ALIBABA CLOUD

阿里云

操作审计
最佳实践

文档版本：20220708

阿里云

法律声明

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

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。

2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。

3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。

4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的“现状”、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。

5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含“阿里云”、“Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。

6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

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

目录

1.保障审计的安全性 ---------- 05

1.保障审计的安全性

操作审计能够记录和查询用户在云上的事件。这些事件能够帮助企业进行日常的问题排查和安全分析，同时也是企业重要的机密数据，代表着企业云上IT管控的模型。在事件的存储和使用过程中需要防范数据篡改和非法访问。您需要启用必要的安全防护措施和安全管理办法，以确保审计本身的完备性以及事件的安全性。本文为您介绍相应的安全实践建议，您可以根据对应场景进行选用。

基于跟踪的完备审计和安全分析

期望效果	解决办法	详细说明	参考文档
等保2.0要求企业将事件存储180天及以上，平台仅有的90天历史事件不满足要求，需获取并存储更长时间的事件。	创建跟踪。	操作审计支持在云平台记录您最近90天的事件，如果您不进行转存保留，每过去一天就会清除最早一天的记录。当您需要存储超过90天的事件时，必须创建跟踪。 您可以创建跟踪，将事件持续投递到对象存储OSS中进行长时间存储。 跟踪也支持将事件持续投递到日志服务SLS中进行监控和分析，但如果是单纯的归档存储诉求，更推荐您存储到对象存储OSS。	• 创建单账号跟踪 • 创建多账号跟踪 • 将事件持续投递到指定服务
国家法规和行业标准要求记录全量事件。	设置跟踪的地域为全部地域，跟踪的事件类型为所有事件。	为了获取阿里云账号中所有事件的记录，建议您将跟踪的地域设置为全部地域，确保对所有地域的事件进行记录。当阿里云支持新的地域时，也将包含其中，无须进行其他设置。 由于合规要求，读操作和写操作都需要保留事件，建议您将跟踪的事件类型设置为所有事件。	• 创建单账号跟踪 • 更新单账号跟踪 • 创建多账号跟踪 • 更新多账号跟踪
• 长时间存储事件（公司IT部门或安全合规部门要求，记录超过90天的云上事件）。 • 对事件进行归档或下载（向合规部门提供近几年的事件）。 • 对敏感操作进行分析和告警。	将事件投递到对象存储OSS或日志服务SLS。	您可以创建跟踪，将事件投递到对象存储OSS或日志服务SLS。 • 对象存储OSS：帮助您低成本、长时间存储事件，根据需要进行下载和使用。 • 日志服务SLS：帮助您分析操作记录，创建统计仪表盘或针对特定事件发送短信、Email和钉钉等告警通知。	• 将事件持续投递到指定服务 • 在日志服务SLS中分析操作事件

事件的安全管理

期望效果	解决办法	详细说明	参考文档

期望效果	解决办法	详细说明	参考文档
将事件投递到对象存储OSS时，加密事件，确保云上事件的安全性。	采用KMS托管密钥加密。	当您创建跟踪并将事件投递到对象存储OSS时，默认使用OSS完全托管密钥进行加解密（SSE-OSS）。 如果您需要使用可以直接管理的加密密钥，可以使用KMS托管密钥进行加解密（SSE-KMS）。您可以进行以下操作： • 在OSS控制台创建开启服务端加密的存储空间，然后在操作审计控制台创建跟踪并将事件投递到该存储空间。 • 在操作审计控制台创建跟踪时，选择创建新的存储空间，并开启服务端加密。	服务器端加密
将事件投递到日志服务SLS时，加密事件，确保云上事件的安全性。	采用KMS托管密钥或日志服务的服务密钥加密。	当您创建跟踪并将事件投递到日志服务SLS时，操作审计会自动创建一个名为 `actiontrail_<跟踪名称>` 的日志库（Logstore）。您可以使用KMS托管密钥或日志服务的服务密钥为Logstore进行加密设置，从而加密事件。	数据加密
事件存储在OSS或SLS的期间禁止事件被修改或删除，以确保事件可靠性。	配置OSS的合规保留策略。	当您创建跟踪并将事件投递到对象存储OSS时，需要设置OSS文件的合规保留策略。例如：添加一条基于时间的合规保留策略，设置用户在保护周期内不可以修改或删除事件。 **说明** 日志服务SLS中的事件不可删除和修改，无需单独进行设置。	合规保留策略
严格控制事件的访问权限。	OSS或SLS的最小化访问授权。	当您创建跟踪并将事件投递到对象存储OSS或日志服务SLS时，需要授予阿里云账号（或RAM用户）访问OSS或SLS的权限，以便成功完成事件投递。而日常使用事件时也要将事件读权限授予相关工作人员。 建议权限配置符合最小化原则，避免不当的授权导致服务实例被删除或篡改，避免非必要人员对事件的访问。	• OSS访问控制 • SLS访问控制
严格控制审计管理员的管控权限。	合理管控操作审计管理员权限。	拥有AliyunActionTrailFullAccess权限（操作审计管理员权限）的用户，可以修改和删除跟踪。跟踪变更后将影响事件的投递，从而影响您对事件的跟踪和审计。 建议将此权限授予尽可能少的用户。	• 为RAM用户授权 • 为RAM用户移除权限