



# 数据安全中心 最佳实践

文档版本: 20220114



## 法律声明

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

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

## 通用约定

格式	说明	样例
⚠ 危险	该类警示信息将导致系统重大变更甚至故 障,或者导致人身伤害等结果。	⚠ 危险 重置操作将丢失用户配置数据。
⚠ 警告	该类警示信息可能会导致系统重大变更甚 至故障,或者导致人身伤害等结果。	警告 重启操作将导致业务中断,恢复业务 时间约十分钟。
〔〕) 注意	用于警示信息、补充说明等,是用户必须 了解的内容。	大意 权重设置为0,该服务器不会再接受新 请求。
⑦ 说明	用于补充说明、最佳实践、窍门等,不是 用户必须了解的内容。	<ul><li>⑦ 说明</li><li>您也可以通过按Ctrl+A选中全部文件。</li></ul>
>	多级菜单递进。	单击设置> 网络> 设置网络类型。
粗体	表示按键、菜单、页面名称等UI元素。	在 <b>结果确认</b> 页面,单击 <b>确定</b> 。
Courier字体	命令或代码。	执行 cd /d C:/window 命令,进入 Windows系统文件夹。
斜体	表示参数、变量。	bae log listinstanceid
[] 或者 [alb]	表示可选项,至多选择一个。	ipconfig [-all -t]
{} 或者 {a b}	表示必选项,至多选择一个。	switch {act ive st and}

## 目录

1.0SS数据安全防护最佳实践	 05
2.数据防泄漏典型案例	 07

## 1.0SS数据安全防护最佳实践

本文介绍如何使用,对OSS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OSS Bucket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OSS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OSS数据资产的安全状态。

#### 应用场景

#### 敏感数据识别

云端OSS中存储了大量的数据与文件,但无法准确获知这些OSS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,如利用OSS的访问控制和加密功能等。

● 数据脱敏

数据进行对外交换供用户分析或使用时,未进行脱敏处理,导致敏感信息的意外泄漏。

DSC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到开发、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

在云端OSS中存在海量数据的场景中,无法准确获知数据被谁使用,以及数据使用上是否存在异常行为或 数据泄漏。

DSC通过智能化的检测模型,针对OSS中敏感数据的访问,实现异常行为检测和审计,同时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能力。

### 方案优势

- 可视化:提供敏感数据识别结果可视化能力,让企业数据安全现状一目了然。
  - 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,强化企业数据治理能力。
  - 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,通过智能化的算法,对敏感数据和高风险活动,诸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**: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,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。

使用说明

DSC目前提供包年包月的计费模式。1000 GB存储量收费为1000元/月。

#### 操作步骤

1. 开通服务。

具体操作,请参见购买数据安全中心。

- 2. 登录数据安全中心控制台。
- 3. 在左侧导航栏,选择数据保护授权 > 数据资产授权。
- 4. 在OSS页签下单击未授权,同时选中多个Bucket,为您需要扫描的OSS Bucket执行批量授权。 您也可以单击目标Bucket右侧授权,为单个Bucket授权。具体操作,请参见OSS文件桶访问授权。 成功完成授权后,在2小时内启动扫描。扫描时长将由您所需扫描的数据量决定。更多信息,请参见数 据源授权完成后需要多长时间完成扫描。

在DSC扫描数据的过程中,已经完成扫描的阶段性结果,会展现在**概览**页面。更多信息,请参见控制台 概览。

5. 在敏感数据识别 > 敏感数据资产页面的OSS页签中,查看OSS敏感数据扫描结果(查看OSS敏感数据)。您还需要根据扫描结果对敏感文件和有风险的事件进行及时的处理,避免数据安全隐患。

处理建议如下:

i. 及时查看高敏感风险等级的Bucket中, 各个敏感等级对应的敏感文件数量, 以及每个敏感等级命中 数量最多的识别规则和对应的文件数量。

OSS ( 26 )	RDS (	(21)	MaxCompute	(1)	自建数据	踳(0)	DRI	DS(2)	PolarDB (4)	OTS (2)	OceanBase	(0)
区域	$\sim$	Bucket		高	故感 ×	$\sim$	起始日期	]	- 1	吉東日期	Ê	捜索
王宣												
区域		Bucket		总3	7件数 ♪	Œ	感等级	敏感文件数	1	最后扫描时间		操作
毕起2(北京)		sddp fi	nancial	2		(	53	1		2020年11月1	8日 12:19:58	文件
毕东2(上海)		test strange	sddp	1		(	规则命中	Top5 : 1) (CustomBa	nkCard11)(性别1)	7月4E	18:32:31	文件
5463(张家口)		sddp	Contract of Contract of Contract	469			邮箱10	(信用卡10)		11月1	8日 08:30:34	文件

- ii. 单击**文件详情**,查看该敏感文件的名称以及其他相关信息(例如:文件类型、文件大小等),确认 该文件是否存在数据安全风险。
- iii. 在**原始日志**列表中,根据敏感文件的名称查看客户端对其执行的相关操作。有必要的情况下,记录 执行该操作的客户端IP地址,排查是否存在可疑用户。
- iv. 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。
- v. 对敏感数据进行脱敏。具体操作,请参见静态脱敏、动态脱敏。
- vi. 在OSS控制台,针对存在风险的Bucket或文件,修改读写权限。具体操作,请参见修改存储空间读 写权限、设置文件读写权限ACL。

⑦ 说明 您还可以设置服务端加密,在OSS上传文件时,就对该文件进行加密,避免敏感数 据泄露。关于如何设置服务端加密,请参见设置服务器端加密。

## 相关文档

### 包年包月计费

常见问题总览

## 2.数据防泄漏典型案例

数据安全中心数据泄漏检测可以发现和避免由于身份冒用、越权操作、违规操作、误操作、基础设施不可 控、故意泄漏、配置失当、安全漏洞等引起的数据泄露事件,当异常检测上报告警后,您需要根据原始日志 排查相关内容的合理性。

## 常见数据泄露原因

在获得用户授权后,数据防泄漏检测可处理以下类型的问题:

- 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
  - 在职员工、待离职员工、合作伙伴、外包人员盗窃数据
  - 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安全漏洞
  - 配置不当导致的外部攻击
  - 敏感数据越权访问和存储

## 操作指导

请参见以下操作指导,查看数据安全中心数据泄漏检测结果及异常检测上报的告警,根据原始日志排查相关 内容的合理性。

- 1. 登录数据安全中心控制台。
- 2. 在左侧导航栏,选择数据资产授权 > 数据资产授权。
- 3. 在云上托管页面,添加资产授权并开启识别权限和审计权限。

关于添加资产授权的具体操作,请参见数据资产授权。

数据安全中心		数据安全中心 / 数据资产授	权 / 云上托管								
概览		云上托管									
数据资产授权	^	山桥平向亦居来。 制众 八			A100400 000 7	<b>B</b> 0.000					+ 04 77
数据资产授权		当前开启关例数:剩余 93	17、已经用117、可保	出一口221年11月政策11年	J⊼102400.00G, E	.m0.00G					云购头
授权账密管理		OSS(3) RDS(1)	RDS-PPAS(0)	DRDS(0)	PolarDB(0)	OTS(0)	自建数据库(0)	MaxCompute(0)	ADB-PG(0)	adb-my $<$ >	批量密码导入
数据库审计	^	已授权 3 未授权 C	区域	✔ 实例 /	Bucket	授权状态	5 ~	数据资产授权 🗸	搜索重置		
C100		批量操作 资产同步	+								
A100		定例 / Bucket	区域	状态	识别权限	的納权限	Ocr权限	审计权限 🙆	识别孚样展示数	审计日志在档	操作
云原生数据审计	^		(Killing (Junks)		517751ARK	BARMANA			E A A	44 FT 62 (547-13)	Den 1 P
审计概览			平162(北京)	♥已授权					5 宗 🗸	用超往	取消投权
原始日志			华东2(上海)	◎ 已授权					5条 ~	30天 ~	取消授权
会话信息		<ul> <li>Bartinetti</li> </ul>	华东1(杭州)	◎ 已授权					5条 ~	30天 ~	取消授权
异常审计告警								_	共3条数据每]	〔显示 20 ∨	< 1 >
审计规则											
敏感数据发现	^										
敏感数据资产											8
敏感数据搜索											
识别任务监控											
识别规则											

- 4. 在左侧导航栏,选择数据防泄漏 > 泄漏风险告警。
- 5. 在泄漏风险告警页面,查看异常检测上报的告警。

数据安全中心		数据安全中心 /	数据防泄漏 / 汎	世漏风险告誓							
概范		泄漏风	<b>俭告</b> 警								
数据资产授权	~	流转异常	行为异常	配置异常	自定义异常						
数据库审计	~										
云原生数据审计	$\sim$	1									
敏感数据发现	^										
敏感数据资产											
敏感数据搜索											
识别任务监控		0									
识别规则							RDS 未处理风险数	白名单IP被设置为公开访问 日本単のにない	确认误报数		
数据脱敏	^										
静态脱敏		<b>本</b> /+米田	×	所办中本	~	ID		却有期	(	<b></b>	音调 垦出
动态脱敏				MALAVEA		10		AE24414743	4475470		
脱敏模板		使用账号				事件类型	事件子类型		告罄时间	所处状态	操作
脱敏算法		10080000		CADAR		配置异常	RDS白名单IP	被设置为公开访问	2021年5月25日 07:40:37	待处理	查看详情 处理
提取水印											
数据防泄漏	^									वगः ।	
泄漏风险告答											

当发现存在告警项后,单击异常事件所在行的**查看详情**。关注事件描述和对象信息,或单击原始日志进行评估和确定事件风险和影响。

泄漏风险详情	
泄漏风险信息	
事件类型	配置异常
事件子类型	RDS白名单IP被设置为公开访问
责任人账号	加入白名单
告警时间	2021年5月25日 07:40:37
处理完成日期	
处理人	
对应产品	RDS
所处状态	待处理
备注	
原始日志	
<b></b>	
实例	the face of a Discontineers
敏感字段类型 IP地址,日期	未校验的身份证号, 统一社会信用代码, 车牌号, MAC地址, 手机号, 港澳通行证, 地址, 身份证, 邮箱, 营业执照号码, 姓名, 银行卡,
事件描述	
异常偏差描述	
实例(	IP白名单存在规则0.0.0.0/0。
事件风险敞口	
该实例IP白名单存在	0.0.0.0/0,则任何外部人员都可以连接到该实例,进行密码的暴力破解。
事件处置建议方案	ξ.
1、通过本产品,与1	须目负责人核查该实例中的敏感数据的分布情况,并根据分布情况确认是否设置为公开。

排查后,在泄漏风险告警页面,单击异常事件所在行的处理,设置处理记录,单击处理完成。
 设置处理记录时,您还可以进行账号封禁、移除白名单等操作。

泄漏风险告警		×
事件核查结果 * ● 确认异常并已处理	() 误报	
处理方式 账号禁用([ ])		
封禁时常	分钟封禁历史	
移除白名单(100.104. ,100.104.2 ,100.104.2 ,100.104.2 ,11.63.2		
处理记录		
添加事件处理记录	<ul> <li>选择后将对该泄漏风险进行检测强化。(增加准确性的同时,漏报率也会有所上升。)</li> </ul>	Ŧ
处理完成		

- 7. 在左侧导航栏,选择**设置 > 白名单**。
- 在白名单页面,单击新增白名单。在新增白名单对话框,配置白名单。
   配置白名单时,可以对一些资产账号加白,不进行审计和异常检测。

数据安全中心	<b>普遍安全中心</b> / 设置 / 白名单						
相比	白名单						
整運費产賬权	新城合名集 白色単素型 >	新揽白名单		×			
数据库审计		814L11+					
云原生数据审计	白名单	• 白名单类型	服号	~	a tu et iki	操作	
辅感数据发现		• 资产类型	RDS	~			
21.16793.92		• 实例	请选择	~			
黄旗防泄漏		• 账号	请输入				
教提安全实验室							
报表中心				ikaz Reiń			
包置							
邮件报告							
实时告誓通知							
白名单							_
							9
							8

- 9. 在左侧导航栏,选择设置 > 实时告警通知。
- 10. 在**实时邮件告**警页面,单击新增告警配置。在新增告警通知配置面板,配置接收邮箱。

当有异常告警事件,设置的邮箱接收人将会第一时间收到邮件。

数据安全中心	教授安全中心 / 设置 / 实际监管通知			新增告警通知	印配置			×
HX.	实时告警通知			* 告望方式	<ul> <li>al 16</li> </ul>			
就通信F 1010	新增合整配置 族教者采取 、		胡顿人	•邮件地址验证	test@aliyun.com		获取验证码	
元商生計測设计	- 横纹客	告答类型	54		验证成功的邮箱自动添加到收代	牛人列表。无用调	次验证	
新香秋级发现					请辅入验证码	验证		
at an an an			1	• 接收人	可选接收人		已选接收人	
数据防过器			here					
数据安全实验室			没有直击的		智无数据		智无数据	
报表中心								
19.22							0現	
影件报告 <b>实时告誓通</b> 知				* 告留失型	☑ 异常审计告誓 □ 泄漏;	风险古景		
889				* 告望等级	■英 □中 □任			_
				* 告營次致限制	10			
					24小时内触发同一规则量多发; 警计数在每天零点清零,若不到 0。	送的次数: 有效注 思接收告警, 请判	直围:0-10, 告 F這项设置为	8
				012 U3	n			

## 典型案例

以下案例均为产品模拟的告警截图。

配置不当风险(某金融公司)

- 问题描述: 数据安全中心检测到Bucket 配置不当, 在控制台和邮件中告警。
- **排查结果**:该公司安全管理员根据告警提示进入对应Bucket后,根据敏感数据识别结果,排查对应文件的 业务情况后确定不能将文件公开,否则会导致数据泄漏。
- 处理方法:选择将敏感文件挪出后,在OSS控制台上删除Bucket内文件或者在数据安全中心控制台的泄漏 风险告警页面单击异常事件所在行的处理,一键将Bucket设置为私有,避免因为Bucket公开导致的敏感

数据泄漏风险。

误操作(某银行)

- 问题描述: 数据安全中心检测到Bucket公开, 且存在AK、SK信息, 在控制台和邮件中告警。
- **排查结果**:发现APK包里写入了AK、SK,且APK包在百度可以公开下载。该AK、SK权限可以访问所有的 OSS Bucket,导致几百TB的数据存在数据泄漏风险。
- 处理方法:在AccessKey管理控制台紧急停用AK、SK,修改APK程序,排除数据泄漏风险。

事件类型	权限使用异常
事件子类型	配置失当-OSS敏感Bucket被设置为公开
责任人账号	
告警时间	2019-10-29 03:17:06
处理完成日期	
处理人	
对应产品	OSS
所处状态	待处理
事件对象信息	
Bucket名称	
最高敏感等级	4
敏感文件数量	10
敏感字段类型	AccessKeySecret(2), 貸份(62), 城市(990), 身份证(2), 性别(84)
敏感文件类型	Zip压缩文件(10)
事件描述	
异常描述	

违规操作(某互联网公司)

- 问题描述: 数据安全中心检测到UA使用异常, 收到邮件告警。
- **排查结果**:查看数据安全中心日志,排查出有内部员工通过 电报App将文件分享出去。
- 处理方法:在OSS控制台将文件下载链接取消,并且编写自定义异常规则,对非常规UA下载进行预警。



### 身份冒用(某教育公司)

• 问题描述: 数据安全中心检测到异常地址访问。

数据资产授权	$\sim$						
		数据安全中心 / 数据防泄漏 / 泄漏风险告答					
数据库审计	~	泄漏风险告警					
云原生数据审计	~						
敏感数据发现	^	流转异常 行为异常 配置异常 自	自定义异常				
敏感数据资产							
敏感数据搜索		1					
识别任务监控							
识别规则							
数据脱敏	^						
静态脱敏		0					
				风险数 🛑 巴外理风险数 🧰 确认语	≣#8%7		
动态脱敏							
脱敏模板							
脱敏算法		事件类型 > 所处状态	✓ ID	起始日期	- 结束日期	i oi	导出
提取水印		使用账号	事件类型事件于	- 类型	告警时间	所处状态	操作
数据防泄漏	^	And all a location of a location of the location of					
泄漏风险告警		of and particular	ELCO INC	11 (14 (1) (1) (1)	2021年5月	待处理	查看详情处理
泄漏检测模型						合计: 1	(上一页 1 下一页
数据安全实验室	^						
数据资产地图							

- **排查结果**:经确认用户本人未进行对应操作,排查后发现地址是出口IP,出口IP无法定位到内部具体执行人。
- 处理方法:修改配置文件中的AK后,在AccessKey管理控制台紧急停用AK、SK,终止异常访问。



#### 突发测试(某物流公司)

#### • 问题描述: 数据安全中心检测到文件下载量异常。

数据资产授权	~	数据安全中心 / 数据防泄漏 / 泄漏风险告答										
数据库审计	$\sim$	洲海风险生獒										
云原生数据审计	~											
敏感数据发现	^	流转异常 行为异常 配置异常 自定义异常										
敏感数据资产												
敏感数据搜索		1										
识别任务监控												
识别规则												
数据脱敏	^											
静态脱敏		0	The second second									
动态脱敏			🛑 未处理风险数 🛑 已处理风险数 🛑 确认课程数									
脱敏模板												
脱敏算法		事件类型 > 所处状态 >	ID 起始日期	- 结束日期	曲 <b>查询</b> 导出							
提取水印		伸田畔亭	事件 <del>发</del> 出 事件 <del>之类</del> 刑	告题时间	<b>新小社本 播作</b>							
数据防泄漏	~	6-4KET.34	ALL-2017 ALL-1 2017		H1960 22 1981 ₩							
泄漏风险告警			En manual const	2021年5月	待处理 查看详情 处理							
泄漏检测模型					合计:1 く 上一页 1 下一页							
数据安全实验室	^											
数据资产地图												

- 排查结果:员工在进行压力测试,因此产生的事件较多。
- 处理方法:未发现违规。

合作方在家办公(某制造企业)

• 问题描述: 数据安全中心检测到文件下载量异常。

数据资产授权	~	数据安全中心 / 数据防泄漏 / 泄漏风险苦警			
数据库审计	~	半足又於牛螫			
云原生数据审计	~				
敏感数据发现	^	流转异常 行为异常 配置异常 自定义界	异常		
敏感数据资产					
敏感数据搜索		1			
识别任务监控					
识别规则					
数据脱敏	^				
静态脱敏		0			
动态脱敏		🛑 未近理风险数 🛑 已处理风险数 🛑 淪认误极数			
脱敏模板					
脱敏算法		事件类型 > 所处状态 >	r ID 起机	· 结束日期	<b>童狗</b> 导出
提取水印		使用账号	事件类型事件子类型	告警时间	所处状态 操作
数据防泄漏	^	Inclusive Conclusion (inclusion, Conclusion,			
泄漏风险告警		- Contraction	tere manage	2021年5月	待处埋 查看详情 处理
泄漏检测模型					合计:1 < 上一页 1 下一页
数据安全实验室	^				
数据资产地图					

- 排查结果:合作方员工在家未经审批下载了大量文件进行办公。
- 处理方法:通过数据安全中心控制台的云原生数据审计 > 原始日志页面中的审计日志持续监控后续行为,观察是否有违规行为。