型	单击下拉框选择事件类型： <ul style="list-style-type: none"> ● 数据库 <ul style="list-style-type: none"> - SQL注入 - 风险操作 ● 应用API <ul style="list-style-type: none"> - 非法访问 - 登录安全 - 接口安全 - 业务安全 - 数据安全
事件等级	单击下拉框选择事件等级： <ul style="list-style-type: none"> ● 提示 ● 低危 ● 中危 ● 高危 ● 致命
状态	单击下拉框选择状态： <ul style="list-style-type: none"> ● 开启 ● 阻塞 ● 关闭
来源功能模块	单击下拉框选择来源功能模块： <ul style="list-style-type: none"> ● 数据库审计 ● 云堡垒机 ● 数据库加密网关 ● 数据库运维 ● API安全网关
来源实例	单击下拉框选择对应的事件来源实例。
责任人	单击下拉框选择对应事件处理责任人。
影响资产（可选）	填写该事件影响资产的信息。
发生时间	事件首次发生时间。
计划关闭时间	事件计划关闭时间。
推荐处理方法（可选）	输入推荐事件处理方法，输入不超过1000个字符。

参数	说明
验证状态	单击下拉框选择事件验证状态： <ul style="list-style-type: none"> 未知 确认 误报
描述（可选）	输入事件描述。


步骤7 单击“确定”。

----结束

查看事件管理列表

步骤1 [登录管理控制台](#)。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全与合规 > 数据安全中心”。

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

步骤5 查看“未处理事件”和“事件总量”。

环状图展示“已超期”和“未超期”的事件数量。

图 10-13 事件处理情况



步骤6 查看告警列表，参数如[表10-11](#)所示。

表 10-11 数据风险事件参数列表

参数名称	参数说明
事件名称/ID	<ul style="list-style-type: none"> 事件的名称。事件名称包含对事件的简要描述，单击事件名称右侧弹出详情界面，界面展示事件的基本信息、事件的处置建议和关联告警等。 单击事件名称查看事件详情。

参数名称	参数说明
事件等级	事件等级分为五种等级： <ul style="list-style-type: none"> ● 提示 ● 低危 ● 中危 ● 高危 ● 致命
子类/类型	事件源类型分为： <ul style="list-style-type: none"> ● 数据库攻击 ● API攻击
来源	来源于数据库审计、数据库安全网关、API安全网关等组件以及实例名称。
状态	状态说明如下： <ul style="list-style-type: none"> ● 开启 ● 阻塞 ● 关闭
影响资产	影响的数据库资产或API。
验证状态	包含如下状态： <ul style="list-style-type: none"> ● 未知 ● 确认 ● 误报
责任人	用户名。
创建时间	事件创建时间。
发生时间	事件首次发生时间。
计划关闭事件	事件计划关闭时间。

---结束

相关操作

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

10.4 告警管理

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


前提条件

已开通DBSS服务，且DBSS中已有资产，详情请参见[购买数据库安全审计](#)。

操作步骤

步骤1 [登录管理控制台](#)。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全与合规 > 数据安全中心”。

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

步骤5 可查看“未处理告警”、“告警来源”、“告警总量”。

图 10-14 告警环形图



步骤6 查看告警列表，参数如[表10-12](#)所示。

表 10-12 数据风险告警参数列表

参数名称	参数说明
告警名称/ID	告警源的名称。告警名称包含对告警的简要描述，单击告警名称右侧弹出详情界面，界面展示告警的基本信息、告警的处置建议和攻击信息等。
告警等级	告警事件等级分为五种等级： <ul style="list-style-type: none"> 提示 低危 中危 高危 致命
子类/类型	告警源类型分为： <ul style="list-style-type: none"> 数据库攻击 API攻击

参数名称	参数说明
来源	来源于数据库审计、数据库安全网关、API安全网关等组件以及实例名称
状态	状态说明如下： <ul style="list-style-type: none"> • 开启 • 阻塞 • 关闭
影响资产	影响的数据库资产或API。
验证状态	包含如下状态： <ul style="list-style-type: none"> • 未知 • 确认 • 误报
责任人	用户名。
创建时间	告警创建时间。
发生时间	告警首次发生时间。

----结束

相关操作

- 转事件
 - a. 单击告警列表“操作”列的“转事件”进入“转事件”界面。
 - b. 根据如表10-13所示，填写“转事件信息”。

表 10-13 转事件信息参数

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

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

10.5 OBS 使用审计

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

前提条件

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

说明


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

- 已对OBS资产进行敏感数据识别，OBS敏感数据识别请参见[新建敏感数据识别任务](#)。

操作步骤

步骤1 [登录管理控制台](#)。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全与合规 > 数据安全中心”。

步骤4 在左侧导航树中选择“数据安全运营 > OBS使用审计”，进入“OBS使用审计”界面，参数说明请参考[表10-14](#)。

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

表 10-14 风险行为检测参数列表

参数名称	参数说明
用户ID	资源所有者对应的ID。

参数名称	参数说明
事件类型	<p>DSC将异常事件分成了三种类型：</p> <ul style="list-style-type: none"> ● 数据访问异常 <ul style="list-style-type: none"> - 敏感文件的越权操作。 - 敏感文件的下载操作。 ● 数据操作异常 <ul style="list-style-type: none"> - 敏感文件的更新操作。 - 敏感文件的文件内容追加操作。 - 敏感文件的删除操作。 - 敏感文件的复制操作。 ● 数据管理异常 <ul style="list-style-type: none"> - 添加桶时，检测到桶为公共读或公共读写桶。 - 添加桶时，检测到私有桶对匿名用户或注册用户组开通了访问/ACL访问权限。 - 含有敏感文件的桶出现桶策略更改、删除操作。 - 含有敏感文件的桶出现桶ACL更改、删除操作。 - 含有敏感文件的桶出现跨区域复制配置的更改、删除操作。 - 敏感文件的对象出现ACL更改、删除操作。
事件名称	导致异常事件发生的具体事件。
告警时间	异常事件发生的具体时间。
状态	<p>状态说明如下：</p> <ul style="list-style-type: none"> ● “待处理”：异常事件未进行处理。 ● “违例确认”：已处理异常事件为违例确认。 ● “违例排除”：已处理异常事件为违例排除。

步骤5 在异常事件的操作列，单击“查看详情”，查看该事件的详细信息。

步骤6 在异常事件的操作列，单击“处理”，处理该事件，处理方式如下：

- 确认该事件为违例事件。
确认违例的事件如未被处理，数据安全中心将会一直对该事件进行异常事件告警。
- 确认事件为正常情况，无需进行处理。
异常事件设为违例排除后，数据安全中心将不再对该事件进行告警提示，即该事件将不会展示在异常事件列表中。

----结束

10.6 水印溯源

10.6.1 数据库水印提取

前提条件

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


约束条件

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

新建任务

步骤1 [登录管理控制台](#)。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全与合规 > 数据安全中心”。

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

步骤5 单击“新建任务”，进入新建任务弹框，请根据[表10-15](#)配置相关参数。

表 10-15 新建水印提取任务

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


步骤6 单击“确定”，完成水印提取任务创建。

----结束

查看结果

步骤1 [登录管理控制台](#)。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全与合规 > 数据安全中心”。

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

步骤5 在目标任务“操作”列单击“查看结果”。


----结束

删除水印提取任务

执行中的提取水印任务不支持删除。

步骤1 [登录管理控制台](#)。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全与合规 > 数据安全中心”。

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

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

说明

删除操作无法恢复，请谨慎操作。

----结束

10.6.2 OBS 桶文件水印提取

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

前提条件

- 已完成OBS资产委托授权，参考[云资产委托授权/停止授权](#)进行操作。
- 如果需要添加自有OBS桶，则需要已开通且已使用过OBS服务。
- 文件格式为PDF、PPT、Word、Excel。

约束条件


- 本章节的方法仅针对提取PDF、PPT、Word、Excel格式文件的单个文件的暗水印。
- PDF文件和Word文件最大50M。
- Excel文件最大70M。

- PPT文件最大20M。

创建 OBS 桶文件水印提取任务

步骤1 [登录管理控制台](#)。

步骤2 单击左上角的, 选择区域或项目。

步骤3 在左侧导航树中, 单击, 选择“安全与合规 > 数据安全中心”。

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


步骤5 选择“OBS文件水印提取”页签。

步骤6 单击左上角“新建任务”, 进入“新建任务”页面。

步骤7 单击添加文件选择需要进行提取水印的文件, OBS桶文件支持多选。

步骤8 单击“确定”, 提取水印任务创建完成。

步骤9 单击目标任务名称, 在弹框中查看水印提取任务状态和OBS桶文件的暗水印内容。

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

----结束

10.6.3 本地文件水印提取

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

前提条件

- 已完成OBS资产委托授权, 参考[云资产委托授权/停止授权](#)进行操作。
- 如果需要添加自有OBS桶, 则需要已开通且已使用过OBS服务。
- 文件格式为PDF、PPT、Word、Excel。


约束条件

- 本章节的方法仅针对提取PDF、PPT、Word、Excel格式文件的单个文件的暗水印。
- PDF文件和Word文件最大50M。
- Excel文件最大70M。
- PPT文件最大20M。

本地文件水印提取

步骤1 [登录管理控制台](#)。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全与合规 > 数据安全中心”。

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

步骤5 选择“本地文件水印提取”页签。

步骤6 单击“添加文件”，将本地需要提取暗水印的文件上传到DSC平台。

说明

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

步骤7 文件上传后，单击“确定”，暗水印内容将展示到弹框中。

---结束

11 告警通知

通过设置告警通知，当敏感数据检测完成后或异常事件处理监测到异常事件时，数据安全中心将敏感数据检测结果以及异常事件通过用户设置的接收通知方式发送给用户。

前提条件

已开通消息通知服务。


约束条件

- 在使用告警通知前，确认已开通消息通知服务，消息通知服务为付费服务，价格详情请参见[SMN价格详情](#)。
- 在设置告警通知前，建议您先以管理员身份在“消息通知服务”中创建“消息主题”，详细操作请参见[创建主题](#)。

操作步骤

步骤1 [登录管理控制台](#)。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全与合规 > 数据安全中心”。

步骤4 在左侧导航树中选择“告警通知”，进入告警通知页面。

步骤5 配置告警通知，相关参数说明如[表11-1](#)所示。

说明

该告警通知为默认通知，如果未添加通知主题，数据使用审计告警将使用默认通知。

图 11-1 设置告警通知

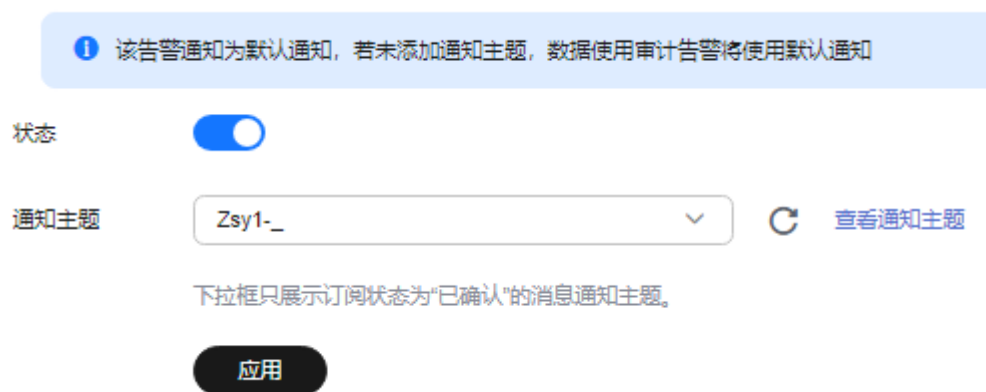




表 11-1 告警通知参数说明

参数名称	说明
状态	<p>是否开启通知。</p> <ul style="list-style-type: none"> ：开启状态。 ：关闭状态。
通知主题	<p>单击下拉列表选择已创建消息通知主题或者单击“查看通知主题”创建新的主题，用于配置接收告警通知的终端。</p> <p>单击“查看通知主题”创建新主题的操作步骤如下：</p> <ol style="list-style-type: none"> 参见创建主题创建一个主题。 配置接收告警通知的手机号码、邮件地址、函数、平台应用的终端、DMS或HTTP(S)终端，即为创建的主题添加一个或多个订阅，具体操作请参见添加订阅。 确认订阅。添加订阅后，完成订阅确认。 <p>更多关于主题和订阅的信息，请参见《消息通知服务用户指南》。</p>

步骤6 单击“应用”。

----结束

12 设备管理

12.1 设备管理概述

设备管理的作用是纳管第三方设备，包含应用数据审计设备、应用数据安全网关设备、数据库防火墙设备、数据库加密设备和静态脱敏设备，进行状态监控和告警展示，将风险和告警呈现给客户。

用户可单击DSC设备列表“操作”列“登录”，跳转到第三方设备管理页面。

功能介绍

表 12-1 功能介绍

功能	描述	相关操作
设备列表	DSC支持将应用数据审计设备、应用数据安全网关设备、数据库防火墙设备、数据库加密设备和静态脱敏设备添加至设备列表，方便查看和管理。	设备列表
设备监控	DSC会对设备状态进行监控，详细的展示设备当前的CPU、内存使用率以及剩余磁盘情况，供您及时查看设备状态。	设备监控
设备告警	DSC会将检测到的设备告警展示在设备告警列表，可以通过单击“忽略”或者“标记为已处理”对设备告警进行处理。	设备告警
策略管理	管理员在DSC设备管理的策略管理页面制定数据库加密、数据库动脱策略，下发给数据库加密（动脱）设备生效。	策略管理

12.2 设备列表

12.2.1 添加设备

DSC支持将应用数据审计设备、应用数据安全网关设备、数据库防火墙设备、数据库加密设备和静态脱敏设备添加至设备列表进行设备告警和监控。


前提条件

已购买第三方设备，购买第三方设备具体方式请联系技术支持。

操作步骤

步骤1 [登录管理控制台](#)。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全与合规 > 数据安全中心”。

步骤4 选择“设备管理 > 设备列表”，进入“数据安全设备列表”界面。

步骤5 在设备列表左上角单击“添加设备”，在“添加设备”弹框中参照[表12-2](#)配置相关参数。

表 12-2 添加设备参数说明

参数	说明
设备名称	您可以自定义设备名称。 设备名称需要满足以下要求： <ul style="list-style-type: none"> 由中文字符、英文字母、数字、下划线和中划线组成。 4-255个字符。 不能有重复的设备名称。
设备类型	单击下拉框选择已部署“设备类型”，包含如下四种： <ul style="list-style-type: none"> 应用数据审计：位于Web应用侧的数据安全产品。 应用数据安全网关：提供综合的应用安全防护系统。 数据库防火墙：主要用来应对数据应用层面的SQL恶意攻击或恶意操作风险。 数据库加密：基于网关代理加密技术，实现敏感数据加密存储。 静态脱敏：对敏感数据进行脱敏处理，以确保隐私和安全，同时保留数据结构和统计特性。
部署模式	单击下拉框选择已部署设备的“部署模式”，包含如下三种模式： <ul style="list-style-type: none"> 单机：一台设备。 主备：两台设备，一台为主设备，一台为备机。 集群：多台设备。
虚拟私有云	单击下拉框选择已部署设备的虚拟私有云。

参数	说明
子网	单击下拉框选择已部署设备的子网。
管理地址（可选）	<ul style="list-style-type: none">请填写第三方设备管理配置地址。也可以在设备添加成功后，单击“编辑”补充填写管理地址。

步骤6 单击“确定”完成添加设备。

----结束

12.2.2 设备上线

如果需要恢复下线状态设备的注册、心跳请求等信息，请参见此章节操作，设备上线后DSC正常接收设备注册、心跳请求等信息。上线后的设备在设备列表可对设备进行单点登录、编辑或者配置。


约束限制

只有处于“下线”状态的设备，才支持设备上线操作。

操作步骤

步骤1 [登录管理控制台](#)。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全与合规 > 数据安全中心”。

步骤4 选择“设备管理 > 设备列表”，进入“数据安全设备列表”界面。

步骤5 勾选要上线的设备，单击设备列表左上角“设备上线”，设备“状态”为“正常”即表示上线成功。

----结束

12.2.3 设备下线

如果需要在设备列表删除该设备，或者不需要DSC继续接受该设备的注册、心跳请求等信息，可将该设备下线，下线后的设备DSC将不再接受该设备信息。下线后的设备在设备列表不可单点登录、编辑或配置。


约束限制

设备状态是异常、正常、丢失。

操作步骤

步骤1 [登录管理控制台](#)。

步骤2 单击左上角的，选择区域或项目。

- 步骤3** 在左侧导航树中，单击 ，选择“安全与合规 > 数据安全中心”。
- 步骤4** 选择“设备管理 > 设备列表”，进入“数据安全设备列表”界面。
- 步骤5** 勾选要下线的设备，单击设备列表左上角“设备下线”，设备“状态”为“下线”即表示下线成功。
- 结束

12.2.4 查看设备列表

将设备添加至设备列表后，可通过此章节查看设备状态和进行管理设备的相关操作。

前提条件

设备已添加至DSC设备列表。

操作步骤



- 步骤1** [登录管理控制台](#)。
- 步骤2** 单击左上角的 ，选择区域或项目。
- 步骤3** 在左侧导航树中，单击 ，选择“安全与合规 > 数据安全中心”。
- 步骤4** 选择“设备管理 > 设备列表”，进入“数据安全设备列表”界面。
- 步骤5** 设备列表页面参数说明如[表 设备列表参数](#)所示。可根据“设备类型”、“部署模式”、和“状态”对设备进行筛选。

表 12-3 设备列表参数

参数	参数说明
设备名称	单击设备名称可查看设备详细信息。 将设备添加至DSC设备列表后将获得设备ID，此设备ID用在设备页面配置，作为注册认证时的唯一标识。
设备类型	设备类型包含如下类型： <ul style="list-style-type: none"> 应用数据审计：位于Web应用侧的数据安全产品。 应用数据安全网关：提供综合的应用安全防护系统。 数据库防火墙：主要用来应对数据应用层面的SQL恶意攻击或恶意操作风险。 数据库加密：基于网关代理加密技术，实现敏感数据加密存储。 静态脱敏：对敏感数据进行脱敏处理，以确保隐私和安全，同时保留数据结构和统计特性。
设备版本	该设备的版本信息。

参数	参数说明
部署模式	部署模式包含如下： <ul style="list-style-type: none"> ● 单机：只有一台设备。 ● 主备：两台设备，一台主设备，一台备机。 ● 集群：多台设备。
管理地址	添加完设备，单击“编辑”添加管理设备地址。
状态	主机状态包含如下： <ul style="list-style-type: none"> ● 异常：“设备状态”为“异常”时，可在操作列单点登录和编辑。 ● 正常：“设备状态”为“正常”时，可在操作列单点登录和编辑。 ● 下线：“设备状态”为“下线”时，可在操作列上线和删除该设备。 ● 新加：“设备状态”为“新加”时，可在操作列上删除和编辑该设备。 ● 丢失：“设备状态”为“丢失”时，可在操作列单点登录和编辑。
更新时间	设备状态的更新时间。

----结束

相关操作

- 单击目标设备操作列“删除”，可删除此设备。

说明

请将设备下线后再删除。

- 单击目标设备操作列“登录”，登录设备管理页面对设备进行配置管理。

12.3 设备监控

DSC会对设备进行实时监控，您可以通过此页面查看设备当前的CPU、内存使用率以及剩余磁盘情况。

约束限制

状态为丢失的不再更新设备数据。


前提条件

设备已添加至设备列表。

操作步骤

步骤1 [登录管理控制台](#)。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全与合规 > 数据安全中心”。

步骤4 选择“设备管理 > 设备监控”，进入“数据安全设备监控”界面。

步骤5 设备监控界面展示您已添加的设备运行状态。

- 设备当前状态：通过CPU使用率、内存利用率和剩余磁盘占比及时了解设备具体状态。
- 设备状态：同步设备列表的设备状态，如异常、正常、新加等，具体请参见[查看设备列表](#)。
- 设备地址：设备管理地址，单击登录三方配置页面。

步骤6 在界面右上角可根据设备类型、设备状态以及设备名称和描述来筛选需要查看的设备。

----结束

12.4 设备告警

12.4.1 处理设备告警

DSC会将检测到的设备告警展示在设备列表，您可以通过此章节对设备告警进行相关处理。

约束限制

状态为丢失和新加的设备不会发送告警。


前提条件

设备已添加至设备列表。

操作步骤

步骤1 [登录管理控制台](#)。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全与合规 > 数据安全中心”。

步骤4 选择“设备管理 > 设备告警”，进入“数据安全设备告警”界面。

步骤5 选择预处理告警，支持多选，单击告警列表左上角“忽略”或者“标记为已处理”，处理此告警。

注意

忽略或者标记为已处理的告警不再展示，请谨慎操作。

----结束

12.4.2 查看设备告警列表

DSC会将检测到的设备告警展示在设备列表，您可以通过此章节查看告警类型、等级等信息。


前提条件

设备已添加至设备列表。

操作步骤

步骤1 [登录管理控制台](#)。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全与合规 > 数据安全中心”。

步骤4 选择“设备管理 > 设备告警”，进入“数据安全设备告警”界面，相关参数如表表12-4所示。

表 12-4 设备告警列表

参数	说明
设备名称/IP地址	设备的名称/IP地址
设备类型	设备类型分为四种类型： <ul style="list-style-type: none"> • 应用数据审计 • 应用数据安全网关 • 数据库防火墙 • 数据库加密 • 静态脱敏
告警类型	设备告警分为两种类型：（设备自己发送的告警，设备自己区分告警类型） <ul style="list-style-type: none"> • 系统告警：设备系统信息（CPU、内存） • 业务告警：设备功能相关告警。

参数	说明
告警等级	告警级别分为五种类型： <ul style="list-style-type: none"> • 紧急 • 重要 • 次要 • 提示 • 未知
告警时间	设备产生告警的时间。
状态	<ul style="list-style-type: none"> • 告警状态包含：未处理。 • 单击忽略和“标记为已处理”都不再展示，不影响同类型告警。
事件描述	告警事件的描述。
操作	单击“忽略”或者“标记为已处理”处理单条告警。

----结束

12.5 策略管理

管理员在数据安全设备管理的策略管理页面制定数据库加密、数据库动脱策略，下发给数据库加密（动脱）设备生效。

数据库加密支持的数据库类型及版本

数据源类型	版本
MySQL	5.6、5.7、5.8、8.0
SQL Server	<ul style="list-style-type: none"> • 2019_SE、2019_EE、2019_WEB • 2017_SE、2017_EE、2017_WEB • 2016_SE、2016_EE、2016_WEB • 2014_SE、2014_EE • 2012_SE、2012_EE、2012_WEB • 2008_R2_EE、2008_R2_WEB
Oracle	11、12
PostgreSQL	13、12、11、10、9.6、9.5、9.4
KingBase(人大金仓)	V8
DMDBMS(达梦)	7、8
TDSQL	10.3.X

数据源类型	版本
DWS	8.1.X


前提条件

已成功添加数据安全设备。

创建策略

步骤1 [登录管理控制台](#)。

步骤2 单击左上角的, 选择区域或项目。

步骤3 在左侧导航树中, 单击, 选择“安全与合规 > 数据安全中心”。

步骤4 选择“设备管理 > 策略管理”, 进入“策略管理”界面。

步骤5 左上角单击“创建策略”, 进入“创建策略”界面。

步骤6 选择策略类型并配置策略信息:

- “数据库加密”: 对数据进行加密处理, 以确保数据的机密性和完整性, 防止未经授权的访问和数据泄露。
 - a. 单击“开始配置”, 进入数据加密策略类型配置界面。
 - b. 参照[表12-5](#)进行参数配置:

表 12-5 数据加密策略类型参数配置表

参数	说明
策略名称	输入策略名称, 只能由中文字符、英文字母、数字、下划线和中划线组成。
加密	仅支持加密。
关联设备	单击下拉框选择关联设备。
目标数据源	单击下拉框选择目标数据源, 支持数据库版本详情请参加 数据库加密支持的数据库类型及版本 。
代理端口	端口范围14000-14999, 不同数据库实例(地址和端口相同)使用不同代理端口, 同一数据库实例使用相同代理端口, 添加同一数据库实例下的数据源, 会自动填充代理端口。
加密算法	单击下拉框选择加密算法, 加密算法有AES128和SM4。
被加密表	单击下拉框选择被加密表。 同一目标表不能重复选。

参数	说明
被加密表信息	被加密表的信息，包含“字段名称”、“字段类型”、“数据分级”。

- c. 单击“保存并下发”，进入策略列表，新创建的策略“状态”显示“启用（下发中）”，“状态”如果是“启用（下发成功）”则策略创建成功。
- “数据库静态脱敏”：对敏感数据进行脱敏处理，以确保隐私和安全，同时保留数据结构和统计特性。

说明

需要将待脱敏数据进行一次敏感数据识别。

- a. 单击“开始配置”，进入数据库静态脱敏策略配置界面。
- b. 参照表12-5进行参数配置：

表 12-6 数据库静态脱敏策略类型参数配置表

参数	说明
策略名称	输入策略名称，只能由中文字符、英文字母、数字、下划线和中划线组成。
关联设备	单击下拉框选择关联设备。
源数据源	单击下拉框选择待脱敏的数据源。
目标数据源	单击下拉框选择脱敏后数据存储的位置。
策略详情	<ul style="list-style-type: none"> ▪ 是否重建表：打开开关将重建表。 ▪ 是否清理目标表：打开开关后对目标表进行清理。 ▪ 是否跳过脏数据：打开开关会跳过表中的脏数据。
抽取方式	<ul style="list-style-type: none"> ▪ 全部抽取：对表中的数据全部抽取。 ▪ 百分比抽取：按照所填的百分比进行抽取，选择百分比抽取时输入百分比的范围为1-100。 ▪ 行抽取：按照所填行数进行抽取，选择行抽取时输入行数范围为100-10000
表	单击下拉框选择表，支持多选，一次最多选10个表。

参数	说明
表信息	选择“表”后显示该参数。 表的信息，包含“字段名称”、“字段类型”、“数据分级”、“脱敏算法”。单击“脱敏算法”下拉框选择合适的脱敏算法，也可以选择“不脱敏”。 “仅迁移”：打开仅迁移的开关只对选中的列进行迁移，不脱敏。

- c. 单击“保存并下发”，进入策略列表，新创建的策略“状态”显示“启用（下发中）”，“状态”如果是“启用（下发成功）”则策略创建成功。
- “数据库动态脱敏”：对敏感数据进行实时脱敏处理，以确保未经授权的数据不可访问。
 - a. 单击“开始配置”，进入数据库动态脱敏策略配置界面。
 - b. 参照表12-7进行参数配置：

表 12-7 数据库动态脱敏策略类型参数配置表

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

- c. 单击“保存并下发”，进入策略列表，新创建的策略“状态”显示“启用（下发中）”，“状态”如果是“启用（下发成功）”则策略创建成功。

----结束

相关操作

- 禁用策略：下发成功的策略可以在“操作”列单击“禁用”，禁用此条策略，单击“禁用”后此条策略的“状态”显示为“禁用（下发中）”，当策略的“状态”变为“禁用（下发成功）”此条策略被禁用。
- 删除策略：下发成功的策略可以在“操作”列单击“删除”，删除此条策略，单击“删除”后界面右上角提示该条策略删除成功。

说明

数据库加密后不允许禁用和删除，只能通过下发解密策略进行抵消。

编辑操作：数据库加密策略不允许编辑，只有动态脱敏策略可以编辑。


13 共享 VPC

操作场景

在设备管理功能中，添加设备时需要绑定VPC，可以通过申请VPC或者使用来自共享的VPC进行绑定。

创建共享 VPC 资源

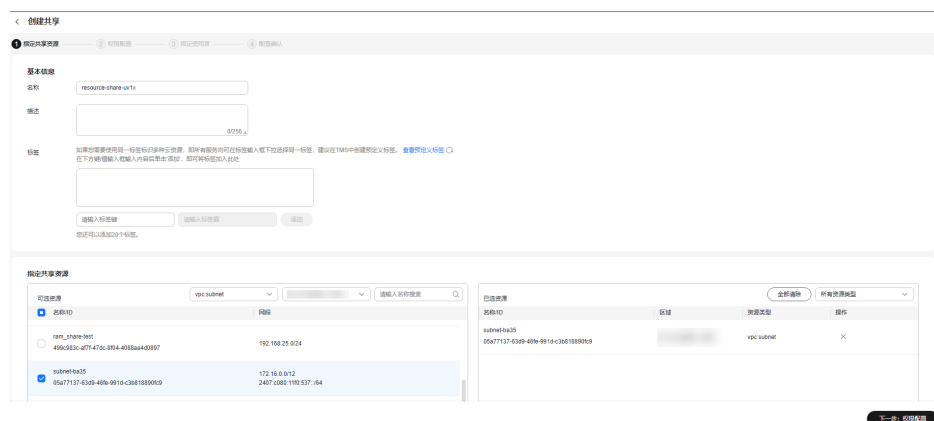
步骤1 登录管理控制台。

步骤2 单击页面左上角的 ，选择“管理与监管 > 资源访问管理”，进入“资源访问管理”页面。

步骤3 单击页面左侧“我的共享 > 共享管理”，进入“共享管理”页面。

步骤4 单击页面右上角的“创建共享”，进入“创建共享”页面。

图 13-1 指定共享资源



步骤5 选择资源类型为“vpc: subnet”，选择对应区域，勾选需进行共享的VPC。单击“下一步：权限配置”。

步骤6 进入“权限配置”页面，选择指定资源类型支持的共享权限，配置完成后，单击页面右下角的“下一步：指定使用者”。

步骤7 进入“指定使用者”页面，指定共享资源的使用者，配置完成后，单击页面右下角的“下一步：配置确认”。

表 13-1 参数说明

参数名称	参数说明
使用者类型	<ul style="list-style-type: none">组织 关于组织创建相关操作可参见创建组织。 <p>说明 如果您未打开“启用与组织共享资源”开关，使用者类型将无法选择“组织”。具体操作可参见启用与组织共享资源。</p> <ul style="list-style-type: none">华为云账号ID


步骤8 进入“配置确认”页面，确认配置无误后，单击页面右下角的“确认”，完成资源共享实例的创建。

----结束

使用共享 VPC 资源

步骤1 [登录管理控制台](#)。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全与合规 > 数据安全中心”。

步骤4 在左侧导航树中，选择“设备管理 > 设备列表”，进入设备列表界面。

步骤5 在设备列表左上角单击“添加设备”。

步骤6 在“虚拟私有云”下拉框中，选择来自共享的VPC实例，配置参数完成并单击“确定”。

----结束

14 多账号管理

14.1 多账号管理概述

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

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

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

📖 说明

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

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

有关组织的详细说明请参见《[组织用户指南](#)》。

📖 说明

为了请求B账号下的数据资产信息，DSC会自动在B账号中创建服务关联委托：

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

14.2 开启多账号管理功能

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

前提条件

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


使用约束

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

操作步骤

步骤1 [登录管理控制台](#)。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全与合规 > 数据安全中心”。

步骤4 单击“多账号管理”，进入“多账号管理”界面。

步骤5 单击“开启多账号管理”，开启多账号管理功能。

---结束

14.3 查看多账号管理


前提条件

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

操作步骤

步骤1 [登录管理控制台](#)。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全与合规 > 数据安全中心”。

步骤4 单击“多账号管理”，进入“多账号管理”界面。

步骤5 进入“账号列表”界面，参数如[表14-1](#)所示。

表 14-1 账号列表

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

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

---结束

15 权限管理

15.1 创建用户并授权使用 DSC

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

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

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

本章节为您介绍对用户授权的方法，操作流程如[图15-1](#)所示。

前提条件

给用户组授权之前，请您了解用户组可以添加的DSC权限，并结合实际需求进行选择，DSC支持的系统权限如[表15-1](#)所示。如果您需要对除DSC之外的其它服务授权，IAM支持服务的所有权限请参见[系统权限](#)。

须知

用户在执行[云资源委托授权/停止授权](#)时必须拥有IAM的管理员权限（“Security Administrator”权限）。

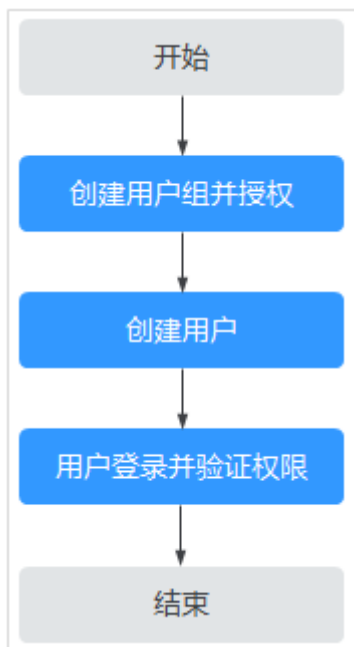
表 15-1 DSC 系统权限

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

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

示例流程

图 15-1 给用户授权服务权限流程



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

15.2 DSC 自定义策略

如果系统预置的DSC权限，不满足您的授权要求，可以创建自定义策略。

目前华为云支持以下两种方式创建自定义策略：

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

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

DSC 自定义策略样例

- 示例1：授权用户查询大数据资产列表

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "dsc:bigdataAsset:list"
      ]
    }
  ]
}
```

- 示例2：拒绝查询OBS资产列表

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

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

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

- 多个授权项策略

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

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

```

```

        "hss:hosts:switchVersion",
        "hss:hosts:manualDetect",
        "hss:manualDetectStatus:get"
    ]
}
]
}

```

15.3 DSC 权限及授权项

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

默认情况下，新建的IAM用户没有任何权限，您需要将其加入用户组，并给用户组授予策略或角色，才能使用户组中的用户获得相应的权限，这一过程称为授权。授权后，用户就可以基于已有权限对云服务进行操作。

权限根据授权的精细程度，分为**角色**和**策略**。角色以服务为粒度，是IAM最初提供了一种根据用户的工作职能定义权限的粗粒度授权机制。策略授权更加精细，可以精确到某个操作、资源和条件，能够满足企业对权限最小化的安全管控要求。

支持的授权项

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

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

权限	授权项
查询OBS资产列表	dsc:obsAsset:list
更新DSC扫描任务规则	scanRule:update
添加大数据资产	dsc:bigdataAsset:create
查询DSC扫描任务规则列表	dsc:scanRule:list
添加OBS资产	dsc:obsAsset:create
查询rds列表	dsc:rds:list
删除数据库资产	dsc:databaseAsset:delete
创建DSC扫描任务规则	dsc:scanRule:create
删除DSC扫描任务	dsc:scanTask:delete
查询DSC服务授权信息	dsc:authorization:get
查询RDS数据库列表	dsc:rdsDatabase:list
更新DSC扫描任务	dsc:scanTask:update

权限	授权项
查询CSS列表	dsc:css:list
创建DSC扫描任务	dsc:scanTask:create
授予DSC服务用户操作权限	dsc:authorization:grant
查询大数据资产列表	dsc:bigdataAsset:list
查询DSC扫描任务列表	dsc:scanTask:list
添加数据库资产	dsc:databaseAsset:create
删除DSC扫描任务规则	dsc:scanRule:delete
查询数据库资产列表	dsc:databaseAsset:list
删除OBS资产	dsc:obsAsset:delete
删除大数据资产	dsc:bigdataAsset:delete
DSC通用资源操作权限	dsc:common:operate
DSC通用资源查询权限	dsc:common:list

16 审计

16.1 支持云审计的操作列表

云审计服务（Cloud Trace Service, CTS）记录了数据安全中心相关的操作事件，方便用户日后的查询、审计和回溯，具体请参见《云审计服务用户指南》。

云审计服务支持的DSC操作列表如表16-1所示。

表 16-1 云审计服务支持的 DSC 操作列表

操作名称	资源类型	事件名称
授权或者取消对DSC的授权	dscGrant	grantOrRevokeTodsc
添加OBS桶资产	dscObsAsset	addBuckets
删除OBS桶资产	dscObsAsset	deleteBucket
添加数据库资产	dscDatabaseAsset	addDatabase
修改数据库资产	dscDatabaseAsset	updateDatabase
删除数据库资产	dscDatabaseAsset	deleteDatabase
添加大数据资产	dscBigdataAsset	addBigdata
修改大数据资产	dscBigdataAsset	updateBigdata
删除大数据资产	dscBigdataAsset	deleteBigdata
更新对象名称	dscAsset	updateAssetName
下载批量添加模板	dscBatchImportTemplate	downloadBatchImportTemplate
批量添加数据库	dscAsset	batchAddDatabase
批量添加资产	dscAsset	batchAddAssets
展示异常事件	dscExceptionEvent	listExceptionEventInfo

操作名称	资源类型	事件名称
获取异常事件详细信息	dscExceptionEvent	getExceptionEventDetail
添加告警配置	dscAlarmConfig	addAlarmConfig
修改告警配置	dscAlarmConfig	updateAlarmConfig
下载报表	dscReport	downloadReport
删除报表	dscReport	deleteReport
添加扫描规则	dscRule	addRule
修改扫描规则	dscRule	editRule
删除扫描规则	dscRule	deleteRule
添加扫描规则组	dscRuleGroup	addRuleGroup
修改扫描规则组	dscRuleGroup	editRuleGroup
删除扫描规则组	dscRuleGroup	deleteRuleGroup
添加扫描任务	dscScanTask	addScanJob
修改扫描任务	dscScanTask	updateScanJob
删除扫描子任务	dscScanTask	deleteScanTask
删除扫描任务	dscScanTask	deleteScanJob
启动扫描任务	dscScanTask	startJob
停止扫描任务	dscScanTask	stopJob
启动扫描子任务	dscScanTask	startTask
停止扫描子任务	dscScanTask	stopTask
启用/停用ES脱敏	dscBigDataMaskSwitch	switchBigDataMaskStatus
获取ElasticSearch field信息	dscBigDataMetaData	getESField
添加ES脱敏模板	dscBigDataMaskTemplate	addBigDataTemplate
编辑ES脱敏模板	dscBigDataMaskTemplate	editBigDataTemplate
删除ES脱敏模板	dscBigDataMaskTemplate	deleteBigDataTemplate
查询ES脱敏模板列表	dscBigDataMaskTemplate	showBigDataTemplates
启动/停止ES脱敏模板	dscBigDataMaskTemplate	operateBigDataTemplate

操作名称	资源类型	事件名称
切换ES脱敏模板状态	dscBigDataMaskTemplate	switchBigDataTemplate
启用/停用数据库脱敏	dscDBMaskSwitch	switchDBMaskStatus
获取数据库字段信息	dscDBMetaData	getColumn
添加数据库脱敏模板	dscDBMaskTemplate	addDBTemplate
修改数据库脱敏模板	dscDBMaskTemplate	editDBTemplate
删除数据库脱敏模板	dscDBMaskTemplate	deleteDBTemplate
查询数据库脱敏模板列表	dscDBMaskTemplate	showDBTemplates
启动/停止数据库脱敏模板	dscDBMaskTemplate	operateDBTemplate
切换数据库脱敏模板状态	dscDBMaskTemplate	switchDBTemplate
添加脱敏算法	dscMaskAlgorithm	addMaskAlgorithm
编辑脱敏算法	dscMaskAlgorithm	editMaskAlgorithm
删除脱敏算法	dscMaskAlgorithm	deleteMaskAlgorithm
测试脱敏算法	dscMaskAlgorithm	testMaskAlgorithm
获取字段与脱敏算法的映射关系	dscMaskAlgorithm	getFieldAlgorithms
添加加密算法配置	dscEncryptMaskConfig	addEncryptConfig
修改加密算法配置	dscEncryptMaskConfig	editEncryptConfig
删除加密算法配置	dscEncryptMaskConfig	deleteEncryptConfig

16.2 在 CTS 事件列表查看云审计事件

操作场景

用户进入云审计服务创建管理类追踪器后，系统开始记录云服务资源的操作。在创建数据类追踪器后，系统开始记录用户对OBS桶中数据的操作。云审计服务管理控制台会保存最近7天的操作记录。

📖 说明

云审计控制台对用户的操作事件日志保留7天，过期自动删除，不支持人工删除。


本节介绍如何在云审计服务管理控制台查看或导出最近7天的操作记录。

- [在新版事件列表查看审计事件](#)
- [在旧版事件列表查看审计事件](#)

使用限制

- 单账号跟踪的事件可以通过云审计控制台查询。多账号的事件只能在账号自己的事件列表页面去查看，或者到组织追踪器配置的OBS桶中查看，也可以到组织追踪器配置的CTS/system日志流下面去查看。
- 用户通过云审计控制台只能查询最近7天的操作记录。如果需要查询超过7天的操作记录，您必须配置转储到对象存储服务(OBS)或云日志服务(LTS)，才可在OBS桶或LTS日志组里面查看历史事件信息。否则，您将无法追溯7天以前的操作记录。
- 云上操作后，1分钟内可以通过云审计控制台查询管理类事件操作记录，5分钟后才可通过云审计控制台查询数据类事件操作记录。
- CTS新版事件列表不显示数据类审计事件，您需要在旧版事件列表查看数据类审计事件。


在新版事件列表查看审计事件

1. 登录管理控制台。
2. 单击左上角 ，选择“管理与监管管理与部署 > 云审计服务 CTS”，进入云审计服务页面。
3. 单击左侧导航树的“事件列表”，进入事件列表信息页面。
4. 事件列表支持通过高级搜索来查询对应的操作事件，您可以在筛选器组合一个或多个筛选条件：
 - 事件名称：输入事件的名称。
 - 事件ID：输入事件ID。
 - 资源名称：输入资源的名称，当该事件所涉及的云资源无资源名称或对应的API接口操作不涉及资源名称参数时，该字段为空。
 - 资源ID：输入资源ID，当该资源类型无资源ID或资源创建失败时，该字段为空。
 - 云服务：在下拉框中选择对应的云服务名称。
 - 资源类型：在下拉框中选择对应的资源类型。
 - 操作用户：在下拉框中选择一个或多个具体的操作用户。
 - 事件级别：可选项为“normal”、“warning”、“incident”，只可选择其中一项。
 - normal：表示操作成功。
 - warning：表示操作失败。
 - incident：表示比操作失败更严重的情况，例如引起其他故障等。

- 企业项目ID：输入企业项目ID。
- 访问密钥ID：输入访问密钥ID（包含临时访问凭证和永久访问密钥）。
- 时间范围：可选择查询最近1小时、最近1天、最近1周的操作事件，也可以自定义最近7天内任意时间段的操作事件。

📖 说明

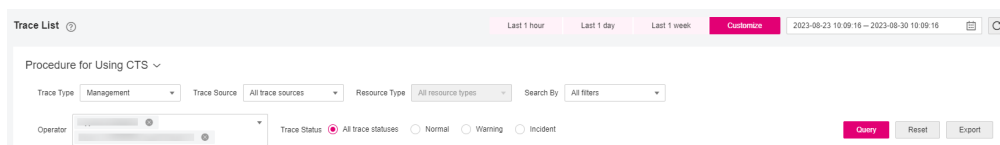
您可以参考[云审计服务应用示例](#)，来学习如何查询具体的事件。

5. 在事件列表页面，您还可以导出操作记录文件、刷新列表、设置列表展示信息等。
 - 在搜索框中输入任意关键字，按下Enter键，可以在事件列表搜索符合条件的数据。
 - 单击“导出”按钮，云审计服务会将查询结果以.xlsx格式的表格文件导出，该.xlsx文件包含了本次查询结果的所有事件，且最多导出5000条信息。
 - 单击🔄按钮，可以获取到事件操作记录的最新信息。
 - 单击⚙️按钮，可以自定义事件列表的展示信息。启用表格内容折行开关，可让表格内容自动折行，禁用此功能将会截断文本，默认停用此开关。
6. 关于事件结构的关键字段详解，请参见[事件结构](#)“云审计服务事件参考 > 事件结构”章节和[事件样例](#)“云审计服务事件参考 > 事件样例”章节。
7. （可选）在新版事件列表页面，单击右上方的“返回旧版”按钮，可切换至旧版事件列表页面。

在旧版事件列表查看审计事件

1. 登录管理控制台。
2. 单击左上角☰，选择“管理与监管管理与部署 > 云审计服务 CTS”，进入云审计服务页面。
3. 单击左侧导航树的“事件列表”，进入事件列表信息页面。
4. 用户每次登录云审计控制台时，控制台默认显示新版事件列表，单击页面右上方的“返回旧版”按钮，切换至旧版事件列表页面。
5. 事件列表支持通过筛选来查询对应的操作事件，如[图16-1](#)所示。当前事件列表支持四个维度的组合查询，详细信息如下：

图 16-1 筛选框



- 事件类型、事件来源、资源类型和筛选类型，在下拉框中选择查询条件。
 - 筛选类型按资源ID筛选时，还需手动输入某个具体的资源ID。
 - 筛选类型按事件名称筛选时，还需选择某个具体的事件名称。

- 筛选类型按资源名称筛选时，还需选择或手动输入某个具体的资源名称。
- 操作用户：在下拉框中选择某一具体的操作用户，此操作用户指用户级别，而非租户级别。
- 事件级别：可选项为“所有事件级别”、“Normal”、“Warning”、“Incident”，只可选择其中一项。
- 时间范围：可选择查询最近1小时、最近1天、最近1周的操作事件，也可以自定义最近7天内任意时间段的操作事件。

📖 说明

您可以参考[云审计服务应用示例](#)，来学习如何查询具体的事件。

6. 选择完查询条件后，单击“查询”。
7. 在事件列表页面，您还可以导出操作记录文件和刷新列表。
 - 单击“导出”按钮，云审计服务会将查询结果以CSV格式的表格文件导出，该CSV文件包含了本次查询结果的所有事件，且最多导出5000条信息。
 - 单击🔄按钮，可以获取到事件操作记录的最新信息。
8. 在需要查看的事件左侧，单击📄展开该记录的详细信息。

The screenshot displays the Cloud Audit Service console interface. It shows a table of events with columns for Event Name, Resource Type, Cloud Service, Trace ID, Resource Name, Event Level, Operator, Operation Time, and Action. Two event entries are expanded to show their details:

- Event 1:** createDockerConfig. Resource Type: dockerlogincmd. Cloud Service: SWR. Trace ID: 179557d1690441269c748b858... Resource Name: dockerlogincmd. Event Level: normal. Operation Time: 2023/11/16 10:54:04 GMT+08:00. Action: 查看事件.
- Event 2:** login. Resource Type: user. Trace Source: IAM. Resource ID: 179557d1690441269c748b858... Trace Status: normal. Operator: [redacted]. Operation Time: Jul 3, 2024 11:26:32 GMT+08:00. Operation: View Trace.

The expanded details for each event include fields like request, trace_id, code, trace_name, resource_type, trace_rating, api_version, message, source_ip, domain_id, and trace_type.

9. 在需要查看的记录右侧，单击“查看事件”，会弹出一个窗口显示该操作事件结构的详细信息。

查看事件 ×

```
{
  "request": "",
  "trace_id": "676d4ae3-842b-11ee-9299-9159eee6a3ac",
  "code": "200",
  "trace_name": "createDockerConfig",
  "resource_type": "dockerlogincmd",
  "trace_rating": "normal",
  "api_version": "",
  "message": "createDockerConfig, Method: POST Url=/v2/management/secret, Reason:",
  "source_ip": "",
  "domain_id": "",
  "trace_type": "ApiCall",
  "service_type": "SWR",
  "event_type": "system",
  "project_id": "",
  "response": "",
  "resource_id": "",
  "tracker_name": "system",
  "time": "2023/11/16 10:54:04 GMT+08:00",
  "resource_name": "dockerlogincmd",
  "user": {
    "domain": {
      "name": "",
      "id": ""
    }
  }
}
```

10. 关于事件结构的关键字段详解，请参见《云审计服务用户指南》中的[事件结构](#)“云审计服务事件参考 > 事件结构”章节和[事件样例](#)“云审计服务事件参考 > 事件样例”章节。
11. （可选）在旧版事件列表页面，单击右上方的“体验新版”按钮，可切换至新版事件列表页面。