ALIBABA CLOUD

阿里云

操作审计

安全公告

文档版本：20201125

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.公告：部分事件从写事件变更为读事件 05
2.公告：操作事件变更资源类型定义格式 07
3.公告：操作审计控制台事件查询功能更新 09
4.公告：操作事件中增加新的资源类型定义格式 11
5.公告：操作审计不支持呈现读事件中的相关资源信息 13
6.公告：补充负载均衡实例购买、变配、续费事件 14
7.公告：操作审计暂停支持GetBucket（ListObjects）事件 16

1.公告：部分事件从写事件变更为读事件

操作审计将于2020年12月20日00:00:00起，将部分原来分类为**写类型**的事件，变更为**读类型**。此次变更优化了事件分类，帮助您提升通过操作审计控制台查询事件的效率，快速定位到真正重要的管控事件。此次变更可能会影响部分用户跟踪所投递的事件范围。

变更说明

以下事件将由**写事件**变更为**读事件**：

服务名称	服务代码	API版本号	事件名称	变更原因
内容安全	Green	2018-05-09	TextScan	对内容素材的扫描评估，并不会影响云上的产品配置和应用运行。由于此类操作为业务高频操作，并非管控操作，因此将相应事件变更为**读事件**。
			ImageSyncScan	
			ImageAsyncScan	
			VideoAsyncScanResults	
			VoiceAsyncScanResults	
			VoiceAsyncScan	
		2017-01-12	TextScan	
			ImageSyncScan	
			ImageAsyncScan	
			ImageAsyncScanResults	
		2016-12-16	ImageDetection	
			ImageResults	
		2017-08-25	ImageSyncScan	
密钥管理服务	Kms	2016-01-20	Decrypt	此类操作主要是使用密钥在客户端进行加密、解密或产生数据密钥，对密钥配置本身无影响。由于操作频率较高，可能会影响重要的**写事件**的分析，因此将相应事件变更为**读事件**。
			Encrypt	
			GenerateDataKey	
安全令牌	Sts	2015-04-01	AssumeRole	RAM角色进行管控操作时，会产生角色扮演事件，该操作并不会对RAM角色配置本身产生影响。相比于关注角色扮演事件本身，您更需要关注扮演后进行的其他操作，因此将该事件变更为**读事件**。

对您的影响

变更生效后：

- 当您查询所有事件时，上述事件会被标记为**读事件**。这使得您对**写事件**的分析更加高效，更容易定位到真正影响云上IT系统的管控事件，同时保留完整的操作事件。
- 当您在操作审计控制台的**详细事件查询**和**事件聚合搜索**页面查询历史事件时，若您指定**读写类型**为**写类型**，将不会看到上述事件的记录。
- 当您通过操作审计控制台创建跟踪，将**事件类型**选择为**写事件**时，上述事件不会投递到您指定的存储空间。如果您需要将上述事件投递到对象存储OSS或日志服务SLS，请在创建跟踪时选择**读事件**或**所有事件**。

2.公告：操作事件变更资源类型定义格式

操作审计将于2020年12月01日00:00:00起，将通过新创建跟踪投递到SLS Logstore或OSS Bucket的操作事件中referencedResources字段取值变更为仅包含以 ACS:: 为前缀的最新格式。此次变更对通过已有跟踪投递的操作事件没有影响，仅影响通过新创建跟踪投递的操作事件。

变更说明

假设您在2020年12月01日00:00:00前创建了跟踪A（已有跟踪），在2020年12月01日00:00:00后创建了跟踪B（新创建跟踪）。

- 变更前

  2020年12月01日00:00:00后通过跟踪A投递的操作事件，在referencedResources字段会包含旧版和新版两种资源类型定义格式，例如：您在阿里云上对云服务器ECS（Elastic Compute Service）实例进行了操作，则事件内容中referencedResources字段内容包含两种定义格式，具体如下：

  ```
  referencedResources: {
    Instance: ["i-bp1fadfadf***"],
    "ACS::ECS::Instance": ["i-bp1fadfadf***"]
  }
  ```

  字段含义如下：

  - Instance：操作的资源类型为实例。
  - ACS::ECS::Instance：操作的资源类型为ECS实例。
  - InstanceId：实例ID。

- 变更后

  2020年12月01日00:00:00后通过跟踪B投递的操作事件，在referencedResources字段仅包含新版资源类型定义格式。该事件通过跟踪A投递时，referencedResources字段仍与变更前一致。

  > **说明** 即使您创建跟踪后将操作事件投递到此前接收过操作事件的SLS Logstore或OSS Bucket，操作事件referencedResources字段也将仅包含新版资源类型定义格式。

  ```
  referencedResources: {
    "ACS::ECS::Instance": ["i-bp1fadfadf***"]
  }
  ```

  字段含义如下：

  - ACS::ECS::Instance：操作的资源类型为ECS实例。
  - InstanceId：实例ID。

对您的影响

此次变更仅修改了通过新创建跟踪投递的操作事件中referencedResources字段的资源类型定义格式，对通过已有跟踪投递的操作事件没有影响。

变更后，当您监控和分析操作事件时，应匹配以 ACS:: 为前缀的新版资源类型定义格式，从而避免通过新旧跟踪投递的事件分析方式不一致对您造成影响，方便长期分析操作事件。

对于此变动给您造成的困扰我们深表歉意。操作审计团队将加快升级步伐，努力为您提供更稳定、更可靠的审计服务。

3.公告：操作审计控制台事件查询功能更新

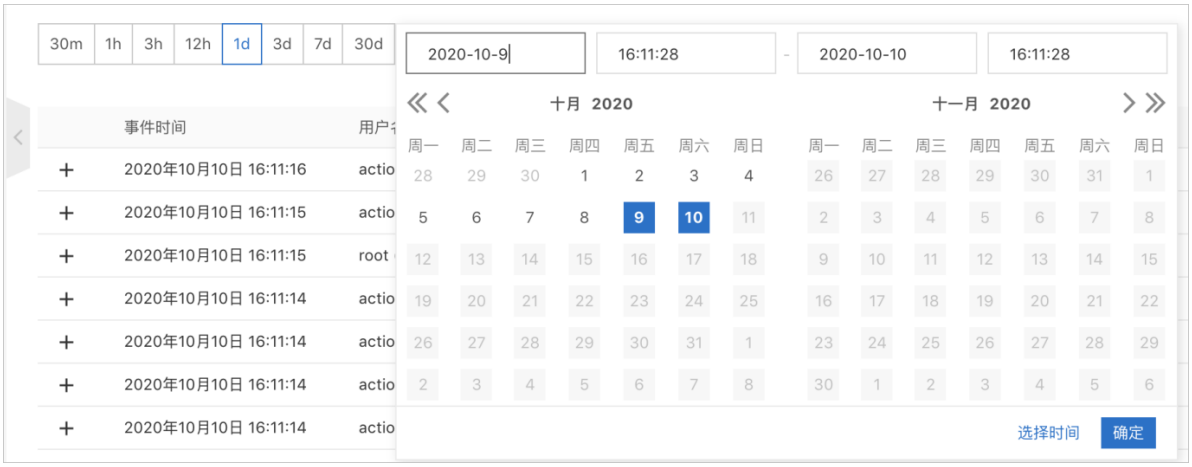
操作审计将于2020年10月14日00:00:00起，逐步上线新版事件查询功能。新版事件查询功能不再支持通过多个条件交叉查询事件，仅支持通过单个条件进行查询。同时，操作审计新增支持事件内容解析和事件聚合查询功能。此次变更仅会影响您在操作审计控制台查询事件的操作。

变更说明

- 更新了控制台事件查询方式。

  操作审计控制台原本支持通过读写类型、用户名（RAM用户）、事件名称、资源类型、资源名称、服务名称、AccessKeyId 7个条件交叉查询事件。随着数据量的增大，这种查询方式严重影响了控制台查询效率和体验。新版事件查询功能将变更为仅支持通过单个条件查询事件。

- 增加了设定时间范围的快捷键，并优化了时间设置体验。

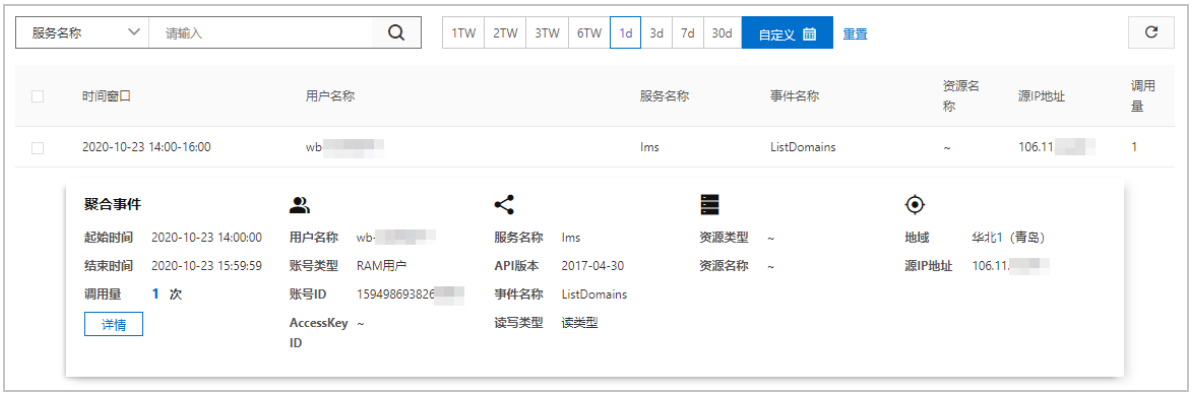


- 增加了对事件关键内容的解释，主要包含事件名称、事件涉及的资源及事件操作者。

- 新增支持事件聚合查询功能。

  操作审计会按照“when/who/what/which/where”五个维度，每两小时对事件聚合一次，方便您查询聚合结果。

  - when：事件发生时所处的聚合时间范围。以每两个整点为统计周期，支持实时查询。
  - who：事件的操作者。包括阿里云账号信息、RAM用户信息、RAM角色信息、AK信息。
  - what：事件。阿里云服务进行了哪些操作，例如：CreateInstance、DeleteInstance。
  - which：资源。对哪个（哪些）资源进行了操作。
  - where：操作了哪个地域的资源，从哪个IP发起的操作。



对您的影响

仅会影响您通过操作审计控制台查询事件的操作。

对于此变动给您造成的困扰我们深表歉意。操作审计团队将加快升级步伐，努力为您提供更稳定、更可靠的审计服务。

4.公告：操作事件中增加新的资源类型定义格式

操作审计将于2020年8月26日00:00:00起，在新产生操作事件的referencedResources字段增加新的资源类型定义格式。此次变更对原有事件没有影响，对新产生事件的原有内容也没有影响。

变更说明

变更前，如果您对云服务器ECS（Elastic Compute Service）实例进行了操作，则操作事件的referencedResources字段如下：

```
referencedResources:{
  Instance:["i-bp1fadfadf****"]
}
```

字段含义如下：

- Instance：操作的资源类型为实例。
- InstanceId：实例ID。

变更生效后，再次执行相同的操作，操作事件的referencedResources字段将增加ACS::ECS::Instance": ["i-bp1fadfadf****"]。

```
referencedResources:{
  Instance:["i-bp1fadfadf****"],
  "ACS::ECS::Instance":["i-bp1fadfadf****"]
}
```

字段含义如下：

- Instance：操作的资源类型为实例。
- ACS::ECS::Instance：操作的资源类型为ECS实例。
- InstanceId：实例ID。

变更原因

- 当前字段中资源类型的声明不准确，例如：Instance既可以表示ECS实例，也可以表示其他产品的实例。
- 在搜索事件时，当前字段定义影响搜索效率。如果不指定产品名称，仅指定资源类型Instance，将筛选出所有产品中Instance资源类型的相关事件列表。
- 变更后，在referencedResources字段增加了资源类型的唯一命名空间。例如：ACS::ECS::Instance指定阿里云平台的唯一资源类型，"ACS::ECS::Instance": ["资源ID"]指定阿里云平台的唯一ECS实例。
- 变更后的字段采用了阿里云平台统一的资源类型定义格式。

对您的影响

此次变更仅在新产生操作事件的referencedResources字段增加了新的资源类型定义格式，对原有事件没有影响，对新产生事件的原有内容也没有影响。

对于此变动给您造成的困扰我们深表歉意。操作审计团队将加快升级步伐，努力为您提供更稳定、更可靠的审计服务。

5.公告：操作审计不支持呈现读事件中的相关资源信息

操作审计将在2020年8月28日23:59:59后不再支持呈现读事件中的相关资源信息。

变更说明

读事件是用户在阿里云上的读操作事件。读操作指本身没有在云上增加、删除或修改配置的操作意图，也不会对云上配置造成变更，仅读取云上产品和资源的信息。例如：DescribeInstances、DescribeRegions、GetInstanceScreenshot等。

相关资源是操作事件所影响的资源列表。在操作审计控制台**历史事件查询**页面展开某一条事件即可查看相关资源信息。若已通过创建跟踪将日志投递到SLS Logstore或OSS Bucket中，则相关资源包含在referencedResources字段中。

本次变更后，操作审计控制台不再支持呈现读事件的相关资源信息，对应referencedResources字段为空。

变更原因

- 读事件不会造成云上配置的变更，在实际的审计工作中读操作具体读取了哪个资源的配置信息价值较低。
- 大多数读事件是批量操作，相关的资源非常多，且不具备查看和审计的可行性。
- 云上的读操作频率很高，当您通过创建跟踪将事件投递到SLS Logstore或OSS Bucket时，记录读操作的相关资源列表也将占用非常多的存储空间，花费很多存储费用。

因此，操作审计将不再支持呈现读事件中的相关资源信息，以便为您提供更简单精炼且有价值的操作事件数据。

对您的影响

- 当您在操作审计控制台查看近90天的读事件历史时，展开事件详情将看到**相关资源**为空，单击**查看事件**时referencedResources字段为空。
- 当您通过创建跟踪将读事件投递到SLS Logstore或OSS Bucket时，事件中referencedResources字段为空。

对于此变动给您造成的困扰我们深表歉意。操作审计团队将加快升级步伐，努力为您提供更稳定、更可靠的审计服务。

6.公告：补充负载均衡实例购买、变配、续费事件

操作审计即将补充发布负载均衡（Server Load Balancer）实例的购买、变配和续费事件。此前由于阿里云售卖实现路径有多种，部分售卖事件未能被跟踪记录。本次发布将补充负载均衡实例的事件，后续会陆续补充其他产品的事件。

本次发布的事件为用户通过控制台而非API进行的负载均衡实例购买、变配、续费事件，使得之前无法追踪的部分行为能够被记录，同时修复了原有事件中不包含角色信息的缺陷。

此类事件的事件类型“eventType”统一取值为“ConsoleOperation”。具体事件如下：

- 负载均衡实例的购买事件：“serviceName”=“Slb”，“eventName”=“Create”
- 负载均衡实例的变配事件：“serviceName”=“Slb”，“eventName”=“Modify”
- 负载均衡实例的续费事件：“serviceName”=“Slb”，“eventName”=“Renew”

对您的影响

自本公告发布之日起至2020年5月31日23:59:59，您将开始收到“eventType”为“ConsoleOperation”的补充事件。补充事件将与原有事件保持并行，您可以通过以下字段说明来区分。

> **说明** 在2020年5月31日23:59:59前，建议您逐步增加对补充事件的监听。

字段	原有事件	补充事件
eventName	CreateLoadBalancer和ModifyLoadBalancerInternetSpec	Create、Modify和Renew
eventType	ApiCall	ConsoleOperation
userIdentity	未正确记录角色信息	正确记录角色信息
eventSource	slb-pop.aliyuncs.com	slb.aliyuncs.com
userAgent	Java/1.8.0_152	AliyunConsole
apiVersion	2014-05-15	无

请确保2020年5月31日23:59:59后，您通过两个渠道关注了负载均衡实例（“serviceName”=“Slb”）的购买、变配、续费事件，即原有的API渠道和补充的控制台渠道。具体事件如下：

- 购买事件：“eventName”=“Create”，“eventName”:=“CreateLoadBalancer”
- 变配事件：“eventName”=“Modify”，“eventName”:=“ModifyLoadBalancerInternetSpec”
- 续费事件：“eventName”=“Renew”，“eventName”:=“CreateLoadBalancer”

一切为了更客观、更准确、更全面的审计数据构建，因数据变动对您造成困扰深表歉意，感谢您的理解与支持。

公告方：阿里云操作审计服务

公告时间：2020年3月6日

补充负载均衡实例购买事件示例


```
{
 "eventId": "1a22a4db-36b0-4738-822d-b200b84f****",
 "requestId": "1a22a4db-36b0-4738-822d-b200b84f****",
 "eventVersion": "1",
 "eventTime": "2020-02-23T07:27:49Z",
 "userAgent": "AliyunConsole",
 "eventSource":"slb.aliyuncs.com",
 "requestParameters": {
  "secureTransport": true,
  "mFAPresent": false,
  "sourceIp": "42.***.74.109",
  "regionId": "cn-hangzhou-dg-a01",
  "stsTokenPlayerUid": "****809276714915"
 },
 "eventName": "Create",
 "sourceIpAddress": "42.***.74.109",
 "acsRegion": "cn-hangzhou",
 "referencedResources": {
  "LoadBalancer": [
   "lb-bp15t2g9omw99scxa****"
  ]
 },
 "userIdentity": {
  "sessionContext": {
   "attributes": {
    "mfaAuthenticated": "false"
   }
  },
  "accessKeyId": "STS.NSmajggZdKxAYnzNx6ujC****",
  "accountId": "****809276714915",
  "principalId": "****53686294945515:yx",
  "userName": "CommonBuyAdminRole:yx_sub_acc****",
  "type": "assumed-role"
 },
 "eventType": "ConsoleOperation",
 "serviceName": "Slb",
 "__expanded": true
}
```

7.公告：操作审计暂停支持GetBucket（ListObjects）事件

操作审计将在2020年3月24日23:59:59后暂停支持GetBucket（ListObjects）事件。

GetBucket（ListObjects）事件是对象存储（OSS）的API事件，用于查询Bucket中所有文件（Object）列表。由于GetBucket（ListObjects）事件流量很大，且峰值波动频繁，当它与其他管控事件放在一起时，将影响操作审计对事件的追踪和分发性能，重要的写事件流量占比将会很少。因此，操作审计决定暂停支持GetBucket（ListObjects）事件，后续上线时间将另行公告。

对您的影响如下：

- 查询历史事件：将不再展示GetBucket（ListObjects）事件，也无法搜索。此时您更容易看到需要重点关注的写事件。
- 跟踪投递：无论您之前是否创建过跟踪，并将事件投递到对象存储（OSS）或日志服务（Log Service），本次变动都不会影响您在存储空间或日志服务中的日志。

> **说明** 在操作审计创建跟踪时，由于会占用大量存储资源，GetBucket（ListObjects）事件不支持投递到存储空间。

对于此变动给您造成的困扰我们深表歉意。操作审计团队将加快升级步伐，努力为您提供更稳定、更可靠的审计服务。