阿里云
访问控制

API 参考（STS）

文档版本：20190910

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 什么是STS.....1
2 调用方式.....2
2.1 请求结构.....2
2.2 接入地址.....2
2.3 公共参数.....5
2.4 计算签名.....6
2.5 返回结果.....8
3 操作接口.....10
3.1 AssumeRole.....10
3.2 GetCallerIdentity.....14
3.3 AssumeRoleWithSAML.....15

1 什么是STS

阿里云临时安全令牌（Security Token Service，STS）是阿里云提供的一种临时访问权限管理服务。

STS功能特性

通过STS服务，您所授权的身份主体（RAM用户、RAM用户组或RAM角色）可以获取一个自定义时效和访问权限的临时访问令牌。STS令牌持有者可以通过以下方式访问阿里云资源：

- 通过编程方式访问被授权的阿里云服务API。
- 登录阿里云控制台操作被授权的云资源。

STS接入地址

用于API访问的STS接入地址：`https://sts.aliyuncs.com`。

STS基本概念

RAM角色（RAM role）	一种虚拟的RAM用户。
RAM角色的全局资源描述符（Role ARN）	Role ARN是角色的全局资源描述符（Aliyun Resource Name，简称ARN），用来指定具体角色。每个角色都有一个唯一的全局资源描述符。格式：`acs:ram::$accountID:role/$roleName`。
可信实体（Trusted entity）	角色的可信实体是指可以扮演角色的实体用户身份。创建角色时必须指定可信实体，角色只能被受信的主体扮演。可信实体可以是受信的阿里云账号、受信的阿里云服务或身份提供商。
扮演角色（Assume role）	扮演角色是实体用户获取角色身份的安全令牌的方法。一个实体用户调用STS API `AssumeRole`可以获得角色的安全令牌，使用安全令牌可以访问云服务API。

2 调用方式

2.1 请求结构

本文介绍了STS的接入地址、通信协议、HTTP请求方法和请求参数等请求结构相关的信息。

接入地址

STS的接入地址请参见接入地址。

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

STS服务支持HTTP GET/POST方法发送请求。

> 说明:
> 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如下信息：

- 要执行的操作：Action参数。
- 每个操作接口都需要包含的公共请求参数。
- 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。

2.2 接入地址

本文介绍了STS服务的所有接入地址，每个地址的功能都相同，请尽量在同区域进行调用。

以下表格分别罗列了各个区域的接入地址，其中接入地址一列包含如下信息：

- 公网：互联网访问地址。
- VPC：可在同区域内VPC中访问，无需开放公网访问权限。

国内中心

区域	接入地址
国内中心	公网：sts.aliyuncs.com

大中华区

区域	Region ID	接入地址
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
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

区域	Region ID	接入地址
中国香港	cn-hongkong	· 公网：sts.cn-hongkong.aliyuncs.com · VPC：sts-vpc.cn-hongkong.aliyuncs.com

亚太

区域	Region ID	接入地址
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
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

美洲/欧洲

区域	Region ID	接入地址
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

2.3 公共参数

公共参数分为公共请求参数和公共返回参数。

公共请求参数

名称	类型	是否必需	描述
Action	String	是	API的名称。
Format	String	否	返回值的类型。支持JSON与XML，默认为XML。
Version	String	是	API版本号。为日期形式：YYYY-MM-DD，本版本对应为 2015-04-01。
Signature	String	是	消息签名。
SignatureMethod	String	是	签名方式，目前仅支持HMAC-SHA1。
SignatureNonce	String	是	唯一随机数。用于防止网络重放攻击。用户在不同请求间要使用不同的随机数值。
SignatureVersion	String	是	签名算法版本，目前版本是1.0。
AccessKeyId	String	是	访问密钥ID。
Timestamp	String	是	请求的时间戳。日期格式按照ISO8601标准表示，并需要使用UTC时间。格式为：YYYY-MM-DDThh:mm:ssZ。

公共返回参数

名称	类型	描述
RequestId	String	请求ID。无论成功与否，系统都会返回一个唯一识别码给用户。 此参数用于识别每一次请求。

请求示例

```
https://sts.aliyuncs.com/?Action=XXXXXX
?Format=xml
&Version=2015-04-01
&Signature=Pc5WB8gokVn0xfeu%2FZV%2BiNM1dg****
&SignatureMethod=HMAC-SHA1
&SignatureNonce=1521552885****
&SignatureVersion=1.0
&AccessKeyId=key-test
&Timestamp=2012-06-01T12:00:00Z
…
```

返回示例

- **XML示例**

```
<?xml version="1.0" encoding="utf-8"?>
<!—结果的根结点-->
<接口名称+Response>
  <!—返回请求标签-->
  <RequestId>4C467B38-3910-447D-87BC-AC049166F216</RequestId>
  <!—返回结果数据-->
</接口名称+Response>
```

- **JSON示例**

```
{
  "RequestId": "4C467B38-3910-447D-87BC-AC049166F216"
  /* 返回结果数据 */
}
```

2.4 计算签名

STS服务会对每个访问的请求进行身份验证，无论使用HTTP还是HTTPS协议提交请求，都需要在请求中包含签名信息。

背景信息

STS通过使用AccessKey ID和AccessKeySecret进行对称加密的方法来验证请求的发送者身份。AccessKey ID和AccessKeySecret由阿里云颁发给访问者，其中AccessKey ID用于标识访问者的身份，AccessKeySecret用于加密签名字符串和服务器端验证签名字符串的密钥，必须严格保密谨防泄露。

操作步骤

1. 使用请求参数构造规范化的请求字符串。

   a) 排序参数。排序规则以首字母顺序排序，排序参数包括ZH-CN_TP_12467_V3.dita#reference_rzc_v4v_xdb和接口自定义参数。不包括公共请求参数中的Signature参数。

   > 说明:
   > 当使用GET方法提交请求时，这些参数就是请求URL中的参数部分，即URL中?之后由&连接的部分。

   b) 编码参数。使用UTF-8字符集对每个请求参数的名称和参数取值进行URL编码，URL编码规则如下：

   - 对于字符A~Z、a~z、0~9以及字符-、_、.和~不编码。
   - 对于其他字符编码成%XY的格式，其中XY是字符对应ASCII码的16进制。例如：半角双引号（"）对应的编码为：%22。
   - 空格（ ）需要被编码成：%20，而不是+。

   > 说明:
   > 一般支持URL编码的库都按照application/x-www-form-urlencoded的MIME格式的规则进行编码，例如：Java中的java.net.URLEncoder。您可以直接使用这类方式进行编码，然后将编码后的字符串中加号+替换成%20、*替换成%2A、%7E替换~，即可得到上述规则描述的编码字符串。

   c) 使用=连接编码后的参数名称和参数取值。

   d) 使用&连接编码后的参数，得到规范化请求字符串。

   > 说明:
   > 参数排序需与排序参数保持一致。

2. 使用规范化请求字符串构造用于计算签名的字符串，规则如下：

```
StringToSign=
HTTPMethod + “&” + //发送请求的HTTP方法，例如GET
percentEncode(“/”) + ”&” + //字符（/）UTF-8编码得到的值，即%2F。
percentEncode(CanonicalizedQueryString)//规范化请求字符串
```

3. 按照RFC2104的定义，计算签名HMAC值。

   > 说明:
   > 计算签名时使用的key就是用户持有的AccessKeySecret加上一个&字符，其ASCII值为38，使用的哈希算法是：SHA1。

4. 按照Base64编码规则将HMAC值编码成字符串，得到签名值。

5. 将签名值作为`Signature`添加到请求参数中。

> **说明:**
> 将签名值添加到请求参数时，需要按照RFC3986的规则进行URL编码。

预期结果

下文以`AssumeRole`为例，介绍签名的一个具体示例及结果。

签名前的请求URL为：

```
https://sts.aliyuncs.com/?SignatureVersion=1.0&Format=JSON&Timestamp=
2015-09-01T05%3A57%3A34Z&RoleArn=acs%3Aram%3A%3A1234567890123%3Arole%
2Ffirstrole&RoleSessionName=client&AccessKeyId=testid&SignatureMethod=
HMAC-SHA1&Version=2015-04-01&Action=AssumeRole&SignatureNonce=571f8fb8
-506e-11e5-8e12-b8e8563dc8d2
```

对应的`StringToSign`为：

```
GET&%2F&AccessKeyId%3Dtestid%26Action%3DAssumeRole%26Format%3DJSON%
26RoleArn%3Dacs%253Aram%253A%253A1234567890123%253Arole%252Ffirstrole
%26RoleSessionName%3Dclient%26SignatureMethod%3DHMAC-SHA1%26Signatur
eNonce%3D571f8fb8-506e-11e5-8e12-b8e8563dc8d2%26SignatureVersion%3D1.0
%26Timestamp%3D2015-09-01T05%253A57%253A34Z%26Version%3D2015-04-01
```

例如：AccessKey ID为：testid，AccessKeySecret为：testsecret，则用于计算HMAC的key为：testsecret&。

计算得到的签名值为：`gNI7b0AyKZHxDgjBGPDgJ1Ce3L4=`。

签名后的请求URL为：

```
https://sts.aliyuncs.com/?SignatureVersion=1.0&Format=JSON&Timestamp=
2015-09-01T05%3A57%3A34Z&RoleArn=acs%3Aram%3A%3A1234567890123%3Arole%
2Ffirstrole&RoleSessionName=client&AccessKeyId=testid&SignatureMethod=
HMAC-SHA1&Version=2015-04-01&Signature=gNI7b0AyKZHxDgjBGPDgJ1Ce3L4%3D&
Action=AssumeRole&SignatureNonce=571f8fb8-506e-11e5-8e12-b8e8563dc8d2
```

2.5 返回结果

调用STS API后返回数据采用统一格式，返回结果格式主要有XML和JSON两种，默认为XML格式。本文档中的返回示例为了便于用户查看，做了格式化处理，实际返回结果是没有进行换行、缩进等处理的。

成功结果

调用STS API后，如果返回的HTTP状态码为：`2xx`，代表调用成功。

- XML示例

```
<?xml version="1.0" encoding="utf-8"?>
<!–结果的根结点-->
<接口名称+Response>
    <!–返回请求标签-->
    <RequestId>4C467B38-3910-447D-87BC-AC049166F216</RequestId>
    <!–返回结果数据-->
</接口名称+Response>
```

- JSON示例

```
{
    "RequestId": "4C467B38-3910-447D-87BC-AC049166F216",
    /* 返回结果数据 */
}
```

错误结果

调用STS API后，如果返回的HTTP状态码为：`4xx`或`5xx`，代表调用失败，系统将不会返回结果数据。此时，返回的消息体中包含：具体的错误代码、错误信息、全局唯一的请求ID：`RequestId`以及本次请求访问的站点ID：`HostId`，您可以通过各个参数中的错误码定位问题。

- XML示例

```
<?xml version="1.0" encoding="UTF-8"?>
<Error>
   <RequestId>8906582E-6722-409A-A6C4-0E7863B733A5</RequestId>
   <HostId>sts.aliyuncs.com</HostId>
   <Code>InvalidParameter</Code>
   <Message>The specified parameter "Action or Version" is not valid
.</Message>
</Error>
```

- JSON示例

```
{
    "RequestId": "7463B73D-35CC-4D19-A010-6B8D65D242EF",
    "HostId": "sts.aliyuncs.com",
    "Code": "InvalidParameter",
    "Message": "The specified parameter \"Action or Version\" is not
 valid."
}
```

3 操作接口

3.1 AssumeRole

调用AssumeRole接口获取一个扮演该角色的临时身份，此处RAM用户扮演的是受信实体为阿里云账号的RAM角色。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	AssumeRole	系统规定参数。取值：AssumeRole
RoleArn	String	是	acs:ram::1234567890 12****:role/adminrole	指定角色的ARN。格式：`acs:ram::$accountID:role/$roleName`。 说明： • `$accountID`：云账号ID。您可以通过登录阿里云控制台，将鼠标悬停在右上角头像的位置，单击安全设置进行查看。 • `$roleName`：RAM角色名称。您可以通过登录RAM控制台，单击左侧导航栏的RAM角色管理，在RAM角色名称列表下进行查看。
RoleSessionName	String	是	alice	用户自定义参数。此参数用来区分不同的令牌，可用于用户级别的访问审计。格式：`^[a-zA-Z0-9\.@\-_]+$`。 说明： 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。

名称	类型	是否必选	示例值	描述
Policy	String	否	{"Statement": [{"Action": ["*"],"Effect": "Allow","Resource": ["*"]}],"Version":"1"}	长度限制为1024字节。此参数可以限制生成的STS token的权限，若不指定则返回的token拥有指定角色的所有权限。
DurationSeconds	Long	否	3600	指定的过期时间，单位为秒。过期时间范围：900~3600秒，默认值为3600秒。

返回数据

名称	类型	示例值	描述
RequestId	String	6894B13B-6D71-4EF5-88FA-F32781734A7F	请求ID。
Credentials			访问凭证。
└ AccessKeyId	String	STS.L4aBSCSJVMuKg5U1****	访问密钥标识。
└ AccessKeySecret	String	wyLTSmsyPGP1ohvvw8xYgB29dlGI8KMiH2pK****	访问密钥。
└ SecurityToken	String	********	安全令牌。
└ Expiration	String	2015-04-09T11:52:19Z	失效时间。
AssumedRoleUser			角色扮演临时身份。

名称	类型	示例值	描述
└Arn	String	acs:sts::123456789012****:assumed-role/AdminRole/alice	指定角色的ARN。格式：acs:ram::$accountID:role/$roleName。 说明： • $accountID：云账号ID。您可以通过登录阿里云控制台，将鼠标悬停在右上角头像的位置，单击安全设置进行查看。 • $roleName：RAM角色名称。您可以通过登录RAM控制台，单击左侧导航栏的RAM角色管理，在RAM角色名称列表下进行查看。
└AssumedRoleUserId	String	34458433936495****:alice	该角色临时身份的用户ID。

示例

请求示例

```
https://sts.aliyuncs.com?Action=AssumeRole
&RoleArn=acs:ram::123456789012****:role/adminrole
&RoleSessionName=alice
&DurationSeconds=3600
&Policy=<url_encoded_policy>
&<公共请求参数>
```

返回示例

XML格式

```
<AssumeRoleResponse>
    <RequestId>6894B13B-6D71-4EF5-88FA-F32781734A7F</RequestId>
    <AssumedRoleUser>
        <arn>acs:sts::123456789012****:assumed-role/AdminRole/alice</
arn>
        <AssumedRoleUserId>34458433936495****:alice</AssumedRoleUserId
>
    </AssumedRoleUser>
    <Credentials>
        <AccessKeyId>STS.L4aBSCSJVMuKg5U1****</AccessKeyId>
        <AccessKeySecret>wyLTSmsyPGP1ohvvw8xYgB29dlGI8KMiH2pK****</
AccessKeySecret>
        <SecurityToken>********</SecurityToken>
        <Expiration>2015-04-09T11:52:19Z</Expiration>
    </Credentials>
```

```
</AssumeRoleResponse>
```

JSON格式

```
{
    "Credentials": {
        "AccessKeyId": "STS.L4aBSCSJVMuKg5U1****",
        "AccessKeySecret": "wyLTSmsyPGP1ohvvw8xYgB29dlGI8KMiH2pK****",
        "Expiration": "2015-04-09T11:52:19Z",
        "SecurityToken": "********"
    },
    "AssumedRoleUser": {
        "arn": "acs:sts::123456789012****:assumed-role/AdminRole/alice
",
        "AssumedRoleUserId":"34458433936495****:alice"
        },
    "RequestId": "6894B13B-6D71-4EF5-88FA-F32781734A7F"
}
```

错误码

HttpCode	错误码	错误信息	描述
400	InvalidParameter	The parameter RoleArn is wrongly formed.	角色ARN格式错误。
400	InvalidParameter.RoleArn	The parameter RoleArn is wrongly formed.	角色ARN格式错误。
400	InvalidParameter.RoleSessionName	The parameter RoleSessionName is wrongly formed.	RoleSessionName格式错误，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\.@\-_]+$。
400	InvalidParameter.DurationSeconds	The Min/Max value of DurationSeconds is 15min/1hr.	DurationSeconds参数设置错误，取值范围：900~3600秒。
400	InvalidParameter.PolicyGrammar	The parameter Policy has not passed grammar check.	权限策略语法错误。
400	InvalidParameter.PolicySize	The size of Policy must be smaller than 1024 bytes.	权限策略长度超限，最大不超过1024字节。

HttpCode	错误码	错误信息	描述
403	NoPermission	You are not authorized to do this action. You should be authorized by RAM.	STS token没有权限。
500	InternalError	STS Server Internal Error happened.	服务器内部错误。

3.2 GetCallerIdentity

调用GetCallerIdentity接口获取当前调用者的身份信息。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	GetCallerIdentity	系统规定参数。取值：GetCallerIdentity

返回数据

名称	类型	示例值	描述
RequestId	String	2C9BE469-4A35-44D5-9529-CAA280B11603	请求ID。
Arn	String	acs:ram::196813200012****:user/admin	当前调用者的ARN。
AccountId	String	196813200012****	当前调用者所属云帐号的数字ID。
UserId	String	216959339000****	· 如果当前调用者是RAM用户，则返回当前调用者的UID。 · 如果当前调用者是云帐号，则返回当前调用者云账号ID。
RoleId	String	33537620082992****	如果当前调用者是RAM角色，则返回当前调用者的角色ID。
PrincipalId	String	28877424437521****	身份标识。

名称	类型	示例值	描述
IdentityType	String	RAMUser	身份类型。

示例

请求示例

```
https://sts.aliyuncs.com?Action=GetCallerIdentity
&<公共请求参数>
```

返回示例

`XML`**格式**

```
<GetCallerIdentityResponse>
    <RequestId>2C9BE469-4A35-44D5-9529-CAA280B11603</RequestId>
    <AccountId>196813200012****</AccountId>
    <UserId>216959339000****</UserId>
    <IdentityType>RAMUser</IdentityType>
    <PrincipalId>28877424437521****</PrincipalId>
    <Arn>acs:ram::196813200012****:user/admin</Arn>
</GetCallerIdentityResponse>
```

`JSON`**格式**

```
{
    "RequestId": "2C9BE469-4A35-44D5-9529-CAA280B11603",
    "AccountId": "196813200012****",
    "UserId": "216959339000****",
    "IdentityType": "RAMUser",
    "PrincipalId": "28877424437521****",
    "Arn": "acs:ram::196813200012****:user/admin"
}
```

错误码

无。

3.3 AssumeRoleWithSAML

进行角色SSO时，通过调用AssumeRoleWithSAML接口，可以获取一个扮演该角色的临时身份。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	AssumeRoleWithSAML	系统规定参数，取值：AssumeRoleWithSAML

名称	类型	是否必选	示例值	描述
SAMLProviderArn	String	是	acs:ram::1234567890 12****:saml-provider/company1	RAM中创建的身份提供商的ARN。格式：acs:ram::$account_ID:saml-provider/$saml_provider_ID。
RoleArn	String	是	acs:ram::1234567890 12****:role/adminrole	要扮演的角色的ARN。格式：acs:ram::$accountID:role/$roleName。
SAMLAssertion	String	是	<base64_encoded_saml_assertion>	Base64编码后的SAML断言。长度限制：4~100000字节。
Policy	String	否	<url_encoded_policy>	长度限制为1024字节。此参数可以限制生成STS token的权限，若不指定则返回的token拥有指定角色的所有权限。
DurationSeconds	Long	否	3600	指定的过期时间，单位为秒。过期时间范围：900~3600秒，默认值为：3600秒。

返回数据

名称	类型	示例值	描述
RequestId	String	6894B13B-6D71-4EF5-88FA-F32781734A7F	请求ID。
Credentials			访问凭证。
└ AccessKeyId	String	STS.L4aBSCSJVMuKg5U1****	访问密钥标识。
└ AccessKeySecret	String	wyLTSmsyPGP1ohvvw8xYgB29dlGI8KMiH2pK****	访问密钥。
└ SecurityToken	String	********	安全令牌。
└ Expiration	String	2015-04-09T11:52:19Z	失效时间。

名称	类型	示例值	描述
AssumedRoleUser			角色扮演临时身份。
└Arn	String	acs:sts::123456789012****:assumed-role/AdminRole/alice	扮演的临时身份的ARN。格式：acs:ram::$accountID:assumed-role/$roleName/$roleSessionName。
└AssumedRoleUserId	String	34458433936495****:alice	该角色临时身份的用户ID。
SAMLAssertionInfo			SAML断言中的部分信息。
└SubjectType	String	persistent	SAML断言中NameID的格式。当前缀为urn:oasis:names:tc:SAML:2.0:nameid-format:时，前缀会被移除。例如：persistant/transient。
└Subject	String	alice@example.com	SAML断言中Subject - NameID字段的值。
└Recipient	String	https://signin.aliyun.com/saml-role/SSO	SAML断言中Subject - SubjectConfirmation - SubjectConfirmationData字段中Recipient属性的值。
└Issuer	String	http://example.com/adfs/services/trust	SAML断言中Issuer字段的值。

示例

> **说明:**
> 由于SAMLAssertion参数较长，可能会导致GET请求失败，请您使用POST方法发送此请求。

返回示例

XML格式

```
<AssumeRoleResponse>
    <RequestId>6894B13B-6D71-4EF5-88FA-F32781734A7F</RequestId>
    <AssumedRoleUser>
        <arn>acs:sts::123456789012****:assumed-role/AdminRole/alice</
arn>
```

```
        <AssumedRoleUserId>34458433936495****:alice</AssumedRoleUserId
>
    </AssumedRoleUser>
    <Credentials>
        <AccessKeyId>STS.L4aBSCSJVMuKg5U1****</AccessKeyId>
        <AccessKeySecret>wyLTSmsyPGP1ohvvw8xYgB29dlGI8KMiH2pK****</
AccessKeySecret>
        <SecurityToken>********</SecurityToken>
        <Expiration>2015-04-09T11:52:19Z</Expiration>
    </Credentials>
    <SAMLAssertionInfo>
        <SubjectType>persistent</SubjectType>
        <Subject>alice@example.com</Subject>
        <Recipient>https://signin.aliyun.com/saml-role/SSO</Recipient>
        <Issuer>http://example.com/adfs/services/trust</Issuer>
    </SAMLAssertionInfo>
</AssumeRoleResponse>
```

JSON格式

```
{
    "Credentials": {
        "AccessKeyId": "STS.L4aBSCSJVMuKg5U1****",
        "AccessKeySecret": "wyLTSmsyPGP1ohvvw8xYgB29dlGI8KMiH2pK****",
        "Expiration": "2015-04-09T11:52:19Z",
        "SecurityToken": "********"
    },
    "AssumedRoleUser": {
        "arn": "acs:sts::1234567890123456:assumed-role/AdminRole/alice
",
        "AssumedRoleUserId":"34458433936495****:alice"
        },
    "SAMLAssertionInfo": {
        "SubjectType": "persistent",
        "Subject": "alice@example.com",
        "Recipient": "https://signin.aliyun.com/saml-role/SSO",
        "Issuer": "http://example.com/adfs/services/trust"
    },
    "RequestId": "6894B13B-6D71-4EF5-88FA-F32781734A7F"
}
```

错误码

HttpCode	错误码	错误信息	描述
400	MissingParameter.SAMLAssertion	Parameter SAMLAssertion is required.	缺少SAMLAssertion参数。
400	MissingParameter.SAMLProviderArn	Parameter SAMLProviderArn is required.	缺少SAMLProviderArn参数。
400	MissingParameter.RoleArn	Parameter RoleArn is required.	缺少RoleArn参数。
400	InvalidParameter.PolicyGrammar	Invalid Policy.	无效的权限策略。

HttpCode	错误码	错误信息	描述
400	InvalidParameter.PolicySize	The max size of policy string is 1024.	权限策略字符串长度超限，最大不超过1024字节。
400	InvalidParameter.RoleSessionName	The RoleSessionName is invalid.	角色会话名称无效。
400	InvalidParameter.DurationSeconds	The DurationSeconds is invalid.	DurationSeconds无效。
404	EntityNotExist.SAMLProvider	Can not find SAML provider.	找不到SAML身份提供商。
404	EntityNotExist.RoleArn	The specified Role does not exists.	指定的角色不存在。
401	AuthenticationFail.IDPMetadata.Invalid	The IdP Metadata of your SAML Provider is invalid.	SAML身份提供商的IdP元数据无效。
401	AuthenticationFail.SAMLAssertion.Expired	The SAML Assertion is expired.	SAML断言已过期。
401	AuthenticationFail.SAMLAssertion.Invalid	The SAML Assertion is invalid.	SAML断言无效。