Cloud Eye API Reference-24.9.0

Issue 01

Date 2025-09-09

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.

Contents

1 Before You Start

Welcome to *Cloud Eye API Reference*. Cloud Eye is a multi-dimensional resource monitoring platform. Customers can use Cloud Eye to monitor the utilization of service resources, track the status of cloud services, configure alarm rules and notifications, and quickly respond to resource changes.

This document describes how to use application programming interfaces (APIs) to perform operations on metrics, alarm rules, and monitoring data, such as querying the metric list and the alarm rule list, creating alarm rules, and deleting alarm rules. For details about all supported operations, see **API Overview**.

If you plan to access Cloud Eye through an API, ensure that you are familiar with Cloud Eye concepts. For details, see **What Is Cloud Eye?**

API Calling

Cloud Eye supports Representational State Transfer (REST) APIs, allowing you to call APIs using HTTPS. For details about API calling, see **Calling APIs**.

Additionally, Cloud Eye offers software development kits (SDKs) of multiple programming languages. For details about how to use SDKs, see **Huawei Cloud SDKs**.

Endpoints

An endpoint is the **request address** for calling an API. Endpoints vary depending on services and regions. For the endpoints of all services, see **Regions and Endpoints**.

Constraints

- The number of alarm rules that you can create is determined by your quota. To view or increase the quota, see **Quota Adjustment**.
- For more constraints, see API description.

Concepts

- Account

  An account is created upon successful signing up. The account has full access permissions for all of its cloud services and resources. It can be used to reset

user passwords and grant user permissions. The account is a payment entity, which should not be used directly to perform routine management. For security purposes, create Identity and Access Management (IAM) users and grant them permissions for routine management.

- User

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

  API authentication requires information such as the account name, username, and password.

- Region

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

  For details, see **Region and AZ**.

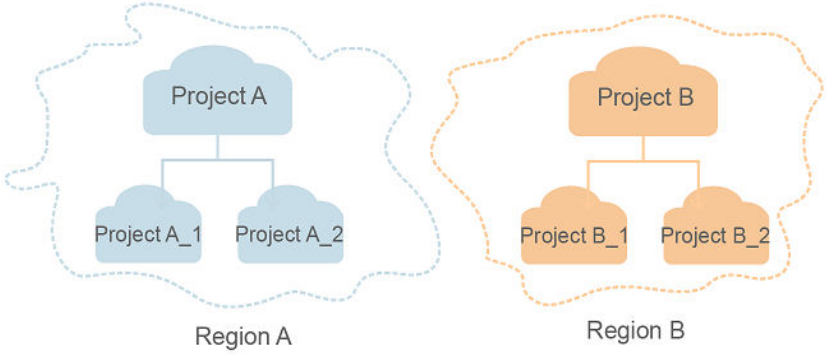
- AZ

  An AZ comprises of one or more physical data centers equipped with independent ventilation, fire, water, and electricity facilities. Computing, network, storage, and other resources in an AZ are logically divided into multiple clusters. AZs within a region are interconnected using high-speed optical fibers to allow you to build cross-AZ high-availability systems.

- Project

  A project corresponds to a region. Default projects are defined to group and physically isolate resources (including computing, storage, and network resources) across regions. Users can be granted permissions in a default project to access all resources under their accounts in the region associated with the project. If you need more refined access control, create subprojects under a default project and create resources in subprojects. Then you can assign users the permissions required to access only the resources in the specific subprojects.

  Figure 1-1 Project isolation model

- Enterprise Project

  Enterprise projects group and manage resources across regions. Resources in different enterprise projects are logically isolated. An enterprise project can

contain resources of multiple regions, and resources can be added to or removed from enterprise projects.

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

2 API Overview

Cloud Eye APIs allow you to use all Cloud Eye functions. For example, you can query the metric list and create alarm rules.

Table 2-1 API description

Type	Subtype	API	Description
API V1	API Version Management	**Querying All API Versions**	Query all API versions supported by Cloud Eye.
		Querying a Specified API Version	Query a specified API version of Cloud Eye.
	Metric Management	**Querying Metrics**	Query metrics supported by Cloud Eye.
	Alarm Rules	**Querying Alarm Rules**	Query alarm rules.
		Querying Details of an Alarm Rule	Query details of an alarm rule based on its ID.
		Enabling or Disabling an Alarm Rule	Enable or disable an alarm rule based on the alarm rule ID.
		Deleting an Alarm Rule	Delete an alarm rule based on its ID.
		Creating an Alarm Rule	Create an alarm rule.
		Creating a Custom Alarm Template	Create a custom alarm template to add an alarm rule for one or more metrics.

Type	Subtype	API	Description
		Deleting a Custom Alarm Template	Delete a custom alarm template.
		Querying the Alarm History of an Alarm Rule	Query the alarm history of an alarm rule based on its ID.
		Querying Custom Alarm Templates	Query the list of custom alarm templates.
		Updating a Custom Alarm Template	Update a custom alarm template.
		Modifying an Alarm Rule	Modify an alarm rule.
	Monitoring Data Management	Querying Monitoring Data of a Metric	Query the monitoring data of a metric at a specified granularity in a specified time range.
		Adding Monitoring Data	Add one or more pieces of metric data.
		Querying Monitoring Data of Multiple Metrics	Batch query data of a specified metric at a specified granularity in a specified time range.
		Querying the Host Configuration	Query the server configuration for a specified event type in a specified time range. You can specify the dimension of data to be queried.
	Quota Management	Querying Quotas	Query the alarm rule quota.
	Resource Groups	Querying Resources in a Resource Group	Query resources in resource groups by resource group ID.
		Creating a Resource Group	Create a resource group. You can use resource groups to manage resources by service, and view monitoring and alarm information by group to ease O&M.

Type	Subtype	API	Description
		Updating a Resource Group	Update a resource group. You can use resource groups to manage resources by service, and view monitoring and alarm information by group to ease O&M.
		Deleting a Resource Group	Delete a resource group.
		Query Resource Groups	Query all resource groups you created.
	Event Monitoring	Reporting Events	Report custom events.
		Querying Events	Query events, including system events and custom events.
		Querying Details of an Event	Query details of an event based on its name.
API V2	Alarm Rules	Creating an Alarm Rule (Recommended)	Create an alarm rule.
		Batch Deleting Alarm Rules	Delete alarm rules in batches.
		Enabling or Disabling Alarm Rules in Batches	Enable or disable alarm rules in batches.
		Querying Alarm Rules (Recommended)	Query the alarm rule list.
	Monitored Resources	Batch Adding Resources to an Alarm Rule	Batch add monitored resources to an alarm rule. (Alarm rules for resources in resource groups are excluded.)
		Batch Deleting Resources from an Alarm Rule	Batch delete monitored resources from an alarm rule. (Alarm rules for resources in resource groups are excluded.)

Type	Subtype	API	Description
		Querying Resources in an Alarm Rule	Query resources in an alarm rule based on the alarm rule ID.
	Alarm Policies	**Modifying All Fields in an Alarm Policy**	Modify policies in an alarm rule.
		Querying Alarm Policies	Query alarm policies based on the alarm rule ID.
	Alarm Notifications	**Modifying Alarm Notification Information in an Alarm Rule**	Modify alarm notification information in an alarm rule.
	Alarm Records	**This API is used to query alarm records.**	Query alarm records.
	Alarm Templates	**Creating a Custom Alarm Template**	Create a custom alarm template.
		Deleting Custom Alarm Templates in Batches	Delete custom templates in batches.
		This API is used to modify a custom template.	Modify a custom template.
		Querying Alarm Templates	Query alarm templates.
		Querying Details of an Alarm Template	Query the alarm template details.
	Alarm Rules Associated with an Alarm Template	**Querying Alarm Rules Associated with an Alarm Template**	Query alarm rules associated with an alarm template.

Type	Subtype	API	Description
	Resource Groups	Creating a Resource Group (Recommended)	Create a resource group.
		This API is used to delete resource groups in batches.	Delete resource groups in batches.
		Modifying a Resource Group	Modify a resource group.
		Querying Details of a Resource Group	Query details of a resource group.
		Querying Resource Groups	Query resource groups.
		Asynchronously Associating a Resource Group with a Custom Alarm Template	Submit an asynchronous task for batch associating custom alarm templates with a resource group. This process will create alarm rules to replace existing ones.
	Resource Association in a Resource Group	Batch Adding Resources to a Resource Group	Batch add resources to a custom resource group.
		Batch Deleting Resources from a Resource Group	Batch delete resources from a resource group whose resources are manually added.
		Querying Resources of a Specified Dimension and a Specified Service Type in a Resource Group	Query resources of a specified dimension for a specified resource type in a resource group.

Type	Subtype	API	Description
	One-Click Monitoring	Enabling One-Click Monitoring	Enable one-click monitoring.
		Querying Services and Resources That Support One-Click Monitoring	Query services and resources that support one-click monitoring.
		Querying Alarm Rules of a Service in One-Click Monitoring	Query alarm rules of a service in one-click monitoring.
		Batch Enabling or Disabling Alarm Rules for One Service in One-Click Monitoring	Batch enable or disable alarm rules for a service in one-click monitoring.
		Batch Disabling One-Click Motoring	Batch disable one-click motoring.
		Batch Modifying Alarm Notifications in Alarm Rules for One Service with One-Click Monitoring Enabled	Batch modify alarm notifications in alarm rules for one service that has one-click monitoring enabled.
		Batch Enabling or Disabling Alarm Rules for One Service with One-Click Monitoring Enabled	Batch enable or disable alarm policies in alarm rules for one service that has one-click monitoring enabled.

Type	Subtype	API	Description
	Alarm Masking	Creating Alarm Masking Rules in Batches	Create alarm masking rules in batches.
		Modifying the Masking Time of Alarm Masking Rules in Batches	Modify the masking duration of alarm masking rules in batches.
		Modifying an Alarm Masking Rule	Modify an alarm masking rule.
		Deleting Alarm Masking Rules in Batches	Delete alarm masking rules in batches.
		Querying Alarm Masking Rules	Query alarm masking rules of a specified type in batches. Currently, a maximum of 100 masking rules can be queried in batches.
		Querying Resources for Which an Alarm Masking Rule Is Applied	Query resources for which alarm notifications have been masked.
	Dashboards	Creating or Copying a Dashboard	Create or copy a dashboard.
		Querying Dashboards	Query dashboards.
		Modifying a Dashboard	Modify a dashboard.
		Deleting Dashboards in Batches	Delete dashboards in batches.

Type	Subtype	API	Description
	Graphs	**Creating, Copying, or Batch Creating Graphs on a Dashboard**	Create, copy, or batch create graphs on a dashboard.
		Querying Graphs Added to a Dashboard	Query graphs added to a dashboard.
		Querying Information About a Graph	Query information about a graph.
		Deleting a Graph	Delete a graph.
		Updating Graphs in Batches	Update graphs in batches.
	Resource Tag Management	**Querying Tags for a Specified Resource Type in a Cloud Eye Project**	Query tags of a type of resources in a Cloud Eye project.
	Metric Management	**Querying the Original Dimension Values in Server Monitoring**	Query metrics by disk, mount point, process, graphics card, or RAID controller based on the ECS or BMS ID.
API V3	Agent Statuses	**Querying Agent Statuses in Batches**	Query the Agent (including the UniAgent) statuses.
	Agent Task-related APIs	**Querying the Agent Maintenance Tasks**	Query the Agent tasks.
		Creating Agent maintenance Tasks in Batches	Batch create Agent tasks.

3 Calling APIs

3.1 Making an API Request

This section describes the structure of a REST API request, and uses the IAM API for **creating an IAM user** as an example to demonstrate how to call an API.

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.

Table 3-1 URI parameter description

Parameter	Description
URI-scheme	Protocol used to transmit requests. All APIs use HTTPS.
Endpoint	Domain name or IP address of the server bearing the REST service. The endpoint varies between services in different regions. It can be obtained from **Regions and Endpoints**. For example, the endpoint of IAM in region **CN-Hong Kong** is **iam.ap-southeast-1.myhuaweicloud.com**.
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.

IAM is a global service. You can create an IAM user using the endpoint of IAM in any region. For example, to create an IAM user in the **CN-Hong Kong** region, obtain the endpoint of IAM (**iam.ap-southeast-1.myhuaweicloud.com**) for this region and the **resource-path** (**/v3.0/OS-USER/users**) in the URI of the API for **creating an IAM user**. Then construct the URI as follows:

```
https://iam.ap-southeast-1.myhuaweicloud.com/v3.0/OS-USER/users
```

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.

Table 3-2 HTTP methods

Method	Description
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 for **creating an IAM user**, the request method is **POST**. An example request is as follows:

```
POST https://iam.ap-southeast-1.myhuaweicloud.com/v3.0/OS-USER/users
```


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.

Table 3-3 Common request header fields

Parameter	Description	Mandatory	Example Value
Host	Specifies the server domain name and port number of the resources being requested. The value can be obtained from the URL of the service API. The value is in the format of *Hostname:Port number*. If the port number is not specified, the default port is used. The default port number for **https** is **443**.	No This field is mandatory for AK/SK authentication.	code.test.com or code.test.com:443
Content-Type	Specifies the type (or format) of the message body. The default value **application/json** is recommended. Other values of this field will be provided for specific APIs if any.	Yes	application/json
Content-Length	Specifies the length of the request body. The unit is byte.	No	3495
X-Project-Id	Specifies the project ID. Obtain the project ID by following the instructions in **Obtaining a Project ID**.	No This field is mandatory for requests that use AK/SK authentication in the Dedicated Cloud (DeC) scenario or multi-project scenario.	e9993fc787d94b6c886cbaa340f9c0f4

Parameter	Description	Mandatory	Example Value
X-Auth-Token	Specifies the user token. It is a response to the API for **obtaining a user token** (This is the only API that does not require authentication). After the request is processed, the value of **X-Subject-Token** in the response header is the token value.	No This field is mandatory for token authentication.	The following is part of an example token: MIIPAgYJKoZIhvcNAQcCo...ggg1BBIINPXsidG9rZ

NOTE

In addition to supporting authentication using tokens, APIs support authentication using AK/SK, which uses SDKs to sign a request. During the signature, the **Authorization** (signature authentication) and **X-Sdk-Date** (time when a request is sent) headers are automatically added in the request.

For more details, see "Authentication Using AK/SK" in **Authentication**.

The following shows an example request of the API for **creating an IAM user** when AK/SK authentication is used:

```
POST https://iam.ap-southeast-1.myhuaweicloud.com/v3.0/OS-USER/users
Content-Type: application/json
X-Sdk-Date: 20240416T095341Z
Authorization: SDK-HMAC-SHA256 Access=**********, SignedHeaders=content-type;host;x-sdk-date,
Signature=**********
```

(Optional) Request Body

This part is optional. A request body is generally sent in a structured format (for example, JSON or XML), which is specified by **Content-Type** in the request header. It is used to transfer content other than the request header. If the request body contains full-width characters, these characters must be coded in UTF-8.

The request body varies depending on APIs. Certain APIs do not require the request body, such as the APIs requested using the GET and DELETE methods.

The following shows an example request (a request body included) of the API for **creating an IAM user**. You can learn about request parameters and related description from this example. The bold parameters need to be replaced for a real request.

- **accountid**: account ID of an IAM user
- **username**: name of an IAM user
- **email**: email of an IAM user
- **password**: login password of an IAM user

```
POST https://iam.ap-southeast-1.myhuaweicloud.com/v3.0/OS-USER/users
Content-Type: application/json
X-Sdk-Date: 20240416T095341Z
```



```
Authorization: SDK-HMAC-SHA256 Access=**********, SignedHeaders=content-type;host;x-sdk-date,
Signature=**********

{
    "user": {
        "domain_id": "accountid",
        "name": "username",
        "password": "**********",
        "email": "email",
        "description": "IAM User Description"
    }
}
```

If all data required for the API request is available, you can send the request to call the API through **curl**, **Postman**, or coding.

3.2 Authentication

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

- Token authentication: Requests are authenticated using tokens.
- AK/SK authentication: Requests are encrypted using AK/SK pairs. AK/SK authentication is recommended because it is more secure than token authentication.

Token Authentication

NOTE

The validity period of a token is 24 hours. When using a token for authentication, cache it to prevent frequently calling the 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. You can obtain a token by calling the **Obtaining User Token** API.

Cloud Eye is a project-level service. When you call the API, set **auth.scope** in the request body to **project**.

```
{
    "auth": {
        "identity": {
            "methods": [
                "password"
            ],
            "password": {
                "user": {
                    "name": "username",   //IAM user name
                    "password": "********",  //IAM user password
                    "domain": {
                        "name": "domainname"  //Name of the account to which the IAM user belongs
                    }
                }
            }
        },
        "scope": {
            "project": {
                "name": "xxxxxxxx"    //Project Name
            }
        }
    }
}
```


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

```
https://iam.ap-southeast-1.myhuaweicloud.com/v3/auth/projects
Content-Type: application/json
X-Auth-Token: ABCDEFG....
```

AK/SK Authentication

NOTE

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

In AK/SK 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 that works with an SK to sign requests cryptographically.
- SK: secret access key, which works with an AK to sign requests cryptographically. It identifies a request sender and prevents the request from being modified.

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

NOTE

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 **create an IAM user**, 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 **create an IAM user**. The **X-Subject-Token** header field is the desired user token. This token can then be used to authenticate the calling of other APIs.

NOTE

For security purposes, you are advised to set the token in ciphertext in configuration files or environment variables and decrypt it when using it.

Figure 3-2 Header fields of the response to the request for creating an IAM user


```
"X-Frame-Options": "SAMEORIGIN",
"X-IAM-ETag-id": "2562365939-d8f6f12921974cb097338ac11fceac8a",
"Transfer-Encoding": "chunked",
"Strict-Transport-Security": "max-age=31536000; includeSubdomains;",
"Server": "api-gateway",
"X-Request-Id": "af2953f2bcc67a42325a69a19e6c32a2",
"X-Content-Type-Options": "nosniff",
"Connection": "keep-alive",
"X-Download-Options": "noopen",
"X-XSS-Protection": "1; mode=block;",
"X-IAM-Trace-Id": "token_[redacted]_null_af2953f2bcc67a42325a69a19e6c32a2",
"Date": "Tue, 21 May 2024 09:03:40 GMT",
"Content-Type": "application/json; charset=utf8"
```


(Optional) Response Body

The body of a response is often returned in a structured format (for example, JSON or XML) as specified in the **Content-Type** header field. The response body transfers content except the response header.

The following shows part of the response body for the API used to **create an IAM user**.


```
{
    "user": {
        "id": "c131886aec...",
        "name": "IAMUser",
        "description": "IAM User Description",
        "areacode": "",
        "phone": "",
        "email": "***@***.com",
        "status": null,
        "enabled": true,
        "pwd_status": false,
        "access_mode": "default",
        "is_domain_owner": false,
        "xuser_id": "",
        "xuser_type": "",
        "password_expires_at": null,
        "create_time": "2024-05-21T09:03:41.000000",
        "domain_id": "d78cbac1.....",
        "xdomain_id": "30086000.....",
        "xdomain_type": "",
        "default_project_id": null
    }
}
```


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


```
{
    "error_msg": "The request message format is invalid.",
    "error_code": "IMG.0001"
}
```


In the response body, **error_code** is an error code, and **error_msg** provides information about the error.

4 Getting Started

Overview

This topic describes how to call Cloud Eye APIs to create an alarm rule for the ECS CPU usage.

NOTE

The validity period of a token obtained from IAM is 24 hours. If you want to use a token for authentication, cache it to avoid frequently calling the IAM API.

Procedure

1. Obtain the token by referring to **Authentication**.
2. Query the list of metrics that can be monitored.

   Send **GET https://***Cloud Eye endpoint***/V1.0/{project_id}/metrics**.

   Add **X-Auth-Token** obtained in **1** to the request header.

   After the request is successfully responded, the **metrics** information is returned, such as **"metric_name": "cpu_util"** in the following figure.


```
{
    "metrics": [
        {
            "namespace": "SYS.ECS",
            "dimensions": [
                {
                    "name": "instance_id",
                    "value": "d9112af5-6913-4f3b-bd0a-3f96711e004d"
                }
            ],
            "metric_name": "cpu_util",
            "unit": "%"
        }
    ],
    "meta_data": {
        "count": 1,
        "marker": "SYS.ECS.cpu_util.instance_id:d9112af5-6913-4f3b-bd0a-3f96711e004d",
        "total": 7
    }
}
```


   If the request fails, an error code and error information are returned. For details, see **Error Codes**.

3. Create an alarm rule.

   Send **POST https://*Cloud Eye endpoint*/V1.0/{project_id}/alarms**.

   Specify the following parameters in the request body:

```
{
   "alarm_name": "alarm-rp0E",  //Alarm rule name (mandatory, string)
   "alarm_description": "",
   "metric": {
      "namespace": "SYS.ECS",  //Namespace (mandatory, string)
      "dimensions": [
         {
            "name": "instance_id",
            "value": "33328f02-3814-422e-b688-bfdba93d4051"
         }
      ],
      "metric_name": "cpu_util"   //Metric name (mandatory, string)
   },
   "condition": {
      "period": 300,      //Monitoring period (mandatory, integer)
      "filter": "average",     //Data rollup method (mandatory, string)
      "comparison_operator": ">=",    //Operator of the alarm threshold (mandatory, string)
      "value": 80, //Threshold (mandatory, string)
      "unit": "%",  //Data unit (mandatory, string)
      "count": 1
   },
   "alarm_enabled": true,
   "alarm_action_enabled": true,
   "alarm_level": 2,
   "alarm_actions": [
      {
         "type": "notification",
         "notificationList": [ ]
      }
   ],
   "ok_actions": [
      {
         "type": "notification",
         "notificationList": [ ]
      }
   ]
}
```

   If the request is responded, the alarm rule ID is returned.

```
{
   "alarm_id":"al1450321795427dR8p5mQBo"
}
```

   If the request fails, an error code and error information are returned. For details, see **Error Codes**.

   You can query, enable, disable, or delete alarm rules based on the alarm rule ID obtained in **3**.

5 API V1

5.1 API Version Management

5.1.1 Querying All API Versions

Function

This API is used to query all API versions supported by Cloud Eye.

URI

GET /

Request

Example request

```
GET https://{Cloud Eye endpoint}/
```

Response

- Response parameters

Table 5-1 Parameter description

Parameter	Type	Description
versions	Array of objects	Specifies the list of all versions. For details, see **Table 5-2**.

Table 5-2 versions data structure description

Parameter	Type	Description
id	String	Specifies the version ID, for example, v1.
links	Array of objects	Specifies the API URL. For details, see **Table 5-3**.
version	String	Specifies the API version. If the APIs of this version support microversions, set this parameter to the supported maximum microversion. If the microversion is not supported, leave this parameter blank.
status	String	Specifies the version status. **CURRENT**: indicates a primary version. **SUPPORTED**: indicates an old version but is still supported. **DEPRECATED**: indicates a deprecated version which may be deleted later.
updated	String	Specifies the version release time, which must be the UTC time. For example, the release time of v1 is **2014-06-28T12:20:21Z**.
min_version	String	If the APIs of this version support microversions, set this parameter to the supported minimum microversion. If not, leave this parameter blank.

Table 5-3 links data structure description

Parameter	Type	Description
href	String	Specifies the reference address of the current API version.
rel	String	Specifies the relationship between the current API version and the referenced address.

- Example response

```
{
 "versions": [
  {
   "id": "V1.0",
   "links": [
    {
     "href": "https://x.x.x.x/V1.0/",
     "rel": "self"
    }
   ],
   "min_version": "",
   "status": "CURRENT",
   "updated": "2018-09-30T00:00:00Z",
   "version": ""
  }
```



```
 ]
}
```

Returned Values

- Normal

  200

- Abnormal

Returned Value	Description
400 Bad Request	Request error.
401 Unauthorized	The authentication information is not provided or is incorrect.
403 Forbidden	Access to the requested page is forbidden.
408 Request Timeout	The request timed out.
429 Too Many Requests	Concurrent requests are excessive.
500 Internal Server Error	Failed to complete the request because of an internal service error.
503 Service Unavailable	The service is currently unavailable.

Error Codes

See **Error Codes**.

5.1.2 Querying a Specified API Version

Function

This API is used to query a specified API version of Cloud Eye.

URI

GET /{api_version}

- Parameter description

  Table 5-4 Parameter description

Parameter	Mandatory	Description
api_version	Yes	**Definition** API version.

- Example

```
GET https://{Cloud Eye endpoint}/V1.0\
```

Request

None

Response

- Response parameters

Table 5-5 Parameter description

Parameter	Type	Description
version	Objects	**Definition** Version details. For details, see **Table 5-6**.

Table 5-6 versions data structure description

Parameter	Type	Description
id	String	**Definition** Version number, for example, **V1.0** **Range** 1 to 64 characters
links	Array of objects	**Definition** API URL. For details, see **Table 5-7**.
version	String	**Definition** API version. If the APIs of this version support micro versions, this parameter indicates the supported maximum micro version. If not, it is left blank. **Range** 1 to 64 characters
status	String	**Definition** Version status. **Range** **CURRENT**: widely used version **SUPPORTED**: earlier version which is still supported **DEPRECATED**: deprecated version which may be deleted later

Parameter	Type	Description
updated	String	**Definition** Version release time in UTC. For example, the release time of v1 is **2014-06-28T12:20:21Z**. **Range** N/A
min_version	String	**Definition** API version. If the APIs of this version support micro versions, this parameter indicates the supported minimum micro version. If not, it is left blank. **Range** 1 to 64 characters

Table 5-7 links data structure description

Parameter	Type	Description
href	String	**Definition** Reference address of the current API version. **Range** N/A
rel	String	**Definition** Relationship between the current API version and the referenced address. **Range** N/A

- Example response

```
{
  "version": {
     "id": "V1.0",
     "links": [
       {
         "href": "https://x.x.x.x/V1.0/",
         "rel": "self"
       }
     ],
     "min_version": "",
     "status": "CURRENT",
     "updated": "2018-09-30T00:00:00Z",
     "version": ""
   }
}
```

Returned Values

- Normal

200

- Abnormal

Returned Value	Description
400 Bad Request	Request error.
401 Unauthorized	The authentication information is not provided or is incorrect.
403 Forbidden	Access to the requested page is forbidden.
408 Request Timeout	The request timed out.
429 Too Many Requests	Concurrent requests are excessive.
500 Internal Server Error	Failed to complete the request because of an internal service error.
503 Service Unavailable	The service is currently unavailable.

Error Codes

See **Error Codes**.

5.2 Metrics

5.2.1 Querying Metrics

Function

This API is used to query metrics supported by Cloud Eye. You can specify the namespace, metric, dimension, sorting order, start records, and the maximum number of records when using this API to query metrics.

NOTICE

After a cloud service resource is deleted, its data is cached for 3 hours, so metrics of the resource can still be queried within the 3 hours.

Debugging

You can debug the API in **API Explorer** which supports automatic authentication. API Explorer can automatically generate and debug example SDK code.

URI

GET /V1.0/{project_id}/metrics

- Parameter description

Table 5-8 Parameter description

Parameter	Mandatory	Description
project_id	Yes	**Definition** Project ID, which is used to specify the project that an asset belongs to. You can query the assets of a project by project ID. You can obtain the project ID from the API or console. For details about how to obtain the project ID, see **Obtaining a Project ID**. **Constraints** N/A **Range** 1 to 64 characters **Default Value** N/A

Table 5-9 Query parameter description

Parameter	Mandatory	Type	Description
namespace	No	String	**Definition** Service metric namespace. For details, see **Services Interconnected with Cloud Eye**. **Constraints** N/A **Range** The namespace must be in the service.item format. **service** and **item** must be strings, and each must start with a letter and contain only letters (case-insensitive), digits, and underscores (_). In addition, **service** cannot start with **SYS**, **AGT**, or **SRE**. **namespace** cannot be **SERVICE.BMS** because this namespace has been used by the system. The value can contain 3 to 32 characters. For example, the ECS namespace is **SYS.ECS**, and the DDS namespace is **SYS.DDS**. **Default Value** N/A

Parameter	Mandatory	Type	Description
metric_name	No	String	**Definition** Metric ID. For example, **metric_name** of ECS CPU usage is **cpu_util**. For details about the metrics of each service, see **Services Interconnected with Cloud Eye**. **Constraints** N/A **Range** The value must start with a letter and can contain only digits, letters (case-insensitive), underscores (_), and hyphens (-). For example, the ECS metric **cpu_util** indicates the CPU usage of an ECS. The DDS metric **mongo001_command_ps** indicates the command execution frequency. The value can contain 1 to 96 characters. **Default Value** N/A
dim	No	String	**Definition** Dimension of a metric. **Constraints** N/A **Range** A maximum of 4 dimensions are supported, numbered from 0 in the **dim.{i}=key,value** format. **key** cannot exceed 32 characters and **value** cannot exceed 256 characters. The following dimensions are only examples. For details about whether multiple dimensions are supported, see **Services Interconnected with Cloud Eye**. Single dimension: **dim.0=instance_id,i-12345** Multiple dimensions: **dim.0=instance_id,i-12345&dim.1=instance_name,i-1234** **Default Value** N/A

Parameter	Mandatory	Type	Description
start	No	String	**Definition** Pagination start value. **Constraints** N/A **Range** The value is in the namespace.metric_name.key:value format. Example: **start=SYS.ECS.cpu_util.instance_id:d9112af5-6913-4f3b-bd0a-3f96711e004d**. **Default Value** N/A
limit	No	Integer	**Definition** Maximum number of records that can be queried at a time. **Constraints** N/A **Range** [1, 1,000] **Default Value** 1,000
order	No	String	**Definition** Result sorting method, which is sorted by timestamp. **Constraints** N/A **Range** The value can be: • **asc**: ascending order • **desc**: descending order **Default Value** asc

- Example requests

  Example request 1: Query all metrics that can be monitored.

  ```
  GET https://{Cloud Eye endpoint}/V1.0/{project_id}/metrics
  ```

  Example request 2: Query the CPU usage of the ECS whose ID is **6f3c6f91-4b24-4e1b-b7d1-a94ac1cb011d**. Retain 10 records in descending order by timestamp.


```
GET https://{Cloud Eye endpoint}/V1.0/{project_id}/metrics?
namespace=SYS.ECS&metric_name=cpu_util&dim.0=instance_id,6f3c6f91-4b24-4e1b-b7d1-
a94ac1cb011d&limit=10&order=desc
```

Request

None

Response

- Response parameters

Table 5-10 Parameter description

Parameter	Type	Description
metrics	Array of objects	**Definition** List of metric objects. For details, see **Table 5-11**.
meta_data	Object	**Definition** Metadata of query results, including the pagination information. For details, see **Table 5-13**.

Table 5-11 metrics data structure description

Parameter	Type	Description
namespace	String	**Definition** Namespace of the metric. **Range** N/A
dimensions	Array of objects	**Definition** List of metric dimensions. For details, see **Table 5-12**.
metric_name	String	**Definition** Metric name, such as **cpu_util**. **Range** N/A
unit	String	**Definition** Metric unit. **Range** N/A

Table 5-12 dimensions data structure description

Parameter	Type	Description
name	String	**Definition** Monitoring dimension name. For example, the ECS dimension is **instance_id**. For details about the dimension of each service, see the **key** column in **Services Interconnected with Cloud Eye**. **Range** N/A
value	String	**Definition** Dimension value, for example, an ECS ID. **Range** N/A

Table 5-13 meta_data data structure description

Parameter	Type	Description
count	Integer	**Definition** Number of returned records. **Range** N/A
marker	String	**Definition** Start of the next page, which is used for pagination. For example, you have queried 10 records this time and the tenth record is about **cpu_util**. In your next query, if **start** is set to **cpu_util**, you can start your query from the next metric of **cpu_util**. **Range** N/A
total	Integer	**Definition** Total number of metrics. **Range** N/A

- Example response

```
{
  "metrics": [
    {
      "namespace": "SYS.ECS",
      "dimensions": [
```



```
            {
                "name": "instance_id",
                "value": "d9112af5-6913-4f3b-bd0a-3f96711e004d"
            }
        ],
        "metric_name": "cpu_util",
        "unit": "%"
    }
  ],
  "meta_data": {
    "count": 1,
    "marker": "SYS.ECS.cpu_util.instance_id:d9112af5-6913-4f3b-bd0a-3f96711e004d",
    "total": 7
  }
}
```


Returned Values

- Normal

  200
- Abnormal

Returned Value	Description
400 Bad Request	Request error.
401 Unauthorized	The authentication information is not provided or is incorrect.
403 Forbidden	Access to the requested page is forbidden.
408 Request Timeout	The request timed out.
429 Too Many Requests	Concurrent requests are excessive.
500 Internal Server Error	Failed to complete the request because of an internal service error.
503 Service Unavailable	The service is currently unavailable.

Error Codes

See **Error Codes**.

5.3 Alarm Rules

5.3.1 Querying Alarm Rules

Function

This API is used to query alarm rules. You can specify the paging parameters to limit the number of query results displayed on a page. You can also set the sorting order of query results.

NOTE

For API V1, only an alarm rule can be configured for a single resource. You are advised to use **Querying Alarm Rules (Recommended)** to work with the console.

Debugging

You can debug the API in **API Explorer** which supports automatic authentication. API Explorer can automatically generate and debug example SDK code.

URI

GET /V1.0/{project_id}/alarms

- Parameter description

Table 5-14 Parameter description

Parameter	Mandatory	Description
project_id	Yes	**Definition** Project ID. It is used to specify the project that an asset belongs to. You can query the assets of a project by project ID. You can obtain the project ID from the API or console. For details about how to obtain the project ID, see **Obtaining a Project ID**. **Constraints** N/A **Range** 1 to 64 characters **Default Value** N/A

Table 5-15 Query parameter description

Parameter	Mandatory	Type	Description
start	No	String	**Definition** Pagination start value. The value is **alarm_id**. **Constraints** N/A **Range** The value starts with **al** and is followed by 22 characters of letters, digits, or a combination of both. The value can contain a total of 24 characters. **Default Value** N/A
limit	No	Integer	**Definition** Number of records that can be returned. **Constraints** N/A **Range** (0,100] **Default Value** **100**
order	No	String	**Definition** Result sorting method, which is sorted by timestamp. **Constraints** N/A **Range** The value can be: • **asc**: The query results are displayed in the ascending order. • **desc**: The query results are displayed in the descending order. **Default Value** desc

- Example

  Request example 1: Query the current alarm rule list.

```
GET https://{Cloud Eye endpoint}/V1.0/{project_id}/alarms
```

  Request example 2: Query the alarm rule list. Start by setting **alarm_id** to **al1441967036681YkazZ0deN** and retain 10 records in the descending order of time stamps.

```
GET https://{Cloud Eye endpoint}/V1.0/{project_id}/alarms?
start=al1441967036681YkazZ0deN&limit=10&order=desc
```

Request

None

Response

- Response parameters

Table 5-16 Parameter description

Parameter	Type	Description
metric_alarms	Array of objects	**Definition** List of alarm objects. For details, see **Table 5-17**.
meta_data	Object	**Definition** Metadata of query results, including the pagination information. For details, see **Table 5-24**.

Table 5-17 metric_alarms data structure description

Parameter	Type	Description
alarm_name	String	**Definition** Alarm name. **Range** N/A
alarm_description	String	**Definition** Provides supplementary information about the alarm rule. **Range** N/A
metric	Object	**Definition** Alarm metrics. For details, see **Table 5-18**.

Parameter	Type	Description
condition	Object	**Definition** Alarm triggering condition. For details, see **Table 5-23**.
alarm_enabled	Boolean	**Definition** Whether to enable the alarm rule. **Range** A boolean value. • **true**: enable • **false**: disable
alarm_level	Integer	**Definition** Alarm severity. **Range** The value can be **1** (critical), **2** (major), **3** (minor), or **4** (warning).
alarm_action_enabled	Boolean	**Definition** Whether to enable the action triggered by the alarm. **Range** A boolean value. • **true**: enable • **false**: disable
alarm_actions	Array of objects	**Definition** Action to be triggered by the alarm. For details, see **Table 5-20**.
ok_actions	Array of objects	**Definition** Action to be triggered after an alarm is cleared. For details, see **Table 5-21**.
insufficientdata_actions	Array of objects	**Definition** Action triggered by data insufficiency. For details, see **Table 5-22**.

Parameter	Type	Description
alarm_action_begin_time	String	**Definition** Time when an alarm rule is applied. Notifications are sent only within the validity period of the alarm rule. For example, if **alarm_action_begin_time** is set to **08:00** and **alarm_action_end_time** is set to **20:00**, notifications are sent only from 08:00 to 20:00. **Range** The value allows 1 to 64 characters and can contain only digits and colons (:).
alarm_action_end_time	String	**Definition** Time when an alarm rule becomes invalid. For example, if **alarm_action_begin_time** is set to **08:00** and **alarm_action_end_time** is set to **20:00**, notifications are sent only from 08:00 to 20:00. **Range** The value allows 1 to 64 characters and can contain only digits and colons (:).
alarm_type	String	**Definition** Alarm rule type. **Range** • **EVENT.SYS**: The alarm rule is created for system events. **EVENT.CUSTOM**: The alarm rule is created for custom events. • **RESOURCE_GROUP**: The alarm rule is created for resource groups. • **MULTI_INSTANCE**: The alarm rule is created for specific resources.
alarm_id	String	**Definition** Alarm rule ID. **Range** The value starts with **al** and is followed by 22 characters of letters, digits, or a combination of both.
update_time	Long	**Definition** Time when the alarm status changed. The value is a UNIX timestamp, in ms. **Range** N/A

Parameter	Type	Description
alarm_state	String	**Definition** Alarm status. **Range** • **ok**: The alarm status is normal. • **alarm**: An alarm is generated. • **insufficient_data**: The required data is insufficient.
enterprise_project_id	String	**Definition** Enterprise project ID. **Range** The value can only contain lowercase letters, digits, hyphens (-), and underscores (_). It allows 36 characters. The value can be **0** (default enterprise project ID) or **all_granted_eps** (all enterprise project IDs).

Table 5-18 metric data structure description

Parameter	Type	Description
namespace	String	**Definition** Namespace of the queried service. For details, see **Services Interconnected with Cloud Eye**. **Range** N/A
dimensions	Array of objects	**Definition** List of metric dimensions. For details, see **Table 5-19**.
metric_name	String	**Definition** Metric ID. For example, **metric_name** of ECS CPU usage is **cpu_util**. For details about the metrics of each service, see **Services Interconnected with Cloud Eye**. **Range** N/A

Parameter	Type	Description
resource_group_id	String	**Definition** ID of the resource group selected during the alarm rule creation, for example, **rg1603786526428bWbVmk4rP**. **Range** N/A
resource_group_name	String	**Definition** Name of the resource group selected during the alarm rule creation, for example, **Resource-Group-ECS-01**. **Range** N/A

Table 5-19 dimensions data structure description

Parameter	Type	Description
name	String	**Definition** Monitoring dimension name. For example, the ECS dimension is **instance_id**. For details about the dimension of each service, see the **key** column in **Services Interconnected with Cloud Eye**. **Range** N/A
value	String	**Definition** Dimension value, for example, an ECS ID. **Range** Enter 1 to 256 characters.

Table 5-20 alarm_actions data structure description

Parameter	Type	Description
type	String	**Definition** Alarm notification type. **Range** • **notification**: A notification will be sent. • **autoscaling**: A scaling action will be triggered.

Parameter	Type	Description
notificationList	Array of strings	**Definition** List of objects to be notified of alarm status changes. **NOTE** The IDs in the list are strings.

Table 5-21 ok_actions data structure description

Parameter	Type	Description
type	String	**Definition** Notification type when an alarm is cleared. **Range** • **notification**: A notification will be sent. • **autoscaling**: A scaling action will be triggered.
notificationList	Array of strings	**Definition** List of IDs of objects to be notified of alarm status changes. **NOTE** The IDs in the list are strings.

Table 5-22 insufficientdata_actions data structure description

Parameter	Type	Description
type	String	**Definition** Type of the alarm notification triggered by insufficient data. **Range** **notification**
notificationList	Array of strings	**Definition** IDs of the notified objects when an alarm notification is triggered due to insufficient data.

Table 5-23 condition data structure description

Parameter	Type	Description
period	Integer	**Definition** Interval (seconds) for checking whether the alarm rule conditions are met. **Range** The value can be: • **0**: triggered immediately (only for event scenarios). • **1**: original metric period. For example, if the original period of an RDS metric is 60s, the metric data is collected and calculated every 60s. • **300**: The metric data is collected and calculated every 5 minutes. • **1200**: The metric data is collected and calculated every 20 minutes. • **3600**: The metric data is collected and calculated every hour. • **14400**: The metric data is collected and calculated every 4 hours. • **86400**: The metric data is collected and calculated every day.
filter	String	**Definition** Data aggregation method. **Range** • **average**: average value of metric data within an aggregation period. • **max**: maximum value of metric data in an aggregation period. • **min**: Cloud Eye calculates the minimum value of metric data within a rollup period. • **sum**: sum of metric data within an aggregation period. • **variance**: variance value of metric data within an aggregation period.
comparison_operator	String	**Definition** Operator of an alarm threshold. **Range** >, =, <, >=, <=, or **!=**

Parameter	Type	Description
value	Double	**Definition** Alarm threshold. For detailed thresholds, see the value range of each metric in the appendix. For example, you can set ECS **cpu_util** in **Services Interconnected with Cloud Eye** to **80**. **Range** [0, Number.MAX_VALUE], where **Number.MAX_VALUE** indicates **1.7976931348623157e+108**
unit	String	**Definition** Data unit. **Range** 0 to 32 characters
count	Integer	**Definition** Number of consecutive times that an alarm is triggered. **Range** [1, 5]
suppress_duration	Integer	**Definition** Interval for triggering an alarm if the alarm persists. **Range** The value can be: • **0**: The alarm is triggered only once. • **300**: An alarm is triggered every 5 minutes. • **600**: An alarm is triggered every 10 minutes. • **900**: An alarm is triggered every 15 minutes. • **1800**: An alarm is triggered every 30 minutes. • **3600**: An alarm is triggered every hour. • **10800**: An alarm is triggered every 3 hours. • **21600**: An alarm is triggered every 6 hours. • **43200**: An alarm is triggered every 12 hours. • **86400**: An alarm is triggered every day.

Table 5-24 meta_data data structure description

Parameter	Type	Description
count	Integer	**Definition** Number of returned records. **Range** N/A
marker	String	**Definition** Pagination marker. For example, you have queried 10 records this time and **alarm_id** of the tenth record is **1441967036681YkazZ0deN**. In your next query, if **start** is set to **al1441967036681YkazZ0deN**, you can start your query from the next alarm rule ID of **al1441967036681YkazZ0deN**. **Range** N/A
total	Integer	**Definition** Total number of query results. **Range** N/A

- Example response

```
{
    "metric_alarms": [
        {
            "alarm_name": "alarm-ttttttt",
            "alarm_description": "",
            "metric": {
                "namespace": "SYS.ECS",
                "dimensions": [
                    {
                        "name": "instance_id",
                        "value": "07814c0e-59a1-4fcd-a6fb-56f2f6923046"
                    }
                ],
                "metric_name": "cpu_util"
            },
            "condition": {
                "period": 300,
                "filter": "average",
                "comparison_operator": ">=",
                "value": 0,
                "unit": "%",
                "count": 3
            },
            "alarm_enabled": true,
            "alarm_level": 2,
            "alarm_action_enabled": false,
            "alarm_id": "al15330507498596W7vmlGKL",
            "update_time": 1533050749992,
            "alarm_state": "alarm"
        },
        {
```



```
            "alarm_name": "alarm-m5rwxxxxxxx",
            "alarm_description": "",
            "metric": {
                "namespace": "SYS.ECS",
                "dimensions": [
                    {
                        "name": "instance_id",
                        "value": "30f3858d-4377-4514-9081-be5bdbf1392e"
                    }
                ],
                "metric_name": "network_incoming_bytes_aggregate_rate"
            },
            "condition": {
                "period": 300,
                "filter": "average",
                "comparison_operator": ">=",
                "value": 12,
                "unit": "Byte/s",
                "count": 3,
                "suppress_duration": 1800
            },
            "alarm_enabled": true,
            "alarm_level": 2,
            "alarm_action_enabled": true,
            "alarm_actions": [
                {
                    "type": "notification",
                    "notificationList": [
                        "urn:smn:region:68438a86d98e427e907e0097b7e35d48:test0315"
                    ]
                }
            ],
            "ok_actions": [
                {
                    "type": "notification",
                    "notificationList": [
                        "urn:smn:region:68438a86d98e427e907e0097b7e35d48:test0315"
                    ]
                }
            ],
            "alarm_id": "al1533031226533nKJexAlbq",
            "update_time": 1533204036276,
            "alarm_state": "ok"
        }
    ],
    "meta_data": {
        "count": 2,
        "marker": "al1533031226533nKJexAlbq",
        "total": 389
    }
}
```


Returned Values

- Normal

  200

- Abnormal

Returned Value	Description
400 Bad Request	Request error.
401 Unauthorized	The authentication information is not provided or is incorrect.

Returned Value	Description
403 Forbidden	Access to the requested page is forbidden.
408 Request Timeout	The request timed out.
429 Too Many Requests	Concurrent requests are excessive.
500 Internal Server Error	Failed to complete the request because of an internal service error.
503 Service Unavailable	The service is currently unavailable.

Error Codes

See **Error Codes**.

5.3.2 Querying Details of an Alarm Rule

Function

This API is used to query details of an alarm rule based on its ID.

NOTE

For API V1, only an alarm rule can be configured for a single resource. You are advised to use **Querying Alarm Rules (Recommended)** and **Querying Resources in an Alarm Rule** to work with the console.

Debugging

You can debug the API in **API Explorer** which supports automatic authentication. API Explorer can automatically generate and debug example SDK code.

URI

GET /V1.0/{project_id}/alarms/{alarm_id}

- Parameter description

Table 5-25 Parameter description

Parameter	Mandatory	Description
project_id	Yes	Project ID. For details about how to obtain the project ID, see **Obtaining a Project ID**.
alarm_id	Yes	Alarm rule ID.

- Example
  GET https://{Cloud Eye endpoint}/V1.0/{project_id}/alarms/al1441967036681YkazZ0deN

Request

None

Response

- Response parameters

Parameter	Type	Description
metric_alarms	Array of objects	List of alarm objects. For details, see **Table 5-26**.

Table 5-26 metric_alarms data structure description

Parameter	Type	Description
alarm_name	String	Alarm name.
alarm_description	String	Provides supplementary information about the alarm rule.
metric	Object	Alarm metric. For details, see **Table 5-27**.
condition	Object	Alarm triggering condition. For details, see **Table 5-32**.
alarm_enabled	Boolean	Whether to enable the alarm rule.
alarm_level	Integer	Alarm severity, which can be **1** (critical), **2** (major), **3** (minor) or **4** (warning). The default value is **2**.
alarm_type	String	Alarm rule type. • **EVENT.SYS**: The alarm rule is created for system events. **EVENT.CUSTOM**: The alarm rule is created for custom events. • **RESOURCE_GROUP**: The alarm rule is created for resource groups. • **MULTI_INSTANCE**: The alarm rule is created for specific resources.
alarm_action_enabled	Boolean	Whether to enable the action triggered by the alarm.
alarm_actions	Array of objects	Action to be triggered by the alarm. For details, see **Table 5-29**.

Parameter	Type	Description
ok_actions	Array of objects	Action to be triggered after an alarm is cleared. For details, see **Table 5-30**.
insufficientdata_actions	Array of objects	Action triggered by data insufficiency. For details, see **Table 5-31**.
alarm_action_begin_time	String	Time when an alarm rule is applied. Notifications are sent only within the validity period of the alarm rule. For example, if **alarm_action_begin_time** is set to **08:00** and **alarm_action_end_time** is set to **20:00**, notifications are sent only from 08:00 to 20:00.
alarm_action_end_time	String	Time when an alarm rule becomes invalid. For example, if **alarm_action_begin_time** is set to **08:00** and **alarm_action_end_time** is set to **20:00**, notifications are sent only from 08:00 to 20:00.
alarm_id	String	Alarm rule ID.
update_time	Long	Time when the alarm status changed. The value is a UNIX timestamp, in milliseconds.
alarm_state	String	Alarm status. The value can be: • **ok**: The alarm status is normal. • **alarm**: An alarm is generated. • **insufficient_data**: The required data is insufficient.
enterprise_project_id	String	Enterprise project ID. • Value **all_granted_eps** indicates all enterprise projects. • Value **0** indicates the default enterprise project **default**.

Table 5-27 metric data structure description

Parameter	Type	Description
namespace	String	Namespace of the queried service. For details, see **Services Interconnected with Cloud Eye**.
dimensions	Array of objects	List of metric dimensions. For details, see **Table 5-28**.

Parameter	Type	Description
metric_name	String	Metric ID. For example, **metric_name** of ECS CPU usage is **cpu_util**. For details about the metrics of each service, see **Services Interconnected with Cloud Eye**.
resource_group_id	String	ID of the resource group selected during the alarm rule creation, for example, **rg1603786526428bWbVmk4rP**.
resource_group_name	String	Name of the resource group selected during the alarm rule creation, for example, **Resource-Group-ECS-01**.

Table 5-28 dimensions data structure description

Parameter	Type	Description
name	String	Monitoring dimension name. For example, the ECS dimension is **instance_id**. For details about the dimension of each service, see the **key** column in **Services Interconnected with Cloud Eye**.
value	String	Dimension value, for example, an ECS ID. Enter 1 to 256 characters.

Table 5-29 alarm_actions data structure description

Parameter	Type	Description
type	String	Alarm notification type. The value can be: • **notification**: indicates that a notification will be sent. • **autoscaling**: indicates that a scaling action will be triggered.
notificationList	Array of strings	List of objects to be notified of alarm status changes. **NOTE** The IDs in the list are strings.

Table 5-30 ok_actions data structure description

Parameter	Type	Description
type	String	Notification type when an alarm is triggered. • **notification**: A notification will be sent. • **autoscaling**: A scaling action will be triggered.
notificationList	Array of strings	List of objects to be notified of alarm status changes. **NOTE** The IDs in the list are strings.

Table 5-31 insufficientdata_actions data structure description

Parameter	Type	Description
type	String	Notification type when an alarm is cleared. The value is **notification**.
notificationList	Array of strings	List of objects to be notified of alarm status changes. **NOTE** The IDs in the list are strings.

Table 5-32 condition data structure description

Parameter	Type	Description
period	Integer	Interval (seconds) for checking whether the alarm rule conditions are met.
filter	String	Data aggregation method. The value can be: • **average**: average value of metric data within an aggregation period. • **max**: maximum value of metric data in an aggregation period. • **min**: minimum value of metric data within an aggregation period. • **sum**: sum of metric data within an aggregation period. • **variance**: variance value of metric data within an aggregation period.
comparison_operator	String	Operator of alarm thresholds, which can be >, =, <, >=, or <=.

Parameter	Type	Description
value	Double	Alarm threshold. Supported range: **0** to **Number. MAX_VALUE (1.7976931348623157e+108)** For detailed thresholds, see the value range of each metric in the appendix. For example, you can set ECS **cpu_util** in **Services Interconnected with Cloud Eye** to **80**.
unit	String	Data unit. The value contains a maximum of 32 characters.
count	Integer	Number of consecutive times that the alarm policy was met. Supported range: **1** to **5**
suppress_duration	Integer	Interval for triggering an alarm if the alarm persists. The value can be: **0**: alarm triggered only once. **300**: alarm triggered every 5 minutes. **600**: alarm triggered every 10 minutes. **900**: alarm triggered every 15 minutes. **1800**: alarm triggered every 30 minutes. **3600**: alarm triggered every 1 hour. **10800**: alarm triggered every 3 hours. **21600**: alarm triggered every 6 hours. **43200**: alarm triggered every 12 hours. **86400**: alarm triggered every day.

- Example response

```
{
"metric_alarms":
 [
  {
   "alarm_name":"alarm-ipwx",
   "alarm_description":"",
   "metric":
    {
     "namespace":"SYS.ELB",
     "dimensions":
     [
      {
       "name":"lb_instance_id",
       "value":"44d06d10-bce0-4237-86b9-7b4d1e7d5621"
      }
     ],
     "metric_name":"m8_out_Bps"
    },
   "condition":
    {
     "period":300,
     "filter":"sum",
     "comparison_operator":">=",
     "value":0,
     "unit":"",
     "count":1,
     "suppress_duration":1800
    },
   "alarm_enabled":true,
   "alarm_level": 2,
   "alarm_action_enabled":true,
```



```
  "alarm_actions":
   [
    {
     "type":"notification",
     "notificationList":["urn:smn:region:68438a86d98e427e907e0097b7e35d48:sd"]
    }
   ],
  "ok_actions":
   [
    {
     "type":"notification",
     "notificationList":["urn:smn:region:68438a86d98e427e907e0097b7e35d48:sd"]
    }
   ],
  "alarm_id":"al1498096535573r8DNy7Gyk",
  "update_time":1498100100000,
  "alarm_state":"alarm"
 }
]
}
```

Returned Values

- Normal

  200

- Abnormal

Returned Value	Description
400 Bad Request	Request error.
401 Unauthorized	The authentication information is not provided or is incorrect.
403 Forbidden	Access to the requested page is forbidden.
408 Request Timeout	The request timed out.
429 Too Many Requests	Concurrent requests are excessive.
500 Internal Server Error	Failed to complete the request because of an internal service error.
503 Service Unavailable	The service is currently unavailable.

Error Codes

See **Error Codes**.

5.3.3 Enabling or Disabling an Alarm Rule

Function

This API is used to enable or disable an alarm rule.

NOTE

For API V1, only an alarm rule can be configured for a single resource. You are advised to use **Enabling or Disabling Alarm Rules in Batches** to work with the console.

Debugging

You can debug the API in **API Explorer** which supports automatic authentication. API Explorer can automatically generate and debug example SDK code.

URI

PUT /V1.0/{project_id}/alarms/{alarm_id}/action

- Parameter description

Table 5-33 Parameter description

Parameter	Mandatory	Description
project_id	Yes	**Definition** Project ID. It is used to specify the project that an asset belongs to. You can query the assets of a project by project ID. You can obtain the project ID from the API or console. For details about how to obtain the project ID, see **Obtaining a Project ID**. **Constraints** N/A **Range** 1 to 64 characters **Default Value** N/A
alarm_id	Yes	**Definition** Alarm rule ID. **Constraints** N/A **Range** The value starts with **al** and is followed by 22 characters of letters, digits, or a combination of both. The value can contain a maximum of 24 characters. **Default Value** N/A

- Example

```
PUT https://{Cloud Eye endpoint}/V1.0/{project_id}/alarms/al1441967036681YkazZ0deN/action
```


Request

- Request parameters

  Table 5-34 Request parameters

Parameter	Mandatory	Type	Description
alarm_enabled	Yes	Boolean	**Definition** Whether to enable the alarm rule. **Constraints** N/A **Range** A boolean value. The value can be **true** (enabled) or **false** (disabled). **Default Value** N/A

- Example request

```
{
   "alarm_enabled":true
}
```

Response

The response has no message body.

Returned Values

- Normal

  204

- Abnormal

Returned Value	Description
400 Bad Request	Request error.
401 Unauthorized	The authentication information is not provided or is incorrect.
403 Forbidden	Access to the requested page is forbidden.
408 Request Timeout	The request timed out.
429 Too Many Requests	Concurrent requests are excessive.
500 Internal Server Error	Failed to complete the request because of an internal service error.
503 Service Unavailable	The service is currently unavailable.

Error Codes

See **Error Codes**.

5.3.4 Deleting an Alarm Rule

Function

This API is used to delete an alarm rule.

NOTE

For API V1, only an alarm rule can be configured for a single resource. You are advised to use **Batch Deleting Alarm Rules** to work with the console.

Debugging

You can debug the API in **API Explorer** which supports automatic authentication. API Explorer can automatically generate and debug example SDK code.

URI

DELETE /V1.0/{project_id}/alarms/{alarm_id}

- Parameter description

  Table 5-35 Parameter description

Parameter	Mandatory	Description
project_id	Yes	Specifies the project ID. For details about how to obtain the project ID, see **Obtaining a Project ID**.
alarm_id	Yes	Specifies the alarm rule ID.

- Example

```
DELETE https://{Cloud Eye endpoint}/V1.0/{project_id}/alarms/al1441967036681YkazZ0deN
```

Request

The request has no message body.

Response

The response has no message body.

Returned Values

- Normal

  204

- Abnormal

Returned Value	Description
400 Bad Request	Request error.
401 Unauthorized	The authentication information is not provided or is incorrect.
403 Forbidden	Access to the requested page is forbidden.
408 Request Timeout	The request timed out.
429 Too Many Requests	Concurrent requests are excessive.
500 Internal Server Error	Failed to complete the request because of an internal service error.
503 Service Unavailable	The service is currently unavailable.

Error Codes

See **Error Codes**.

5.3.5 Creating an Alarm Rule

Function

This API is used to create an alarm rule.

NOTE

For API V1, only an alarm rule can be configured for a single resource. You are advised to use **Creating an Alarm Rule (Recommended)** to work with the console.

Debugging

You can debug the API in **API Explorer** which supports automatic authentication. API Explorer can automatically generate and debug example SDK code.

URI

POST /V1.0/{project_id}/alarms

- Parameter description

Table 5-36 Parameter description

Parameter	Mandatory	Description
project_id	Yes	Specifies the project ID. For details about how to obtain the project ID, see **Obtaining a Project ID**.

- Example
  POST https://{Cloud Eye endpoint}/V1.0/{project_id}/alarms

Request

- Request parameters

Table 5-37 Request parameters

Parameter	Mandatory	Type	Description
alarm_name	Yes	String	Specifies the alarm rule name. Enter 1 to 128 characters. Only letters, digits, underscores (_), and hyphens (-) are allowed.
alarm_description	No	String	Provides supplementary information about the alarm rule. Enter 0 to 256 characters.
metric	Yes	Object	Specifies the alarm metric. For details, see **Table 5-38**.
condition	Yes	Object	Specifies the alarm triggering condition. For details, see **Table 5-43**.
alarm_enabled	No	Boolean	Specifies whether to enable the alarm. The default value is **true**.

Parameter	Mandatory	Type	Description
alarm_action_enabled	No	Boolean	Specifies whether to enable the action to be triggered by an alarm. The default value is **true**. **NOTE** If you set **alarm_action_enabled** to **true**, you must specify either **alarm_actions** or **ok_actions**. (You do not need to configure the deprecated parameter **insufficientdata_actions**.) If **alarm_actions** and **ok_actions** coexist, their **notificationList** must be the same. (You do not need to configure the deprecated parameter **insufficientdata_actions**.)
enterprise_project_id	No	String	Specifies the enterprise project ID. Value **0** indicates the default enterprise project **default**.
alarm_level	No	Integer	Specifies the alarm severity, which can be **1**, **2** (default), **3** or **4**, indicating critical, major, minor, and informational, respectively.
alarm_type	No	String	Specifies the alarm rule type. **EVENT.SYS**: The alarm rule is created for system events. **EVENT.CUSTOM**: The alarm rule is created for custom events.

alarm_actions	No	Array of objects	Specifies the action to be triggered by an alarm.
			An example structure is as follows:
			{
			"type": "notification","notificationList": ["urn:smn:region:68438a86d98e427e907e0097b7e35d47:sd"]
			}
			For details, see **Table 5-40**.

Parameter	Mandatory	Type	Description
ok_actions	No	Array of objects	Specifies the action to be triggered after the alarm is cleared. Its structure is: { "type": "notification","notificationList": ["urn:smn:region:68438a86d98e427e907e0097b7e35d47:sd"] } For details, see **Table 5-41**.
insufficientdata_actions	No	Array of objects	Specifies the action to be triggered by the alarm of insufficient data. (You do not need to configure this deprecated parameter.) Its structure is: { "type": "notification","notificationList": ["urn:smn:region:68438a86d98e427e907e0097b7e35d47:sd"] } For details, see **Table 5-42**.

Table 5-38 metric data structure description

Parameter	Mandatory	Type	Description
namespace	Yes	String	Specifies the namespace of a service. For details, see **Services Interconnected with Cloud Eye**. The namespace must be in the **service.item** format and contain 3 to 32 characters. **service** and **item** each must start with a letter and contain only letters, digits, and underscores (_).
dimensions	No	Array of objects	Specifies the metric dimension list. When **resource_group_id** is not used, **dimensions** is mandatory. For details, see **Table 5-39**.

Parameter	Mandatory	Type	Description
metric_name	Yes	String	Specifies the metric name. Start with a letter. Enter 1 to 64 characters. Only letters, digits, and underscores (_) are allowed. For details, see the metric name queried in **Querying Metrics**.
resource_group_id	No	String	Specifies the resource group ID selected during the alarm rule creation, for example, **rg1603786526428bWbVmk4rP**. **NOTE** If you create alarm rules for resource groups, you must specify **resource_group_id** and **name**, enter at least one dimension for **dimensions**, and set **alarm_type** to **RESOURCE_GROUP**.

Table 5-39 dimensions data structure description

Parameter	Mandatory	Type	Description
name	Yes	String	Specifies the dimension. For example, the ECS dimension is **instance_id**. For details about the dimension of each service, see the **key** column in **Services Interconnected with Cloud Eye**. The value must start with a letter. It allows 1 to 32 characters and can only contain letters, digits, underscores (_), and hyphens (-).
value	Yes	String	Specifies the dimension value, for example, an ECS ID. Specifies the dimension value, for example, an ECS ID. The value must start with a letter or digit. It allows 1 to 256 characters and can only contain letters, digits, underscores (_), and hyphens (-).

Table 5-40 alarm_actions data structure description

Parameter	Mandatory	Type	Description
type	Yes	String	Specifies the alarm notification type. • **notification**: A notification will be sent. • **autoscaling**: A scaling action will be triggered.
notificationList	Yes	Array of strings	Specifies the list of objects to be notified if the alarm status changes. You can add up to 5 object IDs. **topicUrn** can be obtained from SMN. For details, see **Querying Topics**. If you set **type** to **notification**, you must specify **notificationList**. If you set **type** to **autoscaling**, you must set **notificationList** to **[]**. **NOTE** • To apply the Auto Scaling (AS) alarm rule, you must bind the scaling policy. For details, see **Creating an AS Policy**. • If you set **alarm_action_enabled** to **true**, you must specify either **alarm_actions** or **ok_actions**. (You do not need to configure the deprecated parameter **insufficientdata_actions**.) • If **alarm_actions** and **ok_actions** coexist, their **notificationList** must be the same. (You do not need to configure the deprecated parameter **insufficientdata_actions**.) • The IDs in the list are strings.

Table 5-41 ok_actions data structure description

Parameter	Mandatory	Type	Description
type	Yes	String	Specifies the notification type when an alarm is triggered. • **notification**: indicates that a notification will be sent. • **autoscaling**: indicates that a scaling action will be triggered.

Parameter	Mandatory	Type	Description
notificationList	Yes	Array of objects	Specifies the list of objects to be notified if the alarm status changes. The list contains a maximum of 5 object IDs. **topicUrn** can be obtained from SMN. For details, see **Querying Topics**. **NOTE** If you set **alarm_action_enabled** to **true**, you must specify either **alarm_actions** or **ok_actions**. (You do not need to configure the deprecated parameter **insufficientdata_actions**.) If **alarm_actions** and **ok_actions** coexist, their **notificationList** must be the same. (You do not need to configure the deprecated parameter **insufficientdata_actions**.)

Table 5-42 insufficientdata_actions data structure description

Parameter	Mandatory	Type	Description
type	Yes	String	Specifies the notification type when an alarm is triggered. • **notification**: indicates that a notification will be sent. • **autoscaling**: indicates that a scaling action will be triggered.
notificationList	Yes	Array of objects	Specifies the list of objects to be notified if the alarm status changes. You can add up to 5 object IDs. **topicUrn** can be obtained from SMN. For details, see **Querying Topics**. **NOTE** • If you set **alarm_action_enabled** to **true**, you must specify either **alarm_actions** or **ok_actions**. (You do not need to configure the deprecated parameter **insufficientdata_actions**.) • If **alarm_actions** and **ok_actions** coexist, their **notificationList** must be the same. (You do not need to configure the deprecated parameter **insufficientdata_actions**.) • The IDs in the list are strings.

Table 5-43 condition data structure description

Parameter	Mandatory	Type	Description
period	Yes	Integer	Specifies the period during which Cloud Eye determines whether to trigger an alarm. Unit: second Possible periods are **1**, **300**, **1200**, **3600**, **14400**, and **86400**. **NOTE** • If you set **period** to **1**, Cloud Eye uses raw data to determine whether to trigger an alarm.
filter	Yes	String	Specifies the data rollup method. Possible methods are **max**, **min**, **average**, **sum**, or **variance**.
comparison_operator	Yes	String	Specifies the alarm threshold operator. Possible operators are >, =, <, >=, and <=.
value	Yes	Double	Specifies the alarm threshold. Supported range: **0** to **Number. MAX_VALUE (1.7976931348623157e+108)** For detailed thresholds, see the value range of each metric in the appendix. For example, you can set ECS **cpu_util** in **Services Interconnected with Cloud Eye** to **80**.
unit	No	String	Specifies the data unit. Enter up to 32 characters.
count	Yes	Integer	Specifies the number of consecutive occurrence times that the alarm policy was met. Supported range: **1** to **5**

Parameter	Mandatory	Type	Description
suppress_duration	No	Integer	Specifies the interval for triggering an alarm if the alarm persists. Possible intervals are as follows: **0**: Cloud Eye triggers the alarm only once. **300**: Cloud Eye triggers the alarm every 5 minutes. **600**: Cloud Eye triggers the alarm every 10 minutes. **900**: Cloud Eye triggers the alarm every 15 minutes. **1800**: Cloud Eye triggers the alarm every 30 minutes. **3600**: Cloud Eye triggers the alarm every hour. **10800**: Cloud Eye triggers the alarm every 3 hours. **21600**: Cloud Eye triggers the alarm every 6 hours. **43200**: Cloud Eye triggers the alarm every 12 hours. **86400**: Cloud Eye triggers the alarm every day.

- Example request 1

  Creating an alarm rule to monitor a metric

```
{
   "alarm_name": "alarm-rp0E",
   "alarm_description": "",
   "metric": {
      "namespace": "SYS.ECS",
      "dimensions": [
         {
            "name": "instance_id",
            "value": "33328f02-3814-422e-b688-bfdba93d4051"
         }
      ],
      "metric_name": "network_outgoing_bytes_rate_inband"
   },
   "condition": {
      "period": 300,
      "filter": "average",
      "comparison_operator": ">=",
      "value": 6,
      "unit": "Byte/s",
      "count": 1
   },
   "alarm_enabled": true,
   "alarm_action_enabled": true,
   "alarm_level": 2,
   "alarm_actions": [
      {
         "type": "notification",
```



```
            "notificationList": ["urn:smn:region:68438a86d98e427e907e0097b7e35d48:sd"]
        }
    ],
    "ok_actions": [
        {
            "type": "notification",
            "notificationList": ["urn:smn:region:68438a86d98e427e907e0097b7e35d48:sd"]
        }
    ],
    "insufficientdata_actions": [
        {
            "type": "notification",
            "notificationList": ["urn:smn:region:68438a86d98e427e907e0097b7e35d48:sd"]
        }
    ]
}
```

- Example request 2

  Creating an alarm rule to monitor an event

```
{
 "alarm_name": "alarm-test",
 "metric": {
  "namespace": "SYS.ECS",
  "metric_name": "instance_resize_scheduled",
  "dimensions": [
   {
    "name": "instance_id",
    "value": "d53692e5-828b-495b-a5e2-a1b227f6034c"
   }
  ]
 },
 "condition": {
  "comparison_operator": ">=",
  "count": 1,
  "filter": "average",
  "period": 0,
  "unit": "count",
  "value": 1
 },
 "alarm_enabled": true,
 "alarm_action_enabled": true,
 "alarm_level": 2,
 "alarm_type": "EVENT.SYS",
 "alarm_actions": [
  {
   "type": "notification",
   "notificationList": ["urn:smn:region:ce8476c174f94c6991ea7885e3380d99:sd"]
  }
 ],
 "ok_actions": [
  {
   "type": "notification",
   "notificationList": ["urn:smn:region:ce8476c174f94c6991ea7885e3380d99:sd"]
  }
 ]
}
```

Response

- Response parameter

  Table 5-44 Parameter description

Parameter	Type	Description
alarm_id	String	Specifies the alarm rule ID.

- Example response

```
{
   "alarm_id":"al1450321795427dR8p5mQBo"
}
```

Returned Values

- Normal

  201

- Abnormal

Returned Value	Description
400 Bad Request	Request error.
401 Unauthorized	The authentication information is not provided or is incorrect.
403 Forbidden	Access to the requested page is forbidden.
408 Request Timeout	The request timed out.
429 Too Many Requests	Concurrent requests are excessive.
500 Internal Server Error	Failed to complete the request because of an internal service error.
503 Service Unavailable	The service is currently unavailable.

Error Codes

See **Error Codes**.

5.3.6 Creating a Custom Alarm Template

Function

This API is used to create a custom alarm template to add alarm rules for one or more metrics.

Debugging

You can debug the API in **API Explorer** which supports automatic authentication. API Explorer can automatically generate and debug example SDK code.

URI

POST /V1.0/{project_id}/alarm-template

- Parameter description

Table 5-45 Parameter description

Parameter	Mandatory	Description
project_id	Yes	Specifies the project ID. For details about how to obtain the project ID, see **Obtaining a Project ID**.

- Example
  POST https://{Cloud Eye endpoint}/V1.0/{project_id}/alarm-template

Request

- Request parameters

Table 5-46 Request parameters

Parameter	Mandatory	Type	Description
template_name	Yes	String	Specifies the name of the custom alarm template. The name can contain 1 to 128 characters. Only letters, digits, underscores (_), and hyphens (-) are allowed.
template_description	No	String	Provides supplementary information about the custom alarm template. The description can contain 0 to 256 characters.
namespace	Yes	String	Specifies the resource type selected for creating the custom alarm template, that is, the service namespace. For example, if you select ECS, **namespace** is **SYS.ECS**. **NOTICE** If you select OS monitoring, **namespace** must be **SYS.ECS**.
dimension_name	Yes	String	Specifies the dimension corresponding to the resource type. If ECS is selected, the dimension is ECS and **dimension_name** is **instance_id**.
template_items	Yes	Array of objects	Specifies the alarm rules that you add to the custom alarm template. You can add up to 20 alarm rules.

Table 5-47 template_items data structure description

Parameter	Mandatory	Type	Description
metric_name	Yes	String	Specifies the metric you add to the custom alarm template. For example, you can add ECS **cpu_util**. To view metrics of each resource, see **Services Interconnected with Cloud Eye**.
condition	Yes	Condition object	Specifies the alarm policy you created for the custom alarm template. For details, see **Table 5-48**.
alarm_level	No	Integer	Specifies the alarm severity. Possible severities are **1** (critical), **2** (major), **3** (minor), and **4** (informational).

Table 5-48 condition data structure description

Parameter	Mandatory	Type	Description
comparison_operator	Yes	String	Specifies the alarm threshold operator, which can be >, =, <, >=, or <=.
count	Yes	Integer	Specifies the number of consecutive occurrence times that the alarm policy was met. Supported range: **1** to **5**
filter	Yes	String	Specifies the data rollup method, which can be **max**, **min**, **average**, **sum**, or **variance**.

Parameter	Mandatory	Type	Description
period	Yes	Integer	Specifies the period during which Cloud Eye determines whether to trigger an alarm. Unit: second Possible periods are **1**, **300**, **1200**, **3600**, **14400**, and **86400**. **NOTE** If you set **period** to **1**, Cloud Eye uses raw data to determine whether to trigger an alarm. You can set this parameter to **0** when you set **alarm_type** to **(EVENT.SYS|EVENT.CUSTOM)**.
unit	No	String	Specifies the data unit. Enter up to 32 characters.
value	Yes	Double	Specifies the alarm threshold, which ranges from **0** to **Number.MAX_VALUE (1.7976931348623157e+108)**. For detailed thresholds, see the value range of each metric in **Services Interconnected with Cloud Eye**. For example, you can set ECS **cpu_util** to **80**.

Parameter	Mandatory	Type	Description
suppress_duration	No	Integer	Specifies the interval for triggering an alarm if the alarm persists. Possible intervals are as follows: **0**: Cloud Eye triggers the alarm only once. **300**: Cloud Eye triggers the alarm every 5 minutes. **600**: Cloud Eye triggers the alarm every 10 minutes. **900**: Cloud Eye triggers the alarm every 15 minutes. **1800**: Cloud Eye triggers the alarm every 30 minutes. **3600**: Cloud Eye triggers the alarm every 1 hour. **10800**: Cloud Eye triggers the alarm every 3 hours. **21600**: Cloud Eye triggers the alarm every 6 hours. **43200**: Cloud Eye triggers the alarm every 12 hours. **86400**: Cloud Eye triggers the alarm every day.

- Example request

```
{
   "template_name": "alarmTemplate-Test01",
   "template_description": "Creating a custom alarm template",
   "namespace": "SYS.ECS",
   "dimension_name": "instance_id",
   "template_items": [
      {
         "metric_name": "cpu_util",
         "condition": {
            "period": 1,
            "filter": "average",
            "comparison_operator": ">=",
            "value": 90,
            "unit": "%",
            "count": 3,
            "suppress_duration": 300
          },
         "alarm_level": 2
      },
      {
         "metric_name": "mem_util",
         "condition": {
            "period": 1,
            "filter": "average",
            "comparison_operator": ">=",
            "value": 90,
            "unit": "%",
```

```
            "count": 3,
            "suppress_duration": 600
        },
        "alarm_level": 2
    }
  ]
}
```

Response

- Response parameters

  Table 5-49 Response parameters

Parameter	Type	Description
template_id	String	Specifies the ID of the custom alarm template.

- Example response

```
{
   "template_id":"at1603252280799wLRyGLxnz"
}
```

Returned Values

- Normal

  201

- Abnormal

Returned Values	Description
400 Bad Request	Request error.
401 Unauthorized	The authentication information is not provided or is incorrect.
403 Forbidden	Access to the requested page is forbidden.
408 Request Timeout	The request timed out.
429 Too Many Requests	Concurrent requests are excessive.
500 Internal Server Error	Failed to complete the request because of an internal service error.
503 Service Unavailable	The service is currently unavailable.

Error Codes

See **Error Codes**.

5.3.7 Deleting a Custom Alarm Template

Function

This API is used to delete a custom alarm template.

Debugging

You can debug the API in **API Explorer** which supports automatic authentication. API Explorer can automatically generate and debug example SDK code.

URI

DELETE /V1.0/{project_id}/alarm-template/{template_id}

- Parameter description

  Table 5-50 Parameter description

Parameter	Mandatory	Description
project_id	Yes	Specifies the project ID. For details about how to obtain the project ID, see **Obtaining a Project ID**.
template_id	Yes	Specifies the ID of the custom alarm template you want to delete.

- Example
  DELETE https://{Cloud Eye endpoint}/V1.0/{project_id}/alarm-template/at1603252280799wLRyGLxnz

Request

The request has no message body.

Response

The response has no message body.

Returned Values

- Normal

  204

- Abnormal

Returned Value	Description
400 Bad Request	Request error.
401 Unauthorized	The authentication information is not provided or is incorrect.

Returned Value	Description
403 Forbidden	Access to the requested page is forbidden.
408 Request Timeout	The request timed out.
429 Too Many Requests	Concurrent requests are excessive.
500 Internal Server Error	Failed to complete the request because of an internal service error.
503 Service Unavailable	The service is currently unavailable.

Error Codes

See **Error Codes**.

5.3.8 Querying the Alarm History of an Alarm Rule

Function

This API is used to query the alarm history of an alarm rule based on the alarm rule ID.

Debugging

You can debug the API in **API Explorer** which supports automatic authentication. API Explorer can automatically generate and debug example SDK code.

URI

GET /V1.0/{project_id}/alarm-histories

- Parameter description

Table 5-51 Parameter description

Parameter	Mandatory	Description
project_id	Yes	Specifies the project ID. For details about how to obtain the project ID, see **Obtaining a Project ID**.
group_id	No	Specifies the resource group ID, for example, **rg1603107497873DK4O2pXbn**.
alarm_id	No	Specifies the alarm rule ID, for example, **al1603088932912v98rGl1al**.
alarm_name	No	Specifies the alarm rule name, for example, **alarm-test01**.

Parameter	Mandatory	Description
alarm_status	No	Specifies the alarm status, which can be **ok**, **alarm**, or **insufficient_data**.
alarm_level	No	Specifies the alarm severity, which can be **1** (critical), **2** (major), **3** (minor), or **4** (informational).
namespace	No	Specifies the resource namespace. For example, the ECS namespace is **SYS.ECS**. To view the namespace of each service, see **Services Interconnected with Cloud Eye**.
from	No	Specifies the time from when you want to query the alarm history. The time is a UNIX timestamp (ms), for example, **1602501480905**. If you do not configure **from** or **to**, **to** is the current time by default, and **from** is the timestamp of seven days earlier than the current time.
to	No	Specifies when you want your alarm history query to end. The time is a UNIX timestamp (ms). The value of **from** can be **to** or smaller. If you do not configure **from** or **to**, **to** is the current time by default, and **from** is the timestamp of seven days earlier than the current time.
start	No	Specifies the start value of pagination. The value is an integer. The default value is **0**.
limit	No	Specifies the maximum number of records that can be queried at a time. Supported range: **1** to **100** (default)

- Example

```
GET https://{Cloud Eye endpoint}/V1.0/{project_id}/alarm-histories?
limit=10&start=0&from=1602494921346&to=1603099721346&alarm_name=alarm-test01
```

Request

None

Response

- Response parameters

Parameter	Type	Mandatory	Description
alarm_histories	Array of objects	No	Specifies details about one or more alarm history records. For details, see **Table 5-52**.
meta_data	MetaData object	No	Specifies the total number of query results returned. For details, see **Table 5-61**.

Table 5-52 alarm_histories data structure description

Parameter	Type	Mandatory	Description
alarm_id	String	No	Specifies the alarm rule ID, for example, **al1603131199286dzxpqK3Ez**.
alarm_name	String	No	Specifies the alarm rule name, for example, **alarm-test01**.
alarm_description	String	No	Provides supplementary information about the alarm rule.
metric	Metric object	No	Specifies the metric information. For details, see **Table 5-53**.
condition	Condition object	No	Specifies the alarm policy set in the alarm rule. For details, see **Table 5-58**.
alarm_level	Integer	No	Specifies the alarm severity, which can be **1** (critical), **2** (major), **3** (minor), or **4** (informational).
alarm_type	String	No	Specifies the alarm rule type. This parameter applies only to event alarms. The types are as follows: **EVENT.SYS**: system event alarm **EVENT.CUSTOM**: custom event alarm **DNSHealthCheck**: DNS health check alarm **RESOURCE_GROUP**: resource group alarm **MULTI_INSTANCE**: alarm for a specific resource

Parameter	Type	Mandatory	Description
alarm_enabled	Boolean	No	Specifies whether the alarm rule has been enabled. Possible values are **true** and **false**.
alarm_action_enabled	Boolean	No	Specifies whether the alarm action has been triggered. Possible values are **true** and **false**.
alarm_actions	Array of objects	No	Specifies the action to be triggered by an alarm. The structure is as follows: {"type": "notification", "notificationList": ["urn:smn:southchina:68438a86d98e427e907e0097b7e35d47:sd"] } The value of **type** can be one of the following: **notification**: indicates that a notification will be sent. **autoscaling**: indicates that a scaling action will be triggered. **notificationList**: indicates the list of objects to be notified if the alarm status changes. For details, see **Table 5-55**.
ok_actions	Array of objects	No	Specifies the action to be triggered after the alarm is cleared. The structure is as follows: {"type": "notification", "notificationList": ["urn:smn:southchina:68438a86d98e427e907e0097b7e35d47:sd"] } The value of **type** can be one of the following: **notification**: indicates that a notification will be sent. **notificationList**: indicates the list of objects to be notified if the alarm status changes. For details, see **Table 5-56**.

Parameter	Type	Mandatory	Description
insufficientdata_actions	Array of objects	No	Specifies the action triggered by data insufficiency. The structure is as follows: {"type": "notification", "notificationList": ["urn:smn:southchina:68438a86d98e427e907e0097b7e35d47:sd"]} The value of **type** can be one of the following: **notification**: An alarm is triggered due to insufficient data. **notificationList**: Specifies the ID list of the notification objects when an alarm notification is triggered due to insufficient data. For details, see **Table 5-57**.
update_time	Long	No	Specifies when the alarm status changed. The time is a UNIX timestamp (ms), for example, **1603131199000**.
enterprise_project_id	String	No	Specifies the enterprise project ID. Value **all_granted_eps** indicates all enterprise projects. Value **0** indicates enterprise project **default**.
trigger_time	Long	No	Specifies when the alarm was triggered. The time is a UNIX timestamp (ms), for example, **1603131199469**.
alarm_status	String	No	Specifies the alarm status, which can be **ok**, **alarm**, or **insufficient_data**.
datapoints	Array of objects	No	Specifies when the monitoring data of the alarm history is reported and the monitoring data that is calculated. For details, see **Table 5-59**.
additional_info	AdditionalInfo object	No	Specifies the additional field of the alarm history, which applies only to the alarm history generated for event monitoring. For details, see **Table 5-60**.

Table 5-53 metric data structure description

Parameter	Type	Mandatory	Description
dimensions	Array of objects	No	Specifies the metric dimension. For details, see **Table 5-54**.
metric_name	String	No	Specifies the metric name. Start with a letter. Enter 1 to 64 characters. Only letters, digits, and underscores (_) are allowed. For details, see the metric name queried in **Services Interconnected with Cloud Eye**.
namespace	String	No	Specifies the metric namespace in **service.item** format. **service** and **item** each must contain 3 to 32 characters, start with a letter, and contain only letters, digits, and underscores (_). **NOTE** You can leave this parameter blank when you set **alarm_type** to **(EVENT.SYS|EVENT.CUSTOM)**.

Table 5-54 dimensions data structure description

Parameter	Type	Mandatory	Description
name	String	No	Specifies the monitoring dimension name. For example, the ECS dimension is **instance_id**. For details about the dimension of each service, see the **key** column in **Services Interconnected with Cloud Eye**.
value	String	No	Dimension value, for example, an ECS ID. Enter 1 to 256 characters.

Table 5-55 alarm_actions data structure description

Parameter	Type	Mandatory	Description
type	String	Yes	Specifies the alarm notification type. • **notification**: indicates that a notification will be sent. • **autoscaling**: indicates that a scaling action will be triggered.
notificationList	Array of strings	Yes	Specifies the list of objects to be notified if the alarm status changes. **NOTE** The IDs in the list are strings. You can configure up to 5 object IDs.

Table 5-56 ok_actions data structure description

Parameter	Type	Mandatory	Description
type	String	Yes	Specifies the alarm notification type. • **notification**: indicates that a notification will be sent. • **autoscaling**: indicates that a scaling action will be triggered.
notificationList	Array of strings	Yes	Specifies the list of objects to be notified if the alarm status changes. **NOTE** The IDs in the list are strings. You can configure up to 5 object IDs.

Table 5-57 insufficientdata_actions data structure description

Parameter	Type	Mandatory	Description
type	String	Yes	Specifies the alarm notification type. • **notification**: indicates that a notification will be sent. • **autoscaling**: indicates that a scaling action will be triggered.

Parameter	Type	Mandatory	Description
notificationList	Array of strings	Yes	Specifies the list of objects to be notified if the alarm status changes. **NOTE** The IDs in the list are strings. You can configure up to 5 object IDs.

Table 5-58 condition data structure description

Parameter	Type	Mandatory	Description
period	Integer	No	Specifies how often Cloud Eye aggregates data, which can be • **1**: Cloud Eye performs no aggregation and displays raw data. • **300**: Cloud Eye aggregates data every 5 minutes. • **1200**: Cloud Eye aggregates data every 20 minutes. • **3600**: Cloud Eye aggregates data every hour. • **14400**: Cloud Eye aggregates data every 4 hours. • **86400**: Cloud Eye aggregates data every 24 hours. **NOTE** If you set **period** to **1**, Cloud Eye uses raw data to determine whether to trigger an alarm. You can set this parameter to **0** when you set **alarm_type** to **(EVENT.SYS| EVENT.CUSTOM)**.
filter	String	No	Specifies the data rollup method, which can be • **average**: average value of metric data within an aggregation period. • **max**: maximum value of metric data in an aggregation period. • **min**: minimum value of metric data within an aggregation period. • **sum**: sum of metric data within an aggregation period. • **variance**: variance value of metric data within an aggregation period.

Parameter	Type	Mandatory	Description
comparison_operator	String	No	Specifies the alarm threshold operator, which can be >, =, <, >=, or <=.
value	Double	Yes	Specifies the alarm threshold. Supported range: **0** to **Number. MAX_VALUE (1.7976931348623157e+108)** For detailed thresholds, see the value range of each metric in the appendix. For example, you can set ECS **cpu_util** in **Services Interconnected with Cloud Eye** to **80**.
unit	String	No	Specifies the data unit. Enter up to 32 characters.
count	Integer	No	Specifies the number of consecutive occurrence times that the alarm policy was met. Supported range: **1** to **5**
suppress_duration	Integer	No	Specifies the interval for triggering an alarm if the alarm persists. Possible intervals are as follows: **0**: Cloud Eye triggers the alarm only once. **300**: Cloud Eye triggers the alarm every 5 minutes. **600**: Cloud Eye triggers the alarm every 10 minutes. **900**: Cloud Eye triggers the alarm every 15 minutes. **1800**: Cloud Eye triggers the alarm every 30 minutes. **3600**: Cloud Eye triggers the alarm every hour. **10800**: Cloud Eye triggers the alarm every 3 hours. **21600**: Cloud Eye triggers the alarm every 6 hours. **43200**: Cloud Eye triggers the alarm every 12 hours. **86400**: Cloud Eye triggers the alarm every day.

Table 5-59 datapoints data structure description

Parameter	Type	Mandatory	Description
time	Long	No	Specifies when the monitoring data of the alarm history is reported, which is a UNIX timestamp in milliseconds, for example, **1603131028000**.
value	Double	No	Specifies the calculated monitoring data of the alarm history, for example, **7.019**.

Table 5-60 additional_info data structure description

Parameter	Type	Mandatory	Description
resource_id	String	No	Specifies the resource ID corresponding to the alarm history, for example, **22d98f6c-16d2-4c2d-b424-50e79d82838f**.
resource_name	String	No	Specifies the resource name corresponding to the alarm history, for example, **ECS-Test01**.
event_id	String	No	Specifies the event ID of the alarm history, for example, **ev16031292300990kKN8p17J**.

Table 5-61 meta_data data structure description

Parameter	Type	Mandatory	Description
total	Integer	Yes	Specifies the total number of query results.

- Example response

```
{
 "alarm_histories": [
  {
    "alarm_id": "al1604473987569z6n6nkpm1",
    "alarm_name": "TC_CES_FunctionBaseline_Alarm_008",
    "alarm_description": "",
    "metric": {
      "namespace": "SYS.VPC",
      "dimensions": [
        {
          "name": "bandwidth_id",
          "value": "79a9cc0c-f626-4f15-bf99-a1f184107f88"
        }
      ],
```

```
      "metric_name": "downstream_bandwidth"
    },
    "condition": {
      "period": 1,
      "filter": "average",
      "comparison_operator": ">=",
      "value": 0,
      "count": 3
    },
    "alarm_level": 2,
    "alarm_type": "",
    "alarm_enabled": false,
    "alarm_action_enabled": false,
    "alarm_actions": [],
    "ok_actions": [],
    "insufficientdata_actions": [],
    "update_time": 1604473988000,
    "enterprise_project_id": "0",
    "trigger_time": 1604473987607,
    "alarm_status": "alarm",
    "datapoints": [
      {
        "time": 1604473860000,
        "value": 0
      },
      {
        "time": 1604473800000,
        "value": 0
      },
      {
        "time": 1604473740000,
        "value": 0
      }
    ],
    "additional_info": {
      "resource_id": "",
      "resource_name": "",
      "event_id": ""
    }
  },
  {
    "alarm_id": "al1604473978613MvlvlbVZD",
    "alarm_name": "alarm_merge",
    "alarm_description": "",
    "metric": {
      "namespace": "AGT.ECS",
      "dimensions": [
        {
          "name": "instance_id",
          "value": "22d98f6c-16d2-4c2d-b424-50e79d82838f"
        }
      ],
      "metric_name": "load_average5",
      "resource_group_id": "rg16044739783733030 3XQbK",
      "resource_group_name": "group1"
    },
    "condition": {
      "period": 1,
      "filter": "average",
      "comparison_operator": ">=",
      "value": 0,
      "count": 3
    },
    "alarm_level": 2,
    "alarm_type": "RESOURCE_GROUP",
    "alarm_enabled": false,
    "alarm_action_enabled": false,
    "alarm_actions": [],
    "ok_actions": [],
```

```
    "insufficientdata_actions": [],
    "update_time": 1604473979000,
    "enterprise_project_id": "0",
    "trigger_time": 1604473979070,
    "alarm_status": "insufficient_data",
    "datapoints": [],
    "additional_info": {
      "resource_id": "",
      "resource_name": "",
      "event_id": ""
    }
  }
 ],
 "meta_data": {
  "total": 2
 }
}
```


Returned Values

- Normal

  200

- Abnormal

Returned Value	Description
400 Bad Request	Request error.
401 Unauthorized	The authentication information is not provided or is incorrect.
403 Forbidden	Access to the requested page is forbidden.
408 Request Timeout	The request timed out.
429 Too Many Requests	Concurrent requests are excessive.
500 Internal Server Error	Failed to complete the request because of an internal service error.
503 Service Unavailable	The service is currently unavailable.

Error Codes

See **Error Codes**.

5.3.9 Querying Custom Alarm Templates

Function

This API is used to query the custom alarm templates.

Debugging

You can debug the API in **API Explorer** which supports automatic authentication. API Explorer can automatically generate and debug example SDK code.

URI

GET /V1.0/{project_id}/alarm-template

- Parameter description

  Table 5-62 Parameter description

Parameter	Type	Mandatory	Description
project_id	String	Yes	Specifies the project ID. For details about how to obtain the project ID, see **Obtaining a Project ID**.
alarmTemplateId	String	No	Specifies the ID of the custom alarm template, for example, **at1603330892378wkDm77y6B**.
namespace	String	No	Specifies the resource namespace. For example, the ECS namespace is **SYS.ECS**. To view the namespace of each service, see **Services Interconnected with Cloud Eye**.
dname	String	No	Specifies the resource dimension selected for the custom alarm template. For example, the ECS dimension is **instance_id**. For details about the dimensions of each service, see **Services Interconnected with Cloud Eye**.
start	String	No	Specifies the start value of pagination. The value is an integer. The default value is **0**.
limit	String	No	Specifies the maximum number of the custom alarm template that can be queried at a time. The value range is (0,100] and the default value is **100**.

- Example

```
GET https://{Cloud Eye endpoint}/V1.0/{project_id}/alarm-template
```

Request

None

Response

- Response parameters

Parameter	Type	Mandatory	Description
alarm_templates	Array of objects	No	Provides supplementary information about the custom alarm template. For details, see **Table 5-63**.
meta_data	MetaData object	No	Specifies the metadata of query results, including the pagination information. For details, see **Table 5-66**.

Table 5-63 alarm_templates data structure description

Parameter	Type	Mandatory	Description
template_name	String	No	Specifies the custom alarm template name, for example, **alarmTemplate-Test01**.
template_description	String	No	Provides supplementary information about the custom alarm template.
namespace	String	No	Specifies the resource namespace. For example, the ECS namespace is **SYS.ECS**. To view the namespace of each service, see **Services Interconnected with Cloud Eye**.
dimension_name	String	No	Specifies the resource dimension selected for the custom alarm template. For example, the ECS dimension is **instance_id**. For details about the dimensions of each service, see **Services Interconnected with Cloud Eye**.
template_items	Array of objects	No	Specifies the alarm policy or alarm policies added to the custom alarm template. For details, see **Table 5-64**.
template_id	String	No	Specifies the ID of the custom alarm template, for example, **at1603330892378wkDm77y6B**.

Table 5-64 template_items data structure description

Parameter	Type	Mandatory	Description
metric_name	String	Yes	Specifies the metric you add to the custom alarm template. For example, you can add ECS **cpu_util**. To view metrics of each resource, see **Services Interconnected with Cloud Eye**.
condition	Condition object	Yes	Specifies the alarm policy you created for the custom alarm template. For details, see **Table 5-65**.
alarm_level	Integer	No	Specifies the alarm severity, which can be **1** (critical), **2** (major), **3** (minor), or **4** (informational).

Table 5-65 condition data structure description

Parameter	Type	Mandatory	Description
period	Integer	Yes	Specifies how often Cloud Eye aggregates data. Possible values: • **1**: Cloud Eye performs no aggregation and displays raw data. • **300**: Cloud Eye aggregates data every 5 minutes. • **1200**: Cloud Eye aggregates data every 20 minutes. • **3600**: Cloud Eye aggregates data every 1 hour. • **14400**: Cloud Eye aggregates data every 4 hours. • **86400**: Cloud Eye aggregates data every 24 hours.

Parameter	Type	Mandatory	Description
filter	String	Yes	Specifies the data rollup method. The following methods are supported: • **average**: average value of metric data within an aggregation period. • **max**: maximum value of metric data in an aggregation period. • **min**: minimum value of metric data within an aggregation period. • **sum**: sum of metric data within an aggregation period. • **variance**: variance value of metric data within an aggregation period.
comparison_operator	String	Yes	Specifies the alarm threshold operator, which can be >, =, <, ≥, or ≤.
value	Double	Yes	Specifies the alarm threshold. Supported range: **0** to **Number. MAX_VALUE (1.7976931348623157e+108)** For detailed thresholds, see the value range of each metric in the appendix. For example, you can set ECS **cpu_util** to **80**.
unit	String	No	Specifies the data unit, which can contain up to 32 characters.
count	Integer	Yes	Specifies the number of consecutive occurrence times that the alarm policy was met. Supported range: **1** to **5**

Parameter	Type	Mandatory	Description
suppress_duration	Integer	No	Specifies the interval for triggering an alarm if the alarm persists. Possible intervals are as follows: **0**: Cloud Eye triggers the alarm only once. **300**: Cloud Eye triggers the alarm every 5 minutes. **600**: Cloud Eye triggers the alarm every 10 minutes. **900**: Cloud Eye triggers the alarm every 15 minutes. **1800**: Cloud Eye triggers the alarm every 30 minutes. **3600**: Cloud Eye triggers the alarm every 1 hour. **10800**: Cloud Eye triggers the alarm every 3 hours. **21600**: Cloud Eye triggers the alarm every 6 hours. **43200**: Cloud Eye triggers the alarm every 12 hours. **86400**: Cloud Eye triggers the alarm every day.

Table 5-66 meta_data data structure description

Parameter	Type	Mandatory	Description
total	Integer	Yes	Specifies the total number of query results.
count	Integer	Yes	Specifies the number of returned results.
marker	String	Yes	Specifies the pagination marker.

- Response example

```
{
 "alarm_templates": [
  {
    "template_name": "alarmTemplate-Test01",
    "template_description": "Querying custom templates",
    "namespace": "SYS.ECS",
    "dimension_name": "instance_id",
    "template_items": [
```

```
    {
      "metric_name": "cpu_util",
      "condition": {
        "period": 1,
        "filter": "average",
        "comparison_operator": ">=",
        "value": 90,
        "unit": "%",
        "count": 3,
        "suppress_duration": 300
      },
      "alarm_level": 2
    },
    {
      "metric_name": "mem_util",
      "condition": {
        "period": 1,
        "filter": "average",
        "comparison_operator": ">=",
        "value": 90,
        "unit": "%",
        "count": 3,
        "suppress_duration": 600
      },
      "alarm_level": 2
    }
   ],
   "template_id": "at1604474818207Jo7o7R4Nj"
  }
 ],
 "meta_data": {
  "count": 1,
  "marker": "",
  "total": 1
 }
}
```

Returned Value

- Normal

  200

- Abnormal

Returned Value	Description
400 Bad Request	Request error.
401 Unauthorized	The authentication information is not provided or is incorrect.
403 Forbidden	Access to the requested page is forbidden.
408 Request Timeout	The request timed out.
429 Too Many Requests	Concurrent requests are excessive.
500 Internal Server Error	Failed to complete the request because of an internal service error.
503 Service Unavailable	The service is currently unavailable.

Error Codes

See **Error Codes**.

5.3.10 Updating a Custom Alarm Template

Function

This API is used to update a custom alarm template.

Debugging

You can debug the API in **API Explorer** which supports automatic authentication. API Explorer can automatically generate and debug example SDK code.

URI

PUT /V1.0/{project_id}/alarm-template/{template_id}

- Parameter description

  Table 5-67 Parameter description

Parameter	Mandatory	Description
project_id	Yes	Specifies the project ID. For details about how to obtain the project ID, see **Obtaining a Project ID**.
template_id	Yes	Specifies the ID of the custom alarm template you want to update.

- Example

```
PUT https://{Cloud Eye endpoint}/V1.0/{project_id}/alarm-template/{template_id}
```

Request

- Request parameters

  Table 5-68 Request parameters

Parameter	Mandatory	Type	Description
template_name	Yes	String	Specifies the name of the custom alarm template. The name can contain 1 to 128 characters. Only letters, digits, underscores (_), and hyphens (-) are allowed.

Parameter	Mandatory	Type	Description
template_description	No	String	Provides supplementary information about the custom alarm template. The description can contain 0 to 256 characters.
namespace	Yes	String	Specifies the resource type selected for creating the custom alarm template, that is, the service namespace. For example, if you select ECS, **namespace** is **SYS.ECS**.
dimension_name	Yes	String	Specifies the dimension corresponding to the resource type. If ECS is selected, the dimension is ECS and **dimension_name** is **instance_id**.
template_items	Yes	Array of objects	Specifies the alarm rules that you add to the custom alarm template. You can add up to 20 alarm rules. For details, see **Table 5-69**.

Table 5-69 template_items data structure description

Parameter	Mandatory	Type	Description
metric_name	Yes	String	Specifies the metric you add to the custom alarm template. For example, you can add ECS **cpu_util**. To view metrics of each resource, see **Services Interconnected with Cloud Eye**.
condition	Yes	Condition object	Specifies the alarm policy you created for the custom alarm template. For details, see **Table 5-70**.
alarm_level	No	Integer	Specifies the alarm severity. Possible severities are **1** (critical), **2** (major), **3** (minor), and **4** (informational).

Table 5-70 condition data structure description

Parameter	Mandatory	Type	Description
comparison_operator	Yes	String	Specifies the alarm threshold operator, which can be >, =, <, >=, or <=.
count	Yes	Integer	Specifies the number of consecutive occurrence times that the alarm policy was met. Supported range: **1** to **5**
filter	Yes	String	Specifies the data rollup method, which can be **max**, **min**, **average**, **sum**, or **variance**.
period	Yes	Integer	Specifies how often Cloud Eye aggregates data. Possible values: • **1**: Cloud Eye performs no aggregation and displays raw data. • **300**: Cloud Eye aggregates data every 5 minutes. • **1200**: Cloud Eye aggregates data every 20 minutes. • **3600**: Cloud Eye aggregates data every hour. • **14400**: Cloud Eye aggregates data every 4 hours. • **86400**: Cloud Eye aggregates data every 24 hours.
unit	No	String	Specifies the data unit. Enter up to 32 characters.
value	Yes	Double	Specifies the alarm threshold. Supported range: **0** to **Number.MAX_VALUE (1.7976931348623157e+108)** For detailed thresholds, see the value range of each metric in **Services Interconnected with Cloud Eye**. For example, you can set ECS **cpu_util** to **80**.

Parameter	Mandatory	Type	Description
suppress_duration	No	Integer	Specifies the interval for triggering an alarm if the alarm persists. Possible intervals are as follows: **0**: Cloud Eye triggers the alarm only once. **300**: Cloud Eye triggers the alarm every 5 minutes. **600**: Cloud Eye triggers the alarm every 10 minutes. **900**: Cloud Eye triggers the alarm every 15 minutes. **1800**: Cloud Eye triggers the alarm every 30 minutes. **3600**: Cloud Eye triggers the alarm every hour. **10800**: Cloud Eye triggers the alarm every 3 hours. **21600**: Cloud Eye triggers the alarm every 6 hours. **43200**: Cloud Eye triggers the alarm every 12 hours. **86400**: Cloud Eye triggers the alarm every day.

- Example request

```
{
  "template_name": "alarmTemplate-Test01",
  "template_description": "Updating a custom alarm template",
  "namespace": "SYS.ECS",
  "dimension_name": "instance_id",
  "template_items": [
    {
      "metric_name": "cpu_util",
      "condition": {
        "period": 1,
        "filter": "average",
        "comparison_operator": ">=",
        "value": 90,
        "unit": "%",
        "count": 3,
        "suppress_duration": 300
      },
      "alarm_level": 2
    },
    {
      "metric_name": "mem_util",
      "condition": {
        "period": 1,
        "filter": "average",
        "comparison_operator": ">=",
        "value": 90,
        "unit": "%",
```

```
            "count": 3,
            "suppress_duration": 600
        },
        "alarm_level": 2
    }
  ]
}
```

Response

The response has no message body.

Returned Values

- Normal

  204

- Abnormal

Returned Values	Description
400 Bad Request	Request error.
401 Unauthorized	The authentication information is not provided or is incorrect.
403 Forbidden	Access to the requested page is forbidden.
408 Request Timeout	The request timed out.
429 Too Many Requests	Concurrent requests are excessive.
500 Internal Server Error	Failed to complete the request because of an internal service error.
503 Service Unavailable	The service is currently unavailable.

Error Codes

See **Error Codes**.

5.3.11 Modifying an Alarm Rule

Function

This API is used to modify an alarm rule.

NOTE

For API V1, only an alarm rule can be configured for a single resource. You are advised to use **Batch Adding Resources to an Alarm Rule**, **Batch Deleting Resources from an Alarm Rule**, and **Modifying All Fields in an Alarm Policy** to work with the console.

Debugging

You can debug the API in **API Explorer** which supports automatic authentication. API Explorer can automatically generate and debug example SDK code.

URI

PUT /V1.0/{project_id}/alarms/{alarm_id}

- Parameter description

  Table 5-71 Parameter description

Parameter	Mandatory	Description
project_id	Yes	Specifies the project ID. For details about how to obtain the project ID, see **Obtaining a Project ID**.
alarm_id	Yes	Specifies the alarm rule ID.

- Example

```
PUT https://{Cloud Eye endpoint}/V1.0/{project_id}/alarms/{alarm_id}
```

Request

- Request parameters

  Table 5-72 Parameter description

Parameter	Mandatory	Type	Description
alarm_name	No	String	Specifies the alarm rule name. Only letters, digits, underscores (_), and hyphens (-) are allowed.
alarm_description	No	String	Provides supplementary information about the alarm rule. Enter 0 to 256 characters.
condition	No	Condition object	Specifies the alarm policy set in the alarm rule. For details, see **Table 5-73**.

Parameter	Mandatory	Type	Description
alarm_action_enabled	No	Boolean	Specifies whether to enable the action to be triggered by an alarm. The default value is **true**. **NOTE** If you set **alarm_action_enabled** to **true**, you must specify either **alarm_actions** or **ok_actions**. If **alarm_actions** and **ok_actions** coexist, their **notificationList** must be the same.
alarm_level	No	Integer	Specifies the alarm severity, which can be **1**, **2** (default), **3** or **4**, indicating critical, major, minor, and informational, respectively.
alarm_type	No	String	Specifies the alarm rule type. The following enumeration types are supported: **EVENT.SYS**: The alarm rule is created for system events. **EVENT.CUSTOM**: The alarm rule is created for custom events. **RESOURCE_GROUP**: The alarm rule is created for resource groups.
alarm_actions	No	Array of objects	Specifies the action to be triggered by an alarm. The structure is as follows: { "type": "notification","notificationList": ["urn:smn:southchina:68438a86d98e427e907e0097b7e35d47:sd"] } Possible values of **type** are as follows: **notification**: indicates that a notification will be sent. **autoscaling**: indicates that a scaling action will be triggered. For details, see **Table 5-74**.
insufficient_data_actions	No	Array of objects	Specifies the action to be triggered by the alarm of insufficient data. (You do not need to configure this deprecated parameter.) For details, see **Table 5-76**.
ok_actions	No	Array of objects	Specifies the action to be triggered after the alarm is cleared. For details, see **Table 5-75**.

Table 5-73 condition data structure description

Parameter	Mandatory	Type	Description
period	Yes	Integer	Specifies how often Cloud Eye aggregates data, which can be • **1**: Cloud Eye performs no aggregation and displays raw data. • **300**: Cloud Eye aggregates data every 5 minutes. • **1200**: Cloud Eye aggregates data every 20 minutes. • **3600**: Cloud Eye aggregates data every hour. • **14400**: Cloud Eye aggregates data every 4 hours. • **86400**: Cloud Eye aggregates data every 24 hours.
filter	Yes	String	Specifies the data rollup method, which can be • **average**: average value of metric data within an aggregation period. • **max**: maximum value of metric data in an aggregation period. • **min**: minimum value of metric data within an aggregation period. • **sum**: sum of metric data within an aggregation period. • **variance**: variance value of metric data within an aggregation period.
comparison_operator	Yes	String	Specifies the alarm threshold operator, which can be **>**, **=**, **<**, **>=**, or **<=**.
value	Yes	Double	Specifies the alarm threshold. Supported range: **0** to **Number.MAX_VALUE (1.7976931348623157e+108)** For detailed thresholds, see the value range of each metric in the appendix. For example, you can set ECS **cpu_util** to **80**.
unit	No	String	Specifies the data unit. Enter up to 32 characters.

Parameter	Mandatory	Type	Description
count	Yes	Integer	Specifies the number of consecutive occurrence times that the alarm policy was met. Supported range: **1** to **5**
suppress_duration	No	Integer	Specifies the interval for triggering an alarm if the alarm persists. Possible intervals are as follows: **0**: Cloud Eye triggers the alarm only once. **300**: Cloud Eye triggers the alarm every 5 minutes. **600**: Cloud Eye triggers the alarm every 10 minutes. **900**: Cloud Eye triggers the alarm every 15 minutes. **1800**: Cloud Eye triggers the alarm every 30 minutes. **3600**: Cloud Eye triggers the alarm every hour. **10800**: Cloud Eye triggers the alarm every 3 hours. **21600**: Cloud Eye triggers the alarm every 6 hours. **43200**: Cloud Eye triggers the alarm every 12 hours. **86400**: Cloud Eye triggers the alarm every day.

Table 5-74 alarm_actions data structure description

Parameter	Mandatory	Type	Description
type	Yes	String	Specifies the alarm notification type. • **notification**: indicates that a notification will be sent. • **autoscaling**: indicates that a scaling action will be triggered.

Parameter	Mandatory	Type	Description
notificationList	Yes	Array of strings	Specifies the list of objects to be notified if the alarm status changes. You can add up to 5 object IDs. **topicUrn** can be obtained from SMN. For details, see **Querying Topics**. If you set **type** to **notification**, you must specify **notificationList**. If you set **type** to **autoscaling**, you must set **notificationList** to **[]**. **NOTE** • To apply the Auto Scaling (AS) alarm rule, you must bind the scaling policy. For details, see **Creating an AS Policy**. • If you set **alarm_action_enabled** to **true**, you must specify either **alarm_actions** or **ok_actions**. (You do not need to configure the deprecated parameter **insufficientdata_actions**.) • If **alarm_actions** and **ok_actions** coexist, their **notificationList** must be the same. (You do not need to configure the deprecated parameter **insufficientdata_actions**.) • The IDs in the list are strings.

Table 5-75 ok_actions data structure description

Parameter	Mandatory	Type	Description
type	Yes	String	Specifies the notification type when an alarm is triggered. • **notification**: indicates that a notification will be sent. • **autoscaling**: indicates that a scaling action will be triggered.

Parameter	Mandatory	Type	Description
notificationList	Yes	Array of objects	Specifies the list of objects to be notified if the alarm status changes. The list contains a maximum of 5 object IDs. **topicUrn** can be obtained from SMN. For details, see **Querying Topics**. **NOTE** If you set **alarm_action_enabled** to **true**, you must specify either **alarm_actions** or **ok_actions**. (You do not need to configure the deprecated parameter **insufficientdata_actions**.) If **alarm_actions** and **ok_actions** coexist, their **notificationList** must be the same. (You do not need to configure the deprecated parameter **insufficientdata_actions**.)

Table 5-76 insufficientdata_actions data structure description

Parameter	Mandatory	Type	Description
type	Yes	String	Specifies the notification type when an alarm is triggered. • **notification**: indicates that a notification will be sent. • **autoscaling**: indicates that a scaling action will be triggered.

Parameter	Mandatory	Type	Description
notificationList	Yes	Array of objects	Specifies the list of objects to be notified if the alarm status changes. You can add up to 5 object IDs. **topicUrn** can be obtained from SMN. For details, see **Querying Topics**. **NOTE** • If you set **alarm_action_enabled** to **true**, you must specify either **alarm_actions** or **ok_actions**. (You do not need to configure the deprecated parameter **insufficientdata_actions**.) • If **alarm_actions** and **ok_actions** coexist, their **notificationList** must be the same. (You do not need to configure the deprecated parameter **insufficientdata_actions**.) • The IDs in the list are strings.

- Example request

```
{
  "alarm_name": "alarm-update-test01",
  "alarm_description": "alarm-update-test01",
  "condition": {
      "comparison_operator": ">=",
      "count": 3,
      "filter": "average",
      "period": 1,
      "value": 95
  },
  "alarm_action_enabled": false,
  "alarm_level": 2
}
```

Returned Values

- Normal

  204

- Abnormal

Returned Value	Description
400 Bad Request	Request error.
401 Unauthorized	The authentication information is not provided or is incorrect.
403 Forbidden	Access to the requested page is forbidden.
408 Request Timeout	The request timed out.

Returned Value	Description
429 Too Many Requests	Concurrent requests are excessive.
500 Internal Server Error	Failed to complete the request because of an internal service error.
503 Service Unavailable	The service is currently unavailable.

Error Codes

See **Error Codes**.

5.4 Monitoring Data

5.4.1 Querying Monitoring Data of a Metric

Function

This API is used to query the monitoring data of a specified metric at a specified granularity in a specified time range. You can specify the dimension of data to be queried.

Debugging

You can debug the API in **API Explorer** which supports automatic authentication. API Explorer can automatically generate and debug example SDK code.

URI

GET /V1.0/{project_id}/metric-data

Example:

```
GET /V1.0/{project_id}/metric-data?namespace={namespace}&metric_name={metric_name}&dim.{i}=key,value&from={from}&to={to}&period={period}&filter={filter}
```

- Parameter description

Table 5-77 Parameter description

Parameter	Mandatory	Description
project_id	Yes	**Definition** Project ID, which is used to specify the project that an asset belongs to. You can query the assets of a project by project ID. You can obtain the project ID from the API or console. For details about how to obtain the project ID, see **Obtaining a Project ID**. **Constraints** N/A **Range** 1 to 64 characters **Default Value** N/A

Table 5-78 Query parameter description

Parameter	Mandatory	Type	Description
namespace	Yes	String	**Definition** Namespace of a service. For details, see **Services Interconnected with Cloud Eye**. **Constraints** N/A **Range** The namespace must be in the service.item format. **service** and **item** must be strings, and each must start with a letter and contain only letters (case-insensitive), digits, and underscores (_). In addition, **service** cannot start with **SYS**, **AGT**, or **SRE**. **namespace** cannot be **SERVICE.BMS** because this namespace has been used by the system. The value can contain 3 to 32 characters. For example, the ECS namespace is **SYS.ECS**, and the DDS namespace is **SYS.DDS**. **Default Value** N/A

Parameter	Mandatory	Type	Description
metric_name	Yes	String	**Definition** Metric ID. For example, **metric_name** of ECS CPU usage is **cpu_util**. For details about the metrics of each service, see **Services Interconnected with Cloud Eye**. **Constraints** N/A **Range** The value must start with a letter and can contain only digits, letters, underscores (_), and hyphens (-). For example, the ECS metric **cpu_util** indicates the CPU usage of an ECS. The DDS metric **mongo001_command_ps** indicates the command execution frequency. The value can contain 1 to 96 characters. **Default Value** N/A

Parameter	Mandatory	Type	Description
from	Yes	String	**Definition** Start time for the query. The value is a UNIX timestamp, in milliseconds (ms). **Constraints** Cloud Eye aggregates raw data generated within an aggregation period to the start time of the period. If the time range specified by **from** and **to** falls within an ongoing aggregation period, the query result will be empty because the aggregation has not finished yet. Set **from** to at least one period earlier than the current time. Take the 5-minute period as an example. If it is 10:35 now, the raw data generated between 10:30 and 10:35 will be aggregated to 10:30. In this example, if **period** is 5 minutes, **from** should be 10:30. **Range** N/A **Default Value** N/A **NOTE** Cloud Eye rounds up **from** based on the level of granularity required to perform the rollup.
to	Yes	String	**Definition** End time of the query. The value is a UNIX timestamp, in milliseconds (ms). **Constraints** **from** must be earlier than **to**. **Range** N/A **Default Value** N/A

Parameter	Mandatory	Type	Description
period	Yes	Integer	**Definition** Aggregation granularity of metric monitoring data. **Constraints** N/A **Range** The value can be: • **1**: real-time data of monitored resources. • **60**: Data is aggregated every one minute (one data point per minute). • **300**: Data is aggregated every 5 minutes (one data point every 5 minutes). • **1200**: Data is aggregated every 20 minutes (one data point every 20 minutes). • **3600**: Data is aggregated every one hour (one data point per hour). • **14400**: Data is aggregated every 4 hours (one data point every four hours). • **86400**: Data is aggregated every one day (one data point per day). **Default Value** N/A

Parameter	Mandatory	Type	Description
filter	Yes	String	**Definition** Data aggregation method. **Constraints** N/A **Range** The value can be: • **average**: average value of metric data within an aggregation period. • **max**: maximum value of metric data in an aggregation period. • **min**: minimum value of metric data within an aggregation period. • **sum**: sum of metric data within an aggregation period. • **variance**: variance value of metric data within an aggregation period. **Default Value** N/A **NOTE** During an aggregation process, data generated within a specified time range is consolidated to the start point of the aggregation period using the relevant aggregation algorithm. Take the 5-minute period as an example. If the current time is 10:35, the raw data generated between 10:30 and 10:35 will be aggregated to 10:30.

Parameter	Mandatory	Type	Description
dim	Yes	String	**Definition** Dimension of a metric. **Constraints** A maximum of 4 hierarchical dimensions are supported. The dimensions are numbered from 0. **Range** The dimension format is **dim.{i}=key,value**. **key** cannot exceed 32 characters and **value** cannot exceed 256 characters. The following dimensions are only examples. For details about whether multiple dimensions are supported, see the **metric description of each service**. Single-level dimension: **dim.0=instance_id,i-12345** Multi-level dimension: **dim.0=instance_id,i-12345&dim.1=instance_name,i-1234** **NOTE** If the dimensions of a metric have a hierarchical relationship, you need to use multi-level dimension queries. **Default Value** N/A

NOTE

- **dimensions** can be obtained from the response body by calling the API for **Querying Metrics**.
- OBS metric data can be queried only when the related OBS APIs are called.

- Example:

  Request example 1: View the CPU usage of ECS whose ID is **6f3c6f91-4b24-4e1b-b7d1-a94ac1cb011d** from 2019-04-30 20:00:00 to 2019-04-30 22:00:00. The monitoring interval is 20 minutes.

  ```
  GET https://{Cloud Eye endpoint}/V1.0/{project_id}/metric-data?namespace=SYS.ECS&metric_name=cpu_util&dim.0=instance_id,6f3c6f91-4b24-4e1b-b7d1-a94ac1cb011d&from=1556625600000&to=1556632800000&period=1200&filter=min
  ```

Request

None

Response

- Response parameters

Table 5-79 Parameter description

Parameter	Type	Description
datapoints	Array of objects	**Definition** Metric data list. For details, see **Table 5-80**. Since Cloud Eye rounds up **from** based on the level of granularity for data query, **datapoints** may contain more data points than expected.
metric_name	String	**Definition** Metric ID. For example, **metric_name** of ECS CPU usage is **cpu_util**. For details about the metrics of each service, see **Services Interconnected with Cloud Eye**. **Range** N/A

Table 5-80 datapoints data structure description

Parameter	Type	Description
average	Double	**Definition** Average value of metric data within an aggregation period. **Range** N/A
max	Double	**Definition** Maximum value of metric data within an aggregation period. **Range** N/A
min	Double	**Definition** Minimum value of metric data within an aggregation period. **Range** N/A

Parameter	Type	Description
sum	Double	**Definition** Sum of metric data within an aggregation period. **Range** N/A
variance	Double	**Definition** Variance value of metric data within an aggregation period. **Range** N/A
timestamp	Long	**Definition** Time when a metric was collected. It is a UNIX timestamp, in milliseconds. **Range** N/A
unit	String	**Definition** Metric unit. **Range** N/A

- Example response

  Example response 1: The dimension is SYS.ECS, and the average CPU usage of ECSs is displayed.

```
{
   "datapoints": [
      {
         "average": 0.23,
         "timestamp": 1442341200000,
         "unit": "%"
      }
   ],
   "metric_name": "cpu_util"
}
```

  Example response 2: The dimension is SYS.ECS, and the sum CPU usage of ECSs is displayed.

```
{
   "datapoints": [
      {
         "sum": 0.53,
         "timestamp": 1442341200000,
         "unit": "%"
      }
   ],
   "metric_name": "cpu_util"
}
```

  Example response 3: The dimension is SYS.ECS, and the maximum CPU usage of ECSs is displayed.

```
{
   "datapoints": [
```

```
        {
            "max": 0.13,
            "timestamp": 1442341200000,
            "unit": "%"
        }
    ],
    "metric_name": "cpu_util"
}
```

Returned Values

- Normal

  200

- Abnormal

Returned Value	Description
400 Bad Request	Request error.
401 Unauthorized	The authentication information is not provided or is incorrect.
403 Forbidden	Access to the requested page is forbidden.
408 Request Timeout	The request timed out.
429 Too Many Requests	Concurrent requests are excessive.
500 Internal Server Error	Failed to complete the request because of an internal service error.
503 Service Unavailable	The service is currently unavailable.

Error Codes

See **Error Codes**.

5.4.2 Adding Monitoring Data

Function

This API is used to add one or more pieces of custom metric monitoring data to solve the problem that the system metrics cannot meet specific service requirements.

For details about the monitoring data retention period, see **How Long Is Metric Data Retained?** in *Cloud Eye User Guide*.

Debugging

You can debug the API in **API Explorer** which supports automatic authentication. API Explorer can automatically generate and debug example SDK code.

URI

POST /V1.0/{project_id}/metric-data

- Parameter description

  Table 5-81 Parameter description

Parameter	Mandatory	Description
project_id	Yes	**Definition** Project ID, which is used to specify the project that an asset belongs to. You can query the assets of a project by project ID. You can obtain the project ID from the API or console. For details about how to obtain the project ID, see **Obtaining a Project ID**. **Constraints** N/A **Range** 1 to 64 characters **Default Value** N/A

- Example
  POST https://{Cloud Eye endpoint}/V1.0/{project_id}/metric-data

For details about Cloud Eye endpoints, go to **Endpoints** to query the URL of each region.

Request

NOTICE

1. The size of a POST request cannot exceed 512 KB. Otherwise, the request will be denied.
2. The period for sending POST requests must be shorter than the minimum aggregation period. Otherwise, the aggregated data will be noncontinuous. For example, if the aggregation period is 5 minutes and the POST request sending period is 7 minutes, the data will be aggregated every 10 minutes, rather than 5 minutes.
3. Timestamp (collect_time) in the POST request body value must be within the period that starts from three days before the current time to 10 minutes after the current time. If it is not in this range, you are not allowed to insert the metric data.

- Request parameters

Table 5-82 Parameter description

Parameter	Type	Mandatory	Description
Array elements	Array of objects	Yes	**Definition** Request parameters for adding one or more pieces of custom metric data record. For details, see **Table 5-83**. **Constraints** At least one metric data record must be added. A maximum of 10,000 metric data records are allowed. The message body of a single POST request cannot exceed 512 KB.

Table 5-83 Array elements

Parameter	Mandatory	Type	Description
metric	Yes	Object	**Definition** Metric data. For details, see **Table 5-84**. **Constraints** N/A
ttl	Yes	Integer	**Definition** Data validity period, in seconds. If the validity period expires, data will be automatically deleted. **Constraints** N/A **Range** 1 to 604800 **Default Value** N/A

Parameter	Mandatory	Type	Description
collect_time	Yes	Long	**Definition** Time when the data was collected. The value is a UNIX timestamp, in milliseconds. **Constraints** N/A **Range** Since there is a latency between the client and the server, the timestamp when data was inserted must be within the time range [Current time – 3d + 10s, Current time + 10 mins – 10s]. In this way, the data will be inserted to the database without being affected by the latency. **Default Value** N/A
value	Yes	Double	**Definition** Value of the monitored metric data to be added. **Constraints** N/A **Range** The value can be an integer or a floating point number. **Default Value** N/A
unit	No	String	**Definition** Data unit. **Constraints** N/A **Range** 0 to 32 **Default Value** N/A

Parameter	Mandatory	Type	Description
type	No	String	**Definition** Data type. **Constraints** N/A **Range** The value can be: • **int**: integer • **float**: floating point number **Default Value** N/A

Table 5-84 metric data structure description

Parameter	Mandatory	Type	Description
namespace	Yes	String	**Definition** Custom namespace. For details, see **Services Interconnected with Cloud Eye**. **Constraints** N/A **Range** The namespace must be in the service.item format. **service** and **item** must be strings, and each must start with a letter and contain only letters (case-insensitive), digits, and underscores (_). In addition, **service** cannot start with **SYS**, **AGT**, or **SRE**. **namespace** cannot be **SERVICE.BMS** because this namespace has been used by the system. The value can contain 3 to 32 characters. For example, the ECS namespace is **SYS.ECS**, and the DDS namespace is **SYS.DDS**. **Default Value** N/A

Parameter	Mandatory	Type	Description
dimensions	Yes	Array of objects	**Definition** Dimension of a metric. For details, see **Table 5-85**. **Constraints** A maximum of four dimensions are supported.
metric_name	Yes	String	**Definition** Metric ID. For example, **metric_name** of ECS CPU usage is **cpu_util**. For details about the metrics of each service, see **Services Interconnected with Cloud Eye**. **Constraints** N/A **Range** The value must start with a letter and can contain only digits, letters (case-insensitive), underscores (_), and hyphens (-). For example, the ECS metric **cpu_util** indicates the CPU usage of an ECS. The DDS metric **mongo001_command_ps** indicates the command execution frequency. The value can contain 1 to 96 characters. **Default Value** N/A

Table 5-85 dimensions data structure description

Parameter	Mandatory	Type	Description
name	Yes	String	**Definition** Monitoring dimension name. For example, the dimension of an ECS is **instance_id**. For details about the dimension of each service, see the **key** column in **Services Interconnected with Cloud Eye**. **Constraints** The value allows 1 to 32 characters. It must start with a letter and can contain only digits, letters, underscores (_), and hyphens (-). **Range** N/A **Default Value** N/A
value	Yes	String	**Definition** Dimension value, for example, an ECS ID. **Constraints** N/A **Range** The value allows 1 to 256 characters. It must start with a letter or digit and can contain only digits, letters, underscores (_), and hyphens (-). **Default Value** N/A

- Example request

  Example request 1: Add **cpu_util** data of a custom dimension. The instance ID is **6f3c6f91-4b24-4e1b-b7d1-a94ac1cb011d**.

```
[
  {
    "metric": {
      "namespace": "MINE.APP",
      "dimensions": [
        {
          "name": "instance_id",
          "value": "6f3c6f91-4b24-4e1b-b7d1-a94ac1cb011d"
        }
      ],
      "metric_name": "cpu_util"
    },
    "ttl": 172800,
    "collect_time": 1463598260000,
```



```
    "type": "float",
    "value": 0.09,
    "unit": "%"
  },
  {
    "metric": {
      "namespace": "MINE.APP",
      "dimensions": [
        {
          "name": "instance_id",
          "value": "6f3c6f91-4b24-4e1b-b7d1-a94ac1cb011d"
        }
      ],
      "metric_name": "cpu_util"
    },
    "ttl": 172800,
    "collect_time": 1463598270000,
    "type": "float",
    "value": 0.12,
    "unit": "%"
  }
]
```

Example request 2: Add **rds021_myisam_buf_usage** data of the RDS instance whose **rds_cluster_id** is **3c8cc15614ab46f5b8743317555e0de2in01**.

```
[
  {
    "metric": {
      "namespace": "SYS.RDS",
      "dimensions": [
  {
          "name": "rds_cluster_id",
          "value": "3c8cc15614ab46f5b8743317555e0de2in01"
        }
      ],
      "metric_name": "rds021_myisam_buf_usage"
    },
    "ttl": 172800,
    "collect_time": 1463598260000,
    "type": "float",
    "value": 0.01,
    "unit": "Ratio"
  }
]
```

Example request 3: Add **connections_usage** data of the DCS instance whose **dcs_instance_id** is **1598b5d4-3cb5-4f4d-8d99-2425d8e9ed54** and **dcs_cluster_redis_node** is **6666cd76f96956469e7be39d750cc7d9**.

```
[
  {
    "metric": {
      "namespace": "SYS.DCS",
      "dimensions": [
  {
          "name": "dcs_instance_id",
          "value": "1598b5d4-3cb5-4f4d-8d99-2425d8e9ed54"
    },
  {
          "name": "dcs_cluster_redis_node",
          "value": "6666cd76f96956469e7be39d750cc7d9"
        }
      ],
      "metric_name": "connections_usage"
    },
    "ttl": 172800,
    "collect_time": 1463598260000,
    "type": "float",
    "value": 8.3,
    "unit": "%"
```



```
  }
]
```

Response

The response has no message body.

Returned Values

- Normal

  201

- Abnormal

Returned Value	Description
400 Bad Request	Request error.
401 Unauthorized	The authentication information is not provided or is incorrect.
403 Forbidden	Access to the requested page is forbidden.
408 Request Timeout	The request timed out.
429 Too Many Requests	Concurrent requests are excessive.
500 Internal Server Error	Failed to complete the request because of an internal service error.
503 Service Unavailable	The service is currently unavailable.

Error Codes

See **Error Codes**.

5.4.3 Querying Monitoring Data of Multiple Metrics

Function

You can query the data of specified metrics within a specified time range and at a specified granularity. You can query the monitoring data of up to 500 metrics in one batch.

Constraints

- In regions CN East-Shanghai1, CN East-Shanghai2, CN North-Beijing4, and CN South-Guangzhou, you can query raw data as well as data aggregated at 1-minute and 5-minute intervals for any two days within a 20-day period. In other regions, only data from the most recent two days is available for such queries.

- Data aggregated at 20-minute, 1-hour, and 4-hour intervals is available for querying based on the metric data's retention period. For details, see **How Long Is Metric Data Retained?**

Debugging

You can debug the API in **API Explorer** which supports automatic authentication. API Explorer can automatically generate and debug example SDK code.

URI

POST /V1.0/{project_id}/batch-query-metric-data

- Parameter description

Table 5-86 Parameter description

Parameter	Mandatory	Description
project_id	Yes	**Definition** Project ID, which is used to specify the project that an asset belongs to. You can query the assets of a project by project ID. You can obtain the project ID from the API or console. For details about how to obtain the project ID, see **Obtaining a Project ID**. **Constraints** N/A **Range** 1 to 64 characters **Default Value** N/A

Request

NOTICE

1. The size of a POST request cannot exceed 512 KB. Otherwise, the request will be denied.
2. The default maximum query interval (**to**–**from**) varies depending on **period** and the number of metrics to be queried. The rule is as follows: Number of metrics x (**to** - **from**)/Monitoring interval ≤ 3000.
   - If **period** is **1**, the monitoring interval is 60,000 ms (60 x 1000).
   - If **period** is **300**, the monitoring interval is 300,000 ms (300 x 1000).
   - If **period** is **1200**, the monitoring interval is 1,200,000 ms (1200 x 1000).
   - If **period** is **3600**, the monitoring interval is 3,600,000 ms (3600 x 1000).
   - If **period** is **14400**, the monitoring interval is 14,400,000 ms (14400 x 1000).
   - If **period** is **86400**, the monitoring interval is 86,400,000 ms (86400 x 1000).

   For example, if 300 metrics are queried in batches and the monitoring interval is 60,000 ms, the maximum value of (**to**-**from**) is **600000**. If (**to-from**) exceeds 600,000, **from** is automatically changed to **to-600000**.

- Request parameters

Table 5-87 Request parameters

Parameter	Mandatory	Type	Description
metrics	Yes	Array of objects	**Definition** Metric data. For details, see **Table 5-88**. **Constraints** The array can contain a maximum of 500 items.

Parameter	Mandatory	Type	Description
from	Yes	Long	**Definition** Start time of the query. The value is a UNIX timestamp, in milliseconds. **Constraints** Set **from** to at least one period earlier than the current time. Cloud Eye aggregates raw data generated within an aggregation period to the start time of the period. If the time range specified by **from** and **to** falls within an ongoing aggregation period, the query result will be empty because the aggregation has not finished yet. Set **from** to at least one period earlier than the current time. Take the 5-minute period as an example. If it is 10:35 now, the raw data generated between 10:30 and 10:35 will be aggregated to 10:30. In this example, if **period** is 5 minutes, **from** should be 10:30. **Range** N/A **Default Value** N/A **NOTE** Cloud Eye rounds up **from** based on the level of granularity required to perform the rollup.
to	Yes	Long	**Definition** End time of the query. The value is a UNIX timestamp, in milliseconds (ms). **Constraints** **from** must be earlier than **to**. **Range** N/A **Default Value** N/A

Parameter	Mandatory	Type	Description
period	Yes	String	**Definition** Aggregation granularity of metric monitoring data. **Constraints** N/A **Range** The value can be: • **1**: real-time data of monitored resources. • **60**: Data is aggregated every one minute (one data point per minute). • **300**: Data is aggregated every 5 minutes (one data point every 5 minutes). • **1200**: Data is aggregated every 20 minutes (one data point every 20 minutes). • **3600**: Data is aggregated every one hour (one data point per hour). • **14400**: Data is aggregated every 4 hours (one data point every four hours). • **86400**: Data is aggregated every one day (one data point per day). **Default Value** N/A

Parameter	Mandatory	Type	Description
filter	Yes	String	**Definition** Data aggregation method. **Constraints** **filter** does not affect the query result of raw data. (The period is **1**.) **Range** The value can be: • **average**: average value of metric data within an aggregation period. • **max**: maximum value of metric data in an aggregation period. • **min**: minimum value of metric data within an aggregation period. • **sum**: sum of metric data within an aggregation period. • **variance**: variance value of metric data within an aggregation period. **Default Value** N/A

Table 5-88 metrics data structure description

Parameter	Mandatory	Type	Description
namespace	Yes	String	**Definition** Namespace of the queried service. For details, see **Services Interconnected with Cloud Eye**. **Constraints** N/A **Range** The namespace must be in the service.item format. **service** and **item** must be strings, and each must start with a letter and contain only letters (case-insensitive), digits, and underscores (_). In addition, **service** cannot start with **SYS**, **AGT**, or **SRE**. **namespace** cannot be **SERVICE.BMS** because this namespace has been used by the system. The value can contain 3 to 32 characters. For example, the ECS namespace is **SYS.ECS**, and the DDS namespace is **SYS.DDS**. **Default Value** N/A

Parameter	Mandatory	Type	Description
metric_name	Yes	String	**Definition** Metric ID. For example, **metric_name** of ECS CPU usage is **cpu_util**. For details about the metrics of each service, see **Services Interconnected with Cloud Eye**. **Constraints** N/A **Range** The value must start with a letter and can contain only digits, letters (case-insensitive), underscores (_), and hyphens (-). For example, the ECS metric **cpu_util** indicates the CPU usage of an ECS. The DDS metric **mongo001_command_ps** indicates the command execution frequency. The value can contain 1 to 96 characters. **Default Value** N/A

dimensions	Yes	Array of objects	**Definition**
			Dimension of a metric.
			Each dimension is a JSON object, and its structure is as follows:
			{
			"name": "instance_id",
			"value": "33328f02-3814-422e-b688-bfdba93d4050"
			}
			For details, see **Table 5-89**.
			Constraints
			A maximum of four dimensions are supported.

Table 5-89 dimensions data structure description

Parameter	Mandatory	Type	Description
name	Yes	String	**Definition** Monitoring dimension name. For example, the dimension of an ECS is **instance_id**. For details about the dimension of each service, see the **key** column in **Services Interconnected with Cloud Eye**. **Constraints** N/A **Range** The value must start with a letter and can contain 1 to 32 characters. It can contain only digits, letters, underscores (_), and hyphens (-). **Default Value** N/A
value	Yes	String	**Definition** Dimension value, for example, an ECS ID. **dimensions** can be obtained from the response body by calling the API for **querying metrics**. **Constraints** N/A **Range** The value must start with a letter or digit and can contain 1 to 256 characters. It can contain only digits, letters, underscores (_), and hyphens (-). **Default Value** N/A

NOTE

- **dimensions** can be obtained from the response body by calling the API for **querying metrics**.
- OBS metric data can be queried only when the related OBS APIs are called.

- Example requests

Example 1: Query the average disk usage of the disk whose **mount_point** is **012bec14bc176310c19f40e384fd629b** on the ECS whose **instance_id** is **07d878a9-2243-4e84-aeef-c47747d18024** from 20:00:00 to 22:00:00 on April 30, 2019.

```
{
   "from": 1556625600000,
   "to": 1556632800000,
   "period": "1",
   "filter": "average",
   "metrics": [{
      "dimensions": [{
         "name": "instance_id",
         "value": "07d878a9-2243-4e84-aeef-c47747d18024"
      }, {
         "name": "mount_point",
         "value": "012bec14bc176310c19f40e384fd629b"
      }],
      "metric_name": "disk_usedPercent",
      "namespace": "AGT.ECS"
   }]
}
```

Example 2: Query the average memory usage of the ECS whose **instance_id** is **238764d4-c4e1-4274-88a1-5956b057766b** from 20:00:00 to 22:00:00 on April 30, 2019.

```
{
   "from": 1556625600000,
   "to": 1556632800000,
   "period": "1",
   "filter": "average",
   "metrics": [{
      "dimensions": [{
         "name": "instance_id",
         "value": "238764d4-c4e1-4274-88a1-5956b057766b"
      }],
      "metric_name": "mem_usedPercent",
      "namespace": "AGT.ECS"
   }]
}
```

Example 3: Query the average **cpu_util** of the five ECSs whose values of **instance_id** are **faea5b75-e390-4e2b-8733-9226a9026070**, **faea5b75-e390-4e2b-8733-9226a9026071**, **faea5b75-e390-4e2b-8733-9226a9026072**, **faea5b75-e390-4e2b-8733-9226a9026073**, and **faea5b75-e390-4e2b-8733-9226a9026074** from 00:00:00 to 23:59:59 on August 21, 2024. Query five metrics. The monitoring period is 60,000 ms. The maximum value of (**to** – **from**) is **36000000**. The value of the request parameter (**to** – **from**) is **86399000**, which exceeds the maximum value **36000000**. The formula is as follows: Number of metrics × Value of (**to** – **from**)/Monitoring period ≤ 3000. The system automatically sets the value of **from** to **to** – **36000000**, that is, **1724219999000**.

```
{
   "metrics": [
     {
         "namespace": "SYS.ECS",
         "dimensions": [
            {
               "name": "instance_id",
               "value": "faea5b75-e390-4e2b-8733-9226a9026070"
            }
         ],
         "metric_name": "cpu_util"
     },
     {
```

```
            "namespace": "SYS.ECS",
            "dimensions": [
               {
                  "name": "instance_id",
                  "value": "faea5b75-e390-4e2b-8733-9226a9026071"
               }
            ],
            "metric_name": "cpu_util"
         },
            {
            "namespace": "SYS.ECS",
            "dimensions": [
               {
                  "name": "instance_id",
                  "value": "faea5b75-e390-4e2b-8733-9226a9026072"
               }
            ],
            "metric_name": "cpu_util"
         },
            {
            "namespace": "SYS.ECS",
            "dimensions": [
               {
                  "name": "instance_id",
                  "value": "faea5b75-e390-4e2b-8733-9226a9026073"
               }
            ],
            "metric_name": "cpu_util"
         },
            {
            "namespace": "SYS.ECS",
            "dimensions": [
               {
                  "name": "instance_id",
                  "value": "faea5b75-e390-4e2b-8733-9226a9026074"
               }
            ],
            "metric_name": "cpu_util"
         }
      ],
      "from": 1724169600000,
      "to": 1724255999000,
      "period": "1",
      "filter": "average"
}
```


Example 4: View the average **cpu_util** of the ECS whose **instance_id** is **faea5b75-e390-4e2b-8733-9226a9026070** and the average **network_vm_connections** of the ECS whose **instance_id** is **06b4020f-461a-4a52-84da-53fa71c2f42b** from 20:00:00 to 22:00:00 on April 30, 2019.


```
{
   "metrics": [
     {
         "namespace": "SYS.ECS",
         "dimensions": [
            {
               "name": "instance_id",
               "value": "faea5b75-e390-4e2b-8733-9226a9026070"
            }
         ],
         "metric_name": "cpu_util"
      },
      {
         "namespace": "SYS.ECS",
         "dimensions": [
            {
               "name": "instance_id",
               "value": "06b4020f-461a-4a52-84da-53fa71c2f42b"
```

```
            }
         ],
         "metric_name": "network_vm_connections"
      }
   ],
   "from": 1556625600000,
   "to": 1556632800000,
   "period": "1",
   "filter": "average"
}
```

Example 5: View the individual sums of **rds021_myisam_buf_usage** of the RDS instance whose **rds_cluster_id** is **3c8cc15614ab46f5b8743317555e0de2in01** and the RDS instance whose **rds_cluster_id** is **3b2fa8b55a9b4adca3713962a9d31884in01** from 20:00:00 to 22:00:00 on April 30, 2019.

```
{
   "metrics": [
      {
         "namespace": "SYS.RDS",
         "dimensions": [
            {
               "name": "rds_cluster_id",
               "value": "3c8cc15614ab46f5b8743317555e0de2in01"
            }
         ],
         "metric_name": "rds021_myisam_buf_usage"
      },
      {
         "namespace": "SYS.RDS",
         "dimensions": [
            {
               "name": "rds_cluster_id",
               "value": "3b2fa8b55a9b4adca3713962a9d31884in01"
            }
         ],
         "metric_name": "rds021_myisam_buf_usage"
      }
   ],
   "from": 1556625600000,
   "to": 1556632800000,
   "period": "1",
   "filter": "sum"
}
```

Example 6: View the minimum **proc_specified_count** of the server whose **instance_id** is **cd841102-f6b1-407d-a31f-235db796dcbb** and **proc** is **b28354b543375bfa94dabaeda722927f**. The monitoring data is collected from 20:00:00 to 22:00:00 on April 30, 2019 and the aggregation period is 20 minutes.

```
{
   "metrics": [
      {
         "namespace": "AGT.ECS",
         "dimensions": [
            {
               "name": "instance_id",
               "value": "cd841102-f6b1-407d-a31f-235db796dcbb"
            },
            {
               "name": "proc",
               "value": "b28354b543375bfa94dabaeda722927"
            }
         ],
         "metric_name": "proc_specified_count"
      }
   ],
   "from": 1556625600000,
```



```
    "to": 1556632800000,
    "period": "1200",
    "filter": "min"
}
```

Response

- Response parameters

Table 5-90 Parameter description

Parameter	Type	Description
metrics	Array of objects	**Definition** Metric data list. For details, see **Table 5-91**.

Table 5-91 metrics data structure description

Parameter	Type	Description
unit	String	**Definition** Metrics unit. **Range** N/A
datapoints	Array of objects	**Definition** Metric data list. During data query, Cloud Eye rounds up the value of **from** based on the aggregation granularity selected, so there may be more data points in **datapoints** than expected. A maximum of 3,000 data points can be returned. For details, see **Table 5-93**.
namespace	String	**Definition** Metric namespace. **Range** N/A

Parameter	Type	Description

dimensions	Array of objects	**Definition**
		List of metric dimensions.
		Each dimension is a JSON object, and its structure is as follows:
		{
		"name": "instance_id",
		"value": "33328f02-3814-422e-b688-bfdba93d4050"
		}
		For details, see **Table 5-92**.

metric_name	String	**Definition** Metric name. **Range** N/A

Table 5-92 dimensions data structure description

Parameter	Type	Description
name	String	**Definition** Monitoring dimension name. For example, the dimension of an ECS is **instance_id**. For details about the dimension of each service, see the **key** column in **Services Interconnected with Cloud Eye**. **Range** N/A
value	String	**Definition** Dimension value, for example, an ECS ID. **Range** N/A

Table 5-93 datapoints data structure description

Parameter	Type	Description
average	Double	**Definition** Average value of metric data within an aggregation period. **Range** N/A
max	Double	**Definition** Maximum value of metric data within an aggregation period. **Range** N/A
min	Double	**Definition** Minimum value of metric data within an aggregation period. **Range** N/A
sum	Double	**Definition** Sum of metric data within an aggregation period. **Range** N/A
variance	Double	**Definition** Variance value of metric data within an aggregation period. **Range** N/A
timestamp	Long	**Definition** Time when a metric was collected. It is a UNIX timestamp, in milliseconds. **Range** N/A

- Example response

  Example response 1: The average **cpu_util** of the ECS whose **instance_id** is **faea5b75-e390-4e2b-8733-9226a9026070** and the average **network_vm_connections** of the ECS whose **instance_id** is **06b4020f-461a-4a52-84da-53fa71c2f42b** are displayed.

```
{
   "metrics": [
      {
         "namespace": "SYS.ECS",
         "metric_name": "cpu_util",
         "dimensions": [
```

```
            {
                "name": "instance_id",
                "value": "faea5b75-e390-4e2b-8733-9226a9026070"
            }
        ],
        "datapoints": [
            {
                "average": 0.69,
                "timestamp": 1556625610000
            },
            {
                "average": 0.7,
                "timestamp": 1556625715000
            }
        ],
        "unit": "%"
    },
    {
        "namespace": "SYS.ECS",
        "metric_name": "network_vm_connections",
        "dimensions": [
            {
                "name": "instance_id",
                "value": "06b4020f-461a-4a52-84da-53fa71c2f42b"
            }
        ],
        "datapoints": [
            {
                "average": 1,
                "timestamp": 1556625612000
            },
            {
                "average": 3,
                "timestamp": 1556625717000
            }
        ],
        "unit": "count"
    }
  ]
}
```

Response example 2: The **rds021_myisam_buf_usage** sums of the RDS instance whose **rds_cluster_id** are **3c8cc15614ab46f5b8743317555e0de2in01** is displayed, and those of the RDS instance whose **rds_cluster_id** is **3b2fa8b55a9b4adca3713962a9d31884in01** are displayed.

```
{
  "metrics": [
    {
        "unit": "Ratio",
        "datapoints": [
            {
                "sum": 0.07,
                "timestamp": 1556625628000
            },
            {
                "sum": 0.07,
                "timestamp": 1556625688000
            }
        ],
        "namespace": "SYS.RDS",
        "dimensions": [
            {
                "name": "rds_cluster_id",
                "value": "3c8cc15614ab46f5b8743317555e0de2in01"
            }
        ],
        "metric_name": "rds021_myisam_buf_usage"
    },
```

```
    {
        "unit": "Ratio",
        "datapoints": [
            {
                "sum": 0.06,
                "timestamp": 1556625614000
            },
            {
                "sum": 0.07,
                "timestamp": 1556625674000
            }
        ],
        "namespace": "SYS.RDS",
        "dimensions": [
            {
                "name": "rds_cluster_id",
                "value": "3b2fa8b55a9b4adca3713962a9d31884in01"
            }
        ],
        "metric_name": "rds021_myisam_buf_usage"
    }
  ]
}
```


Response example 3: The minimum **rds021_myisam_buf_usage** of the server whose **instance_id** is **cd841102-f6b1-407d-a31f-235db796dcbb** and **proc** is **b28354b543375bfa94dabaeda722927f** is displayed.


```
{
  "metrics": [
    {
        "unit": "Ratio",
        "datapoints": [
            {
                "min": 0,
                "timestamp": 1556625612000
            },
            {
                "min": 0,
                "timestamp": 1556625672000
            }
        ],
        "namespace": "AGT.ECS",
        "dimensions": [
            {
                "name": "instance_id",
                "value": "cd841102-f6b1-407d-a31f-235db796dcbb"
            },
            {
                "name": "proc",
                "value": "b28354b543375bfa94dabaeda722927f"
            }
        ],
        "metric_name": "rds021_myisam_buf_usage"
    }
  ]
}
```


Returned Values

- Normal

  200

- Abnormal

Returned Value	Description
400 Bad Request	Request error.

Returned Value	Description
401 Unauthorized	The authentication information is not provided or is incorrect.
403 Forbidden	Access to the requested page is forbidden.
408 Request Timeout	The request timed out.
429 Too Many Requests	Concurrent requests are excessive.
500 Internal Server Error	Failed to complete the request because of an internal service error.
503 Service Unavailable	The service is currently unavailable.

Error Codes

See **Error Codes**.

5.4.4 Querying the Host Configuration

Function

This API is used to query the host configuration for a specified event type in a specified time range. You can specify the dimension of data to be queried.

NOTICE

This API is provided for SAP Monitor in the HANA scenario to query the host configuration. In other scenarios, the host configuration cannot be queried with this API.

Debugging

You can debug the API in **API Explorer** which supports automatic authentication. API Explorer can automatically generate and debug example SDK code.

URI

GET /V1.0/{project_id}/event-data

- Parameter description

Table 5-94 Parameter description

Parameter	Mandatory	Description
project_id	Yes	**Definition** Project ID, which is used to specify the project that an asset belongs to. You can query the assets of a project by project ID. You can obtain the project ID from the API or console. For details about how to obtain the project ID, see **Obtaining a Project ID**.

- Parameters that are used to query the host configuration

Parameter	Mandatory	Type	Description
namespace	Yes	String	**Definition** Namespace of the queried service. For details, see **Services Interconnected with Cloud Eye**. **Constraints** N/A **Range** The namespace must be in the service.item format. **service** and **item** must be strings, and each must start with a letter and contain only letters (case-insensitive), digits, and underscores (_). In addition, **service** cannot start with **SYS**, **AGT**, or **SRE**. **namespace** cannot be **SERVICE.BMS** because this namespace has been used by the system. The value can contain 3 to 32 characters. For example, the ECS namespace is **SYS.ECS**, and the DDS namespace is **SYS.DDS**. **Default Value** N/A

Parameter	Mandatory	Type	Description
type	Yes	String	**Definition** Event type. It can contain only letters, underscores (_), and hyphens (-). It must start with a letter and cannot exceed 64 characters, for example, **instance_host_info**. **Constraints** N/A **Range** The value cannot exceed 64 characters. Regular matching: ^([a-z]|[A-Z]){1}([a-z]|[A-Z]|[0-9]|_|-)*$ **Default Value** N/A
from	Yes	String	**Definition** Start time of the query. The value is a UNIX timestamp, in milliseconds. **Constraints** N/A **Range** N/A **Default Value** N/A
to	Yes	String	**Definition** End time of the query. The value is a UNIX timestamp, in milliseconds. **Constraints** **from** must be earlier than **to**. **Range** N/A **Default Value** N/A

Parameter	Mandatory	Type	Description
dim	Yes	String	**Definition** Monitoring dimension, for example, **instance_id** for ECSs. For details about the dimensions corresponding to the monitoring metrics of each service, see the monitoring metrics description of the corresponding service in **Services Interconnected with Cloud Eye**. **Constraints** N/A **Range** Metric dimension. A maximum of 3 dimensions are supported, numbered from 0 and in the dim.{i}=key,value format. **key** cannot exceed 32 characters and **value** cannot exceed 256 characters. Example: **dim.0=instance_id,i-12345** **Default Value** N/A

- Example: Query the configuration information about the ECS whose **ID** is **33328f02-3814-422e-b688-bfdba93d4051** and **type** is **instance_host_info**.

```
GET https://{Cloud Eye endpoint}/V1.0/{project_id}/event-data?
namespace=SYS.ECS&dim.0=instance_id,33328f02-3814-422e-b688-
bfdba93d4051&type=instance_host_info&from=1450234543422&to=1450320943422
```

Request

None

Response

- Response parameters

Table 5-95 Parameter description

Parameter	Type	Description
datapoints	Array of objects	**Definition** Configuration list. If the corresponding configuration information does not exist, **datapoints** is an empty array and is **[]**. For details, see **Table 5-96**.

Table 5-96 datapoints data structure description

Parameter	Type	Description
type	String	**Definition** Event type, for example, **instance_host_info**. **Range** N/A
timestamp	Long	**Definition** Time when the event was reported. The value is a UNIX timestamp, in milliseconds. **Range** N/A
value	String	**Definition** Host configuration information. **Range** N/A

- Example response

```
{
  "datapoints": [
    {
      "type": "instance_host_info",
      "timestamp": 1450231200000,
      "value": "xxx"
    },
    {
      "type": "instance_host_info",
      "timestamp": 1450231800000,
      "value": "xxx"
    }
  ]
}
```

Returned Values

- Normal

  200

- Abnormal

Returned Value	Description
400 Bad Request	Request error.
401 Unauthorized	The authentication information is not provided or is incorrect.
403 Forbidden	Access to the requested page is forbidden.
408 Request Timeout	The request timed out.
429 Too Many Requests	Concurrent requests are excessive.
500 Internal Server Error	Failed to complete the request because of an internal service error.
503 Service Unavailable	The service is currently unavailable.

Error Codes

See **Error Codes**.

5.5 Quotas

5.5.1 Querying Quotas

Function

This API is used to query the alarm rule quota and the number of alarm rules that have been created.

Debugging

You can debug the API in **API Explorer** which supports automatic authentication. API Explorer can automatically generate and debug example SDK code.

URI

GET /V1.0/{project_id}/quotas

- Parameter description

Table 5-97 Parameter description

Parameter	Mandatory	Description
project_id	Yes	Specifies the project ID. For details about how to obtain the project ID, see **Obtaining a Project ID**.

- Example: Query the alarm rule quota.
  GET https://{Cloud Eye endpoint}/V1.0/{project_id}/quotas

Request

None

Response

- Response parameters

Table 5-98 Response parameters

Parameter	Type	Description
quotas	Object	Specifies the quota list. For details, see **Table 5-99**.

Table 5-99 Data structure description of **quotas**

Parameter	Type	Description
resources	Array of objects	Specifies the resource quota list. For details, see **Table 5-100**.

Table 5-100 Data structure description of **resources**

Parameter	Type	Description
type	String	Specifies the quota type. **alarm** indicates the alarm rule.
used	Integer	Specifies the used amount of the quota.
unit	String	Specifies the quota unit.
quota	Integer	Specifies the total amount of the quota.

- Example response

```
{
"quotas":
   {
   "resources": [
         {
            "unit":"",
            "type":"alarm",
            "quota":1000,
            "used":10
         }
      ]
   }
}
```

Returned Values

- Normal

  200

- Abnormal

Returned Value	Description
400 Bad Request	Request error.
401 Unauthorized	The authentication information is not provided or is incorrect.
403 Forbidden	Access to the requested page is forbidden.
408 Request Timeout	The request timed out.
429 Too Many Requests	Concurrent requests are excessive.
500 Internal Server Error	Failed to complete the request because of an internal service error.
503 Service Unavailable	The service is currently unavailable.

Error Codes

See **Error Codes**.

5.6 Resource Groups

5.6.1 Querying Resources in a Resource Group

Function

This API is used to query resources in a resource group based on the resource group ID.

Debugging

You can debug the API in **API Explorer** which supports automatic authentication. API Explorer can automatically generate and debug example SDK code.

URI

GET /V1.0/{project_id}/resource-groups/{group_id}

- Parameter description

  Table 5-101 Parameter description

Parameter	Mandatory	Description
project_id	Yes	Specifies the project ID. For details about how to obtain the project ID, see **Obtaining a Project ID**.
group_id	Yes	Specifies the resource group ID.
status	No	Specifies the resource group status, which can be **health**, **unhealth**, or **no_alarm_rule**. • **health**: No alarms have been generated for the resource group. • **unhealth**: An alarm or alarms have been generated for a resource or resources in the resource group. • **no_alarm_rule**: No alarm rules have been set for the resource group.
namespace	No	Specifies the resource namespace. For example, the ECS namespace is **SYS.ECS**. To view the namespace of each service, see **Services Interconnected with Cloud Eye**.
dname	No	Specifies the resource dimension. For example, the ECS dimension is **instance_id**. To view the dimension of each resource, see **Services Interconnected with Cloud Eye**.
start	No	Specifies the start value of pagination. The value is an integer. The default value is **0**.
limit	No	Specifies the maximum number of records that can be queried at a time. The value range is (0,100] and the default value is 100.

- Example: Query resources in a resource group.

```
GET https://{Cloud Eye endpoint}/V1.0/{project_id}/resource-groups/{group_id}
```

Request

None

Response

- Response parameters

Table 5-102 Parameter description

Parameter	Type	Description
group_name	String	Specifies the resource group, for example, **Resource-Group-ECS-01**.
group_id	String	Specifies the resource group ID, for example, **rg1603786526428bWbVmk4rP**.
resources	Array of objects	Specifies information about one or more resource groups. For details, see **Table 5-103**.
status	String	Specifies the resource group status, which can be **health**, **unhealth**, or **no_alarm_rule**. • **health**: No alarms have been generated for the resource group. • **unhealth**: An alarm or alarms have been generated for a resource or resources in the resource group. • **no_alarm_rule**: No alarm rules have been set for the resource group.
create_time	Long	Specifies the time the resource group is created. The time is a UNIX timestamp and the unit is ms. Example: **1603819753000**
meta_data	MetaData object	Specifies the metadata of query results, including the pagination information. For details, see **Table 5-105**.
enterprise_project_id	String	Specifies the enterprise project associated with the resource group. The default value **0** indicates enterprise project **default.**

Table 5-103 resources data structure description

Parameter	Type	Description
namespace	String	Specifies the resource namespace. For example, the ECS namespace is **SYS.ECS**. To view the namespace of each service, see **Services Interconnected with Cloud Eye**.
dimensions	Array of objects	Specifies one or more resource dimensions. For details, see **Table 5-104**.

Parameter	Type	Description
status	String	Specifies the resource group status, which can be **health**, **unhealth**, or **no_alarm_rule**. **health**: No alarms have been generated for the resource group. **unhealth**: An alarm or alarms have been generated for a resource or resources in the resource group. **no_alarm_rule**: No alarm rules have been set for the resource group.
event_type	Integer	Specifies the event type. The default value is **0**.

Table 5-104 dimensions data structure description

Parameter	Type	Description
name	String	Specifies the resource dimension. For example, the ECS dimension is **instance_id**. To view the dimension of each resource, see **Services Interconnected with Cloud Eye**.
value	String	Specifies the resource dimension value, which is the instance ID. Example: **4270ff17-aba3-4138-89fa-820594c39755**

Table 5-105 meta_data data structure description

Parameter	Type	Description
count	Integer	Specifies the number of returned results.
total	Integer	Specifies the total number of query results.
marker	String	Specifies the pagination marker.

- Example response

```
{
 "group_name": "ResourceGroup-Test-01",
 "resources": [
  {
   "namespace": "SYS.ECS",
   "dimensions": [
    {
     "name": "instance_id",
     "value": "6cffb0bd-fd37-400f-ae6f-8f4be021ff7e"
    }
   ],
   "status": "health",
```



```
    "event_type": 0
  },
  {
    "namespace": "SYS.ECS",
    "dimensions": [
      {
        "name": "instance_id",
        "value": "e37d6238-9dd3-4720-abcc-eb9f8fb08ca0"
      }
    ],
    "status": "health",
    "event_type": 0
  }
],
"create_time": 1604476378000,
"group_id": "rg16044763786104XvXvl00a",
"status": "health",
"meta_data": {
  "count": 0,
  "marker": "",
  "total": 2
},
"enterprise_project_id": "0"
}
```


Returned Values

- Normal

  200

- Abnormal

Returned Values	Description
400 Bad Request	Request error.
401 Unauthorized	The authentication information is not provided or is incorrect.
403 Forbidden	Access to the requested page is forbidden.
408 Request Timeout	The request timed out.
429 Too Many Requests	Concurrent requests are excessive.
500 Internal Server Error	Failed to complete the request because of an internal service error.
503 Service Unavailable	The service is currently unavailable.

Error Codes

See **Error Codes**.

5.6.2 Creating a Resource Group

Function

This API is used to create a resource group. You can use resource groups to manage resources by service, and view monitoring and alarm information by group to ease O&M.

Debugging

You can debug the API in **API Explorer** which supports automatic authentication. API Explorer can automatically generate and debug example SDK code.

URI

POST /V1.0/{project_id}/resource-groups

- Parameter description

  Table 5-106 Parameter description

Parameter	Type	Mandatory	Description
project_id	String	Yes	Specifies the project ID. For details about how to obtain the project ID, see **Obtaining a Project ID**.

- Request example
  POST https://{Cloud Eye endpoint}/V1.0/{project_id}/resource-groups

Request

- Request parameters

  Table 5-107 Parameter description

Parameter	Type	Mandatory	Description
group_name	String	Yes	Specifies the resource group name. Enter 1 to 128 characters. Only letters, digits, underscores (_), and hyphens (-) are allowed. Example: **ResourceGroup-Test01**
resources	Array of objects	Yes	Select one or more resources for the resource group to be created. For details, see **Table 5-108**.

Table 5-108 resources data structure description

Parameter	Type	Mandatory	Description
namespace	String	Yes	Specifies the resource namespace. For example, the ECS namespace is **SYS.ECS**. To view the namespace of each service, see **Services Interconnected with Cloud Eye**.
dimensions	Array of objects	Yes	Specifies one or more resource dimensions. For details, see **Table 5-109**.

Table 5-109 dimensions data structure description

Parameter	Type	Mandatory	Description
name	String	Yes	Specifies the resource dimension. For example, the ECS dimension is **instance_id**. To view the dimension of each resource, see **Services Interconnected with Cloud Eye**.
value	String	Yes	Specifies the resource dimension value, which is the instance ID. Example: **4270ff17-aba3-4138-89fa-820594c39755**

Response

- Response parameter

Table 5-110 Parameter description

Parameter	Type	Description
group_id	String	Specifies the resource group ID, for example, **rg1603786526428bWbVmk4rP**.

Example Request

```
{
  "group_name" : "Resource-Group-Test01",
  "resources" : [ {
    "namespace" : "SYS.ECS",
    "dimensions" : [ {
      "name" : "instance_id",
      "value" : "063a83da-a2b5-4630-ab6b-9b4fcfc261ea"
    } ]
  }, {
    "namespace" : "SYS.ECS",
```



```
  "dimensions" : [ {
    "name" : "instance_id",
    "value" : "518ace88-abde-46bf-829b-0d1f0f2fb2e9"
  } ]
 } ]
}
```

Example Responses

Status code: 201

OK

```
{
 "group_id" : "rg1606377637506DmVOENVyL"
}
```

Returned Values

- Normal

  201

- Abnormal

Returned Value	Description
400 Bad Request	Request error.
401 Unauthorized	The authentication information is not provided or is incorrect.
403 Forbidden	Access to the requested page is forbidden.
408 Request Timeout	The request timed out.
429 Too Many Requests	Concurrent requests are excessive.
500 Internal Server Error	Failed to complete the request because of an internal service error.
503 Service Unavailable	The service is currently unavailable.

Error Codes

See **Error Codes**.

5.6.3 Updating a Resource Group

Function

This API is used to update a resource group. You can use resource groups to manage resources by service, and view monitoring and alarm information by group to ease O&M.

Debugging

You can debug the API in **API Explorer** which supports automatic authentication. API Explorer can automatically generate and debug example SDK code.

URI

PUT /V1.0/{project_id}/resource-groups/{group_id}

- Parameter description

  Table 5-111 Parameter description

Parameter	Type	Mandatory	Description
project_id	String	Yes	Specifies the project ID. For details about how to obtain the project ID, see **Obtaining a Project ID**.
group_id	String	Yes	Specifies the resource group ID.

- Request example

```
PUT https://{Cloud Eye endpoint}/V1.0/{project_id}/resource-groups/{group_id}
```

Request

- Request parameters

  Table 5-112 Parameter description

Parameter	Type	Mandatory	Description
group_name	String	Yes	Specifies the resource group name. Enter 1 to 128 characters. Only letters, digits, underscores (_), and hyphens (-) are allowed. Example: **ResourceGroup-Test01**
resources	Array of objects	Yes	Select one or more resources for the resource group to be created. For details, see **Table 5-113**.

Table 5-113 resources data structure description

Parameter	Type	Mandatory	Description
namespace	String	Yes	Specifies the resource namespace. For example, the ECS namespace is **SYS.ECS**. To view the namespace of each service, see **Services Interconnected with Cloud Eye**.
dimensions	Array of objects	Yes	Specifies one or more resource dimensions. For details, see **Table 5-114**.

Table 5-114 dimensions data structure description

Parameter	Type	Mandatory	Description
name	String	Yes	Specifies the resource dimension. For example, the ECS dimension is **instance_id**. To view the dimension of each resource, see **Services Interconnected with Cloud Eye**.
value	String	Yes	Specifies the resource dimension value, which is the instance ID. Example: **4270ff17-aba3-4138-89fa-820594c39755**

- Example request

```
{
  "group_name": "Resource-Group-Test01",
  "resources": [
    {
      "namespace": "SYS.ECS",
      "dimensions": [
        {
          "name": "instance_id",
          "value": "063a83da-a2b5-4630-ab6b-9b4fcfc261ea"
        }
      ]
    },
    {
      "namespace": "SYS.ECS",
      "dimensions": [
        {
          "name": "instance_id",
          "value": "518ace88-abde-46bf-829b-0d1f0f2fb2e9"
        }
      ]
    },
    {
      "namespace": "SYS.ECS",
      "dimensions": [
        {
          "name": "instance_id",
          "value": "675006b5-477a-4aab-948c-0aa467de9c68"
```



```
        }
      ]
    }
  ]
}
```

Response

None

Returned Values

- Normal

  204

- Abnormal

Returned Value	Description
400 Bad Request	Request error.
401 Unauthorized	The authentication information is not provided or is incorrect.
403 Forbidden	Access to the requested page is forbidden.
408 Request Timeout	The request timed out.
429 Too Many Requests	Concurrent requests are excessive.
500 Internal Server Error	Failed to complete the request because of an internal service error.
503 Service Unavailable	The service is currently unavailable.

Error Codes

See **Error Codes**.

5.6.4 Deleting a Resource Group

Function

This API is used to delete a resource group.

Debugging

You can debug the API in **API Explorer** which supports automatic authentication. API Explorer can automatically generate and debug example SDK code.

URI

DELETE /V1.0/{project_id}/resource-groups/{group_id}

- Parameter description

  Table 5-115 Parameter description

Parameter	Type	Mandatory	Description
project_id	String	Yes	Specifies the project ID. For details about how to obtain the project ID, see **Obtaining a Project ID**.
group_id	String	Yes	Specifies the resource group ID.

- Request example

```
DELETE https://{Cloud Eye endpoint}/V1.0/{project_id}/resource-groups/{group_id}
```

Request

None

Response

None

Returned Value

- Normal

  204

- Abnormal

Returned Value	Description
400 Bad Request	Request error.
401 Unauthorized	The authentication information is not provided or is incorrect.
403 Forbidden	Access to the requested page is forbidden.
408 Request Timeout	The request timed out.
429 Too Many Requests	Concurrent requests are excessive.
500 Internal Server Error	Failed to complete the request because of an internal service error.
503 Service Unavailable	The service is currently unavailable.

Error Codes

See **Error Codes**.

5.6.5 Query Resource Groups

Function

This API is used to query all resource groups you created.

Debugging

You can debug the API in **API Explorer** which supports automatic authentication. API Explorer can automatically generate and debug example SDK code.

URI

GET /V1.0/{project_id}/resource-groups

- Parameter description

Table 5-116 Parameter description

Parameter	Type	Mandatory (Yes/No)	Description
project_id	String	Yes	Specifies the project ID. For details about how to obtain the project ID, see **Obtaining a Project ID**.
group_name	String	No	Specifies the resource group, for example, **Resource-Group-ECS-01**.
group_id	String	No	Specifies the resource group ID, for example, **rg1603786526428bWbVmk4rP**.
status	String	No	Specifies the resource group status, which can be **health**, **unhealth**, or **no_alarm_rule**. • **health**: No alarms have been generated for the resource group. • **unhealth**: An alarm or alarms have been generated for a resource or resources in the resource group. • **no_alarm_rule**: No alarm rules have been set for the resource group.
start	Integer	No	Specifies the start value of pagination. The value is an integer. The default value is **0**.
limit	Integer	No	Specifies the maximum number of records that can be queried at a time. Supported range: **1** to **100** (default)

- Example
  GET https://{Cloud Eye endpoint}/V1.0/{project_id}/resource-groups

Request

None

Response

- Response parameters

Table 5-117 Parameter description

Parameter	Type	Mandatory (Yes/No)	Description
resource_groups	Array of objects	No	Specifies information about one or more resource groups. For details, see **Table 5-118**.
meta_data	MetaData object	No	Specifies the number of metadata records in the query result. For details, see **Table 5-120**.

Table 5-118 resource_groups data structure description

Parameter	Type	Mandatory (Yes/No)	Description
group_name	String	No	Specifies the resource group name, for example, **ResourceGroup-Test01**.
group_id	String	No	Specifies the resource group ID, for example, **rg1603786526428bWbVmk4rP**.
create_time	Long	No	Specifies the time the resource group is created. The time is a UNIX timestamp and the unit is ms. Example: **1603819753000**
relation_ids	Array of strings	No	Specifies the enterprise project IDs.

Parameter	Type	Mandatory (Yes/No)	Description
type	String	No	Specifies the method of adding or matching resources to a resource group. The value can be: **EPS**: matching resources by enterprise project. **TAG**: matching resources by tag. **NAME**: matching resources by instance name. **COMB**: matching resources by multiple criteria. **Manual**: add resources manually. If the response parameter is empty, resources are manually added. Minimum length: 0 character Maximum length: 32 characters
resources	Array of Resource objects	No	Specifies information about one or more resources. Array length: 0 to 20
instance_statistics	InstanceStatistics object	No	Specifies the resource statistics in the resource group. For details, see **Table 5-119**.
status	String	No	Specifies the resource group status, which can be **health**, **unhealth**, or **no_alarm_rule**. • **health**: No alarms have been generated for the resource group. • **unhealth**: An alarm or alarms have been generated for a resource or resources in the resource group. • **no_alarm_rule**: No alarm rules have been set for the resource group.
enterprise_project_id	String	No	Specifies the enterprise project associated with the resource group. The default value **0** indicates enterprise project **default.**

Table 5-119 instance_statistics data structure description

Parameter	Type	Mandatory (Yes/No)	Description
unhealth	Integer	No	Specifies the number of resources in the **Alarm** state in the resource group.
total	Integer	No	Specifies the total number of resources in the resource group.
type_statistics	Integer	No	Specifies the total number of resource types in the resource group. For example, if ECS, EIP and bandwidth are added to the resource group, the **type_statistics** value is **2**.

Table 5-120 meta_data data structure description

Parameter	Type	Mandatory (Yes/No)	Description
total	Integer	No	Specifies the total number of query results.

– Example response

```
{
 "resource_groups": [
  {
   "group_name": "ResourceGroup-Test01",
   "create_time": 1606374365000,
   "group_id": "rg16063743652226ew93e64p",
   "relation_ids": ["0"],
   "instance_statistics": {
    "unhealth": 2,
    "total": 10,
    "type_statistics": 1
   },
   "status": "unhealth",
   "enterprise_project_id": "0",
   "type": "TAG",
   "resources": []
  },
  {
   "group_name": "RS",
   "create_time": 1606327955000,
   "group_id": "rg1606327955657LRj1lrE4y",
   "relation_ids": ["0"],
   "instance_statistics": {
    "unhealth": 0,
    "total": 2,
    "type_statistics": 1
```

```
    },
    "status": "no_alarm_rule",
    "enterprise_project_id": "0",
    "type": "TAG",
    "resources": []
  },
  {
    "group_name": "RS",
    "create_time": 1606327947000,
    "group_id": "rg1606327947514v9OWqAD3N",
    "relation_ids": ["0"],
    "instance_statistics": {
      "unhealth": 0,
      "total": 2,
      "type_statistics": 1
    },
    "status": "no_alarm_rule",
    "enterprise_project_id": "0",
    "type": "TAG",
    "resources": []
  },
  {
    "group_name": "RS",
    "create_time": 1606327946000,
    "group_id": "rg1606327946625PYogr059N",
    "relation_ids": ["0"],
    "instance_statistics": {
      "unhealth": 0,
      "total": 2,
      "type_statistics": 1
    },
    "status": "no_alarm_rule",
    "enterprise_project_id": "0",
    "type": "TAG",
    "resources": []
  },
  {
    "group_name": "ResourceGroupCorrect_2",
    "create_time": 1606325669000,
    "group_id": "rg1606325669900Rk4eKkLMZ",
    "relation_ids": ["0"],
    "instance_statistics": {
      "unhealth": 0,
      "total": 1,
      "type_statistics": 1
    },
    "status": "no_alarm_rule",
    "enterprise_project_id": "0",
    "type": "TAG",
    "resources": []
  }
 ],
 "meta_data": {
  "total": 5
 }
}
```


Returned Values

- Normal

  200

- Abnormal

Returned Value	Description
400 Bad Request	Request error.

Returned Value	Description
401 Unauthorized	The authentication information is not provided or is incorrect.
403 Forbidden	Access to the requested page is forbidden.
408 Request Timeout	The request timed out.
429 Too Many Requests	Concurrent requests are excessive.
500 Internal Server Error	Failed to complete the request because of an internal service error.
503 Service Unavailable	The service is currently unavailable.

Error Codes

See **Error Codes**.

5.7 Event Monitoring

5.7.1 Reporting Events

Function

An API for reporting custom events is provided, which helps you collect and report abnormal events or important change events to Cloud Eye.

Debugging

You can debug the API in **API Explorer** which supports automatic authentication. API Explorer can automatically generate and debug example SDK code.

URI

POST /V1.0/{project_id}/events

- Parameter description

Table 5-121 Parameter description

Parameter	Mandatory	Description
project_id	Yes	**Definition** Project ID, which is used to specify the project that an asset belongs to. You can query the assets of a project by project ID. You can obtain the project ID from the API or console. For details about how to obtain the project ID, see **Obtaining a Project ID**. **Constraints** N/A **Range** 1 to 64 characters **Default Value** N/A

- Example
  POST https://{Cloud Eye endpoint}/V1.0/{project_id}/events

Request

NOTE

- Events with the same **time**, **project_id**, **event_source**, **event_name**, **event_type**, **sub_event_type**, **event_state**, **event_level**, **event_user**, **resource_id** and **resource_name** fields are considered as the same event.
- Event subcategory parameters are only available in regions **CN East-Shanghai1**, **CN East-Shanghai2**, **CN North-Beijing4**, and **CN South-Guangzhou**.

- Request parameters

Table 5-122 Parameter description

Parameter	Type	Mandatory	Description
[Array element]	Array of **EventItem** objects	Yes	**Definition** Request parameter for reporting custom events. **Constraints** Array length: [1,100]

Table 5-123 Parameter description of the **EventItem** field

Parameter	Mandatory	Type	Description
event_name	Yes	String	**Definition** Event name. **Constraints** N/A **Range** The value must start with a letter and can contain 1 to 64 characters. It can only contain letters, digits, and and underscores (_). **Default Value** N/A
event_source	Yes	String	**Definition** Event source. **Constraints** N/A **Range** The format is service.item. Set this parameter based on the site requirements. **service** and **item** each must be a string that starts with a letter and contains 3 to 32 characters, including only letters, digits, and underscores (_). **Default Value** N/A

Parameter	Mandatory	Type	Description
time	Yes	Long	**Definition** Time when the event occurred. The value is a UNIX timestamp, in milliseconds. **Constraints** Since there is a latency between the client and the server, the timestamp when data was inserted must be within the time range [Current time – 1h + 10s, Current time + 10 mins – 10s]. In this way, the data will be inserted to the database without being affected by the latency. **Range** The timestamp when data was inserted must be within the time range [Current time – 1h + 10s, Current time + 10 mins – 10s]. **Default Value** N/A
detail	Yes	Detail object	**Definition** Event details. For details, see **Table 5-124**. **Constraints** N/A

Table 5-124 detail data structure description

Parameter	Mandatory	Type	Description
content	No	String	**Definition** Event content. **Constraints** N/A **Range** 0 to 4,096 characters **Default Value** N/A **NOTE** In some scenarios, this field does not support **\n**. When this happens, **\n** is preferentially converted to **\\n**.

Parameter	Mandatory	Type	Description
group_id	No	String	**Definition** Resource group that the event belongs to. This ID must be the ID of an existing resource group. To query the group ID, perform the following steps: 1. Log in to the management console. 2. Click **Cloud Eye**. 3. Choose **Resource Groups**. Obtain the resource group ID in the **Name /ID** column. **Constraints** N/A **Range** 24 characters **Default Value** N/A
resource_id	No	String	**Definition** Resource ID. To query the resource ID, perform the following steps: 1. Log in to the management console. 2. Under **Computing**, select **Elastic Cloud Server**. On the **Resource Overview** page, obtain the resource ID. **Constraints** N/A **Range** The value allows a maximum of 128 characters and can only contain letters, digits, underscores (_), hyphens (-), and colons (:). Example: **6a69bf28-ee62-49f3-9785-845dacd799ec** **Default Value** N/A

Parameter	Mandatory	Type	Description
resource_name	No	String	**Definition** Resource name. **Constraints** N/A **Range** The value allows a maximum of 128 characters and can contain letters, digits, underscores (_), hyphens (-), and periods (.). **Default Value** N/A
event_state	No	String	**Definition** Event status. **Constraints** N/A **Range** The value can be: • **normal**: normal • **warning**: abnormal • **incident**: critical **Default Value** N/A
event_level	No	String	**Definition** Event severity. **Constraints** N/A **Range** The value can be: • **Critical** • **Major** • **Minor** • **Info** **Default Value** N/A

Parameter	Mandatory	Type	Description
event_user	No	String	**Definition** Event user. **Constraints** N/A **Range** The value allows 0 to 64 characters and can contain letters, digits, underscores (_), hyphens (-), and spaces. **Default Value** N/A
event_type	No	String	**Definition** Event type. **Constraints** **EVENT.SYS** indicates a system event, which is not from users. Only **EVENT.CUSTOM** can be transferred. **Range** The value can be: • **EVENT.SYS**: system event • **EVENT.CUSTOM**: custom event **Default Value** N/A
sub_event_type	No	String	**Definition** Event subcategory. **Constraints** N/A **Range** The options are as follows: If the event type is system event, the value can be **SUB_EVENT.OPS** (O&M event) or **SUB_EVENT.PLAN** (planned event). If the event type is custom event, the value is **SUB_EVENT.CUSTOM** (custom event). **Default Value** **SUB_EVENT.OPS**

Parameter	Mandatory	Type	Description
dimensions	No	Array of objects	**Definition** Event dimension. Resource information is described by dimension. Event alarm rules can be configured by dimension to monitor specified resources and resource groups. For parameter details, see **Table 5-125**. **Constraints** A maximum of four dimensions are supported.

Table 5-125 dimensions data structure description

Parameter	Type	Mandatory	Description
name	String	Yes	**Definition** Resource dimension, for example, **instance_id** for ECSs. For details about the dimension of each service, see the **key** field in **Services Interconnected with Cloud Eye**. **Constraints** N/A **Range** 1 to 32 characters **Default Value** N/A
value	String	Yes	**Definition** Resource dimension value, which is the instance ID of the resource, for example, **4270ff17-aba3-4138-89fa-820594c39755** (ECS ID). **Constraints** N/A **Range** 1 to 256 characters **Default Value** N/A

- Example request

```
[
 {
  "event_name": "systemInvaded",
  "event_source": "financial.System",
  "time": 1742264993000,
  "detail": {
   "content": "The financial system was invaded",
   "group_id": "rg15221211517051YWWkEnVd",
   "resource_id": "1234567890sjgggad",
   "resource_name": "ecs001",
   "event_state": "normal",
   "event_level": "Major",
   "event_user": "xiaokong",
   "event_type": "EVENT.CUSTOM",
   "sub_event_type": "SUB_EVENT.CUSTOM",
   "dimensions": [
    {
     "name": "instance_id",
     "value": "instance_xxx"
    }
   ]
  }
 }
]
```

Response

- Response parameters

Table 5-126 Parameter description

Parameter	Type	Description
Array elements	Array of objects	**Definition** Event list. For details, see **Table 5-127**.

Table 5-127 Response parameters

Parameter	Mandatory	Type	Description
event_id	Yes	String	**Definition** Event ID. **Range** N/A
event_name	Yes	String	**Definition** Event name. **Range** N/A

- Example response

```
[
    {
```



```
        "event_id":"evdgiqwgedkkcvhdjcdu346",
        "event_name":"systemInvaded"
    }
]
```

Returned Values

- Normal

  201

- Abnormal

Returned Value	Description
400 Bad Request	Request error.
401 Unauthorized	The authentication information is not provided or is incorrect.
403 Forbidden	Access to the requested page is forbidden.
408 Request Timeout	The request timed out.
429 Too Many Requests	Concurrent requests are excessive.
500 Internal Server Error	Failed to complete the request because of an internal service error.
503 Service Unavailable	The service is currently unavailable.

Error Codes

See **Error Codes**.

5.7.2 Querying Events

Function

This API is used to query events, including system events and custom events.

NOTE

Event subcategory parameters are only available in regions **CN East-Shanghai1**, **CN East-Shanghai2**, **CN North-Beijing4**, and **CN South-Guangzhou**.

Debugging

You can debug the API in **API Explorer** which supports automatic authentication. API Explorer can automatically generate and debug example SDK code.

URI

GET /V1.0/{project_id}/events

- Parameter description

Table 5-128 Parameter description

Parameter	Type	Mandatory	Description
project_id	String	Yes	**Definition** Project ID, which is used to specify the project that an asset belongs to. You can query the assets of a project by project ID. You can obtain the project ID from the API or console. For details about how to obtain the project ID, see **Obtaining a Project ID**. **Constraints** N/A **Range** 1 to 64 characters **Default Value** N/A
event_type	String	No	**Definition** Event type. **Constraints** N/A **Range** The value can be: • **EVENT.SYS**: system event • **EVENT.CUSTOM**: custom event **Default Value** N/A

Parameter	Type	Mandatory	Description
sub_event_type	String	No	**Definition** Event subcategory. **Constraints** N/A **Range** The options are as follows: If the event type is system event, the value can be **SUB_EVENT.OPS** (O&M event) or **SUB_EVENT.PLAN** (planned event). If the event type is custom event, the value is **SUB_EVENT.CUSTOM** (custom event). **Default Value** **SUB_EVENT.OPS**
event_name	String	No	**Definition** Event name. The name can be a system event name or a custom event name. **Constraints** N/A **Range** 1 to 64 characters **Default Value** N/A
from	Integer	No	**Definition** Start time of the query. The value is a UNIX timestamp, in milliseconds. Example: **1605952700911** **Constraints** N/A **Range** N/A **Default Value** N/A

Parameter	Type	Mandatory	Description
to	Integer	No	**Definition** End time of the query. The value is a UNIX timestamp, in milliseconds. Example: **1606557500911** **Constraints** **from** must be earlier than **to**. **Range** N/A **Default Value** N/A
start	Integer	No	**Definition** Pagination start value. The value is an integer. **Constraints** N/A **Range** ≥ 0 **Default Value** 0
limit	Integer	No	**Definition** Maximum number of records that can be queried at a time. **Constraints** N/A **Range** (0,100] **Default Value** 100

- Example
  GET https://{Cloud Eye endpoint}/V1.0/{project_id}/events

Request

None

Response

- Response parameters

Table 5-129 Parameter description

Parameter	Type	Mandatory	Description
events	Array of Events objects	No	**Definition** One or more pieces of event data. For details, see **Table 5-130**.
meta_data	MetaData object	No	**Definition** Number of metadata records in the query results. For details, see **Table 5-131**.

Table 5-130 events field description

Parameter	Type	Mandatory	Description
event_name	String	No	**Definition** Event name. **Range** N/A
event_type	String	No	**Definition** Event type. **Range** N/A
sub_event_type	String	No	**Definition** Event subcategory. **Range** The value can be: • **SUB_EVENT.OPS**: O&M event • **SUB_EVENT.PLAN**: planned event • **SUB_EVENT.CUSTOM**: custom event

Parameter	Type	Mandatory	Description
event_count	Integer	No	**Definition** Number of times that the event occurs within the specified time range. **Range** N/A
latest_occur_time	Long	No	**Definition** Time when the event last occurred. **Range** N/A
latest_event_source	String	No	**Definition** Event source. If the event is a system event, the source is the namespace of each service. To view the namespace of each service, see **Services Interconnected with Cloud Eye**. If the event is a custom event, the event source is defined by the user. **Range** N/A

Table 5-131 meta_data data structure description

Parameter	Type	Mandatory	Description
total	Integer	No	**Definition** Total number of events. **Range** N/A

- Example response

```
{
 "events": [
  {
   "event_name": "rebootServer",
   "event_type": "EVENT.SYS",
   "sub_event_type": "SUB_EVENT.OPS",
   "event_count": 5,
   "latest_occur_time": 1606302400000,
   "latest_event_source": "SYS.ECS"
  },
  {
```

```
    "event_name": "deleteVolume",
    "event_type": "EVENT.SYS",
    "sub_event_type": "SUB_EVENT.OPS",
    "event_count": 6,
    "latest_occur_time": 1606300359126,
    "latest_event_source": "SYS.EVS"
  },
  {
    "event_name": "event_001",
    "event_type": "EVENT.CUSTOM",
    "sub_event_type": "SUB_EVENT.CUSTOM",
    "event_count": 4,
    "latest_occur_time": 1606499035522,
    "latest_event_source": "TEST.System"
  }
 ],
 "meta_data": {
   "total": 10
 }
}
```


Returned Values

- Normal

  200

- Abnormal

Returned Value	Description
400 Bad Request	Request error.
401 Unauthorized	The authentication information is not provided or is incorrect.
403 Forbidden	Access to the requested page is forbidden.
408 Request Timeout	The request timed out.
429 Too Many Requests	Concurrent requests are excessive.
500 Internal Server Error	Failed to complete the request because of an internal service error.
503 Service Unavailable	The service is currently unavailable.

Error Codes

See **Error Codes**.

5.7.3 Querying Details of an Event

Function

This API is used to query details of an event based on the event name.

NOTE

Event subcategory parameters are only available in regions **CN East-Shanghai1**, **CN East-Shanghai2**, **CN North-Beijing4**, and **CN South-Guangzhou**.

Debugging

You can debug the API in **API Explorer** which supports automatic authentication. API Explorer can automatically generate and debug example SDK code.

URI

GET /V1.0/{project_id}/event/{event_name}

- Parameter description

Table 5-132 Parameter description

Parameter	Type	Mandatory	Description
project_id	String	Yes	**Definition** Project ID, which is used to specify the project that an asset belongs to. You can query the assets of a project by project ID. You can obtain the project ID from the API or console. For details about how to obtain the project ID, see **Obtaining a Project ID**. **Constraints** N/A **Range** 1 to 64 characters **Default Value** N/A
event_name	String	Yes	**Definition** Event name. The name can be a system event name or a custom event name. **Constraints** N/A **Range** 1 to 64 characters **Default Value** N/A

Parameter	Type	Mandatory	Description
event_type	String	Yes	**Definition** Event type. **Constraints** N/A **Range** The value can be: • **EVENT.SYS**: system event • **EVENT.CUSTOM**: custom event **Default Value** N/A
sub_event_type	String	No	**Definition** Event subcategory. **Constraints** N/A **Range** The options are as follows: If the event type is system event, the value can be **SUB_EVENT.OPS** (O&M event) or **SUB_EVENT.PLAN** (planned event). If the event type is custom event, the value is **SUB_EVENT.CUSTOM** (custom event). **Default Value** **SUB_EVENT.OPS**
event_source	String	No	**Definition** Event source. The value is the namespace of each cloud service. For details about the namespaces of cloud services, see **Events Supported by Event Monitoring**.
event_level	String	No	**Constraints** N/A **Range** The value cannot exceed 32 characters. Regular matching: ^((([a-z]|[A-Z]){1}([a-z]|[A-Z]|[0-9]|_)*\.([a-z]|[A-Z]){1}([a-z]|[A-Z]|[0-9]|_)*)|)$ **Default Value** N/A

Parameter	Type	Mandatory	Description
event_user	String	No	**Definition** Event severity, which can be **Critical**, **Major**, **Minor**, or **Info**. **Constraints** N/A **Range** **Critical**, **Major**, **Minor**, or **Info** **Default Value** N/A
event_state	String	No	**Definition** Name of the user who reports the event monitoring data. It can also be a project ID. **Constraints** N/A **Range** The value cannot exceed 64 characters. Regular matching: ^([a-z]|[A-Z]|[0-9]|_|-|\/| |@|\.|)+$ **Default Value** N/A
from	Long	No	**Definition** Event status, which can be **normal**, **warning**, or **incident**. **Constraints** N/A **Range** **normal**, **warning**, or **incident** **Default Value** N/A

Parameter	Type	Mandatory	Description
to	Long	No	**Definition** Start time of the query. The value is a UNIX timestamp, in milliseconds. Example: **1605952700911** **Constraints** N/A **Range** N/A **Default Value** N/A
start	Integer	No	**Definition** End time of the query. The value is a UNIX timestamp, in milliseconds. **Constraints** **from** must be earlier than **to**. **Range** N/A **Default Value** N/A

Parameter	Type	Mandatory	Description
limit	Integer	No	**Definition** Pagination start value. **Constraints** N/A **Range** ≥ 0 Regular matching: ^(0|[1-9][0-9]*)$ **Default Value** 0 **Definition** Maximum number of records that can be queried at a time. The value range is (0,100] and the default value is **100**. **Constraints** N/A **Range** 1 to 100 Regular matching: ^([1-9]|[1-9][0-9]|100)$ **Default Value** 100

- Example
  ```
  GET https://{Cloud Eye endpoint}/V1.0/{project_id}/event/{event_name}
  ```

Request

None

Response

- Response parameters

Table 5-133 Parameter description

Parameter	Type	Mandatory	Description
event_name	String	No	**Definition** Event name. The name can be a system event name or a custom event name. **Range** N/A
event_type	String	No	**Definition** Event type. **Range** The value can be: • **EVENT.SYS**: system event • **EVENT.CUSTOM**: custom event
sub_event_type	String	No	**Definition** Event subcategory. **Range** The value can be: If the event type is system event, the value can be **SUB_EVENT.OPS** or **SUB_EVENT.PLAN**. If the event type is custom event, the value is **SUB_EVENT.CUSTOM**. • **SUB_EVENT.OPS**: O&M event • **SUB_EVENT.PLAN**: planned event • **SUB_EVENT.CUSTOM**: custom event
event_users	Array of strings	No	**Definition** Name of the user who reports the event. It can also be a project ID. **Range** N/A

Parameter	Type	Mandatory	Description
event_sources	Array of strings	No	**Definition** Event source. If the event is a system event, the source is the namespace of each service. To view the namespace of each service, see **Services Interconnected with Cloud Eye**. If the event is a custom event, the event source is defined by the user. **Range** N/A
event_info	Array of objects	No	**Definition** Details of one or more events. For details, see **Table 5-134**.
meta_data	MetaData object	No	**Definition** Number of metadata records in the query results. For details, see **Table 5-137**.

Table 5-134 event_info data structure description

Parameter	Type	Mandatory	Description
event_name	String	Yes	**Definition** Event name. **Range** The value must start with a letter. It allows 1 to 64 characters and can only contain letters, digits, and underscores (_).
event_source	String	No	**Definition** Event source. **Range** The namespace must be in the **service.item** format and contain 3 to 32 characters. **service** and **item** each must start with a letter and contain only letters, digits, and underscores (_).

Parameter	Type	Mandatory	Description
time	Long	Yes	**Definition** Time when an incident occurred. The value is a UNIX timestamp, in milliseconds. **Range** Since there is a latency between the client and the server, the timestamp when data was inserted must be within the time range [Current time – 1h + 20s, Current time + 10 mins – 20s]. In this way, the data will be inserted to the database without being affected by the latency.
detail	Detail object	Yes	**Definition** Event details. For details, see **Table 5-135**.
event_id	String	No	**Definition** Event ID. **Range** N/A

Table 5-135 detail data structure description

Parameter	Type	Mandatory	Description
content	String	No	**Definition** Event content. **Range** Max. 4,096 characters
group_id	String	No	**Definition** Resource group that the event belongs to. **Range** 24 characters
resource_id	String	No	**Definition** Resource ID. **Range** Max. 128 characters

Parameter	Type	Mandatory	Description
resource_name	String	No	**Definition** Resource name. **Range** Max. 128 characters
event_state	String	No	**Definition** Event status. **Range** The value can be: • **normal** • **warning** • **incident**
event_level	String	No	**Definition** Event severity. **Range** The value can be: • **Critical** • **Major** • **Minor** • **Info**
event_user	String	No	**Definition** Event user. **Range** Max. 64 characters
event_type	String	No	**Definition** Event type. **Range** The value can be: • **EVENT.SYS**: system event • **EVENT.CUSTOM**: custom event.

Parameter	Type	Mandatory	Description
sub_event_type	String	No	**Definition** Event subcategory. **Range** The options are as follows: If the event type is system event, the value can be **SUB_EVENT.OPS** (default) or **SUB_EVENT.PLAN**. If the event type is custom event, the value is **SUB_EVENT.CUSTOM**. • **SUB_EVENT.OPS**: O&M event • **SUB_EVENT.PLAN**: planned event • **SUB_EVENT.CUSTOM**: custom event
dimensions	Array of objects	No	**Definition** Event dimension. Resource information is described by dimension. Event alarm rules can be configured by dimension to monitor specified resources and resource groups. For details, see **Table 5-136**. **Range** A maximum of four dimensions are supported.

Table 5-136 dimensions data structure description

Parameter	Type	Mandatory	Description
name	String	No	**Definition** Monitoring dimension name. For example, the ECS dimension is **instance_id**. For details about the dimension of each service, see the **key** column in **Services Interconnected with Cloud Eye**. **Range** N/A

Parameter	Type	Mandatory	Description
value	String	No	**Definition** Dimension value, for example, an ECS ID. **Range** 1 to 256 characters

Table 5-137 meta_data data structure description

Parameter	Type	Mandatory	Description
total	Integer	No	**Definition** Total number of records. **Range** N/A

- Example response

```
{
 "event_name": "rebootServer",
 "event_type": "EVENT.SYS",
 "sub_event_type": "SUB_EVENT.OPS",
 "event_users": [
   ""
 ],
 "event_sources": [
   "SYS.ECS"
 ],
 "event_info": [
  {
    "event_id": "ev1606302402256R6doP5YeZ",
    "event_name": "rebootServer",
    "event_source": "SYS.ECS",
    "time": 1606302400000,
    "detail": {
      "content": "{\"resourceSpecCode\":\"kc1.4xlarge.2.linux\",\"enterpriseProjectId
\":\"6efb843e-391a-46a8-afc8-7fe51c9dd575\"}",
      "group_id": "",
      "resource_id": "ef8dad27-0488-4de7-bb43-1a0df9806d90",
      "resource_name": "CES-POROS-0001",
      "event_state": "normal",
      "event_level": "Minor",
      "event_user": "",
      "event_type": "EVENT.SYS",
      "sub_event_type": "SUB_EVENT.OPS",
      "dimensions": [
       {
         "name": "instance_id",
         "value": "fddad01f-e3b6-420d-8fdc-a42451de7c34"
       }
      ]
    }
  },
  {
    "event_id": "ev1606296088071wGoAOxVYa",
```

```
    "event_name": "rebootServer",
    "event_source": "SYS.ECS",
    "time": 1606296086000,
    "detail": {
      "content": "{\"resourceSpecCode\":\"kc1.4xlarge.2.linux\",\"enterpriseProjectId
\":\"6efb843e-391a-46a8-afc8-7fe51c9dd575\"}",
      "group_id": "",
      "resource_id": "ef8dad27-0488-4de7-bb43-1a0df9806d90",
      "resource_name": "CES-POROS-0001",
      "event_state": "normal",
      "event_level": "Minor",
      "event_user": "",
      "event_type": "EVENT.SYS",
      "sub_event_type": "SUB_EVENT.OPS",
      "dimensions": [
       {
         "name": "instance_id",
         "value": "fddad01f-e3b6-420d-8fdc-a42451de7c34"
       }
      ]
    }
   },
   {
    "event_id": "ev1604654426090g7g37E6Yb",
    "event_name": "rebootServer",
    "event_source": "SYS.ECS",
    "time": 1604654425000,
    "detail": {
      "content": "{\"resourceSpecCode\":\"c6.4xlarge.2.linux\",\"enterpriseProjectId\":\"129559eb-
f795-4b5f-9e46-cbd43a462362\"}",
      "group_id": "",
      "resource_id": "0bfa63ee-31f5-40a9-b992-50992c80c58a",
      "resource_name": "ndrv2-pod-ops-0001",
      "event_state": "normal",
      "event_level": "Minor",
      "event_user": "",
      "event_type": "EVENT.SYS",
      "sub_event_type": "SUB_EVENT.OPS",
      "dimensions": [
       {
         "name": "instance_id",
         "value": "fddad01f-e3b6-420d-8fdc-a42451de7c34"
       }
      ]
    }
   }
 ],
 "meta_data": {
   "total": 5
 }
}
```


Returned Values

- Normal

  200

- Abnormal

Returned Value	Description
400 Bad Request	Request error.
401 Unauthorized	The authentication information is not provided or is incorrect.

Returned Value	Description
403 Forbidden	Access to the requested page is forbidden.
408 Request Timeout	The request timed out.
429 Too Many Requests	Concurrent requests are excessive.
500 Internal Server Error	Failed to complete the request because of an internal service error.
503 Service Unavailable	The service is currently unavailable.

Error Codes

See **Error Codes**.

6 API V2

6.1 Alarm Rules

6.1.1 Creating an Alarm Rule (Recommended)

Function

This API is used to create alarm rules.

Debugging

You can debug this API through automatic authentication in **API Explorer** or use the SDK sample code generated by API Explorer.

URI

POST /v2/{project_id}/alarms

Table 6-1 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	**Definition** Tenant ID. **Constraints**: None **Value range**: Project ID, used to specify the project that an asset belongs to. You can query the assets of a project by project ID. You can obtain the project ID by calling an API or on the console. For details, see **Obtaining a Project ID**. The value must contain of 1 to 64 characters. **Default value**: None

Request Parameters

Table 6-2 Request header parameters

Parameter	Mandatory	Type	Description
Content-Type	No	String	**Definition** MIME type of the request body. **Constraints**: None **Value range**: The value can contain 1 to 64 characters. **Default value**: The default type is **application/json; charset=UTF-8**. **Default value:** application/json; charset=UTF-8

Parameter	Mandatory	Type	Description
X-Auth-Token	No	String	**Definition** User token. **Constraints**: None **Value range**: The value can contain 1 to 16,384 characters. **Default value**: None

Table 6-3 Request body parameters

Parameter	Mandatory	Type	Description
name	Yes	String	Name of an alarm rule. The name can contain 1 to 128 characters, including only letters, digits, underscores (_), and hyphens (-).
description	No	String	Alarm rule description. The description can contain 0 to 256 characters.
namespace	Yes	String	Query the namespace of a service. For details about the namespace of each service, see [Service Name](ces_03_0059.xml).
resource_group_id	No	String	Resource group ID, which starts with **rg** and is followed by 22 characters, including letters and digits.
resources	Yes	Array<Array<**Dimension**>>	Resource list. If an alarm rule is created for all resources or resources in a resource group, leave the resource dimension blank. If the alarm rule is created for specified resources, the resource dimension value is mandatory, and you can specify multiple resources to be monitored at a time.

Parameter	Mandatory	Type	Description
policies	No	Array of **Policy** objects	Alarm policy. This parameter is mandatory when **alarm_template_id** is left blank.
type	Yes	String	**Definition**: Alarm rule type. **Constraints**: None **Value range**: Enumerated value. **ALL_INSTANCE** indicates alarm rules for metrics of all resources. **RESOURCE_GROUP** indicates alarm rules for metrics of resources in a resource group. **MULTI_INSTANCE** indicates alarm rules for metrics of specified resources. **EVENT.SYS** indicates alarm rules for system events. **EVENT.CUSTOM** indicates alarm rules for custom events. **DNSHealthCheck** indicates alarm rules for health checks. **Default value**: None Enumeration values: • **EVENT.SYS** • **EVENT.CUSTOM** • **DNSHealthCheck** • **RESOURCE_GROUP** • **MULTI_INSTANCE** • **ALL_INSTANCE**
alarm_notifications	No	Array of **Notification** objects	Action to be triggered by the alarm.
ok_notifications	No	Array of **Notification** objects	Action to be triggered after an alarm is cleared.
notification_begin_time	No	String	Time when the alarm notification was enabled.

Parameter	Mandatory	Type	Description
notification_end_time	No	String	Time when the alarm notification was disabled.
effective_timezone	No	String	Time zone, for example, **GMT-08:00**, **GMT+08:00**, or **GMT+0:00**.
enterprise_project_id	No	String	Enterprise project ID
enabled	Yes	Boolean	Whether to enable the alarm rule. true: enabled; false: disabled.
notification_enabled	Yes	Boolean	Whether to enable alarm notification. true: enabled; false: disabled.
alarm_template_id	No	String	ID of an alarm template associated with an alarm rule. If this parameter is specified, the policy associated with the alarm rule changes accordingly with the alarm template policy.
tags	No	Array of **ResourceTag** objects	Tenant tags.
product_name	No	String	Product name. It needs to be specified when product alarm rules with multiple dimensions are created. Generally, the value format is *Service namespace,First-level dimension of the service*, for example, **SYS.ECS,instance_id**. **Regex Pattern:** ^(([a-z]|[A-Z]){1}([a-z]|[A-Z]|[0-9]|_|-|\.){0,31}(,([a-z]|[A-Z]){1}([a-z]|[A-Z]|[0-9]|_|-|\.){0,31}){0,3}|)$

Parameter	Mandatory	Type	Description
resource_level	No	String	Product alarm rules with multiple dimensions need to be specified as product-level rules during creation. If the value of **resource_level** is **product**, cloud product alarm rules with multiple dimensions are used. If the value of **resource_level** is **dimension** or not specified, the original rule type is used. Enumeration values: • **product** • **dimension**

Table 6-4 Dimension

Parameter	Mandatory	Type	Description
name	Yes	String	Dimension of a resource. For example, the dimension of an ECS can be **instance_id**. A maximum of four dimensions are supported. For the metric dimension of each resource, see **Service metric dimension**. **Regex Pattern:** ^([a-z]|[A-Z]){1}([a-z]|[A-Z]|[0-9]|_|-)*$
value	No	String	Value of a resource dimension, which is the resource ID, for example, **4270ff17-aba3-4138-89fa-820594c39755**. **Regex Pattern:** ^((([a-z]|[A-Z]|[0-9]|*|_|/|#|\(|\)){1}([a-z]|[A-Z]|[0-9]|_|-|\.|*|/|#|\(|\))*))$

Table 6-5 Policy

Parameter	Mandatory	Type	Description
metric_name	Yes	String	Metric name of a resource. The name must start with a letter and contain only digits, letters, and underscores. The length ranges from 1 to 64 characters. For example, **cpu_util** of an ECS indicates the CPU usage of the ECS. **mongo001_command_ps** in DDS indicates the command execution frequency. For details about the metric name of each service, see **Service metric name**.
period	Yes	Integer	Monitoring period of a metric, in seconds. The default value is **0**. For an event alarm, set this parameter to **0**. **1** indicates the original rollup period of a metric. For example, if the original rollup period of an RDS metric is 60s, its data point is calculated every 60 seconds. For details about the original rollup period of each cloud service metric, see **Services Interconnected with Cloud Eye**. **300** indicates that the metric rollup period is 5 minutes. **Value range:** 0-86400 Enumeration values: • **0** • **1** • **300** • **1200** • **3600** • **14400** • **86400**

Parameter	Mandatory	Type	Description
filter	Yes	String	Aggregation mode. average: average value; variance: variance; min: minimum value; max: maximum value; sum: sum; tp99: 99 percentile; tp95: 95 percentile; tp90: 90 percentile
comparison_operator	Yes	String	Threshold symbol. The value can be >, <, >=, <=, =, **!=**, **cycle_decrease**, **cycle_increase**, or **cycle_wave**. **cycle_decrease** indicates the decrease compared with the last period, **cycle_increase** indicates the increase compared with the last period, and **cycle_wave** indicates the increase or decrease compared with the last period. All of them can be used in alarm rules for metrics. >, <, >=, <=, =, and **!=** can be used for alarm rules for events.
value	No	Number	Alarm threshold If there is only one threshold, **value** and **alarm_level** are used in pairs. If there are both **hierarchical_value** and **value**, **hierarchical_value** is used. For detailed thresholds, see the value range of each metric in the appendix. For example, you can set ECS **cpu_util** to **80**. For detailed thresholds, see the value range of each metric in the appendix. For example, you can set ECS **cpu_util** to **80** in **Services Interconnected with Cloud Eye**.

Parameter	Mandatory	Type	Description
hierarchical_value	No	HierarchicalValue object	Multi-level alarm threshold. If there are both **hierarchical_value** and **value**, **hierarchical_value** prevails. When you create or modify an alarm rule, you can set only one threshold in the following scenarios: 1. The alarm type is **Metric** and the alarm policy is **Trigger an alarm when all policies are met**. 2. The alarm type is **Event**.
unit	No	String	Data unit.
count	Yes	Integer	Number of consecutive alarm triggering times. For event alarms, the value ranges from **1** to **180**. For metric and website alarms, the value can be **1**, **2**, **3**, **4**, **5**, **10**, **15**, **30**, **60**, **90**, **120**, or **180**.

Parameter	Mandatory	Type	Description
suppress_duration	No	Integer	Alarm suppression time, in seconds. This parameter corresponds to the last field in the alarm policy when an alarm rule is created on the Cloud Eye console. This field is used to avoid frequent alarms. **0** indicates that the alarm is not suppressed and alarms are generated as long as the conditions are met. **300** indicates that an alarm is generated every 5 minutes as long as the alarm triggering conditions are met. **Value range:** 0-86400 Enumeration values: • **0** • **300** • **600** • **900** • **1800** • **3600** • **10800** • **21600** • **43200** • **86400**
level	No	Integer	Alarm severity, which can be **1** (critical), ** 2** (major), **3** (minor), or **4** (informational). The default value is **2**.
namespace	No	String	**namespace** and **dimension_name** need to be specified for product-level rules. For details about the namespace of each service, see **Service namespace**. **Regex Pattern:** ^((([a-z]|[A-Z]){1}([a-z]|[A-Z]|[0-9]|_)*\.([a-z]|[A-Z]){1}([a-z]|[A-Z]|[0-9]|_)*)|)$

Parameter	Mandatory	Type	Description
dimension_name	No	String	The namespace and dimension_name parameters are added to the product-level rule to specify the policy to which the product belongs. Currently, a maximum of four dimensions are supported. For details about the metric dimension name of each service resource, see [Service dimension name](ces_03_0059.xml). Example: instance_id in the single-dimension scenario; instance_id,disk in the multi-dimension scenario **Regex Pattern:** ^(([a-z]|[A-Z]){1}([a-z]|[A-Z]|[0-9]|_|-|\.){0,31}(,([a-z]|[A-Z]){1}([a-z]|[A-Z]|[0-9]|_|-|\.){0,31}){0,3}|)$

Table 6-6 HierarchicalValue

Parameter	Mandatory	Type	Description
critical	No	Double	Threshold for critical alarms. **Value range:** -1.7976931348623156E108-1.7976931348623156E108
major	No	Double	Threshold for major alarms. **Value range:** -1.7976931348623156E108-1.7976931348623156E108
minor	No	Double	Threshold for minor alarms. **Value range:** -1.7976931348623156E108-1.7976931348623156E108
info	No	Double	Threshold for informational alarms. **Value range:** -1.7976931348623156E108-1.7976931348623156E108

Table 6-7 Notification

Parameter	Mandatory	Type	Description
type	Yes	String	Notification type. The value can be **notification** (SMN notifications), **contact** (account contacts), **contactGroup** (notification groups), or **autoscaling** (AS notifications). **autoscaling** is used only in AS and is not recommended. **groupwatch**, **ecsRecovery**, and **iecAction** are no longer used. Enumeration values: • **notification** • **autoscaling** • **groupwatch** • **ecsRecovery** • **contact** • **contactGroup** • **iecAction**
notification_list	Yes	Array of strings	List of objects to be notified if the alarm status changes. The value of **topicUrn** can be obtained from SMN. For details, see section "Querying Topics". If **type** is set to **notification**, the value of **notificationList** cannot be left blank. If **type** is set to **autoscaling**, the value of **notification_list** must be left blank. Note: If **alarm_action_enabled** is set to **true**, **alarm_actions**, **ok_actions**, or both of them must be specified. If both **alarm_actions** and **ok_actions** are specified, their **notification_list** values must be the same.

Table 6-8 ResourceTag

Parameter	Mandatory	Type	Description
key	Yes	String	Tag key. The value can contain up to 128 Unicode characters. **Regex Pattern:** ^((?!\s)(?!_sys_)[\p{L}\p{Z}\p{N}_.:=+\-@]*)(?<!\s)$
value	Yes	String	Value. Each tag value can contain a maximum of 255 Unicode characters. **Regex Pattern:** ^([\p{L}\p{Z}\p{N}_.:\/=+\-@]*)$

Response Parameters

Status code: 201

Table 6-9 Response body parameters

Parameter	Type	Description
alarm_id	String	ID of an alarm rule, which starts with **al** and is followed by 22 characters, including letters and digits.

Status code: 400

Table 6-10 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 500

Table 6-11 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Example Requests

Creating an alarm rule whose **name** is **alarm-lxy-rg-RDS**, **type** is **RESOURCE_GROUP**, ** suppress_duration** is **86400**, and **level** is **2**.

```
{
  "name" : "alarm-lxy-rg-RDS",
  "description" : "",
  "namespace" : "SYS.RDS",
  "type" : "RESOURCE_GROUP",
  "resources" : [ [ {
    "name" : "rds_cluster_id"
  } ] ],
  "policies" : [ {
    "metric_name" : "rds001_cpu_util",
    "period" : 1,
    "filter" : "average",
    "comparison_operator" : ">=",
    "value" : 0,
    "unit" : "%",
    "count" : 1,
    "suppress_duration" : 86400,
    "level" : 2
  } ],
  "enabled" : true,
  "notification_enabled" : false,
  "resource_group_id" : "rg1623429506587NbRweoa3J",
  "enterprise_project_id" : "a9d919b7-0456-4bb8-b470-6a23b64f4f7e",
  "alarm_template_id" : "at1628592157541dB1klWgY6"
}
```

Example Responses

Status code: 201

Alarm rule created.

```
{
  "alarm_id" : "alCzk8o9dtSQHtiDgb44Eepw"
}
```

Status Codes

Status Code	Description
201	Alarm rule created.
400	Parameter verification failed.

Status Code	Description
500	Internal system error.

Error Codes

See **Error Codes**.

6.1.2 Batch Deleting Alarm Rules

Function

This API (V2) is used to batch delete alarm rules.

Debugging

You can debug this API through automatic authentication in **API Explorer** or use the SDK sample code generated by API Explorer.

URI

POST /v2/{project_id}/alarms/batch-delete

Table 6-12 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	**Definition** Tenant ID. **Constraints**: None **Value range**: Project ID, used to specify the project that an asset belongs to. You can query the assets of a project by project ID. You can obtain the project ID by calling an API or on the console. For details, see **Obtaining a Project ID**. The value must contain of 1 to 64 characters. **Default value**: None

Request Parameters

Table 6-13 Request header parameters

Parameter	Mandatory	Type	Description
Content-Type	No	String	**Definition** MIME type of the request body. **Constraints**: None **Value range**: The value can contain 1 to 64 characters. **Default value**: The default type is **application/json; charset=UTF-8**. **Default value:** application/json; charset=UTF-8
X-Auth-Token	No	String	**Definition** User token. **Constraints**: None **Value range**: The value can contain 1 to 16,384 characters. **Default value**: None

Table 6-14 Request body parameters

Parameter	Mandatory	Type	Description
alarm_ids	Yes	Array of strings	IDs of the alarm rules to be deleted in batches.

Response Parameters

Status code: 200

Table 6-15 Response body parameters

Parameter	Type	Description
alarm_ids	Array of strings	IDs of the alarm rules that are deleted.

Status code: 400

Table 6-16 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 500

Table 6-17 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Example Requests

Deleting alarm rules in batches.

```
{
  "alarm_ids" : [ "al12345678901234567890" ]
}
```

Example Responses

Status code: 200

Alarm rule deleted.

```
{
  "alarm_ids" : [ "alCzk8o9dtSQHtiDgb44Eepw" ]
}
```


Status Codes

Status Code	Description
200	Alarm rule deleted.
400	Parameter verification failed.
500	Internal system error.

Error Codes

See **Error Codes**.

6.1.3 Enabling or Disabling Alarm Rules in Batches

Function

This API is used to enable or disable alarm rules in batches.

Debugging

You can debug this API through automatic authentication in **API Explorer** or use the SDK sample code generated by API Explorer.

URI

POST /v2/{project_id}/alarms/action

Table 6-18 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	**Definition** Tenant ID. **Constraints**: None **Value range**: Project ID, used to specify the project that an asset belongs to. You can query the assets of a project by project ID. You can obtain the project ID by calling an API or on the console. For details, see **Obtaining a Project ID**. The value must contain of 1 to 64 characters. **Default value**: None

Request Parameters

Table 6-19 Request header parameters

Parameter	Mandatory	Type	Description
Content-Type	No	String	**Definition** MIME type of the request body. **Constraints**: None **Value range**: The value can contain 1 to 64 characters. **Default value**: The default type is **application/json; charset=UTF-8**. **Default value:** application/json; charset=UTF-8

Parameter	Mandatory	Type	Description
X-Auth-Token	No	String	**Definition** User token. **Constraints**: None **Value range**: The value can contain 1 to 16,384 characters. **Default value**: None

Table 6-20 Request body parameters

Parameter	Mandatory	Type	Description
alarm_ids	Yes	Array of strings	IDs of alarm rules to be enabled or disabled in batches.
alarm_enabled	Yes	Boolean	Whether to enable the alarm rule. true: enabled; false: disabled.

Response Parameters

Status code: 200

Table 6-21 Response body parameters

Parameter	Type	Description
alarm_ids	Array of strings	IDs of alarm rules that were enabled or disabled.

Status code: 400

Table 6-22 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.

Parameter	Type	Description
request_id	String	Request ID.

Status code: 500

Table 6-23 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Example Requests

Enabling or disabling alarm rules in batches.

```
{
  "alarm_ids" : [ "al12345678901234567890" ],
  "alarm_enabled" : true
}
```

Example Responses

Status code: 200

Alarm rules enabled or disabled.

```
{
  "alarm_ids" : [ "alCzk8o9dtSQHtiDgb44Eepw" ]
}
```

Status Codes

Status Code	Description
200	Alarm rules enabled or disabled.
400	Parameter verification failed.
500	Internal system error.

Error Codes

See **Error Codes**.

6.1.4 Querying Alarm Rules (Recommended)

Function

This API is used to query the alarm rule list.

Debugging

You can debug this API through automatic authentication in **API Explorer** or use the SDK sample code generated by API Explorer.

URI

GET /v2/{project_id}/alarms

Table 6-24 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	**Definition** Tenant ID. **Constraints**: None **Value range**: Project ID, used to specify the project that an asset belongs to. You can query the assets of a project by project ID. You can obtain the project ID by calling an API or on the console. For details, see **Obtaining a Project ID**. The value must contain of 1 to 64 characters. **Default value**: None

Table 6-25 Query Parameters

Parameter	Mandatory	Type	Description
alarm_id	No	String	Alarm rule ID. **Regex Pattern:** ^al([0-9A-Za-z]){22}$

Parameter	Mandatory	Type	Description
name	No	String	Name of an alarm rule. The name can contain 1 to 128 characters, including only letters, digits, underscores (_), and hyphens (-). **Regex Pattern:** ^([\u4E00-\u9FFF]|[a-z]|[A-Z]|[0-9]|_|-){1, 128}$
namespace	No	String	Namespace of a service. For details about the namespace of each service, see **Namespace**. **Regex Pattern:** ^((([a-z]|[A-Z]){1}([a-z]|[A-Z]|[0-9]|_)*\.([a-z]|[A-Z]){1}([a-z]|[A-Z]|[0-9]|_)*)|)$
resource_id	No	String	ID of a resource in an alarm rule. If the resource has multiple dimensions, the resource IDs are sorted in ascending alphabetical order and separated by commas (,). **Regex Pattern:** ^([a-z]|[A-Z]|[0-9]|_|-|:|,|\.|)+$
enterprise_project_id	No	String	Enterprise Project ID. **Regex Pattern:** ^((([a-z]|[0-9]){8}-([a-z]|[0-9]){4}-([a-z]|[0-9]){4}-([a-z]|[0-9]){4}-([a-z]|[0-9]){12})|0|all_granted_eps)$
product_name	No	String	Product name. It needs to be specified when alarm rules with multiple dimensions are used. Generally, the value format is *Service namespace,First-level dimension of the service*, for example, **SYS.ECS,instance_id**.

Parameter	Mandatory	Type	Description
resource_level	No	String	If the value of **resource_level** is **product**, cloud product alarm rules with multiple dimensions are used. If the value of **resource_level** is **dimension** or not specified, the original rule type is used. Enumeration values: • **product** • **dimension**
offset	No	Integer	Pagination offset. **Value range:** 0-10000 **Default value:** 0 **Regex Pattern:** ^([0]|[1-9]|[1-9][0-9]|[1-9][0-9][0-9]|[1-9][0-9][0-9][0-9]|10000)$
limit	No	Integer	Number of records on each page. **Value range:** 1-100 **Default value:** 10 **Regex Pattern:** ^([1-9]|[1-9][0-9]|100)$

Request Parameters

Table 6-26 Request header parameters

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	**Definition** MIME type of the request body. **Constraints**: None **Value range**: The value can contain 1 to 64 characters. **Default value**: The default type is **application/json; charset=UTF-8**. **Default value:** application/json; charset=UTF-8
X-Auth-Token	Yes	String	**Definition** User token. **Constraints**: None **Value range**: The value can contain 1 to 16,384 characters. **Default value**: None

Response Parameters

Status code: 200

Table 6-27 Response body parameters

Parameter	Type	Description
alarms	Array of **alarms** objects	Alarm rule list.
count	Integer	Total number of alarm rules. **Value range:** 0-10000

Table 6-28 alarms

Parameter	Type	Description
alarm_id	String	ID of an alarm rule, which starts with **al** and is followed by 22 characters, including letters and digits.
name	String	Name of an alarm rule. The name can contain 1 to 128 characters, including only letters, digits, underscores (_), and hyphens (-).
description	String	Alarm rule description. The description can contain 0 to 256 characters.
namespace	String	Query the namespace of a service. For details about the namespace of each service, see [Service Name] (ces_03_0059.xml).
policies	Array of **Policy** objects	Alarm policies.
resources	Array of **ResourcesInListResp** objects	Resource list. Associated resources can be obtained by calling the API for querying resources in an alarm rule.

Parameter	Type	Description
type	String	**Definition**: Alarm rule type. **Constraints**: None **Value range**: Enumerated value. **ALL_INSTANCE** indicates alarm rules for metrics of all resources. **RESOURCE_GROUP** indicates alarm rules for metrics of resources in a resource group. **MULTI_INSTANCE** indicates alarm rules for metrics of specified resources. **EVENT.SYS** indicates alarm rules for system events. **EVENT.CUSTOM** indicates alarm rules for custom events. **DNSHealthCheck** indicates alarm rules for health checks. **Default value**: None Enumeration values: • **EVENT.SYS** • **EVENT.CUSTOM** • **DNSHealthCheck** • **RESOURCE_GROUP** • **MULTI_INSTANCE** • **ALL_INSTANCE**
enabled	Boolean	Whether to enable the alarm rule. true: enabled; false: disabled.
notification_enabled	Boolean	Whether to enable alarm notification. true: enabled; false: disabled.
alarm_notifications	Array of **Notification** objects	Action to be triggered by the alarm.
ok_notifications	Array of **Notification** objects	Action to be triggered after an alarm is cleared.
notification_begin_time	String	Time when the alarm notification was enabled.
notification_end_time	String	Time when the alarm notification was disabled.

Parameter	Type	Description
effective_timezone	String	Time zone, for example, **GMT-08:00**, **GMT+08:00**, or **GMT+0:00**.
enterprise_project_id	String	Enterprise project ID
alarm_template_id	String	ID of an alarm template associated with an alarm rule. If this parameter is specified, the policy associated with the alarm rule changes accordingly with the alarm template policy.
product_name	String	Product name. It needs to be specified when product alarm rules with multiple dimensions are used. Generally, the value format is *Service namespace,First-level dimension of the service*, for example, **SYS.ECS,instance_id**.
resource_level	String	Product alarm rules with multiple dimensions need to be specified as product-level rules. If the value of **resource_level** is **product**, cloud product alarm rules with multiple dimensions are used. If the value of **resource_level** is **dimension** or not specified, the original rule type is used. Enumeration values: • **product** • **dimension**

Table 6-29 Policy

Parameter	Type	Description
metric_name	String	Metric name of a resource. The name must start with a letter and contain only digits, letters, and underscores. The length ranges from 1 to 64 characters. For example, **cpu_util** of an ECS indicates the CPU usage of the ECS. **mongo001_command_ps** in DDS indicates the command execution frequency. For details about the metric name of each service, see **Service metric name**.

Parameter	Type	Description
period	Integer	Monitoring period of a metric, in seconds. The default value is **0**. For an event alarm, set this parameter to **0**. **1** indicates the original rollup period of a metric. For example, if the original rollup period of an RDS metric is 60s, its data point is calculated every 60 seconds. For details about the original rollup period of each cloud service metric, see **Services Interconnected with Cloud Eye**. **300** indicates that the metric rollup period is 5 minutes. **Value range:** 0-86400 Enumeration values: • **0** • **1** • **300** • **1200** • **3600** • **14400** • **86400**
filter	String	Aggregation mode. average: average value; variance: variance; min: minimum value; max: maximum value; sum: sum; tp99: 99 percentile; tp95: 95 percentile; tp90: 90 percentile
comparison_operator	String	Threshold symbol. The value can be **>**, **<**, **>=**, **<=**, **=**, **!=**, **cycle_decrease**, **cycle_increase**, or **cycle_wave**. **cycle_decrease** indicates the decrease compared with the last period, **cycle_increase** indicates the increase compared with the last period, and **cycle_wave** indicates the increase or decrease compared with the last period. All of them can be used in alarm rules for metrics. **>**, **<**, **>=**, **<=**, **=**, and **!=** can be used for alarm rules for events.

Parameter	Type	Description
value	Number	Alarm threshold If there is only one threshold, **value** and **alarm_level** are used in pairs. If there are both **hierarchical_value** and **value**, **hierarchical_value** is used. For detailed thresholds, see the value range of each metric in the appendix. For example, you can set ECS **cpu_util** to **80**. For detailed thresholds, see the value range of each metric in the appendix. For example, you can set ECS **cpu_util** to **80** in **Services Interconnected with Cloud Eye**.
hierarchical_value	**HierarchicalValue** object	Multi-level alarm threshold. If there are both **hierarchical_value** and **value**, **hierarchical_value** prevails. When you create or modify an alarm rule, you can set only one threshold in the following scenarios: 1. The alarm type is **Metric** and the alarm policy is **Trigger an alarm when all policies are met**. 2. The alarm type is **Event**.
unit	String	Data unit.
count	Integer	Number of consecutive alarm triggering times. For event alarms, the value ranges from **1** to **180**. For metric and website alarms, the value can be **1**, **2**, **3**, **4**, **5**, **10**, **15**, **30**, **60**, **90**, **120**, or **180**.

Parameter	Type	Description
suppress_duration	Integer	Alarm suppression time, in seconds. This parameter corresponds to the last field in the alarm policy when an alarm rule is created on the Cloud Eye console. This field is used to avoid frequent alarms. **0** indicates that the alarm is not suppressed and alarms are generated as long as the conditions are met. **300** indicates that an alarm is generated every 5 minutes as long as the alarm triggering conditions are met. **Value range:** 0-86400 Enumeration values: • **0** • **300** • **600** • **900** • **1800** • **3600** • **10800** • **21600** • **43200** • **86400**
level	Integer	Alarm severity, which can be **1** (critical), ** 2** (major), **3** (minor), or **4** (informational). The default value is **2**.
namespace	String	**namespace** and **dimension_name** need to be specified for product-level rules. For details about the namespace of each service, see **Service namespace**. **Regex Pattern:** ^((([a-z]|[A-Z]){1}([a-z]|[A-Z]|[0-9]|_)*\.([a-z]|[A-Z]){1}([a-z]|[A-Z]|[0-9]|_)*)|)$

Parameter	Type	Description
dimension_name	String	The namespace and dimension_name parameters are added to the product-level rule to specify the policy to which the product belongs. Currently, a maximum of four dimensions are supported. For details about the metric dimension name of each service resource, see [Service dimension name] (ces_03_0059.xml). Example: instance_id in the single-dimension scenario; instance_id,disk in the multi-dimension scenario **Regex Pattern:** ^(([a-z]|[A-Z]){1}([a-z]|[A-Z]|[0-9]|_|-|\.){0,31}(,([a-z]|[A-Z]){1}([a-z]|[A-Z]|[0-9]|_|-|\.){0,31}){0,3}|)$

Table 6-30 HierarchicalValue

Parameter	Type	Description
critical	Double	Threshold for critical alarms. **Value range:** -1.7976931348623156E108-1.7976931348623156E108
major	Double	Threshold for major alarms. **Value range:** -1.7976931348623156E108-1.7976931348623156E108
minor	Double	Threshold for minor alarms. **Value range:** -1.7976931348623156E108-1.7976931348623156E108
info	Double	Threshold for informational alarms. **Value range:** -1.7976931348623156E108-1.7976931348623156E108

Table 6-31 ResourcesInListResp

Parameter	Type	Description
resource_group_id	String	Resource group ID. This parameter is available when the monitoring scope is **Resource groups**. **Regex Pattern:** ^rg([a-z]|[A-Z]|[0-9]){22}$
resource_group_name	String	Resource group name. This parameter is available when the monitoring scope is **Resource groups**.
dimensions	Array of **MetricDimension** objects	Dimension information.

Table 6-32 MetricDimension

Parameter	Type	Description
name	String	Metric dimension name. **Regex Pattern:** ^([a-z]|[A-Z]){1}([a-z]|[A-Z]|[0-9]|_|-){1,32}$
value	String	Metric dimension value. **Regex Pattern:** ^((([a-z]|[A-Z]|[0-9]){1}([a-z]|[A-Z]|[0-9]|_|-)*)|){0,256}$

Table 6-33 Notification

Parameter	Type	Description
type	String	Notification type. The value can be **notification** (SMN notifications), **contact** (account contacts), **contactGroup** (notification groups), or **autoscaling** (AS notifications). **autoscaling** is used only in AS and is not recommended. **groupwatch**, **ecsRecovery**, and **iecAction** are no longer used. Enumeration values: • **notification** • **autoscaling** • **groupwatch** • **ecsRecovery** • **contact** • **contactGroup** • **iecAction**
notification_list	Array of strings	List of objects to be notified if the alarm status changes. The value of **topicUrn** can be obtained from SMN. For details, see section "Querying Topics". If **type** is set to **notification**, the value of **notificationList** cannot be left blank. If **type** is set to **autoscaling**, the value of **notification_list** must be left blank. Note: If **alarm_action_enabled** is set to **true**, **alarm_actions**, **ok_actions**, or both of them must be specified. If both **alarm_actions** and **ok_actions** are specified, their **notification_list** values must be the same.

Status code: 400

Table 6-34 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 500

Table 6-35 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Example Requests

Query alarm rules.

```
/v2/{project_id}/alarms?offset=0&limit=10
```

Example Responses

Status code: 200

Query succeeded.


```
{
  "alarms" : [ {
    "alarm_id" : "al16558829757444BVVxr999",
    "name" : "alarm01",
    "description" : "",
    "namespace" : "SYS.ECS",
    "policies" : [ {
      "metric_name" : "disk_device_read_bytes_rate",
      "period" : 1,
      "filter" : "average",
      "comparison_operator" : ">",
      "value" : 75,
      "unit" : "byte/s",
      "count" : 3,
      "suppress_duration" : 10800,
      "level" : 2
    } ],
    "resources" : [ {
      "dimensions" : [ {
        "name" : "disk_name"
      } ]
    } ],
    "type" : "ALL_INSTANCE",
    "enabled" : true,
    "notification_enabled" : true,
    "alarm_notifications" : [ {
      "type" : "notification",
      "notification_list" : [ "urn:smn:xxx:xxx70e7359:topic_xxx" ]
    } ],
    "ok_notifications" : [ {
      "type" : "notification",
      "notification_list" : [ "urn:smn:xxx:xxx70e7359:topic_xxx" ]
    } ],
    "notification_begin_time" : "00:00",
```

```
    "notification_end_time" : "23:59",
    "enterprise_project_id" : "0"
  } ],
  "count" : 1
}
```

Status Codes

Status Code	Description
200	Query succeeded.
400	Parameter verification failed.
500	Internal system error.

Error Codes

See **Error Codes**.

6.2 Alarm Resources

6.2.1 Batch Adding Resources to an Alarm Rule

Function

This API is used to batch add resources to an alarm rule. This API does not support alarm rules whose **AlarmType** is **RESOURCE_GROUP**. To modify resources in such alarm rules, use the resource group management APIs.

Debugging

You can debug this API through automatic authentication in **API Explorer** or use the SDK sample code generated by API Explorer.

URI

POST /v2/{project_id}/alarms/{alarm_id}/resources/batch-create

Table 6-36 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	**Definition** Tenant ID. **Constraints**: None **Value range**: Project ID, used to specify the project that an asset belongs to. You can query the assets of a project by project ID. You can obtain the project ID by calling an API or on the console. For details, see **Obtaining a Project ID**. The value must contain of 1 to 64 characters. **Default value**: None
alarm_id	Yes	String	Alarm rule ID. **Regex Pattern:** al([a-z]|[A-Z]|[0-9]){22}$

Request Parameters

Table 6-37 Request header parameters

Parameter	Mandatory	Type	Description
Content-Type	No	String	**Definition** MIME type of the request body. **Constraints**: None **Value range**: The value can contain 1 to 64 characters. **Default value**: The default type is **application/json; charset=UTF-8**. **Default value:** application/json; charset=UTF-8
X-Auth-Token	No	String	**Definition** User token. **Constraints**: None **Value range**: The value can contain 1 to 16,384 characters. **Default value**: None

Table 6-38 Request body parameters

Parameter	Mandatory	Type	Description
resources	Yes	Array<Array< **Dimension**>>	Resource information.

Table 6-39 Dimension

Parameter	Mandatory	Type	Description
name	Yes	String	Dimension of a resource. For example, the dimension of an ECS can be **instance_id**. A maximum of four dimensions are supported. For the metric dimension of each resource, see **Service metric dimension**. **Regex Pattern:** ^([a-z]|[A-Z]){1}([a-z]|[A-Z]|[0-9]|_|-)*$
value	No	String	Value of a resource dimension, which is the resource ID, for example, **4270ff17-aba3-4138-89fa-820594c39755**. **Regex Pattern:** ^((([a-z]|[A-Z]|[0-9]|*|_|/|#|\(|\)){1}([a-z]|[A-Z]|[0-9]|_|-|\.|*|/|#|\(|\))*))$

Response Parameters

Status code: 200

Resources added.

Status code: 400

Table 6-40 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 404

Table 6-41 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 500

Table 6-42 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Example Requests

Batch adding resources to an alarm rule.

```
{
  "resources" : [ [ {
    "name" : "rds_cluster_id",
    "value" : "rds000000000001"
  } ] ]
}
```

Example Responses

None

Status Codes

Status Code	Description
200	Resources added.
400	Parameter verification failed.
404	Resource not found.
500	Internal system error.

Error Codes

See **Error Codes**.

6.2.2 Batch Deleting Resources from an Alarm Rule

Function

This API is used to batch delete resources from an alarm rule. This API does not support alarm rules whose **AlarmType** is **RESOURCE_GROUP**. To modify resources in such alarm rules, use the resource group management APIs.

Debugging

You can debug this API through automatic authentication in **API Explorer** or use the SDK sample code generated by API Explorer.

URI

POST /v2/{project_id}/alarms/{alarm_id}/resources/batch-delete

Table 6-43 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	**Definition** Tenant ID. **Constraints**: None **Value range**: Project ID, used to specify the project that an asset belongs to. You can query the assets of a project by project ID. You can obtain the project ID by calling an API or on the console. For details, see **Obtaining a Project ID**. The value must contain of 1 to 64 characters. **Default value**: None
alarm_id	Yes	String	Alarm rule ID. **Regex Pattern:** al([a-z]|[A-Z]|[0-9]){22}$

Request Parameters

Table 6-44 Request header parameters

Parameter	Mandatory	Type	Description
Content-Type	No	String	**Definition** MIME type of the request body. **Constraints**: None **Value range**: The value can contain 1 to 64 characters. **Default value**: The default type is **application/json; charset=UTF-8**. **Default value:** application/json; charset=UTF-8
X-Auth-Token	No	String	**Definition** User token. **Constraints**: None **Value range**: The value can contain 1 to 16,384 characters. **Default value**: None

Table 6-45 Request body parameters

Parameter	Mandatory	Type	Description
resources	Yes	Array<Array< **Dimension**>>	Resource information.

Table 6-46 Dimension

Parameter	Mandatory	Type	Description
name	Yes	String	Dimension of a resource. For example, the dimension of an ECS can be **instance_id**. A maximum of four dimensions are supported. For the metric dimension of each resource, see **Service metric dimension**. **Regex Pattern:** ^([a-z]|[A-Z]){1}([a-z]|[A-Z]|[0-9]|_|-)*$
value	No	String	Value of a resource dimension, which is the resource ID, for example, **4270ff17-aba3-4138-89fa-820594c39755**. **Regex Pattern:** ^((([a-z]|[A-Z]|[0-9]|*|_|/|#|\(|\)){1}([a-z]|[A-Z]|[0-9]|_|-|\.|*|/|#|\(|\))*))$

Response Parameters

Status code: 200

Resources deleted.

Status code: 400

Table 6-47 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 404

Table 6-48 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 500

Table 6-49 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Example Requests

Deleting resources monitored by an alarm rule.

```
{
  "resources" : [ [ {
    "name" : "rds_cluster_id",
    "value" : "rds000000000001"
  } ] ]
}
```

Example Responses

None

Status Codes

Status Code	Description
200	Resources deleted.
400	Parameter verification failed.
404	Resource not found.
500	Internal system error.

Error Codes

See **Error Codes**.

6.2.3 Querying Resources in an Alarm Rule

Function

This API is used to query resources in an alarm rule by alarm rule ID.

Debugging

You can debug this API through automatic authentication in **API Explorer** or use the SDK sample code generated by API Explorer.

URI

GET /v2/{project_id}/alarms/{alarm_id}/resources

Table 6-50 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	**Definition** Tenant ID. **Constraints**: None **Value range**: Project ID, used to specify the project that an asset belongs to. You can query the assets of a project by project ID. You can obtain the project ID by calling an API or on the console. For details, see **Obtaining a Project ID**. The value must contain of 1 to 64 characters. **Default value**: None
alarm_id	Yes	String	Alarm rule ID. **Regex Pattern:** al([a-z]|[A-Z]|[0-9]){22}$

Table 6-51 Query Parameters

Parameter	Mandatory	Type	Description
offset	No	Integer	Pagination offset. **Value range:** 0-10000 **Default value:** 0 **Regex Pattern:** ^([0]|[1-9]|[1-9][0-9]|[1-9][0-9][0-9]|[1-9][0-9][0-9][0-9]|10000)$
limit	No	Integer	Number of records on each page. **Value range:** 1-100 **Default value:** 10 **Regex Pattern:** ^([1-9]|[1-9][0-9]|100)$

Request Parameters

Table 6-52 Request header parameters

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	**Definition** MIME type of the request body. **Constraints**: None **Value range**: The value can contain 1 to 64 characters. **Default value**: The default type is **application/json; charset=UTF-8**. **Default value:** application/json; charset=UTF-8

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	**Definition** User token. **Constraints**: None **Value range**: The value can contain 1 to 16,384 characters. **Default value**: None

Response Parameters

Status code: 200

Table 6-53 Response body parameters

Parameter	Type	Description
resources	Array<Array<**Dimension**>>	Resource information.
count	Integer	Total number of resources. **Value range:** 0-2147483647

Table 6-54 Dimension

Parameter	Type	Description
name	String	Dimension of a resource. For example, the dimension of an ECS can be **instance_id**. A maximum of four dimensions are supported. For the metric dimension of each resource, see **Service metric dimension**. **Regex Pattern:** ^([a-z]|[A-Z]){1}([a-z]|[A-Z]|[0-9]|_|-)*$

Parameter	Type	Description
value	String	Value of a resource dimension, which is the resource ID, for example, **4270ff17-aba3-4138-89fa-820594c39755**. **Regex Pattern:** ^((([a-z]|[A-Z]|[0-9]|*|_|/|#|\(|\)){1}([a-z]|[A-Z]|[0-9]|_|-|\.|*|/|#|\(|\))*))$

Status code: 400

Table 6-55 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 500

Table 6-56 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Example Requests

Querying resources monitored by an alarm rule whose **alarm_id** is **alCzk8o9dtSQHtiDgb44Eepw** and **limit** is **10**.

```
/v2/{project_id}/alarms/alCzk8o9dtSQHtiDgb44Eepw/resources?offset=0&limit=10
```

Example Responses

Status code: 200

Query succeeded.

```
{
  "resources" : [ [ {
```

```
    "name" : "disk_name"
  } ] ],
  "count" : 10
}
```

Status Codes

Status Code	Description
200	Query succeeded.
400	Parameter verification failed.
500	Internal system error.

Error Codes

See **Error Codes**.

6.3 Alarm Policies

6.3.1 Modifying All Fields in an Alarm Policy

Function

This API is used to modify all fields in an alarm rule.

Debugging

You can debug this API through automatic authentication in **API Explorer** or use the SDK sample code generated by API Explorer.

URI

PUT /v2/{project_id}/alarms/{alarm_id}/policies

Table 6-57 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	**Definition** Tenant ID. **Constraints**: None **Value range**: Project ID, used to specify the project that an asset belongs to. You can query the assets of a project by project ID. You can obtain the project ID by calling an API or on the console. For details, see **Obtaining a Project ID**. The value must contain of 1 to 64 characters. **Default value**: None
alarm_id	Yes	String	Alarm rule ID. **Regex Pattern:** ^al([0-9A-Za-z]){22}$

Request Parameters

Table 6-58 Request header parameters

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	**Definition** MIME type of the request body. **Constraints**: None **Value range**: The value can contain 1 to 64 characters. **Default value**: The default type is **application/json; charset=UTF-8**. **Default value:** application/json; charset=UTF-8
X-Auth-Token	Yes	String	**Definition** User token. **Constraints**: None **Value range**: The value can contain 1 to 16,384 characters. **Default value**: None

Table 6-59 Request body parameters

Parameter	Mandatory	Type	Description
policies	Yes	Array of **UpdatePolicyReq** objects	Policy information.

Table 6-60 UpdatePolicyReq

Parameter	Mandatory	Type	Description
metric_name	Yes	String	Metric name of a resource. The name must start with a letter and contain only digits, letters, and underscores. The length ranges from 1 to 64 characters. For example, **cpu_util** of an ECS indicates the CPU usage of the ECS. **mongo001_command_ps** in DDS indicates the command execution frequency. For details about the metric name of each service, see **Service metric name**.
extra_info	No	**MetricExtraInfo** object	If the policy does not contain additional information, extra_info does not need to be transferred.
period	Yes	Integer	Monitoring period of a metric, in seconds. The default value is **0**. For an event alarm, set this parameter to **0**. **1** indicates the original rollup period of a metric. For example, if the original rollup period of an RDS metric is 60s, its data point is calculated every 60 seconds. For details about the original rollup period of each cloud service metric, see **Services Interconnected with Cloud Eye**. **300** indicates that the metric rollup period is 5 minutes. **Value range:** 0-86400 Enumeration values: • **0** • **1** • **300** • **1200** • **3600** • **14400** • **86400**

Parameter	Mandatory	Type	Description
filter	Yes	String	Aggregation mode. average: average value; variance: variance; min: minimum value; max: maximum value; sum: sum; tp99: 99 percentile; tp95: 95 percentile; tp90: 90 percentile
comparison_operator	Yes	String	Threshold symbol. The value can be >, <, >=, <=, =, **!=**, **cycle_decrease**, **cycle_increase**, or **cycle_wave**. **cycle_decrease** indicates the decrease compared with the last period, **cycle_increase** indicates the increase compared with the last period, and **cycle_wave** indicates the increase or decrease compared with the last period. All of them can be used in alarm rules for metrics. >, <, >=, <=, =, and **!=** can be used for alarm rules for events.
value	No	Number	Alarm threshold If there is only one threshold, **value** and **alarm_level** are used in pairs. If there are both **hierarchical_value** and **value**, **hierarchical_value** is used. For detailed thresholds, see the value range of each metric in the appendix. For example, you can set ECS **cpu_util** to **80**. For detailed thresholds, see the value range of each metric in the appendix. For example, you can set ECS **cpu_util** to **80** in **Services Interconnected with Cloud Eye**.

Parameter	Mandatory	Type	Description
hierarchical_value	No	**HierarchicalValue** object	Multi-level alarm threshold. If there are both **hierarchical_value** and **value**, **hierarchical_value** prevails. When you create or modify an alarm rule, you can set only one threshold in the following scenarios: 1. The alarm type is **Metric** and the alarm policy is **Trigger an alarm when all policies are met**. 2. The alarm type is **Event**.
unit	No	String	Data unit.
type	No	String	Alarm policy type. This API has been deprecated. **Regex Pattern:** ^(auto)$
count	Yes	Integer	Number of consecutive alarm triggering times. For event alarms, the value ranges from **1** to **180**. For metric and website alarms, the value can be **1**, **2**, **3**, **4**, **5**, **10**, **15**, **30**, **60**, **90**, **120**, or **180**.

Parameter	Mandatory	Type	Description
suppress_duration	No	Integer	Alarm suppression time, in seconds. This parameter corresponds to the last field in the alarm policy when an alarm rule is created on the Cloud Eye console. This field is used to avoid frequent alarms. **0** indicates that the alarm is not suppressed and alarms are generated as long as the conditions are met. **300** indicates that an alarm is generated every 5 minutes as long as the alarm triggering conditions are met. **Value range:** 0-86400 Enumeration values: • **0** • **300** • **600** • **900** • **1800** • **3600** • **10800** • **21600** • **43200** • **86400**
level	No	Integer	Alarm severity, which can be **1** (critical), ** 2** (major), **3** (minor), or **4** (informational). The default value is **2**.
namespace	No	String	The namespace and dimension_name parameters are added to the product-level rule to specify the policy to which the product belongs. For details about the namespace of each service, see [Service Namespace](ces_03_0059.xml). **Regex Pattern:** ^((([a-z]|[A-Z]){1}([a-z]|[A-Z]|[0-9]|_)*\.([a-z]|[A-Z]){1}([a-z]|[A-Z]|[0-9]|_)*)|)$

Parameter	Mandatory	Type	Description
dimension_name	No	String	The namespace and dimension_name parameters are added to the product-level rule to specify the policy to which the product belongs. Currently, a maximum of four dimensions are supported. For details about the metric dimension name of each service resource, see [Service dimension name](ces_03_0059.xml). Example: instance_id in the single-dimension scenario; instance_id,disk in the multi-dimension scenario **Regex Pattern:** ^(([a-z]|[A-Z]){1}([a-z]|[A-Z]|[0-9]|_|-|\.){0,31}(,([a-z]|[A-Z]){1}([a-z]|[A-Z]|[0-9]|_|-|\.){0,31}){0,3}|)$

Table 6-61 MetricExtraInfo

Parameter	Mandatory	Type	Description
origin_metric_name	Yes	String	Original metric name. **Regex Pattern:** ^([a-z]|[A-Z]|[0-9]|_|-|~|\.|/|:)*$
metric_prefix	No	String	Metric name prefix. **Regex Pattern:** ^([a-z]|[A-Z]|[0-9]|_|-|~|\.|/|:)*$
custom_proc_name	No	String	Name of a user process.
metric_type	No	String	Metric type. **Regex Pattern:** ^([a-z]|[A-Z]|[0-9]|_|-|~|\.|/|:)*$

Table 6-62 HierarchicalValue

Parameter	Mandatory	Type	Description
critical	No	Double	Threshold for critical alarms. **Value range:** -1.7976931348623156E108-1.7976931348623156E108
major	No	Double	Threshold for major alarms. **Value range:** -1.7976931348623156E108-1.7976931348623156E108
minor	No	Double	Threshold for minor alarms. **Value range:** -1.7976931348623156E108-1.7976931348623156E108
info	No	Double	Threshold for informational alarms. **Value range:** -1.7976931348623156E108-1.7976931348623156E108

Response Parameters

Status code: 200

Table 6-63 Response body parameters

Parameter	Type	Description
policies	Array of **UpdatePolicyResp** objects	Policy information.

Table 6-64 UpdatePolicyResp

Parameter	Type	Description
metric_name	String	Metric name of a resource. The name must start with a letter and contain only digits, letters, and underscores. The length ranges from 1 to 64 characters. For example, **cpu_util** of an ECS indicates the CPU usage of the ECS. **mongo001_command_ps** in DDS indicates the command execution frequency. For details about the metric name of each service, see **Service metric name**.
extra_info	**MetricExtraInfoResp** object	If the policy does not contain additional information, extra_info does not need to be transferred.
period	Integer	Monitoring period of a metric, in seconds. The default value is **0**. For an event alarm, set this parameter to **0**. **1** indicates the original rollup period of a metric. For example, if the original rollup period of an RDS metric is 60s, its data point is calculated every 60 seconds. For details about the original rollup period of each cloud service metric, see **Services Interconnected with Cloud Eye**. **300** indicates that the metric rollup period is 5 minutes. **Value range:** 0-86400 Enumeration values: • **0** • **1** • **300** • **1200** • **3600** • **14400** • **86400**
filter	String	Aggregation mode. average: average value; variance: variance; min: minimum value; max: maximum value; sum: sum; tp99: 99 percentile; tp95: 95 percentile; tp90: 90 percentile

Parameter	Type	Description
comparison_operator	String	Threshold symbol. The value can be **>**, **<**, **>=**, **<=**, **=**, **!=**, **cycle_decrease**, **cycle_increase**, or **cycle_wave**. **cycle_decrease** indicates the decrease compared with the last period, **cycle_increase** indicates the increase compared with the last period, and **cycle_wave** indicates the increase or decrease compared with the last period. All of them can be used in alarm rules for metrics. **>**, **<**, **>=**, **<=**, **=**, and **!=** can be used for alarm rules for events.
value	Number	Alarm threshold If there is only one threshold, **value** and **alarm_level** are used in pairs. If there are both **hierarchical_value** and **value**, **hierarchical_value** is used. For detailed thresholds, see the value range of each metric in the appendix. For example, you can set ECS **cpu_util** to **80**. For detailed thresholds, see the value range of each metric in the appendix. For example, you can set ECS **cpu_util** to **80** in **Services Interconnected with Cloud Eye**.
hierarchical_value	**HierarchicalValueResp** object	Multi-level alarm threshold. If there are both **hierarchical_value** and **value**, **hierarchical_value** prevails. When you create or modify an alarm rule, you can set only one threshold in the following scenarios: 1. The alarm type is **Metric** and the alarm policy is **Trigger an alarm when all policies are met**. 2. The alarm type is **Event**.
unit	String	Data unit.
type	String	Alarm policy type. This API has been deprecated. **Regex Pattern:** ^(auto)$
count	Integer	Number of consecutive alarm triggering times. For event alarms, the value ranges from **1** to **180**. For metric and website alarms, the value can be **1**, **2**, **3**, **4**, **5**, **10**, **15**, **30**, **60**, **90**, **120**, or **180**.

Parameter	Type	Description
suppress_duration	Integer	Alarm suppression time, in seconds. This parameter corresponds to the last field in the alarm policy when an alarm rule is created on the Cloud Eye console. This field is used to avoid frequent alarms. **0** indicates that the alarm is not suppressed and alarms are generated as long as the conditions are met. **300** indicates that an alarm is generated every 5 minutes as long as the alarm triggering conditions are met. **Value range:** 0-86400 Enumeration values: • **0** • **300** • **600** • **900** • **1800** • **3600** • **10800** • **21600** • **43200** • **86400**
level	Integer	Alarm severity, which can be **1** (critical), ** 2** (major), **3** (minor), or **4** (informational). The default value is **2**.
namespace	String	The namespace and dimension_name parameters are added to the product-level rule to specify the policy to which the product belongs. For details about the namespace of each service,see **Services Interconnected with Cloud Eye**. **Regex Pattern:** ^((([a-z]|[A-Z]){1}([a-z]|[A-Z]|[0-9]|_)*\.([a-z]|[A-Z]){1}([a-z]|[A-Z]|[0-9]|_)*)|)$

Parameter	Type	Description
dimension_name	String	The namespace and dimension_name parameters are added to the product-level rule to specify the policy to which the product belongs. Currently, a maximum of four dimensions are supported. For details about the metric dimension name of each service resource, see **Services Interconnected with Cloud Eye**. Example: instance_id in the single-dimension scenario; instance_id,disk in the multi-dimension scenario **Regex Pattern:** ^(([a-z]|[A-Z]){1}([a-z]|[A-Z]|[0-9]|_|-|\.){0,31}(,([a-z]|[A-Z]){1}([a-z]|[A-Z]|[0-9]|_|-|\.){0,31}){0,3}|)$

Table 6-65 MetricExtraInfoResp

Parameter	Type	Description
origin_metric_name	String	Original metric name. **Regex Pattern:** ^([a-z]|[A-Z]|[0-9]|_|-|~|\.|/|:)*$
metric_prefix	String	Metric name prefix. **Regex Pattern:** ^([a-z]|[A-Z]|[0-9]|_|-|~|\.|/|:)*$
custom_proc_name	String	Name of a user process.
metric_type	String	Metric type. **Regex Pattern:** ^([a-z]|[A-Z]|[0-9]|_|-|~|\.|/|:)*$

Table 6-66 HierarchicalValueResp

Parameter	Type	Description
critical	Double	Threshold for critical alarms. **Value range:** -1.7976931348623156E108-1.7976931348623156E108

Parameter	Type	Description
major	Double	Threshold for major alarms. **Value range:** -1.7976931348623156E108-1.7976931348623156E108
minor	Double	Threshold for minor alarms. **Value range:** -1.7976931348623156E108-1.7976931348623156E108
info	Double	Threshold for informational alarms. **Value range:** -1.7976931348623156E108-1.7976931348623156E108

Status code: 400

Table 6-67 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 500

Table 6-68 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Example Requests

Modify an alarm policy whose **metric name** is **disk_device_read_bytes_rate**.

```
{
  "policies" : [ {
```

```
    "metric_name" : "disk_device_read_bytes_rate",
    "period" : 1,
    "filter" : "average",
    "comparison_operator" : ">",
    "value" : 75,
    "unit" : "byte/s",
    "count" : 3,
    "suppress_duration" : 10800,
    "level" : 2
  } ]
}
```

Example Responses

Status code: 200

Modification succeeded.

```
{
  "policies" : [ {
    "metric_name" : "disk_device_read_bytes_rate",
    "period" : 1,
    "filter" : "average",
    "comparison_operator" : ">",
    "value" : 75,
    "unit" : "byte/s",
    "count" : 3,
    "type" : "",
    "suppress_duration" : 10800,
    "level" : 2
  } ]
}
```

Status Codes

Status Code	Description
200	Modification succeeded.
400	Parameter verification failed.
500	Internal system error.

Error Codes

See **Error Codes**.

6.3.2 Querying Alarm Policies

Function

This API is used to query alarm policies by alarm rule ID.

Debugging

You can debug this API through automatic authentication in **API Explorer** or use the SDK sample code generated by API Explorer.

URI

GET /v2/{project_id}/alarms/{alarm_id}/policies

Table 6-69 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	**Definition** Tenant ID. **Constraints**: None **Value range**: Project ID, used to specify the project that an asset belongs to. You can query the assets of a project by project ID. You can obtain the project ID by calling an API or on the console. For details, see **Obtaining a Project ID**. The value must contain of 1 to 64 characters. **Default value**: None
alarm_id	Yes	String	Alarm rule ID. **Regex Pattern:** ^al([0-9A-Za-z]){22}$

Table 6-70 Query Parameters

Parameter	Mandatory	Type	Description
offset	No	Integer	Pagination offset. **Value range:** 0-10000 **Default value:** 0 **Regex Pattern:** ^([0]|[1-9]|[1-9][0-9]|[1-9][0-9][0-9]|[1-9][0-9][0-9][0-9]|10000)$

Parameter	Mandatory	Type	Description
limit	No	Integer	Number of records on each page. **Value range:** 1-100 **Default value:** 10 **Regex Pattern:** ^([1-9]|[1-9][0-9]|100)$

Request Parameters

Table 6-71 Request header parameters

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	**Definition** MIME type of the request body. **Constraints**: None **Value range**: The value can contain 1 to 64 characters. **Default value**: The default type is **application/json; charset=UTF-8**. **Default value:** application/json; charset=UTF-8
X-Auth-Token	Yes	String	**Definition** User token. **Constraints**: None **Value range**: The value can contain 1 to 16,384 characters. **Default value**: None

Response Parameters

Status code: 200

Table 6-72 Response body parameters

Parameter	Type	Description
policies	Array of **ListPolicy** objects	Policy information.
count	Integer	Total number of policies in an alarm rule. **Value range:** 0-100

Table 6-73 ListPolicy

Parameter	Type	Description
metric_name	String	Metric name of a resource. The name must start with a letter and contain only digits, letters, and underscores. The length ranges from 1 to 64 characters. For example, **cpu_util** of an ECS indicates the CPU usage of the ECS. **mongo001_command_ps** in DDS indicates the command execution frequency. For details about the metric name of each service, see **Service metric name**.
extra_info	**MetricExtraInfo** object	If the policy does not contain additional information, extra_info does not need to be transferred.

Parameter	Type	Description
period	Integer	Monitoring period of a metric, in seconds. The default value is **0**. For an event alarm, set this parameter to **0**. **1** indicates the original rollup period of a metric. For example, if the original rollup period of an RDS metric is 60s, its data point is calculated every 60 seconds. For details about the original rollup period of each cloud service metric, see **Services Interconnected with Cloud Eye**. **300** indicates that the metric rollup period is 5 minutes. **Value range:** 0-86400 Enumeration values: • **0** • **1** • **300** • **1200** • **3600** • **14400** • **86400**
filter	String	Aggregation mode. average: average value; variance: variance; min: minimum value; max: maximum value; sum: sum; tp99: 99 percentile; tp95: 95 percentile; tp90: 90 percentile
comparison_operator	String	Threshold symbol. The value can be **>**, **<**, **>=**, **<=**, **=**, **!=**, **cycle_decrease**, **cycle_increase**, or **cycle_wave**. **cycle_decrease** indicates the decrease compared with the last period, **cycle_increase** indicates the increase compared with the last period, and **cycle_wave** indicates the increase or decrease compared with the last period. All of them can be used in alarm rules for metrics. **>**, **<**, **>=**, **<=**, **=**, and **!=** can be used for alarm rules for events.

Parameter	Type	Description
value	Number	Alarm threshold If there is only one threshold, **value** and **alarm_level** are used in pairs. If there are both **hierarchical_value** and **value**, **hierarchical_value** is used. For detailed thresholds, see the value range of each metric in the appendix. For example, you can set ECS **cpu_util** to **80**. For detailed thresholds, see the value range of each metric in the appendix. For example, you can set ECS **cpu_util** to **80** in **Services Interconnected with Cloud Eye**.
hierarchical_value	**HierarchicalValue** object	Multi-level alarm threshold. If there are both **hierarchical_value** and **value**, **hierarchical_value** prevails. When you create or modify an alarm rule, you can set only one threshold in the following scenarios: 1. The alarm type is **Metric** and the alarm policy is **Trigger an alarm when all policies are met**. 2. The alarm type is **Event**.
unit	String	Data unit.
type	String	Alarm policy type. This API has been deprecated.
count	Integer	Number of consecutive alarm triggering times. For event alarms, the value ranges from **1** to **180**. For metric and website alarms, the value can be **1**, **2**, **3**, **4**, **5**, **10**, **15**, **30**, **60**, **90**, **120**, or **180**.

Parameter	Type	Description
suppress_duration	Integer	Alarm suppression time, in seconds. This parameter corresponds to the last field in the alarm policy when an alarm rule is created on the Cloud Eye console. This field is used to avoid frequent alarms. **0** indicates that the alarm is not suppressed and alarms are generated as long as the conditions are met. **300** indicates that an alarm is generated every 5 minutes as long as the alarm triggering conditions are met. **Value range:** 0-86400 Enumeration values: • **0** • **300** • **600** • **900** • **1800** • **3600** • **10800** • **21600** • **43200** • **86400**
level	Integer	Alarm severity, which can be **1** (critical), ** 2** (major), **3** (minor), or **4** (informational). The default value is **2**.
namespace	String	The values of **namespace** (service namespace) and **dimension_name** (service dimension name) need to be returned when product-level rules are used. For details about the namespace of each service, see **Service namespace**.
dimension_name	String	The values of **namespace** (service namespace) and **dimension_name** (service dimension name) need to be returned when product-level rules are used. Currently, a maximum of four dimensions are supported. For details about the metric dimension name of each service resource, see **Service dimension name**.

Table 6-74 MetricExtraInfo

Parameter	Type	Description
origin_metric_name	String	Original metric name. **Regex Pattern:** ^([a-z]|[A-Z]|[0-9]|_|-|~|\.|/|:)*$
metric_prefix	String	Metric name prefix. **Regex Pattern:** ^([a-z]|[A-Z]|[0-9]|_|-|~|\.|/|:)*$
custom_proc_name	String	Name of a user process.
metric_type	String	Metric type. **Regex Pattern:** ^([a-z]|[A-Z]|[0-9]|_|-|~|\.|/|:)*$

Table 6-75 HierarchicalValue

Parameter	Type	Description
critical	Double	Threshold for critical alarms. **Value range:** -1.7976931348623156E108-1.7976931348623156E108
major	Double	Threshold for major alarms. **Value range:** -1.7976931348623156E108-1.7976931348623156E108
minor	Double	Threshold for minor alarms. **Value range:** -1.7976931348623156E108-1.7976931348623156E108
info	Double	Threshold for informational alarms. **Value range:** -1.7976931348623156E108-1.7976931348623156E108

Status code: 400

Table 6-76 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 404

Table 6-77 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 500

Table 6-78 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Example Requests

Query an alarm policy whose **alarm_id** is **alCzk8o9dtSQHtiDgb44Eepw** and **limit** is **10**.

```
/v2/{project_id}/alarms/alCzk8o9dtSQHtiDgb44Eepw/policies?offset=0&limit=10
```

Example Responses

Status code: 200

Query succeeded.

```
{
  "policies" : [ {
```

```
  "namespace" : "AGT.ECS",
  "metric_name" : "disk_device_read_bytes_rate",
  "extra_info" : { },
  "period" : 1,
  "filter" : "average",
  "comparison_operator" : ">",
  "value" : 75,
  "hierarchical_value" : {
    "critical" : 1
  },
  "unit" : "byte/s",
  "count" : 3,
  "type" : "",
  "suppress_duration" : 10800,
  "level" : 2
 } ],
 "count" : 10
}
```


Status Codes

Status Code	Description
200	Query succeeded.
400	Parameter verification failed.
404	Alarm rule not found.
500	Internal system error.

Error Codes

See **Error Codes**.

6.4 Alert Notifications

6.4.1 Modifying Alarm Notification Information in an Alarm Rule

Function

This API is used to modify alarm notification information in an alarm rule.

Debugging

You can debug this API through automatic authentication in **API Explorer** or use the SDK sample code generated by API Explorer.

URI

PUT /v2/{project_id}/alarms/{alarm_id}/notifications

Table 6-79 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	**Definition** Tenant ID. **Constraints**: None **Value range**: Project ID, used to specify the project that an asset belongs to. You can query the assets of a project by project ID. You can obtain the project ID by calling an API or on the console. For details, see **Obtaining a Project ID**. The value must contain of 1 to 64 characters. **Default value**: None
alarm_id	Yes	String	Alarm rule ID. **Regex Pattern:** ^al([0-9A-Za-z]){22}$

Request Parameters

Table 6-80 Request header parameters

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	**Definition** MIME type of the request body. **Constraints**: None **Value range**: The value can contain 1 to 64 characters. **Default value**: The default type is **application/json; charset=UTF-8**. **Default value:** application/json; charset=UTF-8
X-Auth-Token	Yes	String	**Definition** User token. **Constraints**: None **Value range**: The value can contain 1 to 16,384 characters. **Default value**: None

Table 6-81 Request body parameters

Parameter	Mandatory	Type	Description
notification_enabled	Yes	Boolean	Whether to enable alarm notifications. If the value is **true**, other fields are mandatory. If the value is **false**, other fields are optional.
alarm_notifications	No	Array of **Notification** objects	Action to be triggered by the alarm.

Parameter	Mandatory	Type	Description
ok_notifications	No	Array of **Notification** objects	Action to be triggered after an alarm is cleared.
notification_begin_time	No	String	Time when the alarm notification was enabled.
notification_end_time	No	String	Time when the alarm notification was disabled.
effective_timezone	No	String	Time zone, for example, **GMT-08:00**, **GMT+08:00**, or **GMT+0:00**.

Table 6-82 Notification

Parameter	Mandatory	Type	Description
type	Yes	String	Notification type. The value can be **notification** (SMN notifications), **contact** (account contacts), **contactGroup** (notification groups), or **autoscaling** (AS notifications). **autoscaling** is used only in AS and is not recommended. **groupwatch**, **ecsRecovery**, and **iecAction** are no longer used. Enumeration values: • **notification** • **autoscaling** • **groupwatch** • **ecsRecovery** • **contact** • **contactGroup** • **iecAction**

Parameter	Mandatory	Type	Description
notification_list	Yes	Array of strings	List of objects to be notified if the alarm status changes. The value of **topicUrn** can be obtained from SMN. For details, see section "Querying Topics". If **type** is set to **notification**, the value of **notificationList** cannot be left blank. If **type** is set to **autoscaling**, the value of **notification_list** must be left blank. Note: If **alarm_action_enabled** is set to **true**, **alarm_actions**, **ok_actions**, or both of them must be specified. If both **alarm_actions** and **ok_actions** are specified, their **notification_list** values must be the same.

Response Parameters

Status code: 200

Table 6-83 Response body parameters

Parameter	Type	Description
notification_enabled	Boolean	Whether to enable alarm notifications.
alarm_notifications	Array of **Notification** objects	Action to be triggered by the alarm.
ok_notifications	Array of **Notification** objects	Action to be triggered after an alarm is cleared.
notification_begin_time	String	Time when the alarm notification was enabled.
notification_end_time	String	Time when the alarm notification was disabled.

Table 6-84 Notification

Parameter	Type	Description
type	String	Notification type. The value can be **notification** (SMN notifications), **contact** (account contacts), **contactGroup** (notification groups), or **autoscaling** (AS notifications). **autoscaling** is used only in AS and is not recommended. **groupwatch**, **ecsRecovery**, and **iecAction** are no longer used. Enumeration values: • **notification** • **autoscaling** • **groupwatch** • **ecsRecovery** • **contact** • **contactGroup** • **iecAction**
notification_list	Array of strings	List of objects to be notified if the alarm status changes. The value of **topicUrn** can be obtained from SMN. For details, see section "Querying Topics". If **type** is set to **notification**, the value of **notificationList** cannot be left blank. If **type** is set to **autoscaling**, the value of **notification_list** must be left blank. Note: If **alarm_action_enabled** is set to **true**, **alarm_actions**, **ok_actions**, or both of them must be specified. If both **alarm_actions** and **ok_actions** are specified, their **notification_list** values must be the same.

Status code: 400

Table 6-85 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 500

Table 6-86 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Example Requests

Modifying alarm notification information in an alarm rule.

```
{
  "notification_enabled" : true,
  "alarm_notifications" : [ {
    "type" : "notification",
    "notification_list" : [ "urn:smn:cn-north-7:65c438cab60xxxxxxx:CES_notification_group_MGj4AJ03X" ]
  } ],
  "ok_notifications" : [ {
    "type" : "notification",
    "notification_list" : [ "urn:smn:cn-north-7:65c438cab60xxxxxxx:CES_notification_group_MGj4AJ03X" ]
  } ],
  "notification_begin_time" : "00:00",
  "notification_end_time" : "23:59"
}
```

Example Responses

Status code: 200

Alarm notification information modified.

```
{
  "notification_enabled" : true,
  "alarm_notifications" : [ {
    "type" : "",
    "notification_list" : [ ]
  } ],
  "ok_notifications" : [ {
    "type" : "",
    "notification_list" : [ ]
  } ],
  "notification_begin_time" : "00:00",
  "notification_end_time" : "23:59"
}
```


Status Codes

Status Code	Description
200	Alarm notification information modified.
400	Parameter verification failed.
500	Internal system error.

Error Codes

See **Error Codes**.

6.5 Alarm Records

6.5.1 This API is used to query alarm records.

Function

This API is used to query alarm records.

Debugging

You can debug this API through automatic authentication in **API Explorer** or use the SDK sample code generated by API Explorer.

URI

GET /v2/{project_id}/alarm-histories

Table 6-87 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	**Definition** Tenant ID. **Constraints**: None **Value range**: Project ID, used to specify the project that an asset belongs to. You can query the assets of a project by project ID. You can obtain the project ID by calling an API or on the console. For details, see **Obtaining a Project ID**. The value must contain of 1 to 64 characters. **Default value**: None

Table 6-88 Query Parameters

Parameter	Mandatory	Type	Description
alarm_id	No	Array of strings	**Definition**: List of alarm IDs. Alarm ID. It starts with **al** and is followed by 22 characters, including letters or digits. **Constraints**: The list can contain a maximum of 50 alarm IDs.

Parameter	Mandatory	Type	Description
record_id	No	String	**Definition**: Alarm record ID. **Constraints**: None **Value range**: The value can contain 24 characters. It starts with **ah** and is followed by 22 characters, including letters or digits. **Default value**: None **Regex Pattern:** ^ah([0-9A-Za-z]){22}$
name	No	String	**Definition**: Alarm rule name. **Constraints**: None **Value range**: The value can contain a maximum of 128 characters. **Default value**: None
status	No	Array of strings	**Definition**: Alarm rule statuses. The value can be **ok**, **alarm**, or **invalid**. **Constraints**: The list can contain a maximum of three elements. Enumeration values: • **ok** • **alarm** • **invalid**

Parameter	Mandatory	Type	Description
level	No	Integer	**Definition**: Alarm severity. **Constraints**: None **Value range**: The value can be **1** (critical), ** 2** (major), **3** (minor), or **4** (informational). **Default value**: None **Value range:** 1-4
namespace	No	String	**Definition**: Namespace of a service. For details about the namespace of each service, see **Service namespace**. **Constraints**: None **Value range**: The value is in the **service.item** format. The values of **service** and **item** must be a string, starting with a letter and containing only digits (0–9), letters (case-insensitive), and underscores (_). The value must contain 3 to 32 characters. **Default value**: None **Regex Pattern:** ^([a-z]|[A-Z]){1}([a-z]|[A-Z]|[0-9]|_)*.([a-z]|[A-Z]){1}([a-z]|[A-Z]|[0-9]|_)*$

Parameter	Mandatory	Type	Description
resource_id	No	String	**Definition**: Alarm resource ID. **Constraints**: None **Value range**: In the context of multiple dimensions, resource IDs are separated by commas (,) in ascending alphabetical order. The value can contain a maximum of 2,048 characters. **Default value**: None **Regex Pattern:** ^([a-z]|[A-Z]|[0-9]|_|-|:|,|*|\.|/|#|\(|\))+$
from	No	String	**Definition**: Start time of the period during which alarm records are updated, for example, **2022-02-10T10:05:46+08:00**. **Constraints**: None **Value range**: The value can contain a maximum of 64 characters. **Default value**: None
to	No	String	**Definition**: End time of the period during which alarm records are updated, for example, **2022-02-10T10:05:47+08:00**. **Constraints**: None **Value range**: The value can contain a maximum of 64 characters. **Default value**: None

Parameter	Mandatory	Type	Description
alarm_type	No	String	**Definition**: Alarm type. **Constraints**: None **Value range**: Enumerated value. The value can be **event** (querying event alarms) or **metric** (querying metric alarms). **Default value**: None Enumeration values: • **event** • **metric**
create_time_from	No	String	**Definition**: Start time for generating alarm records, for example, **2022-02-10T10:05:46+08:00**. **Constraints**: None **Value range**: The value can contain a maximum of 64 characters. **Default value**: None
create_time_to	No	String	**Definition**: End time of the period during which alarm records are created, for example, **2022-02-10T10:05:47+08:00**. **Constraints**: None **Value range**: The value can contain a maximum of 64 characters. **Default value**: None

Parameter	Mandatory	Type	Description
offset	No	Integer	**Definition**: Pagination offset. **Constraints**: None **Value range**: The value is an integer from **0** to **1000000000**. **Default value**: 0 **Value range:** 0-1000000000 **Default value:** 0
limit	No	Integer	**Definition**: Pagination offset. **Constraints**: None **Value range**: The value is an integer from **1** to **100**. **Default value**: 100 **Value range:** 1-100 **Default value:** 100 **Regex Pattern:** ^([1-9]|[1-9][0-9]|100)$

Parameter	Mandatory	Type	Description
order_by	No	String	**Definition**: Keyword for sorting alarms. **Constraints**: None **Value range**: Enumerated value. The value can be **first_alarm_time** (time for generating the alarm for the first time), **update_time** (alarm update time), **alarm_level** (alarm severity), or **record_id** (primary key of the table record). **Default value**: update_time Enumeration values: • **first_alarm_time** • **update_time** • **alarm_level** • **record_id**

Request Parameters

Table 6-89 Request header parameters

Parameter	Mandatory	Type	Description
Content-Type	No	String	**Definition** MIME type of the request body. **Constraints**: None **Value range**: The value can contain 1 to 64 characters. **Default value**: The default type is **application/json; charset=UTF-8**. **Default value:** application/json; charset=UTF-8

Parameter	Mandatory	Type	Description
X-Auth-Token	No	String	**Definition** User token. **Constraints**: None **Value range**: The value can contain 1 to 16,384 characters. **Default value**: None

Response Parameters

Status code: 200

Table 6-90 Response body parameters

Parameter	Type	Description
alarm_histories	Array of **AlarmHistoryItemV2** objects	**Definition**: Alarm records.
count	Integer	**Definition**: Total number of alarm records. **Value range**: None **Value range:** 0-2147483647

Table 6-91 AlarmHistoryItemV2

Parameter	Type	Description
record_id	String	**Definition**: Alarm record ID. **Value range**: The value can contain a maximum of 24 characters.

Parameter	Type	Description
alarm_id	String	**Definition**: Alarm rule ID, for example, **al1603131199286dzxpqK3Ez**. **Value range**: The value can contain a maximum of 24 characters.
name	String	**Definition**: Alarm rule name, for example, **alarm-test01**. **Value range**: The value can contain 1 to 128 characters.
status	String	**Definition**: Alarm record status. **Value range**: The value can be **ok**, **alarm**, **invalid**, or **ok_manual**. **ok** indicates normal, **alarm** indicates an ongoing alarm, **invalid** indicates an invalid alarm, and **ok_manual** indicates manual recovery. Enumeration values: • **ok** • **alarm** • **invalid** • **ok_manual**
level	Integer	**Definition**: Alarm severity. **Value range**: The value can be **1** (critical), **2** (major), **3** (minor), and **4** (informational). Enumeration values: • **1** • **2** • **3** • **4**

Parameter	Type	Description
type	String	**Definition**: Alarm rule type. **Value range**: Enumerated value. **ALL_INSTANCE** indicates alarm rules for metrics of all resources. **RESOURCE_GROUP** indicates alarm rules for metrics of resources in a resource group. **MULTI_INSTANCE** indicates alarm rules for metrics of specified resources. **EVENT.SYS** indicates alarm rules for system events. **EVENT.CUSTOM** indicates alarm rules for custom events. **DNSHealthCheck** indicates alarm rules for health checks. Enumeration values: • **EVENT.SYS** • **EVENT.CUSTOM** • **DNSHealthCheck** • **RESOURCE_GROUP** • **MULTI_INSTANCE** • **ALL_INSTANCE** **Regex Pattern:** ^(EVENT.SYS|EVENT.CUSTOM|DNSHealthCheck|RESOURCE_GROUP|MULTI_INSTANCE|ALL_INSTANCE)$
action_enabled	Boolean	**Definition**: Whether to send notifications. **Value range**: **true**: Notifications are sent. **false**: Notifications are not sent.
begin_time	String	**Definition**: UTC time when the alarm was generated. **Value range**: None
end_time	String	**Definition**: Alarm end time (UTC time). **Value range**: None

Parameter	Type	Description
first_alarm_time	String	**Definition**: UTC time when the alarm was generated for the first time. **Value range**: None
last_alarm_time	String	**Definition**: UTC time when the alarm was generated for the last time. **Value range**: None
alarm_recovery_time	String	**Definition**: UTC time when the alarm was cleared. **Value range**: None
metric	**metric** object	**Definition** Metric information.
condition	**condition** object	**Definition**: Alarm triggering condition.
additional_info	**AdditionalInfo** object	**Definition**: Additional field of an alarm record. This is only intended for alarm records generated in event monitoring.
alarm_actions	Array of **alarm_actions** objects	**Definition**: Actions triggered by the alarm. The structure is as follows: { "type": "notification", "notification_list": ["urn:smn:southchina:68438a86d98e427e907e0097b7e35d47:sd"] }. The value of **type** can be: **notification**: Notifications will be sent. **autoscaling**: A scaling action will be triggered. **notification_list**: recipients to be notified of the alarm status changes.

Parameter	Type	Description
ok_actions	Array of **ok_actions** objects	**Definition**: Action to be triggered after an alarm is cleared. The structure is as follows: { "type": "notification", "notification_list": ["urn:smn:southchina:68438a86d98e427e907e0097b7e35d47:sd"] }. The value of **type** can be **notification** or **notification_list** (recipients to be notified of the alarm status changes).
data_points	Array of **DataPointInfo** objects	Time when the resource monitoring data is reported and the monitoring data in the alarm record.

Table 6-92 metric

Parameter	Type	Description
namespace	String	**Definition**: Namespace of a service. For details about the namespace of each service, see **Service namespace**. **Value range**: The value can contain 3 to 32 characters.
metric_name	String	**Definition**: Metric name of a resource. For example, the ECS metric **cpu_util** indicates the CPU usage of an ECS. The DDS metric **mongo001_command_ps** indicates the command execution frequency. For details about the metrics of each service, see **Service metric name**. **Value range**: The value can contain 1 to 64 characters.
dimensions	Array of **dimensions** objects	**Definition**: Metric dimension. **Value range**: None

Table 6-93 dimensions

Parameter	Type	Description
name	String	**Definition**: Dimension of a resource. For example, the dimension of an ECS can be **instance_id**. A maximum of four dimensions are supported. For the metric dimension of each resource, see **Service metric dimension**. **Value range**: The value can contain 1 to 32 characters. **Regex Pattern:** ^([a-z]|[A-Z]){1}([a-z]|[A-Z]|[0-9]|_|-)*$
value	String	**Definition**: Resource dimension value, which is an instance ID, for example, **4270ff17-aba3-4138-89fa-820594c39755**. **Value range**: The value can contain 1 to 256 characters. **Regex Pattern:** ^((([a-z]|[A-Z]|[0-9]|*|_|/|#|\(|\)){1}([a-z]|[A-Z]|[0-9]|_|-|\.|*|/|#|\(|\))*))$

Table 6-94 condition

Parameter	Type	Description
period	Integer	**Definition**: Metric period, in seconds. For details about the original metric period for each cloud service, see **Supported Services**. **Value range**: **0**: default value. For example, this value can be used for event alarms. **1**: original metric period. For example, if the original period of an RDS metric is 60s, the metric data is collected and calculated every 60s. **300**: The metric data is collected and calculated every 5 minutes. **1200**: The metric data is collected and calculated every 20 minutes. **3600**: The metric data is collected and calculated every 60 minutes. **14400**: The metric data is collected and calculated every 4 hours. **86400**: The metric data is collected and calculated every day. Enumeration values: • **0** • **1** • **300** • **1200** • **3600** • **14400** • **86400**
filter	String	**Definition**: Aggregation method. **Value range**: Enumerated value. The options are **average**, **min**, **max**, **sum**, **tp99** (99th percentile), **tp95** (95th percentile), and **tp90** (90th percentile). The value can contain 1 to 15 characters. **Regex Pattern:** ^(average|min|max|sum|tp99|tp95|tp90)$

Parameter	Type	Description
comparison_operator	String	**Definition**: Threshold symbol. **Value range**: Enumerated value. The value can be **>**, **<**, **>=**, **<=**, **=**, **!=**, **cycle_decrease**, **cycle_increase**, or **cycle_wave**. **cycle_decrease** indicates the decrease relative to the last period; **cycle_increase** indicates the increase relative to the last period; **cycle_wave** indicates the increase or decrease relative to the last period. The value can contain 1 to 10 characters. **Regex Pattern:** ^(>|<|>=|<=|=|!=|cycle_decrease|cycle_increase|cycle_wave)$
value	Double	**Definition**: Alarm threshold. **Value range**: For detailed thresholds, see the value range of each metric in the appendix. For example, you can set ECS **cpu_util** to **80** in **Services Interconnected with Cloud Eye**. The value ranges from **0** to **1.7976931348623157e+108**. **Value range:** 0-1.7976931348623156E108
unit	String	**Definition**: Data unit. **Value range**: The value can contain a maximum of 32 characters.
count	Integer	**Definition**: Number of consecutive alarm triggers. **Value range**: The value can contain 1 to 180 characters. **Value range:** 1-180

Parameter	Type	Description
suppress_duration	Integer	**Definition**: Alarm suppression duration (alarm interval), in seconds. This parameter corresponds to the last field in the alarm policy when you create an alarm rule. This field is used to address the issue of frequent alarm occurrences. **Value range**: **0**: The alarm is not suppressed. An alarm is generated when the condition is met. **300**: An alarm is generated every 5 minutes once the alarm triggering condition is met. **600**: An alarm is generated every 10 minutes once the alarm triggering condition is met. **900**: An alarm is generated every 15 minutes once the alarm triggering condition is met. **1800**: An alarm is generated every 30 minutes once the alarm triggering condition is met. **3600**: An alarm is generated every 60 minutes once the alarm triggering condition is met. **10800**: An alarm is generated every 3 hours once the alarm triggering condition is met. **21600**: An alarm is generated every 6 hours after the alarm triggering condition is met. **43200**: An alarm is generated every 12 hours once the alarm triggering condition is met. **8600**: An alarm is generated once every day once the alarm triggering condition is met. Enumeration values: • **0** • **300** • **600** • **900** • **1800**

Parameter	Type	Description
		• **3600** • **10800** • **21600** • **43200** • **86400** **Regex Pattern:** ^(0|300|600|900|1800|3600|10800|21600|43200|86400)$

Table 6-95 AdditionalInfo

Parameter	Type	Description
resource_id	String	**Definition**: Resource ID corresponding to the alarm record, for example, **22d98f6c-16d2-4c2d-b424-50e79d82838f**. **Value range**: The value can contain a maximum of 128 characters.
resource_name	String	**Definition**: Resource name corresponding to the alarm record, for example, **ECS-Test01**. **Value range**: The value can contain a maximum of 128 characters.
event_id	String	**Definition**: ID of the event in the alarm record, for example, **ev16031292300990kKN8p17J**. **Value range**: The value can contain a maximum of 24 characters.

Table 6-96 alarm_actions

Parameter	Type	Description
type	String	**Definition**: Notification type. **Value range**: Enumerated value. The value can be **notification** (SMN notifications), **contact** (account contacts), **contactGroup** (notification groups), or **autoscaling** (AS notifications). **autoscaling** is used only in AS and is not recommended. **groupwatch**, **ecsRecovery**, and **iecAction** are no longer used. Enumeration values: • **notification** • **autoscaling** • **groupwatch** • **ecsRecovery** • **contact** • **contactGroup** • **iecAction**
notification_list	Array of strings	**Definition**: Recipients to be notified of the alarm status changes. The value of **topicUrn** can be obtained from SMN. For details, see section "Querying Topics".

Table 6-97 ok_actions

Parameter	Type	Description
type	String	**Definition**: Notification type. **Value range**: Enumerated value. The value can be **notification** (SMN notifications), **contact** (account contacts), **contactGroup** (notification groups), or **autoscaling** (AS notifications). **autoscaling** is used only in AS and is not recommended. **groupwatch**, **ecsRecovery**, and **iecAction** are no longer used. Enumeration values: • **notification** • **autoscaling** • **groupwatch** • **ecsRecovery** • **contact** • **contactGroup** • **iecAction**
notification_list	Array of strings	**Definition**: Recipients to be notified of the alarm status changes. The value of **topicUrn** can be obtained from SMN. For details, see section "Querying Topics".

Table 6-98 DataPointInfo

Parameter	Type	Description
time	String	**Definition**: UTC time when the resource monitoring data of the alarm record is reported. **Value range**: The value can contain 1 to 64 characters.

Parameter	Type	Description
value	Double	**Definition**: Resource monitoring data of the alarm record at the time point, for example, **7.019**. **Value range**: The value is an integer from **0** to **1.7976931348623157e+308**. **Value range:** 0-1.7976931348623157E308

Status code: 400

Table 6-99 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 500

Table 6-100 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Example Requests

Alarm records whose **alarm_name** is **alarm-test01**, and **from** and **to** are **2022-02-10T10:05:46+08:00**.

```
/v2/{project_id}/alarm-histories?
limit=10&offset=0&from=2022-02-10T10:05:46+08:00&to=2022-02-10T12:05:46+08:00&alarm_name=alarm-test01
```


Example Responses

Status code: 200

Query succeeded.


```
{
  "alarm_histories" : [ {
    "alarm_id" : "al1604473987569z6n6nkpm1",
    "record_id" : "ah1655717086704DEnBrJ999",
    "name" : "TC_CES_FunctionBaseline_Alarm_008",
    "metric" : {
      "namespace" : "SYS.VPC",
      "dimensions" : [ {
        "name" : "bandwidth_id",
        "value" : "79a9cc0c-f626-4f15-bf99-a1f184107f88"
      } ],
      "metric_name" : "downstream_bandwidth"
    },
    "condition" : {
      "period" : 1,
      "filter" : "average",
      "comparison_operator" : ">=",
      "value" : 0,
      "count" : 3,
      "suppress_duration" : 3600
    },
    "level" : 2,
    "type" : "ALL_INSTANCE",
    "begin_time" : "2024-02-11T05:48:08+08:00",
    "end_time" : "2024-02-11T08:48:08+08:00",
    "last_alarm_time" : "2024-02-11T06:48:08+08:00",
    "alarm_recovery_time" : "2024-02-11T08:48:08+08:00",
    "action_enabled" : false,
    "alarm_actions" : [ ],
    "ok_actions" : [ ],
    "status" : "alarm",
    "data_points" : [ {
      "time" : "2022-06-22T16:38:02+08:00",
      "value" : 873.1507798960139
    }, {
      "time" : "2022-06-22T16:28:02+08:00",
      "value" : 883.1507798960139
    }, {
      "time" : "2022-06-22T16:18:02+08:00",
      "value" : 873.4
    } ],
    "additional_info" : {
      "resource_id" : "",
      "resource_name" : "",
      "event_id" : ""
    }
  } ],
  "count" : 103
}
```


Status Codes

Status Code	Description
200	Query succeeded.
400	Parameter verification failed.
500	Internal system error.

Error Codes

See **Error Codes**.

6.6 Alarm Templates

6.6.1 Creating a Custom Alarm Template

Function

This API is used to create a custom alarm template.

Debugging

You can debug this API through automatic authentication in **API Explorer** or use the SDK sample code generated by API Explorer.

URI

POST /v2/{project_id}/alarm-templates

Table 6-101 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Tenant ID.

Request Parameters

Table 6-102 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Tenant token.

Table 6-103 Request body parameters

Parameter	Mandatory	Type	Description
template_name	Yes	String	Name of an alarm template. The name must start with a letter and can contain 1 to 128 characters, including letters, digits, underscores (_), and hyphens (-).
template_type	No	Integer	Type of a custom alarm template. **0** indicates an alarm template for metrics. **2** indicates an alarm template for events. **Default value:** 0 Enumeration values: • **0** • **2**
template_description	No	String	Supplementary information about an alarm template. The description can contain 0 to 256 characters and is left blank by default.
is_overwrite	No	Boolean	Whether to overwrite the existing alarm template with the same name. **true**: Overwrite the alarm template. **false**: Create a new one. **Default value:** false
policies	Yes	Array of **Policies** objects	Alarm policies in an alarm template.

Table 6-104 Policies

Parameter	Mandatory	Type	Description
namespace	Yes	String	Namespace of a service. For details about the namespace of each service, see **Namespace**.

Parameter	Mandatory	Type	Description
dimension_name	No	String	Resource dimension, which must start with a letter. A dimension can contain up to 32 characters, including only digits, letters, underscores (_), and hyphens (-). Use commas (,) to separate multiple dimensions. **DimensionName** in event alarm templates must be left blank.
metric_name	Yes	String	Metric name of a resource. The name must start with a letter and contain only digits, letters, and underscores. The length ranges from 1 to 64 characters. For example, **cpu_util** of an ECS indicates the CPU usage of the ECS. **mongo001_command_ps** in DDS indicates the command execution frequency. For details about the metric name of each service, see **Service metric name**.
extra_info	No	**MetricExtraInfo** object	Additional information about an alarm policy. This parameter is left blank by default.
period	Yes	Integer	Interval (seconds) for checking whether the alarm rule conditions are met. Enumeration values: • **0** • **1** • **300** • **1200** • **3600** • **14400** • **86400**

Parameter	Mandatory	Type	Description
filter	Yes	String	Aggregation mode. average: average value; variance: variance; min: minimum value; max: maximum value; sum: sum; tp99: 99 percentile; tp95: 95 percentile; tp90: 90 percentile
comparison_operator	Yes	String	Threshold symbol. The value can be >, <, >=, <=, =, **!=**, **cycle_decrease**, **cycle_increase**, or **cycle_wave**. **cycle_decrease** indicates the decrease compared with the last period, **cycle_increase** indicates the increase compared with the last period, and **cycle_wave** indicates the increase or decrease compared with the last period. All of them can be used in alarm rules for metrics. >, <, >=, <=, =, and **!=** can be used for alarm rules for events.
value	No	Number	Alarm threshold. If there is only one threshold, **value** and **alarm_level** are used in pairs. If there are both **hierarchical_value** and **value**, **hierarchical_value** is used. **Value range:** 0-1.7976931348623156E108
hierarchical_value	No	**HierarchicalValue** object	Multi-level alarm threshold. If there are both **hierarchical_value** and **value**, **hierarchical_value** prevails. When you create or modify an alarm rule, you can set only one threshold in the following scenarios: 1. The alarm type is **Metric** and the alarm policy is **Trigger an alarm when all policies are met**. 2. The alarm type is **Event**.

Parameter	Mandatory	Type	Description
unit	No	String	Data unit. The value can contain up to 32 characters.
selected_unit	No	String	The unit you selected, which is used for subsequent metric data display and calculation.
count	Yes	Integer	Number of consecutive alarm triggering times. For event alarms, the value ranges from **1** to **180**. For metric and website alarms, the value can be **1**, **2**, **3**, **4**, **5**, **10**, **15**, **30**, **60**, **90**, **120**, or **180**.
alarm_level	No	Integer	Alarm severity, which can be **1** (critical), ** 2** (major), **3** (minor), or **4** (informational).
suppress_duration	No	Integer	Alarm suppression period, in seconds. When the period is **0**, only one alarm is generated. Enumeration values: • **0** • **300** • **600** • **900** • **1800** • **3600** • **10800** • **21600** • **43200** • **86400**

Table 6-105 MetricExtraInfo

Parameter	Mandatory	Type	Description
origin_metric_name	Yes	String	Original metric name. **Regex Pattern:** ^([a-z]|[A-Z]|[0-9]|_|-|~|\.|/|:)*$
metric_prefix	No	String	Metric name prefix. **Regex Pattern:** ^([a-z]|[A-Z]|[0-9]|_|-|~|\.|/|:)*$

Parameter	Mandatory	Type	Description
custom_proc_name	No	String	Name of a user process.
metric_type	No	String	Metric type. **Regex Pattern:** ^([a-z]|[A-Z]|[0-9]|_|-|~|\.|/|:)*$

Table 6-106 HierarchicalValue

Parameter	Mandatory	Type	Description
critical	No	Double	Threshold for critical alarms. **Value range:** -1.7976931348623156E108-1.7976931348623156E108
major	No	Double	Threshold for major alarms. **Value range:** -1.7976931348623156E108-1.7976931348623156E108
minor	No	Double	Threshold for minor alarms. **Value range:** -1.7976931348623156E108-1.7976931348623156E108
info	No	Double	Threshold for informational alarms. **Value range:** -1.7976931348623156E108-1.7976931348623156E108

Response Parameters

Status code: 201

Table 6-107 Response body parameters

Parameter	Type	Description
template_id	String	ID of an alarm template. The ID starts with **at** and is followed by up to 64 characters, including letters and digits.

Status code: 400

Table 6-108 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 401

Table 6-109 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 403

Table 6-110 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 500

Table 6-111 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Example Requests

Creating a custom alarm template whose **template_name** is **my_template**, **count** is **2**, **suppress_duration** is **300**, and **alarm_level** is **2**.

```
{
  "template_name" : "my_template",
  "template_description" : "hello world",
  "policies" : [ {
    "namespace" : "SYS.ECS",
    "dimension_name" : "instance_id",
    "metric_name" : "cpu_util",
    "period" : 300,
    "filter" : "sum",
    "comparison_operator" : ">",
    "value" : 2,
    "unit" : "bit/s",
    "count" : 2,
    "alarm_level" : 2,
    "suppress_duration" : 300
  } ]
}
```

Example Responses

Status code: 201

Created

```
{
  "template_id" : "at1628592157541dB1klWgY6"
}
```

Status Codes

Status Code	Description
201	Created
400	Parameter verification failed.
401	Not authenticated.
403	Authentication failed.
500	Internal system error.

Error Codes

See **Error Codes**.

6.6.2 Deleting Custom Alarm Templates in Batches

Function

This API is used to delete custom alarm templates in batches.

Debugging

You can debug this API through automatic authentication in **API Explorer** or use the SDK sample code generated by API Explorer.

URI

POST /v2/{project_id}/alarm-templates/batch-delete

Table 6-112 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Tenant ID.

Request Parameters

Table 6-113 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Tenant token.

Table 6-114 Request body parameters

Parameter	Mandatory	Type	Description
template_ids	Yes	Array of strings	IDs of alarm templates to be deleted in batches. Alarm templates that are not associated with alarm rules can be deleted in batches. For alarm templates that are associated with alarm rules, you can delete only one alarm template at a time. If you delete multiple ones, an exception will be returned.
delete_associate_alarm	Yes	Boolean	Whether alarm rules associated with an alarm template will be deleted when you delete the alarm template. **true** indicates that the alarm rules will be deleted. **false** indicates that only the alarm template will be deleted.

Response Parameters

Status code: 200

Table 6-115 Response body parameters

Parameter	Type	Description
template_ids	Array of strings	IDs of alarm templates that were deleted successfully.

Status code: 400

Table 6-116 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 401

Table 6-117 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 403

Table 6-118 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 500

Table 6-119 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Example Requests

Deleting custom alarm templates in batches.

```
{
  "template_ids" : [ "at1628592157541dB1klWgY6" ],
  "delete_associate_alarm" : false
}
```

Example Responses

Status code: 200

IDs of alarm templates successfully deleted.

```
{
  "template_ids" : [ "at1628592157541dB1klWgY6" ]
}
```

Status Codes

Status Code	Description
200	IDs of alarm templates successfully deleted.
400	Parameter verification failed.
401	Not authenticated.
403	Authentication failed.
500	Internal system error.

Error Codes

See **Error Codes**.

6.6.3 This API is used to modify a custom template.

Function

This API is used to modify a custom template.

Debugging

You can debug this API through automatic authentication in **API Explorer** or use the SDK sample code generated by API Explorer.

URI

PUT /v2/{project_id}/alarm-templates/{template_id}

Table 6-120 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Tenant ID.
template_id	Yes	String	ID of an alarm template.

Request Parameters

Table 6-121 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Tenant token.

Table 6-122 Request body parameters

Parameter	Mandatory	Type	Description
template_name	Yes	String	Name of an alarm template. The name must start with a letter and can contain 1 to 128 characters, including letters, digits, underscores (_), and hyphens (-).

Parameter	Mandatory	Type	Description
template_type	No	Integer	Type of a custom alarm template. **0** indicates an alarm template for metrics. **2** indicates an alarm template for events. Enumeration values: • **0** • **2**
template_description	No	String	Supplementary information about an alarm template. The description can contain 0 to 256 characters and is left blank by default.
policies	Yes	Array of **Policies** objects	Alarm policies in an alarm template.

Table 6-123 Policies

Parameter	Mandatory	Type	Description
namespace	Yes	String	Namespace of a service. For details about the namespace of each service, see **Namespace**.
dimension_name	No	String	Resource dimension, which must start with a letter. A dimension can contain up to 32 characters, including only digits, letters, underscores (_), and hyphens (-). Use commas (,) to separate multiple dimensions. **DimensionName** in event alarm templates must be left blank.

Parameter	Mandatory	Type	Description
metric_name	Yes	String	Metric name of a resource. The name must start with a letter and contain only digits, letters, and underscores. The length ranges from 1 to 64 characters. For example, **cpu_util** of an ECS indicates the CPU usage of the ECS. **mongo001_command_ps** in DDS indicates the command execution frequency. For details about the metric name of each service, see **Service metric name**.
extra_info	No	**MetricExtraInfo** object	Additional information about an alarm policy. This parameter is left blank by default.
period	Yes	Integer	Interval (seconds) for checking whether the alarm rule conditions are met. Enumeration values: • **0** • **1** • **300** • **1200** • **3600** • **14400** • **86400**
filter	Yes	String	Aggregation mode. average: average value; variance: variance; min: minimum value; max: maximum value; sum: sum; tp99: 99 percentile; tp95: 95 percentile; tp90: 90 percentile

Parameter	Mandatory	Type	Description
comparison_operator	Yes	String	Threshold symbol. The value can be **>**, **<**, **>=**, **<=**, **=**, **!=**, **cycle_decrease**, **cycle_increase**, or **cycle_wave**. **cycle_decrease** indicates the decrease compared with the last period, **cycle_increase** indicates the increase compared with the last period, and **cycle_wave** indicates the increase or decrease compared with the last period. All of them can be used in alarm rules for metrics. **>**, **<**, **>=**, **<=**, **=**, and **!=** can be used for alarm rules for events.
value	No	Number	Alarm threshold. If there is only one threshold, **value** and **alarm_level** are used in pairs. If there are both **hierarchical_value** and **value**, **hierarchical_value** is used. **Value range:** 0-1.7976931348623156E108
hierarchical_value	No	**HierarchicalValue** object	Multi-level alarm threshold. If there are both **hierarchical_value** and **value**, **hierarchical_value** prevails. When you create or modify an alarm rule, you can set only one threshold in the following scenarios: 1. The alarm type is **Metric** and the alarm policy is **Trigger an alarm when all policies are met**. 2. The alarm type is **Event**.
unit	No	String	Data unit. The value can contain up to 32 characters.
selected_unit	No	String	The unit you selected, which is used for subsequent metric data display and calculation.

Parameter	Mandatory	Type	Description
count	Yes	Integer	Number of consecutive alarm triggering times. For event alarms, the value ranges from **1** to **180**. For metric and website alarms, the value can be **1**, **2**, **3**, **4**, **5**, **10**, **15**, **30**, **60**, **90**, **120**, or **180**.
alarm_level	No	Integer	Alarm severity, which can be **1** (critical), ** 2** (major), **3** (minor), or **4** (informational).
suppress_duration	No	Integer	Alarm suppression period, in seconds. When the period is **0**, only one alarm is generated. Enumeration values: • **0** • **300** • **600** • **900** • **1800** • **3600** • **10800** • **21600** • **43200** • **86400**

Table 6-124 MetricExtraInfo

Parameter	Mandatory	Type	Description
origin_metric_name	Yes	String	Original metric name. **Regex Pattern:** ^([a-z]|[A-Z]|[0-9]|_|-|~|\.|/|:)*$
metric_prefix	No	String	Metric name prefix. **Regex Pattern:** ^([a-z]|[A-Z]|[0-9]|_|-|~|\.|/|:)*$
custom_proc_name	No	String	Name of a user process.
metric_type	No	String	Metric type. **Regex Pattern:** ^([a-z]|[A-Z]|[0-9]|_|-|~|\.|/|:)*$

Table 6-125 HierarchicalValue

Parameter	Mandatory	Type	Description
critical	No	Double	Threshold for critical alarms. **Value range:** -1.7976931348623156E108-1.7976931348623156E108
major	No	Double	Threshold for major alarms. **Value range:** -1.7976931348623156E108-1.7976931348623156E108
minor	No	Double	Threshold for minor alarms. **Value range:** -1.7976931348623156E108-1.7976931348623156E108
info	No	Double	Threshold for informational alarms. **Value range:** -1.7976931348623156E108-1.7976931348623156E108

Response Parameters

Status code: 204

No Content

Status code: 400

Table 6-126 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 401

Table 6-127 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 403

Table 6-128 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 404

Table 6-129 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 500

Table 6-130 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Example Requests

Modifying a custom template whose **template_name** is **my_template**.

```
{
  "template_name" : "my_template",
  "template_description" : "hello world",
  "policies" : [ {
    "namespace" : "SYS.ECS",
    "dimension_name" : "instance_id",
    "metric_name" : "cpu_util",
    "period" : 300,
    "filter" : "sum",
    "comparison_operator" : ">",
    "value" : 2,
    "unit" : "bit/s",
    "count" : 2,
    "alarm_level" : 2,
    "suppress_duration" : 300
  } ]
}
```

Example Responses

None

Status Codes

Status Code	Description
204	No Content
400	Parameter verification failed.
401	Not authenticated.
403	Authentication failed.
404	Resource not found.
500	Internal system error.

Error Codes

See **Error Codes**.

6.6.4 Querying Alarm Templates

Function

This API is used to query the alarm template list.

Debugging

You can debug this API through automatic authentication in **API Explorer** or use the SDK sample code generated by API Explorer.

URI

GET /v2/{project_id}/alarm-templates

Table 6-131 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Tenant ID.

Table 6-132 Query Parameters

Parameter	Mandatory	Type	Description
offset	No	Integer	Start position for pagination query, indicating the sequence number of the data record where the query starts. The default value is **0**. **Value range:** 0-10000
limit	No	Integer	Maximum number of query results. The value ranges from **1** to **100** (default). **Value range:** 1-100
namespace	No	String	Namespace of a service. For details about the namespace of each service, see **Namespace**. **Regex Pattern:** ^([a-z]|[A-Z]){1}([a-z]|[A-Z]|[0-9]|_)*\.([a-z]|[A-Z]){1}([a-z]|[A-Z]|[0-9]|_)*$
dim_name	No	String	Resource dimension, which must start with a letter. A dimension can contain up to 32 characters, including only digits, letters, underscores (_), and hyphens (-). Use commas (,) to separate multiple dimensions. **Regex Pattern:** ^([a-z]|[A-Z]){1}([a-z]|[A-Z]|[0-9]|_|-){0,31}(,([a-z]|[A-Z]){1}([a-z]|[A-Z]|[0-9]|_|-){0,31}){0,3}$

Parameter	Mandatory	Type	Description
template_type	No	String	Alarm template type. **system** indicates default alarm templates for metrics, **custom** indicates the custom alarm templates for metrics, **system_event** indicates default event templates, **custom_event** indicates the custom event templates, and **system_custom_event** indicates all default and custom event templates. If this parameter is not specified, all metric templates are returned. Enumeration values: • **system** • **custom** • **system_event** • **custom_event** • **system_custom_event**
template_name	No	String	Name of an alarm template. The name must start with a letter and can contain 1 to 128 characters, including letters, digits, underscores (_), and hyphens (-). Fuzzy match is supported. **Regex Pattern:** ^([\u4E00-\u9FFF]|[a-z]|[A-Z]|[0-9]|_|-|\(|\)|\.|\s){1,128}$
product_name	No	String	Alarm templates can be queried by product name. Generally, the product name format is **Service namespace,First-level dimension of the service**, for example, **SYS.ECS,instance_id**.

Request Parameters

Table 6-133 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Tenant token.

Response Parameters

Status code: 200

Table 6-134 Response body parameters

Parameter	Type	Description
alarm_templates	Array of **AlarmTemplates** objects	Alarm template list.
count	Integer	Total number of alarm templates. **Value range:** 0-9999999

Table 6-135 AlarmTemplates

Parameter	Type	Description
template_id	String	ID of an alarm template. The ID starts with **at** and is followed by up to 64 characters, including letters and digits.
template_name	String	Name of an alarm template. The name must start with a letter and can contain 1 to 128 characters, including letters, digits, underscores (_), and hyphens (-).
template_type	String	Type of an alarm template. **custom** indicates custom alarm templates, and **system** indicates default alarm templates. Enumeration values: • **system** • **custom**
create_time	String	Time when an alarm template was created.
template_description	String	Supplementary information about an alarm template. The description can contain 0 to 256 characters and is left blank by default.

Status code: 400

Table 6-136 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 401

Table 6-137 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 403

Table 6-138 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 500

Table 6-139 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Example Requests

Querying alarm templates.

```
/v2/{project_id}/alarm-templates?offset=0&limit=100
```

Example Responses

Status code: 200

OK

```
{
  "alarm_templates" : [ {
    "template_id" : "at1628592157541dB1klWgY6",
    "template_name" : "my_template",
    "template_type" : "custom",
    "create_time" : "2006-01-02T15:04:05.000Z",
    "template_description" : "hello world"
  } ],
  "count" : 100
}
```

Status Codes

Status Code	Description
200	OK
400	Parameter verification failed.
401	Not authenticated.
403	Authentication failed.
500	Internal system error.

Error Codes

See **Error Codes**.

6.6.5 Querying Details of an Alarm Template

Function

This API is used to query details of an alarm template.

Debugging

You can debug this API through automatic authentication in **API Explorer** or use the SDK sample code generated by API Explorer.

URI

GET /v2/{project_id}/alarm-templates/{template_id}

Table 6-140 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Tenant ID.
template_id	Yes	String	ID of an alarm template. The ID starts with **at** and is followed by up to 64 characters, including letters and digits.

Request Parameters

Table 6-141 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Tenant token.

Response Parameters

Status code: 200

Table 6-142 Response body parameters

Parameter	Type	Description
template_id	String	ID of an alarm template. The ID starts with **at** and is followed by up to 64 characters, including letters and digits.
template_name	String	Name of an alarm template. The name must start with a letter and can contain 1 to 128 characters, including letters, digits, underscores (_), and hyphens (-).
template_type	String	Type of an alarm template. **custom** indicates custom alarm templates, and **system** indicates default alarm templates. Enumeration values: • **system** • **custom**
create_time	String	Time when an alarm template was created.

Parameter	Type	Description
template_description	String	Supplementary information about an alarm template. The description can contain 0 to 256 characters and is left blank by default.
policies	Array of **AlarmTemplatePolicies** objects	Alarm policies in an alarm template.

Table 6-143 AlarmTemplatePolicies

Parameter	Type	Description
namespace	String	Namespace of a service. For details about the namespace of each service, see **Namespace**.
dimension_name	String	Resource dimension, which must start with a letter. A dimension can contain up to 32 characters, including only digits, letters, underscores (_), and hyphens (-). Use commas (,) to separate multiple dimensions. **DimensionName** in event alarm templates must be left blank.
metric_name	String	Metric name of a resource. The name must start with a letter and contain only digits, letters, and underscores. The length ranges from 1 to 64 characters. For example, **cpu_util** of an ECS indicates the CPU usage of the ECS. **mongo001_command_ps** in DDS indicates the command execution frequency. For details about the metric name of each service, see **Service metric name**.

Parameter	Type	Description
period	Integer	Interval (seconds) for checking whether the alarm rule conditions are met. Enumeration values: • **0** • **1** • **300** • **1200** • **3600** • **14400** • **86400**
filter	String	Data rollup method. **Regex Pattern:** ^(average|variance|min|max|sum)$
comparison_operator	String	Threshold symbol. The value can be **>**, **<**, **>=**, **<=**, **=**, **!=**, **cycle_decrease**, **cycle_increase**, or **cycle_wave**. **cycle_decrease** indicates the decrease compared with the last period, **cycle_increase** indicates the increase compared with the last period, and **cycle_wave** indicates the increase or decrease compared with the last period. All of them can be used in alarm rules for metrics. **>**, **<**, **>=**, **<=**, **=**, and **!=** can be used for alarm rules for events.
value	Number	Alarm threshold. If there is only one threshold, **value** and **alarm_level** are used in pairs. If there are both **hierarchical_value** and **value**, **hierarchical_value** prevails. **Value range:** 0-2.34854258277383E108

Parameter	Type	Description
hierarchical_value	HierarchicalValue object	Multi-level alarm threshold. If there are both **hierarchical_value** and **value**, **hierarchical_value** prevails. When you create or modify an alarm rule, you can set only one threshold in the following scenarios: 1. The alarm type is **Metric** and the alarm policy is **Trigger an alarm when all policies are met**. 2. The alarm type is **Event**.
unit	String	Data unit. The value can contain up to 32 characters.
count	Integer	Number of consecutive alarm triggering times. For event alarms, the value ranges from **1** to **180**. For metric and website alarms, the value can be **1**, **2**, **3**, **4**, **5**, **10**, **15**, **30**, **60**, **90**, **120**, or **180**.
alarm_level	Integer	Alarm severity, which can be **1** (critical), ** 2** (major), **3** (minor), or **4** (informational).
suppress_duration	Integer	Alarm suppression period, in seconds. When the period is **0**, only one alarm is generated. Enumeration values: • **0** • **300** • **600** • **900** • **1800** • **3600** • **10800** • **21600** • **43200** • **86400**
selected_unit	String	The unit you selected, which is used for subsequent metric data display and calculation.

Table 6-144 HierarchicalValue

Parameter	Type	Description
critical	Double	Threshold for critical alarms. **Value range:** -1.7976931348623156E108-1.7976931348623156E108
major	Double	Threshold for major alarms. **Value range:** -1.7976931348623156E108-1.7976931348623156E108
minor	Double	Threshold for minor alarms. **Value range:** -1.7976931348623156E108-1.7976931348623156E108
info	Double	Threshold for informational alarms. **Value range:** -1.7976931348623156E108-1.7976931348623156E108

Status code: 400

Table 6-145 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 401

Table 6-146 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 403

Table 6-147 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 404

Table 6-148 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 500

Table 6-149 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Example Requests

Querying details of an alarm template.

```
/v2/{project_id}/alarm-templates/{template_id}
```

Example Responses

Status code: 200

OK

```
{
  "template_id" : "at1628592157541dB1klWgY6",
  "template_name" : "my_template",
  "template_type" : "custom",
  "create_time" : "2006-01-02T15:04:05.000Z",
  "template_description" : "hello world",
  "policies" : [ {
    "namespace" : "SYS.ECS",
    "dimension_name" : "instance_id",
    "metric_name" : "cpu_util",
    "period" : 300,
    "filter" : "sum",
    "comparison_operator" : ">",
    "value" : 2,
    "hierarchical_value" : {
      "major" : 85
    },
    "unit" : "bit/s",
    "selected_unit" : "",
    "count" : 2,
    "alarm_level" : 2,
    "suppress_duration" : 300
  } ]
}
```


Status Codes

Status Code	Description
200	OK
400	Parameter verification failed.
401	Not authenticated.
403	Authentication failed.
404	Resource not found.
500	Internal system error.

Error Codes

See **Error Codes**.

6.7 Alarm Rules Associated with an Alarm Template

6.7.1 Querying Alarm Rules Associated with an Alarm Template

Function

This API is used to query alarm rules associated with the alarm template.

Debugging

You can debug this API through automatic authentication in **API Explorer** or use the SDK sample code generated by API Explorer.

URI

GET /v2/{project_id}/alarm-templates/{template_id}/association-alarms

Table 6-150 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Tenant ID.
template_id	Yes	String	ID of an alarm template. The ID starts with **at** and is followed by up to 64 characters, including letters and digits.

Table 6-151 Query Parameters

Parameter	Mandatory	Type	Description
offset	No	Integer	Start position for pagination query, indicating the sequence number of the data record where the query starts. The default value is **0**. **Value range:** 0-10000
limit	No	Integer	Maximum number of query results. The value ranges from **1** to **100** (default). **Value range:** 1-100

Request Parameters

Table 6-152 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Tenant token.

Response Parameters

Status code: 200

Table 6-153 Response body parameters

Parameter	Type	Description
alarms	Array of **alarms** objects	Alarm rule list.
count	Integer	Total number of alarm rules. **Value range:** 0-1000

Table 6-154 alarms

Parameter	Type	Description
alarm_id	String	Alarm rule ID. **Regex Pattern:** ^al([0-9A-Za-z]){22}$
name	String	Alarm rule name. **Regex Pattern:** ^([\u4E00-\u9FFF]|[a-z]|[A-Z]|[0-9]|_|-)+$
description	String	Description of the alarm rule.

Status code: 400

Table 6-155 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 401

Table 6-156 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 403

Table 6-157 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 500

Table 6-158 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Example Requests

Query alarm rules associated with an alarm template.

```
/v2/{project_id}/alarm-templates/{template_id}/association-alarms
```

Example Responses

Status code: 200

OK

```
{
  "alarms" : [ {
    "alarm_id" : "al12345678901234567890",
```

```
    "name" : "test",
    "description" : "Alarm rule list."
  } ],
  "count" : 100
}
```

Status Codes

Status Code	Description
200	OK
400	Parameter verification failed.
401	Not authenticated.
403	Authentication failed.
500	Internal system error.

Error Codes

See **Error Codes**.

6.8 Resource Groups

6.8.1 Creating a Resource Group (Recommended)

Function

This API is used to create a resource group.

Debugging

You can debug this API through automatic authentication in **API Explorer** or use the SDK sample code generated by API Explorer.

URI

POST /v2/{project_id}/resource-groups

Table 6-159 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Tenant ID.

Request Parameters

Table 6-160 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Tenant token.

Table 6-161 Request body parameters

Parameter	Mandatory	Type	Description
group_name	Yes	String	Resource group name. The value can contain up to 128 characters, including letters, digits, hyphens (-), and underscores (_). **Regex Pattern:** ^([\u4E00-\u9FFF]|[a-z]|[A-Z]|[0-9]|_|-)+$
enterprise_project_id	No	String	ID of the enterprise project that a resource group belongs to. **Regex Pattern:** ^((([a-z]|[0-9]){8}-([a-z]|[0-9]){4}-([a-z]|[0-9]){4}-([a-z]|[0-9]){4}-([a-z]|[0-9]){12})|0)$
type	No	String	Method for adding resources to a resource group. The value can only be **EPS** (synchronizing resources from enterprise projects), **TAG** (dynamic tag matching), or **NAME** (instance name). If this parameter is not specified, resources are manually added. **Regex Pattern:** ^(EPS|TAG|Manual|COMB|NAME)$
tags	No	Array of **ResourceGroupTagRelation** objects	Associated tag during dynamic tag matching. This parameter is mandatory when **type** is set to **TAG**.
association_ep_ids	No	Array of strings	ID of the enterprise project from which resources in the resource group come. This parameter is mandatory when **type** is set to **EPS**.

Parameter	Mandatory	Type	Description
providers	No	String	Cloud service name in the **dcs,ecs** format. For details about supported cloud services (**providers**), see section "Supported Services and Resource Types" in Config API Reference.
enterprise_project_id_and_tags	No	Array of **EnterpriseProjectIdAndTags** objects	Parameter for matching resources by enterprise project or tag.
resources	No	Array of **Resource** objects	Resource details when resources are manually added.
product_resources	No	Array of **ProductResource** objects	Resource details when the resource level is cloud product and resources are manually added.
instances	No	Array of **Instance** objects	Parameter transferred for matching resources by instance name.
product_names	No	String	Name of a cloud product when the resource level is cloud product. Generally, the value format is *Service namespace,First-level dimension of the service*, for example, **SYS.ECS,instance_id**. Multiple cloud products are separated by semicolons (;), for example, **SERVICE.BMS,instance_id;SYS.ECS,instance_id**.

Parameter	Mandatory	Type	Description
resource_level	No	String	Resource level, which indicates the resource scope. If you select **Cloud product** for **Resource Level**, resources from the selected cloud product and its dimensions will be added to the resource group. If you select **Specific dimension** for **Resource Level**, only resources from the specific sub-dimension will be added. **product**: cloud product **dimension**: sub-dimension Enumeration values: • **product** • **dimension**
comb_relation	No	**CombRelation** object	Matching resources by multiple criteria.

Table 6-162 ResourceGroupTagRelation

Parameter	Mandatory	Type	Description
key	Yes	String	TMS tag key specifications.

Parameter	Mandatory	Type	Description
operator	No	String	Tag operator, which indicates the relationship between the tag key and value. **include**: indicates include. **prefix**: indicates the prefix. **suffix**: indicates the suffix. **notInclude**: indicates not included. **equal**: indicates equal. If **operator** is **equal** and **value** is an empty string, all tag values of the key are matched. **all**: indicates all. Enumeration values: • **include** • **prefix** • **suffix** • **notInclude** • **equal** • **all**
value	No	String	TMS tag value specifications.

Table 6-163 EnterpriseProjectIdAndTags

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise Project ID. **Regex Pattern:** ^([a-z]|[A-Z]|[0-9]|_|-)+$
tag	No	ResourceGroupTagRelation object	Tag matching rule.

Table 6-164 Resource

Parameter	Mandatory	Type	Description
namespace	Yes	String	Namespace of a service. For details about the namespace of each service, see Namespace.

Parameter	Mandatory	Type	Description
dimensions	Yes	Array of **ResourceDimension** objects	Resource dimension information.

Table 6-165 ResourceDimension

Parameter	Mandatory	Type	Description
name	Yes	String	Dimension of a resource. For example, the dimension of an ECS can be **instance_id**. A maximum of four dimensions are supported. For the metric dimension of each resource, see **Service metric dimension**. **Regex Pattern:** ^([a-z]|[A-Z]){1}([a-z]|[A-Z]|[0-9]|_|-){1,32}$
value	Yes	String	Value of a resource dimension. It is the instance ID, for example, **4270ff17-aba3-4138-89fa-820594c39755**. **Regex Pattern:** ^((([a-z]|[A-Z]|[0-9]){1}([a-z]|[A-Z]|[0-9]|_|-|\.)*)|*){1,256}$

Table 6-166 ProductResource

Parameter	Mandatory	Type	Description
product_name	Yes	String	Cloud product that the resource belongs to. Generally, the value format is *Service namespace,First-level dimension name of the service*, for example, **SYS.ECS,instance_id**.

Parameter	Mandatory	Type	Description
namespace	Yes	String	Namespace of a service. For details about the namespace of each service, see **Namespace**. **Regex Pattern:** ^([a-z]|[A-Z]){1}([a-z]|[A-Z]|[0-9]|_)*\.([a-z]|[A-Z]){1}([a-z]|[A-Z]|[0-9]|_)*$
product_instances	Yes	Array of **ProductInstance** objects	Product instance details.

Table 6-167 ProductInstance

Parameter	Mandatory	Type	Description
first_dimension_name	Yes	String	First-level dimension of the resource. For example, the dimension of an ECS is **instance_id**. **Regex Pattern:** ^([a-z]|[A-Z]){1}([a-z]|[A-Z]|[0-9]|_|-){1,32}$
first_dimension_value	Yes	String	First-level dimension value of the resource, which is the resource ID, for example, **4270ff17-aba3-4138-89fa-820594c39755**. **Regex Pattern:** ^((([a-z]|[A-Z]|[0-9]){1}([a-z]|[A-Z]|[0-9]|_|-|\.)*)|*){1,256}$
resource_name	Yes	String	Resource name.

Table 6-168 Instance

Parameter	Mandatory	Type	Description
product_name	Yes	String	Cloud product name.

Parameter	Mandatory	Type	Description
logical_operator	Yes	String	Logical operator. **ALL**: All conditions are matched. **ANY**: Any condition is matched. Enumeration values: • **ALL** • **ANY**
instance_names	Yes	Array of **ResourceName** objects	Parameter array for matching resources by resource name.

Table 6-169 ResourceName

Parameter	Mandatory	Type	Description
resource_name	No	String	Resource name condition value.
operator	Yes	String	Instance operator, which indicates the operation relationship between the actual resource name and the resource name condition value. **include**: indicates include. **prefix**: indicates the prefix. **suffix**: indicates the suffix. **notInclude**: indicates not included. **equal**: indicates equal. **all**: indicates all. Enumeration values: • **include** • **prefix** • **suffix** • **notInclude** • **equal** • **all**
resource_name_is_ignore_case	No	Boolean	The resource name is case-insensitive.

Table 6-170 CombRelation

Parameter	Mandatory	Type	Description
logical_operator	Yes	String	Logical operator. **ALL**: All conditions are matched. **ANY**: Any condition is matched. Enumeration values: • **ALL** • **ANY**
conditions	Yes	Array of **Condition** objects	Combined matching conditions for resource groups.

Table 6-171 Condition

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise Project ID. **Regex Pattern:** ^((([a-z]|[0-9]){8}-([a-z]|[0-9]){4}-([a-z]|[0-9]){4}-([a-z]|[0-9]){4}-([a-z]|[0-9]){12})|0)$
instance_name	No	**ResourceName** object	Resource name.
tag	No	**ResourceGroupTagRelation** object	Tag matching rule.

Response Parameters

Status code: 200

Table 6-172 Response body parameters

Parameter	Type	Description
group_id	String	Resource group ID, which starts with **rg** and is followed by 22 characters, including letters and digits.

Status code: 400

Table 6-173 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 401

Table 6-174 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 403

Table 6-175 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 500

Table 6-176 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Example Requests

Creating a resource group whose **group _name** is **rg_test** and **type** is **TAG**.

```
{
  "group_name" : "rg_test",
  "enterprise_project_id" : "0",
  "type" : "TAG",
  "tags" : [ {
    "key" : "key1",
    "value" : "value1"
  } ],
  "association_ep_ids" : [ "d61d4705-5658-42f5-8e0c-70eb34d17b02" ]
}
```

Example Responses

Status code: 200

Created

```
{
  "group_id" : "rg0123456789xxx"
}
```

Status Codes

Status Code	Description
200	Created
400	Parameter verification failed.
401	Not authenticated.
403	Authentication failed.
500	Internal system error.

Error Codes

See **Error Codes**.

6.8.2 This API is used to delete resource groups in batches.

Function

This API is used to delete resource groups in batches.

Debugging

You can debug this API through automatic authentication in **API Explorer** or use the SDK sample code generated by API Explorer.

URI

POST /v2/{project_id}/resource-groups/batch-delete

Table 6-177 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Tenant ID.

Request Parameters

Table 6-178 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Tenant token.

Table 6-179 Request body parameters

Parameter	Mandatory	Type	Description
group_ids	Yes	Array of strings	IDs of resource groups to be deleted in batches.

Response Parameters

Status code: 200

Table 6-180 Response body parameters

Parameter	Type	Description
group_ids	Array of strings	IDs of resource groups that were successfully deleted.

Status code: 400

Table 6-181 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.

Parameter	Type	Description
request_id	String	Request ID.

Status code: 401

Table 6-182 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 403

Table 6-183 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 500

Table 6-184 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Example Requests

Batch deleting resource groups.


```
{
  "group_ids" : [ "rg0123456789xxxx" ]
}
```

Example Responses

Status code: 200

IDs of resource groups that were successfully deleted.

```
{
  "group_ids" : [ "rg0123456789xxxx" ]
}
```

Status Codes

Status Code	Description
200	IDs of resource groups that were successfully deleted.
400	Parameter verification failed.
401	Not authenticated.
403	Authentication failed.
500	Internal system error.

Error Codes

See **Error Codes**.

6.8.3 Modifying a Resource Group

Function

This API is used to modify a resource group.

Debugging

You can debug this API through automatic authentication in **API Explorer** or use the SDK sample code generated by API Explorer.

URI

PUT /v2/{project_id}/resource-groups/{group_id}

Table 6-185 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Tenant ID.

Parameter	Mandatory	Type	Description
group_id	Yes	String	Resource group ID, which starts with **rg** and is followed by 22 characters, including letters and digits.

Request Parameters

Table 6-186 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Tenant token.

Table 6-187 Request body parameters

Parameter	Mandatory	Type	Description
group_name	Yes	String	Resource group name. The value can contain up to 128 characters, including letters, digits, hyphens (-), and underscores (_).
tags	No	Array of **ResourceGroupTagRelation** objects	Associated tag during dynamic tag matching. This parameter must be specified when **type** is set to **TAG**.
enterprise_project_id_and_tags	No	Array of **EnterpriseProjectIdAndTags** objects	Parameter transferred when **Matching Resource By** is set to **Multiple criteria**.
extend_relation_ids	No	Array of strings	Parameter transferred for matching resources by enterprise project when **Add Resources** is set to **Automatically**.
instances	No	Array of **Instance** objects	Parameter transferred for matching resources by instance name.

Parameter	Mandatory	Type	Description
product_names	No	String	Value of a cloud product when the resource level is changed to cloud product. Generally, the value format is *Service namespace,First-level dimension of the service*, for example, **SYS.ECS,instance_id**. Multiple cloud products are separated by semicolons (;), for example, **SERVICE.BMS,instance_id;SYS.ECS,instance_id**.
comb_relation	No	**CombRelation** object	Matching resources by multiple criteria.

Table 6-188 ResourceGroupTagRelation

Parameter	Mandatory	Type	Description
key	Yes	String	TMS tag key specifications.
operator	No	String	Tag operator, which indicates the relationship between the tag key and value. **include**: indicates include. **prefix**: indicates the prefix. **suffix**: indicates the suffix. **notInclude**: indicates not included. **equal**: indicates equal. If **operator** is **equal** and **value** is an empty string, all tag values of the key are matched. **all**: indicates all. Enumeration values: • **include** • **prefix** • **suffix** • **notInclude** • **equal** • **all**
value	No	String	TMS tag value specifications.

Table 6-189 EnterpriseProjectIdAndTags

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise Project ID. **Regex Pattern:** ^([a-z]|[A-Z]|[0-9]|_|-)+$
tag	No	**ResourceGroupTagRelation** object	Tag matching rule.

Table 6-190 Instance

Parameter	Mandatory	Type	Description
product_name	Yes	String	Cloud product name.
logical_operator	Yes	String	Logical operator. **ALL**: All conditions are matched. **ANY**: Any condition is matched. Enumeration values: • **ALL** • **ANY**
instance_names	Yes	Array of **ResourceName** objects	Parameter array for matching resources by resource name.

Table 6-191 ResourceName

Parameter	Mandatory	Type	Description
resource_name	No	String	Resource name condition value.

Parameter	Mandatory	Type	Description
operator	Yes	String	Instance operator, which indicates the operation relationship between the actual resource name and the resource name condition value. **include**: indicates include. **prefix**: indicates the prefix. **suffix**: indicates the suffix. **notInclude**: indicates not included. **equal**: indicates equal. **all**: indicates all. Enumeration values: • **include** • **prefix** • **suffix** • **notInclude** • **equal** • **all**
resource_name_is_ignore_case	No	Boolean	The resource name is case-insensitive.

Table 6-192 CombRelation

Parameter	Mandatory	Type	Description
logical_operator	Yes	String	Logical operator. **ALL**: All conditions are matched. **ANY**: Any condition is matched. Enumeration values: • **ALL** • **ANY**
conditions	Yes	Array of **Condition** objects	Combined matching conditions for resource groups.

Table 6-193 Condition

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise Project ID. **Regex Pattern:** ^((([a-z]|[0-9]){8}-([a-z]|[0-9]){4}-([a-z]|[0-9]){4}-([a-z]|[0-9]){4}-([a-z]|[0-9]){12})|0)$
instance_name	No	**ResourceName** object	Resource name.
tag	No	**ResourceGroupTagRelation** object	Tag matching rule.

Response Parameters

Status code: 204

No Content

Status code: 400

Table 6-194 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 401

Table 6-195 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 403

Table 6-196 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 404

Table 6-197 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 500

Table 6-198 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Example Requests

Modify the resource group named **rg_test**.

```
{
  "group_name" : "test",
  "tags" : [ {
    "key" : "key1",
    "value" : "value1"
  } ]
}
```

Example Responses

None

Status Codes

Status Code	Description
204	No Content
400	Parameter verification failed.
401	Not authenticated.
403	Authentication failed.
404	Resource not found.
500	Internal system error.

Error Codes

See **Error Codes**.

6.8.4 Querying Details of a Resource Group

Function

This API is used to query details of a resource group.

Debugging

You can debug this API through automatic authentication in **API Explorer** or use the SDK sample code generated by API Explorer.

URI

GET /v2/{project_id}/resource-groups/{group_id}

Table 6-199 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Tenant ID.
group_id	Yes	String	Resource group ID, which starts with **rg** and is followed by 22 characters, including letters and digits.

Request Parameters

Table 6-200 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Tenant token.

Response Parameters

Status code: 200

Table 6-201 Response body parameters

Parameter	Type	Description
group_name	String	Resource group name. **Regex Pattern:** ^((([a-z]|[0-9]){8}-([a-z]|[0-9]){4}-([a-z]|[0-9]){4}-([a-z]|[0-9]){4}-([a-z]|[0-9]){12})|0)$
group_id	String	Resource group ID, which starts with **rg** and is followed by 22 characters, including letters and digits.
create_time	String	Time when a resource group was created.
enterprise_project_id	String	ID of the enterprise project that a resource group belongs to. **Regex Pattern:** ^((([a-z]|[0-9]){8}-([a-z]|[0-9]){4}-([a-z]|[0-9]){4}-([a-z]|[0-9]){4}-([a-z]|[0-9]){12})|0)$
type	String	Resource adding/matching mode. The value can only be EPS (matching enterprise projects), TAG (matching tags), NAME (matching instance names), COMB (combination matching), or Manual (manual adding). Enumeration values: • **EPS** • **TAG** • **NAME** • **COMB** • **Manual**

Parameter	Type	Description
association_ep_ids	Array of strings	ID of the enterprise project from which resources in the resource group come. This parameter is mandatory when **type** is set to **EPS**.
tags	Array of **ResourceGroupTagRelation** objects	Specified tag rule when the resource matching rule is tag matching.
instances	Array of **Instance** objects	Parameter transferred for matching resources by instance name.
comb_relation	**CombRelation** object	Matching resources by multiple criteria.
related_ep_ids	Array of strings	List of specified enterprise projects when the resource matching rule is enterprise project matching.
enterprise_project_id_and_tags	Array of **EnterpriseProjectIdAndTags** objects	Parameter for matching resources by enterprise project or tag.
status	String	Metric alarm status. The value can be health (alarming), unhealthy (triggered), or no_alarm_rule (no alarm rule is set). Enumeration values: • **health** • **unhealthy** • **no_alarm_rule**
event_status	String	Event alarm status. The value can be health (alarming), unhealthy (triggered), or no_alarm_rule (no alarm rule is set). Enumeration values: • **health** • **unhealthy** • **no_alarm_rule**
resource_statistics	**resource_statistics** object	Resource quantity statistics.

Parameter	Type	Description
resource_level	String	**dimension** indicates the sub-dimension, and **product** indicates the cloud product. Enumeration values: • **dimension** • **product**
product_names	String	Value of a cloud product when the resource level is cloud product. Generally, the value consists of the service namespace and the first-level dimension name of the service, for example, SYS.ECS,instance_id. Use semicolons (;) to separate multiple cloud products, for example, "SERVICE.BMS,instance_id;SYS.ECS,instance_id".
ep_resource_statistics	Array of **EpResourceStatistics** objects	Status of resources associated with each enterprise project

Table 6-202 ResourceGroupTagRelation

Parameter	Type	Description
key	String	TMS tag key specifications.

Parameter	Type	Description
operator	String	Tag operator, which indicates the relationship between the tag key and value. **include**: indicates include. **prefix**: indicates the prefix. **suffix**: indicates the suffix. **notInclude**: indicates not included. **equal**: indicates equal. If **operator** is **equal** and **value** is an empty string, all tag values of the key are matched. **all**: indicates all. Enumeration values: • **include** • **prefix** • **suffix** • **notInclude** • **equal** • **all**
value	String	TMS tag value specifications.

Table 6-203 Instance

Parameter	Type	Description
product_name	String	Cloud product name.
logical_operator	String	Logical operator. **ALL**: All conditions are matched. **ANY**: Any condition is matched. Enumeration values: • **ALL** • **ANY**
instance_names	Array of **ResourceName** objects	Parameter array for matching resources by resource name.

Table 6-204 ResourceName

Parameter	Type	Description
resource_name	String	Resource name condition value.
operator	String	Instance operator, which indicates the operation relationship between the actual resource name and the resource name condition value. **include**: indicates include. **prefix**: indicates the prefix. **suffix**: indicates the suffix. **notInclude**: indicates not included. **equal**: indicates equal. **all**: indicates all. Enumeration values: • **include** • **prefix** • **suffix** • **notInclude** • **equal** • **all**
resource_name_is_ignore_case	Boolean	The resource name is case-insensitive.

Table 6-205 CombRelation

Parameter	Type	Description
logical_operator	String	Logical operator. **ALL**: All conditions are matched. **ANY**: Any condition is matched. Enumeration values: • **ALL** • **ANY**
conditions	Array of **Condition** objects	Combined matching conditions for resource groups.

Table 6-206 Condition

Parameter	Type	Description
enterprise_project_id	String	Enterprise Project ID. **Regex Pattern:** ^((([a-z]|[0-9]){8}-([a-z]|[0-9]){4}-([a-z]|[0-9]){4}-([a-z]|[0-9]){4}-([a-z]|[0-9]){12})|0)$
instance_name	**ResourceName** object	Resource name.
tag	**ResourceGroupTagRelation** object	Tag matching rule.

Table 6-207 EnterpriseProjectIdAndTags

Parameter	Type	Description
enterprise_project_id	String	Enterprise Project ID. **Regex Pattern:** ^([a-z]|[A-Z]|[0-9]|_|-)+$
tag	**ResourceGroupTagRelation** object	Tag matching rule.

Table 6-208 resource_statistics

Parameter	Type	Description
unhealthy	Integer	Number of resources in the alarm **Value range:** 0-9999999
total	Integer	Total number of resources. **Value range:** 0-9999999
event_unhealthy	Integer	Number of triggered resources **Value range:** 0-9999999
namespaces	Integer	Resource Types **Value range:** 0-9999999

Table 6-209 EpResourceStatistics

Parameter	Type	Description
extend_relation_id	String	Enterprise project ID
unhealthy	Integer	Number of resources in the alarm **Value range:** 0-9999999
total	Integer	Total number of resources. **Value range:** 0-9999999
event_unhealthy	Integer	Number of triggered resources **Value range:** 0-9999999
namespaces	Integer	Resource Types **Value range:** 0-9999999

Status code: 400

Table 6-210 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 401

Table 6-211 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 403

Table 6-212 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 404

Table 6-213 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 500

Table 6-214 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Example Requests

Query details of a resource group.

```
/v2/{project_id}/resource-groups/{group_id}
```

Example Responses

Status code: 200

OK


```
{
  "group_name" : "band",
  "type" : "TAG",
  "tags" : [ {
    "key" : "Resource",
    "value" : "VPC"
  }, {
    "key" : "Usage",
    "value" : "Tmp"
  } ],
  "create_time" : "2006-01-02T15:04:05.000Z",
  "group_id" : "rg0123456789xxxx",
  "enterprise_project_id" : "0"
}
```

Status Codes

Status Code	Description
200	OK
400	Parameter verification failed.
401	Not authenticated.
403	Authentication failed.
404	Resource not found.
500	Internal system error.

Error Codes

See **Error Codes**.

6.8.5 Querying Resource Groups

Function

This API is used to query resource groups.

Debugging

You can debug this API through automatic authentication in **API Explorer** or use the SDK sample code generated by API Explorer.

URI

GET /v2/{project_id}/resource-groups

Table 6-215 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Tenant ID.

Table 6-216 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	ID of the enterprise project that a resource group belongs to. **Regex Pattern:** ^((([a-z]|[0-9]){8}-([a-z]|[0-9]){4}-([a-z]|[0-9]){4}-([a-z]|[0-9]){4}-([a-z]|[0-9]){12})|0)$
group_name	No	String	Resource group name. Fuzzy search is supported.
group_id	No	String	Resource group ID, which starts with **rg** and is followed by 22 characters, including letters and digits.
offset	No	Integer	Start position for pagination query, indicating the sequence number of the data record where the query starts. The default value is **0**. **Value range:** 0-10000
limit	No	Integer	Number of items on each page during pagination query. The value ranges from **1** to **100** (default). **Value range:** 1-100

Parameter	Mandatory	Type	Description
type	No	String	Method for adding resources to a resource group. The value can only be **EPS** (synchronizing resources from enterprise projects), **TAG** (dynamic tag matching), **Manual** (manually adding resources), COMB (automatically adding resources – matching by multiple criteria), or **NAME** (fuzzy matching by resource name). If this parameter is not specified, all resource groups are queried. Enumeration values: • **EPS** • **TAG** • **Manual** • **COMB** • **NAME**

Request Parameters

Table 6-217 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Tenant token.

Response Parameters

Status code: 200

Table 6-218 Response body parameters

Parameter	Type	Description
count	Integer	Total number of resource groups. **Value range:** 0-1000

Parameter	Type	Description
resource_groups	Array of **OneResourceGroupResp** objects	Resource group list.

Table 6-219 OneResourceGroupResp

Parameter	Type	Description
group_name	String	Resource group name. **Regex Pattern:** ^((([a-z]|[0-9]){8}-([a-z]|[0-9]){4}-([a-z]|[0-9]){4}-([a-z]|[0-9]){4}-([a-z]|[0-9]){12})|0)$
group_id	String	Resource group ID, which starts with **rg** and is followed by 22 characters, including letters and digits.
create_time	String	Time when a resource group was created.
enterprise_project_id	String	ID of the enterprise project that a resource group belongs to. **Regex Pattern:** ^((([a-z]|[0-9]){8}-([a-z]|[0-9]){4}-([a-z]|[0-9]){4}-([a-z]|[0-9]){4}-([a-z]|[0-9]){12})|0)$
type	String	Resource adding/matching mode. The value can only be EPS (matching enterprise projects), TAG (matching tags), NAME (matching instance names), COMB (combination matching), or Manual (manual adding). Enumeration values: • **EPS** • **TAG** • **NAME** • **COMB** • **Manual**

Parameter	Type	Description
status	String	Metric alarm status. The value can be health (alarming), unhealthy (triggered), or no_alarm_rule (no alarm rule is set). Enumeration values: • **health** • **unhealthy** • **no_alarm_rule**
event_status	String	Event alarm status. The value can be health (alarming), unhealthy (triggered), or no_alarm_rule (no alarm rule is set). Enumeration values: • **health** • **unhealthy** • **no_alarm_rule**
resource_statistics	**resource_statistics** object	Resource quantity statistics.
related_ep_ids	Array of strings	List of specified enterprise projects when the resource matching rule is enterprise project matching.
association_alarm_templates	Array of **AssociationAlarmTemplate** objects	List of associated alarm templates.

Table 6-220 resource_statistics

Parameter	Type	Description
unhealthy	Integer	Number of resources in the alarm **Value range:** 0-9999999
total	Integer	Total number of resources. **Value range:** 0-9999999
event_unhealthy	Integer	Number of triggered resources **Value range:** 0-9999999

Parameter	Type	Description
namespaces	Integer	Resource Types **Value range:** 0-9999999

Table 6-221 AssociationAlarmTemplate

Parameter	Type	Description
template_id	String	ID of an alarm template.
template_name	String	Alarm template name

Status code: 400

Table 6-222 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 401

Table 6-223 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 403

Table 6-224 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 500

Table 6-225 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Example Requests

Query resource groups.

```
/v2/{project_id}/resource-groups?offset=0&limit=100
```

Example Responses

Status code: 200

OK

```
{
  "resource_groups" : [ {
    "group_name" : "group1",
    "create_time" : "2006-01-02T15:04:05.000Z",
    "group_id" : "rg0123456789xxxx",
    "enterprise_project_id" : "0",
    "type" : "Manual"
  }, {
    "group_name" : "band",
    "type" : "EPS",
    "create_time" : "2006-01-02T15:04:05.000Z",
    "group_id" : "rg0123456789xxxx",
    "enterprise_project_id" : "d61d4705-5658-42f5-8e0c-70eb34d17b02"
  }, {
    "group_name" : "group2",
    "type" : "TAG",
    "create_time" : "2006-01-02T15:04:05.000Z",
    "group_id" : "rg0123456789xxxx",
    "enterprise_project_id" : "0"
  } ],
  "count" : 3
}
```


Status Codes

Status Code	Description
200	OK
400	Parameter verification failed.
401	Not authenticated.
403	Authentication failed.
500	Internal system error.

Error Codes

See **Error Codes**.

6.8.6 Asynchronously Associating a Resource Group with a Custom Alarm Template

Function

This API is used to submit an asynchronous task for batch associating a resource group with custom alarm templates. These tasks create or replace existing alarm rules. Each user can create up to 100 asynchronous tasks in the pending state. Each resource group allows only one pending task.

Debugging

You can debug this API through automatic authentication in **API Explorer** or use the SDK sample code generated by API Explorer.

URI

PUT /v2/{project_id}/resource-groups/{group_id}/alarm-templates/async-association

Table 6-226 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	**Definition** Tenant ID. **Constraints**: None **Value range**: Project ID, used to specify the project that an asset belongs to. You can query the assets of a project by project ID. You can obtain the project ID by calling an API or on the console. For details, see **Obtaining a Project ID**. The value must contain of 1 to 64 characters. **Default value**: None
group_id	Yes	String	Resource group ID, which starts with **rg** and is followed by 22 characters, including letters and digits. **Regex Pattern:** ^rg([a-z]|[A-Z]|[0-9]){22}$

Request Parameters

Table 6-227 Request header parameters

Parameter	Mandatory	Type	Description
Content-Type	No	String	**Definition** MIME type of the request body. **Constraints**: None **Value range**: The value can contain 1 to 64 characters. **Default value**: The default type is **application/json; charset=UTF-8**. **Default value:** application/json; charset=UTF-8
X-Auth-Token	No	String	**Definition** User token. **Constraints**: None **Value range**: The value can contain 1 to 16,384 characters. **Default value**: None

Table 6-228 Request body parameters

Parameter	Mandatory	Type	Description
template_ids	Yes	Array of strings	Alarm template IDs. If the ID list is empty, the alarm rules created using the alarm templates associated with the resource group will be deleted.
notification_enabled	Yes	Boolean	Whether to enable alarm notification. true: enabled; false: disabled.

Parameter	Mandatory	Type	Description
alarm_notifications	No	Array of **Notification** objects	Alarm notification list.
ok_notifications	No	Array of **Notification** objects	Alarm clearance notification list.
notification_begin_time	No	String	Time when the alarm notification was enabled.
notification_end_time	No	String	Time when the alarm notification was disabled.
effective_timezone	No	String	Time zone, for example, **GMT-08:00**, **GMT+08:00**, or **GMT+0:00**.
enterprise_project_id	No	String	Enterprise project ID
notification_manner	No	String	Notification mode, which can be **NOTIFICATION_GROUP** (notification groups), **TOPIC_SUBSCRIPTION** (topic subscriptions), or **NOTIFICATION_POLICY** (notification policies). Enumeration values: • **NOTIFICATION_GROUP** • **TOPIC_SUBSCRIPTION** • **NOTIFICATION_POLICY**
notification_policy_ids	No	Array of strings	Associated notification policy IDs.

Table 6-229 Notification

Parameter	Mandatory	Type	Description
type	Yes	String	Notification type. The value can be **notification** (SMN notifications), **contact** (account contacts), **contactGroup** (notification groups), or **autoscaling** (AS notifications). **autoscaling** is used only in AS and is not recommended. **groupwatch**, **ecsRecovery**, and **iecAction** are no longer used. Enumeration values: • **notification** • **autoscaling** • **groupwatch** • **ecsRecovery** • **contact** • **contactGroup** • **iecAction**
notification_list	Yes	Array of strings	List of objects to be notified if the alarm status changes. The value of **topicUrn** can be obtained from SMN. For details, see section "Querying Topics". If **type** is set to **notification**, the value of **notificationList** cannot be left blank. If **type** is set to **autoscaling**, the value of **notification_list** must be left blank. Note: If **alarm_action_enabled** is set to **true**, **alarm_actions**, **ok_actions**, or both of them must be specified. If both **alarm_actions** and **ok_actions** are specified, their **notification_list** values must be the same.

Response Parameters

Status code: 200

Table 6-230 Response body parameters

Parameter	Type	Description
group_id	String	Resource group ID, which starts with **rg** and is followed by 22 characters, including letters and digits.
template_ids	Array of strings	IDs of associated alarm templates.

Status code: 400

Table 6-231 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 401

Table 6-232 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 403

Table 6-233 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 404

Table 6-234 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 500

Table 6-235 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Example Requests

```
{
  "template_ids" : [ "at1628592157541dB1klWgY6", "at1628592157541dxcdfssfd" ],
  "notification_enabled" : false
}
```

Example Responses

Status code: 200

Response body returned after an asynchronous task for associating a resource group with alarm templates is delivered.

```
{
  "group_id" : "rg1619578505263QkW3b66yo",
  "template_ids" : [ "at1628592157541dB1klWgY6", "at1625452115254dB1kllll3" ]
}
```

Status Codes

Status Code	Description
200	Response body returned after an asynchronous task for associating a resource group with alarm templates is delivered.

Status Code	Description
400	Parameter verification failed.
401	Unauthenticated.
403	Authentication failed.
404	Resource not found.
500	Internal error.

Error Codes

See **Error Codes**.

6.9 Resources in a Resource Group

6.9.1 Batch Adding Resources to a Resource Group

Function

This API is used to batch add resources to a resource group whose **type** is **Manual**.

Debugging

You can debug this API through automatic authentication in **API Explorer** or use the SDK sample code generated by API Explorer.

URI

POST /v2/{project_id}/resource-groups/{group_id}/resources/batch-create

Table 6-236 Path Parameters

Parameter	Mandatory	Type	Description
group_id	Yes	String	Resource group ID, which starts with **rg** and is followed by 22 characters, including letters and digits.
project_id	Yes	String	Tenant ID.

Request Parameters

Table 6-237 Request header parameters

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

Table 6-238 Request body parameters

Parameter	Mandatory	Type	Description
resources	No	Array of **Resource** objects	When the resource adding mode is manual creation and the resource level is sub-dimension, only the information about the new resource needs to be transferred when the resource is added to the resource group.
product_resources	No	Array of **ProductResource** objects	If the resource adding mode is manual creation and the resource level is cloud product, information about both existing and new resources needs to be transferred when resources are added to a resource group.

Table 6-239 Resource

Parameter	Mandatory	Type	Description
namespace	Yes	String	Namespace of a service. For details about the namespace of each service, see **Namespace**.
dimensions	Yes	Array of **ResourceDimension** objects	Resource dimension information.

Table 6-240 ResourceDimension

Parameter	Mandatory	Type	Description
name	Yes	String	Dimension of a resource. For example, the dimension of an ECS can be **instance_id**. A maximum of four dimensions are supported. For the metric dimension of each resource, see **Service metric dimension**. **Regex Pattern:** ^([a-z]|[A-Z]){1}([a-z]|[A-Z]|[0-9]|_|-)*$
value	Yes	String	Value of a resource dimension. It is the instance ID, for example, **4270ff17-aba3-4138-89fa-820594c39755**. **Regex Pattern:** ^((([a-z]|[A-Z]|[0-9]|*|_|/|#|\(|\)){1}([a-z]|[A-Z]|[0-9]|_|-|\.|*|/|#|\(|\))*))$

Table 6-241 ProductResource

Parameter	Mandatory	Type	Description
product_name	Yes	String	Cloud product that the resource belongs to. Generally, the value format is *Service namespace,First-level dimension name of the service*, for example, **SYS.ECS,instance_id**.
namespace	Yes	String	Namespace of a service. For details about the namespace of each service, see **Namespace**. **Regex Pattern:** ^([a-z]|[A-Z]){1}([a-z]|[A-Z]|[0-9]|_)*\.([a-z]|[A-Z]){1}([a-z]|[A-Z]|[0-9]|_)*$
product_instances	Yes	Array of **ProductInstance** objects	Product instance details.

Table 6-242 ProductInstance

Parameter	Mandatory	Type	Description
first_dimension_name	Yes	String	First-level dimension of the resource. For example, the dimension of an ECS is **instance_id**. **Regex Pattern:** ^([a-z]|[A-Z]){1}([a-z]|[A-Z]|[0-9]|_|-){1,32}$
first_dimension_value	Yes	String	First-level dimension value of the resource, which is the resource ID, for example, **4270ff17-aba3-4138-89fa-820594c39755**. **Regex Pattern:** ^([a-z]|[A-Z]|[0-9]|*|_|/|#|\(|\)){1}([a-z]|[A-Z]|[0-9]|_|-|\.|/|#|\(|\))*$
resource_name	Yes	String	Resource name.

Response Parameters

Status code: 200

Table 6-243 Response body parameters

Parameter	Type	Description
succeed_count	Integer	Number of resources that were added. **Value range:** 0-1000

Status code: 400

Table 6-244 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 404

Table 6-245 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 500

Table 6-246 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Example Requests

Batch adding resources to a custom resource group.

```
{
  "resources" : [ {
    "namespace" : "SYS.ECS",
    "dimensions" : [ {
      "name" : "instace_id",
      "value" : "4270ff17-aba3-4138-89fa-820594c39755"
    } ]
  } ]
}
```

Example Responses

Status code: 200

Resources added.

```
{
  "succeed_count" : 4
}
```


Status Codes

Status Code	Description
200	Resources added.
400	Parameter verification failed.
404	Resource not found.
500	Internal system error.

Error Codes

See **Error Codes**.

6.9.2 Batch Deleting Resources from a Resource Group

Function

This API is used to batch delete resources from a resource group whose **type** is **Manual**.

Debugging

You can debug this API through automatic authentication in **API Explorer** or use the SDK sample code generated by API Explorer.

URI

POST /v2/{project_id}/resource-groups/{group_id}/resources/batch-delete

Table 6-247 Path Parameters

Parameter	Mandatory	Type	Description
group_id	Yes	String	Resource group ID, which starts with **rg** and is followed by 22 characters, including letters and digits.
project_id	Yes	String	Tenant ID.

Request Parameters

Table 6-248 Request header parameters

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

Table 6-249 Request body parameters

Parameter	Mandatory	Type	Description
resources	No	Array of **Resource** objects	When the resource adding mode is manual creation and the resource level is sub-dimension, only the information about the deleted resource needs to be transferred when the resource is deleted from the resource group.
product_resources	No	Array of **ProductResource** objects	When the resource adding mode is manual creation and the resource level is cloud product, only the information about the deleted resource needs to be transferred when the resource is deleted from the resource group.

Table 6-250 Resource

Parameter	Mandatory	Type	Description
namespace	Yes	String	Namespace of a service. For details about the namespace of each service, see **Namespace**.
dimensions	Yes	Array of **ResourceDimension** objects	Resource dimension information.

Table 6-251 ResourceDimension

Parameter	Mandatory	Type	Description
name	Yes	String	Dimension of a resource. For example, the dimension of an ECS can be **instance_id**. A maximum of four dimensions are supported. For the metric dimension of each resource, see **Service metric dimension**. **Regex Pattern:** ^([a-z]|[A-Z]){1}([a-z]|[A-Z]|[0-9]|_|-)*$
value	Yes	String	Value of a resource dimension. It is the instance ID, for example, **4270ff17-aba3-4138-89fa-820594c39755**. **Regex Pattern:** ^((([a-z]|[A-Z]|[0-9]|*|_|/|#|\(|\)){1}([a-z]|[A-Z]|[0-9]|_|-|\.|*|/|#|\(|\))*))$

Table 6-252 ProductResource

Parameter	Mandatory	Type	Description
product_name	Yes	String	Cloud product that the resource belongs to. Generally, the value format is *Service namespace,First-level dimension name of the service*, for example, **SYS.ECS,instance_id**.
namespace	Yes	String	Namespace of a service. For details about the namespace of each service, see **Namespace**. **Regex Pattern:** ^([a-z]|[A-Z]){1}([a-z]|[A-Z]|[0-9]|_)*\.([a-z]|[A-Z]){1}([a-z]|[A-Z]|[0-9]|_)*$
product_instances	Yes	Array of **ProductInstance** objects	Product instance details.

Table 6-253 ProductInstance

Parameter	Mandatory	Type	Description
first_dimension_name	Yes	String	First-level dimension of the resource. For example, the dimension of an ECS is **instance_id**. **Regex Pattern:** ^([a-z]|[A-Z]){1}([a-z]|[A-Z]|[0-9]|_|-){1,32}$
first_dimension_value	Yes	String	First-level dimension value of the resource, which is the resource ID, for example, **4270ff17-aba3-4138-89fa-820594c39755**. **Regex Pattern:** ^([a-z]|[A-Z]|[0-9]|*|_|/|#|\(|\)){1}([a-z]|[A-Z]|[0-9]|_|-|\.|/|#|\(|\))*$
resource_name	Yes	String	Resource name.

Response Parameters

Status code: 200

Table 6-254 Response body parameters

Parameter	Type	Description
succeed_count	Integer	Number of resources that were successfully deleted. **Value range:** 0-1000

Status code: 400

Table 6-255 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.

Parameter	Type	Description
request_id	String	Request ID.

Status code: 404

Table 6-256 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 500

Table 6-257 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Example Requests

Batch delete resources from a custom resource group.

```
{
  "resources" : [ {
    "namespace" : "SYS.ECS",
    "dimensions" : [ {
      "name" : "instace_id",
      "value" : "4270ff17-aba3-4138-89fa-820594c39755"
    } ]
  } ]
}
```

Example Responses

Status code: 200

Resources deleted.

```
{
  "succeed_count" : 4
}
```

Status Codes

Status Code	Description
200	Resources deleted.
400	Parameter verification failed.
404	Resource not found.
500	Internal system error.

Error Codes

See **Error Codes**.

6.9.3 Querying Resources of a Specified Dimension and a Specified Service Type in a Resource Group

Function

This API is used to query resources of a specified dimension for a specified resource type in a resource group.

Debugging

You can debug this API through automatic authentication in **API Explorer** or use the SDK sample code generated by API Explorer.

URI

GET /v2/{project_id}/resource-groups/{group_id}/services/{service}/resources

Table 6-258 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Tenant ID.
group_id	Yes	String	Resource group ID, which starts with **rg** and is followed by 22 characters, including letters and digits.
service	Yes	String	Service type, for example, **SYS.ECS**.

Table 6-259 Query Parameters

Parameter	Mandatory	Type	Description
dim_name	No	String	Resource dimension name. Multiple dimensions are separated with commas (,) in alphabetical order.
limit	No	String	Number of items on each page during pagination query. The value ranges from **1** to **100** (default).
offset	No	Integer	Start position for pagination query, indicating the sequence number of the data record where the query starts. The default value is **0**. **Value range:** 0-10000
status	No	String	Resource health status. The value can only be **health**, **unhealthy**, or **no_alarm_rule**. **health**: An alarm rule has been created for the resource and there is no alarm triggered. **unhealthy**: An alarm rule has been created for the resource and there are alarms triggered. **no_alarm_rule**: No alarm rule has been created for the resource. Enumeration values: • **health** • **unhealthy** • **no_alarm_rule**
dim_value	No	String	Resource dimension value. Fuzzy match is not supported. If a resource has multiple dimensions, you can specify one of them.
tag	No	String	Resource tag information. The format is *"[key]":"[value]"*, for example: **"ssss":"1111"**.
extend_relation_id	No	String	Enterprise project ID.

Parameter	Mandatory	Type	Description
product_name	No	String	Cloud product of the resource group. Generally, the value format is *Service namespace,First-level dimension name of the service*, for example, **SYS.ECS,instance_id**.
resource_name	No	String	Resource name. **Regex Pattern:** ^$\|^([\u4E00-\u9FFF]\|[a-z]\|[A-Z]\|[0-9]\|_\|-\|\\.\|)+$
event_status	No	String	Resource health status. The value can only be **health**, **unhealthy**, or **no_alarm_rule**. **health**: An event alarm rule has been created for the resource and there is no alarm triggered. **unhealthy**: An event alarm rule has been created for the resource and there are alarms triggered. **no_alarm_rule**: No event alarm rule has been created for the resource. Enumeration values: • **health** • **unhealthy** • **no_alarm_rule**

Request Parameters

Table 6-260 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Tenant token.

Response Parameters

Status code: 200

Table 6-261 Response body parameters

Parameter	Type	Description
count	Integer	Total number of resources. **Value range:** 0-10000
resources	Array of **GetResourceGroupResources** objects	Resources in a resource group.

Table 6-262 GetResourceGroupResources

Parameter	Type	Description
status	String	Metric alarm status. The value can be health (alarming), unhealthy (triggered), or no_alarm_rule (no alarm rule is set). Enumeration values: • **health** • **unhealthy** • **no_alarm_rule**
dimensions	Array of **ResourceDimension** objects	Resource dimension information.
tags	String	Resource tag information. The value is a JSON character string in the format of *key/value*, for example, **"{"sss":"aaa"}"**.
enterprise_project_id	String	Enterprise Project ID.
event_status	String	Event alarm status. The value can be health (alarming), unhealthy (triggered), or no_alarm_rule (no alarm rule is set). Enumeration values: • **health** • **unhealthy** • **no_alarm_rule**
resource_name	String	Resource name

Table 6-263 ResourceDimension

Parameter	Type	Description
name	String	Dimension of a resource. For example, the dimension of an ECS can be **instance_id**. A maximum of four dimensions are supported. For the metric dimension of each resource, see **Service metric dimension**. **Regex Pattern:** ^([a-z]|[A-Z]){1}([a-z]|[A-Z]|[0-9]|_|-)*$
value	String	Value of a resource dimension. It is the instance ID, for example, **4270ff17-aba3-4138-89fa-820594c39755**. **Regex Pattern:** ^((([a-z]|[A-Z]|[0-9]|*|_|/|#|\(|\)){1}([a-z]|[A-Z]|[0-9]|_|-|\.|*|/|#|\(|\))*))$

Status code: 400

Table 6-264 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 401

Table 6-265 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 403

Table 6-266 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 404

Table 6-267 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 500

Table 6-268 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Example Requests

Query resources of a specified dimension for a specified resource type in a resource group.

```
'/v2/{project_id}/resource-groups/{group_id}/services/{service}/resources'
```

Example Responses

Status code: 200

OK

```
{
  "count" : 1000,
```

```
 "resources" : [ {
   "status" : "health",
   "dimensions" : [ {
     "name" : "instance_id",
     "value" : "4270ff17-aba3-4138-89fa-820594c39755"
   } ]
 } ]
}
```

Status Codes

Status Code	Description
200	OK
400	Parameter verification failed.
401	Not authenticated.
403	Authentication failed.
404	Resource not found.
500	Internal system error.

Error Codes

See **Error Codes**.

6.10 One-Click Monitoring

6.10.1 Enabling One-Click Monitoring

Function

This API is used to enable one-click monitoring.

Debugging

You can debug this API through automatic authentication in **API Explorer** or use the SDK sample code generated by API Explorer.

URI

POST /v2/{project_id}/one-click-alarms

Table 6-269 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	**Definition** Tenant ID. **Constraints**: None **Value range**: Project ID, used to specify the project that an asset belongs to. You can query the assets of a project by project ID. You can obtain the project ID by calling an API or on the console. For details, see **Obtaining a Project ID**. The value must contain of 1 to 64 characters. **Default value**: None

Request Parameters

Table 6-270 Request header parameters

Parameter	Mandatory	Type	Description
Content-Type	No	String	**Definition** MIME type of the request body. **Constraints**: None **Value range**: The value can contain 1 to 64 characters. **Default value**: The default type is **application/json; charset=UTF-8**. **Default value:** application/json; charset=UTF-8

Parameter	Mandatory	Type	Description
X-Auth-Token	No	String	**Definition** User token. **Constraints**: None **Value range**: The value can contain 1 to 16,384 characters. **Default value**: None

Table 6-271 Request body parameters

Parameter	Mandatory	Type	Description
one_click_alarm_id	Yes	String	One-click monitoring ID for a service.
dimension_names	Yes	**DimensionNames** object	Dimensions in metric and event alarm rules that have one-click monitoring enabled. One-click monitoring must be enabled for at least one type of alarm rules.
notification_enabled	Yes	Boolean	Whether to enable alarm notification. true: enabled; false: disabled.
alarm_notifications	No	Array of **Notification** objects	Action to be triggered by the alarm.
ok_notifications	No	Array of **Notification** objects	Action to be triggered after an alarm is cleared.
notification_begin_time	No	String	Time when the alarm notification was enabled.
notification_end_time	No	String	Time when the alarm notification was disabled.
effective_timezone	No	String	Time zone, for example, **GMT-08:00**, **GMT+08:00**, or **GMT+0:00**.

Parameter	Mandatory	Type	Description
notification_manner	No	String	Notification mode, which can be **NOTIFICATION_GROUP** (notification groups), **TOPIC_SUBSCRIPTION** (topic subscriptions), or **NOTIFICATION_POLICY** (notification policies). Enumeration values: • **NOTIFICATION_GROUP** • **TOPIC_SUBSCRIPTION** • **NOTIFICATION_POLICY**
notification_policy_ids	No	Array of strings	Associated notification policy IDs.
is_reset	No	Boolean	Whether to reset the default policy of one-click monitoring. **Default value:** true
one_click_update_alarms	No	Array of **one_click_update_alarms** objects	Parameters required when alarm policies and notifications need to be modified at the same time when one-click monitoring is enabled. Currently, you can only modify the notification policies.

Table 6-272 DimensionNames

Parameter	Mandatory	Type	Description
metric	Yes	Array of strings	Dimensions in metric alarm rules that have one-click monitoring enabled. One-click monitoring are disabled by default for unspecified dimensions.
event	Yes	Array of strings	Dimensions in event alarm rules that have one-click monitoring enabled. One-click monitoring are disabled by default for unspecified dimensions. "" indicates enable one-click monitoring for all dimensions.

Table 6-273 Notification

Parameter	Mandatory	Type	Description
type	Yes	String	Notification type. The value can be **notification** (SMN notifications), **contact** (account contacts), **contactGroup** (notification groups), or **autoscaling** (AS notifications). **autoscaling** is used only in AS and is not recommended. **groupwatch**, **ecsRecovery**, and **iecAction** are no longer used. Enumeration values: • **notification** • **autoscaling** • **groupwatch** • **ecsRecovery** • **contact** • **contactGroup** • **iecAction**
notification_list	Yes	Array of strings	List of objects to be notified if the alarm status changes. The value of **topicUrn** can be obtained from SMN. For details, see section "Querying Topics". If **type** is set to **notification**, the value of **notificationList** cannot be left blank. If **type** is set to **autoscaling**, the value of **notification_list** must be left blank. Note: If **alarm_action_enabled** is set to **true**, **alarm_actions**, **ok_actions**, or both of them must be specified. If both **alarm_actions** and **ok_actions** are specified, their **notification_list** values must be the same.

Table 6-274 one_click_update_alarms

Parameter	Mandatory	Type	Description
alarm_id	No	String	ID of an alarm rule, which starts with **al** and is followed by 22 characters, including letters and digits.
name	No	String	Name of an alarm rule. The name can contain 1 to 128 characters, including only letters, digits, underscores (_), and hyphens (-).
description	No	String	Alarm rule description. The description can contain 0 to 256 characters.
namespace	No	String	Namespace of a service. For details about the namespace of each service, see **Namespace**.
policies	No	Array of **Policy** objects	Alarm policies.
resources	No	Array<Array< **Dimension**>>	Resource list. Associated resources can be obtained by calling the API for querying resources in an alarm rule.

Parameter	Mandatory	Type	Description
type	No	String	**Definition**: Alarm rule type. **Constraints**: None **Value range**: Enumerated value. **ALL_INSTANCE** indicates alarm rules for metrics of all resources. **RESOURCE_GROUP** indicates alarm rules for metrics of resources in a resource group. **MULTI_INSTANCE** indicates alarm rules for metrics of specified resources. **EVENT.SYS** indicates alarm rules for system events. **EVENT.CUSTOM** indicates alarm rules for custom events. **DNSHealthCheck** indicates alarm rules for health checks. **Default value**: None Enumeration values: • **EVENT.SYS** • **EVENT.CUSTOM** • **DNSHealthCheck** • **RESOURCE_GROUP** • **MULTI_INSTANCE** • **ALL_INSTANCE**
enabled	No	Boolean	Whether to enable the alarm rule. true: enabled; false: disabled.
notification_enabled	No	Boolean	Whether to enable alarm notification. true: enabled; false: disabled.
alarm_notifications	No	Array of **Notification** objects	Action to be triggered by the alarm.
ok_notifications	No	Array of **Notification** objects	Action to be triggered after an alarm is cleared.

Parameter	Mandatory	Type	Description
notification_begin_time	No	String	Time when the alarm notification was enabled.
notification_end_time	No	String	Time when the alarm notification was disabled.
notification_manner	No	String	Notification method. The value can be **NOTIFICATION_POLICY**, **NOTIFICATION_GROUP**, or **TOPIC_SUBSCRIPTION**. Enumeration values: • **NOTIFICATION_POLICY** • **NOTIFICATION_GROUP** • **TOPIC_SUBSCRIPTION**
notification_policy_ids	No	Array of strings	Associated notification policy IDs.

Table 6-275 Policy

Parameter	Mandatory	Type	Description
metric_name	Yes	String	Metric name of a resource. The name must start with a letter and contain only digits, letters, and underscores. The length ranges from 1 to 64 characters. For example, **cpu_util** of an ECS indicates the CPU usage of the ECS. **mongo001_command_ps** in DDS indicates the command execution frequency. For details about the metric name of each service, see **Service metric name**.

Parameter	Mandatory	Type	Description
period	Yes	Integer	Monitoring period of a metric, in seconds. The default value is **0**. For an event alarm, set this parameter to **0**. **1** indicates the original rollup period of a metric. For example, if the original rollup period of an RDS metric is 60s, its data point is calculated every 60 seconds. For details about the original rollup period of each cloud service metric, see **Services Interconnected with Cloud Eye**. **300** indicates that the metric rollup period is 5 minutes. **Value range:** 0-86400 Enumeration values: • **0** • **1** • **300** • **1200** • **3600** • **14400** • **86400**
filter	Yes	String	Aggregation mode. average: average value; variance: variance; min: minimum value; max: maximum value; sum: sum; tp99: 99 percentile; tp95: 95 percentile; tp90: 90 percentile

Parameter	Mandatory	Type	Description
comparison_operator	Yes	String	Threshold symbol. The value can be **>**, **<**, **>=**, **<=**, **=**, **!=**, **cycle_decrease**, **cycle_increase**, or **cycle_wave**. **cycle_decrease** indicates the decrease compared with the last period, **cycle_increase** indicates the increase compared with the last period, and **cycle_wave** indicates the increase or decrease compared with the last period. All of them can be used in alarm rules for metrics. **>**, **<**, **>=**, **<=**, **=**, and **!=** can be used for alarm rules for events.
value	No	Number	Alarm threshold If there is only one threshold, **value** and **alarm_level** are used in pairs. If there are both **hierarchical_value** and **value**, **hierarchical_value** is used. For detailed thresholds, see the value range of each metric in the appendix. For example, you can set ECS **cpu_util** to **80**. For detailed thresholds, see the value range of each metric in the appendix. For example, you can set ECS **cpu_util** to **80** in **Services Interconnected with Cloud Eye**.
hierarchical_value	No	**HierarchicalValue** object	Multi-level alarm threshold. If there are both **hierarchical_value** and **value**, **hierarchical_value** prevails. When you create or modify an alarm rule, you can set only one threshold in the following scenarios: 1. The alarm type is **Metric** and the alarm policy is **Trigger an alarm when all policies are met**. 2. The alarm type is **Event**.

Parameter	Mandatory	Type	Description
unit	No	String	Data unit.
count	Yes	Integer	Number of consecutive alarm triggering times. For event alarms, the value ranges from **1** to **180**. For metric and website alarms, the value can be **1**, **2**, **3**, **4**, **5**, **10**, **15**, **30**, **60**, **90**, **120**, or **180**.
suppress_duration	No	Integer	Alarm suppression time, in seconds. This parameter corresponds to the last field in the alarm policy when an alarm rule is created on the Cloud Eye console. This field is used to avoid frequent alarms. **0** indicates that the alarm is not suppressed and alarms are generated as long as the conditions are met. **300** indicates that an alarm is generated every 5 minutes as long as the alarm triggering conditions are met. **Value range:** 0-86400 Enumeration values: • **0** • **300** • **600** • **900** • **1800** • **3600** • **10800** • **21600** • **43200** • **86400**
level	No	Integer	Alarm severity, which can be **1** (critical), ** 2** (major), **3** (minor), or **4** (informational). The default value is **2**.

Parameter	Mandatory	Type	Description
namespace	No	String	**namespace** and **dimension_name** need to be specified for product-level rules. For details about the namespace of each service, see **Service namespace**. **Regex Pattern:** ^((([a-z]|[A-Z]){1}([a-z]|[A-Z]|[0-9]|_)*\.([a-z]|[A-Z]){1}([a-z]|[A-Z]|[0-9]|_)*)|)$
dimension_name	No	String	The namespace and dimension_name parameters are added to the product-level rule to specify the policy to which the product belongs. Currently, a maximum of four dimensions are supported. For details about the metric dimension name of each service resource, see [Service dimension name](ces_03_0059.xml). Example: instance_id in the single-dimension scenario; instance_id,disk in the multi-dimension scenario **Regex Pattern:** ^(([a-z]|[A-Z]){1}([a-z]|[A-Z]|[0-9]|_|-|\.){0,31}(,([a-z]|[A-Z]){1}([a-z]|[A-Z]|[0-9]|_|-|\.){0,31}){0,3}|)$

Table 6-276 HierarchicalValue

Parameter	Mandatory	Type	Description
critical	No	Double	Threshold for critical alarms. **Value range:** -1.7976931348623156E108-1.7976931348623156E108
major	No	Double	Threshold for major alarms. **Value range:** -1.7976931348623156E108-1.7976931348623156E108

Parameter	Mandatory	Type	Description
minor	No	Double	Threshold for minor alarms. **Value range:** -1.7976931348623156E108-1.7976931348623156E108
info	No	Double	Threshold for informational alarms. **Value range:** -1.7976931348623156E108-1.7976931348623156E108

Table 6-277 Dimension

Parameter	Mandatory	Type	Description
name	Yes	String	Dimension of a resource. For example, the dimension of an ECS can be **instance_id**. A maximum of four dimensions are supported. For the metric dimension of each resource, see **Service metric dimension**. **Regex Pattern:** ^([a-z]|[A-Z]){1}([a-z]|[A-Z]|[0-9]|_|-)*$
value	No	String	Value of a resource dimension, which is the resource ID, for example, **4270ff17-aba3-4138-89fa-820594c39755**. **Regex Pattern:** ^((([a-z]|[A-Z]|[0-9]|*|_|/|#|\(|\)){1}([a-z]|[A-Z]|[0-9]|_|-|\.|*|/|#|\(|\))*))$

Response Parameters

Status code: 201

Table 6-278 Response body parameters

Parameter	Type	Description
one_click_alarm_id	String	One-click monitoring ID for a service.

Status code: 400

Table 6-279 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 401

Table 6-280 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 403

Table 6-281 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 500

Table 6-282 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.

Parameter	Type	Description
request_id	String	Request ID.

Example Requests

/v2/{project_id}/one-click-alarms

```
{
  "one_click_alarm_id" : "o123456789012345678901 2",
  "dimension_names" : {
    "metric" : [ "disk", "instance_id" ],
    "event" : [ "resource_id" ]
  },
  "notification_enabled" : true,
  "alarm_notifications" : [ {
    "type" : "notification",
    "notification_list" : [ "urn:smn:123" ]
  } ],
  "ok_notifications" : [ {
    "type" : "notification",
    "notification_list" : [ "urn:smn:123" ]
  } ],
  "notification_begin_time" : "00:00",
  "notification_end_time" : "23:59",
  "notification_manner" : "NOTIFICATION_POLICY",
  "notification_policy_ids" : [ "np15563156337845e8A2Wv63" ]
}
```

Example Responses

Status code: 201

Created

```
{
  "one_click_alarm_id" : "o123456789012345678901 2"
}
```

Status Codes

Status Code	Description
201	Created
400	Parameter verification failed.
401	Not authenticated.
403	Authentication failed.
500	Internal system error.

Error Codes

See **Error Codes**.

6.10.2 Querying Services and Resources That Support One-Click Monitoring

Function

This API is used to query services and resources that support one-click monitoring.

Debugging

You can debug this API through automatic authentication in **API Explorer** or use the SDK sample code generated by API Explorer.

URI

GET /v2/{project_id}/one-click-alarms

Table 6-283 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	**Definition** Tenant ID. **Constraints**: None **Value range**: Project ID, used to specify the project that an asset belongs to. You can query the assets of a project by project ID. You can obtain the project ID by calling an API or on the console. For details, see **Obtaining a Project ID**. The value must contain of 1 to 64 characters. **Default value**: None

Request Parameters

Table 6-284 Request header parameters

Parameter	Mandatory	Type	Description
Content-Type	No	String	**Definition** MIME type of the request body. **Constraints**: None **Value range**: The value can contain 1 to 64 characters. **Default value**: The default type is **application/json; charset=UTF-8**. **Default value:** application/json; charset=UTF-8
X-Auth-Token	No	String	**Definition** User token. **Constraints**: None **Value range**: The value can contain 1 to 16,384 characters. **Default value**: None

Response Parameters

Status code: 200

Table 6-285 Response body parameters

Parameter	Type	Description
one_click_alarms	Array of **one_click_alarms** objects	Services and resources that support one-click monitoring.

Table 6-286 one_click_alarms

Parameter	Type	Description
one_click_alarm_id	String	One-click monitoring ID for a service.
namespace	String	Namespace of a service. For details about the namespace of each service, see **Namespace**.
description	String	Supplementary information about one-click monitoring. The description can contain 0 to 256 characters and is left blank by default.
enabled	Boolean	Whether to enable one-click alarm reporting. true: enabled; false: disabled.

Status code: 400

Table 6-287 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 401

Table 6-288 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 403

Table 6-289 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 500

Table 6-290 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Example Requests

None

Example Responses

Status code: 200

OK

```
{
  "one_click_alarms" : [ {
    "one_click_alarm_id" : "o1234567890123456789012",
    "namespace" : "SYS.ECS",
    "description" : "hello world",
    "enabled" : true
  } ]
}
```

Status Codes

Status Code	Description
200	OK
400	Parameter verification failed.
401	Not authenticated.

Status Code	Description
403	Authentication failed.
500	Internal system error.

Error Codes

See **Error Codes**.

6.10.3 Querying Alarm Rules of a Service in One-Click Monitoring

Function

This API is used to query alarm rules of a service in one-click monitoring.

Debugging

You can debug this API through automatic authentication in **API Explorer** or use the SDK sample code generated by API Explorer.

URI

GET /v2/{project_id}/one-click-alarms/{one_click_alarm_id}/alarms

Table 6-291 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	**Definition** Tenant ID. **Constraints**: None **Value range**: Project ID, used to specify the project that an asset belongs to. You can query the assets of a project by project ID. You can obtain the project ID by calling an API or on the console. For details, see **Obtaining a Project ID**. The value must contain of 1 to 64 characters. **Default value**: None

Parameter	Mandatory	Type	Description
one_click_alarm_id	Yes	String	One-click monitoring ID for a service.

Request Parameters

Table 6-292 Request header parameters

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	**Definition** MIME type of the request body. **Constraints**: None **Value range**: The value can contain 1 to 64 characters. **Default value**: The default type is **application/json; charset=UTF-8**. **Default value:** application/json; charset=UTF-8
X-Auth-Token	Yes	String	**Definition** User token. **Constraints**: None **Value range**: The value can contain 1 to 16,384 characters. **Default value**: None

Response Parameters

Status code: 200

Table 6-293 Response body parameters

Parameter	Type	Description
alarms	Array of **alarms** objects	Alarm rule list.

Table 6-294 alarms

Parameter	Type	Description
alarm_id	String	ID of an alarm rule, which starts with **al** and is followed by 22 characters, including letters and digits.
name	String	Name of an alarm rule. The name can contain 1 to 128 characters, including only letters, digits, underscores (_), and hyphens (-).
description	String	Alarm rule description. The description can contain 0 to 256 characters.
namespace	String	Namespace of a service. For details about the namespace of each service, see **Namespace**.
policies	Array of **OneClickAlarmPolicy** objects	Alarm policies.
resources	Array of **ResourcesInListResp** objects	Resource list. Associated resources can be obtained by calling the API for querying resources in an alarm rule.

Parameter	Type	Description
type	String	**Definition**: Alarm rule type. **Constraints**: None **Value range**: Enumerated value. **ALL_INSTANCE** indicates alarm rules for metrics of all resources. **RESOURCE_GROUP** indicates alarm rules for metrics of resources in a resource group. **MULTI_INSTANCE** indicates alarm rules for metrics of specified resources. **EVENT.SYS** indicates alarm rules for system events. **EVENT.CUSTOM** indicates alarm rules for custom events. **DNSHealthCheck** indicates alarm rules for health checks. **Default value**: None Enumeration values: • **EVENT.SYS** • **EVENT.CUSTOM** • **DNSHealthCheck** • **RESOURCE_GROUP** • **MULTI_INSTANCE** • **ALL_INSTANCE**
enabled	Boolean	Whether to enable the alarm rule. true: enabled; false: disabled.
notification_enabled	Boolean	Whether to enable alarm notification. true: enabled; false: disabled.
alarm_notifications	Array of **Notification** objects	Action to be triggered by the alarm.
ok_notifications	Array of **Notification** objects	Action to be triggered after an alarm is cleared.
notification_begin_time	String	Time when the alarm notification was enabled.
notification_end_time	String	Time when the alarm notification was disabled.

Parameter	Type	Description
effective_timezone	String	Time zone, for example, **GMT-08:00**, **GMT+08:00**, or **GMT+0:00**.
notification_manner	String	Notification mode, which can be **NOTIFICATION_GROUP** (notification groups), **TOPIC_SUBSCRIPTION** (topic subscriptions), or **NOTIFICATION_POLICY** (notification policies). Enumeration values: • **NOTIFICATION_GROUP** • **TOPIC_SUBSCRIPTION** • **NOTIFICATION_POLICY**
notification_policy_ids	Array of strings	Associated notification policy IDs.

Table 6-295 OneClickAlarmPolicy

Parameter	Type	Description
alarm_policy_id	String	Alarm policy ID.
metric_name	String	Metric name of a resource. The name must start with a letter and contain only digits, letters, and underscores. The length ranges from 1 to 64 characters. For example, **cpu_util** of an ECS indicates the CPU usage of the ECS. **mongo001_command_ps** in DDS indicates the command execution frequency. For details about the metric name of each service, see **Service metric name**.

Parameter	Type	Description
period	Integer	Period for determining whether to generate an alarm, in seconds. The value can be **1**, **300**, **1200**, **3600**, **14400**, or **86400**. Note: If you set **period** to **1**, Cloud Eye uses raw data to determine whether to trigger an alarm. You can set this parameter to **0** when you set **alarm_type** to **EVENT.SYS** or **EVENT.CUSTOM**. Enumeration values: • **0** • **1** • **300** • **1200** • **3600** • **14400** • **86400**
filter	String	Aggregation mode. average: average value; variance: variance; min: minimum value; max: maximum value; sum: sum; tp99: 99 percentile; tp95: 95 percentile; tp90: 90 percentile
comparison_operator	String	Threshold symbol. The value can be **>**, **<**, **>=**, **<=**, **=**, **!=**, **cycle_decrease**, **cycle_increase**, or **cycle_wave**. **cycle_decrease** indicates the decrease compared with the last period, **cycle_increase** indicates the increase compared with the last period, and **cycle_wave** indicates the increase or decrease compared with the last period. All of them can be used in alarm rules for metrics. **>**, **<**, **>=**, **<=**, **=**, and **!=** can be used for alarm rules for events.

Parameter	Type	Description
value	Number	Alarm threshold If there is only one threshold, **value** and **alarm_level** are used in pairs. If there are both **hierarchical_value** and **value**, **hierarchical_value** is used. For detailed thresholds, see the value range of each metric in the appendix. For example, you can set ECS **cpu_util** to **80**. For detailed thresholds, see the value range of each metric in the appendix. For example, you can set ECS **cpu_util** to **80** in **Services Interconnected with Cloud Eye**.
hierarchical_value	**HierarchicalValue** object	Multi-level alarm threshold. If there are both **hierarchical_value** and **value**, **hierarchical_value** prevails. When you create or modify an alarm rule, you can set only one threshold in the following scenarios: 1. The alarm type is **Metric** and the alarm policy is **Trigger an alarm when all policies are met**. 2. The alarm type is **Event**.
unit	String	Data unit.
count	Integer	Number of consecutive alarm triggering times. For event alarms, the value ranges from **1** to **180**. For metric and website alarms, the value can be **1**, **2**, **3**, **4**, **5**, **10**, **15**, **30**, **60**, **90**, **120**, or **180**.

Parameter	Type	Description
suppress_duration	Integer	Interval for triggering alarms. The value can be **0**, **300**, **600**, **900**, **1800**, **3600**, **10800**, **21600**, **43200**, or **86400**. **0**: Cloud Eye triggers the alarm only once. **300**: Cloud Eye triggers an alarm every 5 minutes. **600**: Cloud Eye triggers an alarm every 10 minutes. **900**: Cloud Eye triggers an alarm every 15 minutes. **1800**: Cloud Eye triggers an alarm every 30 minutes. **3600**: Cloud Eye triggers an alarm every hour. **10800**: Cloud Eye triggers an alarm every 3 hours. **21600**: Cloud Eye triggers an alarm every 6 hour. **43200**: Cloud Eye triggers an alarm every 12 hours. **86400**: Cloud Eye triggers an alarm every day. Enumeration values: • **0** • **300** • **600** • **900** • **1800** • **3600** • **10800** • **21600** • **43200** • **86400**
level	Integer	Alarm severity, which can be **1** (critical), ** 2** (major), **3** (minor), or **4** (informational). The default value is **2**.
enabled	Boolean	Whether to enable one-click alarm reporting. true: enabled; false: disabled.
selected_unit	String	The unit you selected, which is used for subsequent metric data display and calculation.

Table 6-296 HierarchicalValue

Parameter	Type	Description
critical	Double	Threshold for critical alarms. **Value range:** -1.7976931348623156E108-1.7976931348623156E108
major	Double	Threshold for major alarms. **Value range:** -1.7976931348623156E108-1.7976931348623156E108
minor	Double	Threshold for minor alarms. **Value range:** -1.7976931348623156E108-1.7976931348623156E108
info	Double	Threshold for informational alarms. **Value range:** -1.7976931348623156E108-1.7976931348623156E108

Table 6-297 ResourcesInListResp

Parameter	Type	Description
resource_group_id	String	Resource group ID. This parameter is available when the monitoring scope is **Resource groups**. **Regex Pattern:** ^rg([a-z]|[A-Z]|[0-9]){22}$
resource_group_name	String	Resource group name. This parameter is available when the monitoring scope is **Resource groups**.
dimensions	Array of **MetricDimension** objects	Dimension information.

Table 6-298 MetricDimension

Parameter	Type	Description
name	String	Metric dimension name. **Regex Pattern:** ^([a-z]|[A-Z]){1}([a-z]|[A-Z]|[0-9]|_|-){1,32}$
value	String	Metric dimension value. **Regex Pattern:** ^((([a-z]|[A-Z]|[0-9]){1}([a-z]|[A-Z]|[0-9]|_|-)*)|){0,256}$

Table 6-299 Notification

Parameter	Type	Description
type	String	Notification type. The value can be **notification** (SMN notifications), **contact** (account contacts), **contactGroup** (notification groups), or **autoscaling** (AS notifications). **autoscaling** is used only in AS and is not recommended. **groupwatch**, **ecsRecovery**, and **iecAction** are no longer used. Enumeration values: • **notification** • **autoscaling** • **groupwatch** • **ecsRecovery** • **contact** • **contactGroup** • **iecAction**
notification_list	Array of strings	List of objects to be notified if the alarm status changes. The value of **topicUrn** can be obtained from SMN. For details, see section "Querying Topics". If **type** is set to **notification**, the value of **notificationList** cannot be left blank. If **type** is set to **autoscaling**, the value of **notification_list** must be left blank. Note: If **alarm_action_enabled** is set to **true**, **alarm_actions**, **ok_actions**, or both of them must be specified. If both **alarm_actions** and **ok_actions** are specified, their **notification_list** values must be the same.

Status code: 400

Table 6-300 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 401

Table 6-301 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 403

Table 6-302 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 500

Table 6-303 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.

Parameter	Type	Description
request_id	String	Request ID.

Example Requests

None

Example Responses

Status code: 200

OK


```
{
  "alarms" : [ {
    "alarm_id" : "al123232232341232132",
    "name" : "alarm1",
    "description" : "hello world",
    "namespace" : "SYS.ECS",
    "policies" : [ {
      "alarm_policy_id" : "alxdxxxdsw12321321",
      "metric_name" : "cpu_util",
      "period" : 0,
      "filter" : "max",
      "comparison_operator" : "",
      "value" : 1.7976931348623156E108,
      "unit" : "%",
      "count" : 100,
      "suppress_duration" : 0,
      "level" : 2,
      "enabled" : true
    } ],
    "resources" : [ {
      "dimensions" : [ {
        "name" : "string",
        "value" : "string"
      } ]
    } ],
    "type" : "EVENT.SYS",
    "enabled" : true,
    "notification_enabled" : true,
    "alarm_notifications" : [ {
      "type" : "notification",
      "notification_list" : [ "urn:smn:123" ]
    } ],
    "ok_notifications" : [ {
      "type" : "notification",
      "notification_list" : [ "urn:smn:123" ]
    } ],
    "notification_begin_time" : "00:00",
    "notification_end_time" : "23:59",
    "notification_manner" : "NOTIFICATION_POLICY",
    "notification_policy_ids" : [ "np15563156337845e8A2Wv63" ]
  } ]
}
```


Status Codes

Status Code	Description
200	OK
400	Parameter verification failed.
401	Not authenticated.
403	Authentication failed.
500	Internal system error.

Error Codes

See **Error Codes**.

6.10.4 Batch Enabling or Disabling Alarm Rules for One Service in One-Click Monitoring

Function

This API is used to batch enable or disable alarm rules for one service that has one-click monitoring enabled.

Debugging

You can debug this API through automatic authentication in **API Explorer** or use the SDK sample code generated by API Explorer.

URI

PUT /v2/{project_id}/one-click-alarms/{one_click_alarm_id}/alarm-rules/action

Table 6-304 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	**Definition** Tenant ID. **Constraints**: None **Value range**: Project ID, used to specify the project that an asset belongs to. You can query the assets of a project by project ID. You can obtain the project ID by calling an API or on the console. For details, see **Obtaining a Project ID**. The value must contain of 1 to 64 characters. **Default value**: None
one_click_alarm_id	Yes	String	One-click monitoring ID for a service.

Request Parameters

Table 6-305 Request header parameters

Parameter	Mandatory	Type	Description
Content-Type	No	String	**Definition** MIME type of the request body. **Constraints**: None **Value range**: The value can contain 1 to 64 characters. **Default value**: The default type is **application/json; charset=UTF-8**. **Default value:** application/json; charset=UTF-8

Parameter	Mandatory	Type	Description
X-Auth-Token	No	String	**Definition** User token. **Constraints**: None **Value range**: The value can contain 1 to 16,384 characters. **Default value**: None

Table 6-306 Request body parameters

Parameter	Mandatory	Type	Description
alarm_ids	Yes	Array of strings	IDs of alarm rules to be enabled or disabled in batches.
alarm_enabled	Yes	Boolean	Whether to enable the alarm rule. true: enabled; false: disabled.

Response Parameters

Status code: 200

Table 6-307 Response body parameters

Parameter	Type	Description
alarm_ids	Array of strings	IDs of alarm rules that were enabled or disabled.

Status code: 400

Table 6-308 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.

Parameter	Type	Description
request_id	String	Request ID.

Status code: 401

Table 6-309 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 403

Table 6-310 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 404

Table 6-311 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 500

Table 6-312 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Example Requests

```
{
  "alarm_ids" : [ "al123232232341232132" ],
  "alarm_enabled" : true
}
```

Example Responses

Status code: 200

Alarm rules enabled or disabled.

```
{
  "alarm_ids" : [ "al123232232341232132" ]
}
```

Status Codes

Status Code	Description
200	Alarm rules enabled or disabled.
400	Parameter verification failed.
401	Not authenticated.
403	Authentication failed.
404	Resource not found.
500	Internal system error.

Error Codes

See **Error Codes**.

6.10.5 Batch Disabling One-Click Motoring

Function

This API is used to batch disable one-click monitoring.

Debugging

You can debug this API through automatic authentication in **API Explorer** or use the SDK sample code generated by API Explorer.

URI

POST /v2/{project_id}/one-click-alarms/batch-delete

Table 6-313 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	**Definition** Tenant ID. **Constraints**: None **Value range**: Project ID, used to specify the project that an asset belongs to. You can query the assets of a project by project ID. You can obtain the project ID by calling an API or on the console. For details, see **Obtaining a Project ID**. The value must contain of 1 to 64 characters. **Default value**: None

Request Parameters

Table 6-314 Request header parameters

Parameter	Mandatory	Type	Description
Content-Type	No	String	**Definition** MIME type of the request body. **Constraints**: None **Value range**: The value can contain 1 to 64 characters. **Default value**: The default type is **application/json; charset=UTF-8**. **Default value:** application/json; charset=UTF-8
X-Auth-Token	No	String	**Definition** User token. **Constraints**: None **Value range**: The value can contain 1 to 16,384 characters. **Default value**: None

Table 6-315 Request body parameters

Parameter	Mandatory	Type	Description
one_click_alarm_ids	Yes	Array of strings	IDs of services that need to disable one-click monitoring.

Response Parameters

Status code: 200

Table 6-316 Response body parameters

Parameter	Type	Description
one_click_alarm_ids	Array of strings	IDs of services for which one-click monitoring was disabled.

Status code: 400

Table 6-317 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 401

Table 6-318 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 403

Table 6-319 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 500

Table 6-320 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Example Requests

```
{
  "one_click_alarm_ids" : [ "o1619578505263QkW3b66yo" ]
}
```

Example Responses

Status code: 200

IDs of services for which one-click monitoring was disabled.

```
{
  "one_click_alarm_ids" : [ "o1619578505263QkW3b66yo" ]
}
```

Status Codes

Status Code	Description
200	IDs of services for which one-click monitoring was disabled.
400	Parameter verification failed.
401	Not authenticated.
403	Authentication failed.
500	Internal system error.

Error Codes

See **Error Codes**.

6.10.6 Batch Modifying Alarm Notifications in Alarm Rules for One Service with One-Click Monitoring Enabled

Function

This API is used to batch modify alarm notifications in alarm rules for one service that has one-click monitoring enabled.

Debugging

You can debug this API through automatic authentication in **API Explorer** or use the SDK sample code generated by API Explorer.

URI

PUT /v2/{project_id}/one-click-alarms/{one_click_alarm_id}/notifications

Table 6-321 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	**Definition** Tenant ID. **Constraints**: None **Value range**: Project ID, used to specify the project that an asset belongs to. You can query the assets of a project by project ID. You can obtain the project ID by calling an API or on the console. For details, see **Obtaining a Project ID**. The value must contain of 1 to 64 characters. **Default value**: None
one_click_alarm_id	Yes	String	One-click monitoring ID for a service.

Request Parameters

Table 6-322 Request header parameters

Parameter	Mandatory	Type	Description
Content-Type	No	String	**Definition** MIME type of the request body. **Constraints**: None **Value range**: The value can contain 1 to 64 characters. **Default value**: The default type is **application/json; charset=UTF-8**. **Default value:** application/json; charset=UTF-8
X-Auth-Token	No	String	**Definition** User token. **Constraints**: None **Value range**: The value can contain 1 to 16,384 characters. **Default value**: None

Table 6-323 Request body parameters

Parameter	Mandatory	Type	Description
notification_enabled	Yes	Boolean	Whether to enable alarm notifications. If the value is **true**, other fields are mandatory. If the value is **false**, other fields are optional.
alarm_notifications	No	Array of **Notification** objects	Action to be triggered by the alarm.

Parameter	Mandatory	Type	Description
ok_notifications	No	Array of **Notification** objects	Action to be triggered after an alarm is cleared.
notification_begin_time	No	String	Time when the alarm notification was enabled.
notification_end_time	No	String	Time when the alarm notification was disabled.
effective_timezone	No	String	Time zone, for example, **GMT-08:00**, **GMT+08:00**, or **GMT+0:00**.
notification_manner	No	String	Notification mode, which can be **NOTIFICATION_GROUP** (notification groups), **TOPIC_SUBSCRIPTION** (topic subscriptions), or **NOTIFICATION_POLICY** (notification policies). Enumeration values: • **NOTIFICATION_GROUP** • **TOPIC_SUBSCRIPTION** • **NOTIFICATION_POLICY**
notification_policy_ids	No	Array of strings	Associated notification policy IDs.

Table 6-324 Notification

Parameter	Mandatory	Type	Description
type	Yes	String	Notification type. The value can be **notification** (SMN notifications), **contact** (account contacts), **contactGroup** (notification groups), or **autoscaling** (AS notifications). **autoscaling** is used only in AS and is not recommended. **groupwatch**, **ecsRecovery**, and **iecAction** are no longer used. Enumeration values: • **notification** • **autoscaling** • **groupwatch** • **ecsRecovery** • **contact** • **contactGroup** • **iecAction**
notification_list	Yes	Array of strings	List of objects to be notified if the alarm status changes. The value of **topicUrn** can be obtained from SMN. For details, see section "Querying Topics". If **type** is set to **notification**, the value of **notificationList** cannot be left blank. If **type** is set to **autoscaling**, the value of **notification_list** must be left blank. Note: If **alarm_action_enabled** is set to **true**, **alarm_actions**, **ok_actions**, or both of them must be specified. If both **alarm_actions** and **ok_actions** are specified, their **notification_list** values must be the same.

Response Parameters

Status code: 204

No Content

Status code: 400

Table 6-325 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 401

Table 6-326 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 403

Table 6-327 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 404

Table 6-328 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.

Parameter	Type	Description
request_id	String	Request ID.

Status code: 500

Table 6-329 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Example Requests

```
{
  "notification_enabled" : true,
  "alarm_notifications" : [ {
    "type" : "notification",
    "notification_list" : [ "urn:smn:123" ]
  } ],
  "ok_notifications" : [ {
    "type" : "notification",
    "notification_list" : [ "urn:smn:123" ]
  } ],
  "notification_begin_time" : "00:00",
  "notification_end_time" : "23:59",
  "notification_manner" : "NOTIFICATION_POLICY",
  "notification_policy_ids" : [ "np15563156337845e8A2Wv63" ]
}
```

Example Responses

None

Status Codes

Status Code	Description
204	No Content
400	Parameter verification failed.
401	Not authenticated.
403	Authentication failed.
404	Resource not found.
500	Internal system error.

Error Codes

See **Error Codes**.

6.10.7 Batch Enabling or Disabling Alarm Rules for One Service with One-Click Monitoring Enabled

Function

This API is used to batch enable or disable alarm rules for one service with one-click monitoring enabled.

Debugging

You can debug this API through automatic authentication in **API Explorer** or use the SDK sample code generated by API Explorer.

URI

PUT /v2/{project_id}/one-click-alarms/{one_click_alarm_id}/alarms/{alarm_id}/policies/action

Table 6-330 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	**Definition** Tenant ID. **Constraints**: None **Value range**: Project ID, used to specify the project that an asset belongs to. You can query the assets of a project by project ID. You can obtain the project ID by calling an API or on the console. For details, see **Obtaining a Project ID**. The value must contain of 1 to 64 characters. **Default value**: None
one_click_alarm_id	Yes	String	One-click monitoring ID for a service.
alarm_id	Yes	String	Alarm rule ID.

Request Parameters

Table 6-331 Request header parameters

Parameter	Mandatory	Type	Description
Content-Type	No	String	**Definition** MIME type of the request body. **Constraints**: None **Value range**: The value can contain 1 to 64 characters. **Default value**: The default type is **application/json; charset=UTF-8**. **Default value:** application/json; charset=UTF-8
X-Auth-Token	No	String	**Definition** User token. **Constraints**: None **Value range**: The value can contain 1 to 16,384 characters. **Default value**: None

Table 6-332 Request body parameters

Parameter	Mandatory	Type	Description
alarm_policy_ids	Yes	Array of strings	IDs of alarm policies to be enabled or disabled in batches in an alarm rule.
enabled	Yes	Boolean	Whether to enable the alarm policy. true: enabled; false: disabled.

Response Parameters

Status code: 200

Table 6-333 Response body parameters

Parameter	Type	Description
alarm_policy_ids	Array of strings	IDs of alarm policies that were enabled or disabled in batches in an alarm rule.

Status code: 400

Table 6-334 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 401

Table 6-335 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 403

Table 6-336 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.

Parameter	Type	Description
request_id	String	Request ID.

Status code: 404

Table 6-337 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 500

Table 6-338 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Example Requests

```
{
  "alarm_policy_ids" : [ "alxdxxxdsw12321321" ],
  "enabled" : true
}
```

Example Responses

Status code: 200

Alarm rules enabled or disabled.

```
{
  "alarm_policy_ids" : [ "alxdxxxdsw12321321" ]
}
```


Status Codes

Status Code	Description
200	Alarm rules enabled or disabled.
400	Parameter verification failed.
401	Not authenticated.
403	Authentication failed.
404	Resource not found.
500	Internal system error.

Error Codes

See **Error Codes**.

6.11 Alarm Masking Rules

6.11.1 Creating Alarm Masking Rules in Batches

Function

This API is used to create alarm masking rules in batches.

Debugging

You can debug this API through automatic authentication in **API Explorer** or use the SDK sample code generated by API Explorer.

URI

PUT /v2/{project_id}/notification-masks

Table 6-339 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	**Definition** Tenant ID. **Constraints**: None **Value range**: Project ID, used to specify the project that an asset belongs to. You can query the assets of a project by project ID. You can obtain the project ID by calling an API or on the console. For details, see **Obtaining a Project ID**. The value must contain of 1 to 64 characters. **Default value**: None

Request Parameters

Table 6-340 Request header parameters

Parameter	Mandatory	Type	Description
Content-Type	No	String	**Definition** MIME type of the request body. **Constraints**: None **Value range**: The value can contain 1 to 64 characters. **Default value**: The default type is **application/json; charset=UTF-8**. **Default value:** application/json; charset=UTF-8

Parameter	Mandatory	Type	Description
X-Auth-Token	No	String	**Definition** User token. **Constraints**: None **Value range**: The value can contain 1 to 16,384 characters. **Default value**: None

Table 6-341 Request body parameters

Parameter	Mandatory	Type	Description
mask_name	No	String	Masking rule name. The value can contain up to 64 characters, including only letters, digits, hyphens (-), and underscores (_).
relation_type	Yes	String	Method for masking alarm notifications or calculation. **ALARM_RULE**: masking alarm notifications by alarm rule. **RESOURCE**: masking alarm notifications by resource. **RESOURCE_POLICY_NOTIFICATION**: masking alarm notifications by resource or alarm policy. **RESOURCE_POLICY_ALARM**: masking alarm calculation by resource or alarm policy. Enumeration values: • **ALARM_RULE** • **RESOURCE** • **RESOURCE_POLICY_NOTIFICATION** • **RESOURCE_POLICY_ALARM**

Parameter	Mandatory	Type	Description
relation_ids	Yes	Array of strings	Alarm rule or alarm policy ID. If you set **relation_type** to **ALARM_RULE**, set this parameter to the ID of the masked alarm rule. If you set **relation_type** to **RESOURCE_POLICY_NOTIFICATION** or **RESOURCE_POLICY_ALARM**, set this parameter to the ID of the masked alarm policy.
resources	No	Array of **Resource** objects	Associated resource. It is required when you set **relation_type** to **RESOURCE**, **RESOURCE_POLICY_NOTIFICATION**, or **RESOURCE_POLICY_ALARM**.
metric_names	No	Array of strings	Name of the associated metric. This parameter is optional when **relation_type** is set to **RESOURCE**. If this parameter is left blank, the masking rule will be applied to all metrics of the resource.
product_metrics	No	Array of **ProductMetric** objects	Metric information when the masking rule is applied by cloud product.
resource_level	No	String	**dimension** indicates the sub-dimension, and **product** indicates the cloud product. Enumeration values: • **dimension** • **product**
product_name	No	String	Cloud product name specified when **Cloud product** is selected for **Resource Level**.

Parameter	Mandatory	Type	Description
mask_type	Yes	String	Masking type. **START_END_TIME**: Alarms are masked by start time and end time. **FOREVER_TIME**: Alarms are masked permanently. **CYCLE_TIME**: Alarms are masked by period. Enumeration values: • **START_END_TIME** • **FOREVER_TIME** • **CYCLE_TIME**
start_date	No	String	Masking start date, in **yyyy-MM-dd** format.
start_time	No	String	Masking start time, in **HH:mm:ss** format.
end_date	No	String	Masking end date, in **yyyy-MM-dd** format.
end_time	No	String	Masking end time, in **HH:mm:ss** format.
effective_timezone	No	String	Time zone, for example, **GMT-08:00**, **GMT+08:00**, or **GMT+0:00**.

Table 6-342 Resource

Parameter	Mandatory	Type	Description
namespace	Yes	String	Namespace of a service. For details about the namespace of each service, see **Namespace**.
dimensions	Yes	Array of **ResourceDimension** objects	Resource dimension information.

Table 6-343 ResourceDimension

Parameter	Mandatory	Type	Description
name	Yes	String	Dimension of a resource. For example, the dimension of an ECS can be **instance_id**. A maximum of four dimensions are supported. For the metric dimension of each resource, see **Service metric dimension**. **Regex Pattern:** ^([a-z]|[A-Z]){1}([a-z]|[A-Z]|[0-9]|_|-)*$
value	Yes	String	Value of a resource dimension. It is the instance ID, for example, **4270ff17-aba3-4138-89fa-820594c39755**. **Regex Pattern:** ^((([a-z]|[A-Z]|[0-9]|*|_|/|#|\(|\)){1}([a-z]|[A-Z]|[0-9]|_|-|\.|*|/|#|\(|\))*))$

Table 6-344 ProductMetric

Parameter	Mandatory	Type	Description
dimension_name	Yes	String	Metric dimension information when the masking rule is applied by cloud product. Use commas (,) to separate multiple metric dimensions.
metric_name	Yes	String	Metric name of a resource. The name must start with a letter and contain only digits, letters, and underscores. The length ranges from 1 to 64 characters. For example, **cpu_util** of an ECS indicates the CPU usage of the ECS. **mongo001_command_ps** in DDS indicates the command execution frequency. For details about the metric name of each service, see **Service metric name**.

Response Parameters

Status code: 201

Table 6-345 Response body parameters

Parameter	Type	Description
relation_ids	Array of strings	IDs of associated alarm rules or policies that were successfully created.
notification_mask_id	String	Masking rule ID.

Status code: 400

Table 6-346 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 500

Table 6-347 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Example Requests

```
{
  "mask_name" : "mn_test",
  "relation_type" : "ALARM_RULE",
  "relation_ids" : [ "al1232322323412321 32" ],
  "resources" : [ {
    "namespace" : "SYS.ECS",
    "dimensions" : [ {
      "name" : "instance_id",
      "value" : "4270ff17-aba3-4138-89fa-820594c39755"
    } ]
  } ],
```



```
  "mask_type" : "START_END_TIME",
  "start_date" : "yyyy-MM-dd",
  "start_time" : "HH:mm:ss",
  "end_date" : "yyyy-MM-dd",
  "end_time" : "HH:mm:ss"
}
```

Example Responses

Status code: 201

Notification masking rules created.

```
{
  "relation_ids" : [ "al123232232341232132" ],
  "notification_mask_id" : "nm123232232341232132"
}
```

Status Codes

Status Code	Description
201	Notification masking rules created.
400	Parameter verification failed.
500	Internal system error.

Error Codes

See **Error Codes**.

6.11.2 Modifying the Masking Time of Alarm Masking Rules in Batches

Function

Modify the masking time of alarm masking rules in batches.

Debugging

You can debug this API through automatic authentication in **API Explorer** or use the SDK sample code generated by API Explorer.

URI

POST /v2/{project_id}/notification-masks/batch-update

Table 6-348 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	**Definition** Tenant ID. **Constraints**: None **Value range**: Project ID, used to specify the project that an asset belongs to. You can query the assets of a project by project ID. You can obtain the project ID by calling an API or on the console. For details, see **Obtaining a Project ID**. The value must contain of 1 to 64 characters. **Default value**: None

Request Parameters

Table 6-349 Request header parameters

Parameter	Mandatory	Type	Description
Content-Type	No	String	**Definition** MIME type of the request body. **Constraints**: None **Value range**: The value can contain 1 to 64 characters. **Default value**: The default type is **application/json; charset=UTF-8**. **Default value:** application/json; charset=UTF-8

Parameter	Mandatory	Type	Description
X-Auth-Token	No	String	**Definition** User token. **Constraints**: None **Value range**: The value can contain 1 to 16,384 characters. **Default value**: None

Table 6-350 Request body parameters

Parameter	Mandatory	Type	Description
notification_mask_ids	Yes	Array of strings	Association ID.
mask_type	Yes	String	Masking type. **START_END_TIME**: Alarms are masked by start time and end time. **FOREVER_TIME**: Alarms are masked permanently. **CYCLE_TIME**: Alarms are masked by period. Enumeration values: • **START_END_TIME** • **FOREVER_TIME** • **CYCLE_TIME**
start_date	No	String	Masking start date, in **yyyy-MM-dd** format.
start_time	No	String	Masking start time, in **HH:mm:ss** format.
end_date	No	String	Masking end date, in **yyyy-MM-dd** format.
end_time	No	String	Masking end time, in **HH:mm:ss** format.
effective_timezone	No	String	Time zone, for example, **GMT-08:00**, **GMT+08:00**, or **GMT+0:00**.

Response Parameters

Status code: 204

Masking time modified.

Status code: 400

Table 6-351 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 500

Table 6-352 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Example Requests

```
{
  "notification_mask_ids" : [ "nm1232322323412321 32" ],
  "mask_type" : "START_END_TIME",
  "start_date" : "yyyy-MM-dd",
  "start_time" : "HH:mm:ss",
  "end_date" : "yyyy-MM-dd",
  "end_time" : "HH:mm:ss"
}
```

Example Responses

None

Status Codes

Status Code	Description
204	Masking time modified.

Status Code	Description
400	Parameter verification failed.
500	Internal system error.

Error Codes

See **Error Codes**.

6.11.3 Modifying an Alarm Masking Rule

Function

This API is used to modify an alarm masking rule.

Debugging

You can debug this API through automatic authentication in **API Explorer** or use the SDK sample code generated by API Explorer.

URI

PUT /v2/{project_id}/notification-masks/{notification_mask_id}

Table 6-353 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	**Definition** Tenant ID. **Constraints**: None **Value range**: Project ID, used to specify the project that an asset belongs to. You can query the assets of a project by project ID. You can obtain the project ID by calling an API or on the console. For details, see **Obtaining a Project ID**. The value must contain of 1 to 64 characters. **Default value**: None

Parameter	Mandatory	Type	Description
notification_mask_id	Yes	String	Masking rule ID. **Regex Pattern:** ^([a-z]|[A-Z]|[0-9]){1,64}$

Request Parameters

Table 6-354 Request header parameters

Parameter	Mandatory	Type	Description
Content-Type	No	String	**Definition** MIME type of the request body. **Constraints**: None **Value range**: The value can contain 1 to 64 characters. **Default value**: The default type is **application/json; charset=UTF-8**. **Default value:** application/json; charset=UTF-8
X-Auth-Token	No	String	**Definition** User token. **Constraints**: None **Value range**: The value can contain 1 to 16,384 characters. **Default value**: None

Table 6-355 Request body parameters

Parameter	Mandatory	Type	Description
mask_name	Yes	String	Masking rule name. The value can contain up to 64 characters, including only letters, digits, hyphens (-), and underscores (_).
relation_ids	No	Array of strings	Alarm rule or alarm policy ID. If you set **relation_type** to **ALARM_RULE**, set this parameter to the ID of the masked alarm rule. If you set **relation_type** to **RESOURCE_POLICY_NOTIFICATION** or **RESOURCE_POLICY_ALARM**, set this parameter to the ID of the masked alarm policy.
relation_type	No	String	Method for masking alarm notifications or calculation. **ALARM_RULE**: masking alarm notifications by alarm rule. **RESOURCE**: masking alarm notifications by resource. **RESOURCE_POLICY_NOTIFICATION**: masking alarm notifications by resource or alarm policy. **RESOURCE_POLICY_ALARM**: masking alarm calculation by resource or alarm policy. Enumeration values: • **ALARM_RULE** • **RESOURCE** • **RESOURCE_POLICY_NOTIFICATION** • **RESOURCE_POLICY_ALARM**
metric_names	No	Array of strings	Name of the associated metric. This parameter is optional when **relation_type** is set to **RESOURCE**. If this parameter is left blank, the masking rule will be applied to all metrics of the resource.

Parameter	Mandatory	Type	Description
product_metrics	No	Array of ProductMetric objects	Metric information when the masking rule is applied by cloud product.
resource_level	No	String	**dimension** indicates the sub-dimension, and **product** indicates the cloud product. Enumeration values: • **dimension** • **product**
product_name	No	String	Cloud product name specified when **Cloud product** is selected for **Resource Level**.
resources	Yes	Array of Resource objects	Associated resources.
mask_type	Yes	String	Masking type. **START_END_TIME**: Alarms are masked by start time and end time. **FOREVER_TIME**: Alarms are masked permanently. **CYCLE_TIME**: Alarms are masked by period. Enumeration values: • **START_END_TIME** • **FOREVER_TIME** • **CYCLE_TIME**
start_date	No	String	Masking start date, in **yyyy-MM-dd** format.
start_time	No	String	Masking start time, in **HH:mm:ss** format.
end_date	No	String	Masking end date, in **yyyy-MM-dd** format.
end_time	No	String	Masking end time, in **HH:mm:ss** format.
effective_timezone	No	String	Time zone, for example, **GMT-08:00**, **GMT+08:00**, or **GMT+0:00**.

Table 6-356 ProductMetric

Parameter	Mandatory	Type	Description
dimension_name	Yes	String	Metric dimension information when the masking rule is applied by cloud product. Use commas (,) to separate multiple metric dimensions.
metric_name	Yes	String	Metric name of a resource. The name must start with a letter and contain only digits, letters, and underscores. The length ranges from 1 to 64 characters. For example, **cpu_util** of an ECS indicates the CPU usage of the ECS. **mongo001_command_ps** in DDS indicates the command execution frequency. For details about the metric name of each service, see **Service metric name**.

Table 6-357 Resource

Parameter	Mandatory	Type	Description
namespace	Yes	String	Namespace of a service. For details about the namespace of each service, see **Namespace**.
dimensions	Yes	Array of **ResourceDimension** objects	Resource dimension information.

Table 6-358 ResourceDimension

Parameter	Mandatory	Type	Description
name	Yes	String	Dimension of a resource. For example, the dimension of an ECS can be **instance_id**. A maximum of four dimensions are supported. For the metric dimension of each resource, see **Service metric dimension**. **Regex Pattern:** ^([a-z]|[A-Z]){1}([a-z]|[A-Z]|[0-9]|_|-)*$
value	Yes	String	Value of a resource dimension. It is the instance ID, for example, **4270ff17-aba3-4138-89fa-820594c39755**. **Regex Pattern:** ^((([a-z]|[A-Z]|[0-9]|*|_|/|#|\(|\)){1}([a-z]|[A-Z]|[0-9]|_|-|\.|*|/|#|\(|\))*))$

Response Parameters

Status code: 204

No Content

Status code: 400

Table 6-359 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 500

Table 6-360 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Example Requests

```
{
  "mask_name" : "mn_test",
  "relation_ids" : [ "al1232322323412321 32" ],
  "relation_type" : "ALARM_RULE",
  "resources" : [ {
    "namespace" : "SYS.ECS",
    "dimensions" : [ {
      "name" : "instance_id",
      "value" : "4270ff17-aba3-4138-89fa-820594c39755"
    } ]
  } ],
  "mask_type" : "START_END_TIME",
  "start_date" : "yyyy-MM-dd",
  "start_time" : "HH:mm:ss",
  "end_date" : "yyyy-MM-dd",
  "end_time" : "HH:mm:ss"
}
```

Example Responses

None

Status Codes

Status Code	Description
204	No Content
400	Parameter verification failed.
500	Internal system error.

Error Codes

See **Error Codes**.

6.11.4 Deleting Alarm Masking Rules in Batches

Function

This API is used to delete alarm masking rules in batches.

Debugging

You can debug this API through automatic authentication in **API Explorer** or use the SDK sample code generated by API Explorer.

URI

POST /v2/{project_id}/notification-masks/batch-delete

Table 6-361 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	**Definition** Tenant ID. **Constraints**: None **Value range**: Project ID, used to specify the project that an asset belongs to. You can query the assets of a project by project ID. You can obtain the project ID by calling an API or on the console. For details, see **Obtaining a Project ID**. The value must contain of 1 to 64 characters. **Default value**: None

Request Parameters

Table 6-362 Request header parameters

Parameter	Mandatory	Type	Description
Content-Type	No	String	**Definition** MIME type of the request body. **Constraints**: None **Value range**: The value can contain 1 to 64 characters. **Default value**: The default type is **application/json; charset=UTF-8**. **Default value:** application/json; charset=UTF-8
X-Auth-Token	No	String	**Definition** User token. **Constraints**: None **Value range**: The value can contain 1 to 16,384 characters. **Default value**: None

Table 6-363 Request body parameters

Parameter	Mandatory	Type	Description
notification_mask_ids	Yes	Array of strings	Masking rule ID.

Response Parameters

Status code: 200

Table 6-364 Response body parameters

Parameter	Type	Description
notification_mask_ids	Array of strings	ID of a masking rule that was successfully deleted.

Status code: 400

Table 6-365 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 404

Table 6-366 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 500

Table 6-367 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Example Requests

```
{
  "notification_mask_ids" : [ "nm1232322323412321 32" ]
}
```

Example Responses

Status code: 200

Notification masking rules deleted.

```
{
  "notification_mask_ids" : [ "nm1232322323412321 32" ]
}
```

Status Codes

Status Code	Description
200	Notification masking rules deleted.
400	Parameter verification failed.
404	Resource not found.
500	Internal system error.

Error Codes

See **Error Codes**.

6.11.5 Querying Alarm Masking Rules

Function

This API is used to query notification masking rules of a specified type in batches. Currently, a maximum of 100 notification masking rules can be queried in batches.

Debugging

You can debug this API through automatic authentication in **API Explorer** or use the SDK sample code generated by API Explorer.

URI

POST /v2/{project_id}/notification-masks/batch-query

Table 6-368 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	**Definition** Tenant ID. **Constraints**: None **Value range**: Project ID, used to specify the project that an asset belongs to. You can query the assets of a project by project ID. You can obtain the project ID by calling an API or on the console. For details, see **Obtaining a Project ID**. The value must contain of 1 to 64 characters. **Default value**: None

Table 6-369 Query Parameters

Parameter	Mandatory	Type	Description
offset	No	Integer	Pagination offset. **Value range:** 0-10000 **Default value:** 0 **Regex Pattern:** ^([0]|[1-9]|[1-9][0-9]|[1-9][0-9][0-9]|[1-9][0-9][0-9][0-9]|10000)$
limit	No	Integer	Number of records on each page. **Value range:** 1-100 **Default value:** 100 **Regex Pattern:** ^([1-9]|[1-9][0-9]|100)$

Parameter	Mandatory	Type	Description
sort_key	No	String	Sorting keyword, which is used together with **sort_dir**. The value can be **create_time** or **update_time**. **create_time** indicates sorting by creation time, and **update_time** indicates sorting by modification time. Enumeration values: • **create_time** • **update_time**
sort_dir	No	String	Sorting order, which is used together with **sort_key**. **DESC** indicates the descending order, and **ASC** indicates the ascending order. Enumeration values: • **ASC** • **DESC**

Request Parameters

Table 6-370 Request header parameters

Parameter	Mandatory	Type	Description
Content-Type	No	String	**Definition** MIME type of the request body. **Constraints**: None **Value range**: The value can contain 1 to 64 characters. **Default value**: The default type is **application/json; charset=UTF-8**. **Default value:** application/json; charset=UTF-8

Parameter	Mandatory	Type	Description
X-Auth-Token	No	String	**Definition** User token. **Constraints**: None **Value range**: The value can contain 1 to 16,384 characters. **Default value**: None

Table 6-371 Request body parameters

Parameter	Mandatory	Type	Description
relation_type	Yes	String	Method for masking alarm notifications or calculation. **ALARM_RULE**: masking alarm notifications by alarm rule. **RESOURCE**: masking alarm notifications by resource. **RESOURCE_POLICY_NOTIFICATION**: masking alarm notifications by resource or alarm policy. **RESOURCE_POLICY_ALARM**: masking alarm calculation by resource or alarm policy. **DEFAULT**: **RESOURCE** and **RESOURCE_POLICY_NOTIFICATION** (used only for querying alarm masking rules) Enumeration values: • **ALARM_RULE** • **RESOURCE** • **RESOURCE_POLICY_NOTIFICATION** • **RESOURCE_POLICY_ALARM** • **DEFAULT**
relation_ids	Yes	Array of strings	Associated ID (alarm rule ID).

Parameter	Mandatory	Type	Description
metric_name	No	String	Metric name of a resource. The name must start with a letter and contain only digits, letters, and underscores. The length ranges from 1 to 64 characters. For example, **cpu_util** of an ECS indicates the CPU usage of the ECS. **mongo001_command_ps** in DDS indicates the command execution frequency. For details about the metric name of each service, see **Service metric name**.
resource_level	No	String	**dimension** indicates the sub-dimension, and **product** indicates the cloud product. Enumeration values: • **dimension** • **product**
mask_id	No	String	(Optional) Masking rule ID. **Regex Pattern:** ^nm([0-9A-Za-z]){0,62}$
mask_name	No	String	(Optional) Masking rule name. The value can contain up to 64 characters, including only letters, digits, hyphens (-), and underscores (_). **Regex Pattern:** ^([\u4E00-\u9FFF]|[a-z]|[A-Z]|[0-9]|_|-)+$
mask_status	No	String	Masking status. This parameter is optional. **MASK_EFFECTIVE**: The masking rule is in effect. **MASK_INEFFECTIVE**: The masking rule is not in effect. Enumeration values: • **MASK_EFFECTIVE** • **MASK_INEFFECTIVE**
resource_id	No	String	(Optional) Resource dimension value. You can specify one or more resource IDs from one dimension.

Parameter	Mandatory	Type	Description
namespace	No	String	Namespace of a service. For details about the namespace of each service, see **Namespace**.
dimensions	No	Array of **ResourceDimension** objects	Resource dimension information.

Table 6-372 ResourceDimension

Parameter	Mandatory	Type	Description
name	Yes	String	Dimension of a resource. For example, the dimension of an ECS can be **instance_id**. A maximum of four dimensions are supported. For the metric dimension of each resource, see **Service metric dimension**. **Regex Pattern:** ^([a-z]|[A-Z]){1}([a-z]|[A-Z]|[0-9]|_|-)*$
value	Yes	String	Value of a resource dimension. It is the instance ID, for example, **4270ff17-aba3-4138-89fa-820594c39755**. **Regex Pattern:** ^((([a-z]|[A-Z]|[0-9]|*|_|/|#|\(|\)){1}([a-z]|[A-Z]|[0-9]|_|-|\.|*|/|#|\(|\))*))$

Response Parameters

Status code: 200

Table 6-373 Response body parameters

Parameter	Type	Description
notification_masks	Array of **notification_masks** objects	List of alarm notification masking rules.

Parameter	Type	Description
count	Integer	Total number of alarm notification masking rules. **Value range:** 0-99999

Table 6-374 notification_masks

Parameter	Type	Description
notification_mask_id	String	Masking rule ID.
mask_name	String	Masking rule name. The value can contain up to 64 characters, including only letters, digits, hyphens (-), and underscores (_).
relation_type	String	Method for masking alarm notifications or calculation. **ALARM_RULE**: masking alarm notifications by alarm rule. **RESOURCE**: masking alarm notifications by resource. **RESOURCE_POLICY_NOTIFICATION**: masking alarm notifications by resource or alarm policy. **RESOURCE_POLICY_ALARM**: masking alarm calculation by resource or alarm policy. Enumeration values: • **ALARM_RULE** • **RESOURCE** • **RESOURCE_POLICY_NOTIFICATION** • **RESOURCE_POLICY_ALARM**
relation_id	String	Association ID.
resource_type	String	Masked resource type. The value can be **ALL_INSTANCE (all resources) or ** MULTI_INSTANCE** (multi-instance resources). Enumeration values: • **ALL_INSTANCE** • **MULTI_INSTANCE**

Parameter	Type	Description
metric_names	Array of strings	Name of the associated metric. This parameter is available when **relation_type** is set to **RESOURCE**.
product_metrics	Array of **ProductMetric** objects	Metric information when the masking rule is applied by cloud product.
resource_level	String	**dimension** indicates the sub-dimension, and **product** indicates the cloud product. Enumeration values: • **dimension** • **product**
product_name	String	Cloud product name specified when **Cloud product** is selected for **Resource Level**.
resources	Array of **ResourceCategory** objects	Associated resource type. This parameter is available when **relation_type** is set to **RESOURCE**. You only need to query the namespace and dimension name of the resource.
mask_status	String	Masking status. **UN_MASKED**: Alarm notifications are not masked. **MASK_EFFECTIVE**: Masking rules are in effect. **MASK_INEFFECTIVE**: Masking rules are not in effect. Enumeration values: • **UN_MASKED** • **MASK_EFFECTIVE** • **MASK_INEFFECTIVE**
mask_type	String	Masking type. **START_END_TIME**: Alarms are masked by start time and end time. **FOREVER_TIME**: Alarms are masked permanently. **CYCLE_TIME**: Alarms are masked by period. Enumeration values: • **START_END_TIME** • **FOREVER_TIME** • **CYCLE_TIME**
create_time	Integer	Time the alarm masking is created. The value is a UNIX timestamp and the unit is ms.

Parameter	Type	Description
update_time	Integer	Time the alarm masking is updated. The value is a UNIX timestamp and the unit is ms.
start_date	String	Masking start date, in **yyyy-MM-dd** format.
start_time	String	Masking start time, in **HH:mm:ss** format.
end_date	String	Masking end date, in **yyyy-MM-dd** format.
end_time	String	Masking end time, in **HH:mm:ss** format.
effective_timezone	String	Time zone, for example, **GMT-08:00**, **GMT+08:00**, or **GMT+0:00**.
policies	Array of **PoliciesInListResp** objects	Alarm policy list.

Table 6-375 ProductMetric

Parameter	Type	Description
dimension_name	String	Metric dimension information when the masking rule is applied by cloud product. Use commas (,) to separate multiple metric dimensions.
metric_name	String	Metric name of a resource. The name must start with a letter and contain only digits, letters, and underscores. The length ranges from 1 to 64 characters. For example, **cpu_util** of an ECS indicates the CPU usage of the ECS. **mongo001_command_ps** in DDS indicates the command execution frequency. For details about the metric name of each service, see **Service metric name**.

Table 6-376 ResourceCategory

Parameter	Type	Description
namespace	String	Namespace of a service. For details about the namespace of each service, see **Namespace**.
dimension_names	Array of strings	Resource dimension information. Multiple dimensions are sorted in alphabetical order and separated with commas (,).

Table 6-377 PoliciesInListResp

Parameter	Type	Description
alarm_policy_id	String	Alarm policy ID.
metric_name	String	Metric name of a resource. The name must start with a letter and contain only digits, letters, and underscores. The length ranges from 1 to 64 characters. For example, **cpu_util** of an ECS indicates the CPU usage of the ECS. **mongo001_command_ps** in DDS indicates the command execution frequency. For details about the metric name of each service, see **Service metric name**.
extra_info	**MetricExtraInfo** object	Additional information about an alarm policy. This parameter is left blank by default.

Parameter	Type	Description
period	Integer	Period for determining whether to generate an alarm, in seconds. The value can be **1**, **300**, **1200**, **3600**, **14400**, or **86400**. Note: If you set **period** to **1**, Cloud Eye uses raw data to determine whether to trigger an alarm. You can set this parameter to **0** when you set **alarm_type** to **EVENT.SYS** or **EVENT.CUSTOM**. Enumeration values: • **0** • **1** • **300** • **1200** • **3600** • **14400** • **86400**
filter	String	Aggregation mode. average: average value; variance: variance; min: minimum value; max: maximum value; sum: sum; tp99: 99 percentile; tp95: 95 percentile; tp90: 90 percentile
comparison_operator	String	Threshold symbol. The value can be **>**, **<**, **>=**, **<=**, **=**, **!=**, **cycle_decrease**, **cycle_increase**, or **cycle_wave**. **cycle_decrease** indicates the decrease compared with the last period, **cycle_increase** indicates the increase compared with the last period, and **cycle_wave** indicates the increase or decrease compared with the last period. All of them can be used in alarm rules for metrics. **>**, **<**, **>=**, **<=**, **=**, and **!=** can be used for alarm rules for events.

Parameter	Type	Description
value	Number	Alarm threshold If there is only one threshold, **value** and **alarm_level** are used in pairs. If there are both **hierarchical_value** and **value**, **hierarchical_value** is used. For detailed thresholds, see the value range of each metric in the appendix. For example, you can set ECS **cpu_util** to **80**. For detailed thresholds, see the value range of each metric in the appendix. For example, you can set ECS **cpu_util** to **80** in **Services Interconnected with Cloud Eye**.
hierarchical_value	**HierarchicalValue** object	Multi-level alarm threshold. If there are both **hierarchical_value** and **value**, **hierarchical_value** prevails. When you create or modify an alarm rule, you can set only one threshold in the following scenarios: 1. The alarm type is **Metric** and the alarm policy is **Trigger an alarm when all policies are met**. 2. The alarm type is **Event**.
unit	String	Data unit.
count	Integer	Number of consecutive alarm triggering times. For event alarms, the value ranges from **1** to **180**. For metric and website alarms, the value can be **1**, **2**, **3**, **4**, **5**, **10**, **15**, **30**, **60**, **90**, **120**, or **180**.
type	String	Alarm policy type. This API has been deprecated.

Parameter	Type	Description
suppress_duration	Integer	Interval for triggering alarms. The value can be **0**, **300**, **600**, **900**, **1800**, **3600**, **10800**, **21600**, **43200**, or **86400**. **0**: Cloud Eye triggers the alarm only once. **300**: Cloud Eye triggers an alarm every 5 minutes. **600**: Cloud Eye triggers an alarm every 10 minutes. **900**: Cloud Eye triggers an alarm every 15 minutes. **1800**: Cloud Eye triggers an alarm every 30 minutes. **3600**: Cloud Eye triggers an alarm every hour. **10800**: Cloud Eye triggers an alarm every 3 hours. **21600**: Cloud Eye triggers an alarm every 6 hour. **43200**: Cloud Eye triggers an alarm every 12 hours. **86400**: Cloud Eye triggers an alarm every day. Enumeration values: • **0** • **300** • **600** • **900** • **1800** • **3600** • **10800** • **21600** • **43200** • **86400**
alarm_level	Integer	Alarm severity, which can be **1** (critical), ** 2** (major), **3** (minor), or **4** (informational).
selected_unit	String	The unit you selected, which is used for subsequent metric data display and calculation.

Table 6-378 MetricExtraInfo

Parameter	Type	Description
origin_metric_name	String	Original metric name. **Regex Pattern:** ^([a-z]|[A-Z]|[0-9]|_|-|~|\.|/|:)*$

Parameter	Type	Description
metric_prefix	String	Metric name prefix. **Regex Pattern:** ^([a-z]|[A-Z]|[0-9]|_|-|~|\.|/|:)*$
custom_proc_name	String	Name of a user process.
metric_type	String	Metric type. **Regex Pattern:** ^([a-z]|[A-Z]|[0-9]|_|-|~|\.|/|:)*$

Table 6-379 HierarchicalValue

Parameter	Type	Description
critical	Double	Threshold for critical alarms. **Value range:** -1.7976931348623156E108-1.7976931348623156E108
major	Double	Threshold for major alarms. **Value range:** -1.7976931348623156E108-1.7976931348623156E108
minor	Double	Threshold for minor alarms. **Value range:** -1.7976931348623156E108-1.7976931348623156E108
info	Double	Threshold for informational alarms. **Value range:** -1.7976931348623156E108-1.7976931348623156E108

Status code: 400

Table 6-380 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.

Parameter	Type	Description
request_id	String	Request ID.

Status code: 500

Table 6-381 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Example Requests

```
{
  "relation_type" : "DEFAULT",
  "relation_ids" : [ "al123232232341232132" ],
  "mask_id" : "nm1689737291469aj38xNVLK",
  "mask_name" : "mn_test",
  "mask_status" : "MASK_EFFECTIVE",
  "resource_id" : "dse23xw43",
  "namespace" : "SYS.ECS",
  "dimensions" : [ {
    "name" : "instance_id",
    "value" : "4270ff17-aba3-4138-89fa-820594c39755"
  } ]
}
```

Example Responses

Status code: 200

Notification masking rules queried.

```
{
  "notification_masks" : [ {
    "notification_mask_id" : "nm123232232341232132",
    "mask_name" : "mn_test",
    "relation_type" : "ALARM_RULE",
    "relation_id" : "al123232232341232132",
    "resource_type" : "MULTI_INSTANCE",
    "resources" : [ {
      "namespace" : "SYS.ECS",
      "dimension_names" : [ "disk_utils,instance_id" ]
    } ],
    "mask_status" : "UN_MASKED",
    "mask_type" : "START_END_TIME",
    "start_date" : "yyyy-MM-dd",
    "start_time" : "HH:mm:ss",
    "end_date" : "yyyy-MM-dd",
    "end_time" : "HH:mm:ss",
    "policies" : [ {
      "alarm_policy_id" : "0f921f55-89b1-4534-ae54-7b40b597b5a6",
      "metric_name" : "cpu_util",
```



```
    "extra_info" : {
      "origin_metric_name" : "disk_usedPercent",
      "metric_prefix" : "SlAsh_",
      "custom_proc_name" : "proc_zombie_count1",
      "metric_type" : "string"
    },
    "period" : 300,
    "filter" : "average",
    "comparison_operator" : ">",
    "value" : 0,
    "unit" : "%",
    "count" : 3,
    "type" : "string",
    "suppress_duration" : 300,
    "alarm_level" : 2
   } ]
  } ],
  "count" : 100
}
```


Status Codes

Status Code	Description
200	Notification masking rules queried.
400	Parameter verification failed.
500	Internal system error.

Error Codes

See **Error Codes**.

6.11.6 Querying Resources for Which an Alarm Masking Rule Is Applied

Function

This API is used to query resources for which an alarm masking rule is applied.

Debugging

You can debug this API through automatic authentication in **API Explorer** or use the SDK sample code generated by API Explorer.

URI

GET /v2/{project_id}/notification-masks/{notification_mask_id}/resources

Table 6-382 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	**Definition** Tenant ID. **Constraints**: None **Value range**: Project ID, used to specify the project that an asset belongs to. You can query the assets of a project by project ID. You can obtain the project ID by calling an API or on the console. For details, see **Obtaining a Project ID**. The value must contain of 1 to 64 characters. **Default value**: None
notification_mask_id	Yes	String	Masking rule ID. **Regex Pattern:** ^([a-z]|[A-Z]|[0-9]){1,64}$

Table 6-383 Query Parameters

Parameter	Mandatory	Type	Description
offset	No	Integer	Pagination offset. **Value range:** 0-10000 **Default value:** 0 **Regex Pattern:** ^([0]|[1-9]|[1-9][0-9]|[1-9][0-9][0-9]|[1-9][0-9][0-9][0-9]|10000)$

Parameter	Mandatory	Type	Description
limit	No	Integer	Number of records on each page. **Value range:** 1-100 **Default value:** 100 **Regex Pattern:** ^([1-9]|[1-9][0-9]|100)$

Request Parameters

Table 6-384 Request header parameters

Parameter	Mandatory	Type	Description
Content-Type	No	String	**Definition** MIME type of the request body. **Constraints**: None **Value range**: The value can contain 1 to 64 characters. **Default value**: The default type is **application/json; charset=UTF-8**. **Default value:** application/json; charset=UTF-8
X-Auth-Token	No	String	**Definition** User token. **Constraints**: None **Value range**: The value can contain 1 to 16,384 characters. **Default value**: None

Response Parameters

Status code: 200

Table 6-385 Response body parameters

Parameter	Type	Description
resources	Array of **Resource** objects	List of resources for which an alarm masking rule is applied.
count	Integer	Total number of resources. **Value range:** 0-100

Table 6-386 Resource

Parameter	Type	Description
namespace	String	Namespace of a service. For details about the namespace of each service, see **Namespace**.
dimensions	Array of **ResourceDimension** objects	Resource dimension information.

Table 6-387 ResourceDimension

Parameter	Type	Description
name	String	Dimension of a resource. For example, the dimension of an ECS can be **instance_id**. A maximum of four dimensions are supported. For the metric dimension of each resource, see **Service metric dimension**. **Regex Pattern:** ^([a-z]|[A-Z]){1}([a-z]|[A-Z]|[0-9]|_|-)*$
value	String	Value of a resource dimension. It is the instance ID, for example, **4270ff17-aba3-4138-89fa-820594c39755**. **Regex Pattern:** ^((([a-z]|[A-Z]|[0-9]|*|_|/|#|\(|\)){1}([a-z]|[A-Z]|[0-9]|_|-|\.|*|/|#|\(|\))*))$

Status code: 400

Table 6-388 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 500

Table 6-389 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Example Requests

None

Example Responses

Status code: 200

Resources queried.

```
{
  "resources" : [ {
    "namespace" : "SYS.ECS",
    "dimensions" : [ {
      "name" : "instance_id",
      "value" : "4270ff17-aba3-4138-89fa-820594c39755"
    } ]
  } ],
  "count" : 100
}
```

Status Codes

Status Code	Description
200	Resources queried.
400	Parameter verification failed.

Status Code	Description
500	Internal system error.

Error Codes

See **Error Codes**.

6.12 Dashboards

6.12.1 Creating or Copying a Dashboard

Function

This API is used to create or copy a dashboard.

Constraints

This API is not supported in the following regions: CN East-Qingdao, LA-Mexico City1, TR-Istanbul, AP-Jakarta, ME-Riyadh, and AP-Manila.

Debugging

You can debug this API through automatic authentication in **API Explorer** or use the SDK sample code generated by API Explorer.

URI

POST /v2/{project_id}/dashboards

Table 6-390 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	**Definition** Tenant ID. **Constraints**: None **Value range**: Project ID, used to specify the project that an asset belongs to. You can query the assets of a project by project ID. You can obtain the project ID by calling an API or on the console. For details, see **Obtaining a Project ID**. The value must contain of 1 to 64 characters. **Default value**: None

Request Parameters

Table 6-391 Request header parameters

Parameter	Mandatory	Type	Description
Content-Type	No	String	**Definition** MIME type of the request body. **Constraints**: None **Value range**: The value can contain 1 to 64 characters. **Default value**: The default type is **application/json; charset=UTF-8**. **Default value:** application/json; charset=UTF-8

Parameter	Mandatory	Type	Description
X-Auth-Token	No	String	**Definition** User token. **Constraints**: None **Value range**: The value can contain 1 to 16,384 characters. **Default value**: None

Table 6-392 Request body parameters

Parameter	Mandatory	Type	Description
dashboard_name	Yes	String	Custom dashboard name. **Regex Pattern:** ^([\u4E00-\u9FFF]|[a-z]|[A-Z]|[0-9]|_|-)+$
enterprise_id	No	String	Enterprise project ID. **Regex Pattern:** ^((([a-z]|[0-9]){8}-([a-z]|[0-9]){4}-([a-z]|[0-9]){4}-([a-z]|[0-9]){4}-([a-z]|[0-9]){12})|0)$
dashboard_id	No	String	Dashboard ID. **Regex Pattern:** ^db([a-z]|[A-Z]|[0-9]){22}
row_widget_num	No	Integer	How a graph is displayed. **0** indicates that you can customize **top** and **left** of the graph. **1** indicates one graph per row. **Value range:** 0-3 **Default value:** 3

Response Parameters

Status code: 201

Table 6-393 Response body parameters

Parameter	Type	Description
dashboard_id	String	Dashboard ID. **Regex Pattern:** ^db([a-z]|[A-Z]|[0-9]){22}

Status code: 400

Table 6-394 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 401

Table 6-395 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 500

Table 6-396 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Example Requests

```
{
  "dashboard_name" : "dashboard_name",
  "enterprise_id" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
  "dashboard_id" : "dbxxxxxxxxxxxxxxxxxxxxxxx",
  "row_widget_num" : 3
}
```

Example Responses

Status code: 201

OK

```
{
  "dashboard_id" : "dbxxxxxxxxx"
}
```

Status Codes

Status Code	Description
201	OK
400	The server failed to process the request.
401	Token authentication is required.
500	Failed to complete the request because of an internal server error.

Error Codes

See **Error Codes**.

6.12.2 Querying Dashboards

Function

This API is used to query dashboards.

Constraints

This API is not supported in the following regions: CN East-Qingdao, LA-Mexico City1, TR-Istanbul, AP-Jakarta, ME-Riyadh, and AP-Manila.

Debugging

You can debug this API through automatic authentication in **API Explorer** or use the SDK sample code generated by API Explorer.

URI

GET /v2/{project_id}/dashboards

Table 6-397 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	**Definition** Tenant ID. **Constraints**: None **Value range**: Project ID, used to specify the project that an asset belongs to. You can query the assets of a project by project ID. You can obtain the project ID by calling an API or on the console. For details, see **Obtaining a Project ID**. The value must contain of 1 to 64 characters. **Default value**: None

Table 6-398 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_id	No	String	Enterprise project ID. **Regex Pattern:** ^((([a-z]|[0-9]){8}-([a-z]|[0-9]){4}-([a-z]|[0-9]){4}-([a-z]|[0-9]){4}-([a-z]|[0-9]){12})|0|all_granted_eps)$
is_favorite	No	Boolean	Whether a dashboard in an enterprise project is added to favorites. The value can be **true** (added to favorites) and **false** (not added to favorites). If this parameter is specified, **enterprise_id** is mandatory.
dashboard_name	No	String	Dashboard name. **Regex Pattern:** ^([\u4E00-\u9FFF]|[a-z]|[A-Z]|[0-9]|_|-)+$
dashboard_id	No	String	Dashboard ID. **Regex Pattern:** ^db([a-z]|[A-Z]|[0-9]){22}

Parameter	Mandatory	Type	Description
dashboard_type	No	String	Monitoring dashboard type. **monitor_dashboard** indicates a default dashboard, and **other** indicates a custom dashboard. Enumeration values: • **monitor_dashboard** • **other**

Request Parameters

Table 6-399 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	No	String	**Definition** User token. **Constraints**: None **Value range**: The value can contain 1 to 16,384 characters. **Default value**: None

Response Parameters

Status code: 200

Table 6-400 Response body parameters

Parameter	Type	Description
dashboards	Array of **DashBoardInfo** objects	Dashboard list.

Table 6-401 DashBoardInfo

Parameter	Type	Description
dashboard_id	String	Dashboard ID. **Regex Pattern:** ^db([a-z]|[A-Z]|[0-9]){22}
dashboard_name	String	Custom dashboard name. **Regex Pattern:** ^([\u4E00-\u9FFF]|[a-z]|[A-Z]|[0-9]|_|-)+$
enterprise_id	String	Enterprise project ID. **Regex Pattern:** ^((([a-z]|[0-9]){8}-([a-z]|[0-9]){4}-([a-z]|[0-9]){4}-([a-z]|[0-9]){4}-([a-z]|[0-9]){12})|0)$
creator_name	String	Name of the user who created the dashboard. **Regex Pattern:** ^([\u4E00-\u9FFF]|[a-z]|[A-Z]|[0-9]|_|-)+$
create_time	Long	Dashboard creation time. **Value range:** 1111111111111-9999999999999
widgets_num	Integer	Total number of graphs on the dashboard. **Value range:** 0-50
namespace	String	Namespace. **Regex Pattern:** ^([a-z]|[A-Z]){1}([a-z]|[A-Z]|[0-9]|_)*\.([a-z]|[A-Z]){1}([a-z]|[A-Z]|[0-9]|_)*$
sub_product	String	Sub-product ID.
dashboard_template_id	String	Dashboard template ID. **Regex Pattern:** ^mb([a-z]|[A-Z]|[0-9]){22}
row_widget_num	Integer	How a graph is displayed. **0** indicates that you can customize **top** and **left** of the graph. **1** indicates one graph per row. **Value range:** 0-3 **Default value:** 3

Parameter	Type	Description
is_favorite	Boolean	Whether a dashboard is added to favorites. The value can be **true** or **false**.

Status code: 400

Table 6-402 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 401

Table 6-403 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 500

Table 6-404 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Example Requests

None

Example Responses

Status code: 200

OK

```
{
  "dashboards" : [ {
    "dashboard_id" : "dbxxxxxxxxxxxxxxxxxxxxxx",
    "dashboard_name" : "dashboard_name",
    "enterprise_id" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
    "creator_name" : "creator_name",
    "create_time" : 1111111111111,
    "row_widget_num" : 3,
    "is_favorite" : false
  } ]
}
```

Status Codes

Status Code	Description
200	OK
400	The server failed to process the request.
401	Token authentication is required.
500	Failed to complete the request because of an internal server error.

Error Codes

See **Error Codes**.

6.12.3 Modifying a Dashboard

Function

This API is used to modify a dashboard.

Constraints

This API is not supported in the following regions: CN East-Qingdao, LA-Mexico City1, TR-Istanbul, AP-Jakarta, ME-Riyadh, and AP-Manila.

Debugging

You can debug this API through automatic authentication in **API Explorer** or use the SDK sample code generated by API Explorer.

URI

PUT /v2/{project_id}/dashboards/{dashboard_id}

Table 6-405 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	**Definition** Tenant ID. **Constraints**: None **Value range**: Project ID, used to specify the project that an asset belongs to. You can query the assets of a project by project ID. You can obtain the project ID by calling an API or on the console. For details, see **Obtaining a Project ID**. The value must contain of 1 to 64 characters. **Default value**: None
dashboard_id	Yes	String	Dashboard ID, which starts with **db** and follows 22 letters and digits. Example: **db16564943172807wjOmoLyn**. **Regex Pattern:** ^db([a-z]|[A-Z]|[0-9]){22}$

Request Parameters

Table 6-406 Request header parameters

Parameter	Mandatory	Type	Description
Content-Type	No	String	**Definition** MIME type of the request body. **Constraints**: None **Value range**: The value can contain 1 to 64 characters. **Default value**: The default type is **application/json; charset=UTF-8**. **Default value:** application/json; charset=UTF-8
X-Auth-Token	No	String	**Definition** User token. **Constraints**: None **Value range**: The value can contain 1 to 16,384 characters. **Default value**: None

Table 6-407 Request body parameters

Parameter	Mandatory	Type	Description
dashboard_name	No	String	Custom dashboard name. **Regex Pattern:** ^([\u4E00-\u9FFF]|[a-z]|[A-Z]|[0-9]|_|-)+$
is_favorite	No	Boolean	Whether a dashboard is added to favorites. The value can be **true** or **false**.

Parameter	Mandatory	Type	Description
row_widget_num	Yes	Integer	How a graph is displayed. **0** indicates that you can customize **top** and **left** of the graph. **1** indicates one graph per row. **Value range:** 0-4 **Default value:** 3
extend_info	No	**ExtendInfo** object	Extended information about the dashboard.

Table 6-408 ExtendInfo

Parameter	Mandatory	Type	Description
filter	No	String	Metric aggregation mode. The value can be **average**, **min**, **max**, or **sum**. Enumeration values: • **average** • **min** • **max** • **sum**
period	No	String	Metric rollup period. {**1** indicates the original value, **60** indicates one minute, **300** indicates five minutes, **1200** indicates 20 minutes, **3600** indicates one hour, **14400** indicates four hours, and **86400** indicates one day.} **Regex Pattern:** ^(1|60|300|1200|3600|14400|86400)$

Parameter	Mandatory	Type	Description
display_time	No	Integer	Display time. The value **0** indicates that you can customize a time. The value can be 5 minutes, 15 minutes, 30 minutes, 1 hour, 2 hours, 3 hours, 12 hours, 1 day, 7 days, or 30 days. Enumeration values: • **0** • **5** • **15** • **30** • **60** • **120** • **180** • **720** • **1440** • **10080** • **43200**
refresh_time	No	Integer	Refresh interval. The value can be **0** (not refreshed), 10s, 1 min, 5 mins, or 20 mins. Enumeration values: • **0** • **10** • **60** • **300** • **1200**
from	No	Long	Start time. **Value range:** 0-9999999999999
to	No	Long	End time. **Value range:** 0-9999999999999
screen_color	No	String	Background color of the dashboard.
enable_screen_auto_play	No	Boolean	Whether the monitoring dashboard can be automatically switched.

Parameter	Mandatory	Type	Description
time_interval	No	Integer	Auto-switch interval for dashboard. The value can be **10000** (10s), **30000** (30s), and **60000** (1 min). Enumeration values: • **10000** • **30000** • **60000**
enable_legend	No	Boolean	Whether to display the legend.
full_screen_widget_num	No	Integer	Number of graphs displayed on the dashboard. The value must be consistent with an available one on the console. **Value range:** 0-65535

Response Parameters

Status code: 204

No Content

Status code: 400

Table 6-409 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 401

Table 6-410 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.

Parameter	Type	Description
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 500

Table 6-411 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Example Requests

```
{
  "dashboard_name" : "dashboard_name_new",
  "is_favorite" : true,
  "row_widget_num" : 0
}
```

Example Responses

None

Status Codes

Status Code	Description
204	No Content
400	The server failed to process the request.
401	Token authentication is required.
500	Failed to complete the request because of an internal server error.

Error Codes

See **Error Codes**.

6.12.4 Deleting Dashboards in Batches

Function

This API is used to delete dashboards in batches.

Constraints

This API is not supported in the following regions: CN East-Qingdao, LA-Mexico City1, TR-Istanbul, AP-Jakarta, ME-Riyadh, and AP-Manila.

Debugging

You can debug this API through automatic authentication in **API Explorer** or use the SDK sample code generated by API Explorer.

URI

POST /v2/{project_id}/dashboards/batch-delete

Table 6-412 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	**Definition** Tenant ID. **Constraints**: None **Value range**: Project ID, used to specify the project that an asset belongs to. You can query the assets of a project by project ID. You can obtain the project ID by calling an API or on the console. For details, see **Obtaining a Project ID**. The value must contain of 1 to 64 characters. **Default value**: None

Request Parameters

Table 6-413 Request header parameters

Parameter	Mandatory	Type	Description
Content-Type	No	String	**Definition** MIME type of the request body. **Constraints**: None **Value range**: The value can contain 1 to 64 characters. **Default value**: The default type is **application/json; charset=UTF-8**. **Default value:** application/json; charset=UTF-8
X-Auth-Token	No	String	**Definition** User token. **Constraints**: None **Value range**: The value can contain 1 to 16,384 characters. **Default value**: None

Table 6-414 Request body parameters

Parameter	Mandatory	Type	Description
dashboard_ids	No	Array of strings	Dashboard ID list.

Response Parameters

Status code: 200

Table 6-415 Response body parameters

Parameter	Type	Description
dashboards	Array of **BatchDeleteDashboardRespInfo** objects	Response body for deleting dashboards in batches.

Table 6-416 BatchDeleteDashboardRespInfo

Parameter	Type	Description
dashboard_id	String	Dashboard ID. **Regex Pattern:** ^db([a-z]|[A-Z]|[0-9]){22}
ret_status	String	Operation result. The value can be **successful** or **error**. Enumeration values: • **successful** • **error**
error_msg	String	Error message.

Status code: 400

Table 6-417 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 401

Table 6-418 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.

Parameter	Type	Description
request_id	String	Request ID.

Status code: 500

Table 6-419 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Example Requests

```
{
  "dashboard_ids" : [ "dbxxxxxxxxxxxxxxxxxxxxxxx", "dbXXXXXXXXXXXXXXXXXXXXXX" ]
}
```

Example Responses

Status code: 200

OK

```
{
  "dashboards" : [ {
    "dashboard_id" : "dbxxxxxxxxxxxxxxxxxxxxxx",
    "ret_status" : "successful"
  }, {
    "dashboard_id" : "dbXXXXXXXXXXXXXXXXXXXXX",
    "ret_status" : "error",
    "error_msg" : "record not found"
  } ]
}
```

Status Codes

Status Code	Description
200	OK
400	The server failed to process the request.
401	Token authentication is required.
500	Failed to complete the request because of an internal server error.

Error Codes

See **Error Codes**.

6.13 Graphs

6.13.1 Creating, Copying, or Batch Creating Graphs on a Dashboard

Function

This API is used to create, copy, or batch create graphs on a dashboard.

Constraints

This API is not supported in the following regions: CN East-Qingdao, LA-Mexico City1, TR-Istanbul, AP-Jakarta, ME-Riyadh, and AP-Manila.

Debugging

You can debug this API through automatic authentication in **API Explorer** or use the SDK sample code generated by API Explorer.

URI

POST /v2/{project_id}/dashboards/{dashboard_id}/widgets

Table 6-420 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	**Definition** Tenant ID. **Constraints**: None **Value range**: Project ID, used to specify the project that an asset belongs to. You can query the assets of a project by project ID. You can obtain the project ID by calling an API or on the console. For details, see **Obtaining a Project ID**. The value must contain of 1 to 64 characters. **Default value**: None

Parameter	Mandatory	Type	Description
dashboard_id	Yes	String	Dashboard ID, which starts with **db** and follows 22 letters and digits. Example: **db16564943172807wjOmoLyn**. **Regex Pattern:** ^db([a-z]|[A-Z]|[0-9]){22}$

Request Parameters

Table 6-421 Request header parameters

Parameter	Mandatory	Type	Description
Content-Type	No	String	**Definition** MIME type of the request body. **Constraints**: None **Value range**: The value can contain 1 to 64 characters. **Default value**: The default type is **application/json; charset=UTF-8**. **Default value:** application/json; charset=UTF-8
X-Auth-Token	No	String	**Definition** User token. **Constraints**: None **Value range**: The value can contain 1 to 16,384 characters. **Default value**: None

Table 6-422 Request body parameters

Parameter	Mandatory	Type	Description
[items]	No	Array of **BaseWidgetInfo** objects	Graph information.

Table 6-423 BaseWidgetInfo

Parameter	Mandatory	Type	Description
group_id	No	String	Graph partition ID. **Regex Pattern:** ^dg([a-z]|[A-Z]|[0-9]){22}|default$
metrics	Yes	Array of **WidgetMetric** objects	Metric list.
title	Yes	String	Graph name. **Regex Pattern:** ^([\u4E00-\u9FFF]|[\u00C0-\u0204]|[a-z]|[A-Z]|[0-9]|[\'”≤<>&%_:/;“'?+,~， （ ） º\\(\\)\\[\\.\\-]) (*([\u4E00-\u9FFF]|[\u00C0-\u0204]|[a-z]|[A-Z]|[0-9]|[\'” ≤<>&%_:/;“'?+,~， （ ） º\\(\\)\\[\\.\\-]))*$
threshold	No	Double	Threshold of metrics on the graph. **Value range:** 0-1.7976931348623157E308
threshold_enabled	Yes	Boolean	Whether to display thresholds of metrics. The value can be **true** (to display) and **false** (not to display).
view	Yes	String	Graph type. The value can be **bar**, **line**, **bar_chart**, **table**, **circular_bar**, or **area_chart**. Enumeration values: • **bar** • **line** • **bar_chart** • **table** • **circular_bar** • **area_chart**

Parameter	Mandatory	Type	Description
metric_display_mode	Yes	String	Metric display mode. The value can be **single** or **multiple**. Enumeration values: • **single** • **multiple**
properties	No	**properties** object	Additional information.
location	Yes	**location** object	Graph coordinates.
unit	No	String	Unit.

Table 6-424 WidgetMetric

Parameter	Mandatory	Type	Description
namespace	Yes	String	Service dimension. **Regex Pattern:** ^([a-z]|[A-Z]){1}([a-z]|[A-Z]|[0-9]|_)*\.([a-z]|[A-Z]){1}([a-z]|[A-Z]|[0-9]|_)*$
dimensions	Yes	**DimensionInfo** object	Dimension list.
metric_name	Yes	String	Metric name. Multiple metric names are separated by commas (,).
alias	No	Array of strings	Alias list of metrics on the graph.
extra_info	No	**ExtraInfo** object	Metric information.

Parameter	Mandatory	Type	Description
rollup_enable	No	Boolean	**Details**: Whether to enable aggregation. ** Restrictions** When RollupEnable is enabled, RollupFilter and RollupDimension are mandatory. ** Value Range** true indicates that aggregation is enabled. false indicates that aggregation is disabled. **Default value**: false
rollup_filter	No	String	Aggregation rule. The value can be **last**, **max**, **min**, **average**, or **sum**. Enumeration values: • **last** • **max** • **min** • **average** • **sum**
rollup_dimension	No	String	Aggregation dimension.
last_week_compare_enable	No	Boolean	Whether to display comparison data (same period last week). The value can be **true** or **false**.
yesterday_compare_enable	No	Boolean	Whether to display comparison data (same period yesterday). The value can be **true** or **false**.

Parameter	Mandatory	Type	Description
metric_dimension	No	String	Dimension name. Use commas (,) to separate multiple dimensions. For details about the dimensions supported by each cloud service, see **Services Interconnected with Cloud Eye**. **Regex Pattern:** ^([a-z]|[A-Z]){1}([a-z]|[A-Z]|[0-9]|_|-){0,31}(,([a-z]|[A-Z]){1}([a-z]|[A-Z]|[0-9]|_|-){0,31}){0,3}$
top_num	No	Integer	Number of displayed data records. **Value range:** 1-200
unit	No	String	Unit.
order	No	String	How resources of top *N* metrics are sorted on a graph. The value can be **asc** or **desc**. Enumeration values: • **asc** • **desc**
topn_metric_name	No	String	Metric name of a resource. The name must start with a letter and contain only digits, letters, and underscores. The length ranges from 1 to 64 characters. For example, **cpu_util** of an ECS indicates the CPU usage of the ECS. **mongo001_command_ps** in DDS indicates the command execution frequency. For details about the metric name of each service, see **Service metric name**.

Table 6-425 DimensionInfo

Parameter	Mandatory	Type	Description
name	Yes	String	Dimension name. Use commas (,) to separate multiple dimensions. For details about the dimensions supported by each cloud service, see **Services Interconnected with Cloud Eye**. **Regex Pattern:** ^([a-z]|[A-Z]){1}([a-z]|[A-Z]|[0-9]|_|-){0,31}(,([a-z]|[A-Z]){1}([a-z]|[A-Z]|[0-9]|_|-){0,31}){0,3}$
filter_type	Yes	String	Resource type. The value can be **all_instances** (all resources) or **specific_instances** (specified resources). Enumeration values: • **all_instances** • **specific_instances**
values	No	Array of strings	Dimension value list.

Table 6-426 ExtraInfo

Parameter	Mandatory	Type	Description
origin_metric_name	Yes	String	Metric name. **Regex Pattern:** ^([a-z]|[A-Z]|[0-9]|_|-|~|\.|/|:)*$
metric_prefix	No	String	Metric name prefix. **Regex Pattern:** ^([a-z]|[A-Z]|[0-9]|_|-|~|\.|/|:)*$
metric_type	No	String	Metric type. **Regex Pattern:** ^([a-z]|[A-Z]|[0-9]|_|-|~|\.|/|:)*$
custom_proc_name	No	String	Custom process name.

Table 6-427 properties

Parameter	Mandatory	Type	Description
filter	No	String	Aggregation type. Currently, the value can only be **TopN**. A line chart does not support this parameter. Enumeration values: • **topN**
topN	No	Integer	Top N values. In the line chart, this parameter indicates the number of time series data records that are randomly displayed. **Value range:** 1-2147483647 **Default value:** 100
order	No	String	Sorting field. The value can be **asc** (ascending order) or **desc** (descending order). A line chart does not support this parameter. Enumeration values: • **asc** • **desc**
description	No	String	Description of the graph.
last_week_compare_enable	No	Boolean	Whether to display comparison data (same period last week). The value can be **true** or **false**.
yesterday_compare_enable	No	Boolean	Whether to display comparison data (same period yesterday). The value can be **true** or **false**.
legend_location	No	String	Legend position flag. The value can be **hide**, **right**, or **bottom**. Tables do not support this parameter. Enumeration values: • **hide** • **right** • **bottom**

Parameter	Mandatory	Type	Description
legend_values	No	Array of strings	List of statistical values to be displayed in the legend for the current time series. This parameter is not supported in tables. For bar charts and bar charts, only **last** can be selected. Enumeration values: • **last** • **max** • **min** • **avg** • **sum**
thresholds	No	Array of **ThresholdInfo** objects	Threshold line configured for the graph.
is_all_compare_enable	No	Boolean	Whether to enable PoP (weekly/daily). The value can be **true** or **false**.

Table 6-428 ThresholdInfo

Parameter	Mandatory	Type	Description
threshold	Yes	Number	Threshold of the threshold line for the graph. **Value range:** 0-2147483647
threshold_color	Yes	String	Color of the threshold line for the graph, which can be purple (#B50E65), red (#F23030), orange (#FF8800), and yellow (#F2E70C). Enumeration values: • **#B50E65** • **#F23030** • **#FF8800** • **#F2E70C**

Table 6-429 location

Parameter	Mandatory	Type	Description
top	Yes	Integer	Grids between the graph and the top of the dashboard. **Value range:** 0-2147483647
left	Yes	Integer	Grids between the graph and the left side of the dashboard. **Value range:** 0-9
width	Yes	Integer	Graph width. **Value range:** 3-12
height	Yes	Integer	Graph height. **Value range:** 3-2147483647

Response Parameters

Status code: 200

Table 6-430 Response body parameters

Parameter	Type	Description
widget_ids	Array of strings	Response body for creating graphs in batches.

Status code: 400

Table 6-431 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 401

Table 6-432 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 500

Table 6-433 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Example Requests

```
[ {
  "metrics" : [ {
    "namespace" : "SYS.ECS",
    "dimensions" : {
      "name" : "instance_id",
      "filter_type" : "all_instances"
    },
    "metric_name" : "cpu_util",
    "alias" : [ "cpuutilalias" ],
    "extra_info" : {
      "origin_metric_name" : "cpu_util",
      "metric_prefix" : "cpu",
      "metric_type" : "type",
      "custom_proc_name" : "app.sh"
    }
  } ],
  "view" : "bar",
  "metric_display_mode" : "single",
  "threshold" : 0.7,
  "threshold_enabled" : true,
  "title" : "widget_title",
  "properties" : {
    "filter" : "topN",
    "topN" : 100,
    "order" : "desc"
  },
  "location" : {
    "left" : 0,
    "top" : 0,
    "width" : 4,
    "height" : 3
  },
  "unit" : "%"
} ]
```


Example Responses

Status code: 200

OK

```
{
  "widget_ids" : [ "wgx234567890123456789012" ]
}
```

Status Codes

Status Code	Description
200	OK
400	The server failed to process the request.
401	Token authentication is required.
500	Failed to complete the request because of an internal server error.

Error Codes

See **Error Codes**.

6.13.2 Querying Graphs Added to a Dashboard

Function

This API is used to query graphs on a dashboard.

Constraints

This API is not supported in the following regions: CN East-Qingdao, LA-Mexico City1, TR-Istanbul, AP-Jakarta, ME-Riyadh, and AP-Manila.

Debugging

You can debug this API through automatic authentication in **API Explorer** or use the SDK sample code generated by API Explorer.

URI

GET /v2/{project_id}/dashboards/{dashboard_id}/widgets

Table 6-434 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	**Definition** Tenant ID. **Constraints**: None **Value range**: Project ID, used to specify the project that an asset belongs to. You can query the assets of a project by project ID. You can obtain the project ID by calling an API or on the console. For details, see **Obtaining a Project ID**. The value must contain of 1 to 64 characters. **Default value**: None
dashboard_id	Yes	String	Dashboard ID, which starts with **db** and follows 22 letters and digits. Example: **db16564943172807wjOmoLyn**. **Regex Pattern:** ^db([a-z]|[A-Z]|[0-9]){22}$

Table 6-435 Query Parameters

Parameter	Mandatory	Type	Description
group_id	No	String	ID of the group that the graph belongs to. **Regex Pattern:** ^dg([a-z]|[A-Z]|[0-9]){22}|default$

Request Parameters

Table 6-436 Request header parameters

Parameter	Mandatory	Type	Description
Content-Type	No	String	**Definition** MIME type of the request body. **Constraints**: None **Value range**: The value can contain 1 to 64 characters. **Default value**: The default type is **application/json; charset=UTF-8**. **Default value:** application/json; charset=UTF-8
X-Auth-Token	No	String	**Definition** User token. **Constraints**: None **Value range**: The value can contain 1 to 16,384 characters. **Default value**: None

Response Parameters

Status code: 200

Table 6-437 Response body parameters

Parameter	Type	Description
widgets	Array of **WidgetInfoWithId** objects	Graph list.

Table 6-438 WidgetInfoWithId

Parameter	Type	Description
widget_id	String	Graph ID. **Regex Pattern:** ^wg([a-z]|[A-Z]|[0-9]){22}$
group_id	String	Graph partition ID. **Regex Pattern:** ^dg([a-z]|[A-Z]|[0-9]){22}|default$
metrics	Array of **WidgetMetric** objects	Metric list.
title	String	Graph name. **Regex Pattern:** ^([\u4E00-\u9FFF]|[\u00C0-\u0204]|[a-z]|[A-Z]|[0-9]|[\'" ≤<>&%_:/;“'?+,~，（）°\\(\\)\\[\\.\\-]) (*([\u4E00-\u9FFF]|[\u00C0-\u0204]|[a-z]|[A-Z]|[0-9]|[\'"≤<>&%_:/;“'?+,~，（）°\\(\\)\\[\\.\\-]))*$
threshold	Double	Threshold of metrics on the graph. **Value range:** 0-1.7976931348623157E308
threshold_enabled	Boolean	Whether to display thresholds of metrics. The value can be **true** (to display) and **false** (not to display).
view	String	Graph type. The value can be **bar**, **line**, **bar_chart**, **table**, **circular_bar**, or **area_chart**. Enumeration values: • **bar** • **line** • **bar_chart** • **table** • **circular_bar** • **area_chart**
metric_display_mode	String	Metric display mode. The value can be **single** or **multiple**. Enumeration values: • **single** • **multiple**
properties	**properties** object	Additional information.

Parameter	Type	Description
location	**location** object	Graph coordinates.
unit	String	Unit.
create_time	Long	Dashboard creation time. **Value range:** 1111111111111-9999999999999

Table 6-439 WidgetMetric

Parameter	Type	Description
namespace	String	Service dimension. **Regex Pattern:** ^([a-z]|[A-Z]){1}([a-z]|[A-Z]|[0-9]|_)*\.([a-z]|[A-Z]){1}([a-z]|[A-Z]|[0-9]|_)*$
dimensions	**DimensionInfo** object	Dimension list.
metric_name	String	Metric name. Multiple metric names are separated by commas (,).
alias	Array of strings	Alias list of metrics on the graph.
extra_info	**ExtraInfo** object	Metric information.
rollup_enable	Boolean	**Details**: Whether to enable aggregation. ** Restrictions** When RollupEnable is enabled, RollupFilter and RollupDimension are mandatory. ** Value Range** true indicates that aggregation is enabled. false indicates that aggregation is disabled. **Default value**: false

Parameter	Type	Description
rollup_filter	String	Aggregation rule. The value can be **last**, **max**, **min**, **average**, or **sum**. Enumeration values: • **last** • **max** • **min** • **average** • **sum**
rollup_dimension	String	Aggregation dimension.
last_week_compare_enable	Boolean	Whether to display comparison data (same period last week). The value can be **true** or **false**.
yesterday_compare_enable	Boolean	Whether to display comparison data (same period yesterday). The value can be **true** or **false**.
metric_dimension	String	Dimension name. Use commas (,) to separate multiple dimensions. For details about the dimensions supported by each cloud service, see **Services Interconnected with Cloud Eye**. **Regex Pattern:** ^([a-z]|[A-Z]){1}([a-z]|[A-Z]|[0-9]|_|-){0,31}(,([a-z]|[A-Z]){1}([a-z]|[A-Z]|[0-9]|_|-){0,31}){0,3}$
top_num	Integer	Number of displayed data records. **Value range:** 1-200
unit	String	Unit.
order	String	How resources of top *N* metrics are sorted on a graph. The value can be **asc** or **desc**. Enumeration values: • **asc** • **desc**

Parameter	Type	Description
topn_metric_name	String	Metric name of a resource. The name must start with a letter and contain only digits, letters, and underscores. The length ranges from 1 to 64 characters. For example, **cpu_util** of an ECS indicates the CPU usage of the ECS. **mongo001_command_ps** in DDS indicates the command execution frequency. For details about the metric name of each service, see **Service metric name**.

Table 6-440 DimensionInfo

Parameter	Type	Description
name	String	Dimension name. Use commas (,) to separate multiple dimensions. For details about the dimensions supported by each cloud service, see **Services Interconnected with Cloud Eye**. **Regex Pattern:** ^([a-z]|[A-Z]){1}([a-z]|[A-Z]|[0-9]|_|-){0,31}(,([a-z]|[A-Z]){1}([a-z]|[A-Z]|[0-9]|_|-){0,31}){0,3}$
filter_type	String	Resource type. The value can be **all_instances** (all resources) or **specific_instances** (specified resources). Enumeration values: • **all_instances** • **specific_instances**
values	Array of strings	Dimension value list.

Table 6-441 ExtraInfo

Parameter	Type	Description
origin_metric_name	String	Metric name. **Regex Pattern:** ^([a-z]|[A-Z]|[0-9]|_|-|~|\.|/|:)*$

Parameter	Type	Description
metric_prefix	String	Metric name prefix. **Regex Pattern:** ^([a-z]|[A-Z]|[0-9]|_|-|~|\.|/|:)*$
metric_type	String	Metric type. **Regex Pattern:** ^([a-z]|[A-Z]|[0-9]|_|-|~|\.|/|:)*$
custom_proc_name	String	Custom process name.

Table 6-442 properties

Parameter	Type	Description
filter	String	Aggregation type. Currently, the value can only be **TopN**. A line chart does not support this parameter. Enumeration values: • **topN**
topN	Integer	Top N values. In the line chart, this parameter indicates the number of time series data records that are randomly displayed. **Value range:** 1-2147483647 **Default value:** 100
order	String	Sorting field. The value can be **asc** (ascending order) or **desc** (descending order). A line chart does not support this parameter. Enumeration values: • **asc** • **desc**
description	String	Description of the graph.
last_week_compare_enable	Boolean	Whether to display comparison data (same period last week). The value can be **true** or **false**.
yesterday_compare_enable	Boolean	Whether to display comparison data (same period yesterday). The value can be **true** or **false**.

Parameter	Type	Description
legend_location	String	Legend position flag. The value can be **hide**, **right**, or **bottom**. Tables do not support this parameter. Enumeration values: • **hide** • **right** • **bottom**
legend_values	Array of strings	List of statistical values to be displayed in the legend for the current time series. This parameter is not supported in tables. For bar charts and bar charts, only **last** can be selected. Enumeration values: • **last** • **max** • **min** • **avg** • **sum**
thresholds	Array of **ThresholdInfo** objects	Threshold line configured for the graph.
is_all_compare_enable	Boolean	Whether to enable PoP (weekly/daily). The value can be **true** or **false**.

Table 6-443 ThresholdInfo

Parameter	Type	Description
threshold	Number	Threshold of the threshold line for the graph. **Value range:** 0-2147483647
threshold_color	String	Color of the threshold line for the graph, which can be purple (#B50E65), red (#F23030), orange (#FF8800), and yellow (#F2E70C). Enumeration values: • **#B50E65** • **#F23030** • **#FF8800** • **#F2E70C**

Table 6-444 location

Parameter	Type	Description
top	Integer	Grids between the graph and the top of the dashboard. **Value range:** 0-2147483647
left	Integer	Grids between the graph and the left side of the dashboard. **Value range:** 0-9
width	Integer	Graph width. **Value range:** 3-12
height	Integer	Graph height. **Value range:** 3-2147483647

Status code: 400

Table 6-445 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 401

Table 6-446 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.

Parameter	Type	Description
request_id	String	Request ID.

Status code: 500

Table 6-447 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Example Requests

None

Example Responses

Status code: 200

OK

```
[ {
  "widget_id" : "wg123456789012345678901 2",
  "metrics" : [ {
    "namespace" : "SYS.ECS",
    "dimensions" : {
      "name" : "instance_id",
      "filter_type" : "all_instances",
      "metric_name" : "cpu_util",
      "alias" : [ "cpuutilalias" ],
      "extra_info" : {
        "origin_metric_name" : "cpu_util",
        "metric_prefix" : "cpu",
        "metric_type" : "type",
        "custom_proc_name" : "app.sh"
      }
    }
  } ],
  "view" : "bar",
  "metric_display_mode" : "single",
  "threshold" : 0.7,
  "threshold_enabled" : true,
  "title" : "widget_title",
  "properties" : {
    "filter" : "topN",
    "topN" : 100,
    "order" : "desc"
  },
  "location" : {
    "left" : 0,
    "top" : 0,
    "width" : 4,
```

```
    "height" : 3
  },
  "unit" : "%",
  "create_time" : 1111111111111
} ]
```

Status Codes

Status Code	Description
200	OK
400	The server failed to process the request.
401	Token authentication is required.
500	Failed to complete the request because of an internal server error.

Error Codes

See **Error Codes**.

6.13.3 Querying Information About a Graph

Function

This API is used to query information about a graph.

Constraints

This API is not supported in the following regions: CN East-Qingdao, LA-Mexico City1, TR-Istanbul, AP-Jakarta, ME-Riyadh, and AP-Manila.

Debugging

You can debug this API through automatic authentication in **API Explorer** or use the SDK sample code generated by API Explorer.

URI

GET /v2/{project_id}/widgets/{widget_id}

Table 6-448 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	**Definition** Tenant ID. **Constraints**: None **Value range**: Project ID, used to specify the project that an asset belongs to. You can query the assets of a project by project ID. You can obtain the project ID by calling an API or on the console. For details, see **Obtaining a Project ID**. The value must contain of 1 to 64 characters. **Default value**: None
widget_id	Yes	String	Graph ID. **Regex Pattern:** ^wg([a-z]|[A-Z]|[0-9]){22}$

Request Parameters

Table 6-449 Request header parameters

Parameter	Mandatory	Type	Description
Content-Type	No	String	**Definition** MIME type of the request body. **Constraints**: None **Value range**: The value can contain 1 to 64 characters. **Default value**: The default type is **application/json; charset=UTF-8**. **Default value:** application/json; charset=UTF-8
X-Auth-Token	No	String	**Definition** User token. **Constraints**: None **Value range**: The value can contain 1 to 16,384 characters. **Default value**: None

Response Parameters

Status code: 200

Table 6-450 Response body parameters

Parameter	Type	Description
widget_id	String	Graph ID. **Regex Pattern:** ^wg([a-z]|[A-Z]|[0-9]){22}$

Parameter	Type	Description
group_id	String	Graph partition ID. **Regex Pattern:** ^dg([a-z]|[A-Z]|[0-9]){22}|default$
metrics	Array of **WidgetMetric** objects	Metric list.
title	String	Graph name. **Regex Pattern:** ^([\u4E00-\u9FFF]|[\u00C0-\u0204]|[a-z]|[A-Z]|[0-9]|[\'" ≤<>&%_:/;“'?+,~， （ ） º\\(\\)\\[\\.\\-]) (*([\u4E00-\u9FFF]|[\u00C0-\u0204]|[a-z]|[A-Z]|[0-9]|[\'"≤<>&%_:/;“'?+,~， （ ） º\\(\\)\\[\\.\\-]))*$
threshold	Double	Threshold of metrics on the graph. **Value range:** 0-1.7976931348623157E308
threshold_enabled	Boolean	Whether to display thresholds of metrics. The value can be **true** (to display) and **false** (not to display).
view	String	Graph type. The value can be **bar**, **line**, **bar_chart**, **table**, **circular_bar**, or **area_chart**. Enumeration values: • **bar** • **line** • **bar_chart** • **table** • **circular_bar** • **area_chart**
metric_display_mode	String	Metric display mode. The value can be **single** or **multiple**. Enumeration values: • **single** • **multiple**
properties	**properties** object	Additional information.
location	**location** object	Graph coordinates.
unit	String	Unit.

Parameter	Type	Description
create_time	Long	Dashboard creation time. **Value range:** 1111111111111-9999999999999

Table 6-451 WidgetMetric

Parameter	Type	Description
namespace	String	Service dimension. **Regex Pattern:** ^([a-z]|[A-Z]){1}([a-z]|[A-Z]|[0-9]|_)*\.([a-z]|[A-Z]){1}([a-z]|[A-Z]|[0-9]|_)*$
dimensions	**DimensionInfo** object	Dimension list.
metric_name	String	Metric name. Multiple metric names are separated by commas (,).
alias	Array of strings	Alias list of metrics on the graph.
extra_info	**ExtraInfo** object	Metric information.
rollup_enable	Boolean	**Details**: Whether to enable aggregation. ** Restrictions** When RollupEnable is enabled, RollupFilter and RollupDimension are mandatory. ** Value Range** true indicates that aggregation is enabled. false indicates that aggregation is disabled. **Default value**: false
rollup_filter	String	Aggregation rule. The value can be **last**, **max**, **min**, **average**, or **sum**. Enumeration values: • **last** • **max** • **min** • **average** • **sum**
rollup_dimension	String	Aggregation dimension.

Parameter	Type	Description
last_week_compare_enable	Boolean	Whether to display comparison data (same period last week). The value can be **true** or **false**.
yesterday_compare_enable	Boolean	Whether to display comparison data (same period yesterday). The value can be **true** or **false**.
metric_dimension	String	Dimension name. Use commas (,) to separate multiple dimensions. For details about the dimensions supported by each cloud service, see **Services Interconnected with Cloud Eye**. **Regex Pattern:** ^([a-z]|[A-Z]){1}([a-z]|[A-Z]|[0-9]|_|-){0,31}(,([a-z]|[A-Z]){1}([a-z]|[A-Z]|[0-9]|_|-){0,31}){0,3}$
top_num	Integer	Number of displayed data records. **Value range:** 1-200
unit	String	Unit.
order	String	How resources of top *N* metrics are sorted on a graph. The value can be **asc** or **desc**. Enumeration values: • **asc** • **desc**
topn_metric_name	String	Metric name of a resource. The name must start with a letter and contain only digits, letters, and underscores. The length ranges from 1 to 64 characters. For example, **cpu_util** of an ECS indicates the CPU usage of the ECS. **mongo001_command_ps** in DDS indicates the command execution frequency. For details about the metric name of each service, see **Service metric name**.

Table 6-452 DimensionInfo

Parameter	Type	Description
name	String	Dimension name. Use commas (,) to separate multiple dimensions. For details about the dimensions supported by each cloud service, see **Services Interconnected with Cloud Eye**. **Regex Pattern:** ^([a-z]|[A-Z]){1}([a-z]|[A-Z]|[0-9]|_|-){0,31}(,([a-z]|[A-Z]){1}([a-z]|[A-Z]|[0-9]|_|-){0,31}){0,3}$
filter_type	String	Resource type. The value can be **all_instances** (all resources) or **specific_instances** (specified resources). Enumeration values: • **all_instances** • **specific_instances**
values	Array of strings	Dimension value list.

Table 6-453 ExtraInfo

Parameter	Type	Description
origin_metric_name	String	Metric name. **Regex Pattern:** ^([a-z]|[A-Z]|[0-9]|_|-|~|\.|/|:)*$
metric_prefix	String	Metric name prefix. **Regex Pattern:** ^([a-z]|[A-Z]|[0-9]|_|-|~|\.|/|:)*$
metric_type	String	Metric type. **Regex Pattern:** ^([a-z]|[A-Z]|[0-9]|_|-|~|\.|/|:)*$
custom_proc_name	String	Custom process name.

Table 6-454 properties

Parameter	Type	Description
filter	String	Aggregation type. Currently, the value can only be **TopN**. A line chart does not support this parameter. Enumeration values: • **topN**
topN	Integer	Top N values. In the line chart, this parameter indicates the number of time series data records that are randomly displayed. **Value range:** 1-2147483647 **Default value:** 100
order	String	Sorting field. The value can be **asc** (ascending order) or **desc** (descending order). A line chart does not support this parameter. Enumeration values: • **asc** • **desc**
description	String	Description of the graph.
last_week_compare_enable	Boolean	Whether to display comparison data (same period last week). The value can be **true** or **false**.
yesterday_compare_enable	Boolean	Whether to display comparison data (same period yesterday). The value can be **true** or **false**.
legend_location	String	Legend position flag. The value can be **hide**, **right**, or **bottom**. Tables do not support this parameter. Enumeration values: • **hide** • **right** • **bottom**

Parameter	Type	Description
legend_values	Array of strings	List of statistical values to be displayed in the legend for the current time series. This parameter is not supported in tables. For bar charts and bar charts, only **last** can be selected. Enumeration values: • **last** • **max** • **min** • **avg** • **sum**
thresholds	Array of **ThresholdInfo** objects	Threshold line configured for the graph.
is_all_compare_enable	Boolean	Whether to enable PoP (weekly/daily). The value can be **true** or **false**.

Table 6-455 ThresholdInfo

Parameter	Type	Description
threshold	Number	Threshold of the threshold line for the graph. **Value range:** 0-2147483647
threshold_color	String	Color of the threshold line for the graph, which can be purple (#B50E65), red (#F23030), orange (#FF8800), and yellow (#F2E70C). Enumeration values: • **#B50E65** • **#F23030** • **#FF8800** • **#F2E70C**

Table 6-456 location

Parameter	Type	Description
top	Integer	Grids between the graph and the top of the dashboard. **Value range:** 0-2147483647
left	Integer	Grids between the graph and the left side of the dashboard. **Value range:** 0-9
width	Integer	Graph width. **Value range:** 3-12
height	Integer	Graph height. **Value range:** 3-2147483647

Status code: 400

Table 6-457 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 401

Table 6-458 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 500

Table 6-459 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Example Requests

None

Example Responses

Status code: 200

OK


```
{
  "widget_id" : "wg123456789012345678901 2",
  "metrics" : [ {
    "namespace" : "SYS.ECS",
    "dimensions" : {
      "name" : "instance_id",
      "filter_type" : "all_instances"
    },
    "metric_name" : "cpu_util",
    "alias" : [ "cpuutilalias" ],
    "extra_info" : {
      "origin_metric_name" : "cpu_util",
      "metric_prefix" : "cpu",
      "metric_type" : "type",
      "custom_proc_name" : "app.sh"
    }
  } ],
  "view" : "bar",
  "metric_display_mode" : "single",
  "threshold" : 0.7,
  "threshold_enabled" : true,
  "title" : "widget_title",
  "properties" : {
    "filter" : "topN",
    "topN" : 100,
    "order" : "desc",
    "description" : "Simple example.",
    "last_week_compare_enable" : false,
    "yesterday_compare_enable" : false,
    "legend_location" : "right",
    "legend_values" : [ "max", "min" ],
    "thresholds" : [ {
      "threshold" : 90,
      "threshold_color" : "#F23030"
    } ]
  },
  "location" : {
    "left" : 0,
    "top" : 0,
```

```
    "width" : 4,
    "height" : 3
  },
  "unit" : "%",
  "create_time" : 1111111111111
}
```

Status Codes

Status Code	Description
200	OK
400	The server failed to process the request.
401	Token authentication is required.
500	Failed to complete the request because of an internal server error.

Error Codes

See **Error Codes**.

6.13.4 Deleting a Graph

Function

This API is used to delete a graph.

Constraints

This API is not supported in the following regions: CN East-Qingdao, LA-Mexico City1, TR-Istanbul, AP-Jakarta, ME-Riyadh, and AP-Manila.

Debugging

You can debug this API through automatic authentication in **API Explorer** or use the SDK sample code generated by API Explorer.

URI

DELETE /v2/{project_id}/widgets/{widget_id}

Table 6-460 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	**Definition** Tenant ID. **Constraints**: None **Value range**: Project ID, used to specify the project that an asset belongs to. You can query the assets of a project by project ID. You can obtain the project ID by calling an API or on the console. For details, see **Obtaining a Project ID**. The value must contain of 1 to 64 characters. **Default value**: None
widget_id	Yes	String	Graph ID. **Regex Pattern:** ^wg([a-z]|[A-Z]|[0-9]){22}$

Request Parameters

Table 6-461 Request header parameters

Parameter	Mandatory	Type	Description
Content-Type	No	String	**Definition** MIME type of the request body. **Constraints**: None **Value range**: The value can contain 1 to 64 characters. **Default value**: The default type is **application/json; charset=UTF-8**. **Default value:** application/json; charset=UTF-8
X-Auth-Token	No	String	**Definition** User token. **Constraints**: None **Value range**: The value can contain 1 to 16,384 characters. **Default value**: None

Response Parameters

Status code: 204

No Content

Status code: 400

Table 6-462 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.

Parameter	Type	Description
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 401

Table 6-463 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 500

Table 6-464 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
204	No Content
400	The server failed to process the request.

Status Code	Description
401	Token authentication is required.
500	Failed to complete the request because of an internal server error.

Error Codes

See **Error Codes**.

6.13.5 Updating Graphs in Batches

Function

This API is used to update graphs in batches.

Constraints

This API is not supported in the following regions: CN East-Qingdao, LA-Mexico City1, TR-Istanbul, AP-Jakarta, ME-Riyadh, and AP-Manila.

Debugging

You can debug this API through automatic authentication in **API Explorer** or use the SDK sample code generated by API Explorer.

URI

POST /v2/{project_id}/widgets/batch-update

Table 6-465 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	**Definition** Tenant ID. **Constraints**: None **Value range**: Project ID, used to specify the project that an asset belongs to. You can query the assets of a project by project ID. You can obtain the project ID by calling an API or on the console. For details, see **Obtaining a Project ID**. The value must contain of 1 to 64 characters. **Default value**: None

Request Parameters

Table 6-466 Request header parameters

Parameter	Mandatory	Type	Description
Content-Type	No	String	**Definition** MIME type of the request body. **Constraints**: None **Value range**: The value can contain 1 to 64 characters. **Default value**: The default type is **application/json; charset=UTF-8**. **Default value:** application/json; charset=UTF-8

Parameter	Mandatory	Type	Description
X-Auth-Token	No	String	**Definition** User token. **Constraints**: None **Value range**: The value can contain 1 to 16,384 characters. **Default value**: None

Table 6-467 Request body parameters

Parameter	Mandatory	Type	Description
[items]	Yes	Array of **UpdateWidgetInfo** objects	List of graphs to be modified.

Table 6-468 UpdateWidgetInfo

Parameter	Mandatory	Type	Description
group_id	No	String	Graph partition ID. **Regex Pattern:** ^dg([a-z]|[A-Z]|[0-9]){22}|default$
widget_id	Yes	String	Graph ID. **Regex Pattern:** ^wg([a-z]|[A-Z]|[0-9]){22}$
metrics	No	Array of **WidgetMetric** objects	Metric list.
title	No	String	Graph name. **Regex Pattern:** ^([\u4E00-\u9FFF]|[a-z]|[A-Z]|[0-9]|_|-|:|;|\(|\)|\.|~| (|))+$
threshold	No	Double	Threshold of metrics on the graph. **Value range:** 0-1.7976931348623157E308

Parameter	Mandatory	Type	Description
threshold_enabled	No	Boolean	Whether to display thresholds of metrics. The value can be **true** (to display) and **false** (not to display).
view	No	String	Graph type. The value can be **bar**, **line**, **bar_chart**, **table**, **circular_bar**, or **area_chart**. Enumeration values: • **bar** • **line** • **bar_chart** • **table** • **circular_bar** • **area_chart**
metric_display_mode	No	String	Metric display mode. The value can be **single** or **multiple**. Enumeration values: • **single** • **multiple**
properties	No	**properties** object	Graph display configuration.
location	No	**location** object	Graph coordinates.
unit	No	String	Unit.

Table 6-469 WidgetMetric

Parameter	Mandatory	Type	Description
namespace	Yes	String	Service dimension. **Regex Pattern:** ^([a-z]|[A-Z]){1}([a-z]|[A-Z]|[0-9]|_)*\.([a-z]|[A-Z]){1}([a-z]|[A-Z]|[0-9]|_)*$
dimensions	Yes	**DimensionInfo** object	Dimension list.
metric_name	Yes	String	Metric name. Multiple metric names are separated by commas (,).

Parameter	Mandatory	Type	Description
alias	No	Array of strings	Alias list of metrics on the graph.
extra_info	No	**ExtraInfo** object	Metric information.
rollup_enable	No	Boolean	**Details**: Whether to enable aggregation. ** Restrictions** When RollupEnable is enabled, RollupFilter and RollupDimension are mandatory. ** Value Range** true indicates that aggregation is enabled. false indicates that aggregation is disabled. **Default value**: false
rollup_filter	No	String	Aggregation rule. The value can be **last**, **max**, **min**, **average**, or **sum**. Enumeration values: • **last** • **max** • **min** • **average** • **sum**
rollup_dimension	No	String	Aggregation dimension.
last_week_compare_enable	No	Boolean	Whether to display comparison data (same period last week). The value can be **true** or **false**.
yesterday_compare_enable	No	Boolean	Whether to display comparison data (same period yesterday). The value can be **true** or **false**.

Parameter	Mandatory	Type	Description
metric_dimension	No	String	Dimension name. Use commas (,) to separate multiple dimensions. For details about the dimensions supported by each cloud service, see **Services Interconnected with Cloud Eye**. **Regex Pattern:** ^([a-z]|[A-Z]){1}([a-z]|[A-Z]|[0-9]|_|-){0,31}(,([a-z]|[A-Z]){1}([a-z]|[A-Z]|[0-9]|_|-){0,31}){0,3}$
top_num	No	Integer	Number of displayed data records. **Value range:** 1-200
unit	No	String	Unit.
order	No	String	How resources of top *N* metrics are sorted on a graph. The value can be **asc** or **desc**. Enumeration values: • **asc** • **desc**
topn_metric_name	No	String	Metric name of a resource. The name must start with a letter and contain only digits, letters, and underscores. The length ranges from 1 to 64 characters. For example, **cpu_util** of an ECS indicates the CPU usage of the ECS. **mongo001_command_ps** in DDS indicates the command execution frequency. For details about the metric name of each service, see **Service metric name**.

Table 6-470 DimensionInfo

Parameter	Mandatory	Type	Description
name	Yes	String	Dimension name. Use commas (,) to separate multiple dimensions. For details about the dimensions supported by each cloud service, see **Services Interconnected with Cloud Eye**. **Regex Pattern:** ^([a-z]|[A-Z]){1}([a-z]|[A-Z]|[0-9]|_|-){0,31}(,([a-z]|[A-Z]){1}([a-z]|[A-Z]|[0-9]|_|-){0,31}){0,3}$
filter_type	Yes	String	Resource type. The value can be **all_instances** (all resources) or **specific_instances** (specified resources). Enumeration values: • **all_instances** • **specific_instances**
values	No	Array of strings	Dimension value list.

Table 6-471 ExtraInfo

Parameter	Mandatory	Type	Description
origin_metric_name	Yes	String	Metric name. **Regex Pattern:** ^([a-z]|[A-Z]|[0-9]|_|-|~|\.|/|:)*$
metric_prefix	No	String	Metric name prefix. **Regex Pattern:** ^([a-z]|[A-Z]|[0-9]|_|-|~|\.|/|:)*$
metric_type	No	String	Metric type. **Regex Pattern:** ^([a-z]|[A-Z]|[0-9]|_|-|~|\.|/|:)*$
custom_proc_name	No	String	Custom process name.

Table 6-472 properties

Parameter	Mandatory	Type	Description
filter	No	String	Aggregation type. Currently, the value can only be **TopN**. A line chart does not support this parameter. Enumeration values: • **topN**
topN	No	Integer	Top *N* values. In a line chart, this parameter indicates the number of time series data records that are randomly displayed. **Value range:** 1-2147483647 **Default value:** 100
order	No	String	Sorting field. The value can be **asc** (ascending order) or **desc** (descending order). A line chart does not support this parameter. Enumeration values: • **asc** • **desc**
description	No	String	Description of the graph.
last_week_compare_enable	No	Boolean	Whether to display comparison data (same period last week). The value can be **true** or **false**.
yesterday_compare_enable	No	Boolean	Whether to display comparison data (same period yesterday). The value can be **true** or **false**.
legend_location	No	String	Legend position flag. The value can be **hide**, **right**, or **bottom**. Tables do not support this parameter. Enumeration values: • **hide** • **right** • **bottom**

Parameter	Mandatory	Type	Description
legend_values	No	Array of strings	List of statistical values to be displayed in the legend for the current time series. This parameter is not supported in tables. For bar charts and bar charts, only **last** can be selected. Enumeration values: • **last** • **max** • **min** • **avg** • **sum**
thresholds	No	Array of **ThresholdInfo** objects	Threshold line configured for the graph.
is_all_compare_enable	No	Boolean	Whether to enable PoP comparison. The value can be **true** or **false**.

Table 6-473 ThresholdInfo

Parameter	Mandatory	Type	Description
threshold	Yes	Number	Threshold of the threshold line for the graph. **Value range:** 0-2147483647
threshold_color	Yes	String	Color of the threshold line for the graph, which can be purple (#B50E65), red (#F23030), orange (#FF8800), and yellow (#F2E70C). Enumeration values: • **#B50E65** • **#F23030** • **#FF8800** • **#F2E70C**

Table 6-474 location

Parameter	Mandatory	Type	Description
top	Yes	Integer	Grids between the graph and the top of the dashboard. **Value range:** 0-2147483647
left	Yes	Integer	Grids between the graph and the left side of the dashboard. **Value range:** 0-9
width	Yes	Integer	Graph width. **Value range:** 3-12
height	Yes	Integer	Graph height. **Value range:** 3-2147483647

Response Parameters

Status code: 200

Table 6-475 Response body parameters

Parameter	Type	Description
widgets	Array of **BatchUpdateWidgetInfo** objects	Update result list.

Table 6-476 BatchUpdateWidgetInfo

Parameter	Type	Description
widget_id	String	Graph ID. **Regex Pattern:** ^wg([a-z]|[A-Z]|[0-9]){22}$
ret_status	String	Update result. The value can be **successful** or **error**. Enumeration values: • **successful** • **error**

Parameter	Type	Description
error_msg	String	Error message when an operation fails.

Status code: 400

Table 6-477 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 401

Table 6-478 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 500

Table 6-479 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Example Requests

```
[ {
  "widget_id" : "wgXXXXXXXXXXXXXXXXXXXXXX",
  "metrics" : [ {
    "namespace" : "SYS.ECS",
```

```
   "dimensions" : {
     "name" : "instance_id",
     "filter_type" : "all_instances"
   },
   "metric_name" : "cpu_util",
   "alias" : [ "cpuutilalias" ],
   "extra_info" : {
     "origin_metric_name" : "cpu_util",
     "metric_prefix" : "cpu",
     "metric_type" : "type",
     "custom_proc_name" : "app.sh"
   }
  } ],
  "view" : "bar",
  "metric_display_mode" : "single",
  "threshold" : 500,
  "threshold_enabled" : false,
  "title" : "widget_title_new",
  "properties" : {
   "filter" : "topN",
   "topN" : 10,
   "order" : "asc"
  },
  "location" : {
   "left" : 0,
   "top" : 3,
   "width" : 4,
   "height" : 3
  },
  "unit" : "%"
} ]
```

Example Responses

Status code: 200

OK

```
{
  "widgets" : [ {
    "widget_id" : "wgXXXXXXXXXXXXXXXXXXXXXX",
    "ret_status" : "successful"
  }, {
    "widget_id" : "wg987654321012345678 9012",
    "ret_status" : "error",
    "error_msg" : "record not found"
  } ]
}
```

Status Codes

Status Code	Description
200	OK
400	The server failed to process the request.
401	Token authentication is required.
500	Failed to complete the request because of an internal server error.

Error Codes

See **Error Codes**.

6.14 Resource Tag Management

6.14.1 Querying Tags for a Specified Resource Type in a Cloud Eye Project

Function

This API is used to query tags of a type of resources in a Cloud Eye project.

Debugging

You can debug this API through automatic authentication in **API Explorer** or use the SDK sample code generated by API Explorer.

URI

GET /v2/{project_id}/{resource_type}/tags

Table 6-480 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	**Definition** Tenant ID. **Constraints**: None **Value range**: Project ID, used to specify the project that an asset belongs to. You can query the assets of a project by project ID. You can obtain the project ID by calling an API or on the console. For details, see **Obtaining a Project ID**. The value must contain of 1 to 64 characters. **Default value**: None

Parameter	Mandatory	Type	Description
resource_type	Yes	String	Resource type. **CES-alarm** indicates alarm rules. Enumeration values: • **CES-alarm**

Request Parameters

Table 6-481 Request header parameters

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	**Definition** MIME type of the request body. **Constraints**: None **Value range**: The value can contain 1 to 64 characters. **Default value**: The default type is **application/json; charset=UTF-8**. **Default value:** application/json; charset=UTF-8
X-Auth-Token	Yes	String	**Definition** User token. **Constraints**: None **Value range**: The value can contain 1 to 16,384 characters. **Default value**: None

Response Parameters

Status code: 200

Table 6-482 Response body parameters

Parameter	Type	Description
tags	Array of **Tag** objects	Tenant tags.

Table 6-483 Tag

Parameter	Type	Description
key	String	Tag key. The value can contain up to 128 Unicode characters. The key cannot be empty.
values	Array of strings	Tag values. Each value can contain a maximum of 255 Unicode characters. If **values** is not specified, any parameter value can be queried.

Status code: 404

Table 6-484 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Example Requests

None

Example Responses

Status code: 200

OK

```
{
  "tags" : [ {
    "key" : "key1",
    "values" : [ "value1", "value2" ]
  }, {
    "key" : "key2",
    "values" : [ "value1", "value2" ]
  } ]
}
```


Status Codes

Status Code	Description
200	OK
404	Resource not found.

Error Codes

See **Error Codes**.

6.15 Metric Management

6.15.1 Querying the Original Dimension Values in Server Monitoring

Function

This API is used to query the original dimension value based on the ECS/BMS resource ID and special dimension value for disks, mount points, processes, GPUs, and RAID controllers. This API is not required for other dimensions.

Debugging

You can debug this API through automatic authentication in **API Explorer** or use the SDK sample code generated by API Explorer.

URI

GET /v2/{project_id}/instances/{instance_id}/agent-dimensions

Table 6-485 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	**Definition** Tenant ID. **Constraints**: None **Value range**: Project ID, used to specify the project that an asset belongs to. You can query the assets of a project by project ID. You can obtain the project ID by calling an API or on the console. For details, see **Obtaining a Project ID**. The value must contain of 1 to 64 characters. **Default value**: None
instance_id	Yes	String	**Description** Resource ID, for example, **4270ff17-aba3-4138-89fa-820594c39755**. **Constraints**: None **Value range**: The value can contain a maximum of 36 characters. **Default value**: None **Regex Pattern:** ^([a-z]|[A-Z]|[0-9]|/|#|\(|\)){1}([a-z]|[A-Z]|[0-9]|_|-|\.|/|#|\(|\))*$

Table 6-486 Query Parameters

Parameter	Mandatory	Type	Description
dim_name	Yes	String	**Description** Dimension name. **Constraints**: None **Value range**: Enumerated values. The value can be **mount_point**, **disk**, **proc**, **gpu**, or **raid**. **Default value**: None Enumeration values: • **mount_point** • **disk** • **proc** • **gpu** • **raid**
dim_value	No	String	**Description** Dimension value. Under the same **instance_id**, the same **dim_value** * corresponds to the same original dimension value **origin_value**, so you do not need to call this API for multiple times. You are advised to combine **instance_id** and **dim_value** as the key for data cache and reuse. **Constraints**: N/A **Range**: The value can contain a maximum of 32 characters, for example, **2e84018fc8b4484b94e89aae212fe615**. **Default value**: N/A **Regex Pattern:** ([a-f\d]{32}|[A-F\d]{32})

Parameter	Mandatory	Type	Description
offset	No	Integer	**Description** Pagination offset. **Constraints**: None **Value range**: The value ranges from **0** to **2147483647**. **Default value**: 0 **Value range:** 0-2147483647 **Default value:** 0
limit	No	Integer	**Description** Page size. **Constraints**: None **Value range**: The value ranges from **1** to **1000**. **Default value**: 1000 **Value range:** 1-1000 **Default value:** 1000

Request Parameters

Table 6-487 Request header parameters

Parameter	Mandatory	Type	Description
Content-Type	No	String	**Definition** MIME type of the request body. **Constraints**: None **Value range**: The value can contain 1 to 64 characters. **Default value**: The default type is **application/json; charset=UTF-8**. **Default value:** application/json; charset=UTF-8
X-Auth-Token	No	String	**Definition** User token. **Constraints**: None **Value range**: The value can contain 1 to 16,384 characters. **Default value**: None

Response Parameters

Status code: 200

Table 6-488 Response body parameters

Parameter	Type	Description
dimensions	Array of **AgentDimension** objects	**Definition**: Dimension information.

Parameter	Type	Description
count	Integer	**Definition**: Total number of dimensions. **Value range**: The value is an integer from **0** to **2147483647**. **Value range:** 0-2147483647

Table 6-489 AgentDimension

Parameter	Type	Description
name	String	**Definition**: Dimension name. **Value range**: Enumerated values. The value can be **mount_point**, **disk**, **proc**, **gpu**, or **raid**. Enumeration values: • **mount_point** • **disk** • **proc** • **gpu** • **raid**
value	String	**Definition**: Dimension value. **Value range**: The value can contain 32 characters.
origin_value	String	**Definition**: Actual dimension information. **Range** The value can contain 1 to 1,024 characters.

Status code: 400

Table 6-490 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 404

Table 6-491 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Status code: 500

Table 6-492 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs.
error_msg	String	Request error message.
request_id	String	Request ID.

Example Requests

```
/v2/{project_id}/instances/4270ff17-aba3-4138-89fa-820594c39755/agent-dimensions?offset=0&limit=10
```

Example Responses

Status code: 200

Query succeeded.

```
{
  "dimensions" : [ {
    "name" : "disk",
    "value" : "2e84018fc8b4484b94e89aae212fe615",
    "origin_value" : "vda"
  }, {
```

```
    "name" : "disk",
    "value" : "6a1b2de69eeb9a037ea23de6b529394d",
    "origin_value" : "vdc"
  } ],
  "count" : 10
}
```

Status Codes

Status Code	Description
200	Query succeeded.
400	Parameter verification failed.
404	Resource not found.
500	Internal system error.

Error Codes

See **Error Codes**.

7 API V3

7.1 Agent Statuses

7.1.1 Querying Agent Statuses in Batches

Function

This API is used to query the Agent (including the uniagent) statuses.

Debugging

You can debug this API through automatic authentication in **API Explorer** or use the SDK sample code generated by API Explorer.

URI

POST /v3/{project_id}/agent-status/batch-query

Table 7-1 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID. Minimum: **1** Maximum: **64**

Request Parameters

Table 7-2 Request header parameters

Parameter	Mandatory	Type	Description
Content-Type	No	String	Specifies the MIME type of a request body. The default type is **application/json; charset=UTF-8**. Default: **application/json; charset=UTF-8** Minimum: **1** Maximum: **64**
X-Auth-Token	No	String	Specifies the user token. It is a response to the API for obtaining a user token. This API is the only one that does not require authentication. The value of **X-Subject-Token** in the response header is the token. Minimum: **1** Maximum: **16384**

Table 7-3 Request body parameters

Parameter	Mandatory	Type	Description
instance_ids	Yes	Array of strings	Specifies the cloud server ID list. Array Length: **1 - 2000**
uniagent_status	No	String	Specifies the uniagent status. The value can be **none** (not installed), **running**, **silent**, or **unknown** (faulty). Enumeration values: • **none** • **running** • **silent** • **unknown**

Parameter	Mandatory	Type	Description
extension_name	No	String	Specifies the Agent name. If this parameter is not specified, all Agents are queried. Currently, only telescope can be queried. Enumeration values: • **telescope**
extension_status	No	String	Specifies the Agent status. If this parameter is not specified, all statuses are queried. The value can be **none** (not installed), **running**, **stopped**, **fault** (process exception), or **unknown** (connection exception). Enumeration values: • **none** • **running** • **stopped** • **fault** • **unknown**

Response Parameters

Status code: 200

Table 7-4 Response body parameters

Parameter	Type	Description
agent_status	Array of **AgentStatusInfo** objects	Specifies the Agent statuses. Array Length: **1 - 2000**

Table 7-5 AgentStatusInfo

Parameter	Type	Description
instance_id	String	Specifies the cloud server ID. **Regex Pattern:** ^[a-zA-Z0-9-]{1,64}$

Parameter	Type	Description
uniagent_status	String	Specifies the uniagent status. The value can be **none** (not installed), **running**, **silent**, or **unknown** (faulty). Enumeration values: • **none** • **running** • **silent** • **unknown**
extensions	Array of **ExtensionInfo** objects	Specifies the Agent information list. Array Length: **1 - 10**

Table 7-6 ExtensionInfo

Parameter	Type	Description
name	String	Specifies the Agent name. Minimum: **1** Maximum: **64**
status	String	Specifies the Agent status. The value can be **none** (not installed), **running**, **stopped**, **fault** (process exception), or **unknown** (connection exception). Enumeration values: • **none** • **running** • **stopped** • **fault** • **unknown**
version	String	Specifies the Agent version. Minimum: **1** Maximum: **32**

Status code: 400

Table 7-7 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the error code. **Regex Pattern:** ^(taskmgr\.[0-9]{4})$
error_msg	String	Specifies the error message. Minimum: **1** Maximum: **256**

Status code: 401

Table 7-8 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the error code. **Regex Pattern:** ^(taskmgr\.[0-9]{4})$
error_msg	String	Specifies the error message. Minimum: **1** Maximum: **256**

Status code: 403

Table 7-9 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the error code. **Regex Pattern:** ^(taskmgr\.[0-9]{4})$
error_msg	String	Specifies the error message. Minimum: **1** Maximum: **256**

Status code: 500

Table 7-10 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the error code. **Regex Pattern:** ^(taskmgr\.[0-9]{4})$

Parameter	Type	Description
error_msg	String	Specifies the error message. Minimum: **1** Maximum: **256**

Example Requests

```
{
  "instance_ids" : [ "111111111111" ],
  "uniagent_status" : "none",
  "extension_name" : "telescope",
  "extension_status" : "none"
}
```

Example Responses

Status code: 200

Specifies the response body for querying the Agent statuses in batches.

```
{
  "agent_status" : [ {
    "instance_id" : "111111111111",
    "uniagent_status" : "none",
    "extensions" : [ {
      "name" : "telescope",
      "status" : "none",
      "version" : "2.5.6"
    } ]
  } ]
}
```

Status Codes

Status Code	Description
200	Specifies the response body for querying the Agent statuses in batches.
400	Bad Request
401	Unauthorized
403	Forbidden
500	Internal Server Error

Error Codes

See **Error Codes**.

7.2 Agent maintenance tasks

7.2.1 Querying the Agent Maintenance Tasks

Function

This API is used to querying the Agent maintenance tasks.

Constraints

Currently, this API is not supported in the **LA-Buenos Aires1** and **LA-Lima1** regions. This API can only be used to query the Agent tasks within three months.

Debugging

You can debug this API through automatic authentication in **API Explorer** or use the SDK sample code generated by API Explorer.

URI

GET /v3/{project_id}/agent-invocations

Table 7-11 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID. Minimum: **1** Maximum: **64**

Table 7-12 Query Parameters

Parameter	Mandatory	Type	Description
instance_id	No	String	Specifies the server ID. **Regex Pattern:** ^[a-zA-Z0-9-]{1,64}$
instance_type	No	String	Specifies the server type. The value can be **ECS** or **BMS**. Enumeration values: • **ECS** • **BMS**

Parameter	Mandatory	Type	Description
invocation_id	No	String	Specifies the task ID. **Regex Pattern:** ^([0-9A-Za-z]){1}([0-9A-Za-z]|_|-)*$
invocation_type	No	String	Task type. The options are **INSTALL**, **UPDATE**, **ROLLBACK**, **RETRY**, **SET_REMOTE_INSTALLER**, and **REMOTE_INSTALL**. Enumeration values: • **INSTALL** • **UPDATE** • **ROLLBACK** • **RETRY** • **SET_REMOTE_INSTALLER** • **REMOTE_INSTALL**
invocation_target	No	String	Task object. The value can be **telescope**. Default: **telescope** Enumeration values: • **telescope**
offset	No	Long	Specifies the pagination offset. Minimum: **0** Maximum: **9999999999999** Default: **0**
limit	No	Integer	Specifies the number of records on each page. Minimum: **1** Maximum: **100** Default: **100**

Request Parameters

Table 7-13 Request header parameters

Parameter	Mandatory	Type	Description
Content-Type	No	String	Specifies the MIME type of a request body. The default type is **application/json; charset=UTF-8**. Default: **application/json; charset=UTF-8** Minimum: **1** Maximum: **64**
X-Auth-Token	No	String	Specifies the user token. It is a response to the API for obtaining a user token. This API is the only one that does not require authentication. The value of **X-Subject-Token** in the response header is the token. Minimum: **1** Maximum: **16384**

Response Parameters

Status code: 200

Table 7-14 Response body parameters

Parameter	Type	Description
invocations	Array of **InvocationInfo** objects	Specifies the task list. Array Length: **0 - 100**
count	Long	Specifies the total number of tasks in the task list. Minimum: **0** Maximum: **9999999999999**

Table 7-15 InvocationInfo

Parameter	Type	Description
invocation_id	String	Specifies the task ID. **Regex Pattern:** ^([0-9A-Za-z]){1}([0-9A-Za-z]|_|-)*$
instance_id	String	Specifies the server ID. **Regex Pattern:** ^[a-zA-Z0-9-]{1,64}$
instance_name	String	Specifies the server name. Minimum: **1** Maximum: **128**
instance_type	String	Specifies the server type. The value can be **ECS** or **BMS**. Enumeration values: • **ECS** • **BMS**
intranet_ips	Array of strings	Specifies the private IP address list. Array Length: **0 - 10**
elastic_ips	Array of strings	Specifies the EIP list. Array Length: **0 - 10**
invocation_type	String	Task type, which can be **INSTALL**, **UPDATE**, **ROLLBACK**, or **RETRY**. Enumeration values: • **INSTALL** • **UPDATE** • **ROLLBACK** • **RETRY**
invocation_status	String	Specifies the task status. The value can be **PENDING**, **RUNNING**, **TIMEOUT**, **FAILED**, **SUCCEEDED**, **CANCELED**, or **ROLLBACKED**. Enumeration values: • **PENDING** • **RUNNING** • **TIMEOUT** • **FAILED** • **SUCCEEDED** • **CANCELED** • **ROLLBACKED**

Parameter	Type	Description
invocation_target	String	Task object. The value can be **telescope**. Enumeration values: • **telescope**
create_time	Long	Specifies when the task was created. Minimum: **1111111111111** Maximum: **9999999999999**
update_time	Long	Specifies when the task was updated. Minimum: **1111111111111** Maximum: **9999999999999**
current_version	String	Specifies the current version of the Agent. Minimum: **1** Maximum: **64**
target_version	String	Specifies the target version. Minimum: **1** Maximum: **64**
result_msg	String	Task execution result information. Minimum: **1** Maximum: **5000**

Status code: 400

Table 7-16 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the error code. **Regex Pattern:** ^(taskmgr\.[0-9]{4})$
error_msg	String	Specifies the error message. Minimum: **1** Maximum: **256**

Status code: 401

Table 7-17 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the error code. **Regex Pattern:** ^(taskmgr\.[0-9]{4})$
error_msg	String	Specifies the error message. Minimum: **1** Maximum: **256**

Status code: 403

Table 7-18 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the error code. **Regex Pattern:** ^(taskmgr\.[0-9]{4})$
error_msg	String	Specifies the error message. Minimum: **1** Maximum: **256**

Status code: 500

Table 7-19 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the error code. **Regex Pattern:** ^(taskmgr\.[0-9]{4})$
error_msg	String	Specifies the error message. Minimum: **1** Maximum: **256**

Example Requests

None

Example Responses

Status code: 200

OK


```
{
  "invocations" : [ {
    "invocation_id" : "invocationxxx001",
    "instance_id" : "instancexxx001",
    "instance_name" : "xxxx",
    "instance_type" : "ECS",
    "intranet_ips" : [ "10.xxx.xx.1" ],
    "elastic_ips" : [ "1.xx.xx.1" ],
    "invocation_type" : "INSTALL",
    "invocation_status" : "RUNNING",
    "invocation_target" : "telescope",
    "current_version" : "2.5.1",
    "target_version" : "2.6.1",
    "create_time" : 1678070008306,
    "update_time" : 1678070008306,
    "result_msg" : "xxx"
  } ],
  "count" : 1
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
500	Internal Server Error

Error Codes

See **Error Codes**.

7.2.2 Creating Agent maintenance Tasks in Batches

Function

This API is used to create Agent maintenance tasks in batches.

Constraints

Currently, this API is not supported in the **LA-Buenos Aires1** and **LA-Lima1** regions.

Debugging

You can debug this API through automatic authentication in **API Explorer** or use the SDK sample code generated by API Explorer.

URI

POST /v3/{project_id}/agent-invocations/batch-create

Table 7-20 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID. Minimum: **1** Maximum: **64**

Request Parameters

Table 7-21 Request header parameters

Parameter	Mandatory	Type	Description
Content-Type	No	String	Specifies the MIME type of a request body. The default type is **application/json; charset=UTF-8**. Default: **application/json; charset=UTF-8** Minimum: **1** Maximum: **64**
X-Auth-Token	No	String	Specifies the user token. It is a response to the API for obtaining a user token. This API is the only one that does not require authentication. The value of **X-Subject-Token** in the response header is the token. Minimum: **1** Maximum: **16384**

Table 7-22 Request body parameters

Parameter	Mandatory	Type	Description
instance_ids	No	Array of strings	Specifies the server ID list. (This parameter is mandatory when the task type is **INSTALL** or **UPDATE**.) Array Length: **1 - 100**

Parameter	Mandatory	Type	Description
invocation_type	Yes	String	Task type. The options are **INSTALL**, **UPDATE**, **ROLLBACK**, **RETRY**, **SET_REMOTE_INSTALL_HOST**, and **REMOTE_INSTALL**. Enumeration values: • **INSTALL** • **UPDATE** • **ROLLBACK** • **RETRY** • **SET_REMOTE_INSTALL_HOST** • **REMOTE_INSTALL**
invocation_target	No	String	Specifies the task object. Only **telescope** is supported. Default: **telescope** Enumeration values: • **telescope**
invocation_ids	No	Array of strings	Specifies the task ID list. This parameter is mandatory when the task type is **ROLLBACK** or **RETRY**. Array Length: **1 - 100**
version_type	No	String	Specifies the version the Agent will be upgraded to. The value can be **BASIC_VERSION** or **ADVANCE_VERSION**. Enumeration values: • **BASIC_VERSION** • **ADVANCE_VERSION**
origin	No	String	Specifies the source that calls the Agent maintenance task APIs. **CES** indicates the Cloud Eye console, **APICOM_BMS** indicates Bare Metal Server (BMS), and **ADMIN_SERVER** indicates the O&M platform. Enumeration values: • **CES** • **APICOM_BMS** • **ADMIN_SERVER**

Parameter	Mandatory	Type	Description
version	No	String	Version number. Minimum: **0** Maximum: **64** **Regex Pattern:** ^([0-9A-Za-z]|_|-|\.)+$
remote_install_meta	No	Array of **RemoteInstallHostInfo** objects	Information about the server for remotely installing the Agent when a remote installation task is created. Array Length: **0 - 100**

Table 7-23 RemoteInstallHostInfo

Parameter	Mandatory	Type	Description
instance_name	No	String	Name of the server for remotely installing the Agent. Minimum: **1** Maximum: **128**
remote_ip	No	String	IP address of the server for remotely installing the Agent. **Regex Pattern:** ^(([0-9]|\.){1,15})$
user_name	No	String	Username for logging in to the server for remotely installing the Agent. Minimum: **1** Maximum: **16**
port	No	String	Port for logging in to the server for remotely installing the Agent. Minimum: **1** Maximum: **5**
password	No	String	Password for logging in to the server for remotely installing the Agent. Minimum: **1** Maximum: **3000**

Parameter	Mandatory	Type	Description
remote_use_pem	No	Boolean	Whether a key pair is used to connect to the server for remotely installing the Agent. If the value is false, a password is used. Default: **false**

Response Parameters

Status code: 201

Table 7-24 Response body parameters

Parameter	Type	Description
invocations	Array of **BatchCreateInvocationInfo** objects	Specifies the information list of the created task. Array Length: **0 - 100**

Table 7-25 BatchCreateInvocationInfo

Parameter	Type	Description
instance_id	String	Server ID. **Regex Pattern:** ^[a-zA-Z0-9-]{1,64}$
invocation_id	String	Specifies the task ID. **Regex Pattern:** ^[a-zA-Z0-9-]{1,64}$
ret_status	String	Specifies the task result. The value can be **successful** or **error**. Enumeration values: • **successful** • **error**
error_code	String	Specifies the error code. **Regex Pattern:** ^(invocationmgr\.[0-9]{4})$
error_msg	String	Specifies the error message. Minimum: **1** Maximum: **128**

Status code: 400

Table 7-26 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the error code. **Regex Pattern:** ^(taskmgr\.[0-9]{4})$
error_msg	String	Specifies the error message. Minimum: **1** Maximum: **256**

Status code: 401

Table 7-27 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the error code. **Regex Pattern:** ^(taskmgr\.[0-9]{4})$
error_msg	String	Specifies the error message. Minimum: **1** Maximum: **256**

Status code: 403

Table 7-28 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the error code. **Regex Pattern:** ^(taskmgr\.[0-9]{4})$
error_msg	String	Specifies the error message. Minimum: **1** Maximum: **256**

Status code: 500

Table 7-29 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the error code. **Regex Pattern:** ^(taskmgr\.[0-9]{4})$

Parameter	Type	Description
error_msg	String	Specifies the error message. Minimum: **1** Maximum: **256**

Example Requests

```
{
  "instance_ids" : [ "instancexxx001", "instancexxx002" ],
  "invocation_type" : "INSTALL",
  "invocation_target" : "telescope"
}
```

Example Responses

Status code: 201

Created

```
[ {
  "instance_id" : "instancexxx001",
  "ret_status" : "successful"
}, {
  "instance_id" : "instancexxx002",
  "ret_status" : "error",
  "error_msg" : "do not meet the installation conditions"
} ]
```

Status Codes

Status Code	Description
201	Created
400	Bad Request
401	Unauthorized
403	Forbidden
500	Internal Server Error

Error Codes

See **Error Codes**.

8 Permissions Policies and Supported Actions

8.1 Introduction

This chapter describes fine-grained permissions management for your Cloud Eye. If your Huawei Cloud account does not need individual IAM users, then you may skip over this chapter.

Policies: A type of fine-grained authorization mechanism that defines permissions required to perform operations on specific cloud resources under certain conditions. This mechanism allows for more flexible policy-based authorization, meeting requirements for secure access control. By default, new IAM users do not have any permissions assigned. You need to add a user to one or more groups, and assign permissions policies to these groups. The user then inherits permissions from the groups it is a member of. This process is called authorization. After authorization, the user can perform specified operations on Cloud Eye based on the permissions. For details, see **Permissions Management**.

You can grant users permissions by using roles and policies. A policy consists of permissions for an entire service. Users with such a policy assigned are granted all of the permissions required for that service. Policies define API-based permissions for operations on specific resources, allowing for more fine-grained, secure access control of cloud resources.

NOTE

If you want to allow or deny the access to an API, use policies for authorization.

An account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions. The permissions required for calling an API are determined by the actions supported by the API. Only users who have been granted permissions allowing the actions can call the API successfully. For example, if an IAM user queries the alarm rule list using an API, the user must have been granted permissions that allow the **ces:alarms:list** action.

Supported Actions

Cloud Eye provides system-defined policies that can be directly used in IAM. You can also create custom policies and use them to supplement system-defined policies, implementing more refined access control. Operations supported by policies are specific to APIs. The following are common concepts related to policies:

- Permissions: Defined by actions in a custom policy.
- Actions: Added to a custom policy to control permissions for specific operations.
- Related actions: Actions on which a specific action depends to take effect. When assigning permissions for the action to a user, you also need to assign permissions for the dependent actions.
- Authorization Scope: A custom policy can be applied to IAM projects or enterprise projects or both. Policies that contain actions supporting both IAM and enterprise projects can be assigned to user groups and take effect in both IAM and Enterprise Management. Policies that only contain actions supporting IAM projects can be assigned to user groups and only take effect for IAM. Such policies will not take effect if they are assigned to user groups in Enterprise Management. For details about the differences between IAM and enterprise management, see **What Are the Differences Between IAM and Enterprise Management?**
- APIs: REST APIs that can be called in a custom policy

Cloud Eye supports the following actions that can be defined in custom policies:

NOTE

√ indicates that the item is supported, and × indicates that the item is not supported.

Supported Actions of the API Version Management APIs

Supported Actions of the Metric Management API

Supported Actions of the Alarm Rule Management APIs

Supported Actions of the Monitoring Data Management APIs

Supported Actions of the Quota Management API

Supported Actions of the Event Monitoring API

8.2 Supported Actions of the API Version Management APIs

Permission	API	Action	IAM Project	Enterprise Project
Query all API versions supported by Cloud Eye.	GET /	ces:versions:get	√	×

Permission	API	Action	IAM Project	Enterprise Project
Query a specified Cloud Eye API version.	GET /{api_version}	ces:versions:get	√	×

8.3 Supported Actions of the Metric Management API

Permission	API	Action	IAM Project	Enterprise Project
Query the metric list. You can specify the namespace, metric name, dimension, sorting order, start records, and the maximum number of records when using this API to query metrics.	GET /V1.0/{project_id}/metrics	ces:metrics:list	√	×

8.4 Supported Actions of the Alarm Rule Management APIs

Permission	API	Action	IAM Project	Enterprise Project
Query the alarm rule list. You can specify the paging parameters to limit the number of query results displayed on a page. You can also set the sorting order of query results.	GET /V1.0/{project_id}/alarms	ces:alarms:list	√	√
Query an alarm rule based on the alarm rule ID.	GET /V1.0/{project_id}/alarms/{alarm_id}	ces:alarms:get	√	√
Enable or disable an alarm rule.	PUT /V1.0/{project_id}/alarms/{alarm_id}/action	ces:alarmsOnOff:put	√	√
Delete an alarm rule.	DELETE /V1.0/{project_id}/alarms/{alarm_id}	ces:alarms:delete	√	√
Create an alarm rule.	POST /V1.0/{project_id}/alarms	ces:alarms:create	√	√

8.5 Supported Actions of the Monitoring Data Management APIs

Permission	API	Action	IAM Project	Enterprise Project
Query the monitoring data at a specified granularity for a specified metric in a specified period of time. You can specify the dimension of data to be queried.	GET /V1.0/{project_id}/metric-data?namespace={namespace}&metric_name={metric_name}&dim.{i}=key,value&from={from}&to={to}&period={period}&filter={filter}	ces:metricData:list	√	×
Add one or more pieces of custom metric monitoring data to solve the problem that the system metrics cannot meet specific service requirements.	POST /V1.0/{project_id}/metric-data	ces:metricData:create	√	×
Query the monitoring data of specified metrics within a specified time range and specified granularities in batches. At present, you can query the monitoring data of a maximum of 10 metrics in batches.	POST /V1.0/{project_id}/batch-query-metric-data	ces:metricData:list	√	×

Permission	API	Action	IAM Project	Enterprise Project
Query the host configuration for a specified event type in a specified period of time. You can specify the dimension of data to be queried. (This API is provided for SAP Monitor to query the host configuration in the HANA scenario. In other scenarios, the host configuration cannot be queried with this API.)	GET /V1.0/{project_id}/event-data	ces:sapEventData:list	√	×

8.6 Supported Actions of the Quota Management API

Permission	API	Action	IAM Project	Enterprise Project
Query a resource quota and the used amount. Currently, the resource refers to alarm rules only.	GET /V1.0/{project_id}/quotas	ces:quotas:get	√	×

8.7 Supported Actions of the Event Monitoring API

Permission	API	Action	IAM Project	Enterprise Project
Report custom events.	POST /V1.0/{project_id}/events	ces:events:post	√	×

9 Common Parameters

9.1 Status Codes

- Normal

Returned Value	Description
200 OK	The results of GET and PUT operations are returned as expected.
201 Created	The results of the POST operation are returned as expected.
202 Accepted	The request has been accepted for processing.
204 No Content	The results of the DELETE operation are returned as expected.

- Abnormal

Returned Value	Description
400 Bad Request	The server failed to process the request.
401 Unauthorized	You must enter a username and password to access the requested page.
403 Forbidden	You are forbidden to access the requested page.
404 Not Found	The server cannot find the requested page.
405 Method Not Allowed	You are not allowed to use the method specified in the request.
406 Not Acceptable	The response generated by the server cannot be accepted by the client.

Returned Value	Description
407 Proxy Authentication Required	You must use the proxy server for authentication so that the request can be processed.
408 Request Timeout	The request timed out.
409 Conflict	The request could not be processed due to a conflict.
500 Internal Server Error	Failed to complete the request because of a service error.
501 Not Implemented	Failed to complete the request because the server does not support the requested function.
502 Bad Gateway	Failed to complete the request because the request is invalid.
503 Service Unavailable	Failed to complete the request. The service is unavailable.
504 Gateway Timeout	A gateway timeout error occurred.

9.2 Error Codes

Function

If an error occurs during API calling, the system returns error information. This section describes the error codes contained in the error information for Cloud Eye APIs.

v1 Example Response

```
{
    "http_code":"403",
    "message": {
        "details":"Policy doesn't allow [ces:alarms:get] to be performed",
        "code":"403"
    }
}
```

Example Response of a v2 API

```
{
  "error_code": "ces.0001",
  "error_msg": "The content must be specified."
}
```


Glossary

Glossary	Description
Cloud Eye	Cloud Eye
Built-in metric	Each service has its own built-in metrics and dimensions. For example, an ECS (SYS.ECS) supports **cpu_util**.
Metric	A metric consists of the namespace, dimension (optional), and metric name. A metric name solely does not identify any object.

Error Code Description

If an error code starting with **APIGW** is returned after you call an API, rectify the fault by referring to the instructions provided in **Error Codes**.

Module	HTTP Status Code	Error Code	Error Code Description	Error Message	Measure
Cloud Eye	500	ces.0007	Internal service error	Internal service error.	Contact technical support.
API	400	ces.0001	The request content cannot be empty.	The content must be specified.	Specify the request content.
	400	ces.0003	The project ID is left blank or is incorrect.	The tenant ID is left blank or incorrect.	Add or use the correct tenant ID.
	400	ces.0004	The API version is not specified.	The API version must be specified.	Specify the API version in the request URL.
	400	ces.0005	The API version is incorrect.	The API version is incorrect.	Use the correct API version.
	400	ces.0006	The paging address is incorrect.	The paging address is incorrect.	Use correct pagination information.
	403	ces.0009	System metrics cannot be added.	Adding SYS metric is not allowed	Use correct rights to add metrics.

Module	HTTP Status Code	Error Code	Error Code Description	Error Message	Measure
	403	ces.0010	System metrics cannot be deleted.	Deleting SYS metric is not allowed	Use correct rights to delete metrics.
	400	ces.0011	The request is invalid.	The request is invalid.	Check the request.
	400	ces.0013	The URL parameter is invalid or does not exist.	The URL parameter is invalid or does not exist.	Check the URL parameter.
	400	ces.0014	Some content in the message body is incorrect.	Some content in message body is not correct.	Check the request body parameters.
	401	ces.0015	Authentication fails or valid authentication information is not provided.	Authentication fails or the authentication information is not provided.	Check whether the user name or password (or AK or SK) for obtaining the token is correct.
	404	ces.0016	The requested resource does not exist.	The requested resource does not exist.	Check whether the requested resource exists.
	403	ces.0017	The authentication information is incorrect or the service invoker does not have sufficient rights.	The authentication information is incorrect or the service invoker does not have sufficient rights.	Check whether the user name or password (or AK or SK) or the user rights for obtaining the token are correct.
Cassandra	500	ces.0008	Database error	Database error.	Contact technical support.

Module	HTTP Status Code	Error Code	Error Code Description	Error Message	Measure
Zookeeper	500	ces.0021	Internal locking error	Internal locking error	Contact technical support.
Blueflood	500	ces.0019	The metric processing engine is abnormal.	The metric processing engine is abnormal.	Contact technical support.
Alarm	400	ces.0002	The alarm ID cannot be left blank.	The alarm ID must be specified.	Specify the alarm ID.
	403	ces.0018	The number of alarm rules created exceeds the quota.	The number of alarms exceeds the quota	Apply for a higher alarm quota.
	400	ces.0028	The metric and notification type do not match when an alarm rule is created.	The metric does not support the alarm action type.	Modify the metric or notification type according to the parameter description to make them match.

9.3 Obtaining a Project ID

Scenarios

A project ID is required for some URLs when an API is called. Therefore, you need to obtain a project ID in advance. Two methods are available:

- **Obtain the Project ID by Calling an API**
- **Obtain the Project ID from the Console**

Obtain the Project ID by Calling an API

You can obtain a project ID by calling the API used to **query projects based on specified criteria**.

The API used to obtain a project ID is GET https://{Endpoint}/v3/projects. {Endpoint} is the IAM endpoint and can be obtained from **Regions and Endpoints**. For details about API authentication, see **Authentication**.

The following is an example response. The value of **id** is the project ID.

```
{
    "projects": [
        {
            "domain_id": "65ewtrgaggshhk1223245sghjlse684b",
            "is_domain": false,
            "parent_id": "65ewtrgaggshhk1223245sghjlse684b",
            "name": "project_name",
            "description": "",
            "links": {
                "next": null,
                "previous": null,
                "self": "https://www.example.com/v3/projects/a4adasfjljaaaakla12334jklga9sasfg"
            },
            "id": "a4adasfjljaaaakla12334jklga9sasfg",
            "enabled": true
        }
    ],
    "links": {
        "next": null,
        "previous": null,
        "self": "https://www.example.com/v3/projects"
    }
}
```

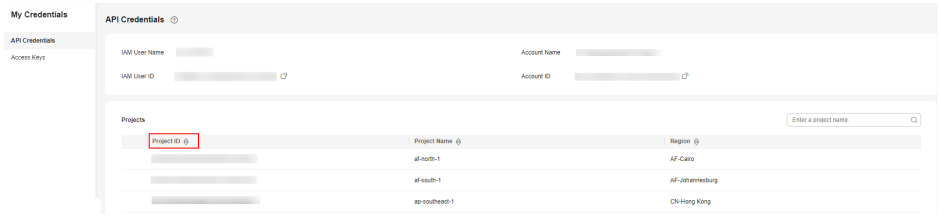
Obtain a Project ID from the Console

To obtain a project ID from the console, perform the following operations:

1. Log in to the management console.
2. Click the username and select **My Credentials** from the drop-down list.

   On the **API Credentials** page, view the project ID in the project list.

Figure 9-1 Viewing the project ID



9.4 Obtaining an Enterprise Project ID

Scenarios

Some URLs need to be filled with the enterprise project IDs when APIs are called, so the enterprise project IDs need to be obtained. This section describes how to obtain an enterprise project ID on the management console.

Procedure

1. Log in to the management console.
2. Choose **Enterprise** > **Project Management** in the upper right corner of the page.

If the screen resolution is low, choose **More** > **Enterprise** > **Project Management**.

3. Locate the target the enterprise project and click its name.

   In the enterprise project details, **ID** is the enterprise project ID.

10 Appendix

10.1 Services Interconnected with Cloud Eye

Category	Service	Namespace	Dimension	Reference
Compute	Elastic Cloud Server	SYS.ECS	Key: instance_id Value: ECS ID	Basic ECS metrics
	ECS (OS monitoring)	AGT.ECS	Key: instance_id Value: ECS ID	OS monitoring metrics supported by ECSs with the Agent installed
	Bare Metal Server	SERVICE.BMS	Key: instance_id Value: BMS ID	BMS metrics (with the Agent installed)
	Auto Scaling	SYS.AS	Key: AutoScalingGroup Value: auto scaling group ID	AS metrics
Storage	Elastic Volume Service (attached to an ECS or BMS)	SYS.EVS	Key: disk_name Value: server ID-drive letter (sda is the drive letter.)	EVS metrics
	Object Storage Service	SYS.OBS	Key: bucket_name Value: bucket name	OBS metrics

Category	Service	Namespace	Dimension	Reference
	Scalable File Service	SYS.SFS	Key: share_id Value: file system	SFS metrics
	SFS Turbo	SYS.EFS	Key: efs_instance_id Value: instance	SFS Turbo metrics
	Scalable File Service Turbo	SYS.EFS	Key: efs_instance_id Value: instance	SFS Turbo metrics
	Key-Value Storage Service	SYS.KVS	For details, see the information in the right column.	KVS metrics
Network	Virtual Private Cloud	SYS.VPC	• Key: publicip_id Value: EIP ID • Key: bandwidth_id Value: bandwidth ID	VPC metrics
	Global EIP	SYS.GEIP	For details, see the information in the right column.	Global EIP metrics
	EIP (Regional)	SYS.VPC	For details, see the information in the right column.	EIP (Regional) metrics
	Elastic Load Balance	SYS.ELB	For details, see the information in the right column.	Dedicated ELB metrics Shared ELB metrics

Category	Service	Namespace	Dimension	Reference
	NAT Gateway	SYS.NAT	Key: nat_gateway_id Value: NAT gateway ID	**NAT Gateway metrics**
	Virtual Private Network	SYS.VPN	For details, see the information in the right column.	**S2C Enterprise Edition VPN metrics** **P2C VPN metrics**
		SYS.VPC	For details, see the information in the right column.	**S2C Classic VPN metrics**
	Cloud Connect	SYS.CC	• Key: cloud_connect_id Value: cloud connection ID • Key: bwp_id Value: bandwidth package ID • Key: region_bandwidth_id Value: inter-region bandwidth ID	**Cloud Connect metrics**
	Direct Connect	SYS.DCAAS	For details, see the information in the right column.	**Direct Connect basic metrics** **Network quality metrics (Agent Required)**

Category	Service	Namespace	Dimension	Reference
	Global Accelerator	SYS.GA	• Key: ga_accelerator_id Value: ID of the global accelerator • Key: ga_listener_id Value: ID of a listener added to the global accelerator	**Global Accelerator metrics**
Middleware	Distributed Message Service	SYS.DMS	For details, see the information in the right column.	**DMS for Kafka metrics** **DMS for RocketMQ metrics** **DMS for RocketMQ metrics**

Category	Service	Namespace	Dimension	Reference
	Distributed Cache Service	SYS.DCS	• Key: dcs_instance_id Value: DCS Redis instance • Key: dcs_cluster_redis_node Value: Redis Server • Key: dcs_cluster_proxy_node Value: Proxy in a Proxy Cluster DCS Redis 3.0 instance • Key: dcs_cluster_proxy2_node Value: Proxy in a Proxy Cluster DCS of Redis 4.0 or Redis 5 instance • Key: dcs_memcached_instance_id Value: DCS Memcached instance	DCS metrics
Databases	Relational Database Service	SYS.RDS	For details, see the information in the right column.	RDS for MySQL metrics RDS for MariaDB metrics RDS for PostgreSQL metrics RDS for SQL Server metrics

Category	Service	Namespace	Dimension	Reference
	Document Database Service	SYS.DDS	• Key: mongodb_node_id Value: DDS node ID • Key: mongodb_instance_id Value: DDS DB instance ID	**DDS metrics**
	GeminiDB	SYS.NoSQL	For details, see the information in the right column.	**GeminiDB Cassandra metrics** **GeminiDB Mongo metrics** **GeminiDB Influx metrics** **GeminiDB Redis metrics**

Category	Service	Namespace	Dimension	Reference
	TaurusDB	SYS.GAUSSDB	• Key: gaussdb_mysql_instance_id Value: TaurusDB instance ID • Key: gaussdb_mysql_node_id Value: TaurusDB instance node ID • Key: dbproxy_instance_id Value: TaurusDB proxy instance ID • Key: dbproxy_node_id Value: TaurusDB proxy node ID	**TaurusDB metrics**

Category	Service	Namespace	Dimension	Reference
	GaussDB	SYS.GAUSSDBV5	• Key: gaussdbv5_instance_id Value: GaussDB instance ID • Key: gaussdbv5_node_id Value: GaussDB node ID • Key: gaussdbv5_component_id Value: GaussDB component ID	GaussDB metrics
EI	Cloud Search Service	SYS.ES	Key: cluster_id Value: CSS cluster	CSS metrics
	ModelArts	SYS.ModelArts	• Key: service_id Value: real-time service ID • Key: model_id Value: model ID	ModelArts metrics
	Data Lake Insight	SYS.DLI	• Key: queue_id Value: queue instance • Key: flink_job_id Value: Flink job	DLI metrics
	Data Ingestion Service (DIS)	SYS.DAYU	Key: stream_id Value: real-time data ingestion	DIS Metrics

Category	Service	Namespace	Dimension	Reference
Security and Compliance	Web Application Firewall	SYS.WAF	• Key: instance_id Value: dedicated WAF instance • Key: waf_instance_id Value: cloud WAF instance	WAF metrics
	Database Security Service	SYS.DBSS	Key: audit_id Value: instance	DBSS metrics
Management & Governance	Simple Message Notification	SYS.SMN	Key: topic_id Value: topic ID	SMN metrics

10.2 Events Supported by Event Monitoring

NOTE

The name of a resource that supports event reporting can contain a maximum of 128 characters, including letters, digits, underscores (_), hyphens (-), and periods (.). If it contains other characters, the event may fail to be reported to Cloud Eye.

Table 10-1 Elastic Cloud Server (ECS)

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
ECS	Restart triggered due to system faults	startAutoRecovery	Major	ECSs on a faulty host would be automatically migrated to another properly-running host. During the migration, the ECSs was restarted.	Wait for the event to end and check whether services are affected.	Services may be interrupted.
	Restart completed due to system faults	endAutoRecovery	Major	The ECS was recovered after the automatic migration.	This event indicates that the ECS has recovered and been working properly.	None
	Auto recovery timeout (being processed on the backend)	faultAutoRecovery	Major	Migrating the ECS to a normal host timed out.	Migrate services to other ECSs.	Services are interrupted.
	GPU link fault	GPULinkFault	Critical	The GPU of the host running the ECS was faulty or recovering from a fault.	Deploy service applications in HA mode. After the GPU fault is rectified, check whether services are restored.	Services are interrupted.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	ECS deleted	deleteServer	Major	The ECS was deleted: • on the management console. • by calling APIs.	Check whether the deletion was performed intentionally by a user.	Services are interrupted.
	ECS restarted	rebootServer	Minor	The ECS was restarted: • on the management console. • by calling APIs.	Check whether the restart was performed intentionally by a user. • Deploy service applications in HA mode. • After the ECS starts up, check whether services recover.	Services are interrupted.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	ECS stopped	stopServer	Minor	The ECS was stopped: • on the management console. • by calling APIs. **NOTE** The ECS is stopped only **after CTS is enabled**.	• Check whether the restart was performed intentionally by a user. • Deploy service applications in HA mode. • After the ECS starts up, check whether services recover.	Services are interrupted.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	NIC deleted	deleteNic	Major	The ECS NIC was deleted: • on the management console. • by calling APIs.	• Check whether the deletion was performed intentionally by a user. • Deploy service applications in HA mode. • After the NIC is deleted, check whether services recover.	Services may be interrupted.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	ECS resized	resizeServer	Minor	The ECS specifications were modified: • on the management console. • by calling APIs.	• Check whether the operation was performed by a user. • Deploy service applications in HA mode. • After the ECS is resized, check whether services have recovered.	Services are interrupted.
	GuestOS restarted	RestartGuestOS	Minor	The guest OS was restarted.	Contact O&M personnel.	Services may be interrupted.
	ECS failure caused by system faults	VMFaultsByHostProcessExceptions	Critical	The host where the ECS resides is faulty. The system will automatically try to start the ECS.	After the ECS is started, check whether this ECS and services on it can run properly.	The ECS is faulty.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Startup failure	faultPowerOn	Major	The ECS failed to start.	Start the ECS again. If the problem persists, contact O&M personnel.	The ECS cannot start.
	Host breakdown risk	hostMayCrash	Major	The host where the ECS resides may break down, and the risk cannot be prevented through live migration due to some reasons.	Migrate services running on the ECS first and delete or stop the ECS. Start the ECS only after the O&M personnel eliminate the risk.	The host may break down, causing service interruption.
	Scheduled migration completed	instance_migrate_completed	Major	Scheduled ECS migration is completed.	Wait until the ECSs become available and check whether services are affected.	Services may be interrupted.
	Scheduled migration being executed	instance_migrate_executing	Major	ECSs are being migrated as scheduled.	Wait until the event is complete and check whether services are affected.	Services may be interrupted.
	Scheduled migration canceled	instance_migrate_canceled	Major	Scheduled ECS migration is canceled.	None	None

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Scheduled migration failed	instance_migrate_failed	Major	ECSs failed to be migrated as scheduled.	Contact O&M personnel.	Services are interrupted.
	Scheduled migration to be executed	instance_migrate_scheduled	Major	ECSs will be migrated as scheduled.	Check the impact on services during the execution window.	None
	Scheduled specification modification failed	instance_resize_failed	Major	Specifications failed to be modified as scheduled.	Contact O&M personnel.	Services are interrupted.
	Scheduled specification modification completed	instance_resize_completed	Major	Scheduled specifications modification is completed.	None	None
	Scheduled specification modification being executed	instance_resize_executing	Major	Specifications are being modified as scheduled.	Wait until the event is completed and check whether services are affected.	Services are interrupted.
	Scheduled specification modification canceled	instance_resize_canceled	Major	Scheduled specifications modification is canceled.	None	None
	Scheduled specification modification to be executed	instance_resize_scheduled	Major	Specifications will be modified as scheduled.	Check the impact on services during the execution window.	None
	Scheduled redeployment to be executed	instance_redeploy_scheduled	Major	ECSs will be redeployed on new hosts as scheduled.	Check the impact on services during the execution window.	None

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Scheduled restart to be executed	instance_reboot_scheduled	Major	ECSs will be restarted as scheduled.	Check the impact on services during the execution window.	None
	Scheduled stop to be executed	instance_stop_scheduled	Major	ECSs will be stopped as scheduled as they are affected by underlying hardware or system O&M.	Check the impact on services during the execution window.	None
	Live migration started	liveMigrationStarted	Major	The host where the ECS is located may be faulty. Live migrate the ECS in advance to prevent service interruptions caused by host breakdown.	Wait for the event to end and check whether services are affected.	Services may be interrupted for less than 1s.
	Live migration completed	liveMigrationCompleted	Major	The live migration is complete, and the ECS is running properly.	Check whether services are running properly.	None
	Live migration failure	liveMigrationFailed	Major	An error occurred during the live migration of an ECS.	Check whether services are running properly.	There is a low probability that services are interrupted.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	ECC uncorrectable error alarm generated on GPU SRAM	SRAMUncorrectableEccError	Major	There are ECC uncorrectable errors generated on GPU SRAM.	If services are affected, submit a service ticket.	The GPU hardware may be faulty. As a result, the SRAM is faulty, and services exit abnormally.
	FPGA link fault	FPGALinkFault	Critical	The FPGA of the host running the ECS was faulty or recovering from a fault.	Deploy service applications in HA mode. After the FPGA fault is rectified, check whether services are restored.	Services are interrupted.
	Scheduled redeployment to be authorized	instance_redeploy_inquiring	Major	As being affected by underlying hardware or system O&M, ECSs will be redeployed on new hosts as scheduled.	Authorize scheduled redeployment.	None
	Local disk replacement canceled	localdisk_recovery_canceled	Major	Local disk failure	None	None

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Local disk replacement to be executed	localdisk_recovery_scheduled	Major	Local disk failure	Check the impact on services during the execution window.	None
	Xid event alarm generated on GPU	commonXidError	Major	An Xid event alarm was generated on the GPU.	If services are affected, submit a service ticket.	The GPU hardware, driver, and application problems lead to Xid events, which may interrupt services.
	nvidia-smi suspended	nvidiaSmiHangEvent	Major	nvidia-smi timed out.	If services are affected, submit a service ticket.	The driver may report an error during service running.
	NPU: uncorrectable ECC error	UncorrectableEccErrorCount	Major	There are uncorrectable ECC errors generated on GPU SRAM.	If services are affected, replace the NPU with another one.	Services may be interrupted.
	Scheduled redeployment canceled	instance_redeploy_canceled	Major	As being affected by underlying hardware or system O&M, ECSs will be redeployed on new hosts as scheduled.	None	None

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Scheduled redeployment being executed	instance_redeploy_executing	Major	As being affected by underlying hardware or system O&M, ECSs will be redeployed on new hosts as scheduled.	Wait until the event is complete and check whether services are affected.	Services are interrupted.
	Scheduled redeployment completed	instance_redeploy_completed	Major	As being affected by underlying hardware or system O&M, ECSs will be redeployed on new hosts as scheduled.	Wait until the redeployed ECSs are available and check whether services are affected.	None
	Scheduled redeployment failed	instance_redeploy_failed	Major	As being affected by underlying hardware or system O&M, ECSs will be redeployed on new hosts as scheduled.	Contact O&M personnel.	Services are interrupted.
	Local disk replacement to be authorized	localdisk_recovery_inquiring	Major	Local disks are faulty.	Authorize local disk replacement.	Local disks are unavailable.
	Local disks being replaced	localdisk_recovery_executing	Major	Local disk failure	Wait until the local disks are replaced and check whether the local disks are available.	Local disks are unavailable.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Local disks replaced	localdisk_recovery_completed	Major	Local disks are faulty.	Wait until the services are running properly and check whether local disks are available.	None
	Local disk replacement failed	localdisk_recovery_failed	Major	Local disks are faulty.	Contact O&M personnel.	Local disks are unavailable.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	GPU throttle alarm	gpuClocksThrottleReasonsAlarm	Informational	1. The GPU power may exceed the maximum operating power threshold (continuous full load). The clock frequency automatically decreases to prevent the GPU from being damaged. 2. The GPU temperature may exceed the maximum operating temperature threshold (continuous full load). The clock frequency automatically decreases to reduce heat. 3. The GPU may remain idle, with the clock frequency automatically decreasing to reduce power consumption.	Check whether the clock frequency decrease is caused by hardware faults. If yes, transfer it to the hardware team.	The GPU slows down, resulting in less powerful compute.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
				4. Hardware faults may cause a decrease in clock frequency.		
	Pending page retirement for GPU DRAM ECC	gpuRetiredPagesPendingAlarm	Major	1. An ECC error occurred on the hardware. DRAM pages need to be retired. 2. An uncorrectable ECC error occurred on the GPU memory page and the page needs to be retired. However, the page is suspended and has not been retired yet.	1. View the event details and check whether the value of **retired_pages.pending** is **yes**. 2. Restart the GPU for automatic retirement.	The GPU cannot work properly.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Pending row remapping for GPU DRAM ECC	gpuRemappedRowsAlarm	Major	Some rows in the GPU memory have errors and need to be remapped. The faulty rows must be mapped to standby resources.	1. View the event metric "RemappedRow" to check if there are any rows that have been remapped. 2. Restart the GPU for automatic retirement.	The GPU cannot work properly.
	Insufficient resources for GPU DRAM ECC row remapping	gpuRowRemapperResourceAlarm	Major	1. This event occurs on GPUs (Ampere and later architectures). 2. The standby GPU memory row resources are exhausted, so row remapping cannot be continued.	Transfer the issue to the hardware team.	The GPU cannot work properly.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Correctable GPU DRAM ECC error	gpuDRAMCorrectableEccError	Major	1. This event occurs on GPUs (Ampere and later architectures). 2. A correctable ECC error occurs in the DRAM of the GPU. However, the ECC mechanism can automatically rectify the error and programs are not affected.	1. View the event metric "ecc.errors.corrected.volatile" to check whether there are any correctable ECC error values. 2. Restart the GPU for automatic retirement.	The GPU may not work properly.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Uncorrectable GPU DRAM ECC error	gpuDRAMUncorrectableEccError	Major	1. This event occurs on GPUs (Ampere and later architectures). 2. An uncorrectable ECC error occurs in the DRAM of the GPU. This error cannot be automatically corrected using the ECC mechanism. The verification process affects system stability and may cause program crashes.	1. View the event metric "ecc.errors.uncorrected.volatile" to check whether there are any uncorrectable ECC error values. 2. Restart the GPU for automatic retirement.	The GPU may not work properly.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Inconsistent GPU kernel versions	gpuKernelVersionInconsistencyAlarm	Major	Inconsistent GPU kernel versions. During driver installation, the GPU driver is compiled based on the kernel at that time. If the kernel versions are identified inconsistent, the kernel has been customized after the driver installation. In this case, the driver would become unavailable and needs to be reinstalled.	1. Run the following commands to rectify the issue: **rmmod nvidia_drm** **rmmod nvidia_modeset** **rmmod nvidia** Then, run **nvidia-smi**. If the command output is normal, the issue has been rectified. 2. If the preceding solution does not work, rectify the fault by referring to **Why Is the GPU Driver**	The GPU cannot work properly.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
					Unavailable?	
	GPU monitoring dependency not met	gpuCheckEnvFailedAlarm	Major	The plug-in cannot identify the GPU driver library path.	1. Check whether the driver is installed. 2. Check whether the driver installation directory has been customized. The driver needs to be installed in the default installation directory **/usr/bin/**.	Collection failure of GPU monitoring metrics

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Initialization failure of the GPU monitoring driver library	gpuDriverInitFailedAlarm	Major	The GPU driver is unavailable.	Run **nvidia-smi** to check whether the driver is unavailable. If the driver is unavailable, reinstall the driver by referring to **Manually Installing a Tesla Driver on a GPU-accelerated ECS**.	Collection failure of GPU monitoring metrics

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Initialization timeout of the GPU monitoring driver library	gpuDriverInitTAlarm	Major	The GPU driver initialization timed out (exceeding 10s).	1. If the driver is not installed, install it by referring to **Manually Installing a Tesla Driver on a GPU-accelerated ECS**. 2. If the driver is installed, run **nvidia-smi** to check whether the driver is availabl e. If the driver is unavailable, reinstall the driver by referring to **Manually Installing a Tesla Driver on a GPU-**	Collection failure of GPU monitoring metrics

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
					accelerated ECS. 3. If the driver is properly installed, check whether the high-performance mode is enabled. If not, run **nvidia-smi -pm 1** to enable it. P0 indicates the high-performance mode.	

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	GPU metric collection timeout	gpuCollectMetricTimeoutAlarm	Major	The GPU metric collection timed out (exceeding 10s).	1. If the library API timed out, run **nvidia-smi** to check whether the driver is availabl e. If the driver is unavaila ble, reinstall the driver by referring to **Manual ly Installin g a Tesla Driver on a GPU-accelera ted ECS**. 2. If the comma nd executio n timed out, check the system logs and determi ne whether there is an issue	GPU monitori ng metric data is missing. As a result, subsequ ent metrics may fail to be collected .

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
					with the system.	
	GPU handle lost	gpuDeviceHandleLost	Major	The GPU metric information cannot be obtained, and the GPU may be lost.	1. Run **nvidia-smi** to check whether there are any errors reported. 2. Run **nvidia-smi -L** to check whether the number of GPUs is the same as the server specifications. 3. Submit a service ticket to contact on-call support.	All metrics of the GPU are lost.
	Failed to listen to the XID of the GPU.	gpuDeviceXidLost	Major	Failed to listen to the XID metric.	1. Check whether the GPU is lost or damaged. 2. Submit a service ticket to contact on-call support.	Failed to obtain XID-related metrics of the GPU.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	ReadOnly issues in OS	ReadOnlyFileSystem	Critical	The file system %s is read-only.	Check the disk health status.	The files cannot be written.
	NPU: driver and firmware not matching	NpuDriverFirmwareMismatch	Major	The NPU's driver and firmware do not match.	Obtain the matched version from the Ascend official website and reinstall it.	NPUs cannot be used.
	NPU: Docker container environment check	NpuContainerEnvSystem	Major	Docker was unavailable.	Check if Docker is normal.	Docker cannot be used.
			Major	The container plug-in Ascend-Docker-Runtime was not installed.	Install the container plug-in Ascend-Docker-Runtime. Or, the container cannot use Ascend cards.	NPUs cannot be attached to Docker containers.
			Major	IP forwarding was not enabled in the OS.	Check the **net.ipv4.ip_forward** configuration in the **/etc/sysctl.conf** file.	Docker containers experience network communication problems.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
			Major	The shared memory of the container was too small.	The default shared memory is 64 MB, which can be modified as needed. Method 1 Modify the **default-shm-size** field in the **/etc/docker/daemon.json** configuration file. Method 2 Use the **--shm-size** parameter in the **docker run** command to set the shared memory size of a container.	Distributed training will fail due to insufficient shared memory.
	NPU: RoCE NIC down	RoCELinkStatusDown	Major	The RoCE link of NPU card %d was down.	Check the NPU RoCE network port status.	The NPU NIC becomes unavailable.
	NPU: RoCE NIC health status abnormal	RoCEHealthStatusError	Major	The RoCE network health status of NPU %d was abnormal.	Check the health status of the NPU RoCE NIC.	The NPU NIC becomes unavailable.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	NPU: RoCE NIC configuration file **/etc/hccn.conf** not found	HccnConfNotExisted	Major	The RoCE NIC configuration file **/etc/hccn.conf** was not found.	Check whether the **/etc/hccn.conf** NIC configuration file can be found.	The RoCE NIC is unavailable.
	GPU: basic components abnormal	GpuEnvironmentSystem	Major	The **nvidia-smi** command was abnormal.	Check whether the GPU driver is normal.	The GPU driver is unavailable.
			Major	The nvidia-fabricmanager version was inconsistent with the GPU driver version.	Check the GPU driver version and nvidia-fabricmanager version.	The nvidia-fabricmanager cannot work properly, affecting GPU usage.
			Major	The container plug-in nvidia-container-toolkit was not installed.	Install the container plug-in nvidia-container-toolkit.	GPUs cannot be attached to Docker containers.
	Local disk attachment inspection	MountDiskSystem	Major	The **/etc/fstab** file contains invalid UUIDs.	Ensure that the UUIDs in the **/etc/fstab** configuration file are correct. Or, the server may fail to be restarted.	The disk attachment process fails, preventing the server from restarting.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	GPU: incorrectly configured dynamic route for Ant series server	GpuRouteConfigError	Major	The dynamic route of the NIC %s of an Ant series server was not configured or was incorrectly configured. CMD [ip route]: %s | CMD [ip route show table all]: %s.	Configure the RoCE NIC route correctly.	The NPU network communication will be interrupted.
	NPU: RoCE port not split	RoCEUdpConfigError	Major	The RoCE UDP port was not split.	Check the RoCE UDP port configuration on the NPU.	The communication performance of NPUs is affected.
	Warning of automatic system kernel upgrade	KernelUpgradeWarning	Major	Warning of automatic system kernel upgrade. Old version: %s; new version: %s.	System kernel upgrade may cause AI software exceptions. Check the system update logs and prevent the server from restarting.	The AI software may be unavailable.
	NPU environment command detection	NpuToolsWarning	Major	The hccn_tool was unavailable.	Check whether the NPU driver is normal.	The IP address and gateway of the RoCE NIC cannot be configured.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
			Major	The npu-smi was unavailable.	Check whether the NPU driver is normal.	NPUs cannot be used.
			Major	The ascend-dmi was unavailable.	Check whether ToolBox is properly installed.	ascend-dmi cannot be used for performance analysis.
	Warning of an NPU driver exception	NpuDriverAbnormalWarning	Major	The NPU driver was abnormal.	Reinstall the NPU driver.	NPUs cannot be used.

NOTE

Automatic recovery: If the hardware where an ECS is located is faulty, the system automatically migrates it to a normal physical host. The ECS will restart during the migration.

Table 10-2 Bare metal server (BMS)

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
BMS	SYS.BMS	ECC uncorrectable error alarm generated on GPU SRAM	SRAMUncorrectableEccError	Major	There are ECC uncorrectable errors generated on GPU SRAM.	If services are affected, submit a service ticket.	The GPU hardware may be faulty. As a result, the SRAM is faulty, and services exit abnormally.
		BMS restarted	osReboot	Major	The BMS instance is restarted. • on the management console. • by calling APIs.	• Deploy service applications in HA mode. • After the BMS is restarted, check whether services recover.	Services are interrupted.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		BMS unexpected restart	serverReboot	Major	The BMS instance restarts unexpectedly. • OS faults. • hardware faults.	• Deploy service applications in HA mode. • After the BMS is restarted, check whether services recover.	Services are interrupted.
		BMS stopped	osShutdown	Major	The BMS instance is stopped. • on the management console. • by calling APIs.	• Deploy service applications in HA mode. • After the BMS is restarted, check whether services recover.	Services are interrupted.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		BMS unexpected shutdown	serverShutdown	Major	The BMS stops unexpectedly due to: • unexpected power-off. • hardware faults.	• Deploy service applications in HA mode. • After the BMS is restarted, check whether services recover.	Services are interrupted.
		Network disconnection	linkDown	Major	The BMS network is disconnected. Possible causes are as follows: • The BMS was stopped or restarted unexpectedly. • The switch was faulty. • The gateway was faulty.	• Deploy service applications in HA mode. • After the BMS is restarted, check whether services recover.	Services are interrupted.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		PCIe error	pcieError	Major	The PCIe device or main board on the BMS is faulty. Possible causes are as follows: • main board faults. • PCIe device faults.	• Deploy service applications in HA mode. • After the BMS is started, check whether services recover.	The network or disk read/write services are affected.
		Disk fault	diskError	Major	The disk of the BMS is faulty. Possible causes are as follows: • disk backplane faults. • disk faults.	• Deploy service applications in HA mode. • After the fault is rectified, check whether services recover.	Data read/write services are affected, or the BMS cannot be started.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		EVS error	storageError	Major	The BMS failed to connect to EVS disks. Possible causes are as follows: • The SDI card was faulty. • Remote storage devices were faulty.	• Deploy service applications in HA mode. • After the fault is rectified, check whether services recover.	Data read/write services are affected, or the BMS cannot be started.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Inforom alarm generated on GPU	gpuInfoROM Alarm	Major	The infoROM of the GPU is abnormal. ROM is an important storage area of the GPU firmware and stores key data loaded during startup.	Non-critical services can continue to use the GPU. For critical services, submit a service ticket to resolve this issue. 1. Restart the VM and check that the issue is not caused by a temporary cache or communication error. 2. If the fault persists after the restart, the hardware may be faulty. Submit	Services will not be affected. If ECC errors are reported on a GPU, faulty pages may not be automatically retired and services are affected.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
						a service ticket to check whether the GPU needs to be replaced.	

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Double-bit ECC alarm generated on GPU	doubleBitEccError	Major	A double-bit error occurs in the ECC memory of the GPU. The ECC cannot correct the error, which may cause program breakdown.	1. If services are interrupted, restart the services. 2. If services cannot be restarted, restart the VM where services are running. 3. If services still cannot be restored, submit a service ticket.	Services may be interrupted. After faulty pages are retired, the GPU can continue to be used.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Too many retired pages	gpuTooManyRetiredPagesAlarm	Major	An ECC page retirement error occurred on the GPU. When an uncorrectable ECC error occurs on a GPU memory page, the GPU marks the page as retired.	If services are affected, submit a service ticket.	If there are too many ECC errors, services may be affected. 1. If there are too many retired pages and the GPU memory capacity decreases too much, the system performance ma

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
							y deteriorate. 2. If there are too many retired pages and the GPU memory capacity decreases too much, the system may run unstably.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		ECC alarm generated on GPU A100	gpuA100EccAlarm	Major	An ECC error occurred on the GPU.	1. If services are interrupted, restart the services. 2. If services cannot be restarted, restart the VM where services are running. 3. If services still cannot be restored, submit a service ticket.	Services may be interrupted. After faulty pages are retired, the GPU can continue to be used.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		ECC alarm generated on GPU Ant1	gpuAnt1EccAlarm	Major	An ECC error occurred on GPU.	1. If services are interrupted, restart the services to restore. 2. If services cannot be restarted, restart the VM where services are running. 3. If services still cannot be restored, submit a service ticket.	Services may be interrupted. After faulty pages are retired, the GPU can continue to be used.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		GPU ECC memory page retirement failure	eccPageRetirementRecordingFailure	Major	Automatic page retirement failed due to ECC errors.	1. If services are interrupted, restart the services to restore. 2. If services cannot be restarted, restart the VM where services are running. 3. If services still cannot be restored, submit a service ticket.	Services may be interrupted, and memory page retirement fails. As a result, services cannot no longer use the GPU.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		GPU ECC page retirement alarm generated	eccPageRetirementRecordingEvent	Minor	Memory pages are automatically retired due to ECC errors.	1. If services are interrupted, restart the services. 2. If services cannot be restarted, restart the VM where services are running. 3. If services still cannot be restored, submit a service ticket.	Generally, this alarm is generated together with the ECC error alarm. If this alarm is generated independently, services are not affected.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Too many single-bit ECC errors on GPU	highSingleBitEccErrorRate	Major	There are too many single-bit errors occurring in the ECC memory of the GPU.	1. If services are interrupted, restart the services to restore. 2. If services cannot be restarted, restart the VM where services are running. 3. If services still cannot be restored, submit a service ticket.	Single-bit errors can be automatically rectified and do not affect GPU-related applications.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		GPU card not found	gpuDriverLinkFailureAlarm	Major	A GPU link is normal, but it cannot be found by the NVIDIA driver.	1. You are advised to try restarting the VM to restore your services. 2. If services still cannot be restored, submit a service ticket.	The GPU cannot be found.
		GPU link faulty	gpuPcieLinkFailureAlarm	Major	GPU hardware information cannot be queried through lspci due to a GPU link fault.	If services are affected, submit a service ticket.	The driver cannot use the GPU.
		VM GPU lost	vmLostGpuAlarm	Major	The number of GPUs on the VM is less than the number specified in the specifications.	If services are affected, submit a service ticket.	GPUs get lost.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		GPU memory page faulty	gpuMemoryPageFault	Major	The GPU memory page is faulty, which may be caused by applications, drivers, or hardware.	If services are affected, submit a service ticket.	The GPU hardware may be faulty. As a result, the GPU memory is faulty, and services exit abnormally.
		GPU image engine faulty	graphicsEngineException	Major	The GPU image engine is faulty, which may be caused by applications, drivers, or hardware.	If services are affected, submit a service ticket.	The GPU hardware may be faulty. As a result, the image engine is faulty, and services exit abnormally.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		GPU temperature too high	highTemperatureEvent	Major	GPU temperature too high	If services are affected, submit a service ticket.	If the GPU temperature exceeds the threshold, the GPU performance may deteriorate.
		GPU NVLink faulty	nvlinkError	Major	A hardware fault occurs on the NVLink.	If services are affected, submit a service ticket.	The NVLink link is faulty and unavailable.
		System maintenance inquiring	system_maintenance_inquiring	Major	The scheduled BMS maintenance task is being inquired.	Authorize the maintenance.	None
		System maintenance waiting	system_maintenance_scheduled	Major	The scheduled BMS maintenance task is waiting to be executed.	Clarify the impact on services during the execution window and ensure that the impact is acceptable to users.	None

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		System maintenance canceled	system_maintenance_canceled	Major	The scheduled BMS maintenance is canceled.	None	None
		System maintenance executing	system_maintenance_executing	Major	BMSs are being maintained as scheduled.	After the maintenance is complete, check whether services are affected.	Services are interrupted.
		System maintenance completed	system_maintenance_completed	Major	The scheduled BMS maintenance is completed.	Wait until the BMSs become available and check whether services recover.	None
		System maintenance failure	system_maintenance_failed	Major	The scheduled BMS maintenance task failed.	Contact O&M personnel.	Services are interrupted.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		GPU Xid error	commonXidError	Major	An Xid event alarm was generated on the GPU.	If services are affected, submit a service ticket.	The GPU hardware, driver, and application problems lead to Xid events, which may interrupt services.
		NPU: device not found by npu-smi info	NPUSMICardNotFound	Major	The Ascend driver is faulty or the NPU is disconnected.	Transfer this issue to the Ascend or hardware team for handling.	The NPU cannot be used normally.
		NPU: PCIe link error	PCIeErrorFound	Major	The **lspci** command returns **rev ff** indicating that the NPU is abnormal.	Restart the BMS. If the issue persists, transfer it to the hardware team for processing.	The NPU cannot be used normally.
		NPU: device not found by lspci	LspciCardNotFound	Major	The NPU is disconnected.	Transfer this issue to the hardware team for handling.	The NPU cannot be used normally.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		NPU: overtemperature	TemperatureOverUpperLimit	Major	The temperature of DDR or software is too high.	Stop services, restart the BMS, check the heat dissipation system, and reset the devices.	The BMS may be powered off and devices may not be found.
		NPU: uncorrectable ECC error	UncorrectableEccErrorCount	Major	There are uncorrectable ECC errors generated on GPU SRAM.	If services are affected, replace the NPU with another one.	Services may be interrupted.
		NPU: request for BMS restart	RebootVirtualMachine	Informational	A fault occurs and the BMS needs to be restarted.	Collect the fault information, and restart the BMS.	Services may be interrupted.
		NPU: request for SoC reset	ResetSOC	Informational	A fault occurs and the SoC needs to be reset.	Collect the fault information, and reset the SoC.	Services may be interrupted.
		NPU: request for restart AI process	RestartAIProcess	Informational	A fault occurs and the AI process needs to be restarted.	Collect the fault information, and restart the AI process.	The current AI task will be interrupted.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		NPU: error codes	NPUErrorCodeWarning	Major	A large number of NPU error codes indicating major or higher-level errors are returned. You can further locate the faults based on the error codes.	Locate the faults according to the *Black Box Error Code Information List* and *Health Management Error Definition*.	Services may be interrupted.
		nvidia-smi suspended	nvidiaSmiHangEvent	Major	nvidia-smi timed out.	If services are affected, submit a service ticket.	The driver may report an error during service running.
		nv_peer_mem loading error	NvPeerMemException	Minor	The NVLink or nv_peer_mem cannot be loaded.	Restore or reinstall the NVLink.	nv_peer_mem cannot be used.
		Fabric Manager error	NvFabricManagerException	Minor	The BMS meets the NVLink conditions and NVLink is installed, but Fabric Manager is abnormal.	Restore or reinstall the NVLink.	NVLink cannot be used normally.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		IB card error	InfinibandStatusException	Major	The IB card or its physical status is abnormal.	Transfer this issue to the hardware team for handling.	The IB card cannot work normally.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		GPU throttle alarm	gpuClocksThrottleReasonsAlarm	Informational	1. The GPU power may exceed the maximum operating power threshold (continuous full load). The clock frequency automatically decreases to prevent the GPU from being damaged. 2. The GPU temperature may exceed the maximum operating temperature threshold (continuous full load). The clock frequency automatically decreases to reduce heat. 3. The GPU may remain	Check whether the clock frequency decrease is caused by hardware faults. If yes, transfer it to the hardware team.	The GPU slows down, resulting in less powerful compute.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
					idle, with the clock frequency automatically decreasing to reduce power consumption. 4. Hardware faults may cause a decrease in clock frequency.		

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Pending page retirement for GPU DRAM ECC	gpuRetiredPagesPendingAlarm	Major	1. An ECC error occurred on the hardware. DRAM pages need to be retired. 2. An uncorrectable ECC error occurred on the GPU memory page and the page needs to be retired. However, the page is suspended and has not been retired yet.	1. View the event details and check whether the value of **retired_pages.pending** is **yes**. 2. Restart the GPU for automatic retirement.	The GPU cannot work properly.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Pending row remapping for GPU DRAM ECC	gpuRemappedRowsAlarm	Major	Some rows in the GPU memory have errors and need to be remapped. The faulty rows must be mapped to standby resources.	1. View the event metric "RemappedRow" to check if there are any rows that have been remapped. 2. Restart the GPU for automatic retirement.	The GPU cannot work properly.
		Insufficient resources for GPU DRAM ECC row remapping	gpuRowRemapperResourceAlarm	Major	1. This event occurs on GPUs (Ampere and later architectures). 2. The standby GPU memory row resources are exhausted, so row remapping cannot be continued.	Transfer the issue to the hardware team.	The GPU cannot work properly.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Correctable GPU DRAM ECC error	gpuDRAMCorrectableEccError	Major	1. This event occurs on GPUs (Ampere and later architectures). 2. A correctable ECC error occurs in the DRAM of the GPU. However, the ECC mechanism can automatically rectify the error and programs are not affected.	1. View the event metric "ecc.errors.corrected.volatile" to check whether there are any correctable ECC error values. 2. Restart the GPU for automatic retirement.	The GPU may not work properly.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Uncorrectable GPU DRAM ECC error	gpuDRAMUncorrectableEccError	Major	1. This event occurs on GPUs (Ampere and later architectures). 2. An uncorrectable ECC error occurs in the DRAM of the GPU. This error cannot be automatically corrected using the ECC mechanism. The verification process affects system stability and may cause program crashes.	1. View the event metric "ecc.errors.uncorrected.volatile" to check whether there are any uncorrectable ECC error values. 2. Restart the GPU for automatic retirement.	The GPU may not work properly.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Inconsistent GPU kernel versions	gpuKernelVersionInconsistencyAlarm	Major	Inconsistent GPU kernel versions. During driver installation, the GPU driver is compiled based on the kernel at that time. If the kernel versions are identified inconsistent, the kernel has been customized after the driver installation. In this case, the driver would become unavailable and needs to be reinstalled.	1. Run the following commands to rectify the issue: **rmmod nvidia_drm** **rmmod nvidia_modeset** **rmmod nvidia** Then, run **nvidia-smi**. If the command output is normal, the issue has been rectified. 2. If the preceding solution does not work, rectify	The GPU cannot work properly.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
						the fault by referring to **Why Is the GPU Driver Unavailable?**	
		GPU monitoring dependency not met	gpuCheckEnvFailedAlarm	Major	The plug-in cannot identify the GPU driver library path.	1. Check whether the driver is installed. 2. Check whether the driver installation directory has been customized. The driver needs to be installed in the default installation directory **/usr/bin/**.	Collection failure of GPU monitoring metrics

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Initialization failure of the GPU monitoring driver library	gpuDriverInitFailedAlarm	Major	The GPU driver is unavailable.	Run **nvidia-smi** to check whether the driver is unavailable. If the driver is unavailable, reinstall the driver by referring to **Manually Installing a Tesla Driver on a GPU-accelerated ECS**.	Collection failure of GPU monitoring metrics

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Initialization timeout of the GPU monitoring driver library	gpuDriverInitTAlarm	Major	The GPU driver initialization timed out (exceeding 10s).	1. If the driver is not installed, install it by referring to **Manually Installing a Tesla Driver on a GPU-accelerated ECS**. 2. If the driver is installed, run **nvidia-smi** to check whether the driver is available. If the driver is unavailable, reinstall the driver by referring to **Manu**	Collection failure of GPU monitoring metrics

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
						ally Installing a Tesla Driver on a GPU-accelerated ECS. 3. If the driver is properly installed, check whether the high-performance mode is enabled. If not, run **nvidia-smi -pm 1** to enable it. P0 indicates the high-performance mode.	

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		GPU metric collection timeout	gpuCollectMetricTimeoutAlarm	Major	The GPU metric collection timed out (exceeding 10s).	1. If the library API timed out, run **nvidia-smi** to check whether the driver is available. If the driver is unavailable, reinstall the driver by referring to **Manually Installing a Tesla Driver on a GPU-accelerated ECS**. 2. If the command execution timed out, check the	GPU monitoring metric data is missing. As a result, subsequent metrics may fail to be collected.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
						system logs and determine whether there is an issue with the system.	

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		GPU handle lost	gpuDeviceHandleLost	Major	The GPU metric information cannot be obtained, and the GPU may be lost.	1. Run **nvidia-smi** to check whether there are any errors reported. 2. Run **nvidia-smi -L** to check whether the number of GPUs is the same as the server specifications. 3. Submit a service ticket to contact on-call support.	All metrics of the GPU are lost.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Failed to listen to the XID of the GPU.	gpuDeviceXidLost	Major	Failed to listen to the XID metric.	1. Check whether the GPU is lost or damaged. 2. Submit a service ticket to contact on-call support.	Failed to obtain XID-related metrics of the GPU.
		Multiple NPU HBM ECC errors	NpuHbmMultiEccInfo	Informational	There are NPU HBM ECC errors.	This event is only a reference for other events. You do not need to handle it separately.	The NPU may not work properly.
		ReadOnly issues in OS	ReadOnlyFileSystem	Critical	The file system %s is read-only.	Check the disk health status.	The files cannot be written.
		NPU: driver and firmware not matching	NpuDriverFirmwareMismatch	Major	The NPU's driver and firmware do not match.	Obtain the matched version from the Ascend official website and reinstall it.	NPUs cannot be used.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		NPU: Docker container environment check	NpuContainerEnvSystem	Major	Docker was unavailable.	Check if Docker is normal.	Docker cannot be used.
				Major	The container plug-in Ascend-Docker-Runtime was not installed.	Install the container plug-in Ascend-Docker-Runtime. Or, the container cannot use Ascend cards.	NPUs cannot be attached to Docker containers.
				Major	IP forwarding was not enabled in the OS.	Check the **net.ipv4.ip_forward** configuration in the **/etc/sysctl.conf** file.	Docker containers experience network communication problems.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
				Major	The shared memory of the container was too small.	The default shared memory is 64 MB, which can be modified as needed. Method 1 Modify the **default-shm-size** field in the **/etc/docker/daemon.json** configuration file. Method 2 Use the **--shm-size** parameter in the **docker run** command to set the shared memory size of a container.	Distributed training will fail due to insufficient shared memory.
		NPU: RoCE NIC down	RoCELinkStatusDown	Major	The RoCE link of NPU card %d was down.	Check the NPU RoCE network port status.	The NPU NIC becomes unavailable.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		NPU: RoCE NIC health status abnormal	RoCEHealthStatusError	Major	The RoCE network health status of NPU %d was abnormal.	Check the health status of the NPU RoCE NIC.	The NPU NIC becomes unavailable.
		NPU: RoCE NIC configuration file **/etc/hccn.conf** not found	HccnConfNotExisted	Major	The RoCE NIC configuration file **/etc/hccn.conf** was not found.	Check whether the **/etc/hccn.conf** NIC configuration file can be found.	The RoCE NIC becomes unavailable.
		GPU: basic components abnormal	GpuEnvironmentSystem	Major	The **nvidia-smi** command was abnormal.	Check whether the GPU driver is normal.	The GPU driver is unavailable.
				Major	The nvidia-fabricmanager version was inconsistent with the GPU driver version.	Check the GPU driver version and nvidia-fabricmanager version.	The nvidia-fabricmanager cannot work properly, affecting GPU usage.
				Major	The container plug-in nvidia-container-toolkit was not installed.	Install the container plug-in nvidia-container-toolkit.	GPUs cannot be attached to Docker containers.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Local disk attachment inspection	MountDiskSystem	Major	The **/etc/fstab** file contains invalid UUIDs.	Ensure that the UUIDs in the **/etc/fstab** configuration file are correct. Or, the server may fail to be restarted.	The disk attachment process fails, preventing the server from restarting.
		GPU: incorrectly configured dynamic route for Ant series server	GpuRouteConfigError	Major	The dynamic route of the NIC %s of an Ant series server was not configured or was incorrectly configured. CMD [ip route]: %s | CMD [ip route show table all]: %s.	Configure the RoCE NIC route correctly.	The NPU network communication will be interrupted.
		NPU: RoCE port not split	RoCEUdpConfigError	Major	The RoCE UDP port was not split.	Check the RoCE UDP port configuration on the NPU.	The communication performance of NPUs is affected.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Warning of automatic system kernel upgrade	KernelUpgradeWarning	Major	Warning of automatic system kernel upgrade. Old version: %s; new version: %s.	System kernel upgrade may cause AI software exceptions. Check the system update logs and prevent the server from restarting.	The AI software may be unavailable.
		NPU environment command detection	NpuToolsWarning	Major	The hccn_tool was unavailable.	Check whether the NPU driver is normal.	The IP address and gateway of the RoCE NIC cannot be configured.
				Major	The npu-smi was unavailable.	Check whether the NPU driver is normal.	NPUs cannot be used.
				Major	The ascend-dmi was unavailable.	Check whether ToolBox is properly installed.	ascend-dmi cannot be used for performance analysis.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Warning of an NPU driver exception	NpuDriverAbnormalWarning	Major	The NPU driver was abnormal.	Reinstall the NPU driver.	NPUs cannot be used.
		GPU: invalid RoCE NIC configuration	GpuRoceNicConfigIncorrect	Major	The RoCE NIC of the GPU is incorrectly configured.	Contact O&M personnel.	The parameter plane network is abnormal, preventing the execution of the multi-node task.
		Local disk replacement to be authorized	localdisk_recovery_inquiring	Major	The local disk is faulty. Local disk replacement authorization is in progress.	Authorize local disk replacement.	Local disks are unavailable.
		Local disks being replaced	localdisk_recovery_executing	Major	The local disk is faulty and is being replaced.	When the replacement is complete, check whether the local disks are available.	Local disks are unavailable.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Local disks replaced	localdisk_recovery_completed	Major	The local disk is faulty and is replaced.	Wait until the services are running properly and check whether local disks are available.	None
		Local disk replacement failed	localdisk_recovery_failed	Major	The local disk is faulty and fails to be replaced.	Contact O&M personnel.	Local disks are unavailable.

Table 10-3 Elastic IP (EIP)

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
EIP	SYS.EIP	EIP bandwidth exceeded	EIPBandwidthOverflow	Major	The used bandwidth exceeded the purchased one, which may slow down the network or cause packet loss. The value of this event is the maximum value in a monitoring period, and the value of the EIP inbound and outbound bandwidth is the value at a specific time point in the period. The metrics are described as follows: **egressDropBandwidth**: dropped outbound packets (bytes) **egressAcceptBandwidth**: accepted outbound packets (bytes) **egressMaxBandwidthPerSec**: peak outbound bandwidth (byte/s) **ingressAcceptBandwidth**: accepted	Check whether the EIP bandwidth keeps increasing and whether services are normal. Increase bandwidth if necessary.	The network becomes slow or packets are lost.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
					inbound packets (bytes) **ingressMaxBandwidthPerSec**: peak inbound bandwidth (byte/s) **ingressDropBandwidth**: dropped inbound packets (bytes) **NOTE** EIP bandwidth overflow is available only in the following regions: CN North-Beijing1, CN North-Beijing4, CN North-Ulanqab1, CN East-Shanghai1, CN East-Shanghai2, CN Southwest-Guiyang1, and CN South-Guangzhou.		
		EIP released	deleteEip	Minor	The EIP was released.	Check whether the EIP was release by mistake.	The server that has the EIP bound cannot access the Internet.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		EIP blocked	blockEIP	Critical	The used bandwidth of an EIP exceeded 5 Gbit/s, the EIP were blocked and packets were discarded. Such an event may be caused by DDoS attacks.	Replace the EIP to prevent services from being affected. Locate and deal with the fault.	Services are impacted.
		EIP unblocked	unblockEIP	Critical	The EIP was unblocked.	Use the previous EIP again.	None
		EIP traffic scrubbing started	ddosCleanEIP	Major	Traffic scrubbing on the EIP was started to prevent DDoS attacks.	Check whether the EIP was attacked.	Services may be interrupted.
		EIP traffic scrubbing ended	ddosEndCleanEip	Major	Traffic scrubbing on the EIP to prevent DDoS attacks was ended.	Check whether the EIP was attacked.	Services may be interrupted.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		QoS bandwidth exceeded	EIPBandwidthRuleOverflow	Major	The used QoS bandwidth exceeded the allocated one, which may slow down the network or cause packet loss. The value of this event is the maximum value in a monitoring period, and the value of the EIP inbound and outbound bandwidth is the value at a specific time point in the period. **egressDropBandwidth**: dropped outbound packets (bytes) **egressAcceptBandwidth**: accepted outbound packets (bytes) **egressMaxBandwidthPerSec**: peak outbound bandwidth (byte/s) **ingressAcceptBandwidth**: accepted inbound packets (bytes) **ingressMaxBandwidthPerSec**: peak inbound	Check whether the EIP bandwidth keeps increasing and whether services are normal. Increase bandwidth if necessary.	The network becomes slow or packets are lost.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
					bandwidth (byte/s) **ingressDropBandwidth**: dropped inbound packets (bytes)		
		EIP unbound with resources	EipNotBoundStatus	Major	The EIP is unbound with instance resources.	None	When an EIP is unbound, you will be billed for IP reservation fees and bandwidth fees (billed by bandwidth).

Table 10-4 Advanced Anti-DDoS (AAD)

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
AAD	SYS.DDOS	DDoS Attack Events	ddosAttackEvents	Major	A DDoS attack occurs in the AAD protected lines.	Judge the impact on services based on the attack traffic and attack type. If the attack traffic exceeds your purchased elastic bandwidth, change to another line or increase your bandwidth.	Services may be interrupted.
		Domain name scheduling event	domainNameDispatchEvents	Major	The high-defense CNAME corresponding to the domain name is scheduled, and the domain name is resolved to another high-defense IP address.	Pay attention to the workloads involving the domain name.	Services are not affected.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Blackhole event	blackHoleEvents	Major	The attack traffic exceeds the purchased AAD protection threshold.	A blackhole is canceled after 30 minutes by default. The actual blackhole duration is related to the blackhole triggering times and peak attack traffic on the current day. The maximum duration is 24 hours. If you need to permit access before a blackhole becomes ineffective, contact technical support.	Services may be interrupted.
		Cancel Blackhole	cancelBlackHole	Informational	The customer's AAD instance recovers from the black hole state.	This is only a prompt and no action is required.	Customer services recover.
		IP address scheduling triggered	ipDispatchEvents	Major	IP route changed	Check the workloads of the IP address.	Services are not affected.

Table 10-5 Elastic Load Balance (ELB)

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
ELB	SYS.ELB	The backend servers are unhealthy.	healthCheckUnhealthy	Major	Generally, this problem occurs because backend server services are offline. This event will not be reported after it is reported for several times.	Ensure that the backend servers are running properly.	ELB does not forward requests to unhealthy backend servers. If all backend servers in the backend server group are detected unhealthy, services will be interrupted.
		The backend server is detected healthy.	healthCheckRecovery	Minor	The backend server is detected healthy.	No further action is required.	The load balancer can properly route requests to the backend server.

Table 10-6 Cloud Backup and Recovery (CBR)

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
CBR	SYS.CBR	Failed to create the backup.	backupFailed	Critical	The backup failed to be created.	Manually create a backup or contact customer service.	Data loss may occur.
		Failed to restore the resource using a backup.	restorationFailed	Critical	The resource failed to be restored using a backup.	Restore the resource using another backup or contact customer service.	Data loss may occur.
		Failed to delete the backup.	backupDeleteFailed	Critical	The backup failed to be deleted.	Try again later or contact customer service.	Charging may be abnormal.
		Failed to delete the vault.	vaultDeleteFailed	Critical	The vault failed to be deleted.	Try again later or contact technical support.	Charging may be abnormal.
		Replication failure	replicationFailed	Critical	The backup failed to be replicated.	Try again later or contact technical support.	Data loss may occur.
		The backup is created successfully.	backupSucceeded	Major	The backup was created.	None	None

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Resource restoration using a backup succeeded.	restorationSucceeded	Major	The resource was restored using a backup.	Check whether the data is successfully restored.	None
		The backup is deleted successfully.	backupDeletionSucceeded	Major	The backup was deleted.	None	None
		The vault is deleted successfully.	vaultDeletionSucceeded	Major	The vault was deleted.	None	None
		Replication success	replicationSucceeded	Major	The backup was replicated successfully.	None	None
		Client offline	agentOffline	Critical	The backup client was offline.	Ensure that the Agent status is normal and the backup client can be connected to Huawei Cloud.	Backup tasks may fail.
		Client online	agentOnline	Major	The backup client was online.	None	None

Table 10-7 Relational Database Service (RDS) — resource exception

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
RDS	SYS.RDS	DB instance creation failure	createInstanceFailed	Major	Generally, the cause is that the number of disks is insufficient due to quota limits, or underlying resources are exhausted.	The selected resource specifications are insufficient. Select other available specifications and try again.	DB instances cannot be created.
		Full backup failure	fullBackupFailed	Major	A single full backup failure does not affect the files that have been successfully backed up, but prolong the incremental backup time during the point-in-time restore (PITR).	Try again.	Restoration using backups will be affected.
		Read replica promotion failure	activeStandBySwitchFailed	Major	The standby DB instance does not take over workloads from the primary DB instance due to network or server failures. The original primary DB instance continues to provide services within a short time.	Perform the operation again during off-peak hours.	The primary/standby switchover will fail.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Replication status abnormal	abnormalReplicationStatus	Major	The possible causes are as follows: The replication delay between the primary instance and the standby instance or a read replica is too long, which usually occurs when a large amount of data is being written to databases or a large transaction is being processed. During peak hours, data may be blocked. The network between the primary instance and the standby instance or a read replica is disconnected.	Database replication is being repaired. You will be notified immediately after the repair.	The replication status is abnormal.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Replication status recovered	replicationStatusRecovered	Major	The replication delay between the primary and standby instances is within the normal range, or the network connection between them has restored.	Check whether services are running properly.	Replication status is recovered.
		DB instance faulty	faultyDBInstance	Major	A single or primary DB instance was faulty due to a catastrophic failure, for example, server failure.	Instance status is being repaired. You will be notified immediately after the repair.	The instance status is abnormal.
		DB instance recovered	DBInstanceRecovered	Major	RDS rebuilds the standby DB instance with its high availability. After the instance is rebuilt, this event will be reported.	The DB instance status is normal. Check whether services are running properly.	The instance is recovered.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Failure of changing single DB instance to primary/ standby	singleToHaFailed	Major	A fault occurs when RDS is creating the standby DB instance or configuring replication between the primary and standby DB instances. The fault may occur because resources are insufficient in the data center where the standby DB instance is located.	Automatic retry is in progress.	Changing a single DB instance to primary/ standby failed.
		Database process restarted	DatabaseProcessRestarted	Major	The database process is stopped due to insufficient memory or high load.	Check whether services are running properly.	The primary instance is restarted. Services are interrupted for a short period of time.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Instance storage full	instanceDiskFull	Major	Generally, the cause is that the data space usage is too high.	Scale up the storage.	The instance storage is used up. No data can be written into databases.
		Instance storage full recovered	instanceDiskFullRecovered	Major	The instance disk is recovered.	Check whether services are running properly.	The instance has available storage.
		Kafka connection failed	kafkaConnectionFailed	Major	The network is unstable or the Kafka server does not work properly.	Check whether services are affected.	None

Table 10-8 Relational Database Service (RDS) — operations

Event Source	Namespace	Event Name	Event ID	Event Severity	Description
RDS	SYS.RDS	Reset administrator password	resetPassword	Major	The password of the database administrator is reset.

Event Source	Name space	Event Name	Event ID	Event Severity	Description
		Operate DB instance	instanceAction	Major	The storage space is scaled or the instance class is changed.
		Delete DB instance	deleteInstance	Minor	The DB instance is deleted.
		Modify backup policy	setBackupPolicy	Minor	The backup policy is modified.
		Modify parameter group	updateParameterGroup	Minor	The parameter group is modified.
		Delete parameter group	deleteParameterGroup	Minor	The parameter group is deleted.
		Reset parameter group	resetParameterGroup	Minor	The parameter group is reset.
		Change database port	changeInstancePort	Major	The database port is changed.
		Primary/ standby switchover or failover	PrimaryStandbySwitched	Major	A switchover or failover is performed.

Table 10-9 Document Database Service (DDS)

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
DDS	SYS.DDS	DB instance creation failure	DDSCreateInstanceFailed	Major	A DDS instance fails to be created due to insufficient disks, quotas, and underlying resources.	Check the number and quota of disks. Release resources and create DDS instances again.	DDS instances cannot be created.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Replication failed	DDSAbnormalReplicationStatus	Major	The possible causes are as follows: 1. The replication delay between the primary instance and the standby instance or a read replica is too long, which usually occurs when a large amount of data is being written to databases or a large transaction is being processed. During peak hours, data may be blocked. 2. The network between the primary instance and the standby instance or a read replica is	Submit a service ticket.	1. Read and write operations on the original instance are not interrupted, but data updates on the standby instance may experience delays. 2. The replication delay keeps growing between the primary and standby instances, and the standby instance may be disconnected.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
					disconnected.		
		Replication status recovered	DDSReplicationStatusRecovered	Major	The replication delay between the primary and standby instances is within the normal range, or the network connection between them has restored.	No action is required.	None
		DB instance failed	DDSFaultyDBInstance	Major	This event is a key alarm event and is reported when an instance is faulty due to a disaster or a server failure.	Submit a service ticket.	The database service may be unavailable.
		DB instance recovered	DDSDBInstanceRecovered	Major	If a disaster occurs, NoSQL provides an HA tool to automatically or manually rectify the fault. After the fault is rectified, this event is reported.	No action is required.	None

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Faulty node	DDSFaultyDBNode	Major	This event is a key alarm event and is reported when a database node is faulty due to a disaster or a server failure.	Check whether the database service is available and submit a service ticket.	The database service may be unavailable.
		Node recovered	DDSDBNodeRecovered	Major	If a disaster occurs, NoSQL provides an HA tool to automatically or manually rectify the fault. After the fault is rectified, this event is reported.	No action is required.	None
		Primary/standby switchover or failover	DDSPrimaryStandbySwitched	Major	This event is reported when a primary/standby switchover or a failover is triggered.	No action is required.	None

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Insufficient storage space	DDSRiskyDataDiskUsage	Major	The storage space is insufficient.	Scale up storage space. For details, see section "Scaling Up Storage Space" in the corresponding user guide.	The instance is set to read-only and data cannot be written to the instance.
		Data disk expanded and being writable	DDS DataDiskUsageRecovered	Major	The capacity of a data disk has been expanded and the data disk becomes writable.	No further action is required.	No adverse impact.
		Schedule for deleting a KMS key	planDeleteKmsKey	Major	A request to schedule deletion of a KMS key was submitted.	After the KMS key is scheduled to be deleted, either decrypt the data encrypted by KMS key in a timely manner or cancel the key deletion.	After the KMS key is deleted, users cannot encrypt disks.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Full backup failure	DDSFullBackupFailed	Major	A single full backup failure does not affect the files that have been successfully backed up, but prolong the incremental backup time during the point-in-time restore (PITR).	Try again.	Full backup fail.

Table 10-10 GeminiDB

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
GeminiDB	SYS.NoSQL	DB instance creation failed	NoSQLCreateInstanceFailed	Major	The instance quota or underlying resources are insufficient.	Release the instances that are no longer used and try to provision them again, or submit a service ticket to adjust the quota.	DB instances cannot be created.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Specifications modification failed	NoSQLResizeInstanceFailed	Major	The underlying resources are insufficient.	Submit a service ticket. The O&M personnel will coordinate resources in the background, and then you need to change the specifications again.	Services are interrupted.
		Node adding failed	NoSQLAddNodesFailed	Major	The underlying resources are insufficient.	Submit a service ticket. The O&M personnel will coordinate resources in the background, and then you delete the node that failed to be added and add a new node.	None
		Node deletion failed	NoSQLDeleteNodesFailed	Major	The underlying resources fail to be released.	Delete the node again.	None

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Storage space scale-up failed	NoSQLScaleUpStorageFailed	Major	The underlying resources are insufficient.	Submit a service ticket. The O&M personnel will coordinate resources in the background and then you scale up the storage space again.	Services may be interrupted.
		Password reset failed	NoSQLResetPasswordFailed	Major	Resetting the password times out.	Reset the password again.	None
		Parameter group change failed	NoSQLUpdateInstanceParamGroupFailed	Major	Changing a parameter group times out.	Change the parameter group again.	None
		Backup policy configuration failed	NoSQLSetBackupPolicyFailed	Major	The database connection is abnormal.	Configure the backup policy again.	None
		Manual backup creation failed	NoSQLCreateManualBackupFailed	Major	The backup files fail to be exported or uploaded.	Submit a service ticket to the O&M personnel.	Data cannot be backed up.
		Automated backup creation failed	NoSQLCreateAutomatedBackupFailed	Major	The backup files fail to be exported or uploaded.	Submit a service ticket to the O&M personnel.	Data cannot be backed up.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Faulty DB instance	NoSQLFaultyDBInstance	Major	This event is a key alarm event and is reported when an instance is faulty due to a disaster or a server failure.	Submit a service ticket.	The database service may be unavailable.
		DB instance recovered	NoSQLDBInstanceRecovered	Major	If a disaster occurs, NoSQL provides an HA tool to automatically or manually rectify the fault. After the fault is rectified, this event is reported.	No action is required.	None
		Faulty node	NoSQLFaultyDBNode	Major	This event is a key alarm event and is reported when a database node is faulty due to a disaster or a server failure.	Check whether the database service is available and submit a service ticket.	The database service may be unavailable.
		Node recovered	NoSQLDBNodeRecovered	Major	If a disaster occurs, NoSQL provides an HA tool to automatically or manually rectify the fault. After the fault is rectified, this event is reported.	No action is required.	None

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Primary/standby switchover or failover	NoSQLPrimaryStandbySwitched	Major	This event is reported when a primary/standby switchover is performed or a failover is triggered.	No action is required.	None
		HotKey occurred	HotKeyOccurs	Major	The primary key is improperly configured. As a result, hotspot data is distributed in one partition. The improper application design causes frequent read and write operations on a key.	1. Choose a proper partition key. 2. Add service cache. The service application reads hotspot data from the cache first.	The service request success rate is affected, and the cluster performance and stability also be affected.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		BigKey occurred	BigKeyOccurs	Major	The primary key design is improper. The number of records or data in a single partition is too large, causing unbalanced node loads.	1. Choose a proper partition key. 2. Add a new partition key for hashing data.	As the data in the large partition increases, the cluster stability deteriorates.
		Insufficient storage space	NoSQLRiskyDataDiskUsage	Major	The storage space is insufficient.	Scale up storage space. For details, see section "Scaling Up Storage Space" in the corresponding user guide.	The instance is set to read-only and data cannot be written to the instance.
		Data disk expanded and being writable	NoSQLDataDiskUsageRecovered	Major	The capacity of a data disk has been expanded and the data disk becomes writable.	No operation is required.	None

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Index creation failed	NoSQLCreateIndexFailed	Major	The service load exceeds what the instance specifications can take. In this case, creating indexes consumes more instance resources. As a result, the response is slow or even frame freezing occurs, and the creation times out.	Select the matched instance specifications based on the service load. Create indexes during off-peak hours. Create indexes in the background. Select indexes as required.	The index fails to be created or is incomplete. As a result, the index is invalid. Delete the index and create an index.
		Write speed decreased	NoSQLStallingOccurs	Major	The write speed is fast, which is close to the maximum write capability allowed by the cluster scale and instance specifications. As a result, the flow control mechanism of the database is triggered, and requests may fail.	1. Adjust the cluster scale or node specifications based on the maximum write rate of services. 2. Measures the maximum write rate of services.	The success rate of service requests is affected.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Data write stopped	NoSQLStoppingOccurs	Major	The data write is too fast, reaching the maximum write capability allowed by the cluster scale and instance specifications. As a result, the flow control mechanism of the database is triggered, and requests may fail.	1. Adjust the cluster scale or node specifications based on the maximum write rate of services. 2. Measures the maximum write rate of services.	The success rate of service requests is affected.
		Database restart failed	NoSQLRestartDBFailed	Major	The instance status is abnormal.	Submit a service ticket to the O&M personnel.	The DB instance status may be abnormal.
		Restoration to new DB instance failed	NoSQLRestoreToNewInstanceFailed	Major	The underlying resources are insufficient.	Submit a service order to ask the O&M personnel to coordinate resources in the background and add new nodes.	Data cannot be restored to a new DB instance.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Restoration to existing DB instance failed	NoSQLRestoreToExistInstanceFailed	Major	The backup file fails to be downloaded or restored.	Submit a service ticket to the O&M personnel.	The current DB instance may be unavailable.
		Backup file deletion failed	NoSQLDeleteBackupFailed	Major	The backup files fail to be deleted from OBS.	Delete the backup files again.	None
		Failed to enable Show Original Log	NoSQLSwitchSlowlogPlainTextFailed	Major	The DB engine does not support this function.	Refer to the *GaussDB NoSQL User Guide* to ensure that the DB engine supports Show Original Log. Submit a service ticket to the O&M personnel.	None
		EIP binding failed	NoSQLBindEipFailed	Major	The node status is abnormal, an EIP has been bound to the node, or the EIP to be bound is invalid.	Check whether the node is normal and whether the EIP is valid.	The DB instance cannot be accessed from the Internet.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		EIP unbinding failed	NoSQLUnbindEipFailed	Major	The node status is abnormal or the EIP has been unbound from the node.	Check whether the node and EIP status are normal.	None
		Parameter modification failed	NoSQLModifyParameterFailed	Major	The parameter value is invalid.	Check whether the parameter value is within the valid range and submit a service ticket to the O&M personnel.	None
		Parameter group application failed	NoSQLApplyParameterGroupFailed	Major	The instance status is abnormal. As a result, the parameter group cannot be applied.	Submit a service ticket to the O&M personnel.	None
		Failed to enable or disable SSL	NoSQLSwitchSSLFailed	Major	Enabling or disabling SSL times out.	Try again or submit a service ticket. Do not change the connection mode.	The connection mode cannot be changed.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Row size too large	LargeRowOccurs	Major	If there is too much data in a single row, queries may time out, causing faults like OOM error.	1. Control the length of each column and row so that the sum of key and value lengths in each row does not exceed the preset threshold. 2. Check whether there are invalid writes or encoding resulting in large keys or values.	If there are rows that are too large, the cluster performance will deteriorate as the data volume grows.
		Schedule for deleting a KMS key	planDeleteKmsKey	Major	A request to schedule deletion of a KMS key was submitted.	After the KMS key is scheduled to be deleted, either decrypt the data encrypted by KMS key in a timely manner or cancel the key deletion.	After the KMS key is deleted, users cannot encrypt disks.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Too many query tombstones	TooManyQueryTombstones	Major	If there are too many query tombstones, queries may time out, affecting query performance.	Select right query and deleting methods and avoid long range queries.	Queries may time out, affecting query performance.
		Too large collection column	TooLargeCollectionColumn	Major	If there are too many elements in a collection column, queries to the column will fail.	1. Limit elements in a collection column. 2. Check for abnormal writes or coding at the service side.	Queries to the collection column will fail.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		GeminiDB Influx instance connection limit reached	InfluxDBConnectionFull	Major	The connections on the instance node reach the upper limit.	1. Upgrade specifications if they cannot meet service requirements. 2. Check whether the client properly manages connections, for example, whether there are unreleased or long connections.	If no new connection can be created on a node, the client may fail to connect to a GeminiDB Influx instance. As a result, services may become instable.
		High availability switchover	nodeHaSwitch	Major	The high availability switchover is triggered by underlying network jitters.	Check whether the business is normal and it can be restored automatically.	The network jitter causes a few seconds of delay.

Table 10-11 GaussDB(for MySQL)

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
GaussDB(for MySQL)	SYS.GAUSSDB	Incremental backup failure	TaurusIncrementalBackupInstanceFailed	Major	The network between the instance and the management plane (or the OBS) is disconnected, or the backup environment created for the instance is abnormal.	Submit a service ticket.	Backup jobs fail.
		Read replica creation failure	addReadonlyNodesFailed	Major	The quota is insufficient or underlying resources are exhausted.	Check the read replica quota. Release resources and create read replicas again.	Read replicas fail to be created.
		DB instance creation failure	createInstanceFailed	Major	The instance quota or underlying resources are insufficient.	Check the instance quota. Release resources and create instances again.	DB instances fail to be created.
		Read replica promotion failure	activeStandBySwitchFailed	Major	The read replica fails to be promoted to the primary node due to network or server failures. The original primary node takes over services quickly.	Submit a service ticket.	The read replica fails to be promoted to the primary node.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Instance specifications change failure	flavorAlterationFailed	Major	The quota is insufficient or underlying resources are exhausted.	Submit a service ticket.	Instance specifications fail to be changed.
		Faulty DB instance	TaurusInstanceRunningStatusAbnormal	Major	The instance process is faulty or the communications between the instance and the DFV storage are abnormal.	Submit a service ticket.	Services may be affected.
		DB instance recovered	TaurusInstanceRunningStatusRecovered	Major	The instance is recovered.	Observe the service running status.	None
		Faulty node	TaurusNodeRunningStatusAbnormal	Major	The node process is faulty or the communications between the node and the DFV storage are abnormal.	Observe the instance and service running statuses.	A read replica may be promoted to the primary node.
		Node recovered	TaurusNodeRunningStatusRecovered	Major	The node is recovered.	Observe the service running status.	None

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Read replica deletion failure	TaurusDeleteReadOnlyNodeFailed	Major	The communications between the management plane and the read replica are abnormal or the VM fails to be deleted from IaaS.	Submit a service ticket.	Read replicas fail to be deleted.
		Password reset failure	TaurusResetInstancePasswordFailed	Major	The communications between the management plane and the instance are abnormal or the instance is abnormal.	Check the instance status and try again. If the fault persists, submit a service ticket.	Passwords fail to be reset for instances.
		DB instance reboot failure	TaurusRestartInstanceFailed	Major	The network between the management plane and the instance is abnormal or the instance is abnormal.	Check the instance status and try again. If the fault persists, submit a service ticket.	Instances fail to be rebooted.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Restoration to new DB instance failure	TaurusRestoreToNewInstanceFailed	Major	The instance quota is insufficient, underlying resources are exhausted, or the data restoration logic is incorrect.	If the new instance fails to be created, check the instance quota, release resources, and try to restore to a new instance again. In other cases, submit a service ticket.	Back up data fails to be restored to new instances.
		EIP binding failure	TaurusBindEIPToInstanceFailed	Major	The binding task fails.	Submit a service ticket.	EIPs fail to be bound to instances.
		EIP unbinding failure	TaurusUnbindEIPFromInstanceFailed	Major	The unbinding task fails.	Submit a service ticket.	EIPs fail to be unbound from instances.
		Parameter modification failure	TaurusUpdateInstanceParameterFailed	Major	The network between the management plane and the instance is abnormal or the instance is abnormal.	Check the instance status and try again. If the fault persists, submit a service ticket.	Instance parameters fail to be modified.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Parameter template application failure	TaurusApplyParameterGroupToInstanceFailed	Major	The network between the management plane and instances is abnormal or the instances are abnormal.	Check the instance status and try again. If the fault persists, submit a service ticket.	Parameter templates fail to be applied to instances.
		Full backup failure	TaurusBackupInstanceFailed	Major	The network between the instance and the management plane (or the OBS) is disconnected, or the backup environment created for the instance is abnormal.	Submit a service ticket.	Back up jobs fail.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Primary/standby failover	TaurusActiveStandbySwitched	Major	When the network, physical machine, or database of the primary node is faulty, the system promotes a read replica to primary based on the failover priority to ensure service continuity.	1. Check whether the service is running properly. 2. Check whether an alarm is generated, indicating that the read replica failed to be promoted to primary.	During the failover, database connection is interrupted for a short period of time. After the failover is complete, you can reconnect to the database.
		Database read-only	NodeReadonlyMode	Major	The database supports only query operations.	Submit a service ticket.	After the database becomes read-only, write operations cannot be processed.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Database read/write	NodeReadWriteMode	Major	The database supports both write and read operations.	Submit a service ticket.	None
		Instance DR switchover	DisasterSwitchOver	Major	If an instance is faulty and unavailable, a switchover is performed to ensure that the instance continues to provide services.	Contact technical support.	The database connection is intermittently interrupted. The HA service switches workloads from the primary node to a read replica and continues to provide services.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Database process restarted	TaurusDatabaseProcessRestarted	Major	The database process is stopped due to insufficient memory or high load.	Log in to the Cloud Eye console. Check whether the memory usage increases sharply or the CPU usage is too high for a long time. You can increase the specifications or optimize the service logic.	When the database process is suspended, workloads on the node are interrupted. In this case, the HA service automatically restarts the database process and attempts to recover the workloads.

Table 10-12 GaussDB

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
GaussDB	SYS.GAUSSDBV5	Process status alarm	ProcessStatusAlarm	Major	Key processes exit, including CMS/CMA, ETCD, GTM, CN, and DN processes.	Wait until the process is automatically recovered or a primary/standby failover is automatically performed. Check whether services are recovered. If no, contact SRE engineers.	If processes on primary nodes are faulty, services are interrupted and then rolled back. If processes on standby nodes are faulty, services are not affected.
		Component status alarm	ComponentStatusAlarm	Major	Key components do not respond, including CMA, ETCD, GTM, CN, and DN components.	Wait until the process is automatically recovered or a primary/standby failover is automatically performed. Check whether services are recovered. If no, contact SRE engineers.	If processes on primary nodes do not respond, neither do the services. If processes on standby nodes are faulty, services are not affected.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Cluster status alarm	ClusterStatusAlarm	Major	The cluster status is abnormal. For example, the cluster is read-only; majority of ETCDs are faulty; or the cluster resources are unevenly distributed.	Contact SRE engineers.	If the cluster status is read-only, only read services are processed. If the majority of ETCDs are fault, the cluster is unavailable. If resources are unevenly distributed, the instance performance and reliability deteriorate.
		Hardware resource alarm	HardwareResourceAlarm	Major	A major hardware fault occurs in the instance, such as disk damage or GTM network fault.	Contact SRE engineers.	Some or all services are affected.
		Status transition alarm	StateTransitionAlarm	Major	The following events occur in the instance: DN build failure, forcible DN promotion, primary/standby DN switchover/failover, or primary/standby GTM switchover/failover.	Wait until the fault is automatically rectified and check whether services are recovered. If no, contact SRE engineers.	Some services are interrupted.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Other abnormal alarm	OtherAbnormalAlarm	Major	Disk usage threshold alarm	Focus on service changes and scale up storage space as needed.	If the used storage space exceeds the threshold, storage space cannot be scaled up.
		DB instance creation failure	GaussDBV5CreateInstanceFailed	Major	Instances fail to be created because the quota is insufficient or underlying resources are exhausted.	Release the instances that are no longer used and try to provision them again, or submit a service ticket to adjust the quota.	DB instances cannot be created.
		Node adding failure	GaussDBV5ExpandClusterFailed	Major	The underlying resources are insufficient.	Submit a service ticket. The O&M personnel will coordinate resources in the background, and then you delete the node that failed to be added and add a new node.	None

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Storage scale-up failure	GaussDBV5EnlargeVolumeFailed	Major	The underlying resources are insufficient.	Submit a service ticket. The O&M personnel will coordinate resources in the background and then you scale up the storage space again.	Services may be interrupted.
		Reboot failure	GaussDBV5RestartInstanceFailed	Major	The network is abnormal.	Retry the reboot operation or submit a service ticket to the O&M personnel.	The database service may be unavailable.
		Full backup failure	GaussDBV5FullBackupFailed	Major	The backup files fail to be exported or uploaded.	Submit a service ticket to the O&M personnel.	Data cannot be backed up.
		Differential backup failure	GaussDBV5DifferentialBackupFailed	Major	The backup files fail to be exported or uploaded.	Submit a service ticket to the O&M personnel.	Data cannot be backed up.
		Backup deletion failure	GaussDBV5DeleteBackupFailed	Major	The backup files fail to be deleted from OBS.	Delete the backup files again.	None

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		EIP binding failure	GaussDBV5BindEIPFailed	Major	The EIP is bound to another resource.	Submit a service ticket to the O&M personnel.	The instance cannot be accessed from the public network.
		EIP unbinding failure	GaussDBV5UnbindEIPFailed	Major	The network is faulty or EIP is abnormal.	Unbind the IP address again or submit a service ticket to the O&M personnel.	IP addresses may be residual.
		Parameter template application failure	GaussDBV5ApplyParamFailed	Major	Modifying a parameter template times out.	Modify the parameter template again.	None
		Parameter modification failure	GaussDBV5UpdateInstanceParamGroupFailed	Major	Modifying a parameter template times out.	Modify the parameter template again.	None
		Backup and restoration failure	GaussDBV5RestoreFromBcakupFailed	Major	The underlying resources are insufficient or backup files fail to be downloaded.	Submit a service ticket.	The database service may be unavailable during the restoration failure.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Failed to upgrade the hot patch	GaussDBV5UpgradeHotfixFailed	Major	Generally, this fault is caused by an error reported during kernel upgrade.	View the error information about the workflow and redo or skip the job.	None
		DB instance faulty	GaussDBV5FaultyDBInstance	Major	This event is a key alarm event and is reported when an instance is faulty due to a disaster or a server failure.	Submit a service ticket.	The database service may be unavailable.
		DB instance recovered	GaussDBV5InstanceRecovered	Major	GaussDB(openGauss) provides an HA tool for automated or manual rectification of faults. After the fault is rectified, this event is reported.	No action is required.	None

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Faulty node	GaussDBV5FaultyDBNode	Major	This event is a key alarm event and is reported when a database node is faulty due to a disaster or a server failure.	This event is a key alarm event and is reported when a database node is faulty due to a disaster or a server failure.	The database service may be unavailable.
		Node recovered	GaussDBV5FaultyDBNodeRecovered	Major	GaussDB(openGauss) provides an HA tool for automated or manual rectification of faults. After the fault is rectified, this event is reported.	No action is required.	None

Table 10-13 Distributed Database Middleware (DDM)

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
DDM	SYS.DDM	Failed to create a DDM instance	createDdmInstanceFailed	Major	The underlying resources are insufficient.	Release resources and create the instance again.	DDM instances cannot be created.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Failed to change class of a DDM instance	resizeFlavorFailed	Major	The underlying resources are insufficient.	Submit a service ticket to the O&M personnel to coordinate resources and try again.	Services on some nodes are interrupted.
		Failed to scale out a DDM instance	enlargeNodeFailed	Major	The underlying resources are insufficient.	Submit a service ticket to the O&M personnel to coordinate resources, delete the node that fails to be added, and add a node again.	The instance fails to be scaled out.
		Failed to scale in a DDM instance	reduceNodeFailed	Major	The underlying resources fail to be released.	Submit a service ticket to the O&M personnel to release resources.	The instance fails to be scaled in.
		Failed to restart a DDM instance	restartInstanceFailed	Major	The DB instances associated are abnormal.	Check whether DB instances associated are normal. If the instances are normal, submit a service ticket to the O&M personnel.	Services on some nodes are interrupted.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Failed to create a schema	createLogicDbFailed	Major	The possible causes are as follows: • The password for the DB instance account is incorrect. • The security group of the DDM instance and the associated DB instance are incorrectly configured. As a result, the DDM instance cannot communicate with the associated DB instance.	Check whether • The username and password of the DB instance are correct. • The security groups associated with the DDM instance and underlying database instance are correctly configured.	Services cannot run properly.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Failed to bind an EIP	bindEipFailed	Major	The EIP is abnormal.	Try again later. In case of emergency, contact O&M personnel to rectify the fault.	The DDM instance cannot be accessed from the Internet.
		Failed to scale out a schema	migrateLogicDbFailed	Major	The underlying resources fail to be processed.	Submit a service ticket to the O&M personnel.	The schema cannot be scaled out.
		Failed to re-scale out a schema	retryMigrateLogicDbFailed	Major	The underlying resources fail to be processed.	Submit a service ticket to the O&M personnel.	The schema cannot be scaled out.

Table 10-14 Cloud Phone Server

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
CPH	SYS.CPH	Server shutdown	cphServerOsShutdown	Major	The cloud phone server was stopped • on the management console. • by calling APIs.	Deploy service applications in HA mode. After the fault is rectified, check whether services recover.	Services are interrupted.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Server abnormal shutdown	cphServerShutdown	Major	The cloud phone server was stopped unexpectedly. Possible causes are as follows: • The cloud phone server was powered off unexpectedly. • The cloud phone server was stopped due to hardware faults.	Deploy service applications in HA mode. After the fault is rectified, check whether services recover.	Services are interrupted.
		Server reboot	cphServerOsReboot	Major	The cloud phone server was rebooted • on the management console. • by calling APIs.	Deploy service applications in HA mode. After the fault is rectified, check whether services recover.	Services are interrupted.
		Server abnormal reboot	cphServerReboot	Major	The cloud phone server was rebooted unexpectedly due to • OS faults. • hardware faults.	Deploy service applications in HA mode. After the fault is rectified, check whether services recover.	Services are interrupted.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Network disconnection	cphServerlinkDown	Major	The network where the cloud phone server was deployed was disconnected. Possible causes are as follows: ● The cloud phone server was stopped unexpectedly and rebooted. ● The switch was faulty. ● The gateway node was faulty.	Deploy service applications in HA mode. After the fault is rectified, check whether services recover.	Services are interrupted.
		PCIe error	cphServerPcieError	Major	The PCIe device or main board on the cloud phone server was faulty.	Deploy service applications in HA mode. After the fault is rectified, check whether services recover.	The network or disk read/write is affected.
		Disk error	cphServerDiskError	Major	The disk on the cloud phone server was faulty due to ● disk backplane faults. ● disk faults.	Deploy service applications in HA mode. After the fault is rectified, check whether services recover.	Data read/write services are affected, or the BMS cannot be started.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Storage error	cphServerStorageError	Major	The cloud phone server could not connect to EVS disks. Possible causes are as follows: • The SDI card was faulty. • Remote storage devices were faulty.	Deploy service applications in HA mode. After the fault is rectified, check whether services recover.	Data read/ write services are affected, or the BMS cannot be started.
		GPU offline	cphServerGpuOffline	Major	GPU of the cloud phone server was loose and disconnected.	Stop the cloud phone server and reboot it.	Faults occur on cloud phones whose GPUs are disconnected. Cloud phones cannot run properly even if they are restarted or reconfigured.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		GPU timeout	cphServerGpuTimeOut	Major	GPU of the cloud phone server timed out.	Reboot the cloud phone server.	Cloud phones whose GPUs timed out cannot run properly and are still faulty even if they are restarted or reconfigured.
		Disk space full	cphServerDiskFull	Major	Disk space of the cloud phone server was used up.	Clear the application data in the cloud phone to release space.	Cloud phone is sub-healthy, prone to failure, and unable to start.
		Disk readonly	cphServerDiskReadOnly	Major	The disk of the cloud phone server became read-only.	Reboot the cloud phone server.	Cloud phone is sub-healthy, prone to failure, and unable to start.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Cloud phone metadata damaged	cphPhoneMetaDataDamage	Major	Cloud phone metadata was damaged.	Contact O&M personnel.	The cloud phone cannot run properly even if it is restarted or reconfigured.
		GPU failed	gpuAbnormal	Critical	The GPU was faulty.	Submit a service ticket.	Services are interrupted.
		GPU recovered	gpuNormal	Informational	The GPU was running properly.	No further action is required.	None
		Kernel crash	kernelCrash	Critical	The kernel log indicated crash.	Submit a service ticket.	Services are interrupted during the crash.
		Kernel OOM	kernelOom	Major	The kernel log indicated out of memory.	Submit a service ticket.	Services are interrupted.
		Hardware malfunction	hardwareError	Critical	The kernel log indicated **Hardware Error**.	Submit a service ticket.	Services are interrupted.
		PCIe error	pcieAer	Critical	The kernel log indicated **PCIe Bus Error**.	Submit a service ticket.	Services are interrupted.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		SCSI error	scsiError	Critical	The kernel log indicated SCSI Error.	Submit a service ticket.	Services are interrupted.
		Image storage became read-only	partReadOnly	Critical	The image storage became read-only.	Submit a service ticket.	Services are interrupted.
		Image storage superblock damaged	badSuperBlock	Critical	The superblock of the file system of the image storage was damaged.	Submit a service ticket.	Services are interrupted.
		Image storage /.sharedpath/master became read-only	isuladMasterReadOnly	Critical	Mount point /.shared path/master of the image storage became read-only.	Submit a service ticket.	Services are interrupted.
		Cloud phone data disk became read-only	cphDiskReadOnly	Critical	The cloud phone data disk became read-only.	Submit a service ticket.	Services are interrupted.
		Cloud phone data disk superblock damaged	cphDiskBadSuperBlock	Critical	The superblock of the file system of the cloud phone data disk was damaged.	Submit a service ticket.	Services are interrupted.

Table 10-15 Layer 2 Connection Gateway (L2CG)

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
L2CG	SYS.ESW	IP addresses conflicted	IPConflict	Major	A cloud server and an on-premises server that need to communicate use the same IP address.	Check the ARP and switch information to locate the servers that have the same IP address and change the IP address.	The communications between the on-premises and cloud servers may be abnormal.

Table 10-16 Virtual Private Cloud (VPC)

Event Source	Namespace	Event Name	Event ID	Event Severity
VPC	SYS.VPC	VPC deleted	deleteVpc	Major
		VPC modified	modifyVpc	Minor
		Subnet deleted	deleteSubnet	Minor
		Subnet modified	modifySubnet	Minor
		Bandwidth modified	modifyBandwidth	Minor
		VPN deleted	deleteVpn	Major
		VPN modified	modifyVpn	Minor

Table 10-17 Elastic Volume Service (EVS)

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
EVS	SYS.EVS	Update disk	updateVolume	Minor	Update the name and description of an EVS disk.	No further action is required.	None
		Expand disk	extendVolume	Minor	Expand an EVS disk.	No further action is required.	None
		Delete disk	deleteVolume	Major	Delete an EVS disk.	No further action is required.	Deleted disks cannot be recovered.
		QoS upper limit reached **NOTE** This event is no longer supported for EVS and will be removed from Cloud Eye.	reachQoS	Major	The I/O latency increases as the QoS upper limits of the disk are frequently reached and flow control triggered.	Change the disk type to one with a higher specification.	The current disk may fail to meet service requirements.

Table 10-18 Identity and Access Management (IAM)

Event Source	Namespace	Event Name	Event ID	Event Severity
IAM	SYS.IAM	Login	login	Minor
		Logout	logout	Minor
		Password changed	changePassword	Major
		User created	createUser	Minor
		User deleted	deleteUser	Major
		User updated	updateUser	Minor
		User group created	createUserGroup	Minor
		User group deleted	deleteUserGroup	Major
		User group updated	updateUserGroup	Minor
		Identity provider created	createIdentityProvider	Minor
		Identity provider deleted	deleteIdentityProvider	Major
		Identity provider updated	updateIdentityProvider	Minor
		Metadata updated	updateMetadata	Minor
		Security policy updated	updateSecurityPolicies	Major
		Credential added	addCredential	Major
		Credential deleted	deleteCredential	Major
		Project created	createProject	Minor
		Project updated	updateProject	Minor
		Project suspended	suspendProject	Major

Table 10-19 Key Management Service (KMS)

Event Source	Namespace	Event Name	Event ID	Event Severity
KMS	SYS.KMS	Key disabled	disableKey	Major
		Key deletion scheduled	scheduleKeyDeletion	Minor
		Grant retired	retireGrant	Major
		Grant revoked	revokeGrant	Major

Table 10-20 Object Storage Service (OBS)

Event Source	Namespace	Event Name	Event ID	Event Severity
OBS	SYS.OBS	Bucket deleted	deleteBucket	Major
		Bucket policy deleted	deleteBucketPolicy	Major
		Bucket ACL configured	setBucketAcl	Minor
		Bucket policy configured	setBucketPolicy	Minor

Table 10-21 Cloud Eye

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution
Cloud Eye	SYS.CES	Agent heartbeat interruption	agentHeartbeatInterrupted	Major	The collecting process of the Agent is faulty.	• Confirm that the Agent domain name cannot be resolved. • Check whether your account is in arrears. • The Agent process is faulty. Restart the Agent. If the Agent process is still faulty after the restart, the Agent files may be damaged. In this case, reinstall the Agent. • Confirm that the server time is inconsistent with the local standard time. • If the DNS server is not a Huawei Cloud DNS server, run the **dig** *domain name* command to obtain the IP address of **agent.ces.myhuaweicloud.com** which is resolved by the Huawei Cloud DNS server over the intranet and then add the IP address

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution
						into the corresponding **hosts** file. • Update the Agent to the latest version.
		Agent back to normal	agentResumed	Informational	The Agent was back to normal.	No action is required.
		Agent faulty	agentFaulty	Major	The Agent was faulty and this status was reported to Cloud Eye.	The Agent process is faulty. Restart the Agent. If the Agent process is still faulty after the restart, the Agent files may be damaged. In this case, reinstall the Agent. Update the Agent to the latest version.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution
		Agent disconnected	agentDisconnected	Major	The communication process of the Agent is faulty.	Confirm that the Agent domain name cannot be resolved. Check whether your account is in arrears. The Agent process is faulty. Restart the Agent. If the Agent process is still faulty after the restart, the Agent files may be damaged. In this case, reinstall the Agent. Confirm that the server time is inconsistent with the local standard time. If the DNS server is not a Huawei Cloud DNS server, run the **dig** *domain-name* command to obtain the IP address of **agent.ces.myhuaweicloud.com** which is resolved by the Huawei Cloud DNS server over the intranet, and then add the IP address into the corresponding **hosts** file. Update the Agent to the latest version.

Table 10-22 DataSpace

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
DataSpace	SYS.HWDS	New revision	newRevision	Minor	An updated version was released.	After receiving the notification, export the data of the updated version as required.	None.

Table 10-23 Enterprise Switch

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
Enterprise Switch	SYS.ESW	IP addresses conflicted	IPConflict	Major	A cloud server and an on-premises server that need to communicate use the same IP address.	Check the ARP and switch information to locate the servers that have the same IP address and change the IP address.	The communications between the on-premises and cloud servers may be abnormal.

Table 10-24 Cloud Secret Management Service (CSMS)

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
CSMS	SYS.CSMS	Operation on secret scheduled for deletion	operateDeletedSecret	Major	A user attempts to perform operations on a secret that is scheduled to be deleted.	Check whether the scheduled secret deletion needs to be canceled.	The user cannot perform operations on the secret scheduled to be deleted.

Table 10-25 Distributed Cache Service (DCS)

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
DCS	SYS.DCS	Full sync retry during online migration	migrationFullResync	Minor	If online migration fails, full synchronization will be triggered because incremental synchronization cannot be performed.	Check whether full sync retries are triggered repeatedly. Check whether the source instance is connected and whether it is overloaded. If full sync retries are triggered repeatedly, contact O&M personnel.	The migration task is disconnected from the source instance, triggering another full sync. As a result, the CPU usage of the source instance may increase sharply.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Automatic failover	masterStandbyFailover	Minor	The master node was abnormal, promoting a replica to master.	Check whether services can recover by themselves. If applications are not recovered, restart them.	Persistent connections to the instance are interrupted.
		Memcached master/standby switchover	memcachedMasterStandbyFailover	Minor	The master node was abnormal, promoting the standby node to master.	Check whether services can recover by themselves. If applications cannot recover, restart them.	Persistent connections to the instance will be interrupted.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Redis server abnormal	redisNodeStatusAbnormal	Major	The Redis server status was abnormal.	Check whether services are affected. If yes, contact O&M personnel.	If the master node is abnormal, an automatic failover is performed. If a standby node is abnormal and the client directly connects to the standby node for read/write splitting, no data can be read.
		Redis server recovered	redisNodeStatusNormal	Major	The Redis server status recovered.	Check whether services can recover. If the applications are not reconnected, restart them.	Recover from an exception.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Sync failure in data migration	migrateSyncDataFail	Major	Online migration failed.	Reconfigure the migration task and migrate data again. If the fault persists, contact O&M personnel.	Data migration fails.
		Memcached instance abnormal	memcachedInstanceStatusAbnormal	Major	The Memcached node status was abnormal.	Check whether services are affected. If yes, contact O&M personnel.	The Memcached instance is abnormal and may not be accessed.
		Memcached instance recovered	memcachedInstanceStatusNormal	Major	The Memcached node status recovered.	Check whether services can recover. If the applications are not reconnected, restart them.	Recover from an exception.
		Instance backup failure	instanceBackupFailure	Major	The DCS instance fails to be backed up due to an OBS access failure.	Retry backup manually.	Automated backup fails.

Event Source	Name space	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Instance node abnormal restart	instanceNodeAbnormalRestart	Major	DCS nodes restarted unexpectedly when they became faulty.	Check whether services can recover by themselves. If applications cannot recover, restart them.	Persistent connections to the instance will be interrupted.
		Long-running Lua scripts stopped	scriptsStopped	Informational	Lua scripts that had timed out automatically stopped running.	Optimize Lua scrips to prevent execution timeout.	The execution of the lua scripts takes a long time and is forcibly interrupted. If the execution of the lua scripts takes a long time, the entire instance will be blocked.
		Node restarted	nodeRestarted	Informational	After write operations had been performed, the node automatically restarted to stop Lua scripts that had timed out.	Check whether services can recover by themselves. If applications cannot recover, restart them.	Persistent connections to the instance will be interrupted.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Bandwidth scaling	bandwidthAutoScalingTriggered	Informational	Instance bandwidth used up.	Check the services on this instance.	A bandwidth increase incurs fees.
		Specification auto scaling triggered	specAutoScalingTriggered	Informational	Specifications auto scaling was triggered.	Check the services on this instance.	The instance specifications were used up, triggering auto scaling. The billing will be changed if the instance specifications are changed.
		Specifications scaled	specAutoScalingTriggeredSuccess	Informational	The instance specifications were scaled successfully.	Check the services on this instance.	Instance scaled up. Check its information.
		Scale specifications failed	specAutoScalingTriggeredFail	Critical	The instance specifications fail to be scaled.	Contact technical support.	Instance scaling failed. Log in to the console to check whether services are affected.

Table 10-26 Intelligent Cloud Access (ICA)

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
ICA	SYS.ICA	BGP peer disconnection	BgpPeerDisconnection	Major	The BGP peer is disconnected.	Log in to the gateway and locate the cause.	Service traffic may be interrupted.
		BGP peer connection success	BgpPeerConnectionSuccess	Major	The BGP peer is successfully connected.	None	None
		Abnormal GRE tunnel status	AbnormalGreTunnelStatus	Major	The GRE tunnel status is abnormal.	Log in to the gateway and locate the cause.	Service traffic may be interrupted.
		Normal GRE tunnel status	NormalGreTunnelStatus	Major	The GRE tunnel status is normal.	None	None
		WAN interface goes up	EquipmentWanGoingOnline	Major	The WAN interface goes online.	None	None
		WAN interface goes down	EquipmentWanGoingOffline	Major	The WAN interface goes offline.	Check whether the event is caused by a manual operation or device fault.	The device cannot be used.
		Intelligent enterprise gateway going online	IntelligentEnterpriseGatewayGoingOnline	Major	The intelligent enterprise gateway goes online.	None	None

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Intelligent enterprise gateway going offline	IntelligentEnterpriseGatewayGoingOffline	Major	The intelligent enterprise gateway goes offline.	Check whether the event is caused by a manual operation or device fault.	The device cannot be used.

Table 10-27 Multi-Site High Availability Service (MAS)

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
MAS	SYS.MAS	Abnormal database instance	dbError	Major	Abnormal database instance is detected by MAS.	Log in to the MAS console to view the cause and rectify the fault.	Services are interrupted.
		Database instance recovered	dbRecovery	Major	The database instance is recovered.	None	Services are interrupted.
		Abnormal Redis instance	redisError	Major	Abnormal Redis instance is detected by MAS.	Log in to the MAS console to view the cause and rectify the fault.	Services are interrupted.
		Redis instance recovered	redisRecovery	Major	The Redis instance is recovered.	None	Services are interrupted.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Abnormal MongoDB database	mongodbError	Major	Abnormal MongoDB database is detected by MAS.	Log in to the MAS console to view the cause and rectify the fault.	Services are interrupted.
		MongoDB database recovered	mongodbRecovery	Major	The MongoDB database is recovered.	None	Services are interrupted.
		Abnormal Elasticsearch instance	esError	Major	Abnormal Elasticsearch instance is detected by MAS.	Log in to the MAS console to view the cause and rectify the fault.	Services are interrupted.
		Elasticsearch instance recovered	esRecovery	Major	The Elasticsearch instance is recovered.	None	Services are interrupted.
		Abnormal API	apiError	Major	The abnormal API is detected by MAS.	Log in to the MAS console to view the cause and rectify the fault.	Services are interrupted.
		API recovered	apiRecovery	Major	The API is recovered.	None	Services are interrupted.
		Area status changed	netChange	Major	Area status changes are detected by MAS.	Log in to the MAS console to view the cause and rectify the fault.	Network of the multi-active areas may change.

Table 10-28 Config

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
Config	SYS.RMS	Configuration noncompliance notification	configurationNoncompliance Notification	Major	The assignment evaluation result is **Non-compliant**.	Modify the noncompliant configuration items of the resource.	None
		Configuration compliance notification	configurationComplianceNotification	Informational	The assignment evaluation result changed to be **Compliant**.	None	None

Table 10-29 SecMaster

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
SecMaster	SYS.SecMaster	Exclusive engine creation failed	createEngineFailed	Major	The underlying resources are insufficient.	Submit a ticket to request sufficient resources from the O&M personnel and try again.	The exclusive engine cannot be created.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Exclusive engine exception	engineException	Critical	The traffic is too heavy or there are malicious processes or plug-ins.	1. Check the executions of plug-ins and processes, see if they occupy too many resources. 2. Check the instance monitoring information to see whether there is a sharp increase in the number of instances.	The instance cannot be executed.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Playbook instance execution failed	playbookInstanceExecFailed	Minor	Playbooks or processes are incorrectly configured.	Check the instance monitoring information to find the cause of the failure, and modify the playbook and process configuration.	None
		Playbook instance increased sharply	playbookInstanceIncreaseSharply	Minor	Playbooks or processes are incorrectly configured.	Check the instance monitoring information to find the cause of the increase, and modify the playbook and process configuration.	None
		Log messages increased sharply	logIncrease	Major	The upstream services suddenly generate a large number of log messages.	Check whether the upstream services are normal.	None

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Log messages decreased sharply	logsDecrease	Major	Logs generated by the upstream services suddenly decrease.	Check whether the upstream services are normal.	None

Table 10-30 Key Pair Service

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
KPS	SYS.KPS	Key pair deleted	KPSDeleteKeypair	Informational	A key pair was deleted. This operation cannot be undone.	If this event occurred frequently within a short period of time, check whether malicious deletion took place.	Deleted key pairs cannot be restored.

Table 10-31 Host Security Service (HSS)

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
HSS	SYS.HSS	HSS agent disconnected	hssAgentAbnormalOffline	Major	The communication between the agent and the server is abnormal, or the agent process on the server is abnormal.	Fix your network connection. If the agent is still offline for a long time after the network recovers, the agent process may be abnormal. In this case, log in to the server and restart the agent process.	Services are interrupted.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Abnormal HSS agent status	hssAgentAbnormalProtection	Major	The agent is abnormal probably because it does not have sufficient resources.	Log in to the server and check your resources. If the usage of memory or other system resources is too high, increase their capacity first. If the resources are sufficient but the fault persists after the agent process is restarted, submit a service ticket to the O&M personnel.	Services are interrupted.

Table 10-32 Image Management Service (IMS)

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
IMS	SYS.IMS	Create Image	createImage	Major	An image was created.	None	You can use this image to create cloud servers.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Update Image	updateImage	Major	Metadata of an image was modified.	None	Cloud servers may fail to be created from this image.
		Delete Image	deleteImage	Major	An image was deleted.	None	This image will be unavailable on the management console.

Table 10-33 Cloud Storage Gateway (CSG)

Event Source	Namespace	Event Name	Event ID	Event Severity	Description
CSG	SYS.CSG	Abnormal CSG process status	gatewayProcessStatusAbnormal	Major	This event is triggered when an exception occurs in the CSG process status.
		Abnormal CSG connection status	gatewayToServiceConnectAbnormal	Major	This event is triggered when no CSG status report is returned for five consecutive periods.
		Abnormal connection status between CSG and OBS	gatewayToObsConnectAbnormal	Major	This event is triggered when CSG cannot connect to OBS.
		Read-only file system	gatewayFileSystemReadOnly	Major	This event is triggered when the partition file system on CSG becomes read-only.

Event Source	Name space	Event Name	Event ID	Event Severity	Description
		Read-only file share	gatewayFileShareReadOnly	Major	This event is triggered when the file share becomes read-only due to insufficient cache disk storage space.

Table 10-34 Global Accelerator

Event Source	Name space	Event Name	Event ID	Event Severity	Description	Solution	Impact
GA	SYS.GA	Anycast IP address blocked	blockAIP	Critical	The used bandwidth of an EIP exceeded 5 Gbit/s, the EIP were blocked and packets were discarded. Such an event may be caused by DDoS attacks.	Locate the root cause and rectify the fault.	Services are affected. The traffic will not be properly forwarded.
		Anycast IP address unblocked	unblockAIP	Critical	The anycast IP address was unblocked.	Ensure that traffic can be properly forwarded.	None

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Unhealthy endpoint	healthCheckError	Major	Health check detects the endpoint unhealthy.	Perform operations as described in **What Should I Do If an Endpoint Is Unhealthy?** If the endpoint is still unhealthy, submit a service ticket.	If an endpoint is considered unhealthy, traffic will not be forwarded to it until the endpoint recovers.
		Unavailable endpoint	endpointAssociatedResourceChanged	Critical	The resource added as an endpoint is unavailable.	Add the resource as a new endpoint.	The network is disconnected.

Table 10-35 Enterprise connection

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
EC	SYS.EC	WAN interface goes up	EquipmentWanGoesOnline	Major	The WAN interface goes online.	None	None

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		WAN interface goes down	EquipmentWanGoesOffline	Major	The WAN interface goes offline.	Check whether the event is caused by a manual operation or device fault.	The device cannot be used.
		BGP peer disconnection	BgpPeerDisconnection	Major	BGP peer disconnection	Check whether the event is caused by a manual operation or device fault.	The device cannot be used.
		BGP peer connection success	BgpPeerConnectionSuccess	Major	The BGP peer is successfully connected.	None	None
		Abnormal GRE tunnel status	AbnormalGreTunnelStatus	Major	Abnormal GRE tunnel status	Check whether the event is caused by a manual operation or device fault.	The device cannot be used.
		Normal GRE tunnel status	NormalGreTunnelStatus	Major	The GRE tunnel status is normal.	None	None
		Intelligent enterprise gateway going online	IntelligentEnterpriseGatewayGoesOnline	Major	The intelligent enterprise gateway goes online.	None	None

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Intelligent enterprise gateway going offline	IntelligentEnterpriseGatewayGoesOffline	Major	The intelligent enterprise gateway goes offline.	Check whether the event is caused by a manual operation or device fault.	The device cannot be used.

Table 10-36 Cloud Certificate Manager (CCM)

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
CCM	SYS.CCM	Certificate revocation	CCMRevokeCertificate	Major	The certificate enters into the revocation process. Once revoked, the certificate cannot be used anymore.	Check whether the certificate revocation is really needed. Certificate revocation can be canceled.	If a certificate is revoked, the website is inaccessible using HTTPS.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Certificate auto-deployment failure	CCMAutoDeploymentFailure	Major	The certificate fails to be automatically deployed.	Check service resources whose certificates need to be replaced.	If no new certificate is deployed after a certificate expires, the website is inaccessible using HTTPS.
		Certificate expiration	CCMCertificateExpiration	Major	An SSL certificate has expired.	Purchase a new certificate in a timely manner.	If no new certificate is deployed after a certificate expires, the website is inaccessible using HTTPS.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Certificate about to expire	CCMcertificateAboutToExpiration	Major	This alarm is generated when an SSL certificate is about to expire in one week, one month, and two months.	Renew or purchase a new certificate in a timely manner.	If no new certificate is deployed after a certificate expires, the website is inaccessible using HTTPS.
		Private certificate is about to expire	CCMPrivateCertificateAboutToExpiration	Major	A private certificate is considered about to expire if it is within 7 or 30 days of its expiration date.	Purchase a new private certificate in a timely manner.	If no new private certificate has been deployed before certificate expires, services may be interrupted.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Private CA is about to expire	CCMPrivateCAAboutToExpiration	Major	A private CA is considered about to expire if it is within one month, three months, or six months of its expiration date.	Purchase a new private CA in a timely manner.	If no new CA has been deployed before a private CA expires, services may be interrupted.

Table 10-37 Workspace

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
Workspace	SYS.Workspace	Abnormal desktop heartbeat	desktopStatusAbnormal	Major	The network is disconnected or the key is lost.	1. Restart the desktop. 2. Check whether the desktop time is the current time. If not, change the desktop time to the current time. 3. Check whether special security software or network connection	The desktop cannot be accessed.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
						software is installed on the desktop. If so, uninstall the software and restart the system. Alternatively, uninstall the software, reinstall the HDC Agent, and restart the system.	

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Failure of assigning desktops in a desktop pool	desktopPoolAssignFailed	Major	This fault is caused by policies.	1. Adjust the desktop pool policy to ensure that there are idle desktops in the desktop pool or desktops can be automatically created. 2. If Linux desktops cannot be assigned to users with digit-only usernames, enabl	New desktops cannot be assigned.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
						e the username prefix function.	

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Desktop access failure	desktopAccessFailed	Major	This fault is caused by VM stopping and restart, access gateway exceptions, or network faults.	1. If you stop or restart a VM, wait for a period of time and try again when the desktop status is normal. 2. Check the network environment and reconnect to the network when the network is normal.	The desktop cannot be accessed.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Desktop startup failure	desktopStartFailed	Major	The underlying resources are insufficient.	Wait for a while and try again.	The desktop cannot be accessed.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Failure of automatic desktop pool capacity expansion	desktopPoolExpandFailed	Major	The instance quota or underlying resources are insufficient.	1. If the quota is insufficient, request a higher quota (such as the number of desktops, CPUs, memory, and VPCs). 2. If underlying resources are insufficient, make purchases in the next capacity expansion period.	Desktop capacity cannot be expanded.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
						3. If automatic desktop capacity expansion is not required, disable the function of automatic desktop pool capacity expansion.	

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Failure of migrating a desktop running on a dedicated host	desktopMigrateFailed	Major	The host malfunctions.	1. Replace the faulty host with a normal one. 2. Contact technical support to rectify the host fault.	No dedicated host is available for desktop scheduling.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		User login failure	userLoginFailed	Major	The client network is disconnected, or the enterprise ID, username, or password is incorrect.	1. Check the network environment and reconnect to the network when the network is normal. 2. Check whether the enterprise ID, username, and password are valid.	Desktops or applications are unavailable.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Screen recording failure	screenRecordFailed	Major	An unknown exception occurred on the desktop.	1. Try reconnecting to the desktop. 2. Check whether special security software is installed on the desktop. If it is, uninstall the software and restart the system.	Screen recording malfunctions and the desktop is disconnected.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Screen recording upload failure	screenRecordUploadFailed	Major	The network between the desktop and OBS malfunctions.	1. Check whether the desktop network is normal. 2. Check whether security group interception has been configured. 3. Check whether interception on access control with VPCEP and OBS has been configured.	Screen recording file upload failed.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Damaged screen recording file	screenRecordFileDamaged	Major	The screen recording file was maliciously damaged.	1. Wait until the screen recording function is automatically restored. 2. Check whether malicious damage occurs.	The screen recording file is abnormal.
		Abnormal agent process	agentAbnormal	Major	The agent process has been killed or reset.	The agent process can be automatically restarted after being killed.	Functions such as application control and upgrade will be affected.
		Bypassing controlled applications	appRestrictFailed	Major	The application control agent was continuously killed.	Check whether a script is used to continuously kill the application control agent.	Application control will fail.

