什么是敏感数据保护

更新时间：2020-12-08 21:34:44

敏感数据保护SDDP（Sensitive Data Discovery and Protection），在满足等保V2.0“安全审计”及“个人信息保护”的合规要求的基础上，为您提供敏感数据识别、数据安全审计、数据脱敏、智能异常检测等数据安全能力，形成一体化的数据安全解决方案。

敏感数据主要包括客户资料、技术资料、个人信息等高价值数据，这些数据以不同形式存在于您的资产中。敏感数据的泄露会给企业带来严重的经济和品牌损失。

SDDP可根据预先定义的敏感数据关键字段，扫描MaxCompute、OSS、阿里云数据库服务（RDS、DRDS、PolarDB、OceanBase、表格存储）和自建数据库中的数据，通过敏感数据规则中的命中次数来判断是否属于敏感数据。

# 敏感数据安全防护方案

更新时间：2020-07-23 16:42:13

[**本页目录**](javascript:void(0))

* [前提条件](https://help.aliyun.com/document_detail/151887.html?spm=a2c4g.11186623.2.19.2bbc679dZJrben#h2-url-1)
* [背景信息](https://help.aliyun.com/document_detail/151887.html?spm=a2c4g.11186623.2.19.2bbc679dZJrben#h2-url-2)
* [应用场景](https://help.aliyun.com/document_detail/151887.html?spm=a2c4g.11186623.2.19.2bbc679dZJrben#title-cmj-a4e-d0r)
* [方案优势](https://help.aliyun.com/document_detail/151887.html?spm=a2c4g.11186623.2.19.2bbc679dZJrben#title-s4y-s2y-0c7)
* [操作步骤](https://help.aliyun.com/document_detail/151887.html?spm=a2c4g.11186623.2.19.2bbc679dZJrben#title-rbz-8ym-9pz)

本文介绍如何将阿里云对象存储OSS与阿里云敏感数据保护SDDP（Sensitive Data Discovery & Protection）结合，对敏感数据进行识别、分类、分级和保护。

## 前提条件

* 已开通SDDP

开通步骤请参见[快速入门](https://help.aliyun.com/document_detail/89531.html?spm=a2c4g.11186623.2.15.1bfc7acb6NFqsB#task-t4v-4rs-sfb)。

* 已开通OSS

开通步骤请参见[开通OSS服务](https://help.aliyun.com/document_detail/31884.html#task-njz-hf4-tdb)。

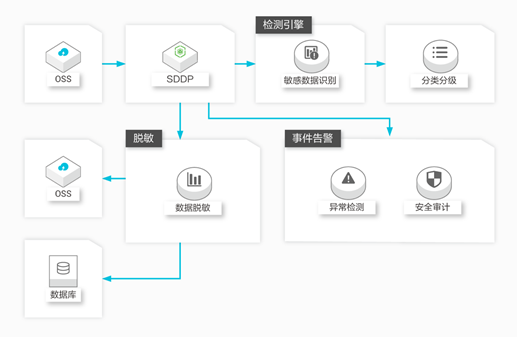
## 背景信息

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各类存储系统中。如何更好地发现、定位、保护这些数据，对您的企业非常重要。OSS本身提供了细粒度的[权限管理](https://help.aliyun.com/document_detail/31867.html#concept-e4s-mhv-tdb)和[数据加密](https://help.aliyun.com/document_detail/31871.html#concept-lqm-fkd-5db)等数据安全选项，[同城冗余存储](https://help.aliyun.com/document_detail/90589.html#concept-ufs-g5m-cfb)、[跨区域复制](https://help.aliyun.com/document_detail/31864.html#concept-zjp-31z-5db)、[版本控制](https://help.aliyun.com/document_detail/109695.html#concept-jdg-4rx-bgb)等数据保护机制，[访问日志存储](https://help.aliyun.com/document_detail/31868.html#concept-t3h-4hd-5db)和[实时日志查询](https://help.aliyun.com/document_detail/99277.html#concept-eyb-1n5-1gb)等记录监控与审计能力。若您希望更好的针对敏感数据进行识别、分类、分级和保护，可使用OSS+SDDP的方案。

SDDP与OSS结合使用，在您完成数据源识别授权后，从您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，以便您随时了解数据资产的安全状态。更多详情请参见[什么是敏感数据保护（SDDP）](https://help.aliyun.com/document_detail/89077.html?spm=a2c4g.11186623.2.24.1bfc7acb6NFqsB#concept-rzh-xx4-y2b)。

**说明** 当您完成OSS资产授权后，在OSS数据初次接入扫描时，SDDP会对已授权的数据源执行全量扫描并收取全量扫描费用。初次扫描任务完成后，SDDP仅对该数据源中新增或修改的文件收取扫描费用，因此计费会大幅降低。详细的计费方式请参见[包年包月计费](https://help.aliyun.com/document_detail/145733.html#concept-2336033)。

## 应用场景

OSS与SDDP结合的常见场景如下：[](http://static-aliyun-doc.oss-cn-hangzhou.aliyuncs.com/assets/img/zh-CN/2373945951/p81537.png)

* 敏感数据识别

企业拥有大量数据，但无法准确获知这些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OSS结合SDDP的方案，利用SDDP内置算法规则或根据行业特点自定义规则，对存储在OSS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。例如利用OSS的访问控制和加密等功能，对数据进行保护。

* 数据脱敏

数据进行对外交换供他人分析或使用时，未进行脱敏处理会导致敏感信息的意外泄漏。OSS与SDDP结合的方案，可以支持灵活多样的内置或自定义脱敏算法，可实现生产类敏感数据脱敏后，供开发、测试等非生产环境使用的场景，并确保脱敏后的数据保真可用。

* 异常检测和审计

SDDP可通过智能化的检测模型，对访问OSS中敏感数据的行为进行检测和审计。为数据安全管理团队提供相关告警，并基于检测结果完善风险预判和规避方案。

## 方案优势

* 可视化
  + 提供敏感数据识别结果可视化能力，让企业数据安全状态一目了然。
  + 数据访问监控和异常审计可追溯，降低企业数据安全风险。
  + 提升整体企业数据资产安全透明度，强化企业数据管理能力。
  + 降低数据安全运维成本，为制定企业数据安全策略提供强有力的数据支撑。
* 智能化
  + 运用大数据和机器学习能力，通过智能化算法，对敏感数据和高风险活动（例如数据异常访问和潜在的泄漏风险）进行有效识别和监控，并提供修复建议。
  + 提供定制化的敏感数据识别能力，便于客户自定义识别标准，实现精准识别和高效防护。
  + 将复杂的数据格式和内容汇总至统一的数据风险模型，并以标准化的方式呈现，实现企业关键数据资产的防御。
* 云原生
  + 生于云，长于云，充分利用云上服务优势，并支持云上多类型数据源。
  + 相较于传统软件化部署方式，OSS+SDDP方案服务架构更为健壮、可用性更高、成本也更低，同时系统自身安全性也更好。

## 操作步骤

1. 登录[敏感数据保护控制台](https://yundun.console.aliyun.com/?p=sddp#/overview)。
2. 在左侧导航栏单击**资产保护授权**。
3. 在**OSS**页签下单击**未授权**。
4. 选中需要授权的OSS Bucket，并单击**批量授权**。

您也可以单击目标Bucket右侧**授权**，为单个Bucket授权。

1. 在**对于选中资产批量处理**页面，根据您的需求配置以下参数：
   * **识别权限**：开启或关闭SDDP识别选中资产敏感数据的权限。
   * **审计权限**：开启或关闭SDDP对选中资产进行数据审计的权限。
   * **脱敏权限**：开启或关闭SDDP对选中资产进行敏感数据脱敏的权限。
   * **敏感数据采样**：设置SDDP对选中资产进行敏感数据采样的条数。可选取值：0条、5条、10条。
   * **审计日志存档**：设置选中资产的审计日志保存时间。可选取值：30天、90天、180天。

**说明** 设置审计日志存档时间无需您额外开通日志服务。

1. 单击**确认**。

完成资产授权后，SDDP将会对开启授权的OSS存储空间中的文件执行敏感数据检测。如果该存储空间是首次开启授权，SDDP将会自动触发全量扫描并收取全量数据扫描的费用。相关内容请参见[数据源授权完成后需要多长时间完成扫描？](https://help.aliyun.com/document_detail/90847.html#section-hv1-nu2-vqi)

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

**说明** SDDP仅对已授权的Bucket进行数据扫描和风险分析。

1. 添加安全策略。

扫描完成后，您可以根据敏感数据扫描结果进行相应的安全加固措施。例如[配置数据加密](https://help.aliyun.com/document_detail/108880.html#concept-r55-np5-xgb)、添加[访问权限](https://help.aliyun.com/document_detail/31867.html#concept-e4s-mhv-tdb)等。您也可以根据需要，在SDDP控制台开启OSS安全审计功能，实现对OSS中存储的敏感文件的异常行为检测和智能安全审计。详情请参见[审计规则](https://help.aliyun.com/document_detail/142128.html#task-2330234)和[自定义规则](https://help.aliyun.com/document_detail/142165.html#task-2330518)。