

ALIBABA CLOUD

阿里云

配置审计
资源快照

文档版本：20201208

 阿里云

法律声明

阿里云提醒您在使用或阅读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 <code>cd /d C:/window</code> 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	<code>bae log list --instanceid</code> <i>Instance_ID</i>
[] 或者 [a b]	表示可选项，至多选择一个。	<code>ipconfig [-all -t]</code>
{ } 或者 {a b}	表示必选项，至多选择一个。	<code>switch {active stand}</code>

目录

1.投递资源快照到对象存储OSS	05
2.资源快照投递到对象存储OSS的代码示例	06

1. 投递资源快照到对象存储OSS

当您需要将资源的配置变更历史和定时配置信息以快照形式投递到对象存储OSS的指定地址时，需要设置存储桶（Bucket）。资源快照投递到指定存储桶后，您可以查看或下载JSON格式文件。

前提条件

请确保您已开通对象存储OSS服务，操作方法请参见[开通OSS服务](#)。

背景信息

- 如果您想深入了解对象存储OSS服务，请参见[什么是对象存储OSS](#)。
- JSON格式文件的代码示例，请参见[资源快照投递到对象存储OSS的代码示例](#)。

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](#) > [投递到对象存储OSS](#)。
3. 在[投递到对象存储OSS](#)页面，打开[设置对象存储OSS](#)开关。
4. 设置用于接收资源快照的存储桶。存储桶的相关参数如下表所示。

参数	描述
地域	存储桶所在地域。
存储桶	对象存储OSS中存储桶的名称。存储桶名称不能重复。 <ul style="list-style-type: none">○ 当您选中本账号中新建存储桶时，通过配置审计控制台新建存储桶，输入存储桶名称。○ 当您选中选择本账号中已有的存储桶时，在对象存储OSS中选择已有存储桶名称。
日志文件加密	存储桶中的日志文件是否加密。当您选中本账号中新建存储桶时，需要设置该参数。 存储桶中日志文件支持的加密方式如下： <ul style="list-style-type: none">○ AES256○ KMS

5. 单击[确定](#)。

后续步骤

资源快照投递到指定存储桶后，您可以在OSS管理控制台的目标存储桶的[文件管理](#)页面，查看或下载JSON格式文件。快照文件所在路径为 `/ACSLogs/AccountId/Config/RegionId/yyyy/mm/dd/`。

2.资源快照投递到对象存储OSS的代码示例

如果您设置了资源快照投递功能，配置审计将资源变更历史快照或资源定时配置快照以指定格式投递到对象存储OSS。通过本文您可以了解资源变更历史快照和资源定时配置快照的代码示例和主要参数说明。

资源变更历史快照

资源变更历史快照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。
arn	资源ARN。各云服务资源类型对应的ARN格式，请参见 ARN格式 。
regionId	资源所在地域ID。
configuration	资源的详细配置。
configurationDiff	资源配置变更的具体变更项及变更前后信息。
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 。
resourceCreateTime	创建资源的时间戳。时间戳转换方法，请参见 Unix时间戳 。
resourceId	资源ID。
resourceName	资源名称。
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 。
tags	资源标签。
resourceEventType	资源变更事件的类型。取值： <ul style="list-style-type: none">DISCOVERED：新建资源事件。MODIFY：修改资源事件。REMOVE：删除资源事件。

新建、更新和删除资源的代码示例如下：

- 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（Bucket）test123，在configurationDiff中显示变更前信息（null）和变更后信息。

```
{
  "configurationItems":[
    {
      "accountId":1208863178****,
      "arn":"acs:oss:cn-shanghai:1208863178****:test123",
      "regionId":"cn-shanghai",
      "configuration":{"AccessControlList":{"Grant":"private"},"ServerSideEncryptionRule":{"SSEAlgorithm":"None"},"Comment":"","CreationDate":"2020-11-16T06:50:36.000Z","Owner":{"DisplayName":"1208863178****","ID":"1208863178****"},"StorageClass":"Standard","DataRedundancyType":"LRS","AllowEmptyReferer":"true","Name":"test123","BucketPolicy":{"LogPrefix":"","LogBucket":""},"ExtranetEndpoint":"oss-cn-shanghai.aliyuncs.com","IntranetEndpoint":"oss-cn-shanghai-internal.aliyuncs.com","Location":"oss-cn-shanghai"}},
      "configurationDiff":{"AccessControlList":[null,{"Grant":"private"}],"ServerSideEncryptionRule":[null,{"SSEAlgorithm":"None"}],"CreationDate":[null,"2020-11-16T06:50:36.000Z"],"Owner":[null,{"DisplayName":"1208863178****","ID":"1208863178****"}],"BucketPolicy":[null,{"LogPrefix":"","LogBucket":""}],"StorageClass":[null,"Standard"],"ExtranetEndpoint":[null,"oss-cn-shanghai.aliyuncs.com"],"DataRedundancyType":[null,"LRS"],"AllowEmptyReferer":[null,"true"],"IntranetEndpoint":[null,"oss-cn-shanghai-internal.aliyuncs.com"],"Name":[null,"test123"],"Location":[null,"oss-cn-shanghai"]},
      "captureTime":1605509680560,
      "resourceCreateTime":1605509436000,
      "resourceId":"test123",
      "resourceName":"test123",
      "resourceType":"ACS::OSS::Bucket",
      "tags":{},
      "resourceEventType":"DISCOVERED"
    }
  ],
  "fileVersion":"1.0"
}
```

- 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test666的Referer白名单，在configurationDiff中显示变更前信息（允许开启空Referer）和变更后信息（不允许开启空Referer）。

```
{
  "configurationItems":[
    {
      "accountId":1208863178****,
      "arn":"acs:oss:cn-shanghai:1208863178****:test666",
      "regionId":"cn-shanghai",
      "configuration":{"AccessControlList":{"Grant":{"private"}}, "ServerSideEncryptionRule":{"SSEAlgorithm":"AES256"}, "Comment":"","CreationDate":"2020-03-16T08:34:49.000Z", "Owner":{"DisplayName":"1208863178****", "ID":"1208863178****"}, "StorageClass":"Standard", "DataRedundancyType":"LRS", "RefererList":{"Referer":["https://www.****.com"]}, "AllowEmptyReferer":"false", "Name":"testoss111", "BucketPolicy":{"LogPrefix":"","LogBucket":"","TagSet":{"Tag":[{"Value":"1", "Key":"1"}, {"Value":"2", "Key":"2"}, {"Value":"001", "Key":"526"}, {"Value":"612", "Key":"612"}, {"Value":"prod2", "Key":"env"}, {"Value":"v0", "Key":"k0"}]}, "ExtranetEndpoint":"oss-cn-shanghai.aliyuncs.com", "Region":"cn-shanghai", "IntranetEndpoint":"oss-cn-shanghai-internal.aliyuncs.com", "Location":"oss-cn-shanghai"}},
      "configurationDiff":{"AllowEmptyReferer":["true", "false"]},
      "captureTime":1605508188495,
      "resourceCreateTime":1584347689000,
      "resourceId":"test666",
      "resourceName":"test666",
      "resourceType":"ACS::OSS::Bucket",
      "tags":"","
      "resourceEventType":"MODIFY"
    }
  ],
  "fileVersion":"1.0"
}
```

● 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test666，在configurationDiff中显示变更前信息和变更后信息（null）。


```

{
  "configurationItems":[
    {
      "accountId":1208863178****,
      "arn":"acs:oss:cn-shanghai:1208863178****:test666",
      "regionId":"cn-shanghai",
      "configuration":{"AccessControlList":{"Grant":"private"},"ServerSideEncryptionRule":{"SSEAlgorithm":"None"},"Comment":"","CreationDate":"2020-11-16T06:50:36.000Z","Owner":{"DisplayName":"1208863178****","ID":"1208863178****"},"StorageClass":"Standard","DataRedundancyType":"LRS","AllowEmptyReferer":"true","Name":"test666","BucketPolicy":{"LogPrefix":"","LogBucket":""},"ExtranetEndpoint":"oss-cn-shanghai.aliyuncs.com","IntranetEndpoint":"oss-cn-shanghai-internal.aliyuncs.com","Location":"oss-cn-shanghai"}},
      "configurationDiff":{"AccessControlList":[{"Grant":"private"},null],"ServerSideEncryptionRule":{"SSEAlgorithm":"None",null],"CreationDate":["2020-11-16T06:50:36.000Z",null],"Owner":[{"DisplayName":"1208863178****","ID":"1208863178****"},null],"BucketPolicy":[{"LogPrefix":"","LogBucket":""},null],"StorageClass":["Standard",null],"ExtranetEndpoint":["oss-cn-shanghai.aliyuncs.com",null],"DataRedundancyType":["LRS",null],"AllowEmptyReferer":["true",null],"IntranetEndpoint":["oss-cn-shanghai-internal.aliyuncs.com",null],"Name":["test666",null],"Location":["oss-cn-shanghai",null]}},
      "captureTime":1605509680560,
      "resourceCreateTime":1605509436000,
      "resourceId":"test666",
      "resourceName":"test666",
      "resourceType":"ACS::OSS::Bucket",
      "tags":{},
      "resourceEventType":"REMOVE"
    }
  ],
  "fileVersion":"1.0"
}

```

资源定时配置快照

资源定时配置快照的参数说明如下表所示。

参数	说明
accountId	资源所属阿里云账号ID。
availabilityZone	资源可用区。
regionId	资源所在地域。

参数	说明
configuration	资源的详细配置。
resourceCreateTime	创建资源的时间戳。时间戳转换方法，请参见 Unix时间戳 。
resourceId	资源ID。
resourceName	资源名称。
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 。
tags	资源的标签。

阿里云账号将对象存储OSS上海地域的存储桶test123的定时配置快照投递到您指定的存储桶中。代码示例如下：

```
{
  "configurationItems":[
    {
      "accountId":12088631786*****,
      "availabilityZone": "",
      "regionId": "cn-shanghai",
      "configuration": {"AccessControlList": {"Grant": "private"}, "ServerSideEncryptionRule": {"SSEAlgorithm": "AES256"}, "Comment": "", "CreationDate": "2019-08-29T06:02:59.000Z", "Owner": {"DisplayName": "12088631786****", "ID": "12088631786****"}, "StorageClass": "Standard", "DataRedundancyType": "LRS", "RefererList": {"Referer": ["https://www.*****.com"]}, "AllowEmptyReferer": "false", "Name": "test123", "BucketPolicy": {"LogPrefix": "", "LogBucket": ""}, "ExtranetEndpoint": "oss-cn-shanghai.aliyuncs.com", "TagSet": {"Tag": [{"Value": "1", "Key": "1"}, {"Value": "2", "Key": "2"}, {"Value": "001", "Key": "526"}, {"Value": "612", "Key": "612"}, {"Value": "prod2", "Key": "env"}, {"Value": "v0", "Key": "k0"}]}, "Region": "cn-shanghai", "IntranetEndpoint": "oss-cn-shanghai-internal.aliyuncs.com", "Location": "oss-cn-shanghai"},
      "resourceCreateTime":1567058579000,
      "resourceId": "test123",
      "resourceName": "test123",
      "resourceType": "ACS::OSS::Bucket",
      "tags": ""
    }
  ],
  "fileVersion": "1.0"
}
```