ALIBABA CLOUD

Alibaba Cloud

API Gateway

Operation and maintenance

Document Version: 20220513

Alibaba Cloud

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 because of product version upgrade, adjustment, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and an updated version of this document will be released through Alibaba Cloud-authorized channels from time to time. You should 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 this document based on the "status quo", "being defective", and "existing functions" of its products and services. 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 take legal responsibility for any errors or lost profits incurred by any organization, company, or individual arising from download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, take responsibility for any indirect, consequential, punitive, contingent, 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 directly contact Alibaba Cloud for any errors of this document.

Document conventions

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

Table of Contents

1.Use API Gateway for monitoring

This topic describes how to view the information about API calls in the API Gateway console as an administrator.

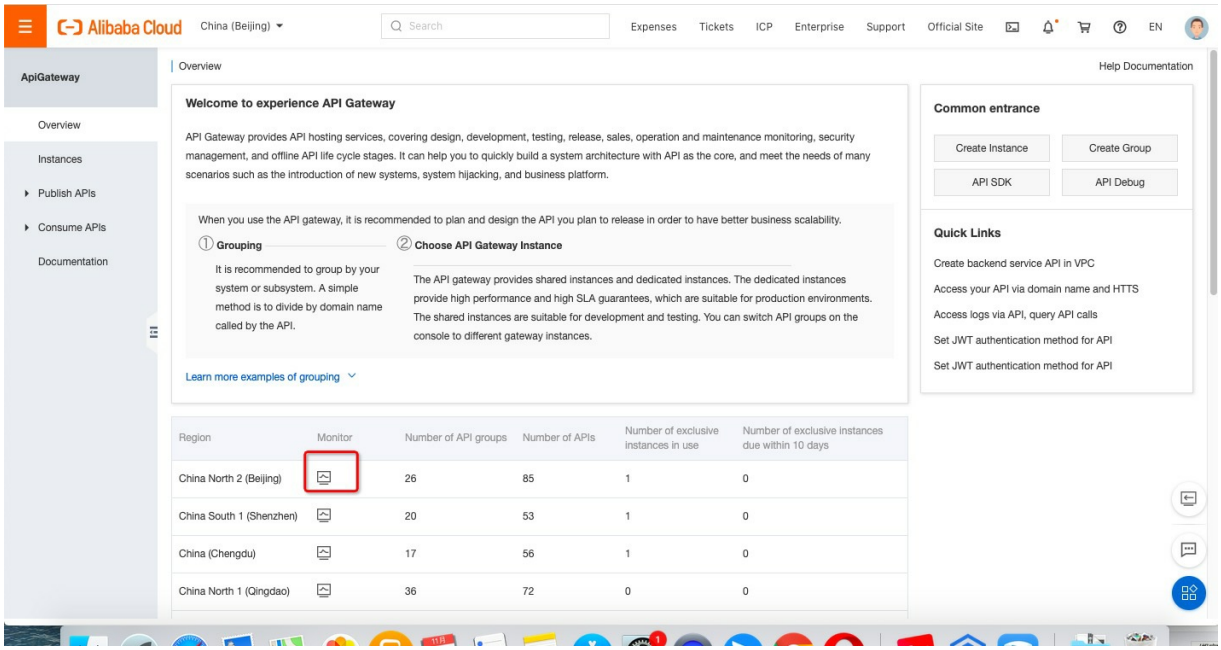
Overview

API Gateway allows you to view monitoring charts about regions, groups, and APIs. The performance metrics of monitoring charts include traffic, delay, HTTP status codes, and the number of requests.

1 Region monitoring

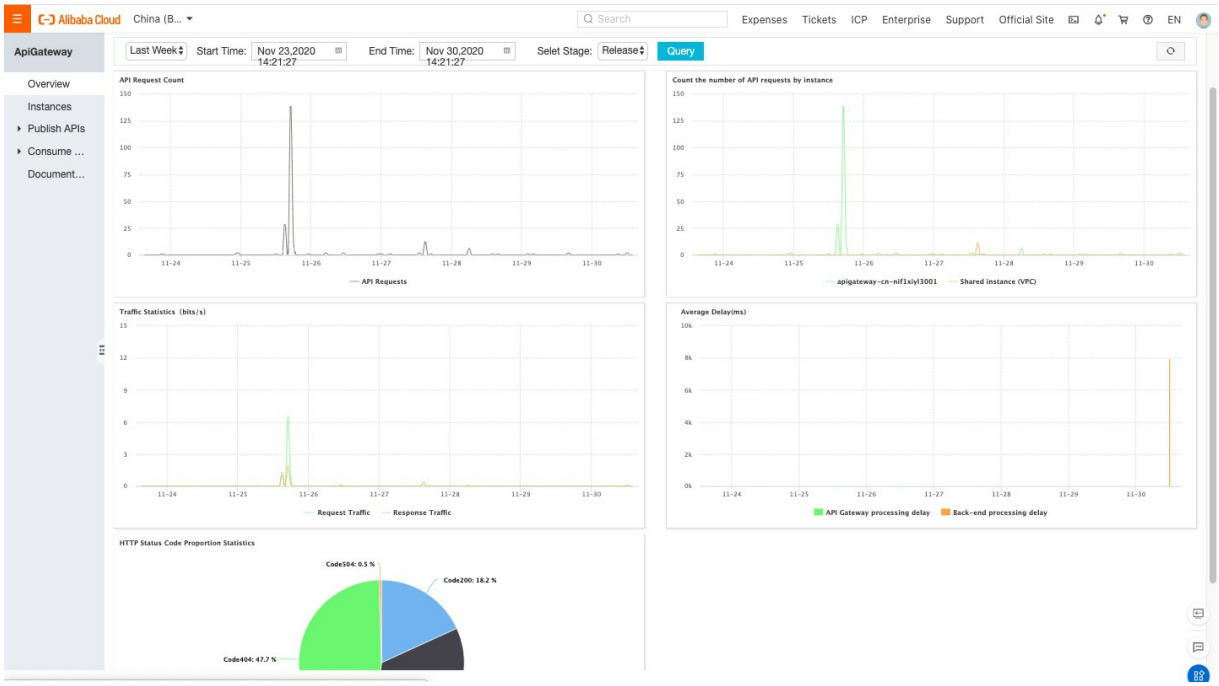
1.1 Log on to the API Gateway console.

1.2 In the left-side navigation pane, click **Overview**. To view the monitoring charts of a region, click the Monitor icon for the region. You can view the monitoring data, the number of API groups, the number of APIs, and the number of dedicated instances in use in every region. You can also view the number of dedicated instances that will expire in 10 days in every region.



1.3 The region monitoring feature provides the statistics about the API calls from only the past seven days. **The APIs that run on shared instances (classic network) are excluded from the statistics.** You can view monitoring charts based on the following environments where APIs are published: online, staging, and testing environments. The monitoring data is collected based on the following performance metrics:

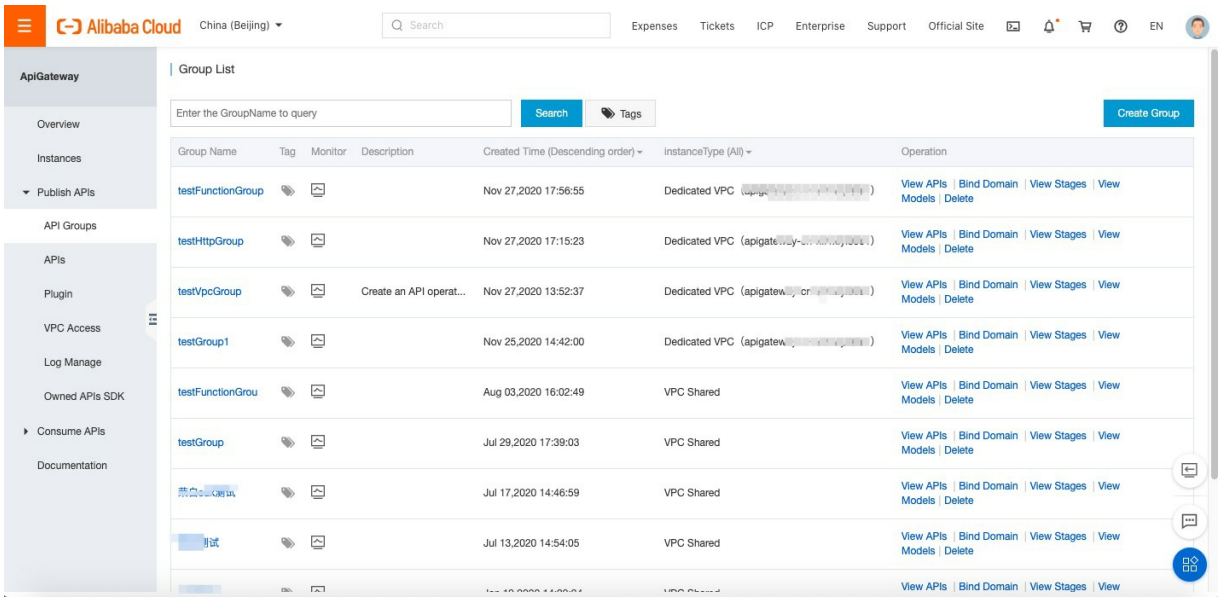
- **The number of API requests**
- **The number of API requests by instance**
- **Traffic statistics** (request traffic and response traffic)
- **Average delay** (processing delay of API Gateway and backend processing delay)
- **Proportions of HTTP status codes**



2 Group monitoring

2.1 Log on to the API Gateway console.

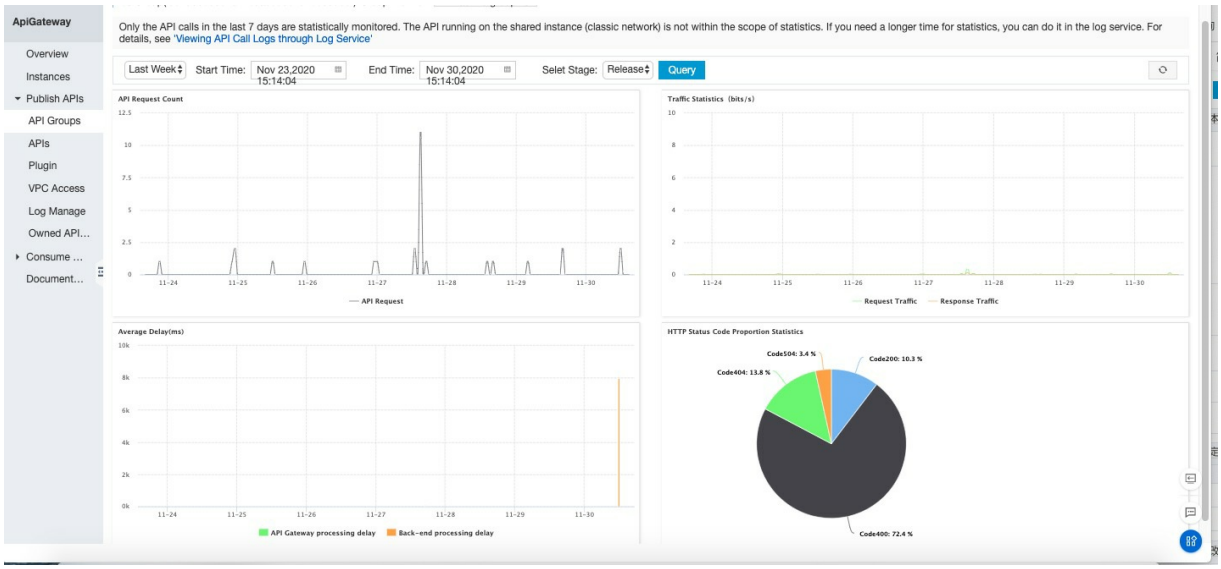
2.2 In the left-side navigation pane, choose Publish APIs > API Groups. On the Groups List page, click the Monitor icon for a group to view the monitoring charts about the group.



2.3 The group monitoring feature provides the statistics about the API calls from only the past seven days. **The APIs that run on shared instances (classic network) are excluded from the statistics**. You can view monitoring charts based on the following environments where APIs are published: online, staging, and testing environments. The monitoring data is collected based on the following performance metrics:

- **The number of API requests**
- **Traffic statistics** (request traffic and response traffic)

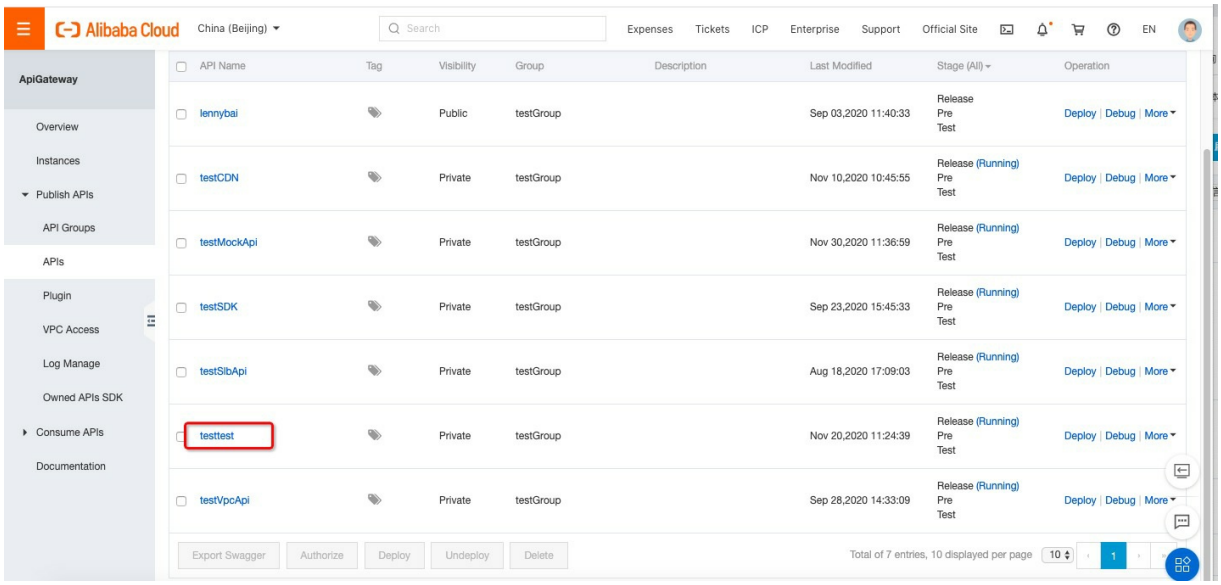
- **Average delay** (processing delay of API Gateway and backend processing delay)
- Proportions of **HTTP status codes**



3 API monitoring

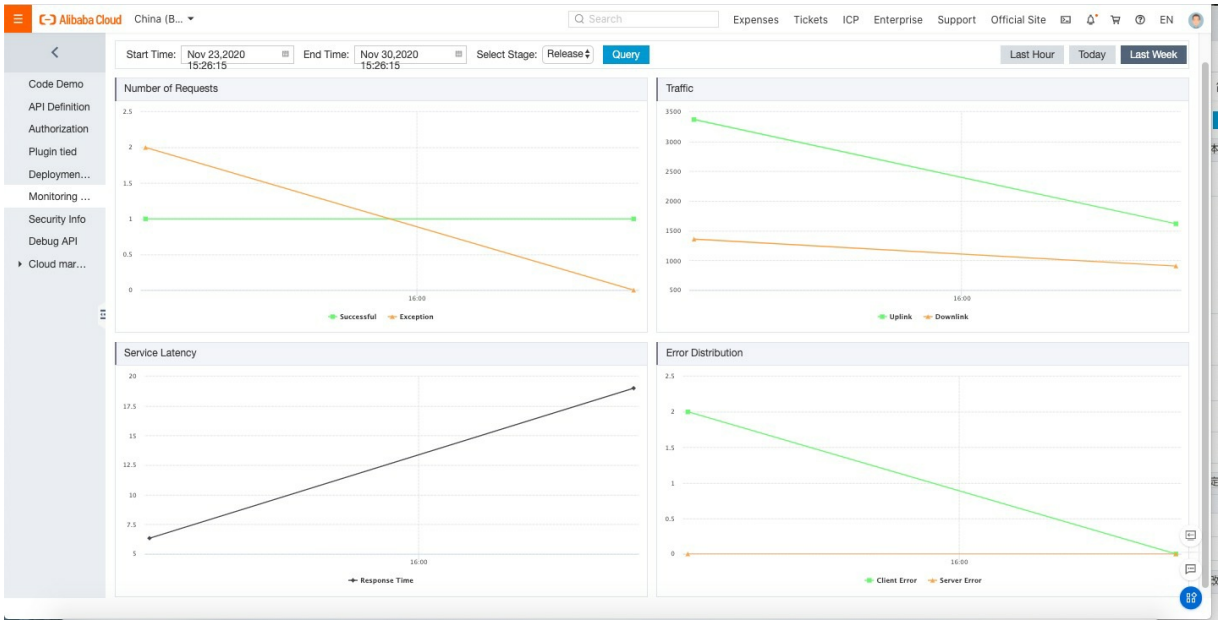
3.1 Log on to the API Gateway console.

3.2 In the left-side navigation pane, choose **Publish APIs** > **APIs**. Click the API that you want to monitor. On the page that appears, you can view the details about the API.



3.3 In the left-side navigation pane, click **Monitoring Info**. On the page that appears, you can view the monitoring data from the past week for the API that is published in the online, test, or staging environment. The monitoring data is collected based on the following performance metrics:

- The number of **requests** (successful requests and exceptions)
- **Traffic** (uplink and downlink)
- **The response time of the backend service**
- **Error distribution** (client errors and server errors)



Note

API Gateway provides monitoring statistics about the API calls from only the past seven days. If you need to obtain statistics from a longer period or have other requirements, you can use Log Service. For more information, see Use Log Service to view logs of API calls.

The monitoring feature of API Gateway is available for dedicated instances that are purchased after September 15, 2020. If your dedicated instance is purchased before September 15, 2020 and you need to use the feature, submit a ticket to update your instance to the new version.

2.Configure tracing analysis

This topic describes how to configure tracing analysis in the API Gateway console to upload tracing logs to Alibaba Cloud Tracing Analysis. Tracing Analysis provides a complete set of tools for you to map complete traces of calling services, calculate the number of requests, offer trace topologies, and analyze application dependencies. These tools help you make development and diagnosis more efficient. **This feature is available for only dedicated instances.**

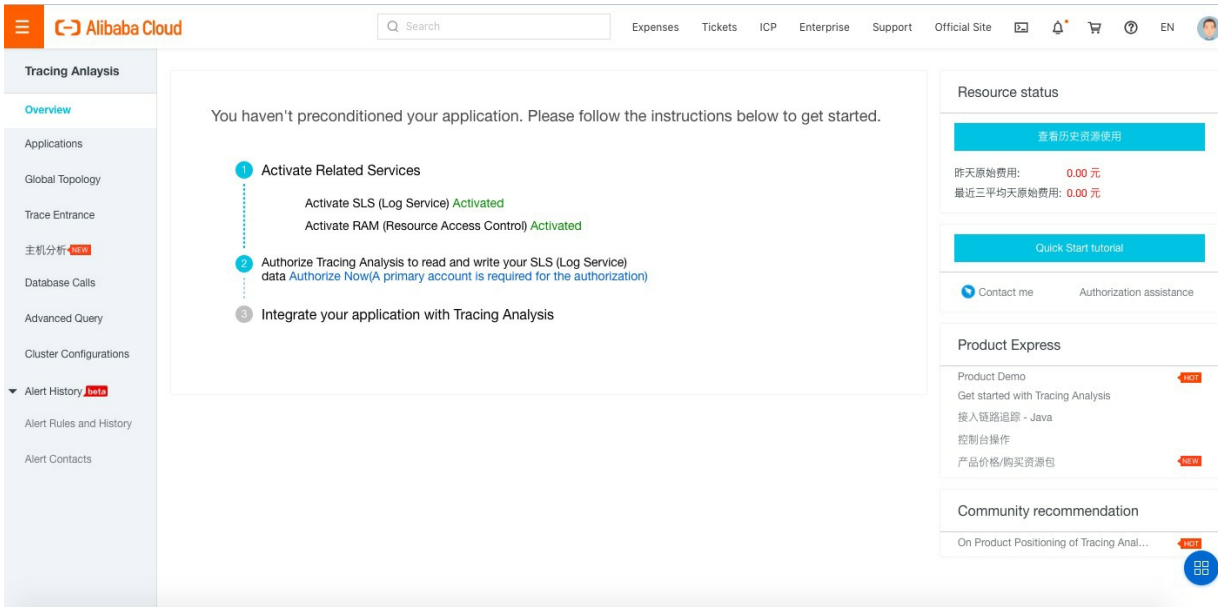
Prerequisites

- A dedicated instance of API Gateway is used.
- Tracing Analysis is activated.
- Log Service is activated.

1 Authorize Tracing Analysis

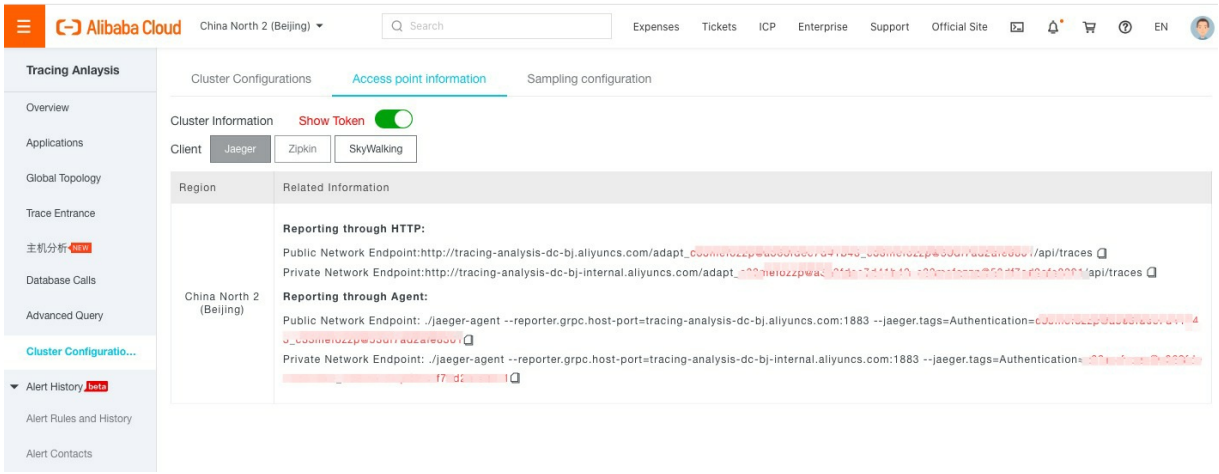
1.1 Log on to the Tracing Analysis console.

1.2 On the Overview page, click Authorize Now to authorize Tracing Analysis to read and write your Log Service data.



1.3 On the Cloud Resource Access Authorization page, select the required permissions and click Confirm Authorization Policy.

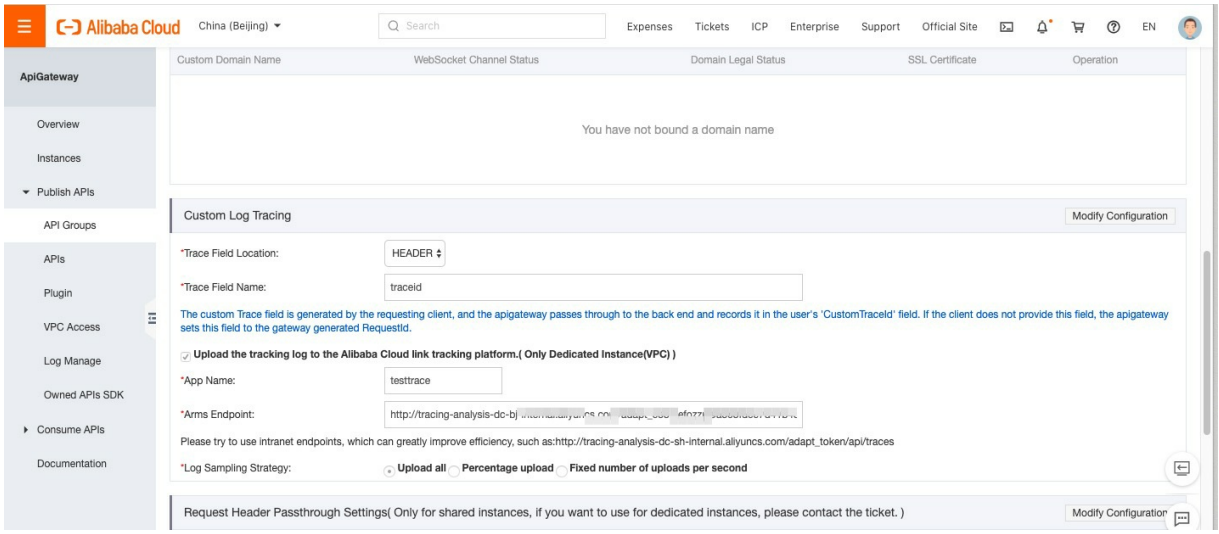
1.4 After authorization, navigate through **Overview** > **Access process** > **View access point information** > **Show Token** to view the endpoint details. Save the endpoints that are displayed in the **Reporting through HTTP** section.



2 Configure tracing analysis in the API Gateway console

2.1 Log on to the API Gateway console.

2.2 In the left-side navigation pane, choose **Publish APIs** > **API Groups**. Then, click the API group that you want to manage. The Group Details page appears. On the Group Details page, configure the settings.



- Trace Field Location: Specify the location of the traced field. Valid values are Header and Query.
- Trace Field Name: Specify the name of the traced field. The custom traced field is generated by the client that sends the request. API Gateway passes the custom traced field through to the backend and records the field data in the `CustomTraceId` field of the user. If the client does not provide the traced field, API Gateway sets the field to RequestId that is generated by the service itself.
- App Name: Specify the name of the application for tracing analysis.
- Arms Endpoint: Enter the endpoint that you obtain in section 1.4. We recommend that you use the private network endpoint for higher efficiency if the services are deployed in the same region.
- Log Sampling Strategy: Valid values are Upload all, Percentage upload, and Fixed number of uploads per second. Select an option based on your needs.

In the Tracing Analysis console, you can view the traces of the requests that are sent after tracing analysis is configured in the API Gateway console.

For more information about how to use Tracing Analysis, see View the information about API calls.

> **Note**
>
> This feature is available for dedicated instances that are purchased after December 3, 2020. If your dedicated instance is purchased before December 3, 2020 and you need to use this feature, submit a ticket to upgrade your instance to the new version.

3.Use RAM to manage user permissions for API Gateway

API Gateway allows you to use Alibaba Cloud Resource Access Management (RAM) to grant different permissions on API operations to different employees in your enterprise. As an API provider, you can create RAM users for employees and grant different permissions on API operations to different employees.

- A RAM user can manage resources in API Gateway, for example, create, view, or delete an API group, an API operation, or a plug-in. However, the RAM user does not own the resources. Permissions of the RAM user on the resources can be revoked by the relevant Alibaba Cloud account at any time.
- You can use tag-based authorization to isolate resources for an Alibaba Cloud account and its RAM users.
- Before you begin, make sure that you have read RAM documentation and API Gateway API Reference.
- **If your business does not require permission management for API operations, skip this topic.**

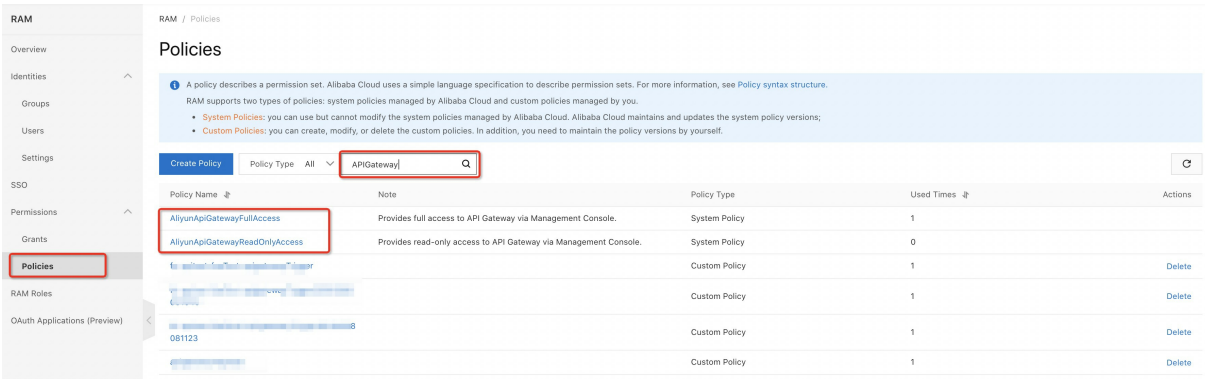
To manage user permissions for API Gateway, log on to the RAM console or call RAM API operations. For more information, see RAM introduction.

Part one: Policy management

An authorization policy describes basic elements of an authorization operation, including the permission effect, authorized resource, allowed action, and authorization condition.

1. System authorization policy

API Gateway provides two built-in system authorization policies: AliyunApiGatewayFullAccess and AliyunApiGatewayReadOnlyAccess. You can log on to the RAM console to view these two policies on the Policies page.



- AliyunApiGatewayFullAccess: authorizes a RAM user to manage all resources under the relevant Alibaba Cloud account, including API groups, API operations, throttling policies, and applications.
- AliyunApiGatewayReadOnlyAccess: allows a RAM user to view all resources under the relevant Alibaba Cloud account, including API groups, API operations, throttling policies, and applications. However, the RAM user cannot perform operations on the resources.

2. Custom authorization policy

You can customize finer-grained authorization policies, such as creating a custom authorization policy to allow a specific action or grant permissions on a specific resource. For example, you can create a custom authorization policy to grant the edit permission on the GetUsers operation. To view custom authorization policies that you have created, log on to the RAM console. In the left-side navigation pane, choose Permissions > Policies. For information about how to create, view, modify, or delete a custom authorization policy, see Manage policies.

For more information about authorization policies and how to create a custom authorization policy, see Part two of this topic, Policy elements, and Policy structure and grammar.

Part two: Authorization policy

An authorization policy is a collection of elements that are defined based on the policy structure and syntax and are used to describe the authorization operation. You can attach an authorization policy to a RAM user or a group, so that the user or the group can obtain the specified permission on the specified resource. For information about how to create a custom authorization policy, see Policy elements and Policy structure and grammar.

The following code snippet shows an example of an authorization policy:

```
{
  "Version": "1",
  "Statement": [
    {
  "Action": "apigateway:Describe*",
      "Resource": "*",
      "Effect": "Allow"
    }
  ]
}
```

This authorization policy allows a RAM user to query all resources in API Gateway.

The Action element in an authorization policy must be in the following format:

```
 "Action":"<service-name>:<action-name>"
```

Each value of the Action element must contain the following parts:

- **service-name**: the name of an Alibaba Cloud service. In this topic, enter apigateway.
- **action-name**: the name of an API operation. You can use a wildcard (*) for the name. For information about API operations that are provided by API Gateway, see the table in Part three.

  "Action": "apigateway:Describe*" indicates that the authorized RAM user can query all resources in API Gateway.

  "Action": "apigateway:*" indicates that the authorized RAM user has all permissions on all resources in API Gateway.

Part three: Resource

A resource is an object on which a RAM user is to be granted permissions. In API Gateway, API groups, throttling policies, and applications are all resources. In each authorization policy, a resource must be specified in the following format:

```
acs:<service-name>:<region>:<account-id>:<relative-id>
```

The format contains the following parts:

- **acs**: the abbreviation of Alibaba Cloud Service, which indicates the public cloud of Alibaba Cloud.
- **service-name**: the name of an Alibaba Cloud service. In this topic, enter apigateway.
- **region**: the region where the current authorization policy applies. You can specify this part as a wildcard (*), which indicates that the current authorization policy applies in all regions.
- **account-id**: the account ID of the RAM user to be authorized, for example, 1234567890123456. You can specify this part as a wildcard (*), which indicates that the current authorization policy is attached to all RAM users under the current Alibaba Cloud account.
- **relative-id**: the description of the resource on which a RAM user is to be granted permissions. You can specify this part as a string that is similar to a file path.

For example, when you create an authorization policy to grant a RAM user permissions on an API group, you can specify the API group in the following format:

```
acs:apigateway:$regionid:$accountid:apigroup/$groupId
```

If you need to authorize all RAM users under the current Alibaba Cloud account to view an API group in all regions, you can specify the API group as shown in the following code snippet:

```
acs:apigateway:*:*:apigroup/cbd157704e624ab58a204fd3e0b5ad79
```

The following table describes the action names that you can use when you create authorization policies to manage permissions on API operations of API Gateway. For more information, see Create an API group.

action-name	Description	Resource
CreateApiGroup	Creates an API group.	acs:apigateway:$regionid:$accountid:apigroup/*
ModifyApiGroup	Modifies an API group.	acs:apigateway:$regionid:$accountid:apigroup/$groupId
DeleteApiGroup	Deletes an API group.	acs:apigateway:$regionid:$accountid:apigroup/$groupId
DescribeApiGroups	Queries available API groups.	acs:apigateway:$regionid:$accountid:apigroup/*
CreateApi	Creates an API operation.	acs:apigateway:$regionid:$accountid:apigroup/$groupId

action-name	Description	Resource
DeployApi	Publishes an API operation.	acs:apigateway:$regionid:$accountid:apigroup/$groupId
AbolishApi	Unpublishes an API operation.	acs:apigateway:$regionid:$accountid:apigroup/$groupId
DeleteApi	Deletes an API operation.	acs:apigateway:$regionid:$accountid:apigroup/$groupId
DescribeApis	Queries available API operations.	acs:apigateway:$regionid:$accountid:apigroup/*
CreatePlugin	Creates a plug-in.	acs:apigateway:$regionid:$accountid:plugin/*
ModifyPlugin	Modifies a plug-in.	acs:apigateway:$regionid:$accountid:plugin/$pluginId
DeletePlugin	Deletes a plug-in.	acs:apigateway:$regionid:$accountid:plugin/$pluginId
AttachPlugin	Binds a plug-in to an API operation.	acs:apigateway:$regionid:$accountid:plugin/$pluginId
DetachPlugin	Unbinds a plug-in from an API operation.	acs:apigateway:$regionid:$accountid:plugin/$pluginId
DescribePluginsByApi	Queries plug-ins that are bound to an API operation.	acs:apigateway:$regionid:$accountid:plugin/$pluginId
CreateApp	Creates an application.	acs:apigateway:$regionid:$accountid:app/*
ModifyApp	Modifies an application.	acs:apigateway:$regionid:$accountid:app/$appId

action-name	Description	Resource
DeleteApp	Deletes an application.	acs:apigateway:$regionid:$accountid:app/$appId
DescribeAppAttributes	Queries available applications.	acs:apigateway:$regionid:$accountid:app/$appId
SetApisAuthorities	Authorizes an application to call one or more API operations.	acs:apigateway:$regionid:$accountid:apigroup/$groupId
DescribeAuthorizedApps	Queries applications that are authorized to call an API operation.	acs:apigateway:$regionid:$accountid:apigroup/$groupId
SetVpcAccess	Creates a virtual private cloud (VPC) authorization entry.	acs:apigateway:$regionid:$accountid:vpcaccess/*
RemoveVpcAccess	Deletes a VPC authorization entry.	acs:apigateway:$regionid:$accountid:vpcaccess/*
DescribeVpcAccesses	Queries available VPC authorization entries.	acs:apigateway:$regionid:$accountid:vpcaccess/*
DescribeInstances	Queries available dedicated instances.	acs:apigateway:$regionid:$accountid:instance/$instanceId

Examples of authorization policies

Authorize a RAM user to query all API operations:

```
{
          "Version": "1",
          "Statement": [
            {
                      "Action": "apigateway:Describe*",
                      "Resource":"acs:apigateway:$regionid:$accountid:apigroup/*",
                      "Effect": "Allow"
            }
          ]
}
```

Authorize a RAM user to query API operations in all API groups with the `version:v1` tag:

```
{
          "Version": "1",
          "Statement": [
            {
                      "Action": "apigateway:Describe*",
                      "Resource":"acs:apigateway:$regionid:$accountid:apigroup/*",
                      "Effect": "Allow",
                "Condition": {
                       "StringEquals": {
                            "apigateway:tag/version": "v1"
                       }
                }
             }
          ]
}
```

Authorize a RAM user to manage all API operations in an API group:

```
{
          "Version": "1",
          "Statement": [
            {
                      "Action": "apigateway:*",
                      "Resource": [
                              "acs:apigateway:$regionid:$accountid:apigroup/$groupId",
                              "acs:apigateway:$regionid:$accountid:app/$appId",
                              "acs:apigateway:$regionid:$accountid:vpcaccess/*"
                      ],
                      "Effect": "Allow"
            }
          ]
}
```

Note: In the preceding examples, you can specify specific parts as * based on your business requirements.

4.Use tags to manage resources

This topic describes how to use tags to manage resources in API Gateway. Each tag is used to identify a group of resources that have common characteristics. This allows you to query and manage resources by group.

Each tag consists of two parts: a key and a value. When you tag a resource, you must specify the type of the resource. Tags for different types of resources are independent of each other, so are the tags in different regions. In API Gateway, the following types of resources can be tagged: API groups, API operations, plug-ins, and applications. The values of the ResourceType parameter are apiGroup, api, plugin, and app, respectively.

1. Scenarios

1. Tags can be used to manage a large amount of resources by group. This makes it convenient to query and manage resources.
2. Tags, combined with the permission management capability of Alibaba Cloud Resource Access Management (RAM), can be used to isolate resources for an Alibaba Cloud account and its RAM users. For more information, see section 3.1.

2. Limits

- A resource can have a maximum of 20 tags.
- For the same resource, the key of each tag must be unique. If you add a tag on a resource that already has a tag with the same key, the value of the new tag will override the value of the existing tag.
- A key can be up to 64 Unicode characters in length. A value can be up to 128 Unicode characters in length.
- Both keys and values are case-sensitive.
- A key cannot start with aliyun or acs:, contain http:// or https://, or be left unspecified.
- A value cannot contain http:// or https://. It can be a null string.

3. Permission control

3.1 Resource isolation for an Alibaba Cloud account and its RAM users

An Alibaba Cloud account is a primary account and can have many RAM users under it. These RAM users can be authorized to manage resources that are owned by the Alibaba Cloud account. For information about how to authorize RAM users to manage resources in API Gateway, see Use RAM to manage user permissions for API Gateway.

As the owner of an Alibaba Cloud account, you can use tags to classify resources. When you create an authorization policy, you can use these tags to specify the authorization condition. In this way, the authorized RAM user can only manage resources with the specified tags. For more information about how to create an authorization policy, see Policy elements. For example, your company has multiple departments. You can appoint an administrator, namely, create a RAM user, for each department. Then, you can authorize each RAM user to manage only resources with tags that are specific to their own department. The following examples show several scenarios in which permissions are granted based on tags.

Example 1:

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "apigateway:*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "apigateway:tag/depart": "dep1"
        }
      }
    }
  ]
}
```

In this example, the authorized RAM user can manage only resources with the depart:dep1 tag, namely, all the resources that belong to Department 1. **When this RAM user queries resources, the RAM user must include the Tag.1.Key=depart and Tag.1.Value=dep1 statements in the query condition.**

Example 2:

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "apigateway:*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "apigateway:tag/depart": ["dep2", "dep3"]
        }
      }
    }
  ]
}
```

In this example, the authorized RAM user can manage resources with the depart:dep2 tag or the depart:dep3 tag, namely, all the resources that belong to Department 2 or 3.

Example 3:

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "apigateway:*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "apigateway:tag/depart": "dep2",
         "apigateway:tag/Enviroment": "test"
        }
      }
    }
  ]
}
```

In this example, the authorized RAM user can manage only resources with both the depart:dep2 tag and the Enviroment:test tag. Namely, the RAM user can manage only resources that belong to Department 2 in the test environment.

API Gateway supports tag-based authorization for API groups, plug-ins, and applications. A RAM user who has permissions on an API group automatically has corresponding permissions on the API operations in the API group. You cannot use tags to authorize a RAM user to access specific API operations.

3.2 Limits of tag-based authorization

This section describes the limits of tag-based authorization on different types of API operations.

Limit on resource creation

When a RAM user creates a resource by calling an API operation in API Gateway, API Gateway checks whether the RAM user has permissions on all the resources to be used by the API operation. API Gateway also checks, based on the specified tag in the authorization policy that is attached to the RAM user, whether the RAM user has the permission to create the resource. Assume that a RAM user, who is authorized based on a tag, calls an API operation to create a resource, such as an API group, an application, or a plug-in. In this case, the RAM user must add the tag on the resource to be created in the API request.

For example, if the following authorization policy is attached to a RAM user, the RAM user must add the `depart:dept1` tag on each resource to be created.

```
{
    "Effect": "Allow",
    "Action": "apigateway:*",
     "Resource": "acs:apigateway:*:*:apigroup/*",
     "Condition": {
           "StringEquals": {
                "apigateway:tag/depart": "dep1"
            }
      }
}
```

Limit on resource management

When a RAM user calls an API operation to manage a resource in API Gateway, API Gateway checks whether the resource has the same tag that was used to authorize the RAM user. For example, if a RAM user calls the DeleteApp operation to delete an application, API Gateway allows the RAM user to delete the application only if the application has the same tag that was used to authorize the RAM user.

Limit on resource query

When a RAM user calls an API operation to query resources, API Gateway decides whether to allow the API request by checking whether the RAM user has permissions on all the resources that meet the query condition. If the RAM user does not have permissions on all the resources that meet the query condition, API Gateway rejects the API request. Therefore, after you authorize a RAM user by using a tag, the RAM user must specify the tag in the query condition when the user calls an API operation to query resources. For example, the ID of the resource to be queried is specified in the query condition. API Gateway allows the API request only if the resource has the same tag that was used to authorize the RAM user.

3.3 Important note that applies when a RAM user calls API operations to query resources

Assume that you have authorized a RAM user by using a tag. If the RAM user needs to call an API operation to query resources, the RAM user must enable tag-based authorization, namely, set the `EnableTagAuth` parameter to true in the API request. Only in this way can query results be returned. The EnableTagAuth parameter must be set to true in each request when a RAM user, who is authorized by using a tag, calls the following API operations to query resources:

- DescribeApiGroups
- DescribeAppAttributes

3.4 Important note that applies when you authorize a RAM user to query resources

In earlier versions of the RAM console, if you use the following authorization policy to authorize a RAM user to query an API group, information about the API group can be returned. However, in the latest version of the RAM console, the information about the API group will not be returned.

```
{
     "Effect": "Allow",
     "Action": "apigateway:*",
     "Resource": "acs:apigateway:*:*:apigroup/f0b34d4c55504a34897f7390a24ce253"
}
```

In the latest version of the RAM console, for a RAM user to query resources, the following adjustments must be made. **Note that to authorize a RAM user to create or manage resources, you create authorization policies as you did in earlier versions of the RAM console and do not need to make adjustments.**

1. Specify the Action and Resource elements in the authorization policy to allow the RAM user to query all API operations in all API groups, as shown in the following code snippet:

```
{
     "Effect": "Allow",
     "Action": ["apigateway:DescribeApiGroups", "apigateway:DescribeApisForConsole"],
     "Resource": "acs:apigateway:*:*:apigroup/*"
}
```

2. Log on to the RAM console by using your Alibaba Cloud account and add a tag on the resource to be authorized, such as

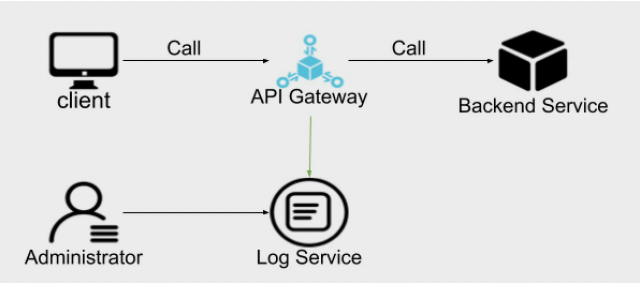
   `depart:dep1`

   . Then, specify the tag in the Condition element of the authorization policy, as shown in the following code snippet. In this way, the authorized RAM user can query resources by adding the tag in the query condition.

```
{
    "Effect": "Allow",
    "Action": "apigateway:*",
     "Resource": "acs:apigateway:*:*:apigroup/*",
     "Condition": {
           "StringEquals": {
                "apigateway:tag/depart": "dep1"
            }
      }
}
```

5.Use Log Service to manage logs of API calls

API Gateway seamlessly integrates with Log Service. Log Service provides various features. For example, you can query logs, download logs, and perform multi-dimensional statistical analysis of logs in real time. You can also ship logs to Object Storage Service(OSS) or MaxCompute.



- For more information about Log Service, see What is Log Service?.
- Log Service allows you to generate 500 MB of log data for free each month. If you generate more log data than this limit, the excess will be charged. For more information, see Pricing.

1. Overview

1.1 Online log query

You can use keywords to query logs. Both exact match and fuzzy match are supported. Log query can be used for troubleshooting or statistical query.

1.2 Detailed logs of API calls

The following table describes information about each API call in detailed logs.

Field	Description
apiGroupUid	The ID of the API group to which the API operation belongs.
apiGroupName	The name of the API group to which the API operation belongs.
apiUid	The ID of the API operation.
apiName	The name of the API operation.
apiStageUid	The ID of the environment where the API operation resides.
apiStageName	The name of the environment where the API operation resides.
httpMethod	The HTTP method that was used by the API request.
path	The request path in the API request.

Field	Description
Domain	The domain name of the requested resources.
statusCode	The HTTP status code of the API response.
errorMessage	The error message.
appId	The ID of the application from which the API request was sent.
appName	The name of the application from which the API request was sent.
clientIp	The IP address of the client from which the API request was sent.
exception	The specific error message that was returned by the backend service of the API operation.
providerAliUid	The ID of the account that owns the API operation.
region	The region where the API operation resides, for example, cn-hangzhou, which indicates the China (Hangzhou) region.
requestHandleTime	The time point in UTC at which the API request was received by API Gateway.
requestId	The ID of the API request. The ID of each API request is unique within API Gateway.
requestSize	The size of the API request. Unit: bytes.
responseSize	The size of the API response. Unit: bytes.
serviceLatency	The latency of the backend service of the API operation. Unit: milliseconds.

1.3 Custom analysis chart

You can use log fields in section 1.2 to customize analysis charts based on your statistical and business requirements.

1.4 Predefined analysis report

API Gateway provides a predefined analysis report, which contains predefined global statistical charts that are easy to use. You can use these charts to obtain information such as the number of API requests, success rate, failure rate, latency, number of applications that called API operations, failure statistics, most-called API groups, most-called API operations, and highest latency.

2. Configure the log service for API Gateway

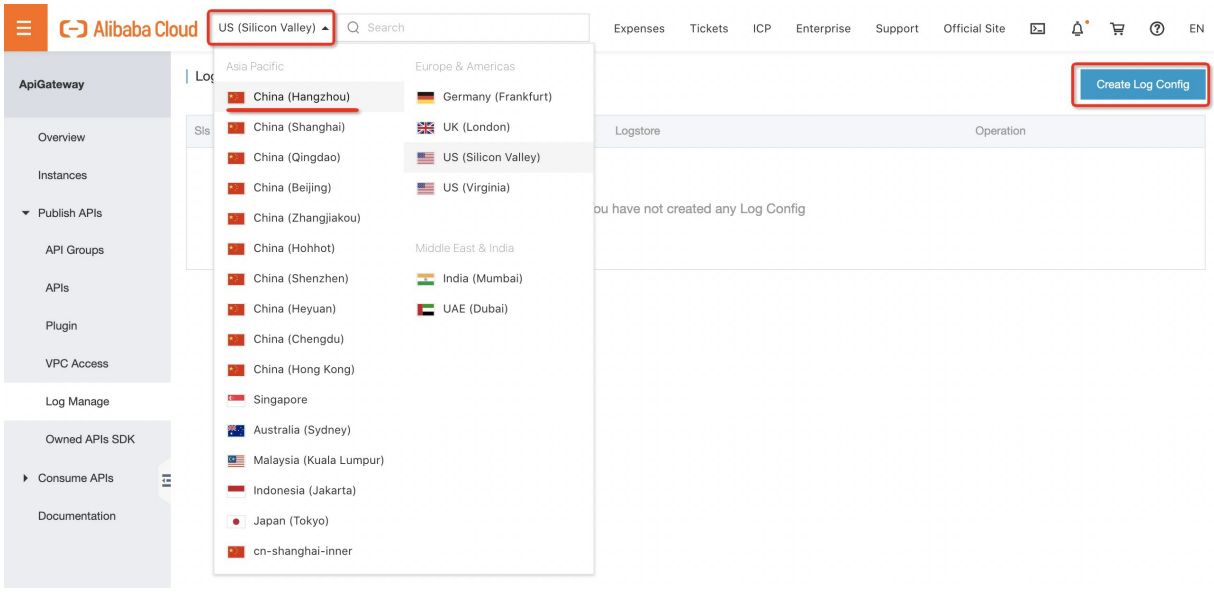
2.1 Configure the log service

Before you begin, make sure that you have activated Log Service and created a project and a Logstore in the Log Service console. For more information, see Log Service documentation.

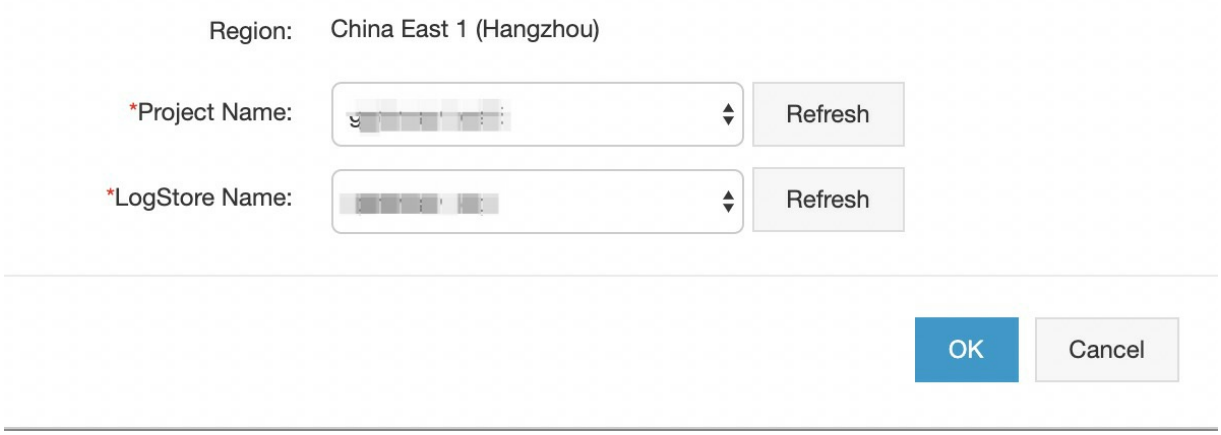
You can configure the log service for API Gateway in the API Gateway console or the Log Service console.

2.1.1 Configure the log service in the API Gateway console

(1) Log on to the API Gateway console. In the left-side navigation pane, choose Publish APIs > Log Manage. Select a region in the top navigation bar, for example, the China (Hangzhou) region.



(2) On the Log Manage page, click Create Log Config. The Create Log Config dialog box appears.



(3) Select a project and a Logstore. If no options are available after you click the drop-down arrow, click create new project to create a project and a LogStore in the Log Service Console.

(4) Go back to the API Gateway console and complete the configurations.

(5) You are navigated to the Log Service console. Enable the indexing feature for the Logstore.

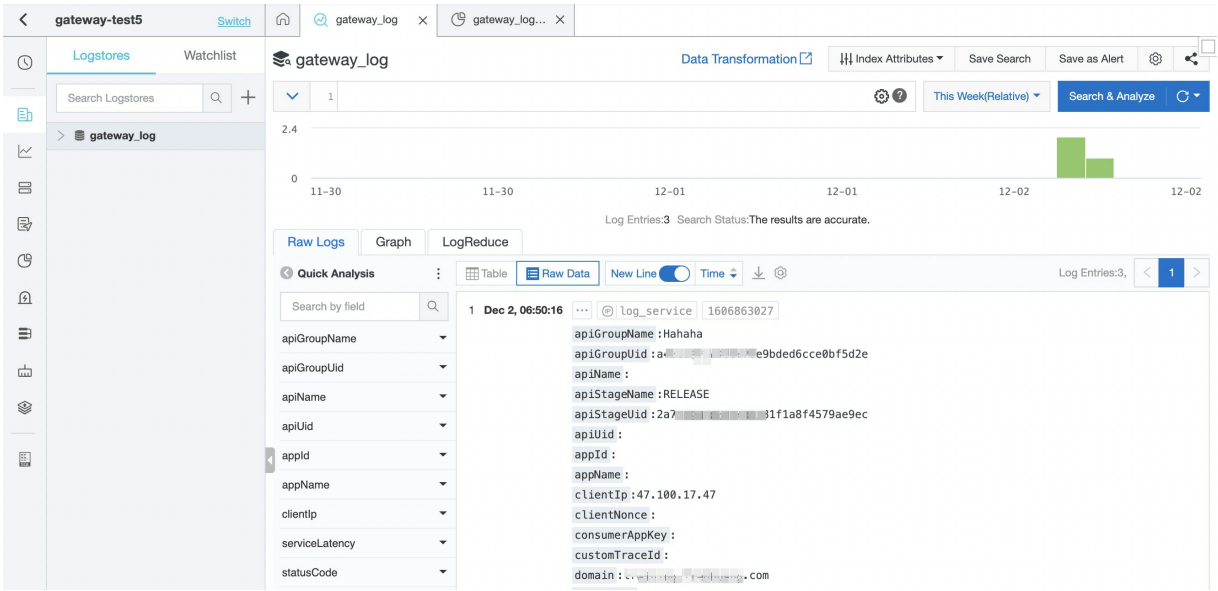
2.1.2 Configure the log service in the Log Service console

For information about how to configure the log service for API Gateway in the Log Service console, see API Gateway access logs.

After configurations are completed, API calls will be recorded in the Logstore that you created in the Log Service console and configured for the log service of API Gateway.

2.2 View logs of API calls

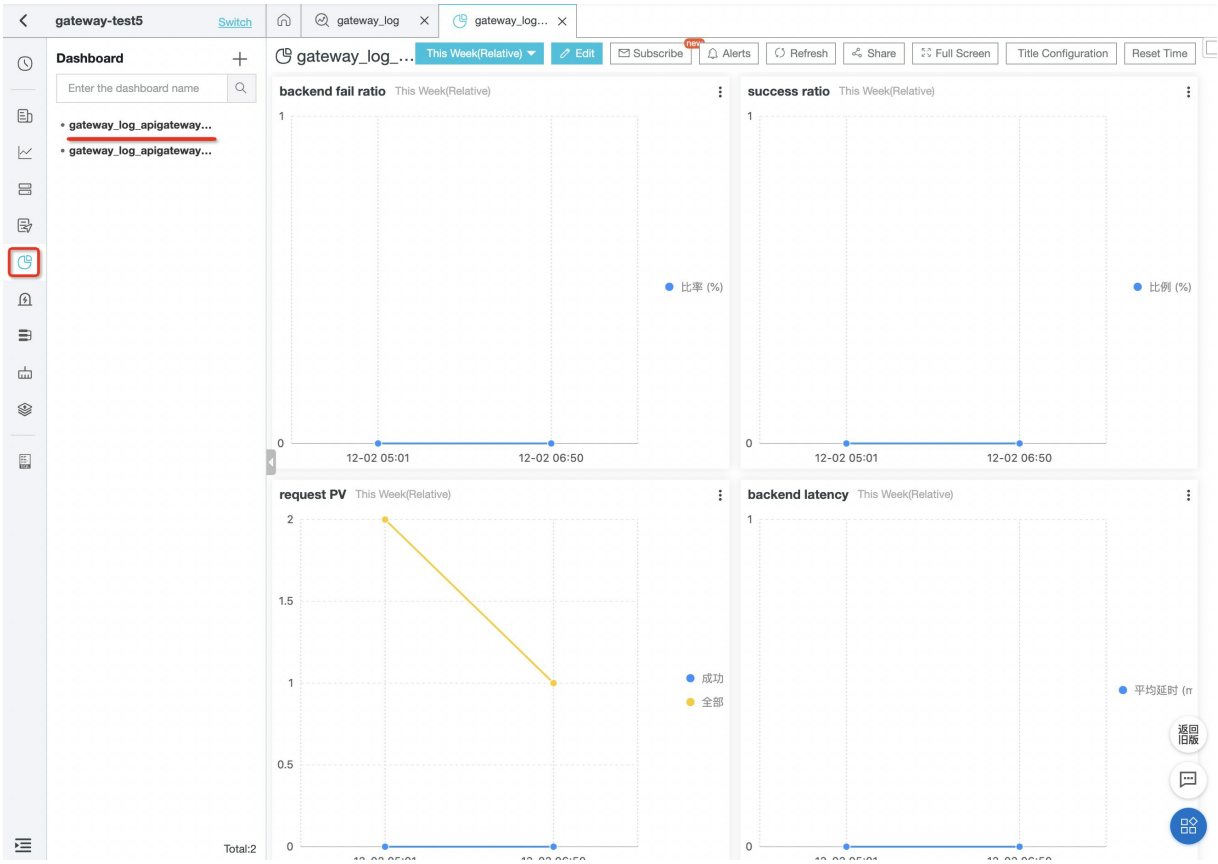
Log on to the API Gateway console. In the left-side navigation pane, choose Publish APIs > Log Manage. On the Log Manage page, click Access Log in the Operation column. You are navigated to the Log Service console, as shown in the following figure. On this page, you can query logs.



You can also log on to the Log Service console to view logs.

2.3 Query the predefined analysis report

The predefined analysis report is provided by API Gateway to facilitate statistical query. To view the predefined analysis report, log on to the API Gateway console. In the left-side navigation pane, choose Publish APIs > Log Manage. On the Log Manage page, click Access Log in the Operation column to go to the Log Service console. You can also directly view the predefined analysis report in the Log Service console, as shown in the following figure.



2.4 Customize query reports

You can customize query reports based on your business requirements. For more information, see Dashboard.

3. Manage logs

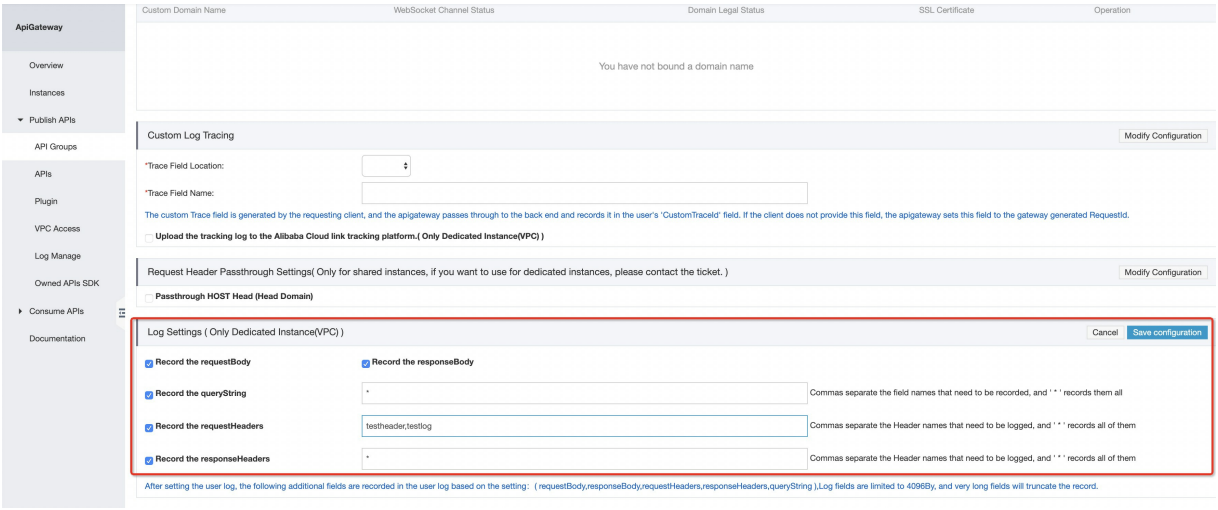
Log on to the API Gateway console. In the left-side navigation pane, choose Publish APIs > Log Manage. On the Log Manage page, click Modify Config or Delete Config in the Operation column.

- **Modify Config**: You can replace the existing project and Logstore with a new project and a new Logstore. After the replacement, API calls will be recorded in the new Logstore. However, historical API calls that were recorded in the original Logstore will not be migrated to the new Logstore.
- **Delete Config**: You can delete the log service configuration. After the deletion, API calls will no longer be recorded by Log Service. However, historical API calls that were recorded in the original Logstore will not be deleted.

6.Configure the logging of HTTP requests and responses

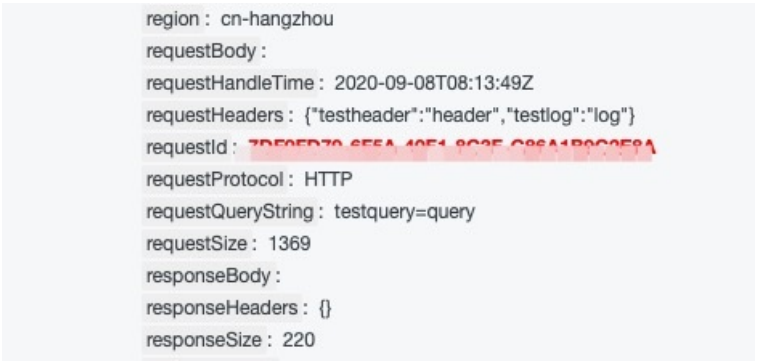
If you want API Gateway to log the HTTP requests it receives and the HTTP responses it returns, you can perform the operations described in this topic.

You can perform these configurations only for dedicated instances.



- Record the requestHeaders: Separate the names of request headers that you want to record with commas (,). You can set the value to ' * '. This value indicates that all headers are recorded.
- Record the responseHeaders: Separate the names of response headers that you want to record with commas (,). You can set the value to ' * '. This value indicates that all headers are recorded.
- Record the queryString: Separate the names of fields that you want to record with commas (,). You can set the value to ' * '. This value indicates that all fields are recorded.

Then, you can view the related information in logs. The following figure shows a log.



After the preceding log settings are configured, the system records the following fields in logs: requestBody, responseBody, requestHeaders, responseHeaders, and queryString. The size of each field must be no more than 4,096 bytes. If the size of a field exceeds this limit, the system truncates the field before it is recorded.

7.Configure alerting for APIs

You can use Cloud Monitor to configure alerting for APIs that are published to API Gateway. This allows you to track the running status of APIs at all times and ensure the stability of API Gateway.

1. Associate alert rules with APIs

The monitoring and alerting feature of API Gateway can meet your various business requirements. API Gateway monitors the following items:

- HttpStatusCode
- Response time of an API
- Number of requests for an API
- Inbound traffic
- Outbound traffic

You can use one of the following methods to create alert rules and associate the rules with APIs:

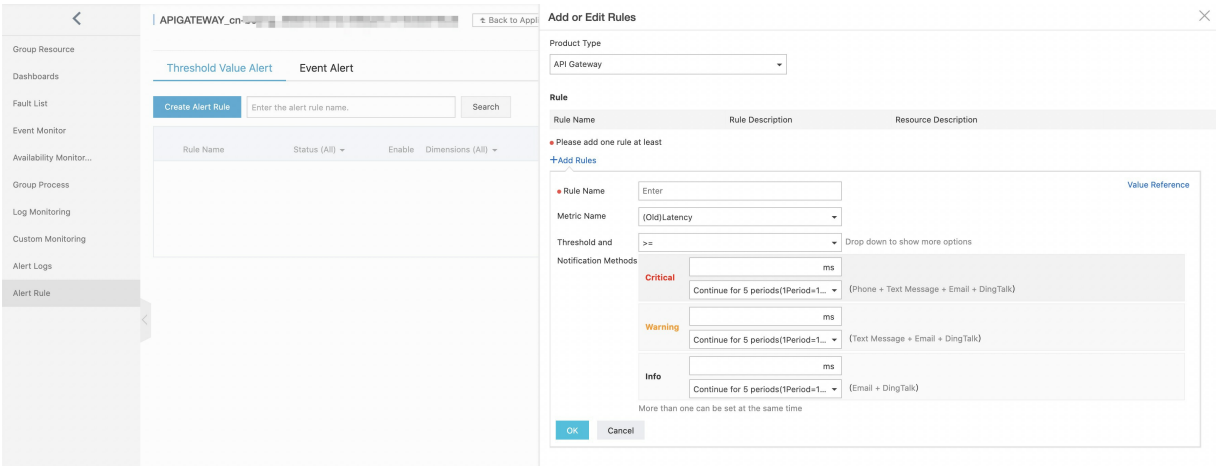
- Associate alert rules with a single API or multiple APIs that reside in the same region. This method is used if you want to configure alert rules for a single API or the same alert rules for multiple APIs that reside in the same region. The alert rules are not affected even if API configurations are modified.
- Associate alert rules with an API group. This method is used if you want to configure the same alert rules for all APIs in an API group. If you want to add, delete, or modify APIs in an API group, the system automatically updates alert rules for the API group.
- Associate alert rules with all APIs under your Alibaba Cloud account. This method is used if you have only a few APIs that need to be managed.

> **Note**
>
> If you use the first or second method, you can select a specific environment, such as RELEASE, PRE, or TEST, to configure monitoring and alerting for APIs.

2. Configure alerting levels and methods

Cloud Monitor allows you to configure three alerting levels: Critical, Warning, and Info. The alert notifications of the three levels are sent by using different methods. For more information about alert notifications, see Overview.

- Critical: phone calls, text messages, emails, and DingTalk ChatBot (use after payment)
- Warning: text messages, emails, and DingTalk ChatBot
- Info: emails and DingTalk ChatBot



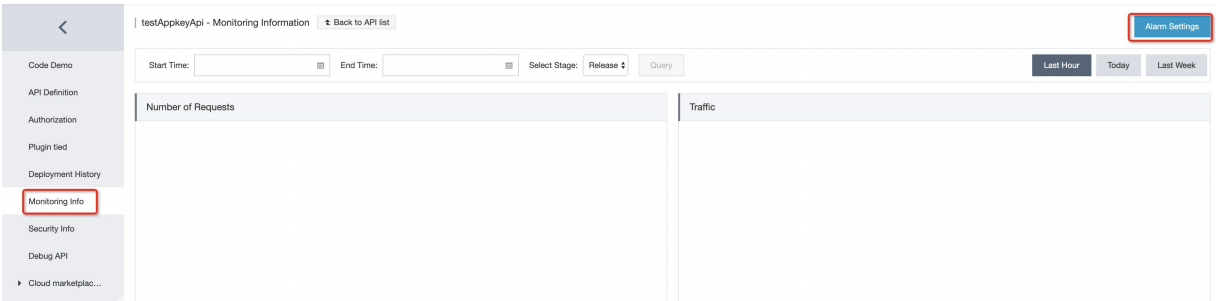
> **Note**
>
> The preceding figure shows a sample alert rule. If the number of 2XX status codes that are returned each minute exceeds 200 for five consecutive minutes, the system sends an alert notification.

3. Configure alert rules for one or more APIs

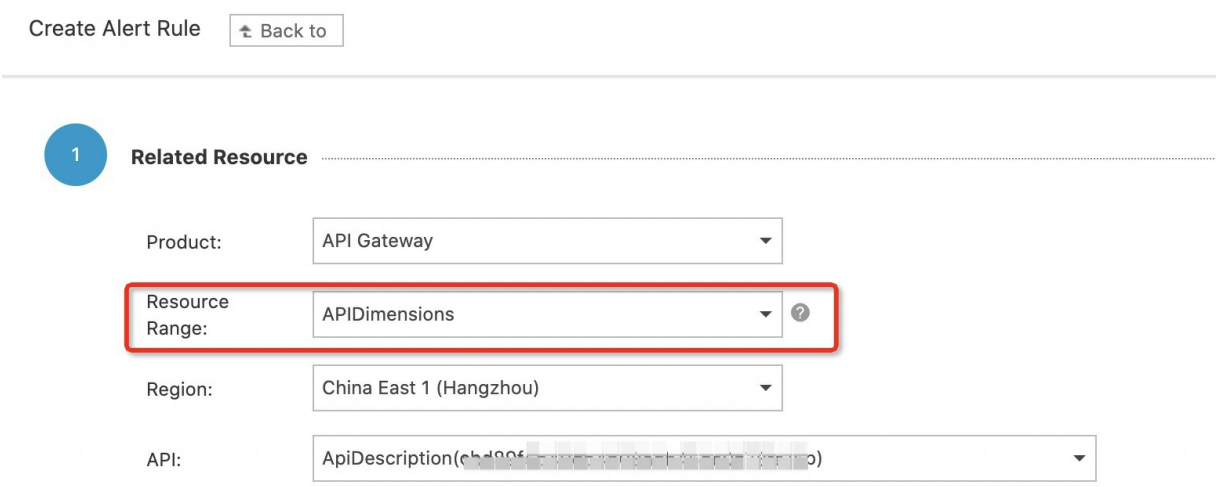
You must configure alert templates, specific rules, alert contacts, and notifications. For more information, see Overview.

1. Log on to the API Gateway console. In the top navigation bar, select a region. In the left-side navigation pane, choose Publish APIs > APIs. On the API List page, find the API for which you want to configure alert rules and click its name.

2. In the left-side navigation pane of the page that appears, click **Monitoring Info**. On the page that appears, click Alarm Settings in the upper-right corner to go to the Cloud Monitor console.

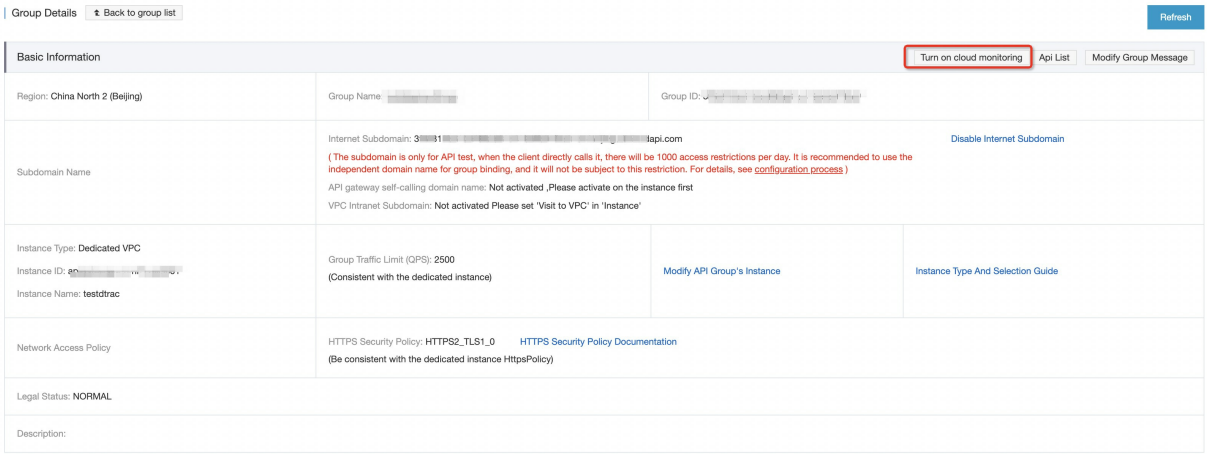


3. On the page that appears, click Create Alert Rule. On the Create Alert Rule page, set Resource Range to **API Dimensions**. In the API field, you can specify one or more APIs with which you want to associate alert rules.



4. Configure alert rules for an API group

1. To apply the same alert rules to all APIs in an API group, perform the following steps: In the left-side navigation pane, choose Publish APIs > API Groups. On the Group List page, find the API group for which you want to configure alert rules and click its name. On the Group Details page, click `Turn on cloud monitoring` in the upper-right corner.



2. If you enable the cloud monitoring feature for an API group for the first time, you must create an AliyunServiceRoleForApiGatewayMonitoring service-linked role in the dialogue box that appears.

3. Click OK. Then, the system displays the "Group cloud monitoring is successfully turned on" message. This message contains the name of a monitoring group. This monitoring group is created by API Gateway after being authorized by users. This monitoring group corresponds to the current API group. The format of the monitoring group name is `APIGATEWAY_${region}_${groupId}`. The region field indicates the region where the API group resides. The groupId field indicates the ID of the API group.

4. After you enable cloud monitoring, click `Click to jump to cloud monitoring configuration` in the upper-right corner of the Group Details page. On the page that appears, you can configure alert rules for the current API group.

5. Configure alert rules for all APIs

The steps are similar to those in Section 3. However, you must set Resource Range to All Resources. After that, all APIs that are published to API Gateway in the current region use the same alert rules.

6. Configure alert rules supported by API Gateway

API Gateway monitors the following items for APIs: HTTP status code, response time of an API, number of requests for an API, inbound traffic, and outbound traffic. You can configure alert rules based on these items.

- Response time of an API: the response time of a backend service of API Gateway.
- Number of requests for an API: the total number of requests that are received by API Gateway for a specific API from clients within a specific period.
- Inbound traffic: the traffic of requests that are received by API Gateway from clients within a specific period.
- Outbound traffic: the traffic of requests that are sent to the backend services of API Gateway within a specific period.
- HTTP status code: the status code that is returned by API Gateway. The state codes include 2XX, 4XX, and 5XX codes.

-Code2XX: The request for an API is successful. Note: A successful request does not mean that the service is successful.

-Code4XX: An error occurs on the client, such as a parameter error.

-Code5XX: An error occurs on a backend service. Users must pay close attention to such errors.

7. Usage notes

- We recommend that users whose API groups reside in the classic network apply alert rules that are marked with `Old` and users whose API groups reside in a virtual private cloud (VPC) use alert rules that are not marked with `Old`.
- You can configure alert rules based on the network environment where your APIs are published. If the alert rules configured for an API that is published in a VPC do not take effect, you can log on to the API Gateway console to go to the API monitoring information page. Then, check whether the monitoring data of the API can be queried based on the network environment. If not, submit a ticket to upgrade the version of your API Gateway.

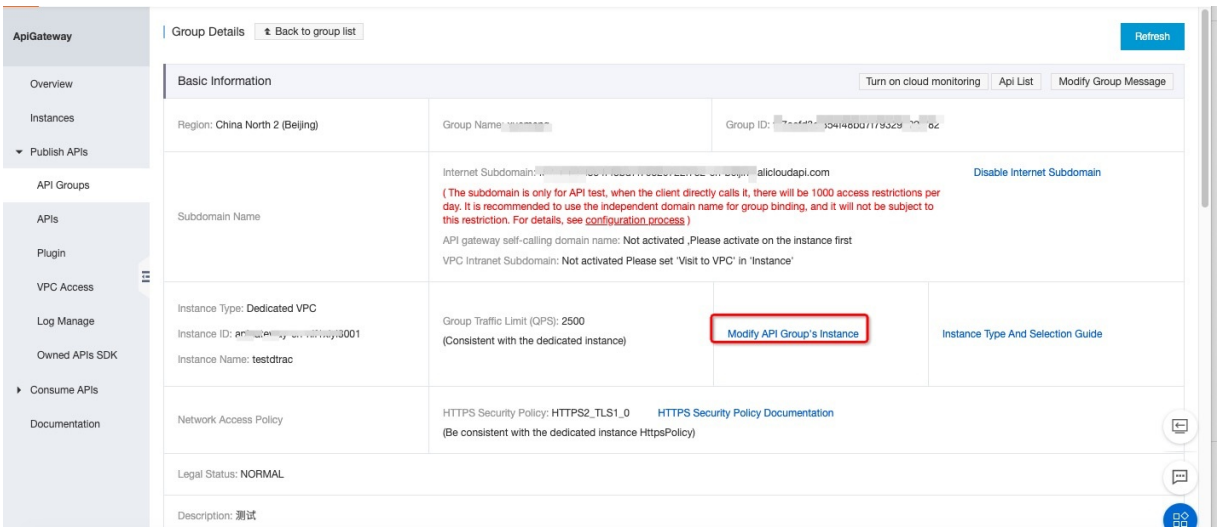
8.Migrate API groups between instances

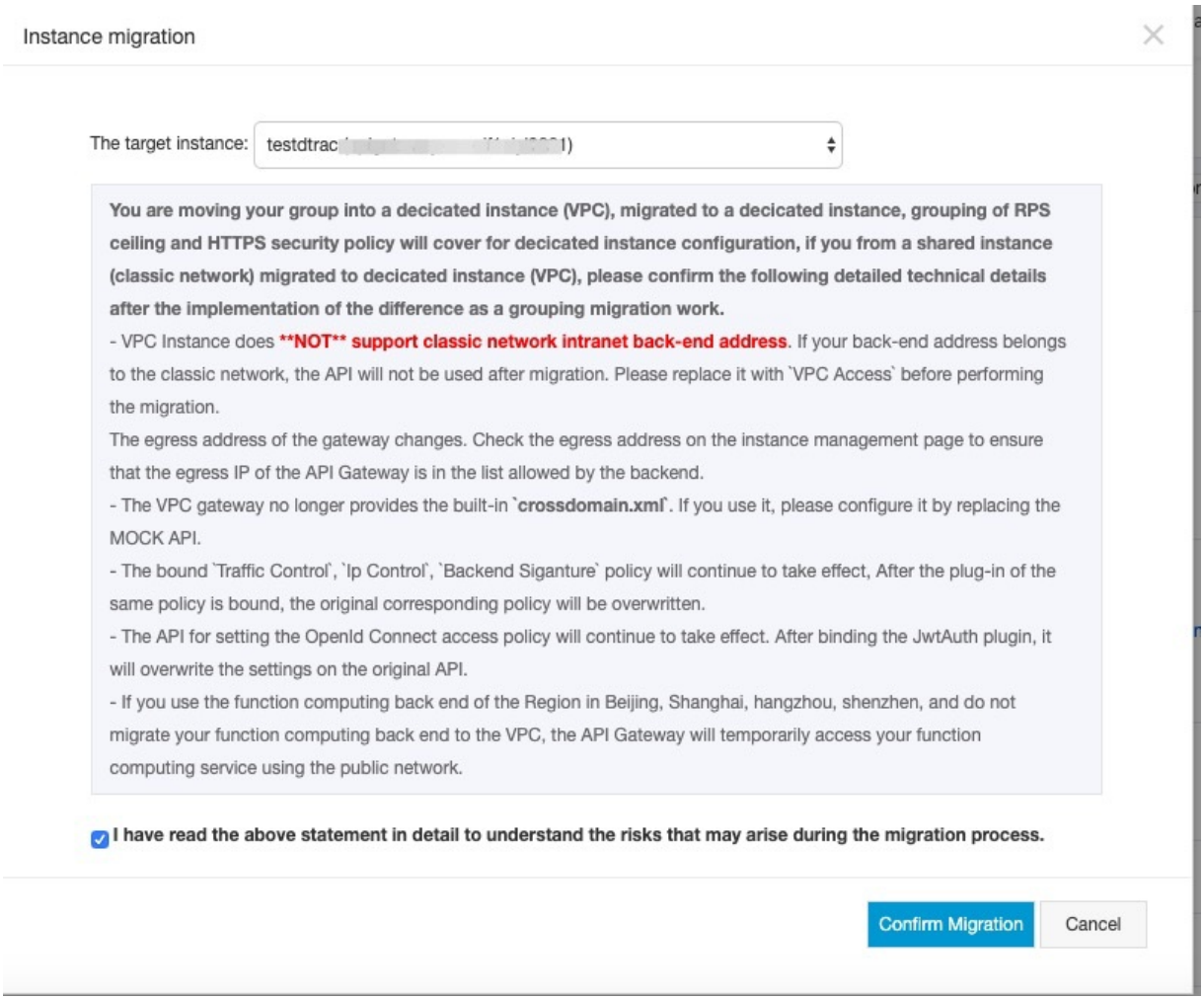
1. Scenarios of different instances

- Shared instance (classic network): This is an earlier instance type that is offered by API Gateway and provides limited features. Shared instances (classic network) are no longer maintained, and new features are unavailable for the instances of this type. We recommend that you migrate your data to shared instances (VPC) or dedicated instances (VPC) at the earliest opportunity.
- Shared instance (VPC): Tenants share the same outbound IP address and bandwidth. Therefore, each tenant is prone to the interference from other tenants. This instance type is more suitable for development testing, evaluation, and small-scale production.
- Dedicated instance (VPC): To obtain a higher-level guarantee in the service level agreement (SLA), you can purchase a higher specification for requests per second (RPS) to use dedicated resources. The resources include inbound public IP addresses, IP addresses for virtual private clouds (VPCs), outbound Internet bandwidth, and isolated server clusters.

2. Migration procedure

Log on to the API Gateway console and choose Open API > `Groups` in the left-side navigation pane. Click the name of the API group that you want to migrate. On the `Group Details` page, click Modify Instance for API Group Deployment. In the Migrate Instance dialog box, select the destination instance from the `Destination Instance` drop-down list. Read the usage notes and select **I have read the preceding statement and know the potential risks associated with the migration.** Then, click `Migration`. The migration immediately takes effect on the Domain Name System (DNS) of the second-level domains of API Gateway. The migration takes effect on your API group about 1 to 10 minutes later based on the DNS cache.


ApiGateway
Overview
Instances
Publish APIs
API Groups
APIs
Plugin
VPC Access
Log Manage
Owned APIs SDK
Consume APIs
Documentation
Group Details
Back to group list
Refresh
Basic Information
Turn on cloud monitoring
Api List
Modify Group Message
Region: China North 2 (Beijing)
Group Name:
Group ID:
Subdomain Name
Internet Subdomain:
alicloudapi.com
Disable Internet Subdomain
(The subdomain is only for API test, when the client directly calls it, there will be 1000 access restrictions per day. It is recommended to use the independent domain name for group binding, and it will not be subject to this restriction. For details, see configuration process)
API gateway self-calling domain name: Not activated ,Please activate on the instance first
VPC Intranet Subdomain: Not activated Please set 'Visit to VPC' in 'Instance'
Instance Type: Dedicated VPC
Instance ID:
Instance Name: testdtrac
Group Traffic Limit (QPS): 2500
(Consistent with the dedicated instance)
Modify API Group's Instance
Instance Type And Selection Guide
Network Access Policy
HTTPS Security Policy: HTTPS2_TLS1_0
HTTPS Security Policy Documentation
(Be consistent with the dedicated instance HttpsPolicy)
Legal Status: NORMAL
Description: 测试


Instance migration
The target instance:
testdtrac
You are moving your group into a decicated instance (VPC), migrated to a decicated instance, grouping of RPS ceiling and HTTPS security policy will cover for decicated instance configuration, if you from a shared instance (classic network) migrated to decicated instance (VPC), please confirm the following detailed technical details after the implementation of the difference as a grouping migration work.
- VPC Instance does **NOT** support classic network intranet back-end address. If your back-end address belongs to the classic network, the API will not be used after migration. Please replace it with `VPC Access` before performing the migration.
The egress address of the gateway changes. Check the egress address on the instance management page to ensure that the egress IP of the API Gateway is in the list allowed by the backend.
- The VPC gateway no longer provides the built-in `crossdomain.xml`. If you use it, please configure it by replacing the MOCK API.
- The bound `Traffic Control`, `Ip Control`, `Backend Siganture` policy will continue to take effect, After the plug-in of the same policy is bound, the original corresponding policy will be overwritten.
- The API for setting the OpenId Connect access policy will continue to take effect. After binding the JwtAuth plugin, it will overwrite the settings on the original API.
- If you use the function computing back end of the Region in Beijing, Shanghai, hangzhou, shenzhen, and do not migrate your function computing back end to the VPC, the API Gateway will temporarily access your function computing service using the public network.
I have read the above statement in detail to understand the risks that may arise during the migration process.
Confirm Migration
Cancel

> **Note**
>
> If your dedicated instance cannot meet your needs, you can migrate the API groups in the dedicated instance to a dedicated instance of higher specifications. Perform the following steps for migration:
>
> 1. Purchase a dedicated instance of the required specifications.
>
> 2. Migrate your API groups to the new instance by following the steps in "2. Migration procedure."
>
> **Note: Due to the DNS cache, some requests are sent to the previous instance after the migration. Make sure that all requests are forwarded to the new instance before you release the previous instance.**

3. Migration notes

If you need to migrate an API group for which you have changed the RPS, submit a ticket. Before you migrate an API group, check each of the following technical details about the differences before and after migration.

3.1 Migrate an API group from a shared instance (classic network) to a shared instance (VPC)

- API Gateway instances of the VPC type **do not support backend service addresses of the classic network type**.
- The outbound IP address of an API Gateway instance may change. You can go to the Instances page to view the outbound IP address. Make sure that the outbound IP address of the API Gateway instance is included in the whitelist of IP addresses that are allowed to access the backend service.
- An API Gateway instance of the VPC type does not provide a preconfigured **crossdomain.xml** file. If you need to use the file, configure an API in mock mode.
- The throttling, IP access control, and backend signature policies that have been configured are still valid. After the plug-ins for the same policies are used, the previously configured policies become invalid.
- The APIs for which you have configured the OpenID Connect access policy are still valid. After the JWT Auth plug-in is used, the original configurations for the APIs become invalid.

3.2 Migrate an API group from a shared instance (classic network) to a dedicated instance (VPC)

- After you migrate an API group to a dedicated instance, the maximum RPS and the HTTPS security policy of the destination dedicated instance apply to the API group.
- API Gateway instances of the VPC type **do not support backend service addresses of the classic network type**. If your backend service address is of the classic network type, API operations cannot be called after you migrate your API group. Change the backend configuration by using the method of VPC access authorization before you migrate your API group.
- The outbound IP address of an API Gateway instance may change. You can go to the Instances page to view the outbound IP address. Make sure that the outbound IP address of the API Gateway instance is included in the whitelist of IP addresses that are allowed to access the backend service.
- An API Gateway instance of the VPC type does not provide a preconfigured **crossdomain.xml** file. If you need to use the file, configure an API in mock mode.

- The throttling, IP access control, and backend signature policies that have been configured are still valid. After the plug-ins for the same policies are used, the previously configured policies become invalid.
- The APIs for which you have configured the OpenID Connect access policy are still valid. After the JWT Auth plug-in is used, the original configurations for the APIs become invalid.
- For example, you use Function Compute as a backend service that is deployed in the China (Beijing), China (Shanghai), China (Hangzhou), or China (Shenzhen) region, and you have not migrated the backend service to a VPC. In this case, API Gateway temporarily accesses your Function Compute services over the Internet.
- If the second-level domain name for access over VPCs is enabled for your API group, make sure that a VPC is bound to the destination instance before you migrate your API group. This makes sure that you can access API Gateway from the bound VPC.

3.3 Migrate an API group from a shared instance (VPC) to a shared instance (classic network)

- For API Gateway instances of the VPC type, the backend service can use the TLS 1.2 protocol. For API Gateway instances of the classic network type, the backend service can use only the TLS 1.0 protocol.
- All plug-in configurations become invalid. The throttling, IP access control, and backend signature policies for API Gateway instances of the classic network type must be reconfigured.
- The outbound IP address of an API Gateway instance may change. You can go to the Instances page to view the outbound IP address. Make sure that the outbound IP address of the API Gateway instance is included in the whitelist of IP addresses that are allowed to access the backend service.
- Some new features may not be supported. Pay attention to the prompts that are displayed in the API Gateway console.

3.4 Migrate an API group from a shared instance (VPC) to a dedicated instance (VPC)

- After you migrate an API group to a dedicated instance, the maximum RPS and the HTTPS security policy of the destination dedicated instance apply to the API group.
- The outbound IP address of an API Gateway instance may change. You can go to the Instances page to view the outbound IP address. Make sure that the outbound IP address of the API Gateway instance is included in the whitelist of IP addresses that are allowed to access the backend service.
- If specific features are enabled for your API group, make sure that relevant features are enabled for the destination instance before you migrate your API group. Specific features for an API group include the second-level domain name for access over VPCs, the internal domain name for API calls from API Gateway, inbound IPv6 traffic, and outbound IPv6 traffic.

3.5 Migrate an API group from a dedicated instance (VPC) to a dedicated instance (VPC)

- After you migrate an API group to a dedicated instance, the maximum RPS and the HTTPS security policy of the destination dedicated instance apply to the API group.
- The outbound IP address of an API Gateway instance may change. You can go to the Instances page to view the outbound IP address. Make sure that the outbound IP address of the API Gateway instance is included in the whitelist of IP addresses that are allowed to access the backend service.

- If specific features are enabled for your API group, make sure that relevant features are enabled for the destination instance before you migrate your API group. Specific features for an API group include the second-level domain name for access over VPCs, the internal domain name for API calls from API Gateway, inbound IPv6 traffic, and outbound IPv6 traffic.