Application Operations Management

API Reference

Issue 01

Date 2024-04-15

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 *Application Operations Management API Reference*. AOM is a one-stop and multi-dimensional O&M management platform for cloud applications. It monitors your applications and related cloud resources in real time, collects and associates the data of resource metrics, logs, and events to analyze application health status, and provides flexible alarms and abundant data visualization. With AOM, you can detect faults in a timely manner and master the running status of applications, resources, and services in real time.

This document describes how to use application programming interfaces (APIs) to perform operations on AOM, such as creation, deletion, and query. For details about all supported operations, see **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 **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, .

1.4 Concepts

- **Region**

  Regions are geographic areas isolated from each other. Resources are region-specific and cannot be used across regions through internal network connections. For low network latency and quick resource access, select the nearest region.

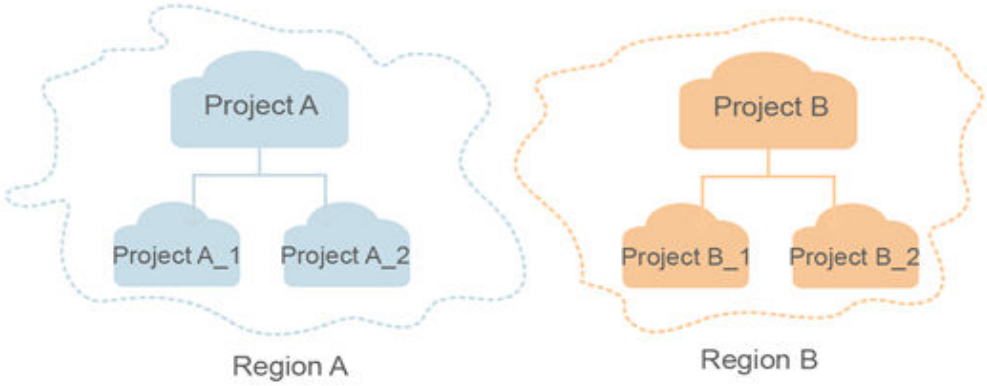
- **AZ**

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

- **Project**

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

  Figure 1-1 Project isolation model



2 API Overview

AOM provides open monitoring, auto scaling, and log APIs, helping you implement application O&M with low costs.

Table 2-1 API overview

Type	Description
Monitoring APIs (v1)	Monitoring APIs, including the APIs that query metrics; query and add monitoring data; add, modify, query, and delete threshold rules; add, modify, query, and delete application discovery rules.
Monitoring APIs (v2)	Monitoring APIs, including the APIs that query time series objects and time series data, and add, modify, query, and delete threshold rules. **NOTE** You are advised to use v2 APIs, which are newly opened. The v1 APIs are not recommended for new users and will be taken offline later.
Auto Scaling APIs	Auto scaling APIs, including the APIs that create, delete, and update policies; query one or all policies; update and query policy group attributes.
Log APIs	Log APIs, including the API that query logs.
Event and Alarm APIs	API that reports events and alarms.
Agent APIs	API that query Agent information.
Application Discovery Rule APIs	Application discovery rule APIs, including the APIs that add, modify, query, and delete application discovery rules.
Prometheus Monitoring APIs	Prometheus monitoring APIs, including the APIs for querying data in a specified period, data at a specified time point, tag values, tag names, and metadata.

Monitoring APIs (v1)

API	Description
Querying metrics	Query the metrics that can be monitored in the system. You can specify the namespace, metric name, dimension, resource ID (format: **resType_resId**), start position, and maximum number of returned records in pagination queries.
Querying monitoring data	Query monitoring data of metrics within a specified period. You can specify a dimension or period to query.
Adding monitoring data	Add one or more monitoring data records.
Adding a threshold rule	Add a threshold rule.
Modifying a threshold rule	Modify a threshold rule.
Querying the threshold rule list	Query all threshold rules.
Querying a threshold rule	Query a threshold rule.
Deleting a threshold rule	Delete a threshold rule.
Adding or modifying one or more application discovery rules	Add or modify one or more application discovery rules.
Deleting one or more application discovery rules	Delete one or more application discovery rules.
Querying an application discovery rule	Query an application discovery rule.

Monitoring APIs (v2)

API	Description
Querying the time series list	Query the time series list that can be monitored in the system. You can specify the time series namespace, name, dimension, and resource ID (format: resType_resId).

API	Description
Querying time series data	Query time series data in a specified period. You can specify a dimension or period to query.
Adding a threshold rule	Add a threshold rule.
Querying the threshold rule list	Query all threshold rules.
Modifying a threshold rule	Modify a threshold rule.
Deleting a threshold rule	Delete a threshold rule.
Querying a threshold rule	Query a threshold rule.
Deleting threshold rules in batches	Delete threshold rules in batches.

Auto Scaling APIs

API	Description
Creating a policy	Create a policy.
Querying the policy list	Query the details about all policies of a specified project.
Deleting a policy	Delete a specified policy.
Modifying a policy	Modify a policy.
Querying a policy	Query the details about a policy of a specified project.
Modifying policy group attributes	Modify policy group attributes.
Querying policy group attributes	Query policy group attributes.

Log APIs

API	Description
Querying logs	Query logs by different dimensions, such as the cluster, IP address, or application.

Event and Alarm APIs

API	Description
Querying events and alarms	Query events and alarms.
Counting events and alarms	Count events and alarms based on specified conditions.
Reporting events and alarms	Report events and alarms.

Agent APIs

API	Description
Querying Agent information	Query the Agent information about an account, a cluster, or a namespace.

Application Discovery Rule APIs

API	Description
Adding or modifying one or more application discovery rules	Add or modify one or more application discovery rules.
Deleting one or more application discovery rules	Delete one or more application discovery rules.
Querying an application discovery rule	Query an application discovery rule.

Prometheus Monitoring APIs

API	Description
Querying the expression calculation result in a specified period	Query the calculation result of a PromQL expression in a specified period.

API	Description
Querying the expression calculation result at a specified time point	Query the calculation result of a PromQL expression at a specified time point.
Querying the values of a tag	Query the values of a specified tag.
Obtaining the tag name list	Obtain the tag name list.
Querying metadata	Query the metadata of time series and corresponding tags.
Querying the calculation results of a PromQL expression in a specified period based on the Prometheus instance	Query the calculation result of a PromQL expression in a specified period based on the Prometheus instance.
Querying the calculation result of a PromQL expression at a specified time point based on the Prometheus instance	Query the calculation result of a PromQL expression at a specified time point based on the Prometheus instance.
Querying the values of a tag based on the Prometheus instance	Query the values of a specified tag based on the Prometheus instance.
Obtaining the tag name list based on the Prometheus instance	Obtain the tag name list based on the Prometheus instance.
Querying metadata based on the Prometheus instance	Query the metadata of time series and corresponding tags based on the Prometheus instance.

3 Calling APIs

3.1 Making an API Request

This section describes the structure of a Representational State Transfer (REST) API request, and uses the Identity and Access Management (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:

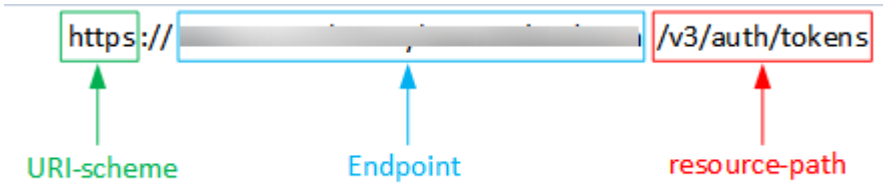
{URI-scheme} :// {Endpoint} / {resource-path} ? {query-string}

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 where the REST service is deployed. The endpoint varies depending on services and regions.
- **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 the 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**: same as GET except that the server must return only the response header.
- **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, 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 **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.
- Access Key ID/Secret Access Key (AK/SK)-based authentication: Requests are authenticated by encrypting the request body using an AK/SK.

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 **Making an API Request**, the process of calling the API used to obtain a user token is described. After a token is obtained, the **X-Auth-Token** header field must be added to requests to specify the token when other APIs are called. 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.

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 **Status Codes**.

For example, if status code **201** is returned for calling the API used to obtain a user token, the request is successful.

Response Header

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

Figure 3-2 shows the response header fields 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. The following shows part of the response body for the API to obtain a user token.

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

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 Monitoring (v1)

4.1.1 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.

URI

POST /v1/{project_id}/ams/metrics

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.

Table 4-2 Query Parameters

Parameter	Mandatory	Type	Description
type	No	String	Metric query mode.
limit	No	String	Number of records that can be returned. Value range: 1–1000. Default value: 1000.

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

Request Parameters

Table 4-3 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**
X-Aom-Prometheus-Id	No	String	Prometheus instance ID. If this parameter is left blank, the default Prometheus instance is used.

Table 4-4 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 type (a URI parameter) is not inventory, the information carried by the array is used to query metrics.

Table 4-5 QueryMetricItemOptionParam

Parameter	Mandatory	Type	Description
dimensions	No	Array of **Dimension** objects	List of metric dimensions.
metricName	No	String	Metric name. Length: 1 to 1000 characters. Values: cpuUage: CPU usage. cpuCoreUsed: used CPU cores. Reported 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. • CUSTOM.Prometheus: namespace of Prometheus metrics. • Namespace of custom metrics. Enumeration values: • **PAAS.CONTAINER** • **PAAS.NODE** • **PAAS.SLA** • **PAAS.AGGR** • **CUSTOMMETRICS**

Table 4-6 Dimension

Parameter	Mandatory	Type	Description
name	Yes	String	Dimension name. It cannot be empty. Enter up to 255 characters.
value	No	String	Dimension value. Enter up to 1024 characters.

Response Parameters

Status code: 200

Table 4-7 Response body parameters

Parameter	Type	Description
errorCode	String	Response code.
errorMessage	String	Response message.
metrics	Array of **MetricItemResultAPI** objects	Metric list.
metaData	**MetaData** object	Metadata, including pagination information.

Table 4-8 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 4-9 Dimension

Parameter	Type	Description
name	String	Dimension name. It cannot be empty. Enter up to 255 characters.
value	String	Dimension value. Enter up to 1024 characters.

Table 4-10 MetaData

Parameter	Type	Description
count	Integer	Number of records that can be returned.

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

Example Requests

- Query metrics by inventory ID.

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

{
  "inventoryId" : "application_************7-b56f-fa163e3fee10"
}
```

- Query metrics by namespace, appName, and clusterName.

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

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

Example Responses

Status code: 200

OK

The request is successful.

```
{
  "errorCode" : "SVCSTG_AMS_2000000",
  "errorMessage" : "success",
  "metaData" : {
    "count" : 1,
    "start" : null,
    "total" : 1
  },
  "metrics" : [ {
    "namespace" : "abc",
    "metricName" : "cpuUsage",
    "unit" : "Percent",
    "dimensions" : [ {
      "name" : "instance_id",
      "value" : "demo1"
    } ]
  } ]
}
```


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 authorization information is incorrect or invalid.
403	ForbiddenThe 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**.

4.1.2 Querying Monitoring Data

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.

URI

POST /v1/{project_id}/ams/metricdata

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.

Table 4-12 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. Enumeration values: • **-1** • **0** • **null** • **average**

Request Parameters

Table 4-13 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**
X-Aom-Prometheus-Id	No	String	Prometheus instance ID. If this parameter is left blank, the default Prometheus instance is used.

Table 4-14 Request body parameters

Parameter	Mandatory	Type	Description
metrics	Yes	Array of **MetricQuery MeritcParam** objects	Metric list. Values: A JSON array can contain up to 20 objects.
period	Yes	Integer	Granularity for monitoring data. Enumerated value. Values: • 60: 1 minute. • 300: 5 minutes. • 900: 15 minutes. • 3600: 1 hour. Enumeration values: • **60** • **300** • **900** • **3600**
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. For example, 1650852000000.-1.5 is equivalent to 1650852000000.1650852300000.5.

Parameter	Mandatory	Type	Description
			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 4-15 MetricQueryMeritcParam

Parameter	Mandatory	Type	Description
dimensions	Yes	Array of **Dimension** objects	List of metric dimensions. Note: 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. Values: cpuUage: 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. • CUSTOM.Prometheus: namespace of Prometheus metrics. • Namespace of custom metrics.

Table 4-16 Dimension

Parameter	Mandatory	Type	Description
name	Yes	String	Dimension name. It cannot be empty. Enter up to 255 characters.
value	No	String	Dimension value. Enter up to 1024 characters.

Response Parameters

Status code: 200

Table 4-17 Response body parameters

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

Table 4-18 MetricDataValue

Parameter	Type	Description
dataPoints	Array of **MetricDataPoints** objects	Key metric.
metric	**MetricQueryMeritcParam** object	Query parameters.

Table 4-19 MetricDataPoints

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

Table 4-20 StatisticValue

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

Table 4-21 MetricQueryMeritcParam

Parameter	Type	Description
dimensions	Array of **Dimension** objects	List of metric dimensions. Note: 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. Values: cpuUage: CPU usage. cpuCoreUsed: used CPU cores. Custom metrics.

Parameter	Type	Description
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. • CUSTOM.Prometheus: namespace of Prometheus metrics. • Namespace of custom metrics.

Table 4-22 Dimension

Parameter	Type	Description
name	String	Dimension name. It cannot be empty. Enter up to 255 characters.
value	String	Dimension value. Enter up to 1024 characters.

Example Requests

Query the monitoring data of a specified metric in the last five minutes.

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

{
  "metrics" : [ {
    "dimensions" : [ {
      "name" : "instance_id",
      "value" : "demo1"
    } ],
    "metricName" : "def",
    "namespace" : "abc"
  } ],
  "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" : "abc",
   "metricName" : "def",
   "dimensions" : [ {
    "name" : "ghi",
    "value" : "lmn"
   } ]
  },
  "dataPoints" : [ {
   "timestamp" : "1467892800000",
   "unit" : "Percent",
   "statistics" : [ {
    "statistic" : "maximum",
    "value" : "23"
   } ]
  } ]
 } ]
}
```

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 authorization information is incorrect or invalid.
403	ForbiddenThe 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**.

4.1.3 Adding Monitoring Data

Function

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

URI

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

Table 4-23 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 4-24 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**
X-Aom-Prometheus-Id	No	String	Prometheus instance ID. If this parameter is left blank, the default Prometheus instance is used.

Table 4-25 Request body parameters

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

Table 4-26 MetricDataItem

Parameter	Mandatory	Type	Description
collect_time	Yes	Long	Data collection time, which ranges from the last 24 hours to the next 0.5 hour. The following requirement must 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. Value range: UNIX timestamp, in ms.
metric	Yes	**RecieveMetricParam** object	Metric details.
values	Yes	Array of **RecieveMetricValues** objects	Metric value.

Table 4-27 RecieveMetricParam

Parameter	Mandatory	Type	Description
dimensions	Yes	Array of **Dimension** 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.

Parameter	Mandatory	Type	Description
namespace	Yes	String	Metric namespace.The namespace cannot contain any colon (:).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.

Table 4-28 Dimension

Parameter	Mandatory	Type	Description
name	Yes	String	Dimension name. It cannot be empty. Enter up to 255 characters.
value	No	String	Dimension value. Enter up to 1024 characters.

Table 4-29 RecieveMetricValues

Parameter	Mandatory	Type	Description
metric_name	Yes	String	Metric name. Length: 1 to 255 characters.
type	No	String	Data type. Value: int or float. Enumeration values: • **int** • **float**
unit	No	String	Data unit. Length: up to 32 characters.
value	Yes	Object	Metric value. Values: valid numeral type and NaN.

Response Parameters

Status code: 200

Table 4-30 Response body parameters

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

Example Requests

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

```
POST 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

The request is successful.

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

Status Codes

Status Code	Description
200	The request is successful.
400	The request is invalid.
401	Invalid authentication information.
403	The server has received the request and understood it, but refuse to respond to it.
500	The server is able to receive the request, but the request is improper.

Status Code	Description
503	The service is unavailable.

Error Codes

See **Error Codes**.

4.1.4 Adding a Threshold Rule

Function

This API is used to add a threshold rule.

URI

POST /v1/{project_id}/ams/alarms

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.

Request Parameters

Table 4-32 Request header parameters

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

Table 4-33 Request body parameters

Parameter	Mandatory	Type	Description
statistic	Yes	String	Statistic. Enumeration values: • **maximum** • **minimum** • **average** • **sum** • **sampleCount**
namespace	No	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. • CUSTOM.Prometheus: namespace of Prometheus metrics. • Namespace of custom metrics.
metricName	Yes	String	Metric name. The value must contain 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.
period	Yes	Integer	Statistical period. Values: 60,000, 300,000, 900,000, and 3,600,000.
alarmLevel	No	Integer	Alarm severity.
evaluationPeriods	Yes	Integer	Number of consecutive periods.

Parameter	Mandatory	Type	Description
comparisonOperator	Yes	String	Threshold criterion expression. It cannot be empty. Options: >, <, >=, and <= Enumeration values: • >= • <= • >= • <=
threshold	Yes	String	Threshold value. Enter up to 255 characters. It cannot be less than 0, or positive or negative infinity.
alarmName	Yes	String	Threshold name. It cannot be empty. Enter up to 255 characters. The following special characters are not allowed: "#%&'+;<=>?\
dimensions	Yes	Array of **Dimension** objects	Metric dimension. The total dimension length (that is, total JSON characters of the array) cannot exceed 65,535. The array cannot contain more than 100 elements.
unit	Yes	String	Metric unit. It cannot be empty. Enter up to 32 characters.
actionEnabled	No	Boolean	Whether to enable alarm reporting.
alarmActions	No	Array of strings	Action to be taken when an alarm is reported. The array can contain up to five elements. It must start with **SMN:** and cannot contain a number sign (#). Example: "SMN:en-us:op_xxx;+08|00:console.xxx/aom/?agencyId=3402daf6xxxxx0e1&locale=en-us&region=xxx$/aom:urn:smn:xxx:06175f8cxxxx391f:aomtest" Parsed: "SMN:{zh-cn | en-us}:{domain_name};{timezone}:{console_uri}:{topic_urn}"

Parameter	Mandatory	Type	Description
alarmAdvice	No	String	Handling suggestion. Enter up to 255 characters.
alarmDescription	No	String	Threshold rule description. Enter up to 1024 characters.
insufficientDataActions	No	Array of strings	Action to be taken when data is insufficient. The array can contain up to five elements. It must start with **SMN:** and cannot contain a number sign (#). Example: "SMN:en-us:op_xxx;+08|00:console.xxx/aom/?agencyId=3402daf6xxxxx0e1&locale=en-us&region=xxx$/aom:urn:smn:xxx:06175f8cxxxx391f:aomtest" Parsed: "SMN:{zh-cn | en-us}:{domain_name};{timezone}:{console_uri}:{topic_urn}"
okActions	No	Array of strings	Action to be taken when restoration is complete. The array can contain up to five elements. It must start with **SMN:** and cannot contain a number sign (#). Example: "SMN:en-us:op_xxx;+08|00:console.xxx/aom/?agencyId=3402daf6xxxxx0e1&locale=en-us&region=xxx$/aom:urn:smn:xxx:06175f8cxxxx391f:aomtest" Parsed: "SMN:{zh-cn | en-us}:{domain_name};{timezone}:{console_uri}:{topic_urn}"

Table 4-34 Dimension

Parameter	Mandatory	Type	Description
name	Yes	String	Dimension name. It cannot be empty. Enter up to 255 characters.
value	No	String	Dimension value. Enter up to 1024 characters.

Response Parameters

Status code: 200

Table 4-35 Response body parameters

Parameter	Type	Description
errorCode	String	Response code.
errorMessage	String	Response message.
alarmId	Long	Threshold rule code.

Example Requests

Add a threshold rule.

```
POST https://{Endpoint}/v1/{project_id}/ams/alarms

{
  "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"
}
```

Example Responses

Status code: 200

OK

The request is successful.

```
{
  "errorCode" : "SVCSTG_AMS_2000000",
  "errorMessage" : "success",
  "alarmId" : 12345678
}
```


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 authorization information is incorrect or invalid.
403	ForbiddenThe 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**.

4.1.5 Modifying a Threshold Rule

Function

This API is used to modify a threshold rule.

URI

PUT /v1/{project_id}/ams/alarms

Table 4-36 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 4-37 Request header parameters

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

Table 4-38 Request body parameters

Parameter	Mandatory	Type	Description
statistic	Yes	String	Statistic. Enumeration values: • **maximum** • **minimum** • **average** • **sum** • **sampleCount**
namespace	No	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. • CUSTOM.Prometheus: namespace of Prometheus metrics. • Namespace of custom metrics.

Parameter	Mandatory	Type	Description
metricName	Yes	String	Metric name. The value must contain 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.
period	Yes	Integer	Statistical period. Values: 60,000, 300,000, 900,000, and 3,600,000.
alarmLevel	No	Integer	Alarm severity.
evaluationPeriods	Yes	Integer	Number of consecutive periods.
comparisonOperator	Yes	String	Threshold criterion expression. It cannot be empty. Options: >, <, >=, and <= Enumeration values: • >= • < • >= • <=
threshold	Yes	String	Threshold value. Enter up to 255 characters. It cannot be less than 0, or positive or negative infinity.
alarmName	Yes	String	Threshold name. It cannot be empty. Enter up to 255 characters. The following special characters are not allowed: "#%&'+;<=>?\
dimensions	Yes	Array of **Dimension** objects	Metric dimension. The total dimension length (that is, total JSON characters of the array) cannot exceed 65,535. The array cannot contain more than 100 elements.
unit	Yes	String	Metric unit. It cannot be empty. Enter up to 32 characters.
actionEnabled	No	Boolean	Whether to enable alarm reporting.

Parameter	Mandatory	Type	Description
alarmActions	No	Array of strings	Action to be taken when an alarm is reported. The array can contain up to five elements. It must start with **SMN:** and cannot contain a number sign (#). Example: "SMN:en-us:op_xxx;+08|00:console.xxx/aom/?agencyId=3402daf6xxxxx0e1&locale=en-us&region=xxx$/aom:urn:smn:xxx:06175f8cxxxx391f:aomtest" Parsed: "SMN:{zh-cn | en-us}:{domain_name};{timezone}:{console_uri}:{topic_urn}"
alarmAdvice	No	String	Handling suggestion. Enter up to 255 characters.
alarmDescription	No	String	Threshold rule description. Enter up to 1024 characters.
insufficientDataActions	No	Array of strings	Action to be taken when data is insufficient. The array can contain up to five elements. It must start with **SMN:** and cannot contain a number sign (#). Example: "SMN:en-us:op_xxx;+08|00:console.xxx/aom/?agencyId=3402daf6xxxxx0e1&locale=en-us&region=xxx$/aom:urn:smn:xxx:06175f8cxxxx391f:aomtest" Parsed: "SMN:{zh-cn | en-us}:{domain_name};{timezone}:{console_uri}:{topic_urn}"

Parameter	Mandatory	Type	Description
okActions	No	Array of strings	Action to be taken when restoration is complete. The array can contain up to five elements. It must start with **SMN:** and cannot contain a number sign (#). Example: "SMN:en-us:op_xxx;+08|00:console.xxx/aom/?agencyId=3402daf6xxxxx0e1&locale=en-us&region=xxx$/aom:urn:smn:xxx:06175f8cxxxx391f:aomtest" Parsed: "SMN:{zh-cn | en-us}:{domain_name};{timezone}:{console_uri}:{topic_urn}"

Table 4-39 Dimension

Parameter	Mandatory	Type	Description
name	Yes	String	Dimension name. It cannot be empty. Enter up to 255 characters.
value	No	String	Dimension value. Enter up to 1024 characters.

Response Parameters

Status code: 200

Table 4-40 Response body parameters

Parameter	Type	Description
errorCode	String	Response code.
errorMessage	String	Response message.
alarmId	Long	Threshold rule code.

Example Requests

Modify a threshold rule.

```
PUT https://{Endpoint}/v1/{project_id}/ams/alarms

{
```



```
 "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"
}
```

Example Responses

Status code: 200

OK

The request is successful.

```
{
 "errorCode" : "SVCSTG_AMS_2000000",
 "errorMessage" : "success",
 "alarmId" : 12345678
}
```

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 authorization information is incorrect or invalid.
403	ForbiddenThe 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	Description
503	Service Unavailable The requested service is invalid. The client should not repeat the request without modifications.

Error Codes

See **Error Codes**.

4.1.6 Querying the Threshold Rule List

Function

This API is used to query the threshold rule list.

URI

GET /v1/{project_id}/ams/alarms

Table 4-41 Path Parameters

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

Table 4-42 Query Parameters

Parameter	Mandatory	Type	Description
limit	No	Integer	Value range: 1–1000. Default value: 1000. Number of records that can be returned.
start	No	Long	Pagination information. Data will be queried based on the sequence number of the current record.

Request Parameters

Table 4-43 Request header parameters

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

Response Parameters

Status code: 200

Table 4-44 Response body parameters

Parameter	Type	Description
errorCode	String	Response code.
errorMessage	String	Response message.
metaData	**MetaData** object	Metadata, including pagination information.
thresholds	Array of **AlarmAPIQueryAlarmResult** objects	Threshold rule list.

Table 4-45 MetaData

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

Table 4-46 AlarmAPIQueryAlarmResult

Parameter	Type	Description
idTurnOn	Boolean	Whether to enable the threshold rule.
type	String	Threshold rule type.
policyName	String	Threshold rule template name.
alarmName	String	Threshold rule name.
id	String	Threshold rule ID.
alarmDescription	String	Threshold rule description.
actionEnabled	Boolean	Whether to enable notification.
okActions	Array of strings	Action to be taken when restoration is complete.
alarmActions	Array of strings	Action to be taken when an alarm is reported.
insufficientDataActions	Array of strings	Action to be taken when data is insufficient.
stateValue	String	Service status.
stateReason	String	Cause description.
stateUpdatedTimestamp	String	Time when the status was updated.
metricName	String	Time series name.
namespace	String	Namespace of time series objects.
statistic	String	Statistic.
dimensions	Array of **Dimension** objects	List of time series dimensions.
resources	Array of strings	Resource information (discarded).
period	Integer	Statistical period.
evaluationPeriods	Integer	Number of consecutive periods.
unit	String	Threshold unit.
threshold	String	Threshold value.
comparisonOperator	String	Comparison operator.

Parameter	Type	Description
alarmAdvice	String	Alarm clearance suggestion.
alarmLevel	String	Alarm severity.

Table 4-47 Dimension

Parameter	Type	Description
name	String	Dimension name. It cannot be empty. Enter up to 255 characters.
value	String	Dimension value. Enter up to 1024 characters.

Example Requests

Query the threshold rule list.

```
GET https://{Endpoint}/v1/{project_id}/ams/alarms
```

Example Responses

Status code: 200

OK

The request is successful.

```
{
  "errorCode" : "SVCSTG_AMS_2000000",
  "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 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 authorization information is incorrect or invalid.
403	ForbiddenThe 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**.

4.1.7 Querying a Threshold Rule

Function

This API is used to query a threshold rule.

URI

GET /v1/{project_id}/ams/alarms/{alarm_id}

Table 4-48 Path Parameters

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

Request Parameters

Table 4-49 Request header parameters

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

Response Parameters

Status code: 200

Table 4-50 Response body parameters

Parameter	Type	Description
errorCode	String	Response code.
errorMessage	String	Response message.
metaData	**MetaData** object	Metadata, including pagination information.
thresholds	Array of **AlarmAPIQueryAlarmResult** objects	Threshold rule list.

Table 4-51 MetaData

Parameter	Type	Description
count	Integer	Number of records that can be returned.

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

Table 4-52 AlarmAPIQueryAlarmResult

Parameter	Type	Description
idTurnOn	Boolean	Whether to enable the threshold rule.
type	String	Threshold rule type.
policyName	String	Threshold rule template name.
alarmName	String	Threshold rule name.
id	String	Threshold rule ID.
alarmDescription	String	Threshold rule description.
actionEnabled	Boolean	Whether to enable notification.
okActions	Array of strings	Action to be taken when restoration is complete.
alarmActions	Array of strings	Action to be taken when an alarm is reported.
insufficientDataActions	Array of strings	Action to be taken when data is insufficient.
stateValue	String	Service status.
stateReason	String	Cause description.
stateUpdatedTimestamp	String	Time when the status was updated.
metricName	String	Time series name.
namespace	String	Namespace of time series objects.
statistic	String	Statistic.
dimensions	Array of **Dimension** objects	List of time series dimensions.
resources	Array of strings	Resource information (discarded).
period	Integer	Statistical period.

Parameter	Type	Description
evaluationPeriods	Integer	Number of consecutive periods.
unit	String	Threshold unit.
threshold	String	Threshold value.
comparisonOperator	String	Comparison operator.
alarmAdvice	String	Alarm clearance suggestion.
alarmLevel	String	Alarm severity.

Table 4-53 Dimension

Parameter	Type	Description
name	String	Dimension name. It cannot be empty. Enter up to 255 characters.
value	String	Dimension value. Enter up to 1024 characters.

Example Requests

Query a threshold rule.

```
GET https://{Endpoint}/v1/{project_id}/ams/alarms/{alarm_id}
```

Example Responses

Status code: 200

OK

The request is successful.


```
{
  "errorCode" : "SVCSTG_AMS_2000000",
  "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 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 authorization information is incorrect or invalid.
403	ForbiddenThe 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**.

4.1.8 Deleting a Threshold Rule

Function

This API is used to delete a threshold rule.

URI

DELETE /v1/{project_id}/ams/alarms/{alarm_id}

Table 4-54 Path Parameters

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

Request Parameters

Table 4-55 Request header parameters

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

Response Parameters

Status code: 200

Table 4-56 Response body parameters

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

Example Requests

Delete a threshold rule.

```
DELETE https://{Endpoint}/v1/{project_id}/ams/alarms/{alarm_id}
```

Example Responses

Status code: 200

OK

The request is successful.

```
{
  "errorCode" : "SVCSTG_AMS_2000000",
  "errorMessage" : "Delete Threshold [aaaaaaaa] successfully"
}
```

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 authorization information is incorrect or invalid.
403	ForbiddenThe 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**.

4.1.9 Adding or Modifying One or More Application Discovery Rules

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

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.

Request Parameters

Table 4-58 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 4-59 Request body parameters

Parameter	Mandatory	Type	Description
appRules	Yes	Array of **AppRules** objects	Service parameters.

Table 4-60 AppRules

Parameter	Mandatory	Type	Description
createTime	No	String	Creation time. When creating an application discovery rule, leave this parameter blank. When modifying an application discovery rule, enter the returned createTime.
enable	Yes	Boolean	Whether a rule is enabled. Value: true or false.

Parameter	Mandatory	Type	Description
eventName	Yes	String	aom_inventory_rules_event Rule event name. For application discovery, the fixed value is aom_inventory_rules_event. Enumeration values: • **aom_inventory_rules_event**
hostid	No	Array of strings	Host ID (not used currently and can be left empty).
id	Yes	String	Rule ID. When creating an application discovery rule, leave this parameter blank. When modifying an application discovery rule, enter a rule ID.
name	Yes	String	Rule name. The value can contain a maximum of 64 characters. It must start with a lowercase letter and 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.

Table 4-61 AppRulesSpec

Parameter	Mandatory	Type	Description
appType	No	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. You can also enter collector or database by function.
attrList	No	Array of strings	Attribute list (not used currently and can be left empty). Value: cmdLine or env.

Parameter	Mandatory	Type	Description
detectLog	No	String	Whether to enable log collection. Value: true or false.
discoveryRule	Yes	Array of DiscoveryRule objects	Discovery rule. When it is an array consisting of multiple conditions, only the processes that meet all the conditions are filtered.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 current rule is the default one. Value: true or 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. Value: true or false.
logFileFix	No	Array of strings	Log file suffix. Value: log, trace, or out.

Parameter	Mandatory	Type	Description
logPathRule	No	Array of **LogPathRule** objects	Log path configuration rule.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.
nameRule	Yes	**NameRule** object	Naming rules for discovered services and applications.
priority	Yes	String	Rule priority. An integer ranging from 1 to 9999. The default value is 9999.

Table 4-62 DiscoveryRule

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

Table 4-63 LogPathRule

Parameter	Mandatory	Type	Description
args	No	Array of strings	Command.
nameType	No	String	Value type. Option: cmdLineHash.
value	No	Array of strings	Log path.

Table 4-64 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 **nameType** is **cmdLine** and **args** is **["start","end"]**, the characters between **start** and **end** in the command are extracted. If **args** is **["start",""]**, the characters from **start** to the end of the command are extracted.If **nameType** is **env** and **args** is **["aa"]**, the environment variable named **aa** is extracted.If **nameType** is **str** and **args** is **["fix"]**, the service name is suffixed with **fix**.If **nameType** is **cmdLineHash**, **args** is **["0001"]**, and **value** is **["ser"]**, the service name is **ser** when the startup command is **0001**.
applicationNameRule	Yes	Array of **ApplicationNameRule** objects	Application name rule.If **nameType** is **cmdLine** and **args** is **["start","end"]**, the characters between **start** and **end** in the command are extracted. If **args** is **["start",""]**, the characters from **start** to the end of the command are extracted.If **nameType** is **env** and **args** is **["aa"]**, the environment variable named **aa** is extracted.If **nameType** is **str** and **args** is **["fix"]**, the service name is suffixed with **fix**.If **nameType** is **cmdLineHash**, **args** is **["0001"]**, and **value** is **["ser"]**, the application name is **ser** when the startup command is **0001**.

Table 4-65 AppNameRule

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

Table 4-66 ApplicationNameRule

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

Response Parameters

Status code: 200

Table 4-67 Response body parameters

Parameter	Type	Description
errorCode	String	Response code.
errorMessage	String	Response message.
responseStatus	Integer	Response status code.

Example Requests

Add or modify one or more application discovery rules.

```
PUT https://{Endpoint}/v1/{project_id}/inv/servicediscoveryrules

{
```



```
 "appRules" : [ {
  "id" : "44d6c4bb-f673-4bf4-8d33-313832f37b28",
  "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",
     "args" : [ "00000000001" ],
     "value" : [ "applicationName1" ]
    }, {
     "nameType" : "str",
     "args" : [ "kubeproxy" ]
    } ]
   },
   "appType" : "",
   "isDefaultRule" : "false",
   "logPathRule" : [ {
    "nameType" : "cmdLineHash",
    "args" : [ "00000000001" ],
    "value" : [ "/xx/xxx/xx.log", "/xx/xxx/xx" ]
   } ]
  }
 } ]
}
```


Example Responses

Status code: 200

OK

The request is successful.


```
{
 "errorCode" : "SVCSTG.INV.2000000",
 "errorMessage" : "success",
```



```
  "id" : [ "44d6c4bb-f673-4bf4-8d33-313832f37b28" ]
}
```

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 authorization information is incorrect or invalid.
403	ForbiddenThe 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**.

4.1.10 Deleting an Application Discovery Rule

Function

This API is used to delete an application discovery rule.

URI

DELETE /v1/{project_id}/inv/servicediscoveryrules

Table 4-68 Path Parameters

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

Table 4-69 Query Parameters

Parameter	Mandatory	Type	Description
appRulesIds	Yes	Array	Discovery rule ID. IDs need to be separated by commas (,).

Request Parameters

Table 4-70 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 4-71 Response body parameters

Parameter	Type	Description
errorCode	String	Response code.
errorMessage	String	Response message.
responseStatus	Integer	Response status code.

Example Requests

Delete an application discovery rule with a specified ID.

```
DELETE https://{Endpoint}/v1/{project_id}/inv/servicediscoveryrules?appRulesIds=b788349e-62b2-3c7a-b597-02c611d59801
```

Example Responses

Status code: 200

OK

The request is successful.


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

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 authorization information is incorrect or invalid.
403	ForbiddenThe 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**.

4.1.11 Querying Application Discovery Rules

Function

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

URI

GET /v1/{project_id}/inv/servicediscoveryrules

Table 4-72 Path Parameters

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

Table 4-73 Query Parameters

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

Request Parameters

Table 4-74 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 4-75 Response body parameters

Parameter	Type	Description
appRules	Array of **AppRules** objects	Rule information.
errorCode	String	Response code. SVCSTG.INV.2000000: Success response.
errorMessage	String	Response message.

Table 4-76 AppRules

Parameter	Type	Description
createTime	String	Creation time. When creating an application discovery rule, leave this parameter blank. When modifying an application discovery rule, enter the returned createTime.
enable	Boolean	Whether a rule is enabled. Value: true or false.
eventName	String	aom_inventory_rules_event Rule event name. For application discovery, the fixed value is aom_inventory_rules_event. Enumeration values: • **aom_inventory_rules_event**
hostid	Array of strings	Host ID (not used currently and can be left empty).
id	String	Rule ID. When creating an application discovery rule, leave this parameter blank. When modifying an application discovery rule, enter a rule ID.
name	String	Rule name. The value can contain a maximum of 64 characters. It must start with a lowercase letter and 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.
spec	**AppRulesSpec** object	Rule details.

Table 4-77 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. You can also enter collector or database by function.
attrList	Array of strings	Attribute list (not used currently and can be left empty). Value: cmdLine or env.
detectLog	String	Whether to enable log collection. Value: true or false.

Parameter	Type	Description
discoveryRule	Array of **DiscoveryRule** objects	Discovery rule. When it is an array consisting of multiple conditions, only the processes that meet all the conditions are filtered.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 current rule is the default one. Value: true or 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. Value: true or false.
logFileFix	Array of strings	Log file suffix. Value: log, trace, or out.
logPathRule	Array of **LogPathRule** objects	Log path configuration rule.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.
nameRule	**NameRule** object	Naming rules for discovered services and applications.
priority	String	Rule priority. An integer ranging from 1 to 9999. The default value is 9999.

Table 4-78 DiscoveryRule

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

Table 4-79 LogPathRule

Parameter	Type	Description
args	Array of strings	Command.
nameType	String	Value type. Option: cmdLineHash.
value	Array of strings	Log path.

Table 4-80 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 **nameType** is **cmdLine** and **args** is **["start","end"]**, the characters between **start** and **end** in the command are extracted. If **args** is **["start",""]**, the characters from **start** to the end of the command are extracted.If **nameType** is **env** and **args** is **["aa"]**, the environment variable named **aa** is extracted.If **nameType** is **str** and **args** is **["fix"]**, the service name is suffixed with **fix**.If **nameType** is **cmdLineHash**, **args** is **["0001"]**, and **value** is **["ser"]**, the service name is **ser** when the startup command is **0001**.

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

Table 4-81 AppNameRule

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

Table 4-82 ApplicationNameRule

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

Example Requests

None

Example Responses

Status code: 200

OK

The request is successful.


```
{
  "appRules" : [ {
    "createTime" : "1599098476654",
    "enable" : true,
    "name" : "ica**nt",
    "eventName" : "aom_in***tory_rules_event",
    "hostid" : [ ],
    "id" : "b53a5152-****-****-****-302367e04c0b",
    "projectid" : "2a473356c*********be891bffc1cf",
    "spec" : {
      "detectLog" : "true",
      "editable" : null,
      "logPathRule" : [ ],
      "priority" : 9999,
      "attrList" : [ "cmdLine" ],
      "nameRule" : {
        "appNameRule" : [ {
          "nameType" : "cmdLineHash",
          "args" : [ "/opt/******** -DNFW=ica**nt" ],
          "value" : [ "aicagentserver" ]
        } ],
        "applicationNameRule" : [ {
          "nameType" : "cmdLineHash",
          "args" : [ "/opt/********** -DNFW=ica**nt" ],
          "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" : null
  } ],
  "errorMessage" : null,
  "errorCode" : "SVCSTG.INV.2000000",
  "responseStatus" : 200
}
```


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 authorization information is incorrect or invalid.

Status Code	Description
403	ForbiddenThe 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 (v2)

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.

URI

POST /v2/{project_id}/series

Table 4-83 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 4-84 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.
X-Aom-Prometheus-Id	No	String	Prometheus instance ID. If this parameter is left blank, the default Prometheus instance is used.

Table 4-85 Request body parameters

Parameter	Mandatory	Type	Description
series	Yes	Array of **QuerySeriesOptionParam** objects	Array with parameters transferred for time series query. An array supports up to 100 parameters.

Table 4-86 QuerySeriesOptionParam

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. • CUSTOM.Prometheus: namespace of Prometheus metrics. • Namespace of custom metrics.

Parameter	Mandatory	Type	Description
metric_name	No	String	Time series name. Length: 1–255 characters.
dimensions	No	Array of **DimensionSeries** objects	List of time series dimensions.

Table 4-87 DimensionSeries

Parameter	Mandatory	Type	Description
name	No	String	Name.
value	No	String	Value.

Response Parameters

Status code: 200

Table 4-88 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 4-89 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 4-90 DimensionSeries

Parameter	Type	Description
name	String	Name.
value	String	Value.

Table 4-91 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	Long	Offset.

Status code: 400

Table 4-92 Response body parameters

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

Example Requests

Query data by namespace+appName+clusterName

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

{
  "series" : [ {
    "namespace" : "PAAS.CONTAINER",
    "dimensions" : [ {
      "name" : "appName",
      "value" : "demo"
    }, {
      "name" : "clusterName",
      "value" : "test"
    } ]
  } ]
}
```


Example Responses

Status code: 200

OK

The request is successful.

```
{
  "meta_data" : {
    "count" : 1,
    "offset" : null,
    "total" : 1
  },
  "series" : [ {
    "namespace" : "abc",
    "metric_name" : "cpuUsage",
    "unit" : "Percent",
    "dimensions" : [ {
      "name" : "instance_id",
      "value" : "demo1"
    } ]
  } ]
}
```

Status code: 400

Bad Request

Invalid request. The client should not repeat the request without modifications.

```
{
  "error_code" : "AOM.04007500",
  "error_msg" : "internal server error",
  "error_type" : "INTERNAL_SERVER_ERROR"
}
```

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 authorization 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	Description
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 time period. You can specify a dimension or period to query.

URI

POST /v2/{project_id}/samples

Table 4-93 Path Parameters

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

Table 4-94 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 4-95 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.
X-Aom-Prometheus-Id	No	String	Prometheus instance ID. If this parameter is left blank, the default Prometheus instance is used.

Table 4-96 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. 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. For example, 1650852000000.-1.5 is equivalent to 1650852000000.1650852300000.5.

Parameter	Mandatory	Type	Description
			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 4-97 QuerySample

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. • CUSTOM.Prometheus: namespace of Prometheus metrics. • Namespace of custom metrics.

Parameter	Mandatory	Type	Description
dimensions	Yes	Array of **DimensionSeries** objects	List of time series dimensions. Neither the array nor the name or value of any dimension in the array can be left blank.
metric_name	Yes	String	Time series name. Values: Length: 1–255 characters.

Table 4-98 DimensionSeries

Parameter	Mandatory	Type	Description
name	No	String	Name.
value	No	String	Value.

Response Parameters

Status code: 200

Table 4-99 Response body parameters

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

Table 4-100 SampleDataValue

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

Table 4-101 QuerySample

Parameter	Type	Description
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. • CUSTOM.Prometheus: namespace of Prometheus metrics. • Namespace of custom metrics.
dimensions	Array of **DimensionSeries** objects	List of time series dimensions. Neither the array nor the name or value of any dimension in the array can be left blank.
metric_name	String	Time series name. Values: Length: 1–255 characters.

Table 4-102 DimensionSeries

Parameter	Type	Description
name	String	Name.
value	String	Value.

Table 4-103 MetricDataPoints

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

Table 4-104 StatisticValue

Parameter	Type	Description
statistic	String	Statistic.

Parameter	Type	Description
value	Double	Statistical result.

Status code: 400

Table 4-105 Response body parameters

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

Example Requests

Querying the monitoring time series data in the last 5 minutes.

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

{
  "samples" : [ {
    "namespace" : "abc",
    "metric_name" : "def",
    "dimensions" : [ {
      "name" : "instance_id",
      "value" : "demo1"
    } ]
  } ],
  "period" : 60,
  "time_range" : "-1.-1.5",
  "statistics" : [ "maximum", "minimum", "sum" ]
}
```

Example Responses

Status code: 200

OK

The request is successful.

```
{
  "samples" : [ {
    "sample" : {
      "namespace" : "abc",
      "metric_name" : "def",
      "dimensions" : [ {
        "name" : "ghi",
        "value" : "lmn"
      } ]
    },
    "data_points" : [ {
      "timestamp" : "1467892800000",
      "unit" : "Percent",
      "statistics" : [ {
```



```
      "statistic" : "maximum",
      "value" : "23"
    } ]
  } ]
 } ]
}
```

Status code: 400

Bad Request

Invalid request. The client should not repeat the request without modifications.

```
{
  "error_code" : "AOM.04008500",
  "error_msg" : "internal server error",
  "error_type" : "INTERNAL_SERVER_ERROR"
}
```

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 authorization 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**.

4.2.3 Adding a Threshold Rule

Function

This API is used to add a threshold rule.

URI

POST /v2/{project_id}/alarm-rules

Table 4-106 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 4-107 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 4-108 Request body parameters

Parameter	Mandatory	Type	Description
alarm_advice	No	String	Alarm clearance suggestion.
alarm_description	No	String	Threshold rule description.
alarm_level	Yes	Integer	Alarm severity. Values: 1 (critical), 2 (major), 3 (minor), and 4 (warning).
alarm_rule_name	Yes	String	Threshold rule name. The following characters are not allowed: $>+<;#";&?%=''
comparison_operator	Yes	String	Comparison operator. Values: >, >=, <, and <=.

Parameter	Mandatory	Type	Description
dimensions	Yes	Array of **Dimension** objects	List of time series dimensions.
evaluation_periods	Yes	Integer	Interval at which data is calculated. Value range: 1–5.
is_turn_on	No	Boolean	Whether to enable the threshold rule.
metric_name	Yes	String	Time series name. Length: 1–255 characters.
namespace	Yes	String	Namespace of time series objects.
period	Yes	Integer	Statistical period. Values: 60,000, 300,000, 900,000, and 3,600,000.
statistic	Yes	String	Statistic. Values: maximum, minimum, average, sum, and sampleCount.
threshold	Yes	String	Threshold value. Length: up to 255 characters. The value must be parsed as a positive number.
unit	No	String	Threshold unit.

Table 4-109 Dimension

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

Response Parameters

Status code: 200

Table 4-110 Response body parameters

Parameter	Type	Description
alarm_rule_id	Long	Threshold rule ID.

Status code: 400

Table 4-111 Response body parameters

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

Example Requests

Add a threshold rule.

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

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

Example Responses

Status code: 200

OK

The request is successful.

```
{
  "alarm_rule_id" : [ ]
}
```

Status code: 400

Bad Request

Invalid request. The client should not repeat the request without modifications.

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


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 authorization 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**.

4.2.4 Querying the Threshold Rule List

Function

This API is used to query the threshold rule list.

URI

GET /v2/{project_id}/alarm-rules

Table 4-112 Path Parameters

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

Table 4-113 Query Parameters

Parameter	Mandatory	Type	Description
offset	No	String	Pagination information.
limit	No	Integer	Number of data records that can be returned. Value range: 1–1000. Default value: 1000.

Request Parameters

Table 4-114 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 4-115 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 4-116 MetaData

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

Table 4-117 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.
dimensions	Array of **Dimension** objects	List of time series dimensions.
evaluation_periods	Integer	Interval at which data is calculated.
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	Namespace of time series objects.
ok_actions	Array of strings	List of normal status notifications.
period	Integer	Statistical period.
policy_name	String	Threshold rule template 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.

Parameter	Type	Description
threshold	String	Threshold value.
type	String	Threshold rule type.
unit	String	Threshold unit.

Table 4-118 Dimension

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

Status code: 400

Table 4-119 Response body parameters

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

Example Requests

None

Example Responses

Status code: 200

OK

The request is successful.


```
{
  "meta_data" : [ {
    "count" : 10,
    "offset" : null,
    "total" : 100
  } ],
  "thresholds" : [ {
    "alarm_actions" : null,
    "alarm_advice" : null,
    "alarm_description" : null,
    "alarm_level" : 3,
    "alarm_rule_id" : 2137,
    "alarm_rule_name" : "aaaaaaaa",
    "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

Invalid request. The client should not repeat the request without modifications.


```
{
  "error_code" : "AOM.02003500",
  "error_msg" : "internal server error",
  "error_type" : "INTERNAL_SERVER_ERROR"
}
```


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 authorization 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	Description
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 Modifying a Threshold Rule

Function

This API is used to modify a threshold rule.

URI

PUT /v2/{project_id}/alarm-rules

Table 4-120 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 4-121 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 4-122 Request body parameters

Parameter	Mandatory	Type	Description
alarm_advice	No	String	Alarm clearance suggestion.

Parameter	Mandatory	Type	Description
alarm_description	No	String	Threshold rule description.
alarm_level	No	Integer	Alarm severity. Values: 1 (critical), 2 (major), 3 (minor), and 4 (warning).
alarm_rule_name	Yes	String	Threshold rule name. The following characters are not allowed: $>+<;#';&?%=''
comparison_operator	Yes	String	Comparison operator. Values: >, >=, <, and <=.
dimensions	Yes	Array of **Dimension** objects	List of time series dimensions.
evaluation_periods	Yes	Integer	Interval at which data is calculated. Value range: 1–5.
id_turn_on	No	Boolean	Whether to enable the threshold rule.
metric_name	Yes	String	Time series name. Length: 1–255 characters.
namespace	Yes	String	Namespace of time series objects.
period	Yes	Integer	Statistical period. Values: 60,000, 300,000, 900,000, and 3,600,000.
statistic	Yes	String	Statistic. Values: maximum, minimum, average, sum, and sampleCount.
threshold	Yes	String	Threshold value. Length: up to 255 characters. The value must be parsed as a positive number.
unit	No	String	Threshold unit.

Table 4-123 Dimension

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

Response Parameters

Status code: 200

Table 4-124 Response body parameters

Parameter	Type	Description
alarm_rule_id	Long	Threshold rule ID.

Status code: 400

Table 4-125 Response body parameters

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

Example Requests

Modify a threshold rule.

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

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

Example Responses

Status code: 200

OK

The request is successful.

```
{
  "errorCode" : "200",
```



```
  "errorMessage" : "success",
  "alarmId" : 91307490000416600
}
```

Status code: 400

Bad Request

Invalid request. The client should not repeat the request without modifications.

```
{
  "error_code" : "AOM.02002500",
  "error_msg" : "internal server error",
  "error_type" : "INTERNAL_SERVER_ERROR"
}
```

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 authorization 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 Deleting a Threshold Rule

Function

This API is used to delete a threshold rule.

URI

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

Table 4-126 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 4-127 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: 400

Table 4-128 Response body parameters

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

Example Requests

Delete a threshold rule.

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

Example Responses

Status code: 400

Bad Request

Invalid request. The client should not repeat the request without modifications.

```
{
  "error_code" : "AOM.02005500",
  "error_msg" : "internal server error",
  "error_type" : "INTERNAL_SERVER_ERROR"
}
```

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 authorization 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 Querying a Threshold Rule

Function

This API is used to query a threshold rule.

URI

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

Table 4-129 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 4-130 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 4-131 Response body parameters

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

Table 4-132 MetaData

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

Table 4-133 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.
dimensions	Array of **Dimension** objects	List of time series dimensions.
evaluation_periods	Integer	Interval at which data is calculated.
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	Namespace of time series objects.
ok_actions	Array of strings	List of normal status notifications.
period	Integer	Statistical period.
policy_name	String	Threshold rule template 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.

Parameter	Type	Description
threshold	String	Threshold value.
type	String	Threshold rule type.
unit	String	Threshold unit.

Table 4-134 Dimension

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

Status code: 400

Table 4-135 Response body parameters

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

Example Requests

None

Example Responses

Status code: 200

OK

The request is successful.


```
{
  "thresholds" : [ {
    "alarm_actions" : null,
    "alarm_advice" : null,
    "alarm_description" : null,
    "alarm_level" : 3,
    "alarm_rule_id" : 2137,
    "alarm_rule_name" : "aaaaaaaa",
    "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_aalue" : "alarm",
    "state_reason" : null,
    "state_updated_timestamp" : null,
    "statistic" : "average",
    "threshold" : 0,
    "type" : "single,",
    "unit" : "Core"
  } ]
}
```


Status code: 400

Bad Request

Invalid request. The client should not repeat the request without modifications.


```
{
  "error_code" : "AOM.02004500",
  "error_msg" : "internal server error",
  "error_type" : "INTERNAL_SERVER_ERROR"
}
```


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 authorization 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**.

4.2.8 Deleting Threshold Rules in Batches

Function

This API is used to delete threshold rules in batches.

URI

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

Table 4-136 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 4-137 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 4-138 Request body parameters

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

Response Parameters

Status code: 400

Table 4-139 Response body parameters

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

Example Requests

Delete threshold rules in batches.

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

{
  "alarm_rules" : [ ]
}
```

Example Responses

Status code: 400

Bad Request

Invalid request. The client should not repeat the request without modifications.

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

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 authorization 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**.

4.3 Auto Scaling

4.3.1 Creating a Policy

Function

This API is used to create a policy. The value must contain 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 of metric_threshold with metric_operation set to <.In an AS group, you can create only one alarm policy with the same metric_operation for each metric.In a policy, 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

Table 4-140 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Request Parameters

Table 4-141 Request header parameters

Parameter	Mandatory	Type	Description
resourcetype	Yes	String	Resource type. Example: node
Content-Type	Yes	String	Content type, which is application/json;charset=utf-8. Enumeration values: • **application/ json;charset=utf-8**
Cluster-Id	Yes	String	Cluster ID.
Namespace	Yes	String	Namespace.
X-Auth-Token	Yes	String	User token obtained from IAM.
Reserved-Info	No	String	Custom field.

Table 4-142 Request body parameters

Parameter	Mandatory	Type	Description
name	Yes	String	Policy name.
policy_type	Yes	String	Policy type. Value: SCHEDULED RECURRENCE ALARM Enumeration values: • **SCHEDULED** • **RECURRENCE** • **ALARM**
group_id	Yes	String	Policy group ID.
rule	Yes	**AlarmRule** object	Policy trigger rule.

Table 4-143 AlarmRule

Parameter	Mandatory	Type	Description
actions	Yes	Array of **Action** objects	Action executed after a specified policy is matched.

Parameter	Mandatory	Type	Description
conditions	Yes	Array of **AlarmConditions** objects	Condition contents. A rule can contain multiple conditions in AND relationships. One condition describes the matching method of one metric.

Table 4-144 Action

Parameter	Mandatory	Type	Description
type	Yes	String	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 scale-in or -out for containerized applications and that containing vm indicates a scale-in or -out for process applications. Enumeration values: • **scale_out_k8s** • **scale_out_vm** • **scale_in_k8s** • **scale_in_vm**
parameters	Yes	Array of **Parameter** objects	Number of scale-in or -out instances.

Table 4-145 Parameter

Parameter	Mandatory	Type	Description
scale_unit	Yes	Integer	Number of scale-in or -out instances. The value is between the minimum number of instances to the maximum number of instances in a policy group.

Table 4-146 AlarmConditions

Parameter	Mandatory	Type	Description
metric_namespace	Yes	String	Metric namespace. Enumeration values: • **PAAS.CONTAINER** • **PAAS.CUSTOMMETRICS**
metric_name	Yes	String	Metric name. Enumeration values: • **^[a-zA-Z_:][a-zA-Z0-9_:]{0** • **254}$**
metric_unit	Yes	String	Unit. Note: The value is retrieved from an AMS API and varies with the metric name.
period	Yes	Integer	Statistical period (unit: s). Enumeration values: • **20** • **60** • **300** • **900** • **1800** • **3600**
evaluation_periods	Yes	Integer	Number of consecutive periods. Enumeration values: • **1** • **2** • **3** • **4** • **5**
statistic	Yes	String	Statistic. Enumeration values: • **average**

Parameter	Mandatory	Type	Description
metric_operation	Yes	String	Metric operator. Option: > or <. For example, you can use > in a threshold criterion (when the value of a metric is greater than metric_thresholdUpdate) to trigger actions. Enumeration values: • >\n• <
metric_threshold	Yes	Integer	Threshold condition.

Response Parameters

Status code: 200

Table 4-147 Response body parameters

Parameter	Type	Description
errorCode	String	Error code.
errorMessage	String	Details.
policy_id	String	Policy ID.

Example Requests

- Example of a periodic policy

```
POST https://{EndPoint}/v1/{project_id}/pe/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


```
POST https://{EndPoint}/v1/{project_id}/pe/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
      }
    } ]
  }
}
```

- Example of a scheduled policy

```
POST https://{EndPoint}/v1/{project_id}/pe/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 Responses

Status code: 200

OK

The request is successful.

```
{
  "errorCode" : "SVCSTG.PE.0",
  "errorMessage" : "",
  "policy_id" : "1b9994f0-847a-45e4-aeee-e8b604dddb34"
}
```


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 authorization information is incorrect or invalid.
403	ForbiddenThe 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**.

4.3.2 Querying the Policy List

Function

This API is used to query details about all policies in a specified project.

URI

GET /v1/{project_id}/pe/policy

Table 4-148 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Request Parameters

Table 4-149 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**
resourcetype	Yes	String	Resource type. Value: nod or app. Enumeration values: • **node** • **app**
Cluster-Id	Yes	String	Cluster ID.

Response Parameters

Status code: 200

Table 4-150 Response body parameters

Parameter	Type	Description
errorCode	String	Error code.
errorMessage	String	Details.
policies	Array of **AllPolicyContext** objects	Details about a modified policy.

Table 4-151 AllPolicyContext

Parameter	Type	Description
id	String	Policy ID.
group_id	String	Policy group ID.
name	String	Policy name.
policy_type	String	Policy type.

Parameter	Type	Description
rule	**AllRule** object	Policy trigger rule.
create_time	String	Creation time.
update_time	String	Update time.
status	String	Status.

Table 4-152 AllRule

Parameter	Type	Description
conditions	Array of **AllConditions** objects	Condition contents. When an alarm policy is used, its conditions cannot conflict. Example: You cannot set a metric greater than 10% in one condition and smaller than 20% in another condition.
actions	Array of **Action** objects	Action executed after a specified policy is matched.
name	String	Policy name.

Table 4-153 AllConditions

Parameter	Type	Description
launch_time	String	Time when the policy is triggered. This parameter is available when policy_type is set to SCHEDULED or RECURRENCE.
recurrence_type	String	Period type. This parameter is left blank for scheduled policies. This parameter is available when policy_type is set to SCHEDULED or RECURRENCE.
recurrence_value	String	Specific trigger time of a periodic policy. This parameter is left blank for scheduled policies. This parameter is available when policy_type is set to SCHEDULED or RECURRENCE.
start_time	Integer	Start time of the periodic policy. This parameter is left blank for the scheduled policy. This parameter is available when policy_type is set to SCHEDULED or RECURRENCE.

Parameter	Type	Description
end_time	Integer	End time of the periodic policy. This parameter is left blank for the scheduled policy. This parameter is available when policy_type is set to SCHEDULED or RECURRENCE.
time_zone	String	Time zone. This parameter is available when policy_type is set to SCHEDULED or RECURRENCE.
metric_namespace	String	Metric namespace. This parameter is available when policy_type is set to ALARM. Enumeration values: • **PAAS.CONTAINER** • **PAAS.CUSTOMMETRICS**
metric_name	String	Metric name. This parameter is available when policy_type is set to ALARM. Enumeration values: • **^[a-zA-Z_:][a-zA-Z0-9_:]{0** • **254}$**
metric_unit	String	Unit. Note: The value is retrieved from an AMS API and varies with the metric name. This parameter is available when policy_type is set to ALARM.
period	Integer	Statistical period (unit: s). This parameter is available when policy_type is set to ALARM. Enumeration values: • **20** • **60** • **300** • **900** • **1800** • **3600**
evaluation_periods	Integer	Number of consecutive periods. This parameter is available when policy_type is set to ALARM. Enumeration values: • **1** • **2** • **3** • **4** • **5**

Parameter	Type	Description
statistic	String	Statistic. This parameter is available when policy_type is set to ALARM. Enumeration values: • **average**
metric_operation	String	Metric operator. Option: > or <. For example, you can use > in a threshold criterion (when the value of a metric is greater than metric_thresholdUpdate) to trigger actions. This parameter is available when policy_type is set to ALARM. Enumeration values: • >\n• <
metric_threshold	Integer	Threshold condition. This parameter is available when policy_type is set to ALARM.

Table 4-154 Action

Parameter	Type	Description
type	String	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 scale-in or -out for containerized applications and that containing vm indicates a scale-in or -out for process applications. Enumeration values: • **scale_out_k8s**\n• **scale_out_vm**\n• **scale_in_k8s**\n• **scale_in_vm**
parameters	Array of **Parameter** objects	Number of scale-in or -out instances.

Table 4-155 Parameter

Parameter	Type	Description
scale_unit	Integer	Number of scale-in or -out instances. The value is between the minimum number of instances to the maximum number of instances in a policy group.

Example Requests

None

Example Responses

Status code: 200

OK

The request is successful.


```
{
  "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" : ">",
        "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"
 } ]
}
```


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 authorization information is incorrect or invalid.
403	ForbiddenThe 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**.

4.3.3 Deleting a Policy

Function

This API is used to delete a policy based on its ID.

URI

DELETE /v1/{project_id}/pe/policy/{policy_id}

Table 4-156 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
policy_id	Yes	String	Policy ID. The policy with this ID is to be deleted.

Request Parameters

Table 4-157 Request header parameters

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

Response Parameters

Status code: 200

Table 4-158 Response body parameters

Parameter	Type	Description
errorCode	String	Error code.
errorMessage	String	Details.

Example Requests

Delete the policy whose ID is 1b9994f0-847a-45e4-aeee-e8b604dddb34.

```
DELETE https://{Endpoint}/v1/{project_id}/pe/policy/1b9994f0-847a-45e4-aeee-e8b604dddb34
```

N/A

Example Responses

None

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 authorization information is incorrect or invalid.
403	ForbiddenThe 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**.

4.3.4 Modifying a Policy

Function

This API is used to modify a policy. Alarm policies can be modified, but scheduled and periodic policies cannot.

URI

PUT /v1/{project_id}/pe/policy/{policy_id}

Table 4-159 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
policy_id	Yes	String	Policy ID.

Request Parameters

Table 4-160 Request header parameters

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Content type, which is application/json;charset=utf-8. Enumeration values: • **application/json;charset=utf-8** • **application/json**
Cluster-Id	Yes	String	Cluster ID.
Namespace	Yes	String	Namespace.
Deployment-Name	Yes	String	Application name.
X-Auth-Token	Yes	String	Project-level token obtained from IAM.

Table 4-161 Request body parameters

Parameter	Mandatory	Type	Description
id	Yes	String	Policy ID.
name	Yes	String	Policy name, which cannot be modified. The value must contain 1 to 64 characters starting with a letter. Only digits, letters, underscores (_), and hyphens (-) are allowed.
policy_type	Yes	String	Policy type. Currently, only ALARM policies are supported. Enumeration values: • **ALARM**
rule	Yes	**AlarmRule** object	Policy trigger rule.
group_id	Yes	String	Policy group ID.

Table 4-162 AlarmRule

Parameter	Mandatory	Type	Description
actions	Yes	Array of **Action** objects	Action executed after a specified policy is matched.
conditions	Yes	Array of **AlarmConditions** objects	Condition contents. A rule can contain multiple conditions in AND relationships. One condition describes the matching method of one metric.

Table 4-163 Action

Parameter	Mandatory	Type	Description
type	Yes	String	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 scale-in or -out for containerized applications and that containing vm indicates a scale-in or -out for process applications. Enumeration values: • **scale_out_k8s** • **scale_out_vm** • **scale_in_k8s** • **scale_in_vm**
parameters	Yes	Array of **Parameter** objects	Number of scale-in or -out instances.

Table 4-164 Parameter

Parameter	Mandatory	Type	Description
scale_unit	Yes	Integer	Number of scale-in or -out instances. The value is between the minimum number of instances to the maximum number of instances in a policy group.

Table 4-165 AlarmConditions

Parameter	Mandatory	Type	Description
metric_namespace	Yes	String	Metric namespace. Enumeration values: • **PAAS.CONTAINER** • **PAAS.CUSTOMMETRICS**
metric_name	Yes	String	Metric name. Enumeration values: • **^[a-zA-Z_:][a-zA-Z0-9_:]{0** • **254}$**
metric_unit	Yes	String	Unit. Note: The value is retrieved from an AMS API and varies with the metric name.
period	Yes	Integer	Statistical period (unit: s). Enumeration values: • **20** • **60** • **300** • **900** • **1800** • **3600**
evaluation_periods	Yes	Integer	Number of consecutive periods. Enumeration values: • **1** • **2** • **3** • **4** • **5**
statistic	Yes	String	Statistic. Enumeration values: • **average**

Parameter	Mandatory	Type	Description
metric_operation	Yes	String	Metric operator. Option: > or <. For example, you can use > in a threshold criterion (when the value of a metric is greater than metric_thresholdUpdate) to trigger actions. Enumeration values: • >\n• <
metric_threshold	Yes	Integer	Threshold condition.

Response Parameters

Status code: 200

Table 4-166 Response body parameters

Parameter	Type	Description
errorCode	String	Error code.
errorMessage	String	Details.
context	**PePolicyContext** object	Details about a modified policy.

Table 4-167 PePolicyContext

Parameter	Type	Description
id	String	Policy ID.
name	String	Policy name, which cannot be modified. The value must contain 1 to 64 characters starting with a letter. Only digits, letters, underscores (_), and hyphens (-) are allowed.
policy_type	String	Policy type. Currently, only ALARM policies are supported. Enumeration values: • **ALARM**
rule	**AlarmRule** object	Policy trigger rule.

Table 4-168 AlarmRule

Parameter	Type	Description
actions	Array of **Action** objects	Action executed after a specified policy is matched.
conditions	Array of **AlarmConditions** objects	Condition contents. A rule can contain multiple conditions in AND relationships. One condition describes the matching method of one metric.

Table 4-169 Action

Parameter	Type	Description
type	String	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 scale-in or -out for containerized applications and that containing vm indicates a scale-in or -out for process applications. Enumeration values: • **scale_out_k8s** • **scale_out_vm** • **scale_in_k8s** • **scale_in_vm**
parameters	Array of **Parameter** objects	Number of scale-in or -out instances.

Table 4-170 Parameter

Parameter	Type	Description
scale_unit	Integer	Number of scale-in or -out instances. The value is between the minimum number of instances to the maximum number of instances in a policy group.

Table 4-171 AlarmConditions

Parameter	Type	Description
metric_namespace	String	Metric namespace. Enumeration values: • **PAAS.CONTAINER** • **PAAS.CUSTOMMETRICS**
metric_name	String	Metric name. Enumeration values: • **^[a-zA-Z_:][a-zA-Z0-9_:]{0** • **254}$**
metric_unit	String	Unit. Note: The value is retrieved from an AMS API and varies with the metric name.
period	Integer	Statistical period (unit: s). Enumeration values: • **20** • **60** • **300** • **900** • **1800** • **3600**
evaluation_periods	Integer	Number of consecutive periods. Enumeration values: • **1** • **2** • **3** • **4** • **5**
statistic	String	Statistic. Enumeration values: • **average**
metric_operation	String	Metric operator. Option: > or <. For example, you can use > in a threshold criterion (when the value of a metric is greater than metric_thresholdUpdate) to trigger actions. Enumeration values: • **>** • **<**
metric_threshold	Integer	Threshold condition.

Example Requests

Modify an alarm policy.

```
PUT https://{Endpoint}/v1/{project_id}/pe/policy/{policy_id}

{
  "group_id" : "943eba0f-b10a-4066-6261-1857a53500ff",
  "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
      }
    } ]
  }
}
```

Example Responses

Status code: 200

OK

The request is successful.

```
{
  "errorCode" : "SVCSTG.PE.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
        }
      } ]
    }
```



```
  }
}
```

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 authorization information is incorrect or invalid.
403	ForbiddenThe 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**.

4.3.5 Querying a Policy

Function

This API is used to query details about a policy in a specified project.

URI

GET /v1/{project_id}/pe/policy/{policy_id}

Table 4-172 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
policy_id	Yes	String	Policy ID.

Request Parameters

Table 4-173 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 4-174 Response body parameters

Parameter	Type	Description
errorCode	String	Error code.
errorMessage	String	Details.
policy	**AllPolicyContext** object	Details about a modified policy.

Table 4-175 AllPolicyContext

Parameter	Type	Description
id	String	Policy ID.
group_id	String	Policy group ID.
name	String	Policy name.
policy_type	String	Policy type.
rule	**AllRule** object	Policy trigger rule.
create_time	String	Creation time.
update_time	String	Update time.
status	String	Status.

Table 4-176 AllRule

Parameter	Type	Description
conditions	Array of **AllConditions** objects	Condition contents. When an alarm policy is used, its conditions cannot conflict. Example: You cannot set a metric greater than 10% in one condition and smaller than 20% in another condition.
actions	Array of **Action** objects	Action executed after a specified policy is matched.
name	String	Policy name.

Table 4-177 AllConditions

Parameter	Type	Description
launch_time	String	Time when the policy is triggered. This parameter is available when policy_type is set to SCHEDULED or RECURRENCE.
recurrence_type	String	Period type. This parameter is left blank for scheduled policies. This parameter is available when policy_type is set to SCHEDULED or RECURRENCE.
recurrence_value	String	Specific trigger time of a periodic policy. This parameter is left blank for scheduled policies. This parameter is available when policy_type is set to SCHEDULED or RECURRENCE.
start_time	Integer	Start time of the periodic policy. This parameter is left blank for the scheduled policy. This parameter is available when policy_type is set to SCHEDULED or RECURRENCE.
end_time	Integer	End time of the periodic policy. This parameter is left blank for the scheduled policy. This parameter is available when policy_type is set to SCHEDULED or RECURRENCE.
time_zone	String	Time zone. This parameter is available when policy_type is set to SCHEDULED or RECURRENCE.

Parameter	Type	Description
metric_namespace	String	Metric namespace. This parameter is available when policy_type is set to ALARM. Enumeration values: • **PAAS.CONTAINER** • **PAAS.CUSTOMMETRICS**
metric_name	String	Metric name. This parameter is available when policy_type is set to ALARM. Enumeration values: • **^[a-zA-Z_:][a-zA-Z0-9_:]{0** • **254}$**
metric_unit	String	Unit. Note: The value is retrieved from an AMS API and varies with the metric name. This parameter is available when policy_type is set to ALARM.
period	Integer	Statistical period (unit: s). This parameter is available when policy_type is set to ALARM. Enumeration values: • **20** • **60** • **300** • **900** • **1800** • **3600**
evaluation_periods	Integer	Number of consecutive periods. This parameter is available when policy_type is set to ALARM. Enumeration values: • **1** • **2** • **3** • **4** • **5**
statistic	String	Statistic. This parameter is available when policy_type is set to ALARM. Enumeration values: • **average**

Parameter	Type	Description
metric_operation	String	Metric operator. Option: > or <. For example, you can use > in a threshold criterion (when the value of a metric is greater than metric_thresholdUpdate) to trigger actions. This parameter is available when policy_type is set to ALARM. Enumeration values: • >\n• <
metric_threshold	Integer	Threshold condition. This parameter is available when policy_type is set to ALARM.

Table 4-178 Action

Parameter	Type	Description
type	String	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 scale-in or -out for containerized applications and that containing vm indicates a scale-in or -out for process applications. Enumeration values: • **scale_out_k8s**\n• **scale_out_vm**\n• **scale_in_k8s**\n• **scale_in_vm**
parameters	Array of **Parameter** objects	Number of scale-in or -out instances.

Table 4-179 Parameter

Parameter	Type	Description
scale_unit	Integer	Number of scale-in or -out instances. The value is between the minimum number of instances to the maximum number of instances in a policy group.

Example Requests

None

Example Responses

Status code: 200

OK

The request is successful.


```
{
  "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" : ">",
        "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"
  }
}
```


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 authorization information is incorrect or invalid.

Status Code	Description
403	ForbiddenThe 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**.

4.3.6 Modifying Policy Group Attributes

Function

This API is used to modify policy group attributes.

URI

PUT /v1/{project_id}/pe/policy/config

Table 4-180 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Request Parameters

Table 4-181 Request header parameters

Parameter	Mandatory	Type	Description
ResourceType	Yes	String	Resource type. Default value: app, indicating that the policy group attributes of an application are modified. Enumeration values: • **app**

Parameter	Mandatory	Type	Description
Cluster-Id	Yes	String	Cluster ID.
Namespace	Yes	String	Namespace.
Deployment-Name	Yes	String	Application name.
X-Auth-Token	Yes	String	Project-level token obtained from IAM.
Content-Type	Yes	String	Content type, which is application/json. Enumeration values: • **application/json**

Table 4-182 Request body parameters

Parameter	Mandatory	Type	Description
max_instances	No	Integer	Maximum number of instances, indicating the upper limit for capacity expansion.
min_instances	No	Integer	Minimum number of instances, indicating the lower limit for capacity expansion.
cooldown_time	No	Integer	Cooldown period (unit: s). After an applied policy is executed, the next policy can be executed only after the cooldown period expires.
deployment_name	No	String	Application name.

Response Parameters

Status code: 200

Table 4-183 Response body parameters

Parameter	Type	Description
errorCode	String	Error code.
errorMessage	String	Details.

Example Requests

Modify policy group attributes.

```
PUT https://{Endpoint}/v1/{project_id}/pe/policy/config

{
  "max_instances" : 100,
  "min_instances" : 1,
  "cooldown_time" : 60,
  "deployment_name" : "test01"
}
```

Example Responses

Status code: 200

OK

The request is successful.

```
{
  "errorCode" : "SVCSTG.PE.0",
  "errorMessage" : ""
}
```

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 authorization information is incorrect or invalid.
403	ForbiddenThe 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**.

4.3.7 Querying Policy Group Attributes

Function

This API is used to query policy group attributes.

URI

GET /v1/{project_id}/pe/policy/config

Table 4-184 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Request Parameters

Table 4-185 Request header parameters

Parameter	Mandatory	Type	Description
ResourceType	Yes	String	Resource type.
Content-Type	Yes	String	Content type, which is application/json;charset=utf-8. Enumeration values: • **application/ json;charset=utf-8** • **application/json**
Cluster-Id	Yes	String	Cluster ID.
Namespace	Yes	String	Namespace.
Deployment-Name	Yes	String	Application name.
X-Auth-Token	Yes	String	Project-level token obtained from IAM.

Response Parameters

Status code: 200

Table 4-186 Response body parameters

Parameter	Type	Description
errorCode	String	Error code.
errorMessage	String	Details.
config	PolicyConfig object	Set of policy group attributes.

Table 4-187 PolicyConfig

Parameter	Type	Description
id	String	ID of a policy group attribute.
max_instances	Integer	Maximum number of instances, indicating the upper limit for capacity expansion.
min_instances	Integer	Minimum number of instances, indicating the lower limit for capacity expansion.
cooldown_time	Integer	Cooldown period (unit: s). After an applied policy is executed, the next policy can be executed only after the cooldown period expires.

Example Requests

None

Example Responses

Status code: 200

OK

The request is successful.

```
{
  "errorCode" : "SVCSTG.PE.0",
  "errorMessage" : "",
  "config" : {
    "id" : "f9c7f57e-b1dc-4ef0-a009-ff2848776803",
    "max_instances" : 100,
    "min_instances" : 1,
    "cooldown_time" : 60
  }
}
```


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 authorization information is incorrect or invalid.
403	ForbiddenThe 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**.

4.4 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. 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. The values of category, searchKey, keyWord, startTime, and endTime must be the same as those in the first query. 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.

URI

POST /v1/{project_id}/als/action

Table 4-188 Path Parameters

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

Table 4-189 Query Parameters

Parameter	Mandatory	Type	Description
type	Yes	String	API call mode. When the value is querylogs, this API is used to query logs. Enumeration values: • **querylogs**

Request Parameters

Table 4-190 Request header parameters

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

Table 4-191 Request body parameters

Parameter	Mandatory	Type	Description
category	Yes	String	Log type. Options: app_log: application log node_log: host log custom_log: log in a custom path Enumeration values: • **app_log** • **node_log** • **custom_log**

Parameter	Mandatory	Type	Description
searchKey	No	SearchKey object	Log filter criteria, which vary according to log sources.
keyWord	No	String	1. Exact search by keyword is supported. A keyword is a word 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 include ,'";=()[]{}@&<>/:\n\t\r and spaces.
startTime	Yes	Long	Start time of the query (UTC, in ms).
endTime	Yes	Long	End time of the query (UTC, in ms).
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.
type	No	String	Pagination query. This parameter is not required for the first query, but is required for subsequent pagination queries. Enumeration values: • **next**
pageSize/size	No	Integer	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.

Parameter	Mandatory	Type	Description
hideSyslog	No	Integer	Whether to hide the system log (icagent\kubectl) during the query. 0 (default): Hide. 1: Display. Enumeration values: • **0** • **1**
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) Enumeration values: • **true** • **false**

Table 4-192 SearchKey

Parameter	Mandatory	Type	Description
clusterId	Yes	String	CCE cluster: CCE cluster ID Custom cluster: APM Host log: CONFIG_FILE
nameSpace	No	String	CCE cluster namespace.
appName	No	String	Service name.
podName	No	String	Container instance name.
pathFile	No	String	Log file name.
hostIP	No	String	IP address of the VM where logs are located.

Response Parameters

Status code: 200

Table 4-193 Response body parameters

Parameter	Type	Description
errorCode	String	Response code. SVCSTG.ALS.200200: Success response.
errorMessage	String	Response message.
result	**LogsResults** object	Metadata, including results and the total number of returned records.

Table 4-194 LogsResults

Parameter	Type	Description
total	Integer	Number of records that can be returned.
data	Array of **LogItem** objects	Data array.

Table 4-195 LogItem

Parameter	Type	Description
category	String	Log type.
loghash	String	Hash value of the log source.
clusterId	String	CCE cluster ID.
clusterName	String	CCE cluster name.
nameSpace	String	CCE cluster namespace.
podName	String	CCE container instance name.
appName	String	Service name.
serviceID	String	Service ID of an AOM resource.
containerName	String	CCE container name.
logContent	String	Raw log data.
pathFile	String	Absolute path of a log file.
hostIP	String	IP address of the VM where log files are located.
hostId	String	ID of a host in a cluster.
hostName	String	Name of the VM where log files are located.

Parameter	Type	Description
collectTime	String	Log collection time (UTC time, in ms).
lineNum	String	Sequence number of a log line.
logContentSize	String	Size of a single-line log.

Example Requests

- Query application logs in a cluster.

```
POST https://{Endpoint}/v1/{project_id}/als/action?type=querylogs

{
  "category" : "app_log",
  "searchKey" : {
    "clusterId" : "874819a2-bd6f-11e9-80be-0255ac1001b3"
  },
  "keyWord" : "",
  "startTime" : 1569463658895,
  "endTime" : 1569463958895,
  "pageSize" : 100,
  "hideSyslog" : 0
}
```

- Query data by page.

```
https://{Endpoint}/v1/{project_id}/als/action

{
  "category" : "app_log",
  "searchKey" : {
    "clusterId" : "874819a2-bd6f-11e9-80be-0255ac1001b3"
  },
  "keyWord" : "",
  "startTime" : 1569463658895,
  "endTime" : 1569463958895,
  "lineNum" : "1569463911294010547",
  "type" : "next",
  "size" : 100,
  "hideSyslog" : 0
}
```

Example Responses

Status code: 200

OK

The request is successful.

```
{
  "errorCode" : "SVCSTR.ALS.200200",
  "errorMessage" : "Query data success",
  "result" : {
    "total" : 5000,
    "data" : [ {
      "category" : "app",
      "loghash" : "496b2070d40a83c17f2625401af8a50aadc316f216771fbe38b94d31feaa30eb",
      "clusterId" : "c693fa7c-54cd-11e8-8055-0255ac101e40",
      "clusterName" : "aomdemo",
      "nameSpace" : "default",
      "podName" : "als0712-7c4875f884-q5wwp",
```



```
    "appName" : "als0712",
    "serviceID" : "",
    "containerName" : "container-0",
    "logContent" : "warn:2018/10/09 06:57:01 helloworld.go:108: the main process is running now.n",
    "pathFile" : "/var/paas/sys/log/apm/debug_erro.trace",
    "hostIP" : "192.168.0.133",
    "hostId" : "c11c7211-5a0b-4925-bef4-d078661299b0",
    "hostName" : "192.168.0.133",
    "collectTime" : "1539068233983",
    "lineNum" : "15390682339830002",
    "logContentSize" : "77"
  } ]
 }
}
```


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 authorization information is incorrect or invalid.
403	ForbiddenThe 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 Events/Alarms

4.5.1 Querying Events and Alarms

Function

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

URI

POST /v2/{project_id}/events

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
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, all information that meets the specified search criteria will be returned. Enumeration values: • **history_alert** • **active_alert**

Request Parameters

Table 4-198 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 4-199 Request body parameters

Parameter	Mandatory	Type	Description
time_range	Yes	String	Time range specified for query.Format: start time (UTC, in ms).end time (UTC, in ms).number of minutes in the time period. If both the start time and end time are -1, it indicates the latest N minutes. Time period specified for query. 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 on August 2, 2017.
step	No	Long	Statistical step. For example, if the step is one minute, set this parameter to 60,000.
search	No	String	Field specified for fuzzy query, which can be left blank. If the value is not empty, fuzzy match will be performed. 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 4-200 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 4-201 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. 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 4-202 Response body parameters

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

Table 4-203 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.

Parameter	Type	Description
timeout	Long	Duration at which an alarm is automatically cleared. Unit: ms. For example, if the duration is 1 minute, set this parameter to 60000. The default value is 3 days (that is, 3 days x 24 hours x 60 minutes x 60s x 1000 ms = 259,200,000 ms).
metadata	Map<String,String>	Details of an event or alarm. The value is a key-value pair. A maximum of 30 sub-fields can be extended. 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: type, which is an enumerated value with string elements. Options: event and alarm. - resource_provider: name of the cloud service corresponding to an event, which is a string. - resource_type: resource type corresponding to an event, which is a string. - resource_id: resource information corresponding to the event, which is a string.
annotations	Map<String,String>	Additional field for an event or alarm, which can be left blank.
id	String	Event or alarm ID, which is automatically generated by the system.

Status code: 400

Table 4-204 Response body parameters

Parameter	Type	Description
error_code	String	Response code. Enumeration values: • **AOM.0403**
error_msg	String	Error message. Enumeration values: • **Invalid projectId**
error_type	String	API call failure type. Enumeration values: • **Forbidden**

Status code: 401

Table 4-205 Response body parameters

Parameter	Type	Description
error_code	String	Response code. Enumeration values: • **AOM.0403**
error_msg	String	Error message. Enumeration values: • **Invalid projectId**
error_type	String	API call failure type. Enumeration values: • **Forbidden**

Status code: 403

Table 4-206 Response body parameters

Parameter	Type	Description
error_code	String	Response code. Enumeration values: • **AOM.0403**
error_msg	String	Error message. Enumeration values: • **Invalid projectId**
error_type	String	API call failure type. Enumeration values: • **Forbidden**

Status code: 500

Table 4-207 Response body parameters

Parameter	Type	Description
error_code	String	Response code. Enumeration values: • **AOM.0403**

Parameter	Type	Description
error_msg	String	Error message. Enumeration values: • **Invalid projectId**
error_type	String	API call failure type. Enumeration values: • **Forbidden**

Status code: 503

Table 4-208 Response body parameters

Parameter	Type	Description
error_code	String	Response code. Enumeration values: • **AOM.0403**
error_msg	String	Error message. Enumeration values: • **Invalid projectId**
error_type	String	API call failure type. Enumeration values: • **Forbidden**

Example Requests

Query the events and alarms of a specified user.

```
POST 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 cause",
      "message" : "Alarm details",
      "alarm_fix_suggestion_zh_cn" : "Solution"
    },
    "arrives_at" : 163773632000,
    "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"
    },
    "policy" : { },
    "starts_at" : 16377362908000,
    "timeout" : 60000
  } ],
  "page_info" : {
    "current_count" : 2,
    "next_marker" : "",
    "previous_marker" : ""
  }
}
```


Status code: 400

Bad Request

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


```
{
  "error_code" : "AOM.0400",
  "error_message" : "param error",
  "error_type" : "SC_BAD_REQUEST"
}
```


Status code: 401

Unauthorized

The authentication information is incorrect or invalid.


```
{
  "error_code" : "AOM.0401",
  "error_message" : "you dont have permission",
  "error_type" : "SC_UNAUTHORIZED"
}
```


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" : "you dont have permission",
  "error_type" : "SC_FORBIDDEN"
}
```

Status code: 500

Internal Server Error

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

```
{
  "error_code" : "AOM.0500",
  "error_message" : "SC_INTERNAL_SERVER_ERROR",
  "error_type" : "SC_INTERNAL_SERVER_ERROR"
}
```

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.

Status Code	Description
503	Service Unavailable The requested service is invalid. The client should not repeat the request without modifications.

Error Codes

See **Error Codes**.

4.5.2 Counting Events and Alarms

Function

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

URI

POST /v2/{project_id}/events/statistic

Table 4-209 Path Parameters

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

Table 4-210 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, all information that meets the specified search criteria will be returned. Enumeration values: • **history_alert** • **active_alert**

Request Parameters

Table 4-211 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 4-212 Request body parameters

Parameter	Mandatory	Type	Description
time_range	Yes	String	Time range specified for query.Format: start time (UTC, in ms).end time (UTC, in ms).number of minutes in the time period. If both the start time and end time are -1, it indicates the latest N minutes. Time period specified for query. 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 on August 2, 2017.
step	No	Long	Statistical step. For example, if the 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 4-213 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 4-214 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. 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 4-215 Response body parameters

Parameter	Type	Description
step	Long	Statistical step. For example, if the step is one minute, set this parameter to 60,000.
timestamps	Array of integers	Time series object corresponding to the statistical result.

Parameter	Type	Description
series	Array of **EventSeries** objects	Statistical results of a time series object's different severities of events or alarms.

Table 4-216 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 4-217 Response body parameters

Parameter	Type	Description
error_code	String	Response code. Enumeration values: • **AOM.0403**
error_msg	String	Error message. Enumeration values: • **Invalid projectId**
error_type	String	API call failure type. Enumeration values: • **Forbidden**

Status code: 401

Table 4-218 Response body parameters

Parameter	Type	Description
error_code	String	Response code. Enumeration values: • **AOM.0403**
error_msg	String	Error message. Enumeration values: • **Invalid projectId**
error_type	String	API call failure type. Enumeration values: • **Forbidden**

Status code: 403

Table 4-219 Response body parameters

Parameter	Type	Description
error_code	String	Response code. Enumeration values: • **AOM.0403**
error_msg	String	Error message. Enumeration values: • **Invalid projectId**
error_type	String	API call failure type. Enumeration values: • **Forbidden**

Status code: 500

Table 4-220 Response body parameters

Parameter	Type	Description
error_code	String	Response code. Enumeration values: • **AOM.0403**

Parameter	Type	Description
error_msg	String	Error message. Enumeration values: • **Invalid projectId**
error_type	String	API call failure type. Enumeration values: • **Forbidden**

Status code: 503

Table 4-221 Response body parameters

Parameter	Type	Description
error_code	String	Response code. Enumeration values: • **AOM.0403**
error_msg	String	Error message. Enumeration values: • **Invalid projectId**
error_type	String	API call failure type. Enumeration values: • **Forbidden**

Example Requests

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

```
POST 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" : "Minor",
    "values" : [ 0, 0, 0, 0, 0, 0 ]
```



```
 }, {
   "event_severity" : "Info",
   "values" : [ 0, 0, 0, 0, 0, 0 ]
 } ],
 "step" : 60000,
 "timestamps" : [ 1642820700000, 1642820760000, 1642820820000, 1642820880000, 1642820940000,
1642821000000 ]
}
```

Status code: 400

Bad Request

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

```
{
 "error_code" : "AOM.0400",
 "error_message" : "param error",
 "error_type" : "SC_BAD_REQUEST"
}
```

Status code: 401

Unauthorized

The authentication information is incorrect or invalid.

```
{
 "error_code" : "AOM.0401",
 "error_message" : "you dont have permission",
 "error_type" : "SC_UNAUTHORIZED"
}
```

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" : "you dont have permission",
 "error_type" : "SC_FORBIDDEN"
}
```

Status code: 500

Internal Server Error

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

```
{
 "error_code" : "AOM.0500",
 "error_message" : "SC_INTERNAL_SERVER_ERROR",
 "error_type" : "SC_INTERNAL_SERVER_ERROR"
}
```

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**.

4.5.3 Reporting Events and Alarms

Function

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

URI

PUT /v2/{project_id}/push/events

Table 4-222 Path Parameters

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

Table 4-223 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 4-224 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 4-225 Request body parameters

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

Table 4-226 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 at which an alarm is automatically cleared. Unit: ms. For example, if the duration is 1 minute, set this parameter to 60000. The default value is 3 days (that is, 3 days x 24 hours x 60 minutes x 60s x 1000 ms = 259,200,000 ms).
metadata	No	Map<String,String>	Details of an event or alarm. The value is a key-value pair. A maximum of 30 sub-fields can be extended. 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: type, which is an enumerated value with string elements. Options: event and alarm. - resource_provider: name of the cloud service corresponding to an event, which is a string. - resource_type: resource type corresponding to an event, which is a string. - resource_id: resource information corresponding to the event, which is a string.
annotations	No	Map<String,String>	Additional field for an event or alarm, which can be left blank.

Parameter	Mandatory	Type	Description
id	No	String	Event or alarm ID, which is automatically generated by the system.

Response Parameters

None

Example Requests

Report an alarm named "test".

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

{
  "events" : [ {
    "starts_at" : 1579420868000,
    "ends_at" : 1579420868000,
    "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 cause",
      "alarm_fix_suggestion_zh_cn" : "fix suggestion",
      "message" : "details"
    }
  } ]
}
```

Example Responses

None

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

Error Codes

See **Error Codes**.

4.6 Agent

4.6.1 Querying Agent Information

Function

This API is used to query the Agent information about an account, a cluster, or a namespace.

URI

GET /v1/{project_id}/{cluster_id}/{namespace}/agents

Table 4-227 Path Parameters

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

Table 4-228 Query Parameters

Parameter	Mandatory	Type	Description
offset	No	Integer	Pagination information.
limit	No	Integer	Default value: 1000. Number of records that can be returned.

Request Parameters

Table 4-229 Request header parameters

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

Response Parameters

Status code: 200

Table 4-230 Response body parameters

Parameter	Type	Description
page_info	**PageInfo** object	Metadata, including pagination information.
agent_list	Array of **AgentDetail** objects	Agent list.

Table 4-231 PageInfo

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

Table 4-232 AgentDetail

Parameter	Type	Description
agent_id	String	Agent ID. This parameter is mandatory.
agent_ip	String	Private IP address of the node where the ICAgent is located. This parameter is mandatory.
node_name	String	Name of the node where the ICAgent is located. This parameter is mandatory.
status	String	ICAgent running status. This parameter is mandatory.
last_modified	String	Time when the ICAgent was modified. This parameter is mandatory.
update_time	String	Time when the ICAgent was upgraded. This parameter is mandatory.
agent_version	String	ICAgent version number. This parameter is mandatory.
os_type	String	OS of the node where the ICAgent is located. This parameter is mandatory.

Status code: 400

Table 4-233 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 401

Table 4-234 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 403

Table 4-235 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 500

Table 4-236 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Status code: 503

Table 4-237 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.

Example Requests

Query information about the Agent whose cluster ID is 0f325*******00cb and namespace is default under the 75f54********0cbd0c4 account.

```
GET https://{endpoint}/v1/75f54********0cbd0c4/0f325*******00cb/default/agents?offset=50&limit=789
```

Example Responses

Status code: 200

OK

The request is successful.

```
{
  "page_info" : {
    "count" : 2,
    "offset" : 0,
    "total" : 2
  },
  "agent_list" : [ {
    "agent_ip" : "192.***.***.102",
    "agent_id" : "8977a034********473f6ef642",
    "node_name" : "192.***.***.102",
```



```
    "status" : "uninstall",
    "last_modified" : "",
    "update_time" : "",
    "agent_version" : "",
    "os_type" : ""
  }, {
    "agent_ip" : "192.***.***.133",
    "agent_id" : "6211b62********a6d1389e233",
    "node_name" : "192.***.***.133",
    "status" : "uninstall",
    "last_modified" : "",
    "update_time" : "",
    "agent_version" : "",
    "os_type" : ""
  } ]
}
```


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 authorization 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**.

4.7 Application Discovery Rules

4.7.1 Adding or Modifying Application Discovery Rules

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}/aom/application-discovery-rules

Table 4-238 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 4-239 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 4-240 Request body parameters

Parameter	Mandatory	Type	Description
app_rules	Yes	Array of **AppRuleV1** objects	Application Discovery Rules

Table 4-241 AppRuleV1

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

Parameter	Mandatory	Type	Description
id	Yes	String	Rule ID. When creating an application discovery rule, leave this parameter blank. When modifying an application discovery rule, enter a rule ID.
name	Yes	String	Rule name. The value can contain a maximum of 64 characters. It must start with a lowercase letter and cannot end with a hyphen (-). Only digits, lowercase letters, and hyphens are allowed.
enable	Yes	Boolean	Whether a rule is enabled. Value: true or false.
host_id	No	Array of strings	Host ID (not used currently and can be left empty).
event_name	Yes	String	aom_inventory_rules_event Rule event name. For service discovery, the fixed name is aom_inventory_rules_event.
spec	Yes	**AppRulesSpecV1** object	Additional information.
create_time	No	String	Creation time. When creating an application discovery rule, leave this parameter blank. When modifying an application discovery rule, enter the returned createTime.
desc	No	String	Rule description.

Table 4-242 AppRulesSpecV1

Parameter	Mandatory	Type	Description
app_type	No	String	Service type, which is used only for rule classification and UI display. You can enter any field. For example, enter Java or Python to specify a technology stack. You can also enter collector or database to specify a function.

Parameter	Mandatory	Type	Description
attr_list	No	Array of strings	Attribute list (not used currently and can be left empty).
discovery_rule	Yes	Array of **DiscoveryRuleV1** objects	Discovery rule. When it is an array consisting of multiple conditions, only the processes that meet all the conditions are filtered.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.
name_rule	Yes	**NameRuleV1** object	Naming rules for discovered services and applications.
detect_log	No	String	Whether to enable log collection. Value: true or false
log_file_fix	No	Array of strings	Log file suffix. Value: log, trace, or out
priority	Yes	Integer	Rule priority. Value: 1–9999 (default)

Parameter	Mandatory	Type	Description
is_detect	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. true or false
data_source	No	String	Data source.
editable	No	String	Whether a rule can be modified. If editable is set to "false", the rule is a system rule and cannot be deleted.
is_default_rule	Yes	String	Whether the current rule is the default one. Value: true or false
log_path_rule	No	Array of **NameRuleContent** objects	Log path configuration rule.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.
aom_metric_relabel_configs	No	Array of Map<String,String> objects	Metric configuration.

Table 4-243 DiscoveryRuleV1

Parameter	Mandatory	Type	Description
check_type	Yes	String	Match type. Value: cmdLine, env, or scope
check_mode	Yes	String	Match condition. Value: contain or equals
check_content	Yes	Array of strings	Matched value.

Table 4-244 NameRuleV1

Parameter	Mandatory	Type	Description
app_name_rule	No	Array of **NameRuleContent** objects	Component naming rule.
application_name_rule	No	Array of **NameRuleContent** objects	Application naming rule.
environment	No	Array of **NameRuleContent** objects	Environment information.

Table 4-245 NameRuleContent

Parameter	Mandatory	Type	Description
name_type	No	String	Value type.
args	No	Array of strings	Command.
value	No	Array of strings	Log path.

Response Parameters

Status code: 200

Table 4-246 Response body parameters

Parameter	Type	Description
id	Array of strings	Application discovery rule ID.

Example Requests

Add or modify one or more application discovery rules.

```
PUT https://{Endpoint}/v1/{project_id}/aom/application-discovery-rules

{
  "app_rules" : [ {
    "id" : "44d6c4bb-f673-4bf4-8d33-313832f37b28",
    "name" : "bytest",
    "create_time" : "",
    "project_id" : "5a6036f48e954fcd84d198cb28db311a",
    "enable" : true,
    "host_id" : [ ],
```



```
  "event_name" : "aom_inventory_rules_event",
  "spec" : {
    "detect_log" : "true",
    "log_file_fix" : [ "log", "trace" ],
    "discovery_rule" : [ {
      "check_type" : "cmdLine",
      "check_mode" : "contain",
      "check_content" : [ "default" ]
    }, {
      "check_type" : "scope",
      "check_mode" : "equals",
      "check_content" : [ "44d6c4bb-f673-4bf4-8d33-313832f37b28" ]
    } ],
    "attr_list" : [ "cmdLine" ],
    "is_detect" : "false",
    "priority" : 1,
    "name_rule" : {
      "app_name_rule" : [ {
        "name_type" : "cmdLineHash",
        "args" : [ "00000000001" ],
        "value" : [ "serviceName1" ]
      }, {
        "name_type" : "cmdLine",
        "args" : [ "/var/paas/kubernetes/", "/kubeconfig" ]
      }, {
        "name_type" : "env",
        "args" : [ "APP_NAME" ]
      }, {
        "name_type" : "str",
        "args" : [ "kube" ]
      } ],
      "application_name_rule" : [ {
        "name_type" : "cmdLineHash",
        "args" : [ "00000000001" ],
        "value" : [ "applicationName1" ]
      }, {
        "name_type" : "str",
        "args" : [ "kubeproxy" ]
      } ]
    },
    "app_type" : "",
    "is_default_rule" : "false",
    "log_path_rule" : [ {
      "name_type" : "cmdLineHash",
      "args" : [ "00000000001" ],
      "value" : [ "/xx/xxx/xx.log", "/xx/xxx/xx" ]
    } ]
  }
 } ]
}
```

Example Responses

None

Status Codes

Status Code	Description
200	OK The request is successful.

Status Code	Description
400	Bad Request The client should not repeat the request without modifications.
401	Unauthorized The authentication information is incorrect or invalid.
403	ForbiddenThe 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	Internal Server Error The server has received the request but could not understand it.
503	Service Unavailable The client should not repeat the request without modifications.

Error Codes

See **Error Codes**.

4.7.2 Deleting an Application Discovery Rule

Function

This API is used to delete an application discovery rule.

URI

DELETE /v1/{project_id}/aom/application-discovery-rules

Table 4-247 Path Parameters

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

Table 4-248 Query Parameters

Parameter	Mandatory	Type	Description
app_rules_ids	Yes	Array	Discovery rule ID. Separate IDs by commas (,).

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.

Response Parameters

None

Example Requests

Delete an application discovery rule with a specified ID.

```
DELETE https://{Endpoint}/v1/{project_id}/aom/application-discovery-rules?
app_rules_ids=b788349e-62b2-3c7a-b597-02c611d59801
```

Example Responses

None

Status Codes

Status Code	Description
204	OK The request is successful.
400	Bad Request The client should not repeat the request without modifications.
401	Unauthorized The authentication information is incorrect or invalid.
403	ForbiddenThe 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	Internal Server Error The server has received the request but could not understand it.
503	Service Unavailable The client should not repeat the request without modifications.

Error Codes

See **Error Codes**.

4.7.3 Querying Application Discovery Rules

Function

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

URI

GET /v1/{project_id}/aom/application-discovery-rules

Table 4-250 Path Parameters

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

Table 4-251 Query Parameters

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

Request Parameters

Table 4-252 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 4-253 Response body parameters

Parameter	Type	Description
app_rules	Array of **AppRuleV1** objects	Application Discovery Rules

Table 4-254 AppRuleV1

Parameter	Type	Description
project_id	String	Project ID obtained from IAM. Generally, a project ID contains 32 characters.
id	String	Rule ID. When creating an application discovery rule, leave this parameter blank. When modifying an application discovery rule, enter a rule ID.
name	String	Rule name. The value can contain a maximum of 64 characters. It must start with a lowercase letter and cannot end with a hyphen (-). Only digits, lowercase letters, and hyphens are allowed.
enable	Boolean	Whether a rule is enabled. Value: true or false.
host_id	Array of strings	Host ID (not used currently and can be left empty).
event_name	String	aom_inventory_rules_event Rule event name. For service discovery, the fixed name is aom_inventory_rules_event.
spec	**AppRulesSpecV1** object	Additional information.
create_time	String	Creation time. When creating an application discovery rule, leave this parameter blank. When modifying an application discovery rule, enter the returned createTime.
desc	String	Rule description.

Table 4-255 AppRulesSpecV1

Parameter	Type	Description
app_type	String	Service type, which is used only for rule classification and UI display. You can enter any field. For example, enter Java or Python to specify a technology stack. You can also enter collector or database to specify a function.
attr_list	Array of strings	Attribute list (not used currently and can be left empty).
discovery_rule	Array of **DiscoveryRuleV1** objects	Discovery rule. When it is an array consisting of multiple conditions, only the processes that meet all the conditions are filtered.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.
name_rule	**NameRuleV1** object	Naming rules for discovered services and applications.
detect_log	String	Whether to enable log collection. Value: true or false
log_file_fix	Array of strings	Log file suffix. Value: log, trace, or out
priority	Integer	Rule priority. Value: 1–9999 (default)
is_detect	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. true or false
data_source	String	Data source.
editable	String	Whether a rule can be modified. If editable is set to "false", the rule is a system rule and cannot be deleted.

Parameter	Type	Description
is_default_rule	String	Whether the current rule is the default one. Value: true or false
log_path_rule	Array of **NameRuleContent** objects	Log path configuration rule.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.
aom_metric_relabel_configs	Array of Map<String,String> objects	Metric configuration.

Table 4-256 DiscoveryRuleV1

Parameter	Type	Description
check_type	String	Match type. Value: cmdLine, env, or scope
check_mode	String	Match condition. Value: contain or equals
check_content	Array of strings	Matched value.

Table 4-257 NameRuleV1

Parameter	Type	Description
app_name_rule	Array of **NameRuleContent** objects	Component naming rule.
application_name_rule	Array of **NameRuleContent** objects	Application naming rule.
environment	Array of **NameRuleContent** objects	Environment information.

Table 4-258 NameRuleContent

Parameter	Type	Description
name_type	String	Value type.
args	Array of strings	Command.
value	Array of strings	Log path.

Example Requests

Query application discovery rules.

```
GET https://{Endpoint}/v1/{project_id}/aom/application-discovery-rules
```

Example Responses

Status code: 200

OK

The request is successful.

```
{
  "app_rules" : [ {
    "create_time" : "1599098476654",
    "enable" : true,
    "name" : "ica**nt",
    "event_name" : "aom_in***tory_rules_event",
    "host_id" : [ ],
    "id" : "b53a5152-****-****-****-302367e04c0b",
    "project_id" : "2a473356c**********be891bffc1cf",
    "spec" : {
      "detect_log" : "true",
      "editable" : null,
      "log_path_rule" : [ ],
      "priority" : 9999,
      "attr_list" : [ "cmdLine" ],
      "name_rule" : {
        "app_name_rule" : [ {
          "name_type" : "cmdLineHash",
          "args" : [ "/opt/******** -DNFW=ica**nt" ],
          "value" : [ "aicagentserver" ]
        } ],
        "application_name_rule" : [ {
          "name_type" : "cmdLineHash",
          "args" : [ "/opt/********** -DNFW=ica**nt" ],
          "value" : [ "aica**nt" ]
        } ]
      },
      "app_type" : "",
      "aom_metric_relabel_configs" : null,
      "log_file_fix" : [ "log", "trace", "out" ],
      "is_detect" : "false",
      "is_default_rule" : null,
      "data_source" : null,
      "discovery_rule" : [ {
        "check_type" : "cmdLine",
        "check_content" : [ "-DNFW=ica**nt" ],
        "check_mode" : "contain"
```



```
    } ]
   },
   "desc" : null
  } ]
}
```

Status Codes

Status Code	Description
200	OK The request is successful.
400	Bad Request The client should not repeat the request without modifications.
401	Unauthorized The authentication information is incorrect or invalid.
403	ForbiddenThe 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	Internal Server Error The server has received the request but could not understand it.
503	Service Unavailable The client should not repeat the request without modifications.

Error Codes

See **Error Codes**.

4.8 Prometheus Monitoring

4.8.1 Querying Expression Calculation Results in a Specified Period

Function

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

URI

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

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
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 4-261 Request header parameters

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

Response Parameters

Status code: 200

Table 4-262 Response body parameters

Parameter	Type	Description
status	String	Response status.
data	**Data** object	Response data.

Table 4-263 Data

Parameter	Type	Description
resultType	String	Type of the returned value.
result	Array of objects	Data information.

Status code: 400

Table 4-264 Response body parameters

Parameter	Type	Description
status	String	Response status.
errorType	String	Error type.
error	String	Error message.

Status code: 403

Table 4-265 Response body parameters

Parameter	Type	Description
status	String	Response status.
errorType	String	Error type.
error	String	Error message.

Status code: 422

Table 4-266 Response body parameters

Parameter	Type	Description
status	String	Response status.
errorType	String	Error type.
error	String	Error message.

Status code: 503

Table 4-267 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

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

Invalid request. Parameters are incorrect or missing. The client should not repeat the request without modifications.

```
{
  "status" : "error",
  "errorType" : "bad_param",
  "error" : "param is invalid."
}
```

Status code: 403

Access denied.

```
{
  "status" : "error",
  "errorType" : "auth",
  "error" : "auth project_id not pass."
}
```

Status code: 422

The expression cannot be executed.

```
{
  "status" : "error",
  "errorType" : "excution",
  "error" : "expression can't be executed."
}
```

Status code: 503

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	The request is successful.
400	Invalid request. Parameters are incorrect or missing. The client should not repeat the request without modifications.
403	Access denied.
422	The expression cannot be executed.
503	The requested service is invalid. The client should not repeat the request without modifications.

Error Codes

See **Error Codes**.

4.8.2 Querying the Expression Calculation Result at a Specified Time Point

Function

This API is used to query the calculation result of a PromQL expression at a specified time point.

URI

POST /v1/{project_id}/aom/api/v1/query

Table 4-268 Path Parameters

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

Table 4-269 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 4-270 Request header parameters

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

Response Parameters

Status code: 200

Table 4-271 Response body parameters

Parameter	Type	Description
status	String	Response status.
data	**Data** object	Response data.

Table 4-272 Data

Parameter	Type	Description
resultType	String	Type of the returned value.
result	Array of objects	Data information.

Status code: 400

Table 4-273 Response body parameters

Parameter	Type	Description
status	String	Response status.
errorType	String	Error type.
error	String	Error message.

Status code: 403

Table 4-274 Response body parameters

Parameter	Type	Description
status	String	Response status.
errorType	String	Error type.
error	String	Error message.

Status code: 422

Table 4-275 Response body parameters

Parameter	Type	Description
status	String	Response status.
errorType	String	Error type.
error	String	Error message.

Status code: 503

Table 4-276 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

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

Invalid request. Parameters are incorrect or missing. The client should not repeat the request without modifications.

```
{
  "status" : "error",
  "errorType" : "bad_param",
  "error" : "param is invalid."
}
```

Status code: 403

Access denied.


```
{
  "status" : "error",
  "errorType" : "auth",
  "error" : "auth project_id not pass."
}
```

Status code: 422

The expression cannot be executed.

```
{
  "status" : "error",
  "errorType" : "excution",
  "error" : "expression can't be executed."
}
```

Status code: 503

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	The request is successful.
400	Invalid request. Parameters are incorrect or missing. The client should not repeat the request without modifications.
403	Access denied.
422	The expression cannot be executed.
503	The requested service is invalid. The client should not repeat the request without modifications.

Error Codes

See **Error Codes**.

4.8.3 Querying Tag Values

Function

This API is used to query the values of a specified tag.

URI

GET /v1/{project_id}/aom/api/v1/label/{label_name}/values

Table 4-277 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 4-278 Request header parameters

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

Response Parameters

Status code: 200

Table 4-279 Response body parameters

Parameter	Type	Description
status	String	Response status.
data	Array of strings	Tag value.

Status code: 400

Table 4-280 Response body parameters

Parameter	Type	Description
status	String	Response status.
errorType	String	Error type.
error	String	Error message.

Status code: 403

Table 4-281 Response body parameters

Parameter	Type	Description
status	String	Response status.
errorType	String	Error type.
error	String	Error message.

Status code: 422

Table 4-282 Response body parameters

Parameter	Type	Description
status	String	Response status.
errorType	String	Error type.
error	String	Error message.

Status code: 503

Table 4-283 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

{
  "status" : "success",
  "data" : [ "node", "prometheus" ]
}
```

Example Responses

Status code: 200

The request is successful.

```
{
  "status" : "success",
```



```
  "data" : [ "node", "prometheus" ]
}
```

Status code: 400

Invalid request. Parameters are incorrect or missing. The client should not repeat the request without modifications.

```
{
  "status" : "error",
  "errorType" : "bad_param",
  "error" : "param is invalid."
}
```

Status code: 403

Access denied.

```
{
  "status" : "error",
  "errorType" : "auth",
  "error" : "auth project_id not pass."
}
```

Status code: 422

The expression cannot be executed.

```
{
  "status" : "error",
  "errorType" : "excution",
  "error" : "expression can't be executed."
}
```

Status code: 503

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	The request is successful.
400	Invalid request. Parameters are incorrect or missing. The client should not repeat the request without modifications.
403	Access denied.
422	The expression cannot be executed.
503	The requested service is invalid. The client should not repeat the request without modifications.

Error Codes

See **Error Codes**.

4.8.4 Obtaining the Tag Name List

Function

This API is used to obtain the tag name list.

URI

POST /v1/{project_id}/aom/api/v1/labels

Table 4-284 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 4-285 Request header parameters

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

Response Parameters

Status code: 200

Table 4-286 Response body parameters

Parameter	Type	Description
status	String	Response status.
data	Array of strings	Tag value.

Status code: 400

Table 4-287 Response body parameters

Parameter	Type	Description
status	String	Response status.
errorType	String	Error type.
error	String	Error message.

Status code: 403

Table 4-288 Response body parameters

Parameter	Type	Description
status	String	Response status.
errorType	String	Error type.
error	String	Error message.

Status code: 422

Table 4-289 Response body parameters

Parameter	Type	Description
status	String	Response status.
errorType	String	Error type.
error	String	Error message.

Status code: 503

Table 4-290 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

{
  "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" ]
}
```

Example Responses

Status code: 200

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

Invalid request. Parameters are incorrect or missing. The client should not repeat the request without modifications.

```
{
  "status" : "error",
  "errorType" : "bad_param",
  "error" : "param is invalid."
}
```

Status code: 403

Access denied.

```
{
  "status" : "error",
  "errorType" : "auth",
  "error" : "auth project_id not pass."
}
```

Status code: 422

The expression cannot be executed.

```
{
  "status" : "error",
  "errorType" : "excution",
  "error" : "expression can't be executed."
}
```

Status code: 503

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	The request is successful.
400	Invalid request. Parameters are incorrect or missing. The client should not repeat the request without modifications.
403	Access denied.
422	The expression cannot be executed.
503	The requested service is invalid. The client should not repeat the request without modifications.

Error Codes

See **Error Codes**.

4.8.5 Querying Metadata

Function

This API is used to query the metadata of time series and corresponding tags.

URI

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

Table 4-291 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 4-292 Request header parameters

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

Response Parameters

Status code: 200

Table 4-293 Response body parameters

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

Status code: 400

Table 4-294 Response body parameters

Parameter	Type	Description
status	String	Response status.
errorType	String	Error type.
error	String	Error message.

Status code: 403

Table 4-295 Response body parameters

Parameter	Type	Description
status	String	Response status.
errorType	String	Error type.
error	String	Error message.

Status code: 422

Table 4-296 Response body parameters

Parameter	Type	Description
status	String	Response status.
errorType	String	Error type.
error	String	Error message.

Status code: 503

Table 4-297 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/metadata
```

Example Responses

Status code: 200

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

Invalid request. Parameters are incorrect or missing. The client should not repeat the request without modifications.

```
{
  "status" : "error",
  "errorType" : "bad_param",
  "error" : "param is invalid."
}
```

Status code: 403

Access denied.

```
{
  "status" : "error",
  "errorType" : "auth",
  "error" : "auth project_id not pass."
}
```

Status code: 422

The expression cannot be executed.

```
{
  "status" : "error",
  "errorType" : "excution",
```



```
  "error" : "expression can't be executed."
}
```

Status code: 503

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	The request is successful.
400	Invalid request. Parameters are incorrect or missing. The client should not repeat the request without modifications.
403	Access denied.
422	The expression cannot be executed.
503	The requested service is invalid. The client should not repeat the request without modifications.

Error Codes

See **Error Codes**.

4.8.6 Querying the Calculation Results of a PromQL Expression in a Specified Period Based on Prometheus Instance

Function

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

URI

POST /v1/{project_id}/{prometheus_instance}/aom/api/v1/query_range

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.
prometheus_instance	Yes	String	Prometheus instance ID.

Table 4-299 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, in seconds).
end	Yes	String	End timestamp (Unix, in seconds).
step	Yes	String	Query step (in seconds). The task is executed on the step basis within the specified period.

Request Parameters

Table 4-300 Request header parameters

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

Response Parameters

Status code: 200

Table 4-301 Response body parameters

Parameter	Type	Description
status	String	Response status.
data	**Data** object	Response data.

Table 4-302 Data

Parameter	Type	Description
resultType	String	Type of the returned value.
result	Array of objects	Data information.

Status code: 400

Table 4-303 Response body parameters

Parameter	Type	Description
status	String	Response status.
errorType	String	Error type.
error	String	Error message.

Status code: 403

Table 4-304 Response body parameters

Parameter	Type	Description
status	String	Response status.
errorType	String	Error type.
error	String	Error message.

Status code: 422

Table 4-305 Response body parameters

Parameter	Type	Description
status	String	Response status.

Parameter	Type	Description
errorType	String	Error type.
error	String	Error message.

Status code: 503

Table 4-306 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

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

Invalid request. Parameters are incorrect or missing. The client should not repeat the request without modifications.

```
{
  "status" : "error",
  "errorType" : "bad_param",
  "error" : "param is invalid."
}
```

Status code: 403

Access denied.

```
{
  "status" : "error",
  "errorType" : "auth",
  "error" : "auth project_id not pass."
}
```

Status code: 422

The expression cannot be executed.

```
{
  "status" : "error",
  "errorType" : "excution",
  "error" : "expression can't be executed."
}
```

Status code: 503

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	The request is successful.
400	Invalid request. Parameters are incorrect or missing. The client should not repeat the request without modifications.
403	Access denied.
422	The expression cannot be executed.
503	The requested service is invalid. The client should not repeat the request without modifications.

Error Codes

See **Error Codes**.

4.8.7 Querying the Calculation Result of a PromQL Expression at a Specified Time Point Based on Prometheus Instance

Function

This API is used to query the calculation result of a PromQL expression at a specified time point.

URI

POST /v1/{project_id}/{prometheus_instance}/aom/api/v1/query

Table 4-307 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.

Table 4-308 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, in seconds).

Request Parameters

Table 4-309 Request header parameters

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

Response Parameters

Status code: 200

Table 4-310 Response body parameters

Parameter	Type	Description
status	String	Response status.
data	**Data** object	Response data.

Table 4-311 Data

Parameter	Type	Description
resultType	String	Type of the returned value.
result	Array of objects	Data information.

Status code: 400

Table 4-312 Response body parameters

Parameter	Type	Description
status	String	Response status.
errorType	String	Error type.
error	String	Error message.

Status code: 403

Table 4-313 Response body parameters

Parameter	Type	Description
status	String	Response status.
errorType	String	Error type.
error	String	Error message.

Status code: 422

Table 4-314 Response body parameters

Parameter	Type	Description
status	String	Response status.
errorType	String	Error type.
error	String	Error message.

Status code: 503

Table 4-315 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

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

Invalid request. Parameters are incorrect or missing. The client should not repeat the request without modifications.

```
{
  "status" : "error",
  "errorType" : "bad_param",
  "error" : "param is invalid."
}
```

Status code: 403

Access denied.

```
{
  "status" : "error",
  "errorType" : "auth",
  "error" : "auth project_id not pass."
}
```

Status code: 422

The expression cannot be executed.

```
{
  "status" : "error",
  "errorType" : "excution",
  "error" : "expression can't be executed."
}
```

Status code: 503

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	The request is successful.
400	Invalid request. Parameters are incorrect or missing. The client should not repeat the request without modifications.
403	Access denied.
422	The expression cannot be executed.
503	The requested service is invalid. The client should not repeat the request without modifications.

Error Codes

See **Error Codes**.

4.8.8 Querying the Values of a Tag Based on Prometheus Instance

Function

This API is used to query the values of a specified tag.

URI

GET /v1/{project_id}/{prometheus_instance}/aom/api/v1/label/{label_name}/values

Table 4-316 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.
label_name	Yes	String	Tag specified for query.

Request Parameters

Table 4-317 Request header parameters

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

Response Parameters

Status code: 200

Table 4-318 Response body parameters

Parameter	Type	Description
status	String	Response status.

Parameter	Type	Description
data	Array of strings	Tag value.

Status code: 400

Table 4-319 Response body parameters

Parameter	Type	Description
status	String	Response status.
errorType	String	Error type.
error	String	Error message.

Status code: 403

Table 4-320 Response body parameters

Parameter	Type	Description
status	String	Response status.
errorType	String	Error type.
error	String	Error message.

Status code: 422

Table 4-321 Response body parameters

Parameter	Type	Description
status	String	Response status.
errorType	String	Error type.
error	String	Error message.

Status code: 503

Table 4-322 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

{
  "status" : "success",
  "data" : [ "node", "prometheus" ]
}
```

Example Responses

Status code: 200

The request is successful.

```
{
  "status" : "success",
  "data" : [ "node", "prometheus" ]
}
```

Status code: 400

Invalid request. Parameters are incorrect or missing. The client should not repeat the request without modifications.

```
{
  "status" : "error",
  "errorType" : "bad_param",
  "error" : "param is invalid."
}
```

Status code: 403

Access denied.

```
{
  "status" : "error",
  "errorType" : "auth",
  "error" : "auth project_id not pass."
}
```

Status code: 422

The expression cannot be executed.

```
{
  "status" : "error",
  "errorType" : "excution",
  "error" : "expression can't be executed."
}
```

Status code: 503

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	The request is successful.
400	Invalid request. Parameters are incorrect or missing. The client should not repeat the request without modifications.
403	Access denied.
422	The expression cannot be executed.
503	The requested service is invalid. The client should not repeat the request without modifications.

Error Codes

See **Error Codes**.

4.8.9 Obtaining the Tag Name List Based on Prometheus Instance

Function

This API is used to obtain the tag name list.

URI

POST /v1/{project_id}/{prometheus_instance}/aom/api/v1/labels

Table 4-323 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 4-324 Request header parameters

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

Response Parameters

Status code: 200

Table 4-325 Response body parameters

Parameter	Type	Description
status	String	Response status.
data	Array of strings	Tag value.

Status code: 400

Table 4-326 Response body parameters

Parameter	Type	Description
status	String	Response status.
errorType	String	Error type.
error	String	Error message.

Status code: 403

Table 4-327 Response body parameters

Parameter	Type	Description
status	String	Response status.
errorType	String	Error type.
error	String	Error message.

Status code: 422

Table 4-328 Response body parameters

Parameter	Type	Description
status	String	Response status.
errorType	String	Error type.
error	String	Error message.

Status code: 503

Table 4-329 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

{
  "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" ]
}
```

Example Responses

Status code: 200

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

Invalid request. Parameters are incorrect or missing. The client should not repeat the request without modifications.

```
{
  "status" : "error",
  "errorType" : "bad_param",
```



```
  "error" : "param is invalid."
}
```

Status code: 403

Access denied.

```
{
  "status" : "error",
  "errorType" : "auth",
  "error" : "auth project_id not pass."
}
```

Status code: 422

The expression cannot be executed.

```
{
  "status" : "error",
  "errorType" : "excution",
  "error" : "expression can't be executed."
}
```

Status code: 503

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	The request is successful.
400	Invalid request. Parameters are incorrect or missing. The client should not repeat the request without modifications.
403	Access denied.
422	The expression cannot be executed.
503	The requested service is invalid. The client should not repeat the request without modifications.

Error Codes

See **Error Codes**.

4.8.10 Querying Metadata Based on Prometheus Instance

Function

This API is used to query the metadata of time series and corresponding tags.

URI

GET /v1/{project_id}/{prometheus_instance}/aom/api/v1/metadata

Table 4-330 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 4-331 Request header parameters

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

Response Parameters

Status code: 200

Table 4-332 Response body parameters

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

Status code: 400

Table 4-333 Response body parameters

Parameter	Type	Description
status	String	Response status.
errorType	String	Error type.
error	String	Error message.

Status code: 403

Table 4-334 Response body parameters

Parameter	Type	Description
status	String	Response status.
errorType	String	Error type.
error	String	Error message.

Status code: 422

Table 4-335 Response body parameters

Parameter	Type	Description
status	String	Response status.
errorType	String	Error type.
error	String	Error message.

Status code: 503

Table 4-336 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

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

Invalid request. Parameters are incorrect or missing. The client should not repeat the request without modifications.

```
{
 "status" : "error",
 "errorType" : "bad_param",
 "error" : "param is invalid."
}
```

Status code: 403

Access denied.

```
{
 "status" : "error",
 "errorType" : "auth",
 "error" : "auth project_id not pass."
}
```

Status code: 422

The expression cannot be executed.

```
{
 "status" : "error",
 "errorType" : "excution",
 "error" : "expression can't be executed."
}
```

Status code: 503

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	The request is successful.
400	Invalid request. Parameters are incorrect or missing. The client should not repeat the request without modifications.
403	Access denied.
422	The expression cannot be executed.

Status Code	Description
503	The requested service is invalid. The client should not repeat the request without modifications.

Error Codes

See **Error Codes**.

5 Appendix

5.1 Status Codes

Table 5-1 describes the status codes.

Table 5-1 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.

Status Code	Message	Description
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.
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.

Status Code	Message	Description
303	See Other	The response to the request can be found under a different URI, and 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.

Status Code	Message	Description
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.
422	Unprocessable Entity	The request is well-formed but is unable to be processed due to semantic errors.

Status Code	Message	Description
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.

5.2 Error Codes

If an error occurs in API calling, no result is returned. Identify the causes of errors based on the error codes of each API. If an error occurs in API calling, HTTP status code 4xx or 5xx is returned. The response body contains the specific error code and information. If you are unable to identify the cause of an error, contact technical support and provide the error code to solve the problem.

Format of an Error Response Body

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.

Error Code Description

Error Code	Message	Solution
SVCSTG_AMS_2000000	Successful operation.	No action is required after the request is executed.
SVCSTG_AMS_4000001	Invalid request parameter.	Check whether parameters meet requirements.
SVCSTG_AMS_4000002	Invalid namespace.	Check whether parameters meet requirements.
SVCSTG_AMS_4000003	Dimensions are left blank.	Check whether parameters meet requirements.
SVCSTG_AMS_4000005	Invalid metric data type.	Check whether parameters meet requirements.
SVCSTG_AMS_4000006	The metric data value is left blank.	Check whether parameters meet requirements.
SVCSTG_AMS_4000007	Invalid name or value length in the dimension.	Check whether parameters meet requirements.
SVCSTG_AMS_4000008	The request exceeds 40 KB.	Check whether parameters meet requirements.
SVCSTG_AMS_4000009	A metric supports a maximum of 20 dimensions.	Check whether parameters meet requirements.
SVCSTG_AMS_4000010	Invalid collection time.	Check whether parameters meet requirements.

Error Code	Message	Solution
SVCSTG_AMS_4000101	Invalid namespace.	Check whether parameters meet requirements.
SVCSTG_AMS_4000101	Projectid is left blank.	Check whether parameters meet requirements.
SVCSTG_AMS_4000101	Invalid alarm name.	Check whether parameters meet requirements.
SVCSTG_AMS_4000102	Invalid inventoryId.	Check whether parameters meet requirements.
SVCSTG_AMS_4000102	The metric data parameter is null.	Check whether parameters meet requirements.
SVCSTG_AMS_4000102	The threshold rule name already exists.	Use another name.
SVCSTG_AMS_4000103	ProjectId is left blank.	Check whether parameters meet requirements.
SVCSTG_AMS_4000103	Invalid period.	Check whether parameters meet requirements.
SVCSTG_AMS_4000103	Invalid alarm description.	Check whether parameters meet requirements.
SVCSTG_AMS_4000104	Invalid statistics.	Check whether parameters meet requirements.
SVCSTG_AMS_4000104	Invalid alarm threshold.	Check whether parameters meet requirements.
SVCSTG_AMS_4000105	Invalid limit.	Check whether parameters meet requirements.
SVCSTG_AMS_4000105	Invalid metric.	Check whether parameters meet requirements.
SVCSTG_AMS_4000105	Invalid alarm period.	Check whether parameters meet requirements.
SVCSTG_AMS_4000106	Invalid start.	Check whether parameters meet requirements.
SVCSTG_AMS_4000106	Invalid time range.	Check whether parameters meet requirements.
SVCSTG_AMS_4000106	Invalid email list.	Check whether parameters meet requirements.
SVCSTG_AMS_4000107	The number of data points in a time range exceeds 1440.	Check whether parameters meet requirements.

Error Code	Message	Solution
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 parameters meet requirements.
SVCSTG_AMS_4000109	Invalid metricName.	Check whether parameters meet requirements.
SVCSTG_AMS_4000109	Invalid project ID.	Check whether parameters meet requirements.
SVCSTG_AMS_4000110	Invalid fillValue.	Check whether parameters meet requirements.
SVCSTG_AMS_4000110	Invalid limit.	Check whether parameters meet requirements.
SVCSTG_AMS_4000111	Invalid start.	Check whether parameters meet requirements.
SVCSTG_AMS_4000114	Invalid dimensions.	Check whether parameters meet requirements.
SVCSTG_AMS_4000115	Invalid request parameter.	Check whether parameters meet requirements.
SVCSTG_AMS_4000116	The dimensions and metricName cannot be empty at the same time.	Check whether parameters meet requirements.
SVCSTG_AMS_4000118	Invalid number of consecutive periods.	Check whether parameters meet requirements.
SVCSTG_AMS_4000119	Invalid alarm statistic.	Check whether parameters meet requirements.
SVCSTG_AMS_4000120	Invalid alarm comparison operator.	Check whether parameters meet requirements.
SVCSTG_AMS_4000121	The alarm does not exist.	Check whether the threshold rule exists.
SVCSTG_AMS_5000000	Internal server error.	Contact technical support.
SVCSTG_AMS_5030001	The Cassandra session is null.	Contact technical support.
SVCSTG_AMS_5030002	The Cassandra execution is abnormal.	Contact technical support.
SVCSTG_AMS_4001019	Parameter verification failed.	Contact technical support.

Error Code	Message	Solution
SVCSTG_AMS_4001020	Invalid request parameter.	Check parameters.
AOM.0400	Invalid request parameter.	Check parameters.
AOM.0401	Invalid authentication information.	Check whether parameters meet requirements.
AOM.0403	Forbidden	Use an authorized account.
AOM.0500	Internal server error.	Contact technical support.
AOM.0503	Failed to query event alarms.	Contact technical support.
SVCSTG.INV.2000000	The request is successful.	No action is required after the request is executed.
SVCSTG.INV.4000115	Invalid request parameter.	Check whether parameters meet requirements.
SVCSTG.INV.4030000	Forbidden	Use an authorized account.
SVCSTG.INV.5000001	The Elasticsearch session is null.	Contact technical support.
SVCSTG.INV.5000002	The Elasticsearch execution is abnormal.	Contact technical support.
SVCSTG.INV.5000003	The call ICMGR is abnormal.	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.
SVCSTG.PE.4001101	Invalid deployment name.	Check whether parameters meet requirements.
SVCSTG.PE.40031002	Deployment name authentication failed.	Change the workload name to the name of an existing workload for which a scaling rule needs to be created.
SVCSTG.PE.4031012	Failed to verify the project ID.	Check whether parameters meet requirements.
SVCSTG.PE.4033008	Failed to update the scheduled or periodic policy.	Check whether parameters meet requirements.
SVCSTG.PE.5001201	Failed to insert or update data in the background.	Contact technical support.

Error Code	Message	Solution
SVCSTG.PE.5001203	Query error.	Contact technical support.
SVCSTG.PE.5001205	Failed to delete records.	Contact technical support.
SVCSTG.PE.5003007	Failed to update the threshold rule.	Contact technical support.
SVCSTG.PE.4041202	Record query failed.	Contact technical support.
SVCSTR.ALS.200200	Logs successfully queried.	No action is required after the request is executed.
SVCSTG.ALS.200.200	Successful query.	-
SVCSTG.ALS.200.201	The maximum length of parameter %s exceeds %s. %s is empty. %s is incorrect.	Check whether parameters meet requirements.
SVCSTG.ALS.200.203	Failed to query logs.	Check whether parameters meet requirements.
SVCSTG.ALS.403.105	Invalid project ID.	Check whether the URL project_id and token project_id are the same.
APM.ICMGR.2001401	Insufficient permissions.	Contact technical support.
AOM.02002010	The alarm rule does not exist.	Check whether the alarm rule exists.

5.3 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 Click the username in the upper right corner, and choose **My Credentials**.

Step 3 On the **My Credentials** page, view the username, user ID, project name, and project ID.

----End

A Change History

Table A-1 Change history

Released On	Description
2024-04-15	This issue is the first official release.

