ALIBABA CLOUD

# 阿里云

## 配置审计

## 资源事件

文档版本：20201217

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<br>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<br>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<br>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<br>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`<br>*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.事件类型

## 1.1. 概述

配置审计持续且自动为您评估资源的合规性，将资源变更事件、资源不合规事件和资源快照投递事件发送到消息服务MNS的指定主题中，使您及时获知云上资源的变化和合规性。

配置审计支持的事件类型如下表所示。

| 事件类型 | 说明 |
| --- | --- |
| 资源变更事件 | 当发现资源变更时，配置审计会及时通过消息服务MNS向您发送通知。 |
| 资源不合规事件 | 当发现资源不合规时，配置审计会及时通过消息服务MNS向您发送通知。 |
| 资源快照投递事件 | 当资源快照投递到对象存储OSS的指定存储桶（Bucket）时，配置审计会及时通过消息服务MNS向您发送通知。 |

## 1.2. 资源变更事件

当配置审计发现资源变更时，会及时通过消息服务MNS向您发送通知。通过本文您可以了解资源变更事件的主要参数说明和代码示例。

资源变更事件的主要参数说明如下表所示。

| 参数 | 说明 |
| --- | --- |
| accountId | 资源所属阿里云账号ID。 |
| resourceName | 资源名称。 |
| AvailabilityZone | 资源可用区。 |
| resourceType | 资源类型。支持的资源类型请参见支持配置审计的云服务。 |
| resourceEventType | 资源变更事件的类型。取值：<br>• DISCOVERED：新建资源事件。<br>• MODIFY：修改资源事件。<br>• REMOVE：删除资源事件。 |
| resourceCreateTime | 新建资源的时间戳。时间戳转换方法，请参见Unix时间戳。 |
| RelationshipDiff | 关联资源的变更项。 |
| captureTime | 配置审计发现资源变更事件并生成日志的时间戳。时间戳转换方法，请参见Unix时间戳。 |
| configurationDiff | 资源事件的变更项。 |
| resourceId | 资源ID。 |

| 参数 | 说明 |
| --- | --- |
| Relationship | 关联资源。 |
| region | 资源所在地域。 |
| tags | 资源的标签。 |

## 新建资源

阿里云账号在对象存储OSS的上海地域新建存储桶new-bucket，在configurationDiff中显示变更前信息（null）和变更后信息。代码示例如下：


```
{
    "AccountId":120886317861****,
    "ResourceName":"new-bucket",
    "AvailabilityZone":"cn-shanghai-a",
    "ResourceType":"ACS::OSS::Bucket",
    "ResourceEventType":"DISCOVERED",
    "ResourceCreateTime":"",
    "RelationshipDiff":"",
    "CaptureTime":1605759241690,
    "ConfigurationDiff":"{\"AccessControlList\":[null,{\"Grant\":\"private\"}],\"ServerSideEncryptionRule\":[null,{\"SSEAlgorithm\":\"None\"}],\"CreationDate\":[null,\"2020-11-19T04:07:44.000Z\"],\"Owner\":[null,{\"DisplayName\":\"120886317861****\",\"ID\":\"120886317861****\"}],\"StorageClass\":[null,\"Standard\"],\"DataRedundancyType\":[null,\"LRS\"],\"AllowEmptyReferer\":[null,\"true\"],\"Name\":[null,\"new-bucket\"],\"Versioning\":[null,\"Enabled\"],\"BucketPolicy\":[null,{\"LogPrefix\":\"\",\"LogBucket\":\"\"}],\"ExtranetEndpoint\":[null,\"oss-cn-shanghai.aliyuncs.com\"],\"IntranetEndpoint\":[null,\"oss-cn-shanghai-internal.aliyuncs.com\"],\"Location\":[null,\"oss-cn-shanghai\"]}",
    "ResourceId":"new-bucket",
    "Relationship":"",
    "Region":"cn-shanghai",
    "Tags":"{}"
  }
```


## 更新资源

阿里云账号在对象存储OSS的上海地域更新存储桶new-bucket的加密方式，在configurationDiff中显示变更前信息None（不加密）和变更后信息AES256。代码示例如下：

```
{
    "AccountId":120886317861****,
    "ResourceName":"new-bucket",
    "AvailabilityZone":"cn-shanghai-a",
    "ResourceType":"ACS::OSS::Bucket",
    "ResourceEventType":"MODIFY",
    "ResourceCreateTime":"",
    "RelationshipDiff":"",
    "CaptureTime":1605779129000,
    "ConfigurationDiff":"{\"ServerSideEncryptionRule\":[{\"SSEAlgorithm\":\"None\"},{\"SSEAlgorithm\":\"
AES256\"}]}",
    "ResourceId":"new-bucket",
    "Relationship":"",
    "Region":"cn-shanghai",
    "Tags":"{}"
  }
```


## 删除资源

阿里云账号在对象存储OSS的上海地域删除存储桶new-bucket，在configurationDiff中显示变更前信息和变更后信息（null）。代码示例如下：

```
{
    "AccountId":12088631786****,
    "ResourceName":"new-bucket",
    "AvailabilityZone":"cn-shanghai-a",
    "ResourceType":"ACS::OSS::Bucket",
    "ResourceEventType":"REMOVE",
    "ResourceCreateTime":"",
    "RelationshipDiff":"",
    "CaptureTime":1605860519000,
    "ConfigurationDiff":"{\"AccessControlList\":[{\"Grant\":\"private\"},null],\"ServerSideEncryptionRule\":[{\"SSEAlgorithm\":\"AES256\"},null],\"CreationDate\":[\"2020-05-15T09:39:59.000Z\",null],\"Owner\":[{\"DisplayName\":\"120886317861****\",\"ID\":\"120886317861****\"},null],\"StorageClass\":[\"Standard\",null],\"DataRedundancyType\":[\"LRS\",null],\"RefererList\":[{\"Referer\":[\"https://www.tmall.com\"]},null],\"AllowEmptyReferer\":[\"false\",null],\"Name\":[\"ddddss\",null],\"BucketPolicy\":[{\"LogPrefix\":\"\",\"LogBucket\":\"\"},null],\"TagSet\":[]},null],\"ExtranetEndpoint\":[\"oss-cn-shanghai.aliyuncs.com\",null],\"Region\":[\"cn-shanghai\",null],\"IntranetEndpoint\":[\"oss-cn-shanghai-internal.aliyuncs.com\",null],\"Location\":[\"oss-cn-shanghai\",null]}",
    "ResourceId":"new-bucket",
    "Relationship":"",
    "Region":"cn-shanghai",
    "Tags":"{}"
  }
```


# 1.3. 资源不合规事件

配置审计自动对资源进行合规性评估，当资源被评估为**不合规**时，可及时通过消息服务MNS向您发送通知。通过本文您可以了解资源不合规事件的主要参数说明和代码示例。

资源不合规事件的主要参数说明如下表所示。

| 参数 | 说明 |
| --- | --- |
| annotation | 资源不合规描述信息。 |
| configuration | 资源当前实际配置，即资源不合规配置。 |
| desiredValue | 资源期望配置，即资源合规配置。 |
| operator | 资源当前配置和期望配置之间的比较运算符。 |
| property | 当前配置在资源属性结构体中的JSON路径，例如：`$.AccessControlList.Grant`。 |
| accountId | 资源所属的阿里云账号ID。 |

| 参数 | 说明 |
| --- | --- |
| riskLevel | 规则风险等级。取值：<br>• Info：低风险。<br>• Warning：中风险。<br>• Critical：高风险。 |
| evaluationResultIdentifier | 合规评估的详细信息。 |
| resourceId | 资源ID。 |
| configRuleName | 规则名称。 |
| configRuleArn | 规则ARN。 |
| configRuleId | 规则ID。 |
| regionId | 资源所在地域ID。 |
| resourceOwnerId | 资源所属的阿里云账号ID。 |
| resourceType | 资源类型。支持的资源类型请参见支持配置审计的云服务。 |
| eventType | 事件类型。取值：<br>• ResourceChange：资源变更事件。<br>• ResourceCompliance：资源不合规事件。<br>• SnapshotDelivery：资源快照投递事件。 |
| complianceType | 规则合规类型。取值：<br>• COMPLIANT：合规。<br>• NON_COMPLIANT：不合规。 |

阿里云账号在企业版配置审计中新建规则test-oss-bucket-public-read-prohibited，用于检测对象存储OSS上海地域的存储桶config-snapshot的读写权限。存储桶config-snapshot的实际配置为public-read（公共读），期望配置为NotContains read（不包含读权限），检测结果为NonCompliant（不合规）。代码示例如下：

```
{
 "annotation": "{\"configuration\":\"public-read\",\"desiredValue\":\"read\",\"operator\":\"NotContains\",\"
property\":\"$.AccessControlList.Grant\"}",
 "accountId": 169827232854****,
 "riskLevel": "Critical",
 "resultRecordedTimestamp": 1595419396740,
 "eventName": "NonCompliant",
 "evaluationResultIdentifier": {
  "orderingTimestamp": 1595419392092,
  "evaluationResultQualifier": {
   "resourceId": "config-snapshot",
   "configRuleName": "test-oss-bucket-public-read-prohibited",
   "configRuleArn": "acs:config::169827232854****:config-rule/cr-610ad6e0007300a8****",
   "configRuleId": "cr-610ad6e0007300a8****",
   "regionId": "cn-shanghai",
   "resourceName":"config-snapshot",
   "resourceOwnerId":169827232854****,
   "resourceType": "ACS::OSS::Bucket"
  }
 },
 "eventType": "ResourceCompliance",
 "invokingEventMessageType": "ConfigurationItemChangeNotification",
 "configRuleInvokedTimestamp": 1595419392092,
 "notificationCreationTime": 1595419396769,
 "complianceType": "NON_COMPLIANT"
}
```


# 1.4. 资源快照投递事件

当资源快照投递到对象存储OSS的指定存储桶（Bucket）时，配置审计向消息服务MNS的指定主题发送资源快照投递事件，消息服务MNS根据主题的推送方式给您发送通知。通过本文您可以了解资源快照投递事件发送到消息服务MNS成功和失败的参数说明以及代码示例。

## 资源快照投递事件发送到消息服务MNS成功

参数说明如下表所示。

| 参数 | 说明 |
| --- | --- |
| requestId | 资源快照投递事件的请求ID。 |
| eventName | 资源快照投递事件的名称。 |

| 参数 | 说明 |
| --- | --- |
| eventType | 事件类型。取值：<br>• ResourceChange：资源变更事件。<br>• ResourceCompliance：资源不合规事件。<br>• SnapshotDelivery：资源快照投递事件。 |
| notificationCreationTime | 新建资源快照投递事件的时间戳。时间戳转换方法，请参见Unix时间戳。 |

代码示例如下：

```
{
  "requestId":"c33f24e9-c715-4c43-b635-e6d1c48b913e",
  "eventName":"SnapshotDeliverySuccess",
  "eventType":"SnapshotDelivery",
  "notificationCreationTime":1605863441996
}
```

## 资源快照投递事件发送到消息服务MNS失败

参数说明如下表所示。

| 参数 | 说明 |
| --- | --- |
| requestId | 资源快照投递事件的请求ID。 |
| eventName | 资源快照投递事件的名称。 |
| eventType | 事件类型。取值：<br>• ResourceChange：资源变更事件。<br>• ResourceCompliance：资源不合规事件。<br>• SnapshotDelivery：资源快照投递事件。 |
| errorCause | 资源快照投递事件发送失败的原因。 |
| notificationCreationTime | 新建资源快照投递事件的时间戳。时间戳转换方法，请参见Unix时间戳。 |

代码示例如下，其中失败原因为NoSuchBucket（目标存储桶不存在）：

```
{
  "errorCause": "NoSuchBucket",
  "requestId": "9ad74955-4195-4f0a-938c-afd5c56477ea",
  "eventName": "SnapshotDeliveryFailed",
  "eventType": "SnapshotDelivery",
  "notificationCreationTime": 1606189671571
}
```

# 2.发送资源事件到消息服务MNS

您可以在配置审计中设置将资源变更事件、资源不合规事件和资源快照投递事件发送到消息服务MNS的指定主题，您还可以根据所需设置该主题的推送方式和内容。

## 前提条件

请确保您已开通消息服务MNS，操作方法请参见开通MNS服务。

## 背景信息

如果您想深入了解消息服务MNS，请参见什么是消息服务MNS。

## 操作步骤

1. 登录配置审计控制台。
2. 在左侧导航栏，选择**投递服务 > 订阅资源事件**。
3. 在**订阅资源事件**页面，打开**设置消息服务MNS**开关。
4. 设置用于接收资源事件的主题。

   主题的相关参数如下表所示。

| 参数 | 描述 |
| --- | --- |
| **主题地域** | 主题名称所在地域。 |
| **主题名称** | 消息服务MNS中的主题名称。同一账号同一地域下，主题名称不能重复。<br>○ 当您选中**本账号中新建主题**时，通过配置审计控制台新建主题，输入主题名称。<br>○ 当您选中**选择本账号中已有的主题**时，在消息服务MNS中选择已有主题。 |
| **消息最大长度（Byte）** | 发送到该主题的消息体的最大长度。取值范围：1024~65536。默认值：65536。<br>**说明** 由于资源信息较大，请您在消息服务MNS控制台上将主题信息的最大长度至少设置为8192，以免因长度限制导致消息发送失败。 |
| **开启Logging** | 当前主题是否开启日志管理功能。 |
| **订阅事件的最低风险等级** | 当您配置事件订阅时，您需配置接收的最低风险等级。取值：<br>○ **全部风险等级**<br>○ **高风险**<br>○ **中风险**<br>○ **低风险**<br>例如：如果您选择**中风险**，则配置审计为您推送**中风险**和**高风险**等级的不合规事件，**低风险**级别的不合规事件将被过滤掉。 |

| 参数 | 描述 |
| --- | --- |
| **订阅指定资源类型事件** | 订阅指定资源类型的事件。取值：<br>○ **服务支持的全部资源类型**：订阅全部资源类型事件。当配置审计对接新产品后，该产品的资源类型将自动纳入监控范围。<br>○ **自定义资源类型**：勾选需监控的资源类型，自定义选择资源类型事件。 |

5. 单击**确定**。

## 后续步骤

资源事件发送到指定主题后，您可以在消息服务MNS控制台的目标主题中设置该主题的推送方式和内容。具体操作请参见发布消息。