Alibaba Cloud 操作审计

教程

文档版本: 20200401

为了无法计算的价值 | [] 阿里云

<u>法律声明</u>

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。
- 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. 阿里云文档中所有内容,包括但不限于图片、架构设计、页面布局、文字描述,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
0	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。	禁止: 重置操作将丢失用户配置数据。
	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。
!	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。
Ê	用于补充说明、最佳实践、窍门 等,不是用户必须了解的内容。	道 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。	执行cd /d C:/window命令,进 入Windows系统文件夹。
##	表示参数、变量。	bae log listinstanceid
		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。	<pre>switch {active stand}</pre>

目录

法律声明	I
通用约定	I
1 使用RAM对操作审计进行权限管理	1
2 通过操作审计监控AccessKev的使用	3
3 通过操作审计监控主账号的使用	7

1 使用RAM对操作审计进行权限管理

通过RAM的权限管理功能,您可以创建自定义策略并授予RAM用户,RAM用户便可以登录操作 审计服务进行相应的操作。

前提条件

- ·进行操作前,请确保您已经注册了阿里云账号。如还未注册,请先完成账号注册。
- ·使用RAM对操作审计进行授权前,请先了解操作审计的权限定义。详情请参见#unique_4。

操作步骤

- **1.** *#unique_5*°
- **2.** *#unique_6*°

您可以根据下述权限策略示例创建自定义策略。

3. *#unique_7*°

权限策略示例

```
・示例1:授予RAM用户只读权限。
```

```
{
    "Version": "1",
    "Statement": [{
        "Effect": "Allow",
        "Action": [
            "actiontrail:LookupEvents",
            "actiontrail:Describe*",
            "actiontrail:Get*"
        ],
        "Resource": "*"
    }]
}
```

・示例2: 仅允许RAM用户从指定的IP地址发起只读操作。

```
{
    "Version": "1",
    "Statement": [{
        "Effect": "Allow",
        "Action": [
            "actiontrail:LookupEvents",
            "actiontrail:Describe*",
            "actiontrail:Get*"
        ],
        "Resource": "*",
        "Condition":{
            "IpAddress": {
               "acs:SourceIp": "42.120.XX.X/24"
        }
```

		}						
	11	2						
2	7 1							
}								

2 通过操作审计监控AccessKey的使用

```
本文将介绍如何通过操作审计将操作事件投递到日志服务(Log Service),从而实现
```

对AccessKey的监控和报警。

前提条件

进行操作前,请确保您已经注册了阿里云账号。如还未注册,请先完成账号注册。

背景信息

开通操作审计之后,可查询最近90天的操作事件,您可以通过AccessKeyId来检索事件,详情请 参见#unique_9。您也可以将操作事件投递到日志服务,从而保存更长时间。

创建跟踪

- 1. 登录操作审计控制台。
- 2. 在顶部导航栏选择您想创建跟踪的地域。



该地域将成为目标跟踪的Home地域。

- 3. 在左侧导航栏,单击操作审计>跟踪列表。
- 4. 单击创建跟踪,输入跟踪名称。
- 5. 适用跟踪到所有的区域选择是。
- 6. 事件类型选择所有类型。
- 7. 打开是否开启日志记录开关,选择投递目标为SLS Logstore。
- 8. 是否新建 SLS Project选择是,选择日志服务Project区域并填写日志服务Project名称。

说明:

此处设置的Project用于存储审计日志。您可以填写已选择地域下的Project名称,也可以输入 一个新的Project名称。

9. 单击确定。

10.在提示对话框中,单击确定。



创建跟踪需要授予访问日志服务和对象存储的权限。如果您已经授权,将不会弹出此对话框。

11在云资源访问授权页面下,单击同意授权。

成功创建跟踪后,操作审计会将所有地域的操作事件都投递到指定的Logstore中。

配置日志服务

1. 找到创建好的跟踪,单击其日志服务列下的日志分析。

您也可以通过登录日志服务控制台进行配置。

2. 输入查询语句: event.userIdentity.accessKeyId: "LTAI******eB7Z" |

select count(1) as use_ak_LTAI******eB7Z, 然后单击查询/分析。

@	● 数据加工 ① 15分钟 (相对) ▼ 分享 查询分析属性 另存为快速查询 另存为告答
✓ 1 event.userIden	tity.accessKeyId: select count(1) as use_ak 💿 💿 董銄分析
40	
20 0 45分55秒	48分15秒 50分45秒 53分15秒 55分45秒 58分15秒 00分40秒
	日志总条数: 86 查询状态: <mark>结果精确</mark>
原始日志	H志聚类 📼 LiveTail 统计图表 内容列显示 列设置 🕌
快速分析	く 时间 ▲▼ 内容
搜索	Q 1 Q 02-12 16:59:34source_: actiontrail_internal topic : actiontrail_audit_event
event	 ▼ event: 0 acsRegion: > additionalEventData: 0
event	eventid: "66CFB16F-E5F1-4735-A476- eventName: "DescribeInstances" eventName: "ces-operanl-share eventSource: "ecs-operanl-share
event	eventTime: "2020-02-12T08:59:34Z" eventType: "ApiCall" eventVersion: "1"
	日志总条数: 86, 每页显示: 20 🗸 🗸 上一页 1 2 3 4 5 下一日

- 3. 将日志另存为快速查询或另存为告警。
 - ・另存为快速查询:单击页面右上角的另存为快速查询,输入快速查询名称后,单击确定。



将日志另存为快速查询后,您可以在日志服务控制台直接选择该快速查询。

关于快速查询的详细信息,请参见#unique_10。

·另存为告警:单击页面右上角的另存为告警,根据下图在告警配置页签下进行告警配置并
 在通知页签下选择通知类型。

创建告警		×
ŧ	「答配置」 通知	
* 告警名称	alarm	5/64
* 添加到仪表盘 🖉	选择已有 V Operation Center	\sim
* 图表名称	alarm	5/64
查询语句		
* 查询区间	◎ 5分钟 (相对) ▼	
* 检查频率	■ 定间隔 > 5 + 分钟	\sim
* 触发条件 🛛	use_ak_ > 0	
高级选项 〉	支持加(+)减(-)乘(*)除(/)取模(%)运算和>,>=,<,<=,==,!=,=~,!~比较运算。 帮助	
	下一步	取消

关于告警的配置详情,请参见#unique_11。

〕 说明:

将日志另存为告警后,当满足条件便可以收到告警通知。按照上图进行告警配置后,如果 accessKeyId在5分钟内被使用过,那么就报警。

预期结果

创建的快速查询和报警均可在日志服务控制台进行快速查看和管理。



3 通过操作审计监控主账号的使用

本文将介绍如何通过操作审计将操作事件投递到日志服务(Log Service),从而实现对主账号的 监控和报警。

前提条件

进行操作前,请确保您已经注册了阿里云账号。如还未注册,请先完成账号注册。

创建跟踪

- 1. 登录操作审计控制台。
- 2. 在顶部导航栏选择您想创建跟踪的地域。

说明:

该地域将成为目标跟踪的Home地域。

3. 在左侧导航栏,单击操作审计>跟踪列表。

- 4. 单击创建跟踪,输入跟踪名称。
- 5. 适用跟踪到所有的区域选择是。
- 6. 事件类型选择所有类型。
- 7. 打开是否开启日志记录开关,选择投递目标为SLS Logstore。
- 8. 是否新建 SLS Project选择是,选择日志服务Project区域并填写日志服务Project名称。

此处设置的Project用于存储审计日志。您可以填写已选择地域下的Project名称,也可以输入 一个新的Project名称。

9. 单击确定。

10.在提示对话框中,单击确定。

蕢 说明:

创建跟踪需要授予访问日志服务和对象存储的权限。如果您已经授权,将不会弹出此对话框。 11在云资源访问授权页面下,单击同意授权。

📋 说明:

成功创建跟踪后,操作审计会将所有地域的操作事件都投递到指定的Logstore中。

配置日志服务

1. 找到创建好的跟踪,单击其日志服务列下的日志分析。



您也可以通过登录日志服务控制台进行配置。

2. 输入查询语句: event.userIdentity.type:"root-account"| select count(1) as use_root, 然后单击查询/分析。

Q	● 数据加工 ① 15分钟(相对)▼ 分享 查询分析属性 另存为快速查询 另存为告告	
v 1 event.userIdentity	y.type:"root-account" select count(1) as use_root	ŕ
24		-
0 45分55秒	48分15秒 50分45秒 53分15秒 55分45秒 58分15秒 00分4	渺
	日志总条数:86 查询状态:结果精确	
原始日志日志	深类 📾 LiveTail 統计图表 内容列显示 列设置 [1
快速分析	〈 时间 ▲▼ 内容	
 ▲ 搜索 Q 	1 Q 02-12 16:59:34source_: actiontrail_internal topic : actiontrail audit event	
event 💿	 v event: } acsRegion: " additionalEventData: } 	
event 💿	apiversion : "2014-05-26" eventId : "66CFB16F-E5F1-4735-A476- eventName: "DescribeInstances" eventSource : "ecs-openapi-share.cnaliyuncs.com"	
event 📀	eventTime: "2020-02-12T08:59:34Z" eventType: "ApiCall" eventVersion: "1"	
	日志总条数:86,每页显示:20 🗸 🖌 上一页 1 2 3 4 5 下一、	

- 3. 将日志另存为快速查询或另存为告警。
 - · 另存为快速查询:单击页面右上角的另存为快速查询,输入快速查询名称后,单击确定。



将日志另存为快速查询后,您可以在日志服务控制台直接选择该快速查询。

关于快速查询的详细信息,请参见#unique_10。

·另存为告警:单击页面右上角的另存为告警,根据下图在告警配置页签下进行告警配置并
 在通知页签下选择通知类型。

创建告警				×
ŧ	吉答配置		通知	
* 告聲名称	alarm			5/64
* 添加到仪表盘 🖉	选择已有 🛛 🗸	Operation Center		~
* 图表名称	alarm			5/64
查询语句	event.userIdentity.ty	pe:"root-account" select count	t(1) as use_root	
* 查询区间	① 5分钟 (相对) 🔻			
* 检查频率	固定间隔	× 5	+ 分钟	~
* 触发条件 🕘	use_root > 0			
高级选项 〉	支持加(+)减(-)乘(*)除(/))取模(%)运算和>,>=,<,<=,==,!:	=,=~,!~比较运算。帮!	助文档
				₿
			下一步	取消

关于告警的配置详情,请参见#unique_11。

📕 说明:

将日志另存为告警后,当满足条件便可以收到告警通知。按照上图进行告警配置后,如果主 账号在5分钟内被使用过,那么就报警。

预期结果

创建的快速查询和报警均可在日志服务控制台进行快速查看和管理。

