

Alibaba Cloud

##控制

開発者ガイド (STS)

Document Version 20200129

目次

1 概要.....	1
2 呼び出す方法.....	2
2.1 リクエストの構成.....	2
2.2 サービスリージョン.....	2
2.3 共通パラメータ.....	5
2.4 署名のしくみ.....	6
2.5 戻り値の処理.....	9
3 操作インターフェイス.....	11
3.1 ロールの引き受け (AssumeRole)	11
3.2 呼び出し元のIDの取得 (GetCallerIdentity)	13
3.3 AssumeRoleWithSAML.....	14
4 (旧バージョン) API リファレンス (STS).....	20
4.1 付録.....	20
4.1.1 エラーコード.....	20
4.2 データ型.....	21
4.2.1 Credentials.....	21
4.2.2 AssumedRoleUser.....	21

1 概要

STS概要

Alibaba Cloudセキュリティトークンサービス (STS) は **Alibaba Cloud** アカウント (または**RAM**ユーザー) に短期のアクセス権限管理を提供します。STSを通して、フェデレーションユーザー (ローカルアカウントシステムで管理される) 向けに有効期限とアクセス権限をカスタマイズしたアクセス資格情報を発行できます。フェデレーションユーザーは、STSの一時的アクセス資格情報を使用することにより、**Alibaba Cloud**サービスAPIを直接呼び出すことや、**Alibaba Cloud**管理コンソールにログインして権限付与されたリソースにアクセスすることができます。

アクセスポイント

デフォルトSTSアクセスポイント: <https://sts.aliyuncs.com>。アクセスポイントに接続するにはHTTPSを利用しなければなりません。

用語集

用語	説明	解説
フェデレーションID	フェデレーションユーザーのID	フェデレーションユーザーIDはカスタマーにより管理されます。
ポリシー	アクセスポリシー	権限付与ポリシーを記述するための言語。
権限付与者	権限付与する人	権限付与トークンの発行者 (Alibaba Cloud アカウントまたは RAM ユーザー)
名前	権限付与される人	権限付与トークンの使用者 (フェデレーションユーザー)

2 呼び出す方法

2.1 リクエストの構成

エンドポイント

STSサービスのアクセスURL：[サービスリージョン](#)。

通信プロトコル

通信セキュリティを確保するため、STSサービスのリクエスト送信はHTTPSセキュアチャネルのみを使用します。

HTTPリクエストメソッド

HTTP GET/POSTリクエストを送信できます。このメソッドを使用するには、リクエストパラメータが含まれたリクエストURLが必要です。(GET リクエストのサイズは4 KBまで、POST リクエストのサイズは10MB までです)。

リクエストパラメータ

各リクエストに「Action」パラメータ（「AddUser」など）を使用して、実行する操作を指定する必要があります。また、パブリックリクエストパラメータとインターフェイスパラメータを指定する必要があります。

文字エンコーディング

リクエストと応答はUTF-8によりエンコードされます。

2.2 サービスリージョン

サービスリージョンの選択

- ・ すべてのリージョンにおける機能はまったく同じですので、呼び出しは同一リージョン内で行うことをお勧めします。
- ・ エンドポイント種類
 - パブリックネットワーク：インターネットアクセスアドレス
 - VPC：パブリックアクセス権限なしで同一リージョン内のVPCからアクセス可能

サービスリージョン

表 2-1 : 中国IDC

リージョン	ドメイン名
中国IDC	パブリックネットワーク: sts.aliyuncs.com

表 2-2 : 中国

リージョン	リージョンID	ドメイン名
中国東部1-杭州	cn-hangzhou	- パブリックネットワーク: sts.cn-hangzhou.aliyuncs.com - VPC: sts-vpc.cn-hangzhou.aliyuncs.com
中国東部2-上海	cn-shanghai	- パブリックネットワーク: sts.cn-shanghai.aliyuncs.com - VPC: sts-vpc.cn-shanghai.aliyuncs.com
中国南部1-深セン	cn-shenzhen	- パブリックネットワーク: sts.cn-shenzhen.aliyuncs.com - VPC: sts-vpc.cn-shenzhen.aliyuncs.com
中国北部1-青島	cn-qingdao	パブリックネットワーク: sts.cn-qingdao.aliyuncs.com
中国北部2-北京	cn-beijing	- パブリックネットワーク: sts.cn-beijing.aliyuncs.com - VPC: sts-vpc.cn-beijing.aliyuncs.com
中国北部3-張家口	cn-zhangjiakou	- パブリックネットワーク: sts.cn-zhangjiakou.aliyuncs.com - VPC: sts-vpc.cn-zhangjiakou.aliyuncs.com

リージョン	リージョンID	ドメイン名
中国北部5-フフホト	cn-huhehaote	- パブリックネットワーク: sts.cn-huhehaote.aliyuncs.com - VPC: sts-vpc.cn-huhehaote.aliyuncs.com
香港	cn-hongkong	- パブリックネットワーク: sts.cn-hongkong.aliyuncs.com - VPC: sts-vpc.cn-hongkong.aliyuncs.com

表 2-3: アジア太平洋

リージョン	リージョンID	ドメイン名
アジア太平洋 SE 1 (シンガポール)	ap-southeast-1	パブリックネットワーク: sts.ap-southeast-1.aliyuncs.com
アジア太平洋 SE 2 (シドニー)	ap-southeast-2	パブリックネットワーク: sts.ap-southeast-2.aliyuncs.com
アジア太平洋 SE 3 (クアラルンプール)	ap-southeast-3	パブリックネットワーク: sts.ap-southeast-3.aliyuncs.com
アジア太平洋 SE 5 (ジャカルタ)	ap-southeast-5	パブリックネットワーク: sts.ap-southeast-5.aliyuncs.com
アジア太平洋 NE 1 (東京)	ap-northeast-1	パブリックネットワーク: sts.ap-northeast-1.aliyuncs.com
アジア太平洋 South 1 (ムンバイ)	ap-south-1	パブリックネットワーク: sts.ap-south-1.aliyuncs.com

表 2-4: アメリカ - ヨーロッパ

リージョン	リージョンID	ドメイン名
アメリカ西部 1 (シリコンバレー)	us-west-1	パブリックネットワーク: sts.us-west-1.aliyuncs.com
アメリカ東部 1 (バージニア州)	us-east-1	パブリックネットワーク: sts.us-east-1.aliyuncs.com
ドイツ 1 (フランクフルト)	eu-central-1	パブリックネットワーク: sts.eu-central-1.aliyuncs.com
中東 1 (ドバイ)	me-east-1	パブリックネットワーク: sts.me-east-1.aliyuncs.com

2.3 共通パラメータ

Format

- ・ 名前: **Format**
- ・ データ型: **String**
- ・ 必須項目: いいえ
- ・ 戻り値のデータ型。「JSON」と「XML」が対応されます。デフォルトでは「XML」になります。

Version

- ・ 名前: **Version**
- ・ データ型: **String**
- ・ 必須項目: はい
- ・ APIバージョン番号。「YYYY-MM-DD」形式です。現在のバージョン番号は「2015-12-01」です。

AccessKeyId

- ・ 名前: **AccessKeyId**
- ・ データ型: **String**
- ・ 必須項目: はい
- ・ Alibabaクラウドがユーザーのために発行したアクセスキーIDです。

Signature

- ・ 名前: **Signature**

- ・ データ型：**String**
- ・ 必須項目：はい
- ・ 署名結果の文字列。署名の計算方法については、「署名のしかけ」を参照してください。

SignatureMethod

- ・ 名前：**SignatureMethod**
- ・ データ型：**String**
- ・ 必須項目：はい
- ・ 署名方法。現時点では、「**HMAC-SHA1**」のみに対応しています。

SignatureVersion

- ・ 名前：**SignatureVersion**
- ・ データ型：**String**
- ・ 必須項目：はい
- ・ 説明：署名アルゴリズムのバージョン、現在のバージョンは**1.0**です。

SignatureNonce

- ・ 名前：**SignatureNonce**
- ・ データ型：**String**
- ・ 必須項目：はい
- ・ ユニークな乱数で、ネットワーク反射攻撃を防ぎます。リクエストごとに異なる乱数を使用する必要があります。

Timestamp

- ・ 名前：**Timestamp**
- ・ データ型：**String**
- ・ 必須項目：はい
- ・ 説明：リクエストのタイムスタンプ。日付形式は**ISO8601** 標準に従っており、**UTC** 時刻が使用されます。タイムスタンプ形式の例を次に示します。YYYY-MM-DDThh:mm:ssZ。例：
2013-01-10T12:00:00Z (北京現地時間 1/10/2013 20:00:00 と同じ)

2.4 署名のしくみ

STSサービスは、アクセスリクエストするたびにID認証を行います。それにより、**HTTP**または**HTTPS**を通じて送信する場合は、リクエストには署名情報が含まれる必要があります。

STSは**AccessKey ID**と**AccessKey Secret** を通じての対称暗号化という方式でリクエスト送信

者の個人情報を認証します。AccessKey IDとAccess Key Secretは、Alibabaクラウドよりリクエスト送信者に対して公式に発行されます（クエスト送信者はAlibabaクラウドの公式Webサイトでこれらの情報を申請し、管理できます）。AccessKey IDはリクエスト送信者のIDを示します。AccessKey Secretは署名文字列を暗号化するために使用される秘密鍵であり、サーバーで署名文字列を認証する際にも用いられます。この情報は機密として厳密に取り扱い、Alibabaクラウドと認証済みリクエスト送信者以外には知られないようにしてください。

リクエスト署名プロセス

1. リクエストパラメータを使用して、正規化クエリ文字列を作成します。

- a. すべてのリクエストパラメータ（「パブリックリクエストパラメーター」と、このドキュメントで取り上げる任意のリクエストインターフェイスに対するユーザー定義パラメータが含まれますが、「パブリックリクエストパラメータ」に説明のあるSignatureパラメータは含まれません）をパラメーター名のアルファベット順に並べ替えます。



注：

「GET」メソッドを使用してリクエストを送信する際に、これらのパラメータはリクエスト URL (URLのアンパーサンド「&」に続く疑問符「?」の後ろの部分) に含まれます。

- b. 各リクエストパラメータの名前と値をエンコードします。UTF-8 文字セットを使用した URL エンコードが必要です。URL エンコーディングのルールは次のとおりです。
 - ・ 大文字 (A ~ Z)、小文字 (a ~ z)、整数 (0 ~ 9)、および一部の記号 (ハイフン “-”、アンダーバー “_”、ピリオド “.”、チルダ “~” など) はエンコードされません。
 - ・ 他の文字は “%XY” 形式でエンコードします。この XY は、文字の ASCII コードを 16 進表記することを意味します。たとえば、二重引用符 (“ ”) は “%22” です。
 - ・ 半角スペース () はプラス記号 “+” ではなく、“%20” としてエンコードされることに注意してください。



注：

一般的に、URL エンコーディングされたライブラリ (Java の「`java.net.URLEncoder`」など) は、「`application/x-www-form-urlencoded`」形式の MIME タイプのルールに基づいてエンコードされます。このエンコーディング方法を使用するには、前述のエンコーディングルールに合わせて、エンコードされた文字列内のプラス記号 “+” を

「%20」に、アスタリスク「*」を「%2A」に直接置き換え、「%7E」をチルダ「~」に戻します。

- c. エンコードしたパラメーター名と値を半角の等号「=」で連結します。
 - d. 等号で結んだパラメーター名と値のペアを、アンパーサンド「&」を使用してパラメーター名のアルファベット順に連結して、正規化クエリ文字列を作成します。
2. 次のルールに従って正規化クエリ文字列を使用し、署名計算用の文字列を作成します：

```
StringToSign=
HTTPMethod + "&" +
percentEncode("/") + "&" +
percentEncode(CanonicalizedQueryString)
```

ここで「**HTTPMethod**」は、リクエストの送信に使用する **HTTP** メソッド (“GET” など) です。「**percentEncode (“/”)**」は、**1.b** で説明した **URL** エンコーディングルールに従って文字 “/” をエンコードした値 (“%2F”) です。

「**percentEncode(CanonicalizedQueryString)**」は、**1.b** の **URL** エンコーディングルールに従ってエンコードした正規化クエリ文字列です。

- 3. [RFC2104](#) の定義に基づいて、署名計算のための文字列を使用して署名の **HMAC** 値を計算します。注意: 署名計算に使用するキーは、**Access Key Secret** にアンパーサンド “&” (**ASCII: 38**) を付加したもので、ハッシュアルゴリズム **SHA1** に基づいています。
- 4. **Base64** コーディングルールに基づいて **HMAC** 値を文字列にエンコードし、署名値を取得します。
- 5. 取得した署名値を「**Signature**」パラメータとしてリクエストパラメータに追加し、リクエスト署名プロセスを完了します。注意: 取得した署名値は、最終的なリクエストパラメーター値として **STS** サーバーに送信する前に、他のパラメーターと同様、**RFC3986** ルールに基づいて **URL** エンコーディングする必要があります。

例

「**AssumeRole**」を例として使用した場合、署名前のリクエスト **URL** は次のようになります：

```
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
```

対応する **StringToSign** は：

```
GET&%2F&AccessKeyId%3Dtestid%26Action%3DAssumeRole%26Format%3DJJSON%
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
```

AccessKeyIdパラメータ値を「**testid**」、**AccessKeySecret**パラメータ値を「**testsecret**」とすると、**HMAC**の計算に使用する**Key**は「**Testsecret&**」、計算結果の署名値は次のようになります：

```
gNI7b0AyKZHxDgjBGPdgJ1Ce3L4=
```

署名付きリクエストURLは次のようになります(「**Signature**」パラメータが追加されています)。

```
https://sts.aliyuncs.com/?SignatureVersion=1.0&Format=JSON&Timestamp=2015-09-01T05%3A57%3A34Z&RoleArn=acs%3Aarn%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 戻り値の処理

APIを呼び出した後、データは一律な形式で返されます。返された**HTTP**ステータスコードが**2xx**である場合、呼び出しは成功です。返された**HTTP**ステータスコードが**4xx**、或いは**5xx**の場合、呼び出しは失敗です。呼び出しが成功した場合、データは主に**XML**と**JSON**の2種類の形式で返されます。リクエストの送信時に、外部システムはパラメータで返されるデータの形式を指定できます。デフォルト形式は**XML**です。本ドキュメントでは、返された結果の例を読みやすい形式で表示しています。実際の結果は、改行やインデントなどで体裁が整えられているわけではありません。

成功時の結果

- **XML**の例

XML形式で返された結果には、リクエストが成功したかどうかを示すメッセージと、特定のサービスデータが含まれます。次に例を示します：

```
<? xml version="1.0" encoding="utf-8"? >
<!--Result root node-->
<interface name+Response>
  <!--return request result-->
  <RequestId> </RequestId>
  <!--Return result data-->
</Interface name + response>
```

- **JSON**の例

```
{
  "RequestId": "4C467B38-3910-447D-87BC-AC049166F216",
  /* return result result */
}
```

```
}
```

エラー時の結果

インターフェイス呼び出しでエラーが発生すると、結果が返されません。エラーの原因は、添付の付録の「エラーコード表」で確認できます。

呼び出しでエラーが発生すると、HTTPリクエストに対して**4xx**または**5xx**という形式のHTTPステータスコードが返されます。戻り値のメッセージ本文には、固有のエラーコードとエラーメッセージが含まれています。また、メッセージ本文には、全体でユニークな「**RequestId**」と、リクエストした「**HostId**」も含まれています。エラーの原因を特定できない場合は、**Alibaba**クラウドカスタマーサービスにご連絡ください。その際、よりスムーズに問題を解決できるよう「**HostId**」と「**RequestId**」をご提示ください。

- ・ XML形式の例

```
<? 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形式の例

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

3 操作インターフェイス

3.1 ロールの引き受け (AssumeRole)

インターフェイス説明

このインターフェイスを使用して、ロールを引き受けるための一時的な **ID** を取得できます。

リクエストパラメータ

Action

- ・ データ型: **String**
- ・ 必須項目: はい
- ・ 説明: 必須のシステムパラメータ。パラメータ値は「**AssumeRole**」。

RoleArn

- ・ データ型: **String**
- ・ 必須項目: はい
- ・ 説明: ロールARN。各ロールには、ユニークなリソースデスク립タ (ARN) があります、その形式は: **acs:ram::\$accountID:role/\$roleName** 例: **acs:ram::1234567890123456:role/samplerole** . RAMロール管理でロールのARNを確認できます。

RoleSessionName

- ・ データ型: **String**
- ・ 必須項目: はい
- ・ 説明: このパラメータを通じて各トークンを識別ができるため、特定のトークンを使用するユーザーを示すことができます。監査に役立ちます。
- ・ 形式:

```
^[a-zA-Z0-9\.
```

2-32文字

Policy

- ・ 名前: **Policy**
- ・ データ型: **String**
- ・ 必須項目: いいえ

- ・ 説明：権限付与ポリシー[#unique_10](#)。ポリシーの長さは最大**1024Bytes**までです。このパラメータを通じて生成されるトークンの権限に制限をかけられます。このパラメータを設定しない場合は、返されたトークンには特定のロールの完全な権限を持ちます。

DurationSeconds

- ・ 名前：**DurationSeconds**
- ・ データ型：**Integer**
- ・ 必須項目：いいえ
- ・ 説明：有効期限を秒まで指定できます。設定可能の有効範囲は**900秒～3600秒**で、デフォルト値は**3600**です。

リターンパラメータ

Credentials

- ・ データ型：[Credentials](#)
- ・ 説明：アクセス資格。

AssumedRoleUser

- ・ 説明：ロールを引き受ける一時的**ID**。

操作の例

HTTP リクエスト

```
https://sts.aliyuncs.com?Action=AssumeRole
&RoleArn=acs:ram::1234567890123456:role/adminrole
&RoleSessionName=alice
&DurationSeconds=3600
&Policy=<url_encoded_policy>
&<Public request parameters>
```

HTTP 応答

- ・ **XML形式**

```
<AssumeRoleResponse>
  <RequestId>6894B13B-6D71-4EF5-88FA-F32781734A7F</RequestId>
  <AssumedRoleUser>
    <arn>acs:sts::1234567890123456:assumed-role/AdminRole/alice
  </arn>
    <AssumedRoleId>344584339364951186:alice<AssumedRol
eUserId>
  </AssumedRoleUser>
  <Credentials>
    <AccessKeyId>STS.L4aBSCSJVMuKg5U1vFDw</AccessKeyId>
    <AccessKeySecret>wyLTsmysPGP1ohvww8xYgB29dLGI8KMiH2pKCNZ9</
AccessKeySecret>
    <SecurityToken>CAESrAIIARKAAShQquMnLIlbvEcIx06wCoqJufs8
sWwieUxu45hS9AvKNEte8KRUWiJWJ6Y+YHAPgNwi7yfRecMFydL2uP0gBI7LDi
```

```
o0RkbYlmJfIxHM2nGBPdm17kYEOxmJp2aDhbvvwVYIyt/8iES/R6N208wQh0Pk2bu
+/9dvalp6wOHF4gkFGhhTVFMuTDRhQLNDU0pWTXVLZzVVMXZGRHciBTQzMjc0K
gVhbGljZTCpnJjwySk6BlJzYU1ENUJuCgExGmkKBUFSbG93Eh8KDEFjdGlvb
kVxdWFscxIGQWN0aW9uGgcKBW9zczoqEj8KDlJlc291cmNlRXF1YWxzEghSZ
XNvdXJjZRoJCiFhY3M6b3NzOio6NDMyNzQ6c2FtcGx1Ym94L2FsaWNlLyo=</
SecurityToken>
    <Expiration>2015-04-09T11:52:19Z</Expiration>
</Credentials>
</AssumeRoleResponse>
```

・ JSON形式

```
{
  "Credentials": {
    "AccessKeyId": "STS.L4aBSCSJVMuKg5U1vFDw",
    "AccessKeySecret": "wyLTSmsyPGP1ohvvw8xYgB29dlGI8KMiH2pKCNZ9",
    "Expiration": "2015-04-09T11:52:19Z",
    "SecurityToken": "CAESrAIIARKAAShQquMnLilbvEcIx06wCoqJufs8sWwieUxu45hS9AvKNEte8KRUiJWJ6Y+YHAPgNwi7yfRecMFydL2uP0gBI7LDio0RkbYlmJfIxHM2nGBPdm17kYEOxmJp2aDhbvvwVYIyt/8iES/R6N208wQh0Pk2bu+/9dvalp6wOHF4gkFGhhTVFMuTDRhQLNDU0pWTXVLZzVVMXZGRHciBTQzMjc0KgVhbGljZTCpnJjwySk6BlJzYU1ENUJuCgExGmkKBUFSbG93Eh8KDEFjdGlvbkVxdWFscxIGQWN0aW9uGgcKBW9zczoqEj8KDlJlc291cmNlRXF1YWxzEghSZXNvdXJjZRoJCiFhY3M6b3NzOio6NDMyNzQ6c2FtcGx1Ym94L2FsaWNlLyo="
  },
  "AssumedRoleUser": {
    "arn": "acs:sts::1234567890123456:assumed-role/AdminRole/alice",
    "AssumedRoleUserId": "344584339364951186:alice"
  },
  "RequestId": "6894B13B-6D71-4EF5-88FA-F32781734A7F"
}
```

3.2 呼び出し元のIDの取得 (GetCallerIdentity)

インターフェイス説明

このインターフェイスを通じて、呼び出し元（或いは現在サインインしているユーザー）のIDを取得できます。

リクエストパラメータ

Action

- ・ データ型: **String**
- ・ 必須項目: はい
- ・ 説明: 必須のシステムパラメータ。パラメータ値は「**GetCallerIdentity**」。

リターンパラメータ

AccountId

- ・ データ型: **String**
- ・ 説明: 呼び出し元のテナントアカウントID。

UserId

- ・ データ型: **String**
- ・ 説明: 呼び出し元のユーザーID。呼び出し元はAlibabaクラウドアカウントの場合、その戻り値はAccountIdと同じです。

Arn

- ・ データ型: **String**
- ・ 説明: 呼び出し元のAliyunリソースデスク립タ(ARN)。

操作の例

HTTP リクエスト

```
https://sts.aliyuncs.com?Action=GetCallerIdentity
&<Public request parameters>
```

HTTP 応答

- ・ XML形式

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

- ・ JSON形式

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

3.3 AssumeRoleWithSAML

この操作では、ロールベースのシングルサインオン (SSO) の使用中にロールを引き受けるための一時 ID を取得します。

リクエストパラメーター

パラメーター	タイプ	必須項目	例	説明
Action	String	必須	AssumeRoleWithSAML	実行する操作。このパラメーターを AssumeRoleWithSAML に設定します。

パラメーター	タイプ	必須項目	例	説明
SAMLProviderArn	String	必須	acs:ram::123456789012****:saml-provider/company1	RAM コンソールで作成された ID プロバイダー (IdP) の Alibaba Cloud リソース名 (ARN)。形式: acs:ram::\$account_ID:saml-provider/\$saml_provider_ID
RoleArn	String	必須	acs:ram::123456789012****:role/adminrole	引き受けるロールの ARN。形式: acs:ram::\$accountID:role/\$roleName
SAMLEnvironment	String	必須	<base64_encoded_saml_assertion>	Base64 エンコードを使用してエンコードされた SAML アサーション。値は 4 ~ 100,000 バイトである必要があります。
Policy	String	任意	<url_encoded_policy>	生成された STS トークンの権限を指定するポリシー。値の長さは最大 1,024 バイトです。このパラメーターを指定しない場合、STS トークンには指定された RAM ロールのすべてのアクセス権限が付与されます。
DurationSeconds	Long	任意	3600	STS トークンの有効期間。単位: 秒 有効値: 900 ~ 3600。既定値: 3600。

応答パラメーター

パラメーター	タイプ	例	説明
RequestId	String	6894B13B-6D71-4EF5-88FA-F32781734A7F	リクエストの ID。
Credentials			アクセス資格情報。
AccessKeyId	String	STS.L4aBSCSJVMuKg5U1****	AccessKey ID。
AccessKeySecret	String	wyLTSmsyPGP1ohvvw8xYgB29dlGI8KMih2pK****	AccessKey Secret。

パラメーター	タイプ	例	説明
<code>SecurityToken</code>	String	*****	STS トークン。
<code>Expiration</code>	String	2015-04-09T11:52:19Z	トークンの有効期限。
<code>AssumedRoleUser</code>			ロールを引き受けるために使用する一時 ID。
<code>Arn</code>	String	acs:sts::123456789012****:assumed-role/AdminRole/alice	ロールを引き受けるために使用する一時 ID の ARN。形式: <code>acs:ram::\$accountID:assumed-role/\$roleName/\$roleSessionName</code> 。
<code>AssumedRoleUserId</code>	String	34458433936495****:alice	ロールを引き受ける一時 ID の ID。
<code>SAMLAssertionInfo</code>			SAML アサーションの情報。
<code>SubjectType</code>	String	persistent	SAML アサーションの NameID の値の形式。名前 ID に <code>urn:oasis:names:tc:SAML:2.0:nameid-format</code> : プレフィックスが含まれている場合、そのプレフィックスは ID から削除されます。たとえば、ID が <code>urn:oasis:names:tc:SAML:2.0:nameid-format:persistent/transient</code> の場合、 <code>persistent/transient</code> のみが表示されます。
<code>Subject</code>	String	alice@example.com	SAML アサーションの Subject-NameID フィールドの値。
<code>Recipient</code>	String	https://signin.aliyun.com/saml-role/SSO	SAML アサーションの Subject-SubjectConfirmation-SubjectConfirmationData フィールドの Recipient 属性。
<code>Issuer</code>	String	http://example.com/adfs/services/trust	SAML アサーションの Issuer フィールドの値。

例



注:

SAMLAssertion パラメーターに大量の本文テキストがあり、**GET** メソッドを使用して **API** リクエストを送信すると、エラーが発生する場合があります。したがって、**POST** メソッドを使用して **API** リクエストを送信することを推奨します。

レスポンスの例

XML 形式

```
<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 形式

```
{
  "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"
}
```

}

Error codes

HTTP ステータス コード	エラーコード	エラーメッセージ	説明
400	MissingParameter. SAMLAssertion	Parameter SAMLAssertion is required.	SAMLAssertion パラ メーターが指定されて いない場合に返される エラーメッセージ。
400	MissingParameter. SAMLProviderArn	Parameter SAMLProviderArn is required.	SAMLProviderArn パラメーターが指定 されていない場合に返 されるエラーメッセー ジ。
400	MissingParameter. RoleArn	Parameter RoleArn is required.	RoleArn パラメー ターが指定されてい ない場合に返されるエ ラーメッセージ。
400	InvalidParameter. PolicyGrammar	Invalid Policy.	指定された権限ポリ シーが無効な場合に返 されるエラーメッセー ジ。
400	InvalidParameter. PolicySize	The max size of policy string is 1024.	指定されたポリシー文 字列の長さが上限に達 した場合に返されるエ ラーメッセージ。ポリ シー文字列の長さは最 大 1,024 バイトです。
400	InvalidParameter. RoleSessionName	The RoleSessio nName is invalid.	指定されたロールセッ ション名が無効な場合 に返されるエラーメッ セージ。
400	InvalidParameter. DurationSeconds	The DurationSe conds is invalid.	指定された DurationSeconds パラメーターの値が無 効な場合に表示される エラーメッセージ。

HTTP ステータス コード	エラーコード	エラーメッセージ	説明
404	EntityNotExist. SAMLProvider	Can not find SAML provider.	指定された SAML IdP が存在しない場合に 表示されるエラー メッセージ。
404	EntityNotExist. RoleArn	The specified Role does not exists.	指定された RAM ロール が存在しない場合に 表示されるエラー メッセージ。
401	AuthenticationFail .IDPMetadata. Invalid	The IdP Metadata of your SAML Provider is invalid.	SAML IdP のメタ データが無効な場合 に返されるエラーメッ セージ。
401	AuthenticationFail .SAMLAssertion. Expired	The SAML Assertion is expired.	SAML アサーション の有効期限が切れて いる場合に返されるエ ラーメッセージ。
401	AuthenticationFail .SAMLAssertion. Invalid	The SAML Assertion is invalid .	SAML アサーション が無効な場合に表示 されるエラーメッセー ジ。

4 (旧バージョン) API リファレンス (STS)

4.1 付録

4.1.1 エラーコード

HTTPステータスコード400

InvalidParameter.InvalidParameter.RoleArn

- ・ HTTPステータスコード：400
- ・ エラーメッセージ：パラメータ**RoleArn**が無効です。

InvalidParameter.RoleSessionName

- ・ HTTPステータスコード：400
- ・ エラーメッセージ：パラメータ**RoleSessionName**が無効です。

InvalidParameter.DurationSeconds

- ・ HTTPステータスコード：400
- ・ エラーメッセージ：**DurationSeconds**の最小/最大値は15分/1時間です。

InvalidParameter.PolicyGrammar

- ・ HTTPステータスコード：400
- ・ エラーメッセージ：パラメータポリシーの構文が間違っています。

InvalidParameter.PolicySize

- ・ HTTPステータスコード：400
- ・ エラーメッセージ：ポリシーの長さは最大**1024bytes**です。

HTTPステータスコード：403

NoPermission

- ・ HTTPステータスコード：403
- ・ エラーメッセージ：操作を実行する権限がありません。 **RAM**から権限を取得 必要があります。

HTTPステータスコード：500

InternalError

- ・ HTTPステータスコード：500
- ・ エラーメッセージ：STS Server内部エラーが発生しました。

4.2 データ型

4.2.1 Credentials

説明

アクセス資格。

ノード名

Credentials

サブノード

AccessKeyId

- ・ データ型：String
- ・ 説明：アクセスキーID

AccessKeySecret

- ・ データ型：String
- ・ 説明：アクセスキー

SecurityToken

- ・ データ型：String
- ・ 説明：セキュリティトークン。

Expiration

- ・ データ型：String
- ・ 説明：有効期限

4.2.2 AssumedRoleUser

説明

「AssumeRole」インターフェイスを通して一時的ロールIDを取得します。

ノード名

AssumedRoleUser

サブノード

Arn

- ・ データ型：**String**
- ・ 説明：一時的ロールIDのリソースデスクリプタ。

AssumedRoleUserId

- ・ データ型：**String**
- ・ 説明：一時的ロールIDのユーザーID。