Basic Cloud Monitor

API Documents

Product Introduction

Tencent Cloud

Copyright Notice

Trademark Notice

Service Statement

This document is intended to provide users with general information about Tencent Cloud's products and services only and does not form part of Tencent Cloud's terms and conditions. Tencent Cloud's products or services are subject to change. Specific products and services and the standards applicable to them are exclusively provided for in Tencent Cloud's applicable terms and conditions.

Contents

API Documents Introduction

Last updated：2017-12-26 09:43:06

Welcome to Tencent Cloud Monitor service. Cloud Monitor provides comprehensive data monitoring for cloud services, intelligent data analysis, real-time failure alarm and customized data report configuration. It allows you to accurately know the health status of businesses and various cloud services in real time. Users can use APIs described in this document to perform related operations, such as reading monitoring data. For information on supported operations, please see API Overview.
Before using these APIs, please make sure that you have a thorough understanding of CM products and how to use them.

The key terms for Cloud Monitor are as follows:

1. Glossary

Term	Full Name	Full Name	Description
Namespace	Namespace	Namespace	Namespace is the container of metrics. Metrics in different namespaces are independent from each other, so the metrics from different applications will not be mistakenly aggregated into the same statistical information.
Metric	Metric	Metric	A metric is used as a monitoring variable, and a data point refers to the time-varying value of the metric. For example, the CPU utilization of a CVM is a metric, and the space usage of a cloud database is another metric.
Dimension	Dimension	Dimension	Dimension is a structure of name/value pair for identifying a monitoring object, and is used to describe the characteristics of the monitoring object.

2. API Quick Start

You can directly query the data by using Cloud Monitor via API:
You can use Read Monitoring Data (New) to query the data.

3. Service Limits

None.

API Overview

Last updated：2018-06-15 11:49:24

Cloud Monitor APIs

Function	Action ID	Description
Get the List of Monitoring Metrics	DescribeMetrics	Query corresponding monitoring metrics based on the namespace and metric name entered by the user
Read Monitoring Data	GetMetricStatistics	Obtain the monitoring data for CVMs, hard disks, and CPU utilization, etc.
Read Monitoring Data (New)	GetMonitorData	Obtain the monitoring data of cloud services. Monitoring data for CVMs and VPC Direct Connect can be obtained currently.

Call Method

Request Structure

Request Structure

Last updated：2017-04-25 11:03:01

The process of calling Tencent Cloud APIs is achieved by sending requests to the server IP addresses of these APIs and adding relevant request parameters in the requests as described in the API descriptions. A request for calling Tencent Cloud API is made up of the following elements:

1. Service Address

The service connection address of Tencent Cloud APIs depends on the modules. For more information, please see the descriptions of each API.

2. Communication Protocol

Most Tencent Cloud APIs communicate over HTTPS to provide high-security channels.

3. Request Method

Tencent Cloud APIs support both POST and GET requests.
**Note:

1. The two methods cannot be used at the same time. If GET method is used, parameters are obtained from Querystring. If POST method is used, parameters are obtained from Request Body, and the parameters in Querystring will be ignored. The rules for parameter formats are the same for both methods. Generally, GET method is used. If the parameter strings are too long, POST method is used.
2. If GET method is used, all request parameters need to be encoded with URL encoding. This is not needed if POST method is used.**

4. Request Parameters

Two types of parameters are needed for each Tencent Cloud API request - common request parameters and API request parameters. Common request parameters are the parameters common to all APIs (For more information, please see Common Request Parameters section), while API request parameters are parameters specific to each API (For more information, please see "Request Parameters" description of each API.)

5. Character Encoding

All requests for Tencent Cloud APIs and their returned results are encoded using UTF-8 character set.

Public Request Parameters

Last updated：2017-12-07 12:57:19

Common request parameters are needed for all APIs. These parameters will not be discussed in the document for each API unless necessary. However, **these parameters are required in each request for the request to be initiated successfully**. The first letter of each common request parameter is in uppercase so that the parameters can be differentiated from API request parameters.

Here's a list of common request parameters:

Name	Type	Description	Required
Action	String	The name of the API for the desired operation. For example, if you want to call API Get the List of Monitoring Metrics, the Action parameter is DescribeMetrics.	Yes
Region	String	Region parameter, used to identify the region to which the instance you want to operate belongs. The parameter values for regions are as follows: Beijing: bj, Guangzhou: gz, Shanghai: sh, Hong Kong: hk, North America: ca. **Note: Normally this parameter is required. Otherwise it will be mentioned in the corresponding API.**	No
Timestamp	UInt	The current UNIX timestamp that records the time at which the API request was initiated.	Yes
Nonce	UInt	A random positive integer that is used in conjunction with Timestamp to prevent replay attacks.	Yes
SecretId	String	The SecretId applied for from Cloud API Key, used for identification. A SecretId corresponds to a unique SecretKey, and the SecretKey is used to generate the request Signature. For more information, please see Signature Method.	Yes
Signature	String	Request signature, used to verify the validity of the request. Automatically generated by the system based on input parameters. For more information, please see Signature Method.	Yes

A complete request needs two types of request parameters: common request parameters and API request parameters. Only six common request parameters are listed above. For more information on API request parameters, please see API Request Parameters section.

API Request Parameters

Last updated：2017-12-07 12:59:34

API request parameters are specific to each API. This means that different APIs support different API request parameters. The first letter of each API request parameter is in lowercase so that the parameters can be differentiated from common request parameters.
Take API Get the List of Monitoring Metrics (DescribeMetrics) as an example. It supports the following API request parameters:

Parameter	Required	Type	Description
namespace	Yes	String	Namespace: A namespace refers to a category of resources. After specifying a namespace, you can obtain all types of monitoring metrics under the specified category of resource. Currently, this parameter can only be specified with "qce/cvm" and is used to get all types of monitoring metrics under the CVM.
metricName	No	String	Monitoring metric name, such as "cpu_usage" and "mem_usage", which should contain 1-64 characters. If it is not specified, the list of all the metrics under the namespace will be returned

Here are the descriptions of each field:

Parameter Name	Name of request parameter supported by the API. The user can use this name as an API request parameter when using this API.
Required	Indicates whether this parameter is required. "Yes" means the parameter is required for the API, while "No" means the parameter is not required.
Type	Data type of the API parameter.
Description	A brief description of the API request parameter.

If a user wants to get the list of monitoring metrics, the request link may be as follows:

```
https://monitor.api.qcloud.com/v2/index.php?
&<Common request parameters>
&namespace=qce/cvm
```

A complete request needs two types of request parameters: common request parameters and API request parameters. Only API request parameters are listed here. For more information on common request parameters, please see Common Request Parameters section.

Final Request Mode

Last updated：2017-12-07 13:00:50

The final request URL is made up of the following elements:
1) Request domain: The request domain of Get the List of Monitoring Metrics (DescribeMetrics) is monitor.api.qcloud.com. The actual request domain varies depending on the module to which the API belongs. For more information, please see descriptions of APIs.
2) Request path: The request path of Cloud API is always /v2/index.php.
3) Final request parameter string: API Request Parameter.

The final request URL is generated as follows:

```
https:// + request domain + request path + ? +final request parameter string
```

The final request URL is as follows. The first six parameters are common request parameters, and the last one is API request parameter.

```
https://monitor.api.qcloud.com/v2/index.php?
Action=DescribeMetrics
&SecretId=xxxxxxx
&Region=gz
&Timestamp=1465055529
&Nonce=59485
&Signature=mysignature
&namespace=qce/cvm
```

Return Codes

Return Success Codes

Last updated：2017-04-25 11:06:13

If the API call succeeds, the error code in the returned result will be 0, the error message field will be empty, and the returned data result will be displayed.

Example:

```
{
"code": 0,
"message": "",
<Returned result>
}
```

Return Error Codes

Last updated：2017-04-25 11:07:12

If the API call fails, the error code in the returned result will not be 0, and the message field will display detailed error information. Users can query detailed error information from the Error Codes page based on code and message.
Example of returned error:

```
{
"code": 4000,
"message": "(-514) Resource already exists"
}
```

Error Codes

Last updated：2017-04-25 11:07:55

1. Common Error Code

The error code in the returned result indicates the result of user's call to the cloud API. `code` is common error code, which applies to APIs of all modules. If the code is 0, it means the call succeeds. If not, it means the call fails. If the call fails, the user can find out the cause of the error based on the following table and take appropriate actions.

Error Code	Error Type	Description
4000	Invalid request parameter	Required parameters are missing, or parameter valuesare not in the correct format. For specific error message, please see the message field in error description.
4100	Authentication failed	Signature authentication failed. For more information, please see the Authentication section in the document.
4200	Request expired	The request has expired. For more information, please see the Request Validity Period section in the document.
4300	Access denied	Account is suspended or not within the user range of the API.
4400	Quota exceed	The number of requests exceeds the quota. For more information, please see the Request Quota section in the document.
4500	Replay attack	The Nonce and Timestamp parameters can ensure that each request will be executed only once on the server. Therefore, the Nonce value cannot be the same as last one, and the difference between Timestamp and Tencent server time cannot be greater than 2 hours.
4600	Protocol is not supported	The protocol is not supported. For more information, please see the relevant document.
5000	Resource does not exist	The instance corresponding to resource ID does not exist, or the instance has been returned, or another user's resource is accessed.
5100	Resource operation failed	The operation performed on the resource failed. For specific error message, please see the message field in error description. Try again later or contact customer service personnel for help.

5200	Failed to purchase resource	Resource purchase failed. This may be caused by unsupported instance configuration or insufficient resource.
5300	Failed to purchase resource	Resource purchase failed because of insufficient balance.
5400	Part of operations performed successfully	Part of the batch operations have been performed successfully. For more information, please see the returned value of method.
5500	User failed to pass identity verification	Resource purchase failed because the user failed to pass identity verification.
6000	Internal error on the server	An internal error occurred on the server. Try again later or contact customer service personnel for help.
6100	Not supported by the version	This API is not supported in this version or the API is under maintenance. Note: When this error occurs, first check whether the domain of the API is correct. Different modules may have different domains.
6200	API is temporarily unavailable	The API is under maintenance and is unavailable. Please try again later.

2. Module Error Code

message field indicates errors related to modules.
Example:
"message": "(-514) Resource already exists"
It consists of two parts - the string within () indicates the module error code, and the string following () is the error description.
Different modules may produce different errors. The user can identify the cause of error based on error description.

Error Code	Meaning	Description
-503	Incorrect request parameter	InvalidParameter

Error Code	Meaning	Description
-507	Limit has been exceeded	OperationDenied.ExceedLimit
-513	DB operation failed	InternalError.DBoperationFail
-514	Resource already exists	OperationDenied.SourceAlreadyExists
-509	Incorrect combination of dimensions	InvalidParameter.DimensionGroupError
-502	Resource does not exist	OperationDenied.SourceNotExists
-515	Unable to operate because a sub-resource exists	OperationDenied.SubresourceExist
-505	Parameter is missing	InvalidParameter.MissingParameter

Signature Method

Last updated：2018-07-07 12:02:54

Tencent Cloud API will authenticate each access request, so each request is required to include the signature information in the common request parameter for user authentication. The Signature is generated with the user's security credential, which consists of a SecretId and a SecretKey. Users who have no security credential can apply for a credential on the Tencent Cloud. Otherwise, the Cloud API cannot be called.

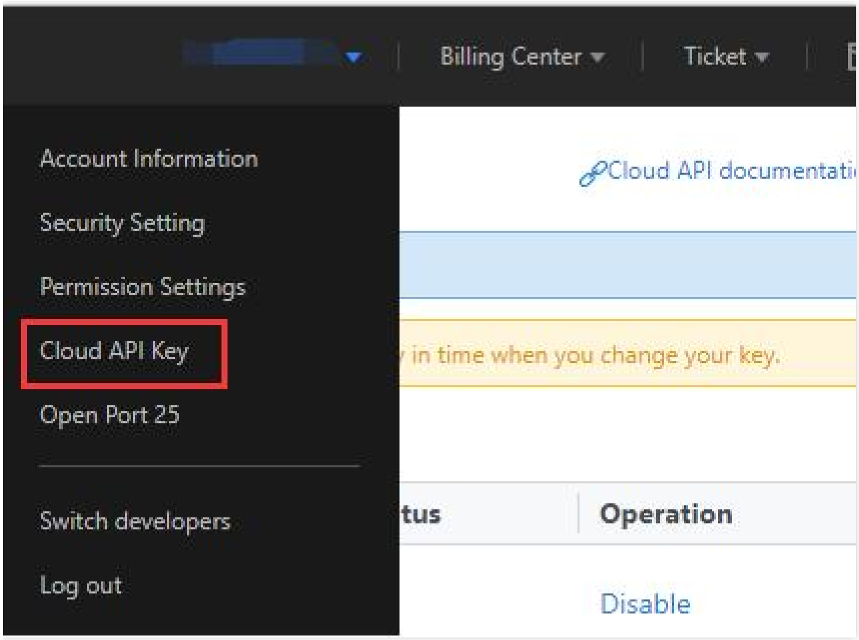
1. Applying for security credential

Before using the Cloud API for the first time, user needs to apply for a security credential on the Tencent Cloud CVM console. A security credential consists of a SecretId, which identifies the API caller, and a SecretKey, which is used to encrypt the signature string and verify the signature string on the server. Users must strictly keep their SecretKeys confidential to avoid disclosure.

To apply for a security credential, please proceed as follows:

1) Log in to the Tencent Cloud Console.

2) Select account name in the top right corner on the navigation bar, and choose "Cloud API Key" in the drop-down box to access the Cloud API key management page.



3) On the Cloud API Key Management page, click "New" to create a pair of SecretId/SecretKey. Each account can have two pairs of SecretId/SecretKey at most.

2. Generating Signature String

With the Secret ID and Secret Key, signature string can be generated. The following is the detailed process for generating signature string.

Suppose that a user has the following SecretId and SecretKey:

```
SecretId: AKIDz8krbsJ5yKBZQpn74WFkmLPx3gnPhESA
SecretKey: Gu5t9xGARNpq86cd98joQYCN3Cozk1qA
```

Note: This is just an example. Please proceed with your actual SecretId and SecretKey!
Take Query Instance List (DescribeInstances) as an example. The possible request parameters are as follows when this API is called:

Parameter name	Description	Parameter Value
Action	Method name	DescribeInstances
SecretId	Key ID	AKIDz8krbsJ5yKBZQpn74WFkmLPx3gnPhESA
Timestamp	Current time stamp	1465185768
Nonce	Random positive integer	11886
Region	Indicate the region where the instance is located	gz
instanceIds.0	ID of the instance to be queried	ins-09dx96dg
offset	Offset value	0
limit	Maximum number of output values	20

According to the above table, among the request parameters, there are only 5 common request parameters (Action, SecretId, Timestamp and Nonce), instead of 6 ones as described in "Common Request

Parameters". Actually, Region is not mandatory for CDN, and Signature (the sixth one) is generated from other parameters (including the instruction request parameters) using the following procedure:

2.1. Sorting Parameters

First, sort all request parameters in ascending lexicographical order by their names, just like sorting words in a dictionary in ascending alphabetical order or numerical order. That is to say, sort the parameters by their first letters, and then sort the parameters with the same first letter by their second letters, and so on. You can complete the sorting with the relevant sorting functions in programming language, such as the ksort function in PHP. The sorting result of the above sample parameters is as follows:

```
{
'Action' : 'DescribeInstances',
'Nonce' : 11886,
'Region' : 'gz',
'SecretId' : 'AKIDz8krbsJ5yKBZQpn74WFkmLPx3gnPhESA',
'Timestamp' : 1465185768,
'instanceIds.0' : 'ins-09dx96dg',
'limit' : 20,
'offset' : 0,
}
```

Any other programming language can be used to sort these parameters as long as the same result is produced.

2.2. Generating Request String

This step is used to generate a request string.

Format the above sorted parameters as "parameter name=parameter value". Take the parameter "Action" as an example. If the parameter value is "DescribeInstances", the resulting format will be "Action=DescribeInstances".

Note: 1. "Parameter value" is the original value instead of url encoded value. 2. If the input parameter contains an underscore"_", you need to convert it to ".".

Then, joint the formatted parameters together using "&" to generate the final request string:

```
Action=DescribeInstances&Nonce=11886&Region=gz&SecretId=AKIDz8krbsJ5yKBZQpn74WFkmLPx3gnPhESA&Timestamp=1465185768&instanceIds.0=ins-09dx96dg&limit=20&offset=0
```

2.3. Generating Original Signature String

This step is used to generate the original signature string.

The original signature string is composed of the following parameters:

1) Request method: The POST and GET methods are supported. In this case, a GET request is used. Note that the methods must be in uppercase.
2) Request CVM: The request domain in View List of Instances (DescribeInstances) is cvm.api.qcloud.com. The actual request domain varies depending on the module to which the API belongs. For more information ,refer to descriptions of APIs.
3) Request path: The request path of Cloud API is always /v2/index.php.
4) Request string: This is the request string generated in the previous step.

Combination rule of original signature string:

```
Request method + Request CVM +Request path + ? + Request string
```

The combination result is as follows:

```
GETcvm.api.qcloud.com/v2/index.php?Action=DescribeInstances&Nonce=11886&Region=gz&SecretId=AKIDz8krbsJ5yKBZQpn74WFkmLPx3gnPhESA&Timestamp=1465185768&instanceIds.0=ins-09dx96dg&limit=20&offset=0
```

2.4. Generating Signature String

This step is used to generate a signature string.
Sign the**original signature string**obtained in the previous step using HMAC-SHA1 algorithm, and then encode the signature string using Base64 to obtain the final signature string.

For example, the codes are as follows if written in PHP:

```
$secretKey = 'Gu5t9xGARNpq86cd98joQYCN3Cozk1qA';
$srcStr = 'GETcvm.api.qcloud.com/v2/index.php?Action=DescribeInstances&Nonce=11886&Region=gz&SecretId=AKIDz8krbsJ5yKBZQpn74WFkmLPx3gnPhESA&Timestamp=1465185768&instanceIds.0=ins-09dx96dg&limit=20&offset=0';
$signStr = base64_encode(hash_hmac('sha1', $srcStr, $secretKey, true));
echo $signStr;
```

The final signature string is as follows:

```
NSI3UqqD99b/UJb4tbG/xZpRW64=
```

When another programming language is used, you can perform the signature verification using the original signature string in the above example. If the resulting signature string is identical to the one in the example, it is considered to pass the verification.

3. Encoding Signature String

The generated signature string cannot be directly used as a request parameter, and needs to be encoded with URL encoding.

Note: If the GET method is used, all request parameters need to be encoded with URL encoding.

For example, the signature string generated as described above is: NSI3UqqD99b/UJb4tbG/xZpRW64=. After encoded, it should be: NSI3UqqD99b/UJb4tbG/xZpRW64=. The resulting signature string request parameter (Signature) is NSI3UqqD99b/UJb4tbG/xZpRW64=, which will be used to generate the final request URL.