Alibaba Cloud
Resource Access Management

API Reference (STS)

Issue: 20190228

Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

1. **You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.**
2. **No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company, or individual in any form or by any means without the prior written consent of Alibaba Cloud.**
3. **The content of this document may be changed due to product version upgrades , adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through Alibaba Cloud-authorized channels. You shall pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.**
4. **This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults " and "as available" basis. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity , applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not bear any liability for any errors or financial losses incurred by any organizations, companies, or individuals arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequential, exemplary, incidental, special, or punitive damages, including lost profits arising from the use**

or trust in this document, even if Alibaba Cloud has been notified of the possibility of such a loss.

5. By law, all the content of the Alibaba Cloud website, including but not limited to works, products, images, archives, information, materials, website architecture, website graphic layout, and webpage design, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of the Alibaba Cloud website, product programs, or content shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates).
6. Please contact Alibaba Cloud directly if you discover any errors in this document.

Generic conventions

Table -1: Style conventions

Style	Description	Example
	This warning information indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	 Danger: Resetting will result in the loss of user configuration data.
	This warning information indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	 Warning: Restarting will cause business interruption. About 10 minutes are required to restore business.
	This indicates warning information, supplementary instructions, and other content that the user must understand.	 Notice: Take the necessary precautions to save exported data containing sensitive information.
	This indicates supplemental instructions, best practices, tips, and other content that is good to know for the user.	 Note: You can use Ctrl + A to select all files.
>	Multi-level menu cascade.	Settings > Network > Set network type
Bold	It is used for buttons, menus , page names, and other UI elements.	Click OK.
`Courier font`	It is used for commands.	Run the `cd / d C :/ windows` command to enter the Windows system folder.
Italics	It is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	It indicates that it is a optional value, and only one item can be selected.	`ipconfig` *[-all|-t]*

Style	Description	Example
{} or {a|b}	It indicates that it is a required value, and only one item can be selected.	`swich {stand | slave}`

Contents

1 Calling method

1.1 Request Structure

Endpoint

For the STS service address, see *Service address*.

Communication protocol

To ensure communication security, the STS service uses only the HTTPS secure channel to send requests.

HTTP request methods

The system allows you to send HTTP GET/POST requests. In this method, the request parameters must be included in the request URL. (The size of a GET request cannot exceed 4 KB, and the size of a POST requests cannot exceed 10 MB.)

Request parameters

You must use an “Action” parameter (such as “AddUser”) in each request to specify the operation to perform, and meanwhile you must add public request parameters and interface-specified request parameters that each operation interface requires.

Character encoding

Requests and responses are encoded using UTF-8.

2 Operation interfaces

2.1 AssumeRole

Interface description

You can use this interface to obtain a temporary identity to assume a role.

Request prameters

Action

- Type: String
- Required: Yes
- Description: A required system parameter. The parameter value is “AssumeRole”.

RoleArn

- Type: String
- Required: Yes
- Description: Role resource descriptor. Each role has a unique Aliyun Resource Name (ARN). The format is: acs:ram::$accountID:role/$roleName Example: acs:ram::1234567890123456:role/samplerole . You can view the ARN of a role in RAM role management.

RoleSessionName

- Type: String
- Required: Yes
- Description: You can use this parameter to identify different tokens in order to indicate who is using a specific token, which facilitates audit.
- Format:

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

Notice:
An input of 2-32 characters is supported. Please enter at least 2 characters. If only 1 character is entered, an error occurs.

Policy

- Name: Policy
- Type: String
- Required: No
- Description: Authorization policy *Policy syntax structure*. The policy length is restricted to 1024 bytes. You can use this parameter to restrict permissions of the generated tokens. If this parameter is not set, the returned token will have all permissions of a specific role.

DurationSeconds

- Name: DurationSeconds
- Type: Integer
- Required: No
- Description: Specified expiration duration, in seconds. The expiration duration ranges from 900 seconds to 3600 seconds, and the default value is “3600”.

Return parameters

Credentials

- Type:*Credentials*
- Description: Access credential.

AssumedRoleUser

- Description: Temporary role assume identity.

Operation example

HTTP Request

```
 https :// sts . aliyuncs . com ? Action = AssumeRole
& RoleArn = acs : ram :: 1234567890  123456 : role / adminrole
& RoleSessio  nName = alice
& DurationSe  conds = 3600
& Policy =< url_encode  d_policy >
&< Public   request   parameters >
```

HTTP Response

- XML format

```
< AssumeRole  Response >
    < RequestId > 6894B13B - 6D71 - 4EF5 - 88FA - F32781734A  7F </
 RequestId >
    < AssumedRol  eUser >
```

```
        < arn > acs : sts :: 1234567890  123456 : assumed - role /
 AdminRole / alice </ arn >
        < AssumedRol  eUserId > 3445843393  64951186 : alice <
 AssumedRol  eUserId >
    </ AssumedRol  eUser >
    < Credential  s >
        < AccessKeyI  d > STS . L4aBSCSJVM  uKg5U1vFDw </
 AccessKeyI  d >
        < AccessKeyS  ecret > wyLTSmsyPG  P1ohvvw8xY  gB29dlGI8K
 MiH2pKCNZ9 </ AccessKeyS  ecret >
        < SecurityTo  ken > CAESrAIIAR  KAAShQquMn  LIlbvEcIxO
 6wCoqJufs8  sWwieUxu45  hS9AvKNEte  8KRUWiJWJ6  Y + YHAPgNwi7y
 fRecMFydL2  uPOgBI7LDi  o0RkbYLmJf  IxHM2nGBPd  ml7kYEOXmJ
 p2aDhbvvwV  YIyt / 8iES / R6N208wQh0  Pk2bu +/ 9dvalp6wOH
 F4gkFGhhTV  FMuTDRhQlN  DU0pWTXVLZ  zVVMXZGRHc  iBTQzMjc0K
 gVhbGljZTC  pnJjwySk6B  lJzYU1ENUJ  uCgExGmkKB  UFsbG93Eh8
 KDEFjdGlvb  kVxdWFscxI  GQWN0aW9uG  gcKBW9zczo  qEj8KDlJlc
 291cmNlRXF  1YWxzEghSZ  XNvdXJjZRo  jCiFhY3M6b  3NzOio6NDM
 yNzQ6c2Ftc  GxlYm94L2F  saWNlLyo =</ SecurityTo  ken >
        < Expiration > 2015 - 04 - 09T11 : 52 : 19Z </ Expiration >
    </ Credential  s >
</ AssumeRole  Response >
```

- **JSON format**

```
{
    " Credential  s ": {
        " AccessKeyI  d ": " STS . L4aBSCSJVM  uKg5U1vFDw ",
        " AccessKeyS  ecret ": " wyLTSmsyPG  P1ohvvw8xY  gB29dlGI8K
 MiH2pKCNZ9 ",
        " Expiration ": " 2015 - 04 - 09T11 : 52 : 19Z ",
        " SecurityTo  ken ": " CAESrAIIAR  KAAShQquMn  LIlbvEcIxO
 6wCoqJufs8  sWwieUxu45  hS9AvKNEte  8KRUWiJWJ6  Y + YHAPgNwi7y
 fRecMFydL2  uPOgBI7LDi  o0RkbYLmJf  IxHM2nGBPd  ml7kYEOXmJ
 p2aDhbvvwV  YIyt / 8iES / R6N208wQh0  Pk2bu +/ 9dvalp6wOH
 F4gkFGhhTV  FMuTDRhQlN  DU0pWTXVLZ  zVVMXZGRHc  iBTQzMjc0K
 gVhbGljZTC  pnJjwySk6B  lJzYU1ENUJ  uCgExGmkKB  UFsbG93Eh8
 KDEFjdGlvb  kVxdWFscxI  GQWN0aW9uG  gcKBW9zczo  qEj8KDlJlc
 291cmNlRXF  1YWxzEghSZ  XNvdXJjZRo  jCiFhY3M6b  3NzOio6NDM
 yNzQ6c2Ftc  GxlYm94L2F  saWNlLyo ="
    },
    " AssumedRol  eUser ": {
        " arn ": " acs : sts :: 1234567890  123456 : assumed - role
 / AdminRole / alice ",
        " AssumedRol  eUserId ":" 3445843393  64951186 : alice "
        },
    " RequestId ": " 6894B13B - 6D71 - 4EF5 - 88FA - F32781734A  7F
 "
}
```

3 Appendix

3.1 Error messages

This topic describes information about RAM STS errors. For more information, see *API Error Center*.

HTTP Status 400

InvalidParameterInvalidParameter.RoleArn

- HTTP Status: 400
- ErrorMessage: The parameter RoleArn is wrongly formed.
- Solution: Use the correct role Arn.

InvalidParameter.RoleSessionName

- HTTP Status: 400
- ErrorMessage: The parameter RoleSessionName is wrongly formed.
- Solution: Modify the value of RoleSessionName. The value must be 2 to 32 characters in length and can contain letters, numbers, and special characters.

InvalidParameter.DurationSeconds

- HTTP Status: 400
- ErrorMessage: The Min/Max value of DurationSeconds is 15min/1hr.
- Solution: Modify the value of DurationSeconds. The value must be in the range of 900 and 3600.

InvalidParameter.PolicyGrammar

- HTTP Status: 400
- ErrorMessage: The parameter Policy has not passed grammar check.
- Solution: Modify the policy content.

InvalidParameter.PolicySize

- HTTP Status: 400
- ErrorMessage: The size of Policy must be smaller than 1024 bytes.
- Solution: Modify the size of Policy. The size cannot exceed 1,024 bytes.

HTTP Status 403

NoPermission

- **HTTP Status: 403**
- **ErrorMessage: You are not authorized to do this action. You should be authorized by RAM.**
- **Solution: Grant relevant permissions to the STS token.**

HTTP Status 500

InternalError

- **HTTP Status: 500**
- **ErrorMessage: STS Server Internal Error happened.**
- **Solution: Open a ticket.**