Application Operations Management

API Reference

Issue 01

Date 2025-01-21

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei Cloud and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Cloud Computing Technologies Co., Ltd.

Address: Huawei Cloud Data Center Jiaoxinggong Road
Qianzhong Avenue
Gui'an New District
Gui Zhou 550029
People's Republic of China

Website: https://www.huaweicloud.com/intl/en-us/

Contents

1 Before You Start

1.1 Overview

Welcome to use Application Operations Management (AOM). AOM is a one-stop, multi-dimensional O&M management platform for cloud applications. It provides one-stop observability analysis. By collecting metrics, logs, and performance data from the cloud and local devices, AOM enables you to monitor real-time running status of applications, resources, and services and detect faults in a timely manner, improving O&M automation capability and efficiency.

This document describes how to use APIs to perform operations on AOM, such as creation, deletion, and query. For details about all supported operations, see **2 API Overview**.

If you plan to call AOM APIs, ensure that you are familiar with AOM concepts..

1.2 API Calling

AOM supports Representational State Transfer (REST) APIs, allowing you to call APIs using HTTPS.

For details about API calling, see **3 Calling APIs**.

1.3 Endpoints

An endpoint is the request address for calling an API. Endpoints vary depending on services and regions.

For the endpoints of all services, see **Regions and Endpoints**.

1.4 Concepts

- Account

  An account is created upon successful registration with the cloud. The account has full access permissions for all of its cloud services and resources. It can be used to reset user passwords and grant user permissions. The account is a payment entity and should not be used directly to perform routine

management. For security purposes, create Identity and Access Management (IAM) users and grant them permissions for routine management.

- IAM User

  An IAM user is created using an account to use cloud services. Each IAM user has its own identity credentials (password and access keys).

  An IAM user can view the account ID and user ID on the **My Credentials** page of the console. The account name, username, and password will be required for API authentication.

- Region

  Regions are divided by geographical location and network latency. Public services, such as Elastic Cloud Server (ECS), Elastic Volume Service (EVS), Object Storage Service (OBS), Virtual Private Cloud (VPC), Elastic IP (EIP), and Image Management Service (IMS), are shared within a region. Regions are classified into universal and dedicated regions. A universal region provides universal cloud services for common tenants. A dedicated region provides specific services for specific tenants.

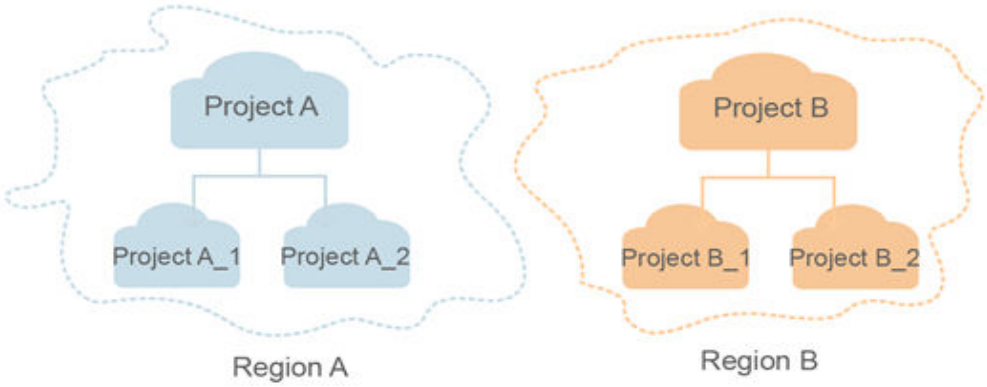
- Availability Zone (AZ)

  AZs are physically isolated locations in a region, but are interconnected through an internal network for enhanced application availability.

- Project

  Projects group and isolate resources (including compute, storage, and network resources) across physical regions. A default project is provided for each cloud region. Users can be granted permissions to access all resources in a specific project. For more refined access control, create subprojects under a project and purchase resources in the subprojects. Users can then be assigned permissions to access only specific resources in the subprojects.

  Figure 1-1 Project isolating model

  To view a project ID, go to the **My Credentials** page.

- Enterprise Project

  Enterprise projects group and manage resources across regions. Resources in enterprise projects are logically isolated. An enterprise project can contain resources in multiple regions, and resources can be transferred between enterprise projects.

For details about how to obtain enterprise project IDs and features, see the ***Enterprise Management User Guide***.

2 API Overview

AOM provides alarm, monitoring, Prometheus monitoring, log, Prometheus instance, configuration management, and APIs, helping you quickly and cost-effectively maintain applications.

Table 2-1 API overview

Type	API
Alarm APIs	Alarm APIs, including the APIs for adding, updating, and deleting event alarm rules.
Monitoring APIs	Monitoring APIs, including the APIs for querying metrics, and querying and adding monitoring data.
Prometheus Monitoring APIs	Prometheus monitoring APIs, including the APIs for querying the expression calculation result in a specified period or at a specified time point.
Log APIs	Log APIs, including the API for querying logs.
Prometheus Instance APIs (AOM 2.0 only)	APIs related to Prometheus instances, including adding and querying Prometheus instances, and uninstalling hosted Prometheus instances.
Configuration Management APIs	Configuration APIs, including the APIs for querying the cloud services for which AOM 2.0 has been granted permissions, and querying ICAgents installed on cluster hosts.

3 Calling APIs

3.1 Making an API Request

This section describes the structure of a REST API request, and uses the IAM API for **obtaining a user token** as an example to demonstrate how to call an API. The obtained token can then be used to authenticate the calling of other APIs.

Request URI

A request URI is in the following format:

{URI-scheme}://{Endpoint}/{resource-path}?{query-string}

Although a request URI is included in the request header, most programming languages or frameworks require the request URI to be transmitted separately.

- **URI-scheme**: Protocol used to transmit requests. All APIs use HTTPS.
- **Endpoint**: Domain name or IP address of the server bearing the REST service. The endpoint varies between services in different regions. It can be obtained from **Regions and Endpoints**.

  For example, the endpoint of IAM in the **CN-Hong Kong** region is **iam.ap-southeast-1.myhuaweicloud.com**.

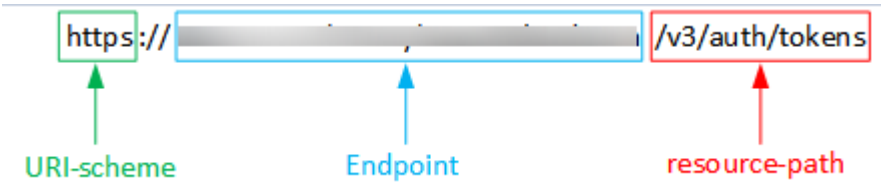
  NOTICE

  For monitoring, log, and auto scaling APIs, use AOM endpoints. For APM APIs, use APM endpoints. For details, see **1.3 Endpoints**.

- **resource-path**: Access path of an API for performing a specified operation. Obtain the path from the URI of an API. For example, the **resource-path** of the API used to obtain a user token is **/v3/auth/tokens**.
- **query-string**: Query parameter, which is optional. Ensure that a question mark (?) is included before each query parameter that is in the format of "Parameter name=Parameter value". For example, **? limit=10** indicates that a maximum of 10 data records will be displayed.

For example, to obtain an IAM token in the *xxx* region, obtain the endpoint of IAM for this region and the **resource-path** in the URI of the API used to obtain a user token. Then, construct the URI as follows:

Figure 3-1 Example URI



NOTE

To simplify the URI display in this document, each API is provided only with a **resource-path** and a request method. The **URI-scheme** of all APIs is **HTTPS**, and the endpoints of all APIs in the same region are identical.

Request Methods

The HTTP protocol defines the following request methods that can be used to send a request to the server:

- **GET**: requests the server to return specified resources.
- **PUT**: requests the server to update specified resources.
- **POST**: requests the server to add resources or perform special operations.
- **DELETE**: requests the server to delete specified resources, for example, an object.
- **HEAD**: requests the server to return the response header only.
- **PATCH**: requests the server to update partial content of a specified resource. If the resource does not exist, a new resource will be created.

For example, in the case of the API used to obtain a user token, the request method is POST. The request is as follows:

```
POST https://Endpoint/v3/auth/tokens
```

Request Header

You can also add additional header fields to a request, such as the fields required by a specified URI or HTTP method. For example, to request for the authentication information, add **Content-Type**, which specifies the request body type.

Common request header fields are as follows:

- **Content-Type**: specifies the request body type or format. This field is mandatory and its default value is **application/json**. Other values of this field will be provided for specific APIs if any.
- **X-Auth-Token**: specifies a user token only for token-based API authentication. The user token is a response to the API used to obtain a user token. This API is the only one that does not require authentication.

> **NOTE**
>
> In addition to supporting token-based authentication, public cloud APIs also support authentication using access key ID/secret access key (AK/SK). During AK/SK-based authentication, an SDK is used to sign the request, and the **Authorization** (signature information) and **X-Sdk-Date** (time when the request is sent) header fields are automatically added to the request.
>
> For more information, see **AK/SK-based Authentication**.

The API used to obtain a user token does not require authentication. Therefore, only the **Content-Type** field needs to be added to requests for calling the API. An example of such requests is as follows:

```
POST https://Endpoint/v3/auth/tokens
Content-Type: application/json
```

Request Body

The body of a request is often sent in a structured format as specified in the **Content-Type** header field. The request body transfers content except the request header.

The request body varies between APIs. Some APIs do not require the request body, such as the APIs requested using the GET and DELETE methods.

In the case of the API used to obtain a user token, the request parameters and parameter description can be obtained from the API request. The following provides an example request with a body included. Replace *username*, *domainname*, ********* (login password), and *xxxxxxxxxxxxxxxxx* (project ID) with the actual values. To learn how to obtain a project ID, see **8.3 Obtaining an Account ID and Project ID**.

> **NOTE**
>
> The **scope** parameter specifies where a token takes effect. You can set **scope** to an account or a project under an account.

```
POST https://Endpoint/v3/auth/tokens
Content-Type: application/json
{
    "auth": {
        "identity": {
            "methods": [
                "password"
            ],
            "password": {
                "user": {
                    "name": "username",
                    "password": "********",
                    "domain": {
                        "name": "domainname"
                    }
                }
            }
        },
        "scope": {
            "project": {
                "id": "xxxxxxxxxxxxxxxxx"
            }
        }
    }
}
```


If all data required for the API request is available, you can send the request to call the API through curl, Postman, or coding. In the response to the API used to obtain a user token, **x-subject-token** is the desired user token. This token can then be used to authenticate the calling of other APIs.

3.2 Authentication

Requests for calling an API can be authenticated using either of the following methods:

- Token-based authentication: Requests are authenticated using a token.
- AK/SK-based authentication: Requests are authenticated by encrypting the request body using an AK/SK pair.

Token-based Authentication

NOTE

The validity period of a token is 24 hours. When using a token for authentication, cache it to prevent frequently calling the Identity and Access Management (IAM) API used to obtain a user token.

A token specifies temporary permissions in a computer system. During API authentication using a token, the token is added to requests to get permissions for calling the API.

In **3.1 Making an API Request**, the process of calling the API used to **obtain a user token** is described. When calling an API to obtain a user token, you must set **auth.scope** in the request body to **project**.

```
{
    "auth": {
        "identity": {
            "methods": [
                "password"
            ],
            "password": {
                "user": {
                    "name": "username",
                    "password": "********",
                    "domain": {
                        "name": "domainname"
                    }
                }
            }
        },
        "scope": {
            "project": {
                "name": "xxxxxxxx"
            }
        }
    }
}
```

After a token is obtained, the **X-Auth-Token** header field must be added to requests to specify the token when calling other APIs. For example, if the token is **ABCDEFJ....**, **X-Auth-Token: ABCDEFJ....** can be added to a request as follows:

```
GET https://Endpoint/v3/auth/projects
Content-Type: application/json
X-Auth-Token: ABCDEFJ....
```


AK/SK-based Authentication

NOTE

AK/SK-based authentication supports API requests with a body not larger than 12 MB. For API requests with a larger body, token-based authentication is recommended.

In AK/SK-based authentication, AK/SK is used to sign requests and the signature is then added to the requests for authentication.

- AK: access key ID, which is a unique identifier used in conjunction with a secret access key to sign requests cryptographically.
- SK: secret access key used in conjunction with an AK to sign requests cryptographically. It identifies a request sender and prevents the request from being modified.

In AK/SK-based authentication, you can use an AK/SK to sign requests based on the signature algorithm or use the signing SDK to sign requests. For details about how to sign requests and use the signing SDK, see **AK/SK Signing and Authentication Guide**.

CAUTION

The signing SDK is only used for signing requests and is different from the SDKs provided by services.

3.3 Response

Status Code

After sending a request, you will receive a response, including a status code, response header, and response body.

A status code is a group of digits, ranging from 1xx to 5xx. It indicates the status of a request. For more information, see **8.1 Status Codes**.

If status code **201** is returned for the calling of the API for **obtaining a user token**, the request is successful.

Response Header

Similar to a request, a response also has a header, for example, **Content-Type**.

For the API used to obtain a user token, the **x-subject-token** header field is the desired user token. This token can then be used to authenticate the calling of other APIs.

Figure 3-2 Header fields of the response to the request for obtaining a user token

Response Body

The body of a response is often returned in structured format as specified in the **Content-Type** header field. The response body transfers content except the response header.

The following is part of the response body for the API used to obtain a user token.

```
{
    "token": {
        "expires_at": "2019-02-13T06:52:13.855000Z",
        "methods": [
            "password"
        ],
        "catalog": [
            {
                "endpoints": [
                    {
                        "region_id": "xx-xxxxxx-1",
.....
```

If an error occurs during API calling, an error code and a message will be displayed. The following shows an error response body.

```
{
    "errorCode": "SVCSTG_AMS_4000001",
    "errorMessage": "Request param invalid"
}
```

In the response body, **errorCode** is an error code, and **errorMessage** provides information about the error.

4 APIs

4.1 Alarm

4.1.1 Querying the Event Alarm Rule List

Function

This API is used to query the event alarm rule list.

Calling Method

For details, see **Calling APIs**.

URI

GET /v2/{project_id}/event2alarm-rule

Table 4-1 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID obtained from IAM. Generally, a project ID contains 32 characters. Minimum: **32** Maximum: **32**

Request Parameters

Table 4-2 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token obtained from IAM. Minimum: **0** Maximum: **40960**
Content-Type	Yes	String	Content type, which is application/json. Enumeration values: • **application/json**

Response Parameters

Status code: 200

Table 4-3 Response body parameters

Parameter	Type	Description
[items]	Array of **Event2alarmRuleBody** objects	OK: The request is successful.

Table 4-4 Event2alarmRuleBody

Parameter	Type	Description
user_id	String	Project ID. Minimum: **32** Maximum: **32**
name	String	Rule name. Enter a maximum of 100 characters and do not start or end with a special character. Only letters, digits, underscores (_), and hyphens (-) are allowed. Minimum: **1** Maximum: **100**

Parameter	Type	Description
description	String	Rule description. Enter a maximum of 1024 characters and do not start or end with an underscore (_) or hyphen (-). Only letters, digits, and special characters (_-<>=,.) are allowed. Minimum: **0** Maximum: **1024**
create_time	Long	Creation time. Minimum: **0** Maximum: **9999999999999**
update_time	Long	Update time. Minimum: **0** Maximum: **9999999999999**
resource_provider	String	Event source. Minimum: **0** Maximum: **64**
metadata	**metadata** object	Source data.
enable	Boolean	Whether to enable the rule.
trigger_policies	Array of **trigger_policies** objects	Trigger policy. Array Length: **0 - 1024**
alarm_type	String	Alarm type. notification: direct alarm reporting. denoising: alarm noise reduction. Minimum: **0** Maximum: **32** Enumeration values: • **notification** • **denoising**
action_rule	String	Alarm action rule. Minimum: **0** Maximum: **128**
inhibit_rule	String	Alarm suppression rule. Minimum: **0** Maximum: **128**

Parameter	Type	Description
route_group_rule	String	Alarm grouping rule. Minimum: **0** Maximum: **128**
event_names	Array of strings	Event name.
migrated	Boolean	Whether to migrate to AOM 2.0.
topics	Array of **SmnTopics** objects	SMN information.

Table 4-5 metadata

Parameter	Type	Description
customField	Array of strings	Custom tag. Minimum: **0** Maximum: **1024** Array Length: **0 - 1024**

Table 4-6 trigger_policies

Parameter	Type	Description
id	Integer	ID. Minimum: **0** Maximum: **128**
name	String	Event name. Minimum: **0** Maximum: **128**
trigger_type	String	Trigger type. accumulative: Accumulated trigger. immediately: Immediate trigger. Minimum: **0** Maximum: **128** Enumeration values: • **accumulative** • **immediately**

Parameter	Type	Description
period	Integer	Trigger cycle. Minimum: **1** Maximum: **86400**
operator	String	Comparison operator. Minimum: **0** Maximum: **8**
count	Integer	Number of trigger times. Minimum: **1** Maximum: **100**
level	String	Alarm severity. Minimum: **0** Maximum: **32**

Table 4-7 SmnTopics

Parameter	Type	Description
display_name	String	Topic display name, which will be the name of an email sender. Max.: 192 bytes. This parameter is left blank by default. Minimum: **1** Maximum: **64**
name	String	Name of the topic. Enter 1 to 255 characters starting with a letter or digit. Only letters, digits, hyphens (-), and underscores (_) are allowed. Minimum: **1** Maximum: **255**
push_policy	Integer	SMN message push policy. Options: 0 and 1. Minimum: **0** Maximum: **1**

Parameter	Type	Description
status	Integer	Status of the topic subscriber. 0: The topic has been deleted or the subscription list of this topic is empty. 1: The subscription object is in the subscribed state. 2: The subscription object is in the unsubscribed or canceled state. Enumeration values: • **0** • **1** • **2**
topic_urn	String	Unique resource identifier of the topic. Minimum: **1** Maximum: **100**

Status code: 401

Table 4-8 Response body parameters

Parameter	Type	Description
error_code	String	Error code. Minimum: **12** Maximum: **12**
error_msg	String	Error message. Minimum: **0** Maximum: **1024**
error_type	String	Error type. Minimum: **0** Maximum: **128**
trace_id	String	Request ID. Minimum: **32** Maximum: **32**

Status code: 403

Table 4-9 Response body parameters

Parameter	Type	Description
error_code	String	Error code. Minimum: **12** Maximum: **12**
error_msg	String	Error message. Minimum: **0** Maximum: **1024**
error_type	String	Error type. Minimum: **0** Maximum: **128**
trace_id	String	Request ID. Minimum: **32** Maximum: **32**

Status code: 500

Table 4-10 Response body parameters

Parameter	Type	Description
error_code	String	Error code. Minimum: **12** Maximum: **12**
error_msg	String	Error message. Minimum: **0** Maximum: **1024**
error_type	String	Error type. Minimum: **0** Maximum: **128**
trace_id	String	Request ID. Minimum: **32** Maximum: **32**

Example Requests

Query the event alarm rule list.

```
https://{endpoint}/v2/{project_id}/event2alarm-rule
```


Example Responses

Status code: 200

OK: The request is successful.


```
[ {
  "action_rule" : "1",
  "alarm_type" : "notification",
  "create_time" : 1701442632968,
  "description" : "",
  "enable" : true,
  "event_names" : [ ],
  "inhibit_rule" : "",
  "metadata" : {
    "customField" : [ "xxx" ]
  },
  "migrated" : false,
  "name" : "1jB5h6GnbY",
  "resource_provider" : "AOM",
  "route_group_rule" : "",
  "topics" : [ ],
  "trigger_policies" : [ {
    "count" : 99,
    "id" : 0,
    "level" : "",
    "name" : "",
    "operator" : ">=",
    "period" : 300,
    "trigger_type" : "accumulative"
  } ],
  "update_time" : 0,
  "user_id" : "2a473356cca5487f8373be891bffc1cf"
} ]
```


Status code: 401

Unauthorized: The authentication information is incorrect or invalid.


```
{
  "error_code" : "SVCSTG.AMS.2000051",
  "error_msg" : "auth failed.",
  "error_type" : "AUTH_FAILED"
}
```


Status code: 403

Forbidden: The request is rejected. The server has received the request and understood it, but the server refuses to respond to it. The client should not repeat the request without modifications.


```
{
  "error_code" : "AOM.0403",
  "error_msg" : "auth failed.",
  "error_type" : "AUTH_FAILED"
}
```


Status code: 500

Internal Server Error: The server is able to receive the request but unable to understand the request.


```
{
  "error_code" : "APM.00000500",
  "error_msg" : "Internal Server Error",
  "trace_id" : ""
}
```


Status Codes

Status Code	Description
200	OK: The request is successful.
401	Unauthorized: The authentication information is incorrect or invalid.
403	Forbidden: The request is rejected. The server has received the request and understood it, but the server refuses to respond to it. The client should not repeat the request without modifications.
500	Internal Server Error: The server is able to receive the request but unable to understand the request.

Error Codes

See **Error Codes**.

4.1.2 Adding an Event Alarm Rule

Function

This API is used to add an event alarm rule.

Calling Method

For details, see **Calling APIs**.

URI

POST /v2/{project_id}/event2alarm-rule

Table 4-11 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID obtained from IAM. Generally, a project ID contains 32 characters. Minimum: **32** Maximum: **32**

Request Parameters

Table 4-12 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token obtained from IAM. Minimum: **0** Maximum: **40960**
Content-Type	Yes	String	Content type, which is application/json. Enumeration values: • **application/json**

Table 4-13 Request body parameters

Parameter	Mandatory	Type	Description
user_id	Yes	String	Project ID. Minimum: **32** Maximum: **32**
name	Yes	String	Rule name. Enter a maximum of 100 characters and do not start or end with a special character. Only letters, digits, underscores (_), and hyphens (-) are allowed. Minimum: **1** Maximum: **100**
description	No	String	Rule description. Enter a maximum of 1024 characters and do not start or end with an underscore (_) or hyphen (-). Only letters, digits, and special characters (_-<>=,.) are allowed. Minimum: **0** Maximum: **1024**
create_time	Yes	Long	Creation time. Minimum: **0** Maximum: **9999999999999**

Parameter	Mandatory	Type	Description
update_time	No	Long	Update time. Minimum: **0** Maximum: **9999999999999**
resource_provider	No	String	Event source. Minimum: **0** Maximum: **64**
metadata	Yes	**metadata** object	Source data.
enable	Yes	Boolean	Whether to enable the rule.
trigger_policies	Yes	Array of **trigger_policies** objects	Trigger policy. Array Length: **0 - 1024**
alarm_type	Yes	String	Alarm type. notification: direct alarm reporting. denoising: alarm noise reduction. Minimum: **0** Maximum: **32** Enumeration values: • **notification** • **denoising**
action_rule	Yes	String	Alarm action rule. Minimum: **0** Maximum: **128**
inhibit_rule	No	String	Alarm suppression rule. Minimum: **0** Maximum: **128**
route_group_rule	No	String	Alarm grouping rule. Minimum: **0** Maximum: **128**
event_names	No	Array of strings	Event name.
migrated	No	Boolean	Whether to migrate to AOM 2.0.
topics	No	Array of **SmnTopics** objects	SMN information.

Table 4-14 metadata

Parameter	Mandatory	Type	Description
customField	No	Array of strings	Custom tag. Minimum: **0** Maximum: **1024** Array Length: **0 - 1024**

Table 4-15 trigger_policies

Parameter	Mandatory	Type	Description
id	No	Integer	ID. Minimum: **0** Maximum: **128**
name	No	String	Event name. Minimum: **0** Maximum: **128**
trigger_type	No	String	Trigger type. accumulative: Accumulated trigger. immediately: Immediate trigger. Minimum: **0** Maximum: **128** Enumeration values: • **accumulative** • **immediately**
period	No	Integer	Trigger cycle. Minimum: **1** Maximum: **86400**
operator	No	String	Comparison operator. Minimum: **0** Maximum: **8**
count	No	Integer	Number of trigger times. Minimum: **1** Maximum: **100**
level	No	String	Alarm severity. Minimum: **0** Maximum: **32**

Table 4-16 SmnTopics

Parameter	Mandatory	Type	Description
display_name	No	String	Topic display name, which will be the name of an email sender. Max.: 192 bytes. This parameter is left blank by default. Minimum: **1** Maximum: **64**
name	Yes	String	Name of the topic. Enter 1 to 255 characters starting with a letter or digit. Only letters, digits, hyphens (-), and underscores (_) are allowed. Minimum: **1** Maximum: **255**
push_policy	Yes	Integer	SMN message push policy. Options: 0 and 1. Minimum: **0** Maximum: **1**
status	No	Integer	Status of the topic subscriber. 0: The topic has been deleted or the subscription list of this topic is empty. 1: The subscription object is in the subscribed state. 2: The subscription object is in the unsubscribed or canceled state. Enumeration values: • **0** • **1** • **2**
topic_urn	Yes	String	Unique resource identifier of the topic. Minimum: **1** Maximum: **100**

Response Parameters

Status code: 400

Table 4-17 Response body parameters

Parameter	Type	Description
error_code	String	Error code. Minimum: **12** Maximum: **12**
error_msg	String	Error message. Minimum: **0** Maximum: **1024**
error_type	String	Error type. Minimum: **0** Maximum: **128**
trace_id	String	Request ID. Minimum: **32** Maximum: **32**

Status code: 401

Table 4-18 Response body parameters

Parameter	Type	Description
error_code	String	Error code. Minimum: **12** Maximum: **12**
error_msg	String	Error message. Minimum: **0** Maximum: **1024**
error_type	String	Error type. Minimum: **0** Maximum: **128**
trace_id	String	Request ID. Minimum: **32** Maximum: **32**

Status code: 403

Table 4-19 Response body parameters

Parameter	Type	Description
error_code	String	Error code. Minimum: **12** Maximum: **12**
error_msg	String	Error message. Minimum: **0** Maximum: **1024**
error_type	String	Error type. Minimum: **0** Maximum: **128**
trace_id	String	Request ID. Minimum: **32** Maximum: **32**

Status code: 500

Table 4-20 Response body parameters

Parameter	Type	Description
error_code	String	Error code. Minimum: **12** Maximum: **12**
error_msg	String	Error message. Minimum: **0** Maximum: **1024**
error_type	String	Error type. Minimum: **0** Maximum: **128**
trace_id	String	Request ID. Minimum: **32** Maximum: **32**

Example Requests

Add an event alarm rule whose user ID is "xxxx", name is "scl_test_event", and event source is "AOM".

```
https://{endpoint}/v2/{project_id}/event2alarm-rule
```



```
{
  "user_id" : "xxxx",
  "name" : "scl_test_event",
  "description" : "",
  "create_time" : 1669276173427,
  "update_time" : 0,
  "resource_provider" : "AOM",
  "metadata" : {
    "customField" : [ "xxx=xxx" ]
  },
  "enable" : true,
  "trigger_policies" : [ {
    "id" : 0,
    "name" : "",
    "trigger_type" : "accumulative",
    "period" : 300,
    "operator" : ">=",
    "count" : 99,
    "level" : ""
  } ],
  "alarm_type" : "notification",
  "action_rule" : "111111",
  "inhibit_rule" : "",
  "route_group_rule" : ""
}
```

Example Responses

Status code: 204

OK: The request is successful.

Status code: 400

Bad Request: The request is invalid. The client should not repeat the request without modifications.

```
{
  "error_code" : "AOM.02011400",
  "error_msg" : "actionRule is invalid!",
  "error_type" : "BAD_REQUEST",
  "trace_id" : ""
}
```

Status code: 401

Unauthorized: The authentication information is incorrect or invalid.

```
{
  "error_code" : "SVCSTG.AMS.2000051",
  "error_msg" : "auth failed.",
  "error_type" : "AUTH_FAILED"
}
```

Status code: 403

Forbidden: The request is rejected. The server has received the request and understood it, but the server refuses to respond to it. The client should not repeat the request without modifications.

```
{
  "error_code" : "SVCSTG.AMS.2000051",
  "error_msg" : "auth failed.",
  "error_type" : "AUTH_FAILED",
  "trace_id" : "8fb508e9e31b44279016f708e1c60e4c"
}
```


Status code: 500

Internal Server Error: The server is able to receive the request but unable to understand the request.

```
{
  "error_code" : "APM.00000500",
  "error_msg" : "Internal Server Error",
  "trace_id" : ""
}
```

Status Codes

Status Code	Description
204	OK: The request is successful.
400	Bad Request: The request is invalid. The client should not repeat the request without modifications.
401	Unauthorized: The authentication information is incorrect or invalid.
403	Forbidden: The request is rejected. The server has received the request and understood it, but the server refuses to respond to it. The client should not repeat the request without modifications.
500	Internal Server Error: The server is able to receive the request but unable to understand the request.

Error Codes

See **Error Codes**.

4.1.3 Modifying an Event Alarm Rule

Function

This API is used to modify an event alarm rule.

Calling Method

For details, see **Calling APIs**.

URI

PUT /v2/{project_id}/event2alarm-rule

Table 4-21 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID obtained from IAM. Generally, a project ID contains 32 characters. Minimum: **32** Maximum: **32**

Request Parameters

Table 4-22 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	No	String	User token obtained from IAM. Minimum: **0** Maximum: **40960**
Content-Type	Yes	String	Content type, which is application/json. Enumeration values: • **application/json**

Table 4-23 Request body parameters

Parameter	Mandatory	Type	Description
user_id	Yes	String	Project ID. Minimum: **32** Maximum: **32**
name	Yes	String	Rule name. Enter a maximum of 100 characters and do not start or end with a special character. Only letters, digits, underscores (_), and hyphens (-) are allowed. Minimum: **1** Maximum: **100**

Parameter	Mandatory	Type	Description
description	No	String	Rule description. Enter a maximum of 1024 characters and do not start or end with an underscore (_) or hyphen (-). Only letters, digits, and special characters (_-<>=,.) are allowed. Minimum: **0** Maximum: **1024**
create_time	Yes	Long	Creation time. Minimum: **0** Maximum: **9999999999999**
update_time	No	Long	Update time. Minimum: **0** Maximum: **9999999999999**
resource_provider	No	String	Event source. Minimum: **0** Maximum: **64**
metadata	Yes	**metadata** object	Source data.
enable	Yes	Boolean	Whether to enable the rule.
trigger_policies	Yes	Array of **trigger_policies** objects	Trigger policy. Array Length: **0 - 1024**
alarm_type	Yes	String	Alarm type. notification: direct alarm reporting. denoising: alarm noise reduction. Minimum: **0** Maximum: **32** Enumeration values: • **notification** • **denoising**
action_rule	Yes	String	Alarm action rule. Minimum: **0** Maximum: **128**
inhibit_rule	No	String	Alarm suppression rule. Minimum: **0** Maximum: **128**

Parameter	Mandatory	Type	Description
route_group_rule	No	String	Alarm grouping rule. Minimum: **0** Maximum: **128**
event_names	No	Array of strings	Event name.
migrated	No	Boolean	Whether to migrate to AOM 2.0.
topics	No	Array of **SmnTopics** objects	SMN information.

Table 4-24 metadata

Parameter	Mandatory	Type	Description
customField	No	Array of strings	Custom tag. Minimum: **0** Maximum: **1024** Array Length: **0 - 1024**

Table 4-25 trigger_policies

Parameter	Mandatory	Type	Description
id	No	Integer	ID. Minimum: **0** Maximum: **128**
name	No	String	Event name. Minimum: **0** Maximum: **128**
trigger_type	No	String	Trigger type. accumulative: Accumulated trigger. immediately: Immediate trigger. Minimum: **0** Maximum: **128** Enumeration values: • **accumulative** • **immediately**

Parameter	Mandatory	Type	Description
period	No	Integer	Trigger cycle. Minimum: **1** Maximum: **86400**
operator	No	String	Comparison operator. Minimum: **0** Maximum: **8**
count	No	Integer	Number of trigger times. Minimum: **1** Maximum: **100**
level	No	String	Alarm severity. Minimum: **0** Maximum: **32**

Table 4-26 SmnTopics

Parameter	Mandatory	Type	Description
display_name	No	String	Topic display name, which will be the name of an email sender. Max.: 192 bytes. This parameter is left blank by default. Minimum: **1** Maximum: **64**
name	Yes	String	Name of the topic. Enter 1 to 255 characters starting with a letter or digit. Only letters, digits, hyphens (-), and underscores (_) are allowed. Minimum: **1** Maximum: **255**
push_policy	Yes	Integer	SMN message push policy. Options: 0 and 1. Minimum: **0** Maximum: **1**

Parameter	Mandatory	Type	Description
status	No	Integer	Status of the topic subscriber. 0: The topic has been deleted or the subscription list of this topic is empty. 1: The subscription object is in the subscribed state. 2: The subscription object is in the unsubscribed or canceled state. Enumeration values: • **0** • **1** • **2**
topic_urn	Yes	String	Unique resource identifier of the topic. Minimum: **1** Maximum: **100**

Response Parameters

Status code: 400

Table 4-27 Response body parameters

Parameter	Type	Description
error_code	String	Error code. Minimum: **12** Maximum: **12**
error_msg	String	Error message. Minimum: **0** Maximum: **1024**
error_type	String	Error type. Minimum: **0** Maximum: **128**
trace_id	String	Request ID. Minimum: **32** Maximum: **32**

Status code: 401

Table 4-28 Response body parameters

Parameter	Type	Description
error_code	String	Error code. Minimum: **12** Maximum: **12**
error_msg	String	Error message. Minimum: **0** Maximum: **1024**
error_type	String	Error type. Minimum: **0** Maximum: **128**
trace_id	String	Request ID. Minimum: **32** Maximum: **32**

Status code: 403

Table 4-29 Response body parameters

Parameter	Type	Description
error_code	String	Error code. Minimum: **12** Maximum: **12**
error_msg	String	Error message. Minimum: **0** Maximum: **1024**
error_type	String	Error type. Minimum: **0** Maximum: **128**
trace_id	String	Request ID. Minimum: **32** Maximum: **32**

Status code: 500

Table 4-30 Response body parameters

Parameter	Type	Description
error_code	String	Error code. Minimum: **12** Maximum: **12**
error_msg	String	Error message. Minimum: **0** Maximum: **1024**
error_type	String	Error type. Minimum: **0** Maximum: **128**
trace_id	String	Request ID. Minimum: **32** Maximum: **32**

Example Requests

Update an event alarm rule whose user ID is "xxxxxxx", event source is "AOM", and name is "scl_test_event".

```
https://{endpoint}/v2/{project_id}/event2alarm-rule

{
  "user_id" : "xxxxxxx",
  "name" : "scl_test_event",
  "description" : "",
  "create_time" : 1669276304343,
  "update_time" : 1669276304343,
  "resource_provider" : "AOM",
  "metadata" : {
    "customField" : [ "xxx" ]
  },
  "enable" : true,
  "trigger_policies" : [ {
    "id" : 0,
    "name" : "",
    "trigger_type" : "accumulative",
    "period" : 300,
    "operator" : ">=",
    "count" : 99,
    "level" : ""
  } ],
  "alarm_type" : "notification",
  "action_rule" : "111111",
  "inhibit_rule" : "",
  "route_group_rule" : ""
}
```

Example Responses

Status code: 204

OK: The request is successful.

Status code: 400

Bad Request: The request is invalid. The client should not repeat the request without modifications.

```
{
  "error_code" : "AOM.02011400",
  "error_msg" : "actionRule is invalid!",
  "error_type" : "BAD_REQUEST",
  "trace_id" : ""
}
```

Status code: 401

Unauthorized: The authentication information is incorrect or invalid.

```
{
  "error_code" : "SVCSTG.AMS.2000051",
  "error_msg" : "auth failed.",
  "error_type" : "AUTH_FAILED"
}
```

Status code: 403

Forbidden: The request is rejected. The server has received the request and understood it, but the server refuses to respond to it. The client should not repeat the request without modifications.

```
{
  "error_code" : "SVCSTG.AMS.2000051",
  "error_msg" : "auth failed.",
  "error_type" : "AUTH_FAILED"
}
```

Status code: 500

Internal Server Error: The server is able to receive the request but unable to understand the request.

```
{
  "error_code" : "APM.00000500",
  "error_msg" : "Internal Server Error",
  "trace_id" : ""
}
```

Status Codes

Status Code	Description
204	OK: The request is successful.
400	Bad Request: The request is invalid. The client should not repeat the request without modifications.
401	Unauthorized: The authentication information is incorrect or invalid.
403	Forbidden: The request is rejected. The server has received the request and understood it, but the server refuses to respond to it. The client should not repeat the request without modifications.

Status Code	Description
500	Internal Server Error: The server is able to receive the request but unable to understand the request.

Error Codes

See **Error Codes**.

4.1.4 Deleting an Event Alarm Rule

Function

This API is used to delete an event alarm rule.

Calling Method

For details, see **Calling APIs**.

URI

DELETE /v2/{project_id}/event2alarm-rule

Table 4-31 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID obtained from IAM. Generally, a project ID contains 32 characters. Minimum: **32** Maximum: **32**

Request Parameters

Table 4-32 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token obtained from IAM. Minimum: **1** Maximum: **40960**

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Content type, which is application/json. Enumeration values: • **application/json**

Table 4-33 Request body parameters

Parameter	Mandatory	Type	Description
[items]	Yes	Array of strings	Name of the rule to be deleted.

Response Parameters

Status code: 400

Table 4-34 Response body parameters

Parameter	Type	Description
error_code	String	Error code. Minimum: **12** Maximum: **12**
error_msg	String	Error message. Minimum: **0** Maximum: **1024**
error_type	String	Error type. Minimum: **0** Maximum: **128**
trace_id	String	Request ID. Minimum: **32** Maximum: **32**

Status code: 401

Table 4-35 Response body parameters

Parameter	Type	Description
error_code	String	Error code. Minimum: **12** Maximum: **12**
error_msg	String	Error message. Minimum: **0** Maximum: **1024**
error_type	String	Error type. Minimum: **0** Maximum: **128**
trace_id	String	Request ID. Minimum: **32** Maximum: **32**

Status code: 403

Table 4-36 Response body parameters

Parameter	Type	Description
error_code	String	Error code. Minimum: **12** Maximum: **12**
error_msg	String	Error message. Minimum: **0** Maximum: **1024**
error_type	String	Error type. Minimum: **0** Maximum: **128**
trace_id	String	Request ID. Minimum: **32** Maximum: **32**

Status code: 500

Table 4-37 Response body parameters

Parameter	Type	Description
error_code	String	Error code. Minimum: **12** Maximum: **12**
error_msg	String	Error message. Minimum: **0** Maximum: **1024**
error_type	String	Error type. Minimum: **0** Maximum: **128**
trace_id	String	Request ID. Minimum: **32** Maximum: **32**

Example Requests

Delete event alarm rule "aomTestLts".

```
https://{endpoint}/v2/{project_id}/event2alarm-rule

[ "aomTestLts" ]
```

Example Responses

Status code: 400

Bad Request: The request is invalid. The client should not repeat the request without modifications.

```
{
  "error_code" : "AOM.02013125",
  "error_msg" : "send kafka message failed",
  "error_type" : "INTERNAL_SERVER_ERROR",
  "trace_id" : "8fb508e9e31b44279016f708e1c60e4c"
}
```

Status code: 401

Unauthorized: The authentication information is incorrect or invalid.

```
{
  "error_code" : "SVCSTG.AMS.2000051",
  "error_msg" : "auth failed.",
  "error_type" : "AUTH_FAILED"
}
```

Status code: 403

Forbidden: The request is rejected. The server has received the request and understood it, but the server refuses to respond to it. The client should not repeat the request without modifications.


```
{
  "error_code" : "SVCSTG.AMS.2000051",
  "error_msg" : "auth failed.",
  "error_type" : "AUTH_FAILED"
}
```

Status code: 500

Internal Server Error: The server is able to receive the request but unable to understand the request.

```
{
  "error_code" : "APM.00000500",
  "error_msg" : "Internal Server Error",
  "trace_id" : ""
}
```

Status Codes

Status Code	Description
204	OK: The request is successful.
400	Bad Request: The request is invalid. The client should not repeat the request without modifications.
401	Unauthorized: The authentication information is incorrect or invalid.
403	Forbidden: The request is rejected. The server has received the request and understood it, but the server refuses to respond to it. The client should not repeat the request without modifications.
500	Internal Server Error: The server is able to receive the request but unable to understand the request.

Error Codes

See **Error Codes**.

4.1.5 Obtaining the Alarm Sending Result

Function

This API is used to obtain the alarm sending result.

Calling Method

For details, see **Calling APIs**.

URI

GET /v2/{project_id}/alarm-notified-histories

Table 4-38 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID obtained from IAM. Generally, a project ID contains 32 characters. Minimum: **32** Maximum: **32**

Table 4-39 Query Parameters

Parameter	Mandatory	Type	Description
event_sn	No	String	Alarm serial number.

Request Parameters

Table 4-40 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token obtained from IAM. Minimum: **1** Maximum: **40960**
Content-Type	Yes	String	Content type, which is application/json. Enumeration values: • **application/json**

Response Parameters

Status code: 200

Table 4-41 Response body parameters

Parameter	Type	Description
notified_histories	Array of **NotifiedHistoriesResult** objects	Historical notification list.

Table 4-42 NotifiedHistoriesResult

Parameter	Type	Description
event_sn	String	Alarm serial number. Minimum: **19** Maximum: **19**
notifications	Array of **Notifications** objects	Notification result. Array Length: **0 - 100**

Table 4-43 Notifications

Parameter	Type	Description
action_rule	String	Alarm action rule name. Minimum: **1** Maximum: **100**
notifier_channel	String	Notification type. SMN: Simple Message Notification. Enumeration values: • **SMN**
smn_channel	**SmnResponse** object	Notification result details.

Table 4-44 SmnResponse

Parameter	Type	Description
sent_time	Long	Sending time. Minimum: **0** Maximum: **9999999999**
smn_notified_history	Array of **SmnInfo** objects	Content of a notification. Array Length: **1 - 100**
smn_request_id	String	ID for requesting SMN. Minimum: **32** Maximum: **32**
smn_response_body	String	Information returned after the SMN service is invoked. Minimum: **0** Maximum: **1024**

Parameter	Type	Description
smn_response_code	String	HTTP status code returned after the SMN service is invoked. Minimum: **3** Maximum: **3**
smn_topic	String	SMN topic. Minimum: **1** Maximum: **100**

Table 4-45 SmnInfo

Parameter	Type	Description
smn_notified_content	String	SMN message content. Minimum: **1** Maximum: **9999999**
smn_subscription_status	Integer	SMN subscription status. Minimum: **1** Maximum: **1**
smn_subscription_type	String	SMN subscription type. Minimum: **1** Maximum: **100**

Status code: 401

Table 4-46 Response body parameters

Parameter	Type	Description
error_code	String	Error code. Minimum: **12** Maximum: **12**
error_msg	String	Error message. Minimum: **0** Maximum: **1024**
error_type	String	Error type. Minimum: **0** Maximum: **128**

Parameter	Type	Description
trace_id	String	Request ID. Minimum: **32** Maximum: **32**

Status code: 403

Table 4-47 Response body parameters

Parameter	Type	Description
error_code	String	Error code. Minimum: **12** Maximum: **12**
error_msg	String	Error message. Minimum: **0** Maximum: **1024**
error_type	String	Error type. Minimum: **0** Maximum: **128**
trace_id	String	Request ID. Minimum: **32** Maximum: **32**

Status code: 500

Table 4-48 Response body parameters

Parameter	Type	Description
error_code	String	Response code. Minimum: **13** Maximum: **13**
error_msg	String	Response message. Minimum: **1** Maximum: **100**
trace_id	String	Response ID. Minimum: **12** Maximum: **12**

Example Requests

Obtain the sending result of the alarm whose serial number is 1044686593798963201.

```
https://{Endpoint}/v2/{project_id}/alarm-notified-histories?event_sn=1044686593798963201
```

Example Responses

Status code: 200

OK: The request is successful.


```
{
  "notified_histories" : [ {
    "event_sn" : "1044686593798963201",
    "notifications" : [ {
      "action_rule" : "lhy_alarm_action_test01",
      "notifier_channel" : "SMN",
      "smn_channel" : {
        "sent_time" : 1669114269797,
        "smn_notified_history" : [ {
          "smn_notified_content" : "<style>    span {        display: inline-block;        float: left;        font-size:
14px;    }    b {        display: inline-block;        float: left;        color: #252B3A;        font-size: 14px    }</
style><table border=\"0\" cellpadding=\"0\" cellspacing=\"0\"       style=\"font-
family:HuaweiFont,Helvetica,Arial,PingFangSC-Regular,Hiragino Sans GB;border-spacing:0px 14px;font-
size:14px;padding-left: 30px;line-height:25px;\">    <thead>    <tr style=\"font-size:14px;\">        <td colspan=
\"2\" style=\"line-height:28px;color:#6e6e6e;font-size:14px\">            <b>Dear </b>
<b>users</b>            <b> </b>        </td>    </tr>    </thead>    <tr>        <td colspan=\"2\">
<span>1 notification has been </span>            <b>generated</b>            <span> in region ***</
span>            <b> based on action rule lhy_alarm_action_test01.</b>            <span></span>
<span></span>                                <span><span>The alarm rule is </
span><b>lhy_test_001</b></span>            <span>. For more information, go to the AOM console.</
span>            <br>            <br>        </td>    </tr>    <tr style=\"font-size:14px;\">        <td colspan=
\"2\">            <p style=\"margin-bottom: -20px; margin-top: -26px;\">                <span style=
\"color:#252B3A;line-height:24px\">Here are the details.</span>            </p>        </td>    </tr>
<td><div>Account: kaifatest;<br>Notification Type: alarm;<br>CAS Application Name:
app-1;<br>Notification Type: NA;<br>Severity: Critical;<br>Name: lhy_test_001;<br>Occurred: 2022-11-22
18:51:05 GMT+08:00;<br>Source: AOM;<br>Resource Type: Application;<br>Resource Identifier:
<br>  casApplicationID: 2d216a2b-9a58-452e-9a82-
fc0c7cbcd322;<br>  casApplicationName: app-1;<br>Possible Cause: If the specified metric
value crosses the threshold and the alarm severity is \\\"critical\\\", an alarm is triggered.;<br>Link: https://
console.xxx/aom/alarmlist;<br>Additional Info: The threshold rule lhy_test_001 status changes from \\\"init\\
\" to \\\"alarm\\\". The value of \\\"cpuCoreLimit\\\" is \\\"0.250\\\" and meets the threshold criterion \\
\">=0\\\"<br>Suggestion: NA;<br><div/></td>  </table>",
          "smn_subscription_status" : 1,
          "smn_subscription_type" : "email"
        }, {
          "smn_notified_content" : "[AOM][Critical_alarm_generated] \nAlert Name: lhy_test_001;\nCAS
Application Name: app-1;\nOccurrence Time: 2022-11-22 18:51:05 GMT+08:00;\nLink: https://
console.xxx/aom/alarmlist;\nAlert Content: The threshold rule lhy_test_001 status changes from \"init\" to
\"alarm\". The value of \"cpuCoreLimit\" is \"0.250\" and meets the threshold criterion \">=0\".;\nThis
message is configured in an AOM alarm rule by kaifatest. For more information, go to the AOM console.\",",
          "smn_subscription_status" : 0,
          "smn_subscription_type" : "sms"
        }, {
          "smn_notified_content" : "[AOM][Critical_alarm_generated] \nAlert Name: lhy_test_001;\nCAS
Application Name: app-1;\nOccurrence Time: 2022-11-22 18:51:05 GMT+08:00;\nLink: https://
console.xxx/aom/alarmlist;\nAlert Content: The threshold rule lhy_test_001 status changes from \"init\" to
\"alarm\". The value of \"cpuCoreLimit\" is \"0.250\" and meets the threshold criterion \">=0\".;\nThis
message is configured in an AOM alarm rule by kaifatest. For more information, go to the AOM console.\",",
          "smn_subscription_status" : 0,
          "smn_subscription_type" : "sms"
        } ],
        "smn_request_id" : "600bfa7447da48068312bba0fb2b3afa",
        "smn_response_body" : "{\"message_id\":\"b5db3a3419b84cc29d438a7dba336c20\",\"request_id
\":\"600bfa7447da48068312bba0fb2b3afa\"}",
        "smn_response_code" : "200",
```



```
      "smn_topic" : "lhy_test01"
    }
   } ]
  } ]
}
```

Status code: 401

Unauthorized: The authentication information is incorrect or invalid.

```
{
  "error_code" : "AOM.0403",
  "error_msg" : "auth failed.",
  "error_type" : "AUTH_FAILED",
  "trace_id" : null
}
```

Status code: 403

Forbidden: The request is rejected. The server has received the request and understood it, but the server refuses to respond to it. The client should not repeat the request without modifications.

```
{
  "error_code" : "AOM.0403",
  "error_msg" : "auth failed.",
  "error_type" : "AUTH_FAILED",
  "trace_id" : null
}
```

Status code: 500

Internal Server Error: The server is able to receive the request but unable to understand the request.

```
{
  "error_code" : "APM.00000500",
  "error_msg" : "Internal Server Error",
  "trace_id" : ""
}
```

Status Codes

Status Code	Description
200	OK: The request is successful.
401	Unauthorized: The authentication information is incorrect or invalid.
403	Forbidden: The request is rejected. The server has received the request and understood it, but the server refuses to respond to it. The client should not repeat the request without modifications.
500	Internal Server Error: The server is able to receive the request but unable to understand the request.

Error Codes

See **Error Codes**.

4.1.6 Deleting a Silence Rule

Function

This API is used to delete a silence rule.

Calling Method

For details, see **Calling APIs**.

URI

DELETE /v2/{project_id}/alert/mute-rules

Table 4-49 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID obtained from IAM. Generally, a project ID contains 32 characters. Minimum: **32** Maximum: **32**

Request Parameters

Table 4-50 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token obtained from IAM. Minimum: **1** Maximum: **40960**
Content-Type	Yes	String	Content type, which is application/json. Enumeration values: • **application/json**

Table 4-51 Request body parameters

Parameter	Mandatory	Type	Description
[items]	Yes	Array of **DeleteMuteRuleName** objects	Name of the rule to be deleted.

Table 4-52 DeleteMuteRuleName

Parameter	Mandatory	Type	Description
name	Yes	String	Name of the silence rule to be deleted. Minimum: **1** Maximum: **100**

Response Parameters

Status code: 400

Table 4-53 Response body parameters

Parameter	Type	Description
error_code	String	Error code. Minimum: **12** Maximum: **12**
error_msg	String	Error message. Minimum: **0** Maximum: **1024**
error_type	String	Error type. Minimum: **0** Maximum: **128**
trace_id	String	Request ID. Minimum: **32** Maximum: **32**

Status code: 401

Table 4-54 Response body parameters

Parameter	Type	Description
error_code	String	Error code. Minimum: **12** Maximum: **12**
error_msg	String	Error message. Minimum: **0** Maximum: **1024**
error_type	String	Error type. Minimum: **0** Maximum: **128**
trace_id	String	Request ID. Minimum: **32** Maximum: **32**

Status code: 403

Table 4-55 Response body parameters

Parameter	Type	Description
error_code	String	Error code. Minimum: **12** Maximum: **12**
error_msg	String	Error message. Minimum: **0** Maximum: **1024**
error_type	String	Error type. Minimum: **0** Maximum: **128**
trace_id	String	Request ID. Minimum: **32** Maximum: **32**

Status code: 500

Table 4-56 Response body parameters

Parameter	Type	Description
error_code	String	Response code. Minimum: **13** Maximum: **13**
error_msg	String	Response message. Minimum: **1** Maximum: **100**
trace_id	String	Response ID. Minimum: **12** Maximum: **12**

Example Requests

Delete silent rule "1112222".

```
https://{Endpoint}/v2/{project_id}/alert/mute-rules

[ {
  "name" : "1112222"
} ]
```

Example Responses

Status code: 400

Bad Request: The request is invalid. The client should not repeat the request without modifications.

```
{
  "error_code" : "AOM.08015002",
  "error_msg" : "the muteName is not exist",
  "error_type" : "PARAM_INVALID",
  "trace_id" : ""
}
```

Status code: 401

Unauthorized: The authentication information is incorrect or invalid.

```
{
  "error_code" : "AOM.0403",
  "error_msg" : "auth failed.",
  "error_type" : "AUTH_FAILED",
  "trace_id" : null
}
```

Status code: 403

Forbidden: The request is rejected. The server has received the request and understood it, but the server refuses to respond to it. The client should not repeat the request without modifications.

```
{
  "error_code" : "AOM.0403",
```



```
  "error_msg" : "auth failed.",
  "error_type" : "AUTH_FAILED",
  "trace_id" : null
}
```

Status code: 500

Internal Server Error: The server is able to receive the request but unable to understand the request.

```
{
  "error_code" : "AOM.08001500",
  "error_message" : "internal server error",
  "error_type" : "INTERNAL_SERVER_ERROR",
  "trace_id" : ""
}
```

Status Codes

Status Code	Description
204	OK: The request is successful.
400	Bad Request: The request is invalid. The client should not repeat the request without modifications.
401	Unauthorized: The authentication information is incorrect or invalid.
403	Forbidden: The request is rejected. The server has received the request and understood it, but the server refuses to respond to it. The client should not repeat the request without modifications.
500	Internal Server Error: The server is able to receive the request but unable to understand the request.

Error Codes

See **Error Codes**.

4.1.7 Adding a Silence Rule

Function

This API is used to add a silence rule.

Calling Method

For details, see **Calling APIs**.

URI

POST /v2/{project_id}/alert/mute-rules

Table 4-57 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID obtained from IAM. Generally, a project ID contains 32 characters. Minimum: **32** Maximum: **32**

Request Parameters

Table 4-58 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token obtained from IAM. Minimum: **1** Maximum: **40960**
Content-Type	Yes	String	Content type, which is application/json. Enumeration values: • **application/json**

Table 4-59 Request body parameters

Parameter	Mandatory	Type	Description
create_time	No	Long	Creation time. Minimum: **0** Maximum: **9999999999999**
desc	No	String	Rule description. Minimum: **0** Maximum: **1024**
match	Yes	Array<Array< **Match**>>	Match condition of the rule. Up to 10 serial or parallel conditions can be created. Array Length: **1 - 10**
mute_config	Yes	**MuteConfig** object	Time when the rule takes effect.

Parameter	Mandatory	Type	Description
name	Yes	String	Rule name. Enter a maximum of 100 characters and do not start or end with an underscore (_). Only letters, digits, and underscores are allowed. Minimum: **1** Maximum: **100**
timezone	Yes	String	Time zone. Minimum: **1** Maximum: **32**
update_time	No	Long	Modification time. Minimum: **0** Maximum: **9999999999999**
user_id	No	String	User ID. Minimum: **32** Maximum: **32**

Table 4-60 Match

Parameter	Mandatory	Type	Description
key	Yes	String	Key specified in the metadata for matching. Minimum: **1** Maximum: **128**
operate	Yes	String	Match mode. EXIST: Exist. REGEX: Regular expression. EQUALS: Equal to. Minimum: **1** Maximum: **100** Enumeration values: • **EQUALS** • **REGEX** • **EXIST**

Parameter	Mandatory	Type	Description
value	No	Array of strings	Value corresponding to the key. If operate is set to EXIST, this parameter is left empty. Minimum: **1** Maximum: **256** Array Length: **0 - 5**

Table 4-61 MuteConfig

Parameter	Mandatory	Type	Description
ends_at	No	Long	End time of the silence rule. Minimum: **0** Maximum: **999999999**
scope	No	Array of integers	When type is set to WEEKLY or MONTHLY, scope cannot be empty. Minimum: **0** Maximum: **31** Array Length: **1 - 100**
starts_at	Yes	Long	Start time of the silence rule. Minimum: **0** Maximum: **999999999**
type	Yes	String	Type of the time for the silence rule to take effect. FIXED: Fixed time. DAILY: Certain time every day. WEEKLY: Certain time every week. MONTHLY: Certain time every month. Minimum: **1** Maximum: **100** Enumeration values: • **FIXED** • **DAILY** • **WEEKLY** • **MONTHLY**

Response Parameters

Status code: 400

Table 4-62 Response body parameters

Parameter	Type	Description
error_code	String	Error code. Minimum: **12** Maximum: **12**
error_msg	String	Error message. Minimum: **0** Maximum: **1024**
error_type	String	Error type. Minimum: **0** Maximum: **128**
trace_id	String	Request ID. Minimum: **32** Maximum: **32**

Status code: 401

Table 4-63 Response body parameters

Parameter	Type	Description
error_code	String	Error code. Minimum: **12** Maximum: **12**
error_msg	String	Error message. Minimum: **0** Maximum: **1024**
error_type	String	Error type. Minimum: **0** Maximum: **128**
trace_id	String	Request ID. Minimum: **32** Maximum: **32**

Status code: 403

Table 4-64 Response body parameters

Parameter	Type	Description
error_code	String	Error code. Minimum: **12** Maximum: **12**
error_msg	String	Error message. Minimum: **0** Maximum: **1024**
error_type	String	Error type. Minimum: **0** Maximum: **128**
trace_id	String	Request ID. Minimum: **32** Maximum: **32**

Status code: 500

Table 4-65 Response body parameters

Parameter	Type	Description
error_code	String	Response code. Minimum: **13** Maximum: **13**
error_msg	String	Response message. Minimum: **1** Maximum: **100**
trace_id	String	Response ID. Minimum: **12** Maximum: **12**

Example Requests

Add a silence rule whose name is "32255" and user ID is "2xxxxxxxxxxxxxxxxxxxxxxxxxcf".

```
https://{Endpoint}/v2/{project_id}/alert/mute-rules

{
  "create_time" : 1668147671966,
  "desc" : "",
  "match" : [ [ {
```



```
    "key" : "event_severity",
    "operate" : "EQUALS",
    "value" : [ "Info" ]
  } ] ],
  "mute_config" : {
    "ends_at" : 86399,
    "scope" : [ ],
    "starts_at" : 0,
    "type" : "DAILY"
  },
  "name" : "32255",
  "timezone" : "xxx",
  "update_time" : 1668147671966,
  "user_id" : "2xxxxxxxxxxxxxxxxxxxxxxxxxcf"
}
```

Example Responses

Status code: 400

Bad Request: Invalid request. The client should not repeat the request without modifications.

```
{
  "error_code" : "AOM.08011001",
  "error_msg" : "the muteName is exist",
  "error_type" : "PARAM_INVALID",
  "trace_id" : ""
}
```

Status code: 401

Unauthorized: The authentication information is incorrect or invalid.

```
{
  "error_code" : "AOM.0403",
  "error_msg" : "auth failed.",
  "error_type" : "AUTH_FAILED",
  "trace_id" : null
}
```

Status code: 403

Forbidden: The request is rejected. The server has received the request and understood it, but the server refuses to respond to it. The client should not repeat the request without modifications.

```
{
  "error_code" : "AOM.0403",
  "error_msg" : "auth failed.",
  "error_type" : "AUTH_FAILED",
  "trace_id" : null
}
```

Status code: 500

Internal Server Error: The server is able to receive the request but unable to understand the request.

```
{
  "error_code" : "APM.00000500",
  "error_msg" : "Internal Server Error",
  "trace_id" : ""
}
```


Status Codes

Status Code	Description
204	OK: Operation successful.
400	Bad Request: Invalid request. The client should not repeat the request without modifications.
401	Unauthorized: The authentication information is incorrect or invalid.
403	Forbidden: The request is rejected. The server has received the request and understood it, but the server refuses to respond to it. The client should not repeat the request without modifications.
500	Internal Server Error: The server is able to receive the request but unable to understand the request.

Error Codes

See **Error Codes**.

4.1.8 Modifying a Silence Rule

Function

This API is used to modify a silence rule.

Calling Method

For details, see **Calling APIs**.

URI

PUT /v2/{project_id}/alert/mute-rules

Table 4-66 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID obtained from IAM. Generally, a project ID contains 32 characters. Minimum: **32** Maximum: **32**

Request Parameters

Table 4-67 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token obtained from IAM. Minimum: **1** Maximum: **40960**
Content-Type	Yes	String	Content type, which is application/json. Enumeration values: • **application/json**

Table 4-68 Request body parameters

Parameter	Mandatory	Type	Description
create_time	No	Long	Creation time. Minimum: **0** Maximum: **9999999999999**
desc	No	String	Rule description. Minimum: **0** Maximum: **1024**
match	Yes	Array<Array<**Match**>>	Match condition of the rule. Up to 10 serial or parallel conditions can be created. Array Length: **1 - 10**
mute_config	Yes	**MuteConfig** object	Time when the rule takes effect.
name	Yes	String	Rule name. Enter a maximum of 100 characters and do not start or end with an underscore (_). Only letters, digits, and underscores are allowed. Minimum: **1** Maximum: **100**
timezone	Yes	String	Time zone. Minimum: **1** Maximum: **32**

Parameter	Mandatory	Type	Description
update_time	No	Long	Modification time. Minimum: **0** Maximum: **9999999999999**
user_id	No	String	User ID. Minimum: **32** Maximum: **32**

Table 4-69 Match

Parameter	Mandatory	Type	Description
key	Yes	String	Key specified in the metadata for matching. Minimum: **1** Maximum: **128**
operate	Yes	String	Match mode. EXIST: Exist. REGEX: Regular expression. EQUALS: Equal to. Minimum: **1** Maximum: **100** Enumeration values: • **EQUALS** • **REGEX** • **EXIST**
value	No	Array of strings	Value corresponding to the key. If operate is set to EXIST, this parameter is left empty. Minimum: **1** Maximum: **256** Array Length: **0 - 5**

Table 4-70 MuteConfig

Parameter	Mandatory	Type	Description
ends_at	No	Long	End time of the silence rule. Minimum: **0** Maximum: **999999999**

Parameter	Mandatory	Type	Description
scope	No	Array of integers	When type is set to WEEKLY or MONTHLY, scope cannot be empty. Minimum: **0** Maximum: **31** Array Length: **1 - 100**
starts_at	Yes	Long	Start time of the silence rule. Minimum: **0** Maximum: **999999999**
type	Yes	String	Type of the time for the silence rule to take effect. FIXED: Fixed time. DAILY: Certain time every day. WEEKLY: Certain time every week. MONTHLY: Certain time every month. Minimum: **1** Maximum: **100** Enumeration values: • **FIXED** • **DAILY** • **WEEKLY** • **MONTHLY**

Response Parameters

Status code: 400

Table 4-71 Response body parameters

Parameter	Type	Description
error_code	String	Error code. Minimum: **12** Maximum: **12**
error_msg	String	Error message. Minimum: **0** Maximum: **1024**

Parameter	Type	Description
error_type	String	Error type. Minimum: **0** Maximum: **128**
trace_id	String	Request ID. Minimum: **32** Maximum: **32**

Status code: 401

Table 4-72 Response body parameters

Parameter	Type	Description
error_code	String	Error code. Minimum: **12** Maximum: **12**
error_msg	String	Error message. Minimum: **0** Maximum: **1024**
error_type	String	Error type. Minimum: **0** Maximum: **128**
trace_id	String	Request ID. Minimum: **32** Maximum: **32**

Status code: 403

Table 4-73 Response body parameters

Parameter	Type	Description
error_code	String	Error code. Minimum: **12** Maximum: **12**
error_msg	String	Error message. Minimum: **0** Maximum: **1024**

Parameter	Type	Description
error_type	String	Error type. Minimum: **0** Maximum: **128**
trace_id	String	Request ID. Minimum: **32** Maximum: **32**

Status code: 500

Table 4-74 Response body parameters

Parameter	Type	Description
error_code	String	Response code. Minimum: **13** Maximum: **13**
error_msg	String	Response message. Minimum: **1** Maximum: **100**
trace_id	String	Response ID. Minimum: **12** Maximum: **12**

Example Requests

Modify a silence rule whose name is "32255", time zone is "xxx", and user ID is "2xxxxxxxxxxxxxxxxxxxxxxxxxxcf".

```
https://{endpoint}/v2/{project_id}/alert/mute-rules

{
  "create_time" : 1668147671966,
  "desc" : "",
  "match" : [ [ {
    "key" : "event_severity",
    "operate" : "EQUALS",
    "value" : [ "Info" ]
  } ] ],
  "mute_config" : {
    "ends_at" : 86399,
    "scope" : [ ],
    "starts_at" : 0,
    "type" : "DAILY"
  },
  "name" : "32255",
  "timezone" : "xxx",
  "update_time" : 1668147671966,
```



```
  "user_id" : "2xxxxxxxxxxxxxxxxxxxxxxxxxcf"
}
```

Example Responses

Status code: 400

Bad Request: The request is invalid. The client should not repeat the request without modifications.

```
{
  "error_code" : "AOM.08012003",
  "error_msg" : "request insertParma probably has error",
  "error_type" : "PARAM_INVALID",
  "trace_id" : ""
}
```

Status code: 401

Unauthorized: The authentication information is incorrect or invalid.

```
{
  "error_code" : "AOM.0403",
  "error_msg" : "auth failed.",
  "error_type" : "AUTH_FAILED",
  "trace_id" : null
}
```

Status code: 403

Forbidden: The request is rejected. The server has received the request and understood it, but the server refuses to respond to it. The client should not repeat the request without modifications.

```
{
  "error_code" : "AOM.0403",
  "error_msg" : "auth failed.",
  "error_type" : "AUTH_FAILED",
  "trace_id" : null
}
```

Status code: 500

Internal Server Error: The server is able to receive the request but unable to understand the request.

```
{
  "error_code" : "APM.00000500",
  "error_msg" : "Internal Server Error",
  "trace_id" : ""
}
```

Status Codes

Status Code	Description
204	OK: The request is successful.
400	Bad Request: The request is invalid. The client should not repeat the request without modifications.
401	Unauthorized: The authentication information is incorrect or invalid.

Status Code	Description
403	Forbidden: The request is rejected. The server has received the request and understood it, but the server refuses to respond to it. The client should not repeat the request without modifications.
500	Internal Server Error: The server is able to receive the request but unable to understand the request.

Error Codes

See **Error Codes**.

4.1.9 Obtaining the Silence Rule List

Function

This API is used to obtain the silence rule list.

Calling Method

For details, see **Calling APIs**.

URI

GET /v2/{project_id}/alert/mute-rules

Table 4-75 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID obtained from IAM. Generally, a project ID contains 32 characters. Minimum: **32** Maximum: **32**

Request Parameters

Table 4-76 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token obtained from IAM. Minimum: **1** Maximum: **40960**
Content-Type	Yes	String	Content type, which is application/json. Enumeration values: • **application/json**

Response Parameters

Status code: 200

Table 4-77 Response body parameters

Parameter	Type	Description
[items]	Array of **MuteRule** objects	OK: The request is successful.

Table 4-78 MuteRule

Parameter	Type	Description
create_time	Long	Creation time. Minimum: **0** Maximum: **9999999999999**
desc	String	Rule description. Minimum: **0** Maximum: **1024**
match	Array<Array< **Match**>>	Match condition of the rule. Up to 10 serial or parallel conditions can be created. Array Length: **1 - 10**
mute_config	**MuteConfig** object	Time when the rule takes effect.

Parameter	Type	Description
name	String	Rule name. Enter a maximum of 100 characters and do not start or end with an underscore (_). Only letters, digits, and underscores are allowed. Minimum: **1** Maximum: **100**
timezone	String	Time zone. Minimum: **1** Maximum: **32**
update_time	Long	Modification time. Minimum: **0** Maximum: **9999999999999**
user_id	String	User ID. Minimum: **32** Maximum: **32**

Table 4-79 Match

Parameter	Type	Description
key	String	Key specified in the metadata for matching. Minimum: **1** Maximum: **128**
operate	String	Match mode. EXIST: Exist. REGEX: Regular expression. EQUALS: Equal to. Minimum: **1** Maximum: **100** Enumeration values: • **EQUALS** • **REGEX** • **EXIST**
value	Array of strings	Value corresponding to the key. If operate is set to EXIST, this parameter is left empty. Minimum: **1** Maximum: **256** Array Length: **0 - 5**

Table 4-80 MuteConfig

Parameter	Type	Description
ends_at	Long	End time of the silence rule. Minimum: **0** Maximum: **999999999**
scope	Array of integers	When type is set to WEEKLY or MONTHLY, scope cannot be empty. Minimum: **0** Maximum: **31** Array Length: **1 - 100**
starts_at	Long	Start time of the silence rule. Minimum: **0** Maximum: **999999999**
type	String	Type of the time for the silence rule to take effect. FIXED: Fixed time. DAILY: Certain time every day. WEEKLY: Certain time every week. MONTHLY: Certain time every month. Minimum: **1** Maximum: **100** Enumeration values: • **FIXED** • **DAILY** • **WEEKLY** • **MONTHLY**

Status code: 401

Table 4-81 Response body parameters

Parameter	Type	Description
error_code	String	Error code. Minimum: **12** Maximum: **12**
error_msg	String	Error message. Minimum: **0** Maximum: **1024**

Parameter	Type	Description
error_type	String	Error type. Minimum: **0** Maximum: **128**
trace_id	String	Request ID. Minimum: **32** Maximum: **32**

Status code: 403

Table 4-82 Response body parameters

Parameter	Type	Description
error_code	String	Error code. Minimum: **12** Maximum: **12**
error_msg	String	Error message. Minimum: **0** Maximum: **1024**
error_type	String	Error type. Minimum: **0** Maximum: **128**
trace_id	String	Request ID. Minimum: **32** Maximum: **32**

Status code: 500

Table 4-83 Response body parameters

Parameter	Type	Description
error_code	String	Response code. Minimum: **13** Maximum: **13**
error_msg	String	Response message. Minimum: **1** Maximum: **100**

Parameter	Type	Description
trace_id	String	Response ID. Minimum: **12** Maximum: **12**

Example Requests

Obtain the silence rule list.

```
https://{Endpoint}/v2/{project_id}/alert/mute-rules
```

Example Responses

Status code: 200

OK: The request is successful.

```
[ {
  "create_time" : 1668147671966,
  "desc" : "",
  "match" : [ [ {
    "key" : "event_severity",
    "operate" : "EQUALS",
    "value" : [ "Info" ]
  } ] ],
  "mute_config" : {
    "ends_at" : 86399,
    "scope" : [ ],
    "starts_at" : 0,
    "type" : "DAILY"
  },
  "name" : "32255",
  "timezone" : "xxx",
  "update_time" : 1668147671966,
  "user_id" : "2a473356cca5487f8373be891bffc1cf"
} ]
```

Status code: 401

Unauthorized: The authentication information is incorrect or invalid.

```
{
  "error_code" : "AOM.0403",
  "error_msg" : "auth failed.",
  "error_type" : "AUTH_FAILED",
  "trace_id" : null
}
```

Status code: 403

Forbidden: The request is rejected. The server has received the request and understood it, but the server refuses to respond to it. The client should not repeat the request without modifications.

```
{
  "error_code" : "AOM.0403",
  "error_msg" : "auth failed.",
  "error_type" : "AUTH_FAILED",
  "trace_id" : null
}
```


Status code: 500

Internal Server Error: The server is able to receive the request but unable to understand the request.

```
{
  "error_code" : "APM.00000500",
  "error_msg" : "Internal Server Error",
  "trace_id" : ""
}
```

Status Codes

Status Code	Description
200	OK: The request is successful.
401	Unauthorized: The authentication information is incorrect or invalid.
403	Forbidden: The request is rejected. The server has received the request and understood it, but the server refuses to respond to it. The client should not repeat the request without modifications.
500	Internal Server Error: The server is able to receive the request but unable to understand the request.

Error Codes

See **Error Codes**.

4.1.10 Querying an Alarm Action Rule Based on Rule Name

Function

This API is used to query an alarm action rule based on the rule name.

Calling Method

For details, see **Calling APIs**.

URI

GET /v2/{project_id}/alert/action-rules/{rule_name}

Table 4-84 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID obtained from IAM. Generally, a project ID contains 32 characters. Minimum: **32** Maximum: **32**
rule_name	Yes	String	Alarm rule name. Minimum: **1** Maximum: **100**

Request Parameters

Table 4-85 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token obtained from IAM. Minimum: **1** Maximum: **40960**
Content-Type	Yes	String	Content type, which is application/json. Enumeration values: • **application/json**

Response Parameters

Status code: 200

Table 4-86 Response body parameters

Parameter	Type	Description
rule_name	String	Rule name. Enter a maximum of 100 characters and do not start or end with a special character. Only letters, digits, and underscores (_) are allowed. Minimum: **1** Maximum: **100**

Parameter	Type	Description
project_id	String	Project ID. Minimum: **32** Maximum: **32**
user_name	String	Member account name. Minimum: **1** Maximum: **100**
desc	String	Rule description. Enter a maximum of 1024 characters and do not start or end with an underscore (_). Only digits, letters, underscores (_), asterisk (*), and spaces are allowed. Minimum: **0** Maximum: **1024**
type	String	Action type. Default: Notification. Minimum: **1** Maximum: **1** Enumeration values: • **1** • **2**
notification_template	String	Message template. Minimum: **1** Maximum: **100**
create_time	Long	Creation time. Minimum: **0** Maximum: **9999999999999**
update_time	Long	Modification time Minimum: **0** Maximum: **9999999999999**
time_zone	String	Time zone. Minimum: **1** Maximum: **100**
smn_topics	Array of **SmnTopics** objects	SMN topic. The total number of topics cannot exceed 5. Array Length: **1 - 5**

Table 4-87 SmnTopics

Parameter	Type	Description
display_name	String	Topic display name, which will be the name of an email sender. Max.: 192 bytes. This parameter is left blank by default. Minimum: **1** Maximum: **64**
name	String	Name of the topic. Enter 1 to 255 characters starting with a letter or digit. Only letters, digits, hyphens (-), and underscores (_) are allowed. Minimum: **1** Maximum: **255**
push_policy	Integer	SMN message push policy. Options: 0 and 1. Minimum: **0** Maximum: **1**
status	Integer	Status of the topic subscriber. 0: The topic has been deleted or the subscription list of this topic is empty. 1: The subscription object is in the subscribed state. 2: The subscription object is in the unsubscribed or canceled state. Enumeration values: • **0** • **1** • **2**
topic_urn	String	Unique resource identifier of the topic. Minimum: **1** Maximum: **100**

Status code: 400

Table 4-88 Response body parameters

Parameter	Type	Description
error_code	String	Response code. Minimum: **13** Maximum: **13**
error_msg	String	Response message. Minimum: **1** Maximum: **100**

Parameter	Type	Description
trace_id	String	Response ID. Minimum: **12** Maximum: **12**

Status code: 401

Table 4-89 Response body parameters

Parameter	Type	Description
error_code	String	Error code. Minimum: **12** Maximum: **12**
error_msg	String	Error message. Minimum: **0** Maximum: **1024**
error_type	String	Error type. Minimum: **0** Maximum: **128**
trace_id	String	Request ID. Minimum: **32** Maximum: **32**

Status code: 403

Table 4-90 Response body parameters

Parameter	Type	Description
error_code	String	Error code. Minimum: **12** Maximum: **12**
error_msg	String	Error message. Minimum: **0** Maximum: **1024**
error_type	String	Error type. Minimum: **0** Maximum: **128**

Parameter	Type	Description
trace_id	String	Request ID. Minimum: **32** Maximum: **32**

Status code: 500

Table 4-91 Response body parameters

Parameter	Type	Description
error_code	String	Response code. Minimum: **13** Maximum: **13**
error_msg	String	Response message. Minimum: **1** Maximum: **100**
trace_id	String	Response ID. Minimum: **12** Maximum: **12**

Example Requests

Query the details of the alarm action rule named 1112222.

```
https://{Endpoint}/v2/{project_id}/alert/action-rules/1112222
```

Example Responses

Status code: 200

OK: The request is successful.

```
{
  "create_time" : 1665991889597,
  "notification_template" : "aom.built-in.template.zh",
  "project_id" : "2xxxxxxxxxxxxxxxxxxxxxxf",
  "rule_name" : "1112222",
  "smn_topics" : [ {
    "display_name" : "",
    "name" : "gxxxxxt",
    "push_policy" : 0,
    "status" : 0,
    "topic_urn" : "urn:smn:xxx:2xxxxxxxxxxxxxxxxxxxxxxf:gxxxxxt"
  } ],
  "time_zone" : "xxx",
  "type" : "1",
  "update_time" : 1665991889597,
  "user_name" : "kxxxxxxxt"
}
```


Status code: 400

Bad Request: Invalid request. The client should not repeat the request without modifications.

```
{
  "error_code" : "AOM.08001001",
  "error_msg" : "bad request",
  "trace_id" : ""
}
```

Status code: 401

Unauthorized: The authentication information is incorrect or invalid.

```
{
  "error_code" : "AOM.0403",
  "error_msg" : "auth failed.",
  "error_type" : "AUTH_FAILED",
  "trace_id" : null
}
```

Status code: 403

Forbidden: The request is rejected. The server has received the request and understood it, but the server refuses to respond to it. The client should not repeat the request without modifications.

```
{
  "error_code" : "AOM.0403",
  "error_msg" : "auth failed.",
  "error_type" : "AUTH_FAILED",
  "trace_id" : null
}
```

Status code: 500

Internal Server Error: The server is able to receive the request but unable to understand the request.

```
{
  "error_code" : "APM.00000500",
  "error_msg" : "Internal Server Error",
  "trace_id" : ""
}
```

Status Codes

Status Code	Description
200	OK: The request is successful.
400	Bad Request: Invalid request. The client should not repeat the request without modifications.
401	Unauthorized: The authentication information is incorrect or invalid.
403	Forbidden: The request is rejected. The server has received the request and understood it, but the server refuses to respond to it. The client should not repeat the request without modifications.

Status Code	Description
500	Internal Server Error: The server is able to receive the request but unable to understand the request.

Error Codes

See **Error Codes**.

4.1.11 Adding an Alarm Action Rule

Function

This API is used to add an alarm action rule.

Calling Method

For details, see **Calling APIs**.

URI

POST /v2/{project_id}/alert/action-rules

Table 4-92 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID obtained from IAM. Generally, a project ID contains 32 characters. Minimum: **32** Maximum: **32**

Request Parameters

Table 4-93 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token obtained from IAM. Minimum: **1** Maximum: **40960**

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Content type, which is application/json. Enumeration values: • **application/json**

Table 4-94 Request body parameters

Parameter	Mandatory	Type	Description
rule_name	Yes	String	Rule name. Enter a maximum of 100 characters and do not start or end with a special character. Only letters, digits, and underscores (_) are allowed. Minimum: **1** Maximum: **100**
project_id	Yes	String	Project ID. Minimum: **32** Maximum: **32**
user_name	Yes	String	Member account name. Minimum: **1** Maximum: **100**
desc	No	String	Rule description. Enter a maximum of 1024 characters and do not start or end with an underscore (_). Only digits, letters, underscores (_), asterisk (*), and spaces are allowed. Minimum: **0** Maximum: **1024**
type	Yes	String	Action type. Default: Notification. Minimum: **1** Maximum: **1** Enumeration values: • **1** • **2**

Parameter	Mandatory	Type	Description
notification_template	Yes	String	Message template. Minimum: **1** Maximum: **100**
create_time	No	Long	Creation time. Minimum: **0** Maximum: **9999999999999**
update_time	No	Long	Modification time Minimum: **0** Maximum: **9999999999999**
time_zone	No	String	Time zone. Minimum: **1** Maximum: **100**
smn_topics	Yes	Array of **SmnTopics** objects	SMN topic. The total number of topics cannot exceed 5. Array Length: **1 - 5**

Table 4-95 SmnTopics

Parameter	Mandatory	Type	Description
display_name	No	String	Topic display name, which will be the name of an email sender. Max.: 192 bytes. This parameter is left blank by default. Minimum: **1** Maximum: **64**
name	Yes	String	Name of the topic. Enter 1 to 255 characters starting with a letter or digit. Only letters, digits, hyphens (-), and underscores (_) are allowed. Minimum: **1** Maximum: **255**
push_policy	Yes	Integer	SMN message push policy. Options: 0 and 1. Minimum: **0** Maximum: **1**

Parameter	Mandatory	Type	Description
status	No	Integer	Status of the topic subscriber. 0: The topic has been deleted or the subscription list of this topic is empty. 1: The subscription object is in the subscribed state. 2: The subscription object is in the unsubscribed or canceled state. Enumeration values: • **0** • **1** • **2**
topic_urn	Yes	String	Unique resource identifier of the topic. Minimum: **1** Maximum: **100**

Response Parameters

Status code: 400

Table 4-96 Response body parameters

Parameter	Type	Description
error_code	String	Response code. Minimum: **13** Maximum: **13**
error_msg	String	Response message. Minimum: **1** Maximum: **100**
trace_id	String	Response ID. Minimum: **12** Maximum: **12**

Status code: 401

Table 4-97 Response body parameters

Parameter	Type	Description
error_code	String	Error code. Minimum: **12** Maximum: **12**
error_msg	String	Error message. Minimum: **0** Maximum: **1024**
error_type	String	Error type. Minimum: **0** Maximum: **128**
trace_id	String	Request ID. Minimum: **32** Maximum: **32**

Status code: 403

Table 4-98 Response body parameters

Parameter	Type	Description
error_code	String	Error code. Minimum: **12** Maximum: **12**
error_msg	String	Error message. Minimum: **0** Maximum: **1024**
error_type	String	Error type. Minimum: **0** Maximum: **128**
trace_id	String	Request ID. Minimum: **32** Maximum: **32**

Status code: 500

Table 4-99 Response body parameters

Parameter	Type	Description
error_code	String	Response code. Minimum: **13** Maximum: **13**
error_msg	String	Response message. Minimum: **1** Maximum: **100**
trace_id	String	Response ID. Minimum: **12** Maximum: **12**

Example Requests

Add an alarm action rule whose name is "66666", username is "kxxxxxxxt", user ID is "21axxxxxxxxxxxxxxxx47c", and notification template is "aom.built-in.template.en".

```
https://{Endpoint}/v2/{project_id}/alert/action-rules

{
  "desc" : "1111",
  "notification_template" : "aom.built-in.template.zh",
  "project_id" : "21axxxxxxxxxxxxxxxx47c",
  "rule_name" : "66666",
  "smn_topics" : [ {
    "display_name" : "",
    "name" : "xiaohama",
    "push_policy" : 0,
    "status" : 0,
    "topic_urn" : "urn:smn:xxx:21axxxxxxxxxxxxxxxx47c:xiaohama"
  } ],
  "type" : "1",
  "user_name" : "kxxxxxxxt",
  "time_zone" : "xxx"
}
```

Example Responses

Status code: 400

Bad Request: Invalid request. The client should not repeat the request without modifications.

```
{
  "error_code" : "AOM.08018012",
  "error_msg" : "actionRule already exists",
  "trace_id" : ""
}
```

Status code: 401

Unauthorized: The authentication information is incorrect or invalid.

```
{
  "error_code" : "AOM.0403",
```



```
  "error_msg" : "auth failed.",
  "error_type" : "AUTH_FAILED",
  "trace_id" : null
}
```

Status code: 403

Forbidden: The request is rejected. The server has received the request and understood it, but the server refuses to respond to it. The client should not repeat the request without modifications.

```
{
  "error_code" : "AOM.0403",
  "error_msg" : "auth failed.",
  "error_type" : "AUTH_FAILED",
  "trace_id" : null
}
```

Status code: 500

Internal Server Error: The server is able to receive the request but unable to understand the request.

```
{
  "error_code" : "APM.00000500",
  "error_msg" : "Internal Server Error",
  "trace_id" : ""
}
```

Status Codes

Status Code	Description
200	OK: Operation successful.
400	Bad Request: Invalid request. The client should not repeat the request without modifications.
401	Unauthorized: The authentication information is incorrect or invalid.
403	Forbidden: The request is rejected. The server has received the request and understood it, but the server refuses to respond to it. The client should not repeat the request without modifications.
500	Internal Server Error: The server is able to receive the request but unable to understand the request.

Error Codes

See **Error Codes**.

4.1.12 Deleting an Alarm Action Rule

Function

This API is used to delete an alarm action rule.

Calling Method

For details, see **Calling APIs**.

URI

DELETE /v2/{project_id}/alert/action-rules

Table 4-100 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID obtained from IAM. Generally, a project ID contains 32 characters. Minimum: **32** Maximum: **32**

Request Parameters

Table 4-101 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token obtained from IAM. Minimum: **1** Maximum: **40960**
Content-Type	Yes	String	Content type, which is application/json. Enumeration values: • **application/json**

Table 4-102 Request body parameters

Parameter	Mandatory	Type	Description
[items]	Yes	Array of strings	Name of the rule to be deleted.

Response Parameters

Status code: 400

Table 4-103 Response body parameters

Parameter	Type	Description
error_code	String	Response code. Minimum: **13** Maximum: **13**
error_msg	String	Response message. Minimum: **1** Maximum: **100**
trace_id	String	Response ID. Minimum: **12** Maximum: **12**

Status code: 401

Table 4-104 Response body parameters

Parameter	Type	Description
error_code	String	Error code. Minimum: **12** Maximum: **12**
error_msg	String	Error message. Minimum: **0** Maximum: **1024**
error_type	String	Error type. Minimum: **0** Maximum: **128**
trace_id	String	Request ID. Minimum: **32** Maximum: **32**

Status code: 403

Table 4-105 Response body parameters

Parameter	Type	Description
error_code	String	Error code. Minimum: **12** Maximum: **12**
error_msg	String	Error message. Minimum: **0** Maximum: **1024**
error_type	String	Error type. Minimum: **0** Maximum: **128**
trace_id	String	Request ID. Minimum: **32** Maximum: **32**

Status code: 500

Table 4-106 Response body parameters

Parameter	Type	Description
error_code	String	Response code. Minimum: **13** Maximum: **13**
error_msg	String	Response message. Minimum: **1** Maximum: **100**
trace_id	String	Response ID. Minimum: **12** Maximum: **12**

Example Requests

Delete alarm action rule 1112222.

```
https://{Endpoint}/v2/{project_id}/alert/action-rules

[ "1112222" ]
```

Example Responses

Status code: 400

Bad Request: The request is invalid. The client should not repeat the request without modifications.

```
{
  "error_code" : "AOM.08020006",
  "error_msg" : "The action rule does not exist",
  "trace_id" : ""
}
```

Status code: 401

Unauthorized: The authentication information is incorrect or invalid.

```
{
  "error_code" : "AOM.0403",
  "error_msg" : "auth failed.",
  "error_type" : "AUTH_FAILED",
  "trace_id" : null
}
```

Status code: 403

Forbidden: The request is rejected. The server has received the request and understood it, but the server refuses to respond to it. The client should not repeat the request without modifications.

```
{
  "error_code" : "AOM.0403",
  "error_msg" : "auth failed.",
  "error_type" : "AUTH_FAILED",
  "trace_id" : null
}
```

Status code: 500

Internal Server Error: The server is able to receive the request but unable to understand the request.

```
{
  "error_code" : "AOM.08020500",
  "error_msg" : "internal server error",
  "error_type" : "INTERNAL_SERVER_ERROR",
  "trace_id" : ""
}
```

Status Codes

Status Code	Description
204	OK: The request is successful.
400	Bad Request: The request is invalid. The client should not repeat the request without modifications.
401	Unauthorized: The authentication information is incorrect or invalid.
403	Forbidden: The request is rejected. The server has received the request and understood it, but the server refuses to respond to it. The client should not repeat the request without modifications.
500	Internal Server Error: The server is able to receive the request but unable to understand the request.

Error Codes

See **Error Codes**.

4.1.13 Modifying an Alarm Action Rule

Function

This API is used to modify an alarm action rule.

Calling Method

For details, see **Calling APIs**.

URI

PUT /v2/{project_id}/alert/action-rules

Table 4-107 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID obtained from IAM. Generally, a project ID contains 32 characters. Minimum: **32** Maximum: **32**

Request Parameters

Table 4-108 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token obtained from IAM. Minimum: **1** Maximum: **40960**
Content-Type	Yes	String	Content type, which is application/json. Enumeration values: • **application/json**

Table 4-109 Request body parameters

Parameter	Mandatory	Type	Description
rule_name	Yes	String	Rule name. Enter a maximum of 100 characters and do not start or end with a special character. Only letters, digits, and underscores (_) are allowed. Minimum: **1** Maximum: **100**
project_id	Yes	String	Project ID. Minimum: **32** Maximum: **32**
user_name	Yes	String	Member account name. Minimum: **1** Maximum: **100**
desc	No	String	Rule description. Enter a maximum of 1024 characters and do not start or end with an underscore (_). Only digits, letters, underscores (_), asterisk (*), and spaces are allowed. Minimum: **0** Maximum: **1024**
type	Yes	String	Action type. Default: Notification. Minimum: **1** Maximum: **1** Enumeration values: • **1** • **2**
notification_template	Yes	String	Message template. Minimum: **1** Maximum: **100**
create_time	No	Long	Creation time. Minimum: **0** Maximum: **9999999999999**

Parameter	Mandatory	Type	Description
update_time	No	Long	Modification time Minimum: **0** Maximum: **9999999999999**
time_zone	No	String	Time zone. Minimum: **1** Maximum: **100**
smn_topics	Yes	Array of **SmnTopics** objects	SMN topic. The total number of topics cannot exceed 5. Array Length: **1 - 5**

Table 4-110 SmnTopics

Parameter	Mandatory	Type	Description
display_name	No	String	Topic display name, which will be the name of an email sender. Max.: 192 bytes. This parameter is left blank by default. Minimum: **1** Maximum: **64**
name	Yes	String	Name of the topic. Enter 1 to 255 characters starting with a letter or digit. Only letters, digits, hyphens (-), and underscores (_) are allowed. Minimum: **1** Maximum: **255**
push_policy	Yes	Integer	SMN message push policy. Options: 0 and 1. Minimum: **0** Maximum: **1**

Parameter	Mandatory	Type	Description
status	No	Integer	Status of the topic subscriber. 0: The topic has been deleted or the subscription list of this topic is empty. 1: The subscription object is in the subscribed state. 2: The subscription object is in the unsubscribed or canceled state. Enumeration values: • **0** • **1** • **2**
topic_urn	Yes	String	Unique resource identifier of the topic. Minimum: **1** Maximum: **100**

Response Parameters

Status code: 400

Table 4-111 Response body parameters

Parameter	Type	Description
error_code	String	Response code. Minimum: **13** Maximum: **13**
error_msg	String	Response message. Minimum: **1** Maximum: **100**
trace_id	String	Response ID. Minimum: **12** Maximum: **12**

Status code: 401

Table 4-112 Response body parameters

Parameter	Type	Description
error_code	String	Error code. Minimum: **12** Maximum: **12**
error_msg	String	Error message. Minimum: **0** Maximum: **1024**
error_type	String	Error type. Minimum: **0** Maximum: **128**
trace_id	String	Request ID. Minimum: **32** Maximum: **32**

Status code: 403

Table 4-113 Response body parameters

Parameter	Type	Description
error_code	String	Error code. Minimum: **12** Maximum: **12**
error_msg	String	Error message. Minimum: **0** Maximum: **1024**
error_type	String	Error type. Minimum: **0** Maximum: **128**
trace_id	String	Request ID. Minimum: **32** Maximum: **32**

Status code: 500

Table 4-114 Response body parameters

Parameter	Type	Description
error_code	String	Response code. Minimum: **13** Maximum: **13**
error_msg	String	Response message. Minimum: **1** Maximum: **100**
trace_id	String	Response ID. Minimum: **12** Maximum: **12**

Example Requests

Modify the alarm action rule whose name is "lhy_test01" and user ID is "2xxxxxxxxxxxxxxxxxcf".

```
https://{endpoint}/v2/{project_id}/alert/action-rules

{
  "project_id" : "2xxxxxxxxxxxxxxxxxcf",
  "rule_name" : "222",
  "desc" : "222",
  "type" : "1",
  "smn_topics" : [ {
    "display_name" : "",
    "name" : "lhy_test01",
    "push_policy" : 0,
    "topic_urn" : "urn:smn:xxx:2xxxxxxxxxxxxxxxxxcf:lhy_test01"
  } ],
  "user_name" : "kxxxxxxxt",
  "notification_template" : "aom.built-in.template.zh",
  "time_zone" : "xxx",
  "create_time" : 1667316727451,
  "update_time" : 1667316727451
}
```

Example Responses

Status code: 400

Bad Request: The request is invalid. The client should not repeat the request without modifications.

```
{
  "error_code" : "AOM.08019006",
  "error_msg" : "The action rule does not exist",
  "trace_id" : ""
}
```

Status code: 401

Unauthorized: The authentication information is incorrect or invalid.

```
{
  "error_code" : "AOM.0403",
```



```
  "error_msg" : "auth failed.",
  "error_type" : "AUTH_FAILED",
  "trace_id" : null
}
```

Status code: 403

Forbidden: The request is rejected. The server has received the request and understood it, but the server refuses to respond to it. The client should not repeat the request without modifications.

```
{
  "error_code" : "AOM.0403",
  "error_msg" : "auth failed.",
  "error_type" : "AUTH_FAILED",
  "trace_id" : null
}
```

Status code: 500

Internal Server Error

The server is able to receive the request but unable to understand the request.

```
{
  "error_code" : "APM.00000500",
  "error_msg" : "Internal Server Error",
  "trace_id" : ""
}
```

Status Codes

Status Code	Description
204	OK: The request is successful.
400	Bad Request: The request is invalid. The client should not repeat the request without modifications.
401	Unauthorized: The authentication information is incorrect or invalid.
403	Forbidden: The request is rejected. The server has received the request and understood it, but the server refuses to respond to it. The client should not repeat the request without modifications.
500	Internal Server Error The server is able to receive the request but unable to understand the request.

Error Codes

See **Error Codes**.

4.1.14 Querying the Alarm Action Rule List

Function

This API is used to query the alarm action rule list.

Calling Method

For details, see **Calling APIs**.

URI

GET /v2/{project_id}/alert/action-rules

Table 4-115 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID obtained from IAM. Generally, a project ID contains 32 characters. Minimum: **32** Maximum: **32**

Request Parameters

Table 4-116 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token obtained from IAM. Minimum: **1** Maximum: **40960**
Content-Type	Yes	String	Content type, which is application/json. Enumeration values: • **application/json**

Response Parameters

Status code: 200

Table 4-117 Response body parameters

Parameter	Type	Description
action_rules	Array of **ActionRule** objects	Alarm action rule list. Array Length: **0 - 1000**

Table 4-118 ActionRule

Parameter	Type	Description
rule_name	String	Rule name. Enter a maximum of 100 characters and do not start or end with a special character. Only letters, digits, and underscores (_) are allowed. Minimum: **1** Maximum: **100**
project_id	String	Project ID. Minimum: **32** Maximum: **32**
user_name	String	Member account name. Minimum: **1** Maximum: **100**
desc	String	Rule description. Enter a maximum of 1024 characters and do not start or end with an underscore (_). Only digits, letters, underscores (_), asterisk (*), and spaces are allowed. Minimum: **0** Maximum: **1024**
type	String	Action type. Default: Notification. Minimum: **1** Maximum: **1** Enumeration values: • **1** • **2**
notification_template	String	Message template. Minimum: **1** Maximum: **100**
create_time	Long	Creation time. Minimum: **0** Maximum: **9999999999999**
update_time	Long	Modification time Minimum: **0** Maximum: **9999999999999**
time_zone	String	Time zone. Minimum: **1** Maximum: **100**

Parameter	Type	Description
smn_topics	Array of **SmnTopics** objects	SMN topic. The total number of topics cannot exceed 5. Array Length: **1 - 5**

Table 4-119 SmnTopics

Parameter	Type	Description
display_name	String	Topic display name, which will be the name of an email sender. Max.: 192 bytes. This parameter is left blank by default. Minimum: **1** Maximum: **64**
name	String	Name of the topic. Enter 1 to 255 characters starting with a letter or digit. Only letters, digits, hyphens (-), and underscores (_) are allowed. Minimum: **1** Maximum: **255**
push_policy	Integer	SMN message push policy. Options: 0 and 1. Minimum: **0** Maximum: **1**
status	Integer	Status of the topic subscriber. 0: The topic has been deleted or the subscription list of this topic is empty. 1: The subscription object is in the subscribed state. 2: The subscription object is in the unsubscribed or canceled state. Enumeration values: • **0** • **1** • **2**
topic_urn	String	Unique resource identifier of the topic. Minimum: **1** Maximum: **100**

Status code: 401

Table 4-120 Response body parameters

Parameter	Type	Description
error_code	String	Error code. Minimum: **12** Maximum: **12**
error_msg	String	Error message. Minimum: **0** Maximum: **1024**
error_type	String	Error type. Minimum: **0** Maximum: **128**
trace_id	String	Request ID. Minimum: **32** Maximum: **32**

Status code: 403

Table 4-121 Response body parameters

Parameter	Type	Description
error_code	String	Error code. Minimum: **12** Maximum: **12**
error_msg	String	Error message. Minimum: **0** Maximum: **1024**
error_type	String	Error type. Minimum: **0** Maximum: **128**
trace_id	String	Request ID. Minimum: **32** Maximum: **32**

Status code: 500

Table 4-122 Response body parameters

Parameter	Type	Description
error_code	String	Response code. Minimum: **13** Maximum: **13**
error_msg	String	Response message. Minimum: **1** Maximum: **100**
trace_id	String	Response ID. Minimum: **12** Maximum: **12**

Example Requests

Query all alarm action rules.

```
https://{Endpoint}/v2/{project_id}/alert/action-rules
```

Example Responses

Status code: 200

OK: The request is successful.

```
{
  "action_rules" : [ {
    "create_time" : 1665991889597,
    "desc" : "",
    "notification_template" : "aom.built-in.template.zh",
    "project_id" : "2xxxxxxxxxxxxxxxxxxxxxf",
    "rule_name" : "1112222",
    "smn_topics" : [ {
      "display_name" : "",
      "name" : "gcmtest",
      "push_policy" : 0,
      "status" : 0,
      "topic_urn" : "urn:smn:xxx:2xxxxxxxxxxxxxxxxxxxxxf:gcmtest"
    } ],
    "time_zone" : "xxx",
    "type" : "1",
    "update_time" : 1665991889597,
    "user_name" : "kxxxxxt"
  } ]
}
```

Status code: 401

Unauthorized: The authentication information is incorrect or invalid.

```
{
  "error_code" : "AOM.0403",
  "error_msg" : "auth failed.",
  "error_type" : "AUTH_FAILED",
  "trace_id" : null
}
```


Status code: 403

Forbidden: The request is rejected. The server has received the request and understood it, but the server refuses to respond to it. The client should not repeat the request without modifications.

```
{
  "error_code" : "AOM.0403",
  "error_msg" : "auth failed.",
  "error_type" : "AUTH_FAILED",
  "trace_id" : null
}
```

Status code: 500

Internal Server Error: The server is able to receive the request but unable to understand the request.

```
{
  "error_code" : "APM.00000500",
  "error_msg" : "Internal Server Error",
  "trace_id" : ""
}
```

Status Codes

Status Code	Description
200	OK: The request is successful.
401	Unauthorized: The authentication information is incorrect or invalid.
403	Forbidden: The request is rejected. The server has received the request and understood it, but the server refuses to respond to it. The client should not repeat the request without modifications.
500	Internal Server Error: The server is able to receive the request but unable to understand the request.

Error Codes

See **Error Codes**.

4.1.15 Querying Metric or Event Alarm Rules

Function

This API is used to query metric or event alarm rules.

Calling Method

For details, see **Calling APIs**.

URI

GET /v4/{project_id}/alarm-rules

Table 4-123 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID obtained from IAM. Generally, a project ID contains 32 characters.

Table 4-124 Query Parameters

Parameter	Mandatory	Type	Description
name	No	String	Alarm rule name.
limit	No	String	Number of records that can be returned. Minimum: **1** Maximum: **1000**
offset	No	String	Start position for a pagination query, which must be a non-negative integer.
sort_by	No	String	Whether to sort alarms by alarm rule name or alarm creation time. • alarm_rule_name.asc • alarm_create_time.desc
event_source	No	String	Source of an event alarm rule. • RDS • EVS • CCE • LTS • AOM
event_severity	No	String	Alarm severity. • Critical • Major • Minor • Info

Parameter	Mandatory	Type	Description
alarm_rule_status	No	String	Alarm rule status. • OK: normal • alarm: threshold-crossing • Effective: in use • Invalid: not in use Enumeration values: • **OK** • **alarm** • **Effective** • **Invalid**
alarm_rule_type	No	String	Alarm rule type. • metric: metric alarm rule • event: event alarm rule Enumeration values: • **metric** • **event**
prom_instance_id	No	String	Prometheus instance ID.
bind_notification_rule_id	No	String	Name of the bound alarm action rule.
related_cce_clusters	No	String	CCE cluster ID.

Request Parameters

Table 4-125 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token obtained from IAM.
Content-Type	Yes	String	Content type, which is application/json.

Parameter	Mandatory	Type	Description
Enterprise-Project-Id	No	String	Enterprise project ID. • To query instances in an enterprise project, enter the enterprise project ID. • To query instances in all enterprise projects, enter **all_granted_eps**.

Response Parameters

Status code: 200

Table 4-126 Response body parameters

Parameter	Type	Description
alarm_rules	Array of **AlarmParamForV4Db** objects	Alarm rule list.
metadata	Object	Metadata information.
count	Integer	Number of alarm rules.

Table 4-127 AlarmParamForV4Db

Parameter	Type	Description
alarm_create_time	Long	Time when an alarm rule was created.
alarm_update_time	Long	Time when an alarm rule was modified.
alarm_rule_name	String	Alarm rule name.
alarm_rule_id	Long	Alarm rule ID.
enterprise_project_id	String	Enterprise project ID.
prom_instance_id	String	Prometheus instance ID.
alarm_rule_description	String	Alarm rule description.

Parameter	Type	Description
alarm_rule_enable	Boolean	Enabled or not.
alarm_rule_status	String	Alarm status. • OK: normal • alarm: threshold-crossing • Effective: in use • Invalid: not in use
alarm_rule_type	String	Rule type. • metric: metric alarm rule • event: event alarm rule Enumeration values: • **metric** • **event**
metric_alarm_spec	**MetricAlarmSpec** object	Structure of a metric alarm rule.
event_alarm_spec	**EventAlarmSpec** object	Structure of an event alarm rule.
alarm_notifications	**AlarmNotification** object	Alarm notification module.
user_id	String	User ID.

Table 4-128 MetricAlarmSpec

Parameter	Type	Description
monitor_type	String	Monitoring type. • all_metric: Select metrics from all metrics. • promql: Select metrics using PromQL. • resource (unavailable soon): Select metrics by resource type. Enumeration values: • **all_metric** • **promql** • **resource**
no_data_conditions	Array of **NoDataCondition** objects	Action taken for insufficient data.

Parameter	Type	Description
alarm_tags	Array of **AlarmTags** objects	Alarm tags.
monitor_objects	Array of Map<String,String> objects	List of monitored objects.
recovery_conditions	**RecoveryCondition** object	Alarm clearance condition.
trigger_conditions	Array of **TriggerCondition** objects	Trigger conditions.
alarm_rule_template_bind_enable	Boolean	(Discarded) Whether to bind an alarm rule template. Default: **false**
alarm_rule_template_id	String	(Discarded) ID of the alarm rule template. Default: **""**

Table 4-129 NoDataCondition

Parameter	Type	Description
no_data_timeframe	Integer	Number of periods without data.
no_data_alert_state	String	Status of the threshold rule when the data is insufficient. • no_data: A notification indicating insufficient data is sent. • alerting: An alarm is triggered. • ok: No exception occurs. • pre_state: Retain the previous state. Enumeration values: • **no_data** • **alerting** • **ok** • **pre_state**
notify_no_data	Boolean	Whether to send a notification when data is insufficient.

Table 4-130 AlarmTags

Parameter	Type	Description
auto_tags	Array of strings	Automatic tag.
custom_tags	Array of strings	Custom tag.
custom_annotations	Array of strings	Alarm annotation.

Table 4-131 RecoveryCondition

Parameter	Type	Description
recovery_timeframe	Integer	Number of consecutive periods for which the trigger condition is not met to clear an alarm.

Table 4-132 TriggerCondition

Parameter	Type	Description
metric_query_mode	String	Metric query mode. • AOM: native AOM • PROM: AOM Prometheus • NATIVE_PROM: native Prometheus Enumeration values: • **AOM** • **PROM** • **NATIVE_PROM**
metric_namespace	String	Metric namespace.
metric_name	String	Metric name.
metric_unit	String	Metric unit.
metric_labels	Array of strings	Metric dimension.
promql	String	Prometheus statement.
promql_expr	Array of strings	Prometheus statement template.
trigger_times	String	Number of consecutive periods.

Parameter	Type	Description
trigger_interval	String	Check interval. • If **trigger_type** is set to **HOURLY***, set this parameter to **""**. • If **trigger_type** is set to **DAILY**, set 00:00–23:00. Example: 03:00. • If **trigger_type** is set to **WEEKLY**, select a day in a week and then select 00:00–23:00. Example: **1 03:00" indicates 03:00 on every Monday. • If **trigger_type** is set to **CRON**, specify a standard cron expression. • If **trigger_type** is set to **FIXED_RATE**, select 15s, 30s, 1–59 min, or 1–24 h.
trigger_type	String	Trigger type. • FIXED_RATE: fixed interval • HOURLY: every hour • DAILY: every day • WEEKLY: every week • CRON: Cron expression Enumeration values: • **FIXED_RATE** • **HOURLY** • **DAILY** • **WEEKLY** • **CRON**
promql_for	String	Native Prometheus monitoring duration.
aggregation_type	String	Statistical mode. • average • minimum • maximum • sum • sampleCount
operator	String	Operator. Options: >, <, =, >=, and <=.
thresholds	Map<String,String>	Key-value pair. The key indicates the alarm severity while the value indicates the alarm threshold.

Parameter	Type	Description
aggregation_window	String	Statistical period. • 15s • 30s • 1m • 5m • 15m • 1h
cmdb	**CmdbInfo** object	CMDB information.
query_match	String	Query filter criteria.
query_param	String	Query parameters.
aom_monitor_level	String	Monitoring layer.
aggregate_type	String	Aggregation mode. • by: not grouped • avg • max • min • sum Enumeration values: • **by** • **avg** • **max** • **min** • **sum**
metric_statistic_method	String	Metric statistics method to be used when you set **Configuration Mode** to **Select from all metrics** during alarm rule setting. • single: single metric • mix: multi-metric combined operations Enumeration values: • **single** • **mix**
expression	String	Expression of a combined operation.
mix_promql	String	PromQL of a combined operation.

Table 4-133 CmdbInfo

Parameter	Type	Description
app_id	String	Application ID.
node_ids	Array of **NodeInfo** objects	Node information list.

Table 4-134 NodeInfo

Parameter	Type	Description
node_type	String	Node type.
node_id	String	Node ID.

Table 4-135 EventAlarmSpec

Parameter	Type	Description
alarm_source	String	Alarm rule source. • systemEvent • customEvent Enumeration values: • **systemEvent** • **customEvent**
event_source	String	Alarm source. • RDS • EVS • CCE • LTS • AOM
monitor_objects	Array of Map<String,String> objects	List of monitored objects. Key-value pair. • event_type: notification type • event_severity: alarm severity • event_name: event name • namespace: namespace • clusterId: cluster ID • customField: user-defined field

Parameter	Type	Description
trigger_conditions	Array of **EventTriggerCondition** objects	Trigger conditions.
alarm_rule_template_bind_enable	Boolean	(Discarded) Whether to bind an alarm rule template. Default: **false**
alarm_rule_template_id	String	(Discarded) ID of the alarm rule template. Default: **""**

Table 4-136 EventTriggerCondition

Parameter	Type	Description
event_name	String	Event name.
trigger_type	String	Trigger mode. • immediately: An alarm is triggered immediately if the alarm condition is met. • accumulative: An alarm is triggered if the alarm condition is met for a specified number of times. Enumeration values: • **immediately** • **accumulative**
aggregation_window	Long	Statistical period, in seconds. For example, **3600** indicates one hour. Leave this parameter empty if **trigger_type** is set to **immediately**.
operator	String	Operator. Options: >, <, =, >=, and <=. Leave this parameter empty if **trigger_type** is set to **immediately**.
thresholds	Map<String,Integer>	Key-value pair. The key indicates the alarm severity while the value indicates the number of accumulated trigger times. Leave this parameter empty if **trigger_type** is set to **immediately**.

Parameter	Type	Description
frequency	String	Event alarm notification frequency. Leave this parameter empty if **trigger_type** is set to **immediately**. • 0: alarm sent only once • 300: every 5 minutes • 600: every 10 minutes • 900: every 15 minutes • 1800: every 30 minutes • 3600: every hour • 10800: every 3 hours • 21600: every 6 hours • 43200: every 12 hours • 86400: every day

Table 4-137 AlarmNotification

Parameter	Type	Description
notification_type	String	Notification type. • direct: direct alarm reporting • alarm_policy: alarm reporting after noise reduction Enumeration values: • **direct** • **alarm_policy**
route_group_enable	Boolean	Whether to enable the grouping rule. • If the notification type is **alarm_policy**, set this parameter to **true**. • If the notification type is **direct**, set this parameter to **false**. Enumeration values: • **true** • **false**
route_group_rule	String	Grouping rule name. • If **route_group_enable** is set to **true**, enter a grouping rule name. • If **route_group_enable** is set to **false**, enter **""**.

Parameter	Type	Description
notification_enable	Boolean	Whether to enable an alarm action rule. ● If the notification type is **direct**, set this parameter to **true**. ● If the notification type is **alarm_policy**, set this parameter to **false**.
bind_notification_rule_id	String	Alarm action rule ID. ● If **notification_enable** is set to **true**, enter an alarm action rule ID. ● If **notification_enable** is set to **false**, enter **""**.
notify_resolved	Boolean	Whether to send a notification when an alarm is cleared. ● true: Send a notification. ● false: Do not send any notification. Enumeration values: ● **true** ● **false**
notify_triggered	Boolean	Whether to send a notification when an alarm is triggered. ● true: Send a notification. ● false: Do not send any notification. Enumeration values: ● **true** ● **false**
notify_frequency	Integer	Notification frequency. ● If the notification type is **alarm_policy**, set this parameter to **-1**. ● If the notification type is **direct**, set this parameter to any of the following: ● 0: alarm sent only once ● 300: every 5 minutes ● 600: every 10 minutes ● 900: every 15 minutes ● 1800: every 30 minutes ● 3600: every hour ● 10800: every 3 hours ● 21600: every 6 hours ● 43200: every 12 hours ● 86400: every day

Status code: 500

Table 4-138 Response body parameters

Parameter	Type	Description
error_code	String	Error code. Minimum: **12** Maximum: **12**
error_msg	String	Error message. Minimum: **0** Maximum: **1024**
error_type	String	Error type. Minimum: **0** Maximum: **128**
trace_id	String	Request ID. Minimum: **32** Maximum: **32**

Example Requests

Query metric or event alarm rules.

```
https://{Endpoint}/v4/{project_id}/alarm-rules?limit=100&offset=0
```

Example Responses

Status code: 200

OK: The request is successful.

```
{
  "alarm_rules" : [ {
    "alarm_create_time" : 1713929265429,
    "alarm_notifications" : {
      "bind_notification_rule_id" : "aom_notification_rule",
      "notification_enable" : true,
      "notification_type" : "direct",
      "notify_frequency" : -1,
      "notify_resolved" : false,
      "notify_triggered" : false,
      "route_group_enable" : false,
      "route_group_rule" : ""
    },
    "alarm_rule_description" : "",
    "alarm_rule_enable" : true,
    "alarm_rule_id" : 0,
    "alarm_rule_name" : "aom_alarm_rule",
    "alarm_rule_status" : "Effective",
    "alarm_rule_type" : "event",
```



```
  "alarm_update_time" : 0,
  "enterprise_project_id" : "0",
  "event_alarm_spec" : {
    "alarm_rule_template_bind_enable" : false,
    "alarm_rule_template_id" : "",
    "alarm_source" : "systemEvent",
    "event_source" : "CCE",
    "monitor_objects" : [ {
      "clusterId" : "a4****6b-f**9-1**e-a**d-02****10***a",
      "event_type" : "event"
    } ],
    "trigger_conditions" : [ {
      "aggregation_window" : 300,
      "event_name" : "",
      "frequency" : "1",
      "operator" : ">=",
      "thresholds" : {
        "Critical" : 2
      },
      "trigger_type" : "immediately"
    } ]
  },
  "user_id" : "2a****56****48****73****1b****cf"
}, {
  "alarm_create_time" : 1711458243395,
  "alarm_notifications" : {
    "bind_notification_rule_id" : "",
    "notification_enable" : false,
    "notification_type" : "direct",
    "notify_frequency" : 0,
    "notify_resolved" : false,
    "notify_triggered" : false,
    "route_group_enable" : false,
    "route_group_rule" : ""
  },
  "alarm_rule_description" : "",
  "alarm_rule_enable" : false,
  "alarm_rule_id" : 1,
  "alarm_rule_name" : "aom_alarm_rule_1",
  "alarm_rule_status" : "Invalid",
  "alarm_rule_type" : "metric",
  "alarm_update_time" : 0,
  "enterprise_project_id" : "0",
  "metric_alarm_spec" : {
    "alarm_rule_template_bind_enable" : false,
    "alarm_rule_template_id" : "",
    "alarm_tags" : [ {
      "auto_tags" : [ ],
      "custom_annotations" : [ ],
      "custom_tags" : [ ]
    } ],
    "monitor_objects" : [ ],
    "monitor_type" : "all_metric",
    "no_data_conditions" : [ {
      "no_data_timeframe" : 0,
      "notify_no_data" : false
    } ],
    "recovery_conditions" : {
      "recovery_timeframe" : 1
    },
    "trigger_conditions" : [ {
      "aggregate_type" : "by",
      "aggregation_type" : "average",
      "aggregation_window" : "30s",
      "aom_monitor_level" : "",
      "cmdb" : {
        "app_id" : "",
        "node_ids" : [ ]
      },
```



```
        "expression" : "",
        "metric_labels" : [ ],
        "metric_name" : "container_memory_rss",
        "metric_namespace" : "",
        "metric_query_mode" : "PROM",
        "metric_statistic_method" : "single",
        "metric_unit" : "",
        "mix_promql" : "",
        "operator" : ">",
        "promql" : "label_replace(container_memory_rss{node=\"172.**.**.206\"},\"__name__
\",\"container_memory_rss\",\"\",\"\") or label_replace(avg_over_time(container_memory_rss{node=
\"172.**.**.206\"}[29999ms]),\"__name__\",\"container_memory_rss\",\"\",\"\")",
        "promql_for" : "1m",
        "query_match" : "[{\"conditionList\":[{\"name\":\"172.**.**.206\"},{\"name
\":\"172.**.**.133\"}],\"addMode\":\"first\",\"conditionValue\":[{\"name\":\"172.**.**.206\"}],\"id\":\"first
\",\"conditionCompare\":\"=\",\"dimension\":\"node\"}]",
        "query_param" : {
          "apmMetricReg" : "",
          "code" : "a"
        },
        "thresholds" : {
          "Critical" : "1"
        },
        "trigger_interval" : "15s",
        "trigger_times" : 1,
        "trigger_type" : "FIXED_RATE"
      } ]
    },
    "prom_instance_id" : "90e***88-1**4-4**9-9**3-1f*******cd3",
    "user_id" : "2a****56****48****73****1b****cf"
  } ],
  "count" : 29,
  "metadata" : {
    "alarm_rule_template_id" : [ ],
    "bind_notification_rule_id" : [ "aom_notification_rule", "1", "00********qq", "00*****3", "m***m" ],
    "event_source" : [ "CCE", "DCS", "ES", "AOM" ],
    "prom_instance_id" : [ "0", "796***7d-1**8-4**9-a**0-99*******ca0", "6cc***c8-f**f-4**4-9**2-90*******fcf",
"90e***88-1**4-4**9-9**3-1f*******cd3" ],
    "resource_kind" : [ "HC:DCS:REDIS_3.0", "CCE", "HC:ES:METRICS", "AOM" ]
  }
}
```


Status code: 500

Internal Server Error: The server is able to receive the request but unable to understand the request.


```
{
  "error_code" : "AOM.02022500",
  "error_msg" : "internal server error",
  "error_type" : "INTERNAL_SERVER_ERROR",
  "trace_id" : ""
}
```


Status Codes

Status Code	Description
200	OK: The request is successful.
500	Internal Server Error: The server is able to receive the request but unable to understand the request.

Error Codes

See **Error Codes**.

4.1.16 Adding or Modifying Metric or Event Alarm Rules

Function

This API is used to add or modify metric or event alarm rules.

Calling Method

For details, see **Calling APIs**.

URI

POST /v4/{project_id}/alarm-rules

Table 4-139 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID obtained from IAM. Generally, a project ID contains 32 characters.

Table 4-140 Query Parameters

Parameter	Mandatory	Type	Description
action_id	Yes	String	Alarm rule ID. • To add an alarm rule, enter **add-alarm-action**. • To modify an alarm rule, enter **update-alarm-action**.

Request Parameters

Table 4-141 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token obtained from IAM.
Content-Type	Yes	String	Content type, which is application/json.

Parameter	Mandatory	Type	Description
Enterprise-Project-Id	No	String	Enterprise project ID. • To query instances in an enterprise project, enter the enterprise project ID. • To query instances in all enterprise projects, enter **all_granted_eps**.

Table 4-142 Request body parameters

Parameter	Mandatory	Type	Description
alarm_notifications	No	**AlarmNotification** object	Alarm notification module.
alarm_rule_description	No	String	Alarm rule description.
alarm_rule_enable	No	Boolean	Enabled or not. Enumeration values: • **true** • **false**
alarm_rule_name	Yes	String	Alarm rule name.
alarm_rule_type	Yes	String	Alarm rule type. • metric: metric alarm rule • event: event alarm rule Enumeration values: • **metric** • **event**
event_alarm_spec	No	**EventAlarmSpec** object	Structure of an event alarm rule.
metric_alarm_spec	No	**MetricAlarmSpec** object	Structure of a metric alarm rule.
prom_instance_id	No	String	Prometheus instance ID.

Table 4-143 AlarmNotification

Parameter	Mandatory	Type	Description
notification_type	Yes	String	Notification type. • direct: direct alarm reporting • alarm_policy: alarm reporting after noise reduction Enumeration values: • **direct** • **alarm_policy**
route_group_enable	Yes	Boolean	Whether to enable the grouping rule. • If the notification type is **alarm_policy**, set this parameter to **true**. • If the notification type is **direct**, set this parameter to **false**. Enumeration values: • **true** • **false**
route_group_rule	Yes	String	Grouping rule name. • If **route_group_enable** is set to **true**, enter a grouping rule name. • If **route_group_enable** is set to **false**, enter **""**.
notification_enable	No	Boolean	Whether to enable an alarm action rule. • If the notification type is **direct**, set this parameter to **true**. • If the notification type is **alarm_policy**, set this parameter to **false**.
bind_notification_rule_id	No	String	Alarm action rule ID. • If **notification_enable** is set to **true**, enter an alarm action rule ID. • If **notification_enable** is set to **false**, enter **""**.

Parameter	Mandatory	Type	Description
notify_resolved	No	Boolean	Whether to send a notification when an alarm is cleared. • true: Send a notification. • false: Do not send any notification. Enumeration values: • **true** • **false**
notify_triggered	No	Boolean	Whether to send a notification when an alarm is triggered. • true: Send a notification. • false: Do not send any notification. Enumeration values: • **true** • **false**
notify_frequency	No	Integer	Notification frequency. • If the notification type is **alarm_policy**, set this parameter to **-1**. • If the notification type is **direct**, set this parameter to any of the following: • 0: alarm sent only once • 300: every 5 minutes • 600: every 10 minutes • 900: every 15 minutes • 1800: every 30 minutes • 3600: every hour • 10800: every 3 hours • 21600: every 6 hours • 43200: every 12 hours • 86400: every day

Table 4-144 EventAlarmSpec

Parameter	Mandatory	Type	Description
alarm_source	No	String	Alarm rule source. • systemEvent • customEvent Enumeration values: • **systemEvent** • **customEvent**
event_source	No	String	Alarm source. • RDS • EVS • CCE • LTS • AOM
monitor_objects	No	Array of Map<String,String> objects	List of monitored objects. Key-value pair. • event_type: notification type • event_severity: alarm severity • event_name: event name • namespace: namespace • clusterId: cluster ID • customField: user-defined field
trigger_conditions	No	Array of **EventTriggerCondition** objects	Trigger conditions.
alarm_rule_template_bind_enable	No	Boolean	(Discarded) Whether to bind an alarm rule template. Default: **false**
alarm_rule_template_id	No	String	(Discarded) ID of the alarm rule template. Default: ""

Table 4-145 EventTriggerCondition

Parameter	Mandatory	Type	Description
event_name	No	String	Event name.
trigger_type	No	String	Trigger mode. • immediately: An alarm is triggered immediately if the alarm condition is met. • accumulative: An alarm is triggered if the alarm condition is met for a specified number of times. Enumeration values: • **immediately** • **accumulative**
aggregation_window	No	Long	Statistical period, in seconds. For example, **3600** indicates one hour. Leave this parameter empty if **trigger_type** is set to **immediately**.
operator	No	String	Operator. Options: **>**, **<**, **=**, **>=**, and **<=**. Leave this parameter empty if **trigger_type** is set to **immediately**.
thresholds	No	Map<String,Integer>	Key-value pair. The key indicates the alarm severity while the value indicates the number of accumulated trigger times. Leave this parameter empty if **trigger_type** is set to **immediately**.

Parameter	Mandatory	Type	Description
frequency	No	String	Event alarm notification frequency. Leave this parameter empty if **trigger_type** is set to **immediately**. • 0: alarm sent only once • 300: every 5 minutes • 600: every 10 minutes • 900: every 15 minutes • 1800: every 30 minutes • 3600: every hour • 10800: every 3 hours • 21600: every 6 hours • 43200: every 12 hours • 86400: every day

Table 4-146 MetricAlarmSpec

Parameter	Mandatory	Type	Description
monitor_type	Yes	String	Monitoring type. • all_metric: Select metrics from all metrics. • promql: Select metrics using PromQL. • resource (unavailable soon): Select metrics by resource type. Enumeration values: • **all_metric** • **promql** • **resource**
no_data_conditions	No	Array of **NoDataCondition** objects	Action taken for insufficient data.
alarm_tags	Yes	Array of **AlarmTags** objects	Alarm tags.
monitor_objects	No	Array of Map<String,String> objects	List of monitored objects.

Parameter	Mandatory	Type	Description
recovery_conditions	Yes	**RecoveryCondition** object	Alarm clearance condition.
trigger_conditions	Yes	Array of **TriggerCondition** objects	Trigger conditions.
alarm_rule_template_bind_enable	No	Boolean	(Discarded) Whether to bind an alarm rule template. Default: **false**
alarm_rule_template_id	No	String	(Discarded) ID of the alarm rule template. Default: ""

Table 4-147 NoDataCondition

Parameter	Mandatory	Type	Description
no_data_timeframe	No	Integer	Number of periods without data.
no_data_alert_state	No	String	Status of the threshold rule when the data is insufficient. • no_data: A notification indicating insufficient data is sent. • alerting: An alarm is triggered. • ok: No exception occurs. • pre_state: Retain the previous state. Enumeration values: • **no_data** • **alerting** • **ok** • **pre_state**
notify_no_data	No	Boolean	Whether to send a notification when data is insufficient.

Table 4-148 AlarmTags

Parameter	Mandatory	Type	Description
auto_tags	No	Array of strings	Automatic tag.
custom_tags	No	Array of strings	Custom tag.
custom_annotations	No	Array of strings	Alarm annotation.

Table 4-149 RecoveryCondition

Parameter	Mandatory	Type	Description
recovery_timeframe	No	Integer	Number of consecutive periods for which the trigger condition is not met to clear an alarm.

Table 4-150 TriggerCondition

Parameter	Mandatory	Type	Description
metric_query_mode	Yes	String	Metric query mode. • AOM: native AOM • PROM: AOM Prometheus • NATIVE_PROM: native Prometheus Enumeration values: • **AOM** • **PROM** • **NATIVE_PROM**
metric_namespace	Yes	String	Metric namespace.
metric_name	Yes	String	Metric name.
metric_unit	Yes	String	Metric unit.
metric_labels	Yes	Array of strings	Metric dimension.
promql	Yes	String	Prometheus statement.
promql_expr	No	Array of strings	Prometheus statement template.

Parameter	Mandatory	Type	Description
trigger_times	No	String	Number of consecutive periods.
trigger_interval	No	String	Check interval. • If **trigger_type** is set to **HOURLY***, set this parameter to **""**. • If **trigger_type** is set to **DAILY**, set 00:00–23:00. Example: 03:00. • If **trigger_type** is set to **WEEKLY**, select a day in a week and then select 00:00–23:00. Example: **1 03:00" indicates 03:00 on every Monday. • If **trigger_type** is set to **CRON**, specify a standard cron expression. • If **trigger_type** is set to **FIXED_RATE**, select 15s, 30s, 1–59 min, or 1–24 h.
trigger_type	No	String	Trigger type. • FIXED_RATE: fixed interval • HOURLY: every hour • DAILY: every day • WEEKLY: every week • CRON: Cron expression Enumeration values: • **FIXED_RATE** • **HOURLY** • **DAILY** • **WEEKLY** • **CRON**
promql_for	No	String	Native Prometheus monitoring duration.
aggregation_type	No	String	Statistical mode. • average • minimum • maximum • sum • sampleCount

Parameter	Mandatory	Type	Description
operator	No	String	Operator. Options: >, <, =, >=, and <=.
thresholds	No	Map<String,String>	Key-value pair. The key indicates the alarm severity while the value indicates the alarm threshold.
aggregation_window	No	String	Statistical period. • 15s • 30s • 1m • 5m • 15m • 1h
cmdb	No	**CmdbInfo** object	CMDB information.
query_match	No	String	Query filter criteria.
query_param	Yes	String	Query parameters.
aom_monitor_level	No	String	Monitoring layer.
aggregate_type	No	String	Aggregation mode. • by: not grouped • avg • max • min • sum Enumeration values: • **by** • **avg** • **max** • **min** • **sum**

Parameter	Mandatory	Type	Description
metric_statistic_method	No	String	Metric statistics method to be used when you set **Configuration Mode** to **Select from all metrics** during alarm rule setting. • single: single metric • mix: multi-metric combined operations Enumeration values: • **single** • **mix**
expression	No	String	Expression of a combined operation.
mix_promql	No	String	PromQL of a combined operation.

Table 4-151 CmdbInfo

Parameter	Mandatory	Type	Description
app_id	No	String	Application ID.
node_ids	No	Array of **NodeInfo** objects	Node information list.

Table 4-152 NodeInfo

Parameter	Mandatory	Type	Description
node_type	No	String	Node type.
node_id	No	String	Node ID.

Response Parameters

Status code: 200

Table 4-153 Response body parameters

Parameter	Type	Description
error_code	String	Error code.

Parameter	Type	Description
error_message	String	Error message.
alarm_rules	Array of **AddOrUpdateAlarmRuleV4ItemResult** objects	Alarm rule list.

Table 4-154 AddOrUpdateAlarmRuleV4ItemResult

Parameter	Type	Description
alarm_rule_name	String	Alarm rule name.
result	String	Whether an alarm rule is successfully added or modified.

Status code: 400

Table 4-155 Response body parameters

Parameter	Type	Description
error_code	String	Error code. Minimum: **12** Maximum: **12**
error_msg	String	Error message. Minimum: **0** Maximum: **1024**
error_type	String	Error type. Minimum: **0** Maximum: **128**
trace_id	String	Request ID. Minimum: **32** Maximum: **32**

Status code: 500

Table 4-156 Response body parameters

Parameter	Type	Description
error_code	String	Error code. Minimum: **12** Maximum: **12**
error_msg	String	Error message. Minimum: **0** Maximum: **1024**
error_type	String	Error type. Minimum: **0** Maximum: **128**
trace_id	String	Request ID. Minimum: **32** Maximum: **32**

Example Requests

- Add a metric alarm rule.

```
https://{Endpoint}/v4/{project_id}/alarm-rules?action_id=add-alarm-action

{
  "alarm_notifications" : {
    "bind_notification_rule_id" : "",
    "notification_enable" : false,
    "notification_type" : "alarm_policy",
    "notify_frequency" : -1,
    "notify_resolved" : true,
    "notify_triggered" : true,
    "route_group_enable" : true,
    "route_group_rule" : "aom_route_group_rule"
  },
  "alarm_rule_description" : "aom_alarm_rule",
  "alarm_rule_enable" : true,
  "alarm_rule_name" : "aom_alarm_rule",
  "alarm_rule_type" : "metric",
  "metric_alarm_spec" : {
    "alarm_rule_template_bind_enable" : false,
    "alarm_rule_template_id" : "",
    "alarm_tags" : [ {
      "auto_tags" : [ ],
      "custom_annotations" : [ "333=rrr" ],
      "custom_tags" : [ "333=rrr" ]
    } ],
    "monitor_objects" : [ ],
    "monitor_type" : "all_metric",
    "no_data_conditions" : [ {
      "no_data_alert_state" : "no_data",
      "no_data_timeframe" : 3,
      "notify_no_data" : true
    } ],
    "recovery_conditions" : {
      "recovery_timeframe" : 2
    },
    "trigger_conditions" : [ {
      "aggregate_type" : "by",
```



```
    "aggregation_type" : "average",
    "aggregation_window" : "5m",
    "aom_monitor_level" : "",
    "cmdb" : {
      "app_id" : "",
      "node_ids" : [ ]
    },
    "expression" : "",
    "metric_labels" : [ ],
    "metric_name" : "aom_metrics_total",
    "metric_namespace" : "",
    "metric_query_mode" : "PROM",
    "metric_statistic_method" : "single",
    "metric_unit" : "",
    "mix_promql" : "",
    "operator" : ">",
    "promql" : "label_replace(avg_over_time(aom_metrics_total{instance=\"1117919565\"}
[59999ms]),\"__name__\",\"aom_metrics_total\",\"\",\"\")",
    "query_match" : [ {
      "addMode" : "first",
      "conditionCompare" : "=",
      "conditionList" : [ {
        "name" : "1117919565"
      } ],
      "conditionValue" : [ {
        "name" : "1117919565"
      } ],
      "dimension" : "instance",
      "id" : "first",
      "regExpress" : null
    } ],
    "query_param" : { },
    "thresholds" : {
      "Info" : "100"
    },
    "trigger_interval" : "15m",
    "trigger_times" : 4,
    "trigger_type" : "FIXED_RATE"
  } ]
 },
 "prom_instance_id" : "0"
}
```

- Modify a metric alarm rule.

```
https://{Endpoint}/v4/{project_id}/alarm-rules?action_id=update-alarm-action

{
 "alarm_notifications" : {
   "bind_notification_rule_id" : "",
   "notification_enable" : false,
   "notification_type" : "alarm_policy",
   "notify_frequency" : -1,
   "notify_resolved" : true,
   "notify_triggered" : true,
   "route_group_enable" : true,
   "route_group_rule" : "aom_route_group_rule"
 },
 "alarm_rule_description" : "aom_alarm_rule",
 "alarm_rule_enable" : true,
 "alarm_rule_name" : "aom_alarm_rule",
 "alarm_rule_type" : "metric",
 "metric_alarm_spec" : {
   "alarm_rule_template_bind_enable" : false,
   "alarm_rule_template_id" : "",
   "alarm_tags" : [ {
     "auto_tags" : [ ],
     "custom_annotations" : [ "333=rrr" ],
     "custom_tags" : [ "333=rrr" ]
   } ],
   "monitor_objects" : [ ],
```



```
    "monitor_type" : "all_metric",
    "no_data_conditions" : [ {
      "no_data_alert_state" : "no_data",
      "no_data_timeframe" : 3,
      "notify_no_data" : true
    } ],
    "recovery_conditions" : {
      "recovery_timeframe" : 2
    },
    "trigger_conditions" : [ {
      "aggregate_type" : "by",
      "aggregation_type" : "average",
      "aggregation_window" : "5m",
      "aom_monitor_level" : "",
      "cmdb" : {
        "app_id" : "",
        "node_ids" : [ ]
      },
      "expression" : "",
      "metric_labels" : [ ],
      "metric_name" : "aom_metrics_total",
      "metric_namespace" : "",
      "metric_query_mode" : "PROM",
      "metric_statistic_method" : "single",
      "metric_unit" : "",
      "mix_promql" : "",
      "operator" : ">",
      "promql" : "label_replace(avg_over_time(aom_metrics_total{instance=\"1117919565\"}
[59999ms]),\"__name__\",\"aom_metrics_total\",\"\",\"\")",
      "query_match" : [ {
        "addMode" : "first",
        "conditionCompare" : "=",
        "conditionList" : [ {
          "name" : "1117919565"
        } ],
        "conditionValue" : [ {
          "name" : "1117919565"
        } ],
        "dimension" : "instance",
        "id" : "first",
        "regExpress" : null
      } ],
      "query_param" : { },
      "thresholds" : {
        "Info" : "100"
      },
      "trigger_interval" : "15m",
      "trigger_times" : 4,
      "trigger_type" : "FIXED_RATE"
    } ]
  },
  "prom_instance_id" : "0"
}
```

- Add an event alarm rule.

```
https://{Endpoint}/v4/{project_id}/alarm-rules?action_id=add-alarm-action

{
  "alarm_notifications" : {
    "bind_notification_rule_id" : "aom_event_notification_rule",
    "notification_enable" : true,
    "notification_type" : "direct",
    "notify_frequency" : "-1",
    "notify_resolved" : false,
    "notify_triggered" : false,
    "route_group_enable" : false,
    "route_group_rule" : ""
  },
  "alarm_rule_description" : "aom_alarm_event_rule",
  "alarm_rule_enable" : true,
```



```
 "alarm_rule_name" : "aom_event_alarm_rule",
 "alarm_rule_type" : "event",
 "event_alarm_spec" : {
  "alarm_source" : "systemEvent",
  "event_source" : "CCE",
  "monitor_objects" : [ {
    "event_name" : "ScaleUpTimedOut; VolumeResizeFailed",
    "event_type" : "event"
  } ],
  "trigger_conditions" : [ {
    "aggregation_window" : 300,
    "event_name" : "ScaleUpTimedOut",
    "frequency" : "-1",
    "operator" : ">",
    "thresholds" : {
      "Critical" : 1
    },
    "trigger_type" : "accumulative"
  }, {
    "event_name" : "VolumeResizeFailed",
    "thresholds" : {
      "Critical" : 1
    },
    "trigger_type" : "immediately"
  } ]
 }
}
```

- Modify an event alarm rule.

```
https://{Endpoint}/v4/{project_id}/alarm-rules?action_id=update-alarm-action

{
 "alarm_notifications" : {
  "bind_notification_rule_id" : "aom_event_notification_rule",
  "notification_enable" : true,
  "notification_type" : "direct",
  "notify_frequency" : "-1",
  "notify_resolved" : false,
  "notify_triggered" : false,
  "route_group_enable" : false,
  "route_group_rule" : ""
 },
 "alarm_rule_description" : "aom_alarm_event_rule",
 "alarm_rule_enable" : true,
 "alarm_rule_name" : "aom_event_alarm_rule",
 "alarm_rule_type" : "event",
 "event_alarm_spec" : {
  "alarm_source" : "systemEvent",
  "event_source" : "CCE",
  "monitor_objects" : [ {
    "event_name" : "ScaleUpTimedOut; VolumeResizeFailed",
    "event_type" : "event"
  } ],
  "trigger_conditions" : [ {
    "aggregation_window" : 300,
    "event_name" : "ScaleUpTimedOut",
    "frequency" : "-1",
    "operator" : ">",
    "thresholds" : {
      "Critical" : 1
    },
    "trigger_type" : "accumulative"
  }, {
    "event_name" : "VolumeResizeFailed",
    "thresholds" : {
      "Critical" : 2
    },
    "trigger_type" : "immediately"
  } ]
```



```
  }
}
```

Example Responses

Status code: 200

OK: The request is successful.

```
{
  "alarm_rules" : [ {
    "alarm_rule_name" : "aom_alarm_rule",
    "result" : "success"
  } ],
  "error_code" : "200",
  "error_message" : "success"
}
```

Status code: 400

Bad Request: Invalid request. The client should not repeat this request without modification.

```
{
  "error_code" : "AOM.02021006",
  "error_msg" : "This rule actionId is invalid",
  "error_type" : "PARAM_INVALID",
  "trace_id" : "58ef0f7c107a2b577f78b9cc7f48b46f"
}
```

Status code: 500

Internal Server Error: The server is able to receive the request but unable to understand the request.

```
{
  "error_code" : "AOM.02021500",
  "error_msg" : "internal server error",
  "error_type" : "INTERNAL_SERVER_ERROR",
  "trace_id" : ""
}
```

Status Codes

Status Code	Description
200	OK: The request is successful.
400	Bad Request: Invalid request. The client should not repeat this request without modification.
500	Internal Server Error: The server is able to receive the request but unable to understand the request.

Error Codes

See **Error Codes**.

4.1.17 Deleting Metric or Event Alarm Rules

Function

This API is used to delete metric or event alarm rules.

Calling Method

For details, see **Calling APIs**.

URI

DELETE /v4/{project_id}/alarm-rules

Table 4-157 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID obtained from IAM. Generally, a project ID contains 32 characters.

Request Parameters

Table 4-158 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token obtained from IAM.
Content-Type	Yes	String	Content type, which is application/json.

Table 4-159 Request body parameters

Parameter	Mandatory	Type	Description
alarm_rules	Yes	Array of strings	Alarm rule name list.

Response Parameters

Status code: 200

Table 4-160 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_message	String	Error message.
resources	Array of **ItemResult** objects	Resource list.

Table 4-161 ItemResult

Parameter	Type	Description
alarm_rule_name	String	Alarm rule name.

Status code: 400

Table 4-162 Response body parameters

Parameter	Type	Description
error_code	String	Error code. Minimum: **12** Maximum: **12**
error_msg	String	Error message. Minimum: **0** Maximum: **1024**
error_type	String	Error type. Minimum: **0** Maximum: **128**
trace_id	String	Request ID. Minimum: **32** Maximum: **32**

Status code: 500

Table 4-163 Response body parameters

Parameter	Type	Description
error_code	String	Error code. Minimum: **12** Maximum: **12**
error_msg	String	Error message. Minimum: **0** Maximum: **1024**
error_type	String	Error type. Minimum: **0** Maximum: **128**
trace_id	String	Request ID. Minimum: **32** Maximum: **32**

Example Requests

- Delete a metric or event alarm rule.

```
https://{Endpoint}/v4/{project_id}/alarm-rules

{
  "alarm_rules" : [ "aom_alarm_rule" ]
}
```

- Delete multiple metric or event alarm rules.

```
https://{Endpoint}/v4/{project_id}/alarm-rules

{
  "alarm_rules" : [ "aom_alarm_rule", "aom_alarm_rule2" ]
}
```

Example Responses

Status code: 200

OK: The request is successful.

```
{
  "error_code" : "200",
  "error_message" : "success",
  "resources" : [ {
    "alarm_rule_name" : "aom_alarm_rule"
  } ]
}
```

Status code: 400

Bad Request: Invalid request. The client should not repeat this request without modification.

```
{
  "error_code" : "AOM.02024016",
  "error_msg" : "delete alarm rule name is empty",
```



```
  "trace_id" : ""
}
```

Status code: 500

Internal Server Error: The server is able to receive the request but unable to understand the request.

```
{
  "error_code" : "APM.00000500",
  "error_msg" : "Internal Server Error",
  "trace_id" : ""
}
```

Status Codes

Status Code	Description
200	OK: The request is successful.
400	Bad Request: Invalid request. The client should not repeat this request without modification.
500	Internal Server Error: The server is able to receive the request but unable to understand the request.

Error Codes

See **Error Codes**.

4.1.18 Querying Events and Alarms

Function

This API is used to query events and alarms of a user.

Calling Method

For details, see **Calling APIs**.

URI

POST /v2/{project_id}/events

Table 4-164 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID obtained from IAM. Generally, a project ID contains 32 characters.

Table 4-165 Query Parameters

Parameter	Mandatory	Type	Description
type	No	String	Type of information to be queried. active_alert: Active alarms are to be queried. history_alert: Historical alarms are to be queried. If this parameter is not transferred or other values are transferred, information that meets the specified search criteria will be returned. Enumeration values: • **history_alert** • **active_alert**

Request Parameters

Table 4-166 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token obtained from IAM.
Content-Type	Yes	String	Content type, which is application/json. Enumeration values: • **application/json**
Enterprise-Project-Id	No	String	Enterprise project ID. • To query instances in an enterprise project, enter the enterprise project ID. • To query instances in all enterprise projects, enter **all_granted_eps**.

Table 4-167 Request body parameters

Parameter	Mandatory	Type	Description
time_range	Yes	String	Time range specified to query data of the last N minutes when the client time is inconsistent with the server time. It can also be used to accurately query the data of a specified period. Example: ● -1.-1.60: indicates that the data of the latest 60 minutes is queried. This query is based on the server time regardless of the current client time. ● 1650852000000.1650852300000.5: indicates the five minutes from 10:00:00 to 10:05:00 on April 25, 2022 GMT+08:00. Format: startTimeInMillis.endTimeInMillis.durationInMinutes Parameter description: ● startTimeInMillis: Start time of the query, in milliseconds. If this parameter is set to -1, the server calculates the start time as follows: endTimeInMillis – durationInMinutes x 60 x 1000. For example, -1.1650852300000.5 is equivalent to 1650852000000.1650852300000.5. ● endTimeInMillis: End time of the query, in milliseconds. If this parameter is set to -1, the server calculates the end time as follows: startTimeInMillis + durationInMinutes x 60 x 1000. If the calculated end time is later than the

Parameter	Mandatory	Type	Description
			current system time, the current system time is used. For example, 1650852000000.-1.5 is equivalent to 1650852000000.1650852300000.5. • durationInMinutes: Time span, in minutes. The value must be greater than 0 and greater than or equal to the result of "(endTimeInMillis – startTimeInMillis)/(60 x 1000) – 1". If both the start time and end time are set to -1, the system sets the end time to the current UTC time (in milliseconds) and calculates the start time as follows: endTimeInMillis – durationInMinutes x 60 x 1000. For example, -1.-1.60 indicates the latest 60 minutes. Constraint: In a single request, the following condition must be met: durationInMinutes x 60/ period ≤ 1440
step	No	Long	Statistical step (unit: ms). For example, if the statistical step is one minute, set this parameter to 60,000.
search	No	String	Field specified for fuzzy query, which can be left blank. If this field is not left blank, fuzzy query can be performed accordingly. In that case, the metadata field is mandatory.
sort	No	**sort** object	Sorting order, which can be left blank.
metadata_relation	No	Array of **RelationModel** objects	Combination of search criteria, which can be left blank.

Table 4-168 sort

Parameter	Mandatory	Type	Description
order_by	No	Array of strings	List of sorted fields. Fields in this list are sorted based on the specified order.
order	No	String	Sorting order. asc: ascending order. desc: descending order. Enumeration values: • **asc** • **desc**

Table 4-169 RelationModel

Parameter	Mandatory	Type	Description
key	No	String	Key specified for query, which corresponds to the key in the metadata.
value	No	Array of strings	Value of the specified key in the search criterion.
relation	No	String	Relationship between search criteria. Values: AND: All criteria must be met. OR: One of the criteria needs to be met. NOT: None of the criteria can be met. Enumeration values: • **AND** • **OR** • **NOT**

Response Parameters

Status code: 200

Table 4-170 Response body parameters

Parameter	Type	Description
events	Array of **EventModel** objects	Event or alarm details.

Table 4-171 EventModel

Parameter	Type	Description
starts_at	Long	Time when an event or alarm is generated (CST timestamp precise down to the millisecond).
ends_at	Long	Time when an event or alarm is cleared (CST timestamp precise down to the millisecond). 0: The event or alarm is not deleted.
timeout	Long	Duration (in milliseconds) at which an alarm is automatically cleared. For example, if an alarm needs to be automatically cleared in one minute, set this parameter to 60000. The default value is 3 days (that is, 3 days x 24 hours x 60 minutes x 1000 ms = 4,320,000 ms).
metadata	Map<String,String>	Details of an event or alarm. The value is a key-value pair. The following fields are mandatory: • **event_name**: event or alarm name, which is a string. • **event_severity**: event severity, which is an enumerated value with string elements. Options: **Critical**, **Major**, **Minor**, and **Info**. • **event_type**: event type, which is an enumerated value with string elements. Options: **event** and **alarm**. • **resource_provider**: name of a cloud service corresponding to an event, which is a string. • **resource_type**: type of the resource corresponding to an event, which is a string. • **resource_id**: resource ID corresponding to an event, which is a string.
annotations	Map<String,Object>	Additional field for an event or alarm, which can be left blank.
attach_rule	Map<String,Object>	Reserved field for an event or alarm, which can be left blank.

Parameter	Type	Description
id	String	Event or alarm ID, which is automatically generated by the system.

Status code: 400

Table 4-172 Response body parameters

Parameter	Type	Description
error_code	String	Response code.
error_msg	String	Error description.
error_type	String	API call failure type.
trace_id	String	Request ID.

Status code: 401

Table 4-173 Response body parameters

Parameter	Type	Description
error_code	String	Response code.
error_msg	String	Error description.
error_type	String	API call failure type.
trace_id	String	Request ID.

Status code: 403

Table 4-174 Response body parameters

Parameter	Type	Description
error_code	String	Response code.
error_msg	String	Error description.
error_type	String	API call failure type.
trace_id	String	Request ID.

Status code: 500

Table 4-175 Response body parameters

Parameter	Type	Description
error_code	String	Response code.
error_msg	String	Error description.
error_type	String	API call failure type.
trace_id	String	Request ID.

Status code: 503

Table 4-176 Response body parameters

Parameter	Type	Description
error_code	String	Response code.
error_msg	String	Error description.
error_type	String	API call failure type.
trace_id	String	Request ID.

Example Requests

Query the events and alarms of a specified user.

```
https://{endpoint}/v2/{project_id}/events

{
  "time_range" : "-1.-1.30",
  "metadata_relation" : [ {
    "key" : "event_type",
    "relation" : "AND",
    "value" : [ "alarm" ]
  }, {
    "key" : "event_severity",
    "relation" : "AND",
    "value" : [ "Critical", "Major", "Minor", "Info" ]
  } ],
  "search" : "",
  "sort" : {
    "order_by" : [ "starts_at" ],
    "order" : "desc"
  }
}
```

Example Responses

Status code: 200

OK: The request is successful.

```
{
  "events" : [ {
```

```
    "annotations" : {
      "alarm_probableCause_zh_cn" : "Possible Causes",
      "message" : "Alarm Details",
      "alarm_fix_suggestion_zh_cn" : "Suggestions"
    },
    "attach_rule" : { },
    "ends_at" : 0,
    "id" : "6775161208461480000",
    "metadata" : {
      "event_type" : "alarm",
      "event_severity" : "Major",
      "resource_type" : "vm",
      "event_name" : "test",
      "resource_id" : "ecs123",
      "resource_provider" : "ecs"
    },
    "starts_at" : 16377362908000,
    "timeout" : 60000
  } ]
}
```

Status code: 400

Bad Request: The request is invalid. The client should not repeat the request without modifications.

```
{
  "error_code" : "AOM.08032002",
  "error_message" : "The request body is illegal",
  "error_type" : "SC_BAD_REQUEST"
}
```

Status code: 401

Unauthorized: The authentication information is incorrect or invalid.

```
{
  "error_code" : "AOM.0403",
  "error_message" : "auth failed.",
  "error_type" : "AUTH_FAILED",
  "trace_id" : null
}
```

Status code: 403

Forbidden: The request is rejected. The server has received the request and understood it, but the server refuses to respond to it. The client should not repeat the request without modifications.

```
{
  "error_code" : "AOM.0403",
  "error_message" : "auth failed.",
  "error_type" : "AUTH_FAILED",
  "trace_id" : null
}
```

Status code: 500

Internal Server Error: The server is able to receive the request but unable to understand the request.

```
{
  "error_code" : "APM.00000500",
  "error_message" : "Internal Server Error",
  "trace_id" : null
}
```

Status code: 503

Service Unavailable: The requested service is invalid. The client should not repeat the request without modifications.

```
{
  "error_code" : "AOM.0503",
  "error_message" : "SC_NOT_IMPLEMENTED",
  "error_type" : "SC_NOT_IMPLEMENTED"
}
```

Status Codes

Status Code	Description
200	OK: The request is successful.
400	Bad Request: The request is invalid. The client should not repeat the request without modifications.
401	Unauthorized: The authentication information is incorrect or invalid.
403	Forbidden: The request is rejected. The server has received the request and understood it, but the server refuses to respond to it. The client should not repeat the request without modifications.
500	Internal Server Error: The server is able to receive the request but unable to understand the request.
503	Service Unavailable: The requested service is invalid. The client should not repeat the request without modifications.

Error Codes

See **Error Codes**.

4.1.19 Counting Events and Alarms

Function

This API is used to count events and alarms that meet specified conditions.

Calling Method

For details, see **Calling APIs**.

URI

POST /v2/{project_id}/events/statistic

Table 4-177 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID obtained from IAM. Generally, a project ID contains 32 characters.

Table 4-178 Query Parameters

Parameter	Mandatory	Type	Description
type	No	String	Type of information to be queried. active_alert: Active alarms are to be queried. history_alert: Historical alarms are to be queried. If this parameter is not transferred or other values are transferred, information that meets the specified search criteria will be returned. Enumeration values: • **history_alert** • **active_alert**

Request Parameters

Table 4-179 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token obtained from IAM.
Content-Type	Yes	String	Content type, which is application/json. Enumeration values: • **application/json**

Table 4-180 Request body parameters

Parameter	Mandatory	Type	Description
time_range	Yes	String	Time range specified to query data of the last N minutes when the client time is inconsistent with the server time. It can also be used to accurately query the data of a specified period. Example: ● -1.-1.60: indicates that the data of the latest 60 minutes is queried. This query is based on the server time regardless of the current client time. ● 1650852000000.1650852300000.5: indicates the five minutes from 10:00:00 to 10:05:00 on April 25, 2022 GMT+08:00. Format: startTimeInMillis.endTimeInMillis.durationInMinutes Parameter description: ● startTimeInMillis: Start time of the query, in milliseconds. If this parameter is set to -1, the server calculates the start time as follows: endTimeInMillis – durationInMinutes x 60 x 1000. For example, -1.1650852300000.5 is equivalent to 1650852000000.1650852300000.5. ● endTimeInMillis: End time of the query, in milliseconds. If this parameter is set to -1, the server calculates the end time as follows: startTimeInMillis + durationInMinutes x 60 x 1000. If the calculated end time is later than the

Parameter	Mandatory	Type	Description
			current system time, the current system time is used. For example, 1650852000000.-1.5 is equivalent to 1650852000000.1650852300000.5. • durationInMinutes: Time span, in minutes. The value must be greater than 0 and greater than or equal to the result of "(endTimeInMillis – startTimeInMillis)/(60 x 1000) – 1". If both the start time and end time are set to -1, the system sets the end time to the current UTC time (in milliseconds) and calculates the start time as follows: endTimeInMillis – durationInMinutes x 60 x 1000. For example, -1.-1.60 indicates the latest 60 minutes. Constraint: In a single request, the following condition must be met: durationInMinutes x 60/ period ≤ 1440
step	Yes	Long	Statistical step (unit: ms). For example, if the statistical step is one minute, set this parameter to 60,000.
search	No	String	Field specified for fuzzy query, which can be left blank. If this field is not left blank, the system will return metadata's mandatory fields that are fuzzily matched.
sort	No	**sort** object	Sorting order, which can be left blank.
metadata_relation	No	Array of **RelationModel** objects	Combination of search criteria, which can be left blank.

Table 4-181 sort

Parameter	Mandatory	Type	Description
order_by	No	Array of strings	List of sorted fields. Fields in this list are sorted based on the specified order.
order	No	String	Sorting order. asc: ascending order. desc: descending order. Enumeration values: • **asc** • **desc**

Table 4-182 RelationModel

Parameter	Mandatory	Type	Description
key	No	String	Key specified for query, which corresponds to the key in the metadata.
value	No	Array of strings	Value of the specified key in the search criterion.
relation	No	String	Relationship between search criteria. Values: AND: All criteria must be met. OR: One of the criteria needs to be met. NOT: None of the criteria can be met. Enumeration values: • **AND** • **OR** • **NOT**

Response Parameters

Status code: 200

Table 4-183 Response body parameters

Parameter	Type	Description
step	Long	Statistical step (unit: ms). For example, if the statistical step is one minute, set this parameter to 60,000.
timestamps	Array of longs	Time series object corresponding to the statistical result.
series	Array of **EventSeries** objects	Statistical results of a time series object's different severities of events or alarms.
summary	Map<String,Integer>	Alarm statistics summary.

Table 4-184 EventSeries

Parameter	Type	Description
event_severity	String	Enumerated values of event or alarm severities. Enumeration values: • **Critical** • **Major** • **Minor** • **Info**
values	Array of integers	Event or alarm statistical result.

Status code: 400

Table 4-185 Response body parameters

Parameter	Type	Description
error_code	String	Response code.
error_msg	String	Error description.
error_type	String	API call failure type.
trace_id	String	Request ID.

Status code: 401

Table 4-186 Response body parameters

Parameter	Type	Description
error_code	String	Response code.
error_msg	String	Error description.
error_type	String	API call failure type.
trace_id	String	Request ID.

Status code: 403

Table 4-187 Response body parameters

Parameter	Type	Description
error_code	String	Response code.
error_msg	String	Error description.
error_type	String	API call failure type.
trace_id	String	Request ID.

Status code: 500

Table 4-188 Response body parameters

Parameter	Type	Description
error_code	String	Response code.
error_msg	String	Error description.
error_type	String	API call failure type.
trace_id	String	Request ID.

Status code: 503

Table 4-189 Response body parameters

Parameter	Type	Description
error_code	String	Response code.
error_msg	String	Error description.
error_type	String	API call failure type.

Parameter	Type	Description
trace_id	String	Request ID.

Example Requests

Query the events and alarms on the step basis in a specified time range.

```
https://{endpoint}/v2/{project_id}/events/statistic

{
  "time_range" : "-1.-1.5",
  "step" : 60000
}
```

Example Responses

Status code: 200

OK: The request is successful.

```
{
  "series" : [ {
    "event_severity" : "Critical",
    "values" : [ 2, 3, 3, 1, 0 ]
  }, {
    "event_severity" : "Major",
    "values" : [ 4, 3, 5, 4, 0 ]
  }, {
    "event_severity" : "Minor",
    "values" : [ 3, 1, 1, 1, 0 ]
  }, {
    "event_severity" : "Info",
    "values" : [ 0, 0, 0, 0, 0 ]
  } ],
  "step" : 60000,
  "summary" : {
    "critical_count" : 9,
    "info_count" : 0,
    "major_count" : 16,
    "minor_count" : 6
  },
  "timestamps" : [ 1711788600000, 1711788660000, 1711788720000, 1711788780000, 1711788840000 ]
}
```

Status code: 400

Bad Request: The request is invalid. The client should not repeat the request without modifications.

```
{
  "error_code" : "AOM.08033002",
  "error_message" : "The request body is illegal",
  "trace_id" : ""
}
```

Status code: 401

Unauthorized: The authentication information is incorrect or invalid.

```
{
  "error_code" : "AOM.0403",
  "error_message" : "auth failed.",
```



```
  "error_type" : "AUTH_FAILED",
  "trace_id" : null
}
```

Status code: 403

Forbidden: The request is rejected. The server has received the request and understood it, but the server refuses to respond to it. The client should not repeat the request without modifications.

```
{
  "error_code" : "AOM.0403",
  "error_message" : "auth failed.",
  "error_type" : "AUTH_FAILED",
  "trace_id" : null
}
```

Status code: 500

Internal Server Error: The server is able to receive the request but unable to understand the request.

```
{
  "error_code" : "APM.00000500",
  "error_message" : "Internal Server Error",
  "trace_id" : ""
}
```

Status code: 503

Service Unavailable: The requested service is invalid. The client should not repeat the request without modifications.

```
{
  "error_code" : "AOM.0503",
  "error_message" : "SC_NOT_IMPLEMENTED",
  "error_type" : "SC_NOT_IMPLEMENTED"
}
```

Status Codes

Status Code	Description
200	OK: The request is successful.
400	Bad Request: The request is invalid. The client should not repeat the request without modifications.
401	Unauthorized: The authentication information is incorrect or invalid.
403	Forbidden: The request is rejected. The server has received the request and understood it, but the server refuses to respond to it. The client should not repeat the request without modifications.
500	Internal Server Error: The server is able to receive the request but unable to understand the request.
503	Service Unavailable: The requested service is invalid. The client should not repeat the request without modifications.

Error Codes

See **Error Codes**.

4.1.20 Reporting Events and Alarms

Function

This API is used to report events and alarms of a user.

Calling Method

For details, see **Calling APIs**.

URI

PUT /v2/{project_id}/push/events

Table 4-190 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID obtained from IAM. Generally, a project ID contains 32 characters.

Table 4-191 Query Parameters

Parameter	Mandatory	Type	Description
action	No	String	Requested action. clear: The alarm is to be cleared. If this parameter is not transferred or other values are transferred, the alarm is reported by default. Enumeration values: • **clear**

Request Parameters

Table 4-192 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token obtained from IAM.

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Content type, which is application/json. Enumeration values: • **application/json**
x-enterprise-prject-id	No	String	ID of the enterprise project to which the alarm belongs.

Table 4-193 Request body parameters

Parameter	Mandatory	Type	Description
events	Yes	Array of **EventModel** objects	Event or alarm details.

Table 4-194 EventModel

Parameter	Mandatory	Type	Description
starts_at	No	Long	Time when an event or alarm is generated (CST timestamp precise down to the millisecond).
ends_at	No	Long	Time when an event or alarm is cleared (CST timestamp precise down to the millisecond). 0: The event or alarm is not deleted.
timeout	No	Long	Duration (in milliseconds) at which an alarm is automatically cleared. For example, if an alarm needs to be automatically cleared in one minute, set this parameter to 60000. The default value is 3 days (that is, 3 days x 24 hours x 60 minutes x 1000 ms = 4,320,000 ms).

Parameter	Mandatory	Type	Description
metadata	No	Map<String,String>	Details of an event or alarm. The value is a key-value pair. The following fields are mandatory: • **event_name**: event or alarm name, which is a string. • **event_severity**: event severity, which is an enumerated value with string elements. Options: **Critical**, **Major**, **Minor**, and **Info**. • **event_type**: event type, which is an enumerated value with string elements. Options: **event** and **alarm**. • **resource_provider**: name of a cloud service corresponding to an event, which is a string. • **resource_type**: type of the resource corresponding to an event, which is a string. • **resource_id**: resource ID corresponding to an event, which is a string.
annotations	No	Map<String,Object>	Additional field for an event or alarm, which can be left blank.
attach_rule	No	Map<String,Object>	Reserved field for an event or alarm, which can be left blank.
id	No	String	Event or alarm ID, which is automatically generated by the system.

Response Parameters

Status code: 400

Table 4-195 Response body parameters

Parameter	Type	Description
error_code	String	Response code.
error_msg	String	Error description.
error_type	String	API call failure type.
trace_id	String	Request ID.

Example Requests

Report an alarm named "test".

```
https://{EndPoint}/v2/{project_id}/push/events

{
  "events" : [ {
    "starts_at" : 1605232501000,
    "timeout" : 60000,
    "metadata" : {
      "event_name" : "test",
      "event_severity" : "Major",
      "event_type" : "alarm",
      "resource_provider" : "ecs",
      "resource_type" : "vm",
      "resource_id" : "ecs123"
    },
    "annotations" : {
      "alarm_probableCause_zh_cn" : "Possible Causes",
      "alarm_fix_suggestion_zh_cn" : "Suggestions",
      "message" : "Alarm Details"
    },
    "attach_rule" : { }
  } ]
}
```

Example Responses

Status code: 400

Bad Request: The request is invalid. The client should not repeat the request without modifications.

```
{
  "error_code" : "AOM.0400",
  "error_msg" : "parse eventParam failed",
  "error_type" : "SC_BAD_REQUEST"
}
```

Status Codes

Status Code	Description
204	OK: The request is successful.

Status Code	Description
400	Bad Request: The request is invalid. The client should not repeat the request without modifications.
401	Unauthorized: The authentication information is incorrect or invalid.
403	Forbidden: The request is rejected. The server has received the request and understood it, but the server refuses to respond to it. The client should not repeat the request without modifications.
500	Internal Server Error: The server is able to receive the request but unable to understand the request.
503	Service Unavailable: The requested service is invalid. The client should not repeat the request without modifications.

Error Codes

See **Error Codes**.

4.2 Monitoring

4.2.1 Querying Time Series Objects

Function

This API is used to query the time series objects that can be monitored in the system. You can specify a namespace, name, dimension, and resource ID (format: resType_resId). You can also specify the start position and the maximum number of returned records for a pagination query.

Calling Method

For details, see **Calling APIs**.

URI

POST /v2/{project_id}/series

Table 4-196 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID obtained from IAM. Generally, a project ID contains 32 characters.

Table 4-197 Query Parameters

Parameter	Mandatory	Type	Description
limit	No	String	Maximum number of returned records. Value range: 1–1000. Default value: 1000.
offset	No	String	Start position of a pagination query. The value is a non-negative integer.

Request Parameters

Table 4-198 Request body parameters

Parameter	Mandatory	Type	Description
series	Yes	Array of **QuerySeriesOptionParam** objects	Array for querying time series objects.

Table 4-199 QuerySeriesOptionParam

Parameter	Mandatory	Type	Description
namespace	Yes	String	Namespace of time series objects. Value range: PAAS.CONTAINER, PAAS.NODE, PAAS.SLA, PAAS.AGGR, or CUSTOMMETRICS. PAAS.CONTAINER: namespace of application time series objects. PAAS.NODE: namespace of node time series objects. PAAS.SLA: namespace of SLA time series objects. PAAS.AGGR: namespace of cluster time series objects. CUSTOMMETRICS: namespace of custom time series objects.
metric_name	No	String	Time series name. Length: 1 to 255 characters. Values: cpuUsage: CPU usage. cpuCoreUsed: used CPU cores. Custom time series names.

Parameter	Mandatory	Type	Description
dimensions	No	Array of **DimensionSeries** objects	List of time series dimensions. You can call the /v2/{project_id}/series API to query the time series dimension list by namespace and metric_name.

Table 4-200 DimensionSeries

Parameter	Mandatory	Type	Description
name	No	String	Dimension name.
value	No	String	Dimension value.

Response Parameters

Status code: 200

Table 4-201 Response body parameters

Parameter	Type	Description
series	Array of **SeriesQueryItemResult** objects	List of time series objects.
meta_data	**MetaDataSeries** object	Metadata, including pagination information.

Table 4-202 SeriesQueryItemResult

Parameter	Type	Description
namespace	String	Namespace.
dimensions	Array of **DimensionSeries** objects	Dimension list.
metric_name	String	Time series name.
unit	String	Time series unit.
dimension_value_hash	String	Time series hash value.

Table 4-203 DimensionSeries

Parameter	Type	Description
name	String	Dimension name.
value	String	Dimension value.

Table 4-204 MetaDataSeries

Parameter	Type	Description
count	Integer	Number of returned records.
offset	Integer	Start of the next page, which is used for pagination. null: No more data.
total	Integer	Total number of records.
nextToken	Integer	Offset.

Status code: 400

Table 4-205 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
error_type	String	Error type.
trace_id	String	Request ID.

Example Requests

Query time series objects by namespace and metric_name.

```
https://{Endpoint}/v2/{project_id}/series

{
  "series" : [ {
    "namespace" : "PAAS.CONTAINER",
    "metric_name" : "aom_process_cpu_usage"
  } ]
}
```

Example Responses

Status code: 200

OK: The request is successful.


```
{
  "meta_data" : {
    "count" : 1,
    "offset" : null,
    "total" : 1,
    "nextToken" : 0
  },
  "series" : [ {
    "namespace" : "PAAS.CONTAINER",
    "metric_name" : "cpuUsage",
    "unit" : "Percent",
    "dimensions" : [ {
      "name" : "appName",
      "value" : "appValue"
    } ],
    "dimension_value_hash" : null
  } ]
}
```

Status code: 400

Bad Request: The request is invalid. The client should not repeat the request without modifications.

```
{
  "error_code" : "AOM.04007101",
  "error_msg" : "Invalid namespace",
  "error_type" : "BAD_REQUEST",
  "trace_id" : ""
}
```

Status Codes

Status Code	Description
200	OK: The request is successful.
400	Bad Request: The request is invalid. The client should not repeat the request without modifications.
401	Unauthorized: The authentication information is incorrect or invalid.
403	Forbidden: The request is rejected. The server has received the request and understood it, but the server refuses to respond to it. The client should not repeat the request without modifications.
500	Internal Server Error: The server is able to receive the request but unable to understand the request.
503	Service Unavailable: The requested service is invalid. The client should not repeat the request without modifications.

Error Codes

See **Error Codes**.

4.2.2 Querying Time Series Data

Function

This API is used to query time series data within a specified period. You can specify a dimension or period to query.

Calling Method

For details, see **Calling APIs**.

URI

POST /v2/{project_id}/samples

Table 4-206 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID obtained from IAM. Generally, a project ID contains 32 characters.

Table 4-207 Query Parameters

Parameter	Mandatory	Type	Description
fill_value	No	String	Value filled for breakpoints in time series data. Default value: –1. –1: Breakpoints are filled with –1. 0: Breakpoints are filled with 0. null: Breakpoints are filled with null. average: Breakpoints are filled with the average value of the adjacent valid data. If there is no valid data, breakpoints are filled with null.

Request Parameters

Table 4-208 Request body parameters

Parameter	Mandatory	Type	Description
samples	Yes	Array of **QuerySample** objects	List of time series objects. A JSON array can contain up to 20 objects.
statistics	Yes	Array of strings	Statistic. Values: maximum, minimum, sum, average, and sampleCount.
period	Yes	Integer	Granularity for monitoring data, which is an enumerated value. Values: 60: The data monitoring granularity is 1 minute. 300: The data monitoring granularity is 5 minutes. 900: The data monitoring granularity is 15 minutes. 3600: The data monitoring granularity is 1 hour.

Parameter	Mandatory	Type	Description
time_range	Yes	String	Time range specified to query data of the last N minutes when the client time is inconsistent with the server time. It can also be used to accurately query the data of a specified period. Example: ● -1.-1.60: indicates that the data of the latest 60 minutes is queried. This query is based on the server time regardless of the current client time. ● 1650852000000.1650852300000.5: indicates the five minutes from 10:00:00 to 10:05:00 on April 25, 2022 GMT+08:00. Format: startTimeInMillis.endTimeInMillis.durationInMinutes Parameter description: ● startTimeInMillis: Start time of the query, in milliseconds. If this parameter is set to -1, the server calculates the start time as follows: endTimeInMillis – durationInMinutes x 60 x 1000. For example, -1.1650852300000.5 is equivalent to 1650852000000.1650852300000.5. ● endTimeInMillis: End time of the query, in milliseconds. If this parameter is set to -1, the server calculates the end time as follows: startTimeInMillis + durationInMinutes x 60 x 1000. If the calculated end time is later than the current system time, the current system time is used.

Parameter	Mandatory	Type	Description
			For example, 1650852000000.-1.5 is equivalent to 1650852000000.1650852300000.5. • durationInMinutes: Time span, in minutes. The value must be greater than 0 and greater than or equal to the result of "(endTimeInMillis – startTimeInMillis)/(60 x 1000) – 1". If both the start time and end time are set to -1, the system sets the end time to the current UTC time (in milliseconds) and calculates the start time as follows: endTimeInMillis – durationInMinutes x 60 x 1000. For example, -1.-1.60 indicates the latest 60 minutes. Constraint: In a single request, the following condition must be met: durationInMinutes x 60/ period ≤ 1440

Table 4-209 QuerySample

Parameter	Mandatory	Type	Description
namespace	Yes	String	Namespace of time series objects. Value range: PAAS.CONTAINER, PAAS.NODE, PAAS.SLA, PAAS.AGGR, or CUSTOMMETRICS. PAAS.CONTAINER: namespace of application time series objects. PAAS.NODE: namespace of node time series objects. PAAS.SLA: namespace of SLA time series objects. PAAS.AGGR: namespace of cluster time series objects. CUSTOMMETRICS: namespace of custom time series objects.
dimensions	Yes	Array of **DimensionSeries** objects	List of time series dimensions.You can call the /v2/{project_id}/series API to query the time series dimension list by namespace and metric_name.
metric_name	Yes	String	Time series name. Length: 1 to 255 characters. Values: cpuUsage: CPU usage. cpuCoreUsed: used CPU cores. Custom time series names.

Table 4-210 DimensionSeries

Parameter	Mandatory	Type	Description
name	No	String	Dimension name.
value	No	String	Dimension value.

Response Parameters

Status code: 200

Table 4-211 Response body parameters

Parameter	Type	Description
samples	Array of **SampleDataValue** objects	List of time series objects.

Table 4-212 SampleDataValue

Parameter	Type	Description
sample	**QuerySample** object	List of time series objects.
data_points	Array of **MetricDataPoints** objects	Time series data.

Table 4-213 QuerySample

Parameter	Type	Description
namespace	String	Namespace of time series objects. Value range: PAAS.CONTAINER, PAAS.NODE, PAAS.SLA, PAAS.AGGR, or CUSTOMMETRICS. PAAS.CONTAINER: namespace of application time series objects. PAAS.NODE: namespace of node time series objects. PAAS.SLA: namespace of SLA time series objects. PAAS.AGGR: namespace of cluster time series objects. CUSTOMMETRICS: namespace of custom time series objects.
dimensions	Array of **DimensionSeries** objects	List of time series dimensions.You can call the /v2/{project_id}/series API to query the time series dimension list by namespace and metric_name.
metric_name	String	Time series name. Length: 1 to 255 characters. Values: cpuUsage: CPU usage. cpuCoreUsed: used CPU cores. Custom time series names.

Table 4-214 DimensionSeries

Parameter	Type	Description
name	String	Dimension name.
value	String	Dimension value.

Table 4-215 MetricDataPoints

Parameter	Type	Description
statistics	Array of StatisticValue objects	Statistic.
timestamp	Long	Timestamp.
unit	String	Time series unit.

Table 4-216 StatisticValue

Parameter	Type	Description
statistic	String	Statistic.
value	Double	Statistical result.

Status code: 400

Table 4-217 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
error_type	String	Error type.
trace_id	String	Request ID.

Example Requests

Query time series data in the last five minutes by namespace, metric_name, and dimensions.

```
https://{Endpoint}/v2/{project_id}/samples

{
   "samples": [
      {
         "namespace": "PAAS.CONTAINER",
         "metric_name": "aom_process_cpu_usage",
         "dimensions": [
            {
               "name": "appName",
               "value": "aomApp"
            }
```



```
        ]
      }
  ],
  "period": 60,
  "time_range": "-1.-1.5",// Last 5 minutes
    "statistics": [
      "sum"
  ]
}
```

Example Responses

Status code: 200

OK: The request is successful.

```
{
  "samples" : [ {
    "sample" : {
      "namespace" : "PAAS.CONTAINER",
      "metric_name" : "aom_process_cpu_usage",
      "dimensions" : [ {
        "name" : "appName",
        "value" : "aomApp"
      } ]
    },
    "data_points" : [ {
      "timestamp" : 1694673300000,
      "unit" : "Percent",
      "statistics" : [ {
        "statistic" : "sum",
        "value" : "23"
      } ]
    } ]
  } ]
}
```

Status code: 400

Bad Request: The request is invalid. The client should not repeat the request without modifications.

```
{
  "error_code" : "AOM.04008105",
  "error_msg" : "Query metric data samples is invalid",
  "error_type" : "BAD_REQUEST",
  "trace_id" : ""
}
```

Status Codes

Status Code	Description
200	OK: The request is successful.
400	Bad Request: The request is invalid. The client should not repeat the request without modifications.
401	Unauthorized: The authentication information is incorrect or invalid.
403	Forbidden: The request is rejected. The server has received the request and understood it, but the server refuses to respond to it. The client should not repeat the request without modifications.

Status Code	Description
500	Internal Server Error: The server is able to receive the request but unable to understand the request.
503	Service Unavailable: The requested service is invalid. The client should not repeat the request without modifications.

Error Codes

See **Error Codes**.

4.2.3 Querying Metrics

Function

This API is used to query the metrics that can be monitored in the system. You can query specific metrics by specifying a namespace, metric name, dimension, and resource ID (format: resType_resId). You can also specify the start position and the maximum number of returned records for a pagination query.

Calling Method

For details, see **Calling APIs**.

URI

POST /v1/{project_id}/ams/metrics

Table 4-218 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID obtained from IAM. Generally, a project ID contains 32 characters.

Table 4-219 Query Parameters

Parameter	Mandatory	Type	Description
type	No	String	Metric query mode.
limit	No	String	Maximum number of returned records. Value range: 1–1000. Default value: 1000. Minimum: **0** Maximum: **4**

Parameter	Mandatory	Type	Description
start	No	String	Start position of a pagination query. The value is a non-negative integer.

Request Parameters

Table 4-220 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token obtained from IAM.
Content-Type	Yes	String	Content type, which is application/json. Enumeration values: • **application/json**

Table 4-221 Request body parameters

Parameter	Mandatory	Type	Description
inventoryId	No	String	Resource ID, which must be in the format of resType_resId. Enumerated values of resType: host, application, instance, container, process, network, storage, and volume.When type (a URI parameter) is inventory, this parameter instead of metricItems is used for associated metric queries.
metricItems	No	Array of **QueryMetricItemOptionParam** objects	If the value of type in the URI is not inventory, metrics are queried based on the information carried by metricItems.

Table 4-222 QueryMetricItemOptionParam

Parameter	Mandatory	Type	Description
dimensions	No	Array of **Dimension** objects	List of metric dimensions.
metricName	No	String	Metric name. Length: 1 to 255 characters. Value range: cpuUsage, cpuCoreUsed, and other basic metrics provided by AOM. cpuUsage: CPU usage. cpuCoreUsed: used CPU cores. Custom metrics.
namespace	Yes	String	Metric namespace. Values: PAAS.CONTAINER: namespace of component, instance, process, and container metrics. PAAS.NODE: namespace of host, network, disk, and file system metrics. PAAS.SLA: namespace of SLA metrics. PAAS.AGGR: namespace of cluster metrics. CUSTOMMETRICS: default namespace of custom metrics. Enumeration values: • **PAAS.CONTAINER** • **PAAS.NODE** • **PAAS.SLA** • **PAAS.AGGR** • **CUSTOMMETRICS**

Table 4-223 Dimension

Parameter	Mandatory	Type	Description
name	Yes	String	Dimension name.
value	Yes	String	Dimension value.

Response Parameters

Status code: 200

Table 4-224 Response body parameters

Parameter	Type	Description
metaData	**MetaDataSeries** object	Metadata, including pagination information.
metrics	Array of **MetricItemResultAPI** objects	Metric list.

Table 4-225 MetaDataSeries

Parameter	Type	Description
count	Integer	Number of returned records.
offset	Integer	Start of the next page, which is used for pagination. null: No more data.
total	Integer	Total number of records.
nextToken	Integer	Offset.

Table 4-226 MetricItemResultAPI

Parameter	Type	Description
dimensions	Array of **Dimension** objects	List of metric dimensions.
dimensionvaluehash	String	Metric hash value.
metricName	String	Metric name.
namespace	String	Namespace.
unit	String	Metric unit.

Table 4-227 Dimension

Parameter	Type	Description
name	String	Dimension name.
value	String	Dimension value.

Example Requests

- Query metrics by inventory ID.

```
https://{Endpoint}/v1/{project_id}/ams/metrics

{
  "metricItems" : [ {
    "namespace" : "PAAS.CONTAINER",
    "dimensions" : [ {
      "name" : "appName",
      "value" : "aomApp"
    }, {
      "name" : "clusterName",
      "value" : "aomCluster"
    } ]
  } ]
}
```

- Query metrics by namespace, appName, and clusterName.

```
https://{Endpoint}/v1/{project_id}/ams/metrics?type=inventory

{
  "inventoryId" : "application_xxxxxxxx-xxxx-xxxx-xxxx-xxxxx3fee10"
}
```

Example Responses

Status code: 200

OK: The request is successful.

```
{
  "errorCode" : "SVCSTG_AMS_2000000",
  "errorMessage" : "success",
  "metaData" : {
    "count" : 1,
    "offset" : 1,
    "nextToken" : null,
    "total" : 1
  },
  "metrics" : [ {
    "namespace" : "PAAS.CONTAINER",
    "metricName" : "aom_process_cpu_usage",
    "unit" : "Percent",
    "dimensions" : [ {
      "name" : "appName",
      "value" : "aomApp"
    } ]
  } ]
}
```

Status Codes

Status Code	Description
200	OK: The request is successful.
400	Bad Request: The request is invalid. The client should not repeat the request without modifications.
401	Unauthorized: The authentication information is incorrect or invalid.

Status Code	Description
403	Forbidden: The request is rejected. The server has received the request and understood it, but the server refuses to respond to it. The client should not repeat the request without modifications.
500	Internal Server Error: The server is able to receive the request but unable to understand the request.
503	Service Unavailable The requested service is invalid. The client should not repeat the request without modifications.

Error Codes

See **Error Codes**.

4.2.4 Querying Monitoring Data

Function

This API is used to query monitoring data of metrics within a specified period. You can specify a dimension or period to query.

Calling Method

For details, see **Calling APIs**.

URI

POST /v1/{project_id}/ams/metricdata

Table 4-228 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID obtained from IAM. Generally, a project ID contains 32 characters.

Table 4-229 Query Parameters

Parameter	Mandatory	Type	Description
fillValue	No	String	Value filled for breakpoints in monitoring data. Default value: –1. –1: Breakpoints are filled with –1. 0: Breakpoints are filled with 0. null: Breakpoints are filled with null. average: Breakpoints are filled with the average value of the adjacent valid data. If there is no valid data, breakpoints are filled with null. Default: **-1** Enumeration values: • **-1** • **0** • **null** • **average**

Request Parameters

Table 4-230 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token obtained from IAM.
Content-Type	Yes	String	Content type, which is application/json. Enumeration values: • **application/json**

Table 4-231 Request body parameters

Parameter	Mandatory	Type	Description
metrics	Yes	Array of **MetricQuery MeritcParam** objects	Metric list. A JSON array can contain up to 20 objects.

Parameter	Mandatory	Type	Description
period	Yes	Integer	Granularity for monitoring data, which is an enumerated value. Values: 60: The data monitoring granularity is 1 minute. 300: The data monitoring granularity is 5 minutes. 900: The data monitoring granularity is 15 minutes. 3600: The data monitoring granularity is 1 hour.
statistics	Yes	Array of strings	Statistic. Values: maximum, minimum, sum, average, and sampleCount.

Parameter	Mandatory	Type	Description
timerange	Yes	String	Time range specified to query data of the last N minutes when the client time is inconsistent with the server time. It can also be used to accurately query the data of a specified period. Example: ● -1.-1.60: indicates that the data of the latest 60 minutes is queried. This query is based on the server time regardless of the current client time. ● 1650852000000.1650852300000.5: indicates the five minutes from 10:00:00 to 10:05:00 on April 25, 2022 GMT+08:00. Format: startTimeInMillis.endTimeInMillis.durationInMinutes Parameter description: ● startTimeInMillis: Start time of the query, in milliseconds. If this parameter is set to -1, the server calculates the start time as follows: endTimeInMillis – durationInMinutes x 60 x 1000. For example, -1.1650852300000.5 is equivalent to 1650852000000.1650852300000.5. ● endTimeInMillis: End time of the query, in milliseconds. If this parameter is set to -1, the server calculates the end time as follows: startTimeInMillis + durationInMinutes x 60 x 1000. If the calculated end time is later than the current system time, the current system time is used.

Parameter	Mandatory	Type	Description
			For example, 1650852000000.-1.5 is equivalent to 1650852000000.1650852300000.5. • durationInMinutes: Time span, in minutes. The value must be greater than 0 and greater than or equal to the result of "(endTimeInMillis – startTimeInMillis)/(60 x 1000) – 1". If both the start time and end time are set to -1, the system sets the end time to the current UTC time (in milliseconds) and calculates the start time as follows: endTimeInMillis – durationInMinutes x 60 x 1000. For example, -1.-1.60 indicates the latest 60 minutes. Constraint: In a single request, the following condition must be met: durationInMinutes x 60/ period ≤ 1440

Table 4-232 MetricQueryMeritcParam

Parameter	Mandatory	Type	Description
dimensions	Yes	Array of **Dimension** objects	List of metric dimensions. Neither the array nor the name or value of any dimension in the array can be left blank.
metricName	Yes	String	Metric name. Length: 1 to 255 characters. Value range: cpuUsage, cpuCoreUsed, and other basic metrics provided by AOM. cpuUsage: CPU usage. cpuCoreUsed: used CPU cores. Custom metrics.

Parameter	Mandatory	Type	Description
namespace	Yes	String	Metric namespace. Values: PAAS.CONTAINER: namespace of component, instance, process, and container metrics. PAAS.NODE: namespace of host, network, disk, and file system metrics. PAAS.SLA: namespace of SLA metrics. PAAS.AGGR: namespace of cluster metrics. CUSTOMMETRICS: default namespace of custom metrics.

Table 4-233 Dimension

Parameter	Mandatory	Type	Description
name	Yes	String	Dimension name.
value	Yes	String	Dimension value.

Response Parameters

Status code: 200

Table 4-234 Response body parameters

Parameter	Type	Description
errorCode	String	Response code.
errorMessage	String	Response message.
metrics	Array of **MetricDataValue** objects	Metric list.

Table 4-235 MetricDataValue

Parameter	Type	Description
dataPoints	Array of **MetricDataPoints** objects	Key metric.

Parameter	Type	Description
metric	**MetricQueryMeritcParam** object	Query parameters.

Table 4-236 MetricDataPoints

Parameter	Type	Description
statistics	Array of **StatisticValue** objects	Statistic.
timestamp	Long	Timestamp.
unit	String	Time series unit.

Table 4-237 StatisticValue

Parameter	Type	Description
statistic	String	Statistic.
value	Double	Statistical result.

Table 4-238 MetricQueryMeritcParam

Parameter	Type	Description
dimensions	Array of **Dimension** objects	List of metric dimensions. Neither the array nor the name or value of any dimension in the array can be left blank.
metricName	String	Metric name. Length: 1 to 255 characters. Value range: cpuUsage, cpuCoreUsed, and other basic metrics provided by AOM. cpuUsage: CPU usage. cpuCoreUsed: used CPU cores. Custom metrics.
namespace	String	Metric namespace. Values: PAAS.CONTAINER: namespace of component, instance, process, and container metrics. PAAS.NODE: namespace of host, network, disk, and file system metrics. PAAS.SLA: namespace of SLA metrics. PAAS.AGGR: namespace of cluster metrics. CUSTOMMETRICS: default namespace of custom metrics.

Table 4-239 Dimension

Parameter	Type	Description
name	String	Dimension name.
value	String	Dimension value.

Example Requests

Query the monitoring data of **cpuUsage** in the **PAAS.CONTAINER** namespace in the last five minutes.

```
https://{Endpoint}/v1/{project_id}/ams/metricdata

{
  "metrics" : [ {
    "dimensions" : [ {
      "name" : "appName",
      "value" : "aomApp"
    } ],
    "metricName" : "cpuUsage",
    "namespace" : "PAAS.CONTAINER"
  } ],
  "period" : 60,
  "statistics" : [ "maximum", "minimum", "sum" ],
  "timerange" : "-1.-1.5"
}
```

Example Responses

Status code: 200

OK: The request is successful.

```
{
  "errorCode" : "SVCSTG_AMS_2000000",
  "errorMessage" : "success",
  "metrics" : [ {
    "metric" : {
      "namespace" : "PAAS.CONTAINER",
      "metricName" : "cpuUsage",
      "dimensions" : [ {
        "name" : "appName",
        "value" : "aomApp"
      } ]
    },
    "dataPoints" : [ {
      "timestamp" : "1467892800000",
      "unit" : "Percent",
      "statistics" : [ {
        "statistic" : "maximum",
        "value" : "23"
      } ]
    } ]
  } ]
}
```


Status Codes

Status Code	Description
200	OK: The request is successful.
400	Bad Request: The request is invalid. The client should not repeat the request without modifications.
401	Unauthorized: The authentication information is incorrect or invalid.
403	Forbidden: The request is rejected. The server has received the request and understood it, but the server refuses to respond to it. The client should not repeat the request without modifications.
500	Internal Server Error: The server is able to receive the request but unable to understand the request.
503	Service Unavailable: The requested service is invalid. The client should not repeat the request without modifications.

Error Codes

See **Error Codes**.

4.2.5 Adding Monitoring Data

Function

This API is used to add one or more monitoring data records to a server.

Calling Method

For details, see **Calling APIs**.

URI

POST /v1/{project_id}/ams/report/metricdata

Table 4-240 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID obtained from IAM. Generally, a project ID contains 32 characters.

Request Parameters

Table 4-241 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token obtained from IAM.
Content-Type	Yes	String	Content type, which is application/json. Enumeration values: • **application/json**

Table 4-242 Request body parameters

Parameter	Mandatory	Type	Description
[items]	Yes	Array of **MetricDataItem** objects	Metric parameters.

Table 4-243 MetricDataItem

Parameter	Mandatory	Type	Description
collect_time	Yes	Long	Data collection time (UNIX timestamp, in ms), which ranges from the last 24 hours to the next 0.5 hour. The following requirement needs to be met: Current UTC time – Data collection time ≤ 24 hours, or Data collection time – Current UTC time ≤ 30 minutes If the data reporting time is earlier than 08:00 of the current day, only the data generated after 08:00 of the current day is displayed on the metric monitoring page.
metric	Yes	**MetricItemInfo** object	Metric details.
values	Yes	Array of **ValueData** objects	Metric value.

Table 4-244 MetricItemInfo

Parameter	Mandatory	Type	Description
dimensions	Yes	Array of **Dimension2** objects	List of metric dimensions. A maximum of 50 dimensions are supported. Each dimension is in JSON format. The structure is as follows: dimension.name: 1–32 characters. dimension.value: 1–64 characters.
namespace	Yes	String	Metric namespace. It cannot contain colons (:). It must be in the format of "service.item". The value must contain 3 to 32 characters starting with a letter. Only letters, digits, and underscores (_) are allowed. In addition, "service" cannot be "PAAS". Minimum: **3** Maximum: **32**

Table 4-245 Dimension2

Parameter	Mandatory	Type	Description
name	Yes	String	Dimension name. Minimum: **1** Maximum: **32**
value	Yes	String	Dimension value. Minimum: **1** Maximum: **64**

Table 4-246 ValueData

Parameter	Mandatory	Type	Description
metric_name	Yes	String	Metric name. Length: 1 to 255 characters.

Parameter	Mandatory	Type	Description
type	No	String	Data type. Values: int and float. Enumeration values: • **int** • **float**
unit	No	String	Data unit. Length: up to 32 characters.
value	Yes	Double	Metric value, which must be of a valid numeric type. Minimum: **0**

Response Parameters

Status code: 200

Table 4-247 Response body parameters

Parameter	Type	Description
errorCode	String	Response code.
errorMessage	String	Response message.

Example Requests

Add a piece of monitoring data to the server. (In the following example, set "collect_time" to the latest timestamp.)

```
https://{Endpoint}/v1/{project_id}/ams/report/metricdata

[ {
  "metric" : {
    "namespace" : "NOPAAS.ESC",
    "dimensions" : [ {
      "name" : "instance_id",
      "value" : "instance-101"
    } ]
  },
  "values" : [ {
    "unit" : "percent",
    "metric_name" : "cpu_util",
    "type" : "int",
    "value" : 35
  } ],
  "collect_time" : 1467787152000
} ]
```

Example Responses

Status code: 200

OK: The request is successful.

```
{
  "errorCode" : "SVCSTG_AMS_2000000",
  "errorMessage" : "success"
}
```

Status Codes

Status Code	Description
200	OK: The request is successful.
400	Bad Request: The request is invalid. The client should not repeat the request without modifications.
401	Unauthorized: The authentication information is incorrect or invalid.
403	Forbidden: The request is rejected. The server has received the request and understood it, but the server refuses to respond to it. The client should not repeat the request without modifications.
500	Internal Server Error: The server is able to receive the request but unable to understand the request.
503	Service Unavailable: The requested service is invalid. The client should not repeat the request without modifications.

Error Codes

See **Error Codes**.

4.2.6 Adding or Modifying One or More Service Discovery Rules

Function

This API is used to add or modify one or more service discovery rules. A maximum of 100 rules can be added to a project.

Calling Method

For details, see **Calling APIs**.

URI

PUT /v1/{project_id}/inv/servicediscoveryrules

Table 4-248 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID obtained from IAM. Generally, a project ID contains 32 characters.

Request Parameters

Table 4-249 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token obtained from IAM.
Content-Type	Yes	String	Content type, which is application/json. Enumeration values: • **application/json**

Table 4-250 Request body parameters

Parameter	Mandatory	Type	Description
appRules	No	Array of **AppRules** objects	Service parameters.

Table 4-251 AppRules

Parameter	Mandatory	Type	Description
createTime	No	String	Creation time. When creating a service discovery rule, leave this parameter blank. When modifying a service discovery rule, enter the returned createTime. Default: **1599098476654**
enable	Yes	Boolean	Whether a rule is enabled. Values: true and false.

Parameter	Mandatory	Type	Description
eventName	Yes	String	aom_inventory_rules_event Rule event name. For service discovery, the fixed value is aom_inventory_rules_event.
hostid	No	Array of strings	Host ID. Currently, this parameter is not used and can be left blank.
id	Yes	String	Rule ID. When creating a service discovery rule, leave this parameter blank. When modifying a service discovery rule, enter a rule ID.
name	Yes	String	Rule name, which contains a maximum of 64 characters. It must start with a lowercase letter but cannot end with a hyphen (-). Only digits, lowercase letters, and hyphens are allowed.
projectid	Yes	String	Project ID obtained from IAM. Generally, a project ID contains 32 characters.
spec	Yes	**AppRulesSpec** object	Rule details.
desc	No	String	Custom description

Table 4-252 AppRulesSpec

Parameter	Mandatory	Type	Description
appType	Yes	String	Service type, which is used only for rule classification and UI display. You can enter any field. For example, enter Java or Python by technology stack, or enter collector or database by function.
attrList	No	Array of strings	Attribute list. Currently, this parameter is not used and can be left blank. Values: cmdLine and env.

Parameter	Mandatory	Type	Description
detectLog	Yes	String	Whether to enable log collection. Values: true and false.
discoveryRule	Yes	Array of **DiscoveryRule** objects	Discovery rule. If the array contains multiple conditions, only the processes that meet all the conditions will be matched. If the value of checkType is cmdLine, set the value of checkMode to contain. checkContent is in the format of ["xxx"], indicating that the process must contain the xxx parameter. If the value of checkType is env, set the value of checkMode to contain. checkContent is in the format of ["k1","v1"], indicating that the process must contain the environment variable whose name is k1 and value is v1. If the value of checkType is scope, set the value of checkMode to equals. checkContent is in the format of ["hostId1","hostId2"], indicating that the rule takes effect only on specified nodes. If no nodes are specified, the rule applies to all nodes of the project.
isDefaultRule	Yes	String	Whether the rule is the default one. Values: true and false.
isDetect	Yes	String	Whether the scenario is a pre-check scenario. No rules will be saved in the pre-check scenario. This scenario is designed only to check whether a rule can detect node processes before it is delivered. Values: true and false.
logFileFix	Yes	Array of strings	Log file suffix. Values: log, trace, and out.

Parameter	Mandatory	Type	Description
logPathRule	No	Array of **LogPathRule** objects	Log path configuration rule. If cmdLineHash is a fixed string, logs in the specified log path or log file are collected. Otherwise, only the files whose names end with .log or .trace are collected. If the value of nameType is cmdLineHash, args is in the format of ["00001"] and value is in the format of ["/xxx/xx.log"], indicating that the log path is /xxx/xx.log when the startup command is 00001.
nameRule	Yes	**NameRule** object	Naming rules for discovered services and applications.
priority	Yes	Integer	Rule priority. Value range: 1 to 9999. Default value: 9999.
dataSource	No	String	Data source.
editable	No	String	Whether to support editing. Options: true and false.
aom_metric_relabel_configs	No	Object	Metric configuration.

Table 4-253 DiscoveryRule

Parameter	Mandatory	Type	Description
checkContent	Yes	Array of strings	Matched value.
checkMode	Yes	String	Match condition. Values: contain and equals.
checkType	Yes	String	Match type. Values: cmdLine, env, and scope.

Table 4-254 LogPathRule

Parameter	Mandatory	Type	Description
args	Yes	Array of strings	Command.

Parameter	Mandatory	Type	Description
nameType	Yes	String	Value type, which can be cmdLineHash.
value	Yes	Array of strings	Log path.

Table 4-255 NameRule

Parameter	Mandatory	Type	Description
appNameRule	Yes	Array of **AppNameRule** objects	Service name rule. If there are multiple objects in the array, the character strings extracted from these objects constitute the service name. If the value of nameType is cmdLine, args is in the format of ["start", "end"], indicating that the characters between start and end in the command are extracted.If the value of nameType is cmdLine, args is in the format of ["aa"], indicating that the environment variable named aa is extracted.If the value of nameType is str, args is in the format of ["fix"], indicating that the service name is suffixed with fix.If the value of nameType is cmdLineHash, args is in the format of ["0001"] and value is in the format of ["ser"], indicating that the service name is ser when the startup command is 0001.

Parameter	Mandatory	Type	Description
applicationNameRule	Yes	Array of **ApplicationNameRule** objects	Application name rule.If the value of nameType is cmdLine, args is in the format of ["start", "end"], indicating that the characters between start and end in the command are extracted.If the value of nameType is cmdLine, args is in the format of ["aa"], indicating that the environment variable named aa is extracted.If the value of nameType is str, args is in the format of ["fix"], indicating that the service name is suffixed with fix.If the value of nameType is cmdLineHash, args is in the format of ["0001"] and value is in the format of ["ser"], indicating that the application name is ser when the startup command is 0001.

Table 4-256 AppNameRule

Parameter	Mandatory	Type	Description
nameType	Yes	String	Value type. Values: cmdLineHash, cmdLine, env, and str.
args	Yes	Array of strings	Input value.
value	No	Array of strings	Service name, which is mandatory only when the value of nameType is cmdLineHash.

Table 4-257 ApplicationNameRule

Parameter	Mandatory	Type	Description
nameType	Yes	String	Value type. Values: cmdLineHash, cmdLine, env, and str.

Parameter	Mandatory	Type	Description
args	Yes	Array of strings	Input value.
value	No	Array of strings	Service name, which is mandatory only when the value of nameType is cmdLineHash.

Response Parameters

Status code: 200

Table 4-258 Response body parameters

Parameter	Type	Description
errorCode	String	Response code.
errorMessage	String	Response message.
responseStatus	Integer	Response status code (no longer used).
id	Array of strings	Service discovery rule ID list. This parameter is used during cross-AZ configuration synchronization.
results	Array of Map<String,String> objects	Details about service discovery rules.

Example Requests

Add an application discovery rule whose name is **aom_inventory_rules_event** and project ID is **684fc87a79d7xxxx22e62a7da95b**.

```
https://{endpoint}/v1/{project_id}/inv/servicediscoveryrules

{
  "appRules" : [ {
    "createTime" : "1694705766730",
    "enable" : true,
    "name" : "ica**nt",
    "eventName" : "aom_inventory_rules_event",
    "hostid" : [ ],
    "id" : "b53a5152-****-****-****-302367e04c0b",
    "projectid" : "684fc87a79d7xxxx22e62a7da95b",
    "spec" : {
      "detectLog" : "true",
      "editable" : null,
      "logPathRule" : [ ],
      "priority" : 9999,
      "attrList" : [ "cmdLine" ],
      "nameRule" : {
```



```
      "appNameRule" : [ {
        "args" : [ "/opt/********* -DNFW=ica**nt" ],
        "nameType" : "cmdLineHash",
        "value" : [ "aicagentserver" ]
      } ],
      "applicationNameRule" : [ {
        "args" : [ "/opt/********** -DNFW=ica**nt" ],
        "nameType" : "cmdLineHash",
        "value" : [ "aica**nt" ]
      } ]
    },
    "appType" : "",
    "aom_metric_relabel_configs" : null,
    "logFileFix" : [ "log", "trace", "out" ],
    "isDetect" : "false",
    "isDefaultRule" : null,
    "dataSource" : null,
    "discoveryRule" : [ {
      "checkType" : "cmdLine",
      "checkContent" : [ "-DNFW=ica**nt" ],
      "checkMode" : "contain"
    } ]
   },
   "desc" : "Custom description"
  } ]
}
```

Example Responses

Status code: 200

OK: The request is successful.

```
{
  "errorCode" : "SVCSTG.INV.2000000",
  "errorMessage" : null,
  "id" : [ ],
  "results" : [ {
    "name" : "aom_inventory_rules_event",
    "id" : "b53a5152-****-****-****-302367e04c0b"
  } ]
}
```

Status code: 400

Bad Request: The request is invalid. The client should not repeat the request without modifications.

```
{
  "errorCode" : "SVCSTG.INV.4000115",
  "errorMessage" : "apprule name has existed",
  "id" : [ ],
  "results" : [ ]
}
```

Status Codes

Status Code	Description
200	OK: The request is successful.
400	Bad Request: The request is invalid. The client should not repeat the request without modifications.

Status Code	Description
401	Unauthorized: The authentication information is incorrect or invalid.
403	Forbidden: The request is rejected. The server has received the request and understood it, but the server refuses to respond to it. The client should not repeat the request without modifications.
500	Internal Server Error: The server is able to receive the request but unable to understand the request.
503	Service Unavailable: The requested service is invalid. The client should not repeat the request without modifications.

Error Codes

See **Error Codes**.

4.2.7 Deleting a Service Discovery Rule

Function

This API is used to delete a service discovery rule.

Calling Method

For details, see **Calling APIs**.

URI

DELETE /v1/{project_id}/inv/servicediscoveryrules

Table 4-259 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID obtained from IAM. Generally, a project ID contains 32 characters.

Table 4-260 Query Parameters

Parameter	Mandatory	Type	Description
appRulesIds	Yes	Array	Discovery rule ID. Multiple IDs need to be separated by commas (,). The parameter cannot be empty.

Request Parameters

Table 4-261 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token obtained from IAM.
Content-Type	Yes	String	Content type, which is application/json. Enumeration values: • **application/json**

Response Parameters

Status code: 200

Table 4-262 Response body parameters

Parameter	Type	Description
errorCode	String	Response code.
errorMessage	String	Response message.
responseStatus	Integer	Response status code (no longer used).
id	Array of strings	Service discovery rule ID list. This parameter is used during cross-AZ configuration synchronization.

Example Requests

Delete a service discovery rule with a specified ID.

```
https://{Endpoint}/v1/{project_id}/inv/servicediscoveryrules?appRulesIds=b788349e-62b2-xxxx-xxxx-02c611d59801
```

Example Responses

Status code: 200

OK: The request is successful.

```
{
  "errorCode" : "SVCSTG.INV.2000000",
  "errorMessage" : null,
  "id" : [ ]
}
```

Status code: 400

Bad Request: The request is invalid. The client should not repeat the request without modifications.

```
{
  "errorCode" : "SVCSTG.INV.40000118",
  "errorMessage" : "Request param is invalid",
  "trace_id" : ""
}
```

Status code: 404

Not Found: The requested resource could not be found. The client should not repeat this request without modification.

```
{
  "errorCode" : "SVCSTG.INV.4040000",
  "errorMessage" : "Inventory does not exists",
  "id" : [ ]
}
```

Status code: 500

Internal Server Error: The server is able to receive the request but unable to understand the request.

```
{
  "error_code" : "APM.00000500",
  "error_msg" : "Internal Server Error",
  "trace_id" : ""
}
```

Status Codes

Status Code	Description
200	OK: The request is successful.
400	Bad Request: The request is invalid. The client should not repeat the request without modifications.
401	Unauthorized: The authentication information is incorrect or invalid.
403	Forbidden: The request is rejected. The server has received the request and understood it, but the server refuses to respond to it. The client should not repeat the request without modifications.
404	Not Found: The requested resource could not be found. The client should not repeat this request without modification.
500	Internal Server Error: The server is able to receive the request but unable to understand the request.
503	Unauthorized: The authentication information is incorrect or invalid.

Error Codes

See **Error Codes**.

4.2.8 Querying Existing Service Discovery Rules

Function

This API is used to query existing service discovery rules in the system.

Calling Method

For details, see **Calling APIs**.

URI

GET /v1/{project_id}/inv/servicediscoveryrules

Table 4-263 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID obtained from IAM. Generally, a project ID contains 32 characters.

Table 4-264 Query Parameters

Parameter	Mandatory	Type	Description
id	No	String	Service discovery rule ID, which corresponds to a service discovery rule. If this parameter is left blank, all service discovery rules in the project are returned.

Request Parameters

Table 4-265 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token obtained from IAM.
Content-Type	Yes	String	Content type, which is application/json. Enumeration values: • **application/json**

Response Parameters

Status code: 200

Table 4-266 Response body parameters

Parameter	Type	Description
appRules	Array of **AppRules** objects	Rule information.
errorCode	String	Response code. AOM_INVENTORY_2000000: Success response.
errorMessage	String	Response message.
id	Array of strings	Service discovery rule ID list. This parameter is used during cross-AZ configuration synchronization.

Table 4-267 AppRules

Parameter	Type	Description
createTime	String	Creation time. When creating a service discovery rule, leave this parameter blank. When modifying a service discovery rule, enter the returned createTime. Default: **1599098476654**
enable	Boolean	Whether a rule is enabled. Values: true and false.
eventName	String	aom_inventory_rules_event Rule event name. For service discovery, the fixed value is aom_inventory_rules_event.
hostid	Array of strings	Host ID. Currently, this parameter is not used and can be left blank.
id	String	Rule ID. When creating a service discovery rule, leave this parameter blank. When modifying a service discovery rule, enter a rule ID.
name	String	Rule name, which contains a maximum of 64 characters. It must start with a lowercase letter but cannot end with a hyphen (-). Only digits, lowercase letters, and hyphens are allowed.
projectid	String	Project ID obtained from IAM. Generally, a project ID contains 32 characters.

Parameter	Type	Description
spec	**AppRulesSpec** object	Rule details.
desc	String	Custom description

Table 4-268 AppRulesSpec

Parameter	Type	Description
appType	String	Service type, which is used only for rule classification and UI display. You can enter any field. For example, enter Java or Python by technology stack, or enter collector or database by function.
attrList	Array of strings	Attribute list. Currently, this parameter is not used and can be left blank. Values: cmdLine and env.
detectLog	String	Whether to enable log collection. Values: true and false.
discoveryRule	Array of **DiscoveryRule** objects	Discovery rule. If the array contains multiple conditions, only the processes that meet all the conditions will be matched. If the value of checkType is cmdLine, set the value of checkMode to contain. checkContent is in the format of ["xxx"], indicating that the process must contain the xxx parameter. If the value of checkType is env, set the value of checkMode to contain. checkContent is in the format of ["k1","v1"], indicating that the process must contain the environment variable whose name is k1 and value is v1. If the value of checkType is scope, set the value of checkMode to equals. checkContent is in the format of ["hostId1","hostId2"], indicating that the rule takes effect only on specified nodes. If no nodes are specified, the rule applies to all nodes of the project.
isDefaultRule	String	Whether the rule is the default one. Values: true and false.
isDetect	String	Whether the scenario is a pre-check scenario. No rules will be saved in the pre-check scenario. This scenario is designed only to check whether a rule can detect node processes before it is delivered. Values: true and false.

Parameter	Type	Description
logFileFix	Array of strings	Log file suffix. Values: log, trace, and out.
logPathRule	Array of **LogPathRule** objects	Log path configuration rule. If cmdLineHash is a fixed string, logs in the specified log path or log file are collected. Otherwise, only the files whose names end with .log or .trace are collected. If the value of nameType is cmdLineHash, args is in the format of ["00001"] and value is in the format of ["/xxx/xx.log"], indicating that the log path is /xxx/xx.log when the startup command is 00001.
nameRule	**NameRule** object	Naming rules for discovered services and applications.
priority	Integer	Rule priority. Value range: 1 to 9999. Default value: 9999.
dataSource	String	Data source.
editable	String	Whether to support editing. Options: true and false.
aom_metric_relabel_configs	Object	Metric configuration.

Table 4-269 DiscoveryRule

Parameter	Type	Description
checkContent	Array of strings	Matched value.
checkMode	String	Match condition. Values: contain and equals.
checkType	String	Match type. Values: cmdLine, env, and scope.

Table 4-270 LogPathRule

Parameter	Type	Description
args	Array of strings	Command.
nameType	String	Value type, which can be cmdLineHash.
value	Array of strings	Log path.

Table 4-271 NameRule

Parameter	Type	Description
appNameRule	Array of **AppNameRule** objects	Service name rule. If there are multiple objects in the array, the character strings extracted from these objects constitute the service name. If the value of nameType is cmdLine, args is in the format of ["start", "end"], indicating that the characters between start and end in the command are extracted.If the value of nameType is cmdLine, args is in the format of ["aa"], indicating that the environment variable named aa is extracted.If the value of nameType is str, args is in the format of ["fix"], indicating that the service name is suffixed with fix.If the value of nameType is cmdLineHash, args is in the format of ["0001"] and value is in the format of ["ser"], indicating that the service name is ser when the startup command is 0001.
applicationNameRule	Array of **ApplicationNameRule** objects	Application name rule.If the value of nameType is cmdLine, args is in the format of ["start", "end"], indicating that the characters between start and end in the command are extracted.If the value of nameType is cmdLine, args is in the format of ["aa"], indicating that the environment variable named aa is extracted.If the value of nameType is str, args is in the format of ["fix"], indicating that the service name is suffixed with fix.If the value of nameType is cmdLineHash, args is in the format of ["0001"] and value is in the format of ["ser"], indicating that the application name is ser when the startup command is 0001.

Table 4-272 AppNameRule

Parameter	Type	Description
nameType	String	Value type. Values: cmdLineHash, cmdLine, env, and str.
args	Array of strings	Input value.
value	Array of strings	Service name, which is mandatory only when the value of nameType is cmdLineHash.

Table 4-273 ApplicationNameRule

Parameter	Type	Description
nameType	String	Value type. Values: cmdLineHash, cmdLine, env, and str.
args	Array of strings	Input value.
value	Array of strings	Service name, which is mandatory only when the value of nameType is cmdLineHash.

Example Requests

Query the application discovery rule whose ID is **-6066-****-8cc7-**.

```
https://{endpoint}/v1/{project_id}/inv/servicediscoveryrules?id=********-6066-****-8cc7-********
```

Example Responses

Status code: 200

OK: The request is successful.

```
{
  "appRules" : [ {
    "createTime" : "1694705814424",
    "enable" : true,
    "name" : "icaaant",
    "eventName" : "aom_inventory_rules_event",
    "hostid" : [ ],
    "id" : "********-6066-****-8cc7-********",
    "projectid" : "684fc87a79d7xxxx22e62a7da95b",
    "spec" : {
      "detectLog" : "true",
      "editable" : null,
      "logPathRule" : [ ],
      "priority" : 9999,
      "attrList" : [ "cmdLine" ],
      "nameRule" : {
        "appNameRule" : [ {
          "args" : [ "/opt/********* -DNFW=ica**nt" ],
          "nameType" : "cmdLineHash",
          "value" : [ "aicagentserver" ]
        } ],
        "applicationNameRule" : [ {
          "args" : [ "/opt/********** -DNFW=ica**nt" ],
          "nameType" : "cmdLineHash",
          "value" : [ "aica**nt" ]
        } ]
      },
      "appType" : "",
      "aom_metric_relabel_configs" : null,
      "logFileFix" : [ "log", "trace", "out" ],
      "isDetect" : "false",
      "isDefaultRule" : null,
      "dataSource" : null,
      "discoveryRule" : [ {
        "checkType" : "cmdLine",
        "checkContent" : [ "-DNFW=ica**nt" ],
        "checkMode" : "contain"
      } ]
```



```
    },
    "desc" : "Custom description"
  } ],
  "errorMessage" : null,
  "errorCode" : "SVCSTG.INV.2000000",
  "id" : [ ]
}
```

Status code: 404

Not Found: The requested resource could not be found. The client should not repeat this request without modification.

```
{
  "appRules" : [ ],
  "errorMessage" : "Inventory does not exists",
  "errorCode" : "SVCSTG.INV.4040000",
  "id" : [ ]
}
```

Status Codes

Status Code	Description
200	OK: The request is successful.
400	Bad Request: The request is invalid. The client should not repeat the request without modifications.
401	Unauthorized: The authentication information is incorrect or invalid.
403	Forbidden: The request is rejected. The server has received the request and understood it, but the server refuses to respond to it. The client should not repeat the request without modifications.
404	Not Found: The requested resource could not be found. The client should not repeat this request without modification.
500	Internal Server Error: The server is able to receive the request but unable to understand the request.
503	Service Unavailable: The requested service is invalid. The client should not repeat the request without modifications.

Error Codes

See **Error Codes**.

4.2.9 Adding a Threshold Rule

Function

This API is used to add a threshold rule.

Calling Method

For details, see **Calling APIs**.

URI

POST /v2/{project_id}/alarm-rules

Table 4-274 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID obtained from IAM. Generally, a project ID contains 32 characters.

Request Parameters

Table 4-275 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token obtained from IAM.
Content-Type	Yes	String	Content type, which is application/json. Enumeration values: • **application/json**

Table 4-276 Request body parameters

Parameter	Mandatory	Type	Description
action_enabled	No	Boolean	Whether to enable notification.
alarm_actions	No	Array of strings	List of alarm notifications.
alarm_advice	No	String	Alarm clearance suggestion. Minimum: **0** Maximum: **255**
alarm_description	No	String	Threshold rule description. Minimum: **0** Maximum: **1024**

Parameter	Mandatory	Type	Description
alarm_level	Yes	Integer	Alarm severity. Values: 1 (critical), 2 (major), 3 (minor), and 4 (warning). Enumeration values: • **1** • **2** • **3** • **4**
alarm_rule_name	Yes	String	Threshold rule name. Enter a maximum of 100 characters and do not start or end with a special character. Only letters, digits, underscores (_), and hyphens (-) are allowed.
comparison_operator	Yes	String	Comparison operator. Options: <: less than the threshold; >: greater than the threshold; <=: less than or equal to the threshold; >=: greater than or equal to the threshold. Enumeration values: • **<** • **>** • **<=** • **>=**
dimensions	Yes	Array of **Dimension** objects	List of time series dimensions.
evaluation_periods	Yes	Integer	Interval. Minimum: **1** Maximum: **5**
is_turn_on	No	Boolean	Whether to enable the threshold rule.
insufficient_data_actions	No	Array of strings	List of insufficient data notifications.
metric_name	Yes	String	Time series name. Length: 1 to 255 characters.
namespace	Yes	String	Time series objects' namespace.

Parameter	Mandatory	Type	Description
ok_actions	No	Array of strings	List of normal status notifications.
period	Yes	Integer	Statistical period. Options: 60000: one minute; 300000: five minutes; 900000: 15 minutes; 3600000: one hour. Enumeration values: • **60000** • **300000** • **900000** • **3600000**
statistic	Yes	String	Statistic. Enumeration values: • **maximum** • **minimum** • **average** • **sum** • **sampleCount**
threshold	Yes	String	Threshold value.
unit	Yes	String	Time series unit.

Table 4-277 Dimension

Parameter	Mandatory	Type	Description
name	Yes	String	Dimension name.
value	Yes	String	Dimension value.

Response Parameters

Status code: 200

Table 4-278 Response body parameters

Parameter	Type	Description
alarm_rule_id	Long	Threshold rule ID.

Status code: 400

Table 4-279 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
error_type	String	Error type.
trace_id	String	Trace ID, which is used to search for logs and locate faults. If **2xx** is returned, **trace_id** is empty. If **4xx**, **trace_id** is not empty.

Status code: 500

Table 4-280 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
error_type	String	Error type.
trace_id	String	Trace ID, which is used to search for logs and locate faults. If **2xx** is returned, **trace_id** is empty. If **4xx**, **trace_id** is not empty.

Example Requests

Add a threshold rule whose name is **testaom**, alarm severity is **3**, namespace is **PAAS.CONTAINER**, and statistical mode is **average**.

```
https://{Endpoint}/v2/{project_id}/alarm-rules

{
  "is_turn_on" : true,
  "action_enabled" : false,
  "alarm_actions" : [ ],
  "alarm_advice" : "",
  "alarm_description" : "",
  "alarm_level" : 3,
  "alarm_rule_name" : "aom_rule",
  "comparison_operator" : ">=",
  "dimensions" : [ {
    "name" : "appName",
    "value" : "rhm-broker"
  } ],
  "evaluation_periods" : 1,
  "insufficient_data_actions" : [ ],
  "metric_name" : "cpuCoreLimit",
  "namespace" : "PAAS.CONTAINER",
  "ok_actions" : [ ],
  "period" : 60000,
  "statistic" : "average",
  "threshold" : 0,
```



```
  "unit" : "Core"
}
```

Example Responses

Status code: 200

OK: The request is successful.

```
{
  "alarm_rule_id" : 1134050083814244400
}
```

Status code: 400

Bad Request: The request is invalid. The client should not repeat the request without modifications.

```
{
  "error_code" : "AOM.02001102",
  "error_msg" : "this Threshold rule name has been existed",
  "error_type" : "BAD_REQUEST",
  "trace_id" : ""
}
```

Status code: 500

Internal Server Error: The server is able to receive the request but unable to understand the request.

```
{
  "error_code" : "AOM.02001500",
  "error_msg" : "internal server error",
  "error_type" : "INTERNAL_SERVER_ERROR",
  "trace_id" : ""
}
```

Status Codes

Status Code	Description
200	OK: The request is successful.
400	Bad Request: The request is invalid. The client should not repeat the request without modifications.
401	Unauthorized: The authentication information is incorrect or invalid.
403	Forbidden: The request is rejected. The server has received the request and understood it, but the server refuses to respond to it. The client should not repeat the request without modifications.
500	Internal Server Error: The server is able to receive the request but unable to understand the request.
503	Service Unavailable: The requested service is invalid. The client should not repeat the request without modifications.

Error Codes

See **Error Codes**.

4.2.10 Querying the Threshold Rule List

Function

This API is used to query the threshold rule list.

Calling Method

For details, see **Calling APIs**.

URI

GET /v2/{project_id}/alarm-rules

Table 4-281 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID obtained from IAM. Generally, a project ID contains 32 characters.

Table 4-282 Query Parameters

Parameter	Mandatory	Type	Description
offset	No	String	Pagination information.
limit	No	Integer	Maximum number of returned records. Value range: 1–1000. Default value: 1000.

Request Parameters

Table 4-283 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token obtained from IAM.
Content-Type	Yes	String	Content type, which is application/json. Enumeration values: • **application/json**

Response Parameters

Status code: 200

Table 4-284 Response body parameters

Parameter	Type	Description
meta_data	**MetaData** object	Metadata, including pagination information.
thresholds	Array of **QueryAlarmResult** objects	Parameters specified for querying a threshold rule.

Table 4-285 MetaData

Parameter	Type	Description
count	Integer	Number of returned records.
start	String	Start of the next page, which is used for pagination. null: No more data.
total	Integer	Total number of records.

Table 4-286 QueryAlarmResult

Parameter	Type	Description
action_enabled	Boolean	Whether to enable notification.
alarm_actions	Array of strings	List of alarm notifications.
alarm_advice	String	Alarm clearance suggestion.
alarm_description	String	Threshold rule description.
alarm_level	String	Alarm severity.
alarm_rule_id	String	Threshold rule ID.
alarm_rule_name	String	Threshold rule name.
comparison_operator	String	Comparison operator.

Parameter	Type	Description
dimensions	Array of **Dimension** objects	List of time series dimensions.
evaluation_periods	Integer	Interval.
id_turn_on	Boolean	Whether to enable the threshold rule.
insufficient_data_actions	Array of strings	List of insufficient data notifications.
metric_name	String	Time series name.
namespace	String	Time series objects' namespace.
ok_actions	Array of strings	List of normal status notifications.
period	Integer	Statistical period.
policy_name	String	Threshold rule name.
resources	Array of strings	Resource information (discarded).
state_reason	String	Cause description.
state_updated_timestamp	String	Time when the status was updated.
state_value	String	Service status.
statistic	String	Statistic.
threshold	String	Threshold value.
type	String	Threshold rule type.
unit	String	Threshold unit.

Table 4-287 Dimension

Parameter	Type	Description
name	String	Dimension name.
value	String	Dimension value.

Status code: 400

Table 4-288 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
error_type	String	Error type.
trace_id	String	Trace ID, which is used to search for logs and locate faults. If **2xx** is returned, **trace_id** is empty. If **4xx**, **trace_id** is not empty.

Example Requests

Obtain the alarm rule list of a user whose ID is **Project_Id**.

```
https://{EndPoint_Id}/v2/{Project_Id}/alarm-rules
```

Example Responses

Status code: 200

OK: The request is successful.

```
{
  "meta_data" : [ {
    "count" : 10,
    "total" : 100
  } ],
  "thresholds" : [ {
    "action_enable" : false,
    "alarm_actions" : null,
    "alarm_advice" : null,
    "alarm_description" : null,
    "alarm_level" : 3,
    "alarm_rule_id" : 2137,
    "alarm_rule_name" : "aom_rule",
    "comparison_operator" : ">=",
    "dimensions" : [ {
      "name" : "appName"
    }, {
      "value" : "rhm-broker"
    } ],
    "evaluation_periods" : 1,
    "id_turn_on" : true,
    "insufficient_data_actions" : null,
    "metric_name" : "cpuCoreLimit",
    "namespace" : "PAAS.CONTAINER",
    "ok_actions" : null,
    "period" : 60000,
    "policy_name" : "23,",
    "resources" : [ ],
    "state_reason" : null,
    "state_updated_timestamp" : null,
    "state_value" : "alarm",
    "statistic" : "average",
    "threshold" : 0,
    "type" : "single,",
    "unit" : "Core"
  } ]
}
```


Status code: 400

Bad Request: The request is invalid. The client should not repeat the request without modifications.

```
{
  "error_code" : "AOM.02003SVCSTG_AMS_4000123",
  "error_msg" : "The rule does not exist",
  "error_type" : "BAD_REQUEST",
  "trace_id" : ""
}
```

Status Codes

Status Code	Description
200	OK: The request is successful.
400	Bad Request: The request is invalid. The client should not repeat the request without modifications.
401	Unauthorized: The authentication information is incorrect or invalid.
403	Forbidden: The request is rejected. The server has received the request and understood it, but the server refuses to respond to it. The client should not repeat the request without modifications.
500	Internal Server Error: The server is able to receive the request but unable to understand the request.
503	Service Unavailable: The requested service is invalid. The client should not repeat the request without modifications.

Error Codes

See **Error Codes**.

4.2.11 Modifying a Threshold Rule

Function

This API is used to modify a threshold rule.

Calling Method

For details, see **Calling APIs**.

URI

PUT /v2/{project_id}/alarm-rules

Table 4-289 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID obtained from IAM. Generally, a project ID contains 32 characters.

Request Parameters

Table 4-290 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token obtained from IAM.
Content-Type	Yes	String	Content type, which is application/json. Enumeration values: • **application/json**

Table 4-291 Request body parameters

Parameter	Mandatory	Type	Description
action_enabled	No	Boolean	Whether to enable notification.
alarm_actions	No	Array of strings	List of alarm notifications.
alarm_advice	No	String	Alarm clearance suggestion, which contains a maximum of 255 characters. Minimum: **0** Maximum: **255**
alarm_description	No	String	Threshold rule description, which contains a maximum of 1024 characters. Minimum: **0** Maximum: **1024**

Parameter	Mandatory	Type	Description
alarm_level	Yes	Integer	Alarm severity. Values: 1 (critical), 2 (major), 3 (minor), and 4 (warning). Enumeration values: • **1** • **2** • **3** • **4**
alarm_rule_name	Yes	String	Threshold rule name. Enter a maximum of 100 characters and do not start or end with a special character. Only letters, digits, underscores (_), and hyphens (-) are allowed.
comparison_operator	Yes	String	Comparison operator. Options: <: less than the threshold; >: greater than the threshold; <=: less than or equal to the threshold; >=: greater than or equal to the threshold. Enumeration values: • **<** • **>** • **<=** • **>=**
dimensions	Yes	Array of **Dimension** objects	List of time series dimensions.
evaluation_periods	Yes	Integer	Interval at which data is calculated.
is_turn_on	No	Boolean	Whether to enable the threshold rule.
insufficient_data_actions	No	Array of strings	List of insufficient data notifications.
metric_name	Yes	String	Time series name. Length: 1 to 255 characters.
namespace	Yes	String	Namespace of time series objects.
ok_actions	No	Array of strings	List of normal status notifications.

Parameter	Mandatory	Type	Description
period	Yes	Integer	Statistical period. Options: 60000: one minute; 300000: five minutes; 900000: 15 minutes; 3600000: one hour. Enumeration values: • **60000** • **300000** • **900000** • **3600000**
statistic	Yes	String	Statistic. Enumeration values: • **maximum** • **minimum** • **average** • **sum** • **sampleCount**
threshold	Yes	String	Threshold.
unit	Yes	String	Time series unit.

Table 4-292 Dimension

Parameter	Mandatory	Type	Description
name	Yes	String	Dimension name.
value	Yes	String	Dimension value.

Response Parameters

Status code: 200

Table 4-293 Response body parameters

Parameter	Type	Description
alarm_rule_id	Long	Threshold rule ID.

Status code: 400

Table 4-294 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
error_type	String	Error type.
trace_id	String	Trace ID, which is used to search for logs and locate faults. If **2xx** is returned, **trace_id** is empty. If **4xx**, **trace_id** is not empty.

Example Requests

Modify a threshold rule whose name is **testaom**, alarm severity is **3**, metric name is **cpuCoreLimit**, and namespace is **PAAS.CONTAINER**.

```
https://{Endpoint}/v2/{project_id}/alarm-rules

{
  "action_enabled" : false,
  "alarm_actions" : [ ],
  "alarm_advice" : "",
  "alarm_description" : "",
  "alarm_level" : 3,
  "alarm_rule_name" : "aom_rule",
  "comparison_operator" : ">=",
  "dimensions" : [ {
    "name" : "appName",
    "value" : "rhm-broker"
  } ],
  "evaluation_periods" : 1,
  "insufficient_data_actions" : [ ],
  "metric_name" : "cpuCoreLimit",
  "namespace" : "PAAS.CONTAINER",
  "ok_actions" : [ ],
  "period" : 60000,
  "statistic" : "average",
  "threshold" : 0,
  "unit" : "Core"
}
```

Example Responses

Status code: 200

OK: The request is successful.

```
{
  "alarm_rule_id" : 91307490000416600
}
```

Status code: 400

Bad Request: The request is invalid. The client should not repeat the request without modifications.

```
{
  "error_code" : "AOM.02002SVCSTG_AMS_4000101",
  "error_msg" : "Invalid alarm name",
```



```
  "error_type" : "BAD_REQUEST",
  "trace_id" : ""
}
```

Status Codes

Status Code	Description
200	OK: The request is successful.
400	Bad Request: The request is invalid. The client should not repeat the request without modifications.
401	Unauthorized: The authentication information is incorrect or invalid.
403	Forbidden: The request is rejected. The server has received the request and understood it, but the server refuses to respond to it. The client should not repeat the request without modifications.
500	Internal Server Error: The server is able to receive the request but unable to understand the request.
503	Service Unavailable: The requested service is invalid. The client should not repeat the request without modifications.

Error Codes

See **Error Codes**.

4.2.12 Deleting a Threshold Rule

Function

This API is used to delete a threshold rule.

Calling Method

For details, see **Calling APIs**.

URI

DELETE /v2/{project_id}/alarm-rules/{alarm_rule_id}

Table 4-295 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID obtained from IAM. Generally, a project ID contains 32 characters.
alarm_rule_id	Yes	String	Threshold rule ID.

Request Parameters

Table 4-296 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token obtained from IAM.
Content-Type	Yes	String	Content type, which is application/json. Enumeration values: • **application/json**

Response Parameters

Status code: 400

Table 4-297 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
error_type	String	Error type.
trace_id	String	Trace ID, which is used to search for logs and locate faults. If **2xx** is returned, **trace_id** is empty. If **4xx**, **trace_id** is not empty.

Example Requests

Delete a threshold rule.

```
https://{Endpoint}/v2/{project_id}/alarm-rules/{alarm_rule_id}
```

Example Responses

Status code: 400

Bad Request: The request is invalid. The client should not repeat the request without modifications.

```
{
  "error_code" : "AOM.02005115",
  "error_msg" : "Invalid request parameter",
  "error_type" : "BAD_REQUEST",
  "trace_id" : ""
}
```


Status Codes

Status Code	Description
200	OK: The request is successful.
400	Bad Request: The request is invalid. The client should not repeat the request without modifications.
401	Unauthorized: The authentication information is incorrect or invalid.
403	Forbidden: The request is rejected. The server has received the request and understood it, but the server refuses to respond to it. The client should not repeat the request without modifications.
500	Internal Server Error: The server is able to receive the request but unable to understand the request.
503	Service Unavailable: The requested service is invalid. The client should not repeat the request without modifications.

Error Codes

See **Error Codes**.

4.2.13 Querying a Threshold Rule

Function

This API is used to query a threshold rule.

Calling Method

For details, see **Calling APIs**.

URI

GET /v2/{project_id}/alarm-rules/{alarm_rule_id}

Table 4-298 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID obtained from IAM. Generally, a project ID contains 32 characters.
alarm_rule_id	Yes	String	Threshold rule ID.

Request Parameters

Table 4-299 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token obtained from IAM.
Content-Type	Yes	String	Content type, which is application/json. Enumeration values: • **application/json**

Response Parameters

Status code: 200

Table 4-300 Response body parameters

Parameter	Type	Description
meta_data	**MetaData** object	Metadata, including pagination information.
thresholds	Array of **QueryAlarmResult** objects	Threshold rule list.

Table 4-301 MetaData

Parameter	Type	Description
count	Integer	Number of returned records.
start	String	Start of the next page, which is used for pagination. null: No more data.
total	Integer	Total number of records.

Table 4-302 QueryAlarmResult

Parameter	Type	Description
action_enabled	Boolean	Whether to enable notification.
alarm_actions	Array of strings	List of alarm notifications.

Parameter	Type	Description
alarm_advice	String	Alarm clearance suggestion.
alarm_description	String	Threshold rule description.
alarm_level	String	Alarm severity.
alarm_rule_id	String	Threshold rule ID.
alarm_rule_name	String	Threshold rule name.
comparison_operator	String	Comparison operator.
dimensions	Array of **Dimension** objects	List of time series dimensions.
evaluation_periods	Integer	Interval.
id_turn_on	Boolean	Whether to enable the threshold rule.
insufficient_data_actions	Array of strings	List of insufficient data notifications.
metric_name	String	Time series name.
namespace	String	Time series objects' namespace.
ok_actions	Array of strings	List of normal status notifications.
period	Integer	Statistical period.
policy_name	String	Threshold rule name.
resources	Array of strings	Resource information (discarded).
state_reason	String	Cause description.
state_updated_timestamp	String	Time when the status was updated.
state_value	String	Service status.
statistic	String	Statistic.
threshold	String	Threshold value.
type	String	Threshold rule type.
unit	String	Threshold unit.

Table 4-303 Dimension

Parameter	Type	Description
name	String	Dimension name.
value	String	Dimension value.

Status code: 400

Table 4-304 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
error_type	String	Error type.
trace_id	String	Trace ID, which is used to search for logs and locate faults. If **2xx** is returned, **trace_id** is empty. If **4xx**, **trace_id** is not empty.

Example Requests

Obtain the details about the alarm rule whose ID is **alarm_rule_id**.

```
https://{Endpoint}/v2/{project_id}/alarm-rules/{alarm_rule_id}
```

Example Responses

Status code: 200

OK: The request is successful.


```
{
  "meta_data" : {
    "count" : 1,
    "start" : null,
    "total" : 1
  },
  "thresholds" : [ {
    "action_enabled" : false,
    "alarm_actions" : null,
    "alarm_advice" : null,
    "alarm_description" : null,
    "alarm_level" : "3",
    "alarm_rule_id" : 2137,
    "alarm_rule_name" : "aom_rule",
    "comparison_operator" : ">=",
    "dimensions" : [ {
      "name" : "appName"
    }, {
      "value" : "rhm-broker"
    } ],
    "evaluation_periods" : 1,
    "id_turn_on" : true,
```

```
    "insufficient_data_actions" : null,
    "metric_name" : "cpuCoreLimit",
    "namespace" : "PAAS.CONTAINER",
    "ok_actions" : null,
    "period" : 60000,
    "policy_name" : "23,",
    "resources" : [ ],
    "state_reason" : null,
    "state_updated_timestamp" : null,
    "statistic" : "average",
    "threshold" : 0,
    "type" : "single,",
    "unit" : "Core"
  } ]
}
```


Status code: 400

Bad Request: The request is invalid. The client should not repeat the request without modifications.


```
{
  "error_code" : "AOM.02004115",
  "error_msg" : "Invalid request parameter",
  "error_type" : "BAD_REQUEST",
  "trace_id" : ""
}
```


Status Codes

Status Code	Description
200	OK: The request is successful.
400	Bad Request: The request is invalid. The client should not repeat the request without modifications.
401	Unauthorized: The authentication information is incorrect or invalid.
403	Forbidden: The request is rejected. The server has received the request and understood it, but the server refuses to respond to it. The client should not repeat the request without modifications.
500	Internal Server Error: The server is able to receive the request but unable to understand the request.
503	Service Unavailable: The requested service is invalid. The client should not repeat the request without modifications.

Error Codes

See **Error Codes**.

4.2.14 Deleting Threshold Rules in Batches

Function

This API is used to delete threshold rules in batches.

Calling Method

For details, see **Calling APIs**.

URI

POST /v2/{project_id}/alarm-rules/delete

Table 4-305 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID obtained from IAM. Generally, a project ID contains 32 characters.

Request Parameters

Table 4-306 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token obtained from IAM.
Content-Type	Yes	String	Content type, which is application/json. Enumeration values: • **application/json**

Table 4-307 Request body parameters

Parameter	Mandatory	Type	Description
alarm_rules	Yes	Array of strings	Name of the rule to be deleted.

Response Parameters

Status code: 400

Table 4-308 Response body parameters

Parameter	Type	Description
error_code	String	Error code.

Parameter	Type	Description
error_msg	String	Error message.
error_type	String	Error type.
trace_id	String	Trace ID, which is used to search for logs and locate faults. If **2xx** is returned, **trace_id** is empty. If **4xx**, **trace_id** is not empty.

Example Requests

Delete threshold rules in batches by rule name.

```
https://{Endpoint}/v2/{project_id}/alarm-rules/delete

{
  "alarm_rules" : [ ]
}
```

Example Responses

Status code: 400

Bad Request: The request is invalid. The client should not repeat the request without modifications.

```
{
  "error_code" : "AOM.02005115",
  "error_msg" : "Invalid request parameter",
  "error_type" : "BAD_REQUEST",
  "trace_id" : ""
}
```

Status Codes

Status Code	Description
200	OK: The request is successful.
400	Bad Request: The request is invalid. The client should not repeat the request without modifications.
401	Unauthorized: The authentication information is incorrect or invalid.
403	Forbidden: The request is rejected. The server has received the request and understood it, but the server refuses to respond to it. The client should not repeat the request without modifications.
500	Internal Server Error: The server is able to receive the request but unable to understand the request.
503	Service Unavailable: The requested service is invalid. The client should not repeat the request without modifications.

Error Codes

See **Error Codes**.

4.3 Prometheus Monitoring

4.3.1 Querying Expression Calculation Results in a Specified Period Using the GET Method

Function

This API is used to query the calculation results of a PromQL expression in a specified period using the GET method.

Calling Method

For details, see **Calling APIs**.

URI

GET /v1/{project_id}/aom/api/v1/query_range

Table 4-309 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID obtained from IAM. Generally, a project ID contains 32 characters.

Table 4-310 Query Parameters

Parameter	Mandatory	Type	Description
query	Yes	String	PromQL expression. For details, see https://prometheus.io/docs/prometheus/latest/querying/basics/.
start	Yes	String	Start timestamp (Unix timestamp, in seconds).
end	Yes	String	End timestamp (Unix timestamp, in seconds).

Parameter	Mandatory	Type	Description
step	Yes	String	Query step (in seconds). The task is executed on the step basis within the specified period.

Request Parameters

Table 4-311 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token obtained from IAM.

Response Parameters

Status code: 200

Table 4-312 Response body parameters

Parameter	Type	Description
status	String	Response status.
data	Object	Response data.

Status code: 400

Table 4-313 Response body parameters

Parameter	Type	Description
status	String	Response status.
errorType	String	Error type.
error	String	Error message.

Status code: 403

Table 4-314 Response body parameters

Parameter	Type	Description
status	String	Response status.
errorType	String	Error type.
error	String	Error message.

Status code: 422

Table 4-315 Response body parameters

Parameter	Type	Description
status	String	Response status.
errorType	String	Error type.
error	String	Error message.

Status code: 503

Table 4-316 Response body parameters

Parameter	Type	Description
status	String	Response status.
errorType	String	Error type.
error	String	Error message.

Example Requests

Query the calculation result of PromQL expression "up" every 15s in a specified period.

```
https://{EndPoint}/v1/{project_id}/aom/api/v1/query_range?
query=up&start=1630124012&end=1630127612&step=15s
```

Example Responses

Status code: 200

OK: The request is successful.

```
{
  "status" : "success",
  "data" : {
    "resultType" : "matrix",
    "result" : [ {
```



```
    "metric" : {
      "__name__" : "up",
      "job" : "prometheus",
      "instance" : "localhost:9090"
    },
    "values" : [ [ 1.435781430781E9, "1" ], [ 1.435781445781E9, "1" ], [ 1.435781460781E9, "1" ] ]
  }, {
    "metric" : {
      "__name__" : "up",
      "job" : "node",
      "instance" : "localhost:9091"
    },
    "values" : [ [ 1.435781430781E9, "0" ], [ 1.435781445781E9, "0" ], [ 1.435781460781E9, "1" ] ]
  } ]
 }
}
```


Status code: 400

Bad Request: The request is invalid. The client should not repeat the request without modifications.


```
{
 "status" : "error",
 "errorType" : "bad_param",
 "error" : "param is invalid."
}
```


Status code: 403

Forbidden: The request is rejected. The server has received the request and understood it, but the server refuses to respond to it. The client should not repeat the request without modifications.


```
{
 "status" : "error",
 "errorType" : "auth",
 "error" : "auth project_id not pass."
}
```


Status code: 422

Unprocessable: The expression cannot be executed.


```
{
 "status" : "error",
 "errorType" : "excution",
 "error" : "expression can't be executed."
}
```


Status code: 503

Service Unavailable: The requested service is invalid. The client should not repeat the request without modifications.


```
{
 "status" : "error",
 "errorType" : "timeout",
 "error" : "query timed out in query execution."
}
```


Status Codes

Status Code	Description
200	OK: The request is successful.
400	Bad Request: The request is invalid. The client should not repeat the request without modifications.
403	Forbidden: The request is rejected. The server has received the request and understood it, but the server refuses to respond to it. The client should not repeat the request without modifications.
422	Unprocessable: The expression cannot be executed.
503	Service Unavailable: The requested service is invalid. The client should not repeat the request without modifications.

Error Codes

See **Error Codes**.

4.3.2 (Recommended) Querying Expression Calculation Results in a Specified Period Using the POST Method

Function

This API is used to query the calculation results of a PromQL expression in a specified period using the POST method.

Calling Method

For details, see **Calling APIs**.

URI

POST /v1/{project_id}/aom/api/v1/query_range

Table 4-317 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID obtained from IAM. Generally, a project ID contains 32 characters.

Table 4-318 Query Parameters

Parameter	Mandatory	Type	Description
query	Yes	String	PromQL expression. For details, see https://prometheus.io/docs/prometheus/latest/querying/basics/.
start	Yes	String	Start timestamp (Unix timestamp, in seconds).
end	Yes	String	End timestamp (Unix timestamp, in seconds).
step	Yes	String	Query step (in seconds). The task is executed on the step basis within the specified period.

Request Parameters

Table 4-319 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token obtained from IAM.

Response Parameters

Status code: 200

Table 4-320 Response body parameters

Parameter	Type	Description
status	String	Response status.
data	Object	Response data.

Status code: 400

Table 4-321 Response body parameters

Parameter	Type	Description
status	String	Response status.

Parameter	Type	Description
errorType	String	Error type.
error	String	Error message.

Status code: 403

Table 4-322 Response body parameters

Parameter	Type	Description
status	String	Response status.
errorType	String	Error type.
error	String	Error message.

Status code: 422

Table 4-323 Response body parameters

Parameter	Type	Description
status	String	Response status.
errorType	String	Error type.
error	String	Error message.

Status code: 503

Table 4-324 Response body parameters

Parameter	Type	Description
status	String	Response status.
errorType	String	Error type.
error	String	Error message.

Example Requests

Query the top N aom_node_status metrics on the step basis in a specified period.

```
https://{EndPoint}/v1/{project_id}/aom/api/v1/query_range?
query=topk(2,aom_node_status)&start=1630386780&end=1630390380&step=15
```


Example Responses

Status code: 200

OK: The request is successful.


```
{
  "status" : "success",
  "data" : {
    "resultType" : "matrix",
    "result" : [ {
      "metric" : {
        "__name__" : "amm_node_status",
        "clusterId" : "000000-0000-0000-0000-0000000",
        "hostID" : "c9xxcb-2x6c-4h54-8fcd-f68xx85",
        "nameSpace" : "default",
        "nodeIP" : "1xx.1xx.0.1xx",
        "nodeName" : "sis-xxn-amm"
      },
      "values" : [ [ 1630386780, "0" ], [ 1630388610, "0" ], [ 1630388625, "0" ] ]
    }, {
      "metric" : {
        "__name__" : "amm_node_status",
        "clusterId" : "00000000-0000-0000-0000-00000000",
        "hostID" : "ec5xxxb-0xx8-4xxx-bxx-9ecxxf",
        "nameSpace" : "default",
        "nodeIP" : "1xx.168.0.1x",
        "nodeName" : "fdx-ibxxst"
      },
      "values" : [ [ 1630388265, "0" ], [ 1630388280, "0" ], [ 1630388295, "0" ] ]
    } ]
  }
}
```


Status code: 400

Bad Request: The request is invalid. The client should not repeat the request without modifications.


```
{
  "status" : "error",
  "errorType" : "bad_param",
  "error" : "param is invalid."
}
```


Status code: 403

Forbidden: The request is rejected. The server has received the request and understood it, but the server refuses to respond to it. The client should not repeat the request without modifications.


```
{
  "status" : "error",
  "errorType" : "auth",
  "error" : "auth project_id not pass."
}
```


Status code: 422

Unprocessable: The expression cannot be executed.


```
{
  "status" : "error",
  "errorType" : "excution",
  "error" : "expression can't be executed."
}
```


Status code: 503

Service Unavailable: The requested service is invalid. The client should not repeat the request without modifications.

```
{
  "status" : "error",
  "errorType" : "timeout",
  "error" : "query timed out in query execution."
}
```

Status Codes

Status Code	Description
200	OK: The request is successful.
400	Bad Request: The request is invalid. The client should not repeat the request without modifications.
403	Forbidden: The request is rejected. The server has received the request and understood it, but the server refuses to respond to it. The client should not repeat the request without modifications.
422	Unprocessable: The expression cannot be executed.
503	Service Unavailable: The requested service is invalid. The client should not repeat the request without modifications.

Error Codes

See **Error Codes**.

4.3.3 Querying the Expression Calculation Result at a Specified Time Point Using the GET Method

Function

This API is used to query the calculation result of a PromQL expression at a specified time point using the GET method.

Calling Method

For details, see **Calling APIs**.

URI

GET /v1/{project_id}/aom/api/v1/query

Table 4-325 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID obtained from IAM. Generally, a project ID contains 32 characters.

Table 4-326 Query Parameters

Parameter	Mandatory	Type	Description
query	Yes	String	PromQL expression. For details, see https://prometheus.io/docs/prometheus/latest/querying/basics/.
time	No	String	Timestamp specified for PromQL calculation (Unix timestamp, in seconds).

Request Parameters

Table 4-327 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token obtained from IAM.

Response Parameters

Status code: 200

Table 4-328 Response body parameters

Parameter	Type	Description
status	String	Response status.
data	Object	Response data.

Status code: 400

Table 4-329 Response body parameters

Parameter	Type	Description
status	String	Response status.
errorType	String	Error type.
error	String	Error message.

Status code: 403

Table 4-330 Response body parameters

Parameter	Type	Description
status	String	Response status.
errorType	String	Error type.
error	String	Error message.

Status code: 422

Table 4-331 Response body parameters

Parameter	Type	Description
status	String	Response status.
errorType	String	Error type.
error	String	Error message.

Status code: 503

Table 4-332 Response body parameters

Parameter	Type	Description
status	String	Response status.
errorType	String	Error type.
error	String	Error message.

Example Requests

Query the calculation result of expression "up" at time point "1630124012".


```
https://{EndPoint}/v1/{project_id}/aom/api/v1/query?query=up&time=1630124012
```

Example Responses

Status code: 200

OK: The request is successful.

```
{
  "status" : "success",
  "data" : {
    "resultType" : "vector",
    "result" : [ ]
  }
}
```

Status code: 400

Bad Request: The request is invalid. The client should not repeat the request without modifications.

```
{
  "status" : "error",
  "errorType" : "bad_param",
  "error" : "param is invalid."
}
```

Status code: 403

Forbidden: The request is rejected. The server has received the request and understood it, but the server refuses to respond to it. The client should not repeat the request without modifications.

```
{
  "status" : "error",
  "errorType" : "auth",
  "error" : "auth project_id not pass."
}
```

Status code: 422

Unprocessable: The expression cannot be executed.

```
{
  "status" : "error",
  "errorType" : "excution",
  "error" : "expression can't be executed."
}
```

Status code: 503

Service Unavailable: The requested service is invalid. The client should not repeat the request without modifications.

```
{
  "status" : "error",
  "errorType" : "timeout",
  "error" : "query timed out in query execution."
}
```


Status Codes

Status Code	Description
200	OK: The request is successful.
400	Bad Request: The request is invalid. The client should not repeat the request without modifications.
403	Forbidden: The request is rejected. The server has received the request and understood it, but the server refuses to respond to it. The client should not repeat the request without modifications.
422	Unprocessable: The expression cannot be executed.
503	Service Unavailable: The requested service is invalid. The client should not repeat the request without modifications.

Error Codes

See **Error Codes**.

4.3.4 (Recommended) Querying Expression Calculation Results at a Specified Time Point Using the POST Method

Function

This API is used to query the calculation result of a PromQL expression at a specified time point using the POST method.

Calling Method

For details, see **Calling APIs**.

URI

POST /v1/{project_id}/aom/api/v1/query

Table 4-333 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID obtained from IAM. Generally, a project ID contains 32 characters.

Table 4-334 Query Parameters

Parameter	Mandatory	Type	Description
query	Yes	String	PromQL expression. For details, see https://prometheus.io/docs/prometheus/latest/querying/basics/.
time	No	String	Timestamp specified for PromQL calculation (Unix timestamp, in seconds).

Request Parameters

Table 4-335 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token obtained from IAM.

Response Parameters

Status code: 200

Table 4-336 Response body parameters

Parameter	Type	Description
status	String	Response status.
data	Object	Response data.

Status code: 400

Table 4-337 Response body parameters

Parameter	Type	Description
status	String	Response status.
errorType	String	Error type.
error	String	Error message.

Status code: 403

Table 4-338 Response body parameters

Parameter	Type	Description
status	String	Response status.
errorType	String	Error type.
error	String	Error message.

Status code: 422

Table 4-339 Response body parameters

Parameter	Type	Description
status	String	Response status.
errorType	String	Error type.
error	String	Error message.

Status code: 503

Table 4-340 Response body parameters

Parameter	Type	Description
status	String	Response status.
errorType	String	Error type.
error	String	Error message.

Example Requests

Query the top N aom_node_status metrics at time point "1630381536".

```
https://{EndPoint}/v1/{project_id}/aom/api/v1/query?query=topk(2,aom_node_status)&time=1630381536
```

Example Responses

Status code: 200

OK: The request is successful.

```
{
  "status" : "success",
  "data" : {
    "resultType" : "vector",
    "result" : [ {
      "metric" : {
        "__name__" : "amm_node_status",
```

```
      "clusterId" : "00000000-0000-0000-0000-00000000",
      "hostID" : "g947xcxh-2xcxc-xxx-xxcd-f6xxx85",
      "nameSpace" : "default",
      "nodeIP" : "1x6.1xx.0.xxx",
      "nodeName" : "sdxx-jxxxgksi-axx"
    },
    "value" : [ 16303810036, "0" ]
  }, {
    "metric" : {
      "__name__" : "amm_node_status",
      "clusterId" : "00000000-0000-0000-0000-00000000",
      "hostID" : "dc1xxxf7e-b095-4e77-bxx-914dhlxxxbf7",
      "nameSpace" : "default",
      "nodeIP" : "1xx.1xx.0.xxx",
      "nodeName" : "sds-jixxxsi-texxt"
    },
    "value" : [ 1630381536, "0" ]
  } ]
 }
}
```


Status code: 400

Bad Request: The request is invalid. The client should not repeat the request without modifications.


```
{
 "status" : "error",
 "errorType" : "bad_param",
 "error" : "param is invalid."
}
```


Status code: 403

Forbidden: The request is rejected. The server has received the request and understood it, but the server refuses to respond to it. The client should not repeat the request without modifications.


```
{
 "status" : "error",
 "errorType" : "auth",
 "error" : "auth project_id not pass."
}
```


Status code: 422

Unprocessable: The expression cannot be executed.


```
{
 "status" : "error",
 "errorType" : "excution",
 "error" : "expression can't be executed."
}
```


Status code: 503

Service Unavailable: The requested service is invalid. The client should not repeat the request without modifications.


```
{
 "status" : "error",
 "errorType" : "timeout",
 "error" : "query timed out in query execution."
}
```


Status Codes

Status Code	Description
200	OK: The request is successful.
400	Bad Request: The request is invalid. The client should not repeat the request without modifications.
403	Forbidden: The request is rejected. The server has received the request and understood it, but the server refuses to respond to it. The client should not repeat the request without modifications.
422	Unprocessable: The expression cannot be executed.
503	Service Unavailable: The requested service is invalid. The client should not repeat the request without modifications.

Error Codes

See **Error Codes**.

4.3.5 Querying Tag Values

Function

This API is used to query the values of a specified tag.

Calling Method

For details, see **Calling APIs**.

URI

GET /v1/{project_id}/aom/api/v1/label/{label_name}/values

Table 4-341 Path Parameters

Parameter	Mandatory	Type	Description
label_name	Yes	String	Tag to be queried.
project_id	Yes	String	Project ID obtained from IAM. Generally, a project ID contains 32 characters.

Request Parameters

Table 4-342 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token obtained from IAM.

Response Parameters

Status code: 200

Table 4-343 Response body parameters

Parameter	Type	Description
status	String	Response status.
data	Array of strings	Tag value.

Status code: 400

Table 4-344 Response body parameters

Parameter	Type	Description
status	String	Response status.
errorType	String	Error type.
error	String	Error message.

Status code: 403

Table 4-345 Response body parameters

Parameter	Type	Description
status	String	Response status.
errorType	String	Error type.
error	String	Error message.

Status code: 422

Table 4-346 Response body parameters

Parameter	Type	Description
status	String	Response status.
errorType	String	Error type.
error	String	Error message.

Status code: 503

Table 4-347 Response body parameters

Parameter	Type	Description
status	String	Response status.
errorType	String	Error type.
error	String	Error message.

Example Requests

Query all values of the "job" tag.

```
https://{EndPoint}/v1/{project_id}/aom/api/v1/label/job/values
```

Example Responses

Status code: 200

OK: The request is successful.

```
{
  "status" : "success",
  "data" : [ "node", "prometheus" ]
}
```

Status code: 400

Bad Request: The request is invalid. The client should not repeat the request without modifications.

```
{
  "status" : "error",
  "errorType" : "bad_param",
  "error" : "param is invalid."
}
```

Status code: 403

Forbidden: The request is rejected. The server has received the request and understood it, but the server refuses to respond to it. The client should not repeat the request without modifications.

```
{
  "status" : "error",
```



```
  "errorType" : "auth",
  "error" : "auth project_id not pass."
}
```

Status code: 422

Unprocessable: The expression cannot be executed.

```
{
  "status" : "error",
  "errorType" : "excution",
  "error" : "expression can't be executed."
}
```

Status code: 503

Service Unavailable: The requested service is invalid. The client should not repeat the request without modifications.

```
{
  "status" : "error",
  "errorType" : "timeout",
  "error" : "query timed out in query execution."
}
```

Status Codes

Status Code	Description
200	OK: The request is successful.
400	Bad Request: The request is invalid. The client should not repeat the request without modifications.
403	Forbidden: The request is rejected. The server has received the request and understood it, but the server refuses to respond to it. The client should not repeat the request without modifications.
422	Unprocessable: The expression cannot be executed.
503	Service Unavailable: The requested service is invalid. The client should not repeat the request without modifications.

Error Codes

See **Error Codes**.

4.3.6 Obtaining the Tag Name List Using the GET Method

Function

This API is used to obtain the tag name list using the GET method.

Calling Method

For details, see **Calling APIs**.

URI

GET /v1/{project_id}/aom/api/v1/labels

Table 4-348 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID obtained from IAM. Generally, a project ID contains 32 characters.

Request Parameters

Table 4-349 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token obtained from IAM.

Response Parameters

Status code: 200

Table 4-350 Response body parameters

Parameter	Type	Description
status	String	Response status.
data	Array of strings	Tag value.

Status code: 400

Table 4-351 Response body parameters

Parameter	Type	Description
status	String	Response status.
errorType	String	Error type.
error	String	Error message.

Status code: 403

Table 4-352 Response body parameters

Parameter	Type	Description
status	String	Response status.
errorType	String	Error type.
error	String	Error message.

Status code: 422

Table 4-353 Response body parameters

Parameter	Type	Description
status	String	Response status.
errorType	String	Error type.
error	String	Error message.

Status code: 503

Table 4-354 Response body parameters

Parameter	Type	Description
status	String	Response status.
errorType	String	Error type.
error	String	Error message.

Example Requests

Return the tag name list.

```
https://{EndPoint}/v1/{project_id}/aom/api/v1/labels
```

Example Responses

Status code: 200

OK: The request is successful.

```
{
  "status" : "success",
  "data" : [ "__name__", "call", "code", "config", "dialer_name", "endpoint", "event", "goversion", "handler",
"instance", "slice", "version" ]
}
```

Status code: 400

Bad Request: The request is invalid. The client should not repeat the request without modifications.

```
{
  "status" : "error",
  "errorType" : "bad_param",
  "error" : "param is invalid."
}
```

Status code: 403

Forbidden: The request is rejected. The server has received the request and understood it, but the server refuses to respond to it. The client should not repeat the request without modifications.

```
{
  "status" : "error",
  "errorType" : "auth",
  "error" : "auth project_id not pass."
}
```

Status code: 422

Unprocessable: The expression cannot be executed.

```
{
  "status" : "error",
  "errorType" : "excution",
  "error" : "expression can't be executed."
}
```

Status code: 503

Service Unavailable: The requested service is invalid. The client should not repeat the request without modifications.

```
{
  "status" : "error",
  "errorType" : "timeout",
  "error" : "query timed out in query execution."
}
```

Status Codes

Status Code	Description
200	OK: The request is successful.
400	Bad Request: The request is invalid. The client should not repeat the request without modifications.
403	Forbidden: The request is rejected. The server has received the request and understood it, but the server refuses to respond to it. The client should not repeat the request without modifications.
422	Unprocessable: The expression cannot be executed.
503	Service Unavailable: The requested service is invalid. The client should not repeat the request without modifications.

Error Codes

See **Error Codes**.

4.3.7 (Recommended) Obtaining the Tag Name List Using the POST Method

Function

This API is used to obtain the tag name list using the POST method.

Calling Method

For details, see **Calling APIs**.

URI

POST /v1/{project_id}/aom/api/v1/labels

Table 4-355 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID obtained from IAM. Generally, a project ID contains 32 characters.

Request Parameters

Table 4-356 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token obtained from IAM.

Response Parameters

Status code: 200

Table 4-357 Response body parameters

Parameter	Type	Description
status	String	Response status.
data	Array of strings	Tag value.

Status code: 400

Table 4-358 Response body parameters

Parameter	Type	Description
status	String	Response status.
errorType	String	Error type.
error	String	Error message.

Status code: 403

Table 4-359 Response body parameters

Parameter	Type	Description
status	String	Response status.
errorType	String	Error type.
error	String	Error message.

Status code: 422

Table 4-360 Response body parameters

Parameter	Type	Description
status	String	Response status.
errorType	String	Error type.
error	String	Error message.

Status code: 503

Table 4-361 Response body parameters

Parameter	Type	Description
status	String	Response status.
errorType	String	Error type.
error	String	Error message.

Example Requests

Return the tag name list.

```
https://{EndPoint}/v1/{project_id}/aom/api/v1/labels
```

Example Responses

Status code: 200

OK: The request is successful.

```
{
  "status" : "success",
  "data" : [ "__name__", "alarm_level", "adfname", "alertstate", "ammApplicationID",
"ammApplicationName", "appID", "appName", "clusterId", "clusterName", "cluster_id",
"comparisonOperator", "containerID", "containerName", "nameSpace", "namespace", "netDevice",
"nodeIP", "nodeName", "node_ip", "pailId", "pailName", "period_expr", "podID", "podName", "processCmd" ]
}
```

Status code: 400

Bad Request: The request is invalid. The client should not repeat the request without modifications.

```
{
  "status" : "error",
  "errorType" : "bad_param",
  "error" : "param is invalid."
}
```

Status code: 403

Forbidden: The request is rejected. The server has received the request and understood it, but the server refuses to respond to it. The client should not repeat the request without modifications.

```
{
  "status" : "error",
  "errorType" : "auth",
  "error" : "auth project_id not pass."
}
```

Status code: 422

Unprocessable: The expression cannot be executed.

```
{
  "status" : "error",
  "errorType" : "excution",
  "error" : "expression can't be executed."
}
```

Status code: 503

Service Unavailable: The requested service is invalid. The client should not repeat the request without modifications.

```
{
  "status" : "error",
  "errorType" : "timeout",
  "error" : "query timed out in query execution."
}
```


Status Codes

Status Code	Description
200	OK: The request is successful.
400	Bad Request: The request is invalid. The client should not repeat the request without modifications.
403	Forbidden: The request is rejected. The server has received the request and understood it, but the server refuses to respond to it. The client should not repeat the request without modifications.
422	Unprocessable: The expression cannot be executed.
503	Service Unavailable: The requested service is invalid. The client should not repeat the request without modifications.

Error Codes

See **Error Codes**.

4.3.8 Querying Metadata

Function

This API is used to query the metadata of time series and corresponding tags.

Calling Method

For details, see **Calling APIs**.

URI

GET /v1/{project_id}/aom/api/v1/metadata

Table 4-362 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID obtained from IAM. Generally, a project ID contains 32 characters.

Request Parameters

Table 4-363 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token obtained from IAM.

Response Parameters

Status code: 200

Table 4-364 Response body parameters

Parameter	Type	Description
status	String	Response status.
data	Object	Metadata information.

Status code: 400

Table 4-365 Response body parameters

Parameter	Type	Description
status	String	Response status.
errorType	String	Error type.
error	String	Error message.

Status code: 403

Table 4-366 Response body parameters

Parameter	Type	Description
status	String	Response status.
errorType	String	Error type.
error	String	Error message.

Status code: 422

Table 4-367 Response body parameters

Parameter	Type	Description
status	String	Response status.
errorType	String	Error type.
error	String	Error message.

Status code: 503

Table 4-368 Response body parameters

Parameter	Type	Description
status	String	Response status.
errorType	String	Error type.
error	String	Error message.

Example Requests

Obtain the metadata.

```
https://{EndPoint}/v1/{project_id}/aom/api/v1/metadata
```

Example Responses

Status code: 200

OK: The request is successful.

```
{
  "status" : "success",
  "data" : {
    "aggregator_openapi_v2_regeneration_count" : [ {
      "type" : "counter",
      "help" : "[ALPHA] Counter of OpenAPI v2 spec regeneration count broken down by causing APIService
name and reason.",
      "unit" : ""
    } ]
  }
}
```

Status code: 400

Bad Request: The request is invalid. The client should not repeat the request without modifications.

```
{
  "status" : "error",
  "errorType" : "bad_param",
  "error" : "param is invalid."
}
```

Status code: 403

Forbidden: The request is rejected. The server has received the request and understood it, but the server refuses to respond to it. The client should not repeat the request without modifications.

```
{
  "status" : "error",
  "errorType" : "auth",
  "error" : "auth project_id not pass."
}
```

Status code: 422

Unprocessable: The expression cannot be executed.

```
{
  "status" : "error",
  "errorType" : "excution",
  "error" : "expression can't be executed."
}
```

Status code: 503

Service Unavailable: The requested service is invalid. The client should not repeat the request without modifications.

```
{
  "status" : "error",
  "errorType" : "timeout",
  "error" : "query timed out in query execution."
}
```

Status Codes

Status Code	Description
200	OK: The request is successful.
400	Bad Request: The request is invalid. The client should not repeat the request without modifications.
403	Forbidden: The request is rejected. The server has received the request and understood it, but the server refuses to respond to it. The client should not repeat the request without modifications.
422	Unprocessable: The expression cannot be executed.
503	Service Unavailable: The requested service is invalid. The client should not repeat the request without modifications.

Error Codes

See **Error Codes**.

4.4 Log

4.4.1 Querying Logs

Function

This API is used to query logs by different dimensions, such as by cluster, IP address, or application. Pagination queries are supported.

Calling Method

For details, see **Calling APIs**.

URI

POST /v1/{project_id}/als/action

Table 4-369 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID obtained from IAM. Generally, a project ID contains 32 characters.

Table 4-370 Query Parameters

Parameter	Mandatory	Type	Description
type	Yes	String	Log API call mode. When the value is querylogs, this API is used to query logs.

Request Parameters

Table 4-371 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token obtained from IAM.
Content-Type	Yes	String	Content type, which is application/json. Enumeration values: • **application/json**

Table 4-372 Request body parameters

Parameter	Mandatory	Type	Description
category	Yes	String	Log type. Values: app_log: application log. node_log: node log.custom_log: log in a custom path.
endTime	Yes	Long	End time of the query (UTC, in ms).
hideSyslog	No	Integer	Whether to hide system logs during log queries. 0: Hide system logs. 1: Show system logs.
keyWord	No	String	Keyword for search. 1. Exact search by keyword is supported. A keyword is between two adjacent delimiters. 2. Fuzzy search by keyword is supported. Example: RROR, ERRO?, *ROR*, ERR*, or ER*OR. 3. Exact search by phrase is supported. Example: Start to refresh alm Statistic. 4. Search using AND (&&) or OR (||) is supported. Example: query&&logs or query||logs. Note: Default delimiters: , '";=()[]{}@&<>/:\n\t\r
lineNum	No	String	Sequence number of the final log in the last query result. This parameter is not required for the first query, but is required for subsequent pagination queries.
pageSize/size	No	String	Number of logs queried each time. Default value: 5000. Recommended value: 100. For the first query, pageSize is used. For subsequent pagination queries, size is used.
searchKey	Yes	**SearchKey** object	Log filter criteria, which vary according to log sources.

Parameter	Mandatory	Type	Description
startTime	Yes	Long	Start time of the query (UTC, in ms).
type	No	String	Pagination query. This parameter is not required for the first query, but is required for subsequent pagination queries.
isDesc	No	Boolean	Whether to query logs based on lineNum in ascending or descending order. true: lineNum in descending order (from the latest time to the earliest time) false: lineNum in ascending order (from the earliest time to the latest time)

Table 4-373 SearchKey

Parameter	Mandatory	Type	Description
appName	No	String	Application name.
clusterId	Yes	String	CCE cluster ID.
hostIP	No	String	IP address of the VM where logs are located.
nameSpace	No	String	CCE cluster namespace.
pathFile	No	String	Log file name.
podName	No	String	Container instance name.

Response Parameters

Status code: 200

Table 4-374 Response body parameters

Parameter	Type	Description
errorCode	String	Response code. SVCSTG_AMS_2000000: Success response.
errorMessage	String	Response message.

Parameter	Type	Description
result	String	Metadata, including results and the total number of returned records.

Status code: 400

Table 4-375 Response body parameters

Parameter	Type	Description
errorCode	String	Response code.
errorMessage	String	Response message.

Status code: 401

Table 4-376 Response body parameters

Parameter	Type	Description
errorCode	String	Response code.
errorMessage	String	Response message.

Status code: 403

Table 4-377 Response body parameters

Parameter	Type	Description
errorCode	String	Response code.
errorMessage	String	Response message.

Status code: 500

Table 4-378 Response body parameters

Parameter	Type	Description
errorCode	String	Response code.
errorMessage	String	Response message.

Status code: 503

Table 4-379 Response body parameters

Parameter	Type	Description
errorCode	String	Response code.
errorMessage	String	Response message.

Example Requests

- Example 1: Query application logs under a cluster.

```
"POST https://{endpoint}/v1/{project_id}/als/action?type=querylogs"

{
  "category" : "app_log",
  "endTime" : 15389000003,
  "hideSyslog" : 0,
  "keyWord" : "",
  "searchKey" : {
    "clusterId" : "c69xxxc-5xxx-1xxx-8xxx5-02xxxxx40"
  },
  "startTime" : 15389000003
}
```

- Example 2: Perform pagination queries. Notes:
  a. For pagination queries, the lineNum (sequence number of the final log in the last query result), type (value: next), and size parameters need to be added.
  b. The values of category, searchKey, keyWord, startTime, and endTime must be the same as those in the first query.
  c. To implement another pagination query, change the value of lineNum to the sequence number of the final log in the last query result. The rest may be deduced by analogy.

```
/v1/{project_id}/als/action?type=querylogs

{
  "category" : "app_log",
  "searchKey" : {
    "clusterId" : "874xxx9a2-xxxf-xxx-8xxe-02xxxxx3"
  },
  "keyWord" : "",
  "startTime" : 156946300095,
  "endTime" : 15694600008895,
  "lineNum" : "1569463900000047",
  "type" : "next",
  "size" : 100,
  "hideSyslog" : 0
}
```

Example Responses

Status code: 200

OK: The request is successful.

```
{
  "errorCode" : "SVCSTG.ALS.200.200",
```



```
 "errorMessage" : "Query data success",
 "result" : [ {
  "data" : [ {
    "appName" : "axxs0712",
    "category" : "apx",
    "clusterId" : "c6xxxx7c-54cd-11e8-8055-025xxx1e40",
    "collectTime" : 153900000983,
    "containerName" : "contsssner-0",
    "hostIP" : "1xx.xxx.0.1xxx",
    "hostId" : "c11xxxxx11-0000b-4925-bef4-d0xxxx9b0",
    "hostName" : "1x2.168.0.xxx",
    "lineNum" : "1xxx23xxxxxx2VW5xxxxxx0ZWdlcg==",
    "logContent" : "warn:2018/10/09 06:57:01 helloworld.go:108: the main processis running now.",
    "logContentSize" : null,
    "loghash" : "4xxxxx0d40a83c17f262540xxxxxxxxfeaa30eb",
    "nameSpace" : "default",
    "pathFile" : "/xxx/xxx/xxx/xxx/xxx/xxx.trxe",
    "podName" : "axxx12-7xxf884-qxxwp",
    "serviceID" : ""
  } ],
  "total" : 5000
 } ]
}
```


Status Codes

Status Code	Description
200	OK: The request is successful.
400	Bad Request: The request is invalid. The client should not repeat the request without modifications.
401	Unauthorized: The authentication information is incorrect or invalid.
403	Forbidden: The request is rejected. The server has received the request and understood it, but the server refuses to respond to it. The client should not repeat the request without modifications.
500	Internal Server Error: The server is able to receive the request but unable to understand the request.
503	Service Unavailable: The requested service is invalid. The client should not repeat the request without modifications.

Error Codes

See **Error Codes**.

4.5 Prometheus Instance

4.5.1 Uninstalling a Hosted Prometheus Instance

Function

This API is used to uninstall a hosted Prometheus instance.

Calling Method

For details, see **Calling APIs**.

URI

DELETE /v1/{project_id}/aom/prometheus

Table 4-380 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID obtained from IAM. Generally, a project ID contains 32 characters.

Table 4-381 Query Parameters

Parameter	Mandatory	Type	Description
prom_id	Yes	String	Prometheus instance ID.

Request Parameters

Table 4-382 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token obtained from IAM.
Content-Type	Yes	String	Content type, which is application/json.
Enterprise-Project-Id	No	String	Enterprise project ID. • To query instances in an enterprise project, enter the enterprise project ID. • To query instances in all enterprise projects, enter **all_granted_eps**.

Response Parameters

Status code: 400

Table 4-383 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
error_type	String	Error type.
trace_id	String	Trace ID.

Example Requests

Delete the Prometheus instance whose **prom_id** is **08****2a-8**b-4**5-b**1-d1******79**.

```
https://{Endpoint}/v1/{project_id}/aom/prometheus?prom_id=08****2a-8**b-4**5-b**1-d1********79
```

Example Responses

Status code: 200

OK: The request is successful.

```
{
  "08****2a-8**b-4**5-b**1-d1********79" : true
}
```

Status code: 400

No Prometheus instance is found.

```
{
  "error_code" : "AOM.11017014",
  "error_msg" : "prom instance not found",
  "trace_id" : ""
}
```

Status Codes

Status Code	Description
200	OK: The request is successful.
400	No Prometheus instance is found.

Error Codes

See **Error Codes**.

4.5.2 Querying a Prometheus Instance

Function

This API is used to query a Prometheus instance.

Calling Method

For details, see **Calling APIs**.

URI

GET /v1/{project_id}/aom/prometheus

Table 4-384 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID obtained from IAM. Generally, a project ID contains 32 characters.

Table 4-385 Query Parameters

Parameter	Mandatory	Type	Description
prom_id	No	String	Prometheus instance ID. If both **prom_id** and **prom_type** exist, only **prom_id** takes effect.
prom_type	No	String	Prometheus instance type (**VPC** and **KUBERNETES** are not supported). Enumeration values: • **default** • **ECS** • **VPC** • **CCE** • **REMOTE_WRITE** • **KUBERNETES**
cce_cluster_enable	No	String	Whether to enable a CCE cluster. Enumeration values: • **true** • **false**
prom_status	No	String	Prometheus instance status. Enumeration values: • **DELETED** • **NORMAL** • **ALL**

Request Parameters

Table 4-386 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token obtained from IAM.
Content-Type	Yes	String	Content type, which is application/json.
Enterprise-Project-Id	No	String	Enterprise project ID. • To query instances in an enterprise project, enter the enterprise project ID. • To query instances in all enterprise projects, enter **all_granted_eps**.

Response Parameters

Status code: 200

Table 4-387 Response body parameters

Parameter	Type	Description
prometheus	Array of **PromInstanceEpsModel** objects	Prometheus instance list.

Table 4-388 PromInstanceEpsModel

Parameter	Type	Description
prom_name	String	Prometheus instance name. Enter 1–100 characters and do not start or end with an underscore (_) or hyphen (-). Only letters, digits, underscores, and hyphens are allowed.
prom_id	String	Prometheus instance ID.

Parameter	Type	Description
prom_type	String	Prometheus instance type (**VPC** and **KUBERNETES** are not supported). Enumeration values: • **default** • **ECS** • **VPC** • **CCE** • **REMOTE_WRITE** • **KUBERNETES**
prom_version	String	Prometheus instance version.
prom_create_timestamp	Long	Timestamp when the Prometheus instance is created.
prom_update_timestamp	Long	Timestamp when the Prometheus instance is updated.
prom_status	String	Prometheus instance status. Enumeration values: • **DELETED** • **NORMAL** • **ALL**
enterprise_project_id	String	Enterprise project that the Prometheus instance belongs to.
project_id	String	ID of the project that the Prometheus instance belongs to.
is_deleted_tag	Long	Whether an instance has been deleted.
deleted_time	Long	Deletion time.
prom_spec_config	**PromConfig Model** object	Special configuration of the Prometheus instance.
cce_spec_config	String	Special configuration of the Prometheus instance in the CCE scenario.

Table 4-389 PromConfigModel

Parameter	Type	Description
remote_write_url	String	Remote write address of the Prometheus instance.
remote_read_url	String	Remote read address of the Prometheus instance.

Parameter	Type	Description
prom_http_api_endpoint	String	URL for calling the Prometheus instance.
dashboard_id	String	ID of the dashboard associated with the Prometheus instance (not used currently).
region_id	String	Region that the Prometheus instance belongs to.

Example Requests

- Query a Prometheus instance.
  https://{Endpoint}/v1/{project_id}/aom/prometheus
- Query the Prometheus instance whose **prom_id** is **08****2a-8**b-4**5-b**1-d1******79**.
  https://{Endpoint}/v1/{project_id}/aom/prometheus?prom_id=08****2a-8**b-4**5-b**1-d1********79

Example Responses

Status code: 200

OK: The request is successful.

```
{
  "prometheus" : [ {
    "deleted_time" : 0,
    "enterprise_project_id" : "0",
    "project_id" : "2a4***56cc***7f837***891***c1cf",
    "prom_create_timestamp" : 1691718171483,
    "prom_id" : "08****2a-8**b-4**5-b**1-d1********79",
    "prom_name" : "aom_prometheus",
    "prom_spec_config" : {
      "prom_http_api_endpoint" : "aom-internal.cn-****-
*.myhuaweicloud.com:***/v1/2a4***56cc***7f837***891***c1cf/08****2a-8**b-4**5-b**1-d1********79",
      "region_id" : "cn-****-*",
      "remote_read_url" : "aom-internal.cn-****-*.myhuaweicloud.com:***/v1/2a4***56cc***7f837***891***c1cf/
08****2a-8**b-4**5-b**1-d1********79/api/v1/read",
      "remote_write_url" : "aom-internal.cn-****-*.myhuaweicloud.com:***/v1/2a4***56cc***7f837***891***c1cf/
08****2a-8**b-4**5-b**1-d1********79/push"
    },
    "prom_type" : "CCE",
    "prom_update_timestamp" : 1691718171483
  } ]
}
```

Status Codes

Status Code	Description
200	OK: The request is successful.

Error Codes

See **Error Codes**.

4.5.3 Adding a Prometheus Instance

Function

This API is used to add a Prometheus instance.

Calling Method

For details, see **Calling APIs**.

URI

POST /v1/{project_id}/aom/prometheus

Table 4-390 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID obtained from IAM. Generally, a project ID contains 32 characters.

Request Parameters

Table 4-391 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token obtained from IAM.
Content-Type	Yes	String	Content type, which is application/json.
region	Yes	String	Region to which the Prometheus instance belongs. Generally, it is the domain name or IP address of the server bearing the REST service endpoint. This parameter varies depending on the service and region.

Table 4-392 Request body parameters

Parameter	Mandatory	Type	Description
prom_name	Yes	String	Prometheus instance name. Enter 1–100 characters and do not start or end with an underscore (_) or hyphen (-). Only letters, digits, underscores, and hyphens are allowed.
prom_type	Yes	String	Prometheus instance type (**VPC** and **KUBERNETES** are not supported). Enumeration values: • **ECS** • **VPC** • **CCE** • **REMOTE_WRITE** • **KUBERNETES**
prom_version	No	String	Prometheus instance version.
enterprise_project_id	No	String	Enterprise project that the Prometheus instance belongs to.
project_id	No	String	ID of the project that the Prometheus instance belongs to.

Response Parameters

Status code: 200

Table 4-393 Response body parameters

Parameter	Type	Description
prometheus	Array of **PromInstanceEpsCreateModel** objects	Prometheus instance list.

Table 4-394 PromInstanceEpsCreateModel

Parameter	Type	Description
prom_name	String	Prometheus instance name. Enter 1–100 characters and do not start or end with an underscore (_) or hyphen (-). Only letters, digits, underscores, and hyphens are allowed.
prom_id	String	Prometheus instance ID.
prom_type	String	Prometheus instance type (**VPC** and **KUBERNETES** are not supported). Enumeration values: • **ECS** • **VPC** • **CCE** • **REMOTE_WRITE** • **KUBERNETES**
prom_version	String	Prometheus instance version.
prom_create_timestamp	Long	Timestamp when the Prometheus instance was created.
prom_update_timestamp	Long	Timestamp when the Prometheus instance was updated.
prom_status	String	Prometheus instance status. Enumeration values: • **DELETED** • **NORMAL** • **ALL**
enterprise_project_id	String	Enterprise project that the Prometheus instance belongs to.
project_id	String	ID of the project that the Prometheus instance belongs to.
deleted_time	Long	Deletion time.
prom_spec_config	**PromConfig Model** object	Special configuration of the Prometheus instance.
cce_spec_config	String	Special configuration of the Prometheus instance in the CCE scenario.

Table 4-395 PromConfigModel

Parameter	Type	Description
remote_write_url	String	Remote write address of the Prometheus instance.
remote_read_url	String	Remote read address of the Prometheus instance.
prom_http_api_endpoint	String	URL for calling the Prometheus instance.
dashboard_id	String	ID of the dashboard associated with the Prometheus instance (not used currently).
region_id	String	Region that the Prometheus instance belongs to.

Example Requests

Add a Prometheus instance for CCE.

```
https://{Endpoint}/v1/{project_id}/aom/prometheus

{
  "prom_type" : "CCE",
  "prom_name" : "aom_prometheus"
}
```

Example Responses

Status code: 200

OK: The request is successful.

```
{
  "prometheus" : [ {
    "deleted_time" : 0,
    "enterprise_project_id" : "0",
    "project_id" : "2a4***56cc***7f837***891***c1cf",
    "prom_create_timestamp" : 1691718171483,
    "prom_id" : "08****2a-8**b-4**5-b**1-d1*******79",
    "prom_name" : "aom_prometheus",
    "prom_spec_config" : {
      "prom_http_api_endpoint" : "aom-internal.cn-****-
*.myhuaweicloud.com:***/v1/2a4***56cc***7f837***891***c1cf/08****2a-8**b-4**5-b**1-d1*******79",
      "remote_read_url" : "aom-internal.cn-****-*.myhuaweicloud.com:***/v1/2a4***56cc***7f837***891***c1cf/
08****2a-8**b-4**5-b**1-d1*******79/api/v1/read",
      "remote_write_url" : "aom-internal.cn-****-*.myhuaweicloud.com:***/v1/2a4***56cc***7f837***891***c1cf/
08****2a-8**b-4**5-b**1-d1*******79/push",
      "region_id" : "cn-****-*"
    },
    "prom_type" : "CCE",
    "prom_update_timestamp" : 1691718171483
  } ]
}
```


Status Codes

Status Code	Description
200	OK: The request is successful.

Error Codes

See **Error Codes**.

4.5.4 Creating a Recording Rule for a Prometheus Instance

Function

This API is used to create a recording rule for a Prometheus instance.

Calling Method

For details, see **Calling APIs**.

URI

POST /v1/{project_id}/{prometheus_instance}/aom/api/v1/rules

Table 4-396 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID obtained from IAM. Generally, a project ID contains 32 characters.
prometheus_instance	Yes	String	Prometheus instance ID.

Request Parameters

Table 4-397 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token obtained from IAM.
Content-Type	Yes	String	Content type, which is application/json.

Table 4-398 Request body parameters

Parameter	Mandatory	Type	Description
recording_rule	Yes	String	Recording rule.

Response Parameters

Status code: 500

Table 4-399 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
error_type	String	Error type.
trace_id	String	Trace ID.

Example Requests

Create a recording rule for a Prometheus instance.

```
https://{Endpoint}/v1/{project_id}/{prometheus_instance}/aom/api/v1/rules

{
  "recording_rule" : "groups:\n    - name: apiserver_request_total\n      interval: 60s\n      rules:\n        - record: job_instance_mode:apiserver_request_total:avg_rate5m\n          expr: avg by (job, instance, mode) (rate(apiserver_request_total[5m]))\n          labels:\n            team: operations\n        - record: job:apiserver_request_total:sum_rate10m\n          expr: sum by (job)(rate(apiserver_request_total[10m]))\n          labels:\n            team: operations"
}
```

Example Responses

Status code: 204

OK: The request is successful.

```
""
```

Status code: 500

The recording rule already exists.

```
{
  "error_code" : "AOM.5001019",
  "error_msg" : "recording rule exist for the prometheus instance"
}
```


Status Codes

Status Code	Description
204	OK: The request is successful.
500	The recording rule already exists.

Error Codes

See **Error Codes**.

4.5.5 Obtaining the Credential for Calling a Prometheus Instance

Function

This API is used to obtain the credential for calling a Prometheus instance.

Calling Method

For details, see **Calling APIs**.

URI

GET /v1/{project_id}/access-code

Table 4-400 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID obtained from IAM. Generally, a project ID contains 32 characters.

Request Parameters

Table 4-401 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token obtained from IAM.
Content-Type	Yes	String	Content type, which is application/json.

Response Parameters

Status code: 200

Table 4-402 Response body parameters

Parameter	Type	Description
access_codes	Array of **AccessCodeModel** objects	Access codes.

Table 4-403 AccessCodeModel

Parameter	Type	Description
access_code	String	Access code.
access_code_id	String	Access code ID.
create_at	Long	Creation time.
status	String	Status.

Example Requests

Obtain the credential for calling a Prometheus instance.

```
https://{Endpoint}/v1/{project_id}/access-code
```

Example Responses

Status code: 200

OK: The request is successful.

```
{
  "access_codes" : [ {
    "access_code" : "b***OOJpV***B4ciU*******NfR2f9xZ******tgpba******yQS66Ih****a",
    "access_code_id" : "c6*04****ee6e******092*****45**3",
    "create_at" : 1700796457506243016,
    "status" : "enable"
  } ]
}
```

Status Codes

Status Code	Description
200	OK: The request is successful.

Error Codes

See **Error Codes**.

4.6 Configuration Management

4.6.1 Querying the Cloud Services for Which AOM 2.0 Has Been Granted Permissions

Function

This API is used to query the cloud services for which AOM 2.0 has been granted permissions.

Calling Method

For details, see **Calling APIs**.

URI

GET /v1/{project_id}/aom/auth/grant

Table 4-404 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID obtained from IAM. Generally, a project ID contains 32 characters.

Request Parameters

Table 4-405 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token obtained from IAM.
Content-Type	Yes	String	Content type, which is application/json.

Response Parameters

None

Example Requests

Query the cloud services for which AOM 2.0 has been granted permissions.

```
https://{Endpoint}/v1/{project_id}/aom/auth/grant
```

Example Responses

Status code: 200

OK: The request is successful.

```
{
  "CES" : {
    "role_name" : [ "CES ReadOnlyAccess" ],
    "status" : true
  },
  "ECS" : {
    "role_name" : [ "ECS CommonOperations", "ECS ReadOnlyAccess" ],
    "status" : true
  },
  "CCE" : {
    "role_name" : [ "CCE FullAccess" ],
    "status" : true
  },
  "CCI" : {
    "role_name" : [ "CCI FullAccess" ],
    "status" : true
  },
  "RMS" : {
    "role_name" : [ "RMS ReadOnlyAccess" ],
    "status" : true
  },
  "LTS" : {
    "role_name" : [ "LTS FullAccess" ],
    "status" : true
  },
  "DMS" : {
    "role_name" : [ "DMS UserAccess" ],
    "status" : true
  }
}
```

Status Codes

Status Code	Description
200	OK: The request is successful.

Error Codes

See **Error Codes**.

4.6.2 Querying the ICAgent Installed on a Host

Function

This API is used to query the ICAgent installed on a cluster host or a custom host.

Calling Method

For details, see **Calling APIs**.

URI

GET /v1/{project_id}/{cluster_id}/{namespace}/agents

Table 4-406 Path Parameters

Parameter	Mandatory	Type	Description
cluster_id	Yes	String	• Enter a cluster ID when a cluster host is queried. • Enter **APM** when a custom host is queried.
namespace	Yes	String	• Enter a namespace when a cluster host is queried. • Enter **APM** when a custom host is queried.
project_id	Yes	String	Project ID obtained from IAM. Generally, a project ID contains 32 characters.

Request Parameters

Table 4-407 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token obtained from IAM.
Content-Type	Yes	String	Content type, which is application/json.

Response Parameters

None

Example Requests

Query the ICAgent installed on a host.

```
https://{Endpoint}/v1/{project_id}/{cluster_id}/{namespace}/agents
```

Example Responses

Status code: 200

OK: The request is successful.


```
[ {
  "ip" : "10.**.**.13",
  "agentId" : "7b****93-7**1-4**e-8**b-3d****35**84",
  "devCloudId" : "",
  "nodeName" : "aom-docker-75079-iul66",
  "status" : "running",
  "lastModified" : "1700577655170",
  "updateTime" : "1701141177267",
  "version" : "5.13.110.52",
  "osType" : "linux",
  "pinpointVersion" : "1.0.29",
  "pinpointStatus" : "",
  "phpProbeVersion" : "",
  "dotnetProbeVersion" : "",
  "extendInfo" : null,
  "customHostTag" : null,
  "enterprise_project_id" : "d64fbcc8-c296-4a6f-8988-6850dfb08b47",
  "reserved" : "{\"cpu_used\":\"1.5\",\"goroutine_used\":9507,\"mem_used\":\"181556\",\"net_used
\":0.1923828125}"
} ]
```


Status Codes

Status Code	Description
200	OK: The request is successful.

Error Codes

See **Error Codes**.

5 Historical APIs

5.1 Auto Scaling APIs (Offline Soon)

5.1.1 Creating a Policy

Function

This API is used to create a policy.

NOTICE

- The value must be 1 to 64 characters starting with a letter. Only digits, letters, underscores (_), and hyphens (-) are allowed.
- In an AS group, for the same metric (**metric_name**), the value of **metric_threshold** with **metric_operation** set to **>** must be greater than that with **metric_operation** set to **<**.
- In an AS group, the **metric_operation** for a metric must be unique.
- In a policy, the logic of **conditions** of metrics with the same **metric_name** cannot conflict.
- The year in the trigger time (**launch_time**) of a scheduled policy cannot be later than 2099.
- The year in the start time (**start_time**) and end time (**end_time**) of a periodic policy cannot be later than 2099.
- An AS group supports a maximum of 10 scheduled and periodic policies, and 10 alarm policies.
- In an AS group, alarm policies cannot affect each other.

URI

POST /v1/{project_id}/pe/policy

Request

Request headers

Table 5-1 describes the request headers.

Table 5-1 Request headers

Parameter	Description	Mandatory	Example
Deployment-Name	Application name.	Yes	-
Content-Type	Content type, which is **application/json;charset=utf-8**.	Yes	application/json;charset=utf-8
Cluster-Id	Cluster ID.	Yes	-
Namespace	Namespace.	Yes	-
X-Auth-Token	User token obtained from IAM.	Yes	-
Reserved-Info	Custom parameter of the product.	No	-

Request parameters

Table 5-2 describes the request parameters.

Table 5-2 Request parameters

Parameter	Mandatory	Type	Value Range	Description
name	Yes	String	The value must be 1 to 64 characters starting with a letter. Only digits, letters, underscores (_), and hyphens (-) are allowed.	Policy name.
policy_type	Yes	String	• SCHEDULED • RECURRENCE • ALARM	Policy type.
rule	Yes	See **Table 5-3**.	-	Policy trigger rule.

Table 5-3 rule parameters

Parameter	Mandatory	Type	Value Range	Description
conditions	Yes	See **Table 5-4**.	Only one condition is allowed.	Condition contents. When multiple alarm policies are used, their conditions cannot overlap. Example: You cannot set a metric greater than 10% in one condition and smaller than 20% in another condition.
actions	Yes	See **Table 5-5**.	Only one action is allowed.	Action executed after a specified policy is successfully matched.

Table 5-4 conditions parameters

Parameter	Mandatory	Type	Value Range	Description
launch_time	Yes	String	-	Trigger time, which must comply with ISO 8601 or UTC specifications. • If the value of **policy_type** is **SCHEDULED**, the time format is **YYYY-MM-DDThh:mmZ**. • If the value of **policy_type** is **RECURRENCE**, the time format is **hh:mm**.
recurrence_type	Yes	String	Value: Daily, Weekly, or Monthly. • Daily: Execution by day • Weekly: Execution by week • Monthly: Execution by month	Trigger period.

Parameter	Mandatory	Type	Value Range	Description
recurrence_value	Yes	String	• When the value of **recurrence_type** is **Daily**, the value of this parameter is **null**. • When the value of **recurrence_type** is **Weekly**, this parameter indicates the Nth day within a week. Its value ranges from 0 to 6. **0** indicates Sunday, **1** indicates Monday, and the same rule applies to other values. To select multiple values, separate them using commas (,). Example: 0,2,4, which indicates Sunday, Tuesday, and Thursday, respectively. • When the value of **recurrence_type** is **Monthly**, this parameter indicates a day in a month. To select multiple values, separate them using commas (,). Example: 1,10,13,28.	Number of tasks executed when a periodic policy is triggered.
start_time	Yes	String	-	Time when periodic policy execution starts, which must comply with ISO 8601 or UTC specifications. Format: YYYY-MM-DDThh:mmZ.

Parameter	Mandatory	Type	Value Range	Description
end_time	Yes	String	-	Time when periodic policy execution stops, which must comply with ISO 8601 or UTC specifications. Format: YYYY-MM-DDThh:mmZ.
metric_namespace	Yes	String	• PAAS.CONTAINER: application metric namespace. • PAAS.CUSTOMMETRICS: custom metric namespace.	Namespace.
metric_name	Yes	String	The value must be 1 to 255 characters long and meet the [a-zA-Z_:][a-zA-Z0-9_:]* expression. That is, the value must start with a letter, underscore (_), or colon (:). Only letters, digits, underscores, and colons are allowed.	Metric name.
metric_unit	Yes	String	-	Unit.
period	Yes	Integer	20, 60, 300, 900, 1800, or 3600	Statistical period (unit: s).
evaluation_periods	Yes	Integer	1, 2, 3, 4, or 5	Number of consecutive periods.
statistic	Yes	String	Currently, only **average** is supported.	Statistic.
metric_operation	Yes	String	**>** and **<**. For example, you can use **>** in a threshold criterion (when the value of a metric is greater than **metric_thresholdUpdate**) to trigger actions.	Metric operator.
metric_threshold	Yes	Float	[0, 2147483647]	Threshold criterion.

The following describes the meaning of each field in the **conditions** parameter.

```
"conditions": [{
  "metric_namespace" : "PAAS.CONTAINER",
  "metric_name" : "cpuUsage",
  "metric_unit" : "Percent",
  "period" : 300,
  "evaluation_periods" : 2,
  "statistic" : "average",
  "metric_operation" : ">",
  "metric_threshold" : 70
  }]
```

For **cpuUsage** (**metric_name**) in **PAAS.CONTAINER** (**metric_namespace**), when its **average** value (**statistic**) exceeds 70% (**metric_threshold**) for two (**evaluation_periods**) consecutive periods (with a duration of 300s), the policy is triggered.

Table 5-5 actions parameters

Parameter	Mandatory	Type	Value Range	Description
type	Yes	String	• scale_out_k8s • scale_out_vm • scale_in_k8s • scale_in_vm • scale_set_k8s • scale_set_vm	• **scale_out_k8s** and **scale_out_vm** indicate a scale-out. • **scale_in_k8s** and **scale_in_vm** indicate a scale-in. • **scale_set_k8s** and **scale_set_vm** indicate the number of application instances. **NOTE** The value containing **k8s** indicates a container application and that containing **vm** indicates a process application.
parameters	Yes	See **Table 5-6**.	-	Number of scale-in or -out instances.

Table 5-6 parameters

Parameter	Mandatory	Type	Value Range	Description
scale_unit	Yes	Integer	Minimum number of instances to the maximum number of instances in a policy group.	Number of scale-in or -out instances.

Example request

- Example of a scheduled policy

```
{
   "name" : "policy1",
   "policy_type" : "SCHEDULED",
   "rule" : {
      "conditions" : [{
            "launch_time" : "2017-03-04T03:37Z",
            "recurrence_type" : null,
            "recurrence_value" : null,
            "start_time" : null,
            "end_time" : null
         }
      ],
      "actions" : [{
            "type" : "scale_set_k8s",
            "parameters" : {
               "scale_unit" : 1
            }
         }
      ]
   }
}
```

- Example of a periodic policy

```
{
   "name" : "policy_2",
   "policy_type" : "RECURRENCE",
   "rule" : {
      "conditions" : [{
            "launch_time" : "13:45",
            "recurrence_type" : "Weekly",
            "recurrence_value" : "0,1,4",
            "start_time" : "2017-01-26T03:33Z",
            "end_time" : "2099-01-31T03:33Z"
         }
      ],
      "actions" : [{
            "type" : "scale_set_k8s",
            "parameters" : {
               "scale_unit" : 1
            }
         }
      ]
   }
}
```

- Example of an alarm policy

```
{
   "name" : "policy_1",
   "policy_type" : "ALARM",
   "rule" : {
```



```
    "conditions" : [{
            "metric_namespace" : "PAAS.CONTAINER",
            "metric_name" : "cpuUsage",
            "metric_unit" : "Percent",
            "period" : 60,
            "evaluation_periods" : 1,
            "statistic" : "average",
            "metric_operation" : ">",
            "metric_threshold" : 70
        }
    ],
    "actions" : [{
            "type" : "scale_out_k8s",
            "parameters" : {
                "scale_unit" : 1
            }
        }
    ]
  }
}
```

Response

Response parameters

Table 5-7 describes the response parameters.

Table 5-7 Response parameters

Parameter	Type	Description
errorCode	String	Error code.
errorMessage	String	Error details.
policy_id	String	Policy ID.

Example response

```
{
  "errorCode": 0,
  "errorMessage": "",
  "policy_id": "1b9994f0-847a-45e4-aeee-e8b604dddb34"
}
```

Error Code

Table 5-8 Error codes

Error Code	Message	Solution
SVCSTG.PE.4001101	Invalid parameter.	Check whether the parameter meets requirements.
SVCSTG.PE.4031012	Failed to verify the project ID.	Check whether the parameter meets requirements.

Error Code	Message	Solution
SVCSTG.PE.5001201	Failed to insert or update data in the background.	Contact technical support.

5.1.2 Deleting a Policy

Function

This API is used to delete a specified policy.

URI

DELETE /v1/{project_id}/pe/policy

Request

Request headers

Table 5-9 describes the request headers.

Table 5-9 Request headers

Parameter	Description	Mandatory	Example
Deployment-Name	Application name.	Yes	-
Policy-Id	Policy ID.	Yes	-

Request parameters

None

Example request

None

Response

Response parameters

If a policy is successfully deleted, only **204** is returned. If a policy fails to be deleted, the response body containing error information is returned.

Table 5-10 describes the response parameters.

Table 5-10 Response parameters

Parameter	Type	Description
errorCode	String	Error code.
errorMessage	String	Error details.

Example response

None

Error Code

Table 5-11 Error codes

Error Code	Message	Solution
SVCSTG.PE.4031012	Failed to verify the project ID.	Check whether the parameter meets requirements.
SVCSTG.PE.5001205	Failed to delete records.	Contact technical support.

5.1.3 Modifying a Policy

Function

This API is used to modify a policy.

NOTICE

Alarm policies can be modified, but scheduled and periodic policies cannot.

URI

PUT /v1/{project_id}/pe/policy/{policy_id}

Table 5-12 describes the parameters.

Table 5-12 Parameters

Parameter	Mandatory	Description
project_id	Yes	Project ID.
policy_id	Yes	Policy ID.

Request

Request headers

Table 5-13 describes the request headers.

Table 5-13 Request headers

Parameter	Description	Mandatory	Example
Content-Type	Content type, which is **application/json;charset=utf-8**.	Yes	application/json;charset=utf-8
Cluster-Id	Cluster ID.	Yes	-
Namespace	Namespace.	Yes	-
Deployment-Name	Application name.	Yes	-

Request parameters

Table 5-14 describes the request parameters.

Table 5-14 Request parameters

Parameter	Mandatory	Type	Value Range	Description
id	Yes	String	-	Policy ID.
name	Yes	String	The value must be 1 to 64 characters starting with a letter. Only digits, letters, underscores (_), and hyphens (-) are allowed.	Policy name, which cannot be modified.
policy_type	Yes	String	ALARM	Policy type. Currently, only ALARM policies are supported.
rule	Yes	See Table 5-15.	-	Policy trigger rule.

Table 5-15 rule parameters

Parameter	Mandatory	Type	Value Range	Description
conditions	Yes	See **Table 5-16**.	1–5	Condition contents. A rule can contain multiple conditions in AND relationships. One condition describes the matching method of one metric.
actions	Yes	See **Table 5-17**.	1–5	Action executed after a specified policy is successfully matched.

Table 5-16 conditions parameters

Parameter	Mandatory	Type	Value Range	Description
metric_namespace	Yes	String	• PAAS.CONTAINER: application metric namespace. • PAAS.CUSTOMMETRICS: custom metric namespace.	Metric namespace.

Parameter	Mandatory	Type	Value Range	Description
metric_name	Yes	String	The value must be 1 to 255 characters long and meet the [a-zA-Z_:][a-zA-Z0-9_:]* expression. That is, the value must start with a letter, underscore (_), or colon (:). Only letters, digits, underscores, and colons are allowed.	Metric name.
metric_unit	Yes	String	-	Unit. **NOTE** The value is retrieved from an AMS API and varies with the metric name.
period	Yes	Integer	20, 60, 300, 900, 1800, or 3600	Statistical period (unit: s).
evaluation_periods	Yes	Integer	1, 2, 3, 4, or 5	Number of consecutive periods.
statistic	Yes	String	Currently, only **average** is supported.	Statistic.

Parameter	Mandatory	Type	Value Range	Description
metric_operation	Yes	String	> and <. For example, you can use > in a threshold criterion (when the value of a metric is greater than **metric_thresholdUpdate**) to trigger actions.	Metric operator.
metric_threshold	Yes	Float	[0, 2147483647]	Threshold criterion.

Table 5-17 actions parameters

Parameter	Mandatory	Type	Value Range	Description
type	Yes	String	• scale_out_k8s • scale_out_vm • scale_in_k8s • scale_in_vm	• **scale_out_k8s** and **scale_out_vm** indicate a scale-out. • **scale_in_k8s** and **scale_in_vm** indicate a scale-in. **NOTE** The value containing **k8s** indicates a container application and that containing **vm** indicates a process application.
parameters	Yes	See **Table 5-18**.	-	Number of scale-in or -out instances.

Table 5-18 parameters

Parameter	Mandatory	Type	Value Range	Description
scale_unit	Yes	Integer	Minimum number of instances to the maximum number of instances in a policy group.	Number of scale-in or -out instances.

Example request

Example of an alarm policy

```
{
   "id" : "5c2eecea-32ac-42c0-be30-f73b15d68429",
   "name" : "policy_1",
   "policy_type" : "ALARM",
   "rule" : {
      "conditions" : [{
            "metric_namespace" : "PAAS.CONTAINER",
            "metric_name" : "cpuUsage",
            "metric_unit" : "Percent",
            "period" : 60,
            "evaluation_periods" : 1,
            "statistic" : "average",
            "metric_operation" : ">",
            "metric_threshold" : 70
         }
      ],
      "actions" : [{
            "type" : "scale_out_k8s",
            "parameters" : {
               "scale_unit" : 1
            }
         }
      ]
   }
}
```

Response

Response parameters

Table 5-19 describes the response parameters.

Table 5-19 Response parameters

Parameter	Type	Description
errorCode	String	Error code.
errorMessage	String	Error details.
context	String	Details about a modified policy.

Example response

```
{
  "errorCode": 0,
  "errorMessage": "",
  "context": {
      "id" : "5c2eecea-32ac-42c0-be30-f73b15d68429",
      "name" : "policy_1",
      "policy_type" : "ALARM",
      "rule" : {
          "conditions" : [{
                "metric_namespace" : "PAAS.CONTAINER",
                "metric_name" : "cpuUsage",
                "metric_unit" : "Percent",
                "period" : 60,
                "evaluation_periods" : 1,
                "statistic" : "average",
                "metric_operation" : ">",
                "metric_threshold" : 70
            }
          ],
          "actions" : [{
                "type" : "scale_out_k8s",
                "parameters" : {
                   "scale_unit" : 1
                }
            }
          ]
      }
  }
}
```

Error Code

Table 5-20 Error codes

Error Code	Message	Solution
SVCSTG.PE.4001101	Invalid parameter.	Check whether the parameter meets requirements.
SVCSTG.PE.4031012	Failed to verify the project ID.	Check whether the parameter meets requirements.
SVCSTG.PE.4033008	Failed to update the scheduled or periodic policy.	Check whether the parameter meets requirements.
SVCSTG.PE.5001201	Failed to insert or update data in the background.	Contact technical support.
SVCSTG.PE.5001203	Query error.	Contact technical support.
SVCSTG.PE.5003007	Failed to update the threshold rule.	Contact technical support.

5.1.4 Querying a Policy List

Function

This API is used to query details about all policies of a specified project.

URI

GET /v1/{project_id}/pe/policy

Table 5-21 describes the parameters.

Table 5-21 Parameters

Parameter	Mandatory	Description
project_id	Yes	Project ID.

Request

Request headers

None

Request parameters

None

Example request

None

Response

Response parameters

Table 5-22 describes the response parameters.

Table 5-22 Response parameters

Parameter	Type	Description
errorCode	String	Error code.
errorMessage	String	Error details.
policy	See Table 5-23.	Details about a modified policy.

Table 5-23 policy parameters

Parameter	Type	Description
id	String	Policy ID.
name	String	Policy name.
policy_type	String	Policy type.
rule	See **Table 5-24**.	Policy trigger rule.
create_time	String	Creation time.
update_time	String	Update time.
status	String	Status

Table 5-24 rule parameters

Parameter	Type	Description
name	String	Policy name.
conditions	See **Table 5-25**.	Condition contents.
actions	See **Table 5-26**.	Action executed after a specified policy is successfully matched.

Table 5-25 conditions parameters

Parameter	Type	Description
metric_namespace	String	Namespace.
metric_name	String	Metric name.
metric_unit	String	Unit.
period	Integer	Statistical period (unit: s).
evaluation_periods	Integer	Number of consecutive periods.
statistic	String	Statistic.
metric_operation	String	Metric operator.
metric_threshold	Float	Threshold criterion.

Table 5-26 actions parameters

Parameter	Type	Description
type	String	Scale-in or -out. The value containing **k8s** indicates a container application and that containing **vm** indicates a process application.
parameters	See **Table 5-27**.	Number of scale-in or -out instances.

Table 5-27 parameters

Parameter	Type	Description
scale_unit	Integer	Number of scale-in or -out instances.

Example response


```
{
   "errorCode" : "SVCSTG.PE.0",
   "errorMessage" : "",
   "policies" : [{
      "id" : "8accffb6-e0ed-4433-b216-ccf6960eb1ad",
         "name" : "alarm",
         "group_id" : "77c37e1f-aa0c-438d-8445-39b3997786a2",
         "policy_type" : "ALARM",
         "rule" : {
            "name" : "",
            "conditions" : [{
                  "metric_namespace" : "PAAS.CONTAINER",
                  "metric_name" : "cpuCoreLimit",
                  "metric_unit" : "Percent",
                  "period" : 60,
                  "evaluation_periods" : 1,
                  "statistic" : "average",
                  "metric_operation" : "\u003e",
                  "metric_threshold" : 100,
                  "metric_dimensions" : null
               }
            ],
            "actions" : [{
                  "type" : "scale_out_k8s",
                  "parameters" : {
                     "scale_unit" : 1
                  }
               }
            ]
         },
         "create_time" : "2017-12-21T09:13:42Z",
         "update_time" : "2017-12-21T09:13:42Z",
         "status" : "enabled"
      }, {
         "id" : "9aafbd3d-eac4-4a92-a342-5b6f8d60fff2",
         "name" : "dingshi2",
         "group_id" : "77c37e1f-aa0c-438d-8445-39b3997786a2",
         "policy_type" : "SCHEDULED",
```



```
        "rule" : {
            "name" : "",
            "conditions" : [{
                    "launch_time" : "2017-12-22T06:30Z",
                    "recurrence_type" : "",
                    "recurrence_value" : "",
                    "start_time" : "",
                    "end_time" : ""
                }
            ],
            "actions" : [{
                    "type" : "scale_set_k8s",
                    "parameters" : {
                        "scale_unit" : 1
                    }
                }
            ]
        },
        "create_time" : "2017-12-21T09:14:00Z",
        "update_time" : "2017-12-21T09:14:00Z",
        "status" : "enabled"
    }
  ]
}
```


Error Code

Table 5-28 Error codes

Error Code	Message	Solution
SVCSTG.PE.4031012	Failed to verify the project ID.	Check whether the parameter meets requirements.
SVCSTG.PE.5001203	Query error.	Contact technical support.

5.1.5 Querying a Policy

Function

This API is used to query details about a policy of a specified project.

URI

GET /v1/{project_id}/pe/policy/{policy_id}

Table 5-29 describes the parameters.

Table 5-29 Parameters

Parameter	Mandatory	Description
project_id	Yes	Project ID.
policy_id	Yes	Policy ID.

Request

Request headers

None

Request parameters

None

Example request

None

Response

Response parameters

Table 5-30 describes the response parameters.

Table 5-30 Response parameters

Parameter	Type	Description
errorCode	String	Error code.
errorMessage	String	Error details.
policy	See **Table 5-31**.	Details about a modified policy.

Table 5-31 policy parameters

Parameter	Type	Description
id	String	Policy ID.
name	String	Policy name.
policy_type	String	Policy type.
rule	See **Table 5-32**.	Policy trigger rule.
create_time	String	Creation time.
update_time	String	Update time.
status	String	Status.

Table 5-32 rule parameters

Parameter	Type	Description
name	String	Policy name.
conditions	See **Table 5-33**.	Condition contents.
actions	See **Table 5-34**.	Action executed after a specified policy is successfully matched.

Table 5-33 conditions parameters

Parameter	Type	Description
metric_namespace	String	Namespace.
metric_name	String	Metric name.
metric_unit	String	Unit.
period	Integer	Statistical period (unit: s).
evaluation_periods	Integer	Number of consecutive periods.
statistic	String	Statistic.
metric_operation	String	Metric operator.
metric_threshold	Float	Threshold criterion.

Table 5-34 actions parameters

Parameter	Type	Description
type	String	Scale-in or -out. The value containing **k8s** indicates a container application and that containing **vm** indicates a process application.
parameters	See **Table 5-35**.	Number of scale-in or -out instances.

Table 5-35 parameters

Parameter	Type	Description
scale_unit	Integer	Number of scale-in or -out instances.

Example response


```
{
   "errorCode" : "SVCSTG.PE.0",
   "errorMessage" : "",
   "policy" : {
      "id" : "8accffb6-e0ed-4433-b216-ccf6960eb1ad",
      "name" : "alarm",
      "group_id" : "77c37e1f-aa0c-438d-8445-39b3997786a2",
      "policy_type" : "ALARM",
      "rule" : {
         "name" : "",
         "conditions" : [{
               "metric_namespace" : "PAAS.CONTAINER",
               "metric_name" : "cpuCoreLimit",
               "metric_unit" : "Percent",
               "period" : 60,
               "evaluation_periods" : 1,
               "statistic" : "average",
               "metric_operation" : "\u003e",
               "metric_threshold" : 100,
               "metric_dimensions" : null
            }
         ],
         "actions" : [{
               "type" : "scale_out_k8s",
               "parameters" : {
                  "scale_unit" : 1
               }
            }
         ]
      },
      "create_time" : "2017-12-21T09:13:42Z",
      "update_time" : "2017-12-21T09:13:42Z",
      "status" : "enabled"
   }
}
```


Error Code

Table 5-36 Error codes

Error Code	Message	Solution
SVCSTG.PE.4031012	Failed to verify the project ID.	Check whether the parameter meets requirements.
SVCSTG.PE.5001203	Query error.	Contact technical support.

5.1.6 Modifying Policy Group Attributes

Function

This API is used to modify policy group attributes.

URI

PUT /v1/{project_id}/pe/policy/config

Table 5-37 describes the parameters.

Table 5-37 Parameters

Parameter	Mandatory	Description
project_id	Yes	Project ID.

Request

Request headers

Table 5-38 describes the request headers.

Table 5-38 Request headers

Parameter	Description	Mandatory	Example
ResourceType	Resource type.	Yes	Default value: app, indicates modifying the policy group attributes of an application.
Cluster-Id	Cluster ID.	Yes	-
Namespace	Namespace.	Yes	-
Deployment-Name	Application name.	Yes	-

Request parameters

Table 5-39 describes the request parameters.

Table 5-39 Request parameters

Parameter	Type	Description
max_instances	Integer	Maximum number of instances.
min_instances	Integer	Minimum number of instances.
cooldown_time	Integer	Cooldown period (unit: s).
deployment_name	String	Microservice name.
cluster_id	String	Cluster ID.

Parameter	Type	Description
namespace	String	Namespace.

Example request

```
{
      "max_instances": 100,//Maximum number of instances
      "min_instances": 1,//Minimum number of instances
        "cooldown_time": 60//Cooldown period, which is the execution interval between two policies.
}
```

Response

Response parameters

Table 5-40 describes the response parameters.

Table 5-40 Response parameters

Parameter	Type	Description
errorCode	String	Error code.
errorMessage	String	Error details.

Example response

```
{
    "errorCode": "SVCSTG.PE.0",
    "errorMessage": ""
}
```

Error Code

Table 5-41 Error codes

Error Code	Message	Solution
SVCSTG.PE.4001101	Invalid parameter.	Check whether the parameter meets requirements.
SVCSTG.PE.4031012	Failed to verify the project ID.	Check whether the parameter meets requirements.
SVCSTG.PE.5001201	Failed to insert or update data in the background.	Contact technical support.
SVCSTG.PE.5001203	Query error.	Contact technical support.

5.1.7 Querying Policy Group Attributes

Function

This API is used to query policy group attributes.

URI

GET /v1/{project_id}/pe/policy/config

Table 5-42 describes the parameters.

Table 5-42 Parameters

Parameter	Mandatory	Description
project_id	Yes	Project ID.

Request

Request headers

Table 5-43 describes the request headers.

Table 5-43 Request headers

Parameter	Description	Mandatory	Example
ResourceType	Resource type.	Yes	Default value: app, indicates querying the policy group attributes of an application.
Content-Type	Content type, which is **application/json;charset=utf-8**.	Yes	application/json;charset=utf-8
Cluster-Id	Cluster ID.	Yes	-
Namespace	Namespace.	Yes	-
Deployment-Name	Application name.	Yes	-

Response

Response parameters

Table 5-44 describes the response parameters.

Table 5-44 Response parameters

Parameter	Type	Description
errorCode	String	Error code.
errorMessage	String	Error details.
config	See Table 5-45.	Set of policy group attributes.

Table 5-45 config parameters

Parameter	Type	Description
id	String	ID of a policy group attribute.
max_instances	Integer	Maximum number of instances.
min_instances	Integer	Minimum number of instances.
cooldown_time	Integer	Cooldown period (unit: s).

Example response

```
{
    "errorCode": "SVCSTG.PE.0",
     "errorMessage": "",
     "config": {
         "id":"f9c7f57e-b1dc-4ef0-a009-ff2848776803",
         "max_instances": 100,//Maximum number of instances
         "min_instances": 1,//Minimum number of instances
         "cooldown_time": 60//Cooldown period, which is the execution interval between two policies.
     }
}
```

Error Code

Table 5-46 Error codes

Error Code	Message	Solution
SVCSTG.PE.4031012	Failed to verify the project ID.	Check whether the parameter meets requirements.
SVCSTG.PE.5001203	Query error.	Contact technical support.

5.2 Common Monitoring APIs (Offline Soon)

5.2.1 Adding or Modifying One or More Application Discovery Rules (Offline Soon)

Function

This API is used to add or modify one or more application discovery rules. A maximum of 100 rules can be added to a project.

URI

PUT /v1/{project_id}/inv/servicediscoveryrules

Request

Request parameters

Table 5-47 describes the request parameter.

Table 5-47 Request parameter

Parameter	Mandatory	Type	Value Range	Description
appRules	No	Array	-	See Table 5-48.

Table 5-48 appRules parameters

Parameter	Mandatory	Type	Value Range	Description
projectid	Yes	String	-	Project ID obtained from IAM. Generally, a project ID contains 32 characters.

Parameter	Mandatory	Type	Value Range	Description
id	Yes	String	-	Rule ID. When creating a discovery rule, leave this parameter blank. When modifying a discovery rule, enter a rule ID.
name	Yes	String	The value can contain a maximum of 64 characters. It must start with a lowercase letter but cannot end with a hyphen (-). Only digits, lowercase letters, and hyphens are allowed.	Rule name.
createTime	No	String	-	Creation time. When creating a discovery rule, leave this parameter blank. When modifying a discovery rule, enter the returned **createTime**.
enable	Yes	Boolean	true or false	Whether to enable a rule.
hostid	No	Array	-	Host ID. Currently, this parameter is not used and can be left blank.

Parameter	Mandatory	Type	Value Range	Description
eventName	Yes	String	aom_inventory_rules_event	Rule event name. For application discovery, the value is fixed to **aom_inventory_rules_event**.
spec	Yes	Object	-	Rule details. See **Table 5-49**.

Table 5-49 spec parameters

Parameter	Mandatory	Type	Value Range	Description
detectLog	Yes	String	true or false	Whether to enable log collection.
logFileFix	Yes	Array	**log**, **trace**, or **out**	Log file suffix.

Parameter	Mandatory	Type	Value Range	Description
discoveryRule	Yes	Array	• If the value of **checkType** is **cmdLine**, set the value of **checkMode** to **contain**. **checkContent** is in the format of **["xxx"]**, indicating that the process must contain the **xxx** parameter. • If the value of **checkType** is **env**, set the value of **checkMode** to **contain**. **checkContent** is in the format of **["k1","v1"]**, indicating that the process must contain the environment variable whose name is **k1** and value is **v1**. • If the value of	Discovery rule. When it is an array consisting of multiple conditions, only the processes that meet all the conditions are filtered. See **Table 5-50**.

Parameter	Mandatory	Type	Value Range	Description
			checkType is **scope**, set the value of **checkMode** to **equals**. **checkContent** is in the format of **["hostId1","hostId2"]**, indicating that the rule takes effect only on specified nodes. If no nodes are specified, the rule applies to all nodes of the project.	
attrList	No	Array	**cmdLine** or **env**	Attribute list. Currently, this parameter is not used and can be left blank.
isDetect	Yes	String	true or false	Whether the scenario is a pre-check scenario. No rules will be saved in the pre-check scenario. This scenario is designed only to check rules before they are delivered.

Parameter	Mandatory	Type	Value Range	Description
isDefaultRule	Yes	String	true or false	Whether this rule will become the default rule.
priority	Yes	Integer	An integer from 1 to 9999. Default value: 9999.	Rule priority.
nameRule	Yes	Object	-	Naming requirements of the application discovery rule. See **Table 5-51**.
appType	Yes	String	-	Application type, which is used to categorize applications and is used only for rule classification and UI display. Enter any field. For example, enter **Java** or **Python** by technology stack, or enter **collector** or **database** by function.

Parameter	Mandatory	Type	Value Range	Description
logPathRule	No	Array	• If **cmdLineHash** is a fixed string, a log path or log file is specified. Otherwise, only the files whose names end with **.log** and **.trace** are collected. • If the value of **nameType** is **cmdLineHash**, **args** is in the format of **["00001"]** and **value** is in the format of **["/xxx/xx.log"]**, indicating that the log path is **/xxx/xx.log** when the startup command is **00001**.	Log path configuration rule. See **Table 5-54**.

Table 5-50 discoveryRule parameters

Parameter	Mandatory	Type	Value Range	Description
checkType	Yes	String	**cmdLine**, **env**, or **scope**	Match type.
checkMode	Yes	String	**contain** or **equals**	Match condition.

Parameter	Mandatory	Type	Value Range	Description
checkContent	Yes	Array	-	Matched value.

Table 5-51 nameRule parameters

Parameter	Mandatory	Type	Value Range	Description
appNameRule	Yes	Array	• If the value of **nameType** is **cmdLine**, **args** is in the format of **["start", "end"]**, indicating that the characters between **start** and **end** in the command are extracted. • If the value of **nameType** is **cmdLine**, **args** is in the format of **["aa"]**, indicating that the environment variable named **aa** is extracted. • If the value of **nameType** is **str**, **args** is in the format of **["fix"]**, indicating that the application name is suffixed with **fix**.	Application name rule. If there are multiple objects in an array, the character strings extracted from these objects constitute the application name. See **Table 5-52**.

Parameter	Mandatory	Type	Value Range	Description
			• If the value of **nameType** is **cmdLineHash**, **args** is in the format of **["0001"]** and **value** is in the format of **["ser"]**, indicating that the application name is **ser** when the startup command is **0001**.	

Parameter	Mandatory	Type	Value Range	Description
applicationNameRule	Yes	Array	• If the value of **nameType** is **cmdLine**, **args** is in the format of **["start", "end"]**, indicating that the characters between **start** and **end** in the command are extracted. • If the value of **nameType** is **cmdLine**, **args** is in the format of **["aa"]**, indicating that the environment variable named **aa** is extracted. • If the value of **nameType** is **str**, **args** is in the format of **["fix"]**, indicating that the application name is suffixed with **fix**. • If the value of	Application name rule. See **Table 5-53**.

Parameter	Mandatory	Type	Value Range	Description
			nameType is **cmdLineHash**, **args** is in the format of **["0001"]** and **value** is in the format of **["ser"]**, indicating that the application name is **ser** when the startup command is **0001**.	

Table 5-52 appNameRule parameters

Parameter	Mandatory	Type	Value Range	Description
nameType	Yes	String	**cmdLineHash**, **cmdLine**, **env**, or **str**	Value type.
args	Yes	Array	-	Input value.
value	No	Array	-	Application name, which is mandatory only when the value of **nameType** is **cmdLineHash**.

Table 5-53 applicationNameRule parameters

Parameter	Mandatory	Type	Value Range	Description
nameType	Yes	String	**cmdLineHash**, **cmdLine**, **env**, or **str**	Value type.
args	Yes	Array	-	Input value.

Parameter	Mandatory	Type	Value Range	Description
value	No	Array	-	Application name, which is mandatory only when the value of **nameType** is **cmdLineHash**.

Table 5-54 logPathRule parameters

Parameter	Mandatory	Type	Value Range	Description
nameType	Yes	String	cmdLineHash	Value type.
args	Yes	Array	-	Command.
value	Yes	Array	-	Log path.

Request headers

Table 5-55 describes the request headers.

Table 5-55 Request headers

Parameter	Mandatory	Description
X-Auth-Token	Yes	User token obtained from IAM.
Content-Type	Yes	Content type, which is **application/json**.

Example request

```
{
   "appRules": [
      {
         "id": "",
         "name": "bytest",
         "createTime": "",
         "projectid": "5a6036f48e954fcd84d198cb28db311a",
         "enable": true,
         "hostid": [],
         "eventName": "aom_inventory_rules_event",
         "spec": {
            "detectLog": "true",
            "logFileFix": ["log","trace"],
            "discoveryRule": [
               {
                  "checkType": "cmdLine",
```



```
                "checkMode": "contain",
                "checkContent": ["default"]
            },{
                "checkType": "scope",
                "checkMode": "equals",
                "checkContent": [
                    "44d6c4bb-f673-4bf4-8d33-313832f37b28"
                ]
            }
        ],
        "attrList": ["cmdLine"],
        "isDetect": "false",
        "priority": "1",
        "nameRule": {
            "appNameRule": [
                {
                    "nameType":"cmdLineHash",
                    "args":["00000000001"],
                    "value":["serviceName1"]
                },
                {
                    "nameType": "cmdLine",
                    "args": [
                        "/var/paas/kubernetes/","/kubeconfig"
                    ]
                },
                {
                    "nameType": "env",
                    "args": ["APP_NAME"]
                },
                {
                    "nameType": "str",
                    "args": ["kube"]
                }
            ],
            "applicationNameRule": [
                {
                    "nameType":"cmdLineHash",
                    "agrs":["00000000001"],
                    "value":["applicationName1"]
                },

                {
                    "nameType": "str",
                    "args": ["kubeproxy"]
                }
            ]
        },
        "appType": "",
        "isDefaultRule":"false",
        "logPathRule": [
            {
                "nameType":"cmdLineHash",
                "agrs":["00000000001"],
                "value":["/xx/xxx/xx.log","/xx/xxx/xx"]
            }
        ]
    }
  }
 ]
}
```

Response

Response parameters

Table 5-56 describes the response parameters.

Table 5-56 Response

Parameter	Type	Description
errorCode	String	Response code.
errorMessage	String	Response message.

Example response

```
{
    "errorCode":"SVCSTG.INV.2000000",
    "errorMessage":""
}
```

Status Code

- Success response

  Table 5-57 describes the status code.

  Table 5-57 Status code

Status Code	Message	Description
200	OK	The request is successful.

- Error response

  Table 5-58 describes the status codes. For more information, see 8.1 Status Codes.

  Table 5-58 Status codes

Status Code	Message	Description
400	Bad Request	Invalid request. The client should not repeat the request without modifications.
401	Unauthorized	The authentication information is incorrect or invalid.
403	Forbidden	The request is rejected. The server has received the request and understood it, but the server refuses to respond to it. The client should not repeat the request without modifications.
500	Internal Server Error	The server is able to receive the request but unable to understand the request.

Status Code	Message	Description
503	Service Unavailable	The requested service is invalid. The client should not repeat the request without modifications.

Error Code

Table 5-59 Error codes

Error Code	Error Message	Solution
SVCSTG.INV.4030000	Forbidden	Use an authorized account.
SVCSTG.INV.4000115	Invalid request parameter.	Check the parameter.
SVCSTG.INV.5000002	The Elasticsearch execution is abnormal.	Contact technical support.
SVCSTG.INV.5000003	The call ICMGR is abnormal.	Contact technical support.
SVCSTG.INV.5000001	The Elasticsearch session is null.	Contact technical support.
SVCSTG.INV.5000006	The apprule name already exists.	Use another name.
SVCSTG.INV.5000007	The maximum number of rules has been reached.	Delete unnecessary rules and add new rules.

5.2.2 Querying Threshold Rules (Offline Soon)

Function

This API is used to query a threshold rule list.

URI

GET /v1/{project_id}/ams/alarms

For details about the substitute of this API, see **Querying the Threshold Rule List**.

Request

Request parameters

Table 5-60 describes the request parameters.

Table 5-60 Request parameters

Parameter	Mandatory	Type	Value Range	Description
project_id	Yes	String	-	Project ID applied from Identity and Access Management (IAM). Generally, it is a string containing 32 characters.
limit	No	Integer	(0,1000]	Maximum number of returned records. Value range: 1–1000. Default value: 1000.
start	No	String	-	Pagination information.

Request headers

Table 5-61 describes the request headers.

Table 5-61 Request headers

Name	Mandatory	Description
X-Auth-Token	Yes	User token obtained from IAM.
Content-Type	Yes	Content type, which is **application/json**.

Response

Response parameters

Table 5-62 describes the response parameters.

Table 5-62 Response parameters

Parameter	Type	Description
errorCode	String	Response code.
errorMessage	String	Response message.
metaData	Object	Metadata, including pagination information.
metaData.count	Integer	Number of returned records.
metaData.total	Integer	Total number of records.
metaData.start	String	Start of the next page, which is used for pagination.
thresholds	Array	Threshold rule list.

Example response


```
{
   "errorCode": "SVCSTG.AMS.2000",
   "errorMessage": "success",
   "metaData": {
     "count": 10,
     "start": null,
     "total": 100
   },
   "thresholds":
   [
   {
       "id": "2137",
       "alarmName": "aaaaaaaa",
       "alarmDescription": "",
       "actionEnabled": false,
       "okActions": [],
       "alarmActions": [],
       "insufficientDataActions": [],
       "stateValue": "alarm",
       "stateReason": "",
       "stateUpdatedTimestamp": null,
       "metricName": "cpuCoreLimit",
       "namespace": "PAAS.CONTAINER",
       "statistic": "average",
       "dimensions": [
          {
              "name": "appName",
              "value": "rhm-broker"
          }
       ],
       "period": 60000,
       "evaluationPeriods": 1,
       "unit": "Core",
       "threshold": "0",
       "comparisonOperator": ">=",
       "alarmAdvice": "",
       "alarmLevel": 3
   }
   ]
}
```


Status Code

- Success response

  Table 5-63 describes the status code.

  Table 5-63 Status code

Status Code	Message	Description
200	OK	The request has succeeded.

- Error response

  Table 5-64 describes the status codes. For more information, see 8.1 Status Codes.

  Table 5-64 Status codes

Status Code	Message	Description
400	Bad Request	The request is invalid. The client should not repeat the request without modifications.
401	Unauthorized	The authorization information provided by the client is incorrect or invalid.
403	Forbidden	The request is rejected. The server has received the request and understood it, but the server is refusing to respond to it. The client should not repeat the request without modifications.
500	InternalServerError	The server is able to receive the request but unable to understand the request.
503	Service Unavailable	The requested service is invalid. The client should not repeat the request without modifications.

Error Code

Table 5-65 Error codes

Error Code	Message	Solution
SVCSTG_AMS_4000109	Invalid project ID.	Check whether the parameter meets requirements.

Error Code	Message	Solution
SVCSTG_AMS_4000110	Invalid limit.	Check whether the parameter meets requirements.
SVCSTG_AMS_4000111	Invalid start.	Check whether the parameter meets requirements.
SVCSTG_AMS_5030001	The Cassandra session is null.	Contact technical support.
SVCSTG_AMS_5030002	The Cassandra execution is abnormal.	Contact technical support.

5.2.3 Modifying a Threshold Rule (Offline Soon)

Function

This API is used to modify a threshold rule.

URI

PUT /v1/{project_id}/ams/alarms

For details about the substitute of this API, see **Modifying a Threshold Rule**.

Request

Request parameters

Table 5-66 describes the request parameters.

Table 5-66 Request parameters

Parameter	Mandatory	Type	Value Range	Description
project_id	Yes	String	-	Project ID applied from Identity and Access Management (IAM). Generally, it is a string containing 32 characters.
statistic	Yes	String	maximum, minimum, average, sum, or sampleCount.	Statistic.

Parameter	Mandatory	Type	Value Range	Description
namespace	Yes	String	-	Namespace. The value of this parameter is saved in the backend when a threshold rule is added. It cannot be changed.
metricName	Yes	String	The value must be 1 to 255 characters long and meet the [a-zA-Z_:][a-zA-Z0-9_:]* expression. That is, the value must start with a letter, underscore (_), or colon (:). Only letters, digits, underscores, and colons are allowed.	Metric name. The value of this parameter is saved in the backend when a threshold rule is added. It cannot be changed.
period	Yes	Integer	-	Statistical period.
alarmLevel	Yes	Integer	-	Alarm severity.
evaluationPeriods	Yes	Integer	-	Number of consecutive periods.
comparisonOperator	Yes	String	-	Threshold criterion expression.
threshold	Yes	String	-	Threshold.
alarmName	Yes	String	-	Threshold name.
dimensions	Yes	String	-	Metric dimension. The value of this parameter is saved in the backend when a threshold rule is added. It cannot be changed.

Parameter	Mandatory	Type	Value Range	Description
unit	Yes	String	-	Metric unit. The value of this parameter is saved in the backend when a threshold rule is added. It cannot be changed.
actionEnabled	No	Boolean	-	Whether to enable the alarm function.
alarmActions	No	Array	-	Alarm action.
alarmAdvice	No	String	-	Alarm suggestion, which is an empty string.
alarmDescription	No	String	-	Threshold rule description.
insufficientDataActions	No	Array	-	Action to be taken when data is insufficient.
okActions	No	Array	-	Recovery action.

Request headers

Table 5-67 describes the request headers.

Table 5-67 Request headers

Name	Mandatory	Description
X-Auth-Token	Yes	User token obtained from IAM.
Content-Type	Yes	Content type, which is **application/json**.

Example request

```
{
  "actionEnabled": false,
  "alarmActions": [],
  "alarmAdvice": "",
  "alarmDescription": "",
  "alarmLevel": 3,
  "alarmName": "aaaaaaaa",
  "comparisonOperator": ">=",
```



```
  "dimensions": [
    {
      "name": "appName",
      "value": "rhm-broker"
    }
  ],
  "evaluationPeriods": 1,
  "insufficientDataActions": [],
  "metricName": "cpuCoreLimit",
  "namespace": "PAAS.CONTAINER",
  "okActions": [],
  "period": 60000,
  "statistic": "average",
  "threshold": 0,
  "unit": "Core"
}
```

Response

Response parameters

Table 5-68 describes the response parameters.

Table 5-68 Response parameters

Parameter	Type	Description
errorCode	String	Response code.
errorMessage	String	Response message.
alarmId	Integer	Threshold rule code.

Example response

```
{
  "errorCode": "SVCSTG.AMS.2000",
  "errorMessage": "success",
  "alarmId": 12345678
}
```

Status Code

- Success response

  Table 5-69 describes the status code.

  Table 5-69 Status code

Status Code	Message	Description
200	OK	The request has succeeded.

- Error response

  Table 5-70 describes the status codes. For more information, see 8.1 Status Codes.

Table 5-70 Status codes

Status Code	Message	Description
400	Bad Request	The request is invalid. The client should not repeat the request without modifications.
401	Unauthorized	The authorization information provided by the client is incorrect or invalid.
403	Forbidden	The request is rejected. The server has received the request and understood it, but the server is refusing to respond to it. The client should not repeat the request without modifications.
500	InternalServerError	The server is able to receive the request but unable to understand the request.
503	Service Unavailable	The requested service is invalid. The client should not repeat the request without modifications.

Error Code

Table 5-71 Error codes

Error Code	Message	Solution
SVCSTG_AMS_4000101	Invalid alarm name.	Check whether the parameter meets requirements.
SVCSTG_AMS_4000102	The threshold rule name already exists.	Use another name.
SVCSTG_AMS_4000103	Invalid alarm description.	Check whether the parameter meets requirements.
SVCSTG_AMS_4000104	Invalid alarm threshold.	Check whether the parameter meets requirements.
SVCSTG_AMS_4000105	Invalid alarm period.	Check whether the parameter meets requirements.

Error Code	Message	Solution
SVCSTG_AMS_4000106	Invalid email list.	Check whether the parameter meets requirements.
SVCSTG_AMS_4000107	The maximum number of threshold rules has been reached.	Contact technical support to expand the capacity.
SVCSTG_AMS_4000108	Invalid time range for alarm queries.	Check whether the parameter meets requirements.
SVCSTG_AMS_4000109	Invalid project ID.	Check whether the parameter meets requirements.
SVCSTG_AMS_4000115	Invalid request parameter.	Check whether the parameter meets requirements.
SVCSTG_AMS_4000118	Invalid number of consecutive periods.	Check whether the parameter meets requirements.
SVCSTG_AMS_4000119	Invalid alarm statistic.	Check whether the parameter meets requirements.
SVCSTG_AMS_4000120	Invalid alarm comparison operator.	Check whether the parameter meets requirements.
SVCSTG_AMS_4000121	The alarm does not exist.	Check whether the threshold rule exists.
SVCSTG_AMS_5000000	Internal server error.	Contact technical support.

5.2.4 Adding a Threshold Rule (Offline Soon)

Function

This API is used to add a threshold rule.

URI

POST /v1/{project_id}/ams/alarms

For details about the substitute of this API, see **Adding a Threshold Rule**.

Request

Request parameters

Table 5-72 describes the request parameters.

Table 5-72 Request parameters

Parameter	Mandatory	Type	Value Range	Description
project_id	Yes	String	-	Project ID applied from Identity and Access Management (IAM). Generally, it is a string containing 32 characters.
statistic	Yes	String	maximum, minimum, average, sum, or sampleCount.	Statistic.
namespace	Yes	String	-	Namespace.
metricName	Yes	String	The value must be 1 to 255 characters long and meet the [a-zA-Z_:][a-zA-Z0-9_:]* expression. That is, the value must start with a letter, underscore (_), or colon (:). Only letters, digits, underscores, and colons are allowed.	Metric name.
period	Yes	Integer	-	Statistical period.
alarmLevel	Yes	Integer	-	Alarm severity.
evaluationPeriods	Yes	Integer	-	Number of consecutive periods.
comparisonOperator	Yes	String	-	Threshold criterion expression.

Parameter	Mandatory	Type	Value Range	Description
threshold	Yes	String	-	Threshold.
alarmName	Yes	String	-	Threshold name.
dimensions	Yes	String	-	Metric dimension.
unit	Yes	String	-	Metric unit.
actionEnabled	No	Boolean	-	Whether to enable the alarm function.
alarmActions	No	Array	-	Alarm action.
alarmAdvice	No	String	-	Suggestion.
alarmDescription	No	String	-	Threshold rule description.
insufficientDataActions	No	Array	-	Action to be taken when data is insufficient.
okActions	No	Array	-	Recovery action.

Request headers

Table 5-73 describes the request headers.

Table 5-73 Request headers

Name	Mandatory	Description
X-Auth-Token	Yes	User token obtained from IAM.
Content-Type	Yes	Content type, which is **application/json**.

Example request

```
{
   "actionEnabled": false,
   "alarmActions": [],
   "alarmAdvice": "",
   "alarmDescription": "",
   "alarmLevel": 3,
   "alarmName": "aaaaaaaa",
   "comparisonOperator": ">=",
   "dimensions": [
      {
         "name": "appName",
         "value": "rhm-broker"
```



```
      }
   ],
   "evaluationPeriods": 1,
   "insufficientDataActions": [],
   "metricName": "cpuCoreLimit",
   "namespace": "PAAS.CONTAINER",
   "okActions": [],
   "period": 60000,
   "statistic": "average",
   "threshold": 0,
   "unit": "Core"
}
```

Response

Response parameters

Table 5-74 describes the response parameters.

Table 5-74 Response parameters

Parameter	Type	Description
errorCode	String	Response code.
errorMessage	String	Response message.
alarmId	Integer	Threshold rule code.

Example response

```
{
   "errorCode": "SVCSTG.AMS.2000",
   "errorMessage": "success",
   "alarmId": 12345678
}
```

Status Code

- Success response

  Table 5-75 describes the status code.

  Table 5-75 Status code

Status Code	Message	Description
200	OK	The request has succeeded.

- Error response

  Table 5-76 describes the status codes. For more information, see **8.1 Status Codes**.

Table 5-76 Status codes

Status Code	Message	Description
400	Bad Request	The request is invalid. The client should not repeat the request without modifications.
401	Unauthorized	The authorization information provided by the client is incorrect or invalid.
403	Forbidden	The request is rejected. The server has received the request and understood it, but the server is refusing to respond to it. The client should not repeat the request without modifications.
500	InternalServerError	The server is able to receive the request but unable to understand the request.
503	Service Unavailable	The requested service is invalid. The client should not repeat the request without modifications.

Error Code

Table 5-77 Error codes

Error Code	Message	Solution
SVCSTG_AMS_4000101	Invalid alarm name.	Check whether the parameter meets requirements.
SVCSTG_AMS_4000102	The threshold rule name already exists.	Use another name.
SVCSTG_AMS_4000103	Invalid alarm description.	Check whether the parameter meets requirements.
SVCSTG_AMS_4000104	Invalid alarm threshold.	Check whether the parameter meets requirements.
SVCSTG_AMS_4000105	Invalid alarm period.	Check whether the parameter meets requirements.

Error Code	Message	Solution
SVCSTG_AMS_4000106	Invalid email list.	Check whether the parameter meets requirements.
SVCSTG_AMS_4000107	The maximum number of threshold rules has been reached.	Contact technical support to expand the capacity.
SVCSTG_AMS_4000108	Invalid time range for alarm queries.	Check whether the parameter meets requirements.
SVCSTG_AMS_4000109	Invalid project ID.	Check whether the parameter meets requirements.
SVCSTG_AMS_4000115	Invalid request parameter.	Check whether the parameter meets requirements.
SVCSTG_AMS_4000118	Invalid number of consecutive periods.	Check whether the parameter meets requirements.
SVCSTG_AMS_4000119	Invalid alarm statistic.	Check whether the parameter meets requirements.
SVCSTG_AMS_4000120	Invalid alarm comparison operator.	Check whether the parameter meets requirements.
SVCSTG_AMS_4000121	The alarm does not exist.	Check whether the threshold rule exists.
SVCSTG_AMS_5000000	Internal server error.	Contact technical support.

5.2.5 Querying Monitoring Data (Offline Soon)

Function

This API is used to query monitoring data of metrics within a specified time period. You can specify a dimension or period to query data.

URI

POST /v1/{project_id}/ams/metricdata?fillValue=xx

For details about the substitute API, see **Querying Monitoring Data**.

Table 5-78 describes the parameters.

Table 5-78 Parameters

Parameter	Mandatory	Type	Value Range	Description
project_id	Yes	String	-	Project ID applied from Identity and Access Management (IAM). Generally, it is a string containing 32 characters.
fillValue	No	String	–1, 0, null, and average	Filled value for breakpoints in monitoring data. Default value: –1. • -1: Breakpoints are filled with –1. • 0: Breakpoints are filled with 0. • null: Breakpoints are filled with null. • average: Breakpoints are filled with the average value of adjacent valid data. If there is no valid data, breakpoints are filled with null.

Request

Request parameters

Table 5-79 describes the request parameters.

Table 5-79 Request parameters

Parameter	Mandatory	Type	Value Range	Description
metrics	Yes	Array	The JSON array can contain a maximum of 20 metrics.	List of metrics.
namespace	Yes	String	PAAS.CONTAINER, PAAS.NODE, PAAS.SLA, PAAS.AGGR, and CUSTOMMETRICS.	Metric namespace.

Parameter	Mandatory	Type	Value Range	Description
metricName	Yes	String	1–255 characters.	Metric name.
dimensions	Yes	Array	Neither the array, nor the name/value of any dimension in the array can be left blank.	Metric dimension. dimensions.name: dimension name. Example: appName. dimensions.value: dimension value, such as a specific application name.
period	Yes	Integer	Enumerated value. Options: • 60: The data monitoring granularity is 1 minute. • 300: The data monitoring granularity is 5 minutes. • 900: The data monitoring granularity is 15 minutes. • 3600: The data monitoring granularity is 1 hour.	Data monitoring granularity.

Parameter	Mandatory	Type	Value Range	Description
timerange	Yes	String	Format: start time (UTC, in ms).end time (UTC, in ms).number of minutes in the time period When the start time and end time are –1, it indicates the latest *N* minutes. *N* indicates the time period by the granularity of minute.	Query time period. For example, **–1.–1.5** indicates the latest 5 minutes. **1501545600000.1501632000000.1440** indicates the fixed time period from 08:00:00 on August 1, 2017 to 08:00:00 August 2, 2017. **NOTE** Time range/period ≤ 1440 During calculation, **timerange** and **period** must be in the same unit.
statistics	Yes	Array	maximum, minimum, sum, average, or sampleCount.	Statistic.

Request headers

Table 5-80 describes the request headers.

Table 5-80 Request headers

Name	Mandatory	Description
X-Auth-Token	Yes	User token obtained from IAM.
Content-Type	Yes	Content type, which is **application/json**.

Example request

```
{
   "metrics": [
      {
         "namespace": "abc",
         "metricName": "def",
         "dimensions": [
            {
               "name": "instance_id",
```



```
                "value": "demo1"
            }
        ]
    }
  ],
  "period": 60,
  "timerange": "-1.-1.5",//Last 5 minutes
    "statistics": [
      "maximum",
      "minimum",
      "sum"
  ]
}
```

Response

Response parameters

Table 5-81 describes the response parameters.

Table 5-81 Response parameters

Parameter	Type	Description
errorCode	String	Response code.
errorMessage	String	Response message.
metrics	Object	-

Example response

```
{
  "errorCode": "SVCSTG.AMS.2000",
  "errorMessage": "success",
  "metrics": [{
    "metric": {
      "namespace": "abc",
      "metricName": "def",
      "dimensions": [{
        "name": "ghi",
        "value": "lmn"
      }]
    },
    "dataPoints": [{
      "timestamp": 1467892800000,
      "unit": "Percent",
      "statistics": [{
        "statistic": "maximum",
        "value": 23
      }]
    }]
  }]
}
```

Status Code

- Success response

  Table 5-82 describes the status code.

Table 5-82 Status code

Status Code	Message	Description
200	OK	The request has succeeded.

- Error response

  Table 5-83 describes the status codes. For more information, see **8.1 Status Codes**.

  Table 5-83 Status codes

Status Code	Message	Description
400	Bad Request	The request is invalid. The client should not repeat the request without modifications.
401	Unauthorized	The authorization information provided by the client is incorrect or invalid.
403	Forbidden	The request is rejected. The server has received the request and understood it, but the server is refusing to respond to it. The client should not repeat the request without modifications.
500	InternalServerError	The server is able to receive the request but unable to understand the request.
503	Service Unavailable	The requested service is invalid. The client should not repeat the request without modifications.

Error Code

Table 5-84 Error codes

Error Code	Message	Solution
SVCSTG_AMS_4000101	Projectid is left blank.	Check whether the parameter meets requirements.
SVCSTG_AMS_4000102	The metric data parameter is null.	Check whether the parameter meets requirements.

Error Code	Message	Solution
SVCSTG_AMS_4000103	Invalid period.	Check whether the parameter meets requirements.
SVCSTG_AMS_4000104	Invalid statistics.	Check whether the parameter meets requirements.
SVCSTG_AMS_4000105	Invalid metrics.	Check whether the parameter meets requirements.
SVCSTG_AMS_4000106	Invalid time range.	Check whether the parameter meets requirements.
SVCSTG_AMS_4000107	The number of data points in a time range exceeds 1440.	Check whether the parameter meets requirements.
SVCSTG_AMS_4000110	Invalid fillValue.	Check whether the parameter meets requirements.
SVCSTG_AMS_5000000	Internal server error.	Contact technical support.

6 Examples

6.1 Querying Time Series Objects

Scenario

Host Metrics - Dimension This sec**Host Metrics**tion describes how to query time series objects about a node's CPU usage.

Obtaining Basic Information

Before querying time series objects, obtain the value of the node ID from **dimensions** on the ECS console, and the value of the cluster ID from **dimensions** on the cluster management page of the CCE console.

For **metric_name** of CPU usage, see **Host Metrics**. For the **name** corresponding to the cluster ID or node ID, see **Host Metrics - Dimension**. For the namespace, see **Table 4 QuerySeriesOptionParam**.

Querying Time Series Objects

- URI format

  POST /v2/*{project_id}***/series**
- Example request

  POST https://{aom_endpoint}/v2/{project_id}/series

  To obtain the value of *{aom_endpoint}*, see **Regions and Endpoints**..

  Body:

```
{
   "series": [
      {
         "namespace": "PAAS.NODE",
         "metric_name": "aom_node_cpu_usage",
         "dimensions":[
            {
               "name":"clusterId",
               "value":"4fae3587-0202-11eb-9ba9-0255ac100b02"
            },
            {
               "name":"hostID",
               "value":"4100f512-c4e9-4b65-b0dd-2b94ea5e1a84"
            }
```



```
            ]
        }
    ]
}
```

- Example response

```
{
    "meta_data": {
        "count": 0,
        "offset": 0,
        "total": 1,
        "nextToken": 9007148492074133276
    },
    "series": [{
        "namespace": "PAAS.NODE",
        "metric_name": "cpuUsage",
        "unit": "Percent",
        "dimensions": [{
            "name": "clusterId",
            "value": "4fae3587-0202-11eb-9ba9-0255ac100b02"
        },
        {
            "name": "clusterName",
            "value": "testdiskrate"
        },
        {
            "name": "hostID",
            "value": "4100f512-c4e9-4b65-b0dd-2b94ea5e1a84"
        },
        {
            "name": "nameSpace",
            "value": "default"
        },
        {
            "name": "nodeIP",
            "value": "192.168.0.123"
        },
        {
            "name": "nodeName",
            "value": "192.168.0.123"
        }]
    }]
}
```

6.2 Querying Time Series Data

Scenario

This section describes how to query the time series data about a node's CPU usage.

Obtaining Basic Information

Before querying time series data, obtain the value of the node ID from **dimensions** on the ECS console, and the value of the cluster ID from **dimensions** on the cluster management page of the CCE console.

Some metrics may be renamed due to format standardization. For the input parameter **metric_name** for CPU usage used in this scenario, see the **metric_name** (not renamed) returned when you call the API for **querying time series objects** (to call this API, set the input parameter **metric_name** to the name queried in s**Host Metrics**.. In this example, the name is **aom_node_cpu_usage**

(renamed)). For the **name** corresponding to the cluster ID or node ID, see **Host Metrics - Dimension**. For the namespace, see **Table 4 QuerySeriesOptionParam**.

Querying Time Series Data

- URI format

  POST /v2/*{project_id}*/samples

- Example request

  POST https://*{aom_endpoint}*/v2/*{project_id}*/samples

  To obtain the value of *{aom_endpoint}*, see **Regions and Endpoints**..

  Body:

```
{
   "samples": [
      {
         "namespace": "PAAS.NODE",
         "metric_name": "cpuUsage",
           "dimensions": [ {
               "name": "clusterId",
               "value": "4fae3587-0202-11eb-9ba9-0255ac100b02"
            },
            {
               "name": "hostID",
               "value": "4100f512-c4e9-4b65-b0dd-2b94ea5e1a84"
            }
         ]
      }
   ],
   "period": 60,
   "time_range": "-1.-1.2",
   "statistics": [
      "maximum",
      "minimum",
      "sum"
   ]
}
```

- Example response

```
{
   "samples": [{
      "sample": {
         "namespace": "PAAS.NODE",
         "metric_name": "cpuUsage",
         "dimensions": [{
            "name": "clusterId",
            "value": "4fae3587-0202-11eb-9ba9-0255ac100b02"
         },
         {
            "name": "hostID",
            "value": "4100f512-c4e9-4b65-b0dd-2b94ea5e1a84"
         }]
      },
      "data_points": [{
         "timestamp": 1608191880000,
         "unit": "Percent",
         "statistics": [{
            "statistic": "maximum",
            "value": 14.5
         },
         {
            "statistic": "minimum",
            "value": 14.5
         },
         {
            "statistic": "sum",
            "value": 14.5
```



```
            }]
        },
        {
            "timestamp": 1608191940000,
            "unit": "Percent",
            "statistics": [{
                "statistic": "maximum",
                "value": 12.0
            },
            {
                "statistic": "minimum",
                "value": 12.0
            },
            {
                "statistic": "sum",
                "value": 12.0
            }]
        }]
    }]
}
```


6.3 Querying Details About a Specified Alarm Action Rule

Scenario

This section describes how to query an alarm action rule by name.

Obtaining Basic Information

Before querying the details about an alarm action rule, obtain its rule name first. You can call the API for obtaining the alarm action rule list or go to the AOM 2.0 console to obtain the rule name.

Querying Details About a Specified Alarm Action Rule

- URI format

  URI format: GET /v2/{*project_id*}/alert/action-rules/{*rule_name*}

- Example request

  GET https://{Endpoint}/v2/{project_id}/alert/action-rules/{rule_name}

  You can obtain the value of *{aom_endpoint}* from **Regions and Endpoints**.

- Example response


```
{
    "create_time": 1665991889597,
    "notification_template": "aom.built-in.template.zh",
    "project_id": "2xxxxxxxxxxxxxxxxxxxxxxf",
    "rule_name": "1112222",
    "smn_topics": [{
        "display_name": "",
        "name": "gxxxxxt",
        "push_policy": 0,
        "status": 0,
        "topic_urn": "urn:smn:xxxx:2xxxxxxxxxxxxxxxxxxxxxxf:gxxxxxt"
    }],
    "time_zone": "xx/XXX",
    "type": "1",
    "update_time": 1665991889597,
```



```
    "user_name": "kxxxxxxxt"
}
```


7 Permissions Policies and Supported Actions

7.1 Introduction

You can use Identity and Access Management (IAM) for fine-grained permissions management of your AOM. If your account does not need individual IAM users, you can skip this topic.

By default, new IAM users do not have any permissions assigned. You need to add a user to one or more groups, and assign permissions policies or roles to these groups. The user then inherits permissions from the groups it is a member of. This process is called authorization. After authorization, the user can perform specified operations on AOM.

You can grant users permissions by using roles and policies. Roles are provided by IAM to define service-based permissions that match users' job responsibilities. Policies define API-based permissions for operations on specific resources under certain conditions, allowing for more fine-grained, secure access control of cloud resources.

NOTE

If you want to allow or deny the access to an API, use policy-based authorization.

Your account has all the permissions required to call all APIs, but IAM users under your account must be assigned the required permissions. The required permissions are determined by the actions supported by the API. Only users with the policies allowing for those actions can call the API successfully. For example, if an IAM user wants to query metrics using an API, the user must have been granted permissions that allow the **aom:metric:get** action.

Supported Actions

AOM provides system-defined policies that can be directly used in IAM. You can also create custom policies to supplement system-defined policies for more refined access control. Operations supported by policies are specific to APIs. The following are common concepts related to policies:

- Permissions: actions defined in custom policies.

- APIs: REST APIs that can be called by a user who has been granted specific permissions.
- Actions: specific operations that are allowed or denied in a custom policy.
- IAM projects/Enterprise projects: the authorization scope of a custom policy. A custom policy can be applied to IAM projects or enterprise projects or both. Policies that contain actions for both IAM and enterprise projects can be used and applied for both IAM and Enterprise Management. Policies that contain actions only for IAM projects can be used and applied to IAM only. Administrators can check whether an action supports IAM projects or enterprise projects in the action list. For details about the differences between IAM and enterprise management, see **What Are the Differences Between IAM and Enterprise Management?**

AOM supports the following actions that can be defined in custom policies:

- **7.2.1 Alarm APIs**: includes the actions supported by alarm APIs, such as the API for querying alarms.
- **7.2.2 Monitoring APIs**: includes the actions supported by monitoring APIs, such as the API for querying metrics.
- **7.2.3 Prometheus Monitoring APIs**: includes the actions supported by Prometheus monitoring APIs, such as the API for querying the expression calculation result in a specified period.
- **7.2.4 Log APIs**: includes the actions supported by log APIs, such as the API for querying logs.

7.2 Actions Supported by Policy-based Authorization

7.2.1 Alarm APIs

NOTE

√: supported; x: not supported

Table 7-1 Alarm APIs

Permission	API	Action	IAM Project	Enterprise Project
Adding an event alarm rule	POST /v2/{project_id}/event2alarm-rule	aom:event2AlarmRule:create	√	×
Querying the event alarm rule list	GET /v2/{project_id}/event2alarm-rule	aom:event2AlarmRule:list	√	×

Permission	API	Action	IAM Project	Enterprise Project
Modifying an event alarm rule	PUT /v2/{project_id}/event2alarm-rule	aom:event2AlarmRule:set	√	×
Deleting an event alarm rule	DELETE /v2/{project_id}/event2alarm-rule	aom:event2AlarmRule:delete	√	×
Obtaining the sent alarm content	GET /v2/{project_id}/alarm-notified-histories	aom:alarm:list	√	×
Querying an alarm action rule by name	GET /v2/{project_id}/alert/action-rules/{rule_name}	aom:actionRule:get	√	√
Adding an alarm action rule	POST /v2/{project_id}/alert/action-rules	aom:actionRule:create	√	√
Deleting an alarm action rule	DELETE /v2/{project_id}/alert/action-rules	aom:actionRule:delete	√	√
Modifying an alarm action rule	PUT /v2/{project_id}/alert/action-rules	aom:actionRule:update	√	√
Querying the alarm rule list	GET /v2/{project_id}/alert/action-rules	aom:actionRule:list	√	√
Querying events and alarms	POST /v2/{project_id}/events	aom:alarm:list	√	×
Counting events and alarms	POST /v2/{project_id}/events/statistic	aom:alarm:list	√	×

Permission	API	Action	IAM Project	Enterprise Project
Reporting events and alarms	PUT /v2/{project_id}/push/events	aom:alarm:put	√	×

7.2.2 Monitoring APIs

NOTE

√: supported; x: not supported

Table 7-2 Monitoring APIs

Permission	API	Action	IAM Project	Enterprise Project
Querying time series objects	POST /v2/{project_id}/series	aom:metric:list	√	×
Querying time series data	POST /v2/{project_id}/samples	aom:metric:list	√	×
Querying metrics	POST /v1/{project_id}/ams/metrics	aom:metric:get	√	×
Querying monitoring data	POST /v1/{project_id}/ams/metricdata	aom:metric:get	√	×
Adding or modifying a service discovery rule	PUT /v1/{project_id}/inv/servicediscoveryrules	aom:discoveryRule:set	√	×
Deleting a service discovery rule	DELETE /v1/{project_id}/inv/servicediscoveryrules	aom:discoveryRule:delete	√	×

Permission	API	Action	IAM Project	Enterprise Project
Querying existing service discovery rules	GET /v1/{project_id}/inv/servicediscoveryrules	aom:discoveryRule:list	√	×
Adding a threshold rule	POST /v2/{project_id}/alarm-rules	aom:alarmRule:create	√	×
Querying the threshold rule list	GET /v2/{project_id}/alarm-rules	aom:alarmRule:get	√	×
Modifying a threshold rule	PUT /v2/{project_id}/alarm-rules	aom:alarmRule:set	√	×
Deleting a threshold rule	DELETE /v2/{project_id}/alarm-rules/{alarm_rule_id}	aom:alarmRule:delete	√	×
Querying a threshold rule	GET /v2/{project_id}/alarm-rules/{alarm_rule_id}	aom:alarmRule:get	√	×
Deleting threshold rules in batches	POST /v2/{project_id}/alarm-rules/delete	aom:alarmRule:delete	√	×

7.2.3 Prometheus Monitoring APIs

NOTE

√: supported; x: not supported

Table 7-3 Prometheus monitoring APIs

Permission	API	Action	IAM Project	Enterprise Project
Querying the expression calculation result in a specified period	GET /v1/{project_id}/aom/api/v1/query_range	aom:metric:list	√	√
Querying the expression calculation result in a specified period	POST /v1/{project_id}/aom/api/v1/query_range	aom:metric:list	√	√
Querying the expression calculation result at a specified time point	GET /v1/{project_id}/aom/api/v1/query	aom:metric:list	√	√
Querying the expression calculation result at a specified time point	POST /v1/{project_id}/aom/api/v1/query	aom:metric:list	√	√
Querying tag values	GET /v1/{project_id}/aom/api/v1/label/{label_name}/values	aom:metric:list	√	√
Obtaining the tag name list	GET /v1/{project_id}/aom/api/v1/labels	aom:metric:list	√	√

Permission	API	Action	IAM Project	Enterprise Project
Obtaining the tag name list	POST /v1/{project_id}/aom/api/v1/labels	aom:metric:list	√	√
Querying metadata	GET /v1/{project_id}/aom/api/v1/metadata	aom:metric:list	√	√

7.2.4 Log APIs

NOTE

√: supported; x: not supported

Table 7-4 Log APIs

Permission	API	Action	IAM Project	Enterprise Project
Querying logs	POST /v1/{project_id}/als/action	aom:log:list	√	×

7.2.5 CMDB APIs

NOTE

√: supported; x: not supported

Table 7-5 CMDB APIs

Permission	API	Action	IAM Project	Enterprise Project
Adding an application	POST /v1/applications	aom:cmdbApplication:create	√	×
Deleting an application	DELETE /v1/applications/{application_id}	aom:cmdbApplication:delete	√	×

Permission	API	Action	IAM Project	Enterprise Project
Querying the details about an application	GET /v1/applications/{application_id}	aom:cmdbApplication:get	√	×
Modifying an application	PUT /v1/applications/{application_id}	aom:cmdbApplication:update	√	×
Adding a component	POST /v1/components	aom:cmdbComponent:create	√	×
Deleting a component	DELETE /v1/components/{component_id}	aom:cmdbComponent:delete	√	×
Querying the details about a component	GET /v1/components/{component_id}	aom:cmdbComponent:get	√	×
Modifying a component	PUT /v1/components/{component_id}	aom:cmdbComponent:update	√	×
Creating an environment	POST /v1/environments	aom:cmdbEnvironment:create	√	×

Permission	API	Action	IAM Project	Enterprise Project
Deleting an environment	DELETE /v1/environments/{environment_id}	aom:cmdbEnvironment:delete	√	×
Querying the details about an environment	GET /v1/environments/{environment_id}	aom:cmdbEnvironment:get	√	×
Modifying an environment	PUT /v1/environments/{environment_id}	aom:cmdbEnvironment:update	√	×
Querying the list of resources bound to a node	POST /v1/resource/{rf_resource_type}/type/{type}/ci-relationships	aom:cmdbResources:list	√	×
Querying the details about an application	GET /v1/applications	aom:cmdbApplication:get	√	×

Permission	API	Action	IAM Project	Enterprise Project
Querying the details about an environment	GET /v1/environments/name/{environment_name}	aom:cmdbEnvironment:get	√	×
Querying the details about a component	GET /v1/components/application/{application_id}/name/{component_name}	aom:cmdbComponent:get	√	×

8 Appendix

8.1 Status Codes

Table 8-1 describes status codes.

Table 8-1 Status codes

Status Code	Message	Description
100	Continue	The client should continue with its request. This interim response is used to inform the client that the initial part of the requests has been received and not rejected by the server.
101	Switching Protocols	The protocol should be switched. The protocol can only be switched to a more advanced protocol. For example, a new HTTP protocol.
200	OK	The request has succeeded.
201	Created	The request has been fulfilled, resulting in the creation of a new resource.
202	Accepted	The request has been accepted, but the processing has not been completed.
203	Non-Authoritative Information	The server successfully processed the request, but is returning information that may be from another source.
204	No Content	The server has successfully processed the request, but does not return any content. The status code is returned in response to an HTTP OPTIONS request.
205	Reset Content	The server has fulfilled the request, but the requester is required to reset the content.

Status Code	Message	Description
206	Partial Content	The server has successfully processed a part of the GET request.
300	Multiple Choices	There are multiple options for the location of the requested resource. The response contains a list of resource characteristics and addresses from which a user terminal (such as a browser) can choose the most appropriate one.
301	Moved Permanently	The requested resource has been assigned with a new permanent URI. This new URI is contained in the response.
302	Found	The requested resource resides temporarily under a different URI.
303	See Other	The response to the request can be found under a different URI. It should be retrieved using a GET or POST method.
304	Not Modified	The requested resource has not been modified. When the server returns this status code, it does not return any resources.
305	Use Proxy	The requested resource must be accessed through a proxy.
306	Unused	This HTTP status code is no longer used.
400	Bad Request	The request is invalid. The client should not repeat the request without modifications.
401	Unauthorized	The authorization information provided by the client is incorrect or invalid.
402	Payment Required	This status code is reserved for future use.
403	Forbidden	The request is rejected. The server has received the request and understood it, but the server is refusing to respond to it. The client should not repeat the request without modifications.
404	Not Found	The requested resource cannot be found. The client should not repeat the request without modifications.

Status Code	Message	Description
405	Method Not Allowed	The method specified in the request is not supported by the requested resource. The client should not repeat the request without modifications.
406	Not Acceptable	The server cannot fulfill the request based on the content characteristics of the request.
407	Proxy Authentication Required	This status code is similar to 401, but indicates that the client must authenticate itself with the proxy first.
408	Request Timeout	The client does not produce a request within the time that the server was prepared to wait. The client may repeat the request without modifications later.
409	Conflict	The request cannot be processed due to a conflict. The resource that the client attempts to create already exits, or the request fails to be processed because of the update of the conflict request.
410	Gone	The requested resource cannot be found. The requested resource has been deleted permanently.
411	Length Required	The server refuses to process the request without a defined Content-Length.
412	Precondition Failed	The server does not meet one of the preconditions that the requester puts on the request.
413	Request Entity Too Large	The server refuses to process a request because the request entity is too large. The server may disable the connection to prevent the client from sending requests consecutively. If the server cannot process the request temporarily, the response will contain a Retry-After field.
414	Request-URI Too Long	The request URI is too long for the server to process.
415	Unsupported Media Type	The server cannot process the media format in the request.
416	Requested Range Not Satisfiable	The requested range is invalid.
417	Expectation Failed	The server fails to meet the requirements of the Expect request-header field.

Status Code	Message	Description
422	Unprocessable Entity	The request is well-formed but is unable to be processed due to semantic errors.
429	Too Many Requests	The client sends excessive requests to the server within a given time (exceeding the limit on the access frequency of the client), or the server receives excessive requests within a given time (beyond its processing capability). In this case, the client should repeat requests after the time specified in the Retry-After header of the response expires.
500	Internal Server Error	The server is able to receive the request but unable to understand the request.
501	Not Implemented	The server does not support the function required to fulfill the request.
502	Bad Gateway	The server acting as a gateway or proxy receives an invalid response from a remote server.
503	Service Unavailable	The requested service is invalid. The client should not repeat the request without modifications.
504	Server Timeout	The request cannot be fulfilled within a given time. This status code is returned to the client only when the timeout parameter is specified in the request.
505	HTTP Version Not Supported	The server does not support the HTTP protocol version used in the request.

8.2 Error Codes

If an error code starting with **APIGW** is returned after you call an API, rectify the fault according to **APIG Error Codes**.

Status Code	Error Code	Message	Description	Solution
200	SVCSTG.INV.2000000	null	The request is properly executed.	No action is required after the request is executed.

Status Code	Error Code	Message	Description	Solution
200	SVCSTG_AMS_2000000	null	The request is properly executed.	No action is required after the request is executed.
300	AOM.08001300	The maximum number of rules has been reached.	The maximum number of rules has been reached.	Delete unneeded rules and try again.
400	AOM.0400	Bad request.	Incorrect request parameter.	Check whether the parameter meets requirements.
400	AOM.02001101	Invalid rule name.	Invalid rule name.	Check whether the parameter meets requirements.
400	AOM.02001102	The rule name already exists.	The rule name already exists.	Check whether the parameter meets requirements.
400	AOM.02001103	Invalid description.	Invalid description.	Check whether the parameter meets requirements.
400	AOM.02001104	Invalid threshold.	Invalid threshold.	Check whether the parameter meets requirements.
400	AOM.02001105	Invalid period.	Invalid period.	Check whether the parameter meets requirements.
400	AOM.02001106	Invalid email.	Invalid email.	Check whether the parameter meets requirements.
400	AOM.02001107	The maximum number of rules has been reached.	The maximum number of rules has been reached.	Check whether the parameter meets requirements.

Status Code	Error Code	Message	Description	Solution
400	AOM.02001108	Invalid time range.	Invalid time range.	Check whether the parameter meets requirements.
400	AOM.02001109	Threshold rule xxx does not exist.	Threshold rule xxx does not exist.	Check whether the parameter meets requirements.
400	AOM.02001110	Invalid limit.	Invalid limit.	Check whether the parameter meets requirements.
400	AOM.02001111	Invalid offset.	Invalid offset.	Check whether the parameter meets requirements.
400	AOM.02001112	Invalid request parameter.	Invalid request parameter.	Check whether the parameter meets requirements.
400	AOM.02001115	Invalid request parameter.	Invalid request parameter.	Check whether the parameter meets requirements.
400	AOM.02001118	Invalid number of consecutive periods.	Invalid number of consecutive periods.	Check whether the parameter meets requirements.
400	AOM.02001119	Invalid statistic.	Invalid statistic.	Check whether the parameter meets requirements.
400	AOM.02001120	Invalid comparison operator.	Invalid comparison operator.	Check whether the parameter meets requirements.
400	AOM.02001121	The rule does not exist.	The rule does not exist.	Check whether the parameter meets requirements.

Status Code	Error Code	Message	Description	Solution
400	AOM.02001400	Bad request.	Bad request.	Check whether the parameter meets requirements.
400	AOM.02002101	Invalid rule.	Invalid rule.	Check whether the parameter meets requirements.
400	AOM.02002102	The rule name already exists.	The rule name already exists.	Check whether the parameter meets requirements.
400	AOM.02002103	Invalid description.	Invalid description.	Check whether the parameter meets requirements.
400	AOM.02002104	Invalid threshold.	Invalid threshold.	Check whether the parameter meets requirements.
400	AOM.02002105	Invalid period.	Invalid period.	Check whether the parameter meets requirements.
400	AOM.02002106	Invalid email.	Invalid email.	Check whether the parameter meets requirements.
400	AOM.02002107	The maximum number of rules has been reached.	The maximum number of rules has been reached.	Check whether the parameter meets requirements.
400	AOM.02002108	Invalid time range.	Invalid time range.	Check whether the parameter meets requirements.
400	AOM.02002109	Invalid project ID.	Invalid project ID.	Check whether the parameter meets requirements.

Status Code	Error Code	Message	Description	Solution
400	AOM.02002110	Invalid limit.	Invalid limit.	Check whether the parameter meets requirements.
400	AOM.02002111	Invalid offset.	Invalid offset.	Check whether the parameter meets requirements.
400	AOM.02002112	Invalid request parameter.	Invalid request parameter.	Check whether the parameter meets requirements.
400	AOM.02002115	Invalid request parameter.	Invalid request parameter.	Check whether the parameter meets requirements.
400	AOM.02002118	Invalid number of consecutive periods.	Invalid number of consecutive periods.	Check whether the parameter meets requirements.
400	AOM.02002119	Invalid statistic.	Invalid statistic.	Check whether the parameter meets requirements.
400	AOM.02002120	Invalid comparison operator.	Invalid comparison operator.	Check whether the parameter meets requirements.
400	AOM.02002121	The rule does not exist.	The rule does not exist.	Check whether the parameter meets requirements.
400	AOM.02002400	Bad request.	Bad request.	Check whether the parameter meets requirements.
400	AOM.02003101	Invalid rule.	Invalid rule.	Check whether the parameter meets requirements.

Status Code	Error Code	Message	Description	Solution
400	AOM.02003102	The rule name already exists.	The rule name already exists.	Check whether the parameter meets requirements.
400	AOM.02003103	Invalid description.	Invalid description.	Check whether the parameter meets requirements.
400	AOM.02003104	Invalid threshold.	Invalid threshold.	Check whether the parameter meets requirements.
400	AOM.02003105	Invalid period.	Invalid period.	Check whether the parameter meets requirements.
400	AOM.02003106	Invalid email.	Invalid email.	Check whether the parameter meets requirements.
400	AOM.02003107	The maximum number of rules has been reached.	The maximum number of rules has been reached.	Check whether the parameter meets requirements.
400	AOM.02003108	Invalid time range.	Invalid time range.	Check whether the parameter meets requirements.
400	AOM.02003109	Invalid project ID.	Invalid project ID.	Check whether the parameter meets requirements.
400	AOM.02003110	Invalid limit.	Invalid limit.	Check whether the parameter meets requirements.
400	AOM.02003111	Invalid offset.	Invalid offset.	Check whether the parameter meets requirements.

Status Code	Error Code	Message	Description	Solution
400	AOM.02003112	Invalid request parameter.	Invalid request parameter.	Check whether the parameter meets requirements.
400	AOM.02003115	Invalid request parameter.	Invalid request parameter.	Check whether the parameter meets requirements.
400	AOM.02003118	Invalid number of consecutive periods.	Invalid number of consecutive periods.	Check whether the parameter meets requirements.
400	AOM.02003119	Invalid statistic.	Invalid statistic.	Check whether the parameter meets requirements.
400	AOM.02003120	Invalid comparison operator.	Invalid comparison operator.	Check whether the parameter meets requirements.
400	AOM.02003121	The rule does not exist.	The rule does not exist.	Check whether the parameter meets requirements.
400	AOM.02003400	Bad request.	Bad request.	Check whether the parameter meets requirements.
400	AOM.02004101	Invalid rule.	Invalid rule.	Check whether the parameter meets requirements.
400	AOM.02004102	The rule name already exists.	The rule name already exists.	Check whether the parameter meets requirements.
400	AOM.02004103	Invalid description.	Invalid description.	Check whether the parameter meets requirements.

Status Code	Error Code	Message	Description	Solution
400	AOM.02004104	Invalid threshold.	Invalid threshold.	Check whether the parameter meets requirements.
400	AOM.02004105	Invalid period.	Invalid period.	Check whether the parameter meets requirements.
400	AOM.02004106	Invalid email.	Invalid email.	Check whether the parameter meets requirements.
400	AOM.02004107	The maximum number of rules has been reached.	The maximum number of rules has been reached.	Check whether the parameter meets requirements.
400	AOM.02004108	Invalid time range.	Invalid time range.	Check whether the parameter meets requirements.
400	AOM.02004109	Invalid project ID.	Invalid project ID.	Check whether the parameter meets requirements.
400	AOM.02004110	Invalid limit.	Invalid limit.	Check whether the parameter meets requirements.
400	AOM.02004111	Invalid offset.	Invalid offset.	Check whether the parameter meets requirements.
400	AOM.02004112	Invalid request parameter.	Invalid request parameter.	Check whether the parameter meets requirements.
400	AOM.02004115	Invalid request parameter.	Invalid request parameter.	Check whether the parameter meets requirements.

Status Code	Error Code	Message	Description	Solution
400	AOM.02004118	Invalid number of consecutive periods.	Invalid number of consecutive periods.	Check whether the parameter meets requirements.
400	AOM.02004119	Invalid statistic.	Invalid statistic.	Check whether the parameter meets requirements.
400	AOM.02004120	Invalid comparison operator.	Invalid comparison operator.	Check whether the parameter meets requirements.
400	AOM.02004121	The rule does not exist.	The rule does not exist.	Check whether the parameter meets requirements.
400	AOM.02004400	Bad request.	Bad request.	Check whether the parameter meets requirements.
400	AOM.02005101	Invalid rule.	Invalid rule.	Check whether the parameter meets requirements.
400	AOM.02005102	The rule name already exists.	The rule name already exists.	Check whether the parameter meets requirements.
400	AOM.02005103	Invalid description.	Invalid description.	Check whether the parameter meets requirements.
400	AOM.02005104	Invalid threshold.	Invalid threshold.	Check whether the parameter meets requirements.
400	AOM.02005105	Invalid period.	Invalid period.	Check whether the parameter meets requirements.

Status Code	Error Code	Message	Description	Solution
400	AOM.02005106	Invalid email.	Invalid email.	Check whether the parameter meets requirements.
400	AOM.02005107	The maximum number of rules has been reached.	The maximum number of rules has been reached.	Check whether the parameter meets requirements.
400	AOM.02005108	Invalid time range.	Invalid time range.	Check whether the parameter meets requirements.
400	AOM.02005109	Invalid project ID.	Invalid project ID.	Check whether the parameter meets requirements.
400	AOM.02005110	Invalid limit.	Invalid limit.	Check whether the parameter meets requirements.
400	AOM.02005111	Invalid offset.	Invalid offset.	Check whether the parameter meets requirements.
400	AOM.02005112	Invalid request parameter.	Invalid request parameter.	Check whether the parameter meets requirements.
400	AOM.02005115	Invalid request parameter.	Invalid request parameter.	Check whether the parameter meets requirements.
400	AOM.02005118	Invalid number of consecutive periods.	Invalid number of consecutive periods.	Check whether the parameter meets requirements.
400	AOM.02005119	Invalid statistic.	Invalid statistic.	Check whether the parameter meets requirements.

Status Code	Error Code	Message	Description	Solution
400	AOM.02005120	Invalid comparison operator.	Invalid comparison operator.	Check whether the parameter meets requirements.
400	AOM.02005121	The rule does not exist.	The rule does not exist.	Check whether the parameter meets requirements.
400	AOM.02005400	Bad request.	Bad request.	Check whether the parameter meets requirements.
400	AOM.02017001	Invalid param.	Invalid parameters.	Check whether the parameter meets requirements.
400	AOM.04007101	Invalid namespace.	Invalid namespace.	Check whether the parameter meets requirements.
400	AOM.04007102	Invalid inventory ID.	Invalid inventory ID.	Check whether the parameter meets requirements.
400	AOM.04007103	The project ID cannot be left blank.	The project ID cannot be left blank.	Check whether the parameter meets requirements.
400	AOM.04007104	Invalid type.	Invalid type.	Check whether the parameter meets requirements.
400	AOM.04007105	Invalid limit.	Invalid limit.	Check whether the parameter meets requirements.
400	AOM.04007106	Invalid offset.	Invalid offset.	Check whether the parameter meets requirements.

Status Code	Error Code	Message	Description	Solution
400	AOM.04007107	Invalid parent inventory ID.	Invalid parent inventory ID.	Check whether the parameter meets requirements.
400	AOM.04007108	Invalid type and relation.	Invalid type and relation.	Check whether the parameter meets requirements.
400	AOM.04007109	Invalid metric name.	Invalid metric name.	Check whether the parameter meets requirements.
400	AOM.04007110	Invalid relation.	Invalid relation.	Check whether the parameter meets requirements.
400	AOM.04007111	The type and relation cannot be left blank.	The type and relation cannot be left blank.	Check whether the parameter meets requirements.
400	AOM.04007112	Invalid request parameter.	Invalid request parameter.	Check whether the parameter meets requirements.
400	AOM.04007115	Invalid request parameter.	Invalid request parameter.	Check whether the parameter meets requirements.
400	AOM.04007118	Invalid number of consecutive periods.	Invalid number of consecutive periods.	Check whether the parameter meets requirements.
400	AOM.04007119	Invalid statistic.	Invalid statistic.	Check whether the parameter meets requirements.
400	AOM.04007120	Invalid comparison operator.	Invalid comparison operator.	Check whether the parameter meets requirements.

Status Code	Error Code	Message	Description	Solution
400	AOM.04007400	Bad request.	Bad request.	Check whether the parameter meets requirements.
400	AOM.04008101	Invalid namespace.	Invalid namespace.	Check whether the parameter meets requirements.
400	AOM.04008102	Invalid inventory ID.	Invalid inventory ID.	Check whether the parameter meets requirements.
400	AOM.04008103	The project ID cannot be left blank.	The project ID cannot be left blank.	Check whether the parameter meets requirements.
400	AOM.04008104	Invalid type.	Invalid type.	Check whether the parameter meets requirements.
400	AOM.04008105	Invalid limit.	Invalid limit.	Check whether the parameter meets requirements.
400	AOM.04008106	Invalid offset.	Invalid offset.	Check whether the parameter meets requirements.
400	AOM.04008107	Invalid parent inventory ID.	Invalid parent inventory ID.	Check whether the parameter meets requirements.
400	AOM.04008108	Invalid type and relation.	Invalid type and relation.	Check whether the parameter meets requirements.
400	AOM.04008109	Invalid metric name.	Invalid metric name.	Check whether the parameter meets requirements.

Status Code	Error Code	Message	Description	Solution
400	AOM.04008110	Invalid relation.	Invalid relation.	Check whether the parameter meets requirements.
400	AOM.04008111	The type and relation cannot be left blank.	The type and relation cannot be left blank.	Check whether the parameter meets requirements.
400	AOM.04008112	Invalid request parameter.	Invalid request parameter.	Check whether the parameter meets requirements.
400	AOM.04008115	Invalid request parameter.	Invalid request parameter.	Check whether the parameter meets requirements.
400	AOM.04008118	Invalid number of consecutive periods.	Invalid number of consecutive periods.	Check whether the parameter meets requirements.
400	AOM.04008119	Invalid statistic.	Invalid statistic.	Check whether the parameter meets requirements.
400	AOM.04008120	Invalid comparison operator.	Invalid comparison operator.	Check whether the parameter meets requirements.
400	AOM.04008400	Bad request.	Bad request.	Check whether the parameter meets requirements.
400	AOM.07001400	Invalid parameter.	Invalid parameter.	Check whether the parameter meets requirements.
400	AOM.11015003	The request body is empty.	The request body is empty.	Check whether the parameter meets requirements.

Status Code	Error Code	Message	Description	Solution
400	AOM.11015004	Parse request parameter failed.	Parse request parameter failed.	Check whether the parameter meets requirements.
400	AOM.11015005	Too many Prometheus instances.	Too many Prometheus instances.	Check whether the parameter meets requirements.
400	AOM.11017013	The Prometheus instance ID is empty.	The Prometheus instance ID is empty.	Check whether the parameter meets requirements.
400	AOM.11017014	Prometheus instance not found.	Prometheus instance not found.	Check whether the parameter meets requirements.
400	AOM.11017015	Invalid Prometheus instance name	Invalid Prometheus instance name.	Check whether the parameter meets requirements.
400	AOM.11017016	Invalid Prometheus instance ID.	Invalid Prometheus instance ID.	Check whether the parameter meets requirements.
400	AOM.11017017	Invalid Prometheus instance type.	Invalid Prometheus instance type.	Check whether the parameter meets requirements.
400	AOM.11017018	Invalid Prometheus instance status.	Invalid Prometheus instance status.	Check whether the parameter meets requirements.
400	AOM.11017019	Invalid application name.	Invalid application name.	Check whether the parameter meets requirements.
400	AOM.4001021	Group name repeate.	Duplicate group name.	Check whether the parameter meets requirements.

Status Code	Error Code	Message	Description	Solution
400	AOM.4001023	Group name must be set.	The group name cannot be empty.	Check whether the parameter meets requirements.
400	AOM.4001024	The recording field cannot be empty.	The recording field cannot be empty.	Check whether the parameter meets requirements.
400	AOM.4001025	The expression cannot be empty.	The expression cannot be empty.	Check whether the parameter meets requirements.
400	AOM.4001026	Recording rule format invalid.	Invalid recording rule format.	Check whether the parameter meets requirements.
400	AOM.4001028	The requested content exceeds the maximum.	The request is too long.	Check whether the parameter meets requirements.
400	AOM.05001002	The dashboard type is empty.	The dashboard type is empty.	Check whether the parameter meets requirements.
400	SVCSTG.INV.4000115	Invalid request parameter.	Invalid request parameter.	Check whether the parameter meets requirements.
400	SVCSTG_AMS_4000001	Invalid request parameter.	Invalid request parameter.	Check whether the parameter meets requirements.
400	SVCSTG_AMS_4000002	Invalid namespace.	Invalid namespace.	Check whether the parameter meets requirements.
400	SVCSTG_AMS_4000003	Dimensions cannot be left blank.	Dimensions cannot be left blank.	Check whether the parameter meets requirements.

Status Code	Error Code	Message	Description	Solution
400	SVCSTG_AMS_4000005	Invalid metric data type.	Invalid metric data type.	Check whether the parameter meets requirements.
400	SVCSTG_AMS_4000006	The metric data value cannot be left blank.	The metric data cannot be left blank.	Check whether the parameter meets requirements.
400	SVCSTG_AMS_4000007	Invalid dimension.	Invalid dimension.	Check whether the parameter meets requirements.
400	SVCSTG_AMS_4000008	The request exceeds 40 KB.	The request cannot exceed 40 KB.	Check whether the parameter meets requirements.
400	SVCSTG_AMS_4000009	The number of elements in the dimension array exceeds the allowed limit.	Too many elements in the dimension array.	Check whether the parameter meets requirements.
400	SVCSTG_AMS_4000010	Invalid collection time.	Invalid collection time.	Check whether the parameter meets requirements.
400	SVCSTG_AMS_4000101	The namespace or alarm name is invalid, or the project ID is left blank.	The namespace or alarm name is invalid, or the project ID is left blank.	Check whether the parameter meets requirements.
400	SVCSTG_AMS_4000102	The inventory ID is invalid, the metric data value is left blank, or the threshold rule name already exists.	The inventory ID is invalid, the metric data value is left blank, or the threshold rule name already exists.	Check whether the parameter meets requirements, or change the rule name and try again.
400	SVCSTG_AMS_4000103	Invalid range or alarm description.	Invalid range or alarm description.	Check whether the parameter meets requirements.

Status Code	Error Code	Message	Description	Solution
400	SVCSTG_AMS_4000104	Invalid statistics or alarm threshold.	Invalid statistics or alarm threshold.	Check whether the parameter meets requirements.
400	SVCSTG_AMS_4000105	Invalid limit, metric, or alarm period.	Invalid limit, metric, or alarm period.	Check whether the parameter meets requirements.
400	SVCSTG_AMS_4000106	Invalid offset, time range, or email.	Invalid offset, time range, or email.	Check whether the parameter meets requirements.
400	SVCSTG_AMS_4000107	The number of data points in a time range exceeds 1440 or the maximum number of threshold rules has been reached.	The number of data points in a time range exceeds 1440 or the maximum number of threshold rules has been reached.	Check whether the parameter meets the requirements or contact technical support.
400	SVCSTG_AMS_4000108	Invalid time range.	Invalid time range.	Check whether the parameter meets requirements.
400	SVCSTG_AMS_4000109	Invalid metric name or project ID.	Invalid metric name or project ID.	Check whether the parameter meets requirements.
400	SVCSTG_AMS_4000110	Invalid filled value or limit.	Invalid filled value or limit.	Check whether the parameter meets requirements.
400	SVCSTG_AMS_4000111	Invalid offset.	Invalid offset.	Check whether the parameter meets requirements.
400	SVCSTG_AMS_4000115	Invalid request parameter.	Invalid request parameter.	Check whether the parameter meets requirements.

Status Code	Error Code	Message	Description	Solution
400	SVCSTG_AMS_4000118	Invalid number of consecutive periods.	Invalid number of consecutive periods.	Check whether the parameter meets requirements.
400	SVCSTG_AMS_4000119	Invalid statistic.	Invalid statistic.	Check whether the parameter meets requirements.
400	SVCSTG_AMS_4000120	Invalid comparison operator.	Invalid comparison operator.	Check whether the parameter meets requirements.
400	SVCSTG_AMS_4000121	The rule does not exist.	The rule does not exist.	Check whether the threshold rule exists.
400	SVCSTG_AMS_4001019	Send MetricData check param invalid	Invalid MetricData parameter.	Check whether the parameter meets requirements.
400	AOM.02006404	The rule to be deleted does not exist.	The rule does not exist.	Check whether the threshold rule exists.
400	AOM.02005404	The rule does not exist.	The rule does not exist.	Check whether the threshold rule exists.
400	AOM.02004404	The rule does not exist.	The rule does not exist.	Check whether the threshold rule exists.
400	AOM.02004001	Incorrect request parameter.	Incorrect request parameter.	Check whether the parameter meets requirements.
400	AOM.02005001	Incorrect request parameter.	Incorrect request parameter.	Check whether the parameter meets requirements.
400	AOM.02003001	Incorrect request parameter.	Incorrect request parameter.	Check whether the parameter meets requirements.

Status Code	Error Code	Message	Description	Solution
400	AOM.02021006	This rule actionId is invalid.	The action rule does not exist.	Check whether the parameter meets requirements.
400	AOM.02011400	Incorrect request parameter.	Incorrect request parameter.	Check whether the parameter meets requirements.
400	AOM.02013125	send kafka message failed	Failed to send data to Kafka.	Contact technical support.
400	AOM.02024016	Delete alarm rule name is empty.	The alarm rule is empty.	Check whether the parameter meets requirements.
400	AOM.08015002	The muteName is not exist	The silence rule name does not exist.	Check whether the parameter meets requirements.
400	AOM.08011001	The muteName is exist	The silence rule name already exists.	Check whether the parameter meets requirements.
400	AOM.08012003	Invalid request parameter.	Incorrect request body parameter.	Check whether the parameter meets requirements.
400	AOM.08018012	ActionRule already exists	The alarm action rule already exists.	Check whether the parameter meets requirements.
400	AOM.08020006	The action rule does not exist	The alarm action rule does not exist.	Check whether the parameter meets requirements.
400	AOM.08019006	The action rule does not exist	The alarm action rule does not exist.	Check whether the parameter meets requirements.

Status Code	Error Code	Message	Description	Solution
400	AOM.08032002	The request body is illegal	Invalid request body.	Check whether the parameter meets requirements.
400	AOM.08033002	The request body is illegal	Invalid request body.	Check whether the parameter meets requirements.
400	AOM.02001SVCSTG_AMS_4000115	Invalid request parameter.	Incorrect request parameter.	Check whether the parameter meets requirements.
400	AOM.02003SVCSTG_AMS_4000123	The rule does not exist	The rule does not exist.	Check whether the parameter meets requirements.
400	AOM.02001102	This Threshold rule name has been existed	The threshold rule already exists.	Check whether the parameter meets requirements.
401	AOM.0401	Unauthorized.	Incorrect authentication information.	Check the authentication information carried in the request.
401	AOM.02001401	Unauthorized.	Unauthorized.	Contact technical support.
401	AOM.02002401	Unauthorized.	Unauthorized.	Contact technical support.
401	AOM.02003401	Unauthorized.	Unauthorized.	Contact technical support.
401	AOM.02004401	Unauthorized.	Unauthorized.	Contact technical support.
401	AOM.02005401	Unauthorized.	Unauthorized.	Contact technical support.
401	AOM.04007401	Request unauthorized.	Request unauthorized.	Contact technical support.
401	AOM.04008401	Request unauthorized.	Request unauthorized.	Contact technical support.

Status Code	Error Code	Message	Description	Solution
401	AOM.05401000	auth failed	Authentication failed.	Check the authentication information carried in the request.
401	SVCSTG.AMS.2000051	auth failed	Authentication failed.	Check the authentication information carried in the request.
401	SVCSTG.AMS.4010000	auth failed	Authentication failed.	Check the authentication information carried in the request.
403	AOM.0403	Forbidden.	Insufficient permissions.	Check your permissions.
403	AOM.02001403	Forbidden.	Forbidden.	Contact technical support.
403	AOM.02002403	Forbidden.	Forbidden.	Contact technical support.
403	AOM.02003403	Forbidden.	Forbidden.	Contact technical support.
403	AOM.02004403	Forbidden.	Forbidden.	Contact technical support.
403	AOM.02005403	Forbidden.	Forbidden.	Contact technical support.
403	AOM.04007403	Request forbidden.	Request forbidden.	Contact technical support.
403	AOM.04008403	Request forbidden.	Request forbidden.	Contact technical support.
403	AOM.07001403	Insufficient permissions.	Insufficient permissions.	Obtain required permissions.
403	SVCSTG.INV.4030000	Insufficient permissions.	Insufficient permissions.	Use an authorized account.
404	SVCSTG.INV.4040000	Inventory does not exists.	The resource does not exist.	Check whether the resource exists.

Status Code	Error Code	Message	Description	Solution
429	AOM.07001429	The traffic has been restricted.	The traffic has been restricted.	Send fewer API call requests.
429	AOM.08001429	Too many requests.	Too many requests.	Check whether the parameter meets requirements.
500	AOM.0500	Internal server error.	Internal server error.	Contact technical support.
500	AOM.12000002	Internal server error.	Internal server error.	Contact technical support.
500	AOM.02001500	Internal server error.	Internal server error.	Contact technical support.
500	AOM.02001501	The Cassandra session is null.	The Cassandra session is null.	Contact technical support.
500	AOM.02001502	The Cassandra execution is abnormal.	The Cassandra execution is abnormal.	Contact technical support.
500	AOM.02002500	Internal server error.	Internal server error.	Contact technical support.
500	AOM.02002501	The Cassandra session is null.	The Cassandra session is null.	Contact technical support.
500	AOM.02002502	The Cassandra execution is abnormal.	The Cassandra execution is abnormal.	Contact technical support.
500	AOM.02003500	Internal server error.	Internal server error.	Contact technical support.
500	AOM.02003501	The Cassandra session is null.	The Cassandra session is null.	Contact technical support.
500	AOM.02003502	The Cassandra execution is abnormal.	The Cassandra execution is abnormal.	Contact technical support.
500	AOM.02004500	Internal server error.	Internal server error.	Contact technical support.

Status Code	Error Code	Message	Description	Solution
500	AOM.02004501	The Cassandra session is null.	The Cassandra session is null.	Contact technical support.
500	AOM.02004502	The Cassandra execution is abnormal.	The Cassandra execution is abnormal.	Contact technical support.
500	AOM.02005500	Internal server error.	Internal server error.	Contact technical support.
500	AOM.02005501	The Cassandra session is null.	The Cassandra session is null.	Contact technical support.
500	AOM.02005502	The Cassandra execution is abnormal.	The Cassandra execution is abnormal.	Contact technical support.
500	AOM.02021500	Internal server error.	Internal server error.	Contact technical support.
500	AOM.02022500	Internal server error.	Internal server error.	Contact technical support.
500	AOM.02024500	Internal server error.	Internal server error.	Contact technical support.
500	AOM.04007500	Internal server error.	Internal server error.	Contact technical support.
500	AOM.04007501	The Cassandra session is null.	The Cassandra session is null.	Contact technical support.
500	AOM.04007502	The Cassandra execution is abnormal.	The Cassandra execution is abnormal.	Contact technical support.
500	AOM.04008500	Internal server error.	Internal server error.	Contact technical support.
500	AOM.04008501	The Cassandra session is null.	The Cassandra session is null.	Contact technical support.
500	AOM.04008502	The Cassandra execution is abnormal.	The Cassandra execution is abnormal.	Contact technical support.

Status Code	Error Code	Message	Description	Solution
500	AOM.11014001	Internal server error.	Internal server error.	Contact technical support.
500	AOM.11014002	Incorrect conversion result.	Incorrect conversion result.	Contact technical support.
500	AOM.05001005	Internal server error.	Internal server error.	Contact technical support.
500	AOM.5001010	Internal server error.	Internal server error.	Contact technical support.
500	AOM.5001019	Recording rule exist for the prometheus instance.	The rule already exists.	Contact technical support.
500	APM.00000500	Internal Server Error	Internal server error.	Contact technical support.
500	AOM.08001500	Internal Server Error	Internal server error.	Contact technical support.
500	AOM.08020500	Internal server error.	Internal server error.	Contact technical support.
500	AOM.02001500	Internal server error.	Internal server error.	Contact technical support.
500	SVCSTG.INV.5000001	The Elasticsearch session is null.	The Elasticsearch session is null.	Contact technical support.
500	SVCSTG.INV.5000002	The Elasticsearch execution is abnormal.	The Elasticsearch execution is abnormal.	Contact technical support.
500	SVCSTG.INV.5000003	The ICMGR invocation is abnormal.	The ICMGR invocation is abnormal.	Contact technical support.
500	SVCSTG.INV.5000006	The rule name already exists.	The rule name already exists.	Use another name.
500	SVCSTG.INV.5000007	The maximum number of rules has been reached.	The maximum number of rules has been reached.	Delete unnecessary rules and add new ones.

Status Code	Error Code	Message	Description	Solution
500	SVCSTG_AMS_5000000	Internal server error.	Internal server error.	Contact technical support.
503	AOM.0503	Server unavailable.	Server unavailable.	Contact technical support.
503	AOM.02001503	Server unavailable.	Server unavailable.	Contact technical support.
503	AOM.02002503	Server unavailable.	Server unavailable.	Contact technical support.
503	AOM.02003503	Server unavailable.	Server unavailable.	Contact technical support.
503	AOM.02004503	Server unavailable.	Server unavailable.	Contact technical support.
503	AOM.02005503	Server unavailable.	Server unavailable.	Contact technical support.
503	AOM.04007503	Server unavailable.	Server unavailable.	Contact technical support.
503	AOM.04008503	Server unavailable.	Server unavailable.	Contact technical support.
503	AOM.07001503	Service error.	Service error.	Check whether the backend service is normal.
503	SVCSTG_AMS_5030001	The Cassandra session is null.	The Cassandra session is null.	Contact technical support.
503	SVCSTG_AMS_5030002	The Cassandra execution is abnormal.	The Cassandra execution is abnormal.	Contact technical support.

8.3 Obtaining an Account ID and Project ID

When making API calls, you may need to enter the username, user ID, project name, and project ID in some URIs. You can obtain them on the **My Credentials** page.

Step 1 Log in to the management console.

Step 2 Hover over the username in the upper right corner, and choose **My Credentials**.

Step 3 On the **API Credentials** page, view the username, account ID, project name, and project ID.

----End

Obtaining a Project ID by Calling an API

You can also call the API for **querying project information based on the specified criteria** to obtain a project ID.

The API is **GET https://*{Endpoint}*/v3/projects/**, where *{Endpoint}* indicates the Identity and Access Management (IAM) endpoint. For details, see **Regions and Endpoints**. For details about API authentication, see **3.2 Authentication**.

In the following example, **id** indicates the project ID.

```
{
    "projects": [
        {
            "domain_id": "65382450e8f64ac0870cd180d14e684b",
            "is_domain": false,
            "parent_id": "65382450e8f64ac0870cd180d14e684b",
            "name": "cn-north-4",
            "description": "",
            "links": {
                "next": null,
                "previous": null,
                "self": "https://www.example.com/v3/projects/a4a5d4098fb4474fa22cd05f897d6b99"
            },
            "id": "a4a5d4098fb4474fa22cd05f897d6b99",
            "enabled": true
        }
    ],
    "links": {
        "next": null,
        "previous": null,
        "self": "https://www.example.com/v3/projects"
    }
}
```

8.4 Common Request Headers

Table 8-2 Common request headers

Name	Description	Mandatory	Example
X-Auth-Token	User token.	Yes for token-based authentication	-
Content-Type	Content type. Enter **application/json;charset=utf-8**.	Yes	application/json;charset=utf8

Name	Description	Mandatory	Example
x-sdk-date	Time to send a request. The format is *YYYYMMDD'T'HHMMSS'Z'*. GMT time is used.	Yes for AK/SK-based authentication	20160629T101459Z
Authorization	Signature authentication information. It can be obtained from the result of request signing.	Yes for AK/SK-based authentication	-
Host	Request server information, which is obtained from the URL of a service API. The value is **hostname[:port]**. If no port is specified, the default port will be used. For HTTPS, port 443 is used by default.	Yes for AK/SK-based authentication	-

8.5 Common Response Headers

A response usually contains the following headers:

Table 8-3 Response headers

Name	Description	Example
Date	(Standard HTTP header) Time when a message is sent. This field complies with RFC822 definitions.	Mon, 12 Nov 2007 15:55:01 GMT
Server	(Standard HTTP header) Software that a server uses to process the request.	Apache

Name	Description	Example
Content-Length	(Standard HTTP header) Length of the response body, which is represented by a decimal number and stored in bytes.	xxx
Content-Type	(Standard HTTP header) Media type of the response body sent to the recipient.	application/json

