数据安全中心

最佳实践

文档版本 06

发布日期 2024-10-15

华为云计算技术有限公司

商标声明


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 如何防止个人敏感数据在开发测试中被泄露?

敏感数据是指那些如果被未经授权的人访问、泄露或滥用，可能会对个人或组织造成严重风险的信息。

- 对个人而言，身份证号码、家庭住址、工作单位、银行卡号等隐私信息都是敏感数据。
- 对企业或组织而言，客户资料、财务信息、技术资料、重大决策等公司核心信息都是敏感数据。

华为云数据安全中心（Data Security Center，简称DSC）提供静态数据脱敏功能：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。

常见数据泄露原因

- 内部数据泄漏
  - 笔记本电脑和移动设备的丢失或失窃
  - 敏感数据越权访问和存储
  - 员工外发、打印和复制敏感数据
  - 意外传输敏感数据
- 外部攻击导致的数据泄漏
  - 基础措施不可控，避免数据存储系统存在漏洞
  - 配置不当导致的外部攻击
  - 敏感数据越权访问和存储

场景

假设“rsd-dsc-test”数据库中“dsc_bank”表中存储了如下银行员工信息：

图 1-1 银行员工示例信息

Name	Birthday	Email	address
San Zhang	1999-06-03 10:10:00	13577 3@163.com	Chengdu, Sichuan
Si Li	1990-08-03 05:05:00	552 3@qq.com	Beijing

现需对该表进行敏感数据识别并完成脱敏，识别出敏感数据并生成识别结果数据报告，再对识别出的敏感数据进行“Hash脱敏”中的SHA256算法进行脱敏处理。

步骤一：购买数据安全中心专业版

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 1-2 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 1-3 选择扩展包

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

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

图 1-4 购买时长

说明

勾选“自动续费”后，当服务期满时，系统会自动按照购买周期进行续费。

步骤8 在页面的右下角，单击“立即购买”。

如果您对价格有疑问，可以单击页面左下角的“了解计费详情”，了解产品价格。

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

图 1-5 详情页面

步骤10 进入“付款”页面，请选择付款方式进行付款。

----结束

步骤二：识别敏感数据

步骤1 登录管理控制台。

步骤2 在左侧导航树中，单击 ☰，选择“安全 > 数据安全中心”。

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

步骤4 单击“新建任务”，在弹出的“新建任务”对话框中，配置任务基本信息。

表 1-1 新建任务参数说明

参数	说明	取值样例
任务名称	您可以自定义敏感数据识别任务名称。 任务名称需要满足以下要求： ● 4~255个字符。 ● 字符可由中文、英文字母、数字、下划线或中划线组成。 ● 开头需为中文或者字母。 ● 任务名称不能与已有的任务名称重复。	DSC_Test
数据类型	选择识别的数据类型，可多选。 ● OBS：授权DSC访问您的华为云OBS资产后，DSC将对华为云OBS里的资产进行敏感数据识别，添加OBS资产的相关操作请参见**添加OBS资产**。 ● 数据库：DSC将对已授权的数据库资产进行敏感数据识别，授权数据库资产的相关操作请参见**授权数据库资产**。 ● 大数据：DSC将对已授权的大数据资产进行敏感数据识别，授权大数据源资产请参见**授权大数据资产**。 ● MRS：DSC将对已授权的MRS资产进行敏感数据识别，授权MRS资产请参见**授权大数据资产**。 ● LTS：DSC将对已授权的LTS资产进行敏感数据识别，添加日志流请参见**添加日志流**。	数据库 > rsd-dsc-test
识别模板	选择内置模板或者自定义模板，DSC将根据您选择的模板对数据进行分级分类展示。添加模板请参见**新增识别模板**。	华为云数据安全分类分级模板
识别周期	设置数据识别任务的执行策略： ● 单次：根据设置的执行计划，在设定的时间执行一次该识别任务。 ● 每天：选择该选项，即在每天的固定时间执行该识别任务。 ● 每周：选择该选项，即在设定的每周这一时间点执行该识别任务。 ● 每月：选择该选项，即在设定的每月这一时间点执行该识别任务。	单次

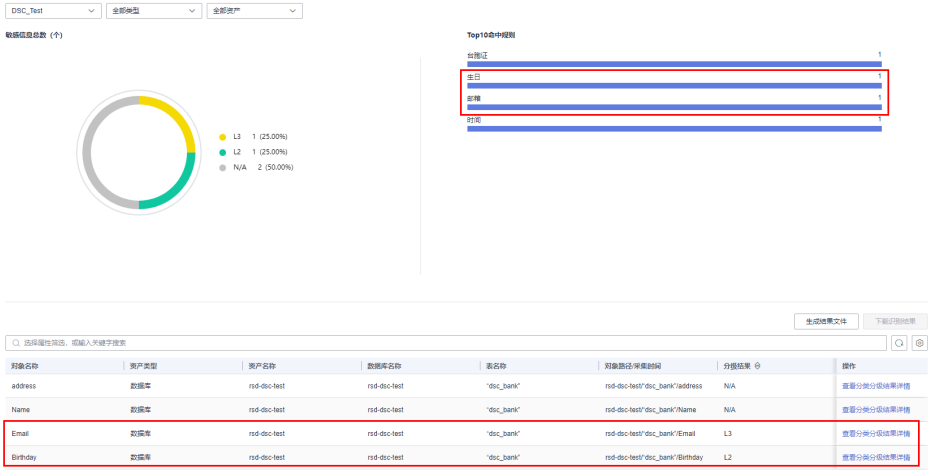
参数	说明	取值样例
执行计划	“识别周期”为“单次”时，显示该选项： • 立即执行：选择该选项，单击“确定”，系统立即执行数据识别任务。 • 定时启动：在指定时间执行一次该识别任务。	立即执行

步骤5 单击“确定”，返回敏感数据任务列表。

图 1-6 敏感数据识别任务列表

步骤6 任务状态为“识别完成”后，在该任务的操作列，单击“识别结果”，查看数据识别结果。

图 1-7 识别结果明细



如上图1-7所示，Birthday和Email列被识别为敏感数据风险。

步骤7 单击“查看分类分级结果详情”，查看结果详情。

图 1-8 分类分级结果详情

执行**步骤三：数据静态脱敏**对数据库“rsd-dsc-test”中的表“dsc_bank”的Birthday和Email列进行脱敏。

----结束

步骤三：数据静态脱敏

DSC支持对数据库、ES、MRS以及Hive等数据类型的脱敏任务，本节以创建数据库静态脱敏任务为例进行演示，如需了解其他脱敏相关的方法请参见：

- ES脱敏，请参见**创建ES脱敏任务**。
- MRS脱敏，请参见**创建MRS脱敏**。
- Hive脱敏，请参见**创建Hive脱敏**。
- HBase脱敏，请参见**创建HBase脱敏**。
- DLI脱敏，请参见**创建DLI脱敏**。
- OBS脱敏，请参见**创建OBS脱敏**。

步骤1 在左侧导航树中，选择“数据资产保护 > 数据静态脱敏”，进入“数据脱敏”页面。

步骤2 将“数据库脱敏”设置为  ，开启数据库脱敏。

步骤3 单击“新建任务”，进行“数据源配置”。

如果您想脱敏后生成一张完整的表，此处勾选所有数据类型。

图 1-9 数据源配置

步骤4 单击“下一步”，进行“脱敏算法配置”。

图 1-10 脱敏算法配置

步骤5 单击“下一步”，进入“脱敏周期”页面，配置脱敏周期。

图 1-11 脱敏周期配置

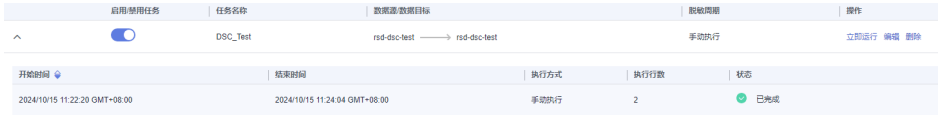
步骤6 单击“下一步”，进行“数据目标配置”，配置脱敏后生成的表的存放位置。

图 1-12 数据目标配置

步骤7 单击“完成”，返回到数据库脱敏任务列表，单击  ，启用脱敏任务，并在任务所在行的“操作”列，单击“立即运行”，执行脱敏任务。

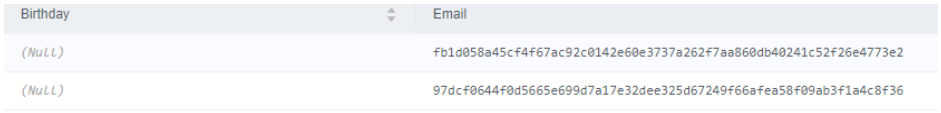
当“状态”为“已完成”时，表示脱敏成功。

图 1-13 完成识别脱敏



----结束

效果验证



2 OBS 数据安全防护最佳实践

本文介绍如何使用数据安全中心（DSC），对OBS中存储的敏感数据进行识别、分类分级和保护。

背景信息

敏感数据主要包括个人隐私信息、密码、密钥、敏感图片等高价值数据，这些数据通常会以不同的格式存储在您的OBS桶中，一旦发生泄漏，会给企业带来重大的经济和名誉损失。

DSC在您完成数据源识别授权后，从您存储在OBS的海量数据中快速发现和定位敏感数据，对敏感数据分类分级并统一展示，同时追踪敏感数据的使用情况，并根据预先定义的安全策略，对数据进行保护和审计，以便您随时了解OBS数据资产的安全状态。

应用场景

- 敏感数据识别

  OBS中存储了大量的数据与文件，但无法准确获知这些OBS数据中是否包含敏感信息以及敏感数据所在的位置。

  您可以使用DSC内置算法规则，或根据其行业特点自定义规则，对其存储在OBS中的数据进行整体扫描、分类、分级，并根据结果做进一步的安全防护，如利用OBS的访问控制和加密功能等。

- 异常检测和审计

  DSC可检测敏感数据相关的访问、操作、管理等异常，并提供告警提示信息，用户可以对异常事件进行确认和处理。通常情况下，以下行为均被视为异常事件：

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

操作步骤

步骤1 **购买数据安全中心服务**。

步骤2 登录**管理控制台**。

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

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OBS资产所在行的“操作”列，单击 开启授权。

步骤6 添加OBS资产，具体的操作请参见**添加OBS资产**。

步骤7 在左侧导航树中，选择“敏感数据识别 > 识别任务”，单击“新建任务”，配置敏感数据的扫描任务。

“数据类型”选择**步骤6**中添加的OBS资产，其他配置请参见**创建敏感数据识别任务**。

表 2-1 新建任务参数说明

参数	说明	取值样例
任务名称	您可以自定义敏感数据识别任务名称。 任务名称需要满足以下要求： ● 4~255个字符。 ● 字符可由中文、英文字母、数字、下划线或中划线组成。 ● 开头需为中文或者字母。 ● 任务名称不能与已有的任务名称重复。	test
数据类型	选择识别的数据类型，可多选。 ● OBS：授权DSC访问您的华为云OBS资产后，DSC将对华为云OBS里的资产进行敏感数据识别，添加OBS资产的相关操作请参见**添加OBS资产**。 ● 数据库：DSC将对已授权的数据库资产进行敏感数据识别，授权数据库资产的相关操作请参见**授权数据库资产**。 ● 大数据：DSC将对已授权的大数据资产进行敏感数据识别，授权大数据源资产请参见**授权大数据资产**。 ● MRS：DSC将对已授权的MRS资产进行敏感数据识别，授权MRS资产请参见**授权大数据资产**。 ● LTS：DSC将对已授权的LTS资产进行敏感数据识别，添加日志流请参见**添加日志流**。	OBS
识别模板	选择内置模板或者自定义模板，DSC将根据您选择的模板对数据进行分级分类展示。添加模板请参见**新增识别模板**。	华为云数据安全分类分级模板

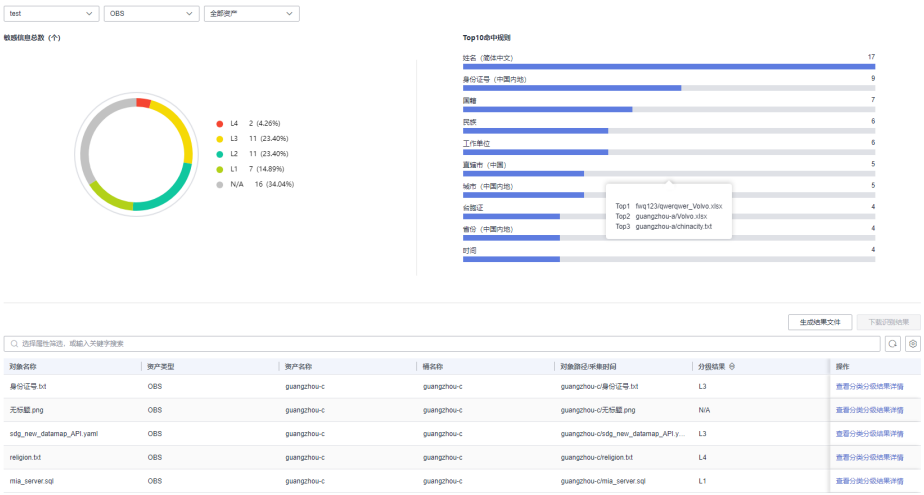
参数	说明	取值样例
识别周期	设置数据识别任务的执行策略： ● 单次：根据设置的执行计划，在设定的时间执行一次该识别任务。 ● 每天：选择该选项，即在每天的固定时间执行该识别任务。 ● 每周：选择该选项，即在设定的每周这一时间点执行该识别任务。 ● 每月：选择该选项，即在设定的每月这一时间点执行该识别任务。	单次
执行计划	“识别周期”为“单次”时，显示该选项： ● 立即执行：选择该选项，单击“确定”，系统立即执行数据识别任务。 ● 定时启动：在指定时间执行一次该识别任务。	立即执行

步骤8 在左侧导航树中选择“敏感数据识别 > 识别任务”，进入识别任务页面。

步骤9 单击目标任务“操作”列的“识别结果”查看识别结果。

在页面左上角，识别任务名称选择dsc-test、资产类型选择OBS、资产名称选择全部资产，筛选OBS敏感数据识别结果，识别结果如图2-1所示。

图 2-1 识别结果明细



步骤10 在目标扫描对象所在行的“操作”列，单击“查看分类分级结果详情”，进入“分类分级结果详情”弹框，如图2-2所示。

图 2-2 分类分级结果详情

1. 在异常告警列表中，根据风险等级查看异常情况，排查是否存在高风险事件。具体操作请参见**OBS使用审计**。
2. 在OBS控制台，针对存在风险的桶或文件，修改读写权限。具体操作请参见**桶策略**。

----结束