Alibaba Cloud Resource Access Management

API参考

檔案版本：20181211

目錄

1 簡介

STS介紹

阿里雲STS (Security Token Service) 是為阿里雲帳號（或RAM使用者）提供短期存取權限管理的雲端服務。通過STS，您可以為同盟使用者（您的本地帳號系統所管理的使用者）頒發一個自訂時效和存取權限的訪問憑證。同盟使用者可以使用STS短期訪問憑證直接調用阿里雲服務API，或登入阿里雲管理主控台操作被授權訪問的資源。

訪問點

STS的預設訪問點地址是: `https://sts.aliyuncs.com` ，使用者必須使用https接入訪問點。

術語表

術語	中文	說明
Federated identity	同盟使用者身份	同盟使用者的身份認證由客戶自己管理
Policy	存取原則	用來描述授權策略的一種描述語言
Grantor	授權者	授權令牌的頒發者(雲帳號或RAM使用者)
Name	被授權者	授權令牌的使用者(即同盟使用者)

2 調用方式

2.1 請求結構

服務地址

STS服務地址請參考####。

通訊協定

為了保證通訊的安全性，STS服務僅支援使用HTTPS安全通道發送請求。

HTTP要求方法

支援HTTP GET/POST方法發送請求，這種方式下請求參數需要包含在請求的URL中。(GET請求最大不得超過4KB, POST請求最大不得超過10MB)。

請求參數

每個請求都需要指定要執行的操作，即Action參數（例如AddUser），以及每個操作介面都需要包含的公用請求參數和指定操作介面所特有的請求參數。

字元編碼

請求及返回結果都使用UTF-8字元集進行編碼。

2.2 公用參數

Format

- 名稱: Format
- 類型: String
- 必須: 否
- 說明: 傳回值的類型，支援JSON與XML，預設為XML。

Version

- 名稱: Version
- 類型: String
- 必須: 是
- 說明: API版本號碼，為日期形式：YYYY-MM-DD，本版本對應為2015-04-01。

AccessKeyId

- 名稱: AccessKeyId

- 類型: String
- 必須: 是
- 說明: 阿里雲頒發給使用者的訪問服務所用的密鑰ID。

Signature

- 名稱: Signature
- 類型: String
- 必須: 是
- 說明: 簽名結果串，關於簽名的計算方法，請參見簽名機制。

SignatureMethod

- 名稱: SignatureMethod
- 類型: String
- 必須: 是
- 說明: 簽名方式，目前僅支援HMAC-SHA1。

SignatureVersion

- 名稱: SignatureVersion
- 類型: String
- 必須: 是
- 說明: 簽名演算法版本，目前版本是1.0

SignatureNonce

- 名稱: SignatureNonce
- 類型: String
- 必須: 是
- 說明: 唯一隨機數，用於防止網路重放攻擊。使用者在不同請求間要使用不同的隨機數值。

Timestamp

- 名稱: Timestamp
- 類型: String
- 必須: 是
- 說明: 請求的時間戳記。日期格式按照ISO8601標準表示，並需要使用UTC時間。格式為：`YYYY-MM-DDThh:mm:ssZ`。 例如，2013-01-10T12:00:00Z（為北京時間2013年1月10日20點0分0秒）

2.3 返回結果

調用API服務後返回資料採用統一格式，返回的HTTP狀態代碼為2xx，代表調用成功；返回4xx或5xx的HTTP狀態代碼代表調用失敗。調用成功返回的資料格式主要有XML和JSON兩種，外部系統可以在請求時傳入參數來制定返回的資料格式，預設為XML格式。本文檔中的返回樣本為了便於使用者查看，做了格式化處理，實際返回結果是沒有進行換行、縮排等處理的。

成功結果

- **XML**樣本

  XML返回結果包括請求是否成功資訊和具體的業務資料。樣本如下：

```
<?xml version="1.0" encoding="utf-8"?>
<!—結果的根結點-->
<介面名稱+Response>
    <!—返回請求標籤-->
    <RequestId>4C467B38-3910-447D-87BC-AC049166F216</RequestId>
    <!—返回結果資料-->
</介面名稱+Response>
```

- **JSON**樣本

```
{
    "RequestId": "4C467B38-3910-447D-87BC-AC049166F216",
    /* 返回結果資料 */
}
```

錯誤結果

調用介面出錯後，將不會返回結果資料。調用方可根據附表<錯誤碼表>來定位錯誤原因。

當調用出錯時，HTTP請求返回一個4xx或5xx的HTTP狀態代碼。返回的訊息體中是具體的錯誤碼及錯誤資訊。另外還包含一個全域唯一的請求ID：RequestId和一個您該次請求訪問的網站ID：HostId。在調用方找不到錯誤原因時，可以聯絡阿里雲客服，並提供該HostId和RequestId，以便我們儘快幫您解決問題。

- **XML**樣本

```
<?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**樣本

```
{
    "RequestId": "7463B73D-35CC-4D19-A010-6B8D65D242EF",
```

```
    "HostId": "sts.aliyuncs.com",
    "Code": "InvalidParameter",
    "Message": "The specified parameter \"Action or Version\" is not
 valid."
}
```

2.4 簽名

STS服務會對每個訪問的請求進行身分識別驗證，所以無論使用HTTP還是HTTPS協議提交請求，都需要在請求中包含簽名（Signature）資訊。STS通過使用**Access Key ID**和**Access Key Secret**進行對稱式加密的方法來驗證請求的寄件者身份。**Access Key ID**和**Access Key Secret**由阿里雲官方頒發給訪問者（可以通過阿里雲官方網站申請和管理），其中**Access Key ID**用於標識訪問者的身份；**Access Key Secret**是用於加密簽名字串和伺服器端驗證簽名字串的密鑰，必須嚴格保密，只有阿里雲和使用者知道。

簽名步驟

1. 使用請求參數構造正常化的請求字串（Canonicalized Query String）
    1. 按照參數名稱的字典順序對請求中所有的請求參數（包括文檔中描述的“公用請求參數”和給定了的請求介面的自訂參數，但不能包括“公用請求參數”中提到Signature參數本身）進行排序。

        说明：
        當使用GET方法提交請求時，這些參數就是請求URI中的參數部分（即URI中“?”之後由“&”串連的部分）。
    2. 對每個請求參數的名稱和值進行編碼。名稱和值要使用UTF-8字元集進行URL編碼，URL編碼的編碼規則是：
        - 對於字元 A-Z、a-z、0-9以及字元“-”、“_”、“.”、“~”不編碼；
        - 對於其他字元編碼成“%XY”的格式，其中XY是字元對應ASCII碼的16進位表示。比如英文的雙引號（"）對應的編碼就是%22
        - 需要說明的是英文空格（ ）要被編碼是%20，而不是加號（+）。

        说明：
        一般支援URL編碼的庫（比如Java中的java.net.URLEncoder）都是按照“application/x-www-form-urlencoded”的MIME類型的規則進行編碼的。實現時可以直接使用這類方式進行編碼，把編碼後的字串中加號（+）替換成%20、星號（*）替換成%2A、%7E替換回波浪號（~），即可得到上述規則描述的編碼字串。
    3. 對編碼後的參數名稱和值使用英文等號（=）進行串連。

4. 再把英文等號串連得到的字串按參數名稱的字典順序依次使用&符號串連，即得到正常化請求字串。

2. 使用上一步構造的正常化字串按照下面的規則構造用於計算簽名的字串：

```
StringToSign=
HTTPMethod + “&” +
percentEncode(“/”) + ”&” +
percentEncode(CanonicalizedQueryString)
```

其中HTTPMethod是提交請求用的HTTP方法，比GET。 percentEncode(“/”)是按照1.b中描述的URL編碼規則對字元“/”進行編碼得到的值，即“%2F”。

percentEncode(CanonicalizedQueryString)是對第1步中構造的正常化請求字串按1.b中描述的URL編碼規則編碼後得到的字串。

3. 按照*RFC2104*的定義，使用上面的用於簽名的字串計算簽名HMAC值。注意：計算簽名時使用的Key就是使用者持有的Access Key Secret並加上一個“&”字元(ASCII:38)，使用的雜湊演算法是SHA1。
4. 按照Base64編碼規則把上面的HMAC值編碼成字串，即得到簽名值（Signature）。
5. 將得到的簽名值作為Signature參數添加到請求參數中，即完成對請求籤名的過程。 注意：得到的簽名值在作為最後的請求參數值提交給STS伺服器的時候，要和其他參數一樣，按照RFC3986的規則進行URL編碼）。

樣本

以AssumeRole為例，簽名前的請求URL為：

```
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
```

對應的StringToSign是：

```
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
```

假如使用的Access Key Id是“testid”，Access Key Secret是“testsecret”，用於計算HMAC的Key就是“testsecret&”，則計算得到的簽名值是：

```
gNI7b0AyKZHxDgjBGPDgJ1Ce3L4=
```

簽名後的請求URL為（注意增加了Signature參數）：

```
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
```

3 操作介面

3.1 AssumeRole

介面描述

通過該介面，擷取一個扮演該角色的臨時身份。

請求參數

Action

- 類型：String
- 必須：是
- 描述：系統規定參數，取值：AssumeRole

RoleArn

- 類型：String
- 必須：是
- 描述：指定角色的全域資源描述符(Aliyun Resource Name，簡稱Arn)。每個角色都有一個唯一的全域資源描述符，規定格式為 acs:ram::$accountID:role/$roleName ，一個範例：acs:ram::1234567890123456:role/samplerole 。您可以在RAM控制台的角色管理頁面RAM控制台的角色管理列表中，進入角色詳情頁可以查看一個角色的RoleArn。

RoleSessionName

- 類型：String
- 必須：是
- 描述：使用者自訂參數。此參數用來區分不同的Token，可用於使用者層級的訪問審計。
- 格式：

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

2-32個字元

Policy

- 名稱：Policy
- 類型：String
- 必須：否

- 描述：授權策略*Policy ####*，Policy長度限制為1024位元組；您可以通過此參數限制產生的Token的許可權，不指定則返回的Token將擁有指定角色的所有許可權。

DurationSeconds

- 名稱：DurationSeconds
- 類型：Integer
- 必須：否
- 描述：指定的到期時間，單位為秒。到期時間範圍：900 ~ 3600，預設值為3600。

返回參數

Credentials

- 類型：*Credentials*
- 描述：訪問憑證

AssumedRoleUser

- 描述：角色扮演臨時身份

操作樣本

HTTP Request

```
https://sts.aliyuncs.com?Action=AssumeRole
&RoleArn=acs:ram::1234567890123456:role/adminrole
&RoleSessionName=alice
&DurationSeconds=3600
&Policy=<url_encoded_policy>
&<公用請求參數>
```

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"
}
```

3.2 GetCallerIdentity

介面描述

通過該介面，可以擷取當前調用者的身份資訊。

請求參數

Action

- 類型：String
- 必須：是
- 描述：系統規定參數，取值：GetCallerIdentity

返回參數

AccountId

- 類型：String
- 描述：當前調用者所屬雲帳號的數字ID

UserId

- 類型：String
- 描述：當前調用者的使用者ID。如果當前調用者是雲帳號，則傳回值與AccountId相同。

Arn

- 類型：String
- 描述：當前調用者的阿里雲資源描述符(Aliyun Resource Names)

操作樣本

HTTP Request

```
https://sts.aliyuncs.com?Action=GetCallerIdentity
&<公用請求參數>
```

HTTP Response

- **XML**格式

```
<GetCallerIdentityResponse>
    <RequestId>2C9BE469-4A35-44D5-9529-CAA280B11603</RequestId>
    <AccountId>1968132000123456</AccountId>
    <UserId>216959339000654321</UserId>
    <Arn>acs:ram::1968132000123456:user/admin</Arn>
</GetCallerIdentityResponse>
```

- **JSON**格式

```
{
    "RequestId": "2C9BE469-4A35-44D5-9529-CAA280B11603",
    "AccountId": "1968132000123456",
    "UserId": "216959339000654321",
    "Arn": "acs:ram::1968132000123456:user/admin"
}
```

4 資料類型

4.1 Credentials

描述

訪問憑證

節點名稱

Credentials

子節點

AccessKeyId

- 類型：String
- 描述：存取金鑰標識

AccessKeySecret

- 類型：String
- 描述：存取金鑰

SecurityToken

- 類型：String
- 描述：安全性權杖

Expiration

- 類型：String
- 描述：失效時間

4.2 AssumedRoleUser

描述

通過扮演角色介面擷取的臨時身份

節點名稱

AssumedRoleUser

子節點

Arn

- 類型：String
- 描述：該角色臨時身份的資源描述符

AssumedRoleUserId

- 類型：String
- 描述：該角色臨時身份的使用者ID

5 附錄

5.1 錯誤碼表

HTTP Status 400

InvalidParameterInvalidParameter.RoleArn

- HTTP Status: 400
- ErrorMessage: The parameter RoleArn is wrongly formed.

InvalidParameter.RoleSessionName

- HTTP Status: 400
- ErrorMessage: The parameter RoleSessionName is wrongly formed.

InvalidParameter.DurationSeconds

- HTTP Status: 400
- ErrorMessage: The Min/Max value of DurationSeconds is 15min/1hr.

InvalidParameter.PolicyGrammar

- HTTP Status: 400
- ErrorMessage: The parameter Policy has not passed grammar check.

InvalidParameter.PolicySize

- HTTP Status: 400
- ErrorMessage: The size of Policy must be smaller than 1024 bytes.

HTTP Status 403

NoPermission

- HTTP Status: 403
- ErrorMessage: You are not authorized to do this action. You should be authorized by RAM.

HTTP Status 500

InternalError

- HTTP Status: 500
- ErrorMessage: STS Server Internal Error happened.

5.2 服務地址

服務地址選擇建議

- 每個服務地址功能完全一樣，請盡量同Region調用；
- Endpoint類型
  - 公網：互連網訪問地址；
  - VPC：可在同Region內VPC中訪問，無需開放公網存取權限；

服務地址

表 **5-1:** 國內中心

地區	網域名稱
國內中心	公網:sts.aliyuncs.com

表 **5-2:** 大中華區

地區	**RegionId**	網域名稱
華東 1-杭州	cn-hangzhou	• 公網:sts.cn-hangzhou.aliyuncs.com • VPC:sts-vpc.cn-hangzhou.aliyuncs.com
華東 2-上海	cn-shanghai	• 公網:sts.cn-shanghai.aliyuncs.com • VPC:sts-vpc.cn-shanghai.aliyuncs.com
華南 1-深圳	cn-shenzhen	• 公網:sts.cn-shenzhen.aliyuncs.com • VPC: sts-vpc.cn-shenzhen.aliyuncs.com
華北 1-青島	cn-qingdao	公網:sts.cn-qingdao.aliyuncs.com
華北 2-北京	cn-beijing	• 公網:sts.cn-beijing.aliyuncs.com • VPC:sts-vpc.cn-beijing.aliyuncs.com

地區	RegionId	網域名稱
華北 3-張家口	cn-zhangjiakou	• 公網:sts.cn-zhangjiakou.aliyuncs.com • VPC:sts-vpc.cn-zhangjiakou.aliyuncs.com
華北 5-呼和浩特	cn-huhehaote	• 公網:sts.cn-huhehaote.aliyuncs.com • VPC:sts-vpc.cn-huhehaote.aliyuncs.com
香港	cn-hongkong	• 公網:sts.cn-hongkong.aliyuncs.com • VPC:sts-vpc.cn-hongkong.aliyuncs.com

表 **5-3:** 亞太地區

地區	RegionId	網域名稱
亞太地區東南 1 (新加坡)	ap-southeast-1	公網:sts.ap-southeast-1.aliyuncs.com
亞太地區東南 2 (雪梨)	ap-southeast-2	公網:sts.ap-southeast-2.aliyuncs.com
亞太地區東南 3 (吉隆坡)	ap-southeast-3	公網:sts.ap-southeast-3.aliyuncs.com
亞太地區東南 5 (雅加達)	ap-southeast-5	公網:sts.ap-southeast-5.aliyuncs.com
亞太地區東北 1 (東京)	ap-northeast-1	公網:sts.ap-northeast-1.aliyuncs.com
亞太地區南部 1 (孟買)	ap-south-1	公網:sts.ap-south-1.aliyuncs.com

表 **5-4:** 美洲-歐洲

地區	RegionId	網域名稱
美國西部 1 (矽谷)	us-west-1	公網:sts.us-west-1.aliyuncs.com

地區	RegionId	網域名稱
美國東部 1 (維吉尼亞)	us-east-1	公網:sts.us-east-1.aliyuncs.com
歐洲中部 1 (法蘭克福)	eu-central-1	公網:sts.eu-central-1.aliyuncs.com
中東東部 1 (杜拜)	me-east-1	公網:sts.me-east-1.aliyuncs.com

6 API 參考（STS）