阿里云
访问控制

API 参考（STS）

文档版本：20190221

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
	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，恢复业务所需时间约10分钟。
	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。	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。	单击 **确定**。
`courier` 字体	命令。	执行 `cd /d C:/windows` 命令，进入Windows系统文件夹。
*## *	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。	`swich` *`{stand | slave}`*

目录

法律声明.....I
通用约定.....I
1 调用方式..... 1
1.1 请求结构.....1
2 操作接口..... 2
2.1 AssumeRole.....2
3 附录..... 5
3.1 错误代码表.....5
3.2 服务地址.....6

1 调用方式

1.1 请求结构

服务地址

STS服务地址请参考服务地址。

通信协议

为了保证通信的安全性，STS服务仅支持使用HTTPS安全通道发送请求。

HTTP请求方法

支持HTTP GET/POST方法发送请求，这种方式下请求参数需要包含在请求的URL中。(GET请求最大不得超过4KB, POST请求最大不得超过10MB)。

请求参数

每个请求都需要指定要执行的操作，即Action参数（例如AddUser），以及每个操作接口都需要包含的公共请求参数和指定操作接口所特有的请求参数。

字符编码

请求及返回结果都使用UTF-8字符集进行编码。

2 操作接口

2.1 AssumeRole

接口描述

通过该接口，获取一个扮演该角色的临时身份。

请求参数

Action

- 类型：String
- 必须：是
- 描述：系统规定参数，取值：AssumeRole

RoleArn

- 类型：String
- 必须：是
- 描述：指定角色的全局资源描述符(Aliyun Resource Name，简称Arn)。每个角色都有一个唯一的全局资源描述符，规定格式为 acs:ram::$accountID:role/$roleName ，一个样例：acs:ram::1234567890123456:role/samplerole 。您可以在RAM控制台的角色管理页面RAM控制台的角色管理列表中，进入角色详情页可以查看一个角色的RoleArn。

RoleSessionName

- 类型：String
- 必须：是
- 描述：用户自定义参数。此参数用来区分不同的Token，可用于用户级别的访问审计。
- 格式：

```
^[a-zA-Z0-9\.@\-_]+$
```

注意:
支持输入 2-32 个字符，请输入至少 2 个字符，如果只有 1 个字符，会出现错误。

Policy

- 名称：Policy
- 类型：String

- 必须：否
- 描述：授权策略*Policy*语法结构，Policy长度限制为1024字节；您可以通过此参数限制生成的Token的权限，不指定则返回的Token将拥有指定角色的所有权限。

DurationSeconds

- 名称：DurationSeconds
- 类型：Integer
- 必须：否
- 描述：指定的过期时间，单位为秒。过期时间范围：900 ~ 3600，默认值为3600。

返回参数

Credentials

- 类型：*Credentials*
- 描述：访问凭证

AssumedRoleUser

- 描述：角色扮演临时身份

操作示例

HTTP Request

```
https://sts.aliyuncs.com?Action=AssumeRole
&RoleArn=acs:ram::1234567890123456:role/adminrole
&RoleSessionName=alice
&DurationSeconds=3600
&Policy=<url_encoded_policy>
&<公共请求参数>
```

HTTP Response

- XML格式

```
<AssumeRoleResponse>
    <RequestId>6894B13B-6D71-4EF5-88FA-F32781734A7F</RequestId>
    <AssumedRoleUser>
        <arn>acs:sts::1234567890123456:assumed-role/AdminRole/alice
</arn>
        <AssumedRoleUserId>344584339364951186:alice<AssumedRol
eUserId>
    </AssumedRoleUser>
    <Credentials>
        <AccessKeyId>STS.L4aBSCSJVMuKg5U1vFDw</AccessKeyId>
        <AccessKeySecret>wyLTSmsyPGP1ohvvw8xYgB29dlGI8KMiH2pKCNZ9</
AccessKeySecret>
        <SecurityToken>CAESrAIIARKAAShQquMnLIlbvEcIxO6wCoqJufs8
sWwieUxu45hS9AvKNEte8KRUWiJWJ6Y+YHAPgNwi7yfRecMFydL2uPOgBI7LDi
o0RkbYLmJfIxHM2nGBPdml7kYEOXmJp2aDhbvvwVYIyt/8iES/R6N208wQh0Pk2bu
+/9dvalp6wOHF4gkFGhhTVFMuTDRhQlNDU0pWTXVLZzVVMXZGRHciBTQzMjc0K
```

```
gVhbGljZTCpnJjwySk6BlJzYU1ENUJuCgExGmkKBUFsbG93Eh8KDEFjdGlvb
kVxdWFscxIGQWN0aW9uGgcKBW9zczoqEj8KDlJlc291cmNlRXF1YWxzEghSZ
XNvdXJjZRojCiFhY3M6b3NzOio6NDMyNzQ6c2FtcGxlYm94L2FsaWNlLyo=</
SecurityToken>
        <Expiration>2015-04-09T11:52:19Z</Expiration>
    </Credentials>
</AssumeRoleResponse>
```

- **JSON格式**

```
{
    "Credentials": {
        "AccessKeyId": "STS.L4aBSCSJVMuKg5U1vFDw",
        "AccessKeySecret": "wyLTSmsyPGP1ohvvw8xYgB29dlGI8KMiH2pKCNZ9
",
        "Expiration": "2015-04-09T11:52:19Z",
        "SecurityToken": "CAESrAIIARKAAShQquMnLIlbvEcIxO6wCoqJufs8
sWwieUxu45hS9AvKNEte8KRUWiJWJ6Y+YHAPgNwi7yfRecMFydL2uPOgBI7LDi
o0RkbYLmJfIxHM2nGBPdml7kYEOXmJp2aDhbvvwVYIyt/8iES/R6N208wQh0Pk2bu
+/9dvalp6wOHF4gkFGhhTVFMuTDRhQlNDU0pWTXVLZzVVMXZGRHciBTQzMjc0K
gVhbGljZTCpnJjwySk6BlJzYU1ENUJuCgExGmkKBUFsbG93Eh8KDEFjdGlvb
kVxdWFscxIGQWN0aW9uGgcKBW9zczoqEj8KDlJlc291cmNlRXF1YWxzEghSZ
XNvdXJjZRojCiFhY3M6b3NzOio6NDMyNzQ6c2FtcGxlYm94L2FsaWNlLyo="
    },
    "AssumedRoleUser": {
        "arn": "acs:sts::1234567890123456:assumed-role/AdminRole/
alice",
        "AssumedRoleUserId":"344584339364951186:alice"
        },
    "RequestId": "6894B13B-6D71-4EF5-88FA-F32781734A7F"
}
```

3 附录

3.1 错误代码表

本文描述了 RAM STS 错误相关信息。详细信息请参考*API* 错误中心。

HTTP Status 400

InvalidParameterInvalidParameter.RoleArn

- HTTP Status: 400
- ErrorMessage: The parameter RoleArn is wrongly formed.
- 解决方案：角色 Arn 不正确。请确认该角色 Arn。

InvalidParameter.RoleSessionName

- HTTP Status: 400
- ErrorMessage: The parameter RoleSessionName is wrongly formed.
- 解决方案：RoleSessionName 输入错误。支持输入 2-32 个字符，请输入至少 2 个字符；允许输入^[a-zA-Z0-9\.@\-_]+$。

InvalidParameter.DurationSeconds

- HTTP Status: 400
- ErrorMessage: The Min/Max value of DurationSeconds is 15min/1hr.
- 解决方案：DurationSeconds 参数设置错误。取值范围 900 ~ 3600。

InvalidParameter.PolicyGrammar

- HTTP Status: 400
- ErrorMessage: The parameter Policy has not passed grammar check.
- 解决方案：Policy 语法错误。请修改 Policy 内容。

InvalidParameter.PolicySize

- HTTP Status: 400
- ErrorMessage: The size of Policy must be smaller than 1024 bytes.
- 解决方案：Policy 最大长度为 1024 字节。请修改 Policy 以缩减长度。

HTTP Status 403

NoPermission

- HTTP Status: 403
- ErrorMessage: You are not authorized to do this action. You should be authorized by RAM.
- 解决方案：STS Token 没有权限。请在生成 STSToken 时正确授权。

HTTP Status 500

InternalError

- HTTP Status: 500
- ErrorMessage: STS Server Internal Error happened.
- 解决方案：服务内部错误。可提交工单联系售后技术工程师。

3.2 服务地址

服务地址选择建议

- 每个服务地址功能完全一样，请尽量同Region调用。
- Endpoint类型：
  - 公网：互联网访问地址。
  - VPC：可在同Region内VPC中访问，无需开放公网访问权限。

服务地址

表 3-1: 国内中心

区域	域名
国内中心	公网：sts.aliyuncs.com

表 3-2: 大中华区

区域	RegionId	域名
华东 1-杭州	cn-hangzhou	· 公网：sts.cn-hangzhou.aliyuncs.com · VPC：sts-vpc.cn-hangzhou.aliyuncs.com
华东 2-上海	cn-shanghai	· 公网：sts.cn-shanghai.aliyuncs.com · VPC：sts-vpc.cn-shanghai.aliyuncs.com

区域	RegionId	域名
华南 1-深圳	cn-shenzhen	· 公网：sts.cn-shenzhen.aliyuncs.com · VPC： sts-vpc.cn-shenzhen.aliyuncs.com
华北 1-青岛	cn-qingdao	公网：sts.cn-qingdao.aliyuncs.com
华北 2-北京	cn-beijing	· 公网：sts.cn-beijing.aliyuncs.com · VPC：sts-vpc.cn-beijing.aliyuncs.com
华北 3-张家口	cn-zhangjiakou	· 公网：sts.cn-zhangjiakou.aliyuncs.com · VPC：sts-vpc.cn-zhangjiakou.aliyuncs.com
华北 5-呼和浩特	cn-huhehaote	· 公网：sts.cn-huhehaote.aliyuncs.com · VPC：sts-vpc.cn-huhehaote.aliyuncs.com
香港	cn-hongkong	· 公网：sts.cn-hongkong.aliyuncs.com · VPC：sts-vpc.cn-hongkong.aliyuncs.com

表 3-3: 亚太

区域	RegionId	域名
亚太东南 1 （新加坡）	ap-southeast-1	公网：sts.ap-southeast-1.aliyuncs.com
亚太东南 2 （悉尼）	ap-southeast-2	公网：sts.ap-southeast-2.aliyuncs.com
亚太东南 3 （吉隆坡）	ap-southeast-3	公网：sts.ap-southeast-3.aliyuncs.com
亚太东南 5 （雅加达）	ap-southeast-5	公网：sts.ap-southeast-5.aliyuncs.com

区域	RegionId	域名
亚太东北 1（东京）	ap-northeast-1	公网：sts.ap-northeast-1.aliyuncs.com
亚太南部 1（孟买）	ap-south-1	公网：sts.ap-south-1.aliyuncs.com

表 3-4: 美洲-欧洲

区域	RegionId	域名
美国西部 1（硅谷）	us-west-1	公网：sts.us-west-1.aliyuncs.com
美国东部 1（弗吉尼亚）	us-east-1	公网：sts.us-east-1.aliyuncs.com
欧洲中部 1（法兰克福）	eu-central-1	公网：sts.eu-central-1.aliyuncs.com
中东东部 1（迪拜）	me-east-1	公网：sts.me-east-1.aliyuncs.com
英国（伦敦）	eu-west-1	公网：sts.eu-west-1.aliyuncs.com