Alibaba Cloud AnalyticDB for MySQL

API Reference

Issue: 20200707

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 contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, 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 this document 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.

Document conventions

Style	Description	Example
	A danger notice 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.
	A warning notice 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 restart an instance.
	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	 **Notice:** If the weight is set to 0, the server no longer receives new requests.
	A note indicates supplemental instructions, best practices, tips, and other content.	 **Note:** You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click **Settings** > **Network** > **Set network type**.
Bold	Bold formatting is used for buttons, menus, page names, and other UI elements.	Click **OK**.
`Courier font`	Courier font is used for commands.	Run the `cd /d C:/window` command to enter the Windows system folder.
Italic	Italic formatting is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	This format is used for an optional value, where only one item can be selected.	`ipconfig [-all|-t]`

Style	Description	Example
{} or {a|b}	This format is used for a required value, where only one item can be selected.	switch {active|stand}

Contents

Legal disclaimer..... I
Document conventions.....I
1 List of operations by function..... 1
2 Request syntax..... 4
3 Signature method..... 6
4 Common parameters.....9
5 RAM authorization..... 11

1 List of operations by function

The following tables list API operations available for use in AnalyticDB for MySQL.

Cluster management

API	Description
DescribeDBClusters	Queries AnalyticDB for MySQL clusters under an Alibaba Cloud account or a Resource Access Management (RAM) user.
DescribeDBClusterAttribute	Queries details about an AnalyticDB for MySQL cluster.
ModifyDBClusterMaintainTime	Modifies the maintenance window of an AnalyticDB for MySQL cluster.
DescribeAutoRenewAttribute	Queries the auto-renewal attribute of AnalyticDB for MySQL clusters billed in the subscription mode.
ModifyAutoRenewAttribute	Modifies the auto-renewal attribute for an AnalyticDB for MySQL cluster billed in the subscription mode.
ModifyDBClusterDescription	Modifies the description of an AnalyticDB for MySQL cluster to facilitate cluster maintenance and management.

Log management

API	Description
DescribeSlowLogTrend	Queries the trend of slow query logs of an AnalyticDB for MySQL cluster.
DescribeSlowLogRecords	Queries slow query logs of an AnalyticDB for MySQL cluster.

Region management

API	Description
DescribeRegions	Queries the regions and zones where AnalyticDB for MySQL is available.

Network management

API	Description
DescribeDBClusterNetInfo	Queries network information about an AnalyticDB for MySQL cluster.
AllocateClusterPublicConnection	Applies for a public endpoint for an AnalyticDB for MySQL cluster.
ReleaseClusterPublicConnection	Releases the public endpoint of an AnalyticDB for MySQL cluster.

Account management

API	Description
CreateAccount	Creates a privileged database account for an AnalyticDB for MySQL cluster.
DescribeAccounts	Queries database account information about an AnalyticDB for MySQL cluster.
DeleteAccount	Deletes a privileged database account for an AnalyticDB for MySQL cluster.
ResetAccountPassword	Resets the password of a privileged database account for an AnalyticDB for MySQL cluster.
DescribeOperatorPermission	Queries details about the permissions granted to the service account of an AnalyticDB for MySQL cluster.
RevokeOperatorPermission	Revokes the permissions from the service account of an AnalyticDB for MySQL cluster.
GrantOperatorPermission	Grants permissions to the service account of an AnalyticDB for MySQL cluster.

Backup and restore

API	Description
DescribeBackups	Queries the backup sets of an AnalyticDB for MySQL cluster.
DescribeBackupPolicy	Queries the backup settings of an AnalyticDB for MySQL cluster.

Security management

API	Description
DescribeDBClusterAccessWhiteList	Queries the IP address whitelists of an AnalyticDB for MySQL cluster.
ModifyDBClusterAccessWhiteList	Modifies an IP address whitelist of an AnalyticDB for MySQL cluster.

Monitoring management

API	Description
DescribeDBClusterPerformance	Queries the performance data of an AnalyticDB for MySQL cluster.

2 Request syntax

This topic describes the syntax of requests to call AnalyticDB for MySQL API operations.

Endpoints

The following table lists the endpoints of AnalyticDB for MySQL in different regions.

Region	Endpoint
China (Qingdao), China (Beijing), China (Hangzhou), China (Shanghai), China (Shenzhen), China (Hong Kong), Singapore, US (Virginia), and US (Silicon Valley).	ads.aliyuncs.com
China (Zhangjiakou-Beijing Winter Olympics)	ads.cn-zhangjiakou.aliyuncs.com
Japan (Tokyo)	ads.ap-northeast-1.aliyuncs.com
Malaysia (Kuala Lumpur)	ads.ap-southeast-3.aliyuncs.com
Australia (Sydney)	ads.ap-southeast-2.aliyuncs.com
UAE (Dubai)	ads.me-east-1.aliyuncs.comm
China (Hohhot)	ads.cn-huhehaote.aliyuncs.com
India (Mumbai)	ads.ap-south-1.aliyuncs.com
Indonesia (Jakarta)	ads.ap-southeast-5.aliyuncs.com
Germany (Frankfurt)	ads.eu-central-1.aliyuncs.com
UK (London)	ads.eu-west-1.aliyuncs.com
China (Chengdu)	ads.cn-chengdu.aliyuncs.com

Communication protocols

You can call AnalyticDB for MySQL API operations by sending HTTP or HTTPS requests. We recommend that you use HTTPS for enhanced security.

Request methods

You can use the HTTP GET method to send requests. If you use this method, the request parameters must be included in the URL of the request.

Request parameters

In each request, you must specify the operation such as CreateDatabase that you want to perform by using the Action parameter. You must also specify the common request parameters and operation-specific parameters.

Encoding

All requests and responses are encoded in UTF-8.

3 Signature method

The AnalyticDB for MySQL service authenticates the sender identity of each access request. Therefore, each request must contain signature information, regardless of whether it is sent through HTTP or HTTPS.

AnalyticDB for MySQL implements symmetric encryption with an AccessKey pair to verify the identity of the request sender. An AccessKey pair consists of an AccessKey ID and an AccessKey secret. The AccessKey ID and AccessKey secret are issued to you by Alibaba Cloud. You can apply for and manage them on the Alibaba Cloud website. The AccessKey ID is used to verify your identity, whereas the AccessKey secret is used to encrypt and verify the signature string on the server. The AccessKey secret must be kept confidential and only be known to Alibaba Cloud and you.

To sign a request, follow these steps:

1. Create a canonicalized query string based on the request parameters.
   a. Arrange the request parameters (including all common and operation-specific parameters except Signature) in alphabetical order.

      Note:
      If you use the GET method to send a request, the request parameters are included as a part of the request URL. The request parameters in the URL are placed after a question mark (?) and separated with ampersands (&).

   b. Encode the name and value of each request parameter in UTF-8. The encoding rules are as follows:

      - Uppercase letters, lowercase letters, digits, hyphens (-), underscores (_), periods (.), and tildes (~) do not need to be encoded.
      - Other characters must be percent encoded in %XY format. XY represents the ASCII code of the characters in hexadecimal notation. For example, the double quotation mark (") is encoded as %22.
      - Extended UTF-8 characters are encoded in %XY%ZA... format.
      - Spaces must be encoded as %20. Do not encode spaces as plus signs (+).

        Note:

Most libraries that support URL encoding, such as java.net.URLEncoder, comply with the Multipurpose Internet Mail Extensions (MIME) encoding rules of "application/x-www-form-urlencoded". If this encoding method is used, replace the plus signs (+) in the encoded strings with %20, the asterisks (*) with %2A, and %7E with tildes (~) to conform to the encoding rules.

c. Use an equal sign (=) to connect the name and value of each URL-encoded request parameter as a key-value pair.

d. Sort the key-value pairs connected by equal signs (=) in alphabetical order and separate them with ampersands (&).

2. Create a string-to-sign from the encoded canonicalized query string based on the following rules:

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

Parameter description

- HTTPMethod: the HTTP method used to submit a request, such as GET.
- percentEncode("/"): the encoded value for the forward slash (/) based on the URL encoding rules described in the previous step, which is %2F.
- percentEncode(CanonicalizedQueryString): the encoded string of the canonicalized query string constructed in the previous step, produced by following the URL encoding rules described in the previous step.

3. Calculate the HMAC value of the string-to-sign as defined in RFC 2104.

Note:

Use the SHA1 algorithm to calculate the HMAC value of the string-to-sign. The AccessKey secret appended by an ampersand (&) (ASCII:38) is used as the key for HMAC calculation.

4. Encode the HMAC value in Base64 to obtain the signature string.

5. Add the signature string to the request as the value of the Signature parameter.

Note:

The signature string must be encoded like other parameters in the URL based on RFC 3986 rules before it can be submitted to the DNS Domain Name System (DNS) server as the final request parameter value.

For example, the request URL of the DescribeDBClusters operation before signature is as follows:

```
http://adb.aliyuncs.com/?Timestamp=2013-06-01T10:33:56Z&Format=XML&
AccessKeyId=testid&Action=DescribeDBClusters&SignatureMethod=HMAC-SHA1&
RegionId=region1&SignatureNonce=NwDAxvLU6tFE0DVb&Version=2014-08-15&
SignatureVersion=1.0
```

The string-to-sign is as follows:

```
GET&%2F&AccessKeyId%3Dtestid&Action%3DDescribeDBClusters&Format%3DXML
&RegionId%3Dregion1&SignatureMethod%3DHMAC-SHA1&SignatureNonce%
3DNwDAxvLU6tFE0DVb&SignatureVersion%3D1.0&Timestamp%3D2013-06-01T10%
253A33%253A56Z&Version%3D2014-08-15
```

Assume that the AccessKey ID is "testid", the AccessKey secret is "testsecret", and the key used for HMAC calculation is "testsecret&". The calculated signature string is `uRpHwaSEt3J+6KQD//svCh/x+pI=`.

The signed request URL with the Signature parameter added is as follows:

```
http://adb.aliyuncs.com/?Timestamp=2013-06-01T10%3A33%3A56Z&Format=XML
&AccessKeyId=testid&Action=DescribeDBClusters&SignatureMethod=HMAC-SHA1&
RegionId=region1&SignatureNonce=NwDAxvLU6tFE0DVb&SignatureVersion=1.0&
Version=2014-08-15&Signature=BIPOMlu8LXBeZtLQkJTw6iFvw1E%3D
```

4 Common parameters

Common parameters, including common request parameters and common response parameters, are required by all API operations.

Common request parameters

Common request parameters must be included in all AnalyticDB for MySQL API requests.

Parameter	Type	Required	Description
Format	String	No	The format in which to return the response. Valid values: JSON and XML. Default value: JSON
Version	String	Yes	The version number of the API, in the YYYY-MM-DD format. The current version is 2019-03-15.
AccessKeyId	String	Yes	The AccessKey ID provided to you by Alibaba Cloud.
Signature	String	Yes	The signature string of the current request. For more information about how signatures are calculated, see Signature method.
SignatureMethod	string	Yes	The encryption method of the signature string. Set the value to HMAC-SHA1.

Parameter	Type	Required	Description
Timestamp	String	Yes	The timestamp of the request. Specify the time in the ISO 8601 standard in the YYYY-MM-DDThh:mm:ssZ format. The time must be in UTC. For example, the value 2013-08-15T12:00:00Z indicates 20:00:00 on August 15, 2013, UTC+8.
SignatureVersion	String	Yes	The version of the signature encryption algorithm. Set the value to 1.0.
SignatureNonce	String	Yes	A unique, random number used to prevent replay attacks. You must use different numbers for different requests.

5 RAM authorization

Overview

All AnalyticDB for MySQL clusters created by using an Alibaba Cloud account are resources owned by that account. By default, the account has full operation permissions on the resources.

The Alibaba Cloud Resource Access Management (RAM) service allows you to grant access and management permissions on your AnalyticDB for MySQL clusters to RAM users.

Currently, you can only grant RAM users with permissions on AnalyticDB for MySQL clusters but not on finer-grained objects. The following table lists the descriptions of resources when you use RAM to grant access permissions on these resources.

Request parameters

Resource type	Resource description in an authorization policy
dbcluster	acs:adb:$regionid:$accountid:dbcluster/ acs:adb:::dbcluster/

Parameter description

Parameter	Description
$regionid	The ID of the region where the resource is available, which can be replaced by an asterisk (*).
$accountid	The ID of your Alibaba Cloud account, which can be replaced by an asterisk (*).

Note:

You can only grant permissions on all AnalyticDB for MySQL clusters under your Alibaba Cloud account in a unified manner. You cannot grant permissions on a single cluster. That is, you cannot use the following resource description in an authorization policy: acs:adb:::dbcluster/pc-xxxxxxx.

Sample success responses

```
{
  "Version": "1",
```

```
 "Statement": [
  {
   "Action": [
    "adb:Describe*"
   ],
   "Effect": "Allow",
   "Resource": [
    "acs:adb:cn-hangzhou:12345678901234:dbcluster/*"
   ]
  },
  {
   "Action": "adb:Describe*",
   "Effect": "Allow",
   "Resource": [
    "*"
   ]
  }
 ]
}
```